
# Mirasys Admin Guide V9.7 (English)

# Table of Contents

System Administration

# 1 Overview of This Guide

This guide is intended for those who set up a Mirasys system.
It shows how to add servers to the system and change their settings, add user accounts and user profiles, and monitor the system.

Please see AI guides for Mirasys LPR, FR, LM, Easy LPR, and VCA guide.

# 2 Technical Support

For technical support and warranty issues, please contact the system supplier.

# 3 What is the Mirasys VMS software?

Mirasys software is a distributed digital video management system (VMS or DVMS) for video and audio surveillance applications.
The software can monitor real-time and recorded video, audio and text data and control PTZ cameras, I/O devices, and IP cameras.
The software supports systems consisting of analogue or digital surveillance cameras, supporting the creation of analogue, digital or hybrid (consisting of both analogue and digital) surveillance systems.
A centralized surveillance system domain can consist of up to 150 local or remote VMS Servers.
Mirasys software is sold separately and part of Mirasys video management systems consisting of both the software and the VMS Server hardware.
Please contact your Mirasys supplier for information on Mirasys software or hardware.

## 3.1 What does a System Contain?

The Mirasys system consists of these components:

- 1-150 VMS Servers
    - **Master Server** (dedicated server – recommended -, one of the video recording VMS Servers, or the only server in a single-server, non-networked environment)
    - **VMS Server** (“recording servers” if the system consists of multiple servers)
- Client applications:
    - Mirasys System Manager
    - Mirasys Spotter
    - Mirasys Spotter Web
    - Mirasys Spotter Mobile

## 3.2 VMS Servers

The VMS servers record video and audio from multiple cameras and audio channels and write the data to a storage device.
You can access a VMS Server locally or over a network using the System Manager and Spotter programs and monitor server functionality through the Spotter Diagnostics plugin.
A server is a computer with storage, the Windows operating system, and the installed VMS software with required drivers.

Several devices can be connected to a VMS Server:

- PTZ (dome) cameras and keyboards
- External devices, such as sensors, to the digital inputs
- External devices, such as doors, lights, and gates, connected to digital outputs
- Special integrated devices like radar, IoT device or 3rd party system
- Storage or backup unit (NAS, SAN, or RAID, for example)

## 3.3 Master Server

In a networked system, one of the servers must be set as the Master Server.
A Master Server is the central server of a surveillance system.
All other VMS Servers connect to it, and all client applications communicate through the Master Server.
If the system contains only one server, then that server is the Master Server.
If there is more than one server, the Master Server can be set freely.
It is recommended that the Master Server is a dedicated server for this purpose alone in a more extensive system.

**NOTE:** Master Servers must have *SQL Server Express 2014* or other *Microsoft SQL Server 2014* installed.

The Master Server does these things:

- It verifies the identity of all programs and users who try to log on to the system (authentication).
- It stores all system configuration data.
- It stores all user data.
- It monitors the system.
- It synchronizes the clocks on all servers.
- It generates reports.
- It stores watchdog events.
- It stores alarms.
- It stores audit trails.

## 3.4 Client Programs

System administrators use the **System Manager** program for these tasks:

- Configuring the servers.
- Adding user accounts and user profiles.
- Monitoring the system.

System operators use the **Spotter** application for:

- Monitor real-time and recorded video and audio
- Control digital I/O switches and PTZ cameras
- Export video and audio clips to local media
- Receive and handle alarm notifications
- Create video matrixes via the optional, separately sold Agile Video Matrix (AVM) software
- Use other plugins like Grafana reporting or list management

## 3.5 Network Requirements

The network requirements apply to systems where users access the servers over a network.

# 4 OS Compatibility

Mirasys VMS V9 supports the following operating systems:

| Operating System | Server with analogue camera support via capture cards | Server with only IP cameras or connected video servers (encoders) | Gateway server | System Manager application | Spotter application |
|---|---|---|---|---|---|
| Windows 10 | - | X | X | X | X |
| Windows 11 | - | X | X | X | X |
| Windows Server 2016 | - | X | X | X | X |
| Windows Server 2019 | - | X | X | X | X |
| Windows Server 2022 | - | X | X | X | X |

Make sure that the “Desktop Experience” and “Media Foundation” features is activated for Windows server operating systems.

# 5 Configuring the System

After connecting the cameras and other devices to the servers, configure the system settings and add user accounts and user profiles.

To configure the system, perform these steps:

1. Add servers to the system and configure their settings.
2. Add the correct licenses for the servers.
3. Add IP cameras and other IP devices.
4. Add user profiles.
5. Add user accounts.

***Note:*** *Install the client programs on each computer used to access the system over a network.*

*A separate "Spotter only" installer is provided.*

**Note***: After configuring the system,* ***back up system settings and all VMS Server settings*** *on the* ***System*** *tab.This way, you can restore the settings, for example, if a hard disk fails.*

# 6 Log In

This section describes how to log in and log off from System Manager.
Only system administrators or users with monitoring rights are allowed to log in to System Manager.

## 6.1 Logging in

### 6.1.1 User credentials

Default username and password

Username: Admin
Password: 0308

The default username and password should not be used even in closed networks.
Please ensure that the default username and password are not in use after installing the system.

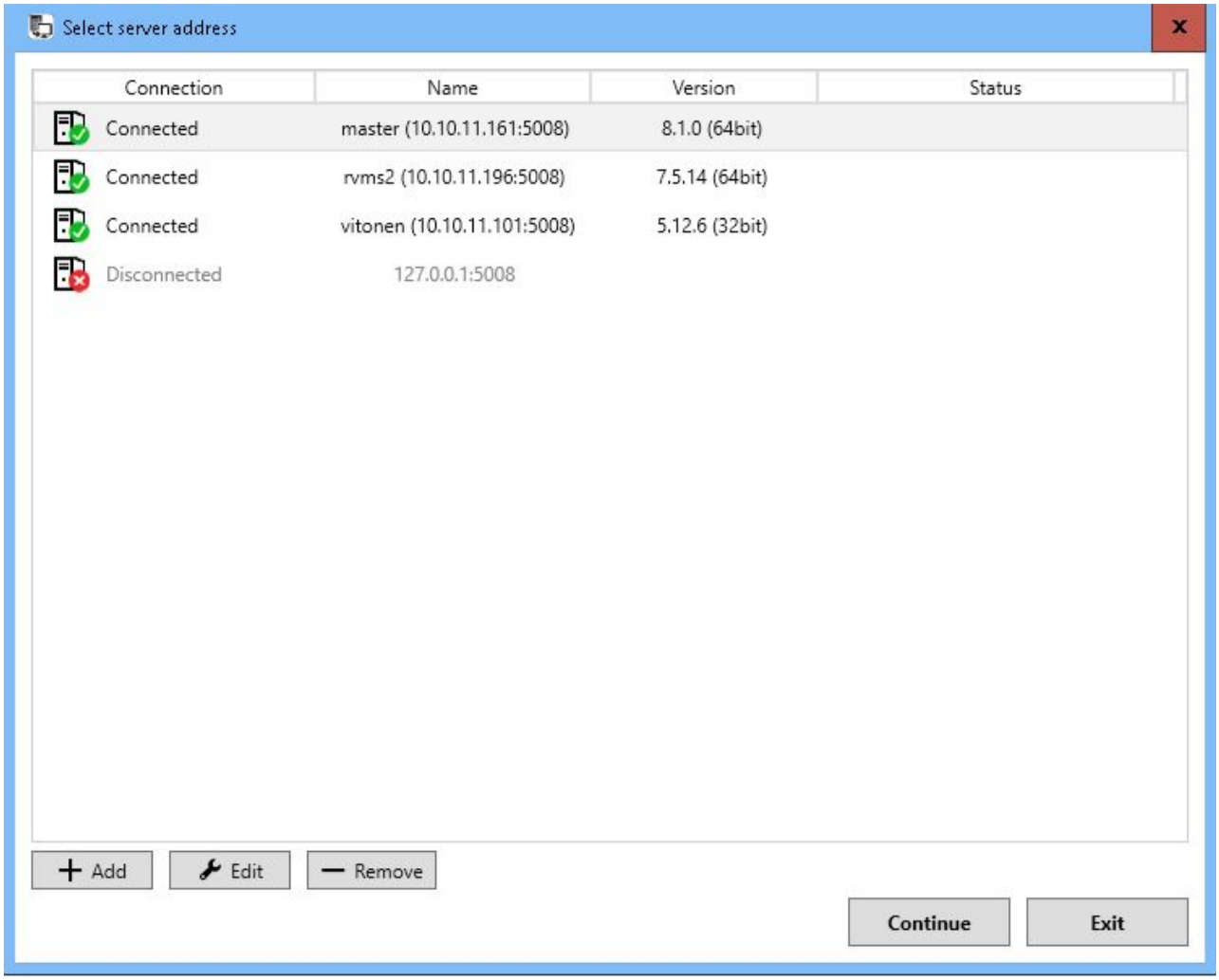
### 6.1.2 How to log in

To login to System Manager:

Do one of the following:

- Double-click the shortcut icon **System Manager** on the desktop.
- Click **Start**, point to **Programs,** and then to **DVMS**. Click **System Manager**.

In systems that have only one Master Server address configured, the System Manager login screen is shown.
In systems with multiple masters and addresses configured, or if the user presses the “Delete” key in the initial startup phase, the site selection screen is shown.
The user can add, remove or edit Master Server addresses or choose a server to log on on this screen.
After selecting a server and pressing the “Continue” button, a user is taken to the login screen.




On the login screen, type your username in the **Username** box and your password in the **Password** field.


**Note:** *The username and password are case-sensitive.*

Click **OK**. A progress bar is shown on the screen while the program loads.

**After the program starts, the user interface is shown.** To **log off** or to **change the user** click on the menu bar **File** and then **Log off. To quit** the program**:**

- On the menu bar, click **File** and then **Exit**.
- Close the application window.

**Note:** The user can only have one System Manager application running at any one time.
It is not possible to have the System Manager simultaneously connected to multiple servers.
To connect to another Master Server, exit from the current Master and choose another Master Server from the site selection screen.

## 6.2 Locking System Manager

You can manually lock the program to protect it, for example, when you go away from your desk.

To lock the program, do one of the following:

- On the menu bar, click **File** and then **Lock Program**.
- On the status bar, click **Lock program**.

To unlock the program:

- After locking the program, the login screen is shown.
    - Type the user name in the **User name** box and the password in the **Password** box.

**Note:** *The password is case sensitive.*

# 7 Management User Interface

The System Manager User interface

The System Manager User Interface contains these elements:

## 7.1 **Menu bar**.

- **File**
- **Log Off**
- **Lock Program**
- **Import**
- **Export**

## 7.2 Maintenance

**Set maintenance state on** to control the failover transition state off.

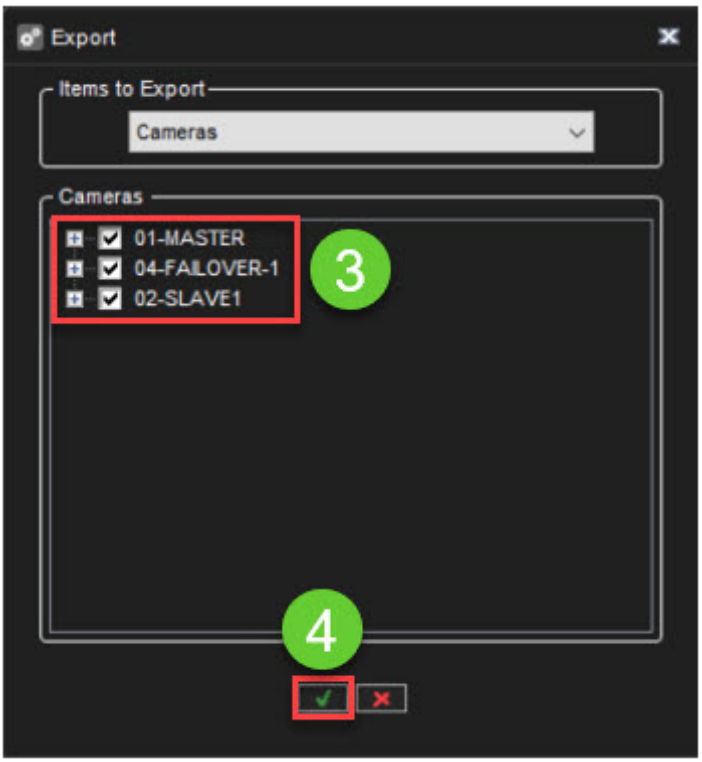
## 7.3 **Help**

**About**

to see information about the program version.
and then **Help Topics** to use the online guide.

## 7.4 Exporting system camera information to the CSV

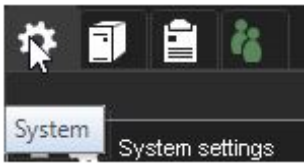
1. Click **File**
2. Click **Export**
3. Select the servers
4. Click **OK**




1. Select the location
2. Enter the name of the export
3. Click **OK**


Export To
Local Disk D:\ (Materials1)
5
D:\
Asetukset
dvr
testi
Select Directory
Name:
Cameras_20220505_031900.cs
6
7

# 8 System




You can edit and backup system settings on the System tab, monitor the system and examine diagnostic information about the course.
You can also change license keys for servers on this tab, such as adding more camera channels and installing a new IP camera, metadata, and client plugin drivers.
Also, you can configure the software watchdog.

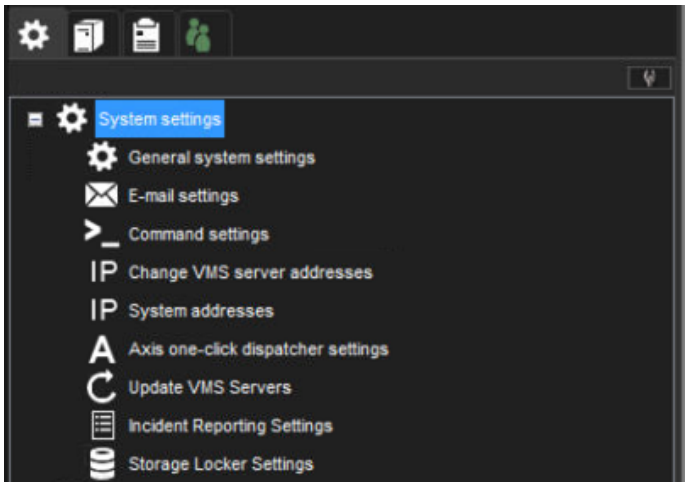
The tab contains these tools:

- System settings
- General system settings
- E-mail settings
- Command settings
- Change VMS server addresses
- System addresses
- Update VMS Servers
- Backup
- Export logs
- Backup settings
- Restore settings
- Monitoring
- SM Server diagnostics
- Local recorder diagnostics
- Licenses
- Watchdog
- Watchdog settings
- Watchdog logs
- Add-ins
- Install driver
- Install metadata driver
- Install client driver
- Install client plugin

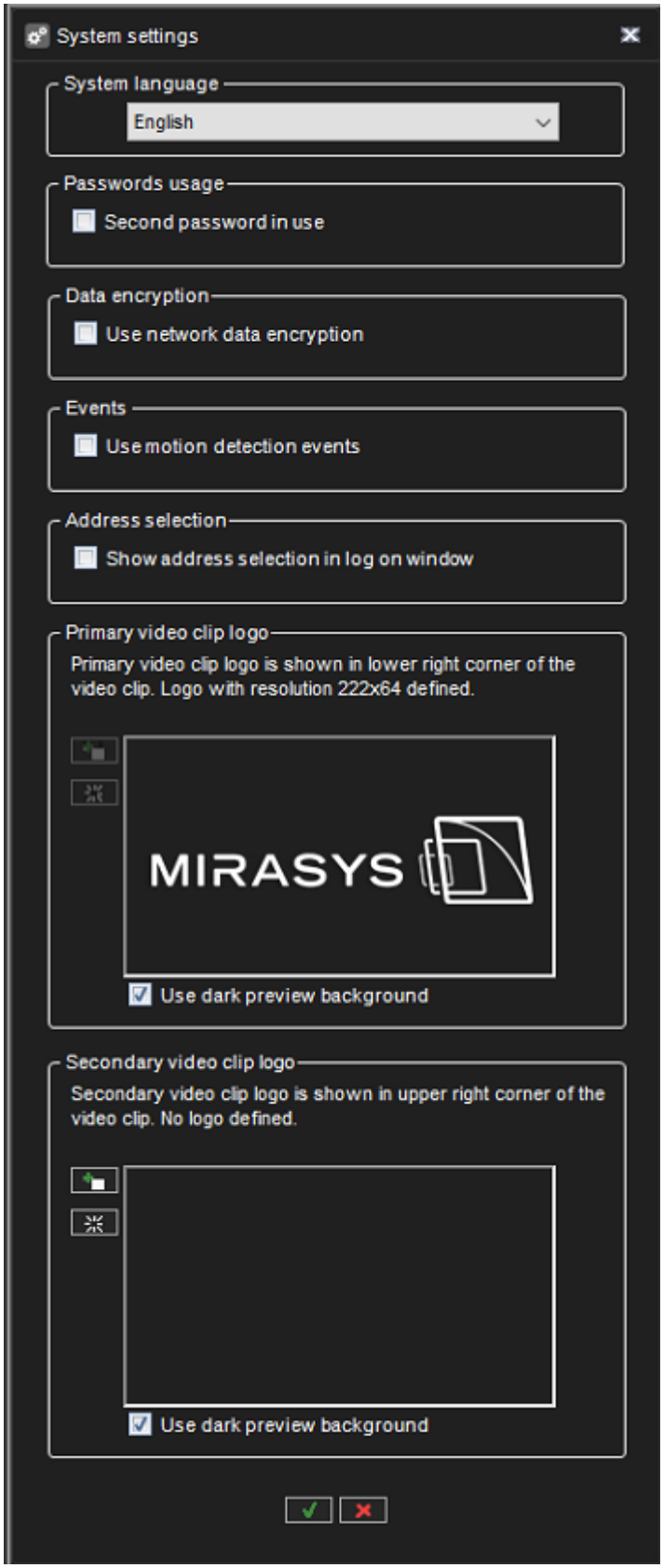
To open a tool, do one of the following:

- Click the tool and then click Edit
- Double-click the tool.
- Drag the tool from the **System** tab to the workspace

## 8.1 System settings



### 8.1.1 General System Settings


System settings
System language
English
Passwords usage
Second password in use
Data encryption
Use network data encryption
Events
Use motion detection events
Address selection
Show address selection in log on window
Primary video clip logo
Primary video clip logo is shown in lower right corner of the video clip. Logo with resolution 222x64 defined.
MIRASYS
Use dark preview background
Secondary video clip logo
Secondary video clip logo is shown in upper right corner of the video clip. No logo defined.
Use dark preview background

#### 8.1.1.1 In this section, you can control the following:

- System language
- The password usage

It is possible to configure the system to require two separate passwords for all users.
This is done by activating the “Second password in use” option in general system settings.
When this mode is selected, all users are required to give two passwords.
The default second password is empty. This feature allows limiting that no single person can review videos alone.
If one password is known to one person and the other password is known to another person, both persons must be present when reviewing videos.

- Data encryption
- Events(the setting for sending motion information to clients)
- Address selection
- Primary video clip logo(Logos that are attached to exported video clips)
- Secondary video clip logo(Logos that are attached to exported video clips)

### 8.1.2 E-Mail Settings


You can specify e-mail addresses and groups which can be defined to receive reports about events specified in the Software Watchdog.

### 8.1.2.1 To set the e-mail notification settings:

1. On the **System** tab, open **E-mail settings**.
2. Type the sender's e-mail address into the **Sender** field. Note that some e-mail applications are configured to accept messages only from valid e-mail addresses.
3. Type the name of the outgoing mail server into the **Outgoing mail (SMTP)** field. The specified server will be used for sending all e-mail notifications.
4. Type the login information and port for the SMTP server into the appropriate fields.
5. Set the events for which notifications will be sent as instructed in the Software Watchdog.

***Note:*** Emails are not sent to all system email recipients.

The administrator can control which Watchdog events and alarms to which email recipients or groups the email is sent.

### 8.1.2.2 To add new e-mail addresses to the system:

1. On the **System** tab, open **E-mail settings**.
2. Click **Add new e-mail address** to add a new address.

3. Type the recipient's name and e-mail address into the **Name** and **Address** fields.
4. Click **OK**.

#### 8.1.2.2.1 To add a new e-mail group to the system:

1. On the **System** tab, open **E-mail settings**.
2. Click **Add new e-mail address** to add a new address.

3. Type the group name
4. Click **OK**.

### 8.1.2.3 To add one or more recipients to a group:

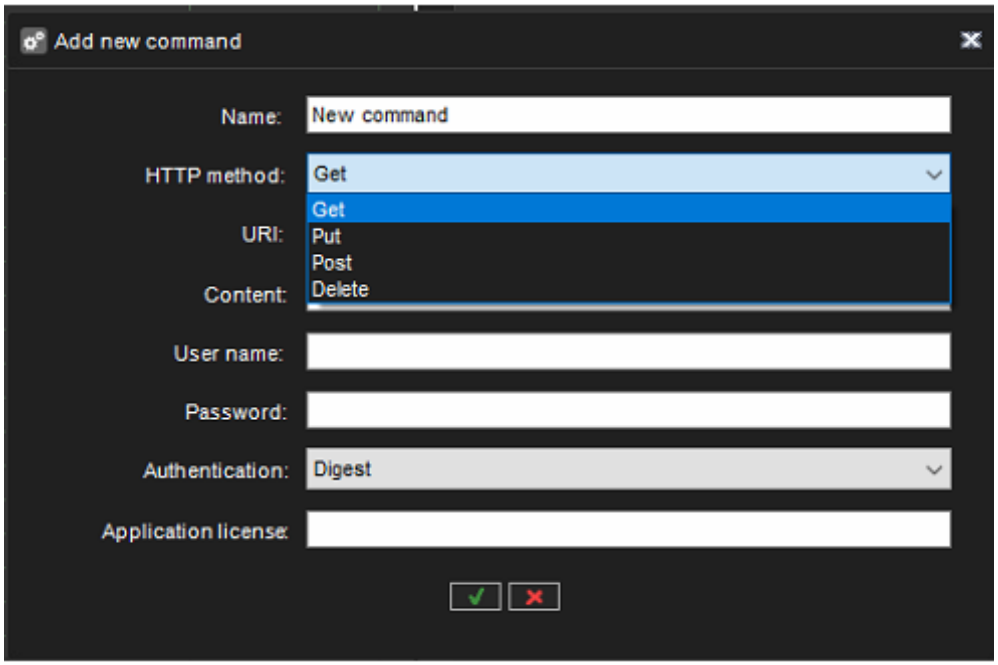
1. Highlight the desired group on the group list
2. Highlight the desired recipient(s) in the recipient list
3. Click on the arrow to add the selected recipients to the selected group

### 8.1.2.4 Other available actions:

| | |
|---|---|
|  | Editing email names, addresses, and group names and removing persons from groups is possible with the edit buttons. |
|  | Persons can be removed from groups with the arrow. |
|  | Persons and groups can be removed with the button. |
|  | Test email can be sent with a button to a selected email address using the settings defined in the email settings dialogue. |

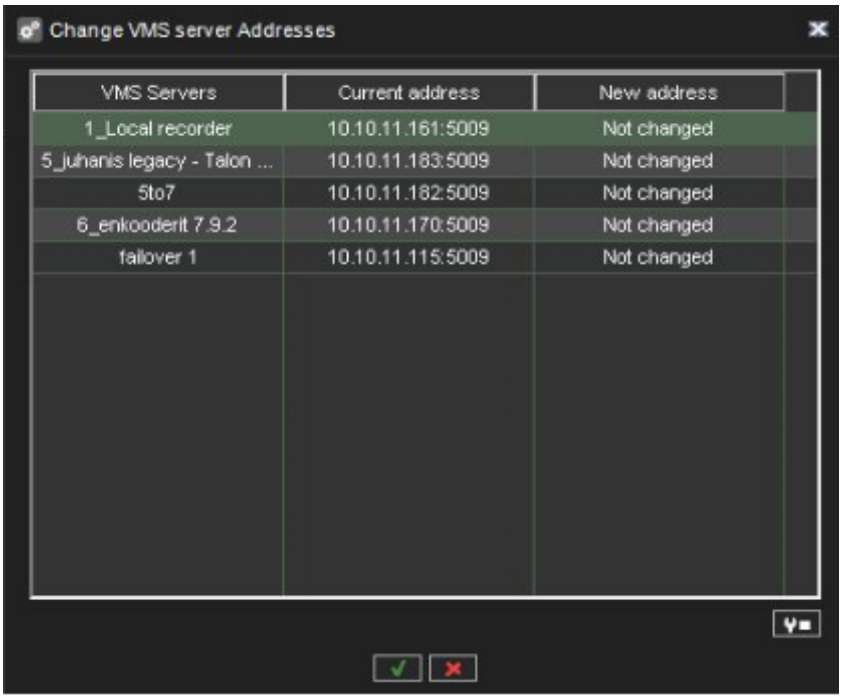
## 8.1.3 Command Settings

Command settings are used for HTTP command sending



### 8.1.4 Change VMS Server Addresses

If the IP address or DNS name of a server changes, you can define the new address/name through the **Change VMS Server addresses** tool.



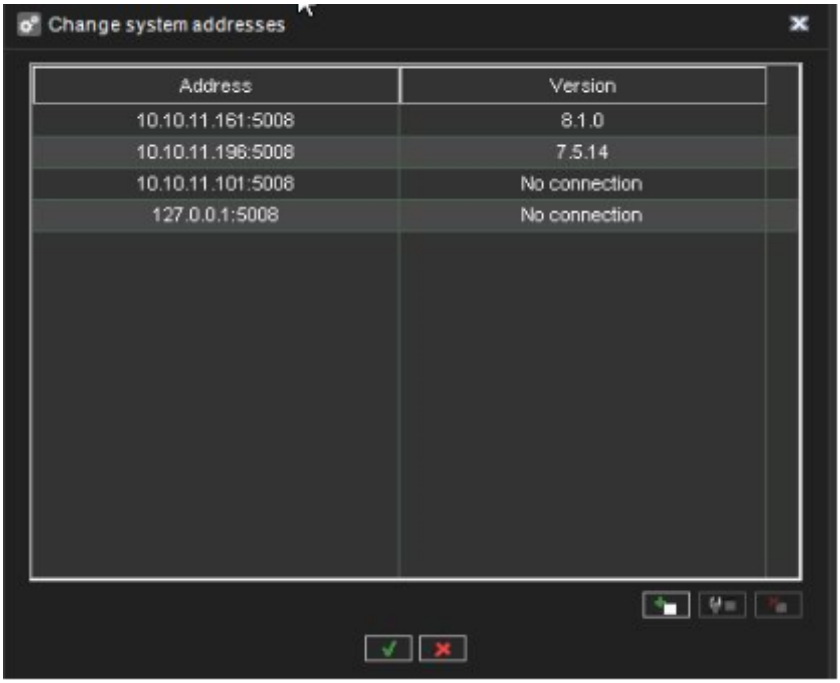

To change a server's IP address or DNS name:

1. On the **System** tab, open **Change VMS Server addresses**.
2. Click on the name of the server with the changed IP address.
3. Click **Change VMS Server address**
   
4. Type the new IP address or DNS name of the server into the **New VMS Server address** field.
5. Click **OK**.

### 8.1.5 System Addresses

A Master Server is the central server of a surveillance system.

All other VMS Servers connect to it, and all client applications communicate through the Master Server. During the login phase, the client applications can select the Master Server they will connect to.



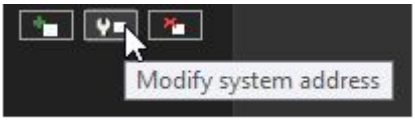

You can define multiple Master Server addresses that the client applications can connect to.
The addresses can be provided as IP addresses (e.g. *http://195.168.0.1*) or DNS names (e.g. http://www.example.com ).

**Note:** *Users can connect to any of the defined Master Server addresses provided they have a compatible username and password for the Master Server.*

### 8.1.5.1 To add a Master Server address:

1. On the **System** tab, open **System addresses**
2. Click **Add new system address**.
   
3. Type the new system address (either IP address or DNS name) to the **Add** field.
4. Click **OK**.

### 8.1.5.2 To edit a Master Server address:

1. On the **System** tab, open **System addresses**.
2. Click on the Master Server address with the changed IP address.
   
   
3. Click Modify system address .

4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

#### 8.1.5.3 To remove a Master Server address:

1. On the **System** tab, open **System addresses**.
2. Click on the Master Server address you want to remove.
3. Click **Remove system address**.


### 8.1.6 Axis one-click dispatcher settings

#### 8.1.6.1 Installation steps

Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

##### 8.1.6.1.1 Important things:

1. Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

Important things:

- setup provider certificate authority:

Directory in which the CA should be set up [default: ca]: (by default ca)

Passphrase for the CA key (DO NOT FORGET THIS!) [default: N/A]: pAs_sw!ord (some password)

Valid time, in days [default: 7300]: 100 (any number)

##### 8.1.6.1.1.1 Issue a server certificate:

Path to the CA directory [default: ca]: (as above)

Passphrase for the CA key [default: N/A]: pAs_sw!ord (as above)

Subject Alternative Names (separated by comma) [default: N/A]: 172.17.102.56 (very important!!! Should be equal IP address of O3C server)

Valid time, in days [default: 398]: 100 (as above)

Result:

Concatenated server certificate and key saved to: ca/issued/stserver_EA363E5578E696E7.pem

Register O3C server as service in Windows SCM: there is needed the Power Shell tool for Windows! And for install call:

.\setup_service.ps1 add -c C:\o3c-server\o3c-server.conf

#### 8.1.6.1.2 Configure o3c-server.conf

listen_client = 172.17.102.56:80

IP and port where the server will wait for the client (the camera) connections

stserverid = test_o3c_server

Any string

cert_file = C:\o3c-server\stserver_EA363E5578E696E7.pem

issued server certificate created after command: "pkitool issue-server-cert"

provider_ca = C:\o3c-server\stserver_ca.crt

CA certificate from ca directory created after the command: "pkitool setup-provider-ca"

provider_name =

can be left blank

credentials = root:root

for device access requests

#### 8.1.6.1.3 O3C-server service

By default, the service is called Axis O3C Server in Services or O3C-server in command prompt.

1. Start the O3C-server service
2. Enable One-click technology on the camera as described in the 4.1 part of the guide.
3. Disable firewalls or add O3C-server to the exceptions
4. Register the camera as described in guide 4.2 part.
    a. http://172.17.102.56/admin/dispatch.cgi?action=register&user=adp_mirasys_100&pass=GQ41lSRbbEb4w3sorkN8&mac=B8A44F17AAFA&oak=8A22D6434817&server=172.17.102.56:80
    b. where:user=adp_mirasys_100, pass=GQ41lSRbbEb4w3sorkN8 - Mirasys credentials (Provider name and password) from Axismac=B8A44F17AAFA, oak=8A22D6434817 - MAC address and OAK key from the camera
    c. To find the MAC address using the following string in the browser: http://172.17.100.84/axis-cgi/admin/param.cgi?action=list&group=Network
    d. server=172.17.102.56:80 - as "listen_client" in o3c-server.conf
5. Check that the camera was connected to the O3C-server: call in the browser th string: http://172.17.102.56:80/admin/status.cgi 172.17.102.56 - IP address of O3C-server
6. And check that there is a comment about the connected client as follows: "id=4.b8a44f17aafa srcaddr=172.17.100.84:34148 accepted=1 v=2 rx=0 tx=0 connected=2022-01-10T12:45:40.875571Z

Total number of clients: 1"

PS: the camera tries to connect to the server every 20 seconds

1. Check that we can get options from the camera: for that, it needed to configure the proxy settings for browser -
2. Open system Internet Options
3. Select Connections tab -> Select LAN settings button -> to enable "Use a proxy server for LAN (...)" and input the proxy IP address and port. (in the current case there is a local IP address and port 80)
4. After that we can get the camera capabilities in the browser:
    a. http://b8a44f17aafa/axis-cgi/param.cgi?action=list&group=root.RemoteService where b8a44f17aafa - MAC address of the camera

#### 8.1.6.1.3.1 Filter for wireshark for Axis P1375:

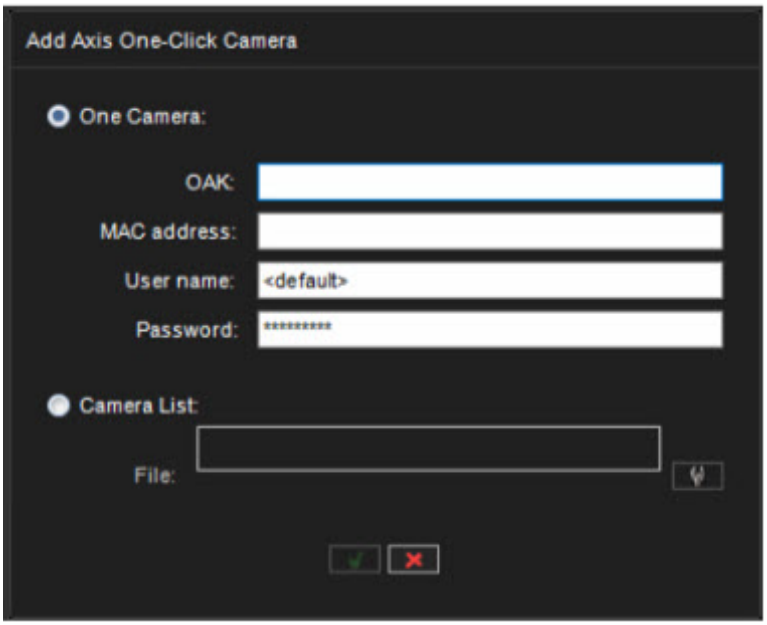
((ip.src == 172.17.100.84) && (ip.dst == 172.17.102.56)) || ((ip.src == 172.17.102.56) && (ip.dst == 172.17.100.84))

### 8.1.6.2 Add Axis One-Click Camera

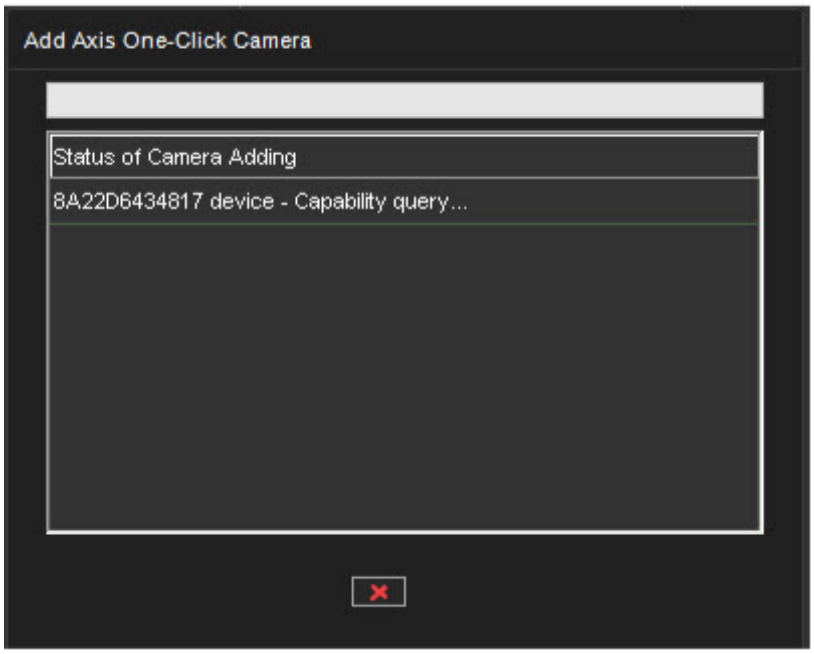
1. Open **System tab**
2. Go to **System Settings** and open **Axis one-click dispatcher settings**
3. Enter all necessary details and click **OK**


4. Open the **VMS Servers tab**
5. Click **Hardware**
6. Click **Add Axis One-Click Camera** icon


7. Enter Axis One-Click Camera details and click **OK**

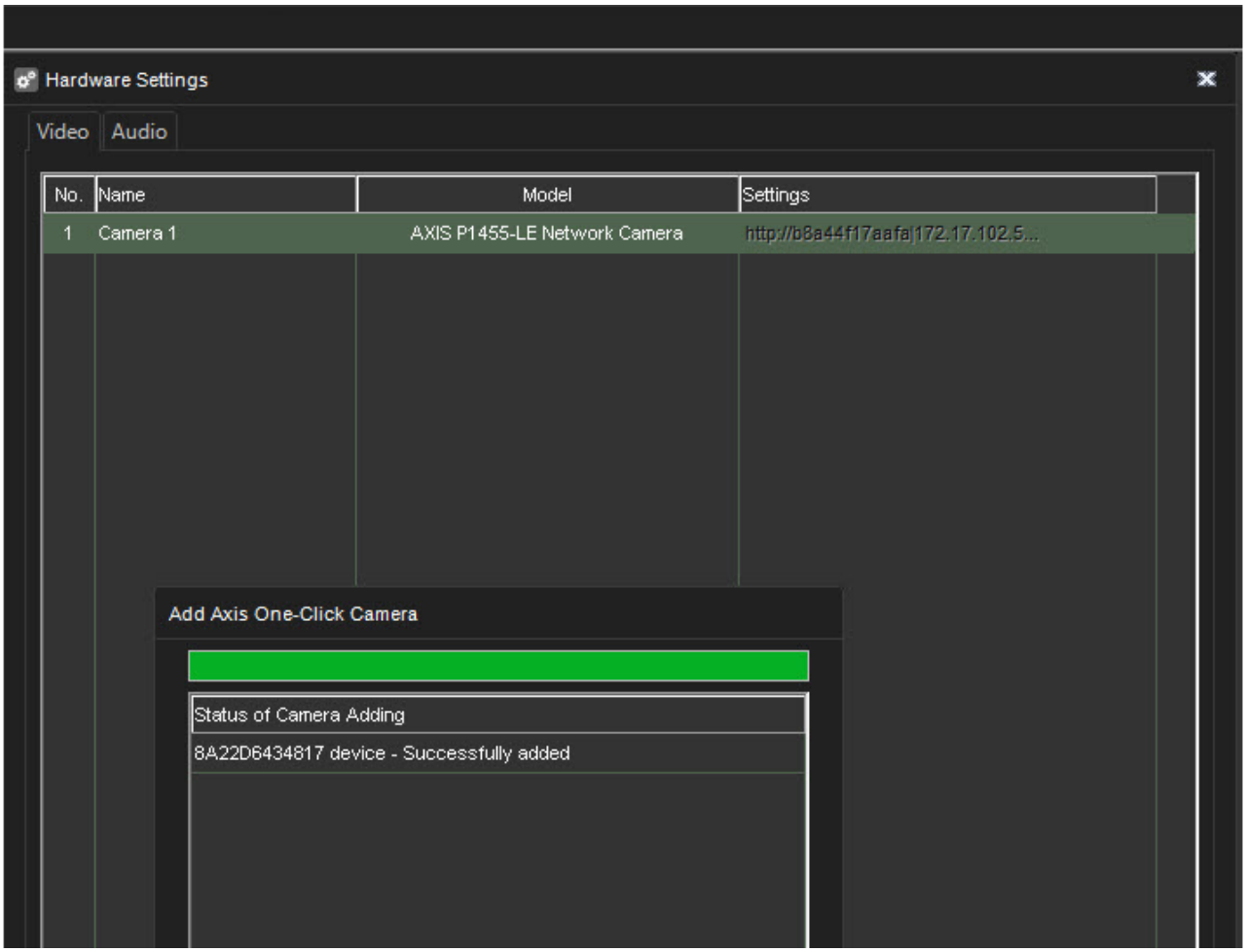


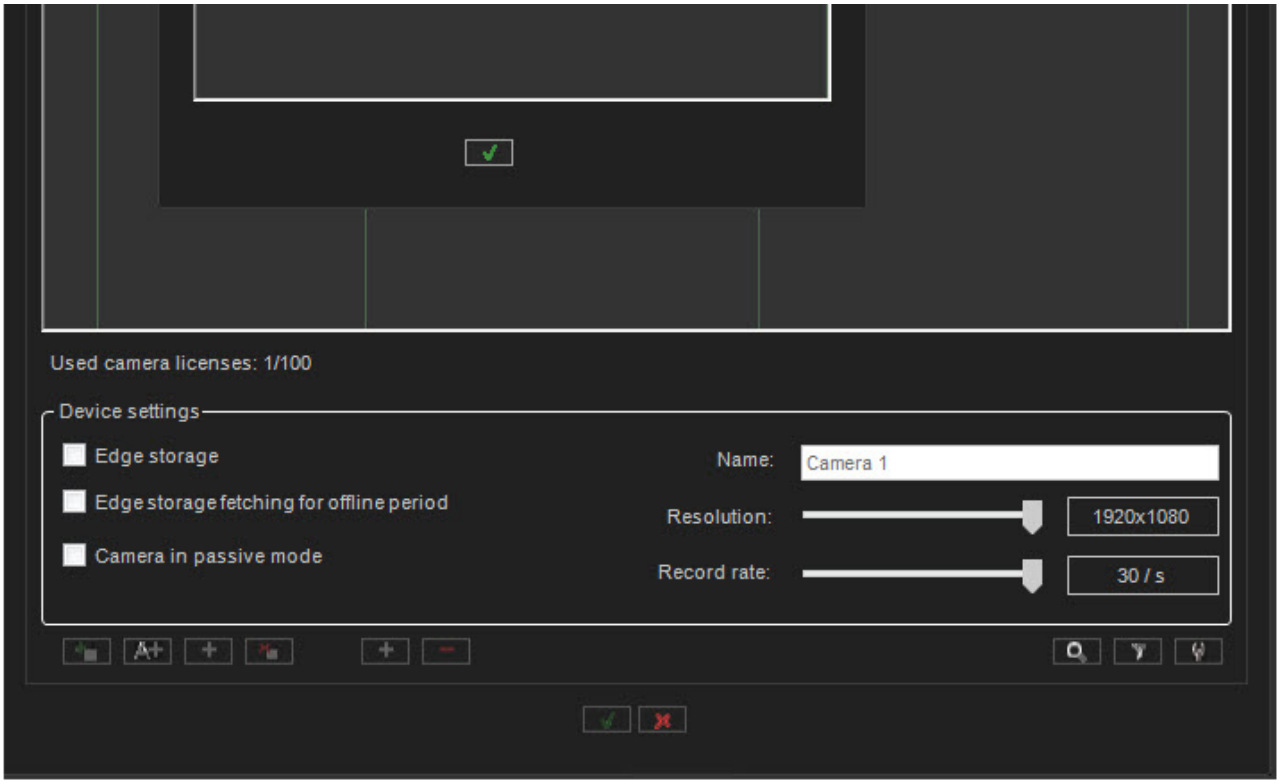

After clicking the OK, the camera query starts




When the camera query is finished, the device will be added to the hardware list

8. Click **OK** to finalize





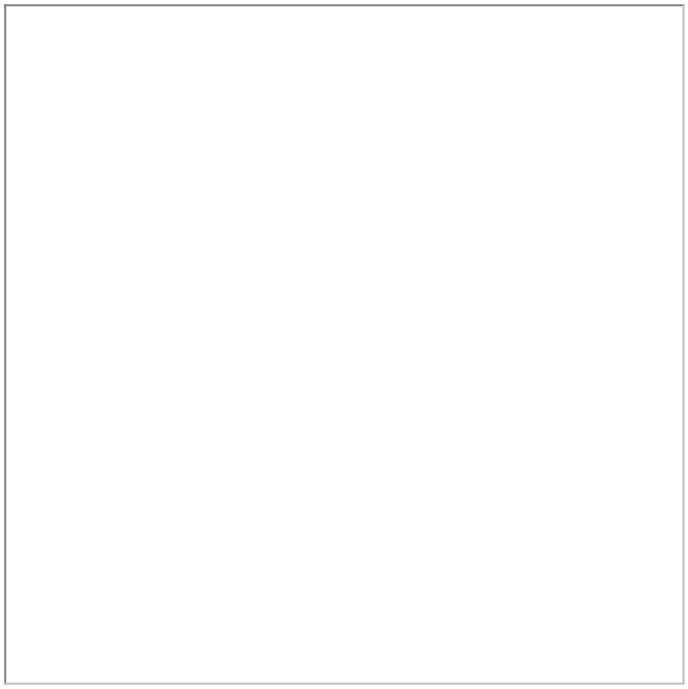

## 8.1.7 Update VMS Servers

It is possible to update all connected VMS Servers remotely via the **Update VMS Servers** –option The master server must be upgraded from the Windows **Control Panel\Programs\Programs and Features\Uninstall or change a program.**

! Please remember to set the **Maintenance state on** before upgrading.

1. Click **Maintenance**
2. Select **Set maintenance state on**
3. Select the duration of the maintenance mode

### 8.1.7.1 Updating VMS servers



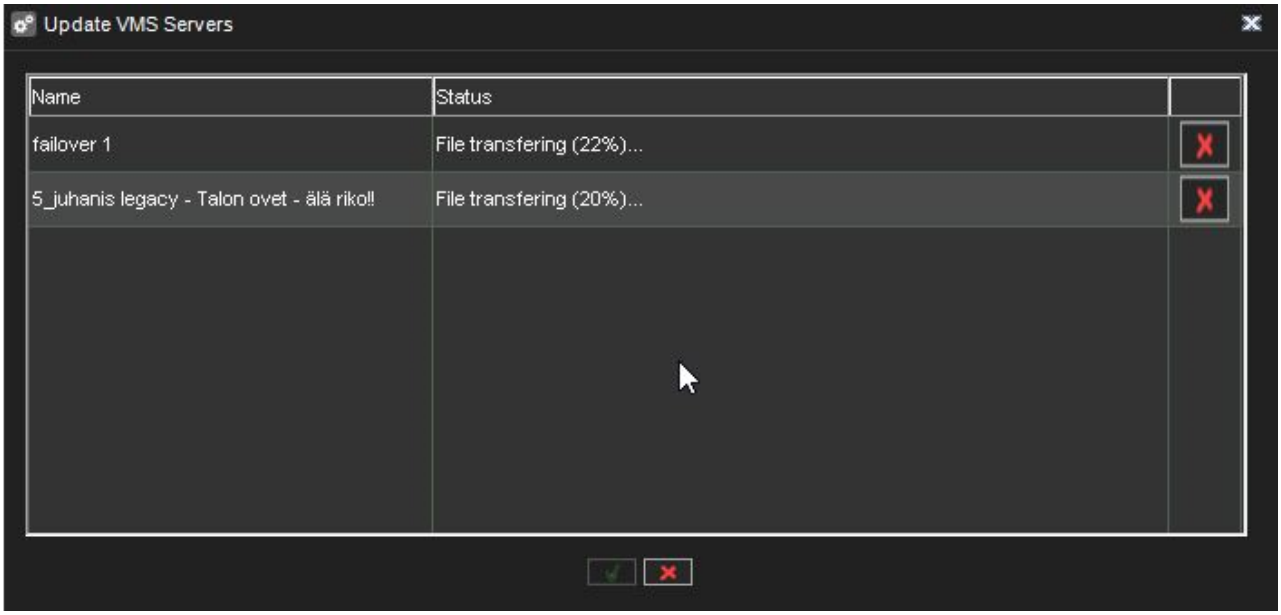
To update servers, first, select the installation file with the button:

The list is updated to show which servers can be updated with the selected installation file.

**Note:** *When performing a major version upgrade, for example, from VMS 6. x to 7. x, it is usually necessary to first upgrade the server licenses, and only after this upgrade the VMS software.The Update VMS Servers dialogue will inform the user if a license upgrade is needed before the software update.*Next, choose which servers you want to update and if you want to perform a backup before updating.

By selecting this button

you will start the update, and an update progress dialogue is shown:




This dialogue can be closed at any time without affecting the server updates.

**Notes:**

- The progress dialogue might display no status information for the installation file transfer and update progress if the network connection is slow or intermittent.
    - This is no cause for alarm; in most cases, the update will be successful, but it might take a long time (20 – 30 minutes).
    - It is recommended to prepare for the possibility to have remote access to any such servers.
- If a local server were selected to be updated, the system manager would automatically close after this dialogue is shown.
- In rare cases, some servers require system restart after remote VMS software update if the connection between the Master Server and VMS Server is not returning after the update.
    - It is recommended to monitor the connection to VMS Servers after the update.
- Since Version 7.4.3, Mirasys VMS has had support for 64-bit servers. The upgrade from 32-bit (x86) to 64-bit can be achieved precisely by installing any DVMS version.
    - After the update, the control panel of windows will show DVMS-x64 for 64-bit DVMS.

## 8.1.8 Incident Reporting Settings

From the Incident Reporting settings, the user predefines the parameters, which will be used while viewing or exporting the Incident or Daily log reports.

### 8.1.8.1 Company information

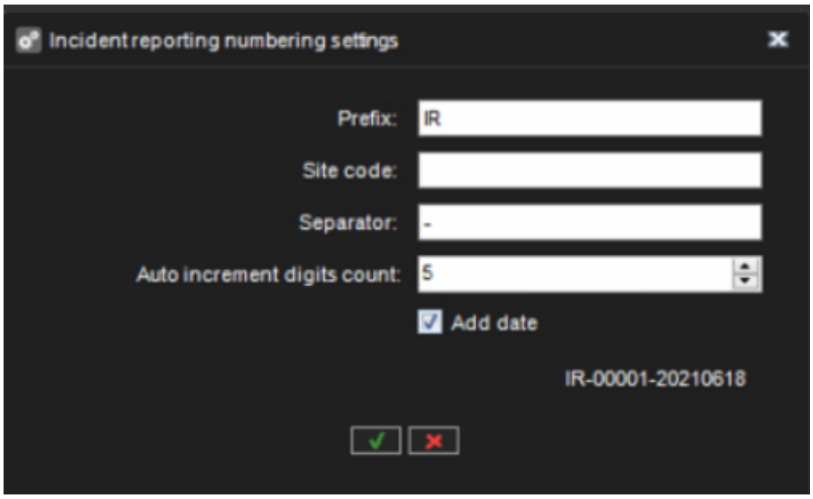
- Company name
- Company address

- Company logo

### 8.1.8.2 Reporting numbering

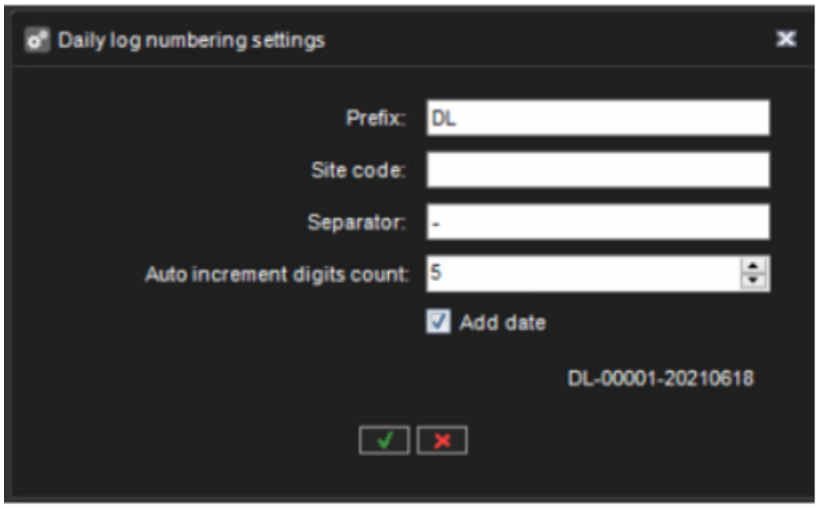
Incident Reporting numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



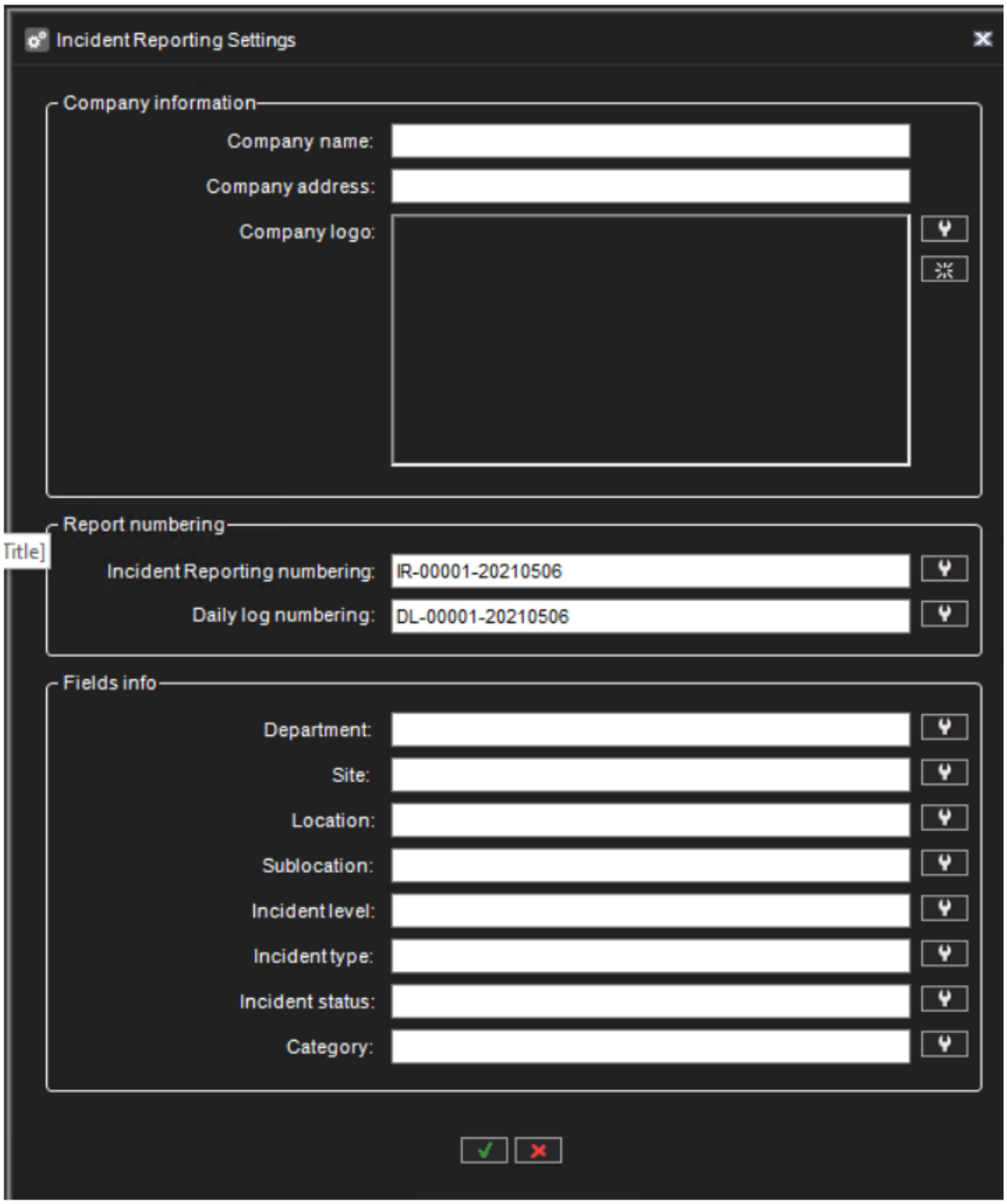

### 8.1.8.3 Daily log numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



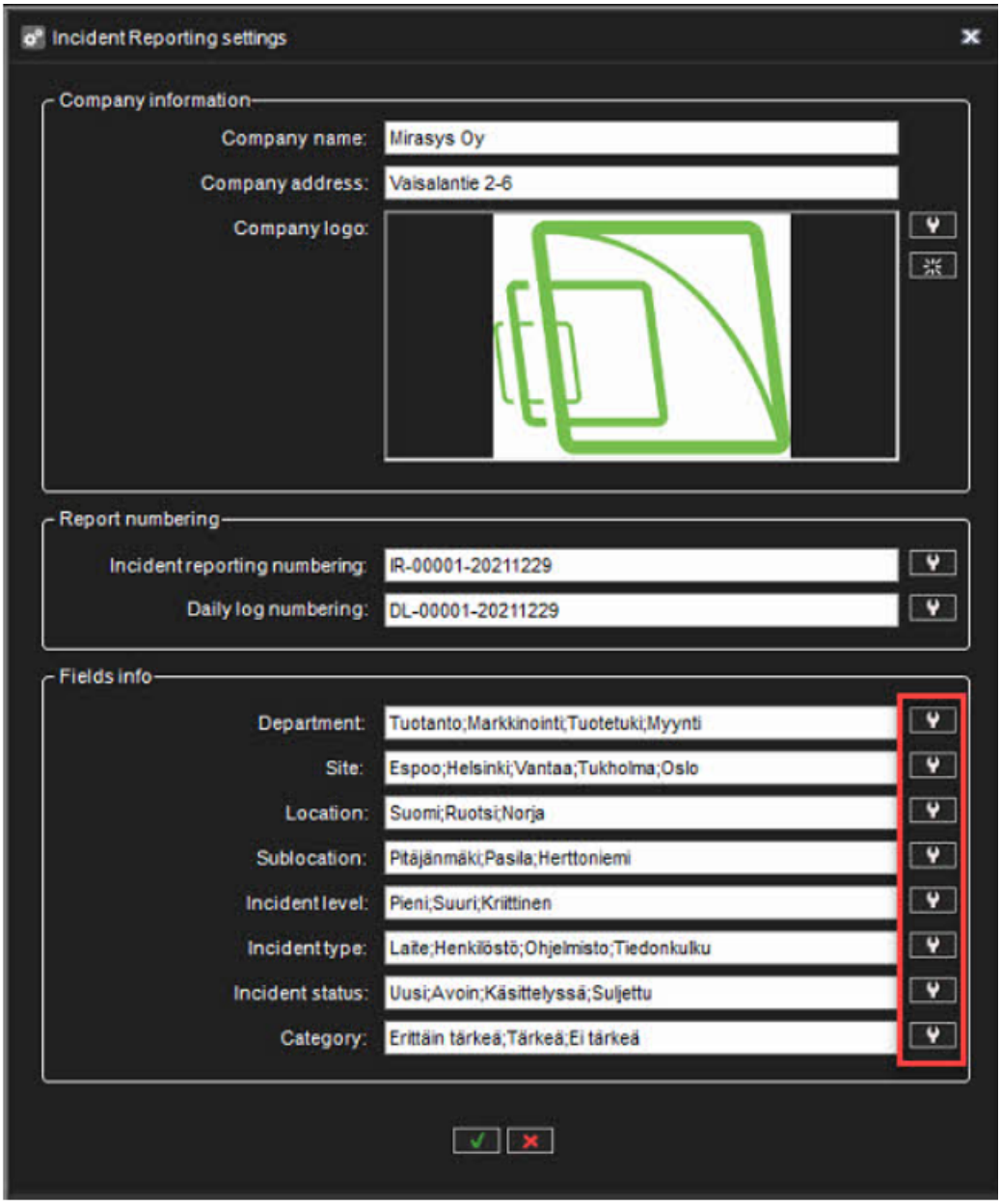
#### 8.1.8.4 Fields info

- Department
- Site
- Location
- Sublocation
- Incident level
- Incident type
- Incident status
- Category

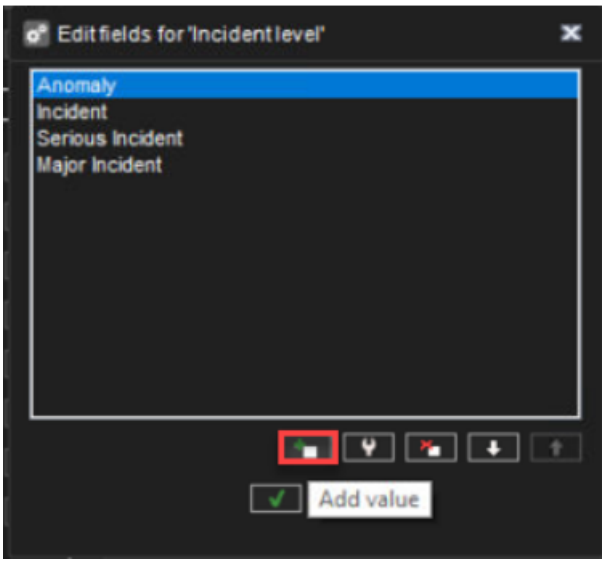



### 8.1.8.5 Add values

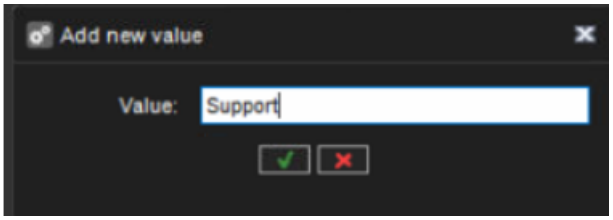
1. Select the correct field and click **Update values**



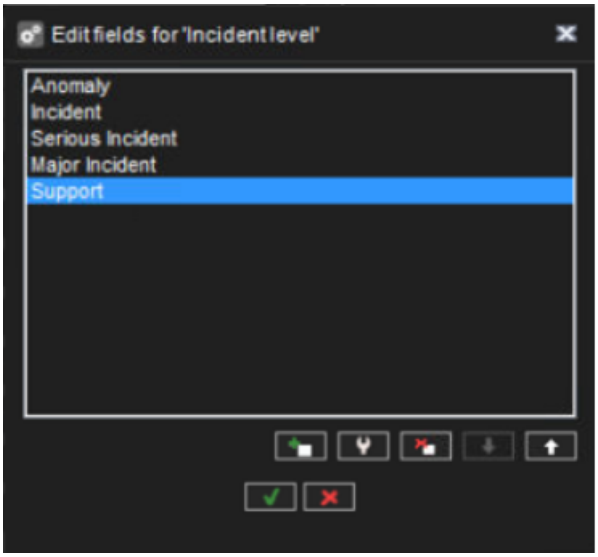

2. Click **Add value**




3. Enter the name of the value
4. Click **OK**



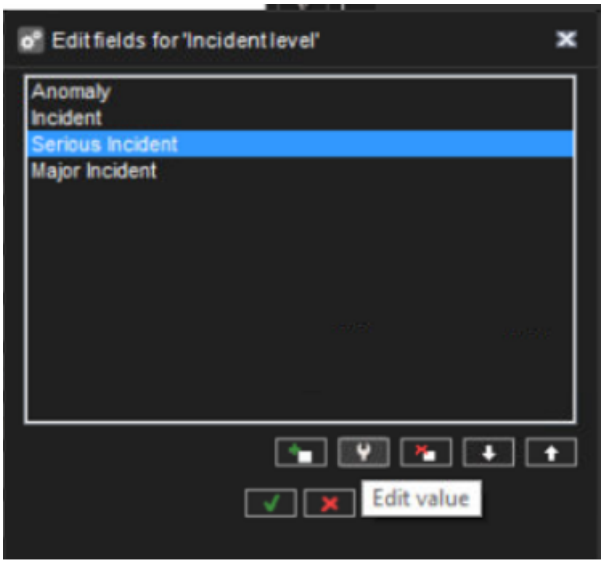

5. New added value can be seen in the list



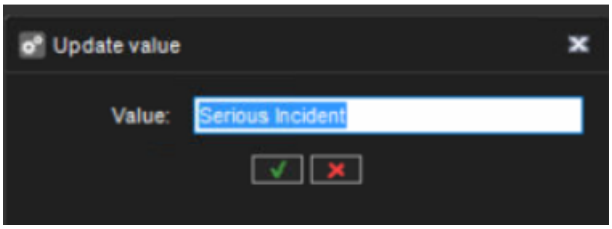

### 8.1.8.6 Edit values

1. Click icon **Update values**


2. Select a value from the list and click **Edit value**

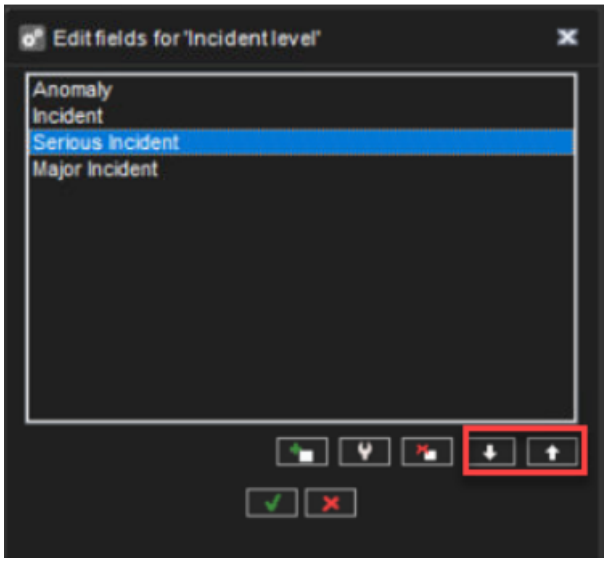



3. Enter a new value name and click **OK**




### 8.1.8.7 Changing the order of the values

1. Select the value and click arrows to set the proper order of the values.
2. Click **OK** to confirm changes



## 8.1.9 Storage Locker Settings

Storage Locker Settings contains the following values:

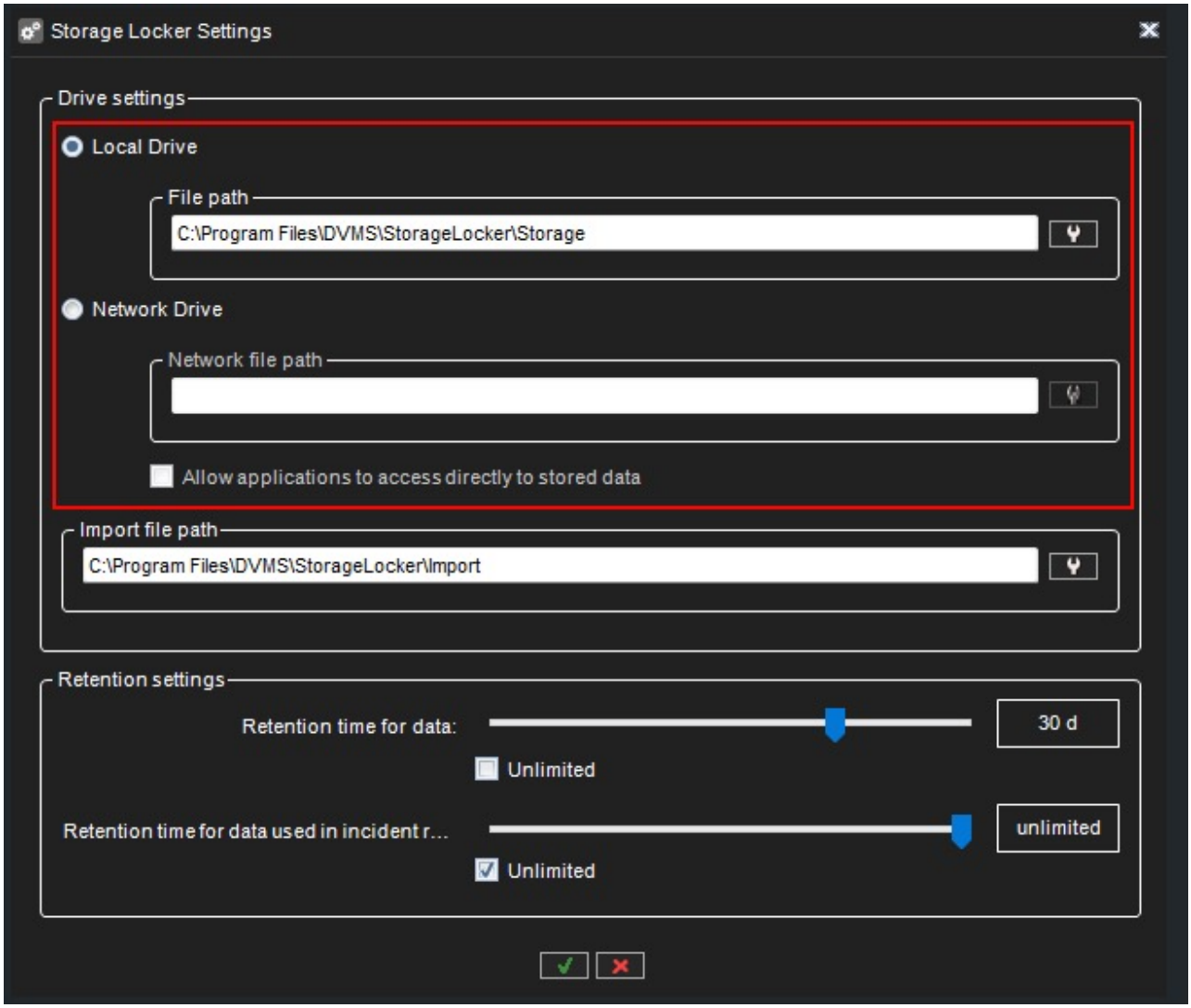
### 8.1.9.1 File path:

Defines the location of the Storage Locker file storage that can be either local or network disk. As the default location, Storage Locker file storage is located in the master server's local disk.

#### 8.1.9.1.1 Changing the file path

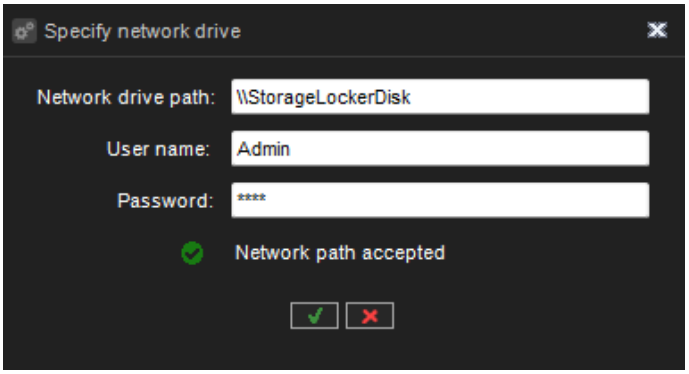
**Please note that old storage locker data is not copied to the new location**

1. Select if a local drive or network drive is used.



2. If the local drive is selected, click **Set file path for data storage.** Select a new location and click **OK.**

3. If a network drive is selected, click **Set network file path for data storage.** Specify network path, username, and password and click **OK.**

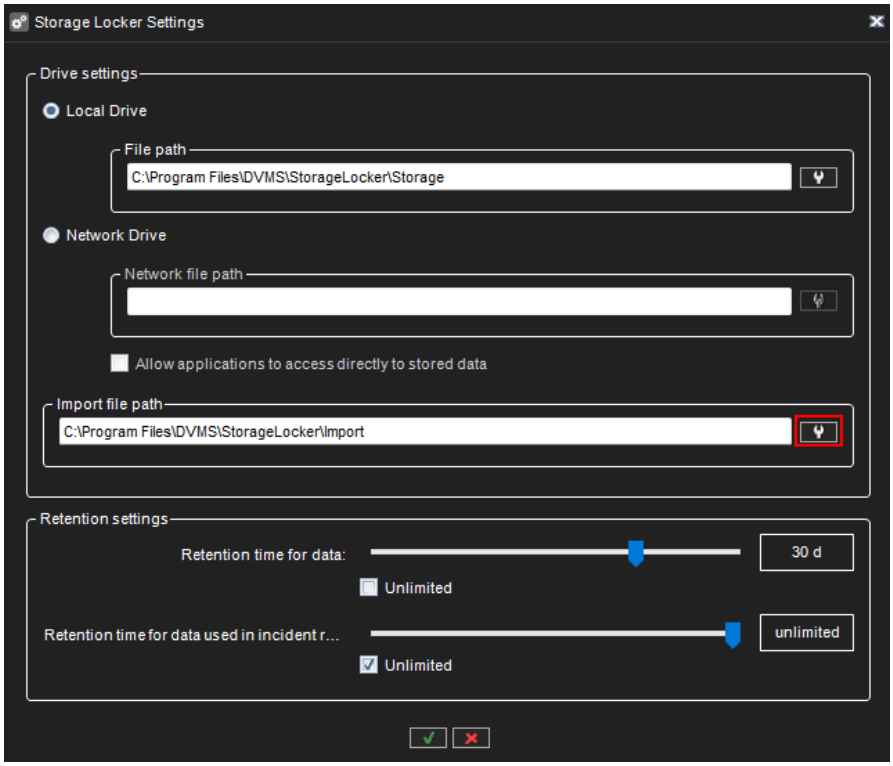



When a network drive is used for Storage Locker data storage, it is possible to allow Spotter applications directly to access saved data from the network disk by checking the option **Allow applications to access directly to stored data**.

### 8.1.9.2 Import file path:

If someone has exports that are needed to be added to the Storage locker, those exports should be placed in a folder that is defined in Storage locker settings as "Import file path". How to use:

- Each import data need to be in its own folder, files that will be placed into the import folder directly will be ignored
- Each import folder can have several subfolders
- Images and clips can be placed in one folder, Storage locker will import them one by one
- SEF archives should be in their own folder and not mixed with other data (like images, clips, etc.)
- Import data should be copied all at once if something should be added - it should be copied with its own folder, files added to existing folders are not supported (those files will not be processed)

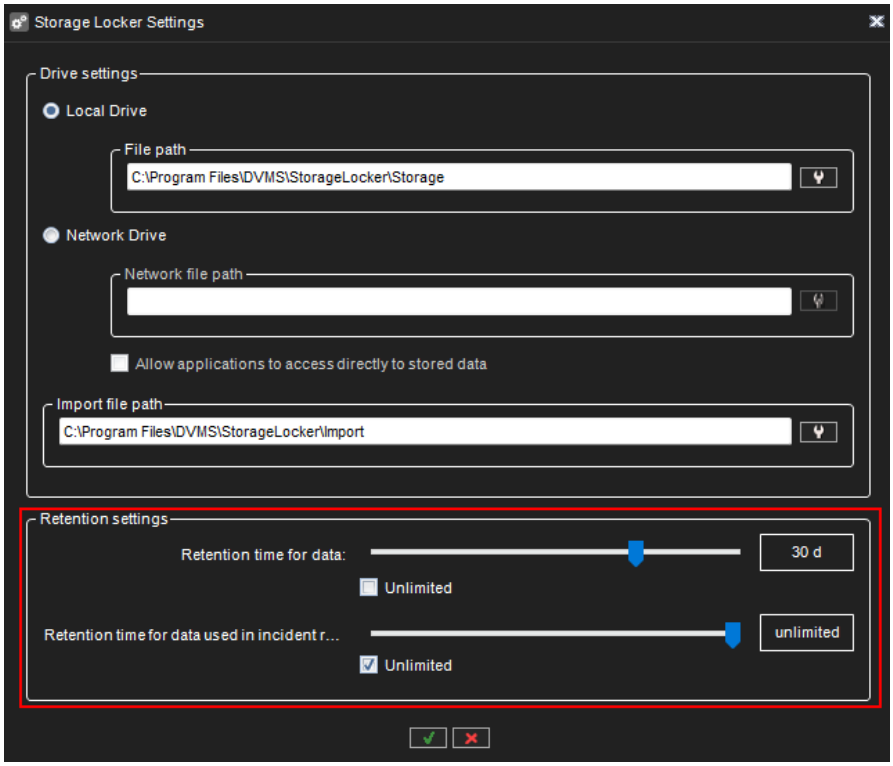



### 8.1.9.3 The retention time for data

The retention time for data sets defines how long Storage Locker retains data, which are not used in any Incident Report

### 8.1.9.4 The retention time for data used in the incident reports

The retention time for data used in incident reports defines how long Storage Locker retains data, which are used in any Incident Report




## 8.1.10 List Management settings

List management makes it possible to define identities and lists so that the allowed or not allowed identities can be defined.

The settings define and manage identity and list management settings. Settings allow you to:

- Add, edit, and delete identities containing license plates and face images
- Add, edit, and delete lists and manage list content
- Import and export lists and identities
- Configure LPR and FR event database retention limits
- Enable and define integration and its settings

The System manager application provides several dialogs to access and modify list management service data and settings. The dialogs can be found in the “System settings“ section.

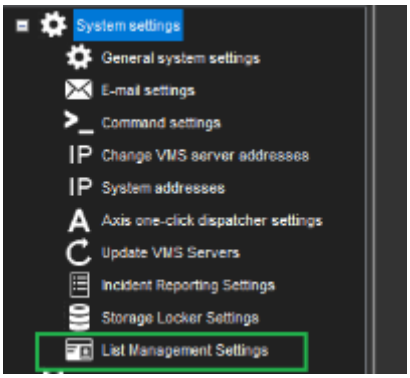
Integration requires LPR and FR integration license.

### 8.1.10.1 List Management Settings

How to open the **List Management Settings** dialog:

1. Go to the **System** tab

2. Under **System settings**, double-click the **List Management Settings** tree node, as shown in the picture below:




3. When you double-click **List Management Settings** he dialog loads request the settings from the list management service and display them if successful. If loading fails, the error message is displayed to the user, and the dialog is closed.

### 8.1.10.1.1 List Management Settings dialog

In the dialog, you can find the following tabs:

- **Identities** - list of identities and their settings
- **Lists** - identity lists and their settings
- **Import/Export** - import/export functionality to restore/save list management data to CSV text format
- **Database Settings** - parameters related to the list management service database
- **Integration Settings** - integration enabling and integration settings

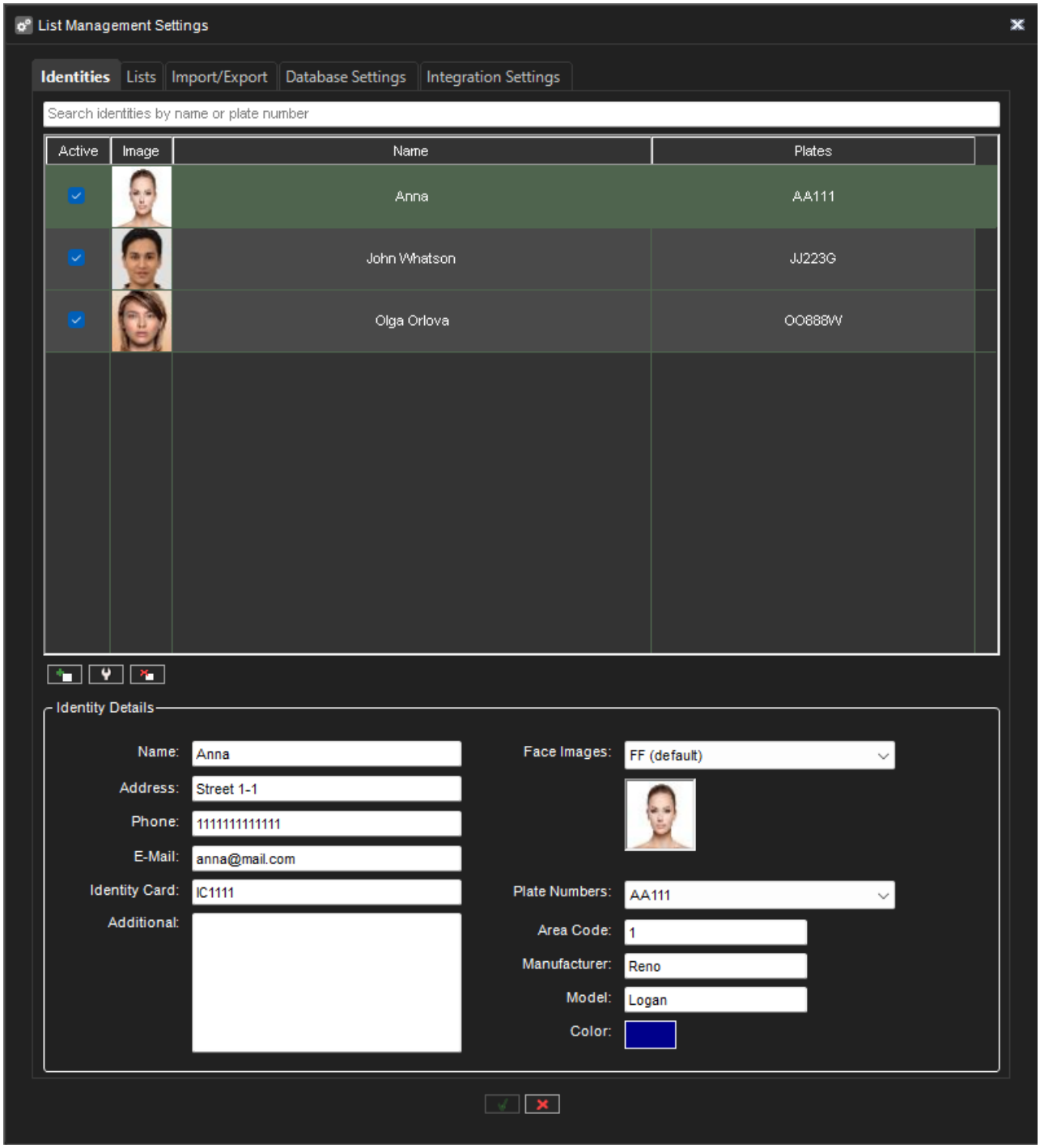
All changes you make in these dialog tabs can be saved by clicking the **OK** button.

If you do not need to keep the changes, you can close the dialog with the **Close** or the **Cancel** button.

Below you can find a detailed description of each tab.

#### 8.1.10.1.1.1 Identities tab

In the “Identities” tab you can perform operations with identities:




1 Identities tab

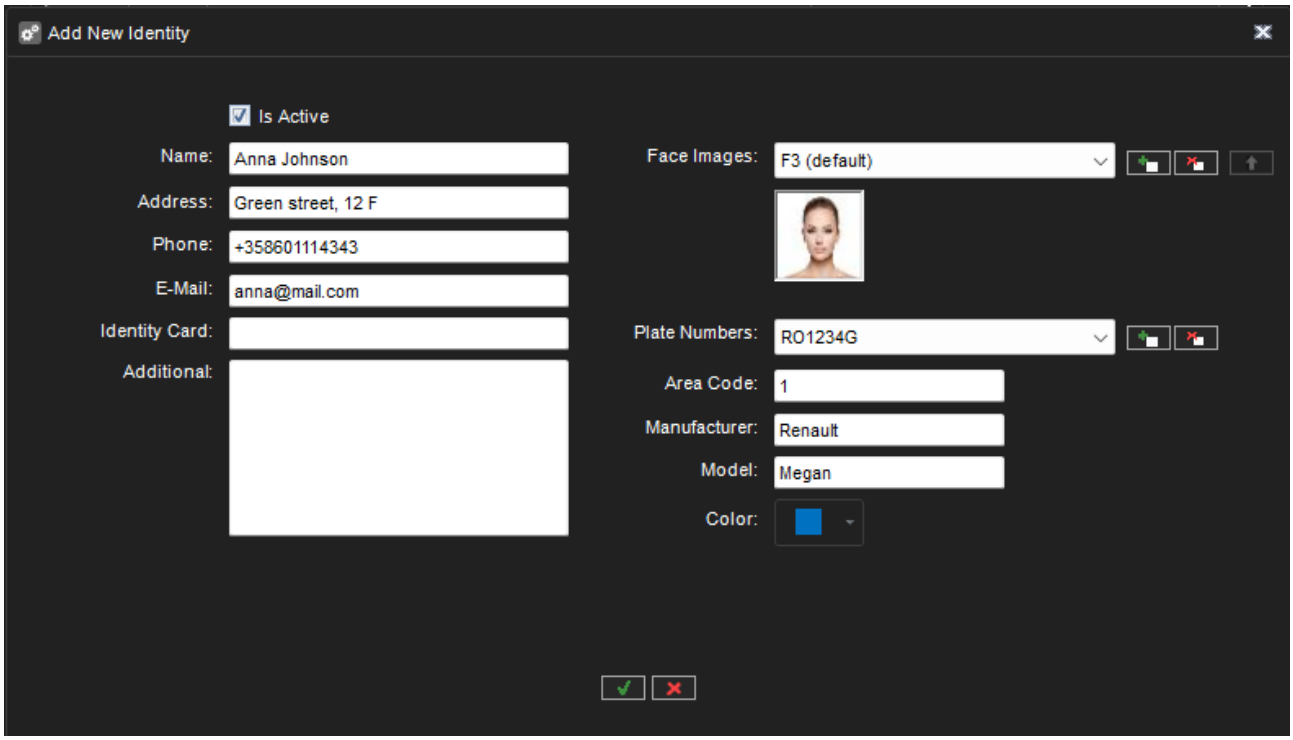
Identity selection is done using the left mouse button. If you must select multiple identities (multiple rows in the list), you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected identities to the "active" or "not active" state by clicking the checkboxes in the “Active“ column.

Above the list of identities, you can find the **Search** field: when you type here, the list of identities is automatically filtered if the text is found in identity names or plates.

You can add and remove selected identities with the **Add** and **Remove** buttons below the identity list.

You can see detailed information about identity in the **Identity Details** area, but all these fields are read-only. To modify the selected identity, you can click the **Modify** button or double-click it with the mouse button.

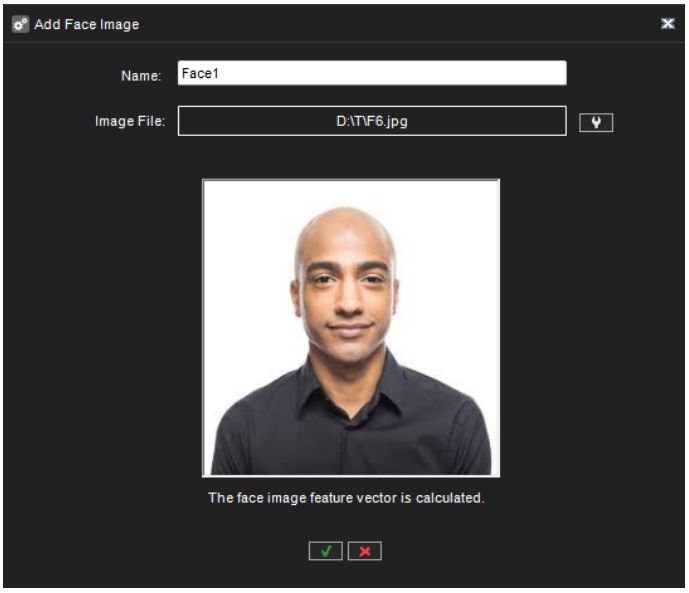
When you add or modify identity, the following dialog is shown:




2 Add/modify identity dialog

You can change any field data or add/remove identity face images or vehicles (license plates).

To add a face image, click the “Add a new face image” button, and the following dialog will open:




3 Add Face Image dialog

> Several face images can be defined for an identity. All face images will be used when doing identity face matching, so using multiple face images for an identity, may increase the face detection confidence

You can write a face image name and select a face image file here. After file selection, the image will be loaded, and the feature vector data of the image will be calculated.

> To calculate the face feature vector, at least one face recognition service must be started and registered in VMS

To remove a face image, you need to select it in the combo box and click the **Remove Selected face image** button.

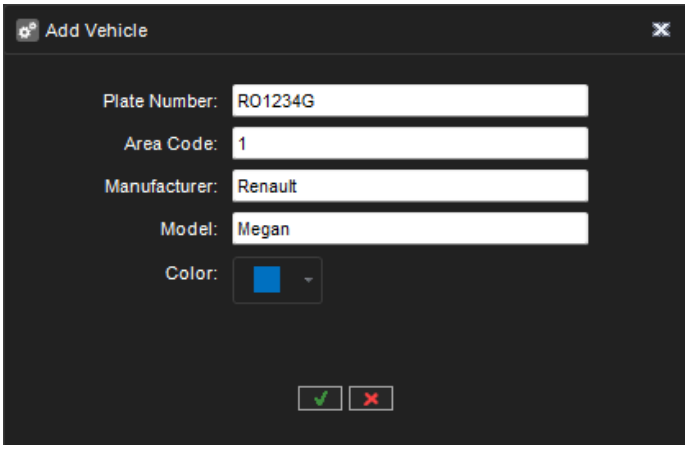
#### 8.1.10.1.1.2 Set face image as default

One face image is the default, which is used as a thumbnail in all plugins and identity lists. To set the face image as the default, you need to select the face image in the combo box and click on the **Set selected face image as default** button:


4 Set selected face image as default

#### 8.1.10.1.1.3 Add or remove vehicles

You can add or remove vehicles. To add a vehicle, click the **Add a new vehicle** button, and the following dialog will open:

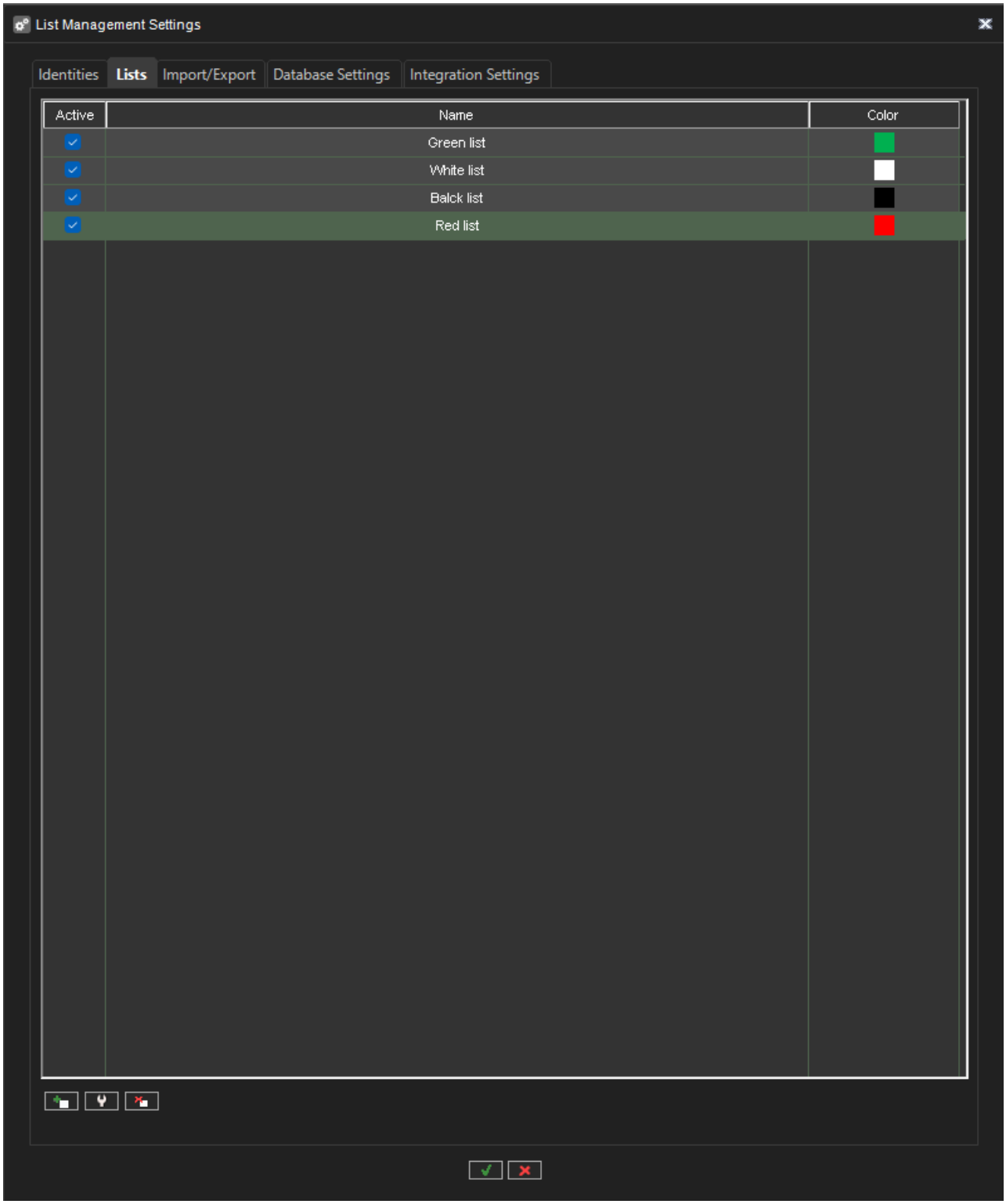



5 Add Vehicle dialog

In the **Add Vehicle** dialog, you can type the license plate number, area code, manufacturer, model, and vehicle color. To remove a vehicle, you need to select it in the combo box and click the **Remove selected vehicle** button.

#### 8.1.10.1.1.4 Lists tab

In the **Lists** tab you can perform operations with identity lists:


List Management Settings
Identities
Lists
Import/Export
Database Settings
Integration Settings
Active
Name
Color
Green list
White list
Balck list
Red list

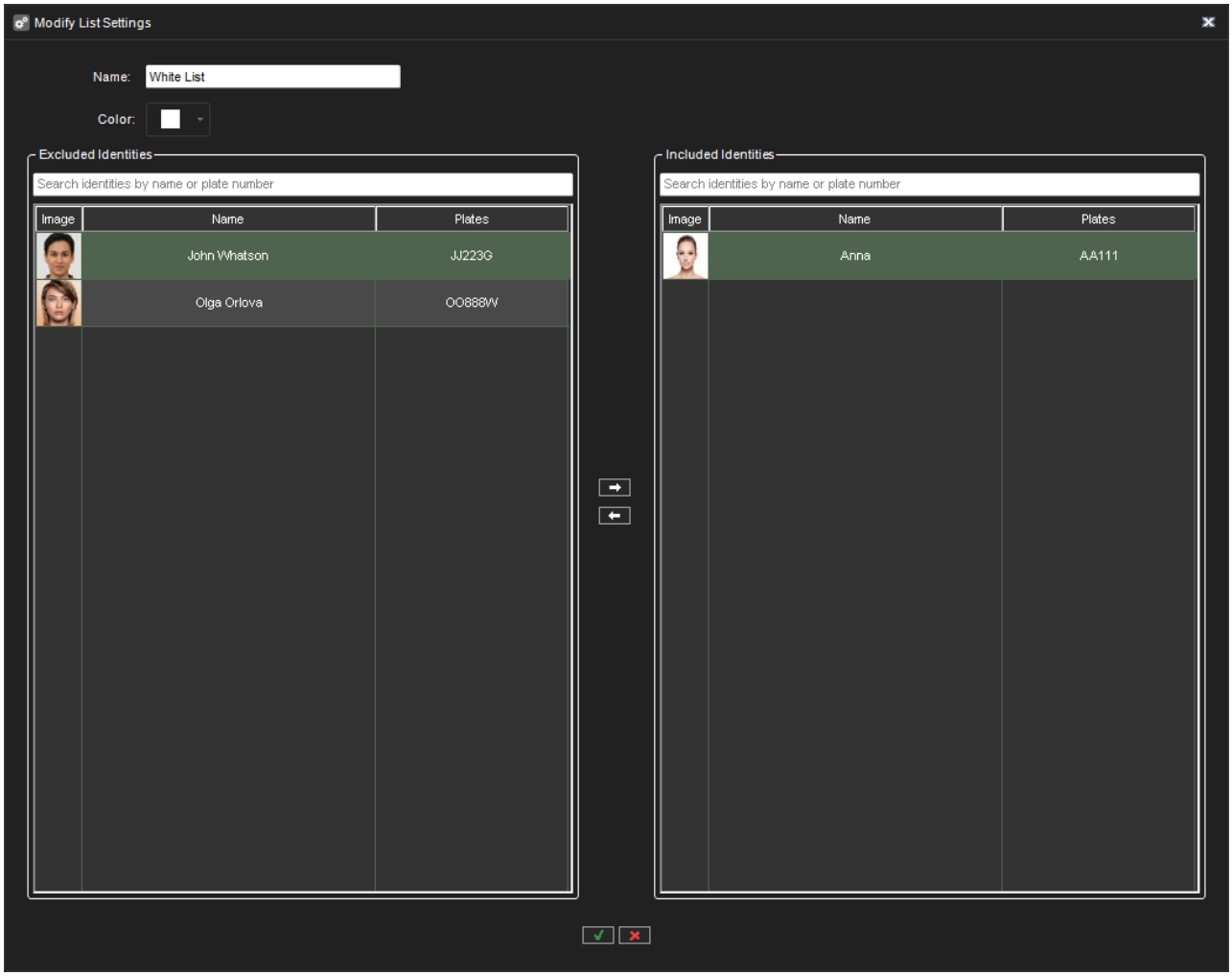
6 Lists tab

List selection is done using the left mouse button. If you need to select multiple lists (multiple rows), then you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected lists to the **active** or **not active** state by clicking the checkboxes in the **Active** column.

You can add and remove selected lists with the **Add** and **Remove** buttons below the lists.

To modify the selected identity list, you can click the **Modify** button or double-click it with the mouse button.

When you add or modify the identity list, the following dialog is shown:




7 Add/Modify List Settings dialog

You can move identities to the list or remove them from the list, define the name of the list, and color.

### 8.1.10.1.1.5 Import/Export tab

In the "Import/Export" tab you can import list management data from a CSV file or export list management data to a CSV file:


8 Import/Export tab

### 8.1.10.1.1.6 Import parameters

The following parameters must be set for the import process:

- **File path** - path to the CSV file which contains list management data
- **Import type** - “Identities only“ or “Identities and lists“
- **CSV delimiter** - “Comma” or “Semicolon“
- **Items with the same identifier** - “Skip“ them, “Overwrite“ or “Create new“ identifier for them

When the correct parameters are selected, the **Import data from file** button is active, and users can start the import process. During the process, users will see the progress and result of the import.

#### 8.1.10.1.1.7 Export parameters

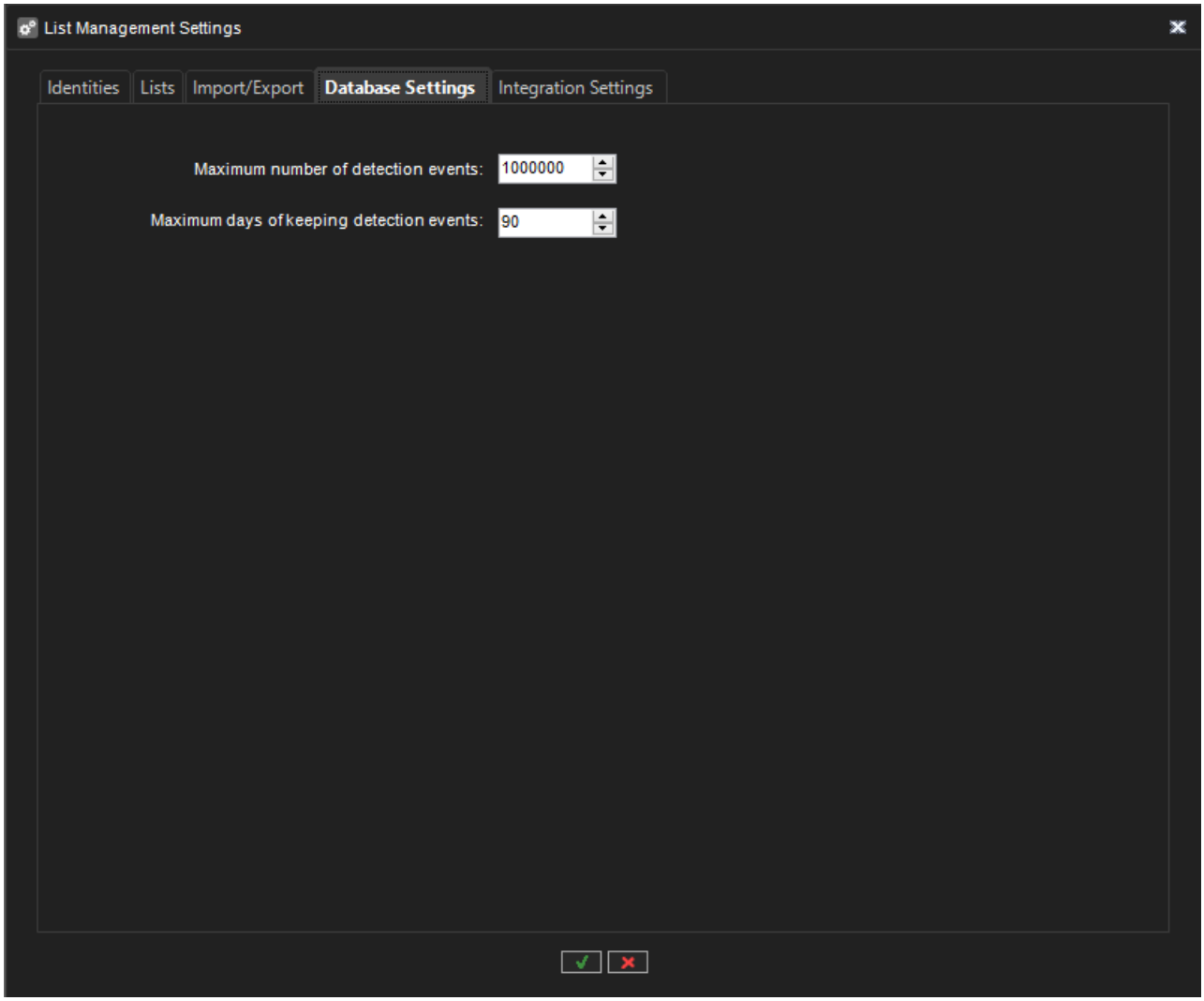
The following parameters must be set for the export process:

- **Folder path** - path to the folder where list management data will be exported and where the CSV file will be created
- **Export type** - “Identities only“ or “Identities and lists“
- **CSV delimiter** - “Comma” or “Semicolon“

When the correct parameters are selected, the “Export data to file“ button is active, and users can start the export process. During the process, users will see the progress and result of the export.

#### 8.1.10.1.1.8 Database Settings tab

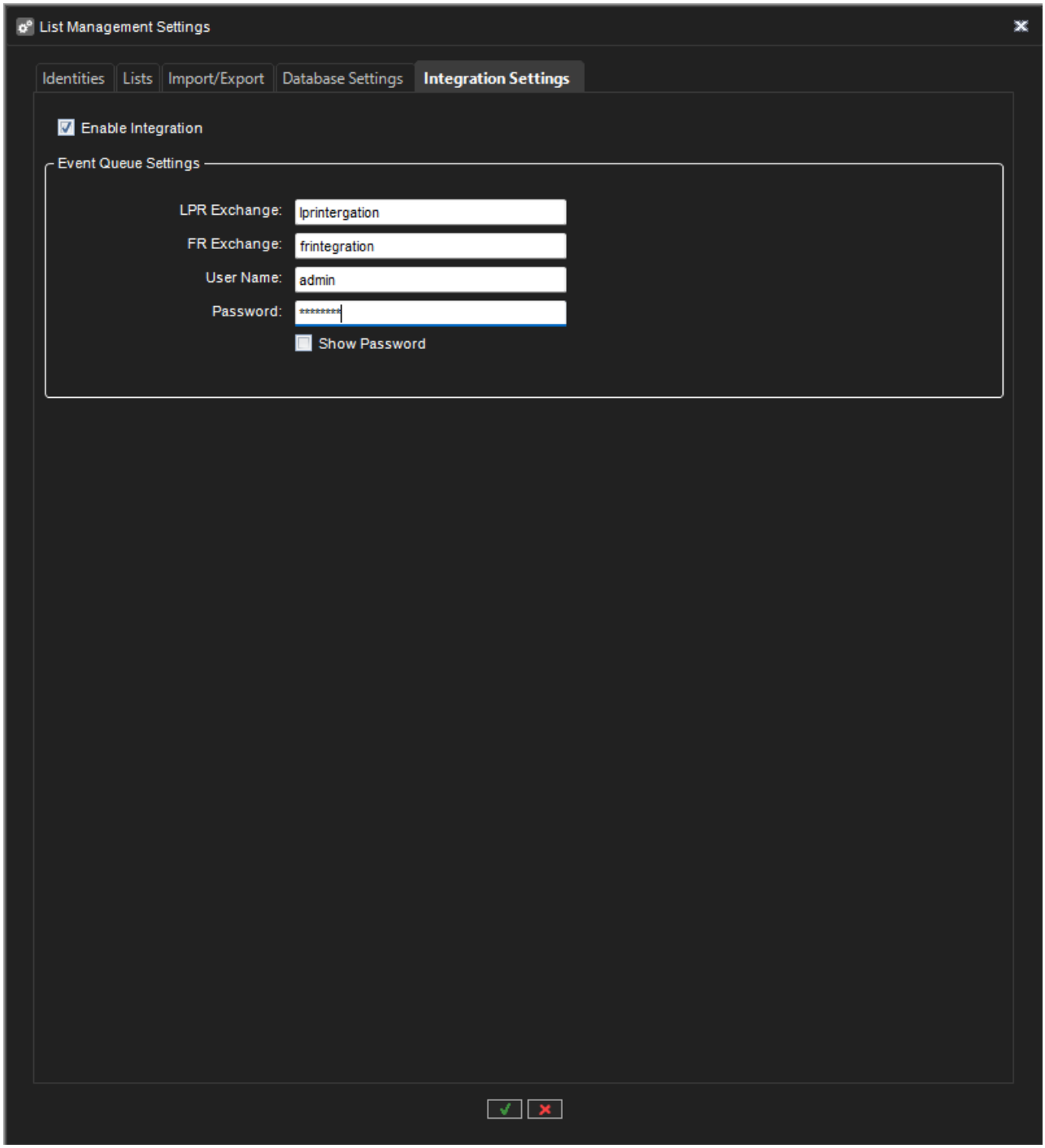
In the **Database Settings** tab, you can setup database settings for the list management service:




9 Database Settings tab

### 8.1.10.1.1.9 Integration Settings tab

In the **Integration Settings** tab, you can setup integration settings for the list management service:

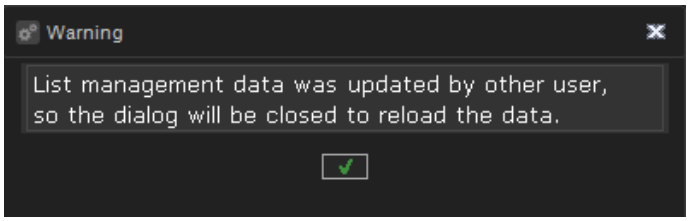



10 Integration Settings tab

Here you can define settings for the event queue and enable/disable integration settings. The tab is not visible if the license does not enable list management integration.

### 8.1.10.2 List management data update notification

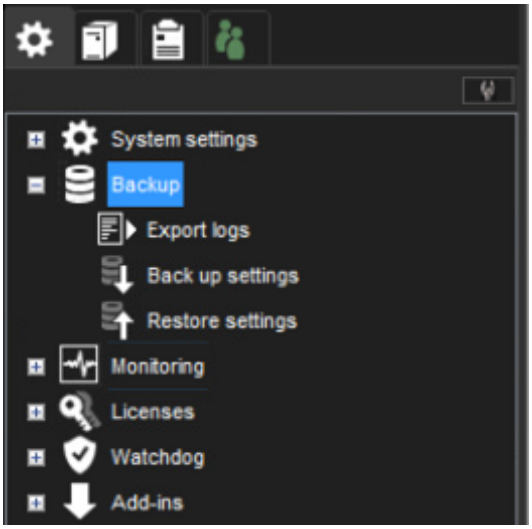
If list management data has been changed in another application, the System Manager will receive an event with updated information and display the following message:




11 Data update warning

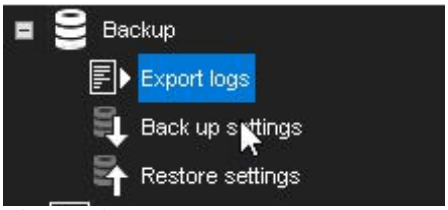
When you click the **OK** button of the message dialog, all settings dialogs will be closed to reload data from the list management service. All changes that were not saved will be lost.

## 8.2 Backup




### 8.2.1 Export logs

Export log files and send them to the system supplier should there be a problem with the system.




Log files are saved to a compressed (zipped) file that can be placed to a removable or non-removable device.

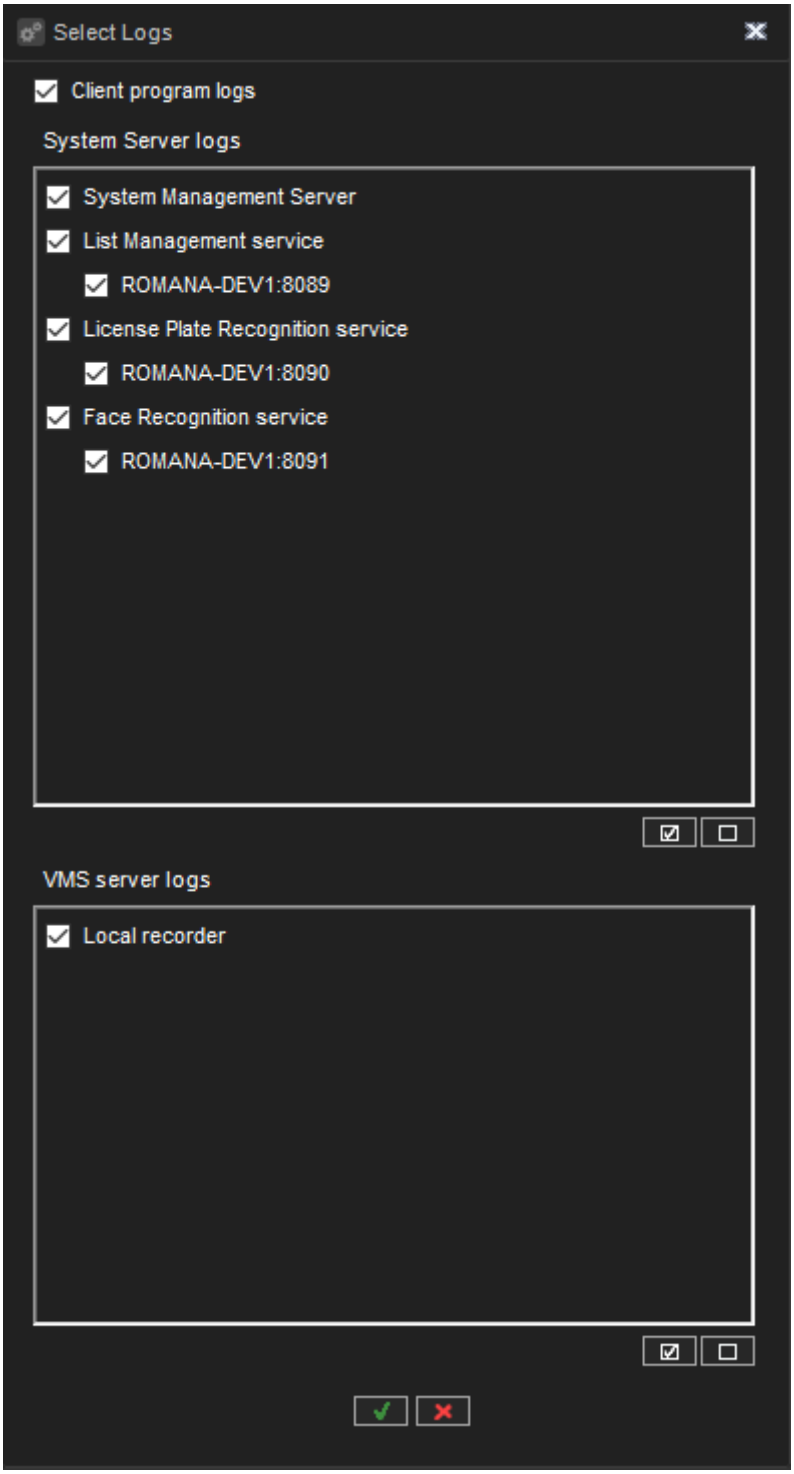
### 8.2.1.1 Export log files via System Manager

1. Open the System Manager application for export logs and choose the **Export logs** subitem in the **Backup** tree item on the **System** tab.
2. Select logs that can be exported in the

**Select Logs** window.

If there are problems with a server select logs on the **System Server logs** panel. In addition, select client program logs.

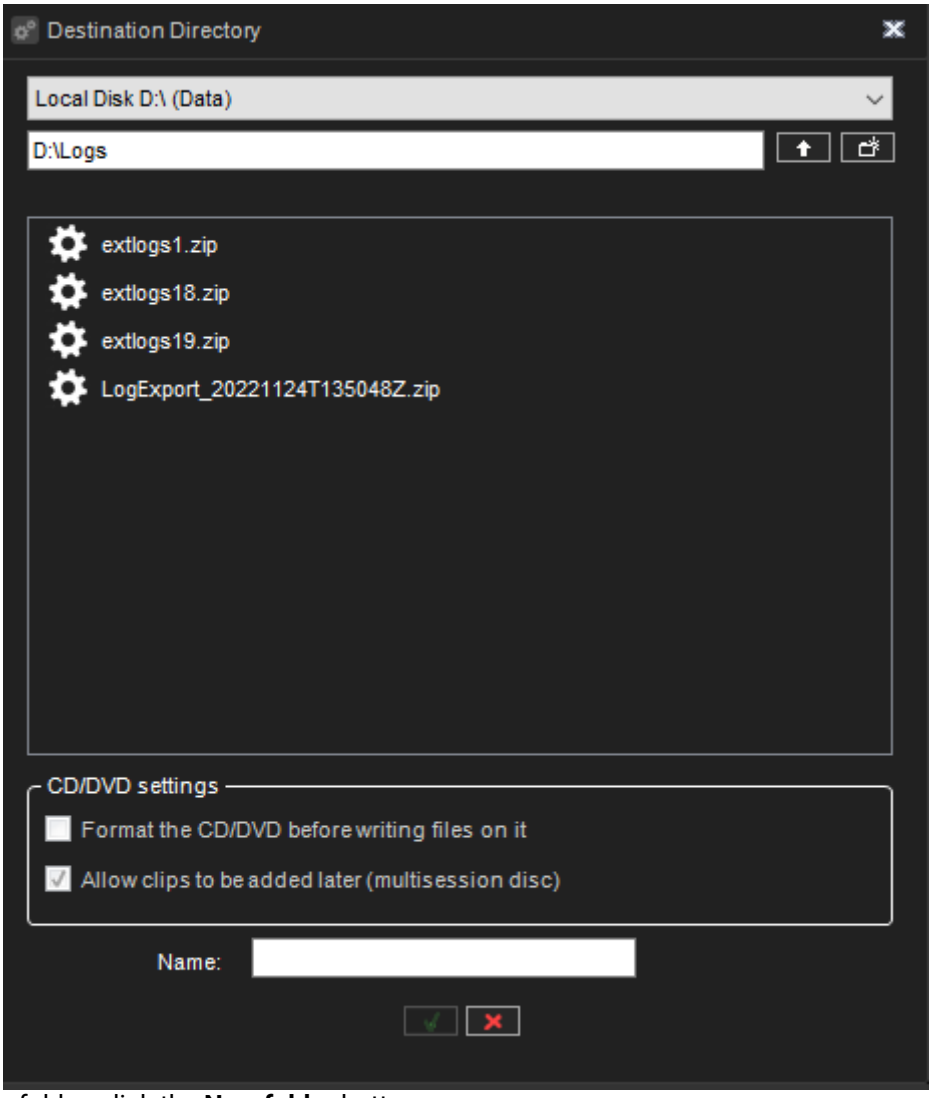
> The client logs are from the machine where you are accessing the system manager application.




For fast selection, you can use the **Select All** and **Clear Selections** buttons placed under the **System Server logs** and **VMS server logs** panels. Select or clear all selections for specific service groups (e.g. **License Plate Recognition service**) that contain specific services by clicking on the services group checkbox.

3. Click **OK**.

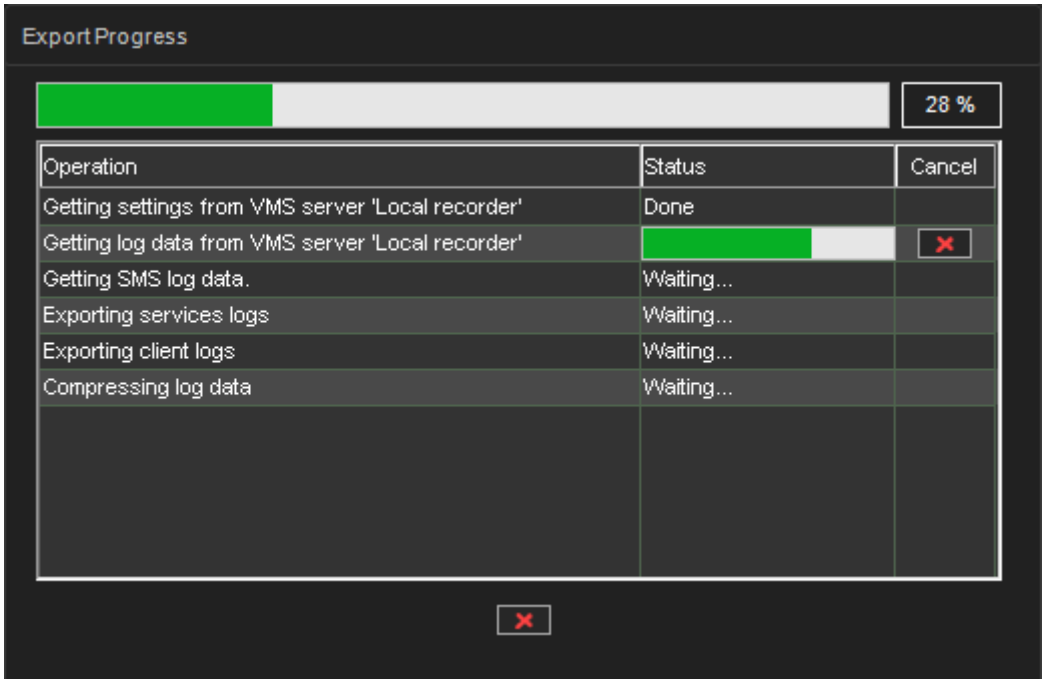
4. Select the storage device and the folder where you want to save the log files in the **Destination Directory** window.




To create a new folder, click the **New folder** button.

Type a name for the ZIP file in the **Name** fields and click **OK**

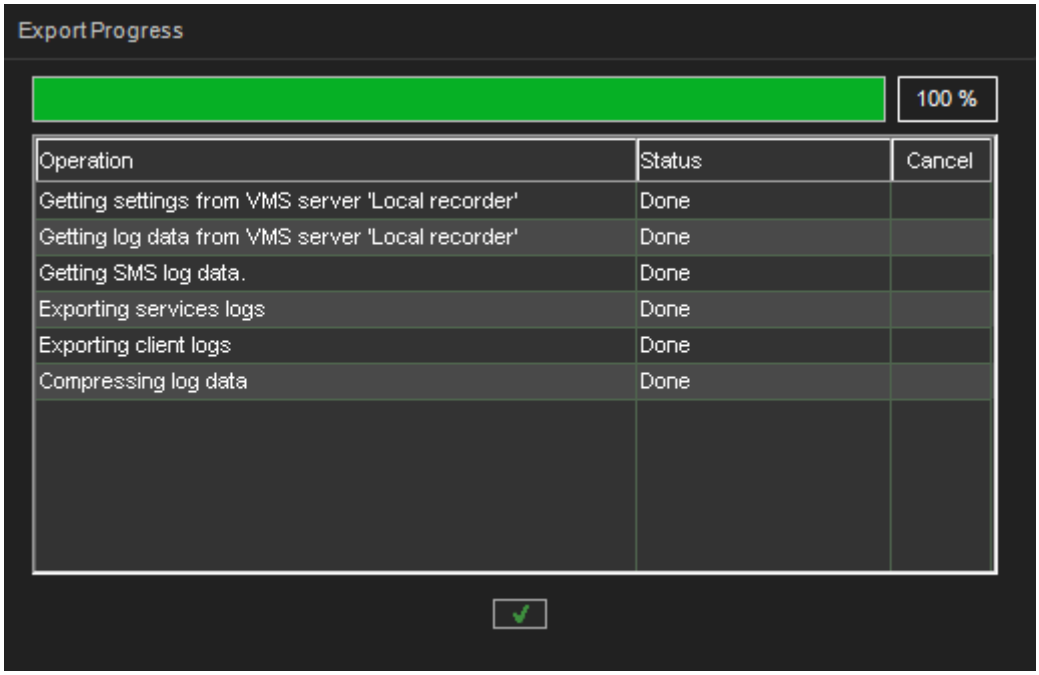
You can see the progress of exporting in the **Export Progress** window. Operations are executed in order from top to bottom.




It is seems like the operation is stuck it can be cancelled.

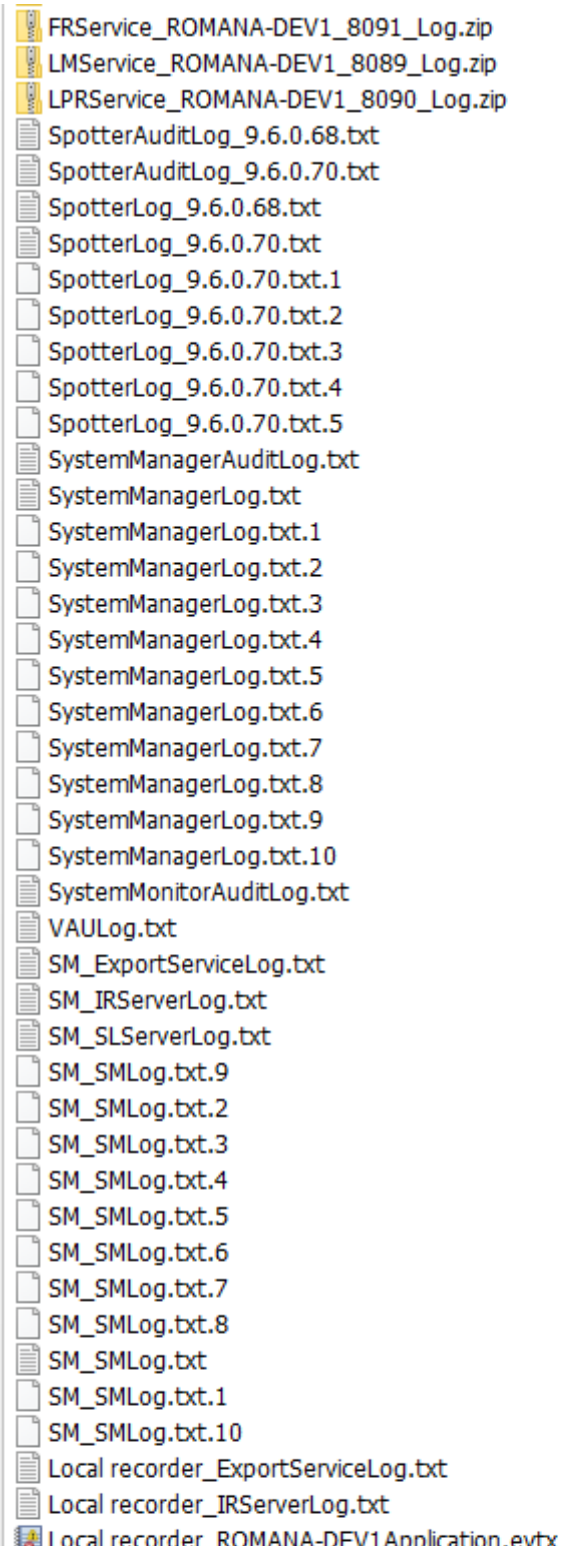
Cancel all export by clicking on the **Cancel** button at the bottom of the window.

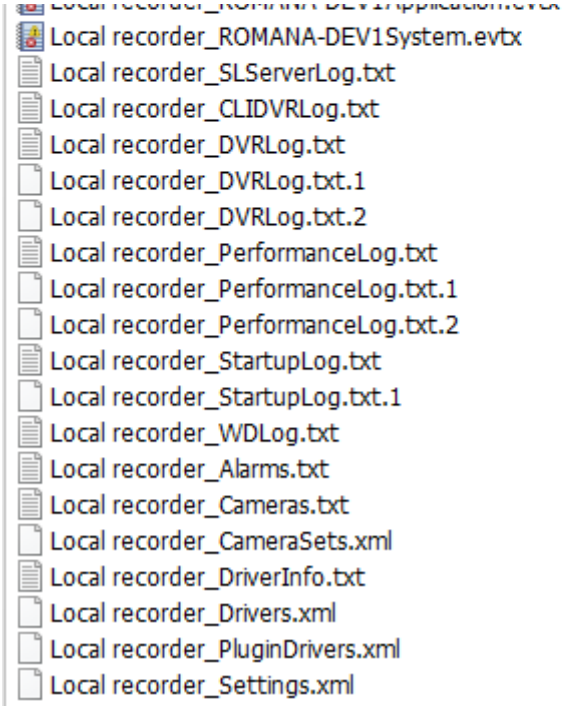
5. Click **OK** to close the window once the export is completed.



6. The system exports the files to a ZIP file. Send the ZIP file to the system supplier. Services log files are stored in inner ZIP archives in the main ZIP file.

The typical content of logs ZIP archive is the following:





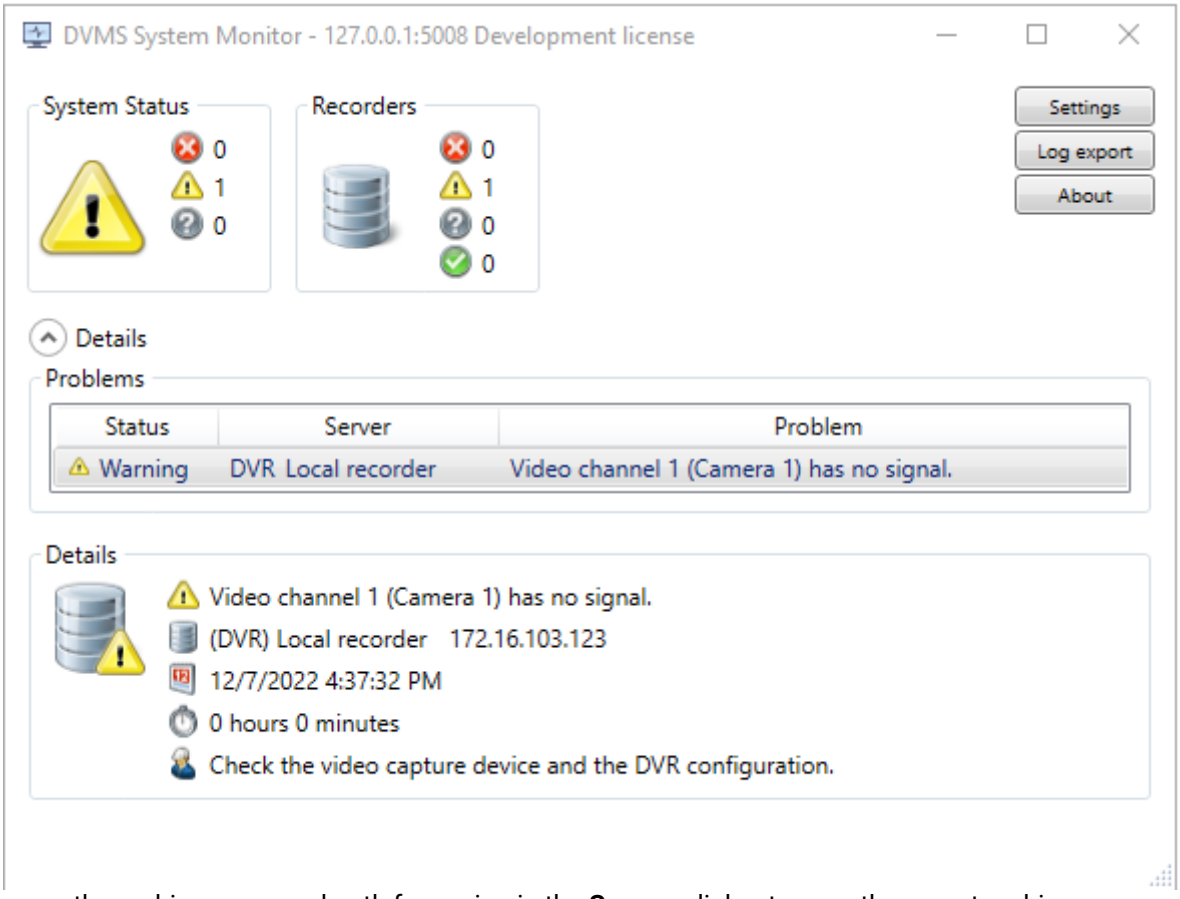

Some service sub-archives can be missed if there are no connections to services.

### 8.2.1.2 Export log files via System Monitor

It is possible to collect system logs via the System Monitor application.

1. Open System Monitor and click the

**Log export** button:



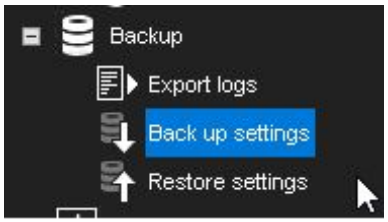

2. Choose the archive name and path for saving in the **Save as** dialog to save the export archive.

3. Click **Ok** to start collecting logs.

The System Monitor can collect **SM server** logs (also ones include **Incident Reporting** log, **Storage Locker** log, and **Export services** log), **DVRs** logs, clients' logs (**Spotter**, **System Manager**, etc.), and logs of all **List management**, **Face Recognition,** and **License Plate Recognition** services observed in the current system.

The typical content of logs ZIP archive is the same as for ZIP archive from System Manager. Some service sub-archives can be missed if there are no connections to services.

## 8.2.2 Back up settings



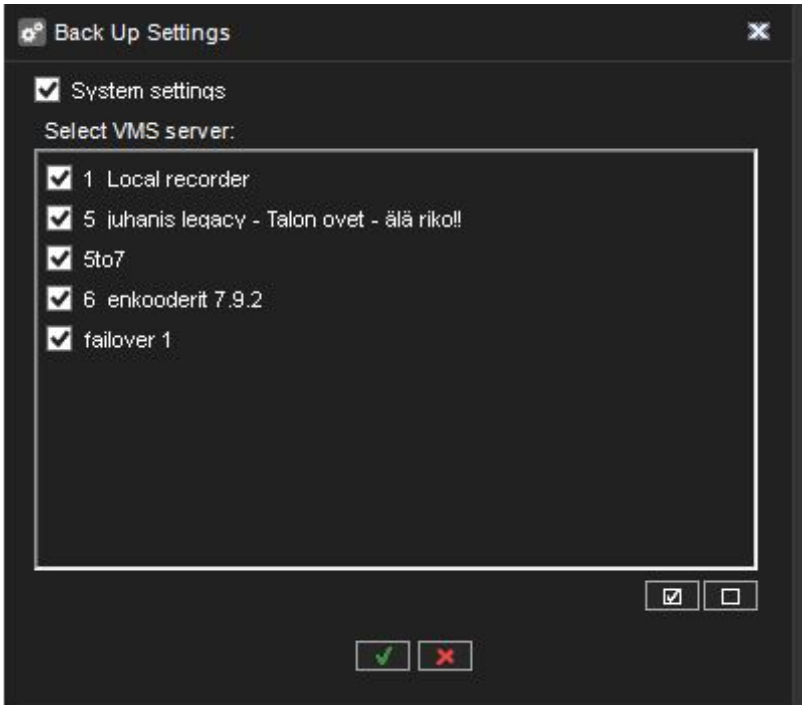

Backup system settings to be able to restore them if the hard disk that contains the settings fails.

You can back up system settings and server settings.
System settings contain data about the servers, profiles, and user accounts.
VMS Server settings contain data about the devices connected to the servers and their parameters.
You can save the backup copy to a hard disk, network drive, CD/DVD, floppy disk, or another removable or

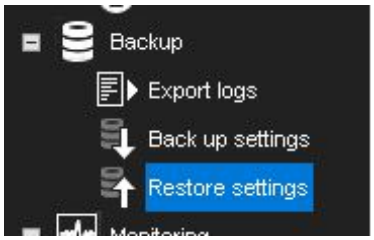
non-removable device.
Backup files have the file extension ".vbk".

To backup settings:

1. On the **System** tab, open **Backup settings**. The **Backup settings** dialogue box is shown.
2. Select the system and server-specific settings that you want to back up and click **OK**.
3. Select the storage device and the folder where you want to save the backup file. To create a new folder, click the **New folder** button.
4. Type a name for the file and a description and click **OK**. The description is optional. The system creates the backup file.



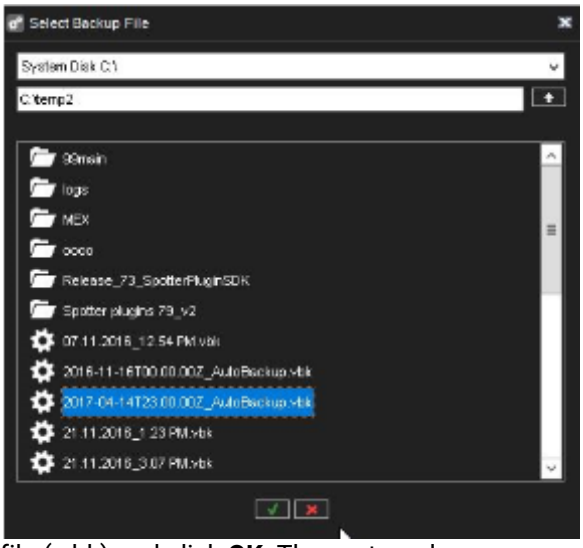

## 8.2.3 Restore settings




If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

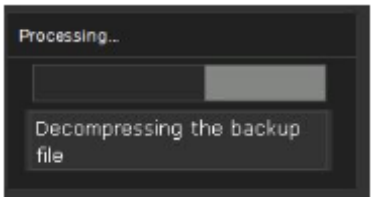
To restore settings:

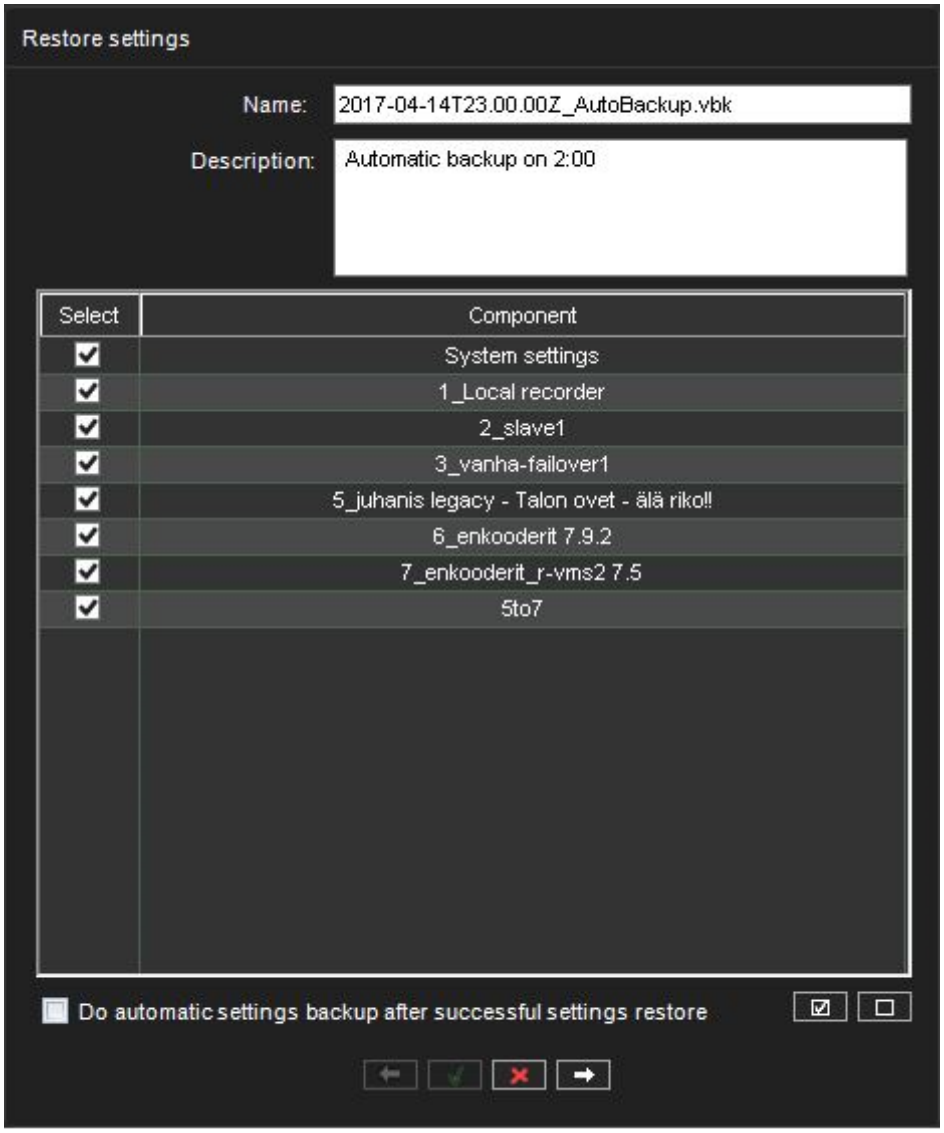
1. On the **System** tab, open **Restore settings**. The Select backup file dialogue box is shown.




2. Find and select the backup file (.vbk) and click **OK**. The system decompresses the file and then shows the **Restore settings** dialogue box.

The dialogue box also shows a description of the settings.






3. Select the system and server-specific settings that you want to restore and click **Start Restore**. The settings are restored.

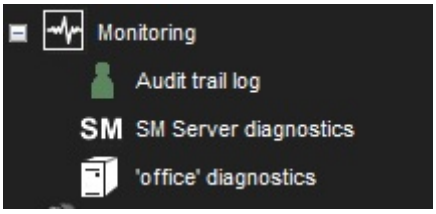
4. Click **OK** to accept the new settings or **Start the restore process again** to return to the **Restore settings** dialogue.

**Do automatic settings backup after successful settings restore** recommended, especially when restoring the system after failover has happened.

