MIRASYS

Mirasys AI Guide

Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

1 CONTENTS

2 Mirasys Object Recognition (OR) 7
2.1 Object Recognition Introduction 7
2.2 OR Service Installation 7
2.2.1 Requirements 7
2.2.2 NVIDIA libraries 8
2.2.3 OR Installation 8
2.2.4 Updating the ODS Service 9
2.2.5 ODS Installation 10
2.3 OR Performance 11
2.3.1 Test setup 11
2.3.2 Test results 12
2.3.3 Performance test results for persons 13
3 Mirasys List Management (LM) 14
3.1 List Management Introduction 14
3.2 LM Service Installation 14
3.2.1 Requirements 14
3.2.2 Updating the List Management Service 14
3.2.3 Installation 15
3.3 PostgreSQL 15 upgrade to PostgreSQL 16 version 21
3.3.1 This guide applies to 21
3.3.2 Requirements 22
3.3.3 How to do upgrade 22
4 Mirasys Face Recognition (FR) 35
4.1 Face Recognition Introduction 35
4.2 FR Service Installation 36
4.2.1 Requirements 36
4.2.2 NVIDIA libraries 36
4.2.3 FR Installation 37
4.3 Privacy masks 46
4.4 FR processing, events, and detection 46

4.4.1 Devices 46
4.4.2 FR events 47
4.4.3 Detected face visualization 47
4.5 FR Alarm triggers and configuration 47
4.5.1 Alarm triggers 47
4.5.2 FR configuration 47
4.6 FR Performance 47
4.6.1 Test computer hardware 47
4.6.2 9.10 version 47
4.6.3 9.9.6 version 49
5 Mirasys License Plate Recognition (LPR) 50
5.1 License Plate Recognition Introduction 50
5.2 LPR Service Installation 50
5.2.1 Requirements 51
5.2.2 NVIDIA libraries 51
5.2.3 Installing the LPR service 52
5.3 LPR Privacy masks 60
5.4 Country Detection 60
5.4.1 Plate number country detection 60
5.4.2 License plate types 61
5.5 Supported countries in Eurasia (LPR) 61
5.5.1 Area codes 61
5.5.2 List of supported countries in Eurasia 62
5.6 Supported countries in the Americas (LPR) 64
5.6.1 Countries and states 64
5.7 LPR processing, events, and detection 67
5.7.1 Devices 67
5.7.2 LPR events 67
5.7.3 Detected license plate visualization 67
5.8 LPR Alarm triggers and configuration 67
5.8.1 Alarm triggers 67

5.8.2 LPR configuration 67
5.9 LPR Performance 67
5.9.1 Test machine 67
5.9.2 How test is done 67
5.9.3 Test results 68
6 Easy LPR (Camera side license plate detection) 72
6.1 Licensing for Easy LPR 72
6.2 Easy LPR configuration 73
6.2.1 Configuration process 73
6.2.2 Camera-specific configurations 74
6.3 Enable Easy LPR 76
7 LPR Camera Installation tips 79
7.1 It is recommended to install the camera in the center of the vehicle 79
7.2 If the camera is installed on the side of the road or lane, the angle should not exceed 30 degrees. 80
7.3 The camera should be installed higher than the vehicle headlights so that the vehicle's headlights don't point directly at the camera 81
7.4 Ensure the license plate width is at least 120 pixels and height at least 50 pixels 81
7.5 License plate tilt angle must be within +/- 10 degrees 81
7.6 LPR settings in the System Manager application 82
7.6.1 Setting the region of interest 82
7.6.2 Enabling country recognition 83
7.7 Common problems and solutions 83
7.7.1 Incomplete license plate 83
7.7.2 View angle makes plate numbers unreadable 84
7.7.3 Other vehicles headlights reflect from license plate 84
7.7.4 The license plate is too small 84
7.7.5 The license plate is blurry 84
7.7.6 The license plate is overexposed 84
8 Mirasys VCA Guide 85
8.1 About Mirasys VCA 85
8.1.1 Motion object tracking 85
8.1.2 Tripwire counting 85

8.1.3 Object behaviour/attributes detection 86
8.1.4 Related analytics options 86
8.2 Quick start guide for VCA 86
8.3 Prerequisites for Mirasys VCA 87
8.3.1 Exporting VCA Core HW GUID file 87
8.3.2 Activating VCA licenses 89
8.3.3 Setting up the resolution and record rate 92
8.3.4 Selecting VCA Stream 93
8.3.5 Activating VCA Core for the cameras 93
8.4 Supported operating systems 94
8.5 VCA Settings on System Manager 95
8.5.1 View Channels 95
8.5.2 Settings 96
8.5.3 Edit Sources 97
8.5.4 Licenses 98
8.5.5 Support 98
8.6 Mirasys VCA Deep Learning 99
8.6.1 Requirements 99
8.6.2 Installation 99
8.7 Mirasys VCA License Server 101
8.7.1 Port 101
8.7.2 Installation 101
8.7.3 Usage and licensing 103
8.7.4 Mirasys VMS Configuration 107
8.8 Cloud Licensing 109
8.9 VCA Channel Settings 110
8.9.1 Initialization 111
8.9.2 VCA Trackers 111
8.9.3 VCA Zones 118
8.9.4 VCA Calibration 123
8.9.5 VCA Classification 130

8.9.6 VCA Burnt-in Annotation 132
8.9.7 VCA Rules 134
8.9.8 VCA - Deep-Learning Filter 173
8.10 VCA - Filters 174
8.10.1 Speed Filter 175
8.10.2 VCA Filters - Object Filter 177
8.10.3 VCA Filters - Colour Filter 179
8.10.4 VCA Filters - Retrigger Filter 183
8.10.5 VCA Filters - Deep Learning Filter 183
8.11 Conditional Rule Types 187
8.11.1 And 187
8.11.2 Continuously 188
8.11.3 Counter 189
8.11.4 Not 194
8.11.5 Or 195
8.11.6 Previous 197
8.11.7 Repeatedly 197
8.12 Other Sources 198
8.12.1 HTTP 199
8.12.2 Schedule 199
8.13 VCA - Tamper Detection 200
8.13.1 How to enable Tamper Detection 200
8.13.2 How to create an alarm from Tamper Detection 202
8.14 How to create rules 204
8.15 How to test rules 207
8.16 How to view VCA events in the Mirasys Spotter 210
8.17 How to create an alarm from VCA event 211
8.18 Configuration 218
8.19 Combined Rule Examples 219
8.19.1 Double-knock Rule 219
8.19.2 Presence in A or B 221

8.20 GPU Performance 221

2 MIRASYS OBJECT RECOGNITION (OR)

2.1 OBJECT RECOGNITION INTRODUCTION

Object Recognition Search allows operators to search recordings for attributes for both persons and vehicles. The object recognition search searches by the following criteria: where (which cameras), when (time frame), and what (humans or vehicles and their attributes).

For persons, searchable attributes are upper body clothing color (Black, White, Gray, Blue, Green, Red, Yellow), lower body clothing color (Black, Blue, White, Gray, Brown, Green), if they are carrying a bag (generic), and if they are wearing a headwear (generic).

Vehicles can be searched by type (car, motorcycle, van, truck, bicycle, or bus) and by color (Black, Blue, Brown, Gray, Green, Orange, Red, White, and Yellow).

Objects to be detected can be selected in the Object Recognition settings. OR will detect only the selected objects, making resource usage more effective. The following setting options are available:

- Enable person attributes
- Enable vehicle attributes
- Enable person similarity identification

2.2 OR SERVICE INSTALLATION

For Object Recognition (OR), you need to install the ORService and ODSService packages. OR carries out the object recognition, and ODS stores the object recognition events in PostgreSQL.

2.2.1 Requirements

- Administrator rights
- Object Recognition license on the VMS Management Server
- RTSP license feature on the VMS Management Server and the VMS Server
- Required NVIDIA libraries (CUDA, cuDNN, TensorRT) are installed

The Object Data Store Service has a similarity search cache to speed up Similarity Search, which can be switched on or off.
Note: Using the cache will increase the memory consumption.

You can enable or disable the similarity search cache when installing the service.

NVIDIA libraries (CUDA cuDNN, TensorRT) are not included in the OR installer. The installer will detect the presence of the NVIDIA library installers from the 'NVIDIA' subfolder and install the libraries automatically if they are found.

2.2.2 NVIDIA libraries

Required NVIDIA libraries should be installed before installing the OR service if they have not yet been installed. Installation of the OR service requires the installation of the following NVIDIA libraries for Windows:

- CUDA Toolkit 12.9 Update 1: https://developer.nvidia.com/cuda-12-9-1-download-archive
- cuDNN 9.20.0: https://developer.nvidia.com/cudnn-9-20-0-download-archive
- TensorRT v10.16.0.72 GA for Windows 10, 11, Server 2022 and CUDA 12.0 to 12.9 ZIP Package: https://developer.nvidia.com/tensorrt/download/10x

2.2.2.1 Installing NVIDIA libraries

1. Download the Mirasys OR service installer and place it in a folder on your machine
2. Create a subfolder 'NVIDIA'
3. Download the NVIDIA libraries mentioned above
4. Save the downloaded NVIDIA libraries to the 'NVIDIA' subfolder
5. Run the Mirasys OR service installer
    a. Mirasys OR service installer automatically installs the NVIDIA libraries that it detects from the 'NVIDIA' subfolder before the service is installed
6. Follow the installation instructions to finalize the installation

2.2.3 OR Installation

The installer has a step for accepting the End-User License Agreement (EULA). You must confirm that you accept the terms presented in the agreement to continue with the installation.

1. Download the latest version from Extranet.
2. Unzip the files e.g. to the `C:\temp` folder.
3. Start the installation by double-clicking the installation file.
4. Click **Install** to continue.

5. Click **Next** to continue.
6. Check **I accept the terms in the License Agreement** and click **Next**.
7. Change the installation location if needed; if not, click **Next** to continue.
8. Change the service address, service HTTP port, main server address and port, the event queue address and port if needed.
    a. If you install the service on a machine other than VMS Main, you need to change the Main server address to the correct one. The same applies for Event queue address.
    b. Change the service address to one accessible from client applications. By default, the service address is the machine's first detected IP address.

The HTTP port where the OR service is hosted is by default 8092. Change the port in case the default port is reserved for some other use.
The main server uses port 8082 by default. Set the main server address and port to allow the OR service to connect to the correct main server.
Event queue uses port 5672 by default. The event queue is installed with the ODS service installation, where the used event queue port is set. Set the event queue address to the machine where the ODS service is installed.

1. Click **Next** to continue.
2. Select at least one of the devices that will be used for OR:
    - CPU
    - Intel GPU
    - NVIDIA GPU
3. Click **Install** to continue and wait.

Installation will take some time until it is finished.
Model creation can take up to 30 minutes. This depends on how powerful the graphics card in use is.

1. Click **Finish** to continue.
2. Click **Close** to close the installation.

2.2.4 Updating the ODS Service

Before updating the Object Data Store Service to a newer version, create a full backup in System Manager and uninstall RabbitMQ Server and Erlang OTP – these can be uninstalled in the Windows settings or the Control Panel. After uninstalling the old ODS version and the extra components, you can proceed with the installation with the instructions below. Note that the uninstallation needs to be done only once; there is no need to uninstall RabbitMQ

Server and Erlang OTP if that is already done by the List Management Service or the Object Data Storage Service update phase.

The minimum version required of RabbitMQ is 3.13.0. The ODS installation includes Erlang 27.3.4.6 and RabbitMQ 4.2.0

2.2.5 ODS Installation

The installer has a step for accepting the End-User License Agreement (EULA). You must confirm that you accept the terms presented in the agreement to continue with the installation.

1. Download the latest version from Extranet.
2. Unzip the files e.g. to the `C:\temp` folder.
3. Start the installation by double-clicking the installation file.
4. Set the PostgreSQL database password
    a. The default password is postgres

PostgreSQL will be installed with the ODS service if it hasn't already been installed earlier.

Currently, there is no support for a separate PostgreSQL server, with the exception of an existing installation of PostgreSQL version 15 or 16.

1. Click **Install** to continue.
2. Click **Next** to continue.
3. Change the installation location if needed, and click **Next** to continue.
4. Change the service address, service HTTP port, main server address and port, the event queue address and port if needed.
    a. If you install the service on a machine other than VMS Main, you need to change the Main server address to the correct one. The same applies for Event queue address.
    b. Change the service address to one accessible from client applications. By default, the service address is the machine's first detected IP address.

The HTTP port where the ODS service is hosted is by default 8093. Change the port in case the default port is reserved for some other use.
The main server uses port 8082 by default. Set the main server address and port to allow the ODS service to connect to the correct main server.
Event queue uses port 5672 by default. The event queue is installed with the ODS service. Change the event queue port in case the default port is reserved for some other use.

1. Click **Next** to continue.
2. Click **Install** to continue and wait.
3. Click **Finish** to continue.
4. Click **Close** to close the installation.

2.3 OR PERFORMANCE

2.3.1 Test setup

Object recognition performance tests were done using a dedicated machine that only runs the Object Recognition service with the following hardware:

- CPU: 12th Gen Intel(R) Core(TM) i9-12900KF @ 3.20 GHz.
- NVIDIA GPU: NVIDIA GeForce RTX 3080 Ti.
- Intel GPU: Intel UHD Graphics 750.

During the test, the following metrics were observed and collected:

- Input frame rate
- Output frame rate
- Memory usage (RAM)
- CPU usage
- GPU usage for model interference
- GPU usage for video decompression
- GPU memory usage

Tests were performed by using H.264 compressed video clip with 1920x1080 resolution.

2.3.2 Test results

2.3.2.1 Performance Test Results for Vehicles

2.3.2.1.1 CPU: 12th Gen Intel(R) Core(TM) i9-12900KF @ 3.20 GHz

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	GPU memory
1	4	4	25%	4.6 GB	4%	3%	3.5 GB
2	8	8	45 %	4.8 GB	8%	8%	3.8 GB
3	10	10	88%	5.6 GB	11%	11%	4.1 GB

2.3.2.1.2 NVIDIA GPU: NVIDIA GeForce RTX 3080 Ti

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	GPU memory
1	4	4	3%	2.8 GB	25%	3%	3.9 GB
2	8	8	4 %	3.5 GB	30%	5%	4.2 GB
3	12	12	5%	3.7 GB	30%	5%	4.6 GB
4	16	16	5%	3.8 GB	35%	5%	4.9 GB
5	20	20	6%	4.0 GB	35%	4%	5.2 GB
6	24	24	6%	4.1 GB	35%	5%	5.5 GB
7	28	28	7%	4.3 GB	43%	6%	5.9 GB
8	32	32	8%	4.4 GB	50%	6%	6.2 GB
9	36	36	10%	4.6 GB	95%	6%	6.6 GB
10	40	40	10%	4.8 GB	95%	6%	7.0 GB
11	44	44	13%	4.9 GB	98%	6%	7.4 GB
12	48	48	13%	5.1 GB	98%	6%	7.8 GB
13	52	52	17%	5.2 GB	98%	6%	8.1 GB
14	56	56	17%	5.7 GB	99%	7%	8.5 GB
15	60	60	20%	6.5 GB	99%	7%	8.9 GB
16	55	55	21%	5.5 GB	98%	7%	9.2 GB

2.3.2.2 *Intel GPU: Intel UHD Graphics 750*

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	Intel GPU	Intel GPU memory
1	4	4	23%	3.5 GB	2%	2%	50%	0.7 GB
2	8	8	50%	4.2 GB	3%	3%	99%	0.9 GB
3	7	7	50%	4.6 GB	3%	3%	100%	0.9 GB

2.3.3 Performance test results for persons

2.3.3.1 *CPU: 12th Gen Intel(R) Core(TM) i9-12900KF 3.20 GHz*

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	GPU memory
1	4	4	60%	4.9 GB	3%	3%	3.5 GB
2	6	6	86 %	5.4 GB	3%	3%	3.8 GB

2.3.3.2 *NVIDIA GPU: NVIDIA GeForce RTX 3080 Ti*

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	GPU memory
1	4	4	4%	3.3 GB	31%	2%	4.6 GB
2	8	8	6%	3.6 GB	35%	2%	5.0 GB
3	12	12	9%	3.7 GB	90%	2%	5.3 GB
4	16	16	12%	3.9 GB	95%	2%	5.6 GB
5	20	20	14%	4.3 GB	98%	2%	6.1 GB
6	20	20	17%	5.0 GB	99%	2%	6.4 GB

2.3.3.3 *Intel GPU: Intel UHD Graphics 750*

Streams	Input FPS	Output FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	Intel GPU	Intel GPU memory
1	4	4	23%	0.6 GB	4%	4%	60%	0.7 GB
2	2	0	75%	3.1 GB	6%	6%	100%	1.0 GB

These tests are indicative and may not be directly applicable to production systems.

3 MIRASYS LIST MANAGEMENT (LM)

3.1 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 up to 5000 identities
- 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.

3.2 LM SERVICE INSTALLATION

3.2.1 Requirements

- Administrator rights
- List Management Service feature is included in V9.6.0 and forward

3.2.2 Updating the List Management Service

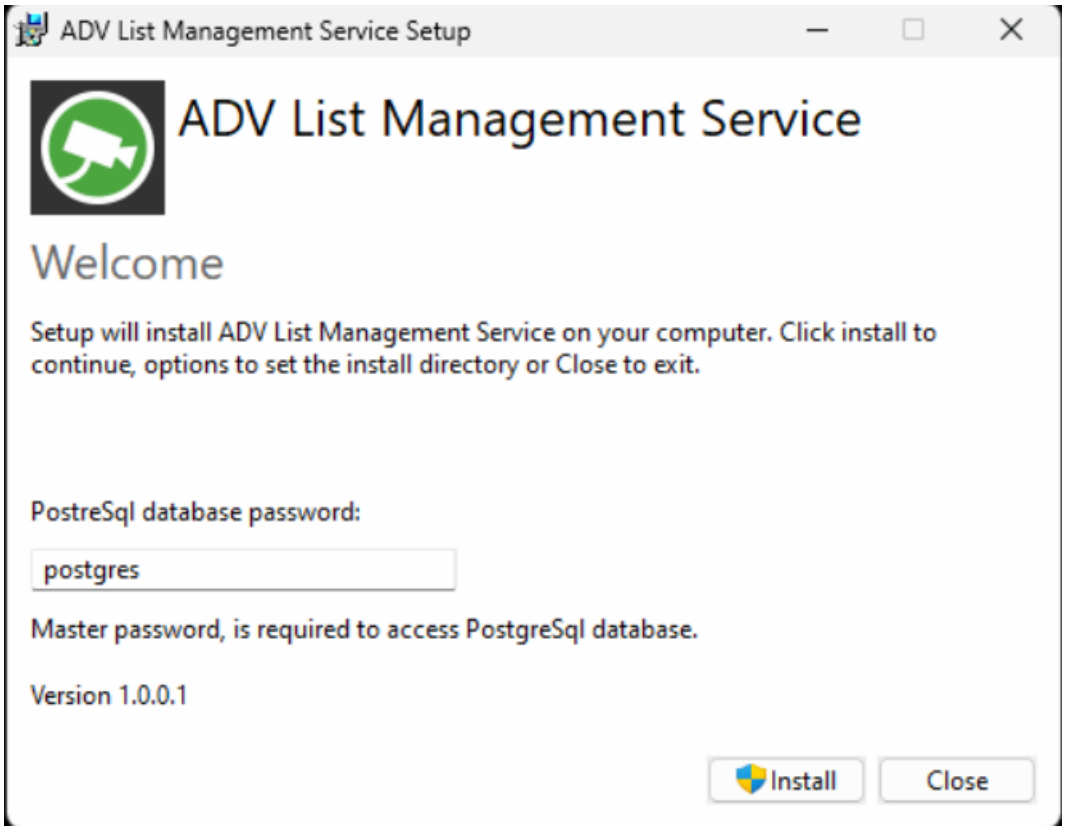
Before updating the List Management Service to a newer version, create a full backup in System Manager and uninstall RabbitMQ Server and Erlang OTP – these can be uninstalled in the Windows settings or the Control Panel. After uninstalling the old LM version and the extra components, you can proceed with the installation with the instructions below. Note that the uninstallation needs to be done only once; there is no need to uninstall RabbitMQ Server and Erlang OTP if that is already done by the List Management Service or the Object Data Storage Service update phase.

The minimum version required of RabbitMQ is 3.13.0. The LM installation includes Erlang 27.3.4.6 and RabbitMQ 4.2.0

3.2.3 Installation

The installer has a step for accepting the End-User License Agreement (EULA). You must confirm that you accept the terms presented in the agreement to continue with the installation.

1. Download the latest version from Extranet.
2. Unzip this e.g. to the C:\temp folder.
3. Start installation by double-clicking the installation file.
4. Click **Install** to continue.
    a. Change the PostgreSQL database password



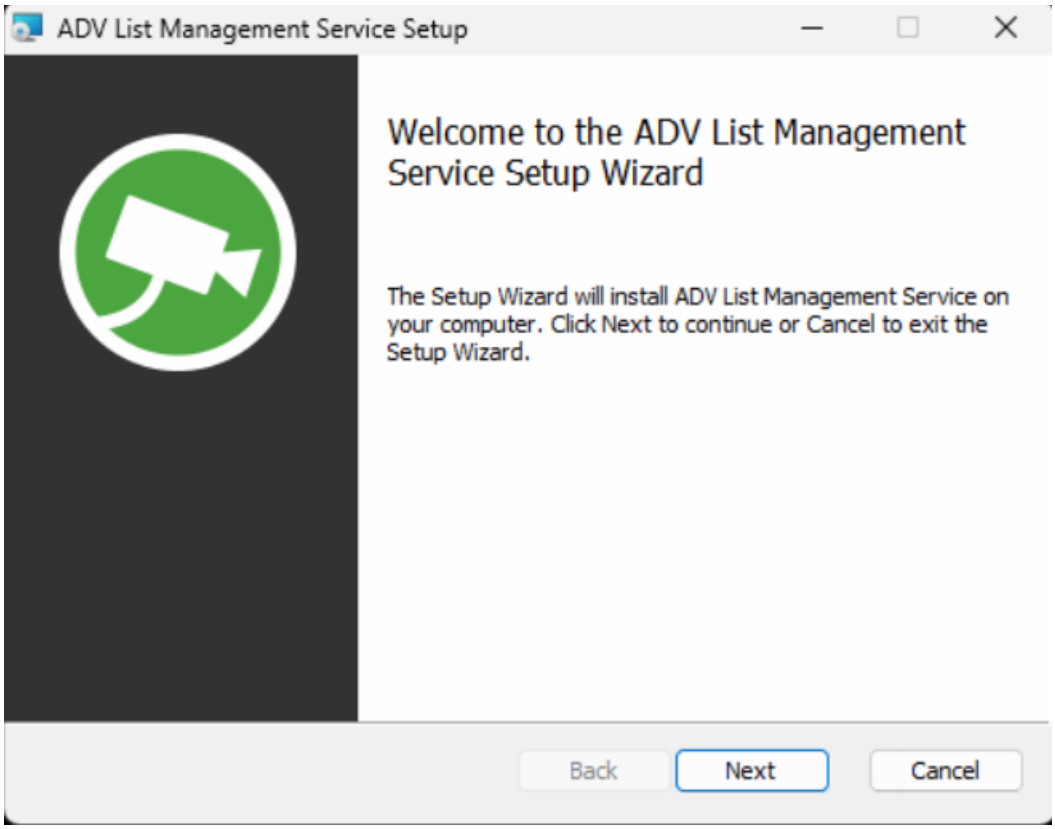
5. Wait that PostgreSQL is installed.

a. You may need to apply firewall rules when the installation is going forward.

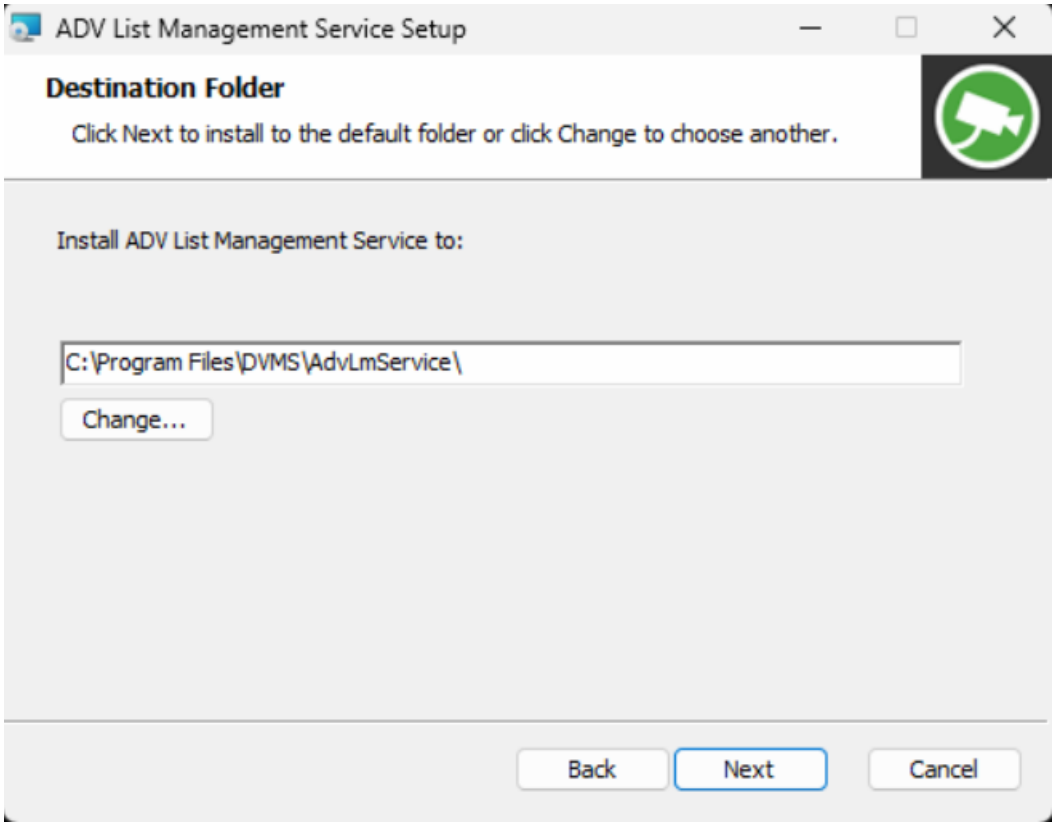
PostgreSQL will be installed with the LM service if it hasn't already been installed earlier.

Currently, there is no support for a separate PostgreSQL server, with the exception of an existing installation of PostgreSQL version 15 or 16.

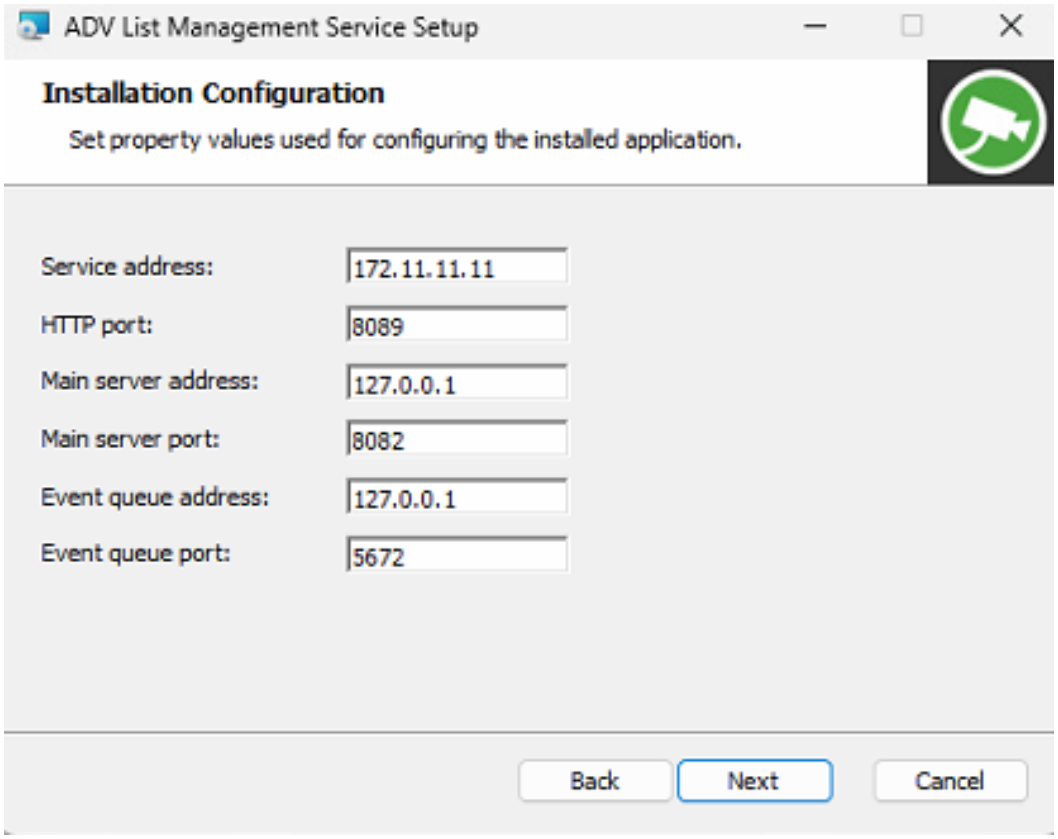
1. Click **Next** to continue.



2. Change installation location if needed; if not, click **Next** to continue.

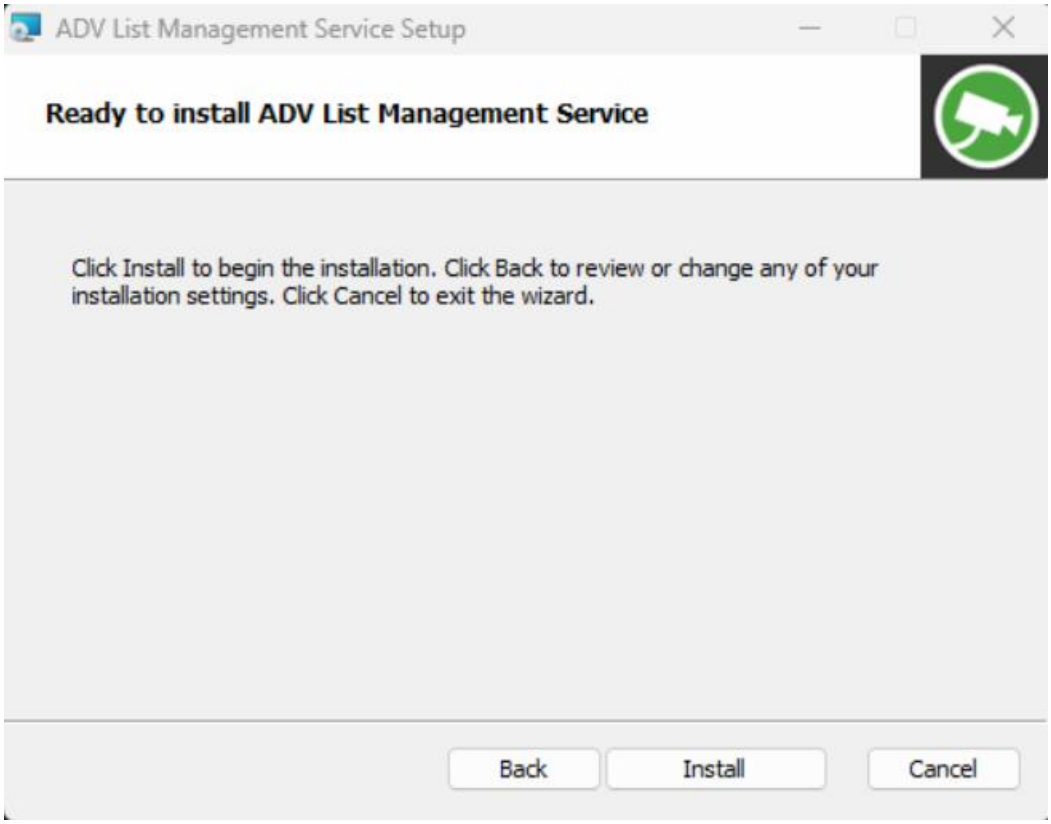


3. Change ports and addresses if needed.
    a. If you are installing List Management Service on another server, you need to change this.
    b. The event queue address is the same address as where the List Management Service is installed. Keep this as the default.
    c. Change the service address to one accessible from client applications. By default, the service address is the machine's first detected IP address.
4. Click **Next** to continue.

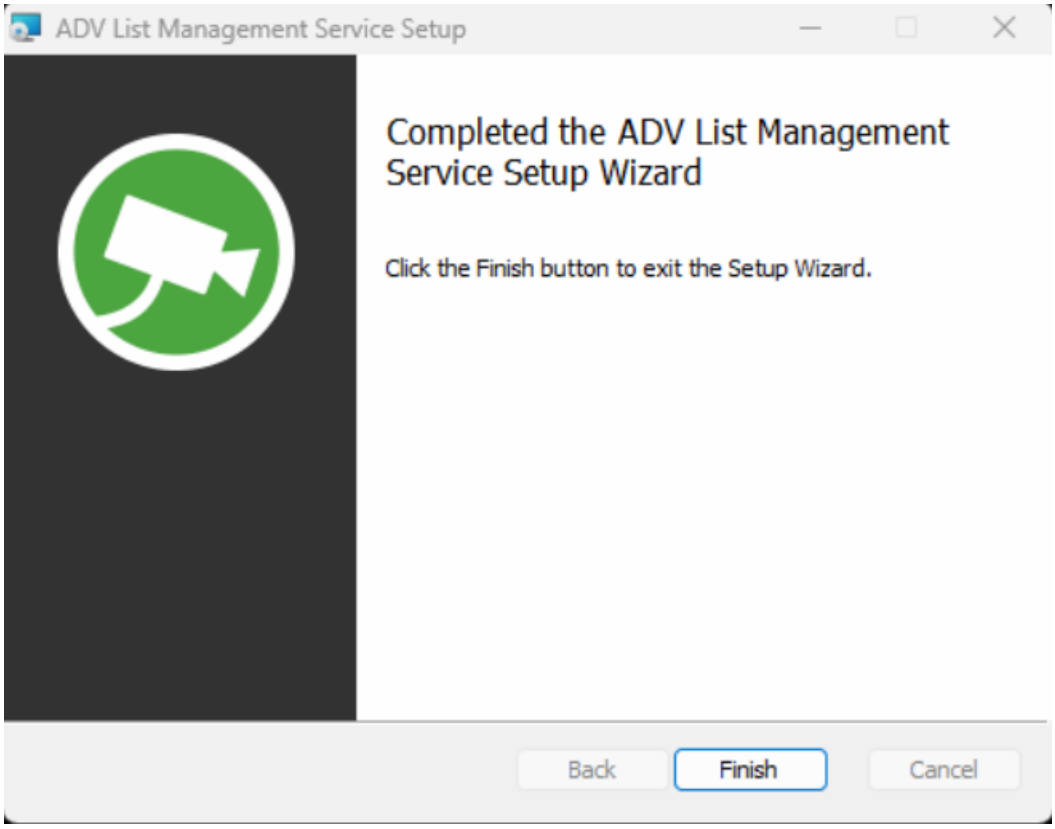


The HTTP port where the LM service is hosted is by default 8089. Change the port in case the default port is reserved for some other use.
The main server uses port 8082 by default. Set the main server address and port to allow the LM service to connect to the correct main server.
Event queue uses port 5672 by default. The event queue is installed with the LM service. Change the event queue port in case the default port is reserved for some other use.

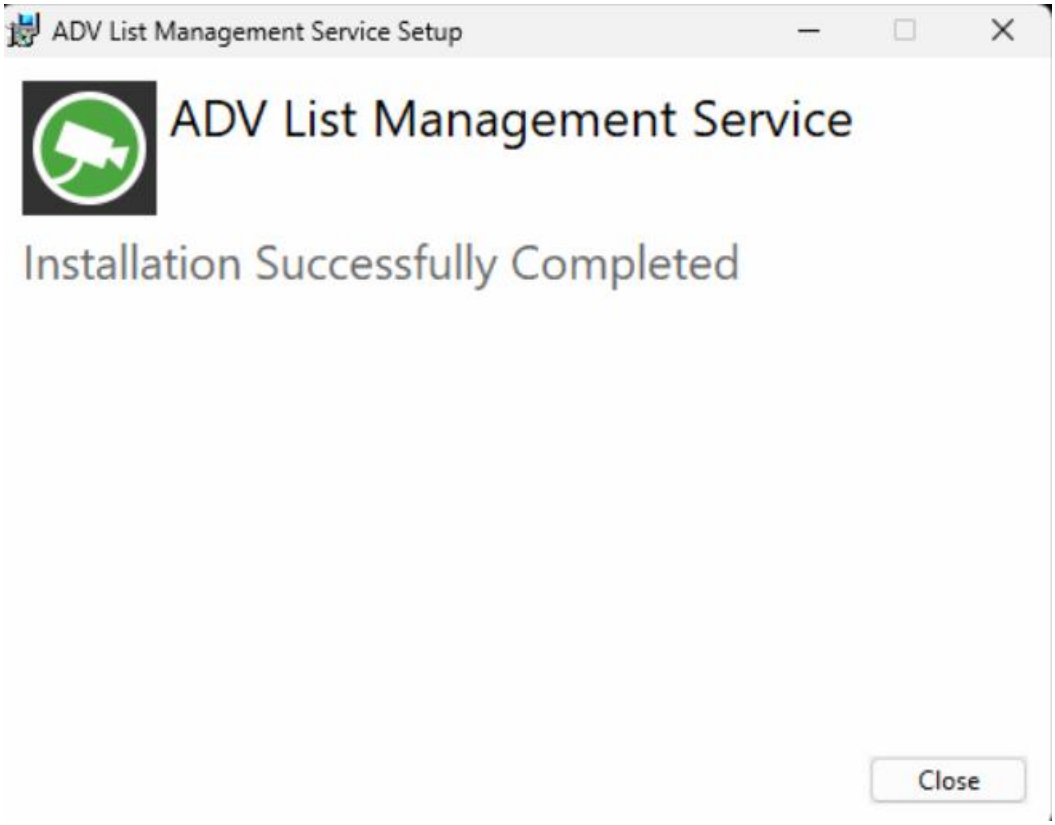
1. Click **Install** to continue.



2. Wait until the installation is finished.
    a. You may need to apply firewall rules when the installation is going forward.
    b. The installer installs RabbitMQ Server, which handles events from the List Management Service, Face Recognition Service, and License Plate Recognition Service.
    c. Default port 5672 TCP.
3. Click **Finish** to end installation.



4. Click **Close** to close the installation window.



5. Now the List Management Service is installed to server and ready to use.
    a. List Management Service sends details to the VMS Main server, and you can configure the service via System Manager.

3.3 PostgreSQL 15 upgrade to PostgreSQL 16 version

If you are using Mirasys List Management Service version 9.6.1 or earlier, it includes PostgreSQL 15. Before upgrading to Mirasys List Management Service 9.6.2 or later while retaining your current database, you must first migrate the database to PostgreSQL 16.

During the PostgreSQL upgrade process, the system will not store any data in the database.

3.3.1 This guide applies to

- Mirasys VMS V9.6.2
- Mirasys VMS V9.6.3
- Mirasys VMS V9.7.0
- Mirasys VMS V9.8.0

- Mirasys VMS V9.9.0
- Mirasys VMS V9.10.0

3.3.2 Requirements

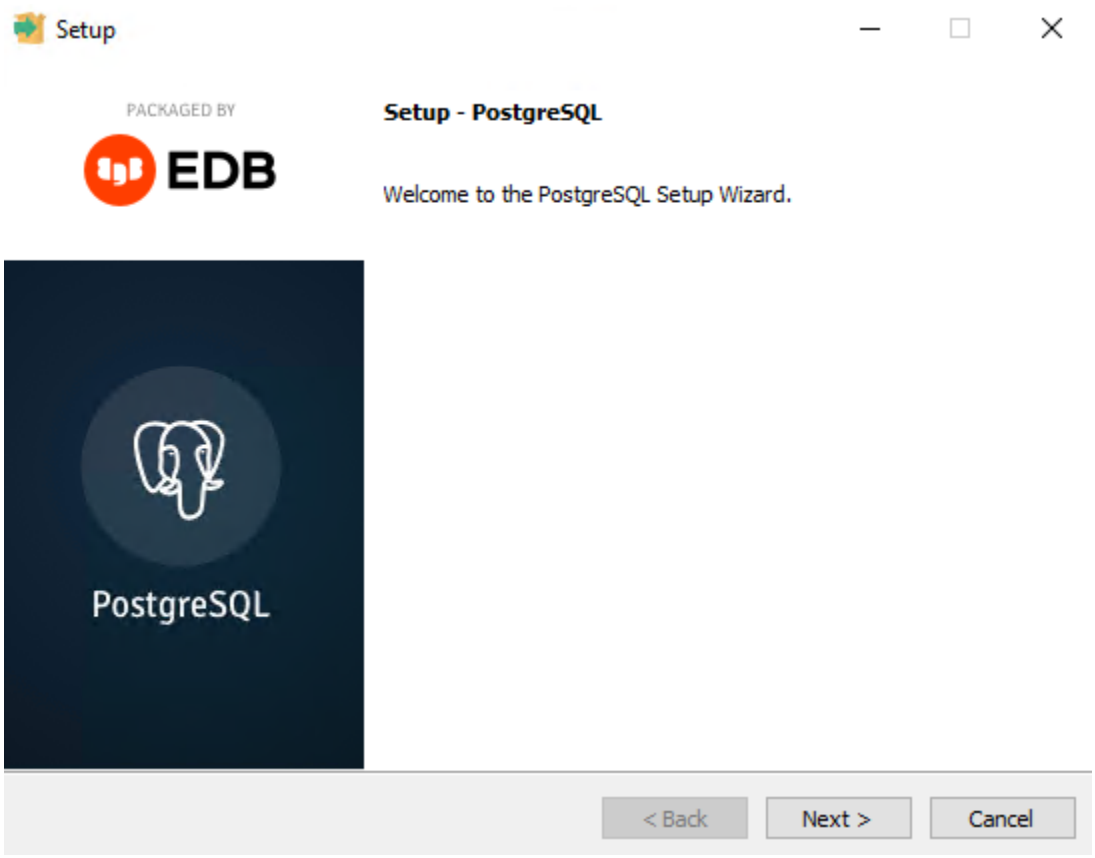
- Backup of database
- Notepad++
- PostgreSQL 16 installation package
    - postgresql-16.1-1-windows-x64.exe
- Mirasys List Management Service 9.6.2 or newer installation package
- The system where Mirasys List Management Service 9.6.1 or an earlier version is installed.

