Name	Description
Select picture	Specify the path to a file with a picture of the cardholder. This button is not visible if the access control system manages the pictures. Allowed file-formats are .bmp, .png, and .jpg. Pictures are resized to maximize the view. Milestone recommends that you use a quadratic picture.
Delete picture	Click to delete the picture. If the access control system had a picture, then this picture is shown after deletion.

XProtect LPR

LPR system overview

About XProtect LPR

Available functionality depends on the system you are using. See the Product comparison chart for more information.

XProtect LPR offers video-based content analysis (VCA) and recognition of vehicle license plates that interacts with your surveillance system and your XProtect Smart Client.

To read the characters on a plate, XProtect LPR uses optical character recognition on images aided by specialized camera settings.

You can combine LPR (license plate recognition) with other surveillance features such as recording and event-based activation of outputs.

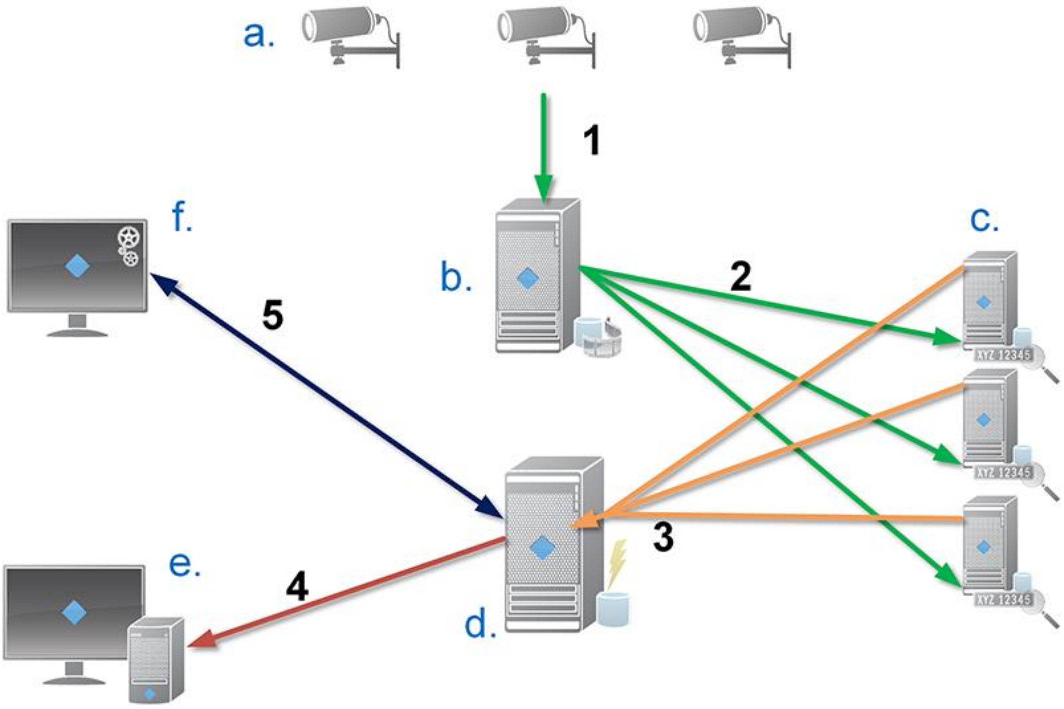
Examples of events in XProtect LPR:

- Trigger surveillance system recordings in a particular quality.
- Activate alarms.
- Match against positive/negative license plate match lists.
- Open gates.
- Switch on lights.
- Push video of incidents to computer screens of particular security staff members.
- Send mobile phone text messages.

With an event, you can activate alarms in XProtect Smart Client.

LPR system architecture

Basic data flow:



1. LPR cameras (a) send video to the recording server (b).
2. The recording server sends video to the LPR servers (c) to recognize license plates by comparing them with the license plate characteristics in the installed country modules.
3. LPR servers send recognitions to the event server (d) to match with the license plate match lists.
4. The event server sends events and alarms to XProtect Smart Client (e) when there is a match.
5. The system administrator manages the entire LPR configuration, for example, setting up events, alarms, and lists from the Management Client (f).

LPR server: The LPR server handles LPR video recorded by your surveillance system. It analyzes the video and sends information to the event server that uses it for triggering the defined events and alarms. Milestone recommends that you install the LPR server on a computer especially allocated for this purpose.

LPR camera: The LPR camera captures video as any other camera, but some cameras are dedicated for LPR use. The better suited camera you use, the more successful recognitions you will get.

Country module: A country module is a set of rules that defines license plates of a certain type and form as belonging to a certain country or region. It dictates plate and character specifics such as color, height, spacing, and similar, which is used during the recognition process.

License plate match list: A license plate match list is a user-defined list that you create. License plate match lists are collections of license plates that you want your system to treat in a special way. Once you have specified a list, you can set up events to recognize license plates on these lists and in this way trigger events and alarms.

Compatibility

XProtect LPR 2016 is compatible with the version 2014 SP3 or newer of:

- XProtect Corporate
- XProtect Expert
- Milestone Husky™ M30
- Milestone Husky™ M50.

XProtect LPR 2016 is compatible with Milestone Husky M30 and Milestone Husky M50, but these products do not currently support the full functionality of XProtect LPR 2016.

Minimum system requirements

For information about the minimum system requirements for the various components of your system, go to the Milestone website http://www.milestonesys.com/SystemRequirements.

Milestone recommends that you install the LPR server on a computer especially allocated for this purpose.

LPR licenses

XProtect LPR requires the following LPR-related licenses:

- A **base license** for XProtect LPR that covers an unlimited number of LPR servers.
- One **LPR camera license** per LPR camera you want to use in XProtect LPR.
- A **LPR country module license** for each country, state or region you need in your XProtect LPR solution. **Five** LPR country module license are included with the XProtect LPR base license. All country modules are automatically installed when you install your XProtect LPR product. However, the installed modules are by default disabled and you must enable the modules (see "Country modules tab" on page 315) that you want to use. You can only enable as many country modules as you have LPR country module licenses for.

Example: You have five LPR country module licenses and you have installed 10 country modules. Once you have selected five country modules, you cannot select any more. You must clear some of your selections before you can select other modules.

To find information about the current status of your licenses, see View LPR server information (on page 305).

To buy additional LPR licenses or country modules, contact your vendor.

About preparing cameras for LPR

LPR differs from other kinds of video surveillance. Normally, you choose cameras based on their ability to provide the best possible images for viewing by the human eye. When you choose cameras for LPR, only the area where you expect to detect license plates is important. The more clear and consistent you capture an image in that small area, the higher recognition rate you will get.

This section helps you to prepare cameras for license plate recognition, but it also introduces you to important theories about cameras and lenses that are crucial to understand in order to get optimal images.

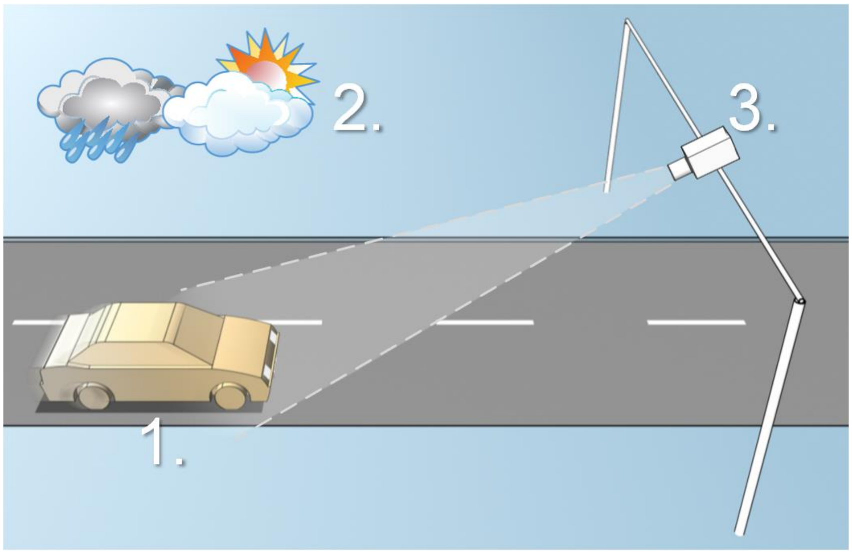


Illustration of an LPR solution

Factors that influence your configuration of LPR:

1. Vehicle

- Speed
- Plate size and position

2. Physical surroundings

- Lightning conditions
- Weather

3. Camera

- Exposure
- Field of view
- Shutter speed
- Resolution
- Positioning

It is important to take these factors into consideration as they have a critical influence on successful license plate recognition. You must mount cameras and configure XProtect LPR in a way that matches each specific environment. You cannot expect the product to run successfully without configuration. A camera used for LPR has a CPU consumption that is about five times higher than a normal camera. If a camera has not been set up correctly, it will highly affect the level of successful recognitions and the CPU performance.

Read the following sections to learn about the factors that influence your LPR solution:

Positioning the camera (on page 293)

Camera angles (on page 294)

Plate width recommendations (on page 295)

Image resolution (on page 296)

Understanding camera exposure (on page 297)

Physical surroundings (on page 300)

Lens and shutter speed (on page 301)

Contrast (on page 303)

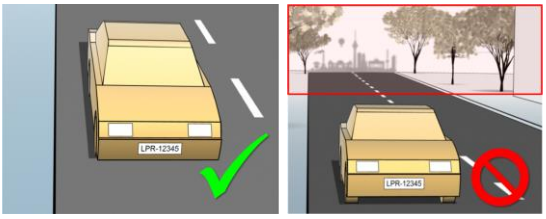
Unwanted camera features (on page 303)

Positioning the camera

When you mount cameras for LPR use, it is important to get a good, clear view of the area of interest so the plate can be detected consistently. This ensures the best possible performance and low risk of false detection:

- The area should cover **only** the part of the image where the license plate is visible as the vehicle moves in and out of the image.
- Avoid to have objects that block the view path of the camera, such as pillars, barriers, fences, gates.
- Avoid irrelevant moving objects such as people, trees, or traffic in

If too many irrelevant items are included, they will interfere with the detection, and the LPR server will use CPU resources on analyzing irrelevant items instead of license plates.

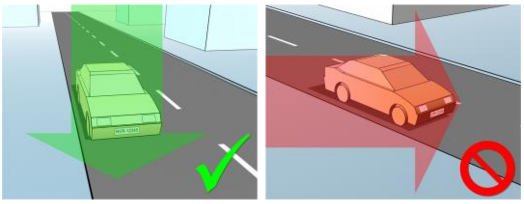


Left image shows a correct mounting without interference in the field of view. Right image shows an incorrect mounting. The camera is mounted too low and with too much background 'noise' in the view.

To help you obtain a clear and undisturbed view, you can:

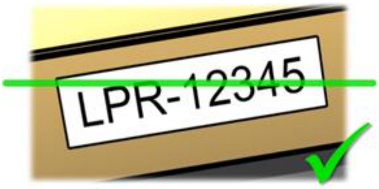
- Mount the camera as close as possible to the area of interest.
- Angle your camera.
- Zoom. If you zoom, always use the camera's optical zoom.

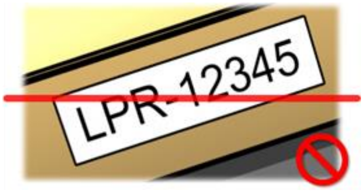
Mount the camera so the license plate appears from the top of the image (or bottom if traffic is driving away from the camera) instead of from the right or left side. In this way you make sure that the recognition process of a license plate only starts when the whole plate is in the view:



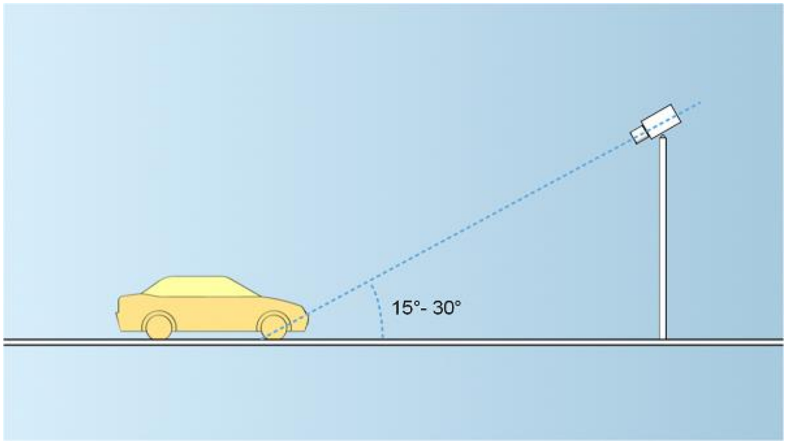
Camera angles

- **Single-line rule:** Mount the camera so that you can draw a horizontal line that crosses both the left and right edge of the license plate in the captured images. See the illustrations below for correct and incorrect angles for recognition.





- **Vertical angle:** The recommended vertical view angle of a camera used for LPR is between 15°-30°.



- **Horizontal angle:** The recommended maximum horizontal view angle of a camera used for LPR is between 15°-25°.

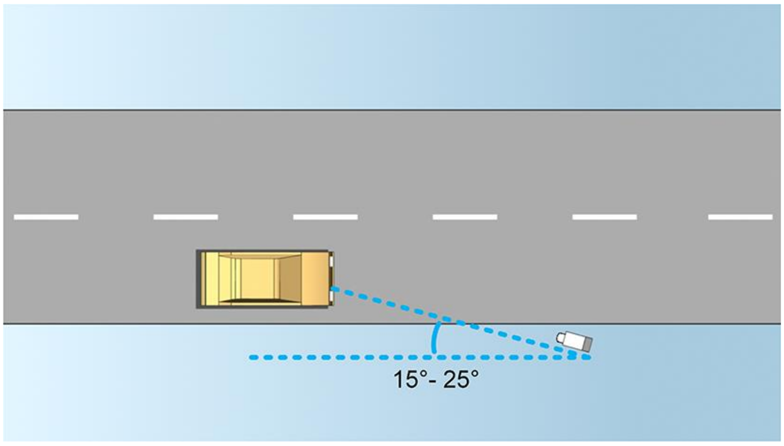
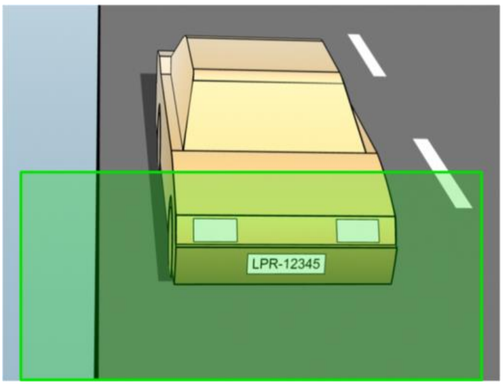


Plate width recommendations

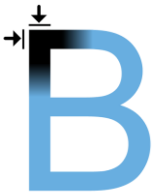
Mount the camera so that the ideal snapshot of the license plate is captured when the license plate is in the center or lower half of the image:



Take a snapshot and make sure that the requirements to stroke width and plate width as described below are fulfilled. Use a standard graphics editor to measure the amount of pixels. When you start the process of reaching the minimum plate width, begin with a low resolution on the camera, and then work your way up in a higher resolution until you have the required plate width.

Stroke width

The term *pixels per stroke* is used to define a minimum requirement for fonts that should be recognized. The following illustration outlines what is meant by *stroke*:



Because the thickness of strokes depends on country and plate style, measurements like pixels/cm or pixels/inch are not used.

The resolution for best LPR performance should be at least 2.7 pixels/stroke.

Plate width

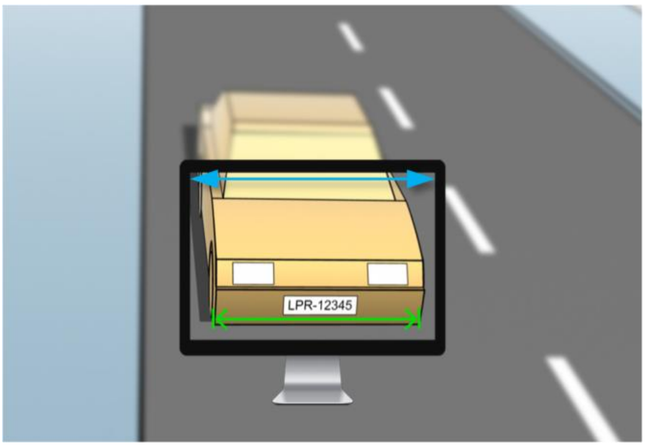
Plate type	Plate width	Setup	Minimum plate width (pixels)
Single line US plates	• plate width 12 inches • stroke width around ¼ inches	vehicles stopped; no interlacing	130
		vehicles are moving; interlaced	215
Single line European plates	• plate width 52 cm • stroke width around 1 cm	vehicles stopped; no interlacing	170
		vehicles are moving; interlaced	280

If vehicles are moving when recorded, and an interlaced camera is used, only a half of the image can be used (only the even lines) for recognition compared with a camera configured for stopped vehicles and no interlacing. This means that the resolution requirements are almost double as high.

Image resolution

Image quality and resolution is important for a successful license plate recognition. On the other hand, if the video resolution is too high, the CPU might be overloaded with the risk of skipped or faulty detections. The lower you can set the acceptable resolution, the better CPU-performance and the higher detection rate you get.

In this example we explain how to do a simple image quality calculation and find a suitable resolution for LPR. The calculation is based on the width of a car.



Example of a capture where we want to calculate a suitable resolution.

We estimate that the horizontal width is 200 cm/78 inches, as we assume the width of a standard car is 177 cm/70 inches, and besides that we add ~10% for the extra space. You can also do a physical measuring of the area of interest if you need to know the exact width.

The recommended resolution of the stroke thickness is 2.7 pixels/stroke, and the physical stroke thickness is 1 cm for a European plate and 0.27 inches for a US plate. This gives the following calculation:

Calculation for European plates in cm:

200 × 2.7 ÷ 1 = 540 pixels

Recommended resolution = VGA (640×480)

Calculation for US plates in inches:

78 × 2.7 ÷ 0.27 = 780 pixels

Recommended resolution = SVGA (800×600)

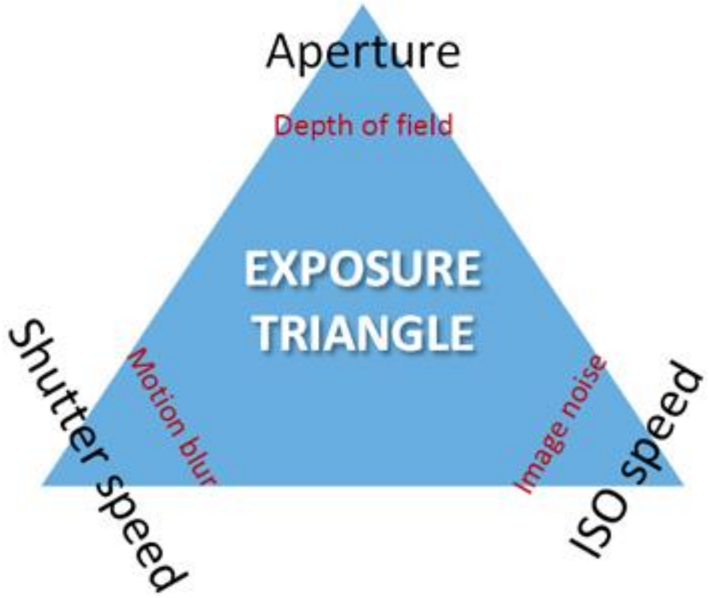
Because US plates use a font with a narrow stroke, a higher resolution is needed than for European plates.

Common video resolutions

Name	Pixels (W×H)
QCIF	176×120
CIF	352×240
2CIF	704×240
VGA	640×480
4CIF	704×480
D1	720×576
SVGA	800×600
XGA	1024×768
720p	1280×1024

Understanding camera exposure

Camera exposure determines how light/dark and sharp/blurry an image appears when it has been captured. This is determined by three camera settings: aperture, shutter speed, and ISO speed. Understanding their use and interdependency can help you to set up the camera correctly for LPR.