# 8.3 Monitoring

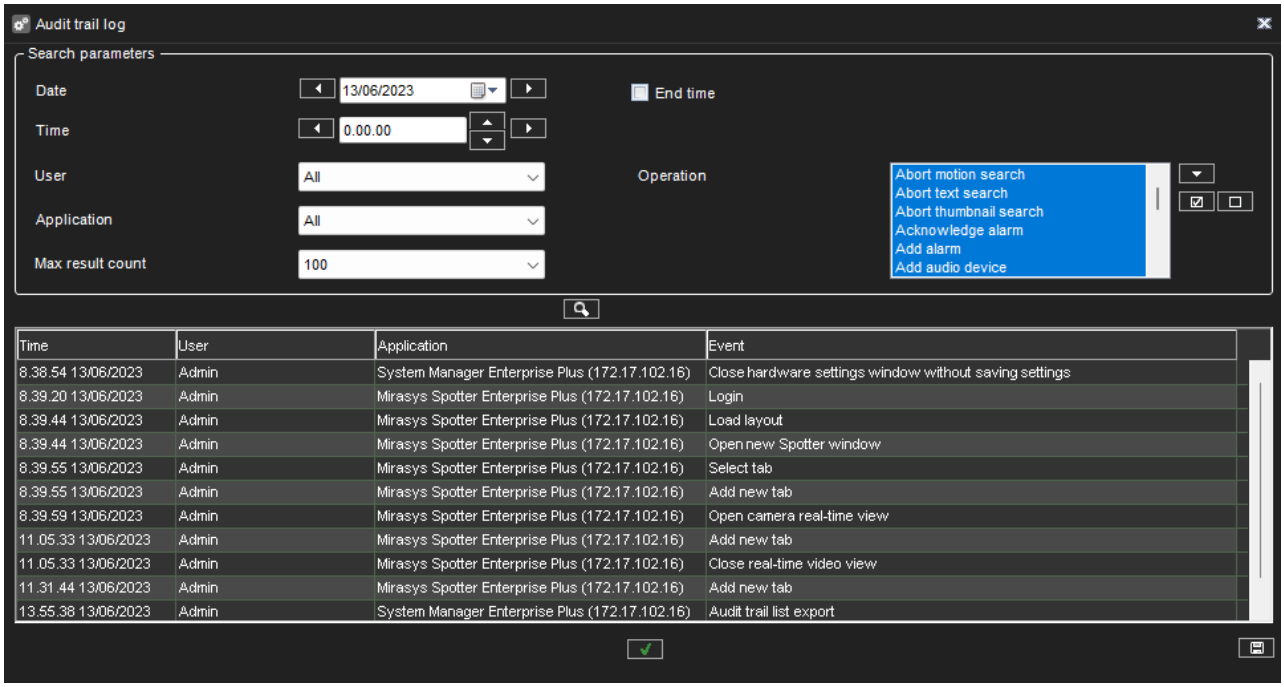
## 8.3.1 Audit trail log

The Audit trail log can be used to search VMS system user activity information. It can be accessed in System Manager at the System tab tree under Monitoring.




### 8.3.1.1 Audit trail log

In the audit trail log dialog admin can search for audit trail events using several search parameters.




The search button under the search parameters group starts the audit trail event search with selected parameters. Results are listed in the result list ordered by time. Found audit trail events can be sorted by other audit trail event information by clicking the list headers.

### 8.3.1.2 Search parameters

Following search parameters can be used for audit trail event searching.

- **Date** - Select the date for the search to start. Buttons on the left and right decrease or increase the day of the date.
- **Time** - Select the time of the date for the search to start. Buttons on the left and right decrease or increase the hour of the time. Buttons up and down increase or decreases minutes of the time by ten.
- **End time check box** - If checked, it enables search end date and time selection similar way as for start time. If not checked, end time is not used as a search filter (= search until now)
- **User** - User whose audit trail events will be searched. All = search without filtering users.
- **Application** - Application to search. All = search without filtering applications.
- **Max result count** - Maximum number for how many audit trail events will be searched starting from start time.

- **Operation** - Operation to search: none, one, many, or all operations can select. If none or all is selected, then search without filtering operations. The following buttons can be used with operations:
    - Enlarge operation list view
    - Select all
    - Unselect all

#### 8.3.1.3 Results list

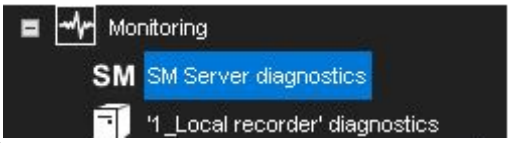
Found audit trail events are listed in the search result list. The list contains information about each audit trail event.

- **Time** - Time of the user action.
- **User** - Username who did the user action.
- **Application** - Application where the user action was taken.
- **Event** - Name of the user action.

#### 8.3.1.4 Audit log export

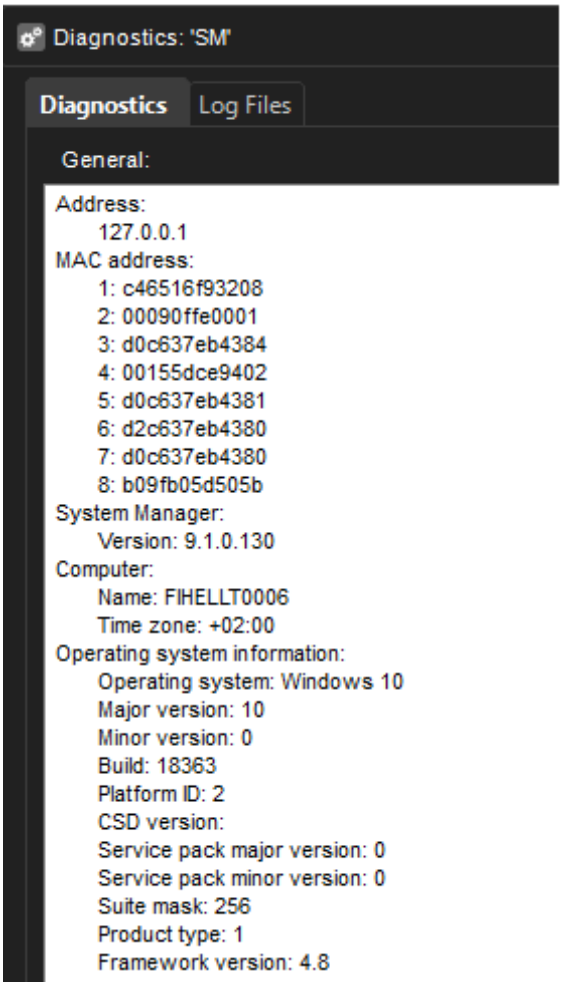
Listed audit trail events can be exported to a PDF file as an audit trail report by clicking the button under the audit trail events results list. The location and the name of the exported file and the comment for the report can be given on the save report dialog. The audit trail log report title is created of the export time and the user who exported the report. The report contains all the audit log entries with the same information that is listed in the audit trail event result list.

### 8.3.2 SM Server Diagnostics




SM Server Diagnostics shows information about the System Management Server that runs on the Master Server.

### 8.3.2.1 General




In SMServer Diagnostics, you can examine this information:

- SM Server version
- Computer name and time zone
- Operating system information
- Major version
- Minor version
- Build
- Platform ID
- CSD version
- Service pack major version
- Service pack minor version
- Suite mask
- Product type
- Framework version

#### 8.3.2.2 Log Files

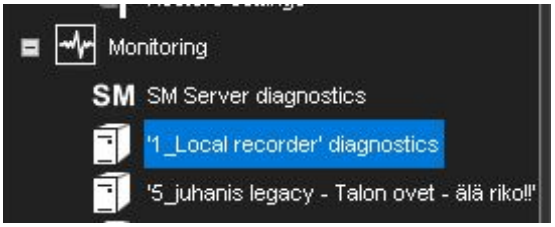
If there are problems with the system, you can access the system log files on the **Log Files** tab.

To examine a log file:

- Select the file from the drop-down list.

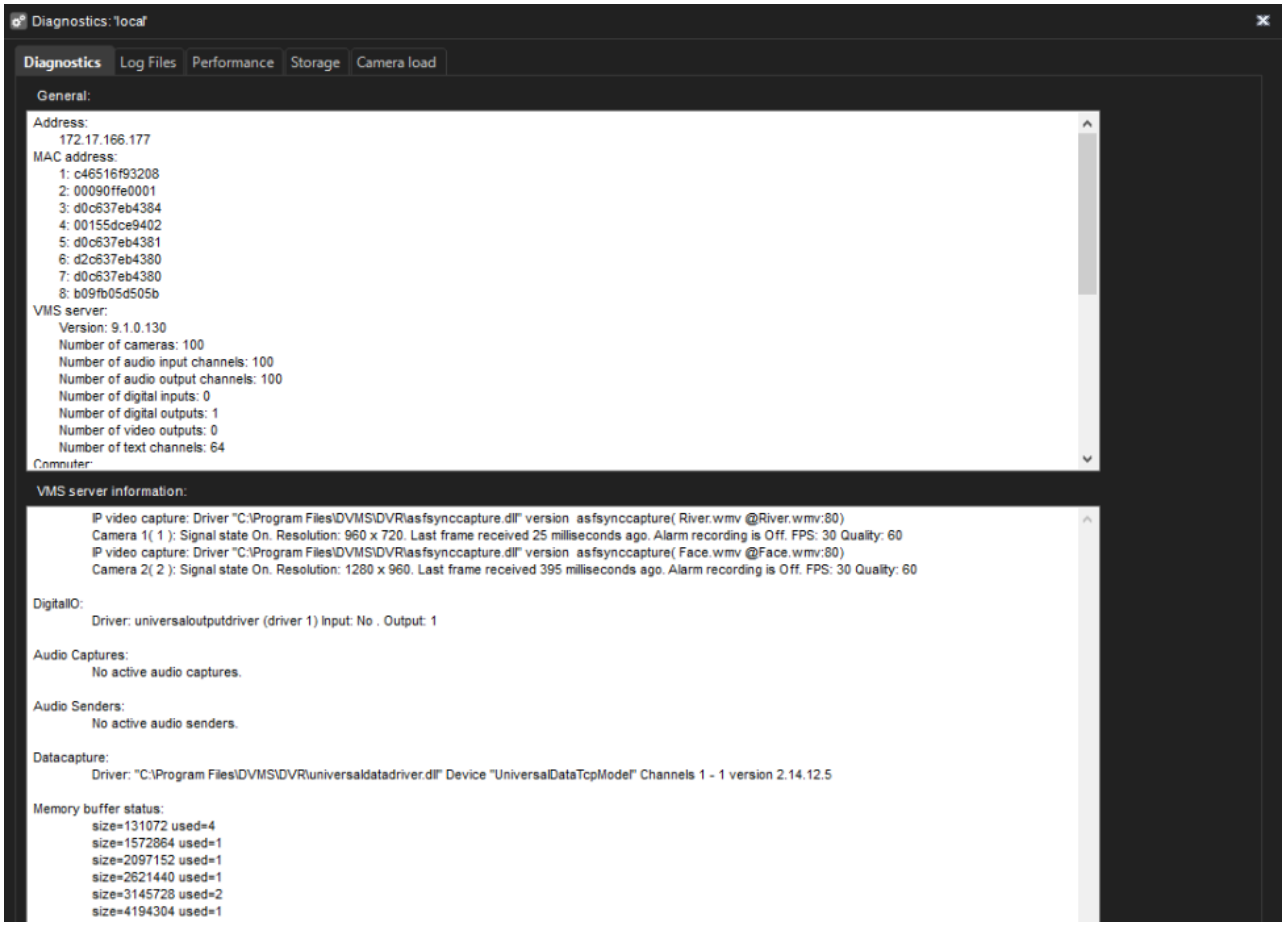
The contents are shown in the **Contents of the selected log file.**

### 8.3.3 Server Diagnostics




VMS Server diagnostics shows information about the server and the CPU and network usage.

### 8.3.3.1 Diagnostics




The **Diagnostics** tab shows this information:

- Information about the server:
- Software version
- Model
- Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
- The name of the computer and the time zone
- Operating system information
- Processor information
- Installed drivers, for example, capture drivers, video output drivers, digital output drivers, and PTZ drivers.

### 8.3.3.2 Log Files

The **Log files** tab shows a list of log files.

To see the contents of a log file:

- Select the file from the drop-down list. The contents are shown in the **Contents of the selected log file**.

### 8.3.3.3 Performance

On the **Performance** tab, you can monitor these:

- CPU usage.
- Usage of physical memory.
- Usage of virtual memory.
- Network traffic.
- Used disk space.

### 8.3.3.4 Storage

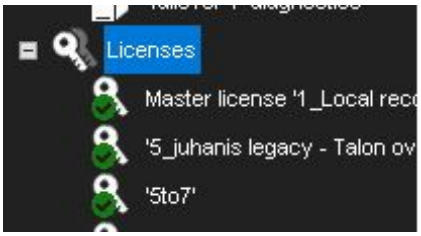
On the **Storage** tab, you can monitor disk and file properties. For example, you can examine free disk space or monitor saved data by the camera and audio channel.

**General**Total recording capacity. Shows the total storage capacity that is reserved for the recordings.

**Used space**. The quantity of space that the recordings have used.
**Free space**. Free space is available for recordings.
**% used**. The percentage of the disk's capacity that is used.
**Average saving speed**. Calculated by dividing the quantity of data saved since the server was last started by the uptime.
**VMS Server uptime**. Shows the time that the server has been operating since it was last started.
The counter shows the difference between the current time and the start time in days, hours and minutes.
**Disks**Total recording capacity. Shows the storage capacity that is reserved for the recordings on the selected disk.
**Used space**. Used recording space on the selected disk.
**Free space**. Free space is available for recordings on the selected disk.
**% used**. The percentage of space used of the total capacity reserved for the recordings.
**Total recording cache.** Shows the total capacity of the cache that is used for the temporary storage of data before it is permanently written on a disk.
Because of the cache, video and audio can be recorded immediately when the server is started. The cache is also used for pre-event recording.
The system automatically calculates how much cache space it must have and allocates space accordingly.
**Used recording cache**. Temporary space that is currently in use.
**Free recording cache**. Temporary space that is currently free.
**Cameras**Oldest time. The date and time of the oldest image in the store.
**Newest time**. The date and time of the newest image in the store.
**Total no. of images**. The total number of images in the store.
**Average image size**. The average image size.
**Used space**. This value shows how much space the images and metadata files from this camera use.
**% used**. This value shows what percentage of space this camera has used of the total capacity reserved for the recordings.
**Audio channels**Oldest time. The date and time of the oldest audio sample in store.
**Newest time**. The date and time of the newest sample in store.
**A total number of samples**. The total number of audio samples in store.
**Average sample size**. The average audio sample size.
**Used space**. This value shows how much space the audio samples and metadata files from the audio

channel use.
**% used**. This value shows what percentage of space the audio channel has used of the total capacity reserved for the recordings.
**Text channels**Oldest time. The date and time of the oldest text data sample in store.
**Newest time**. The date and time of the newest sample in store.
**A total number of samples**. The total number of text data samples in store.
**Average sample size**. The average text data sample size.
**Used space**. This value shows how much space the text data samples and metadata files from the text channel use.
**% used**. This value shows what percentage of space the text channel has used of the total capacity reserved for the recordings.

## 8.4 Licenses



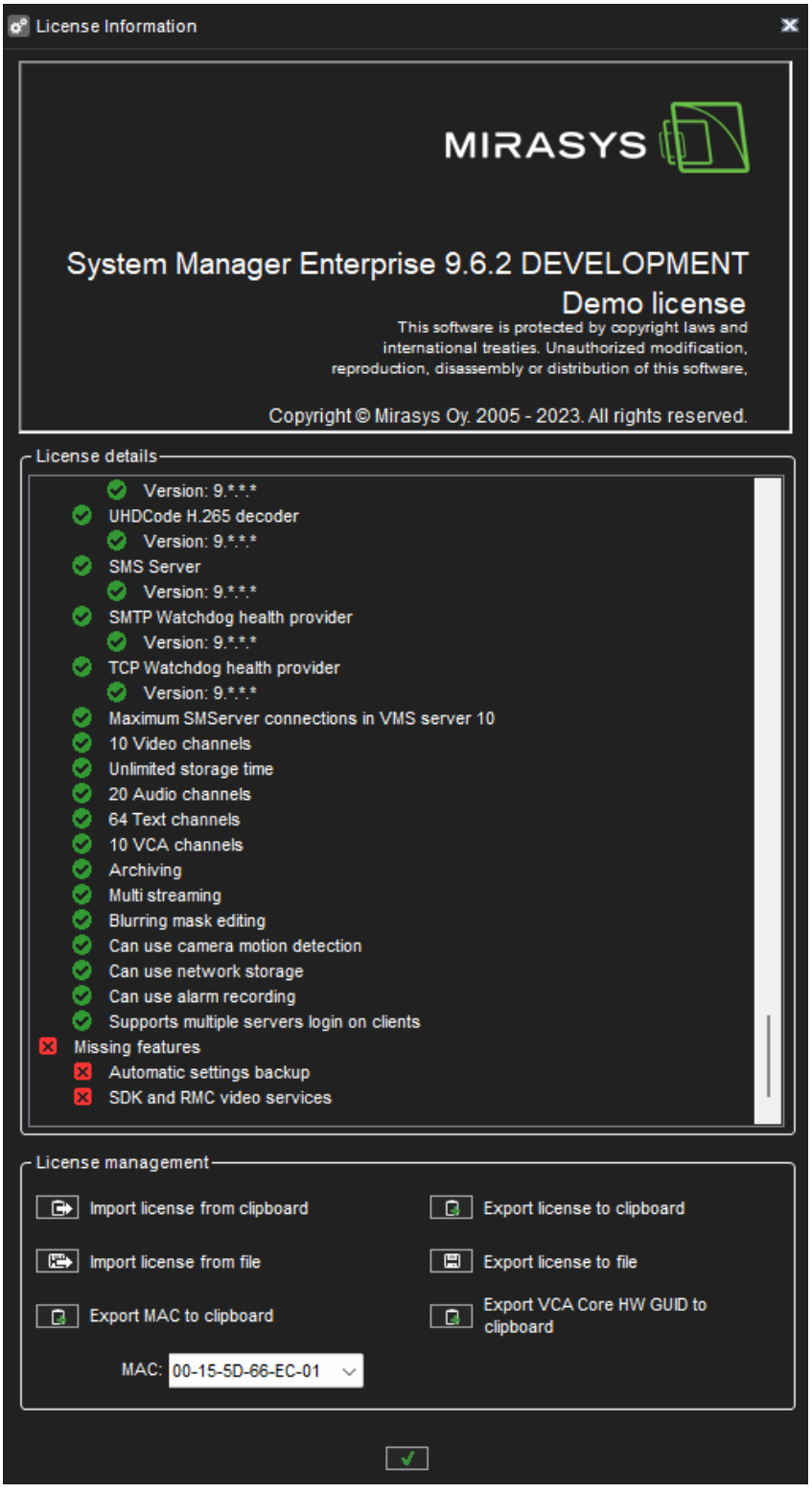

The server needs a valid license for full functionality.
Depending on the installation, you may need to upgrade the license information when adding new functionality or cameras to the system.

To get a license key, please contact your supplier and follow the license upgrade procedure as detailed by the supplier.

If you have any problems in upgrading the license, please contact *orders@mirasys.com*[1].

You can also add more camera channels and features such as VCA capabilities to a server by getting a new license key.

1 mailto:orders@mirasys.com




### 8.4.1 License details

License details show all supported features of the license.


License Information
MIRASYS
System Manager Enterprise 9.6.2 DEVELOPMENT
Demo license
This software is protected by copyright laws and international treaties. Unauthorized modification, reproduction, disassembly or distribution of this software,
Copyright © Mirasys Oy. 2005 - 2023. All rights reserved.
License details
Version: 9.*.*.*
UHDCode H.265 decoder
Version: 9.*.*.*
SMS Server
Version: 9.*.*.*
SMTP Watchdog health provider
Version: 9.*.*.*
TCP Watchdog health provider
Version: 9.*.*.*
Maximum SMServer connections in VMS server 10
10 Video channels
Unlimited storage time
20 Audio channels
64 Text channels
10 VCA channels
Archiving
Multi streaming
Blurring mask editing
Can use camera motion detection
Can use network storage
Can use alarm recording
Supports multiple servers login on clients
Missing features
Automatic settings backup
SDK and RMC video services
License management
Import license from clipboard
Export license to clipboard
Import license from file
Export license to file
Export MAC to clipboard
Export VCA Core HW GUID to clipboard
MAC:
00-15-5D-66-EC-01

### 8.4.2 License Management

#### 8.4.2.1 To import a license key:

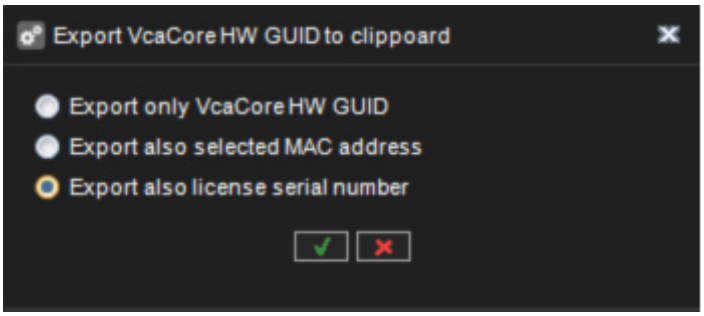
1. Click **Import license from the file**.
2. Browse to the license file location
3. Click **OK**. The new license is updated immediately.

#### 8.4.2.2 To export a license key:

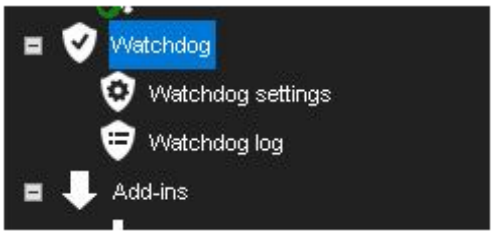
1. Click **Export license key to file** to create a text file for the license or **Export license key to the clipboard** to copy the key to the clipboard.
2. If exporting the license to a file, set the destination folder and the name of the file.
3. Click **OK**.

#### 8.4.2.3 To export VCA Core HW GUID

1. Click **Export VCA Core HW GUID to clipboard**
2. Select **Export also license serial number**
3. **Click Ok**




## 8.5 Watchdog



The system has a software watchdog (system monitoring service) that monitors the system and performs specific actions if problems occur.

In the Watchdog tool, you can select the events for which the notification list is notified through e-mail and access watchdog logs, which contain the events that have occurred and the actions that have taken place.

## 8.5.1 Watchdog settings

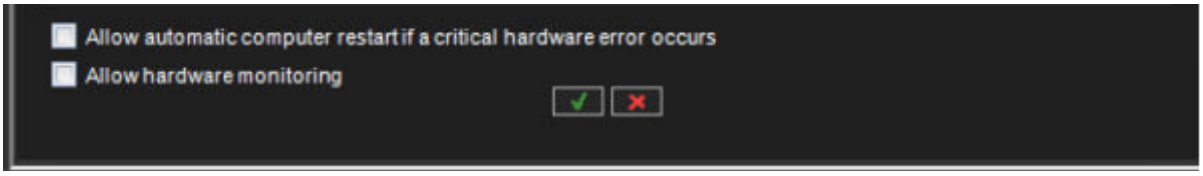
In watchdog settings, you can select what events trigger a report to be sent to e-mail addresses specified in E-Mail Settings (see page 36)
You can select different events for each server.
Alternatively, you can select the same events for all servers by selecting **All VMS Servers** from the drop-down list.
In addition to e-mail notifications, notifications can be performed through digital outputs.
All event types are written to the watchdog logs, regardless of the e-mail settings.

### 8.5.1.1 To add or remove events on the notification list:

1. On the **System** tab, select **Watchdog settings**.
2. Mark the **Send mail** checkbox for each event type for which a notification e-mail should be sent.
3. Click **OK**.

### 8.5.1.2 Automatic restart

Select the check box. **Allow automatic computer restart if a critical hardware error occurs** to restart the computer when serious hardware errors occur automatically.
The computer will not be restarted more than once a day.
Select **Allow hardware monitoring** if needed.




### 8.5.1.3 Digital output notifications

In addition to e-mail notifications, notifications can be performed through digital outputs.
Notifications through digital output are created as server-specific; you need to select a specific server from the **VMS Server** drop-down list.

To set a digital output notification:

1. On the **System** tab, select **Watchdog settings**.
2. Select a server from the **VMS Server** drop-down list. As digital output signals are server-specific, you cannot select **All VMS Servers**.
3. Click on an event.

4. Select the digital output channel you want to use from the **In Use** drop-down menu.
5. If you want to send a pulse signal to the output channel, mark the **Pulse** checkbox and select the pulse length with the slider.
6. Click **OK**.

## 8.5.2 Watchdog log

By default, the system shows the watchdog logs from all servers.
However, you can select one or several servers from the list on the left.
You can sort the logs by clicking the column headings.
To update the list without closing the window, click the **Refresh** button.

### 8.5.2.1 Additional Watchdog Delivery Methods

The Watchdog functionality includes three new protocols: TCP, SMS (requires an external SMS module), and customizable e-mail form.

Each new protocol has its driver:

C:\Program Files\DVMS\DVR\WDEventProviders\

- WDEventProviderSMS.xml
- WDEventProviderSMTP.xml
- WDEventProviderTCP.xml

At this moment, these files need to be edited manually. Each XML file contains the documentation regarding the configuration options.
The new configuration options include filtered and conditional warnings (i.e. “send warning X only once in every 60 minutes” or “send warning X only if condition Y is not met in two minutes”), and customizable warning message format.
After the files have been edited, Watchdog needs to be restarted for the changes to take effect.

***Note**: This feature is recommended only for advanced users. XML files are highly vulnerable to spelling errors and mistyped strings and keys.*
*Even a tiny error can cause fatal errors. Mirasys takes no responsibility for XML errors caused by editing the files.*

## 8.5.3 Watchdog event list

| Id | Event | Description |
|---|---|---|
| 0 | SmServerDown | WDServer detected that SMServer process stopped |
| 1 | SmServerUp | WDServer detected that SMServer process started |

| Id | Event | Description |
|---|---|---|
| 2 | DvrServerDown | WDServer detected that DVRService process stopped |
| 3 | DvrServerUp | WDServer detected that DVRServer process started |
| 4 | NetworkDown | WDServer detected that network is down |
| 5 | NetworkUp | WDServer detected that network is up |
| 6 | DvrStatusOK | WDServer got ok status from recorder |
| 7 | DvrRefreshing | WDServer got settings refreshing status from recorder |
| 8 | DvrVideoCaptureLoadFailure | WDServer got video capture driver load error status from recorder |
| 9 | DvrAudioCaptureLoadFailure | WDServer got audio capture driver load error status from recorder |
| 10 | DvrDataCaptureLoadFailure | WDServer got text data driver load error status from recorder |
| 11 | DvrNoFileSystem | WDServer got no file system status from recorder |
| 12 | DvrDiskFailure | WDServer got disk failure status from recorder |
| 13 | VideoChannelOK | WDServer got video channel ok status from recorder |
| 14 | VideoChannelNoSignal | WDServer got video channel no signal status from recorder |
| 15 | VideoChannelNotStarted | WDServer got video channel not started status from recorder |
| 16 | VideoChannelNoCapture | WDServer got video channel no capture status from recorder |

| Id | Event | Description |
|---|---|---|
| 17 | AudioChannelOK | WDServer got audio channel ok status from recorder |
| 18 | AudioChannelNoSignal | WDServer got audio channel not started status from recorder |
| 19 | AudioChannelNotStarted | WDServer got audio channel no capture status from recorder |
| 20 | AudioChannelNoCapture | WDServer got audio channel not started status from recorder |
| 21 | DataChannelOK | WDServer got text data channel ok status from recorder |
| 22 | DataChannelNoSignal | WDServer got text data channel not started status from recorder |
| 23 | DataChannelNotStarted | WDServer got text data channel no capture status from recorder |
| 24 | DataChannelNoCapture | WDServer got text data channel not started status from recorder |
| 25 | WDConnectionDown | Connection between WDServer and SMServer is down |
| 26 | WDConnectionUp | Connection between WDServer and SMServer is up |
| 27 | DvrSecurityFailure | WDServer got security failure status from recorder |
| 28 | DvrOtherInitFailure | WDServer got other initialization status from recorder |
| 29 | DvrArchiveFailed | WDServer got archive failed status from recorder |
| 30 | DvrMapNetworkDriveFailed | WDServer got map network drive failed status from recorder |

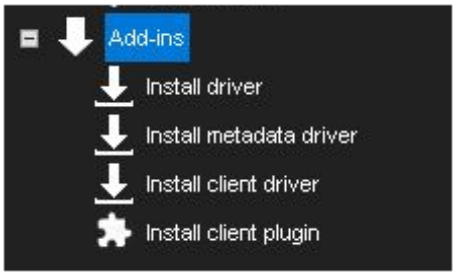
| Id | Event | Description |
|---|---|---|
| 31 | DvrInsufficientDiskSpace | WDServer got insufficient disk space status from recorder |
| 32 | DvrNASDiskConnectionLostFailure | WDServer got NAS disk connection lost status from recorder |
| 33 | DvrNASDiskInitializationFailure | WDServer got NAS disk initialization failed status from recorder |
| 34 | SMServerDBConnectionLost | SMServer has detected that database connection lost |
| 35 | SMServerDBConnectionRestored | SMServer has detected that database connection is restored |
| 36 | SMServerAuditTrailCacheFull | SMServer has detected that audit trail cache is full |
| 37 | DvrTemperatureLpcOk | NOT IN USE |
| 38 | DvrTemperatureLpcWarning | NOT IN USE |
| 39 | DvrTemperatureLpcFailure | NOT IN USE |
| 40 | DvrTemperatureCpuOk | NOT IN USE |
| 41 | DvrTemperatureCpuWarning | NOT IN USE |
| 42 | DvrTemperatureCpuFailure | NOT IN USE |
| 43 | DvrTemperatureHddOk | WDServer has detected that HDD temperature is ok |
| 44 | DvrTemperatureHddWarning | WDServer has detected that HDD temperature is in warning level |
| 45 | DvrTemperatureHddFailure | WDServer has detected that HDD temperature is in failed level |

| Id | Event | Description |
|---|---|---|
| 46 | DvrTemperatureDisplayAdapterOk | NOT IN USE |
| 47 | DvrTemperatureDisplayAdapterWarning | NOT IN USE |
| 48 | DvrTemperatureDisplayAdapterFailure | NOT IN USE |
| 49 | DvrTemperaturePsuOk | NOT IN USE |
| 50 | DvrTemperaturePsuWarning | NOT IN USE |
| 51 | DvrTemperaturePsuFailure | NOT IN USE |
| 52 | DvrTemperatureAcpiOk | NOT IN USE |
| 53 | DvrTemperatureAcpiWarning | NOT IN USE |
| 54 | DvrTemperatureAcpiFailure | NOT IN USE |
| 55 | DvrTemperatureRamOk | NOT IN USE |
| 56 | DvrTemperatureRamWarning | NOT IN USE |
| 57 | DvrTemperatureRamFailure | NOT IN USE |
| 58 | DvrMetadataDatabaseConnectionError | WDServer got metadata database connection error status from recorder |
| 59 | GatewayUp | WDServer has detected that Gateway service is started |
| 60 | GatewayDown | WDServer has detected that Gateway service is stopped |
| 61 | DvrFatalRuntimeError | WDServer got fatal runtime error status from recorder |

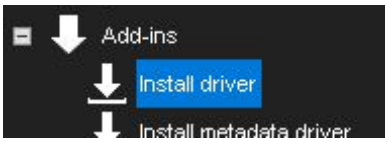
| Id | Event | Description |
|---|---|---|
| 62 | SMSServerUp | WDServer has detected that SMSServer service is started |
| 63 | SMSServerDown | WDServer has detected that SMSServer service is stopped |
| 64 | LicenseIsAboutToExpire | SMServer has detected that license is about to expire |
| 65 | LicenseHasExpired | SMServer has detected that license is expired |
| 66 | AutomaticBackupFailed | Automatic backup generation has failed in SMServer |
| 67 | DvrBrokenAtMaintenance | Recorder failure has been detected on maintenance mode and failover is ignored |
| 68 | DvrBrokenAndChangedWithFailoverDvr | Recorder failover has occurred |
| 69 | DvrBrokenWithoutPossibilityToChangeWithFailoverDvr | Recorder failure has been detected but there is no free failover servers |
| 70 | RPMServerUp | NOT IN USE |
| 71 | RPMServerDown | NOT IN USE |
| 72 | PublicWebApiServerUp | NOT IN USE |
| 73 | PublicWebApiServerDown | NOT IN USE |
| 74 | ExportServerUp | WDServer has detected that Export service has started |
| 75 | ExportServerDown | WDServer has detected that Export service has shutdown |
| 76 | StorageLockerServerUp | WDServer has detected that Storage Locker service has started |

| Id | Event | Description |
|---|---|---|
| 77 | StorageLockerServerDown | WDServer has detected that Storage Locker service has shutdown |
| 78 | IncidentReportingServerUp | WDServer has detected that Incident Reporting service has started |
| 79 | IncidentReportingServerDown | WDServer has detected that Incident Reporting service has shutdown |
| 80 | DvrFailbackDone | Recorder failback operation has been performed successfully on SMServer |
| 81 | DvrFailbackFailed | Recorder failback operation has failed on SMServer |
| 82 | DvrFailbackOnMaintenance | Recorder failback operation has been ignored because recorder is in maintenance mode |

## 8.6 Add-ins




### 8.6.1 Installing External Driver Packages




To use IP cameras, digital I/O devices or text data in the VMS system, the driver for each device must be installed on the server.
The software includes all drivers and plugins that have been included in the previous versions of the software.
However, if necessary, new drivers and plugins can be installed manually.
To install a new driver, you need a device-specific driver installation package.
The driver installation package is a compressed (zipped) folder that contains the driver files.

When installing a driver installation package, the system compares the files in the installation package to the existing files on the servers.
It usually installs the files only if they do not exist on the servers or if the files in the installation package are newer than the files on the servers.
However, you can force the system to install any driver version if necessary.

***Note**: If you want to update an already existing camera driver, remove the camera from the system before updating the driver.After removing the camera, install the driver file, after which you can reinstall the camera.After installing a new driver, you need to configure the devices that use the driver.*

To install a driver package:

1. On the **System** tab, under **Add-ins**, open **Install driver**.
2. Select the drive where the driver package is located, find and select the driver package (.zip file). The **Install Driver** dialogue box is shown.


3. Select the servers on which you want to install the driver.

4. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**

5. Click **Install**. The **Status** column shows the text **Installed** if the driver is successfully installed. If the driver is not installed, the column shows an error message.

6. Click **Close** to exit the dialogue box.

**Notes***:*

- If you need to update drivers for hardware other than IP cameras, please contact the system supplier.
- A 32-bit system requires a 32-bit driver package, and a 64-bit system required a 64-bit driver package.

## 8.6.2 Installing Metadata Drivers

It is possible to update and install new metadata drivers using the **Install metadata drivers** –option in the **System** tab.

## 8.6.3 Installing Client Drivers

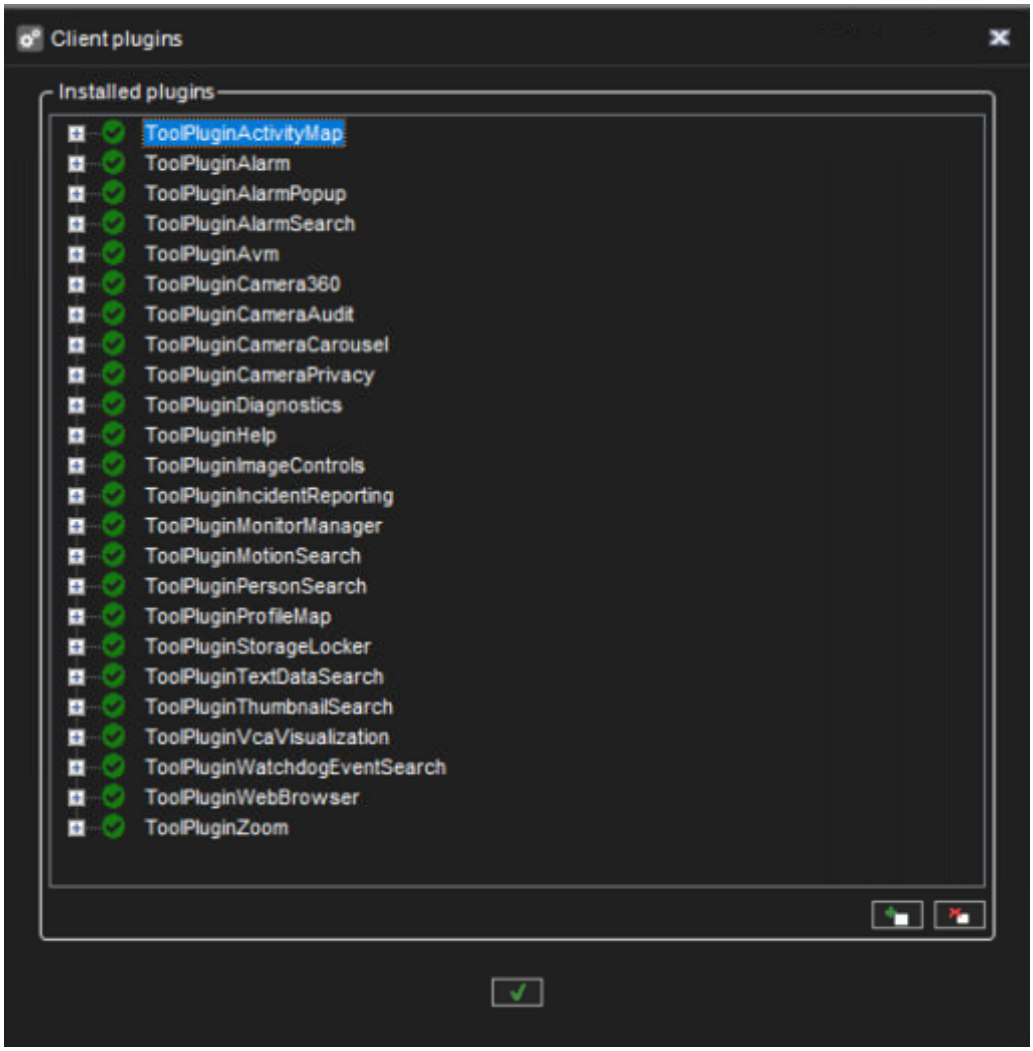
TruCast (direct streaming from camera to Spotter client) requires a different type of camera driver.

These are called (Managed) TruCast Client drivers.

The client camera drivers are installed similarly as spotter plugins and metadata drivers, using the **Install client driver** option in the system manager.

## 8.6.4 Install client plugin

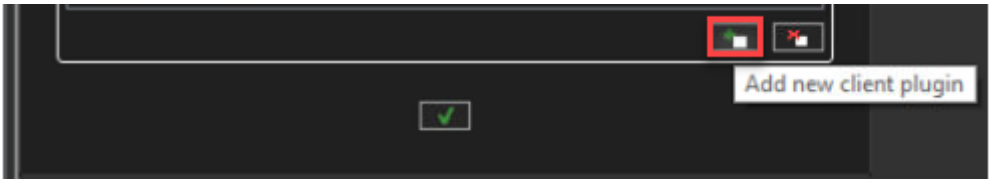
Client plugins for user interfaces such as Spotter can be installed through System Manager.




Plugin installation can be opened from the system tab under Add-ins.

### 8.6.4.1 To install a client plugin:

1. Open the **Install client plugin**.
2. Click **Add new client plugin**. Browse for the correct file and select it.

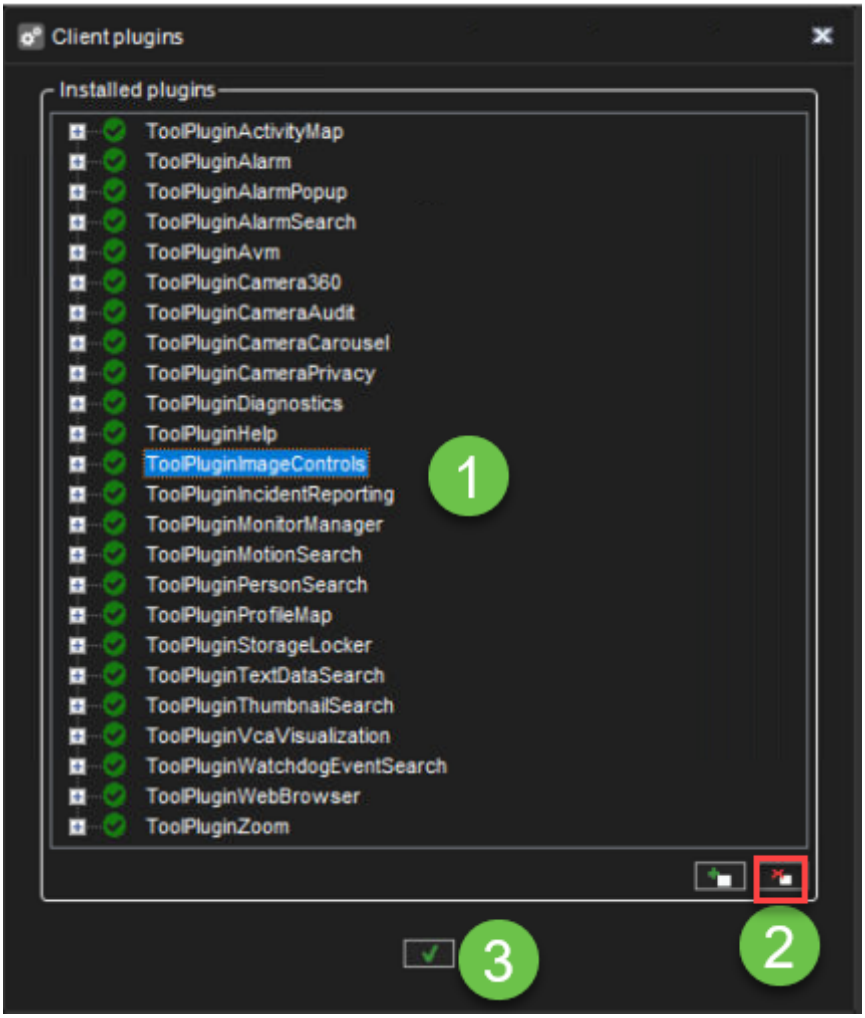



1. Find and select the plugin package (.zip file) and click **OK**. The **Install Plugin** dialogue box is shown.
2. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**
3. Click **Ok**

### 8.6.4.2 To remove a client plugin:

Open the **Install client plugin**

1. Select plugin from the list
2. Click **Remove client plugin**
3. Click **Ok**


Client plugins
Installed plugins
ToolPluginActivityMap
ToolPluginAlarm
ToolPluginAlarmPopup
ToolPluginAlarmSearch
ToolPluginAvm
ToolPluginCamera360
ToolPluginCameraAudit
ToolPluginCameraCarousel
ToolPluginCameraPrivacy
ToolPluginDiagnostics
ToolPluginHelp
ToolPluginImageControls
ToolPluginIncidentReporting
ToolPluginMonitorManager
ToolPluginMotionSearch
ToolPluginPersonSearch
ToolPluginProfileMap
ToolPluginStorageLocker
ToolPluginTextDataSearch
ToolPluginThumbnailSearch
ToolPluginVcaVisualization
ToolPluginWatchdogEventSearch
ToolPluginWebBrowser
ToolPluginZoom
1
2
3

# 9 The VMS Servers

On the **VMS Servers** tab, you can configure these settings for each server:

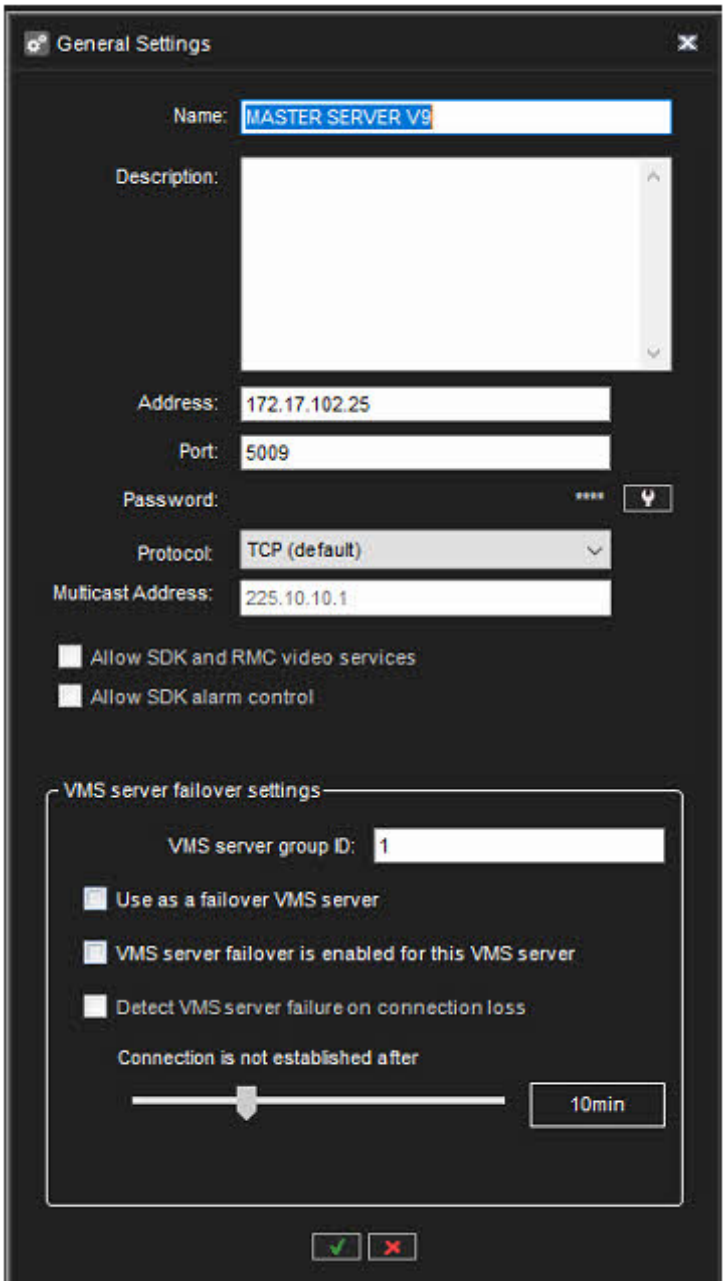
| Icon | Name | Description |
|---|---|---|
|  | General | Change the name and the description of the server. Here you will also find the IP address of the server. |
|  | Port forwarding | Users can see what the automatic port forwarding has configured as ports for this server. The ports can be changed if necessary. |
|  | Hardware | Add IP cameras and select camera and audio drivers. |
|  | Cameras | Change camera parameters, recording schedules and motion detection settings. |
|  | Audio | Change audio detection settings and recording schedules. |
|  | Digital I/O | Set digital I/O settings. |
|  | Alarms | Set up alarm conditions and alarm actions. |
|  | Storage | Add a hard disk to a server and set the storage times for video, audio, and alarm files. |
|  | Text channels | Set the names and descriptions of text data channels here. |

To access the settings, do one of the following:

- Select the settings you want to configure (for example, Cameras) and then click Edit in the lower-right corner of the navigation pane.
  
- Double-click the settings that you want to configure.
- Drag the settings from the **VMS Servers** tab to the workspace.

## 9.1 General

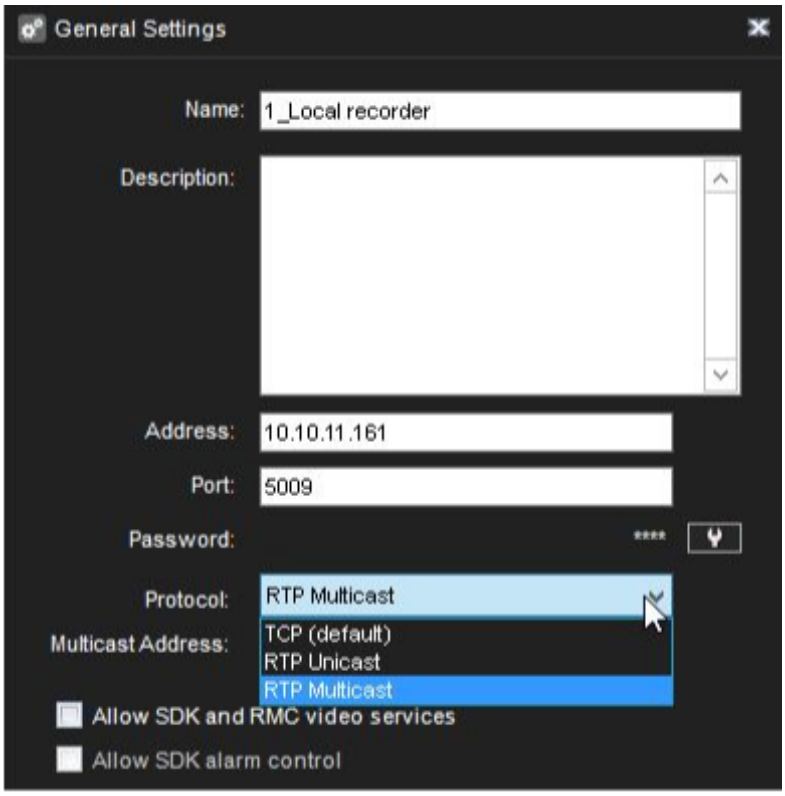
- VMS server name
- Description
- Password
- Protocol
- Multicast Address
- VMS server failover settings




### 9.1.1 Multicast address

When a single workstation stream is opened multiple times, the server – and the network – face unnecessary strain as each stream is treated as a separate entity.
Multi-casting enables a single stream to be opened and sent to multiple workstations simultaneously.
When using multi-casting, the stream for each video channel is sent to the LAN only once.
All applications on the LAN can receive the single stream, so network bandwidth usage is lower than when sending a stream for each application separately.
The feature needs to be configured in System Manager and through network settings.
Please refer to your network infrastructure service for information on enabling multi-casting support on the network level.

To configure multi-casting in System Manager:




1. In the server's General settings, change the protocol from **TCP (default)** to **RTP Multicast**.
2. Edit the multicast address.
3. Repeat steps 1-2 for all required servers in the system. Note: Each multicast address needs to be separate.

### 9.1.2 VMS server failover settings

When adding a new server to the system, it can be defined to be a failover server.
A failover server is a backup server that shall assume any server duties determined to be under failover protection.

Failover servers must have the same file system (same drive letters) as the VMS Servers under failover protection, and they can only be used for IP camera backup purposes.

When in standby mode, failover servers appear under a separate folder in the *VMS Server* list.
When any VMS Server is deemed to be broken or inaccessible, they have moved under the *"Broken VMS Servers"* folder.

Any available failover server shall take the responsibilities of the failed server.
Failover settings can be controlled from the general settings of the selected server.
The failover transition is done if all material disks are broken or the server is inaccessible for longer than a defined period.

### 9.1.3 Use as a failover VMS server

This setting define that the server is used as a failover VMS server

### 9.1.4 VMS Server failover is enabled for this VMS server

This setting defines the selected server role that will be transferred to the failover server during the error situation

### 9.1.5 Delay failover to prevent data loss

During material copy from the failover recorder, the restored recorder checks its recorded data first, then copies only missing material (including video, audio, text data, metadata, and ANPR data).

This functionality can be enabled in the System Manager > VMS Servers General dialog, checkbox *Wait for the recorder to apply settings*).

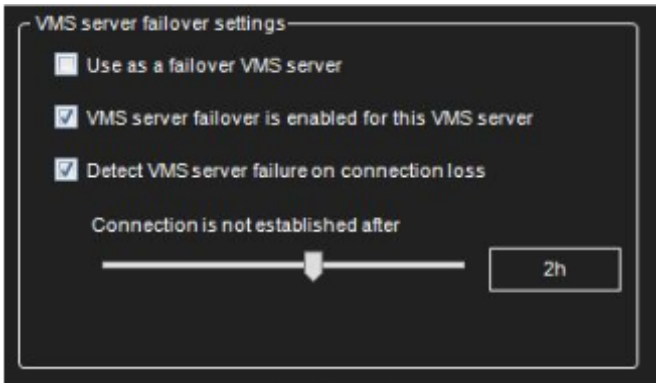
> Delay Failover can be enabled only for recorders V9.7 or newer, as recorders pre-V9.7 do not support selective material copy, and data will overlap.

### 9.1.6 Use automatic failback

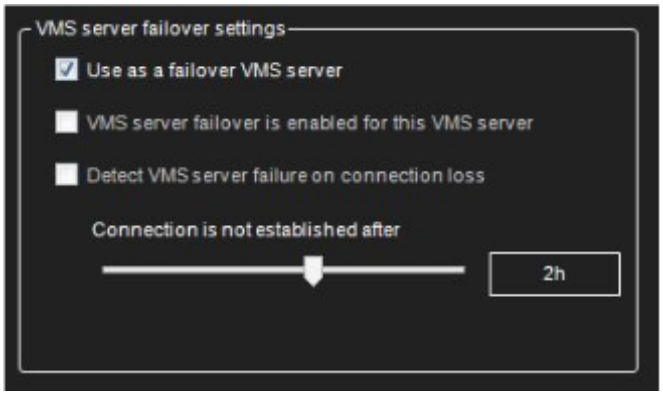
This setting enables the automatic failback feature to this server

### 9.1.7 Use automatic material copying

This setting enables the automatic material copying feature to this server




For example, under failover protection, if inaccessible for longer than 2 hours, the failover switch would happen.




## 9.2 Port Forwarding

*The basic idea with port forwarding is that it* can access one or more VMS Servers or Master Servers behind a router that does Network Address Translation (NAT).

Typically, this situation happens when the client is outside the network and needs to access servers inside a company network.When installing a VMS Server, the installer offers the option to turn on the automatic port forwarding. The default state is off
If the port forwarding is not activated when the system is installed, it can be activated from the second tab, “VMS Servers”.
Open the view “Port forwarding” and activate the selection “UPnP is in use.”

### 9.2.1 Automatic Router Configuration

*When a* VMS Server starts up, it tries to discover UPnP devices from the network.
The router needs to support UPnP (Universal Plug and Play), which must be enabled on the device.
The server has continuous UPnP device discovery when running, so if any network changes are done, the server will automatically detect new routers and do port forwarding to them.
Only UPnP devices with external (WAN) addresses are detected.

If the user wants to remove port forwarding automatically, he can do this from the system manager.
After this, the server will remember that the settings were removed and not port forward to this router.
The software does not allow to delete port forwarding mapping if the server is added to the system with an external address.

Deleting the port forward mapping would disconnect the system, and no further configuration would be possible.

If forward port settings are changed, and the connection to the server has not returned after a while, it might be necessary to reboot the router.

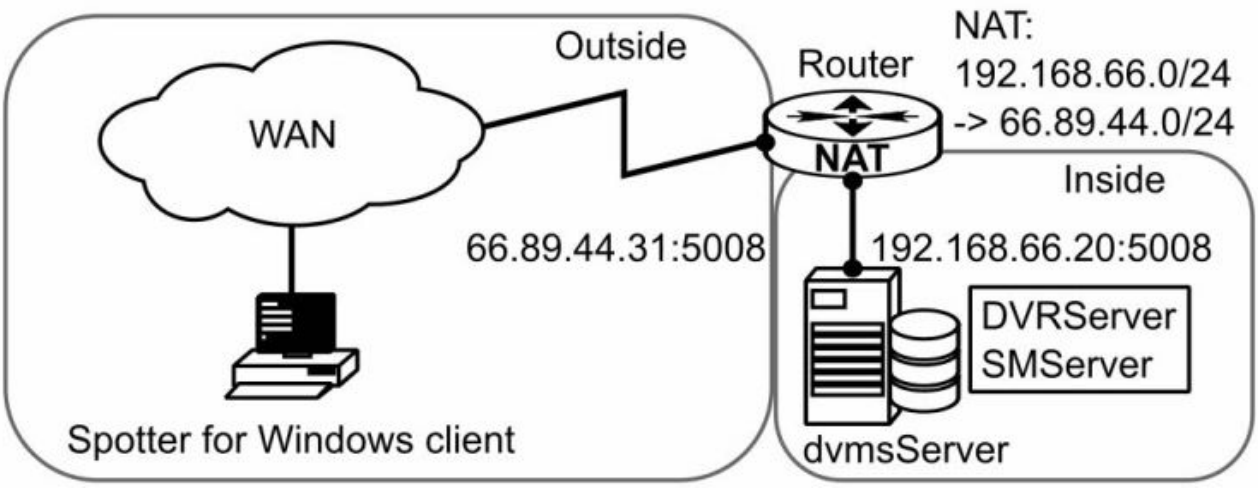
Servers need four ports for the server to server communication. The first server that does port forwarding will claim ports **5008**, **5009**, **5010** and **5011**.

The second server will claim ports **5012**-**5015**, the third server ports 5016-5019. And so on. (Assuming all the ports are available).

The first port is used for SMServer communication (**5008, 5012, 5016…**)
The second port is used for DVRServer process communication (**5009, 5013, 5017…**)
When connecting to a Master Server, the port is typically 5008. When adding new servers to the master, the port is typically 5009. If there are more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.

### 9.2.2 Single Server Behind Router

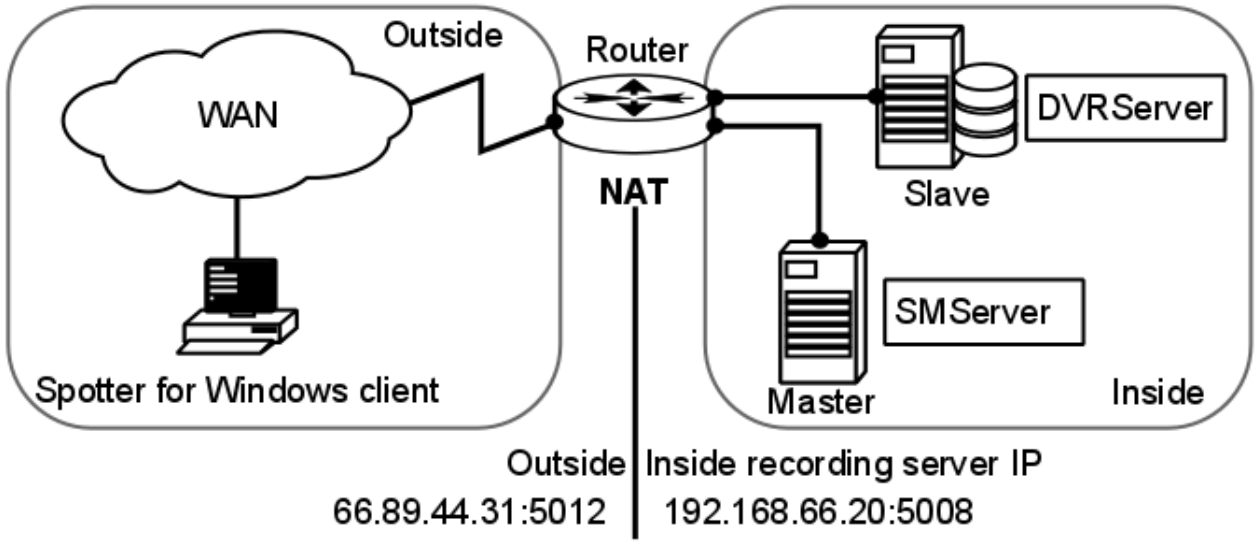
*Scenario 1: Using a system with* **a single server behind a router/firewall**




If the user is accessing a single server from the WAN, he needs to connect to the VMS Server with the outside IP address that the router has translated.
The user can check the port forwarding what the port in use is, but it is highly likely port 5008.

### 9.2.3 More Than One Server Behind Router

*Scenario 2: More than one server behind a single router (WAN address)*

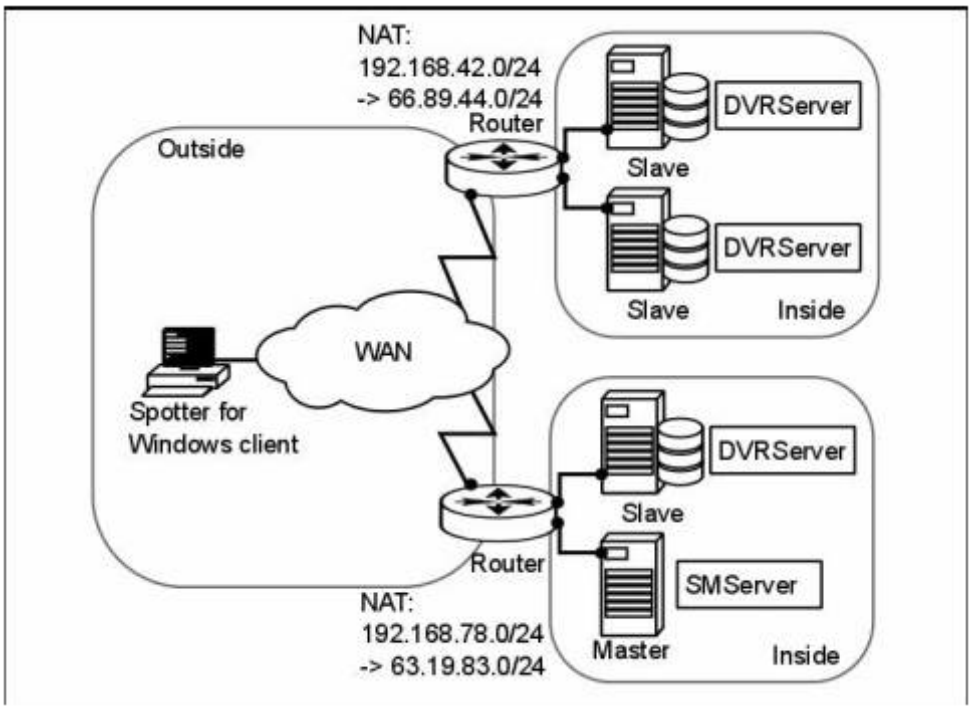



If the user configures a more extensive system with multiple servers on a single site, he can add the servers to the System Manager application with the external or internal IP addresses.
When adding a new VMS Server, if the server has done automatic port forwarding, a note shows that he can choose between an internal IP address and an external IP address.
If the server is to be used from the WAN, then the external IP address should be chosen.
The exact ports that the server has done port forwarding to can be found by starting the System Manager on the local server.

When adding a server to a Master Server when not on the local site (cannot use the local IP address), the user must know the external IP address and know the first port that the port forwarding was done to.
If the added server is a single, standalone server, the port is most likely 5009.
If multiple servers are on the same site, they most likely get the ports starting with **5009, 5013, 5017, 5021**…

### 9.2.4 More Than One Server On Multiple Sites

*Scenario 3: More than one server on more than one site*

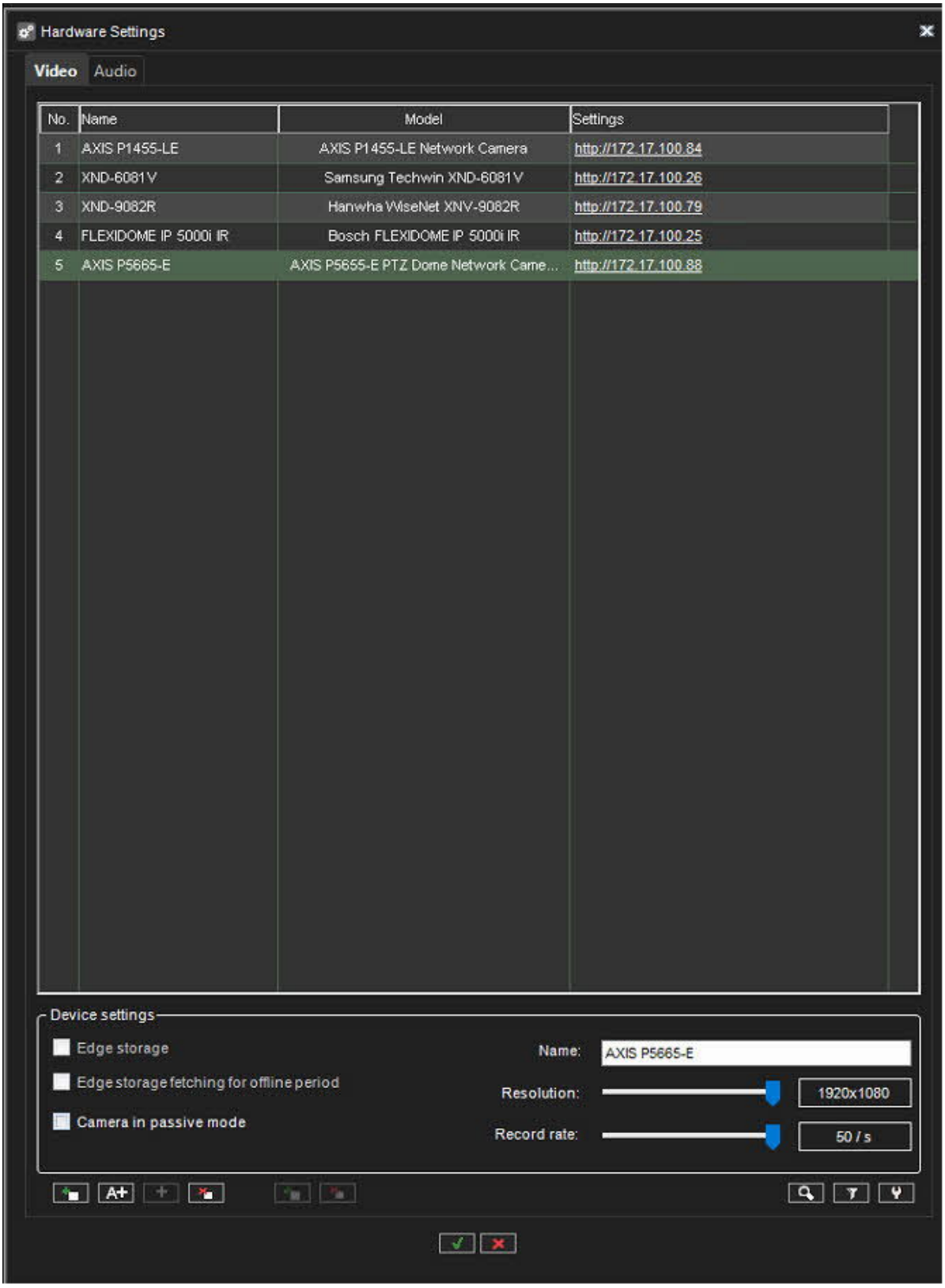



The same principle applies as in Scenario 2, but this time NAT needs to be taken into account when assigning VMS Servers to the Master Server from the other site.

## 9.3 Hardware

Before using the system manager application to search for the camera, please do the following actions:

- Configure the IP address to the camera
- Define the username and password to the IP cameras
- Check that the camera time zone and time is the same as the VMS server


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
AXIS P1455-LE
AXIS P1455-LE Network Camera
http://172.17.100.84
2
XND-6081V
Samsung Techwin XND-6081V
http://172.17.100.26
3
XND-9082R
Hanwha WiseNet XNV-9082R
http://172.17.100.79
4
FLEXIDOME IP 5000i IR
Bosch FLEXIDOME IP 5000i IR
http://172.17.100.25
5
AXIS P5665-E
AXIS P5655-E PTZ Dome Network Came...
http://172.17.100.88
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
AXIS P5665-E
Resolution:
1920x1080
Record rate:
50 / s
A+

Also the information about used/total license count and information about used/total channels for selected multi-channel device were added below the "Devices" list in the "Hardware settings" dialog.

## 9.3.1 Video

When adding an IP camera, the following search modes are available.

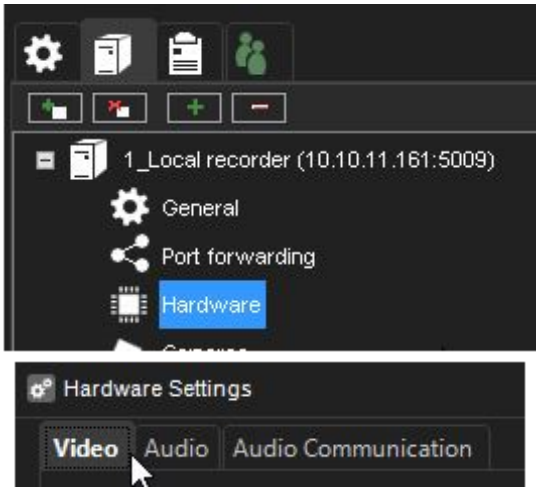
- ***All drivers***: Automatic search with all drivers. The system will attempt to use all available drivers. The mode option combo-box is disabled.
- ***Selected drivers***: Automatic search with specific drivers only. The system will use only the drivers specified via the Selected Drivers dialogue during the automatic search.
    - The additional combo box will show all drivers that are currently selected. A user may use all of them (using the “All” option) or select only one driver.
- ***Currently active drivers***: Search the camera using all drivers who are currently used. If this option is selected, the system will use only drivers currently used for already added cameras.
    - For example, if we have Sony and Axis cameras subscribed, the search will be done by Sony and Axis drivers only.
    - The mode option combo-box will contain a list of used drivers if the user wants to use one of them and an “All” option for using all drivers from this list for searching.
- ***Driver***: Add a camera using a specific driver. The system will use only the specific driver for search.
    - The mode option combo-box will contain a list of all installed driver names to search.
    - If a search with specified drivers fails, the system will prompt whether the user wishes to search using all drivers.
    - The driver currently used for the search also should be excluded.
- ***Camera model***: Add camera by model name. This mode is used for adding a camera by using an older capture driver using pre-defined capabilities from the driver configuration XML file.
    - The mode option combo box will contain a list of available models.

The ***Selected drivers*** -mode will be selected by default for adding the new camera for the first time.

Next time the dialogue is opened, the system will remember the previous model and driver selection to allow the user to add similar cameras faster.
Opening the existing camera using the Modify button will show a dialogue with the Currently active drivers search mode and driver name in mode option combo-box (except cameras added by mod, el of course).
The system will not store last used options for modifying cases because the options will be available for adding cameras only

### 9.3.1.1 Add device

IP cameras or analogue video servers (encoders) can be managed through the **Video** tab of **Hardware settings**.




To add a new IP camera when the IP address is known:

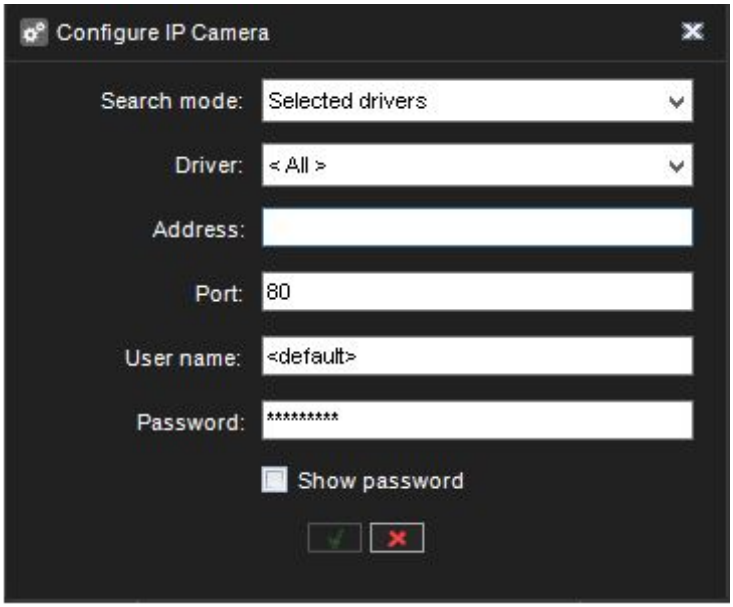
1. On the **Video** tab, click **Add device**


2. Type the IP address or DNS name of the camera or video server.

Change the port number if needed. Usually, port 80 is used.

3. Type the username and password for the camera.

4. Click **OK**.

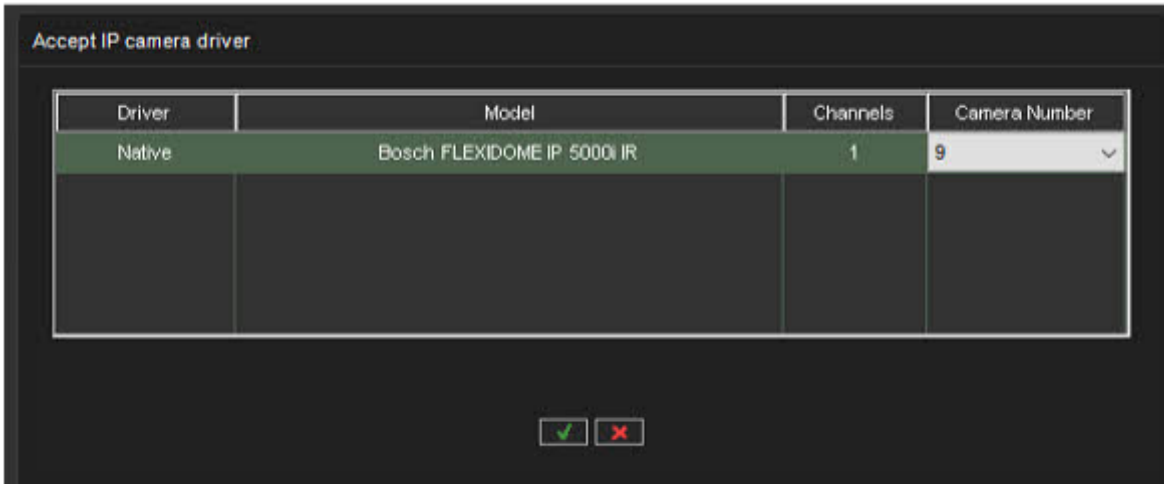



The system will now communicate with the camera and display which drivers can connect to the camera. The camera may support **ONVIF**. In this case, the **ONVIF** driver may also detect it.

5. Select a driver from the list.

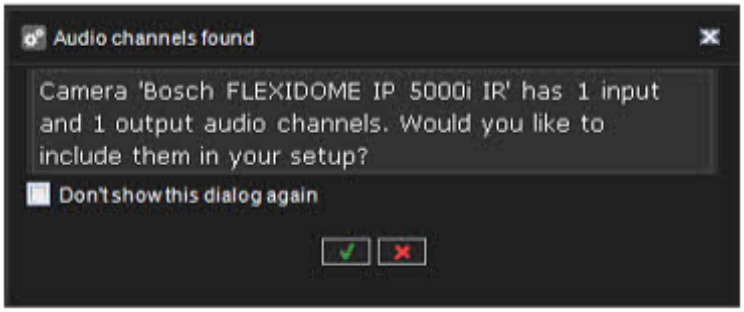
Typically, it is recommended to use the **Native** driver if it exists.
For multichannel devices, the **Channels** option can add the device with less than the maximum number of channels.
The user can also see what will be device camera number

6. Click **OK**

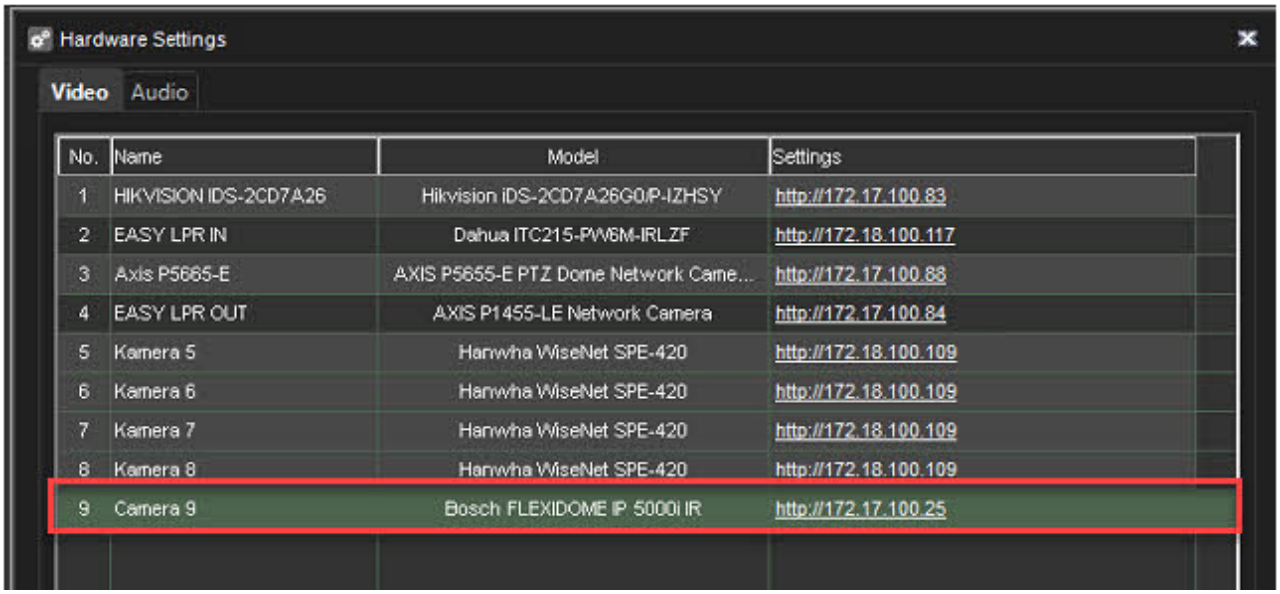


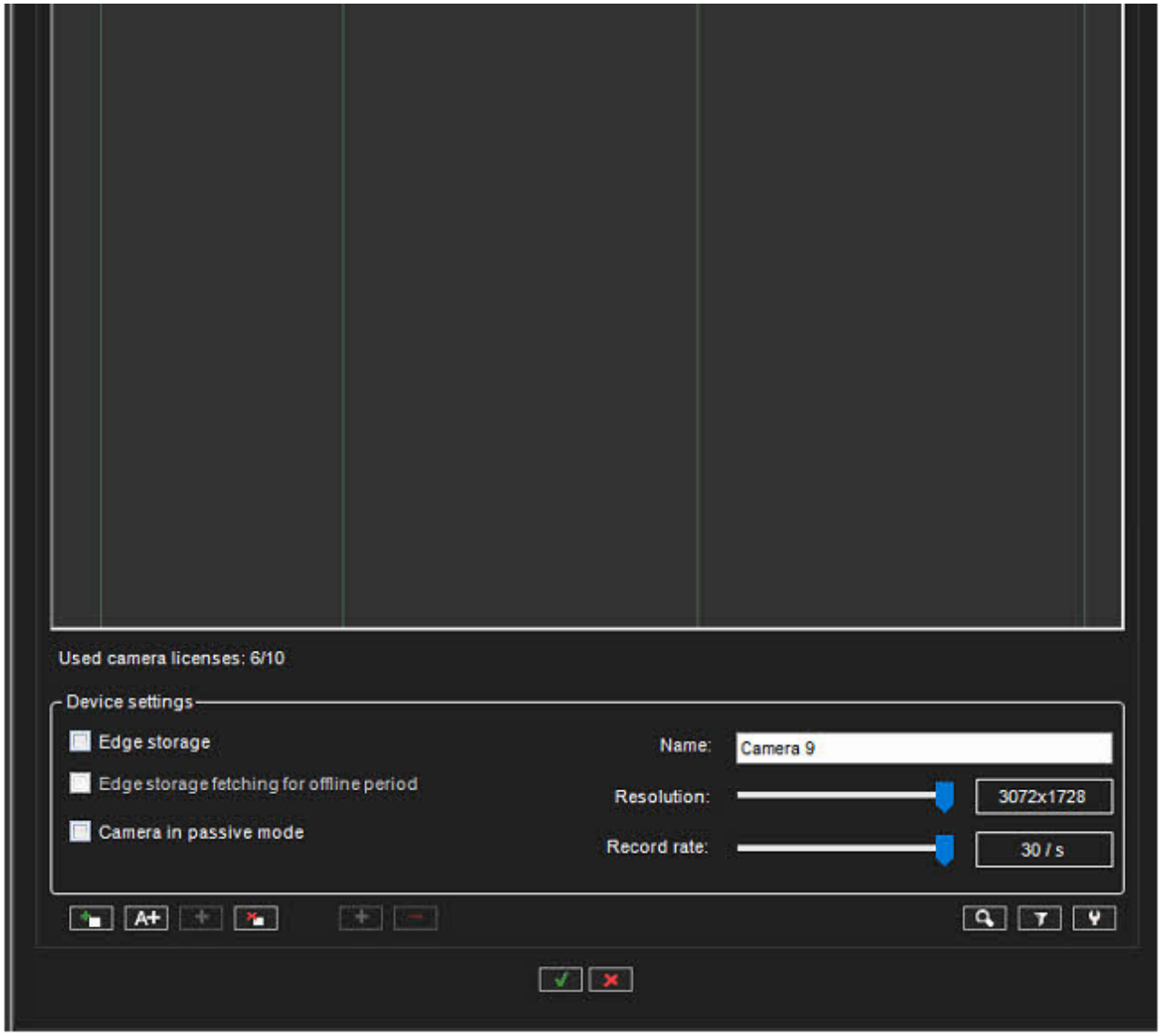

If the camera supports audio channels, you will see dialogue about this.

7. Click **OK** to add also audio channels or **X** add an only video channel




After the camera adding device can be found from the **Hardware settings** list





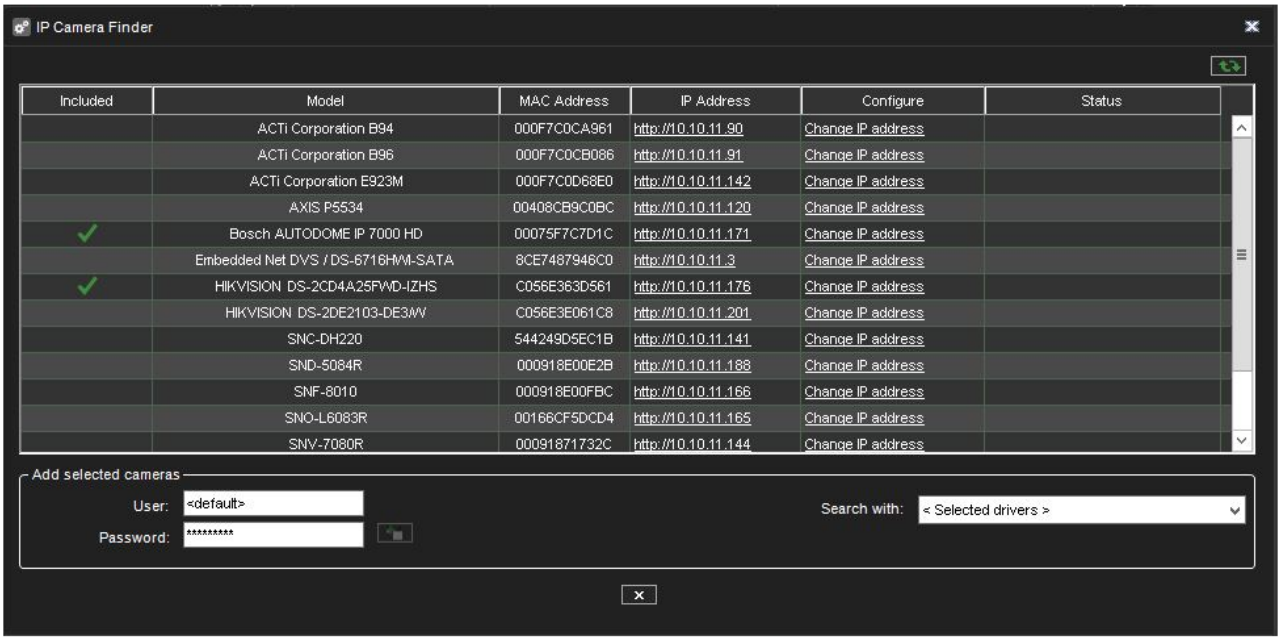

New device can be inserted to the empty "slot" if its number of channels is the same or less then number of consecutive "not used" camera numbers.

User can select channels that will be added during device acceptance. When he start device search and device is found, he will see the following dialog:

### 9.3.1.2 IP Camera Finder

1. Click the **IP camera finder**


The system will now scan the local IP network for active IP addresses and then communicate with each found IP address if it is a supported IP camera.
The resulting list is displayed after the search is complete.




Cameras can be selected from the list. Selecting multiple cameras is possible with SHIFT or CTRL keys.

1. Type the username and password for the cameras.
2. Click **Add Selected Cameras**.


3. The system adds the selected cameras to the system with the selected username and password.

4. If the system cannot add some of the selected cameras, an error status message is displayed in the **Status** column; you can repeat steps 4-5 for the cameras with the correct credential information.

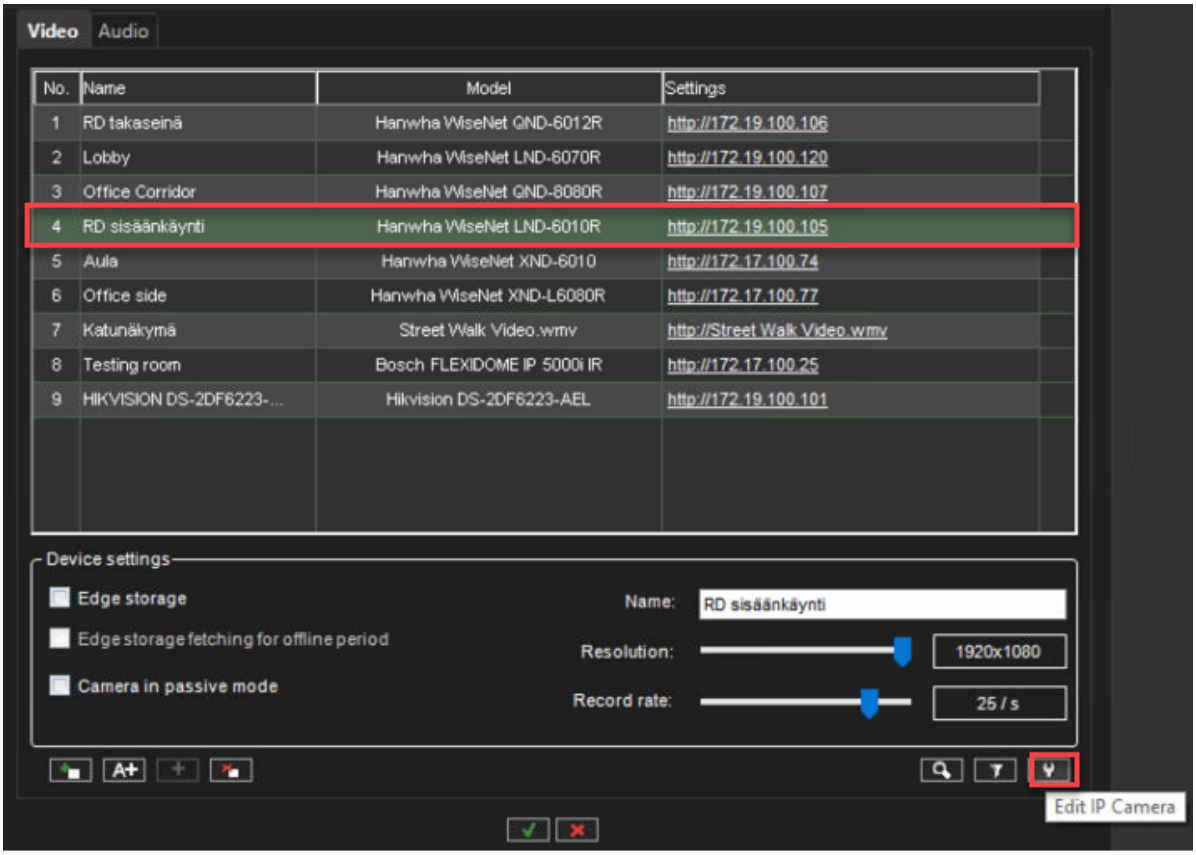
5. Click **Close** to exit the **IP camera finder**.

6. Save the Hardware settings by pressing **OK** in the list:

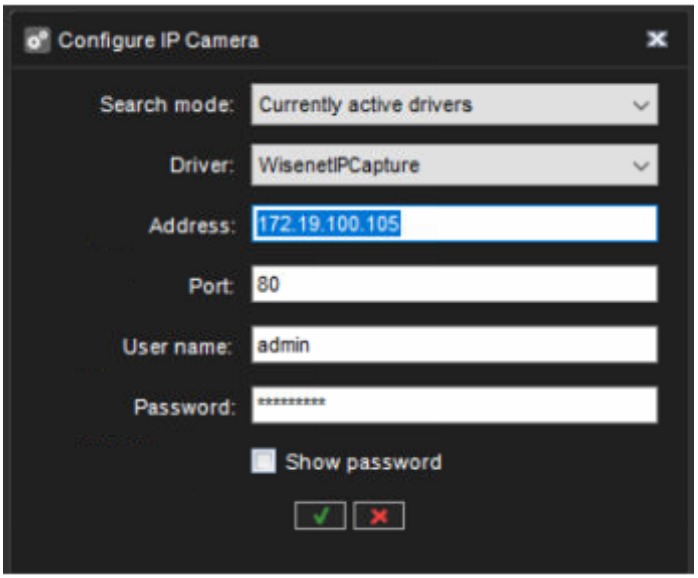

### 9.3.1.3 Edit IP Camera

Edit IP Camera allows users to change **camera address, port, username or password**

1. Select camera from the list
2. Click **Edit IP Camera**




1. Do needed modifications
2. Click Ok to confirm changes



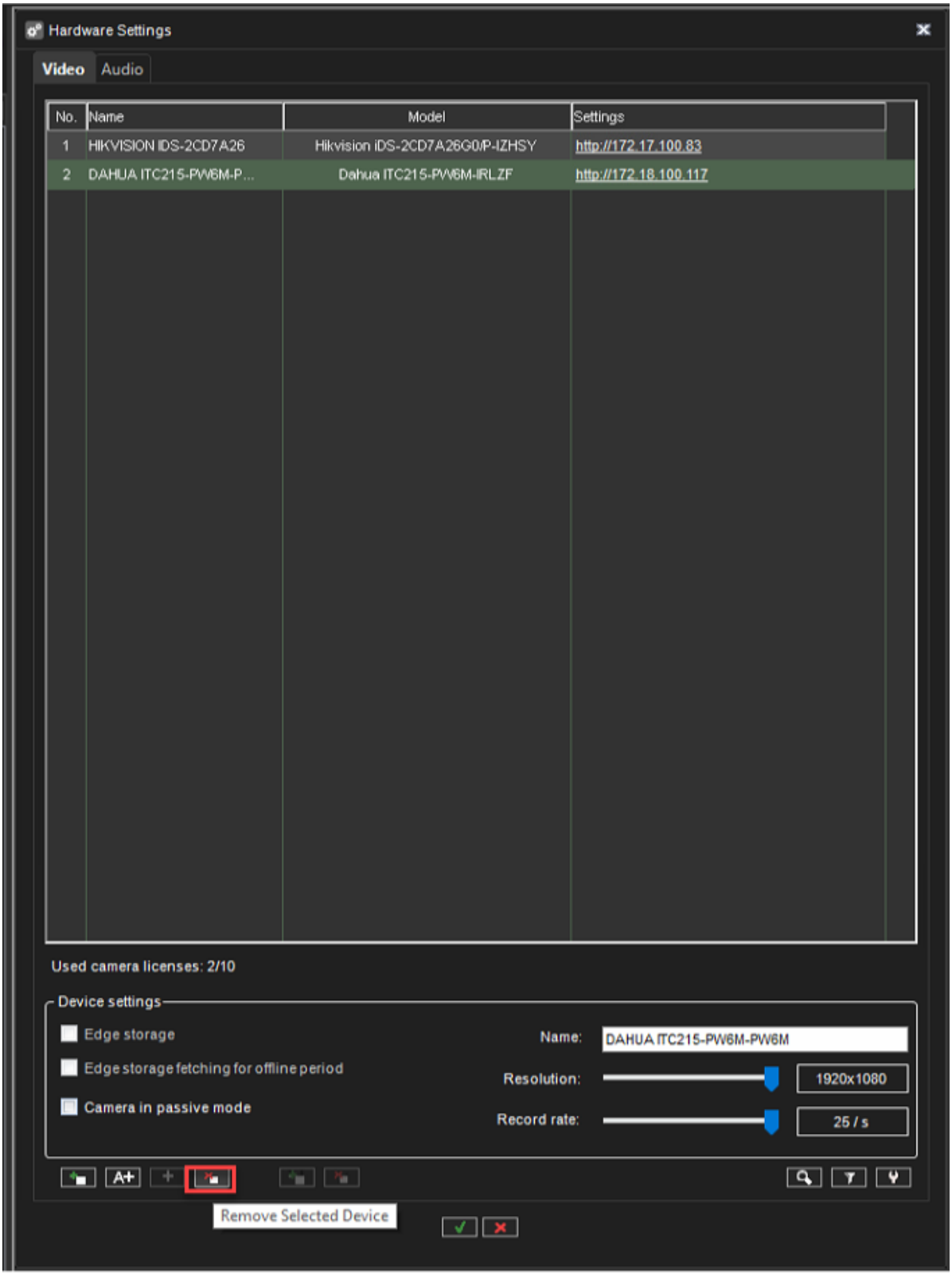
### 9.3.1.4 Removing IP cameras and encoders

If you open the "**Hardware Settings**" dialogue in System Manager, you will see 2 buttons below the list of cameras:

- The "**Add video channel to the selected device**" button
- The "**Remove video channel from the selected device**" button

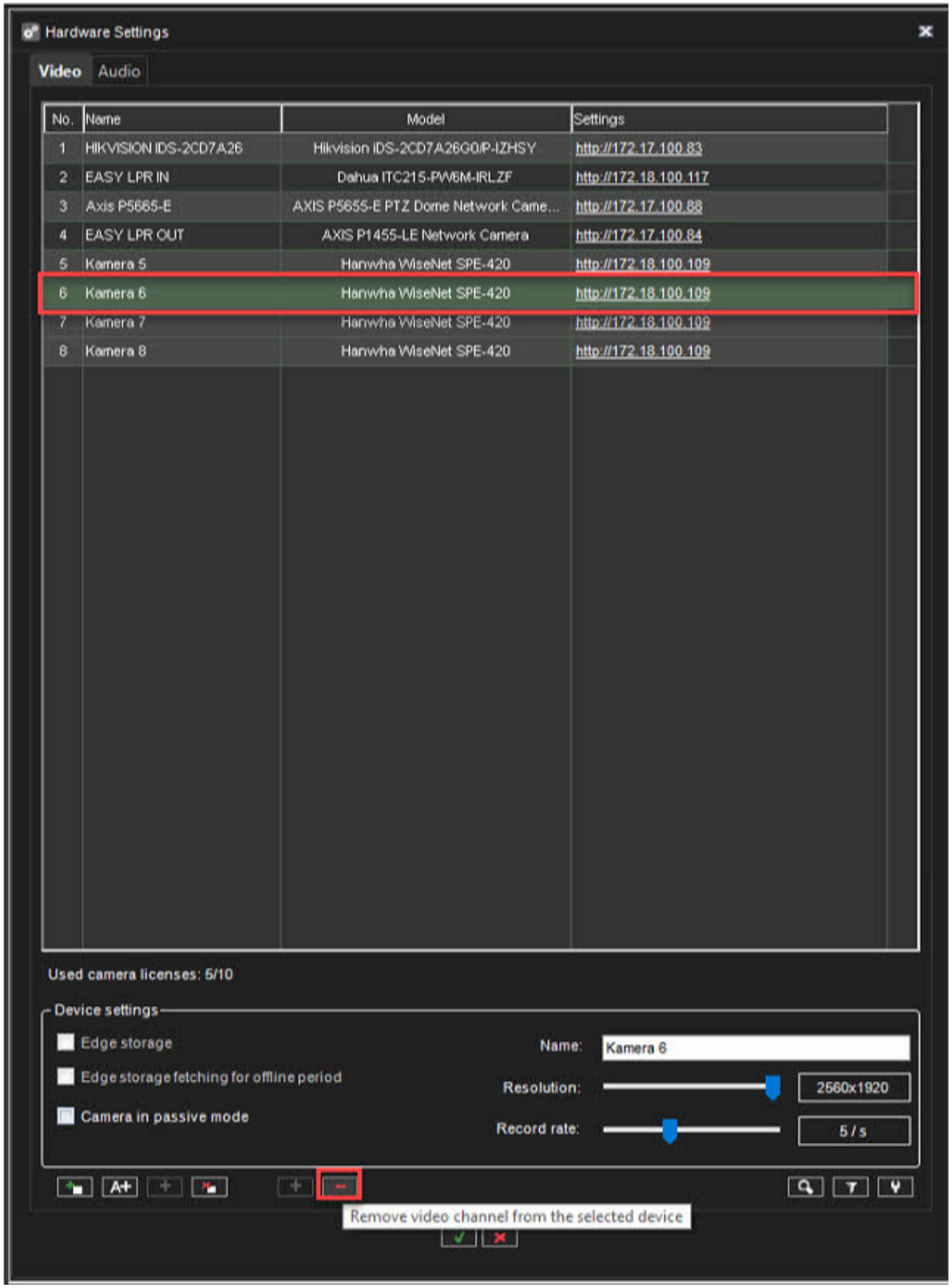
#### 9.3.1.4.1 To remove an IP camera:

1. Select camera from the list on the **Video** tab
2. Click **Remove Selected Device** in the lower right corner of the tab.
3. When asked to confirm the deletion, click **OK**.


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
HIKVISION IDS-2CD7A26
Hikvision iDS-2CD7A26G0/P-IZHSY
http://172.17.100.83
2
DAHUA ITC215-PW6M-P...
Dahua ITC215-PW6M-IRLZF
http://172.18.100.117
Used camera licenses: 2/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
DAHUA ITC215-PW6M-PW6M
Resolution:
1920x1080
Record rate:
25 / s
Remove Selected Device

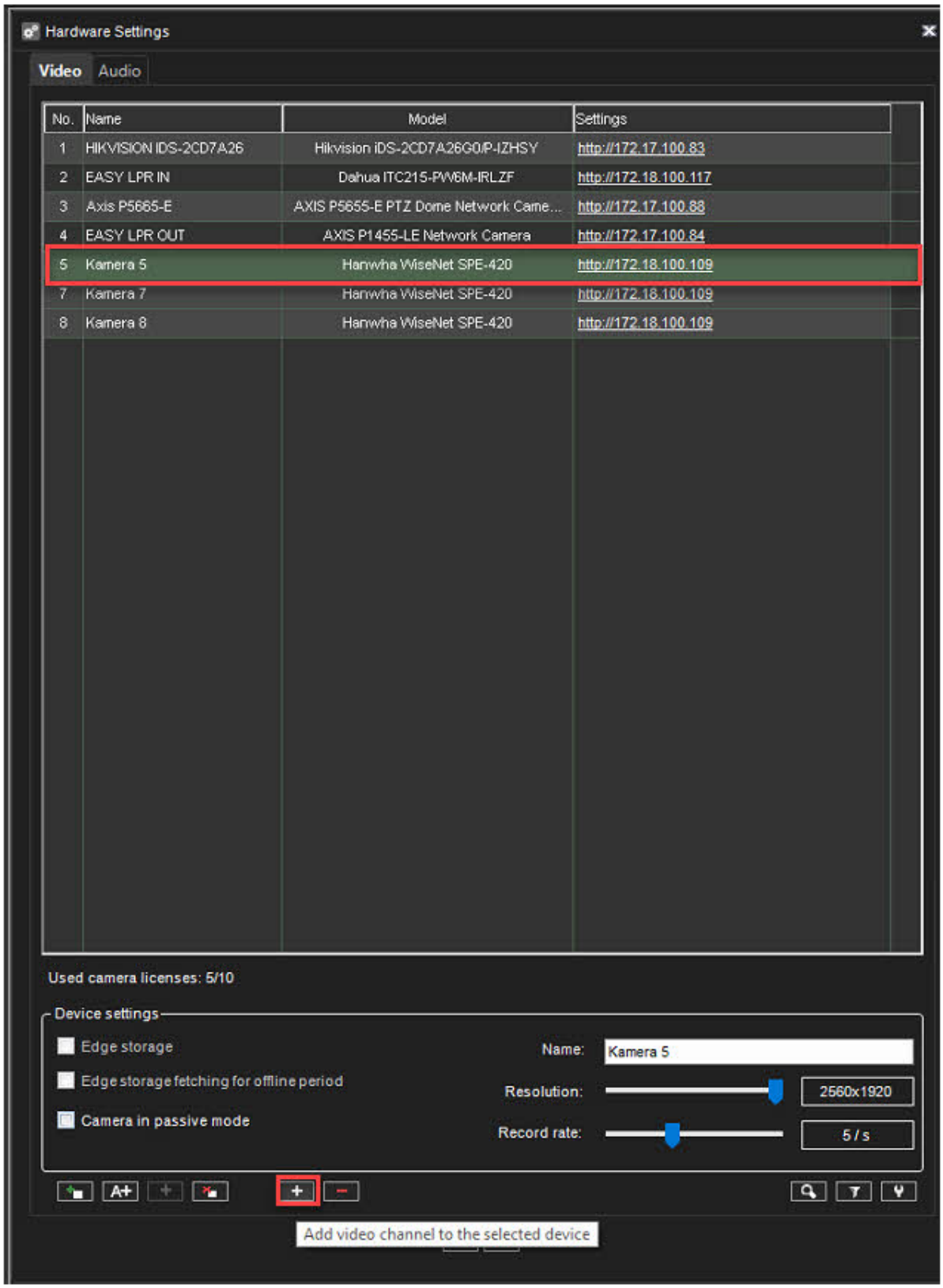
#### 9.3.1.4.2 To remove video channels from the encoder or multi-lens cameras:

1. Select the correct channel from the list
2. Click **Remove video channel from the selected device**
3. Click **OK**


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network Camera http://172.17.100.84
5 Kamera 5 Hanwha WiseNet SPE-420 http://172.18.100.109
6 Kamera 6 Hanwha WiseNet SPE-420 http://172.18.100.109
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
Used camera licenses: 5/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Kamera 6
Resolution:
2560x1920
Record rate:
5 / s
Remove video channel from the selected device

#### 9.3.1.4.3 To add video channels to the encoder or multi-lens cameras:

1. Select the correct device from the list
2. Click **Add video channel to the selected device**
3. Click **OK**

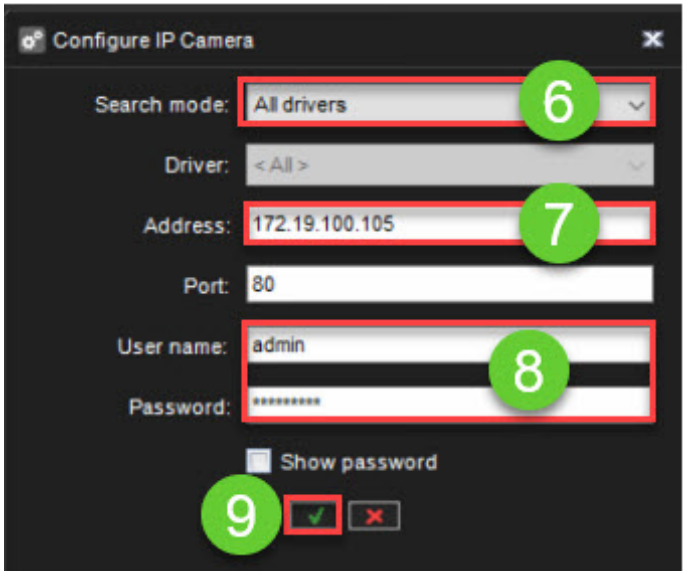

Hardware Settings
Video
Audio
No.
Name
Model
Settings
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network Camera http://172.17.100.84
5 Kamera 5 Hanwha WiseNet SPE-420 http://172.18.100.109
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
Used camera licenses: 5/10
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Kamera 5
Resolution:
2560x1920
Record rate:
5 / s
Add video channel to the selected device

### 9.3.1.5 Replacing an IP camera

#### 9.3.1.5.1 The user can replace an existing IP camera in the Mirasys VMS

- Add an existing IP camera address to the new IP camera
- Set same username and password to the new IP camera
- Connect camera to the network
- Select camera from the **Hardware** list
- Click **Edit IP camera**

1. Select **Search mode: All drivers**
2. Check that camera has correct IP address
3. Check that username and password are correct
4. Click **OK**
5. Select the correct driver from the **Accept IP camera driver** selection
6. Click **OK**




## 9.3.2 Audio

If a camera has compatible IP audio input or output channels, you can add them simultaneously when adding the camera through the automated search tools.
After IP audio inputs and outputs for a camera have been added to the system, they can be edited and removed through the **Audio** tab.

#### 9.3.2.1 Information shown:

1. Camera hardware ID
2. Channel type(Input)
3. Channel type(Output(
4. Device model


### 9.3.3 Device Settings

#### 9.3.3.1 Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in-network blackout, the video feed can be stored on an SD memory card on the camera.
Once the network connection has been re-established, video is transmitted from the camera's SD card to the server.
Please refer to the camera manufacturer documentation to see what cameras support the feature.
Edge storage must be enabled in the device settings.
This feature is configured solely through the camera's configuration utility.
Please refer to the camera's documentation for instructions on enabling Edge storage.

#### 9.3.3.2 Edge storage fetching for offline period

When this is enabled, then Mirasys VMS transfers recordings from the camera SD card only from the time of the period, when the connection has been lost between the Mirasys VMS and IP camera

#### 9.3.3.3 Camera in passive mode

- If multiple servers have the same camera configured, then one should be made **Active,** and the others should be **Passive**.
- This way, only the Active server settings are communicated to the camera.

#### 9.3.3.4 Camera information

Camera name, resolution and record rate can be set directly from the **Video** tab


### 9.3.4 Adding cameras by using CSV file

VSM camera settings can be exported to a CSV file and imported to VMS from a CSV file. This allows administrators to make bulk changes to camera settings and then import changed settings to the VMS system. It is also possible to add new cameras to VMS using this functionality.

#### 9.3.4.1 CSV file import and export

System Manager Hardware settings have the following buttons for exporting camera settings to a file and importing camera settings from a file in CSV format.

##### 9.3.4.1.1 CSV file format

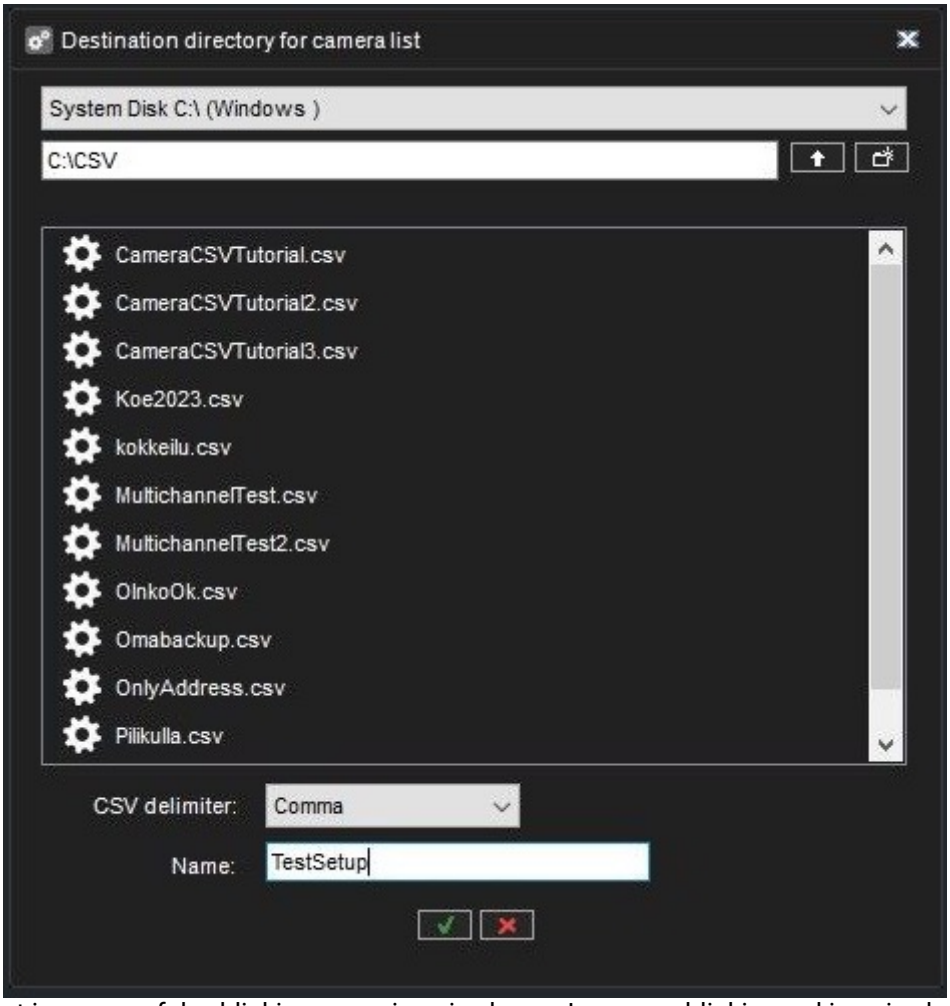
CSV file format for each camera uses the following header names.

- **Name** - Name of the camera channel.
- **Number** - Number of the camera channel on the VMS server.
- **Description** - Camera channel description.
- **AdmDescription** - Camera channel administrative description.
- **Address** - Camera device address.
- **Port** - Camera device port.
- **UserName** - Camera device user name.
- **Password** - Camera device password.

- **Driver** - Driver name / native (search from all available native drivers) / ONVIF (use of ONVIF driver). Logic uses the first driver that includes the given driver name string. For example, axis → NewAxisIPCapture.
- **Channel** - Used channel of the driver if the device supports more than one channel. With one-channel devices, this can be left empty.
- **IsInUse** - Is the camera in use?
- **IsAudioInUse** - Is audio in use if the driver supports it?
- **IsIOInUse** - Is I/O in use. This has meaning only when exporting CSV files. At import, I/O is used automatically if the device supports it.
- **Is360** - Is 360 camera.
- **Framerate** - Recording stream frames / second rounded to close available value. The header for other streams: Framerate1, Framerate2, Framerate3.
- **Resolution** - Recording stream resolution in format width x height (for example 1920x1080) rounded to close available value. For other streams: Resolution1, Resolution2, Resolution3.
- **Codec** - Recording stream used compression codec. Rounded to close available value: JPEG, MPEG, H264, WMC9, PARSE, H265, MXPEG. For other streams: Codec1, Codec2, Codec3.
- **Quality** - Recording stream compression quality rounded to close available value in range 1-100. For other streams: Quality1, Quality2, Quality3.
- **Bitrate** - Recording stream bit rate rounded to close available value. For other streams: Bitrate1, Bitrate2, Bitrate3.

#### 9.3.4.1.2 Export

Users can select the folder where the camera settings CSV file is exported to and give the name of the file. Users can also define the delimiter that is used in the CSV file.



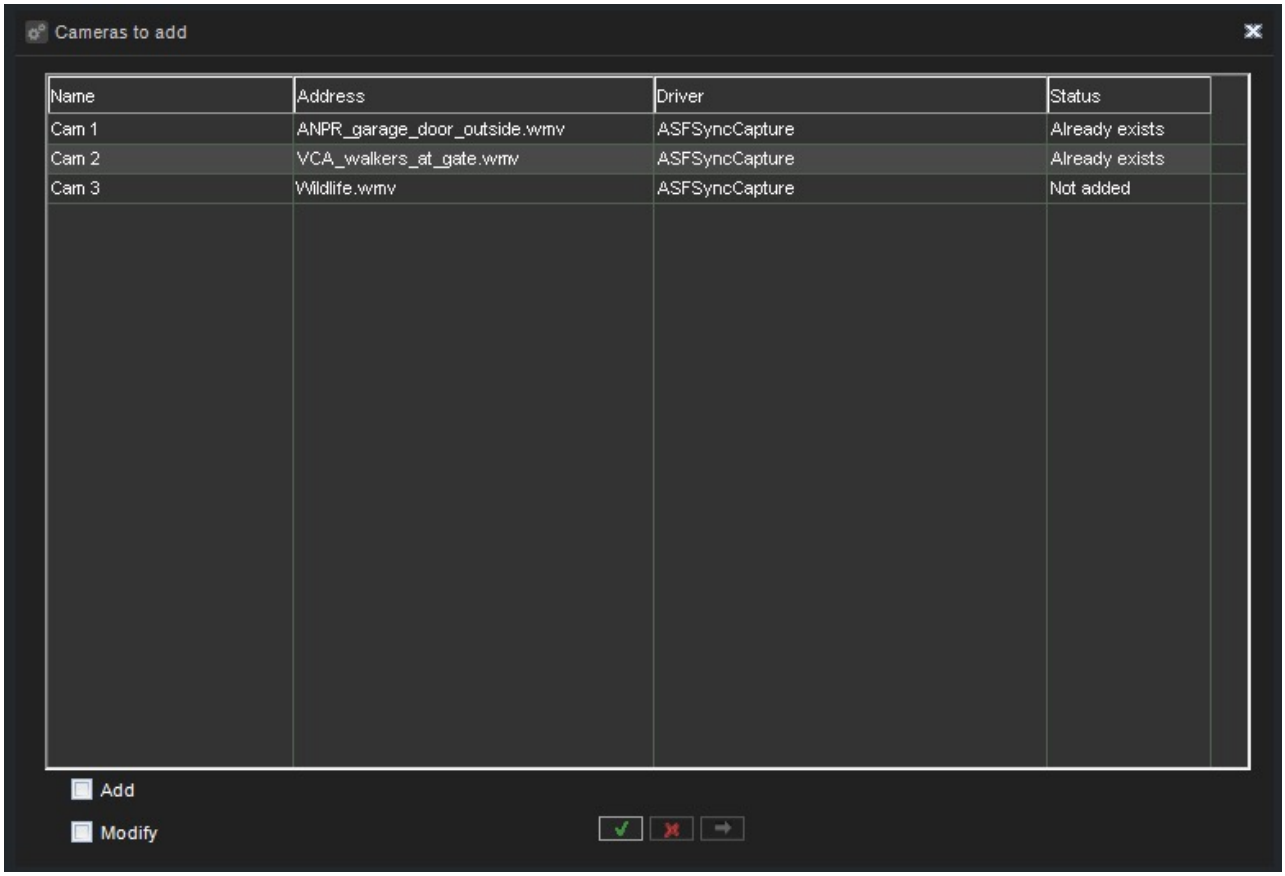

When the export is successful, a blinking green icon is shown. In error, a blinking red icon is shown.

#### 9.3.4.1.2.1 Import

When the user clicks the import button, the select file dialog is shown to select the CSV file to import. When the file is selected, the camera adding view is shown if CSV file parsing and validation are done successfully.

The following validation rules are used when parsing imported CSV files.

- CSV file column delimiter is a comma (,) or semicolon (;).
- The order of the header names (i.e. column order) is free.
- Unused header names (i.e. columns) can be left off.
- Only the Address header name is mandatory. If it is missing, CSV file data is not accepted.
- If some property names and data do not exist, an internal default value is used.
- For validation errors and warnings, a message popup is generated, and more information is printed in the System Manager log.




After the CSV file validation and parsing, the status column informs if the camera is already added to the system (Already exists) or if it is the new camera (Not added). Add and Modify check boxes appear if there are modifications to existing cameras and new camera configurations in the imported CSV file. These options can be used to select if cameras from the CSV file are added and/or modified. Execute button is enabled when there are cameras to be added or modified. By clicking the execute button, settings from the CSV file are applied (modified and/or added) to the current settings. After the settings apply, the status for each camera is updated, Dialog can be closed after the settings apply by clicking the ok button or from the cancel button before the settings apply. Modified camera settings and/or added cameras are applied to the VMS server once the hardware settings are saved.

## 9.4 Adding and Removing VMS Servers

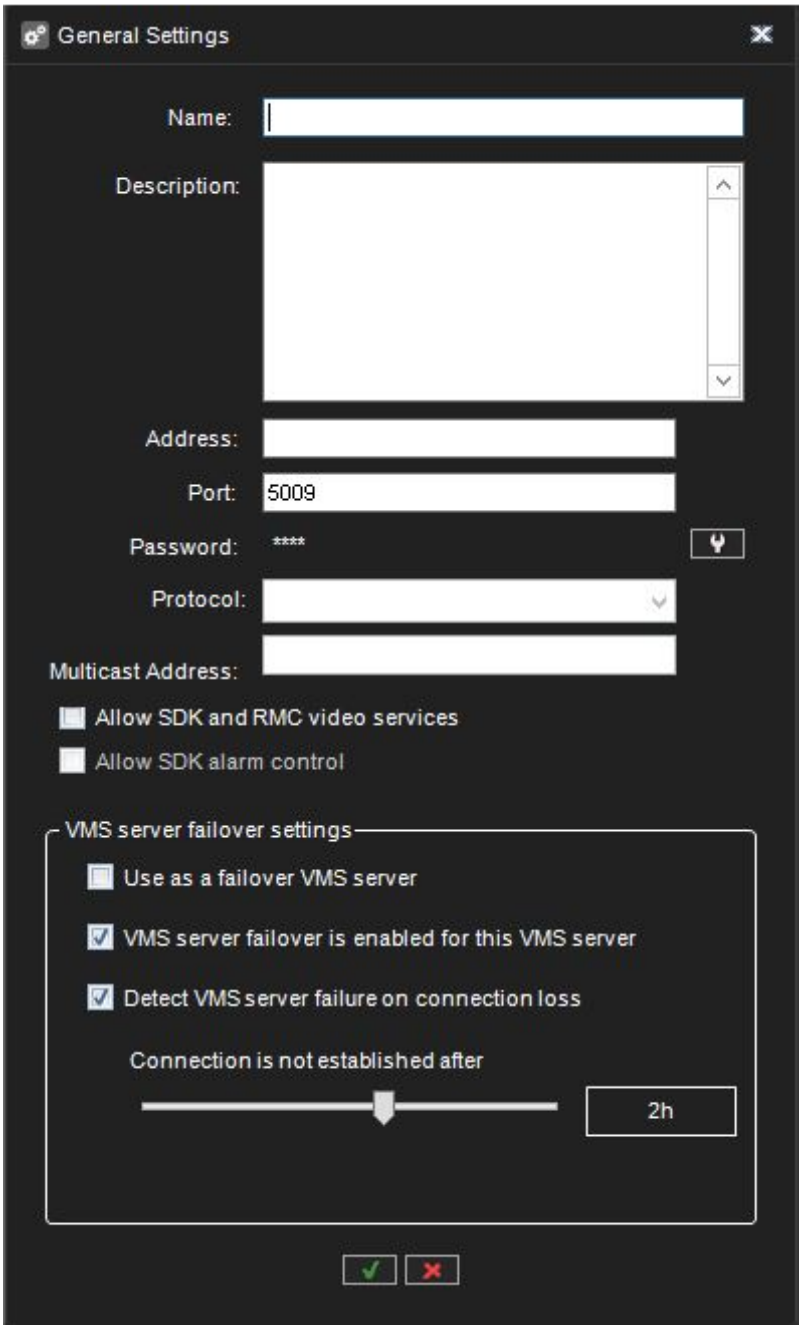
You can have (depending on the license) from 1 to unlimited servers in one system.
One server should not belong to more than one Master Server (SMServer).
You can specify a password for each server.
The system will prompt for the password if someone tries to add the server to another system.

### 9.4.1 To add a server to the system(recording server):

1. Open the **VMS Servers** tab

2. Click Add VMS Server

3. The **General Settings** dialogue box is shown.
4. Type name for the server
5. Enter a description, if needed
6. Type the IP address or DNS name of the server.
7. Enter the password for the server, if needed
8. Click **OK**. The server and the devices connected to it (cameras and audio channels) are added to the list.
    a. Note: *If the server is password-protected, the system prompts for the password.*




### 9.4.2 To remove a server from the system:

1. Select the server that you want to remove.
2. Click Remove **VMS Server**
   
3. Click **OK** to confirm.

### 9.4.3 Connection status:

If the connection to the server is lost, the System Manager application will automatically try to connect to the server.

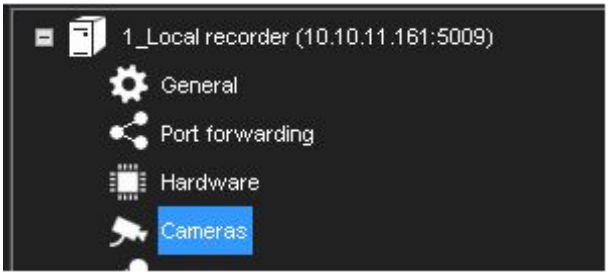
### 9.4.4 NOTE:

When you have added Mirasys VMS as a slave server, please do the following actions:

1. Change Admin user password using a slave server System Manager
2. Disable SMServer service from the slave server

## 9.5 Cameras

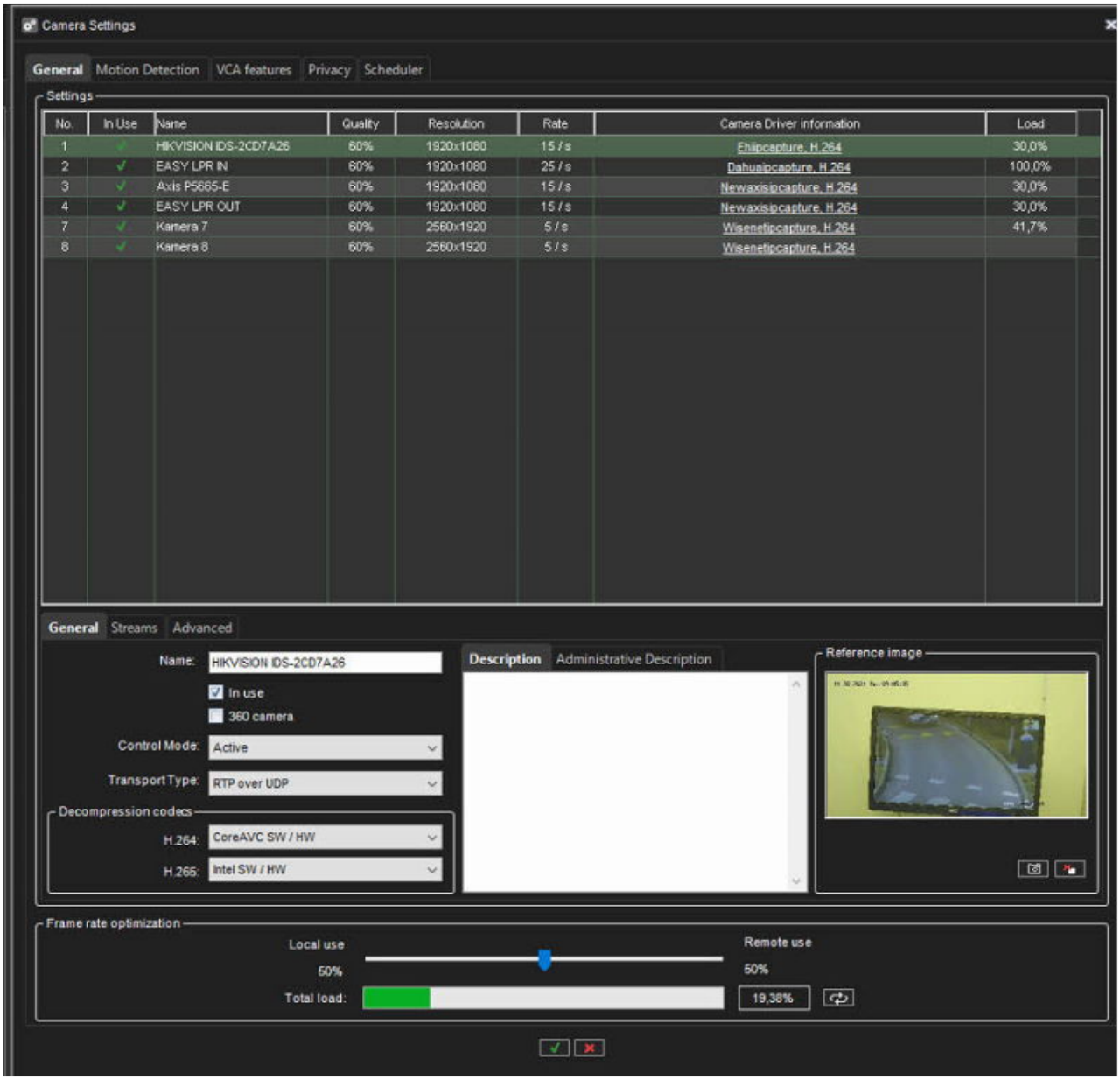
After the camera has been added to the server, the camera settings can be configured from the **Cameras** page.




### 9.5.1 Camera Settings contain settings for:

- General
- Motion Detection
- VCA features
- Privacy
- Scheduler

## 9.5.2 Camera settings




### 9.5.2.1 General settings

#### 9.5.2.1.1 Name

The name of the camera. The system suggests names of the type *Camera 1*, *Camera 2*, and so on.

#### 9.5.2.1.2 In Use

Clear this check box if no camera is connected to the camera input or if you want to disable the camera.

#### 9.5.2.1.3 360 camera.

This tells the Spotter client that the camera is a 360 camera, and Spotter will show the image de-warping options in the camera toolbar (if installed)

#### 9.5.2.1.4 Control Mode

This setting has two options, **Active** (default) and **Passive**.
If multiple servers have the same camera configured, then one should be made **Active,** and the others should be **Passive**.
This way, only the Active server settings are communicated to the camera.

#### 9.5.2.1.5 Transport Type

This setting controls how the media stream is transported from camera to server.
The available options are **RTP over UDP** (default) and **RTP over RTSP**.
If the camera seems to work poorly with one setting (for example, if there are holes in camera material or difficulty to get all frames from a camera), then the other set can be used.

#### 9.5.2.1.6 Decompression codecs.

Codecs are used for encoding and decoding video data

#### 9.5.2.1.7 Description.

Here you can type a description of the camera shown to all users in the Spotter program.

#### 9.5.2.1.8 Administrative Description.

Here you can type a description of the camera. The description will be shown in the Spotter program to only system administrators.

#### 9.5.2.1.9 Reference image

A reference image is an image captured from the camera, making it easier to identify the cameras.
In addition, in the Spotter program, the users can compare what they see in the video view against the reference image to ensure that the camera is pointed in the right direction.
To change the current reference image, click the **Capture image** button. To delete a reference image, click the **Delete image** button.

## 9.5.2.2 Streams

By default, Mirasys VMS receives recording quality stream from the camera.
Mirasys VMS server send recording stream by default to the Mirasys Spotter.


### 9.5.2.2.1 Codec

The codec is used for transmitting the video between the server and the client applications, and in the case of IP cameras, for transmitting the video between the IP camera and the server.
In the case of analogue cameras, the codec used by the system is JPEG.
In IP cameras, any codec supported by both the camera and the server software can be selected.
The codecs supported by the server software are JPEG, MPEG-4, H.264, H.265 and Mobotix MxPEG.

### 9.5.2.2.2 Bitrate mode.

This setting controls if the Variable bit rate (VBRMax) or Constant bit rate (CBR) is used.

### 9.5.2.2.3 Quality

Set this value between 0%-100%. A higher value means better image quality but also a large image data size. To decrease the image data size, set the value lower. However, setting the value lower also decreases the quality of the images.
50% is usually sufficient. For wireless and low bandwidth connections, select 0%.

### 9.5.2.2.4 Resolution

For automatically configured IP cameras, the exact image resolutions supported by the camera model are displayed.

### 9.5.2.2.5 Record rate

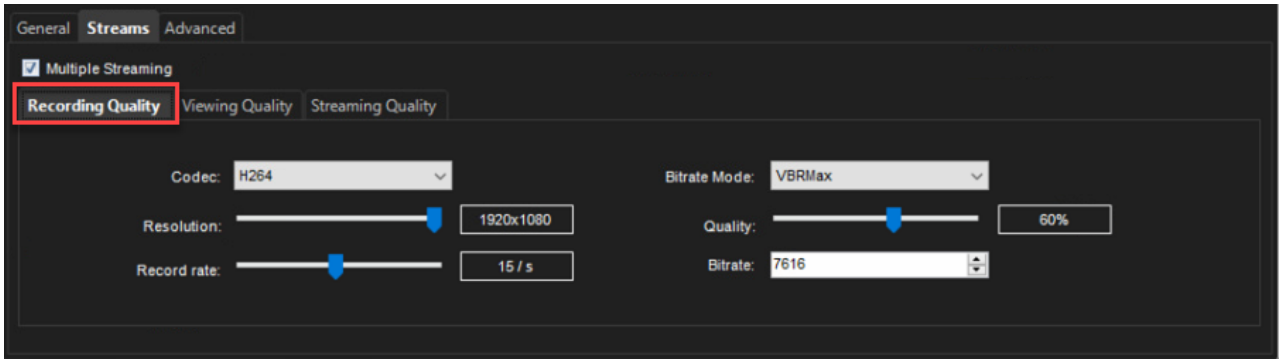
The record rate defines how many frames the camera sends to the VMS and how many frames are recorded. The maximum rate depends on the video standard and the camera type.
Multiple streaming (multi-streaming)

#### 9.5.2.2.6 Multi-Streaming

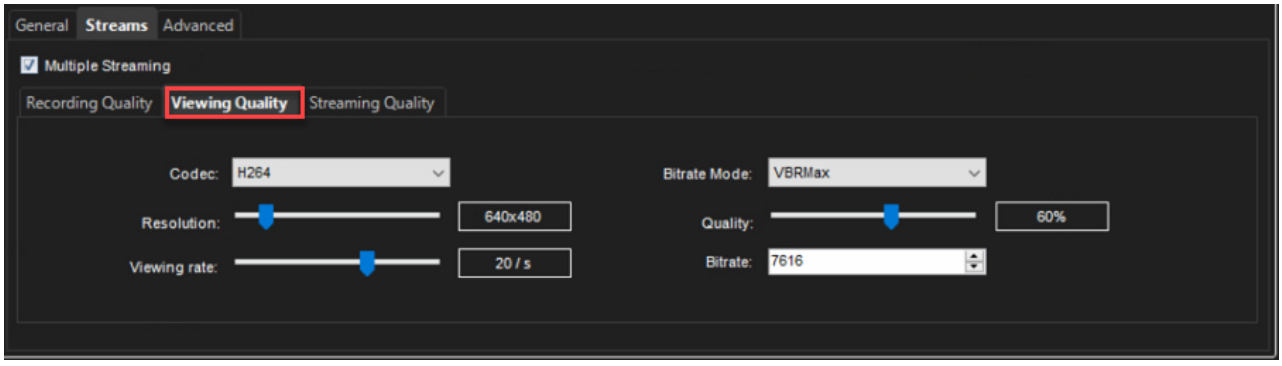
Multi-streaming enables separate feeds from a single camera.
The feature allows for separate streams to be used for recording and viewing.
The feature is available only if the camera and driver support it.

##### 9.5.2.2.6.1 Recording Quality

By default, Mirasys VMS receives recording quality stream from the camera.
Mirasys VMS server send recording stream by default to the Mirasys Spotter




##### 9.5.2.2.6.2 Viewing Quality



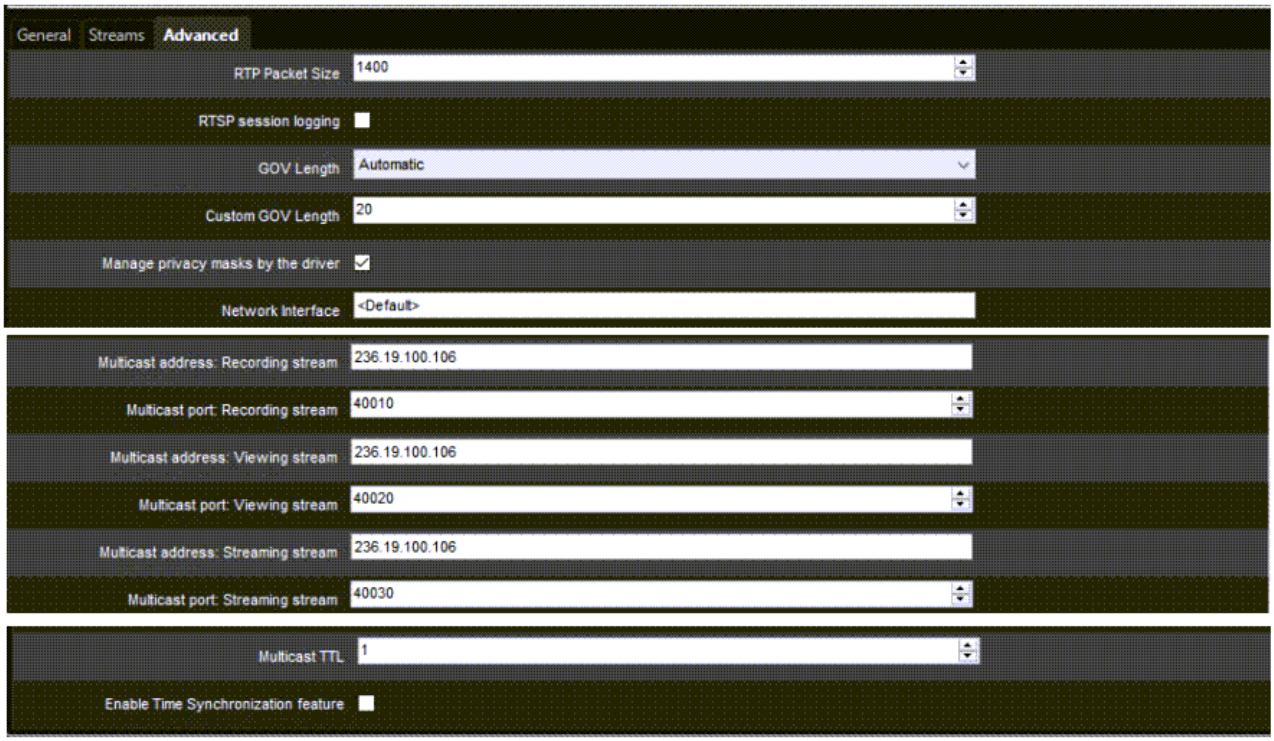

##### 9.5.2.2.6.3 Streaming Quality

## 9.5.2.3 Advanced

This tab contains camera or driver-specific unique settings. A driver update may bring additional values to this tab.
Selecting multiple cameras is possible with SHIFT or CTRL keys.
Please note that if you select more than one camera, you cannot set parameters not supported by all selected cameras.

### 9.5.2.3.1 Configurable values

- RTP Packet Size
- RTSP session logging
- GOV Lenght
- Custom GOV Lenght
- Manage privacy mask by the driver
- Network interface
- Multicast address: Recording stream
- Multicast port: Recording stream
- Multicast address: Viewing stream
- Multicast port: Viewing stream
- Multicast address: Streaming stream
- Multicast port: Streaming stream
- Multicast TTL



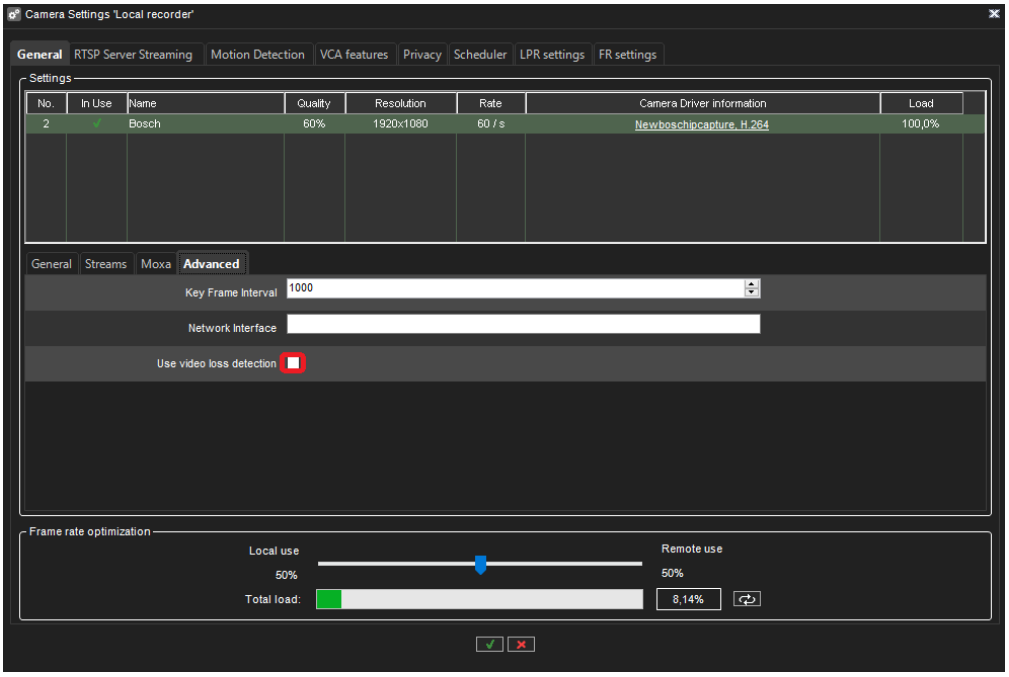
#### 9.5.2.3.2 Signal Lost Event in Bosch Native Driver

A 'signal lost event' can be enabled in the Bosch native driver when utilizing Bosch encoders.

The setting is adjusted in the System Manager desktop application.

When a user sets this option to 'true,' it will remain so even after VMS updates or driver updates.

This ensures that user preferences for monitoring signal events are maintained consistently without reconfiguring settings post-update.