3.3.3 How to do upgrade

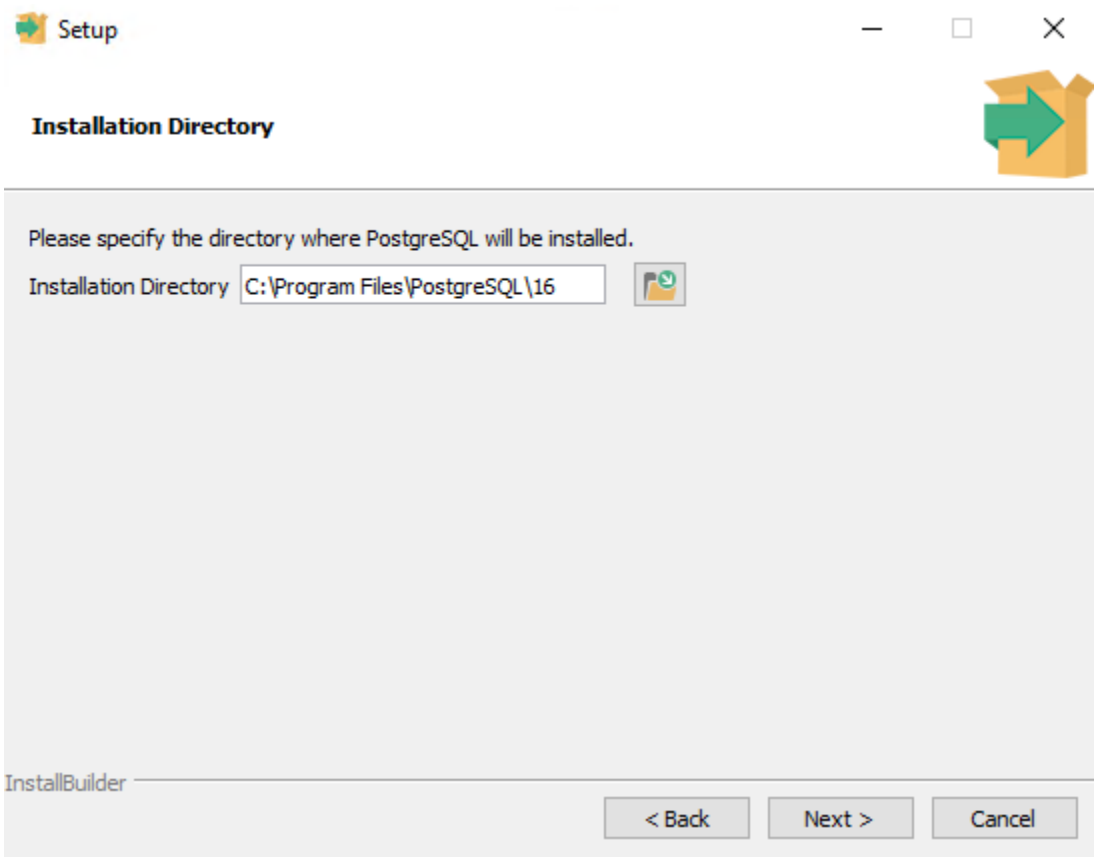
1. Stop the AdvPostgreDatabase and ADVLmService services in Windows Services.
2. Change AdvPostgreDatabase service startup type to manual.
3. Go to location C:\Program Files\PostgreSQL\15\data and open postgresql.conf file using the Notepad++ application.
   a. Find line port = 5432 and change this to port = 5433.

```
port = 5432 -> port = 5433
```

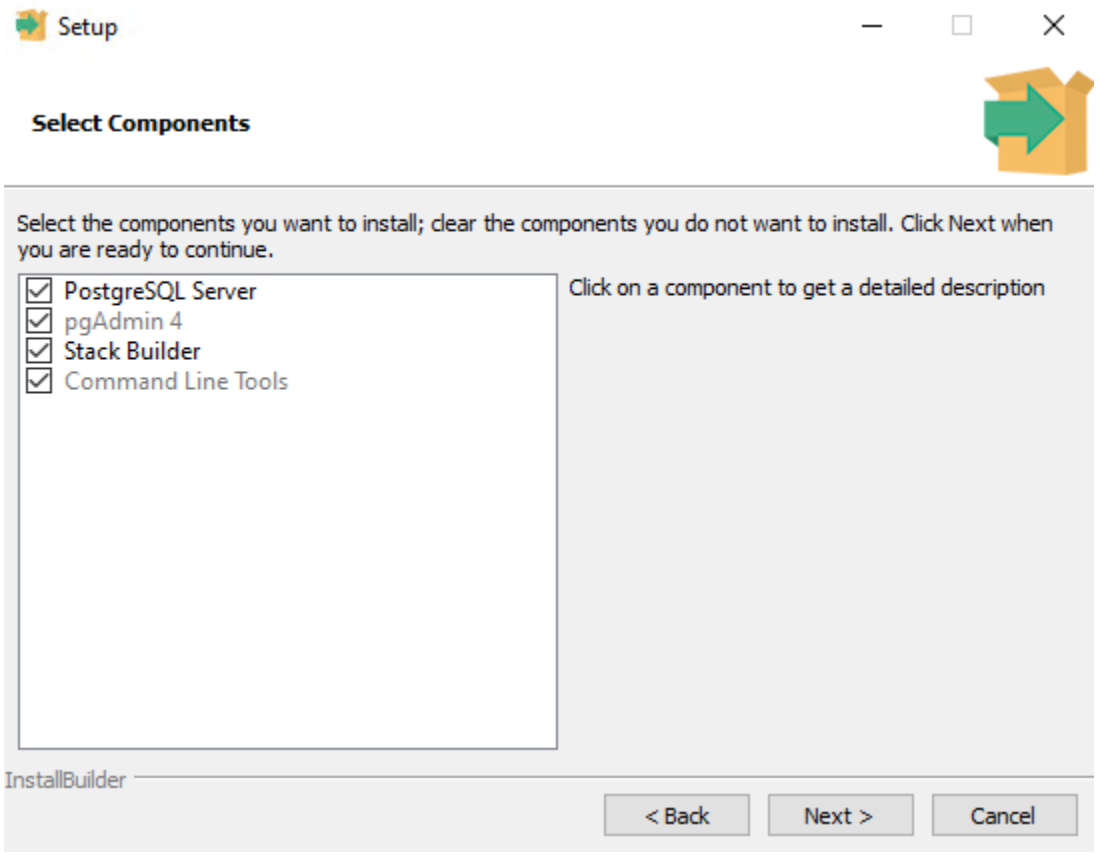
1. Save the postgresql.conf configuration file.
2. Start the installation of PostgreSQL 16 by double-clicking the PostgreSQL 16 installation package
3. Click **Next** to continue.



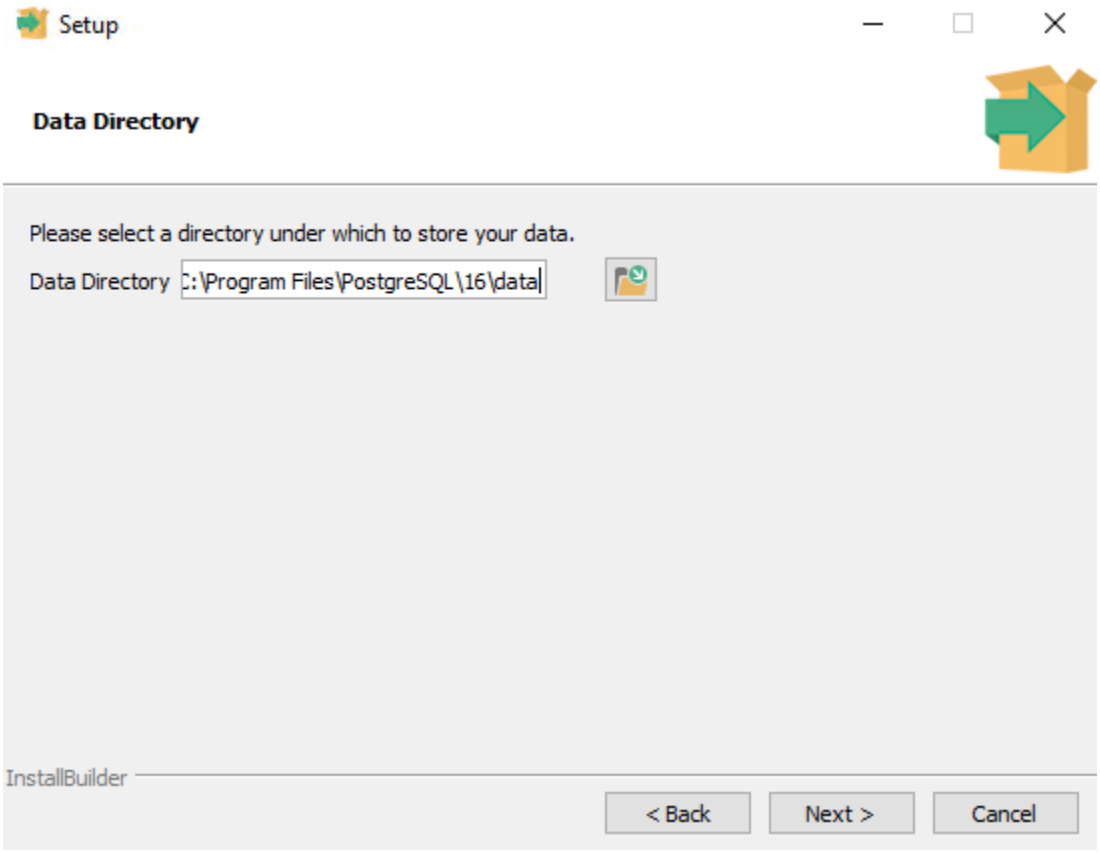
4. Use the default installation location and click **Next**.



5. Install with all components.

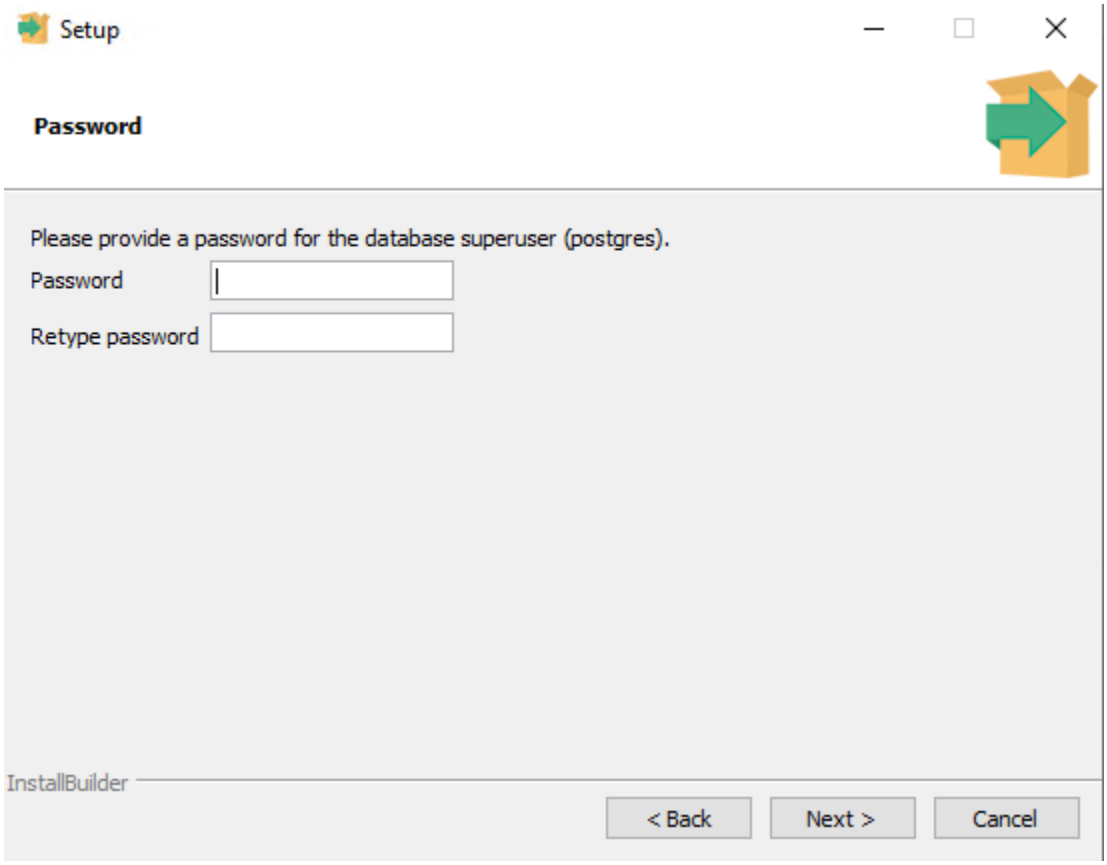


6. Use the default Data Directory location and click **Next**.

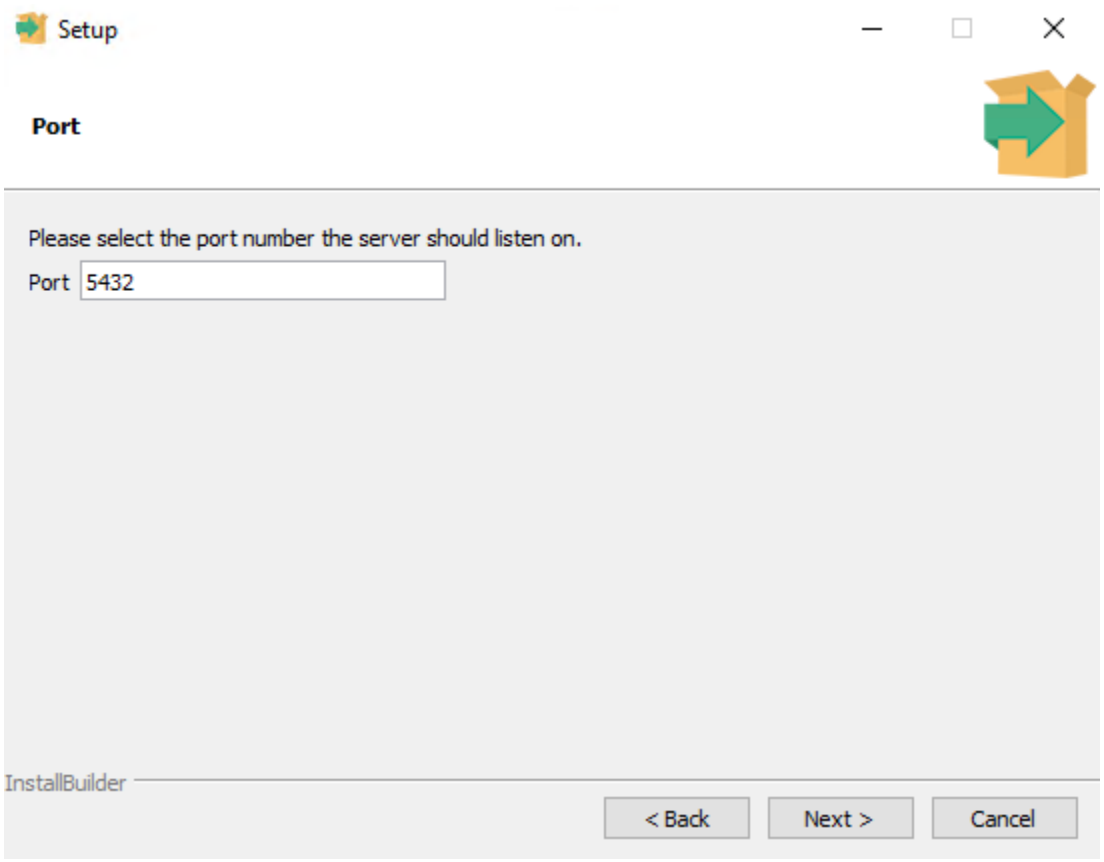


7. Enter the same password you used during the installation of Mirasys List Management Service.

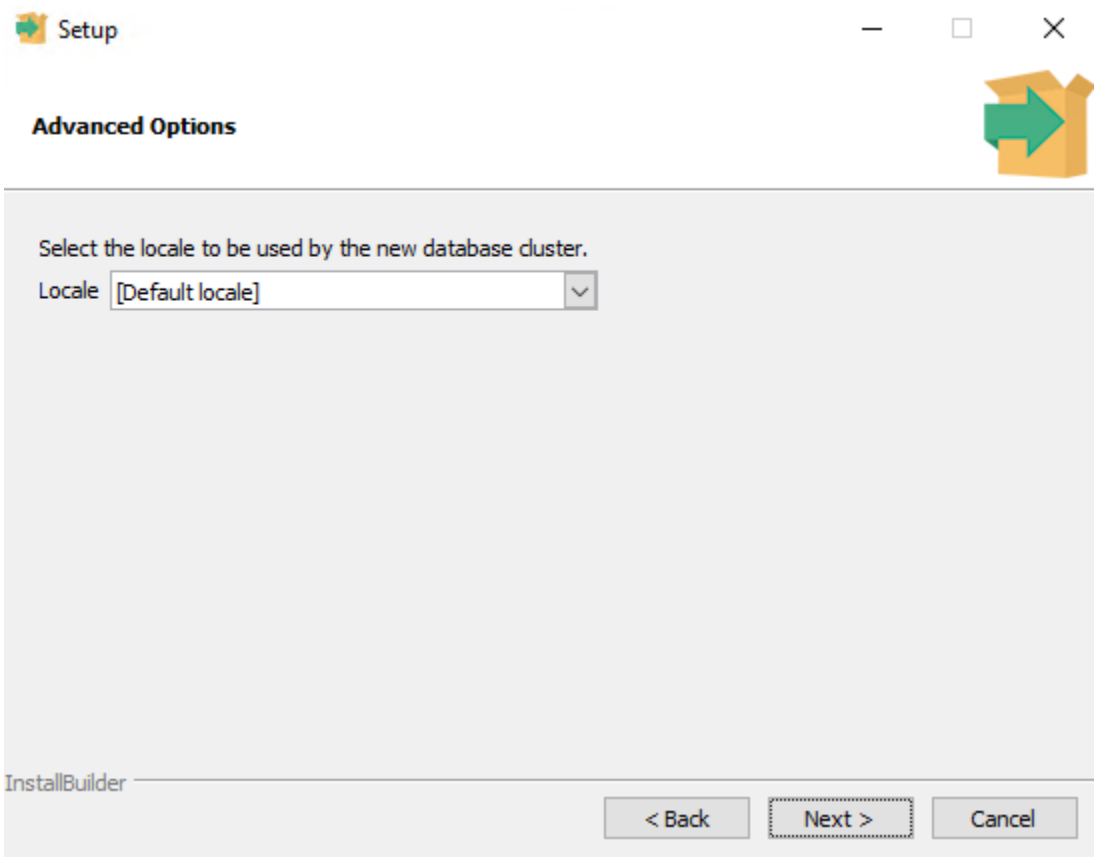
- Default is postgres



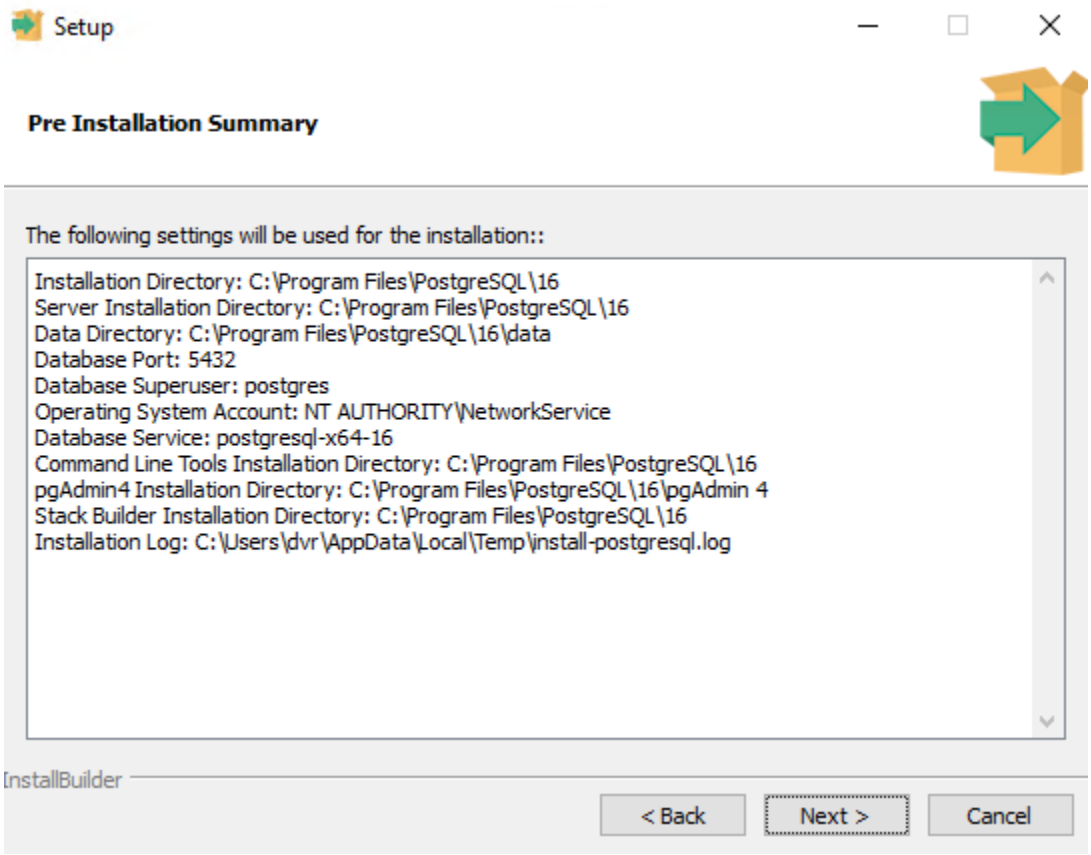
1. Use the default port 5432 and click **Next**.



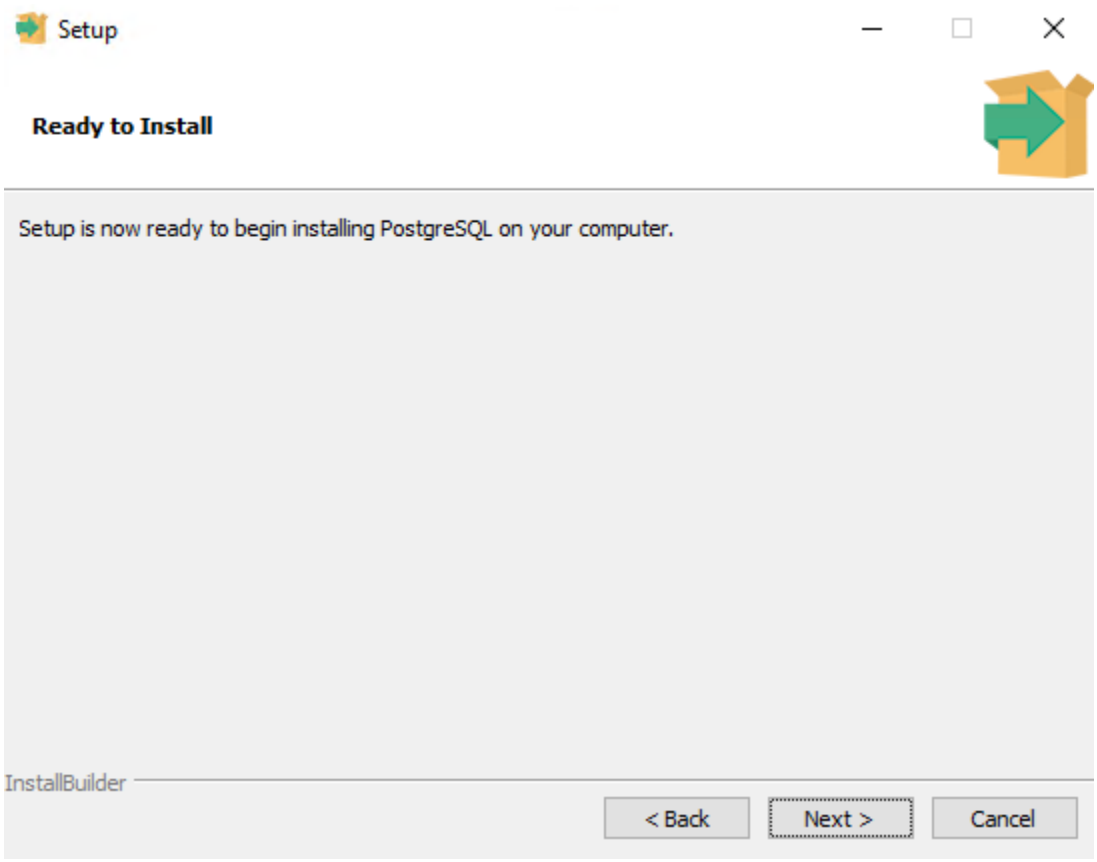
2. Use the default Advanced Options and click **Next**.



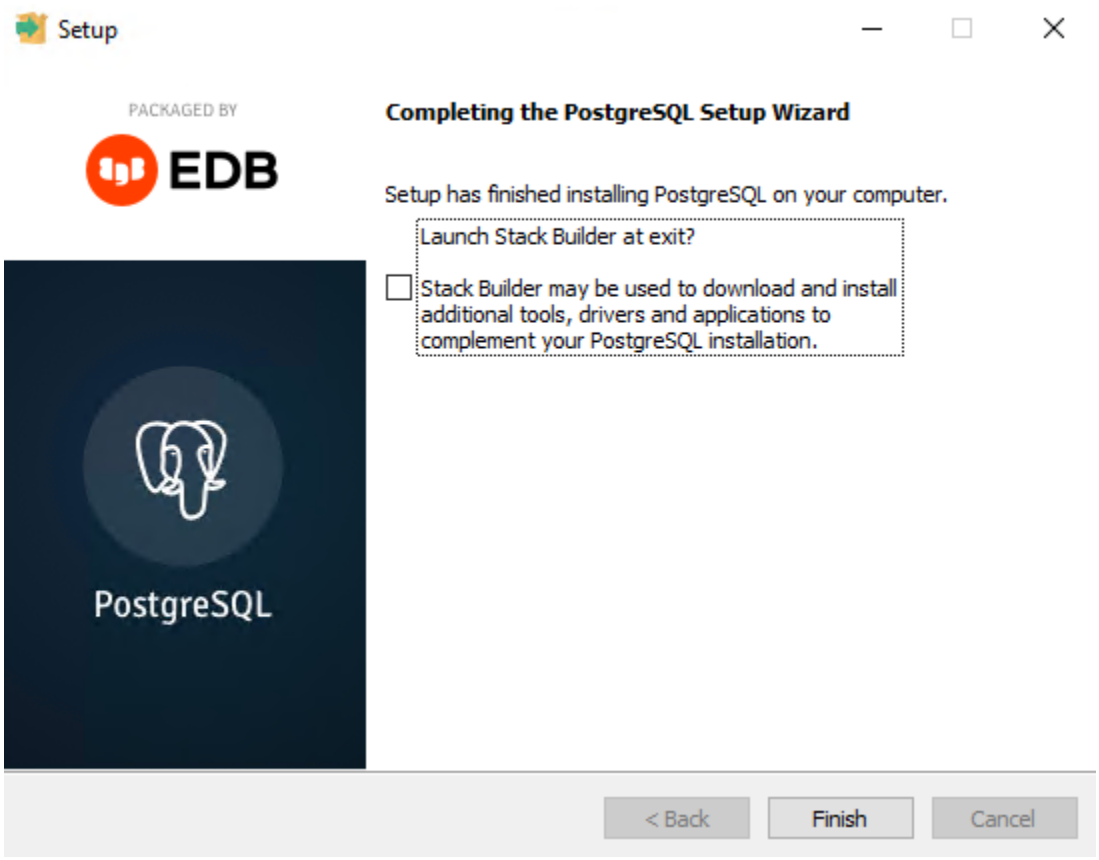
3. You can now review the installation settings. If any changes are needed, go back and modify the desired section. Otherwise, click **Next**.



4. Click **Next** and the installation starts. This takes some time, so wait until the installation is finished.



5. Untick the Launch Stack Builder option and click **Finish**.



6. Stop the postgresql-x64-16 service using Windows Services.
7. Change postgresql-x64-16 startup type to Manual.
8. Go to location C:\Program Files\PostgreSQL\16\data and open postgresql.conf file in Notepad++ and check that the port is the default 5432.
   a. If not, change the port to 5432 and save the configuration file.
9. Allow local access to edit old and new PostgreSQL pg_hba.conf files.

   a. Locations are C:\Program Files\PostgreSQL\15\data and C:\Program Files\PostgreSQL\16\data

   b. Open pg_hba.conf file from both locations and change local connections to trusted.

```
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
To this
```

```
# IPv4 local connections:
host    all             all             127.0.0.1/32            trust
# IPv6 local connections:
host    all             all             ::1/128                 trust
```

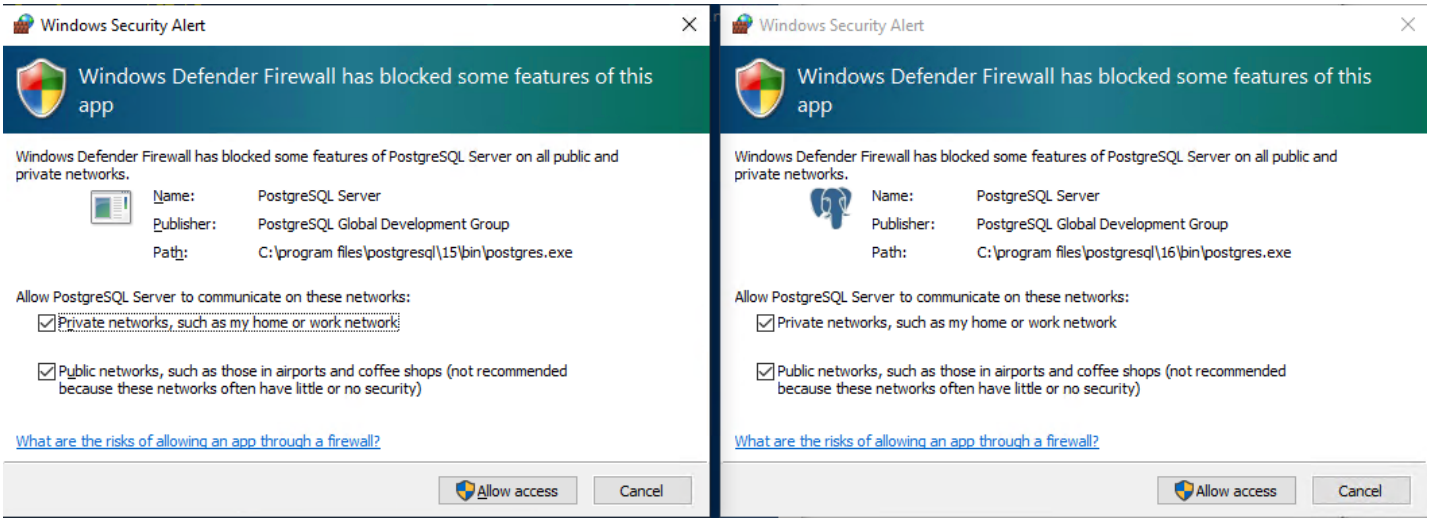
1. Save both configuration files.
2. Open the PowerShell window and copy this script there.

   a. Verify the file paths are correct; if not, modify necessary paths to correct ones

```
C:\Program Files\PostgreSQL\16\bin\pg_upgrade.exe --old-datadir 'C:\Program
Files\PostgreSQL\15\data' --new-datadir 'C:\Program Files\PostgreSQL\16\data' --old-bindir
'C:\Program Files\PostgreSQL\15\bin' --new-bindir 'C:\Program Files\PostgreSQL\16\bin' -U
postgres
```

1. Then press **Enter** and wait until the upgrade is done.

   a. Allow network rules for Firewall if those are requested.



1. Verify that you see a similar result once the upgrade is complete.

```
Performing Consistency Checks
-----------------------------
Checking cluster versions                                   ok
Checking database user is the install user                  ok
Checking database connection settings                       ok
Checking for prepared transactions                          ok
Checking for system-defined composite types in user tables  ok
Checking for reg* data types in user tables                 ok
Checking for contrib/isn with bigint-passing mismatch       ok
```

```
Checking for incompatible "aclitem" data type in user tables  ok
Creating dump of global objects                               ok
Creating dump of database schemas
                                                              ok
Checking for presence of required libraries                   ok
Checking database user is the install user                    ok
Checking for prepared transactions                            ok
Checking for new cluster tablespace directories               ok
If pg_upgrade fails after this point, you must re-initdb the
new cluster before continuing.
Performing Upgrade
------------------
Setting locale and encoding for new cluster                   ok
Analyzing all rows in the new cluster                         ok
Freezing all rows in the new cluster                          ok
Deleting files from new pg_xact                               ok
Copying old pg_xact to new server                             ok
Setting oldest XID for new cluster                            ok
Setting next transaction ID and epoch for new cluster         ok
Deleting files from new pg_multixact/offsets                  ok
Copying old pg_multixact/offsets to new server                ok
Deleting files from new pg_multixact/members                  ok
Copying old pg_multixact/members to new server                ok
Setting next multixact ID and offset for new cluster          ok
Resetting WAL archives                                        ok
Setting frozenxid and minmxid counters in new cluster         ok
Restoring global objects in the new cluster                   ok
Restoring database schemas in the new cluster
                                                              ok
Copying user relation files
                                                              ok
Setting next OID for new cluster                              ok
Sync data directory to disk                                   ok
Creating script to delete old cluster                         ok
Checking for extension updates                                ok
Upgrade Complete
----------------
Optimizer statistics are not transferred by pg_upgrade.
Once you start the new server, consider running:
    C:/Program Files/PostgreSQL/16/bin/vacuumdb -U postgres --all --analyze-in-stages
Running this script will delete the old cluster's data files:
    delete_old_cluster.bat
```

1. Check for any errors, as they indicate an issue preventing the upgrade. Identify the possible cause and attempt the upgrade again.
2. Close the PowerShell window.
3. Change pg_hba.conf back to normal.

   a. Locations are C:\Program Files\PostgreSQL\15\data and C:\Program Files\PostgreSQL\16\data

```
# IPv4 local connections:
host    all             all             127.0.0.1/32            trust
# IPv6 local connections:
host    all             all             ::1/128                 trust
To this
# IPv4 local connections:
host    all             all             127.0.0.1/32            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128                 scram-sha-256
```

1. Uninstall the following applications using Windows Programs And Features

   a. ADV List Management Service

   b. PostgreSQL 15 and select Entire application

      No need to care about warning messages related to data folder removal, click **OK**.

   c. PostgreSQL 16 and select Entire application

      No need to care about warning messages related to data folder removal, click **OK**.

1. Now you can install the newer Mirasys List Management Service and follow our guide on how to install it.
2. Verify that the upgrade was successful. The older PostgreSQL version should now be updated to the newer version, and you should be able to see both old and new data via System Manager and Spotter.
3. If desired, you can clean up the old PostgreSQL version by navigating to C:\Program Files\PostgreSQL and deleting the "15" folder.

4 MIRASYS FACE RECOGNITION (FR)

4.1 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. Face Recognition and List Management include face tracking and a face similarity value to match a face to an identity. This is done to prevent excessive face detection events of the same person. The maximum number of faces that can be detected from one image in FR is 20.

Note that anti-spoofing is not included in the current version.

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 168x256 image size. If the face is larger in the picture, it is first reduced to 168x256 before identification is made. Likewise, if the face is smaller in the picture, it is first enlarged to the 168x256 size. The recommended size of the face in the image is at least 112 pixels.

On licensing side there is need to add RTSP Streaming Server feature to Management Server and all those servers where is plan to use SmartFR feature. On Management Server side there is need to be add wanted amount of channels of SmartFR feature.

4.2 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.

NVIDIA libraries (CUDA cuDNN, TensorRT) are not included in the FR installer. The installer will detect the presence of the NVIDIA library installers from the 'NVIDIA' subfolder and install the libraries automatically if they are found.

For Face Recognition (FR), you need to install the FRService and LMService packages. FR carries out the face recognition, and LM stores the face recognition events in PostgreSQL.

4.2.1 Requirements

- Administrator rights
- List Management Service installed
- Face Recognition license on the VMS Management Server
- RTSP license feature on the VMS Management Server and the VMS Server
- Required NVIDIA libraries (CUDA, cuDNN, TensorRT) are installed

4.2.2 NVIDIA libraries

Required NVIDIA libraries should be installed before installing the FR service if they have not yet been installed. Installation of the FR service requires the installation of the following NVIDIA libraries for Windows:

- CUDA Toolkit 12.9 Update 1: https://developer.nvidia.com/cuda-12-9-1-download-archive
- cuDNN 9.20.0: https://developer.nvidia.com/cudnn-9-20-0-download-archive

- TensorRT v10.16.0.72 GA for Windows 10, 11, Server 2022 and CUDA 12.0 to 12.9 ZIP Package: https://developer.nvidia.com/tensorrt/download/10x

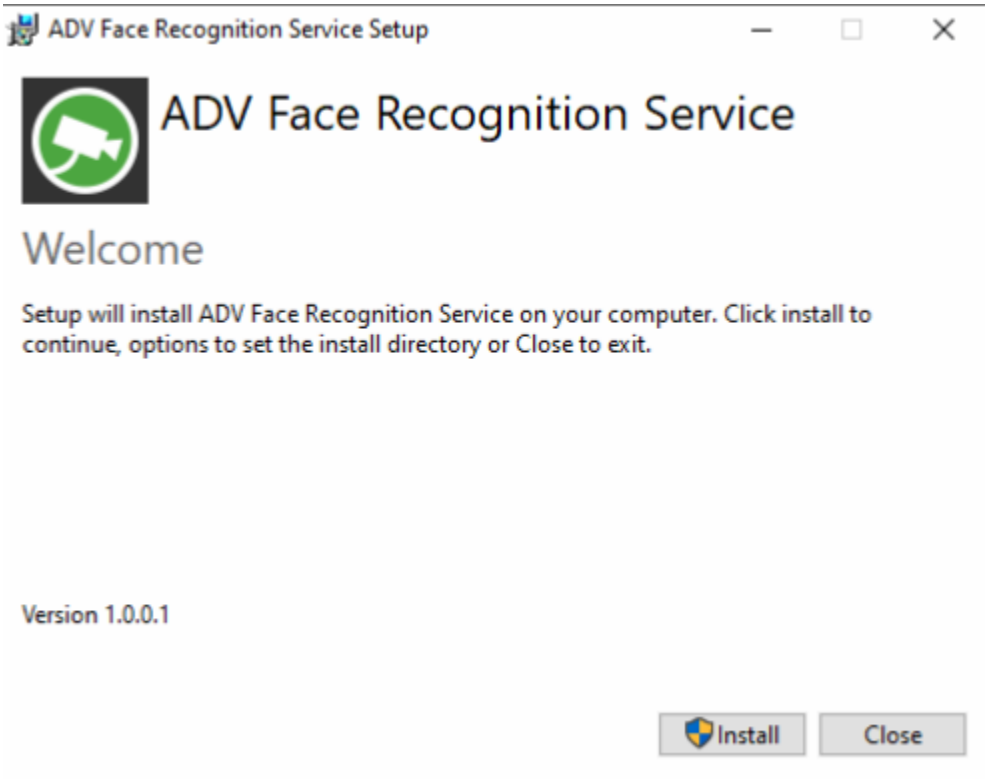
4.2.2.1 Installing NVIDIA libraries

1. Download the Mirasys FR service installer and place it in a folder on your machine
2. Create a subfolder 'NVIDIA'
3. Download the NVIDIA libraries mentioned above
4. Save the downloaded NVIDIA libraries to the 'NVIDIA' subfolder
5. Run the Mirasys FR service installer
    a. Mirasys FR service installer automatically installs the NVIDIA libraries that it detects from the 'NVIDIA' subfolder before the service is installed
6. Follow the installation instructions to finalize the installation

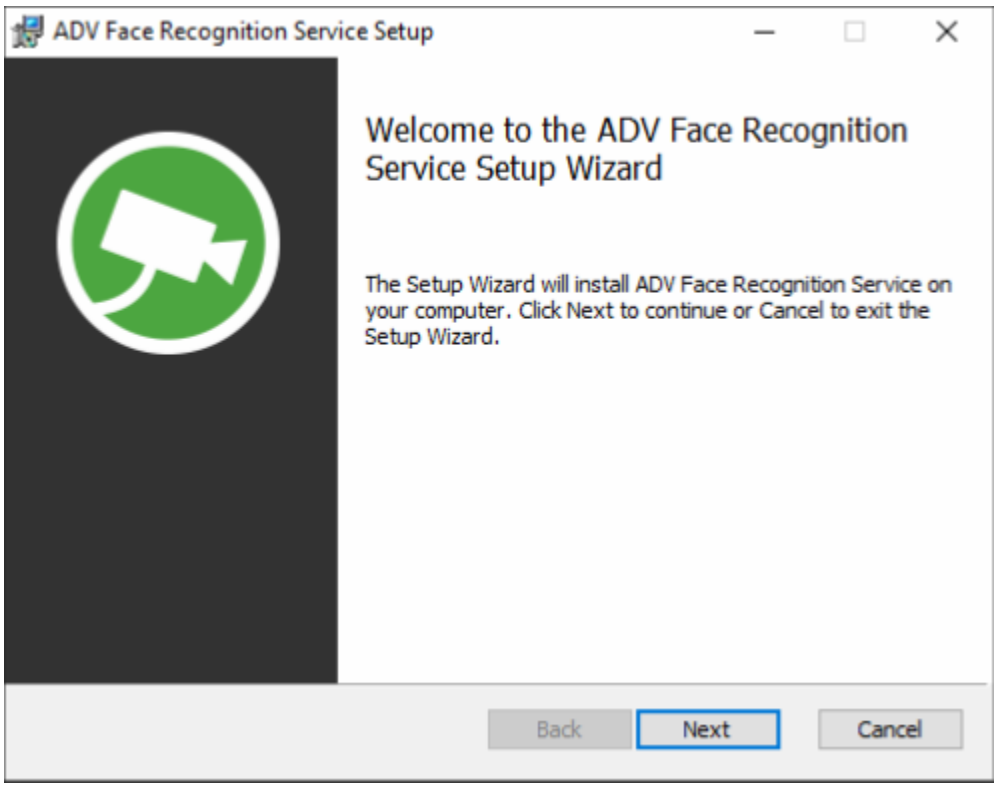
4.2.3 FR Installation

The installer has a step for accepting the End-User License Agreement (EULA). You must confirm that you accept the terms presented in the agreement to continue with the installation.

1. Download the latest version from Extranet.
2. Unzip the files e.g. to the C:\temp folder.
3. Start the installation by double-clicking the installation file.
4. Click **Install** to continue.



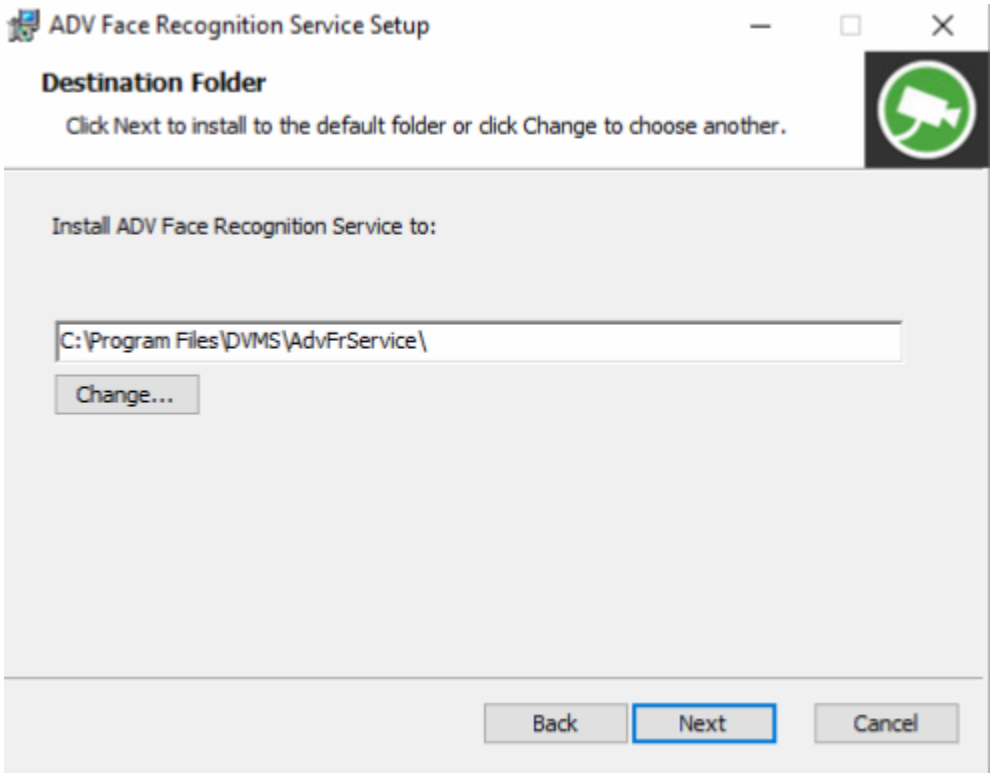
5. Click **Next** to continue.



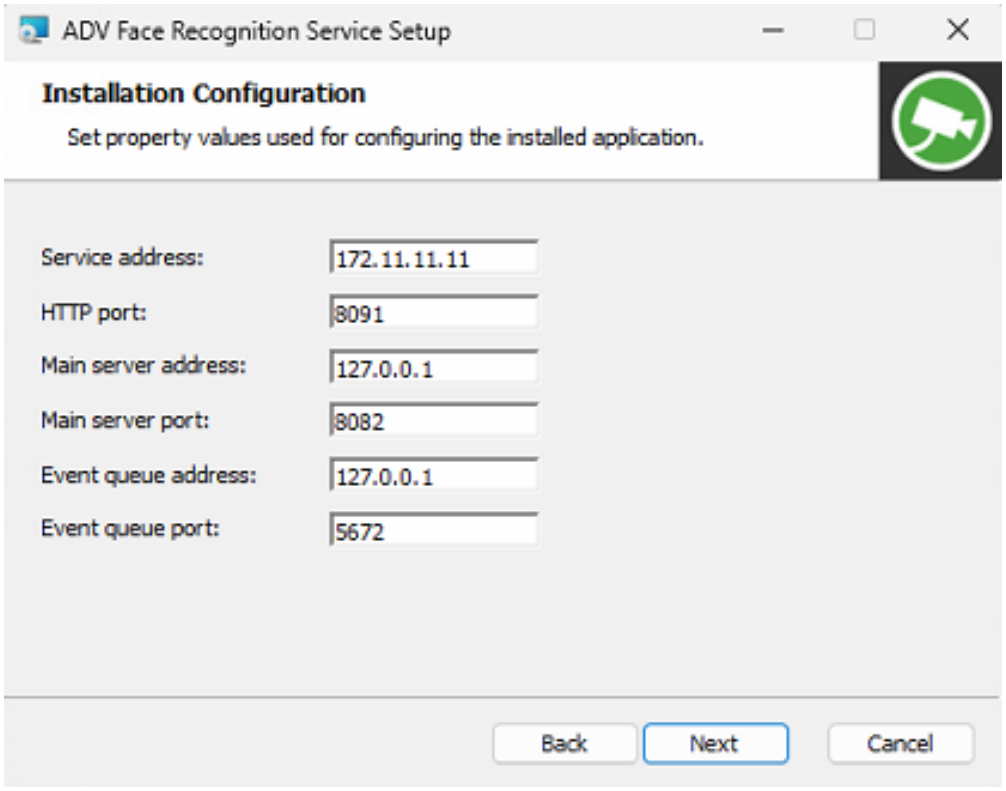
6. Check **I accept the terms in the License Agreement** and click **Next**.