Exposure triangle

You can use different combinations of the three settings to achieve the same exposure. The key is to know which trade-offs to make, since each setting also influences the other image settings:

Camera settings	Controls...	Affects...
Aperture	The adjustable opening that limits the amount of light to enter the camera	Depth of field
Shutter speed	The duration of the exposure	Motion blur
ISO speed	The sensitivity of the camera's sensor to a given amount of light	Image noise

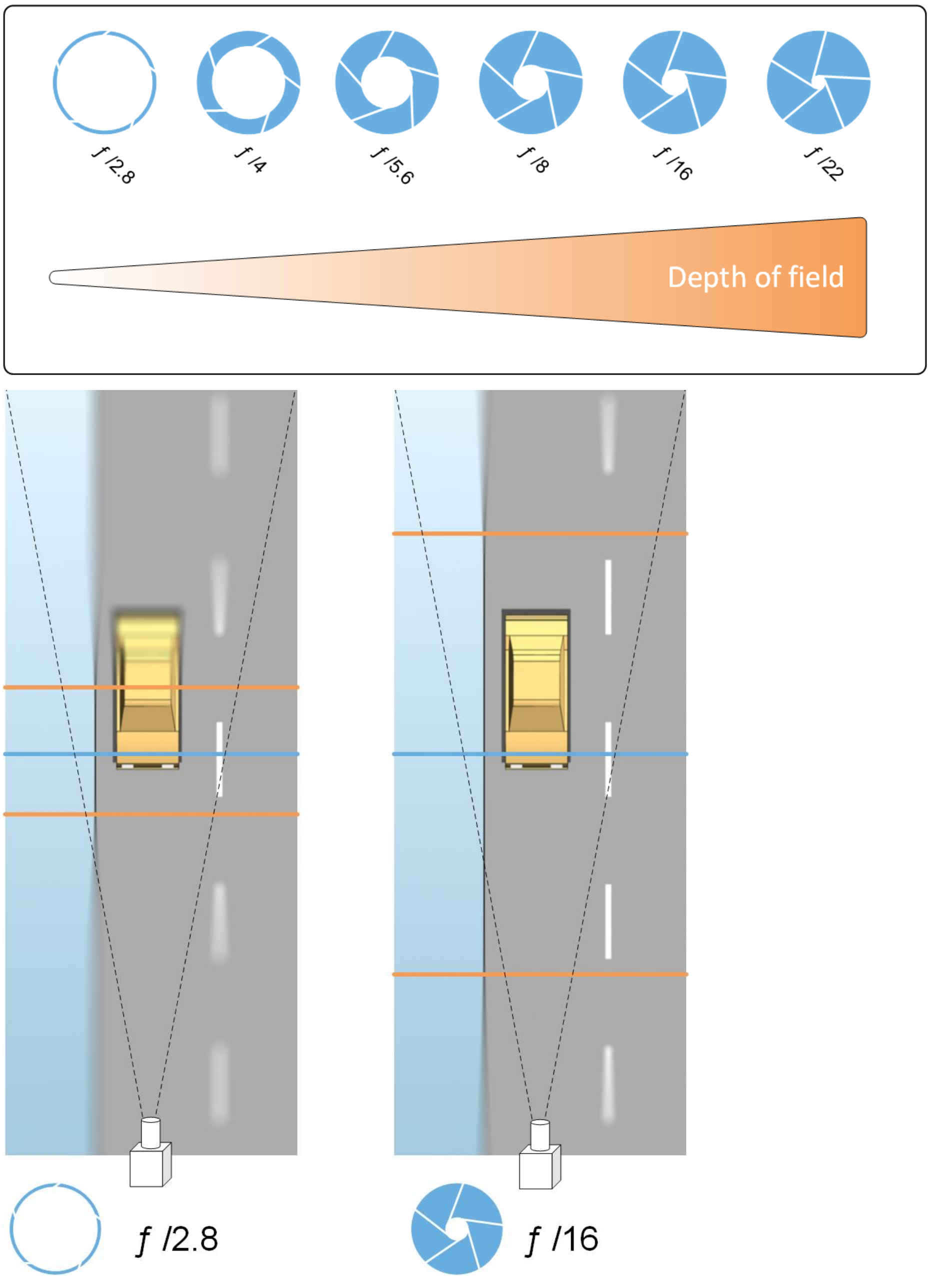
The next sections describe how each setting is specified, what it looks like, and how a given camera exposure mode affects this combination:

Aperture settings

The aperture setting controls the amount of light that enters your camera from the lens. It is specified in terms of an f-stop value, which can at times be counterintuitive, because the area of the opening increases as the f-stop decreases.

Low f-stop value/wide aperture = shallow depth of field

High f-stop value/narrow aperture = large depth of field



The example illustrates how the depth of field is affected by the f-stop value. The blue line indicates the focus point.

A high f-stop value makes it possible to have a longer distance where the license plate is in focus. Good light conditions are important for sufficient exposure. If lightning conditions are insufficient, the exposure time needs to be longer, which again increases the risk of getting blurry images.

A low f-stop value reduces the focus area and thereby the area used for recognition, but is suitable for conditions with low light. If it is possible to ensure that vehicles are passing the focus area at a low speed, a low f-stop value is suitable for a consistent recognition.

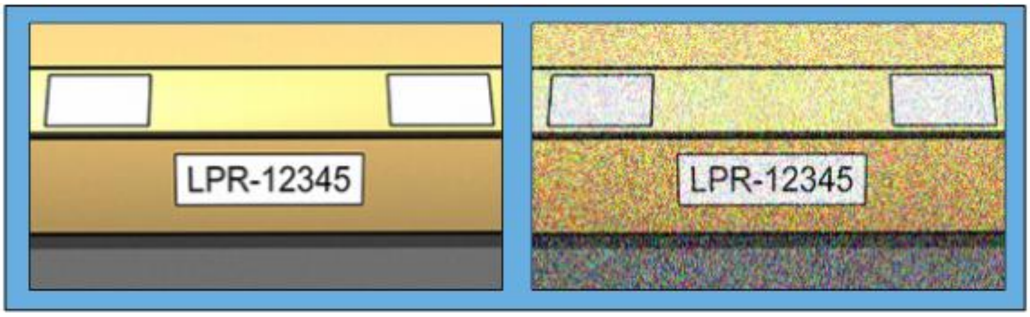
Shutter speed

A camera's shutter determines when the camera sensor is open or closed for incoming light from the camera lens. The shutter speed refers to the duration when the shutter is open and light can enter the camera. Shutter speed and exposure time refer to the same concept, and a faster shutter speed means a shorter exposure time.

Motion blur is undesired for license plate recognition and surveillance. In many occasions vehicles are in motion while license plates are detected which makes a correct shutter speed an important factor. The rule of thumb is to keep the shutter speed high enough to avoid motion blur, but not too high as this may cause under-exposed images depending on light and aperture.

ISO speed

The ISO speed determines how sensitive the camera is to incoming light. Similar to shutter speed, it also correlates 1:1 with how much the exposure increases or decreases. However, unlike aperture and shutter speed, a lower ISO speed is in general desirable, since higher ISO speeds dramatically increase image noise. As a result, ISO speed is usually only increased from its minimum value if the desired image quality is not obtainable by modifying the aperture and shutter speed settings solely.



Example of low and high ISO speed images. High ISO speed on the right image affects the level of image noise negatively.

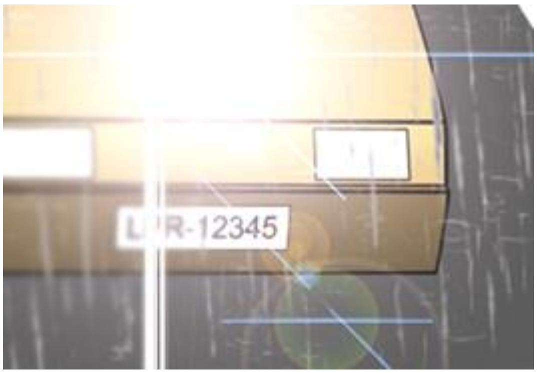
Common ISO speeds include 100, 200, 400 and 800, although many cameras also permit lower or higher values. With digital single-lens reflex (DSLR) cameras, a range of 50-800 (or higher) is often acceptable.

Physical surroundings

When you mount and use cameras for LPR, note the following factors related to the surroundings:

- **Much light:** Too much light in the surroundings can lead to overexposure or smear.
    - **Overexposure** is when images are exposed to too much light, resulting in a burnt-out and overly white appearance. To avoid overexposure, Milestone recommends that you use a camera with a high dynamic range and/or use an auto-iris lens. **Iris** is the adjustable aperture. For that reason, iris has a significant effect on the exposure of images.

- **Smear** is an effect that leads to unwanted light vertical lines in images. It is often caused by slight imperfections in the cameras' charge-coupled device (CCD) imagers. The CCS imagers are the sensors used to digitally create the images.



License plate image with smear because of overexposure

- **Little light:** Too little light in the surroundings or too little external lighting can lead to underexposure.
  - **Underexposure** is when images are exposed to too little light, resulting in a dark image with hardly any contrast (on page 303). When auto-gain (see "Unwanted camera features" on page 303) cannot be disabled or when you are not able to configure a maximum allowed shutter time (see "Lens and shutter speed" on page 301) for capturing moving vehicles, too little light will initially lead to gain noise and motion blur in the images, and ultimately to underexposure. To avoid underexposure, use sufficient external lighting and/or use a camera that has sufficient sensitivity in low-light surroundings without using gain.
- **Infrared:** Another way to overcome difficult lighting conditions is to use artificial infrared lighting combined with an infrared-sensitive camera with an infrared pass filter. Retro-reflective license plates are particularly suitable for use with infrared lighting.
  - **Retro-reflectivity** is achieved by covering surfaces with a special reflective material which sends a large portion of the light from a light source straight back along the path it came from. Retro-reflective objects appear to shine much more brightly than other objects. This means that at night they can be seen clearly from considerable distances. Retro-reflectivity is frequently used for road signs, and is also used for different types of license plates.
- **Weather:** Snow or very bright sunlight may for example require special configuration of cameras.
- **Plate condition:** Vehicles may have damaged or dirty license plates. Sometimes this is done deliberately in an attempt to avoid recognition.

Lens and shutter speed

When configuring cameras' lenses and shutter speeds for LPR, note the following:

- **Focus:** Always make sure the license plate is in focus.
- **Auto-iris:** If using an auto-iris lens, always set the focus with the aperture as open as possible. In order to make the aperture open, you can use neutral density (ND) filters or—if

the camera supports manual configuration of the shutter time—the shutter time can be set to a very short time.

  - **Neutral Density** (ND) filters or gray filters basically reduce the amount of light coming into a camera. They work as "sunglasses" for the camera. ND filters affect the exposure of images (see "Understanding camera exposure" on page 297).

- **Infrared:** If using an infrared light source, focus may change when switching between visible light and infrared light. You can avoid the change in focus by using an infrared compensated lens, or by using an infrared pass filter. Note that if you use an infrared pass filter, an infrared light source is required—also during daytime.
- **Vehicle speed:** When vehicles are moving, cameras' shutter time should be short enough to avoid motion blur. A formula for calculating the longest suitable shutter time is:
  - **Vehicle speed in km/h:** Shutter time in seconds = 1 second / (11 × max vehicle speed in kilometers per hour)
  - **Vehicle speed in mph:** Shutter time in seconds = 1 second / (18 × max vehicle speed in miles per hour)

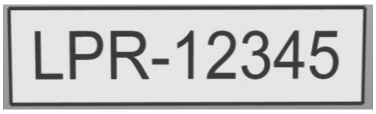
  where / denotes "divided by" and × denotes "multiplied by."

The following table provides guidelines for recommended camera shutter speeds for different vehicle speeds:

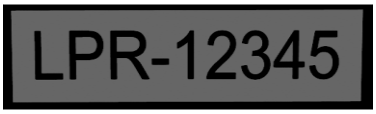
Shutter time in seconds	**Max. vehicle speed in kilometers per hour**	**Max. vehicle speed in miles per hour**
1/50	4	2
1/100	9	5
1/200	18	11
1/250	22	13
1/500	45	27
1/750	68	41
1/1000	90	55
1/1500	136	83
1/2000	181	111
1/3000	272	166
1/4000	363	222

Contrast

When you determine the right contrast for your LPR camera, consider the difference in gray value (when images are converted to 8-bit grayscale) between the license plate’s characters and the license plate’s background color:



Good contrast



Acceptable contrast; recognition is still possible

Pixels in an 8-bit grayscale image can have color values ranging from 0 to 255, where grayscale value 0 is absolute black and 255 is absolute white. When you convert your input image to an 8-bit grayscale image, the minimum pixel value difference between a pixel in the text and a pixel in the background should be at least 15.

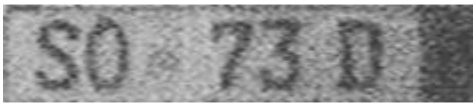
Note that noise in the image (see "Unwanted camera features" on page 303), the use of compression (see "Unwanted camera features" on page 303), the light conditions, and similar can make it difficult to determine the colors of a license plate’s characters and background.

Unwanted camera features

When you configure cameras for LPR, note the following:

- **Automatic gain adjustment:** One of the most common types of image interference caused by cameras is gain noise.
    - **Gain** is basically the way that a camera captures a picture of a scene and distributes light into it. If light is not distributed optimally in the image, the result is gain noise.

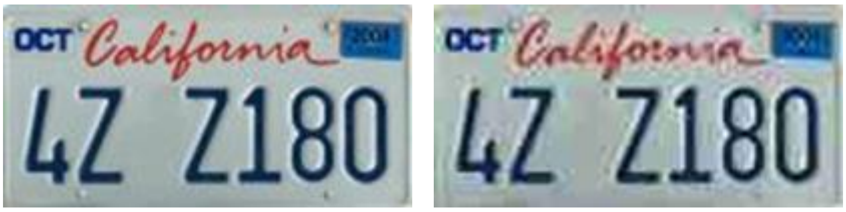
      Controlling gain requires that complex algorithms are applied, and many cameras have features for automatically adjusting gain. Unfortunately, such features are rarely helpful in connection with LPR. Milestone recommends that you configure your cameras’ auto-gain functionality to be as low as possible. Alternatively, disable the cameras’ auto-gain functionality.

      License plate image with gain noise

      In dark surroundings, you can avoid gain noise by installing sufficient external lighting.
- **Automatic enhancement:** Some cameras use contour, edge or contrast enhancement algorithms to make images look better to the human eye. Such algorithms can interfere with the algorithms used in the LPR process. Milestone recommends that you disable the cameras’ contour, edge and contrast enhancement algorithms whenever possible.
- **Automatic compression:** High compression rates can have a negative influence on the quality of license plate images. When a high compression rate is used, more resolution (see "Plate width recommendations" on page 295) is required in order to achieve optimal LPR performance. If a low JPEG compression is used, the negative impact on LPR is very low, as

long as the images are saved with a JPEG quality level of 80% or above, and images have normal resolution, contrast and focus as well as a low noise level.



Left: License plate image saved with a JPEG quality level of 80% (i.e. low compression); acceptable

Right: License plate image saved with a JPEG quality level of 50% (i.e. high compression); unacceptable

LPR installation

Install XProtect LPR

To run XProtect LPR, you must install:

- At least one LPR server.
- The LPR plug-in on all computers that run the Management Client and the event server.
- Make sure that the user selected for running the LPR Server service can access the management server.

Milestone recommends that you do not install the LPR server on the same computer as your management server or recording servers.

Start installation:

1. Go to the download page on the Milestone website http://www.milestonesys.com/downloads.
2. Download the two installers:
   - *Milestone XProtect LPR Plug-in* installer to all computers that run the Management Client and the event server.
   - *Milestone XProtect LPR Server* installer to all computers allocated for this purpose. You can also create virtual servers for LPR on one computer.
3. First, run all the *Milestone XProtect LPR Plug-in* installers.
4. Then, run the *Milestone XProtect LPR Server* installer(s).

   During installation, specify the IP address or hostname of the management server for XProtect Advanced VMS products or the image server for XProtect Professional VMS products including the domain user name and password of a user account that has administrator rights to the surveillance system.
5. Launch the Management Client.

   In the **Site Navigation pane**, your Management Client automatically lists the installed LPR servers in the **LPR Servers** list.

6. Make sure that you have the necessary licenses (see "LPR licenses" on page 291).
7. All country modules are automatically installed when you install your XProtect LPR product. However, the installed modules are by default disabled and you must enable the modules (see "Country modules tab" on page 315) that you want to use. You can only enable as many country modules as you have LPR country module licenses for.

You cannot add LPR servers from the Management Client.

If you need to install more LPR servers after the initial installation, run the *Milestone XProtect LPR Server* installer on these servers.

If an antivirus program is installed on a computer running XProtect software, it is important that you exclude the C:\ProgramData\Milestone\XProtect LPR folder. Without implementing this exception, virus scanning uses a considerable amount of system resources and the scanning process can temporarily lock files.

Upgrade XProtect LPR

To upgrade XProtect LPR, you follow the same steps as for installation (see "Install XProtect LPR" on page 304).

If you upgrade from XProtect LPR 1.0 to XProtect LPR 2016, some recognition settings are not compatible with those from the previous configuration. To apply the new settings, you must save your configuration. The settings that previously allowed you to flip, rotate and invert the colors of the video have been removed. If you still need these functions, you must change the settings on the cameras themselves.

LPR configuration

View LPR server information

To check the state of your LPR servers:

1. In the **Site Navigation pane**, expand **Servers** and select **LPR servers**. Go to the Overview pane.

   The **LPR server information** window opens with a summary of the server status:

   - Name
   - Host name
   - Status

2. Select the relevant LPR server and review all details for this server (see "LPR server information properties" on page 305).

LPR server information properties

Field	Description
Name	Here you can change the name of the LPR server.

Field	Description
Host name	Shows the LPR server host name. The first part of the name of the LPR server consists of the name of the host computer for your LPR server installation. Example: *MYHOST.domainname.country*.
Status	Shows the status of the LPR server. If the server has just been added, the status is: • *No LPR cameras configured*. If the system is running without problems, the status is: • *All LPR cameras are running*. Alternatively, the system returns: • *Service not responding.* • *Not connected to surveillance system.* • *Service not running.* • *Event Server not connected.* • *Unknown error.* • *X of Y LPR cameras running.*
Service up time	Shows the up time since the LPR server was last down and the LPR server service started.
Computer CPU usage	Shows the current CPU usage on the entire computer with the LPR server(s) installed.
Memory available	Shows how much memory is available on the LPR server.
Recognized license plates	Shows the number of license plates that the LPR server has recognized in this session.
LPR cameras	Shows a list of enabled LPR cameras that run on the LPR server and their status.
LPR cameras available	Based on your license, this number shows how many additional LPR cameras you are allowed to add and use on all your LPR servers in total.
Country modules available	Based on your license, this number shows how many additional country modules you are allowed to use on all your LPR servers in total. It also lists the number of country modules already in use.

Configuring cameras for LPR

Prerequisites in the Management Client

Once cameras have been mounted and added in the Management Client, adjust each camera's settings so that they match the requirements for LPR. You adjust camera settings on the properties tabs for each camera device.

For the relevant cameras Milestone recommends to:

- Set the video codec to JPEG.

  Note that if you use H.264 or H.265 codec, only key frames are supported. This is usually only one frame per second which is not enough for LPR. For higher frame rates, always use a JPEG codec.

- Specify a frame rate of four frames per second.
- Avoid compression, so set a fine quality.
- If possible, specify a resolution below one megapixel.
- If possible, keep automatic sharpness at a low level.

To learn about LPR fundamentals, make yourself familiar with the information in About preparing cameras for LPR (on page 291).

About snapshots

The system uses snapshots to optimize the configuration automatically and to visualize the effect of the recognition settings as they are applied.

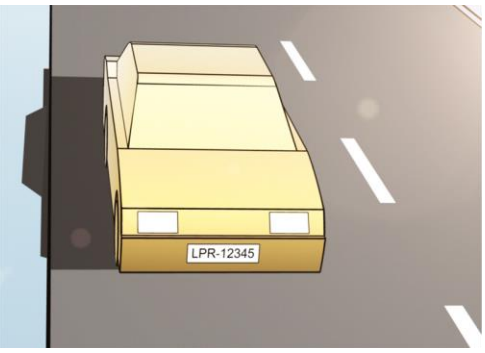
You need to provide at least one valid snapshot in order to complete the initial configuration of a camera.

As a guideline, capture snapshots of vehicles in the real physical surroundings and conditions, in which you want to be able to recognize license plates.

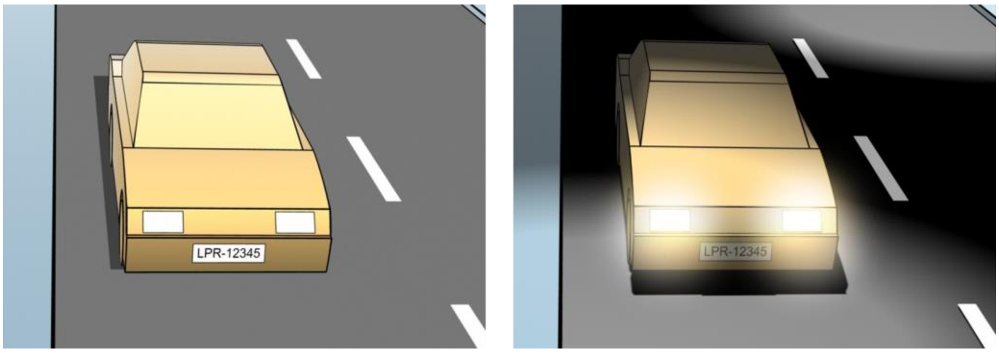
The list below illustrates examples of the situations that you should consider when you capture and select snapshots. Not all may be applicable for your surroundings.

Milestone recommends that you select minimum 5-10 snapshots that represent typical conditions of:

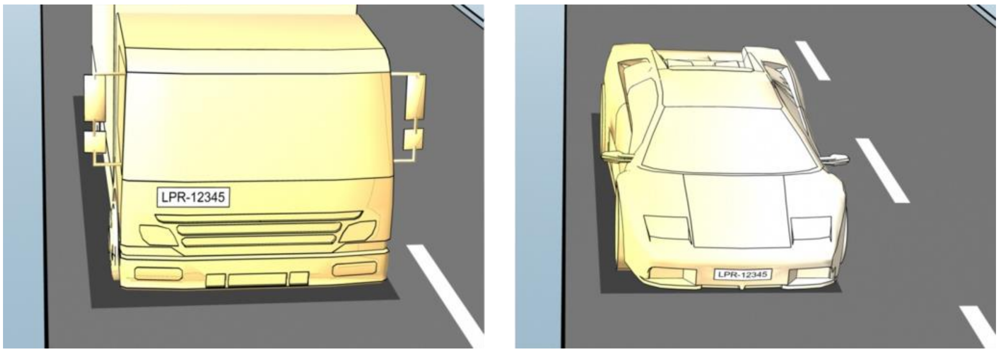
- **The weather; for example sunlight and rain**



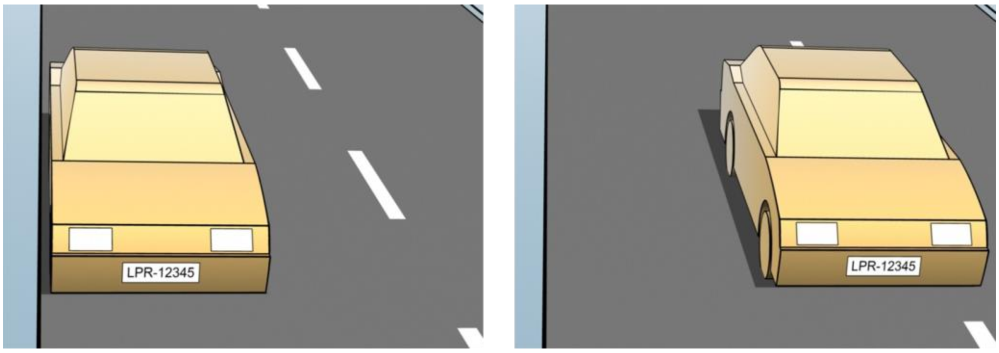
- **The light; for example daylight and nighttime**



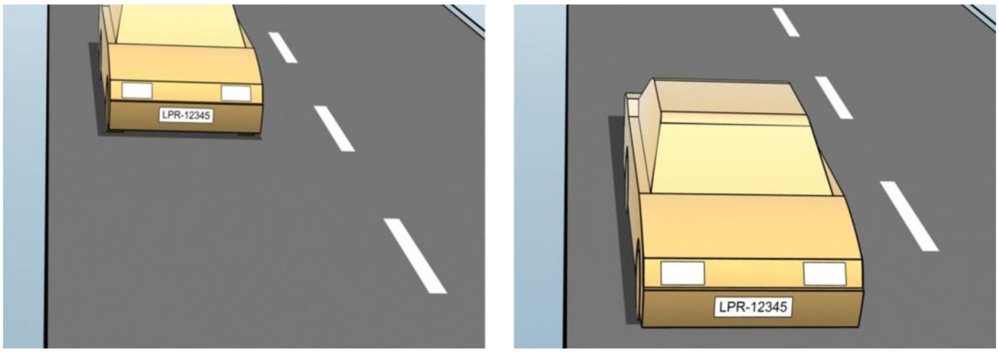
- **Vehicle types; to define the top and bottom of the recognition area**



- **Position in the lane; to define the left and right of the recognition area**



- **Distance to the car; to define the area where LPR analyzes license plates**



Add LPR camera

To configure cameras for LPR, you initially run the **Add LPR camera** wizard. The wizard takes you through the main configuration steps and automatically optimizes the configuration.

