GEUTEBRÜCK

Perimeter+ User Manual

Version: 202.1

31.07.2023

Table Of Contents

About This Documentation

Current software version: **Perimeter+ 202.1**.

The latest features and changes of the current software version are listed in the Release Notes.

Note that the illustrations in this documentation may not match those of your software version.

Legal Notice

This documentation may not be copied, translated or converted to a machine-readable form, whether in whole or in part, without prior permission.

GEUTEBRÜCK GmbH cannot guarantee the correctness of any information provided in this documentation, nor for the software or the information it contains. Any suggested guarantee, assurance of marketable quality or suitability for a specific purpose of the documentation, the software or other information is hereby explicitly rejected.

Under no circumstances is GEUTEBRÜCK GmbH liable for direct or indirect subsequent damage or for special subsequent damage resulting from or in association with this documentation, regardless of whether this arises as a result of illegitimate action, of a contract, or for other reasons in association with this documentation, the software or of the information contained or used within it.

GEUTEBRÜCK GmbH retains the right to change this documentation or the information contained within it at any time without warning. The software described in it is subject to the conditions of a special license contract.

Note that the illustrations in this documentation may not match those of your software version.

Getting Started

Installation

Install the server in a suitable location and connect the appropriate connections.

Power Supply

Connect the supplied power cord to the equipment.

Network

The system can be operated in standalone mode or connected to a local Ethernet network using TCP/IP protocol. In the following cases, your equipment must be connected to a network:

- If the installation consists of more than one unit.
- If you want to access alarms from a unit other than the server.
- If you want the system to send alarm messages to G-Core.

If none of the above cases apply, you do not need to connect the equipment to the local network.

To connect the system to the local network, use the RJ45 connector on the back of the unit.

IP Cameras

The system is compatible with most IP cameras on the market and can be set up with any IP device that communicates using the ONVIF or RTSP protocol.

If you use IP cameras, ensure that the system is connected to the same local area network as the cameras.

Follow these steps:

1. Connect the system to the local area network.
2. Connect the cameras to the local area network.
3. Connect a computer monitor, mouse and keyboard to the system.
4. Turn on the server and wait for the system to start automatically.

System Overview

After connecting the cameras, monitor and keyboard to the system, press the power button and wait for the system to start.

The unit starts up and the server home screen is displayed, which consists of the following sections:

- 1 Menu items
- 2 Error messages
- 3 License information
- 4 Software version
- 5 Icon to open the keyboard

Menu Items

Icon	Option	Description
	Cameras	Starts the display and management application of the system.
	Configuration	Displays the basic configuration information of the equipment.
	Support	Opens the support contact dialog window.
	Shutdown	Restarts or shuts down the system. In the latter case, it shuts down the system and turns off the server.

Error Messages

Error Message	Description
Demo version	Unit with demo version.
No license detected	No license detected in the unit.
End of try period. Contact with your distributor.	End of the trial period of the demo license.
End of try period. Contact with your distributor before: <date>	End of the trial period, grace period active until <date>.
No license detected. Contact with your distributor before: <date>	No license detected, grace period active until <date>.
Trying to access system database <name>	No access to the database.
Please, install the relay	Input/Output module configured, but not detected.

Error Message	Description
module	
Can't access to external I/O device	External input/output module configured, but not detected.
Working <name>	Unit with logs enabled.
GPU not found	GPU not found in a unit where a GPU is expected.
BSI-XY	BSI means error of the DFusion engine in a unit of the system. X means there is an error in the local unit (X=1), Y means there is an error in other units.
Lost communication with a machine in the system	Communication with slave unit lost.
Slave machine with older version	Slave unit with a different version than the master unit detected.
Check network configuration	The configured IP does not match the actual IP of the unit.

Setting Your Password

When you log in to the platform for the first time, use the following default login credentials:

- Username: **admin**
- Password: **masterkey**

The following dialog window appears where you can create a new password:

Create your new password and then proceed with the configuration.

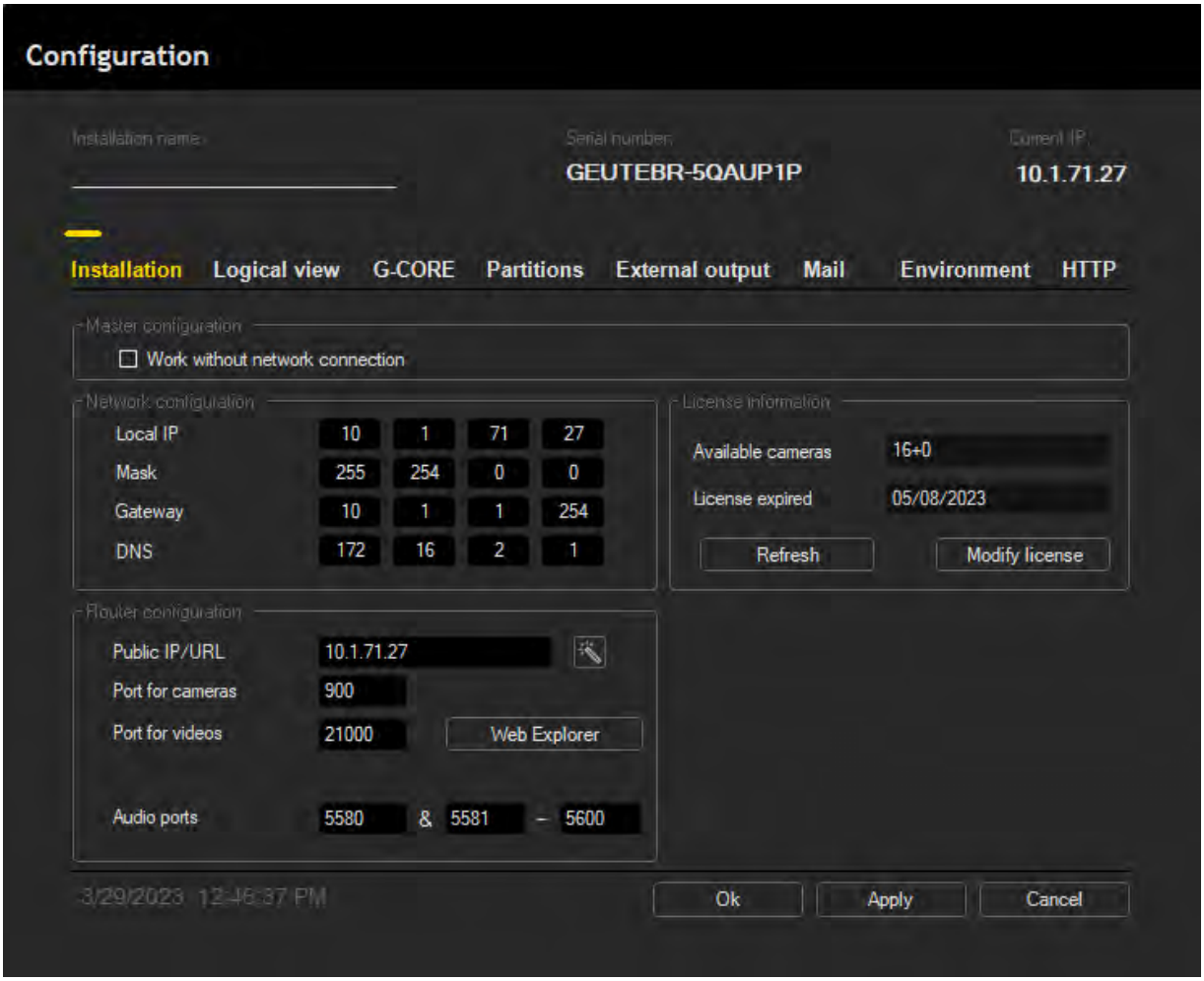
From now on, you can manage your login credentials using the options in the **Users** menu.

Configuration

Installation

How to open this dialog window:
Click the Configuration icon in the system overview window, enter your username and password, and click the Installation tab.

On the **Installation** tab you can define the connection settings of the system.



The general information of the installation is displayed in the upper section of the **Configuration** dialog window:

Name	Description
Installation name	Enter the name of the installation. This name applies to all devices in this installation.
Serial number	The serial number of the installation. It is assigned automatically during installation and cannot be changed.
Current IP	The IP address currently configured in the installation.

Master Configuration

Enable the Work without network connection option to work with only one unit that is not connected to a network. The network and router configuration is then disabled.

This option is available if only one unit is assigned to the installation (see **Logical View**).

Network Configuration

Note that Perimeter+ cannot be operated in a network segment that manages IP addresses via a DHCP server.

If you have questions about the network information, contact your local network administrator.

Name	Description
Local IP	Enter the IP address of the equipment.
Mask	Enter the local network mask.
Gateway	Enter the IP address of the local network gateway.
DNS	Enter the IP address of the network DNS.

Router Configuration

Name	Description
Public IP/URL	Enter the public IP address of the router.

Name	Description
	If the installation is not connected to G-Core and does not have a router, enter the IP address of the master unit (see **Logical View**). If the installation does not have a statistic IP address or there are multiple installations in the same network, enter a DNS address.
	Click this button to automatically retrieve the public IP address of the router.
Port for cameras	Enter the open port of the router used to view live cameras in G-Core.
Port for videos	Enter the open port of the router used to send videos to G-Core.
Audio Ports (Simple)	Enter the open ports of the router used to establish the audio communication with Simple. Enter the main port and the range of communication ports.
Web Explorer	Click this button to check the configured network connection or to access the router or cameras.

IMPORTANT: The TCP/UDP ports must be opened in the installation and redirected to the video analysis systems. If you do not know how to open the ports or are not authorized to manage the installation router, contact the network administrator.

License Information

Name	Description
Available cameras	Displays the number of cameras that can be installed in the system.
License expired	Displays the expiration date of the license.
Refresh	Click this button to update the license information.
Modify license	Click this button to activate or modify the license offline.

Logical View

How to open this dialog window:
Click the Configuration icon in the system overview window, enter your username and password, and click the Logical view tab.

If there is only one unit in the installation, you can skip this section and continue in the following section.

You can add or remove units from the installation in the Logical view tab. If the system consists of more than one unit, have the following settings in mind. Select the units that appear on the right (Available machines) to create the installation (This installation).

In the Available machines column, only units are displayed if the Work without network connection option is disabled (see Master Configuration).

The following buttons are available:

Button	Name	Description
	Add to installation	Adding units from the right panel as slaves allows you to integrate more cameras into the system. The unit moves into the left panel when you enter the IP it should have when you request it.
	Delete from installation	Releases a slave from the left panel so that it can be physically removed when it appears as a free unit in the right panel.
	Refresh	Refreshes the panel. The panel is automatically refreshed every few seconds.

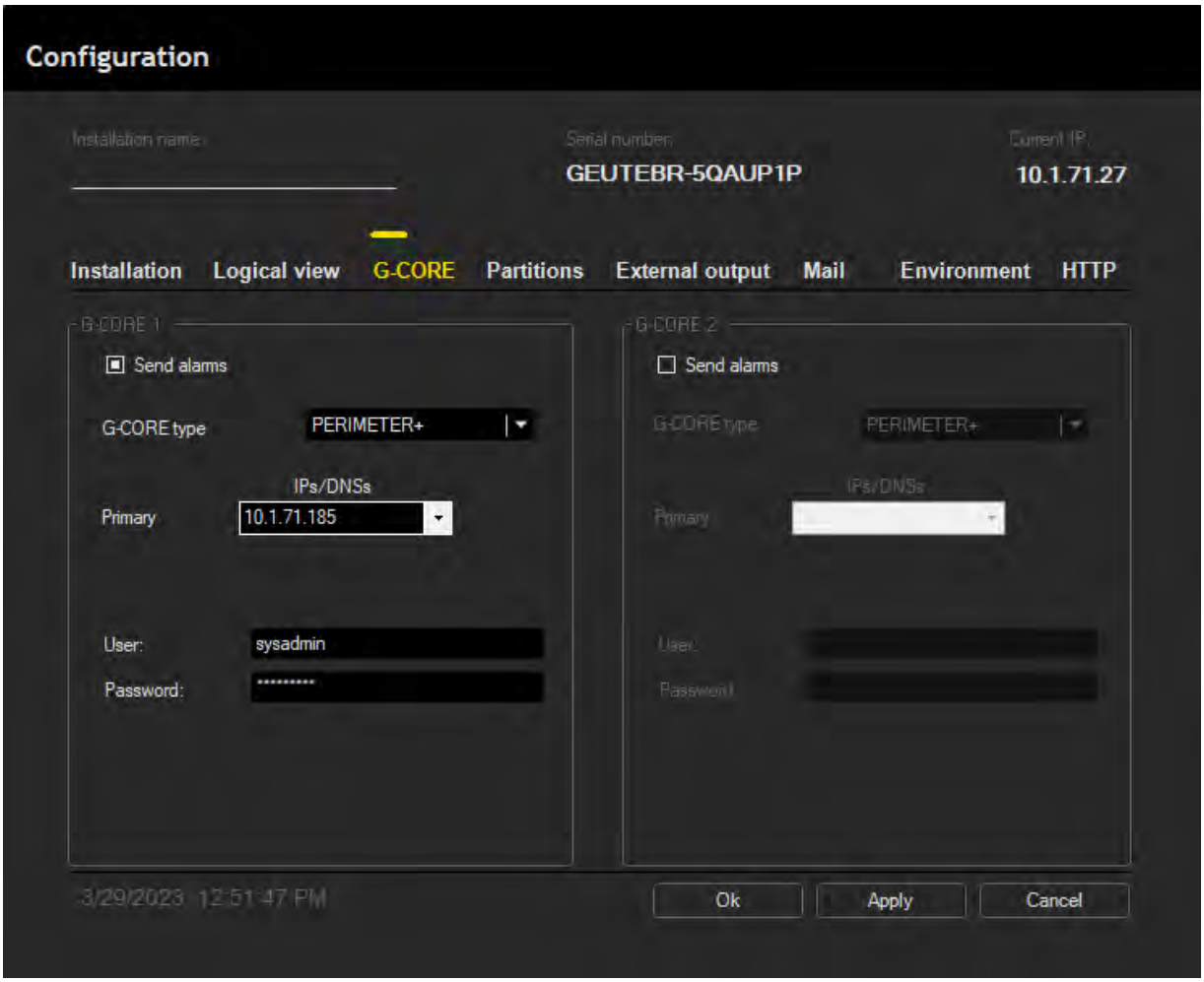
Button	Name	Description
	Change IP	Change the IP of the selected slave server.
	Save Backup	Creates a backup of the configuration.
	Replace installation machine	Restore a backup or replace a faulty server in the system.
	Reset	Reset the equipment to factory settings. **IMPORTANT:** If you reset the equipment to factory settings, you will lose all alarm information, videos and images from previous events. You do this at your own risk.
	Remote Access	Opens the remote console.

The units in the system can display different status icons:

Icon	Description
	This icon appears in the left panel to indicate that the unit in question is the master unit. This unit is displayed when the **Installation** tab has been configured and the unit has been restarted.
	This icon appears in the left panel to indicate that the unit in question is a slave unit that is functioning correctly. It also appears in the right panel to indicate that the unit in question can be added to the installation.
	This icon appears in the left panel to indicate that the unit in question is currently being turned on or off.
	This icon appears in the left panel to indicate that the server in question is turned off or has been incorrectly removed from the system.
	This icon appears in the right panel to indicate that the unit in question belongs to another installation and already has cameras, so it cannot be used in this installation.

G-Core

How to open this dialog window:
Click the Configuration icon in the system overview window, enter your username and password, and click the G-Core tab.



In the **G-Core** tab, in addition to the primary G-Core (**G-Core 1**), you can add a second one (**G-Core 2**). You can enter the following information:

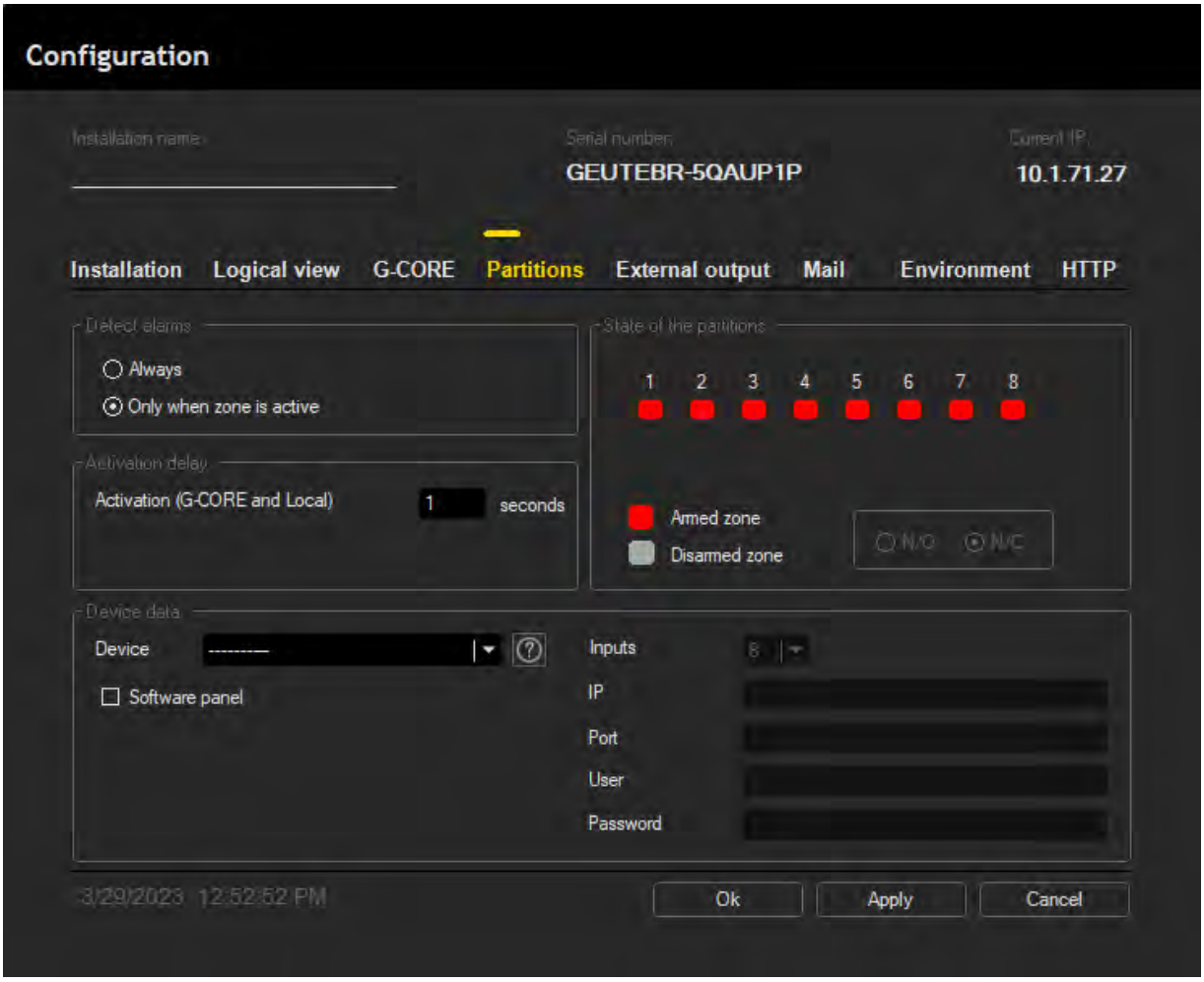
Name	Description
Send alarms (G-	Enable this option to send alarms to G-Core.

Name	Description
Core 1)	
Send alarms (G-Core 2)	Enable this option if you want to send each alarm with redundancy to another destination. You must enter the IP addresses of the new destination. The alarms will then be sent G-Core 1 and G-Core 2 simultaneously.
G-Core type	Select the protocol for sending alarms. • **PERIMETER+**: "VCA Alarm" actions are sent. • **G-CORE GENERIC**: "Custom Action Extended" actions are sent.
Primary (G-Core 1)	This is the primary IP address of G-Core. The IP part also accepts domain names.
Primary (G-Core 2)	This is the TCP port. The IP part also accepts domain names. This address is used if the primary address fails. If G-Core does not have two connections or different IP addresses, enter the primary address twice.
User	Enter the G-Core username.
Password	Enter the G-Core password.

Partitions

How to open this dialog window:
Click the Configuration icon in the system overview window, enter your username and password, and click the Partitions tab.

On the Partitions tab, you can define the behavior of the system depending on the signals from an external device, such as an alarm or detection device.



The following options are available:

Detect Alarms

Name	Description
Always	**Always** means that the detection rules work even if the partition to which they belong is disarmed with the peculiarity that they neither send the alarms to G-Core nor activate the relay, although these options would be active in the rule configuration. When the partition is armed, the generated alarms are sent to G-Core and the relay activated, provided that these response options are configured in the rule.

Name	Description
Only when zone is active	**Only when alarm is triggered** means that the detection rules do not work if the partition they belong to is disarmed. As for the other option, when the partition is armed, the generated alarms are sent to G-Core and the relay activated, provided these responses are configured in the rule.

Select Always if you want to store videos of everyday activity, or Only when zone is active to optimize storage capacity.

Activation Delay

These are the seconds that must elapse from the activation of a partition until detection begins, or until the transmission to G-Core begins or, in the case of Detect alarms always. This delayed output feature gives the user time to leave the site without alerting the G-Core.

Device Data

Data from external device: Inputs/Outputs can come from an internal device, an USB device, an IP external device or through the Software panel. If you use the internal inputs INTERNAL TYPE-A, you can choose between 4 and 8 inputs.

Which is my device: The ? button next to the device type. It opens a document with information about the different devices which are compatible with the system.

State of the Partitions

Partition status (N/O, N/C): Select whether the input signal is normally open or normally closed.

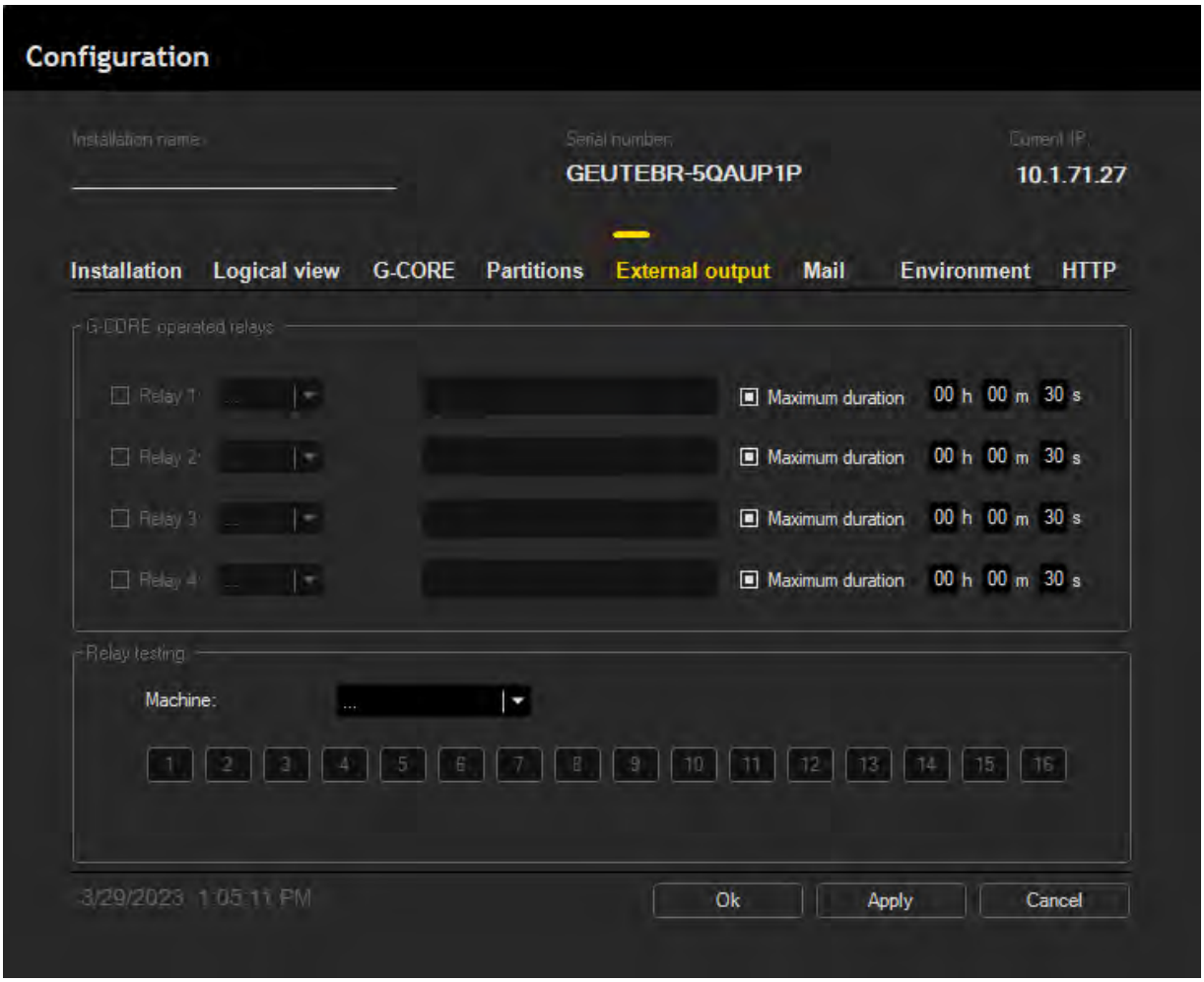
In the boxes numbered 1 to 8 you can view the status of the inputs in real time (the active inputs are displayed in red and the inactive ones in gray). If you change the status from N/O to N/A or vice versa, you must apply the changes to view the new status.

External Output

How to open this dialog window:
Click the Configuration icon on the system overview window, enter your username and password, and click the External output tab.

On the **External Output** tab, you can configure the relay output of the system if you have acquired the additional output module.

G-Core Operated Relays



You can set up to four external outputs per installation which can be activated from G-Core. In other words, here you define the information that are operated by G-Core when you have subscribed to this service.

Each relay output has the following options:

Name	Description
Relay (Y/N)	Select the check box if the respective output of the additional module is available.

Name	Description
Drop-down menu	Select the type of alarm to activate the relay (a light, an audible warning, etc.)
Test	This button is available when the relay has been defined for remote activation. Press the button to check if the device is correctly activated or deactivated.
Text box	Add additional information about the respective output that the G-Core operators see.
Maximum duration	Check this option to set a maximum relay activation time. Enter the maximum time that the alarm will be continuously activated.

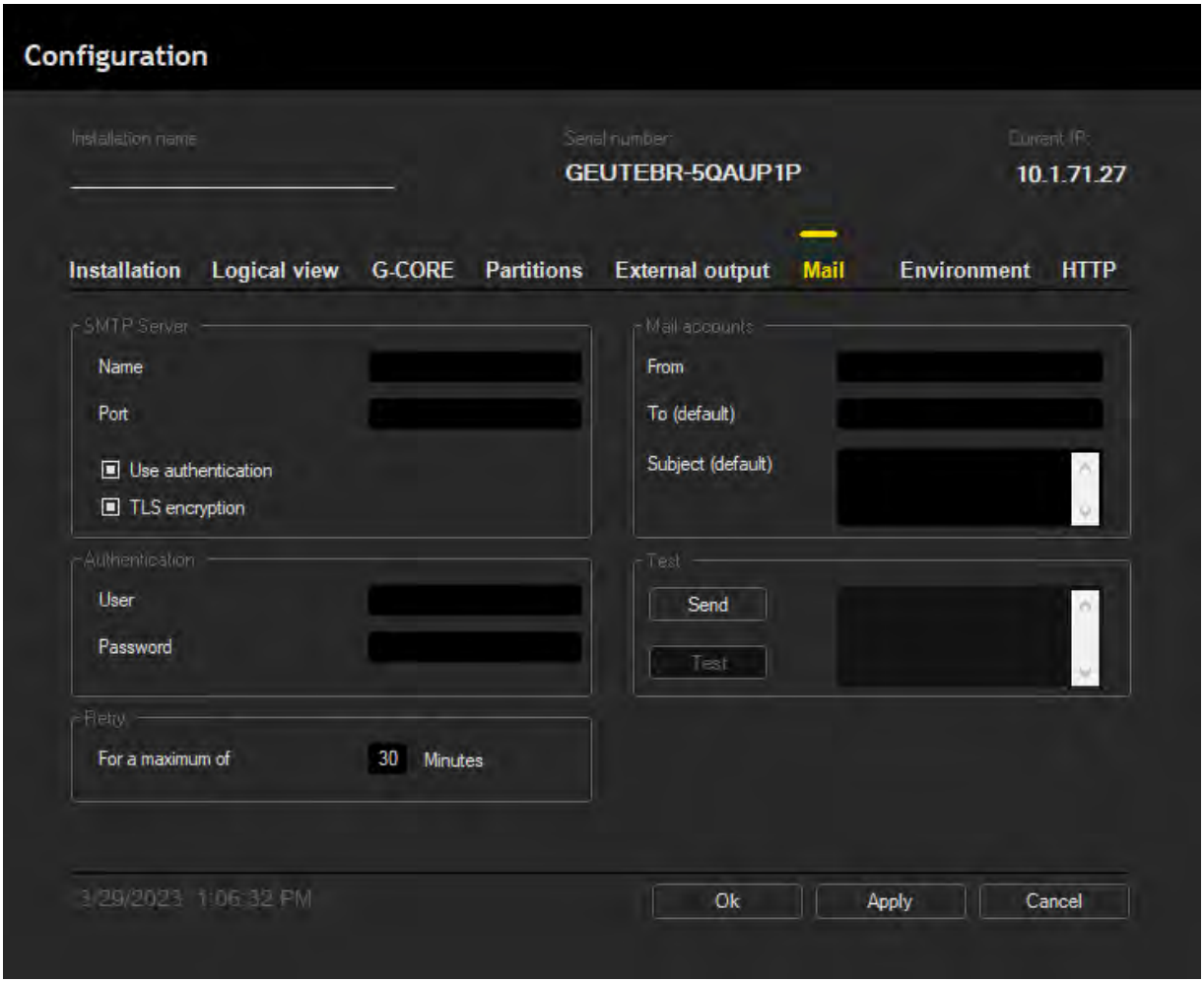
Relay Testing

In the Relay testing section, you can test whether the relays are correctly activated in all units of the installation. Select the desired unit in the Machine drop-down menu and then click the corresponding button to activate the selected relay.

Mail

How to open this dialog window:
Click the Configuration icon in the system overview window, enter your username and password, and click the Mail tab.

On the Mail tab, you can configure the email account to be used for sending alarm notifications. For sending email alarm notifications, this option must be enabled (**Send E-Mail**).



SMTP Server

If you do not know your account settings, contact your email provider.

Name	Description
Name	Enter the name of the outgoing mail server (SMTP).
Port	Enter the port of the SMTP server. The default port for SMTP is 25. If your server requires a secure connection (SSL), the default port is 995, although other providers such as G-Mail use 587 or other ports.

Name	Description
Use authen-tication	Enable this option if the SMTP server requires authentication.
TLS encryption	Enable this option if the SMTP server uses the TLS encryption method.

Authentication

Name	Description
User	Enter the username of the outgoing mail server (SMTP).
Password	Enter the user password.

Retry

Specify the maximum time in minutes for retries if the email could not be send.

Mail Accounts

Name	Description
From	Enter the email of the sender account. The username and email can be the same.
To (default)	Enter the default recipient. This information is used to automatically fill in the fields when alarm rules are created. The recipient can be changed manually to send to a different addressee (see **Send E-Mail**).
Subject (default)	Enter the email subject that the recipient sees when they receive an alarm notification.

Test

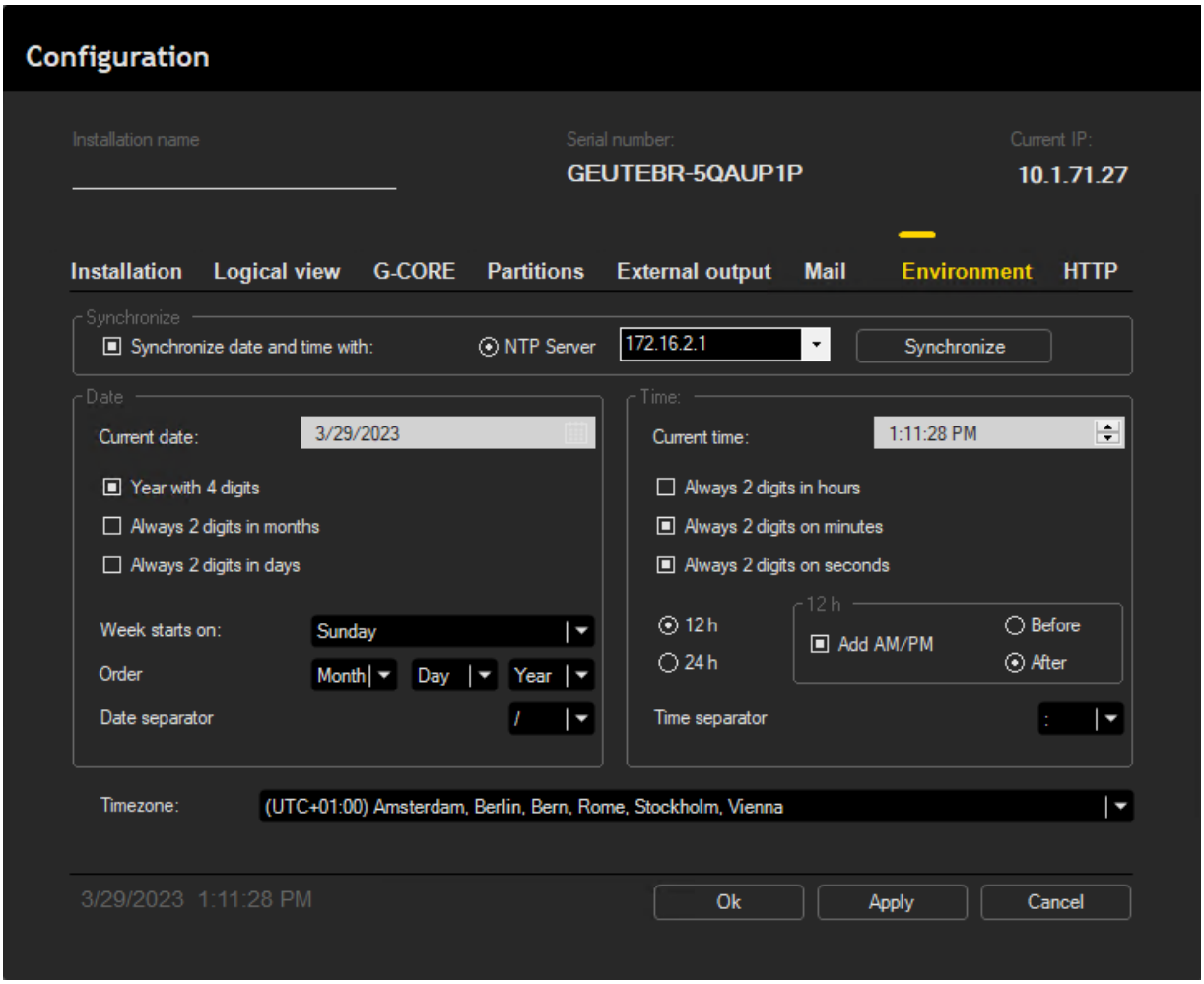
Name	Description
Send	Click this button to send a test email from the configured sender

Name	Description
	account (**From**) to the default address (**To (default)**).
Test	Click this button to check if the email was sent correctly.

