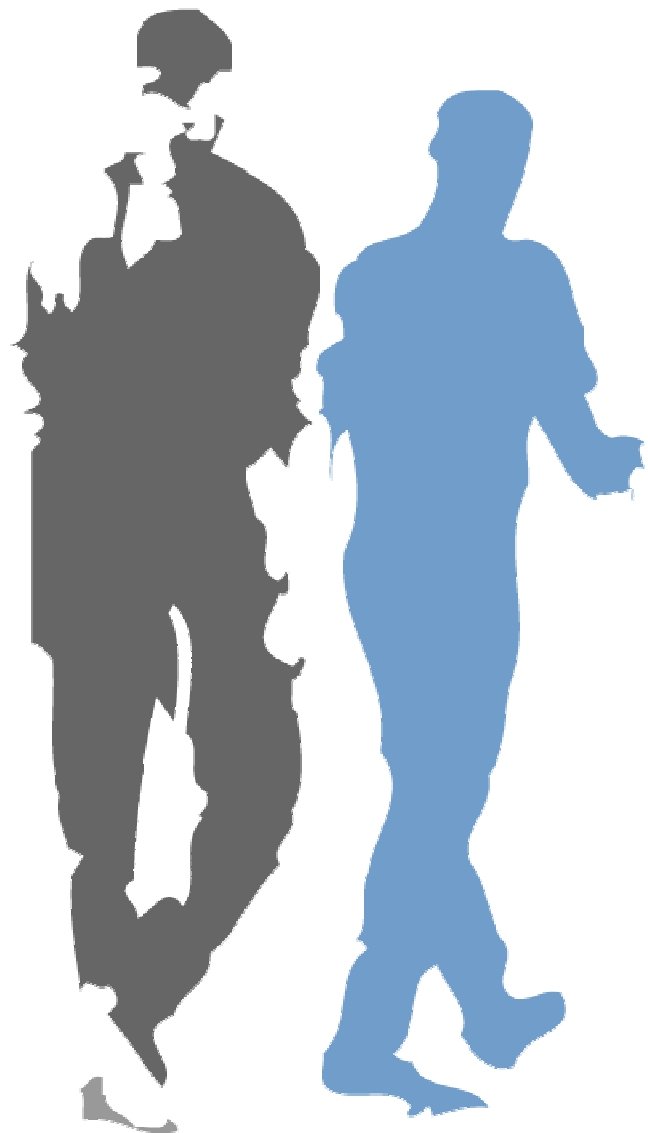milestone
XProtect

Enterprise 5.6
Complete Manual

milestone

Target Audience for this Document

This document covers all applications in Milestone XProtect Enterprise, and is therefore primarily aimed at Milestone XProtect Enterprise system administrators.

This document provides detailed descriptions of Milestone XProtect Enterprise applications, features, windows and fields. It furthermore provides a number of targeted "how-to" examples, guiding users through completing common tasks in Milestone XProtect Enterprise.

Users who do not have surveillance system administrator responsibilities—such as users of Milestone XProtect Enterprise's *Monitor* and *Viewer*, or users accessing the surveillance system through Milestone XProtect Enterprise's *Remote Client* or *Smart Client* applications—may find that large parts of this manual are not relevant to them. Such users will be able to find information targeted at their needs in the separate *Monitor & Viewer*, *Remote Client* and *Smart Client* manuals available on the Milestone XProtect Enterprise software CD as well as from www.milestonesys.com.

Contents

Introduction

Product Overview

With the purchase of Milestone XProtect Enterprise you have chosen an extremely powerful, flexible and intelligent surveillance solution.

Milestone XProtect Enterprise provides a state-of-the-art IP video surveillance system, supporting the widest choice of network cameras and video servers, with the equipment connected to an office LAN or other TCP/IP network, such as the internet.

Milestone XProtect Enterprise is the perfect choice for large installations. Milestone XProtect Enterprise handles an unlimited number of cameras (up to 64 cameras per server), multiple servers and multiple sites. It is a top performance solution, well suited to the sophisticated high-end of the security market.

Milestone XProtect Enterprise is:

- *Compatible* with more than 90 different IP video products from the leading manufacturers, so you choose the hardware you want—in combinations too

- *Dependable*; with robust and stable performance proven in operation on more than 90,000 cameras worldwide

- *Flexible*; with remote access features that let you use the surveillance system from any place and at any time, using a PC, laptop or PDA

- *Scalable*; with open architecture based on IP technology with ongoing development and regular updates, which gives you long-term returns on your surveillance investment

- *Future-safe*; the IP network approach is the foundation for tomorrow—available today

Several Targeted Applications in One

Milestone XProtect Enterprise consists of a number of applications, each targeted at specific tasks and user types:

- **The *Administrator* application** (see page 30): Used by the surveillance system administrator for configuring Milestone XProtect Enterprise, including the *Monitor* application, upon installation or whenever configuration adjustments are required, e.g. when adding new cameras or users to the system.

- **The *Monitor* application** (see page 133): The main user interface in day-to-day operation, the *Monitor* is used for recording and displaying images from connected cameras, with optional indications of registered activity.
  Camera images are only transferred to Milestone XProtect Enterprise while the *Monitor* is running. Depending on user rights and configuration, the *Monitor* may also be used for controlling PTZ (Pan/Tilt/Zoom) cameras, for manually starting and stopping cameras, for manually triggering outputs, etc.

- **The *Image Server Administrator* application** (see page 162): Used by the system administrator to manage access to the surveillance system for remote users logging in to the surveillance system with the *Remote Client* or *Smart Client*.

The *Image Server* itself does not require separate hardware; it runs as a service on the computer running the Milestone XProtect Enterprise software.

- **The *Remote Client*** (see page 171) **and *Smart Client*** (see page 210): Choice of two types of remote access clients, each providing users with intuitive remote access to the surveillance system.

  The *Remote Client* and *Smart Client* let users view live images, play back recorded images, activate outputs, print and export evidence, etc.

  The *Remote Client* can be installed locally on remote users' computers, or the users can access it straight from the surveillance system server through an Internet Explorer browser.

  The extra feature-rich *Smart Client* is installed on remote users' computers.

- **The *Web Server* and *RealtimeFeed Server*** (see page 251): Alternatives to the *Image Server*/*Remote Client*/*Smart Client* for providing remote access to the surveillance system, the *Web Server* and *RealtimeFeed Server* let system administrators manage remote access.

  Remote users access the *Web Server* and *RealtimeFeed Server* through an Internet Explorer browser.

Tip: For total freedom, you can also use the Milestone XProtect PDA Client for convenient remote access to the surveillance system. The Milestone XProtect PDA Client is a separate product, purchased in addition to Milestone XProtect Enterprise.

Updates

Milestone Systems regularly release service updates for our products, offering improved functionality and support for new devices.

If you are a Milestone XProtect Enterprise system administrator, it is recommended that you check the Milestone Systems website www.milestonesys.com for updates at regular intervals in order to make sure you are using the most recent version of Milestone XProtect Enterprise.

Tip: Customers with a valid Product Maintenance Agreement (read more in the following) are automatically notified when an update becomes available.

Product Maintenance Agreement (PMA)

As the cornerstone of its support to customers, Milestone Systems offers a Product Maintenance Agreement (PMA).

The first six months' PMA is free of charge and included in the standard license price for Milestone XProtect Enterprise. Additional PMA coverage can easily be purchased together with a new Milestone XProtect Enterprise product, but cannot be bought as an add-on to a previously bought product.

During the period covered by the PMA, customers are entitled to receive all generally-released new versions of their Milestone software, including both interim and major releases, changes, service packs and any patches for the product.

When an update becomes available, customers with a valid PMA are automatically notified via e-mail.

Having a valid PMA may easily lead to measurable savings for your organization: The standard cost of a product upgrade (for example from version X.1 to X.2) is normally 35% of the full product's recommended retail price; with a PMA it would never be more than 18% of the full product's recommended retail price.

Read more about PMAs on the Milestone Systems website, www.milestonesys.com.

System Requirements

Server

The following are minimum system requirements for the server running Milestone XProtect Enterprise:

Operating System	Windows 2000 Pro, Windows 2000 Server, Windows XP Pro, Windows 2003 server. It is highly recommended that the latest service pack for the operating system is installed.
CPU	Single or multiple CPUs, limited only by operating system; Intel recommended for optimum performance.
RAM	Minimum 1 GB.
Network	Ethernet 100 Mbit/s.
Video Card	AGP (minimum 1024×768).
Video Colors	True 24-bit.
Hard Disk	E-IDE (7200 rpm recommended); for best performance use Fast SCSI.

DirectX 9.0 must be installed on the server.

Tip: Visit the Milestone website, www.milestonesys.com, for the most recent system performance parameters.

Users' Computers

The following is required on users' computers:

- Internet Explorer 6.0

- DirectX 9.0

    Tip: DirectX is a Windows extension providing advanced multimedia capabilities; these capabilities are required when using the *Remote Client* and *Smart Client* to connect to the Milestone XProtect Enterprise surveillance system. To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type *dxdiag*. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. Latest DirectX versions are available from http://www.microsoft.com/downloads/.

- .Net Framework 1.1, available from http://www.microsoft.com/downloads/, is required on computers running the *Smart Client*.

Administrators' Getting Started Checklist

This chapter outlines the tasks typically involved in setting up a working Milestone XProtect Enterprise system. The information in this chapter is primarily aimed at system administrators.

Note that although information in this chapter is presented as a checklist, a completed checklist does not in itself guarantee that the Milestone XProtect Enterprise system will match the exact needs of your organization. To make the system match the needs of your organization, it is highly recommended that you monitor and adjust the system once it is running.

For example, it is often a very good idea to spend some time on testing and adjusting the motion detection sensitivity settings for individual cameras under different physical conditions (day/night, windy/calm, etc.) once the system is running.

☑ You may check the boxes in this checklist as you go along.

☐ **Verify Initial Configuration of Devices**. Make sure the devices (IP network cameras or IP video servers) you are going to use are configured with IP addresses, passwords, etc. as specified by the manufacturer.

Such initial configuration is required in order to be able to connect the devices to the network and the Milestone XProtect Enterprise solution.

☐ **Obtain Device License Keys**. You must have a Device License Key (DLK) for each device (IP network camera or IP video server) to be used with the Milestone XProtect Enterprise solution.

You obtain DLKs through the *Software Registration* section of the Milestone Systems website, www.milestonesys.com. When ready, the DLKs will be sent to you via e-mail.

Note that you are only allowed to use the number of cameras listed on your license sheet, regardless of the number of available DLKs. For example, a fully used four-port video server counts as four cameras even if it only requires a single DLK to install.

☐ **Install Milestone XProtect Enterprise** (see *Installing Milestone XProtect Enterprise* on page 26).

☐ **Import Device License Keys** (see *How to Import Device License Keys (DLKs)* on page 35).

☐ **Add Devices** (see *How to Add a device* on page 36).

In Milestone XProtect Enterprise you do not have to worry about having to add individual cameras to the system. This is because cameras area connected to devices, so once you have added the required devices to your Milestone XProtect Enterprise system, all cameras connected to the devices are connected to the system as well.

☐ **Configure Cameras on Milestone XProtect Enterprise**. You are able to specify a wide variety of settings for each camera connected to the Milestone XProtect Enterprise system.

Your entry point for configuring cameras is the *Administrator* window, the main window in Milestone XProtect Enterprise's *Administrator* application (see page 30).

To configure a camera, first select the required device in the *Administrator* window's *Device Manager* section, then click the plus sign next to the device to view a list of cameras attached to the device, as illustrated in the following:

Select the required camera from the list, and click the *Administrator* window's *Settings* button. This will open the *Camera Settings for [Device Name] [Camera Name]* window, in which you are able to specify settings for the camera in question.

Settings include the highly important motion detection sensitivity settings. They also include PTZ (Pan/Tilt/Zoom) preset position settings for any PTZ cameras supporting preset positions on your system.

The *Camera Settings for [Device Name] [Camera Name]* window is described in detail on page 44.

☐ **Configure the *Monitor* Layout**. To include cameras for display in the *Monitor* application, you use the *Monitor Manager* feature in the *Administrator* application.

The *Monitor Manager* feature is described in detail on page 71.

☐ **Configure Milestone XProtect Enterprise's General Settings**. The *Administrator* application's *General Settings* window lets you configure a number of important settings related to user rights, logging, e-mail and SMS accounts, etc.

The *General Settings* window is described in detail on page 79.

☐ **Configure Scheduling**. You may want some cameras to be transferring images to Milestone XProtect Enterprise at all times, whereas you may want other cameras to transfer images only within specific periods of time, or when specific events occur.

With Milestone XProtect Enterprise's scheduling feature, you are able to specify when each camera should transfer images to the *Monitor*.

You are also able to specify whether alerts should be triggered if motion is detected during specific periods of time.

For PTZ cameras with patrolling (the automatic movement of a camera between several preset positions), you are furthermore able to specify whether any specific patrol schemes should be used during specific periods of time.

You configure scheduling in the *Administrator* application's *Camera/Alert Scheduler* window, described in detail on page 74.

☐ **Configure Archiving**. By default, images received from camera are stored by Milestone XProtect Enterprise in a database for each camera. However, the camera databases are each capable of containing a maximum of 600.000 records or 40 GB before the oldest records are deleted.

By using Milestone XProtect Enterprise's archiving feature, you are able to overcome these limitations by automatically moving the contents of camera databases to specified archiving locations one or more times every day.

With archiving the amount of records you will be able to store will thus be limited only by your available hardware storage capacity.

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

Archiving is described in detail on page 124.

☐ **Configure the *Image Server*.** The *Image Server* is the service handling *Remote Client* and *Smart Client* access to the Milestone XProtect Enterprise system.

Remote Clients (see page 171) and *Smart Clients* (see page 210) are included in your Milestone XProtect Enterprise license, and provide flexible, client/server based, remote access to the Milestone XProtect Enterprise system, with 16-channel viewing live or recordings from multiple servers simultaneously.

If you are going to use *Remote Clients* or *Smart Clients*, configuring the *Image Server* is a prerequisite. Configuration includes specifying whether the *Image Server* should be accessible from the internet, specifying user rights, etc.

You configure the *Image Server* through the *Image Server Administrator* window, described in detail on page 162.

Installing Milestone XProtect Enterprise

Note: Read the License Terms on the Product License Sheet (enclosed with the software CD) before installing Milestone XProtect Enterprise.

To install Milestone XProtect Enterprise, do the following:

1. Shut down any Milestone software running, including any Web and RealtimeFeed Servers. If upgrading, it is highly recommended that you remove (see page 265) any previous versions of Milestone XProtect before upgrading.

2. Insert the Milestone XProtect Enterprise software CD. If the installation wizard does not start automatically when inserting the CD, run the following file from the CD:

   `MilestoneXProtectEnterprise.exe`

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

3. When the installation wizard starts, click *Next* to continue the installation.

4. Read and accept the License Agreement.

5. Select required language version, and click *Next*.

6. Select the *Licensed Version* option, and click *Next*.

7. Type your Software License Code, as listed on your Product License Sheet.

   You have the option of installing the software for anyone using the computer, or for yourself only.

   If installing for yourself only, bear in mind that if your login is not an administrator login, you will need to change the login name for the *Image Server* service (see page 162) so it matches your own login, i.e. uses the same user name and password.

8. Follow the remaining steps in the installation wizard, and click *Finish* on the last step to complete the installation.

Milestone XProtect Enterprise 5.6; Complete Manual

Using the Built-in Help System

To use Milestone XProtect Enterprise's built-in help system, simply press F1 on your keyboard whenever you are working in the *Administrator*, *Monitor* or *Image Server*.

When you press F1, Milestone XProtect Enterprise's built-in help system will open in a separate window, allowing you to easily switch between help and Milestone XProtect Enterprise itself.
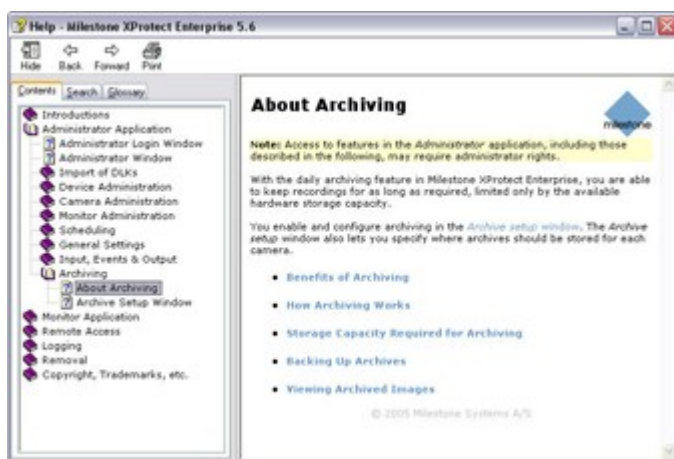
Example of the Milestone XProtect Enterprise help window

The built-in help system in Milestone XProtect Enterprise is context sensitive. This means that when you press F1 for help while working in a particular Milestone XProtect Enterprise window, the help system automatically displays the help topic describing that window.

Navigating the Built-in Help System

Even though the help system initially takes you to a topic describing the window you are working in, you are always able to freely navigate between the help system's contents. To do this, simply use the help window's three tabs: *Contents*, *Search* and *Glossary,* or use the links inside the help topics.

Help system's three tabs

Contents Tab

The *Contents* tab lets you navigate the help system based on a tree structure. Many users will be familiar with this type of navigation from, for example, Windows Explorer.

Search Tab

The *Search* tab lets you search for help topics containing particular terms of interest. For example, you can search for the term *camera*, and every help topic containing the term *camera* will be listed in the search results. Clicking a help topic title in the search results list will open the required topic.

The *Search* tab contains a number of advanced search features; among these are the ability to quickly run previous searches, the ability to search topic titles only as well as the ability to display search results ranked according to presumed relevance.

Example of help system's *Search* tab

Glossary Tab

What do abbreviations such as DLK, PTZ or SMTP stand for? The *Glossary* tab in the help window's navigation pane provides a glossary of common surveillance and network-related terms.

Simply select a term to view a corresponding definition in the small window below the list of terms.

Three Types of Links in Help Topics

The actual content of each help topic is displayed in the right pane of the help window. Help topic texts may contain three types of links. Each type of link is described in the following:

Links to Related Topics

Clicking this type of link will take you to another topic within the help system.

Expanding Drop-Down Links

Clicking this type of link will display detailed information about a specific part of the help topic; for example a detailed description of a particular feature in one of Milestone XProtect Enterprise's windows.

The detailed information is displayed immediately below the link itself; you are not taken to another page, instead the content on the current page simply expands.

Expanding drop-down links help save space; without them some detailed help topics would appear overly long and difficult to get an overview of.

Links to External Resources

Clicking this type of link will open an external resource in a separate browser window.

Tip: If you wish to quickly collapse all texts from expanding drop-down links in a help topic, simply click the title of the topic in the help system's Contents menu.

Printing Help Topics

To print a help topic, navigate to the required topic and click the help window's *Print* button.

Print
Help window's *Print* button

When you click the *Print* button, a dialog box may ask you whether you wish to print the selected topic only or all topics under the selected heading. When this is the case, select *Print the selected topic* and click *OK*.
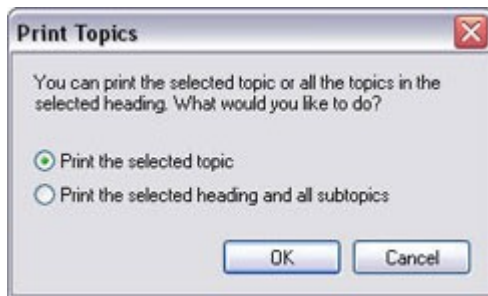
Print Topics Dialog

When printing a selected help topic, the topic will be printed as you see it on your screen. Therefore, if a topic contains expanding drop-down links (see *Three Types of Links in Help Topics* on page 28), click each required drop-down link to display the text in order for it to be included in your printout. This allows you to create targeted printouts, containing exactly the amount of information you require.

Administrator Application

Milestone XProtect Enterprise's *Administrator* application is used by the surveillance system administrator for configuring Milestone XProtect Enterprise, including the *Monitor* application, upon installation or whenever configuration adjustments are required, e.g. when adding new devices to the system.

Administrator Login Window

For users without administrator rights, access to certain features in Milestone XProtect Enterprise may in some organizations have been restricted.

When this is the case, you will be asked to specify the administrator password in the *Administrator Login* window in order to get access to the restricted features.

The *Administrator Login* window

You will only be asked to specify the administrator password in two situations:

- When you click the *Administrator* shortcut on the desktop in order to open the *Administrator* application. This will only be the case when access to the *Administrator* application has been password-protected.

- When you click the *Admin Login* button in the *Monitor* application (see page 133).

Administrator Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Administrator* window, the main window in the *Administrator* application, is used by the surveillance system administrator for configuring Milestone XProtect Enterprise.

Access: You access the *Administrator* window by clicking the *Administrator* shortcut on the desktop. If access from the *Monitor* application is enabled, the *Administrator* window may also be accessed from the *Monitor* application. Access to the *Administrator* window may be password protected, in which case you will be asked to provide the administrator password in the *Administrator Login* window.

The *Administrator* desktop shortcut
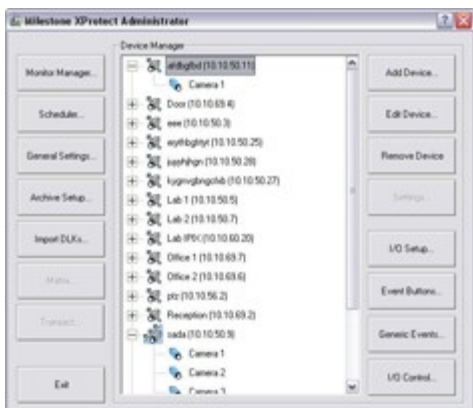
The *Administrator* window

The *Administrator* window features a *Device Manager* section as well as a number of buttons providing access to configuration.

Device Manager Section

The *Device Manager* section—located in the middle of the *Administrator* window—lists all added devices and attached cameras. The Device Manager section thus provides you with an overview of your surveillance system.

Detail from the Administrator window's Device Manager section—two devices have been added; the first device has a single camera attached, whereas the second device has four cameras attached

Until you have added devices, the *Device Manager* section will be empty.

Adding Devices

You add devices through an intuitive *Device Setup Wizard*, available by clicking the *Administrator* window's *Add Device* button. The process of adding devices is described in *How to Add a Device* on page 36.

When devices have been added, they will be listed in the *Device Manager* section.

Clicking the plus sign next to a device in the *Device Manager* section will list cameras attached to the device.

Editing Settings for Devices

To edit settings for a device listed in the *Device Manager* section, select the device, then click the *Edit device...* button to open the *Edit device settings* window (see page 38)*.*

Editing Settings for Cameras

To edit the settings for a camera listed in the *Device Manager* section, clicking the plus sign next to the device to which the camera is attached, select the required camera, then click the *Settings* button to open the *Camera Settings for [Device name] [Camera Name]* window (see page 44).

To rename a camera, select the required camera name in the *Device Manager* section, wait for a second, then select the camera name again to change it.

Disabling/Enabling Cameras

Individual cameras listed in the *Device Manager* section are by default enabled, meaning that images from the cameras are by default transferred to Milestone XProtect Enterprise—provided that the cameras are marked as *online* (also default) in the *Camera/Alert Scheduler* Window (see page 74).

If required, you can disable individual cameras listed in the *Device Manager* section. When a camera is disabled, no images will be transferred from the camera to Milestone XProtect Enterprise.

Note: If images from a camera are displayed in the *Monitor* application (configured in the *Monitor Manager* window, see page 71), the camera cannot be disabled. When this is the case, remove the camera from the *Monitor Manager* window's layout before disabling the camera.

To disable a camera, right-click the required camera in the *Device Manager* section, then select *Disable*:

When a camera is disabled, it will be indicated as follows:

To enable a previously disabled camera, simply right-click the required camera in the *Device Manager* section, then select *Enable*:

Tip: Individual cameras can also be disabled/enabled in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Administrator Window's Buttons

The *Administrator* window features the following buttons:

Button	Description
Monitor Manager...	Opens the *Monitor Manager* window (see page 71), in which you specify which cameras should record and display images in the *Monitor* application (see page 133). It also lets you configure the layout of the *Monitor* application.

Note: Camera images are only recorded and transferred to Milestone XProtect Enterprise while the *Monitor* application is running. |
| **Scheduler...** | Opens the *Camera/Alert Scheduler* window (see page 74), in which you |

specify online periods for each camera.

You are also able to specify if cameras should go online when specific events occur (e.g. when a door is opened), and if e-mail, SMS or sound alerts should be used if motion is detected during specific periods of time (e.g. during working hours). If using PTZ cameras with patrolling, you are furthermore able to specify if certain patrol schemes should be used during specific periods of time.

Tip: By default, all cameras are online at all times. You will only need to modify scheduler settings if you require cameras to be online only at specific times or events, or if you want to use specific alerts or PTZ patrol schemes.

General Settings...	Opens the *General Settings* window (see page 79), in which you specify a number of settings related to: • Administrator password • User rights • Milestone XProtect Central settings (if using Milestone XProtect Central monitoring solution in connection with Milestone XProtect Enterprise) • PTZ patrolling pause time out (if using PTZ cameras with patrolling) • Joystick setup for PTZ cameras • E-mail settings (for alerts sent via e-mail) • SMS settings (for alerts sent via SMS) • Log file settings • Event recording settings • Other advanced settings, such as the ability to disable screen update in order to minimize CPU usage
Archive Setup...	Opens the *Archive setup* window (see page 127), in which you specify Milestone XProtect Enterprise's archiving settings. Archiving lets you keep recordings for as long as required, limited only be the available hardware storage capacity.
Import DLKs...	Lets you import all required Device License Keys (DLKs) in one go, thus avoiding the need to specify each DLK manually when adding a device. See also *How to Import Device License Keys (DLKs)* on page 35.
Matrix...	**Note:** The *Matrix* button is only available if you are using the Milestone XProtect Matrix monitoring solution in connection with Milestone XProtect Enterprise. Lets you access Milestone XProtect Matrix configuration.
Transact...	**Note:** The *Transact* button is only available if you are using the Milestone XProtect Transact solution for integrating transactions monitoring with Milestone XProtect Enterprise. Lets you access Milestone XProtect Transact configuration.

Add Device...	Starts the *Device Setup Wizard*, which guides you through the process of adding a new device. See also *How to Add a Devic*e on page 36.
Edit Device...	To use the *Edit Device…* button, first select a device in the *Administrator* window's *Device Manager* section. When you have selected a device in the *Administrator* window's *Device Manager* section, clicking the *Edit Device...* button lets you edit settings for the selected device in the *Edit device settings* window (see page 38).
Remove Device	Lets you remove a device selected in the *Administrato*r window's *Device Manager* section. In order to prevent accidental removal of devices, you will be asked to confirm that you want to remove the device.
Settings...	Lets you specify settings for a particular camera. When you have selected a camera in the Administrator window's *Device Manager* section, clicking the *Settings* button will open the *Camera Settings for [Device Name] [Camera Name]* window (see page 44), in which you specify camera settings.
I/O Setup...	Opens the *I/O Setup* window (see page 93), in which you are able to define events based on external input (for example when a door sensor detects that a door is opened) and VMD (Video Motion Detection). The *I/O Setup* window also lets you specify output (e.g. a siren). When defined, events can be used for a variety of purposes. For example, an input event can be used for triggering output, for starting a particular camera, and for triggering that an e-mail or SMS message is sent to a particular user, notifying the user of the recorded event. See also the description of the *I/O Control...* button.
Event Buttons...	Opens the *Event Buttons* window (see page 106), in which you are able to define events for use on event buttons. Event buttons can be used in the Monitor application and Smart Client for manually triggering events.
Generic Events...	Opens the *Generic Events* window (see page 110), in which you are able to define events based on input from external sources using the TCP and UDP protocols.
I/O Control...	Opens the *I/O Control* window (see page 121), in which you are able to associate outputs with events. This way you can, for example, define that a siren should sound (output) when a sensor detects that a door is opened (input event).
Exit	Closes the *Administrator* application.

Device License Keys (DLKs)

How to Import Device License Keys (DLKs)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

You must have a Device License Key (DLK) for every device (IP network camera or IP video server) installed on your Milestone XProtect Enterprise surveillance system.

Remember that you are allowed to install and use only the number of cameras listed on your organization's license sheet; regardless of you number of available DLKs. For example, a fully used four-port video server device counts as four cameras even though it only requires a single DLK to install.

System administrators obtain DLKs as part of the software registration process on the Milestone website, www.milestonesys.com. Upon registration, DLKs are sent to system administrators via e-mail.

You are able to specify each DLK manually when adding a device through the *Device Setup Wizard*, available by clicking the *Add Device...* button in the *Administrator* window (see page 30). However, you can avoid having to specify each DLK manually by using the following procedure to import all received DLKs into Milestone XProtect Enterprise in one go:

Prerequisites: The DLKs, received in a .dlk file, must have been saved at a location accessible by the surveillance server, for example on a network drive or on a USB stick.

1. Open the *Administrator* window by clicking the *Administrator* shortcut on the desktop.

   The *Administrator* desktop shortcut

2. In the *Administrator* window, click the *Import DLKs...* button.

3. Browse to the location at which you have saved the received .dlk file.

   Select the file, and click *Open*.

   All DLKs are now automatically imported, and the relevant DLK will automatically appear when you add a device through the *Device Setup Wizard* (see *How to Add a Device* on page 36).

Device Administration

How to Add a Device

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

In Milestone XProtect Enterprise you add devices (IP video camera devices or IP video server devices) rather than actual cameras. This is because devices have their own IP addresses or host names. Being IP-based, Milestone XProtect Enterprise primarily identifies units on the surveillance system based on their IP addresses or host names.

Even though each device has its own IP address or host name, several cameras can be attached to a single device and thus share the same IP address or host name. This is typically the case with cameras attached to video server devices.

You can of course configure and use each camera individually, even when several cameras are attached to a single device.

In addition to IP video camera devices and IP video server devices it is possible to add a number of dedicated I/O (input/output) devices to Milestone XProtect Enterprise. When such I/O devices are added, they can be used in events-based system setup (see *About Input, Events and Output* on page 91) in the same way as a camera. For information about which I/O devices are supported, refer to the release note.

When a device is added in Milestone XProtect Enterprise, any cameras attached to the device are automatically recognized by the software, and listed in the *Administrator* window's *Device Manager* section:

Detail from the Administrator window's *Device Manager* section—two devices have been added; the first device has a single camera attached, whereas the second device has four cameras attached

To add a device, use the following procedure:

Prerequisites: You must have configured IP address, password, etc. on the device itself as described by the manufacturer.

1. Open the *Administrator* window (see page 30) by clicking the *Administrator* shortcut on the desktop.

    The *Administrator* desktop shortcut

2. In the *Administrator* window, click the *Add Device...* button.

    This will start the *Device Setup Wizard*.

3. On the first step of the wizard, identify the required device, either by

    - Typing the IP address of the device

      - or -

    - Typing the DNS host name of the device. This requires that you select the *Use DNS host names* box

Specifying the IP address of a device

Note: By default, HTTP port 80 and FTP port 21 will be used for the device. If the device you are adding uses other port numbers, click the *Port Setup* button and specify required port numbers. The need for specifying different ports may often apply if the device is located behind a NAT-enabled router or a firewall. When this is the case, also remember to configure the router/firewall so it maps the ports and IP address used by the device.

When ready, click *Next* to go to the second step of the wizard.

4. If a password is used for the device, type the password for the device's administrator account (called an "admin" or ""root" account on some devices).

    Leave the *Autodetect Device* option selected.

    Click *Next.*

5. When the device has been detected, type the Device License Key (DLK) for the device in the *DLK* field.

Specifying DLK for the device

🛈 **Tip:** If you have imported DLKs (see *How to Import Device License Keys* on page 35), the *DLK* field will already be filled with the DLK for the device.

Click *Next*.

6. Assign a unique and descriptive name to the device.

   Upon completion of the wizard, the name will be used when listing devices and associated cameras in the *Administrator* window's *Device Manager* section.

   The name may, for example, refer to the physical location of the camera(s) attached to the device.

Assigning a name to the device

   Tip: You may click the *Camera Setup* button to access the *Camera Settings for …* window (see page 41), in which you are able to specify certain settings related to camera name and PTZ control. The latter requires that the camera is a PTZ (Pan/tilt/Zoom) camera.

7. Click *Finish*.

8. The device will be listed in the *Administrator* window's *Device Manager* section.

   To view a list of cameras attached to the device, click the plus sign next to the device name.

   Tip: Cameras are listed for each device with default names, such as *Camera 1*, etc. If you want to change the name of a camera, simply select the required camera name, wait for a second, then select the camera name again to change it.

   Tip: Individual cameras listed in the *Device Manager* section are by default enabled, meaning that images from the cameras are by default transferred to Milestone XProtect Enterprise—provided that the cameras are marked as *online* (also default) in the *Camera/Alert Scheduler* Window (see page 74). If required, you can disable a camera listed in the *Device Manager* section by right-clicking the name of the camera in question. Read more information under *Administrator* window on page 32.

Edit Device Settings Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Edit device settings* window lets you edit the settings of an already installed device.

The *Edit device settings* window

Access: To access the Edit device settings window, select the required device in the *Device Manager* section of the *Administrator* window (see page 30), and click the *Edit Device...* button.

The *Edit device settings* window is divided into three sections: *Identify Video Device*, *Network Settings for Video device* and *Audio*.

Identify Video Device Section

The *Identify Video Device* section contains the following fields and buttons:

Field, Button	Description
Device Type	Select required device type from list. **Tip:** Milestone XProtect Enterprise is able to automatically detect device type as well as serial number, provided the IP address/hostname and password of the device have been specified in the *IP-address/DNS Host Name* and *Root Password* fields: Simply click the *Detect Device* button to auto-detect device type and serial number.
Detect Device	Click button to auto-detect device type and serial number. **Note:** Use of the auto-detect feature requires that the IP address and password of the device have been specified in the *IP-address* and *Root Password* fields.
Device Name	Name used to identify the device. **Tip:** To enable easy identification of devices, it is often a good idea to use a device name that refers to the physical area covered by the cameras attached to the device (examples: Reception Area, Car Park B, Entrance Door, ...). **Note:** Device names must be unique; you cannot use the same name for several devices.
Camera Settings...	Opens the *Camera Settings for [Device Name]* window (see page 41), in which you are able to specify a number of settings for cameras attached to the device: • Port through which PTZ (Pan/tilt/Zoom) cameras are controlled

	• Camera names, types, and ports **Note:** The number of settings available in the *Camera Settings for [Device Name]* window may be limited if cameras are not PTZ cameras or connected to a video server device.
Device Serial Number	Serial number of device; usually identical to the 12-character MAC address of the device (example: 0123456789AF). 🛈 **Tip:** Milestone XProtect Enterprise is able to automatically detect serial number as well as device type, provided the IP address/host name and password of the device have been specified in the *IP-address/DNS Host Name* and *Root Password* fields: Simply click the *Detect Device* button to auto-detect device type and serial number.
Device License Key	A 16-character license key (DLK) for the device, obtained when registering the software.
Enable iPIX	Enables the use of IPIX, a technology that allows viewing of 360-degree panoramic images. Check box is selected by default if the device in question is for a dedicated IPIX camera. **Note:** Use of the IPIX technology requires a dedicated IPIX camera or a special IPIX camera lens with a special IPIX license key.
iPIX License Key	License key for using the IPIX technology, obtained when registering the software. Only required if *Enable iPIX* check box is selected manually.

Network Settings for Video Device Section

The *Network Settings for Device* section contains the following fields:

Field	Description
IP-address -or- **DNS Host Name**	IP address or DNS host name of the device in question. **Note:** If *Use DNS host name* check box is selected, the name of the *IP-address* field changes to *DNS/Host Name* in order to accommodate a DNS host name rather than an IP address.
Use DNS host name	By selecting the check box you are able to use a DNS host name for identifying the device instead of using the device's IP address. When check box is selected, the *IP-address* field changes its name to *DNS/Host Name*, ready to accommodate a DNS host name rather than an IP address.
Default Http Port	When selected, HTTP traffic to the device will go through the default port, port 80.

	If you want to use another port for HTTP traffic to the device, clear the check box, and specify required port number in the field to the left of the check box.
Default Ftp Port	When selected, FTP traffic to the device will go through the default port, port 21. If you want to use another port for FTP traffic to the device, clear the check box, and specify required port number in the field to the left of the check box.
Root Password	Password required in order to log in to the device using the root account (occasionally known as an *admin* or *administrator* account).

Audio Section

The *Audio* section lets you enable audio on the device.

Select the *Audio Enabled* check box to enable audio.

Note: The use of audio requires that audio is supported by the device.

Camera Settings for [Device Name] Window

Note: The number of settings available in the *Camera Settings for [Device Name]* window may be limited if cameras are not PTZ (Pan/Tilt/Zoom) cameras or connected to a video server device. Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Camera Settings for [Device Name]* window lets you specify certain information about cameras. This is particularly interesting for PTZ cameras and cameras attached to a video server device.
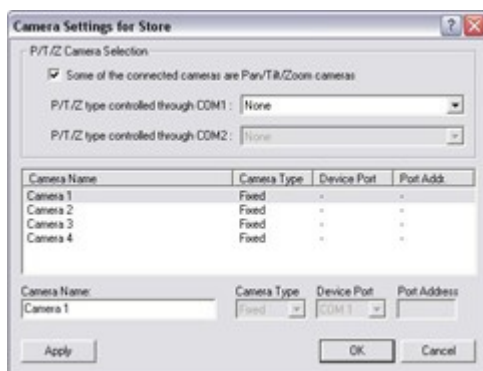
The *Camera Settings for [Device Name]* window

Access: You access the *Camera Settings for [Device Name] window* by clicking the *Camera Settings...* button in the *Edit device settings* window (see page 38).

The *Camera Settings for [Device Name]* window is divided into a *P/T/Z Camera Selection* section and an editable camera list.

P/T/Z Camera Selection Section

The *P/T/Z Camera selection* section contains the following fields:

Field	Description
Some of the connected cameras are Pan/Tilt/Zoom cameras	Select check box if any of the cameras attached to the video server device is a PTZ camera. If the check box is not available, PTZ is not supported for the device in question.
P/T/Z type controlled through COM1	Field available only if *Some of the connected cameras are Pan/Tilt/Zoom cameras* check box is selected. If a PTZ camera is controlled through the COM1 port on the video server device, select the required PTZ camera type from the list. If no PTZ cameras are controlled through the COM1 port, select *None*.
P/T/Z type controlled through COM2	Field available only if *Some of the connected cameras are Pan/Tilt/Zoom cameras* check box is selected. If a PTZ camera is controlled through the COM2 port on the video server device, select the required PTZ camera type from the list. If no PTZ cameras are controlled through the COM2 port, select *None*.

Camera List

The camera list contains a line for each camera channel on the device. First line from the top corresponds to camera channel 1, second line from the top corresponds to camera channel 2, etc.

To change camera settings, select the required camera channel from the list, specify required information in the following fields, and click the *Apply* button:

Field	Description
Camera Name	Name used to identify the selected camera. Existing names, such as the default camera names *Camera 1, Camera 2*, etc. can be changed by overwriting the existing names. **Note:** Camera names must be unique for each device.
Camera Type	Lets you select whether the camera on the selected camera channel is *Fixed* or *Moveable*: • *Fixed*: Camera mounted in a fixed position • *Moveable*: PTZ camera
Device Port	Available only if *Moveable* is selected in the *Camera Type* field. Lets you select which control port on the video server should be used for controlling PTZ functionality on the camera.

Port Address	Available only if *Moveable* is selected in the *Camera Type* field.
	Lets you specify port address of the camera. The port address would normally be *0* or *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 camera manuals.

Camera Administration

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Adding Cameras

In Milestone XProtect Enterprise you do not have to worry about having to add individual cameras to the system:

Cameras are connected to devices, so once you have added the required devices to your Milestone XProtect Enterprise system (see *How to Add a Device* on page 36), all cameras connected to the devices are connected to the system as well.

Configuring Cameras

You are able to specify a wide variety of settings for each camera connected to the Milestone XProtect Enterprise system. Your entry point for such camera configuration is the *Administrator* window (see page 30).

To configure a camera, select the required camera in the *Administrator* window's *Device Manager* section, then click the *Administrator* window's *Settings...* button.

This will open the *Camera Settings for [Device Name] [Camera Name]* window (see page 44), in which you have access to settings for the camera in question, including:

- How the camera should record (frame rate, image quality, etc.)
- Where and when to store recorded images from the camera
- Motion detection sensitivity
- How images from the camera should appear when displayed in the *Monitor* application (see page 133)
- Triggering of notifications and external output
- ... and more

This also applies if you want to edit the settings for an already configured camera.

Camera Settings for [Device Name] [Camera Name] Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Camera Settings for [Device Name] [Camera Name]* window lets you specify settings for a particular camera.
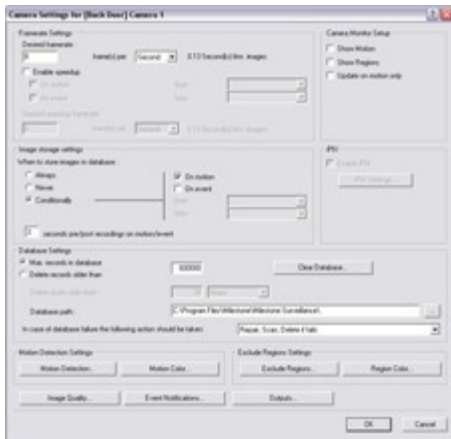
Example: The *Camera Settings for [Device Name] [Camera Name]* window for a non-PTZ camera

Access: You are able to access the *Camera Settings for [Device Name] [Camera Name]* window in two ways:

- From the *Administrator* window (see page 30), by selecting a camera in the *Device Manager* section, then clicking the *Settings...* button.
- From the *Monitor Manager* window (see page 71), by selecting the required camera, then clicking the *Settings* button

The *Camera Settings for [Device Name] [Camera Name]* window is divided into eleven sections:

- Framerate Settings
- Camera Monitor Setup
- Image Storage Settings
- iPIX
- Database Settings
- Motion Detection Settings
- Exclude Regions Settings
- Image Quality...
- Event Notifications...
- Outputs...
- PTZ Preset Positions... (PTZ cameras only)

Each section is described in the following.

Framerate Settings Section

The *Camera Settings for [Device Name] [Camera Name]* window's *Framerate Settings* section lets you specify the camera's recording speeds:

Field	Description
Desired framerate	Lets you specify required frame rate. Specify required number of frames in first field, and select required unit (per *Second*, per *Minute*, or per *Hour*) from the list. Example: 8 frames per second. **Tip:** When you specify a frame rate, the interval between images is automatically calculated and displayed to the right of the frame rate fields.
Enable speedup	Milestone XProtect Enterprise is able to increase the frame rate of a camera if motion is detected, or if an external event occurs. Select the check box to enable increased frame rate on motion detection or on an external event, then specify the required conditions in the following fields.
On motion	Available only if the *Enable speedup* check box is selected. Select check box to use a higher frame rate when motion is detected. Remember to specify the required higher frame rate in the *Desired speedup framerate* fields. The camera will return to the original frame rate two seconds after the last motion is detected.
On event	**Note:** Use of speedup on event requires that events have been defined in the *I/O Setup* window (see page 93), accessed by clicking the *I/O Setup...* button in the *Administrator* window (see page 30). Available only if the *Enable speedup* check box is selected. Select check box to use a higher frame rate when an external event occurs and until another external event occurs, then select required start and stop events in the *Start* and *Stop* lists. The camera will increase its frame rate when the start event occurs, and return to the original frame rate when the stop event occurs. Remember to specify the required higher frame rate in the *Desired speedup framerate* fields.
Desired speedup framerate	Available only if the *Enable speedup* check box is selected. Specify required number of frames to be used when motion is detected and/or an external event occurs in first field and select required unit (per *Second*, per *Minute*, or per *Hour*) from the list. The frame rate must be higher than the frame rate specified in the *Desired framerate* field.

| | Example: 16 frames per second. |
| | **ⓘ Tip:** When you specify a frame rate, the interval between images is automatically calculated and displayed to the right of the frame rate fields. |

Camera Monitor Setup Section

In the *Camera Settings for [Device Name] [Camera Name]* window's *Camera Monitor* section you are able to specify how images from the camera are displayed when viewed in the *Monitor* application (see page 133):

Field	Description
Show Motion	If selected, detected motion will be highlighted in the camera's images.
	Motion highlighted in green when viewed in *Monitor*
	ⓘ Tip: You are able to select the motion detection highlight color by clicking the *Motion Color...* button in the *Motion Detection Settings* section (see page 51).
Show Regions	If selected, areas in which motion detection has been disabled will be highlighted in the camera's images.
	Default highlighting color is blue.
	ⓘ Tip: You are able to select the color used to highlight areas with disabled motion detection by clicking the *Region Color...* button in the *Exclude Regions Settings* section (see page 51).
	Area with disabled motion detection highlighted in red when viewed in *Monitor*. Default highlighting color is blue.
Update on motion only	If selected, the camera's images will only be updated in the *Monitor* application when motion is detected.

Disabled	Cameras are by default enabled, meaning that images from the cameras are by default transferred to Milestone XProtect Enterprise—provided that the cameras are marked as *online* (also default) in the *Camera/Alert Scheduler* Window (see page 74). If required, you can disable the camera. When the camera is disabled, no images will be transferred from the camera to Milestone XProtect Enterprise. **Note:** If images from a camera are displayed in the *Monitor* application (configured in the *Monitor Manager* window, see page 71), the camera cannot be disabled. When this is the case, remove the camera from the *Monitor Manager* window's layout before disabling the camera. *i* **Tip:** Individual cameras can also be disabled/enabled in the *Administrator* window's *Device Manager* section (see page 32).

Image Storage Settings Section

The Camera Settings for [Device Name] [Camera Name] window's *Image storage settings* section lets you specify when images received from the camera should be stored in the database.

You specify this information in the following fields:

Field	Description
When to store images in database	Select when images received from the camera should be stored in the database: • *Always*: Always store all received images in the database. • *Never*: Never store any received images in the database. Live images will be displayed in the *Monitor* application, but, since no images are kept in the database, *Monitor* users will not be able to browse images from the camera. • *Conditionally*: Store received images in the database when certain conditions are met. When you select this option, specify required conditions in the following fields.
On motion	Available only when the option *Conditionally* is selected, i.e. when images received from the camera should be stored in the database on certain conditions only. Select check box to store all images in which motion is detected.
On event	Available only when the option *Conditionally* is selected, i.e. when images received from the camera should be stored in the database on certain conditions only. **Note:** Use of storage on event requires that events have been defined. Read more about events in *About Input, Events and Output* on page 91. Select check box to store all images, regardless of motion, when an event occurs and until another event occurs, then select required start and stop events in the *Start* and *Stop* lists.

[Number of] seconds pre/post recordings on event	Available only when the option *Conditionally* is selected, i.e. when images received from the camera should be stored in the database on certain conditions only. You are able to store recordings from periods preceding and following detected motion and/or specified events. Using such a "pre/post buffer" can be advantageous: If, for example, you have defined that images should be stored when a door is opened, being able to see what happened immediately prior to the door being opened may be important. Specify the number of seconds for which you want to store images from before and after the storage conditions are met. Example: You have specified that images should be stored conditionally on event, with a start event called *Door Opened* and a stop event called *Door Closed*. With a pre/post buffer of three seconds, images will be stored from three seconds **before** *Door Opened* occurs to three seconds **after** *Door Closed* occurs.

iPIX Section

Note: Functionality in the *iPIX* section is only available if the use of IPIX technology has been enabled for the device to which the camera is attached. For dedicated IPIX cameras, the use of IPIX technology is automatically enabled. If not dealing with a dedicated IPIX camera, you enable use of IPIX technology for a device in the *Edit device settings* window (see page 38). The *Edit device settings* window is accessed by selecting the required device in the *Device Manager* section of the *Administrator* window (see page 30), then clicking the *Administrator* window's *Edit Device...* button.