To run the wizard:

1. In the **Site Navigation pane**, expand **Servers**, expand **LPR servers**, and select **LPR camera**.
2. Go to the Overview pane. Right-click **LPR camera**.
3. From the menu that appears, select **Add LPR camera** and follow the instructions in the wizard:
   - Select the camera you want to configure for LPR.
   - Select which country modules you want to use with your LPR camera (see "Country modules tab" on page 315).
   - Select snapshots to use for validating the configuration (see "About snapshots" on page 307).
   - Validate the result of the snapshot analysis (see "Validate configuration" on page 316).
   - Select which license plate match lists to use (see "About license plate match lists" on page 317). Choose the default selection, if you have not yet created any lists.
4. On the last page, click **Close**.

   The LPR camera appears in the Management Client and based on your selections, the system has optimized the recognition settings for the camera (see "Recognition settings tab" on page 310).
5. Select the camera you have added and review its settings. You only need to change the configuration if the system does not recognize license plates as well as expected.
6. In the **Recognition settings** tab, click Validate configuration (on page 316).

Adjust settings for your LPR camera

The system automatically optimized the configuration of your LPR camera, when you added the LPR camera with the **Add LPR camera** wizard. If you want to make changes to the initial configuration, you can:

- Change the name of the server or change server (see "Info tab" on page 310).
- Adjust and validate the recognition settings (see "Recognition settings tab" on page 310).
- Add more license plate match lists (see "Match lists tab" on page 314).
- Enable additional country modules (see "Country modules tab" on page 315).

Info tab

This tab provides information about the selected camera:

Name	Description
Enable	LPR cameras are by default enabled after the initial configuration. Disable any camera that is not used in connection with LPR. Disabling an LPR camera does not stop it from performing normal recording in the surveillance system.
Camera	Shows the name of the selected camera as it appears in the XProtect Management Client and the clients.
Description	Use this field to enter a description (optional).
Change Server	Click to change LPR server. Changing the LPR server can be a good idea if you need to load balance. For example, if the CPU load is too high on an LPR server, Milestone recommends that you move one or more LPR cameras to another LPR server.

Recognition settings tab

Recognition settings are auto-configured and optimized by the system during the initial configuration of your LPR camera, primarily based on the snapshots you have provided.

Action buttons

Use these buttons to update and validate your settings after the initial configuration.

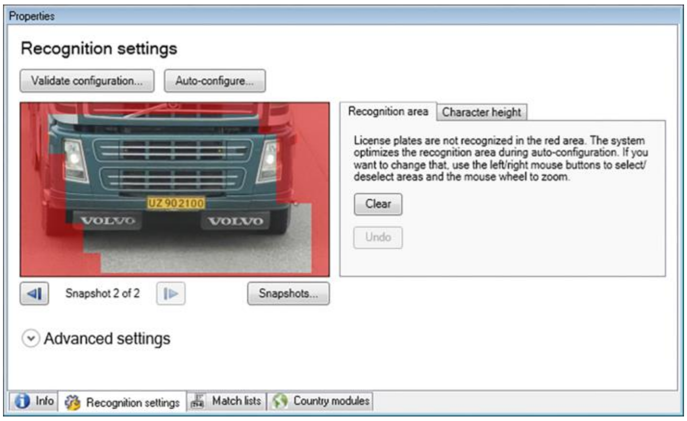
Name	Description
Snapshots	Add or delete snapshots (see "Select snapshots" on page *316*).
Validate configuration	Test that license plates are recognized as expected (see "Validate configuration" on page *316*).
Auto-configure	Disregard manual changes and optimize settings (see "Auto-configure" on page *317*).

Recognition area

The system optimizes the recognition area during auto-configuration, but you can change it manually.

To ensure the best possible performance and low risk of false detection, Milestone recommends that you always select a clearly defined and "well-trimmed" recognition area. The area should cover **only** the part of the image where the license plate is visible as the vehicle moves in and out of the image. Avoid irrelevant moving objects such as people, trees, or traffic in the recognition area (see "Positioning the camera" on page 293).

License plates are not recognized in the red area.



License plates are not recognized in the red area. The system optimizes the recognition area during auto-configuration. If you want to change that, use the left/right mouse buttons to select/deselect areas and the mouse wheel to zoom.

When you specify an area of recognition, you have the following options:

Name	Description
Clear	Click to remove all selections, so no areas are used for LPR. Select new areas.
Undo	Click to revert to your latest saved configuration of the recognition area.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 316) to see if the system recognizes license plates as well as expected.

Character height

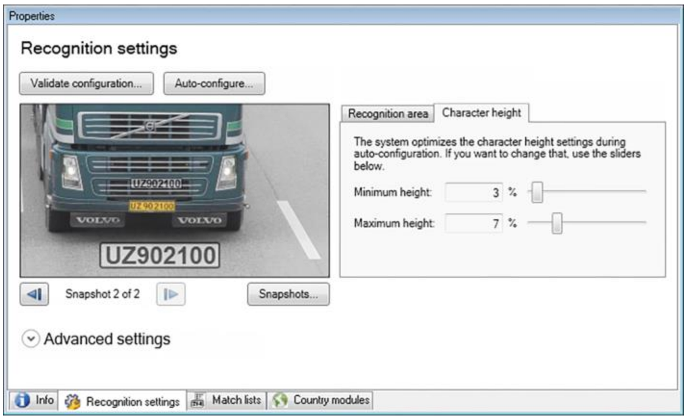
The system optimizes the character height during auto-configuration, but you can change it manually.

You define the minimum and maximum height of the license plate characters (in percent). Select character heights as close as possible to the height of the characters in the real license plate.

These character settings influence the recognition process as they partly determine the recognition time. As a rule, the larger the difference between the minimum and the maximum character height:

- The more complex the LPR process is.
- The higher the CPU load is.

- The longer you have to wait for the results.



The system optimizes the character height settings during auto-configuration. If you want to change that, use the sliders below.

Minimum height: 3 %

Maximum height: 7 %

The overlay in the snapshot displays the currently defined character height setting. The overlay grows and shrinks proportionally with the character height settings to the right. For easy comparison, you can drag the overlay on top of the real license plate in the snapshot. If needed, use the mouse wheel to zoom.

Name	Description
Minimum height	Use the sliders to set the minimum character height to be included in a recognition process. The system will not start the recognition process on license plates that contain characters below the specified value.
Maximum height	Use the sliders to set the maximum character height to be included in a recognition process. The system will not start the recognition process on license plates that contain characters above the specified value.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 316) to see if the system recognizes license plates as well as expected.

Advanced settings

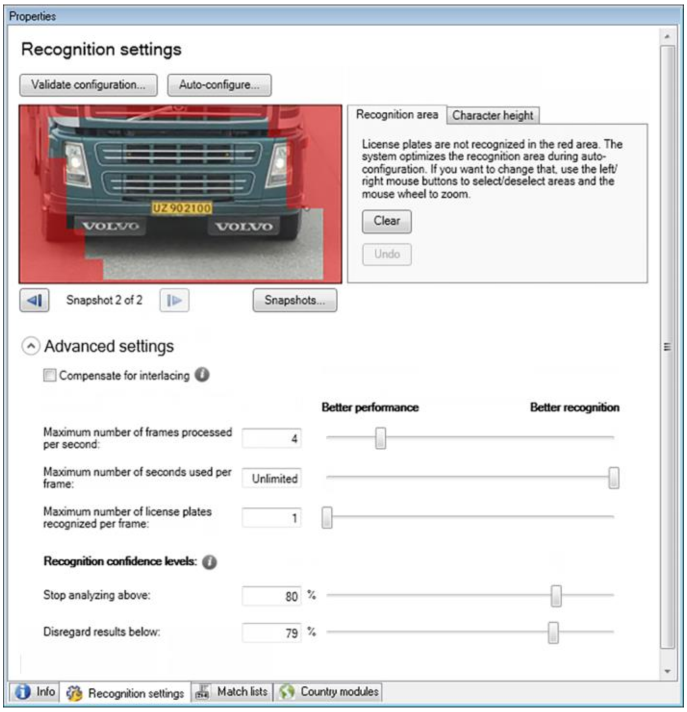
The system optimizes the advanced settings during auto-configuration, but you can change them manually.

The recognition process can be divided into two steps: finding the plate(s) and recognizing the characters on the plates. The advanced settings allow you to define a trade-off between processing speed and recognition quality.

The general rule is that high recognition quality:

- needs the highest computational effort,
- results in higher CPU load,

- requires more time to return results.



License plates are not recognized in the red area. The system optimizes the recognition area during auto-configuration. If you want to change that, use the left/ right mouse buttons to select/deselect areas and the mouse wheel to zoom.

Advanced settings

□ Compensate for interlacing

Maximum number of frames processed per second: 4

Maximum number of seconds used per frame: Unlimited

Maximum number of license plates recognized per frame: 1

Recognition confidence levels:

Stop analyzing above: 80 %

Disregard results below: 79 %

By adjusting the advanced settings, you define the trade-off. The recognition process stops if any of the stop criteria are met and returns the license plate it recognized at that point.

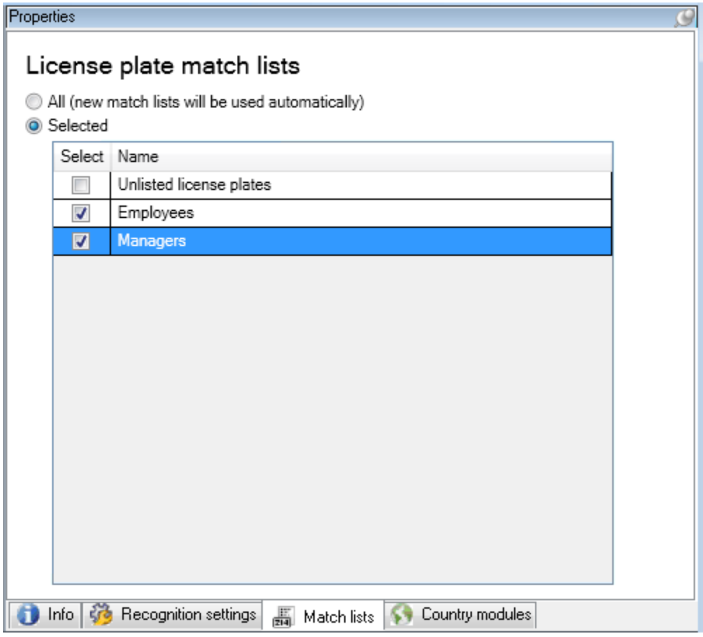
Name	Description
Compensate for interlacing	In case your LPR camera sends interlaced video and you observe combing effects in the de-interlaced image in LPR, you can enable this function. This may improve the quality of the image and thereby your recognition results.
Maximum number of frames processed per second	Specifies a limit to the number of frames that your LPR solution processes per second. If you keep the number of frames low for LPR processes, you can apply a higher frame rate on the camera for recording without adding unnecessary load to the LPR Server. **Unlimited** means that you have not defined a stop criterion for this setting.
Maximum number of seconds used per frame	Specifies a limit to the number of seconds that your LPR solution is allowed to spend on recognition of one frame. If adjusted, recommended value is *200* ms per frame. **Unlimited** means that you have not defined a stop criterion for this setting.
Maximum number of license plates recognized per frame	Specifies a limit to the number of recognized license plates returned per frame. Do only change this setting if really needed, for example, if you are detecting multiple lanes with one LPR camera. **Unlimited** means that you have not defined a stop criterion for this setting.

Name	Description
Stop analyzing above	Specifies a minimum confidence level (in percent). The recognition process continues until the system can return a license plate reading with a confidence level equal to or higher than the specified value.
Disregard results below	The system rejects license plate readings with a confidence level equal to or lower than the specified value. As a rule, the smaller you keep the difference between the **Stop analyzing above** and **Disregard results below** values, the lower is the CPU load and the system returns recognition results faster.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 316) to see if the system recognizes license plates as well as expected.

Match lists tab

On this tab you select which license plate match list(s) you want a specific LPR camera to match license plates against. You can create as many lists as you need (see "Add new license plate match lists" on page 318).



Properties

License plate match lists

○ All (new match lists will be used automatically)
● Selected

Select	Name
□	Unlisted license plates
☑	Employees
☑	Managers

Name	Description
All	License plates are matched against all available and future lists.
Selected	License plates are matched against the selected lists only. Select one or more from the available lists.

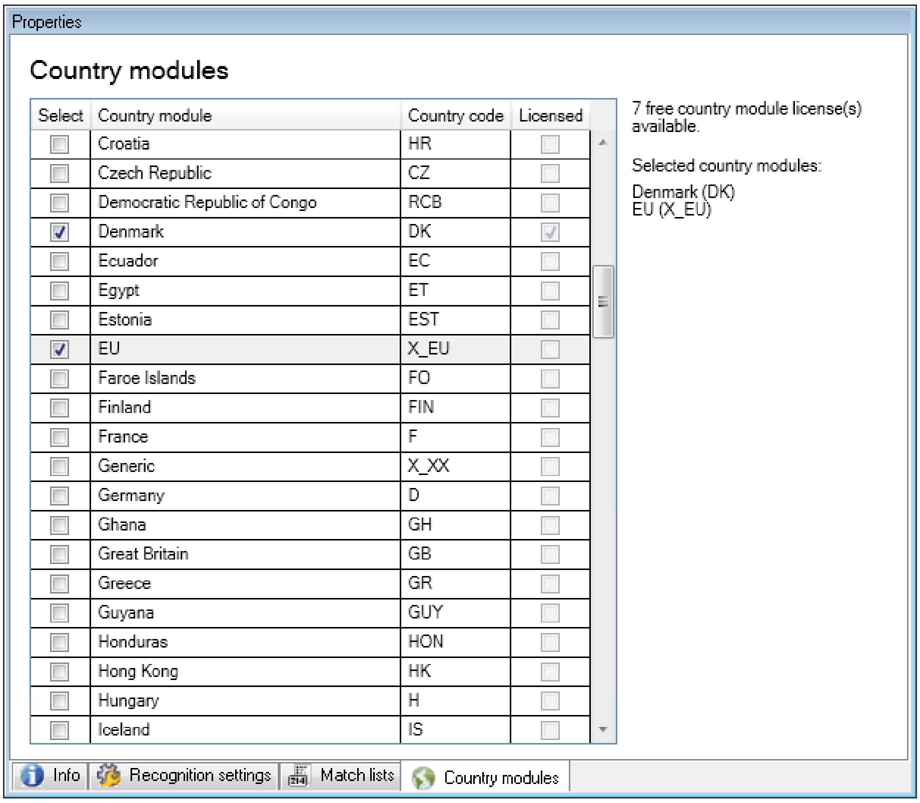
When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 316) to see if the system recognizes license plates as well as expected.

Country modules tab

Here you select the country modules that you want to use with a specific LPR camera. The list that you can select from, depends on which modules you have installed and your licenses (see "LPR licenses" on page 291).

A country module is a set of rules that defines license plates of a certain type and form belonging to a certain country, state or region.

Already licensed modules appear with a check mark in the **Licensed** column. If the country module you are looking for is not on your list, contact your vendor.



Country modules

Select	Country module	Country code	Licensed
□	Croatia	HR	□
□	Czech Republic	CZ	□
□	Democratic Republic of Congo	RCB	□
☑	Denmark	DK	☑
□	Ecuador	EC	□
□	Egypt	ET	□
□	Estonia	EST	□
☑	EU	X_EU	□
□	Faroe Islands	FO	□
□	Finland	FIN	□
□	France	F	□
□	Generic	X_XX	□
□	Germany	D	□
□	Ghana	GH	□
□	Great Britain	GB	□
□	Greece	GR	□
□	Guyana	GUY	□
□	Honduras	HON	□
□	Hong Kong	HK	□
□	Hungary	H	□
□	Iceland	IS	□

7 free country module license(s) available.

Selected country modules:

Denmark (DK)
EU (X_EU)

Name	Description
Select	Click to select or deselect a country module. The list of selected country modules on the right side updates automatically.
Country Module	Lists the installed country modules.
Country Code	Letters that identify a country module.
Licensed	Shows if a country module is already licensed. You can select a licensed country module for as many cameras as you like.

When you have changed the settings for your LPR camera, validate your configuration (see "Validate configuration" on page 316) to see if the system recognizes license plates as well as expected.

Select snapshots

When you configured the LPR initially with the **Add LPR camera** wizard, you also added snapshots (see "About snapshots" on page 307). You can always add additional representative snapshots to improve the optimization of the configuration.

1. Select the relevant camera.
2. In the **Recognition settings** tab, click **Snapshots**.
3. Capture snapshots from live video or import them from an external location. Click **Next**.

   The system analyzes the snapshots you have selected for the camera.
4. On the next page, approve or reject each of the snapshots. If the system could not recognize any license plates, click **Previous** to add new snapshots in a better quality. If the system still cannot provide correct recognitions, you probably need to change your configuration. Check that the camera is mounted and configured correctly (see "About preparing cameras for LPR" on page 291).
5. When you have approved all snapshots, click **Next** and close the wizard.
6. On the **Recognition settings** tab, click **Validate configuration** (on page 316).

Validate configuration

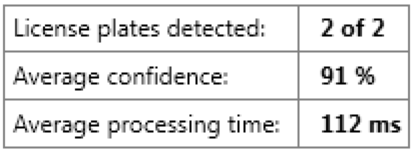
You can validate your current configuration to see if you need to change any settings or provide more snapshots. The validation function informs you about how many license plates your system recognizes, and if they are recognized correctly.

It can help you decide if your confidence level is set correctly and if your system configuration is optimal.

1. Select the relevant camera.
2. From the **Recognition settings** tab, click **Validate configuration**.

   Based on the current settings, the system analyzes the snapshots you have selected for the camera and provides a result summary:

   - **License plates detected:** The number of recognized license plates, for example, 3 of 3.
   - **Average confidence:** The average percent of confidence with which the license plates have been recognized.
   - **Average processing time**: The average time it took to analyze a snapshot and return a reading measured in ms.

License plates detected:	**2 of 2**
Average confidence:	**91 %**
Average processing time:	**112 ms**

3. If the current configuration meets your requirements, click **Close**.

4. If you want to investigate the results further, click **Next**, and you can review the results for each snapshot. This helps you to identify the situations that cause problems.

You can validate the configuration as many times as you like and on any LPR camera and with different settings.

Auto-configure

Auto-configuration of the LPR camera overwrites any manual changes you have made to the settings. You can select this option if, for example, you have made manual changes that have not given you good recognition results.

1. From the **Recognition settings** tab, click **Auto-configure**.

   A new dialog box appears.

2. Confirm that you want to return to auto-configured settings by clicking **Next**.

   The system optimizes the settings.

3. Click **Close**.

4. If prompted, confirm to save the configuration.

5. Review and validate (see "Validate configuration" on page 316) the new settings.

Working with license plate match lists

About license plate match lists

License plate lists are collections of license plates that you want your LPR solution to treat in a special way. License plate recognitions are compared with these lists and if there is a match, the system triggers an LPR event. The events are stored on the event server and can be searched for and viewed on the **LPR** tab in XProtect Smart Client.

By default, events are only stored for 24 hours. To change this, open the **Options** dialog box in the Management Client and on the **Event Server Settings** tab, in the **Keep events for** field, enter a new time frame.

When you have specified a license plate match list, you can set up additional events and alarms to be triggered on a match.

Examples:

- A company headquarter uses a list of executive management's company car license plates to grant executives access to a separate parking area. When executives' license plates are recognized, the LPR solution triggers an output signal that opens the gate to the parking area.

- A chain of gas stations creates a list of license plates from vehicles that have previously left gas stations without paying for their gas. When such license plates are recognized, the LPR solution triggers output signals that activate an alarm and temporarily block the gas supply to certain gas pumps.

Triggered events can also be used for making cameras record in high quality or similar. You can even use an event to trigger combinations of such actions.

About Unlisted license plates list

Often you would trigger an event when a license plate that is included in a list is recognized, but you can also trigger an event with a license plate, which is **not** included in a list.

> **Example:** A private car park uses a list of license plates to grant residents' vehicles access to the car park. If a vehicle with a license plate that is not on the list approaches the car park, the LPR solution triggers an output signal which lights a sign telling the driver to obtain a temporary guest pass from the security office.

To trigger a surveillance system event, when a license plate that is **not** on a list is recognized, use the **Unlisted license plates** list. You select it for a camera like any other list (see "Match lists tab" on page 314) and set it up like any other list (see "Events triggered by LPR" on page 321).

Add new license plate match lists

1. In the **Site Navigation pane**, select **License plate match lists**, right-click and select **Add New**.
2. In the window that appears, give the list a name and click **OK**.

   As soon as you have created a license plate list, it becomes visible in the **License plate match list** and on the **Match lists** tab for all your LPR cameras.
3. If you want to add columns to the match list, click **Custom field** and specify the columns in the dialog box that opens (see "Edit custom fields properties" on page 320).
4. To update the match list, use the **Add**, **Edit**, **Delete** buttons (see "Edit license plate match lists" on page 318).
5. Instead of defining the match list directly in the Management Client, you can import a file (see "Import/export license plate match lists" on page 319).
6. If prompted, confirm to save changes.