Environment

How to open this dialog:
Click the Configuration icon in the system overview window, enter your username and password, and click the Environment tab.

On the **Environment** tab you can define the time configuration of the equipment.



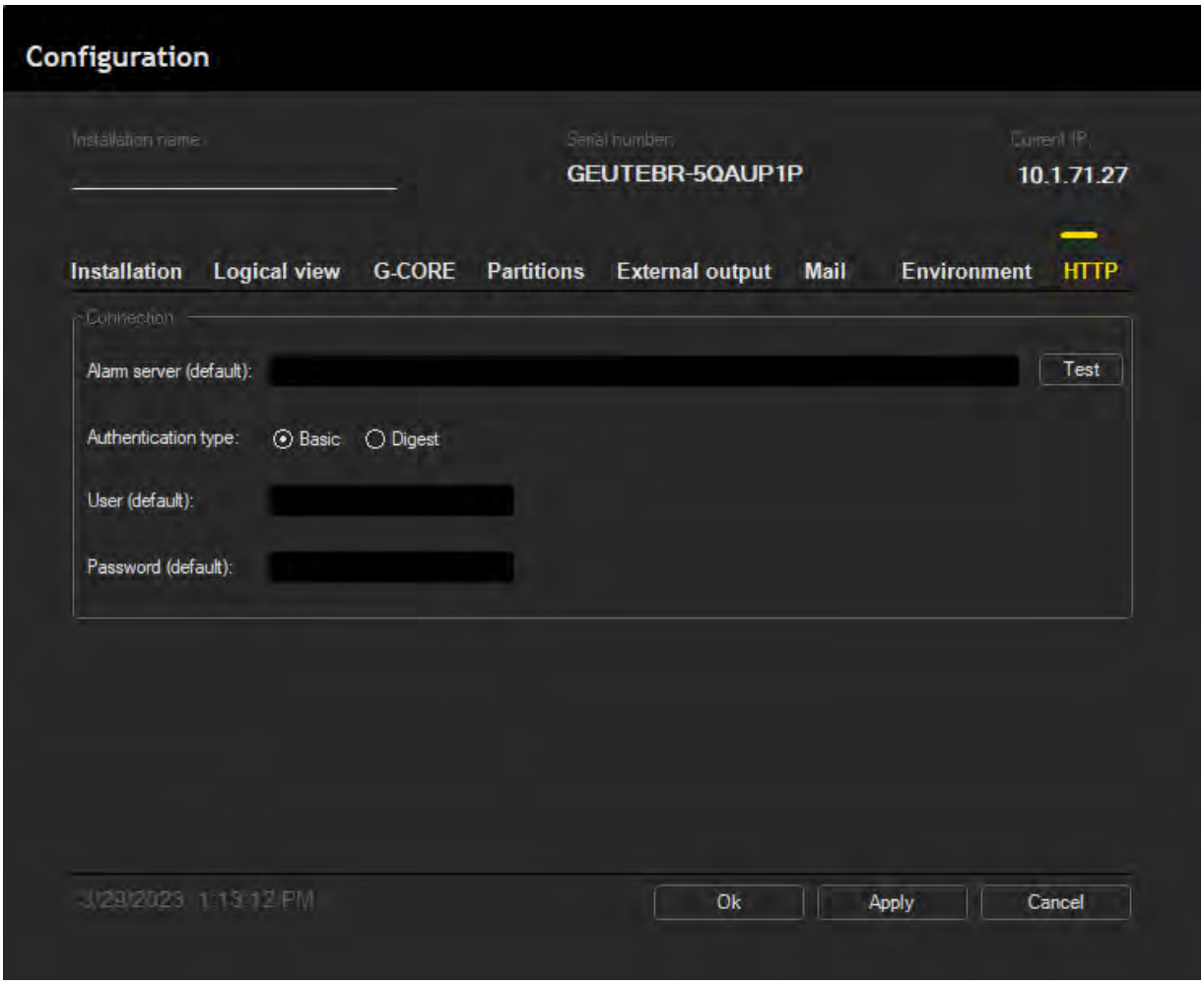
To automatically synchronize the time with an NTP server, enable the **Synchronize date and time with** option. You can enter any address or choose from a set of default options. Then click **Synchronize**.

Alternatively, you can define the date and time manually using the options available in the **Date** and **Time** sections. Select the **Timezone** for your location to automatically adjust the system time.

HTTP

How to open this dialog:
Click the Configuration icon in the system overview window, enter your username and password, and click the HTTP tab.

On the **HTTP** tab, you can define the default configuration for the HTTP feature that used in the **Response** dialog window of the camera **Rule Configuration**.



Name	Description
Alarm server (default)	Enter the HTTP address.
Test	This button allows you to test the connection with the specified HTTP address. Depending on whether the connection is established or not, the background of the URL text box turns green or red.
Authentication type	Select whether the authentication type is **Basic** or **Digest**.
User (default)	Enter your username.
Password (default)	Enter your user password.

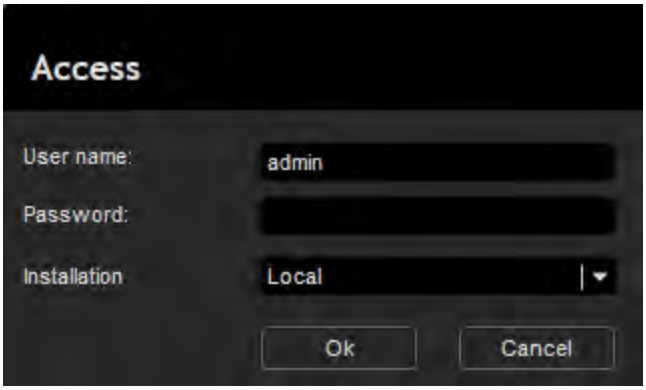
Cameras

Login

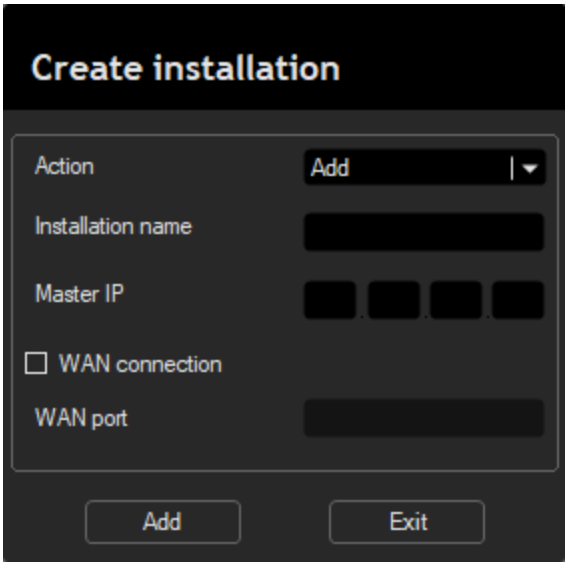
How to open this dialog window:
Click the Cameras icon in the system overview window.

You will be asked to enter your username and password before the system allows you to view cameras or make changes. The name reserved for the system administrator is **admin**. When you start the system for the first time, leave the default password blank to log in to the system (see **Setting Your Password**).

It is recommended to configure the system with several user types to enhance security when logging in to the system.



The system allows you to manage other installations from the same camera viewer. This option is only useful for surveillance system with the **ViewClient** program installed that control remote installations. To do this, select the **Manage installations** option from the **Installation** drop-down menu:



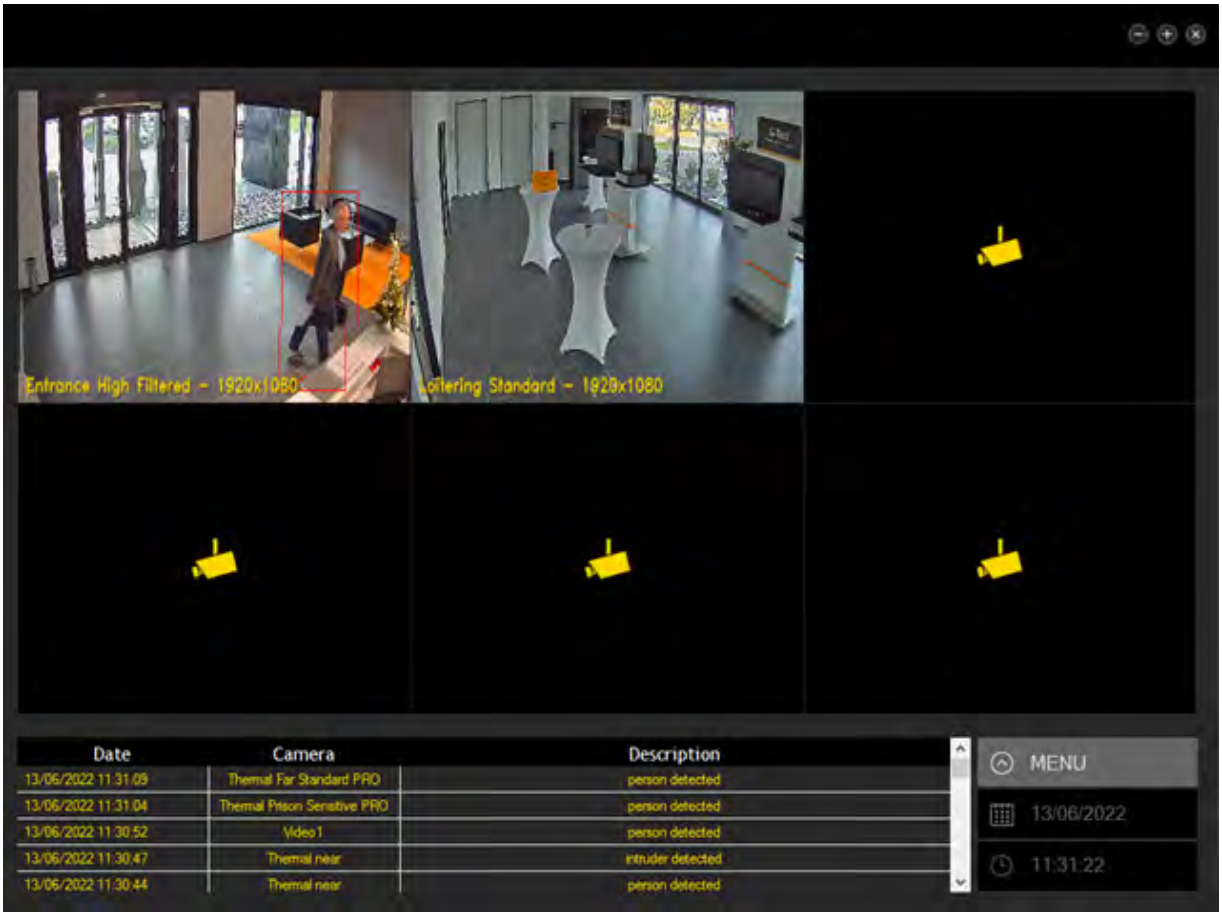
Name	Description
Action	You can select between **Add**, **Add this**, **Edit** or **Delete**. Select **Add this** to add the local installation automatically.
Installation name	Enter the local name of the installation.
Master IP	Enter the local IP of the master equipment of the installation you want to connect to.
WAN Connection	Enable this option if the server is not on your local network.
WAN port	This port is required for the communication between your unit and the master server unit. **You must have advanced knowledge of network administration and SQL redirection to use this setting. Contact your network administrator or the supplier of the unit to obtain more information.**

Click **Add** to save the changes. You can then select the new created site from the **Installation** drop-down menu.

Viewer

How to open this dialog window:
Click the Cameras icon in the system overview window and enter your username and password.

After a few seconds the system starts and the main window appears:



The display area is divided into several viewers. You can define the number of viewers in **View** menu.

To assign a camera to an empty viewer, right-click the viewer in which you want to display the camera and select a camera (or camera group) from the drop-down menu.

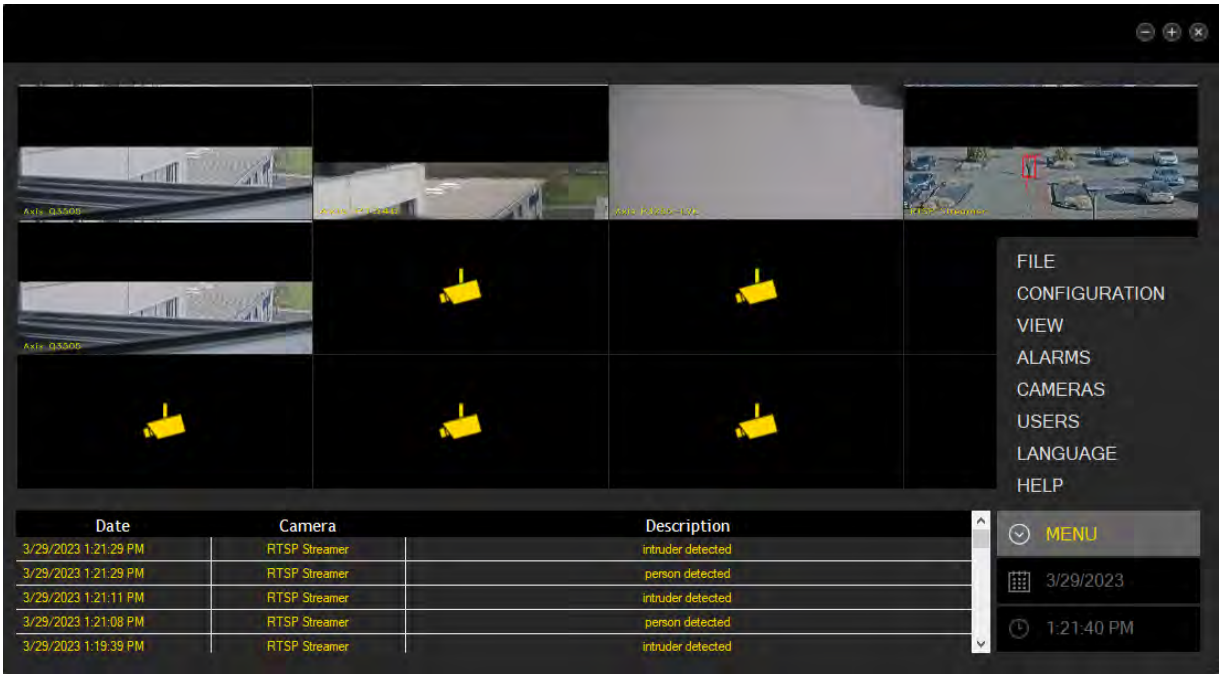
Repeat the process until you have assigned the images from the cameras to the viewers.

Menu

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, and click the Menu button.

The menu bar is located at the bottom right of the main screen. When you click on the Menu button, the following menu items are displayed:

- **File**
- **Configuration**
- **View**
- **Alarms**
- **Cameras**
- **Users**
- **Language**
- **Help**



File

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select File.

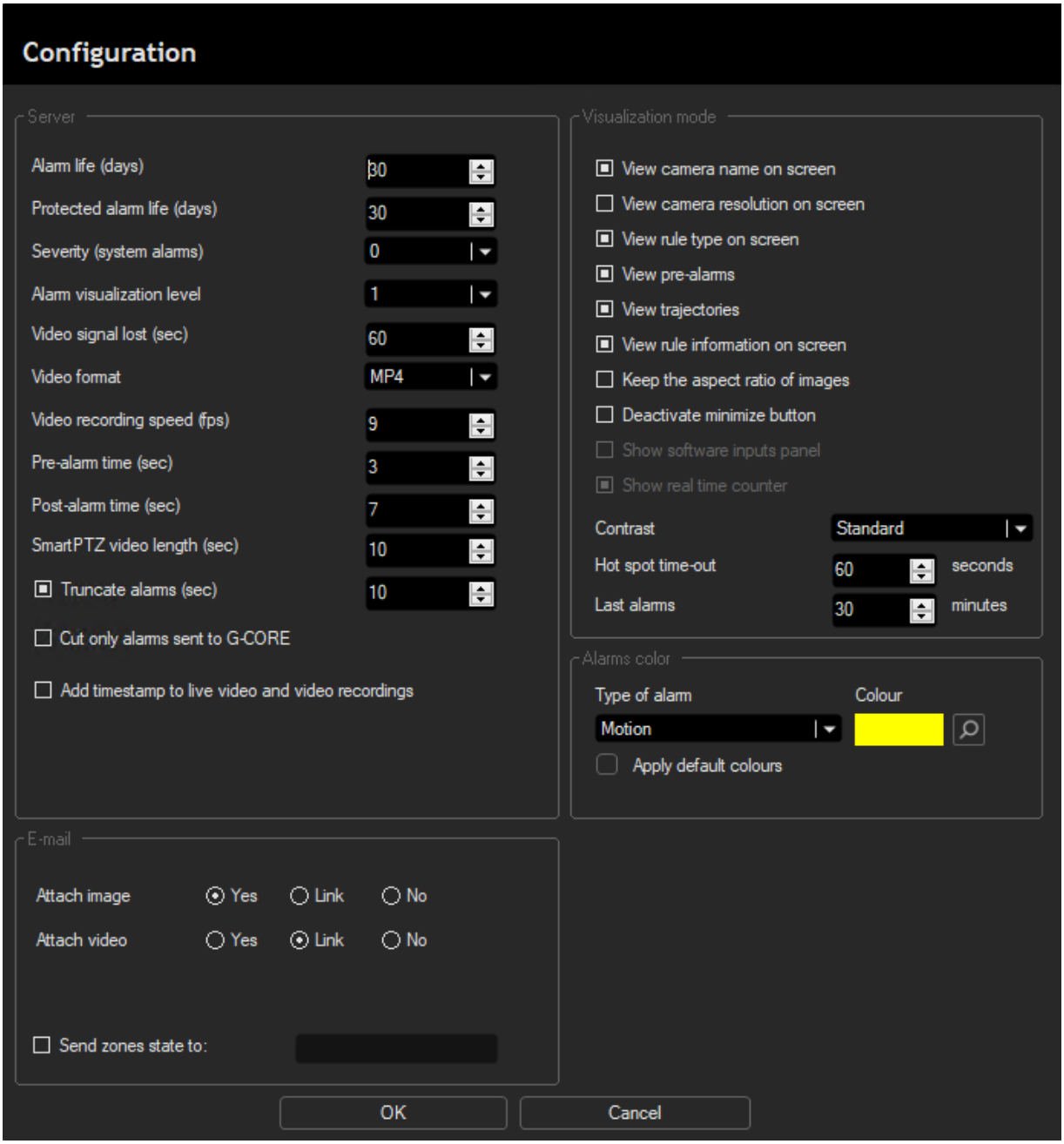
Selecting the Restart option restarts all equipments at the same time.

Selecting the Exit option closes the graphical user interface of the application. In the latter case, the system overview no longer displays the cameras, but the defined detection rules continue to operate on the server and the system continues to detect the defined alarms.

Configuration

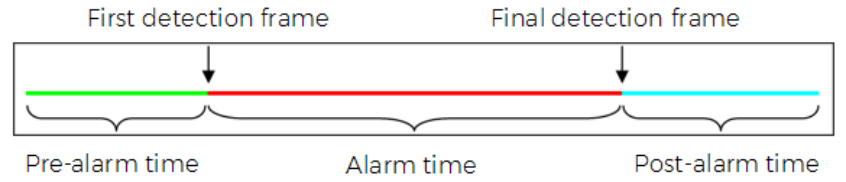
How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Configuration.

In the Configuration menu item you can configure some global settings:



Server

Name	Description
Alarm life (days)	Set the maximum alarm life in the system.

Name	Description
Protected alarm life (days)	Set the maximum protected alarm life in the system.
Severity (system alarms)	Severity of alarms generated by the system (loss of connection, loss of camera signals, etc.).
Alarm visualization level	Display of alarms above a certain severity level in the section of the last alarms.
Video signal lost (sec)	The number of seconds that elapse without a camera signal before a loss of signal alarm is generated.
Video format	Format of the recording file.
Video recording speed (fps)	Specifies the speed (fps) of the recorded video.
Pre-alarm time (sec)	Recording time before the alarm.
Post-alarm time (sec)	Recording time after the alarm.
SmartPTZ video length (sec)	Recording time of the SmartPTZ video.
Truncate alarms (sec)	Maximum alarm recording time including pre-alarm time. The alarm recording time consists of pre-alarm time, the alarm time and the post-alarm time, as shown in the following diagram.  **Example** 3 seconds pre-alarm time, 7 seconds post-alarm time and the intruder is detected in the scene for 30 seconds: - If the **Truncate alarms** option is disabled, you

Name	Description
	get 40-second alarm recording time. - If the **Truncate alarms** option is enabled, you get only the first seconds of the alarm video.
Cut only alarms sent to G-Core	The alarm video is truncated only if the rule that generated it has to be sent to G-Core.
Add timestamp to live video and video recordings	Add timestamps to live video and video recordings.

E-Mail

Name	Description
Attach image	Select whether you want to attach the image to the alarm notification email as an image file, as a link, or not at all.
Attach video	Select whether you want to attach the video to the alarm notification email as an video file, as a link, or not at all. By default, the file is not attached to the email to speed up transmission.
Send zones state to	Enable this option to send the zones status to a specified email address.

Visualization Mode

Name	Description
View camera name on screen	Displays the camera name.
View camera resolution on screen	Displays the resolution of the camera.
View rule type on	Displays the name of the rule type (e.g. intruder, person,

Name	Description
screen	etc.).
View pre-alarms	Displays the systems detection. This is for display only and does not generate alarms.
View trajectories	Displays the trajectories of the detections superimposed on the screen.
View rule information on screen	Displays additional information with rules as arrows.
Keep the aspect ratio of images	Keeps the image proportions constant by increasing or decreasing the resolution of the display monitor.
Deactivate minimize button	Removes the minimize button from the application.
Show software inputs panel	Allows the user to arm and disarm the system using this application.
Show real time counter	Displays the counter in a corner of the image when a counter rule is created.
Contrast	Choose between standard, maximized, darker, clearer or equalized contrast.
Hot spot time-out	The number of seconds that hot spot mode is activated.
Last alarms	The maximum time that events are stored in the recent alarms section.

Alarms Color

Name	Description
Type of alarm and Color	This option allows you to assign different colors to each alarm.
Apply default colors	This option allows you to to reset the default colors to the factory settings.

View

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select View.

This menu contains the following options:

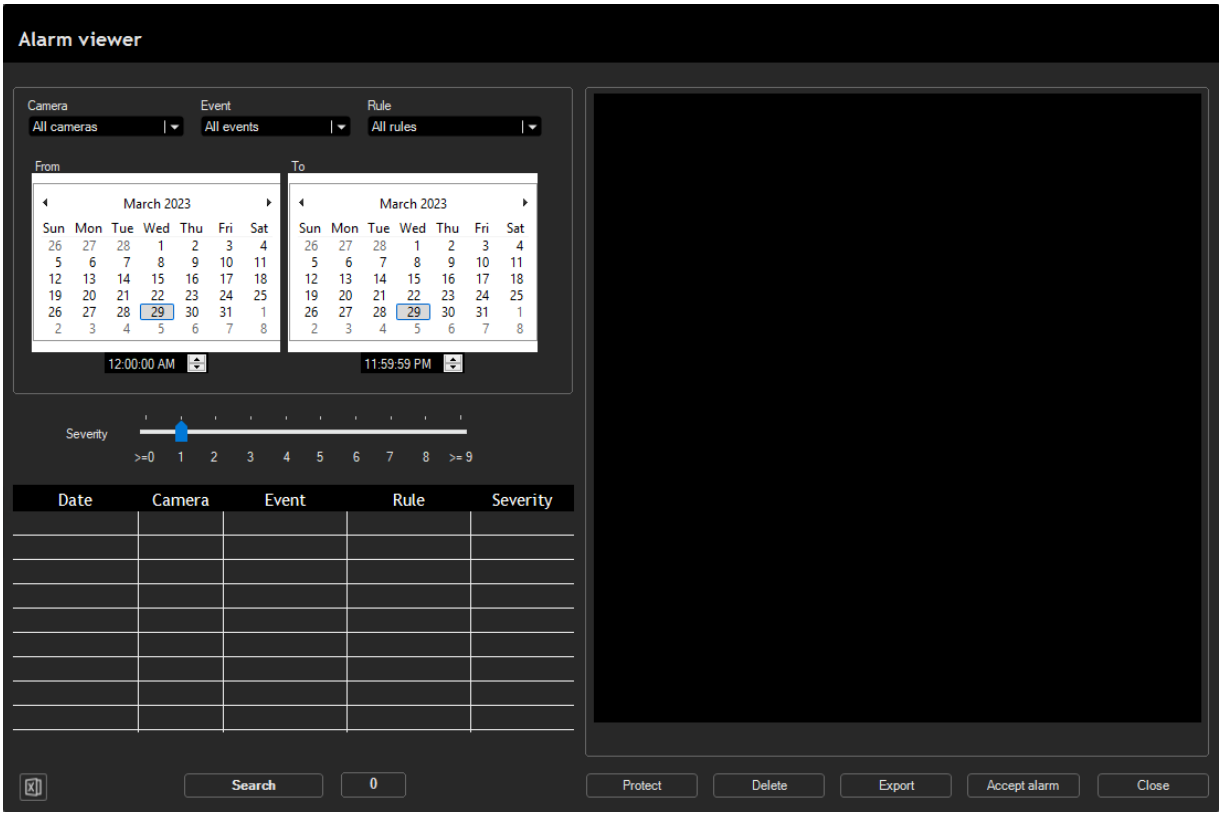
Name	Description
Distribution	The dialog window for configuring the camera layout opens. You can choose between 1 and 4 rows and 1 and 4 columns, so that you can observe a maximum of 16 cameras simultaneously.
Full Screen	Switches the selected monitoring window to full screen mode. The graphical interface disappears, so that only the viewers currently in the display area are visible. To switch back to the graphical interface, press the **Esc** key.
Select	Allows you to select one of the predefined views. Camera views are groups of cameras used to quickly display sets of cameras.
Add / Delete	Allows you to save the current view (viewer and camera selection configuration) or to delete the current view.
Colormap	For thermal images, you can choose to view the images as gray scale images or view the images with a color map to increase the contrast at certain temperatures.

Alarms

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Alarms.

The Alarm viewer dialog window displays the events and alarms detected by the system. The system records a few seconds/minutes from the time an alarm is activated. In the alarm viewer you can play back the recording.

The alarm viewer can be opened from the menu or by double-clicking on the required alarm in the list of recent alarms.



Alarm Search

By default, the filter menus are in the **All** position, which means that no filtering is performed and events from all cameras, all events and all rules are selected.

The following filters are available for alarm search:

Name	Description
Camera	Select a camera if you only want to see alarms triggered by a specific camera.
Event	Select an event if you want to see only alarms of a specific type.
Rule	Select a rule if you only want to see only alarms generated by a specific camera rule.
From	Select a date and time. The system will only show alarms after this date.
To	Select a date and time. The system will only show alarms before this date.

Name	Description
Severity	Select a severity level if you only want to display only alarms whose severity level is equal to or higher than the specified number. Alarms with a lower severity level than the selected one are filtered out during the search.

When you have configured all of the alarm filter options, click the **Search** button to start the alarm search. If there are more than 1,000 alarms, the system will display only the first 1,000 in the search.

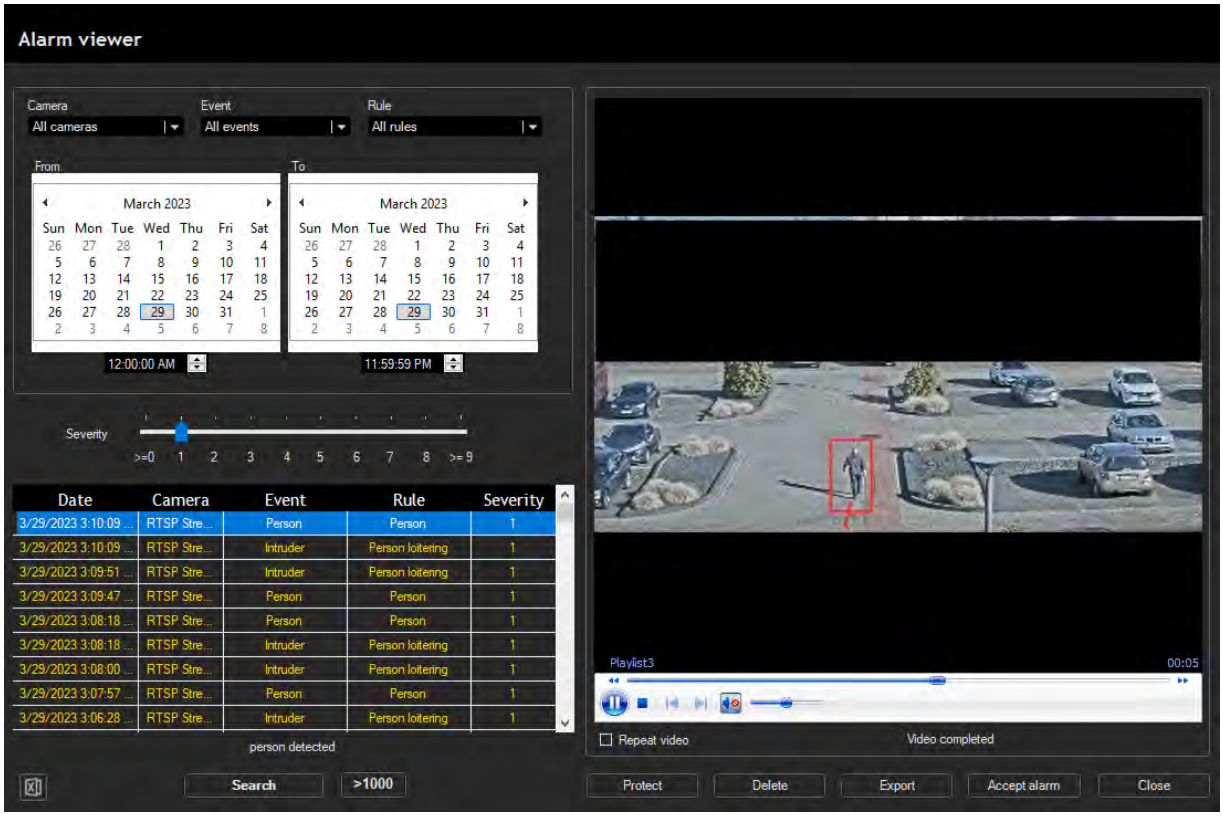
The following information is available for each alarm:

Name	Description
Date	Date and time when the event was detected.
Camera	Camera on which the event was detected.
Event	Event type defined in the rule (detection of people, vehicles, other objects, movements, tampering, etc.).
Rule	User-defined rule that was violated and triggered the alarm.
Severity	Severity of the alarm.

Displaying an Alarm

To view an alarm, click on the list of found events/alarms. The video area shows the image of the time of detection. To view the video of the event, double-click on the alarm list or video area.

The video area starts playing the recorded video of the event related to the alarm.



Use the controls of the video window to play the video:

Control	Function	Description
⏪	Rewind	Click this button to rewind the camera images.
Time bar		You can instantly jump to a specific time in the video. Click and drag the time bar to a specific position in the video.
⏩	Fast forward	Click this button to fast forward the camera images.
▶ / ⏸	Play / Pause	Click this button to start or pause the playback of the selected video.
	Stop button	Click this button to stop the playback of the selected video.

Control	Function	Description
	Previous / Next	Click this button to jump forward one picture in the video playback.
	Volume keys	Click this button to enable or disable the video sound.
Repeat video		Select this option to repeatedly display a video sequence or event. The same sequence will play indefinitely until you close the video window or deselect this option.

Other Actions

The following buttons are available for other actions:

Name	Description
Save As 	To export the list of alarms from the current search to a .csv file, click this button and select a destination for your file.
Search	When you have configured all of the alarm filter options, click this button to start the alarm search. If there are more than 1,000 alarms, the system will display only the first 1,000 in the search.
Protect	When you select an alarm and click this button, the alarm is defined as a "protected alarm". It is marked in yellow and has a specific configuration, as these types of alarms have a different maximum lifetime than other alarms.
Delete	To delete an alarm from the system, click on the alarm you want to delete and click this button. The alarm will be automatically deleted from the alarm list, along with the video and image of the event. **When you delete an alarm, all information about the selected alarm is lost. Only profiles in administrator mode can perform this action.**
Export	To export the video of an alarm, insert a USB stick, select an alarm from the list and click this button. There are two ways to export an alarm:

Name	Description
	• Full signed alarm: A signed binary file is exported along with the video file, verifying of the authenticity of the video. This method is used to protect the video from copying, manipulation, or fraud. • Only the video file is exported: A file browser window appears where you can select the USB drive.
Accept alarm	The alarms appear in red if they have not been validated and black if they have been validated. Validating an alarm means confirming to the system that the alarm has been verified by the personnel responsible for controlling it. To accept an alarm, click with the mouse on the alarm you want to accept. Click the **Accept alarm** button and the alarm automatically turn black. If the rules are configured with the **Repeat sound until alarm acknowledged** option (see **Response**), the system will make a sound until the security personnel accept the alarm.

Cameras

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.