The *Camera Settings for [Device Name] [Camera Name]* window's *iPIX* section lets you enable the use of IPIX technology—a technology that allows viewing of 360-degree panoramic images through an advanced "fish eye" lens.

The section contains the following fields and buttons:

Field	Description
Enable iPIX	Select check box to enable the use of IPIX technology on the particular camera. Check box is selected by default if the device in question is for a dedicated IPIX camera.
iPIX Settings...	Opens the *iPIX Camera Configuration* window (see page 69), in which you configure the camera's IPIX functionality.

Database Settings Section

The Camera Settings for [Device Name] [Camera Name] window's *Database Settings* section lets you specify database settings for the camera, such as where the database is kept, how much data to store, etc.

Tip: By using archiving (see page 124) it is possible to store images beyond the capabilities of the camera's database.

Field	Description
Max. records in database	Select this option to limit the database size based on a maximum allowed number of records in the database.
	Specify required maximum number of records in the neighboring field.
	When the maximum number of records in the database is reached, the oldest record in the database will automatically be overwritten.
	A database can contain up to 600,000 records.
Delete records older than	Select this option to limit the database size based on the age of records in the database.
	Specify required number in neighboring field, and select required unit (*Minutes*, *Hours*, or *Days*) from the list.
	When records become older than the specified number of minutes, hours, or days, they will automatically be deleted.
	Note: A database can contain no more than 600,000 records, regardless of what maximum age has been defined.
Delete audio older than	Lets you define how long audio recordings should be stored for.
	Available only if audio has been enabled for the device to which the camera is attached. You enable audio for a device in the *Edit device settings* window (see page 38), accessed from the *Administrator* window (see page 30) by selecting the required device in the *Device Manager* section, then clicking the *Edit Device...* button.
	Specify required storage length by typing a number and selecting the required unit (*Minutes*, *Hours*, or *Days*) from the list.
	When audio recordings become older than the specified number of minutes, hours, or days, they will automatically be deleted.
Clear Database...	Click button to delete all records stored in the database for the camera in question.
	WARNING: Use with caution; all records in the database for the camera will be permanently deleted. As a security measure, you will be asked to confirm that you want to permanently delete all stored records for the camera.
	Records stored in archived databases will be saved.
Database path	Specify which local directory the database for the camera should be kept in.
	Default database path is the path at which the Milestone XProtect Enterprise software is installed, typically C:\Program Files\Milestone\Milestone Surveillance\
	To browse for a folder, click the browse button next to the *Database path* field.
	Note: Even though it is possible to specify a path to a network drive, it is highly recommended that you specify a path to a *local* drive. If using a path to a network drive, it will not be possible to save to the database should the

	network drive become unavailable. **Tip:** If you have several cameras, and several local drives are available, performance can be improved by distributing the databases of individual cameras across the local drives.
In case of database failure the following action should be taken	Select which action to take if the database becomes corrupted. The number of available actions depends on whether archiving has been enabled. You enable archiving for a camera in the *Archive setup* window (see page 127), accessed from the *Administrator* window (see page 30) by clicking the *Archive Setup...* button. • *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*: Available only if archiving is enabled for the camera. If the database becomes corrupted, a fast repair will be attempted. If the fast repair fails, the contents of the database will be archived. This action is recommended if archiving is enabled for the camera. • *Delete (no repair)*: If the database becomes corrupted, the contents of the database will be deleted. • *Archive (no repair)*: Available only if archiving is enable for the camera. If the database becomes corrupted, the contents of the database will be archived. **Tip:** An archived corrupt database can be repaired by the *Monitor* application's *Viewer*. When the contents of the local database for the camera are either deleted or archived, the database is reset and will be ready for storing new recordings. **Note:** No images can be recorded while the database is being repaired. For large installations, a repair may take several hours, especially if the *Repair, Scan, Delete if fails* action involving two different repair methods is selected, and the first repair method (fast repair) fails.

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

If archives are present on the same drive as the camera's database, the oldest archive for all cameras archived on that drive will be deleted
If no archives are present on the drive containing the camera's database, the size of all camera databases on the drive will be reduced by deleting a percentage of their oldest recordings, thus temporarily limiting the size of all databases

When the *Monitor* application (see page 133) 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.
Should the database resizing procedure take place, you will be informed on-screen, in log files, and (if set up) through an e-mail and/or SMS alert.

Motion Detection Settings Section

The *Camera Settings for [Device Name] [Camera Name]* window's *Motion Detection Settings* section contains two buttons for configuring the camera's motion detection:

Button	Description
Motion Detection...	Opens the *Adjust Motion Detection* window (see page 53), in which you are able to specify motion detection sensitivity levels.
Motion Color...	Opens the *Color* window (see page 55), in which you are able to select a color to be used for highlighting detected motion when images from the camera are viewed in the *Monitor* application. **Note:** Highlighting of detected motion in the *Monitor* application requires that the *Show Motion* check box in the *Camera Settings for [Device Name] [Camera Name]* window's *Camera Monitor* section (see page 46) is selected.

Exclude Regions Settings Section

The *Camera Settings for [Device Name] [Camera Name]* window's *Exclude Regions Settings* section contains two buttons for specifying areas in the camera's images in which motion detection should **not** be used:

Button	Description
Exclude Regions...	Opens the *Define Exclusion Regions* window (see page 55), in which you are able to disable motion detection in specific areas of the camera's images. Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.
Region Color...	Opens the *Select Color* window (see page 57), in which you are able to select between three colors to be used for highlighting areas with disabled motion detection when images from the camera are viewed in the *Monitor* application. **Note:** Highlighting of areas with disabled motion detection in the *Monitor* application requires that the *Show Regions* check box in the *Camera Settings for [Device Name] [Camera Name]* window's *Camera Monitor* section (see page 46) is selected.

Image Quality...

The *Camera Settings for [Device Name] [Camera Name]* window's *Image Quality...* button opens the *Configure Device* window (see page 52), in which you are able to configure image resolution, compression, etc. for the camera.

Event Notifications...

The *Camera Settings for [Device Name] [Camera Name]* window's *Event Notifications...* button opens the *Setup Notifications on Events* window (see page 60), in which you are able to select

events for triggering event indications for the camera when displayed in the *Monitor* application (see page 133).

Note: The use of event notifications requires that at least one event has been specified on your Milestone XProtect Enterprise system; the event does not have to be specified for the particular camera. You specify input events and VMD (Video Motion Detection) events in the *I/O Setup* window (see page 93), event buttons (for manual event generation) in the e window (see page) and generic events (based on received TCP/UDP data packages) in the *Generic Events* window.

Outputs...

The *Outputs...* button opens the *Output Settings for [Device Name] [Camera Name]* window (see page 57), in which you are able to specify which outputs (e.g. the sounding of a siren or the switching on of the lights) should be associated with motion detection and/or with output buttons (buttons for manually triggering particular output in the *Monitor* application).

Note: The use of outputs requires that at least one event has been specified for a device on your Milestone XProtect Enterprise system; the event does not have to be specified for the particular camera. Read more about events in *About Input, Events and Output* on page 91.

PTZ Preset Positions...

Available only if the camera is a PTZ (Pan/Tilt/Zoom) camera supporting PTZ preset positions, the PTZ Preset Positions... button opens *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 61), in which you are able to specify preset positions and patrolling for the camera.

Configure Device Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights. Settings in the *Configure Device* window are to a large extent camera-specific. The window's contents will therefore vary from camera to camera; descriptions in the following are thus for guidance only.

The *Configure Device* window lets you specify image quality settings, such as compression, resolution, etc. for a specific camera.

Example of the *Configure Device* window, with a preview image

Access: You access the *Configure Device* window by clicking the *Image Quality...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

The *Configure Device* window typically contains a *Camera Settings* section and an image preview feature.

Camera Settings Section

The *Configure Device* window's *Camera Settings* section will typically contain controls for compression, bandwidth, resolution, color, contrast, brightness, image rotation, and similar.

Include Date and Time in Image

The *Camera Settings* section may feature an *Include Date and Time in Image* check box. When selected, date and time **from the camera** will be included in images from the camera.

Note: As cameras are separate units which may have separate timing devices, power supplies, etc., camera time and Milestone XProtect Enterprise system time may not correspond fully, and this may occasionally lead to confusion.

As all images are time-stamped by Milestone XProtect Enterprise upon reception, and exact date and time information for each image is thus already known, it is recommended that you keep the *Include Date and Time in Image* check box cleared.

Should you want to use the *Include Date and Time in Image* feature, it is recommended that you click the *Synchronize Time* button, if available. Clicking the *Synchronize Time* button will set camera time to system time, but does not guarantee that camera time will match system time indefinitely.

Tip: For consistent synchronization, you may, if supported by the camera, auto-synchronize camera and system time via a time server.

Preview Image

When adjusting camera settings, you are able to view the effect of your settings by clicking the *Preview Image* button, located at the bottom of the window.

Clicking the *Preview Image* button will provide you with an image from the camera in question, as it would look with the settings specified in the *Camera Settings* section.

When you have found the best possible camera settings, click *OK* to apply the settings for the camera.

Adjust Motion Detection Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Adjust Motion Detection* window lets you specify motion detection sensitivity for a specific camera.

Depending on your configuration, motion detection sensitivity settings may determine when images from the camera are recorded and transferred to the surveillance system, when alerts are generated, when external outputs (such as lights or sirens) are triggered, etc.

Motion detection sensitivity is therefore a key element in your Milestone XProtect Enterprise surveillance solution, and time spent on finding the best possible motion detection settings for each camera may help you later avoid unnecessary alerts, etc.

Depending on the physical location of the camera, it may be a very good idea to test motion detection settings under different physical conditions (day/night, windy/calm weather, etc.).
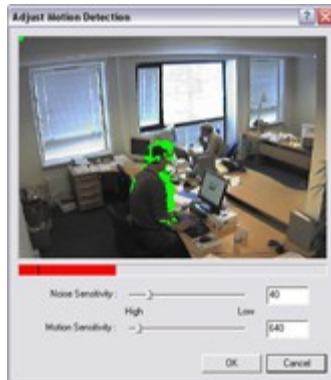
The *Adjust Motion Detection* window

Access: You access the *Adjust Motion Detection* window by clicking the *Motion Detection...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Note: Before you configure motion detection sensitivity for a camera, it is highly recommended that you have configured the camera's image quality settings, such as resolution, compression, etc., in the *Configure Device* window (see page 52)*,* and that you have specified any areas to be excluded from motion detection (for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background) in the *Define Exclusion Regions* window (see page 55)*.*

If you later change image quality settings and/or exclusion area settings, you should always test motion detection sensitivity settings afterwards.

Noise Sensitivity

The *Adjust Motion Detection* window's *Noise Sensitivity* slider determines how much each pixel must change before it is regarded as motion. Insignificant changes, which should not be regarded as motion, are considered acceptable noise, hence the name of the slider.

With a high noise sensitivity, very little change in a pixel is required before it is regarded as motion.

Areas in which motion is detected are highlighted in the preview image. Select a slider position in which only detections you consider motion are highlighted.

As an alternative to using the slider, you may specify a value between 0 and 256 in the field next to the slider to control the noise sensitivity setting.

Tip: If you find the concept of noise sensitivity difficult to grasp, try dragging the slider to the left towards the *High* position: The more you drag the slider towards the *High* position, the more of the preview image becomes highlighted. This is because a high noise sensitivity means that even the slightest change in a pixel will be regarded as motion.

Motion Sensitivity

The *Adjust Motion Detection* window's *Motion Sensitivity* slider determines how many pixels must change in the image before it is regarded as motion.

The selected motion sensitivity level is indicated by the black vertical line in the motion level indication bar below the preview image. The black vertical line serves as a threshold: When detected motion is above the selected sensitivity level, the bar changes color from green to red, indicating a positive detection.

As an alternative to using the slider, you may specify a value between 0 and 10,000 in the field next to the slider to control the motion sensitivity setting.

Color Window

Note: Access to features in the Administrator application, including those described in the following, may require administrator rights.

The *Color* window lets you select a color to be used for highlighting detected motion when images from a camera are viewed in the *Monitor* application (see page 133).

 Access: You access the *Color* window by clicking the *Motion Color...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Selecting a Color for Highlighting Detected Motion

To select a color, pick the required color from the *Basic Colors* palette, and click *OK*.

The ability to define custom colors is not available.

Note: Highlighting of detected motion in the *Monitor* application requires that the *Show Motion* check box in the *Camera Monitor* section of the *Camera Settings for [Device Name] [Camera Name]* window (see page 44) is selected.

Define Exclusion Regions Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Define Exclusion Regions* window lets you disable motion detection in specific areas of a camera's images.

Disabling motion detection in certain areas may help you avoid detection of irrelevant motion, for example if the camera covers an area where a tree is swaying in the wind or where cars regularly pass by in the background.
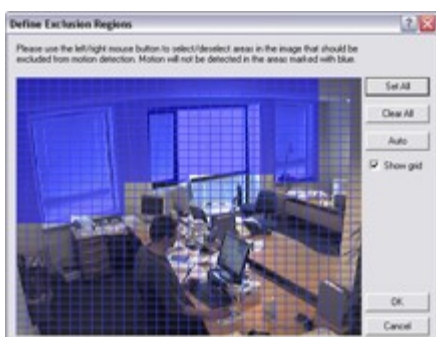
The *Define Exclusion Regions* window, with an exclusion area highlighted in blue

Access: You access the *Define Exclusion Regions* window by clicking the *Exclude Regions...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Defining Areas in which Motion Detection Should Be Disabled

The *Define Exclusion Regions* window features a preview image from the camera. You define the areas in which motion detection should be disabled in the preview image, which is divided into small sections by a grid.

To define areas in which motion detection should be disabled, drag the mouse pointer over the required areas in the preview image while pressing the mouse button down. Left mouse button selects a grid section; right mouse button clears a grid section. Selected areas are highlighted in blue.

Tip: Even though areas in which motion detection should be disabled are always highlighted in blue in the *Define Exclusion Regions* window itself, you are able to select a different color for (the optional) highlighting of areas with disabled motion detection when images from the camera are viewed in the *Monitor* application. Such color selection takes place in the *Select Color* window (see page 57).

The *Define Exclusion Regions* window features the following buttons and check boxes:

Button, Check Box	Description
Set All	Lets you quickly select all grid sections in the preview image. This may be advantageous if you want to disable 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 disable motion detection.
Clear All	Lets you quickly clear all grid sections in the preview image.
Auto	By clicking the *Auto* button you can make Milestone XProtect Enterprise automatically detect areas with noise (insignificant changes in individual pixels which should not be regarded as motion) in the image, and automatically mark such areas as areas in which motion detection should be disabled. As the automatic detection is based on an analysis of a number of images, it may take a few seconds from you click the *Auto* button to noisy areas are

	detected and marked as areas in which motion detection should be disabled.
	Note: The automatic detection of noisy areas happens according to the noise sensitivity setting specified in the Adjust Motion Detection window (see page 53). In order for the automatic detection of noisy areas to work as intended, it is recommended that you specify a noise sensitivity setting that matches your requirements before you make use of the automatic detection feature.
Show Grid	With the *Show grid* check box selected (default), the preview image contains a grid indicating the division of the preview image into selectable sections. With the *Show grid* check box cleared, the grid in the preview image is removed. This may provide a less obscured view of the preview image. Selection of areas in which motion detection should be disabled takes place the same way as when the grid is visible.

Select Color Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Select Color* window lets you select between three colors to be used for highlighting areas with disabled motion detection when images from the camera are viewed in the *Monitor* application (see page 133).

Color changes only have effect in the *Monitor* application; the default blue highlight color will always be used in the *Administrator* application.

 Access: You access the *Select Color* window by clicking the *Region Color...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Note: Highlighting of areas with disabled motion detection in the *Monitor* application requires that the *Show Regions* check box in the *Camera Monitor* section of the *Camera Settings for [Device Name] [Camera Name]* window is selected.

Output Settings for [Device Name] [Camera Name] Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

In the *Output Settings for [Device Name] [Camera Name]* window you are able to associate a camera with particular external outputs, defined in the *I/O Setup* window (see page 93), for example the sounding of a siren or the switching on of lights.

The associated outputs can be triggered automatically when motion is detected as well as manually through output buttons available when the camera is selected in the Monitor application (see page 131), *Remote Client* (see page 171) and *Smart Client* (see page 210).

The *Output Settings for [Device Name] [Camera Name]* window

Access: You access the *Output Settings for [Device Name] [Camera Name]* window from the *Camera Settings for [Device Name] [Camera Name]* window (see page 44), by clicking the *Outputs...* button.

Associating Outputs with Manual Control and Detected Motion

Note: Use of features in the *Output Settings for [Device Name] [Camera Name]* window requires that output has been defined in the *I/O Setup* window (see page 93).

You have a high degree of flexibility when associating a camera with particular outputs:

- You are able to select between all available outputs, i.e. outputs defined as output events for the camera itself **as well as** outputs defined as output events for other devices on the Milestone XProtect Enterprise system
- The same output may be used for manual control through an output button **as well as** for automatic triggering when motion is detected

Selecting Output for Manual Control

You are able to specify outputs to be triggered manually through output buttons in the *Monitor* application or from a list in the *Remote Client* or *Smart Client*.

Output buttons will become available in the Monitor when the camera is selected and the Monitor's Output button is clicked. In the *Remote Client* and *Smart Client*, users will be able to trigger outputs by selecting them from a list.

Example of output buttons available in the *Monitor* application. Note that the *Monitor*'s *Output* button has been clicked in order to view the output buttons.

To specify an output for manual triggering in the *Monitor* or *Remote Client*/*Smart Client*, do the following:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   i **Tip:** When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Manual Control* list.

   This will copy the selected output to the *On Manual Control* list.

Note: An unlimited number of outputs may be selected this way, but only the top eight outputs in the list will be available as output buttons in the *Monitor*. In the *Remote Client* and *Smart Client* there are no limitations to the number of available outputs.

You are able to move a selected output up or down in the *On Manual Control* list with the *up* and *down* buttons located to the right of the list. The selected output is moved up one step each time you click the *up* button. Likewise, each time you click the *down* button, the selected output is moved down one step.

To remove an output from the *On Manual Control* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Manual Control* list.

Selecting Output for Use on Motion Detection

You are able to select outputs to be triggered automatically when motion is detected in images from the camera.

i **Tip:** This feature does *not* require that a VMD (Video Motion Detection) event has been defined for the camera in the *I/O Setup* window (see page 93).

To select an output for use when motion is detected in images from the camera:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   i **Tip:** When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Motion Detected* list.

   This will copy the selected output to the *On Motion Detected* list.

To remove an output from the *On Motion Detected* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Motion Detected* list.

Setup Notifications on Events Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights. The use of event notifications requires that at least one event has been specified for a device on your Milestone XProtect Enterprise system; the event does not have to be specified for the particular camera. For information about how to specify events, see *About Input, Events and Output* on page 91.

The *Setup Notifications on Events* window lets you select events for triggering event indications for the camera when displayed in the *Monitor* application (see page 133).

The *Setup Notifications on Events* window

Access: You access the *Setup Notifications on Events* window from the *Camera settings for [Device Name] [Camera Name]* window (see page 44), by clicking the *Event Notifications* button.

What Is an Event Indication?

In the *Monitor*, *Remote Client* and *Smart Client*, three different color indicators are available for each camera: a yellow indicator, a red indicator, and a green indicator. When event indication is used for a camera, the yellow indicator will light up when the specified events have occurred.

Event indications can be valuable for camera operators, as they will be able to quickly detect that an event has occurred, even though their focus was perhaps on something else the moment the event occurred.

Available indicators; the yellow indicator serves as the event indicator

Tip: The other two indicators serve the following purposes: The red indicator lights up when motion has been detected, and the green indicator is used for indicating that images are received from a camera.

Specifying Events for which Event Indication Should Be Used

To specify which events should trigger an event indication for the camera, do the following for each required event:

1. In the *Available Events* list, select the required event.

    ⓘ Tip: You are not limited to events associated with a particular device: You are able to select between all available events (input events, timer events, VMD events, generic events, event buttons) from all cameras on the Milestone XProtect Enterprise surveillance system.

2. Click the >> button to copy the selected event to the *Active Events* list.

    When an event listed in the *Active Events* list occurs, the event indicator will light up.

3. Repeat for each required event.

To remove an event from the *Active Events* list, select the event in question, and click the << button.

PTZ Preset Positions for [Device Name] [Camera Name] Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Available only when dealing with a PTZ (Pan/Tilt/Zoom) camera supporting PTZ preset positions, the *PTZ Preset Positions for [Device Name] [Camera Name]* window lets you view and—for absolute positioning PTZ cameras—define preset positions for the PTZ camera.

The *PTZ Preset Positions for [Device Name] [Camera Name]* window

Access: To access the *PTZ Preset Positions for [Device Name] [Camera Name]* window, click the *PTZ Preset Positions...* button in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44). The button is only available if the camera supports PTZ preset positions.

Your configuration options depend on whether the PTZ camera in question is of the absolute positioning or relative positioning kind:

- For an absolute positioning PTZ camera, you are able to define up to 50 preset positions. You define a preset position by moving the PTZ camera to the required position with the controls in the *PTZ View* section, then naming the position in the *Preset Positions* section.

- For a relative positioning PTZ camera, the number of preset positions will depend on the camera/video server and PTZ driver used, and only preset positions defined on the camera/video server will be available.

Defined preset positions can be used for making the PTZ camera automatically go to particular preset positions when particular events occur, and for specifying PTZ patrolling scheme.

Defined preset positions will also become selectable in the *Monitor* application (see page 133) and in the *Remote Client* (see page 171) and *Smart Client* (see page 210), allowing users of these applications to move the PTZ camera to the preset positions.

Note: For an absolute positioning PTZ camera you may define up to 50 preset positions. All 50 preset positions can be used in the *Remote Client* and *Smart Client*. However, only the first 25 preset positions can be used in the *Monitor* application.

Defining a Preset Position

First use the controls in the *PTZ Preset Positions for [Device Name] [Camera Name]* window's *PTZ View* section to move the PTZ camera to the required position.

Having moved the PTZ camera to the required position, select an undefined item in the *Preset Positions* section's list of preset position names, and click the *Set Position* button to define a name for the preset position.

Each of the *PTZ Preset Positions for [Device Name] [Camera Name]* window's sections are described in the following:

PTZ View Section

The *PTZ View* section lets you control the PTZ camera, and watch the PTZ camera's movements.

You use this section to move the PTZ camera to the positions you then define as presets positions in the *Preset Positions* section.

The preview provided in the *PTZ View* section is not suitable for PTZ testing.

To move the PTZ camera, simply click the required position in the preview picture.

The *PTZ View* section also features sliders allowing you to move the PTZ camera along each of its axes: the X-axis (allowing you to pan left/right), the Y-axis (allowing you to tilt the camera up/down), and the Z-axis (enabling you to zoom in and out; the camera will zoom in when you move the slider towards *Tele*, and zoom out when you move the slider towards *Wide*).

As an alternative to clicking the required position in the preview or using the sliders, you can use the PTZ camera 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
H	Moves the PTZ camera to its home 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
🔍	Zoom out (one zoom level per click)
🔍	Zoom in (one zoom level per click)

Preset Positions Section

Having specified a camera position in the *PTZ Preset Positions for [Device Name] [Camera Name]* window's *PTZ View* section, you define the required position as a preset in the *Preset Positions* section:

Button, Check Box	Description
Use preset positions from device	Available only for cameras supporting this feature. Check box to use preset positions defined on the camera or video server device. Using preset positions from the camera or video server device will clear any preset positions you have defined for the PTZ camera; you will therefore be asked to confirm your selection. **Note:** In order for preset positions from the camera or video server device to work with Milestone XProtect Enterprise, the names of the preset positions must contain only the characters A-Z, a-z and 0-9, and must not contain spaces. If preset position names on the camera or video server device contain other characters, or spaces, change the preset position names on the device before selecting the *Use preset positions from device* feature.
Set Position	Associates the preset position selected in the list with the position specified in the *PTZ View* section. If the preset position selected in the list is yet undefined, you will be asked to specify a name for the preset position. ⓘ **Tip:** Since the name will appear on buttons in the *Monitor* application,

	specify a name that is short enough to appear on a button. If the name is too long, it will be truncated when used on the button in the *Monitor*. The *Remote Client* and *Smart Client* are capable of displaying even long preset position names.
Edit Name…	Lets you edit a preset position name selected in the list. Only works for an already defined preset position name.
Test	Lets you test a defined preset position. Select the required preset position in the list, then click the *Test* button. The effect is displayed instantly in the *PTZ View* section.
Delete	Lets you delete a preset position selected in the list. When a preset position name is deleted, it will appear as *Undefined* in the list.
[Move up] **[Move down]**	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 position up or down, you are able to control the sequence in which available preset positions are presented in the *Monitor* application and in the *Remote Client* and *Smart Client*: In the *Monitor*, preset position buttons are grouped in five preset banks (A-E) of five buttons each (1-5). By moving a preset position up or down, you can thus determine which preset bank and which button number should be used for a particular preset position. In the *Remote Client* and *Smart Client*, users select preset positions from a list. By moving a preset position up or down in the *Preset Positions* section's list, you can thus determine the sequence in which preset positions are presented in the *Remote Client*'s or *Smart Client*'s list. Display of preset positions in *Monitor* and *Remote Client/Smart Client* respectively. Administrators are able to specify the sequence in which available preset positions are displayed in the two applications.

Preset Position on Events Section

If you have specified input or VMD events (see page 93), event buttons (see page 105) or generic events (see page 110), you are able to make the PTZ camera automatically go to particular preset positions when particular events occur.

To configure the use of preset positions on events, click the *Setup...* button. This will open the *Event* window (for preset positions on event) (see page 65), in which you are able to associate particular preset positions with particular events.

To use preset positions on event, select the *Goto preset on event* check box.

Patrolling Section

To configure PTZ patrolling (the automatic movement of a PTZ camera between several preset positions), click the *Setup...* button to go to the *Setup PTZ Patrolling* window (see page 66).

PTZ patrolling requires that at least two preset positions have been defined.

Event Window (for PTZ Preset Positions on Event)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Available only when dealing with a PTZ camera, the *Event* window (for preset positions on events) lets you associate particular preset positions with particular events, timer events or event buttons. You are thus able to make the PTZ camera automatically go to a particular preset position when a particular event occurs.

The *Event* window (for preset positions on events)

Access: To access the *Event* window (for preset positions on events), click the *Setup...* button in *Preset Position on Events* section of the *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 61).

Note: To use preset positions on events, you must have specified input or VMD events (see *I/O Setup* window on page 93), event buttons (see page 105) or generic events (see page 110). Only one PTZ preset position can be defined per event per camera.

Associating Preset Positions with Particular Events

When associating a preset position from a particular PTZ camera with one or more events, you are able to select between **all** events defined on the Milestone XProtect Enterprise system; you are not limited to selecting events defined on a particular device.

To associate a particular preset position with a particular event, do the following:

1. Select the required preset position in the *Available Preset Positions* list in the left side of the *Event* window.

2. Select the required event in the list of available events (the list in the middle of the window)

3. Click the >> button located to the right of the *Available Events* list.

   This will copy the selected event to the window's rightmost list, in which events associated with the selected preset position are listed. When the selected event occurs, or when the selected event button is clicked, the PTZ camera will automatically move to the required preset position.

You are able to associate a preset position with more than one event: Simply repeat the process for each required association.

To end the association between a particular preset position and a particular event, simply select the required event in the window's rightmost list, and click the << button.

Setup PTZ Patrolling Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Available only when dealing with a PTZ (Pan/Tilt/Zoom) camera, the *Setup PTZ Patrolling* window lets you configure patrol schemes for PTZ patrolling (the automatic movement of a PTZ camera between several preset positions) for the camera.
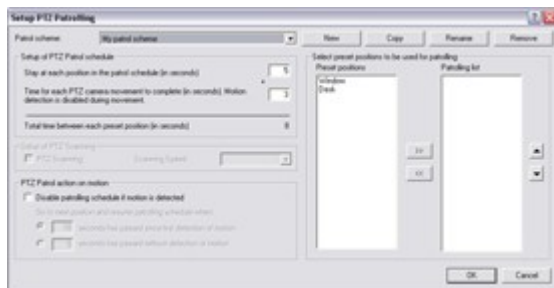
The *Setup PTZ Patrolling* window

Access: To access the *Setup PTZ Patrolling* window, click the *Setup...* button in *Patrolling* section of the *PTZ Preset Positions for [Device Name] [Camera Name]* window (see page 61).

Note: To define a patrol scheme, you must have specified at least two preset positions for the PTZ camera in question. When you have defined patrol schemes, also remember to schedule use of the patrol schemes in the *Camera/Alert Scheduler* window (see page 74).

Patrol Scheme

A PTZ camera may patrol according to several different patrol schemes.

For example, a PTZ camera in a supermarket may patrol according to one patrol scheme during opening hours, and according to another patrol scheme when the supermarket is closed.

The *Patrol scheme* list lets you select which patrol scheme to configure.

Defining a New Patrol Scheme

To define a new patrol scheme, click the *New* button. This will add a *New patrol scheme* listing to the *Patrol Scheme* list.

To change the name from *New patrol scheme* to a name of your choice, select the *New patrol scheme* listing, and click the *Rename* button.

Copying an Existing Patrol Scheme

If you want to create a new patrol scheme based on an existing one, you can copy the existing patrol scheme.

To copy an existing patrol scheme, select the required patrol scheme in the *Patrol Scheme* list, and click the *Copy* button. This will add a copy of the selected patrol scheme to the list. The copy will initially be named *Copy of [Patrol Scheme Name]*.

To change the name to a name of your choice, select the *Copy of [Patrol Scheme Name]* listing, and click the *Rename* button.

Renaming an Existing Patrol Scheme

To change the name of an existing patrol scheme, select the required patrol scheme in the *Patrol Scheme* list, and click the *Rename* button.

Removing an Existing Patrol Scheme

To remove an existing patrol scheme, select the required patrol scheme in the *Patrol Scheme* list, and click the *Remove* button.

Note: The selected patrol scheme will be removed from the list without further warning.

Selecting Preset Positions to Be Used for a PTZ Patrol Scheme

Having selected a patrolling scheme in the *Patrol scheme* list, you are able to 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 names of 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 or SHIFT buttons on your keyboard while selecting from the *Preset Positions* list, you are able to 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 name, and use the *move up* or *move down* buttons to move the selected preset position name.

To remove a preset position from the *Patrolling list*, select the preset position in question, and click the << button.

Specifying Timing Settings for a PTZ Patrol Scheme

Having selected a patrolling scheme in the *Patrol scheme* list, you are able to specify timing settings for the patrol scheme:

1. In the *Stay at each position in the patrol schedule* field, specify the number of seconds for which the PTZ camera should stay at each preset position.

2. In the *Time for each PTZ camera movement to complete* field, specify the number of seconds required for the PTZ camera to move between preset positions.

   In order not to generate false motion alarms, motion detection for the PTZ camera is automatically disabled while the camera moves between two preset positions.

   After the specified number of seconds, motion detection is automatically enabled again.

   It is thus important that the camera is able to reach all of the patrolling scheme's preset positions within the number of seconds you specify. If not, false motion is likely to be detected.

   Bear in mind that it takes longer for the PTZ camera to move between positions that are located physically far apart (e.g. from an extreme left position to an extreme right position) than between positions that are located physically close together.

3. The total number of seconds between each preset position will be listed below the two fields.

PTZ Patrolling Actions on Detected Motion

You are able to combine a PTZ patrol scheme with motion detection, so that when motion is detected, the PTZ camera will pause its patrolling and remain at the position where motion was detected for a specified period of time.

To use this feature, do the following:

1. Select the *Disable patrolling schedule if motion is detected* check box.

2. Select whether the PTZ camera should resume patrolling:

   - When a certain number of seconds has passed since first detection of motion, regardless whether further motion is detected, or …

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

3. Specify the required number of seconds for selected option.

   Example:

You may specify that the PTZ camera should go to the next preset position and resume patrolling when 10 seconds has passed without detection of motion.

PTZ Scanning

PTZ scanning is supported on a few devices only. If your device supports PTZ scanning, the *Setup of PTZ Scanning* section lets you enable PTZ scanning and select a PTZ scanning speed.

iPIX Camera Configuration Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Use of the IPIX technology requires a dedicated IPIX camera or a special IPIX camera lens with a special IPIX license key, specified in the *Edit Device Settings* window (see page 38).

IPIX is a technology that allows viewing of 360-degree panoramic images through an advanced "fish eye" lens.

The *iPIX Camera Configuration* window lets you configure the IPIX functionality of a camera.
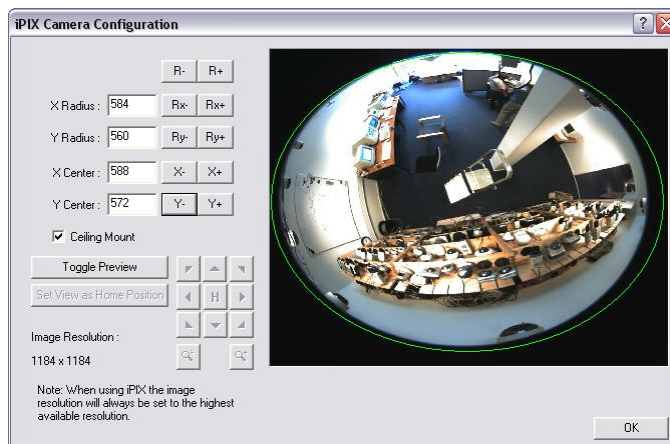
The *iPIX Camera Configuration* window

Access: You access the *iPIX Camera Configuration* window from the *Camera Settings for [Device Name] [Camera name]* window (see page 44), by selecting the *Enable iPIX* check box, and clicking the *iPIX Settings...* button.

IPIX View Adjustment

The camera's IPIX functionality is configured by adjusting its IPIX view field, indicated by a green ellipse in the preview image, so that it encloses the actual image area of the "fish eye" lens.

You do this by specifying a number of values which will be used by the IPIX technology for converting the elliptic image into an ordinary rectangular image.

You are able to set the ellipse's X-radius, Y-radius, X-center, and Y-center, either by specifying the required values directly in the four fields, or by using the following buttons to adjust the ellipse:

Button	Description
R-	Decreases the radius of the IPIX view field. The ellipse's horizontal (X) and vertical (Y) radiuses are changed at the same time, keeping the aspect ratio.
R+	Increases the radius of the IPIX view field. The ellipse's horizontal (X) and vertical (Y) radiuses are changed at the same time, keeping the aspect ratio.
Rx-	Decreases the horizontal (X) radius of the ellipse.
Rx+	Increases the horizontal (X) radius of the ellipse.
Ry-	Decreases the vertical (Y) radius of the ellipse.
Ry+	Increases the vertical (Y) radius of the ellipse.
X-	Moves the ellipse to the left.
X+	Moves the ellipse to the right.
Y-	Moves the ellipse up.
Y+	Moves the ellipse down.

Previewing the IPIX View

You are able to toggle between previewing the "fish eye" view and the IPIX-rendered view, i.e. the original elliptic view as well as the rectangular view resulting from applying the IPIX algorithm according to your specified values.

To toggle between the two different types of preview, click the *Toggle Preview* button.

When previewing the IPIX-rendered view, the following navigation buttons become available for moving around within the preview image area:

Moves the IPIX-rendered view up and to the left
Moves the IPIX-rendered view up
Moves the IPIX-rendered view up and to the right
Moves the IPIX-rendered view to the left
Moves the IPIX-rendered view to its home position
Moves the IPIX-rendered view to the right
Moves the IPIX-rendered view down and to the left

▼	Moves the IPIX-rendered view down
▲	Moves the IPIX-rendered view down and to the right
🔍	Zoom out (one zoom level per click)
🔍	Zoom in (one zoom level per click)

Ceiling Mounted Cameras

If the camera is mounted on a ceiling, you can adjust the behavior of the navigation buttons to reflect this by selecting the *Ceiling Mount* check box.

Setting a View as Home Position

When previewing the IPIX-rendered view, you are able to set a particular position in the IPIX-rendered view as the camera's home position: Navigate to the required position, using the navigation buttons, then click the *Set View as Home Position* button.

Image Resolution

Image resolution values are automatically displayed in the lower part of the window, next to the navigation buttons. When using IPIX, image resolution will automatically be set to the highest available resolution.

Monitor Administration

Monitor Manager Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Monitor Manager* window lets you specify which cameras should record and display images in the *Monitor*, Milestone Protect Enterprise's application for recording and displaying images from connected cameras (see page 133).

The *Monitor Manager* also lets you configure the layout of the *Monitor* application.

 Access: You access the *Monitor Manager* window by clicking the *Monitor Manager...* button in the *Administrator* window (see page 30).

Layout Size

In the *Layout Size* list you select the required grid for use in the *Monitor* application's camera layout.

Options are 1×1, 2×2, 3×3, etc. up to an 8×8 grid. A 3×3 camera layout grid, for example, will allow display of up to nine cameras.
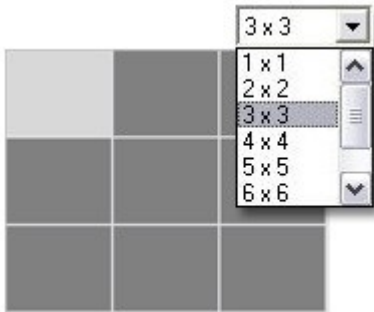
Selecting a 3×3 camera layout grid

Configuration Section

The *Monitor Manager* window's *Configuration* section contains the following features for selecting cameras and for specifying the layout of the *Monitor* application:

Feature	Description
Select Camera	Lets you select a particular camera for use in a particular position in the camera layout grid. Select a position in the camera layout grid, then select a camera from the list to display images from the selected camera in the selected position. **Note:** Remember that camera images are only transferred to Milestone XProtect Enterprise while the *Monitor* application is running. Read more about the *Monitor* application on page 133.
Hot Spot Window	Lets you select the required hot spot functionality. With the hot spot, *Monitor* users are able to select a camera in the *Monitor*'s camera layout grid, and view enlarged images from the camera. The hot spot may also be used for point-and-click operations on some PTZ cameras. Select between three hot spot options: • *None*: No hot spot; default • *Hot Spot*: Select required size for the hot spot • *In separate window*: hot spot is a separate, floating window When a hot spot is enabled, it will appear as a dark gray field in the camera layout grid (unless you have selected the *In separate window* option):
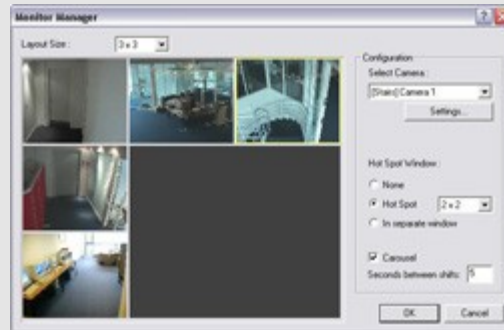
Configuration: A 3×3 grid with a 2×2 hot spot
defined in the *Administrator*'s *Monitor Manager*
window
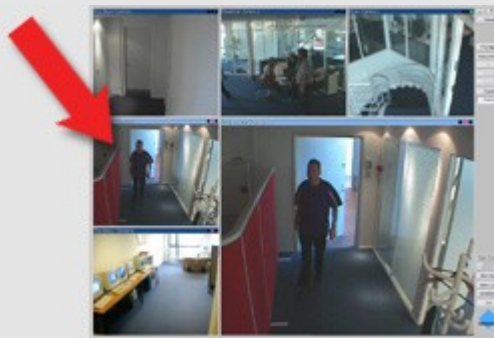
Effect: The hot spot appearing in the *Monitor*
(arrow indicates the camera the user has selected
for viewing in the hot spot)

Carousel	**Note:** Use of the carousel feature requires that a hot spot is enabled.
	With the carousel feature, you can make the hot spot automatically change between cameras in the *Monitor*'s camera layout grid. You specify the required interval between changes in the *Seconds between shifts* field.

How to Specify which Cameras Should Display Images in the Monitor

To specify which cameras should display images in the *Monitor* application, do the following:

1. In the *Monitor Manager* window, select a grid size for the camera layout grid, e.g. 3×3.

    Note that if you want to use a hot spot (see description of *Monitor Manager* window's *Configuration* section on page 72), the space required for the hot spot will affect the number of camera positions available in the camera layout grid. For example, a 3×3 grid will normally contain nine camera positions; with a 2×2 hot spot, however, only five camera positions will be available.

2. Select a position in the *Monitor Manager* window's camera layout grid.

    The selected position will be indicated in light gray, whereas non-selected positions will be dark gray.

3. Select the required camera from the *Select Camera* list.

   An image from the selected camera will be displayed in the selected camera layout grid position. If an image from the camera is not yet available, a camera icon will appear.

   Note that a disabled camera cannot be selected (for more information about disabling/enabling cameras, see the description of the Administrator window on page 32).
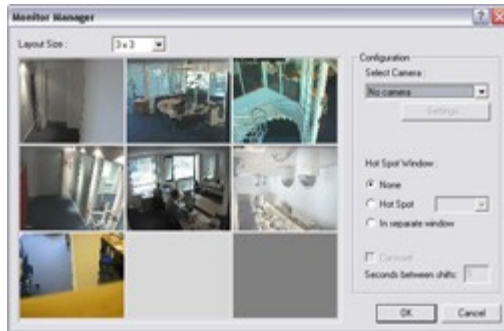
Selecting cameras for positions in the *Monitor Manager* window's camera layout grid

4. Repeat step 2-3 for other required cameras.

Tip: You are always able to change the camera selection for a position in the layout grid. Simply select the required position (when a position already contains a camera image it will be highlighted with a yellow border when you select it), then select a different camera from the *Select Camera* list.

Tip: A Milestone XProtect Enterprise server is capable of handling images from up to 64 cameras at a time. In the *Monitor Manager* window, you are thus able to allocate a maximum of 64 cameras for displaying images in the *Monitor* application. However, a single Milestone XProtect Enterprise server may have an unlimited number of cameras connected to it even though a maximum of 64 of the connected cameras can be used for recording/live viewing simultaneously. Read more in *Cameras Not Included in Monitor Application* on page 131.

Scheduling

Camera/Alert Scheduler Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Camera/Alert Scheduler* window lets you specify when each camera should be online. A camera is online when it is transferring images to the Milestone XProtect Enterprise server for processing.

You are able to specify whether cameras should be online within specific periods of time, or whether they should start and stop transferring images when specific events occur within specific periods of time.

You are also able to specify if e-mail alerts, SMS alerts or sound alerts should be triggered if motion is detected during specific periods of time. If using PTZ (Pan/Tilt/Zoom) cameras with patrolling, you are furthermore able to specify if certain patrol schemes should be used during specific periods of time.

Note: By default, cameras added to Milestone XProtect Enterprise will automatically be online, and you will only need to modify the *Camera/Alerts Scheduler* window's settings if you require cameras to be online only at specific times or events, or if you want to use specific alerts or PTZ patrol schemes. Note, however, that this default may be changed by clearing the *Create Default schedule for new cameras* check box in the *General Settings* window's *Advanced* section (see page 82): If the check box is cleared, added cameras will *not* automatically be online, in which case online schedules must be specified manually.

IMPORTANT: The fact that a camera is online (i.e. transferring images to the Milestone XProtect Enterprise server) will not necessarily mean that images from the camera are recorded (i.e. stored in the camera's database on the Milestone XProtect Enterprise server). Image storage settings for individual cameras are specified in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

Access: To access the *Scheduler* window, click the *Scheduler...* button in the *Administrator* window (see page 30).
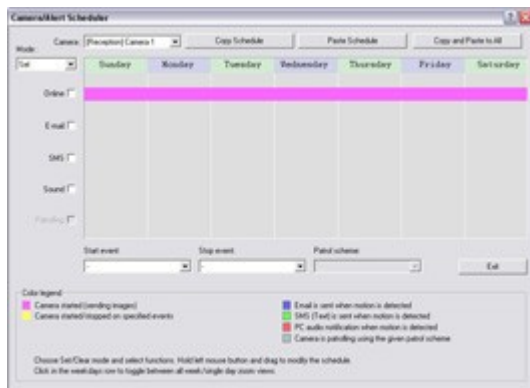
Camera/Alert Scheduler Window

Camera/Alert Scheduler Window's Fields and Check Boxes

Field, Check Box	Description
Camera	Lets you select a particular camera, for which to specify or view a schedule in the window's calendar section. **Note:** Always verify that you have selected the required camera in the list; even though schedules displayed in the calendar section may look—and indeed sometimes be—similar, the displayed schedule refers specifically to the selected camera.
Mode	Select whether to add or delete periods in the calendar section: • *Set*: Add periods. May also be used to overwrite existing periods. • *Clear*: Delete existing periods.

Online	Check the *Online* box when you want to set or clear online periods for the selected camera.
E-mail	Check the *E-mail* box when you want to set or clear periods with e-mail alerts for the selected camera. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
SMS	Check the *SMS* box when you want to set or clear periods with SMS alerts for the selected camera. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).
Sound	Check the *Sound* box when you want to set or clear periods with sound alerts for the selected camera. **Note:** The *Sound* box is solely used when setting or clearing periods with sound alerts. It cannot be used for scheduling audio recordings, as audio recordings are not scheduled separately. If one or more devices on your system supports audio recording, audio is automatically recorded on the devices' camera channel one when the camera is online.
Patrolling	Check the *Patrolling* box when you want to set or clear periods with patrolling for a selected PTZ (Pan/Tilt/Zoom) camera. **Note:** The *Patrolling* box is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.
Start event	When you set an *Online* period, you will be asked whether you want the selected camera to transfer images to the Milestone XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*). If using *On Event*, the *Start event* list lets you select the required start event. **Note:** The use of event-based online periods requires that events have been defined. Read more about events in *About Input, Events and Output* on page 91.
Stop event	When you set an *Online* period, you will be asked whether you want the selected camera to transfer images to the Milestone XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*). If using *On Event*, the *Stop event* list lets you select the required stop event. **Note:** The use of event-based online periods requires that events have been defined. Read more about events in *About Input, Events and Output* on page 91.

Patrol scheme	When you set a *Patrolling* period for a PTZ camera with patrolling, the *Patrol scheme* list lets you select the required patrol scheme.
	Note: The *Patrol scheme* list is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.

Camera/Alert Scheduler Window's Calendar Section

The *Camera/Alert Scheduler* window's calendar section lets you specify exact periods of time for each option for each camera selected in the window's *Camera* list.

Set and Clear modes

Depending on your selection in the *Mode* list, you *Set* or *Clear* periods in the calendar. Your selection is indicated by your mouse pointer turning into either a pencil (*Set*) or an eraser (*Clear*) when inside the calendar section.

Mouse pointer turns into pencil (*Set*) or
eraser (*Clear*) when inside calendar section

Zoom Feature

When placing your mouse pointer inside the weekday band in the top part of the calendar section you get access to the calendar's zoom feature.

With the zoom feature you are able to toggle between the calendar's default seven-day view and a single-day view.

The single-day view provides you with five-minute interval indications, allowing you to specify periods precisely.