Edit license plate match lists

1. In the **Site Navigation pane**, select **License plate match lists**.
2. Go to the Overview pane. Click the relevant list.
3. The **License plate match list** i**nformation** window opens.
4. To include new rows to your list, click **Add** and fill out the fields:
   - Do not include any spaces.
   - Always use capital letters.

     Examples: *ABC123* (correct), *ABC 123* (incorrect), *abc123* (incorrect)
   - You can use wildcards in your license plate match lists. Do this by defining plates with a number of ?'s and the letter(s) and/or number(s) which must appear at specific places.

     Examples: *?????A*, *A?????*, *???1??*, *22??33*, *A?B?C?* or similar.
5. If prompted, confirm to save changes.

Import/export license plate match lists

You can import a file with a list of license plates that you want to use in a license plate match list. You have the following import options:

- Add license plates to the existing list.
- Replace the existing list.

This is useful if, for example, the lists are managed from a central location. Then all local installations can be updated by distributing a file.

Similarly, you can export the complete list of license plates from a match list to an external location.

Supported file formats are .txt or .csv.

To import:

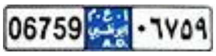
1. In the **Site Navigation pane**, click **License plate match lists** and select the relevant list.
2. To import a file, click **Import**.
3. In the dialog box, specify the location of the import file and the import type. Click **Next**.
4. Await the confirmation and click **Close**.

To export:

1. To export a file, click **Export**.
2. In the dialog box, specify the location of the export file and click **Next**.
3. Click **Close**.
4. You can open and edit the exported file in, for example, Microsoft Excel.

License plate match list properties

Name	Description
Name	Shows the name of the list. If needed, you can change the name.
Custom fields	Click to specify which license plate entry columns that you or the client user can add additional information to. See Custom fields (properties) (see "Edit custom fields properties" on page *320*).
Search	Search the list for specific license plates, numbers, patterns or similar. If needed, you can use *?* as a single wildcard

Name	Description
Add	Click to add a license plate. • Do not include any spaces. • Always use capital letters. **Examples:** *ABC123* (correct), *ABC 123* (incorrect), *abc123* (incorrect) • You can use wildcards in your license plate lists. Do this by defining plates with a number of ?'s and the letter(s) and/or number(s) which must appear at specific places. **Examples:** *?????A*, *A?????*, *???1??*, *22??33*, *A?B?C?* and similar. Some regional areas might have exceptions to these rules. For example, personalized plates with spaces. Plates with two sets of characters which must be recognized separately by an underscore character (_). Or plates from certain regions with letters on a different background color on parts of the license plate. **Example:** 
Edit	Click to edit a license plate. You can select multiple rows for editing.
Delete	Click to delete the selected license plate(s).
Import	Click to import license plates from any comma-separated file, for example a .txt-file or .csv-file (see "Import/export license plate match lists" on page *319*).
Export	Click to export the entire license plate list to a comma-separated file, for example a .txt-file or .csv-file (see "Import/export license plate match lists" on page *319*).
Rows per page	Select how many license plates to display in one page (one screen). You can choose between 50 to 1000 rows.
Events triggered by list match	Select which event(s) should be triggered by a list match (see "Events triggered by LPR" on page *321*). You can choose between all available types of events defined in your system.

Edit custom fields properties

You can add columns to your license plate match lists for additional information. You define the name and number of columns as well as the field content.

The XProtect Smart Client users can update the information in the columns but not the columns themselves.

Name	Description
Add	Adds a column to the match list. Type a name for the column.

Name	Description
Edit	Click to edit the name of the column.
Delete	Deletes a column.
Up	Changes the order of the columns.
Down	Changes the order of the columns.

Events triggered by LPR

After you have created license plate match lists (see "Add new license plate match lists" on page 318), you can associate them with all types of events defined in your system.

The type of events available depends on the configuration of your system. In connection with LPR, events are used to trigger output signals for, for example, raising of parking barrier or making cameras record in high quality. You can also use an event to trigger combinations of such actions. See About license plate match lists (on page 317) for more examples.

Set up system events triggered by list matches

1. Expand **Servers**, click **License plate match list** and select the list to which you want to associate an event.
2. In the **License plate match list information** window, next to the **Events triggered by list match** selection field, click **Select**.
3. In the **Select triggered events** dialog box, select one or more events.
4. If prompted, confirm to save changes.
5. The event is now associated with recognitions on the selected license plate match list.

To trigger a surveillance system event, when a license plate that is **not** on a list is recognized, configure the **Unlisted license plates** list.

Alarms triggered by LPR

You can associate some types of alarms with events from XProtect LPR. Do the following:

1. Create the license plate match list (see "Add new license plate match lists" on page 318) you want to match license plates against.
2. Add and configure your LPR camera(s) (see "Add LPR camera" on page 309).
3. In the **Site Navigation pane**, expand **Alarms**, right-click **Alarm Definitions** and select to create a new alarm.
4. The **Alarm Definition Information** window appears. Select the relevant properties (see "Alarm Definitions for LPR" on page 322).
5. If prompted when done, confirm to save changes.

6. Configure the alarm data settings for LPR (see "Alarm Data Settings for LPR" on page 322).

Alarm Definitions for LPR

Except for defining **Triggering events**, the settings for **Alarm Definitions** are the same for LPR as for the remaining part of the system.

To define triggering events related to LPR, select the event message to use when the alarm is triggered:

a) In the **Triggering events** field, in the top drop-down list, decide what type of event to use for the alarm. The list offers **License plate match lists** and **LPR server** events (see "Working with license plate match lists" on page 317).

   b) In the second drop-down list, select the specific event message to use. If you selected **License plate match lists** in the drop-down above, select a license plate list. If you selected **LPR server**, select the relevant LPR server event message:

   - LPR camera connection lost
   - LPR camera running
   - LPR server not responding
   - LPR server responding

For information about the remaining alarm definition settings, see the **Alarms** section.

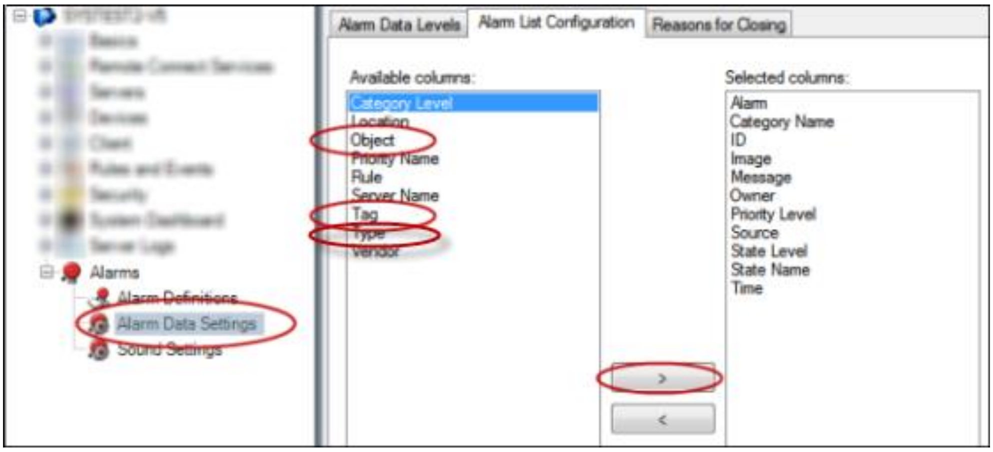
Alarm Data Settings for LPR

In the Management Client, you must make two specific **Alarm List Configuration** elements available for selection in XProtect Smart Client.

These two elements are used for configuring alarm lists in the **Alarm Manager** tab in XProtect Smart Client. The relevant elements are **Object**, **Tag**, and **Type**, which are essential for recognizing license plate numbers (Object) and country codes (Tag).

Do the following in the Management Client:

1. In the **Site Navigation pane**, expand **Alarms**, select **Alarm Data Settings**.
2. On the **Alarm List Configuration** tab, select **Object**, **Tag**, and **Type** and click **>**.



3. If prompted, confirm to save changes.

LPR maintenance

About LPR Server Manager

When you have installed an LPR server, you can check the state of its services with the XProtect LPR Server Manager. You can, for example, start and stop the LPR Server Service, view status messages, and read log files.

- You access LPR server state information via the **LPR Server Manager** icon in the notification area of the **computer running the LPR server**.

  Example: LPR Server Manager
  icon in notification area.

In the Management Client, you can get a full overview of the status of all your LPR servers (see "View LPR server information" on page 305).

Start and stop LPR Server Service

The LPR Server Service starts automatically after installation. If you have stopped the service manually, you can restart it manually.

1. Right-click the **LPR Server Manager** icon in the notification area.
2. From the menu that appears, select **Start LPR Server Service**.
3. If needed, select **Stop LPR Server Service** to stop the service again.

Show LPR server status

1. On your LPR server, right-click the **LPR Server Manager** icon in the notification area.
2. From the menu that appears, select **Show LPR server status**.

   If the system is running without problems, the status is: *All LPR cameras running*.

   Other statuses are:

   - *Service not responding*
   - *Not connected to surveillance system*
   - *Service not running*
   - *Event Server not connected*
   - *Unknown error*
   - *X of Y LPR cameras running*

Show LPR server log

Log files are a useful tool for monitoring and troubleshooting the status of the LPR Server Service. All entries are time-stamped, with the most recent entries at the bottom.

1. In the notification area, right-click the **LPR Server Manager** icon.
2. From the menu that appears, select **Show LPR server Log File**.

   A log-viewer lists the server activities with time stamps.

Change LPR server settings

The LPR server must be able to communicate with your management server. To enable this, you specify the IP address or hostname of the management server during the installation of the LPR server.

If you need to change the address of the management server, do the following:

1. Stop (see "Start and stop LPR Server Service" on page 323) the LPR Server Service.
2. In the notification area, right-click the **LPR Server Manager** icon.
3. From the menu that appears, select **Change settings**. The **LPR Server Service settings** window appears.
4. Specify the new values and click **OK**.
5. Restart the LPR Server Service.

Uninstall XProtect LPR

If you want to remove XProtect LPR from your system, uninstall the two components separately using the regular Windows removal procedure:

- On the computers where the LPR plug-in is installed, uninstall *Milestone XProtect LPR [version] Plug-in.*
- On the computers where the LPR server is installed, uninstall *Milestone XProtect LPR [version] Server.*

XProtect Transact

XProtect Transact introduction

About XProtect Transact

Available functionality depends on the system you are using. See the Product comparison chart for more information.

XProtect Transact is an add-on to Milestone's IP video surveillance solutions XProtect Advanced VMS and XProtect Professional VMS.

XProtect Transact is a tool for observing ongoing transactions and investigating transactions in the past. The transactions are linked with the digital surveillance video monitoring the transactions, for example to help you prove fraud or provide evidence against a perpetrator. There is a 1-to-1 relationship between the transaction lines and video images.

The transaction data may originate from different types of transaction sources, typically point of sales (PoS) systems or automated teller machines (ATM).

XProtect Transact system architecture

There are several components in the XProtect Transact communication flow. The input data originates from the video surveillance cameras and the transaction sources providing the transaction data, for example cash registers or ATMs. The transaction data is stored on the event server, whereas the video stream is stored on the recording server. From the servers, the data is passed on to XProtect Smart Client.

If you are using Advanced VMS, there may be several recording servers.

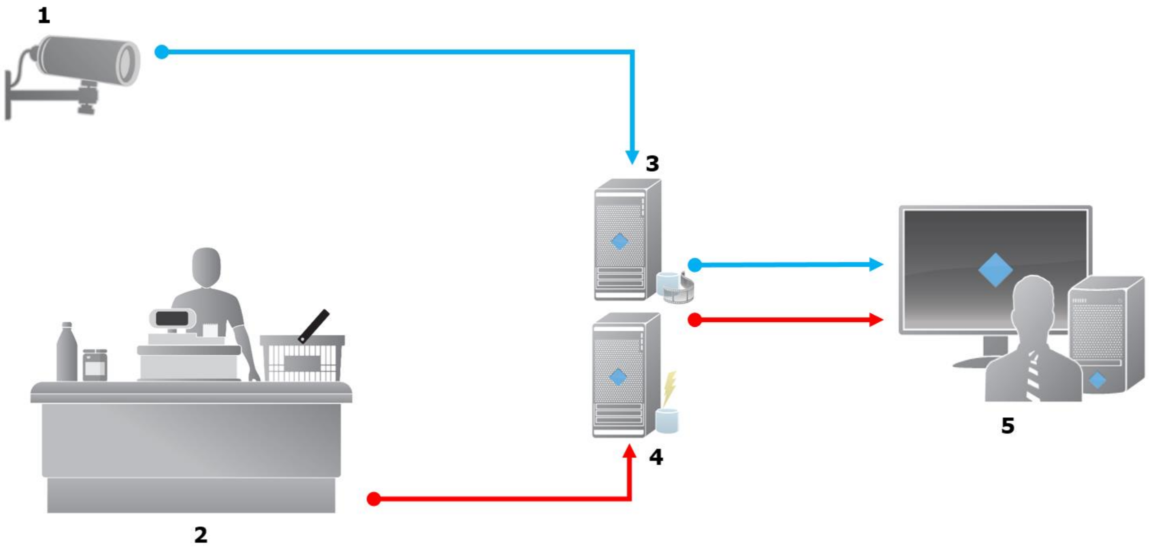


Illustration:

- 1 = Camera.
- 2 = Cash register.
- 3 = Recording server.
- 4 = Event server.
- 5 = Smart Client.
- The blue arrows outline video recordings from the surveillance system.
- The red arrows outline transaction data from the transaction sources.

By standard, XProtect Transact supports two types of transaction sources:

- Serial port clients.
- TCP server clients.

Additional types of transaction sources may be supported through custom connectors developed with the MIP software development kit (SDK), for example a connector that retrieves transaction data from an enterprise resource planning (ERP) system.

About connectors

A connector facilitates import of raw transaction data from the transaction source, for example the ATM, into the event server associated with the video management software.

The built-in connectors available are described in the table:

Name	Description
TCP client connector	Use when the transaction source delivers the transaction data through a TCP server interface. This connector has two settings that you can specify: host name and port number.
Serial port connector	Use when receiving transaction data as input on a serial port on the event server.

Connectors developed through the MIP software development kit may also be available.

See also

Add transaction source (wizard)

About transaction definitions

A transaction definition is a group of settings that help you control how raw data from the transaction sources are displayed in XProtect Smart Client together with the video recordings. The output is a reader-friendly format that resembles real-life receipts, for example till receipts and receipts from automated teller machines.

More specifically, transaction definitions let you:

- define when the individual transactions begin and end.
- insert line breaks as required.
- filter out unwanted characters or text strings, for example if the data comes from a printer connection and contains unprintable characters for indicating line breaks, when to cut off a till receipt.
- substitute characters with other characters.

You can use the same transaction definition on multiple transaction sources.

See also

Add transaction definitions

About transaction events

A transaction event is the occurrence of specific words, numbers, or characters in the stream of transaction data that flows from the transactions sources, for example the cash registers, to the event server. As a system administrator, you need to define what the events are. This allows the operator to track and investigate transaction events in XProtect Smart Client. For each event, a method (match type) must be specified to identify strings in the transaction data: exact match, wildcard, or regular expression.

See also

Define a transaction event (see "Define transaction events" on page 333)

Create a transaction alarm (see "Create alarms based on transaction events" on page 334)

Compatibility

XProtect Transact 2016 is compatible with version 2016 or newer of these products:

- XProtect Corporate
- XProtect Expert

Getting started

The XProtect Transact functionality is standard in Management Client. When you have activated the base license and transaction source licenses, the features are available immediately. Before using the XProtect Transact features in XProtect Smart Client, you should:

1. Verify that your base license for XProtect Transact has been activated. In addition, verify that you have a transaction source license for each transaction source that you need to monitor. License information is available under the **Basics** node.

   If you do not have the sufficient number of transaction source licenses, make sure that you acquire additional licenses before the 30-days grace period expires.

2. Add and configure the sources providing the transaction data, for example the cash registers. For more information, see Add transaction source (wizard) (on page 328).
3. (optional) Define the transaction events and potentially configure them to trigger rules or alarms. In XProtect Smart Client, the operator can investigate the transaction events.

Even if you have not purchased any XProtect Transact licenses, you can try out XProtect Transact with a trial license. For more information, see XProtect Transact trial license (on page 327).

See also

Setting up transactions

Setting up events (see "Setting up transaction events and alarms" on page 333)

XProtect Transact trial license

With an XProtect Transact trial license, you can try out the XProtect Transact functionality up to 30 days. All related features are enabled, and you can add one transaction source, for example a cash register. When the 30 days trial period expires, all XProtect Transact features are deactivated, including the **Transact** workspace and transaction view items. By purchasing and activating an XProtect Transact base license and the transaction source licenses you need, you can use XProtect Transact again, and your settings and data are maintained.

If you are using products from the Advanced VMS product suite, you need to acquire the trial license from Milestone. The system administrator must activate the trial license in the configuration.

If you are using products from the Professional VMS product suite, the trial license is a built-in license. The trial license is activated when the system administrator adds a transaction source in the configuration.

XProtect Transact configuration

Setting up transactions

In this section, you will learn how to add and configure the transaction sources, and how to create the transaction definitions.

Add transaction source (wizard)

To connect data from a transaction source to XProtect Transact, you need to add the sources of the transactions, for example an automated teller machine. In the wizard, you select a connector, and you can connect one or more cameras.

If you do not have a transaction source license for the transaction source you are about to add, the system will work during the 30-days grace period. Make sure that you acquire an additional transaction source license and activate it in due time.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.
2. Go to the Overview pane. Right-click the **Transaction sources** node and select **Add source**. The wizard appears.
3. Follow the steps in the wizard.
4. Depending on the connector you select, different fields appear that you need to fill in. For more information, see Transaction sources (properties) (on page 328). You can change these settings after completing the wizard.
5. If the transaction definition you need is not available, click **Add new** to create a new transaction definition.

See also

Add transaction definitions

About connectors

Transaction sources (properties)

The settings for transaction sources are described in the table.

Name	Description
Enable	If you want to disable the transaction source, clear this check box. The stream of transaction data stops, but the data already imported remains on the event server. You can still view transactions from a disabled transaction source in XProtect Smart Client during its retention period. Even a disabled transaction source requires a transaction source license.
Name	If you want to change the name, enter a new name here.
Connector	You cannot change the connector you selected when you created the transaction source. To select a different connector, you need to create a new transaction source, and during the wizard, select the connector you want.
Transaction definition	You can select a different transaction definition that defines how to transform the transaction data received into transactions and transaction lines. This includes defining: • when a transaction begins and ends. • how transactions are displayed in XProtect Smart Client.
Retention period	Specify, in days, for how long transaction data is maintained on the event server. The default retention period is 30 days. When the retention period expires, automatically the data is deleted. This is to avoid the situation, where the storage capacity of the database is exceeded. The minimum value is 1 day, whereas the maximum value is 1000 days.
TCP client connector	If you selected **TCP client connector**, specify these settings: • **Host name**: enter the host name of the TCP server associated with the transaction source. • **Port**: enter the port name on the TCP server associated with the transaction source.

Name	Description
Serial port connector	If you selected **Serial port connector**, specify these settings and make sure that they match the settings on the transaction source: • **Serial port**: select the COM port. • **Baud rate**: specify the number of bits transmitted per second. • **Parity**: specify the method for detecting errors in the transmissions. By default, **None** is selected. • **Data bits**: specify the number of bits used to represent one character of data. • **Stop bits**: specify the number of bits to indicate when a byte has been transmitted. Most devices need 1 bit. • **Handshake**: specify the handshaking method determining the communication protocol between the transaction source and event server.

See also

Add transaction source (wizard) (on page 328)

Add transaction definitions

Add transaction definitions

As part of defining a transaction source, you specify a definition for the source. A definition transforms the raw data received into presentable data, so that users can view the data in XProtect Smart Client in a format that matches real-life receipts. This is necessary, because typically the raw data consists of a single string of data, and it can be difficult to see where the individual transactions begin and end.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.
2. Select **Transaction definitions**.
3. Go to the Overview pane. Right-click **Transaction definition** and select **Add new**. A number of settings appear in the **Properties** section.
4. Use the **Start pattern** and **Stop pattern** fields to specify what data defines the start and end of a receipt.
5. Click **Start collecting data** to collect raw data from the connected data source. The more data you collect, the smaller the risk of missing characters, for example control characters, you want to replace or omit.
6. In the **Raw data** section, highlight the characters you want to replace or omit. If you want to type the characters manually, skip this step and click **Add filter**.

7. Click **Add filter** to define how the selected characters from the transaction source data are displayed in XProtect Smart Client.

8. For each filter, select an action to determine how the characters are transformed. The **Preview** section gives you a preview of how data is presented with the filters defined.

For detailed information about the fields, see Transaction definitions (properties).

You can also load previously collected data stored locally on your computer. To do this, click **Load from file**.

Transaction definitions (properties)

The settings for transaction definitions are described in the table.

Name	Description
Name	Type a name.
Encoding	Select the character set used by the transaction source, for example the cash register. This helps XProtect Transact convert the transaction data to understandable text that you can work with when configuring the definition. If you select the wrong encoding, the data may appear as non-sense text.
Start collecting data	Collect transaction data from the connected transaction source. You can use the data to configure a transaction definition. Wait for at least one, but preferably more, transactions to complete.
Stop collecting data	When you have collected sufficient data to configure the definition, click this button.
Load from file	If you want to import data from an already existing file, click this button. Typically this is a file that you have created previously in the file format .capture. It can be other file formats. What is important here is that the encoding of the import file matches the encoding selected for the current definition.
Save to file	If you want to save the collected raw data to a file, click this button. You can reuse it later.