1. Change the installation location if needed and click **Next** to continue.

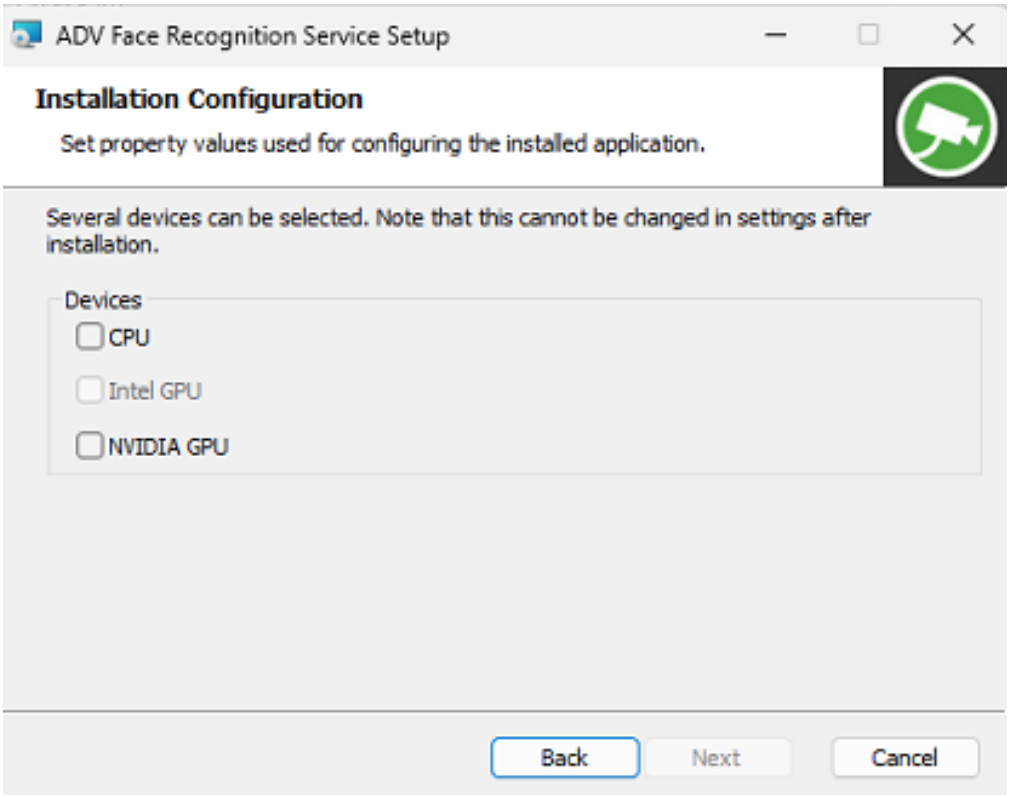


2. Change ports and addresses if needed.
    a. If you e.g. install the Face Recognition service on a machine other than the VMS main server, you need to change the main server address to the correct one.
    b. The same applies to the Event queue address. Replace this address with the server address where List Management Service is installed.
    c. Change the service address to one accessible from client applications. By default, the service address is the machine's first detected IP address.
3. Click **Next** to continue.

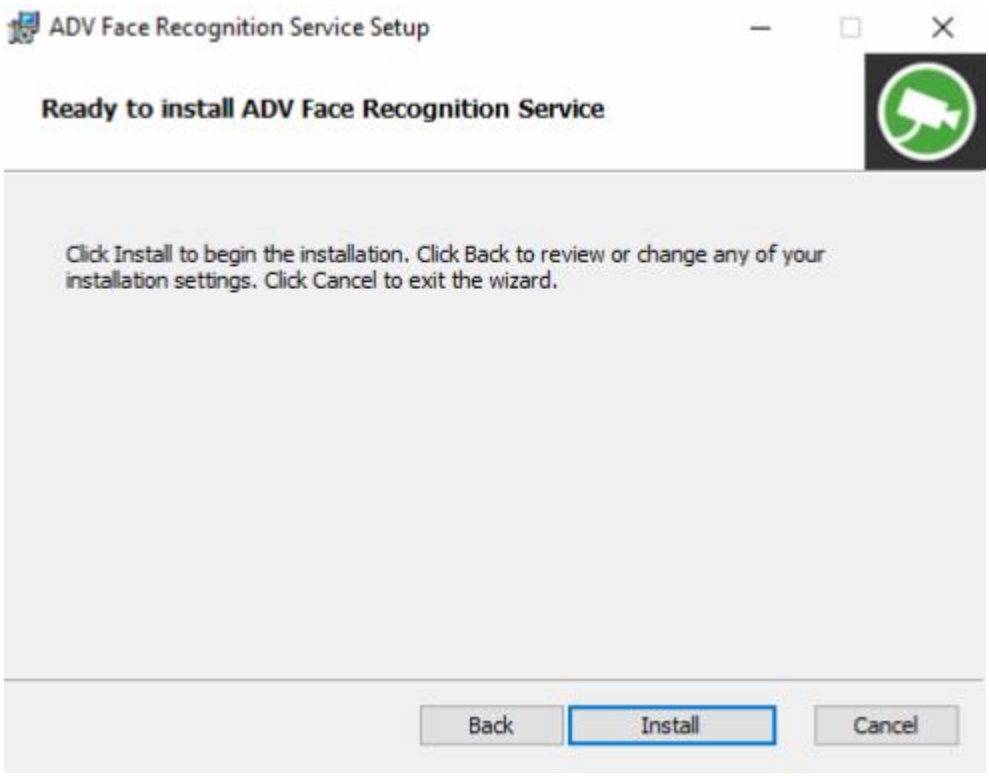


The HTTP port where the FR service is hosted is by default 8091. Change the port in case the default port is reserved for some other use.
The main server uses port 8082 by default. Set the main server address and port to allow the FR service to connect to the correct main server.
Event queue uses port 5672 by default. The event queue is installed with the LM service installation, where the used event queue port is set. Set the event queue address to the machine where the LM service is installed.

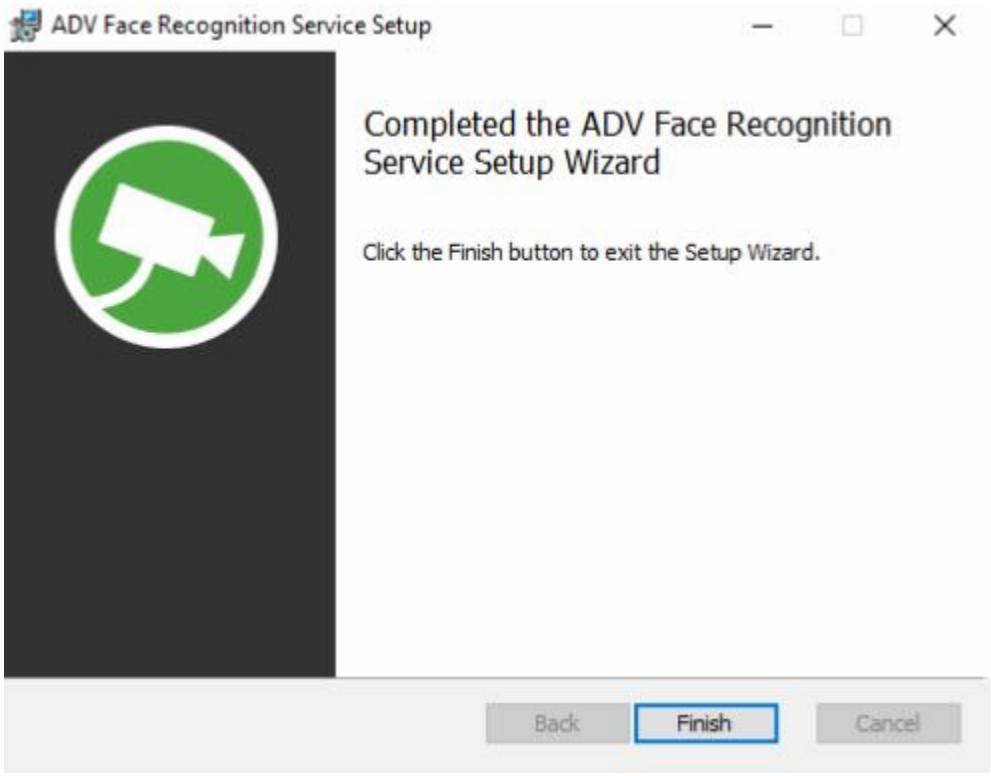
1. Select devices and click **Next**



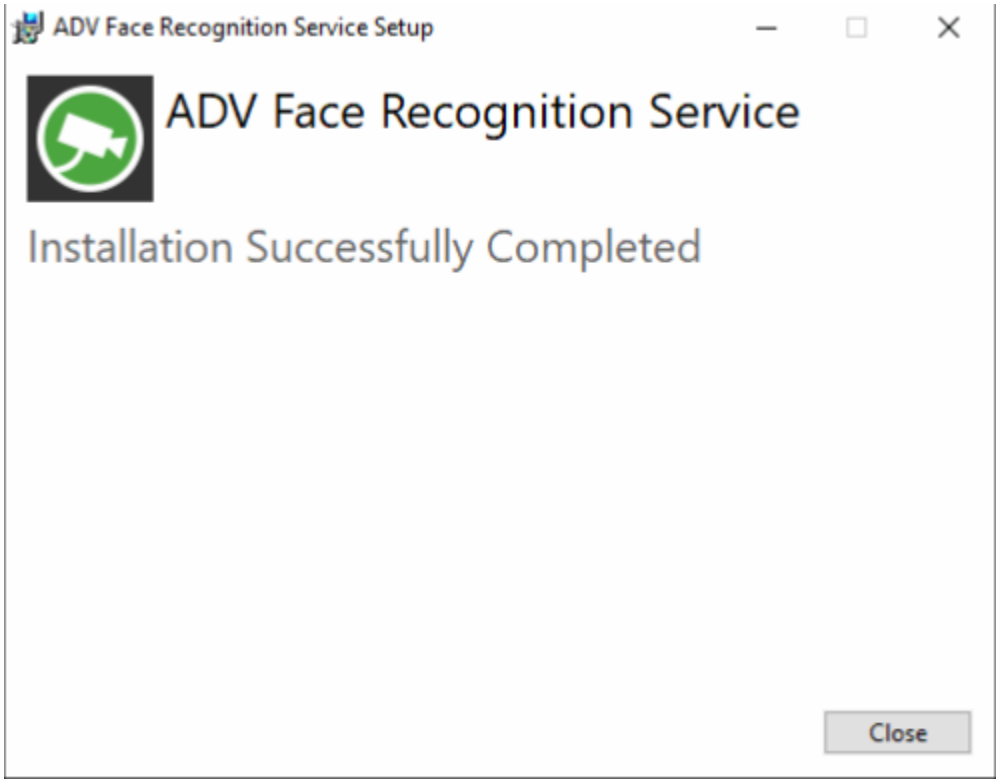
1. Click **Install** to continue and wait.
2. Installation will take some time until it is finished.
3. Model creation can take up to 30 minutes. This depends on how powerful the graphics card in use is.



4. Click **Finish** to continue.



5. Click **Close** to close the installation.



6. Now the Face Recognition Service is installed on the server and is ready to use.
    a. Face Recognition Service sends details to the VMS Main server. You can configure the service via System Manager.

4.3 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.

4.4 FR PROCESSING, EVENTS, AND DETECTION

4.4.1 Devices

Face recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

4.4.2 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.

4.4.3 Detected face visualization

Detected faces can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

4.5 FR Alarm triggers and configuration

4.5.1 Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

4.5.2 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.

4.6 FR Performance

4.6.1 Test computer hardware

- Intel(R) Core(TM) Ultra 7 265K (3.90 GHz)
- NVIDIA RTX 4000 Ada Generation
- Intel Graphics

For performance reasons, face detection for CPU and Intel GPU has been optimized for speed and has slightly worse accuracy than the detection for NVIDIA GPU. To gain the best accuracy, the NVIDIA GPU should be used.

4.6.2 9.10 version

4.6.2.1 CPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA decode
1	1920 x 1080	8	9%	1.8 GB	2%

Streams	Size	FPS	Process CPU	Process memory	NVIDIA decode
2	1920 x 1080	18	22%	2.5 GB	4%
3	1920 x 1080	25	29%	3.4 GB	7%
4	1920 x 1080	24	31%	4.0 GB	7%

4.6.2.2 INTEL GPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA decode	INTEL GPU	INTEL memory
1	1920 x 1080	21	1%	1.8 GB	5%	23%	0.5 GB
2	1920 x 1080	41	3%	2.2 GB	9%	52%	0.6 GB
3	1920 x 1080	61	4%	2.9 GB	12%	64%	1.0 GB
4	1920 x 1080	82	5%	3.4 GB	17%	74%	1.1 GB
5	1920 x 1080	103	8%	4.0 GB	19%	93%	1.3 GB
6	1920 x 1080	122	14%	4.3 GB	23%	99%	1.4 GB
7	1920 x 1080	121	16%	4.7 GB	24%	100%	1.7 GB

4.6.2.3 NVIDIA GPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	NVIDIA memory
1	1920 x 1080	20	3%	1.9 GB	35%	4%	2.6 GB
2	1920 x 1080	40	4%	2.3 GB	95%	6%	2.9 GB
3	1920 x 1080	60	5%	2.5 GB	95%	6%	3.2 GB
4	1920 x 1080	80	6%	2.6 GB	96%	7%	3.6 GB
5	1920 x 1080	100	8%	2.7 GB	97%	9%	3.9 GB
6	1920 x 1080	120	9%	2.8 GB	97%	10%	4.3 GB
7	1920 x 1080	140	11%	3.0 GB	97%	11%	4.6 GB
8	1920 x 1080	160	13%	3.2 GB	98%	10%	5.0 GB
9	1920 x 1080	180	15%	3.5 GB	97%	11%	5.3 GB

Streams	Size	FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	NVIDIA memory
10	1920 x 1080	180	17%	4.0 GB	97%	11%	5.6 GB

4.6.3 9.9.6 version

4.6.3.1 CPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA decode
1	1920 x 1080	4	4%	2.6 GB	2%
2	1920 x 1080	5	4%	3.3 GB	2%
3	1920 x 1080	6	4%	3.6 GB	3%
4	1920 x 1080	6	5%	4.3 GB	3%

4.6.3.2 INTEL GPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA decode	INTEL GPU	INTEL memory
1	1920 x 1080	20	2%	2.5 GB	5%	45%	0.4 GB
2	1920 x 1080	41	4%	3.3 GB	8%	60%	0.7 GB
3	1920 x 1080	61	5%	3.8 GB	14%	70%	0.8 GB
4	1920 x 1080	82	7%	4.6 GB	16%	80%	1.0 GB
5	1920 x 1080	102	9%	5.3 GB	18%	94%	1.2 GB
6	1920 x 1080	115	15%	6.0 GB	25%	0%	1.4 GB
7	1920 x 1080	114	17%	6.3 GB	23%	0%	1.4 GB

4.6.3.3 NVIDIA GPU

Streams	Size	FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	NVIDIA memory
1	1920 x 1080	20	2%	2.9 GB	37%	5%	2.6 GB
2	1920 x 1080	41	3%	3.1 GB	44%	7%	3.0 GB
3	1920 x 1080	61	5%	3.3 GB	93%	7%	3.4 GB

Streams	Size	FPS	Process CPU	Process memory	NVIDIA GPU	NVIDIA decode	NVIDIA memory
4	1920 x 1080	82	6%	3.5 GB	97%	8%	3.7 GB
5	1920 x 1080	103	7%	3.7 GB	97%	9%	4.1 GB
6	1920 x 1080	123	9%	3.9 GB	97%	11%	4.5 GB
7	1920 x 1080	144	10%	4.0 GB	97%	11%	4.8 GB
8	1920 x 1080	164	12%	4.2 GB	98%	11%	5.1 GB
9	1920 x 1080	185	14%	4.4 GB	98%	11%	5.4 GB
10	1920 x 1080	198	18%	5.1 GB	98%	11%	5.8 GB
11	1920 x 1080	184	18%	5.3 GB	98%	11%	6.1 GB

5 MIRASYS LICENSE PLATE RECOGNITION (LPR)

5.1 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.

On licensing side there is need to add RTSP Streaming Server feature to Management Server and all those servers where is plan to use SmartLPR feature. On Management Server side there is need to be add wanted amount of channels of SmartLPR feature.

5.2 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.

NVIDIA libraries (CUDA cuDNN, TensorRT) are not included in the LPR installer. The installer will detect the presence of the NVIDIA library installers from the 'NVIDIA' subfolder and install the libraries automatically if they are found.

For License Plate Recognition (LPR), you need to install the LPRService and LMService packages. LPR carries out the license plate recognition, and LM stores the license plate recognition events in PostgreSQL.

5.2.1 Requirements

- Administrator rights
- List Management Service installed
- License Plate Recognition license on the VMS Management Server
- RTSP license feature on the VMS Management Server and the VMS Server
- Required NVIDIA libraries (CUDA, cuDNN, TensorRT) are installed

5.2.2 NVIDIA libraries

Required NVIDIA libraries should be installed before installing the LPR service if they have not yet been installed. Installation of the LPR service requires the installation of the following NVIDIA libraries for Windows:

- CUDA Toolkit 12.9 Update 1: https://developer.nvidia.com/cuda-12-9-1-download-archive
- cuDNN 9.20.0: https://developer.nvidia.com/cudnn-9-20-0-download-archive
- TensorRT v10.16.0.72 GA for Windows 10, 11, Server 2022 and CUDA 12.0 to 12.9 ZIP Package: https://developer.nvidia.com/tensorrt/download/10x

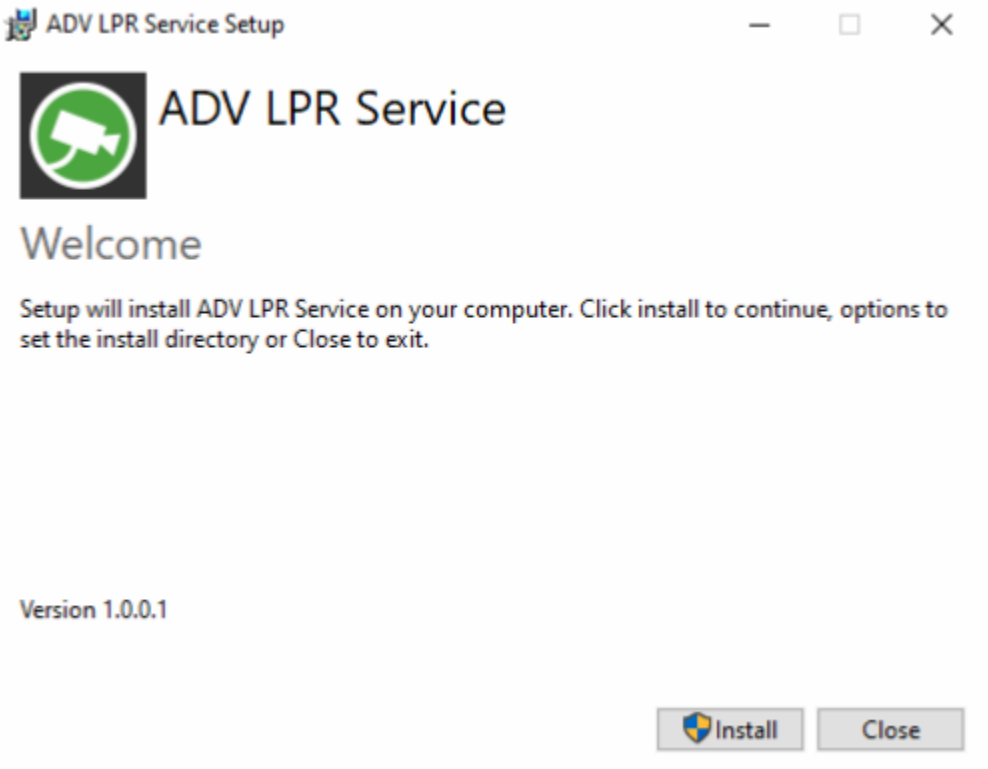
5.2.2.1 Installing NVIDIA libraries

1. Download the Mirasys LPR service installer and place it in a folder on your machine
2. Create a subfolder 'NVIDIA'
3. Download the NVIDIA libraries mentioned above
4. Save the downloaded NVIDIA libraries to the 'NVIDIA' subfolder
5. Run the Mirasys LPR service installer
    a. Mirasys LPR service installer automatically installs the NVIDIA libraries that it detects from the 'NVIDIA' subfolder before the service is installed
6. Follow the installation instructions to finalize the installation

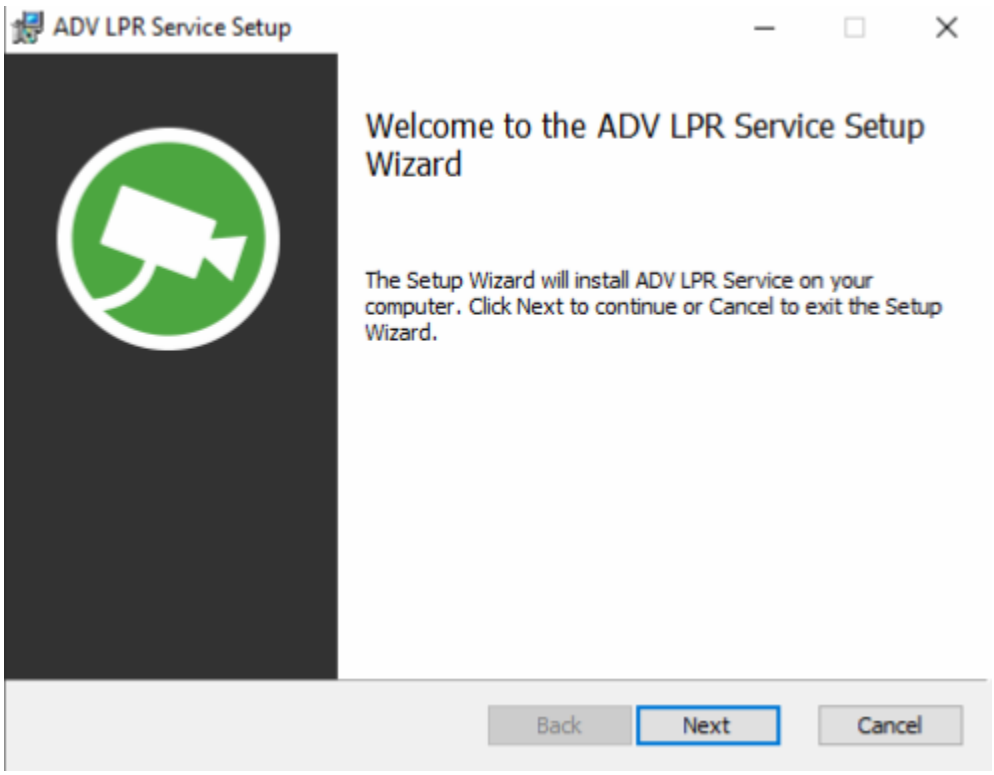
5.2.3 Installing the LPR service

The installer has a step for accepting the End-User License Agreement (EULA). You must confirm that you accept the terms presented in the agreement to continue with the installation.

1. Download the latest version from Extranet.
2. Unzip the files e.g. to the C:\temp folder.
3. Start the installation by double-clicking the installation file.
4. Click **Install** to continue.



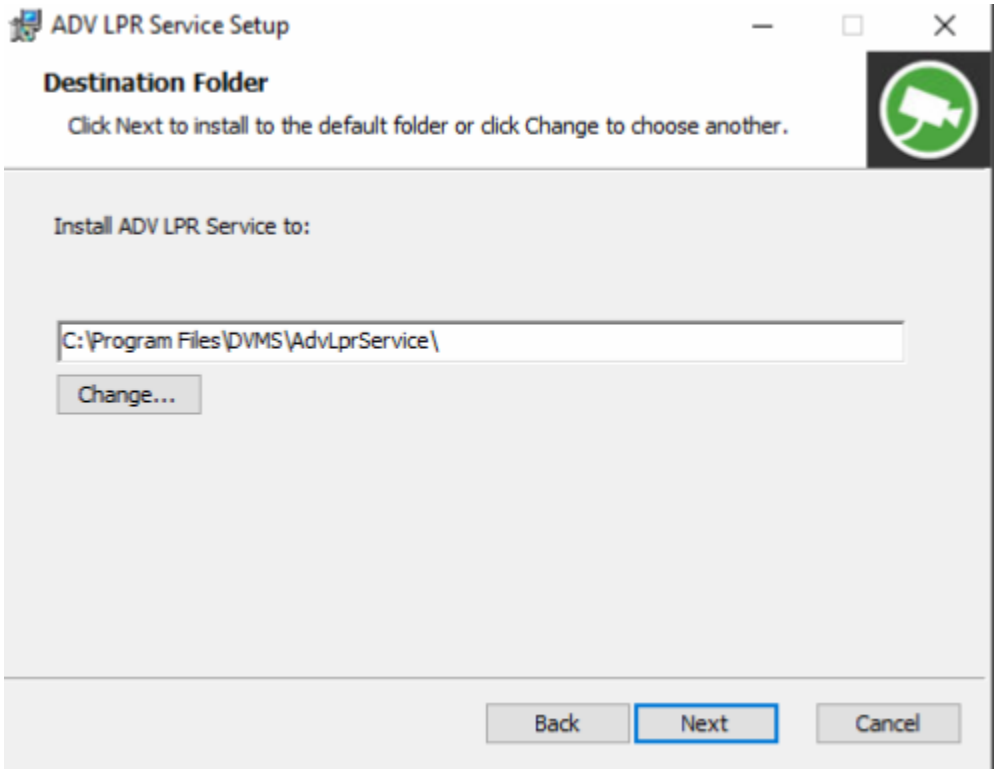
5. Click **Next** to continue.



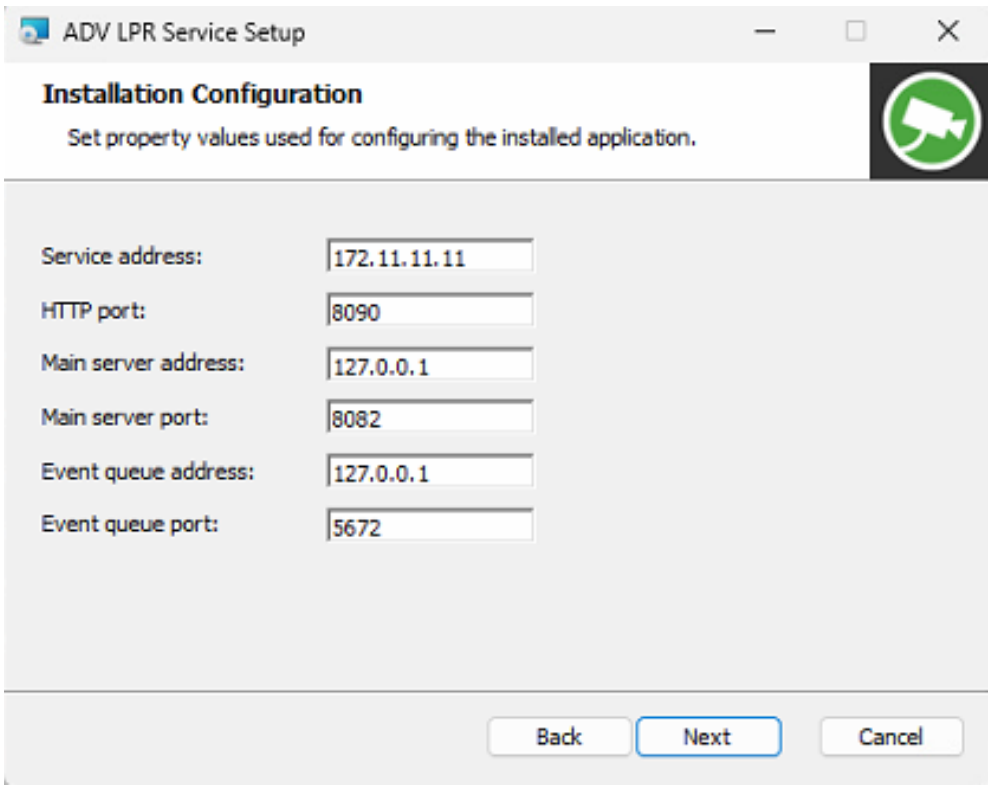
6. Check **I accept the terms in the License Agreement** and click **Next**.



1. Change the installation location if needed and click **Next** to continue.

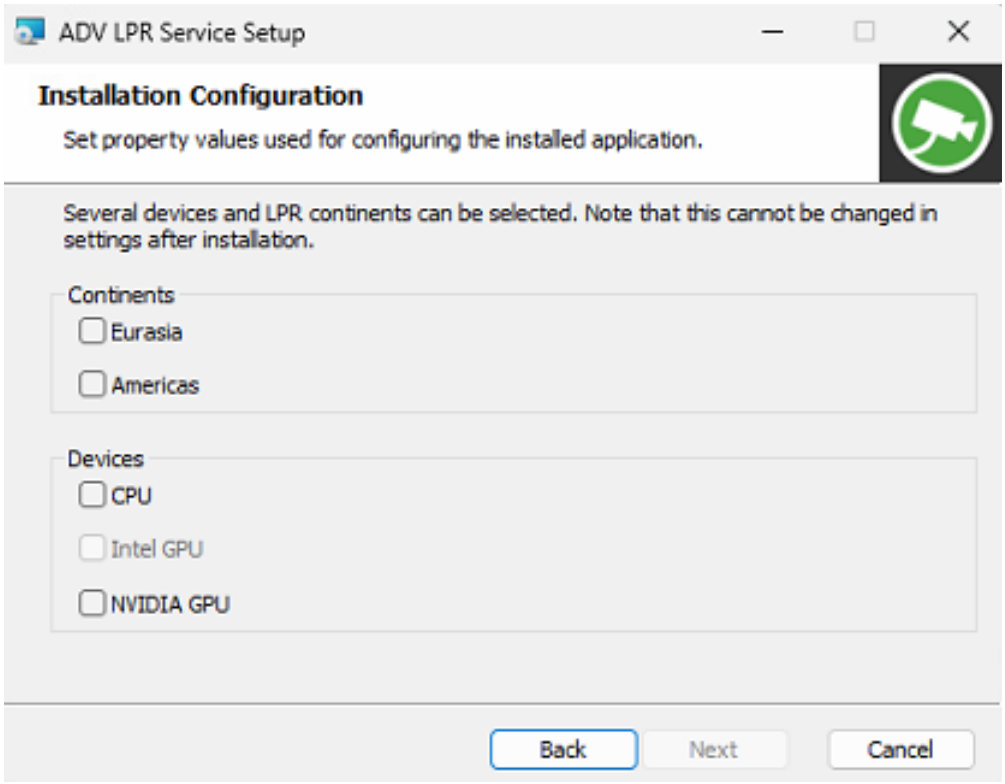


2. Change ports and addresses if needed.
    a. If you install the service on a machine other than VMS Main, you need to change the Main server address to the correct one.
    b. The same applies for Event queue address. Replace this address with the server address where the List Management Service is installed.
    c. Change the service address to one accessible from client applications. By default, the service address is the machine's first detected IP address.
3. Click **Next** to continue.

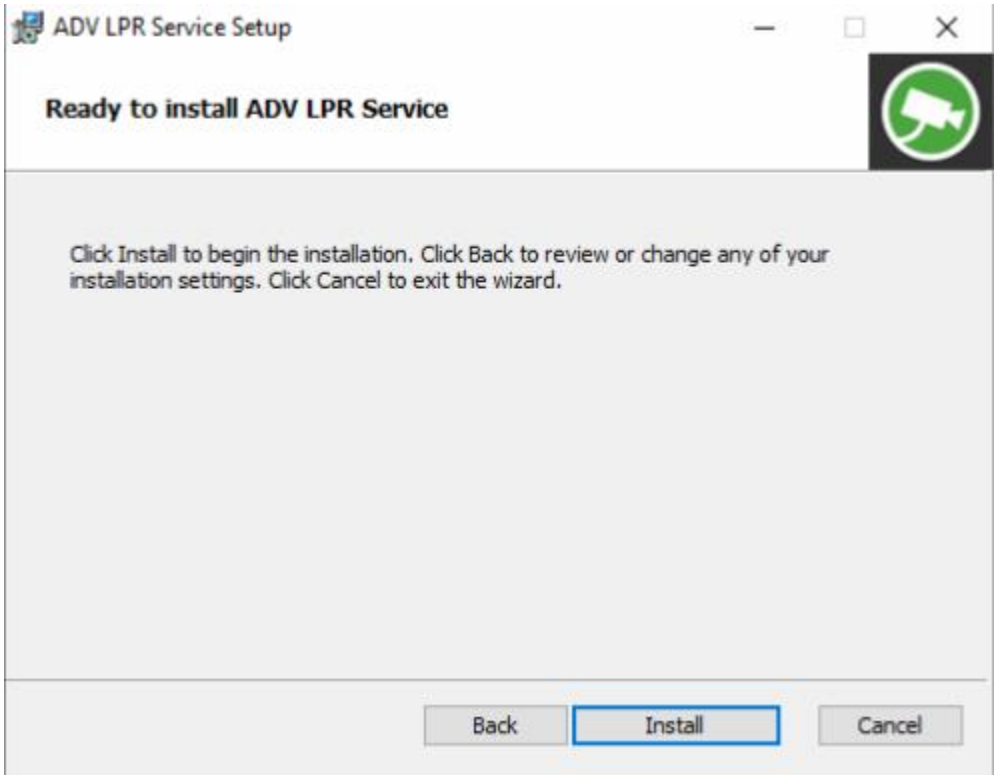


The HTTP port where the LPR service is hosted is by default 8090. Change the port in case the default port is reserved for some other use.
The main server uses port 8082 by default. Set the main server address and port to allow the LPR service to connect to the correct main server.
Event queue uses port 5672 by default. The event queue is installed with the LM service installation, where the used event queue port is set. Set the event queue address to the machine where the LM service is installed.

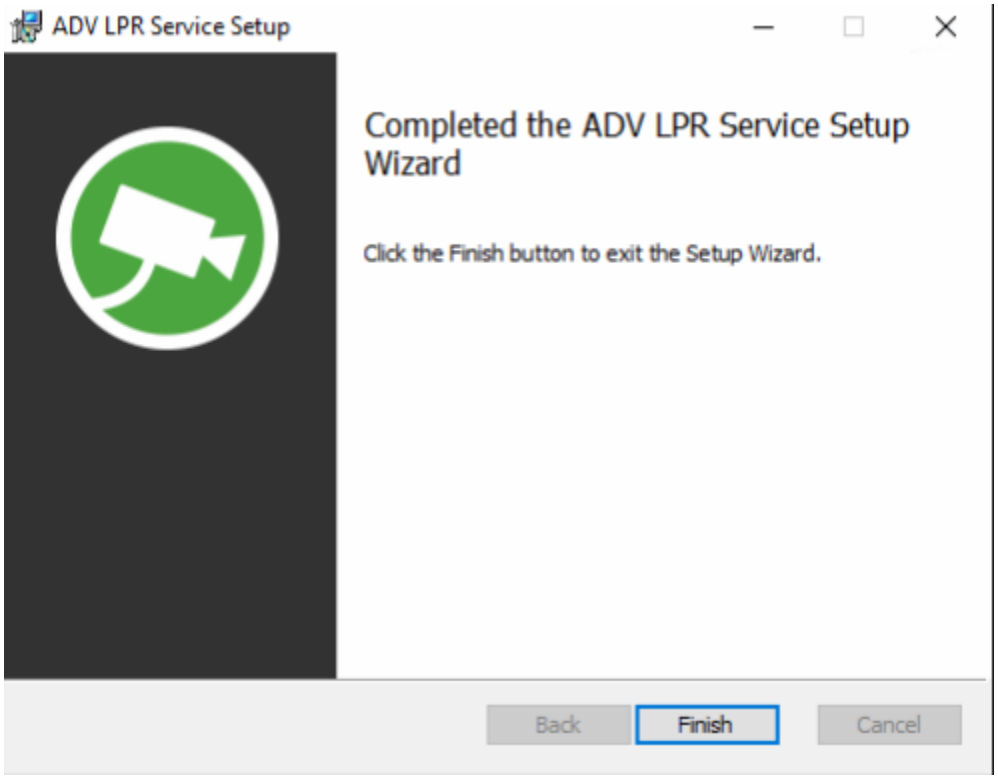
1. Select continents and devices and click **Next** to continue.



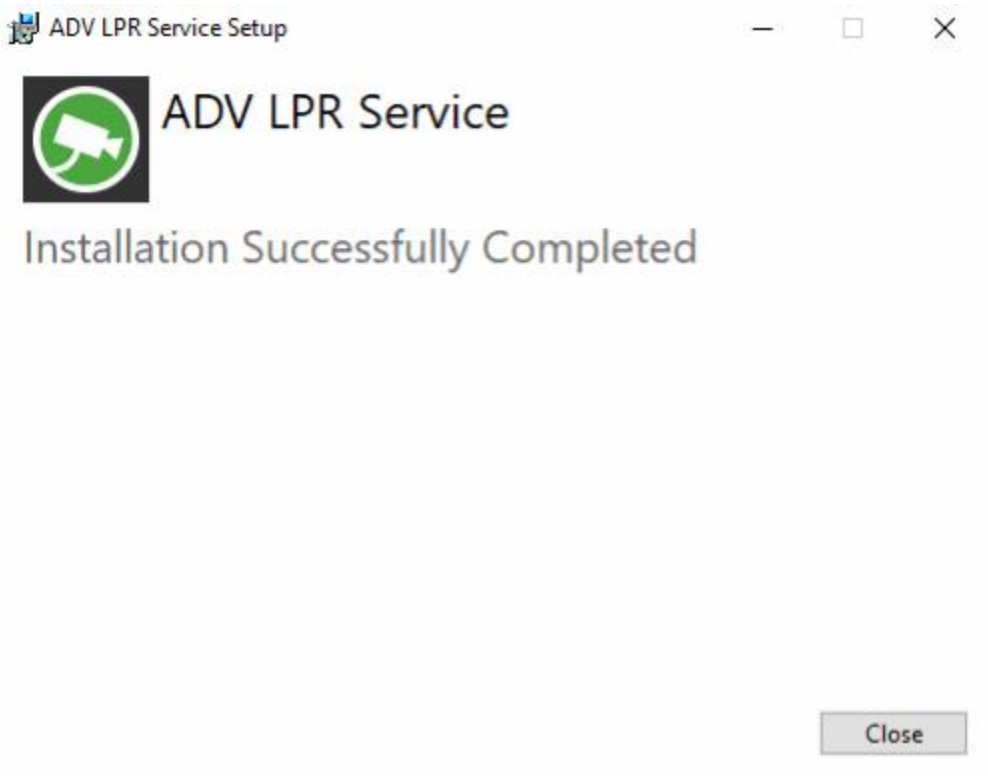
1. Click **Install** to continue and wait.
    a. Installation will take some time until it is finished.
    b. Model creation can take up to 30 minutes. This depends on how powerful the graphics card in use is.



2. Click **Finish** to continue.



3. Click **Close** to close the installation.



4. Now the License Plate Recognition Service is installed on the server and is ready to use.
    a. License Plate Recognition Service sends details to the VMS Main server. You can configure the service via System Manager.

5.3 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.

5.4 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.

5.4.1 Plate number country detection

Plate number detection is available for Eurasia and the Americas.

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.

5.4.2 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

5.5 Supported countries in Eurasia (LPR)

5.5.1 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.

5.5.2 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

5.6 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.

5.6.1 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

5.7 LPR PROCESSING, EVENTS, AND DETECTION

5.7.1 Devices

License plate recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

5.7.2 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.

5.7.3 Detected license plate visualization

Detected license plates can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

5.8 LPR ALARM TRIGGERS AND CONFIGURATION

5.8.1 Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

5.8.2 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.

5.9 LPR PERFORMANCE

5.9.1 Test machine

- 12th Gen Intel(R) Core(TM) i9-12900KF 3.19 GHz
- NVIDIA GeForce RTX 3080 Ti
- Intel UHD Graphics 750

5.9.2 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.

5.9.3 Test results

5.9.3.1 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

5.9.3.2 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
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

MIRASYS

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
12	1920 x 1080	252	**252**	26 %	95 %	34 %		5.6 GB
13	1920 x 1080	249	249	29 %	93 %	33 %		6.5 GB

Tel +358 (0)9 2533 3300 Email info@mirasys.com https://www.mirasys.com

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

5.9.3.3 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.

6 Easy LPR (Camera side license plate detection)

Easy LPR is a Spotter plugin that provides the option to receive camera-side license plate detections to the Mirasys VMS and update camera license plate lists.

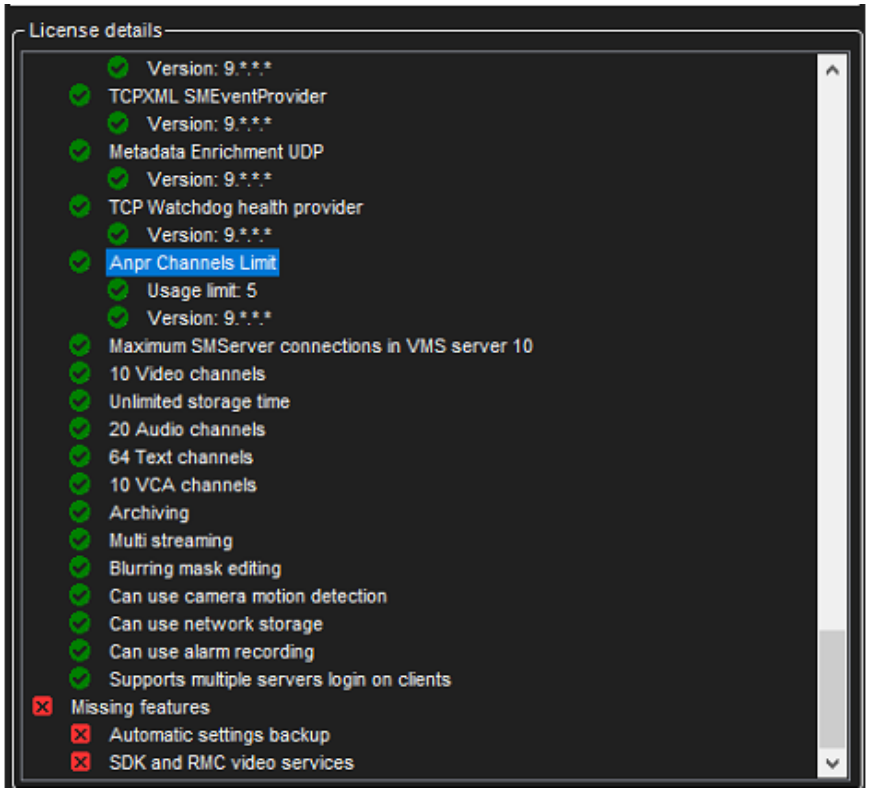
You can find instructions on how to use the plugin here.

Information on supported cameras is available here.

6.1 Licensing for Easy LPR

The plugin does not require a separate license. The Mirasys VMS server license defines how many ANPR channels can be added.

The feature name is **Anpr Channels limit,** and the controllable value name is **Usage limit**.



6.2 EASY LPR CONFIGURATION

6.2.1 Configuration process

1. Configure the LPR functionality for the cameras in use (please see the manufacturer's website for more information)
2. Check that license plates are correctly detected on the camera side
3. Add cameras to the Mirasys VMS
    a. Use a camera native driver
4. Check that the Mirasys VMS license supports LPR cameras
5. Enable Easy LPR (detailed instructions on this are available here)

You can find a list of supported cameras here. The list includes tested ANPR/LPR cameras.
Depending on the camera manufacturer's API, there may be a need to modify the camera-side XML.

6.2.2 Camera-specific configurations

If there is no camera manufacturer-specific guidance, you can follow the instructions here: Enable Easy LPR.