The **Camera** menu contains the following areas:

- 1 Cameras (see **Camera Configuration**, **Device Configuration**, **Tune**)
- 2 Camera Groups (see **Camera Groups**)
- 3 Rules (see **Rule Configuration**)
- 4 Preview of the selected camera image
- 5 (see **Conceptual View**)

Users

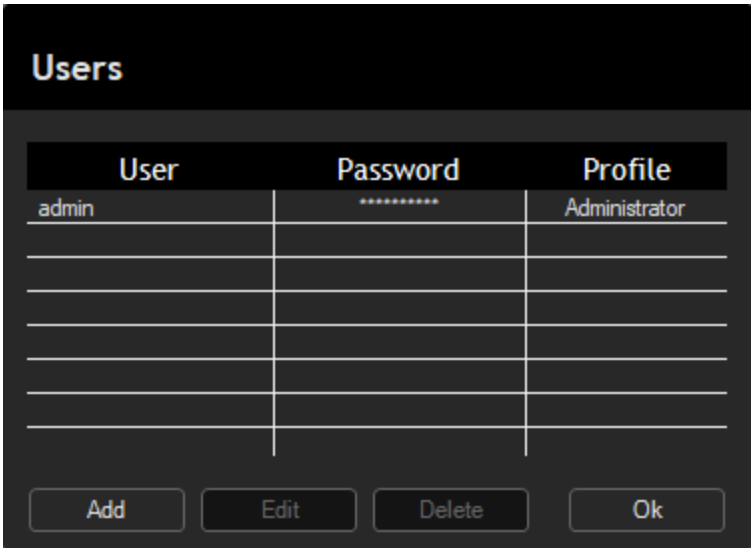
How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Users.

The **Users** menu contains the following options:

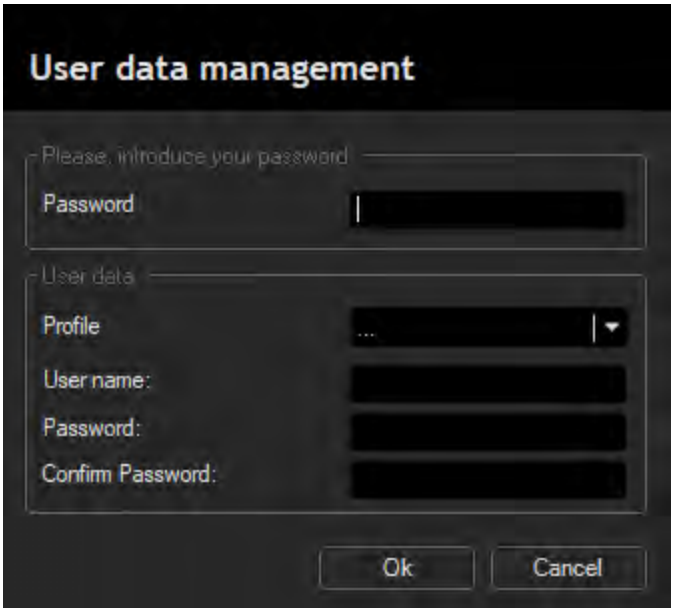
- **Manage**: Create new users, or modify or delete existing users.
- **Profiles**: Create, modify, or delete the specific actions allowed for each profile.
- **Log**: View the command log with the actions executed by each operator.

Manage

When you select **Manage**, the following window appears showing the existing users:



You can add, edit or delete all user information: security profile, user name and password.



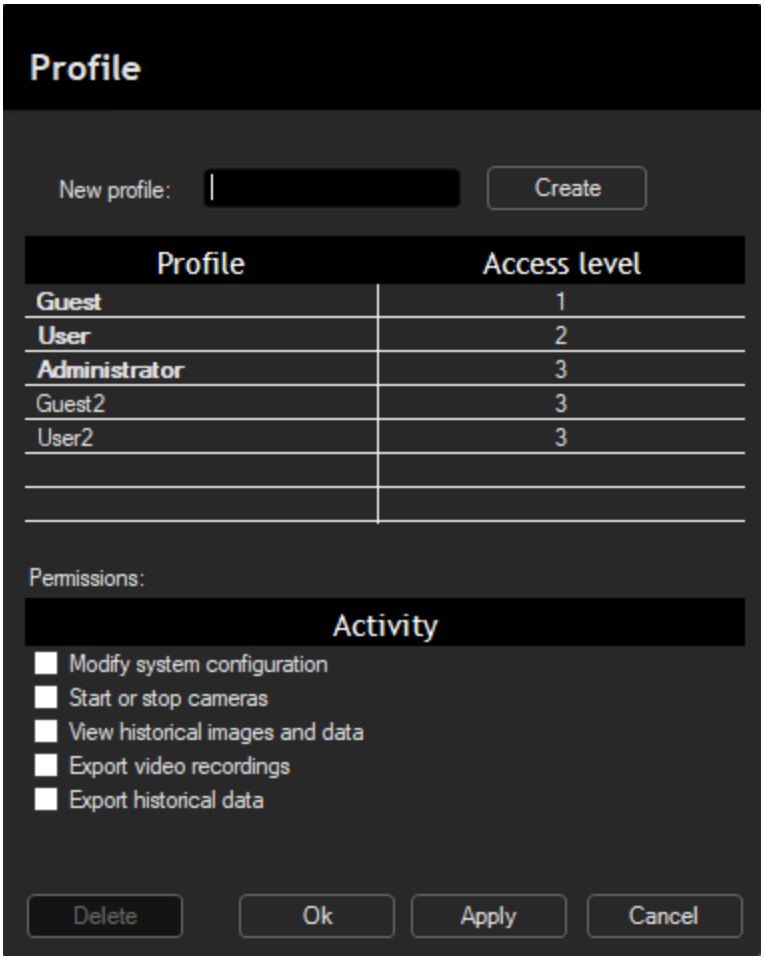
The three security levels are:

- **Administrator** (with all options available except camera adjustment)
- **User** (with more limited options)
- **Guest**

The system has two alternative profiles, **User2** and **Guest2**, with some extra options for the User and Guest profiles, respectively.

Profile

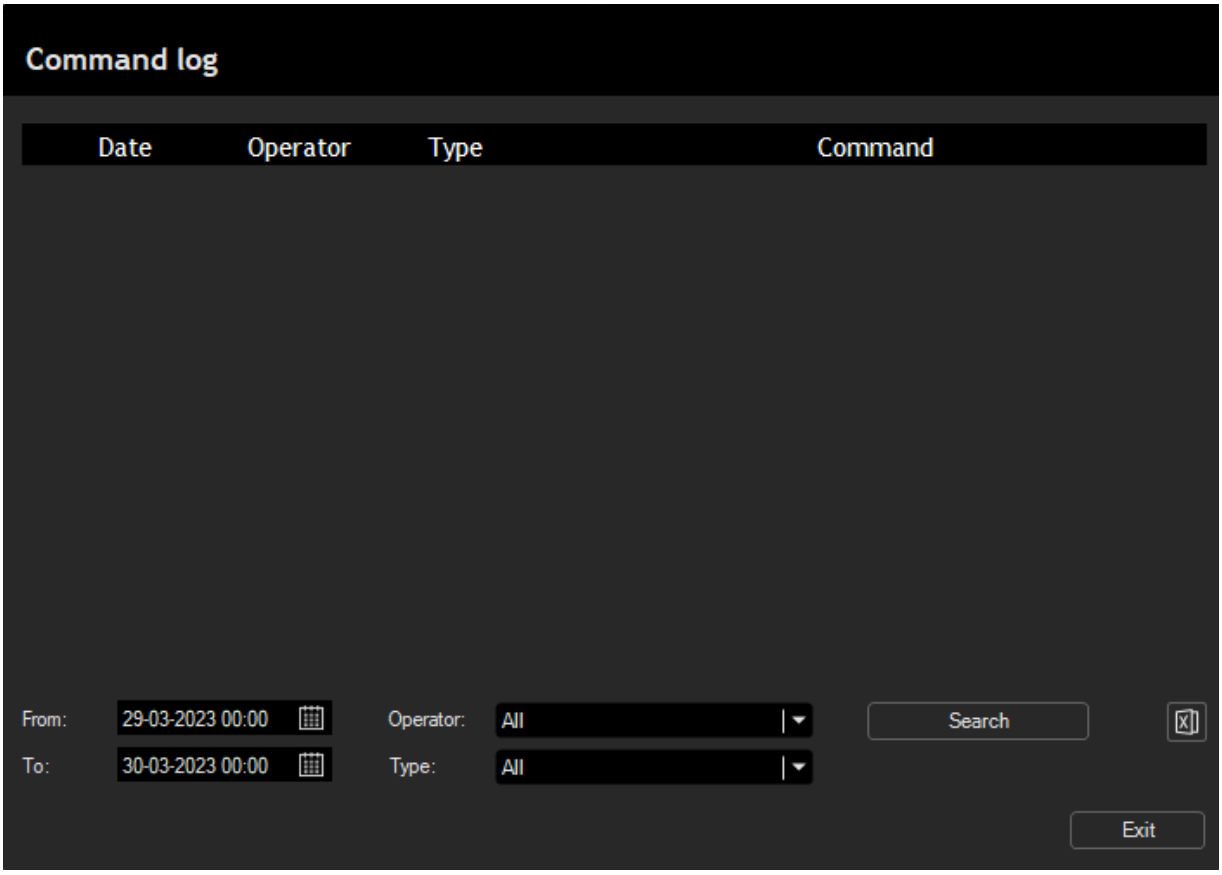
The **Profile** option allows you to define new user profiles with customized options for each of them.



To create a new profile, enter the name of the new profile (or select one from the list to modify it). Then select the permissions for the new profile from the list. Depending on the permissions you choose, an "Access level" is assigned to the profile. Guest, User and Administrator profiles are system-specific and cannot be modified or deleted.

Log

When you select **Log**, the following dialog window appears:



You can display the action log sorted by **Operator**, filtered by defined **Types** (general, cameras and rules) and by time periods selected by **Calendar**.

Language

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Language.

Use the **Language** option to change the language of the application. The languages available are English, French, Spanish, Italian, German, Portuguese, Catalan and Hebrew.

For your changes to take effect, close the application and restart the graphical interface.

Help

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Help.

This menu contains the following options:

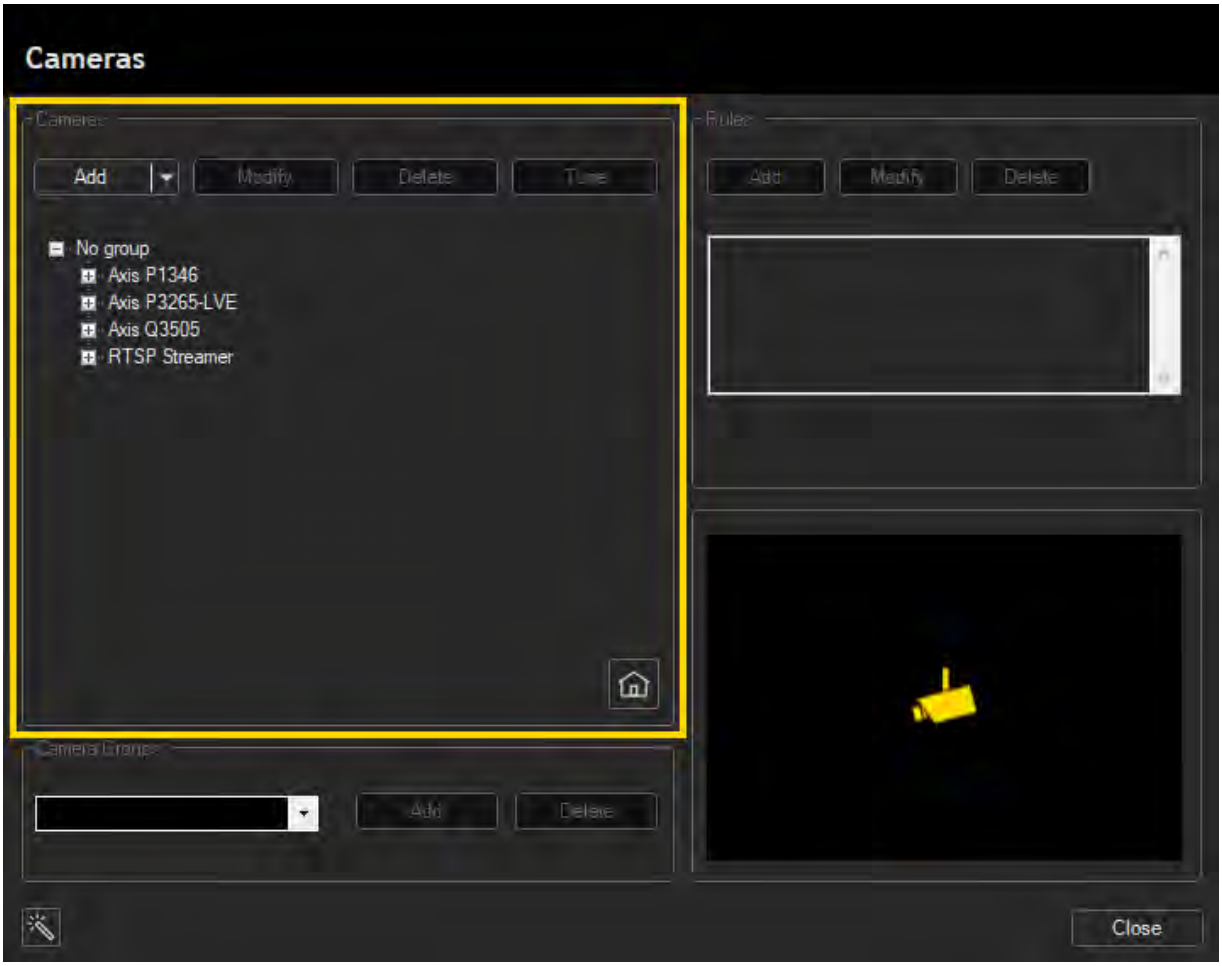
Name	Description
System information	Displays statistics about the available storage space and the total time of recordings in the equipment.
View license terms	Displays the terms and conditions of the agreement.
About	Displays the software version and information about the manufacturer.

Camera Configuration

The first step to configure your system is to define the cameras that are physically connected to the system. The cameras defined in the system are displayed in the camera list.

Note that the system cannot receive images from a camera until it has been configured.

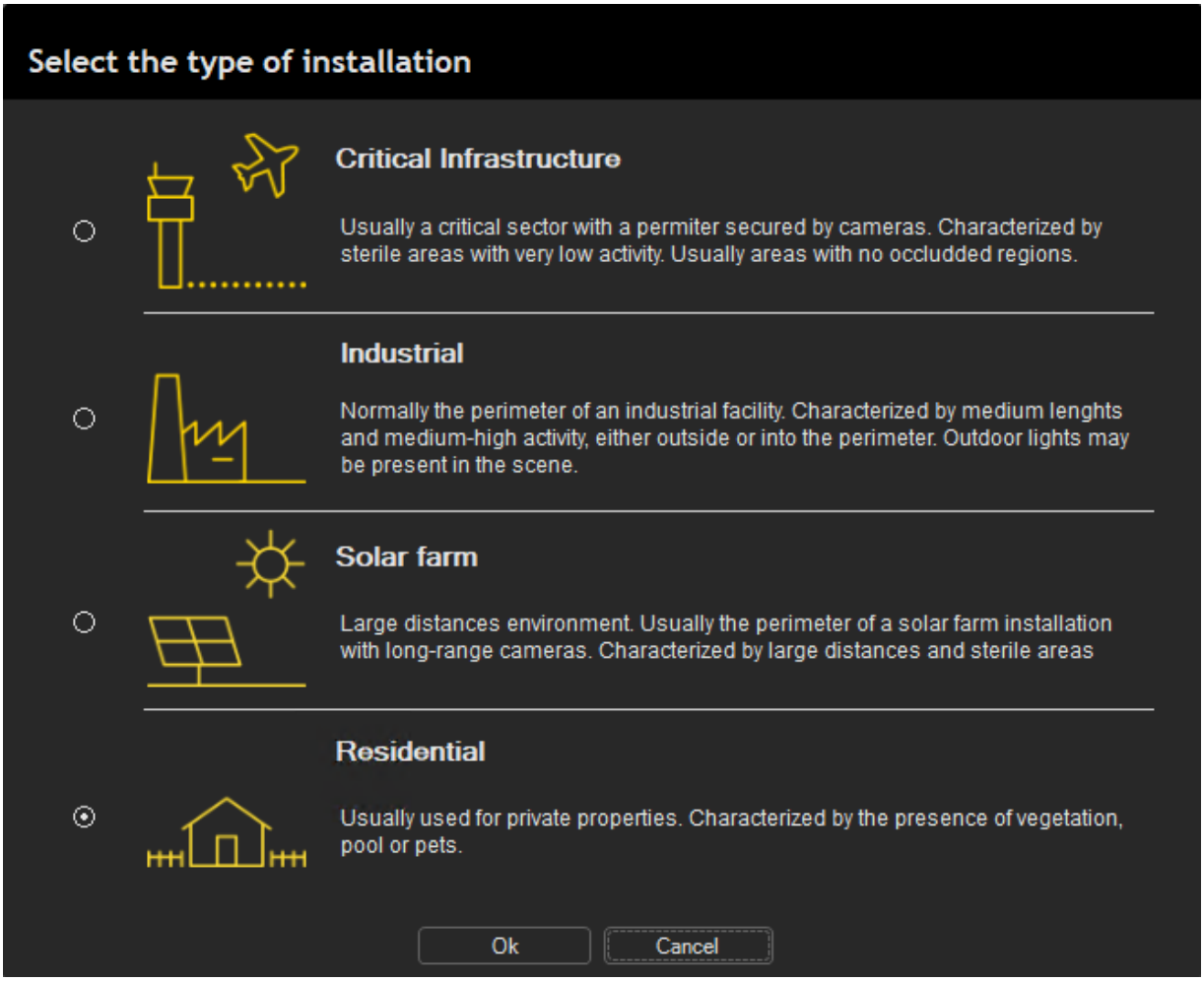
In addition to cameras, you can add other devices supported by the system (see **Device Configuration**).



Select the Type of Installation

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, click the Add button in the Cameras section.

The first time you access the camera menu, you will be asked what type of installation you want to set up: Critical Infrastructures, Industrial, Solar farm or Residential.

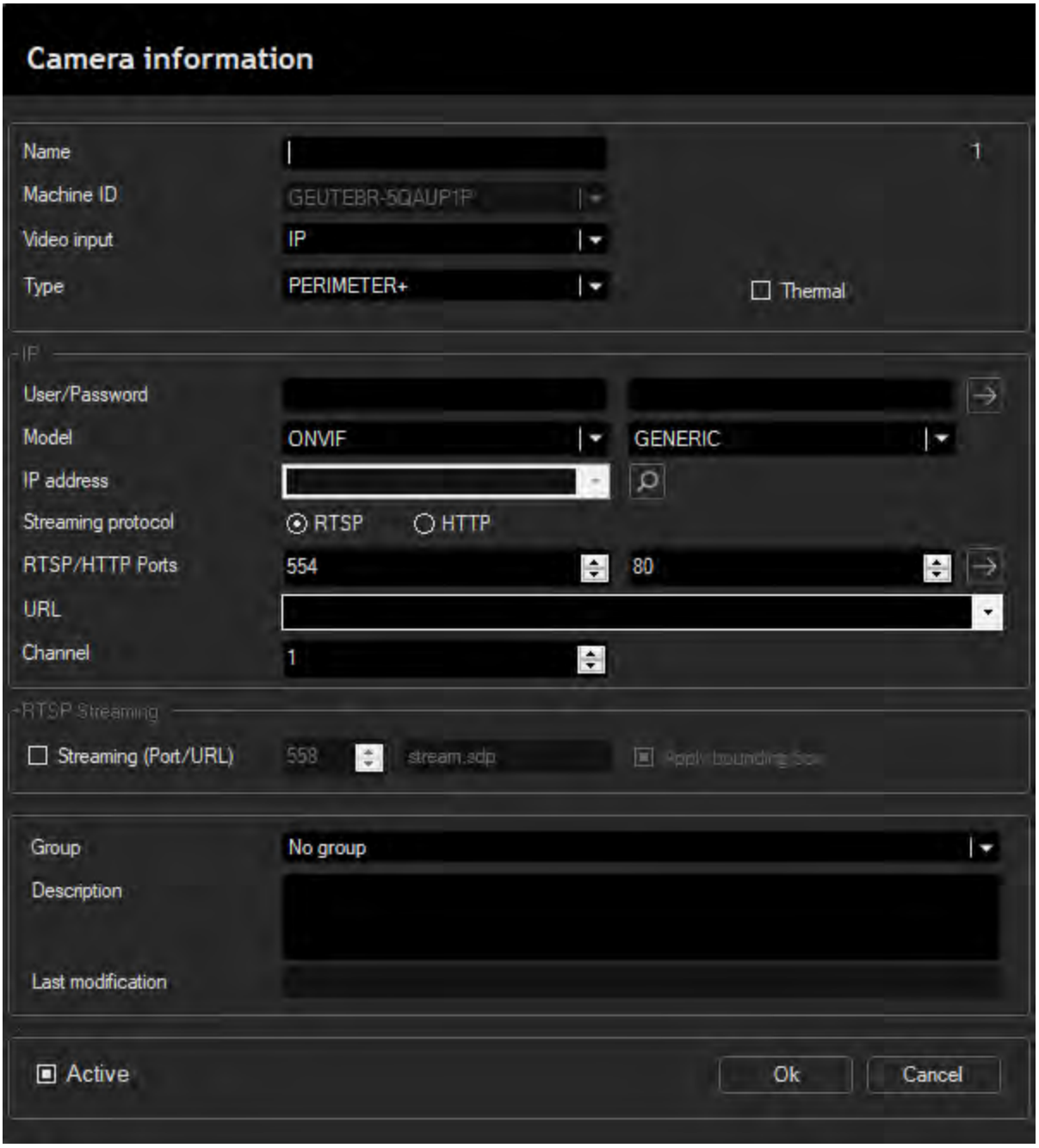


Select the type that best describes your installation to predefine the cameras according to the type of setting. This option can be changed later from the camera menu, but this should rarely be used as it is difficult to change the type of scene. When you have selected the site profile, an icon appears in the camera menu that allows you to change it if necessary.

Add a Camera

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, click the Add button in the Cameras section.

The following window appears:



General Settings

These are the general settings you need to define a camera:

Name	Description
Name	Enter the name of the camera. **IMPORTANT:** The specified camera name must be identical to the camera name in G-Core. The camera name must not contain spaces when sending alarms to G-Core using the action interface (see **Add Perimeter+ Alarms**), because Perimeter+ suppresses the spaces.
Machine ID	Select the identifier of the server that processes the camera. This drop-down menu is active in installations with more than one server.
Video input	Select the video input: **IP**: IP cameras with an IP address. **Video file**: Video file for forensic analysis.
Type	Select the camera type: • **PERIMETER+**: Standard camera with Perimeter+ technology. • **PERIMETER+ ALR**: Advanced Long Range camera with Perimeter+ technology. • **PERIMETER+ PTZ**: PTZ camera with autotracking and Perimeter+ DeepFusion technology. • **SmartPTZ**: PTZ support camera or fixed support camera. **For PERIMETER+ ALR and PERIMETER+ PTZ, you need an expanding function license.** **If you select a camera with SmartPTZ support, you cannot create video analysis rules for the camera. However, you can define presets for this camera to record a secondary video when a video analytics camera detects an event.**
Thermal	Enable this option if you connect a thermal camera. When this option is enabled, the **Advanced thermal functions** section appears, allowing you to choose between different camera manufacturers to apply specific algorithms for thermal cameras for better performance.

Name	Description
Corridor view	If the **Perimeter+ ALR** license extension is enabled, you can select the **Corridor view** mode from the different rotation options. This feature increases detection capability at long ranges and reduces the dead zone below the camera.

IP

When you select the video input **IP**, the following options are available:

Name	Description
User/Password	Enter the username and password of the IP camera. Click the ➜ button to refresh the URL list with the new user and password.
Model	Select the camera manufacturer from the drop-down list.
IP address	Enter the IP address assigned to the camera. You can find the IP address in the user manual of the camera.
Streaming protocol	You can choose between RTSP and HTTP protocol.
RTSP/HTTP Ports	These are the communication ports assigned to the camera for transferring images. The default ports are 554 (RTSP) and 80 (HTTP). Click the ➜ button to check the ports.
URL	For cameras that transmit via RTSP, the URL indicates the direction of the video stream you want to retrieve. This field is filled in automatically when you select the IP camera model. If your camera model is not in the list or you want to specify another URL, select **Generic** from the list of camera models and modify the URL field.
Channel	If you have connected camera streams from DVR/NVR, you must select the channel of the camera connected to the DVR/NVR. This option can be used to specify the channel or video stream in the URL as a setting. If the URL contains '#c' in the string, it will be replaced by the channel number.

Most IP cameras can handle multi streams. In a typical installation, the camera should have a main stream with high resolution for the DVR/NVR and a sub stream or secondary stream for video analysis.

To optimize network bandwidth and image quality, go to camera settings and edit the secondary video stream according to the recommended specifications:

- **Protocol**: H264, H265
- **Resolution**: VGA (640x480) or 4CIF (704x576)
- **Frame rate**: 15 fps
- **Bitrate**: ~768 kbps – 1024 kbps (CBR Constant)

Video File

If you are select the video input **video file**, the following options are available:

Name	Description
File	Select the video file from a folder on the hard disk of the unit.
Frames per second	Enter the number of images per second that the system processes to detect events. A minimum of six images per second is recommended for smart intelligent event and motion detection.

RTSP Streaming

Name	Description
Streaming	Enable this option to transmit images from the video analytics unit to a third-party unit using RTSP protocol.
Port	TCP port for image transmission using RTSP protocol.
URL	The URL address for image transmission using RTSP protocol.
Apply bounding box	Enable this option to apply the bounding boxes in the RTSP stream as well.

Advanced Settings

Name	Description
Group	Select the group to which the camera is assigned (see **Camera Groups**).
Description	Enter the description of the camera.
Last modification	It is not possible to enter the value in this field. The system automatically updates this field when a change is made to an existing camera configuration.
Active	Enabled or disabled the camera. It is recommended to disable cameras that are not in use.

Modify a Camera

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera and click the Modify button in the Cameras section.

To modify a camera in the system, select the camera you want to edit and click the Modify button.

The Camera information window opens, with all the information about the camera opens, where you can edit the previously entered data about the selected camera (see **Add a Camera**).

Delete a Camera

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera and click the Delete button in the Cameras section.

To delete a camera from the system, select the camera you want to delete and then click the Delete button.

IMPORTANT: When you delete a camera from the system, you delete all information about the camera, as well as all the alarms and video sequences recorded by that camera.

Device Configuration

In addition to cameras, you can add other devices supported by the system.

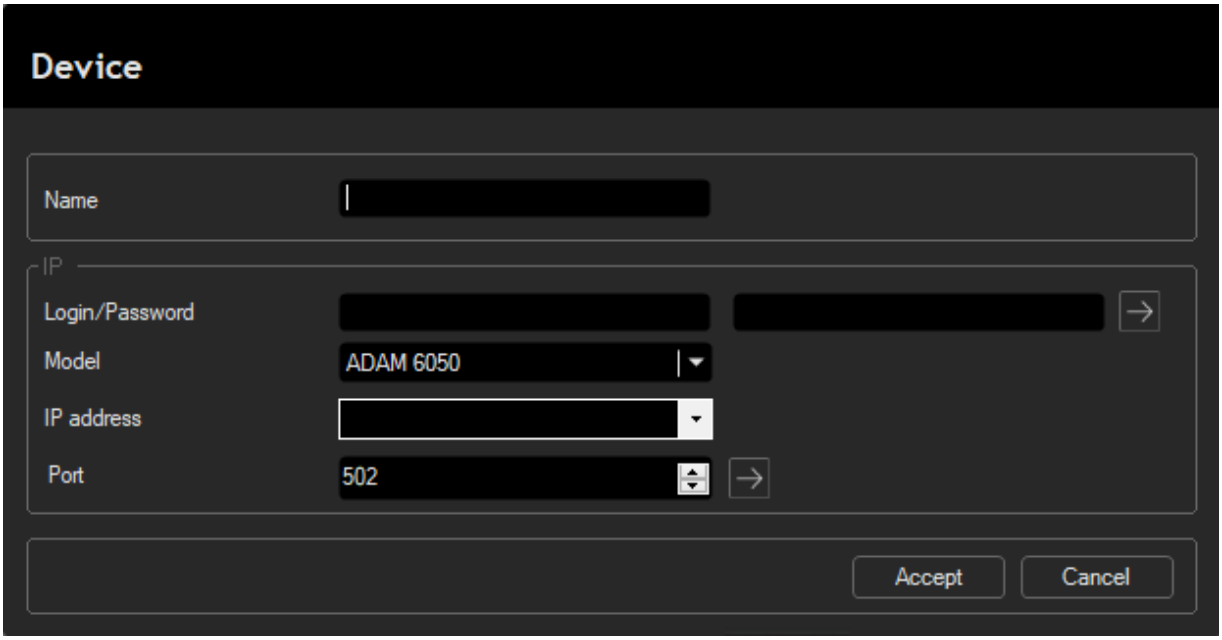
By adding devices to the system, it is possible to trigger relay outputs when an alarm is triggered (see **Trigger Relay**).

Note that the system cannot trigger the device relay outputs with camera rules until the device is defined.

Add a Device

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, click expand the Add drop down menu in the Cameras section and select Device.

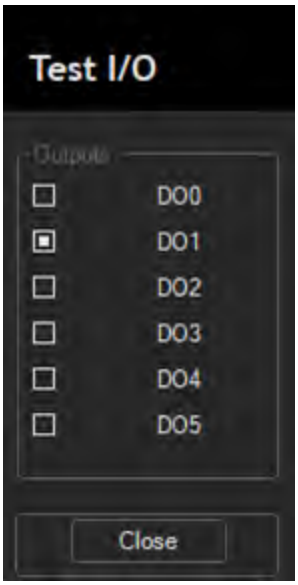
The Device dialog window looks like this:



Name	Description
Name	Enter the name of the device.
Login/Password	Enter the username and password of the device. Click the ➜ **Login test** button to check the login credentials.
Model	Select the model of the device.
IP address	Enter the IP address of the device.
Port	Enter the port of the device. Click the ➜ **IP and port test** button to check the connection.

Test a Device

To test the device, click the Test I/O button. A window appears that allows you to test the device outputs:



Camera Groups

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.

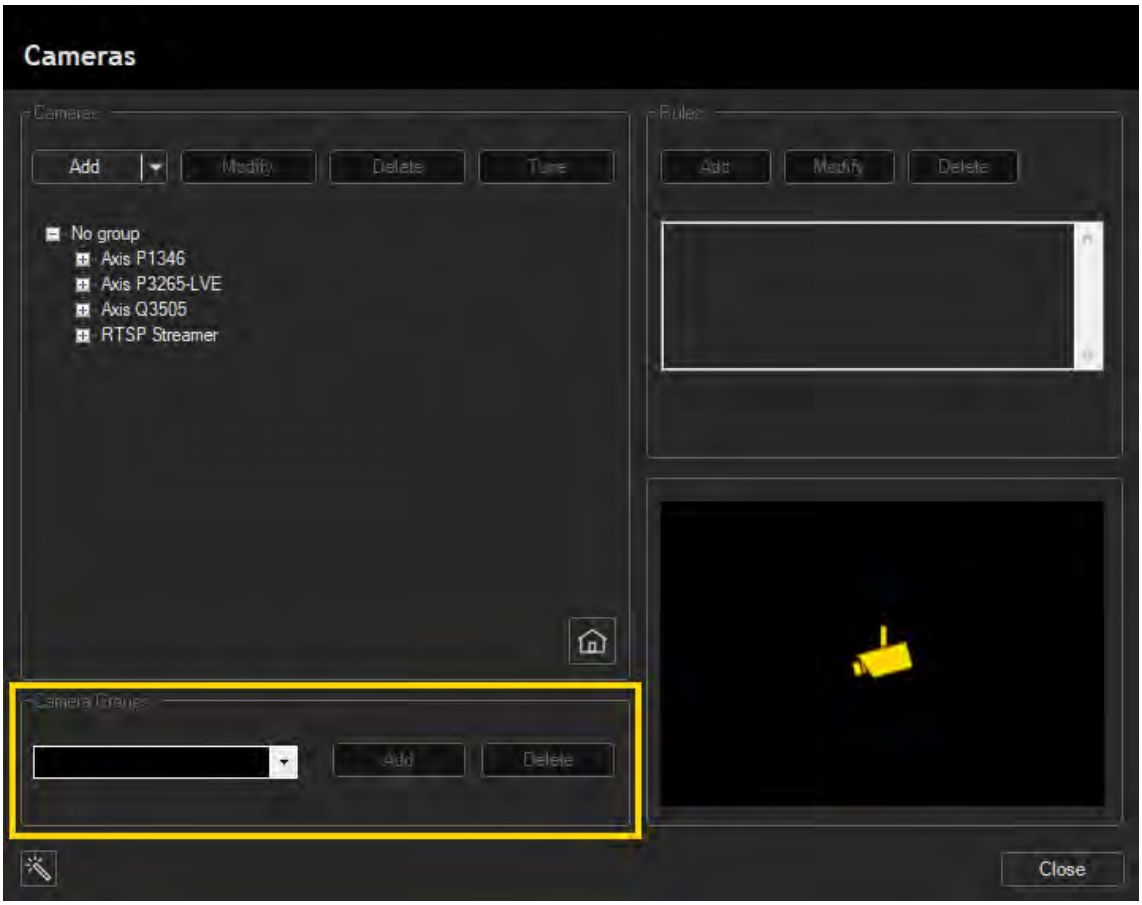
Camera groups help the user to manage cameras. For example, they can be used to group cameras by areas to monitor or floors of a building, etc.

Camera views are groups of cameras that are similar to camera groups, but are used only to group live cameras for display on the screen. Camera views do not have to be the identical to camera groups.

Create a Camera Group

Follow these steps to create a camera group:

1. Click on the Group field and enter the name of the camera group.



2. Click the **Add** button to create your camera group automatically.

When you define or modify a camera, you can add it to the existing camera groups.

Delete a Camera Group

To delete a camera group, select the name of the group from the drop-down menu and click the **Delete** button. The group will be removed automatically.