Calendar's zoom feature allows you to toggle between seven-day and single-day views'

How to Set or Clear Periods in the Calendar

To set or clear a period in the *Camera/Alert Scheduler* window's calendar section, simply select the required functionality (e.g. *Online* or *E-mail*), then click at the required start point in the calendar, and drag to set/clear a period (depending on whether you have selected *Set* or *Clear* in the window's *Mode* list).

Good to Know when You Set Online Periods

When you set an *Online* period, you will be asked whether you want the selected camera to transfer images to the Milestone XProtect Enterprise software continuously within the specified period (*Always*), or only when an event occurs within the specified period (*On Event*).

If using *On Event*, remember to specify required start and stop events in the *Start event* and *Stop event* lists.

Good to Know when You Set Patrolling Periods

When you set a *Patrolling* period, you may be able to select between several patrol schemes. This will depend upon how many patrol schemes have been specified in the *Setup PTZ Patrolling window* (see page 66).

You select the required patrol scheme from the *Patrol scheme* list, located below the calendar section.

If you set patrolling periods with different patrol schemes immediately following each other in time, changes between patrolling schemes will be indicated by a thin vertical line (see also *Colored Bars* in the following).

Note: The Patrol scheme list is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.

Colored Bars

The calendar uses colored bars to indicate active periods for each option (*Online*, *E-mail*, *SMS*, etc.):

Colored bars indicating
active periods

- In the *Online* bar, active periods are indicated in either pink or yellow:

    - Pink (•) indicates that the selected camera is continuously transferring images to the Milestone XProtect Enterprise software.

    - Yellow (•) indicates that the selected camera transfers images to the Milestone XProtect Enterprise software when a specified event occurs.

- In the *E-mail* bar, active periods are indicated in blue (•).

- In the *SMS* bar, active periods are indicated in green (•).

- In the *Sound* bar, active periods are indicated in red (•).

- In the *Patrolling* bar, active periods are indicated in gray (•). Changes between patrolling schemes are indicated by a thin vertical line. Note that the *Patrolling* bar is only available if you have selected a PTZ camera for which at least one patrol scheme has been set up.

     Tip: When several patrol schemes are in use, you are able to see which patrol scheme is used for a particular period: Click the relevant section of the gray bar; the name of the patrol scheme in question will appear in the *Patrol scheme* list, located below the calendar section.

Camera/Alert Scheduler Window's Buttons

Button	Description
Copy Schedule	Lets you copy the schedule displayed in the calendar section. When used in combination with the *Paste Schedule* button, you are able to quickly re-use schedules from one camera to another.
Paste Schedule	Lets you paste a copied schedule for use with the selected camera. The same copied schedule can be pasted to several cameras simply by selecting, and pasting to, one camera after the other. ⓘ **Tip:** If you want to use a schedule for all cameras, specify a schedule for one camera, then use the *Copy and Paste to All* button to copy the schedule and paste it to all cameras in one go.
Copy and Paste to All	Lets you copy the schedule displayed in the calendar section and paste it to all cameras in one go.
Exit	Closes the *Camera/Alert Scheduler* window and returns you to the *Administrator* window.

General Settings

General Settings Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *General Settings* window lets you manage a number of settings, such as user rights, e-mail and SMS settings, logging, etc.

➡ **Access:** To access the *General Settings* window, click the *General Settings...* button in the *Administrator* window (see page 30).

The *General Settings* window

The *General Settings* window is divided into a number of sections:

Administrator Settings Section

The *General Settings* window's *Administrator Settings* section lets you password protect access to the *Administrator* application, and restrict user rights.

When the *Enable Protection* check box is selected, users must supply the administrator password in order to be able to access the *Administrator* application and in order to be able to use any of the features to which access has been restricted.

Changing the Administrator Password

To change the administrator password, click the *Change Password...* button to open the *Change Password* window (see page 84).

When an administrator password is in use, users accessing the Administrator application, or wishing to use protected features, must type the administrator password in the window before access is granted.

Restricting User Rights

To restrict the rights of users who are not administrators, select the *Enable Protection* check box, then select the features to which users who are not administrators **should** have access:

- *Application Startup*: Allows users to start the *Monitor* application without having to specify the Administrator password.

- *Application Shutdown*: Allows users to close the *Monitor* application.

- *Manual Control*: Allows users to start and stop cameras manually in the *Monitor* application.

- *Start Administrator from Monitor*: Allows users to open the *Administrator* application from the *Monitor* application without having to specify the administrator password.

- *Browser*: Allows users to start the *Viewer* feature in the *Monitor* application. The *Viewer* lets users browse stored images, export images, etc.

- *PTZ Control*: Allows users to use the *Monitor* application's *PTZ Menu* with Pan/Tilt/Zoom controls for installed PTZ cameras.

- *Quick Browse*: Allows users to use the *Monitor* application's *Quick Browse* buttons for browsing newly stored images. Note that use of the *Quick Browse* buttons requires that a Hot Spot is enabled in the *Monitor* application.

Tip: Configuration of user rights may vary from organization to organization. However, users are typically allowed access to the following features: *Application Setup*, *Browser*, *PTZ Control*, and *Quick Browse*.

Milestone XProtect Central Settings Section

Note: Settings in this section are relevant only if you are using the Milestone XProtect Central monitoring solution in connection with Milestone XProtect Enterprise.

The *General Settings* window's *Milestone XProtect Central* section lets you enable and configure access to the surveillance system from a Milestone XProtect Central server in order to retrieve status information and alarms.

To enable access from a Milestone XProtect Central server, select the *Enable Milestone XProtect Central connections* check box, and click the *Settings...* button to open the *Milestone XProtect Central Settings* window (see page 85), in which you specify which login settings the Milestone XProtect Central server should use in order to access the surveillance system.

Patrolling Settings Section

Note: Settings in this section are relevant only if you are using PTZ cameras for which patrolling has been set up.

The regular patrolling of PTZ cameras may be interrupted, either manually or when a particular event occurs.

The *General Settings* window's *Patrolling settings* section lets you specify how many seconds should pass before the regular patrolling is resumed after a manual or event-based interruption. Default is 30 seconds.

The settings in this section will apply for all installed PTZ cameras.

Tip: PTZ patrolling for individual PTZ cameras is configured in the *Setup PTZ Patrolling* window (see page 66).

Joystick Section

Clicking the *Joystick Setup...* button in the *General Settings* window's *Joystick* section opens the *Joystick Setup* window (see page 85), in which you are able to configure a joystick for use with PTZ cameras.

Logfile Settings Section

The *Logfile Settings* section lets you specify where to keep the general log files containing information about activity in the *Administrator* and *Monitor* applications system, and how long for.

Separate log files are generated for the *Administrator* and *Monitor* applications.

Logfile Path

By default, the *Administrator* and *Monitor* log files are stored in the folder containing the Milestone XProtect Enterprise software, typically C:\ProgramFiles\Milestone\Milestone Surveillance\.

To specify another location for your log files, type the path to the required folder in the *Logfile 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 every day. A log file older than the number of days specified in the *Days to log* field is automatically deleted. By default, the log file will be stored for five days.

To specify another number of days, simply overwrite the value in the *Days to log* field.

The current day's activity is always logged, even with a value of *0* in the *Days to log* field. The maximum number of days to log is *9999*.

Tip: Read more about Milestone XProtect Enterprise logging on page 265.

Event Recording Settings Section

As opposed to the general log files, which contain information about activity on the surveillance system itself, event log files contain information about registered events (read more about the various types of events in *Input, Events and Output* on page 91).

The *General Settings* window's *Event Recording Settings* section lets you specify where to keep event log files, and how long for.

Event log files should be viewed using the *Monitor application*'s *Viewer* (see page 142) or the *Smart Client* (see page 210):

- Viewer: Select the *Viewer*'s Alarm Overview control panel, then click the *Events* button to view the events log.

- *Smart Client*: In the *Browse* tab's *Alerts* section, select the required event, then click the *Get List* button to see when the event in question was detected.

Path

By default, the log files are stored in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\Milestone Surveillance\.

To specify another location for your event log files, type the path to the required folder in the *Path* field, or click the browse button next to the field to browse to the required folder.

Days to Keep

A new event log file is created every day. Event log files older than the number of days specified in the *Days to keep* field are automatically overwritten. By default, event log files will be stored for five days.

To specify another number of days, simply overwrite the value in the *Days to keep* field.

The current day's activity is always logged, even with a value of *0* in the *Days to keep* field. The maximum number of days to log is *9999*.

Tip: Read more about Milestone XProtect Enterprise logging on page 265.

Advanced Section

The *General Settings* window's *Advanced* section lets you specify a number of additional settings:

- *Disable Screen Update*: Turns off screen update in the *Monitor* application (see page 133). If selected, all camera images displayed in the *Monitor* application will remain static, with the note "*Screen Update OFF*" displayed across the image from each camera. This will free up system resources, resulting in improved system performance, but will prevent users from viewing any live images through the *Monitor* application.

  Select this option if the *Monitor* application is not used on a daily basis, e.g. if the *Monitor* application is only used when the system administrator adjusts the software configuration.

- *Keyframe-only decoding*: With the MPEG standard, keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. If selected, only MPEG keyframes will be decoded and displayed in the *Monitor* application.

  Note that all frames from the MPEG stream will be stored in the camera database

regardless of whether keyframe-only decoding is selected or not.

- *Disable Online Indicator*: Turns off the blinking green online indicator normally displayed for each camera in the *Monitor* application (see page 133).

- *Keep Aspect Ratio*: If selected, camera images in the *Monitor* application (see page 133) will not be stretched to fit the cells in the *Monitor* application's camera layout. Rather, images will be displayed with the aspect radio with which they have been recorded.

  This may result in horizontal or vertical black bars appearing around the images from some cameras, almost as when viewing a film in the widescreen format on a regular TV screen.

- *Don't send e-mail on camera failures*: If selected, no e-mail alerts will be sent if *Milestone XProtect Enterprise* loses contact with a camera. Otherwise, e-mail alerts will (provided the e-mail alert feature has been enabled in the *E-Mail setup* window (see page 87)) automatically be sent if Milestone XProtect Enterprise loses contact with a camera, regardless of any e-mail alerts periods defined in the *Camera/Alert Scheduler* window (see page 74).

- D*on't send SMS on camera failures*: If selected, no SMS alerts will be sent if *Milestone XProtect Enterprise* loses contact with a camera. Otherwise, SMS alerts will (provided the SMS alert feature has been enabled in the *SMS settings* window (see page 90)) automatically be sent if Milestone XProtect Enterprise loses contact with a camera, regardless of any e-mail alerts periods defined in the *Camera/Alert Scheduler* window (see page 74).

- *Add Monitor to Startup group*: Adds the *Monitor* application (see page 133) to Windows' Startup group, making the *Monitor* application open automatically each time Windows is started on the computer.

- *Allow cameras to run in the background*:
  If selected, it will be possible to let some or all of the cameras connected to the Milestone XProtect Enterprise server run "in the background," i.e. without the cameras being included in the *Monitor* application (see page 133). For such "background" cameras, the features of the *Monitor* application will not be immediately available (although recorded images from such cameras can still be browsed in the *Monitor* application's *Viewer* (see page 142)). However, "background" cameras can be accessed for viewing of live and recorded images through a *Remote Client* (see page 171) or *Smart Client* (see page 210). For further information, see *Using Background Cameras* on page 131. If *Allow cameras to run in the background* is not selected, cameras *must* be included in the in the *Monitor* application in order to be accessible; you include cameras in the *Monitor* through the *Monitor Manager* window (see page 71).

- *Start cameras on remote live requests*: Cameras may be stopped, either manually in the *Monitor* application (see page 133) or because they have reached the end of an online schedule (see page 74), in which case *Remote Client* (see page 173) and *Smart Client* (see page 210) users will not be able to view live images from the cameras. However, if *Start cameras on remote live requests* is selected, *Remote Client* and *Smart Client* users will be able to start the camera in the *Monitor* in order to view live images from the cameras.

- *Create default schedule for new cameras*: If selected (default), a schedule specifying that the camera is always online (i.e. transferring images to Milestone XProtect Enterprise) will automatically be created in the *Camera/Alert Scheduler* window (see page 74). The automatically created schedule can be edited manually at any time. If not selected, no schedule will automatically be created; meaning that the camera will not automatically be transferring images to Milestone XProtect Enterprise. When required, schedules can then be added manually in the *Camera/Alert Scheduler* window.

Email Settings

Clicking the *General Settings* window's *Email Settings...* button opens the *E-Mail setup* window (see page 87), in which you enable and configure the use of e-mail alerts.

Sms Settings

Clicking the *General Settings* window's *Sms Settings...* button opens the *SMS settings* window (see page 90), in which you enable and configure the use of SMS alerts.

Note: Use of the SMS alert feature requires that an external Siemens TC-35 GSM modem has been attached to a serial port on the computer running the Milestone XProtect Enterprise software.

Change Password Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Change Password* window lets you change the administrator password for your Milestone XProtect Enterprise solution.

The *Change Password* window

 Access: To access the *Change Password* window, click the *Change Password...* button in the *General Settings* window (see page 79).

How to Change the Administrator Password

To change the administrator password, do the following:

1. Specify the current administrator password in the *Old password* field

2. Specify the new administrator password in the *New password* field

3. Repeat the new administrator password in the *New password (confirm)* field

4. Click *OK*.

Milestone XProtect Central Settings Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights. Settings in the *Milestone XProtect Central Settings* window are relevant only if you are using the Milestone XProtect Central monitoring solution in connection with Milestone XProtect Enterprise.

The *Milestone XProtect Central Settings* window lets you specify the login settings required for a Milestone XProtect Central server to access the surveillance system (the Milestone XProtect Enterprise server) in order to retrieve status information and alarms.

The *Milestone XProtect Central Settings* window

Access: To access the *Milestone XProtect Central Settings* window, click the *Settings...* button in the *Milestone XProtect Central Settings* section of the *General Settings* window (see page 79).

Specify login settings for the Milestone XProtect Central server in the following fields:

- *Engine Login*: Type the name of Milestone XProtect Enterprise server, also known as an *engine*. Must match the name specified on the Milestone XProtect Central server itself. Default name is *Engine1Name*.

- *Engine Password*: Type the password used for accessing the Milestone XProtect Enterprise server. Must match the password specified on the Milestone XProtect Central server itself. Default password is *Engine1Pass*.

- *Engine Port*: Type the port number the Milestone XProtect Central server should connect to when accessing the Milestone XProtect Enterprise server. Must match the port number specified on the Milestone XProtect Central server itself. Default port is 1237.

- *Engine IP*: When the Milestone XProtect Central server retrieves alarms from the Milestone XProtect Enterprise server, the Milestone XProtect Enterprise server includes information about its IP address in the alarm information. If the Milestone XProtect Central server accesses the Milestone XProtect Enterprise server over the internet, or if the Milestone XProtect Enterprise server has two or more network adapters, you must specify the IP address to which the Milestone XProtect Central server should connect in order to retrieve alarms. If you do not specify an IP address, the IP address of the first network adaptor found on the surveillance system will be used.

Joystick Setup Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Joystick Setup* window lets you configure joystick control of PTZ cameras. Joystick configuration control requires that a joystick is attached to the computer running Milestone XProtect Enterprise.

The *Joystick Setup* window

➡ **Access:** To access the *Joystick Setup* window, click the *Joystick Setup...* button in the *General Settings* window (see page 79).

The *Joystick Setup* window is divided into two sections: a *Joystick Axes* section and a *Joystick Buttons* section.

Joystick Axes Section

The *Joystick Setup* window's *Joystick Axes* section lets you configure the axes used for the joystick.

With a joystick, you are able to navigate PTZ camera images three-dimensionally, along three axes: an X-axis, a Y-axis, and a Z-axis, where the Z-axis refers to the depth (zoom) level:
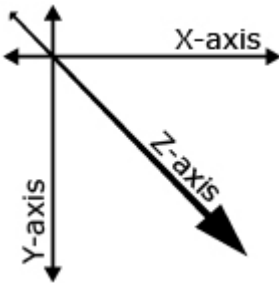
Example: X-, Y-, and Z-axes

Button, Check Box	Description
Invert y-axis	Lets you invert the joystick's Y-axis. This way, you are able to select whether the PTZ camera should move up or down when you move the joystick towards you and away from you respectively.
z-axis uses a relative positioning scheme	Lets you specify whether the Z-axis should use a relative or an absolute positioning scheme. This will affect the way you zoom in and out with PTZ camera.
Default values	Resets axes settings, letting you use the joystick's default axes settings.

Joystick Buttons Section

The *Joystick Buttons* section lets you specify which joystick buttons should be used for particular actions.

To assign an action to a particular joystick button, select the required action in the list, then click the required joystick button.

When a button is assigned to an action, the name of the button will be listed together with the name of the action.

To stop using a particular joystick button for a particular action, select the button/action in the list, then click the *Unselect* button.

To free all joystick buttons from their associated actions, click the *Unselect All* button.

E-Mail Setup Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *E-Mail setup* window lets you enable and configure the use of e-mail alerts.

The *E-mail setup* window

Access: To access the *E-Mail setup* window, click the *Email Settings...* button in the *General Settings* window (see page 79).

Enabling E-mail Alerts

You enable e-mail alerts separately for the *Monitor* application (see page 133) and its *Viewer* feature (see page 142):

- *Enable E-Mail (Monitor)*: Select check box to enable the use of e-mail alerts in the *Monitor* application.

- *Enable E-Mail (Viewer)*: Select check box to enable the use of e-mail alerts in the *Monitor* application's *Viewer* feature. In effect, this will display the *E-Mail Report* button in the *Viewer*'s toolbar, enabling users to send evidence via e-mail. If you clear the check box, users will not see the *E-Mail Report* button in the *Viewer*'s toolbar.

Note: When enabling e-mail alerts, also consider the e-mail alert schedules configured for each camera in the *Camera/Alert Scheduler* window (see page 74).

Specifying Recipients and Default Texts

Specify e-mail alert recipients and texts in the following fields:

- *Recipient(s)*: Specify e-mail addresses to which alerts should be sent. If specifying more than one e-mail address, separate e-mail addresses with semicolons (example: aa@aa.aa;bb@bb.bb).

- *Subject text*: Specify required subject text for e-mail alerts.

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

Note: If e-mail alerts are enabled for the *Viewer*, the content you specify in the *Recipient(s)*, *Subject text*, and *Message text* fields will appear as default values in the *Viewer*'s dialog for sending evidence via e-mail. Users will be able to overwrite these default values.

Specifying Image and Interval Options

You are able to specify whether e-mail alerts should include images, and how much time should pass between alerts per camera:

- *Include Image*: Select check box to include images in e-mail alerts. When selected, a JPG file containing the image that generated the alert will be attached to each alert e-mail.

- *Time btw. mails (minutes)*: Specify required minimum time (in minutes) to pass between the sending of each e-mail alert per camera.

  Examples: If specifying *5*, a minimum of five minutes will pass between the sending of each e-mail alert per camera, even if motion is detected in between. If specifying *0*, e-mail alerts will be sent each time motion is detected, potentially resulting in a very large number of e-mail alerts being sent. If using the value *0,* you should therefore consider the motion detection sensitivity configured for each camera in the *Adjust Motion Detection* window (see page 53).

Advanced E-mail Settings

By default, your existing e-mail client, e.g. Microsoft Office Outlook, is used for sending e-mail alerts.

However, use of SMTP (Simple Mail Transfer Protocol) is recommended. Using SMTP will help you avoid automatically triggered warnings from your e-mail client. Such automatically triggered warnings may otherwise inform you that your e-mail client is trying to automatically send an e-mail message on your behalf whenever an e-mail alert is triggered.

By clicking the *Advanced...* button to access the *Advanced e-mail setup* window (see page 89), you are able to specify that SMTP should be used. You are also able to specify settings for the SMTP server.

Testing Your E-mail Alert Configuration

You are able to test your e-mail alert configuration by clicking the *Test* button.

This will send a test e-mail to the specified recipients. If *Include Image* is selected, the test e-mail will have a test JPG image attached.

Advanced E-mail Setup Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Advanced e-mail setup* window lets you specify whether your existing e-mail client, e.g. Microsoft Office Outlook, or SMTP (Simple Mail Transfer Protocol) should be used for sending e-mail alerts

Use of SMTP is recommended. Using SMTP will help you avoid automatically triggered warnings from your e-mail client. Such automatically triggered warnings may otherwise inform you that your e-mail client is trying to automatically send an e-mail message on your behalf whenever an e-mail alert is triggered.

If selecting SMTP, you are able to specify settings for the SMTP server.

The *Advanced e-mail setup* window

Access: To access the *Advanced e-mail setup* window, click the *Advanced...* button in the *E-Mail setup* window (see page 87).

Selecting Required E-mail Method

Specify required method by selecting one of the following options:

- *Use existing mail profile to send mail*: Select to use existing e-mail client, such as Microsoft Office Outlook, for sending e-mail alerts. Default selection.

- *Use SMTP to send mail*: Select to use SMTP for sending e-mail alerts.

SMTP Settings

If you select to use SMTP for sending e-mail alerts, specify the following:

- *Sender e-mail address*: Type e-mail address of sender.

- *Outgoing mail (SMTP) server name*: Type name of SMTP server to be used for sending e-mail alerts.

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

- *Username*: Field available only when *Server requires login* is selected. Type user name required for using SMTP server.

- *Password*: Field available only when *Server requires login* is selected. Type password required for using SMTP server.

SMS Settings Window

The *SMS settings* window lets you enable and configure the use of SMS alerts.

The *SMS settings* window

Access: To access the *SMS settings* window, click the *Sms Settings...* button in the *General Settings* window (see page 79).

Enabling SMS Alerts

You enable SMS alerts by selecting the *Enable SMS* check box.

Specifying SMS Alert Settings

Having selected the *Enable SMS* check box, specify SMS alert settings in the following fields:

- *GSM modem con. to*: Select port connecting the computer running Milestone XProtect Enterprise to the GSM modem.

- *SIM card PIN code*: Specify PIN code for the SIM card inserted in the GSM modem.

- *SIM card PUK code*: Specify PUK code for the SIM card inserted in the GSM modem.

- *SMS Central Phone No.*: Specify the number of the SMS central to which the GSM modem should connect in order to send an SMS.

- *Recipient Phone No.*: Specify the telephone number of the telephone to which SMS alerts should be sent.

- *Message*: Specify required message text for SMS alerts. Message text must be no longer that 100 characters, and must only contain the following characters: a-z, A-Z, 0-9 as well as commas (,) and full stops (.).

  Note that camera information as well as date and time information is automatically included in alerts.

- *Time btw. transmissions*: Specify required minimum time (in minutes) to pass between the sending of each SMS alert per camera.

  Examples: If specifying *5*, a minimum of five minutes will pass between the sending of each SMS alert per camera, even if motion is detected in between. If specifying *0*, SMS alerts will be sent each time motion is detected, potentially resulting in a very large number of SMS alerts being sent. If using the value *0*, you should therefore consider the motion detection sensitivity configured for each camera in the *Adjust Motion Detection* window (see page 53).

Testing Your SMS Alert Configuration

You are able to test your SMS alert configuration by clicking the *SMS settings* window's *Test* button. This will send a test SMS to the specified recipients.

Input, Events and Output

About Input, Events and Output

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Input received from a wide variety of sources can be used to generate events in Milestone XProtect Enterprise.

Events can in turn be used for automatically triggering actions in Milestone XProtect Enterprise, such as starting or stopping recording on cameras, triggering e-mail or SMS notifications, making PTZ cameras move to specific preset positions, etc. Events can also be used for activating output.

Output units can be attached to output ports on many devices, allowing you to activate lights, sirens, etc. from Milestone XProtect Enterprise. Such external output can be activated automatically by events, or manually from the *Monitor* application (see page 133), *Remote Client* (see page 171) and *Smart Client* (see page 210).

Four Types of Events

You specify which types of input should generate which types of events. Basically, four types of events exist:

- On many devices you are able to attach external input units to input ports on the device. Events based on input from such external input units—typically sensors attached to doors, windows, etc.—are called **input events**.

- Input may also be received in the form of TCP or UDP data packages, which can be analyzed and, if matching specified criteria, used to generate events. Such events are called **generic events**.

- Events may be based on detected motion on a camera. Such events are called **VMD (i.e. Video Motion Detection) events**.

- Finally, events may be generated manually by users clicking custom-made buttons in Milestone XProtect Enterprise. Such buttons are called **event buttons**.
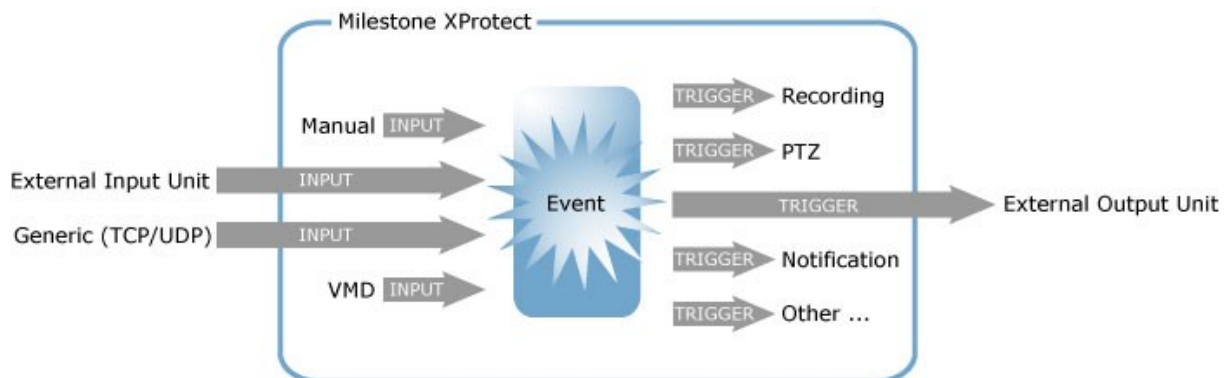
Events—whether based on manual input, based on input from external input units, based on received TCP/UDP data packages, or based on detected motion—can trigger a wide variety of actions.

Specifying Input, Events and Output

In Milestone XProtect Enterprise, your main entry point for configuration of input, event and output handling is the *Administrator* window (see page 30):

- By clicking the *Administrator* window's *I/O Setup...* button, you open the *I/O Setup* window (see page 93), in which you are able to specify each individual **input event**, **VMD event** as well as **output**.

- By clicking the *Administrator* window's *Event Buttons...* button, you open the *Event Buttons* window (see page 106), in which you are able to specify **event buttons** for manually triggering events-controlled activity.

- By clicking the *Administrator* window's *Generic Events...* button, you open the *Generic Events* window (see page 110), in which you are able to specify **generic events**.

- By clicking the *Administrator* window's *I/O Control...* button, you open the *I/O Control* window (see page 121), in which you are able to **associate specific events with specific output**. This way you can, for example, specify that when motion is detected on a camera (VMD event) a siren should automatically sound (output). If you want users to be able to manually activate output when operating specific cameras, you specify this in the *Output Settings for [Device Name] [Camera Name]* window (see page 57).

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

Using Dedicated I/O Devices

In addition to IP video camera devices and IP video server devices it is possible to add a number of dedicated I/O (input/output) devices to Milestone XProtect Enterprise (see *How to Add a Device* on page 36). For information about which I/O devices are supported, refer to the release note.

When such I/O devices are added, input on the I/O devices can be used to generate events in Milestone XProtect Enterprise, and events in Milestone XProtect Enterprise can be used for activating output on the I/O devices. This means that I/O devices can be used in your events-based system setup in the same way as a camera.

Note: When using some I/O devices it is necessary for the surveillance system to regularly check the state of the devices' input ports in order to detect whether input has been received. Such state checking at regular intervals is called *polling*. The interval between state checks, called a *polling frequency*, is specified in the *Advanced* window (see page 104). For such I/O 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 devices require polling, see the release note.

I/O Setup

I/O Setup window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *I/O Setup* window lets you define external input events, VMD (Video Motion Detection) events and output for devices on your surveillance system.

When events occur, they can trigger one or more actions:

- *Input events* occur when input from an external input unit is received on a device's input port, for example when an external sensor detects that a door is opened

- *VMD events* occur when motion is detected on a particular camera

- *Outputs* are used for activating external output units, for example for switching on lights or sounding a siren

The *I/O Setup* window is used for defining which input events, VMD events and outputs should be available on your system.

Input and VMD events can be used for triggering outputs or for triggering various actions on the surveillance system itself, such as for starting or stopping cameras (configured in the *Camera/Alert Scheduler* window (see page 74)) or for moving a PTZ camera to a particular preset position (configured in the *Event* window (for PTZ preset positions on event) (see page 65)).

Once you have defined input events, VMD events and outputs, you are able to associate specific input events or VMD events with specific outputs in the *I/O Control* window (see page 121), so that, for example, lights are switched on when a door is opened or when motion is detected on a camera. Outputs may also be triggered by motion detection on a specific camera—even without a defined VMD event—or manually through output buttons in the Monitor application; both are configured in the *Output Settings for [Device Name] [Camera Name]* window (see page 57).
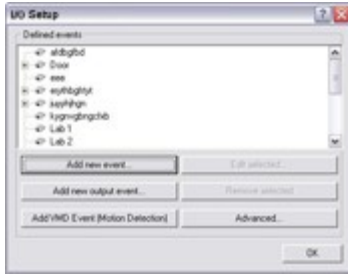
The *I/O Setup window*

Access: You access the *I/O Setup* window by clicking the *I/O Setup...* button in the *Administrator* window (see page 30).

Note: Before you specify inputs and outputs for a device, verify that sensor operation is recognized by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the Milestone XProtect Enterprise release note to verify that input and output controlled operations are supported for the device and firmware used.

I/O Setup Window's Defined Events List and Buttons

The *I/O Setup* window features a *Defined events* list, in which events and output defined for each device are listed, as well a number of buttons used when configuring the events:

Button	Description
Add new event...	Used for defining input events on the device selected in the *Defined events* list. Depending on the type of device, you may be able to define one or more input events on the device. Some devices do not support input/output at all. Refer to the release notes for device-specific information. **Devices Capable of Handling One Input Event Only** If the device is capable of handling one input event only, the button will open the *Add New Event* window (for devices handling one input only) (see page 96), in which you define the input event, and any e-mail or SMS alerts to be associated with it. If you have already defined an input event on a device capable of handling one input event only, the *Add new event...* button will not be available when the device is selected in the *Defined events* list. However, if you click the plus sign next to the device in the *Defined events* list, and select the defined input event, the *Add new event...* button becomes available for defining timer events (see *Timer Events* in the following). **Devices Capable of Handling Several Input Events** If the device is capable of handling more than one input event, the button will open the *Multiple Input Events* window (see page 97), in which you define which of the device's possible input events should be enabled, and whether any alerts should be associated with enabled input events. **Timer Events** When you click the plus sign next to the device in the *Defined events* list,

	and select a defined input event, the *Add new event...* button becomes available for defining timer events:
	When clicked, the button will open the *New Timer* window (see page 101), in which you are able to specify the settings for timer events.
	Timer events are separate events, triggered by the input event under which they are defined.
	Timer events occur a specified number of seconds or minutes after the input event under which they are defined.
	Timer events may be used for a wide variety of purposes; the following are examples only:
	• A camera starts based on an input event, e.g. when a door is opened, a timer event stops the camera after 15 seconds
	• A camera starts and the lights are switched on based on an input event, e.g. when a door is opened, a timer event stops the camera after one minute, and another timer event switches the lights off after two minutes
Add new output event...	Opens the *Add New Output* window (see page 102), in which you are able to specify a name for the required output event, which of the device's output ports to use, and how long to keep the output for.
Add VMD Event (Motion Detection)	Lets you add a VMD (Video Motion Detection) event to the device selected in the *Defined Events* list.
	VMD events are events triggered by detected motion on a specific camera. VMD events can be used just like regular input events. For example, a PTZ (Pan/Tilt/Zoom) camera could move to a specific preset position when a VMD event occurs.
	Note: Exactly what constitutes motion on a particular camera depends on the camera-specific motion detection settings defined in the *Adjust Motion Detection* window (see page 53).
	Only one VMD event can be defined per camera.
	In order to avoid the risk of an excessively high number of VMD events being generated, a VMD event cannot occur more frequently than every five seconds.
	The *Add VMD Event (Motion Detection)* button works slightly different depending on whether the selected device is a single-camera device or a multi-camera device, such as a video server:
	• *Single-camera devices*: Clicking the *Add VMD Event (Motion Detection)* button will instantly add a VMD event to the selected device, provided a VMD event has not already been defined for the device.
	• *Multi-camera devices*: Clicking the *Add VMD Event (Motion Detection)* button will open a simple dialog in which you select the required camera. This way you are able to define a VMD event for each camera on a multi-camera device.

Edit selected...	Lets you edit the settings for an item selected in the *Defined events* list.

For devices capable of handling a single input event only, the button will open the *Edit Event* window (for editing input events) (see page 100).

For devices capable of handling several input events, the button will open the *Multiple Input Events* window (see page 97).

If the selected item is a timer event, the button will open the *New Timer* window (see page 101).

If the selected item is an output, the button will open the *Edit Output* window (see page 103). |
| **Remove selected** | Lets you remove an event selected in the *Defined events* list.

Note: The selected event will be removed without further warning. |
| **Advanced** | Opens the *Advanced* window (see page 104), in which you are able to specify network settings to be used in connection with event handling: which ports to use for FTP, alerts and SMTP input/output events as well as which polling frequency to use on devices requiring polling. |

Add New Event Window (for Devices Handling One Input Only)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Add New Event* window (for devices handling one input only) lets you specify the settings for an input event on devices capable of handling one input event only.
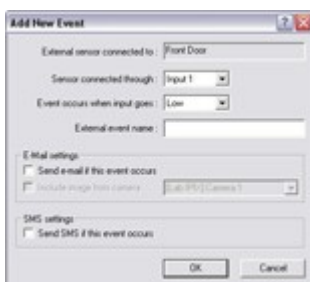
The *Add New Event* window (for devices handling one input only)

Access: You access the *Add New Event* window (for devices handling one input only) by selecting the required device and clicking the *Add new event...* button in the *I/O Setup* window (see page 93). Note that this only applies when the selected device is capable of handling a single input event only. Some devices are capable of handling several input events, in which case a different window, the *Multiple Input Events* window (see page 97), will open when the *Add new event...* button is clicked.

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

Add New Event Window's Fields

The *Add New Event* window (for devices handling one input only) contains the following fields:

Field	Description
External sensor connected to	Read-only field, displaying the name of the device on which the input event is defined.
Sensor connected through	Lets you select which of the device's input ports the sensor used for the input event is connected to.
Event occurs when input goes	Lets you select whether input event should be triggered when the signal on the input sensor rises or falls: • *Low*: Trigger input event when the signal on the sensor is falling • *High*: Trigger input event when the signal on the sensor is rising For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the sensor and device in question.
External event name	Lets you specify a name for the input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the input occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert, then select the required camera in the list next to the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

Multiple Input Events Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Multiple Input Events* window is used for devices capable of handling several input events. It lets you define which of the device's possible input events should be enabled, and whether any alerts should be associated with enabled input events.

The *Multiple Input Events* window

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

Access: You access the *Multiple Input Events* window by clicking the *Add new event...* button in the *I/O Setup* window (see page 93). Note that this only applies when the device selected in the *I/O Setup* window is capable of handling several input events. Some devices are capable of handling a single input event only, in which case a different window, the *Add New Event* window (for devices handling one input only) (see page 96), will open when the *Add new event...* button is clicked.

Multiple Input Events Window's Fields and Buttons

The *Multiple Input Events* window features the following fields and buttons:

Field	Description
External sensor connected to	Read-only field, displaying the name of the device on which the input events are defined.
Available Input Event(s)	Lists available input events for the device, typically with an input event for rising and falling signals on each of the device's input ports. For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the sensors and device in question.
Enabled Input Event(s)	Lists enabled input events for the device. You enable an event by selecting it in the *Available Input Event(s)* list, then clicking the >> button. See description in the following.
>>	You enable an event by selecting it in the *Available Input Event(s)* list, then clicking the >> button to open the *Add New Event* window (for devices handling several inputs) (see page 99) in which you specify a name for the input event, and any e-mail or SMS alerts to be associated with it. When you click *OK* in the *Add New Event* window (for devices handling several inputs), the selected input event is automatically transferred from *Available Input Event(s)* list to the *Enabled Input Event(s)* list.
<<	Lets you move an input event selected in the *Enabled Input Event(s)* list to the *Available Input Event(s)* list, thus disabling it.
Edit	Lets you edit the settings for an input event selected in the *Enabled Input Event(s)* list.

Add New Event Window (for Devices Handling Several Inputs)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Add New Event* window (for devices handling several inputs) lets you specify the settings for a particular input event on devices capable of handling several input events.
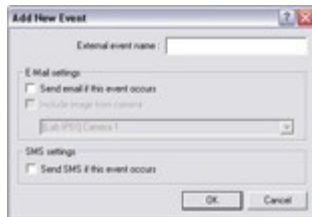
The *Add New Event* window (for devices handling several inputs)

Access: You access the *Add New Event* window (for devices handling several inputs) by clicking the >> button in the *Multiple Input Events* window (see page 97).

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

Add New Event Window's Fields

The *Add New Event* window (for devices handling several inputs) contains the following fields:

Field	Description
External event name	Lets you specify a name for the particular input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send email if this event occurs	Select check box to send an e-mail alert when the input occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

Edit Event Window (for Editing Input Events)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Edit Event* window (for editing input events) lets you edit the settings for an existing input event on devices capable of handling one input event only.

The *Edit Event* window (for editing input events)

Access: You access the *Edit Event* window (for editing input events) by selecting the required device and clicking the *Edit selected...* button in the *I/O Setup* window (see page 93). Note that this only applies when the selected device is capable of handling a single input event only. Some devices are capable of handling several input events, in which case a different window, the *Multiple Input Events* window (see page 97), will open when the *Edit selected...* button is clicked.

Edit Event Window's Fields

The *Edit Event* window (for editing input events) contains the following fields:

Field	Description
External sensor connected to	Read-only field, displaying the name of the device on which the input event is defined.
Sensor connected through	Lets you select which of the device's input ports the sensor used for the input event should be connected to.
Event occurs when input goes	Lets you select whether the input event should be triggered when the signal on the input sensor rises or falls: • *Low*: Trigger input event when the signal on the sensor is falling • *High*: Trigger input event when the signal on the sensor is rising For exact information about what constitutes a falling and a rising signal respectively, refer to documentation for the sensor and device in question.
External event name	Lets you edit the name of the input event. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the input occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must

	have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the input event is triggered, in the e-mail alert then select the required camera in the list next to the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

New Timer Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *New Timer* window lets you specify the settings for timer events.

Timer events are separate events, triggered by the input event, VMD Event, Generic Event or event button 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 or the event button under which they have been defined has been clicked.

Timer events may be used for a wide variety of purposes; the following are examples only:

- A camera starts when an event button is clicked; a timer event stops the camera after 15 seconds

- A camera starts and the lights are switched on based on an input event, e.g. when a door is opened; a timer event stops the camera after one minute, and another timer event switches the lights off after two minutes

The *New Timer* window

Access: You are able to access the *New Timer* window in three ways:

- If dealing with input or VMD events in the *I/O Setup* window (see page 93): When you click the plus sign (⊞) next to a device in the window's *Defined events* list, and select a defined event, you are able to click the *Add new event...* button to access the *New Timer* window.

- If dealing with event buttons in the *Event Buttons* window (see page 106): When select an already specified event button in the *Defined Events* list, you are able to click the *Add new event...* button to access the *New Timer* window.

- If dealing with TCP- and/or UDP-based events in the *Generic Events* window (see page 110): When selecting an already specified event in the *Defined Events* list, you are able to click the *Add new event...* button to access the *New Timer* window.

New Timer Window's Fields

The *New Timer* window features the following fields:

Field	Description
Timer event is started by	Read-only field, displaying the name of the event or event button under which the timer event is defined.
Timer event name	Lets you specify a name for the timer event.

Note: Event names must not contain the following characters: < > & ' " \ / : * ?| [ ] |
| Timer event occurs after | Lets you specify the amount of time that should pass between the event occurring/event button being clicked and the timer event.

Specify the required amount of time in either seconds or minutes.

Examples:

- The timer event should occur 15 seconds after the event under which it is defined has occurred

- The timer event should occur 2 minutes after the event button under which it has been defined has been clicked |

Add New Output Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Add New Output* window lets you specify the settings for an output on a device.
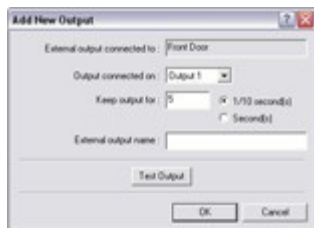
The *Add New Output* window

Note: Before you specify output for a device, verify that the output is supported by the device. Most devices are capable of showing this in their configuration interfaces, or via CGI script commands. Also check the Milestone XProtect Enterprise release note to verify that output is supported for the device and firmware used.

Access: You access the *Add New Output* window by selecting the required device and clicking the *Add new output event...* button in the *I/O Setup* window (see page 93). If the device does not support output, the button will not be available.

Add New Output Window's Fields

The *Add New Output* window contains the following fields:

Field	Description
External output connected to	Read-only field, displaying the name of the device on which the output event is defined.
Output connected on	Lets you select which of the device's output ports the output is connected to.
Keep output for	Lets you specify the amount of time for which the output should be applied, in either 1/10 seconds or seconds. Example: The output should be kept for five tenths of a second.
External output name	Lets you specify a name for the output. **Note:** Output names must not contain the following characters: < > & ' " \ / : * ? | [ ]

Testing Defined Output

When you have defined settings for the output in question, you are able to test the output by clicking the *Test Output* button.

Edit Output Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Edit Output* window lets you specify the settings for an output on a device.

The *Edit Output* window

Access: You access the *Edit Output* window by selecting the required output in the *I/O Setup* window (see page 93), then clicking the *Edit selected...* button.

Edit Output Window's Fields

The *Edit Output* window contains the following fields:

Field	Description
External output connected to	Read-only field, displaying the name of the device on which the output event is defined.
Output connected on	Lets you edit which of the device's output ports the output is connected to.

Keep output for	Lets you edit the amount of time for which the output should be applied, in either 1/10 seconds or seconds.
External output name	Lets you edit the name of the output.
	Note: Output names must not contain the following characters: < > & ' " \ / : * ? | [ ]

Testing Defined Output

When you have defined settings for the output in question, you are able to test the output by clicking the *Test Output* button.

Advanced Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

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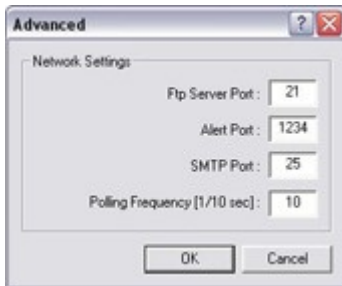
The *Advanced* window

 Access: You access the *Advanced* window by clicking the *Advanced...* button in the *I/O Setup* window (see page 93).

Advanced Window's Fields

The *Advanced* window contains the following fields:

Field	Description
Ftp Server Port	Lets you specify port number to use for sending event information from the device to the surveillance system via FTP. Default port is port 21.
Alert Port	Lets you specify port number to use for handling event-based alerts. Default port is port 1234.
SMTP Port	Lets you specify port number to use for sending event information from the device to the surveillance system via SMTP. Default port is port 25.
Polling Frequency [1/10 sec]	For a small number of devices, primarily I/O devices (see *Using Dedicated I/O Devices* on page 93), it is necessary for the surveillance system to regularly check the state of the devices' input ports in order to detect whether input has been received.

> Such state checking at regular intervals is called *polling*. The *Polling Frequency* field lets you specify the interval between state checks.
>
> Interval is specified in tenths of a second. Default value is 10 tenths of a second (i.e. one second).
>
> For I/O 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 devices require polling see the release note.

Event Buttons

About Event Buttons

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

Event buttons are configurable buttons allowing users to manually trigger events from the *Monitor* application (see page 133) and *Smart Client* (see page 210). In the *Smart Client*, event buttons are actually not buttons; instead users manually trigger events by selecting them from a list.
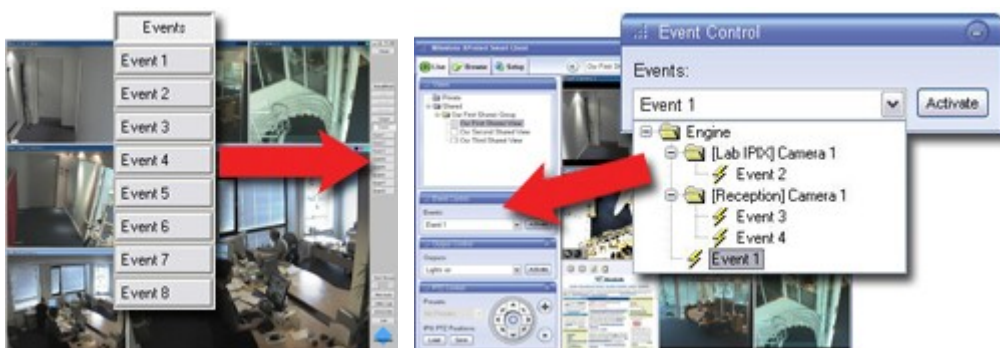
Example of event buttons displayed in the *Monitor* application and as a list in the *Smart Client*

You are able to configure event buttons to suit the exact needs of your organization.

Your main entry point for configuring event buttons is the *Administrator* window (see page 30): Clicking the *Administrator* window's *Event Buttons...* button will open the *Event Buttons* window (see page 106), in which you specify each individual event button.

Event buttons can be used for a wide variety of purposes, for example:

- As start and stop events for use in the *Camera/Alert Scheduler* window (see page 74).

  For example, you can make a camera start or stop transferring images to the surveillance system when an event button is clicked in the *Monitor* application.

- As start and stop events for use in the *Camera Settings for [Device Name] [Camera Name]* window (see page 44).

  For example, you can make a camera use a higher frame rate when an event button is clicked in the *Monitor*, or you can use an event button for manually triggering PTZ preset positions on event (see page 65).

- For triggering outputs. Particular outputs can be associated with the clicking of an event button; you do this in the *I/O Control* window (see page 121).

- For triggering event-based e-mail and/or SMS alerts.

- In combinations. For example, the clicking of an event button could make a camera start transferring images to the surveillance system while two outputs are triggered and an e-mail alert is sent to relevant people.

Global and Camera-specific Event Buttons

Event buttons can be global (available for all cameras included in the *Monitor*) or tied to a particular camera (only available when the camera is selected in the *Monitor*).

Read more about specifying the two types of event buttons in the following description of the *Event Buttons* window.

Event Buttons Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Event Buttons* window (for specifying event buttons) lets you specify buttons for manually triggering events-controlled activity.

When specified, event buttons become available in the *Monitor* application (see page 133) and *Smart Client* (see page 210) (in the *Smart Client*, event buttons are actually not buttons; instead users manually trigger events by selecting them from a list).

Event buttons can be global (available for all cameras in the *Monitor*) or tied to a particular camera (only available when the camera is selected in the *Monitor).*
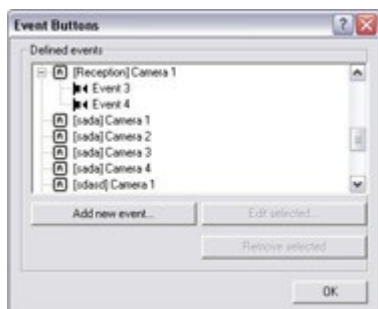
The *Even Buttons* window

Access: You access the *Event Buttons* window by clicking the *Event Buttons...* button in the *Administrator* window (see page 30).

Defined Events List

The *Event Buttons* window features a list of specified event buttons.