6.2.2.1 Axis and Axis License Plate Verifier

- Check that you have the latest Axis License Plate Verifier software installed on the camera
- Check that the Axis License Plate Verifier is licensed and working correctly
- Check that you are using the latest Axis driver for VMS

To get the Axis License Plate Verifier to send data to the VMS Server, there is a need to edit the driver XML file

- Open NewAxisIPCapture.xml and edit this using Notepad
    - Default location C:\Program Files\DVMS\DVR
- Find this section:

```
<!-- Axis License Plate Verifier configuration -->
<AxisANPR>
  <!-- Possible values: Any IPv4 address. An empty value means the default
interface. -->
  <!-- Several IP addresses should be semicolon separated, can be used to set
failover and master recorder addresses. -->
  <NetworkInterface></NetworkInterface>
  <!-- HTTP Web server URI -->
  <URI>/vms/server</URI>
  <!-- Plate cache timeout in sec -->
  <CacheTimeout>30</CacheTimeout>
  <!-- URI for getting thumbnail image -->
  <ThumbnailBaseUri>/axis-cgi/jpg/image.cgi</ThumbnailBaseUri>
  <ThumbnailUseCamera>Yes</ThumbnailUseCamera>
  <ThumbnailResolution>320x240</ThumbnailResolution>
  <!-- Boolean flag to enable or disable additional output of metadata to the log
(default value is 'No') -->
  <EnableDebugOutput>No</EnableDebugOutput>
</AxisANPR>
```

- In this section, you need to edit <NetworkInterface></NetworkInterface>
- Add here the VMS Server IP address, and if there is a failover, add this too
    - Do this for all needed servers
    - Please remember that the driver update or the VMS update overwrites these parameters
- Now you can save this file and replace the file in the DVR folder, and restart the DVRServer service

- If you need to see the debug output for the LPR handler, you can enable additional logging with the "EnableDebugOutput" parameter.

6.2.2.2 Hanwha Wisenet and Vaxtor

- Check that you have the latest Vaxtor LPR software installed on the camera
- Check that Vaxtor LPR is licensed and working correctly
- Check that you are using the latest Hanwha Wisenet driver for VMS

To get Vaxtor to send data to the VMS Server, there is a need to edit the driver XML file

- Open WisenetIPCapture.xml and edit this using Notepad
    - Default location C:\Program Files\DVMS\DVR
- Find this section:

```
<!-- Vaxtor ANPR configuration -->
<Vaxtor>
  <!-- Possible values: Any IPv4 address. Empty value means default interface -->
  <!-- Several IP addresses should be semicolon separated, can be used to set
failover and master recorder addresses. -->
  <NetworkInterface></NetworkInterface>
  <!-- HTTP Web server port (minimum port in range) -->
  <PortMin>9999</PortMin>
  <!-- HTTP Web server port (maximum port in range) -->
  <PortMax>11000</PortMax>
  <!-- HTTP Web server URI -->
  <URI>/vms/server</URI>
  <!-- Add or not thumbnail image to Vaxtor LPR event -->
  <Thumbnail>Yes</Thumbnail>
</Vaxtor>
```

- In this section, you need to edit <NetworkInterface></NetworkInterface>
- Add here the VMS Server IP address, and if there is a failover, add this too
    - Do this for all needed servers
    - Please remember that the driver update or the VMS update overwrites these parameters
- Now you can save this file and replace the file in the DVR folder, and restart the DVRServer service

6.2.2.3 Panasonic and Vaxtor

- Check that you have the latest Vaxtor LPR software installed on the camera
- Check that Vaxtor LPR is licensed and working correctly
- Check that you are using the latest Panasonic driver for VMS

To get Vaxtor to send data to the VMS Server, there is a need to edit the driver XML file.

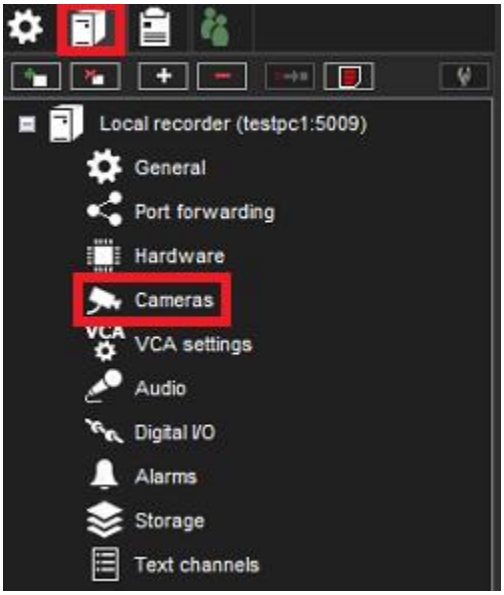
- Open NewPanasonicIPCapture.xml and edit this using Notepad
    - Default location C:\Program Files\DVMS\DVR
- Find this section:

```
<!-- Vaxtor ANPR configuration -->
<Vaxtor>
  <!-- Several IP addresses should be semicolon separated, can be used to set
failover and master recorder addresses. -->
  <NetworkInterface></NetworkInterface>
  <!-- HTTP Web server port (minimum port in range) -->
  <PortMin>9999</PortMin>
  <!-- HTTP Web server port (maximum port in range) -->
  <PortMax>11000</PortMax>
  <!-- HTTP Web server URI -->
  <URI>/vms/server</URI>
</Vaxtor>
```

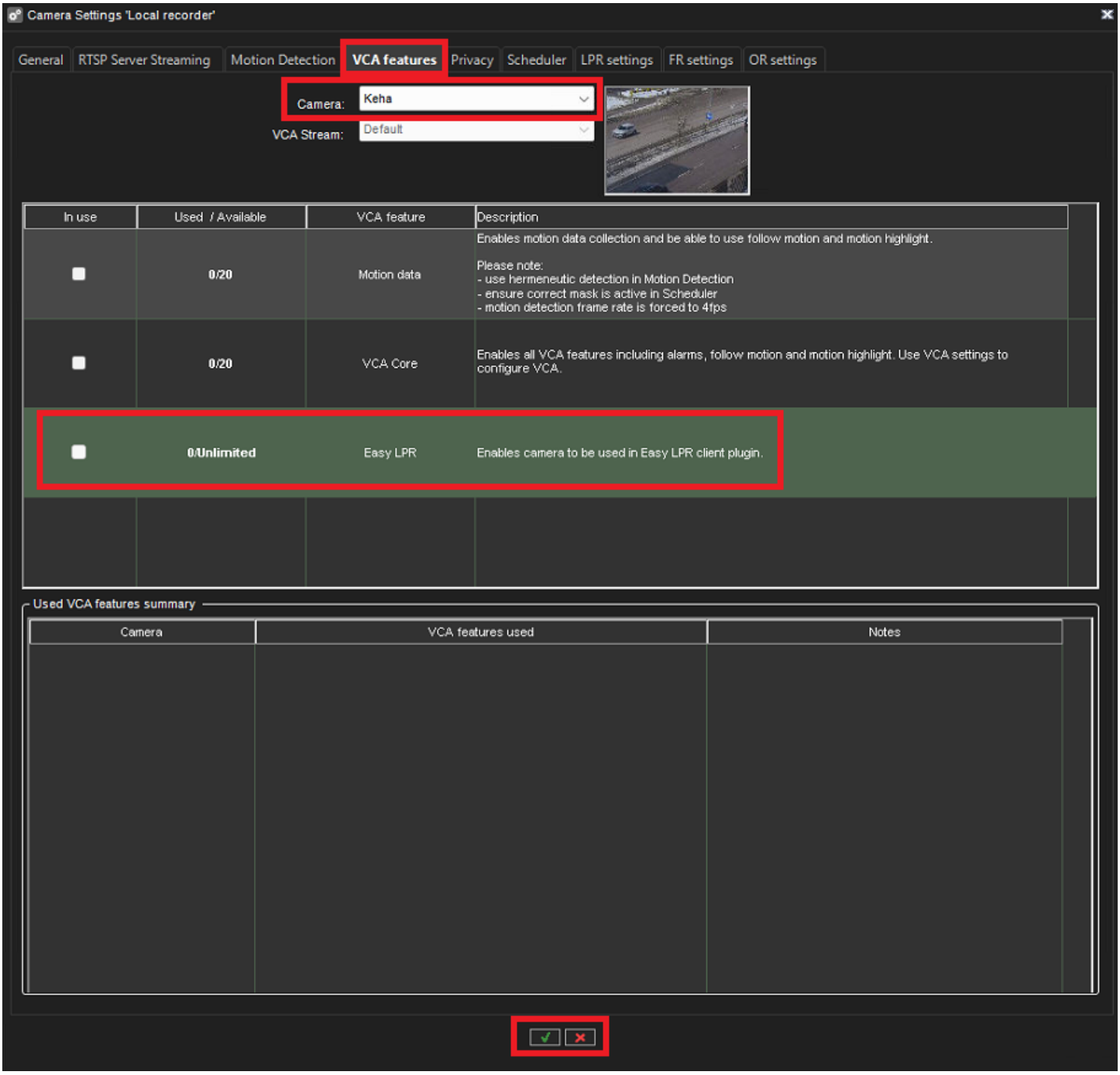
- In this section, you need to edit <NetworkInterface></NetworkInterface>
- Add here the VMS Server IP address, and if there is a failover, add this too
    - Do this for all needed servers
    - Please remember that the driver update or the VMS update overwrites these parameters
- Now you can save this file and replace the file in the DVR folder, and restart the DVRServer service

6.3 ENABLE EASY LPR

1. Open **VMS Servers**
2. Open **Cameras**



1. Click **VCA features**
2. Select LPR Camera
3. Enable **Easy LPR**
4. Click **Save**

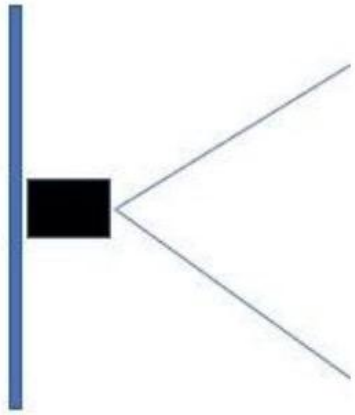


If the selected camera does not support Easy LPR, the option to mark it as “In use” is disabled.

Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

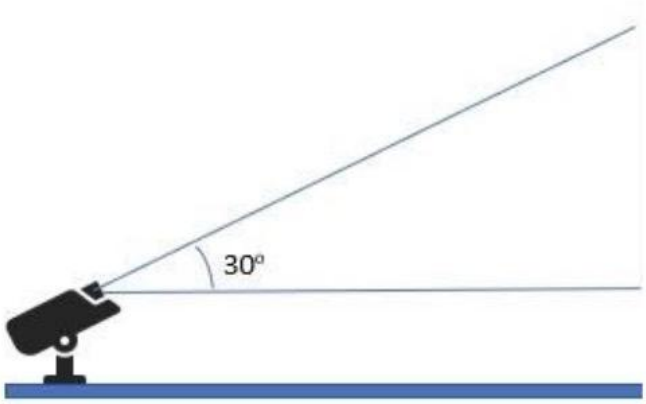
7 LPR CAMERA INSTALLATION TIPS

7.1 IT IS RECOMMENDED TO INSTALL THE CAMERA IN THE CENTER OF THE VEHICLE



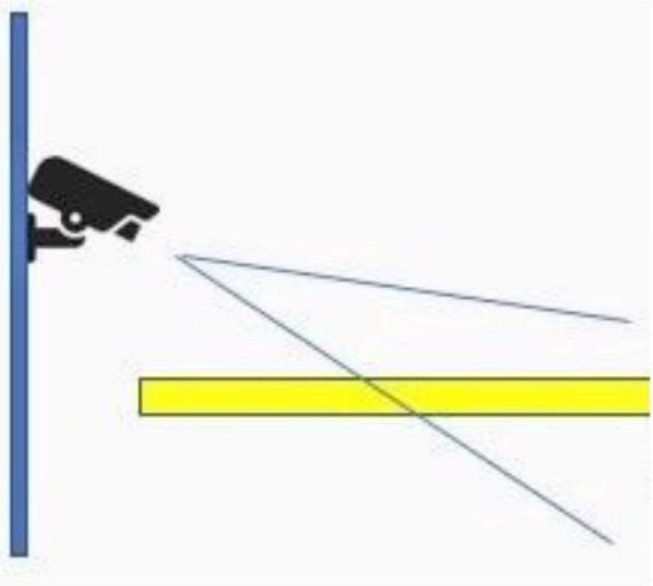


7.2 IF THE CAMERA IS INSTALLED ON THE SIDE OF THE ROAD OR LANE, THE ANGLE SHOULD NOT EXCEED 30 DEGREES.





7.3 THE CAMERA SHOULD BE INSTALLED HIGHER THAN THE VEHICLE HEADLIGHTS SO THAT THE VEHICLE'S HEADLIGHTS DON'T POINT DIRECTLY AT THE CAMERA





7.4 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

7.5 LICENSE PLATE TILT ANGLE MUST BE WITHIN +/- 10 DEGREES



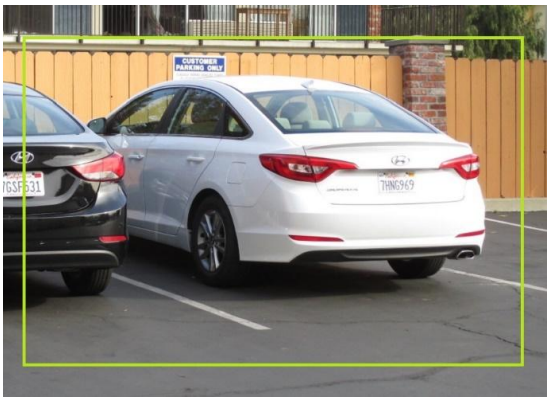


7.6 LPR SETTINGS IN THE SYSTEM MANAGER APPLICATION

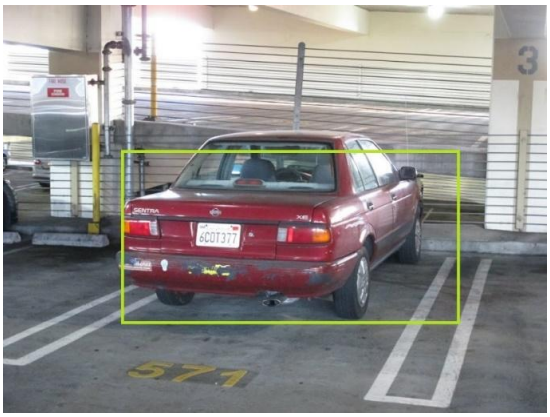
Ensure the correct region (Americas / Eurasia) is selected.

7.6.1 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.

7.6.2 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”.

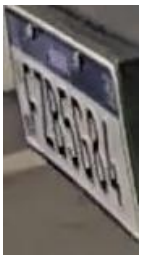
7.7 COMMON PROBLEMS AND SOLUTIONS

7.7.1 Incomplete license plate



Solution: Don’t set the region of interest too close to image borders.

7.7.2 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.

7.7.3 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.

7.7.4 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.

7.7.5 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.

7.7.6 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.

8 MIRASYS VCA GUIDE

8.1 ABOUT MIRASYS VCA

Mirasys VCA (Video Content Analytics) comprises a set of real-time video analytics solutions that utilize 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:

8.1.1 Motion object tracking

Motion-data-based object highlighting and tracking, auto-zoom functionality.

The motion data is produced by server-based, hermeneutic motion detection.

8.1.2 Tripwire counting

In addition to motion object tracking functionality, line counting for over-head installed cameras and Spotter client-based counter visualization.

8.1.3 Object behaviour/attributes detection

To continuously track and classify moving and stationary targets and features a full suite of rule-based filters, including 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.

8.1.4 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.

8.2 QUICK START GUIDE FOR VCA

Mirasys VMS 9.10.0 includes VCA Deep Learning analytics files for VCA AI detection V2.2.5 that requires NVIDIA GPU and CUDA Toolkit 11.8 GPU drivers. The NVIDIA CUDA toolkit v11.8 can be downloaded from NVIDIA site: https://developer.nvidia.com/cuda-11-8-0-download-archive

To help you get started quickly, we have listed essential topics below. Please execute the following steps for each server:

1. Decide what VCA functionality meets your requirements. For guidance, consult your Mirasys representative.
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. Configure alarms based on the VCA events if required.
9. Verify VCA functionality visualisation using the Spotter for Windows application.

To get the HWGUID for the VCA license, one camera has to be enabled in the System Manager camera settings to get the VCA engine running. After the VCA is running, the VCA HWGUID can be retrieved from the VMS server license dialog in the System Manager.

The VCA engine is started in the VMS server when at least one camera is configured to use the VCA in the System Manager camera settings. The very first VCA engine start will compile the NVIDIA libraries if Deep Learning is in use. This can take a lot of time, and it depends on the hardware used. During the compilation time, the VCA is not functioning.
It is highly recommended to wait until the NVIDIA libraries are compiled after the VCA is enabled, before doing any other operations on the VMS server.

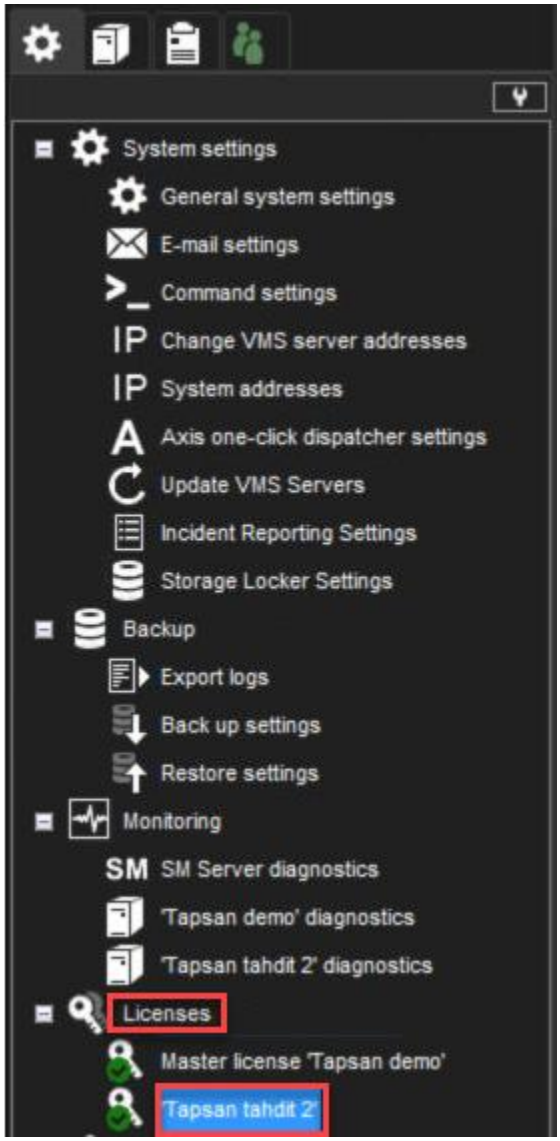
8.3 Prerequisites for Mirasys VCA

- Exporting VCA Core HW GUID file
- Activating the VCA license
- Setting up the motion detection method
- Activating VCA Core for the cameras
- NVIDIA GPU and CUDA Toolkit 11.8 GPU drivers

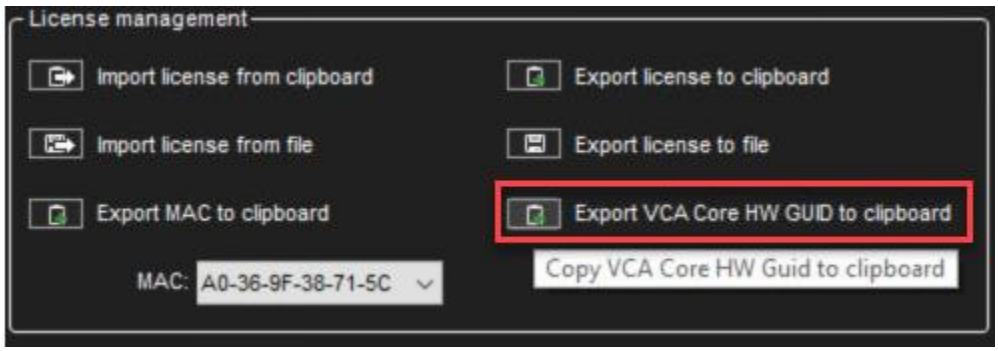
Mirasys VMS 9.10.0 includes VCA Deep Learning analytics files for VCA AI detection V2.2.5 that requires NVIDIA GPU and CUDA Toolkit 11.8 GPU drivers. The NVIDIA CUDA toolkit v11.8 can be downloaded from NVIDIA site: https://developer.nvidia.com/cuda-11-8-0-download-archive

8.3.1 Exporting VCA Core HW GUID file

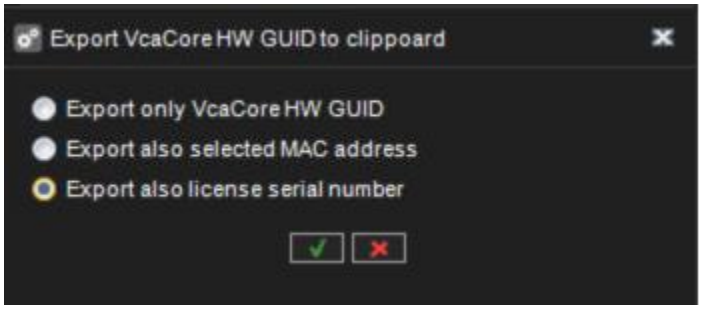
1. Go to the **System** tab
2. Open **Licenses**
3. Double-click the license



4. Select Export VCA Core HW GUID to clipboard



5. Select **Export also license serial number**
6. Click Ok



7. Paste the clipboard data into the text document.
8. Send it to Mirasys to receive the VCA license.

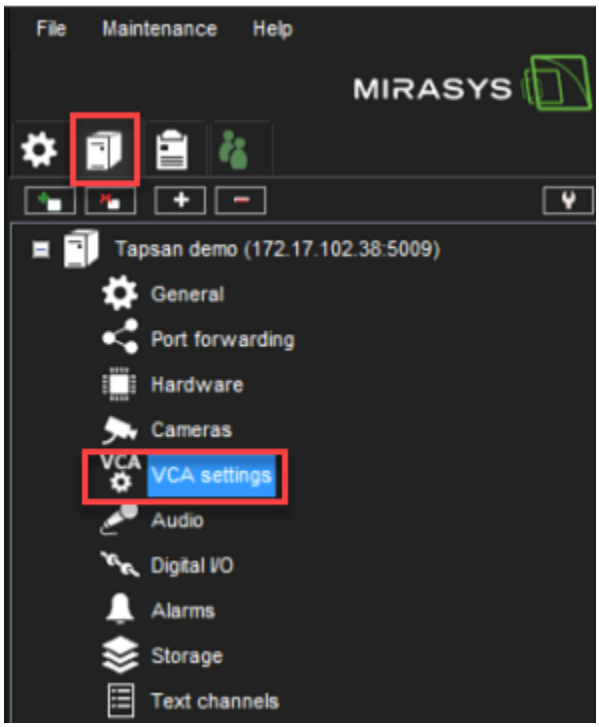
VcaCore Hw Guid: C1092267BD20344A5853FFD2BEA65406C1884F6FA19B503395E85F8545F75E2D

License serial number: YL9QMELM9QK5

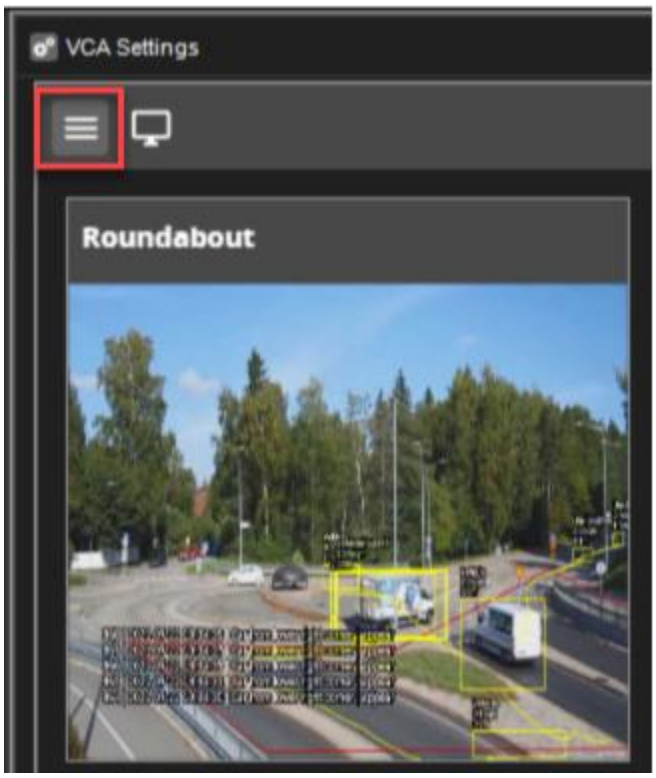
To get the HWGUID for the VCA license, one camera has to be enabled in the System Manager camera settings to get the VCA engine running. After the VCA is running, the VCA HWGUID can be retrieved from the VMS server license dialog in the System Manager.

8.3.2 Activating VCA licenses

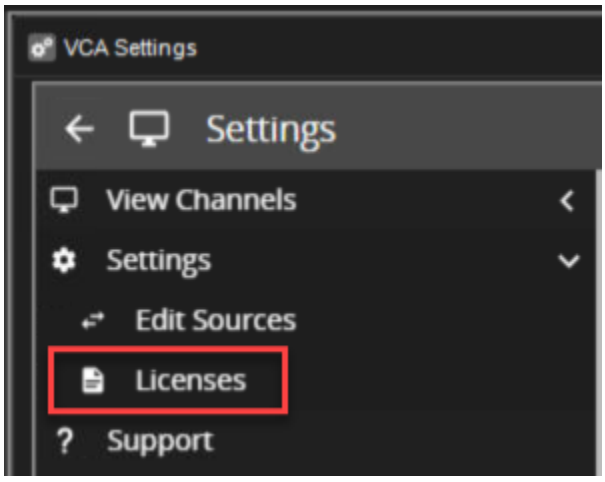
1. Go to the **VMS Servers** tab
2. Open **VCA settings**



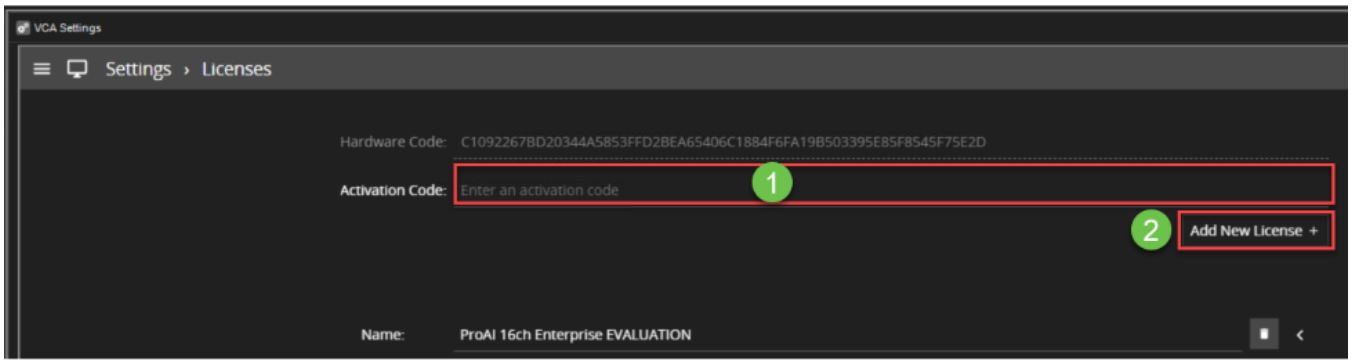
3. Click the **Settings** icon in the upper left corner



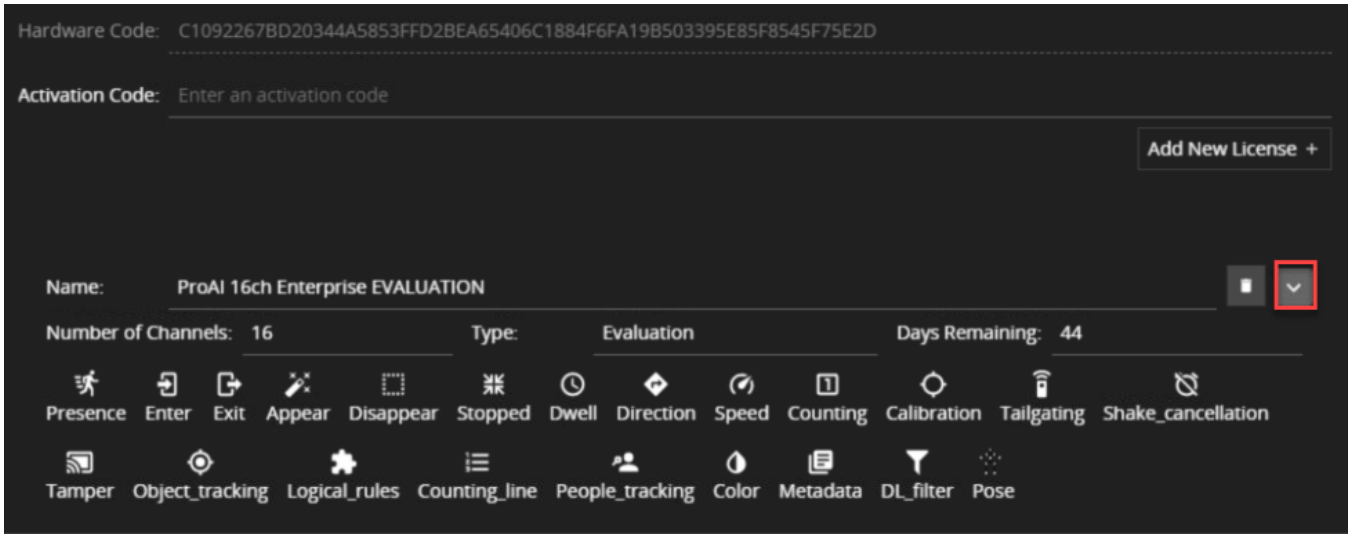
4. Select **Licenses**



5. Paste the license, which you have received from Mirasys, into the **Activation Code field**
6. Click **Add New License**

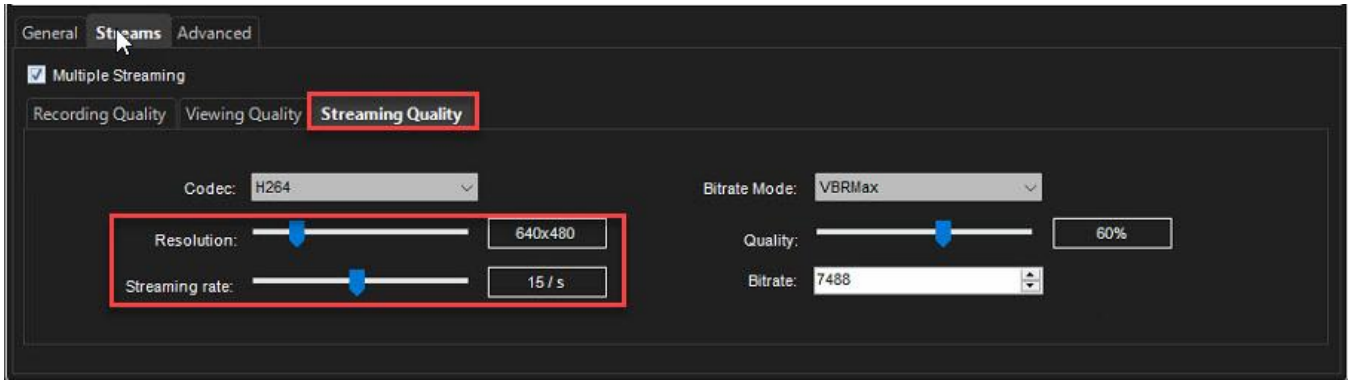


7. When the license is added, you will see overall information about the license and supported features



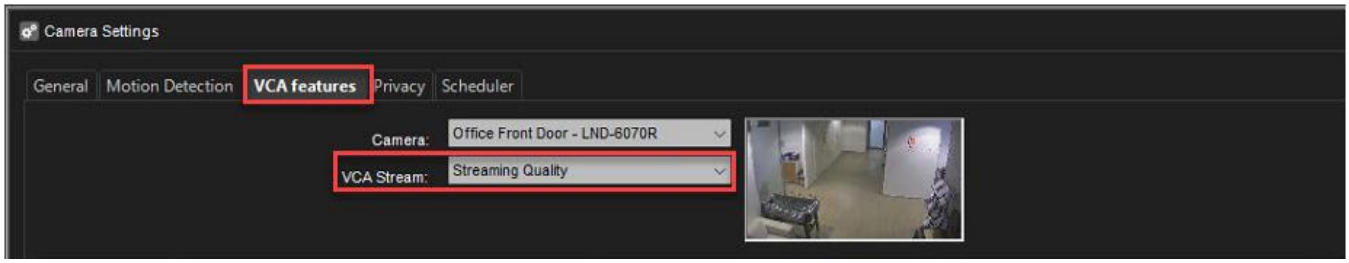
8.3.3 Setting up the resolution and record rate

1. Enable **Multiple Streaming** to the cameras that are used for the Mirasys VCA
2. Set **Streaming Quality** resolution to **640x480**
3. Set **Streaming Quality** Streaming rate to **15/s**



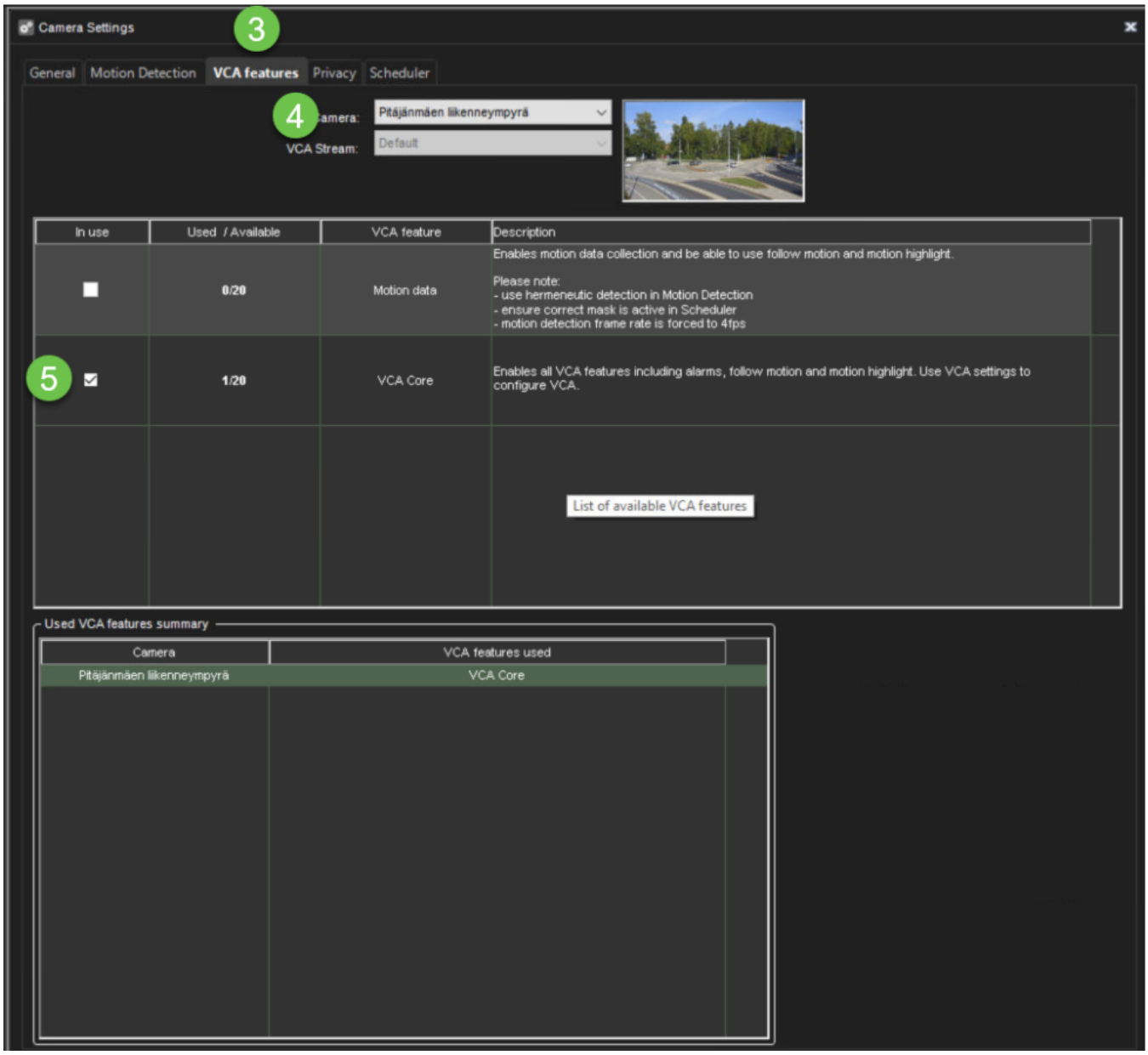
8.3.4 Selecting VCA Stream

1. Open the **VCA Features** tab
2. Select a camera from the list
3. Open the **VCA Stream** dropdown list and select **Streaming Quality**



8.3.5 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**



8.4 SUPPORTED OPERATING SYSTEMS

Mirasys uses a third-party solution for VCA, which is integrated to the Mirasys VMS.

The officially supported operating systems are:

- Windows 11 / Server 2016 (or higher)

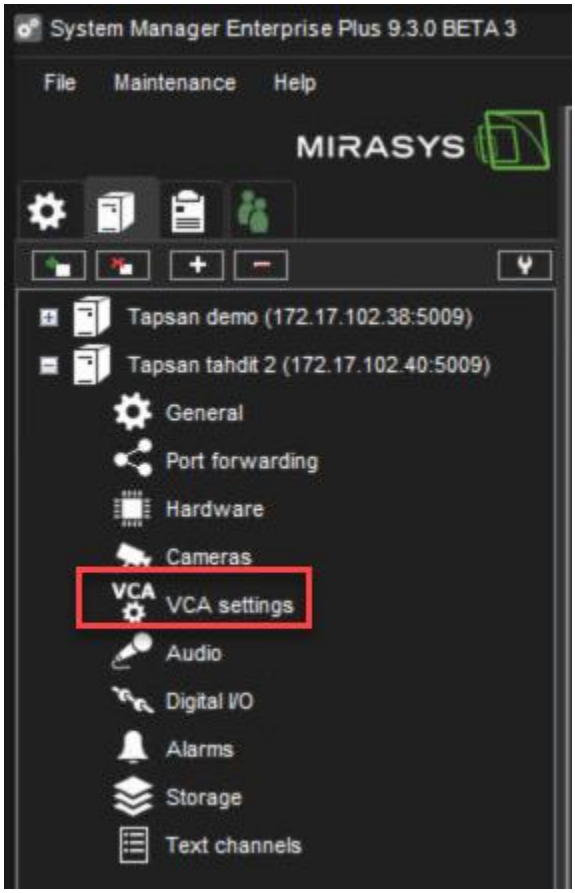
- Ubuntu 22.04 LTS Desktop / Server (or higher)

With these operating systems, you get the best performance.

You can still use any other newer operating system or server operating system for the Mirasys VMS server.

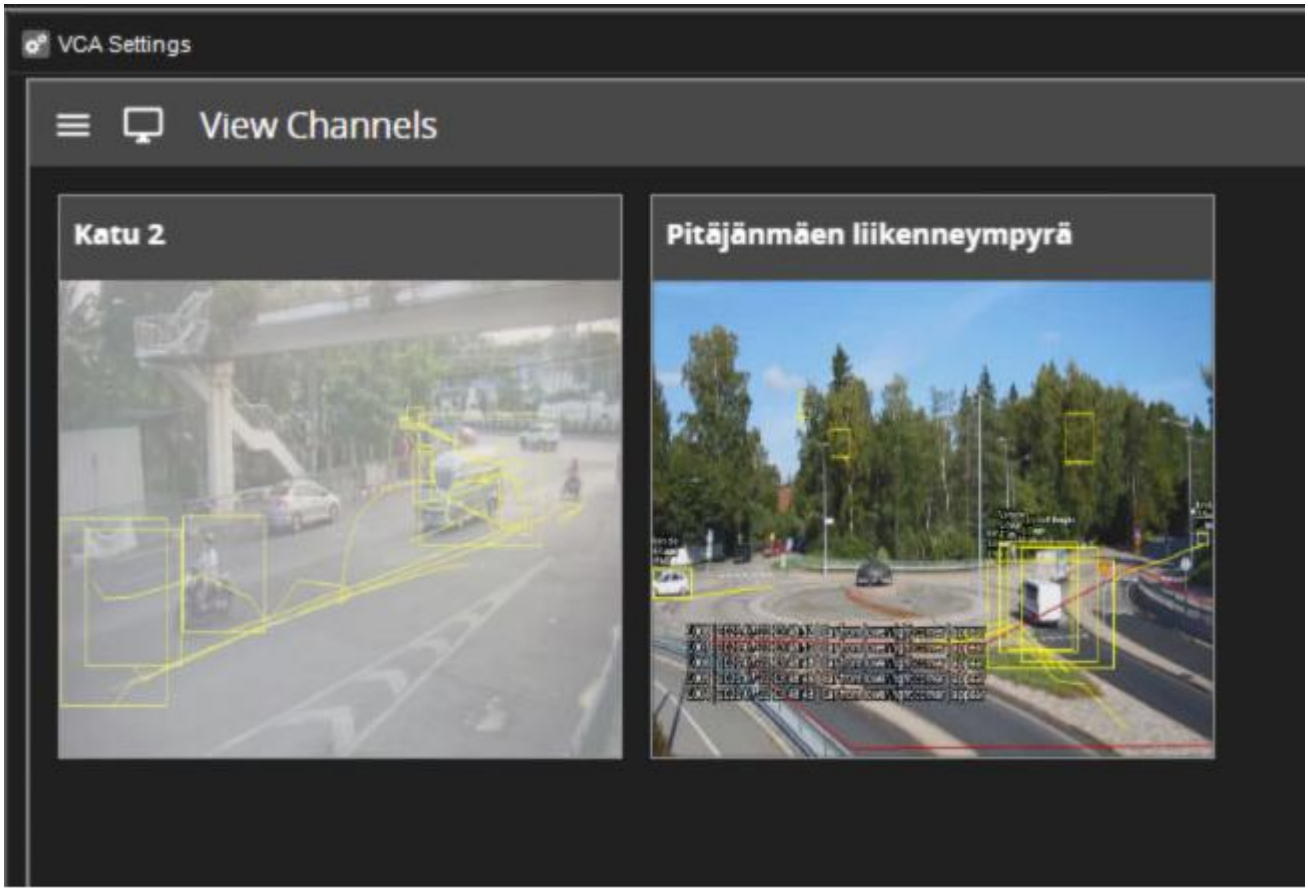
8.5 VCA Settings on System Manager

1. Go to the **VMS Server** tab
2. Open **VCA Settings**



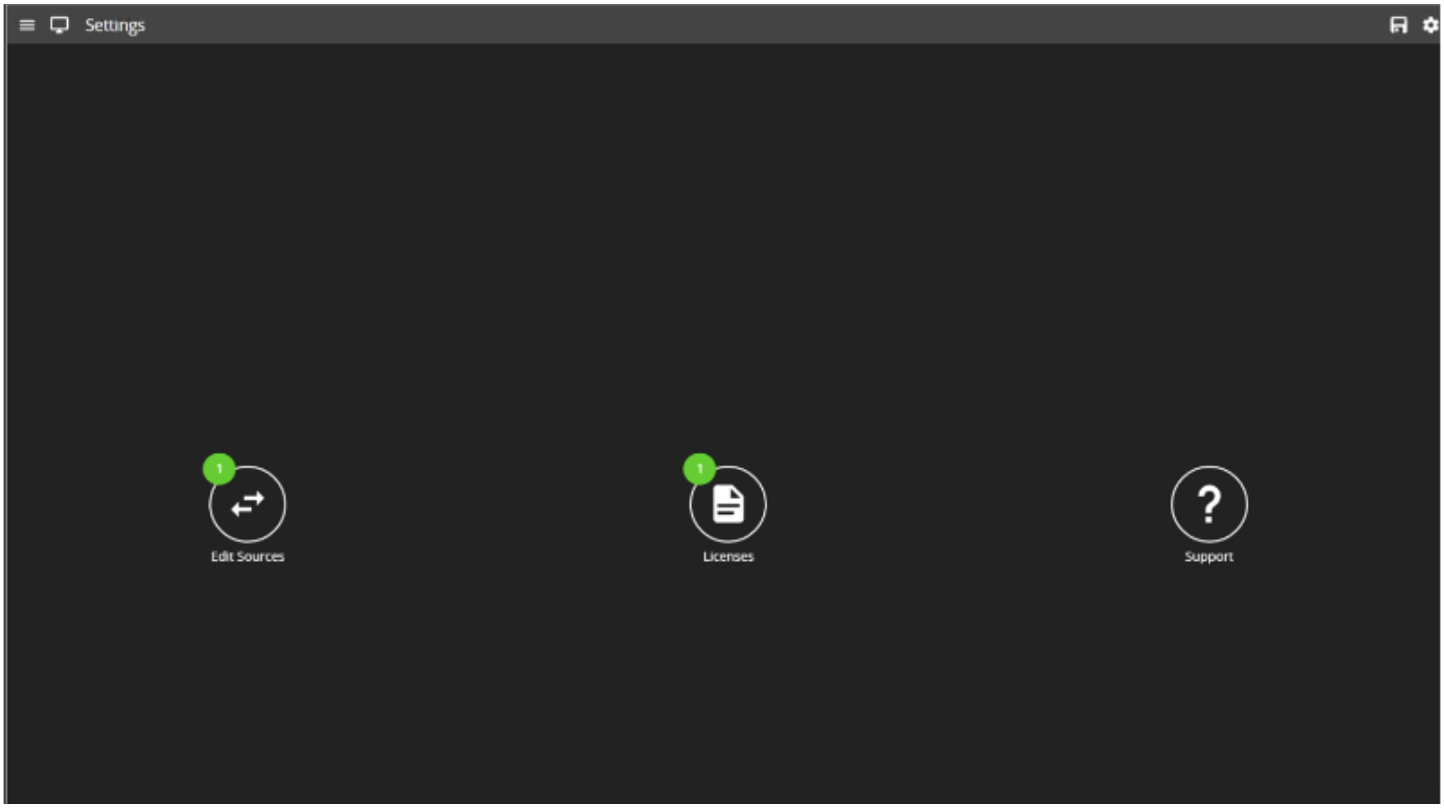
8.5.1 View Channels

View Channels show all cameras, which **VCA Core** is enabled.