You can only delete groups that have no cameras assigned to them. To delete a group assignment, select a camera, click Modify and leave the Group section blank.

Tune

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera and click the Tune button.

Camera adjustments are essential for correct detection and to minimizing the number of false alarms.

The following types of camera adjustments are available:

- **Region of Exclusion**
- **Perspective**
- **Parameters**
- **Privacy**
- **Virtual IR**
- **Presets**
- **Zoom Calibration**

Note that any changes you make in these camera adjustments apply to the camera and therefore affect all detection rules associated with that camera.

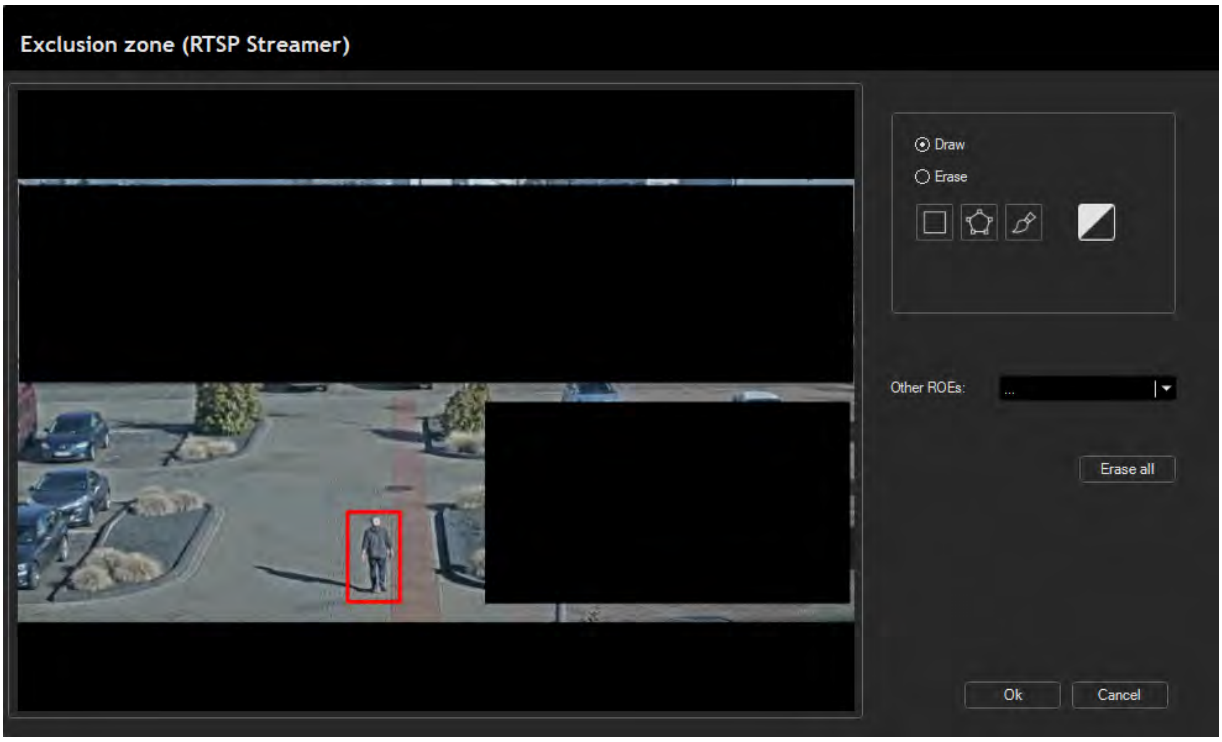
Region of Exclusion

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Tune button in the Cameras section and select Region of exclusion.

The purpose of the exclusion zone is to exclude areas that the system does not need to analyze. The marked area is excluded, which improves the performance of the unit.

For the system, the exclusion zone is a black area. Therefore, any part of an object (person or vehicle) within the exclusion zone is removed by the system and the system is unable to detect the object.

The exclusion zone allows you to ignore areas where the presence of an intruder is impossible, such as sky areas, building walls (but never as low as street level, otherwise the system would not be able to detect a person walking near the wall), roads, areas where monitoring is unnecessary, etc. When in doubt, do not create exclusion zones.



The tools for drawing the exclusion zone are the same as the tools for drawing the exclusion zone for a rule, but the two should not be confused.
While exclusion zone defined for a camera prevents the system from analyzing that area, the exclusion zone for a rule shows only the areas that trigger an alarm and those that do not. If the entire body of a person, except for the feet, is in an exclusion zone defined for a rule, the system detects the person and triggers an alarm. Conversely, if the entire body of a person except the feet is in an exclusion zone defined for a camera, the system does not detect anything.

You can use the following options to define exclusion zones:

Option	Description
Draw / Erase	This option allows you to select tools to define the exclusion zone or to delete part of the zone.
Erase all	This option allows you to delete the entire exclusion zone you have defined.
Rectangle Tool	Use this option to define an exclusion zone in rectangular form. Click and drag the mouse over the camera image and then release the mouse button.
Polygon Tool	Use this option to define an exclusion zone in polygon form. Use the mouse to create your polygon. When it's done, click the first vertex to close it.
Brush Tool	Use this option to define an exclusion zone by brushing over the camera image while holding down the left mouse button. When you have selected the brush tool, you can change the thickness of the brush used.
Black/White Button	This option allows you to set the color of your exclusion zone. It is only used to improve visibility and does not affect the function of the system.
Other REOs	This option allows you to select the ROEs set in the equipment for other cameras and rules.

Perspective

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Tune button in the Cameras section and select Perspective.

The purpose of this dialog window is to teach the system depth of the scene and to determine the size of a person at any point of the image.

There are two operating modes:

- **Automatic Mode**
- **Manual Mode**

Automatic Mode

The automatic mode appears by default when you enter the Perspective screen. When the system is in this mode, the Learn option is enabled.

In this mode, the system automatically learns the perspective of the scene.

If you want to pause the sample acquisition during the learning process, disable the Learn option. You may need to pause the sample acquisition if unwanted objects enter the scene (animals, vehicles, etc.) that could distort the learned model. To resume sample acquisition, enable the Learn option again.

If you want to delete all the acquired samples and start the process again, click the Clear all button. The system automatically exits the perspective screen, so you have to log in again to accept a new model.

Size of a Person

You need a person to walk around the entire image:

- We recommend that the person first walk around the areas closest to the camera and, once the system has detected them, they zigzag away from the camera.
- It is important that the person is framed at the most distant point for the system to detect (see **Zoom Adjustment**).
- It is important to avoid obstructions during the learning process so that the system can always see the entire body of the person.

During the learning process, the system displays the estimated perspective using boxes that indicate the size of a person in different parts of the image.

The outlines of the people are filled in as the learning bar progresses:

- An unfilled sample indicates that the number of samples at one level is insufficient.
- A half-filled sample indicates that you need to obtain more samples at that level.
- A completely filled sample indicates that you have now obtained enough samples.

Zoom Adjustment

To adjust the zoom or field of view for each camera, the system displays an outline of a person indicating the minimum size of a person in the camera zone.

Follow these steps to adjust the zoom or field of view of your camera:

1. Disable the **Learn** option.
2. Position the person in the most distant part of the image where you want to detect intruders.
3. Use the mouse to bring the outline of the person close to the real person.
4. If the real person is the same size or larger than the outline at this point, the zoom is correct.
5. If the real person is smaller than the drawing of a person, increase the camera zoom and try again.

   If you cannot increase the camera zoom, you can increase the sensitivity settings of the system (see **Parameters**) to enable the system to detect objects smaller than the outline of a person.

   Increasing the sensitivity also increases the number of false alarms.

Detection Limit

The model also displays two horizon lines.

- The red line represents the theoretical detection limit of the equipment. It is important that this line is above the area you want to monitor. Beyond this line, the system will not detect anything.
- The yellow line represents the optimal detection limit of the equipment. If these horizons are too low, you need to take more samples above these lines, and if the situation persists, you need to increase the camera zoom.

Manual Mode

The system may not be able to learn an appropriate perspective model. In this case, you can use manual mode.

1. To activate the manual mode, disable the **Learn** option and enable the **Manual** option.
2. Then select the **Far person** option and draw a rectangle around a person you want to detect at the furthest point.

3. Repeat the procedure by selecting the **Near person** option and draw the rectangle at the nearest possible position.
4. Draw the rectangle so that the top touches the head of the person and their feet touch the bottom. Do the same with the sides of the rectangle.
5. When you have drawn both rectangles, click the model that fits the size of the image of the person in all parts of the image.

If you want to pause the manual learning process, click the **Pause** button. To display the moving image, click the **Play** button.

If you want to delete all the samples you have drawn and start the process again, click the **Clear all** button. The system automatically exits the perspective screen, so you have to log in again to accept a new model.

Parameters

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Tune button in the Cameras section and select Parameters.

When you have created the camera, set the perspective and defined the rules, the unit is ready to detect intruders in the specified area. However, various factors can cause the system to generate false alarms.

The sliders in this dialog window are generally used to improve detection reliability and avoid false alarms caused by animals, trees, wind, camera movement, etc.

However, they can affect the detection performance of the system. In general, the system becomes more sensitive when the sliders are in low positions, but false alarms are more likely to occur. On the other hand, if the sliders are in a high position, the system will be able to filter out more false alarms, but will be slower at detecting an intruder.

> ⚠ **IMPORTANT:** The procedure for adjusting the settings is critical for proper configuration. Incorrect settings can affect the proper functioning of the system (see **Adjustment Procedure**).

If you change these settings, check that the system still detects intruders.

Predefined Setups

The system provides the option to choose between three predefined configurations:

Setup	Description
Standard	The standard configuration, which is used by default, has been val-

Setup	Description
	idated under adverse weather conditions in a variety of different scenarios and should cover your needs without any further adjustments.
Extra sensitive	This configuration is intended for close-range cameras focused on the street. • Since this is a close-range camera where vehicles spend little time in the scene, the object tracking tolerance is increased. • Since there is no need to differentiate between people and vehicles, fast detection is enabled for the intruder rule. • In addition, it is assumed that there is no excessive vegetation or that it is nullified by an exclusion zone. Therefore, fast intruder detection is enabled and the random motion filter is disabled.
Highly filtered	This predefined configuration is best suited for low activity environments with good camera contrast. It is best suited for open scenes with little activity that enable a longer detection time.

However, in some scenarios with specific characteristics, the number of false alarms generated by the system with the default settings may not meet your requirements. In this case, you can reduce the number of false alarms by adjusting some of the parameters.

Perimeter+

Parameter	Description
Appearance	This slider controls the extent to which the system relies on the appearance of objects to trigger an alarm. The further to the right, the more evidence that the observed object is a vehicle or a person the system needs to trigger an alarm. If the system is generating unwanted false alarms, under good standard conditions (full view of the object, open, well-lit scene with enough time to observe the object), increasing this slider reduces the number of false alarms without compromising detections. ⚠ **IMPORTANT:** Above position 7, if the system is processing a low resolution stream, it may miss

Parameter	Description
	⚠ small objects in day/night channels. In the lowest position, only very rough information about the appearance is used to take a decision. To detect an object moving coherently for a time without considering its appearance, set this filter to the lowest position.
Boost Detections	This slider controls whether the minimum time or minimum distance criterion can trigger an alarm if it looks like a person or a vehicle. Enabling this slider improves detection in difficult conditions. In contrast, if the system consistently detects objects as people when they are not, you can try disabling this option, as the system may confuse the object with a person or a vehicle. **ⓘ After disabling this option, you should check that the system is continues to detect intruders under all conditions.**
Animals	This slider control filters out objects that look like animals. The further you move the slider to the right, the more accurate the system. **ⓘ It is important to distinguish the Perimeter+ animal filter from the Advanced Parameters animal filter. While the former is based on appearance, the latter uses size criteria that depend on perspective.**

Advanced Parameters

Parameter	Description
Intruders detection	This slider controls the detection reliability. When the slider is increased, the system has more time to decide whether the analyzed object is a person, vehicle or a false alarm. Increasing this slider directly reduces the number of false alarms. Thus, it is a powerful tool to reduce false alarms, and in combination with the distance filter, it is the primary measure to solve a false alarm problem. In these cases, it is advis-

Parameter	Description
	able to set the filter between positions 15 and 18. If the false alarms persist in this position and it looks like more time can be allowed for the system make a to decision, the slider can be set to position 19 or 20, but only in exceptional cases. Conversely, if you want faster detection from the system, you can set the slider control to position 13 or 14. For critical infrastructures, thermal imaging camera installations and other high-security sites with difficult intrusions (e.g. body dragging, log rolling, etc.), it is recommended to set the slider control to position 5, and only in exceptional cases to values around 2.
Minimum size	This slider is specially designed to eliminate false alarms caused by small animals (cats, dogs, etc.) and other small objects moving on the ground (plastic bags, papers, etc.). The higher the position of the slider, the larger objects in relation to the size of a person the system can filter out. If the false alarms are caused by cats or dogs, the slider should be set to position 3 or 4.
Maximum size	With this filter it is possible to filter objects by size. The higher the position of the slider, the smaller the objects the system can detect. If the false alarms are triggered by large objects such as airplanes or trucks, it is recommended to set the slider to a higher position. **This filter is only available for thermal cameras.**
Distance	This slider controls the minimum distance an object must move before the system detects an intrusion. If the distance filter is increased, an object has to move further before the system detects an intrusion. When calculating the scene, the system considers the perspective of the scene. This filter is useful for filtering out false alarms caused by trees, wind, slight camera movement, shadows, etc. For false alarms of this type, it is recommended to set this filter to position 9 or 10. In these positions, the object needs to move at least two meters before it is detected. For scenes with many obstructions or low light or contrast, it

Parameter	Description
	is recommended to set the slider to a value 4 between 7. If you have problems with false alarms and the area to be monitored is clear, you can set the slider to position 11 or 12.
Time	This slider indirectly controls the time the system needs to detect an intrusion. When the time filter is increased, the system takes longer to detect an intrusion. This slider can be useful for filtering out false alarms of short duration (1 or 2 seconds), such as false alarms caused by light changes, streetlights turning on and off, or car headlights. You should only change this setting in open scenes where the system has enough time to detect the intrusion. For very close cameras or cameras where objects are only in the scene for a very short time, it is not advisable to increase this setting, and in very extreme cases where you want to detect objects that are only visible for a very short time, it is recommended to set this filter to position 3 or 4. If you set the slider to position 10, the object must have been visible in the scene for at least two seconds. If you have problems with false alarms, you can set this slider to position 12 or 13.
Oscillatory movement	This filter is enabled in the configuration by default and is specially designed to filter small oscillatory movements, such as that of a tree branch swaying in the wind. This filter should only be disabled in exceptional cases when you want the system to detect any object that enters the scene very quickly, such as very close cameras with people or vehicles moving very fast and visible for a short time. **If this filter is disabled, the number of false alarms in the system increases.**
Fast objects	This slider should not be changed in the most typical video surveillance scenes. It should only be decreased slightly in scenes where objects are moving very quickly, or in scenes where objects are very close to the camera and their size occupies a significant portion of the image (for example, when a car occupies more than half of the image). In these cases, you should set the slider to position 1 or 2.

Parameter	Description
	This control is not intended to control the number of false alarms in the system. However, if you decrease it for no reason, this can lead to an increase in false alarms.
Intensity	This slider affects the ability of the system to filter intensity changes and affects color and black-and-white cameras. This filter should be increased if the system detects false alarms in scenes where no objects appear to be in motion and no color distortion is detected, or if it is determined that the camera is very noisy (e.g., at night). In this case, the filter can be increased to position 9. If the intensity filter is increased in dark areas, it is possible that people or vehicles will not be fully detected. In this case, decrease the filter level slightly until you find the optimal point where objects are completely detected but no false alarms are triggered. In the case of very dark cameras, it is also possible that the system does not completely detect the person or vehicle with the default configuration. In this case, reduce the filter to position 5 or 4. Only in extreme cases where maximum sensitivity is needed should the filter be set to position 2 or 3.
Tampering	This filter controls the detection sensitivity of the tamper rule. A tamper is any significant change in the image that persists for a specified time. A tamper alarm can be triggered either by an object covering the camera lens or by a significant movement of the lens. In the case that the tamper rule generates false alarms (e.g. due to light changes), the tamper filter should be moved to the right.
Camera stabilizer	This slider allows you to enable or disable image stabilization. The improved image stabilization increases the detection capability at long range and reduces false alarms caused by camera vibrations. **This slider is only available for systems with Perimeter+ ALR option.**

Adjustment Procedure

The technician should visit the premises of the client at least twice to adjust the cameras.

On the first visit, you need to:

1. Create the cameras.
2. Define new rules or modify existing rules to meet the requirements of the client.
3. Configure the perspective and areas of interest for each camera.

> **During the first visit, the camera settings do not be modified unless necessary to ensure detection under difficult conditions.**

On second visit, at least 24 hours after the first, you need to:

1. Analyze any false alarms that each camera has generated since the last visit:

   Open the Alarm viewer and review the alarms generated by the system from each camera since the last visit. It is important to analyze the different causes of the false alarms, group them and log the number of false alarms by type. The starting point should be the type of false alarm that triggered the most false alarms.

2. Adjust the rules configuration to reduce the impact of false alarms:

   The first strategy to reduce the number of false alarms is to increase the exclusion zone.

   - If false alarms are generated in an area that does not need to be monitored, this area should be eliminated from the exclusion zone using the rule configuration menu.
   - If the false alarms originate from a wall, they can probably be eliminated with the exclusion zone.

     > **Note that the exclusion zone only considers the position of the feet of a person or the bottom of a vehicle, so if the feet of the person are not within the exclusion zone, the system will still detect the intrusion. In the specific case of a wall, it is recommended to extend the exclusion zone to knee height.**

- It is also possible that the false alarm originates somewhere that you want to monitor, but that in order to reach this place you have to pass through an area that is monitored by the system. In this case, the area causing the false alarms can be eliminated because the system will detect intruders before they can get there.
- If the system continues to trigger false alarms and you cannot stop them with this strategy, try adjusting the camera settings.

3. Adjust the camera settings, if necessary:

   See **Parameters**.

Troubleshooting Guide

The following table is intended to support you in troubleshooting false alarms or adjusting the detection speed. It contains an overview of the most common problems and recommendations on how to solve them.

Problem	Solution
The system generates false alarms **in places where nothing is moving**. Small **color distortions** are observed.	Increase the color filter to level 6 or 7. If the false alarms persist, increase it to level 8 or 9.
With a color camera, the system generates false alarms caused by the **outlines of objects in places where nothing is moving**. For example, a tree trunk, street light, or traffic light post.	Increase the color filter to level 6 or 7. If the false alarms persist, increase it to level 8 or 9.
With a black-and-white camera, false alarms are generated **in places where nothing is moving**. The **Noise** is visible when you look closely at the image.	Increase the intensity filter to level 8. If the false alarms persist, increase it to level 9 or 10.
After increasing the color and intensity filter, the system does **not frame objects correctly or has difficulty detecting certain areas** of the image.	Reduce the changed filter. Find the optimal point between detection quality and false alarms.

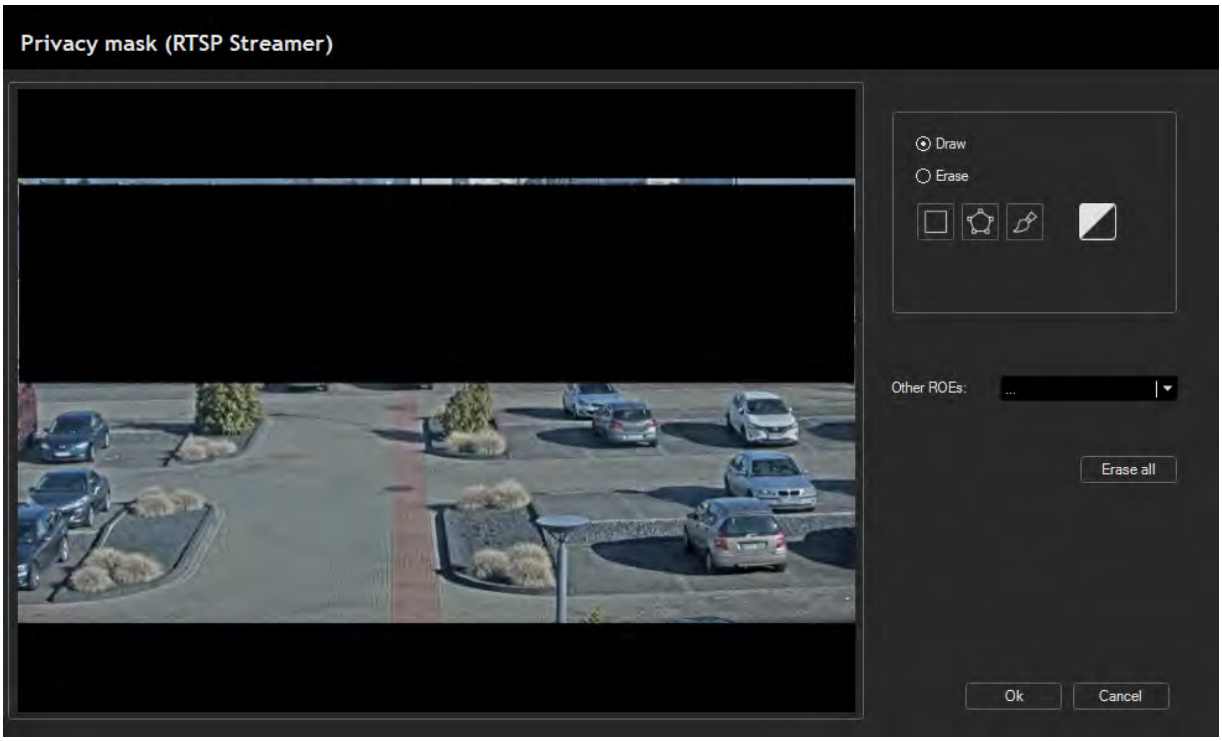
Problem	Solution
The system does not correctly frame people **in very dark or low-contrast areas**.	Reduce the intensity filter to level 4 or 5.
The system detects false alarms caused by **trees swaying** in the wind.	Increase the intruder detection to level 16 or 17. Also increase the distance filter to level 4 or 5. Make sure that the oscillatory movement filter is enabled.
The system detects false alarms caused by **headlights of vehicles** that are not in the scene.	Increase the time filter to level 8 or 9 or use the "Person" rule only.
The system detects **insects** that are in front of the camera.	Increase the intruder detection to level 16 or 17. If possible, use the "Person" rule only.
The system **detects objects too late** when they are about to leave the image.	Reduce the intruder detection to level 12 or 13. If this is not sufficient, reduce the intruder detection further to level 4 or 5. Also increase the object filter to level 4 or 5. If the problem persists, set the time filter to level 2 and the oscillatory movement filter to level 0.
The system detects false alarms caused by **tree shadows** projected on the ground.	Increase the distance filter to level 9 or 10. Increase the intruder detection to level 16 or 17 and increase the animal filter to level 4.
The image moves or is **distorted**. There is interference or synchronization problems.	Secure the camera firmly, fix the signal problems. If this is not possible, increase the intruder detection to the maximum level allowed for the scene.
The system detects cats, dogs or other **animals**.	Increase the animal filter to level 3 or 4.
The system detects false alarms when the light conditions change due to **clouds**.	Increase the intensity filter to level 8 or 9.

Problem	Solution
The system detects false alarms in a **swimming pool**.	If possible, exclude the swimming pool from the detection area. Increase the distance filter to level 7, 8 or 9 and increase the intruder detection to level 16 or 17.
The system detects false alarms caused by **sprinklers**.	If possible, use virtual barriers for people only or vehicles only. Increase the intruder detection to level 16, 17 or 18.
The system detects false alarms when a **streetlight** is turned on or off.	Try to exclude the streetlight by using an exclusion zone or a virtual barrier. If this is not possible, increase the time filter to level 6, 8 or even 10. If possible, increase the intensity filter to level 8 or 9.
The system does not detect **in seemingly simple areas**.	Check the camera exclusion zones and the rules.
The system does not detect the **enter / exit rule**.	Ensure that the object is visible before and after crossing the perimeter. Check that the direction of movement is configured correctly.
The system detects **raindrops** on the camera.	If possible, restrict the detection zones and avoid using the intruder rule.
The system does not detect **in very distant areas**.	Check if the perspective settings are correct. If the undetected area is above the perspective line, increase the camera zoom.
The system detects **vehicles as people** or **people as vehicles**.	Check that the perspective settings are correct. Ensure that the size of the images is suitable for people in all parts of the image. If the perspective is configured correctly, increase the intruder detection to position 17, 18 or 19 and make sure that the fast detection for the intruder rule is not enabled.
Light changes cause false tamper alarms.	Slide the tampering filter one or two levels to the right.
Trucks passing in front of the camera generate false tamper alarms.	In the **Detection Type** dialog window, increase the tamper detection time.

Privacy

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Tune button in the Cameras section and select Privacy.

The purpose of the privacy mask is to exclude areas that the operator is not allowed to see for privacy reasons. These areas are analyzed by the video analysis system, but the images displayed to the operator locally or remotely are colored black in these image areas.



Virtual IR

Subject to license

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, click the Tune button in the Cameras section and select Virtual IR.

This feature is available for thermal cameras and only with the Perimeter+ ALR license.

The main purpose is to enhance the image contrast in a specific region of the image. This region is ellipsoidal and is known as the spotlight.

VirtualIR Activation

Option	Description
Auto	Virtual IR is enabled by default. The result of this mode depends on the underlying thermal intensity in the spotlight. Therefore, there is a possibility that you will sometimes not notice any enhancement of the image contrast even when with a defined spotlight. When the thermal conditions are more favorable, Virtual IR is automatically enabled and the results are clearer.
Always	Select this option to force Virtual IR to be permanently active regardless of thermal conditions.

Option	Description
Never	Select this option if you do not want to use Virtual IR.
Activation Sensivity	If you select **Auto**, you can set the sensitivity level at which the spotlight is activated using the **Activation Sensitivity** progress bar, which ranges from less sensitive (far left) to more sensitive (far right).

Spotlight Position

There are two available options:

Option	Description
Manual	You can draw the elliptical spotlight freely.
Auto	The Spotlight is automatically defined by the system according to the perspective of the scene, the ROE of the camera and the ROE of the intruder rule. You must define the perspective before using the auto mode.

Presets

Subject to license

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a PTZ camera, click the Tune button in the Cameras section and select Presets.

This feature is only available for PTZ cameras and with the Perimeter+ ALR license.

This dialog window allows you to define several presets for a SmartPTZ or a Perimeter+ PTZ camera. These presets are used to move and zoom the PTZ camera when a fixed camera with analytics detects an event. This event has two associated videos: one from the main fixed camera and one from the additional PTZ camera.

To streamline the configuration process, as long as the Presets dialog window is open, the system ignores preset positioning or auto-tracking requests that are triggered in response to a rule.


Presets
PRESETS
...
New
Overwrite
Clear
ZOOM
SPEED
Auto tracking
Delay to start tracking (seconds):
1
Create preset ROE
Maximum tracking time (seconds):
120
Save
Stop tracking if dome stays still over (seconds):
60
Pan-tilt speed:
0
100

Set a Preset

1. You can set the camera position using the following controls:

Control	Description
Zoom	Set the zoom level of the camera view.
Move	Set the camera position using the arrows.
Speed	Set the speed for moving the camera position.

2. When you have set the correct position for your event and the camera supports it, click the **New** button, enter a name for this preset and click the **Save** button to create the preset.
3. To change an existing preset, select it from the drop-down list, set the new position and click the **Overwrite** button to save the new position.
4. To delete an existing preset, select it from the drop-down list and click the **Clear** button.

The system displays both the presets created by the user with the software (prefix "DAV") and the presets created internally in the camera (prefix "CAM"). The list is sorted alphabetically, with the presets created with the software displayed first.

Auto Tracking

This feature is only available with the Perimeter+ PTZ license.

To enable Autotracking, enable the Enable Autotracking option in the rule dialog window Response.

In this section the following settings are available:

Name	Description
Delay to start tracking	Wait time (in seconds) before the start of auto tracking. The time starts counting when the PTZ camera starts moving to the specified preset position. This delay is intended to give the PTZ camera time to reach the final preset position before auto tracking is started.
Maximum tracking	Auto Tracking is canceled when the maximum tracking time is reached.

Name	Description
time	
Stop tracking if dome stays still over	Auto Tracking is stopped when the PTZ camera has remained still for this specified period of time.
Pan-tilt speed	Controls the minimum and maximum pan-tilt speed of the camera. The PTZ camera moves at minimum speed when the intruder is near the center of the image, speeds up as it moves away, and reaches the maximum speed when the intruder is at the edge of the image. If the system tends to lose track of fast-moving objects, you should increase the minimum and maximum speeds. On the other hand, if the movements of the camera are too abrupt, reduce these speeds.

You can also configure a region of interest for each preset by clicking the **Create preset ROE** button.

This area is used to define the search area of the objects to be followed before tracking starts and after the camera has already been positioned in the specified preset. Once the PTZ camera moves and starts following the intruder, this area is no longer used. The region of interest can be used, for example, to exclude areas outside the perimeter where there are moving objects that could interfere with tracking an intruder inside the perimeter.

The region of interest is defined using the same method as the other areas, with the excluded areas marked in color.

Zoom Calibration

Subject to license

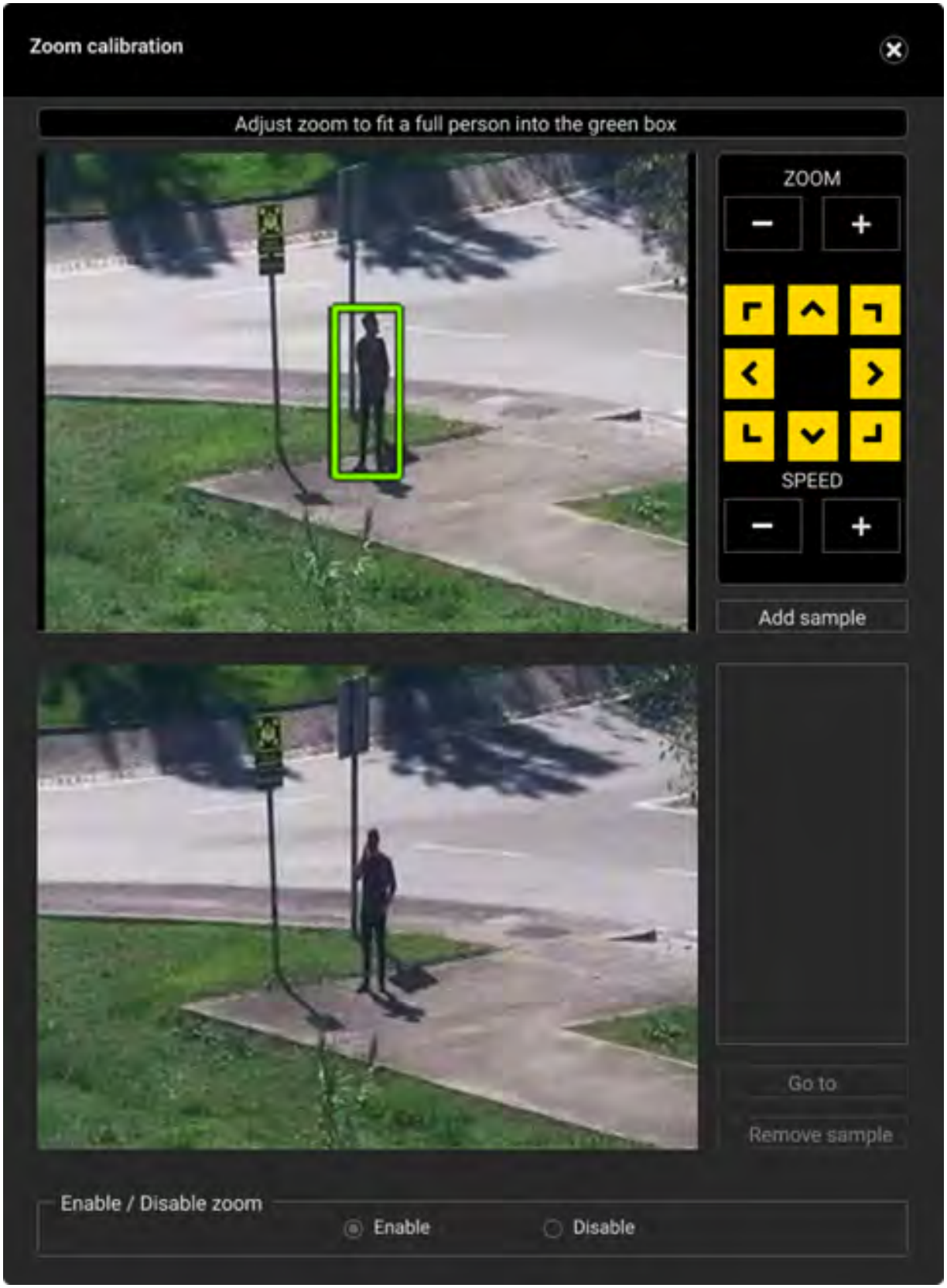
How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a PTZ camera, click the Tune button in the Cameras section and select Zoom calibration.

This feature is only available for PTZ cameras and with the Perimeter+ ALR license.

This dialog window allows you to manually define a zoom level for a representative set of pan/ tilt positions that cover the area of interest. When the PTZ camera starts following a target, it automatically adjusts the zoom level according to this calibration.

Note that this calibration step is optional. If you do not calibrate zoom or select the Disable option in the Enable / Disable zoom section, the PTZ camera will only apply pan and tilt while following a target, but not Zoom.

To streamline the configuration process, as long as the Zoom calibration dialog window is open, the system ignores preset positioning or autotracking requests that are triggered in response to a rule.


Zoom calibration
Adjust zoom to fit a full person into the green box
ZOOM
SPEED
Add sample
Go to
Remove sample
Enable / Disable zoom
Enable
Disable

To capture a zoom sample, move the PTZ controls to fit (approximately) a whole person into the green square.

1. You can move the camera position using the following controls:

Control	Description
Zoom	Set the zoom level of the camera view.
Move	Set the camera position using the arrows.
Speed	Set the speed for moving the camera position.

2. When you have set the correct position and zoom, click the Add sample button to create a sample. The sample will be added to the sample list and a screenshot will be saved for further information. Repeat this process as many times as necessary.