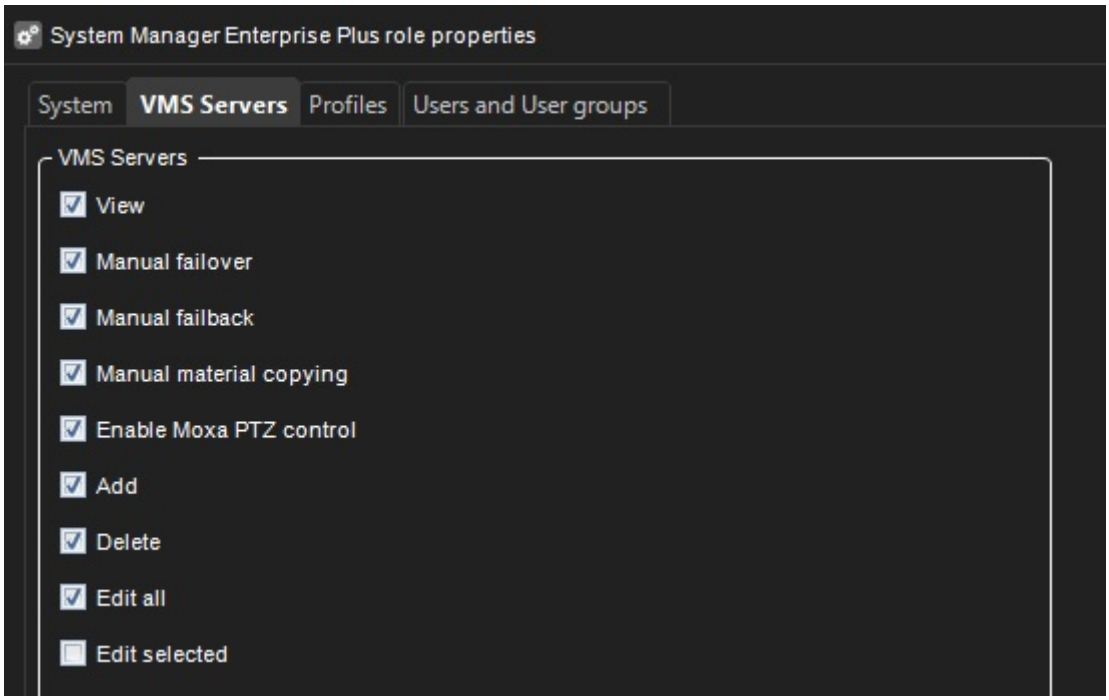

## 9.5.2.4 Frame rate optimization

The slider is intended to estimate load when using the server both as a recording server and a client workstation.
The default assumption for local/remote use is 50%.
If this limits the number of cameras or use of desired camera settings, the slider can be dragged towards 100% to add all desired cameras with desired settings.
However, care should be taken not to overload the server in such a situation.
After specifying whether frame rates should be optimized for local or remote viewing, click **Optimize.**The system sets the record rates to the highest possible values.

## 9.5.2.5 Moxa settings

### 9.5.2.5.1 Enable Moxa PTZ editing

In System Manager role properties / VMS Servers settings, Moxa PTZ settings editing for user group can be selected. If Enable Moxa PTZ control is not selected, Moxa PTZ settings under camera settings can be seen but those cannot be changed.




### 9.5.2.5.2 Moxa PTZ settings

In Camera settings, an additional Moxa settings tab is available for those cameras that have configured Moxa Ptz driver settings or if Moxa editing is enabled for users user group.

#### 9.5.2.5.2.1 Device

**Enable** Moxa PTZ settings for the camera

- If the camera does not have PTZ settings, open the device and PTZ control tab pages with default values.
- If the camera has Moxa PTZ settings and **Enable** is not selected, the settings saving removes Moxa PTZ settings from the camera

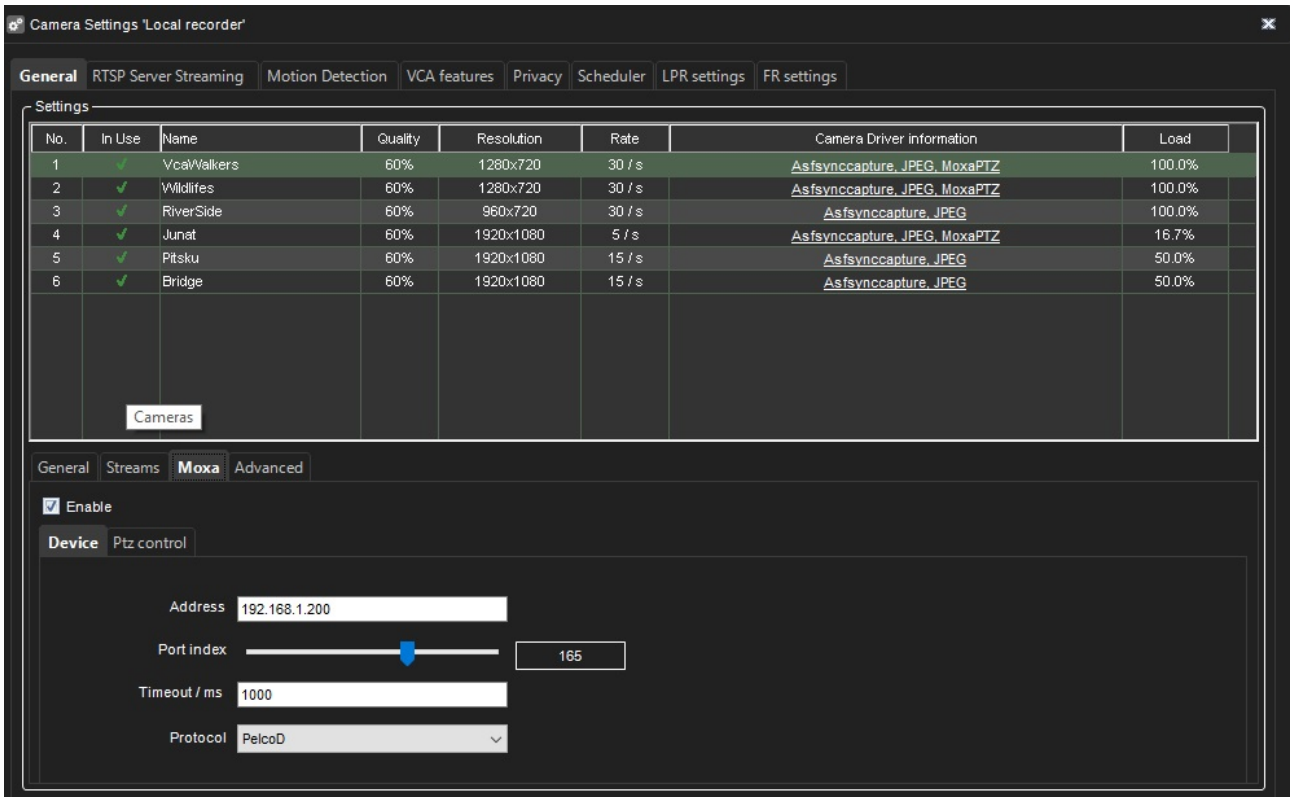
**Address** enter IP or DNS address of MOXA device.

**Port index** is the index of the serial port (1 - 255) in the MOXA device where the PTZ camera is connected.

**Timeout/ms** is the timeout in milliseconds for communications with MOXA device (5000 ms as default)

**Protocol** is the communication protocol with the PTZ camera from the following enumeration:

- { “PelcoD”, “BoschOSRD” }
    - Default value is “PelcoD“




### 9.5.2.5.2.2 PTZ control

**Camera index** - address of PTZ analog camera which is set in camera (usually it is hardware jumpers) (0 - 255)

**Baud rate** - serial port baud rate in bits per second. MOXA supports following set of baud rates:

- { 50, 75, 110, 134, 150, 300, 600, 1200, 2400, 4800, 6400, 7200, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600 }.
- Default value is 38400 bps.

**Data bits** - (byte) - value from the following set:

- {5, 6, 7, 8 }
- Default value is 8.

**Stop bit** - (byte) - value from the following set:

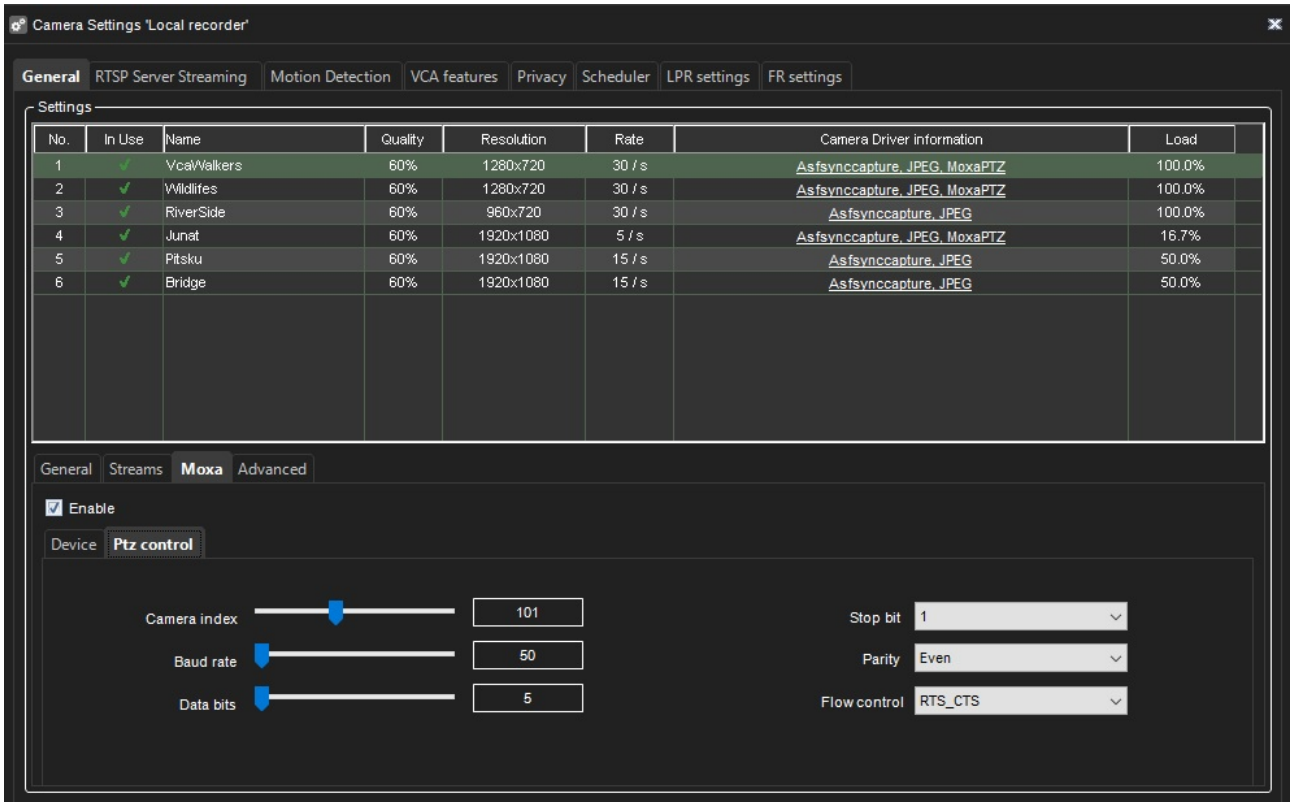
- { 1, 2 }
- Default value is 1.

**Parity** - value from the following enumeration:

- { “None” = 0, “Even” = 1, “Odd” = 2, “Mark” = 3, “Space” = 4 }
- Default value is “None“

**Flow control** - value from the following enumeration:

- { “None” = 0, “RTS / CTS” = 1, “XON / XOFF” = 2, “Both” = 3 }
- Default value is “None“



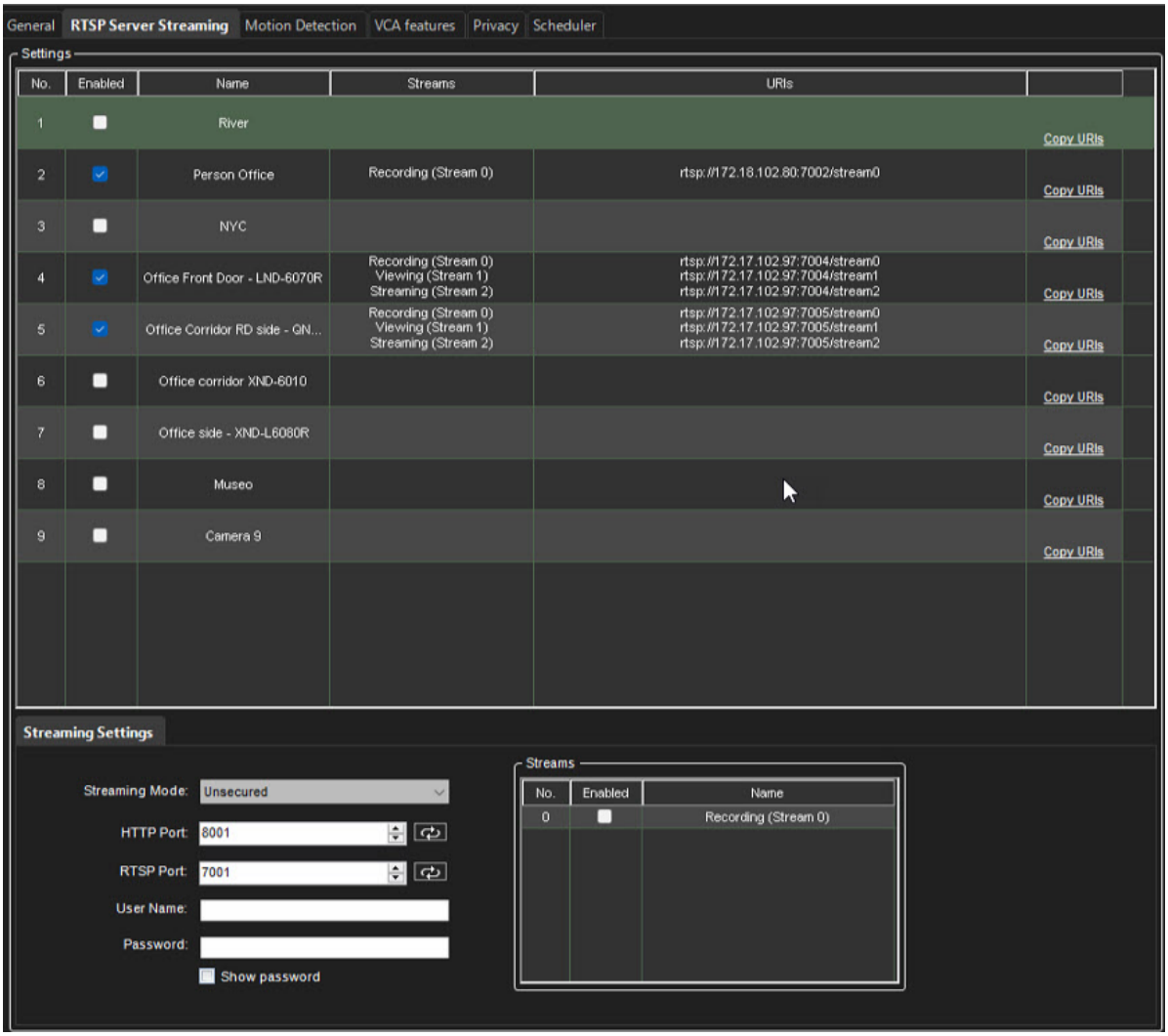

## 9.5.3 RTSP Server Streaming

*Supported from V9.5*

RTSP/RTSPS server is used to stream video from the server to any third-party client that supports RTSP/RTSPS protocol.

### 9.5.3.1 Settings

- Camera number
- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- Camera name
- List of configured streams
- List of configured stream URIs
- Copy URIs link - to copy to clipboard URIs for specified camera



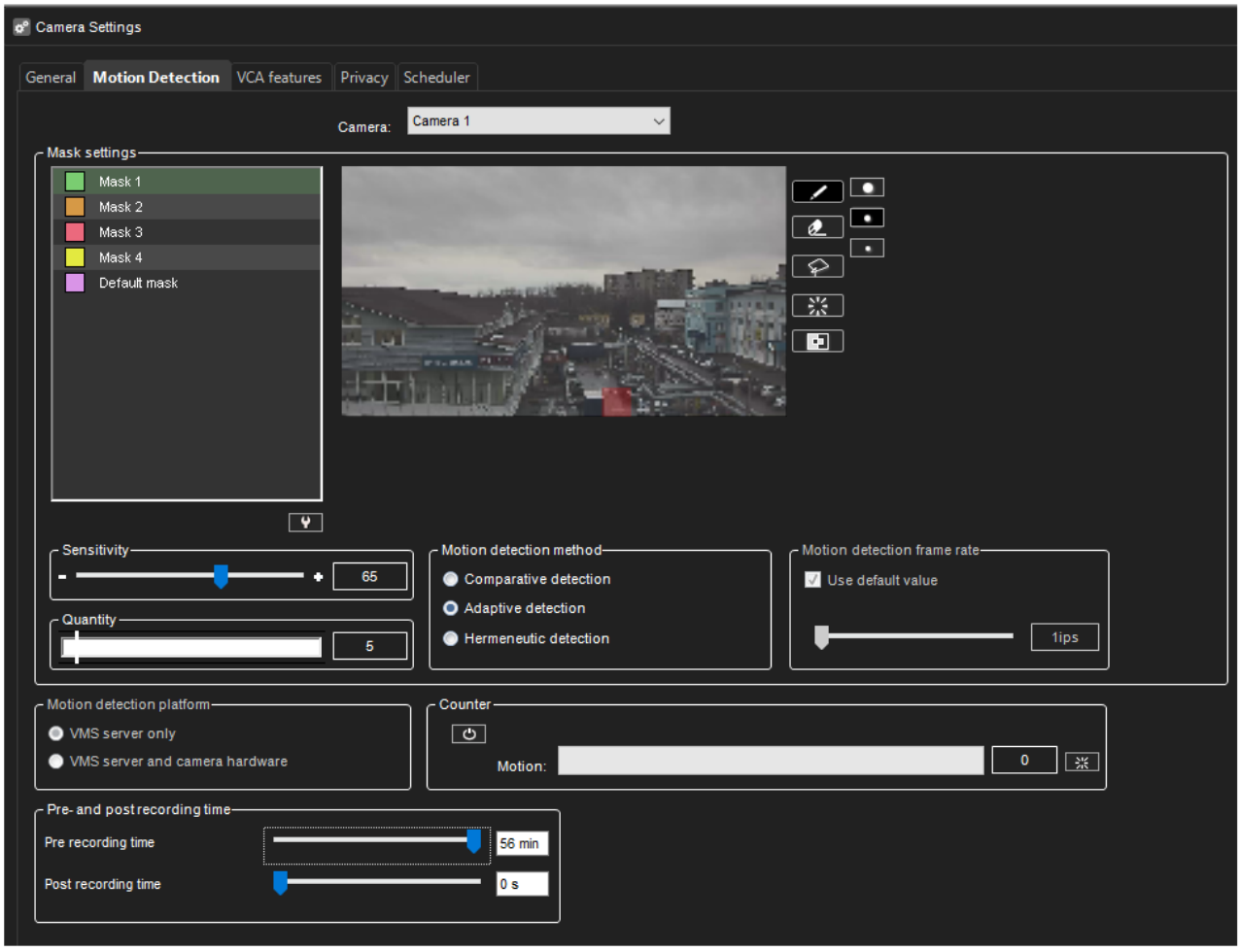

## 9.5.3.2 Streaming Settings

- Streaming mode - can be "Unsecured", Secured (UDP) and Secured (TCP). In secured mode instead of user name and password the certificate should be specified.
- HTTP Port - port for HTTP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.
- RTSP Port - port for RTSP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.
- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- User Name
- Password
- List of streams (multiple if multiple streaming is active) - each stream can be enabled/disabled separately

### 9.5.3.3 Enabling RTSP Server stream to the camera

1. Check the **Enabled** box from the selected camera
2. Select the line of the camera
3. Set **Streaming Mode**, **HTTP Port**, **RTSP Port**, **Username** and **Password**
4. Define used streams

## 9.5.4 Motion Detection




### 9.5.4.1 Sensitivity and quantity

The system detects motion when:

- Pixels change more than the set limit (**Sensitivity**).
- The specified number of pixels change (**Quantity**).

If there is a lot of background noise in the image, for example, changes in lighting conditions, decrease the sensitivity by dragging the slider to the left or increase the quantity limit by dragging the slider to the right.

## 9.5.4.2 Motion detection methods

### 9.5.4.2.1 Comparative detection

Compares an image to the image before it. If the differences exceed the set limits, the system detects motion.
You can use comparative motion detection in most conditions.
However, if there is a lot of movement in the background, for example, rain, moving leaves, or changes in light levels, use adaptive motion detection.

### 9.5.4.2.2 Adaptive detection

Compares each image to a background image. The system learns the background image and the movement that belongs there automatically.
Thus, the system does not interpret, for example, moving leaves as motion.
In addition, if more than half of the pixels in an image change, the system concludes that the lighting conditions have changed.
As a result, it resets the reference image and starts learning it again.

### 9.5.4.2.3 Hermeneutic detection

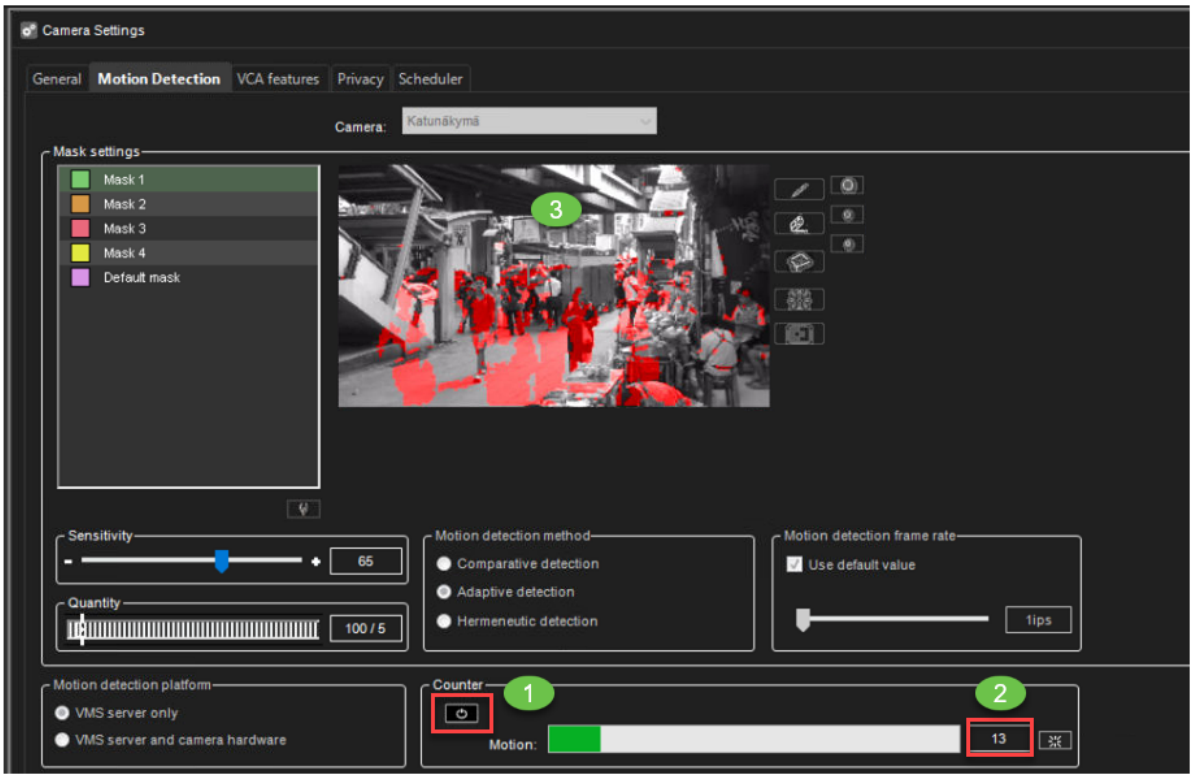
Is a sophisticated motion detection system for challenging weather conditions (e.g. heavy rain, “noisy” background image, etc.) and situations in which external video content analytics (VCA) tools are used.
It should be noted that hermeneutic detection requires more processing resources than the other detection methods.

## 9.5.4.3 Motion detection frame rate

Defines the frame rate used in motion detection.
It is generally recommended to use the default frame rate.
For IP cameras, motion detection uses intra-frames and matches the intra-frame rate.
Typically, this is one image per second.

## 9.5.4.4 Counter

1. Enable **Counter**
2. Check the motion values
3. The camera image shows which area of the camera image causes motion detection recording




## 9.5.4.5 Pre- and Post- recording time

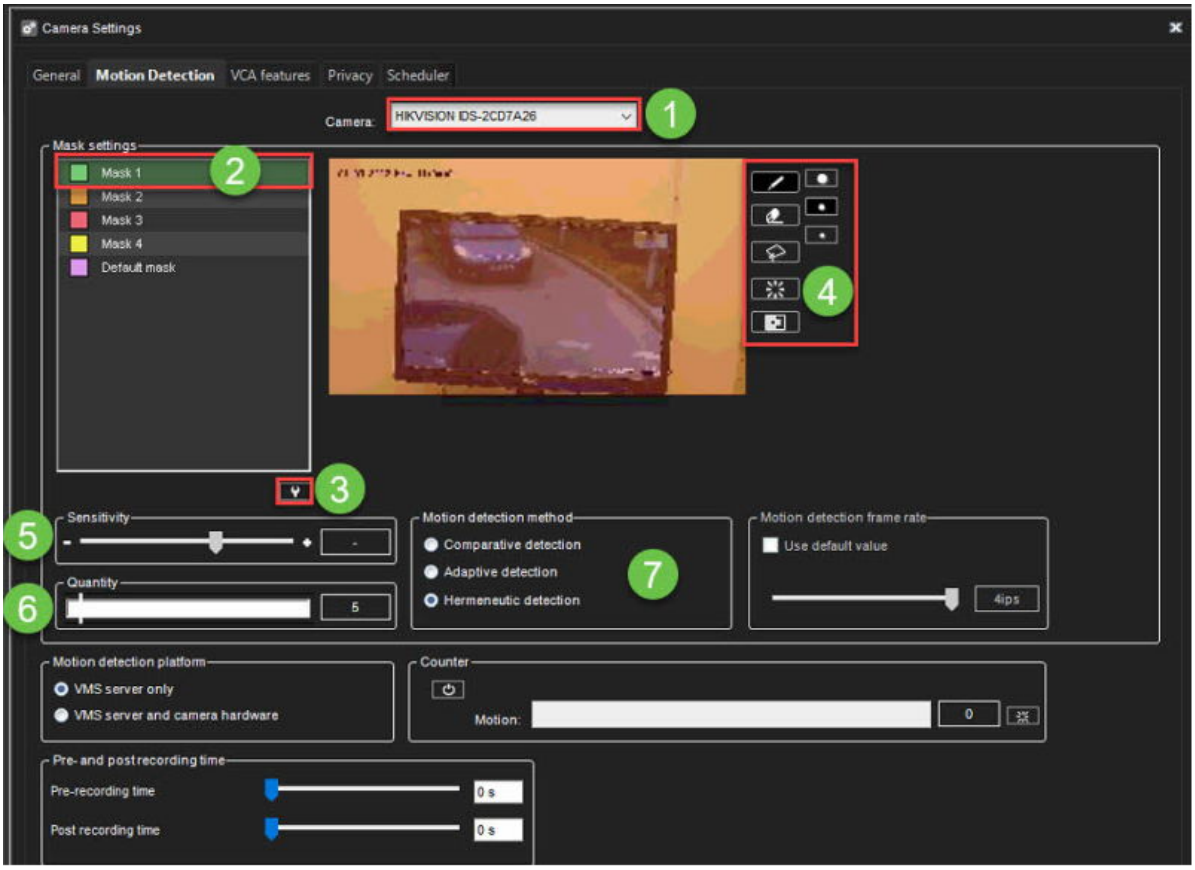
*Supported from V9.5*

Motion pre-and post-recording is used to have recorded material before and after the motion.
Each mask can be configured separately.
Values are from 0s to 60 minutes.

The user can copy selected values to the all cameras using button **Copy pre-and post recording time for all cameras.**

## 9.5.4.6 Editing a mask

1. In the **Motion Detection** tab, select the camera from the camera list.
2. Click the mask that you want to edit.
3. To change the mask's name, click **Change Mask Name** and type a new name for the mask.




1. With the drawing tools presented in the following table, paint the areas red where you want the system to detect movement and remove the red from areas where you want to ignore the movement.
2. Set the detection sensitivity.
3. Set the minimum quantity of movement.
4. Select the motion detection method: comparative, adaptive, or hermeneutic motion detection.

Detected motion is shown in red in the image, and the counter increments each time motion is detected.

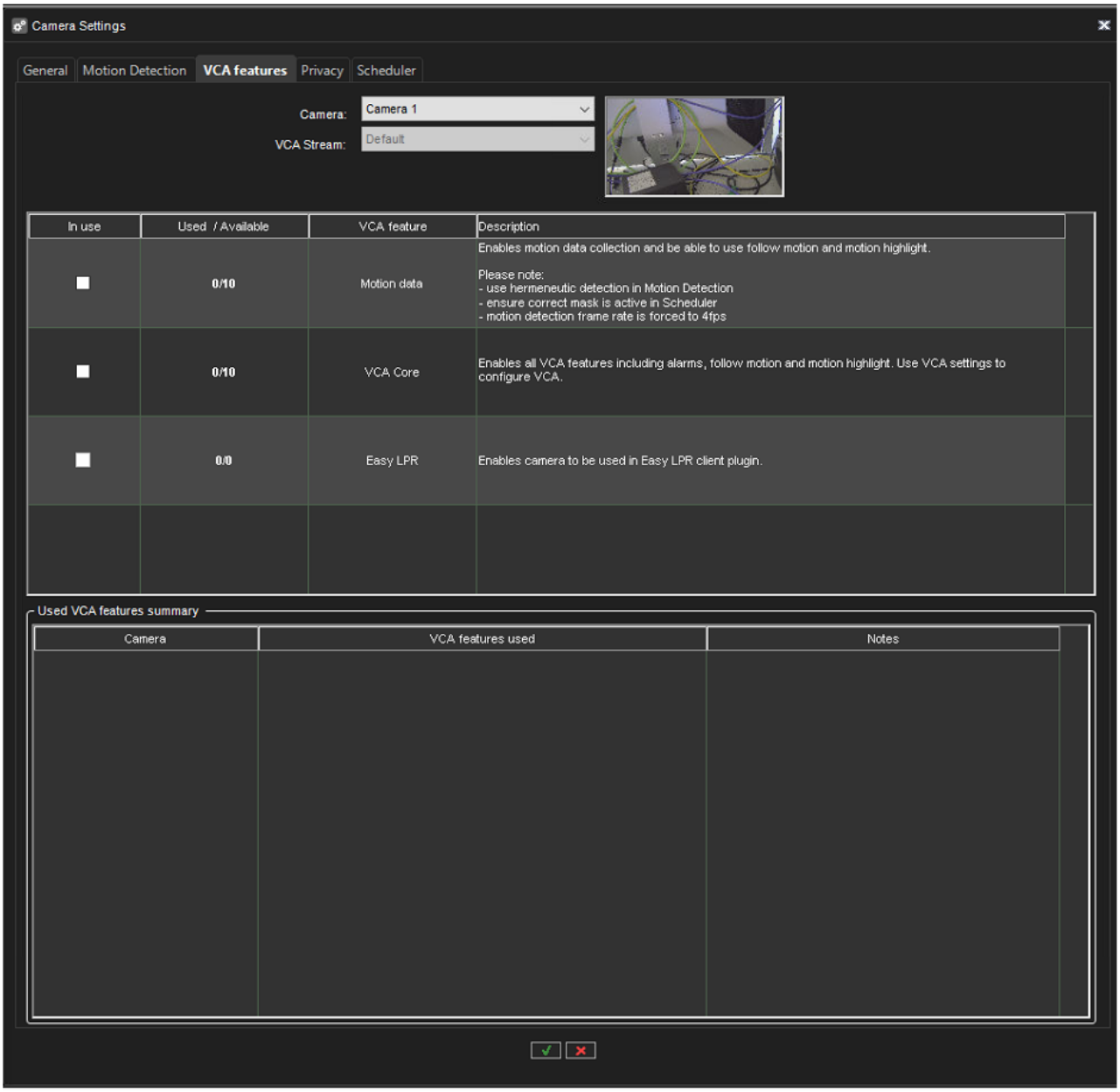
#### 9.5.4.6.1 Drawing Tools:

| Tool | Name | Description |
|---|---|---|
|  | Pencil | Use to set the motion detection area. Select the pencil size by clicking one of the tool size buttons (large, medium, small). |
|  | Eraser | Use to erase selected areas that you do not want to include. Select the eraser size by clicking one of the tool size buttons (large, medium, small). |

| | | |
|---|---|---|
|  | Lasso | Use to select areas using straight lines. If the pen tool is selected, using this tool adds to selected areas. If the eraser tool is selected, this tool removes from the selection. Click the image where you want to start the selection. Click again where you want to anchor the line and change direction. To complete the selection, click the starting point. The selected area is painted red, or the red colour is removed. |
|  | Fill/Clear | If the pen tool is selected, clicking this button selects the total image area. If the eraser tool is selected, clicking this button removes all selections. |
|  | Invert | Reverses selected and unselected areas. Sometimes it is easier to select the area you do not want to mask and then invert the selection. |
|  | Tool Size | Click one of the buttons to select the size of the pencil or eraser (large, medium, small). |

### 9.5.5 VCA features

If the software license includes Video Content Analytics (VCA) functionality, it can be administered on a camera-specific basis on the **VCA Features** -tab.
Depending on the license, specific VCA functionalities can be enabled or disabled on the tab.
It is possible to control which stream (in a configured camera to use multiple streaming) is used for VCA. This is achieved from the pull-down menu below the camera selector (see the following mage)




12 The VCA Features tab

In the primary state, the tab contains the following VCA features:

- **Motion data:** Internal VCA motion data, enabling data collection, motion following, and motion highlighting. Visualized in **Mirasys Spotter**.
- **VCA Core:** enables full VCA functionality. Configured through VCA settings in system manager.
- **Easy LPR**: Enables the camera to be used in the Easy LPR Client plugin

Please note that the VCA features are only available if enabled through the license.

## 9.5.6 Privacy

Under the Privacy menu, you can control the privacy zones of the camera and the facial- and movement blurring functionality.

To be noted: the content of the privacy functionalities is available (for the user) only if they are defined for the camera.
(I.e. if the camera does not have, e.g. the facial blurring defined, this camera shall not have the faces blurred – even if the user group of the end-user would have permission level set to view only unblurred materials. This also applies when exporting the materials.

### 9.5.6.1 Privacy zone on the camera

#### 9.5.6.1.1 Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the camera**
3. Click **Add privacy zone**.
4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.


#### 9.5.6.1.2 Removing the privacy zone

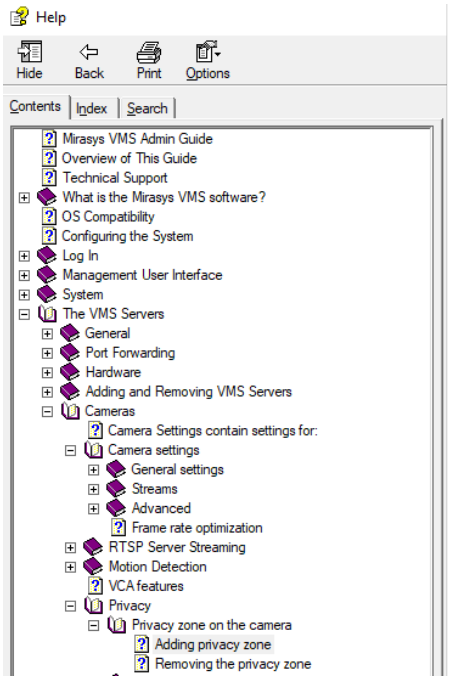
To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

#### 9.5.6.1.3 ONVIF Profile T privacy masking support

The ONVIF automatically detects if a Profile T device supports privacy masking. This feature provides greater control over video surveillance content and allows users to add, remove, or modify privacy masking for our VMS in the System Manager.

For more information, see the System Manager Desktop Application's **Help tab** > **Help Topics** > **VMS Admin Guide** > **The VMS Servers** > **Cameras** > **Privacy**




Adding privacy zone[2]

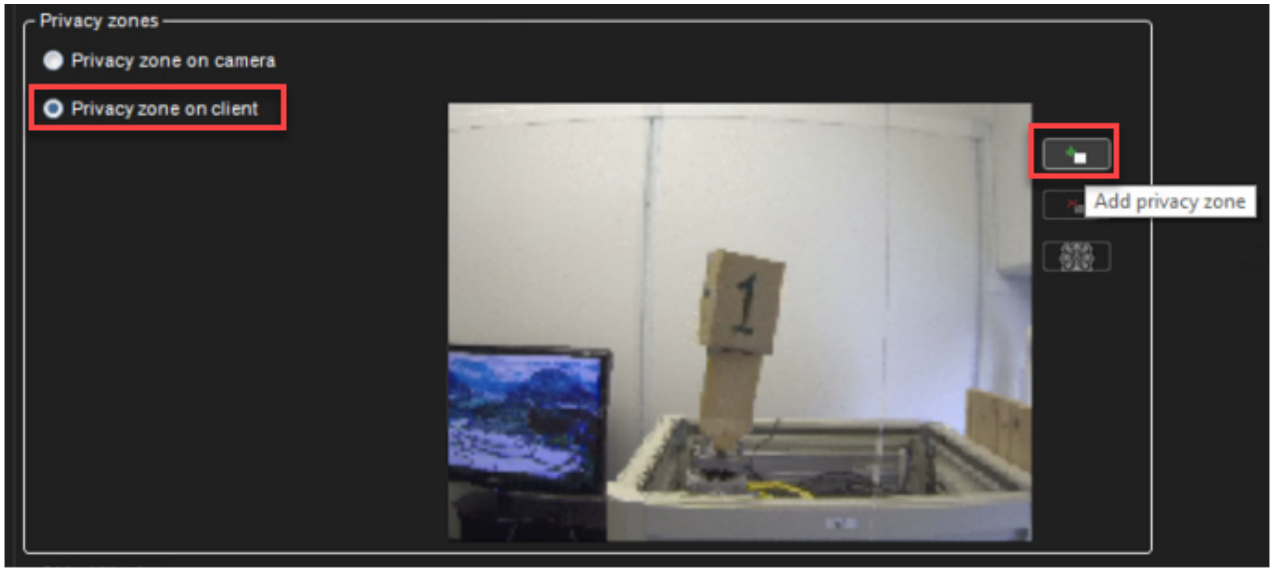
### 9.5.6.2 Privacy zone on the client

On the Spotter client: these privacy zones are implemented only on the viewing client.
This allows the complete video to be recorded and exported, but the privacy-screened areas are only accessible for users who have the right to do so.

2 https://mirasys.atlassian.net/mirasys-vms-admin-guide/V-9.7/privacy-zone-on-the-camera-1

#### 9.5.6.2.1 Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the client**
3. Click **Add privacy zone**.
4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.




#### 9.5.6.2.2 Removing the privacy zone

To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

### 9.5.6.3 Object Blurring

“Blur faces” and “Blur moving objects” settings are available to be set up as additional privacy.
If the facial- or motion-based blurring is enabled for a camera, these are also available on the Spotter side (provided that the user has sufficient permissions.)
The blurring will not be functional on the spotter side- or for exports of the video material for the cameras if they have not been selected on the system administrator side.

Higher resolutions used for the algorithms mean higher accuracy for the algorithms- but also higher CPU loads.

#### 9.5.6.3.1 Blur Faces

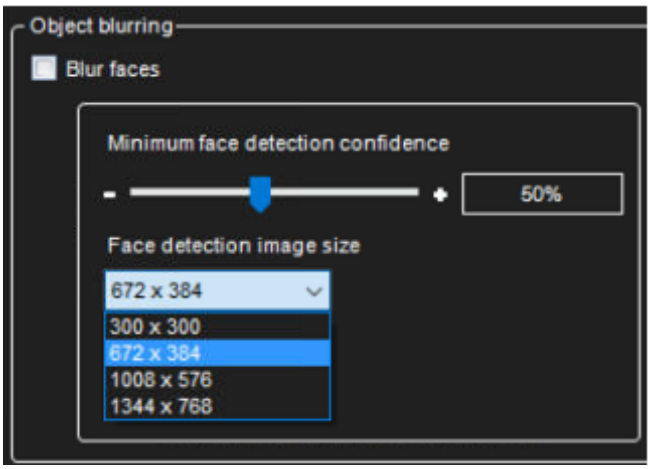
##### 9.5.6.3.1.1 Minimum face detection confidence

##### 9.5.6.3.1.2 Face detection image size

Using a small face detection size value, a person face must be closer to the camera. Face detection will be faster.

Using bigger face detection size value. a person's face is detected more away from the camera.

- 300x384
- 672x384
- 1008*576
- 1344x768




#### 9.5.6.3.2 Blur Moving objects

##### 9.5.6.3.2.1 Motion detection sensitivity

How sensitively pixel in the image is detected as motion pixel

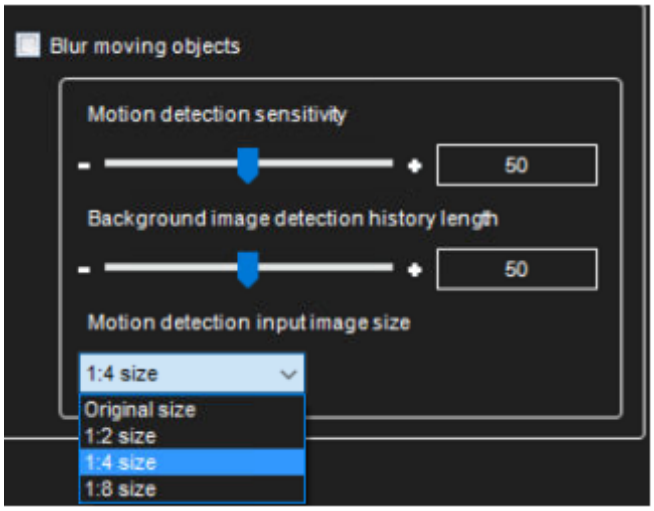
##### 9.5.6.3.2.2 Background image detection history length

How quickly stationary objects are detected as background

##### 9.5.6.3.2.3 Motion detection input image size

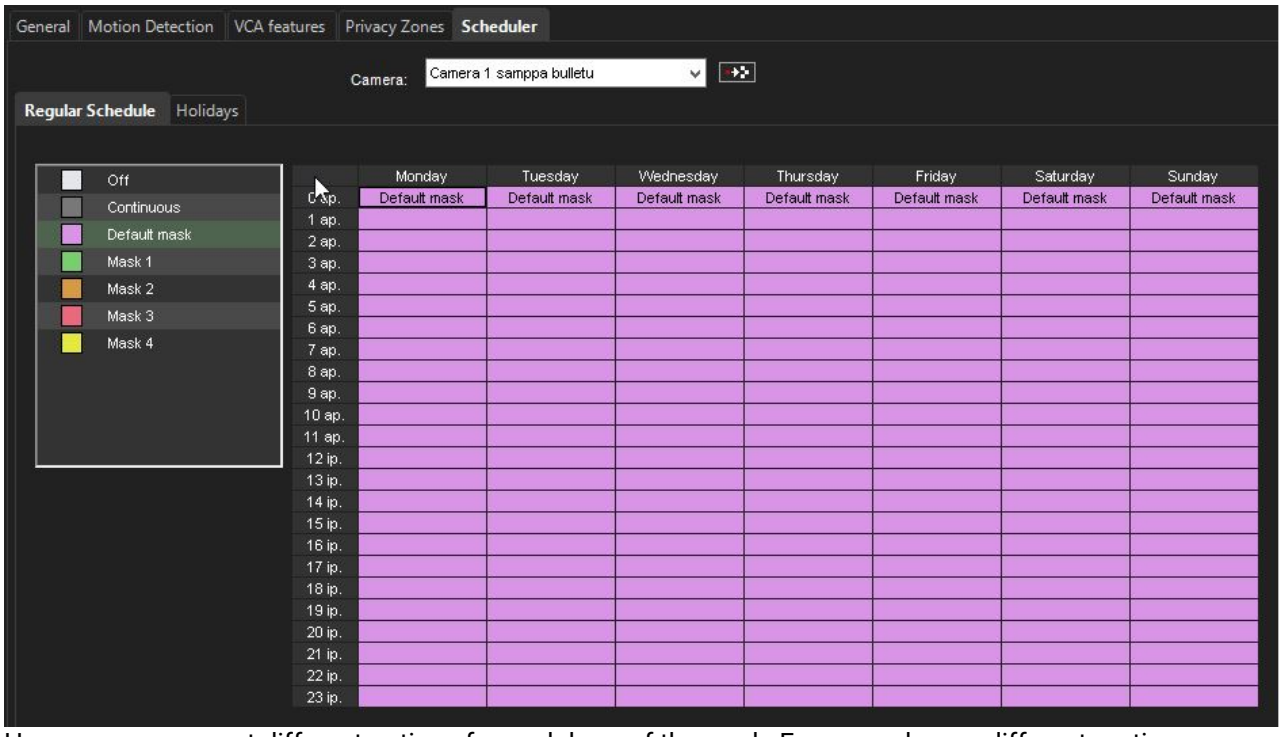
The smaller size is quicker to process but outputs the worse results.

- Original size
- 1:2 size
- 1:4 size
- 1:8 size




## 9.5.7 Scheduler

Scheduler defines which mask is used on each camera and what is active days and hours for the mask. By default, video is recorded when the system detects motion in the default mask. The default mask is active 24/7.




However, you can set different options for each hour of the week. For example, use different motion detection masks during the day and the night.
First, set the regular weekly schedule on the **Regular Schedule** tab and then, if necessary, set holiday

schedules on the **Holidays** tab.
To change the schedule, click on the mask you want to activate, and then click on the scheduled hour where you want it to be used.

***Tip:*** *To change more than one hour at the same time, drag with the mouse.*

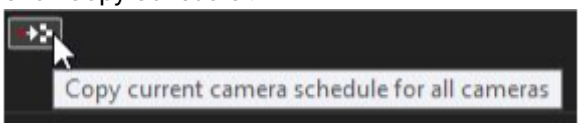
*You can also click the first cell, keep the SHIFT key pressed and then click the last* http://cell. To *change all hours in a column or a row, click the column or row heading. To change all hours of the week, click the cell above the hour's column (on the left side of the weekday heading row).*

These options are available:

- **Off**. Video is not recorded. However, possible alarms are recorded. Alarms are configured in **Alarm Settings**.
- **Continuous.** The camera records all images. This option uses a lot of disk space.
- **Default mask.** The camera records video using the default motion detection mask and default motion detection parameters.
- **Custom mask.** The camera records video using a custom mask. Each camera can have as many as four custom masks.

To copy the current schedule for all cameras:

You can copy the currently selected recording schedule for all cameras in the system.

1. Click Copy Schedule .


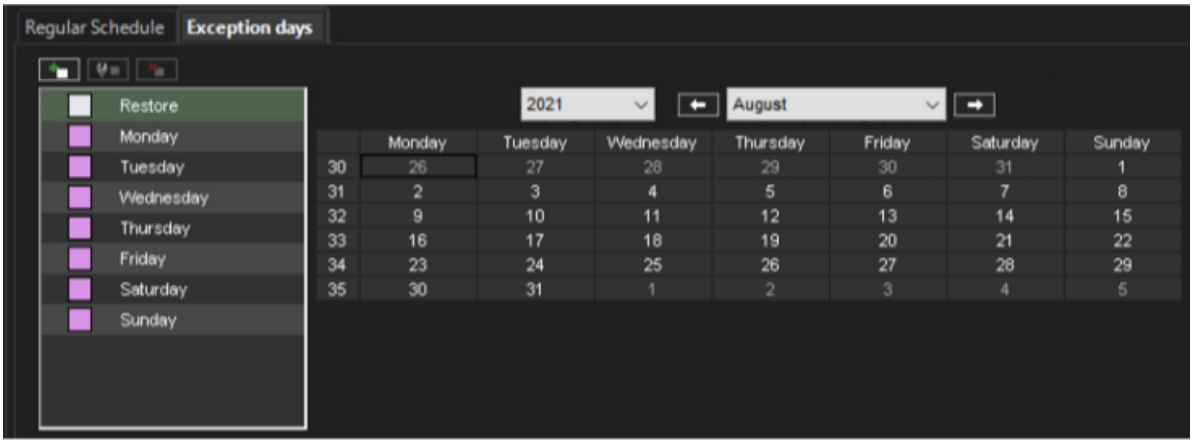
2. When asked for confirmation, click **OK**.

## 9.5.7.1 An exception days settings allow you to set holidays to the calendar.

### 9.5.7.1.1 To set an exception day schedule:

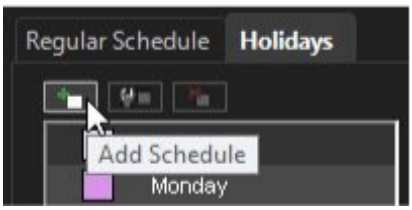
You can use different recording schedules for holidays.
You can apply a daily schedule from the **Regular Schedule** or use an **Exception days** schedule.

1. On the **Exceptions days** tab, select the year and month.
2. Click the schedule that you want to apply from the left panel and then click the holiday in the calendar.




#### 9.5.7.1.2 To add a custom schedule:

Click **Add Schedule**




1. Type a name for the schedule.
2. Click the mask you want to apply and then click the hours you want to apply the mask to.
3. Click **OK**.

#### 9.5.7.1.3 To edit a custom schedule:

1. Select the schedule and click **Edit Schedule**.
2. Edit the schedule and click **OK**.

#### 9.5.7.1.4 To delete a custom schedule:

- Select the schedule from the left pane and click **Delete Schedule**.

#### 9.5.7.1.5 To restore the original schedule:

Click **Restore** and then click the day that you want to restore.

## 9.5.8 License Plate Recognition settings

The **Smart LPR** feature requires an **RTSP Server Streaming** license.

### 9.5.8.1 Configuration

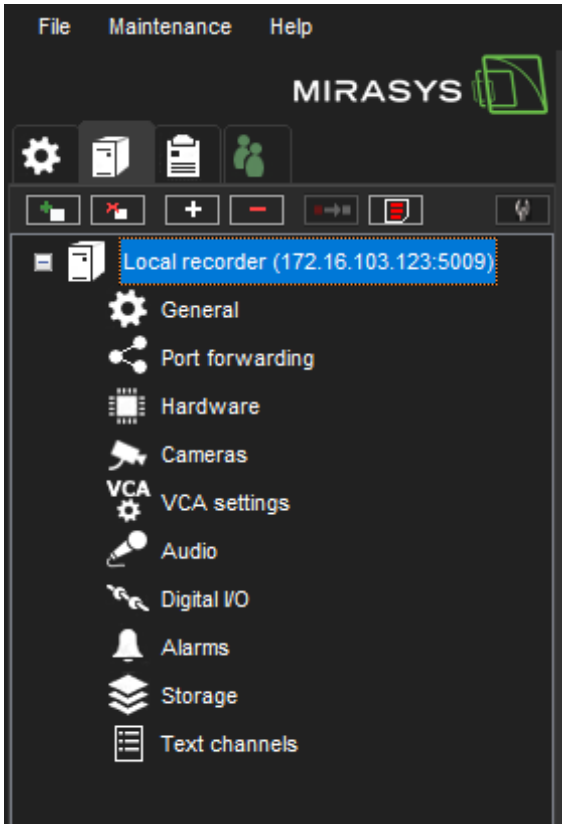
How to configure License Plate Recognition (LPR) services via System Manager:

Open the System Manager application. The LPR settings and settings' limits start loading during the open application after inputting the login and password.

If your license does not support the **Smart LPR** feature, the **LPR settings** tab will be hidden.

#### 9.5.8.1.1 Change or set LPR settings

1. To change or set LPR settings, select recorder on the **VMS servers** tab and open the tree node:




2. Double-click the item “Cameras” to open the **Camera Settings** window

3. Click on the **LPR settings** tab to manage LPR settings.

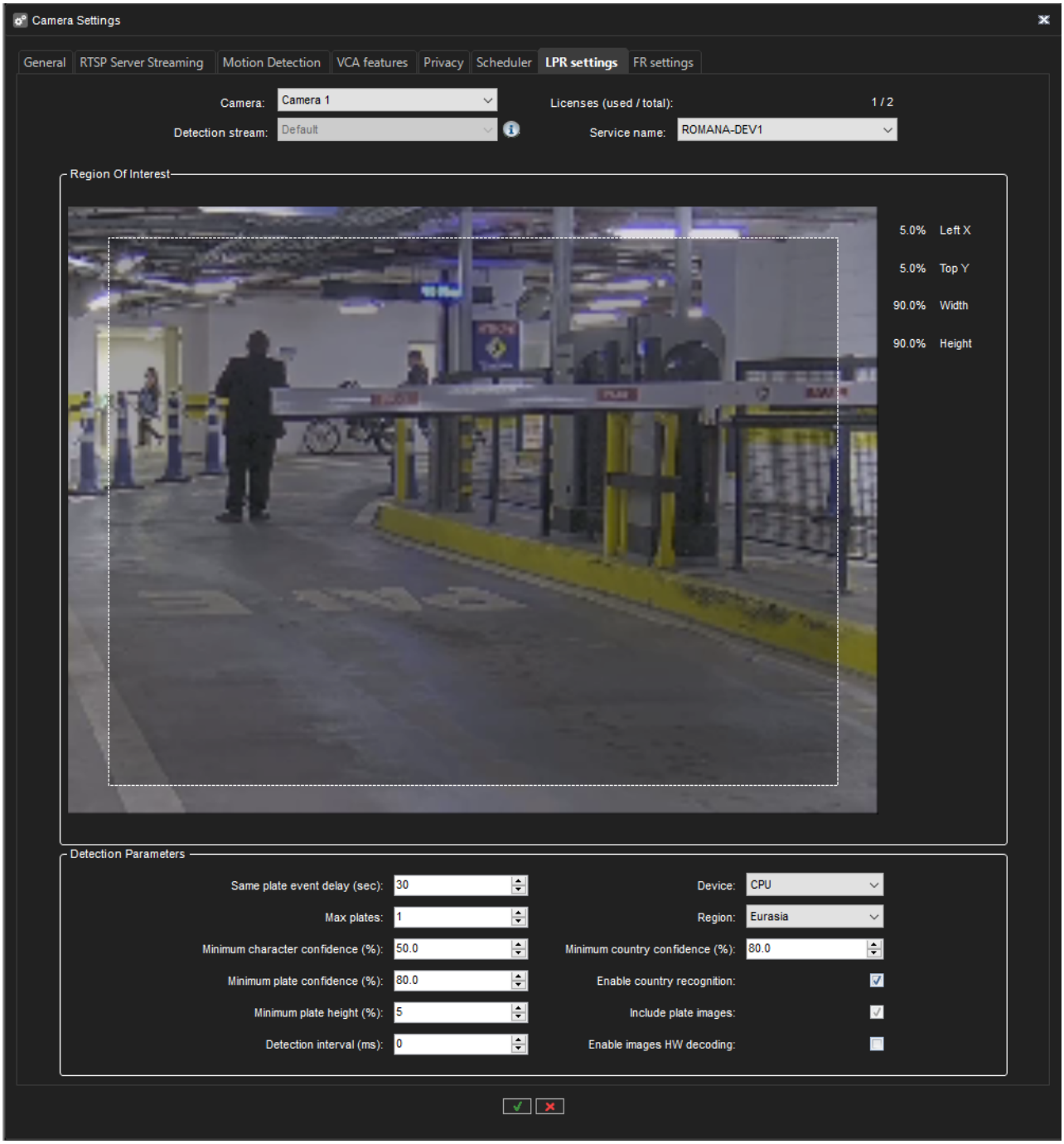
Please note when you double-click the item **Cameras** in the open **Camera Settings** window, your license checks for the ability to use the **Smart LPR** feature and generates a list of cameras (for Combobox **Camera** on the **LPR settings** tab) that are used or can be used in the LPR services.

4. When you select the **LPR settings** tab, the first camera from the Combobox **Camera** is selected.

If the selected camera can be found in services settings, the settings of this service are loaded.

Above the **Service name** Combobox, you will find the **Licenses (used / total)** Label with the number of currently used LPR licenses and total LPR licenses. When you choose a service for a camera and stream current license count is increased, and if you choose a “None” service for a camera, then the current license count is decreased.

*Note: a stream is started in the **Region Of Interest** group area immediately after the current camera is selected in the **Camera** Combobox.*




If no LPR service contains settings for this camera, then the “None” value is selected in the Combobox **Service name**, and the LPR settings are disabled.

You cannot enter service settings if RTSP streaming is not enabled for the selected camera and the stream on the **RTSP Server Streaming** tab. In this case **RTSP streaming should be enabled for selected camera and stream for change the license plate recognition settings** will appear instead of group boxes with LPR settings' controls

If the selected camera is used in some LPR service but is not allowed by the current LPR license for this service, then the **Selected camera for the current service is not allowed by the license. Release LPR service for this camera or for any other camera to keep the license for this one** comment will appear.

In such a case, switching the service name to the “None” value for the free license is possible.

If you need to keep the selected camera in the services settings, then should be a free license for the other camera. You need to select the other camera and switch the service name to the “None” value.

When configured licenses number equals total licenses number it is not possible to switch the service name for cameras with “None” service name value. In this case, **Service name** field will be disable for such cameras.

If the camera supports **ANPR**, you can select “Camera Engine” service in the **Service name** Combobox for such a camera. It means that all events created by the camera itself will be handled by the List Management service as normal **LPR** events.

When the “Camera Engine” service is selected, **Settings for Camera Engine are configured on the camera itself** will appear instead of group boxes with LPR settings' controls because, in this case, it is possible to change ANPR settings on the camera side only.

“License (used / total)” field shows how many licenses are used by LPR services and how many licenses are available. If license is unlimited “Unlimited” value is shown in this field.

#### 9.5.8.1.2 Plate detection settings

After the camera, its stream and the LPR detection service are selected, license plate detection settings can be adjusted. Plate detection settings can be found in the **Detection Parameters** group box in the **LPR settings** tab in the **Camera Settings** window.

Plate detection settings are used for configuring the plate recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Same plate event delay** - the number of seconds that should elapse before reading the same plate twice.

- **Max plates** - maximum number of plates to detect. Detected plates are sorted by plate confidence number in descending order.
- **Minimum character confidence** - plate characters recognizer confidence level. Valid values are between 25% - 95%.
- **Minimum plate confidence** - recognizer confidence level. Valid values are in the range of 25% - 95%.
- **Minimum plate height** - minimum plate height in %. Valid values are in the range 1% - 50%. The default value is 5%.
- **Detection interval** - the number of milliseconds that describes how often plate detection is done: if it is, for example, 250ms, then plate detection is done 4 times in a second (even if the video stream frame rate is much higher, like 30 fps).
- **Device** - is used for inference. Available devices depend on the hardware of the actual service.
- **Region** - The detection model (Eurasia or Americas) to be used for detection.
- **Minimum country confidence** - country recognizer confidence level. Valid values are between 25% - 95%.
- **Enable country recognition** - enable or disable country detection. Enabling country detection can improve plate number detection in some cases.
- **Include plate images** - include plate images or not in returned data.
- **Enable images HW decoding** - enable to decode input images with the most suitable computing platform (CUDA, DXVA, or DirectX).

### 9.5.8.2 Save settings

Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window.

Click the **Cancel** button with the red cross icon to cancel saving LPR settings and return to the settings values loaded after opening the **System Manager** application.

LPR settings for the selected camera are temporarily saved after switching on other cameras, streams, or tabs.

If you need to delete stream settings for the selected camera and detection stream, then select “None” in the **Service name** Combobx for the selected camera and detection stream.

### 9.5.8.3 Influence on settings

The following actions affect the service settings regardless of the actions on the **LPR settings** tab:

- *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all LPR services that worked with the remote recorder and saving the LPR settings.
- *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all LPR services that worked with this camera and saving LPR settings. There is a rule - one camera with one stream can only be used by one LPR service, but one LPR service can work with multiple cameras.
- *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the RTSP streaming settings in the **Streaming Settings** group of the **RTSP Server Streaming** tab:* in case of changing the "Password," “User Name“, "RTSP Port",

"Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.

- *Changing the image size in the **Device Settings** group of the **Video** tab in the **Hardware Settings** window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any LPR service, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.
- *Changing the camera by clicking on the **Edit IP camera** button on the **Video** tab in the **Hardware Settings** window:* in case of changing the camera by clicking on the ***Edit IP camera*** *button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in LPR services settings, where camera ID is presented, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.

## 9.5.9 Face Recognition Settings

How to configure Face Recognition (FR) Services in the System Manager.

Open the System Manager application. The FR settings and settings' limits start loading during the open application after inputting the login and password.

If your license does not support the **Smart FR** feature, the **FR settings** tab will be hidden.

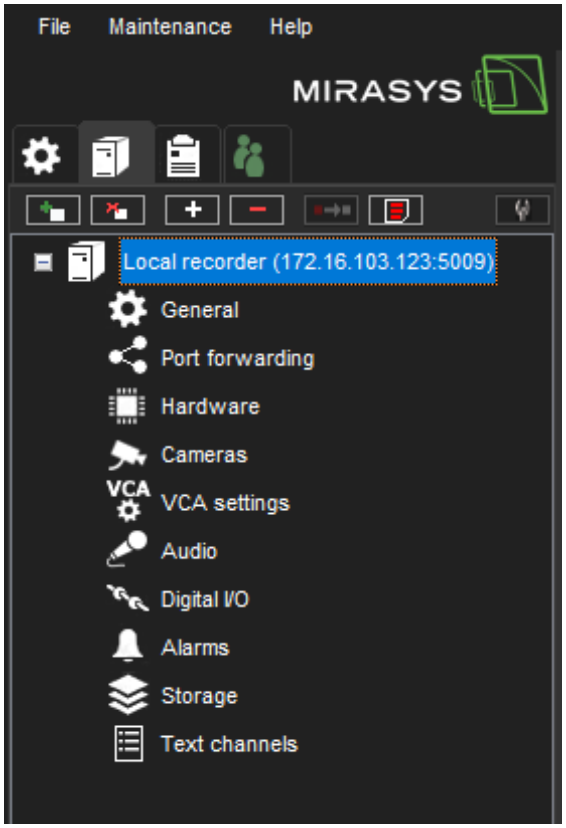
The feature requires an **RTSP Server Streaming** license.

Note that anti-spoofing is **not** included in version 9.6.

### 9.5.9.1 Open settings

1. To change or set FR settings, select recorder on the

**VMS servers** tab and open the tree node:




2. Double-click the item “Cameras” to open the **Camera Settings** window:

3. Click the **FR settings** tab to manage FR settings.

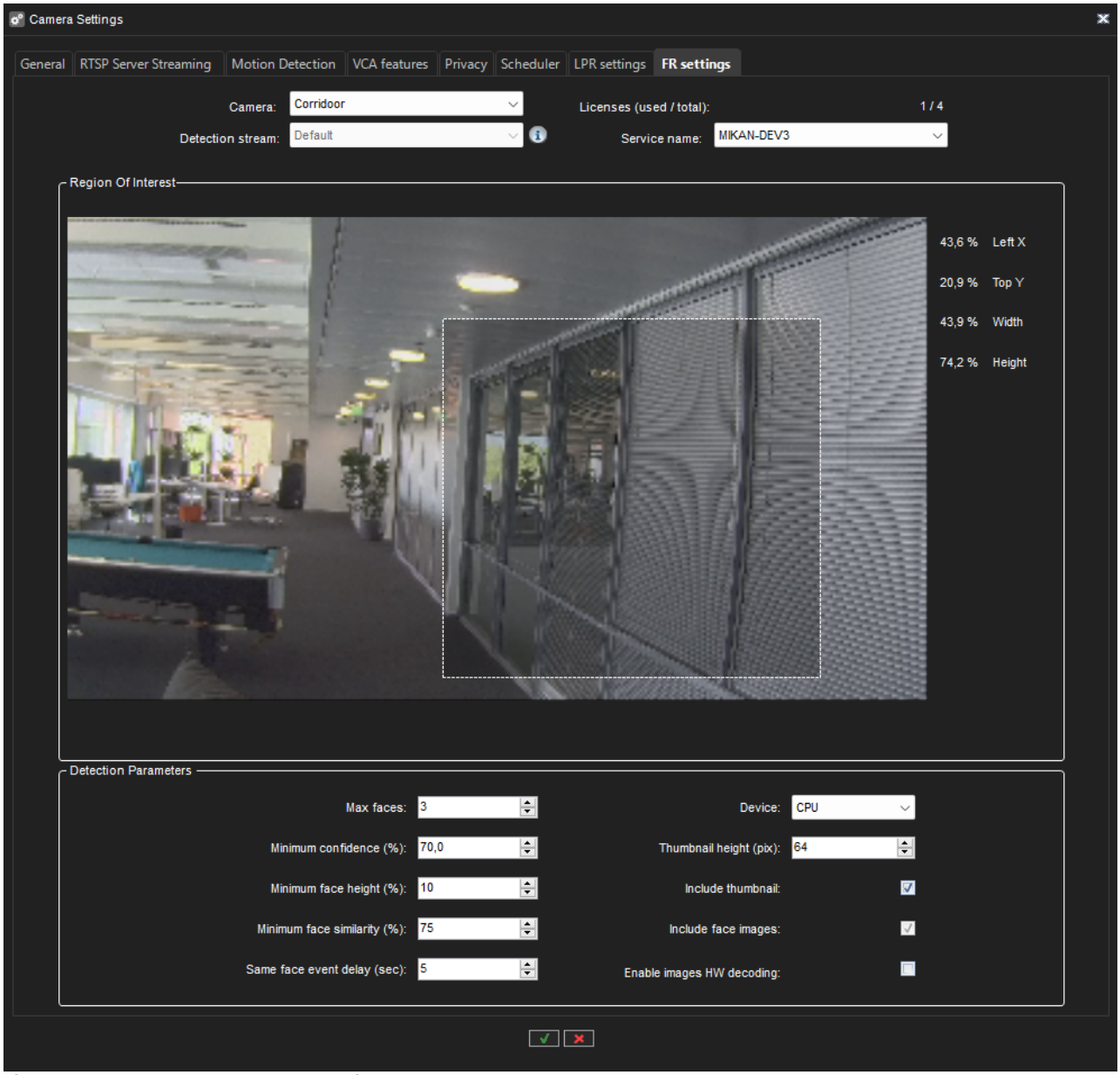
Please note that when double-clicking the item **Cameras** in the open **Camera Settings** window, the user license checks for the ability to use the **Smart FR** feature and generates a list of cameras (for Combobox **Camera** on the **FR settings** tab) that are used or can be used in FR services.

4. When selecting the **FR settings** tab, the first camera from the Combobox **Camera** is selected.

If the selected camera can be found in services settings, the settings of this service are loaded.

Above the **Service name** Combobox, you will find the **Licenses (used / total)** Label with the number of currently used FR licenses and total FR licenses. When you choose a service for a camera and stream current license count is increased, and if you choose a “None” service for a camera, then the current license count is decreased.

*Note: a video stream in the **Region Of Interest** group area is started immediately after the current camera is selected in the **Camera** Combobox.*




If no FR service contains settings for this camera, then the "**None**" value is selected in the Combobox **Service name**, and the FR settings are disabled.

You cannot access service settings if RTSP streaming is not enabled for the selected camera and streams on the **RTSP Server Streaming** tab. Enable the **RTSP streaming for selected cameras, and stream for changing the license plate recognition settings** will appear instead of group boxes with FR settings' controls.

If the selected camera is used in some service but isn't allowed by the current FR license for this service, then **Selected camera for current service is not allowed by the license. Release FR service for this camera or for any other camera to keep a license for this one** comment will appear.

It is possible to switch the service name to **None** value for the selected camera but it’s not possible to switch service names for cameras with a **None** service name value when configured licenses number equals the total licenses number. In this case, the **Service name** field will be disabled for such cameras.

"License (used / total)" field shows how many licenses are used by FR services and how many licenses are available. If license is unlimited "Unlimited" value is shown in this field.

#### 9.5.9.1.1 Face detection settings

After the camera, its stream, and the FR detection service are selected, face detection settings can be adjusted. Face detection settings can be found in the **Detection Parameters** group box on the **FR settings** tab in the **Camera Settings** window.

Face detection settings are used for configuring the face recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Max faces** – maximum number of faces to detect from the image. The value should be between 1 and 5.
- **Minimum confidence** – recognizer confidence level. If confidence for the detected face is below this threshold, then the face is ignored. Valid values are between 25% - 95%.
- **Minimum face height** – minimum face height in %. Valid values are from 5 to 50%%. Default value 10%.
- **Minimum face similarity** – If the similarity is greater than or equal to this value, then it is the same face. The value should be between 50% and 95%.
- **Same face event delay** – the number of seconds that should elapse before arising an event with the same face.
- **Device** – is used for inference. Available devices depend on the hardware of the actual service.
- **Thumbnail height** – the height of the thumbnail image in pixels. The value should be between 32 and 128 pixels.
- **Include thumbnail** – include detection source image thumbnail or not in returned data.
- **Include face images** – include face images or not in returned data.
- **Enable images HW decoding** – enable to decode input images with the most suitable computing platform (CUDA, DXVA or DirectX).

### 9.5.9.2 Save settings

Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window to save.

Click the **Cancel** button with the red cross icon to cancel saving FR settings and return to settings values loaded after opening the **System Manager** application.

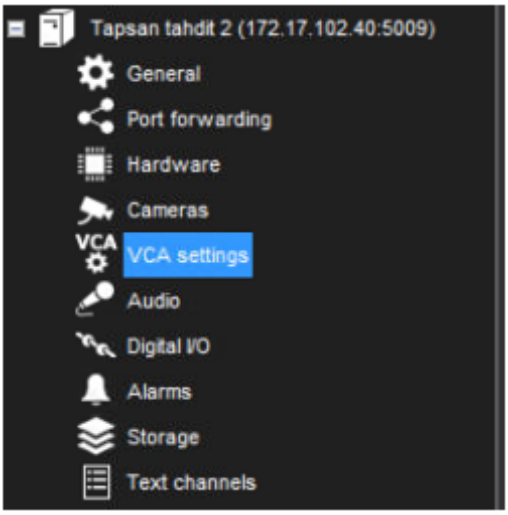
When deleting stream settings for the selected camera and detection stream, the "None" value should be selected in the **Service name** Combobox for the selected camera and detection stream.

### 9.5.9.3 Influence on settings

The following actions affect the service settings regardless of the actions on the **FR settings** tab:

- *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all FR services that worked with the remote recorder and saving the FR settings.
- *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all FR services that worked with this camera and saving FR settings. There is a rule - one camera with one stream can only be used by one FR service, but one FR service can work with multiple cameras.
- *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are present in the settings of any FR service, the FR service settings are changed, and saved when the **Camera Settings** window is closed.
- *Changing the RTSP streaming settings in the **Streaming Settings** group of the **RTSP Server Streaming** tab:* in case of changing the "Password," "User Name", "RTSP Port", "Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any FR service, the FR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the image size in the **Device Settings** group of the **Video** tab in the **Hardware Settings** window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any FR service, the FR service settings are changed and saved when the **Hardware Settings** window is closed.
- *Changing the camera by clicking on the **Edit IP camera** button on the **Video** tab in the **Hardware Settings** window:* in case of changing the camera by clicking on the ***Edit IP camera** button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in FR services settings, where camera ID is presented, the FR service settings are changed and saved when the **Hardware Settings** window is closed.

## 9.6 VCA settings




Please see the Mirasys VCA Guide[3].

3 https://documentation.mirasys.com/ai-guides/V-9.6/mirasys-vca-guide

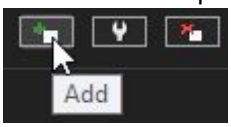
In some cases detection may not work correctly. Please try to increase image quality or move/zoom camera image to closer wanted detection area.
Models are trained using clear images and some cases when using black/white image or thermal camera image this may cause that detection is working correctly. For this you can try use Deep Learning Filter with Object Tracker.

# 9.7 Audio .

## 9.7.1 Adding, Editing and Removing Audio Devices

The system supports three basic types of audio components: one-way analog and IP audio channels, two-way IP audio channels, and a single audio communication channel.

To configure audio devices:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the **Add**-option


5. Select the capture driver from the list.
6. Select one of these options:

1. **Mono**. Select to use two mono channels.
2. **Stereo**. Select to combine two mono channels into one stereo channel.

1. Click **OK**.

**Note:** *IP camera-based IP audio input and output channels are added to the system primarily through the automated camera search tools.If an IP camera-based audio channel cannot be added through the camera search tools, or if the channel is added belatedly, follow the instructions above to add the audio channel.*

### 9.7.1.1 To edit an audio device:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.

4. Select the audio channel.
5. Click **Edit Audio Channel** in the lower right corner of the tab. The **Configure Audio** dialogue box is shown.

6. Edit the information fields.
7. Click **OK**.

#### 9.7.1.2 To remove an audio device:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the audio channel.
5. Click **Remove Last Audio Channel from the List**in the lower right corner of the tab.**Note:** *You cannot remove an audio device from the middle of the list; only the most recently added audio device can be removed.*

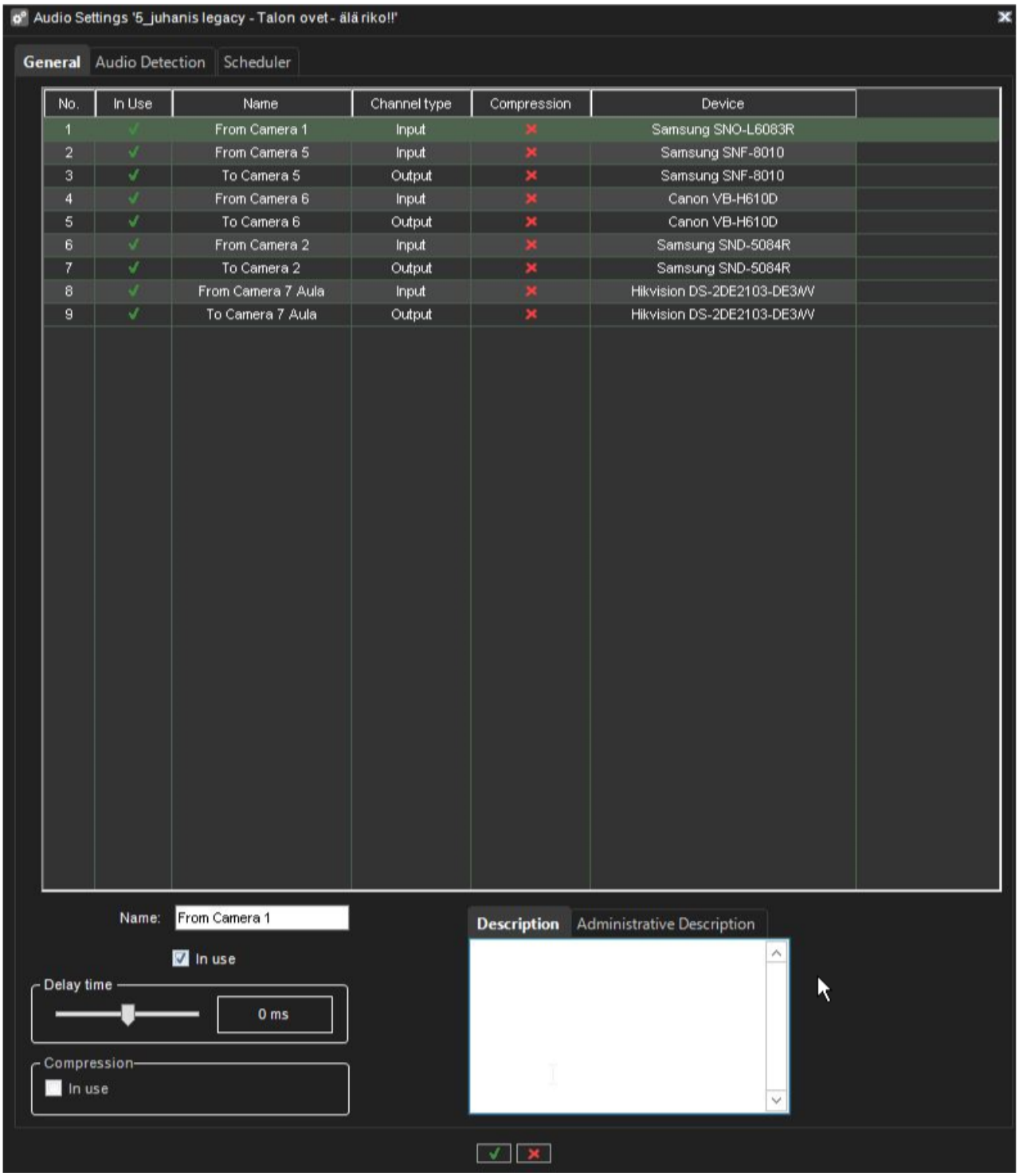
6. The last audio device on the list is removed from the server.

### 9.7.2 Audio Settings

The system supports three basic types of audio components:

- **One-way analogue and IP audio channels:** These include mainly camera-based and separate microphones.
- **Two-way IP audio channels:** Two-way IP audio channels require an IP camera with an audio input and output channel.
    - Two-way IP audio channels are used for communication between the camera site and a Spotter client.
    - Only one Spotter client can be used for communication at any time, but other clients in the system can listen to the channel and take over the communication if required.
    - All communication that passes through a two-way IP audio channel is recorded in the system.
- **A single audio communication channel:** An older communication model. Each system contains one communication channel.
    - The drawback in using the audio communication channel is that the signal bypasses the server, meaning that the communication is not recorded in the system.

### 9.7.3 General Settings tab




The **General** tab in the **Audio** page lists the basic settings of all audio channels:

- **No.** The number of the channel.
- **In Use.** Shows if a channel is enabled or disabled.
- **Name**. The name of the channel.
- **Mono / Stereo**. Shows if a channel is a mono or stereo channel.

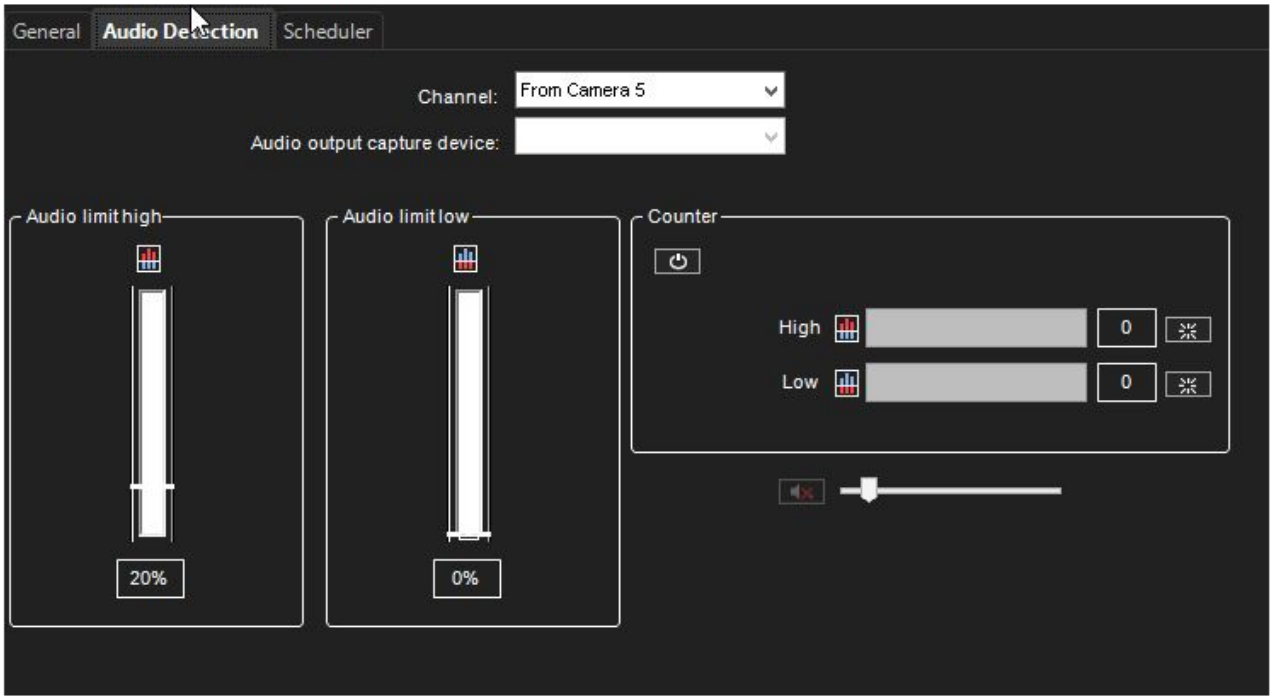
- **Compression**. Shows if compression is on or off. A checkmark means that compression is used.
- **Capture Driver**. Shows what capture driver is used. Select the driver in **Hardware Settings**.

To change general settings:

1. Select the channel from the list.
2. You can change these settings in the lower part of the window:

1. **Name**. The name of the channel.
2. **In use**. Select to enable the channel. Clear the check box to disable the channel.
3. **Delay time**. Sets the delay time in synchronizing the audio stream with other devices.
4. The delay time can be used to optimize the audio and video stream synchronization to, for example, enable better lip synchronization.
5. **Compression**. Select to use compression. Compressed audio files use less disk space, but the quality of the audio is a bit lower. Clear the check box to not use compression.
6. **Description**. Here you can type a description of the channel that will be shown to the users in the Spotter program.
7. **Administrative Description**. Here you can type a description of the channel that will be shown in the Spotter program to only system administrators.

## 9.7.4 Audio Detection




On the **Audio Detection** tab on the **Audio** page, set the high and low limits for audio detection.
The system records audio when the audio level exceeds the high limit.

In addition, you can set the system to give an alarm when the audio level exceeds the high limit or drops below the low limit.

To set the limits:

1. Select the audio channel from the list.
2. Click **Turn Audio Counter On/Off**.
    a. The system shows the audio level in the **Audio Limit High** and **Audio Limit Low** indicators, and the counters increment each time audio detection is activated.
    b. The top counter increments when the audio level exceeds the high limit. The lower counter increments when the audio level drops below the lower limit.
3. Set the high limit so that in usual conditions, the audio level stays below the limit.
    a. Audio detection is activated when the level exceeds the limit.
4. Set the low limit so that in usual conditions, the audio level stays above the limit.
    a. Audio detection is activated when the level drops below the limit.
5. To reset the counters, click the reset buttons.
6. Turn the counters off by clicking the **Turn Audio Counter On/Off** button.
7. To save the settings, click **OK**.

You can adjust the volume of audio and also mute the audio channel.

These settings are not saved; they only change how audio is played in the audio settings.

- **Mute**. Mutes the audio channel.
- **Adjust Volume**. Adjusts the audio volume.

### 9.7.5 Scheduler (Audio)

By default, audio is recorded when the detected level of audio exceeds the default detection limit (**Audio limit high**).

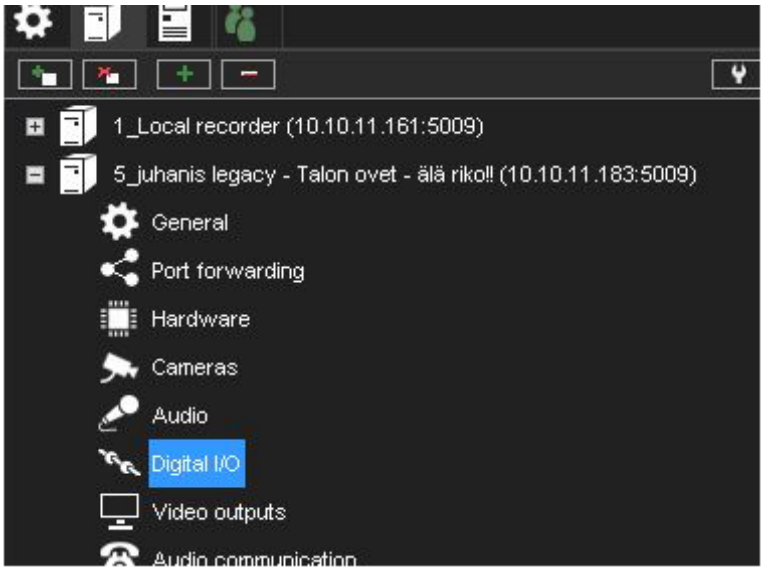
Similarly, to the video scheduler, it is possible to control the audio recording with the following options both for regular weeks and holidays.

1. **Off.** Audio is not recorded. However, possible alarms are recorded.
2. **Continuous.** All audio is recorded.
3. **Audio detection.** Audio is recorded when the measured level of audio exceeds the limit **Audio level is high.**
    a. Set the limit on the Audio Settings[4]

The functionality of this view is similar to the video scheduler.

4 https://documentation.mirasys.com/articles/mirasys-vms-administrator-guide-v9-4-en/audio-settings-1

# 9.8 Digital I/O

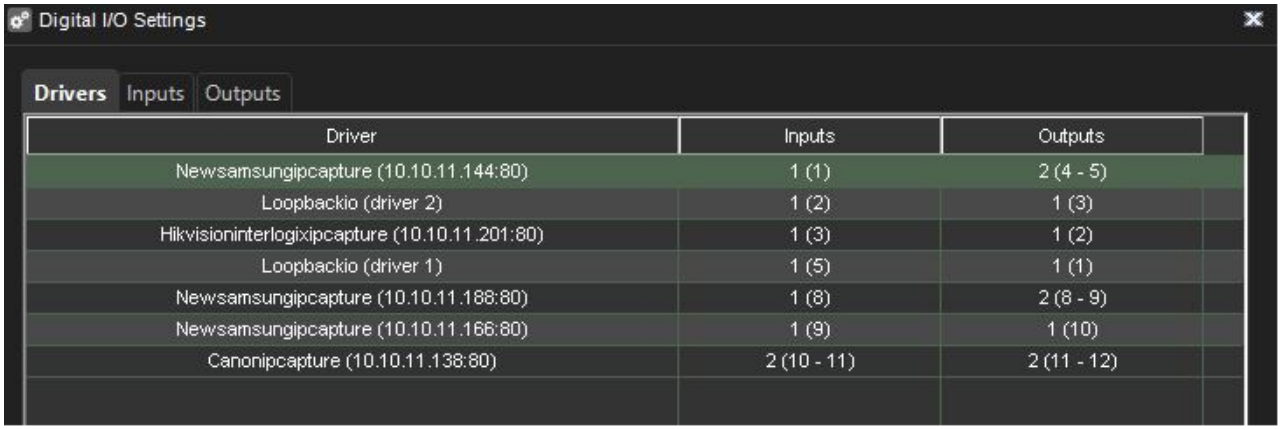



## 9.8.1 Digital I/O Settings

In **Digital I/O** settings, you can add digital input and output devices and configure the input and output settings.
These sections describe how to set up digital I/O devices.

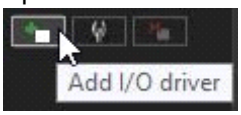
### 9.8.1.1 Drivers

In addition to the default digital I/O drivers included in the system, new drivers can be added to the system by installing them as plugins.
Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.




To take an I/O device driver into use:

1. If necessary, install the device driver package.
2. Open the **VMS Servers** tab.




1. Select the correct server and open the **Digital I/O** page from the menu.
2. Click **Add I/O driver** in the lower right corner of the screen.
3. Select the driver from the **Model** drop-down menu.
4. Configure the device settings in the **Properties** list.
5. To save the settings, click **OK**.

***Note:*** *After configuring a digital I/O device driver, you may need to configure the inputs and/or outputs.*

To edit I/O device driver settings:

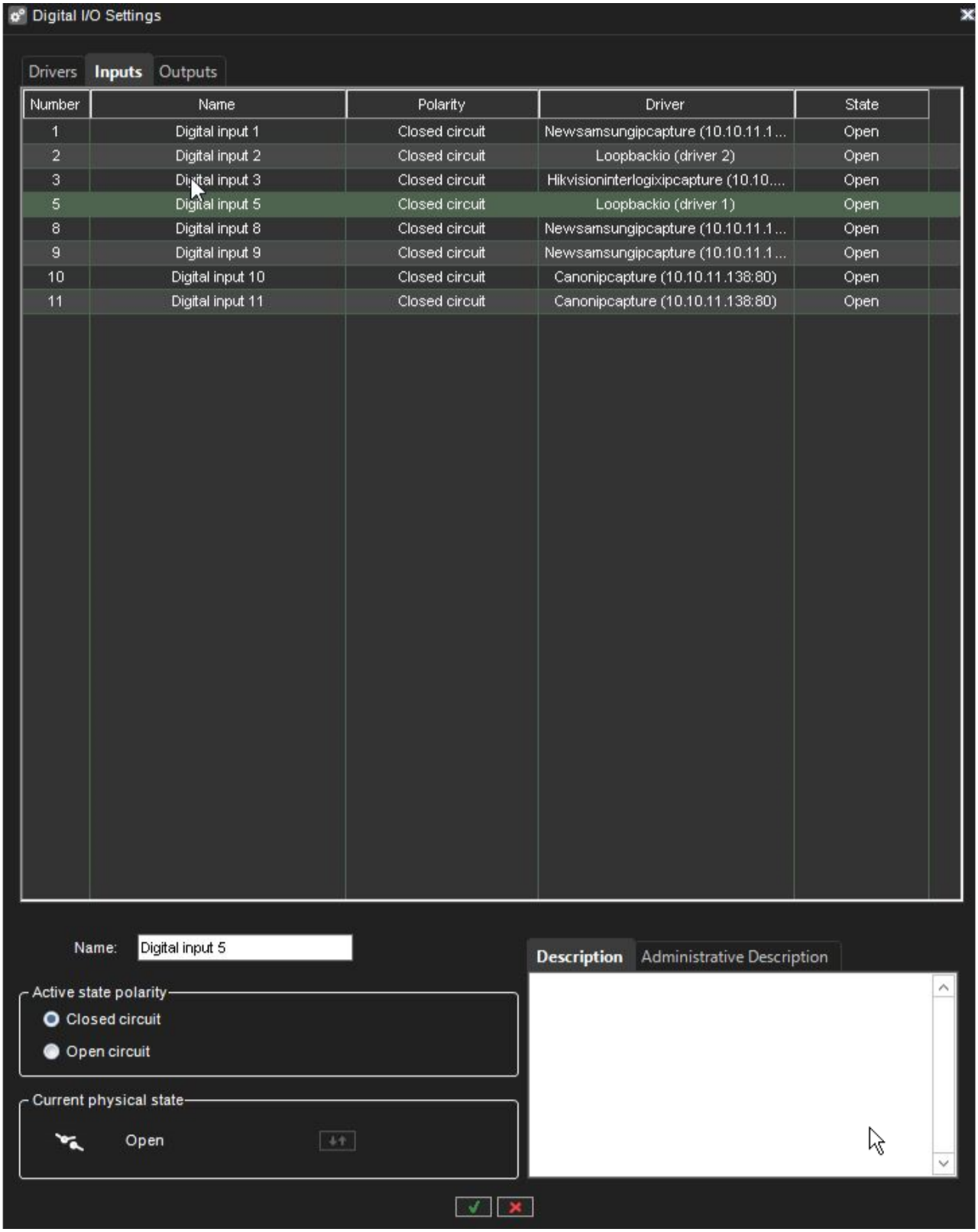
1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Double click on the device driver you want to edit.
4. Edit the device settings in the **Properties** list.
5. To save the settings, click **OK**.

To delete an I/O device driver:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Click on the I/O device driver you want to delete.
4. Click **Delete I/O driver** in the lower right corner of the screen.
5. Click **Ok** to confirm the deletion.

### 9.8.1.2 Digital Inputs

You can use digital inputs to activate alarms.
In digital input settings, set the polarity of the inputs. Set the alarm actions in alarm settings.




**Name.** To rename an input, select the input and then type a new name for the input in **Name.Active state polarity.** Select the input and then select if the input is activated when the circuit is opened or closed. **Current physical state.** Shows the state of a relay in real-time (**Open** or **Closed**).

**Description.** Here you can type a description of the selected input shown to all users in the Spotter program.
**Administrative Description**. Here you can type a description of the selected input shown in the Spotter program to only system administrators.

#### 9.8.1.3 Digital Outputs

In digital outputs, select if a relay is opened or closed (polarity) when the output is triggered.

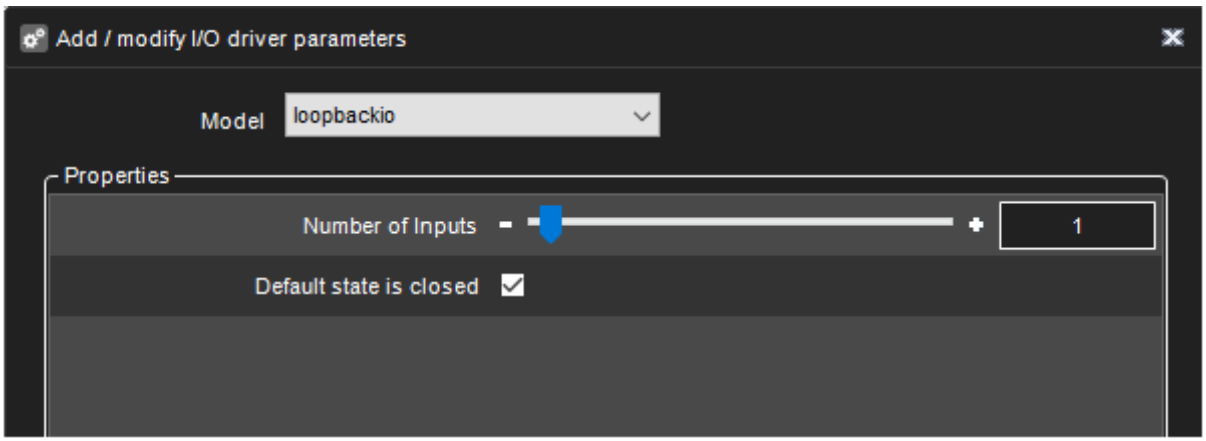
**Name.** To rename an output, select the output and then type a new name for the output in **Name**.
**Active state polarity.** Select the output and then select if the output is closed or opened when it is activated.
**Current physical state.** Shows the state of a relay in real-time (**Open** or **Closed**).
**Description.** Here you can type a description of the selected output shown to all users in the Spotter program.
**Administrative Description**. Here you can type a description of the selected output shown in the Spotter program to only system administrators.

To test a digital output, click the **Change State (Toggle)** button.

### 9.8.2 LoopBack I/O

The LoopBack I/O allows you to create virtual I/O devices where the input is directly connected to the output.

This driver enables you to create buttons in the Spotter application to trigger alarms manually.




### 9.8.3 Logical I/O

With Logical I/O, it is possible to create actions based on the OR and AND operators.

The I/O driver emulates an external I/O that is connected to itself. Example:

For example, if the customer wants to confirm that an Automatic Number Plate Recognition (ANPR) event is triggered when a car is in front of the camera, the Logical I/O can be used to create a “rule” that results in action only when VCA detects a car, AND at the same time, there is an ANPR read event.

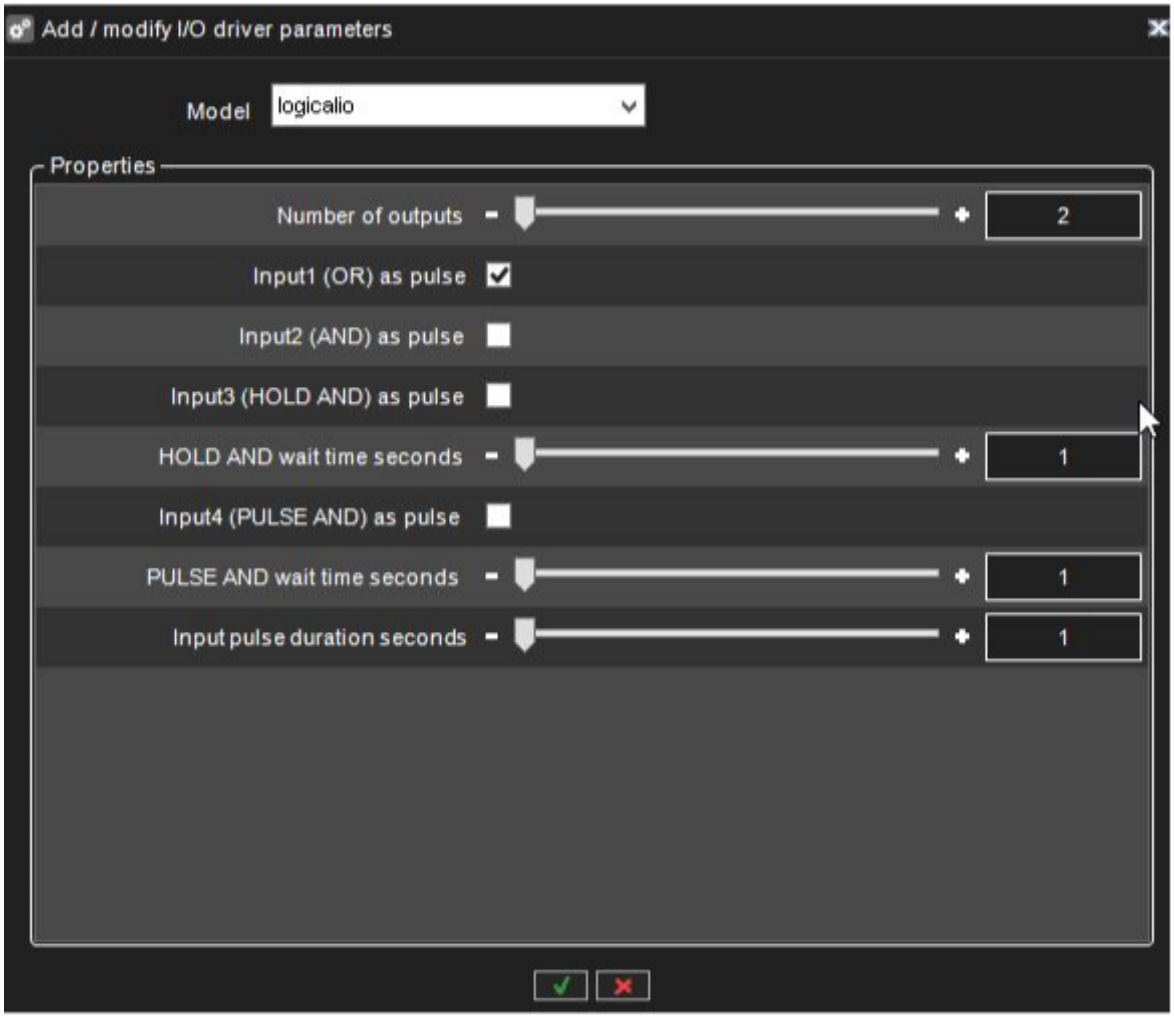
Another example could be that an entry “gate” with two doors only allows the second door to be opened when the first one is closed.

Logical I/O can be operated from the same interface as the rest of the Digital I/O in System Manager.

A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

When a new Logical I/O is being added, the first option in the dialogue is how many output states are used as operands in the AND/OR decision making.

The minimum number is two, and the maximum is 32.

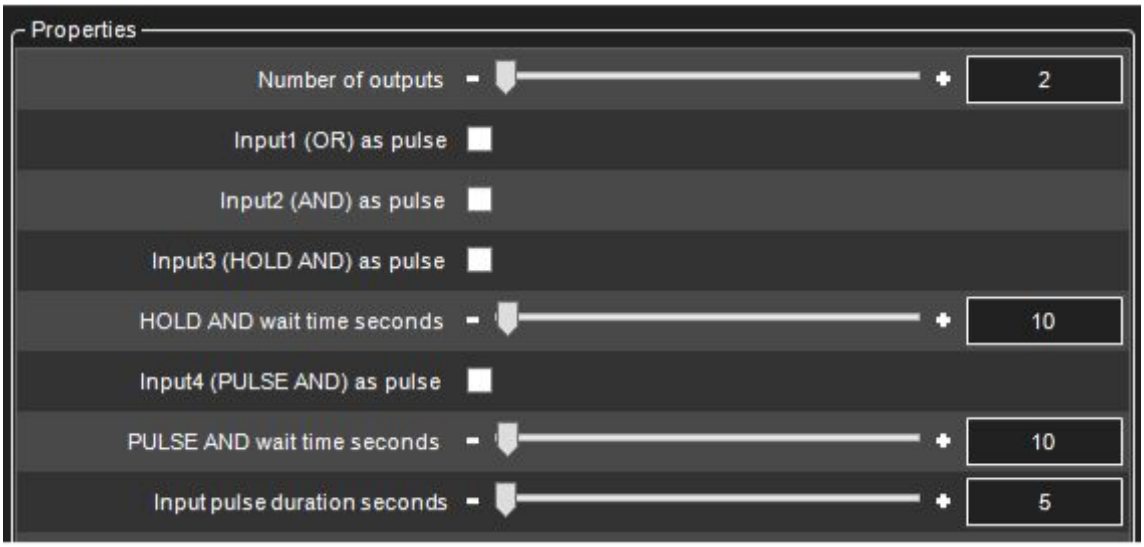



All Logical I/Os will automatically generate four inputs that can be used.

| Input | Type |
|---|---|
| 1 | OR |
| 2 | AND |
| 3 | HOLD AND |

| | |
|---|---|
| 4 | PULSE AND |

The following sections will describe the different inputs in more detail by using the below example:

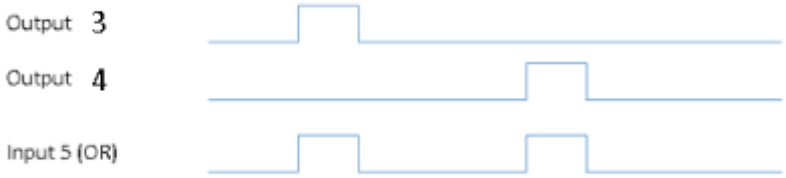



The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

The automatically created 4 inputs are seen in the list as inputs 5,6,7 and 8.

### 9.8.3.1 **“OR” Input**

The first input that the Logical I/O will generate is OR signal. If any of the outputs are on, the OR input will be turned on.

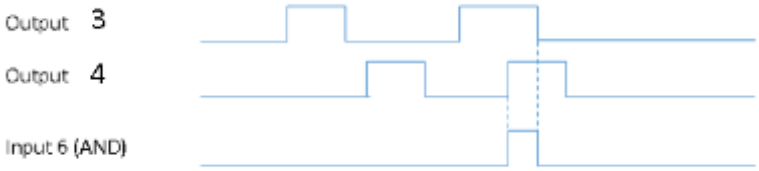



In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, input 5 will be turned on as a result.

Input will remain on as long as any of the outputs remains on. (Unless pulse mode is selected, see below for details)

### 9.8.3.2 **“AND” Input**

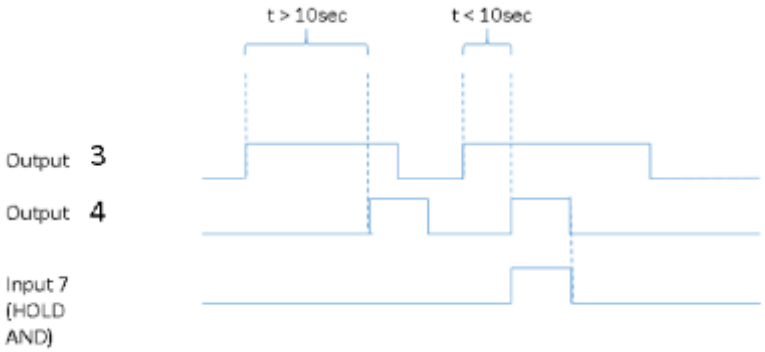
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.




Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details)

### 9.8.3.3 "HOLD AND" Input

HOLD AND input become active if all the outputs are active simultaneously, and the time from the first activation to the last activation is less than the time defined in the HOLD AND wait time slider.



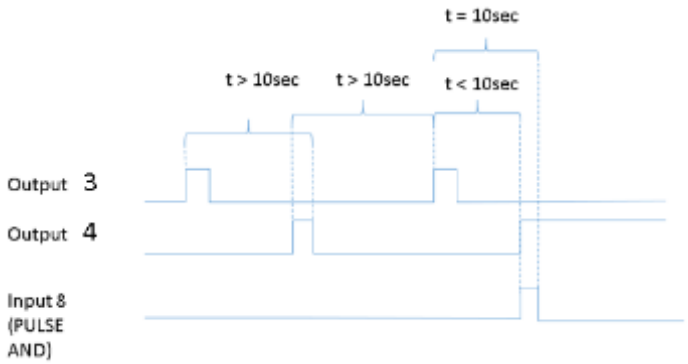

In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details

### 9.8.3.4 "PULSE AND" Input

PULSE AND input will become active if all outputs *have been* active within a specified time.

In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then input 8 will be turned on.

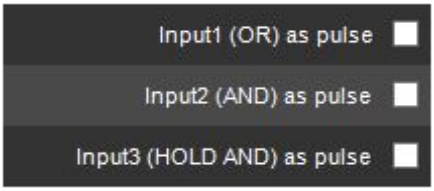



Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

In our example, when 10 seconds have elapsed from output 3 activation, input 8 will be turned off.

### 9.8.3.5 Pulse Mode For Inputs

For each of the four inputs, it is possible to define pulse mode to be in use.



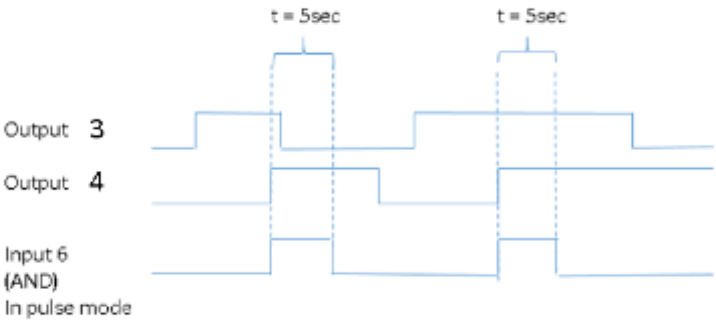

and


The pulse duration can also be adjusted.


If the pulse mode is in use, the input will turn off after the set pulse duration.

If in our example, we would set the AND input to be in pulse mode like this:


It would mean behaviour like this:




## 9.8.4 Countdown I/O

With Countdown I/O, it is possible to create actions based on whether some events happen or do not happen at a defined period.

When a new Countdown I/O is created in System Manager, it automatically creates 4 inputs and 4 outputs.

Countdown I/O has two basic modes. The first two input/output pairs are of type 1, and the last two pairs are of type 2.

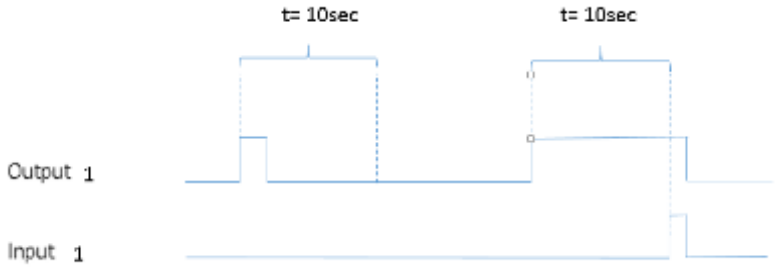
A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

### 9.8.4.1 Event Duration Exceeded Mode (Type 1)

Firstly, it is possible to trigger an alarm if some event takes longer than the planned duration.

For example, let's say the time is 10 seconds. If output one is triggered and stays active for less than the defined duration, there is no alarm.

If the output is triggered and stays active for longer than the defined duration, there is an alarm.



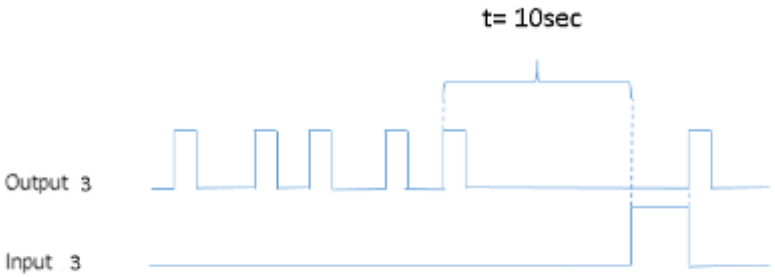

When creating a new Countdown I/O, the first two input-output pair is of this type.

### 9.8.4.2 Expected Trigger Mode (Type 2)

Secondly, it is possible to trigger an alarm if an expected pulse is not received inside the defined time.

For example, the time is 10 seconds, and we expect the regular operation to get pulses from output 3 every 2-3 seconds.

When the pulse is missing for longer than 10 seconds, the input state is changed to active. It stays active until the next output trigger is received.



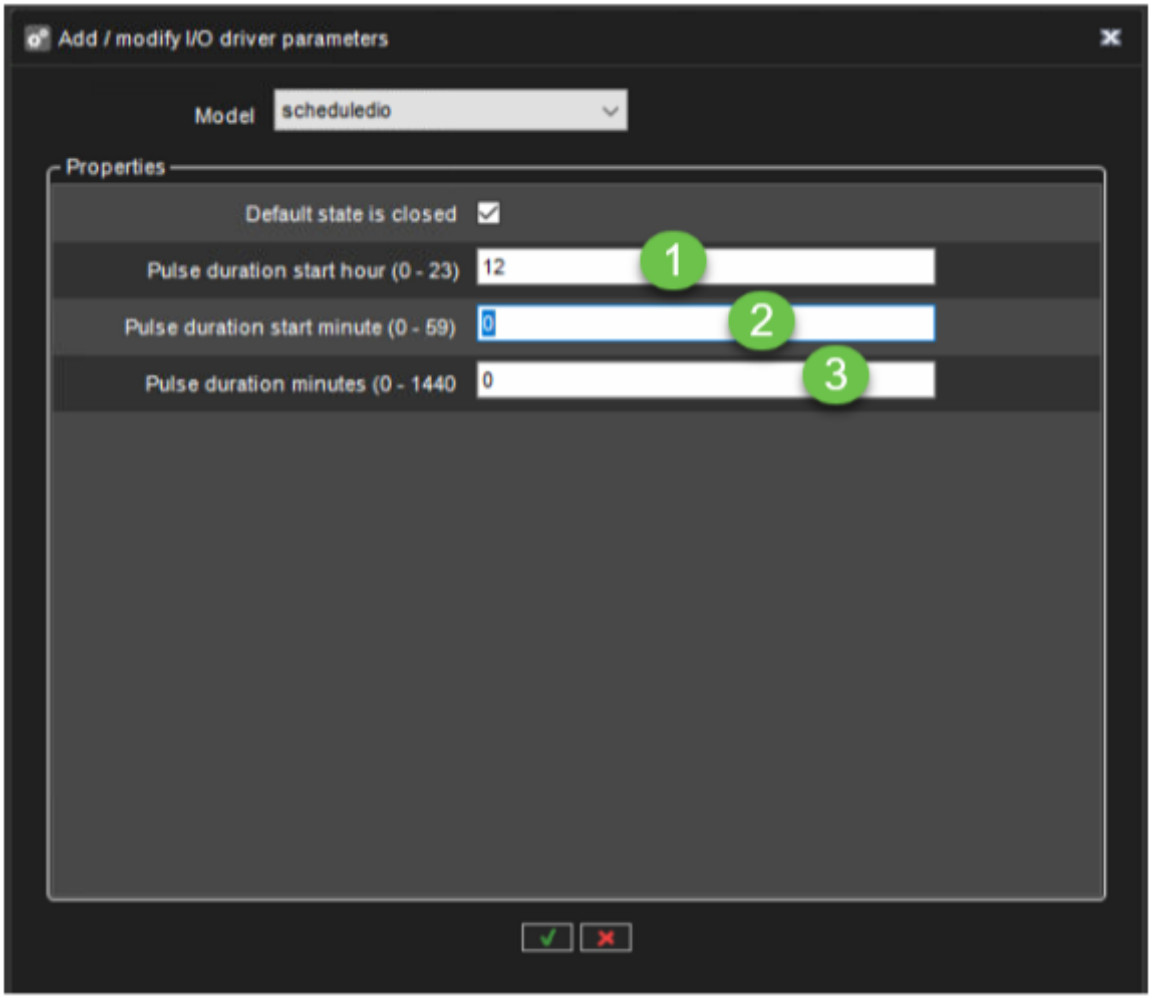

When creating a new Countdown I/O, the last input-output pair is of this type.

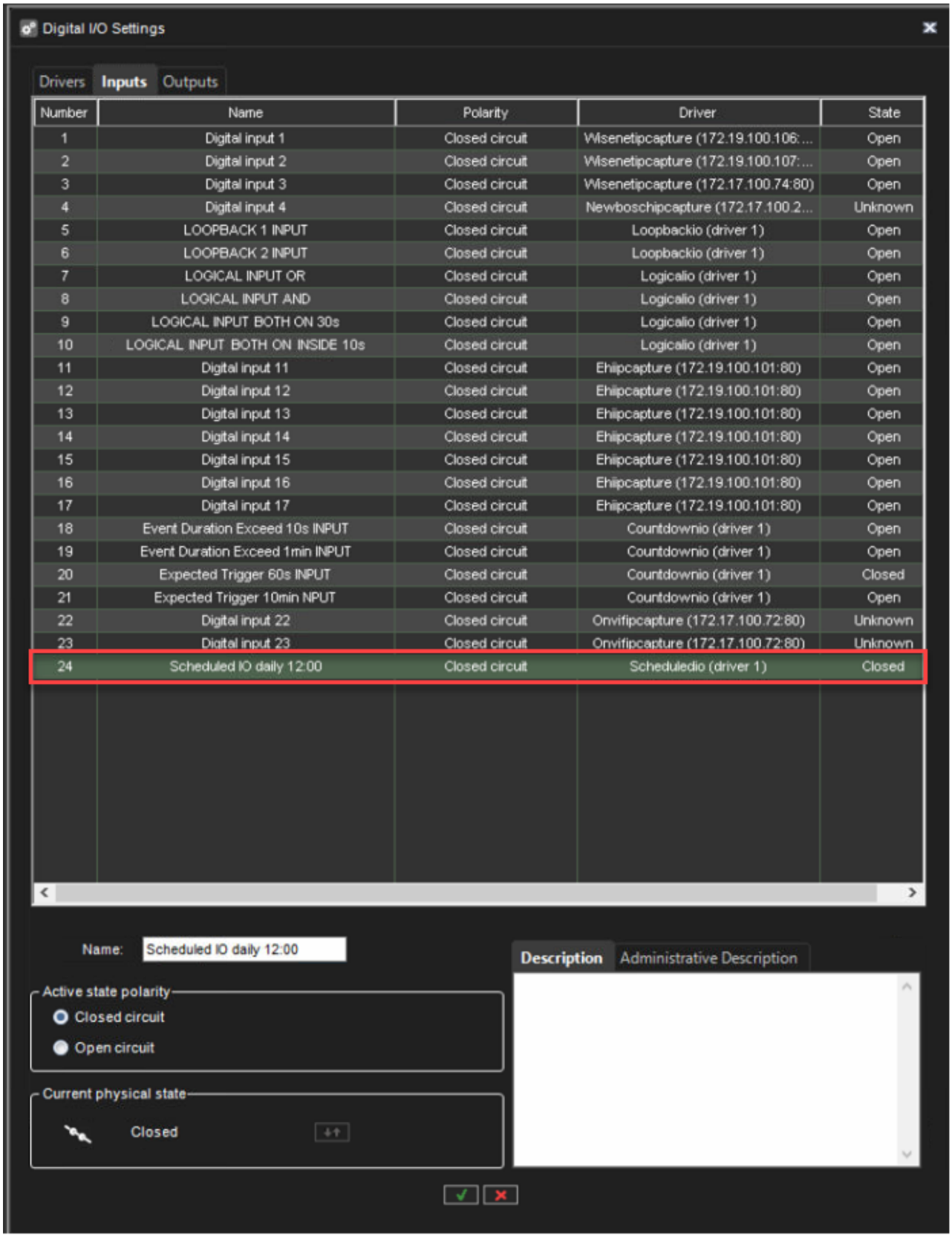
### 9.8.5 Scheduled IO

9.8.5.1 With the Scheduled IO is possible to create a schedule for any digital output, which are connected to the VMS server.

9.8.5.2 Only the same VMS server digital outputs can be scheduled.

1. Set Pulse duration start an hour
2. Set Pulse duration start minute
3. Set Pulse duration minutes




Digital I/O Settings
Drivers
Inputs
Outputs
Number
Name
Polarity
Driver
State
1 Digital input 1 Closed circuit Wisenetipcapture (172.19.100.106:... Open
2 Digital input 2 Closed circuit Wisenetipcapture (172.19.100.107:... Open
3 Digital input 3 Closed circuit Wisenetipcapture (172.17.100.74:80) Open
4 Digital input 4 Closed circuit Newboschipcapture (172.17.100.2... Unknown
5 LOOPBACK 1 INPUT Closed circuit Loopbackio (driver 1) Open
6 LOOPBACK 2 INPUT Closed circuit Loopbackio (driver 1) Open
7 LOGICAL INPUT OR Closed circuit Logicalio (driver 1) Open
8 LOGICAL INPUT AND Closed circuit Logicalio (driver 1) Open
9 LOGICAL INPUT BOTH ON 30s Closed circuit Logicalio (driver 1) Open
10 LOGICAL INPUT BOTH ON INSIDE 10s Closed circuit Logicalio (driver 1) Open
11 Digital input 11 Closed circuit Ehiipcapture (172.19.100.101:80) Open
12 Digital input 12 Closed circuit Ehiipcapture (172.19.100.101:80) Open
13 Digital input 13 Closed circuit Ehiipcapture (172.19.100.101:80) Open
14 Digital input 14 Closed circuit Ehiipcapture (172.19.100.101:80) Open
15 Digital input 15 Closed circuit Ehiipcapture (172.19.100.101:80) Open
16 Digital input 16 Closed circuit Ehiipcapture (172.19.100.101:80) Open
17 Digital input 17 Closed circuit Ehiipcapture (172.19.100.101:80) Open
18 Event Duration Exceed 10s INPUT Closed circuit Countdownio (driver 1) Open
19 Event Duration Exceed 1min INPUT Closed circuit Countdownio (driver 1) Open
20 Expected Trigger 60s INPUT Closed circuit Countdownio (driver 1) Closed
21 Expected Trigger 10min NPUT Closed circuit Countdownio (driver 1) Open
22 Digital input 22 Closed circuit Onvifipcapture (172.17.100.72:80) Unknown
23 Digital input 23 Closed circuit Onvifipcapture (172.17.100.72:80) Unknown
24 Scheduled IO daily 12:00 Closed circuit Scheduledio (driver 1) Closed
Name:
Scheduled IO daily 12:00
Description
Administrative Description
Active state polarity
Closed circuit
Open circuit
Current physical state
Closed

## 9.8.6 HTTP IO

### 9.8.6.1 Properties

**HTTP Method(Opened)**

- GET
- PUT
- POST
- DELETE

**URL(Opened)**

**Content(Opened)**

**User(Opened)**

**Password(Opened)**

**HTTP Method(Closed)**

- GET
- PUT
- POST
- DELETE

**URL(Closed)**

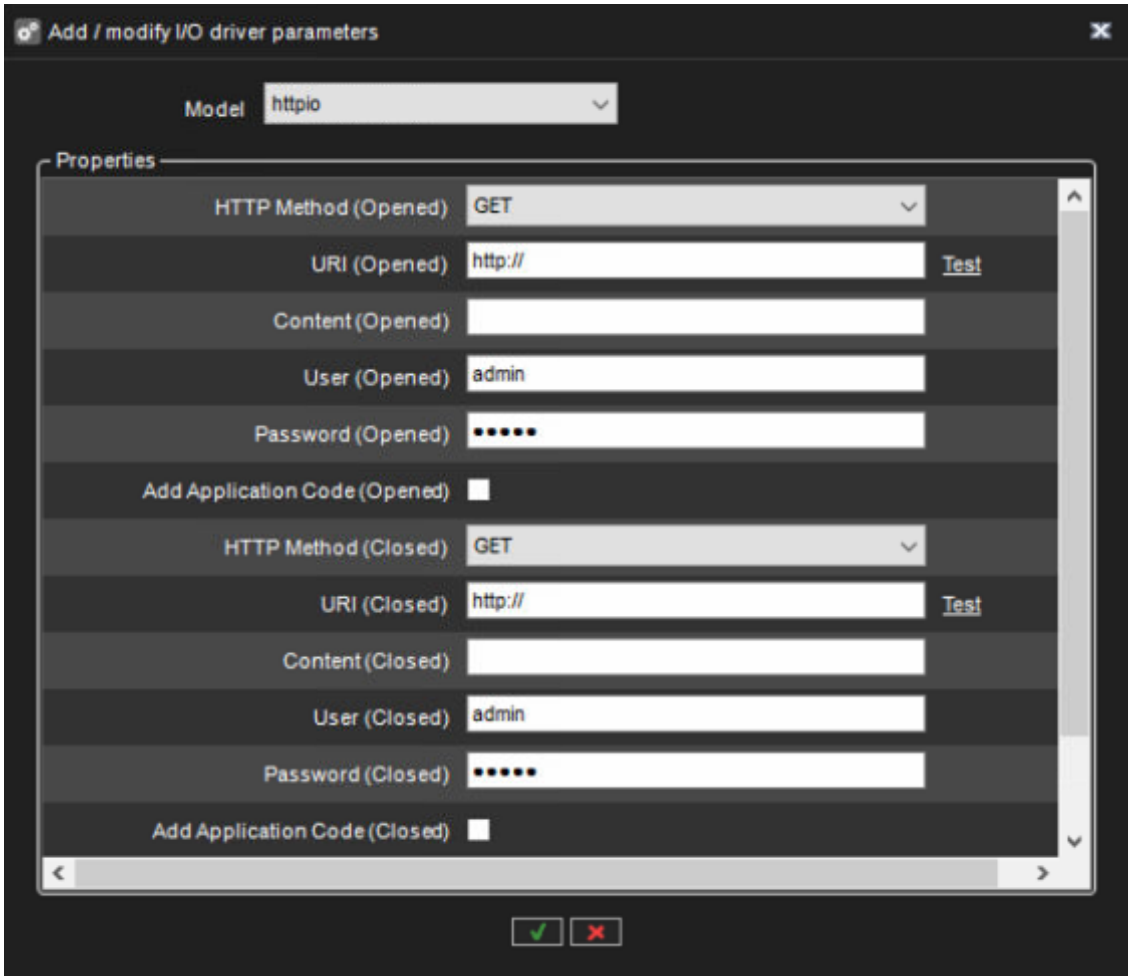
**Content(Closed)**

**User(Closed)**

**Password(Closed)**

**Authentication**

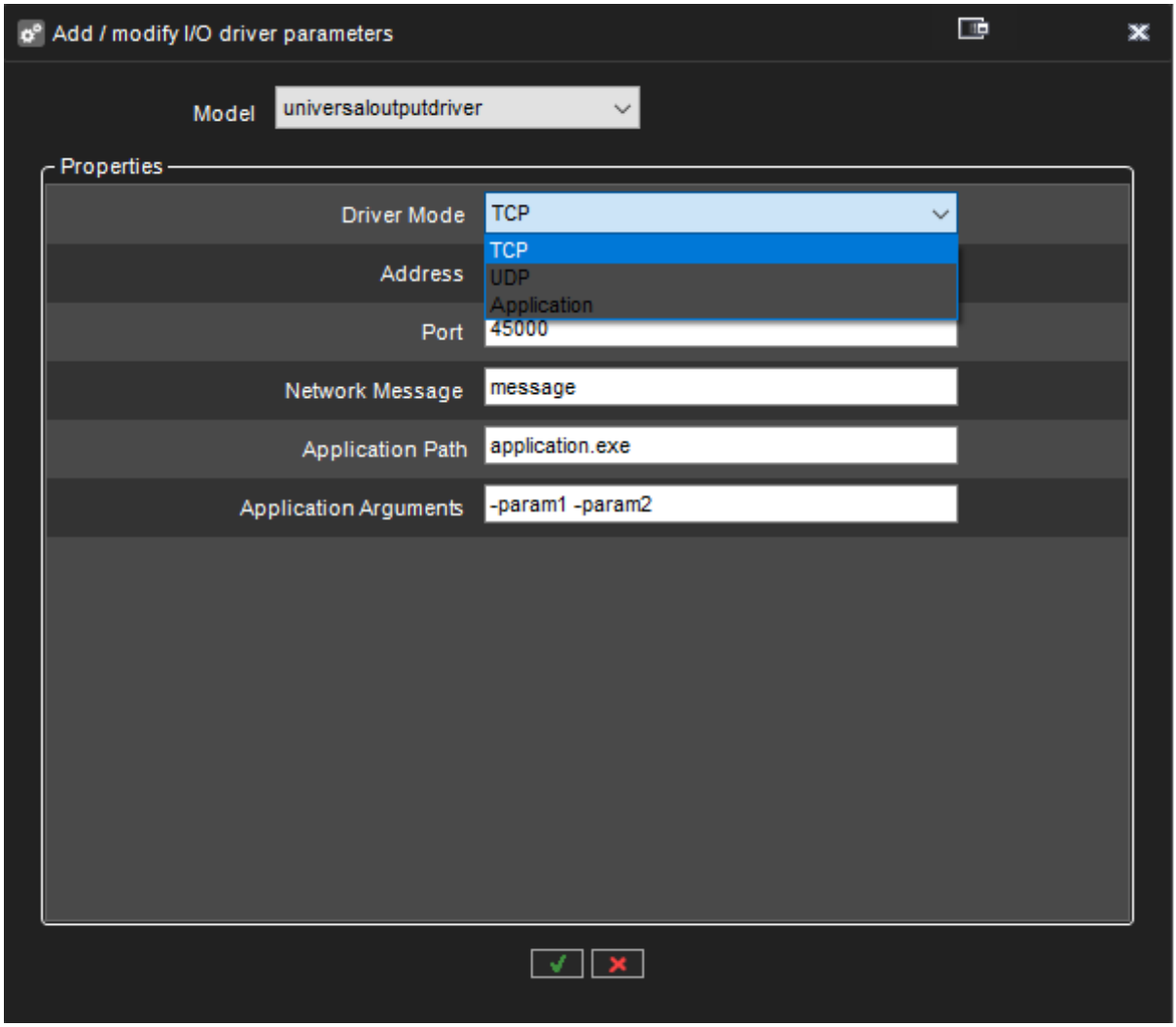
- BASIC
- DIGEST



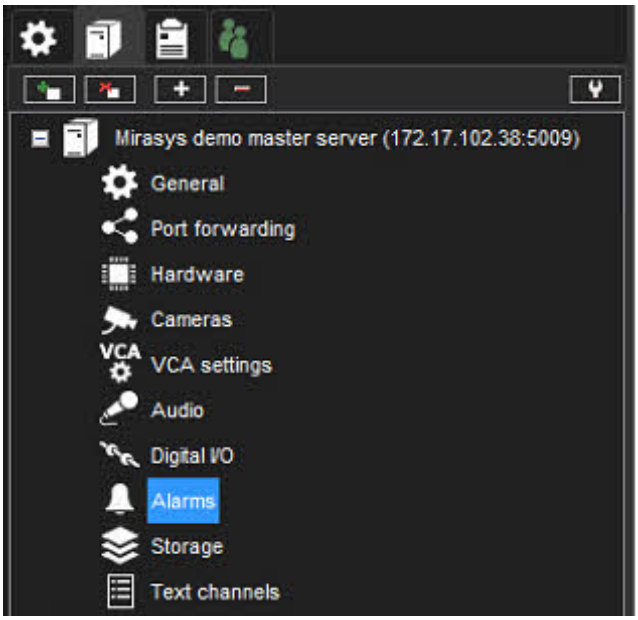

### 9.8.7 UniversalOutputDriver

This driver enables you to send data to 3rd party systems or start applications on the server or remote systems.

Please see additional documentation for this driver from our extranet or contact support.


Add / modify I/O driver parameters
Model
universaloutputdriver
Properties
Driver Mode
TCP
TCP
UDP
Application
Address
Port
45000
Network Message
message
Application Path
application.exe
Application Arguments
-param1 -param2

# 9.9 Alarms




## 9.9.1 Alarm Settings

The alarm management tools enable the creation of server-specific alarms based on various triggers based on motion, sound level or specific text data triggers.

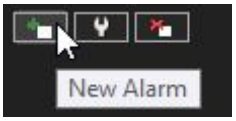
In addition, the triggers can include custom-made third-party triggers.

Alarms can be created, edited and deleted through the **Alarms** screen in the **VMS Servers** tab.

## 9.9.2 Adding a New Alarm

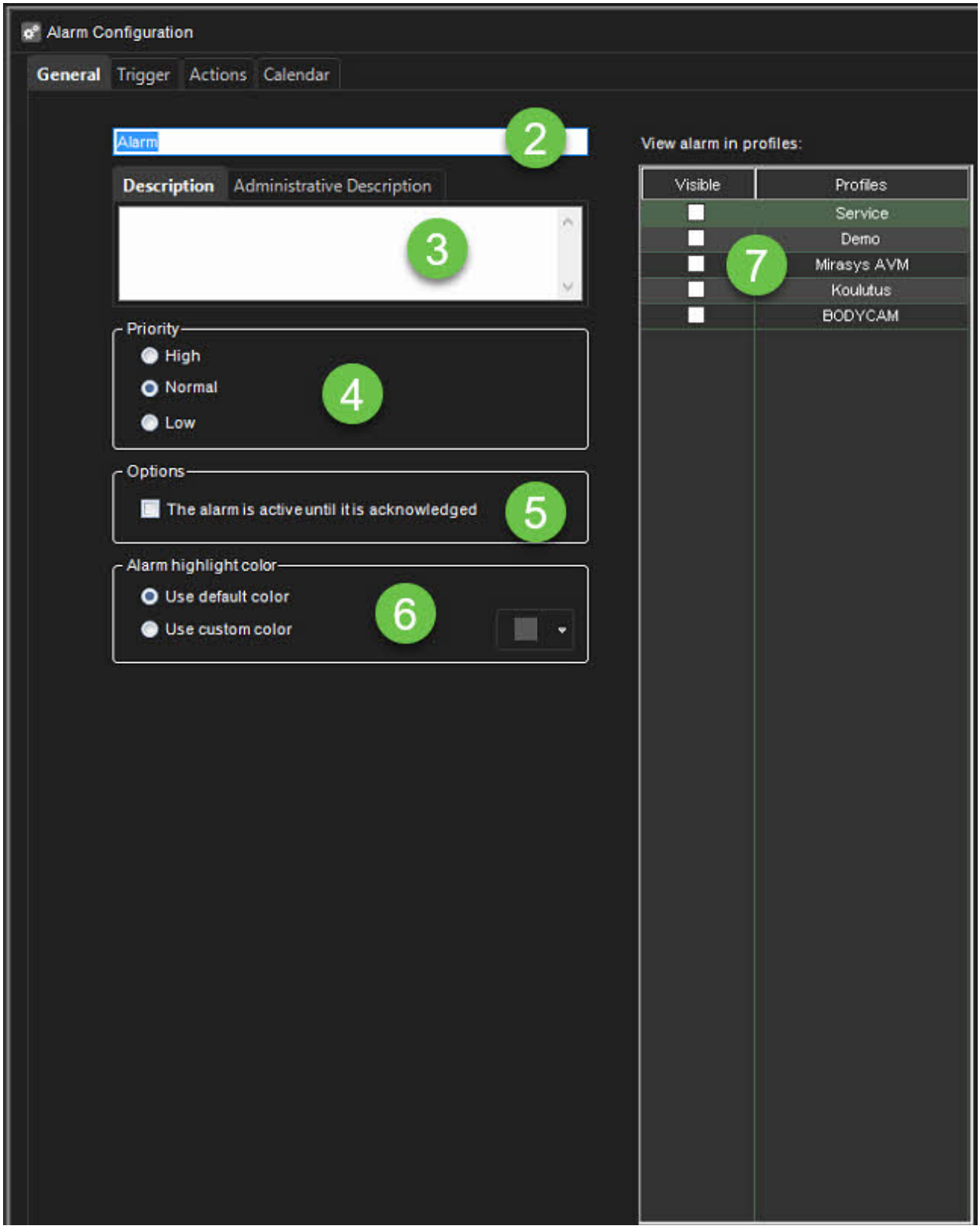
### 9.9.2.1 General

1. Click New Alarm at the lower-left corner of the Alarms screen.



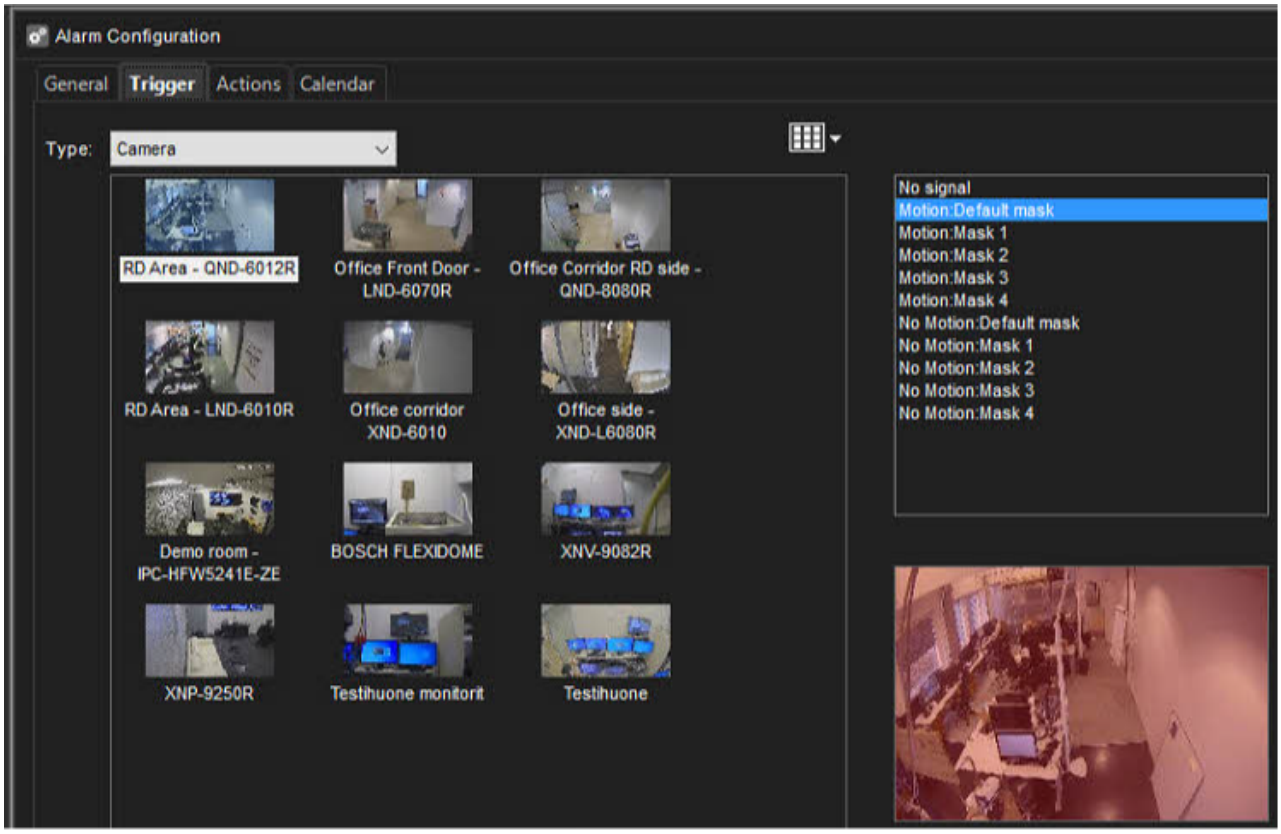

2. Type the name of the new alarm in the **Name** field.
3. Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.
4. Select whether the alarm is of **high**, **average** or **low priority**. The priority is used to define the order in which alarms are executed in case of multiple simultaneous alarms.

5. Select **The Alarm is active until it is acknowledged** to create the alarm as continuous; if the option is selected, the alarm will continue until a user acknowledges it through the **Spotter** application.
6. **Alarm highlight colour** allows administrators to define a custom colour for each alarm separately.
7. In the **View Alarms in Profiles** menu, select the profiles in which the alarm will be used. *Note: Alarms can also be added to profiles through the **Profiles** tab.*


Alarm Configuration
General
Trigger
Actions
Calendar
Alarm
2
Description
Administrative Description
3
Priority
High
Normal
4
Low
Options
The alarm is active until it is acknowledged
5
Alarm highlight color
Use default color
6
Use custom color
View alarm in profiles:
Visible
Profiles
Service
Demo
7
Mirasys AVM
Koulutus
BODYCAM

### 9.9.2.2 Trigger

8. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.




9. Select the trigger type from the **Type** drop-down menu.

    1. Camera
    2. Audio
    3. Metadata
    4. Text data
    5. Digital input

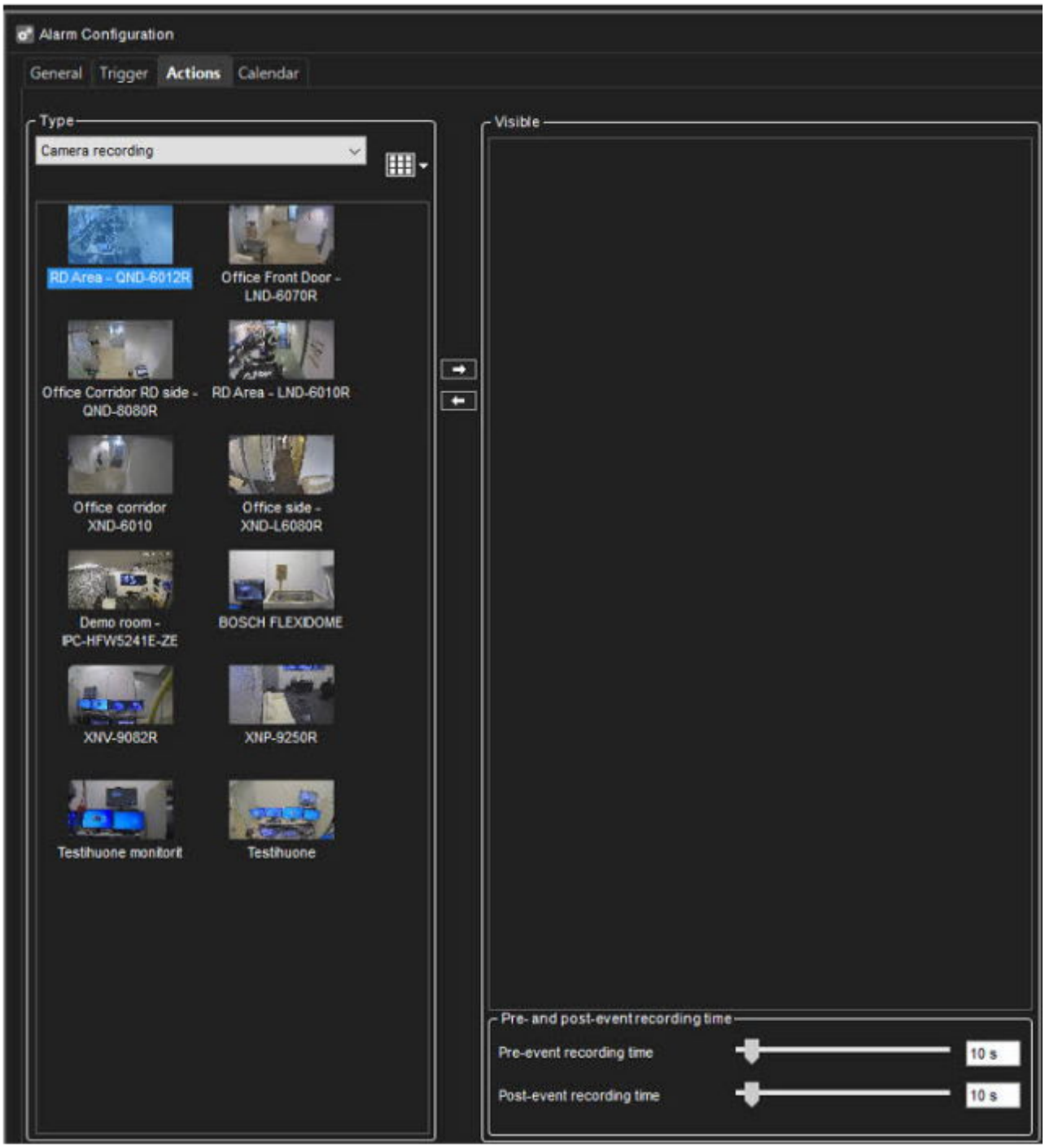
10. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.
11. Select the triggering condition from the condition list on the right side of the screen.