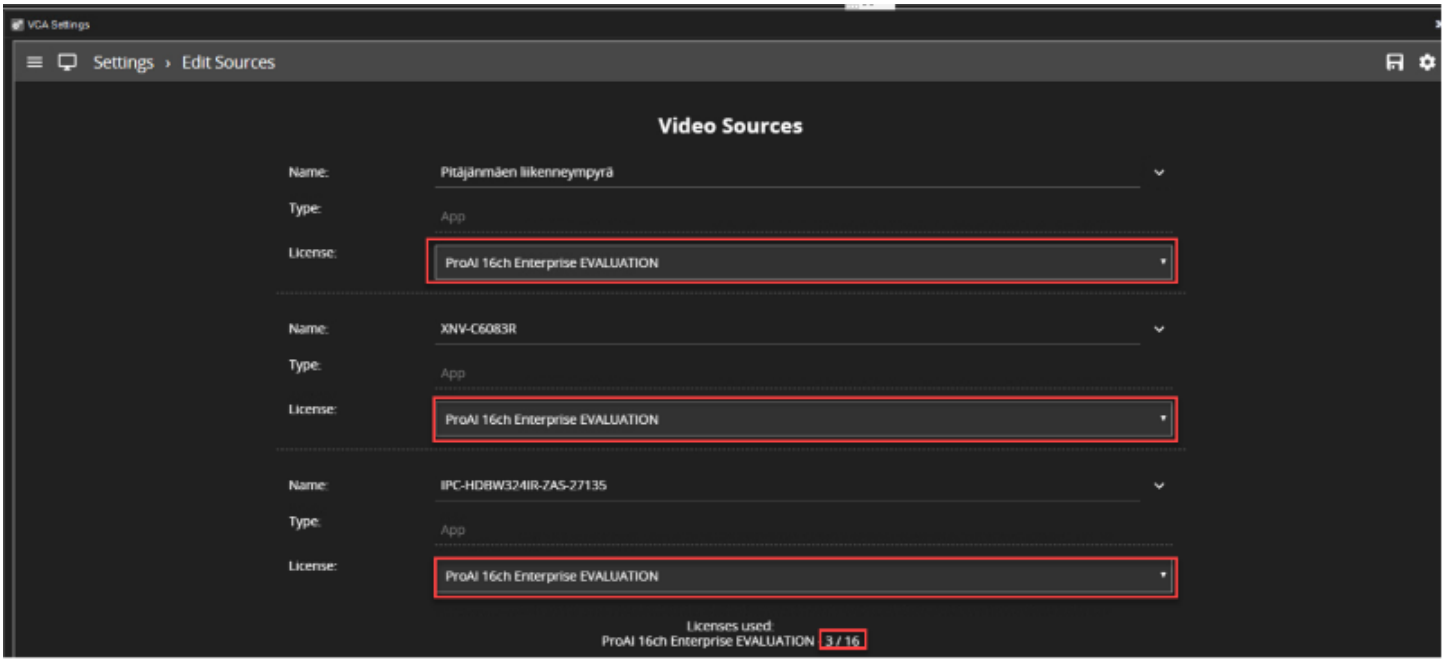
8.5.2 Settings

- Edit Sources
- Licenses
- Support



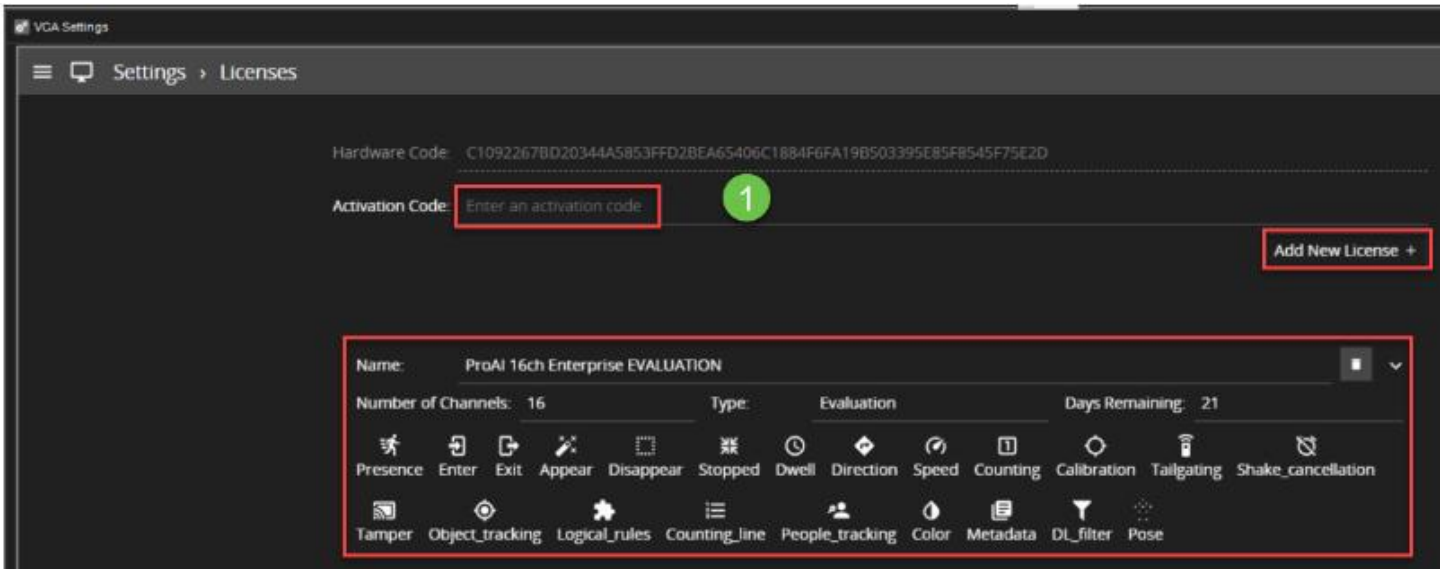
8.5.3 Edit Sources

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.



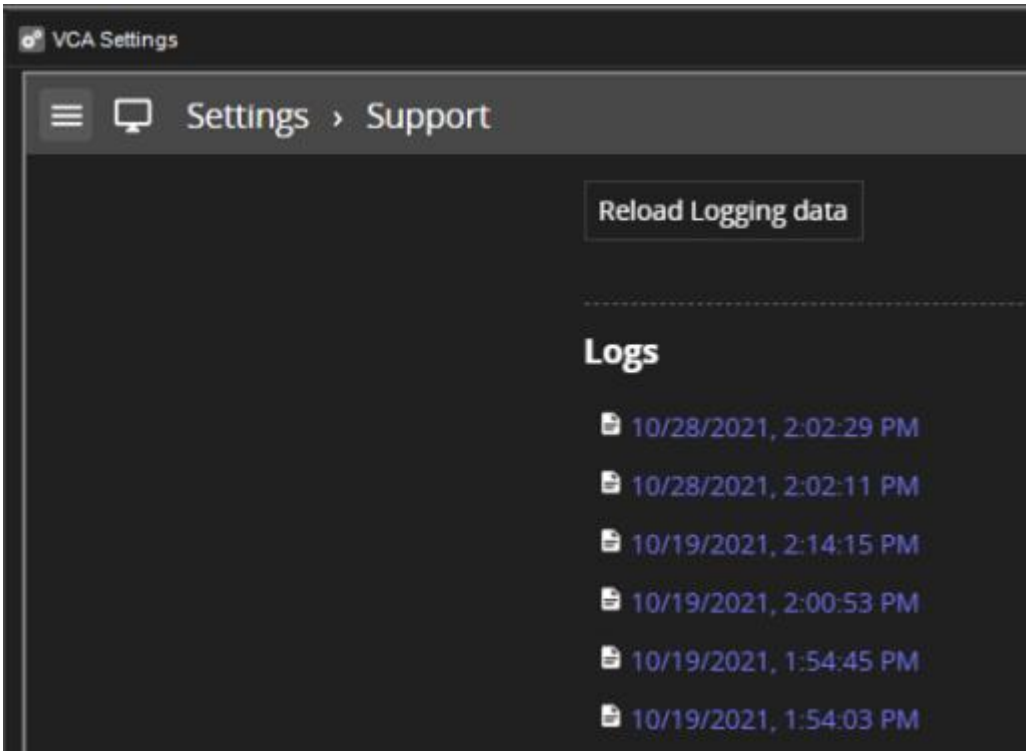
8.5.4 Licenses

Licenses show existing license type and that features
Users can add more VCA licenses



8.5.5 Support

Support show logs from the Mirasys VCA and users can download logs



8.6 MIRASYS VCA DEEP LEARNING

8.6.1 Requirements

- Nvidia GPU with CUDA cores
    - An NVIDIA GPU with CUDA Compute Capability 7.5 or higher
    - Depending on the 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

8.6.2 Installation

1. Install the latest Nvidia drivers in the system
2. Download the **Mirasys VCA Deep Learning** package from the Mirasys Extranet
3. Extract the package
4. Browse to the folder **CUDA Toolkit**

5. Install **CUDA Toolkit** with all features
    a. You can find a detailed installation guide here.
    b. Some features are not installed because Microsoft Visual Studio is not needed to install, but the toolkit provides example files
    c. If you have already installed Mirasys VMS, before copying files, the VMS services need to be stopped.
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
    b. This path is the default installation location of Mirasys VMS: if you have installed Mirasys VMS in another location, copy the files there
8. 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.

The VCA engine is started in the VMS server when at least one camera is configured to use the VCA in the System Manager camera settings. The very first VCA engine start will compile the NVIDIA libraries, which can take a lot of time. The time of the compilation depends on the hardware used. During the compilation time, the VCA is not functioning.
It is highly recommended to wait until the NVIDIA libraries are compiled after the VCA is enabled, before doing any other operations on the VMS server.

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). To get the HWGUID for the VCA license, one camera has to be enabled in the System Manager camera settings to get the VCA engine running. After the VCA is running, the VCA HWGUID can be retrieved from the VMS server license dialog in the System Manager.

In some cases, detection may not work correctly. Please try to increase the image quality or move/zoom the camera image closer to the wanted detection area.
Models are trained using clear images, and in some cases, when using a black and white image or a thermal camera image, the detection might not work correctly. To solve this, you can try using the Deep Learning Filter with Object Tracker.

8.7 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 in 9.4 and onward.

Do not install any other services on the license server. This can cause issues on licensing side.

You don't need to install the VCA License Server if you are using the Main Server as the License Server, and this is a physical server. In this case, the VMS includes VCA, and you can install licenses via System Manager - VCA Settings. Then connect each server to the Main Server IP-address.

It is recommended to use the same VMS version when one VMS is working as a VCA license server.

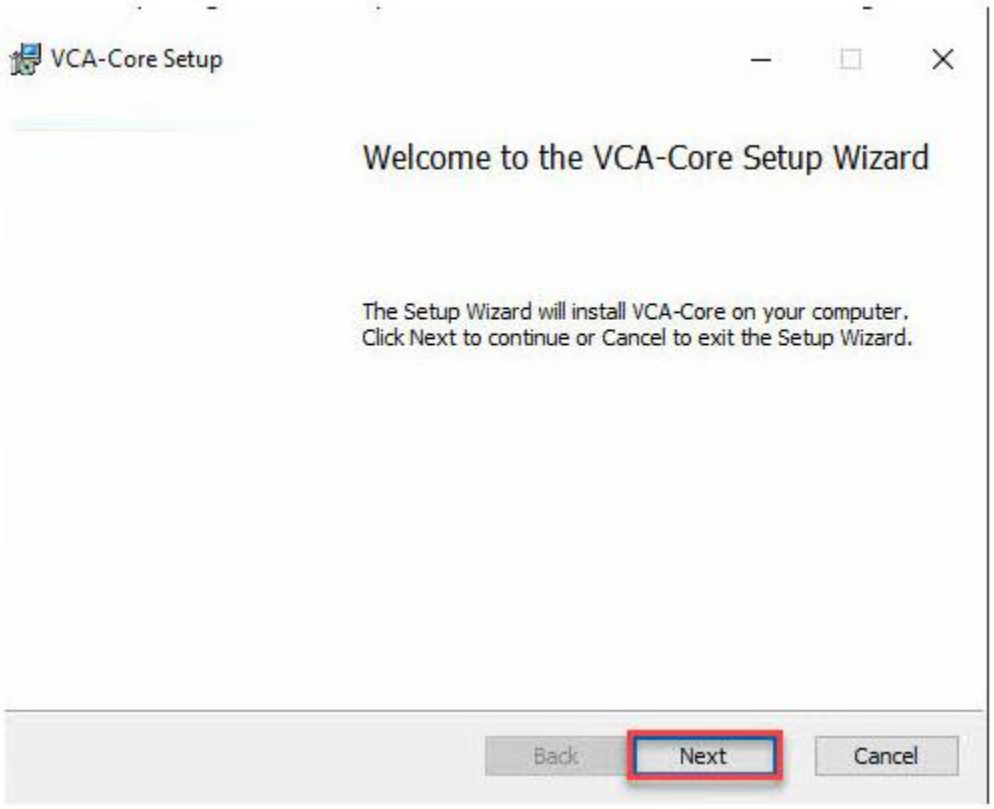
The VCA license server needs to be installed on a separate physical machine, and cannot be installed on the same machine where VMS is installed, as this will cause the VCA functions to overlap.

8.7.1 Port

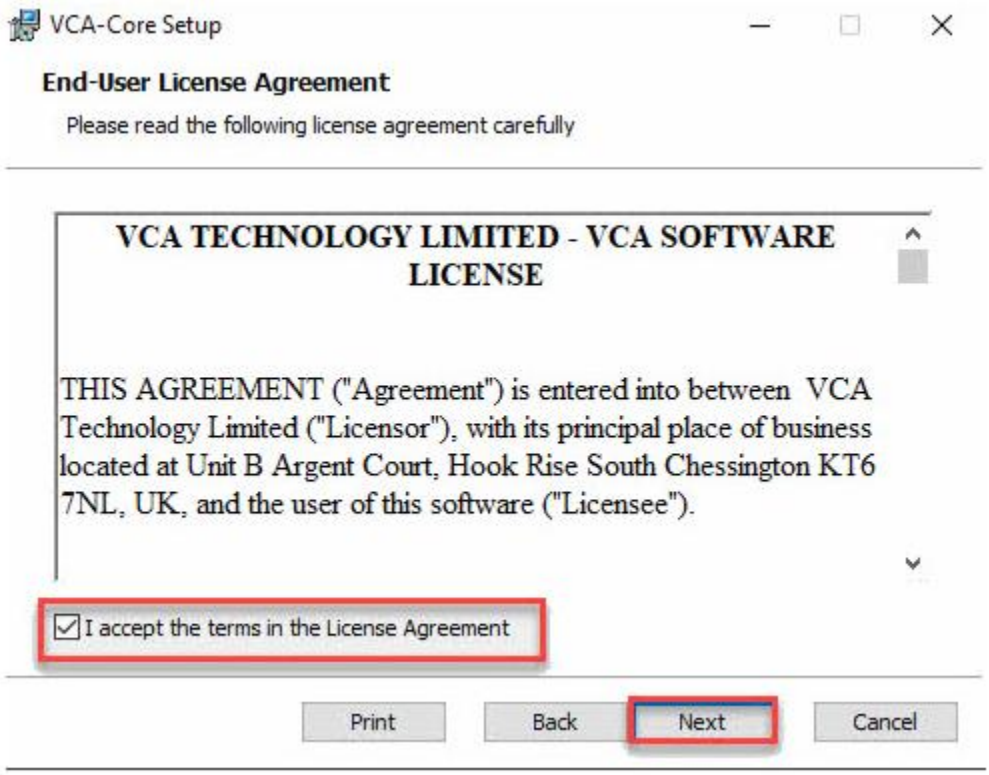
- 8080, TCP for VCA License Server Management
- 15769, TCP for VCA License Port

8.7.2 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

8.7.3 Usage and licensing

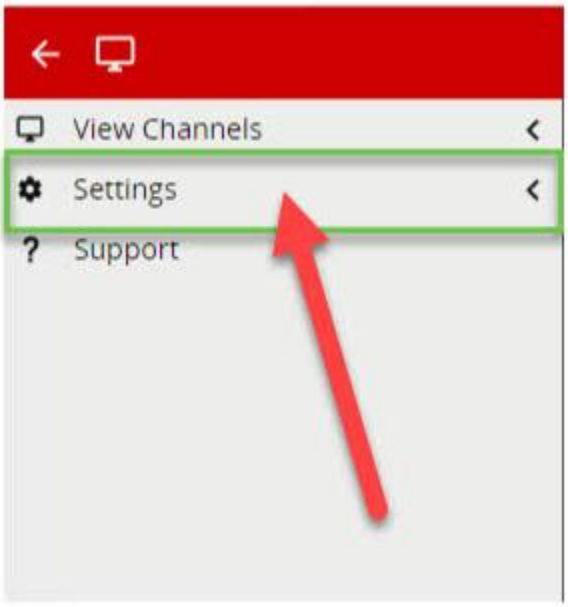
To log in to Mirasys VCA License Server, you need to use the browser and go to the site http://localhost:8080/.
The default username is **admin,** and the default password is **admin**

8.7.3.1 On the main page, you can access settings via the burger menu.

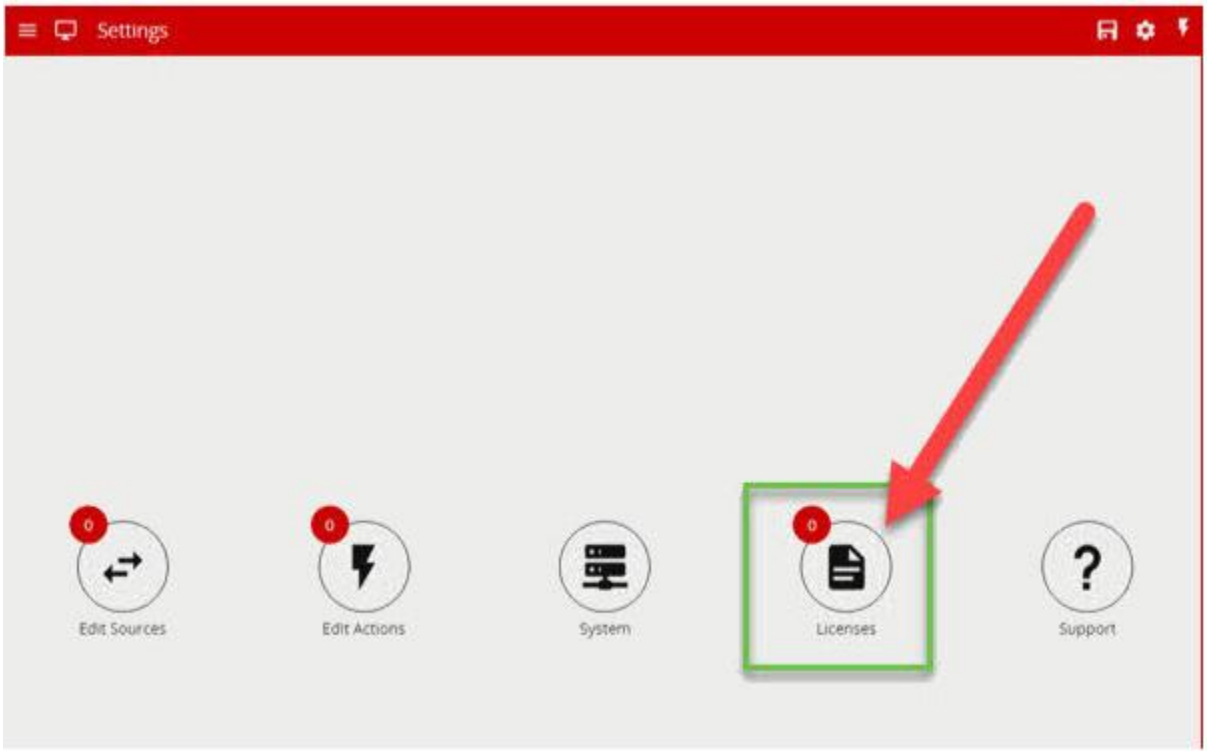


8.7.3.2 Adding the license

1. Open **Settings**



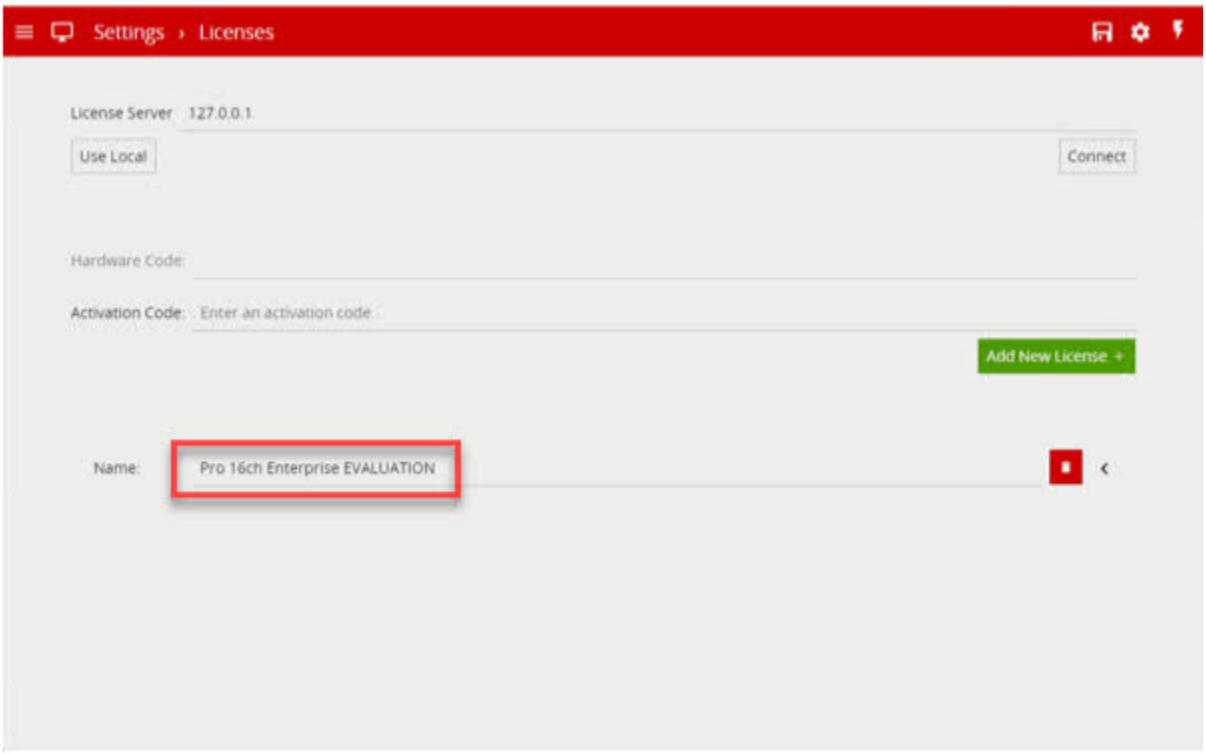
2. Open **Licenses**



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**

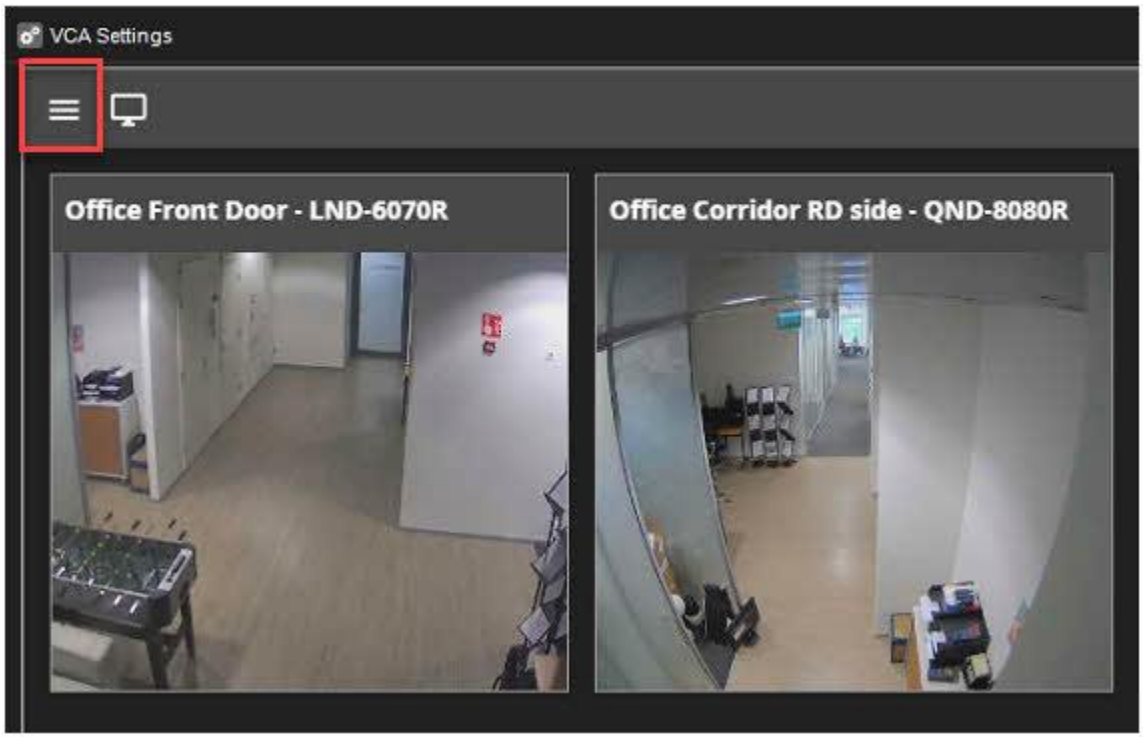


5. When you have added wanted licenses or licenses to the system, you can proceed on Mirasys VMS side.

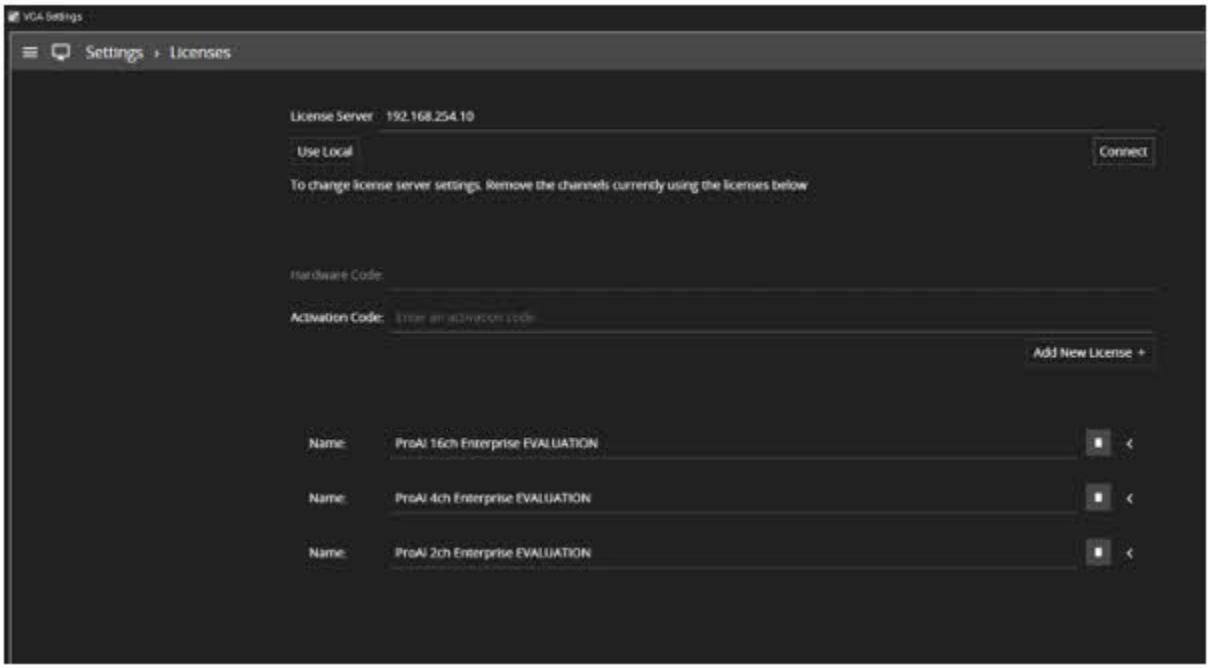


8.7.4 Mirasys VMS Configuration

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.

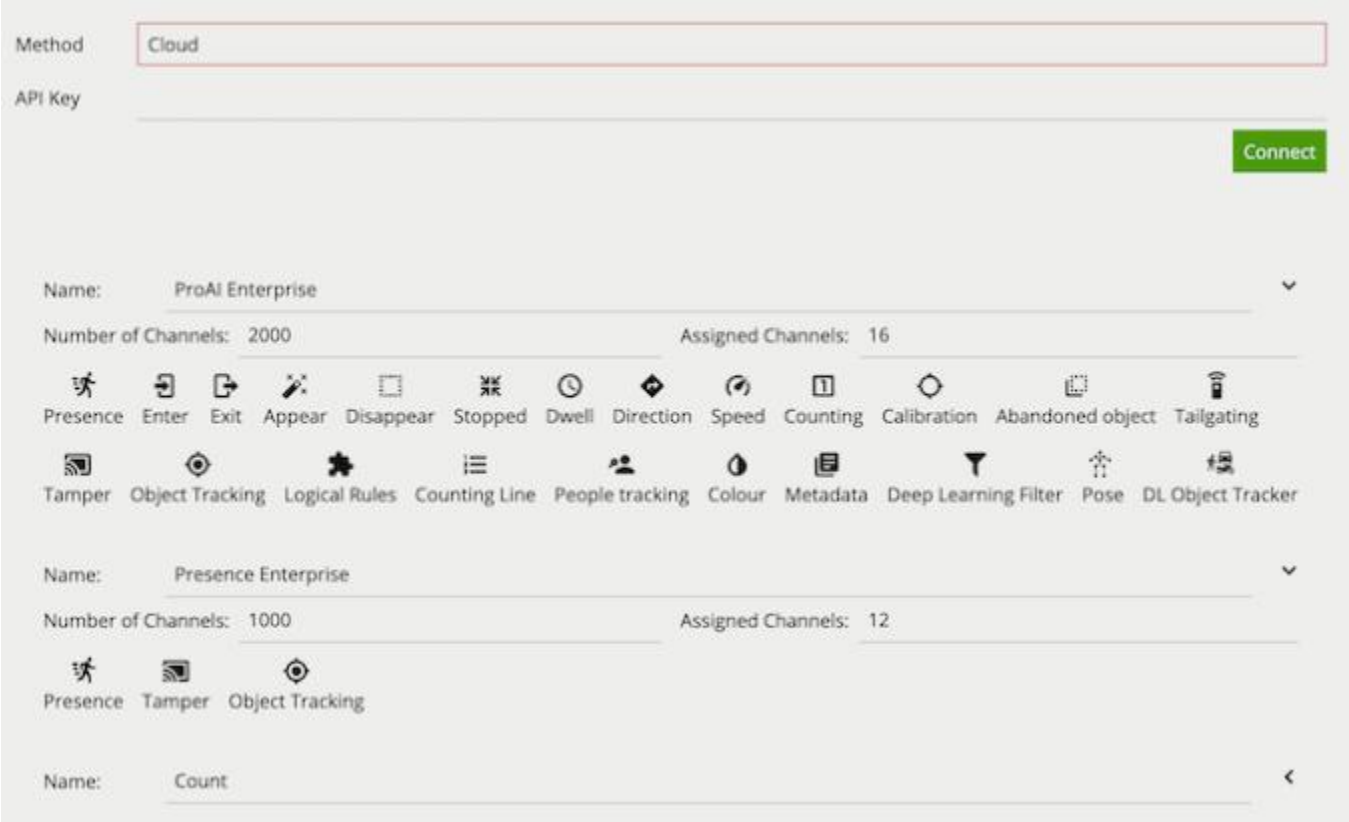


4. When you have to fill License Server address, you can click Connect to this.

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.

8.8 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.

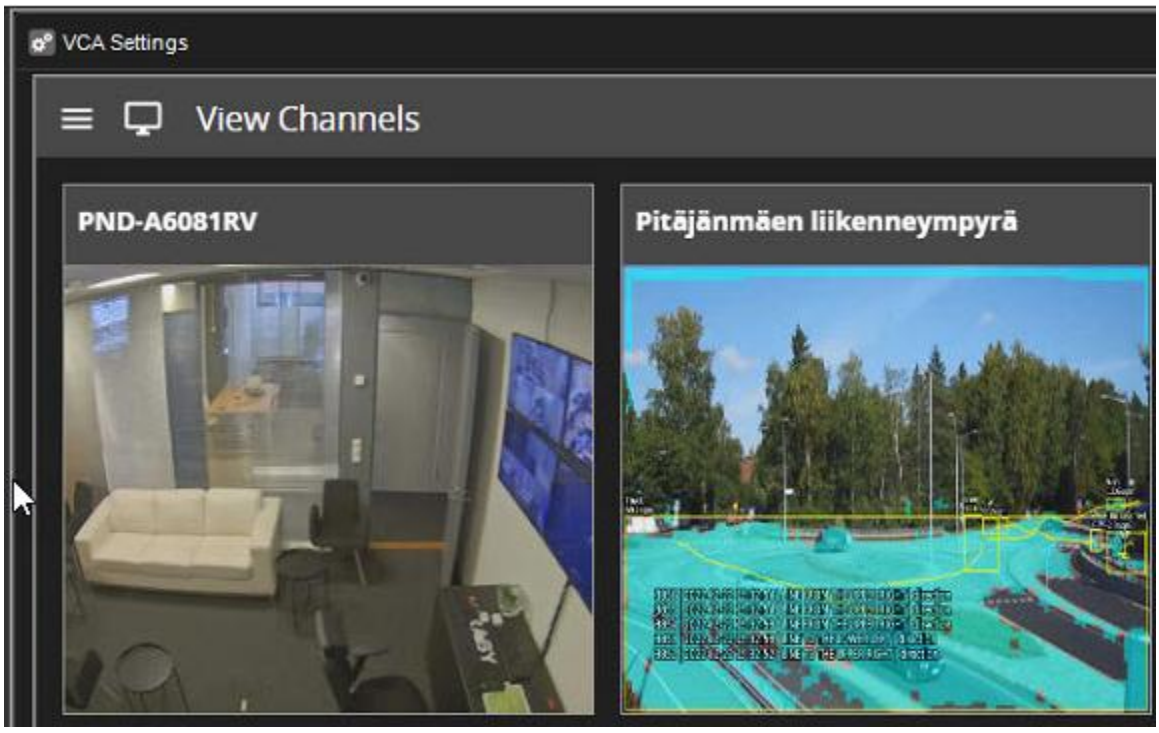
On new installations, before a user is able to add sources, the Cloud Licensing account will need a license added to the license pool.

8.9 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 Initialization

- VCA Trackers
- VCA Zones
- VCA Calibration
- VCA Classification
- VCA Burnt-in Annotation
- VCA Rules
- VCA - Deep-Learning Filter

8.9.1 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.

8.9.2 VCA Trackers

- VCA Object Tracker

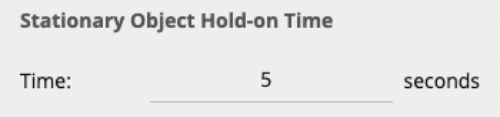
- VCA Deep Learning People Tracker
- VCA Deep Learning Object Tracker
- VCA Deep Learning Skeleton Tracker
- VCA Hand Object Interaction Tracker

8.9.2.1 VCA 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:

8.9.2.1.1 Stationary Object Hold-on Time

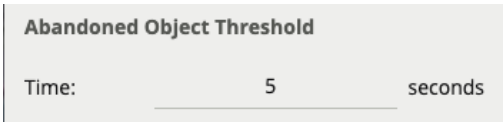
The Stationary Object Hold-on Time defines the amount of time an object will be tracked by the engine once it becomes stationary.
Since objects that become stationary must be "merged" into the scene after some finite time, the tracking engine will forget about objects that have become stationary after the Stationary Object Hold-on Time.



The default setting is 60 seconds.

8.9.2.1.2 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.

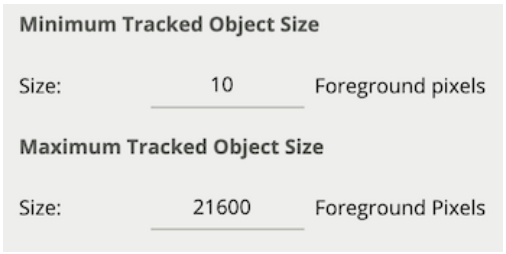


The default setting is 5 seconds.

8.9.2.1.3 Minimum Tracked Object Size

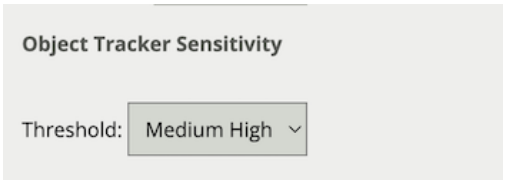
The **Minimum Tracked Object Size** defines the size of the smallest object that will be considered for tracking.

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.



8.9.2.1.4 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.

8.9.2.1.5 Scene Change Detection (Object Tracker)

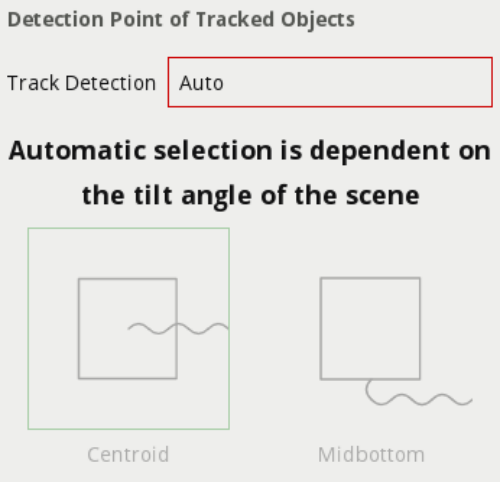
Learn more about Scene Change Detection.

8.9.2.1.6 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:

8.9.2.1.6.1 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.



8.9.2.1.6.2 Centroid

In this mode, the detection point is forced to be the centroid of the object.



8.9.2.1.6.3 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).



8.9.2.1.7 Tamper Detection (Object Tracker)

Learn more about Tamper Detection.

8.9.2.1.8 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

8.9.2.2 VCA Deep Learning People Tracker

The Deep Learning People tracker is designed to track people in situations where the camera's 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:

8.9.2.2.1 Tamper Detection (DLPT)

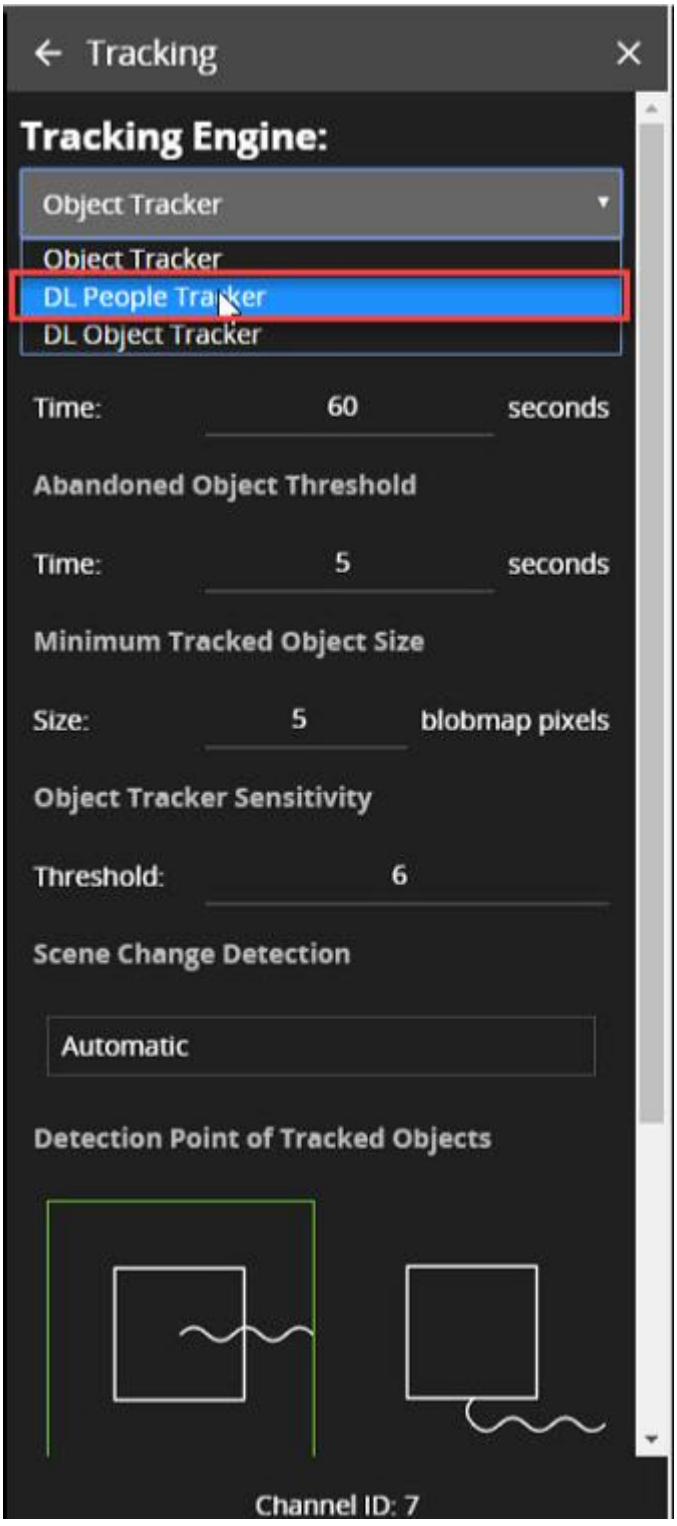
Learn more about Tamper Detection.

8.9.2.2.2 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

8.9.2.2.3 Enabling DL People Tracker

1. Open **View Channels**
2. Select the camera
3. Open **Tracking**
4. Open the **Tracking Engine** dropdown box and select **DL People Tracker**



Tel +358 (0)9 2533 3300 Email info@mirasys.com https://www.mirasys.com

8.9.2.3 VCA 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)

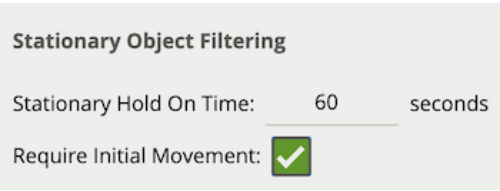
The Deep Learning Object Tracker is based on a classification and detection model, providing the location of an object in the field of view. See Deep Learning Requirements for hardware requirements for this algorithm.

The Deep Learning Object Tracker has the following settings:

8.9.2.3.1 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 that have not moved from being tracked.



8.9.2.3.2 Detection Point of Tracked Objects

See Detection Point of Tracked Objects.

8.9.2.3.3 Tamper Detection (DLOT)

Learn more about Tamper Detection.

8.9.2.3.4 Loss Of Signal Emit Interval

See Loss Of Signal Emit Interval

8.9.2.4 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 for hardware requirements for this algorithm.

The Deep Learning Skeleton Tracker has the following settings:

8.9.2.4.1 Tamper Detection (DLST)

Learn more about Tamper Detection.