Name	Description
Match type	Select the match type to use to search for the start mask and the stop mask in the collected raw data: • Use exact match: The search identifies strings that contain exactly what you have entered in the **Start mask** and **Stop mask** fields. • Use wildcards: The search identifies strings that contain what you have entered in the **Start mask** and **Stop mask** fields in combination with a wild card symbol (*, #, ?). * matches any number of characters. For example, if you have entered "Start tra*tion", the search identifies strings that contain "Start transaction". # matches exactly 1 digit. For example, if you have entered "# watermelon", the search identifies strings that contain, for example, "1 watermelon". ? matches exactly 1 character. For example, you may use the search expression "Start trans?ction" to identify strings that contain "Start transaction". • Use regular expression: Use this match type to identify strings that contain specific notation methods or conventions, for example a date format or credit card number. For more information, see the Microsoft website https://msdn.microsoft.com/en-us/library/az24scfc(v=vs.110).aspx.
Raw data	Transaction data strings from the connected transaction source are displayed in this section.
Start mask	Specify a start mask to indicate where a transaction begins. Horizontal lines are inserted in the **Preview** field to visualize where the transaction starts and ends, and will help to keep individual transactions separated.
Stop mask	Specify a stop mask to indicate where a transaction ends. A stop mask is not mandatory, but is useful if the received data contains irrelevant information, such as information about opening hours or special offers, between actual transactions. If you do not specify a stop mask, the end of the receipt is defined in terms of where the next receipt starts. The start is determined by what is entered in the **Start mask** field.
Add filter	Use the **Add filters** button to point out the characters that you want to be omitted in XProtect Smart Client or replaced by other characters or a line break. Replacing characters is useful when the transaction source string contains control characters for non-printing purposes. Adding lines breaks is necessary to make receipts in XProtect Smart Client resemble the original receipts.

Name	Description
Filter text	Displays the characters currently selected in the **Raw data** section. If you are aware of characters that you want to be omitted or replaced, but they do not occur in the collected raw data string, you can enter the characters manually in the **Character** field. If the character is a control character, you need to enter its hexadecimal byte value. Use this format for the byte value: {XX} and {XX,XX,...} if a characters consists of more bytes.
Action	For each filter you add, you should specify how the characters you have selected are handled: • Omit: the characters you select are filtered out. • Substitute: the characters you select are replaced with the characters you specify. • Add line break: the characters you select are replaced by a line break.
Substitution	Type the text to replace the characters selected. Only relevant if you have selected the action **Substitute**.
Preview	Use the **Preview** section to verify that you have identified and filtered out unwanted characters. The output you see here resembles what the real-life receipt looks like in XProtect Smart Client.

See also

Add transaction definitions

Setting up transaction events and alarms

In this section, you will learn how to define the transaction events and set up alarms.

Define transaction events

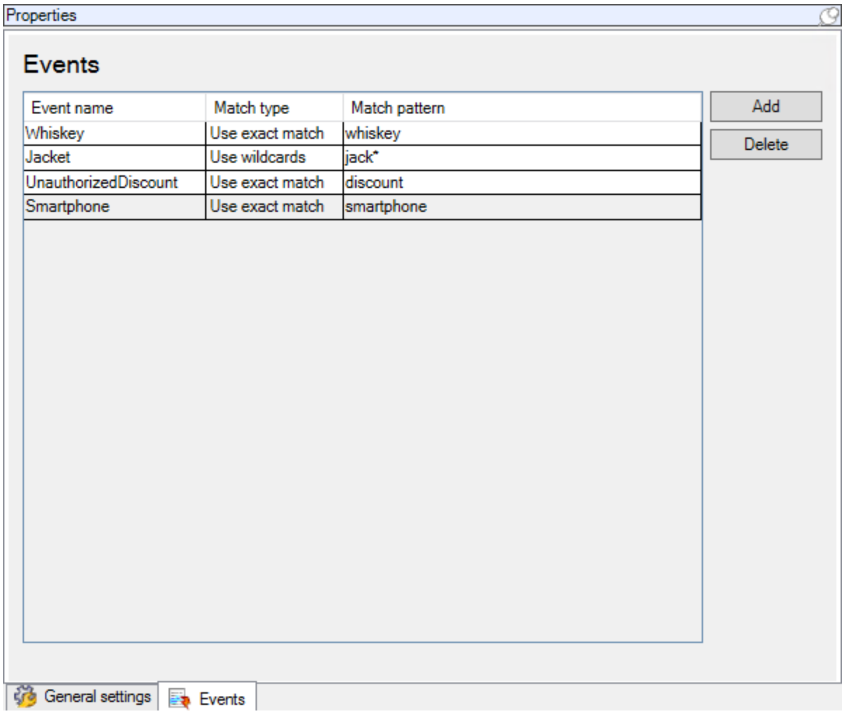
To track and investigate transaction events in XProtect Smart Client, first you need to define what the events are, for example the acquisition of a smartphone. You define transaction events on a transaction definition, so that the events defined apply to all transaction sources, for example cash registers, that use the transaction definition.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.

2. Go to the Overview pane. Select the transaction definition, where you want to define an event.

3. Click the **Events** tab.



Event name	Match type	Match pattern
Whiskey	Use exact match	whiskey
Jacket	Use wildcards	jack*
UnauthorizedDiscount	Use exact match	discount
Smartphone	Use exact match	smartphone

4. In the **Properties** pane, click **Add**. A new line is added.

5. Type a name for the event.

6. Select the match type to use to identify a specific string in the transaction data as an event. You can choose between exact match, wildcard symbols, and regular expressions. For more information, see the description of match type in Transaction definitions (properties).

7. In the **Match pattern** column, specify what you want the system to identify as an event, for example "smartphone".

8. For each event, repeat the steps above.

See also

About rules and events (on page 158)

About transaction definitions (on page 326)

Create alarms based on transaction events

To notify the XProtect Smart Client operator whenever a specific transaction event occurs, first you need to create a transaction alarm in Management Client. The alarm will appear on the **Alarm Manager** tab in XProtect Smart Client allowing the operator to investigate the event and, if required, take action.

Steps:

1. In the **Site Navigation pane**, expand **Alarms**.

2. Go to the Overview pane. Right-click the **Alarm Definitions** node and select **Add New...**. The settings in the **Properties** pane become active.
3. Type a name for the alarm and, in the **Description** field, possibly also instructions for XProtect Smart Client operator on what action to take.
4. In the **Triggering event** drop-down menu, select **Transaction events.**
5. In the drop-down menu below **Transaction events**, select the specific event.
6. In the **Sources** field, click the **Select...** button. A pop-up window appears.
7. Click the **Servers** tab and select the transaction source.
8. Specify additional settings. For more information, see Alarm Definitions (see "Alarm Definitions (properties)" on page 239).

See also

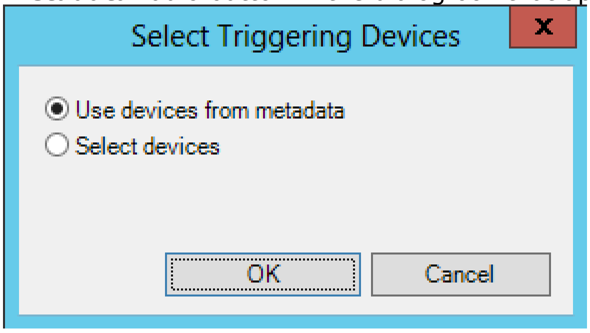
Define transaction events (on page 333)

Set up rules on an event

To trigger an action when a specific transaction event occurs, you need to configure a rule, where you select an event and specifies what needs to happen, for example that a camera starts recording or an e-mail is sent.

Steps:

1. In the **Site Navigation pane**, expand **Rules and Events**.
2. Go to the Overview pane. Right-click **Rules** and select **Add Rule...**. A wizard appears.
3. Follow the steps in the wizard.
4. Make sure that the **Perform an action on <event>** radio button is selected.
5. Select the transaction event under **Transact** > **Transaction events**.
6. If an action involves recording, and you want to use the cameras associated with the transaction sources, for example the cash registers, select the **Use devices from metadata** radio button in the dialog box that appears during the wizard.



See also

Define transaction events (on page 333)

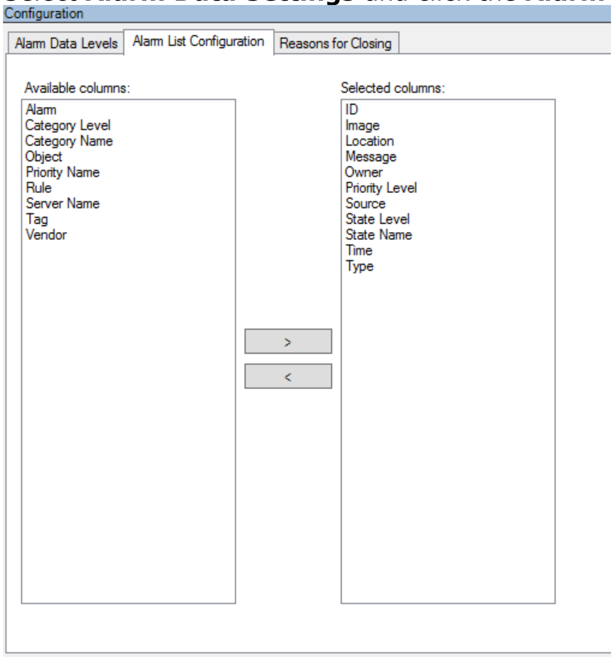
About rules and events (on page 158)

Enable filtering of transaction events or alarms

If you want the XProtect Smart Client operator to be able to filter events or alarms by transactions, first you need to enable the **Type** field in Management Client. Once enabled, the field is available in the filter section on the **Alarm Manager** tab in XProtect Smart Client.

Steps:

1. In the **Site Navigation pane**, expand **Alarms**
2. Select **Alarm Data Settings** and click the **Alarm List Configuration** tab.



Available columns:
Alarm
Category Level
Category Name
Object
Priority Name
Rule
Server Name
Tag
Vendor

Selected columns:
ID
Image
Location
Message
Owner
Priority Level
Source
State Level
State Name
Time
Type

3. In the **Available columns** section, select the **Type** field.
4. Add the field to **Selected columns**.
5. Save the changes. Now, the field is available in XProtect Smart Client.

Maintaining transaction setup

In this section, you will learn how to edit, disable, and delete transaction sources.

Edit transaction source settings

After adding a transaction source, you can change the name or select a different transaction definition. Depending on the connector selected, there may be additional settings you can modify, for example the host name and port number of a connected TCP server. In addition, you can disable a transaction source. This will interrupt the flow of transaction data from the transaction source to the event server.

Once you have selected a connector, you cannot change it.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.

2. Select **Transaction sources**.
3. Go to the Overview pane. Click the transaction source. The properties are displayed.
4. Make the required changes and save them. For more information, see Transaction sources (properties) (on page 328).

See also

Add transaction source (wizard)

Disable transaction sources (on page 337)

Disable transaction sources

You can disable a transaction source, for example if an ATM is temporarily out of order, or a service on a registered cash register is disabled. The flow of transaction data to the event server is disrupted.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.
2. Select **Transaction sources**.
3. Go to the Overview pane. Click the transaction source. The properties are displayed.
4. Clear the **Enable** check box and save the changes. The transaction source is disabled.

See also

Add transaction source (wizard)

Delete transaction source (see "Delete transaction sources" on page 337)

Delete transaction sources

You can delete the transaction sources you have added. The stored transaction data from that source is deleted from the event server.

As an alternative, you can disable the transaction source to avoid that stored transaction data is deleted. A disabled transaction source also requires a transaction source license.

Steps:

1. In the **Site Navigation pane**, expand **Transact**.
2. Select **Transaction sources**.
3. Go to the Overview pane. Click the **Transaction sources** item. Right-click the source you want to delete.
4. Select **Delete**. A dialog box appears.
5. Click **OK** to confirm that you want to delete the transaction source.

See also

Add transaction source (wizard)

Verify XProtect Transact configuration

When you are done configuring XProtect Transact and its components, you can test that Transact works as expected in XProtect Smart Client.

1. Verify that the all required transaction sources have been added correctly in Management Client:

1. Open XProtect Smart Client and click the **Transact** tab.

    2. Click the **All sources** drop-down menu and verify that all the transaction sources appear.

2. Verify that the transaction definitions have been configured correctly in Management Client. If configured correctly, there is one receipt per transaction, and the lines break correctly:

1. Open XProtect Smart Client and click the **Transact** tab.

    2. Select a transaction source that you know is active and click 🔄. The transaction lines for today appear.

    3. Click a line to view the associated receipt and video recordings.

3. Verify that transaction events are configured correctly:

1. Define a transaction test event in Management Client, for example an item that is likely to be purchased and registered on a connected transaction source, for example a cash register.

    2. When the event has occurred, open XProtect Smart Client and click the **Alarm Manager** tab.

    3. Open the alarm list and select **Event**. The most recent events are displayed at the top of the list. The test event you created should appear in the list.

Milestone Mobile

Milestone Mobile introduction

About Milestone Mobile

Milestone Mobile consists of three components:

- **Milestone Mobile client**
- **Milestone Mobile server**
- **Milestone Mobile plug-in**

The Milestone Mobile client is a mobile surveillance app that you can install and use on your Android device, Apple device or Windows 8 Phone device. You can use as many installations of Milestone Mobile client as you need.

For more information, download the Milestone Mobile Client User Guide from the Milestone Systems website http://www.milestonesys.com/support/manuals-and-guides/.

The Milestone Mobile server and Milestone Mobile plug-in are covered in this manual.

Prerequisites for using Milestone Mobile

Before you can start using Milestone Mobile, you must make sure that you have the following:

- A running VMS installed and configured with at least one user.
- Cameras and views set up in XProtect® Smart Client.
- A mobile device running Android, iOS or Windows 8 with access to Google Play, App Store℠ or Windows Phone Store from which you can download the Milestone Mobile client application.

Milestone Mobile configuration

About Milestone Mobile server

Milestone Mobile server handles log-ins to the system from Milestone Mobile client from a mobile device or XProtect Web Client.

A Milestone Mobile server distributes video streams from recording servers to Milestone Mobile clients. This offers a secure setup where recording servers are never connected to the Internet. When a Milestone Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

You must install Milestone Mobile server on any computer from which you want to access recording servers. When you install Milestone Mobile server, make sure you log in using an account that has administrator rights. Otherwise, installation will not complete successfully.

About Milestone Federated Architecture and master/slave servers

If your system supports Milestone Federated Architecture or servers in a master/slave setup, you can access such servers with your Milestone Mobile client. Use this functionality to gain access to all cameras on all slave servers by logging in to the master server.

If in a Milestone Federated Architecture setup, you gain access to child sites via the central site. Install the Milestone Mobile server only on the central site.

This means that when users of the Milestone Mobile client log in to a server to see cameras from all servers in your system, they must connect to the IP address of the master server. Users must have administrator rights on all servers in the system in order for the cameras to show up in the Milestone Mobile client.

Add or edit a Mobile server

1. Go to **Servers** > **Mobile Servers**. From the menu that appears, select **Create New**. Enter or edit the settings.

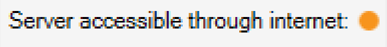
Important: If you edit settings for **Login method**, **All cameras view**, and **Outputs and events** while you or others are connected to the Milestone Mobile client, you must restart the Milestone Mobile client for the new settings to take effect.

Set up Smart Connect

Enable Universal Plug and Play discoverability on your router

To make it easy to connect mobile devices to Milestone Mobile servers, you can enable Universal Plug and Play (UPnP) on your router. UPnP enables Milestone Mobile server to configure port forwarding automatically. However, you can also manually set up port forwarding on your router by using its web interface. Depending on the router, the process for setting up port mapping can differ. If you are not sure how to set up port forwarding on your router, see the documentation for that device.

Note: Every five minutes, the Milestone Mobile server service verifies that the server is available to users on the Internet. The status displays in the upper left corner of the **Properties** pane:



Server accessible through internet: ●

.

Requirements

- Your Milestone Mobile server must use a public IP address. The address can be static or dynamic, but typically it's a good idea to use static IP addresses.
- You must have a valid license for Smart Connect.

Configure connection settings

1. In Management Client, in the navigation pane, expand **Servers**, and select **Mobile Server**.
2. Select the server and click the **Connectivity** tab.
3. Use the options in the **General** group to specify the following:
    - To make it easy for users to connect mobile devices to Milestone Mobile servers, select the **Enable Smart Connect** check box.
    - Specify the protocol to use in the **Connection type** field.
    - **Note:** If you turn on secure connections, devices running iOS 9.0 or later, or Windows Phone, can connect only if you have a certificate from a certificate authority (CA) installed on your Milestone Mobile server. CAs issue digital certificates that verify the identities of users and websites that exchange data on the Internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy.
    - Before you turn on secure connections, make sure that you are familiar with digital certificates. To learn how to add a certificate in Milestone Mobile server, see Edit certificates (see "Edit certificate" on page 354).
    - Specify the number of seconds before the connection times out.
    - To let mobile devices find the Milestone Mobile servers that are within range, select the **Enable UPnP discoverability** check box.
    - To enable routers to forward mobile devices to a specific port, select the **Enable automatic port mapping** check box.

Send an email message to help users connect

You can make it easy for users to get started with Milestone Mobile by sending them an email message that includes connection information. You can send the message directly from Management Client, or you can copy the information to the messaging program you use.

1. In the **Email invitation to** field, enter the email address for the recipient, and then specify a language.
2. Next, do one of the following:
    - To send the message, click **Send**.
    - Copy the information to the messaging program you use.

Enable connections on a complex network

If you have a complex network where you have custom settings, you can provide the information users need to connect.

In the **Internet Access** group, specify the following:

- If you use UPnP port mapping, to direct connections to a specific connection, select the **Configure custom Internet access** check box. Then provide the **IP address or hostname**, and the port to use for the connection. For example, you might do this if your router does not support UPnP, or if you have a chain of routers.
- If your IP addresses often change, select the **Check to retrieve IP address dynamically** check box.

Set up investigations

Set up investigations so that people can use Web Client and Milestone Mobile to access recorded video and investigate incidents, and prepare and download video evidence.

To set up investigations, follow these steps:

1. In Management Client, click the mobile server, and then click the **Investigations** tab.
2. Select the **Enabled** check box. By default, the check box is selected.
3. In the **Investigations folder** field, specify where to store video for investigations.
4. In the **Limit size of investigations to** field, enter the maximum number of megabytes that the investigation folder can contain.
5. Optional: To allow users to access investigations that other users create, select the **View investigations made by others** check box. If you do not select this check box, users can see only their own investigations.
6. Optional: To include the date and time that a video was downloaded, select the **Include timestamps for AVI exports** check box.
7. In the **Used codec for AVI exports** field, select the compression format to use when preparing AVI packages for download.

   Note: The codecs in the list can differ, depending on your operating system. If you do not see the codec you want to use, you can install it on the computer where Management Client is running and it will display in this list.

   Additionally, codecs can use different compression rates, which can affect video quality. Higher compression rates reduce storage requirements but can also reduce quality. Lower compression rates require more storage and network capacity, but can increase quality. It's a good idea to research the codecs before you select one.

8. In the **Failed export data (for MKV and AVI export)** field, specify whether to keep the data that was successfully downloaded, although it can be incomplete, or delete it.
9. To enable users to save investigations, you must grant the following permissions to the security role assigned to the users:
   - In XProtect Advanced VMS products, grant the **Export** permission.
   - In XProtect Professional VMS products, grant the **Database** permission.

Clean up investigations

If you have investigations or video exports that you no longer need to keep, you can delete them. For example, this can be useful if you want to make more disk space available on the server.

- To delete an investigation, and all of the video exports that were created for it, select the investigation in the list, and then click **Delete**.
- To delete individual video files that were exported for an investigation, but keeping the investigation, select the investigation in the list. In the **Investigation details** group, click the **Delete** icon to the right of the **Database**, **AVI**, or **MKV** fields for exports.

About sending notifications

You can enable Milestone Mobile to notify users when an event occurs, such as when an alarm triggers or something goes wrong with a device or server. When Milestone Mobile is open on the mobile device, the app delivers the notification. Users can specify the types of notifications they want to receive. For example, a user can choose to receive notifications for the following:

- All alarms
- Only alarms that they own
- Only alarms related to the system. These might be when a server goes offline or comes back online.

You can also use push notifications to notify users who don't have Milestone Mobile open. These are called push notifications. Push notifications are delivered to the mobile device, and are a great way to keep users informed while they're on the go.

Using push notifications

Note: To use push notifications, your system must have access to the Internet.

Push notifications use cloud services from Apple, Microsoft, and Google:

- Apple Push Notification service (APN)
- Microsoft Azure Notification Hub
- Google Cloud Messaging Push Notification service

There is a limit to the number of notifications that your system is allowed to send during a period of time. If your system exceeds the limit, it can send only one notification every 15 minutes during the next period. The notification contains a summary of the events that occurred during the 15 minutes. After the next period, the limitation is removed.

Requirements for push notifications

The following are requirements for using push notifications:

- You must associate one or more alarms with one or more events and rules. This is not required for system notifications.
- Make sure that your Milestone Care™ agreement with Milestone Systems is up-to-date.

Send notifications to mobile devices

You can enable Milestone Mobile to notify users when an event occurs, such as when an alarm triggers or something goes wrong with a device or server.

Set up system notifications

To send notifications related to the system, such as when a server goes offline, follow these steps:

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. Select the **Notifications** check box.

Set up push notifications on the Milestone Mobile server

To set up push notifications, follow these steps:

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. To send notifications to all mobile devices that connect to the server, select the **Notifications** check box.
3. To store information about the users and mobile devices that connect to the server, select the **Maintain device registration** check box.

   Note: The server sends notifications only to the mobile devices in this list. If you clear the **Maintain device registration** check box and save the change, the system clears the list. To receive push notifications again, users must reconnect their device.

Stop sending push notifications to specific mobile devices, or all mobile devices

There are several ways to stop sending push notifications to mobile devices.

1. In Management Client, select the mobile server, and then click the **Notifications** tab.
2. Do one of the following:
   - For individual devices, clear the **Enabled** check box for each mobile device. The user can use another device to connect to the Milestone Mobile server.
   - For all devices, clear the **Notifications** check box.

To temporarily stop for all devices, clear the **Maintain device registration** check box and then save your change. The system sends notifications again after users reconnect.

About using Video Push to stream video

You can set up Video Push so that users can keep others informed about a situation, or record video to investigate it later, by streaming video from their mobile device's camera to your XProtect surveillance system.

Set up Video Push to stream video

To let users stream video from their mobile devices to an XProtect surveillance system, set up Video Push on a Milestone Mobile server.