    1. For camera-based triggers, you can select the mask used in motion detection to trigger the alarm.
    2. For audio-based triggers, you can set the alarm to trigger based on a high or low audio level.
    3. For text data based (e.g., VCA, metadata, etc.) triggers, you can set the alarm to trigger based on a text data string.
       In addition, you can set an optional alarm ending trigger by marking **Define ending input** and selecting a string for ending the alarm.

4. For digital input-based triggers, the alarm is triggered based on the change of the input's polarity.

### 9.9.2.3 Actions

12. Open the **Actions** tab. The **Actions** tab is used to define the actions performed by the alarm when it is triggered.



13. Select the action type from the **Type** drop-down menu. The action type defines the basic functionality of the alarm.

## 9.9.2.4 Action Types and Settings

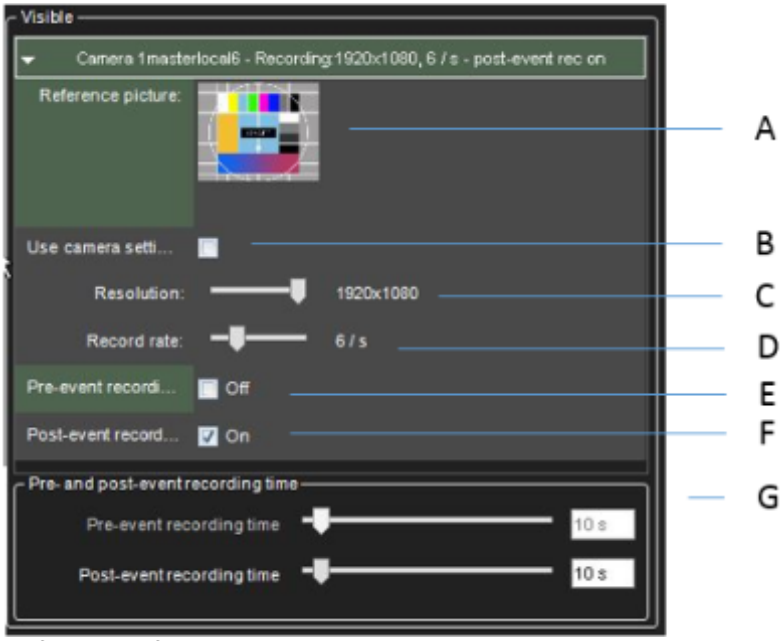
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

***Note:*** *In addition to the default actions, the system may include alarm actions installed through third-party modules.*

### 9.9.2.4.1 Camera Recording

Camera recording is the default action for cameras. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the camera's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Camera recording** action are displayed in the alarm pop-up view when the alarm is triggered.




The action includes the following fields and parameters:

**A) Reference picture**. This static field contains the reference picture (image) of the camera.

**B) Use camera settings**. The alarm recording will be performed using the camera-specific resolution and record rate setting by marking this checkbox.

**C) Resolution**. Use the slider to change an IP camera's resolution during alarm recording. The slider is active only for IP cameras.

**D) Record rate**. Use the slider to change the camera's IPS rate during alarm recording. The slider is inactive if the **Use camera settings** checkbox is marked.

**E) Pre-event recording**. Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider.

**F) Post-event recording**. Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider.

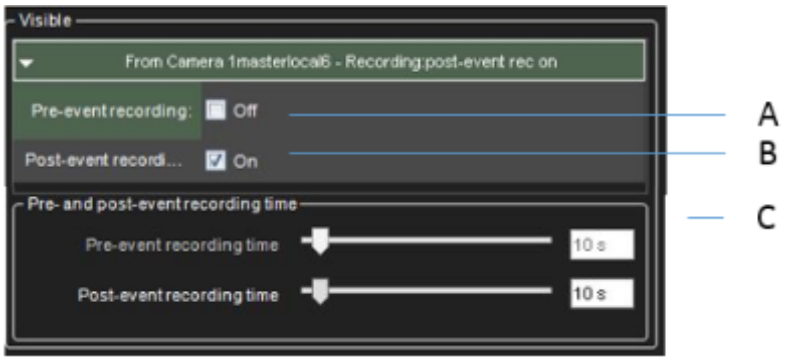
**G) Pre- & post-event recording duration**. These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

***Note*** *All devices (cameras and microphones) are connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.*

#### 9.9.2.4.2 Audio Recording

Audio recording is the default action for microphones. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the microphone's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Audio recording** action are displayed in the alarm pop-up view when the alarm is triggered.




The action includes the following fields and parameters:

**A) Pre-event recording**. Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider.

**B) Post-event recording**. Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider.

**C) Pre- & Post Recording duration**. These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

***Note:*** *All devices (cameras and microphones) connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.*

#### 9.9.2.4.3 Digital output

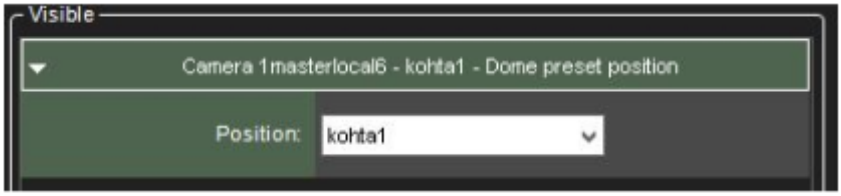
The d**igital output** is the default action for digital I/O devices. When an alarm that contains this action type is triggered, the I/O device is activated.

***Note:*** *Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

#### 9.9.2.4.4 PTZ (Dome) Preset Position

*The **PTZ preset position** action can be used to set a PTZ camera to a specified preset position. When an alarm that contains this action type is triggered, the PTZ camera will automatically move to the selected preset position. Please see Mirasys VMS Spotter User's Guide for information on setting PTZ camera preset positions.*

It should be noted that this action moves the PTZ camera to a preset position but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.




The action includes the following fields and parameters:

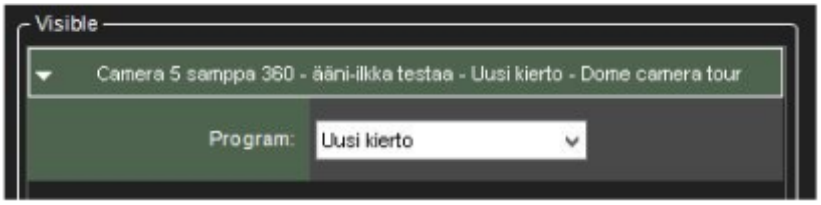
- **Position**. Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

***Note:** Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

#### 9.9.2.4.5 PTZ (Dome) Camera Tour

The **PTZ camera tour** action can be used to set a PTZ camera to start a pre-programmed PTZ camera tour. When an alarm that contains this action type is triggered, the selected PTZ camera tour is started. Please see *Mirasys VMS Spotter User's Guide* for information on setting PTZ camera tours.

It should be noted that this action starts the PTZ camera tour but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.



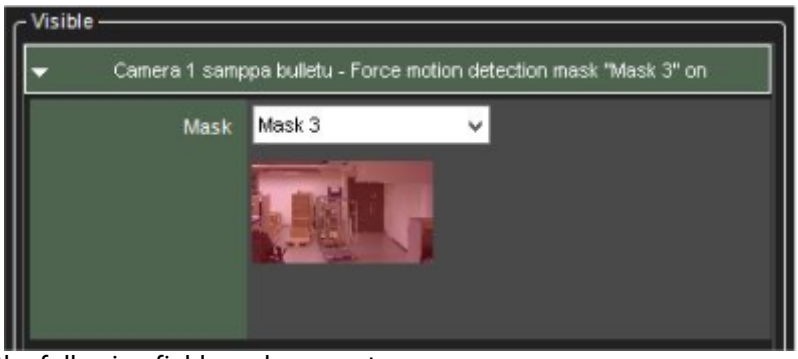

The action includes the following fields and parameters:

- **Program**. Use the drop-down menu to select the PTZ camera tour, starting when the alarm is triggered.

***Note:** Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

#### 9.9.2.4.6 Set Motion Detection Mask

The **Set motion detection mask** action can change the motion detection mask used by a specific camera during the alarm. When the alarm occurs, the motion detection mask used for the designated camera is changed to the alarm specific mask. After the alarm ends, the system restores the default mask.




The action includes the following fields and parameters:

- **Mask**. Use the drop-down menu to select the motion detection mask that will be used during the alarm.

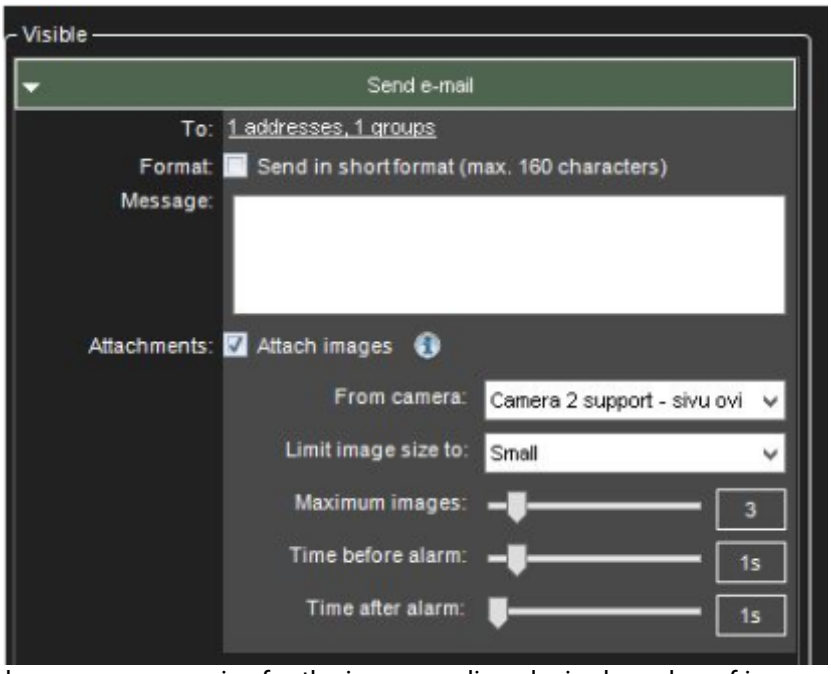
***Note:*** *Even though the* ***Pre- & Post Recording duration*** *sliders are displayed for the action type, they do not affect the functionality of the action.*

#### 9.9.2.4.7 Send E-Mail

The **Send e-mail** action can be used to send e-mail to any email address or group configured in the **E-mail settings** in the **System** tab.

You can choose which recipient or group should receive the alarm.

You can also include one or more unscaled or scaled-down images in the alarm email. To do this, uncheck the **Send in a short format** -option and check the **Attach images** –option




After this, you can choose a camera, size for the image scaling, desired number of images, and the time span from which the images are fetched.

**Note:**

- The number of images in this configuration is the maximum amount delivered. Fewer images might arrive
- Attaching images to alarm emails might lead to high data traffic, so it is recommended to test the configuration settings to find the optimum setting.
- If you experience issues that no images are arriving with the default settings, it is recommended to select more than one image to the “maximum images” setting and adjust the sliders slightly to have a longer duration of time where the images are being fetched.

The action includes the following fields and parameters:

**Format** – Defines the message format as short or usual.

- A short message will contain only up to 160 characters and cannot contain additional message text or image attachments (see below).

**Message** – This field contains the message that will be sent to the recipients if the alarm occurs. The message field is active only if the e-mail format has been set as long.

**Note:**

- *Unlike other alarm actions, the **Send e-mail** action can be selected only once for each alarm. Once selected, the action will disappear from the list of available actions.*
- The message will have the alarm name in the title.

#### 9.9.2.4.8 Disable Alarms

The **Disable alarms** action can be used to send disable alarms based on one alarm. The configuration can be done so that all alarms are disabled, low and medium priority alarms, or low alarms.

This option allows specific alarms to remain active while others are suppressed.

The alarms are disabled only while the alarm that disables them is active.

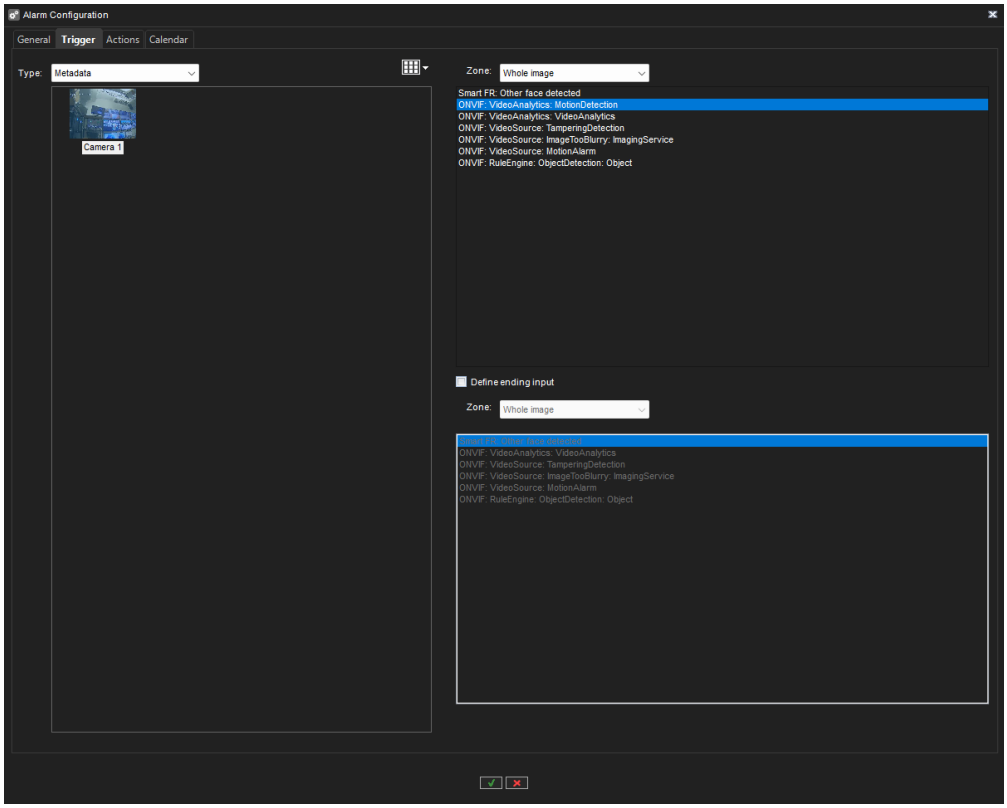
## 9.9.2.5 ONVIF Profile M

ONVIF profile M support enables our system to respond to the triggering of an alarm generated by camera analytics.

### 9.9.2.5.1 ONVIF alarm

When you have added a device that supports ONVIF Profile M, you do not need to take any special steps to enable or disable these triggers. They are automatically added to the camera's metadata triggers.

In the Alarm Configuration in System Manager, this will be displayed in the **Trigger tab** and listed as ONVIF. You can use these to create new alarms.




### 9.9.2.5.2 Creating an ONVIF alarm trigger

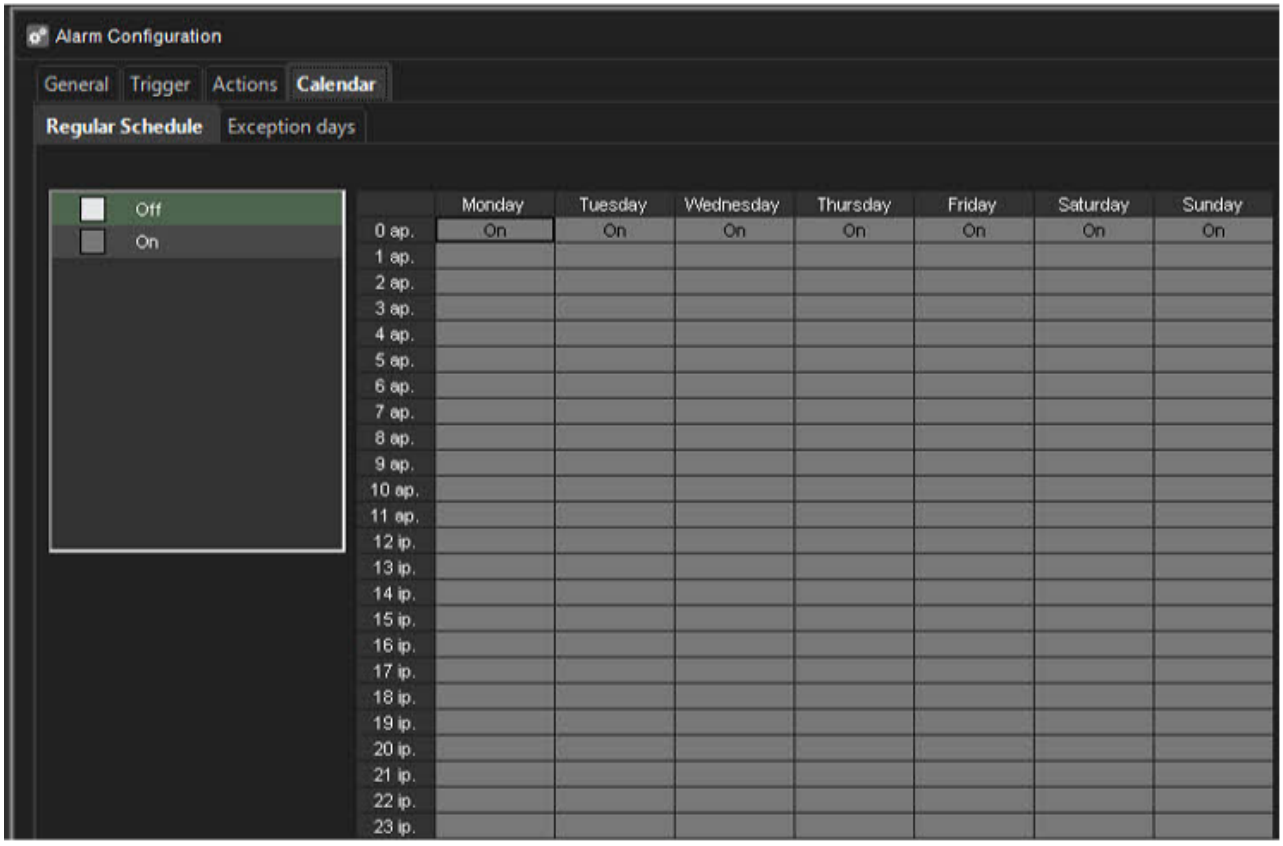
**Note** that device alarms/triggers itself should be configured using device web interface, not in the System Manager.

This configuration should be done **before** you add device to VMS. Otherwise device capabilities should be refreshed in System Manager for it to include the changes in device.

1. Start the System Manager desktop application.
2. Add a device with ONVIF Profile M support.
3. Go to the VMS Servers tab.
4. Select **Alarms**.
5. Select a **New Alarm**.
6. The **General** tab opens. Name the alarm in the general tab, and select which profiles will use the alarm.
7. Go to the **Trigger** tab.
8. Select **Metadata** as the type.
9. Select the type of ONVIF metadata you want to use to trigger the alarm.
10. Go to the **Actions** tab and select the desired action for the alarm.
11. Go to the **Calendar** tab and select which days/hours are enabled for the alarm. By default, the alarm is active 24 hours each day.
12. Click the OK checkmark ☑ at the bottom of the page

#### 9.9.2.6 Calendar

1. Define that when the alarm is active
2. Click **OK**




### 9.9.3 Holiday Schedules

Alarm specific holiday schedules can create schedules for specific dates or set a specific date to use an alarm schedule designed for another weekday. The **Holidays** sub-tab can be accessed through the alarm's **Schedule** tab.

#### 9.9.3.1 To set a specific date to function with another weekday's schedule:

1. Select the weekday from the schedule list on the left side of the screen.
2. Select the desired year and month from the drop-down menus above the calendar.
3. Click on a date in the calendar to add the schedule.

#### 9.9.3.2 To create a custom schedule:

1. Click Add at the upper left side of the screen.

2. Type the name of the holiday schedule in the **Schedule name** field.

3. To create the schedule, select **Off** from the **On**/**Off** list on the left side of the screen and mark the hours the alarm is switched off for the day.
4. Click **OK** to save the schedule.
5. Select the desired year and month from the drop-down menus above the calendar.
6. Click on a date in the calendar to add the schedule.

#### 9.9.3.3 To edit a custom schedule:

1. Select the custom schedule from the schedule list on the left side of the screen.
2. Click **Edit** at the upper left side of the screen.

3. Edit the schedule.
4. Click **OK** to save the changes.

#### 9.9.3.4 To delete a custom schedule:

1. Select the custom schedule from the schedule list on the left side of the screen.
2. Click **Remove** at the upper left side of the screen.


#### 9.9.3.5 To restore the original schedule:

1. Click **Restore** in the schedule list on the left side of the screen.
2. On the calendar, click the day that you want to restore.

### 9.9.4 Deleting an Alarm

#### 9.9.4.1 To delete an alarm:

1. On the **VMS Servers** tab, select the server.
2. Double-click on **Alarms**.
3. Select the alarm you want to delete by clicking on its name.
4. Click **Remove Alarm** at the lower-left corner of the **Alarms** screen.
5. The alarm is deleted from the system.

# 9.10 Storage

In storage settings, you can set the storage time of the recorded video, audio and text data, and alarm data.

In addition, after adding a hard disk to a server, you can set it as additional data storage through the storage settings.

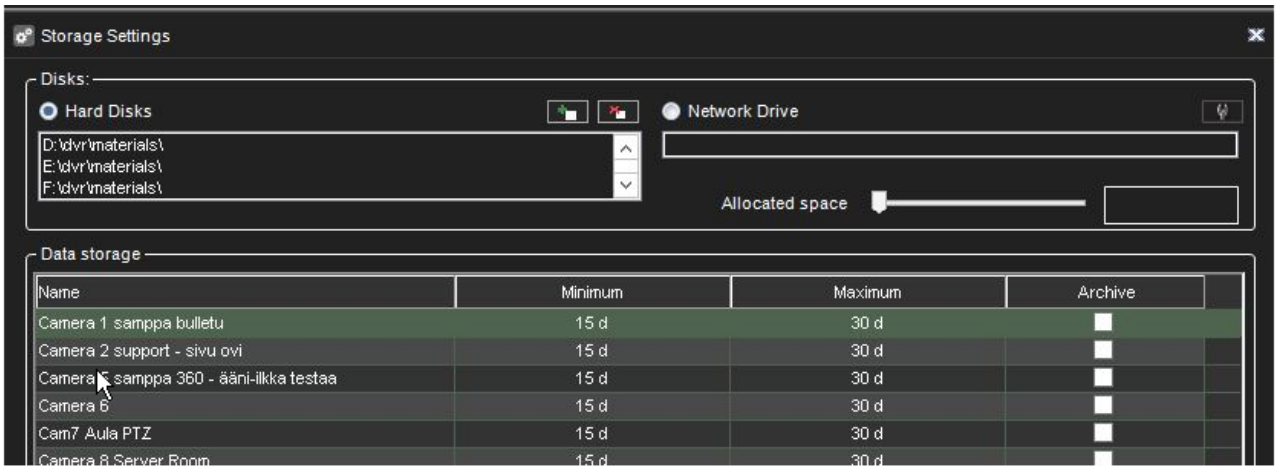
The storage settings are also used to configure the automatic archiving functionality, enabling the creation of backup copies of the server-specific video, audio, and text data daily or weekly.

Video, audio, text data, and alarm recordings are kept until their defined **Maximum** date has been exceeded or until the allocated storage space has run out.

## 9.10.1 Adding Storage Space

If additional storage space is required, you can add new hard disks or map a network drive for data storage (i.e., NAS support).

There can be multiple network storage disks, and local disks used simultaneously, as seen in the picture.




***Note:*** *When adding storage drives to legacy Mirasys filesystem (VMS server version 7.5.x or earlier), the storage drives are recommended to be all of the same capacity, and any single disk should be less than 10TB in size, and the total amount per VMS server should be less than 25 TB in size.*

The use of multiple storage disks has the benefit of allowing material write to be distributed to all the drives, making a loss of any single material drive less likely to wipe out large parts of the stored material.

### 9.10.1.1 To add a hard disk:

1. Install the new disk.
2. In Storage Settings, click **Add Disk**.
   
3. The Add Disk dialogue box is shown. The Minimum free space on the new disk box shows how much free space the new disk must-have.

4. Select the disk from the list and click **OK**.

#### 9.10.1.2 To map a network drive:

1. In **Storage Settings**, mark the **Network drive** checkbox.
2. If needed, click **Define network drive** to open the network drive configuration screen.

3. Type the network drive username and password into the **Username** and **Password** fields.
4. Type the location of the network drive into the **Network drive path** field.
5. Click **OK**.
6. Use the **Allocated space** slider to set the space reserved on the network drive for data storage.

#### 9.10.1.3 To map multiple network drives:

1. Install and configure the networks storage to work as a locally mapped drive (for example, use iSCSI initiator or similar).
2. In Storage Settings, click **Add Disk**.

The Add Disk dialogue box is shown.
3. Storage size cannot be configured for iSCSI disks.
4. Click ok to store settings. Repeat for other disks.

### 9.10.2 Video, audio and text data storage settings

#### 9.10.2.1 Minimum

To prioritize recordings from one or more video, audio or text data channels, ensure that the minimum values are sufficiently low for other channels.

Then set the value higher for the high priority channel or channels.

If you select **Automatic**, the system deletes recordings from channels that use the most storage space.

#### 9.10.2.2 Maximum

The system examines the recordings daily and deletes those that are older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

***Note**: If the minimum values are too high for some channels while, at the same time, they are not set for other channels, the system will delete recordings from the channels with no set minimum.*

### 9.10.2.3 Alarm limits

#### 9.10.2.3.1 Minimum

The system deletes alarms that are older than the minimum value.

If you select **Automatic**, the system deletes alarm recordings from channels that use the most storage space.

#### 9.10.2.3.2 Maximum

The system examines the alarm recordings daily and deletes them older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

##### 9.10.2.3.2.1 Log entries

This value specifies how many alarm events will be kept in the alarm log at the most.

The system examines the number of log entries hourly and deletes the oldest entries if they are exceeded.

##### 9.10.2.3.2.2 % maximum

This value specifies how much storage space alarm recordings are allowed to use of all storage space.

As long as all storage space is not used, alarm recordings can use more space than this value.

The system first deletes the oldest alarm recordings before deleting other video or audio recordings if all storage space is used.

## 9.10.3 Automatic Deletion of Video, Audio and Text Data

After exceeding the defined maximum storage time, stored video, audio, text, and alarm data is automatically deleted—the maximum storage time for data the system checks daily.

As the size of a stored data stream can vary significantly due to movement in the video image, changes in audio levels, or the number of text data events, it may be hard to predict storage space requirements accurately.

Thus, sometimes the system may deem it necessary to ensure free storage space by automatically deleting old material regardless of the maximum storage time.

If data needs to be deleted to ensure free storage space, the deletion process proceeds through the following pattern:

In simple words this retention process goes like this when FS need a new free file:

1. Check alarm quota, if alarm material files count in more then set in quota (% from all data) we cleanup oldest alarm file and reuse it
2. Check min settings for alarm data - if alarm channels have data that exceed min alarm settings – we take the oldest file from those, cleanup it and reuse
3. Check min settings for all material channels (video, audio, data) - if some channels have data that exceed min settings – we take the oldest file from those, cleanup it and reuse
4. Check the oldest file from channels with auto min settings if they are present, if so - we take the oldest file from those, cleanup it and reuse
5. If still, nothing is found – we just take the oldest file from all channels (material and alarm), clean up it and reuse

Also, we have a background task that cleans up material files according to max settings.

The launch period is set to a minimum max setting from all channels (material and alarm).

***Note:*** *To ensure that the need for automatic deletion due to a lack of disk space is minimized, it is good to monitor the disk usage regularly and alter the maximum storage time and allocated disk space.*

*It is advisable to use manual or automatic archiving tools to ensure that no relevant data is deleted in storage space issues.*

**Hint:** *You can set a Watchdog event to notify you if the storage space runs low.*

## 9.10.4 Archiving

You can set the system to automatically archive video, audio, and text data daily or weekly.

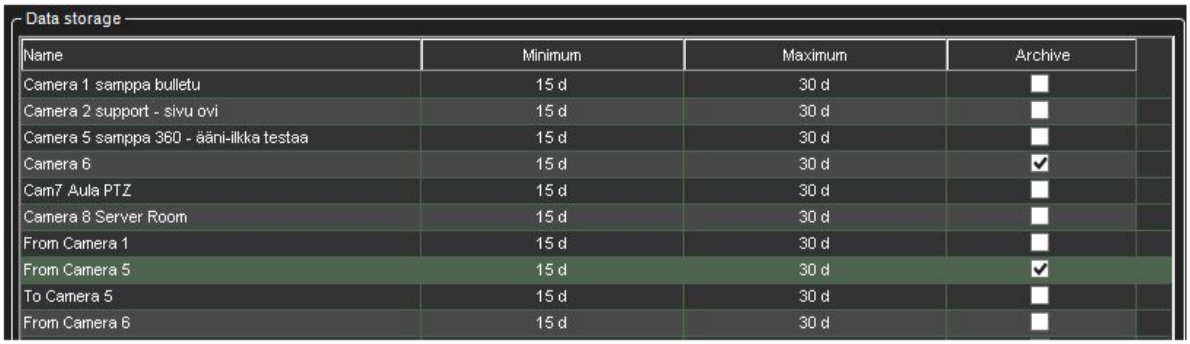
The archive files can be automatically created on the server's hard disks or a network drive.

The archive files can be opened on any Spotter client.

***Note:*** *Archive files can be huge, and thus they can fill storage space quickly. Archive files should be regularly copied and removed from the server hard disks or network drives on which they are automatically saved.*

### 9.10.4.1 To set an automatic archiving schedule:

1. In the **Data storage** pane, click on the devices you want to include in the automating archiving process.
   **TIP**: Select adjacent devices or folders, hold down the SHIFT key and then click the first and last device you want to select.
   a. To add a device to a selection or remove it from a selection, keep the CTRL key pressed and then click the device you want to add or remove.
      **Note**: *Selecting a device group (folder) also selects its contents.*
2. Mark the **Archive** checkbox.




3. Click **Modify archive settings**


4. Set the archive password by clicking **Change archive password**

5. Select whether to create the archive daily or weekly by selecting **Every day or Once a week**

6. If you set archiving to occur daily, use the **Archiving time** drop-down menu to select the time on which the archive files are created.

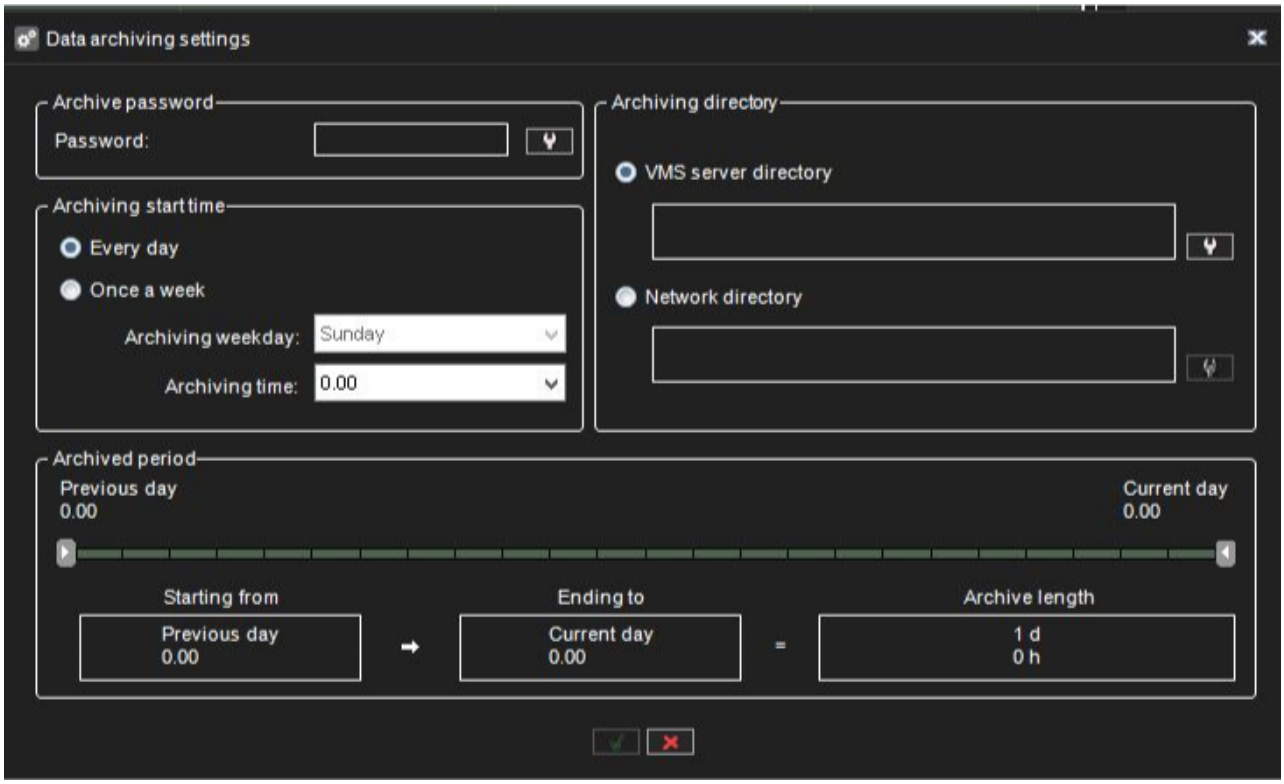
7. If you set archiving to happen every week, use the **Archiving weekday** and **Archiving time** drop-down menus to select the date and time on which the archive files are created.

8. Use the **Archived period** slider to set the period used in the archive files.

9. Select whether to create the archives on a local drive (on the server) or a network drive by selecting the **VMS Server directory** or **Network directory**.

10. Click the **Change directory** or **Change network drive** button to set the directory to save the archives.

11. Click **OK** to set the archiving schedule




## 9.10.5 Use OS cache

DVMS 8. x and newer have the possibility to enable OS cache usage when accessing the physical disk.

DVMS 9.4 and newer have the possibility to set maximum OS cache size.

Any software can access the disk in direct access mode when OS doesn't use any caching and using OS cache.

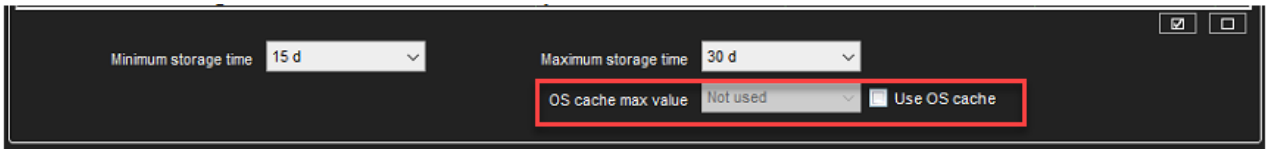
The last one helps to deal with unstable load to HDD and caching most used parts of data.

Windows Server and Windows desktop versions have different priorities for applications - Windows Service priorities background services and desktop version priorities UI applications.

Also, Windows Server uses more system resources to cache e.g. HDD access and can use up to 90% of RAM for this.

To avoid situations when all RAM is occupied by file system cache DVMS 9.4 and newer has an option to limit max OS cache size.

Max OS cache setting is valid until PC reboot, so they are set each time recorder starts.



# 9.11 Text Channels

## 9.11.1 Text Channel Settings

The servers can receive text data from devices such as cash registers or gas station pumps.

The driver specifies what text data is recorded and what is shown to the users. It also specifies custom events and searches criteria.

In addition to the default text data drivers included in the software, new drivers can be installed.

In-text channel settings, you can change the name of a text channel and add or edit its description.

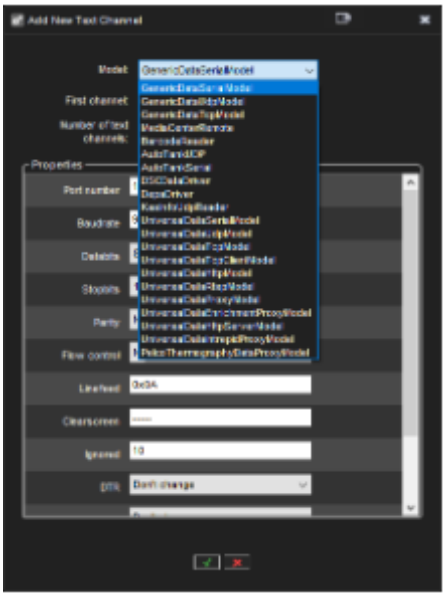
In profile **settings**, you can set the user rights and the device window options for each channel and each profile.

An additional document for UniversalData drivers can be downloaded from our extranet or contact support. This driver opens endless possibilities for integration to 3rd party systems.

### 9.11.1.1 To add text data channels:

1. Click **Add channels** in the lower right corner of the **Text channel settings** screen.

2. Select the text data channel driver from the **Model** drop-down menu.




3. Use the **No. of data channels** slider control to select the number of channels you want to create.
4. Fill the driver-specific information into the fields in the **Properties** list.
5. Click **OK** to save the channels.

## 9.11.1.2 To edit text channels:

### 9.11.1.2.1 To edit the name and description of a text data channel:

1. Select a text data channel from the channel list.
2. Type a name for the channel into the Name field.
3. Type general and administrative descriptions of the channel into the respective fields.
    a. All users can see the general description, whereas only system administrators can see the administrative description.
4. Mark the **In use** checkbox to set the channel as active, or unmark the checkbox to set the channel as inactive.

### 9.11.1.2.2 To edit the configuration setting of a text data channel:

1. Select a text data channel from the channel list.
2. Click **Modify channels**.

3. Edit the driver-specific information to the fields in the **Properties** list.
4. Click **OK** to save the changes.

***Note:*** *When editing the configuration settings of a text data channel, the settings are changed for all text data channels that use the exact driver.*

## 9.11.1.3 To remove all text channels that use the same driver:

1. Select a text data channel from the channel list.
2. Click **Delete channels** in the lower right corner of the **Text channel settings** screen.

3. All text data channels that use the same driver as the selected text data channel are removed.

***Note:*** *To remove text data channels without deleting all channels that use the specific driver, click* ***Modify channels*** *and specify the new number of text data channels using the* ***No. of channels slider****.*

# 10 Profiles

Profiles define which VMS components the user has access to and what kind of user rights the user has for the components.

The system has one default profile, Service.

The default profile contains the devices that the license key of the Master Server specifies.

The devices are grouped by device type. For example, all cameras are in one group and all audio channels are in a different group.

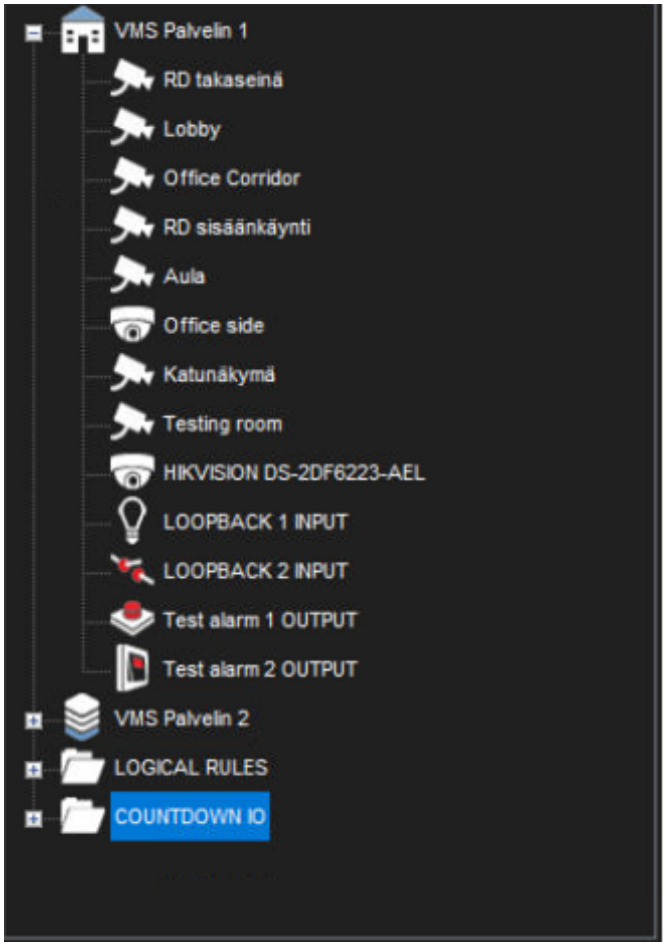
You can use the default profile as such or edit it freely, for example, group cameras at the exact location.

Or you can add new profiles. A profile can contain devices from different servers.

A *profile* sets a user's rights in the system. Each user can have 1 to 5 profiles that contain these *devices*:

- Cameras (fixed cameras and PTZ cameras)
- Audio channels
- Audio communication channel
- Digital inputs (alarm inputs)
- Digital outputs (control outputs)
- Video outputs
- Text channels
- Alarms
- Plugin instances
- Web browser home pages

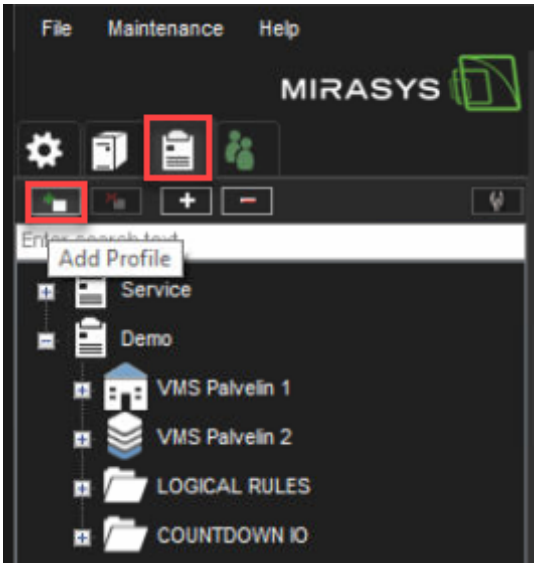
You can add as many as 2,000 groups and devices to a profile. Furthermore, you can put the devices into groups as you like.



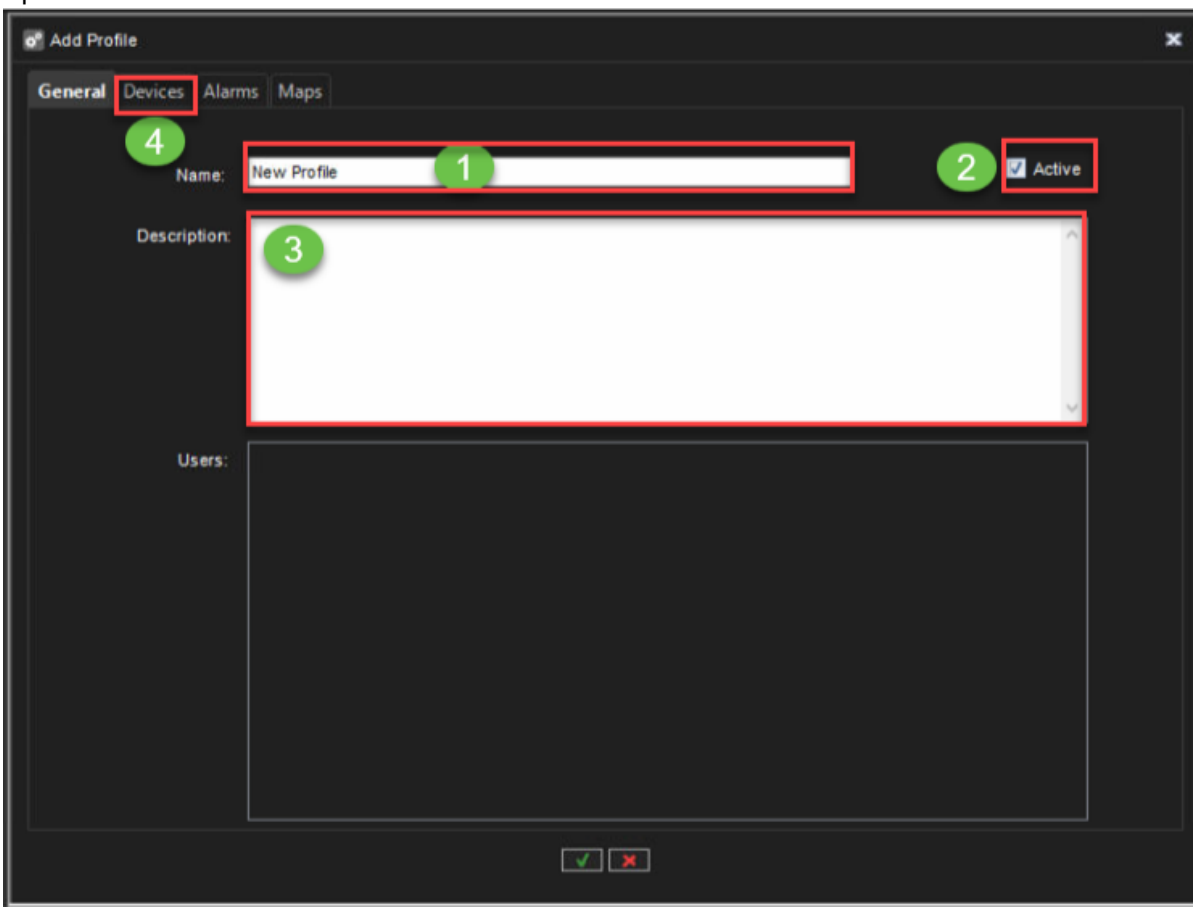

## 10.1 Creating a customer-specific profile

To add a profile:

1. Click **Add Profile**

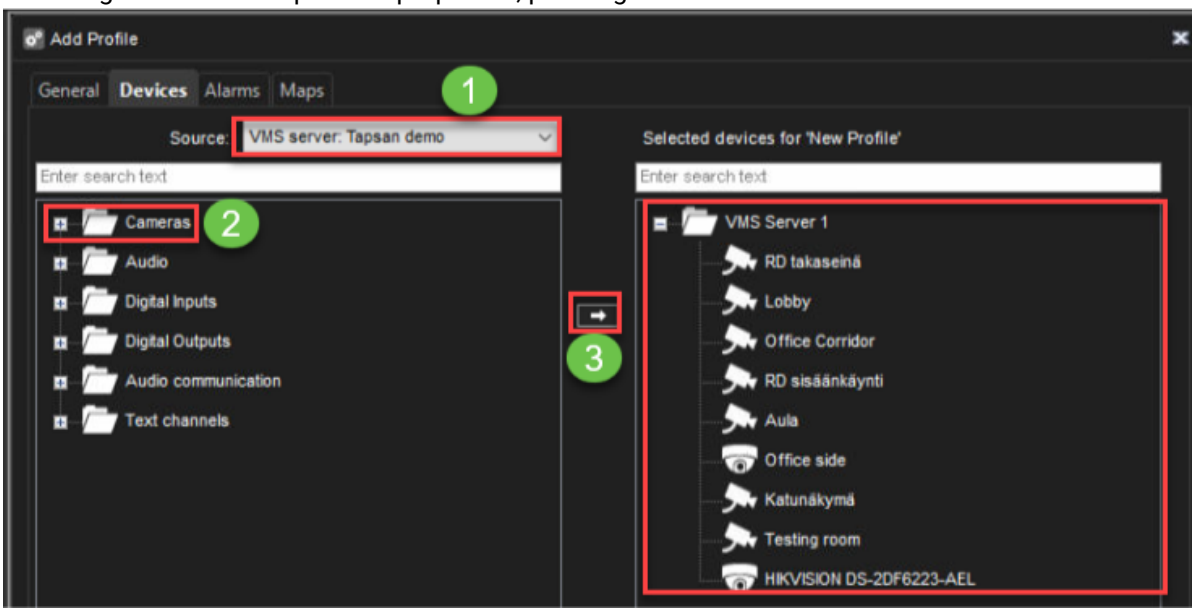



2. Set the name of the profile
3. Set profile status: **Active** or **Disabled**
4. Set description, if needed. The description is shown only in System Manager
5. Open **Devices**



### 10.1.1 Devices

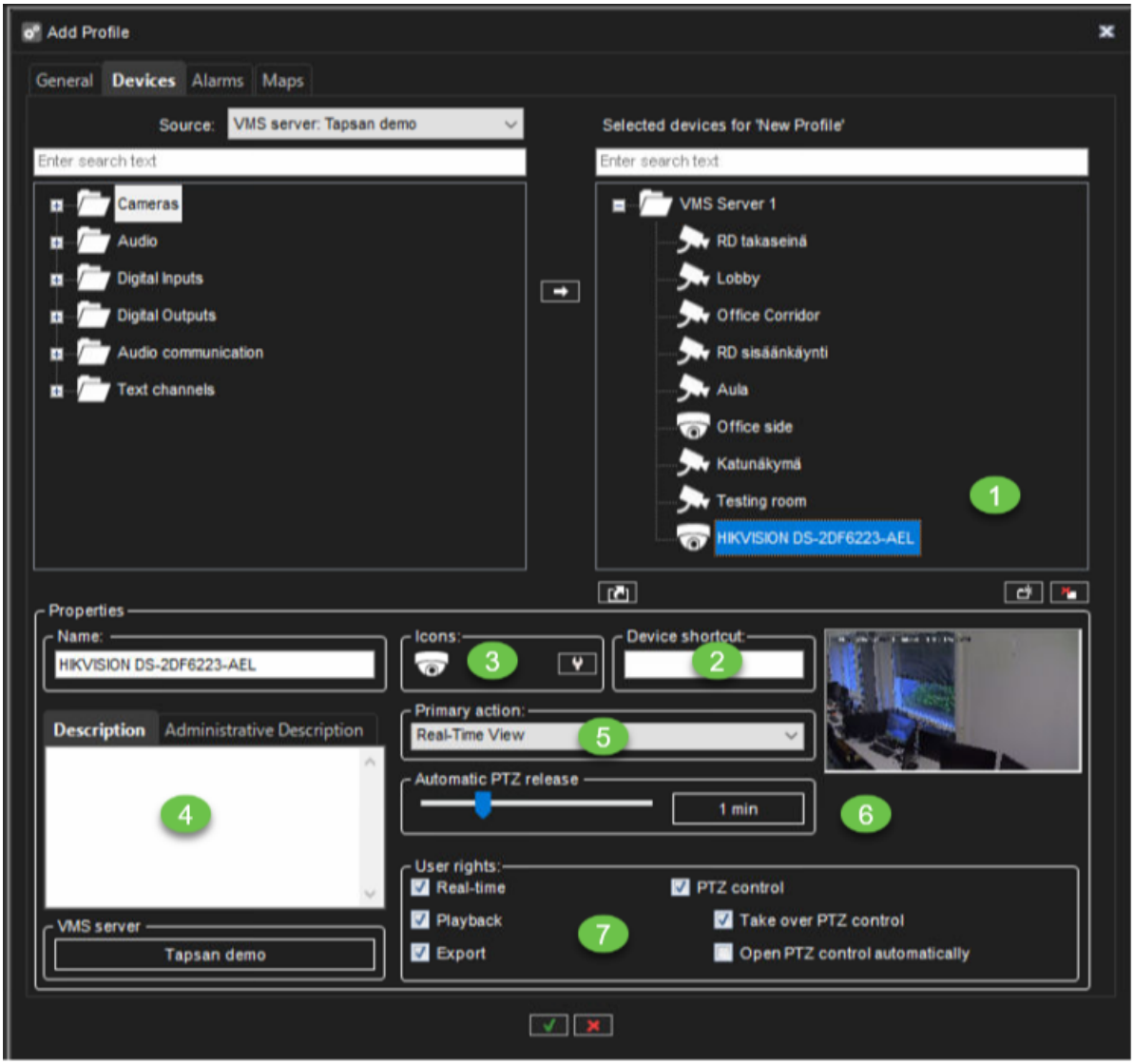
1. From the Source drop-down list select **VMS server or another profile**
2. Select needed components or device groups from the left box
3. Click **Add**
4. To change selected components properties, please go to **Selected Devices**




### 10.1.2 Selected Device Properties

1. Select component from the list of the selected device
2. Set **Device shortcut**
3. Change the device icon by clicking **Change Icon**
4. Set **Description** and **Administrative Description**, if needed
5. Select the **Primary action**, select the action that will occur when a user double-clicks the device in Spotter.
6. Set **Automatic PTZ release**(only for the PTZ cameras)
7. Set user rights for the component
    a. **Real-time**
    b. **Playback**
    c. **Export**
    d. **PTZ Control**(only for the PTZ cameras)
        i. **Take over PTZ control**
        ii. **Open PTZ control automatically**

8. Click **OK** to finalize the profile creation



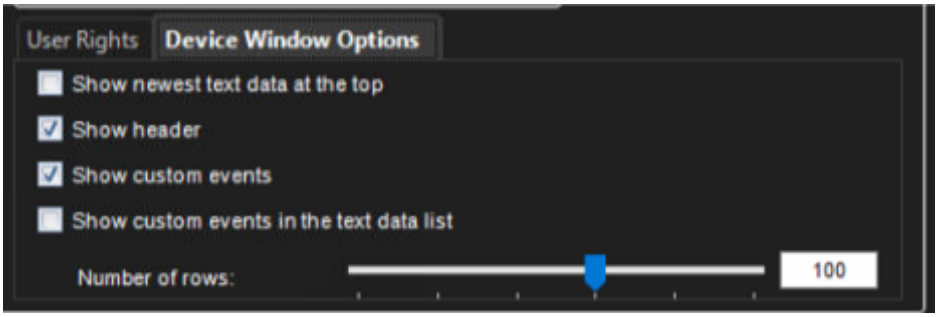

## 10.1.3 PTZ control

- Automatic dome release
  - Values: 10s, 20s, 30s, 40s, 50s 1 min, 2 min, 3 min, 4 min, 5 min, 10 min, 20 min, 30 min
- Take over PTZ control
  - No warning popup
- Open PTZ control automatically

## 10.1.4 Sort selected device nodes

Alphanumeric sorting ( a -> z) of selected folder profile nodes is executed when pressing sort button, second press will execute reverse sorting (z -> a,).

## 10.1.5 Text channel Device Window Options




In Device Window Options, you can select how text data is shown to users. These options are available:

### 10.1.5.1 Show the newest text data at the top.

By default, the newest text data is added to the bottom of the text data list. Select this option to show the newest text data at the top of the text data list instead.

### 10.1.5.2 Show header

Select to show identification data specified by the text data capture driver.

### 10.1.5.3 Show custom events

Select to show custom events specified by the text data capture driver.

### 10.1.5.4 Show custom events in the text data list

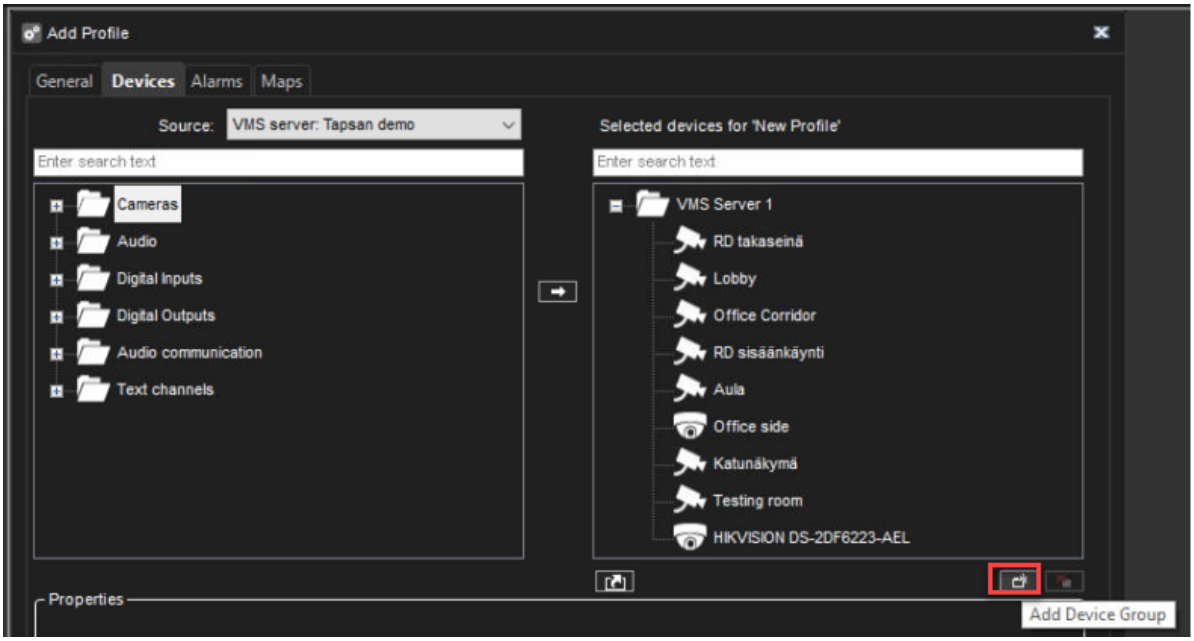
Select to show custom events in the text data list (instead of the custom event list).

### 10.1.5.5 The number of rows

Specify the number of rows that are shown in the text data list at the most.

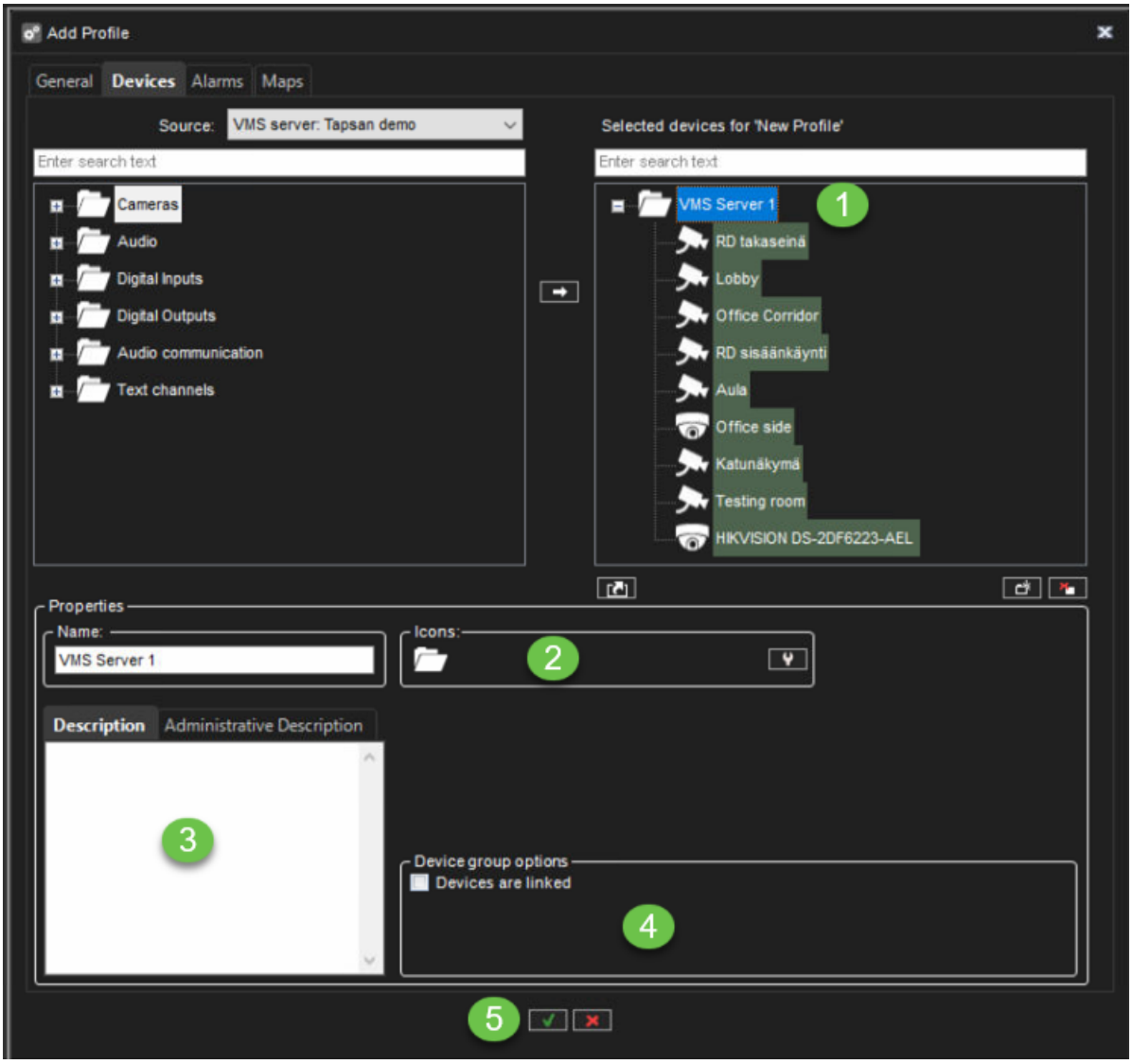
## 10.1.6 Adding Device Groups to the list of the selected device

1. Click **Add Device Group** below the **Selected devices** panel. A new device group is shown.




Note: *A new device group is always added under the selected device group. To add a device group to the top level, make sure that none of the existing device groups is selected.*

1. Click the device group and type a name for it
2. To change the icon that is used for the device group, click **Change Icon**. Then select the icon that you want to use.
3. Type a description of the device group in **Description**.
4. Set Device group options, if needed(**Devices are linked** to automatically open all device views from the same group when the user opens one of the device views).



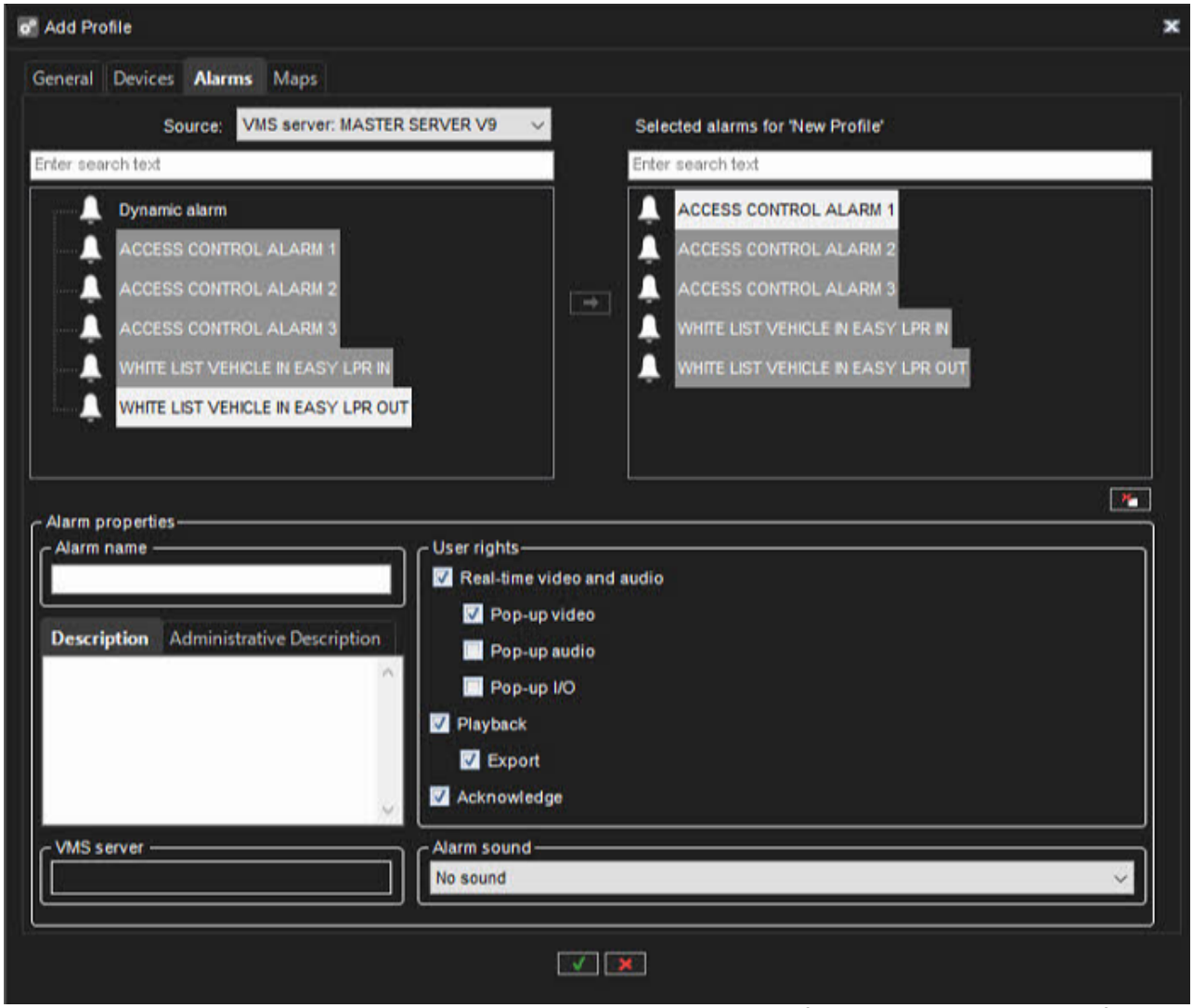

## 10.1.7 Sort Alphabetically

Sorting rules:

- to the folder or root level where the currently selected component is located (but not to subfolders)
- to the selected folders (but nor to subfolders)
- if no profile node is selected, root nodes are sorted (but nor subfolders)
- if multiple folders are selected from same level, all selected folders are sorted (but not subfolders)

## 10.1.8 Alarms

### 10.1.8.1 Editing Profile Specific Alarm Settings




On the **Alarms** tab, you can select the alarms you want to include in a profile and edit the alarms' profile-specific user rights.

### 10.1.8.2 To add alarms to a profile:

1. Open the **Alarms** tab.
2. Select a server from the **Source** drop-down menu. The available alarms are shown in the left pane.
3. Select the alarm or alarms that you want to add and then click the right arrow. You can also drag alarms from the left pane to the right.

4. Save the profile by clicking **OK**.

***Note:*** *You can also add alarms to profiles through the alarm creation/editing screen.*

#### 10.1.8.3 To edit profile-specific alarm user rights:

1. Open the **Alarms** tab.
2. Click on an alarm in the **Selected alarms** pane.
3. Set the user rights for each alarm. The user rights settings are located on the bottom right side of the **Alarms** tab.
    a. You can set individual rights for each alarm or select multiple alarms (by holding the shift or control keys down while selecting alarms) and set the same options for multiple alarms.
4. To have the computer play a sound when an alarm occurs, select **Alarm sound** and then select the played sound. To test the sounds, select the sound from the list and click **Play**.
5. Save the settings by clicking **OK**.

##### 10.1.8.3.1 The user rights include:

- **Real-time video and audio**. Select to let the users see real-time alarm video or audio.
- **Pop-up video**. Select to let users receive alarm video automatically.
- **Pop-up audio**. Select to let users receive alarm audio automatically.
- **Playback**. Select to let the user's playback alarm video.
- **Export**. Select to let the users save alarm video on local media.
- **Acknowledge**. Select to let the users acknowledge alarms.

## 10.1.9 Maps

### 10.1.9.1 Adding Maps to Profiles

#### 10.1.9.1.1 To add a map:

1. Click the **Change Level** button and then select the device group to which you want to attach a map. The devices that belong to the selected group are shown in the left pane.
    a. Subgroups are also shown. You can also double-click the subgroup icons in the left pane to move to a lower level.
2. Click **Add Map** and find the image that you want to use as a map.
3. Select the devices and device groups you want to add to the map from the left pane and click the **Add to Map** arrow.
    a. Items that are already on the map appear dimmed in the left pane. If you add subgroup icons to the map, the icons will act as links to the subgroup maps.

b. Users can move to a lower level map by double-clicking the subgroup icon.

**Tip:** To select more than one device simultaneously, keep the SHIFT or CTRL key pressed.

1. Select a device or device group from the map, and then, under **Device properties,** you can set these options:
2. For cameras, you can select the direction that the camera icon points to.
3. By default, the name label of each device is shown on the map. To avoid label clutter, clear the check box **Label**. The name will be shown as a popup label instead.
4. If you need to fit several device icons in a small space, you can use placemarks.
5. Select the **Placemark** check box. A placemark (x) and a connecting line are shown on the map. Drag the placemark (x) to the device's correct position.
6. Then drag the icon to a convenient position on the map.

#### 10.1.9.1.2 To remove a site map:

- Display the map that you want to remove and click **Remove Map**

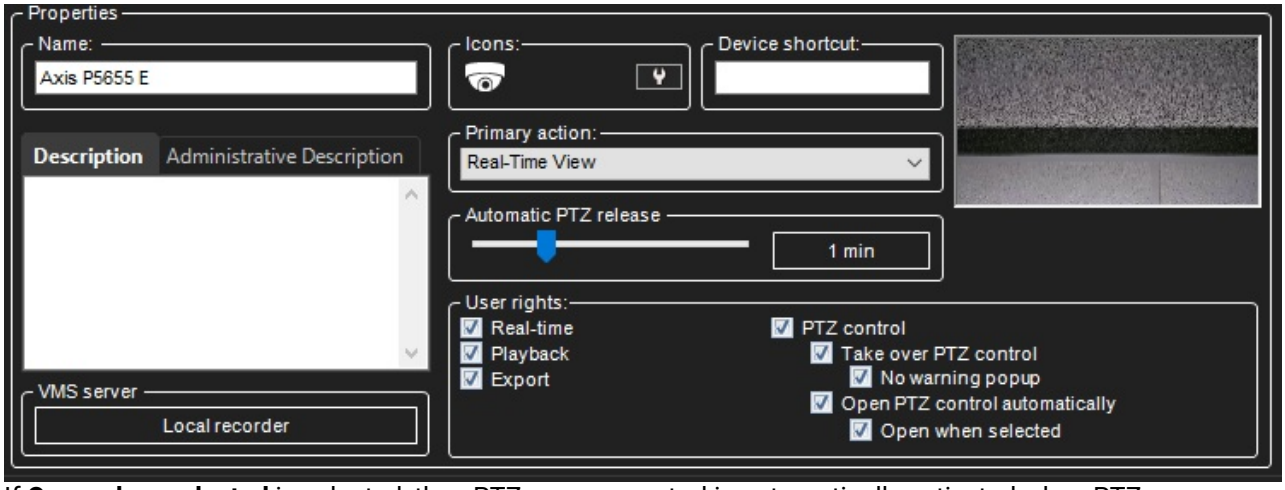
#### 10.1.9.1.3 To remove an icon from the map:

- Select the icon and click **Remove**

Supported map image files are
- .jpeg
- .jpg
- .png
- .bmp

## 10.2 PTZ camera profile settings

In System Manager camera profile settings in PTZ camera user rights, selection **Open when selected** is added.




If **Open when selected** is selected, then PTZ camera control is automatically activated when PTZ camera view is selected in Spotter.

# 11 Users and User groups

All users belong to a user group (see below), through which their use rights are defined and managed.

The administrator can add new user groups, set varying use rights for the groups, and add users.

The system supports domain-level user rights integration (LDAP), enabling users to be synchronized from domain groups.

Each user group must have at least one profile that sets the user group's devices in the system.

One user group can have five profiles at the most.

A username and a password protect all user accounts.

## 11.1 Logging Users Off

If you have administrative rights, you can log a user off from the Spotter program.

## 11.2 To log a user off:

Right-click the username on the Users tab and click **Log User Off.**

> NOTE:
> Please change always the Admin user password after you have finalized the installation.
> You should never leave default passwords in the Mirasys VMS system.

## 11.3 Monitoring Users

The **Users** tab shows if users are logged on to the system:

| Icon | Description |
|---|---|
|  | (Green). The user is logged on. Click the plus sign (+) to see the name of the program the user is logged on to and the IP address of the user's computer. In addition, the date and time of logon are shown. |

| | |
|---|---|
|  | (Red). The user is not logged on. |
|  | (Grey) The user account is disabled. |

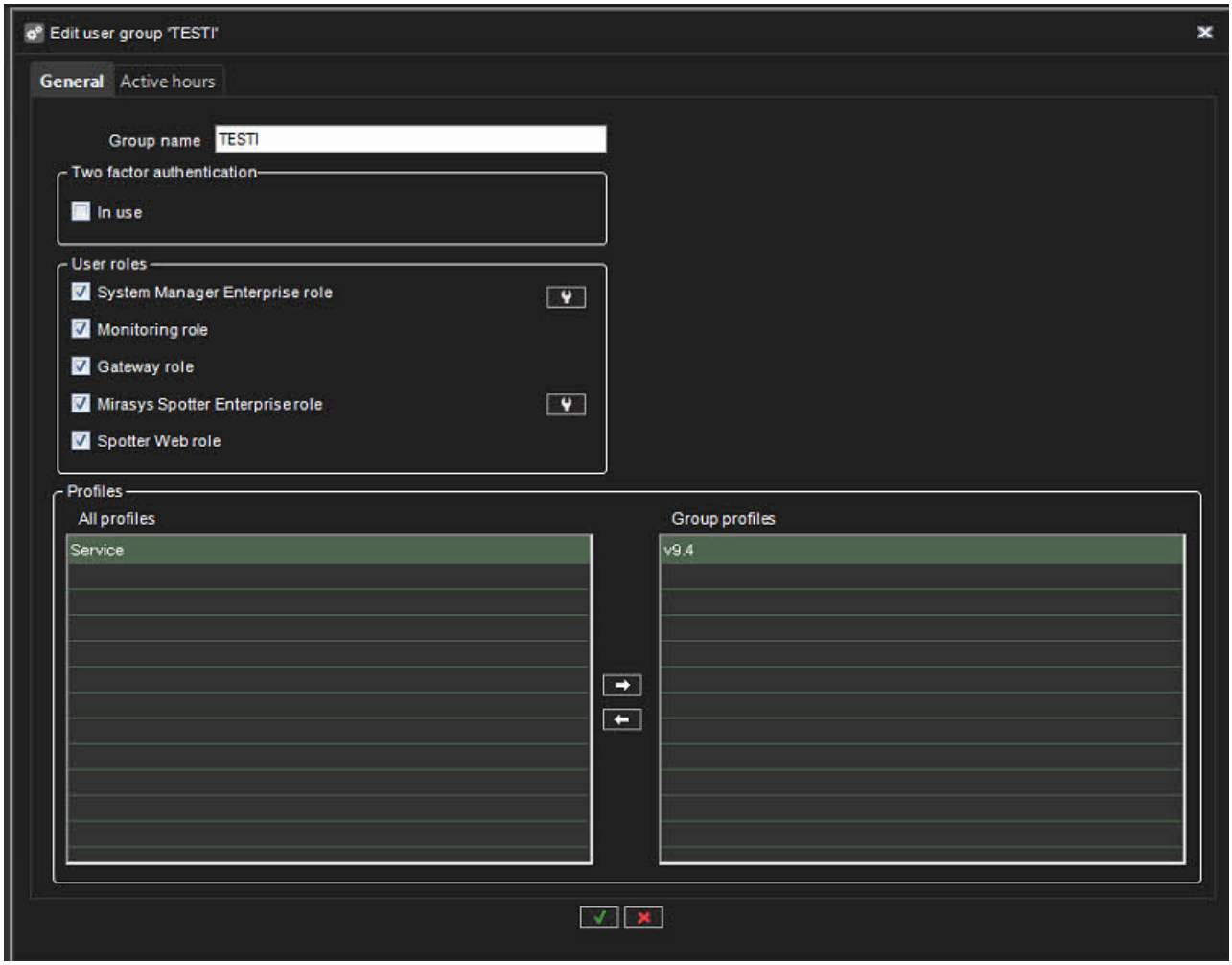
## 11.4 User group

The user group defines which Mirasys VMS applications the user group has access to and what kind of permissions the user group has regarding the applications.

### 11.4.1 User Roles

The system supports the following types of user roles (defined through user groups)

- **System Manager role:** Administrators are allowed to log in to System Manager and change all settings, such as changing camera settings or adding new profiles or user accounts.
- **Monitoring role:** Users with monitoring rights are allowed to log in to System Manager and monitor the system on the **System** tab, but they are not allowed to change the settings.
- **Gateway role:** if this role is active, the user group can access the DVMS gateway
- **Mirasys Spotter Enterprise role:** End users can log in to Spotter but not to System Manager.
- **Spotter Web role:** End users can log in to the Spotter Web




## 11.4.1.1 User group level automatic lock / log off

### 11.4.1.1.1 Possibility to force other user log off when starting System Manager

- Enabled only if System Manager Enterprise Plus role is enabled
- Possible values for Wait time: 0s, 10s, 20s, 30s, 45s, 1 min
- When creating new group, default value is 10 seconds

### 11.4.1.1.2 Functionality at log on

There is changes from previous versions only if other user log off is enabled and there is other user logged in System Manager with administrator rights.

When trying to log on, following choices will appear:

- Kick off current user: start sequence to kick off current user with administrator rights in System Manager

- Login with limited system monitoring rights: continue login with monitoring rights, no effect to current System Manager users
- Cancel login: go back to start login page (cancel button has this same effect)

**Kick off current user**

Current user is selected, new processing window is opened:

This processing window is open until:

- Other user is logged off
- Other user has cancelled force log off
- Cancel button is pressed

#### 11.4.1.1.2.1 Other user is logged off

User is automatically logged in with administrator rights.

Other user has cancelled force log off

#### 11.4.1.1.2.2 Other user has cancelled force log off

After OK button, go back to login page, other user with administrator rights continue logged in.

#### 11.4.1.1.2.3 Cancel button is pressed

Go back to login page, other user with administrator rights continue logged in.

#### 11.4.1.1.2.4 Other (already logged with Administrator rights) side

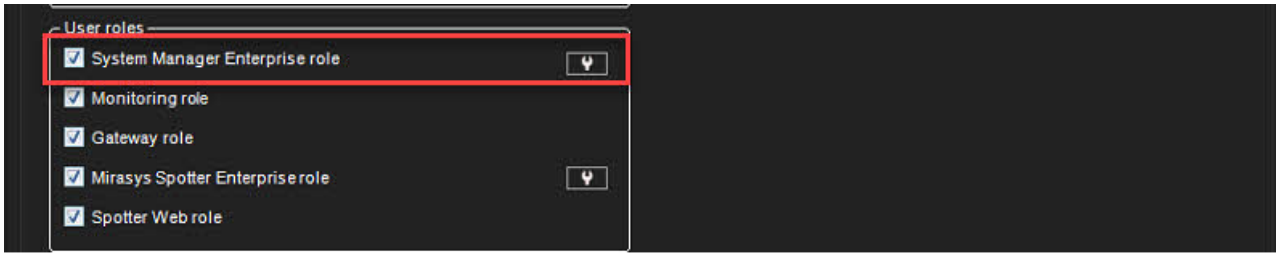
If there is timeout in forced log off settings, warning of coming forced log off appears:

Remaining seconds before forced log off is updated. During this timeout, user can cancel forced log off by cancel button.

If timeout is past or Ok button is pressed, current user session is logged off.

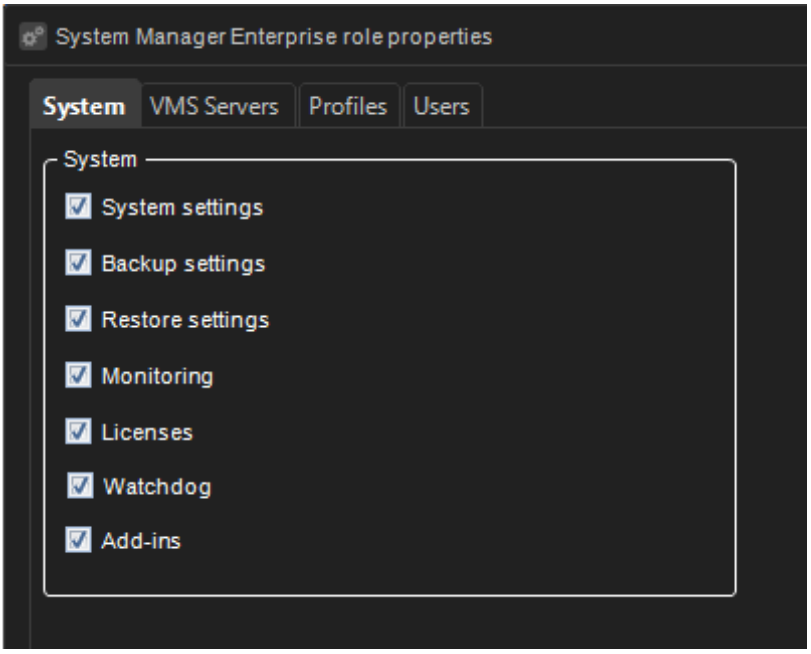
### 11.4.1.2 System Manager Enterprise role

It is possible to set explicit permissions for the system manager for different user groups.
This allows, for instance, implementing functionality for allowing different user groups for hardware maintenance and user administration, which is helpful for large scale systems.
To enable the functionality - check the "System manager enterprise role" tickbox for the user group and click the "wrench" icon to edit the details for this group.




#### 11.4.1.2.1 System

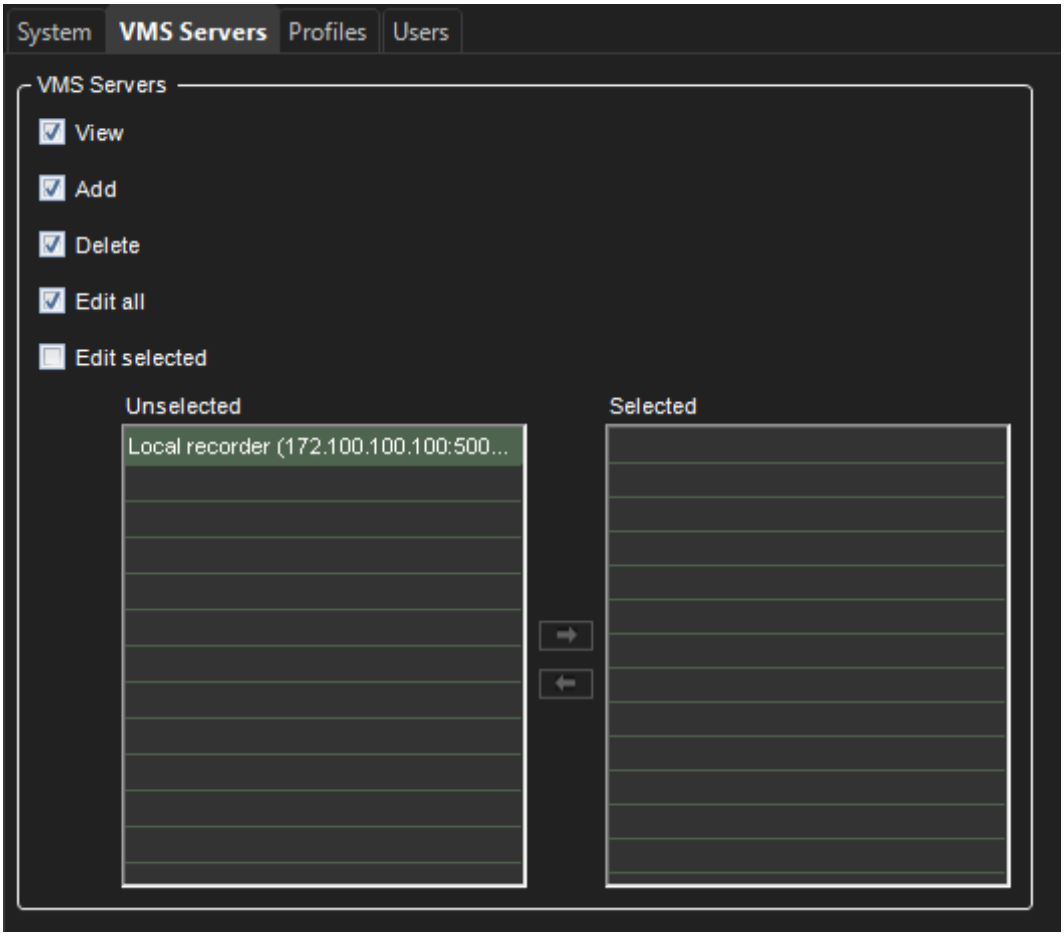
The System tab permissions can be enabled or disabled for a user group, disabling, for example, System settings hides system settings for all users in the user group




#### 11.4.1.2.2 VMS Servers

The VMS servers tab allows permissions for a user group to View, Add, Delete and edit either all or only selected VMS Servers to be noted: if "Edit selected" is checked, the shuttle box below enables defining which specific servers this user group has access to.

This is convenient in large installations if specific user groups are working with specific servers (e.g. if there are separate maintenance groups for different sites - and the recording servers are site-specific.)



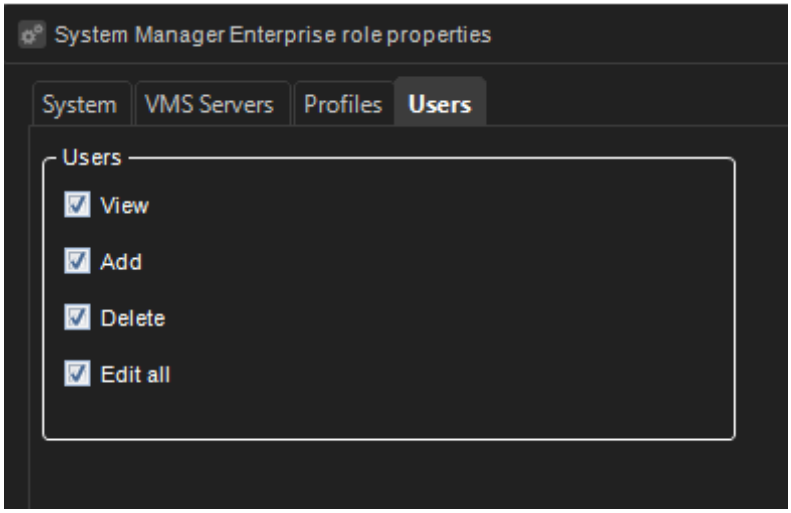

#### 11.4.1.2.3 Profiles

The Profiles tab/permissions that can be set for the user group:

“Edit selected” enables you to decide to which profiles the functionality applies (similar to the "servers" permission configuration).

#### 11.4.1.2.4 Users

The user tab/permissions that can be set for the user group:




Edit all or Edit selected must be enabled for a user group for users to add and/or delete (these options get automatically disabled if Edit all or Edit selected is disabled).

This functionality affects VMS Servers, Profiles and Users tabs

### 11.4.1.3 Monitoring role

The users with the role Monitoring role have permission to:

#### 11.4.1.3.1 System

- Export logs
- SM Server and VMS server diagnostic
- Licenses
- Watchdog log

#### 11.4.1.3.2 Profiles

Can view the content of the profiles

#### 11.4.1.3.3 Users

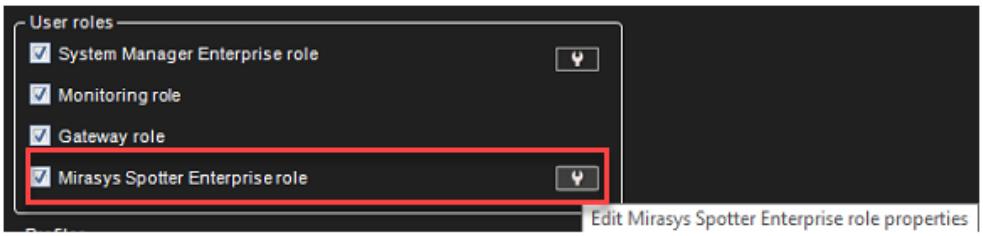
Can view the system user groups and users

### 11.4.1.4 Gateway role

Gateway role enables old Spotter Mobile usage

### 11.4.1.5 Mirasys Spotter Enterprise role

Custom user role properties can be edited by clicking the custom role properties edit button.

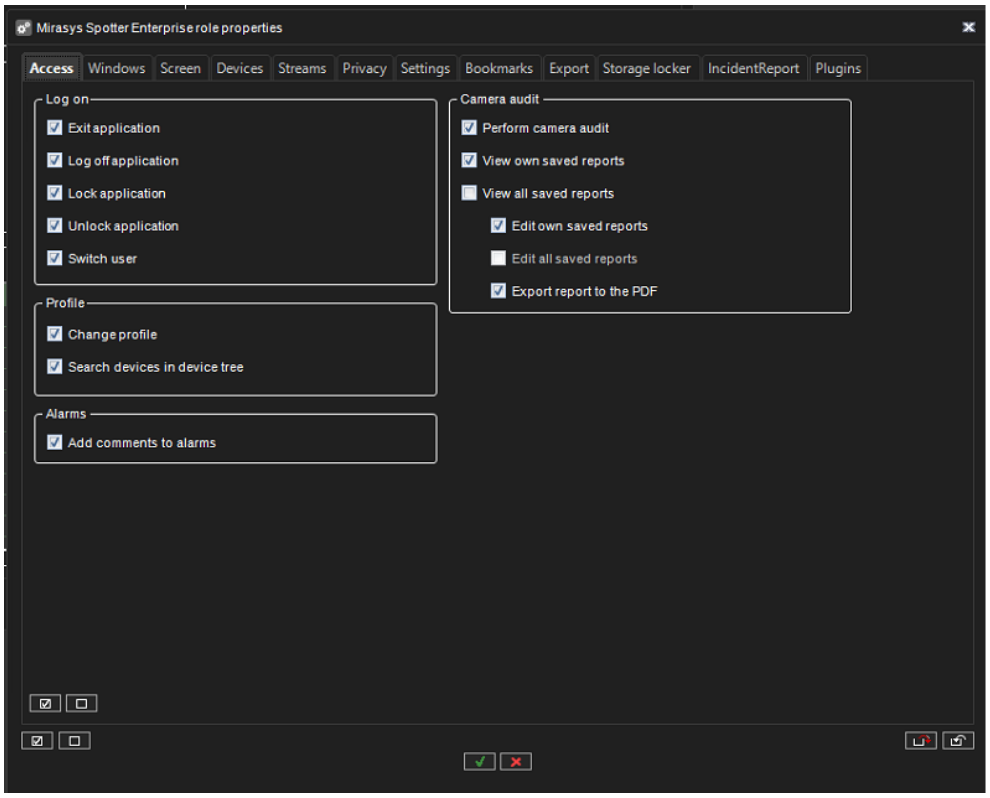



The **Spotter** custom roles can be customized with close to a hundred different options (not including plugin-specific adjustments).

---

### 11.4.1.5.1 Access

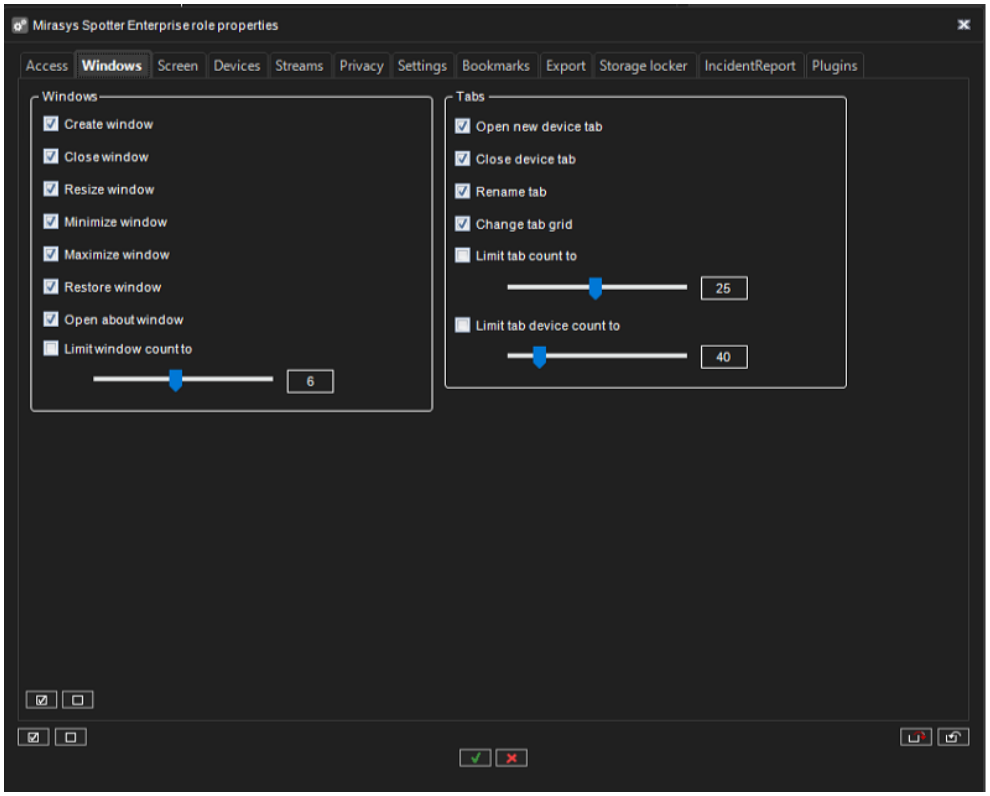
The Access tab of the role customization contains options for the application access and accessing profiles and alarm commenting.




---

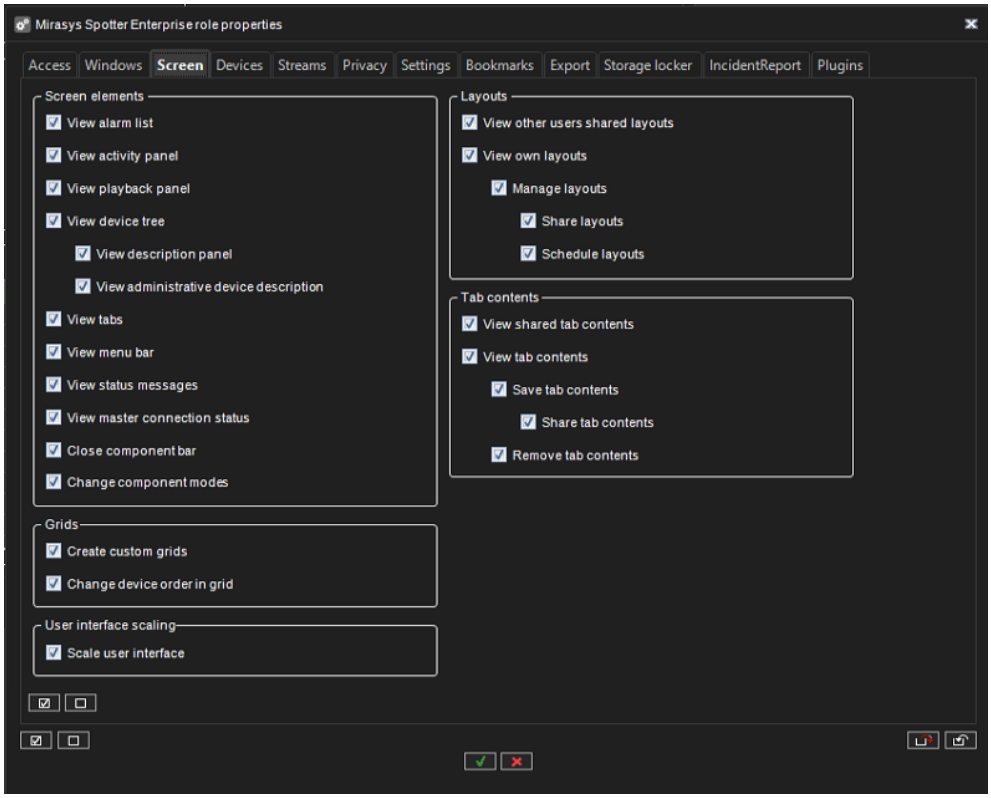
### 11.4.1.5.2 Windows

The Windows tab contains options for Spotter window management and tab management.



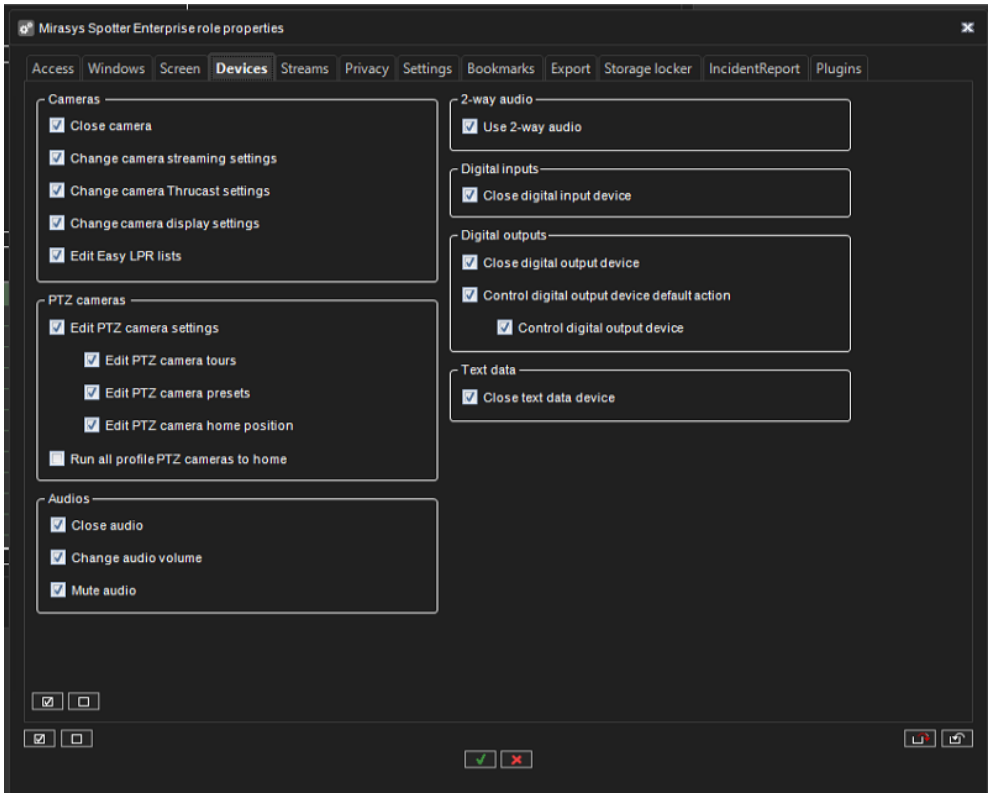

### 11.4.1.5.3 Screen

The Screen tab contains options for different screen element access and layout access, bookmarks, camera grid and saved camera tabs.




### 11.4.1.5.4 Devices

The Devices tab contains options for media control.



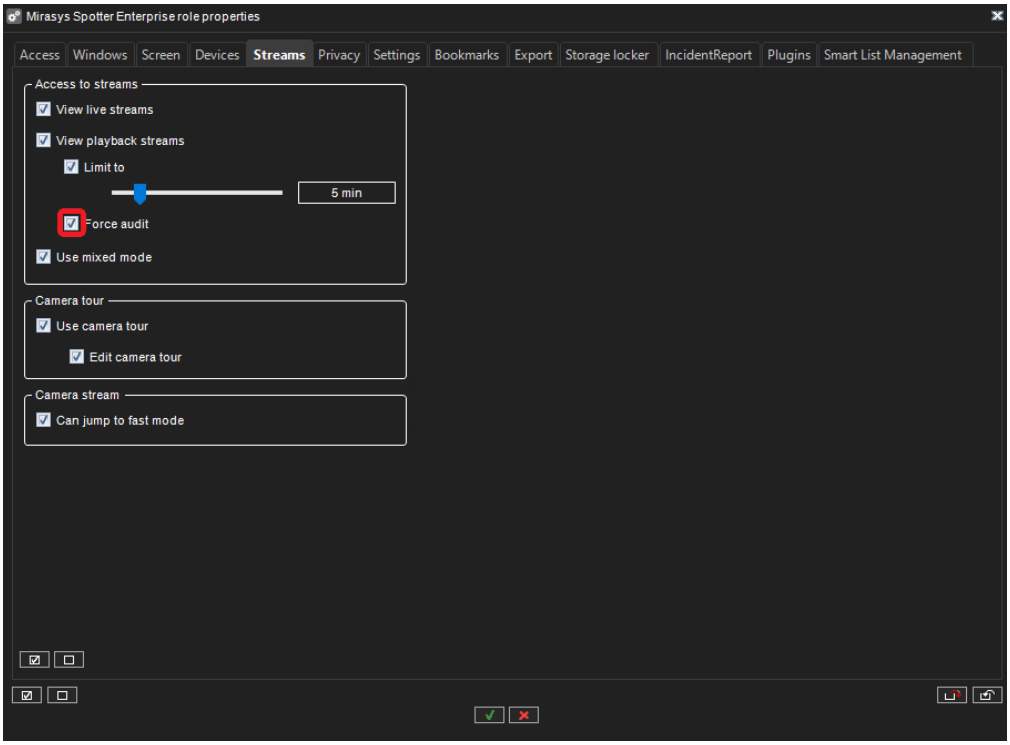

### 11.4.1.5.5 Streams

The Streams tab contains options for stream access and exporting.

In the Video Wall, the operator can force a user to add a comment before using playback.

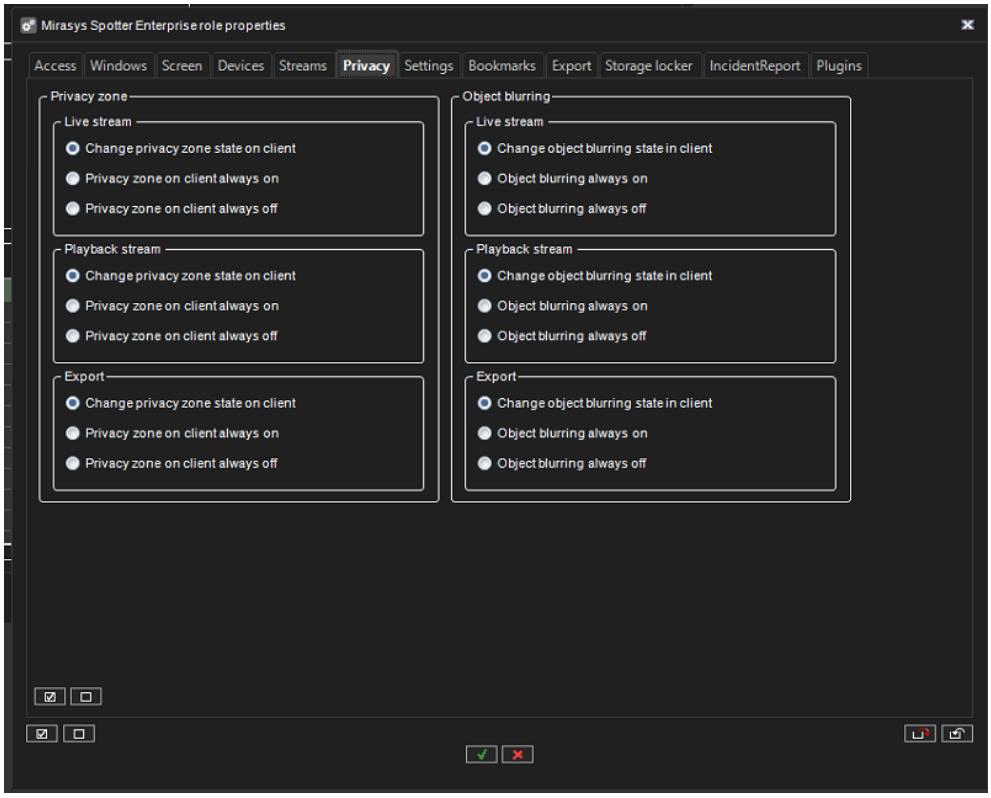
This functionality can be used when the operator requires a reason for using the playback mode before a user can move into playback mode.

The playback comment will be added to the audit log.



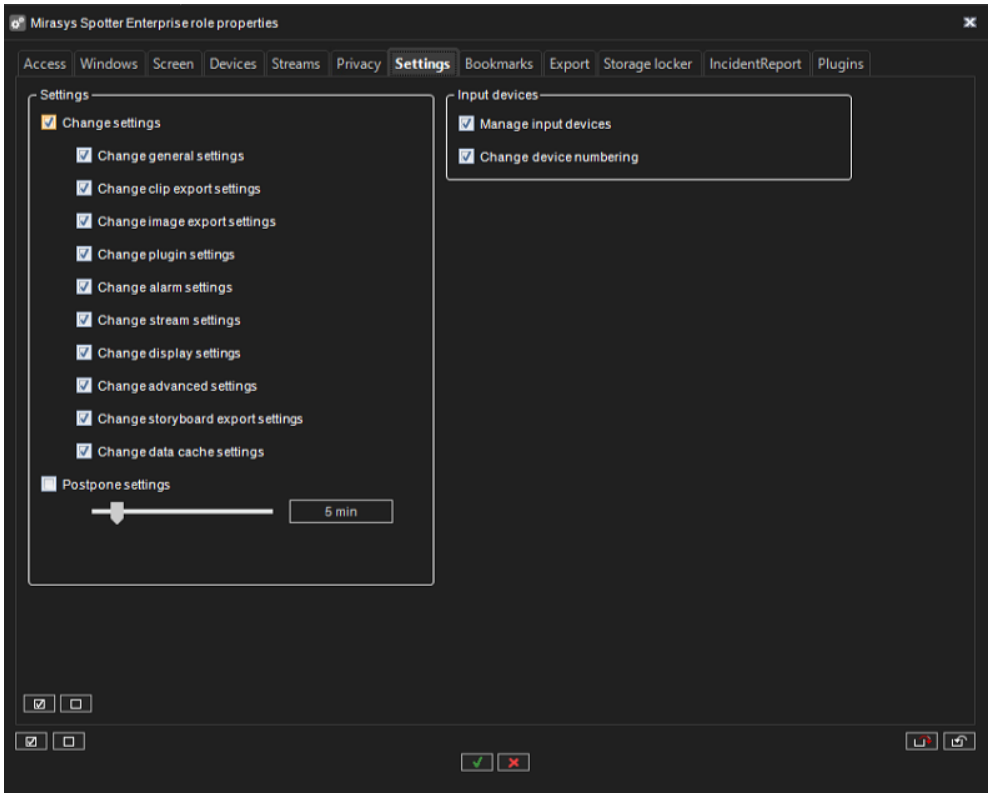

### 11.4.1.5.6 Privacy

The Privacy tab contains options for privacy.



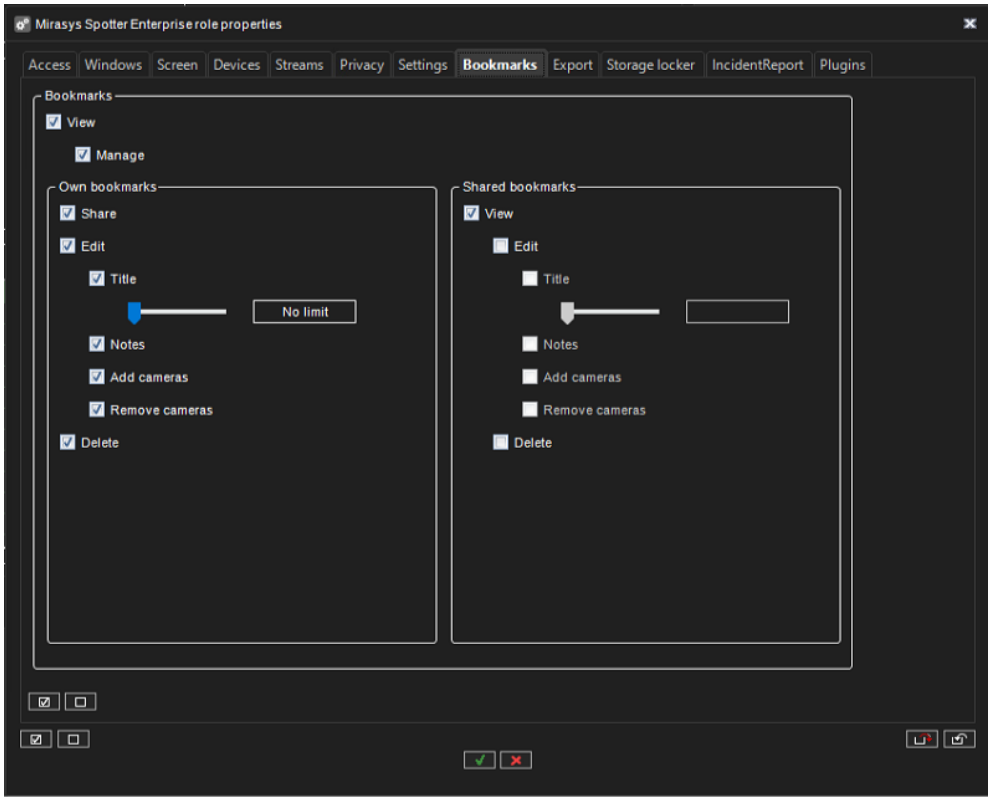

### 11.4.1.5.7 Settings

The Settings tab contains options for Spotter settings.



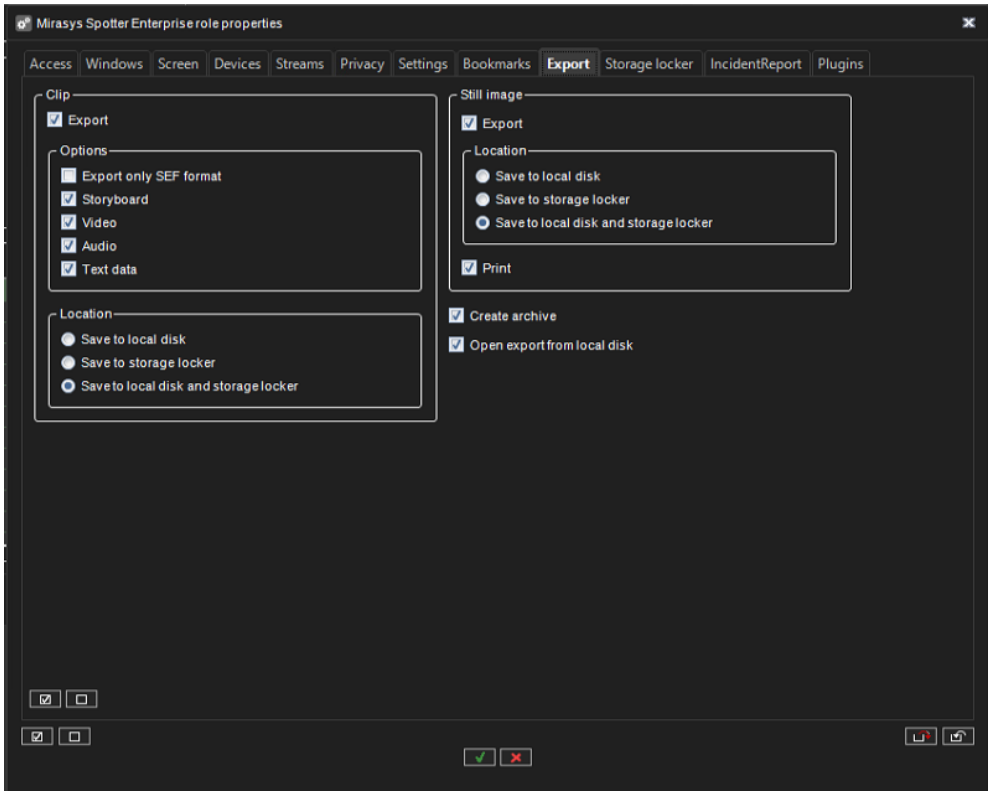

### 11.4.1.5.8 Bookmarks

The Bookmarks tab contains options for bookmarks.



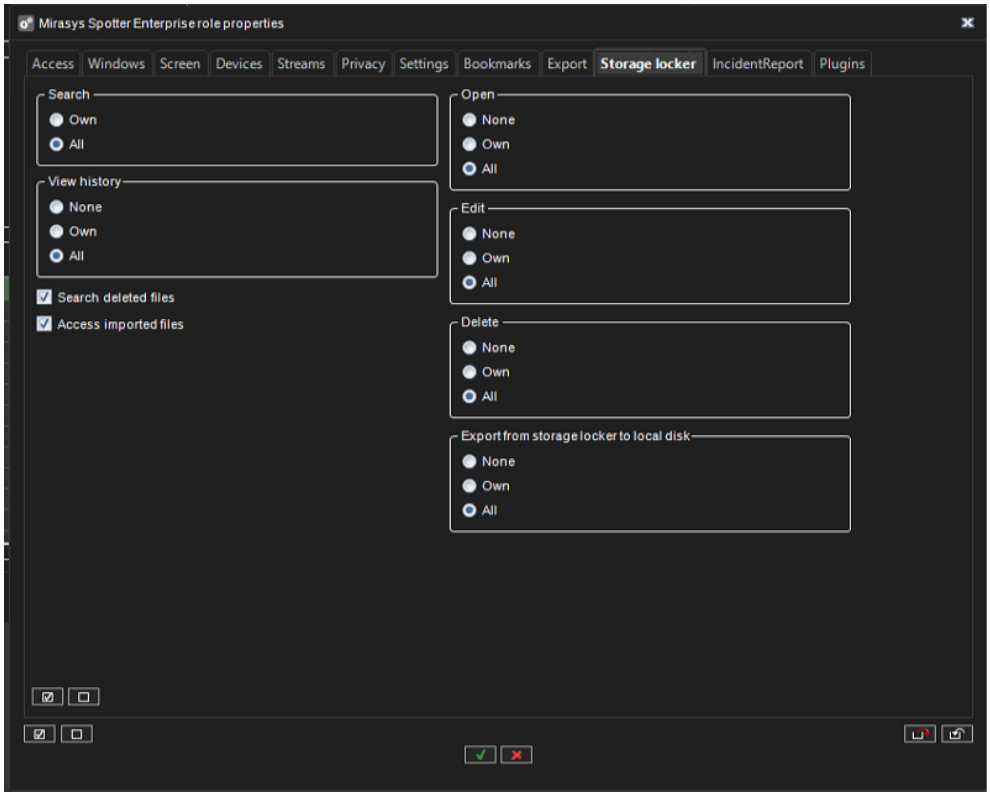

### 11.4.1.5.9 Export

The Export tab contains options for Export functions.



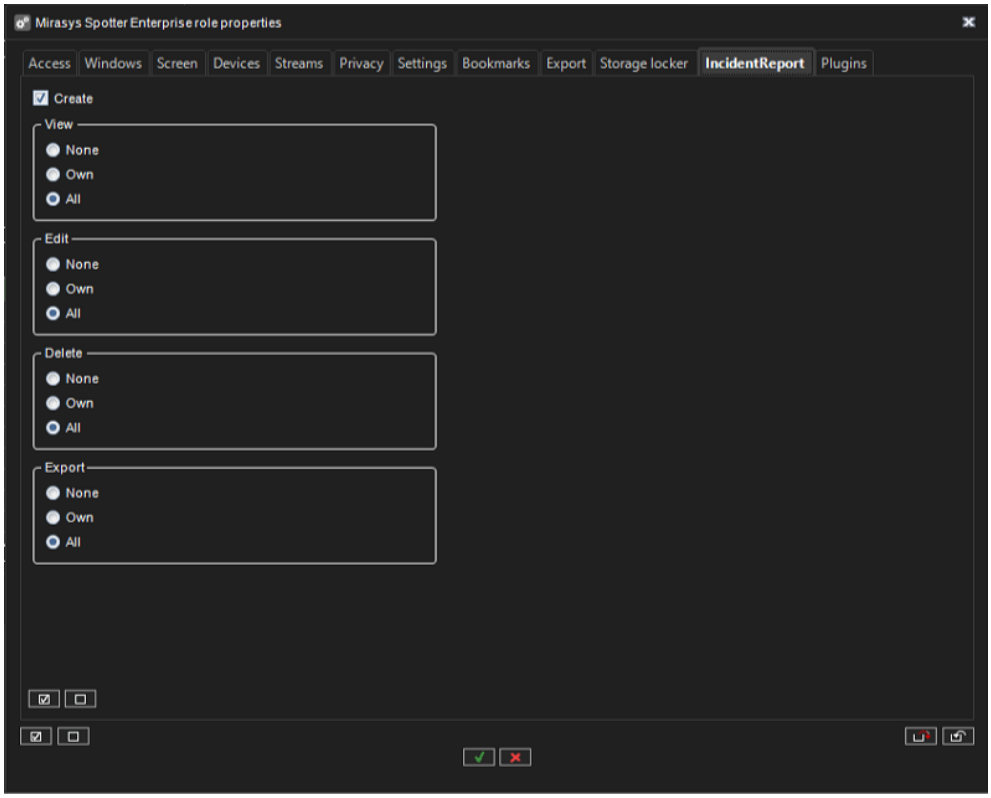

### 11.4.1.5.10 Storage Locker

The Storage Locker tab contains options for the Storage Locker plugin.



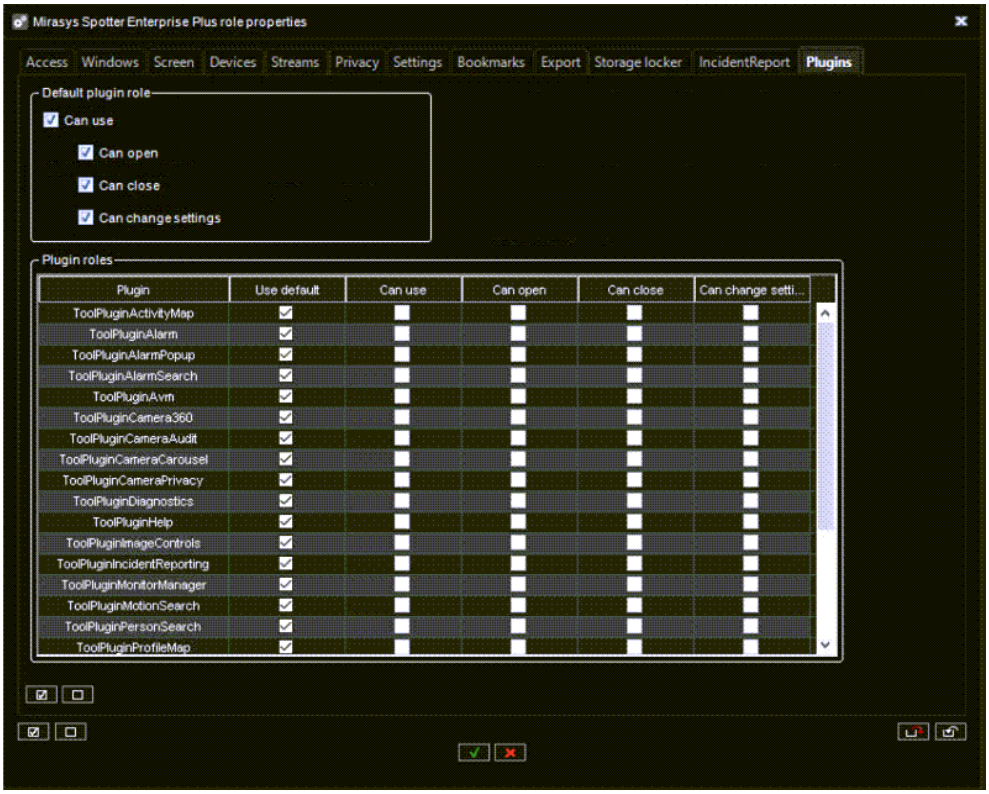

### 11.4.1.5.11 Incident Reporting

The Incident Reporting tab contains options for the Incident Reporting plugin.




### 11.4.1.5.12 Plugins

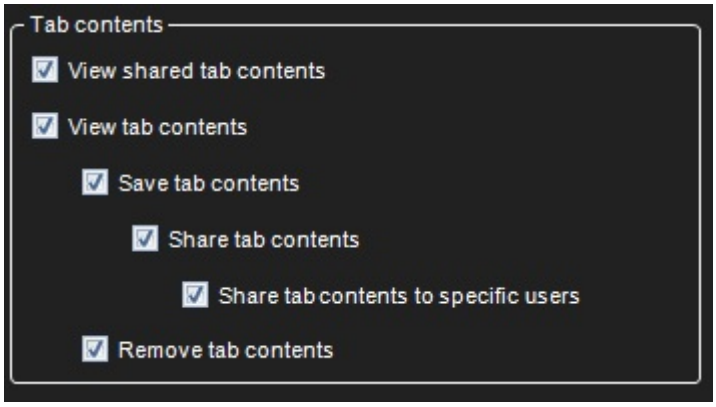
The Plugins tab contains options for Spotter plugins.




Each plugin behaviour can be either default or custom. The default behaviour can be controlled from the ”Default plugin role” controls.

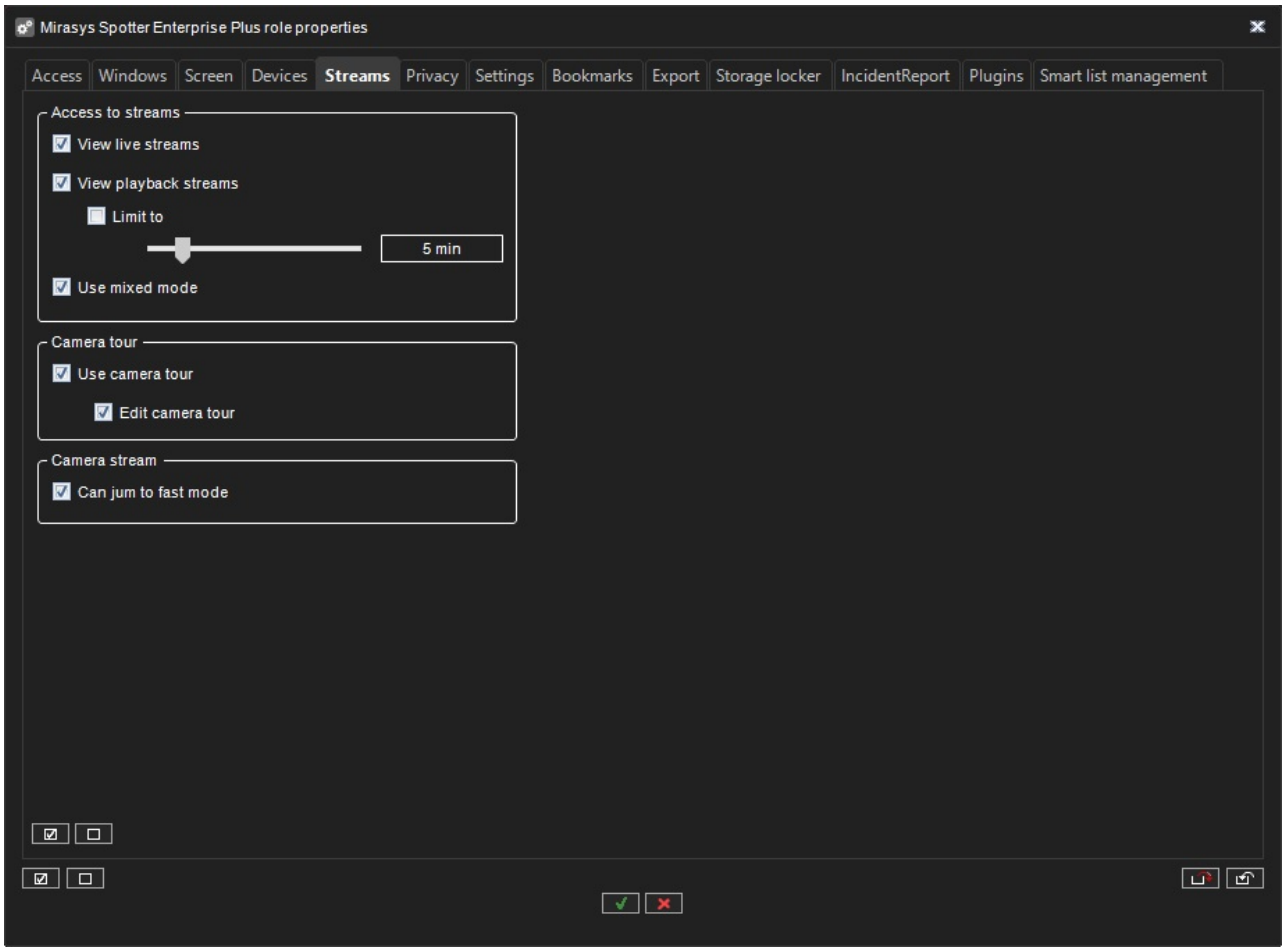
### 11.4.1.5.13 Share tab content with selected users

1. In the System Manager desktop application, under Mirasys Spotter Role properties, go to **Tab contents**.
2. Check the box **Share tab contents to specific users** to enable the feature.



### 11.4.1.6 Playback Speed Role

Spotter playback automatic speed adjustment can be enabled or disabled in the Spotter role settings “Streams” tab.




In the Camera streams group, there is a selection for fast playback mode. If selected, with 2x, 4x, and 8x playback speeds, if the playback cannot keep the pace because of too much load, it will jump to fast forward/backward. By default, automatic playback speed adjustment is not selected.

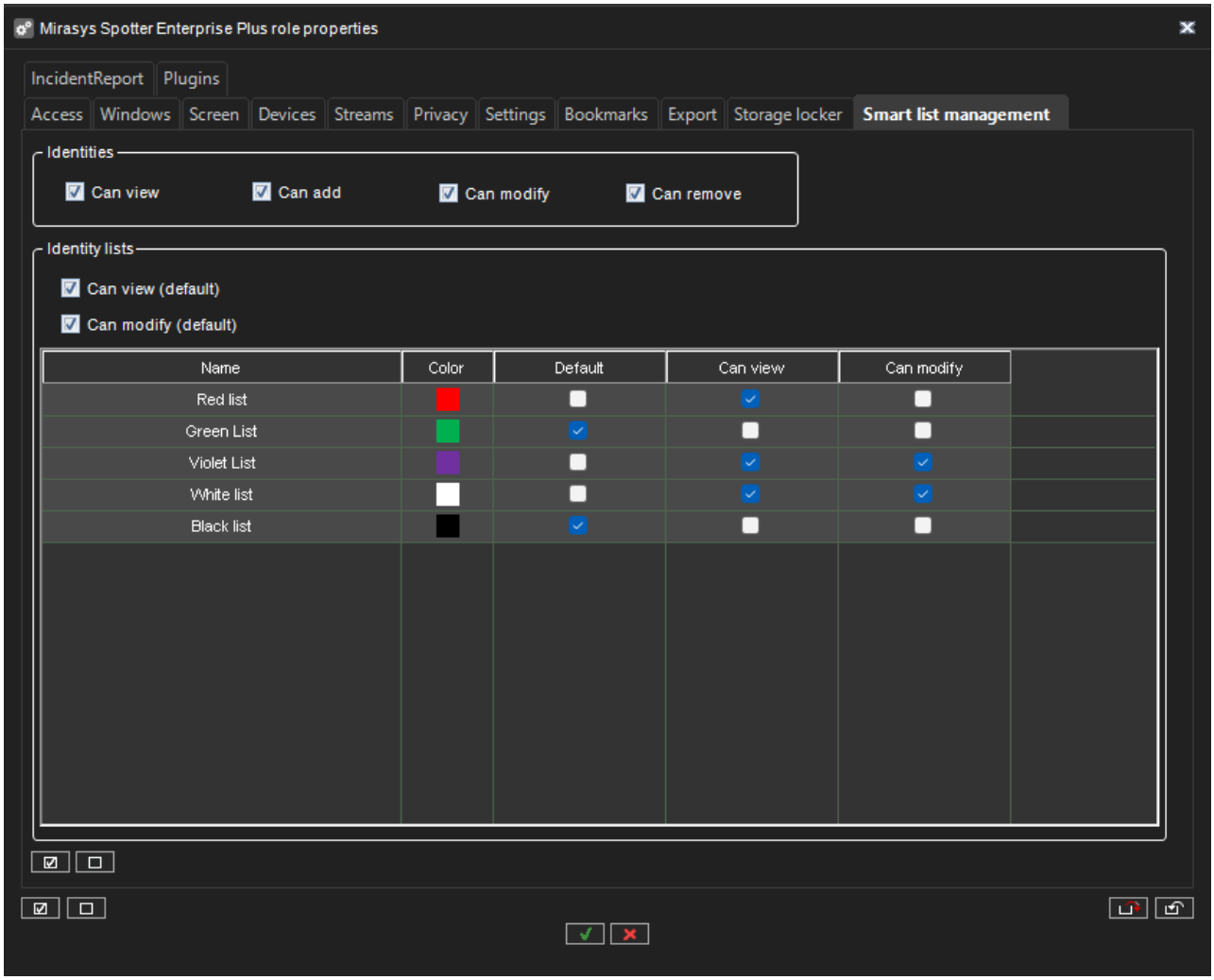
### 11.4.1.7 Smart List Management role

The Spotter List Management plugin can be enabled on the Spotter user role settings, where it is also possible to limit the permissions to manage identities and identity lists.

#### 11.4.1.7.1 Smart list management properties

The “Smart list management“ tab contains role properties related to smart list management functionality:

- Possibility to view, add, modify, and remove identities.
- Possibility to view and modify identity lists (default properties and properties for each list separately).




13 “Smart list management“ tab

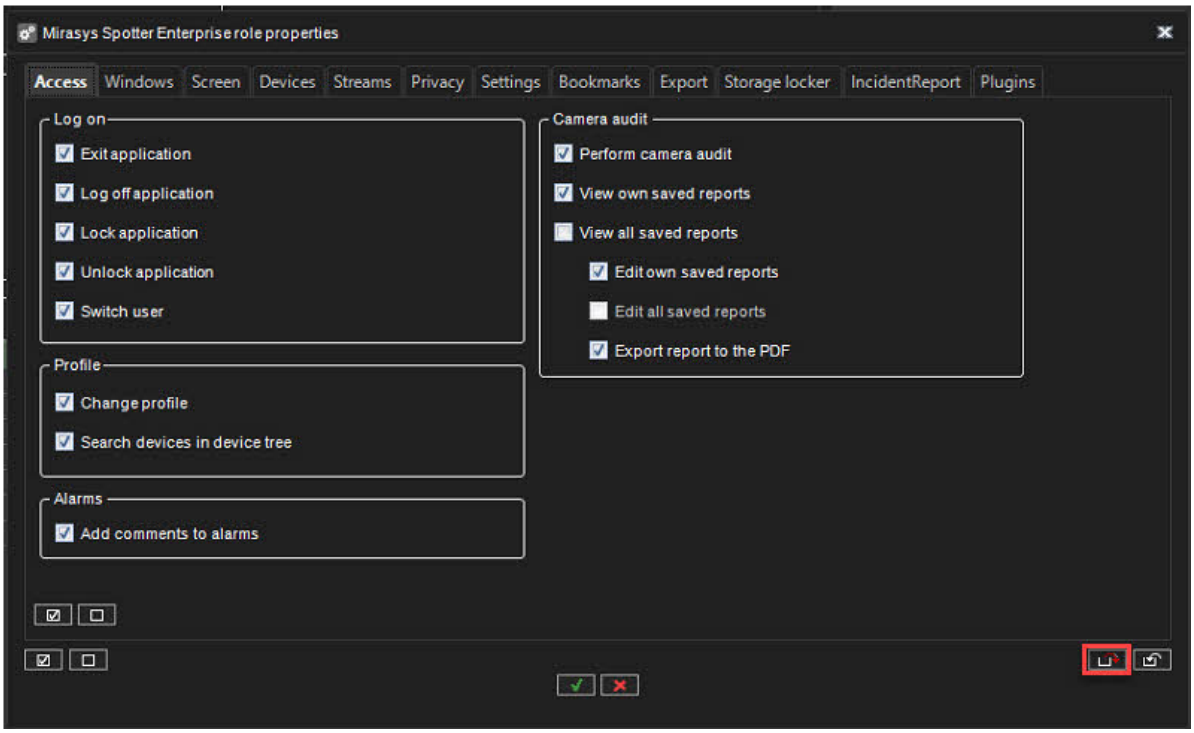
## 11.4.1.8 Spotter Web role

Spotter Web role enables new Spotter Web and Spotter Mobile usage

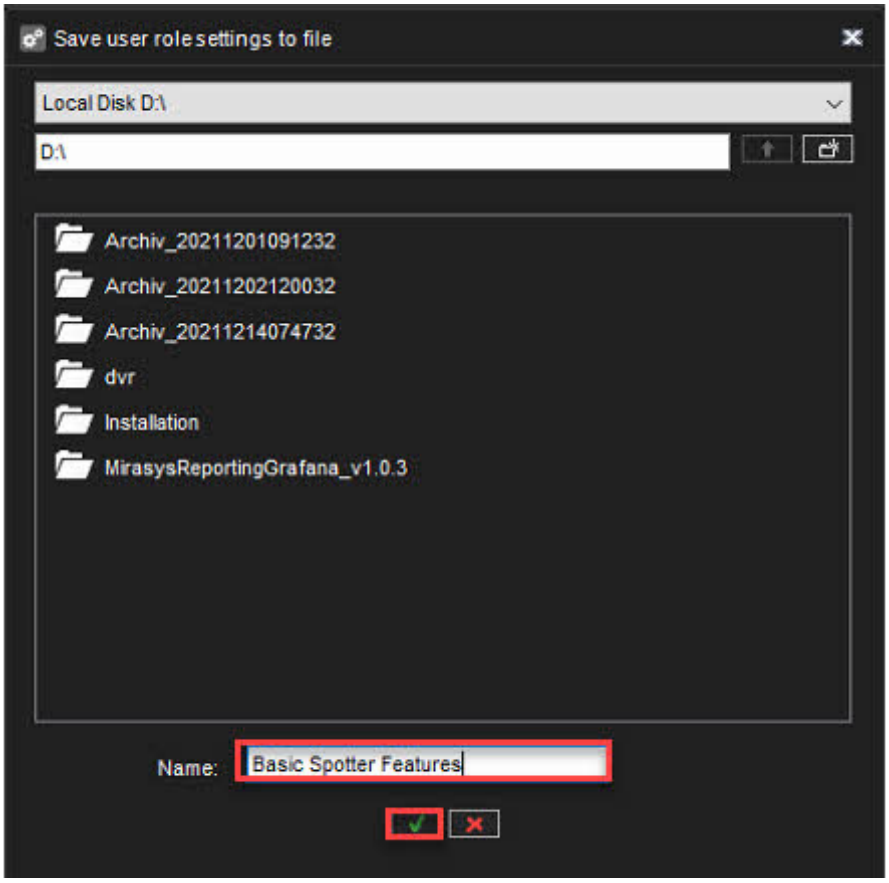
## 11.4.1.9 Exporting and Importing User Role Settings

### 11.4.1.9.1 Exporting User role settings

1. Click **Export user role settings to file**

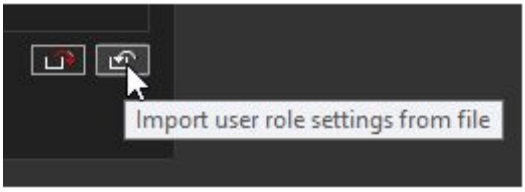



2. Select destination
3. Set the name of the file
4. Click **OK**

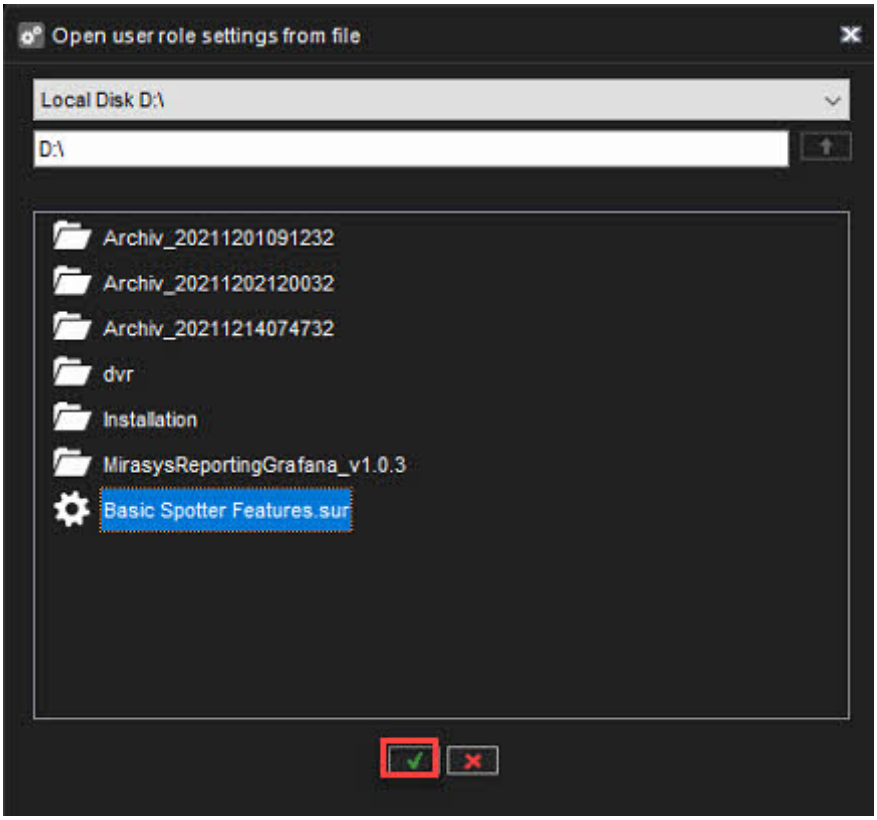



#### 11.4.1.9.2 Importing User role settings

1. Click **Import user role settings from the file**




2. Select file(.sur)
3. Click **OK**




## 11.4.2 Two-factor authentication

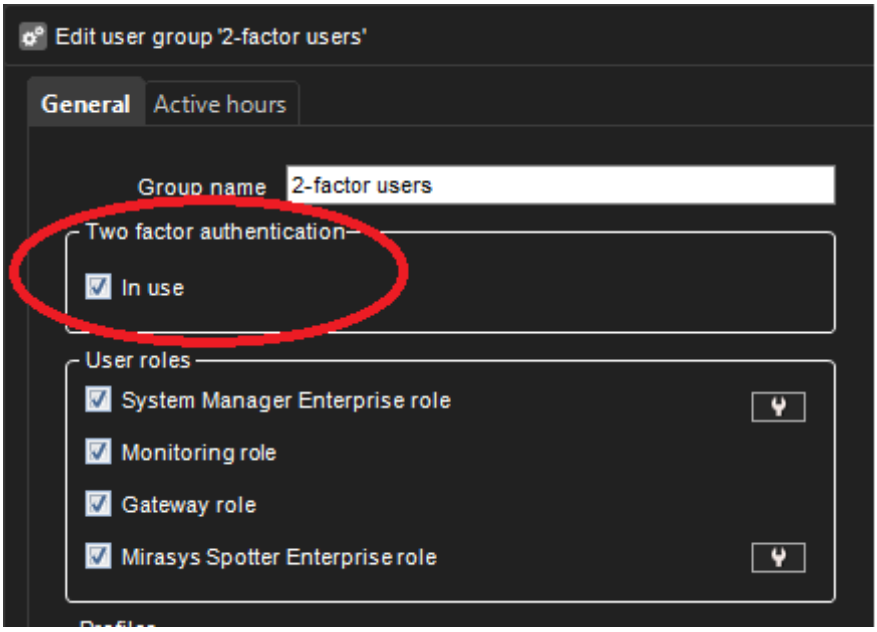
Two-factor authentication is functionality to improve the user's identification by requiring the username and password and a code from an external physical device.