When event buttons have been defined, you are able to expand elements in the list (by clicking ⊞) to get an overview of all defined event buttons; global event buttons as well as event buttons specified for individual cameras.

Example:

Expanded *Defined Event* list: A global event button with an associated timer event has been specified. Also, two event buttons have been specified for an individual camera.

Specifying Event Buttons and Timer Events

To specify an event button, first determine whether you want the event button to be available globally or for a particular camera only.

Note: Only eight event buttons can be displayed at a time in the *Monitor* application. When specifying event buttons for individual cameras, bear in mind that global event buttons are displayed for all cameras: If you have already defined, for example, three global event buttons, you will be able to specify a maximum of five event buttons for each individual camera before you reach the maximum of eight displayable event buttons.

In the *Smart Client*, users select manually triggered events from a list rather than by clicking event buttons. The *Smart Client* is thus able to display an unlimited number of events for manual triggering (for simplicity reasons also referred to here as *event buttons*).

Specifying Global Event Buttons

To specify a global event button, select the *Global* entry at the top of the *Defined Events* list, then click the *Add new event...* button.

This will open the *Add New Event* window (for adding event buttons) (see page 108), in which you specify a name for the event button as well as whether the event button should trigger any e-mail or SMS alerts when clicked.

When you click *OK* in the *Add New Event* window (for adding event buttons), you are returned to the *Event Buttons* window, in which your new event button will appear in the *Defined Events* list.

Specifying Camera-specific Event Buttons

To specify an event button for a specific camera, select the required camera in the *Defined Events* list, then click the *Add new event...* button.

This will open the *Add New Event* window (for adding event buttons) (see page 108), in which you specify a name for the event button as well as whether the event button should trigger any e-mail or SMS alerts when clicked.

When you click *OK* in the *Add New Event* window (for adding event buttons), you are returned to the *Event Buttons* window, in which your new event button will appear in the *Defined Events* list.

Specifying Timer events

When you have specified an event button, you are able to associate timer events with the event button.

Timer events are separate events, occurring a specified number of seconds or minutes after the event button has been clicked. Timer events may be used for a wide variety of purposes; the following are examples only:

- A camera starts when an event button is clicked in the *Monitor* application; a timer event stops the camera after 15 seconds

- A camera starts and the lights are switched on when an event button is clicked in the *Monitor* application; a timer event stops the camera after one minute, and another timer event switches the lights off after two minutes

To define a timer event for an event button, select the required event button in he *Defined Events* list, then click the *Add new event...* button.

When you click the *Add new event...* button while an already specified event button is selected in the *Defined Events* list, the *New Timer* window (see page 101) opens, allowing you to specify the required timer event.

Tip: You may specify several timer events under a single event button. However, you cannot use a timer event under another timer event.

Editing Event Buttons and Timer Events

To edit an event button, or a timer event specified under an event button, select the required event button or timer event in the *Defined Events* list, then click the *Edit selected...* button.

If you have selected an event button, clicking the *Edit selected...* button will open the *Edit Event* window (for editing event buttons) (see page 109).

If you have selected a timer event, clicking the *Edit selected...* button will open the *New Timer* window (see page 101).

Associating Event Buttons with External Outputs

As is the case with input events (see *About Input, Events and Output* on page 91), you are able to associate an event button with specific external outputs. This way, external output, for example the sounding of a siren, can be triggered automatically when an event button is clicked.

Like with input, VMD and generic events, the association between event buttons and outputs is made in the *I/O Control* window (see page 121).

Add New Event Window (for Adding Event Buttons)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Add New Event* window (for adding event buttons) lets you specify the settings for an event button.

The *Add New Event* window (for specifying event buttons)

Access: You access the *Add New Event* window (for adding event buttons) from the *Event Buttons* window (see page 106): Select an entry (either global or for a specific camera) in the *Defined Events* list, then click the *Add new event...* button.

Add New Event Window's Fields

The *Add New Event* window (for adding event buttons) features the following fields:

Field	Description
Button related to	Read-only field, displaying the name of the camera for which the event will be specified. If the field displays *Global*, the event button will be a global event button (available for all cameras).
Manual event name	Lets you specify a name for the event button. **Note:** Event button names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the event button is clicked. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the event button is clicked, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the event button is clicked. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

Edit Event Window (for Editing Event Buttons)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Edit Event* window (for editing event buttons) lets you edit the settings for an existing event button.

The *Edit Event* window (for editing input events)

Access: You access the *Edit Event* window (for editing event buttons) from the *Event Buttons* window (see page 106), by first selecting the required event button in the *Defined Events* list, then clicking the *Edit selected...* button.

Edit Event Window's Fields

The *Edit Event* window (for editing event buttons) features the following fields:

Field	Description
Button related to	Read-only field, displaying the name of the camera for which the event button has been specified. If the field displays *Global*, the event button is a global event button (available for all cameras).
Manual event name	Lets you edit the name of the event button. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Send e-mail if this event occurs	Select check box to send an e-mail alert when the event button is clicked. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the *Send e-mail if this event occurs* check box is selected. Select check box to include an image, recorded at the time the event button is clicked, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the event button is clicked. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

Generic Events

About Generic Events

Milestone XProtect Enterprise is able to analyze received TCP and/or UDP data packages, and automatically trigger an event when specified criteria are met. This way you are able to easily integrate your Milestone XProtect Enterprise surveillance system with a very wide range of external sources, for example access control systems, alarm systems, etc.

Events based on the analysis of received TCP and/or UDP packets are called generic events. The *Generic Events* window lets you manage such events.

Generic Events Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Generic Events* window lets you manage events based on the analysis of received TCP and/or UDP packets.

The *Generic Events* window

Access: You access the *Generic Events* window by clicking the *Generic Events* button in the *Administrator* window (see page 30).

Generic Events Window's Events List and Buttons

The *Generic E*vents window features a *Defined events* list, in which defined TCP- and/or UDP-based events are listed, as well a number of buttons used when configuring the events:

Button	Description
Add new event…	Lets you define new events. The type of event you are able to define is determined by what you have selected in the *Defined events* list: • When nothing is selected, or you have selected the list's *Global* item, clicking the *Add New Event...* button will open the *Add New Event* window (for specifying generic events) (see page 111), in which you are able to specify the rules and alert settings for individual TCP- and/or UDP-based events. • When an existing event is selected in the list, clicking the *Add new event...* button will open the *New Timer* window (see page 101), in which you are able to specify timer events. Timer events are separate events, triggered by the 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.
Edit selected…	Opens the *Edit Event* window (for editing generic events) (see page 116), in which you are able to edit the settings for an existing event selected in the *Defined events* list.
Remove selected	Lets you remove an existing event selected in the *Defined events* list. **Note:** The selected event will be removed without further warning.

Add New Event Window (for Specifying Generic Events)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Add New Event* window (for specifying generic events) lets you specify the settings for an event based on input from external sources using the TCP and UDP protocols: You are able to specify the criteria according to which Milestone XProtect Enterprise should analyze received TCP and/or UDP data packages, and whether any notifications should be triggered by a detected event.

Tip: TCP and UDP packages used for generic events may contain special characters, such as @, #, +, å, ~, etc. within the text string to be analyzed.

The *Add New Event* window (for specifying generic events)

Access: You access the *Add New Event* window (for specifying generic events) from the *Generic Events* window (see page 110), by clicking the *Add new event...* button.

The *Add New Event* window (for specifying generic events) is divided into three sections:

General Event Settings Section

The *Add New Event* window (for specifying generic events) contains the following fields in the *General Event settings* section:

Field	Description
Event Name	Lets you specify a name for the event. Each event must have a unique name. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Event Protocol	Lets you select which protocol Milestone XProtect Enterprise 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	Lets you select how particular Milestone XProtect Enterprise should be when analyzing received packages: • *Match*: In order for the event to be triggered, the received

	package must contain *exactly* the message specified in the *Event rule string* section's *Event message include* field, and nothing else. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will not be triggered if the received package contains the terms "User001" and "Door053" and "Sunday" since this does not exactly match your requirements. • *Search*: In order for the event to be triggered, the received package must contain the message specified in the *Event rule string* section's *Event message include* 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" as your required terms are contained in the received package.
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 XProtect Enterprise 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. In case a package matches the criteria for several events with an identical priority, e.g. two events with a priority of *999*, all events with the priority in question will be triggered.

Event Rule String Section

The *Add New Event* window (for specifying generic events) contains the following fields and buttons in the *Event rule string* section:

Field, Button	Description
Event substring	Lets you specify the individual items for which Milestone XProtect Enterprise should look out when analyzing data packages. Specify one or more terms, then click the *Add* button to add the specified term(s) to the *Event message include* field, the content of which will be used for the actual analysis. Examples: • Single term: User001 (when added to the *Event message include* field, the term will appear as "User001")

	• Several terms as one item: User001 Door053 Sunday (when added to the *Event message include* field, the terms will appear as "User001 Door053 Sunday") When you add several terms as one item (appearing as e.g. "User001 Door053 Sunday" in the *Event message include* 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 (i.e. so they will appear as "User001" "Door053" "Sunday" in the *Event message include* field).
Event message include	Displays the string which will be used for the actual package analysis. The field is not directly editable. However, you are able to 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. Likewise, you are able to 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.
Add	Adds the content of the *Event substring* field to the *Event message include* field, the content of which will be used for the actual analysis. See also the description of the *Event substring* and *Event message includes* fields.
(	Lets you add a start parenthesis character to the *Event message include* 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: ("User001" OR "Door053") AND "Sunday" In the example, 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, the system 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 include* field.
AND	Lets you add an AND operator to the *Event message include* field. With an AND operator you specify that the terms on both sides of the AND operator must be present. Example: User001 AND Door053 AND Sunday

In the above example, 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:

Example: Few results match the criterion
User001 AND Door053 AND Sunday

OR	Lets you add an OR operator to the *Event message include* field.
	With an OR operator, you specify that either one or another term must be present.
	Example: User001 OR Door053 OR Sunday
	In the above example, 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:
	Example: Many results match the criterion *User001 OR Door053 OR Sunday*
Remove	Lets you remove the item immediately to the left of a cursor positioned in the *Event message include* field.
	If no cursor has been positioned in the *Event message include* field, the last item in the field will be removed.

Notification Settings section

The *Add New Event* window (for specifying generic events) contains the following fields in the *Notification settings* section:
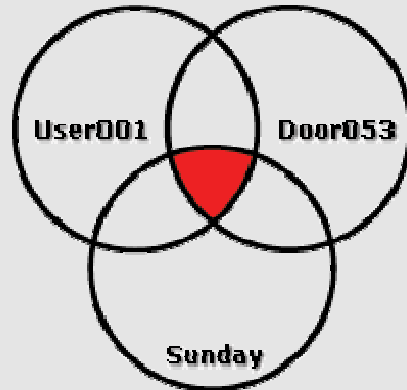
Button	Description
Send Email if this event occurs	Select check box to send an e-mail alert when the event occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the Send e-mail if this event occurs check box is selected. Select check box to include an image, recorded at the time the event is triggered, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

When you have specified a new generic event, click *OK*.

Edit Event Window (for Editing Generic Events)

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The *Edit Event* window (for editing generic events) lets you edit the settings for an event based on input from external sources using the TCP and UDP protocols: You are able to edit the criteria according to which Milestone XProtect Enterprise should analyze received TCP and/or UDP data packages, and whether any notifications should be triggered by a detected event.

i **Tip:** TCP and UDP packages used for generic events may contain special characters, such as @, #, +, å, ~, etc. within the text string to be analyzed.

The *Edit Event* window (for specifying generic events)

Access: You access the *Edit Event* window (for specifying generic events) from the *Generic Events* window (see page 110), by selecting an event from the list, then clicking the *Edit selected...* button.

The *Edit Event* window (for editing generic events) is divided into three sections:

General Event Settings section

The *Edit Event* window (for editing generic events) contains the following fields in the *General Event settings* section:

Field	Description
Event Name	Lest you edit the name of the event. Each event must have a unique name. **Note:** Event names must not contain the following characters: < > & ' " \ / : * ? | [ ]
Event Protocol	Lets you select which protocol Milestone XProtect Enterprise 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	Lets you select how particular Milestone XProtect Enterprise should be when analyzing received packages: • *Match*: In order for the event to be triggered, the received package must contain *exactly* the message specified in the *Event rule string* section's *Event message include* field, and nothing else. Example: If you have specified that the received package should contain the terms "User001" and "Door053", the event will not be triggered if the received package contains the terms "User001" and "Door053" and "Sunday" since this does not exactly match your requirements. • *Search*: In order for the event to be triggered, the received package must contain the message specified in the *Event rule string* section's *Event message include* 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" as your required terms are contained in the received package.
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 XProtect Enterprise 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.

In case a package matches the criteria for several events with an identical priority, e.g. two events with a priority of *999*, all events with the priority in question will be triggered.

Event Rule String Section

The *Edit Event* window (for editing generic events) contains the following fields and buttons in the *Event rule string* section:

Field, Button	Description
Event substring	Lets you specify the individual items for which Milestone XProtect Enterprise should look out when analyzing data packages.
	Specify one or more terms, then click the *Add* button to add the specified term(s) to the *Event message include* field, the content of which will be used for the actual analysis.
	Examples:
	• Single term: User001 (when added to the *Event message include* field, the term will appear as "User001")
	• Several terms as one item: User001 Door053 Sunday (when added to the *Event message include* field, the terms will appear as "User001 Door053 Sunday")
	When you add several terms as one item (appearing as e.g. "User001 Door053 Sunday" in the *Event message include* 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 (i.e. so they will appear as "User001" "Door053" "Sunday" in the *Event message include* field).
Event message include	Displays the string which will be used for the actual package analysis.
	The field is not directly editable.
	However, you are able to 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*.
	Likewise, you are able to 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.

Add	Adds the content of the *Event substring* field to the *Event message include* field, the content of which will be used for the actual analysis.
	See also the description of the *Event substring* and *Event message includes* fields.
(	Lets you add a start parenthesis character to the *Event message include* 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: ("User001" OR "Door053") AND "Sunday"
	In the example, 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, the system 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 include* field.
AND	Lets you add an AND operator to the *Event message include* field.
	With an AND operator you specify that the terms on both sides of the AND operator must be present.
	Example: User001 AND Door053 AND Sunday
	In the above example, 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:
	Example: Few results match the criterion *User001 AND Door053 AND Sunday*
OR	Lets you add an OR operator to the *Event message include* field.
	With an OR operator, you specify that either one or another term must be

present.

Example: User001 OR Door053 OR Sunday

In the above example, 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:

Example: Many results match the criterion
User001 OR Door053 OR Sunday

Remove	Lets you remove the item immediately to the left of a cursor positioned in the *Event message include* field. If no cursor has been positioned in the *Event message include* field, the last item in the field will be removed.

Notification Settings section

The *Edit Event* window (for specifying generic events) contains the following fields in the *Notification settings* section:

Button	Description
Send Email if this event occurs	Select check box to send an e-mail alert when the event occurs. **Note:** In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Include image from camera	Available only if the Send e-mail if this event occurs check box is selected. Select check box to include an image, recorded at the time the event is triggered, in the e-mail alert, then select the required camera in the list below the check box.
Send SMS if this event occurs	Select check box to send an SMS alert when the input occurs. **Note:** In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).

When you have edited the generic event, click *OK*.

I/O Control

About I/O Control

Milestone XProtect Enterprise's I/O Control features let you associate events and manual actions with output.

This way, you are able to specify that output should be triggered when particular events or manual actions occur.

I/O Control Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights. Use of features in the *I/O Control* window requires that events and output have been defined (see *About Input, Events and Output* on page 91).

In the *I/O Control* window you are able associate particular events and event buttons with one or more particular outputs. This way you are able to define that when a selected event occurs, or when a particular event button is clicked, one or more selected outputs will be triggered.
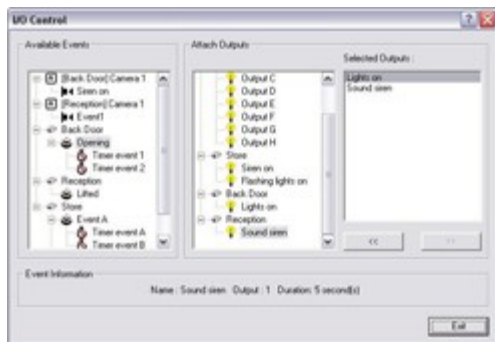
The *I/O Control* window

Access: You access the *I/O Control* window from the *Administrator* window (see page 30), by clicking the *I/O Control...* button.

Associating Events with Particular Outputs

When associating an event with one or more outputs, you are able to select between **all** outputs defined on the Milestone XProtect Enterprise system; you are not limited to selecting outputs defined on a particular device.

To associate a particular event with a particular output, do the following:

1. Select the required event in the *Available Events* list in the left side of the *I/O Control* window.

   Tip: Events as well as event buttons may be listed.

   Tip: When you select an event or event button in the *Available Events* list, you can view detailed information about the selected event or event button under *Event Information* in the lower part of the window.

2. Select the required output in the list of available outputs (the list in the middle of the window).

3. Click the >> button located below the *Selected Outputs* list.

   This will copy the selected output to the *Selected Outputs* list. When the selected event occurs, or when the selected event button is clicked, the selected output will be triggered.

You are able to associate an event or an event button with more than one output: Simply repeat the process for each required output.

To remove an output from the *Selected Outputs* list, simply select the required output, and click the << button located below the *Selected Outputs* list.

Output Settings for [Device Name] [Camera Name] Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

In the *Output Settings for [Device Name] [Camera Name]* window you are able to associate a camera with particular external outputs, defined in the *I/O Setup* window (see page 93), for example the sounding of a siren or the switching on of lights.

The associated outputs can be triggered automatically when motion is detected as well as manually through output buttons available when the camera is selected in the *Monitor* application (see page 133), *Remote Client* (see page 171) and *Smart Client* (see page 210).

The *Output Settings for [Device Name] [Camera Name]* window

⮕ **Access:** You access the *Output Settings for [Device Name] [Camera Name]* window from the *Camera Settings for [Device Name] [Camera Name]* window (see page 44), by clicking the *Outputs...* button.

Associating Outputs with Manual Control and Detected Motion

Note: Use of features in the *Output Settings for [Device Name] [Camera Name]* window requires that output has been defined in the *I/O Setup* window (see page 93).

You have a high degree of flexibility when associating a camera with particular outputs:

- You are able to select between all available outputs, i.e. outputs defined as output events for the camera itself **as well as** outputs defined as output events for other devices on the Milestone XProtect Enterprise system

- The same output may be used for manual control through an output button **as well as** for automatic triggering when motion is detected

Selecting Output for Manual Control

You are able to specify outputs to be triggered manually through output buttons in the *Monitor* application or from a list in the *Remote Client* or *Smart Client*.

Output buttons will become available in the Monitor when the camera is selected and the Monitor's Output button is clicked. In the *Remote Client* and *Smart Client*, users will be able to trigger outputs by selecting them from a list.

Example of output buttons available in the *Monitor* application. Note that the *Monitor's Output* button has been clicked in order to view the output buttons.

To specify an output for manual triggering in the *Monitor* or *Remote Client/Smart Client*, do the following:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

   i **Tip:** When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Manual Control* list.

   This will copy the selected output to the *On Manual Control* list.

Note: An unlimited number of outputs may be selected this way, but only the top eight outputs in the list will be available as output buttons in the *Monitor*. In the *Remote Client* and *Smart Client* there are no limitations to the number of available outputs.

You are able to move a selected output up or down in the *On Manual Control* list with the *up* and *down* buttons located to the right of the list. The selected output is moved up one step each time you click the *up* button. Likewise, each time you click the *down* button, the selected output is moved down one step.
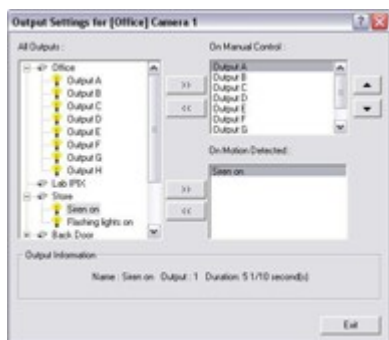
To remove an output from the *On Manual Control* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Manual Control* list.

Selecting Output for Use on Motion Detection

You are able to select outputs to be triggered automatically when motion is detected in images from the camera.

Tip: This feature does *not* require that a VMD (Video Motion Detection) event has been defined for the camera in the *I/O Setup* window (see page 93).

To select an output for use when motion is detected in images from the camera:

1. Select the required output in the *All Outputs* list in the left side of the *Output Settings for [Device Name] [Camera Name]* window.

    Tip: When you select an output in the *All Outputs* list, you can view detailed information about the selected output under *Output Information* in the lower part of the window.

2. Click the >> button located between the *All Outputs* list and the *On Motion Detected* list.

    This will copy the selected output to the *On Motion Detected* list.

To remove an output from the *On Motion Detected* list, simply select the required output, and click the << button located between the *All Outputs* list and the *On Motion Detected* list.

Archiving

About Archiving

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

With the archiving feature in Milestone XProtect Enterprise, you are able to keep recordings for as long as required, limited only by the available hardware storage capacity.

You enable and configure archiving in the *Archive setup* window (see page 127). The *Archive setup* window also lets you specify where archives should be stored for each camera.

Benefits of Archiving

By default, information received from cameras is stored by Milestone XProtect Enterprise in a database for each camera.

The database for each camera (configured in the *Camera Settings for [Device Name] [Camera Name]* window; see page 44) is capable of containing a maximum of 600.000 records or 40 GB before the oldest records in the database are overwritten.

With daily archiving, the amount of records you are able to store is limited only by the available hardware storage capacity.

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

How Archiving Works

For each camera, for which archiving has been specified, the contents of the camera database will be moved to a default archiving directory called *Archives*. This will happen automatically one or more times every day, depending on your archiving settings.

The default archiving directory is located on the computer running the Milestone XProtect Enterprise software, by default in the directory containing the Milestone XProtect Enterprise software (typically c:\program files\milestone\milestone surveillance\ archives\).

In the archiving directory, separate sub-directories for storing archives for each camera are automatically created. These sub-directories are named after the MAC address of the device to which the camera is connected.

Since you are able to keep archives spanning many days of recordings, and since archiving may take place several times a day, further sub-directories, named after the archiving date and time, are also automatically created.

The sub-directories will be named according to the following structure:

        ...\Archives\CameraMACAddress_VideoServerChannel\DateAndTime

An example:

With the default archiving folder located under C:\MyFiles\MySurveillanceSystem, images from an archiving taking place at 23.15 on 1st June 2005 for a camera attached to channel 2 on a video server device with the MAC address 00408c51e181 would be stored at the following destination:

    C:\MyFiles\MySurveillanceSystem\Archives\00408c51e181_2\2005-06-01-23-15

If the device to which the camera is attached is not a video server device with several channels, the video server channel indication in the sub-directory named after the device's MAC address will always be _*1*. Example: (e.g. 00408c51e181_1)

Storing Archives at Other Locations than Default Archiving Directory

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

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

While this may at first glance seem unnecessary, it greatly speeds up the archiving procedure, which is important because all cameras are stopped during archiving:

Archiving directly to a network drive would mean that archiving time would vary depending on the available bandwidth on the network. First storing the archive locally, then moving it, ensures that the archiving is always performed as fast as possible.

If archiving to a network drive, note the regular camera database **must** still be stored on a local drive, i.e. a drive attached directly to the computer running the Milestone XProtect Enterprise system.

Storage Capacity Required for Archiving

The storage capacity required for archiving depends entirely on the amount of images you plan to archive.

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 images from one or two cameras, and they may want keep their archives for much shorter periods of time.

However, before enabling archiving, you should always consider the storage capacity of the **local** drive containing the default archiving directory to which archives are always moved, even though they may immediately after be moved to an archiving location on a network drive:

As a rule of thumb, the capacity of the local drive should be at least twice the size required for storing the databases of all cameras for which archiving has been specified.

Backing Up Archives

Many organizations want to back up recorded images from cameras, using tape drives or similar.

Creating such backups based on the content of the default camera databases is not recommended; it may cause sharing violations or other malfunctions.

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

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

Viewing Archived Images

You view archived images with the *Monitor* application's *Viewer* (see page 142). This allows you to use all of *Viewer*'s advanced features (image browsing, smart search, evidence generation, etc.) for archived images.

Archives Stored Locally or on Network Drives

For archived images stored locally or on network drives you simply use the *Viewer*'s image browsing features, for example the timeline or the playback controls, for finding and viewing the required images; just like you would with images stored in a camera's regular database.

Exported Archives

For exported archives, e.g. archives stored on a CD, you click the *browse* button in the *Viewer*'s *Database Information* control panel to browse for the archive you want to view.

Once you have specified the required archive this way, you can use all of the *Viewer*'s image browsing features for navigating the images in the archive.

Viewing archived images in the *Viewer*.
Arrow indicates the browse button in the
Viewer's *Database Information* control panel.

Archive Setup Window

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

The Archive setup window lets you enable and configure the archiving feature in Milestone XProtect Enterprise. It also lets you specify where archives should be stored for each camera.
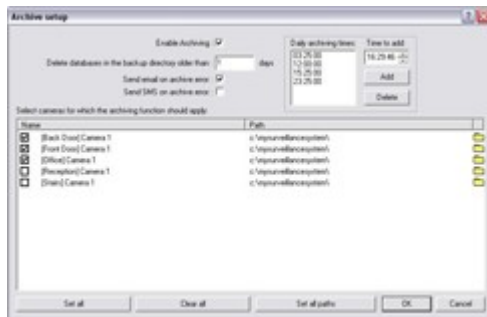
The *Archive setup* window

Access: To access the *Archive setup* window, click the *Archive Setup...* button in the *Administrator* window (see page 30).

Archive Setup Window's Fields and Buttons

The *Archive setup* window contains the following fields and buttons:

Field, Button	Description
Enable Archiving	Select check box to enable the daily archiving feature. **Note:** Remember to specify for which cameras the archiving feature should be used; you do this in the *Archive setup* window's *Select cameras for which the archiving function should apply* section.
Delete databases in the backup directory older than	Lets you specify how many days you want to keep archived images for. Archived images older than the specified number of days will automatically be deleted.

Send email on archive error	Select check box if Milestone XProtect Enterprise should send an e-mail alert if archiving fails, for example because the disk is full.
	Note: In order to be able to use e-mail alerts, the e-mail alert feature must have been set up in the *E-Mail setup* window (see page 87).
Send SMS on archive error	Select check box if Milestone XProtect Enterprise should send an SMS alert if archiving fails, for example because the disk is full.
	Note: In order to be able to use SMS alerts, the SMS alert feature must have been set up in the *SMS settings* window (see page 90).
Daily archiving times	Lists specified archiving times. Archiving will take place every day at the specified times.
	Archiving once a day will normally suffice. However, if you expect the daily database per camera to exceed 40 GB or 600,000 images (roughly corresponding to storing seven images per second 24 hours a day), you should specify additional archiving times.
	To add an archiving time to the list, specify the required time in the *Time to add* field, then click the *Add* button. There must be at least one hour between each archiving time.
	To remove an archiving time from the list, select the archiving time to remove from the list, and click the *Delete* button.
	Note: While archiving takes place, cameras for which archiving applies will briefly stop recording, one after the other. Although the pause is very brief (typically less than a second), it is therefore recommended that you specify archiving times that are outside periods in which you expect to record important images.
Time to add	Lets you add an archiving time to the *Daily archiving times* list.
	You specify the required time by selecting the hour, minute and second values respectively, then clicking the field's *up* and *down* buttons to increase or decrease values.
	🛈 **Tip:** You may also simply overwrite selected hour, minute or second values.
Add	Adds the archiving time specified in the *Time to add* field to the *Daily archiving times* list.
Delete	Removes a selected archiving time from the *Daily archiving times* list.
Select cameras for which the archiving function should apply	If the Archive Setup window's Enable Archiving check box is selected, this section lists cameras for which archiving is possible.
	The section lists all enabled cameras, i.e. cameras which, depending on their individual settings, may transfer images to the surveillance system.
	The section also lists the path to the archiving directory for each camera.
	🛈 **Tip:** If a particular camera is not listed, it is highly likely that the camera is disabled. To check if a camera is disabled, look for the camera in the *Administrator* window's *Device Manager* section (see page 32). A disabled camera

will be clearly indicated by an icon , and can be enabled by right-clicking the camera name.

Specifying that Archiving Should Apply for Specific Cameras

To specify that archiving should apply for a specific camera, select the check box next to the name of the required camera.

Specifying that archiving should
apply for a specific camera

Remember that only when you click *OK* is archiving actually enabled for the selected cameras.

Specifying Archiving Locations for Specific Cameras

A default archiving location (typically c:\program files\milestone\ milestone surveillance\) is specified for each camera. The default archiving directory, called *Archives*, will be located at this location.

To specify another location for the archiving directory for a camera, either click the *browse* icon next to the path listing for the required camera and browse to the required location, or click the default path listing to overwrite it.

Overwriting an existing path
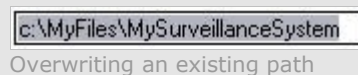
 Tip: To maximize load sharing and optimize performance, distribute archives across your available storage space, if possible.

Note: If specifying another archiving location than the default location (typically c:\program files\milestone\milestone surveillance\), the location you specify must exist. You are not able to create new directories as part of the process.

If archiving to a network drive, the regular camera database **must** still be stored on a local drive, i.e. a drive attached directly to the computer running the Milestone XProtect Enterprise system.

Archives for the selected camera will be stored in separate subdirectories under the *Archives* directory at the location you specify.

The subdirectories will be named according to the following structure:

```
...\Archives\CameraMACAddress_VideoServerChannel\DateAndTime
```

Example:

With the default archiving folder located under C:\MyFiles\MySurveillanceSystem, images from an archiving taking place at 23.15 on 1st June 2005 for a camera attached to channel 2 on a video server device with the MAC address 00408c51e181 would be stored at the following destination:

```
C:\MyFiles\MySurveillanceSystem\Archives\00408c51e181_2\2005-06-01-
23-15
```

If the device to which the camera is attached is not a video server device with

	several channels, the video server channel indication in the subdirectory named after the device's MAC address will always be _1. Example: (e.g. 00408c51e181_1)
	### *Archiving Audio*
	If audio is enabled on a device, audio from the device will also be archived.
	If the device is a video server with several channels, audio will be archived with the camera on channel 1.
Set all	Selects the check boxes for all cameras listed in the *Select cameras for which the archiving function should apply* section.
	Clicking the *Set all* button is thus a quick way to specify that archiving should apply for all cameras listed.
	Remember that only when you click *OK* is archiving actually enabled for the selected cameras.
Clear all	Clears the check boxes for all cameras listed in the *Select cameras for which the archiving function should apply* section.
	Clicking the *Clear all* button is thus a quick way to specify that archiving should not apply for any of the cameras listed.
	Remember that only when you click *OK* is archiving actually disabled for the selected cameras.
Set all paths	Copies the selected path listing to all cameras listed in the *Select cameras for which the archiving function should apply* section.
	If using the same archiving directory for all cameras, this can save you having to manually specify identical paths for each camera.
	Example:
	You have specified the path C:\MyFiles\MySurveillanceSystem for a camera. To quickly use this path for all cameras, select the path listing and click the *Set all paths* button.

Tip: Milestone's *Storage Calculator*, found in the support section of the Milestone website, www.milestonesys.com, can help you easily determine the storage capacity required for your surveillance system.

Cameras Not Included in Monitor Application

Using "Background" Cameras

It is possible to let some or all of the cameras connected to a Milestone XProtect Enterprise server run "in the background," i.e. without the cameras being included in the *Monitor* application (see page 71 and 133).

For such "background" cameras, the features of the *Monitor* application will not be immediately available (although recorded images from such cameras can still be browsed in the *Monitor* application's *Viewer*).

However, "background" cameras can be accessed for viewing of live and recorded images through a *Remote Client* (see page 171) or *Smart Client* (see page 210).

Apart from the fact that "background" cameras cannot be immediately accessed through the *Monitor*, other settings, such as scheduling (see page 74), input/events/output (see page 91), archiving (see page 124), the ability for cameras to be started on remote live requests (see description of the *General Settings* window's *Advanced* section on page 82), etc., fully apply for "background" cameras.

Tip: If you require *Monitor* access to a camera which has been running "in the background," you can simply include the camera in the *Monitor*, provided not all of the *Monitor*'s 64 positions are already in use. You do this in the *Monitor Manager* window, see page 71.

The use of "background" cameras may be relevant in a number of scenarios, entirely depending on your needs.

Possible Scenario: Using More than 64 Cameras on a Single Server

For large installations, one scenario could be if wishing to use more than 64 cameras *on the same server*.

Normally, if a surveillance solution requires more than 64 cameras, several servers are used, and a master/slave setup (configured in the *ImageServer Administrator* window, see page 162) is used to let *Remote Client* and *Smart Client* users access cameras effortlessly across the servers.

However, a single Milestone XProtect Enterprise server may have an unlimited number of cameras *connected to it* even though a maximum of 64 of the connected cameras can be running simultaneously.

Using "background" cameras allows you to take advantage of this fact, since none of the "background" cameras will be tied to a particular position in the *Monitor* application: Up to 64 out of a potentially unlimited number of "background" cameras can be accessed on a first-come/first-served basis. Some organizations using a large number of "background" cameras simply do not include any cameras in the *Monitor* application.

Important Guidelines for Using "Background" Cameras

Maximum 64 Cameras Running on a Single Server

Since "background" cameras are not displayed in the *Monitor* application, it may occasionally be difficult to determine how many cameras are running.

Therefore, when using "background" cameras, always bear in mind that a maximum of 64 cameras at a time can be running on a single server—regardless of whether they are running in the *Monitor* application or running through remote activation of "background" cameras. If more than 64 cameras *must* be able to run at any one time, you should use a multi-server master-slave setup.

If the maximum of 64 cameras on a single server are running, *Remote Client* and *Smart Client* users will receive an error message if requesting access to cameras beyond the maximum limit.

Example: 64 cameras are already running on a single server when a *Remote Client* user requests that a 65th camera on the server is started. Since it is only possible to run 64 cameras on a single server, the *Remote Client* user will receive an error message.

Use of "Background" Cameras Must be Enabled

For "background" cameras to work, the *Allow cameras to run in the background* check box in the *General Settings* window's *Advanced* section (see page 82) must be selected.

Cameras Must be Enabled

For "background" cameras to work, they must be *enabled* (see description of the *Administrator* window's *Device Manager* section on page 32).

Monitor Must be Running

Even if no cameras are included in the *Monitor* application, remember that camera images are only transferred to Milestone XProtect Enterprise while the *Monitor* application is running.

The *Monitor* application *must* therefore run whenever you want to record images from cameras on your surveillance system.

A running *Monitor* is also a prerequisite for viewing live images in the *Remote Client* and *Smart Client*.

Monitor Application

Milestone XProtect Enterprise's main user interface in day-to-day operation, the *Monitor* application is used for recording and displaying images from connected cameras, with optional indications of registered activity. Depending on user rights and configuration, the *Monitor* may also be used for controlling PTZ (Pan/Tilt/Zoom) cameras, for manually starting and stopping cameras, for manually triggering outputs, etc.

From the *Monitor*, you also have access to the *Viewer* (see page 142), with which you are able to browse and play back recordings, print images, send images via e-mail, and export entire video and audio sequences in a variety of formats.

The exact look and functionality of the *Monitor* depends on how the *Monitor* has been configured in the *Administrator* application (see page 30). Ask your system administrator if in doubt.

Monitor application. In this example, a 3×3 view with a hot spot is used in the *Monitor*'s camera layout.

IMPORTANT: Camera images are only transferred to Milestone XProtect Enterprise while the *Monitor* application is running. The *Monitor* application **must** therefore run whenever you want to record images from cameras on your surveillance system. A running *Monitor* is also a prerequisite for viewing live images in the *Remote Client* (see page 171) and *Smart Client* (see page 210). The *Monitor* application cannot run if the *Administrator* application is already running; close down the *Administrator* application before running the *Monitor* application. Once the *Monitor* application is running, you can run the *Administrator* application as required.

Accessing the Monitor

Access: You access the *Monitor* application by clicking the *Monitor* shortcut on the desktop.

The *Monitor* desktop shortcut

Alternatively, you may access the *Monitor* from Window's *Start* menu, by selecting *All Programs > Milestone XProtect Enterprise > Monitor*.

Depending on your organizations security settings, you may be required to specify a password in order to use the *Monitor*.

When you start the *Monitor*, all cameras scheduled to be online will start transferring images to Milestone XProtect Enterprise.

Scheduling is handled by the system administrator in the *Administrator* application (see page 30).

Even if a camera is not scheduled to be online, users with sufficient user rights can start a camera (i.e. make it transfer images to Milestone XProtect Enterprise) from the *Monitor* by using the *Monitor*'s *Manual Mode* feature. See further information in the description of the *Monitor*'s control panel on page 136.

The *Monitor* application opens in full-screen view. This provides you with the best possible view of the camera images displayed.

The *Monitor* basically consists of two sections: a camera layout section, in which camera images are displayed, and a control panel with buttons for controlling the various features of the *Monitor*.

Monitor's Camera Layout

The *Monitor*'s camera layout section displays images from each camera specified by the system administrator.

Depending on the system administrator's settings in the *Administrator* application, the camera layout may contain images from up to 64 different cameras.

Note: A Milestone XProtect Enterprise server is capable of handling images from up to 64 cameras at a time; the *Monitor* can thus display images from a maximum of 64 cameras. However, a single Milestone XProtect Enterprise server may have an unlimited number of cameras *connected to it* even though a maximum of 64 of the connected cameras can be used for recording/live viewing simultaneously. This depends on how the *Monitor* has been configured in the *Administrator* application (see page 30). Ask your surveillance system administrator if in doubt.

Image Bars

Each camera, from which images are displayed in the camera layout, is identified by an image bar, located in the top of each camera image.

The image bar is blue. When you select a particular camera in the camera layout, the image bar of the selected camera image becomes a lighter blue.
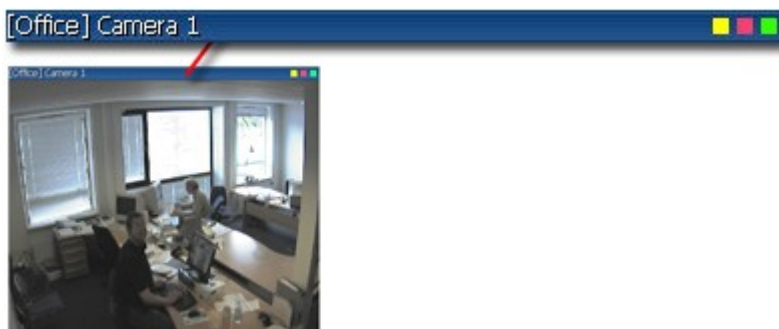
Camera image; enlarged detail shows image bar

The image bar displays the name of the camera as well as the name of the device to which the camera is connected. The device name is displayed first, in square brackets, followed by the camera name.

Each image bar also features three colored indicators:

- *Event indicator (the leftmost of the three indicators, solid yellow)*: Lights up when events specified in the *Administrator* application occur. Click anywhere inside the image to reset the event indicator. This indicator may appear black if event indication has not been specified for the camera in question, of if no specified events have occurred. Consult your system administrator if in doubt.

- *Motion indicator (the indicator in the middle, solid red)*: Lights up when motion is detected in the image. Click anywhere inside the image to reset the motion indicator.

- *Online indicator (the rightmost of the three indicators, blinking green)*: Changes state every time an image is received from the camera.

Hot Spot

If enabled in the *Administrator* application, a hot spot provides you with an enlarged view of images from a selected camera.

When enabled, the hot spot can either appear inside the camera layout, or as a separate floating window:

- If the hot spot is located inside the camera layout, simply click inside an image to select the camera from which you want to view images in the hot spot.
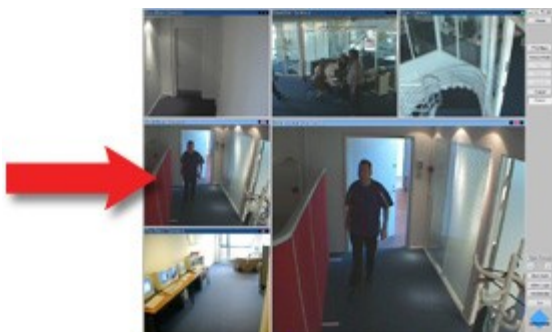
Example of hot spot located inside the camera layout; arrow indicates camera image featured in the hot spot

- If the hot spot runs in a separate floating window, you will see a *HotSpot* button in the *Monitor*'s control panel: When this is the case, simply click the *HotSpot* button to open the separate hot spot window. A hot spot in a separate floating window otherwise works just like a hot spot located inside the camera layout.

Tip: The hot spot may also be used for point-and-click operations on some PTZ (Pan/Tilt/Zoom) cameras. See the description of the *PTZ menu* on page 139 for more information.

Hot Spot with Carousel

Depending on hot spot configuration in the *Administrator* application, the hot spot may automatically display images from all cameras available in the camera layout; one after the other, with specified intervals. This is known as a carousel.

When this feature has been enabled, a *Carousel* button appears in the *Monitor*'s control panel. To toggle the carousel feature on and off, simply click the *Carousel* button.

Monitor's Control Panel

The *Monitor*'s control panel section contains a number of buttons for controlling the *Monitor*'s features:

Button	Description
Viewer	Opens the *Viewer* (see page 142), with which you are able to browse and play back recordings, print images, send images via e-mail, and export entire video and audio sequences in a variety of formats. **Note:** Use of the *Viewer* may require certain user rights. See the description of the *Admin Login* button.
HotSpot	Available only when use of a hot spot in a separate floating window has been set up by the system administrator. Opens the separate hot spot window.
Carousel	Available only when use of the hot spot's carousel feature has been enabled by the system administrator. Click to toggle the carousel feature on and off.
PTZ Menu	Opens the *PTZ menu*, with which you are able to control PTZ (Pan/Tilt/Zoom) cameras. The *PTZ menu* is only functional when the camera selected in the camera layout is a PTZ camera. See the detailed description of the *PTZ menu* on page 139 for more information. *ⓘ* **Tip:** To hide the *PTZ menu*, simply click the *PTZ Menu* button again.
Manual Mode	Lets you toggle between scheduled mode (cameras transferring images to Milestone XProtect Enterprise according to a schedule defined in the *Administrator* application) and manual mode. With manual mode, you can start a camera (i.e. make it transfer images to Milestone XProtect Enterprise) from the *Monitor*, even if the camera is not scheduled to be online. When manual mode is selected (*Manual Mode* button depressed), three buttons (the *Stop*/*Start* button, the *Start All* button, and the *Stop All* button) become available, enabling you to start and stop cameras manually. **Note:** When in manual mode, all scheduled camera activity for all cameras, including automatic reconnection and any scheduled PTZ patrolling, is disabled. Use of manual mode may require certain user rights. See the description of the *Admin Login* button.
Stop or **Start**	Available only when the *Manual Mode* button is depressed. Stops the camera selected in the camera layout. When stopped, no images are transferred from the camera to Milestone XProtect Enterprise. *ⓘ* **Tip:** In the camera layout, the selected camera is indicated by a light

	blue image bar.
	When the selected camera is stopped, the button becomes a *Start* button. Click the *Start* button to make the camera transfer images to Milestone XProtect Enterprise again.
Start All	Available only when the *Manual Mode* button is depressed.
	Starts all cameras, i.e. makes all cameras transfer images to Milestone XProtect Enterprise.
Stop All	Available only when the *Manual Mode* button is depressed.
	Stops all cameras. When all cameras are stopped, no images are transferred to Milestone XProtect Enterprise from any of the cameras.
Output	Displays all available output buttons for the selected camera.
	Output buttons are used for manually triggering external output, for example for switching on lights, sirens, or similar.
	When *Output* is selected (*Output* button depressed), any output buttons for the selected camera will be displayed below the *Events* button: Example of output buttons Simply click an output button to trigger the associated output. Up to eight output buttons can be displayed for each camera. Output buttons are defined in the *Administrator* application. Ask your surveillance system administrator if in doubt about using output buttons defined for use with cameras in your organization.
Events	Displays all available event buttons for the selected camera.
	Depending on configuration, event buttons can be used for a wide variety of purposes, including triggering combinations of actions. For example, the clicking of an event button could make a camera use a higher frame rate, trigger two different outputs, and send an e-mail alert to three different recipients.
	Event buttons can be global or tied to a particular camera: • Global: available for all cameras in the *Monitor* • Tied to a particular camera: only available when the camera is selected in the *Monitor*

When *Events* is selected (*Events* button depressed), any global event buttons as well as any event buttons for the selected camera will be displayed below the *Events* button:

Events
Event 1
Event 2
Event 3
Event 4
Event 5
Event 6
Event 7
Event 8

Example of event buttons

Simply click an event button to trigger the associated event.

Up to eight event buttons can be displayed for each camera. Event buttons are defined in the *Administrator* application.

Ask your surveillance system administrator if in doubt about using event buttons defined for use with cameras in your organization.

Quick Browse	Available only when a hot spot is enabled. Lets you browse images from the selected camera in the hot spot. Use the *back* and *forward* buttons below the *Quick Browse* button to move backwards and forwards. **Tip:** The *Viewer* (see page 142) offers more advanced browsing features. **Note:** Use of the Quick Browse feature may require certain user rights. See the description of the *Admin Login* button.
Mute Audio	Lets you mute audio from cameras on which audio is enabled. Recording is not affected by muting audio in the *Monitor*.
Admin Login	For users without administrator rights, access to certain features in Milestone XProtect Enterprise may in some organizations have been restricted. Provided you know the administrator password, the *Admin Login* button lets you access such protected features. Clicking the *Admin Login* button opens the *Administrator Login* window (see page 30), in which you are able to specify the administrator password and log in to Milestone XProtect Enterprise as an administrator. When you are logged in as an administrator, the *Admin Login* button changes to *Admin Logout*. Clicking the *Admin Logout* button will restore any restrictions.
Administrator	Lets you access the *Administrator* application (see page 30). The *Administrator* application is used for configuring Milestone XProtect

	Enterprise upon installation or whenever configuration adjustments are required, e.g. when adding new cameras to the system. **Note:** Accessing the *Administrator* application from the *Monitor* may require certain user rights. See the description of the *Admin Login* button. When you close the *Administrator* application and return to the *Monitor* application, the *Monitor* application will be restarted. Certain settings, notably settings for PTZ (Pan/Tilt/Zoom) cameras, are not configurable when the *Administrator* application is accessed from the *Monitor* application. To configure such settings, you must close the *Monitor* application and open the *Administrator* application separately.
Exit	Exits the *Monitor;* closing down the application, and thereby stopping the transfer of images from cameras to Milestone XProtect Enterprise. You will be asked to confirm that you want to close down the application. **IMPORTANT:** Use with caution. Exiting the *Monitor* will stop recordings. Certain user rights may be required in order to be able to close down the *Monitor*.

PTZ Menu

Note: Use of the *Monitor*'s *PTZ Menu* may require certain user rights.

Clicking the *PTZ Menu* button in the *Monitor*'s control panel gives you access to a menu for controlling a PTZ (Pan/Tilt/Zoom) camera selected in the *Monitor*'s camera layout.

Example of *PTZ Menu* with preset position buttons

Navigation Buttons

The *PTZ Menu*'s navigation buttons let you move the PTZ camera in steps:

	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

H   Moves the PTZ camera to its home 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

Zoom Buttons and Zoom Slider

With the *PTZ Menu*'s zoom buttons you are able to control the zoom level of the PTZ camera:

🔍   Zoom out (one zoom level per click)

🔍   Zoom in (one zoom level per click)

As an alternative to using the zoom buttons, use the slider, located below the two zoom buttons, to control the zoom level.