In Management Client, perform these steps in the following order:

1. Set up a channel that the mobile device can use to stream video to the recording server.
2. Add the Video Push Driver as a hardware device on the recording server. The driver simulates a camera device so that you can stream video to the recording server.
3. Assign the Video Push Driver device to the channel.

This topic describes each of these steps.

Set up a channel for streaming video

Note: Each channel requires a hardware device license.

To add a channel, follow these steps:

1. In the navigation pane, select **Mobile Server**, and select the mobile server.
2. On the **Video Push** tab, select the **Video Push** check box.
3. In the bottom right corner, click **Add** to add a video push channel under **Channels mapping**.
4. Enter the user name of the user account that will use the channel. This user account must be allowed to access the Milestone Mobile server and recording server.

   Note: To use Video Push, users must log in to Milestone Mobile on their mobile device using the user name and password for this account.
5. Make a note of the port number. You will need it when you add the Video Push driver as a hardware device on the recording server.
6. Click **OK** to close the Video Push Channel dialog box and the save the channel.

Add the Video Push Driver as a hardware device on the recording server

1. In the navigation pane, click **Recording Servers**.
2. Right-click the server that you want to stream video to, and click **Add Hardware** to open the **Add Hardware** wizard.
3. Select **Manual** as the hardware detection method, and click **Next**.
4. Enter credentials for the camera, as follows:
   - To use the factory default credentials from the camera factory, click **Next**. Typically, factory settings are used.
   - If you have changed the credentials on the device, enter that information, and then click **Next**.

   Note: These are the credentials for the hardware, not for the user. They are not related to the user name for the channel.
5. In the list of drivers, expand **Other**, select the **Video Push Driver** check box, and then click **Next**.

   Note: The system generates a MAC address for the Video Push Driver device. We recommend that you use this address. Change it only if you experience problems with the Video Push Driver device. For example, if you need to add a new address and port number.

6. In the **Address** field, enter the IP address of the computer where Milestone Mobile server is installed.
7. In the **Port** field, enter the port number for the channel you created for streaming video. The port number was assigned when you created the channel.
8. In the **Hardware model** column, select **Video Push Driver**, and then click **Next**.
9. When the system detects the new hardware, click **Next**.
10. In the **Hardware name template** field, specify whether to display either the model of the hardware and the IP address, or the model only.
11. Specify whether to enable related devices by selecting the **Enabled** check box. You can add related devices to the list for **Video Push Driver**, even though they are not enabled. You can enable them later.

    Note: If you want to use location information when you stream video, you must enable the **Metadata** port.

12. Select the default groups for the related devices on the left, or select a specific group in the **Add to Group** field. Adding devices to a group can make it easier to apply settings to all devices at the same time or replace devices.

Add the Video Push Driver device to the channel for video push

1. In the **Site navigation** pane, click **Mobile Servers**, and then click the **Video Push** tab.
2. Click **Find Cameras**. If successful, the name of the Video Push Driver camera displays in the Camera Name field.
3. Save your configuration.

Remove a channel that you don't need

You can remove channels that you no longer use.

- Select the channel to remove, and then click **Remove** in the lower right corner.

About actions

You can manage the availability of the **Actions** tab in the Milestone Mobile client by enabling or disabling this on the Mobile server tab. **Actions** are by default enabled, and all available actions for the connected devices are shown here.

About naming an output for use in Milestone Mobile

In order to get actions shown correctly together with current camera, it is important that the output uses the exact same name as the camera.

Example:

If you have a camera named "AXIS P3301,P3304 - 10.100.50.110 - Camera 1", you must also name the action "AXIS P3301,P3304 - 10.100.50.110 - Camera 1".

You can add a further description to the title afterwards, for example "AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch".

Important: If you do not follow these naming conventions, actions are not available in the action list for the associated camera's view. Instead, actions appear in the list of other actions on the **Actions** tab.

Add an automatic export rule

1. In the Management Client, click the relevant Mobile server **> Export** Tab.
2. Under **Automatic Exports**, click **Add** to open the **Auto Export Rule** window**.**
3. Set the relevant Auto Export Rule window settings.
4. When finished, click **OK**.

Mobile server settings

General

The following table describes the settings on this tab.

Name	Description
Server name	Enter a name of the Milestone Mobile server.
Description	Enter an optional description of the Milestone Mobile server.
Mobile server	Choose between all Milestone Mobile servers currently installed to the specific system. Only Milestone Mobile servers that are running are shown in the list.
Login method	Select the authentication method to use when users log in to the server. You can choose between the following options: **Automatic**, **Windows authentication,** or **Basic authentication**.
Enable XProtect Web Client	Enable access to XProtect Web Client.
Enable all cameras view	Include the **All Cameras** view. This view displays all of the cameras that a user is allowed to view on a recording server.
Enable actions (outputs and events)	Enable access to actions in Milestone Mobile clients.
Enable keyframes	Stream only keyframes when streaming video. This uses less bandwidth.
Enable full-size images	Enable the Milestone Mobile server to send full-size images to the Milestone Mobile client or XProtect Web Client. Note that enabling full-size images uses more bandwidth. Additionally, enabling this option disables all rules set up in the **Performance** settings.
Enable direct streaming	Choose how to handle direct streaming in XProtect Web Client. Choose between enforcing the use of direct streaming, enforcing it when possible, or never enforcing it.
Enabled	Enable/disable logging of Milestone Mobile client's actions in a separate log file.

Name	Description
Log file location	Path to where log files are saved.
Keep logs for	Number of days to keep logs for (default three days).
Configuration backup	Import or export your Milestone Mobile server configuration. Your system stores the configuration in an XML file.

Connectivity

In the **General** section, specify the following settings.

Name	Description
Connection type	Choose how clients should connect to the Milestone Mobile server. You can choose between the following options: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**. **Note:** If you select **HTTPS Only**, devices running iOS 9.0 or later, or Windows Phone, can connect only if you have a certificate from a certificate authority (CA) installed on your Milestone Mobile server. CAs issue digital certificates that verify the identities of users and websites that exchange data on the Internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy. Before you turn on secure connections, make sure that you are familiar with digital certificates. To learn how to add a certificate in Milestone Mobile server, see Edit certificate (on page *354*).
Client timeout (HTTP)	Set a time frame for how often the Milestone Mobile client must indicate to the Mobile server that it is up and running. The default value is 30 seconds. Milestone recommends that you do **not** increase the time frame.

Settings in the **Internet Access** section are used in the following tasks:

- Configure connection settings.
- Send an email message to help users connect their mobile device to Milestone Mobile servers.
- Enable connections to Milestone Mobile servers on a complex network.

For step-by-step descriptions of these tasks, see Set up Smart Connect (on page 340).

Server Status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since	Shows how long the Mobile server has been running since it was last stopped.
CPU usage	Shows current CPU usage on the Mobile server.

Name	Description
Internal bandwidth	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column	Shows the current relation between the Mobile server and the Milestone Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: **Connected** and **Logged In** XProtect.
Bandwidth Usage column	Shows the level of bandwidth used by the Mobile server client user in question.
Live Streams column	Shows the number of live video streams currently open for the Milestone Mobile client user in question.
Playback Streams column	Shows the number of playback video streams currently open for the relevant mobile client user.
Video Push streams	Shows the number of Video Push stream currently open for the relevant mobile client user.
Direct Streams	Shows the number of live video streams using Direct Streaming that are currently open for the relevant mobile user.

Video Push

You can specify the following settings if you enable Video push:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your XProtect system.
Channel column	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant video push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see "Set up Video Push to stream video" on page 344), click **Find Cameras** to search for the relevant camera.

Investigations

You can enable investigations so that people can use XProtect Web Client and Milestone Mobile to access recorded video and investigate incidents, and prepare and download video evidence.

The following table describes the settings for investigations.

Name	Description
Investigations folder	Specify where to store video for investigations.
Limit size of investigations to	Enter the maximum number of megabytes that the investigations folder can contain.
View investigations made by others	Select this check box to allow users to access investigations that they did not create.
Include timestamps for AVI exports	Select this check box to include the date and time that the AVI file was downloaded.
Used codec for AVI exports	Select the compression format to use when preparing AVI packages for download. The codecs you can choose from can differ, depending on your operating system. If you do not see the codec you want, you can add it to the list by installing it on the computer where the Milestone Mobile server is running.
Failed export data (for MKV and AVI export)	Select whether to keep the data that was not successfully prepared for download in an investigation, or delete it.

Notifications

Use the **Notifications** tab to turn on or turn off system notifications and push notifications.

If you turn on notifications, and have configured one or more alarms and events, Milestone Mobile notifies users when an event occurs. When the app is open, notifications are delivered in Milestone Mobile on the mobile device. Push notifications notify users who don't have the Milestone Mobile open. These notifications are delivered to the mobile device.

For more information, see Send notifications to mobile devices (on page 344).

The following table describes the settings on this tab.

Name	Description
Notifications	Select this check box to turn on notifications.
Maintain device registration	Select this check box to store information about the devices and users who connect to this server. The system sends notifications to these devices. If you clear this check box, you also clear the list of devices. For users to start receiving notifications again, you must select the check box, and the users must connect their devices to the server again.
Enabled	Select this check box to send notifications to the device.

Name	Description
Registered devices	A list of the mobile devices that have connected to this server. You can start or stop sending to specific devices by selecting or clearing the **Enabled** check box.

Performance

On the **Performance** tab, you can set the following limitations on the Milestone Mobile server's performance:

Level 1

Level 1 is the default limitation placed on the Milestone Mobile server. Any limitations you set here are always applied to the Milestone Mobile's video stream.

Name	Description
Level 1	Select the check box to enable the first level of limitations to Milestone Mobile server performance.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 2

If you would rather like to enforce a different level of limitations that the default one in **Level 1**, you can select the **Level 2** check box instead. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or below.

Name	Description
Level 3	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Note that if you enable **Enable full-size images** on the **General** tab, none of the **Performance** levels are applied.

Log Settings

Fill in and specify the following log settings:

Name	Description
Enabled	Enable/disable logging of Milestone Mobile client's actions in a separate log file.
Log file location	Path to where log files are saved.
Keep logs for	Number of days to keep logs for (default three days).
CPU usage	Default level of CPU usage which will trigger a warning in the log.
Internal bandwidth	Default internal bandwidth usage which will trigger a warning in the log.
External bandwidth	Default external bandwidth usage which will trigger a warning in the log.
Check every	Default time frame (30 sec.) for checking warning levels.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to the Mobile server. Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which you can easily access Mobile server functionality.

You can:

- Open XProtect Web Client (see "Access XProtect Web Client" on page 353)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 356)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 355)
- Show/edit port numbers (on page 355)
- Edit certificate (on page 354)
- Open today's log file (see "About accessing logs and exports" on page 354)
- Open log folder (see "About accessing logs and exports" on page 354)
- Open export folder (see "About accessing logs and exports" on page 354)
- Show Mobile server status (see "About show status" on page 354)

Access XProtect Web Client

If you have a Milestone Mobile server installed on your computer, you can use the XProtect Web Client to access your cameras and views. Because you do not need to install XProtect Web Client, you can access it from the computer where you installed the Milestone Mobile server, or any other computer you want to use for this purpose.

1. Set up the Milestone Mobile server in the Management Client.
2. If you are using the computer where Milestone Mobile server is installed, you can right-click the Milestone Mobile Server icon in the system tray, and select **Open XProtect Web Client**.
3. If you are not using the computer where Milestone Mobile server is installed, you can access it from a browser. Continue with step 4 in this process.
4. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari).
5. Type the external IP address, that is, the external address and port of the server on which the Milestone Mobile server is running.

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

   In the address bar of your browser, type: http://1.2.3.4:8081 or https://1.2.3.4:8082, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using XProtect Web Client.

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

You must clear the cache of Internet browsers running the XProtect Web Client before you can use a new version of the XProtect Web Client. System administrators must ask their XProtect Web Client users to clear their browser cache after upgrading, or force this action remotely (you can do this action only in Internet Explorer in a domain).

About show status

Right-click the Mobile Server Manager icon and select **Show Status** or double-click the Mobile Server Manager icon to open a window that shows the status of the Mobile server. You can see the following information:

Name	Description
Server running since	Time and date of the time when the Mobile server was last started.
Connected users	Number of users currently connected to the Mobile server.
Hardware decoding	Indicates if hardware accelerated decoding is in action on the Mobile server.
CPU usage	How many % of the CPU is currently being used by the Mobile server.
CPU usage history	A graph detailing the history of CPU usage by the Mobile server.

About accessing logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved.

To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall Milestone Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between a Milestone Mobile server and your mobile device or the XProtect Web Client, you must have a valid certificate for the device or web browser to accept the connection. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install Milestone Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you can choose between generating a self-signed certificate or loading a file that contains a certificate issued by another trusted site.

Note: If you want to use secure connections (HTTPS) devices running iOS 9.0 or later, or Windows Phone, can connect only if you have a certificate from a certificate authority (CA) installed on your

Milestone Mobile server. CAs issue digital certificates that verify the identities of users and websites that exchange data on the Internet. Examples of CAs are companies like Comodo, Symantec, and GoDaddy. Before you turn on secure connections, make sure that you are familiar with digital certificates.

If you want use a different certificate, you can do the following.

1. On a computer where Management Client are installed, right-click the **Milestone Mobile Server** icon and select **Edit Certificate...**
2. Choose one of the following:
   - Generate a self-signed certificate
   - Load a certificate file

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.
2. Wait for a few seconds while the system installs the certificate.
3. When finished, a window opens and informs you that the certificate was installed successfully. The Mobile service restarts to apply the change.

Locate a certificate file

1. Choose the **Load a certificate file** option.
2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.
3. Fill in the password connected to the certificate file.
4. When finished, click **OK**.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials**.
2. Fill in the **Server URL**.
3. Select what user you want to log in as:
   - Local system administrator (no credentials needed) or
   - A specified user account (credentials needed).
4. If you have chosen a specified user account, fill in **User Name** and **Password**.
5. When finished, click **OK**.

Show/edit port numbers

1. Right-click the **Mobile Server Manager** and select **Show/Edit Port Numbers**.
2. To edit the port numbers, type the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).

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

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager.

- To perform any of these tasks, right-click the **Mobile Server Manager** and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Frequently asked questions (FAQs)

1. **Why can't I connect from my Milestone Mobile client to my recordings/Milestone Mobile server?**

   In order to connect to your recordings, the Milestone Mobile server must be installed on the server that runs your XProtect system or alternatively on a dedicated server. The relevant Milestone Mobile settings are also needed in your XProtect video management setup. These are installed as either plug-ins or as part of a product installation or upgrade. For details on how to get the Milestone Mobile server and how to integrate the Milestone Mobile client-related settings in your XProtect system, see the configuration section (see "Milestone Mobile configuration" on page 340).

2. **I installed the Milestone Mobile server to XProtect Corporate, but I can’t connect to the server from my device. What is the problem?**

   After you have installed the Milestone Mobile server to your XProtect Corporate (4.0+), you must install the Milestone Mobile plug-in to see the Milestone Mobile server in your XProtect Corporate setup (see "Install Milestone Mobile server" on page 45). When you have installed the Milestone Mobile plug-in, locate the plug-in under **Servers** > **Mobile Servers** and right-click to add a new mobile server. Here, you add the details about your Milestone Mobile server (Server name, Description (optional), Server Address, Port and more). Once you finish, restart the Milestone Mobile Service (from Windows Services) and try to reconnect with your device.

3. **How do I add a Milestone Mobile server/location/site to my Milestone Mobile client?**

   You do this from the Milestone Mobile client. When you open it for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. Your added Milestone Mobile servers will be listed alphabetically. You can add as many Milestone Mobile servers as needed, as long as you have the needed log-in credentials.

4. **Why is the image quality sometimes poor when I view video in the Milestone Mobile client?**

   The Milestone Mobile server automatically adjusts image quality according to the available bandwidth between the server and client. If you experience lower image quality than in the XProtect® Smart Client, you might have too little bandwidth to get full resolution images through the Milestone Mobile client. The reason for this can either be too little upstream bandwidth from the server or too little downstream bandwidth on the client. See the **XProtect Smart Client User Manual** which you can download from our website http://www.milestonesys.com/support/manuals-and-guides/.

   If you are in an area with mixed wireless bandwidth, you may notice that the image quality improves when you enter an area with better bandwidth.

5. **How do I create views?**

You cannot create or configure views in the Milestone Mobile client. It uses views and related names already created in the XProtect Smart Client. If you do not have any views set up, you can use the **All cameras** view to see all the cameras in your system. You can always add more views to the XProtect Smart Client at a later time.

6. **How do I add a new Milestone Mobile user?**

   A Milestone Mobile user is just like any other XProtect user. You add a new Milestone Mobile user the same way you normally add a new user in your Management Client: right-click on **Users** in the Navigation Pane and select **Add new basic user** or **Add new Windows user**. If you select new basic user, you must change the server login method to **Automatic** or **Basic Only** depending on your system. You change your server login method from the **Login method** drop-down menu on the **General** tab of the Mobile Server entry under **Servers** > **Mobile Servers** in the Management Client.

7. **Can I control my pant-tilt-zoom (PTZ) cameras and use presets from Milestone Mobile client?**

   Yes, in the Milestone Mobile client, you can control your connected PTZ cameras and use presets in live mode.

8. **How can I navigate my recordings?**

   Android: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and choose **Menu** > **Playback**. Once you are in playback mode you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu** > **Go to time**. Once you have chosen **Go To time**, select the date and time you want to view.

   iOS: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and tap Playback. Once you are in playback mode, you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu** > **Go to time**. Once you have chosen **Go to time**, select the date and time you want to view and click **Confirm**.

9. **Can I view live and recorded video at the same time?**

   Yes, in playback mode, you get a small picture-in-picture (PiP) view live from the same camera.

10. **Can I use the Milestone Mobile client without a 3G data plan?**

    Yes, you can use Milestone Mobile through Wi-Fi. Either locally on the same network as your XProtect system or at a different location, such as a public network in a café or a home network. Note that bandwidth on public networks vary and may affect the image quality of the video streams.

11. **Can I use the Milestone Mobile client with a 4G/LTE data plan?**

    Yes, you can use any data connection on your mobile device that allows you to access the internet to connect to your XProtect video management system.

12. **Can I add multiple servers to the Milestone Mobile client?**

    When you open the Milestone Mobile client for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. These mobile servers are listed alphabetically. If you want to retrieve video from additional servers, repeat this process. You can add as many mobile servers as needed, as long as you have the relevant log-in credentials.

13. **Why is the image quality poor when I connect to my XProtect video management system at home through Wi-Fi at my office?**

    Check your home internet bandwidth. Many private internet connections have different download and upload bandwidths often described as, for example, 20 Mbit/2 Mbit. This is because home users rarely need to upload large amounts of data to the internet, but consume a lot of data instead. The XProtect video management system needs to send video to the Milestone Mobile client and is limited by your connection's upload speed. If low image quality is consistent on multiple locations where the download speed of the Milestone Mobile client's network is good, the problem might be solved by upgrading the upload speed of your home internet connection.

14. **Where are my screenshots saved?**

    Android: Snapshots are saved to your device's SD card at: **/mnt/sdcard/XProtect**.

    iOS: Snapshots are saved to your device and can be accessed from **Photos** on your device.

    You cannot change the default settings on neither Android nor iOS.

15. **How do I avoid the security warning when I run XProtect Web Client through an HTTPS connection?**

    The warning appears because the server address information in the certificate is incorrect. The connection will still be encrypted.
    The self-signed certificate in the Milestone Mobile server needs to be replaced with your own certificate matching the server address used to connect to the Milestone Mobile server. These certificates are obtained through official certificate signing authorities such as Verisign. Consult the chosen signing authority for more details.
    Milestone Mobile server does not use Microsoft IIS. This means that instructions provided for generating certificate signing request (CSR) files by the signing authority using the IIS is not applicable for the Milestone Mobile server. You must manually create CSR-file using command line certificate tools or other similar third-party application. Note that this process should be performed by system administrators and advanced users only.

16. **Does my processor support hardware-accelerated decoding?**

    Only newer processors from Intel support hardware accelerated decoding. Check Intel website
    http://ark.intel.com/search/advanced?s=t&MarketSegment=DT&QuickSyncVideo=true if your processor is supported.

    In the menu, make sure **Technologies** > **Intel Quick Sync Video** is set to **Yes**.

    If your processor is supported, hardware-accelerated decoding is enabled by default. You can see the current status in **Show status** in the Mobile Server Manager (see "About show status" on page 354).

17. **Does my operating system support hardware-accelerated decoding?**

    Only Windows 8 and Windows Server 2012 or newer are supported.

    Make sure you install the newest graphic drivers from the Intel website on your system. These drivers are not available from Windows Update.

    Hardware-accelerated decoding is not supported, if the mobile server is installed in a virtual environment.

18. **How do I disable hardware-accelerated decoding on the mobile server? (Advanced)**

If the processor on the mobile server supports hardware accelerated decoding, it is by default enabled. To turn hardware-accelerated decoding off, do the following:

1. Locate the file VideoOS.MobileServer.Service.exe.config. The path is typically: C:\Program Files\Milestone\Milestone Mobile Server\VideoOS.MobileServer.Service.exe.config.
2. Open the file in Notepad or a similar text editor. If necessary, associate the file type .config with Notepad.
3. Locate the field <add key="HardwareDecodingMode" value="Auto" />.
4. Replace the value "Auto" with "Off".
5. Save and close the file.

19. **I just turned on my firewall, and now I can't connect a mobile device to my server. Why not?**

    If your firewall was turned off while you installed Milestone Mobile server, you must manually enable TCP and UDP communications.

Milestone ONVIF Bridge

About Milestone ONVIF Bridge

Available functionality depends on the system you are using. See the Product comparison chart for more information.

ONVIF is an open, global forum that is working to standardize and secure the way that IP video surveillance products communicate. The goal is to make it easy to exchange video and audio data. For example, to enable law enforcement, surveillance centers, or similar organizations to quickly access live and recorded video streams in any IP-based surveillance system.

Milestone Systems wants to support this goal, and has developed the Milestone ONVIF Bridge toward that end. Milestone ONVIF Bridge is a part of the Milestone Open Platform, and offers an interface that supports the parts of the ONVIF standard for retrieving live and recorded video from any Milestone Husky™ NVR or XProtect® VMS product.