   To properly calibrate the zoom for a specific scene, capture the samples so that they cover approximately the entire area where the targets can pass.

3. When you select a sample from the sample list, the corresponding screenshot is displayed in the lower window.
4. Click the Go to button to move the PTZ camera to the position where the sample was captured.
5. Click the Remove sample button to delete the sample.

Rule Configuration

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. Select a camera.

A rule is a situation that triggers an alarm in the system when it occurs. Rules are always associated with a response from the system.

> Example
>
> The following is an example of a rule with associated alarm:
>
> - Rule: In case of detecting: <movement> in camera <1>
>
> - Alarm: Trigger the following response: alarm <sound> and <maximize camera>

How to add a rule:

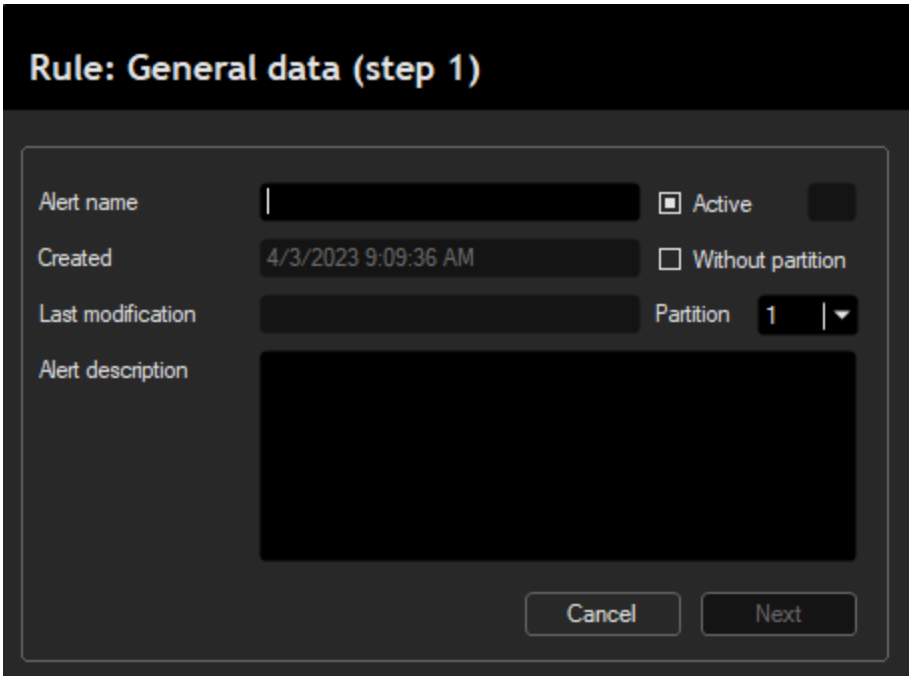
1. Select a camera.
2. Click the Add button in Rules section.
3. Follow the rule configuration steps:
    - Step 1: **General Data**
    - Step 2: **Detection Type**
        - Step 3: **Configuration (Motion Detection Type)** (only available if you select the motion detection type)
    - Step 3: **Response**
4. Once you have selected your options, click Finish and the rule is defined in the system.

When you leave the camera definition screen, you return to the system overview. After a few seconds, the system starts detecting according to the program rules, triggering the corresponding alarms.

General Data

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera and click the Add button in the Rules section.

The General data dialog window looks like this:



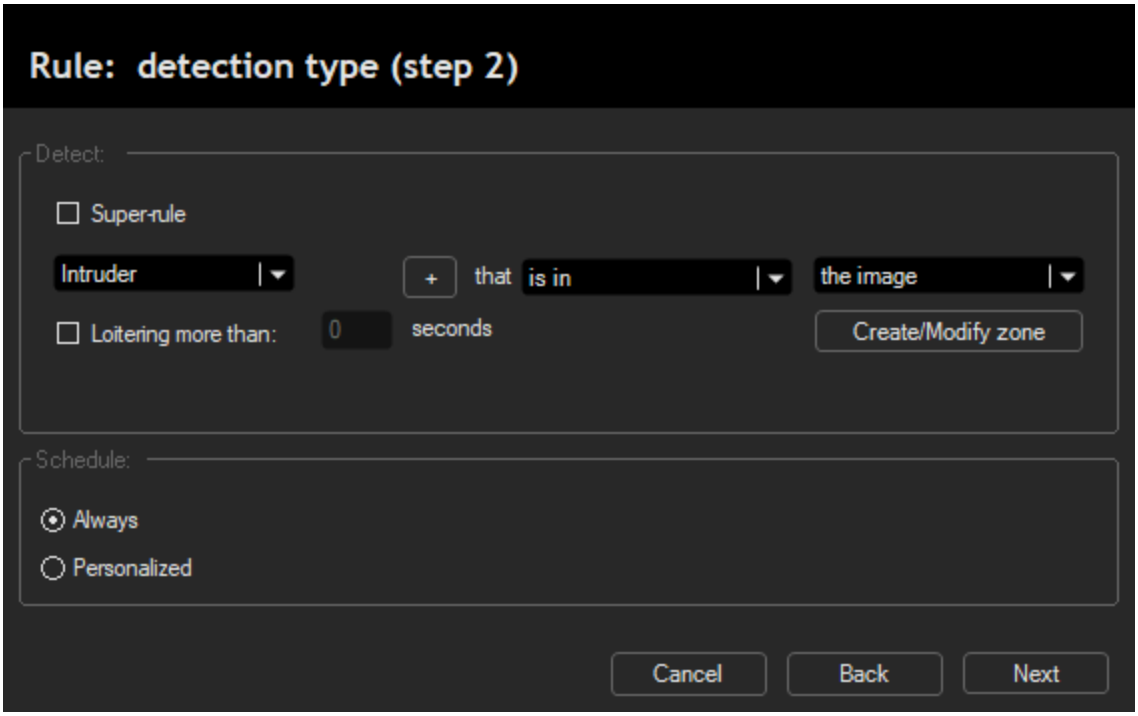
The following settings are available:

Name	Description
Alert name	Name of the rule. **It is recommend to give the rules meaningful names to avoid confusion with other systems.**
Created	This is automatically filled in with the data on the basis of which the rule was created.
Last modification	This is automatically filled with the date when the rule was last modified.
Alert description	Enter a description of the rule so that you can identify it later.
Active	Use this option to enable or disable the rule. Inactive rules are grayed out in the rules list.
Without partition	Enable this option to enable the rule without external input.
Partition	Select the partition to relate the rule to this input.

Detection Type

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next.

In this dialog window you can configure the detection type.



Create a Rule

To create a rule, you must define the type of detection, the motion pattern and the detection area.

1. Select the required type of detection. The following options are available:

Name	Description
Motion	Any pixel movement in the video image generates an event. If you have selected this detection type, the **Configuration** dialog window appears in the next step, where you can configure the motion detection (see **Configuration (Motion Detection Type)**).
Person	An event is only triggered when a person is detected (e.g. vehicles are ignored).
Vehicle	An event is only triggered when a vehicle is detected (persons are ignored).
All	Detection of any movement with relevance, e.g. people, vehicles, animals or other objects.
Intruder	Intruders or vehicles entering zones trigger actions.
External inputs	Detection of the activation of inputs from an external camera device. **Only available if a device is added.**

2. Assign a motion pattern to the selected detection type. The following options are available:

Name	Description
Is in	An object is in the image or the defined detection area.
Enters in	An object enters the detection area.
Exits from	An object exits the detection area.
Enters/Exits	An object enters or exits the detection area.
Disappears from	An object disappears from the image or the detection area (e.g. through a door in the image).

3. Select the detection area for applying the rule. The following options are available:

Name	Description
The image	The entire video image is used to detect objects.
Region of interest	The region of interest is used to detect objects. It can be narrowed by defining exclusion zones. Click the **Create/Modify Zone** button to create or modify the exclusion zones.
Zone	The zone is used to detect whether objects enter or exit the detection area. The detection area can be narrowed by defining zones. Object movements in the zone itself are not detected. Click the **Create/Modify Zone** button to create or modify the exclusion zones.

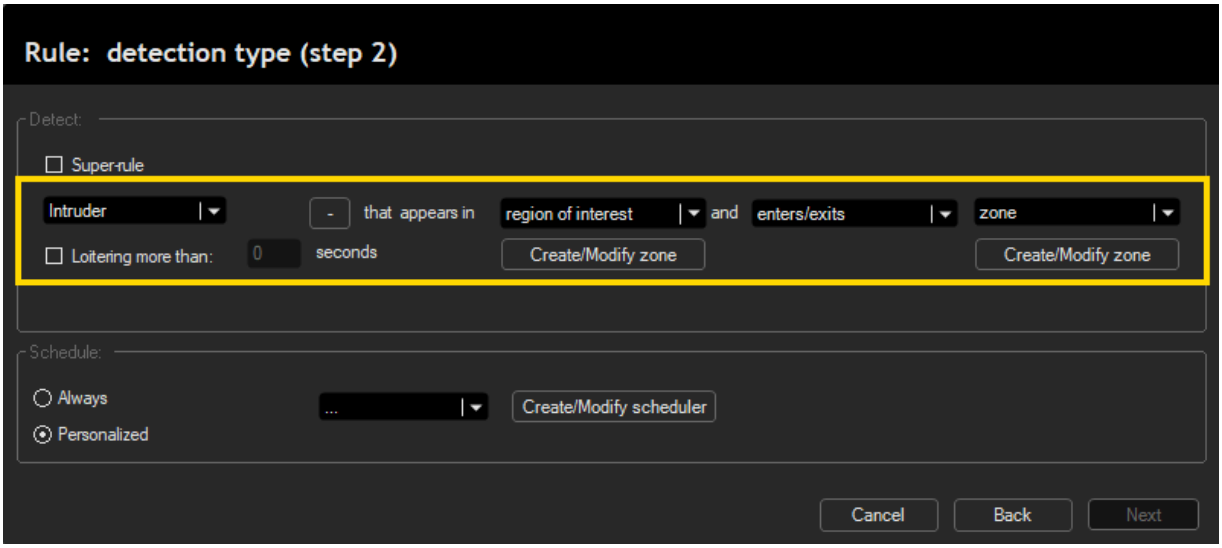
4. To detect "loitering" of people, enable the **Loitering more than** option and enter the maximum number of seconds that moving objects are allowed to stay in an area. If moving objects stay in the area longer than the defined period of time, an event is generated.

Combine Rules

Combining rules allows two types of procedures.

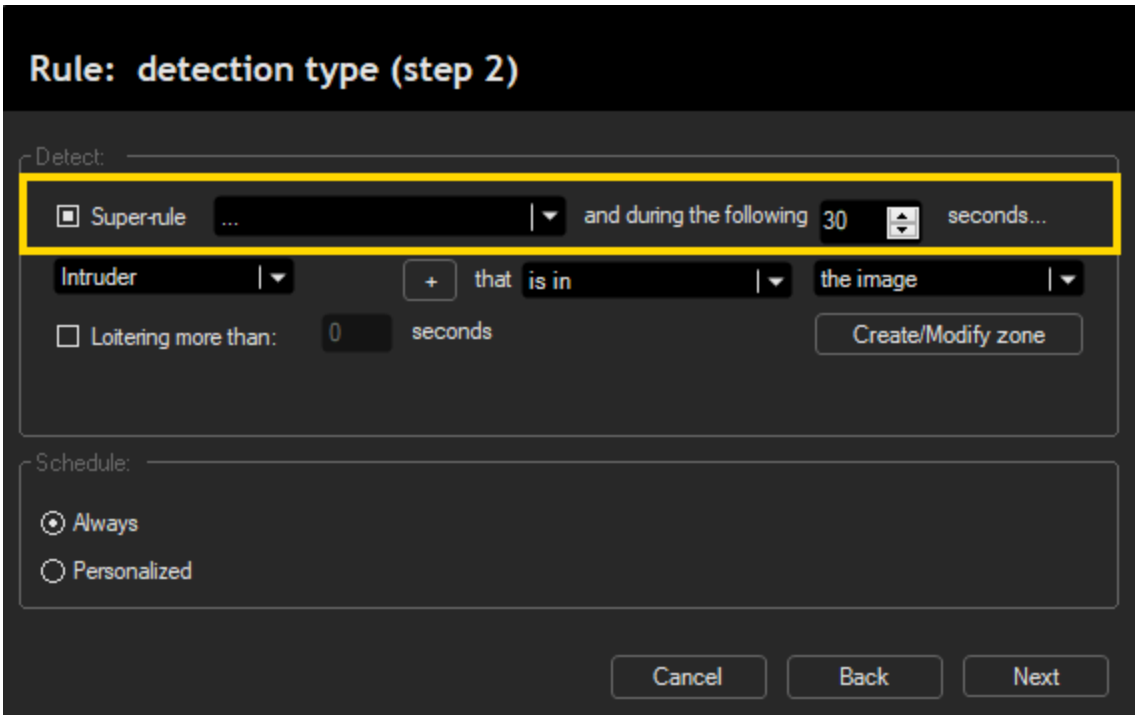
Appears in

Refers to an intruder who is seen for the first time in a specific part of the image. This is a prerequisite that can be combined with all the rules described above. The most significant aspect of this combination is that the subject detected in the above case must be the same that triggers any of the other subsequent combinations.



Super-rule

With a super-rule you can define a sequence of two different detection rules. Thereby a previously created rule activates another rule for an adjustable duration.



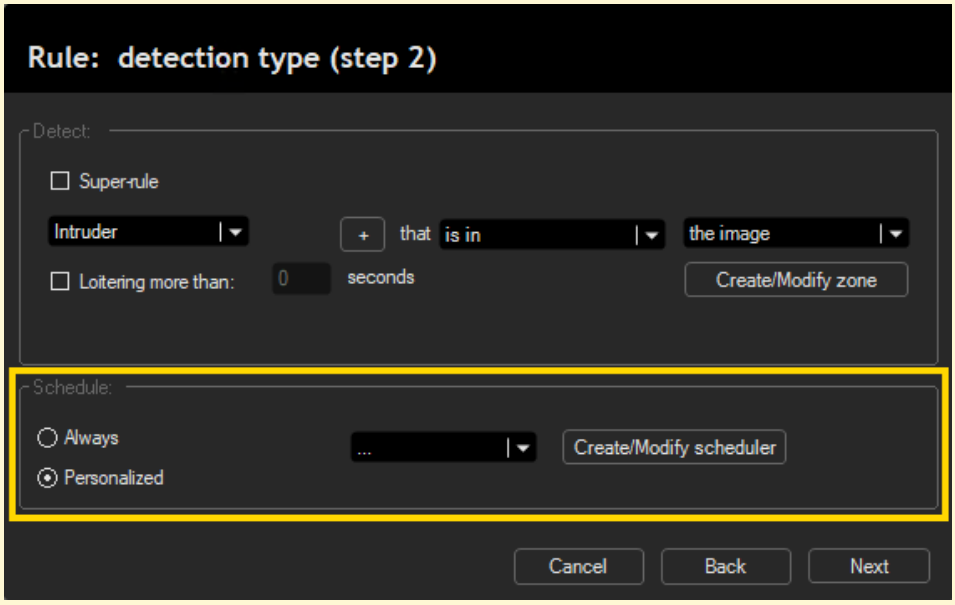
The most significant aspect of this combination is that the subject detected in the previous condition is independent from the one triggering any of the above possible combinations.

> Example
>
> Alarm is triggered only if a person is detected and within the next 30 seconds a vehicle stops for at least 10 seconds in a defined area.

Schedule

In the **Schedule** section you can define when the alarm triggered by the respective rule is to be activated. During the inactive periods, rules are ignored by the system and do not generate alerts.

You can choose between the following options:

Option	Description
Always	Select this option to activate the rule always.
Personalized	Select this option to activate the rule only on specific days and times of the week. Select an existing schedule from the drop-down list or click the **Create/Modify Scheduler** button to create or modify a schedule for the rule. 

Create/Modify Zone

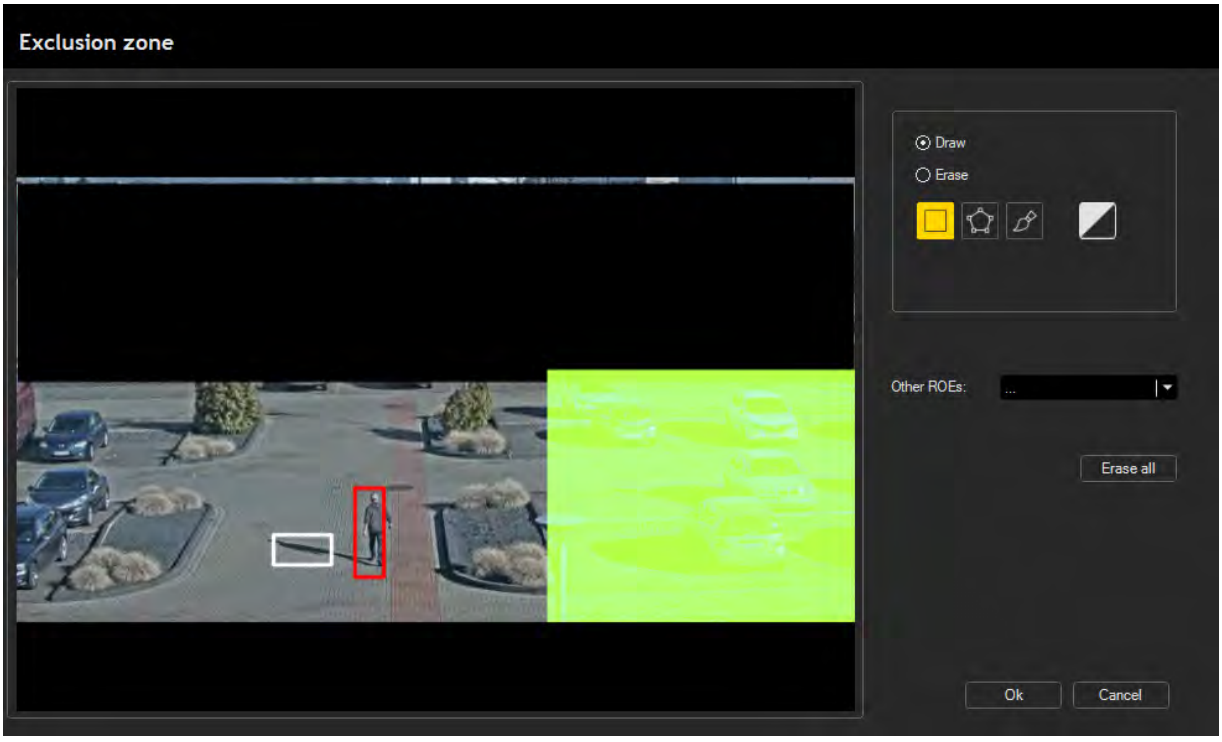
How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next. In the Detection type (step 2) window, click the Create/Modify zone button in the Detect section.

Region of Interest

You can narrow down the Region of interest in the video image by using exclusion zones to exclude the areas that the system does not need to analyze.

Exclusion zones are very useful for ignoring areas that are busy but have little useful information, e.g. a busy street, a public entrance, etc.

You can use an exclusion zone to reduce the number of false alarms in a certain area of the video image. The shaded area is the exclusion zone, and movements in this area will not trigger an alarm.



You use the following options to define exclusion zones:

Option	Description
Draw / Erase	This option allows you to select tools to define the exclusion zone or to delete part of the zone.
Erase all	This option allows you to delete the entire exclusion zone you have defined.
Rectangle Tool	Use this option to define an exclusion zone in rectangular form. Click and drag the mouse over the camera image and then release the mouse button.
Polygon Tool	Use this option to define an exclusion zone in polygon form. Use the mouse to create your polygon. When it's done, click the first vertex to close it.
Brush Tool	Use this option to define an exclusion zone by brushing over the camera image while holding down the left mouse button. When you have selected the brush tool, you can change the thickness of the brush used.
Black/White Button	This option allows you to set the color of your exclusion zone. It is only used to improve visibility and does not affect the function of the system.
Other REOs	This option allows you to select the ROEs set in the equipment for other cameras and rules.

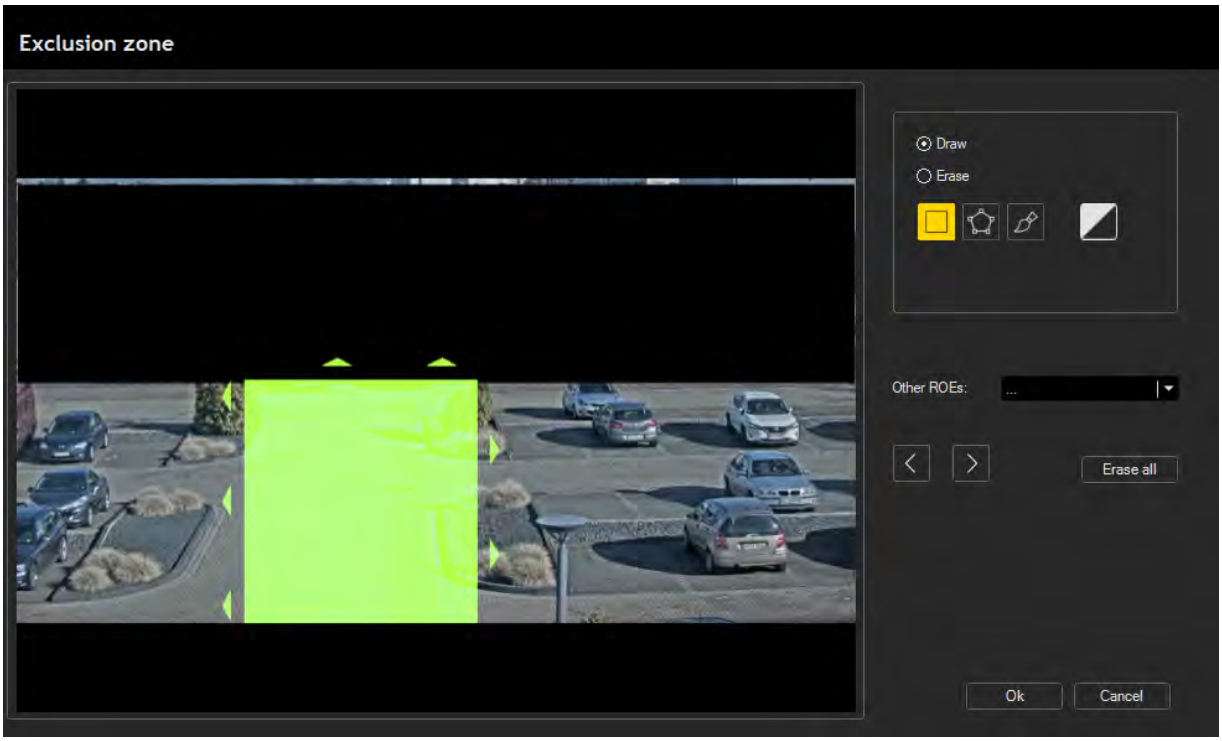
Zone

The zone is used to detect whether objects enter or exit the detection area. You can narrow down the detection area by defining zones. Object movements in the zone itself are not detected.

Alarms are triggered when an object enters or exits the detection area from a zone.

- The **Enter** rule (▶) is triggered when the object moves from the zone (green area) to the detection area (non-green area).
- The **Exit** rule (◀)is triggered when the object moves out of the detection area (non-green area), into the zone (green area).
- The **Enters/Exits** rule (◀▶) is triggered in both cases.

In crowded scenarios, the object moving from one area to the other area in a certain direction must be clearly visible before, during and after moving to the new area. Otherwise, the alarm may not be triggered.



You use the following options to define exclusion zones:

Option	Description
Draw / Erase	This option allows you to select tools to define the exclusion zone or to delete part of the zone.
Erase all	This option allows you to delete the entire exclusion zone you have defined.
Rectangle Tool	Use this option to define an exclusion zone in rectangular form. Click and drag the mouse over the camera image and then release the mouse button.
Polygon Tool	Use this option to define an exclusion zone in polygon form. Use the mouse to create your polygon. When it's done, click the first vertex to close it.

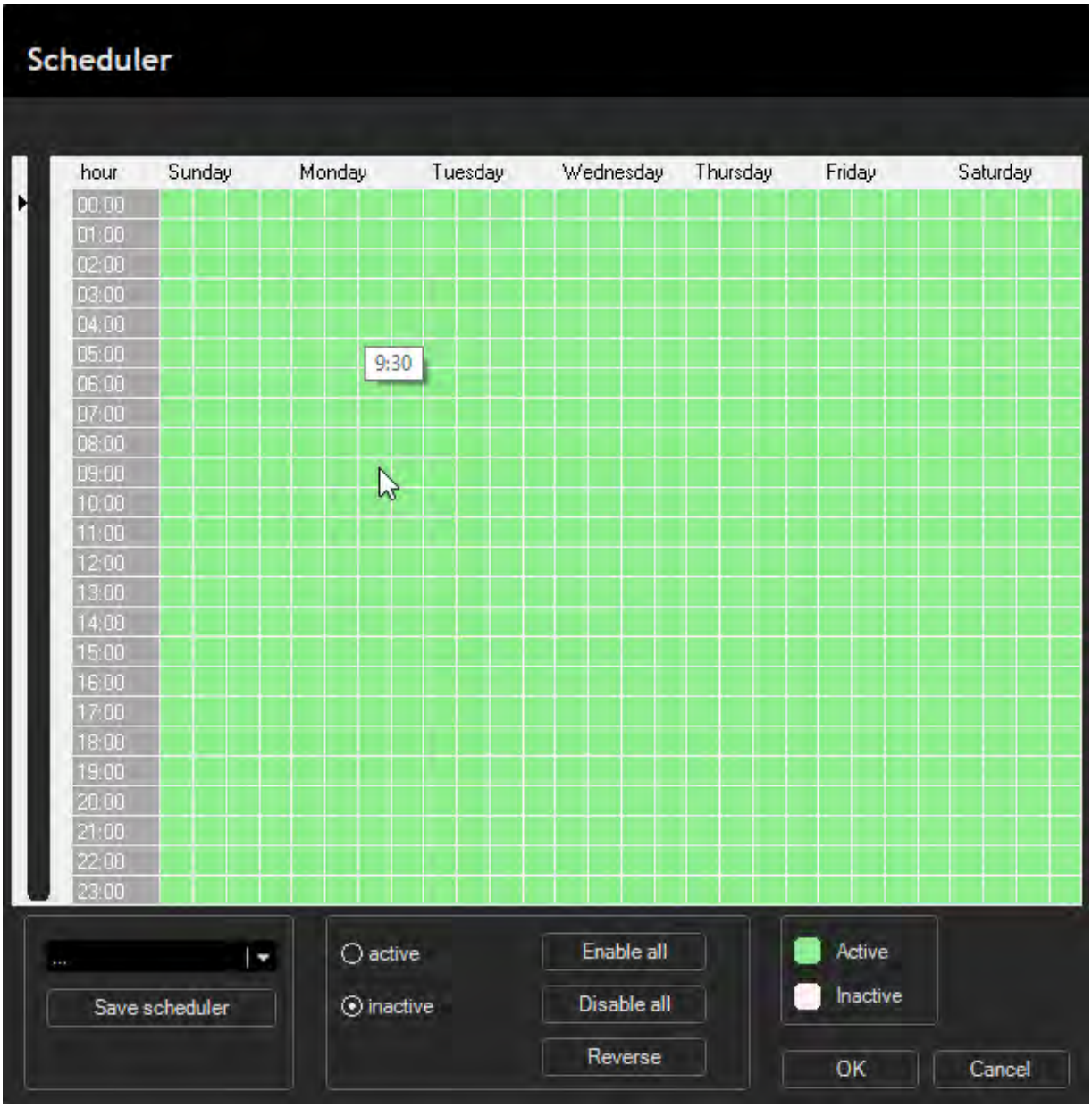
Option	Description
Brush Tool	Use this option to define an exclusion zone by brushing over the camera image while holding down the left mouse button. When you have selected the brush tool, you can change the thickness of the brush used.
Black/White Button	This option allows you to set the color of your exclusion zone. It is only used to improve visibility and does not affect the function of the system.
Other REOs	This option allows you to select the ROEs set in the equipment for other cameras and rules.
◀ ▶	Use these buttons to change the applied rule for the zone.

Create/Modify Scheduler

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next. In the Detection type (step 2) window, select Personalized in the Schedule section and click the Create/Modify scheduler button.

In the Scheduler dialog window you can set the days and times when the alarm triggered by the respective rule is to be activated. During the inactive periods, rules are ignored by the system and do not generate alerts.

Each box in the scheduler represents a 15-minute period. When you move the mouse over the box, the respective time is displayed.



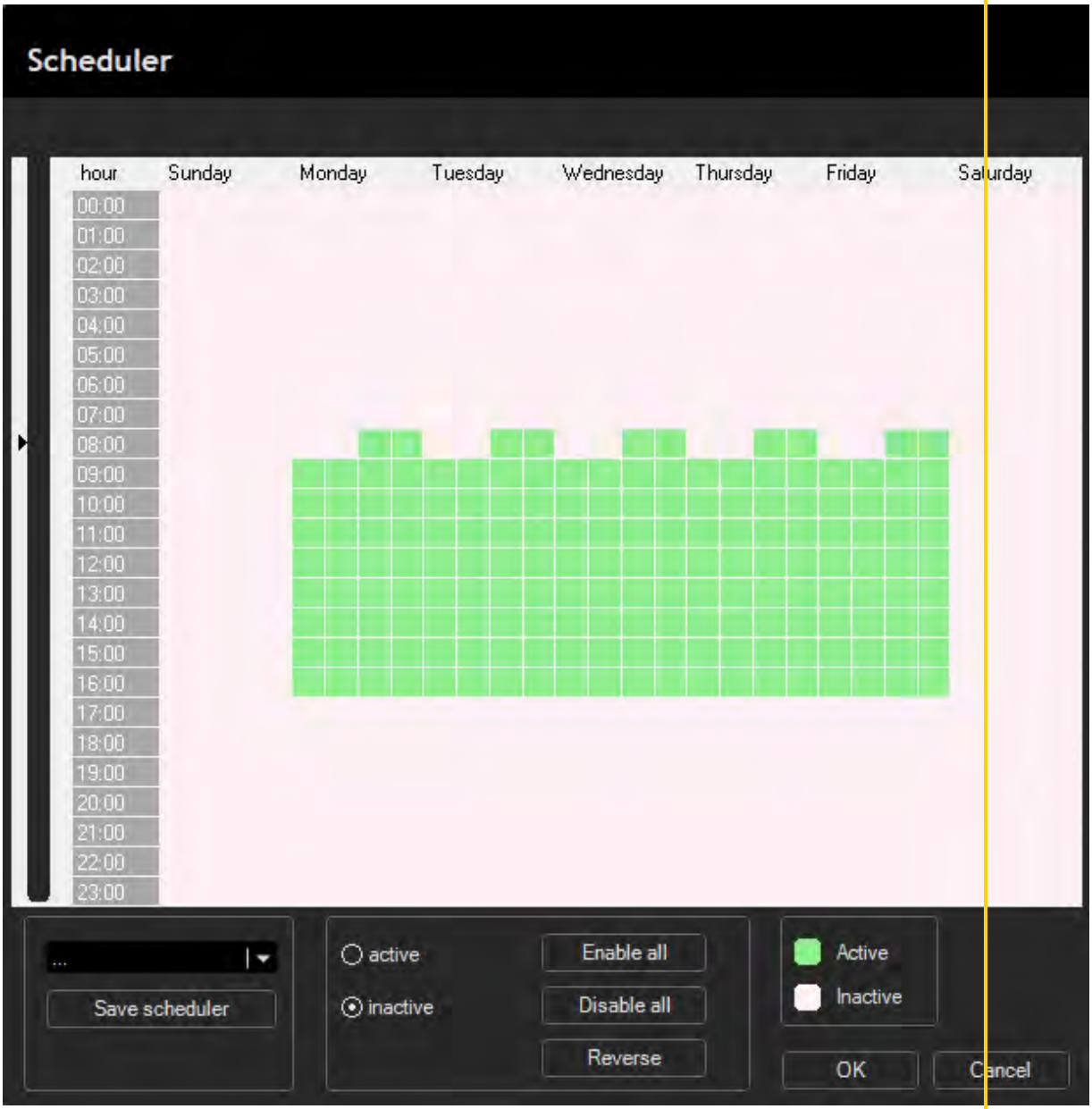
Create a Scheduler

1. Select the **active** or **inactive** option to set the times when the rule should be active or inactive.
2. Click on the required time boxes.
3. To undo your changes, click the **Enable all** button to activate all time boxes or the **Disable all** button to deactivate all time boxes.
4. Click the **Reverse** button to reverse the selected active or inactive times.

5. Click the **Save scheduler** button to save the scheduler. The **Scheduler** dialog window appears.
6. Enter the name of the scheduler and click **OK**.

Example

The example shows a schedule in which the rule is active from Monday to Friday from 8:30 am to 7:00 pm.



Edit a Scheduler

1. Select the respective scheduler from the drop-down list.
2. Edit the scheduler.
3. Click the **Save scheduler** button. The **Edit scheduler** dialog window appears.
4. Confirm the dialog **This scheduler already exists. Modify scheduler for all involved rules?** with **Yes**.