Note that the slider can be used only with absolute positioning PTZ cameras only.

Preset Positions

If preset positions have been defined in the *Administrator* application (see page 30), you are able to move the PTZ camera to the stored preset positions by clicking the preset position buttons displayed in the lower part of the PTZ menu.

Preset position buttons are grouped into five preset banks (A-E) with up to five preset position buttons (1-5) in each.

To use preset positions, first click a preset bank button (A-E) to display the preset position buttons in the required bank, then click the required preset position button (1-5) to move the PTZ camera to the required preset position.

ℹ️ **Tip:** You may use the A-E and 1-5 keys on your keyboard to move the PTZ camera to preset positions.

Point-and-Click PTZ Control

Point-and-click control is supported for absolute positioning PTZ cameras as well as some relative positioning PTZ cameras, when a hot spot and the *PTZ Menu* are enabled.

If the mouse pointer changes to crosshairs when positioned in the hot spot, you are able to control the PTZ camera by clicking in the hot spot.

Crosshairs

The PTZ camera will center on the point you click.

If you click and hold down the left mouse button, then move the mouse up or down, you will get access to a zoom slider.

For some cameras, crosshairs surrounded by a square may be displayed. When this is the case, you are able to zoom in on an area by dragging a square around the required area in the hot spot. For such cameras, zoom level is controlled by holding down the SHIFT key on your keyboard while moving the mouse up or down; this will display a zoom level slider inside the hot spot.

PTZ Patrolling and PTZ On Event

PTZ cameras may be set up to move automatically, either according to a scheme (PTZ patrolling) or when particular events occur (PTZ On Event). This is configured in the *Administrator* application (see page 30).

- With PTZ patrolling, the PTZ camera will automatically move between preset positions.
- With PTZ On Event, the PTZ camera will automatically move to a particular preset position when a particular event occurs. For example, the PTZ camera may move to a preset position covering a door area when a door is opened.

Note: PTZ patrolling and PTZ On Event is stopped for all cameras as long as *Manual Mode* is used to allow cameras to be controlled manually.

Pausing PTZ Patrolling

If PTZ patrolling is enabled for the selected PTZ camera, you can pause PTZ patrolling for the camera by clicking the *PTZ Menu*'s *Pause Patrol* button. The button is only available for PTZ cameras for which PTZ patrolling has been enabled.

Note that pausing applies for the selected camera; other PTZ cameras may still patrol. Depending on configuration, the pause may automatically time out after a while.

Monitoring Audio

If the camera selected in the *Monitor*'s camera layout is recording audio, you are able to listen to live audio through speakers attached to the computer running Milestone XProtect Enterprise.

If using a multi-port video server device, audio will always be attached to the first video input on the device.

To mute live audio, click the *Mute Audio* button in the *Monitor*'s control panel. Recording is not affected by muting audio in the *Monitor*.

Running Out of Disk Space! Alert

In order to warn you of an impending possibility of losing data, the *Monitor* will prominently display the message *Running out of disk space!* if available disk space on the Milestone XProtect Enterprise server goes below 150 MB plus 20 MB per camera.

Example: For a system with ten cameras, the alert will show if the available disk space goes below 350 MB (150 MB plus 20 MB for each of the ten cameras).

Viewer

Using the Viewer

The *Viewer* lets you browse and play back recordings from cameras available in the *Monitor* application (see page 133).

The *Viewer* also lets you print images, send images via e-mail, and export entire video and audio sequences in a variety of formats.

The *Viewer*: In this example, the *Viewer* displays images from a single camera.
The *Viewer* can display images from up to 16 cameras in a single view. Note
that content of the *Viewer*'s toolbar may vary depending on configuration.

Access: You access the *Viewer* from the *Monitor* application, by clicking the *Viewer* button.

Toolbar

The *Viewer*'s toolbar lets you quickly switch between the *Viewer*'s different features. Icons in the toolbar serve as shortcuts to the features available from the *File* and *Tools* menus in the *Viewer*'s menu bar.

When you select a feature in the toolbar, settings for the feature typically become available in the *Viewer*'s control panel, located in the lower part of the window, below the camera layout.

Note: Depending on your rights, not all of the following toolbar icons may be available to you.

Settings: Opens the *Viewer*'s *Settings* control panel, in which you are able to specify settings for the camera layout, and specify the time span for use in the timeline.

See also *Setting Up the Camera Layout* on page 144.

Single View: Switches to a single, enlarged view of images from the camera selected in the camera layout.

Tip: You may also simply double-click a camera in the camera layout to switch between single view and multi-view.

Multi View: Switches to multi-view, displaying all cameras in the selected camera layout view.

Tip: You may also simply double-click a camera in the camera layout to switch between single view and multi-view.

Database Information: Opens the *Database Information* control panel, in which you select the cameras you want displayed in the camera layout.

See also *Assigning Cameras* on page 144.

Motion View: Opens the *Motion View* control panel, in which you are able to view a graph displaying sequences with motion.

The graph is draggable, allowing you to browse the sequences.

See also the description of *Motion View* on page 147.

Alarm Overview: Opens the *Alarm Overview* control panel, in which you are able to view a list of generated motion and event alarms.

By clicking alarms in the list, you are able to browse recordings from around the time at which the alarms were generated.

See also the description of *Alarm Overview* on page 148.

Image Controls: Opens the *Image Controls* control panel, in which you have access to digital zoom and de-interlacing settings.

See also *Digital Image Controls and Optimization* on page 150.

Export: Opens the *Export* control panel, with which you are able to export entire video and audio sequences in three different formats.

See also *How to Export Video and Audio Evidence* on page 153.

Print: Opens the *Print* control panel, from which you are able to print images from the camera selected in the camera layout.

See also *How to Print Evidence* on page 152.

Smart Search: Opens the *Smart Search* control panel, in which you are able to search for motion in one or more selected areas of recorded images from a particular camera.

See also the description of *Smart Search* on page 148.

Send E-mail Report: Opens the *Send E-mail Report* control panel, from which you are able to send evidence via e-mail.

See also *How to send Evidence via E-mail* on page 153.

Help: Lets you view the Viewer's built-in help.

Setting Up the Camera Layout

The camera layout is the area of the *Viewer* in which you view images. The camera layout section may display images from up to 16 different cameras at a time.

You can configure the camera layout to suit your exact needs: First specify the camera layout's grid size (i.e. how many camera slots you want the camera layout to contain), then specify which camera to use in each camera slot.

Selecting Grid Size

To specify how many camera slots you want in the camera layout, do the following:

1. Click the *Settings* icon in the *Viewer*'s toolbar.

   Settings icon

   This will open the *Settings* control panel.

2. In the *Settings* control panel's *Layout* list, select the required camera layout grid: 1×1, 2×2, 3×3 or 4×4.

   With a 4×4 grid, you will be able to display images from 16 cameras simultaneously in the camera layout.

3. Assign cameras to the camera layout's camera slots, as described in the following.

Assigning Cameras

Having specified the required grid size for the camera layout, assign cameras to the camera layout's camera slots the following way:

1. Click the *Database Information* icon in the *Viewer*'s toolbar.

   Database Information icon

   This will open the *Database Information* control panel.

2. Select a camera slot in the camera layout by clicking the required slot.

3. In the *Database Information* control panel's *Video Feed*, select the camera you want to assign to the selected slot.

   An image from the selected camera will show up in the selected slot (unless the selected time happens to be before the first recorded image from the camera).

   Tip: Your cameras may not all transfer images in a size that exactly matches the size of the camera layout's slots. This may result in black bars around images from some cameras when displayed in the camera layout. If you want to adjust the images from all cameras to fit the camera layout's camera slots, select the *Stretch Images To Fit* check box

in the *Settings* control panel. This may distort some images slightly, but will help you avoid any black bars around images.

4. If audio is enabled, you may also select a microphone from the *Audio Feed* list, in which case recordings from the selected microphone will be coupled with recordings from the selected camera.

5. Repeat for all cameras you want displayed in the camera layout.

Image Bars

Each camera slot in the camera layout is identified by an image bar, located in the top of each camera slot.

The image bar is blue. When you select a particular camera in the camera layout, the image bar of the selected camera image becomes a lighter blue.
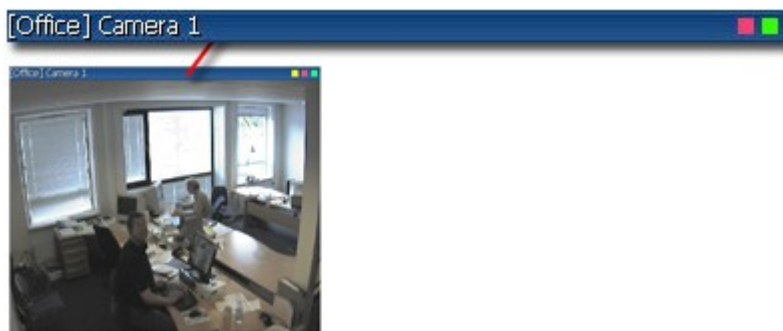
Camera slot; enlarged detail shows image bar

The image bar displays the name of the camera as well as the name of the device to which the camera is connected. The device name is displayed first, in square brackets, followed by the camera name.

Each image bar also features two colored indicators:

- *Motion indicator (the left indicator, red)*: Lights up during periods of motion.

- *Online indicator (the right indicator, green)*: Lights up during periods with recordings.

Storing and Recalling Views

You are able to save particular configurations of the camera layout as so-called views, and switch between them using the *Views* menu in the *Viewer*'s menu bar.

For example, you may store one view displaying images from 16 cameras and another view displaying images from eight other cameras.
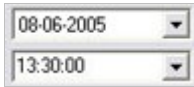
Browsing Recordings

With the *Viewer*, you are able to browse recordings in five different ways. Each is described in the following:

Time & Date Selector

Using the time & date selector, it is possible to jump straight to recordings from a specific point in time.

08-06-2005	▼
13:30:00	▼

Time & date selector

Simply select the required date in the date field, and the required time in the time field.

i **Tip:** You are able to overwrite the fields' date and time values.

Having used the data & time selector to jump to recordings from a specific point in time, you are able to use e.g. the timeline browser or the playback controls to browse through recordings from around the specified point in time.

Timeline Browser

The timeline browser displays an overview of periods with recordings from all cameras displayed in your current camera layout.

The number of timelines displayed in the timeline browser reflects the number of cameras displayed in the camera layout you are viewing. The timeline of the camera selected in the camera layout is highlighted.

Timeline browser; displaying timelines for
a camera layout with four cameras

The timeline browser uses the following colors:

Red (•): Recordings with motion

Green (•): Recordings without motion

Black (•): Periods without recordings

Yellow (•): Audio recordings

The timeline browser's white horizontal line indicates the point in time from which recordings are being displayed in the camera layout.

The area between the timeline browser's two blue horizontal lines is a magnification of the 30 seconds preceding and following the point in time from which recordings are being displayed in the camera layout.

You are able to specify which time span (1 hour, 2 hours or 12 hours) should be used in the timeline, and whether the newest recordings should be indicated at the top or at the bottom of the timeline. You specify this in the *Settings* control panel.

Tip: Use 1-hour or 2-hour time spans for the best possible overview of recordings.

Browsing Recordings with the Timeline Browser

To browse recordings using the timeline browser, click inside the timeline browser, and move your mouse up or down without releasing the mouse button. Browsing is fast when clicking outside the magnification area, and slow when clicking inside the magnification area.

Playback Controls

The *Viewer*'s playback controls are used for browsing and playing recordings, just like on a video recorder

Playback controls

Click [icon] or [icon] to browse to the oldest or the most recent recordings from the selected camera.

Click [icon] or [icon] to browse to the previous or next motion sequence from the selected camera.

Click [icon] or [icon] to browse to the previous or next image from the selected camera.

Use [icon] to start and stop playback. When playback is started, all cameras in the camera layout will play back recordings.

Use [icon] to control the playback speed. When the slider is in its middle position, playback is real-time, regardless of the recorded frame rates.

Motion View

Motion view lets you view a graph displaying sequences of recordings from the selected camera. The motion levels indicated in the graph can be used as an indication of what has been recorded. The graph is draggable, allowing you to browse the sequences.
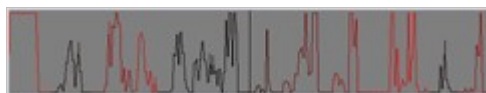
Motion view graph

To use motion view, click the *Motion View* icon in the toolbar to open the *Motion View* control panel, in which the draggable graph is displayed.

Motion View icon

A change in the color of the graph indicates the start of a new motion sequence.

The black vertical line at the center of the graph indicates the point in time from which recordings are being displayed in the camera layout.

Browsing Motion Sequences with Motion View

To browse recordings using motion view, click inside the graph area, and move your mouse sideways to browse recordings.

Images are updated when you release the mouse button.

Alarm Overview

Alarm overview lets you view a list of sequences with detected motion or events for a selected camera.

Listed motion sequences or events are clickable, allowing you to quickly jump to the time at which motion was detected or an event occurred.

To use the alarm overview, click the *Alarm Overview* icon in the toolbar to open the *Alarm Overview* control panel, in which the list is displayed.

Alarm Overview icon

By default, the list shows motion sequences from the most recent database for the selected camera.

If you want to view a list of sequences from archived databases as well, click the *Alarm Overview* control panel's *Get All* button.

Alarm Overview control panel

In addition to listing motion sequences, the *Alarm Overview* control panel can also display a list of occurred events (the camera's event log).

To toggle between viewing a list of motion sequences and a list of occurred events, click the *Alarm Overview* control panel's *Sequences* and *Events* buttons.

Browsing Recordings with the Alarm Overview

To view recordings from the time at which motion was detected, or an event occurred, select the required sequence/event in the list.

When you select a sequence/event in the list, the camera layout will display images matching the exact time of the motion detection or event.

To view what took place prior to and after the motion detection or event, use the timeline browser or playback controls to browse recordings from around the time of the motion detection or event.

Smart Search

Smart search lets you search for motion in one or more selected areas of the view from a particular camera.

To use smart search, do the following:

1. Select the required camera in the camera layout.

2. Single view is required to use smart search.

    If you are not already viewing images from the selected camera in single view, click the *Single View* icon in the toolbar to switch to single view.

    Single View icon

3. Click the *Smart Search* icon in the toolbar to open the *Smart Search* control panel.
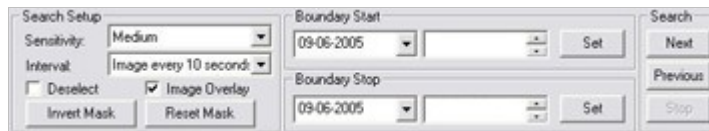
    Smart Search control panel

    When the *Smart Search* control panel opens, a blue grid will also appear as an overlay on the image in the camera layout.

4. Click and drag inside the image to select the areas in which you want to perform the smart search.

    The areas you select will become visible through the blue overlay. The blue overlay thus indicates areas to be excluded from the smart search.

    Example of selected area

5. In the *Smart Search* control panel, select required sensitivity in the *Sensitivity* list.

6. Select required image interval in the *Interval* list.

    If you select *All Images*, all images will be analyzed; if you select e.g. *Image every 10 seconds*, only one image per ten seconds of recordings will be analyzed.

    Selecting a long interval will greatly reduce the time required to complete the search. However, with a long interval, the search may not find motion sequences that are shorter than the specified interval.

7. In the *Boundary Start* and *Boundary Stop* sections, specify the period of time to be covered by the search.

Note that the smart search is always carried out from the time of the image you are viewing and forwards or backwards. The information you specify in the *Boundary Start* and *Boundary Stop* sections is only used to limit the search.
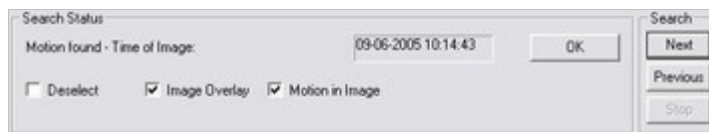
8. Click the *Next* (move forward in time) or *Previous* (move back in time) buttons to search through images with motion detected in the selected areas within the specified period of time.

Each image in which motion has been found will be displayed in the camera layout. The *Smart Search* control panel will show corresponding time information.

Smart Search control panel, displaying search status information

For each image found, you have the following options in the *Smart Search* control panel:

- *Deselect*: Even while viewing images in which motion has been found, you are able to adjust the area covered by smart search by dragging in the image.

  When the *Deselect* check box is cleared, areas you select in the image will be included in the smart search.

  When the *Deselect* check box is selected, areas you select in the image will be excluded from the smart search.

- *Image Overlay*: Select check box to display the blue image overlay grid indicating areas excluded from the search.

- *Motion in Image*: Select check box to highlight found motion in images.

Digital Image Control and Optimization

With the *Viewer*'s *Image Controls* control panel, you are able to adjust the image selected in the camera layout.

The *Image Controls* control panel also lets you view areas of the selected image in greater magnification.

To access the *Image Controls* control panel, click the *Image Controls* icon in the toolbar.

Image Controls icon

Image Controls control panel

De-interlacing

Interlacing is a method determining how an image is refreshed when shown on a screen.

With interlacing, the image is refreshed by first scanning every other line in the image, then scanning every opposite line, and so forth.

Interlacing thus allows for a faster refresh rate because less information must be processed during each scan.

However, in some situations, interlacing may cause flickering, or the changes in only half of the image's lines for each scan may be noticeable.

If images from the selected camera are interlaced, you are able to de-interlace the image by viewing only odd or even lines in the image.

Zoom Controls

With the zoom controls, you are able to view areas of the selected image in greater magnification.

Use the large *zoom in* and *zoom out* buttons to find the required zoom level.

When you have zoomed in on an area of an image, you are able to move around within the zoomed image by clicking the arrow buttons.

To quickly return to normal view of the selected image (i.e. without zoom), click the *H* (i.e. home) button.

Tip: To move around within the zoomed image, you may also simply click and drag the image in the required direction.

Smoothing and Scaling

To digitally smoothen images from the camera, select the *Smooth Images* check box.

To display images from the selected camera in the resolution they were recorded in, select the *Scale 1 : 1* check box.

If images are larger than the resolution available in the camera layout's camera slot, they will be reduced in size to fit the camera slot.

The correct aspect ratio will be maintained when reducing size this way.

Viewer: How to Store and Recall Views

You are able to save particular configurations of the camera layout as so-called views, and switch between them using the *Views* menu in the *Viewer*'s menu bar.

For example, you may store one view displaying images from 16 cameras and another view displaying images from eight other cameras.

Storing a View

To store your current camera layout as a view, do the following:

1. In the *Viewer*'s menu bar, select the *Views* menu.

2. In the *Views* menu, select the *Add to Views...* command.

   This will open the *Name of View* window:

The *Name of View* window

3. In the *Name of View* window, specify a name for the view, and click *OK*.

4. The view will now be selectable in the *Views* menu.

    If storing several different configurations of the camera layout as views, you will thus be able to switch between them using the *Views* menu.

Recalling a View

To recall a stored view, simply select the required view in the *Views* menu.

Editing or Deleting a Stored View

To edit or delete stored views, select *Organize Views...* in the *Views* menu.

This will open the *Views* control panel, in which you are able to rename views, change the sequence in which stored views appear in the menu, and delete views.

Viewer: How to Print Evidence

To print evidence from the *Viewer*, use the following procedure:

1. Select the required camera in the camera layout (see *Using the Viewer* on page 142), and browse to the image you want to print.

2. Click the *Print* icon:

    The *Print* icon

    This will open the *Print* control panel:

    The *Print* control panel

3. Fill in the *Operator's Note*, *Company*, and *Operator* fields.

4. Click the *Print* button to print the evidence on your default Windows printer.

   The printed surveillance report will contain the selected image, information about camera name, image capture time and report print time as well as the specified operator's name and operator's note.

Viewer: How to Send Evidence via E-mail

Note: The e-mail feature must be set up by the surveillance system administrator before you can use it. Ask if in doubt.
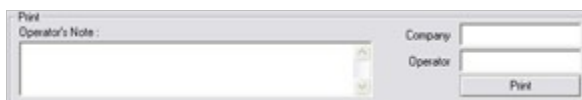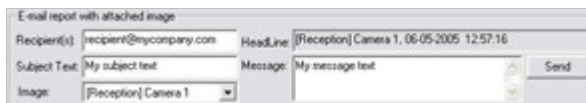
To send evidence from the *Viewer* via e-mail, use the following procedure:

1. Select the required camera in the camera layout (see *Using the Viewer* on page 142), and browse to the image you want to send via e-mail.

2. Click the *Send E-mail Report* icon:

   The *Send E-mail Report* icon

   This will open the *E-mail Report* control panel:

   The *E-mail Report* control panel

3. Type the e-mail address of the recipient.

   If sending to several recipients, separate e-mail addresses with a semicolon (example: aa@aa.aa;bb@bb.bb).

4. Type a subject text for the e-mail.

5. Verify that the *Image* field lists the camera you require.

6. Type a message, typically a description of the recorded incident.

7. Click the *Send* button.

Viewer: How to Export Video and Audio Evidence

You are able to export entire video and audio sequences in three different formats:

- AVI file (movie clip)

- Database files (you can include the Viewer itself in the export, so others can easily view the database files)

- JPG/WAV files (image/audio clip)

To export evidence from the *Viewer*, use the following procedure:

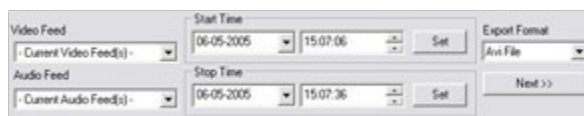1. Click the *Export* icon:

   The *Export* icon

   This will open the *Export* control panel.

   The *Export* control panel

2. In the *Export* control panel's *Video Feed* and *Audio Feed* lists, select the camera and—if required—microphone you want to export.

   Tip: With the options *Current Video Feed(s)* and *Current Audio Feed(s)* you can batch export all cameras and microphones in your current view.

3. Browse to the required start time for the export, and click the *Start Time* section's *Set* button.

4. Browse to the required stop time of the export, and click the *Stop Time* section's *Set* button.

5. Select required *Export Format*, click the *Next* button, and follow **one** of the procedures described in the following.

   Note that procedures vary depending on the selected export format.

   Export format: AVI File

   a. Select required *Export Path* (if you keep the default setting, the files will be exported to an *Exported Images* folder on your desktop).

   b. Select required frame rate.

      Full will export all images to the AVI file.

      Half will reduce the size of the AVI file by only exporting every second image, yet still play back in real-time speed.

   c. Select whether timestamps from the surveillance system should be added to the AVI file.

   d. In the *Codec* list, select the video codec (compression/decompression technology) you want to use for generating the AVI file.

The *Codec* list only lists codecs supporting the resolution of the camera.

ⓘ **Tip:** If available, the codec *Indeo® Video 5.10* is recommended.

e. Click *Next* to start the export.

Export format: Database Files

a. Select required *Export Path* (if you keep the default setting, the database files will be exported to an *Exported Images* folder on your desktop).

b. Select whether the *Viewer* program files should be included in the export. If you include the *Viewer* in the export, the exported databases can be viewed on any PC.

c. Click *Next*. Fill in the *Operator* and *Operator's Note* fields.

d. Click *Next*, and select whether to encrypt and/or compress the exported databases.

If you select encryption, specify a password for decrypting the exported databases, and remember to send the password to the recipient **separately**.

e. Click *Next* to start the export.

ⓘ **Tip:** If you included the Viewer application in your export, copying all exported files to the root of a CD or DVD will start the CD/DVD automatically when the recipient inserts it.

Export format: JPG/WAV files

a. Select required *Export Path* (if you keep the default setting, the files will be exported to an *Exported Images* folder on your desktop).

b. Select whether timestamps from the surveillance system should be added to the exported JPGs.

c. Click *Next* to start the export.

Viewer: How to View Archived Images

With Milestone XProtect Enterprise's archiving feature (see page 124), it is possible to keep recordings for as long as required, limited only by the available hardware storage capacity.

Archived recordings can be viewed using the *Viewer*, allowing you to use all of the *Viewer*'s features for image browsing for archived recordings as well.

The way in which you find the archived images to view varies slightly depending on how the archives are stored.

To view archived images in the *Viewer*, do the following:

Archives Stored Locally or on Network Drives

For archived images stored locally or on network drives you simply use the *Viewer*'s image browsing features, for example the timeline or the playback controls, for finding and viewing the required images; just like you would with images stored in a camera's regular database.

Exported Archives

For exported archives, e.g. archives stored on a CD, you click the *browse* button in the *Viewer*'s *Database Information* control panel to browse for the archive you want to view.

Once you have specified the required archive this way, you can use all of the *Viewer*'s image browsing features for navigating the images in the archive.

Viewing archived images in the *Viewer*. Arrow indicates the browse button in the *Viewer*'s Database Information control panel.

Remote Access

Remote Access Overview

Remote users can access a Milestone XProtect Enterprise surveillance system in three different ways:

- With a *Remote Client* (see page 171). The feature-rich *Remote Client* can be installed locally or run from server)

- With a *Smart Client* (see page 210). The very feature-rich *Smart Client* is installed locally. The *Smart Client* is based on the .Net development platform, and is thus highly flexible for integration of plugins, etc.

- With a regular Microsoft Internet Explorer browser (limited feature set, recommended only for remote users on slow connections)

Server End

The way remote access is handled at the surveillance system server end is different, depending on remote access method:

Providing Remote Client and Smart Client Access

Images viewed by *Remote Client* and *Smart Client* users are provided by the Milestone XProtect Enterprise surveillance system's *Image Server*.

The *Image Server* runs as a service on the Milestone XProtect Enterprise server; it does not require separate hardware. The Milestone XProtect Enterprise system administrator uses the *Image Server Administrator* window (see page 162) to manage *Remote Client* and *Smart Client* access to the surveillance system.

Providing Regular Browser Access

As an alternative to using *Remote Client* or *Smart Client*, images can also be provided through the Milestone XProtect Enterprise surveillance system's built-in *Web Server* and *RealtimeFeed Server* (see page 251). When this is the case, remote users connect to the *Web Server* and the *RealtimeFeed Server* through a regular browser; no client software is required.

The *Web Server* and the *RealtimeFeed Server* do by no means offer as advanced functionality as the *Image Server/Remote Client/Smart Client*; neither at the server end, nor at the client end. However, if remote users are to access the surveillance system through very slow connections, such as 28.8 Kbps connections, using the *Web Server* and the *RealtimeFeed Server* may be advisable.

For a remote user perspective of regular browser access through the *Web Server* and *RealtimeFeed Server*, see *Remote Access through Web and RealtimeFeed Servers* on page 259.

Choosing a Remote Access Solution

Your organization's choice of remote access solution will depend on the organization's requirements:

Determining the Organization's Needs

When deciding which remote access solution is the best choice for your organization, system administrators may find it helpful to review the following:

Note: Systems and requirements differ from organization to organization. The following questions and answers are thus for guidance only.

Will remote users access the surveillance system over very slow connections, such as 28.8 Kbps connections?

- **Yes:** Use regular browser access through the *Web Server/RealtimeFeed Server*.

- **No:** Use *Remote Client* or *Smart Client* access through the *ImageServer*.

Is it acceptable to install client software on remote users' computers?

- **Yes:** Use *Remote Client* or *Smart Client* access through the *ImageServer*.

- **No:** Use *Remote Client* access through the *ImageServer*, as remote users can run the *Remote Client* straight from the Milestone XProtect Enterprise server as an alternative to the client being installed on remote users' computers. Remote access can also be provided through the *Web Server/RealtimeFeed Server*, as this does not require any client software, but this is only recommended for remote access through very slow connections.

Will you require a large amount of future flexibility from your remote access solution?

- **Yes:** Use *Smart Client* access through the *ImageServer*. Due to the way the software has been developed, the *Smart Client* offers a high degree of flexibility for integration of new features, plugins, etc.

- **No:** Use *Remote Client* access through the *ImageServer*.

Do you require a very feature-rich client application?

- **Yes:** Use *Smart Client* access through the *ImageServer*. The *Smart Client* offers more features for remote users than the other solutions.

- **No:** Use *Remote Client* access through the *ImageServer*.

Will you use a .Net-based client application?

The. Net software development platform allows the interconnection of computers and services for the exchange and combination of data and objects. The platform makes extensive use of so-called web services, which provide the ability to use the web rather than single applications for various services. This in turn provides the ability for centralized data storage as well as automated updating and synchronization of information.

The .Net platform enhances software developers' ability to create re-usable and customizable modules, which makes it possible to develop highly flexible software solutions. You can therefore, as a rule of thumb, expect .Net-based software to be highly flexible, ready for integration of new features, plugins, etc. However, organizations and their requirements are different, and some organizations find that the high degree of interconnection of services and computers inherent in a .Net-based solution is not desirable. Instead, such organizations rely on more classic Windows solutions.

- **Yes:** Use *Smart Client* access through the *ImageServer*. The .Net-based *Smart Client* offers more features for remote users than the other solutions. .Net Framework 1.1, downloadable from http://www.microsoft.com/downloads/, is required on computers running the *Smart Client*.

- **No:** Use *Remote Client* access through the *ImageServer*. The *Remote Client* is not a .Net-based solution.

Differences between the Three Remote Access Solutions

The following table outlines the main differences between the three remote access solutions:

Remote Access Solutions at a Glance	Regular Browser Access through *Web Server/ RealtimeFeed Server*	*Remote Client* Access through *ImageServer*	*Smart Client* Access through *ImageServer*
Remote User's Installation	None; remote user access system through regular browser.	Optional; client can be installed on remote user's computer or accessed from server.	Client must be installed on remote user's computer. .Net Framework 1.1 is required on computers running the *Smart Client*.
Remote User's Feature Set	Limited.	Feature-rich.	Very feature-rich.
Remote User's Ease of Use	Easy to use.	Very easy to use. Setup of camera views can be handled locally as well as centrally. With central views handling, remote users can begin using their *Remote Client* instantly upon first login.	Very easy to use. Setup of camera views can be handled locally as well as centrally. With central views handling, remote users can begin using their *Smart Client* instantly upon first login.
System Administrator's Installation	None; the *Web Server* and *RealtimeFeed Server* are integrated in Milestone XProtect Enterprise.	None; the *ImageServer* runs as a service on the Milestone XProtect Enterprise server.	None; the *ImageServer* runs as a service on the Milestone XProtect Enterprise server.
System Administrator's Feature Set	Limited; configuration primarily through *Web Server*.	Very flexible; configuration through *ImageServer Administrator* includes master-slaves handling, handling of local IP address ranges, etc.	Very flexible; configuration through *ImageServer Administrator* includes master-slaves handling, handling of local IP address ranges, etc.

System Administrator's Access Control Options	Limited; user rights primarily determined on a per-camera basis.	Very flexible; rights for accessing individual *Remote Client* and camera features are determined on a per-user basis.	Very flexible; rights for accessing individual *Smart Client* and camera features are determined on a per-user basis.
Client Flexibility re. Future Features and Plugins	Very limited.	Limited.	.Net-based, thus offering a high degree of flexibility for integration of new features, plugins, etc. The client solution of the future.
Recommended Use	Systems with remote users on very slow connections.	Systems on which installation of client software must be optional. Systems on which a .Net client solution is not desirable.	Systems on which a .Net client solution is desirable. Systems on which a high degree of flexibility, e.g. use of remote access plugin features, will be required.

Differences between Remote Client and Smart Client Specifically

The *Remote Client* and *Smart Client* may initially look quite similar. However, the two clients are programmed differently, they have different installation requirements, and one client offers more features than the other:

Programming Differences: .Net or Not?

As opposed to the *Remote Client*, the *Smart Client* has been developed based on the .Net software development platform.

Net Framework 1.1, downloadable from http://www.microsoft.com/downloads/, is required on computers running the *Smart Client*.

The. Net software development platform allows the interconnection of computers and services for the exchange and combination of data and objects. The platform makes extensive use of so-called web services, which provide the ability to use the web rather than single applications for various services. This in turn provides the ability for centralized data storage as well as automated updating and synchronization of information.

The .Net platform enhances software developers' ability to create re-usable and customizable modules, which makes it possible to develop highly flexible software solutions. You can therefore expect the .Net-based *Smart Client* to be a highly flexible client, ready for integration of new features, plugins, etc.

However, organizations and their requirements are different, and some organizations find that the high degree of interconnection of services and computers inherent in a .Net-based solution is not desirable. If your organization has chosen to apply a conservative approach regarding .Net-based software, using the *Remote Client* will be the perfect solution for you.

Installation Differences

The *Remote Client* can be installed on the remote user's computer or the user can connect to the Milestone XProtect Enterprise server and run the *Remote Client* from the server.

The *Smart Client* must be installed on the remote user's computer.

.Net Framework 1.1, downloadable from http://www.microsoft.com/downloads/, is required on computers running the *Smart Client*.

Feature Differences

The *Smart Client* offers more features than the *Remote Client*.

With the *Remote Client*, remote users are able to:

- View live images from cameras on the surveillance system.

- Browse recordings from cameras on the surveillance system.

- Create and switch between an unlimited number of views, each able to display images from up to 16 cameras from multiple servers at a time. Views can placed in *private* groups (only accessible by the user who created them) or *shared* groups (accessible by all remote users connected to the Milestone XProtect Enterprise server).

- Include static images and HTML pages in views.

- Control PTZ (Pan/Tilt/Zoom) and IPIX (360° view) cameras.

- Activate external outputs.

- Get quick overviews of sequences with detected motion.

- Print images.

- Generate and export evidence in AVI (movie clip) and JPEG (still image) formats.

The *Smart Client* offers all of the above, plus:

- The ability to activate manually triggered events (also known as *event buttons*).

- The ability to get quick overviews of detected events.

- The ability to quickly search selected areas of camera images for motion (also known as *Smart Search*).

- The ability to create special views for widescreen monitors.

- The ability to individually configure and use several different joysticks.

- The ability to assign user-specific keyboard shortcuts to common actions*.*

- The ability to skip gaps during playback of recordings.

- More features for printing images.

Image Server Administration

Images viewed by *Remote Client* (see page 171) and *Smart Client* (see page 210) users are provided by the Milestone XProtect Enterprise surveillance system's *Image Server*.

The *Image Server* runs as a service on the Milestone XProtect Enterprise server; it does not require separate hardware.

The Milestone XProtect Enterprise system administrator uses the *Image Server Administrator* to manage *Remote Client* and *Smart Client* access to the surveillance system:

Image Server Administrator Window

The *Image Server Administrator* window is used by the surveillance system administrator to manage the *Image Server*.

Access: To access the *ImageServer Administrator* window, click the *Image Server Administrator* shortcut on the desktop:

Image Server Administrator
desktop shortcut

The *ImageServer Administrator* window lets you specify settings for *Remote Client* and *Smart Client* access in a number of sections, each targeted at a particular part of the remote access configuration. Each section of the *ImageServer Administrator* window is described in the following.

ImageServer Administrator window

Note: Computers running Milestone XProtect Enterprise act as servers. Such servers are occasionally referred to as *Engines*. When you see the term *Engine* in the *ImageServer Administrator* window or in the *Remote Client* or *Smart Client*, the term basically means *server*.

The *ImageServer Administrator* window is divided into six sections:

Engine Setup Section (for Specifying Name, Port and Outside Access)

The *ImageServer Administrator* window features two *Engine Setup* sections. The *Engine Setup* section in the top part of the window is used for specifying server name and port, for enabling optional external access to the server, and for optional definition of IP address ranges which should be recognized as being local:

Field, Button	Description
Engine Name	Lets you specify a name for the server. By default, the name is *Engine*. You are able to change the default name. *Remote Client* and *Smart Client* users will see the name of the server when they configure views on their *Remote Client*'s or *Smart Client*'s *Setup* tab

(provided their user rights permit them to use the *Setup* tab).
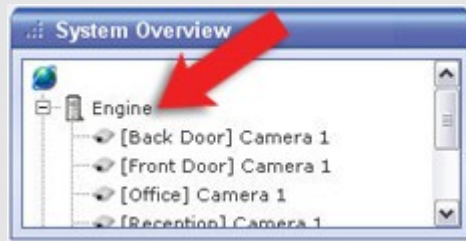
Engine name, as remote users will see it in the *System Overview* section of the *Remote Client*'s or *Smart Client*'s *Setup* tab. In this case, the default name *Engine* has been used.

Engine Port	Lets you specify a port number to use for the server. The default port number is 80. You are able to change the default port number.
Enable Outside Access	Select check box if *Image Server* should be accessible from the internet via a router or firewall. If selecting this option, also specify the outside (public) IP address and port number in the *Outside IP Address* and *Outside Port* fields. **Note:** When using outside access, the router or firewall used must be configured so requests sent to the outside (public) IP address and port are forwarded to the inside (local) IP address and port of the server running the *Image Server* service.
Outside IP Address	Lets you specify a public IP address for use when the server should be available from the internet.
Outside Port	Lets you specify a port number for use when the server should be available from the internet. The default port number is 80. You are able to change the default port number.
Local IP Ranges...	Opens the *Define local IP ranges* window (see page 166), in which you are able to define IP address ranges which the *Image Server* should recognize as coming from a local network. Background: When a *Remote Client or Smart Client* connects to a surveillance system, an amount of initial data communication, including the exchange of contact IP addresses goes on in the background, completely automatically and transparent to users. However, when a *Remote Client or Smart Client* on a local network connects to a surveillance system which is also on the local network, the *Image Server* may, if different subnets are involved, not recognize the *Remote Client*'s or *Smart Client*'s IP address as being local. When this is the case, the *Image Server* may not return a suitable IP

address to the *Remote Client* or *Smart Client* for further communication between the two.

Therefore, you are able to define a list of IP ranges which the *Image Server* should recognize as coming from a local network, in which case it will respond with a suitable IP address and seamless communication will be possible.

User Administration Section

Accounts and rights for *Remote Client* and *Smart Client* users are configured in the *ImageServer Administrator* window's *User Administration* section. *Remote Client* and *Smart Client* users must be defined in this section in order to be able to log in to the surveillance system.

Defining Users and Passwords

To define *Remote Client* and *Smart Client* users and passwords, click the *User Setup* button. This will open the *User administration* window (see page 167), in which you define individual users and their passwords.

Defining User Access Rights

Having defined users, you are able to define whether all users should have access to all *Remote Client/Smart Client* features and all available cameras, or whether access should be restricted by user.

Full Access for All Users

To give all users access to all *Remote Client/Smart Client* features and all available cameras, select *Full access for all users*.

Restricted Access

To use restricted access, select *Restrict user access*. Then click the *User Access...* button to open the *Define rights for individual users* window (see page 168), in which you define access rights for each user.

Engine Setup Section (for Specifying Max. Clients and Slaves Settings)

The ImageServer Administrator window features two Engine Setup sections. The Engine Setup section in the middle part of the window is used for specifying the maximum number of *Remote Clients* and *Smart Clients* allowed to connect simultaneously, and for specifying any other Milestone XProtect Enterprise servers that should run as slaves:

Specifying Max. Number of Simultaneously Connected Clients

You are able to limit the number of *Remote Clients* and *Smart Clients* allowed to connect at the same time. Depending on your Milestone XProtect Enterprise 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 *Remote Clients/Smart Clients* attempt to log in, only the allowed number of *Remote Clients/Smart Clients* will be allowed access. Any *Remote Clients/Smart 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 *Remote Clients/Smart Clients* are allowed.

To specify a different maximum number of *Remote Clients/Smart Clients* allowed to connect at the same time, overwrite the value in the *Max. number of clients* field with the required value.

Tip: To allow an unlimited number of simultaneously connected *Remote Clients/Smart Clients*, type *0* (zero) in the *Max. number of clients* field.

Specifying Slave Servers

In addition to viewing images from cameras connected to the Milestone XProtect Enterprise server you are configuring, *Remote Client* and *Smart Client* users are able to view images from cameras connected to other Milestone XProtect Enterprise servers as well.

This is achieved by defining such other Milestone XProtect Enterprise servers as slave servers. When this is the case, the Milestone XProtect Enterprise server you are configuring will act as the master server each slave server. When *Remote Clients* or *Smart Clients* connect to the master server, they will instantly get access to the slave servers as well.

Note: When using slave servers, *Remote Client/Smart Client* users must be defined on the master server as well as on each of the slave servers. Only cameras to which a user has access will be visible to the user, regardless of whether the camera is connected to the master server or to a slave server. If accessed from the internet, *Outside Access* must be enabled on all slave servers, and ports must be mapped accordingly in the router or firewall used.

To define other Milestone XProtect Enterprise servers as slave servers, click the *Slaves* button. This will open the *Slave Administration* window (see page 170), in which you are able to list all required slave servers.

Log Files Section

In the *Log Files* section, specify the number of days to keep log files in the *Image Server*'s regular event log.

By default, such log files are kept for ten days before they are deleted.

Tip: Read more about Milestone XProtect Enterprise logging on page 265.

Audit Log Section

Audit logging is the logging of *Remote Client* and *Smart Client* user actions.

If this type of logging is required, select the *Enable Audit Logging* check box.

When audit logging is enabled, you are able to specify the following values:

Field	Description
Days to log	Number of days in which audit log files should be kept before they are deleted. Default is 30 days. If you specify *0* (zero), audit log files will be kept indefinitely (disk storage 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	Maximum number of seconds to pass for viewed images to be considered to be within the same sequence. Specifying a high number of seconds may thus help limit the number of viewed sequences logged, and reduce the size of the audit log. Default is ten seconds.

Tip: Read more about Milestone XProtect Enterprise logging on page 265.

Language Support and XML Encoding Section

The *Image Server*, *Remote Client* and *Smart Client* support local character sets, such as Greek, Hebrew, Japanese, etc. for use in camera names, user names, passwords, etc.

Select the required language in the *Language* list.

Define Local IP Ranges Window

The *Define local IP ranges* window lets you define IP address ranges which the *Image Server* should recognize as coming from a local network.
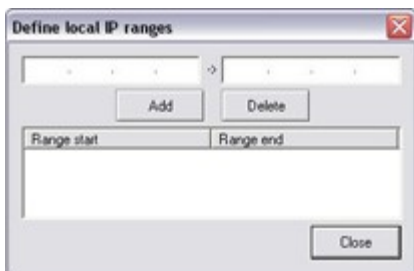
Define local IP ranges window

Access: You access the *Define local IP ranges* window by clicking the *Local IP Ranges...* button in the *ImageServer Administrator* window (see page 162).

To define a local IP address range in the *Define local IP ranges* window, do the following:

1. Specify the beginning of the IP address range in the *Define local IP ranges* window's first field, and the end of the IP address range in the second field.

2. Click the *Add* button.

   The IP address range will be added to the list in the lower part of the *Define local IP ranges* window.

You may define as many local IP address ranges as required. If required, an IP address range may include only one IP address (example: 192.168.10.1-192.168.10.1).

3. When ready, click the *Define local IP ranges* window's *Close* button to return to the *ImageServer Administrator* window.

Tip: As such, there is no feature for editing an already defined IP address range in the *Define local IP ranges* window. However, you can simply select the range in question in the *Define local IP ranges* window's list, delete it by clicking the *Delete* button, and then simply add a new range reflecting your requirements.

User Administration Window

The *User administration* window lets you define individual *Remote Client* and *Smart Client* users and their passwords.

User administration window

Access: You access the *User administration* window by clicking the *User Setup...* button in the *ImageServer Administrator* window (see page 162).

Adding a New User

To define a new user, click the *User administration* window's *Add user...* button, specify required user name and password, and click *OK*. This will add the user to the *User administration* window's list of users.

Editing an Existing User Name or Password

To edit the user name or password for a user already listed in the *User administration* window's list of users, select the required user in the *Current users* list and click the *User administration* window's *Edit user* button.

Removing an Existing User

To remove a user from the *User administration* window's list of users, select the user in the list and click the *Delete user* button. When removed from the list, the user will no longer be able to log in with the *Remote Client* or *Smart Client*.

Define Rights for Individual Users Window

The *Define rights for individual users* window lets you define access rights for individual *Remote Client* and *Smart Client* users.

Define rights for individual users window

Access: You access the *Define Rights for Individual Users* window by clicking the *User Access...* button in the *ImageServer Administrator* window (see page 162).

To define access rights for a particular user, do the following in the *Define Camera Access for individual users* window:

1. In the *User* list, select the required user.

2. In the *Global User Rights* section, select the user's global (i.e. non-camera-specific) rights:

   - *View Live*: Ability to view the *Live* tab in the *Remote Client/Smart Client*. If the user does not have this right, the *Live* tab will not be selectable in the *Remote Client/Smart Client*.

   - *Browse*: Ability to view the *Browse* tab in the *Remote Client/Smart Client*. If the user does not have this right, the *Browse* tab will not be selectable in the *Remote Client/Smart Client*.

   - *Setup*: Ability to view the *Setup* tab in the *Remote Client/Smart Client*. If the user does not have this right, the *Setup* tab will not be selectable in the *Remote Client/Smart Client*.

   - *Edit Shared Views*: Ability to create and edit shared views in shared groups in the *Remote Client/Smart Client*. Views placed in shared groups can be accessed by every *Remote Client/Smart Client* user (for more information about views, see *Creating Views (Remote Client)* on page 176 or *Creating Views (Smart Client)* on page 214). If the user does not have this right, shared groups in the *Remote Client/Smart Client* will be protected, indicated by a padlock icon.

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

- *Edit Private Views*: Ability to create and edit views in private groups in the *Remote Client/Smart Client*. Views placed in private groups can only be accessed by the *Remote Client/Smart Client* user who created them (for more information about views, see *Creating Views (Remote Client)* on page 176 or *Creating Views (Smart Client)* on page 214). Denying remote users the ability to create their own views may make sense in some cases; for example in order to limit bandwidth use. If the user does not have this right, private groups in the *Remote Client/Smart Client* will be protected, indicated by a padlock icon.

Tip: By clearing the *View Live*, *Browse* and *Setup* check boxes you can effectively disable the user's ability to use the *Remote Client/Smart Client*, for example while the user is on vacation. This would typically be a temporary alternative to deleting the user.

3. In the *User Rights for Camera* section's *Defined Cameras* list, select each camera to which the user should have access via the *Remote Client/Smart Client*.

   Tip: By pressing the CTRL or SHIFT buttons on your keyboard while selecting cameras in the *Defined Cameras* list, you are able to select several or all of the listed cameras in one go.

4. Click the >> button to move the selected cameras to the *Viewable by selected user* list.

5. For **each** camera now listed in the *Viewable by selected user* list, specify the features to which the user should have access by selecting the features in the *User Rights for the Selected Camera* section.

   The following features, all selected by default, are available:

   - *Live*: Ability to view live images from the selected camera.

   - *Browse*: Ability to browse recorded images from the selected camera.

   - *PTZ*: Ability to use the *Remote Client*'s or *Smart Client*'s navigation features for PTZ (Pan/Tilt/Zoom) cameras. The user will only be able to use this right if having access to one or more PTZ cameras.

   - *PTZ Preset Positions*: Ability to use the *Remote Client*'s or *Smart Client*'s navigation features for moving a PTZ camera to particular preset positions. The user will only be able to use this right if having access to one or more PTZ cameras with defined preset positions.

   - *Outputs*: Ability to trigger outputs (e.g. switching on lights, sounding sirens, or similar), if such outputs are available.

   - *Events*: Ability to use the *Smart Client*'s *Event Control* feature for manually triggering events.

     Note: The *Event Control* feature is available in the *Smart Client* only.

   - *Smart Search*: Ability to use the *Smart Client*'s *Smart Search* feature, with which users are able to search for motion in one or more selected areas of images from the selected camera.

     Note: The *Smart Search* feature is available in the *Smart Client* only.