This document provides the following:

- Information about the ONVIF standard and links to reference materials.
- Instructions for installing and configuring the Milestone ONVIF Bridge in an XProtect VMS product.
- Examples of how to enable various types of ONVIF clients to stream live and recorded video from XProtect VMS products.

Milestone ONVIF Bridge and the ONVIF standard

The ONVIF standard facilitates information exchange by defining a common protocol. The protocol contains ONVIF profiles, which are collections of specifications for interoperability between ONVIF compliant devices.

Milestone ONVIF Bridge is compliant with the parts of ONVIF Profile G and Profile S that provide access to live and recorded video, and the ability to control pan-tilt-zoom cameras:

- Profile G - Provides support for video recording, storage, search, and retrieval. For more information, see ONVIF Profile G Specification (https://www.onvif.org/Portals/0/documents/specs/ONVIF_Profile_G_Specification_v1-0.pdf.)
- Profile S - Provides support for streaming live video using the H.264 codec, audio streaming, and pan-tilt-zoom (PTZ) controls. For more information, see ONVIF Profile S Specification (http://www.onvif.org/Portals/0/documents/op/ONVIF_Profile_S_Specification_v1-1-1.pdf).

For more information about the ONVIF standard, see the ONVIF® website http://www.onvif.org/.

ONVIF Profiles support "get" functions that retrieve data, and "set" functions that configure settings. Each function is either mandatory, conditional, or optional. For security reasons, Milestone ONVIF Bridge supports only the mandatory, optional, and conditional "get" functions that do the following:

- Request video
- Authenticate users
- Stream video
- Play recorded video

Note: Although the Milestone ONVIF Bridge currently supports only ONVIF Profile S and Profil G, work is underway to add support for additional ONVIF Profiles.

About ONVIF clients

Examples of ONVIF clients are servers, bridges like the Milestone ONVIF Bridge, media players, or IP-based surveillance systems.

The Real Time Streaming Protocol (RTSP) is used to establish and control media sessions between two or more endpoints. The Milestone ONVIF Bridge uses ONVIF Profile S and RTSP to handle requests for video from an ONVIF client, and to stream video from an XProtect video management software installation to the ONVIF client.

By default, communication between ONVIF clients and the ONVIF Bridge server uses the following ports:

- ONVIF port 580. ONVIF clients use this port to submit requests for video streams
- RTSP port 554. Milestone ONVIF Bridge uses this port to stream video to ONVIF clients

ONVIF clients can access the RTSP port on the Milestone ONVIF Bridge directly. For example, the VLC media player or a VLC plug-in in a browser can retrieve and display video. This is described later in this document in a section titled Use a media player to connect to a live stream.

You can use different ports, for example, to avoid a port conflict. If you change the port numbers, you must also update the RTSP stream for the ONVIF client URI.

RTSP supports only the H.264 codec. Cameras must be able to stream video in the H.264 codec.

Milestone ONVIF Bridge security controls

Milestone ONVIF Bridge enforces user authorization of ONVIF clients. This controls the ONVIF client's ability to access cameras, and the types of operations the ONVIF clients can perform. For example, whether ONVIF clients can use pan-tilt-zoom (PTZ) controls on cameras.

Milestone recommends that you create and add a dedicated user account for the Milestone ONVIF Bridge, and for each ONVIF client, as follows:

1. Create a Basic user in Management Client, or a Windows user in Active Directory.
2. Assign the user to a role that can access cameras, and specify permissions for the ONVIF Bridges security group on the Overall Security tab for the role.
3. Assign the user to the Milestone ONVIF Bridge during installation, and in Management Client or Management Application for each ONVIF client afterward.

Milestone ONVIF Bridge allows ONVIF clients only to request and receive video streams from cameras. ONVIF clients cannot configure settings in the XProtect VMS system or the Milestone ONVIF Bridge.

As a security precaution, Milestone recommends that you install the ONVIF Bridge server in a demilitarized zone (DMZ). If you install the bridge in a DMZ, you must also configure port forwarding for the internal and external IP addresses.

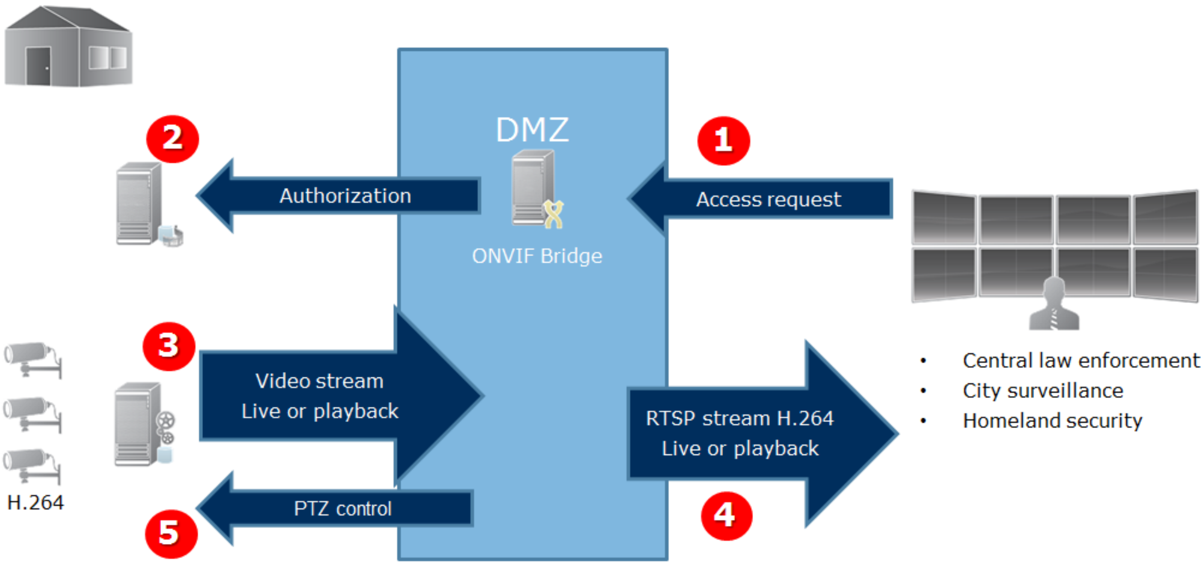
Milestone ONVIF Bridge architecture

The Milestone ONVIF Bridge is comprised of the following components:

- Milestone ONVIF Bridge server
- Milestone ONVIF Bridge 32-bit plug-in for Management Application
- Milestone ONVIF Bridge 64-bit plug-in for Management Client

The following image shows a high-level view of the interoperability between an ONVIF client, the Milestone ONVIF Bridge, and XProtect VMS.

XProtect VMS **ONVIF clients**



1. An ONVIF client connects to the XProtect VMS via the ONVIF Bridge server through Internet. To do this, the ONVIF client needs IP address or domain name (domain/hostname) of the server where Milestone ONVIF Bridge is installed, and the ONVIF port number.
2. The ONVIF Bridge server connects to the management server to authorize the ONVIF client user.

3. After authorization, the recording server starts sending H.264 video streams from the cameras to the ONVIF Bridge server.

   Note: If a camera supports multiple streams, only the default stream is sent.

4. The ONVIF Bridge server sends the video as RTSP streams to the ONVIF client.
5. If available, the ONVIF client user can pan-tilt-zoom PTZ cameras.

Note: Milestone recommends that you install the ONVIF Bridge server in a demilitarized zone (DMZ).

Licensing

Milestone ONVIF Bridge does not require additional licenses. You can download and install the software for free from the Milestone Systems website.

Installing Milestone ONVIF Bridge

When you install Milestone ONVIF Bridge, you install a server and a plug-in for the Management Client, which are the central administration components for XProtect Advanced VMS, and XProtect Professional VMS products, respectively. For example, you use these components to manage cameras, set up users, grant permissions, and so on.

You can install and add one or more Milestone ONVIF Bridges to your system. However, this increases the load on the network, and can impact performance. Typically, only one Milestone ONVIF Bridge is added to a system because multiple ONVIF clients can connect via one bridge.

Supported versions of XProtect video management software and Milestone Husky products

You can use the Milestone ONVIF Bridge with any version of XProtect video management software or Milestone Husky product.

System requirements

The computer where you want to install the Milestone ONVIF Bridge server component must have access to the Internet, and the following software installed:

- Microsoft® .NET Framework 3.5.
- Microsoft® .NET Framework 4.5.1 or higher.
- Visual C++ Redistributable Package for Visual Studio 2013 (x64).

Important: Cameras must support H.264 streaming via the Internet.

What's installed?

During installation, the following components are installed:

- Milestone ONVIF Bridge server, including the Milestone ONVIF Bridge service, the Milestone RTSP Bridge service, and the Milestone ONVIF Bridge Manager.
- Milestone ONVIF Bridge plug-in. The plug-in will be available in the Servers node in Management Client. This happens automatically if you use a **Typical** installation method. If you use a **Custom** installation method, you install it in a second step.

Installation also does the following:

- Registers and starts the Milestone ONVIF Bridge service and the Milestone RTSP Bridge service
- Starts the Milestone ONVIF Bridge Manager, which is available in the Windows notification area on the server where the ONVIF Bridge Server is installed

Note: The actions in the ONVIF Bridge Manager apply to both the Milestone ONVIF Bridge service and the Milestone RTSP Bridge service. For example, when you start or stop the ONVIF Bridge service, the Milestone RTSP Bridge service also starts or stops.

Before you begin

Before you start the installation, get the following information:

- The domain name and password for the dedicated user account that was created for the Milestone ONVIF Bridge. For more information, see the section titled Milestone ONVIF Bridge security controls (see "About Milestone ONVIF Bridge" on page 359).
- The URL or IP address, and the port number, of the management server.

You will need this information during installation.

Install the Milestone ONVIF Bridge

Download the installation file:

1. On the computer where you want to install Milestone ONVIF Bridge, go to the Milestone website https://www.milestonesys.com/support/download-software/ and locate the Milestone ONVIF Bridge product.
2. Click the Milestone ONVIF Bridge installer file.
3. Select **Run** or **Save** and follow the instructions.

Run the installer:

1. Select the language you want to use, and then click **Continue**.
2. Read and accept the license agreement, and then click Continue.
3. Select the installation type, as follows:
    - To install the ONVIF Bridge server and plug-in on one computer, and apply default settings, click **Typical**. Go to step 7.
    - To install the ONVIF Bridge server and plug-in on separate computers, click **Custom**. Use this method if you have a distributed system. If you choose **Custom**, select the server option, and then click **Continue**.
4. To establish a connection to management server, specify the following:
    - The URL or IP address, and the port number, of the management server. The default port is 80. If you omit the port number, the system will use port 80.
    - The domain user name and password of the Windows user or Basic user that the service will use. Click **Continue**.
    - **Note:** Leave **User account** in the **Log in as** field.

5. Select the file location and product language, and then click **Install**.
6. When the installation is complete, a list of successfully installed components displays. Depending on the installation method you chose, do one of the following:
   - If you selected a **Typical** installation, click **Close**.
   - If you chose **Custom**, click Close, and then install the ONVIF Bridge plug-in on the computer where Management Client is installed. To install the plug-in, run the installer again on that computer.

The following components are now installed:

- Milestone ONVIF Bridge server.
- Milestone ONVIF Bridge plug-in that is visible in Management Client in the **Servers** node.
- Milestone ONVIF Bridge Manager that is running and accessible from the notification area on the server with the ONVIF Bridge server installed.
- Milestone ONVIF Bridge service that is registered as a service.

You are ready for initial configuration (see "Configuring the Milestone ONVIF Bridge" on page 364).

Configuring the Milestone ONVIF Bridge

After you install the Milestone ONVIF Bridge, the ONVIF Bridge service is running and the icon in the system tray turns green. The next steps are to:

- Add the ONVIF Bridge plug-in to the Management Client
- Enable ONVIF clients to access your XProtect video management software product

Add a Milestone ONVIF Bridge to the Management Client

1. Open the Management Client.
2. Expand **Servers**, right-click **ONVIF Bridge**, and select **Add New**.
3. Enter a name for the Milestone ONVIF Bridge, and then click **OK**.

Configure user settings for an ONVIF client

Before you can complete these steps, you must have already created a basic user in Management Client, or a Windows user in Active Directory for the ONVIF client. The user must be assigned to a role that has permission to view cameras and access the Milestone ONVIF Bridge. For more information, see the section titled "Milestone ONVIF Bridge security controls" in About Milestone ONVIF Bridge (on page 359). For information about how to set up a basic user in Management Client, see the Help for those programs.

To provide an ONVIF client access to your XProtect video management software, follow these steps:

1. Open the Management Client.
2. Expand **Servers**, select **ONVIF Bridge**, and then select the bridge you just added.

3. On the **User settings** tab, enter the domain user name (domain/user) and the password of the dedicated user created for the ONVIF client.

4. Click the **Add user** button.

The name of the ONVIF client user appears in the list of **ONVIF user credentials**.

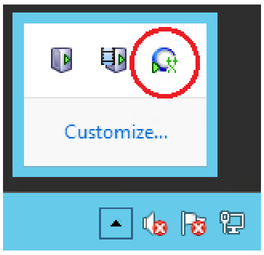
Managing Milestone ONVIF Bridge

After you configure Milestone ONVIF Bridge, you can monitor the service and change configuration settings in several ways.

Check the status of the ONVIF Bridge service

To view the status of the ONVIF Bridge service, follow these steps.

1. On the computer where the ONVIF Bridge server is installed, look in the notification area. The ONVIF Bridge tray icon indicates the status of the ONVIF Bridge service. If the service is running, the icon is green.



2. If it is not running, the icon is yellow or red. Right-click the icon and select **Start ONVIF Bridge service**.

View logs

The ONVIF Bridge Manager saves log information about the ONVIF Bridge server and the RTSP streams.

1. In the notification area on the computer where the ONVIF Bridge server installed, right-click the ONVIF Bridge tray icon.

2. Select **Show latest ONVIF log** or **Show latest RTSP log**.

Change the level of information in your logs

The ONVIF Bridge Manager saves log information about the ONVIF Bridge server and the RTSP streams.

To change the level of information, follow these steps:

1. Right-click the ONVIF Bridge tray icon, and then stop the ONVIF Bridge service.

2. Right-click the ONVIF Bridge tray icon again, and select **Configuration**.

3. In the **Log level for ONVIF** and **Log level for RTSP** fields, specify the type of information, and how much information, you want to save in your ONVIF and RTSP logs. The default value is Information.

> **Note:** From top to bottom in the list, the options are ordered from lowest level to highest level. Each level includes the level above it in the list. For example, the Warning level includes the Error level. If you can, only use the Error, Warning, and Information levels. The Trace and Message levels capture more information and use more disk space, which can decrease performance.

4. Click **OK**.

5. Right-click the ONVIF Bridge tray icon, and then start the ONVIF Bridge service.

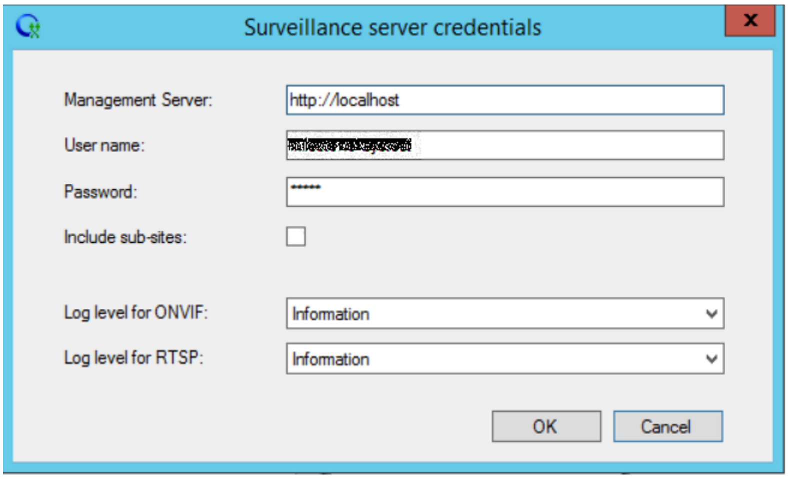
Change configuration settings for the Milestone ONVIF Bridge

If you change the IP address or host name of the surveillance server, or if you have changed the user accounts that have access to the surveillance server service, you must update this information for Milestone ONVIF Bridge.

To change the VMS address or login credentials, follow these steps:

1. On the computer where Milestone ONVIF Bridge server is installed, right-click the ONVIF Bridge tray icon, and then stop the ONVIF Bridge service.

2. Right-click the ONVIF Bridge tray icon again, and select **Configuration**.



Management Server: http://localhost

User name: [redacted]

Password: *****

Include sub-sites: □

Log level for ONVIF: Information

Log level for RTSP: Information

3. Specify the new information, and then click **OK**.

> **Note:** You must use the fully qualified domain name or the IP address of the server where the management server is installed.

4. Right-click the ONVIF Bridge tray icon, and then start the ONVIF Bridge service.

The ONVIF Bridge service is now running and the tray icon turns green.

Including sub-sites

By default, the Milestone ONVIF Bridge is configured to exclude sub-sites. This means that ONVIF client users cannot access video from cameras that are installed on sub-sites.

You can change this to include sub-sites. However, Milestone recommends that you do so only for systems where sub-sites do not contain large numbers of cameras The Milestone ONVIF Bridge aggregates and displays all cameras, including those from sub-sites, in one list. For example, if the system and sub-sites have more than 50 cameras, the list will be difficult to use.

Tip: If you must include sub-sites, consider installing the Milestone ONVIF Bridge on each management server. You will have more than one list of cameras, however, the cameras will be easier to identify and navigate.

To include sub-sites:

1. Right-click the ONVIF Bridge tray icon, and then stop the ONVIF Bridge service.
2. Right-click the ONVIF Bridge tray icon again, and click **Configuration**.
3. Select the **Include sub-sites** checkbox, and then click **OK**.
4. Right-click the ONVIF Bridge tray icon, and then start the ONVIF Bridge service.

Tips and tricks

The configuration created by ONVIF Bridge Manager is stored locally in a file at ProgramData\Milestone\Milestone ONVIF Bridge. The name of the file is serverconfiguration.xml. If this file is deleted, you must update the configuration in the ONVIF Bridge Manager.

To update a configuration, follow the steps described in the section of this document titled Change configuration settings for a Milestone ONVIF Bridge.

Milestone ONVIF Bridge properties

This section provides information about the settings for managing users and connections, and configuration settings for cameras.

User settings tab (properties)

The following table describes the settings for the ONVIF Bridge server and ONVIF clients.

Name	Description
ONVIF port	The port number of the ONVIF port. ONVIF clients use this port to connect to the ONVIF Bridge server. The default port number is 580.
RTSP port	The port number of the RTSP port. The ONVIF Bridge server sends RTSP video streams through this port to ONVIF clients. The default port number is 554.
ONVIF user credentials	Lists the ONVIF client users that have access to the XProtect VMS system through the ONVIF Bridge server.
User name	The domain user name of the user created for an ONVIF client. Prerequisite: You have set up the ONVIF client users as users in Management Client with access to cameras and the Milestone ONVIF Bridge.
Password	The password for the ONVIF client user.
Add user	After you enter a domain user name and password, click the **Add user** button to add the user.
Remove user	Prevent an ONVIF client from accessing the Milestone ONVIF Bridge. Remove a selected user from the **ONVIF user credentials** list.

Advanced settings tab (properties)

The advanced settings for the ONVIF Bridge list the default settings for all cameras that the ONVIF Bridge provides to the ONVIF clients when the clients connect and request video streams.

The settings do not reflect the actual configuration of the cameras, and do not affect the video stream. The system uses the settings to speed up the exchange of video between the ONVIF Bridge and the ONVIF client. The ONVIF client will use the actual settings from the RTSP stream.

You can change the default settings that ONVIF Bridge provides to the ONVIF client, for example, if you want the values to reflect the actual configuration of the cameras.

Name	Description
Max days of retention	Default value is 30.
Frame per seconds	Default value is 5.
Width	Default value is 1920. This corresponds to full HD quality.
Height	Default value is 1080. This corresponds to full HD quality.
Bitrate Kbps	Default value is 512.
GOP size	Default value is 5.
Codec	Select one of the H.264 codec profiles. The default value is H.264 Baseline Profile.
Use configurations from cameras	Enable this to use the actual configuration of the cameras instead of the default average values defined above. **Note:** If you enable this setting, the response time between the XProtect system and the ONVIF clients increases.

Using ONVIF clients to view video streams

ONVIF clients can be many different things, ranging from advanced custom surveillance systems to basic media players.

This section provides examples of how to connect a Network Video Client and a media player to the Milestone ONVIF Bridge.

Use a Network Video Client to view a live stream

This example describes how to install the ONVIF Device Manager, and configure it to stream live video from an XProtect Advanced VMS installation.

The ONVIF Device Manager is a free, open source Network Video Client from iDeviceDesign that complies with ONVIF standards. The tool is widely used to because it makes it easy to discover and view video from ONVIF compliant cameras on a network. Note, however, that you use ONVIF Device Manager to stream only live video. Additionally, you cannot capture and save the video data in the stream.

Before you start, get the following information from the person who administrates the XProtect Advanced VMS installation:

- The login credentials for the user that was created for the Milestone ONVIF Bridge
- The IP address or computer name of the computer where the Milestone ONVIF Bridge is installed

To install the ONVIF Device Manager, follow these steps:

1. Go to https://sourceforge.net/projects/onvifdm (https://sourceforge.net/projects/onvifdm), and then download and run the installer. You can install the ONVIF Device Manager on any computer.
2. When the installation completes, an icon is available on your desktop. Double-click the icon to start the ONVIF Device Manager.
3. When you start the ONVIF Device Manager, it automatically discovers ONVIF compliant devices on the network. However, it might not discover the Milestone ONVIF Bridge.
   - If it does, go to step 6.
   - If it does not, add the bridge manually. Continue with step 4.
4. To add a Milestone ONVIF Bridge, click **ADD**.
5. In the **Add device** dialog box, in the **URI** field, provide the name or IP address of the computer where the Milestone ONVIF Bridge is installed, and the ONVIF port number. For example, the string should look like this: http://<IP address>:580/onvif/device_service.
6. After you add the bridge, it is available at the bottom of the **Device** list. Select it.
7. Enter the login credentials for the basic user that was created for the ONVIF client above the list. For the user name, you must enter the domain user name.
8. Restart the ONVIF Bridge service to apply the change.