This makes it practically impossible, e.g. certain user groups (e.g. system administrators), to use shared credentials.

(Using shared credentials would make it almost impossible, e.g. to monitor specific user actions from the audit logs later on.)

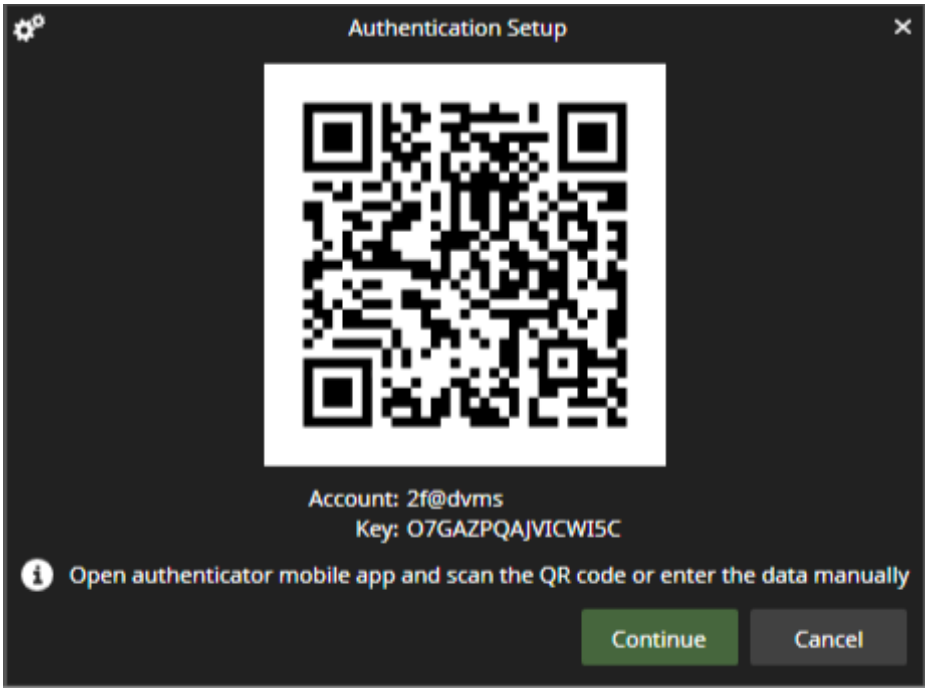
### 11.4.2.1 Setup:

1. The admin enables the 2-factor authentication for the specific user group.




2. When the user in the group tries to log in for the first time, the user is requested to use or install the 2-factor authentication client (e.g. Authy, Google authenticator, MS Authenticator (available for free)) on his/her mobile device.
3. The VMS and the authentication client are then synchronized with the software with VMS.
4. This happens by transferring the "secret key" generated by the VMS to the authentication software via QR code or directly typing it to the software.

Example below:

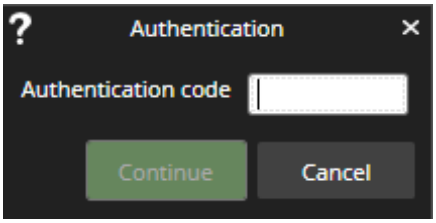



1. After that, the authentication client automatically generates new one-time passwords.

a. (The passwords change periodically and are kept in sync as the VMS clocks and the authentication app have the same time.
b. Note that this does not require any direct data communication link between the software.)

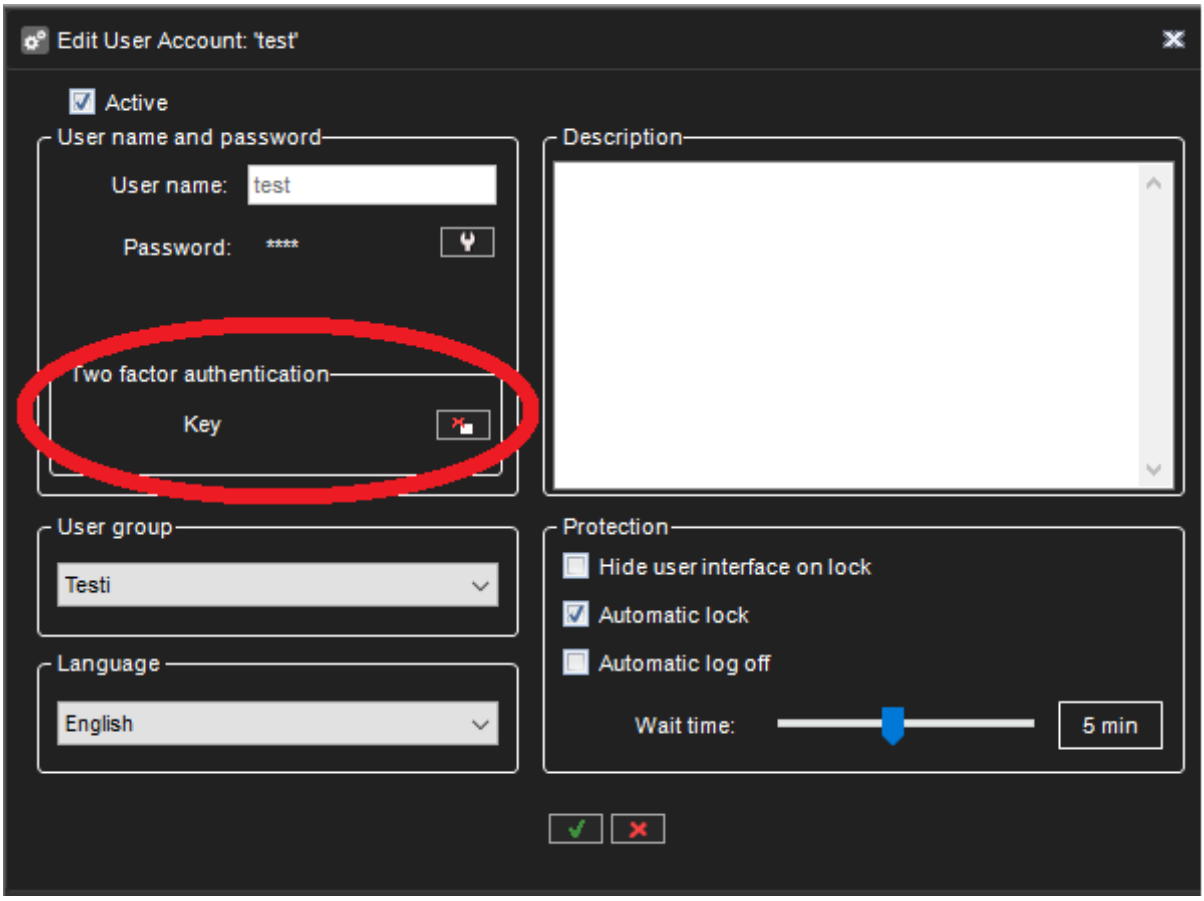
### 11.4.2.2 Login:

1. The user provides the standard credentials to VMS (username, password)
2. The VMS requests an authentication code from the authentication app for each login.
3. The user provides the one-time password from the authentication app. The user types them to the VMS client.




### 11.4.2.3 Maintenance:

1. If the user forgets his / her 2-factor secret key, the administrator can then reset the key from the system manager.
2. After the 2-factor secret key reset, the user needs to update the private key next time he/she logs in. (See step 2).



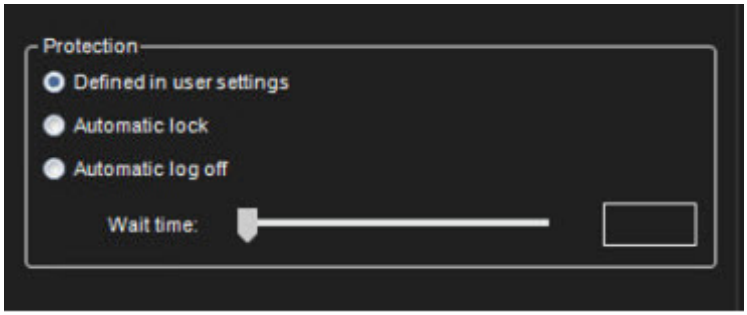

## 11.4.3 Protection

Protection group box is added in user group / general settings.

As default, "**Defined in user settings**" is set and Automatic lock, Automatic log off are not selected and Wait time settings is disabled.

Only one of the check box selections can be set at the time.

If user group level automatic lock / log off settings are selected, then user level automatic lock / log off settings are not enabled in user account settings

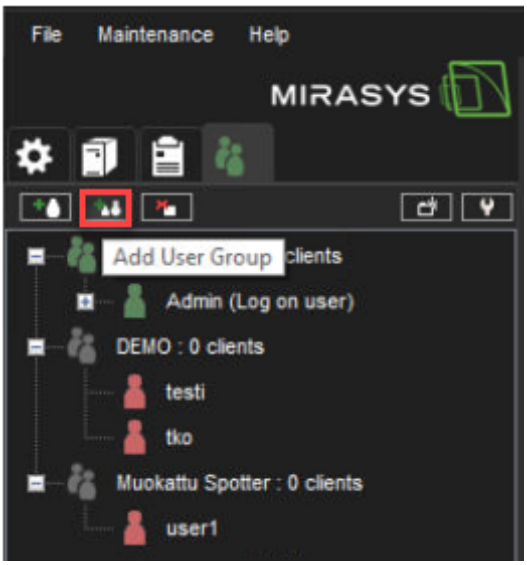


#### 11.4.3.1 Automatic lock and Automatic log off values

- 1-5 min, 10, 15, 20, 30 min, 1-12 hour and 24 hour

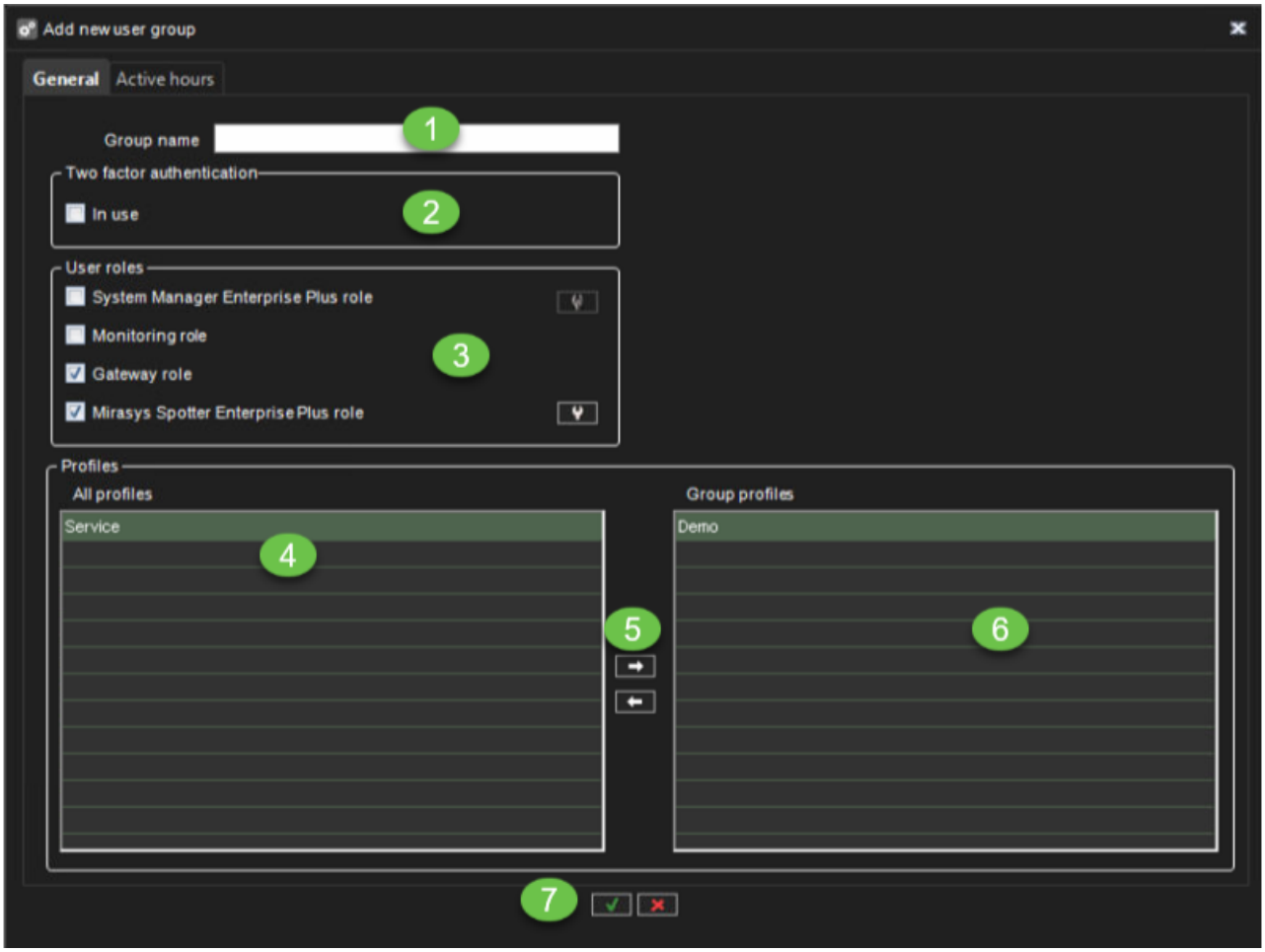
### 11.4.4 Creating a customer-specific User Group

1. Click **Add User Group**




2. Type a name for the group in the **Group name** box
3. Enable **Two-factor authentication**, if needed
4. Select the **User roles** for the group.
5. Select the **Profile** or **Profiles** you want to assign to the user group.
6. Click the right arrow button or drag the profiles from the left panel to the group profiles box
7. Check that correct profiles is found
8. Click **Ok** to confirm user group creation

**Tip:** *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*




### 11.4.4.1 Editing a User group

To edit a user group (whether system or domain**-based):**

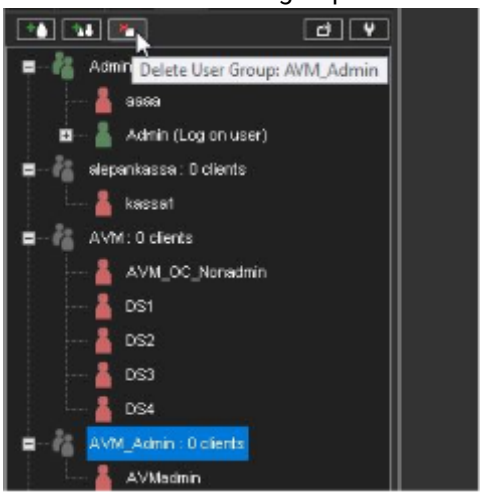
1. Open the **Users** tab.
2. Click on the user group you want to edit.
3. You can edit the following settings:
   a. Type a name for the group in the **Group name** box.
   b. Select the user roles for the group.
   c. Select the profile or profiles you want to assign to the user group. Click the right arrow button or drag the profiles from the left pane to the right.
4. Click **OK** to save the changes.

- **Tip:** *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*

### 11.4.4.2 Deleting a user group

To delete a user group (whether system or domain**-based):**

1. Open the **Users** tab.
2. Click on the user group you want to delete. Note that you cannot delete the default **Administrators** group.




3. Click **Delete User Group** in the upper-left corner.
4. Click **OK** to delete the group.

***Note:*** *Domain-based (LDAP) user groups cannot be deleted through System Manager. If deleted, an LDAP group is removed from System Manager, but the domain group is not affected.*

## 11.4.5 Domain Based User Groups (LDAP)

### 11.4.5.1 Domain Based User Groups (LDAP)

The system supports domain-level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups.

Domain-based users can log into the VMS system with their domain usernames and passwords.

By default, user group rights are synchronized with their parent domain every 30 minutes.

Please contact your system supplier if f you need to change the default interval.

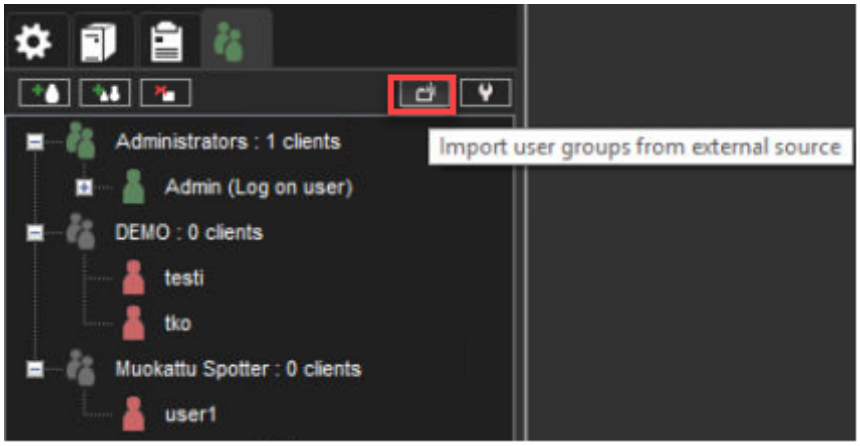
This feature requires a license update.

#### 11.4.5.1.1 To add a new domain-based user group to the system:

1. Click **Import User Groups from an external source** in the upper-left corner of the **Users** tab

The Master Server needs to be connected to a domain for the button to be displayed.

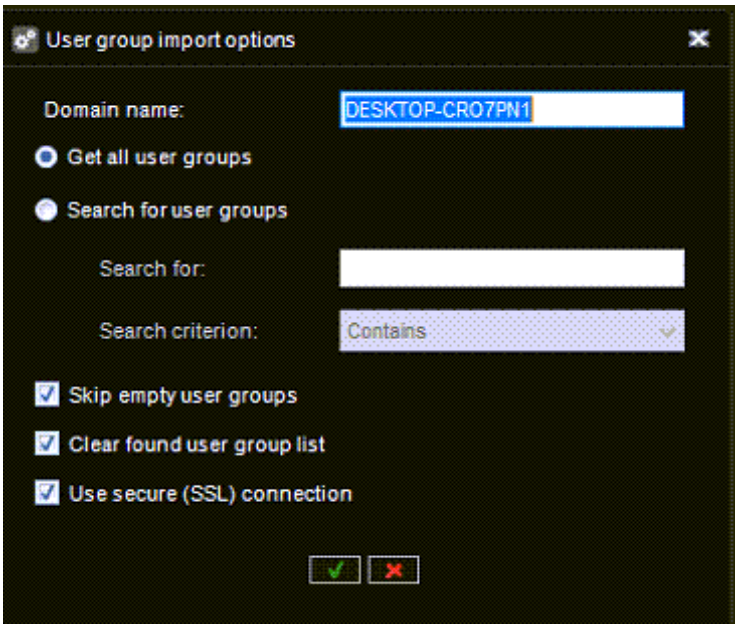
If the server is not connected to a domain, the button is not visible.




2. Type the name of the domain into the **Domain name** dialogue box.
3. Select whether to get all user groups or to search for specific groups.

If you want to search specific groups by name, you can add a search criterion based on the text string being equal to the group name, contained in the group name, or the group name starting or ending in the text string.

4. Select whether to skip or include open user groups.
5. Select whether to clear or keep previous search results.
6. Enable **Use secure(SSL) connection**. If needed
7. Click **Ok**.
8. In the **Import user groups** window, select the user groups you wish to import from the domain.
9. Click **Ok** to import the selected groups.
10. Edit the imported user groups to set their user roles as instructed below.



## 11.5 Creating a customer-specific user

To add a new user to the system:

1. Open the **Users** tab.
2. Click the name of the user group to which you want to add the user.
    a. Note that you can only add users to the system's native groups, not in domain-based groups.
3. Click **Add User** in the upper-left corner of the Users tab. The Add User dialogue box is shown.
4. Do the following:
    a. Type a name for the account in the **Username** box.
    b. To add a password to the account, click **Change password** and type the password two times.
    c. Type an optional description about the user account.
    d. Use the pull-down menu to select the user group into which you want to assign to the user.
    e. Select the user interface language for the user.
    f. Set protection settings for the programs:
        i. **Hide user interface on lock**
        ii. **Automatic lock**
        iii. **Automatic log-off**
        iv. **Wait time**: if the user does not use the program for the specified time, the program is locked, or the user is logged off.

***Note:*** Users can change their passwords and user interface language in the Spotter program.

### 11.5.1 Identify users through a user name separate from the user login ID

To improve platform security, users can be identified through a separate user name so as not to display and compromise the user login ID.

The System Administrator can define a public name for users in the System Manager user settings. The public user name should be unique. This is not mandatory, and the field can also be left blank.

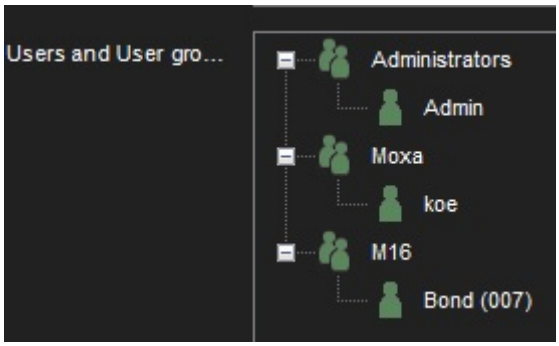
As before, the user will use the login user name to log into any application, but if a public user name has been entered for the user, this public user name will be displayed in the client UI.

### 11.5.2 Adding a public username in the System Manager

1. In the System Manager Desktop Application, go to User Settings and click edit.
2. In the **Public name** field, the system admin can choose to provide a public name for a user:


This name is displayed in the System Manager's users list:

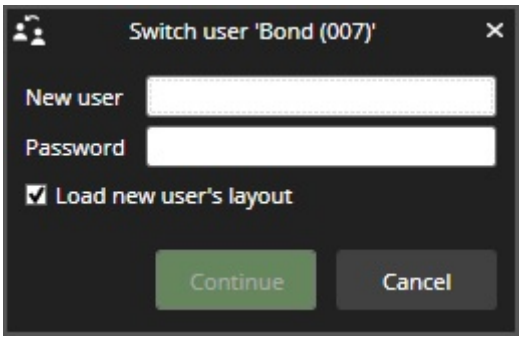

It is displayed in the profile settings user list:



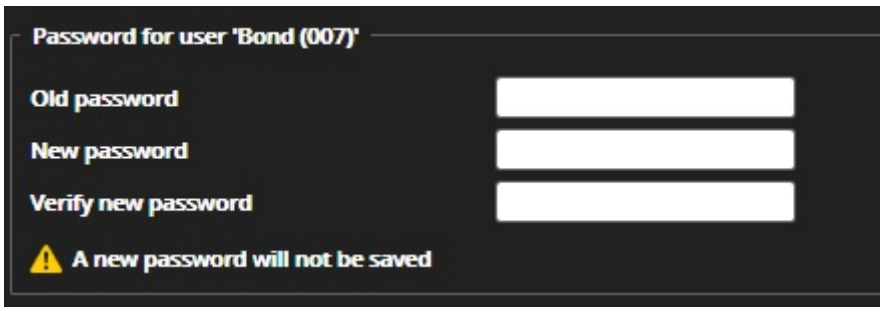

And also as logged on user:


### 11.5.3 Displaying a public user name to the user in Spotter

If there is a public user name set for a user in System Manager, the public user name is displayed together with the user identity, in switch user:




The users can also view their public user name when changing their password:




### 11.5.4 Public user name in Spotter web client

The public user name is displayed in Spotter Web in the top right corner if it has been defined in the System Manager.

If the public name has not been defined, the user's login name is shown.

If the user's public name is changed in the System Manager, the Spotter Web user is logged out, and the user needs to log in again. After the login, a new public name is shown on the main screen. If it has been removed in the System Manager, the same process applies, and after login the user's login name is shown.

## 11.6 User account settings

### 11.6.1 User account settings contain the following options:

- Account status
- Password
- Two-factor authentication key management, see more from Two-factor authentication (see page 244)
- User group
- Language
- Protection settings
    - Hide user interface on lock
    - Automatic lock
    - Automatic log off

### 11.6.2 Supported languages

- Arabic
- Chinese
- Czech
- Danish
- Dutch
- Estonian
- Finnish
- French
- German
- Hungarian
- Icelandic
- Italian
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Thai

## 11.7 Disabling or Activating a User Account

If you want to prevent a user from logging on to the system but want to keep the user account for later use, you can disable the account.

You can activate the account when the user is again permitted to log in to the system.

To disable or activate a user account:

1. On the **Users** tab, select the user account
2. Click **Edit User Account**
3. Do one of the following:

- To disable the account, clear the check box **Active**.
- To activate the account, select the check box **Active**.

4. Click **OK**.

***Note:*** *Domain-based (LDAP) users cannot be deleted or removed with System Manager.*

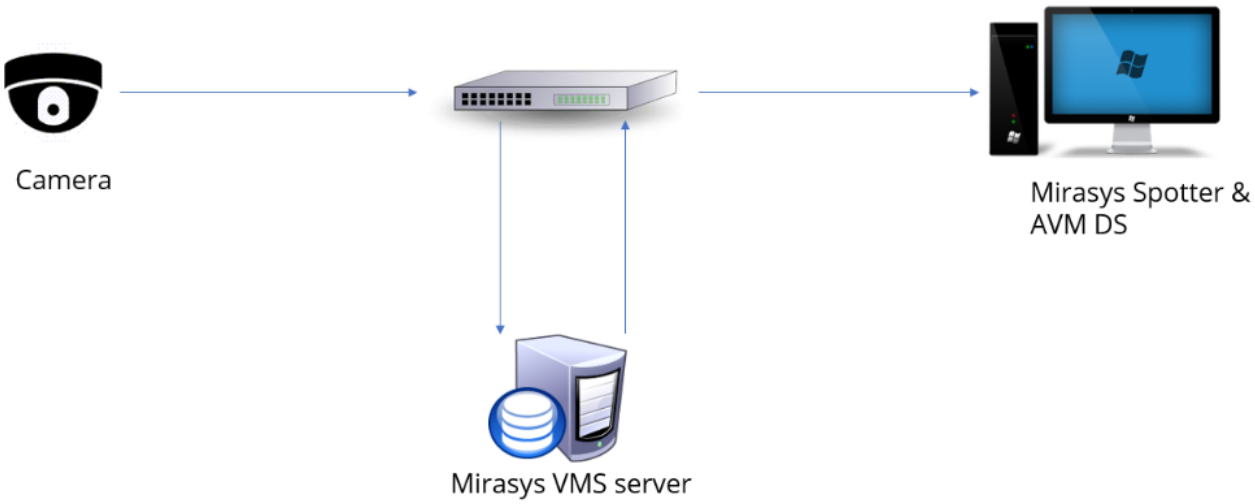
# 12 TruCast

TruCast is the direct camera video streaming feature in Mirasys VMS.

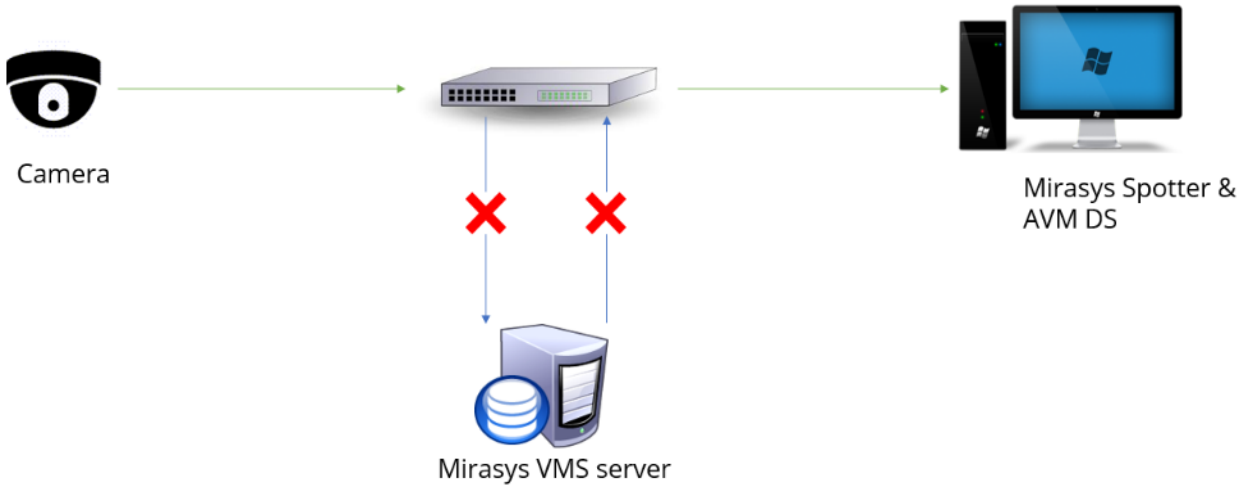
With TruCast, the video stream comes directly from the camera to the viewing client, the Spotter for Windows application.

In a standard streaming scenario, the stream to the client comes from the VMS Server.

## 12.1 Stream from the server to the client




## 12.2 Stream from the camera directly to the client




It is possible to get the direct stream from the camera to the client when the VMS Server connection is OK. This can be useful if users want to optimize network utilization.

# 12.3 Supported Cameras

## 12.3.1 Supported Cameras

TruCast requires a separate camera capture driver for the client.

Currently, drivers exist for the following camera manufacturers:

- Acti
- Axis
- Bosch
- Dahua
- Hikvision
- Lilin
- Samsung
- Sony
- Stanley
- ONVIF

Use the ONVIF TruCast driver for cameras that are not on the supported list.

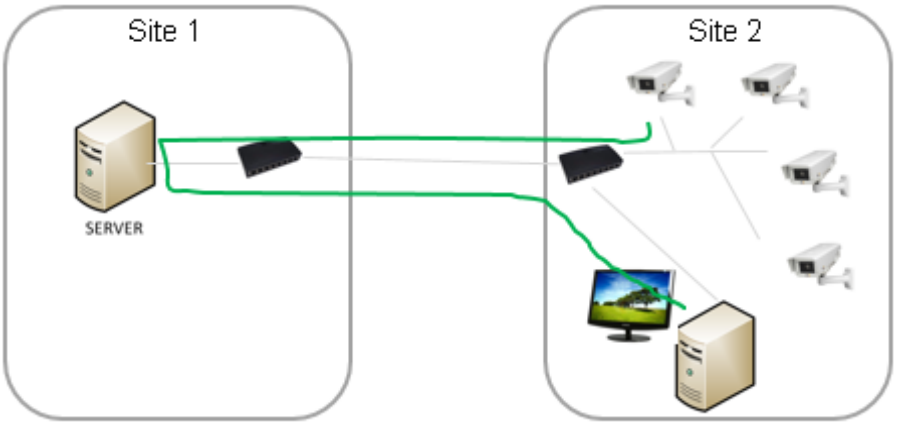
The use of the ONVIF driver requires that the camera is added to the VMS system with the ONVIF driver, not the camera's native driver.

# 12.4 Network Optimization

TruCast can be used to reduce network load in specific scenarios.

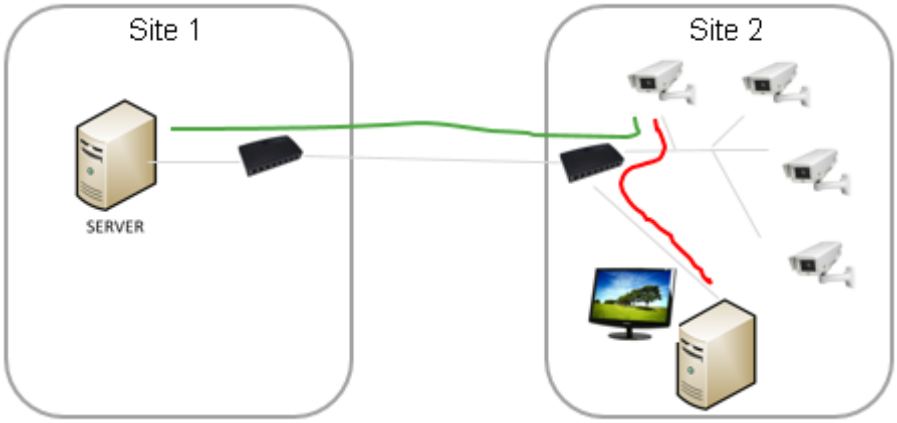
The load reduction mainly occurs when the server is located off-site (remote) and the viewing client is on-site (local to the cameras).

An example scenario 1, we have two sites where the recording is off-site, and the viewing client is on-site. In the following diagram, the viewing is done without TruCast, and the video goes first to the server and then from the server to the viewing client.




In this solution, the traffic between the two sites is increased.

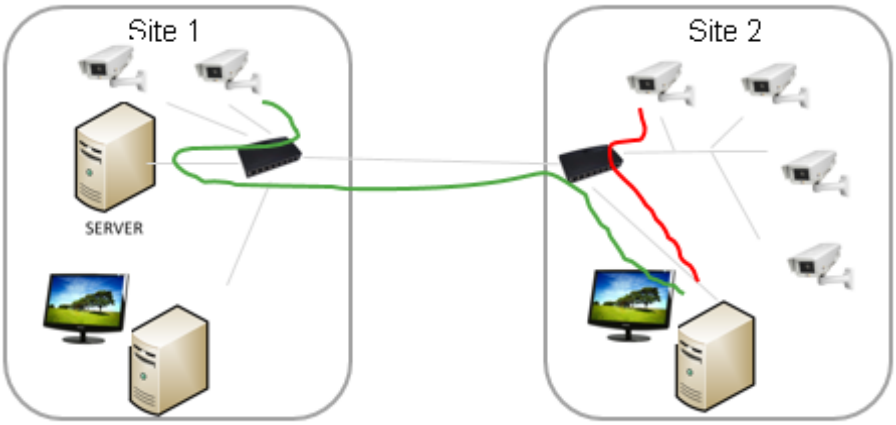
If the stream is consumed directly from the camera with TruCast, the traffic between the two sites is reduced.



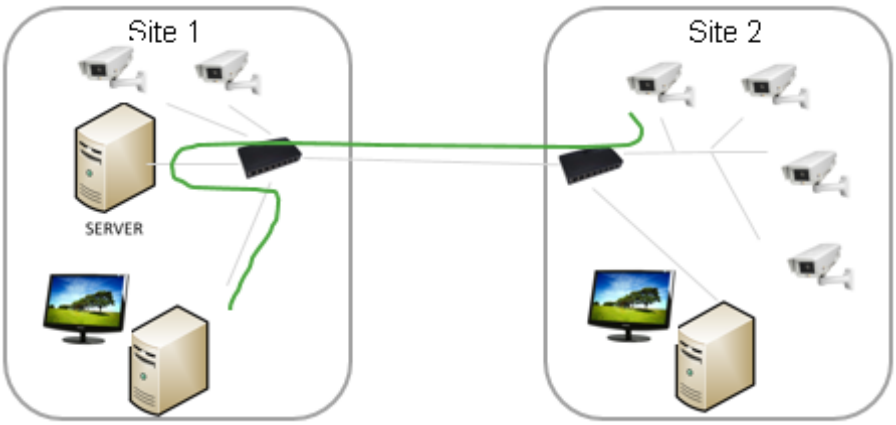

An example scenario 2, there are cameras on two sites and viewing clients on two sites.

For the Site 2 user, the use of TruCast makes more sense for the on-site cameras.

The user can choose to use TruCast for all cameras or only for the on-site cameras.




For the Site 1 user, the use of TruCast only reduces the amount of traffic from the server to the nearest network connection.




Users have complete control over which cameras are using TruCast and which cameras are viewed typically.

The setting is memorized for each camera and each user and saved to Spotter layouts.

# 12.5 Multistreaming and TruCast for Network Optimization and Storage

Since it is also possible to use a different stream for TruCast than the recording stream, this should be considered when planning the network capacity.

For example, users can choose to view live images with TruCast at a higher framerate (for example, 25 fps) and always record at a lower framerate (for example, eight fps).

This reduces the storage and network requirements considerably.

## 12.5.1 Impact of TruCast on Image Delay

Since the TruCast stream does not travel to the VMS Server and back, the delay from the camera to the client is slightly smaller, but the difference to the stream received from the server is not large, only some milliseconds.

The difference in the two-stream modes is complicated to observe in real life.

## 12.5.2 Features Not Supported in TruCast Streaming

TruCast does not support PTZ control or Audio

Also, currently, TruCast supports only live images. Playback (recorded images) is currently always received from the server.

## 12.5.3 Licenses

TruCast requires the VMS license to have the TruCast feature and the TruCast client driver identifiers used.

These TruCast driver licenses, and the TruCast feature, are always enabled in the Mirasys V9 product version.

## 12.5.4 Multiple Viewers

Since each TruCast-viewer opens an individual new stream from the camera to the client, users should trial how many streams can reliably be opened from the cameras they are using. In practice, 3-5 streams typically work ok.

## 12.5.5 Installing Client Drivers

Before using TruCast, the necessary client drivers need to be installed with the System Manager application if they have not been installed with the original system installation.

The client driver packages are available in the whole setup package from Mirasys. They are named with the “.sdi” filename extension.

These drivers are installed on the System Manager application’s first page, “Install client driver.”

The new drivers can be added by pressing the “Install new client driver” button and choosing the SDI packages.

After this, click the “OK” button.

After installing the drivers, they still need to be downloaded to the viewing Spotter clients. This is done when Spotter is restarted from the desktop.

After Spotter has downloaded the new drivers, the system is ready for TruCast use.

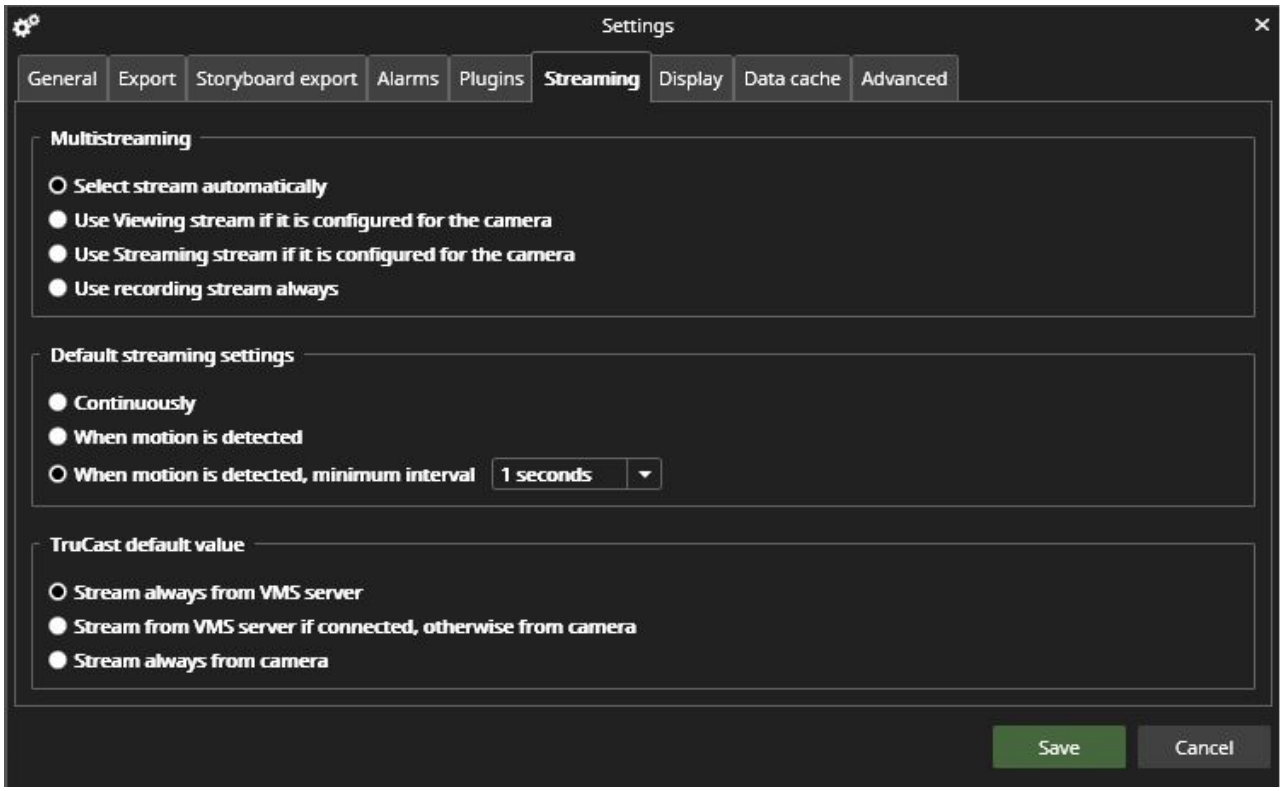
Please note that only those cameras which’ client driver was installed will appear as TruCast enabled.

### 12.5.6 Configuring multi-streaming

TruCast can use any stream from the camera, the Recording, Live viewing or Remote streams.

The multi-streaming is enabled and configured typically in System Manager – cameras.

In the Spotter client settings – streaming – multi-streaming, the user can choose which one of the streams is used for viewing. The same setting is used for standard and TruCast viewing.




### 12.5.7 TruCast Default Setting

The default setting for all cameras that have not been used for TruCast before can be defined in Spotter settings – streaming – TruCast default value.

The possible values are

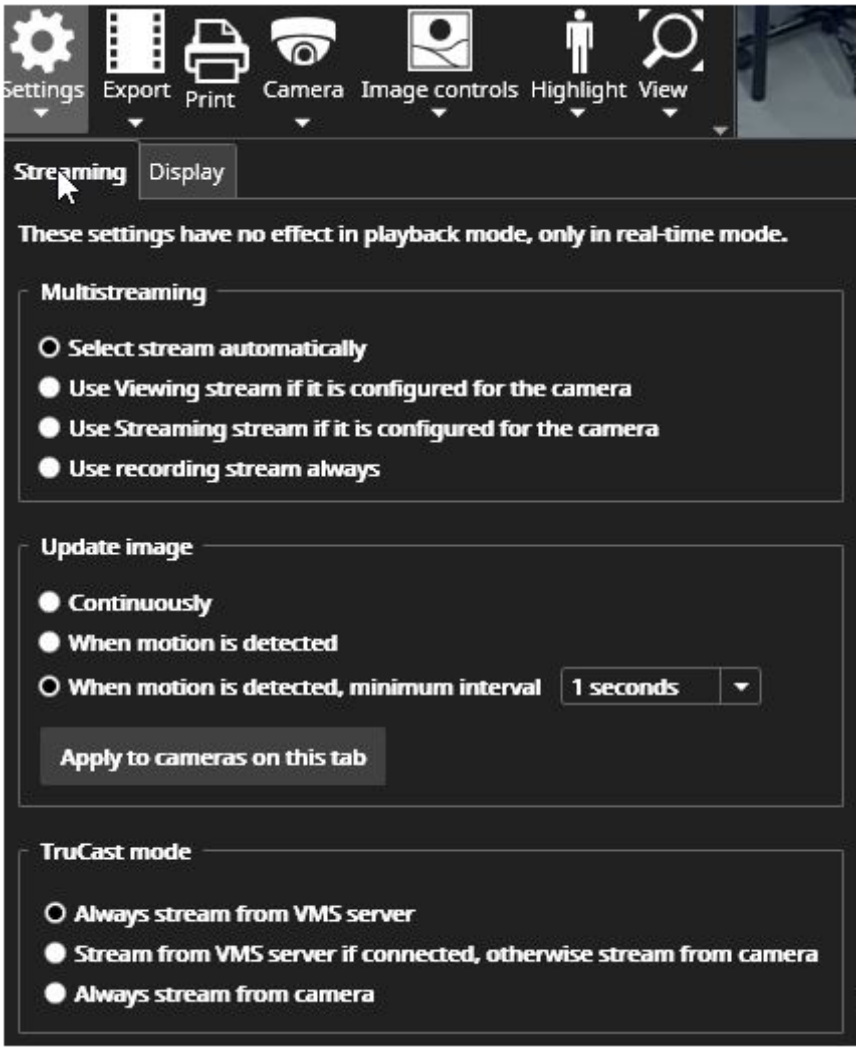
- Always stream from the VMS Server
- Stream from the VMS Server normally, but switch to TruCast if the connection to the server is lost

- Always stream using TruCast

## 12.6 Using TruCast

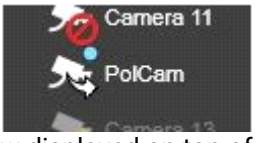
The user can see the cameras that have TruCast capability from the camera toolbar – settings.

For those cameras that have TruCast the setting is available.




For cameras that do not have TruCast, the lower part of the dialogue is disabled.

The setting is memorized for each camera separately.




When TruCast is active, there is a small arrow displayed on top of the camera in the device tree.

# 13 Failover Servers

❗ If you need to failover also the VCA channels, the failover server must contain the correct amount of the activated VCA channels.

Mirasys VMS supports failover video servers as a Mirasys VMS option.
Failover servers are VMS Servers on a passive standby until the system recognizes that one of the active video recording VMS Servers has broken down; at this point, a failover server takes the place of the broken server.
The failed server can be repaired and replaced as a new failover server, while the failover server that took its place can continue operating as an active server.
***Note**: When a failover server takes the place of an active server, any Spotter plugins (such as Grafana or List Management Application) that are not built-in are not included in the switch and must be re-installed manually after a server restore.*

*Recording and failover servers should be of a similar hardware setup and share drive letter assignments and version numbers.*
*Analogue cameras connected to a server's capture card will not be transferred to the failover server. Only previously assigned IP cameras are reassigned during the switch.*

## 13.1 Failover Functionality

When adding a new server into the system, the administrator can select whether the added server is a standard server or failover server.
There can be any number of failover servers (0-n).
If the server is the standard server, the administrator can choose if that particular server will be added to the failover monitoring, i.e., in case of server failure (hardware or software), this server will migrate to the available failover server.
It is important to note that the Master server needs to be installed on hardware separate from those operating with recording licenses or failover licenses.
The minimum hardware setup consists of three servers: one Master Server, one video recording VMS Server, and one standby failover server.

### 13.1.1 Failover migration will be triggered in the following conditions:

- The Master Server has lost the connection to a VMS Server, and the timeout set by the administrator has been reached
- A VMS Server has informed the Master Server that connection to all the material disks (recording storage) on the server has failed
    - Manual data recovery from server hard drives can be attempted if the disks are still functional
- A server's Watchdog service has informed the Master Server that it cannot initialize the recording service

A recording is continuous after the failover server has taken over to keep the system operational.
The only exception is the timeout time between disconnect and failover trigger. The administrator configures this.

After a failover server has assumed the recording role of a failed server, a system backup will automatically be created to set a new baseline.

#### 13.1.1.1 During the failover restore process and the following system backup:

- Users cannot perform manual backup operations
- Any following broken servers are added to a failover queue

The failover queue is handled after the failover restore has been completed.

## 13.2 Failover summary since V9.5.0

In V9.5.0 VMS, failover functionality was renewed to work quicker than before. It can be triggered manually. In the same version, failback functionality and material copying from failover server to recorder after failback was also implemented.
Failover log was also added where the user can see all occurred failovers and how those are processing, and the user can also trigger failback and material copying manually.

## 13.3 Description

Failover in V9.5.0 was changed not to use system backup files. Instead, SMServer will store recorder settings with schedules and motion masks to recorder settings cache and uses these settings when doing the failover.
Recorder settings, schedules and masks are requested from the recorder when SMServer makes connection to the recorder.
As a part of the making failover quicker, recorder startup was also optimized to start as quickly as possible.

There are now also smaller network disconnection detection times added. In earlier version the smallest time was 1min, but now there are options for 10s, 20s, 30s, 40s and 50s.

## 13.4 Recorder settings cache

- Recorder settings are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSettingsStore"
- Recorder masks are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderMasksStore"
- Recorder schedules are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSchedulesStore"

## 13.5 Failover process

1. When failover is started (triggered manually by user, by network connection lost or by critical recorder failure), SMServer will do following operation

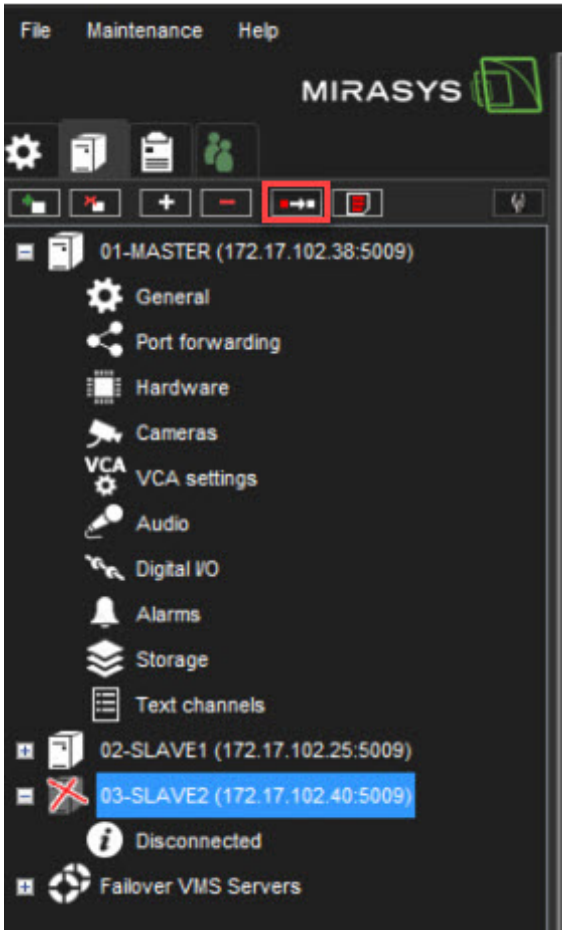
2. Check if there is failover server available that belongs to same failover group as failed recorder and there is connection to the failover server
3. Creates failover log entry about the failover
4. Get settings, masks and schedules of the failed recorder from recorder settings cache
5. Saves failed recorder settings to failover server
6. Makes changes to system data that failover server has taken the tasks of the failed server
7. Makes changes to the system data that failover server is now acting as normal recorder and failed recorder is in broken state
8. Sets failover progress result to failover log
9. Sends system change notification to clients

## 13.6 Manual failover triggering

User can trigger manual failover from System Manager UI in recorder settings tab. Manual failover is possible, if

- there is connection to a failover server that belongs to same failover group as the selected recorder
- selected recorder has failover enabled
- User has role that allows to trigger failover manually

1. Select the broken VMS server from the list
2. Click **Start failover from selected VMS server to the failover server**




## 13.7 Minimum requirements

- **Master server installed on separate PC**
  - The license must contain an automatic backup feature
  - The license must contain one or more failover server
- **1 slave server for recording**
- **1 standby failover server**
- The license must contain at least the same amount of video channels as recording slave server
- Same size material HDD and assigned drive letters

### 13.7.1 IP camera drivers

Please make sure that failover servers contains the same version drivers, which normal recording servers has

## 13.8 VMS Server roles

### 13.8.1 VMS Server role FAILOVER

To set a server as a failover server, there has to be a free failover license slot available.
When a server is added as a failover server, the System Manager sets the server to standby mode.
The Failover VMS Servers group shows server connection states and server general settings if the connection is available.

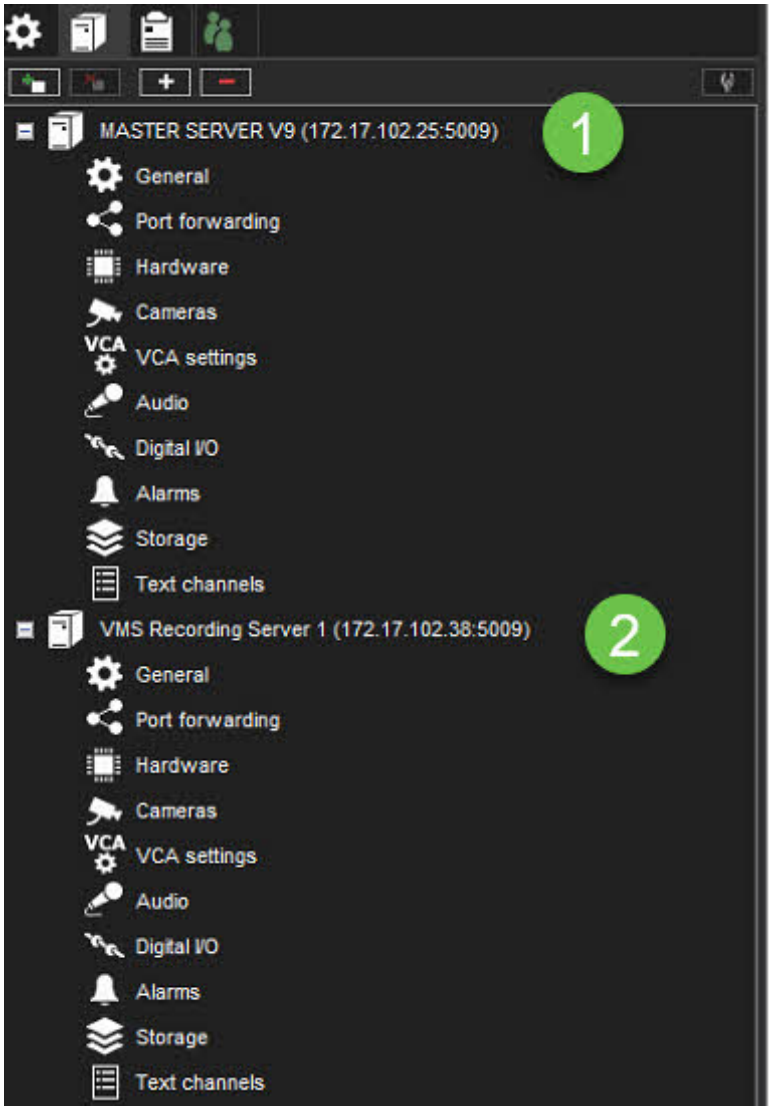
### 13.8.2 VMS Server role BROKEN

The Broken VMS Servers group displays connection states; the settings on broken servers cannot be changed.
Users can, however, export server logs if there is a connection to a broken server.
To get a broken server that has been replaced by a failover server back into the system, it must first be removed manually and then added again as a new server.

## 13.9 Building Failover system

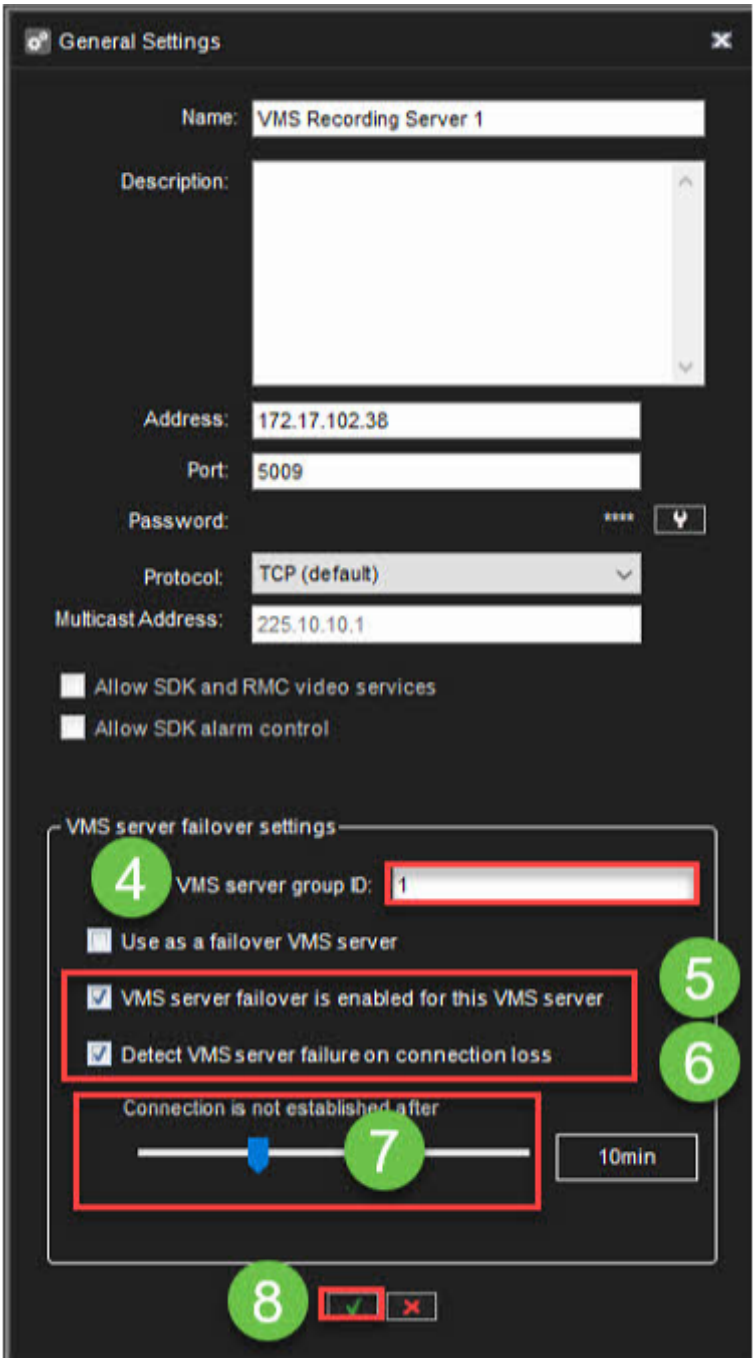
### 13.9.1 Starting point

The master server and 1 recording slave server were added to the system




#### 13.9.1.1 Enabling VMS failover server to the recording server

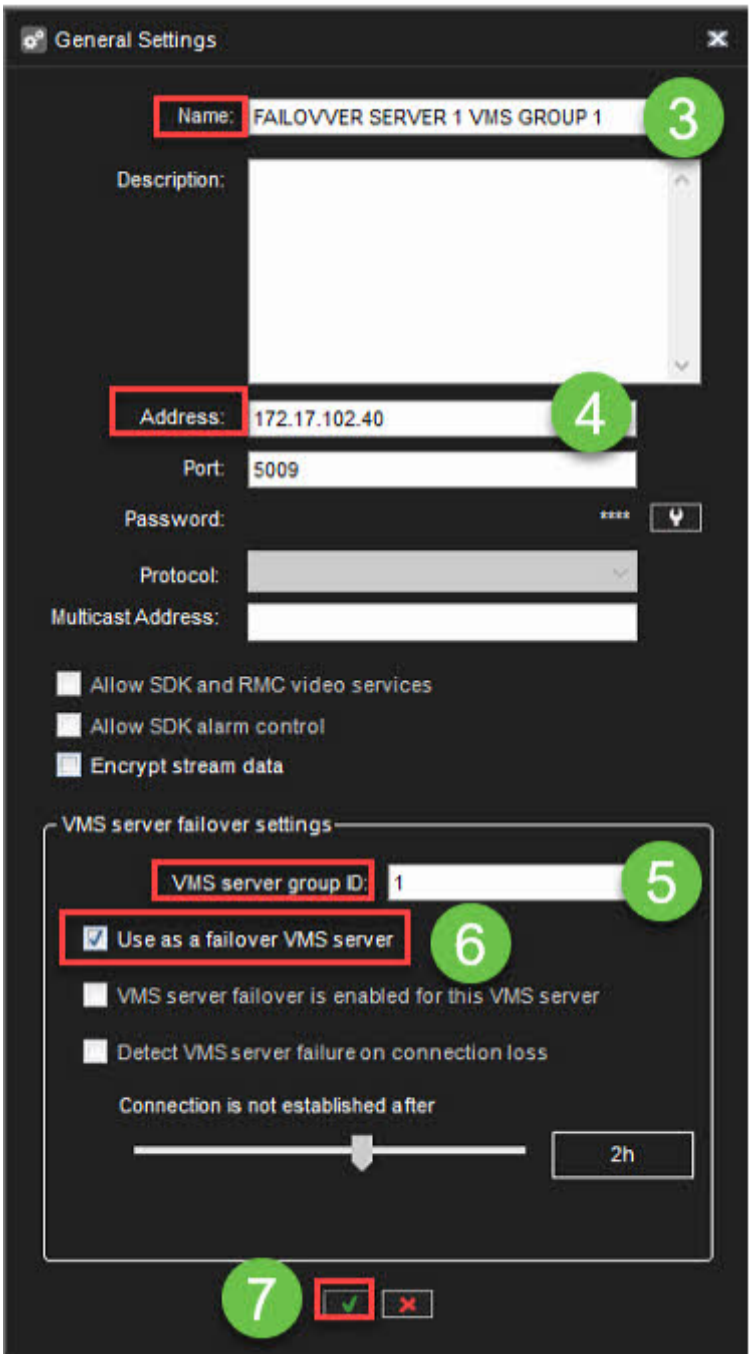
1. Open the **VMS Servers** tab
2. Select slave server from the list
3. Click **General**
4. Define **VMS server group ID(default 1)**
5. Enable **VMS server failover is enabled for this VMS server**
6. Enable **Detect VMS server failure on connection loss**
7. Define value **Connection is not established an after**
8. Click **OK**



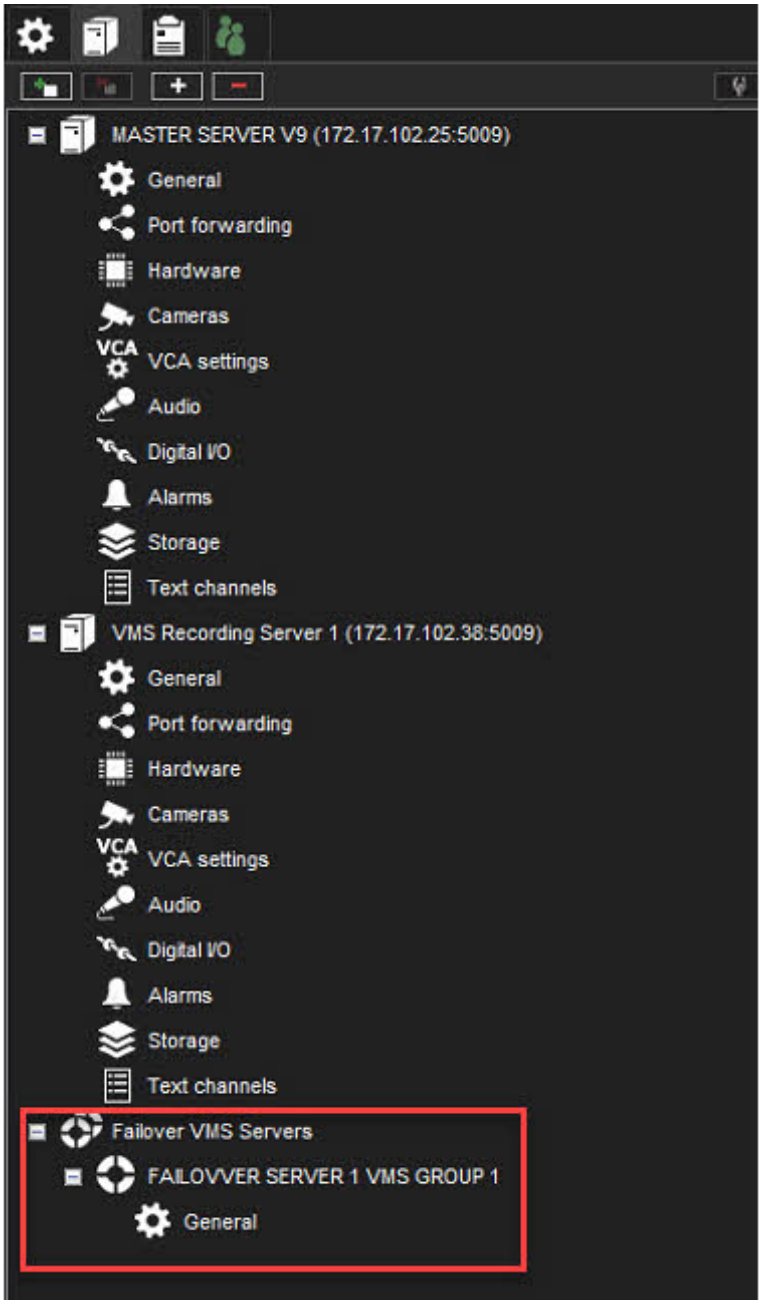

### 13.9.1.2 Adding FAILOVER server

1. Open the **VMS Servers** tab
2. Click **Add VMS server**
3. Set the name for the server

4. Set IP address of the server
5. Define the **VMS server group ID**
6. Enable **Use as a failover VMS server**
7. Click **OK**




After the adding, the VMS Server tab shows **Failover VMS Server** line


MASTER SERVER V9 (172.17.102.25:5009)
General
Port forwarding
Hardware
Cameras
VCA settings
Audio
Digital I/O
Alarms
Storage
Text channels
VMS Recording Server 1 (172.17.102.38:5009)
General
Port forwarding
Hardware
Cameras
VCA settings
Audio
Digital I/O
Alarms
Storage
Text channels
Failover VMS Servers
FAILOVVER SERVER 1 VMS GROUP 1
General

# 14 Failback

*Supported from V9.5.0*

In V9.5.0 failback can be done either automatically or manually and there is no need to use settings backup to revert the failover.
The Failback uses same functionality as failover, but in reverse order by moving server functionality from failover server back to failed server. Manual failback can be triggered from failover log.
Automatic failback will trigger failback when automatic failback is enabled and connection to failed server is restored successfully.

## 14.1 Failback process

When failback is triggered (manually or automatically):

1. Check that there is valid failover log entry and the failover state in the log is correct
2. Check that failover server is still acting as normal recorder
3. Check that failed server is still in broken state
4. Check that failover is enabled in the license
5. Check that there is no ongoing failback process running for the failed recorder
6. Update the failover log that failback is started
7. Get failover server recorder settings, configuration files, masks and schedules from recorder settings cache
8. Set failed recorder settings
9. Mark failover server to act as failover server again and mark failed recorder to be in ok state
10. Update the failover log that failback has been performed
11. Send system change notification to clients

### 14.1.1 Manual failback triggering

Failback can be triggered manually from failover log. Manual failback is possible if

- failover has performed successfully
- failback is not in progress or failback is not performed already
- user has role that allows to trigger failover manually

### 14.1.2 Automatic failback

Automatic failback can be enabled from server general settings when failover is enabled for the server.
Automatic failback will not occur if maintenance mode is on.
Automatic failback is triggered when SMServer service connects successfully to failed server.

Failback functionality will then get all failover log entries from failover log database for the failed server where failover has been done successfully and failback process has not been done successfully and failback process is not ongoing.
If one or more log entries are found, failback process (described above) is processed.
If there are more than one failover log entry that fulfills the automatic failback requirement, newest log entry is used for failback process.
When the failback process have been successfully done, log entry that was used for failback is updated that failback is done successfully. For other log entries, failback and material copying are marked as done successfully.

## 14.2 Material copying from failover period

Material copy is done from failover server to main server, this task is added to server's processing using DVRFailoverService.

DVRFailoverService has those methods:

- **StartDataCopy** - add new material copy task to server processing queue
- **UpdateClientInfo** - update client information for server in case of connection between server and SMServer was lost to communicate with failover server correctly
- **UpdateFailoverTaskState**s - update material copy state in case of connection between server and SMServer was lost
- Server saves material copy task to database and process those tasks one by one. If some task will be failed, server save last task times and state and continue with other tasks.

What is copied during material copy for a specified time period (start of failover operation and end of failback operation):

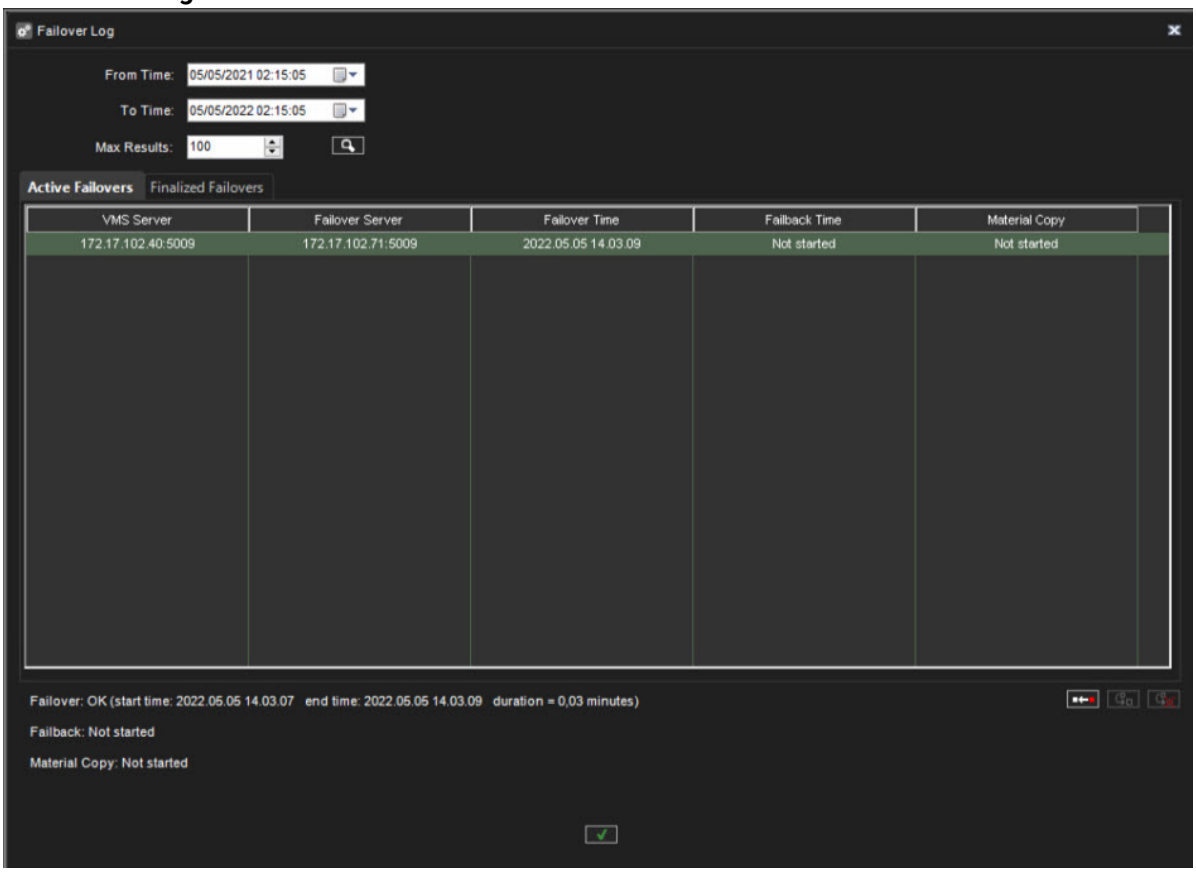
- Audio data for all configured audio channels
- Video data for all configured video channels
- Text data for all configured text channels
- Metadata for all configured video and text data channels
- ANPR data for all configured video channels
- Alarms for all configured alarm id's
- Server process each channel listed above one by one and save last received channel time. If connection between servers will be broken or some error will happen, recorder saves last state of material copy task and continue from last unprocessed channel (and last processed channel time).

Server use playback functionality for audio, video, text and metadata and ANPR and Alarms search services to get required data for specified time period.
Also, due to Geniune channels security limitations we can't use server as ZpaServer and ZpaClient at the same time, so calllbacks are not working in communication server to server.
So, ANPR and Alarms search services now have additional methods to get required data without using callbacks.

## 14.3 Failover log

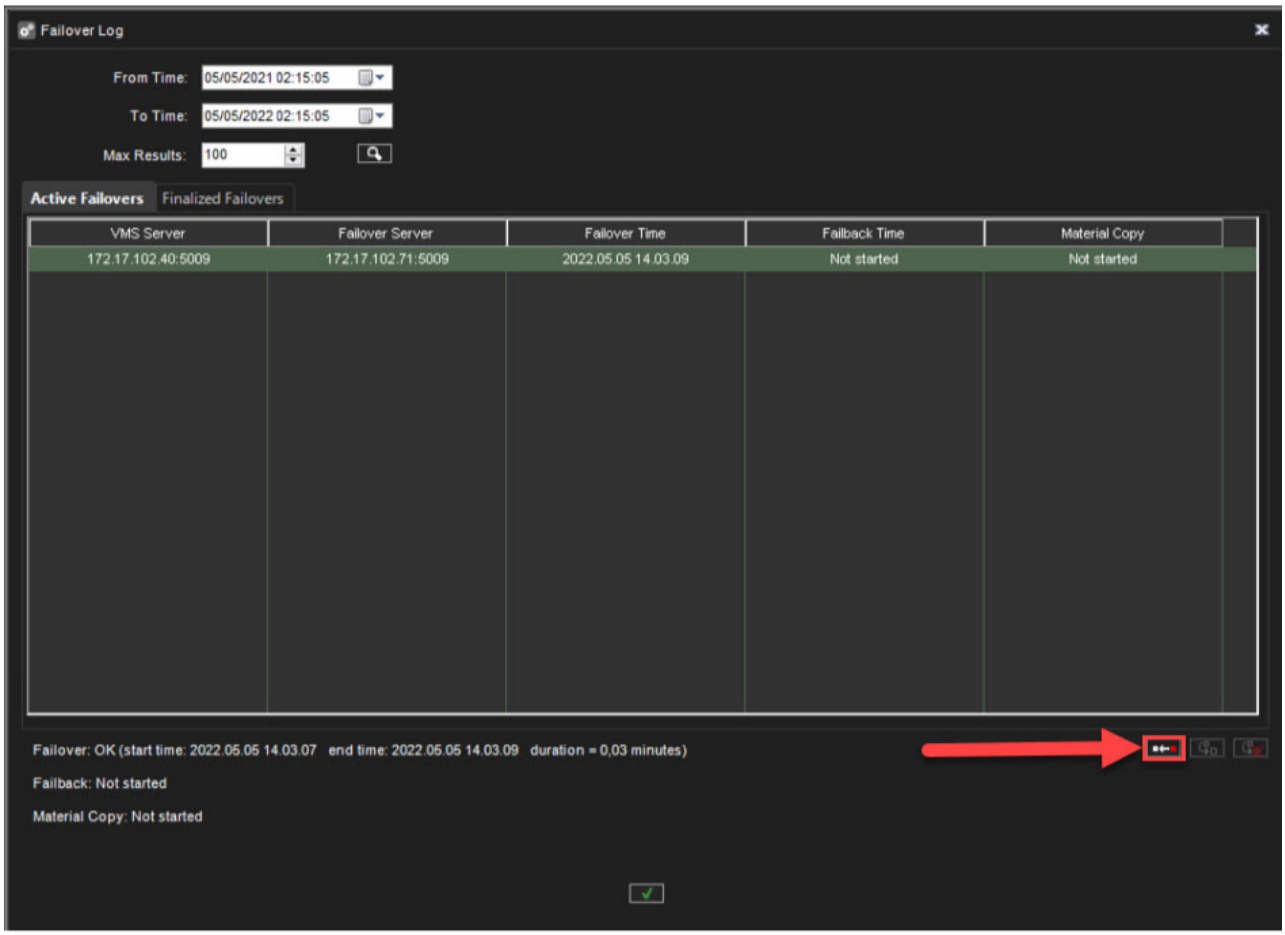
1. Click **Open failover log** from the **VMS servers tab**


2. The **Failover log** shows **Active Failovers** and **Finalized Failovers**

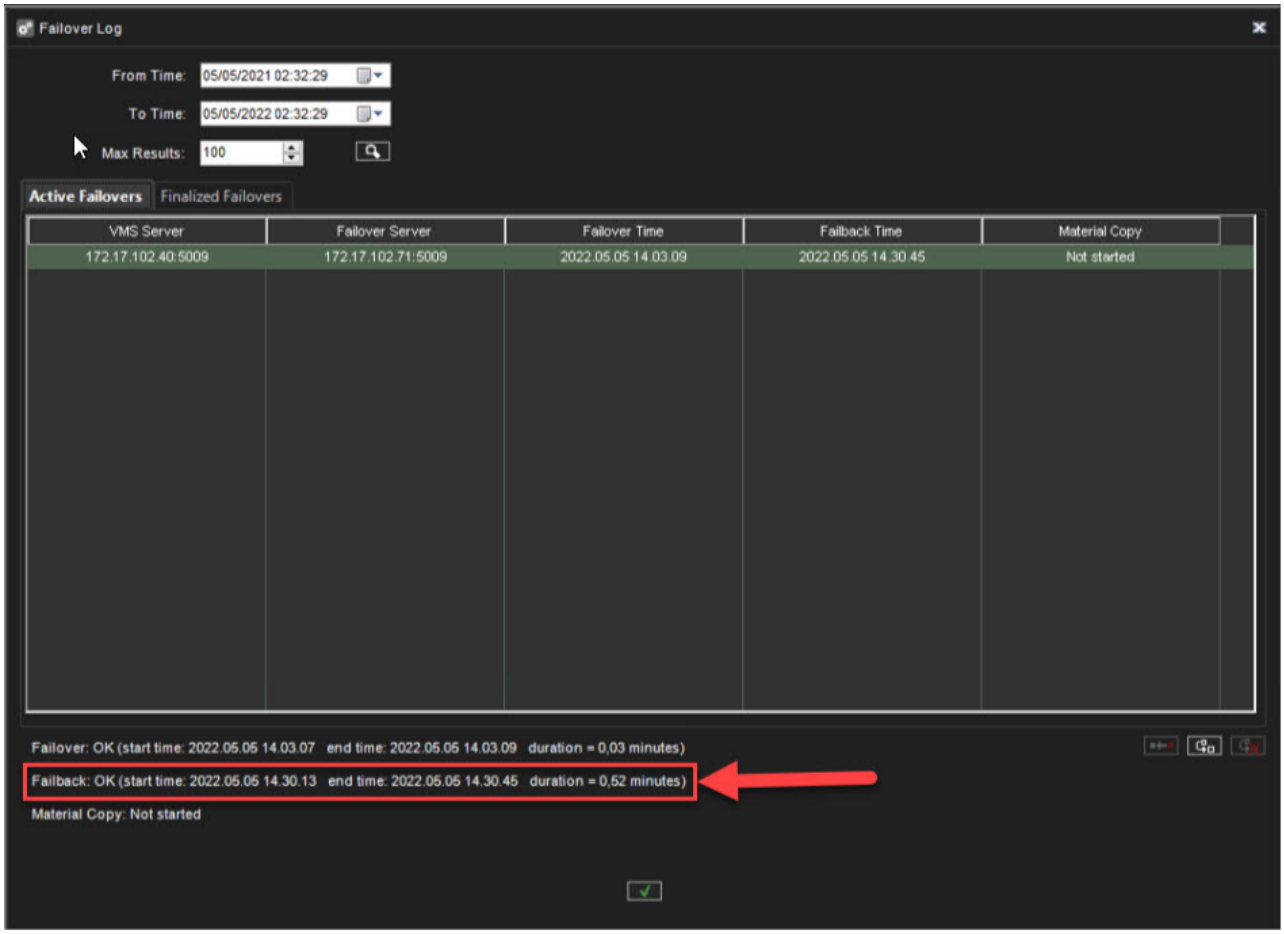


### 14.3.1 Start Failback for the selected server

3. Set fixed VMS server to the network with the same IP address
4. Select the server from the list
5. Click **Start failback to the selected server**

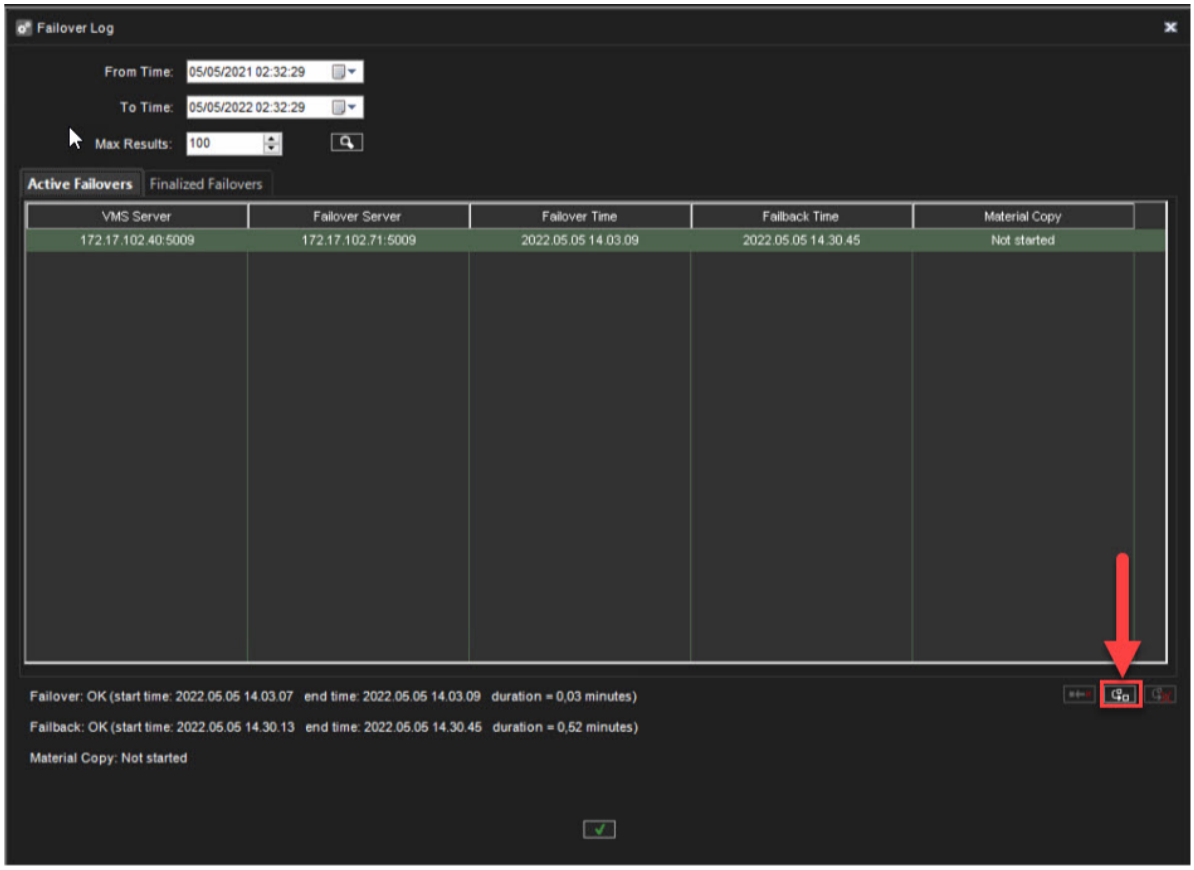



When the failback is successfully done, Failback OK message with the **start time**, **end time** and **duration** is shown




## 14.3.2 Start material copying to the selected server

1. Select the server from the list
2. Select the first material copy, which has not been finalized from the list
3. Click **Start material copying to the selected server**


Failover Log
From Time: 05/05/2021 02:32:29
To Time: 05/05/2022 02:32:29
Max Results: 100
Active Failovers
Finalized Failovers
VMS Server
Failover Server
Failover Time
Failback Time
Material Copy
172.17.102.40:5009
172.17.102.71:5009
2022.05.05 14.03.09
2022.05.05 14.30.45
Not started
Failover: OK (start time: 2022.05.05 14.03.07 end time: 2022.05.05 14.03.09 duration = 0,03 minutes)
Failback: OK (start time: 2022.05.05 14.30.13 end time: 2022.05.05 14.30.45 duration = 0,52 minutes)
Material Copy: Not started

# 15 AI Guides

## 15.1 Mirasys List Management (LM)

### 15.1.1 Mirasys List Management Introduction

List Management (LM) is used to process Face Recognition (FR) and License Plate Recognition (LPR) events by matching detected faces and license plates to an identity and identity list. LM service is used to store identities and identity list information, receive and save LPR and FR events, send LPR and FR events to clients, do searches in saved events, and send LPR and FR events to the VMS server for processing.

LM service has the following abilities:

- Store identities and identity lists in the database
- Receive and store LPR and FR events in the database
- Match detected license plates and faces to defined identities and identity lists
- Search LPR and FR events from the database using search parameters
- Send real-time LPR and FR events for clients and recorders
- Send LPR and FR events to the VMS server for processing
- Notify clients and recorders about changes in identities and identity lists
- Enable integration to License Plate and Face recognition

The list Management service has a separate installer, so it can execute on a separate server or on some VMS server.

List Management settings (identities and identity lists) can be managed in System Manager List Management settings and in the Spotter Smart List Management plugin.

### 15.1.2 LM Service Installation

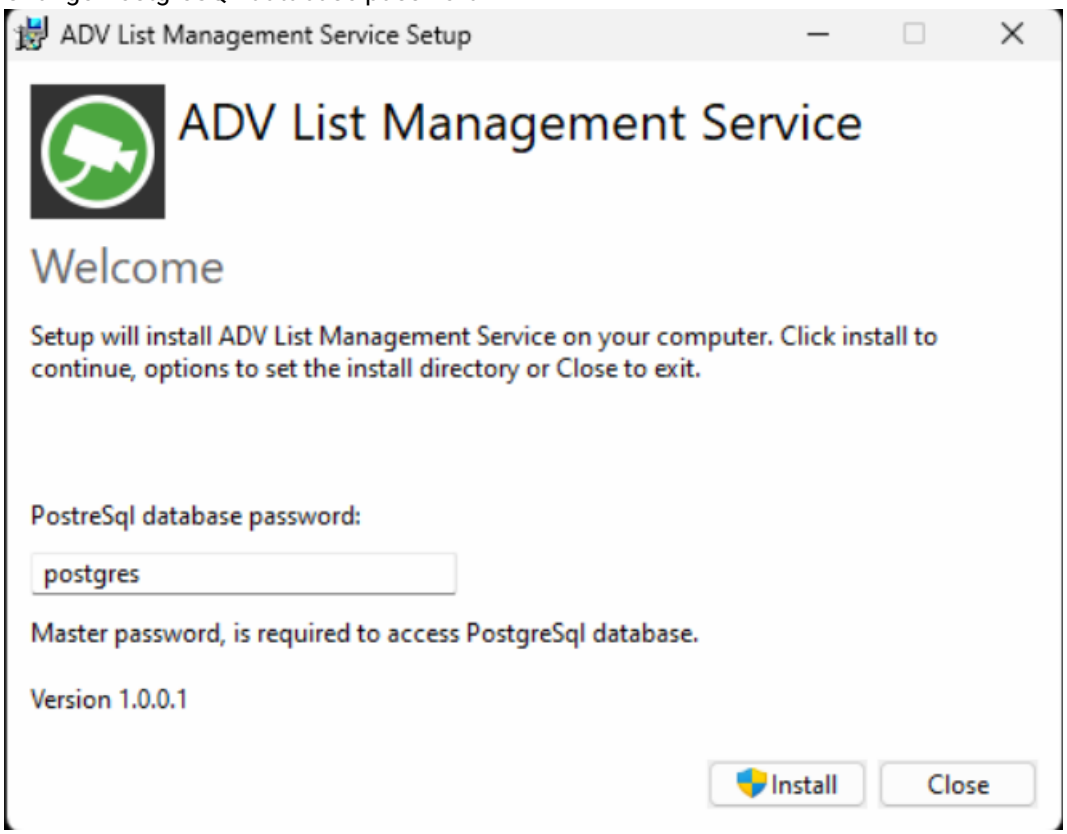
#### 15.1.2.1 Requirements

- Administrator rights
- List Management Service feature is included on V9.6.0.

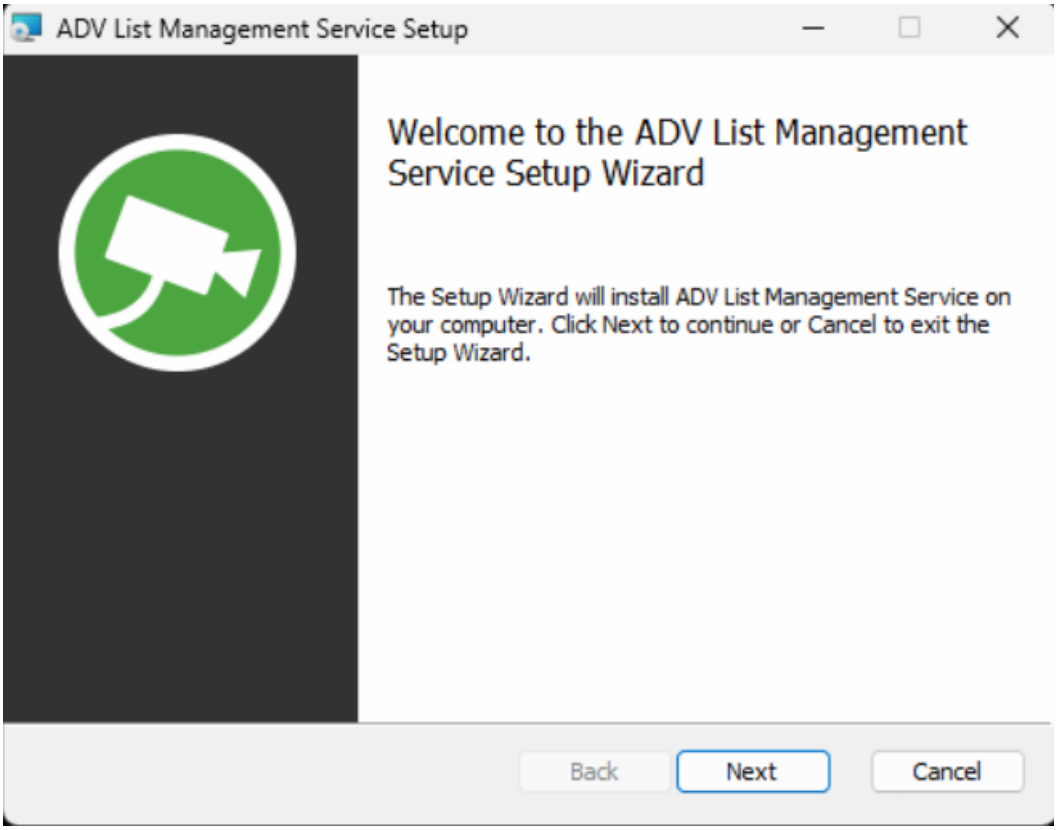
#### 15.1.2.2 Installation

1. Download latest version from Extranet.
2. Unzip this example to C:\temp folder.
3. Start installation double clicking installation file.

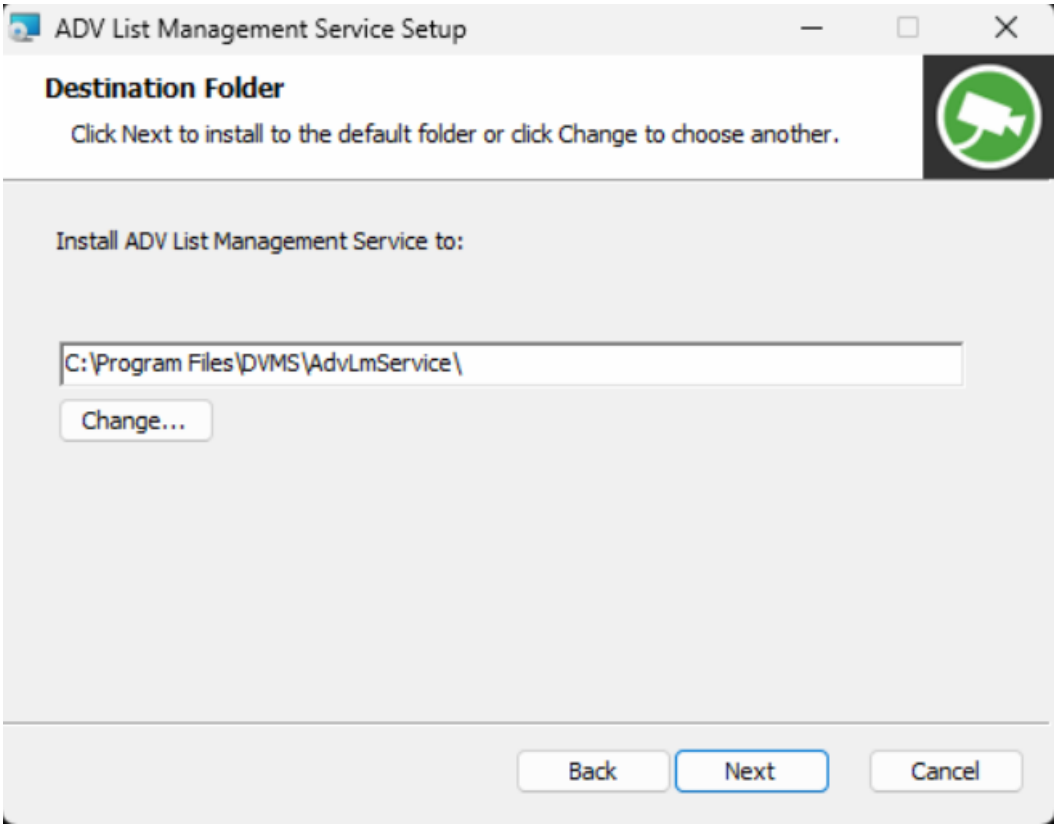
4. Click Install to continue.
    a. Change PostgreSQL database password



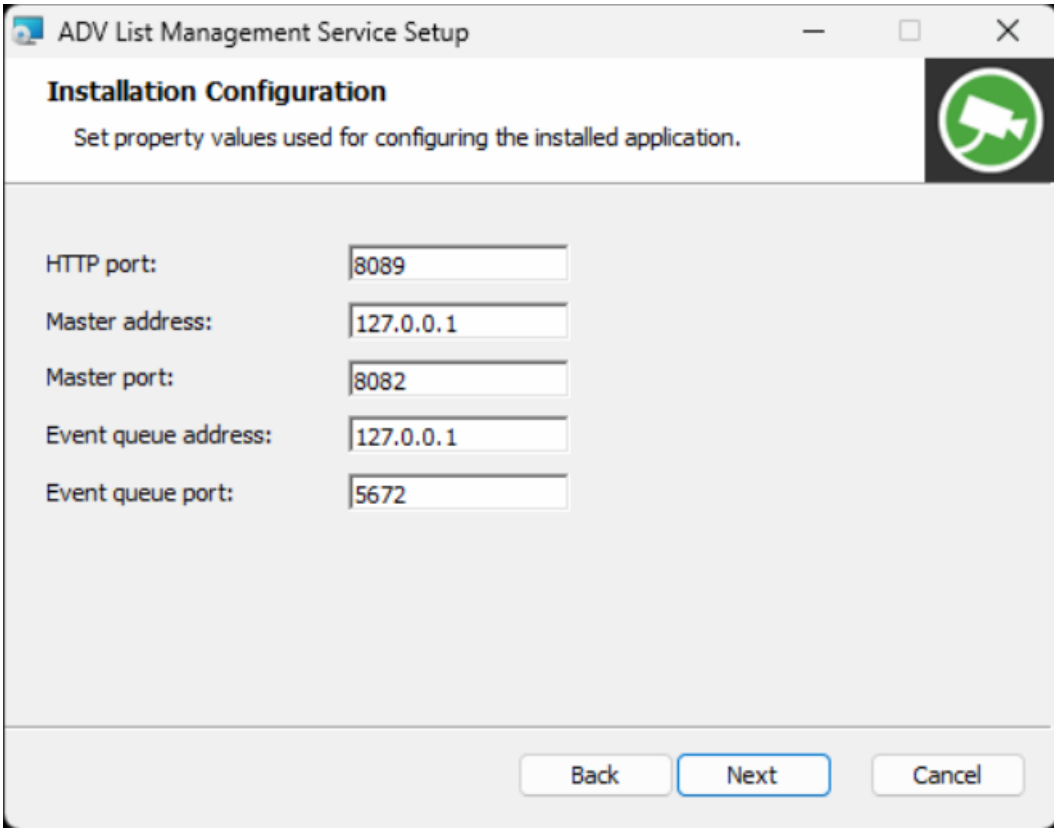

5. Wait that PostgreSQL is installed.
    a. You made need to apply firewall rules when installation is going forward.
6. Click Next to continue.



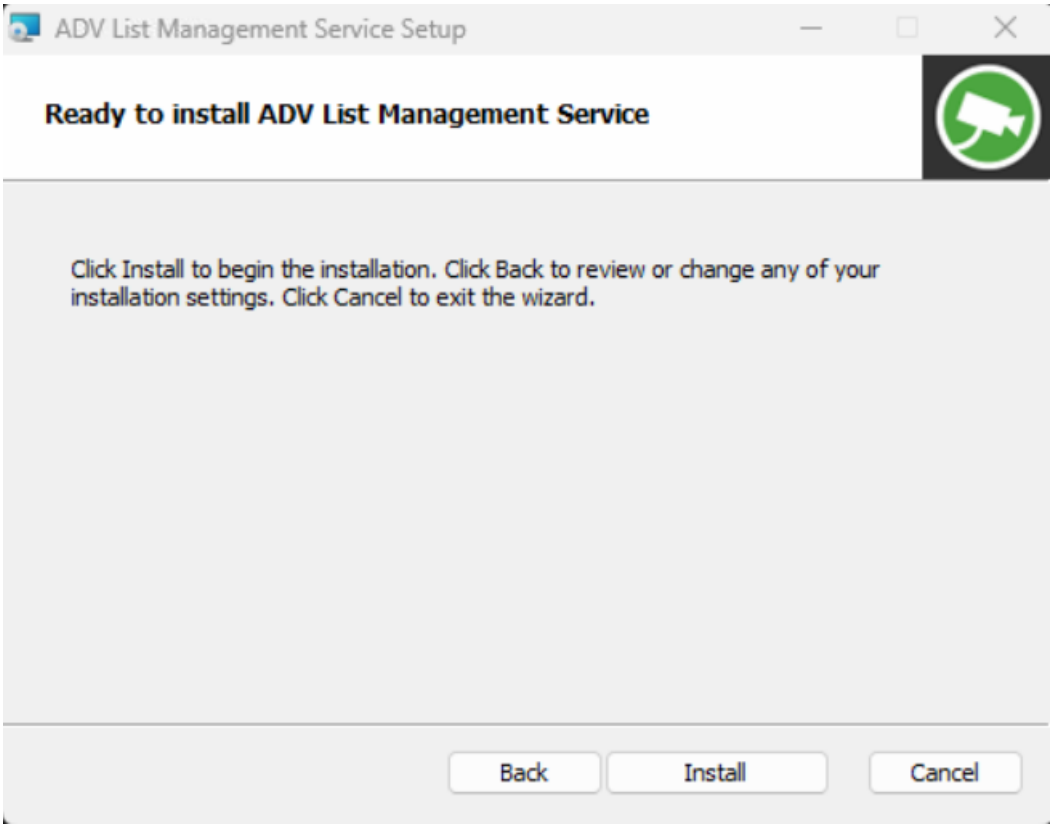

7. Change installation location if needed, if not then click Next to continue.



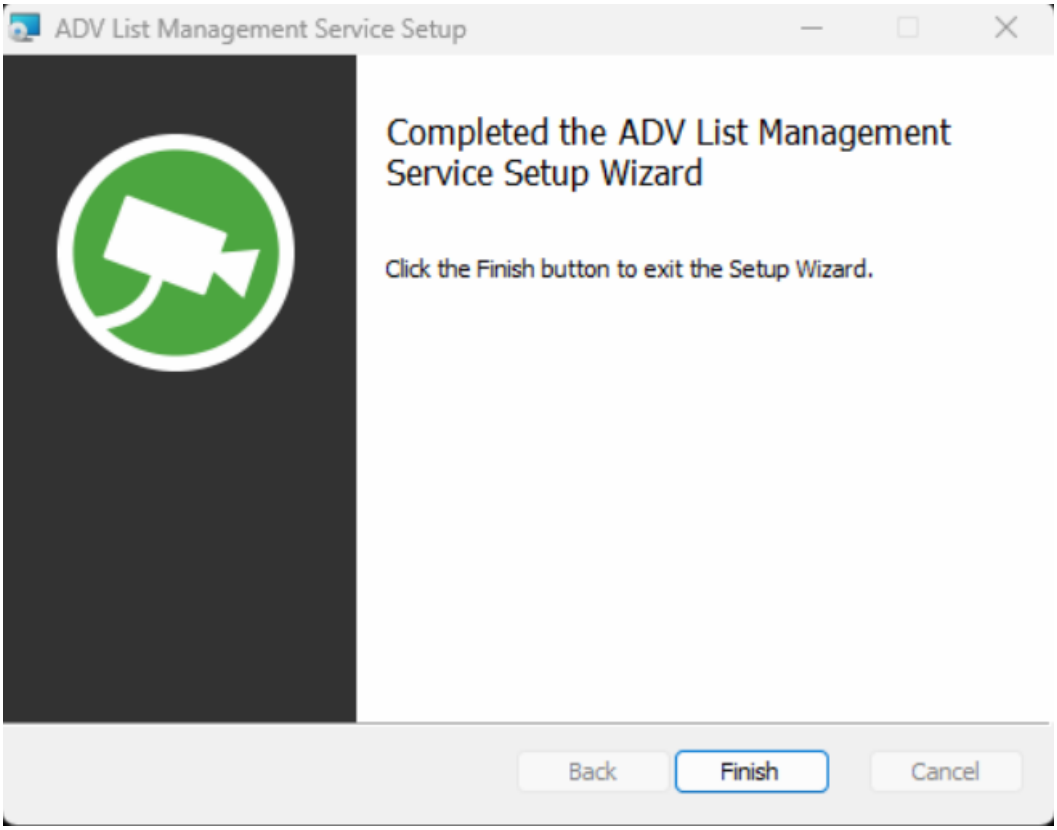

8. Change ports and addresses if needed.
    a. If you are installing List Management Service on other server, then you need to change this.
    b. Event queue address is same address where List Management Service is installed. Keep this as default.
9. Click Next to continue.



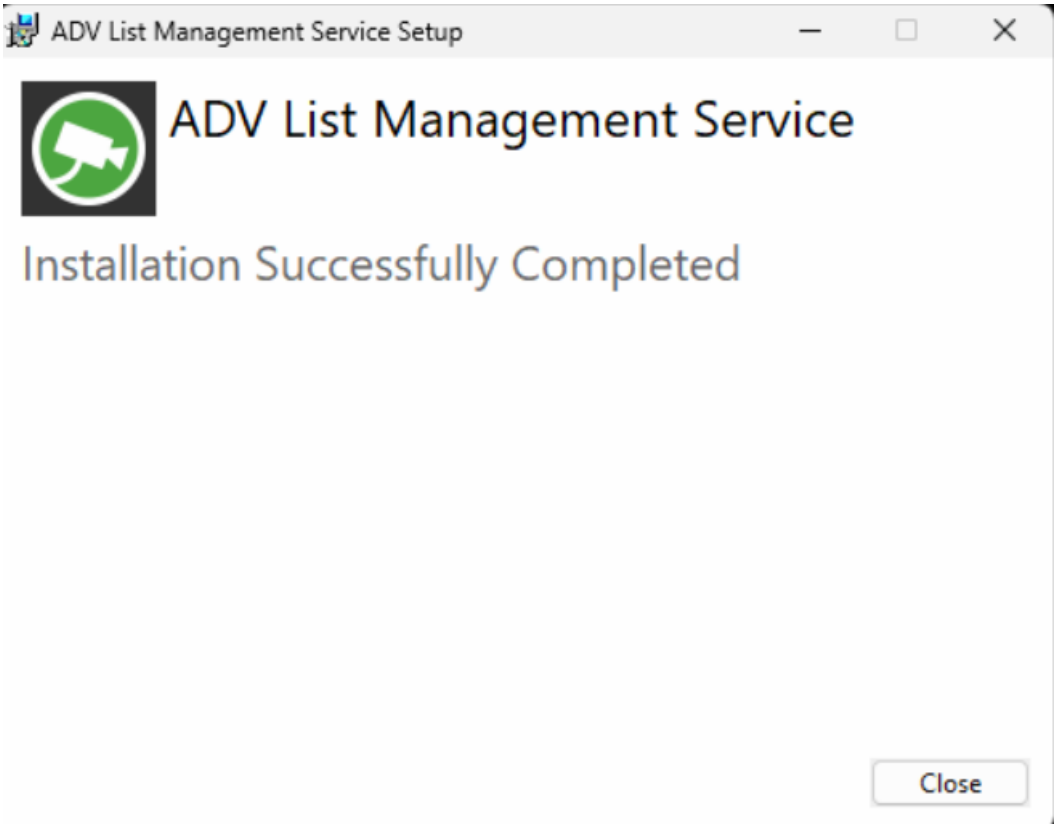

10. Click Install to continue.




11. Wait that installation is finished.
    a. You made need to apply firewall rules when installation is going forward.
    b. Installer install RabbitMQ Server which handle events from List Management Service, Face Recognition Service and License Plate Recognition Service.
    c. Default port 5672 TCP.
12. Click Finish to end installation.




13. Click Close to close installation.




14. Now List Management Service is installed to server and ready to use.
    a. List Management Service send details to VMS Master server and you can configure service via System Manager.

## 15.2 Mirasys Face Recognition (FR)

### 15.2.1 Face Recognition Introduction

Face Recognition (FR) is used to identify a human face. It is used in the VMS System to get events when faces are detected from selected video streams and to detect when specific persons are seen in the video. Together with the Mirasys List Management, this allows you to, for example, create an automatic detection system of a person's access to the premises.

> ⚠ Note that anti-spoofing is **not** included in version 9.6.

The FR service receives video streams, processes images, detects faces, and sends notifications with detection data to List Management (LM) service for identity and list matching.

Face Recognition service has a separate installer, so it can execute on a separate server or on some VMS server.

Face recognition works with 112 x 112 image size. If the face is larger in the picture, it is first reduced to 112 x 112 assembled before identification is made. Likewise, if the face is smaller in the picture, it is first enlarged to that 112 x112 to size. The recommended size of the face in the image is at least 112 pixels.

## 15.2.2 FR Service Installation

> Smart services can be used together with the VCA Deep Learning feature. In this case, you should note that you are using the latest NVIDIA drivers, and not the ones that come with the CUDA Toolkit package. More information can be found here[5].

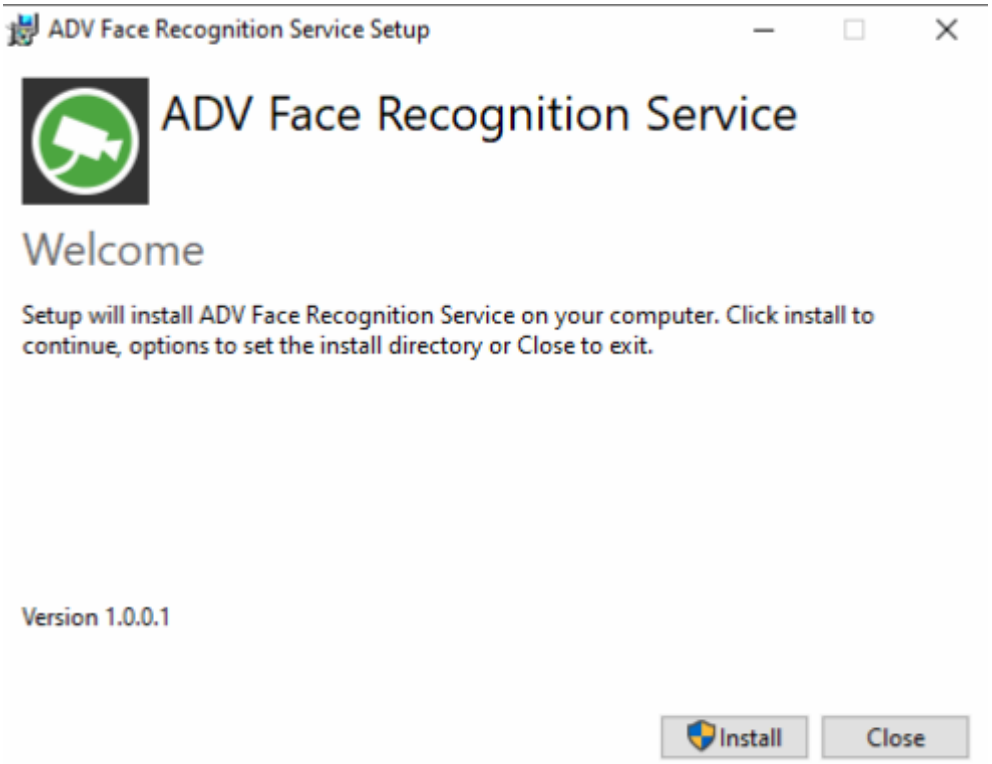
### 15.2.2.1 Requirements

- Administrator rights
- List Management Service installed
- Face Recognition license on VMS server

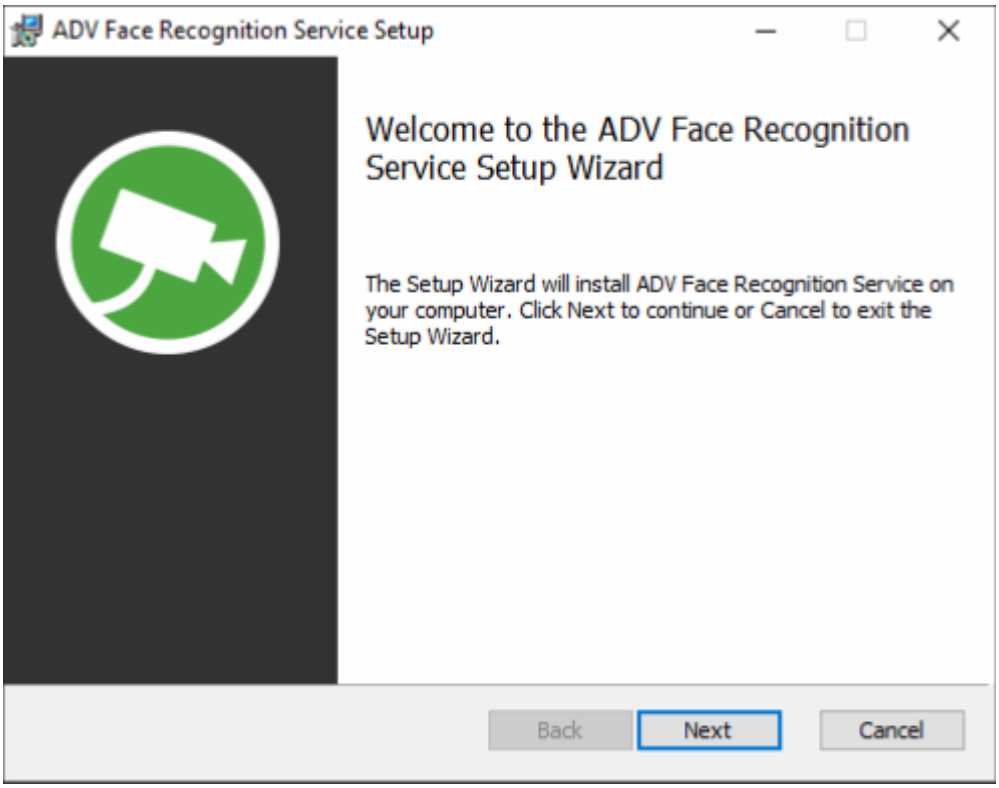
### 15.2.2.2 Installation

1. Download latest version from Extranet.
2. Unzip this example to C:\temp folder.
3. Start installation double clicking installation file.
4. Click Install to continue.

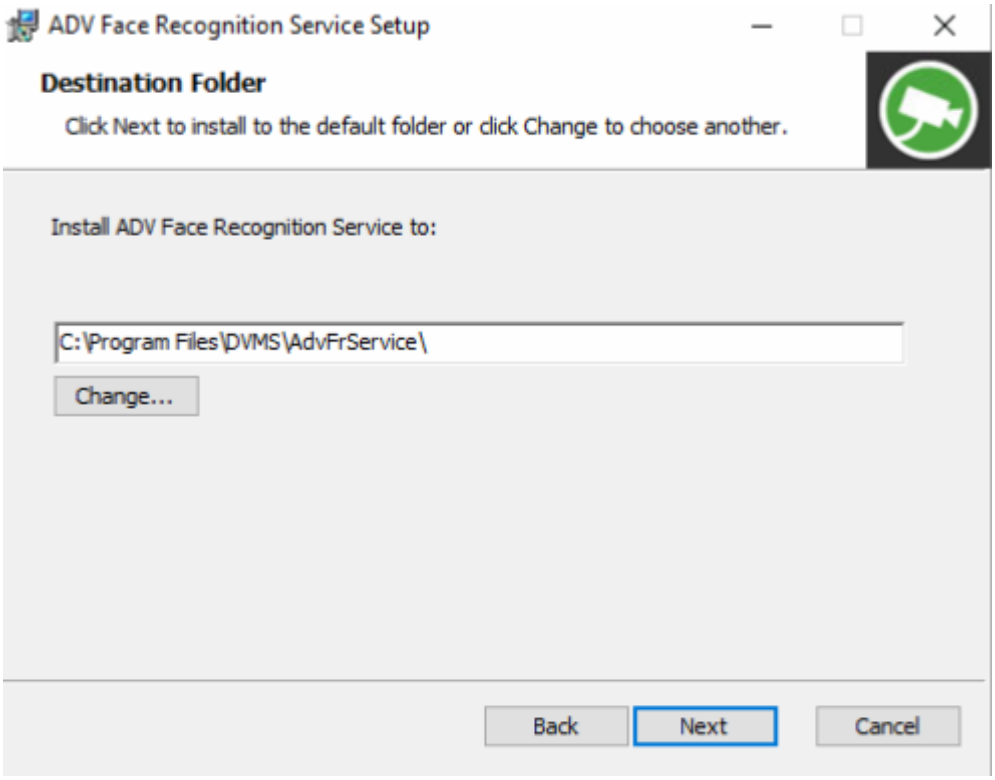
5 https://documentation.mirasys.com/frequently-asked-questions/faq/how-to-install-nvidia-cuda-toolkit



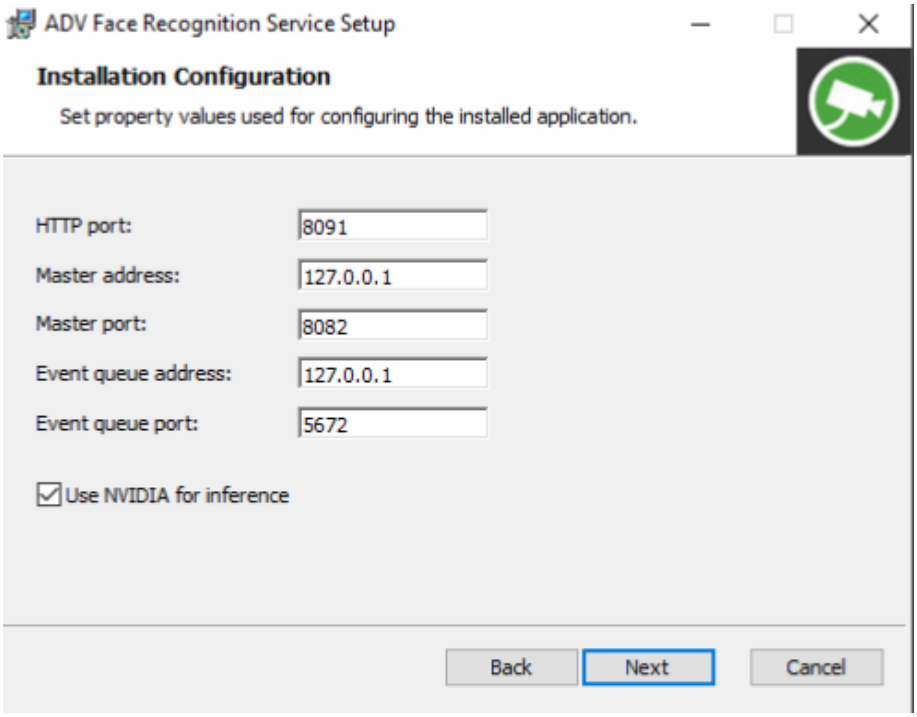

5. Click Next to continue.




6. Change installation location if needed, if not then click Next to continue.

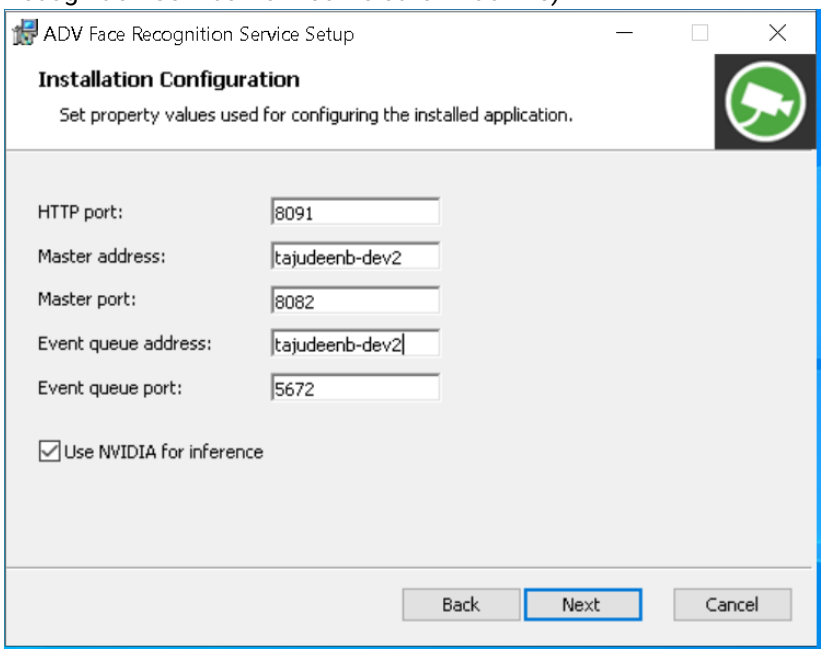



7. Change ports and addresses if needed.
    a. If you example install Face Recognition service to other machine than VMS Master, you need change Master address to correct one.
    b. Same apply for Event queue address. Replace this address with that server address where List Management Service is installed.
    c. If you have Nvidia graphics card installed to server, you can keep Use NVIDIA for inference enabled. This create Nvidia models to use graphics card.
8. Click Next to continue.




14 FR Installed on local machine

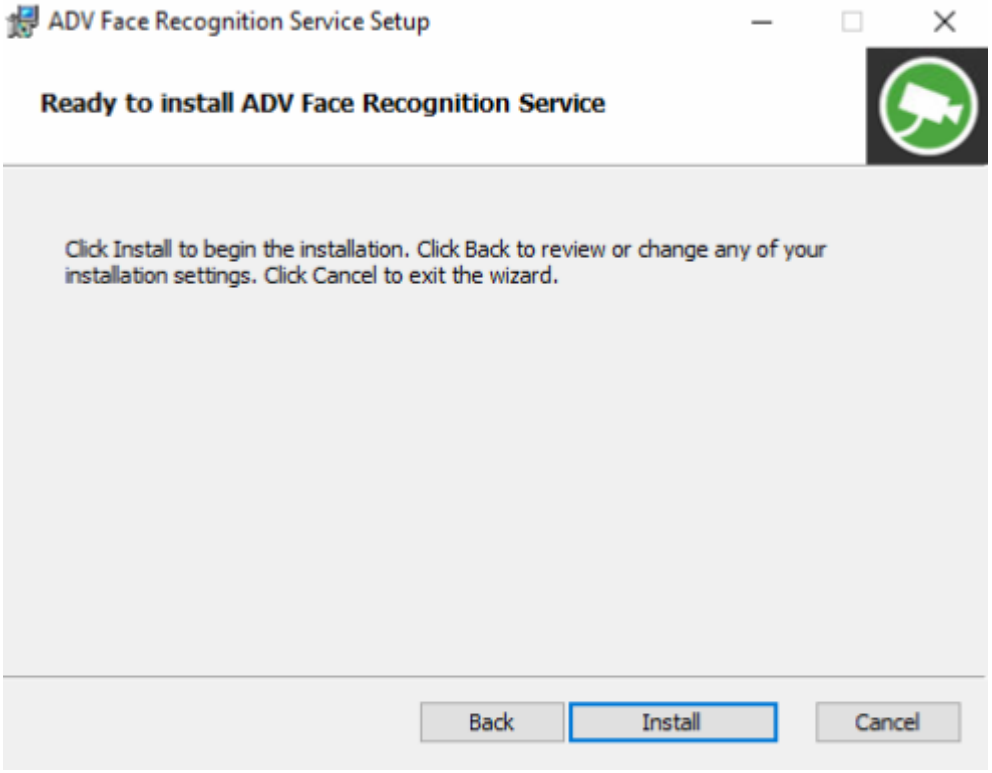
a. If Face Recognition Service is installed on other machine specifying the name or IP address of the machine using the Face Recognition Service (in this case, tajudeenb-dev2 is using Face Recognition Service from some other machine)



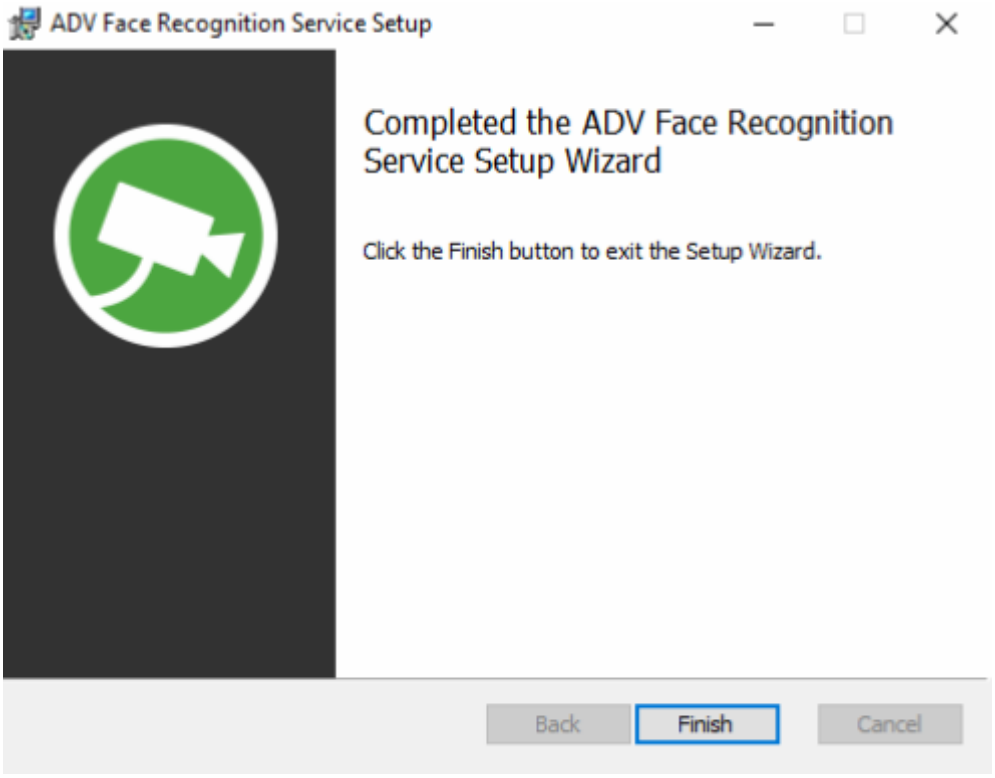

15 FR Installed on other machine

9. Click Install to continue and wait.

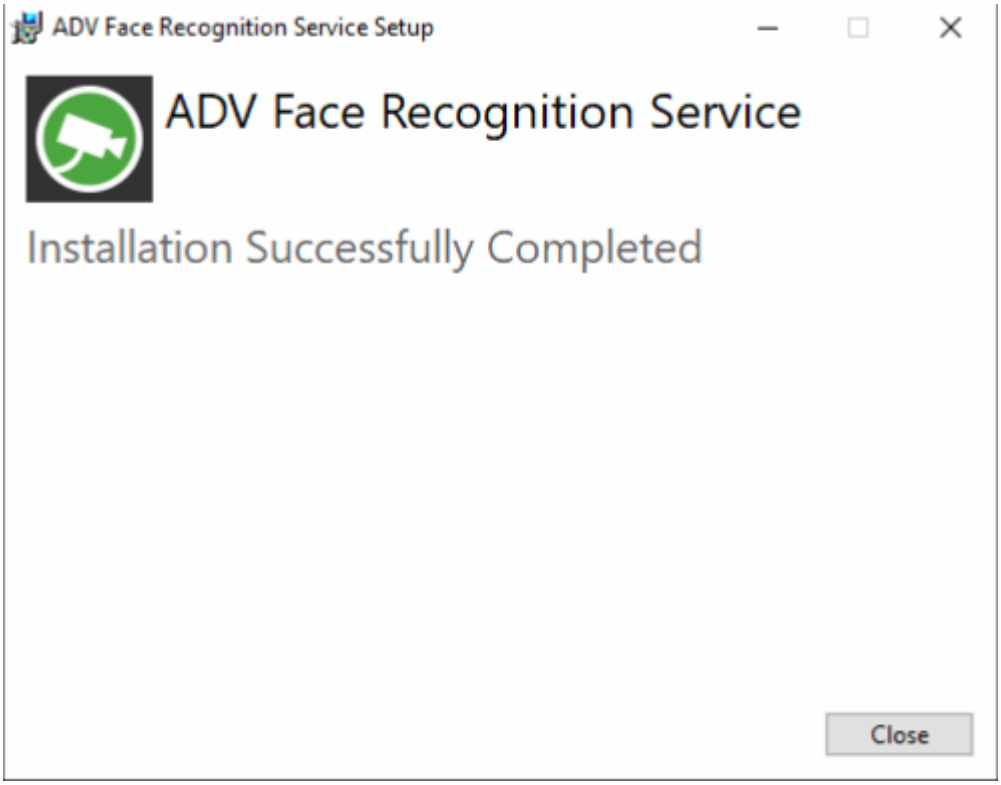
10. Installation will take some times until it finished.
11. Models creation can take up to 30 minutes. This depends how powerful graphics card is in use.




12. Click Finish to continue.




13. Click Close to close installation.




14. Now Face Recognition Service is installed to server and ready to use.

a. Face Recognition Service send details to VMS Master server and you can configure service via System Manager.

### 15.2.3 FR Privacy masks

#### 15.2.3.1 Privacy masks

If any client privacy masks are defined for the camera, the FR service draws privacy masks to input images before inference.

- No face can be detected inside the privacy zone.
- Thumbnail images have privacy zones.

### 15.2.4 FR processing, events, and detection

#### 15.2.4.1 Devices

Face recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

#### 15.2.4.2 FR events

Live FR events are shown in the Smart Recognition plugin in Spotter. FR events can be searched using the Smart Search plugin in Spotter.

#### 15.2.4.3 Detected face visualization

Detected faces can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

### 15.2.5 FR Alarm triggers and configuration

#### 15.2.5.1 Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

#### 15.2.5.2 FR configuration

FR service can be configured in the System Manager application on the FR settings tab in the **Camera Settings** window.

The FR settings contain information about camera video streams processed by the service. Each stream setting is related to the camera and stream on the recorder. Each FR service can have its own set of limits.

## 15.2.6 FR Performance

### 15.2.6.1 Test machine

- 12th Gen Intel(R) Core(TM) i9-12900KF 3.19 GHz
- NVIDIA GeForce RTX 3080 Ti
- Intel UHD Graphics 750

### 15.2.6.2 How test is done

- FR service is restarted before starting to do test.
    - This free memory from test machine.
- HW video decoding used.
- Best FPS value is marked as orange.
    - This is best value without frame skipping.

### 15.2.6.3 Test results

#### 15.2.6.3.1 CPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | 21 | 15 % | | 3 % | | 2.8 GB |
| 2 | 640 x 480 | 42 | 42 | 27 % | | 6 % | | 3.1 GB |
| 3 | 640 x 480 | 63 | 63 | 46 % | | 8 % | | 3.5 GB |
| 4 | 640 x 480 | 84 | **83** | 53 % | | 11 % | | 3.9 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 5 | 640 x 480 | 105 | 85 | 50 % | | 11 % | | 4.2 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | Process memory |
|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | 21 | 16 % | | 9 % | 2.5 GB |
| 2 | 1920 x 1080 | 42 | 42 | 36 % | | 18 % | 3.1 GB |
| 3 | 1920 x 1080 | 63 | **63** | 51 % | | 27 % | 3.4 GB |
| 4 | 1920 x 1080 | 80 | 80 | 62 % | | 33 % | 4.9 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | Process memory |
|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | 21 | 17 % | | 33 % | 2.9 GB |
| 2 | 3840 x 2160 | 42 | 42 | 35 % | | 60 % | 3.7 GB |
| 3 | 3840 x 2160 | 63 | **63** | 53 % | | 64 % | 4.4 GB |
| 4 | 3840 x 2160 | 80 | 80 | 70 % | | 60 % | 9.2 GB |

#### 15.2.6.3.2 NVIDIA GPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | 21 | 2 % | 25 % | 3 % | | 2.4 GB |
| 2 | 640 x 480 | 42 | 42 | 4 % | 30 % | 5 % | | 2.6 GB |
| 3 | 640 x 480 | 63 | 63 | 4 % | 30 % | 5 % | | 2.8 GB |
| 4 | 640 x 480 | 84 | 84 | 4 % | 30 % | 5 % | | 3.0 GB |
| 5 | 640 x 480 | 105 | 105 | 5 % | 30 % | 7 % | | 3.2 GB |
| 6 | 640 x 480 | 126 | 126 | 6 % | 35 % | 8 % | | 3.3 GB |
| 7 | 640 x 480 | 147 | 147 | 7 % | 38 % | 9 % | | 3.4 GB |
| 8 | 640 x 480 | 168 | 168 | 8 % | 90 % | 9 % | | 3.6 GB |
| 9 | 640 x 480 | 189 | 189 | 8 % | 96 % | 9 % | | 3.7 GB |
| 10 | 640 x 480 | 210 | 210 | 11 % | 96 % | 9 % | | 3.8 GB |
| 11 | 640 x 480 | 231 | 231 | 11 % | 96 % | 9 % | | 3.9 GB |
| 12 | 640 x 480 | 252 | **252** | 14 % | 96 % | 10 % | | 4.0 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 13 | 640 x 480 | 273 | 243 | 15 % | 92 % | 10 % | | 4.8 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | 21 | 4 % | 25 % | 9 % | | 2.4 GB |
| 2 | 1920 x 1080 | 42 | 42 | 3 % | 28 % | 15 % | | 2.7 GB |
| 3 | 1920 x 1080 | 63 | 63 | 5 % | 28 % | 14 % | | 2.9 GB |
| 4 | 1920 x 1080 | 84 | 84 | 6 % | 30 % | 17 % | | 3.2 GB |
| 5 | 1920 x 1080 | 105 | 105 | 7 % | 35 % | 22 % | | 3.3 GB |
| 6 | 1920 x 1080 | 126 | 126 | 10 % | 35 % | 24 % | | 3.6 GB |
| 7 | 1920 x 1080 | 147 | 147 | 11 % | 95 % | 25 % | | 3.7 GB |
| 8 | 1920 x 1080 | 168 | 168 | 13 % | 95 % | 25 % | | 3.9 GB |
| 9 | 1920 x 1080 | 189 | 189 | 17 % | 95 % | 25 % | | 4.0 GB |
| 10 | 1920 x 1080 | 210 | 210 | 19 % | 95 % | 28 % | | 4.2 GB |
| 11 | 1920 x 1080 | 231 | 231 | 22 % | 95 % | 31 % | | 4.4 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 12 | 1920 x 1080 | 252 | **252** | 26 % | 95 % | 34 % | | 5.6 GB |
| 13 | 1920 x 1080 | 249 | 249 | 29 % | 93 % | 33 % | | 6.5 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | 21 | 3 % | 32 % | 32 % | | 2.7 GB |
| 2 | 3840 x 2160 | 42 | 42 | 7 % | 37 % | 37 % | | 3.1 GB |
| 3 | 3840 x 2160 | 63 | 63 | 10 % | 44 % | 44 % | | 3.5 GB |
| 4 | 3840 x 2160 | 84 | 84 | 13 % | 60 % | 60 % | | 3.8 GB |
| 5 | 3840 x 2160 | 105 | 105 | 21 % | 95 % | 60 % | | 4.2 GB |
| 6 | 3840 x 2160 | 126 | 126 | 22 % | 95 % | 61 % | | 4.5 GB |
| 7 | 3840 x 2160 | 147 | 147 | 28 % | 97 % | 71 % | | 4.8 GB |
| 8 | 3840 x 2160 | 168 | 168 | 30 % | 96 % | 81 % | | 5.1 GB |
| 9 | 3840 x 2160 | 189 | 189 | 35 % | 95 % | 91 % | | 5.9 GB |
| 10 | 3840 x 2160 | 210 | **210** | 37 % | 100 % | 100 % | | 14.7 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 11 | 3840 x 2160 | 209 | 209 | 40 % | 100 % | 100 % | | 14.9 GB |

#### 15.2.6.3.3 INTEL GPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | **21** | 7 % | | 3 % | 52 % | 1.8 GB |
| 2 | 640 x 480 | 40 | 40 | 20 % | | 7 % | 100 % | 2.6 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | **21** | 8 % | | 5 % | 55 % | 1.8 GB1 |
| 2 | 1920 x 1080 | 39 | 39 | 22 % | | 15 % | 99 % | 3.2 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | **21** | 10 % | | 30 % | 55 % | 2.0 GB |
| 2 | 3840 x 2160 | 39 | 39 | 27 % | | 60 % | 98 % | 5.2 GB |

These tests are indicative and may not be directly applicable to production systems.

# 15.3 Mirasys License Plate Recognition (LPR)

## 15.3.1 License Plate Recognition Introduction

License Plate Recognition (LPR) is used to identify a car using its license plate. It is used in the VMS System to get events when license plates are detected from selected video streams and to detect when specific cars are seen in the video. Together with the Mirasys List Management, this allows you to, for example, create an automatic detection system of cars' access to the parking hall.

The LPR service receives video streams, processes images, detects license plates, and sends notifications with detection data to List Management (LM) service for identity and list matching.

License Plate Recognition service has a separate installer, so it can execute on a separate server or on some VMS server.

## 15.3.2 LPR Service Installation

Smart services can be used together with the VCA Deep Learning feature. In this case, you should note that you are using the latest NVIDIA drivers, and not the ones that come with the CUDA Toolkit package. More information can be found here[6].