- *AVI Export*: Ability to generate and export evidence as movie clips in the AVI format.

- *JPG Export*: Ability to generate and export evidence as JPG images.

- *Alarms*: Ability to use the *Alarms* feature for browsing images from a selected camera.

ℹ️ **Tip:** Note that some of the features are mutually dependent: For example, in order have access to PTZ or output features, the user must also have access to viewing live images; and in order to use AVI and JPG export, the user must have access to browsing recorded images.

6. Repeat as required for other users.

Slave Administration Window

The *Slave Administration* window lets you define all servers required to run as slaves under the Milestone XProtect Enterprise server you are configuring.

Slave Administration window

➡️ **Access:** You access the *Slave Administration* window by clicking the *Slaves...* button in the *ImageServer Administrator* window (see page 162).

Adding a Slave Server

To add a slave server, click the *Slave Administration* window's *Add Slave...* button, specify the host name of the slave server, specify the required port number, and click *OK*. This will add the slave server to the *Slave Administration* window's list of slave servers.

ℹ️ **Tip:** Instead of specifying a host name when adding a slave server, you may specify the IP address of the slave server. Simply type the IP address in the *Hostname* field when adding the slave server. Remember that if on a local network, the *local* IP address of the slave server must be used.

Removing a Slave Server

To remove a slave server from the *Slave Administration* window's list of slave servers, select the slave server in the list and click the *Delete Slave* button.

Remote Viewing of Live Images from Stopped Cameras

Remote Client and *Smart Client* users are able to view live images from cameras even though the cameras in question are stopped. This, however, requires that a particular setting in the *Administrator* application (see page 30) is enabled.

Note: Access to features in the *Administrator* application, including those described in the following, may require administrator rights.

To enable the required setting, open the *Administrator* application, and do the following:

1. In the *Administrator* window (see page 30), click the *General Settings...* button.

   This will open the *General Settings* window (see page 79).

2. In the *General Settings* window's *Advanced* section, select *Start cameras on remote live requests*.

3. Click *OK*.

Remote Client

About the Remote Client

The *Remote Client* provides remote users with feature-rich access to the surveillance system. It lets users access multiple servers at a time, allowing remote user access across systems.

Example of the *Remote Client*, displaying images from 16 cameras

The *Remote Client* may either be installed locally on the remote user's computer, or it may be accessed through the internet and run from the Milestone XProtect Enterprise server.

DirectX 9.0 must be installed on the remote user's computer. DirectX is a Windows extension providing advanced multimedia capabilities; these capabilities are required when using the *Remote Client* to connect to the Milestone XProtect Enterprise surveillance system.

To check which DirectX version is installed on a computer, click *Start*, select *Run...*, and type dxdiag. When you click *OK*, the *DirectX Diagnostic Tool* window will open; version information is displayed near the bottom of its *System* tab. DirectX is available from http://www.microsoft.com/downloads/.

What are Remote Users Able to do with the Remote Client?

With the *Remote Client*, remote users are able to:

- View live images from cameras on the surveillance system.

- Browse recordings from cameras on the surveillance system.

- Create and switch between an unlimited number of views, each able to display images from up to 16 cameras from multiple servers at a time. Views can placed in *private* groups (only accessible by the user who created them) or *shared* groups (accessible by all *Remote Client* users connected to the Milestone XProtect Enterprise server).

- Control PTZ (Pan/Tilt/Zoom) and IPIX (360° view) cameras.

- Activate external outputs.

- Get quick overviews of sequences with detected motion.

- Print images.

- Generate and export evidence in AVI (movie clip) and JPEG (still image) formats.

- View HTML pages and static images.

How does the Remote Client Get Images from the Surveillance System?

Images viewed by *Remote Client* users are provided by the *Image Server*. The *Image Server* runs as a service on the Milestone XProtect Enterprise server; it does not require separate hardware. The Milestone XProtect Enterprise system administrator uses the *Image Server Administrator* window (see page 162) to manage *Remote Clients'* access to the surveillance system.

How can User Rights Affect Use of the Remote Client?

The rights of individual remote users are specified centrally by the surveillance system administrator. The rights of an individual user will determine the user's ability to use the *Remote Client*'s features.

Basically, the surveillance system administrator is able to restrict a user's rights to the following:

- Access to the *Remote Client*

- Access to each of the *Remote Client*'s tabs: *Live*, *Browse* and *Setup*

- Ability to use features on the *Remote Client*'s tabs

- Ability to create views (views determine the way in which images from one or more cameras are displayed)

- Ability to view images from specific cameras

The ability to use various features of the *Remote Client* may therefore vary considerably from user to user. Ask your surveillance system administrator if in doubt about your user rights.

How does the Remote Client Differ from the Smart Client?

For a description of how the *Remote Client* differs from the *Smart Client*, see *Remote Access Overview* on page 157.

Downloading and Installing the Remote Client

Note: Downloading and installation of the *Remote Client* may not be necessary: The *Remote Client* may indeed be downloaded and installed locally on the remote user's computer, but it may also be run directly from the Milestone XProtect Enterprise server. If you choose to run the *Remote Client* directly from the Milestone XProtect Enterprise server, you simply access it through the internet (see *Accessing a Remote Client Run from Server* on page 174). When this is the case, no downloading or installation is required.

If you wish to download and install the *Remote Client*, do the following:

1. Open an Internet Explorer browser (version 6.0 or later), and connect to the URL or IP address specified by your system administrator in order to connect to the Milestone XProtect Enterprise server.

   When you connect to the Milestone XProtect Enterprise server, you will see a welcome page.

2. In the *XProtect Remote Client* section of the welcome page, click the *Download and install XProtect Remote Client locally* link:

Detail from welcome page; arrow indicates *Download and install XProtect Remote Client locally* link

3. Depending on your security settings, you may receive a security warning (*Do you want to run or save this file?*).

When this is the case, click the *Run* button.

4. Depending on your security settings, you may receive a further security warning (*Do you want to run this software?*).

   When this is the case, click the *Run* button.

5. The *Milestone XProtect Remote Client Setup Wizard* begins.

   In the wizard, click *Next* and follow the installation instructions.

Accessing the Remote Client

Accessing and configuring the *Remote Client* is very straightforward. Even first time users will typically be able to start and set up their *Remote Client* in a matter of minutes.

The *Remote Client* may either be installed locally on the remote user's computer, or it may be run from the Milestone XProtect Enterprise server.

The way you access the *Remote Client* differs slightly depending on which of the two options is used.

Accessing a Remote Client Run from Server

If you want to run the *Remote Client* straight from the Milestone XProtect Enterprise server, open an Internet Explorer browser (version 6.0 or later), and connect to the URL or IP address specified by your system administrator.

When you connect to the Milestone XProtect Enterprise server, you will see a welcome page:
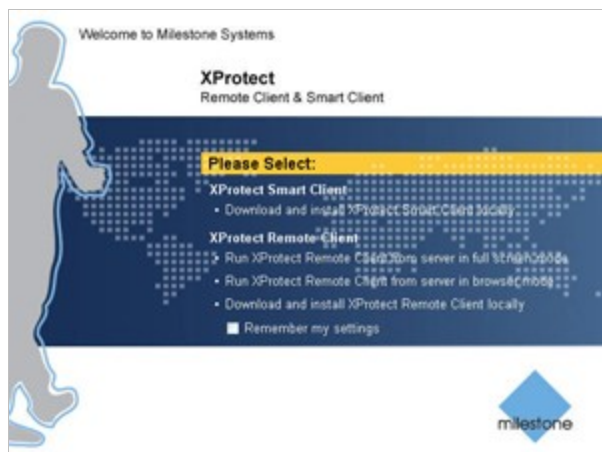
Detail from welcome page

In the *XProtect Remote Client* section of the welcome page, select between three ways of accessing the *Remote Client*:

- *Run XProtect Remote Client from server in full screen mode*:
  Lets you use the *Remote Client* directly from the Milestone XProtect Enterprise server, in full screen mode. In full screen mode, Internet Explorer's usual navigation buttons are not shown, which means that more screen space is available for viewing the *Remote Client*

window. If selecting this option, you may be required to download the file *full.hta*. Downloading this file ensures that the *Remote Client* will work properly in full screen mode.

- *Run XProtect Remote Client from server in browser mode*:
  Lets you use the *Remote Client* directly from the Milestone XProtect Enterprise server, in browser mode. In browser mode, you view the *Remote Client* just like a regular web page in Internet Explorer.

- *Download and install XProtect Remote Client locally*:
  Lets you download and install the *Remote Client* on your computer. If you prefer this option, see *Downloading and Installing the Remote Client* on page 173.

Tip: By selecting *Remember my settings*, you can save your preferred access method (e.g. browser mode) and automatically use it the next time you connect. This requires that your browser's privacy settings allow cookies; to check your browser's privacy settings, select the *Tools* menu, then *Internet Options...*, then the *Privacy* tab, on which privacy settings are determined in the *Settings* section.

Accessing a Locally Installed Remote Client

If the *Remote Client* is already installed locally, simply click the *Remote Client* shortcut to access it.

Depending on your selections when installing the *Remote* Client locally, the shortcut may be located in Windows' quick launch bar (next to the *Start* button), or it may be placed on your desktop.

You may also access a locally installed *Remote Client* by selecting *Start > All Programs > Milestone XProtect Enterprise Remote Client*, then selecting either browser or full screen mode.

Upon Accessing: Logging In

When accessing the *Remote Client*, either running it from the Milestone XProtect Enterprise server or by opening a locally installed version, you will be asked to log in:

Detail from *Remote Client* login window

To log in, do the following:

1. Specify your login information in the following fields:

   - *Username*: Type your user name as specified by your system administrator. The user name is case-sensitive, i.e. there is a difference between typing, for example, *amanda* and *Amanda*.

   - *Password*: Type your password as specified by your system administrator. The password is case-sensitive.

- *Address*: Type the URL or IP address specified by your system administrator. This will typically be the same URL or IP address you used if connecting to the *Remote Client* through a browser, although it may occasionally be a different one.

- *Port*: Internet connections may use different ports for different purposes. Specify the port number, your system administrator has asked you to use when logging in to the *Remote Client*. In most circumstances, port 80 is used.

Tip: The vast majority of *Remote Client* users will always log in to the same address and port number. However, if you occasionally log in to different addresses and ports, or log in with different user names, the *Previous Logins* list lets you select your previously specified logins, in which case all you have to do is specify your password.

2. Click the *Login* link.

   After a short wait, the *Remote Client* window will open.

   The *Remote Client* window has three tabs: *Live*, *Browse* and *Setup*.

Remote Client's three tabs

The *Live* tab is used for viewing live images from cameras, the *Browse* tab is used for browsing recorded images from cameras, and the *Setup* tab is used for configuring the *Remote Client*.

Note: Depending on your user rights, you may not be able to access all three tabs.

If You Log In for the First Time

If you have logged in for the first time, you need to determine whether any *views* exist.

Views determine how images from cameras are displayed in the *Remote Client*, and are thus required in order to be able to use the *Remote Client*.

One or more views may already have been created for you, or you may need to create views yourself.

Read more about views, including how to determine if any views have already been created for you, in *Creating Views* on page 176.

Logging in on Different Computers

Your user settings are stored on the Milestone XProtect Enterprise server. This means that your login can be used on any computer that has a *Remote Client* installed.

Creating Views

The way in which images from one or more cameras are displayed in the *Remote Client* is called a *view*.

A view may contain images from up to 16 cameras. A *Remote Client* can handle an unlimited number of views, allowing you to switch between various collections of camera images.
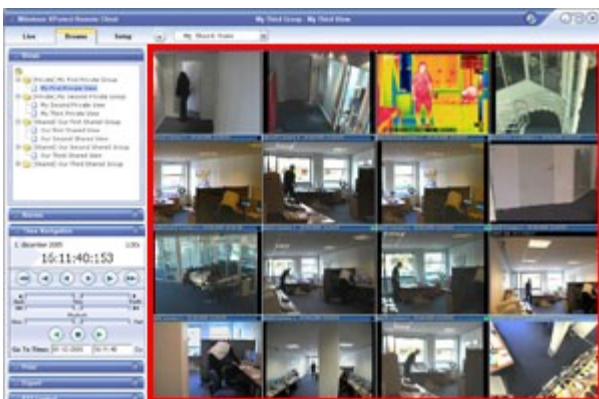
Example of a *Remote Client* displaying a view with images from
16 different cameras; the view is highlighted in red frame

Views/Groups Concept

In order to help you maintain an easy overview when you navigate between various views in your *Remote Client*, all views are placed in folders called *groups*. A group can contain any number of views.

Private and Shared Groups

Groups, in turn, can be *private* or *shared*. Views placed in private groups can only be accessed by the user who created them, whereas views placed in shared groups can be accessed by all *Remote Client* users connected to the Milestone XProtect Enterprise server.

Simplified example of *views* in
private and shared *groups*

Before you create any views, it is important that you know the difference between views placed in *shared* and *private* groups—not least because a number of views may already have been created and placed in shared groups for *Remote Client* users in your organization.

When that is the case, you can start using your *Remote Client* straight away; creating further views in your *Remote Client* will not be necessary unless you want to supplement the views in the shared groups with views of your own, placed in private groups.

If you want to create views yourself, for example if no views in shared groups are available in your organization, the *Remote Client*'s *Setup* tab lets you create groups and views, and specify which cameras should be included in each view.

Note: Particular user rights may be required in order to access the *Setup* tab. Your ability to create groups and views also depends on your user rights. From time to time your surveillance system administrator may make changes to camera or user properties on the Milestone XProtect Enterprise server. When this is the case, such changes will take effect in the *Remote Client* the first time you log in after the changes were made. Such changes may require you to re-create your views. Ask your surveillance system administrator if in doubt.

Are any Views in Shared Groups Available?

Especially if you are a first-time user of the *Remote Client*, you will want to know whether any views have already been created and placed in *shared* groups for your organization's *Remote Client* users.

Typically, your surveillance system administrator will have told you if shared groups are used in your organization.

Alternatively, to quickly determine whether any views have already been created and placed in shared groups, do the following:

Note: This method requires that your user rights permit you to access the *Remote Client*'s *Live* tab and/or *Browse* tab. Most users will have access to at least one of these tabs.

1. Go to the *Remote Client*'s *Live* or *Browse* tab.

2. On the *Live* or *Browse* tab, look at the *Views* section:

   - If the *Views* section contains any expandable folders labeled *[Shared] ...*, shared groups are available, and you may—your user rights permitting—begin using the views in the shared groups for viewing live and recorded images. See *Viewing Live Images* on page 191 and *Viewing Recorded Images* on page 194. Only if you want to add more views, e.g. customize your *Remote Client* with views in private groups, do you need to create further views on the *Setup* tab.

     Example of *Views* section containing shared groups with views

   - If the *Views* section contains no expandable folders at all, no views are available, and you must create at least one view on the *Setup* tab before you can begin using the *Remote Client*.

     Example of *Views* section containing no expandable folders

   - If the *Views* section contains one or more expandable folders labeled *[Private] ...*, you have already created one or more views in private groups.

Which Types of Groups Can You Create Views in?

Depending on your user rights, you may be able to create and edit views in the following types of groups:

- Private and shared

- Private, but not shared

- Shared, but not private

- None at all (in which case you simply rely on views created by others and placed in shared groups)

Typically only a few people in an organization are able to create and edit views in shared groups. For example, the surveillance system administrator may create and maintain a number of views and place them in shared groups: When *Remote Client* users log in, the views placed in the shared groups will automatically be available to them, and the users will basically not need to create further views unless they want their own views in *private* groups.

To quickly determine which types of groups your user rights permit you to create and edit views in, do the following:

1. Select the *Remote Client*'s *Setup* tab.

   Note: Particular user rights may be required in order to access the *Setup* tab. If you are not able to access the *Setup* tab, you are not able to create views.

2. On the *Setup* tab, look at the *Views* section:

   Group folders to which you do **not** have access will be indicated by padlock icons.

Example: The user is able to create and edit views in private groups, but not in shared groups. Note the padlock icon on the shared group folder.

Consult your system administrator if in doubt about your user rights.

Creating Views in Private Groups

To create your first view in a private group, you first create a group, and then create the required view within the group.

If you have created views in private groups before, you may create new views in existing private groups, or you may create a new private group for the view.

Note: Views are created on the *Remote Client*'s *Setup* tab. Particular user rights may be required in order to access the *Setup* tab.

Creating a Private Group

To create a private group, do the following on the *Setup* tab:

1. In the *Setup* tab's *Views* section, select the *[Private]* folder, or—if you have created private groups before—any folder labeled *[Private]*.

2. In the *Setup* tab's *Group Control* section, type a name for the group in the *Group Name* field, then click the *New* button.

Typing a name in *Setup* tab's *Group Control* section

Your new group will now appear in the *Setup* tab's *Views* section, with the name you have specified, and labeled as *[Private]*:

Newly created group appearing in *Views* section

You are now able to create a view within the group.

Creating a View in a Private Group

To create a view in a private group, make sure the group in which you want to create the view is selected in the *Setup* tab's *Views* section, and do the following:

1. In the *Setup* tab's *View Control* section, type a name for the view in the *View Name* field.

Typing a name in *Setup* tab's *View Control* section

2. Click one of the *View Control* section's seven available *New View* layouts:

Your new view is automatically added to the selected group:

Newly created view appearing under group

Tip: A group, whether private or shared, can contain an unlimited number of views. More than one private and shared group can exist.

Adding Cameras to the View

Having created a view within a group, you are able to specify which cameras should be included in the view.
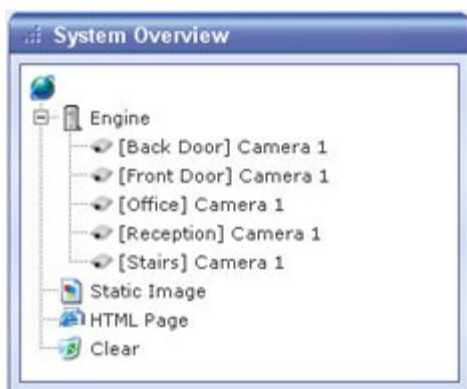
To add cameras to a view, do the following:

1. In the *Setup* tab's *Views* section, select the required view.

    When you select a view, the layout of the selected view is outlined in the main section of the *Remote Client* window.

    Layout of selected view is outlined in main section
    (indicated in red frame in this example)

2. In the *Setup* tab's *System Overview* section, click the plus sign ⊞ next to the required engine (server) to view a list of available cameras.

    Example: Engine with five available cameras

3. In the list, select a camera and drag the camera to the required position in the view.

    When you have dragged a camera to a position in the view, the name of the camera will appear in the selected position. You will not see images from the camera yet, as the *Setup* tab is only for configuration, not for viewing images.

    Repeat for each camera required in the view.

    Tip: If you want to use all of the cameras under an engine, you may simply drag the

required engine to the view; this will automatically place all of the engine's cameras in the view, beginning at the selected position. Remember to have sufficient positions available in the view.

i **Tip:** You can always change the cameras in your view: Either drag the *System Overview* section's *Clear* link to a position in the view to clear the position, or simply overwrite a position by dragging a different camera to the position.

4. You are now able to use your view: You may—your user rights permitting—select the view on the *Live* tab (see *Viewing Live Image*s on page 191) and on the *Browse* tab (see *Viewing Recorded Images* on page 194).

i **Tip:** In addition to cameras, you are able to add static images and HTML pages to views. See *Further Configuration* on page 185.

Creating Views in Shared Groups

To create view in a shared group, you first create a group, then create the required view within the group.

If you have created views in shared groups before, you may create new views in existing shared groups, or you may create a new shared group for the view.

Note: Views are created on the *Remote Client*'s *Setup* tab. Particular user rights may be required in order to access the *Setup* tab and in order to be able to create shared views. When creating a shared view, bear in mind that depending on their user rights not all users may have access to all cameras on the surveillance system.

Creating a Shared Group

To create a shared group, do the following on the *Setup* tab:

1. In the *Setup* tab's *Views* section, select the *[Shared]* folder, or—if you have created shared groups before—any folder labeled *[Shared]*.

2. In the *Setup* tab's *Group Control* section, type a name for the group in the *Group Name* field, then click the *New* button.

Typing a name in *Setup* tab's *Group Control* section

i **Tip:** Bear in mind that since the group is shared, it will also appear in other users' *Remote Clients*; therefore use a name which other users will immediately be able to understand.

Your new group will now appear in the *Setup* tab's *Views* section, with the name you have specified, and labeled as *[Shared]*:

Newly created group appearing in *Views* section

You are now able to create a view within the group.

Creating a View in a Shared Group

To create a view in a shared group, make sure the group in which you want to create the view is selected in the *Setup* tab's *Views* section, and do the following:

1. In the *Setup* tab's *View Control* section, type a name for the view in the *View Name* field.

Typing a name in *Setup* tab's *View Control* section

Tip: Bear in mind that since the view will appear in a shared group, it will also appear in other users' *Remote Clients*; therefore use a name which other users will immediately be able to understand.

2. Click one of the *View Control* section's seven available *New View* layouts:

Your new view is automatically added to the selected group:

Newly created shared view appearing under group

Tip: A group, whether private or shared, can contain an unlimited number of views. More than one private and shared group can exist.

Adding Cameras to the View

Having created a view within a group, you are able to specify which cameras should be included in the view.

Note: Bear in mind that depending on their user rights not all users may have access to all cameras on the surveillance system. Thus, even though you may be able to view images from all cameras in a shared view, other users may not necessarily be able to view images from all the cameras. Consult your surveillance system administrator if in doubt.

To add cameras to a view, do the following:

1. In the *Setup* tab's *Views* section, select the required view.

   When you select a view, the layout of the selected view is outlined in the main section of the *Remote Client* window.

   Layout of selected view is outlined in main section
   (indicated in red frame in this example)

2. In the *Setup* tab's *System Overview* section, click the plus sign ⊞ next to the required engine (server) to view a list of available cameras.

   Example: Engine with five available cameras

3. In the list, select a camera and drag the camera to the required position in the view.

   When you have dragged a camera to a position in the view, the name of the camera will appear in the selected position. You will not see images from the camera yet, as the *Setup* tab is only for configuration, not for viewing images.

   Repeat for each camera required in the view.

   ⓘ **Tip:** If you want to use all of the cameras under an engine, you may simply drag the required engine to the view; this will automatically place all of the engine's cameras in the view, beginning at the selected position. Remember to have sufficient positions available in the view.

Tip: You can always change the cameras in the view: Either drag the *System Overview* section's *Clear* link to a position in the view to clear the position, or simply overwrite a position by dragging a different camera to the position.

4. *Remote Client* users on your surveillance system will now able to access the view in the shared group as from their next login.

Tip: In addition to cameras, you are able to add static images and HTML pages to views. See *Further Configuration* in the following.

Using Your Views on Different Computers

Your user settings, including your private views, are stored on the Milestone XProtect Enterprise server. This means that you are able to use your private views on any computer that has a *Remote Client* installed, provided you log in to the *Remote Client* with your own user name and password.

Further Configuration

In addition to creation of groups and views, the *Remote Client*'s *Setup* tab lets you edit existing groups and views. The *Setup* tab furthermore lets you adjust camera settings, and set up joystick control for PTZ (Pan/Tilt/Zoom) cameras.

Note: Particular user rights may be required in order to access the *Setup* tab. Your ability to edit groups and views also depends on your user rights. Basically, if you are able to create groups and views, you are also able to edit them. From time to time your surveillance system administrator may make changes to camera or user properties on the Milestone XProtect Enterprise server. When this is the case, such changes will take effect in the *Remote Client* the first time you log in after the changes were made. Such changes may require you to re-create your views. Ask your surveillance system administrator if in doubt.

Which Type of Groups Can You Edit Views in?

Depending on your user rights, you may be able to create and edit views in the following types of groups:

- Private and shared

- Private, but not shared

- Shared, but not private

- None at all (in which case you simply rely on views created by others and placed in shared groups)

To quickly determine which types of groups your user rights permit you to create and edit views in, do the following:

1. Select the *Remote Client*'s *Setup* tab.

    Note: Particular user rights may be required in order to access the *Setup* tab. If you are not able to access the *Setup* tab, you are not able to create views.

2. On the *Setup* tab, look at the *Views* section:

Group folders to which you do **not** have access will be indicated by padlock icons.

Example: The user is able to create and edit views in private groups, but not in shared groups. Note the padlock icon on the shared group folder.

Consult your system administrator if in doubt about your user rights.

Using Static Images in Views

You are not limited to viewing camera images in a view; you are able to view static images (such as GIF or JPEG) as well.

Example: A company logo inserted as a static image (in this case viewed on the *Live* tab). The feature could equally well be used for inserting maps, floor plans, photos of wanted persons, etc.

To use a static image in a view, do the following on the *Setup* tab:

1. Drag the *System Overview* section's *Static Image* link to the required position in the view.

2. Release the mouse button over the required position.

   When you release the mouse button, the *Choose File* window opens, letting you select the required static image file.

Using HTML Pages in Views

In addition to viewing camera images and static images in a view, you are able to import HTML pages and display them in the view. This way, you are able to include company web pages, intranet pages, navigation pages, link collections, etc. together with the camera images in the view.

Example: A company web page inserted in a view (in this case viewed on the *Live* tab). The feature could equally well be used for inserting clickable maps, e-learning courses, etc.

Tip: When your imported HTML pages contain links, it is recommended that links have the `target='blank'` attribute. Example: `<a href="otherwebpage.htm" target="blank">Link</a>`. This will make the links open in separate windows, which will help you avoid losing view of the *Remote Client* window itself due to a link opening a web page in the same browser window as the *Remote Client*. This, however, does not apply if using an imported HTML page for navigation between the *Remote Client*'s *different* views; read more about this in *Using an HTML Page for Remote Client Navigation* on page 204.

To include an HTML page in a view, do the following:

1. Drag the *System Overview* section's *HTML Page* link to the required position in the view.

   When you release the mouse button over the required position, the *Import HTML Page* window opens:

   Import HTML Page window

2. In the *Import HTML Page* window's *Url* field, type the URL of the required HTML page (example: http://www.mywebsite.com/mywebpage.htm). Always include the *http://* prefix.

   - or -

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

3. In the *Title* field, you are able to specify a title for the HTML page. The title will appear in blue title bar above the HTML page itself when it is displayed in the view.

4. Select scaling for the HTML page, either *No scaling* (default) or the required scaling (640×480, 800×600, 1024×768 or 1280×1024).

5. Click the *OK* link.

Renaming Groups

To rename a group, do the following:

1. Select the required group in the *Views* section.

2. In the *Group Control* section, overwrite the existing name in the *Group Name* field.

3. Click the *Rename* button.

Deleting Groups

Note: Deleting a group will delete all views within the group as well.

To delete a group, do the following:

1. Select the required group in the *Views* section.

2. In the *Group Control* section, click the *Delete* button.

   You will be asked to confirm that you want to delete the group and all of its views.

Renaming Views

To rename a view, do the following:

1. Select the required view in the *Views* section.

2. In the *View Control* section, overwrite the existing name in the *View Name* field.

3. Click the *Rename* button.

Deleting Views

To delete a view, do the following:

1. Select the required view in the *Views* section.

2. In the *View Control* section, click the *Delete* button.

You will be asked to confirm that you want to delete the view.

Adjusting Camera Settings

In the *Setup* tab's *Camera Control* section, you are able to adjust camera settings. To adjust camera settings, select the position of the required camera in the view. The position you select will be indicated by a bold border.

Image Quality

The *Image Quality* setting determines the quality of the images when viewed, but also affects bandwidth usage. If the *Remote Client* is used over the internet, over a slow network connection, or if for other reasons you need to limit the bandwidth used by the *Remote Client*, image quality can be reduced on the server side by selecting e.g. *Low* or *Medium*

Tip: You can quickly reduce the bandwidth usage for all cameras in the view by reducing the image quality for a single camera, then clicking the *Apply To All* button.

Tip: If you have selected reduced image quality for a camera, images from the camera will be displayed in full quality when viewed enlarged (see *Enlarging Images from a Particular Camera* on page 192 and 195).

Frame Rate

The *Frame Rate* setting lets you select a frame rate for the selected camera. Default is *Unlimited*.

IPIX Split Mode

Available only if the selected camera is an IPIX camera. IPIX is a technology that allows creation and viewing of 360-degree panoramic images. The *Remote Client* supports up to four different viewpoints from a single IPIX camera. The IPIX Split Mode list lets you select the required spilt mode:

- *One by One* lets you view a single viewpoint.
- *Two by Two* lets you view four different viewpoints at a time.

When viewed on the *Live* and *Browse* tabs, the IPIX camera will appear as specified, with either one or four viewpoints from the same image:

Two by Two: Live tab displaying four different viewpoints from a single IPIX camera; in this example, the IPIX camera's four viewpoints are enlarged for clarity.

Tip: When viewing different viewpoints from an IPIX camera on the *Live* or *Browse* tabs, you are able to navigate each viewpoint independently by clicking inside each viewpoint, or by using the buttons in the *PTZ Control* section.

Apply to All

The *Apply To All* button lets you quickly apply the camera settings for the selected camera to all cameras in the view.

Configuring Joystick Control

The *Joystick Control* section lets you configure joystick control of PTZ (Pan/Tilt/Zoom) cameras. Joystick configuration control requires that a joystick is attached to the computer running the *Remote Client*.

Note: Even though joystick control is supported for a large number of PTZ cameras, not all PTZ cameras may be joystick-controlled. Refer to the release note for information about joystick support for cameras.

Click the *Joystick Control* section's *Setup...* button to access the *Joystick Setup* window.

The *Joystick Setup* window

The *Joystick Setup* window's *Joystick Axes* section lets you configure the axes used for the joystick.

With a joystick, you are typically able to navigate camera images three-dimensionally, along three axes: an X-axis, a Y-axis, and a Z-axis, where the Z-axis refers to the depth (zoom) level:
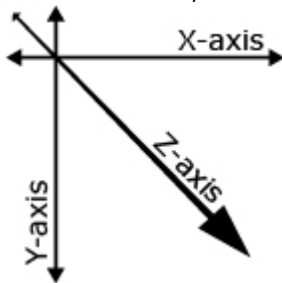
Example: X-, Y-, and Z-axes

Button, Check Box	Description
Invert y-axis	Lets you invert the Y-axis. This way, you are able to select whether the camera should move up or down when you move the joystick towards you and away from you respectively.

Z-axis uses a relative positioning scheme	Lets you specify whether the Z-axis should use a relative or an absolute positioning scheme. This will affect the way you zoom in and out with camera.
Default values	Resets axes settings, letting you use the joystick's default axes settings.

The *Joystick Buttons* section lets you specify which joystick buttons should be used for particular actions.

To assign an action to a particular joystick button, select the required action in the list, then click the required joystick button.

When a button is assigned to an action, the name of the button will be listed together with the name of the action.

To stop using a particular joystick button for a particular action, select the button/action in the list, then click the *Unselect* button.

To free all joystick buttons from their associated actions, click the *Unselect All* button.

Viewing Live Images

You view live images on the *Remote Client*'s *Live* tab.

When you select the *Remote Client*'s *Live* tab, the *Remote Client* will connect to the Milestone XProtect Enterprise server, and display live images from the cameras in the selected view.

Note: In order to view live images in the *Remote Client*, the *Monitor* application (see page 133) must be running on the Milestone XProtect Enterprise server; consult your surveillance system administrator if in doubt. Depending on your user rights, access to viewing live images from some cameras may be restricted.

The *Live* tab, in this example displaying a view with images from eight cameras

Selecting a View

You are able to select a view for display on the *Live* tab in two ways:

- By selecting the required view in the *Live* tab's *Views* section:

Detail from *Live* tab's *Views* section

- By selecting the required view from the *Views* list located in the upper part of the window:

Views list

Image Bars

Each camera in the view is identified by an image bar, located in the top of each camera image.

The image bar is blue. When you select a particular camera in the view, the image bar of the selected camera image becomes a lighter blue.

Camera image; enlarged detail shows image bar

The image bar displays the name of the camera as well as the name of the device to which the camera is connected. The device name is displayed first, in square brackets, followed by the camera name.
Each image bar will display the word *Live* when live images are displayed, and the word *Stopped* if the camera is stopped.

Each image bar features three colored indicators:

- *Event indicator (the leftmost of the three indicators, solid yellow)*: Lights up when specific events, defined by the surveillance system administrator, occur. Click anywhere inside the image to reset the event indicator. This indicator may appear black if event indication has not been specified for the camera in question, of if no specified events have occurred. Consult your surveillance system administrator if in doubt.

- *Motion indicator (the indicator in the middle, solid red)*: Lights up when motion is detected in the image. Click anywhere inside the image to reset the motion indicator.

- *Online indicator (the rightmost of the three indicators, blinking green)*: Changes state every time an image is received from the camera.

Enlarging Images from a Particular Camera

To enlarge images from a particular camera in a view, double-click the blue image bar above the image.

Double-clicking blue bar above image enlarges view

To return to normal view, simply double-click the blue image bar again.

Tip: If you have selected reduced image quality for the camera (on the *Setup* tab), images from the camera will be displayed in full quality when viewed enlarged.

Output Control

If the selected camera has external outputs defined, for example for switching on lights or sounding a siren, such outputs can be triggered from the *Remote Client*.

Note: Depending on your user rights, access to triggering outputs for some cameras may be restricted.

To trigger an output, first select the required camera in the view, then select the required output in the *Output Control* section, and click the *Fire* link.

Output Control section

PTZ Control

PTZ (Pan/Tilt/Zoom) and IPIX (technology allowing creation and viewing of 360-degree panoramic images) cameras can be controlled from the *Remote Client*.

Note: Depending on your user rights, access to PTZ controls from some cameras may be restricted.

Point-and-Click Control

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

Crosshairs indicate point-and-click control.
For some cameras, crosshairs may look different.

For some cameras, crosshairs surrounded by a square may be displayed. When this is the case, you are able to zoom in on an area by dragging a square around the required area in the image. For such cameras, zoom level is controlled by holding down the SHIFT key on your keyboard while moving the mouse up or down; this will display a zoom level slider inside the image.

PTZ Navigation Buttons

As an alternative to point-and-click PTZ control, use the navigation buttons in the *PTZ Control* section to move the selected PTZ or IPIX camera.

The round middle button lets you quickly move the camera to its home (i.e. default) position.

The *plus* and *minus* buttons lets you zoom in and out respectively.

PTZ Control section

PTZ Preset Positions

If preset positions have been defined for the selected PTZ camera, you are able to select such positions from the *Presets* list. Selecting a preset position from the list will make the PTZ camera move to the specified position.

Preset positions are defined by the system administrator; the *Presets* list will be empty if no preset positions have been defined for the selected PTZ camera.

Tip: You may be able to use a joystick for controlling your PTZ cameras. Joystick control is configured on the *Remote Client*'s *Setup* tab. See *Further Configuration* on page 185.

Note: Even though joystick and point-and-click control is supported for a large number of PTZ cameras, not all PTZ cameras may be controlled this way. Refer to the release note for information about joystick and point-and-click support for PTZ cameras.

IPIX PTZ Positions

You are able to move to a specific position in an IPIX view, and then save that position by clicking the *Save* button. When you later want to return to the saved position, click the *Load* button.

Viewing Recorded Images

You view recorded images on the *Remote Client*'s *Browse* tab.

When you select the *Remote Client*'s *Browse* tab, the *Remote Client* will connect to the Milestone XProtect Enterprise server, and display recorded images from the cameras in the selected view. This way, you are able to browse recorded images.

Note: Depending on your user rights, access to browsing images from some cameras may be restricted. Date and time formats used when browsing recorded images may vary depending on your computer's regional settings. Illustrations in this help topic, and date and time formats used in the illustrations, are thus for guidance only.

The *Browse* tab provides you with a number of advanced features for browsing recorded images. In addition to image browsing features, the *Browse* tab also lets you print images, and export AVIs (movie clips) and JPEGs (still images).

The *Browse* tab, in this example displaying a view with images from eight cameras

Selecting a View

You are able to select a view for display on the *Browse* tab in two ways:

- By selecting the required view in the *Browse* tab's *Views* section:

Detail from *Live* tab's *Views* section

- By selecting the required view from the *Views* list located in the upper part of the window:

Views list

Enlarging Images from a Particular Camera

To enlarge images from a particular camera in a view, double-click the blue title bar above the image.

Double-clicking blue bar above image enlarges view

To return to normal view, simply double-click the blue title bar again.

 Tip: If you have selected reduced image quality for the camera (on the *Setup* tab), images from the camera will be displayed in full quality when viewed enlarged.

Time Navigation

The *Browse* tab's *Time Navigation* section provides you with controls for browsing and playing back recorded images from the camera selected in the view.

Time Navigation section. Date and time format may be different on your computer.

Master Time

The *Time Navigation* section's *Master Time* area shows the master time and date of the recordings viewed. The master time is the time to which all the cameras viewed are tied. This means that when you browse recordings, all the images you see in the view will, in principle, be from exactly the same point in time.

Some cameras, however, may only record if motion is detected. Also, there may be no recorded images from one or more cameras in the view matching the specified point in time. When this is the case, the last image in the camera's database prior to the specified point in time will be displayed in the view.

Master Time area. Date and time format may be different on your computer.

The *Master Time* area also displays the current playback speed (example: 1.00x, indicating real-time).

Browse Buttons

The *Time Navigation* section's browse buttons lets you manually navigate through recordings from the camera selected in the view.

Browse buttons

Previous image: Moves to the image just before the one currently viewed

Next image: Moves to the image just after the one currently viewed

(I◄)	*Previous sequence*: Moves to the first image in the previous sequence
(►I)	*Next sequence*: Moves to the first image in the following sequence
(I◄◄)	*First image*: Moves to the first image in the database for the selected camera
(►►I)	*Last image*: Moves to the last image in the database for the selected camera

Time Sliders

The *Time Navigation* section's time sliders let you browse recordings simply by dragging the sliders' handles. Drag to the left to move backwards in time; drag to the right to move forward in time.

Use the upper times slider for fine browsing within a limited period of time; use the lower slider for coarser browsing within longer time spans.

Time sliders

Playback Slider and Buttons

The *Time Navigation* section's playback slider lets you specify the required playback speed. In the slider's middle position, playback speed is real-time (1.00x). Drag the slider to the left for a slower playback speed; drag to the right for a faster playback speed. An indication of the exact playback speed is displayed in the upper right corner of the *Time Navigation* section's *Master Time* area.

Playback slider and buttons

Use the playback buttons to play back recordings:

(◄)	*Play reverse*: Plays back recordings backwards in time
(►)	*Play forward*: Plays back recordings forward in time
(■)	*Stop*: Stops playback

Tip: Dragging the playback slider to its leftmost position pauses playback.

Go To Time

The *Time Navigation* section's *Go To Time* fields let you quickly jump to a specific point in time.
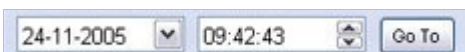
Go To Time fields. Date and time format may be different on your computer.

Specify required date in the first field and required time in the second field, then click the *Go To* link.

Sequences

The *Browse* tab's *Sequences* section provides you with an overview of recorded sequences for the camera selected in the view.

To use the *Sequences* section, select the required camera in the view, then click the *Sequences* section's *Get Sequences* button. Clicking the *Get Sequences* button will retrieve a list of up to 40 sequences: 20 sequences prior to the point in time displayed in the view, and 20 sequences following the point in time displayed in the view.

Each sequence will be listed with date and time as well as the length of the sequence. Clicking a sequence in the list will move all images in the view to the time the sequence.

If the *Preview* check box is selected, you are able to quickly view each sequence by placing the mouse pointer over the required sequence in the list:

Sequences section; placing mouse pointer over a sequence indication lets you
quickly view the incident. Date and time format may be different on your computer.

Clicking the *expand* icon ⊞ next to a sequence in the list will show you the exact date and time of the first and last image in the sequence as well as the exact date and time of the motion detection, event, etc. triggering the recording.

Sequences may often begin some seconds before a motion detection, event, etc. and end some seconds after. This so-called buffer allows you to be able to see what happens immediately before and after an incident; the buffer length is determined by the surveillance system administrator.

Detail from *Sequences* section, showing
expanded sequence indication. Date
and time format may be different on
your computer.

PTZ Control

The Browse tab's PTZ Control section lets you navigate recorded images from IPIX cameras (IPIX is a technology allowing creation and viewing of 360-degree panoramic images).

Note: The *Browse tab's PTZ Control section* cannot be used for controlling PTZ (Pan/Tilt/Zoom) cameras, as the *Browse* tab is used for viewing already recorded images.

Navigation by Dragging Inside IPIX Images

Many IPIX images may be navigated simply by dragging inside the images.

If your mouse pointer changes to ⊕ or similar when placed over an image from an IPIX camera, navigation by dragging is supported for the camera.

Refer to the release note for information about point-and-click support.

PTZ Navigation Buttons

As an alternative to navigation by dragging inside IPIX images, use the navigation buttons in the *PTZ Control* section to move around the view from the selected IPIX camera.

The round middle button lets you quickly move the camera to its home (i.e. default) position.

The *plus* and *minus* buttons lets you zoom in and out respectively.

PTZ Control section

Presets

The *Presets* list does not apply for navigating recorded images from IPIX cameras.

IPIX PTZ Positions

You are able to move to a specific position in the IPIX view, and then save that position by clicking the *Save* button. When you later want to return to the saved position, click the *Load* button.

Printing Images

With the *Browse* section's *Print* section, you are able to print recorded images.

Print section

To print an image, do the following:

1. Select the required camera from the *Print* section's *Source* list. Alternatively, you may select the camera in the view.

2. Select the required date and time by using the controls in the *Time Navigation* section.

3. Click the *Print* section's *Print* button.

   This will open a separate window with a preview of the image to be printed as well as information about camera name, image capture time, print time and user name of the user printing the image.

   You also have the option of including a user's note, for example a description of the recording.
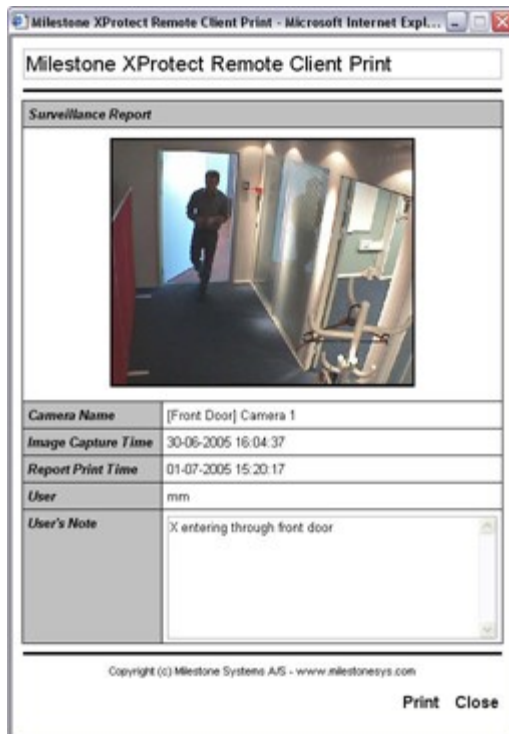
Window with preview and information about printed image

4. Click the separate window's *Print* link to print the image and associated details.

Exporting Images

With the *Browse* section's *Export* section, you are able to export recorded images in the AVI (movie clip) and JPEG (still image) formats.
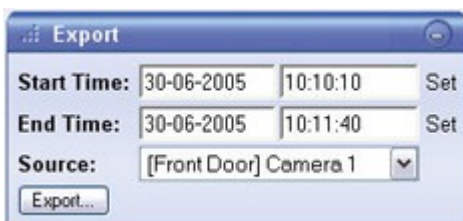
Export section. Date and time format may be different on your computer.

See *How to Export Video Evidence in AVI and JPEG Formats* in the following for detailed information about exporting recorded images.

How to Export Video Evidence in AVI and JPEG Formats

With the *Remote Client* you are able to quickly generate and export video evidence in the AVI (movie clip) and JPEG (still image) formats.

Note: Depending on your user rights, access to generating AVI or JPEG evidence from some cameras may be restricted.

Date and time formats used when browsing recorded images may vary depending on your computer's regional settings. Illustrations in this help topic, and date and time formats used in the illustrations, are thus for guidance only.

To export video evidence, do the following:

1. Select the *Remote Client*'s *Browse* tab.

2. In the *Browse* tab's *Export* section, specify start date and time for the export by typing the date in the first *Start Time* field and the time in the second field.

    Export section. Date and time format may be different on your computer.

     Tip: Instead of manually specifying date and time, you may use the *Browse* tab's *Time Navigation* features to move to the required start point, then click the upper of the *Export* section's *Set* links. This will automatically set the date and time of the viewed image into the *Start Time* fields.

3. In the *End Time* fields, specify end date and time for the export.

    As was the case with the start date and time, end date and time must be in the correct format if specified manually.

    Alternatively, use the *Set* link as described above.

4. Select the required camera from the *Source* list.

5. Click the *Export* button.

    This will open an export dialog, listing the specified start time, end time, and camera:

Export dialog. Date and time format may be different on your computer.

6. In the export dialog, select the required export format: *AVI* (movie clip) or *JPEG* (still images).

7. Select whether to add timestamps from the surveillance system to the exported images. If selected, timestamps will appear in the corner of the images:

Timestamps; arrow indicates actual position. Date and time format may be different on your computer.

8. ***This step applies for export in the AVI format only; if using the JPEG format, go to step 11***
Select required frame rate for the export. With the *Full* option, all images between the start and end times will be included in the export; with the *Half* option, only every second image will be included, yet still play back in real-time.

9. ***This step applies for export in the AVI format only; if using the JPEG format, go to step 11***
In the *AVI Codec* list, select required AVI codec. The list will contain the video codecs available on your computer.

A video codec is a particular compression/decompression technology used when generating video files. Your choice of codec will affect the quality and size of the AVI file.

i **Tip:** The Indeo® video 5.10 codec, if available on your computer, generally provides a very good compromise between quality and file size.

10. ***This step applies for export in the AVI format only; if using the JPEG format, go to step 11***
By default, the AVI file will get a file name based on the export start time, along the structure yyyymmddhhmmss.avi (year, month, day, hour, minute, second; example: 20050630160430 for a file with a start time of 16:04:30 on 30th June 2005). The name will automatically appear in the *AVI File Name* field.

The default file name format is independent of regional settings on your computer.

You are always able to change the default file name to a name of your choice, simply by overwriting the default file name. Remember that the file name *must* include the .avi file extension.

11. Specify export destination.

If you select *Desktop*, your exported file will be saved in an automatically created *Exported Images* folder on the desktop of your computer.

If you select *Path*, you are able to specify a path yourself. The exported file will be saved in an automatically created *Exported Images* folder under the path you specify (example: If you specify a path like C:\My Stuff\My Files, the exported file will be saved in C:\My Stuff\My Files\Exported Images).

When specifying a path this way, the folders you specify do not have to be existing ones; if they do not already exist, they will be created automatically.

12. Click the *Export* link to begin the export.

The status bar in the upper part of the export dialog will display the status of the export:
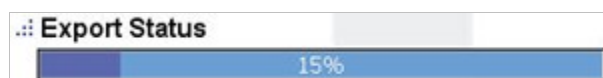
.:: Export Status
15%

Export status bar

i **Tip:** If you are exporting very long sequences, export may—depending on your selected export settings—take a while. You can continue to use the *Remote Client* for other purposes while the export process is underway.

If the *Close On Completion* check box is selected (default), the export dialog will automatically close when the export is finished.

Upon completion, you are able to view and distribute the exported file.