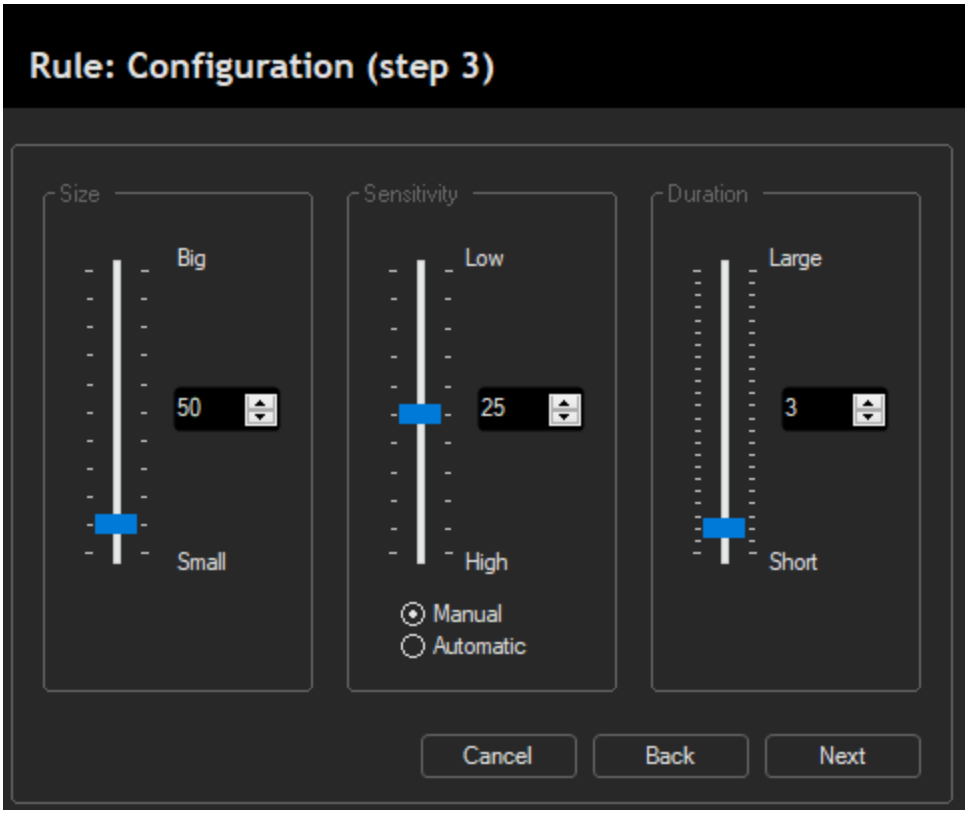
Delete a Scheduler

1. Select the respective scheduler from the drop-down list.
2. Click the **Delete scheduler** button. The **Attention** dialog window appears.
3. Confirm the dialog **Delete selected scheduler?** with **Yes**.

Configuration (Motion Detection Type)

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next. In the Detection type (step 2) window, select the detection type Motion in the Detect section and click Next.

This dialog window is only available if you have selected the **Motion Detection Type**. If you have selected another detection type, the system goes directly to the **Response** step.



You can configure the following settings by dragging the slider or setting the value in the box:

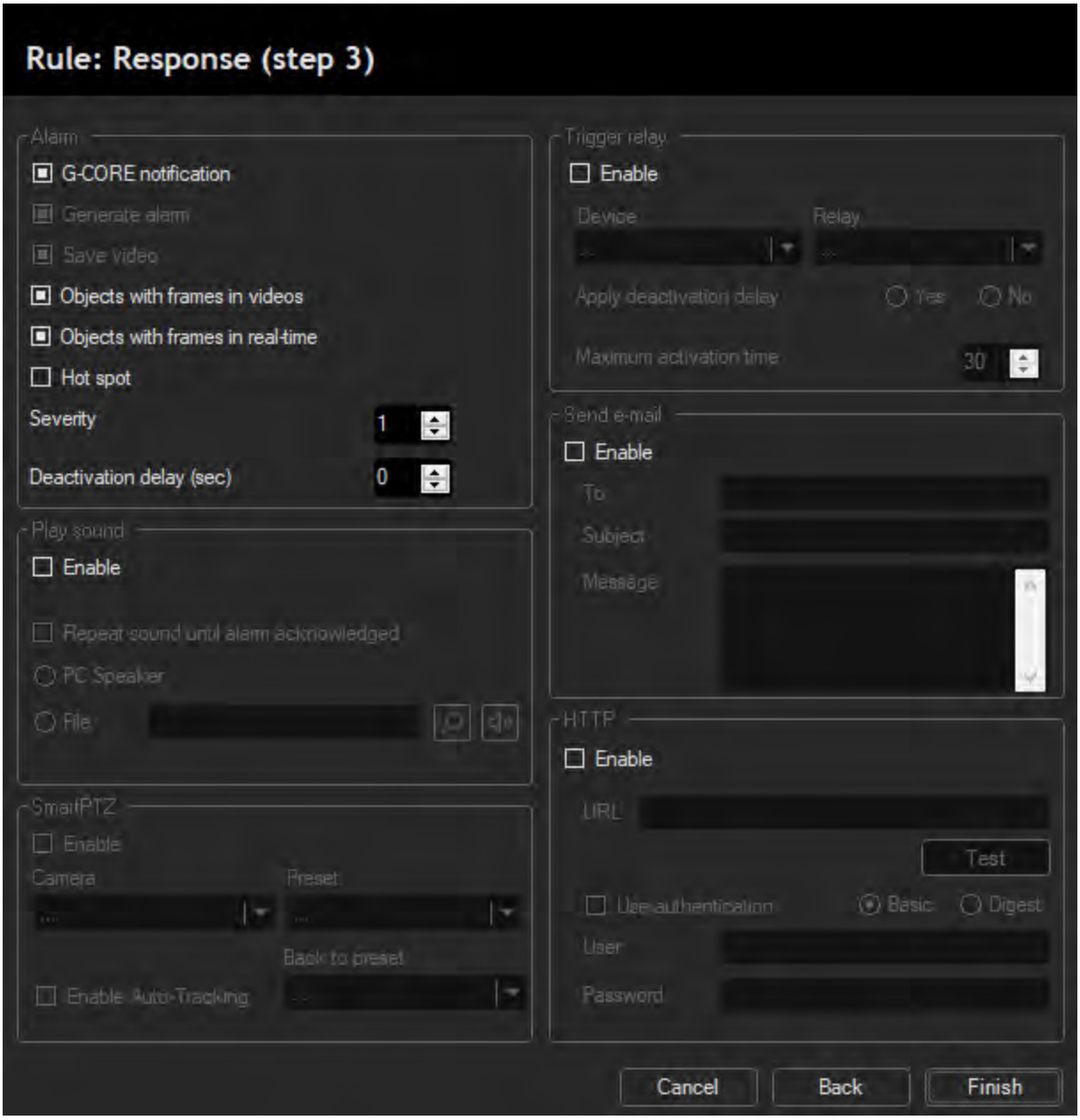
Setting	Description
Size	The size specifies the minimum number of pixels in the image that must be changed for motion detection to be activated. If the number of pixel changes is lower, the detection will not be activated. **Example** For example, if a person moving in the scene causes a change of 45 pixels compared to the previous image, the setting must be at least 45 pixels for the person to be detected.
Sensitivity	The sensitivity specifies the minimum change that a pixel must

Setting	Description
	have for motion detection to be activated. If the sensitivity is too low, the system reacts to the slightest changes in the scene and triggers false alarms due to minor light changes. If the sensitive is too high, the system becomes immune to minor light changes and there is a risk that moving objects with similar colors to the background will not be detected. You can choose between two options: • Select the **Manual** option to set the sensitivity manually. • Select the **Automatic** option to have the system adjust the sensitivity automatically.
Duration	The duration specifies the number of consecutive frames the system needs for motion detection to be activated. Example For example, if a system operates at six frames per second and the duration is set to four frames, a bird with three frames (half a second) in the scene will not be detected, while a motorcycle with 12 frames (two seconds) in the scene will be detected.

Response

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next and Next.

In this dialog window you can define how the system responds when an alarm is triggered.



Alarm

Name	Description
G-Core notification	Sends alarm messages to G-Core.

Name	Description
Generate alarm	Enables the detection log. This option is enabled by default.
Save video	Saves the video generated by each alarm.
Objects with frames in videos	Draws frames around objects that trigger alarms so that they can be easily recognized on the screen. This option is valid for video recordings.
Objects with frames in real-time	Draws frames around objects that trigger alarm so that they can be easily recognized on the screen. This option is valid for live images.
Hot spot	Switches the monitoring screens of the system to Hot Spot mode when an alarm is triggered. The camera from which the alarm was triggered occupies the entire screen and all other windows are momentarily hidden.
Severity	Set the severity level of the alarm triggered by the rule. The severity level is useful for subsequent filtering of alarms (see **Alarm Search**).
Deactivation delay	Set the number of seconds the system will wait according to the rule before sending the alarm to G-Core. This delay alarm feature gives the user time to turn off the alarm using the alarm keypad or disable the device without alerting G-Core.

Play Sound

Name	Description
Enable	Enable this option to play a sound each time an alarm is triggered.
Repeat sound until alarm acknowledge	If this option is enabled, the system plays the sound until the alarm is acknowledged.
PC Speaker	If this option is enabled, the computer generates a beep via the internal speaker.
File	If this option is enabled, the system generates the sound

Name	Description
	with a selected file. Click the button to select a file. Any WAV file can be played. The system provides a set of WAV files, but you can also use other WAV files. Click the button to play the selected sound.

SmartPTZ

This feature is only available for ONVIFPTZ cameras and with the Perimeter+ ALR license.

Name	Description
Enable	Enable this option to automatically move an ONVIF PTZ camera to a new position when an event is detected. After moving the camera to a new predefined position, a secondary video is recorded, as an additional check.
Camera	Select the required PTZ camera.
Preset	Select the preset (see **Presets**).
Enable auto-tracking	Enable this option to automatically track everything detected by the selected PTZ camera, after moving the PTZ camera to a specified preset position. This automatic tracking is configured by the preset auto-tracking settings (see **Auto Tracking**).
Back to preset	Selected the preset position that the PTZ camera will move to after autotracking is complete.

Trigger Relay

Name	Description
Enable	Enable this option to activate external devices via relays.
Device / Relay	Select the device to be activated by the relay. Available devices are:

Name	Description
	• The camera for which the rule is defined (ONVIF cameras with output relays only). • Compatible external devices added via the camera menu (see **Device Configuration**).
Relay	Select the relay that can be used to activate the device (see **External Output**).
Apply deactivation delay	Select **Yes** to synchronize the relay activation with the alarm notification to G-Core.
Maximum activation time	Set the maximum duration that the relay should remain activated. If you do not set the duration, the default maximum activation will be applied.

Send E-Mail

Name	Description
Enable	Enable this option to trigger the sending of an email containing an alarm image, video or link to a specific recipient with an optional message. **To use this option, you must enter the SMTP mail server connection details in the Mail tab of the configuration window.**
To	Enter the recipient of the email.
Subject	Enter the subject of the email.
Message	Enter the message of the email.

HTTP

Name	Description
Enable	Enable this option to send a GET type HTTP request to the specified URL.

Name	Description
URL	Enter the URL of the HTTP address.
Test	This button allows you to test the connection with the specified HTTP address. Depending on whether the connection is established or not, the background of the URL text box turns green or red.
Use authentication	Enable this option to add authentication credentials to the connection with the specified URL. Select whether the authentication type is **Basic** or **Digest**.
User	Enter the username for the connection to the specified URL.
Password	Enter the password for the connection to the specified URL.

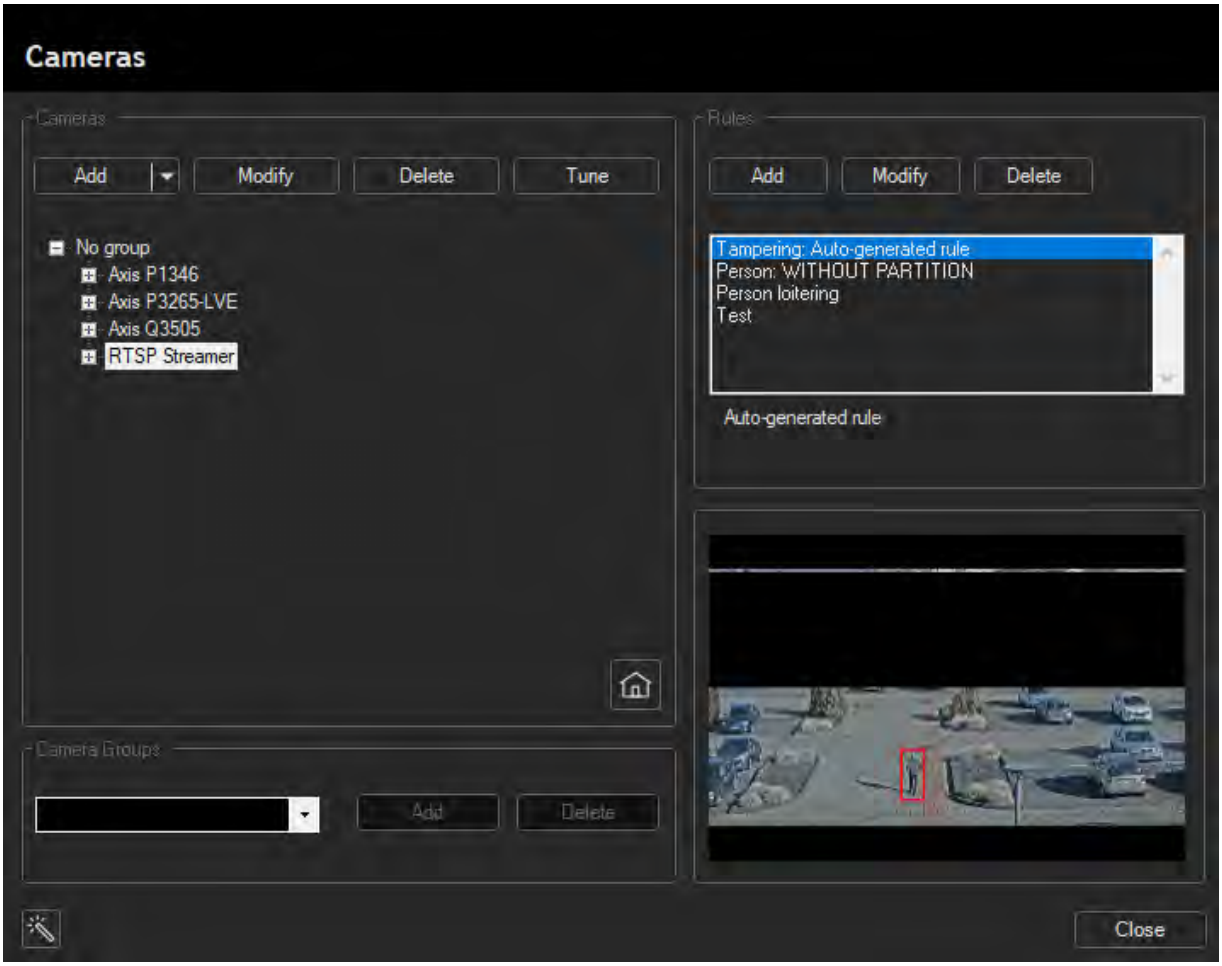
Tampering Rule

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. Select a camera.

The tamper rule is responsible for the detection of sudden changes in the camera image. The rule triggers an alarm when a sudden change in the camera image is detected, such as a changes in the scene or an unwanted change in the image.

This rule is created automatically when you create a camera, so it does not need to be created later. By default, the rule is not associated with any of the partitions.

It is highly recommended not to assign the rule to partitions, because in this state it will always work and generate alarms even if the system is not armed.



The sensitivity of the rule can be adjusted using the Tampering setting (see **Parameters**).

External Trigger Rule

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras. In the Cameras window, select a camera, click the Add button in the Rules section and click Next. In the Detection type (step 2) window, select the detection type External inputs in the Detect section and click Next.

Only available if a device is added.

This rule is used to detect changes of state of external inputs. You can choose between two types of inputs:

- External camera
- External device inputs

To select a camera or device input for external trigger detection, it must be compatible with the system (see **Add a Camera** or **Device Configuration**).

Once you have added the camera or device to the system, you can create external trigger rules associated with the available inputs.

Conceptual View

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.
In the Cameras window, click the icon.

The icon in the bottom left corner of the Cameras dialog window opens the conceptual view.

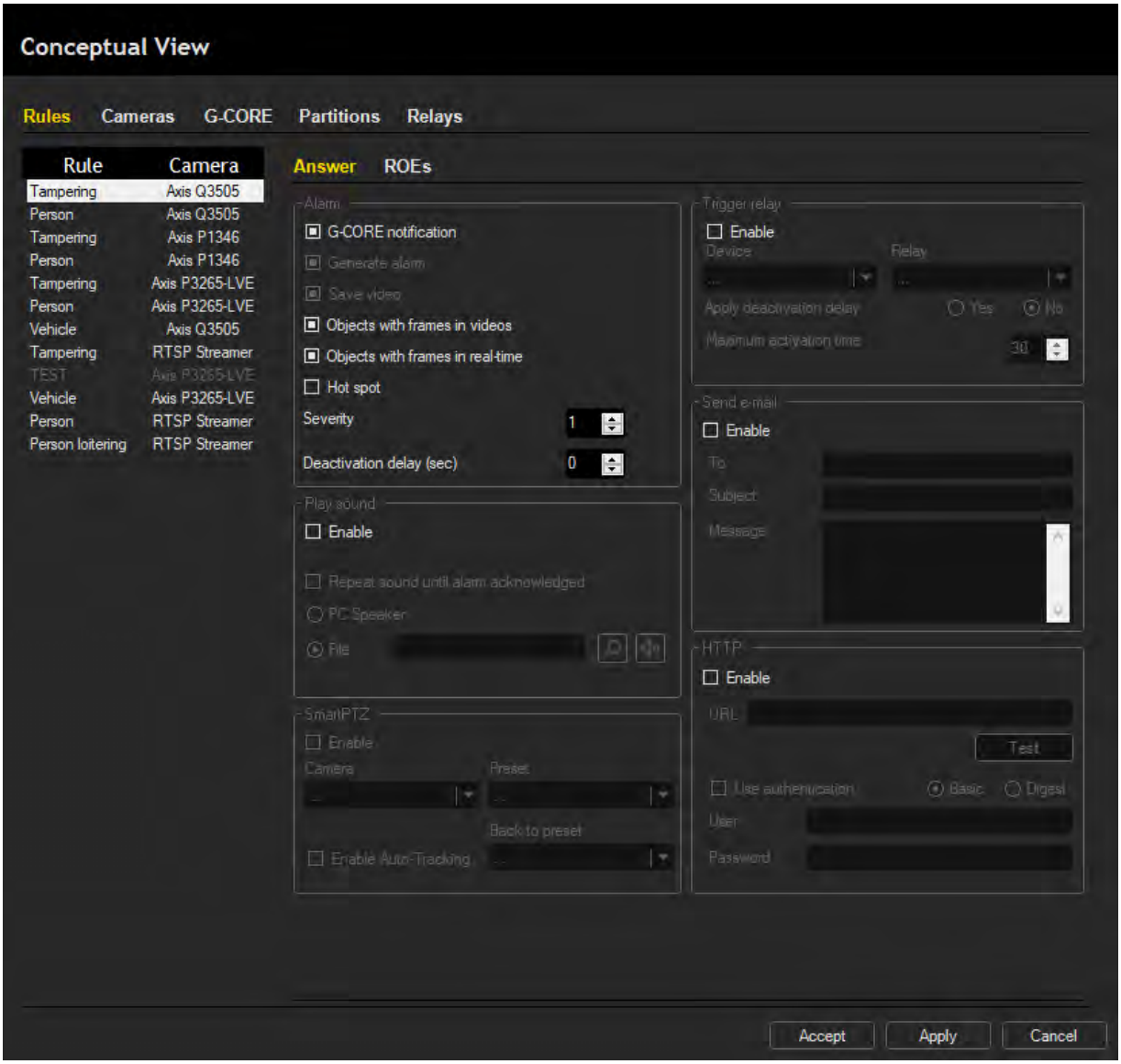
Clicking the icon after you have created cameras and rules opens a new window that allows you to view and modify some of the key features and rules of the camera and provides an overview of the installation.

The window contains several tabs with different options for camera and/or rule configuration. All changes made in a tab or sub-tab are saved by clicking Accept or Apply. However, if you temporarily change an option in a tab, the temporary change is retained when you switch to another tab and is displayed in the other tabs that refer to the same information.

Rules

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.
In the Cameras window, click the icon and then click the Rules tab.

On the **Rules** tab, you can access the **Response** configuration window (see **Response**) of the selected rule and the configuration window of the associated ROE (see **Create/Modify Zone**).



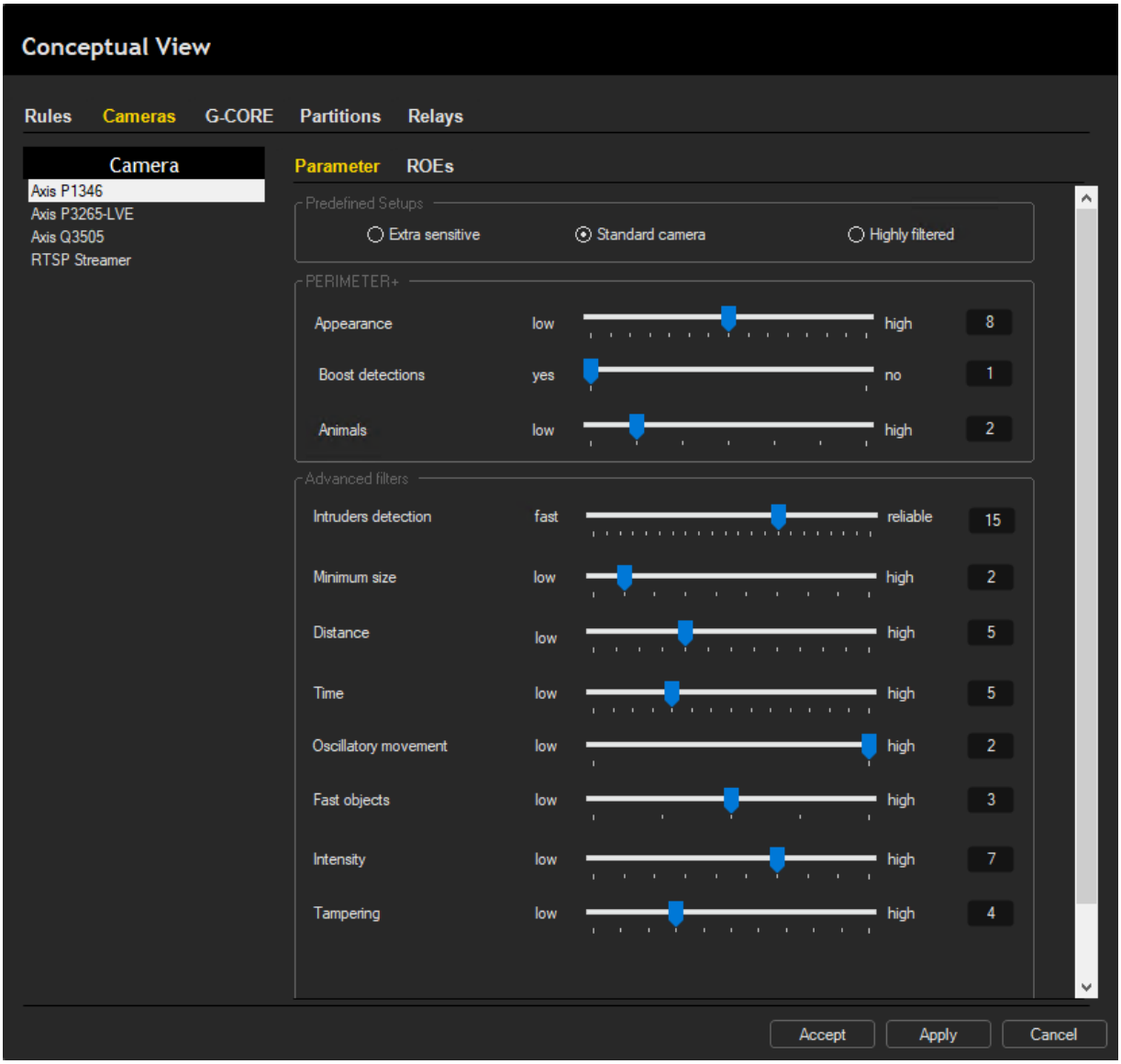
Cameras

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.

In the Cameras window, click the icon and then click the Cameras tab.

On the **Cameras** tab, you can access the configuration window of the camera settings and camera exclusion zone (ROE).

On the **Cameras** tab, you can access the **Parameter** configuration window (see **Parameters**) of the selected camera and the configuration window of the associated **ROE** (see **Create/Modify Zone**).



G-Core

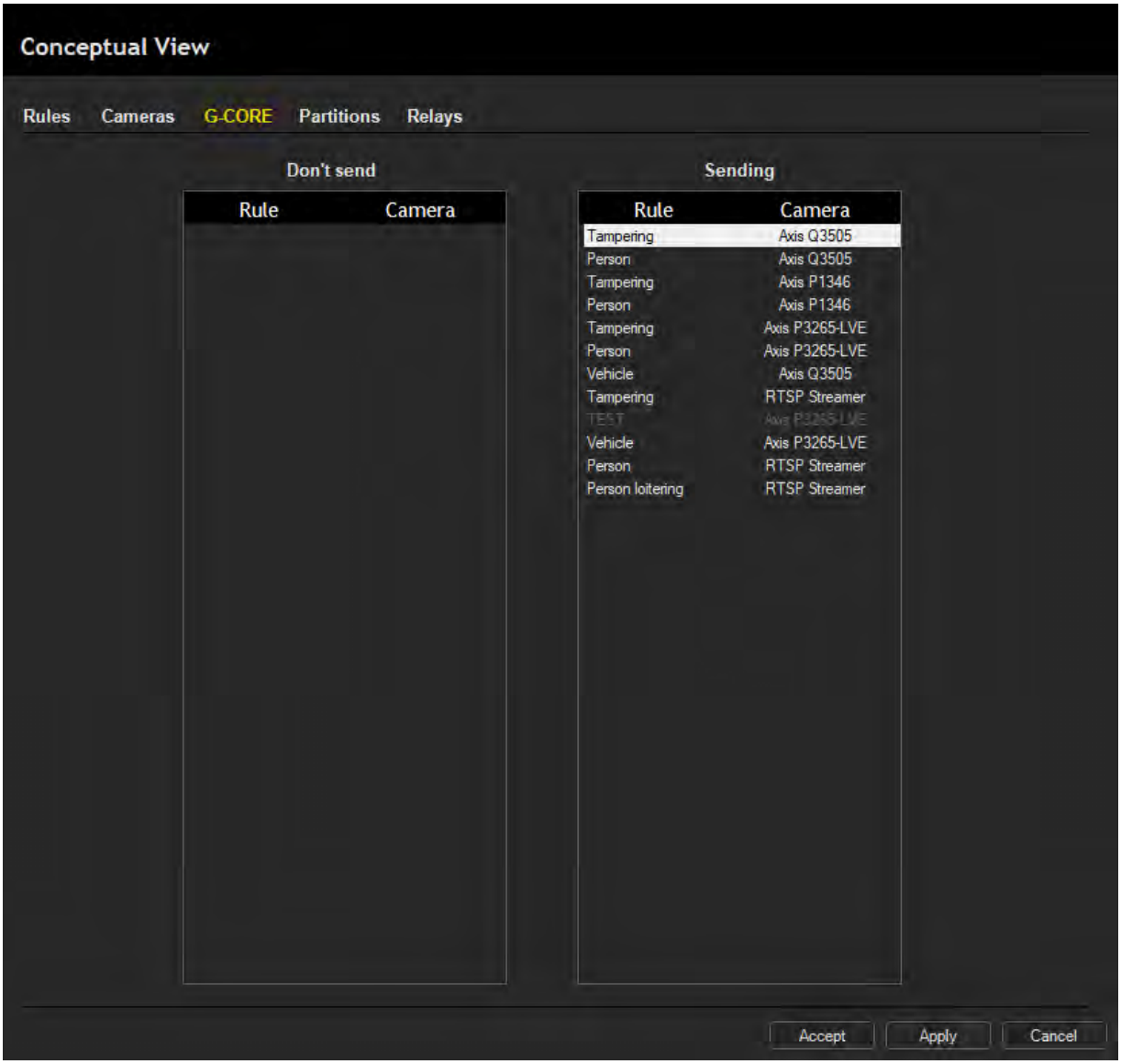
How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.

In the Cameras window, click the icon and then click the G-Core tab.

The **G-Core** tab contains two lists:

- The **Don't send** list contains rules that are not sent to G-Core.
- The **Sending** list contains the rules that are sent to G-Core.

You can change this in the window by dragging the rules from the list on one side to the list on the other side.



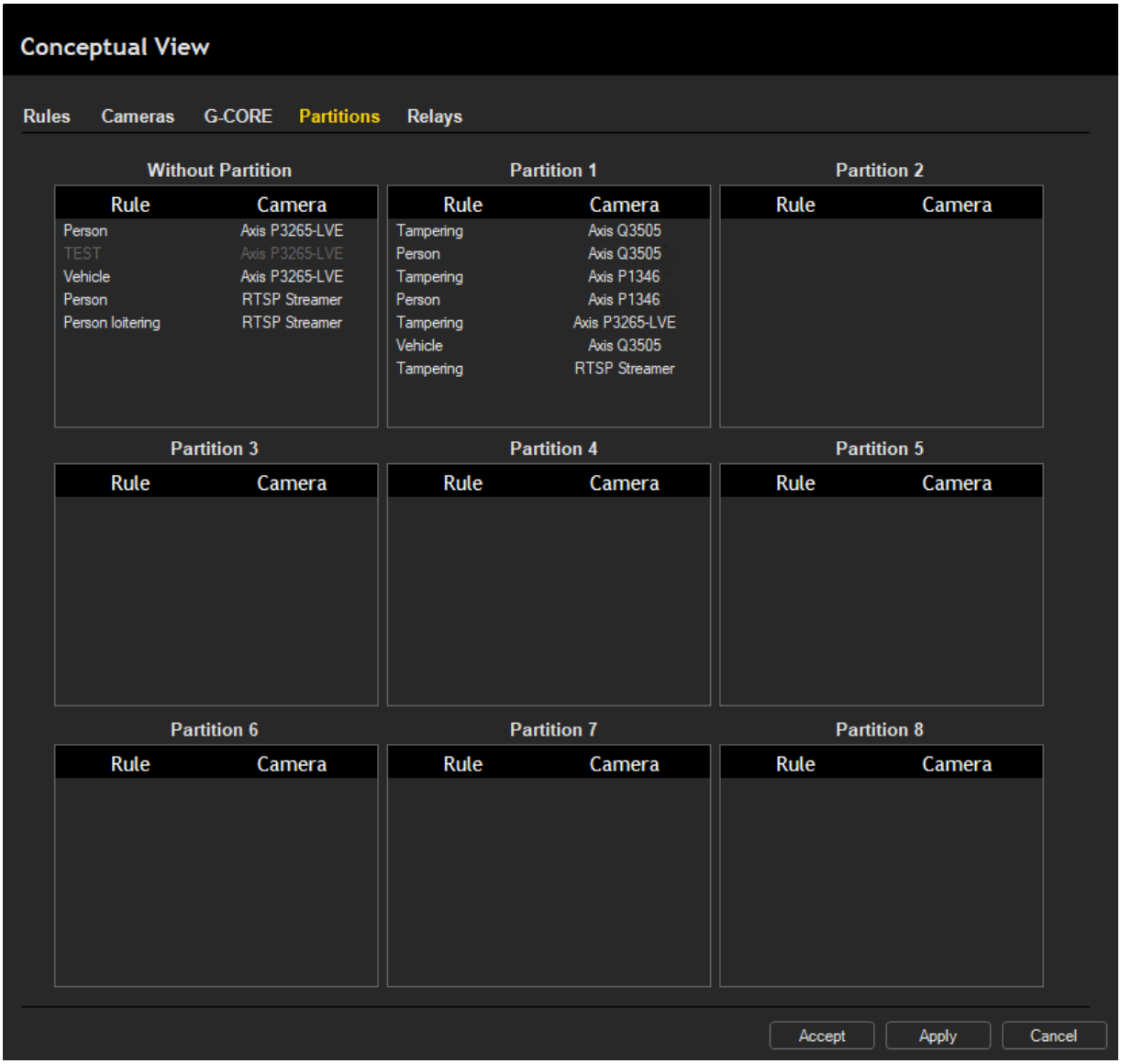
Partitions

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.
In the Cameras window, click the icon and then click the Partitions tab.

The Partitions tab is divided into nine lists representing the nine possible partitions (see **Partitions**) accepted by the system:

- Without Partition
- The eight external inputs (Partition 1 to Partition 8)

The rules are displayed in their corresponding partition, which can be changed by dragging each rule from one partition to another.



Relays

How to open this dialog window:
Click the Cameras icon in the system overview window, enter your username and password, click the Menu button, and select Cameras.

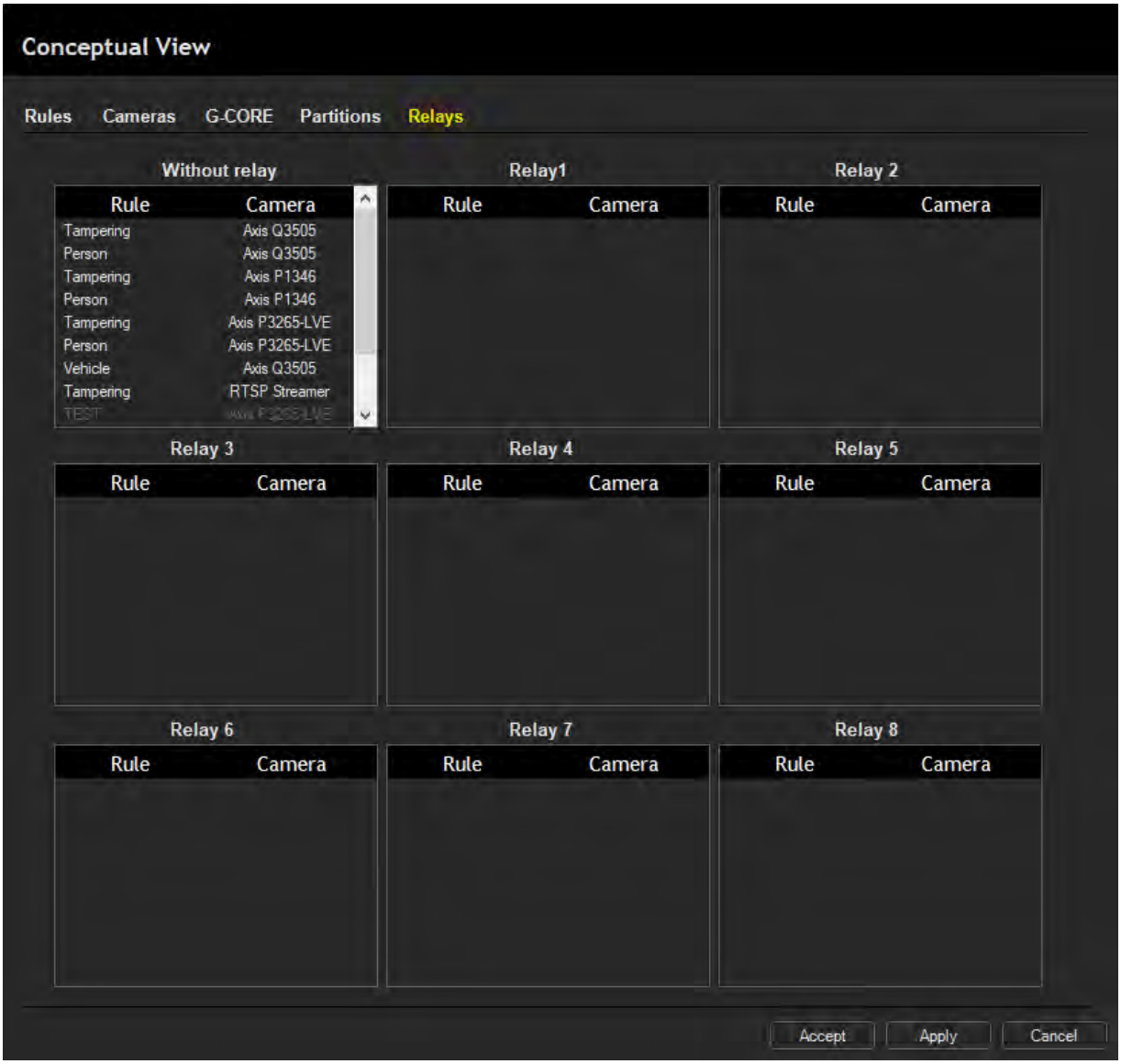
In the Cameras window, click the icon and then click the Relays tab.