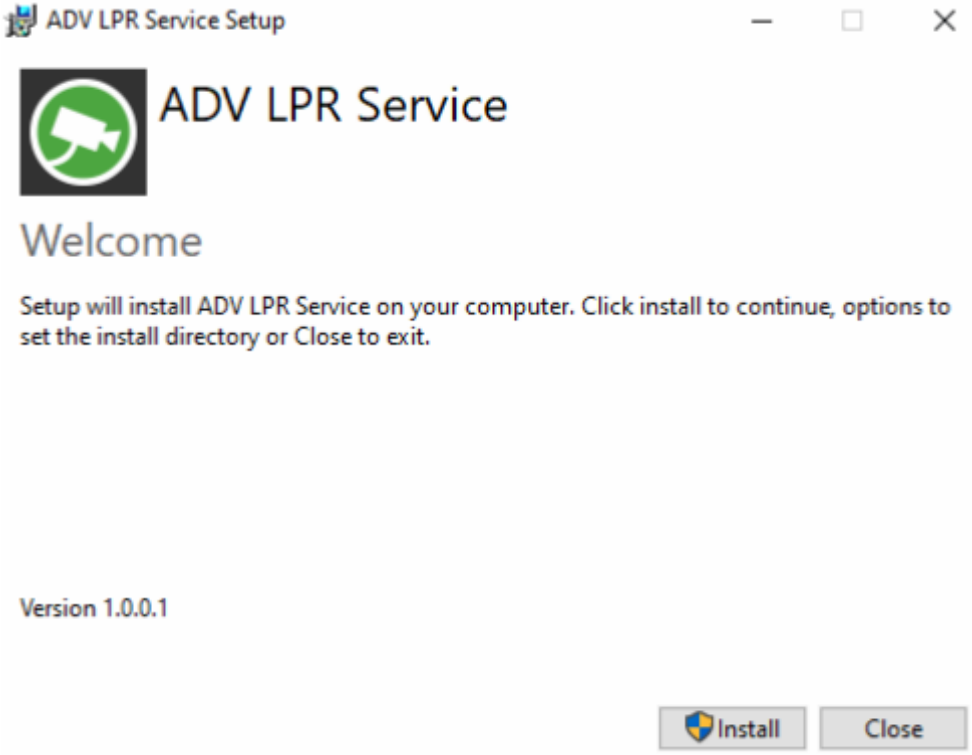
### 15.3.2.1 Requirements

- Administrator rights
- List Management Service installed
- License Plate Recognition license on VMS server

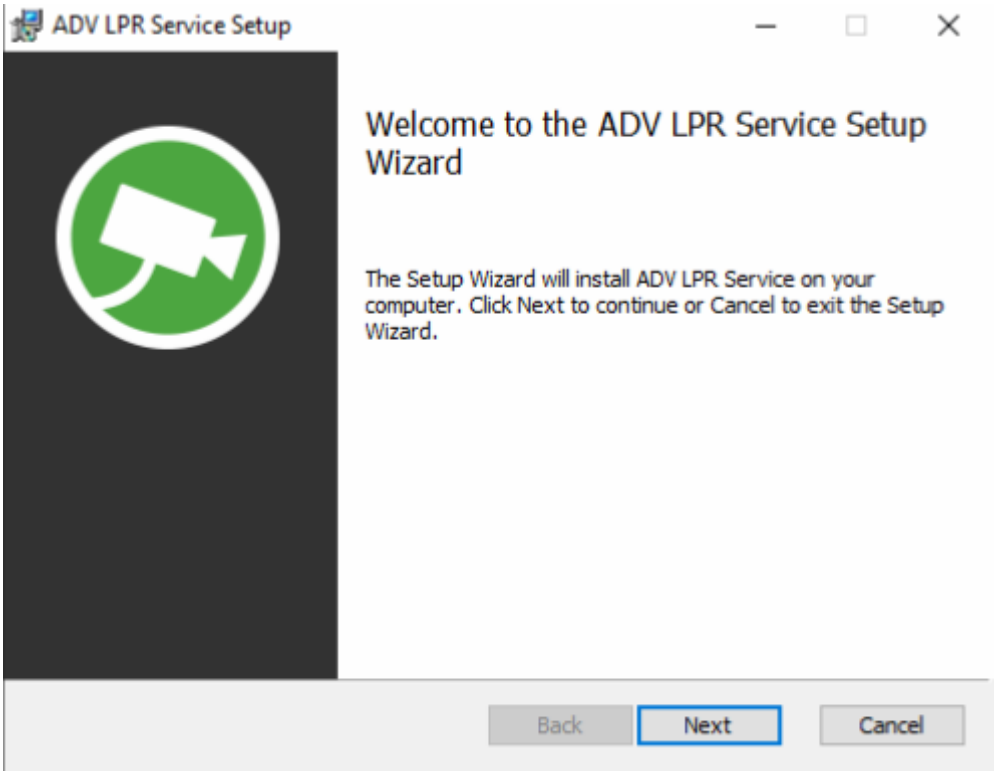
### 15.3.2.2 Installation

1. Download latest version from Extranet.
2. Unzip this example to C:\temp folder.
3. Start installation double clicking installation file.
4. Click Install to continue.

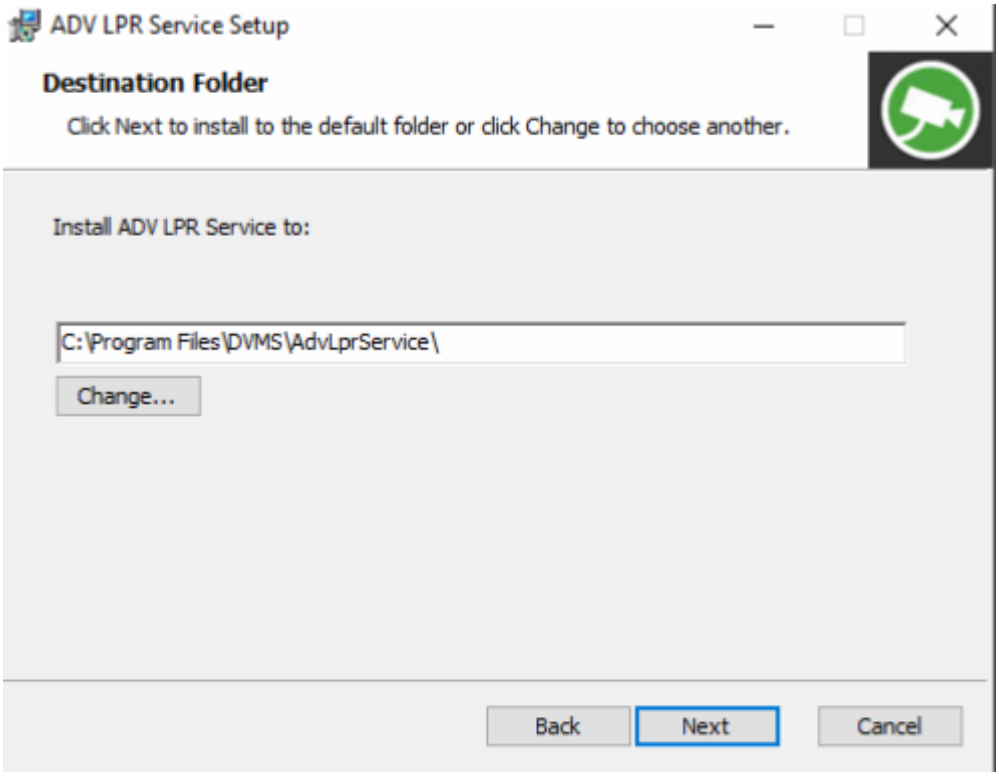
6 https://documentation.mirasys.com/frequently-asked-questions/faq/how-to-install-nvidia-cuda-toolkit



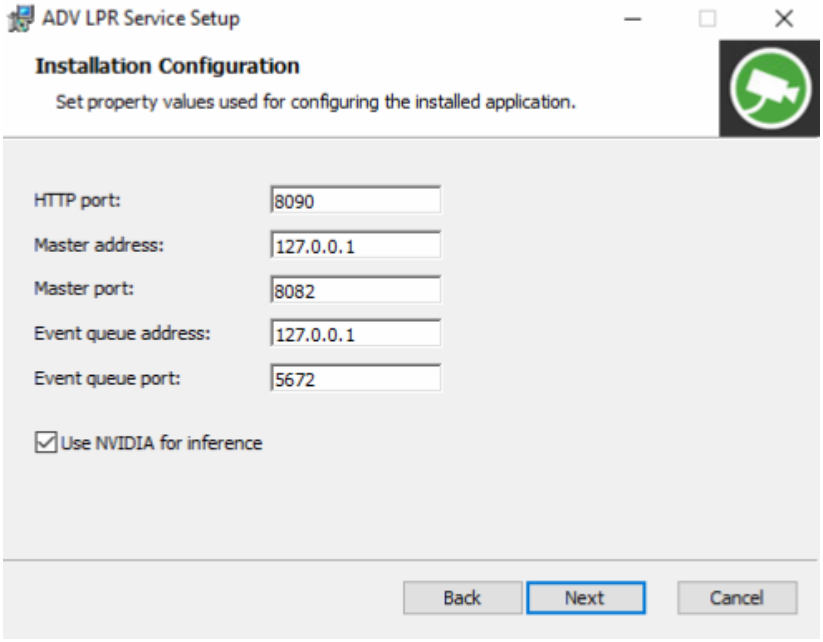

5. Click Next to continue.




6. Change installation location if needed, if not then click Next to continue.

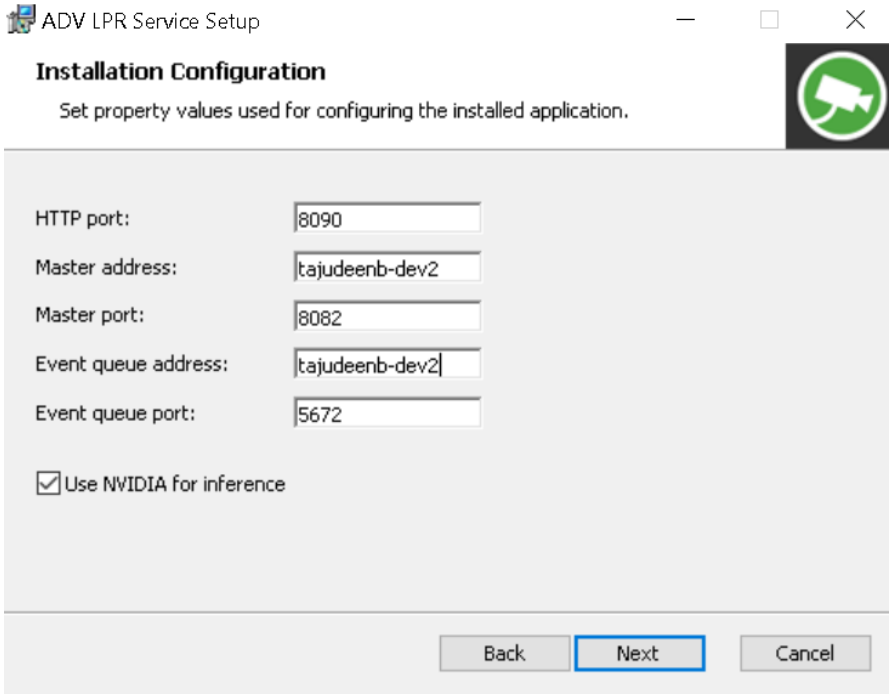



7. Change ports and addresses if needed.
    a. If you example install Face Recognition service to other machine than VMS Master, you need change Master address to correct one.
    b. Same apply for Event queue address. Replace this address with that server address where List Management Service is installed.
    c. If you have Nvidia graphics card installed to server, you can keep Use NVIDIA for inference enabled. This create Nvidia models to use graphics card.
8. Click Next to continue.




16 LPR Installed on local machine

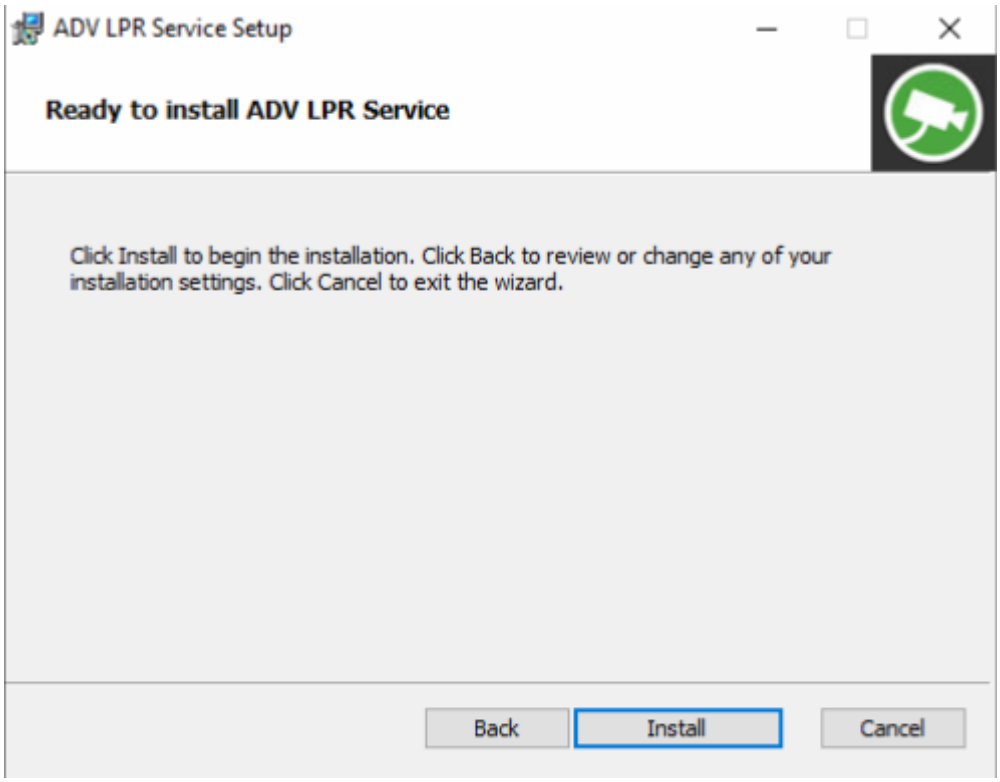
a. If License Plate Recognition Service is installed on some other machine specifying the machine name or IP address using the service (in this case, tajudeenb-dev2 is using License Plate Recognition Service from some other machine)



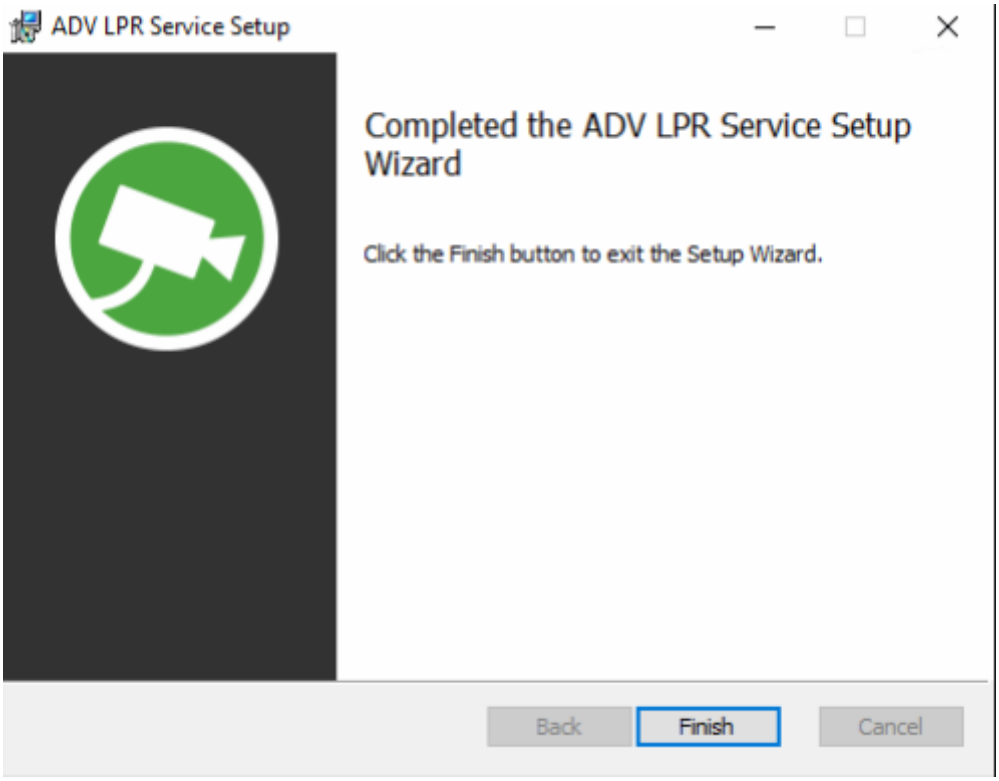

17 LPR service installed on some other machine

9. Click Install to continue and wait.
   a. Installation will take some times until it finished.

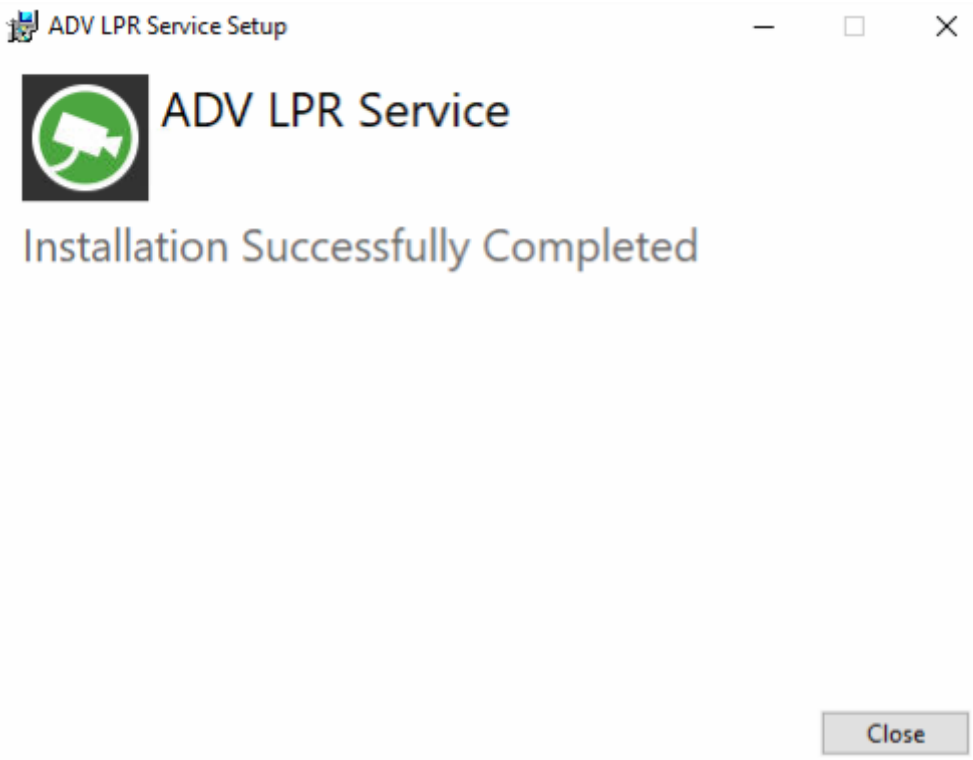
b. Models creation can take up to 30 minutes. This depends how powerful graphics card is in use.




10. Click Finish to continue.



11. Click Close to close installation.




12. Now License Plate Recognition Service is installed to server and ready to use.
    a. License Plate Recognition Service send details to VMS Master server and you can configure service via System Manager.

### 15.3.3 LPR Privacy masks

If any client privacy masks are defined for the camera, then the LPR service draws privacy masks to input images before doing inference.

- No license plate can be detected inside the privacy zone.
- Thumbnail images have privacy zones.

### 15.3.4 LPR Country Detection

#### 15.3.4.1 Country Detection

Country detection is optional, but in some countries, it is recommended to be used: plate number detection accuracy can be improved when the country is known.

##### 15.3.4.1.1 Plate number country detection

Plate number detection is available for Eurasia (see page 305) and the Americas (see page 307).

Country detection is optional. It is useful in countries like Finland, where the letters I and O are the same as numbers 1 and 0. If the country is recognized with high confidence, then country-specific rules can be used to improve plate number detection accuracy.

#### 15.3.4.1.2 License plate types

If country detection is enabled, then license plate type can sometimes be detected. License plate type can be undefined or one of these:

- antique
- diplomatic
- export
- military
- provisional
- rental
- taxi
- test
- work

## 15.3.5 Supported countries in Eurasia (LPR)

### 15.3.5.1 Area codes

In some countries, license plates have area codes. If country detection is enabled, then also area code is detected for the following countries:

- Austria
- Germany
- Romania
- Slovenia
- Switzerland

In a special case, a region inside a country can be detected. For example, Åland Islands has its own plate styles, different from those used in other parts of Finland.

Please note that accuracy vary from country to country.
A plate from **unsupported** countries could be detected as one of the countries listed below. For example some Tajikistan plates can be detected as Kazakhstan plates.

### 15.3.5.2 List of supported countries in Eurasia

- Albania
- Andorra

- Armenia
- Austria
- Azerbaijan
- Belarus
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland (including Åland Islands)
- France
- Georgia
- Germany
- Gibraltar
- Greece
- Hungary
- Iceland
- Ireland
- Isle of Man
- Italy
- Kazakhstan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Moldova
- Monaco
- Montenegro
- Netherlands
- North Macedonia
- Norway
- Poland
- Portugal
- Romania
- Russia
- San Marino
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden

- Switzerland
- Turkey
- Ukraine
- United Kingdom
- Vatican

### 15.3.6 Supported countries in the Americas (LPR)

> Please note that accuracy vary from country to country.
> A plate from **unsupported** countries could be detected as one of the countries listed below.

#### 15.3.6.1 Countries and states

The countries/states listed below are supported.

- Argentina
- Bolivia
- Brazil (old and new plate styles)
- Canada
    - Alberta
    - British Columbia
    - Manitoba
    - Ontario
    - Quebec
    - Saskatchewan
- Chile
- Colombia
- Mexico
- Paraguay
- Peru
- United States
    - Alabama
    - Alaska
    - Arizona
    - Arkansas
    - California
    - Colorado
    - Connecticut

- Delaware
- District of Columbia
- Florida
- Georgia
- Hawaii
- Idaho
- Illinois
- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas

    - Utah
    - Vermont
    - Virginia
    - Washington
    - West Virginia
    - Wisconsin
    - Wyoming
- Uruguay
- Venezuela

## 15.3.7 LPR processing, events, and detection

### 15.3.7.1 Devices

License plate recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

### 15.3.7.2 LPR events

Live LPR events are shown in the Smart Recognition plugin in Spotter. LPR events can be searched using the Smart Search Plugin in Spotter.

### 15.3.7.3 Detected license plate visualization

Detected license plates can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

## 15.3.8 LPR Alarm triggers and configuration

### 15.3.8.1 Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

### 15.3.8.2 LPR configuration

LPR service can be configured in the System Manager application on the LPR settings tab in the **Camera Settings** window.

The LPR settings contain information about camera video streams processed by the service. Each stream setting is related to the camera and stream on the recorder. Each LPR service can have its own set of limits.

## 15.3.9 LPR Performance

### 15.3.9.1 Test machine

- 12th Gen Intel(R) Core(TM) i9-12900KF 3.19 GHz
- NVIDIA GeForce RTX 3080 Ti
- Intel UHD Graphics 750

### 15.3.9.2 How test is done

- LPR service is restarted before starting to do test.
    - This free memory from test machine.
- HW video decoding used.
- Best FPS value is marked as orange.
    - This is best value without frame skipping.

### 15.3.9.3 Test results

#### 15.3.9.3.1 CPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | 21 | 15 % | | 3 % | | 2.8 GB |
| 2 | 640 x 480 | 42 | 42 | 27 % | | 6 % | | 3.1 GB |
| 3 | 640 x 480 | 63 | 63 | 46 % | | 8 % | | 3.5 GB |
| 4 | 640 x 480 | 84 | **83** | 53 % | | 11 % | | 3.9 GB |
| 5 | 640 x 480 | 105 | 85 | 50 % | | 11 % | | 4.2 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | Process memory |
|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | 21 | 16 % | | 9 % | 2.5 GB |
| 2 | 1920 x 1080 | 42 | 42 | 36 % | | 18 % | 3.1 GB |
| 3 | 1920 x 1080 | 63 | **63** | 51 % | | 27 % | 3.4 GB |
| 4 | 1920 x 1080 | 80 | 80 | 62 % | | 33 % | 4.9 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | Process memory |
|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | 21 | 17 % | | 33 % | 2.9 GB |
| 2 | 3840 x 2160 | 42 | 42 | 35 % | | 60 % | 3.7 GB |
| 3 | 3840 x 2160 | 63 | **63** | 53 % | | 64 % | 4.4 GB |
| 4 | 3840 x 2160 | 80 | 80 | 70 % | | 60 % | 9.2 GB |

#### 15.3.9.3.2 NVIDIA GPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | 21 | 2 % | 25 % | 3 % | | 2.4 GB |
| 2 | 640 x 480 | 42 | 42 | 4 % | 30 % | 5 % | | 2.6 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 3 | 640 x 480 | 63 | 63 | 4 % | 30 % | 5 % | | 2.8 GB |
| 4 | 640 x 480 | 84 | 84 | 4 % | 30 % | 5 % | | 3.0 GB |
| 5 | 640 x 480 | 105 | 105 | 5 % | 30 % | 7 % | | 3.2 GB |
| 6 | 640 x 480 | 126 | 126 | 6 % | 35 % | 8 % | | 3.3 GB |
| 7 | 640 x 480 | 147 | 147 | 7 % | 38 % | 9 % | | 3.4 GB |
| 8 | 640 x 480 | 168 | 168 | 8 % | 90 % | 9 % | | 3.6 GB |
| 9 | 640 x 480 | 189 | 189 | 8 % | 96 % | 9 % | | 3.7 GB |
| 10 | 640 x 480 | 210 | 210 | 11 % | 96 % | 9 % | | 3.8 GB |
| 11 | 640 x 480 | 231 | 231 | 11 % | 96 % | 9 % | | 3.9 GB |
| 12 | 640 x 480 | 252 | **252** | 14 % | 96 % | 10 % | | 4.0 GB |
| 13 | 640 x 480 | 273 | 243 | 15 % | 92 % | 10 % | | 4.8 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | 21 | 4 % | 25 % | 9 % | | 2.4 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 2 | 1920 x 1080 | 42 | 42 | 3 % | 28 % | 15 % | | 2.7 GB |
| 3 | 1920 x 1080 | 63 | 63 | 5 % | 28 % | 14 % | | 2.9 GB |
| 4 | 1920 x 1080 | 84 | 84 | 6 % | 30 % | 17 % | | 3.2 GB |
| 5 | 1920 x 1080 | 105 | 105 | 7 % | 35 % | 22 % | | 3.3 GB |
| 6 | 1920 x 1080 | 126 | 126 | 10 % | 35 % | 24 % | | 3.6 GB |
| 7 | 1920 x 1080 | 147 | 147 | 11 % | 95 % | 25 % | | 3.7 GB |
| 8 | 1920 x 1080 | 168 | 168 | 13 % | 95 % | 25 % | | 3.9 GB |
| 9 | 1920 x 1080 | 189 | 189 | 17 % | 95 % | 25 % | | 4.0 GB |
| 10 | 1920 x 1080 | 210 | 210 | 19 % | 95 % | 28 % | | 4.2 GB |
| 11 | 1920 x 1080 | 231 | 231 | 22 % | 95 % | 31 % | | 4.4 GB |
| 12 | 1920 x 1080 | 252 | **252** | 26 % | 95 % | 34 % | | 5.6 GB |
| 13 | 1920 x 1080 | 249 | 249 | 29 % | 93 % | 33 % | | 6.5 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | 21 | 3 % | 32 % | 32 % | | 2.7 GB |
| 2 | 3840 x 2160 | 42 | 42 | 7 % | 37 % | 37 % | | 3.1 GB |
| 3 | 3840 x 2160 | 63 | 63 | 10 % | 44 % | 44 % | | 3.5 GB |
| 4 | 3840 x 2160 | 84 | 84 | 13 % | 60 % | 60 % | | 3.8 GB |
| 5 | 3840 x 2160 | 105 | 105 | 21 % | 95 % | 60 % | | 4.2 GB |
| 6 | 3840 x 2160 | 126 | 126 | 22 % | 95 % | 61 % | | 4.5 GB |
| 7 | 3840 x 2160 | 147 | 147 | 28 % | 97 % | 71 % | | 4.8 GB |
| 8 | 3840 x 2160 | 168 | 168 | 30 % | 96 % | 81 % | | 5.1 GB |
| 9 | 3840 x 2160 | 189 | 189 | 35 % | 95 % | 91 % | | 5.9 GB |
| 10 | 3840 x 2160 | 210 | **210** | 37 % | 100 % | 100 % | | 14.7 GB |
| 11 | 3840 x 2160 | 209 | 209 | 40 % | 100 % | 100 % | | 14.9 GB |

#### 15.3.9.3.3 INTEL GPU

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 640 x 480 | 21 | **21** | 7 % | | 3 % | 52 % | 1.8 GB |
| 2 | 640 x 480 | 40 | 40 | 20 % | | 7 % | 100 % | 2.6 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 1920 x 1080 | 21 | **21** | 8 % | | 5 % | 55 % | 1.8 GB1 |
| 2 | 1920 x 1080 | 39 | 39 | 22 % | | 15 % | 99 % | 3.2 GB |

| Streams | Size | Input FPS | Output FPS | Process CPU | NVIDIA GPU | NVIDIA decode | INTEL GPU | Process memory |
|---|---|---|---|---|---|---|---|---|
| 1 | 3840 x 2160 | 21 | **21** | 10 % | | 30 % | 55 % | 2.0 GB |
| 2 | 3840 x 2160 | 39 | 39 | 27 % | | 60 % | 98 % | 5.2 GB |

These tests are indicative and may not be directly applicable to production systems.

## 15.4 Easy LPR Guide

### 15.4.1 EASY LPR main features

- Live monitoring from the one camera at the same time

- Plate number search from the one camera at the same time
- Plate number list Management
    - Black list
    - White list
- Importing and exporting plate number lists
- Uploading plate number list to the cameras
- Digital output controlling based on:
    - Other plate detected
    - Black list plate detected
    - White list plate detected

Please check supported cameras from Supported IP Camera List[7].

### 15.4.2 Easy LPR Configuration process

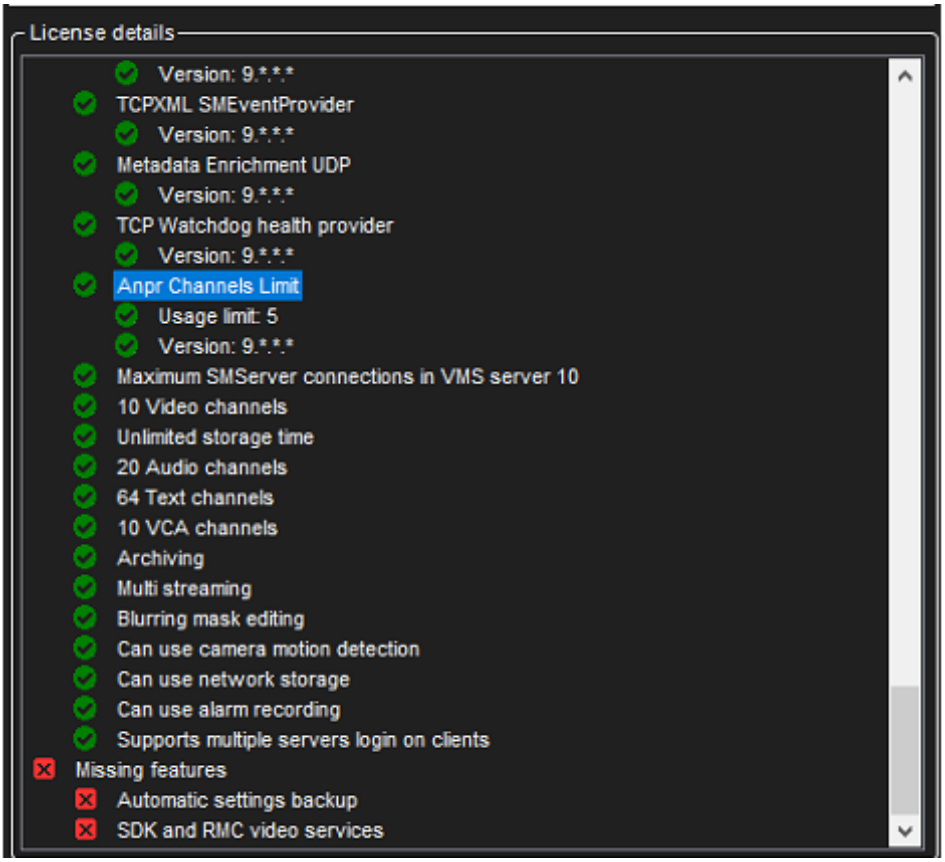
1. Configure LPR functionality to the used cameras. Please see the manufacturer website for more information
2. Check that license plates are correctly detected in the camera side
3. Add cameras to the Mirasys VMS
4. Check that Mirasys VMS license support LPR cameras
5. Enable Easy LPR

### 15.4.3 Easy LPR Licensing

Mirasys VMS server license defines how many ANPR channels can be added.

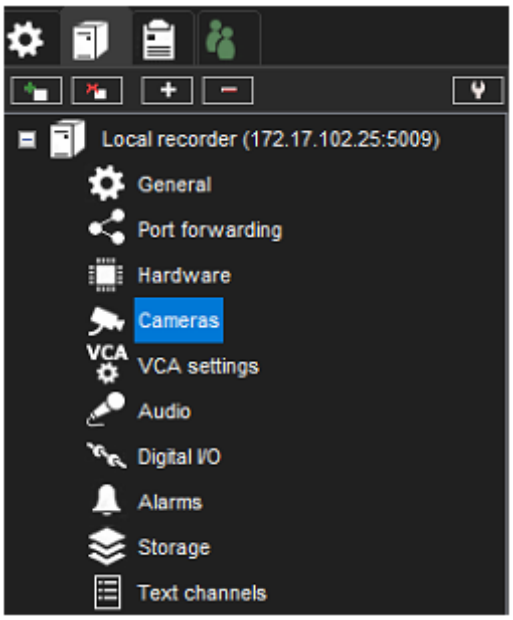
The feature name is **Anpr Channels limit** and controllable value name **Usage limit**

7 https://mirasys.atlassian.net/wiki/spaces/M9/pages/2063728922/Supported+IP+Camera+List

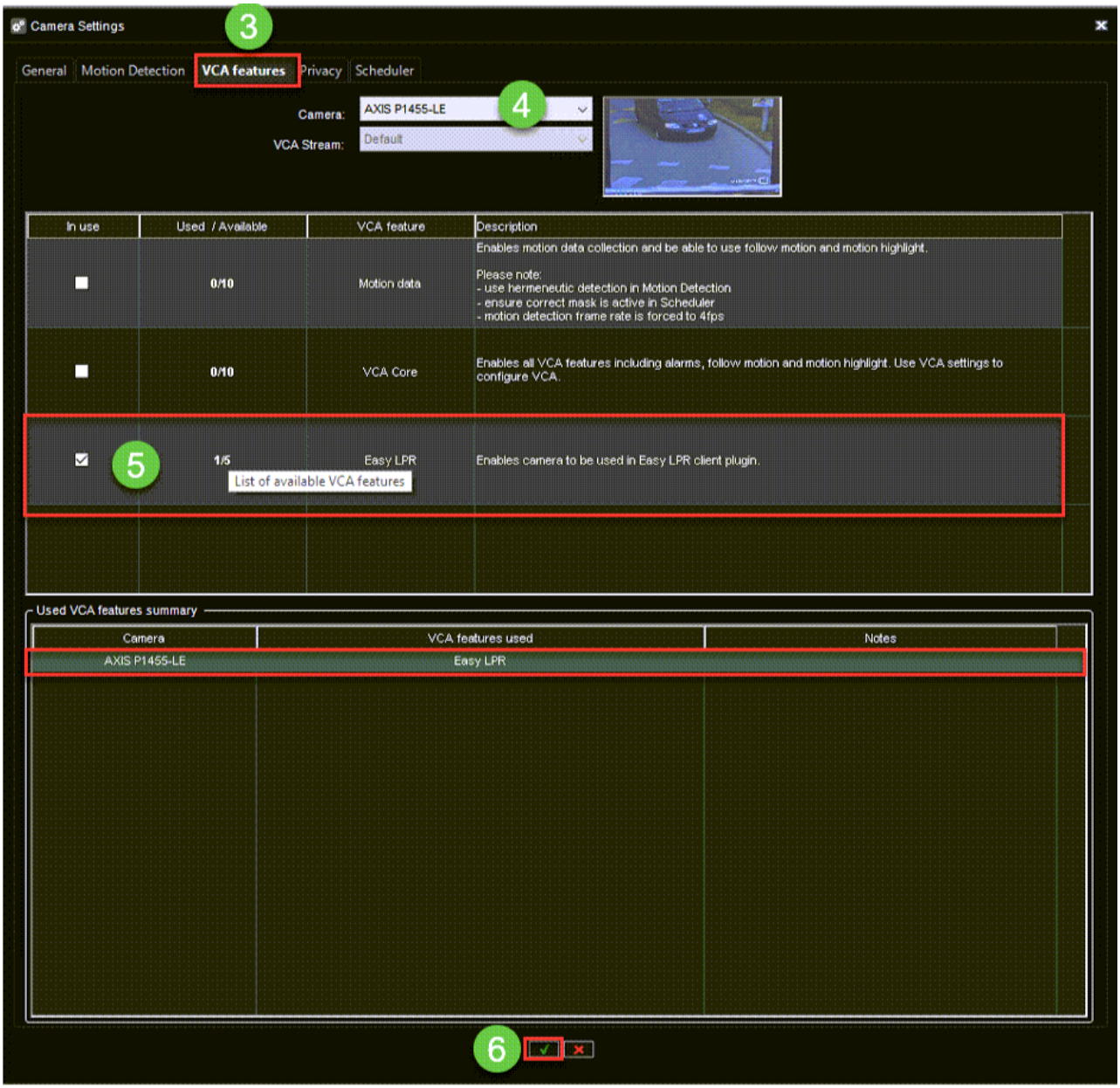



### 15.4.4 How to enable Easy LPR

1. Open **VMS servers**
2. Open **Cameras**

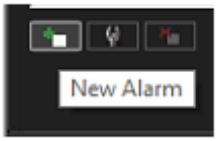



3. Click **VCA features**
4. Select LPR camera
5. Enable **Easy LPR**
6. Click **Save**

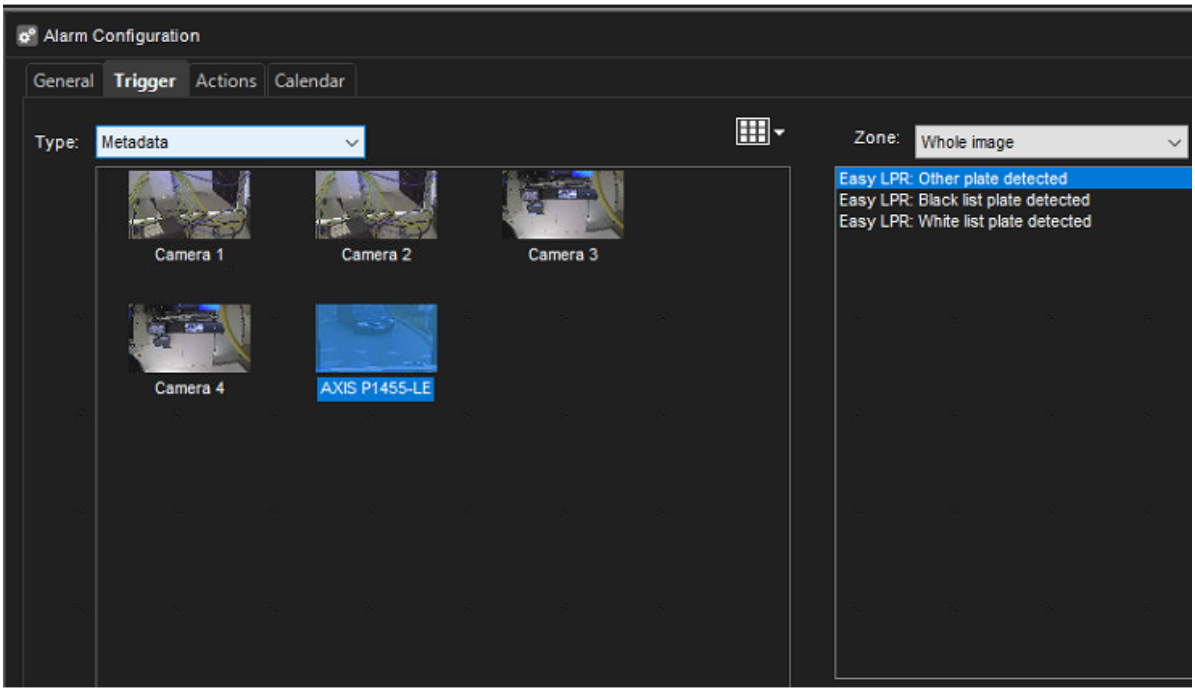



## 15.4.5 Create an alarm from an Easy LPR event

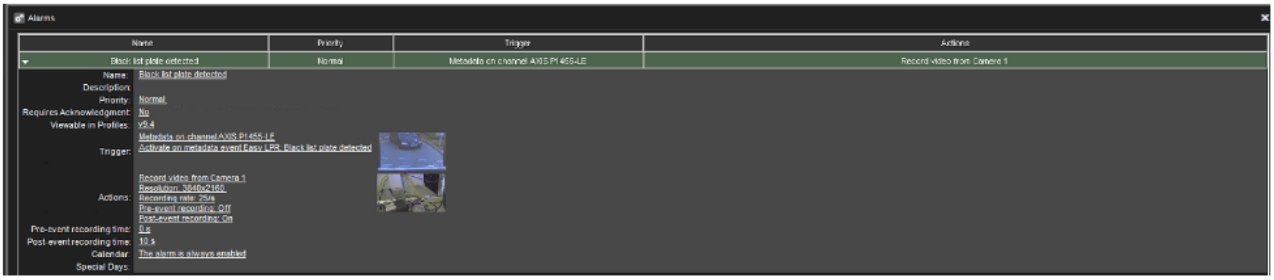
1. Go to the **VMS Servers** tab
2. Open **Alarms**
3. Click **New Alarm**



4. Enter all needed information in the **General** tab
5. Open **Trigger** tab
6. Select trigger type **Metadata**
7. Select LPR camera
8. Select correct event:
    - **Easy LPR: Other plate detected**
    - **Easy LPR: Black list plate detected**
    - **Easy LPR: White list plate detected**



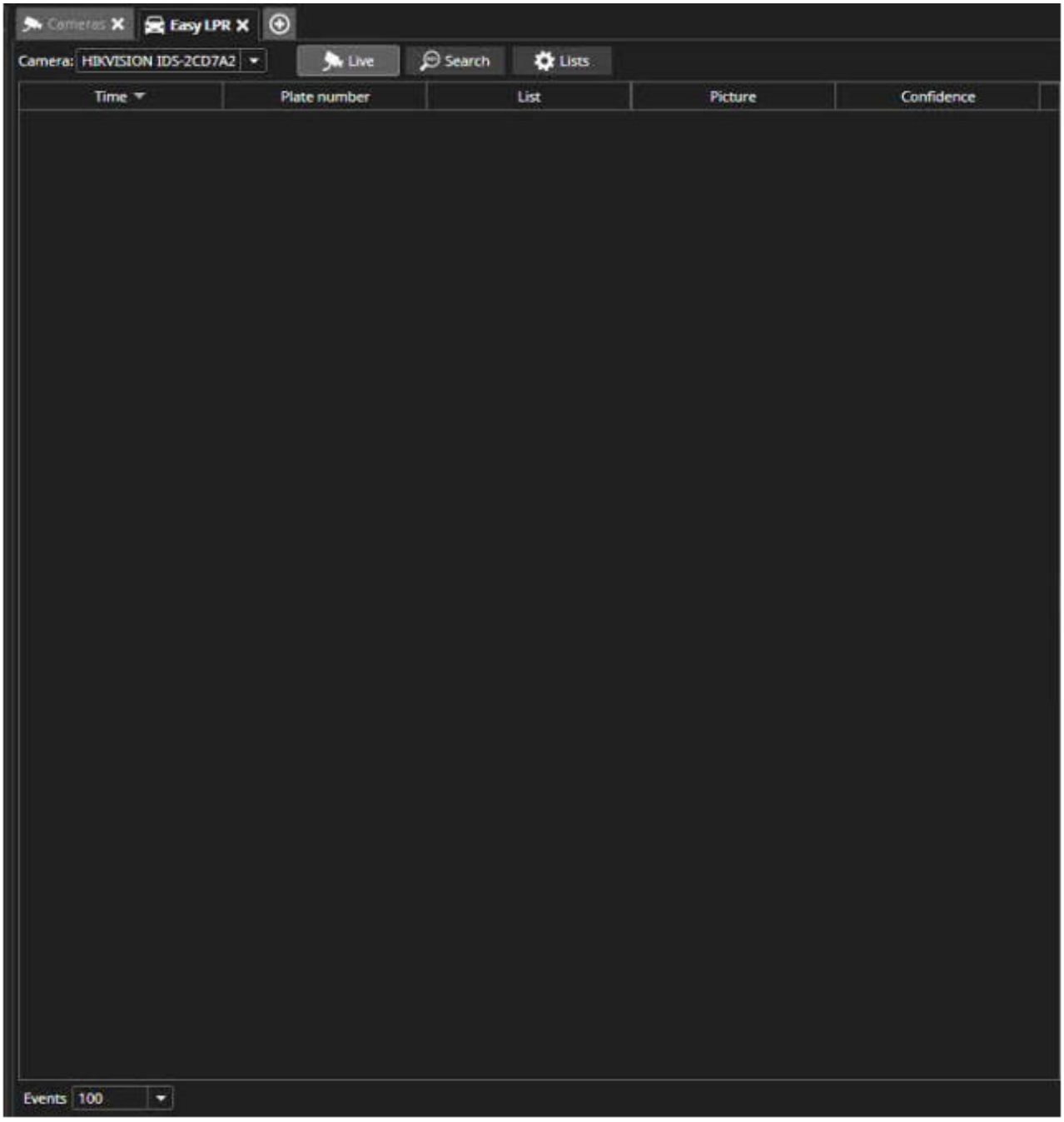

9. Enter the actions of the alarms
10. Set calendar
11. Check overall view of the alarm
12. Click **OK** to confirm an alarm creation



## 15.4.6 Using Easy LPR

Easy LPR contains the following functionalities:

- Live monitoring from the 1 camera at the same time
- The search of the number plates
- Lists Management
- Digital output controlling based on lists

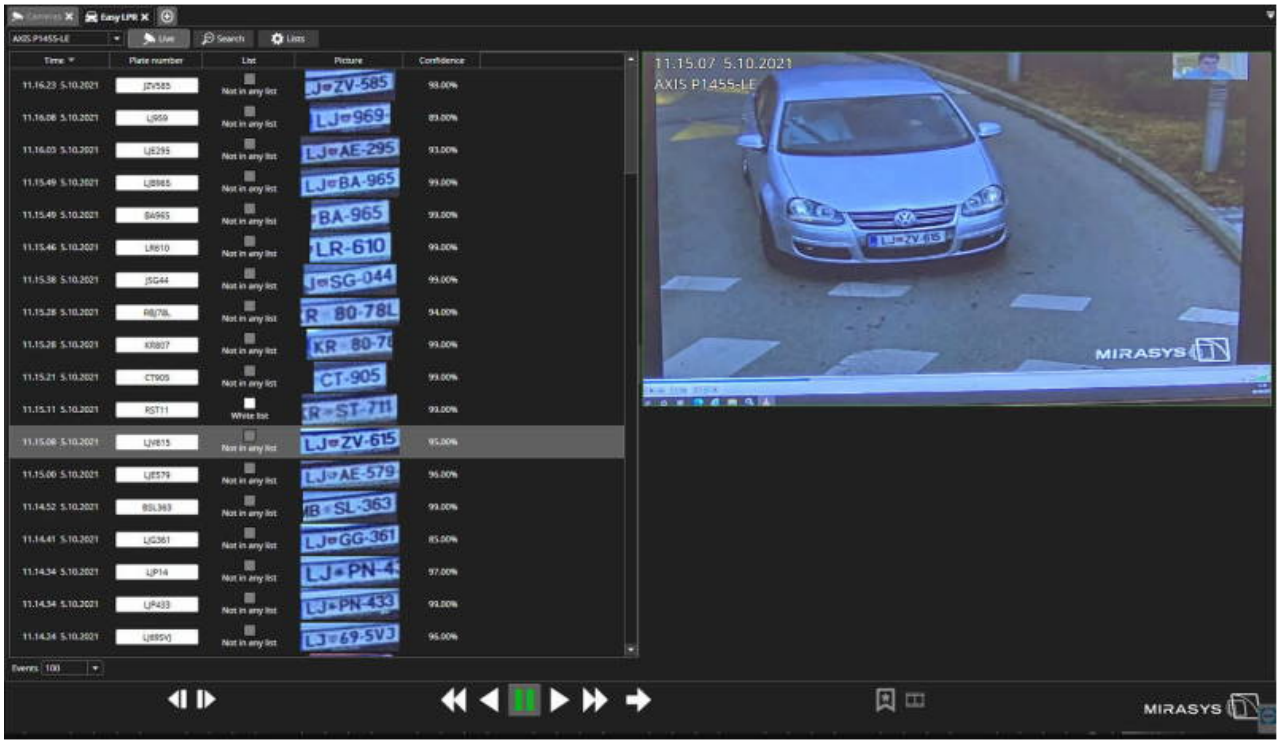



## 15.4.7 Live

The live tab shows the following information:

1. The selection of the LPR camera
2. Time of the plate detection
3. Plate number
4. Plate list
5. Picture of the plate number
6. Confidence of the plate reading
7. Live view from the LPR camera


When the plate information is clicked by the mouse, then the view changes to the playback mode and show the recorded situation.



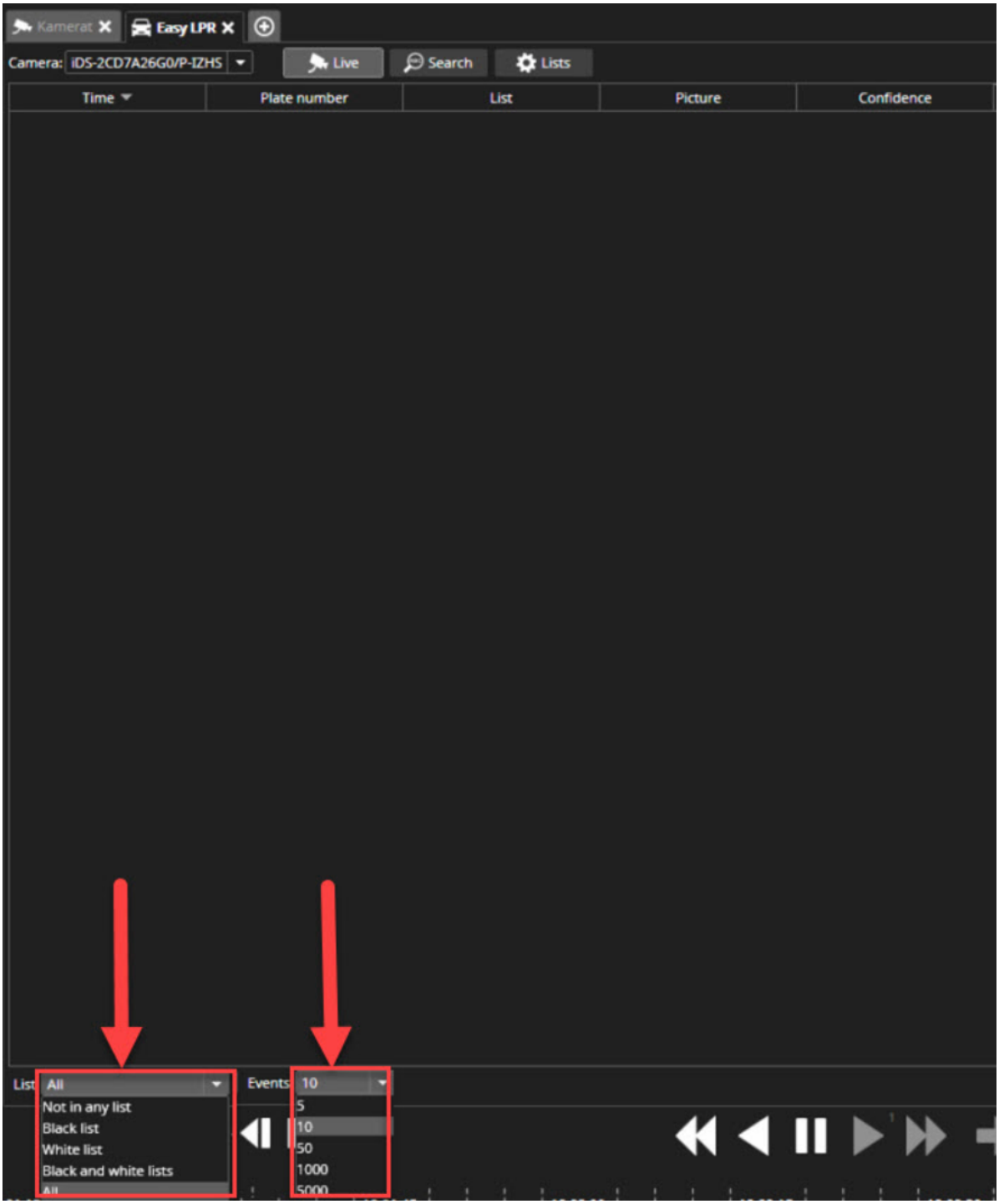

### 15.4.7.1 Filtering the Live view (supported since V9.5.0)

The user can which list are shown in the Live view. Options are:

- All
- Not in any list
- Black list
- White list
- Black list and White list

The user can set the amount of the result in the Live view. Options are:

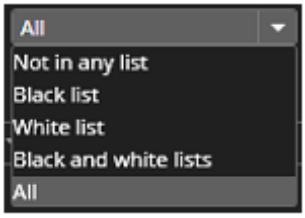
- 5, 10, 50, 1000 and 5000


Kamerat
Easy LPR
Camera: iDS-2CD7A26G0/P-IZHS
Live
Search
Lists
Time
Plate number
List
Picture
Confidence
List
All
Not in any list
Black list
White list
Black and white lists
Events
10
5
10
50
1000
5000

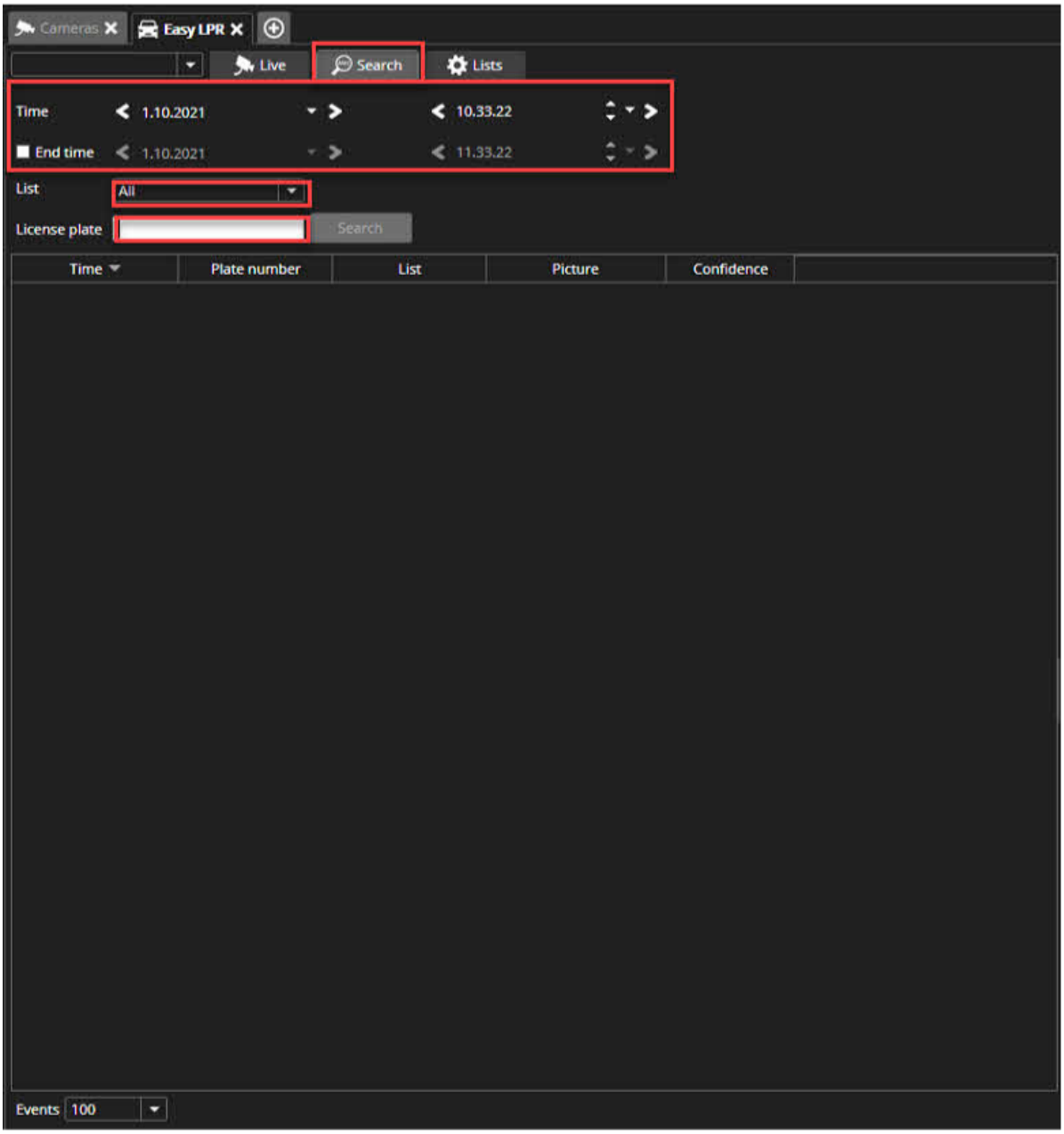
## 15.4.8 Search

### 15.4.8.1 Searching License plates

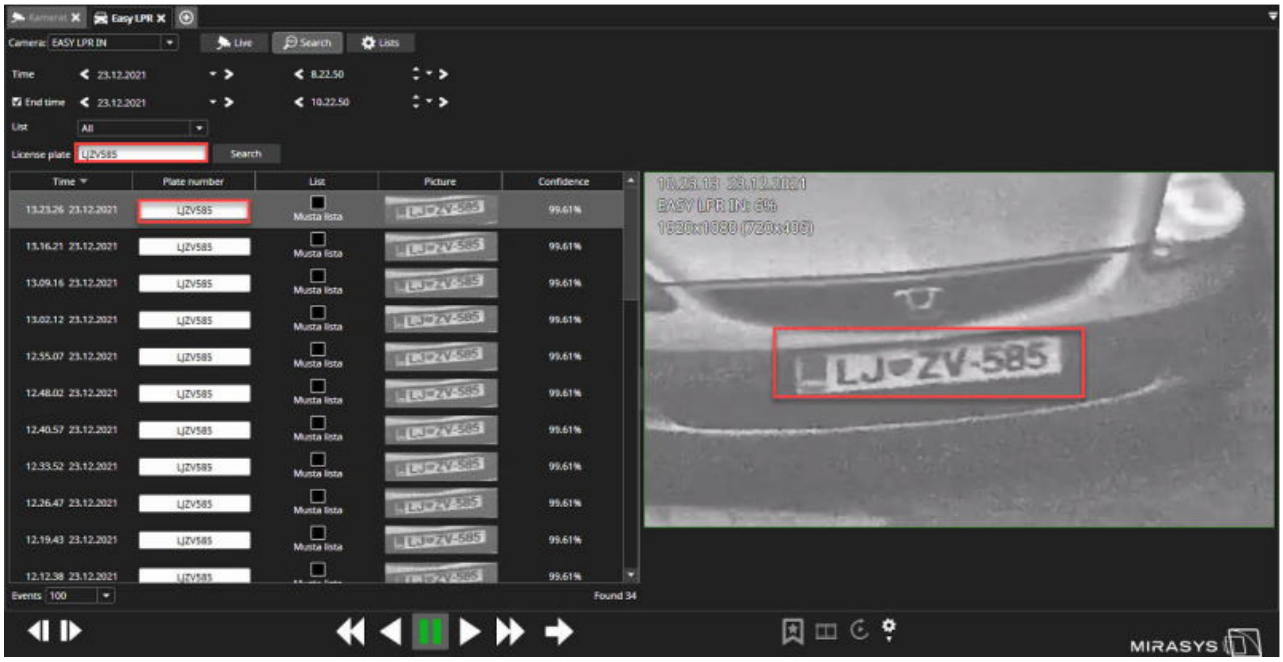
1. Open **Search** tab
2. Select LPR camera from the upper left corner
3. Select time and date
4. Enter **End time**, if needed
5. Select list for the search
    a. All
    b. Not in any list
    c. Black list
    d. White list
    e. Black and white list




1. Enter license plate(partial information is also accepted)
2. Click **Search**




Search will show all results. The user can playback selected time and use all normal playback functions.




## 15.4.9 Lists

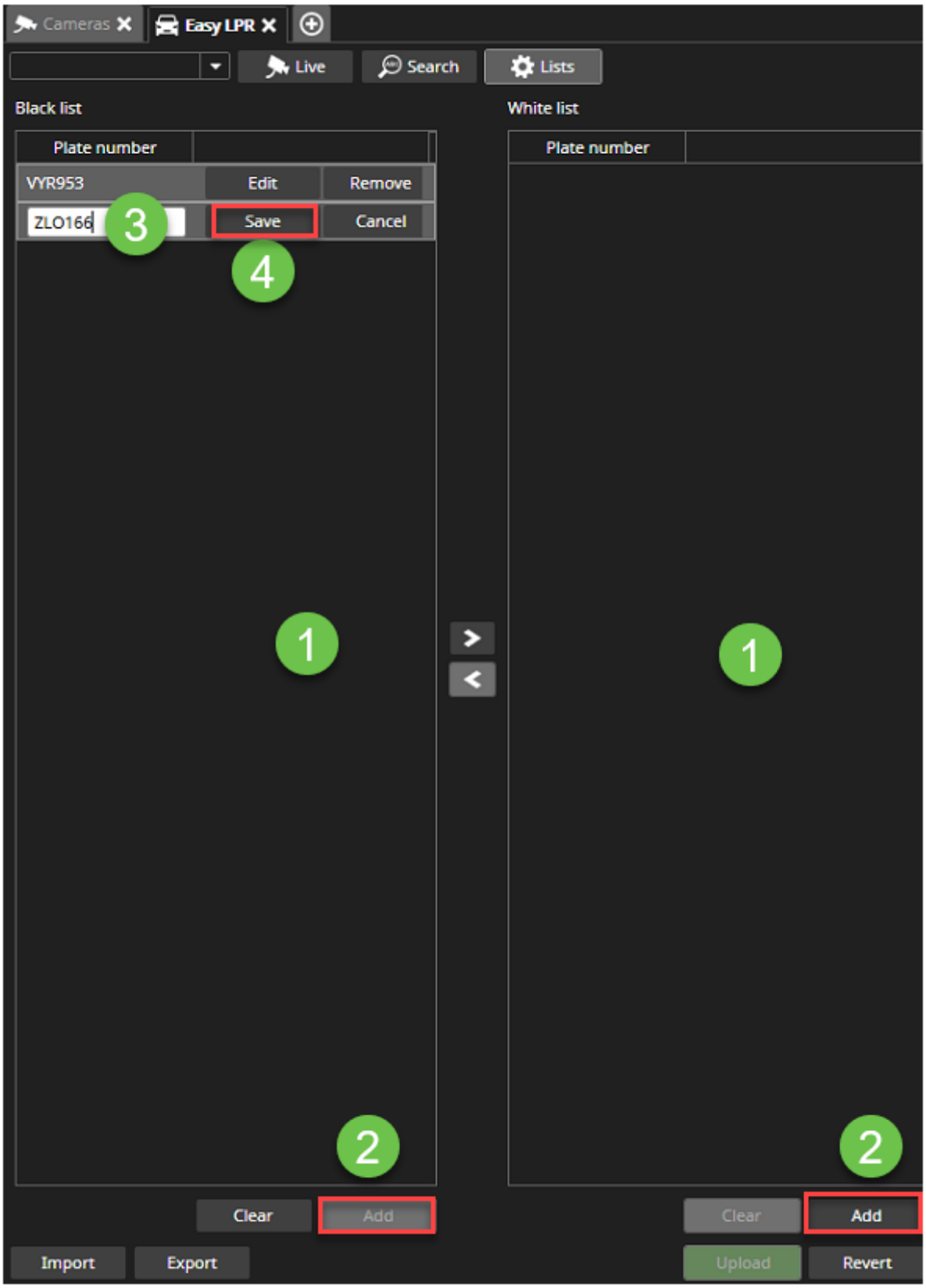
### 15.4.9.1 With the Easy LPR Lists Management, the users can do the following actions:

- Add plate number
- Edit plate numbers
- Move plate numbers between the lists
- Export plate numbers from the Spotter to the PC(**CSV**)
- Import edited plate number lists to the Spotter
- Upload lists from the Spotter to the LPR cameras

### 15.4.9.2 Please remember to upload lists to the cameras after any change.

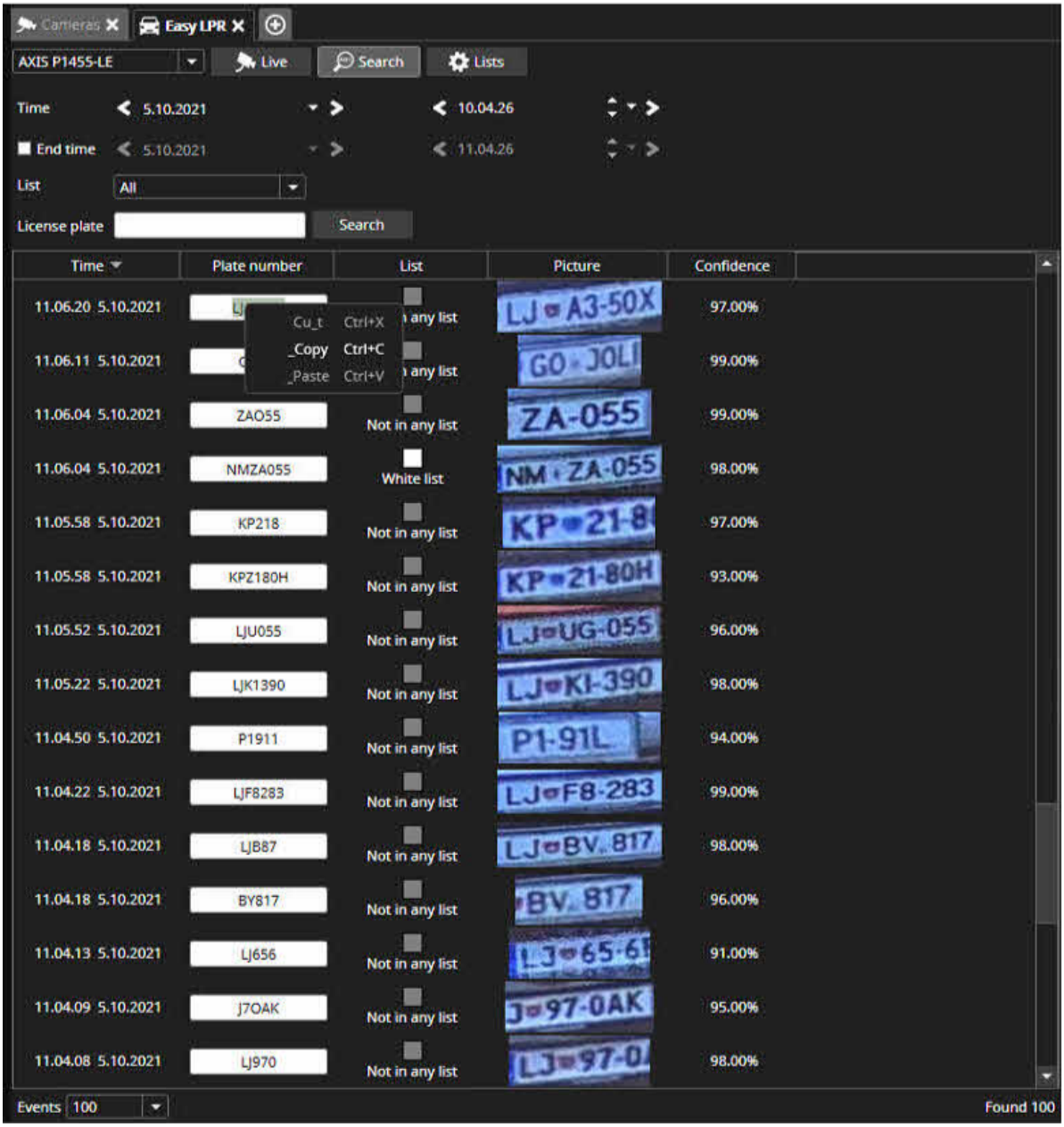
### 15.4.9.3 Adding Plate number

1. Select the **Black list** or **White list**
2. Click **Add**
3. Type the plate number
4. Click **Save**


Cameras
Easy LPR
Live
Search
Lists
Black list
White list
Plate number
VYR953
Edit
Remove
ZLO166
Save
Cancel
3
4
1
2
Clear
Add
Import
Export
Upload
Revert

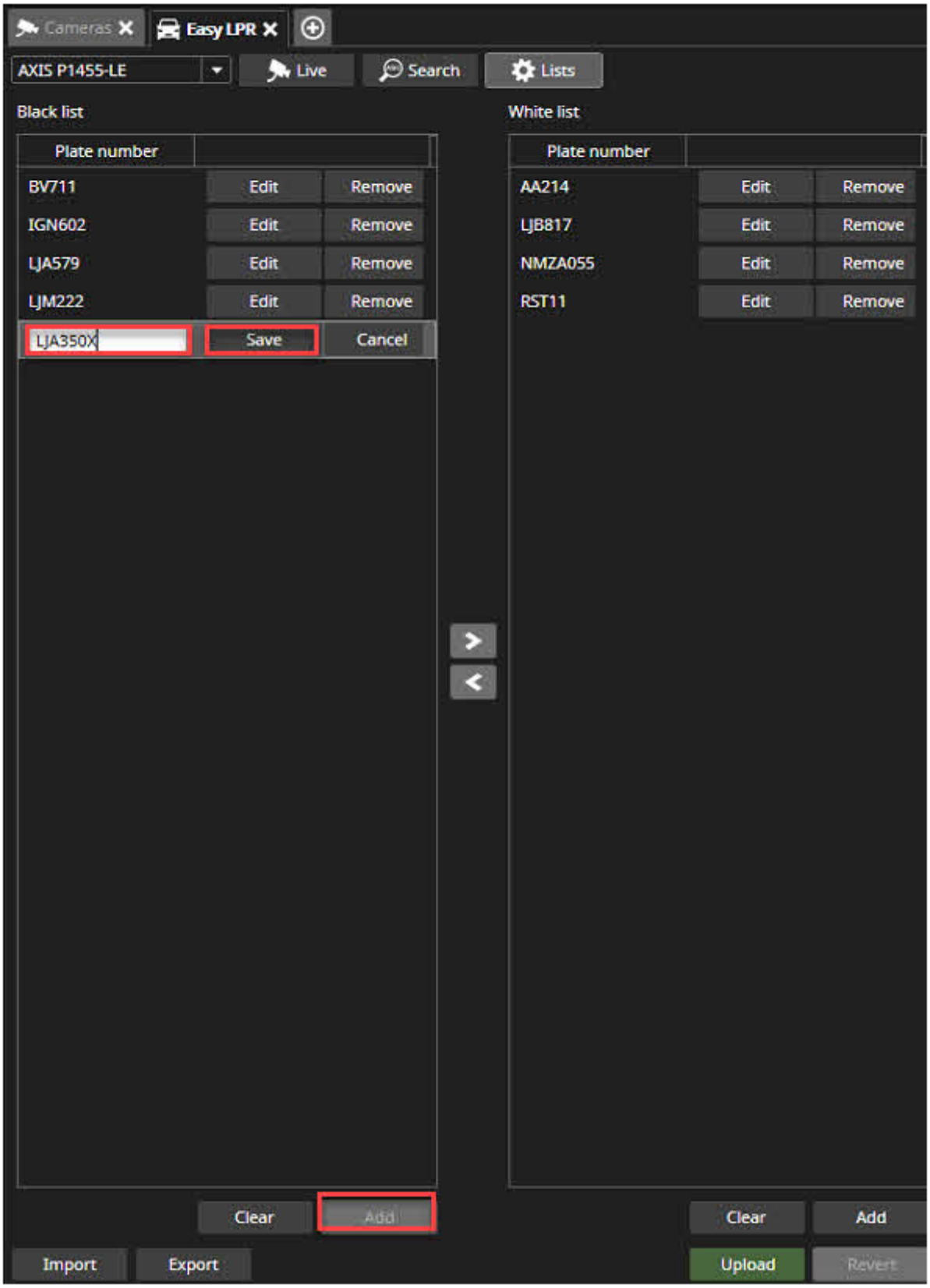
#### 15.4.9.3.1 Adding plate number from the search view

1. Double-click plate number field
2. Right mouse click top of the plate number
3. Click **Copy**



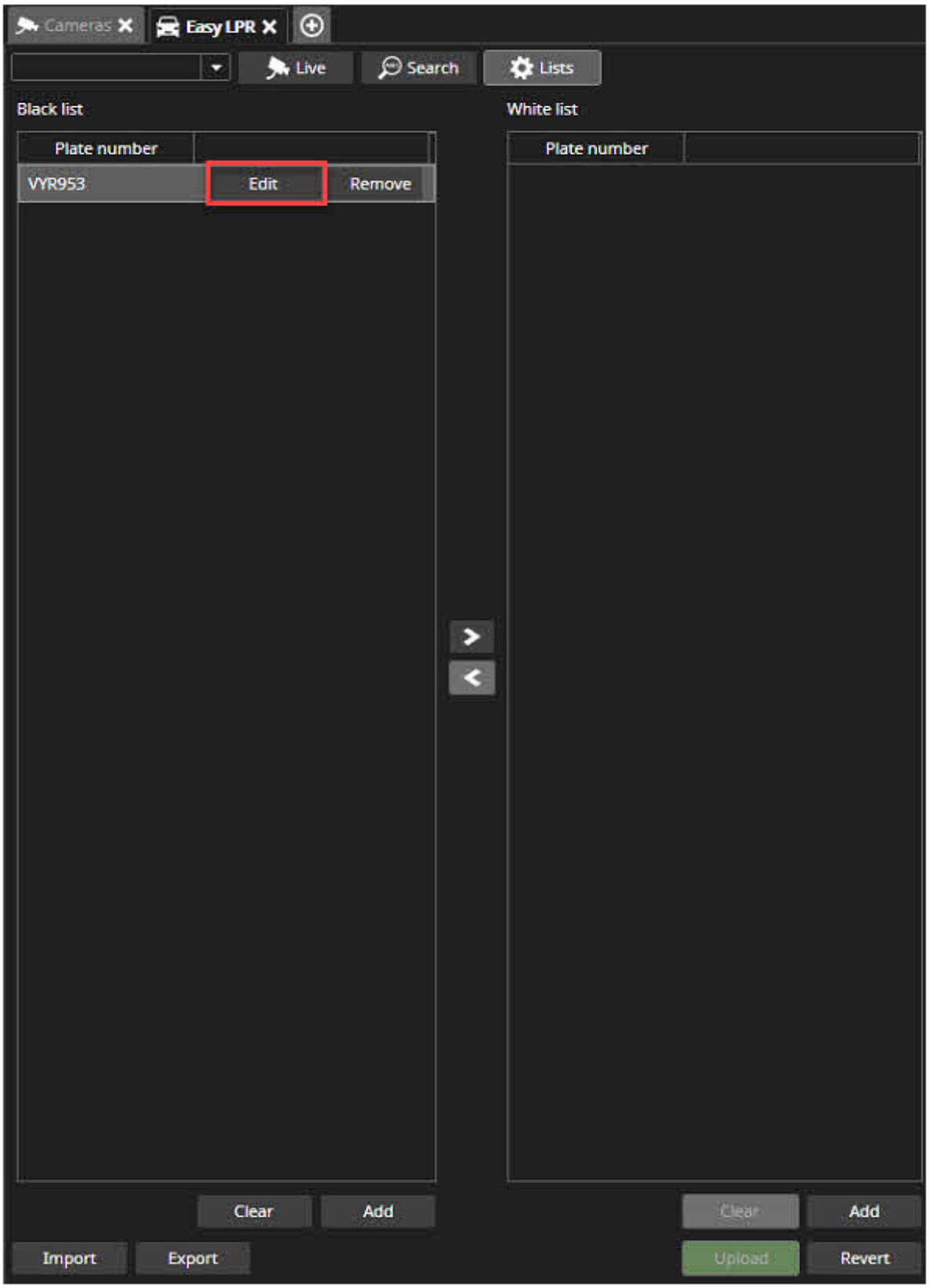

4. Open **Lists**
5. Select current list
6. Click **Add**

7. Paste plate number
8. Click **Save**

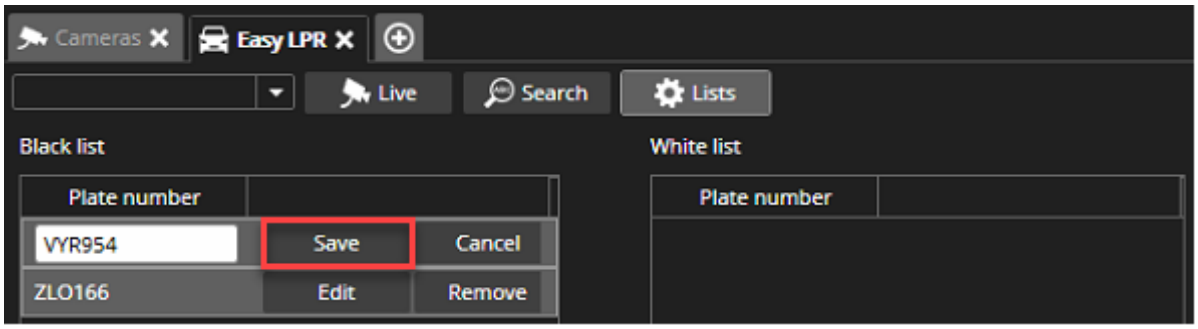

Cameras
Easy LPR
AXIS P1455-LE
Live
Search
Lists
Black list
Plate number
BV711 Edit Remove
IGN602 Edit Remove
LJA579 Edit Remove
LJM222 Edit Remove
LJA350X Save Cancel
White list
Plate number
AA214 Edit Remove
LJB817 Edit Remove
NMZA055 Edit Remove
RST11 Edit Remove
Clear
Add
Clear
Add
Import
Export
Upload
Revert

### 15.4.9.4 Editing Plate Number

1. Select the plate number
2. Click **Edit**

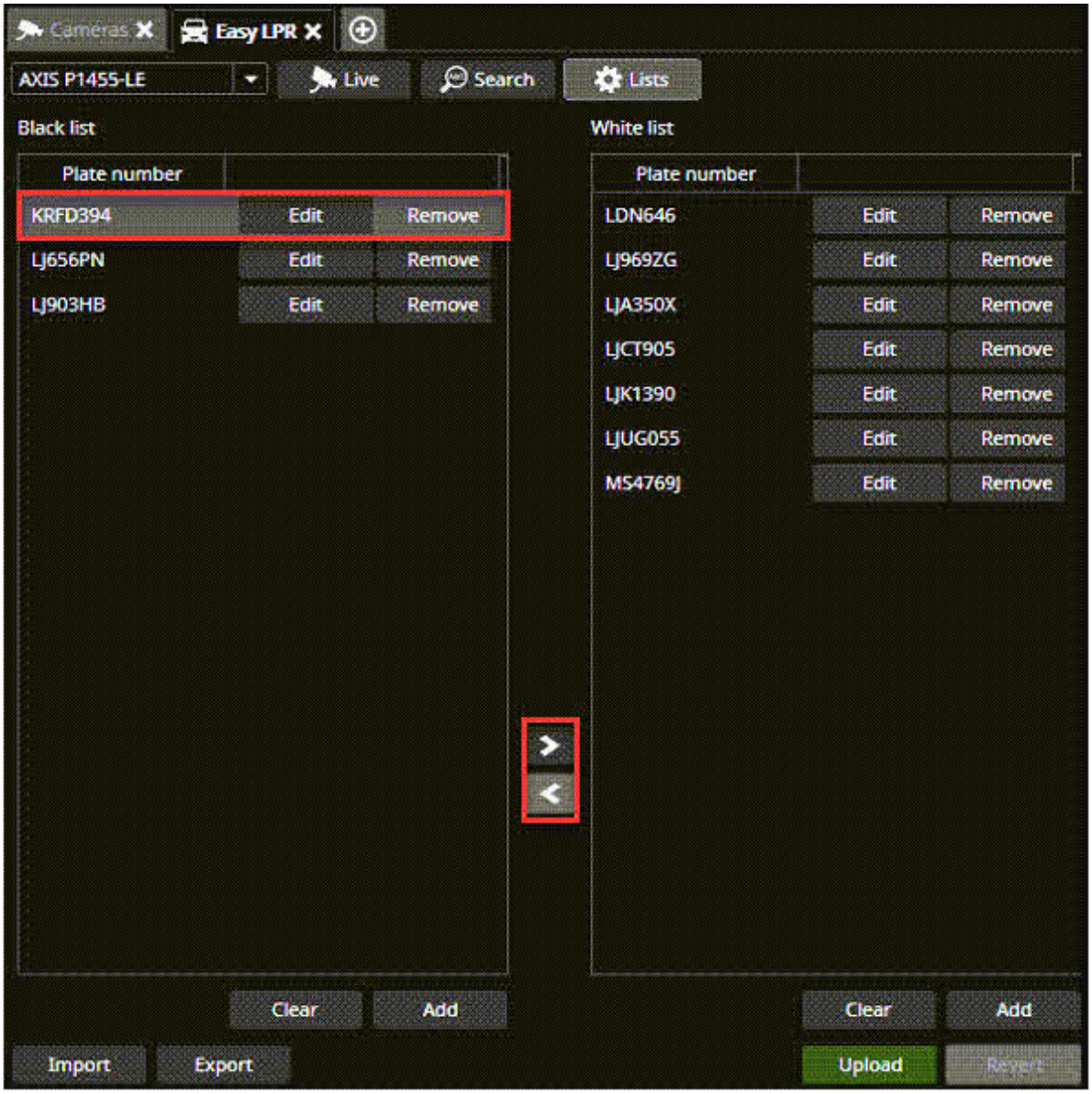

Cameras
Easy LPR
Live
Search
Lists
Black list
Plate number
VYR953
Edit
Remove
White list
Plate number
Clear
Add
Clear
Add
Import
Export
Upload
Revert

3. Do the modification and click **Save**



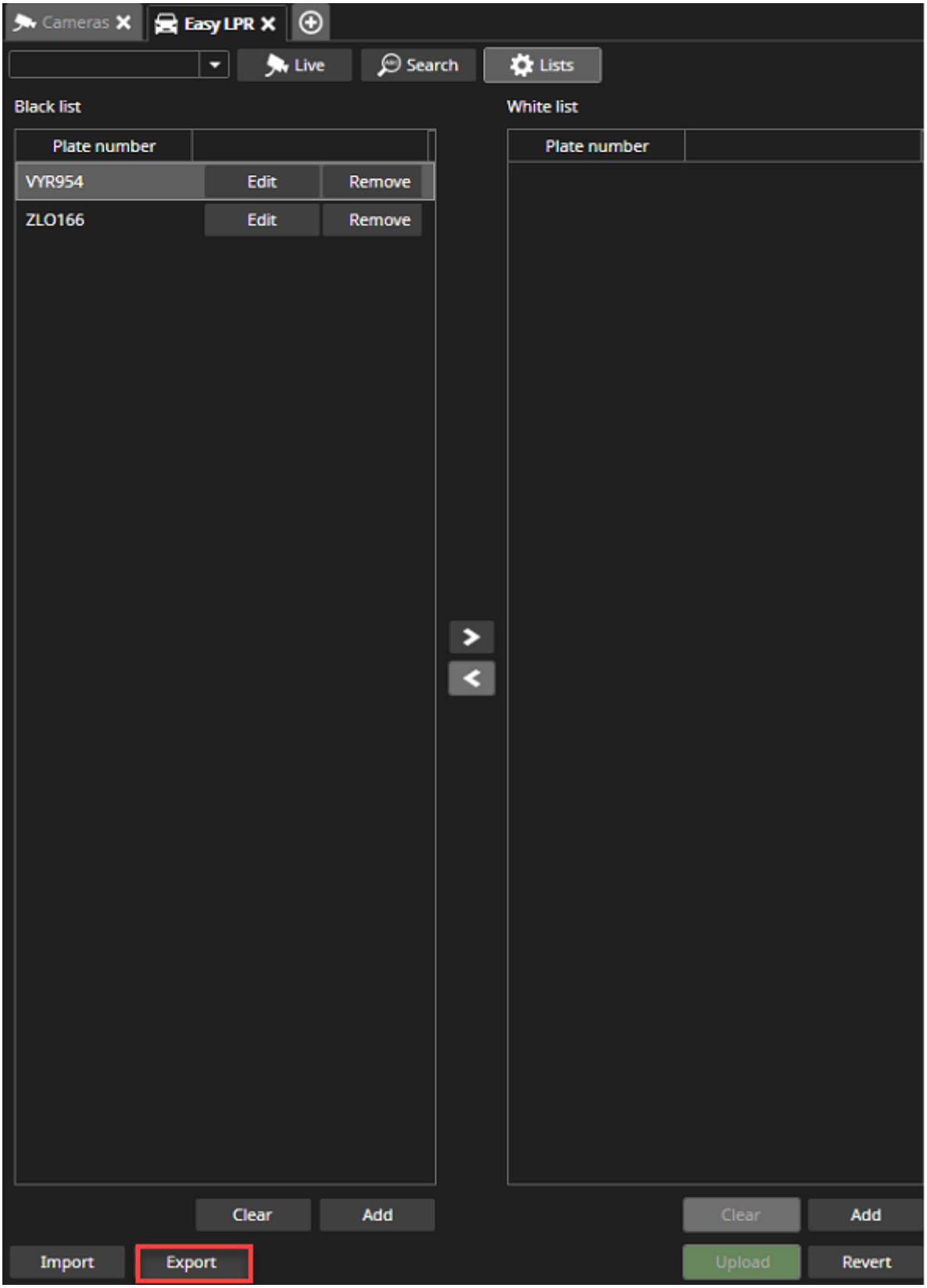

### 15.4.9.5 Moving Plate Number between the lists

1. Select the plate number from the list
2. Click arrow to move needed list

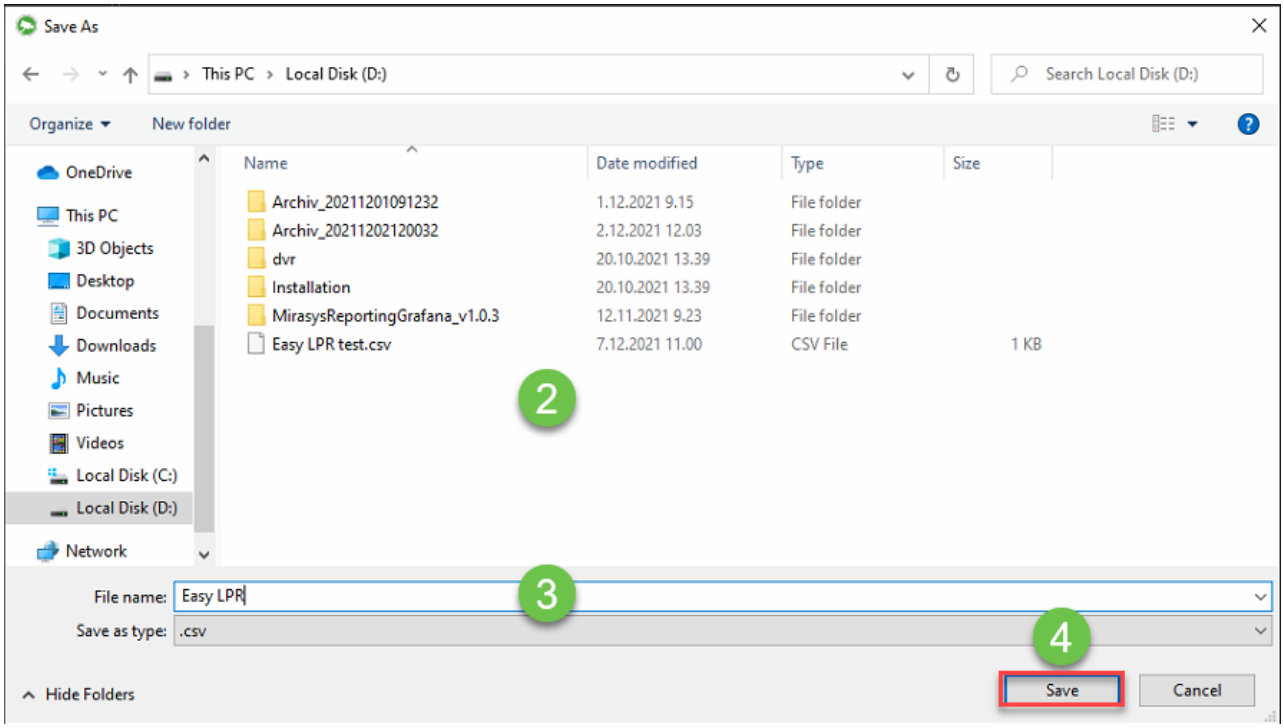



## 15.4.9.6 Export Plate Number lists

1. Click **Export**

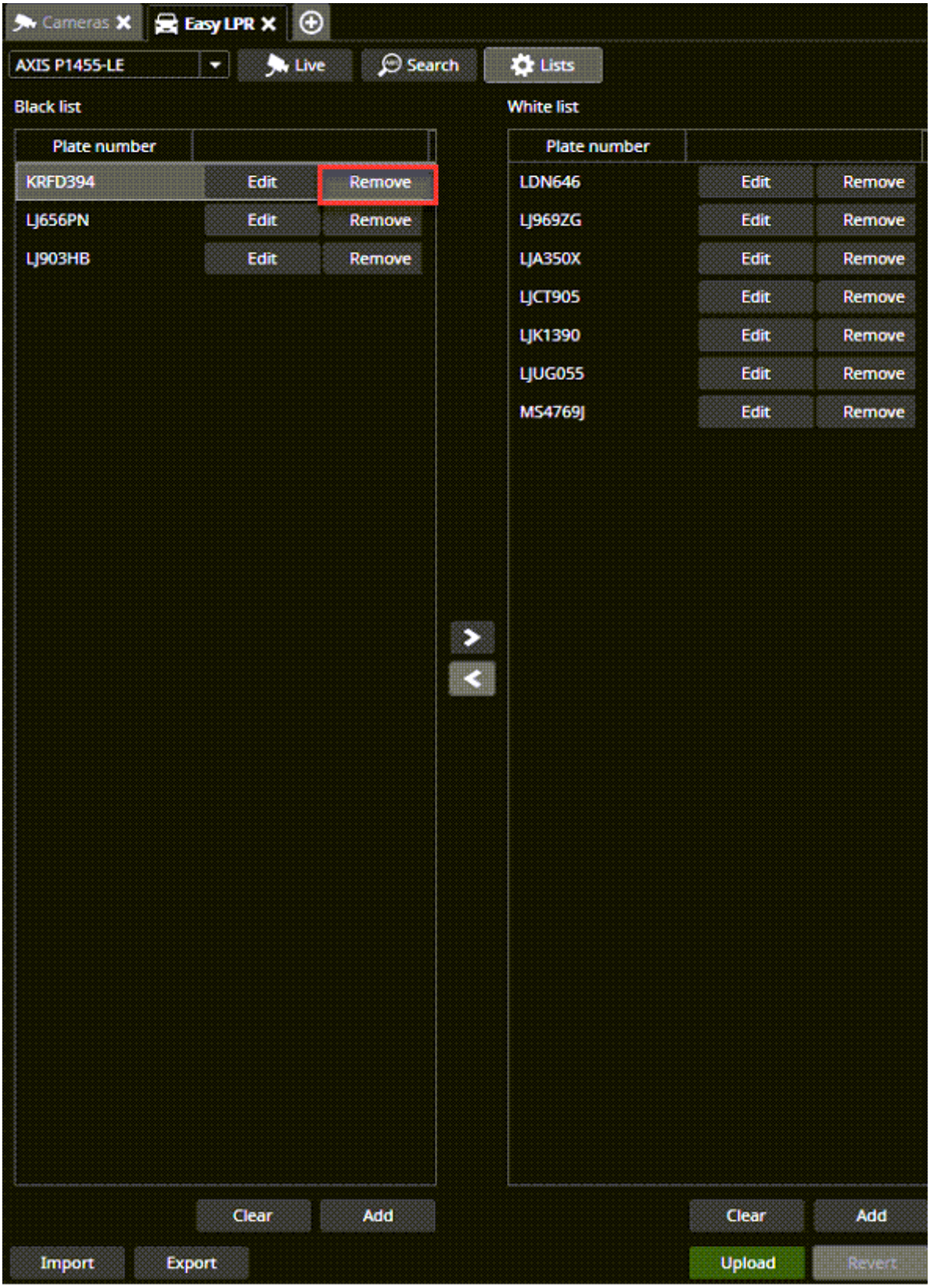

Cameras
Easy LPR
Live
Search
Lists
Black list
Plate number
VYR954
Edit
Remove
ZLO166
Edit
Remove
White list
Plate number
Clear
Add
Clear
Add
Import
Export
Upload
Revert

2. Define the destination folder
3. Set the file name(.csv)
4. Click **Save**




## 15.4.9.7 Removing Plate Numbers

1. Select the plate number from the list
2. Click Remove


Cameras
Easy LPR
AXIS P1455-LE
Live
Search
Lists
Black list
Plate number
KRFD394
Edit
Remove
LJ656PN
Edit
Remove
LJ903HB
Edit
Remove
White list
Plate number
LDN646
Edit
Remove
LJ969ZG
Edit
Remove
LJA350X
Edit
Remove
LJCT905
Edit
Remove
LJK1390
Edit
Remove
LJUG055
Edit
Remove
MS4769J
Edit
Remove
Clear
Add
Clear
Add
Import
Export
Upload
Revert

## 15.4.9.8 Importing Plate Numbers

### 15.4.9.8.1 With the import, the user can import a large number of plate numbers at the same time

1. Open exported CSV file

CSV content is shown below:

Plate number, List (1 = black list / 2 = white list)

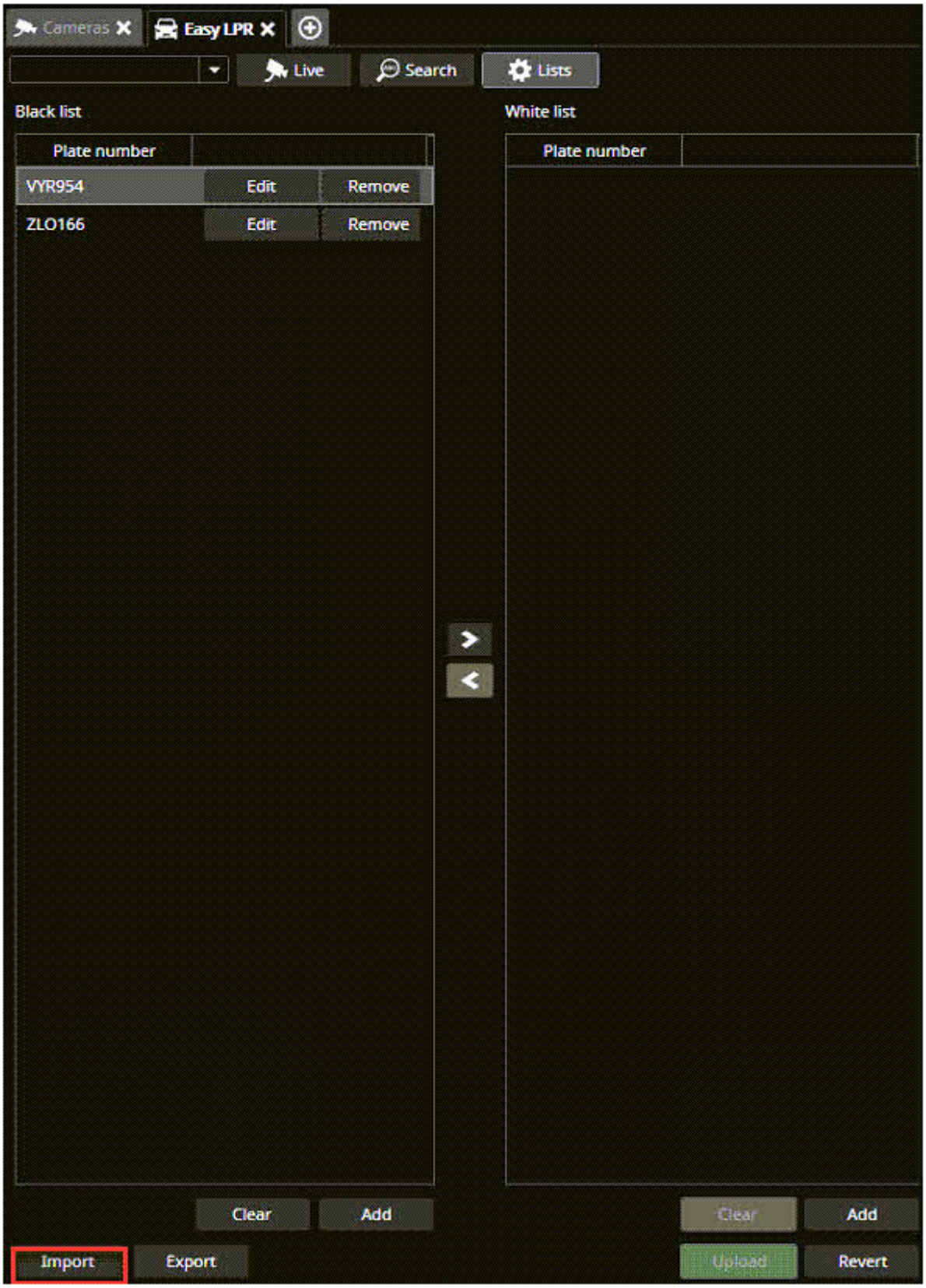
LJ656PN,1

LJ731CV,1

LJZV585,1

LJZV584,2

1. Add a new line with format ZLO166,2  for each new plate number
2. Select correct list(**List 1 = Black list, List 2 = White Lis**t)
3. Save changes
4. Click **Import**

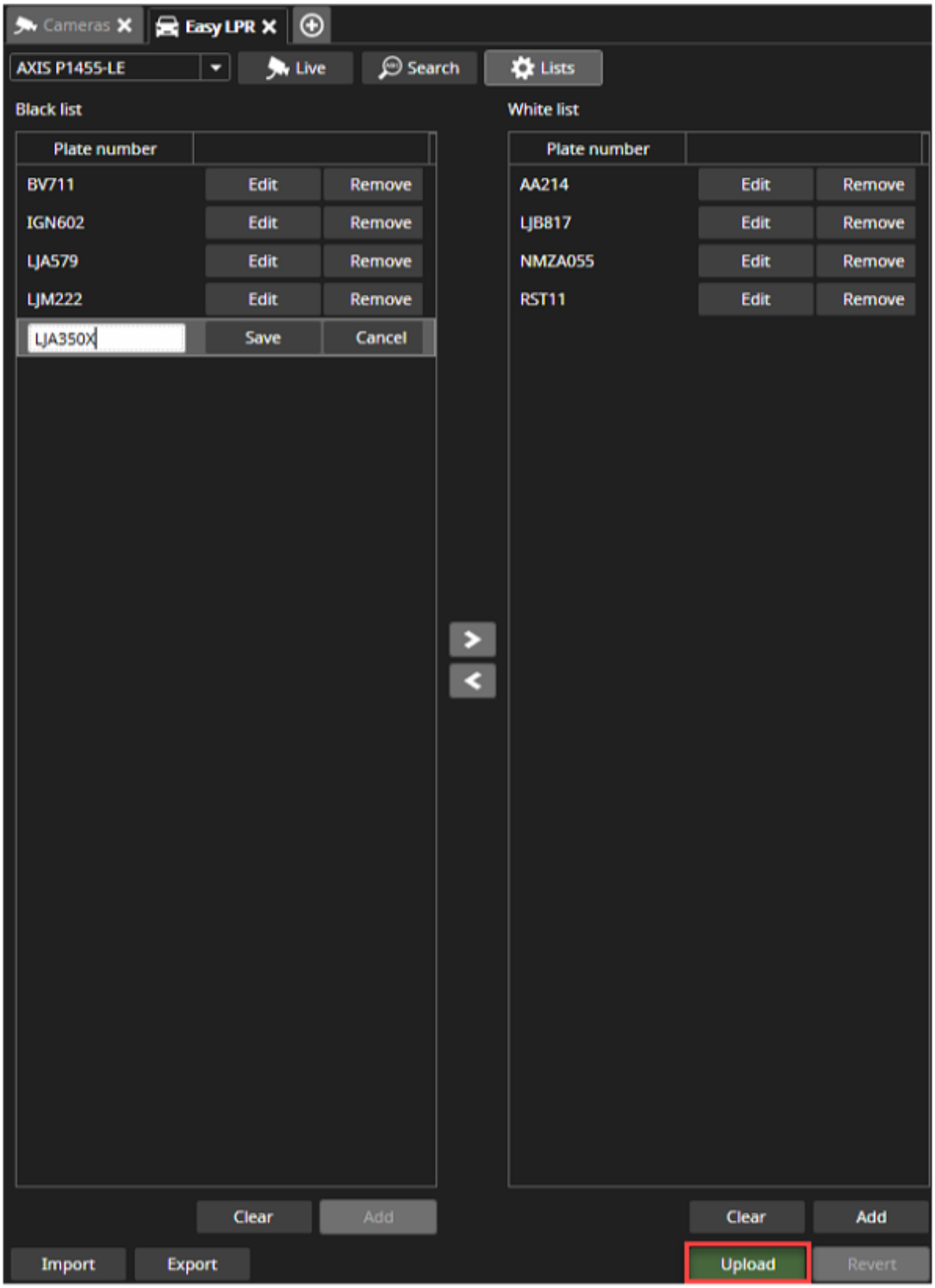

Cameras
Easy LPR
Live
Search
Lists
Black list
Plate number
VYR954
Edit
Remove
ZLO166
Edit
Remove
White list
Plate number
Clear
Add
Clear
Add
Import
Export
Upload
Revert

5. Browse to the location of the CSV file
6. Select the file and click **Open**

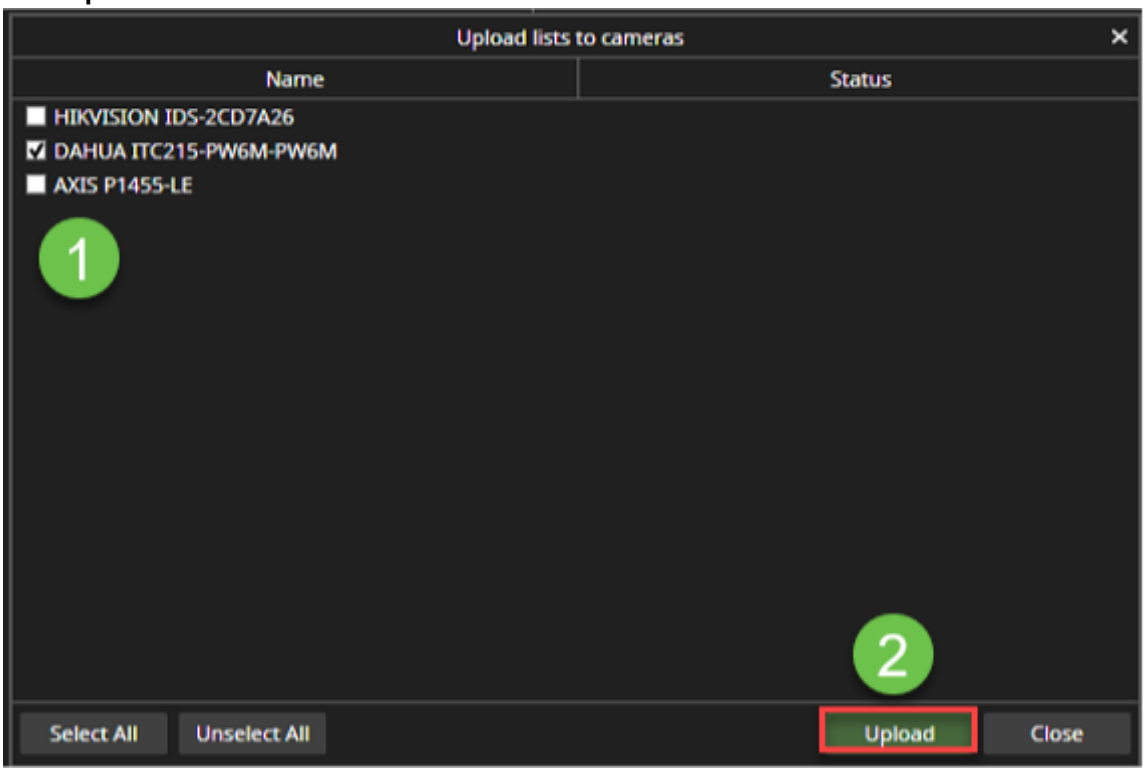
## 15.4.9.9 Uploading lists

### 15.4.9.9.1 With the upload, the user can upload created black & white lists to the camera

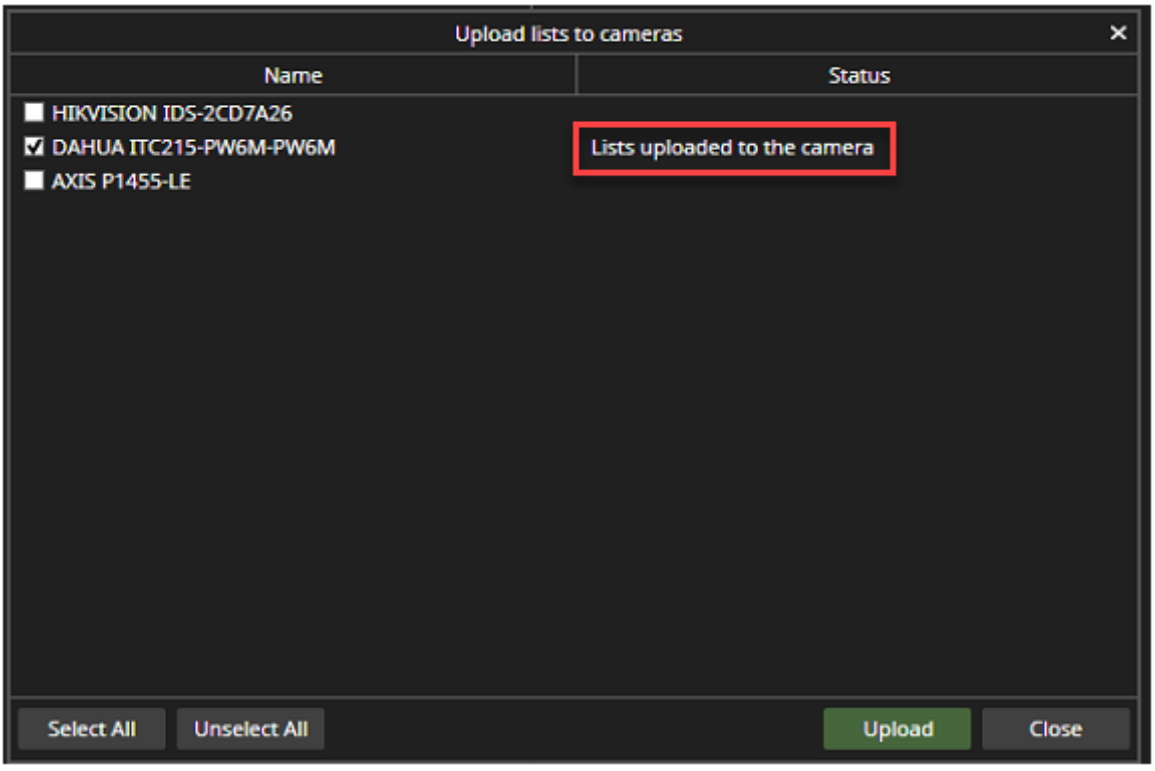
1. Select camera, which list will be uploaded
2. Click **Upload**


Cameras
Easy LPR
AXIS P1455-LE
Live
Search
Lists
Black list
Plate number
BV711
Edit
Remove
IGN602
Edit
Remove
LJA579
Edit
Remove
LJM222
Edit
Remove
LJA350X
Save
Cancel
White list
Plate number
AA214
Edit
Remove
LJB817
Edit
Remove
NMZA055
Edit
Remove
RST11
Edit
Remove
Clear
Add
Clear
Add
Import
Export
Upload
Revert

1. Select cameras, where lists are uploaded
2. Click **Upload**

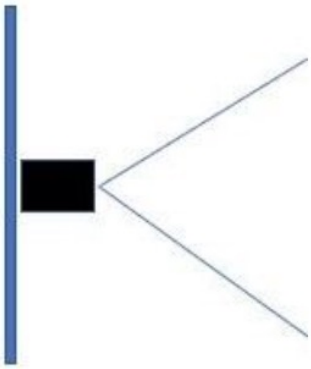


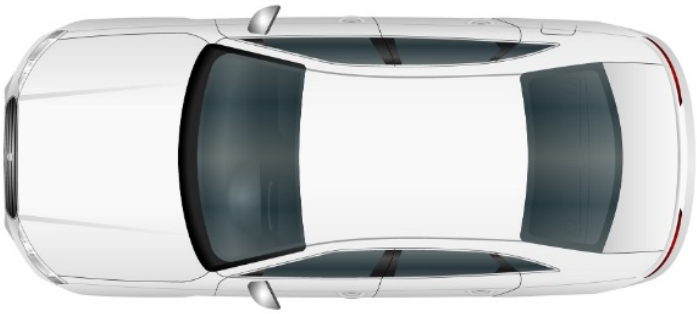

After the upload, the status field shows information **List uploaded to the camera**



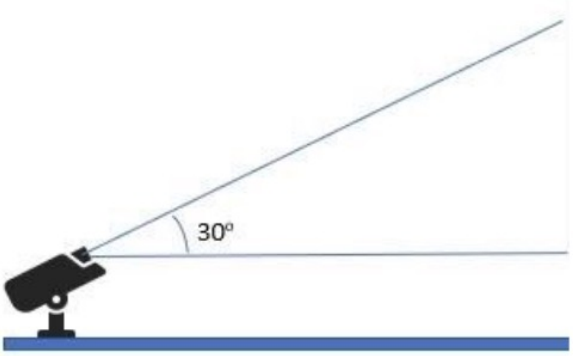
## 15.5 LPR Camera Installation tips

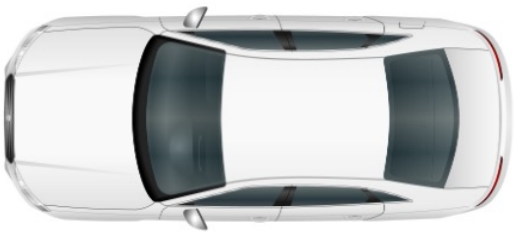
### 15.5.1 It is recommended to install the camera in the center of the vehicle



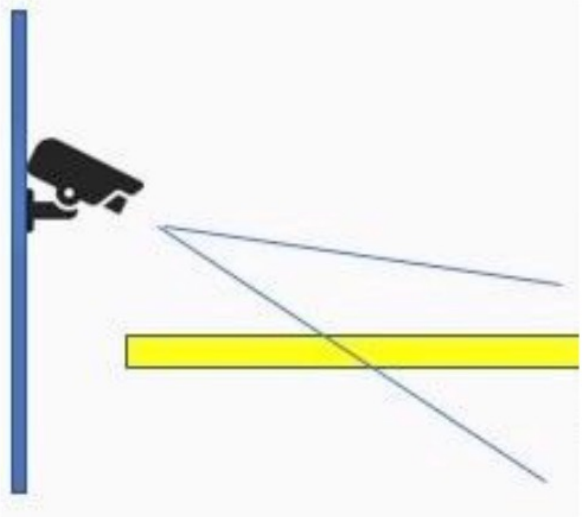


### 15.5.2 If the camera is installed on the side of the road or lane, the angle should not exceed 30 degrees.



### 15.5.3 The camera should be installed higher than the vehicle headlights so that the vehicle's headlights don't point directly at the camera



### 15.5.4 Ensure the license plate width is at least 120 pixels and height at least 50 pixels


Height at least 50 pixels

Width at least 120 pixels

### 15.5.5 License plate tilt angle must be within +/- 10 degrees

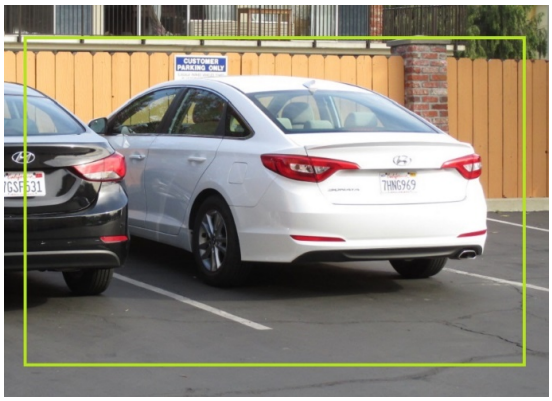


## 15.5.6 LPR settings in the System Manager application

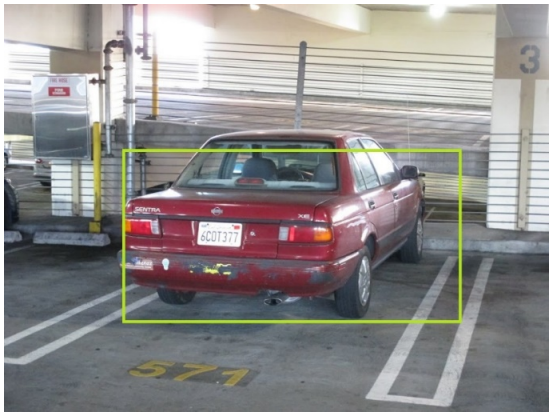
Ensure the correct region (Americas / Eurasia) is selected.

### 15.5.6.1 Setting the region of interest

Region of interest is used to define where detection will find license plates.



Leave some margin to the region of interest to not detect partially visible plates.



The whole license plate is inside the region of interest, and the plate is detected.

The license plate is not completely inside the region of interest, and the plate is not detected.

---

### 15.5.6.2 Enabling country recognition

In many countries letter **O** is similar to the number **0**, and the letter **I** looks the same as the number **1**. Enabling country detection improves detection accuracy in these cases.


For example, the format for Brazil plate number is “abc1d23”.

---

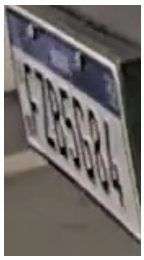
## 15.5.7 Common problems and solutions

### 15.5.7.1 Incomplete license plate

Solution: Don’t set the region of interest too close to image borders.

---

### 15.5.7.2 View angle makes plate numbers unreadable



Solution 1: Move the camera to a better place.

Solution 2: Set the region of interest so that the plate is detected when it is visible from better angle.

---

### 15.5.7.3 Other vehicles headlights reflect from license plate

Solution 1: Move the camera to a better place.

Solution 2: Set the region of interest so that the plate is detected when other vehicles’ headlights don’t point to the license plate direction.

---

### 15.5.7.4 The license plate is too small

Solution 1: Move the camera to a better place or zoom in.

Solution 2: Set the region of interest so that the plate is detected when the vehicle is nearer to the camera.

Solution 3: Increase the minimum plate height value in LPR settings so that small plate detections are ignored.

---

#### 15.5.7.5 The license plate is blurry

Solution 1: Adjust sharpness and increase shutter speed in the camera's settings.

Solution 2: Increase the lighting of the area.

---

#### 15.5.7.6 The license plate is overexposed

Solution 1: Adjust camera's image settings.

Solution 2: Check the camera installation location and move it higher so that headlights doesn't reflect from the plate.

---

## 15.6 Mirasys VCA Guide

### 15.6.1 About Mirasys VCA

Mirasys VCA (Video Content Analytics) comprises a set of real-time video analytics solutions that utilizes advanced image processing algorithms to turn video into actionable intelligence.
The product's core is an advanced object recognition and tracking engine that continually tracks moving and stationary targets.

The tracking engine features built-in robustness to environmental nuisance conditions such as changing illumination, moving foliage, rippling water, etc.

Mirasys VCA is a generic name for a suite of video analytics add-on product options that include functionality such as:

- Ability to detect aggressive behavior.
- Ability to detect falls.
- Ability to detect directional crossing.
- Ability to detect repeated behavior.
- Ability to detect persons with their hands up.
- Deep learning object tracker classes are now person, bus, motorcycle, bicycle, car, van, truck, forklift, and bag for triggering alarms
- Support for different event state possibilities: start (default), on, stop. Note that the states on and stop are only available if defined in VCA Core config files.

Other Features are:

#### 15.6.1.1 Motion object tracking

Motion-data based object highlighting and tracking, auto-zoom functionality.
The motion data is produced by server-based, hermeneutic motion detection.

#### 15.6.1.2 Tripwire counting

In addition to motion object tracking functionality, line counting for over-head installed cameras, and Spotter client-based counter visualization.

#### 15.6.1.3 Object behaviour/attributes detection

In addition to the functionality mentioned above, to continuously track and classify moving and stationary targets and features a full suite of rule-based filters including as enter, exit, appear, disappear, stopped objects, directionality constraints, object counting, loitering, object type and object speed.

Multiple filters and rules are supported on any combination of multiple overlapping detection zones, in addition to an advanced people tracking engine optimized for tracking people in cluttered indoor scenes such as retail scenarios. Includes specific high accuracy counting functions optimized for use in busy scenes.

#### 15.6.1.4 Related analytics options

Available as separate applications, products or through project-based integrations:

- Camera-based (built-in, edge) analytics support selected camera manufacturers and their functionality through manufacturer-specific integration connectors.
- Audio analytics technologies refer to software for extracting information and meaning from audio signals, such as detecting sounds of breaking glass, etc.
- Facial recognition technologies refer to software or camera feature for automatically identifying or verifying the identity, age, gender, etc., of a person from video footage.
- Number plate recognition technologies (ANPR/LPR) refer to software or camera features for automatically identifying vehicle or container numbers.

## 15.6.2 Quick start guide for VCA

This user guide documents each topic in detail. However, to get started quickly, the essential topics are listed below.

### 15.6.2.1 The following steps should be executed for each server:

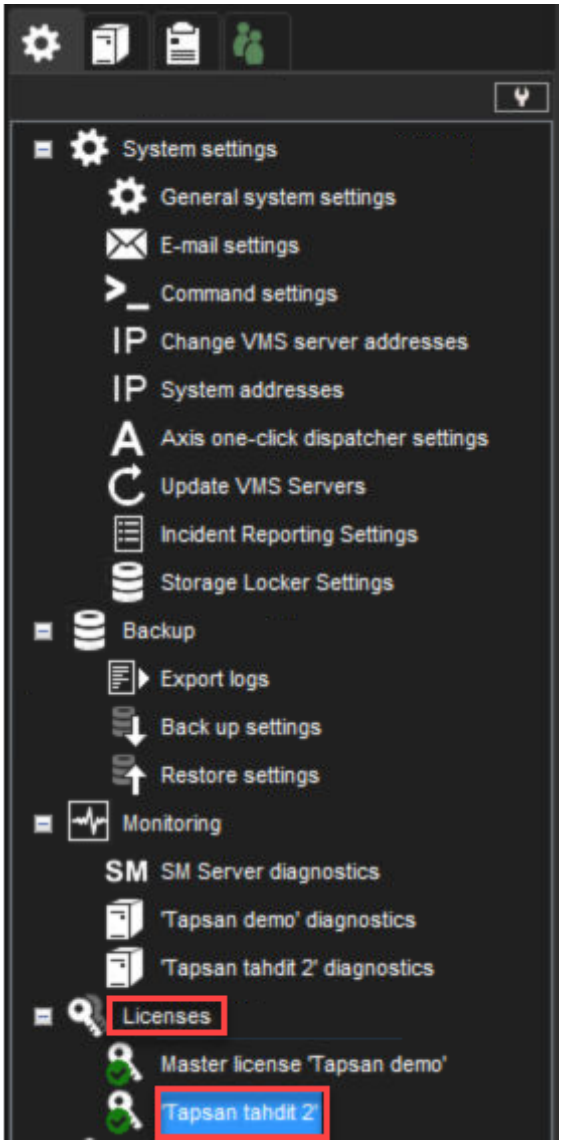
1. Decide upon the VCA functionality that meets your requirements. For guidance or consult your Mirasys representative or check the Mirasys VCA training.
2. Acquire and install a Mirasys VMS system and the related software license key with other required features enabled.
3. Add and configure the video cameras you intend to use for VCA and enable the VCA capability in the camera settings.
4. Enable hermeneutic motion detection mode for each camera used for VCA.
5. Export the VCA core HW GUID and obtain the VCA activation license code from Mirasys and activate Mirasys VCA with these licenses.
6. Calibrate each camera in VCA settings if object classification is required.
7. Configure the detection zone and rules for each camera.
8. If required configure alarms based on the VCA events.
9. Verify VCA functionality visualisation using the Spotter for Windows application.

## 15.6.3 Prerequisites for Mirasys VCA

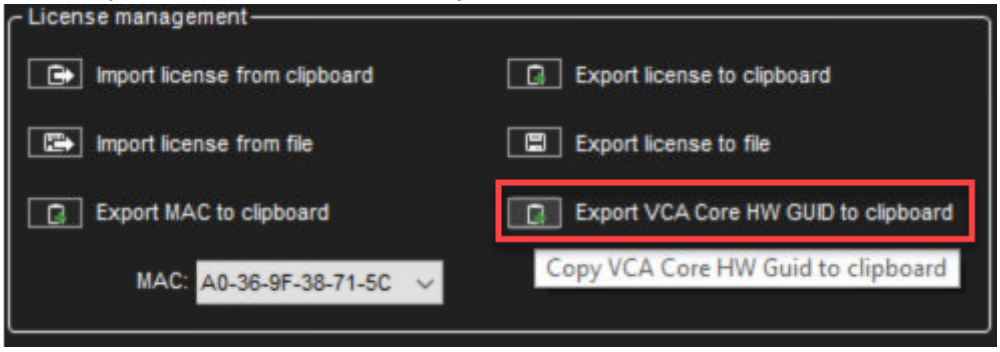
- Exporting VCA Core HW GUID file
- Activating VCA license
- Setting up the motion detection method
- Activating VCA Core for the cameras

### 15.6.3.1 Exporting VCA Core HW GUID file

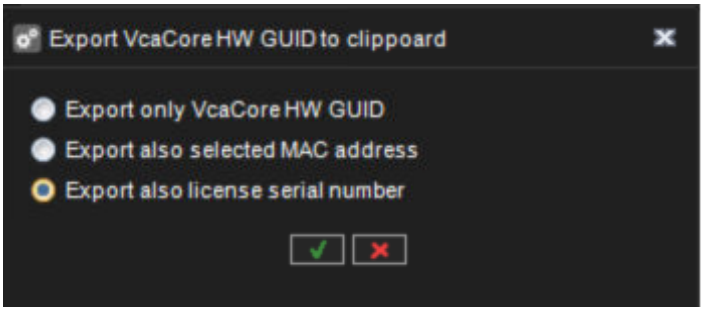
1. Go to the **System** tab
2. Open **Licenses**
3. Double-click the license




4. Select Export VCA Core HW GUID to clipboard




5. Select **Export also license serial number**
6. Click Ok



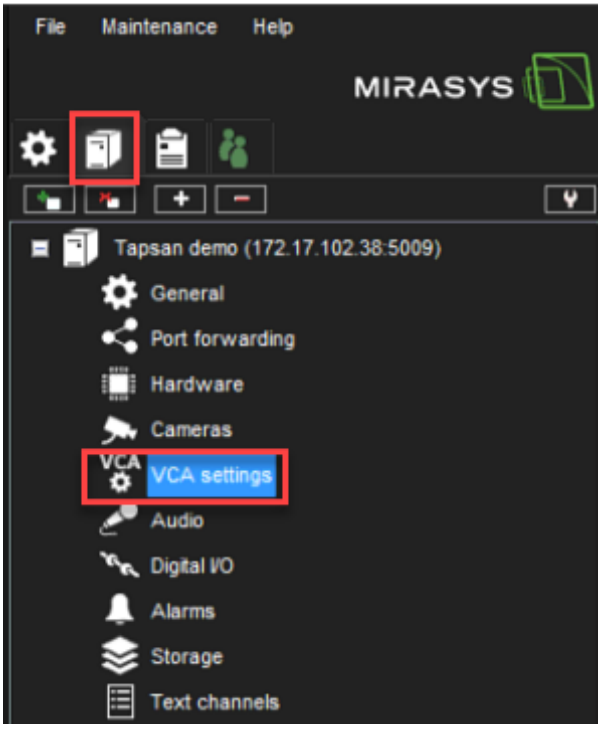

7. Paste clipboard data to the text document.
8. Send it to Mirasys to receive the VCA license.

VcaCore Hw Guid: C1092267BD20344A5853FFD2BEA65406C1884F6FA19B503395E85F8545F75E2D

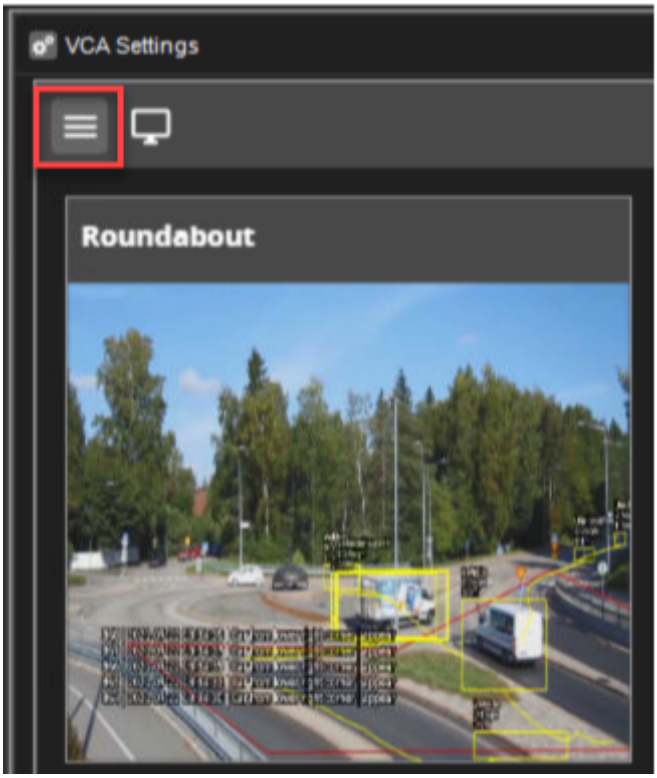
License serial number: YL9QMELM9QK5

### 15.6.3.2 Activating VCA licenses

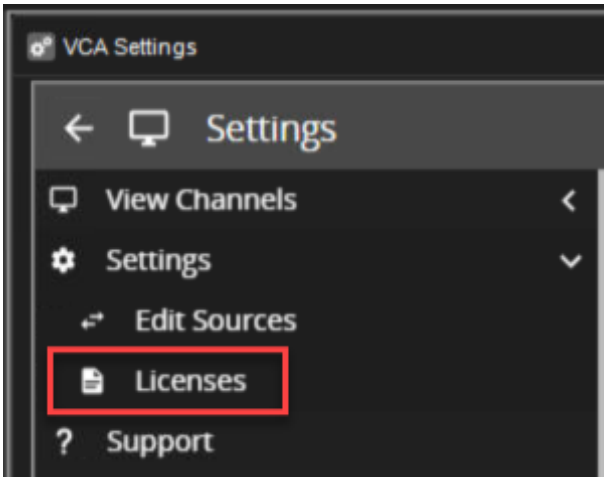
1. Go to the **VMS Servers** tab
2. Open **VCA settings**



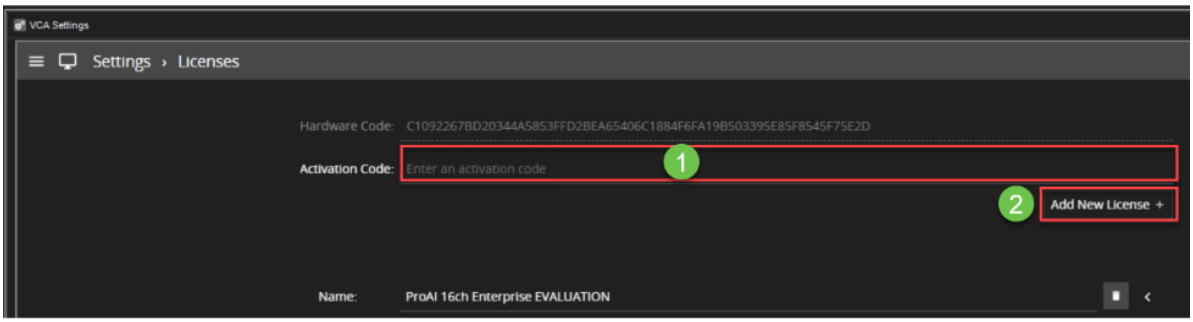

3. Click the **Settings** icon from the upper left corner



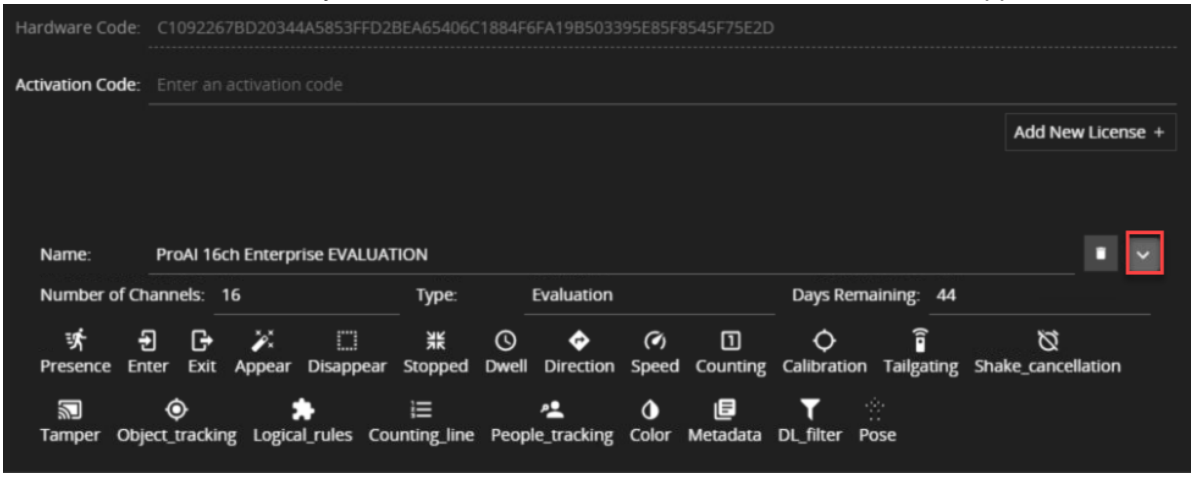

4. Select **Licenses**




5. Paste the license, which you have received from Mirasys to the **Activation Code field**
6. Click **Add New License**

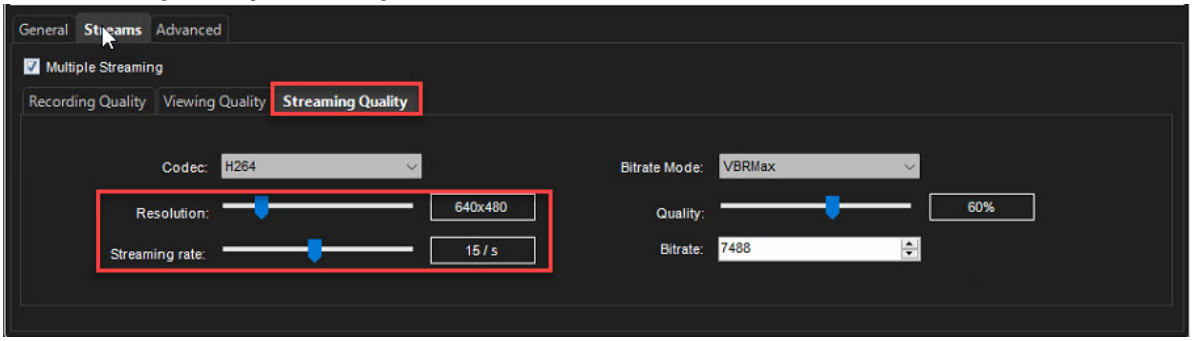



7. When the license is added, you will see overall information about the license and supported features




### 15.6.3.3 Setting up the resolution and record rate

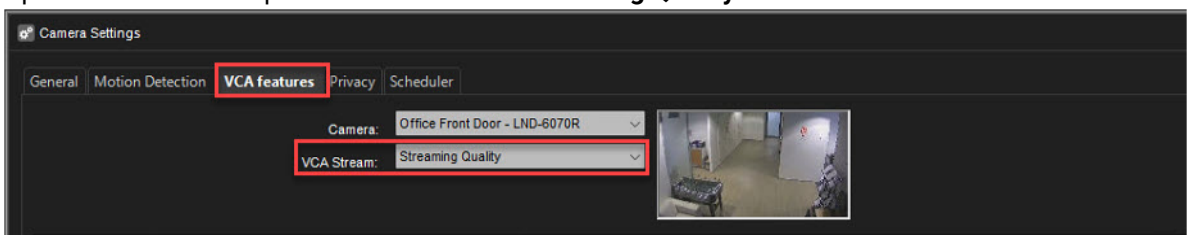
1. Enable **Multiple Streaming** to the cameras which are used for the Mirasys VCA
2. Set **Streaming Quality** resolution to **640x480**
3. Set **Streaming Quality** Streaming rate to **15/s**




### 15.6.3.4 Selecting VCA Stream

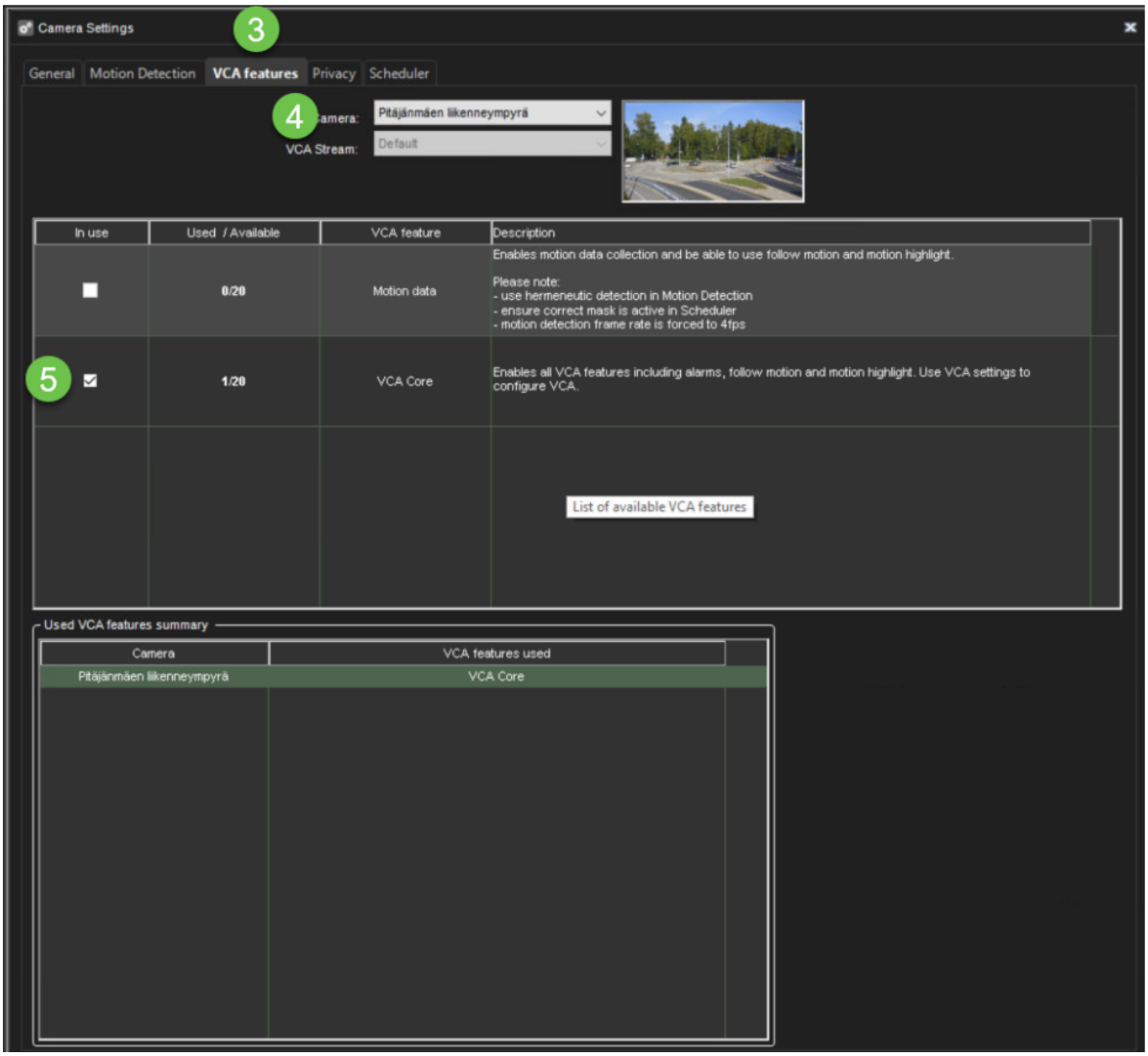
1. Open **VCA Features** tab

2. Select camera from the list
3. Open **VCA Stream** dropdown list and select **Streaming Quality**




### 15.6.3.5 Activating VCA Core for the cameras

1. Go to the **VMS servers tab**
2. Open **Cameras**
3. Select **VCA features**
4. Select camera
5. Enable **In use**
6. Click **OK**




## 15.6.4 Supported operating systems

Mirasys use third party solution for VCA which is integrated to Mirasys VMS.