8.9.2.5 VCA Hand Object Interaction Tracker

> **The last version to include the Hand Object Interaction Tracker is 9.6.2.** This feature has been removed in later versions.

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

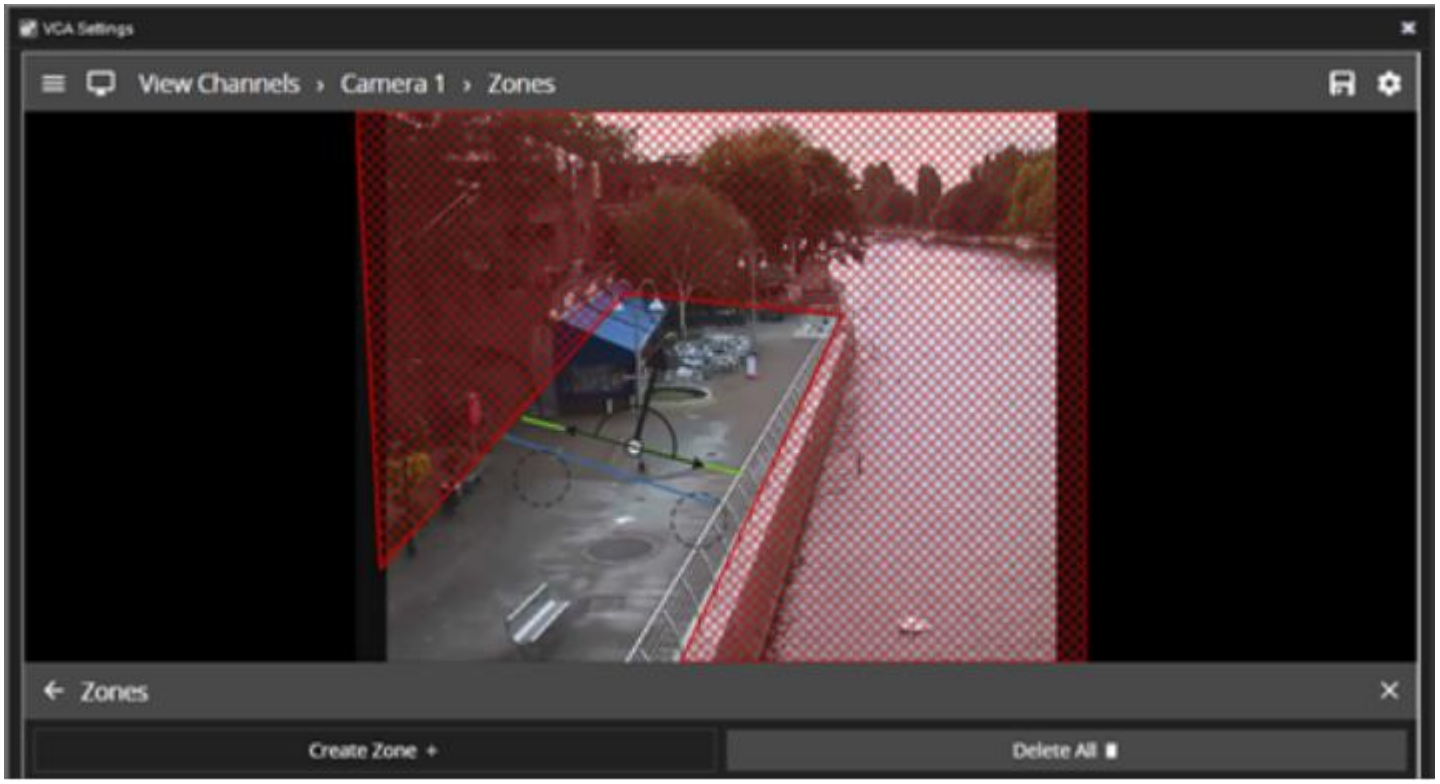
The Hand Object Interaction Tracker is based on a classification and detection model, providing the location of an object in the field of view. See Deep Learning Requirements for hardware requirements for this algorithm.

The Hand Object Interaction Tracker has the following settings:

- Detection Point of Tracked Objects (HOI)
- Tamper Detection (HOI)
- Loss Of Signal Emit Interval (HOI)

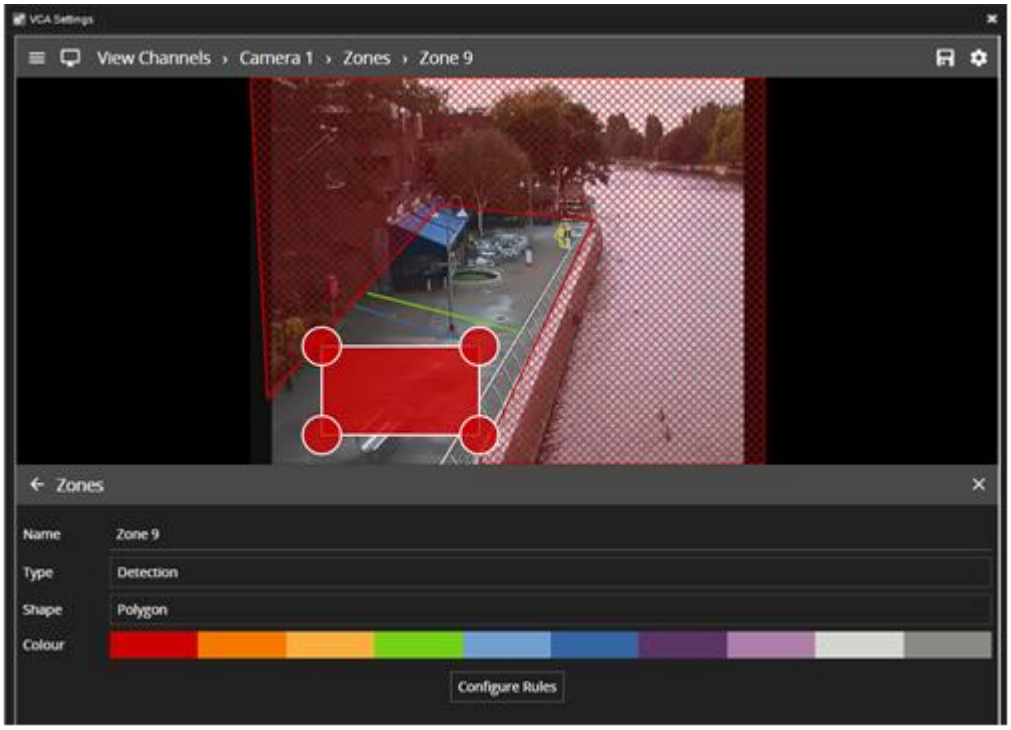
8.9.3 VCA Zones

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.



8.9.3.1 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 rules configuration page

8.9.3.2 Adding a zone

8.9.3.3 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



8.9.3.3.1 The context menu

Right-clicking or tap-holding (on mobile devices) displays a context menu that contains commands specific to the current context.



8.9.3.3.1.1 The possible actions from the context menu are:

 Adds a new zone.

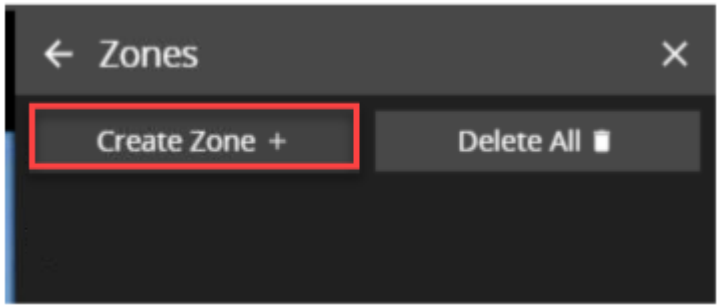
 Deletes an existing zone.

 Adds a node to a zone.

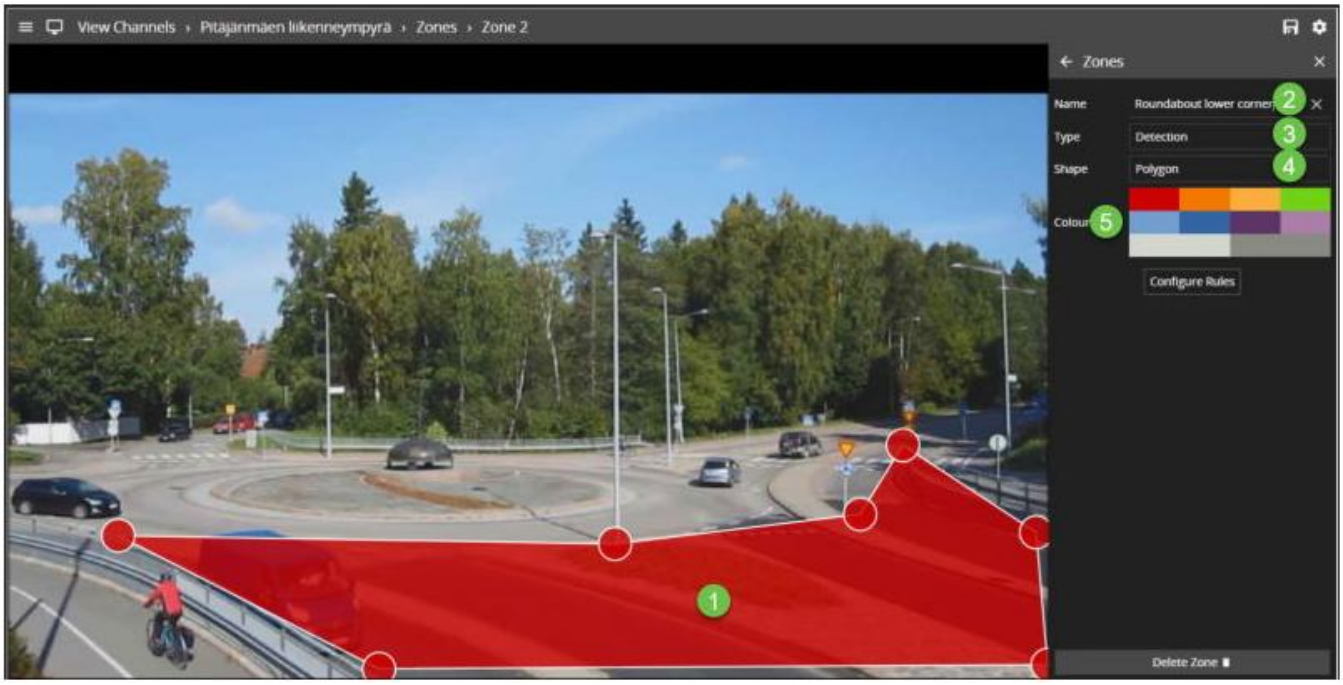
 Deletes an existing node from a zone.

8.9.3.3.2 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



8.9.3.4 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.

8.9.3.5 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

8.9.4 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.

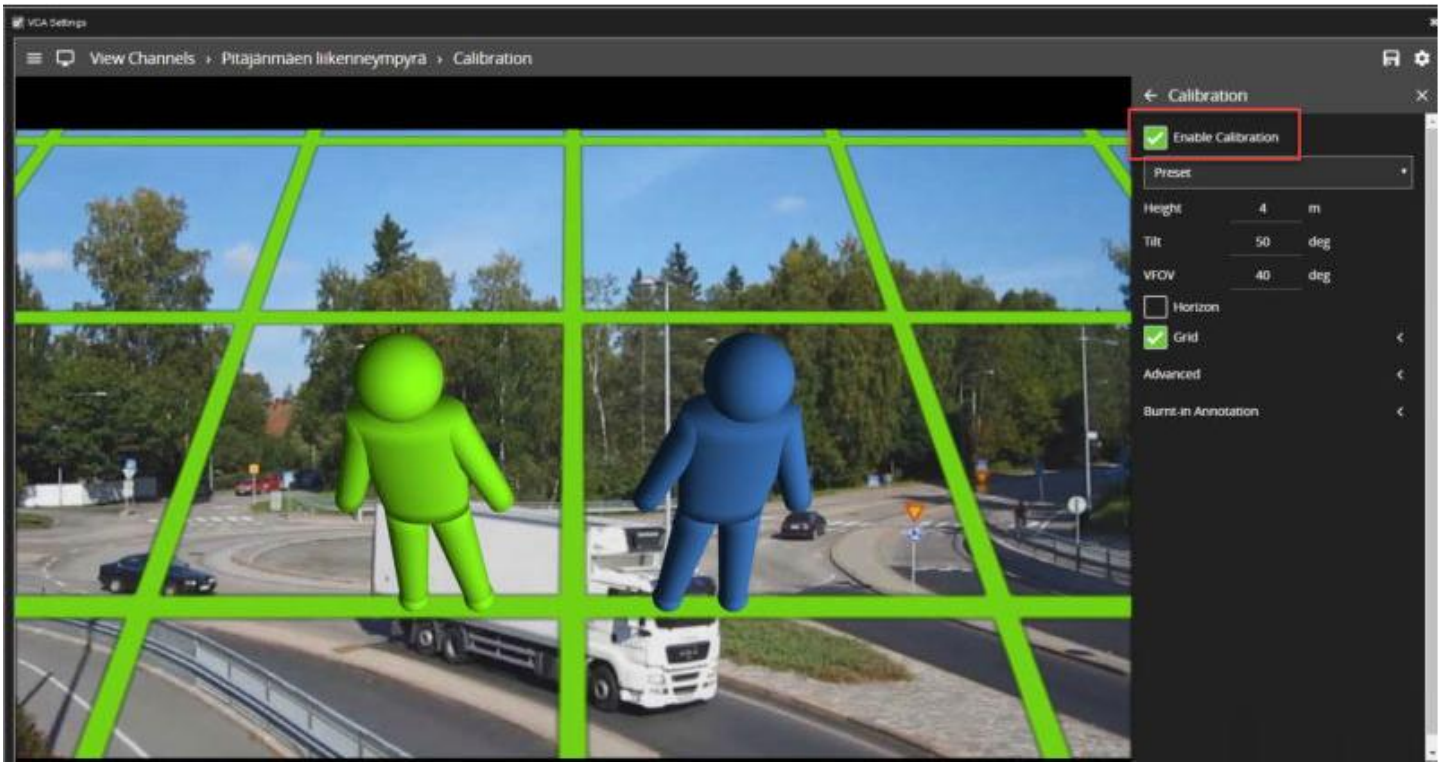
Calibration is not needed to do when using Deep Learning tracking, only when using normal VCA or Deep Learning Filter.

8.9.4.1 Camera calibration is split into the following sub-topics:

1. Enabling Calibration
2. Calibration Controls
3. Calibrating a Channel
4. Advanced Calibration Parameters

8.9.4.2 Enabling Calibration

By default calibration is disabled.
To enable calibration on a channel, check the **Enable Calibration** checkbox.



8.9.4.2.1 Calibration Controls

8.9.4.2.1.1 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.

8.9.4.2.1.2 Mouse Controls

The calibration parameters can be adjusted with the mouse as follows:

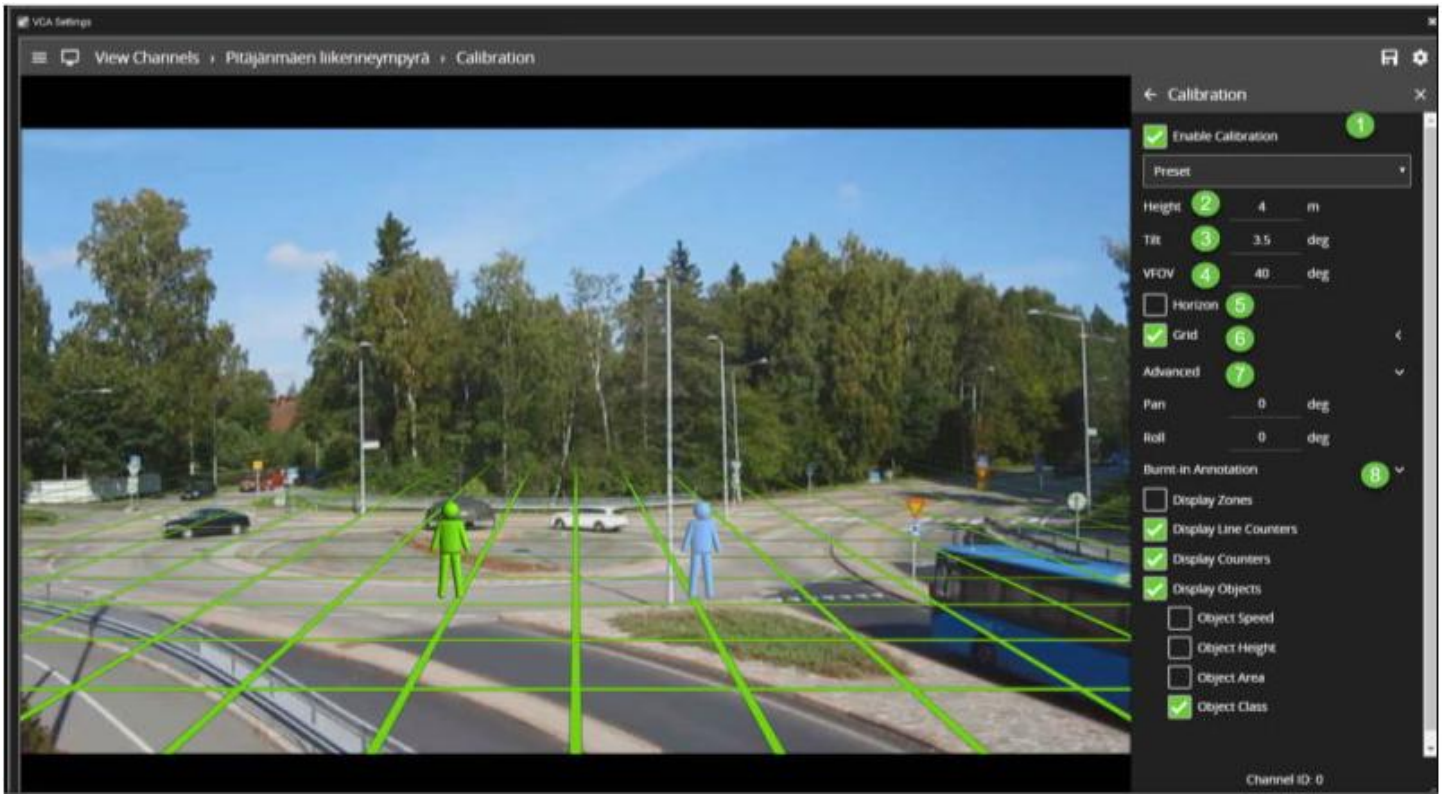
- Click and drag the ground plane to change the camera tilt angle.
- Use the mouse wheel to adjust the camera height. - Drag the slider to change the vertical field of view.

Note: The sliders in the control panel can also be used to adjust the camera tilt angle and height.

8.9.4.2.1.3 Control Panel Items

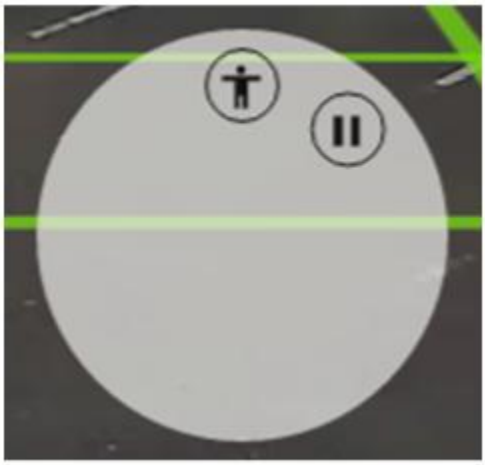
The control panel (shown on the right-hand side in the image above) contains the following controls:

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.

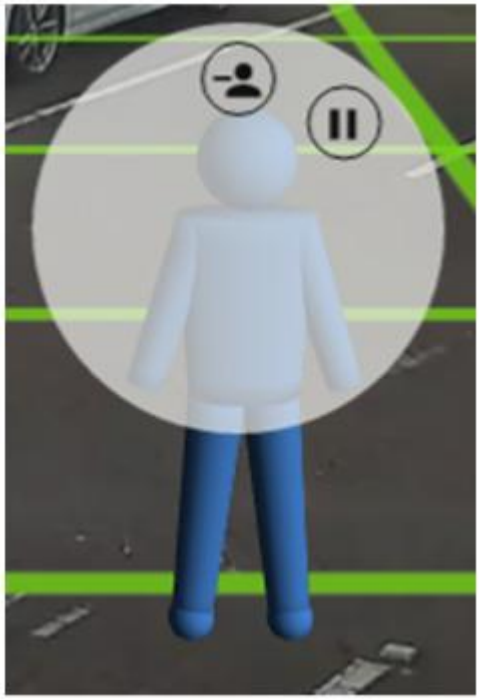


8.9.4.2.1.4 Context Menu Items

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.

8.9.4.3 Calibrating a Channel

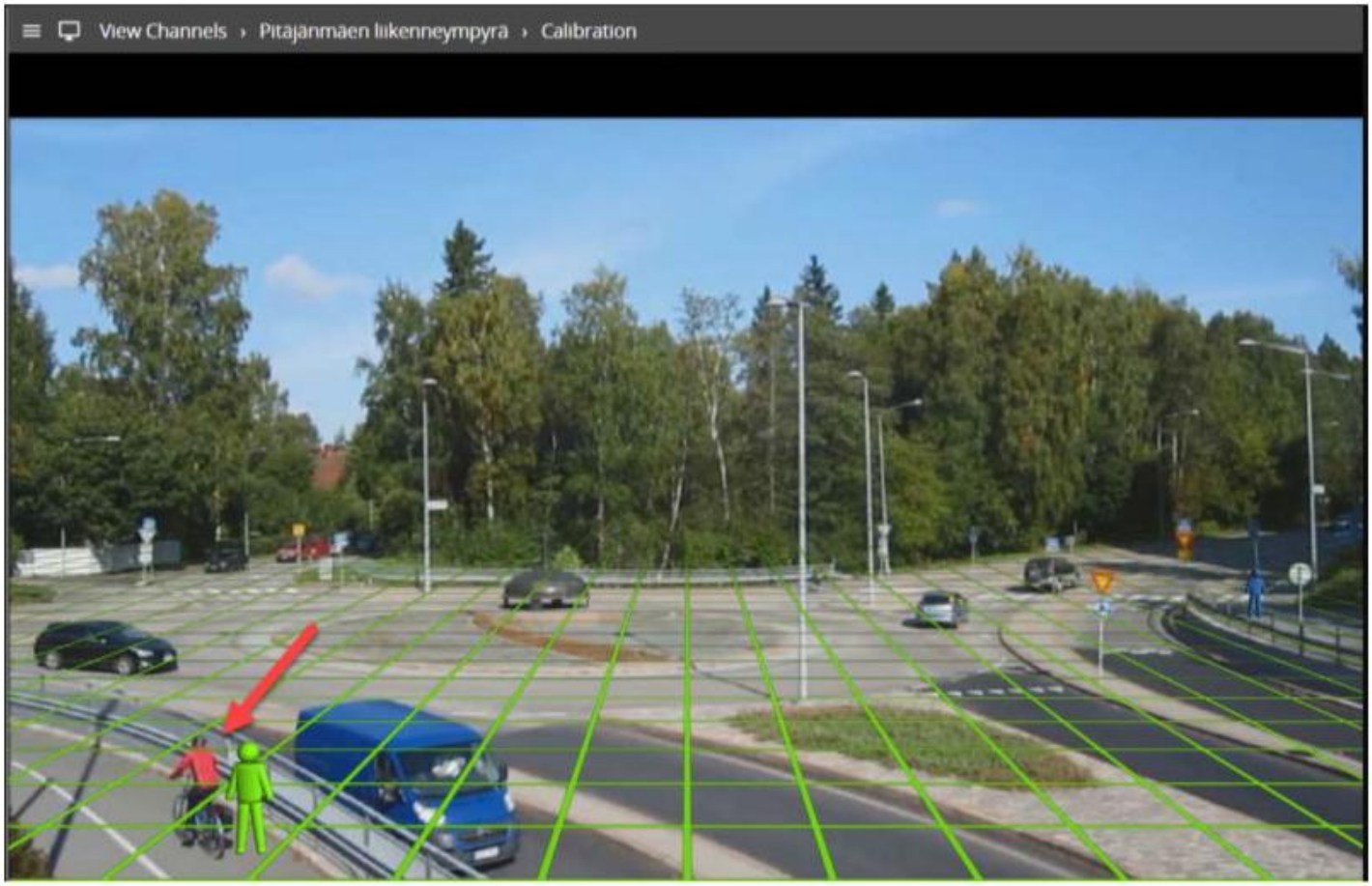
Calibrating a channel is necessary in order to estimate object parameters such as height, area, speed and classification.

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.

8.9.4.3.1 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:



8.9.4.3.2 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.

8.9.4.3.3 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.

8.9.4.3.4 Step 4: Adjust the Tilt Angle and Camera Height

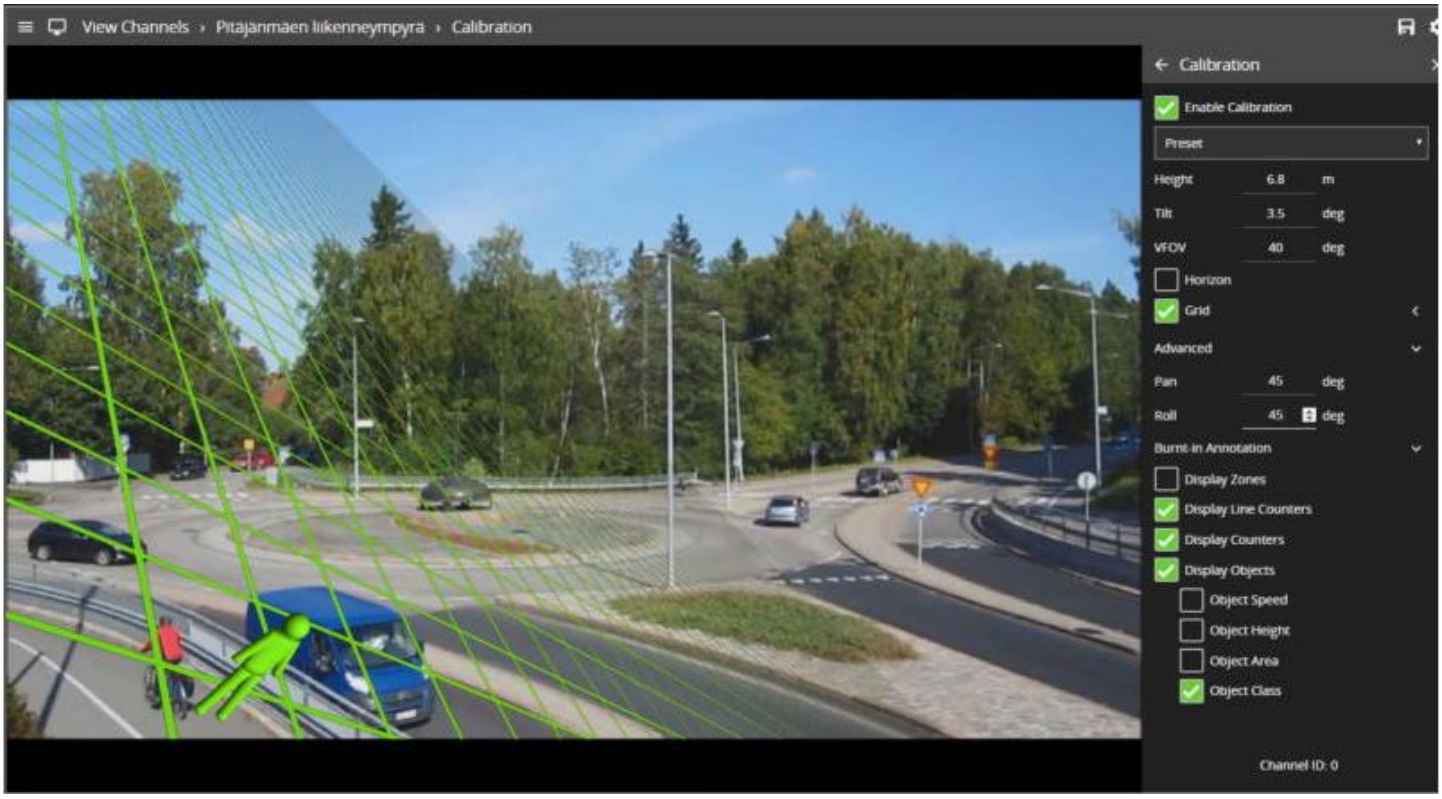
Adjust the camera tilt angle (and height if necessary) until both mimics are approximately the same size as a real person at that position in the scene.
Click and drag the ground plane to change the tilt angle and use the mouse wheel or control panel to adjust the camera height.
The objective is to ensure 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.

8.9.4.3.5 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.

8.9.4.4 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.

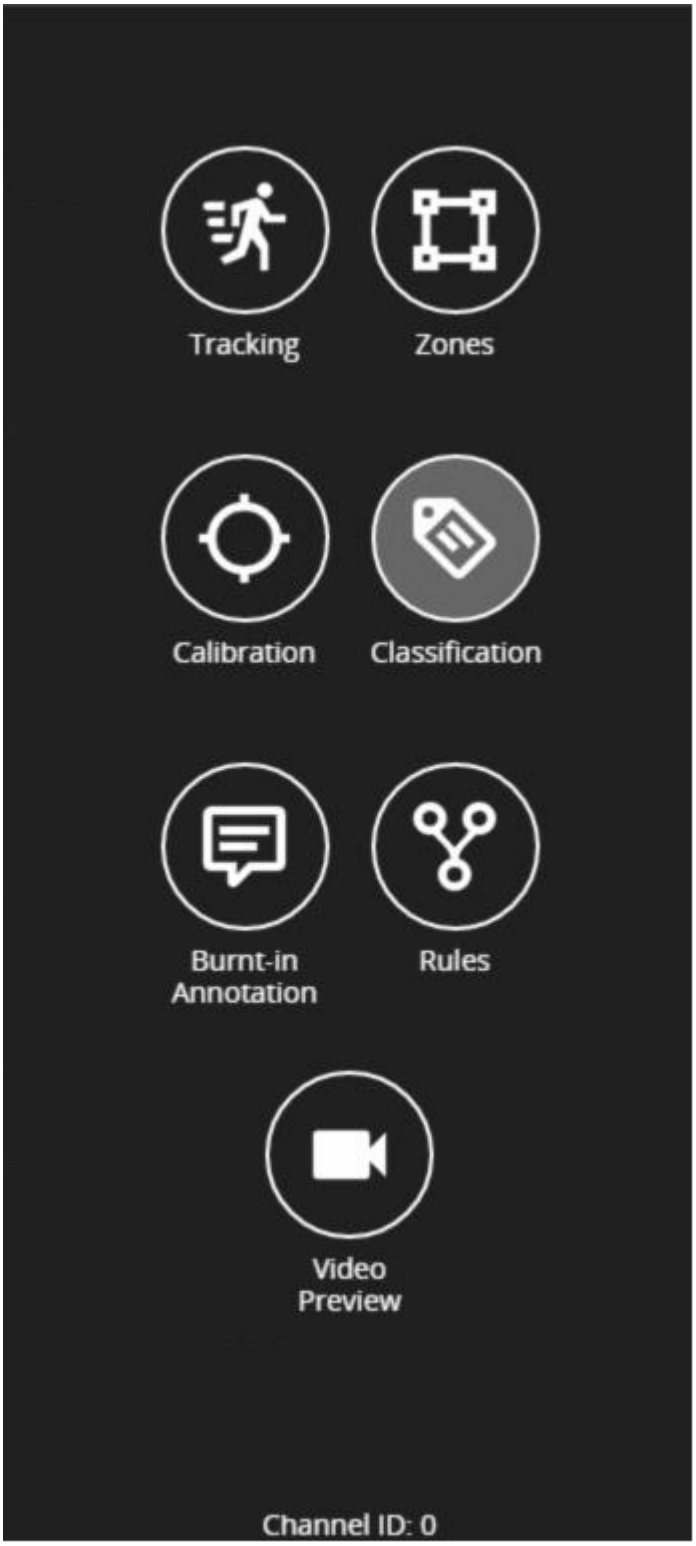
8.9.5 VCA Classification

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.

MIRASYS



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

8.9.5.1 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.

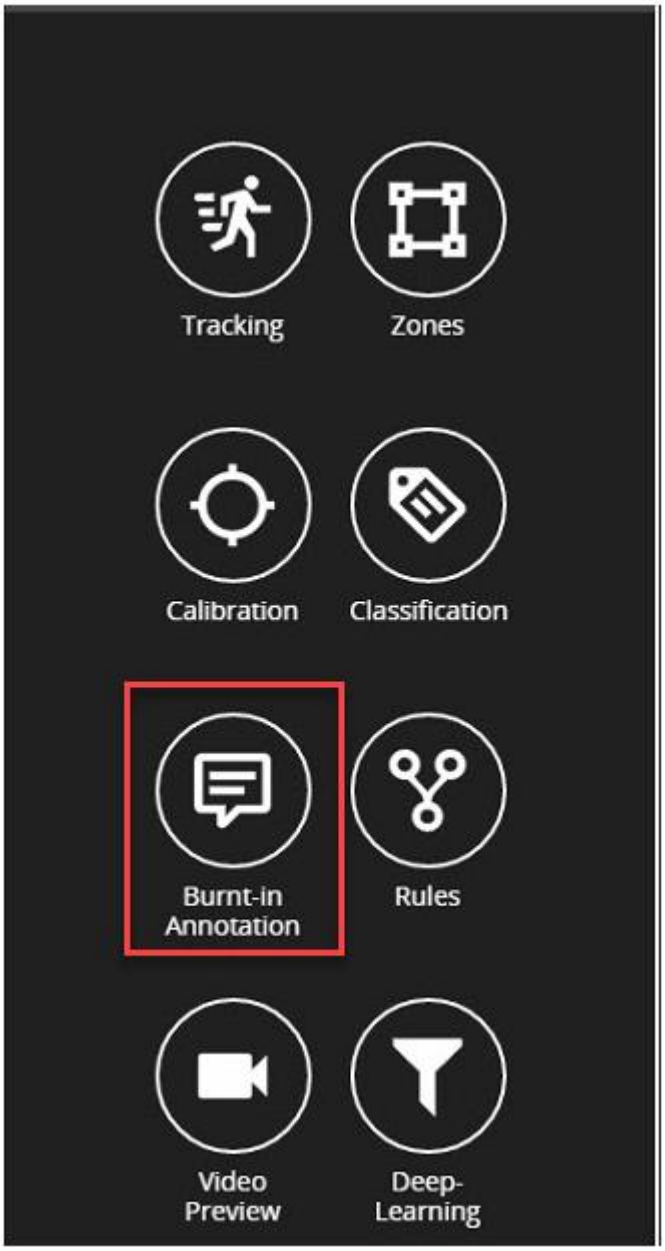
VCAserver's object classification performs classification by comparing these properties to a set of configurable object classifiers.

VCAserver comes pre-loaded with the most common object classifiers, and in most cases these will not need to be modified.

8.9.6 VCA Burnt-in Annotation

Burnt-in Annotations allow VCAserver metadata to be overlaid on to the raw video stream.

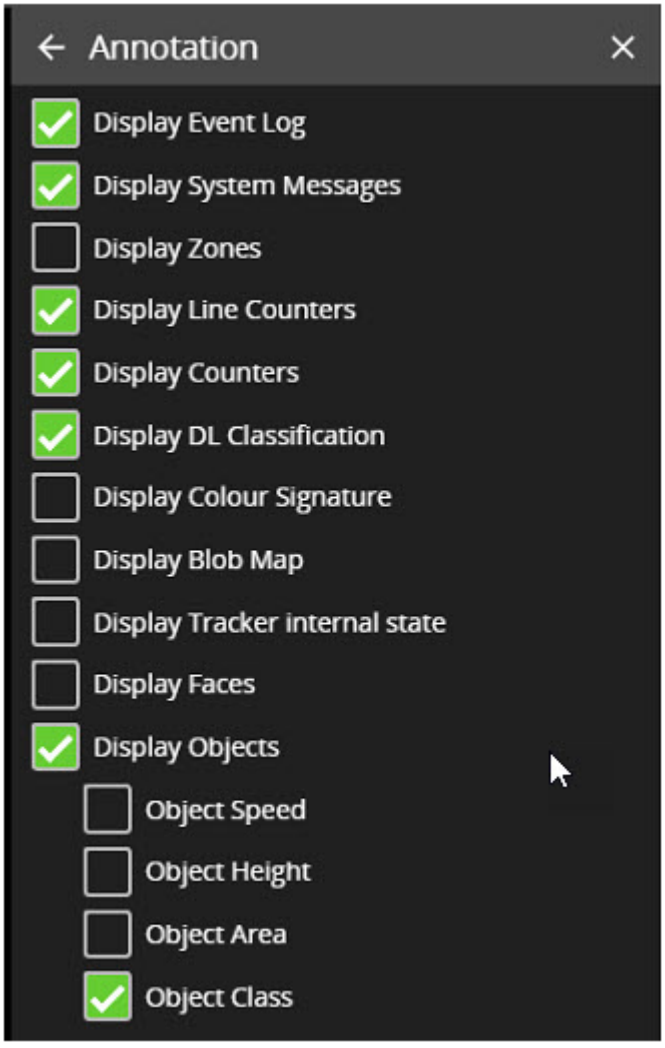
The burnt-in annotation settings control which VCAserver metadata (objects, events, etc) is rendered into the video stream.



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.



8.9.7 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:

8.9.7.1 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.

8.9.7.2 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.

8.9.7.3 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
- VCA - Aggressive Behaviour
- VCA - Abandoned and Removed object
- VCA - Appear and Disappear
- VCA - Enter and exit
- VCA - Direction
- VCA - Directional Crossing
- VCA - Dwell
- VCA - Fall
- VCA - Presence
- VCA - Tailgating
- VCA - Stopped
- VCA - Line Counter
- VCA - Conditional rules
- VCA - Counters
- VCA - Object trails
- VCA - Object display

8.9.7.4 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.

8.9.7.5 VCA - Aggressive Behaviour

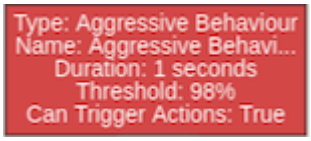
A rule which fires when aggressive behaviour is detected in the field of view for longer than the specified duration.

> 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.



8.9.7.5.1 Graphical View



8.9.7.5.2 Form View



8.9.7.5.3 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

8.9.7.6 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.

MIRASYS



Tel +358 (0)9 2533 3300

Email info@mirasys.com

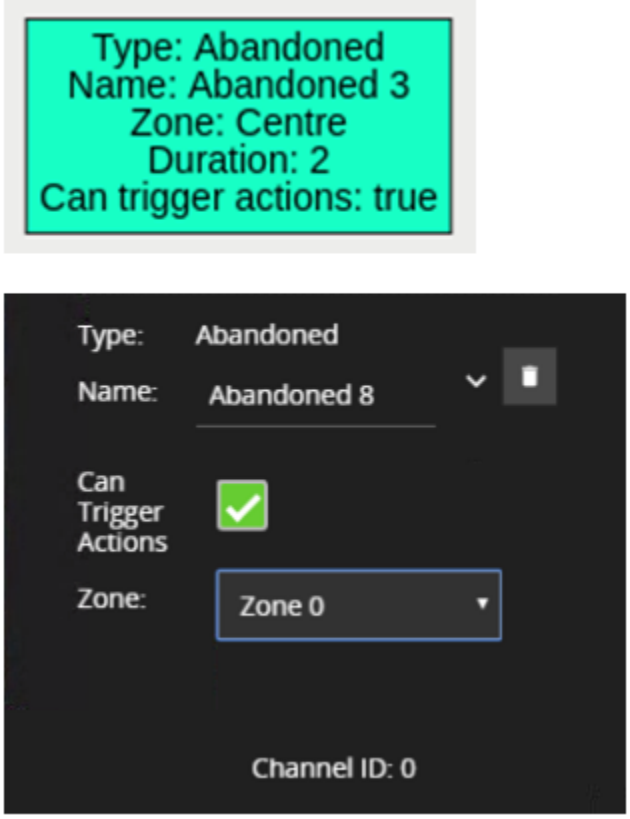
https://www.mirasys.com

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.

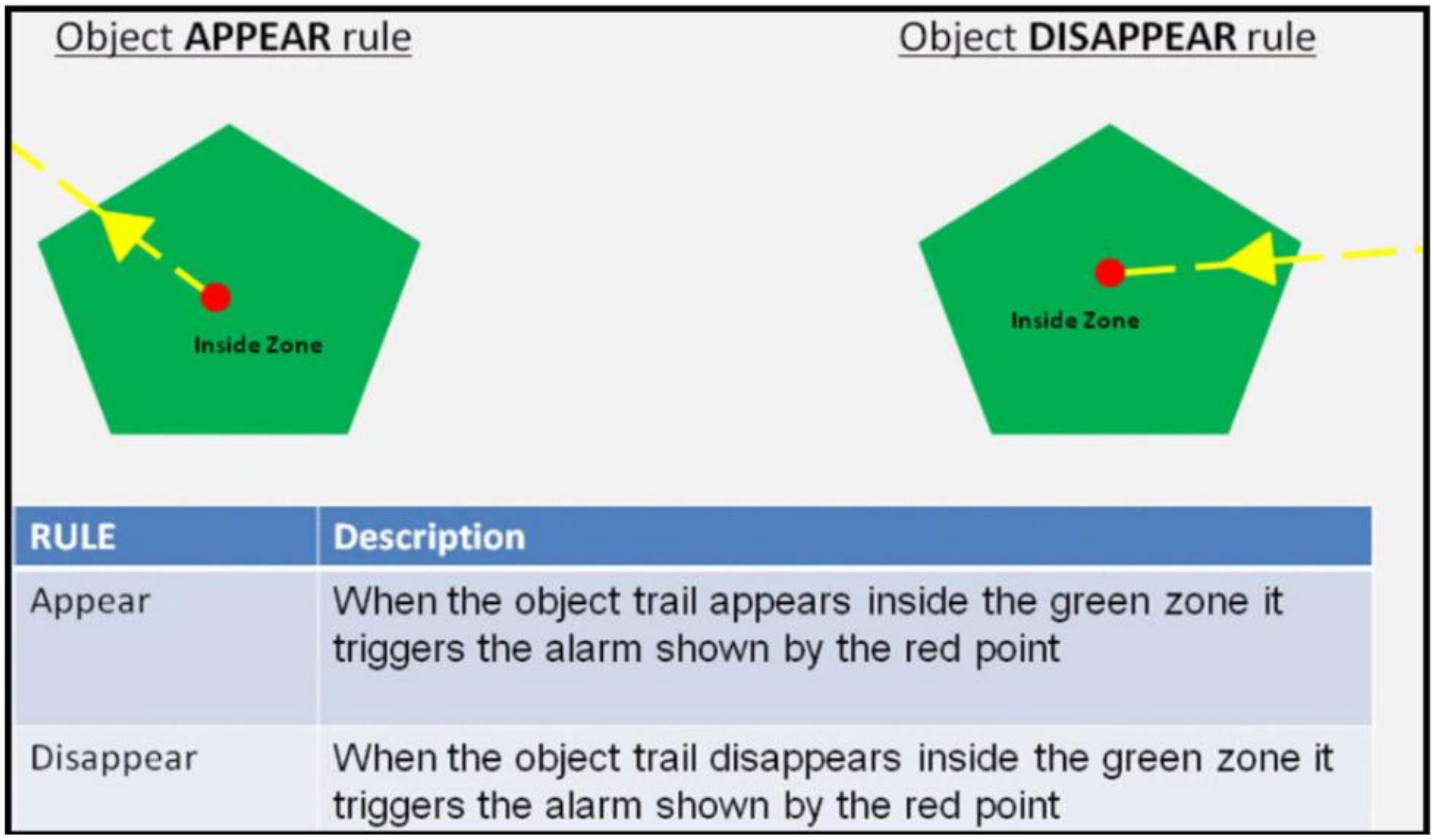


Property	Description	Default Value
Name	A user-specified name for this rule	"Abandoned #"
Zone	The zone this rule is associated with	None
Duration	Period of time an object must have been abandoned or removed before the rule triggers	0
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active

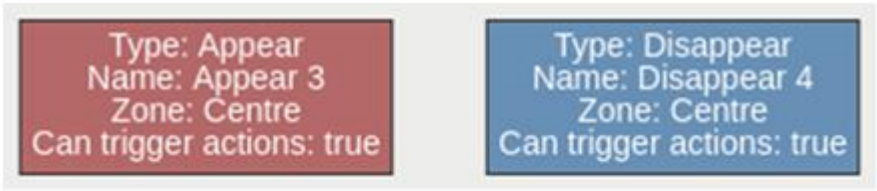
8.9.7.7 VCA - Appear and Disappear

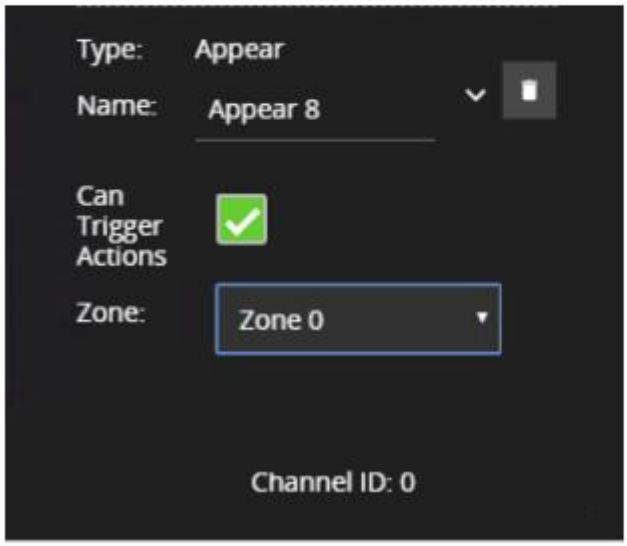
The appear rule detects objects that start being tracked within a zone, e.g. a person who appears in the scene from a doorway.