Keyboard Shortcuts

You are able to use the following keyboard shortcuts in the *Remote Client*:

On All Tabs

CTRL+1	Go to *Live* tab
CTRL+2	Go to *Browse* tab
CTRL+3	Go to *Setup* tab
CTRL+DOWN ARROW	Go to the next view in the *Views* list (located in the upper part of the window)
CTRL+UP ARROW	Go to the previous view in the *Views* list (located in the upper part of the window)

On Live Tab Only

PLUS SIGN	PTZ camera, zoom in
MINUS SIGN	PTZ camera, zoom out
UP ARROW	PTZ camera, move up
DOWN ARROW	PTZ camera, move down
LEFT ARROW	PTZ camera, move left
RIGHT ARROW	PTZ camera, move right
HOME (numeric keypad only)	PTZ camera, move up and left
END (numeric keypad only)	PTZ camera, move down and left
PAGE UP (numeric keypad only)	PTZ camera, move up and right
PAGE DOWN (numeric keypad only)	PTZ camera, move down and right
5 (numeric keypad only)	PTZ camera, move to default position

On Browse Tab Only

RIGHT ARROW	Move to next image
LEFT ARROW	Move to previous image
PAGE DOWN	Move to next sequence
PAGE UP	Move to previous sequence
HOME	Move to first image
END	Move to last image

Using an HTML page for Remote Client Navigation

In addition to displaying images from cameras, the *Remote Client* is able to display HTML pages and static images. This provides a high degree of flexibility as such HTML pages may be used for intuitively switching between different views in the *Remote Client*. For example, you may insert a clickable floor plan of a building, and you would be able to simply click a part of the floor plan to instantly switch to a view displaying images from the required part of the building.

In the following, you will see examples of HTML pages for *Remote Client* navigation: a simple HTML page with buttons, and a more advanced HTML page with a clickable image map. For Milestone XProtect Enterprise system administrators wishing to create and distribute such HTML pages to *Remote Client* users, a check list outlining the tasks involved is also provided.

Note: The method described here requires that you run a locally installed version of the *Remote Client*, and that the HTML page to be imported and used for navigation is also stored locally on your computer.

Creating a Simple HTML Page with Button Navigation

A very quick solution is to create an HTML page with buttons for navigation.
You are able to create five categories of buttons on the HTML page:

Buttons for Switching between Remote Client's Views

Required HTML syntax:

```
<input type="button" value="Buttontext" onclick="top.changeView('Groupname',
'Viewname');">
```

Buttons for Switching between Remote Client's Three Tabs

Note: Bear in mind that, depending on their user rights, some users may not be able to access all three tabs.

Required HTML syntax:

Switch to *Live* tab:
`<input type="button" value="Buttontext" onclick="top.selectPane('live');">`

Switch to *Browse* tab:
`<input type="button" value="Buttontext" onclick="top.selectPane('browse');">`

Switch to *Setup* tab:
`<input type="button" value="Buttontext" onclick="top.selectPane('setup');">`

Buttons for Hiding/Showing Remote Client's Navigation Pane

Required HTML syntax:

Hiding:
`<input type="button" value="Buttontext" onclick="top.showPane(false);">`

Showing:
`<input type="button" value="Buttontext" onclick="top.showPane(true);">`

Buttons for Hiding/Showing Remote Client's Title Bar

Required HTML syntax:

Hiding:
```
<input type="button" value="Buttontext" onclick="top.showTopTitle(false);">
```

Showing:
```
<input type="button" value="Buttontext" onclick="top.showTopTitle(true);">
```

Buttons for Switching to a Particular Time in Time Navigation

Required HTML syntax:

```
<input type="button" value="Buttontext" onclick="top.setTime('Mmm dd yyyy
hh:mm:ss');">
```

Example of an HTML Page with Buttons

In the following example we have created two shared groups in the *Remote Client*. We have called them *[Shared] Group1* and *[Shared] Group2*. Each group contains two views, called *View1* and *View2*:

Two groups, each containing two views

We have also created an HTML page with examples of all available button types, including the ability to switch between our four different views. The HTML for the page looks like this:

```
<html>
<body>
<input type="button" value="Change to: Group1-View1"
onclick="top.changeView('[Shared] Group1', 'View1');"><br>
<input type="button" value="Change to: Group1-View2"
onclick="top.changeView('[Shared] Group1', 'View2');"><br>
<input type="button" value="Change to: Group2-View1"
onclick="top.changeView('[Shared] Group2', 'View1');"><br>
<input type="button" value="Change to: Group2-View2"
onclick="top.changeView('[Shared] Group2', 'View2');"><br>
<input type="button" value="Live" onclick="top.selectPane('live');"><br>
<input type="button" value="Browse" onclick="top.selectPane('browse');"><br>
<input type="button" value="Setup" onclick="top.selectPane('setup');"><br>
<input type="button" value="Show pane" onclick="top.showPane(true);"><br>
<input type="button" value="Hide pane" onclick="top.showPane(false);"><br>
<input type="button" value="Show top title" onclick="top.showTopTitle(true);"><br>
<input type="button" value="Hide top title" onclick="top.showTopTitle(false);"><br>
<input type="button" value="Set time to New Year's Eve" onclick="top.setTime('Dec
31 2004 23:59:50');"><br>
</body>
</html>
```

Tip: You may copy the HTML, and modify it for an HTML page of your own.

When viewed in a browser, our HTML page looks like this:
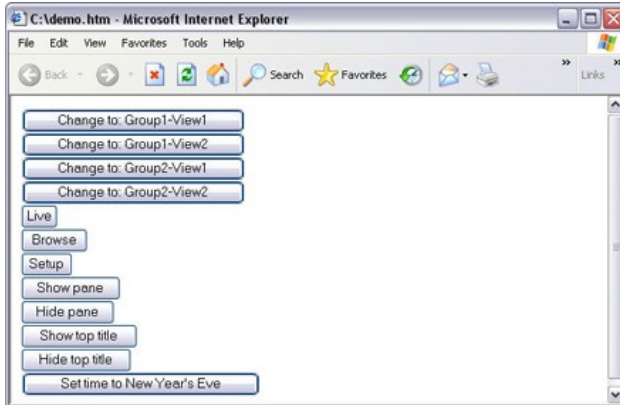
HTML page with buttons for navigating between views

We have saved the HTML page locally, on the C: drive.

When the HTML page is to be used for navigation, saving the HTML page locally is necessary because of security features in Internet Explorer.

When the HTML page is saved locally, a locally installed *Remote Client* will always be able to display it.

Using an HTML Page with Image Map Navigation

You may also create an HTML page with more advanced content, for example an image map allowing users to switch between views.

Example of an HTML Page with an Image Map

In the following example we have kept the *Remote Client* groups and views from the previous example.

Instead of using buttons, we have created an HTML page with an image of a floor plan, and created an image map based on the floor plan.

Viewed in a browser, our HTML page looks like this:
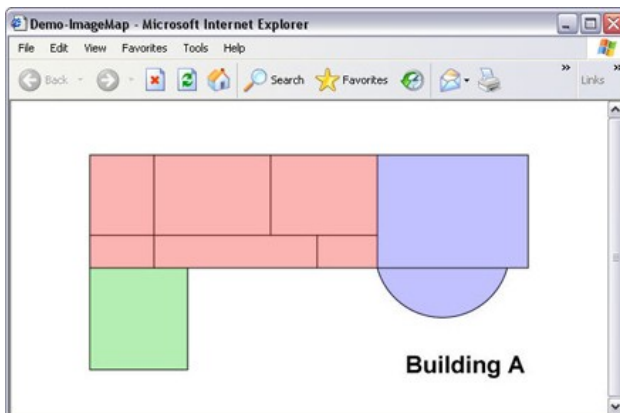
HTML page with image map for navigating between views

How you structure an image map is of course highly individual.

For this example, we divided the floor plan into colored zones, and defined an image map area for each zone.
This way, you will be able to simply click a zone in order to go to the view containing cameras from that zone.

For instance, the red zone on our image map mirrors the *Change to: Group2-View2* button from the previous example: When clicking the red zone, you will go to View2 in Group2.

When used in one of our *Remote Client* views, the HTML page looked like this:
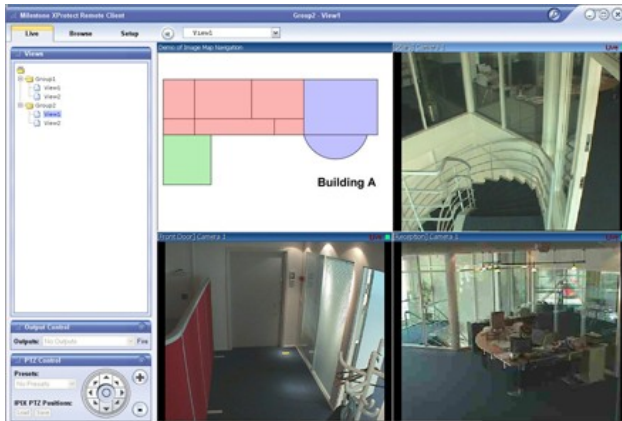
Example of HTML page with clickable floor plan imported into a view

Importing the HTML Page

Importing an HTML page for navigation is no different from importing any other type of HTML page into a view in the *Remote Client*.

The important thing to remember is that the HTML page should be stored locally on your computer.

To import an HTML page, go to the *Remote Client*'s *Setup* tab.

From the *setup* tab's *System Overview* section, drag the *HTML Page* link to the required position in the required view.
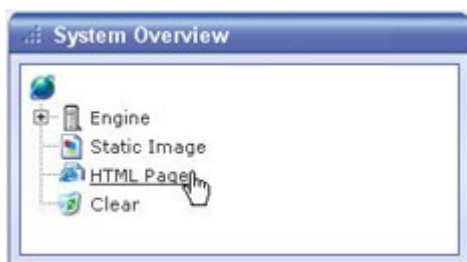
Click and drag *HTML Page* link to required position in view

This will open the *Import HTML Page* window, in which you specify the required HTML page.

You are also able to specify a title for it; the title will appear in the title bar of the HTML page when displayed in the view.

Depending on the navigation features you have included on your HTML page, you may often want to import the HTML page into several views in order for the navigation to fully work.

System Administrator's Check List

Milestone XProtect Enterprise system administrators wishing to create and distribute such HTML pages to *Remote Client* users, do the following:

1. **Create** the required HTML page.

   The navigation controls in the HTML page must match the views users see in their *Remote Clients.*

   For example, in order for a button leading to View2 to work, a view called View2 must exist.

   If you intend to distribute a navigation HTML page to a group of users, it is highly recommended that the views in which the HTML page will be used are placed in shared groups.

2. **Save** the HTML page locally on each computer on which it will be used.

   When saving the HTML page locally, save it at a location to which an unambiguous path can be defined, for example in a folder on the user's C: drive (example: C:\myfolder).

   Saving the HTML page on the user's desktop or in the user's *My Documents* folder will not work properly due to the way Windows constructs the path to such locations.

3. **Verify** that the *Remote Clients* in which the HTML page will be used are locally installed versions.

   If not, download and install the *Remote Client* software on each computer on which the HTML page will be used.

4. **Import** the HTML page into the *Remote Client* views in which it will be used.

5. **Test** that the navigation controls on the imported HTML page work as intended.

6. **Enjoy** simple and intuitive *Remote Client* navigation, tailored to meet your organization's needs.

Logging Out of the Remote Client

To log out of the *Remote Client*, simply click the *Log Out* button in the *Remote Client*'s top bar:

Log Out button

Smart Client

About the Smart Client

The *Smart Client* provides remote users with extremely feature-rich access to the surveillance system. It lets users access multiple servers at a time, allowing remote user access across systems.

Example of the *Smart Client*, displaying images from 16 cameras

The *Smart Client* must be installed locally on the remote user's computer.

DirectX 9.0 and .Net Framework 1.1 are required on computers running the *Smart Client*; both are available from http://www.microsoft.com/downloads/.

What are Remote Users Able to do with the Smart Client?

With the *Smart Client*, remote users are able to:

- View live images from cameras on the surveillance system.

- Browse recordings from cameras on the surveillance system.

- Create and switch between an unlimited number of views, each able to display images from up to 16 cameras from multiple servers at a time. Views can placed in *private* groups (only accessible by the user who created them) or *shared* groups (accessible by all *Smart Client* users connected to the Milestone XProtect Enterprise server).

- Use HTML pages and static images in views.

- Control PTZ (Pan/Tilt/Zoom) and IPIX (360° view) cameras.

- Activate manually triggered events.

- Activate external outputs.

- Get quick overviews of sequences with detected motion.

- Get quick overviews of detected events.

- Quickly search selected areas of camera images for motion.

- Print images.

- Generate and export evidence in AVI (movie clip) and JPEG (still image) formats.

- Assign keyboard shortcuts to common actions.

How does the Smart Client get Images from the Surveillance System?

Images viewed by *Smart Client* users are provided by the *Image Server*. The *Image Server* runs as a service on the Milestone XProtect Enterprise server; it does not require separate hardware. The Milestone XProtect Enterprise system administrator uses the *Image Server Administrator* window (see page 162) to manage *Smart Clients'* access to the surveillance system.

How can User Rights Affect Use of the Smart Client?

The rights of individual remote users are specified centrally by the surveillance system administrator. The rights of an individual user will determine the user's ability to use the *Smart Client*'s features.

Basically, the surveillance system administrator is able to restrict a user's rights to the following:

- Access to the *Smart Client*

- Access to each of the *Smart Client*'s tabs: *Live*, *Browse* and *Setup*

- Ability to use features on the *Smart Client*'s tabs

- Ability to create views (views determine the way in which images from one or more cameras are displayed)

- Ability to view images from specific cameras

The ability to use various features of the *Smart Client* may therefore vary considerably from user to user. Ask your surveillance system administrator if in doubt about your user rights.

How Does the Smart Client Differ from the Remote Client?

For a description of how the *Remote Client* differs from the *Smart Client*, see *Remote Access Overview* on page 157.

Downloading and Installing the Smart Client

The *Smart Client* must be installed on your computer before you are able to use it.

Typically, you download the *Smart Client* from the Milestone XProtect Enterprise server, and then install it on your computer. Alternatively, your surveillance system administrator may ask you to install the *Smart Client* from a CD.

To download and install the *Smart Client*, do the following:

1. Open an Internet Explorer browser (version 6.0 or later), and connect to the URL or IP address specified by your system administrator in order to connect to the Milestone XProtect Enterprise server. When you connect to the Milestone XProtect Enterprise server, you will see a welcome page.

2. In the *XProtect Smart Client* section of the welcome page, click the *Download and install XProtect Smart Client locally* link:

Detail from welcome page; arrow indicates *Download And install XProtect Smart Client locally* link

3. Depending on your security settings, you may receive a security warning (*Do you want to run or save this file?*).

   When this is the case, click the *Run* button.

4. Depending on your security settings, you may receive a further security warning (*Do you want to run this software?*).

   When this is the case, click the *Run* button.

5. The *Smart Client Setup Wizard* begins.

   In the wizard, click *Next* and follow the installation instructions.

Installing the Smart Client from a CD

To install the *Smart Client* from a CD, do the following:

1. Insert the Milestone XProtect Enterprise software CD, and run the file *Smart Client* installation file (*MilestoneXProtectSmartClient.exe*) from the CD.

2. When the installation wizard starts, click *Next* to continue the installation and follow the steps in the installation wizard.

Logging In to the Smart Client

Logging in to the *Smart Client* is very straightforward. So is the initial configuration of the *Smart Client* upon your first login; in fact, configuration may in some cases not be required at all.

To log in to the *Smart Client*, do the following:

1. Double-click the *Smart Client* shortcut on your desktop:

   Milestone
   Smart Client

   If no *Smart Client* desktop shortcut is available, select the *Smart Client* from Windows' *Start* menu (exactly how you do this is determined by where and how you have installed the *Smart Client* on your computer, but you would typically select *Start > All Programs > Milestone XProtect Smart Client > Smart Client*).

2. A splash screen is displayed while the *Smart Client* loads.

   Loading the *Smart Client* typically takes a few seconds only.

3. The *Smart Client* login window appears:

   XProtect Smart Client Log On

   milestone
   IP Video Surveillance

   Enter or select the server you wish to connect to.
   Connect to:

   Enter your log on information.
   Username:
   Password:

   OK   Cancel

   The *Smart Client* login window

4. Specify your login information in the following fields:

   - *Connect to*: Type the URL or IP address specified by your surveillance system administrator. Internet connections may use different ports for different purposes; therefore, the URL or IP address may include a port number, in most cases port 80 (example: 123.123.123.123:80, where :80 indicates the port number). If you have logged in before, you may simply select the required server from the *Connect to* list.

   - *Username*: Type your user name as specified by your system administrator. The user name is case-sensitive, i.e. there is a difference between typing, for example, *amanda* and *Amanda*.

   - *Password*: Type your password as specified by your system administrator. The password is case-sensitive.

5. Click *OK*.

6. After a short wait, the *Smart Client* window will open.

    The *Smart Client* window has three tabs: *Live*, *Browse* and *Setup*:

    The *Live* tab is used for viewing live images from cameras, the *Browse* tab is used for browsing recorded images from cameras, and the *Setup* tab is used for configuring the *Smart Client*.

    Note: Depending on your user rights, you may not be able to access all three tabs.

If You Log In for the First Time

If you have logged in for the first time, you need to determine whether any *views* exist. Views determine how images from cameras are displayed in the *Smart Client*, and are thus required in order to be able to use the *Smart Client*.

One or more views may already have been created for you, or you may need to create views yourself. Read more about views, including how to determine if any views have already been created for you, in the following.

Logging in on Different Computers

Your user settings are stored on the Milestone XProtect Enterprise server. This means that your login can be used on any computer that has a *Smart Client* installed.

Creating Views

The way in which images from one or more cameras are displayed in the *Smart Client* is called a *view*. A view may contain images from up to 16 cameras. A *Smart Client* can handle an unlimited number of views, allowing you to switch between various collections of camera images.
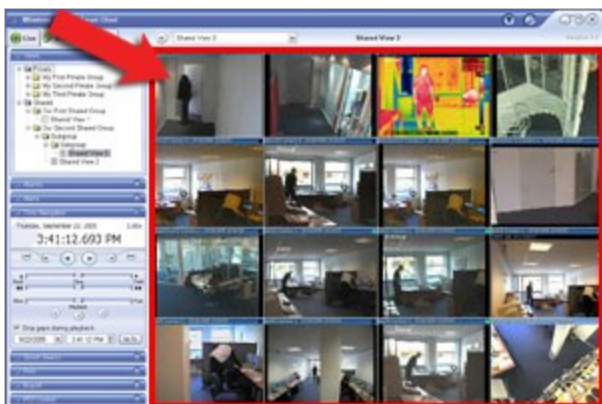
Example of a *Smart Client* displaying a view with images from 16 different cameras (the view is highlighted in red frame)

Views/Groups Concept

In order to help you maintain an easy overview when you navigate between various views in your *Smart Client*, all views are placed in folders called *groups*.

A group can contain any number of views and, if required, subgroups.

Private and Shared Groups

Groups, in turn, can be *private* or *shared*. Views placed in private groups can only be accessed by the user who created them, whereas views placed in shared groups can be accessed by all *Smart Client* users connected to the Milestone XProtect Enterprise server.
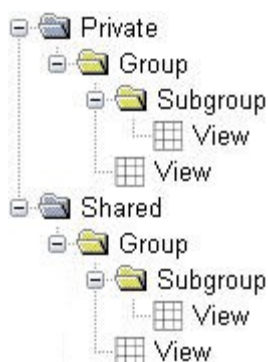
Simplified example of *views* in
private and shared *groups*

Before you create any views, it is important that you are sure about the difference between views placed in *shared* and *private* groups—not least because a number of views in shared groups may already have been created for *Smart Client* users in your organization.

When that is the case, you can start using your *Smart Client* straight away; creating further views in your *Smart Client* will not be necessary unless you want to supplement the views in the shared groups with views of your own, placed in private groups.

If you want to create views yourself, for example if no views in shared groups are available in your organization, the *Smart Client*'s *Setup* tab lets you create groups and views, and specify which cameras should be included in each view.

Note: Particular user rights may be required in order to access the *Setup* tab. Your ability to create groups and views also depends on your user rights. From time to time your surveillance system administrator may make changes to camera or user properties on the Milestone XProtect Enterprise server. When this is the case, such changes will take effect in the *Smart Client* the first time you log in after the changes were made. Such changes may require you to re-create your views. Ask your surveillance system administrator if in doubt.

Are Any Views in Shared Groups Available?

Especially if you are a first-time user of the *Smart Client*, you will want to know whether any views have already been created and placed in *shared* groups for your organization's *Smart Client* users.

Typically, your surveillance system administrator will have told you if views in shared groups are used in your organization.

Alternatively, to quickly determine whether any views have already been created and placed in shared groups, do the following:

Note: This method requires that your user rights permit you to access the *Smart Client*'s *Live* tab and/or *Browse* tab. Most users will have access to at least one of these tabs.

1. Go to the *Smart Client*'s *Live* or *Browse* tab.

2. On the *Live* or *Browse* tab, look at the *Views* section:

   - If the *Views* section contains any folders under the *Shared* folder, shared groups are available.

   Example of *Views* section containing shared groups with a number of views

   When this is the case you may—your user rights permitting—immediately begin using the views in the shared groups for viewing live and recorded images. See *Viewing Live Images* on page 232 and *Viewing Recorded Images* on page 236. Only if you want to add more views, e.g. customize your *Smart Client* with views in private groups, do you need to create further views on the *Setup* tab.

   - If the *Views* section contains only the two top-level folders, *Private* and *Shared*, without any content in any of the two folders, no views are available.

   Example of *Views* section containing no expandable folders

   In this case, you must create at least one view on the *Setup* tab before you can begin using the *Smart Client*.

   - If the *Views* section contains one or more expandable folders labeled *[Private] ...*, you have already created one or more views in private groups.

Which Types of Groups Can You Create Views in?

Depending on your user rights, you may be able to create and edit views in the following types of groups:

- Private and shared

- Private, but not shared

- Shared, but not private

- Neither private, nor shared (in which case you simply rely on views created by others and placed in shared groups)

Typically only a few people in an organization are able to create and edit views in shared groups.

For example, the surveillance system administrator may create and maintain a number of views and place them in shared groups: When *Smart Client* users log in, the views placed in the shared groups will automatically be available to them, and the users will basically not need to create further views unless they want their own views in *private* groups.

To quickly determine which types of groups your user rights permit you to create and edit views in, do the following:

1. Select any of the *Smart Client*'s tabs.

2. Look at the *Views* section: You are able to create and edit views in any groups **not** marked by a padlock icon. If a group is marked by a padlock icon, it is protected: You can still use any views in the group, but you cannot create or edit views in the group.

   Example: The user is able to create and edit views in private groups, but not in shared groups. Note the padlock icon on the shared group folder (clearly visible in the enlarged example).

   Consult your system administrator if in doubt about your user rights.

Creating Views in Private Groups

To create your first view in a private group, you first create a group under the *Private* top-level group, and then create the required view within the group. If you have created views in private groups before, you may create new views in existing private groups, or you may create a new private group for the view.

Note: Views are created on the *Smart Client*'s *Setup* tab. Particular user rights may be required in order to access the *Setup* tab.

Creating a Private Group

To create a private group, do the following on the *Setup* tab:

1. In the *Setup* tab's *Views* section, select the group under which you wish to create the new group. This may be the top-level *Private* group, or it may be a group under the top-level *Private* group.

   Example: Selecting the top-level *Private* group

2. Click the *Create New Group* button:

3. A new group is created under the group you selected. The new group is simply named *New Group*:

Example: A new group is created

4. Overwrite the default name *New Group* with a group name of your choice:

Example: Overwriting default group name

You are now able to create a view within the group.

Creating a View in a Private Group

To create a view in a private group, do the following:

1. In the *Setup* tab's *Views* section, make sure the group in which you want to create the view is selected:

Example: Selecting required group

2. Click the *Create New View* button:

3. Select the required layout for your new view:

Tip: Layouts marked *Wide* are particularly suited for widescreen monitors.

4. A new view is created under the group you selected. The new view carries the default name *New View* plus an indication of the selected layout:

Example: A new view is created

5. Overwrite the default name with a view name of your choice:

Example: Overwriting the default view name

You are now able to add cameras to the view.

Tip: A group, whether private or shared, can contain an unlimited number of views. More than one private and shared group can exist.

Creating Views in Shared Groups

To create your first view in a shared group, you first create a group under the *Shared* top-level group, and then create the required view within the group. If you have created views in shared groups before, you may create new views in existing shared groups, or you may create a new shared group for the view.

Note: Views are created on the *Smart Client*'s *Setup* tab. Particular user rights may be required in order to access the *Setup* tab. When creating a shared view, bear in mind that depending on their user rights not all users may have access to all cameras on the surveillance system.

Creating a Shared Group

To create a shared group, do the following on the *Setup* tab:

1. In the *Setup* tab's *Views* section, select the group under which you wish to create the new group. This may be the top-level *Shared* group, or it may be a group under the top-level *Shared* group.

Example: Selecting the top-level *Shared* group

2. Click the *Create New Group* button:

3. A new group is created under the group you selected. The new group is simply named *New Group*:

Example: A new group is created

4. Overwrite the default name *New Group* with a group name of your choice:

Example: Overwriting default group name

You are now able to create a view within the group.

Creating a View in a Shared Group

To create a view in a shared group, do the following:

1. In the *Setup* tab's *Views* section, make sure the group in which you want to create the view is selected:

Example: Selecting required group

2. Click the *Create New View* button:

3. Select the required layout for your new view:

Tip: Layouts marked *Wide* are particularly suited for widescreen monitors.

4. A new view is created under the group you selected. The new view carries the default name *New View* plus an indication of the selected layout:

Example: A new view is created

5. Overwrite the default name with a view name of your choice:

Example: Overwriting the default view name

You are now able to add cameras to the view.

Tip: A group, whether private or shared, can contain an unlimited number of views. More than one private and shared group can exist.

Adding Cameras to a View

Having created a view within a group, you can specify which cameras to include in the view.

Note: Bear in mind that depending on their user rights not all users may have access to all cameras on the surveillance system. Thus, even though you may be able to view images from all cameras in a shared view, other users may not necessarily be able to view images from all the cameras. Consult your surveillance system administrator if in doubt.

To add cameras to a view, do the following:

1. In the *Setup* tab's *Views* section, select the required view.

   When you select a view, the layout of the selected view is outlined in the main section of the *Smart Client* window.
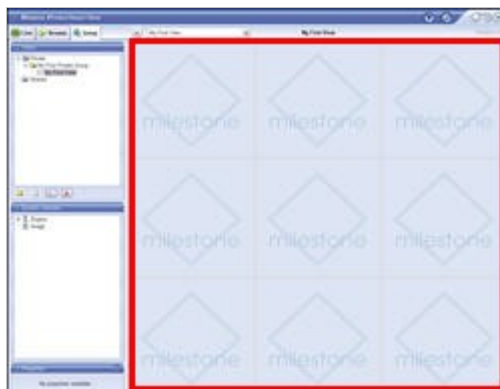
Layout of selected view is outlined in main section (indicated in red frame in this example)

2. In the *Setup* tab's *System Overview* section, click the plus sign ⊞ next to the required engine (server) to view a list of available cameras:
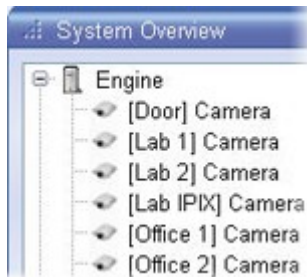
Example: Engine with a number of available cameras

3. Click the name of a camera, and drag the camera name to the required position in the view.

When you have dragged a camera to a position in the view, an image from the camera will—provided a connection can be established—appear in the selected position.

If a connection cannot be established, for example if the surveillance system's *Monitor* application is not running, the name of the camera will be displayed in the selected position.

Repeat for each camera required in the view.

Tip: If you want to use all of the cameras under an engine, you may simply drag the required engine link to the view; this will automatically place all of the engine's cameras in the view *from the selected position onwards*. Remember to have sufficient positions available in the view.

Tip: You can easily change the cameras in your view: Either clear the position by clicking the clear button ⊠, then drag another camera to the cleared position, or simply "overwrite" a position by dragging a different camera to the position.

4. You are now able to use your view: You may—your user rights permitting—select the view on the *Live* tab (see *Viewing Live Images* on page 232) and on the *Browse* tab (see *Viewing Recorded Images* on page 236).

Tip: In addition to cameras, you are able to add static images and HTML pages to views. Read more in *Further Configuration* on page 223.

Using Your Views on Different Computers

Your user settings, including your private views, are stored on the Milestone XProtect Enterprise server. This means that you are able to use your private views on any computer that has a *Smart Client* installed, provided you log in to the *Smart Client* with your own user name and password.

Further Configuration

In addition to creation of groups and views, the *Smart Client*'s *Setup* tab lets you edit existing groups and views. The *Setup* tab furthermore lets you adjust camera settings, and set up joystick control for PTZ (Pan/Tilt/Zoom) cameras.

Note: Particular user rights may be required in order to access the *Setup* tab. Your ability to edit groups and views also depends on your user rights. Basically, if you are able to create groups and views, you are also able to edit them. From time to time your surveillance system administrator may make changes to camera or user properties on the Milestone XProtect Enterprise server. When this is the case, such changes will take effect in the *Smart Client* the first time you log in after the changes were made. Such changes may require you to re-create your views. Ask your surveillance system administrator if in doubt.

Which Types of Groups Can You Edit Views in?

Depending on your user rights, you may be able to create and edit views in the following types of groups:

- Private and shared

- Private, but not shared

- Shared, but not private

- Neither private, nor shared (in which case you simply rely on views created by others and placed in shared groups)

Typically only a few people in an organization are able to create and edit views in shared groups. For example, the surveillance system administrator may create and maintain a number of views and place them in shared groups: When *Smart Client* users log in, the views placed in the shared groups will automatically be available to them, and the users will basically not need to create further views unless they want their own views in *private* groups.

To quickly determine which types of groups your user rights permit you to create and edit views in, do the following:

1. Select any of the *Smart Client*'s tabs.

2. Look at the *Views* section: You are able to create and edit views in any groups ***not*** marked by a padlock icon. If a group is marked by a padlock icon, it is protected: You can still use any views in the group, but you cannot create or edit views in the group.

Example: The user is able to create and edit views in private groups, but not in shared groups. Note the padlock icon on the shared group folder (clearly visible in the enlarged example).

Consult your surveillance system administrator if in doubt about your user rights.

Using Static Images in Views

You are not limited to viewing camera images in a view; you are able to view static images (such as GIF or JPEG) as well.

Example: A company logo inserted as a static image (in this case viewed on the *Live* tab). The feature could equally well be used for inserting maps, floor plans, photos of wanted persons, etc.

To use a static image in a view, do the following on the *Setup* tab:

1. Drag the *System Overview* section's *Static Image* link to the required position in the view.

2. Release the mouse button over the required position.

   When you release the mouse button you are able to select the required static image file.

Using HTML Pages in Views

In addition to viewing camera images and static images in a view, you are able to import HTML pages and display them in the view. This way, you are able to include company web pages, intranet pages, navigation pages, link collections, etc. together with the camera images in the view.

Example: A company web page inserted in a view (in this case viewed on the *Live* tab). The feature could equally well be used for inserting clickable maps, news services, e-learning courses, etc.

Tip: When your imported HTML pages contain links, it is recommended that links have the target='blank' attribute (example: Link). This will make the links open in separate windows, which will help you avoid losing view of the *Smart Client* window itself due to a link opening a web page in the same browser window as the *Smart Client*.

To include an HTML page in a view, do the following on the *Setup* tab:

1. Drag the *System Overview* section's *HTML Page* link to the required position in the view.

    When you release the mouse button over the required position, the *Open URL* window opens:
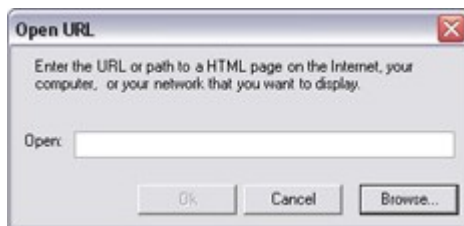
    Open URL window

2. In the *Open URL* window's *Open* field, type the URL of the required HTML page (example: http://www.mywebsite.com/mywebpage.htm).

    - or -

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

3. Click the *OK* link.

Changing the Properties of an Imported HTML Page

Once an HTML page is imported into a view, you are able to change its properties by doing the following:

1. On the *Setup* tab, select the imported HTML page in the view.

    Properties of the HTML page will appear in the *Setup* tab's *Properties* section:

2. Change the required property:

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

- *Scaling*: Select the required scaling of the HTML page. The optimal scaling depends entirely on the content of the imported HTML page and how you want to display it.

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

Examples of the same HTML page viewed with different scaling values

Navigating an Imported HTML Page

An imported HTML page can be navigated using the links on the HTML page itself. Furthermore, each HTML page imported into a view features four navigation buttons in the top bar:

From left to right the buttons are: *Back*, *Forward*, *Refresh* and *Home*.

Renaming Groups

To rename a group, do the following on the *Setup* tab:

1. Select the required group in the *Views* section.

2. Click the *Rename* button:

3. Overwrite the existing group name with a new name of your choice.

Deleting Groups

Note: Deleting a group will delete all views and any subgroups within the group as well.

To delete a group, do the following on the *Setup* tab:

1. Select the required group in the *Views* section.

2. Click the *Delete* button:

    You will be asked to confirm that you want to delete the selected group and all of its content.

Renaming Views

To rename a group, do the following on the *Setup* tab:

1. Select the required group in the *Views* section.

2. Click the *Rename* button:

3. Overwrite the existing group name with a new name of your choice.

Deleting Views

To delete a group, do the following on the *Setup* tab:

1. Select the required group in the *Views* section.

2. Click the *Delete* button:

    You will be asked to confirm that you want to delete the selected group and all of its content.

Adjusting Camera Settings

In the *Setup* tab's *Camera Control* section, you are able to adjust camera settings.

To adjust camera settings, select the position of the required camera in the view. The position you select will be indicated by a bold border.

Camera Name

The *Camera Name* field displays the name of the selected camera. The field is read-only.

Image Quality

The *Image Quality* setting determines the quality of the images when viewed, but also affects bandwidth usage. If the *Smart Client* is used over the internet, over a slow network connection, or

if for other reasons you need to limit the bandwidth used by the *Smart Client*, image quality can be reduced on the server side by selecting e.g. *Low* or *Medium*

Tip: You can quickly reduce the bandwidth usage for all cameras in the view by reducing the image quality for a single camera, then clicking the *Apply To All* button.

Frame Rate

The *Frame Rate* setting lets you select a frame rate for the selected camera. Default is *Unlimited*.

IPIX Split Mode

Available only if the selected camera is an IPIX camera. IPIX is a technology that allows creation and viewing of 360-degree panoramic images. The *Smart Client* supports up to four different viewpoints from a single IPIX camera.

The IPIX Split Mode list lets you select the required spilt mode:

- *One by One* lets you view a single viewpoint.
- *Two by Two* lets you view four different viewpoints at a time.

When viewed on the *Live* and *Browse* tabs, the IPIX camera will appear as specified, with either one or four viewpoints from the same image:

Two by Two: Live tab displaying four different viewpoints from a single IPIX camera;
in this example, the IPIX camera's four viewpoints are enlarged for clarity.

Tip: When viewing different viewpoints from an IPIX camera on the *Live* or *Browse* tabs, you are able to navigate each viewpoint independently by clicking inside each viewpoint, or by using the buttons in the *PTZ Control* section.

Apply to All

The *Apply To All* button lets you quickly apply the camera settings for the selected camera to all cameras in the view.

Customizing Joystick setup

You are able to customize joystick setup for control of PTZ (Pan/Tilt/Zoom) cameras in the *Smart Client*. Customizing joystick setup requires that a joystick is attached to the computer running the *Smart Client*.

Note: Even though joystick control is supported for a large number of PTZ cameras, not all PTZ cameras may be joystick-controlled. Refer to the release note for information about joystick support for cameras.

To customize joystick setup, do the following:

1. Click the *Show Application Menu* button in the *Smart Client*'s top bar:

2. From the menu that appears, select *Joystick Setup*:

   The *Joystick Setup* window will appear.

3. In the *Joystick Setup* window, select the required joystick in the *Selected Joystick* list.

   The axes and buttons available on then selected joystick will be listed in the *Axis Setup* and *Button Setup* sections respectively:
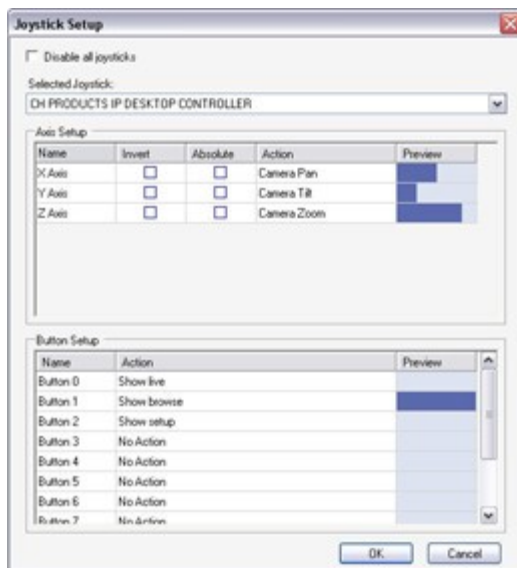
   Joystick Setup window, displaying available axes and buttons on a selected joystick

4. In the *Axis Setup* section, specify settings for the available axes.

   With a joystick, you are typically able to navigate camera images three-dimensionally, along three axes: an X-axis, a Y-axis, and a Z-axis, where the Z-axis typically refers to the depth (zoom) level:
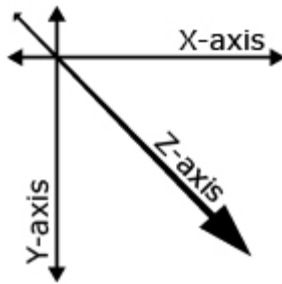
Example: X-, Y-, and Z-axes

- *Invert*: By default, a PTZ camera will move to the right when you move the joystick to the right along the X-axis, move up when you move the joystick towards you along the Y-axis, etc. By selecting *Invert*, you are able to change this to the opposite. You are thus able to freely determine whether the camera should, for example, move up or down when you move the joystick towards you and away from you respectively.

- *Absolute*: By default, joystick control takes place based on a relative positioning scheme. This means that moving a joystick will move the joystick-controlled object based on the object's current position rather than based on any fixed position. By selecting *Absolute*, you are able to change this and use an absolute rather than a relative positioning scheme.

- *Action*: Lets you select the required action for an axis: *Camera Pan*, *Camera Tilt*, *Camera Zoom* or *No action*.

- *Preview*: Lets you quickly test the effect of your selections. When you have selected an action for the axis you want to test, simply move the joystick along the required axis to view the effect, indicated by a movement of the dark blue bar.

5. In the *Button Setup* section, specify an action for each required joystick button. You select the required action in the *Action* column.

Tip: To quickly verify that you are indeed configuring the required button, simply press the required button on the joystick. When the button is pressed, a dark blue color will appear in the *Button Setup* section's *Preview* column for the button in question.

Disabling Joystick Use

To disable the use of joysticks on your *Smart Client*, select the *Joystick Setup* window's *Disable all joysticks* check box.

Assigning Keyboard Shortcuts

You are able to assign shortcut key combinations to particular actions in the *Smart Client*.

To assign shortcut key combinations, do the following:

1. Click the *Show Application Menu* button in the *Smart Client*'s top bar:

2. From the menu that appears, select *Keyboard Setup*:

The *Keyboard Setup* window will appear:

Keyboard setup window

3. When the *Keyboard Setup* window appears, click in the *Press shortcut key* field, then press the required key combination.

   Note: Key combinations must begin with CTRL or ALT. Example: CTRL + B (i.e. first pressing the CTRL key, then—while still pressing the CTRL key—pressing the B key).

   This will display the pressed key combination in the *Press shortcut key* field.

4. In the *Select action* list, select the required action for the shortcut key combination.

5. In the *Use new shortcut in* list, select when the shortcut key combination should apply:

   - *Global*: When working on any of the *Smart Client*'s three tabs (*Live*, *Browse* and *Setup*).

   - *Browse Mode*: When working on the *Smart Client*'s *Browse* tab only.

   - *Live Mode*: When working on the *Smart Client*'s *Live* tab only.

   - *Setup Mode*: When working on the *Smart Client*'s *Setup* tab only.

6. Click the *Assign* button. This will add the specified shortcut key combination to the *Assigned keys* list:

Key	Use in	Action
B, Control	Browse Mode	Browse Next Image
D, Control	Global	Toggle Side Pane
Delete, Alt	Global	Show keyboard setup
Q, Alt	Global	Close the application
Z, Control, Alt	Live Mode	Camera PTZ Zoom In

Example of user-defined keyboard shortcuts

7. Click *OK*.

ℹ️ **Tip:** Your keyboard shortcuts are kept as part of your user settings on the surveillance system server. This means that you will be able to use your keyboard shortcuts on any computer that has a *Smart Client* installed, provided you log in to the *Smart Client* with your own user name and password.

Deleting a Keyboard Shortcut

To delete an existing keyboard shortcut from the *Assigned keys* list, simply select the required row in the list, then click the *Delete* button.

Viewing Live Images

You view live images on the *Smart Client*'s *Live* tab. When you select the *Smart Client*'s *Live* tab, the *Smart Client* will connect to the Milestone XProtect Enterprise server, and display live images from the cameras in the selected view.

Note: Particular user rights may be required in order to access the *Live* tab. In order to view live images in the Smart Client, the *Monitor* application (see page 133) must be running on the Milestone XProtect Enterprise server, consult your surveillance system administrator if in doubt. Depending on your user rights, access to viewing live images from some cameras may be restricted.

The *Live* tab, in this example displaying a view with images from nine cameras

Selecting a View

You are able to select a view for display on the *Live* tab in two ways:

- By selecting the required view in the *Live* tab's *Views* section:

Detail from *Live* tab's *Views* section

- By selecting the required view from the *Views* list located in the upper part of the window:

Views list

Image Bars

Each camera in the view is identified by an image bar, located in the top of each camera image.

The image bar is blue. When you select a particular camera in the view, the image bar of the selected camera image becomes a lighter blue.

Camera image; enlarged detail shows image bar

The image bar displays the name of the camera as well as the name of the device to which the camera is connected. The device name is displayed first, in square brackets, followed by the camera name.

Each image bar will display the word *Live* when live images are displayed, and the word *Stopped* if the camera is stopped.

Each image bar features three colored indicators:

- *Event indicator (the leftmost of the three indicators, solid yellow)*: Lights up when specific events, defined by the surveillance system administrator, occur. Click anywhere inside the image to reset the event indicator. This indicator may appear black if event indication has not been specified for the camera in question, of if no specified events have occurred. Consult your surveillance system administrator if in doubt.

- *Motion indicator (the indicator in the middle, solid red)*: Lights up when motion is detected in the image. Click anywhere inside the image to reset the motion indicator.

- *Online indicator (the rightmost of the three indicators, blinking green)*: Changes state every time an image is received from the camera.

Enlarging Images from a Particular Camera

To enlarge images from a particular camera in a view, double-click the blue title bar above the image.

Double-clicking blue bar above image enlarges view

To return to normal view, simply double-click the blue title bar again.

Tip: If you have selected reduced image quality for the camera (on the *Setup* tab), images from the camera will be displayed in full quality when viewed enlarged.

Event Control

If manual triggering of events has been defined on your surveillance system, you can trigger events from the *Smart Client*.

Note: Depending on your user rights, access to manually triggering events may be restricted.

What is an Event?

Events are used by the surveillance system for triggering *actions*.

Typically, events on the surveillance system are generated automatically. For example, detected movement can be defined as an event which in turn triggers an action, such as recording on a camera. However, it is also possible to trigger events manually.

Depending on configuration, manually triggered events can be used for a wide variety of purposes, including triggering combinations of actions.

For example, the manual triggering of an event could make a camera record with a particular frame rate, activate two different outputs, and send an e-mail alert to three different recipients.

Manual events can be global or tied to a particular camera/device.

Exactly what happens when you manually trigger an event is defined by your surveillance system administrator.

Ask your surveillance system administrator if in doubt about using manually triggered events in your organization. Your surveillance system administrator may occasionally know manually triggered events under the name *event buttons*.

Manually Triggering an Event

To manually trigger an event, select the required event in the *Event Control* section, and click the *Activate* button.

The list of selectable events is grouped by server (engine) and camera/device with which the event is associated. Global events are displayed immediately under the relevant server (engine). In the above example, *Event 1* (the selected event) is a global event.

Output Control

If external outputs have been defined on your surveillance system, for example for switching on lights or sounding a siren, such outputs can be triggered from the *Smart Client*.

Note: Depending on your user rights, access to triggering outputs may be restricted.

To trigger an output, select the required output in the *Output Control* section, and click *Activate*.

The list of selectable outputs is grouped by server (engine) and camera/device to which the output is attached. In the above illustration, the output *Lights on* is attached to the device *[Door] Camera 1* on the server with the default name *Engine*.

PTZ Control

PTZ (Pan/Tilt/Zoom) and IPIX (technology allowing creation and viewing of 360-degree panoramic images) cameras can be controlled from the *Smart Client*.

Note: Depending on your user rights, access to PTZ controls from some cameras may be restricted.

Point-and-Click Control

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

Crosshairs indicate point-and-click control.
For some cameras, crosshairs may look different.

For some cameras, crosshairs surrounded by a square may be displayed. When this is the case, you are able to zoom in on an area by dragging a square around the required area in the image.

For such cameras, zoom level is controlled by holding down the SHIFT key on your keyboard while moving the mouse up or down; this will display a zoom level slider inside the image.

PTZ Navigation Buttons

As an alternative to point-and-click PTZ control, use the navigation buttons in the *PTZ Control* section to move the selected PTZ or IPIX camera. The round middle button lets you quickly move the camera to its home (i.e. default) position. The *plus* and *minus* buttons lets you zoom in and out respectively.

PTZ Control section

PTZ Preset Positions

If preset positions have been defined for the selected PTZ camera, you are able to select such positions from the *Presets* list. Selecting a preset position from the list will make the PTZ camera move to the specified position.

Preset positions are defined by the system administrator; the *Presets* list will be empty if no preset positions have been defined for the selected PTZ camera.

IPIX PTZ Positions

You are able to move to a specific position in an IPIX view, and then save that position by clicking the *Save* button. When you later want to return to the saved position, click the *Load* button.

Tip: You may be able to use a joystick for controlling your PTZ cameras. Joystick control is configured in the *Smart Client*'s *Application Menu*; see *Further Configuration* on page 223. Note that even though joystick and point-and-click control is supported for a large number of PTZ cameras, not all PTZ cameras may be controlled this way. Refer to the release note for information about joystick and point-and-click support for PTZ cameras.

Viewing Recorded Images

You view recorded images on the *Smart Client*'s *Browse* tab.

Note: Particular user rights may be required in order to access the *Browse* tab. Depending on your user rights, access to browsing images from some cameras may be restricted. Date and time formats used when browsing recorded images may vary depending on your computer's regional settings. Illustrations in this help topic, and date and time formats used in these illustrations, are thus for guidance only.

When you select the *Smart Client*'s *Browse* tab, the *Smart Client* will connect to the Milestone XProtect Enterprise server, and display recorded images from the cameras in the selected view. This way, you are able to browse recorded images.

The *Browse* tab provides you with a number of advanced features for browsing recorded images. In addition to image browsing features, the *Browse* tab also lets you print images, and export AVIs (movie clips) and JPEGs (still images).