Offically supported operating system are

- Windows 10
- Ubuntu 18.04

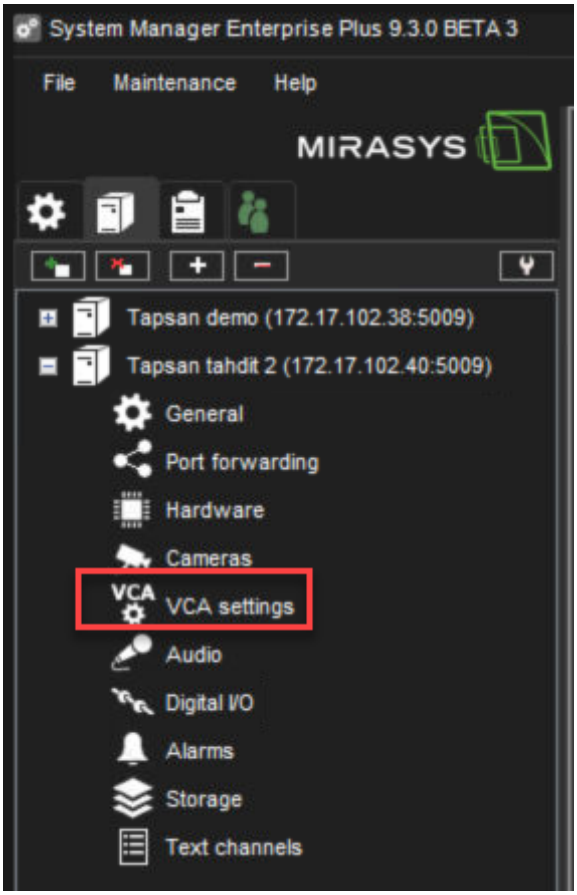
With these operating system you get best performance out.

You can still use any other newer operating system or server operating system for Mirasys VMS server.

## 15.6.5 VCA Settings on System Manager

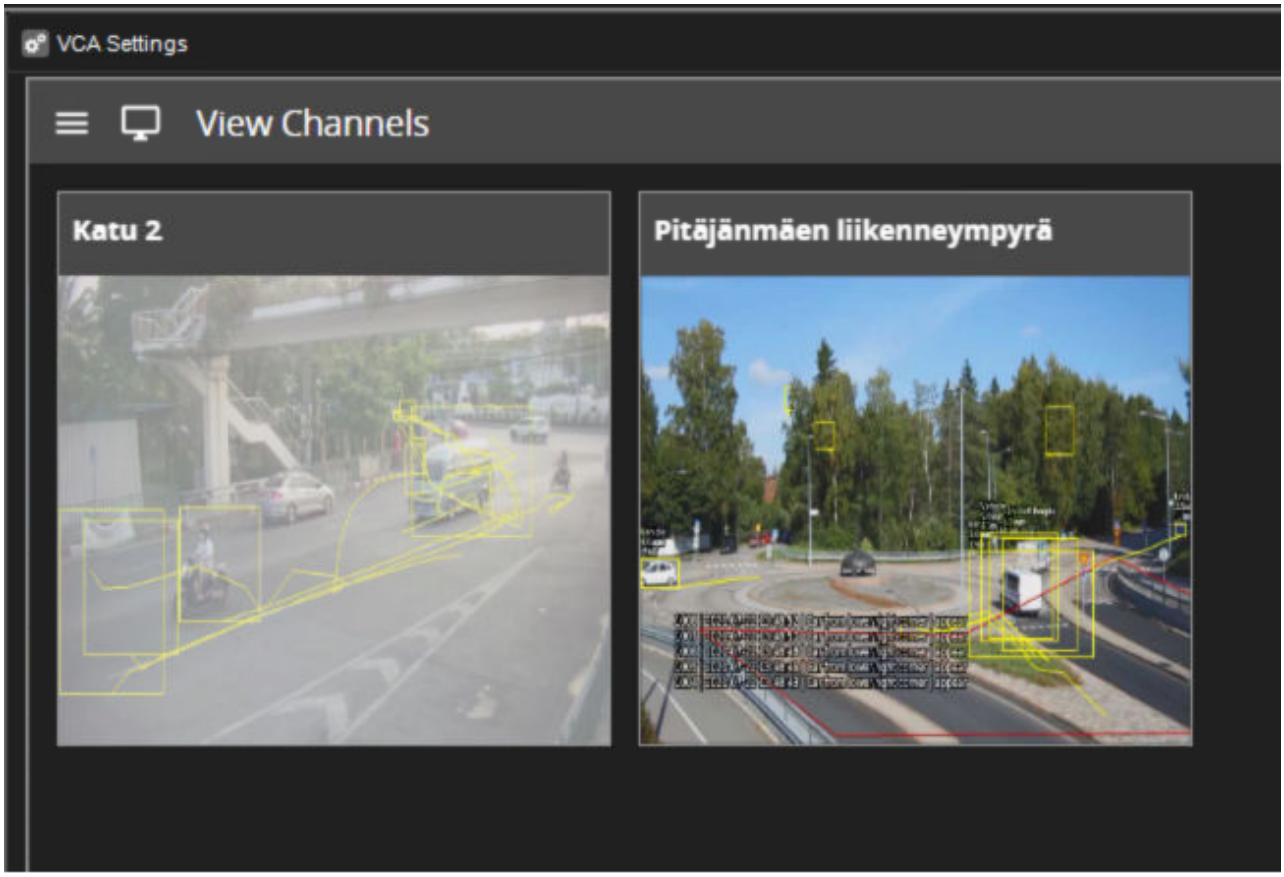
1. Go to the **VMS Server** tab

2. Open **VCA Settings**



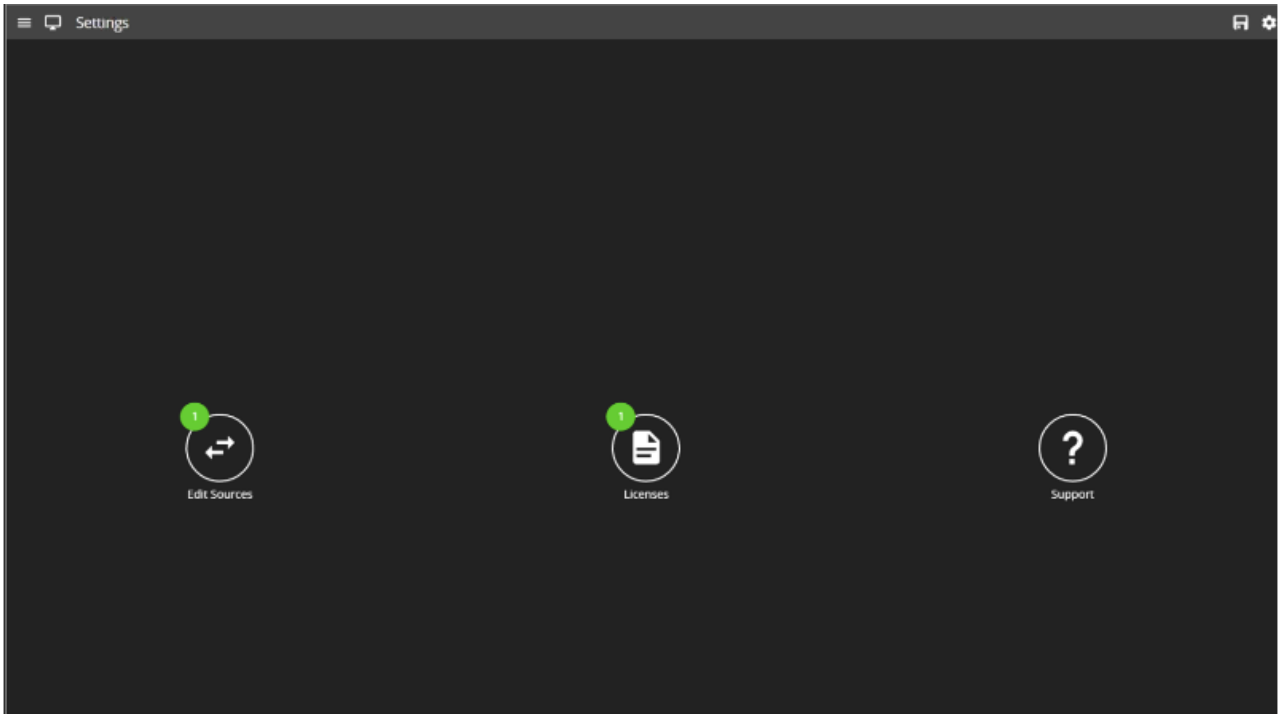

### 15.6.5.1 View Channels

View Channels show all cameras, which **VCA Core** is enabled.



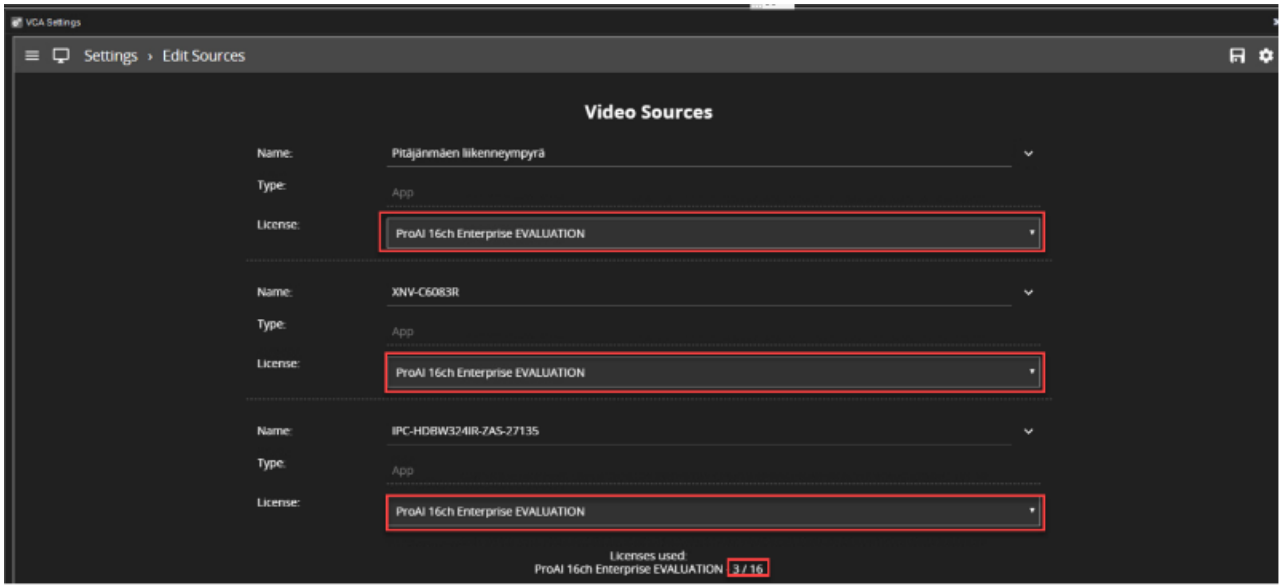

### 15.6.5.2 Settings

- Edit Sources
- Licenses
- Support



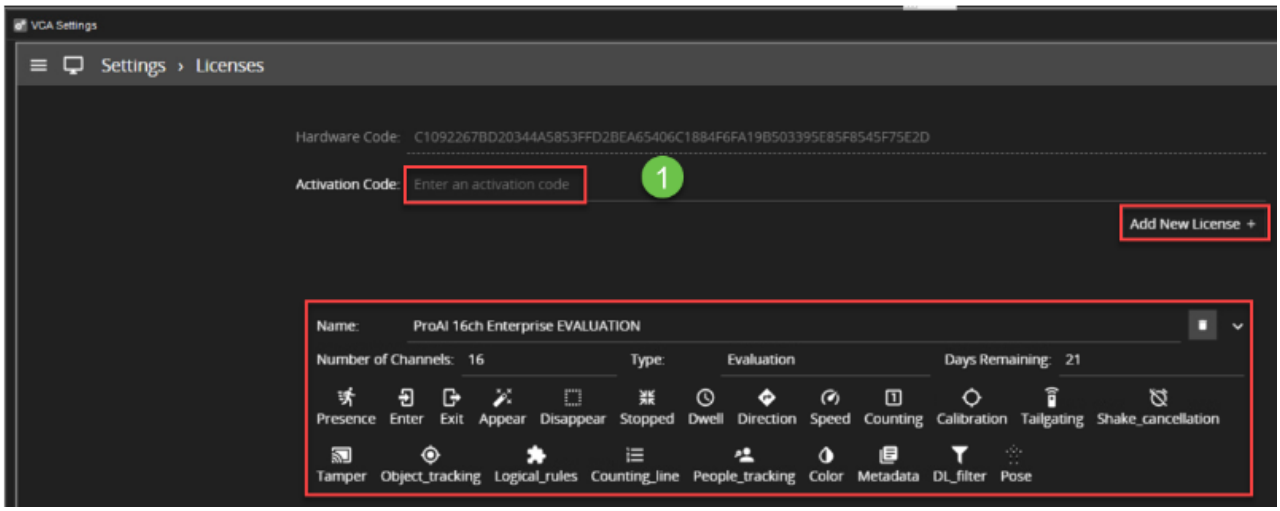

### 15.6.5.3 Edit Sources

Edit Sources shows which cameras have been used for the VCA Core.
Users can also see the type of the VCA license and how many channels have been used for the VCA license.



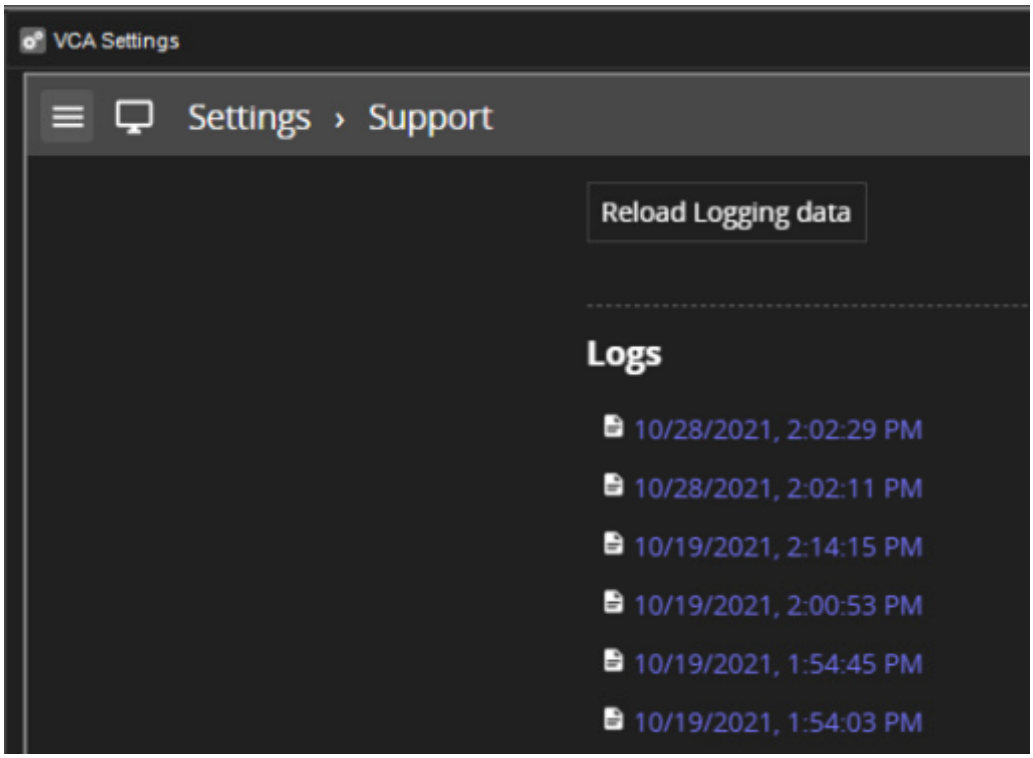

### 15.6.5.4 Licenses

Licenses show existing license type and that features
Users can add more VCA licenses




#### 15.6.5.5 Support

Support show logs from the Mirasys VCA and users can download logs




### 15.6.6 Mirasys VCA Deep Learning

#### 15.6.6.1 Requirements

- Nvidia GPU with CUDA cores

    - A NVIDIA GPU with CUDA Compute Capability 7.5 or higher
    - Depending on GPU CUDA cores, how many Deep Learning channels you can use on the system
- The latest NVIDIA graphics drivers (at least 460.73 or higher).
- CUDA Toolkit
- Mirasys VMS 9.4 or newer
- Deep Learning object files

### 15.6.6.2 Installation

1. Install latest Nvidia drivers to the system
2. Download **Mirasys VCA Deep Learning** package from Mirasys Extranet
3. Extract the package
4. Browse to folder **CUDA Toolkit**
5. Install **CUDA Toolkit** with all features
    a. You can find detailed installation guide here[8].
    b. Some features are not installed because Microsoft Visual Studio is not needed to install but the toolkit is providing example files
    c. If you have installed already Mirasys VMS, before copying files VMS services need to stop
6. Stop services: **WDServer**, **DVRServer** and **SMServer**
    a. This is not needed to do if you are using V9.6 or newer
7. Copy the content of the **VCA Deep Learning file**s folder to **C:\Program Files\DVMS\DVR\vca\bin** location
    a. This is not needed to do if you are using V9.6 or newer

This path is the default installation location of Mirasys VMS
If you have installed Mirasys VMS to another location, copy files there

1. Start **WDServer**, **DVRServer** and **SMServer** services
    a. This is not needed to do if you are using V9.6 or newer

Now you have installed and are ready to go with Deep Learning tracking (see page 370).

Licensing is done via local VCA Deep Learning licensing or using License Server (Virtual Environment or if you want to handle licenses in one place).

> Some cases detection may not work correctly. Please try to increase image quality or move/zoom camera image to closer wanted detection area.
> Models are trained using clear images and some cases when using black/white image or thermal camera image this may cause that detection is working correctly. For this you can try use Deep Learning Filter with Object Tracker.

8 https://documentation.mirasys.com/frequently-asked-questions/faq/how-to-install-nvidia-cuda-toolkit

## 15.6.7 Mirasys VCA License Server

This license server allows the use of VCA in virtual machine/s or if you want to handle licensing in one place for all servers. For this, you need to install Mirasys VCA License Server to physical hardware and license it. This server can then share licenses to virtual machine/s.

This feature is supported by 9.4 forward.

Do not install any other services to license server. This can cause issues on licensing side.

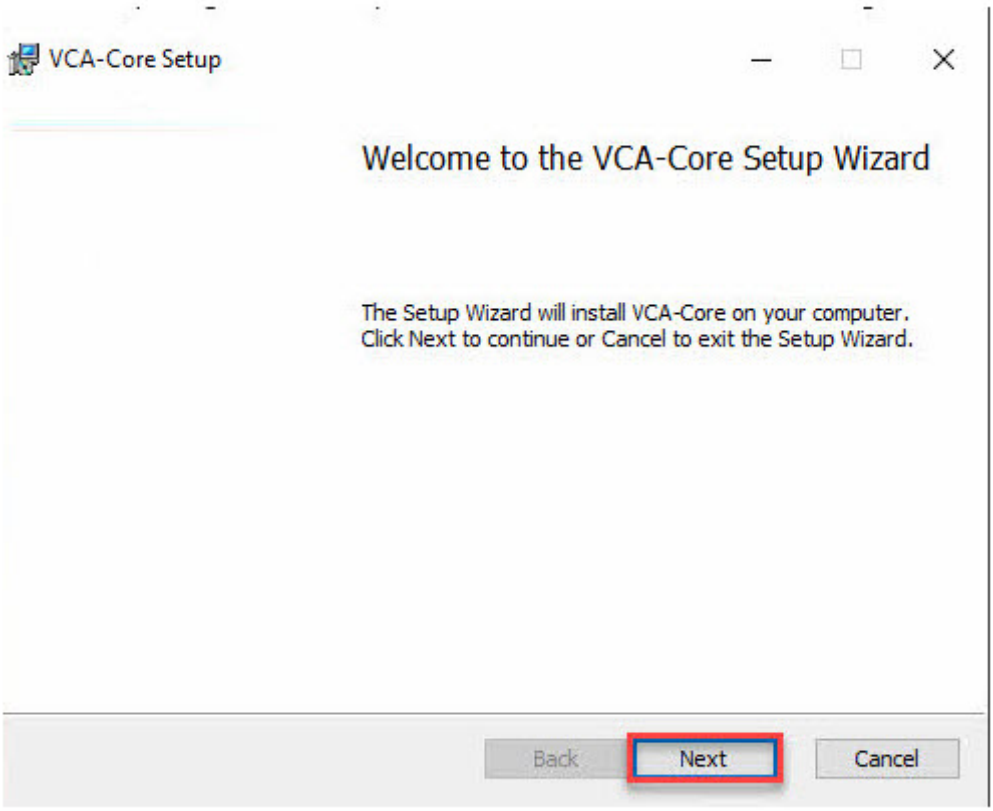
You don’t need install VCA License Server if you are using example Master as License Server and this is physical server. On this case VMS include VCA and you can install licenses via System Manager - VCA Settings. Then connect each servers to this Master IP-address.

### 15.6.7.1 Port

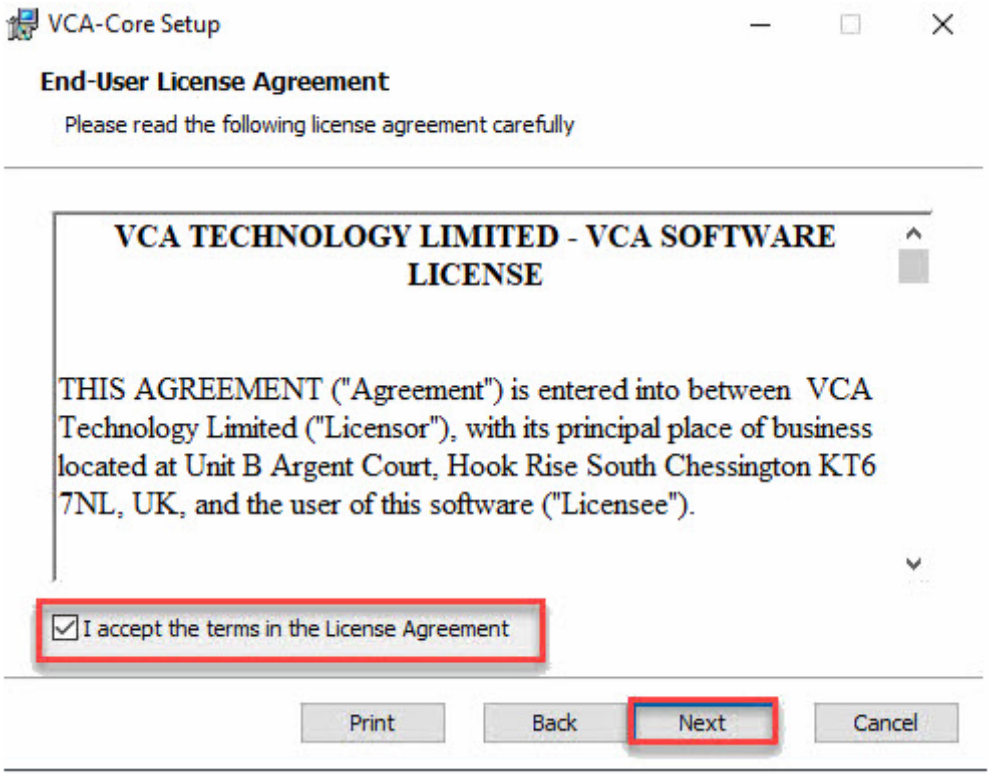
- 8080, TCP for VCA License Server Management
- 15769, TCP for VCA License Port

### 15.6.7.2 Installation

1. Download the latest Mirasys VCA License Server package from Mirasys Extranet.
2. Extract ZIP-package on the wanted place and start installation double-clicking installation file
3. Click **Next** to proceed




4. Accept **End-User License Agreement** and click **Next**

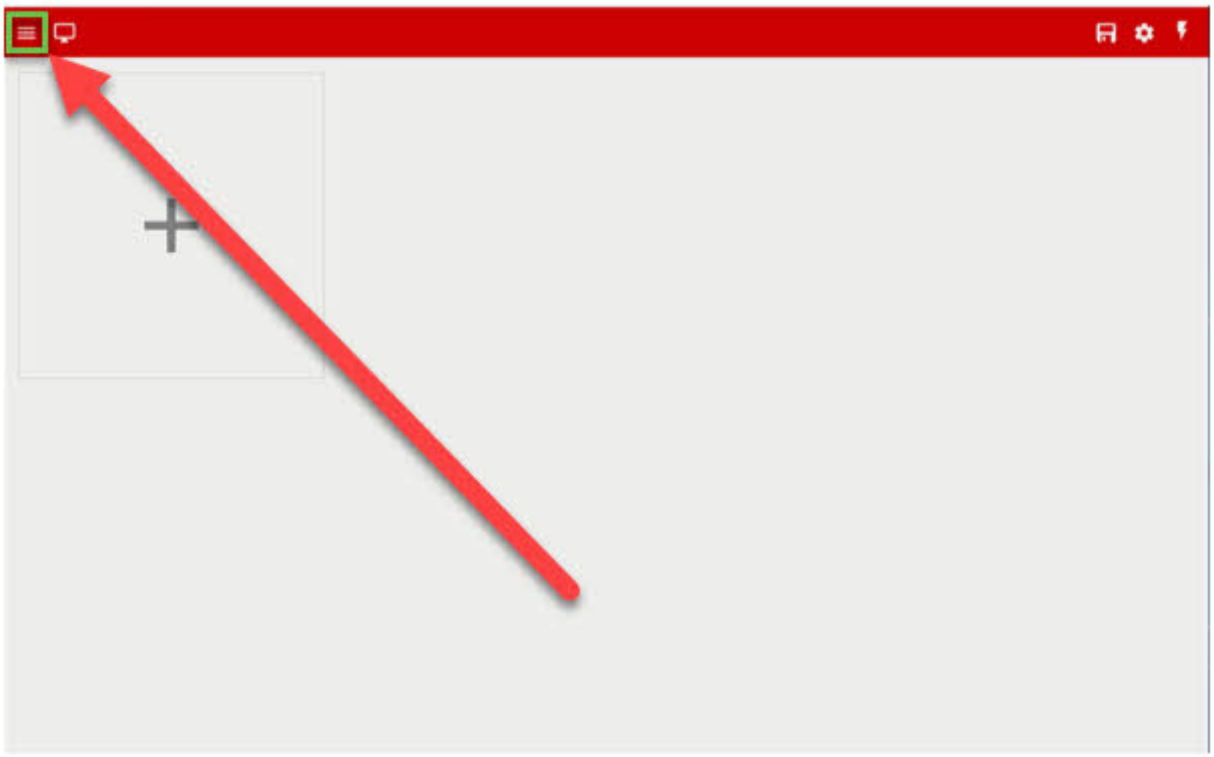


5. Follow instructions until the installation is finalized

### 15.6.7.3 Usage and licensing

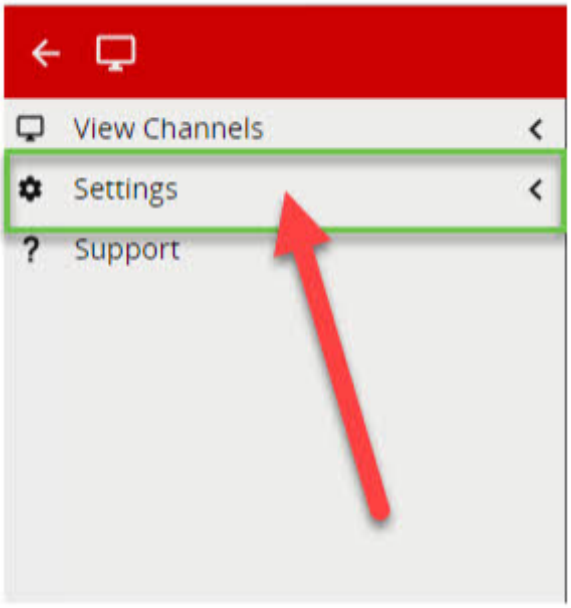
To log in to Mirasys VCA License Server, you need to use the browser and go to the site http://localhost:8080/.
The default username is **admin,** and the default password is **admin**

#### 15.6.7.3.1 On the main page, you can access settings via the burger menu.

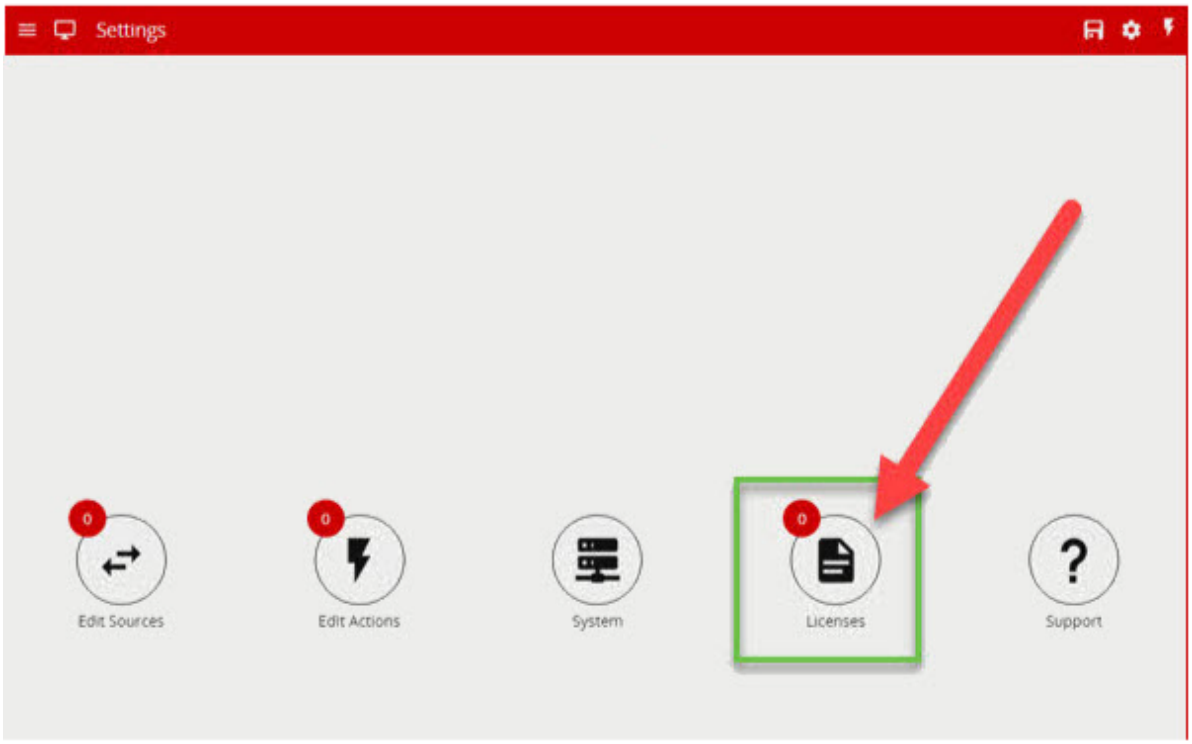


#### 15.6.7.3.2 Adding the license

1. Open **Settings**

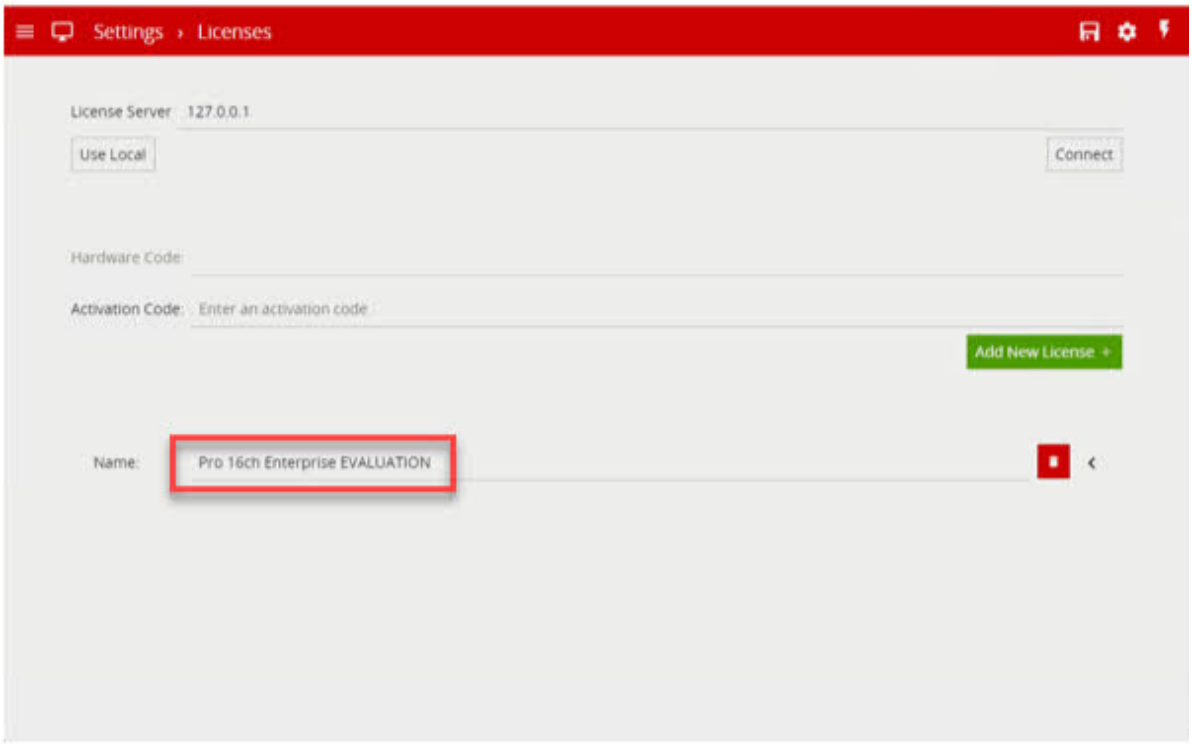



2. Open **Licenses**



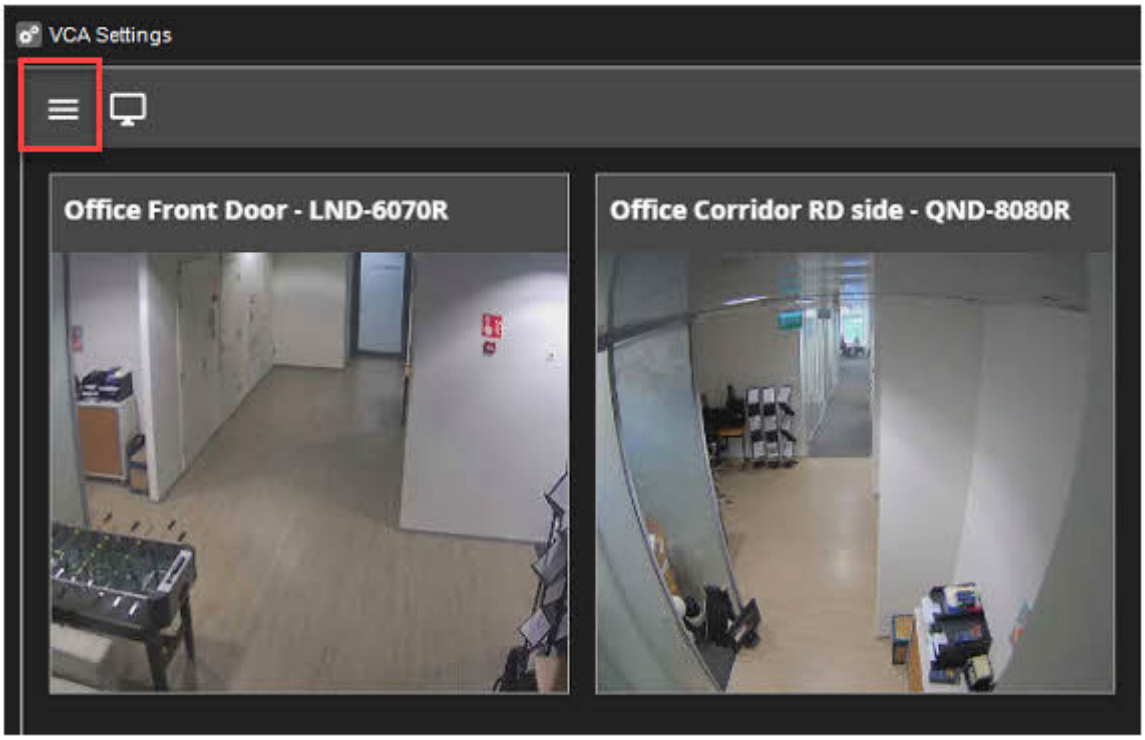

3. Copy Hardware Code and send it to Mirasys to receive license details.
4. When you have received the activation code from Mirasys, paste the code to the **Activation Code** field and click **Add the new license**


5. When you have added wanted licenses or licenses to the system, you can proceed on Mirasys VMS side.

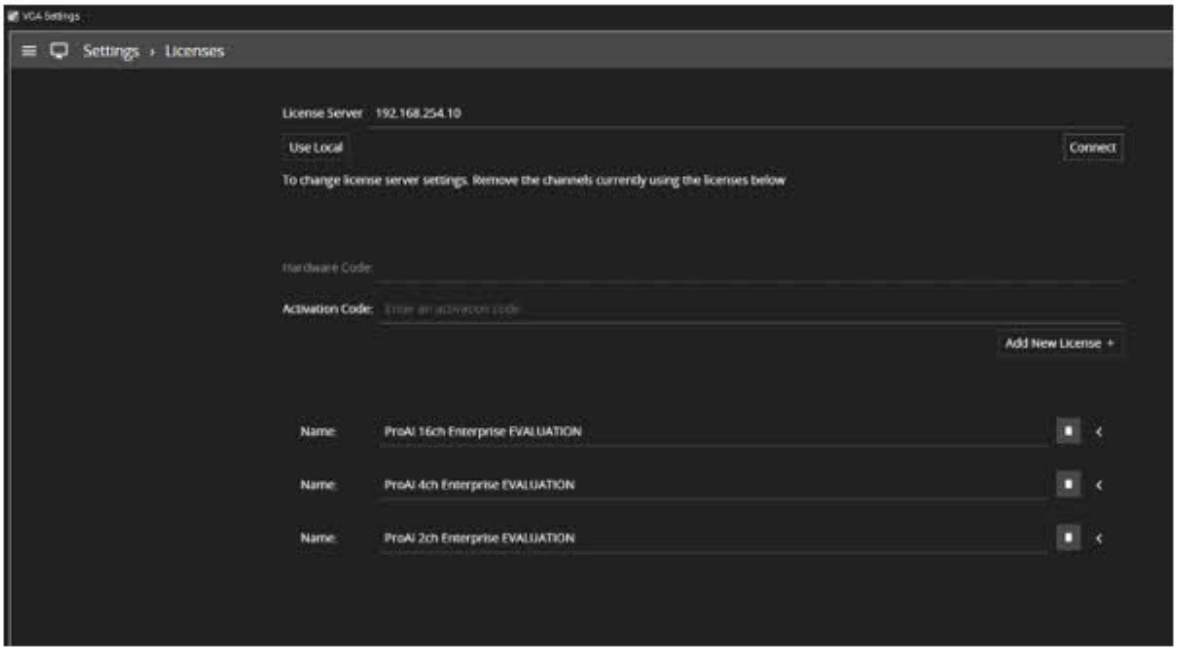


### 15.6.7.4 Mirasys VMS Configuration

1. Open System Manager, go to the server section and select VCA Settings.
2. This opens a new window to find a similar burger menu like earlier.




3. Under this menu, you can find Settings to tell license server address DNS/IP-address.

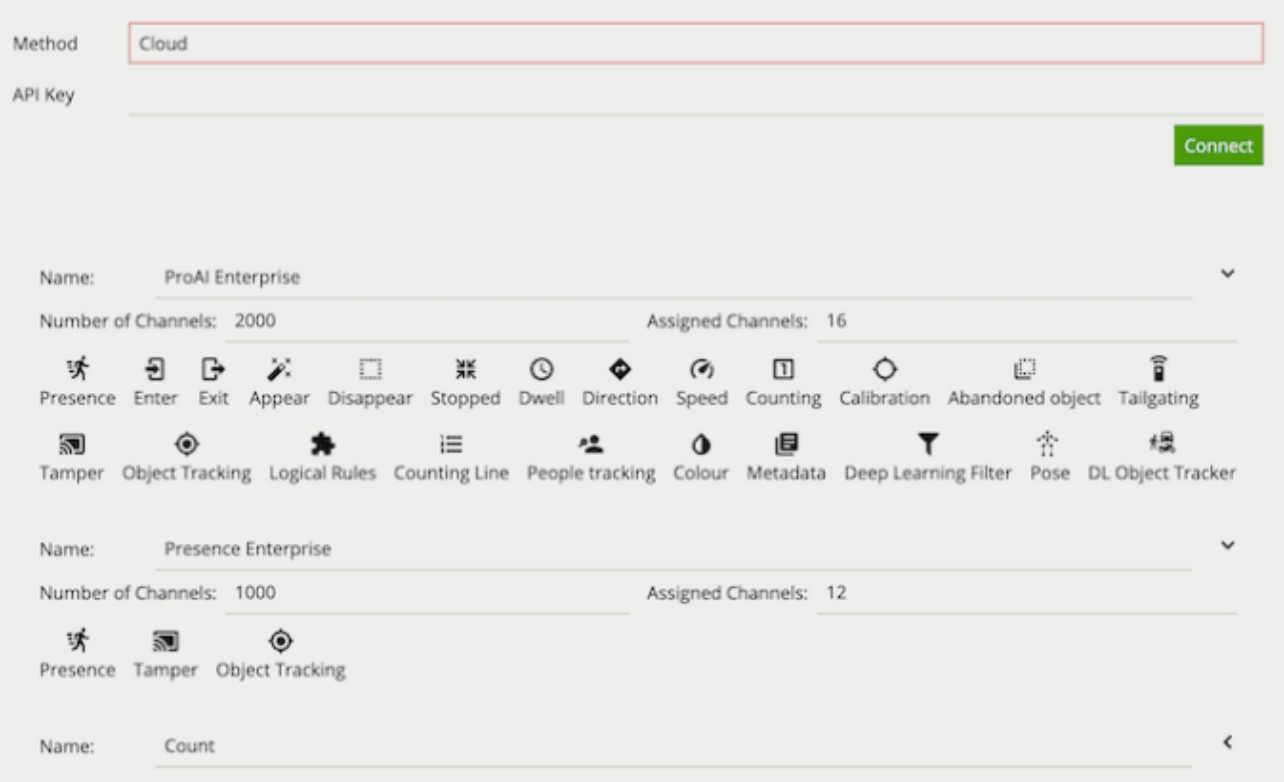


4. When you have to fill License Server address, you can click Connect to this.

If the connection is made successfully, this shows Mirasys VCA License Server licenses.

After this, you can go to VCA Settings and sources to assign a wanted license to the wanted camera channel.

## 15.6.8 Cloud Licensing




Once a valid API Key is provided and the connection to the Cloud Licensing Server is established, the license pool associated with that API key will be shown.

When using Cloud Licensing the license pool available to VCAserver is managed using a cloud portal.

- **Method:** Switches between Cloud Licensing or a License Server.
- **API Key:** An authorization token that links to a Cloud Licensing Account.
- **Connect:** Connects this instance of VCAserver to the Cloud Licensing Servers.
- The list of installed licenses and their features are displayed underneath.

On new installations, before a user is able to add sources, the Cloud Licensing account will need a license added to the license pool.

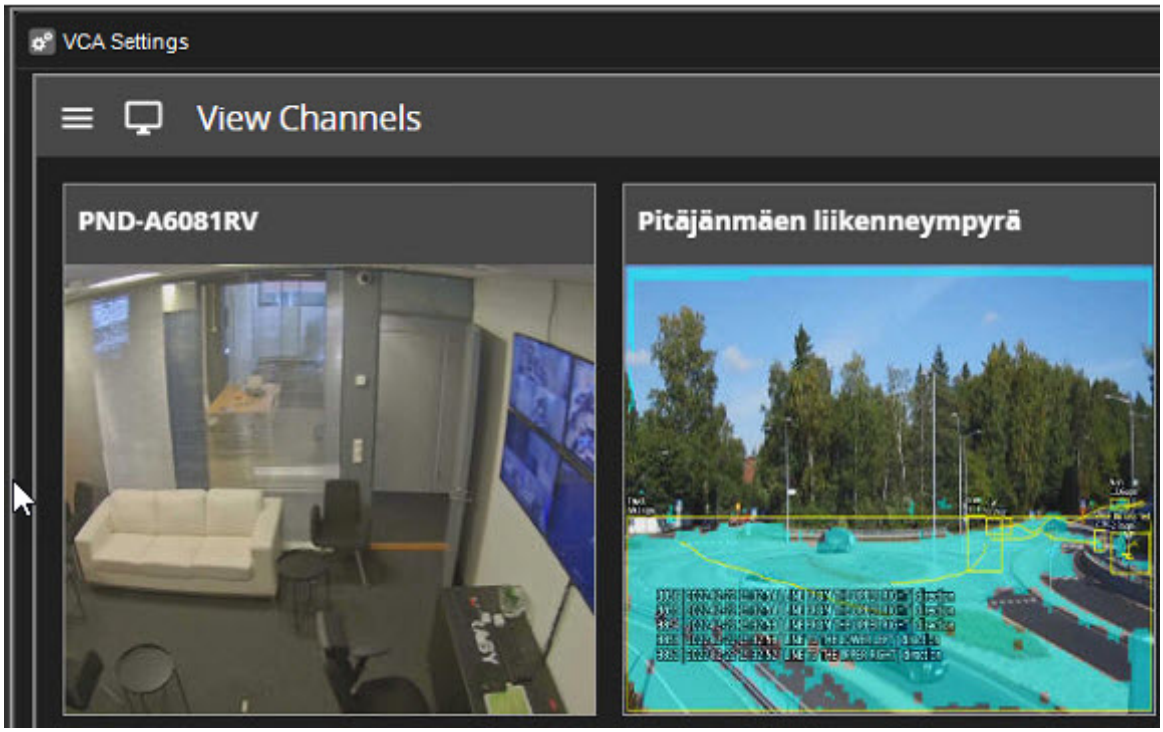
## 15.6.9 VCA Channel Settings

VCA Channel Settings contains all configuration related to video channels, where VCACore is enabled.

- Tracking
- Zones
- Calibration

- Classification
- Burnt-in Annotation
- Rules
- Video Preview
- Deep-Learning

You can open under VCA Settings wanted camera by clicking it.




- VCA Tracking (see page 370)
- VCA Deep Learning Skeleton Tracker (see page 377)
- VCA Hand Object Interaction Tracker (see page 377)
- VCA Zones (see page 378)
- VCA Calibration (see page 381)
- VCA Classification (see page 388)
- VCA Burnt-in Annotation (see page 390)
- VCA Rules (see page 392)
- VCA - Deep-Learning Filter (see page 433)

## 15.6.9.1 VCA Tracking

### 15.6.9.1.1 Initialization

When a tracker is selected by the user, an initialization phase will be required. This will vary based on the selected tracker.

**Object Tracker**: when selected the tracker will need to 'learn the scene' to determine background from moving foreground objects.

Whilst learning the scene the following message will be displayed in the live view, and no objects will be tracked during this time.

**DL People Tracker & DL Object Tracker**: when first selected, the DL engine will run a model generation process. This optimizes the DL models to run on the available GPU hardware.

Irrespective of which tracker is selected, the DL People tracker model, DL Object Tracker model and the DL Filter model will all be optimized in one go.

This process can take up to 10 minutes per model and may increase with different GPU configurations. Once complete the optimized models are stored in the configuration folder.

The process will not need to be run again unless the GPU hardware is changed. Whilst optimization is performed a message will be displayed in the live view, and no objects will be tracked during this time.

Please note: The DL Filter requires the same initialization process but does not display a message.

Once initialized, VCAserver will begin analyzing the video stream with the selected tracker. Settings specific to that tracker will also be displayed below the tracker engine selection option.

Regardless of the tracker selected, any tracked object can be passed through the available rules. However, in some cases, certain rules or algorithms will only be available with a specific tracker.
For example, Deep Learning Filter and the abandoned and removed object rules are only available with the Object Tracker.

#### 15.6.9.1.2 Object Tracker

The Object Tracker is a motion based detection engine. Based on changes detected in the image, the algorithm separates the image into foreground and background, tracking any foreground object that is moving above a set threshold. The Object Tracker has the following settings:

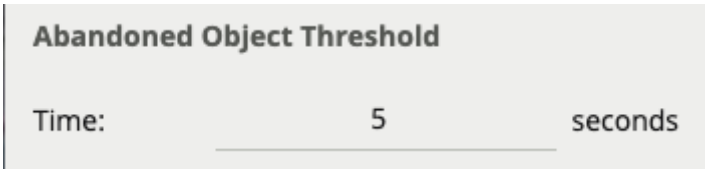
##### 15.6.9.1.2.1 Stationary Object Hold-on Time

The Stationary Object Hold-on Time defines the amount of time an object will be tracked by the engine once it becomes stationary.
Since objects which become stationary must be "merged" into the scene after some finite time, the tracking engine will forget about objects that have become stationary after the Stationary Object Hold-on Time.


The default setting is 60 seconds.

##### 15.6.9.1.2.2 Abandoned / Removed Object Threshold

This threshold amount of time an object must be classed as abandoned or removed before an Abandoned / Removed rule will trigger.

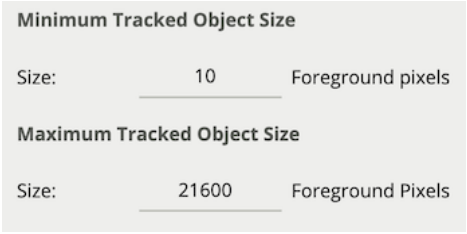


The default setting is 5 seconds.

#### 15.6.9.1.2.3 Minimum Tracked Object Size

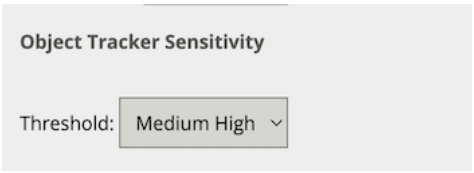
The **Minimum Tracked Object Size** defines the size of the smallest object that will be considered for tracking.

For most applications, the default setting of 10 is recommended. In some situations, where extra sensitivity is required, the value can be manually specified.
While lower values allow the engine to track smaller objects, it may increase the susceptibility to false detections.




#### 15.6.9.1.2.4 Object Tracker Sensitivity

The **Object Tracker Sensitivity** value allows the object tracker to be tuned to ignore movement below a certain threshold.
Combined with the Blob Map burnt in annotation, which visualizes the area of the scene the object tracker is detecting movement, this value can be adjusted to filter out environmental noise.




The default setting is 4.

#### 15.6.9.1.2.5 Scene Change Detection (Object Tracker)

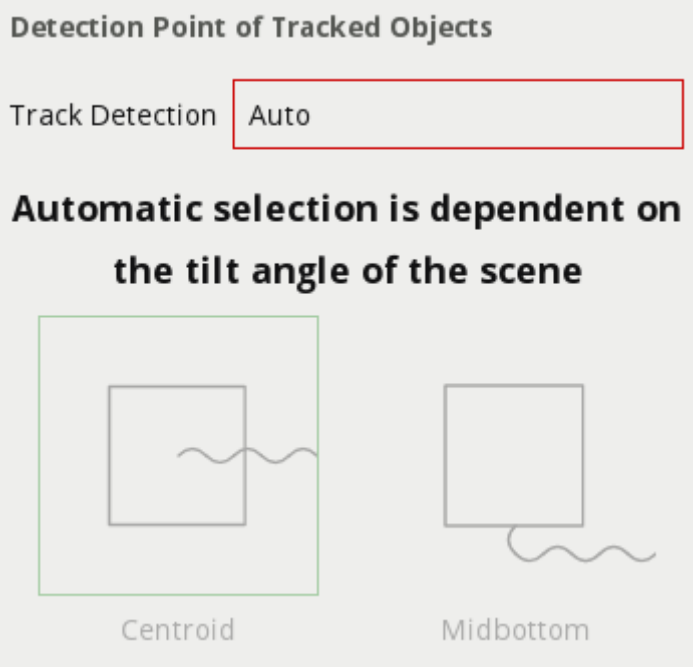
Learn more about Scene Change Detection.

#### 15.6.9.1.2.6 Detection Point of Tracked Objects

For every tracked object, a point is used to determine the object's position, and evaluate whether it intersects a zone and triggers a rule. This point is called the detection point.
There are 3 modes that define the detection point relative to the object:

##### Automatic

In automatic mode, the detection point is automatically set based on how the channel is configured.
It selects 'Centroid' if the camera is calibrated overhead, or 'Mid-bottom' if the camera is calibrated side-on or not calibrated.




**Centroid**

In this mode, the detection point is forced to be the centroid of the object.

**Mid-bottom**

In this mode, the detection point is forced to be the middle of the bottom edge of the tracked object. Normally this is the ground contact point of the object (where the object intersects the ground plane).

#### 15.6.9.1.2.7 Tamper Detection (Object Tracker)

Learn more about Tamper Detection.

#### 15.6.9.1.2.8 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

### 15.6.9.1.3 Deep Learning People Tracker

The Deep Learning People tracker is designed to track people in situations where the camera field of view is relatively close.
The Deep Learning People Tracker is based on Pose Estimation technology, providing the location of a person in the field of view as well as additional key point metadata on the parts of the body.
See Deep Learning Requirements for hardware requirements for this algorithm.

The Deep Learning People Tracker has the following settings:

#### 15.6.9.1.3.1 Tamper Detection (DLPT)

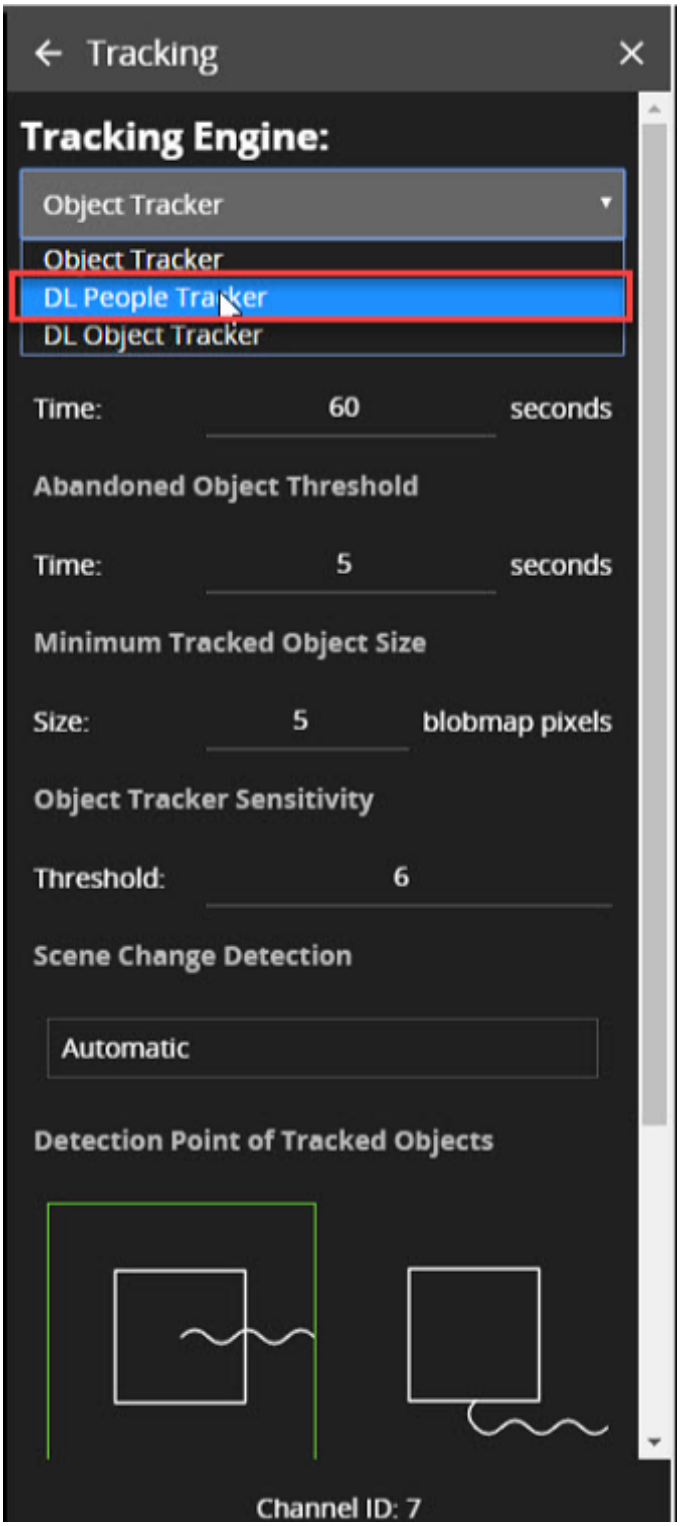
Learn more about Tamper Detection.

#### 15.6.9.1.3.2 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

#### 15.6.9.1.3.3 Enabling DL People Tracker

1. Open **View Channels**
2. Select the camera
3. Open **Tracking**
4. Open **Tracking Engine** dropdown box and select **DL People Tracker**


Tracking
Tracking Engine:
Object Tracker
Object Tracker
DL People Tracker
DL Object Tracker
Time: 60 seconds
Abandoned Object Threshold
Time: 5 seconds
Minimum Tracked Object Size
Size: 5 blobmap pixels
Object Tracker Sensitivity
Threshold: 6
Scene Change Detection
Automatic
Detection Point of Tracked Objects
Channel ID: 7

#### 15.6.9.1.4 Deep Learning Object Tracker

The Deep Learning Object Tracker is designed for accurate detection and tracking of people, vehicles and key objects in challenging environments where motion based tracking methods would struggle.
The list of objects detected by the Deep Learning Object Tracker is given below:

| Class Name | Description |
|---|---|
| `person` | A person, or tracked object with a person present (e.g bicycle) |
| `motorcycle` | A motorcycle |
| `bicycle` | A bicycle |
| `cyclist` | Person riding a bicycle, can be reported as two separate objects |
| `bus` | A bus |
| `car` | A car |
| `van` | A van, including mini-vans and mini-buses |
| `truck` | A truck, including lorries and commercial work vehicles, |
| `forklift` | A forklift truck |
| `bag` | A backpack or holdall (sports bag) |
| | |

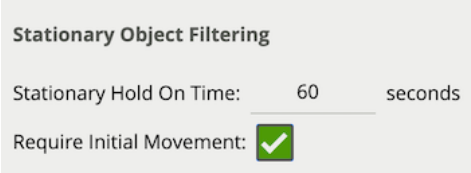
The Deep Learning Object Tracker is based on a classification and detection model, providing the location of an object in the field of view. See Deep Learning Requirements for hardware requirements for this algorithm.

The Deep Learning Object Tracker has the following settings:

#### 15.6.9.1.4.1 Stationary Object Filtering

See Stationary Hold On Time

In addition to the `Stationary Hold On Time`, an additional setting `Require Initial Movement`, is available which will prevent objects which have not moved from being tracked.




#### 15.6.9.1.4.2 Detection Point of Tracked Objects

See Detection Point of Tracked Objects

#### 15.6.9.1.4.3 Tamper Detection (DLOT)

Learn more about Tamper Detection.

#### 15.6.9.1.4.4 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

### 15.6.9.2 VCA Deep Learning Skeleton Tracker

The Deep Learning Skeleton tracker tracks people in situations where the camera field of view is relatively close.

The Deep Learning Skeleton Tracker is based on Pose Estimation technology, providing the location of a person in the field of view as well as additional key point metadata on the parts of the body. See Deep Learning Requirements (see page 361) for hardware requirements for this algorithm.

The Deep Learning Skeleton Tracker has the following settings:

#### 15.6.9.2.1 Tamper Detection (DLST)

Learn more about Tamper Detection (see page 459).

### 15.6.9.3 VCA Hand Object Interaction Tracker

The Hand Object Interaction (HOI) Tracker is designed for the detection of hands, and the objects they hold. The HOI tracker requires a top down and relatively close field of view to detect optimally. The list of objects detected by the Hand Object Interaction Tracker is given below:

| Class Name | Description |
|---|---|
| hand | A hand |
| object | An object being held by a hand object |

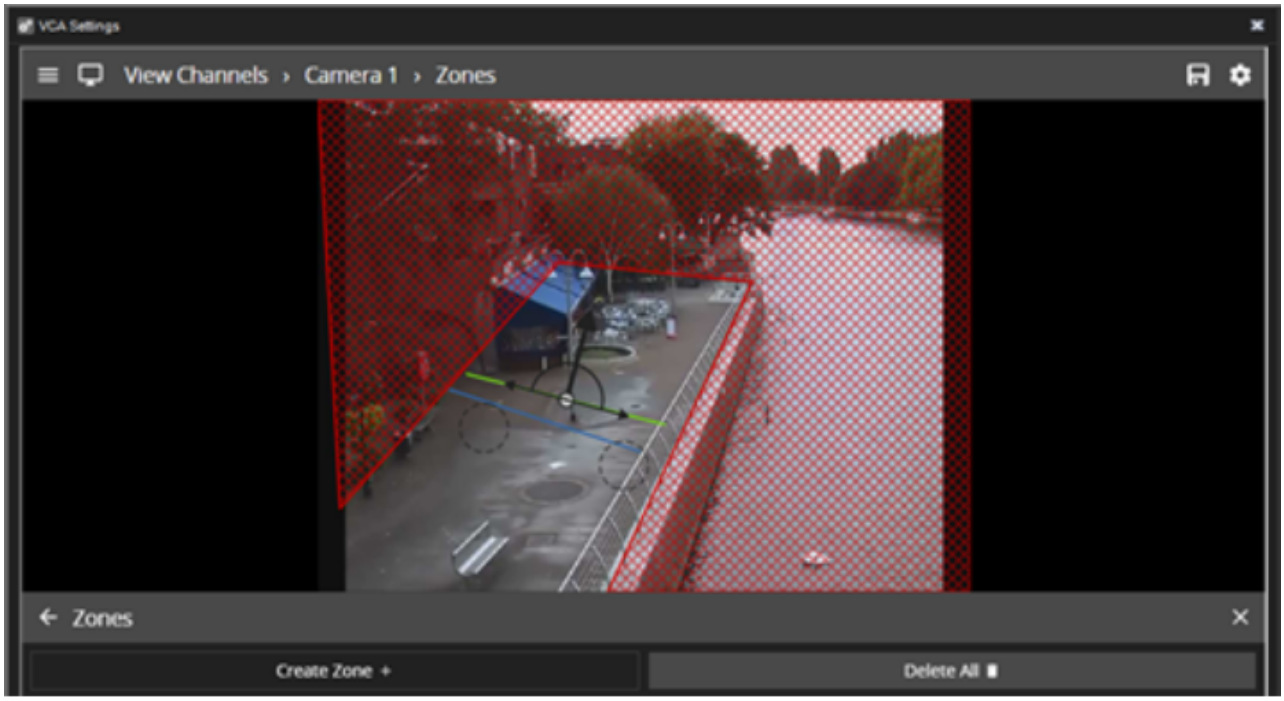
The Hand Object Interaction Tracker is based on a classification and detection model, providing the location of an object in the field of view. See Deep Learning Requirements (see page 361) for hardware requirements for this algorithm.

The Hand Object Interaction Tracker has the following settings:

- Detection Point of Tracked Objects (HOI)
- Tamper Detection (HOI)
- Loss Of Signal Emit Interval (HOI)

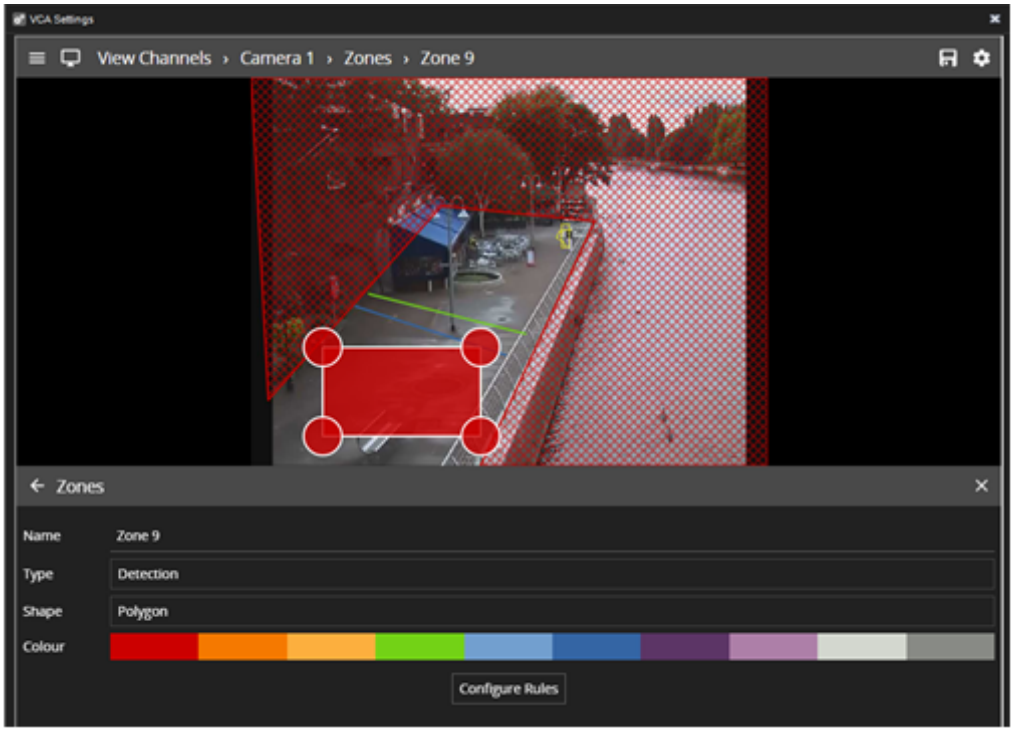
## 15.6.9.4 VCA Zones

Zones are the detection areas on which VCAcore operate.
To detect a specific behaviour, a zone must be configured to specify the area where a rule applies.




### 15.6.9.4.1 Zone specific settings

The zone configuration menu contains a range of zone-specific configuration parameters:




- **Name** The name of the zone, which appears in event notifications.
- **Type:** The type of the zone. Can be one of:
- **Detection**: A zone that detects tracked objects and to which rules can be applied.
- **Non-detection:** A zone that specifies an area that should be excluded from VCAcore analysis.
    - Objects are not detected in non-detection zones.
    - Useful for excluding areas of potential nuisance alarms from a scene (e.g. waving trees, flashing lights, etc).
- **Shape**: The shape of the zone. Can be one of:
    - **Polygon:** A polygonal detection area with at least three nodes. Rules apply to the whole area.
    - **Line:** A single- or multi-segment line with at least two nodes. Rules apply to the length of the line.
- **Colour:** The colour of the zone.
- **Configure Rules:** A shortcut button to navigate directly to the r[9]ules configuration page

#### 15.6.9.4.2 Adding a zone

#### 15.6.9.4.3 Zones can be added in multiple ways:

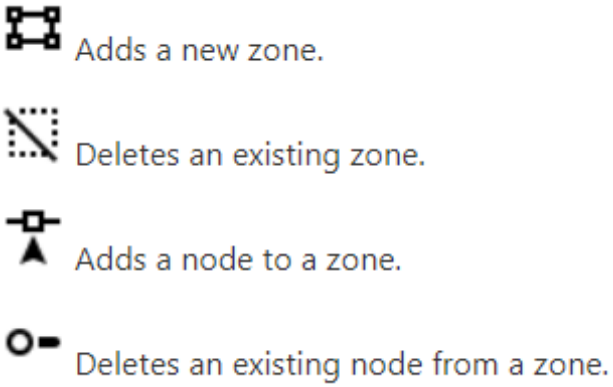
1. Double-click anywhere on the video display.
2. Click the Create Zone button in the zone settings menu.
3. Right-click or tap-hold to display the context menu and select the add zone icon

9 https://documentation.mirasys.com/articles/src/rules.md

### 15.6.9.4.3.1 The context menu

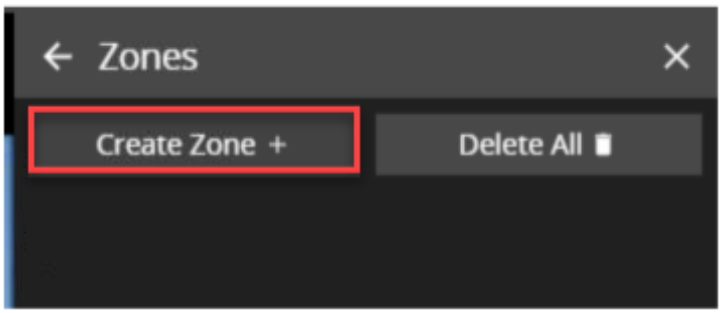
Right-clicking or tap-holding (on mobile devices) displays a context menu that contains commands specific to the current context.

**The possible actions from the context menu are:**



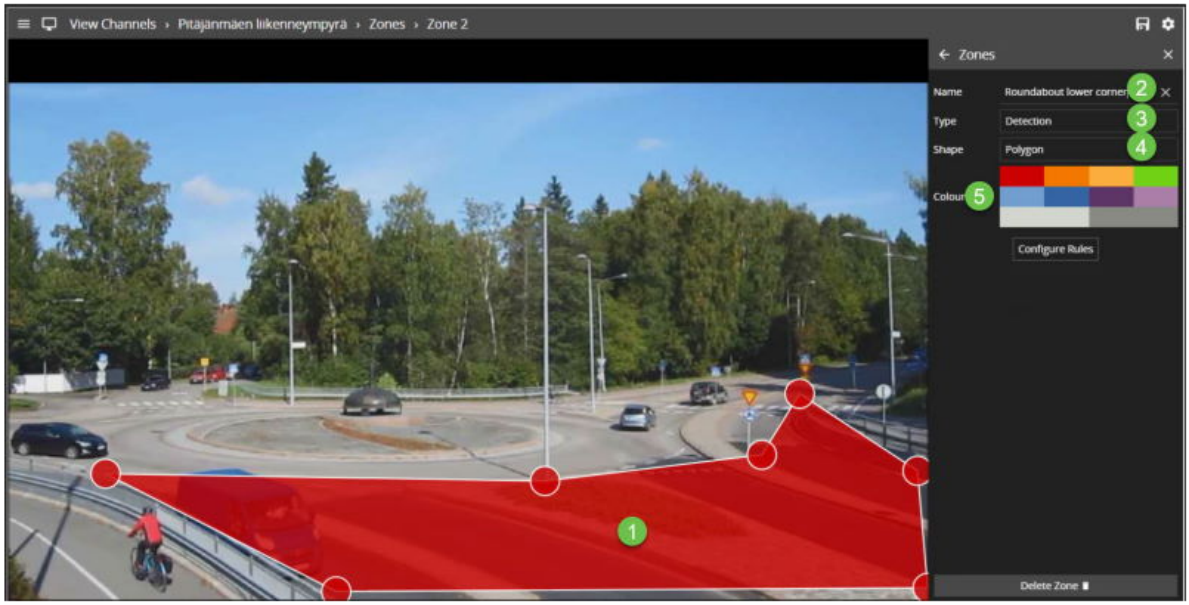

### 15.6.9.4.3.2 Creating a zone

Click **Create Zone** icon




1. Draw zone and set the location to the image

2. Set name of the zone
3. Set detection type
4. Set shape
5. Define color




#### 15.6.9.4.4 Positioning zones

To change the position of a zone, click and drag the zone to a new position. To change the shape of a zone, drag the nodes to create the required shape. New nodes can be added by double-clicking on the edge of the zone or clicking the add node icon  from the context menu.

#### 15.6.9.4.5 Deleting the zone

Zones can be deleted in the following ways:

- Select the zone and click the Delete Zone button from the zone settings menu.
- Select the zone, display the context menu and select the delete zone icon

### 15.6.9.5 VCA Calibration

Camera calibration is required in order for VCAcore to classify objects into different object classes. Once a channel has been calibrated, VCA Core can infer real-world object properties such as speed, height and area and classify objects accordingly.

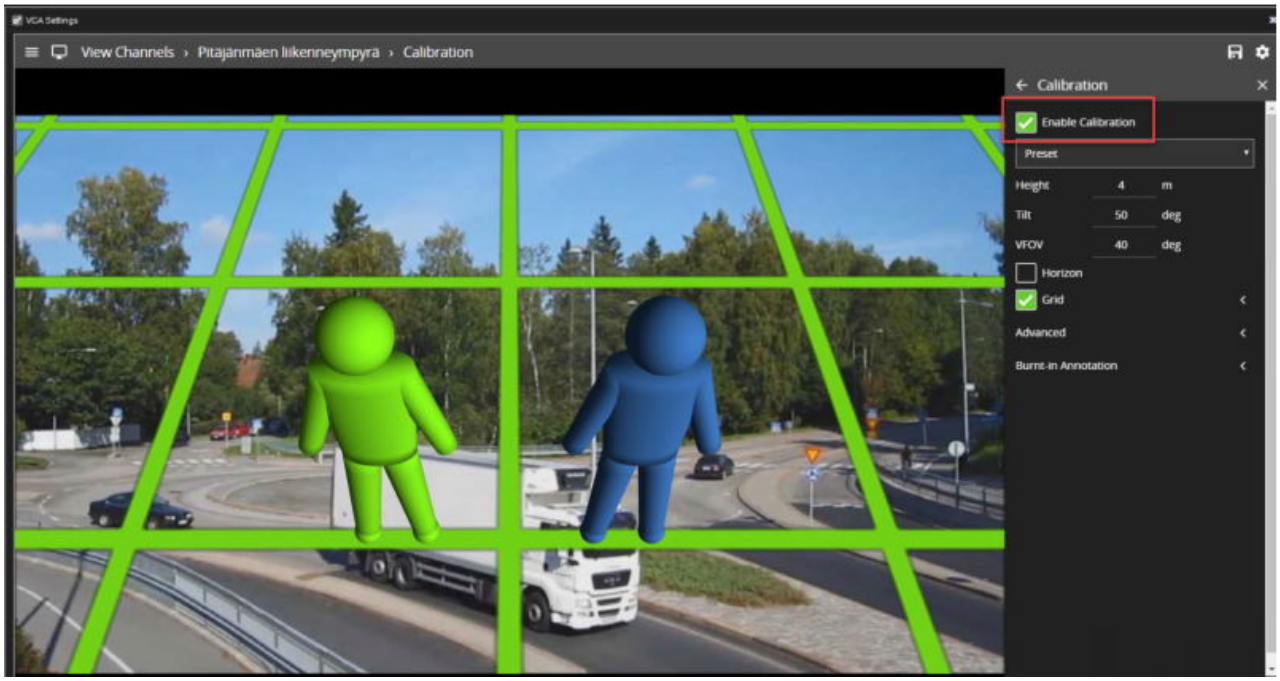
Calibration is not needed to do when using Deep Learning tracking, only when using normal VCA or Deep Learning Filter.

### 15.6.9.5.1 Camera calibration is split into the following sub-topics:

1. Enabling Calibration
2. Calibration Controls
3. Calibrating a Channel
4. Advanced Calibration Parameters

### 15.6.9.5.2 Enabling Calibration

By default calibration is disabled.
To enable calibration on a channel, check the **Enable Calibration** checkbox.




#### 15.6.9.5.2.1 Calibration Controls

**3D Graphics Overlay**

During the calibration process, the features in the video image need to be matched with a 3D graphics overlay.
The 3D graphics overlay consists of a green grid that represents the ground plane.
Placed on the ground plane are a number of 3D mimics (people-shaped figures) that represent the dimensions of a person with the current calibration parameters.
The calibration mimics are used for verifying the size of a person in the scene and are 1.8 metres tall.
The mimics can be moved around the scene to line up with people (or objects which are of a known, comparable height) to a person.

#### Mouse Controls

The calibration parameters can be adjusted with the mouse as follows:

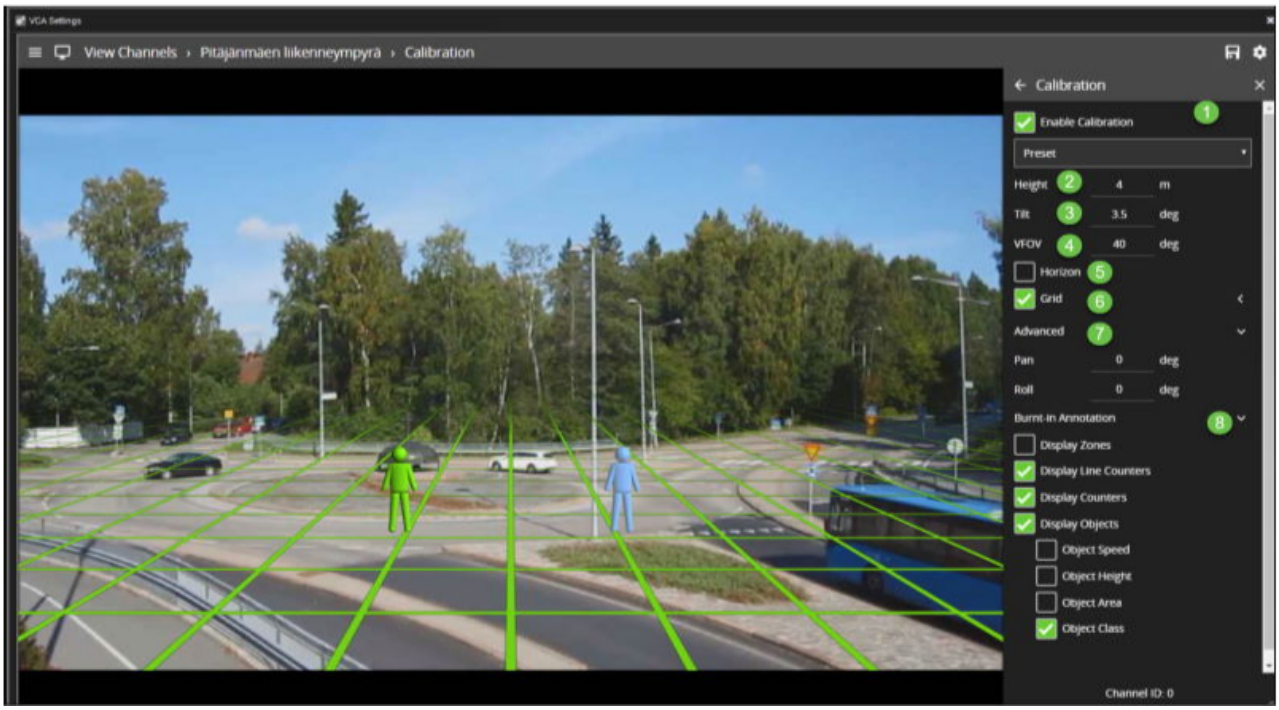
- Click and drag the ground plane to change the camera tilt angle.
- Use the mouse wheel to adjust the camera height. - Drag the slider to change the vertical field of view.

**Note**: The sliders in the control panel can also be used to adjust the camera tilt angle and height.

#### Control Panel Items

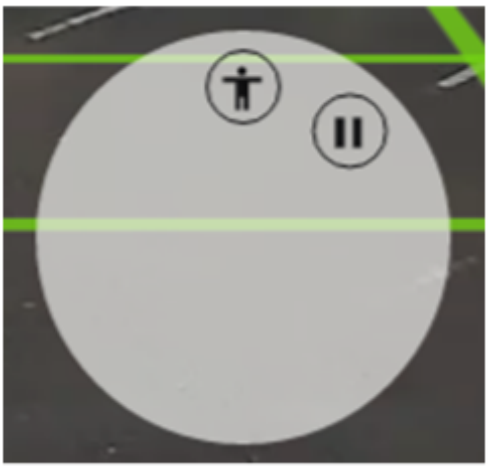
The control panel (shown on the right-hand side in the image above) contains the following controls:

1. **Height**: Adjusts the height of the camera
2. **Tilt**: Adjusts the tilt angle of the camera
3. **VFOV**: Adjusts the vertical field of view of the camera. Note: A correct value for the vertical camera field of view is essential for accurate calibration and classification.
4. **Horizon**: Enables/disables the horizon display. Useful to line up against a horizon in a deep scene.
5. **Grid**: Enables/disables the ground plane grid display. The expand/collapse control (<) exposes additional settings to vary the colour, opacity and size of the ground plane grid.
6. **Advanced**: Exposes advanced settings for controlling the pan and roll of the camera.
7. **Burnt-in Annotation**: Exposes the Burnt-in Annotation controls for convenience.

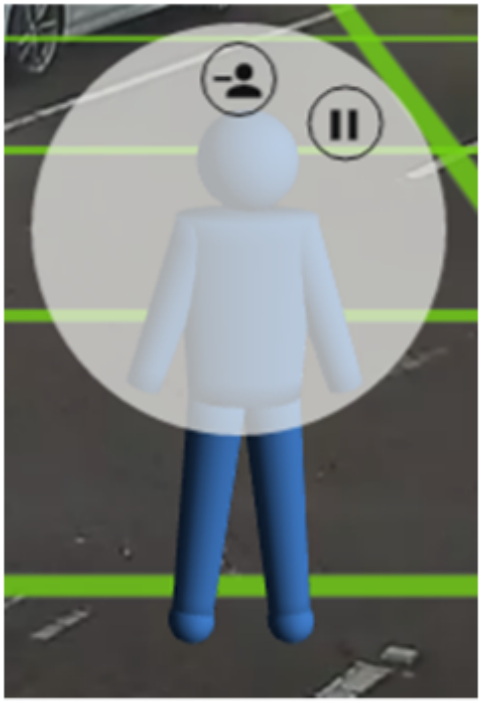



#### Context Menu Items

Right-clicking the mouse (or tap-and-hold on a tablet) on the grid displays the context menu:



Performing the same action on a mimic display the mimic context menu:



The possible actions from the context menu are:

- Pause the video. Pausing the video can make it easier to align mimics up with objects in the scene.
- Re-starts playing the video after it was previously paused.
- Adds an extra mimic to the ground plane.
- Removes the currently selected mimic from the ground plane.

### 15.6.9.5.3 Calibrating a Channel

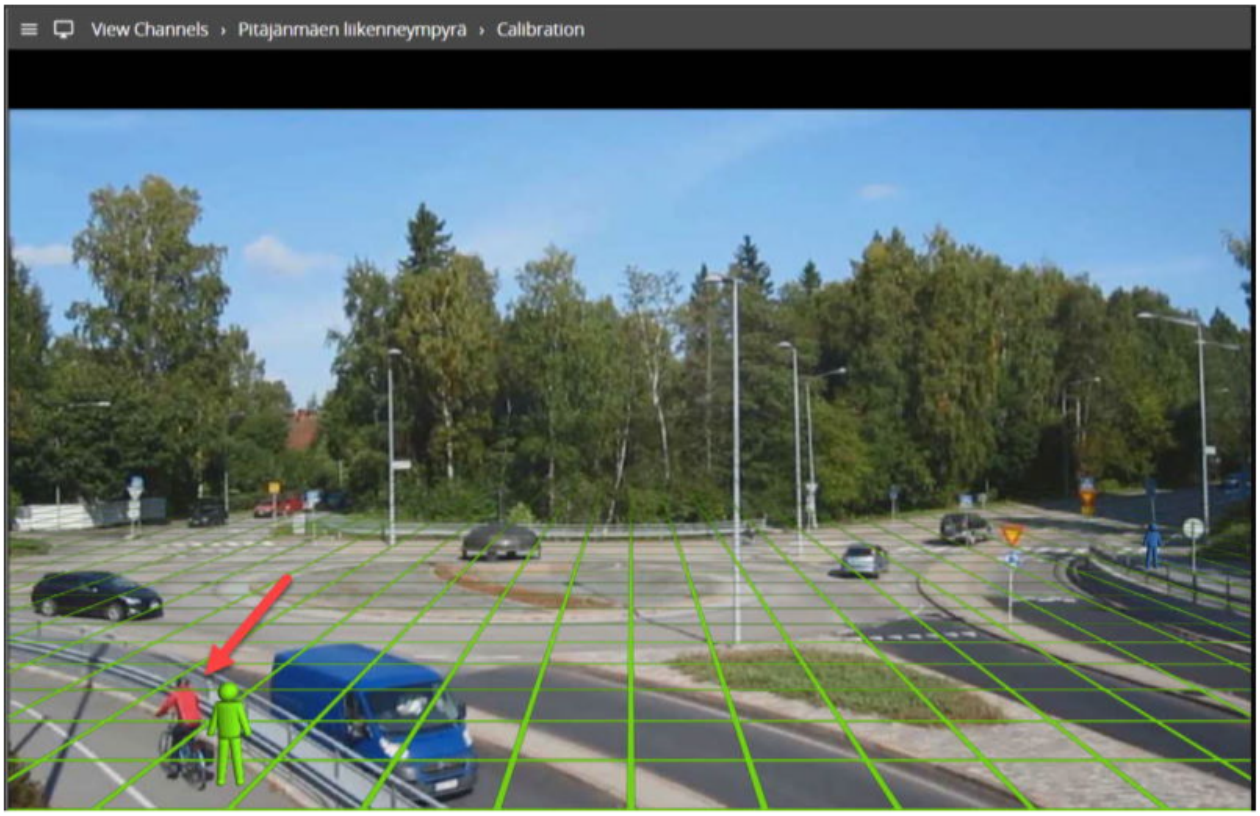
Calibrating a channel is necessary in order to estimate object parameters such as height, area, speed and classification.

If the height, tilt angle and vertical field of view corresponding to the installation are known, these can simply be entered as parameters in the appropriate fields in the control panel.

If however, these parameters are not explicitly known this section provides a step-by-step guide to calibrating a channel.

#### 15.6.9.5.3.1 Step 1: Find People in the Scene

Find some people or some people-sized objects in the scene.
Try to find a person near the camera, and a person further away from the camera.
It is useful to use the play/pause control to pause the video so that the mimics can be accurately placed.
Place the mimics on top of or near the people:




#### 15.6.9.5.3.2 Step 2: Enter the Camera Vertical Field of View

Determining the correct vertical field of view is important for accurate calibration.
The following table shows pre-calculated values for the vertical field of view for different sensor sizes.

| | Focal Length(mm) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 15 | 20 | 30 | 40 | 50 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| CCD Size (in) | CCD Height(mm) | | | | | | | | | | | | | | | |
| 1/6" | 1.73 | 82 | 47 | 32 | 24 | 20 | 16 | 14 | 12 | 11 | 10 | 7 | | | | |
| 1/4" | 2.40 | 100 | 62 | 44 | 33 | 27 | 23 | 19 | 17 | 15 | 14 | 9 | 7 | | | |
| 1/3.6" | 3.00 | 113 | 74 | 53 | 41 | 33 | 28 | 24 | 21 | 19 | 12 | 11 | 9 | 6 | | |
| 1/3.2" | 3.42 | 119 | 81 | 59 | 46 | 38 | 32 | 27 | 24 | 21 | 16 | 13 | 10 | 7 | | |
| 1/3" | 3.60 | 122 | 84 | 62 | 48 | 40 | 33 | 29 | 25 | 23 | 20 | 14 | 10 | 7 | 5 | |
| 1/2.7" | 3.96 | 126 | 89 | 67 | 53 | 43 | 37 | 32 | 28 | 25 | 22 | 15 | 11 | 8 | 6 | |
| 1/2" | 4.80 | 135 | 100 | 77 | 62 | 51 | 44 | 38 | 33 | 30 | 27 | 18 | 14 | 9 | 7 | 5 |
| 1/1.8" | 5.32 | 139 | 106 | 83 | 67 | 56 | 48 | 42 | 37 | 33 | 30 | 20 | 15 | 10 | 8 | 6 |
| 2/3" | 6.60 | | 118 | 95 | 79 | 67 | 58 | 50 | 45 | 40 | 37 | 25 | 19 | 13 | 9 | 8 |
| 1" | 9.60 | | 135 | 116 | 100 | 88 | 77 | 69 | 62 | 56 | 51 | 35 | 27 | 18 | 14 | 11 |
| 4/3" | 13.50 | | | 132 | 119 | 107 | 97 | 88 | 80 | 74 | 68 | 48 | 37 | 25 | 19 | 15 |

If the table does not contain the relevant parameters, the vertical FOV can be estimated by viewing the extremes of the image at the top and bottom.

Note that without the correct vertical FOV, it may not be possible to get the mimics to match people at different positions in the scene.

#### 15.6.9.5.3.3 Step 3: Enter the Camera Height

If the camera height is known, type it indirectly. If the height is not known, estimate it as far as possible and type it indirectly.

#### 15.6.9.5.3.4 Step 4: Adjust the Tilt Angle and Camera Height

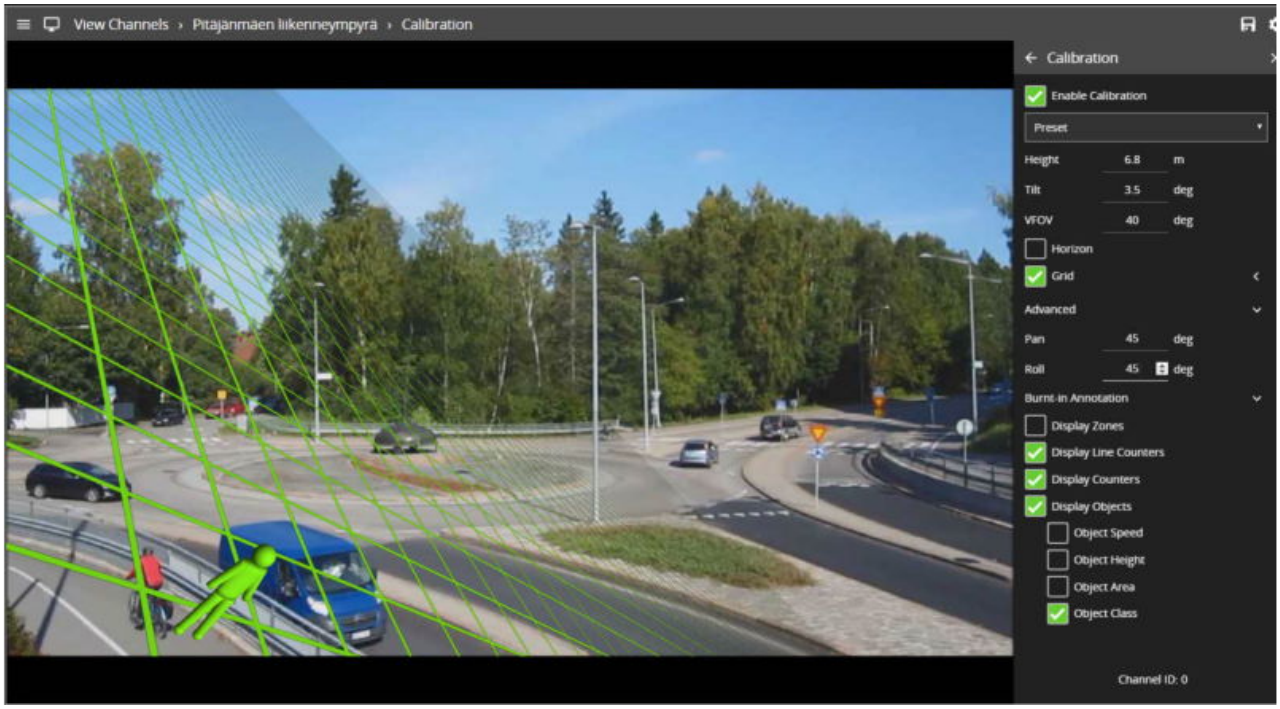
Adjust the camera tilt angle (and height if necessary) until both mimics are approximately the same size as a real person at that position in the scene.
Click and drag the ground plane to change the tilt angle and use the mouse wheel or control panel to adjust the camera height.
The objective is to ensure that mimics placed at various locations on the grid line up with people or people-sized- objects in the scene.
Once the parameters have been adjusted, the object annotation will reflect the changes and classify the objects accordingly.

#### 15.6.9.5.3.5 Step 5: Verify the Setup

- Once the scene is calibrated, drag or add mimics to different locations in the scene and verify they appear at the same size/height as a real person would.
- Validate that the height and area reported by the VCAcore annotation look approximately correct.
- Note that the burnt-in -annotation settings in the control panel can be used to enable and disable the different types of annotation.
- Repeat step 4 until the calibration is acceptable.

### 15.6.9.5.4 Advanced Calibration Parameters

The advanced calibration parameters allow the ground plane to be panned and rolled without affecting the camera calibration parameters.
This can be useful to visualize the calibration setup if the scene has a pan or roll with respect to the camera.



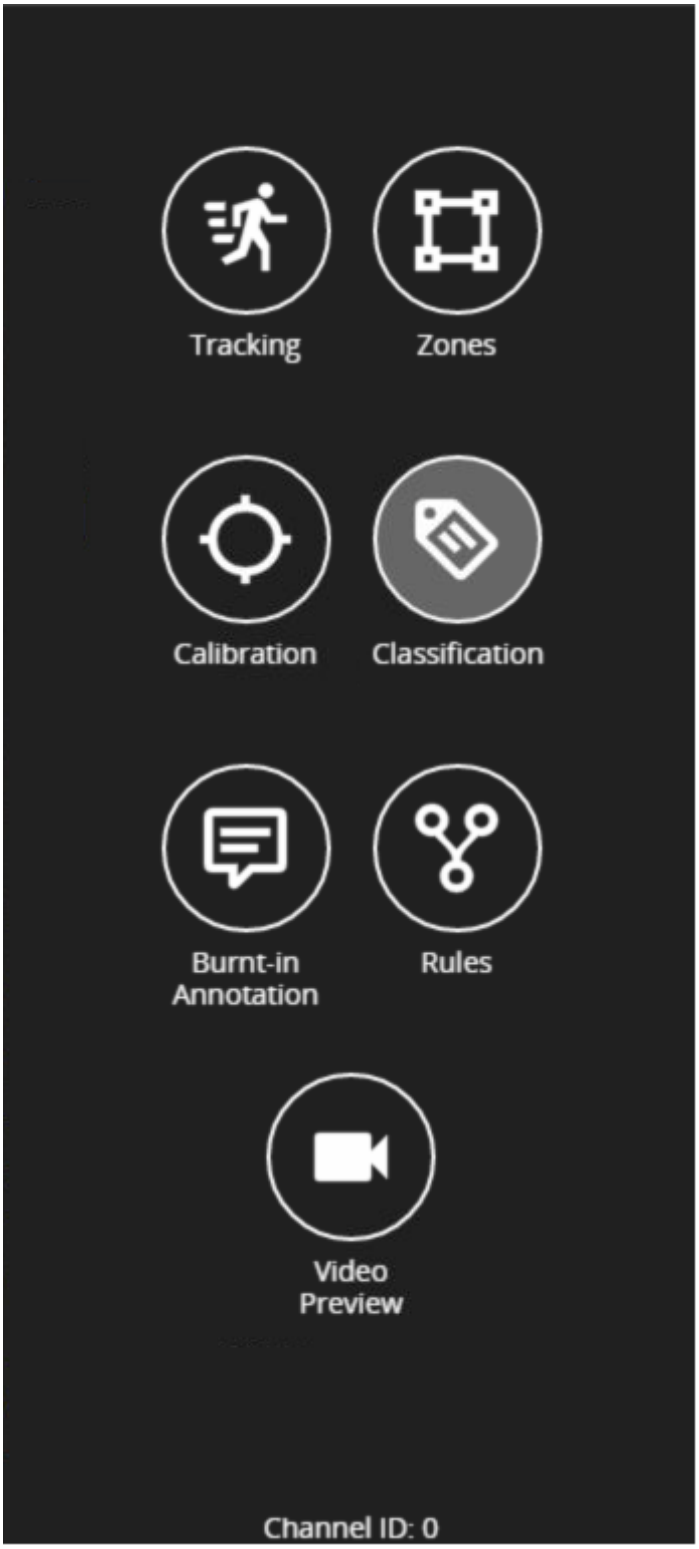

**Note:** the pan and roll advanced parameters only affect the orientation of the 3D ground plane so that it can be more conveniently aligned with the video scene, and does not actually affect the calibration parameters.

### 15.6.9.6 VCA Classification

VCAcore can define a moving objects class using either its Deep Learning models or by using properties extracted from an object in a calibrated scene.

Both methods of classification are applied through the use of filters in the rules interface.

Classification filters allow an object, which has triggered a rule, to be evaluated against its predicted class and filtered out if needed.


Tracking
Zones
Calibration
Classification
Burnt-in Annotation
Rules
Video Preview
Channel ID: 0

#### 15.6.9.6.1 Object classification

Once a camera view has been calibrated, each detected object in that view will have a number of properties extracted including object area and speed.

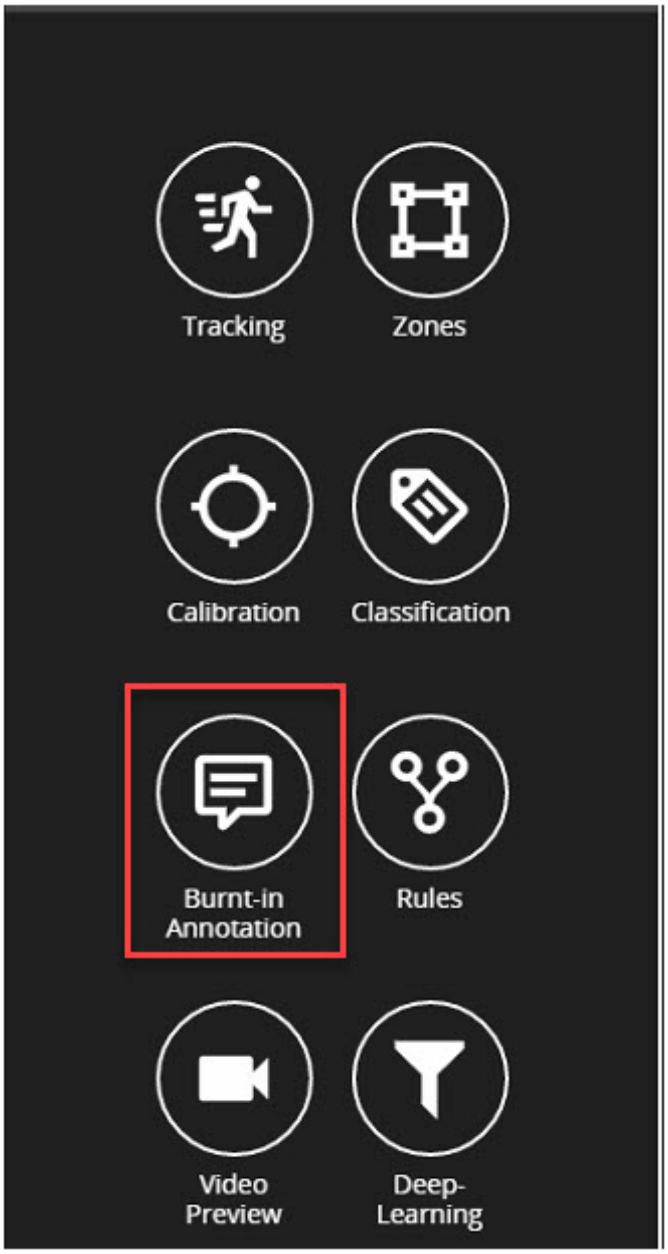
VCAserver's object classification performs classification by comparing these properties to a set of configurable object classifiers.

VCAserver comes pre-loaded with the most common object classifiers, and in most cases these will not need to be modified.

### 15.6.9.7 VCA Burnt-in Annotation

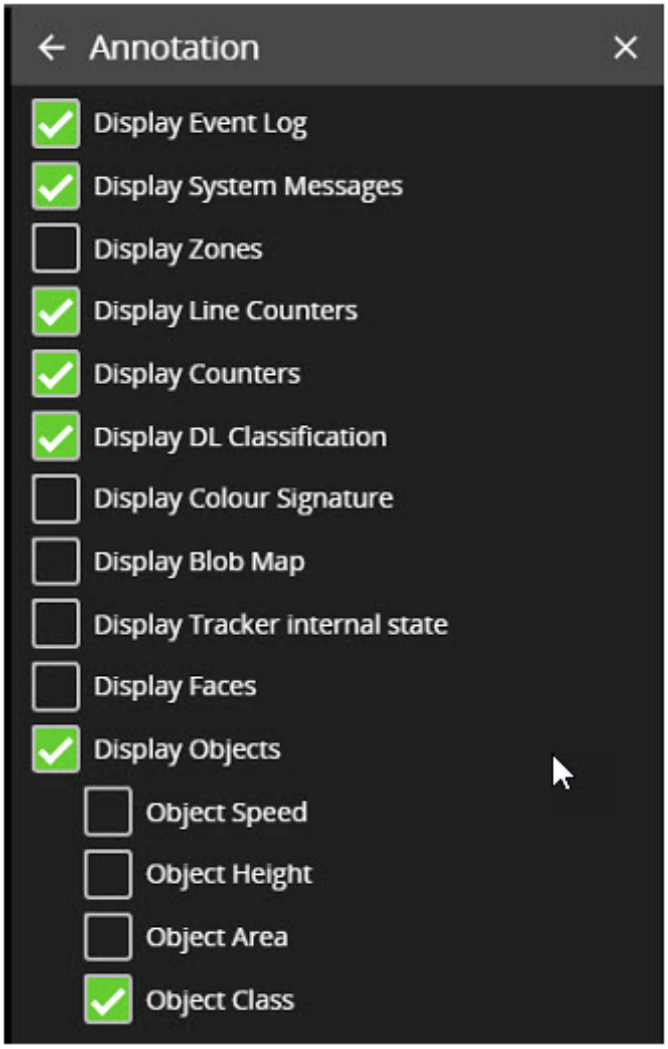
Burnt-in Annotations allow VCAserver metadata to be overlaid on to the raw video stream.

The burnt-in annotation settings control which VCAserver metadata (objects, events, etc) is rendered into the video stream.




**Note:**

- To display object parameters such as speed, height, area and classifications, the channel must first be calibrated.
- To display DL Classification annotations, the channel must have an active Deep Learning Filter rule configured or the DL People Tracker enabled.
- To display colour signature annotations, the channel must have an active Colour Filter rule configured.
- Some annotations only apply to certain trackers, in such cases the required tracker is listed in brackets.




## 15.6.9.8 VCA Rules

VCAcore's rules are used to detect specific events in a video stream.
There are three rule types that can be utilized to detect events and trigger actions:

#### 15.6.9.8.1 Basic Inputs / Rule:

An algorithm that will trigger when a particular behaviour or event has been observed e.g. Presence. Basic inputs can be used to trigger an action.

#### 15.6.9.8.2 Filters:

A filter that will trigger if the object which has triggered the input rule / logical rule meets the filter requirements e.g. is moving at a specific speed. Filters can be used to trigger an action.

#### 15.6.9.8.3 Conditional Rule:

A logical link between one or more inputs to allow the detection of more complex behaviours e.g. AND. Conditional rules can be used to trigger an action.
Within VCAcore, rule configurations can be as simple as individual basic inputs attached to a zone used to trigger an action.

Alternatively, rules can be combined into more complex logical rule configurations using conditional rules and filters.

The overarching goal of the rules in VCAcore is to help eliminate erroneous alerts being generated by providing functions to prevent unwanted behaviour from triggering an action.


- VCA - Basic inputs (see page 393)
- VCA - Aggressive Behaviour (see page 393)
- VCA - Abandoned and Removed object (see page 395)
- VCA - Appear and Disappear (see page 399)
- VCA - Enter and exit (see page 401)
- VCA - Direction (see page 404)
- VCA - Directional Crossing (see page 406)
- VCA - Dwell (see page 409)
- VCA - Fall (see page 411)
- VCA - Presence (see page 413)
- VCA - Tailgating (see page 415)
- VCA - Stopped (see page 417)
- VCA - Counting Line (see page 418)
- VCA - Conditional rules (see page 423)
- VCA - Counters (see page 428)
- VCA - Object trails (see page 431)
- VCA - Object display (see page 432)


#### 15.6.9.8.4 VCA - Basic inputs

A basic input or rule can only be used to trigger an action or as an input to another rule type.
Basic inputs always require a zone, and potentially some additional parameters.
A basic input can be used on its own to trigger an action, although they are often used as an input to other filters or conditional rules.

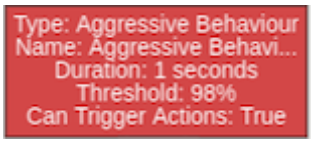
#### 15.6.9.8.5 VCA - Aggressive Behaviour

A rule which fires when aggressive behaviour is detected in the field of view for longer than the specified duration.

Aggressive behaviour does not require a zone and runs independently of the tracker. Enabling this algorithm, by adding this rule, will impact channel capacity, as the algorithm runs in addition to the channels selected tracker.

Separate VCAbehaviour license needed for this feature.


#### 15.6.9.8.5.1 Graphical View



#### 15.6.9.8.5.2 Form View


#### 15.6.9.8.5.3 Configuration

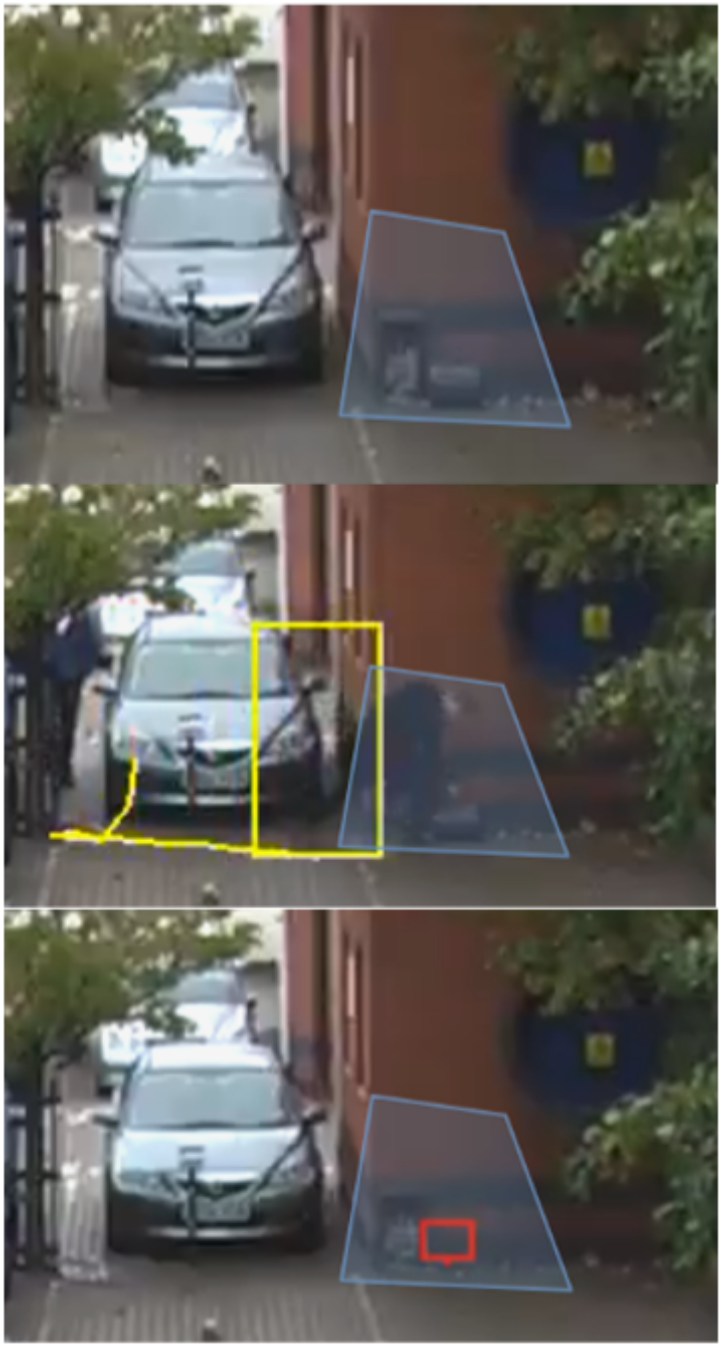
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Aggressive #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Duration | Period of time before an aggressive behaviour triggers the rule | 1 to 60 seconds |

### 15.6.9.8.6 VCA - Abandoned and Removed object

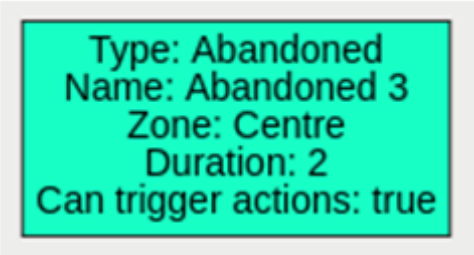
The abandoned and removed object rule triggers when an object has been either left within a defined zone, e.g. a person leaving a bag on a train platform, or when an object is removed from a defined zone.
The abandoned rule has a duration property which defines the amount of time an object must have been abandoned for or removed, to trigger the rule.

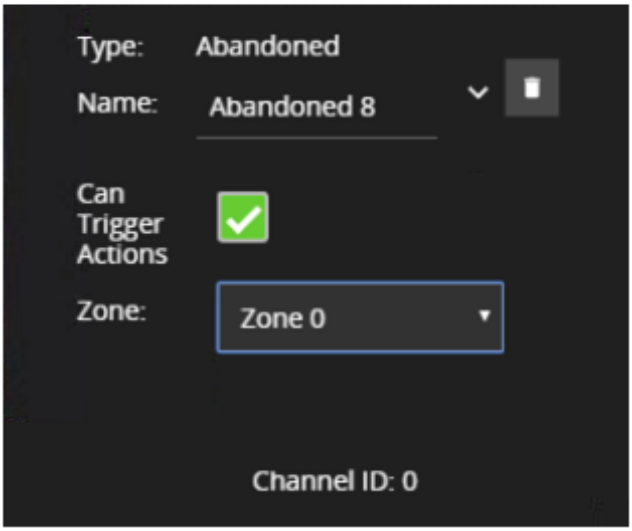
**Below is a sample scenario where a bag is left in a defined zone resulting in the rule triggering.**

**Below is a similar example scenario where the bag is removed from the defined zone resulting in the rule triggering.**



**Note:** The algorithm used for abandoned and removed object detection is the same in each case, and therefore cannot differentiate between objects which have been abandoned or removed.
This arises because the algorithm only analyses how blocks of pixels change with respect to a background model which is constructed over time.

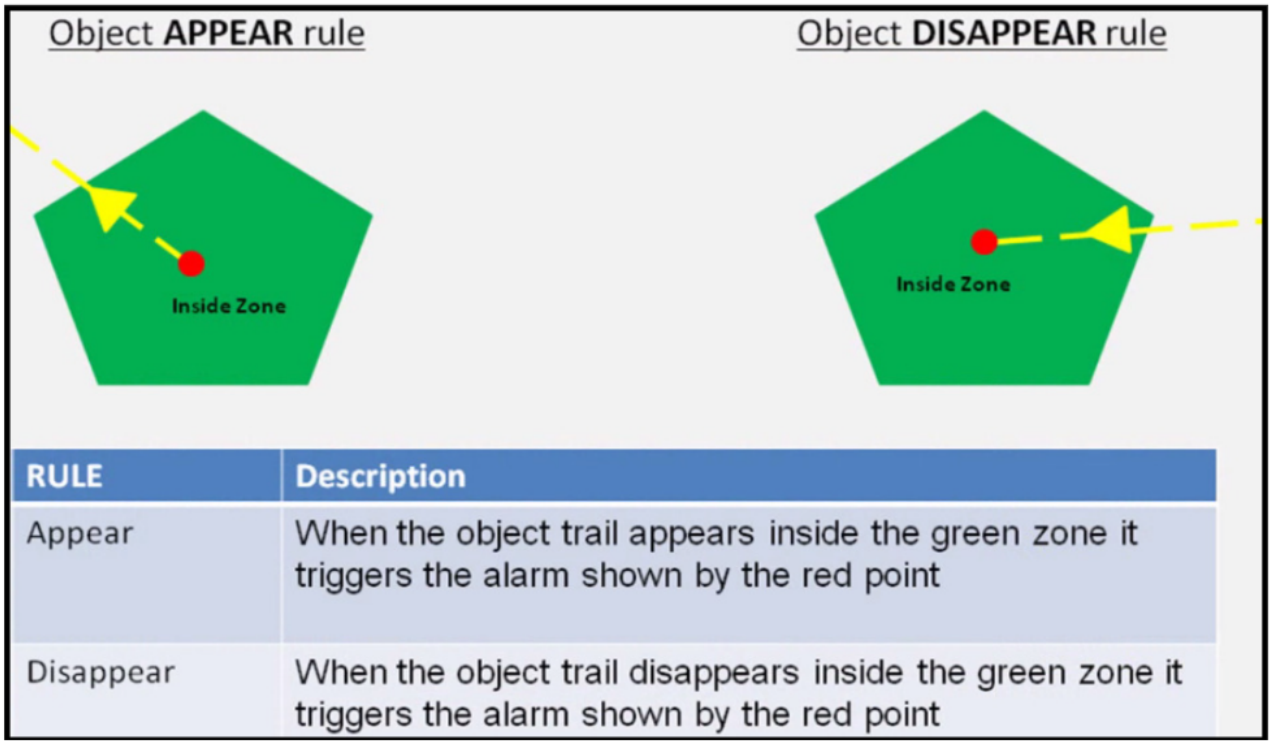


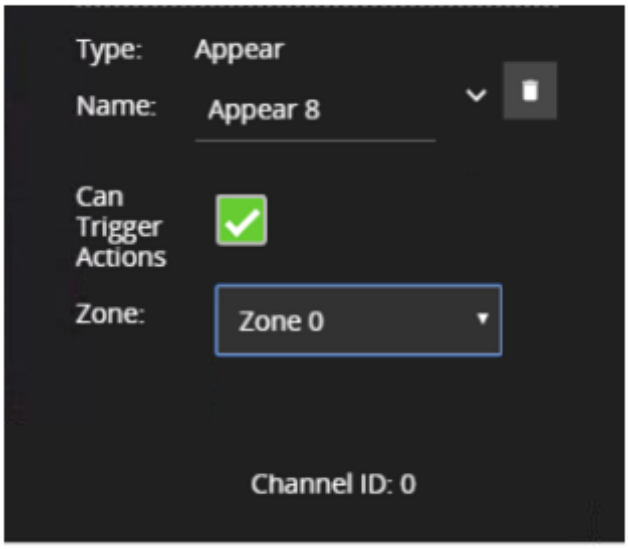

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Abandoned #" |
| Zone | The zone this rule is associated with | None |
| Duration | Period of time an object must have been abandoned or removed before the rule triggers | 0 |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |

### 15.6.9.8.7 VCA - Appear and Disappear

The appear rule detects objects that start being tracked within a zone, e.g. a person who appears in the scene from a doorway.
Conversely, the disappear rule detects objects that stop being tracked within a zone, e.g. a person who exits the scene through a doorway.
Note: The appear and disappear rules differ from the enter and exit rules as detailed in the enter and exit rule descriptions.




| RULE | Description |
|---|---|
| Appear | When the object trail appears inside the green zone it triggers the alarm shown by the red point |
| Disappear | When the object trail disappears inside the green zone it triggers the alarm shown by the red point |


#### 15.6.9.8.7.1 Configuration Appear

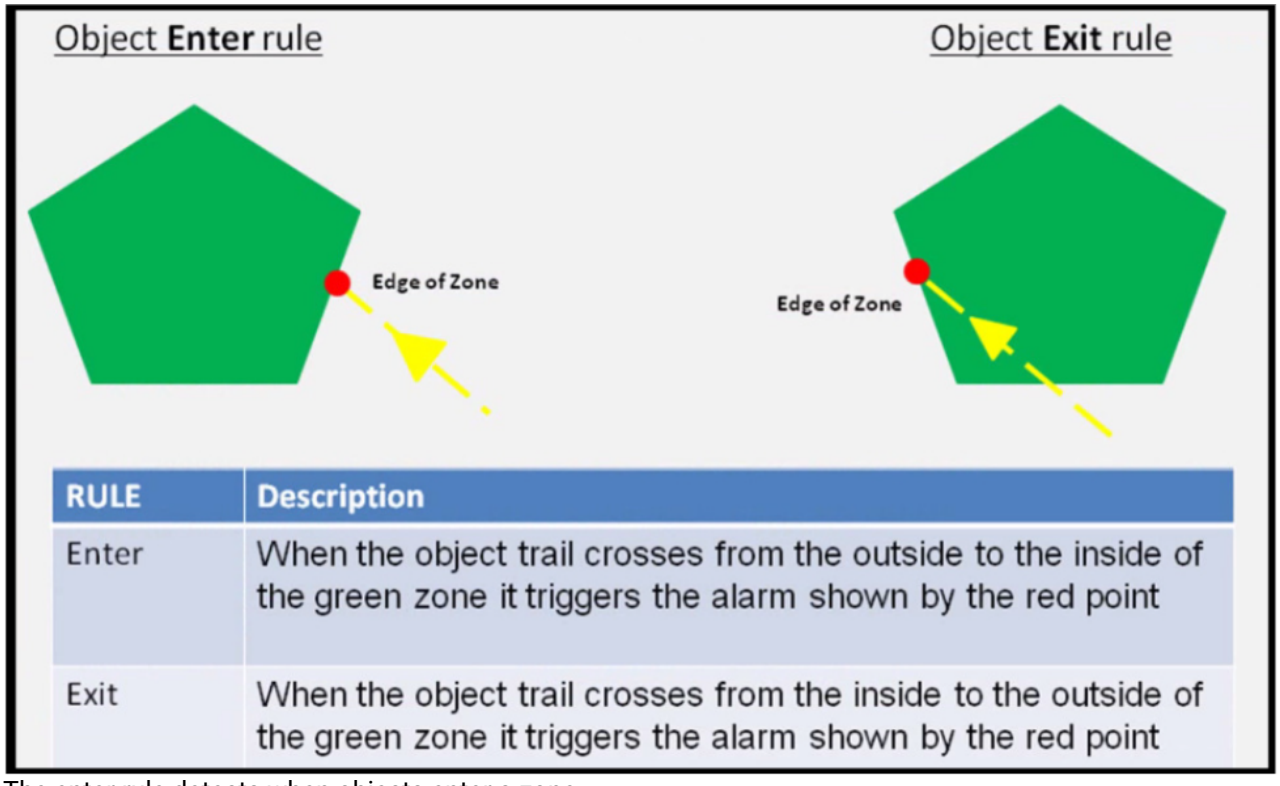
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Appear #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |

#### 15.6.9.8.7.2 Configuration Disappear

| Property | Description | Default Value |
|---|---|---|

| | | |
|---|---|---|
| Name | A user-specified name for this rule | "Disappear #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |

#### 15.6.9.8.8 VCA - Enter and exit

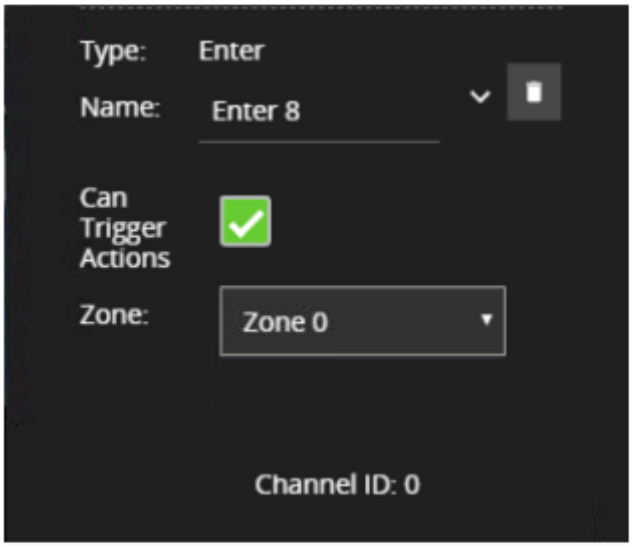


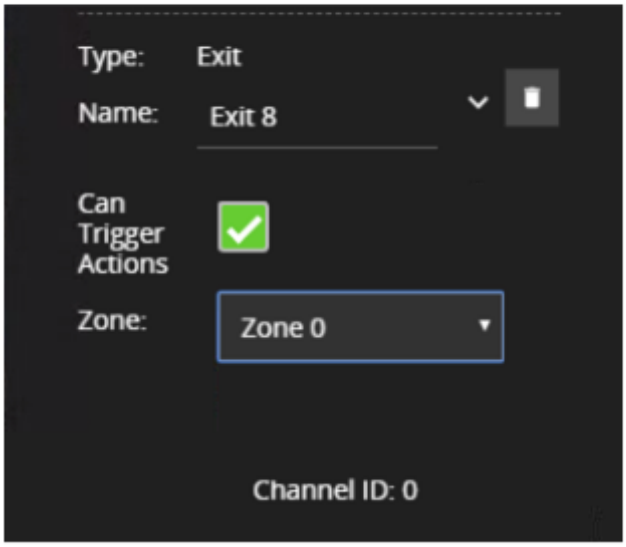

The enter rule detects when objects enter a zone.
In other words, when objects cross from the outside of a zone to the inside of a zone.
Conversely, the exit rule detects when an object leaves a zone: when it crosses the border of a zone from the inside to the outside.

**Note:** Enter and exit rules differ from appear and disappear rules, as follows:

1. Whereas the enter rule detects already-tracked objects crossing the zone border from outside to inside, the appear rule detects objects which start being tracked within a zone (e.g. appear in the scene through a door).

2. Whereas the exit rule detects already-tracked objects crossing the zone border from inside to outside, the disappear rule detects objects which stop being tracked within the zone (e.g. leave the scene through a door).

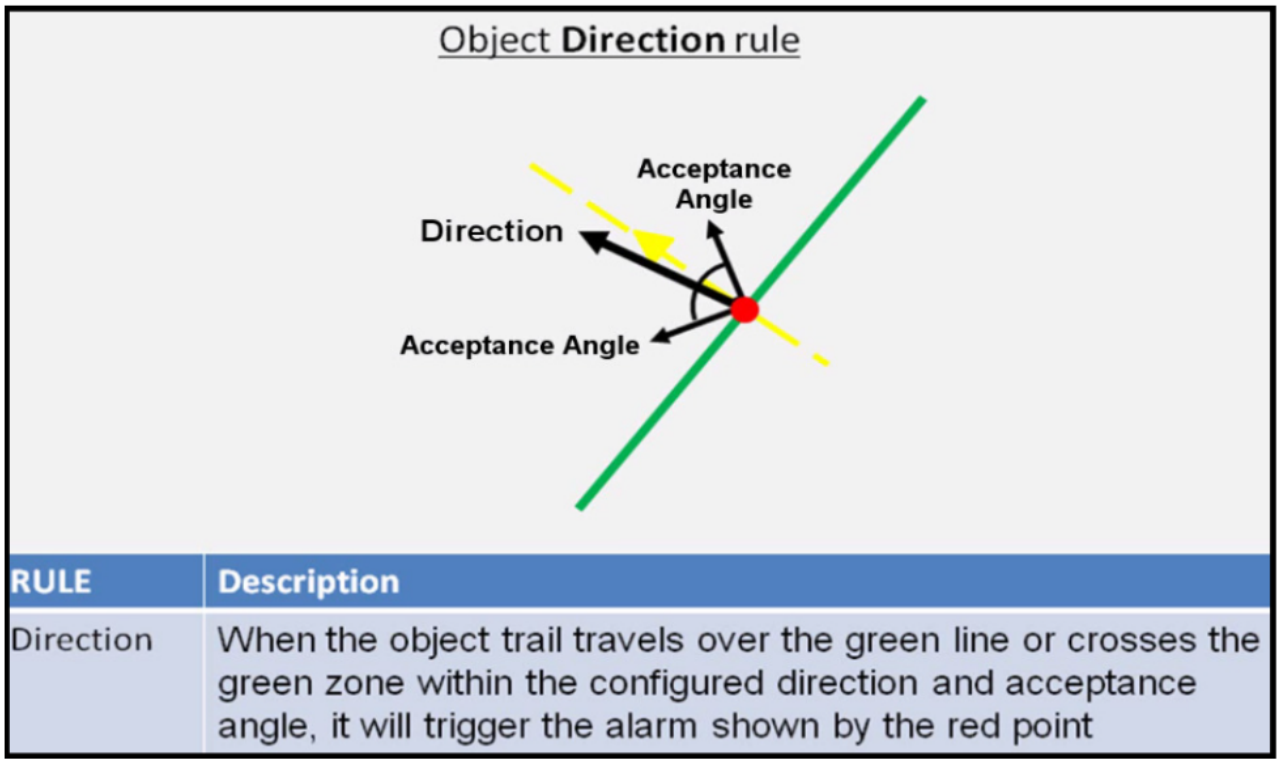
#### 15.6.9.8.8.1 Configuration Enter

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Enter #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |

#### 15.6.9.8.8.2 Configuration Exit

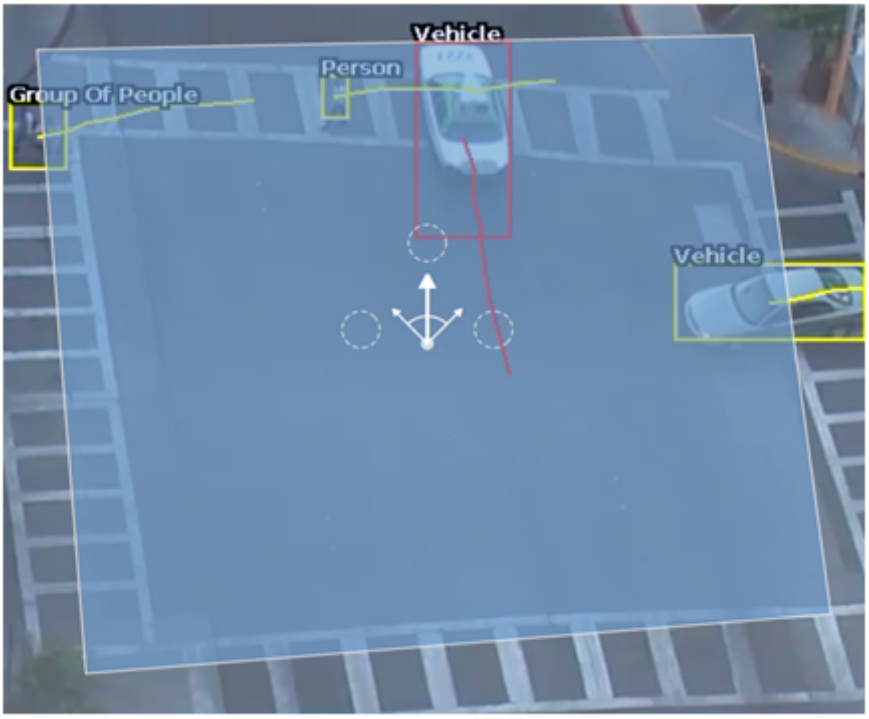
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Exit #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |

### 15.6.9.8.9 VCA - Direction

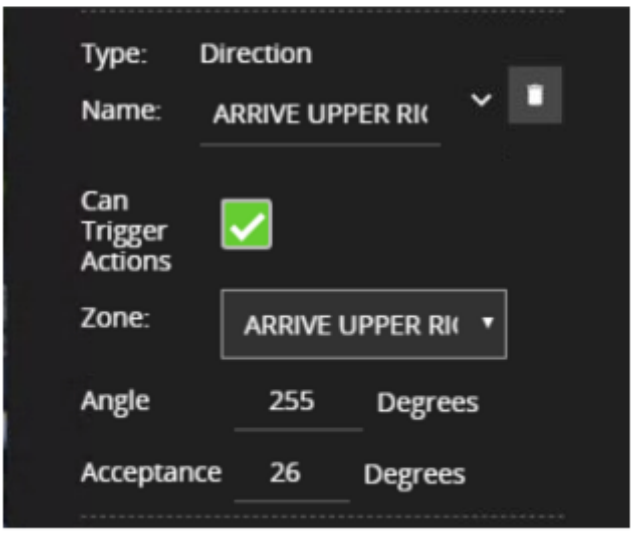



| RULE | Description |
|---|---|
| Direction | When the object trail travels over the green line or crosses the green zone within the configured direction and acceptance angle, it will trigger the alarm shown by the red point |

The direction rule detects objects moving in a specific direction.
Configure the direction and acceptance angle by moving the arrows on the direction control widget.
The primary direction is indicated by the large central arrow.
The acceptance angle is the angle between the two smaller arrows.
Objects that travel in the configured direction (within the limits of the acceptance angle), through a zone or over a line, trigger the rule and raise an event.
The following image illustrates how the white car moving in the configured direction triggers the rule whereas the other objects do not.




Type: Direction
Name: Direction 3
Zone: Centre
Angle: 358
Angle Threshold: 27
Can trigger actions: true



#### 15.6.9.8.9.1 Configuration Direction

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Direction #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |
| Angle | Primary direction angle, 0 - 359. 0 references up. | 0 |
| Acceptance | Allowed variance on each side of the primary direction that will still trigger rule | 0 |

### 15.6.9.8.10 VCA - Directional Crossing

The directional crossing rule is designed to reduce false alarms common with simple line crossing use cases. Directional Crossing is designed for use with a zone rather than a line, and adds a number of additional checks for an object as it enters as well as exits that zone.

For an object to trigger the Directional Crossing rule it must:

- Enter the zone travelling in a direction that falls within the acceptance angle.
- Be classified as one of the specified object classes.
- Exit that zone travelling in a direction that falls within the acceptance angle.

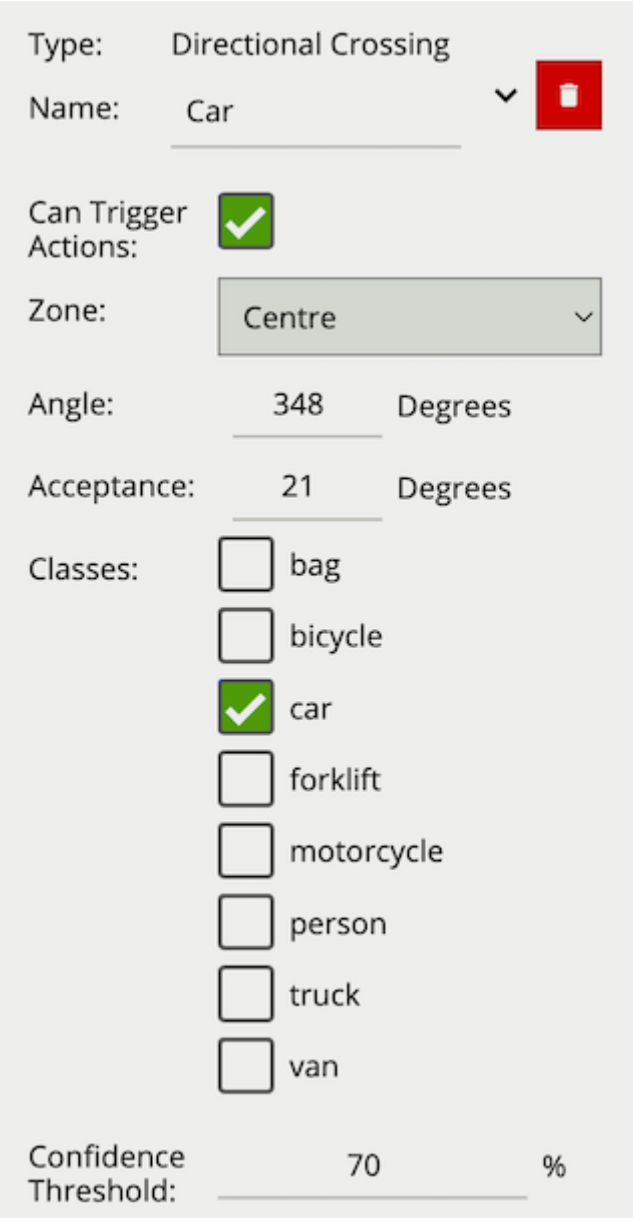
Configure the direction and acceptance angle by moving the arrows on the direction control widget. The primary direction is indicated by the large central arrow. The acceptance angle is the angle between the two smaller arrows.

The following image illustrates how the white car, moving in the configured direction, triggers the rule whereas the other objects do not.


#### 15.6.9.8.10.1 Graphical View

Type: Directional Crossing
Name: Car
Zone: Centre
Angle: 348
Acceptance: 21
Filters: car
Confidence Threshold: 70%
Can Trigger Actions: True

#### 15.6.9.8.10.2 Form View




#### 15.6.9.8.10.3 Configuration

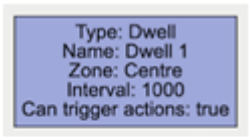
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Directional #” |

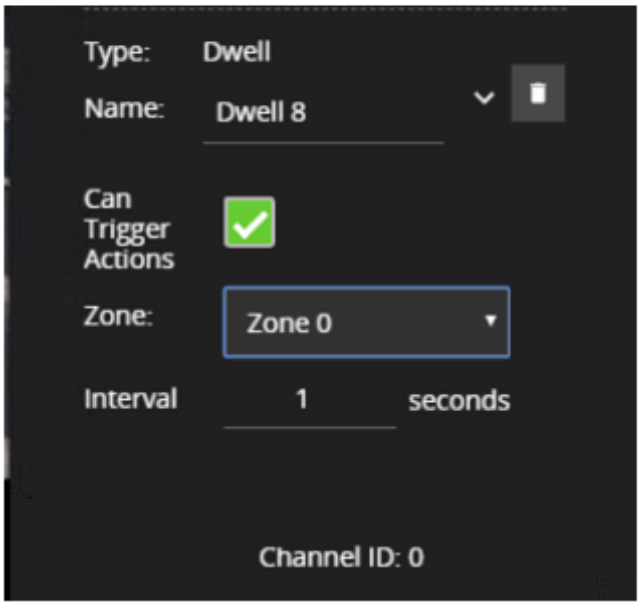
| Property | Description | Default Value |
|---|---|---|
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |
| Angle | Primary direction angle, 0 - 359. 0 references up. | 0 |
| Acceptance | Allowed variance each side of primary direction that will still trigger rule | 0 |
| Classes | The object classes allowed to trigger an alert | None |

#### 15.6.9.8.11 VCA - Dwell

A dwell rule triggers when an object has remained in a zone for a specified amount of time.
The interval parameter is the time the object has to remain in the zone before an event is triggered.
The following image illustrates how the person detected in the zone is highlighted red as they have dwelt in the zone for the desired period of time.
The two vehicles have not been present in the zone for long enough yet to trigger the dwell rule.


Person
Vehicle
Vehicle


Type: Dwell
Name: Dwell 1
Zone: Centre
Interval: 1000
Can trigger actions: true


Type: Dwell
Name: Dwell 8
Can Trigger Actions
Zone: Zone 0
Interval 1 seconds
Channel ID: 0

#### 15.6.9.8.11.1 Configuration Dwell

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Direction #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |
| Interval | Period of time in seconds) | 1 |

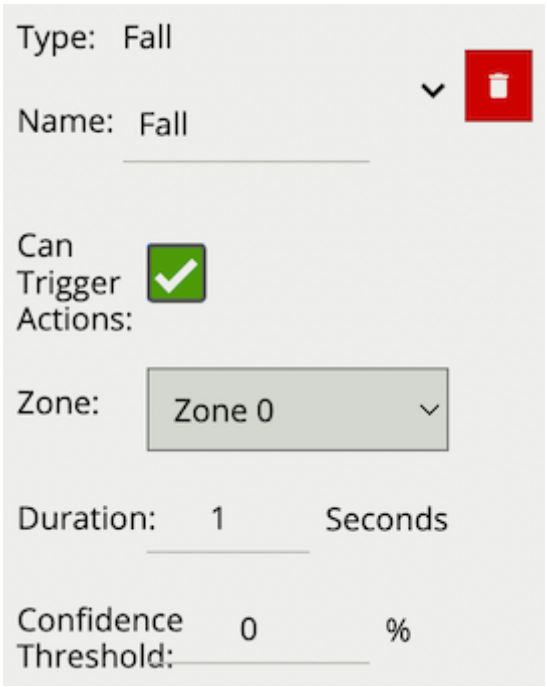
### 15.6.9.8.12 VCA - Fall

The fall rule detects when a object classified as a Person, by the Deep Learning People Tracker, is in the fallen state.

When the Fall rule is added to a channel configuration, the fall detection algorithm begins to run in the background which will have a GPU overhead. Currently this rule is only available when using the Deep Learning People Tracker.

#### 15.6.9.8.12.1 Graphical View


#### 15.6.9.8.12.2 Form View



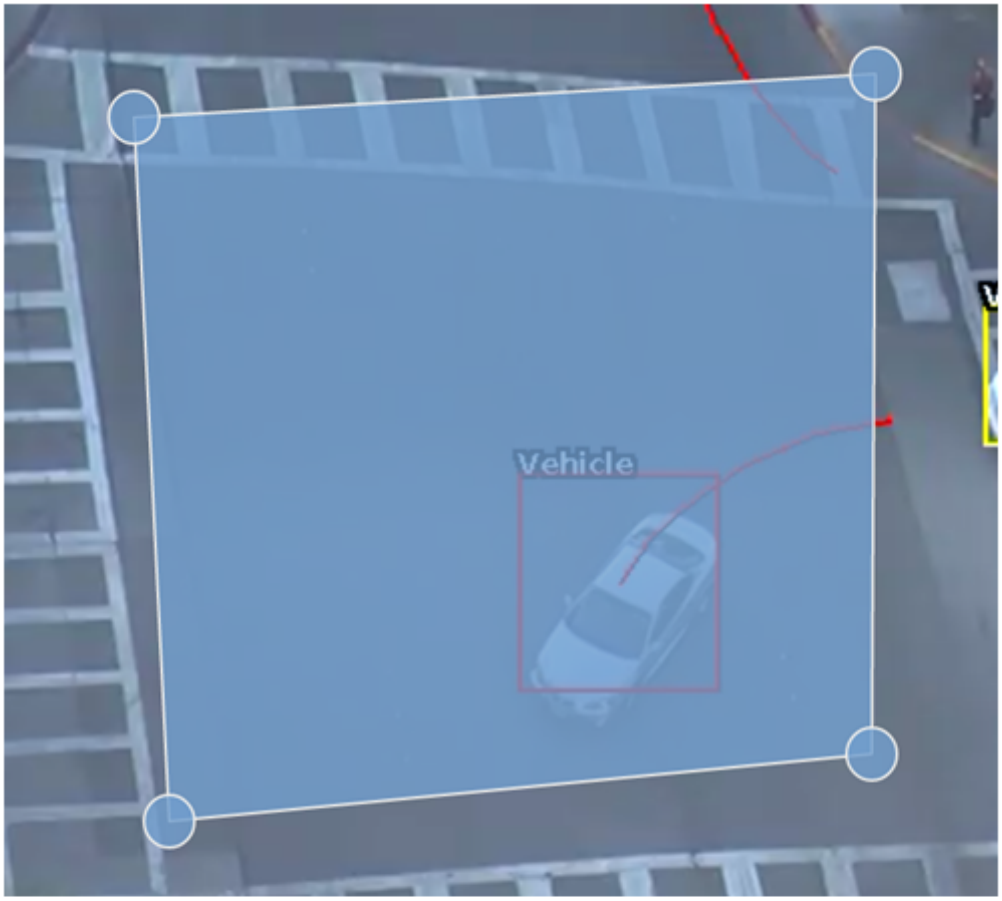

#### 15.6.9.8.12.3 Configuration

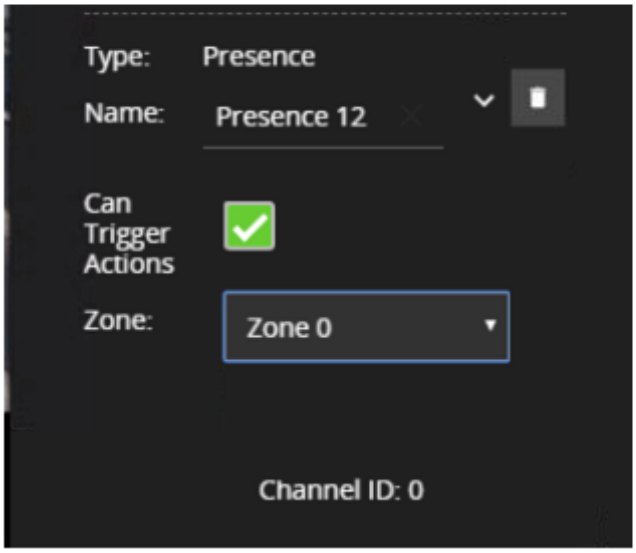
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Fall #” |
| Zone | The zone this rule is associated with | None |
| Duration | Period of time a object must have been fallen before the rule triggers | 1 to 60 seconds |

| Property | Description | Default Value |
|---|---|---|
| Confidence Threshold | The algorithm confidence (as a percentage) required to trigger the rule | 0 |
| Can Trigger Actions | The algorithm confidence (as a percentage) required to trigger the rule | Active |

#### 15.6.9.8.13 VCA - Presence

A rule which fires an event when an object is first detected in a particular zone.
Note: The Presence rule encapsulates a variety of different behaviour, for example, the Presence rule will trigger in the same circumstances as an Enter and Appear rule.
The choice of which rule is most appropriate will be dependent on the scenario.