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





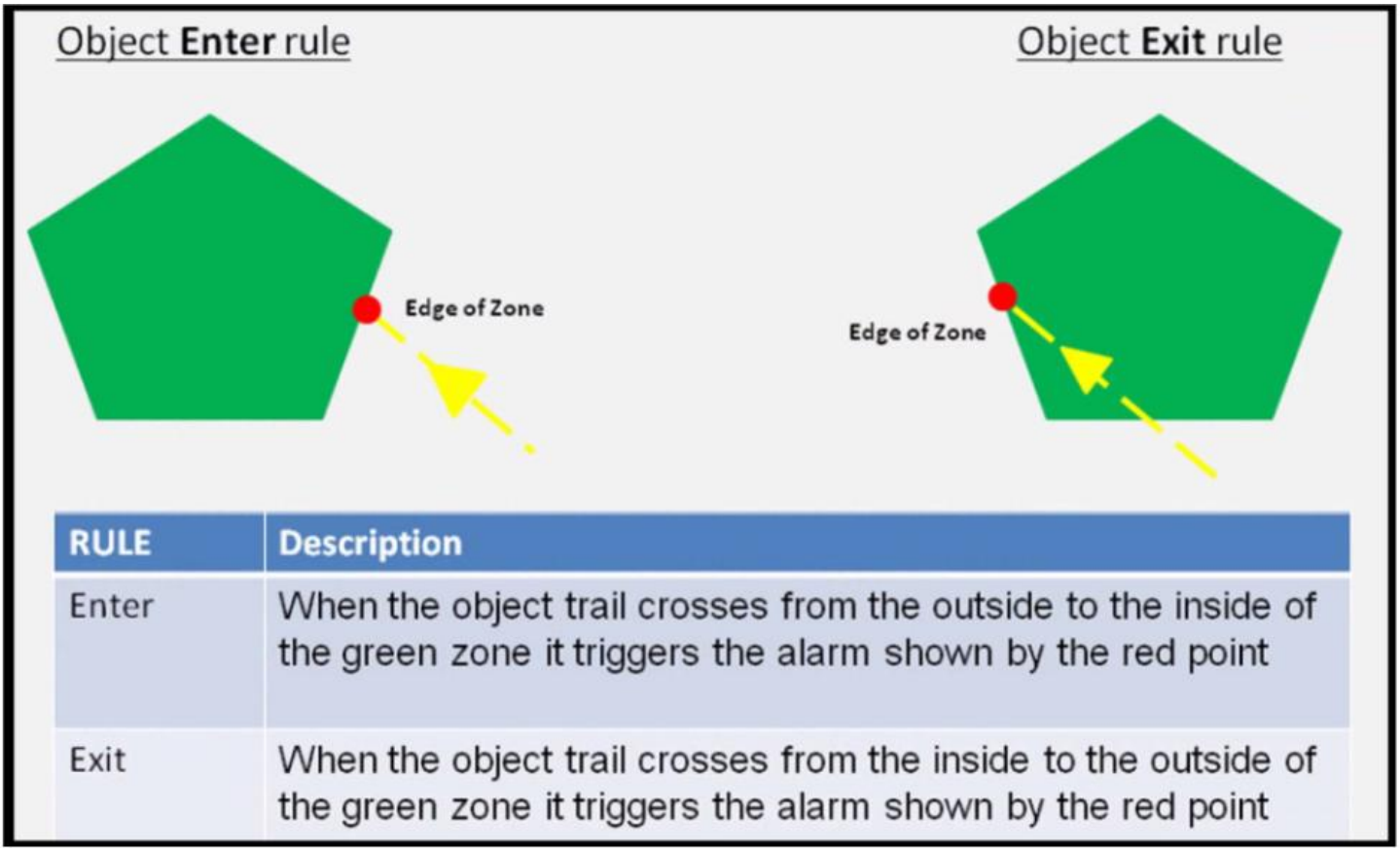
8.9.7.7.1 Configuration Appear

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

8.9.7.7.2 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

8.9.7.8 VCA - Enter and exit

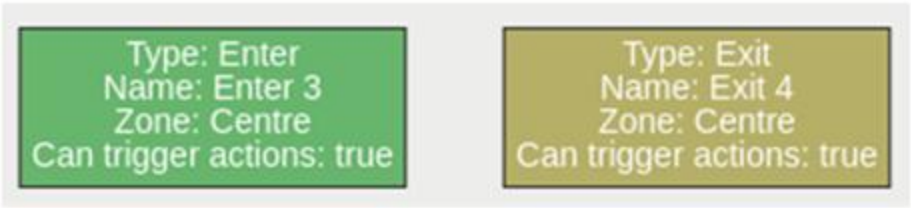


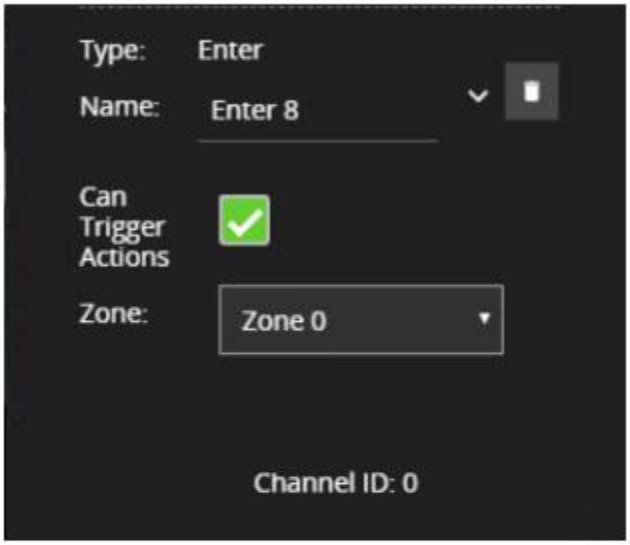
RULE	Description
Enter	When the object trail crosses from the outside to the inside of the green zone it triggers the alarm shown by the red point
Exit	When the object trail crosses from the inside to the outside of the green zone it triggers the alarm shown by the red point

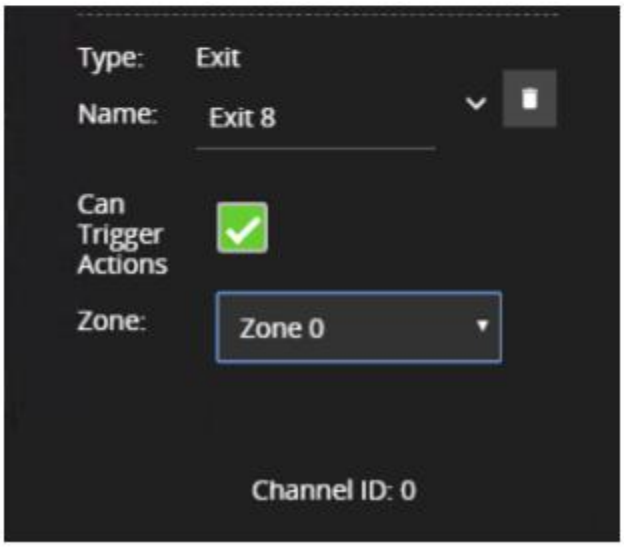
The enter rule detects when objects enter a zone.
In other words, when objects cross from the outside of a zone to the inside of a zone.
Conversely, the exit rule detects when an object leaves a zone: when it crosses the border of a zone from the inside to the outside.

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).







8.9.7.8.1 Configuration Enter

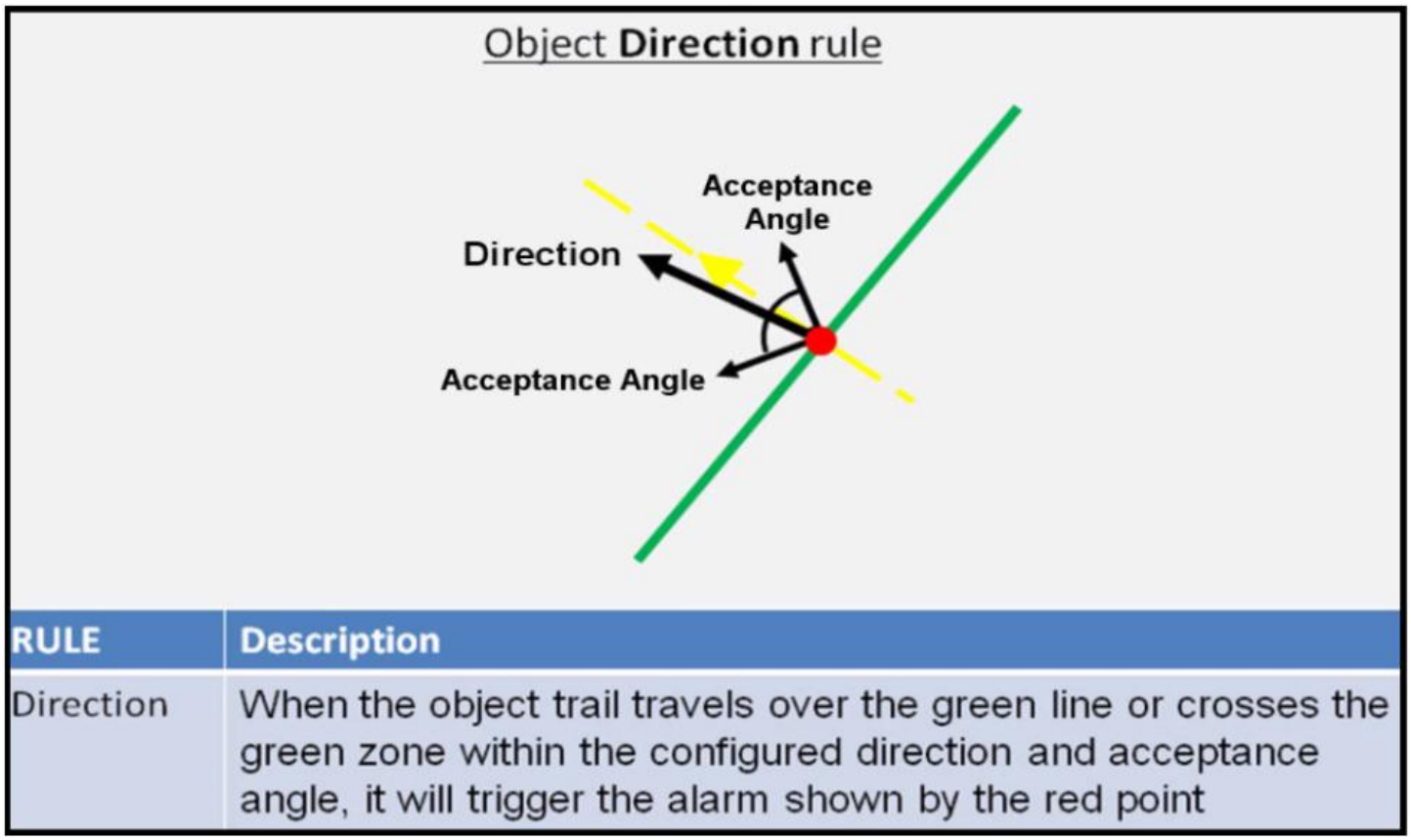
Property	Description	Default Value

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

8.9.7.8.2 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

8.9.7.9 VCA - Direction

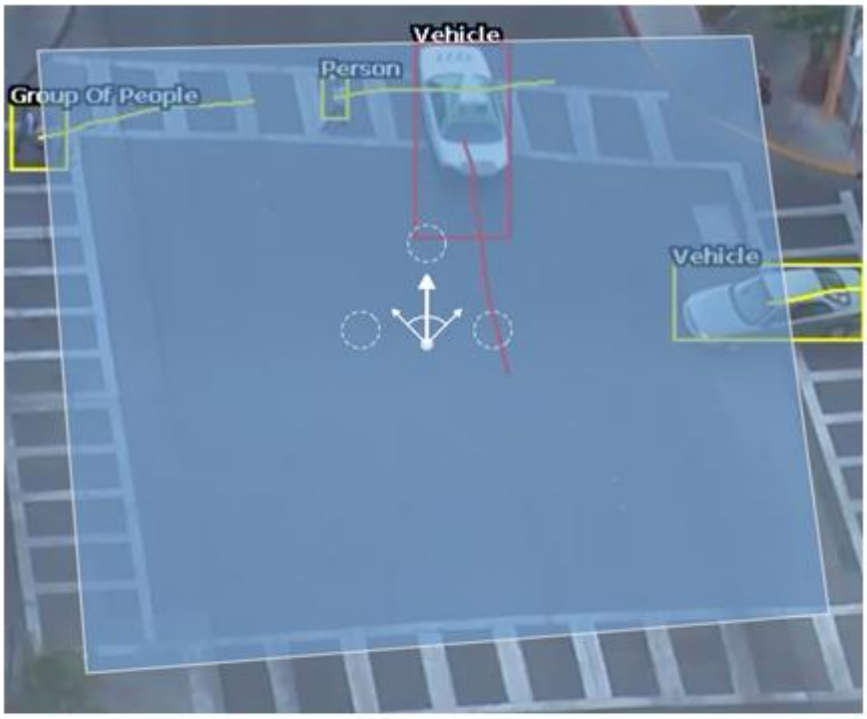


RULE	Description
Direction	When the object trail travels over the green line or crosses the green zone within the configured direction and acceptance angle, it will trigger the alarm shown by the red point

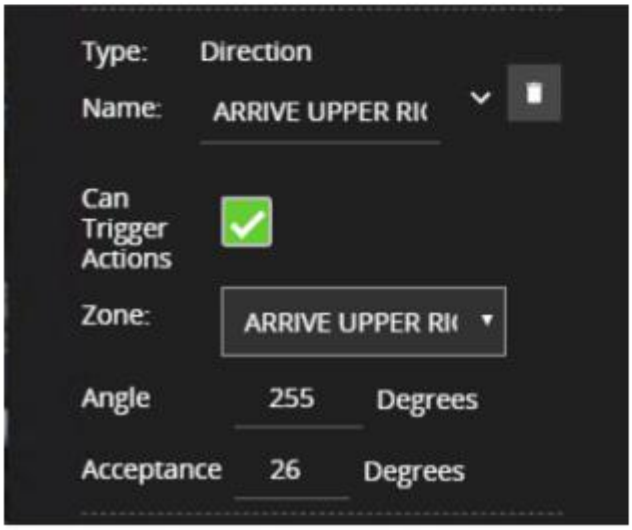
The direction rule detects objects moving in a specific direction.
Configure the direction and acceptance angle by moving the arrows on the direction control widget.
The primary direction is indicated by the large central arrow.
The acceptance angle is the angle between the two smaller arrows.

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.

MIRASYS



Type: Direction
Name: Direction 3
Zone: Centre
Angle: 358
Angle Threshold: 27
Can trigger actions: true



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

8.9.7.9.1 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

8.9.7.10 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.



8.9.7.10.1 Graphical View

Type: Directional Crossing
Name: Car
Zone: Centre
Angle: 348
Acceptance: 21
Filters: car
Confidence Threshold: 70%
Can Trigger Actions: True

8.9.7.10.2 Form View



8.9.7.10.3 Configuration

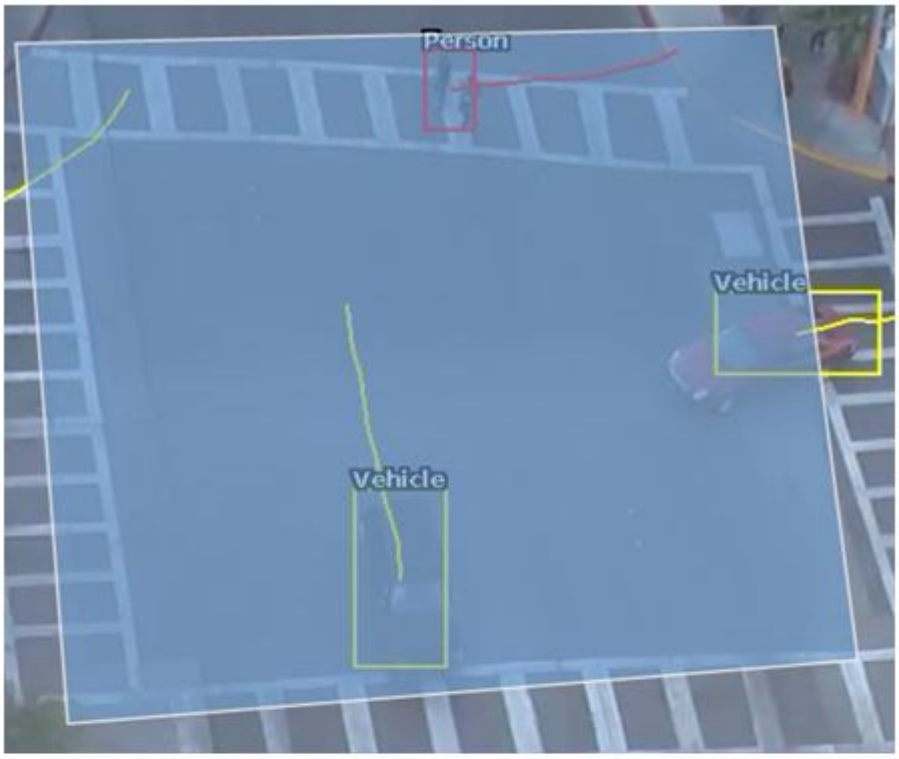
Property	Description	Default Value
Name	A user-specified name for this rule	“Directional #”
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Zone	The zone this rule is associated with	None

Property	Description	Default Value
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

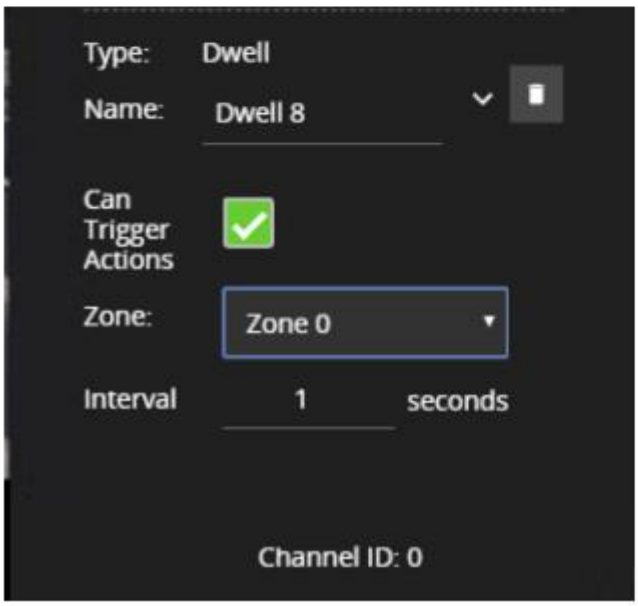
8.9.7.11 VCA - Dwell

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.

MIRASYS



Type: Dwell
Name: Dwell 1
Zone: Centre
Interval: 1000
Can trigger actions: true



Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

8.9.7.11.1 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

8.9.7.12 VCA - Fall

The fall rule detects when a object classified as a Person, by the Deep Learning People Tracker, is in the fallen state.

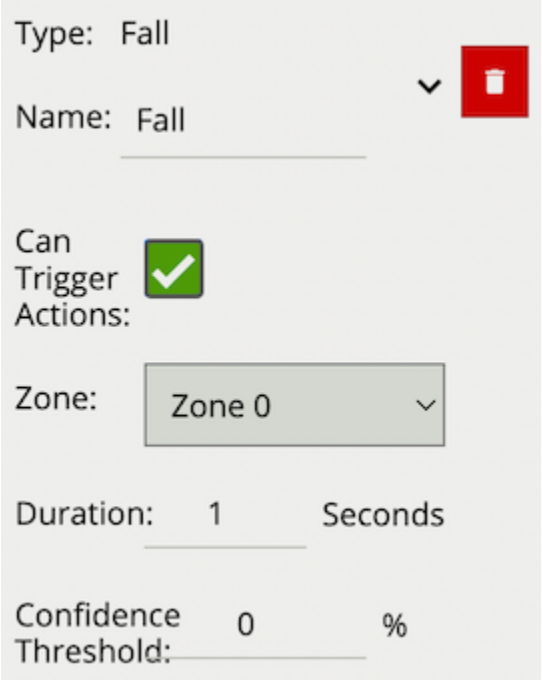
When the Fall rule is added to a channel configuration, the fall detection algorithm begins to run in the background which will have a GPU overhead. Currently this rule is only available when using the Deep Learning People Tracker.



8.9.7.12.1 Graphical View



8.9.7.12.2 Form View



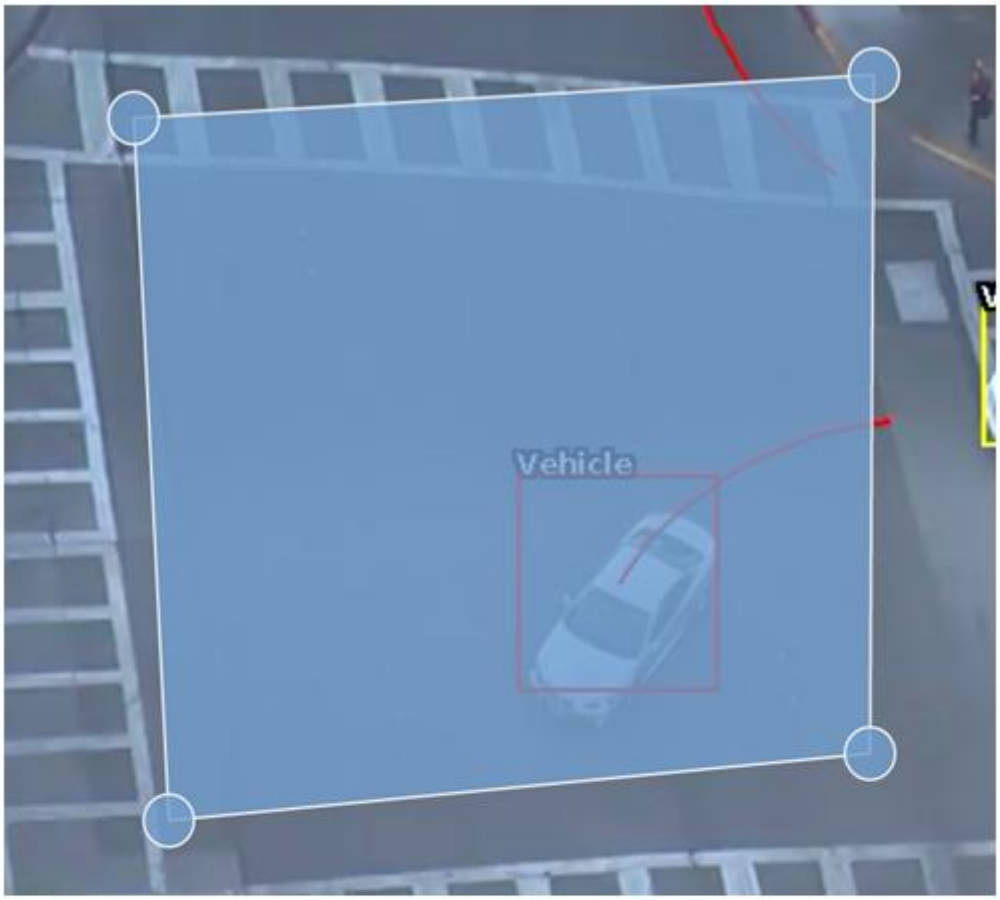
8.9.7.12.3 Configuration

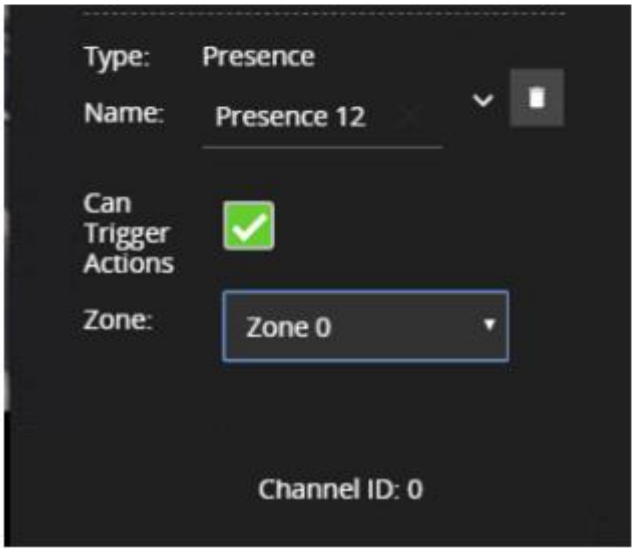
Property	Description	Default Value
Name	A user-specified name for this rule	"Fall #"
Zone	The zone this rule is associated with	None
Duration	Period of time a object must have been fallen before the rule triggers	1 to 60 seconds
Confidence Threshold	The algorithm confidence (as a percentage) required to trigger the rule	0
Can Trigger Actions	The algorithm confidence (as a percentage) required to trigger the rule	Active

8.9.7.13 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.

MIRASYS





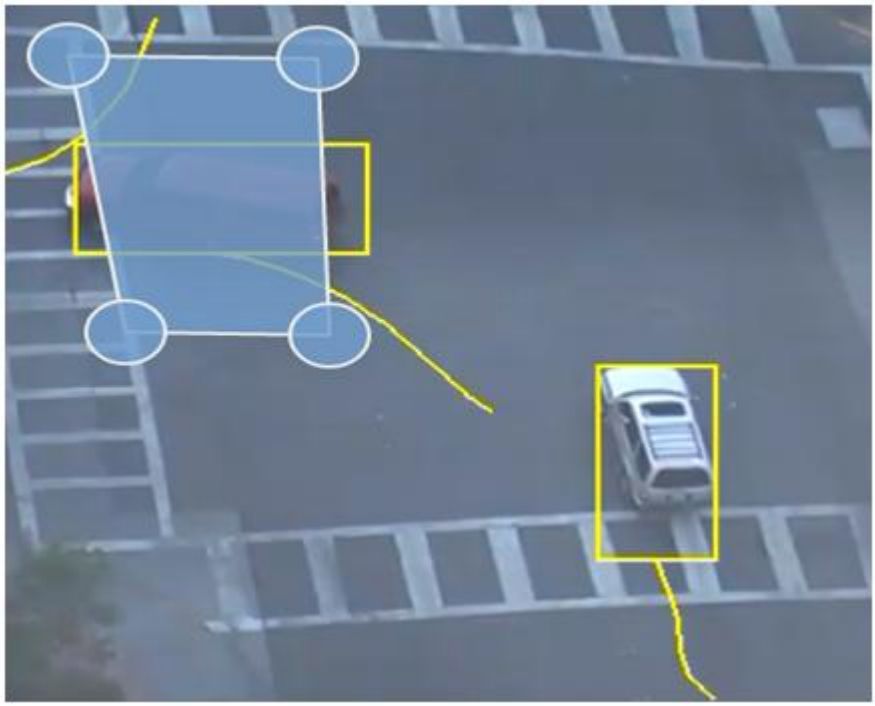
Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

8.9.7.13.1 Configuration Presence

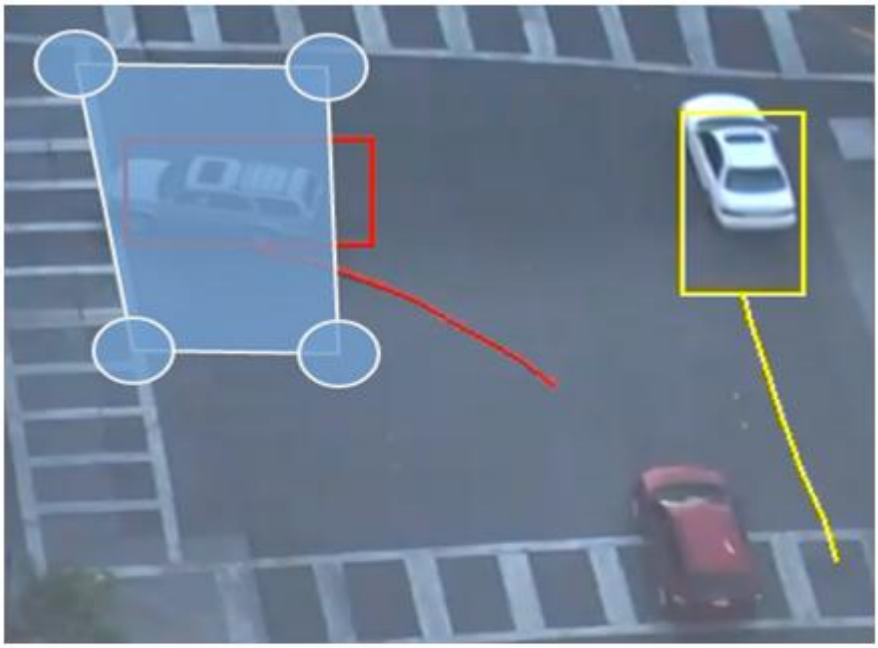
Property	Description	Default Value
Name	A user-specified name for this rule	"Deep Learning Presence #"
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Zone	The zone this rule is associated with	None

8.9.7.14 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.



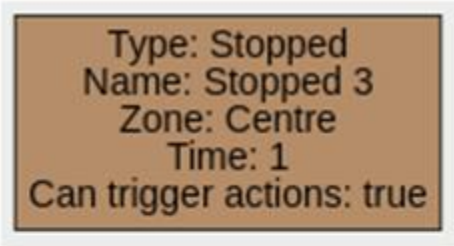


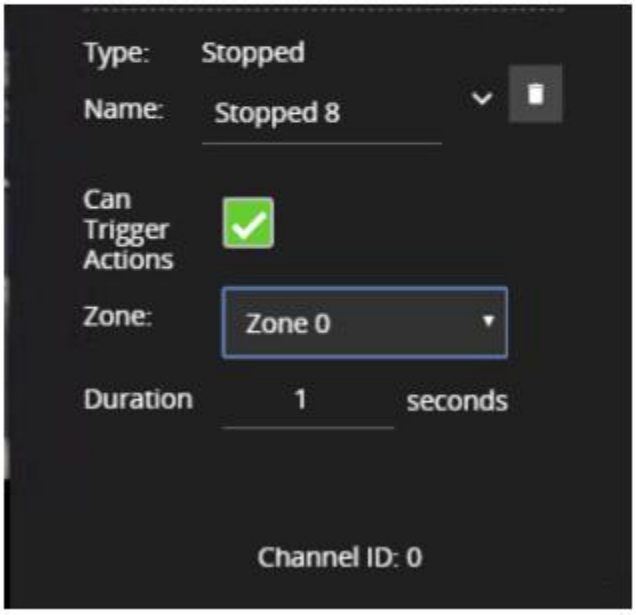
Property	Description	Default Value
Name	A user-specified name for this rule	"Tailgating #"
Zone	The zone this rule is associated with	None
Duration	The maximum amount of time between first and second object entering a zone to trigger the rule	0
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active

8.9.7.15 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.





8.9.7.15.1 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

8.9.7.16 VCA - Line Counter

The last version to include the Line Counter rule is 9.6.2. In place of the Line Counter, it is recommended to use the Direction and Directional Crossing rules with Counters, as these options provide greater flexibility and compatibility with trackers.

A line counter 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.

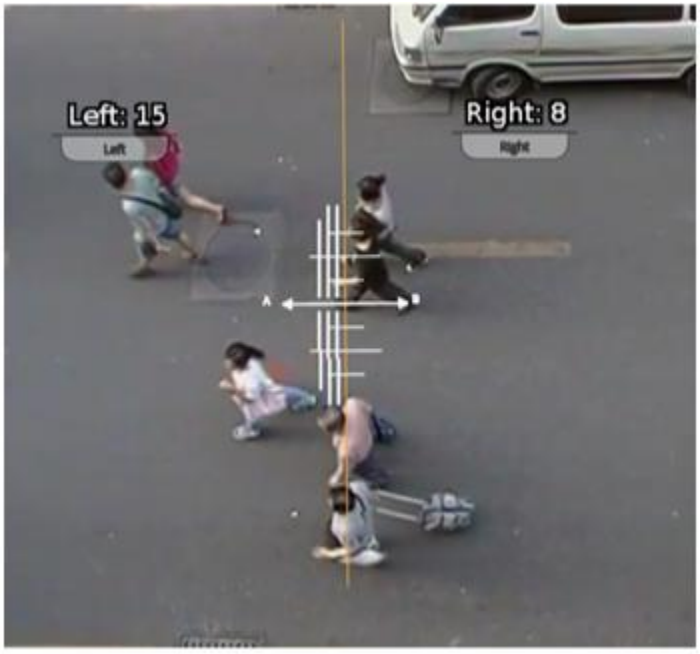
In some scenes, such as entrances with cameras installed overhead, the line counter typically will generate a higher accuracy count than using the aforementioned counters connected to a presence rule.

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.
Line Counters are attached to zones configured with a Line shape.
See **Zones** for more information.

If a Line Counter 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 Line Counter stops referencing the zone in question).

Line Counters 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 Line Counter rule must be added to the same zone with the opposite direction selected.
An example rule graph of a two-way Line Counter configured with a counter is provided to illustrate this below.

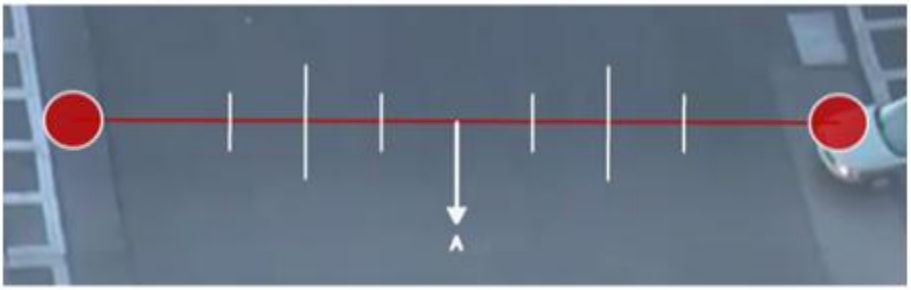
NOTE: The maximum number of Line Counter filters that can be applied per video channel is 5.



8.9.7.16.1 Calibrating the Line Counter

In order to generate accurate counts, the Line Counter 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 Line Counter is not always placed on the ground plane; it may be placed at any orientation at any location in the scene.

For example, a Line Counter could be configured vertically with a side-on camera view.
Instead of the 3D calibration tool, the Line Counter has its own calibration setting.
Two bars equidistant from the center of the line represent the width of the expected object. This allows the Line Counter to reject noise and also count multiple objects.



8.9.7.16.1.1 To calibrate the Line Counter:

1. Select the Line Counter rule.
2. Check the Enable width calibration option.

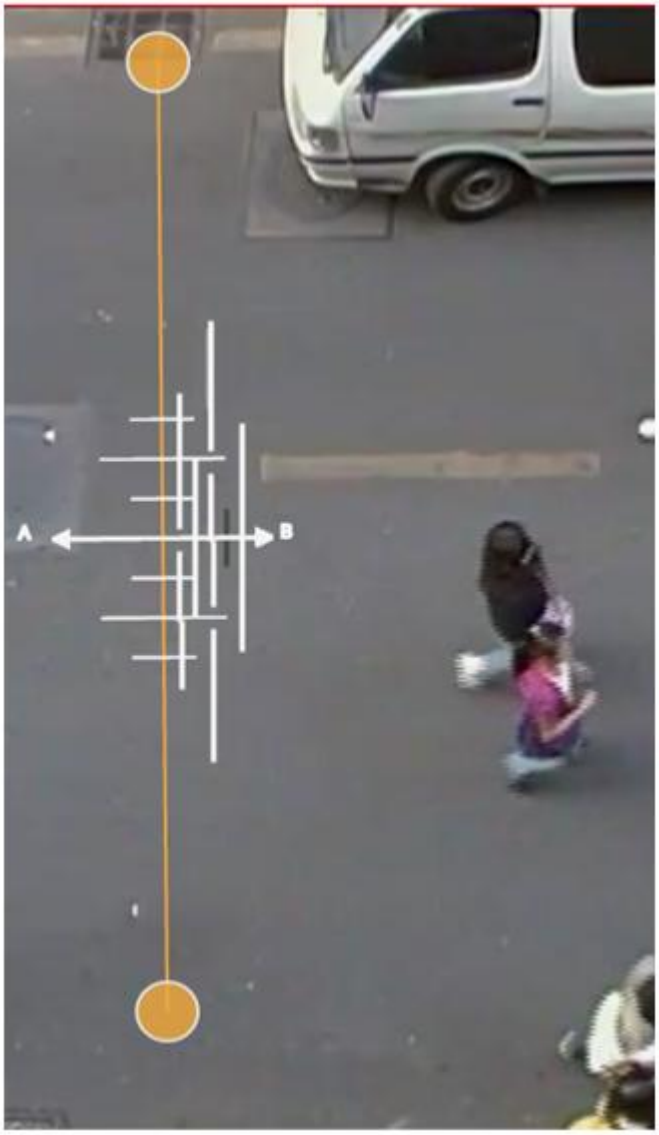
3. Drag the calibration markers to adjust the distance between the calibration markers until the distance is approximately the size of the objects to be counted. Alternatively, move the Width slider to achieve the same result.
4. The calibration width is displayed within the Line Counter rule and can 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.

8.9.7.16.1.2 Line Counter Calibration Feedback

To enable the user to more accurately configure the calibration for the Line Counter, the widths of detected objects are displayed as an overlay next to the Line Counter 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 Line Counter 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 Line Counter



8.9.7.16.2 Shadow Filter

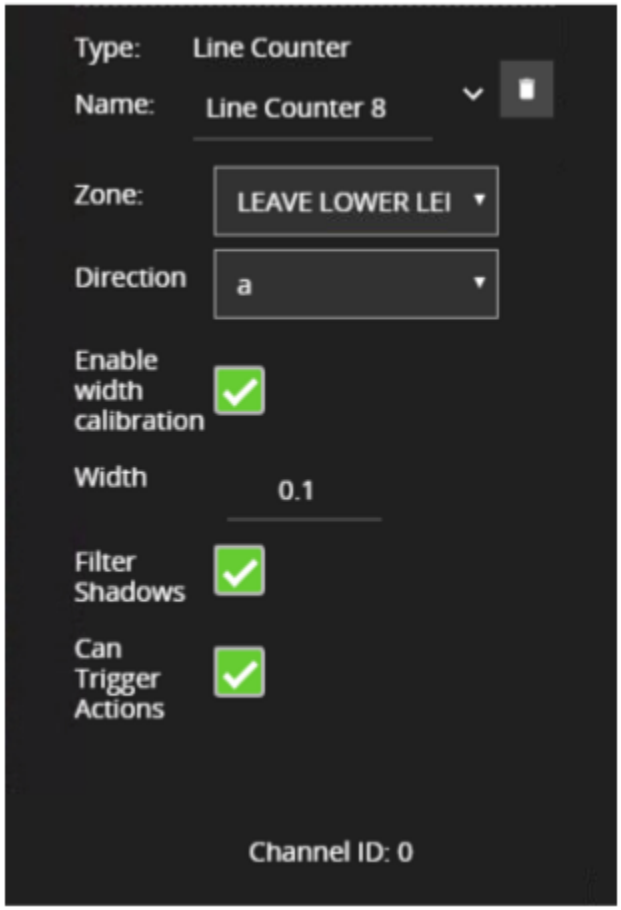
The Line Counter features a shadow filter which is designed to remove the effects of object shadows affecting the counting algorithm.

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 Line Counter)	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

8.9.7.17 VCA - Conditional rules

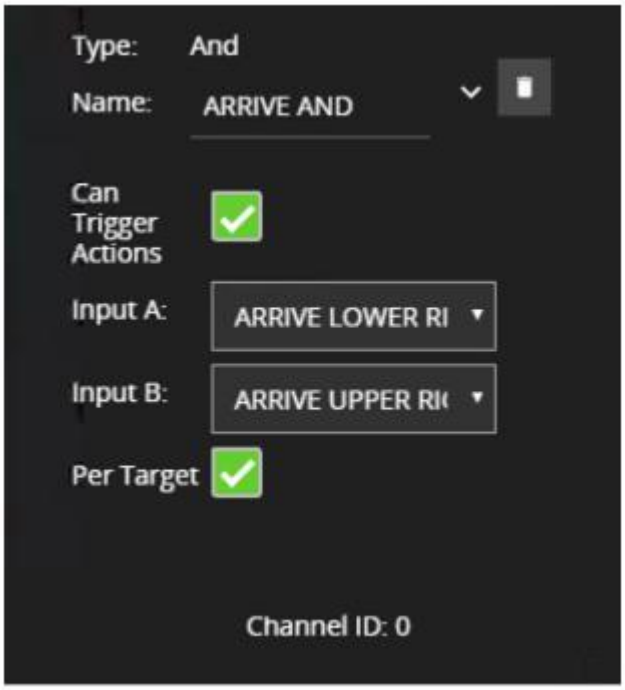
A conditional input, like a filter, is one that cannot trigger an action on its own.
It requires the input of another basic input, conditional rule or filter to be meaningful.
An example of this is the AND rule. The AND rule requires two inputs to compare in order to function.

8.9.7.17.1 The complete list of conditional rules are:

- And
- Continuously
- Counter
- Or
- Previous

8.9.7.17.2 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

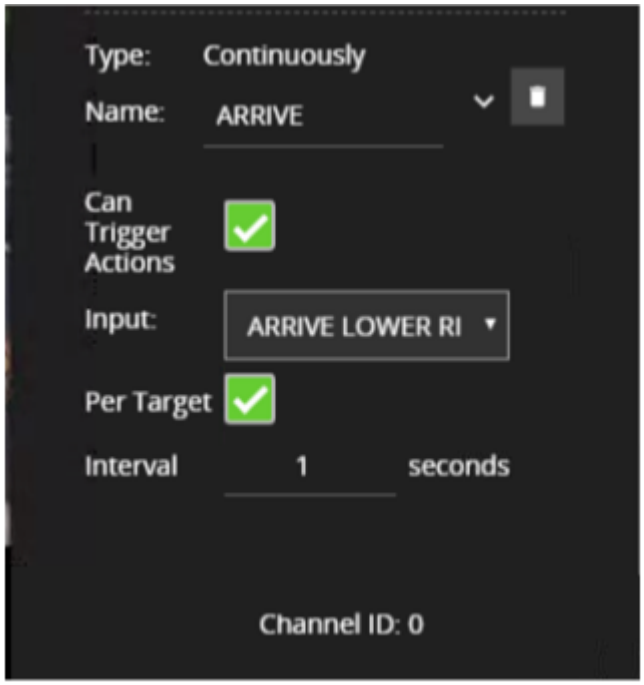
If we consider a scene with two presence rules, connected to two separate zones, connected by an AND rule, the table below explains the behaviour of the Per Target property.
Note that object here refers to a tracked object, as detected by the VCA tracking engine.

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.

8.9.7.17.3 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.

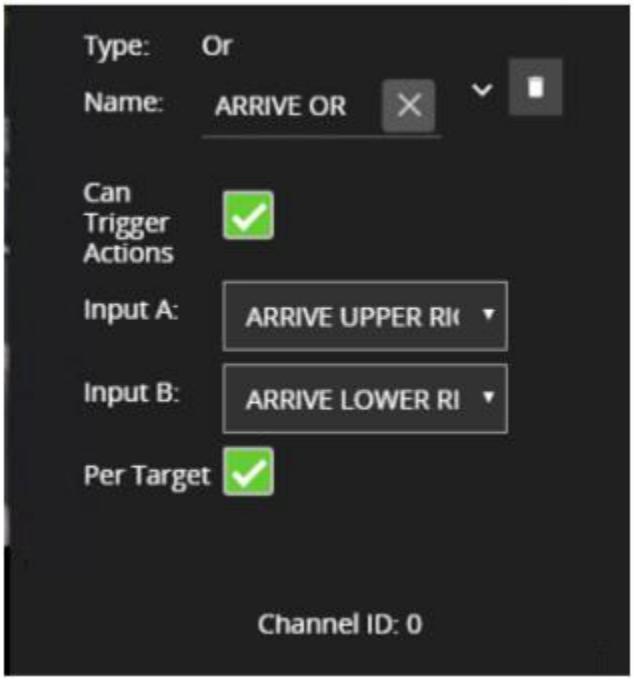
When it is off, only one event will be generated by the rule, even if there are multiple tracked objects within the zone.
Additionally, when Per Target is off, the rule will only generate events when there is a change of state - i.e. the rule condition changes from true to false or vice versa.