The **Relays** tab is also divided into nine lists that represent the nine possible relay trigger cases (see **External Output**) accepted by the system. From **Without relay** to the relays that range from **Relay 1** to **Relay 8**. Like the other tabs, the rules are shown in the corresponding list. To change the relay that activates each rule, drag the rule from one list to another.

The **Relays** tab is divided into nine lists representing the nine possible relay trigger cases accepted by the system:

- **Without relay**
- The relays (**Relay 1** to **Relay 8**)

The rules are displayed in the corresponding list. To change the relay that activates each rule, drag the rule from one list to another.


Conceptual View
Rules
Cameras
G-CORE
Partitions
Relays
Without relay
Rule
Camera
Tampering
Axis Q3505
Person
Axis Q3505
Tampering
Axis P1346
Person
Axis P1346
Tampering
Axis P3265-LVE
Person
Axis P3265-LVE
Vehicle
Axis Q3505
Tampering
RTSP Streamer
Relay1
Relay 2
Relay 3
Relay 4
Relay 5
Relay 6
Relay 7
Relay 8
Accept
Apply
Cancel

G-Core Configuration

Add Perimeter+ Streams

Before you can add Perimeter+ streams in G-Core, you must enable the **RTSP Streaming** feature for all desired Perimeter+ streams in Perimeter+ (see **G-Core Configuration in Perimeter+** and **RTSP Streaming**).

Recording Perimeter+ streams is an advanced and optional feature that allows you to receive and record live feeds from Perimeter+ units. The Perimeter+ streams contain a detection frame around the detected object.

Notice that is not required nor necessary to add Perimeter+ streams in G-Core to receive Perimeter+ alarms in G-Core.

There are two different plugins in G-Core that you can use to add Perimeter+ streams in G-Core:

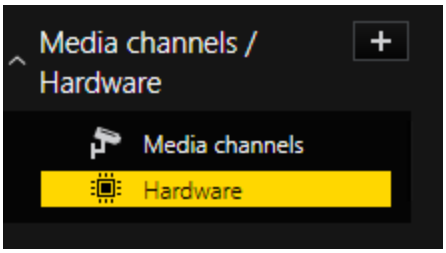
- **Universal RTSP Plugin**
- **GngMetaDataInjector Plugin**

For more information about the G-Core plugins, refer to the G-Core Addition Technical Information.

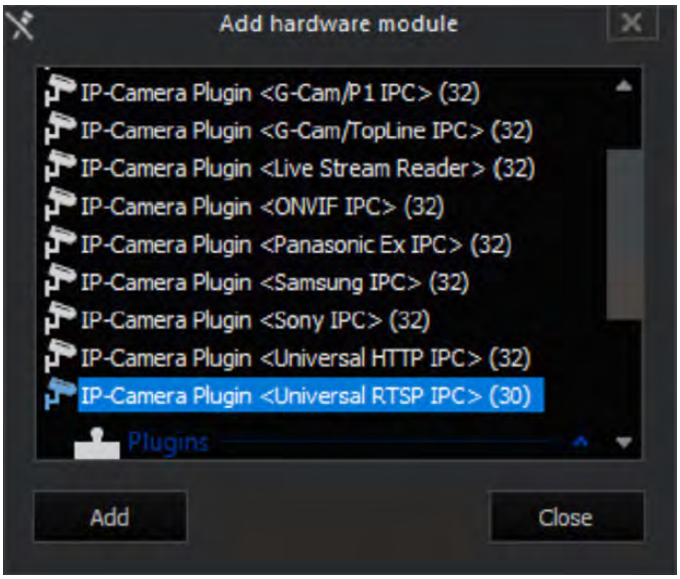
Universal RTSP Plugin

How to add Perimeter+ streams in G-Core with the Universal RTSP plugin:

1. Open G-Set.
2. In the drop-down menu of the **Media channels / Hardware** sidebar item, click **Hardware**.

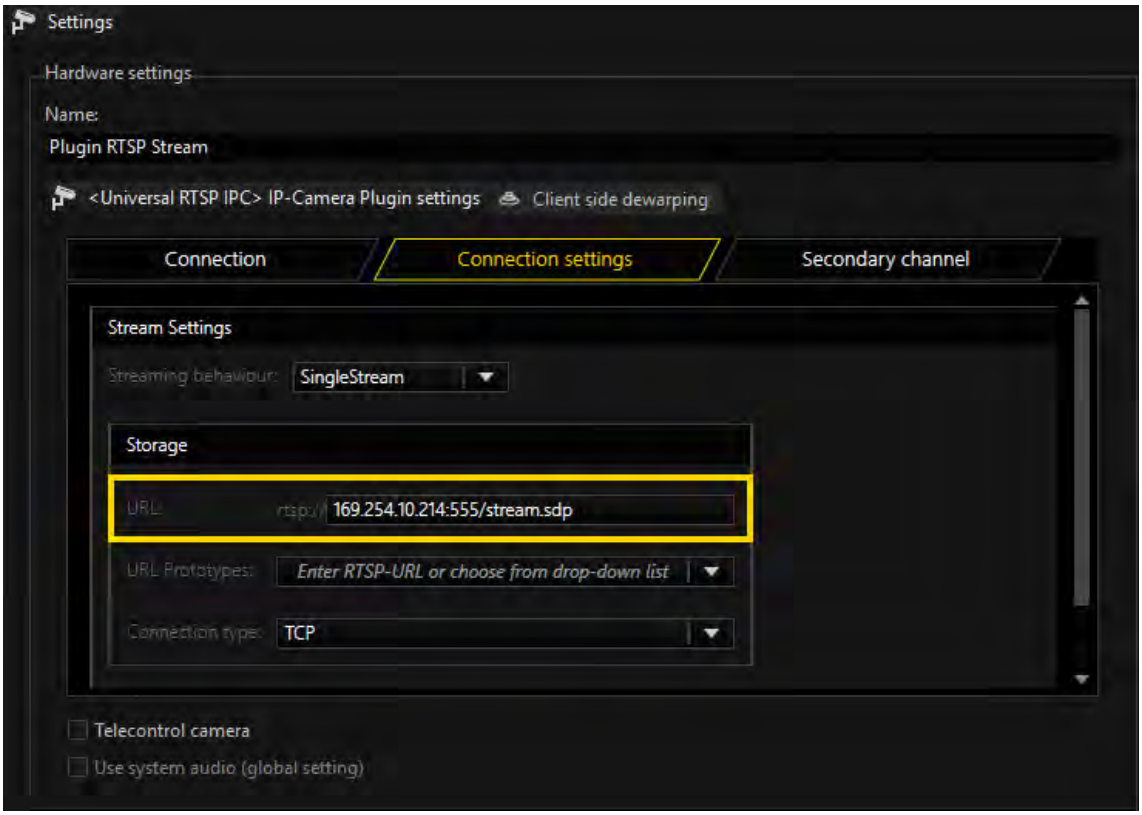


3. Click the icon in the toolbar of the **Hardware configuration** window. The **Add hardware module** dialog window opens.
4. Select the **IP-Camera Plugin <Universal RTSP IPC>** and click **Add**.

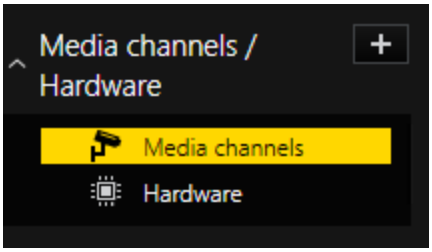


5. Select the plugin from the **Hardware module list**.
6. On the **Connection settings** tab, enter the RTSP URL using the following format: `ip:port/stream.sdp` (example: `169.254.10.214:555/stream.sdp`)

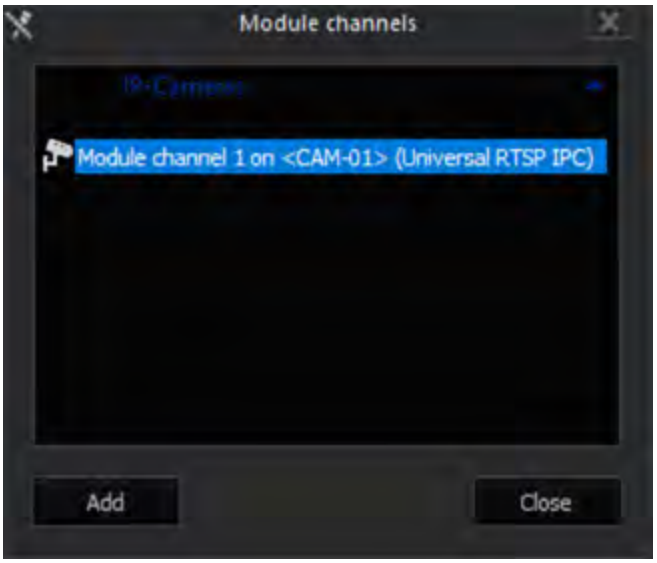
> **Port and stream name (stream.sdp) must correspond to the RTSP streaming setting in Perimeter+ (see RTSP Streaming).**



7. In the drop-down menu of the **Media channels / Hardware** sidebar item, click **Media channels**.



8. Click the icon in the toolbar of the **Media channel configuration** window. The **Module channels** dialog window opens.
9. Select the previously created module.



10. Select the media channel from the **Media channel list**.
11. Enter the required settings for the media channel.
12. Click the icon in the menu bar to send all changes to the server.

GngMetaDataInjector Plugin

The MetaDataInjector plugin allows you to receive metadata from Perimeter+, assign it to a media channel, and thus display it directly in the high-resolution video stream of the camera.

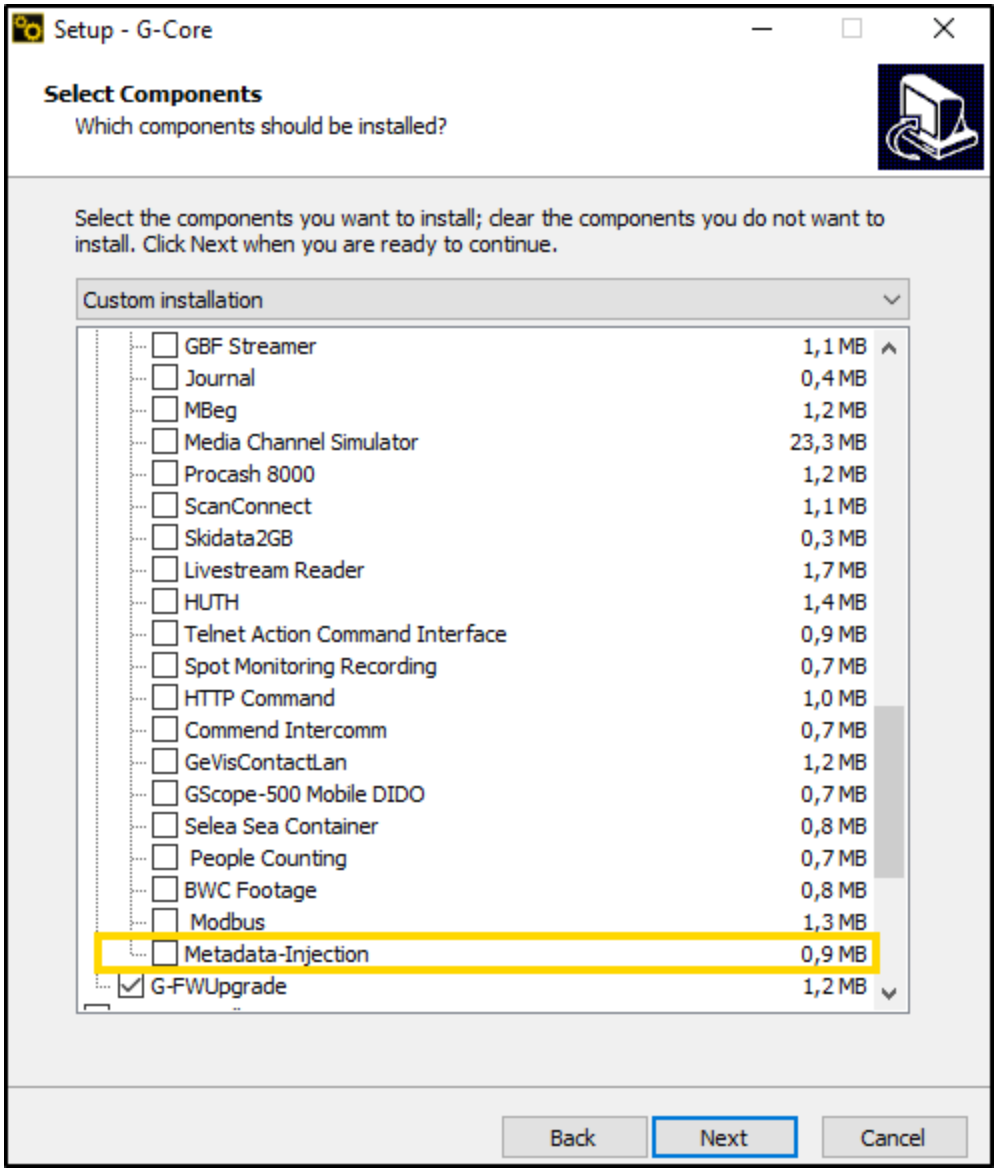
An example is the analysis of a video stream that is both analyzed on Perimeter+ and processed in G-Core. In this case, Perimeter+ provides only the results of the analysis to G-Core, since the video images from Perimeter+ themselves are not of sufficient quality. The metadata is transmitted to the MetaDataInjector plugin via an RTSP port and linked to the corresponding images from the camera via this plugin. This allows the live and recorded streams to display the images and associated metadata synchronously.

Since the metadata is received by the G-Core system via Perimeter+ with a slight delay, the images are buffered for an adjustable time (see Video stream delay) and there is a slight delay in the live stream.

The representation of the received metadata can be taken over from Perimeter+ or customized in G-Core to the respective conditions (see **Metadata Representation**).

Installation

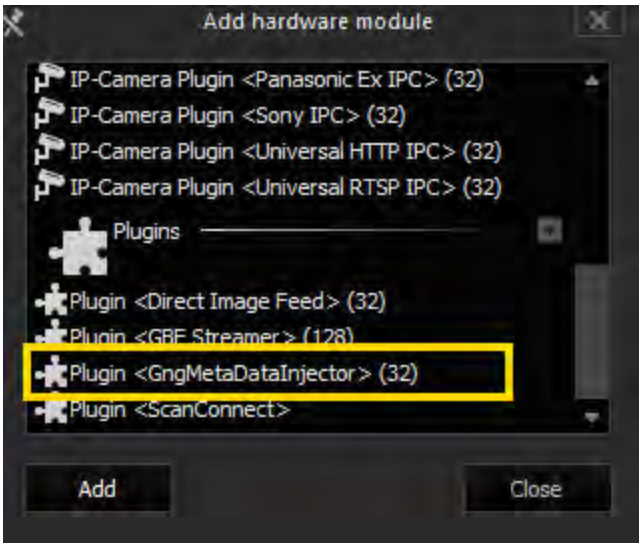
During the installation of G-Core, enable the **Metadata-Injection** plugin in the **Select Components** list.



Add the Plugin

How to add the MetaDataInjector plugin:

1. Click the icon in the toolbar of the **Hardware configuration** window. The **Add hardware module** dialog window opens.
2. Select the **Plugin <GngMetaDataInjector>**.



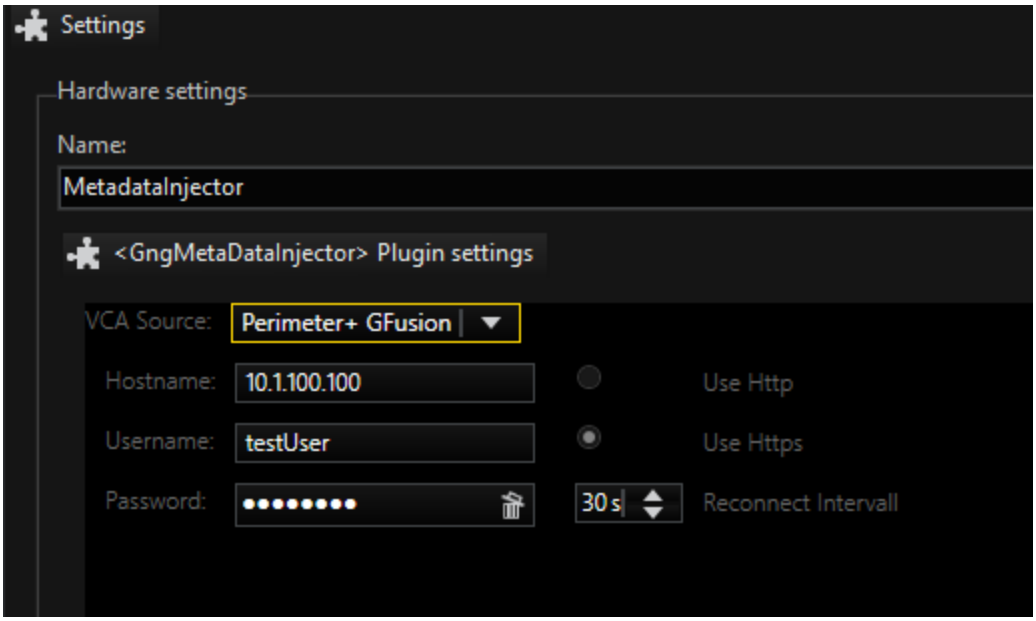
3. Click **Add**.

Set Perimeter+

The MetaDataInjector plugin allows you to map metadata from any source to any channel.

How to set Perimeter+:

1. Select the plugin from the **Hardware module list**.



2. Enter the following settings:

Name	Description
VCA Source	Select **Perimeter+ GFusion**.
Hostname	Enter the hostname or IP address of Perimeter+.
Username	If authentication is enabled in Perimeter+, you must enter the username.
Password	If authentication is enabled in Perimeter+, you must enter the password.
Use Http Use Https	Select this option to use HTTP or HTTPS for encryption. **This setting is currently not active.**
Reconnect Interval	Enter the interval in seconds between reconnection attempts when the connection is lost. The default is 30 seconds.

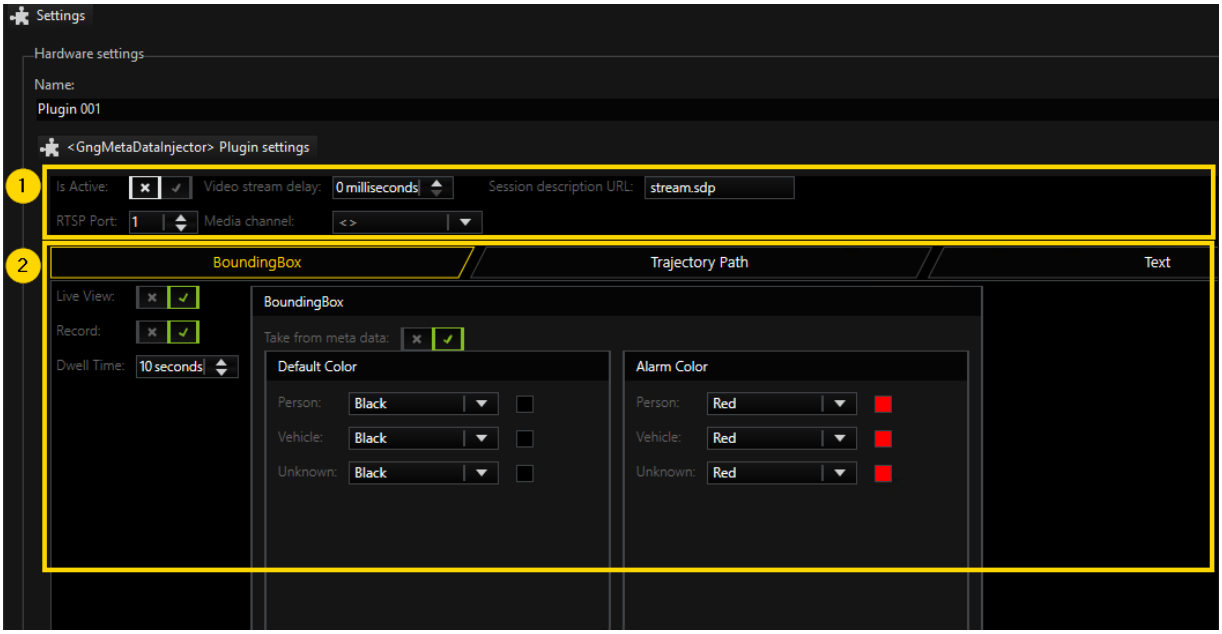
3. Click the icon in the menu bar to send all changes to the server.

Set the Channel

You can set up to 16 channels with one MetaDataInjector plugin.

To set a channel, select the media channel from the **Media channel list**. The settings window of the respective channel opens, which consists of two settings areas:

- **Channel Mapping**
- **Metadata Representation**:
  - **Bounding Box**
  - **Trajectory Path**
  - **Text**



Channel Mapping

In this setting area, you set the mapping information that is relevant for connecting to the metadata stream. The following settings are available:

Name	Description
Is Active	Enable the mapping or drawing of all metadata in the stream. Disabled by default.
Video stream delay	Set how long the video will be delayed to synchronize the metadata coming from Perimeter+ with the images. The default is 0 milliseconds.
Session description URL	Enter the stream name. This information is appended to the URL of the metadata stream. The default is **stream.sdp**.
RTSP Port	Enter the port corresponding to the metadata source of the metadata stream set in Perimeter+. In Perimeter+, a port must be defined for each configured channel. The default is 1.
Media channel	Select the media channel in which to display the metadata. Each configured channel is displayed in this drop-down list.

Metadata Representation

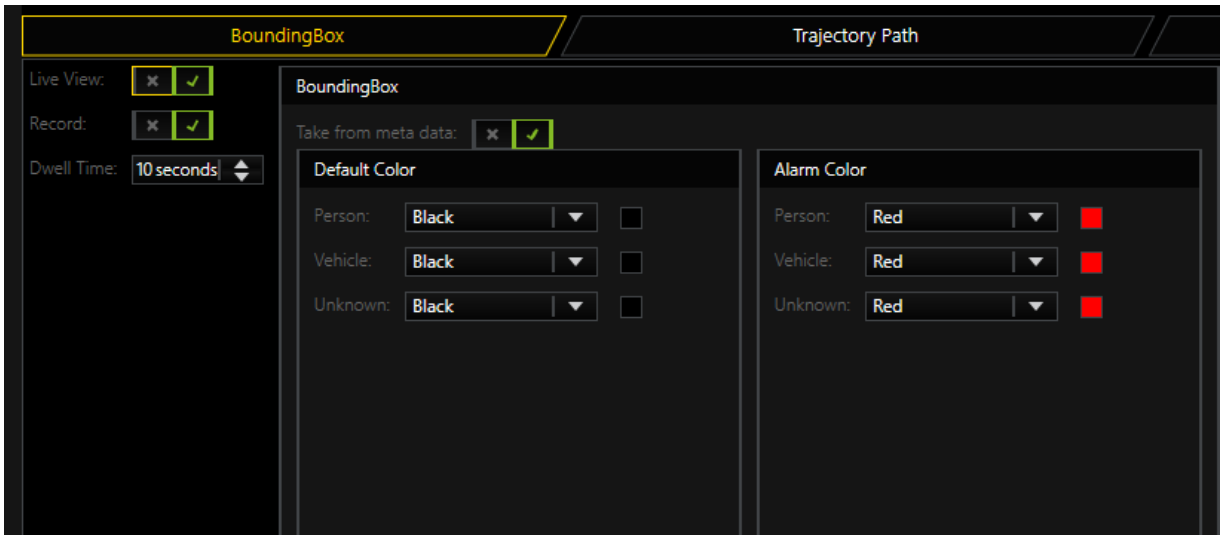
In this settings area, you set the representation of the metadata in the media channel. Configured channels then display bounding box, trajectory path and text as overlays in the viewer.

Bounding Box

The bounding box is a polygon drawn around an object detected in the scene, for example a person or vehicle.

Name	Description
Live View	Enable the drawing of the bounding box in the live stream. Enabled by default.
Record	Enable the drawing of the bounding box in the recorded stream. Enabled by default. **Drawing the bounding box for the live and recorded stream can be enabled or disabled independently.**

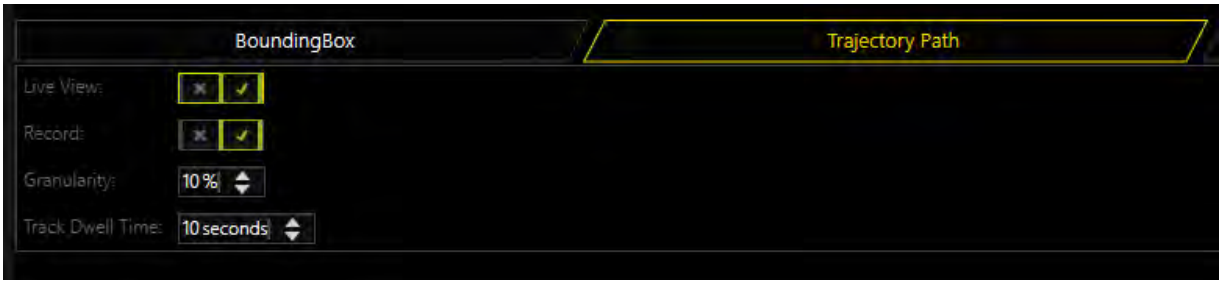
Name	Description
Dwell Time	Set how long the metadata information (bounding box, trajectory path and text) is displayed when the object is no longer tracked. The default is 10 seconds.
Take from metadata	Enable this option to take the color for displaying the metadata from the metadata provided by Perimeter+. If you disable this option, the colors you define in the **Default Color** area will be used. Enabled by default.
Default Color	Select the color of the metadata information (bounding box, trajectory path and text) for objects classified as person, vehicle or unknown object. The default color is black.
Alarm Color	Select the color of the metadata information (bounding box, trajectory path and text) for objects classified as person, vehicle, or unknown object, when the metadata has assigned an alarm to the object. The default color is red. **This setting is currently not active.**



Trajectory Path

The trajectory path shows where the detected object has moved in the scene.

Name	Description
Live View	Enable the drawing of the trajectory path in the live stream. Enabled by default.
Record	Enable the drawing of the trajectory path in the recorded stream. Enabled by default. **Drawing the trajectory path for the live and recorded stream can be enabled or disabled independently.**
Granularity	Set how granular the trajectory path is represented. A higher granularity indicates that the path contains more points and is more accurate. A lower granularity indicates that the path is coarser and less accurate. The default is 10%.
Track Dwell Time	Set how long the trajectory path is represented. A dwell time of 1 second indicates a short path and a dwell time of 20 seconds a long path. The default is 10 seconds.



Text

The text details of the detected object are displayed as text in the upper left corner of the bounding box.

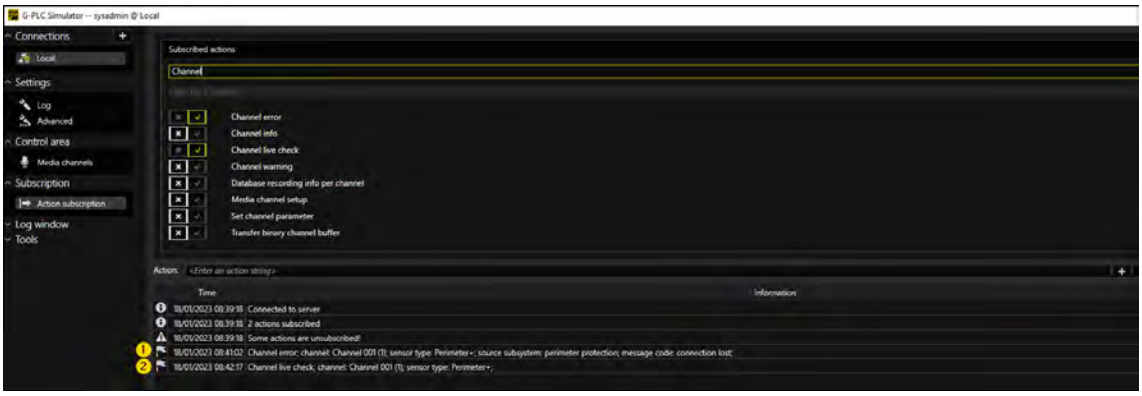
Name	Description
Live View	Enable the displaying of the text in the live stream. Enabled by default.

Name	Description
Record	Enable the displaying of the text in the recorded stream. Enabled by default. **Displaying the text for the live and recorded stream can be enabled or disabled independently.**
Class name	Enable the displaying of the class name of the detected object (e.g. "Person" or "Vehicle"). Enabled by default.
Speed	Enable the displaying of the speed of the object detected object. Enabled by default. **This setting is currently not active with the Perimeter+ GFusion VCA source.**
Confidence	Enable the displaying of the percentage confidence of reliable detection of the object. Enabled by default.

Lost Connection

When the connection to Perimeter+ is lost, the following actions are sent:

- 1 Channel error: The connection is lost.
- 2 Channel live check: The connection is restored.

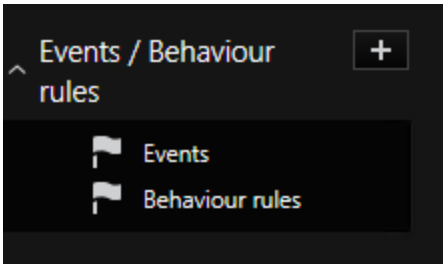


The note **Perimeter+ Device disconnected** is displayed in the viewer. No metadata is displayed.

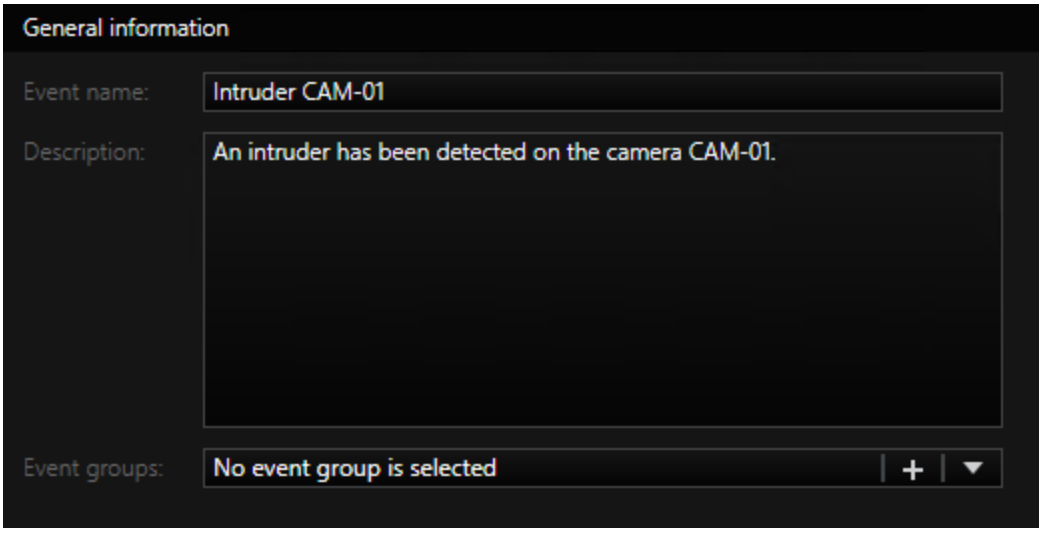
Add Perimeter+ Alarms

How to add Perimeter+ alarms in G-Core:

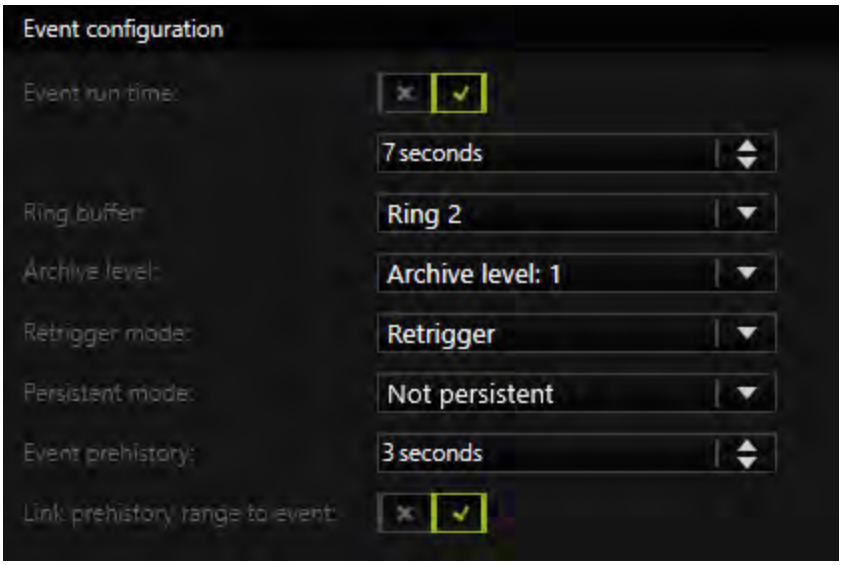
1. In the **Events / Behaviour rules** sidebar item, click the **+** icon, to open the Event/Alarm wizard.