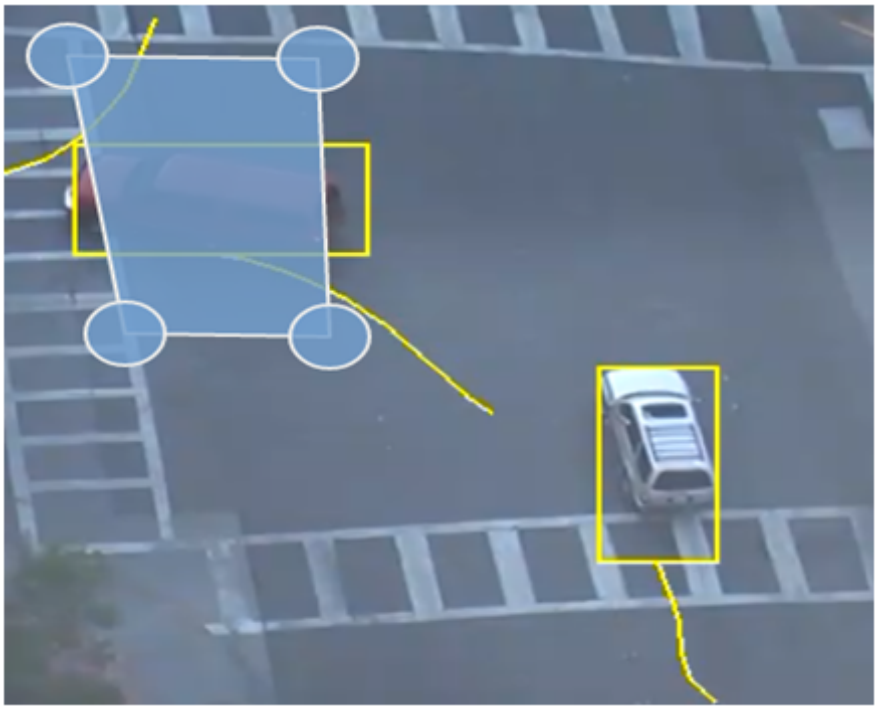

#### 15.6.9.8.13.1 Configuration Presence

| Property | Description | Default Value |
|---|---|---|

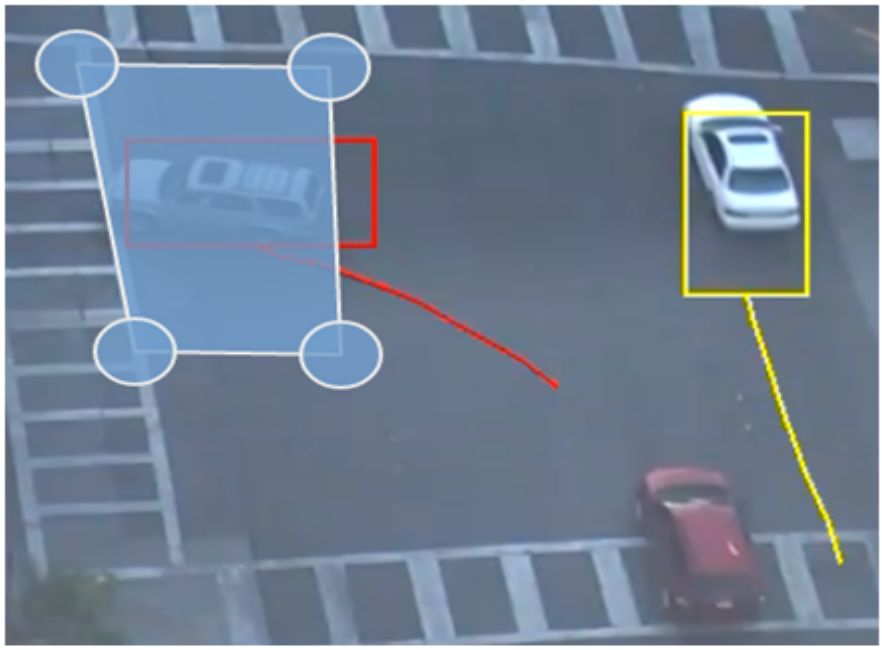
| | | |
|---|---|---|
| Name | A user-specified name for this rule | "Deep Learning Presence #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Zone | The zone this rule is associated with | None |

### 15.6.9.8.14 VCA - Tailgating

The tailgating rule detects objects which cross through a zone or over a line within quick succession of each other.
In this example, object 1 is about to cross a detection line. Another object (object 2) is following closely behind.
The tailgating detection threshold is set to 5 seconds.
That is, any object crossing the line within 5 seconds of an object having already crossed the line will trigger the object tailgating rule.



Object 2 crosses the line within 5 seconds of object 1. This triggers the tailgating filter and raises an event.

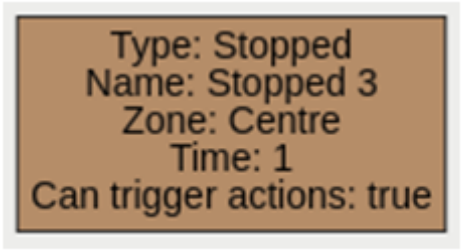


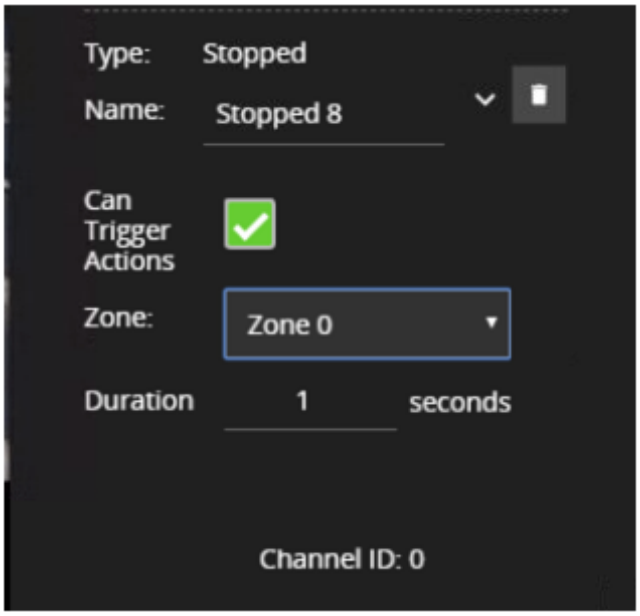

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Tailgating #" |
| Zone | The zone this rule is associated with | None |
| Duration | The maximum amount of time between first and second object entering a zone to trigger the rule | 0 |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |

### 15.6.9.8.15 VCA - Stopped

The stopped rule detects objects which are stationary inside a zone for longer than the specified amount of time.
The stopped rule requires a zone to be selected before being able to configure an amount of time.

**Note**: The stopped rule does not detect abandoned objects. It only detects objects which have moved at some point and then become stationary.




#### 15.6.9.8.15.1 Configuration Stopped

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Stopped #" |
| Zone | The zone this rule is associated with | None |

| | | |
|---|---|---|
| Time | Period of time before a stopped object triggers the rule | 0 |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |

### 15.6.9.8.16 VCA - Counting Line

A counting line is a detection filter optimized for directional object counting (e.g. people or vehicles) in busier detection scenarios.

**Examples of such applications may include**:

- People counting with overhead cameras in a retail environment.
- Vehicle counting with overhead cameras on public highways.

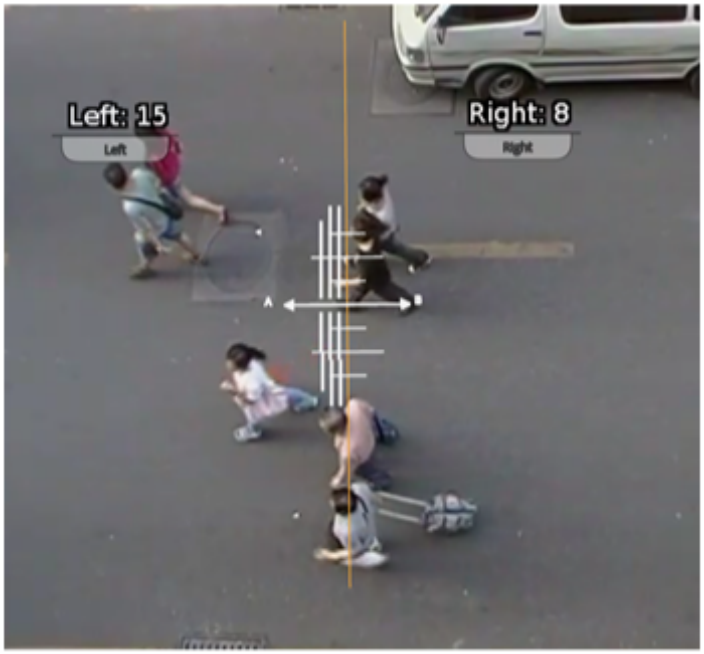
In some scenes, such as entrances with cameras installed overhead, the counting line typically will generate a higher accuracy count than using the aforementioned counters connected to a presence rule.

An event is generated every time an object crosses the line in the configured direction.
If multiple objects cross the line together, multiple corresponding events are generated.
These events can be directly used to trigger actions if the Can Trigger Actions property is checked.
Counting lines are attached to zones configured with a Line shape.
See **Zones** for more information.

If a counting line is configured with a zone not defined with a Line shape, the zone property will be automatically changed (it will not be possible to change the zone shape back until the counting line stops referencing the zone in question).

Counting lines have a specified direction indicated by the arrow in the UI (direction A or B), the direction of this arrow is governed by the configured zone.
Each instance of the rule counts in a single direction. To count in both directions a second counting line rule must be added to the same zone with the opposite direction selected.
An example rule graph of a two-way counting line configured with a counter is provided to illustrate this below.

**NOTE:** The maximum number of counting line filters that can be applied per video channel is 5.




### 15.6.9.8.16.1 Calibrating the Counting Line

In order to generate accurate counts, the counting line requires calibration.
Unlike the object tracking function engine, this cannot be performed at a general level for the whole scene using the 3D Calibration tool.
This is because the counting line is not always placed on the ground plane; it may be placed at any orientation at any location in the scene.

For example, a counting line could be configured vertically with a side-on camera view.
Instead of the 3D calibration tool, the counting line has its own calibration setting.
Two bars equidistant from the center of the line represent the width of the expected object. This allows the counting line to reject noise and also count multiple objects.

**To calibrate the counting line:**

1. Select the counting line rule.
2. Check the Enable width calibration option.

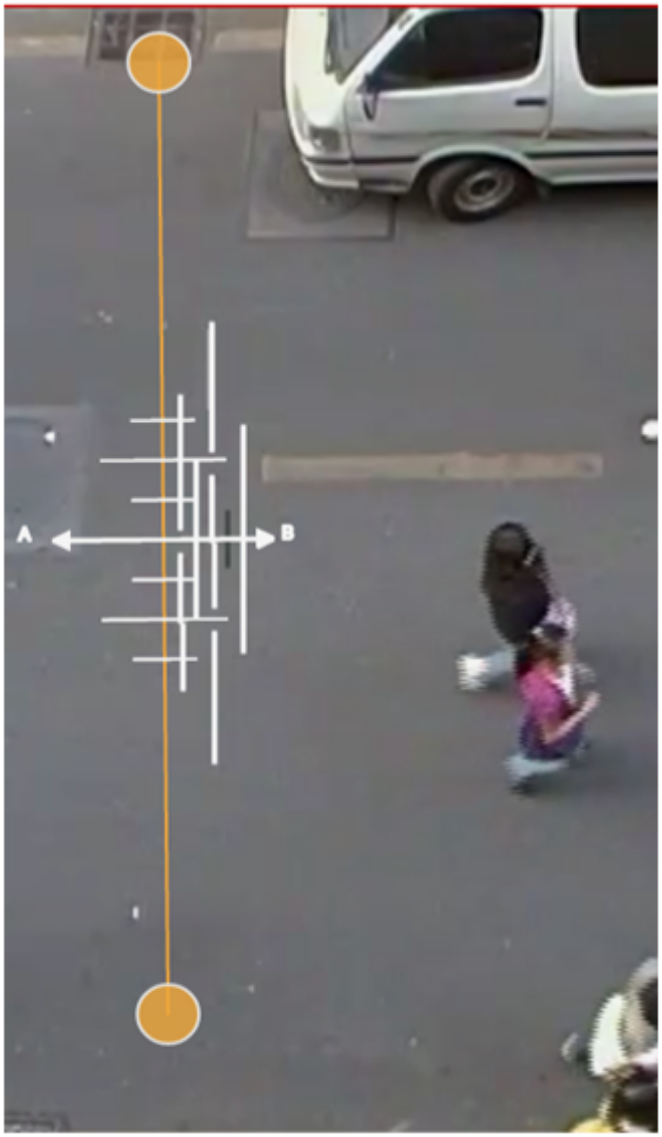
3. Drag the calibration markers to adjust the distance between the calibration markers until the distance is approximately the size of the objects to be counted. Alternatively, move the Width slider to achieve the same result.
4. The calibration width is displayed within the counting line rule and can be edited directly to change the calibration width.
5. The small markers on either side of the big markers indicate the minimum and maximum width which is counted as a single object.

**NOTE:** if the Width slider is set to zero then the Enable width calibration checkbox is automatically disabled.

#### Counting Line Calibration Feedback

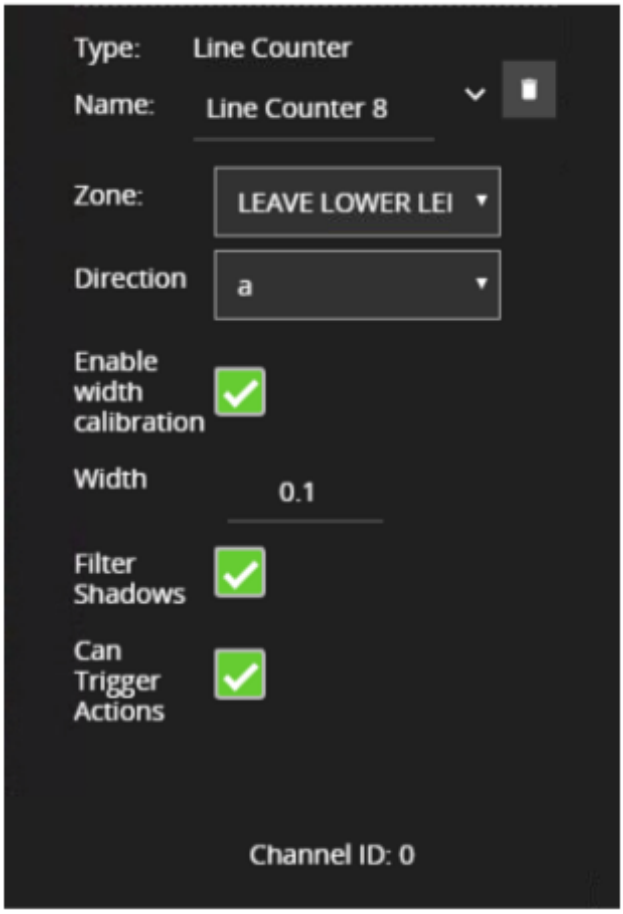
To enable the user to more accurately configure the calibration for the counting line, the widths of detected objects are displayed as an overlay next to the counting line when objects pass over it.
By default, this display option is enabled. However, if it does not appear, ensure that the option is enabled on the Burnt-in Annotation settings.

The calibration feedback is rendered as black and white lines on either side of the counting line on the Zones configurations page.Each line represents an object detected by the counting algorithm.The width of the line shows the width of the object detected by the line.The last few detections are displayed for each direction with the latest one appearing closest to the counting line




### 15.6.9.8.16.2 Shadow Filter

The counting line features a shadow filter which is designed to remove the effects of object shadows affecting the counting algorithm.
Shadows can cause inaccurate counting results by making an object appear larger than its true size or by joining two or more objects together.
If shadows are causing inaccurate counting, the shadow filter should be enabled by selecting the Shadow Filter check box for the line.
It is recommended that the shadow filter only be enabled when shadows are present because the algorithm can mistake certain parts of an object for shadows and this may lead to worse counting results.
This is especially the case for objects that have little contrast compared to the background (e.g. people wearing black coats against a black carpet).




| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | Line_Counter |
| Zone | The zone this rule is associated with | None |
| Direction | Enable counting in the 'A' or 'B' direction (one direction per counting line) | None |
| Enable Width Calibration | Width calibration to allow more accurate counting | None |
| Width | Width calibration value | 0 |

| | | |
|---|---|---|
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |

### 15.6.9.8.17 VCA - Conditional rules

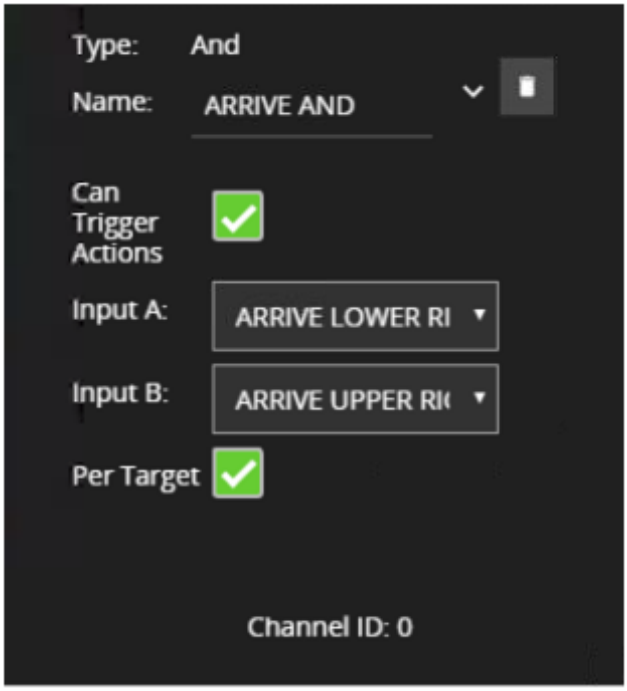
A conditional input, like a filter, is one that cannot trigger an action on its own.
It requires the input of another basic input, conditional rule or filter to be meaningful.
An example of this is the AND rule. The AND rule requires two inputs to compare in order to function.

#### 15.6.9.8.17.1 The complete list of conditional rules are:

- And
- Continuously
- Counter
- Or
- Previous

#### 15.6.9.8.17.2 And

A logical operator that combines two rules and only fires events if both inputs are true.




| Property | Description | Default Value |
|---|---|---|

| | | |
|---|---|---|
| Name | A user-specified name for this rule | "And #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input A | The first input | None |
| Input B | The second input | None |
| Per Target | Fire one event per tracked object | Active |

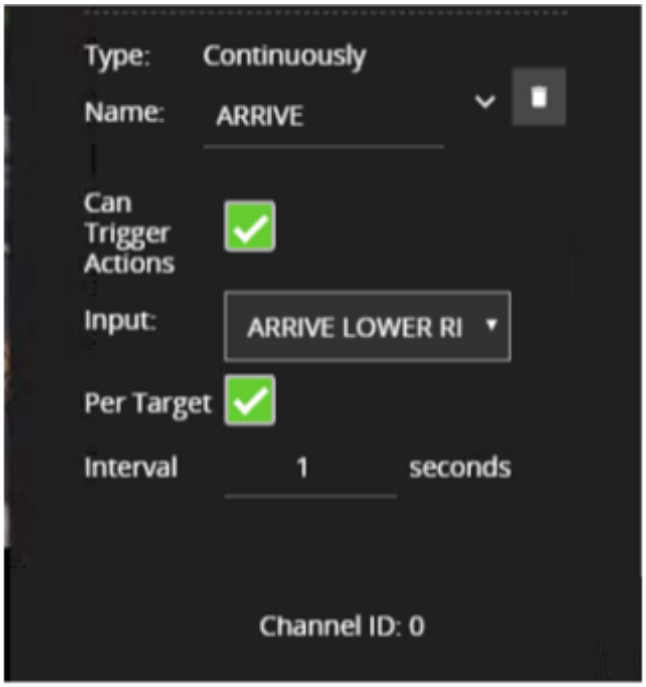
If we consider a scene with two presence rules, connected to two separate zones, connected by an AND rule, the table below explains the behaviour of the Per Target property.
Note that object here refers to a tracked object, as detected by the VCA tracking engine.

| State | Per Target | Outcome |
|---|---|---|
| Object A in Input A, Object B in input B | On | Two events were generated, one for each object |
| Object A in Input A, Object B in input B | Off | Only one event generated |

Additionally, it is important to note that if the rule fires when Per Target is switched off, it will not fire again until it is 'reset', i.e. until the AND condition is no longer true.

#### 15.6.9.8.17.3 Continuously

A logical operator fires events when its input has occurred continuously for a user-specified time.




| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Continuously #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Per Target | Fire one event per tracked object. See the description below for more details | Active |
| Interval | The time in milliseconds | 1000 ms |

Considering a scene with one zone, a presence rule associated with that zone, and a Continuously rule attached to that presence rule, when the Per Target property is on, the rule will generate an event for each tracked object that is continuously present in the zone.

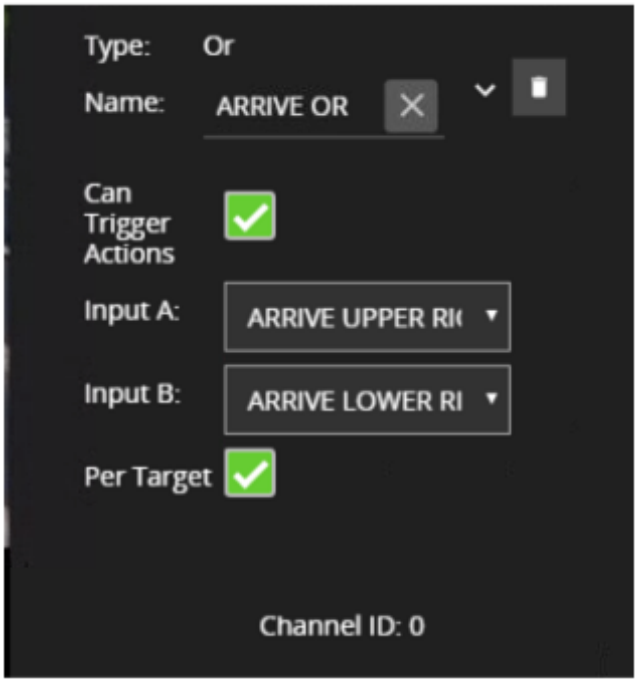
When it is off, only one event will be generated by the rule, even if there are multiple tracked objects within the zone.
Additionally, when Per Target is off, the rule will only generate events when there is a change of state - i.e. the rule condition changes from true to false or vice versa.

**When Per Target is off, the state will change when:**

1. Any number of objects enter the zone in question and remain in the zone
2. All objects leave the zone in question

### 15.6.9.8.17.4 Or

A logical operator that combines two rules and fires events if either input is true.



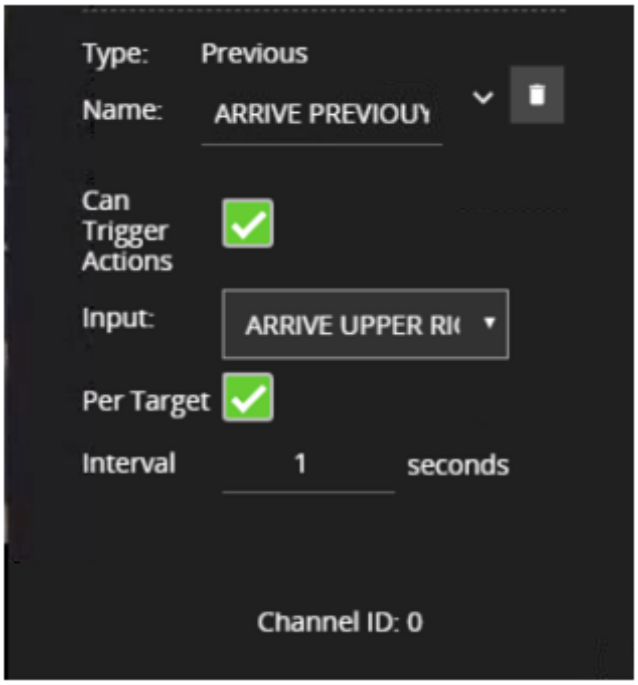

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Or #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input A | The first input | None |
| Input B | The second input | None |
| Per Target | Fire one event per tracked object | Active |

If we consider a scene with two presence rules, connected to two separate zones, connected by an OR rule, the table below explains the behaviour of the Per Target property.

| State | Per Target | Outcome |
|---|---|---|
| Object A in Input A, No object in input B | On | Two events were generated, one for each object |
| No object in Input A, Object B in input B | On | Only one event was generated (for Object B) |
| Object A in Input A, No object in input B | On | Only one event generated (for Object A) |
| Object A in Input A, No object in input B | Off | Only one event generated |
| No object in Input A, Object B in input B | Off | Only one event generated |
| Object A in Input A, No object in input B | Off | Only one event generated |

#### 15.6.9.8.17.5 Previous

A logical operator triggers for input events that were active at some point in a past window of time.
This window is defined by between the current time and the period before the current time (specified by the interval parameter value).




| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Previous #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Per Target | Fire one event per tracked object | Active |
| Interval | The time in milliseconds | 1000 ms |

#### 15.6.9.8.18 VCA - Counters

These counters are only visible in the VCA configuration. To use counters in the Spotter please refer to the Spotter manual.
Counters can be configured to count the number of times a rule is triggered, for example, the number of people crossing a line.

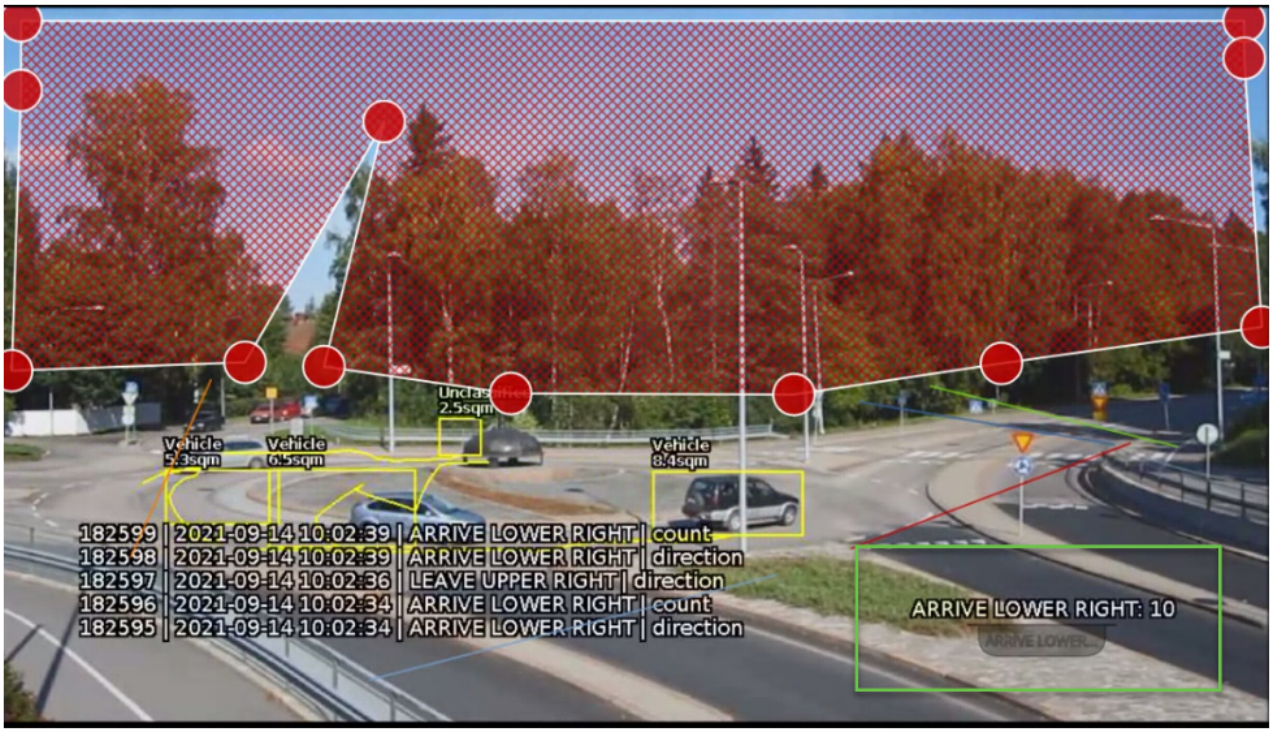
The counter rule is designed to be utilized in two ways:

- Increment / Decrement: whereby a counter is incremented by the attached rule(s) (+1 for each rule trigger) and decremented by another attached rule(s) (-1 for each rule trigger).

- Occupancy: whereby the counter reflects the number of objects that are currently triggering the attached rule(s).

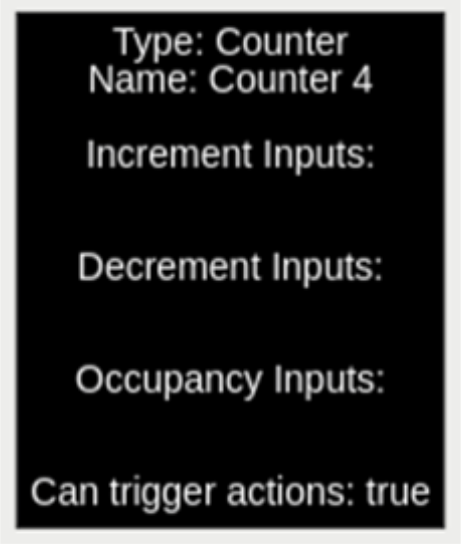
More than one rule can be assigned to any of a counter's three inputs.
This allows, for example, the occupancy of two presence rules to be reflected in a single counter or more than one entrance/exit gate to reflect in a single counter, an example rule graph is provided to illustrate this below.
Broadly speaking a single counter should not be used for both purposes occupancy and increment/ decrement.

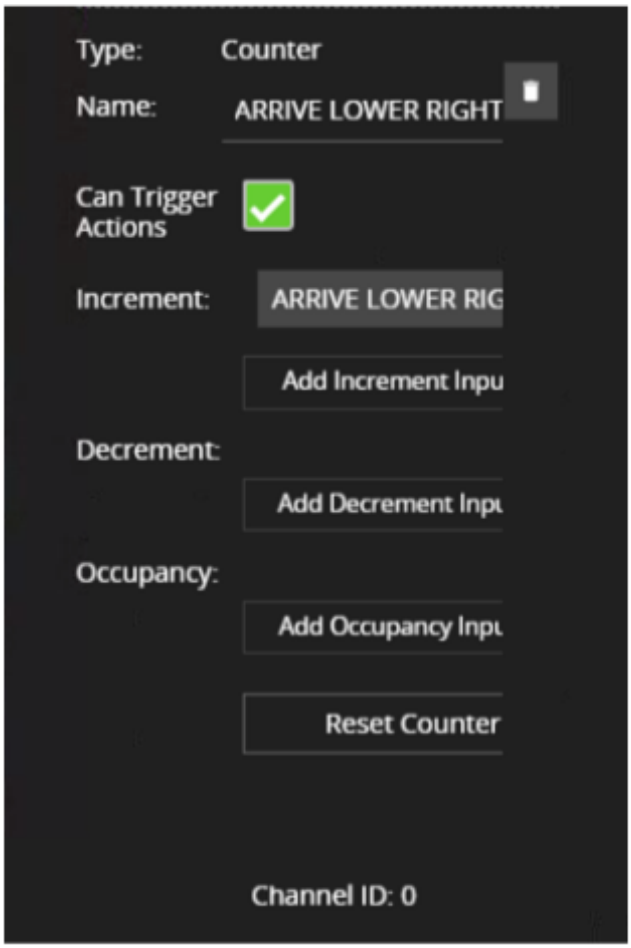
Note: events created by a counter will not trigger the Deep-Learning Filter, even if enabled on the channel.




### 15.6.9.8.18.1 Positioning Counters

When added, a counter object is visualized on the video stream as seen below.
The counter can be repositioned by grabbing the 'handle' beneath the counter name and moving the counter to the desired location.



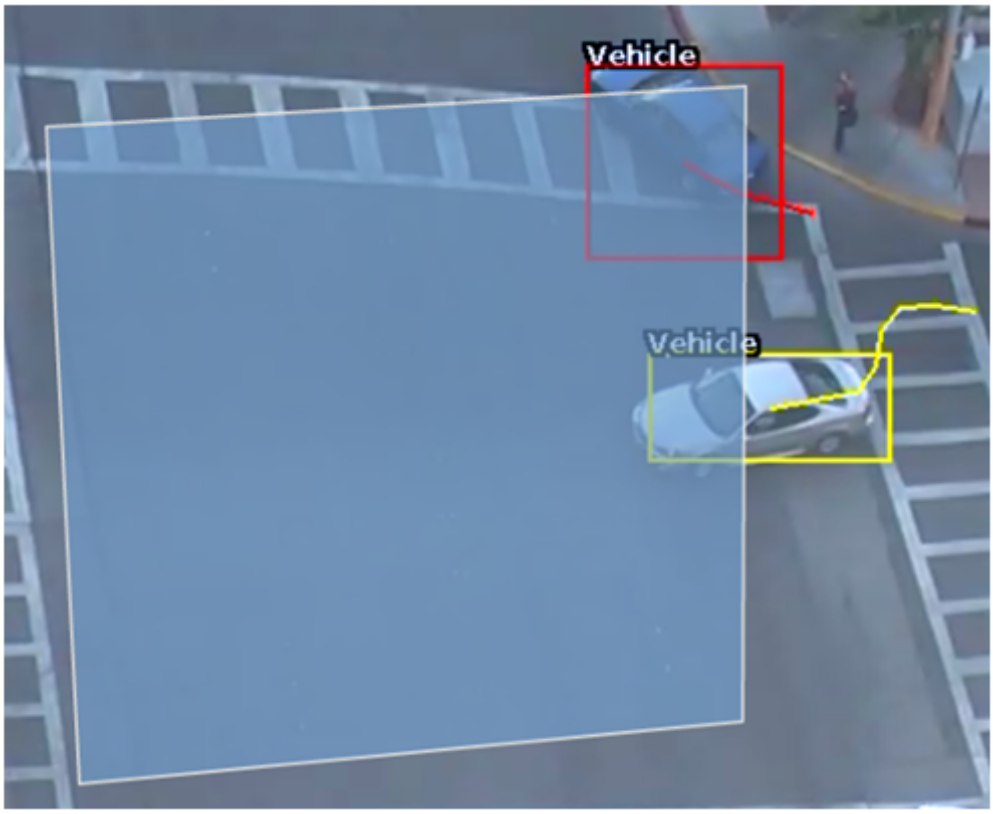

| Property | Description | Default Value |
|---|---|---|

| | | |
|---|---|---|
| Name | A user-specified name for this rule | "Counter #" |
| Increment | The rule which, when triggered, will add one to the counter | None |
| Decrement | The rule which, when triggered, will subtract one from the counter | None |
| Occupancy | Sets counter to the current number of the rule's active triggers* | None |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Reset Counter | A button allowing the counter value to be reset to 0 | None |

- E.g. if a presence rule is set as the occupancy target and two objects are currently triggering that presence rule, the counter will show the value of '2'.

### 15.6.9.8.19 VCA - Object trails

The trail shows the history of where the object has been.
Depending on the calibration the trail can be drawn from the centroid or the mid-bottom point of the object. (See Advanced Settings for more information).
The trail is important for determining how a rule is triggered.
The intersection of the trail point with a zone or line determines whether a rule is triggered or not.
The following image illustrates this point: the blue vehicle's trail intersects with the detection zone and is rendered in red.
Conversely, while the white vehicle intersects the detection zone, its trail does not (yet) intersect and hence it has not triggered the rule and is rendered in yellow.




### 15.6.9.8.20 VCA - Object display

As rules are configured, they are applied to the channel in real-time allowing feedback on how they work. Objects which have triggered a rule are annotated with a bounding box and a trail. Objects can be rendered in two states:

1. **Non-alarmed:** Default rendered in yellow. A detected object which does not meet any criteria trigger a rule and raise an event.
2. **Alarmed:** Default rendered in red. A detected object which has triggered one or more rules. Causes an event to be raised.

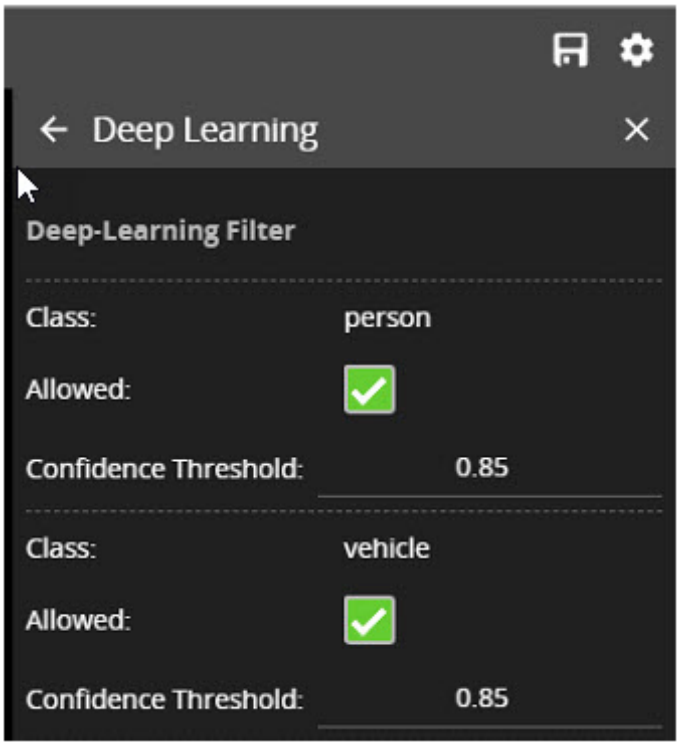
As seen below, when an event is raised, the default settings render details of the event in the lower half of the video stream.
Object class annotations in this example are generated through


### 15.6.9.9 VCA - Deep-Learning Filter

VCAserver also supports classification through the use of the deep learning filter. In this case an object, which has triggered a rule, can be analyzed using the deep learning filter and a predicted class and confidence level returned. The available object classes are defined by the model.

On VCAserver the Deep Learning Filter can use GPU acceleration, see **Deep Learning Requirements** for hardware requirements.

Without GPU acceleration the deep learning filter will use the CPU, enabling the deep learning filter on multiple channels which are generating a high volume of events, (more than 1 per second) may result in poor performance of the system and is not advised.




#### 15.6.9.9.1 Each of the possible object classes has additional parameters:

**Allowed**: Whether this object type will be allowed to pass through the filter. If this is unchecked, any objects classified as this type will not trigger any actions.

**Confidence Threshold**: A value (0.0 - 1.0) representing the minimum confidence level required for classification. Any objects with a lower classification score than this minimum value will be filtered out and will not trigger any actions.

## 15.6.10 VCA - Filters

A filter cannot trigger an action on its own as it requires another basic input, filter or conditional rule to trigger.

- VCA Filters - Speed Filter (see page 435)
- VCA Filters - Object Filter (see page 437)
- VCA Filters - Colour Filter (see page 439)
- VCA Filters - Retrigger Filter (see page 442)
- VCA Filters - Deep Learning Filter (see page 443)

## 15.6.10.1 VCA Filters - Speed Filter

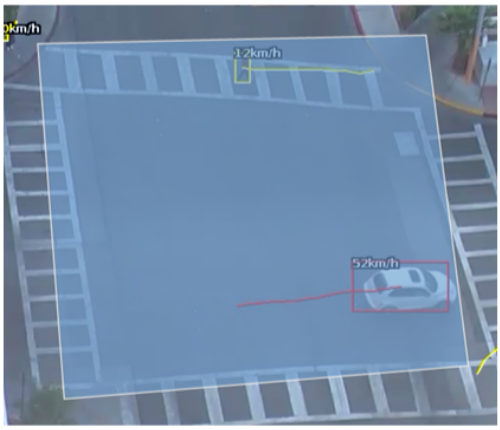
### 15.6.10.1.1 Speed Filter

The speed filter provides a way to check if the speed of an object which has triggered an input is moving within the range of speeds defined by a lower and upper boundary.

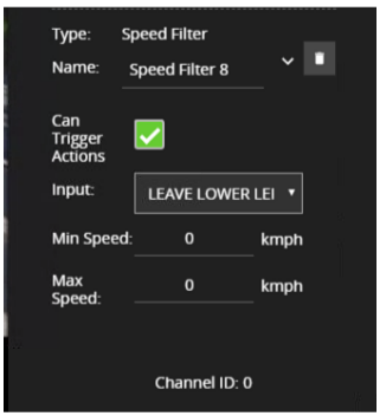
> The channel must be Calibrated in order for the speed filter to be available.

Commonly this rule is combined with a presence rule, an example rule graph is provided to illustrate this below.

The following image illustrates how such a rule combination triggers on the car moving at 52 km/h but the person moving at 12 km/h falls outside the configured range (25-100 km/h) and thus does not trigger the rule.



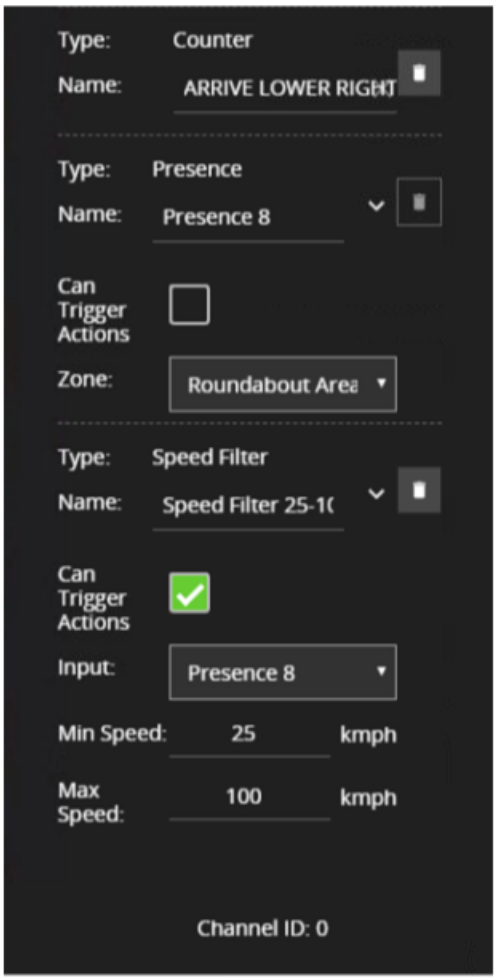




| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Speed #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Min Speed | The minimum speed (km/h) an object must be going to trigger the rule | 0 |
| Max Speed | The maximum speed (km/h) an object can be going to trigger the rule | 0 |

#### 15.6.10.1.1.1 Typical Logical Rule Combination

The below example logical rule checks if an object triggering the presence rule attached to zone Centre, is also travelling between 25 and 100 km/h as specified by the speed rule Speed Filter 25-100 km/h.
Only the Speed Filter is set to Can Trigger Actions, meaning only this component of the logical rule will be available as a source for actions. Additionally, any activity generated by the speed filter will have the event type Presence




## 15.6.10.2 VCA Filters - Object Filter

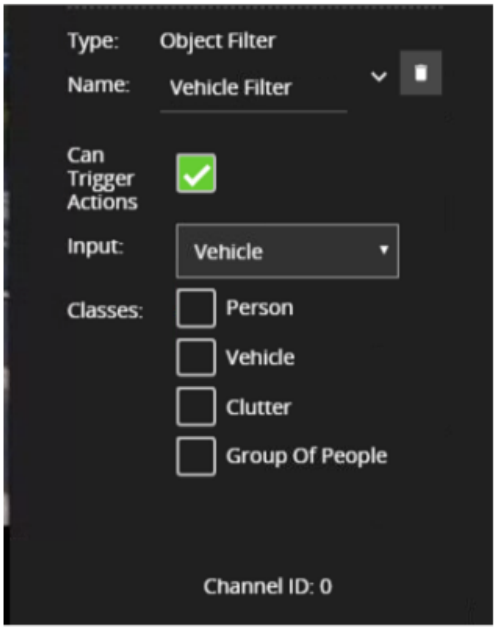
The object classification filter provides the ability to filter out objects, which trigger a rule if they are not classified as a certain class (e.g. person, vehicle).

The object classification filter must be combined with another rule(s) to prevent unwanted objects from triggering an alert, an example rule graph is provided to illustrate this below.

The previous image illustrates how the object classification filter configured with Vehicle class, includes only Vehicle objects.

The person in the zone is filtered out since the Person class is not selected in the filter list.

> The channel must be calibrated for the object classification filter to be available.

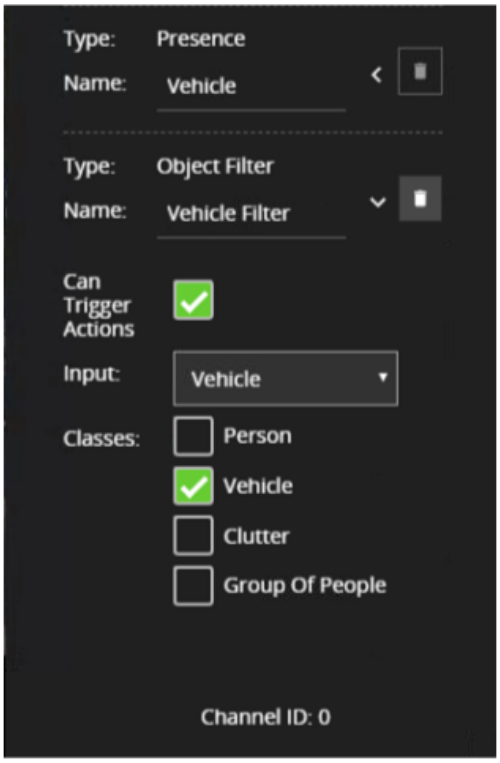

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Object Filter #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Classes | The object classes allowed to trigger an alert | None |

#### 15.6.10.2.1 Typical Logical Rule Combination

The below example logical rule checks if the object triggering the presence rule attached to zone Centre, is also classified as a Vehicle as specified by the Object Filter Vehicle Filter.

Only the Object filter is set to Can Trigger Actions, meaning only this component of the logical rule will be available as a source for actions.

Additionally, any activity generated by the speed filter will have the event type Presence.




### 15.6.10.3 VCA Filters - Colour Filter

The colour filter utilizes the Colour Signature algorithm and provides the ability to filter out objects based on whether that object contains a certain colour component.

The colour signature algorithm is responsible for grouping every pixel from a detected object into one of 10 colour bins.

The colour filter allows you to select one or more of these colour bins and will trigger if the subject-object is made up of one or more of those selected colours.

The below image shows an example tracked object with the colour signature annotations enabled.
Here the top four colours which make up more than 5% of the object are represented by the colour swatch attached to the object.

In this case, a person is being tracked in the scene with high visibility safety clothing. Here the colour filter is set to trigger on Yellow, detecting the person but ignoring the shadow.

Typically, the colour classification filter would be combined with another rule(s) to prevent unwanted objects from triggering an alert, an example rule graph is provided to illustrate this below.

The previous image illustrates how the object classification filter configured with Vehicle class, includes only Vehicle objects.

The person in the zone is filtered out since the Person class is not selected in the filter list.

The channel must have the Colour Signature enabled for the colour filter to work.


| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "Object Filter #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Colours | The colours allowed to trigger an alert | All Unchecked |

#### 15.6.10.3.1 Typical Logical Rule Combination

The below example logical rule checks if the object triggering the presence rule Train line attached to zone Centre, also contains the colour Green as one of the top four colours by percentage.

Only the Colour filter is set to Can Trigger Actions, meaning only this component of the logical rule will be available as a source for actions.

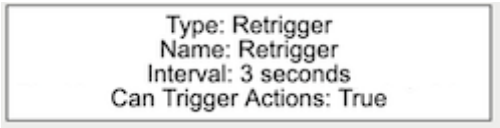
Additionally, any activity generated by the speed filter will have the event type Presence.


## 15.6.10.4 VCA Filters - Retrigger Filter

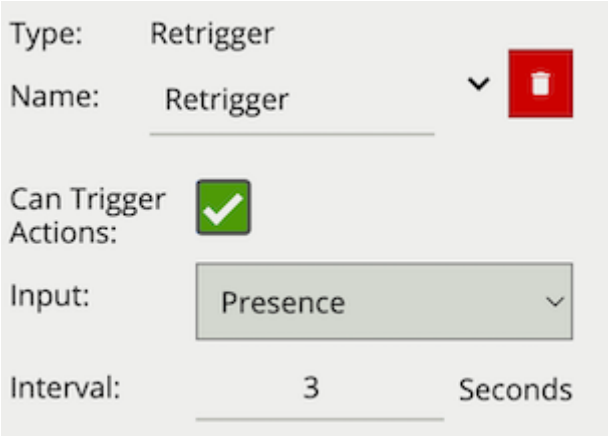
The Retrigger Filter acts as an event pass through, which only generates an event if the input has not fired previously within the defined interval.

Typically, the Retrigger Filter would be applied at the end of a rule(s) combination to prevent duplicate alarms being sent, this provides more granular control than the Event Retrigger Time option. Events produced by the Retrigger Filter will have the event type of the input rule.

#### 15.6.10.4.1 Graphical View




#### 15.6.10.4.2 Form View




#### 15.6.10.4.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Retrigger #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Interval | Period in which the input event cannot generate another event | 3 |

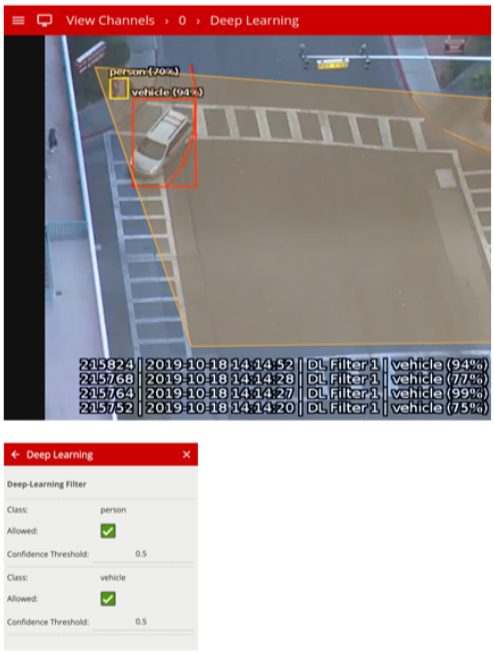
### 15.6.10.5 VCA Filters - Deep Learning Filter

The deep learning filter provides the ability to filter out objects, which trigger a rule if they are not classified as a certain class by the deep learning model.

The deep learning filter settings are configured on the Deep Learning page.

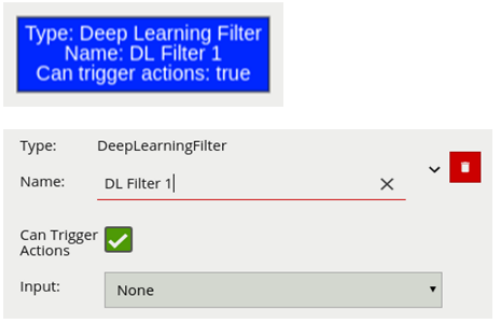
See Deep Learning Filter for an in-depth description of how the filter works.

Typically the deep learning filter would be combined with another rule(s) to prevent unwanted objects from triggering an alert, an example rule graph is provided to illustrate this below. Please note that the deep learning filter cannot be used as an input to any other rule type. As such it must be the last rule in a graph




The previous image illustrates how the deep learning filter configured with just vehicle class (Confidence Threshold 0.5), only triggers on the vehicle object.

The person in the zone is filtered out since the person class Allowed setting is not enabled in the Deep Learning configuration page.




| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | "DL Filter #" |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |

#### 15.6.10.5.1 Typical Logical Rule Combination

The below example logical rule checks if the object triggering the presence rule attached to zone Centre, is one of the classes of interest defined in the Deep Learning settings page (see above settings page image). Only the deep learning filter is set to Can Trigger Actions, meaning only this component of the logical rule will be available as a source for actions.

Additionally, any activity generated by the speed filter will have the event type Presence.


## 15.6.11 Conditional Rule Types

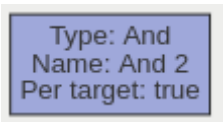
The currently supported conditional rules, along with a detailed description of each.

- And (see page 445)
- Continuously (see page 447)
- Counter (see page 448)
- Not (see page 452)
- Or (see page 453)
- Previous (see page 455)
- Repeatedly (see page 456)

### 15.6.11.1 And

A logical operator that combines two rules and only fires events if both inputs are true.

#### 15.6.11.1.1 Graphical View



#### 15.6.11.1.2 Form View


#### 15.6.11.1.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “And #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input A | The first input | None |
| Input B | The second input | None |
| Per Target | Fire one event per tracked object | Active |

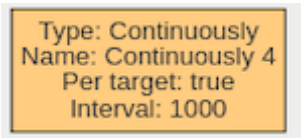
If we consider a scene with two presence rules, connected to two separate zones, connected by an AND rule, the table below explains the behaviour of the Per Target property. Note that object here refers to a tracked object, as detected by the VCA tracking engine.

| State | Per Target | Outcome |
|---|---|---|
| Object A in Input A, Object B in input B | On | Two events generated, one for each object |
| Object A in Input A, Object B in input B | Off | Only one event generated |

## 15.6.11.2 Continuously

A logical operator that fires events when its input has occurred continuously for a user-specified time.

### 15.6.11.2.1 Graphical View




### 15.6.11.2.2 Form View


### 15.6.11.2.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Continuously #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Per Target | Fire one event per tracked object. See description below for more details | Active |
| Interval | The time in milliseconds | 1 |

Considering a scene with a Presence rule associated with a zone and a Continuously rule attached to that Presence rule, when the **Per Target** property is on, the rule will generate an event for each tracked object that is continuously present in the zone. When it is off, only one event will be generated by the rule, even if there are multiple tracked objects within the zone. Additionally, when **Per Target** is off, the rule will only generate events when there is change of state, i.e. the rule condition changes from true to false or vice versa. When **Per Target** is off, the state will change when:

- Any number of objects enter the zone in question and remain in the zone
- **All** objects leave the zone in question

### 15.6.11.3 Counter

Counters can be configured to count the number of times a rule is triggered. For example, the number of people crossing a line. The counter rule is designed to be utilised in two ways:

- **Increment / Decrement**: whereby a counter is incremented by the attached rule(s) (+1 for each rule trigger), and decremented by another attached rule(s) (-1 for each rule trigger).
- **Occupancy**: whereby the counter reflects the number of objects that are currently triggering the attached rule(s).

More than one rule can be assigned to any of a counter's three inputs. This allows, for example, the occupancy of two presence rules to be reflected in a single counter, or more than one entrance / exit gate to reflect in a single counter. An example rule graph is provided to illustrate this below.

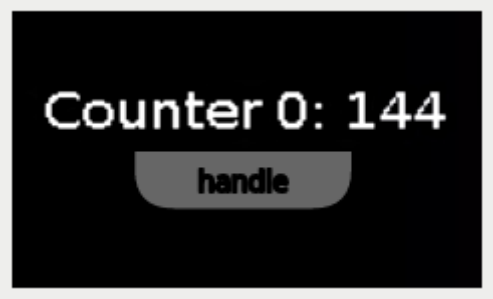
Broadly speaking a single counter should not be used for both purposes occupancy and increment / decrement.

The Counter's Threshold Operator allows the user to limit when a counter generates an event. Based on the selected behaviour and a defined Threshold Value, the counter can be configured to only send events in specific scenarios. Threshold Operators include:

- Greater than or equal to
- Less than or equal to
- Greater than
- Less than
- Equal to
- Not Equal to
- None

#### 15.6.11.3.1 Positioning Counters

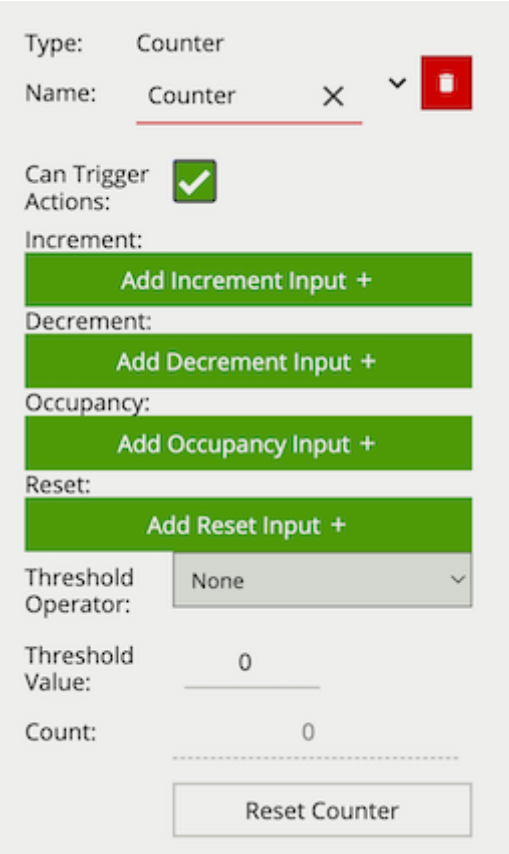
When added, a counter object is visualised on the video stream as seen below. The counter can be repositioned by grabbing the 'handle' beneath the counter name and moving the counter to the desired location.




Right-clicking the mouse (or tap-and-hold on a tablet) on the grid displays the context menu.

#### 15.6.11.3.2 Graphical View

#### 15.6.11.3.3 Form View




#### 15.6.11.3.4 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Counter #” |
| Increment | The rule which, when triggered, will add one to the counter | None |
| Decrement | The rule which, when triggered, will subtract one from the counter | None |
| Occupancy | Sets counter to current number of the rule’s active triggers | None |
| Reset | Resets the `count` to `0` when the assigned rule(s) trigger | None |
| Threshold Operator | Defines when a Counter will trigger events based on the threshold | None |

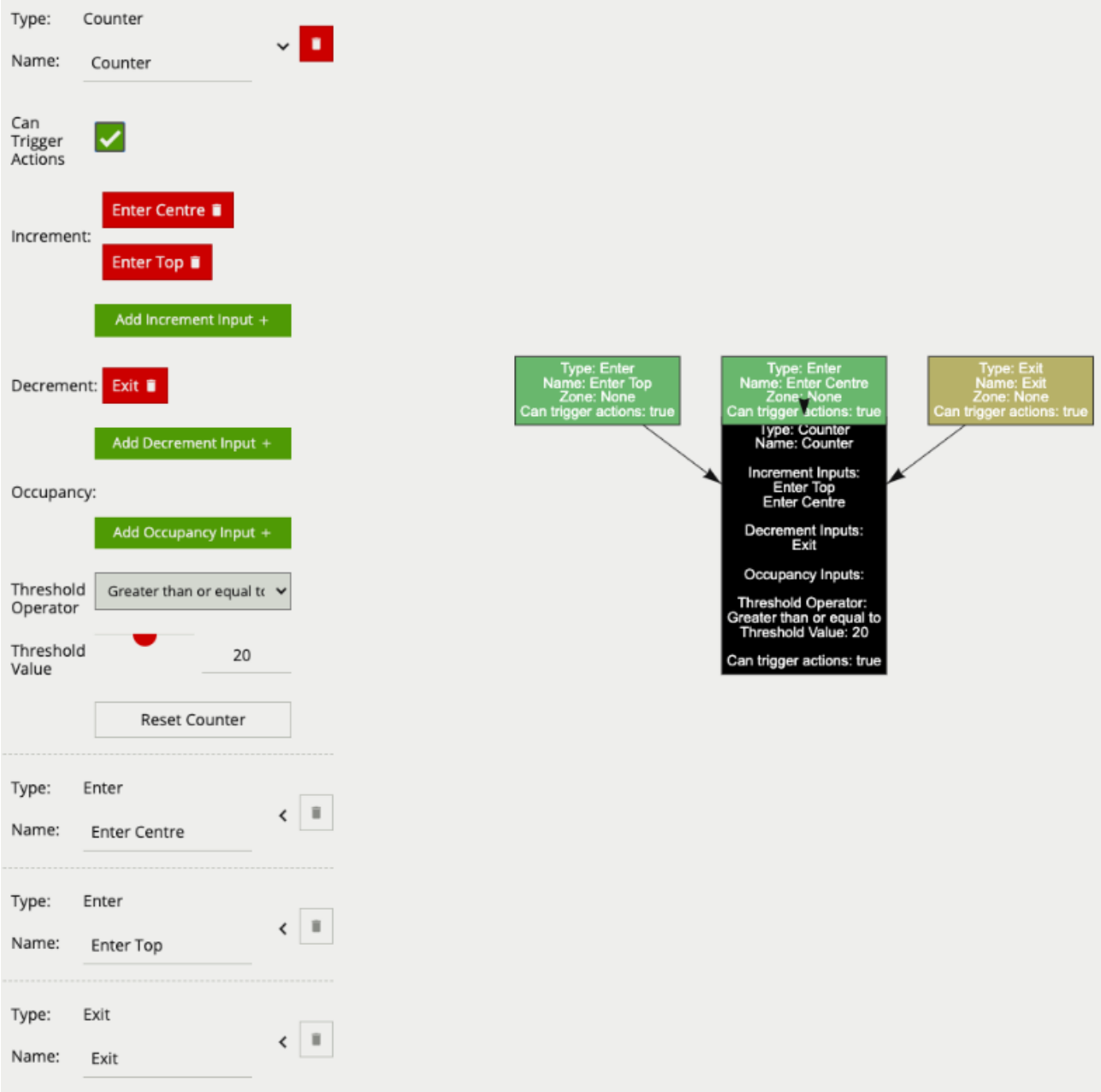
| Property | Description | Default Value |
|---|---|---|
| Threshold Value | The value used by the Threshold Operator to define the behaviour | 0 |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Reset Counter | A button allowing the counter value to be reset to 0 | None |

E.g. if a Presence rule is set as the occupancy target and two objects are currently triggering that Presence rule, the counter will show the value of 2.

#### 15.6.11.3.5 Typical Logical Rule Combination

The below counter example increments a counter based on two enter rules, **Enter Centre** and **Enter Top** attached to the zones **Centre** and **Top** respectively, this means that when either of these enter rules triggers the counter will be incremented by + 1. The counter also decrements based on the exit rule **Exit**, which will subtract 1 from the counter each time an object exits the zone **Centre**. The Threshold Operator and Threshold Value, limit the counter to only generate events when the count is more than 20.

Only the counter rule **Counter** is set to **Can Trigger Actions**, meaning only this component of the logical rule will be available as a source for actions. In this case an action using this rule as a source will trigger every time the counter changes.

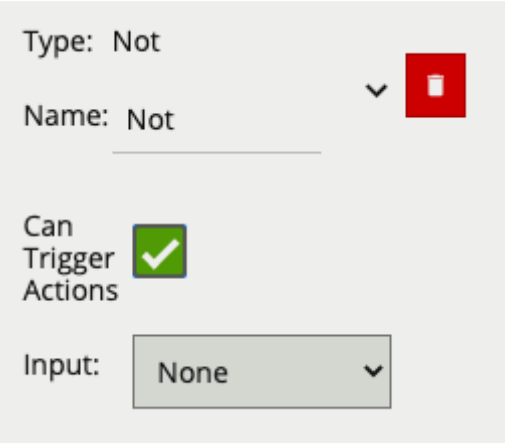



## 15.6.11.4 Not

A logical operator that generates an event when the input rule becomes false.

### 15.6.11.4.1 Graphical View

#### 15.6.11.4.2 Form View



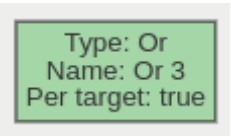

#### 15.6.11.4.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Not #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |

### 15.6.11.5 Or

A logical operator that combines two rules and fires events if either input is true.

#### 15.6.11.5.1 Graphical View



### 15.6.11.5.2 Form View


### 15.6.11.5.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Not #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input A | The first input | None |
| Input B | The second input | None |
| Per Target | Fire one event per tracked object | Active |

If we consider a scene with two Presence rules connected to two separate zones, connected by an OR rule, the table below explains the behaviour of the **Per Target** property.

| State | Per Target | Outcome |
|---|---|---|
| Object A in Input A, No object in input B | On | Two events generated, one for each object |
| No object in Input A, Object B in input B | On | Only one event generated (for Object B) |

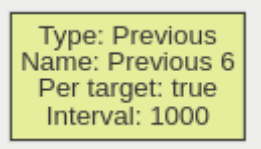
| State | Per Target | Outcome |
|---|---|---|
| Object A in Input A, No object in input B | On | Only one event generated (for Object A) |
| Object A in Input A, No object in input B | Off | Only one event generated |
| No object in Input A, Object B in input B | Off | Only one event generated |
| Object A in Input A, No object in input B | Off | Only one event generated |

Additionally, it is important to note that if the rule fires when **Per Target** is switched off, it will not fire again until it is 'reset', i.e. until the OR condition is no longer true.

## 15.6.11.6 Previous

A logical operator that triggers for input events which were active at some point in a past window of time. This window is defined as between the current time and the period before the current time (specified by the Interval value).

### 15.6.11.6.1 Graphical View




### 15.6.11.6.2 Form View

#### 15.6.11.6.3 Configuration

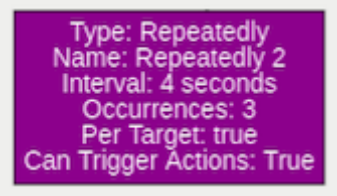
| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Previous #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Per Target | Fire one event per tracked object. See description below for more details | Active |
| Interval | The time in milliseconds | 1 |

## 15.6.11.7 Repeatedly

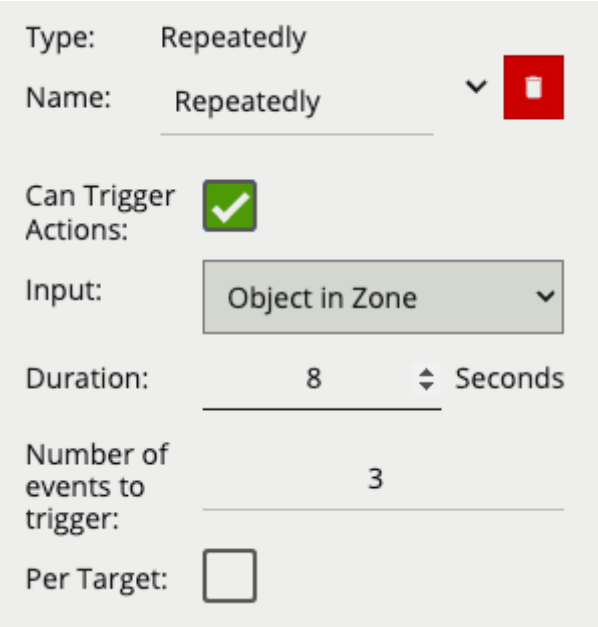
A logical operator that triggers when an input rule is triggered a set number of times within a defined period. The Duration period is a window of time computed from every input event. For example, with a Repeatedly rule configured to generate an event when the input triggers three times in eight seconds, and that input rule triggers four times in eight seconds, the repeatedly rule will trigger after both the third input rule trigger and again after the fourth. This is because the first three triggers (events 1-3) fired within an 8 second window, additionally the second set (events 2-4) also occurred within their own 8 second window.

The Per Target option specifies that it must be the same tracked object that triggers the input.

#### 15.6.11.7.1 Graphical View



#### 15.6.11.7.2 Form View




#### 15.6.11.7.3 Configuration

| Property | Description | Default Value |
|---|---|---|
| Name | A user-specified name for this rule | “Repeatedly #” |
| Can Trigger Actions | Specifies whether events generated by this rule trigger actions | Active |
| Input | The input rule | None |
| Duration | The time in which the Number of Events to Trigger must fire | 3 |
| Number of Events to Trigger | The number of times the input is required to trigger | 4 |
| Per Target | Specifies if the input needs to be triggered by the same object | Inactive |

## 15.6.12 Other Sources



### 15.6.12.1 HTTP

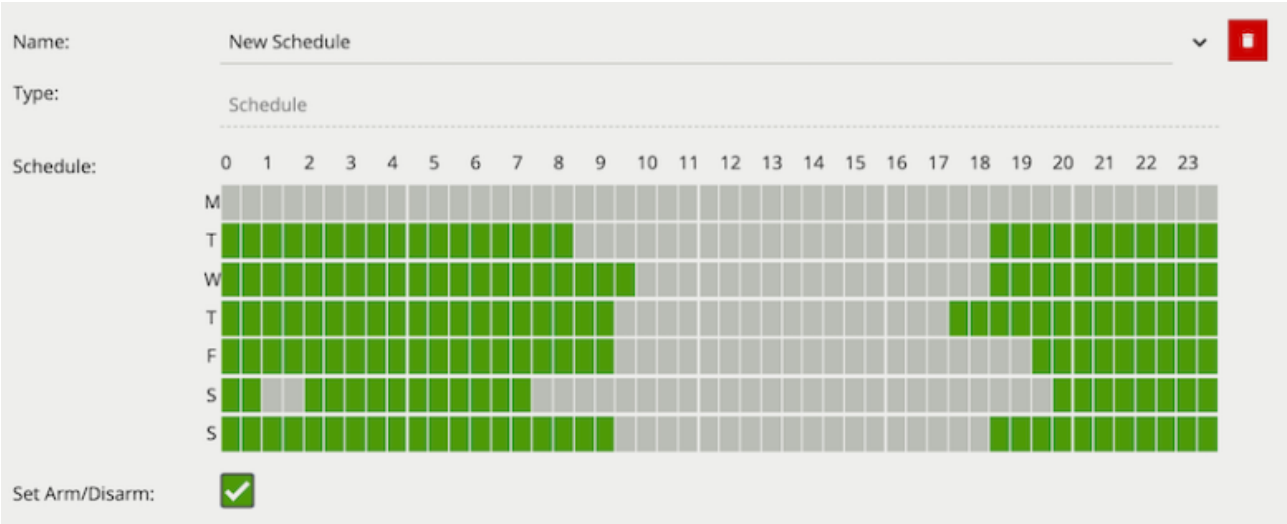
The HTTP source creates an arbitrary REST API endpoint with a state variable that can be set true or false. This creates a virtual Digital Input which third party systems can enable or disable. The HTTP source can be referenced by the [Source Filter] in a rule graph.


#### 15.6.12.1.1 Properties

- **Endpoint URL:** The REST API endpoint defining the state variable.

### 15.6.12.2 Schedule

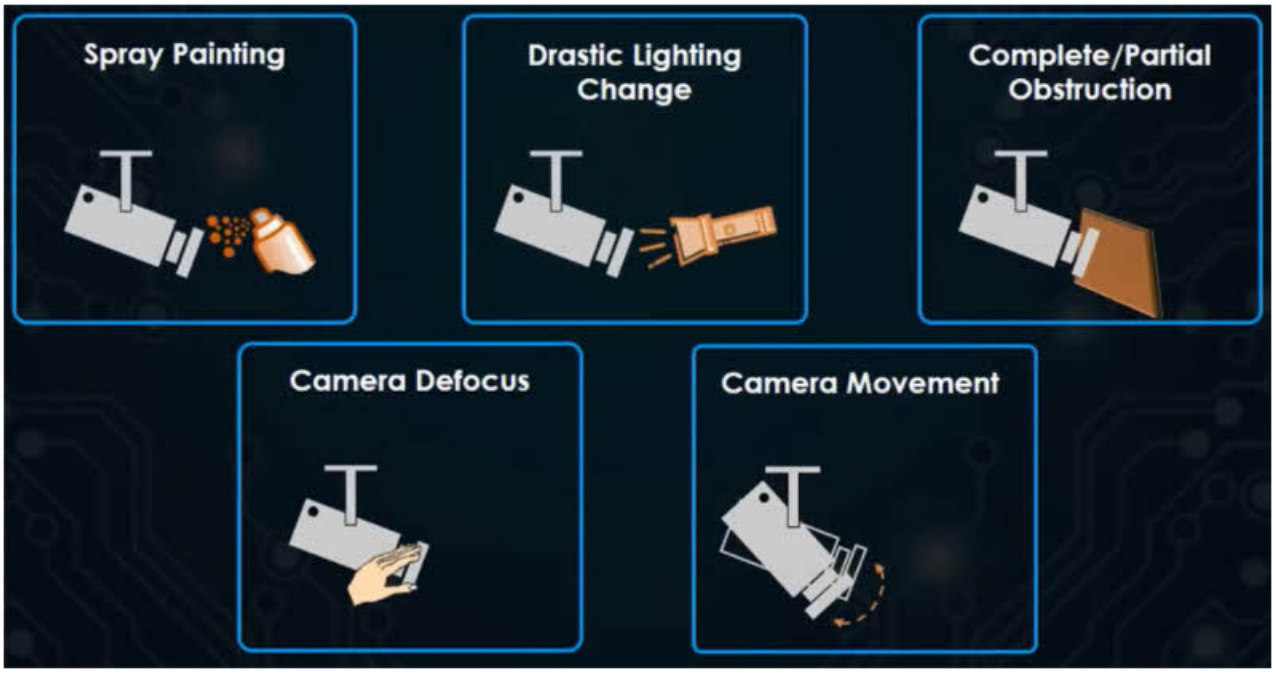
The Schedule source allows the definition of a schedule of time when the source is either on or off. The Schedule other source can be referenced by the [Source Filter] in a rule graph. Additionally, the schedule source can be used to directly control the armed state of VCA.



#### 15.6.12.2.1 Properties

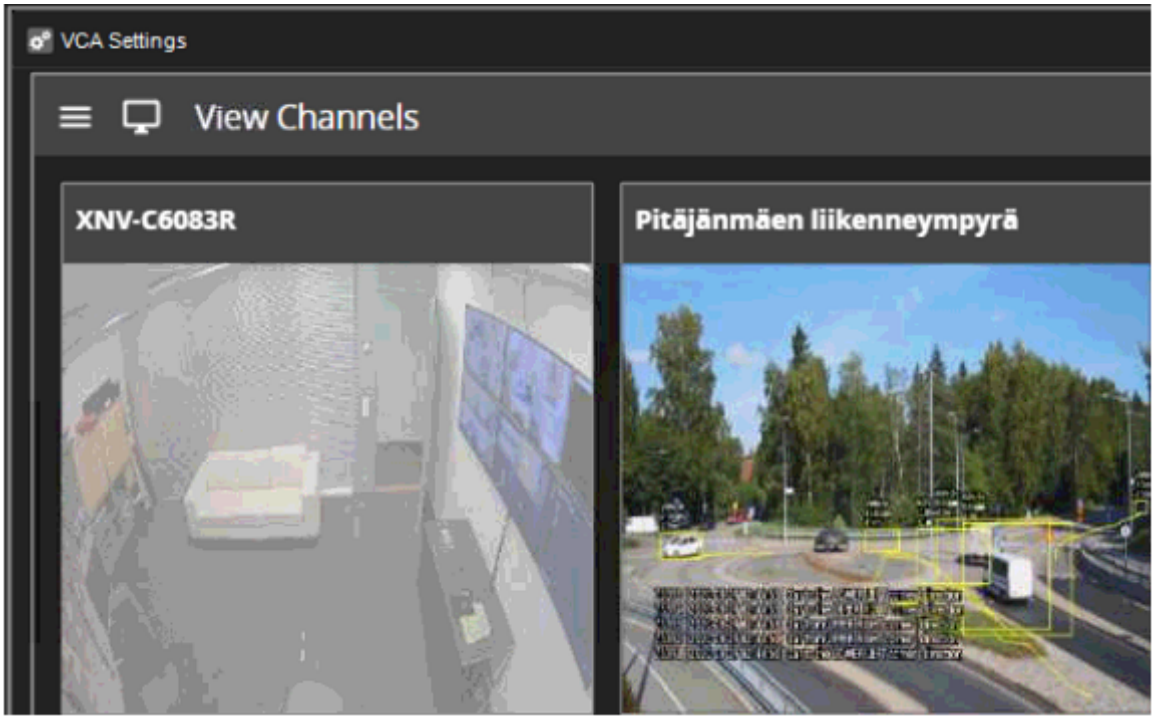
- **Schedule:** A click and drag interface which allows the definition of on periods (in green) and off periods (in grey). Each row represents one of the seven days in a week and each column represents a half hour period in that 24 hours.
- **Set Arm/Disarm:** When checked, the schedule source directly sets VCA Armed state according to the schedule defined above.

## 15.6.13 VCA - Tamper Detection

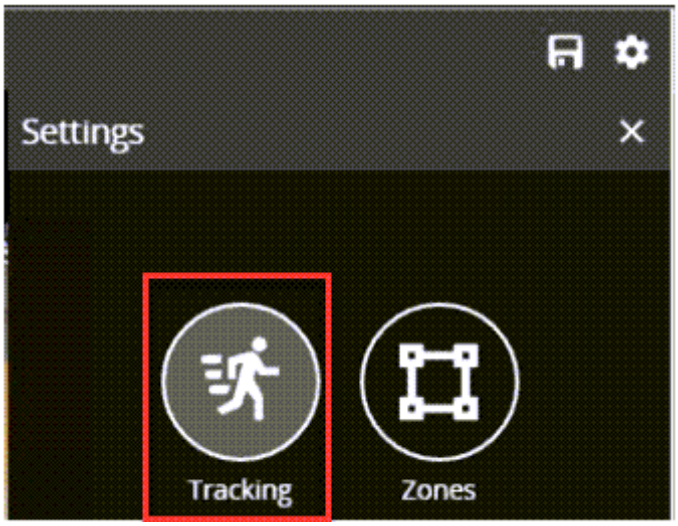



### 15.6.13.1 How to enable Tamper Detection

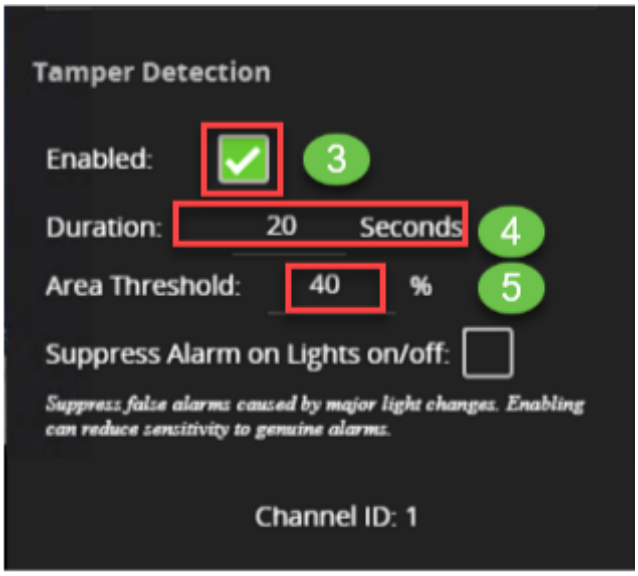
1. Open camera from the View Channels




2. Open **Tracking**

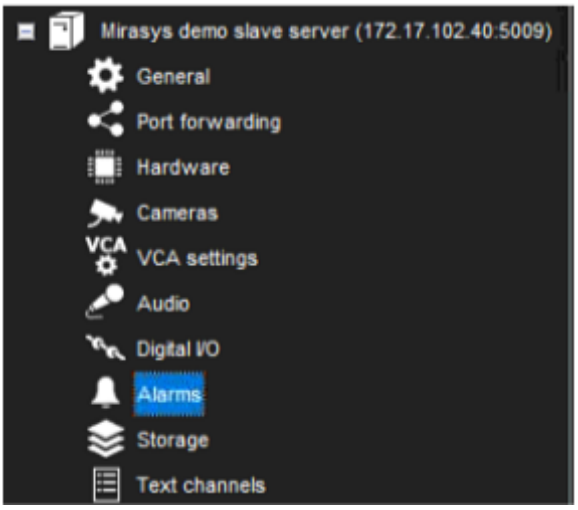



3. Enable Tamper Detection
4. Set **Duration**
5. Set **Area Threshold**

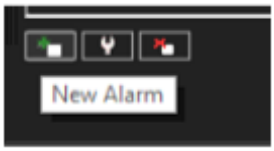



### 15.6.13.2 How to create an alarm from Tamper Detection

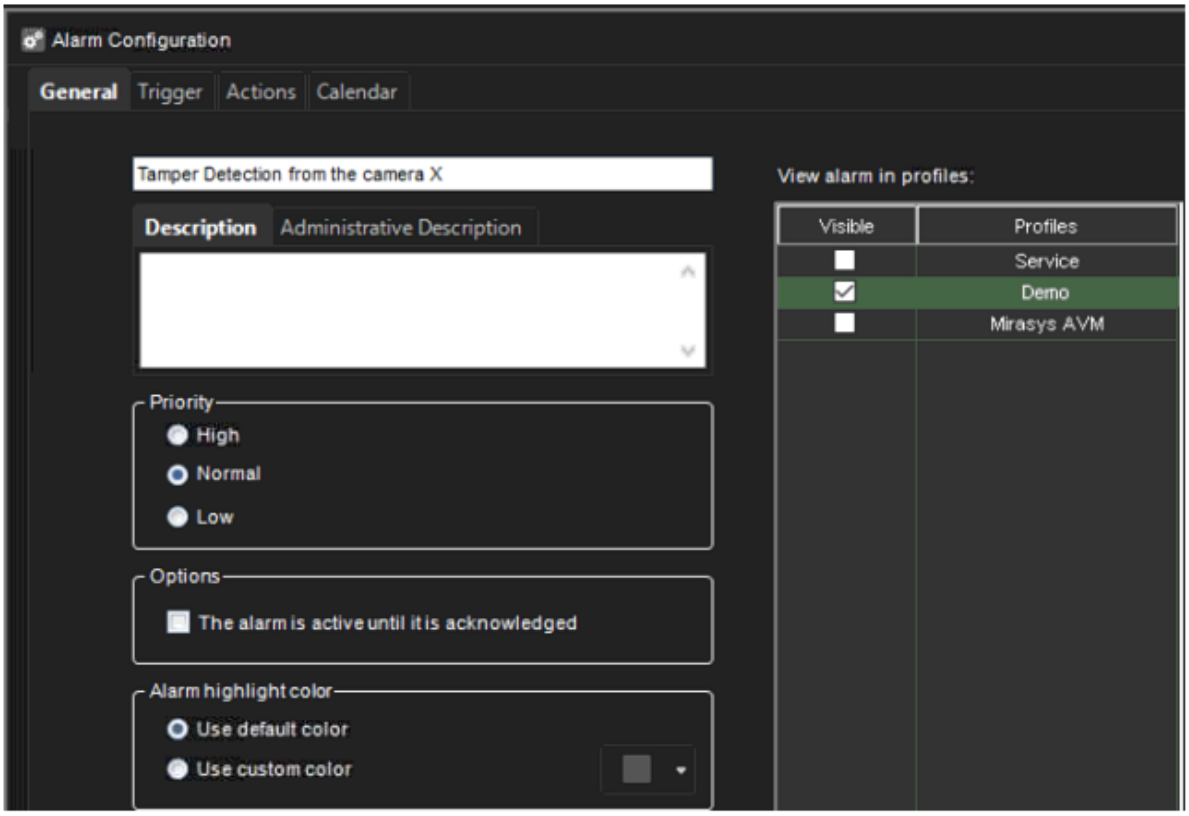
1. Open Alarms from the needed VMS server



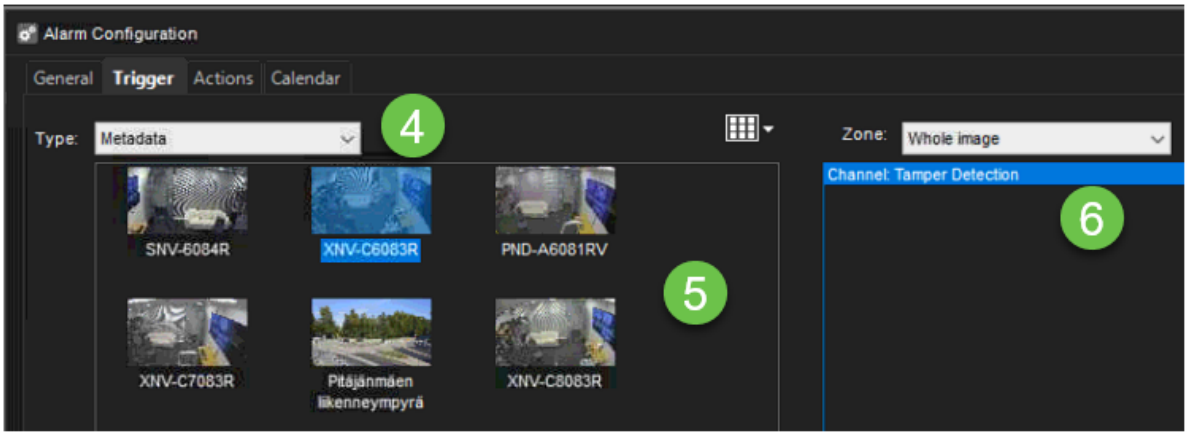

2. Click **New Alarm**




3. Enter the name of the alarm

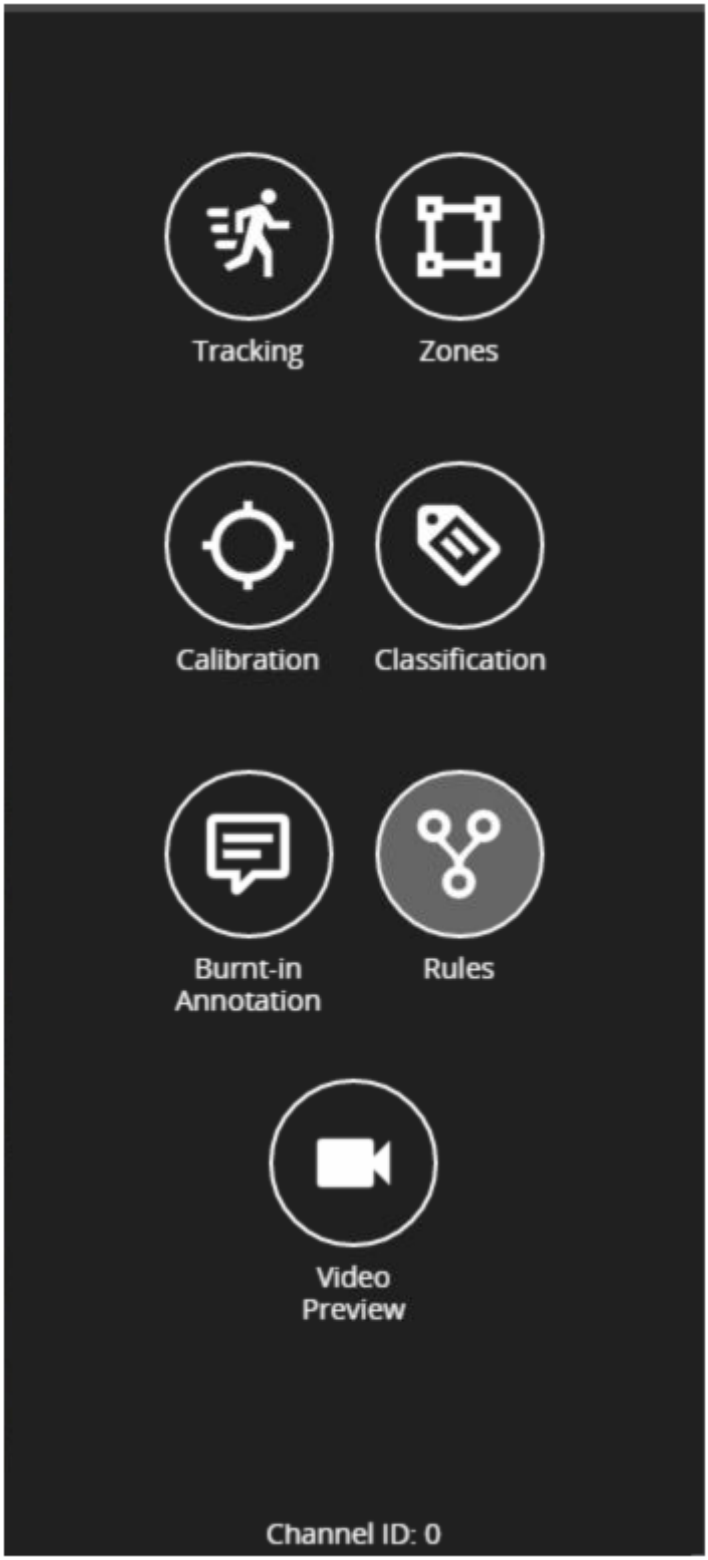



4. Select Trigger **Metadata**
5. Select camera from the list
6. Select Tamper Detection

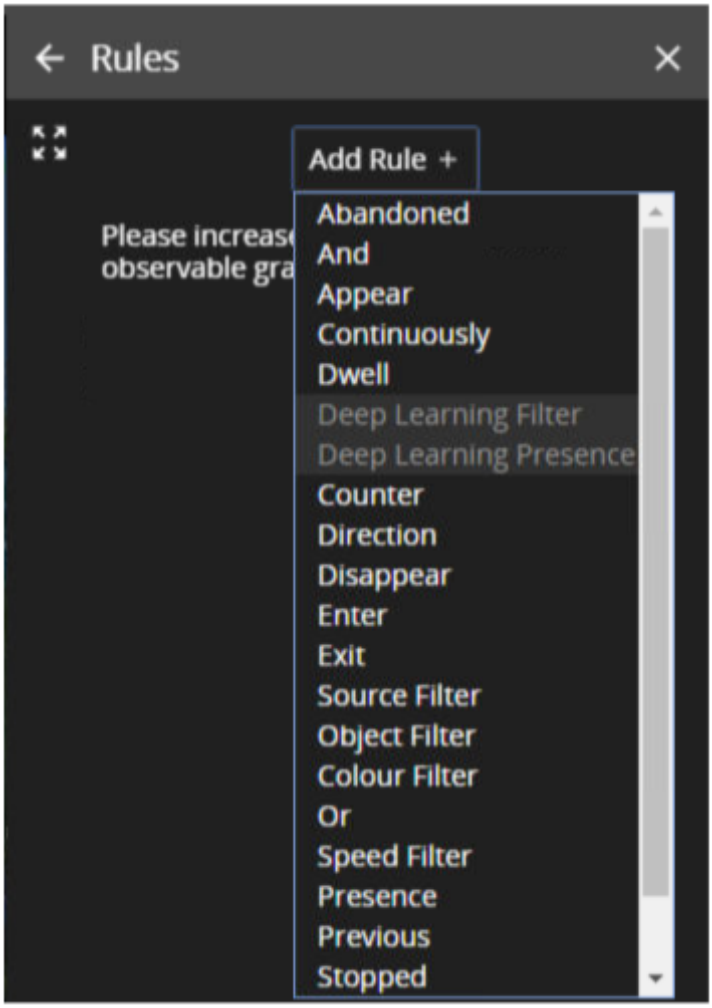



## 15.6.14 How to create rules

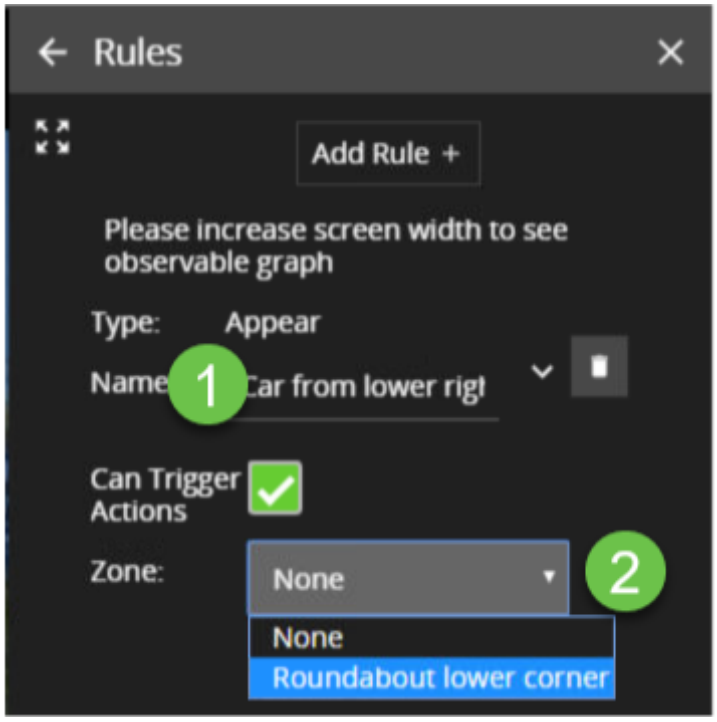
1. Click **Rules**




2. Click **Add Rule**
3. Select rule from the list

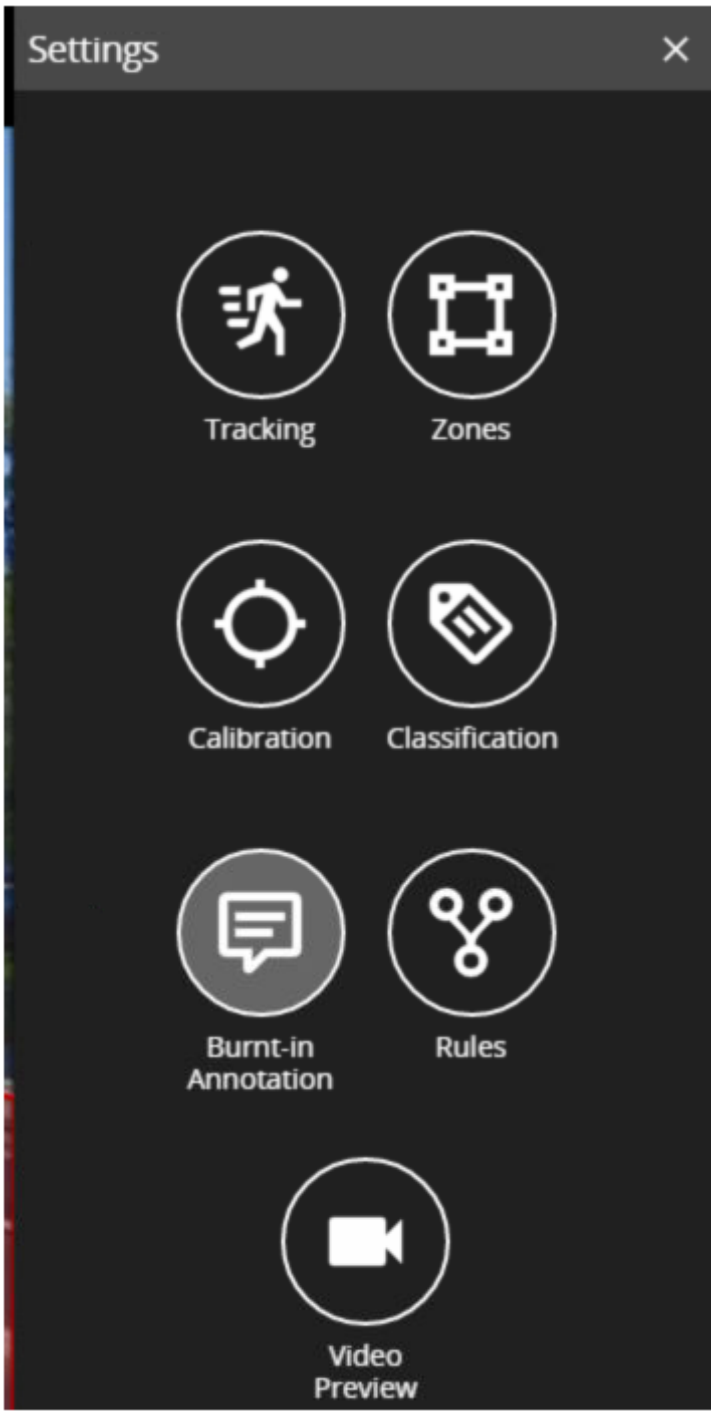



4. Set the name for the rule
5. Select zone

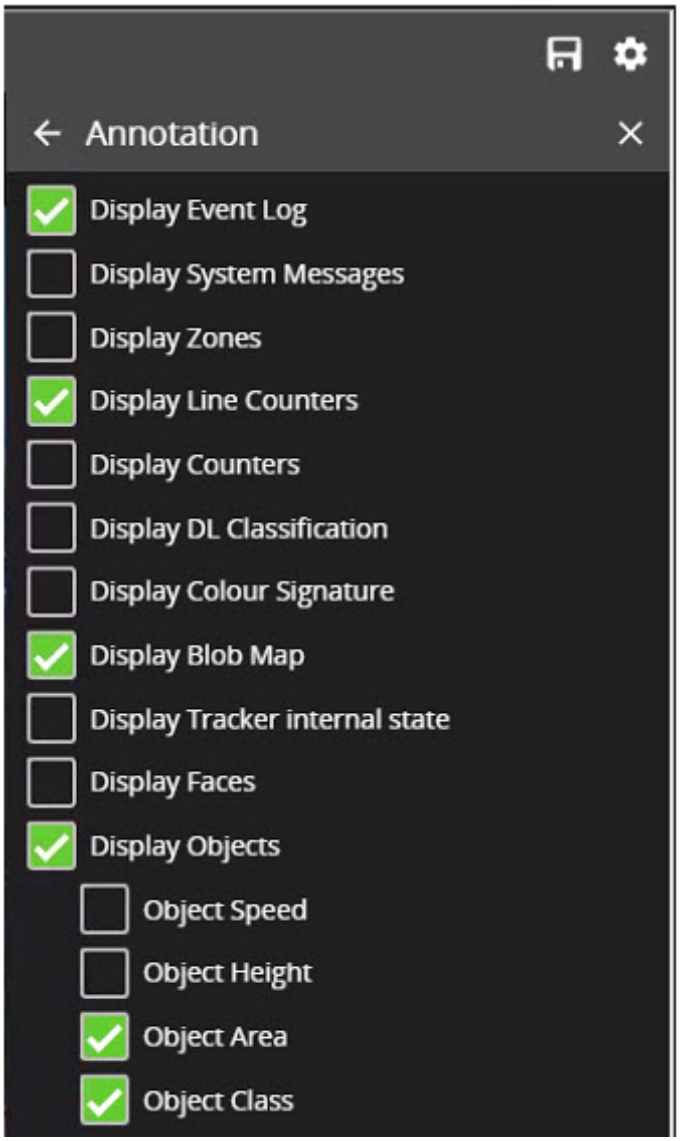



### 15.6.15 How to test rules

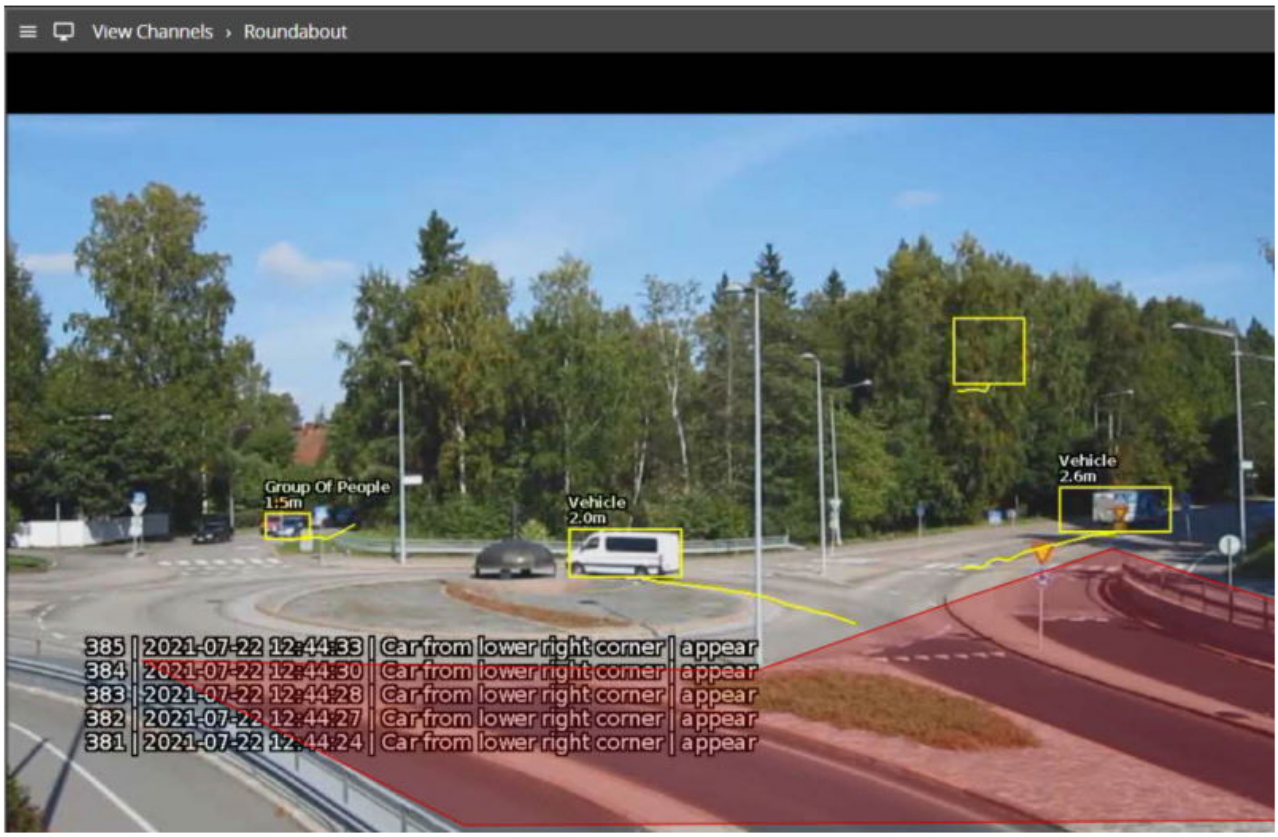
1. Open **Burnt-in Annotation**




2. Enable **Event Log**
3. Enable **Display Line Counters**
4. Enable **Display Blob Map**
5. Enable **Display Objects**
    a. Enable **Object Area**
    b. Enable **Object Class**

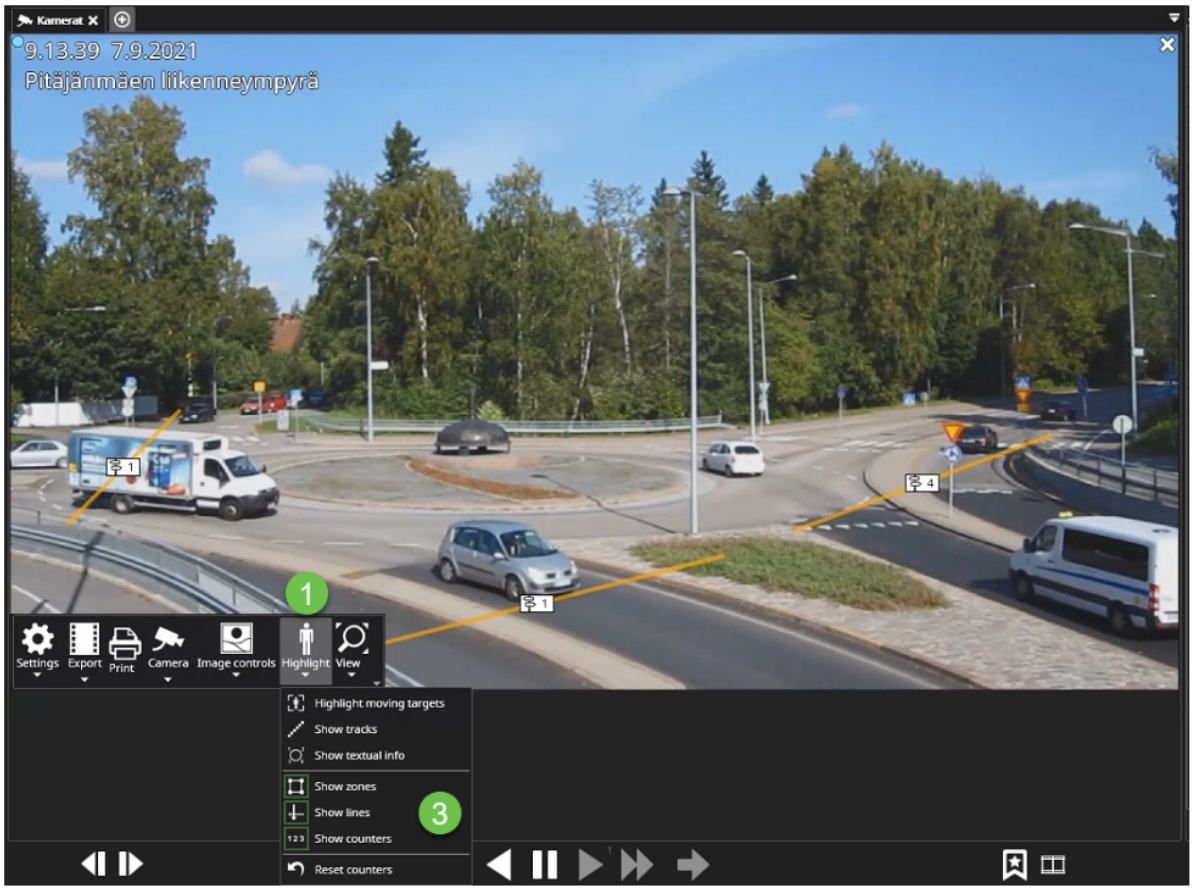



Open the correct camera and check that triggered events can be seen




## 15.6.16 How to view VCA events in the Mirasys Spotter

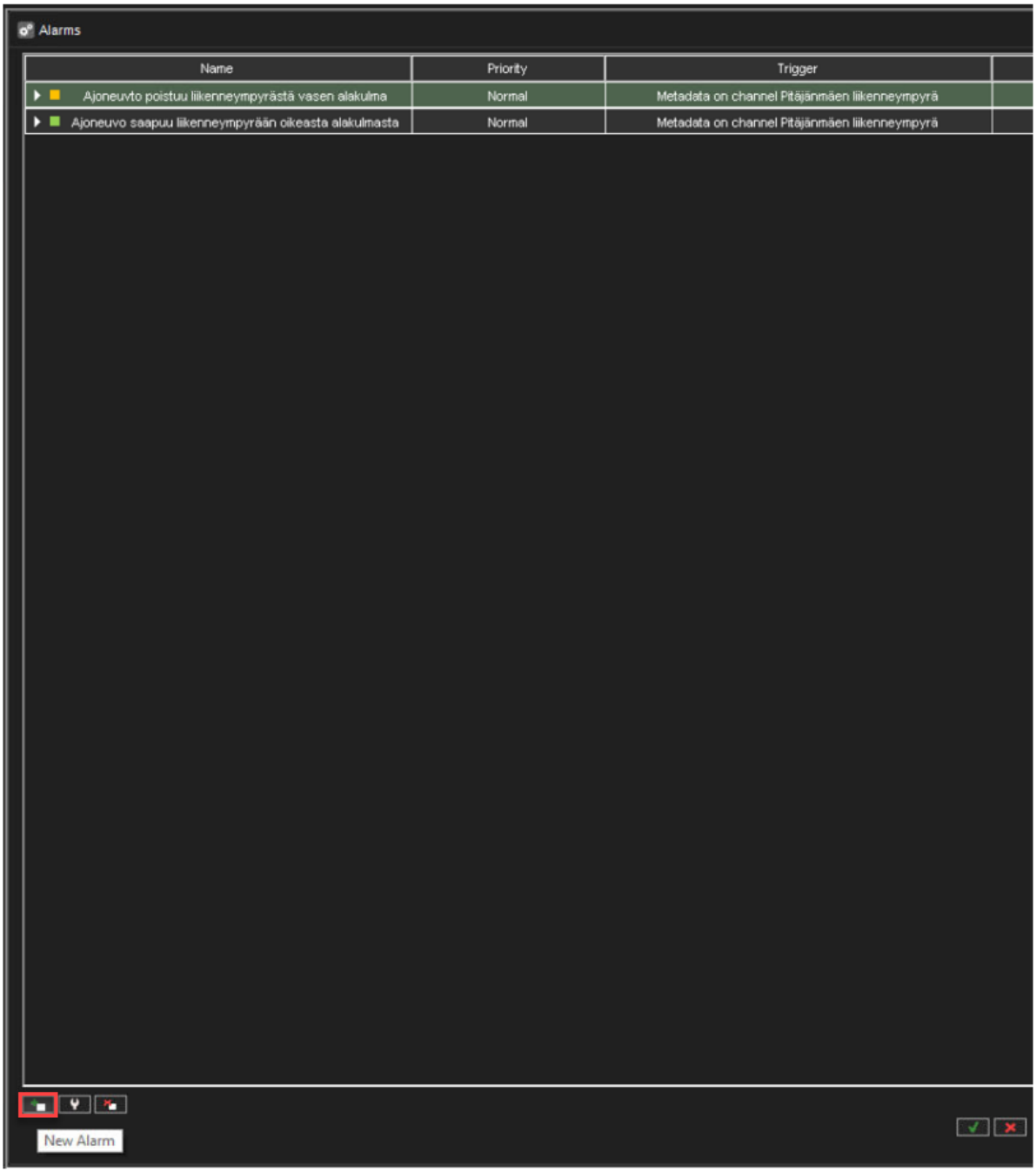
1. Open camera to the real-time view
2. Open camera toolbar and click **Highlight**
3. Enable needed options(**Show zone**s, **Show lines** or **Show counters**



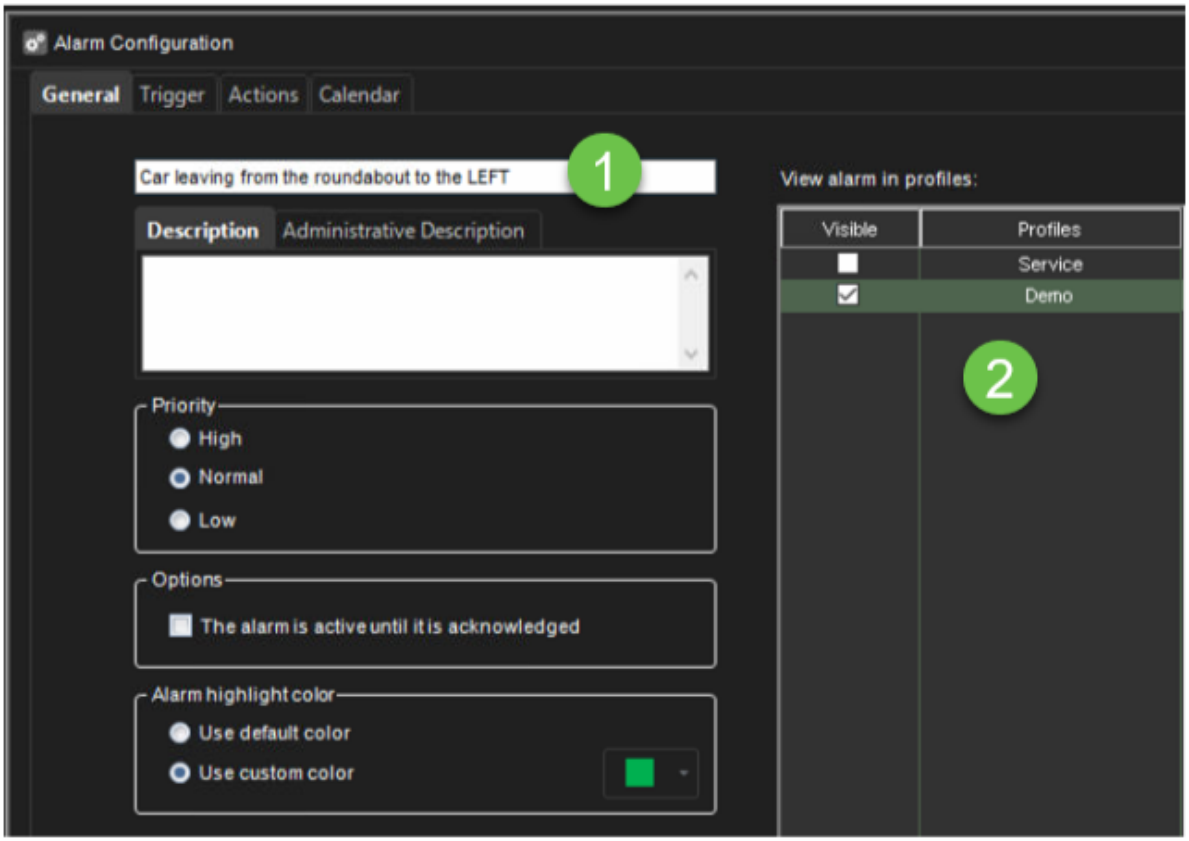

1.

## 15.6.17 How to create an alarm from VCA event

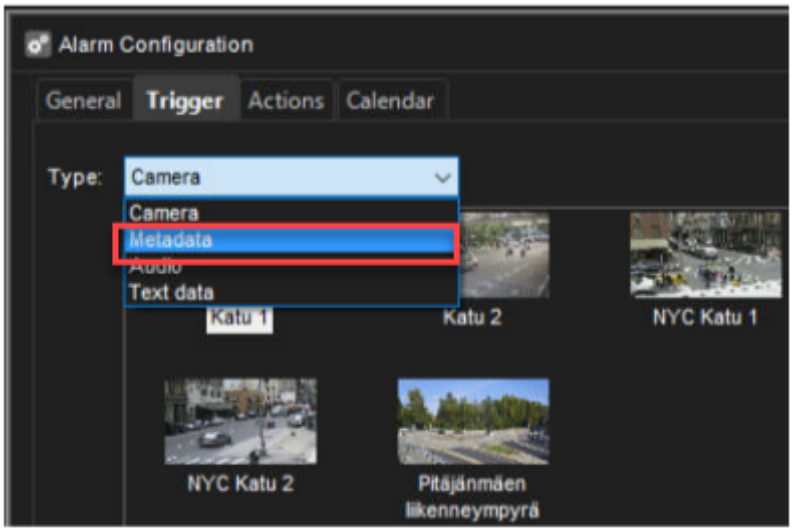
1. Go to the **VMS servers** tab
2. Click **Alarms**
3. Click **New Alarm**



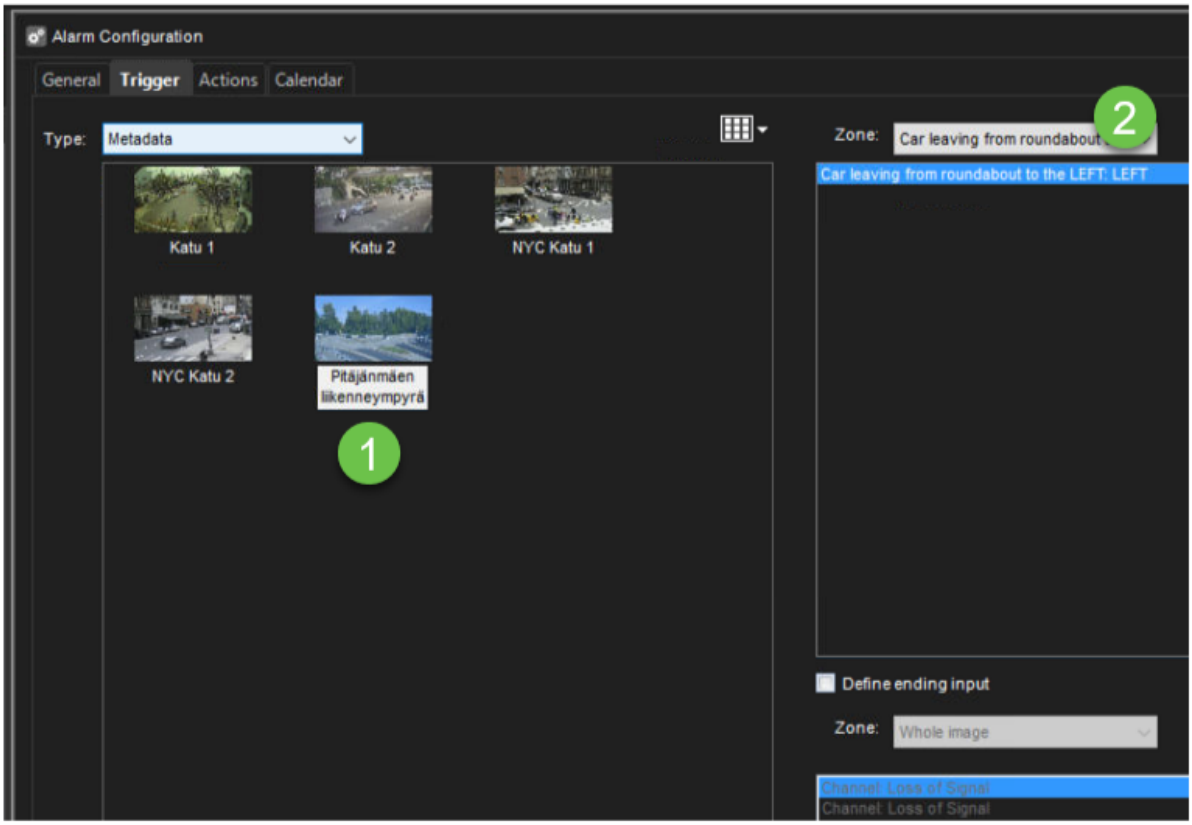

4. Enter the name of the alarm
5. Select the **View alarm in profiles**
6. Go to the **Trigger** tab



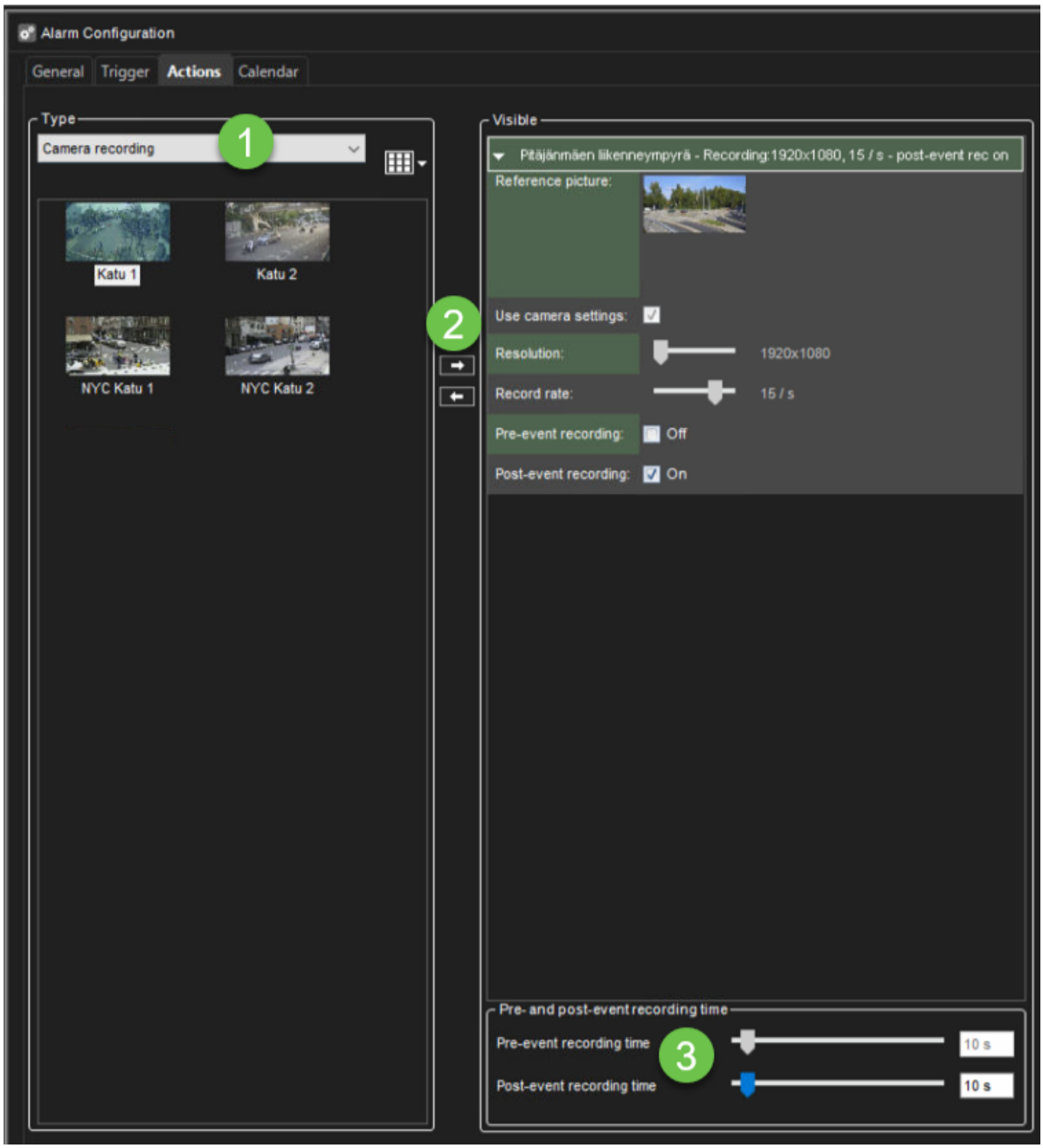

7. Select **Type**: **Metadata**



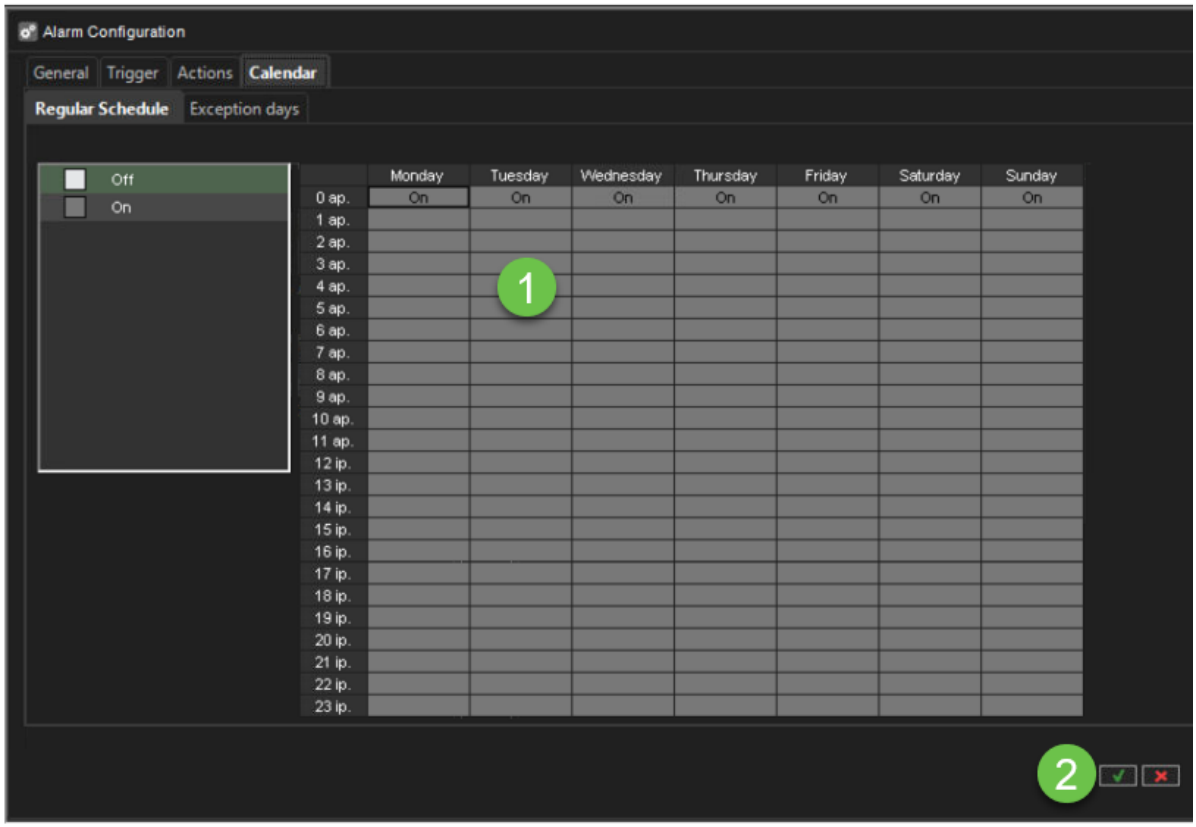

8. Select the correct camera from the list
9. Select zone
10. Go to the **Actions** tab



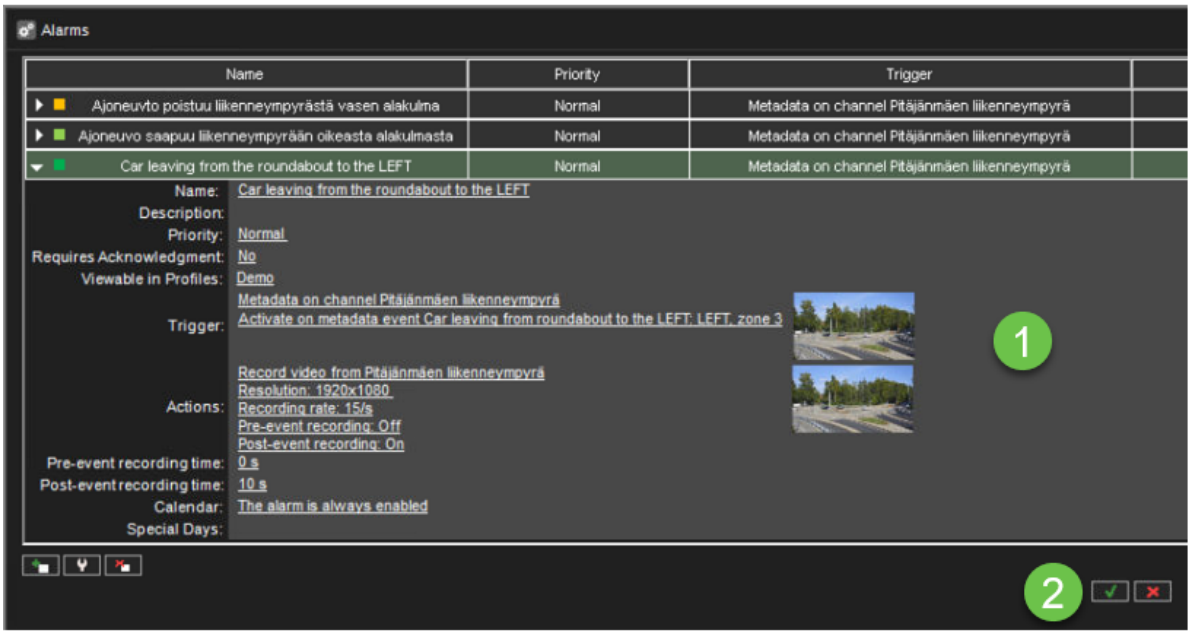

11. Select needed actions
12. Add them to the Visible list
13. Set Pre - and post-event recording time, if needed
14. Go to the **Calendar** tab




15. Set alarm schedule
16. Click OK




17. Check alarm configuration
18. Click OK to finalize alarm creation

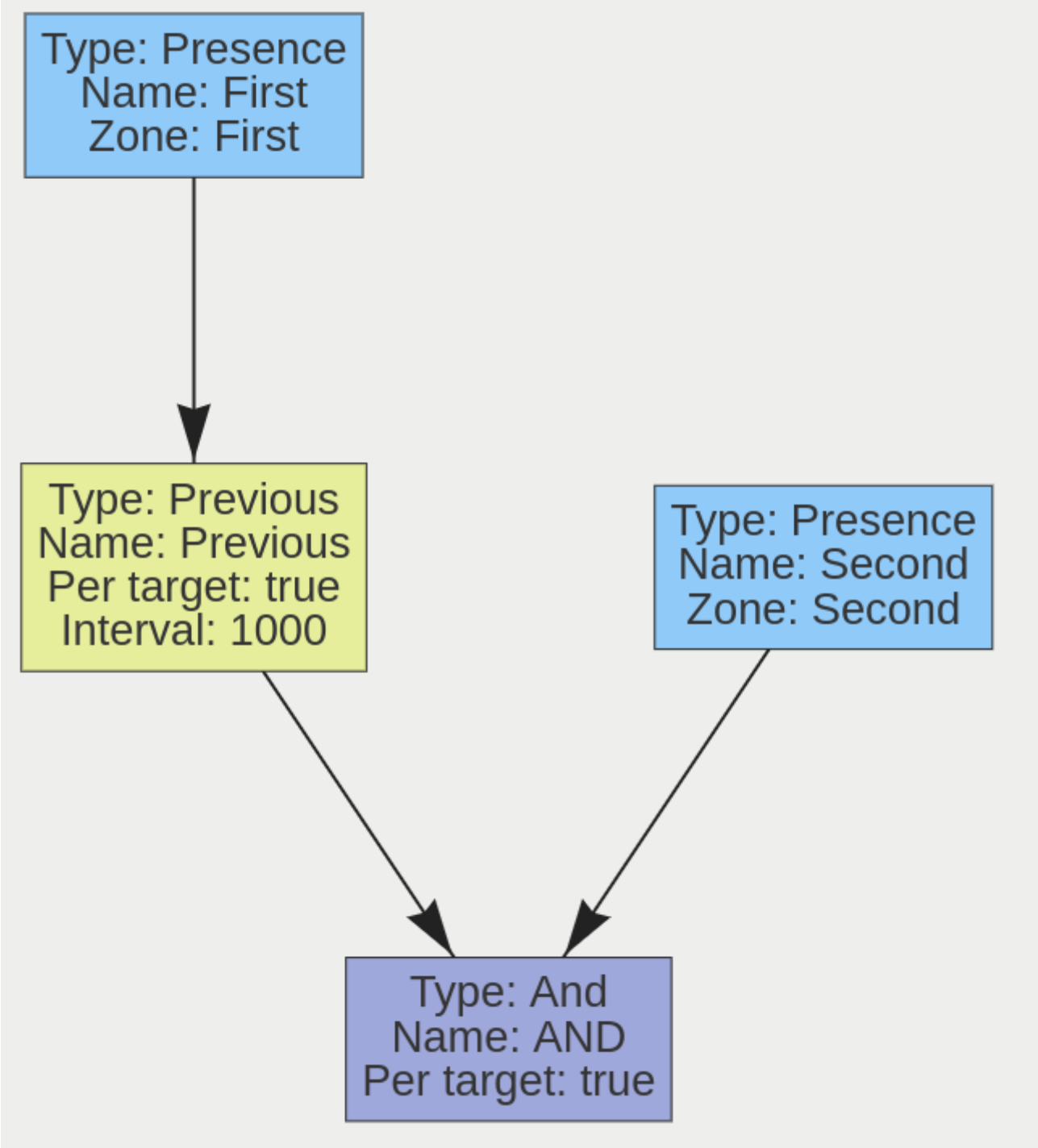


## 15.6.18 Combined Rule Examples



### 15.6.18.1 Double-knock Rule

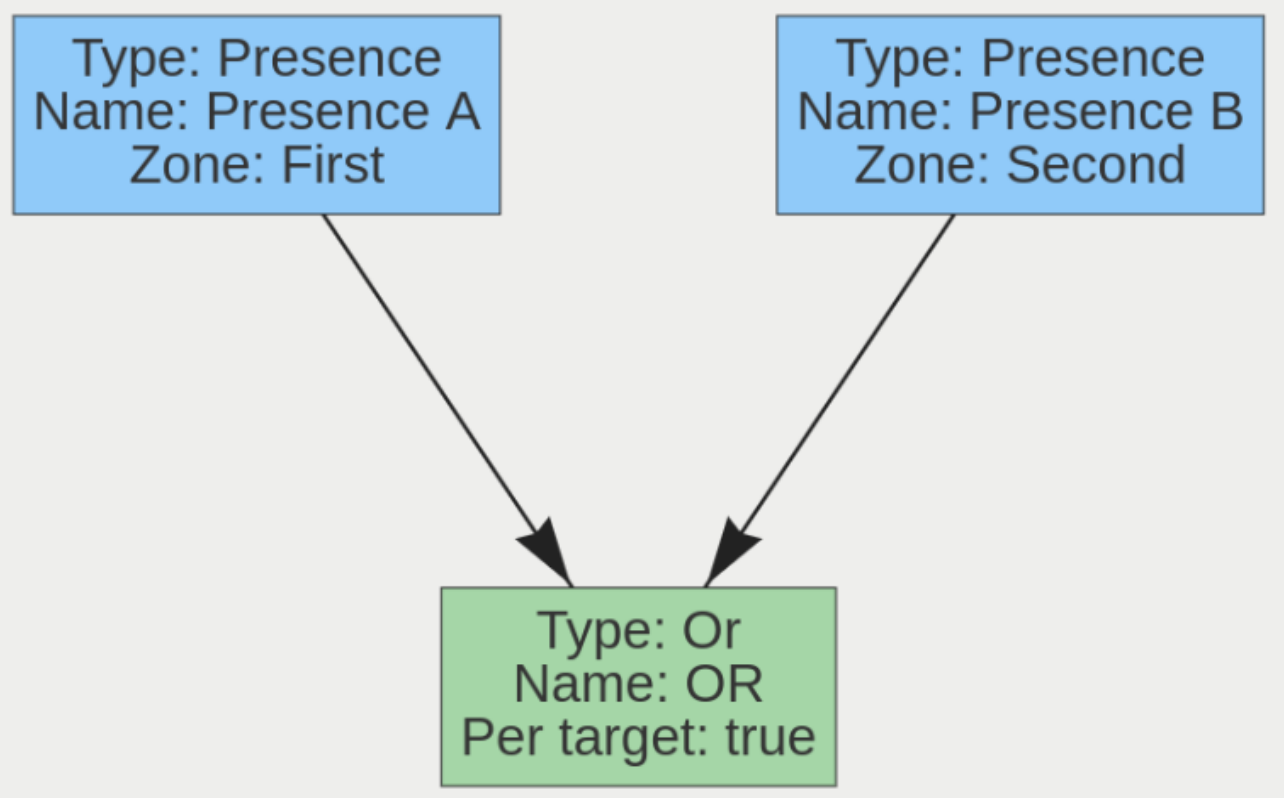
The “double-knock” logical rule triggers when an object enters a zone which had previously entered another defined, zone within a set period of time. The interval on the Previous rule decides how much time can elapse between the object entering the first and second zone. The graph for a double-knock logical rule is as follows:




The rule may be interpreted as follows: “An object is in Zone 2, and was previously in Zone 1 in the last 1000 milliseconds”. This rule can be used as a robust way to detect entry into an area. Since the object has to enter two zones in a specific order, it has the ability to eliminate false positives that may arise from a simple Presence rule.

#### 15.6.18.2 Presence in A or B

This rule triggers when an object is present in either Zone A or Zone B. Its graph is as follows:




A typical use case for this rule is having multiple areas where access is prohibited, but the areas cannot be easily covered by a single zone. Two zones can be created, associated with two separate Presence rules, and they can then be combined using an Or rule.

### 15.6.19 GPU Performance

Here is a basic explanation of what the CPU is used for. The CPU is used for the following

- Decoding the incoming RTSP stream
- Encoding any outgoing annotated RTSP
- Resizing frames before being passed to the analytic engine
- Preprocessing before the frame is passed to the GPU for the DL tracker to process

The first 3 points are currently performed for all trackers, the standard motion object tracker and the DL trackers.

The last point is performed when using the DL trackers and requires some additional resources from the CPU. As a result, the number of channels that can be supported on a particular CPU is reduced when using the DL trackers.

This chart is giving some overview how VCA can perform with GPU. Different scenarios may affect performance.

| GPU | CUDA cores | Tensor cores | Memory | Processor frequency | Memory Bandwidth (GB/sec) | Actual channels DLOT tested |
|---|---|---|---|---|---|---|
| RTX A4000 | 6144 | 192 | 16 GB | 1750 | 448 | 56 |
| GeForce RTX 3070 | 5888 | 180 | 8 GB | 1440-1710 | 19 | 54 |
| GeForce RTX 2080 Ti | 4352 | 368 | 11GB | 1350-1545 | 616 | 50 |
| Tesla T4 | 2560 | 320 | 16GB | | 320 | 45 |
| GeForce GTX 1660 SUPER | 1408 | | 6 GB | 1530-1785 | 336 | 28 |
| GeForce GTX 1650 | 896 | | 4 GB | 1485-1665 | 128 | 18 |