Use a media player to view a video stream

This example describes how to use the VLC media player to retrieve and view a live video feed or recorded video from a camera in an XProtect Advanced VMS installation.

VLC media player is a free, open source multimedia player from VideoLan that supports various streaming protocols, including RTSP. For example, using VLC media player is useful when you want a very fast way to connect to a camera, or just to test the connection to a camera.

When you connect to a camera to view recorded video, the Milestone ONVIF Bridge streams the video sequences, starting with the first sequence.

Before you start, get the following information from the person who administrates the XProtect Advanced VMS installation:

- The login credentials for the user account that is assigned to the Milestone ONVIF Bridge.
- The IP address or computer name of the computer where the Milestone ONVIF Bridge is installed.
- The GUID of the device that you want to stream video from.

Tip: The camera GUID is available in Management Client. To find the GUID, select the recording server where the camera has been added, and then select the camera. Click the **Info** tab, press and hold CTRL on your keyboard, and then click the camera’s video preview.

This description is based on VLC 2.2.4 for Windows.

To install the VLC media player, and connect it to an XProtect Advanced VMS, follow these steps:

1. Go to http://www.videolan.org/vlc/index.html, and then download the installer for the VLC media player.
2. Run the installer, and follow the instructions for each step.
3. On the toolbar, click **Media**, and select **Open Network Stream**.
4. In the **Open media** dialog box, enter the following RSTP string. Replace the variables in the angle brackets "<ONVIF Bridge IP Address>" and "<Camera GUID>" with the correct information:
    - To view a live video stream, enter **rtsp://<ONVIF Bridge IP Address>:554/live/<Camera GUID>**
    - To view recorded video, enter **rtsp://<ONVIF Bridge IP Address>:554/vod/<Camera GUID>**
5. Click **Play**, and then enter the user name and password of the user account that was added to the Milestone ONVIF Bridge.

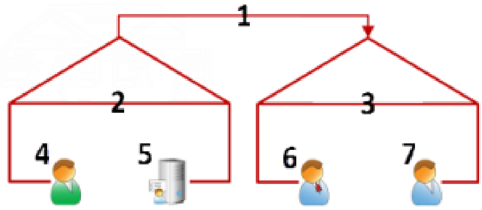
Multi-domain with one-way trust

Setup with one-way trust

If you run your system in a multi-domain environment, you can configure this setup with one-way trust. The system is installed on the **trusting** domain and users log in from **trusting** and **trusted** domains.

1. Create a service account in the **trusted** domain. You can name it whatever you want, for example, **svcMilestone**.
2. Add the new service account to the following local Windows user groups on the server running the system, in the **trusting** domain:
    - Administrators
    - IIS_IUSRS (Windows Server 2008, necessary for Internet Information Services (IIS) Application Pools)
    - IIS_WPG (Windows Server 2003, necessary for IIS Application Pools).
3. Make sure that the service account has system administrator rights on your SQL Database or SQL Server Express, either directly or through the **BUILTIN\Administrators** group.
4. Set the identity of the **ManagementServerAppPool** Application Pool in the IIS to the service account.
5. Reboot the server to make sure that all group membership and permission changes take effect.

Important: To add **trusted** domain users to new or existing XProtect system roles, log in to Windows as a **trusted** domain user. Next, launch the Management Client and log in as user of either the **trusting** domain or the **trusted** domain. If you log in to Windows as a **trusting** domain user, you are asked for credentials for the **trusted** domain in order to browse for users.



Example illustration of multi-domain environments with one-way trust.

Legend:

1. One-way outgoing domain trust
2. MyDomain.local
3. OtherDomain.edu
4. Trusting domain user
5. Management server
6. Milestone service account
7. Trusted domain user

SNMP

About SNMP support

Your system supports Simple Network Management Protocol (SNMP), a standard protocol for monitoring and controlling network devices, for managing their configuration, collecting statistics and more.

The system acts as an SNMP agent, which can generate an SNMP trap as a result of a triggered rule. A third-party SNMP management console can then receive information about the rule-triggering event, and operators of the SNMP management console can configure their system for further action as required.

The implementation uses Microsoft® Windows® SNMP Service for triggering SNMP traps. This means that you must install the SNMP Service on recording servers. When you have configured the SNMP Service through its own user interface, this enables recording servers to send .mib (Management Information Base) files to the SNMP management console.

Install SNMP service

1. On the relevant recording servers, open Windows' **Programs and Features** functionality.
2. In the left side of the **Programs and Features** dialog box, click **Turn Windows functionality on or off**. This opens the **Windows feature** window.
3. In the dialog box, select the check box next to **Simple Network Management Protocol (SNMP)** and click **OK**.

Configure SNMP service

1. On the required recording servers, select **Start** > **Control Panel** > **Administrative Tools** > **Services**.
2. Double-click the SNMP Service.
3. Select the **Traps** tab.
4. Specify a community name, and click **Add to list**.
5. Select the **Destinations** tab.
6. Click **Add**, and specify the IP address or host name of the server running your third-party SNMP management station software.
7. Click **OK**.

XProtect Enterprise servers

About XProtect Enterprise servers

This section is only relevant if you use:

- XProtect Corporate
- your system does not use IPv6, and
- you have installations with XProtect Enterprise version 7 or later.

In all other cases, use Milestone Federated Architecture or Milestone Interconnect.

You can add XProtect Enterprise servers to your XProtect Corporate system. When added, the servers act as recording servers and their video can be viewed by the clients.

In the Management Client, you can see the status of added XProtect Enterprise servers. You must still define all XProtect Enterprise server settings (cameras, scheduling, user rights etc.) in XProtect Enterprise's Management Application. See the XProtect Enterprise documentation.

To give users access to video from XProtect Enterprise servers, you must match roles in XProtect Corporate with user rights defined on the XProtect Enterprise servers.

- Add XProtect Enterprise servers (on page 372)
- Define roles with access to XProtect Enterprise servers (on page 373)
- Edit XProtect Enterprise servers (on page 373)

Add XProtect Enterprise servers

Even if the XProtect Enterprise system has an internal master/slave setup, you cannot reuse it in your XProtect Corporate system. You must add each XProtect Enterprise server that you need device data from individually.

To add an existing XProtect Enterprise server to your system:

1. From the Management Client's **Tools** menu, select **Enterprise Servers**.

2. In the **Add/Remove Enterprise Servers** dialog box, click **Add**.
3. Enter the IP address or the host name of the XProtect Enterprise server.
4. Enter the port number used by the XProtect Enterprise server.

   The default port number is 80. If in doubt, you can find the port number in XProtect Enterprise's Management Application under Server Access.
5. Enter the user credentials for the administrator of the XProtect Enterprise server to give yourself unlimited rights to the device data from it.
6. If the XProtect Corporate system accesses the XProtect Enterprise server through an Internet connection, click **Network** to specify the WAN address of XProtect Corporate's management server. You need only define the WAN address once.

Next step is to give your users access to devices from the XProtect Enterprise server.

Define roles with access to XProtect Enterprise servers

To give the users access to devices from the added XProtect Enterprise servers:

1. On the XProtect Enterprise server, open the Management Application to find an XProtect Enterprise user who has user rights you can reuse and match with a role in your XProtect Corporate system. If not, create a new XProtect Enterprise user that matches the role in your XProtect Corporate system.
2. Take careful note of the XProtect Enterprise user's user name, password and authentication type (basic or Windows). The XProtect Corporate system does not verify that the information you specify later in these steps corresponds to a defined user in XProtect Enterprise.
3. In the XProtect Corporate Management Client's **Site Navigation** pane, expand **Security**, and select **Roles**.
4. Select the role you want to use or define a new role.
5. At the bottom of the **Role Settings** pane, select the **Servers** tab and then the XProtect Enterprise server.
6. Select the XProtect Enterprise user with the user rights you want to match with your role.
7. Click **Save**.

Edit XProtect Enterprise servers

To edit an XProtect Enterprise server added to your system:

1. From the **Tools** menu, select **Enterprise Servers**.
2. Select the XProtect Enterprise server from the list, and click **Edit**.
3. Edit the relevant settings and click **OK**.

System maintenance

Ports used by the system

All XProtect components and the ports needed by them are listed in individual sections below. To ensure, for example, that the firewall blocks only unwanted traffic, you need to specify the ports that the XProtect Advanced VMS uses. You should only enable these ports. The lists also include the ports used for local processes.

They are arranged in two groups:

- **Server components** (services) offer their service on particular ports which is why they need to listen for client requests on these ports. Therefore, these ports need to be opened in the Windows Firewall for inbound connections.
- **Client components** (clients) initiate connections to particular ports on server components. Therefore, these ports need to be opened for outbound connections. Outbound connections are typically open by default in the Windows Firewall.

If nothing else is mentioned, ports for server components must be opened for inbound connections, and ports for client components must be opened for outbound connections.

Do keep in mind that server components can act as clients to other server components as well.

The port numbers are the default numbers, but this can be changed. Contact Milestone Support, if you need to change ports that are not configurable through the Management Client.

Server components (inbound connections)

Each of the following sections list the ports which need to be opened for a particular service. In order to figure out which ports need to be opened on a particular computer, you need to consider all services running on this computer.

Management Server service and related processes

Port number	Protocol	Process	Connections from...	Purpose
80	HTTP	IIS	All XProtect components	Main communication, for example, authentication and configurations.
443	HTTPS	IIS	XProtect Smart Client and the Management Client	Authentication of basic users.
6473	TCP	Management Server service	Management Server tray controller, local connection only.	Showing status and managing the service.

Port number	Protocol	Process	Connections from...	Purpose
7475	TCP	Management Server service	Windows SNMP Service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect Advanced VMS 2014 systems or older, the port number was 6475.
8080	TCP	Management server	Local connection only.	Communication between internal processes on the server.
9993	TCP	Management Server service	Recording Server services	Authentication, configuration, token exchange.
12345	TCP	Management Server service	XProtect Smart Client	Communication between the system and Matrix recipients. You can change the port number in the Management Client.

SQL Server service

Port number	Protocol	Process	Connections from...	Purpose
1433	TCP	SQL Server	Management Server service	Storing and retrieving configurations.
1433	TCP	SQL Server	Event Server service	Storing and retrieving events.
1433	TCP	SQL Server	Log Server service	Storing and retrieving log entries.

Data Collector service

Port number	Protocol	Process	Connections from...	Purpose
7609	HTTP	IIS	On the Management Server computer: Data Collector services on all other servers. On other computers: Data Collector service on the Management Server.	System Monitor.

Event Server service

Port number	Protocol	Process	Connections from...	Purpose
1234	TCP/UDP	Event Server Service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
1235	TCP	Event Server service	Any server sending generic events to your XProtect system.	Listening for generic events from external systems or devices. Only if the relevant data source is enabled.
9090	TCP	Event Server service	Any system or device that sends analytics events to your XProtect system.	Listening for analytics events from external systems or devices. Only relevant if the Analytics Events feature is enabled.
22331	TCP	Event Server service	XProtect Smart Client and the Management Client	Configuration, events, alarms, and map data.
22333	TCP	Event Server service	MIP Plug-ins and applications.	MIP messaging.

Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled per default.

Port number	Protocol	Process	Connections from...	Purpose
5210	TCP	Recording Server Service	Failover recording servers.	Merging of databases after a failover recording server had been running.
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices.
7474	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP. In XProtect Advanced VMS 2014 systems or older, the port number was 6474.
7563	TCP	Recording Server Service	XProtect Smart Client, Management Client	Retrieving video and audio streams, PTZ commands.
8966	TCP	Recording Server Service	Recording Server tray controller, local connection only.	Showing status and managing the service.
11000	TCP	Recording Server Service	Failover recording servers	Polling the state of recording servers.
65101	UDP	Recording Server service	Local connection only	Listening for event notifications from the drivers.

Note that in addition to the inbound connections to the Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

Failover Server service and Failover Recording Server service

Port number	Protocol	Process	Connections from...	Purpose
25	SMTP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices. The port is disabled per default.
5210	TCP	Recording Server Service	Failover recording servers	Merging of databases after a failover recording server had been running.
5432	TCP	Recording Server Service	Cameras, encoders, and I/O devices.	Listening for event messages from devices.

Port number	Protocol	Process	Connections from...	Purpose
7474	TCP	Recording Server Service	Windows SNMP service	Communication with the SNMP extension agent. Do not use the port for other purposes even if your system does not apply SNMP.
7563	TCP	Recording Server Service	XProtect Smart Client	Retrieving video and audio streams, PTZ commands.
8844	UDP	Failover recording servers	Local connection only.	Communication between the servers.
8966	TCP	Failover Recording Server Service	Failover Recording Server tray controller, local connection only.	Showing status and managing the service.
8967	TCP	Failover Server Service	Failover Server tray controller, local connection only.	Showing status and managing the service.
8990	TCP	Failover Server Service	Management Server service	Monitoring the status of the Failover Server service.

Note that in addition to the inbound connections to the Failover Recording Server service listed above, the Recording Server service establishes outbound connections to the cameras.

Mobile Server service

Port number	Protocol	Process	Connections from...	Purpose
8000	TCP	Mobile Server service	Mobil Server management (tray icon), local connection only.	SysTray application.
8081	HTTP	Mobile Server service	Mobile clients, Web clients, and Management Client.	Sending data streams; video and audio.
8082	HTTPS	Mobile Server service	Mobile clients and Web clients.	Sending data streams; video and audio.

LPR Server service

Port number	Protocol	Process	Connections from...	Purpose
22334	TCP	LPR Server Service	Event server	Retrieving recognized license plates and server status. In order to connect, the Event server must have the LPR plug-in installed.
22334	TCP	LPR Server Service	LPR Server management (tray icon), local connection only.	SysTray application

Screen Recorder service

Port number	Protocol	Process	Connections from...	Purpose
52111	TCP	XProtect Screen Recorder	Recording Server Service	Provides video from a monitor. It appears and acts in the same way as a camera on the recording server. You can change the port number in the Management Client.

Cameras, encoders, and I/O devices

Inbound connections

Port number	Protocol	Connections from...	Purpose
80	TCP	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
443	HTTPS	Recording servers and failover recording servers	Authentication, configuration, and data streams; video and audio.
554	RTSP	Recording servers and failover recording servers	Data streams; video and audio.

Outbound connections

Port number	Protocol	Connections to...	Purpose
25	SMTP	Recording servers and failover recording servers	Sending event notifications (deprecated).
5432	TCP	Recording servers and failover recording servers	Sending event notifications.

Note that only a few camera models are able to establish outbound connections.

Client components (outbound connections)

XProtect Smart Client, XProtect Management Client, Milestone Mobile server

Port number	Protocol	Connections to...	Purpose
80	HTTP	Management server service	Authentication
443	HTTPS	Management server service	Authentication of basic users.
7563	TCP	Recording server service	Retrieving video and audio streams, PTZ commands.
22331	TCP	Event Server service	Alarms.

Web Client, Milestone Mobile client

Port number	Protocol	Connections to...	Purpose
8081	HTTP	Milestone Mobile server	Retrieving video and audio streams.
8082	HTTPS	Milestone Mobile server	Retrieving video and audio streams.

Backing up and restoring system configuration

About backing up and restoring your system configuration

Milestone recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration.

The system offers a built-in feature that backs up all the system configuration you can define in the Management Client. Note that the log server database and the log files, including audit log files, are not included in this backup.

If your system is large, Milestone recommends that you define scheduled backups. This is done with the third-party tool: Microsoft® SQL Server Management Studio. This backup includes the same data as a manual backup.

During a backup, your system stays online. Depending on your system configuration, your hardware, and on whether you have installed the SQL server, Event Server service and Management Client on a single server or several servers (a distributed setup), backing up the system configuration can take some time.

Each time you make a backup both manual and scheduled, the SQL Server's transaction log file is flushed. For additional information about how to flush this log file, go to the Microsoft website and search for "SQL Server transaction log".

Back up log server database

Handle the **SurveillanceLogServer** database by using the method that you use when handling system configuration as described earlier. The **SurveillanceLogServer** database (the name may be different if you renamed the system configuration database) contains all your system logs, including errors reported by recording servers and cameras.

The database is located where the Log Server's SQL server is installed, typically the same place as your management server's SQL server. Backing up this database is not vital since it does not contain any system configuration, but you may later appreciate having access to system logs from before the management server backup/restore.

Manual backup and restore of system configuration

About manually backing up your system configuration

When you want to perform a manual backup of your system configuration, make sure that your system stays online. Here are a few things to consider before you start the backup:

- You cannot use a backup to copy configurations to other systems.
- It can take some time to back up your configuration. It depends on your system configuration, your hardware, and on whether your SQL server, management server and Management Client are installed on the same computer.
- Logs, including audit logs, are **not** part of the configuration backup.

About backing up and restoring the event server configuration

The content of your event server configuration is included when you back up and restore system configuration.

The first time you run the event server, all its configuration files are automatically moved to the SQL server. You can apply the restored configuration to the event server without needing to restart the event server, and the event server can start and stop all external communication while the restoration of the configuration is being loaded.

About back up/restore fail and problem scenarios

If, after your last system configuration backup, you have moved the event server or other registered services such as the log server, you must select which registered service configuration you want for the new system. You can decide to keep the new configuration after the system is restored to the old version. You decide by looking at the host names of the services.

If your restore of the system configuration fails because the event server is not located at the specified destination (for example, if you have chosen the old registered service setup), do another restore.

Back up system configuration manually

1. From the menu bar, select **File** > **Backup Configuration**.
2. Read the note in the dialog box and click **Backup**.
3. Enter a file name for the .cnf file.
4. Enter a folder destination and click **Save**.
5. Wait until the backup is finished and click **Close**.

Note: All relevant system configuration files are combined into one single .cnf file that is saved at a specified location. During the backup, all backup files are first exported to a temporary system backup folder on the management server. You can select another temporary folder by right-clicking the notification area's management server service icon and by selecting Select shared backup folder.

Restore system configuration from a manual backup

Important information:

- Both the user who installs and the user who restores must be local administrator of the database on the management server **and** on the SQL server.
- Except for your recording servers, your system is completely shut down for the duration of the restore, which can take some time.
- A backup can only be restored on the system installation where it was created. Make sure that the setup is as similar as possible to when the backup was made. Otherwise, the restore might fail.
- If you do a backup of the database and restore it on a clean SQL server, then the raise errors from the database will not work and you will only receive one generic error message

from the SQL server. To avoid that, first reinstall your XProtect system using the clean SQL server and then restore the backup on top of that.

- If restoring fails during the validation phase, you can start the old configuration again because you have made no changes.
  If restoring fails elsewhere in the process, you cannot roll back to the old configuration. As long as the backup file is not corrupted, you can do another restore.
- Restoring replaces the current configuration. This means that any changes to the configuration since last backup are lost.
- No logs, including audit logs, are restored.
- Once restoring has started, you cannot cancel it.

Restoring:

1. Right-click the notification area's Management Server service icon and select **Restore Configuration**.
2. Read the important note and click **Restore**.
3. In the file open dialog box, browse to the location of the configuration backup file, select it, and click **Open**.

   The backup file is located on the Management Client computer. If the Management Client is installed on a different server, copy the backup file to this server before you select the destination.
4. The **Restore Configuration** window opens. Wait for the restore to finish and click **Close**.

Select shared backup folder

Before backing up and restoring any system configuration, you must set a backup folder for this purpose.

1. Right-click the notification area's management server service icon and select **Select shared backup folder**.
2. In the window that appears, browse to the wanted file location.
3. Click **OK** twice.
4. If asked if you want to delete files in the current backup folder, click **Yes** or **No** depending on your needs

Scheduled backup and restore

About scheduled backup and restore of system configuration

Milestone recommends that you make regular backups of your system configuration as a disaster recovery measure. While it is rare to lose your configuration, it can happen under unfortunate circumstances. Luckily, it takes only a minute to back up your existing configuration. Regular backups also have the added benefit that they flush your Microsoft® SQL Server’s transaction log.

If you have a smaller setup and do not need scheduled backups, you can back up your system configuration manually. For instructions, see Manual backup and restore of system configuration (on page 381).

The management server stores your system's configuration in a database. When you back up/restore management server(s), make sure that this database is included in the backup/restore.

Prerequisites for using scheduled backup and restore

Microsoft® SQL Server Management Studio, a tool download-able for free from their website http://www.microsoft.com/downloads.

Apart from managing SQL Server databases, the tool includes some easy-to-use backup and restoration features. Download and install the tool on your management server.

About the SQL server transaction log

Each time a change in the system's data occurs, the SQL Server log this change in its transaction log, regardless whether it is a SQL Server on your network or a SQL Server Express edition.

The transaction log is essentially a security feature that makes it possible to roll back and undo changes to the SQL Server database. By default, the SQL Server stores its transaction log indefinitely, and over time the transaction log build up more and more entries. The SQL Server's transaction log is by default located on the system drive, and if the transaction log keeps growing, it may in the end prevent Windows from running properly.

To avoid such a scenario, flushing the SQL Serve's transaction log from time to time is a good idea. However, flushing it does not in itself make the transaction log file smaller, but it prevents it from growing out of control. Your system does not, however, automatically flush the SQL Server's transaction log at specific intervals. You can also do several things on the SQL Server itself to keep the size of the transaction log down.

For more information on this topic, go to the Microsoft support page http://support.microsoft.com and search for SQL Server transaction log.

Back up system configuration with scheduled backup

1. From Windows' **Start** menu, launch Microsoft® SQL Server Management Studio..
2. When connecting, specify the name of the required SQL Server. Use the account under which you created the database.

   a) Find the **Surveillance** database that contains your entire system configuration, including event server, recording servers, cameras, inputs, outputs, users, rules, patrolling profiles, and more.

   We assume that the database uses the default name.

   b) Make a backup of the **Surveillance** database and make sure to:

   - Verify that the selected database is **Surveillance**.
   - Verify that the backup type is **full**.
   - Set the schedule for the recurrent backup. You can read more about scheduled and automated backups on the Microsoft website https://support.microsoft.com/en-us/kb/2019698.
   - Verify that the suggested path is satisfactory or select alternative path.
   - Select to **verify backup when finished** and to **perform checksum before writing to media**.