The *Browse* tab, in this example displaying a view with eight cameras and an imported HTML page

Selecting a View

You are able to select a view for display on the *Browse* tab in two ways:

- By selecting the required view in the *Browse* tab's *Views* section:

Detail from *Live* tab's *Views* section

- By selecting the required view from the *Views* list located in the upper part of the window:

Views list

Enlarging Images from a Particular Camera

To enlarge images from a particular camera in a view, double-click the blue title bar above the image.

Double-clicking blue bar above image enlarges view

To return to normal view, simply double-click the blue title bar again.

Tip: If you have selected reduced image quality for the camera (on the *Setup* tab), images from the camera will be displayed in full quality when viewed enlarged.

Time Navigation

The *Browse* tab's *Time Navigation* section provides you with controls for browsing and playing back recorded images from the camera selected in the view.

Time Navigation section. Date and time format may be different on your computer.

Master Time Area

The *Time Navigation* section's *Master Time* area shows the master time and date of the recordings viewed. The master time is the time to which all the cameras viewed are tied. This means that when you browse recordings, all the images you see in the view will, in principle, be from exactly the same point in time.

Some cameras, however, may only record if motion is detected. Also, there may be no recorded images from one or more cameras in the view matching the specified point in time. When this is the case, the last image in the camera's database prior to the specified point in time will be displayed in the view.

Master Time area. Date and time format may be different on your computer.

The *Master Time* area also displays the current playback speed (example: 1.00x, indicating real-time).

Browse Buttons

The *Time Navigation* section's browse buttons lets you manually navigate through recordings from the camera selected in the view.

Browse buttons

Previous image: Moves to the image just before the one currently viewed

Next image: Moves to the image just after the one currently viewed

Previous sequence: Moves to the first image in the previous sequence

Next sequence: Moves to the first image in the following sequence

First image: Moves to the first image in the database for the selected camera

Last image: Moves to the last image in the database for the selected camera

Time Sliders

The *Time Navigation* section's time sliders let you browse recordings simply by dragging the sliders' handles.

Drag to the left to move backwards in time; drag to the right to move forward in time.

Use the upper times slider for fine browsing within a limited period of time; use the lower slider for coarser browsing within longer time spans.

Time sliders

Playback Slider and Buttons

The *Time Navigation* section's playback slider lets you specify the required playback speed. In the slider's middle position, playback speed is real-time (1.00x). Drag the slider to the left for a slower playback speed; drag to the right for a faster playback speed.

An indication of the exact playback speed is displayed in the upper right corner of the *Time Navigation* section's *Master Time* area.

Playback slider and buttons

Use the playback buttons to play back recordings:

Play reverse: Plays back recordings backwards in time

Play forward: Plays back recordings forward in time

Stop: Stops playback

ⓘ **Tip:** Dragging the playback slider to its leftmost position pauses playback.

To automatically skip gaps in recordings during playback, select the *Skip gaps during playback* check box. Such gaps are primarily evident when a camera has relatively few recordings.

Go To Time

The *Time Navigation* section's *Go To Time* fields let you quickly jump to a specific point in time.
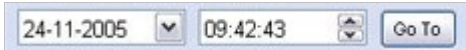
Go To Time fields. Date and time format
may be different on your computer.

Specify required date in the first field and required time in the second field, then click the *Go To* button.

Sequences

The *Browse* tab's *Sequences* section provides you with an overview of recorded sequences for the camera selected in the view.

To use the *Sequences* section, select the required camera in the view, then click the *Sequences* section's *Get Sequences* button.

Clicking the *Get Sequences* button will retrieve a list of up to 40 sequences: 20 sequences prior to the point in time displayed in the view, and 20 sequences following the point in time displayed in the view.

Each sequence will be listed with date and time as well as the length of the sequence. Clicking a sequence in the list will move all images in the view to the time of the sequence.

If the *Preview* check box is selected, you are able to quickly view each sequence by placing the mouse pointer over the required sequence in the list:

Sequences section; placing mouse pointer over a sequence
indication lets you quickly view the incident. Date and
time format may be different on your computer.

Clicking the *expand* icon ⊞ next to a sequence in the list will show you the exact date and time of the first and last image in the sequence as well as the exact date and time of the motion detection, event, etc. triggering the recording.

Sequences may often begin some seconds before a motion detection, event, etc. and end some seconds after. This so-called *buffer* allows you to be able to see what happens immediately before and after an incident; the buffer length is determined by the system administrator.

Expanded sequence indication. Date and
time format may be different on your computer.

Alerts

The *Browse* tab's *Alerts* section lets you view a list of detected events (occasionally known as alerts). Listed events are clickable, allowing you to quickly jump to the time at which an event occurred.
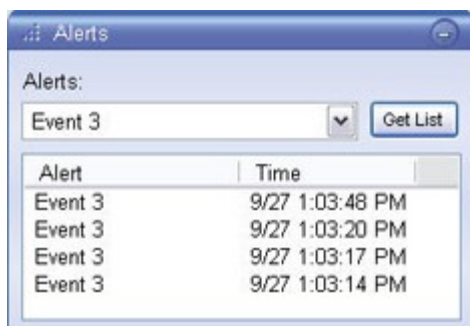
To get a list of events, do the following:

1. Select the required event or events in the *Alerts* list.

   You may either select a single event:
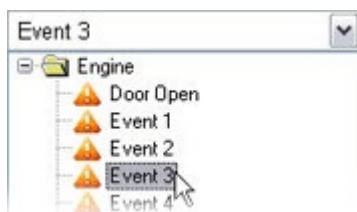
   Or all events on a particular server (engine):
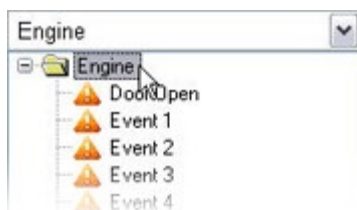
2. Click the *Get List* button. This will display a list of detected events.

   You are able to click the listed events to view recordings from the required event in the view.

Tip: To view what took place prior to and after the event, use the *Time Navigation* controls to browse recordings from around the time of the event.

Smart Search

Smart search lets you search for motion in one or more selected areas of images from a particular camera.

Note: Smart search cannot be used for images from IPIX cameras.

To use smart search, do the following:

1. Select the *Browse* tab's *Smart Search* section:

2. Select the *Smart Search* section's *Show Grid* check box:

3. Select the required camera in the view. A blue grid overlay will appear on the image from the camera; this is the grid you selected in the previous step:
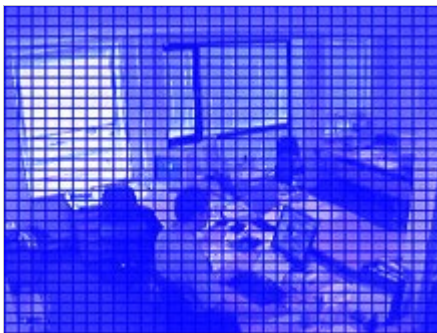
   The overlay can be removed by clearing the *Show Grid* check box.

   Tip: For a better view, enlarge the camera image by double-clicking the blue bar above the image.

4. Click and drag inside the image to select the area in which you want to perform the smart search.

   ![i] **Tip:** You are able to select more than one area.

   The areas you select will become visible through the blue overlay. The blue overlay thus indicates areas to be *excluded* from the smart search:
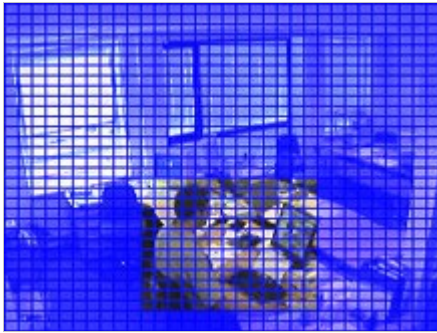
   Example of selected area

   With the *Smart Search* section's *Include* and *Exclude* options, you are able to toggle between including/excluding areas when you drag. With the *Smart Search* section's *Invert* button, you are able to quickly invert your selection, if required. Example:
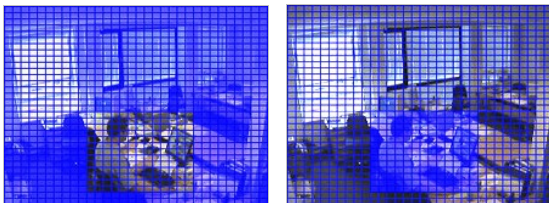
   Original selection (left) and inverted selection (right)

5. Click the *Smart Search* section's *Save* button to save your search area settings.

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

6. In the *Smart Search* section, select required search sensitivity (*Very Low-Very High*) in the *Sensitivity* list.

7. Select required image interval in the *Interval* list.

   If you select *All Images*, all images will be analyzed. If you select e.g. *10 seconds*, only one image per ten seconds of recordings will be analyzed. Selecting a long interval will greatly reduce the time required to complete the search. However, with a long interval, the search may not find motion sequences that are shorter than the specified interval.

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

   Note: Smart search is always carried out from the time of the image you are viewing and forwards or backwards.

9. The smart search begins, and a progress window displays search progress:
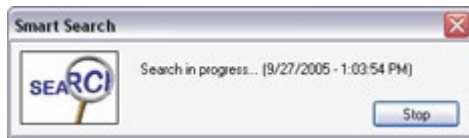
When a sequence with motion inside the selected area(s) is found, it will be displayed in the view. Motion will be highlighted:
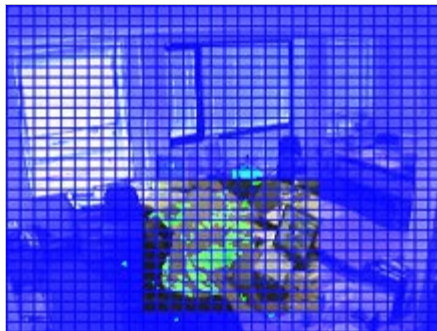
Motion highlighted in light green color

ⓘ **Tip:** The *Browse* tab's *Time Navigation* section control panel will show exact corresponding time information.

10. If required, click the *Next* or *Previous* button again to continue the smart search.

PTZ Control

The Browse tab's PTZ Control section lets you navigate recorded images from IPIX cameras (IPIX is a technology allowing creation and viewing of 360-degree panoramic images).

Note: The *Browse tab's PTZ Control section* cannot be used for controlling PTZ (Pan/Tilt/Zoom) cameras, as the *Browse* tab is used for viewing already recorded images.

Navigation by Dragging inside IPIX Images

Many IPIX images may be navigated simply by dragging inside the images.

If your mouse pointer changes to ⊕ or similar when placed over an image from an IPIX camera, navigation by dragging is supported for the camera.

Refer to the release note for information about supported features for individual IPIX cameras.

Navigation Buttons

As an alternative to navigation by dragging inside IPIX images, use the navigation buttons in the *PTZ Control* section to move around the view from the selected IPIX camera.

The round middle button lets you quickly move the camera to its home (i.e. default) position.

The *plus* and *minus* buttons lets you zoom in and out respectively.

PTZ Control section

Presets

The *Presets* list does not apply for navigating recorded images from IPIX cameras.

IPIX PTZ Positions

You are able to move to a specific position in the IPIX view, and then save that position by clicking the *Save* button.

When you later want to return to the saved position, click the *Load* button.

Printing Images

With the *Browse* tab's *Print* section, you are able to print recorded images.
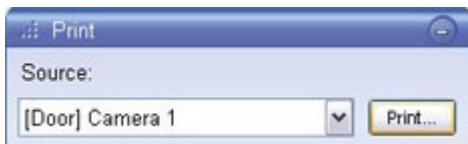
Print section

To print an image, do the following:

1. Select the required camera from the *Print* section's *Source* list. Alternatively, you may select the camera in the view.

2. Select the required date and time by using the controls in the *Time Navigation* section.

3. Click the *Print* section's *Print...* button.

   This will open the *Smart Client Surveillance Report* window with a preview of the image to be printed as well as information about camera name, image capture time, print time and user name of the user printing the image.

   You have the option of including a user's note, for example a description of the recording.

Window with preview and information about printed image.
Date and time format may be different on your computer.

4. **Optional:** If you want to change or verify paper size, source and orientation for the printout, click the *Smart Client Surveillance Report* window's *Page Setup* button to open the *Page Setup* window:

Page Setup window

When ready, click the *Page Setup* window's *OK* button to return to the *Smart Client Surveillance Report* window.

5. **Optional:** If you want to preview your printout, click the *Smart Client Surveillance Report* window's *Preview* button.

6. Click the *Print* button to print the image and associated details.

Exporting Images

With the *Browse* tab's *Export* section, you are able to export recorded images in the AVI (movie clip) and JPEG (still image) formats.
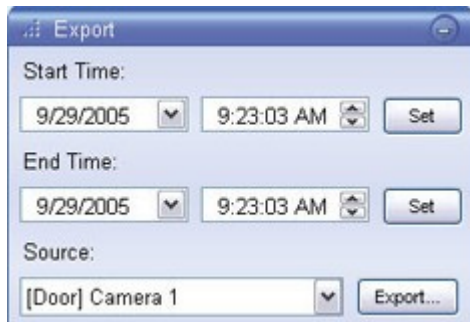
Export section. Date and time format may be different on your computer.

For detailed information about exporting recorded images, see *How to Export Video Evidence* in the following.

How to Export Video Evidence

With the *Smart Client* you are able to quickly generate and export video evidence in the AVI (movie clip) and JPEG (still image) formats.

Note: Depending on your user rights, access to generating AVI or JPEG evidence from some cameras may be restricted.

Date and time formats used when browsing recorded images may vary depending on your computer's regional settings. Illustrations in this help topic, and date and time formats used in these illustrations, are thus for guidance only.

To export video evidence, do the following:

1. Select the *Smart Client*'s *Browse* tab.

2. In the *Browse* tab's *Export* section, specify start date and time for the export by typing the date in the first *Start Time* field and the time in the second field.
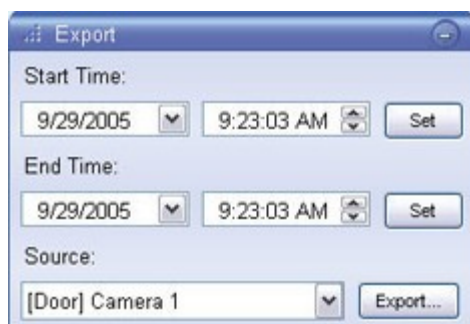
Export section. Date and time format may Be different on your computer.

ⓘ **Tip:** Instead of manually specifying date and time, you may use the *Browse* tab's *Time Navigation* features to move to the required start point, then click the upper of the *Export* section's *Set* buttons.
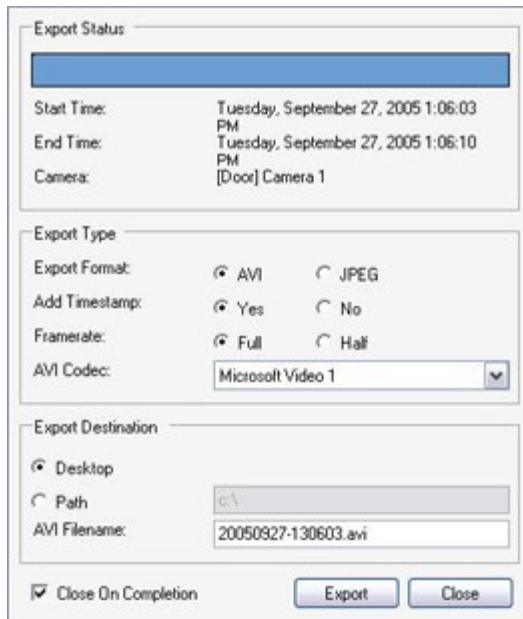
This will automatically set the date and time of the viewed image in the *Start Time* fields.

3. In the *End Time* fields, specify end date and time for the export.

   You may use the *Set* button as described above.

4. Select the required camera from the *Source* list.

5. Click the *Export...* button. This will open a separate export dialog:

Export dialog. Date and time format may be different on your computer.

The export dialog will list the specified start time, end time, and camera.

6. In the export dialog's *Export Type* section, select the required export format: *AVI* (movie clip) or *JPEG* (still images).

7. Select whether to add timestamps from the surveillance system to the exported images.

   If selected, timestamps will appear in the corner of the images:

Timestamps; arrow indicates actual position. Date
and time format may be different on your computer.

8. ***This step applies for export in the AVI format only; if using the JPEG format, go to
   step 10***
   Select required frame rate for the export. With the *Full* option, all images between the start
   and end times will be included in the export; with the *Half* option, only every second image
   will be included, yet still play back in real-time.

9. ***This step applies for export in the AVI format only; if using the JPEG format, go to
   step 10***
   In the *AVI Codec* list, select required AVI codec. The list will contain the video codecs
   available on your computer.

   🛈 **Tip:** A video codec is a particular compression/decompression technology used when
   generating video files. Your choice of codec will affect the quality and size of the AVI file.
   The Indeo® video 5.10 codec, if available on your computer, generally provides a very
   good compromise between quality and file size.

10. Specify export destination in the export dialog's *Export Destination* section.

    - *Desktop*: If you select *Desktop*, your exported file will be saved in an automatically
      created *Exported Images* folder on the desktop of your computer.

    - *Path*: If you select *Path*, you are able to specify a path yourself. The exported file will
      be saved in an automatically created *Exported Images* folder under the path you
      specify (example: If you specify a path like C:\My Stuff\My Files, the exported file will
      be saved in C:\My Stuff\My Files\Exported Images).
      When specifying a path this way, the folders you specify do not have to be existing
      ones; if they do not already exist, they will be created automatically.

11. ***This step applies for export in the AVI format only; if using the JPEG format, go to
    step 12***
    By default, the AVI file will get a file name based on the export start time in the 24-hour
    format, along the structure yyyymmdd-hhmmss.avi (year, month, day, hour, minute,
    second; example: 20050927-130603 for a file with a start time of 13:06:03 on 27th
    September 2005). The name will automatically appear in the *AVI File Name* field.

    The default file name format is independent of regional settings on your computer.

You are always able to change the default file name to a name of your choice, simply by overwriting the default file name. Remember that the file name *must* include the .avi file extension.

12. Click the *Export* link to begin the export.

The status bar in the upper part of the export dialog will display the status of the export:

Export status bar

ℹ️ **Tip:** If you are exporting very long sequences, export may—depending on your selected export settings—take a while. You can continue to use the *Smart Client* for other purposes while the export process is underway.

If the *Close On Completion* check box is selected (default), the export dialog will automatically close when the export is finished.

Upon completion, you are able to view and distribute the exported file.

Example: AVI file viewed in the Winamp player; other popular players include the Windows Media Player and the RealPlayer

Logging Out of the Smart Client

To log out of the *Smart Client*, simply click the *Log Out* button in the *Smart Client*'s top bar:

Log Out button

Web and RealtimeFeed Servers

Milestone XProtect Enterprise features two alternatives to the *Image Server*/*Remote Client*/*Smart Client* for providing remote access to the surveillance system: The *Web Server* and the *RealtimeFeed Server*.

Remote users connect to the *Web Server* and the *RealtimeFeed Server* through a regular browser; no client software is required.

The *Web Server* and the *RealtimeFeed Server* do not offer as advanced functionality as the *Image Server*/*Remote Client*/*Smart Client*; neither at the server end, nor at the client end. However, if remote users are to access the surveillance system through very slow connections, such as 28.8 Kbps connections, using the *Web Server* and the *RealtimeFeed Server* may be advisable.

Both servers can be started from Windows' *Start* menu if they have not been added to the Startup folder when Milestone XProtect Enterprise was installed.

The *Web Server* handles navigation and still image viewing, whereas the *RealtimeFeed Server* handles all live and playback feeds.

By default, the *Web Server* uses port 81, and the *RealtimeFeed Server* uses port 9513.

Note: Both servers must be started before they are active and remote users are able to connect to them. If remote users should be able to view live images, the *Monitor* application (see page 133) must be running as well.

Web Server: Configuration

To configure the *Web Server*, open the *Web Server*'s *Settings* window the following way:

1. Open Windows' *Start* menu.

2. Click *All Programs*.

3. Select *Milestone XProtect Enterprise > Web Server*.

    The *Web Server* icon now appears in the notification area (system tray), at the far right of the Windows taskbar.

    Web Server icon

4. Click the *Web Server* icon.

    This will open the *Milestone XProtect HTTP Server* window:

Milestone XProtect HTTP Server window

5. In the *Milestone XProtect HTTP Server* window, click the *Settings* button.

    This will open the *Settings* window, in which you configure the *Web Server*:

Settings window

The *Settings* window lets you configure the *Web Server*. The *Settings* window is divided into two sections: the *HTTP server setup* section and the *User administration* section:

HTTP Server Setup

The *Settings* window's *HTTP Server setup* section contains the following fields:

Field	Description
HTTP port	Indicates the port used by the *Web Server*. Default is port 81. Field is editable only when the *Web Server* is stopped (see *Stopping the Web Server* on page 256).
Auto Start	The *Web Server* must be started before it is active and remote users are able to connect to it. The *Auto Start* check box lets you enable automatic start of the *Web*

	Server. With automatic start enabled, the *Web Server* will start automatically when you click the *Web Server* icon in the notification area at the far right of the Windows taskbar. *Web Server* icon When automatic start is not enabled, you must start the *Web Server* manually by clicking the *Start server* button in the *Milestone XProtect HTTP Server* window. You access the *Milestone XProtect HTTP Server* window by clicking the *Web Server* icon in the notification area at the far right of the Windows taskbar.
Log Activity to File	Select check box to log *Web server* activity in a log file. The log file will be stored in the directory in which the Milestone XProtect Enterprise software is installed, typically C:\Program Files\Milestone\Milestone Surveillance.
Days to log	Available only if *Log Activity to File* check box is selected. Lets you specify the number of days in which log files should be kept before they are deleted. Default is ten days. 🛈 **Tip:** Read more about logging on page 265.
Timeout for connections	Lets you specify a number of minutes within which the remote user must have been active (requested information from the *Web Server*) in order to keep the connection open. If the remote user has not been active within the specified time, the connection will be closed, and the remote user will have to log in again if more information is required from the *Web Server*. Default period is five minutes.
Realtime feed quality	**Note:** This setting specifically concerns the *RealtimeFeed Server*. Lets you specify the default image quality used by the *RealtimeFeed Server*: • *Low*: Low image quality. Recommended for slow connections, such as modem connections. • *Medium*: Medium image quality. Recommended for connections of reasonable speed, such of ISDN connections. • *High*: High image quality. Recommended for fast connections, such as ADSL or LAN connections. Remote users will be able to manually override the *RealtimeFeed Server*'s default image quality.

User Administration

Accounts and access rights for remote users are configured in the *Settings* window's *User Administration* section. Unrestricted anonymous remote access is possible; however, if you want to restrict remote access, you must define user accounts, i.e. user names and passwords, for the remote users.

Defining User Accounts

To define user names and passwords for remote users, click the *User setup* button. This will open the *User administration* window, in which you define individual user names and their associated passwords.

To add a user, click the *User administration* window's *Add user...* button, specify the required user name and password, and click *OK*. This will add the user to the *User administration* window's list of users. To remove a user from the *User administration* window's list of users, select the user in the list, and click the *Delete user* button.

Defining Access Rights

Three different types of access right are available:

- *Allow anonymous access*: Allows unrestricted access; users will not have to specify a user name or password to access.

- *Access for predefined users only*: Allows access only to users you have defined by clicking the *User setup* button. Those users must provide their user name and password when accessing, after which they will have access to all available cameras.

- *Restrict user access by camera*: Allows access only to users you have defined by clicking the *User setup* button. You are able to restrict those users' access to particular cameras and features as described in the following.

Restricting Defined Users' Access

When you select the option *Restrict user access by camera*, you are able to restrict defined users' access to particular cameras and features in the following way:

1. Click the *User Access* button. This will open the *Define Camera Access for individual users* window:

Define User Access for individual users window

2. In the *User* list, select the required user.

3. In the *Defined Cameras* list, select the name of each camera to which the user should have access.

    ![info] **Tip:** By pressing the CTRL or SHIFT buttons on your keyboard while selecting camera names in the *Defined Cameras* list, you are able to select several or all of the listed camera names in one go.

4. Click the >> button to move the selected camera names to the *Viewable by selected user* list.

5. If the user in question should be able to play back recordings from the selected cameras, select the *Allow playback functionality via HTTP server* check box.

6. If the user in question should be able to generate AVI movie clips from recordings from the selected cameras, select the *Allow AVI creation via HTTP server* check box.

7. Repeat as required for other users.

![info] **Tip:** For the remote user's perspective, also see *Remote Access through Web and RealtimeFeed Servers* on page 259.

Testing the Web Server Configuration

To test the *Web Server*, open an Internet Explorer browser (version 6.0 or later is required) on the computer running the Milestone XProtect Enterprise software, and go to the following address:

        http://localhost:81

Note: For remote users to view live images, the *RealtimeFeed Server* as well as the *Monitor* application must be running.

Web Server: Day-to-Day Operation

Once it has been configured, you are able to run the *Web Server*, and remote users will be able to connect to it for image navigation and still image viewing.

Starting the Web Server

The *Web Server* may already be running. When the *Web Server* is running, the *Web Server* icon appears in the notification area (system tray), at the far right of the Windows taskbar.

![Web Server icon]

Web Server icon

If the icon is not present, you must start the *Web Server*.

To start the *Web Server*, do the following:

1. Open Windows' *Start* menu.

2. *Select All Programs*.

3. Select *Milestone XProtect Enterprise > Web Server*.

    The *Web Server* icon now appears in the notification area, at the far right of the Windows taskbar.

4. Click the *Web Server* icon.

    This will open the *Milestone XProtect HTTP Server* window:

    Milestone XProtect HTTP Server window

    If *Auto Start* was selected when configuring the *Web Server*, the *Web Server* will automatically start, and remote users are able to connect to it.

    If *Auto Start* was not selected when configuring the *Web Server*, the *Web Server* must be started manually by clicking the *Start server* button.

5. *Web Server* and user activity can be monitored in the *Milestone XProtect HTTP Server* window's *Log* section.

Stopping the Web Server

To stop the *Web Server*, click the *Milestone XProtect HTTP Server* window's *Stop server* button. This will stop the *Web Server* without shutting it down.

This means that you will quickly be able to start the *Web Server* again by clicking the *Start server* button.

Shutting Down the Web Server

To shut down the *Web Server*, click the *Milestone XProtect HTTP Server* window's *Shut down...* button. This will shut down the *Web Server*, and you will have to access it from Window's *Start* menu in order to start it again.

When clicking the *Shut down...* button, you will be asked to confirm that you want to shut down the *Web Server*.

RealtimeFeed Server: Configuration

The *RealtimeFeed Server* does not require any configuration as such, apart from its default image quality, specified as part of the configuration of the *Web Server*.

Changing RealtimeFeed Server Port Number

You are, however, able to change the port number used by the *RealtimeFeed Server* when communicating with the ActiveX Real Time Client (default is port 9513).

To change the port number, do the following:

1. Make sure the *RealtimeFeed Server* is started (see *Starting the RealtimeFeed Server* on page 257).

2. Access the *Realtime Feed Server* window by clicking the *RealtimeFeed Server* icon in the notification area at the far right of the Windows taskbar.

3. Stop the *RealtimeFeed Server* by clicking the *Stop* button.

4. Change the port number in the *Server Port* field.

5. Locate the file *playbackfeed.html* in the *HTML* directory under the directory in which the Milestone XProtect Enterprise software is installed.

6. Edit the file *playbackfeed.html* by changing the port number in the line *RTFeed.port = 9513;* to the required port number.

RealtimeFeed Server: Day-to-Day Operation

Once you run the *RealtimeFeed Server*, remote users will be able to connect to it for live image feeds.

Starting the RealtimeFeed Server

The *RealtimeFeed Server* may already be running. When the *RealtimeFeed Server* is running, the *RealtimeFeed Server* icon appears in the notification area (system tray), at the far right of the Windows taskbar.

RealtimeFeed Server icon

If the icon is not present, you must start the *RealtimeFeed Server*.

To start the *RealtimeFeed Server*, do the following:

1. Open Windows' *Start* menu.

2. *Select All Programs*.

3. Select *Milestone XProtect Enterprise > Live Feed Server*.

   The *RealtimeFeed Server* icon now appears in the notification area, at the far right of the Windows taskbar.

4. Click the *RealtimeFeed Server* icon.

   This will open the *Milestone XProtect Realtime Feed Server* window:

Milestone XProtect Realtime Feed Server window

   If the *Autostart* check box is selected, the *RealtimeFeed Server* will automatically start.

   If the *Autostart* check box is not selected, the *RealtimeFeed Server* must be started manually by clicking the *Start* button.

5. Connecting users' IP addresses and progress can be viewed in the *Milestone XProtect Realtime Feed Server* window's *Connections* section.

Stopping the RealtimeFeed Server

To stop the *RealtimeFeed Server*, click the *Milestone XProtect Realtime Feed Server* window's *Stop* button. This will stop the *RealtimeFeed Server* without shutting it down.

This means that you will quickly be able to start the *RealtimeFeed Server* again by clicking the *Start* button.

Shutting Down the RealtimeFeed Server

To shut down the *RealtimeFeed Server*, click the *Milestone XProtect Realtime Feed Server* window's *Shut down...* button. This will shut down the *RealtimeFeed Server*, and you will have to access it from Window's *Start* menu in order to start it again.

When clicking the *Shut down...* button, you will be asked to confirm that you want to shut down the *RealtimeFeed Server*.

Remote Access through Web and RealtimeFeed Servers

Provided the *Web Server* and the *RealtimeFeed Server* are running on the Milestone XProtect Enterprise surveillance system, remote users are able to connect to the surveillance system's web server through a regular Microsoft Internet Explorer browser.

When accessing the surveillance system this way, remote users will—their access rights permitting—be able to view live images from cameras on the surveillance system, browse recorded images as well as generate and export AVI movie clips of recorded events.

Remote users should be aware that a more advanced and feature-rich way of accessing the surveillance system may be available: Ask your Milestone XProtect Enterprise system administrator if it is possible to connect with a *Remote Client* (see page 171) or *Smart Client* (see page 210).

Logging in to the Surveillance System

Note: To log in to the surveillance system, you must connect to a particular IP address and port number; ask your Milestone XProtect Enterprise system administrator if in doubt about which IP address and port number to use.

Log in to the surveillance system the following way:

1. Open a Microsoft™ Internet Explorer browser.

    Microsoft™ Internet Explorer Version 6.0 or later is required.

    i **Tip:** To find out which Microsoft™ Internet Explorer version you are using, select *About Internet Explorer* in your browser's *Help* menu.

2. In the browser's *Address* field, type `http://` followed by the IP address or host name of the Milestone XProtect Enterprise server you want to connect to. You must specify the server's port number after the IP address. Use a colon to separate the IP address and the port number.

    Example: If the IP address of the server is 123.123.123.123 and its port number is 81, type `http://123.123.123.123:81`

3. Click the browser's *Go* button—or simply press the ENTER key on your keyboard—to go to the IP address you have specified.

    When the connection to the *Web Server* has been successfully established, a login page will appear:

    Detail from login page

4. Access to the *Web Server* is likely to be restricted. When this is the case, specify your user name and password.

5. If you want to be able to view live images, or to be able to browse recorded images, select the *ActiveX support* check box.

6. Click the *Login* button.

7. A web page with a menu for selecting cameras, navigating images, etc. will appear:

Example of remote viewing of images from a surveillance camera

The menu is divided into three sections: *Single View* (light yellow background), *Quad View* (purple background) and *Help* (green background). The features available in each menu section are described in the following.

Single View

The *Single View* menu section is used for handling images from a single camera at a time.

The following features are available in the *Single View* menu section:

Feature	Description
Select Camera	Lets you select a camera. Selection is based either on a simple clickable list of cameras or on a graphic representation of the Milestone XProtect Enterprise surveillance system's Monitor application (see page 133). When the graphic representation is used, available cameras are indicated by green squares: To select a camera, click a green square. The selected square will be highlighted, and a still image from the selected camera will appear next to

	the menu. Blue squares may appear. Such blue squares simply indicate that no camera is available in the particular section of the Milestone XProtect Enterprise surveillance system's *Monitor* application.
Archives	Non-recent images are typically saved in so-called archives. The *Archives* link lets you select and view archived images from the selected camera, provided such archives are available.
Image	Lets you browse recorded images from the recent database of the selected camera, image by image. Clicking the l*eft arrow* will take you to the image preceding the currently viewed image, unless the currently viewed image is the first stored image. Clicking the *right arrow* will take you to the image following the currently viewed image, unless the currently viewed image is the last stored image. *i* **Tip:** To view non-recent images from the selected camera, try the *Archives* feature.
Motion	Lets you browse images from the recent database of the selected camera, in which motion has been detected. Clicking the *left arrow* will take you to the previous image in which motion was detected, unless the currently viewed image is the first stored image. Clicking the *right arro*w will take you to the next image in which motion was detected, unless the currently viewed image is the last stored image. *i* **Tip:** To view non-recent images from the selected camera, try the *Archives* feature.
Sequence	Lets you browse sequences from the recent database of the selected camera. Clicking the *left arrow* will take you to the previous sequence. If motion was detected within the sequence, you will be taken to the first image in which motion was detected within the sequence. If no motion was detected within the sequence, you will be taken to the first image in the sequence. Clicking the *right arrow* will take you to the next sequence. If motion was detected within the sequence, you will be taken to the first image in which motion was detected within the sequence. If no motion was detected within the sequence, you will be taken to the first image in the sequence. *i* **Tip:** To view non-recent images from the selected camera, try the *Archives* feature.
End	Lets you quickly jump to the oldest or newest image from the recent

<table>
<tr>
<td></td>
<td>database of the selected camera.

Clicking the left arrow will take you to the oldest image in the recent database of the selected camera.

Clicking the right arrow will take you to the newest image in the recent database of the selected camera

i **Tip:** To view non-recent images from the selected camera, try the *Archives* feature.</td>
</tr>
<tr>
<td>**Overview**</td>
<td>Lets you browse sequences from the recent database of the selected camera, in which motion has been detected.

Overview browsing is based on thumbnail image representations of the sequences.

Clicking the *left arrow* provides you with an overview of the previous four sequences in which motion was detected, with information about each sequence.

You are able to jump to a sequence by clicking the thumbnail image representing it.

Example of overview

Likewise, clicking the *right arrow* provides you with an overview of the next four sequences in which motion was detected, with information about each sequence, and you are able to jump to a sequence by clicking the thumbnail image representing it.

Clicking the *Overview* link lets you browse the four-sequence overviews. For each click, you are taken forward in time.</td>
</tr>
<tr>
<td>**Alarms**</td>
<td>Lets you browse sequences from the recent database of the selected camera, in which motion has been detected.

Alarms browsing is based on a list of the sequences.

Clicking the *left arrow* lets you browse back in time in a list of sequences in which motion was detected.

The list displays information about start time, first motion detection (alarm) time and end time for each sequence.

By clicking the list's links, you are able to jump to the images matching each sequence's start time, first motion detection (alarm) time and end time.</td>
</tr>
</table>

Example of *Alarms* list

Likewise, clicking the *right arrow* lets you browse forward in time in a list of sequences in which motion was detected.

The list displays information about start time, first motion detection (alarm) time and end time for each sequence. By clicking the list's links, you are able to jump to the images matching each sequence's start time, first motion detection (alarm) time and end time.

Clicking the *Overview* link lets you quickly jump to a list of the newest sequences in which motion was detected.

Live	Switches to live view for the selected camera. Live view lets you view live images from the selected camera.
	When viewing live images, you are able to select between low, medium and high image quality.
	The *pause* button *start* buttons in the live view lets you pause and start the live feed as required.
	If configured for the selected camera, output buttons may also be available. Output buttons are used for triggering external output, for example for switching on lights, sounding a siren, etc. Ask your Milestone XProtect Enterprise system administrator if in doubt.
	For PTZ (Pan/Tilt/Zoom) cameras, PTZ navigation buttons will also become available in the live view, provided you have the user rights required to control PTZ cameras.
	To return to viewing still images from the selected camera, click the *Still* link in the live view.
Playback	**Note:** Particular user rights may be required in order to use this feature.
	Switches to playback view for the selected camera.
	Playback view lets you play back recorded images from the selected camera, based on a date and time you specify in the playback view.
	The *pause* and *start* buttons in the playback view lets you pause and start the live feed as required.
	To return to viewing still images from the selected camera, click the *Still* link in the playback view.
Build AVI file	**Note:** Particular user rights may be required in order to use this feature.
	Starts a wizard, with which you are able to create and export an AVI movie clip of selected recordings.

	Such movie clips may, for example, be used as evidence.
Print	Lets you print the currently viewed image. A time stamp will automatically be included with the print. You are furthermore able to include your name and a comment, if required.
Go To	Lets you jump straight to images from a date and time specified in the field above the *Go To* button.

Quad View

The *Quad View* menu section is used for viewing live images from up to four cameras at a time.

Example of quad view

You are able to create and save up to ten different quad views.

To save a quad view, click the *Save Setup* link at the top of the quad view in question.

ⓘ **Tip:** You are able to give each saved quad view a name of your choice: Type the required name in the *Quad* field at the top of the quad view in question, then click the *Save Setup* link.

Help

The *Help* menu section provides access to a help text describing use of the menu's features.

Logging

Various types of log files can be generated by Milestone XProtect Enterprise:

Log File Types, Locations and Names

Milestone XProtect Enterprise is able to generate the following types of log files:

Administrator Log Files

These files log activity in the *Administrator*. A log file is created for each day the *Administrator* is used.

*Administrato*r log files are by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Logfile Settings* section (see page 81).

Administrator log files are named according to the structure AdminYYYYMMDD.log, e.g. *Admin20051231.log*.

Monitor Log Files

These files log activity in the *Monitor*. A log file is created for each day the *Monitor* is used.

Monitor log files are by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Logfile Settings* section (see page 81).

Monitor log files are named according to the structure MonitorYYYYMMDD.log, e.g. *Monitor20051231.log*.

Event Log Files

These files log information about registered events (read more about events in *About Input, Events and Output* on page 91). A log file is created for each day on which events have occurred.

Event log files are by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\. Note, however, that the location as well as the number of days to log can be changed in the *General Settings* window's *Event Recording Settings* section (see page 82).

Event log files should be viewed using the *Monitor application*'s *Viewer* (see page 142) or the *Smart Client* (see page 210):

- Viewer: Select the *Viewer*'s Alarm Overview control panel, then click the *Events* button to view the events log.

- *Smart Client*: In the *Browse* tab's *Alerts* section, select the required event, then click the *Get List* button to see when the event in question was detected.

Image Server Log Files

These files log activity on the *Image Server* service. A log file is created for each day the *Image Server* is used.

Image Server log files are by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\.

Image Server log files are named according to the structure ISLog_YYYYMMDD.log, e.g. *ISLog_20051231.log*.

Image Server Audit Log Files

These files log *Remote Client* (see page 171) and *Smart Client* (see page 210) user activity, if audit logging is enabled in the *Image Server Administrator* (see page 162). A log file is created for each day with remote user activity.

By default placed in a subfolder named *ISAuditLog* under the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\.

Image Server audit log files are named according to the structure is_auditYYYYMMDD.log, e.g. *is_audit20053112.log*.

Export Log Files

These files log activity regarding database export from the *Monitor* application's *Viewer* (see page 142). A log file is created for each day on which export was performed.

By default, exported databases as well as the export log file are placed in an *Exported Images* folder on the desktop of the computer on which the export was performed. Note, however, that the export location may be changed as part of the export process (see page 153).

Export log files are named according to the structure ExportYYYYMMDD.log, e.g. *Export20053112.log*. Note, however, that database exports may be encrypted and/or compressed, in which case export log files are also encrypted/compressed and further file extensions, such as *.mzi* or *.men* may appear in export log file names.

Web Server Log Files

These files log activity on the *Web Server* (see page 251), if logging is enabled in the *Milestone XProtectHTTP Server* window.

Web Server log files are by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\.

Web Server log files are named according to the structure www_YYYYMMDD.log, e.g. *www_20051231.log*.

Log File Structures

Most log files generated by Milestone XProtect Enterprise 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 and an encrypted part. The encrypted part makes it possible—through decryption and comparison—to assert that a log file has not been tampered with.

Integrity Checks and Possible Error Messages

Log files are subjected to an integrity check once every 24 hours. The result of the integrity check is automatically written to a file named *ELFFLogCheckerResult.txt*.

The *ELFFLogCheckerResult.txt* file is by default placed in the folder containing the Milestone XProtect Enterprise software, typically C:\Program Files\Milestone\MilestoneSurveillance\.

Only a single *ELFFLogCheckerResult.txt* file will exist; new integrity check information is automatically appended in the existing file.

Any inconsistencies will be reported in the form of error messages written in the *ELFFLogCheckerResult.txt* file. The following table lists possible error messages:

Error Message	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. Thus, log integrity cannot be guaranteed.
"[Log file name] not found."	The log file was not present.
"[Log file name] is empty."	The log file was present, but empty.
"Last line changed/removed in [log file name]."	The last line of the log file did not match validation criteria.
"Encrypted data missing in [log file name] near line [#]."	The encrypted part of the log line in question was not present.
"Inconsistency found in [log file name] near line [#]."	The log line does not match the encrypted part.
"Inconsistency found in [log file name] at beginning of log file."	The log file header is not correct. This situation is most likely to occur if a user has attempted to delete the beginning of a log file.

Removing Milestone XProtect Enterprise

Note: If you are not a Milestone XProtect Enterprise system administrator, it is highly recommended that you consult your system administrator before removing the software.

To remove your Milestone XProtect Enterprise software, use the following procedure:

1. Shut down all Milestone XProtect Enterprise applications, including the *Web Server* and *RealtimeFeed Server* if they are running.

2. Open Windows' Control Panel, and select *Add or Remove Programs*. This will open the *Add or Remove Programs* window.

3. In the *Add or Remove Programs* window, select the *Milestone XProtect Enterprise* entry and click the *Change/Remove* button.

The *Add or Remove Programs* window

4. You will be asked to confirm that you want to remove the Milestone XProtect Enterprise package.

   If you want to keep your existing configuration and/or databases, make sure the *Remove Database Files* and *Remove Registry Settings* check boxes are **cleared**.

Confirmation window—note the *Remove Database Files* and *Remove Registry Settings* check boxes.

   If you are sure that you want to remove the software, click *OK*.

5. Click *Finish*.

6. Back in the *Add or Remove Programs* window, now select the *Video Device Driver VX.X* entry (where *VX.X* refers to the version number for your installation) and click the *Change/Remove* button.

   This will remove the video device drivers used with Milestone XProtect Enterprise. Drivers

are small programs used for controlling and communicating with devices.

7. You will be asked to confirm that you want to remove the video device drivers.

    If you are sure that you want to remove the drivers, click *Yes*.

8. When the drivers have been removed, click *Finish*.

Glossary

A

AVI: A popular file format for video. Files in this format carry the .avi file extension.

B

Browser: 1) A software application for finding and displaying web pages. 2) In Milestone XProtect Enterprise specifically, the term *Browser* may occasionally be used when referring to the *Monitor* application's *Viewer* feature, as the *Viewer* feature was formerly known under the name *Browser*.

Background Camera: In Milestone XProtect Enterprise specifically, the term "Background Camera" refers to a camera which is enabled but not included in the Monitor application.

C

Codec: A technology for compressing and decompressing audio and video data, for example in an exported AVI file. MPEG and Indeo are examples of frequently used codecs.

D

DirectX: A Windows extension providing advanced multimedia capabilities.

DLK: Device License Key; a registration code required for every device (IP network camera or IP video server) installed on the surveillance system. If you do not have system administration responsibilities, you do not have to deal with DLKs. System administrators obtain DLKs as part of the software registration process. System administrators use the Import DLKs... feature in the *Administrator* application (see page 30) to import DLKs into the surveillance system.

DNS: Domain Name System; a system that allows translation between alphabetic host names (example: mycomputer) or domain names (example: www.mydomain.com) and numeric IP addresses (example: 192.168.212.2). Many people find alphabetic names easier to remember than numeric IP addresses.

Driver: A small program used for controlling/communicating with a device.

F

FPS: Frames Per Second, a measure indicating the amount of information contained in 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 will appear. Note, however, that a high FPS may also lead to a large file size when video is saved.

Frame Rate: A measure indicating the amount of information contained in motion video. Frame rate is typically measured in FPS (Frames Per second). The higher frame rate, the smoother motion in video sequence will appear.

FTP: File Transfer Protocol, a 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

GSM: Global System for Mobile communications, a system for mobile telephony.

H

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

I

I/O: Short for Input/Output.

IP: Internet Protocol; a protocol (i.e. standard) specifying the format and addressing scheme used for sending data packets across networks. IP is often combined with another protocol, TCP (Transmission Control Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

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

IPIX: A technology that allows creation and viewing of 360-degree panoramic images. IPIX is a trademark of Internet Picture Corporation (IPIX).

J

JPEG: An image compression technology, named after the Joint Photographic Experts Group. Files created with JPEG compression usually carry the .jpg file extension.

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 following frames record only the pixels that change. This helps greatly reduce the size of MPEG files.

M

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

MPEG: A group of compression standards and file formats for digital video developed by the Moving Pictures Experts Group (MPEG). MPEG standards use so-called lossy compression as they store only the changes between frames, removing often considerable amounts of redundant information: Keyframes stored at specified intervals record the entire view of the camera, whereas the following frames record only pixels that change. This helps greatly reduce the size of MPEG files.

P

PDA: Personal Digital Assistant; a handheld computer device with networking features.

PIN: Personal Identity Number (or Personal Identification Number), a number used to identify and authenticate users.

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.

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

PUK: Personal Unblocking Key, or PIN Unlock Key, a number used as an extra security measure for SIM cards.

R

Recording: In IP video surveillance systems, the term *recording* means *saving images from a camera in the camera's database on the surveillance system*. In many IP video surveillance systems, all of the images received from cameras are not necessarily saved. Saving of images in a camera's database—recording—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, when motion is no longer detected, when an event occurs, when a time period ends, or similar. The term originates from the analog world, where images were not taped until the record button was pressed.

S

SIM: Subscriber Identity Module, a small card inserted into a GSM mobile phone, a GSM modem, etc. The SIM card is used to identify and authenticate the user.

SLC: Software License Code; a product registration code required for using the surveillance system 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, a system for sending text messages to mobile phones.

SMTP: Simple Mail Transfer Protocol, a 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 123.123.123 is the shared prefix. Network administrators use so-called subnet masks to divide networks into subnets.

T

TCP: Transmission Control Protocol; a protocol (i.e. standard) used for sending data packets across networks. IP is often combined with another protocol, IP (Internet Protocol). The combination, known as TCP/IP, allows data packets to be sent back and forth between two points on a network for longer periods of time, and is used when connecting computers and other devices on the internet.

TCP/IP: Transmission Control Protocol/Internet Protocol; a combination of protocols (i.e. standards) used when connecting computers and other devices on networks, including the internet.

U

UDP: User Datagram Protocol; a 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 e.g. the TCP protocol.

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

V

Video Server: A device, typically a standalone device, which is able to stream video from a number of connected client cameras. Video servers contain image digitizers, making it possible to connect analog cameras to a network.

VMD: Video Motion Detection.

Copyright, Trademarks and Important Information

Copyright

© 2005 Milestone Systems A/S.

Trademarks

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

Microsoft and Windows are registered trademarks of Microsoft Corporation.

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

Disclaimer

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

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

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

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

Index

Milestone Systems A/S
Copenhagen, Denmark
Tel.: +45 88 300 300
Fax: +45 88 300 301
info@milestonesys.com
www.milestonesys.com

XPE56-cm-3-231205