2. On the **Event settings** tab, in the **General information** area, enter the **Event name** and **Description** of the event.



3. In the **Event configuration** area, enable the **Event run time** option and enter the runtime in seconds (at least 7 seconds are recommended).

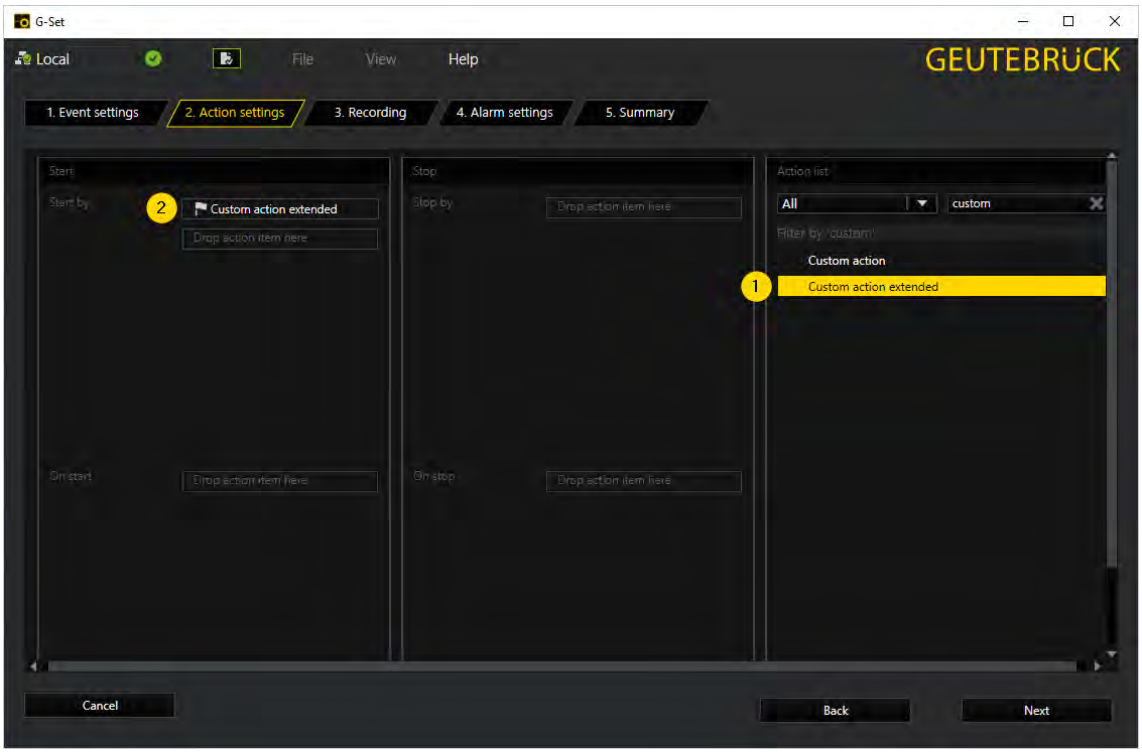


4. Enter the time range of the **Event prehistory** in seconds (at least 3 seconds are recommended).
5. Enable the **Link prehistory range to event** option.
6. On the **Actions settings** tab, select the **Custom action extended** or the **VCA Alarm** action from the **Action list** (1).

   The action to select depends on the protocol type for sending alarms that you have selected in Perimeter+ (see **G-Core**):

   - **PERIMETER+**: Select the **VCA Alarm** action.
   - **G-CORE GENERIC**: Select the **Custom action extended** action.

7. Drag and drop the action in the **Start by** field in the **Start** area (2).



8. Click on the action to open the dialog window of the action.

   For the **Custom action extended** enter the following parameters:

   - text A: Name of the Perimeter+ unit (see **Installation**)
   - text B: Name of the camera defined in Perimeter+ (see **Add a Camera**)

     IMPORTANT: The specified camera name must be identical to the camera name in Perimeter+.
     The camera name must not contain spaces when sending alarms to G-Core using the action interface, because Perimeter+ suppresses the spaces.

   - text C: Name of the detection rule defined in Perimeter+ (see **General Data**)

   To ensure the correct integration with Perimeter+, the parameters specified must be identical to those configured in the Perimeter+ unit.

Note that you need to create at least one event in G-Core for each detection rule defined in the Perimeter+ unit, so that administrators in G-Core are able to handle each Perimeter+ detection separately.

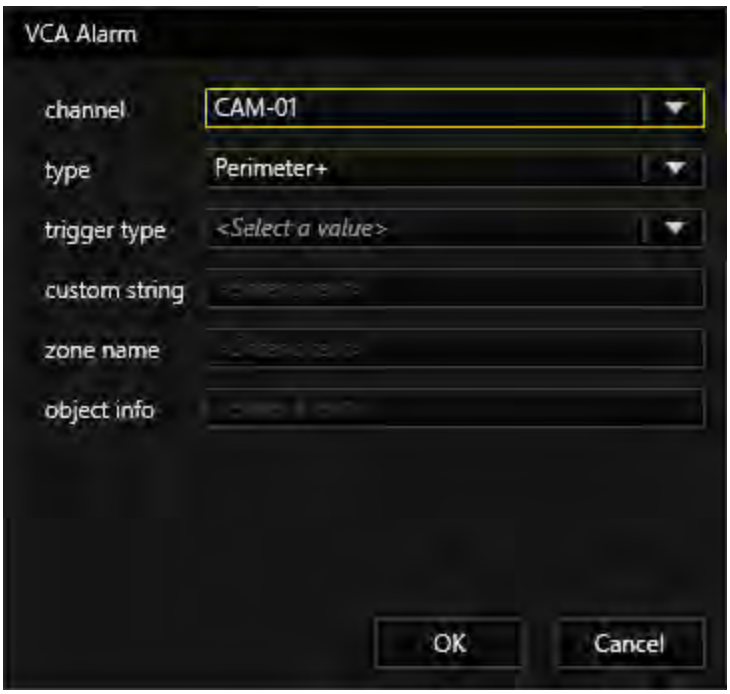
For the VCA Alarm enter the following parameters:

- channel: Select the media channel of the selected rule.

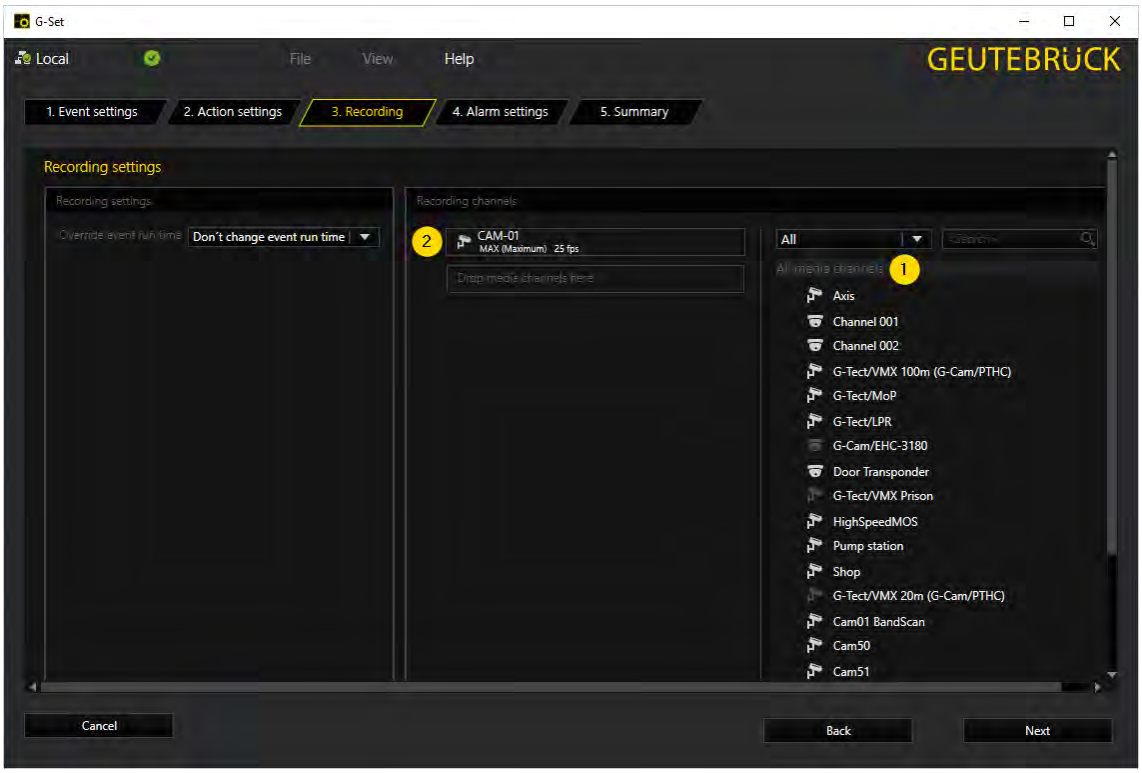
> **IMPORTANT:** The specified camera name must be identical to the camera name in Perimeter+.
> The camera name must not contain spaces when sending alarms to G-Core using the action interface, because Perimeter+ suppresses the spaces.

- type: Select Perimeter+.

> **IMPORTANT:** If you use the Perimeter+ version 202.1, select the type **unspecified** or no type at all. This version cannot process the **Perimeter+** type and does not trigger any alarms otherwise.



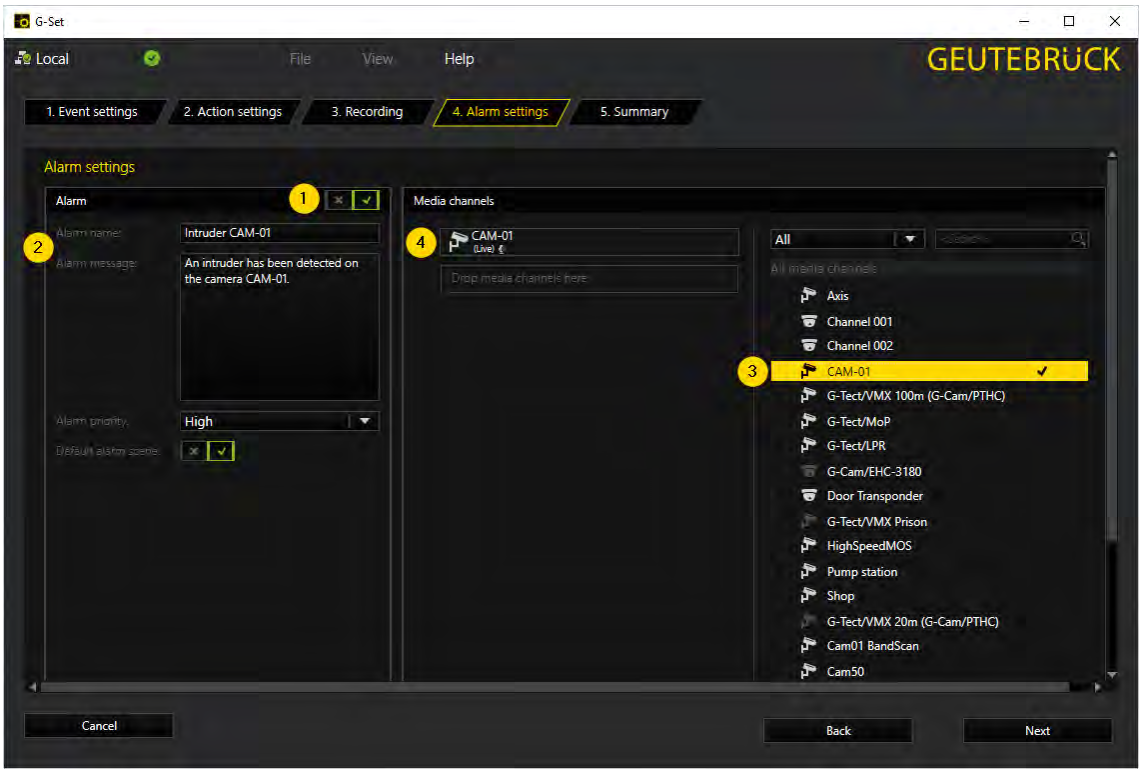
9. On the Recording settings tab, select the media channel of the selected rule from the All media channels list (1).
10. Drag and drop the media channel in the field in the Recording channels area (2).



11. On the **Alarm settings** tab, enable the **Alarm** option (1).
12. In the **Alarm** area, enter the alarm settings (2):

Setting	Description
Alarm name	Enter the name of the alarm.
Alarm message	Enter the message of the alarm.
Alarm priority	Select the priority of the alarm.
Default alarm scene	Enable this option to assign the default alarm scene to the alarm.

13. Select the media channel you want to activate when the alarm is active from the **All media channels** list (3).
14. Drag and drop the media channel in the field in the **Media channels** area (4).



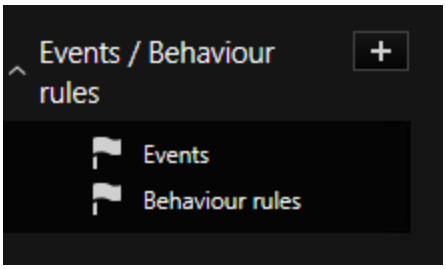
15. On the **Summary** tab, check your settings and click the **Save & Finish** button.

16. Click the icon in the menu bar to send all changes to the server.

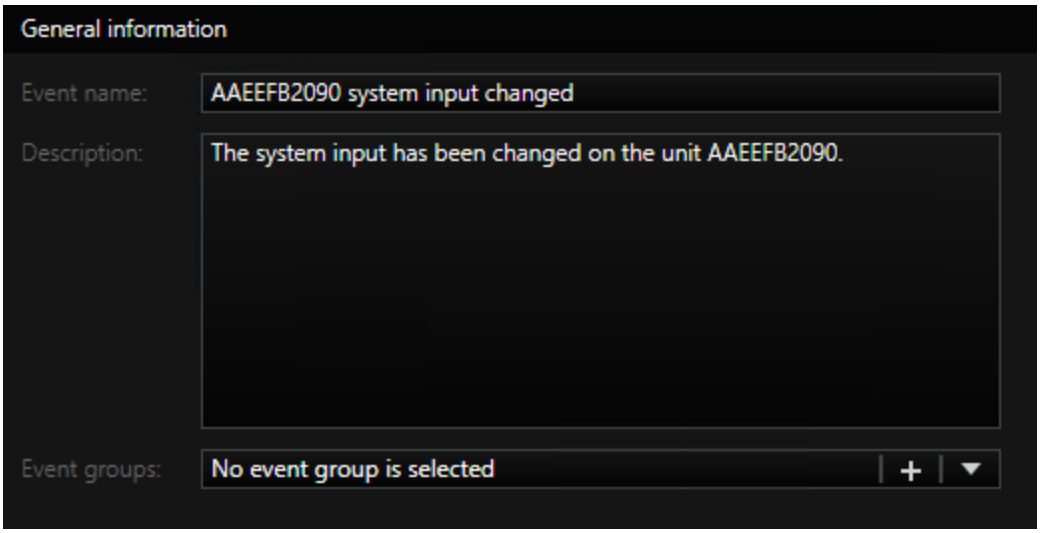
Add Perimeter+ Technical Alarms

How to add Perimeter+ technical alarms in G-Core:

1. In the **Events / Behaviour rules** sidebar item, click the **+** icon, to open the Event/Alarm wizard.



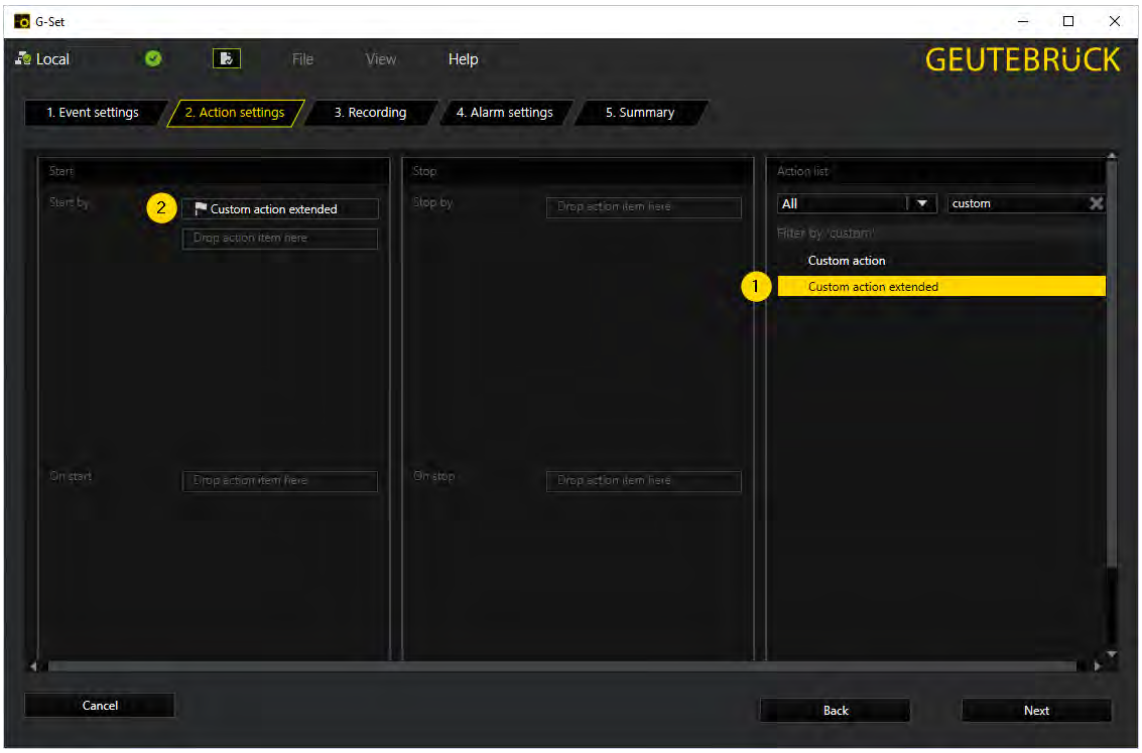
2. On the **Event settings** tab, in the **General information** area, enter the **Event name** and **Description** of the event.



3. In the **Event configuration** area, enable the **Event run time** option and enter one second as the runtime.

4. On the **Action settings** tab, select the **Custom action extended** action from the **Action list** 1.

5. Drag and drop the action in the **Start by** field in the **Start** area 2.



6. Click on the action to open the dialog window of the action and enter the following parameters:

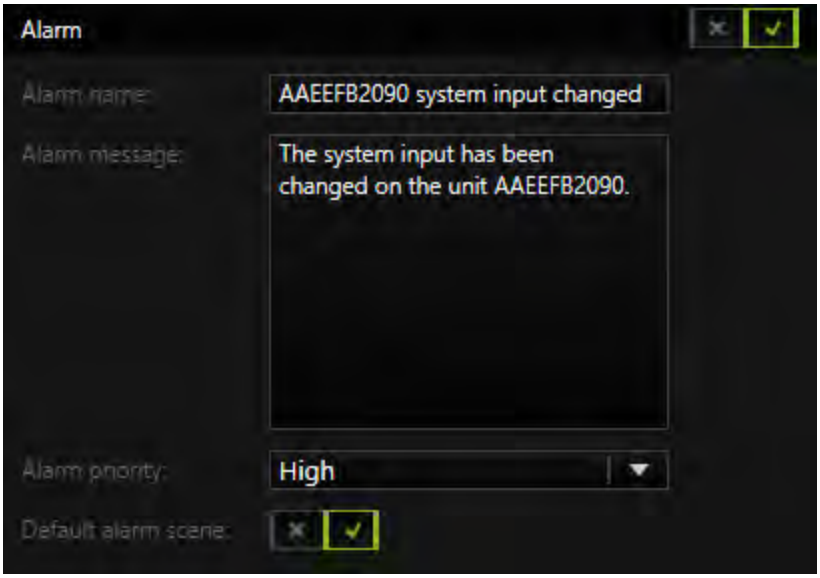
   - text A: Name of the Perimeter+ unit (see **Installation**)
   - text B: Enter "system.input.changed" as name of the detection rule (see **General Data**)

   To ensure the correct integration with Perimeter+, the unit name and rule name must be identical to those configured in the Perimeter+ unit.

7. On the **Recording settings** tab, do not make any changes and click **Next**.
8. On the Alarm settings tab, enable the **Alarm** option.
9. In the **Alarm** area, enter the alarm settings:

Setting	Description
Alarm name	Enter the name of the alarm.

Setting	Description
Alarm message	Enter the message of the alarm.
Alarm priority	Select the priority of the alarm.
Default alarm scene	Enable this option to assign the default alarm scene to the alarm.



10. Do not add any media channels from the **All media channels** list as this specific alarm is not associated with any camera.
11. On the Summary tab, check your settings and click the **Save & Finish** button.
12. Click the icon in the menu bar to send all changes to the server.

G-Core Configuration in Perimeter+

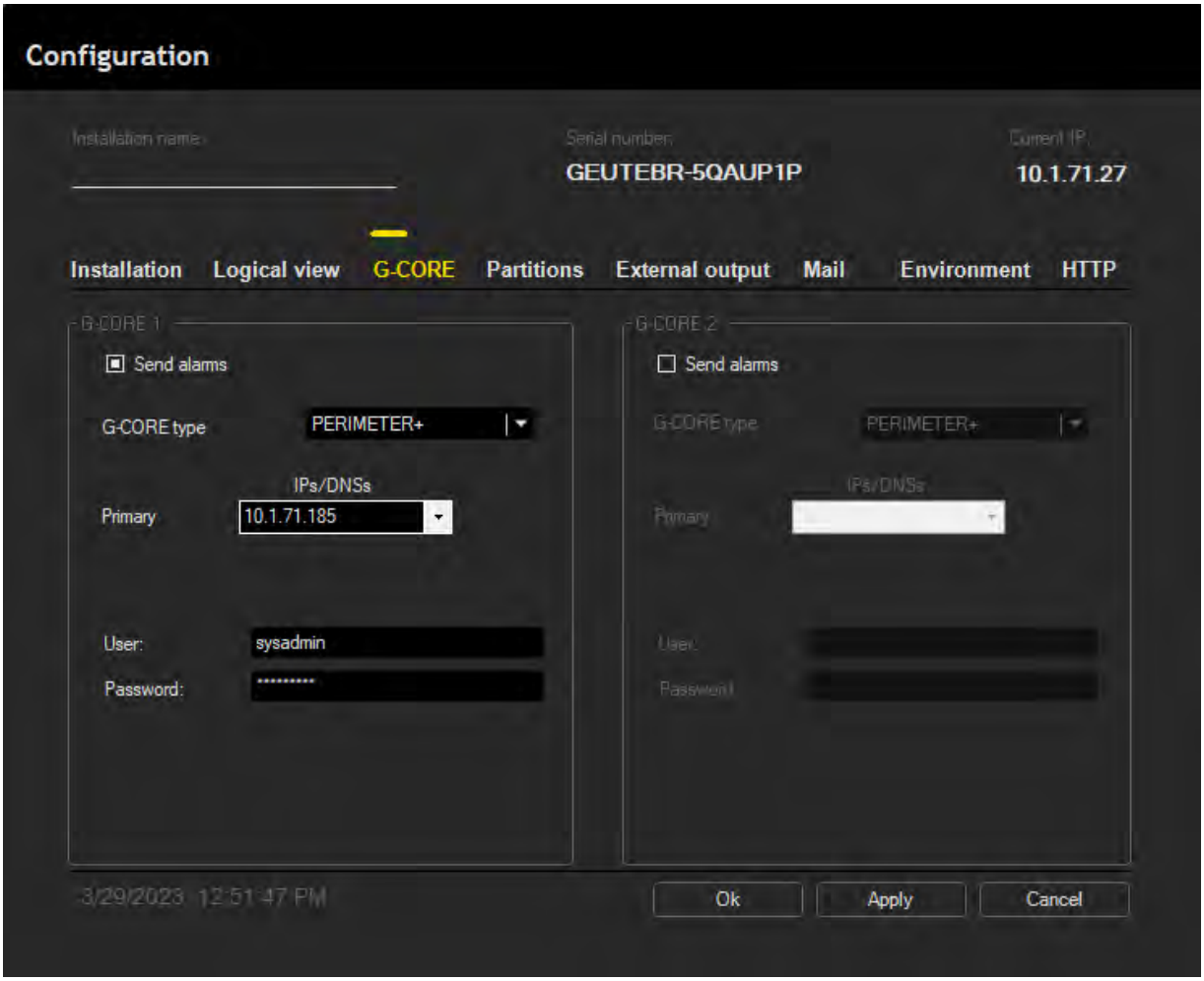
Perimeter+ video analysis units can be configured to send alarms or events to G-Core.

How to configure G-Core in Perimeter+:

1. Click the **Configuration** icon in the system overview window and enter your username and password.
2. Click the **G-Core** tab.

3. Enable the **Send alarms** option.
4. Select the **G-CORE type**:
   - **PERIMETER+**: "VCA Alarm" actions are sent.
   - **G-CORE GENERIC**: "Custom Action Extended" actions are sent.
5. Enter the IP address of the G-Core server in the **Primary** field. Domain names are also accepted.
6. Enter the **User** of the G-Core server.
7. Enter the **Password** of the G-Core server.

For more information about the G-Core configuration in Perimeter+ see G-Core.

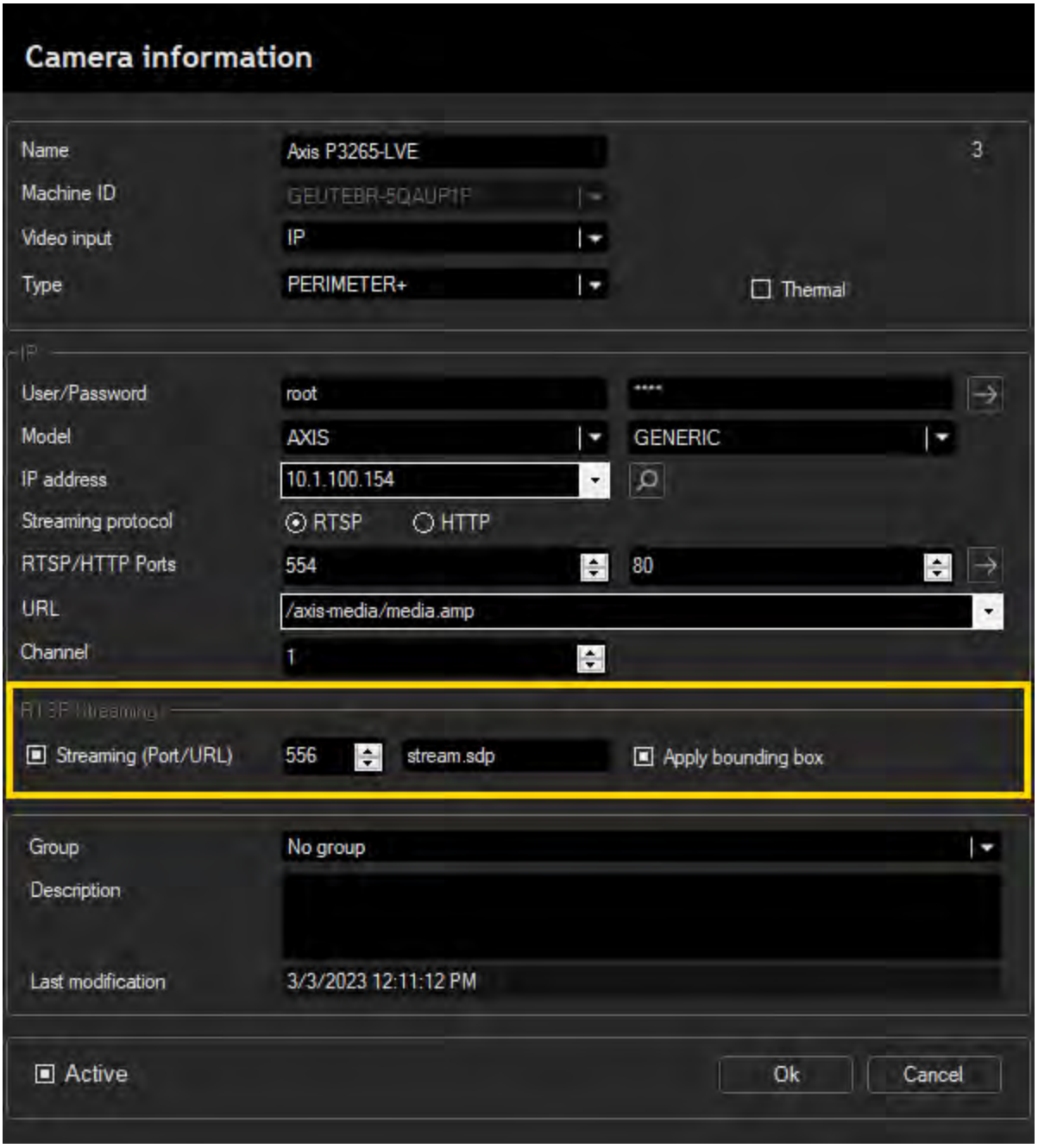


Enable RTSP Streaming for recording in G-Core:

Before you can add Perimeter+ streams in G-Core, you must enable the RTSP streaming feature for all desired Perimeter+ streams in Perimeter+.

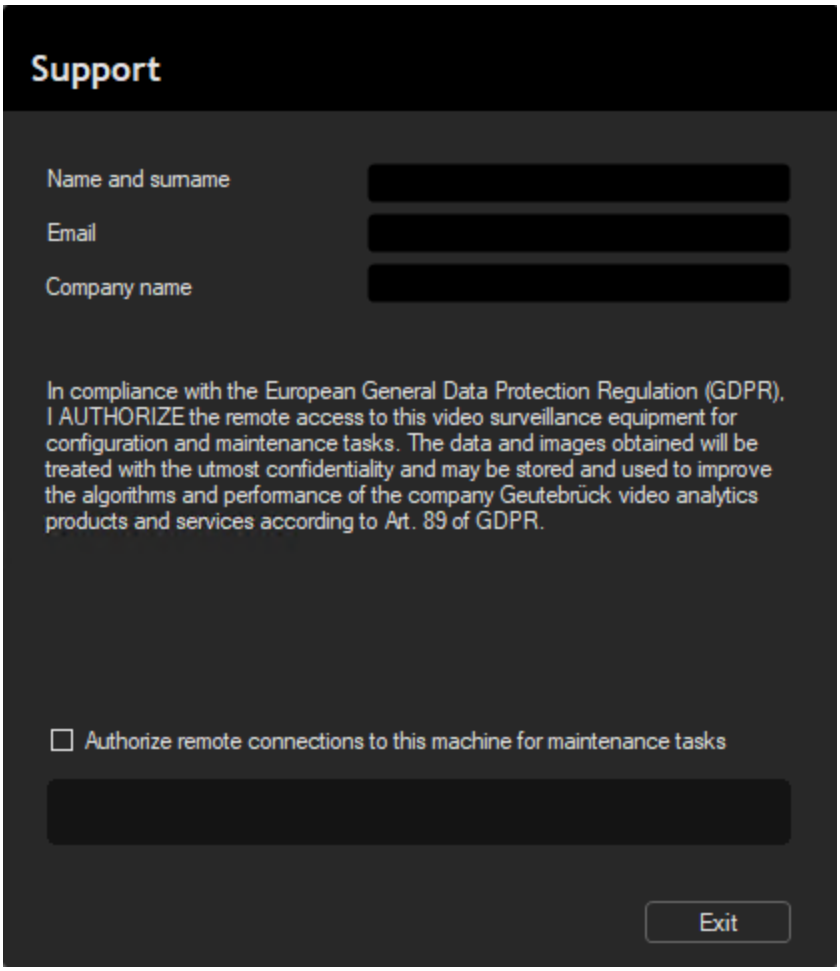
1. Click the **Cameras** icon in the system overview and enter your username and password.
2. Click the **Menu** button and select **Cameras**.
3. In the **Cameras** window, click the **Add** button or select a camera and click the **Modify** button in the **Cameras** section. The **Camera information** dialog window opens (see **Add a Camera**).
4. Enable the **RTSP Streaming** option for each camera to receive and record streams directly in G-Core from Perimeter+ (see **RTSP Streaming**).

Recording Perimeter+ streams is an advanced and optional feature that allows you to receive and record live feeds from Perimeter+ units. The Perimeter+ streams contain a detection frame around the detected object.


Camera information
Name
Axis P3265-LVE
3
Machine ID
GEUTEBR-5QAUP1F
Video input
IP
Type
PERIMETER+
Thermal
IP
User/Password
root
Model
AXIS
GENERIC
IP address
10.1.100.154
Streaming protocol
RTSP
HTTP
RTSP/HTTP Ports
554
80
URL
/axis-media/media.amp
Channel
1
RTSP Streaming
Streaming (Port/URL)
556
stream.sdp
Apply bounding box
Group
No group
Description
Last modification
3/3/2023 12:11:12 PM
Active
Ok
Cancel

Support

How to open this dialog window:
Click the Support icon in the system overview window and enter your username and password.



To authorize remote access to the unit for support and maintenance, click **Authorize remote connections to this machine for maintenance tasks** and provide your support team with the nine-digit code that appears on the screen.

Remote access with TeamViewer may not be available in the Perimeter+ version if it is uninstalled in the factory image.

Shutdown

How to open this dialog window:
Click the Shutdown icon in the system overview window and enter your username and password.

A menu appears with three different options:

Name	Description
Restart	Select this option to automatically shut down and restart the server.
Shutdown	Select this option to shut down the unit. It will not be active again until the device is manually started.
Cancel	Closes these options and returns to the system overview window.

If you click the key combination `Ctrl` + `Shift` + `D`, the following menu appears instead:

Name	Description
Open Explorer	Select this option to open the windows explorer.
Stop Watchdog	Select this option to stop the Perimeter+ application.
End Explorer	Select this option to close the windows explorer.

Technical alterations reserved.

GEUTEBRÜCK GmbH
Im Nassen 7-9 | D-53578 Windhagen
Tel. +49 (0)2645 137-0 | Fax-999
info@geutebrueck.com

www.geutebrueck.com