8.9.7.17.3.1 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

8.9.7.17.4 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 #"

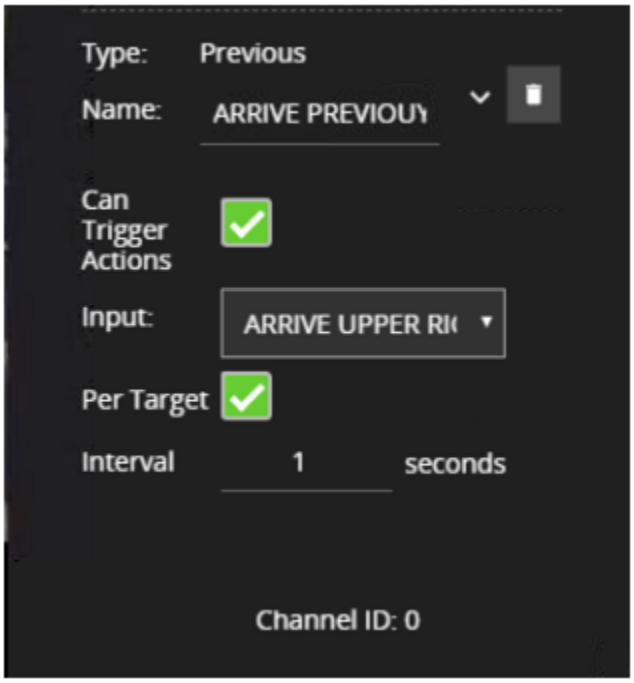
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Input A	The first input	None
Input B	The second input	None
Per Target	Fire one event per tracked object	Active

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

8.9.7.17.5 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

8.9.7.18 VCA - Counters

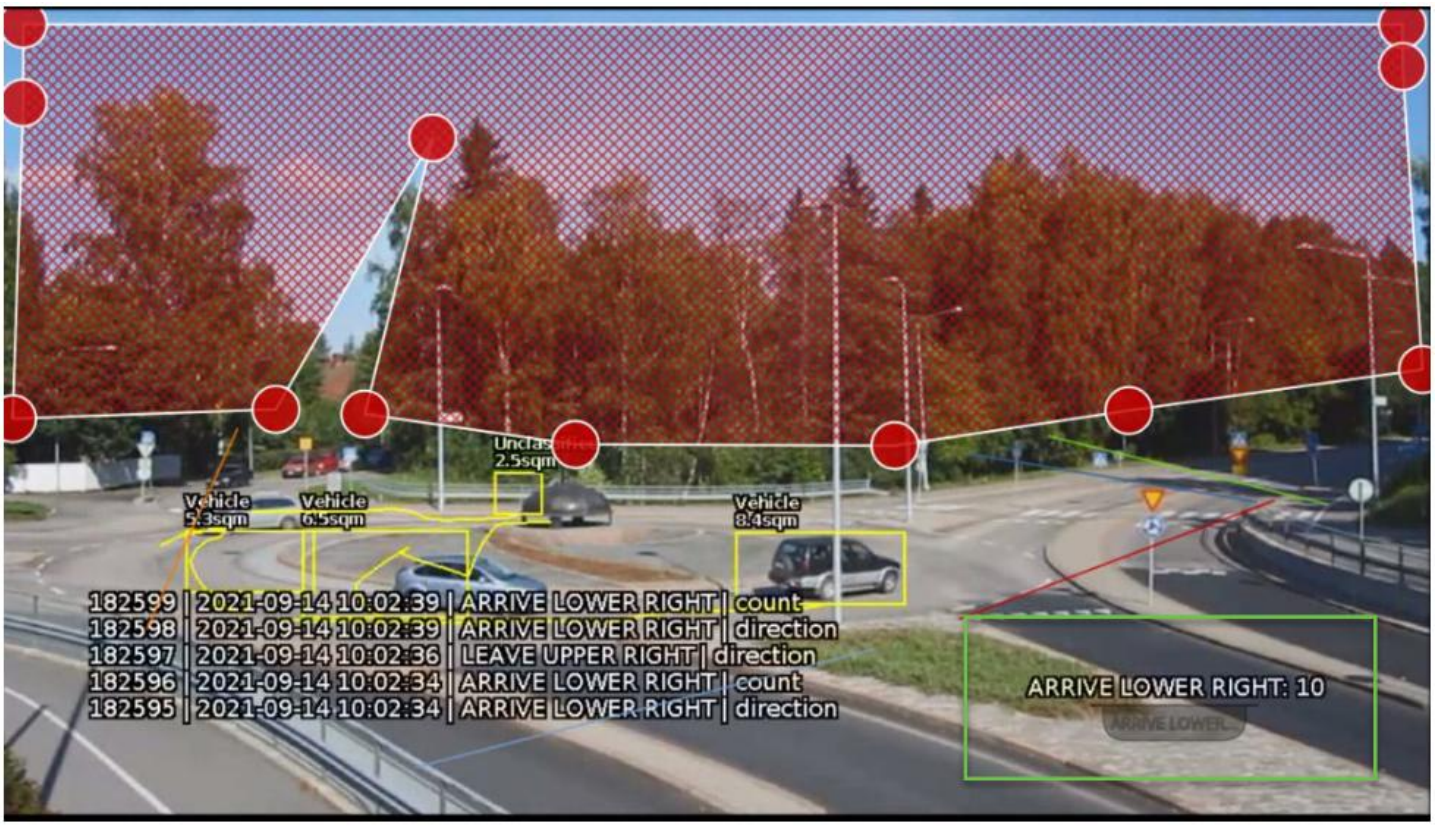
These counters are only visible in the VCA configuration. To use counters in the Spotter please refer to the Spotter manual.
Counters can be configured to count the number of times a rule is triggered, for example, the number of people crossing a line.

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.

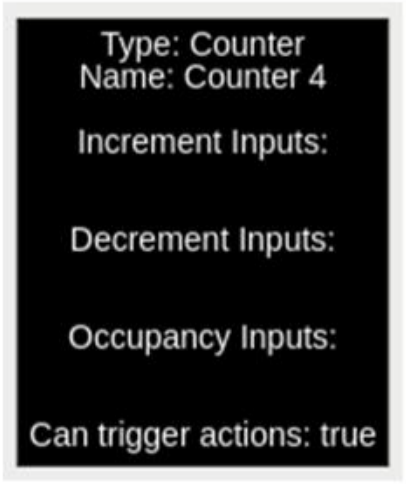
Note: events created by a counter will not trigger the Deep-Learning Filter, even if enabled on the channel.

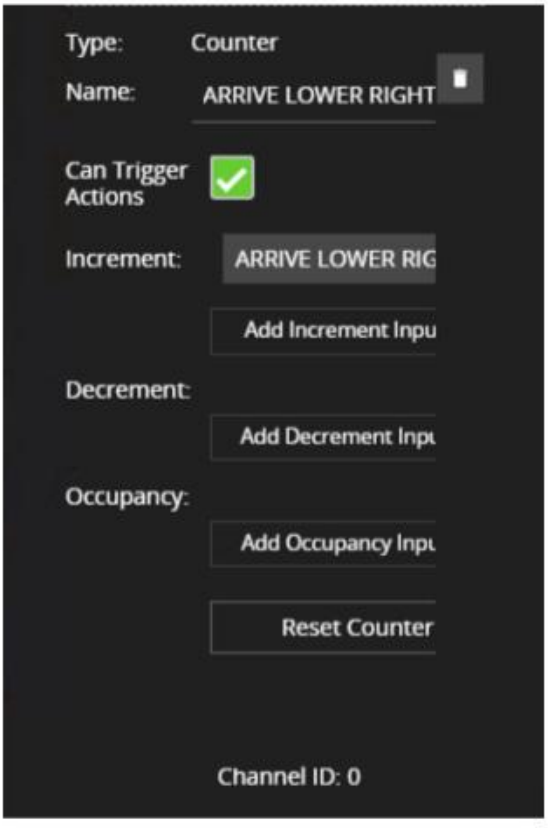


8.9.7.18.1 Positioning Counters

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.


Counter 0: 144
handle


Type: Counter
Name: Counter 4
Increment Inputs:
Decrement Inputs:
Occupancy Inputs:
Can trigger actions: true

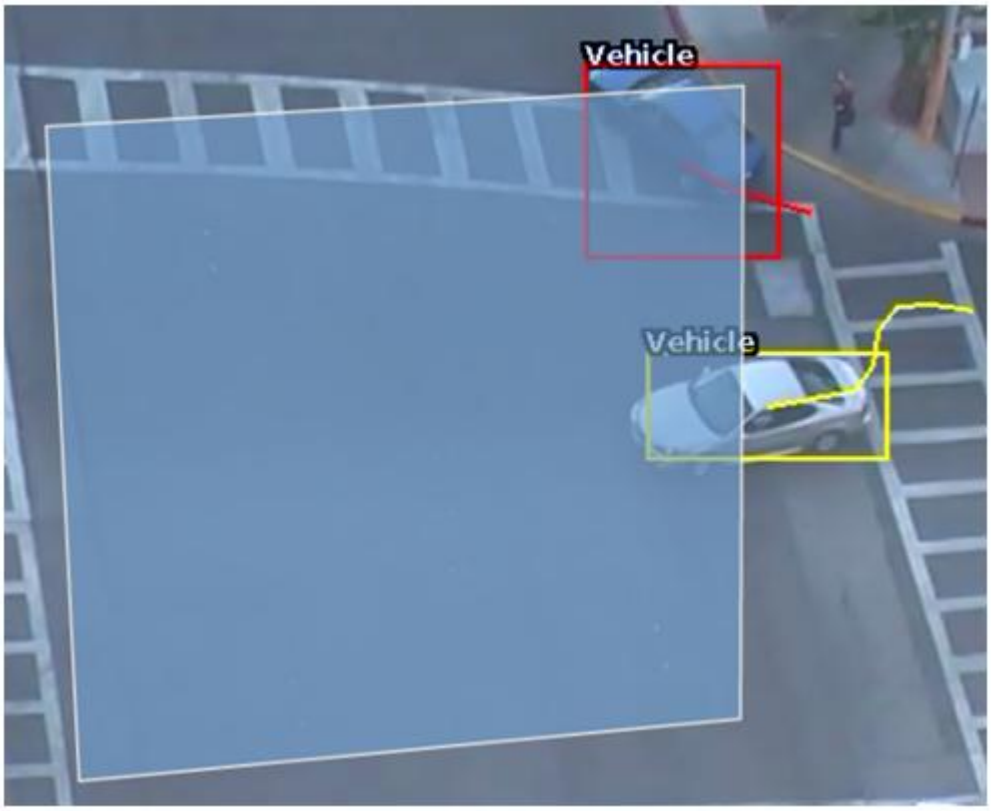

Type: Counter
Name: ARRIVE LOWER RIGHT
Can Trigger Actions
Increment:
ARRIVE LOWER RIG
Add Increment Inpu
Decrement:
Add Decrement Inpu
Occupancy:
Add Occupancy Inpu
Reset Counter
Channel ID: 0

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'.

8.9.7.19 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.



8.9.7.20 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

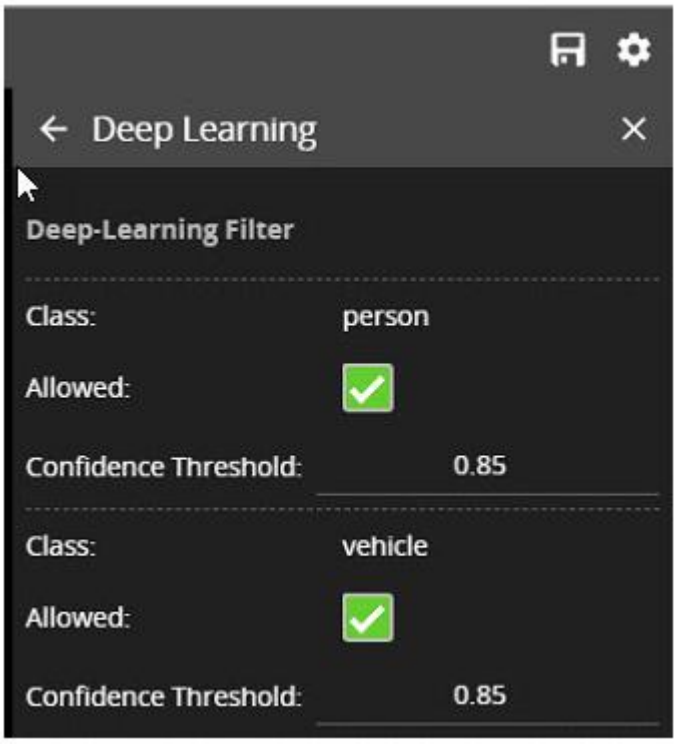


8.9.8 VCA - Deep-Learning Filter

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.



8.9.8.1 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.

8.10 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
- VCA Filters - Object Filter
- VCA Filters - Colour Filter
- VCA Filters - Retrigger Filter
- VCA Filters - Deep Learning Filter

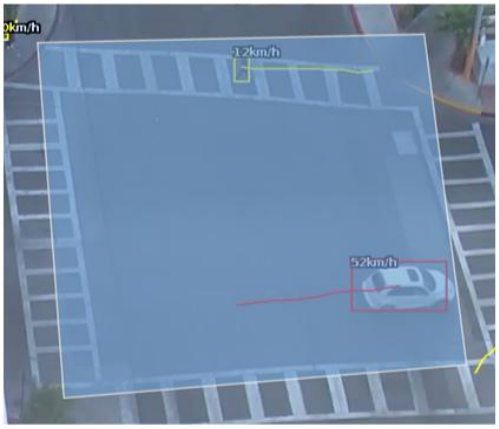
8.10.1 Speed Filter

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.

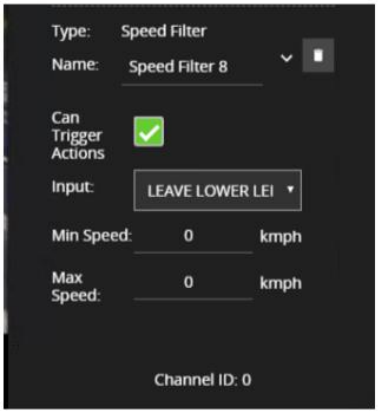
> The channel must be Calibrated in order for the speed filter to be available.

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.





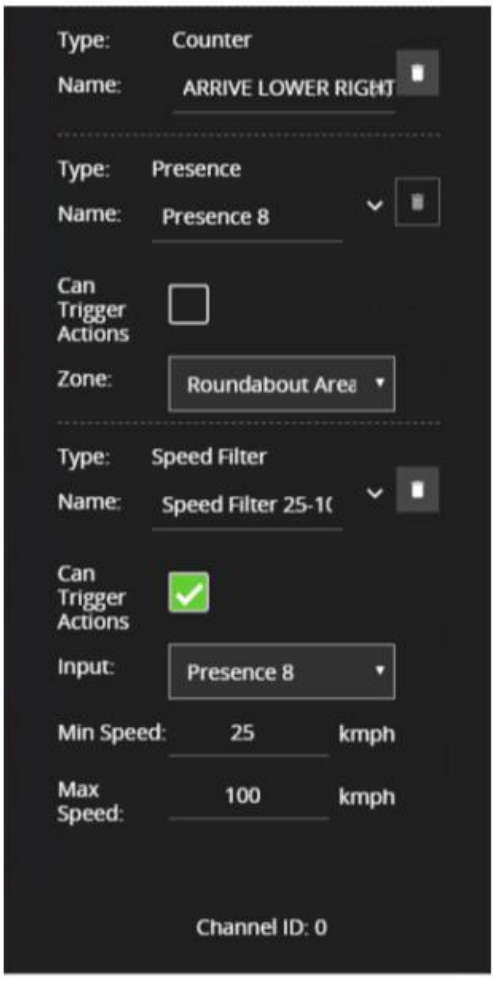


Property	Description	Default Value
Name	A user-specified name for this rule	"Speed #"

Property	Description	Default Value
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

8.10.1.1 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



8.10.2 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.

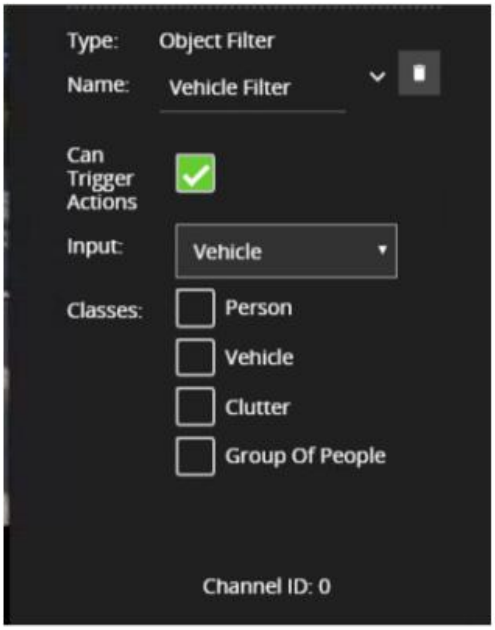


The previous image illustrates how the object classification filter configured with Vehicle class, includes only Vehicle objects.

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.





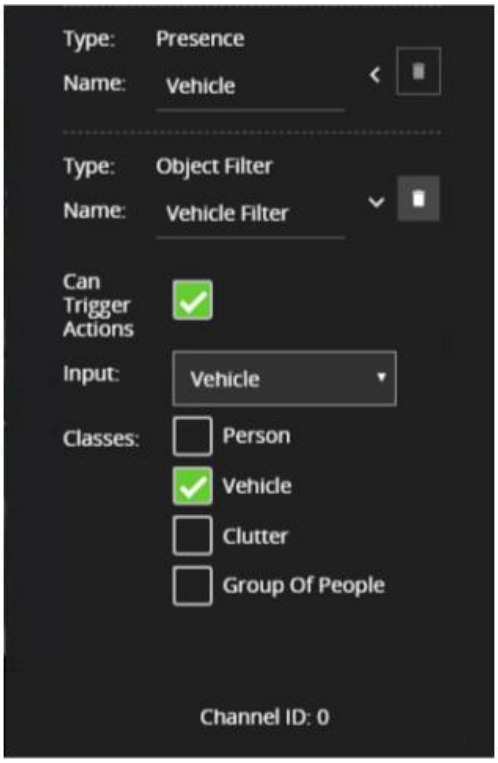
Property	Description	Default Value
Name	A user-specified name for this rule	"Object Filter #"
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Input	The input rule	None
Classes	The object classes allowed to trigger an alert	None

8.10.2.1 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.



8.10.3 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.

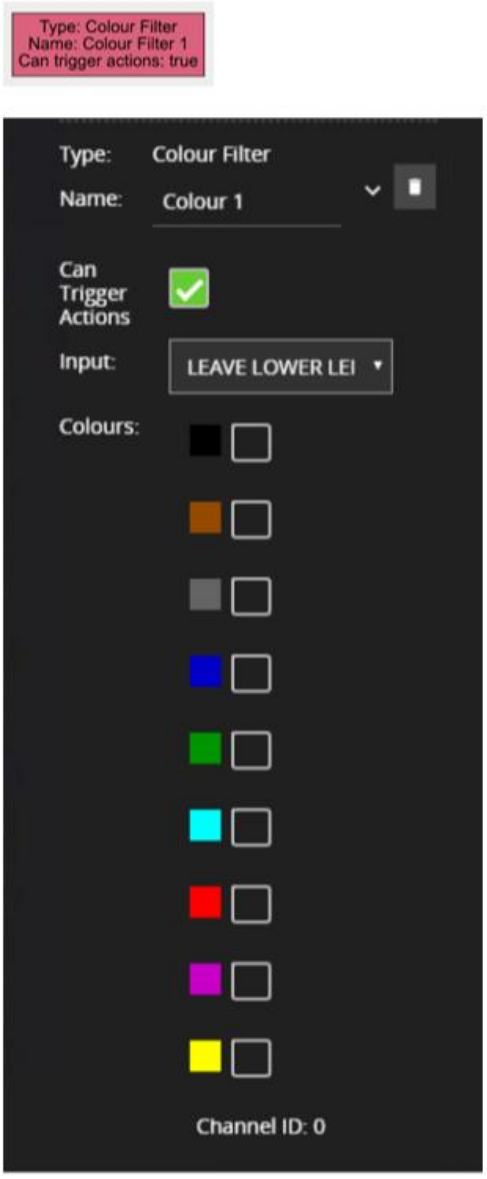
Typically, the colour classification filter would be combined with another rule(s) to prevent unwanted objects from triggering an alert, an example rule graph is provided to illustrate this below.



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.



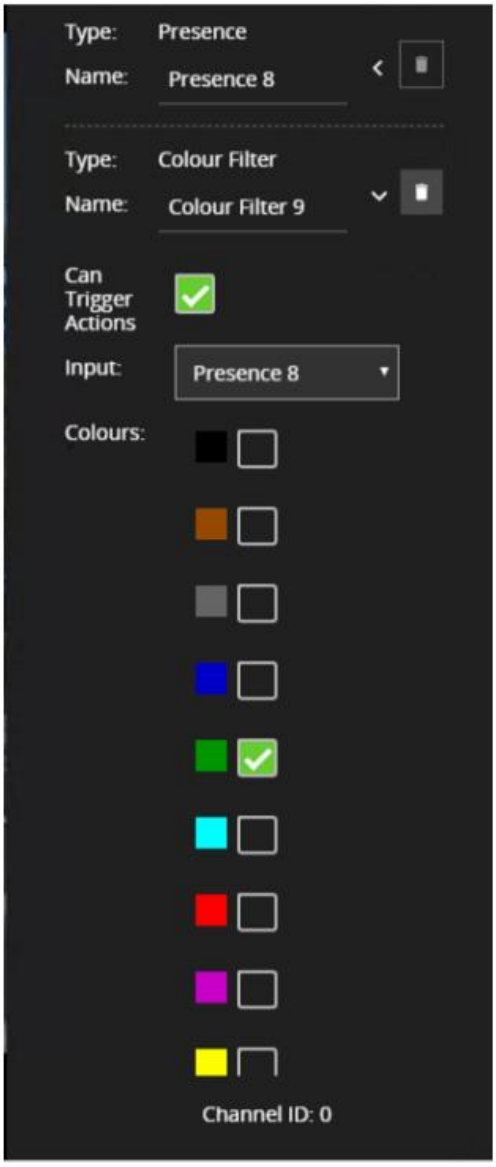
Property	Description	Default Value
Name	A user-specified name for this rule	"Object Filter #"
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Input	The input rule	None
Colours	The colours allowed to trigger an alert	All Unchecked

8.10.3.1 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.

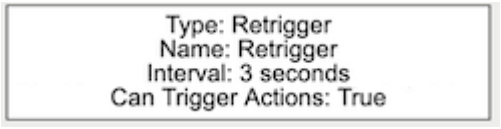


8.10.4 VCA Filters - Retrigger Filter

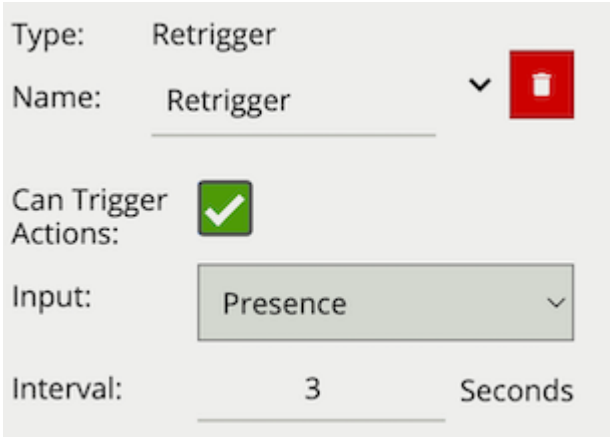
The Retrigger Filter acts as an event pass through, which only generates an event if the input has not fired previously within the defined interval.

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.

8.10.4.1 Graphical View



8.10.4.2 Form View



8.10.4.3 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

8.10.5 VCA Filters - Deep Learning Filter

The deep learning filter provides the ability to filter out objects that trigger a rule if they are not classified as a certain class by the deep learning model. The available object classes are defined by the model.

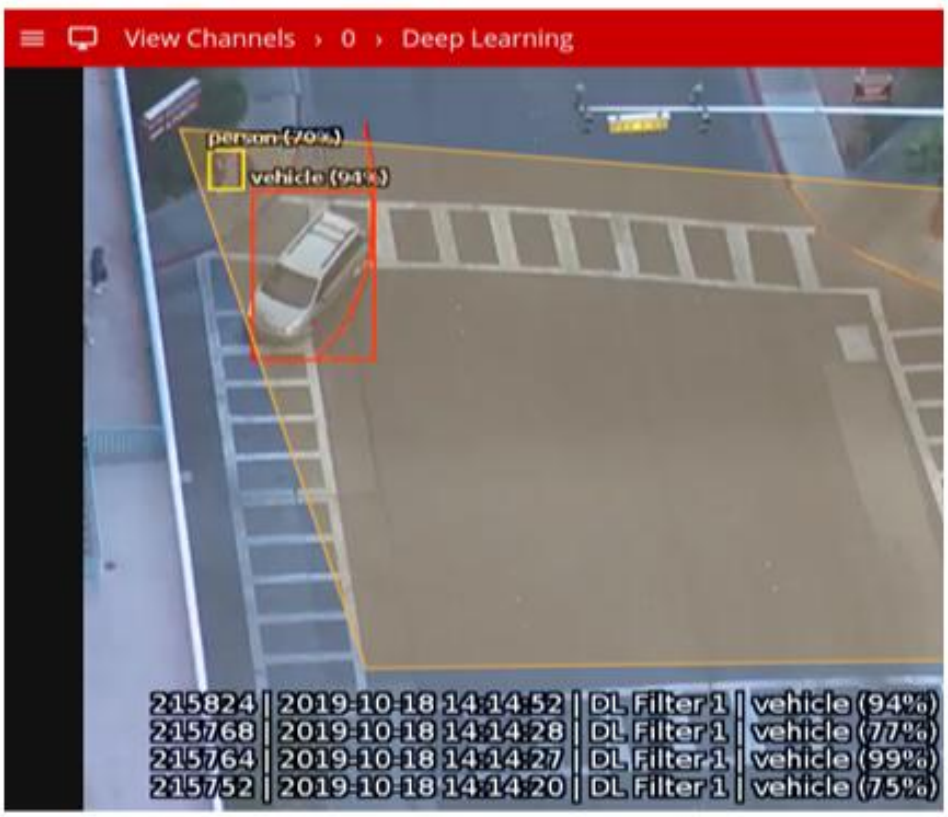
The deep learning filter settings are configured on the Deep Learning page.

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 that generate a high volume of events (more than 1 per second), **which may result in poor performance of the system and is not advised.**

8.10.5.1 Rule combining and object class parameters

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.





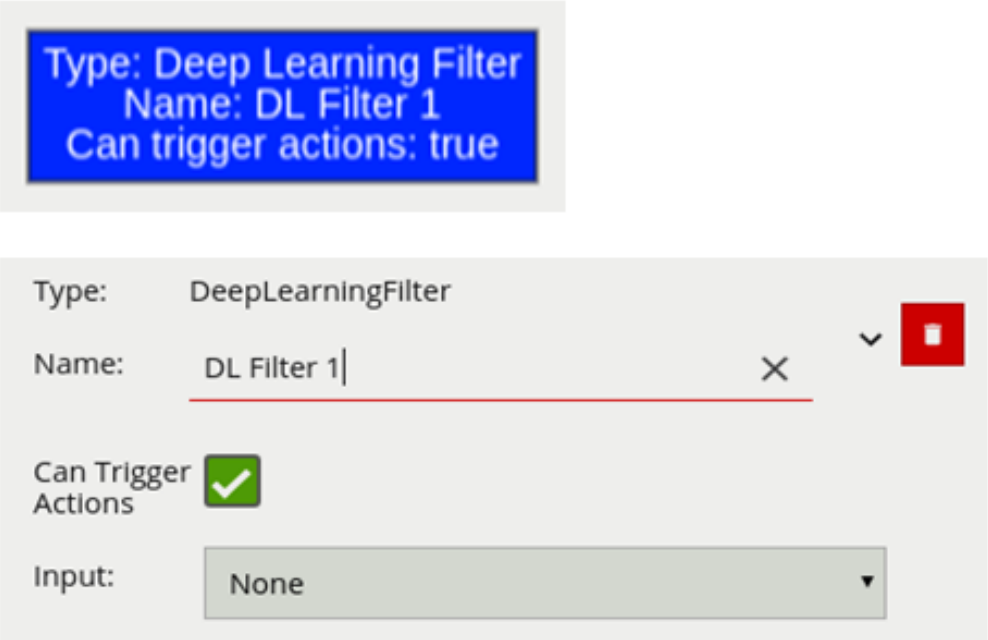
Each of the possible object classes has additional parameters:

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.

The previous image illustrates how the deep learning filter configured with just the 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

8.10.5.2 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.



8.11 Conditional Rule Types

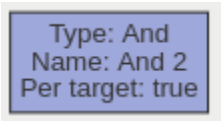
The currently supported conditional rules, along with a detailed description of each.

- And
- Continuously
- Counter
- Not
- Or
- Previous
- Repeatedly

8.11.1 And

A logical operator that combines two rules and only fires events if both inputs are true.

8.11.1.1 Graphical View



8.11.1.2 Form View



8.11.1.3 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

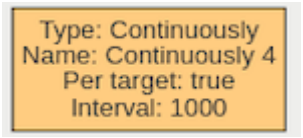
If we consider a scene with two presence rules, connected to two separate zones, connected by an AND rule, the table below explains the behaviour of the Per Target property. Note that object here refers to a tracked object, as detected by the VCA tracking engine.

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

8.11.2 Continuously

A logical operator that fires events when its input has occurred continuously for a user-specified time.

8.11.2.1 Graphical View



8.11.2.2 Form View



8.11.2.3 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

8.11.3 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.

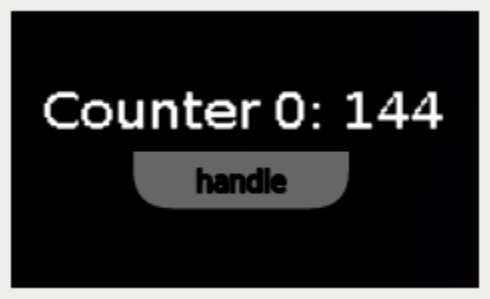
Broadly speaking a single counter should not be used for both purposes occupancy and increment / decrement.

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

8.11.3.1 Positioning Counters

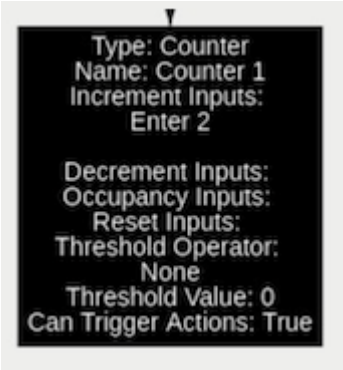
When added, a counter object is visualised on the video stream as seen below. The counter can be repositioned by grabbing the 'handle' beneath the counter name and moving the counter to the desired location.



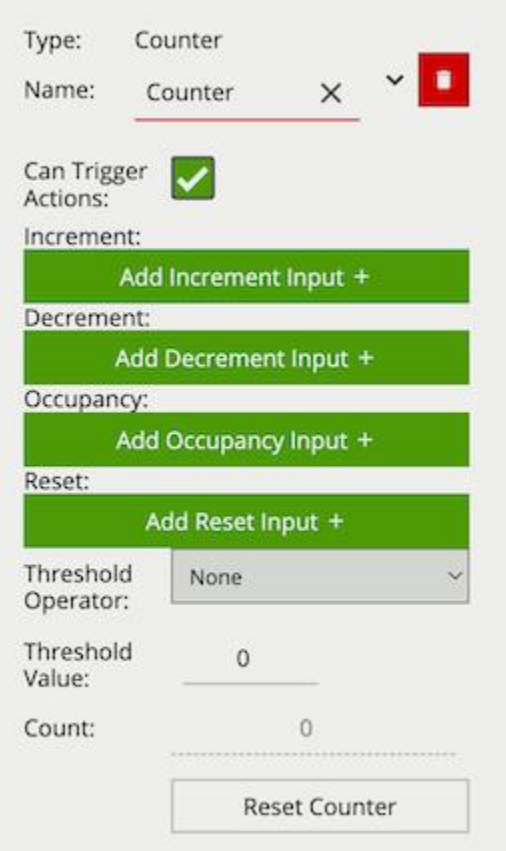
Right-clicking the mouse (or tap-and-hold on a tablet) on the grid displays the context menu.



8.11.3.2 Graphical View



8.11.3.3 Form View



8.11.3.4 Configuration

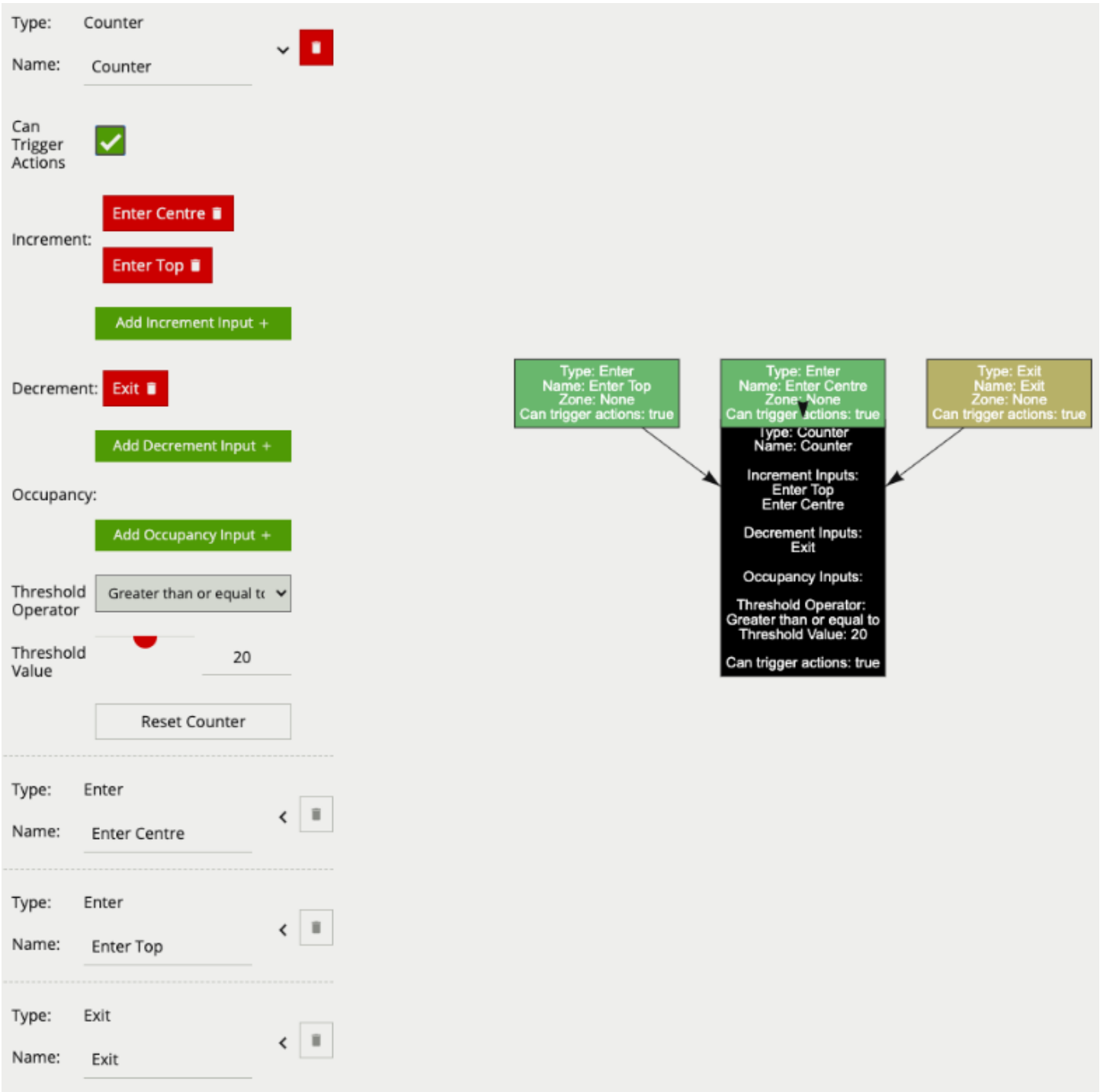
Property	Description	Default Value
Name	A user-specified name for this rule	"Counter #"
Increment	The rule which, when triggered, will add one to the counter	None
Decrement	The rule which, when triggered, will subtract one from the counter	None
Occupancy	Sets counter to current number of the rule's active 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
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.

8.11.3.5 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.



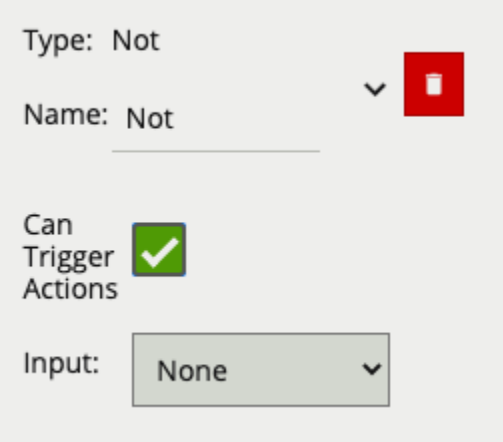
8.11.4 Not

A logical operator that generates an event when the input rule becomes false.

8.11.4.1 Graphical View



8.11.4.2 Form View



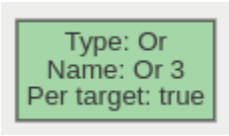
8.11.4.3 Configuration

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

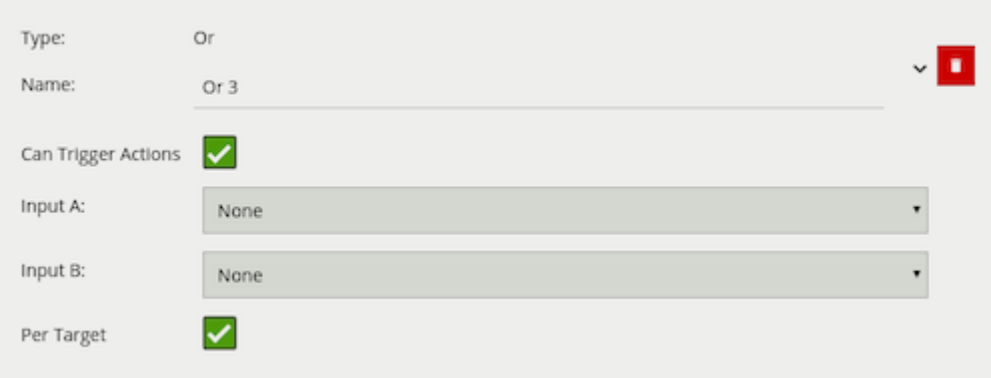
8.11.5 Or

A logical operator that combines two rules and fires events if either input is true.

8.11.5.1 Graphical View



8.11.5.2 Form View



8.11.5.3 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.

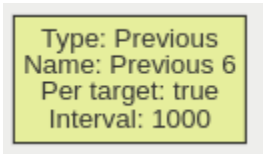
State	Per Target	Outcome
Object A in Input A, No object in input B	On	Two events generated, one for each object
No object in Input A, Object B in input B	On	Only one event generated (for Object B)
Object A in Input A, No object in input B	On	Only one event generated (for Object A)
Object A in Input A, 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.

8.11.6 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).

8.11.6.1 Graphical View



8.11.6.2 Form View



8.11.6.3 Configuration

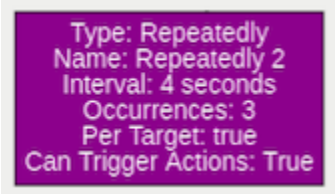
Property	Description	Default Value
Name	A user-specified name for this rule	"Previous #"
Can Trigger Actions	Specifies whether events generated by this rule trigger actions	Active
Input	The input rule	None
Per Target	Fire one event per tracked object. See description below for more details	Active
Interval	The time in milliseconds	1

8.11.7 Repeatedly

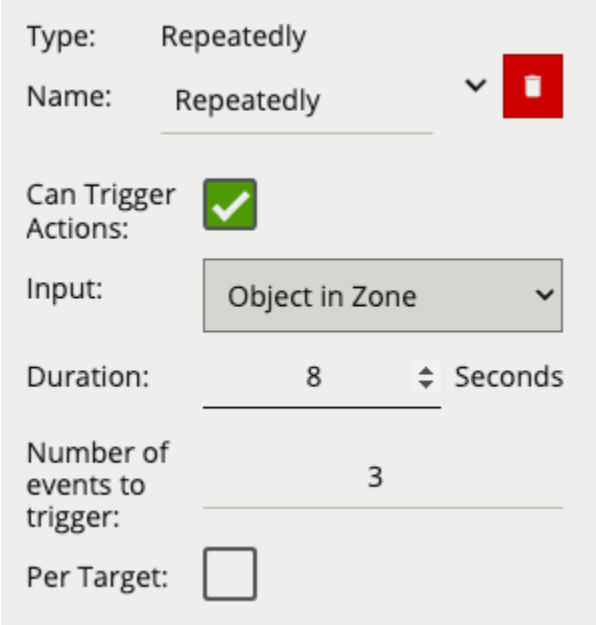
A logical operator that triggers when an input rule is triggered a set number of times within a defined period. The Duration period is a window of time computed from every input event. For example, with a Repeatedly rule configured to generate an event when the input triggers three times in eight seconds, 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.

8.11.7.1 Graphical View



8.11.7.2 Form View



8.11.7.3 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

8.12 Other Sources

- HTTP

- Schedule

8.12.1 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.

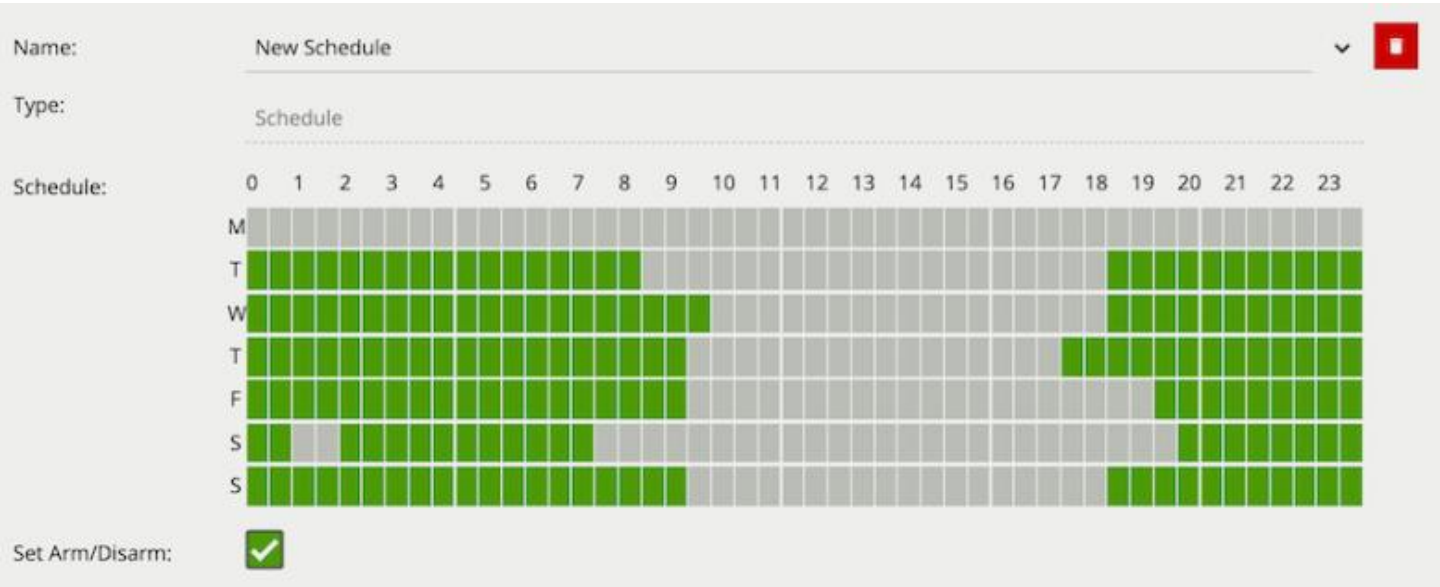


8.12.1.1 Properties

- **Endpoint URL:** The REST API endpoint defining the state variable.

8.12.2 Schedule

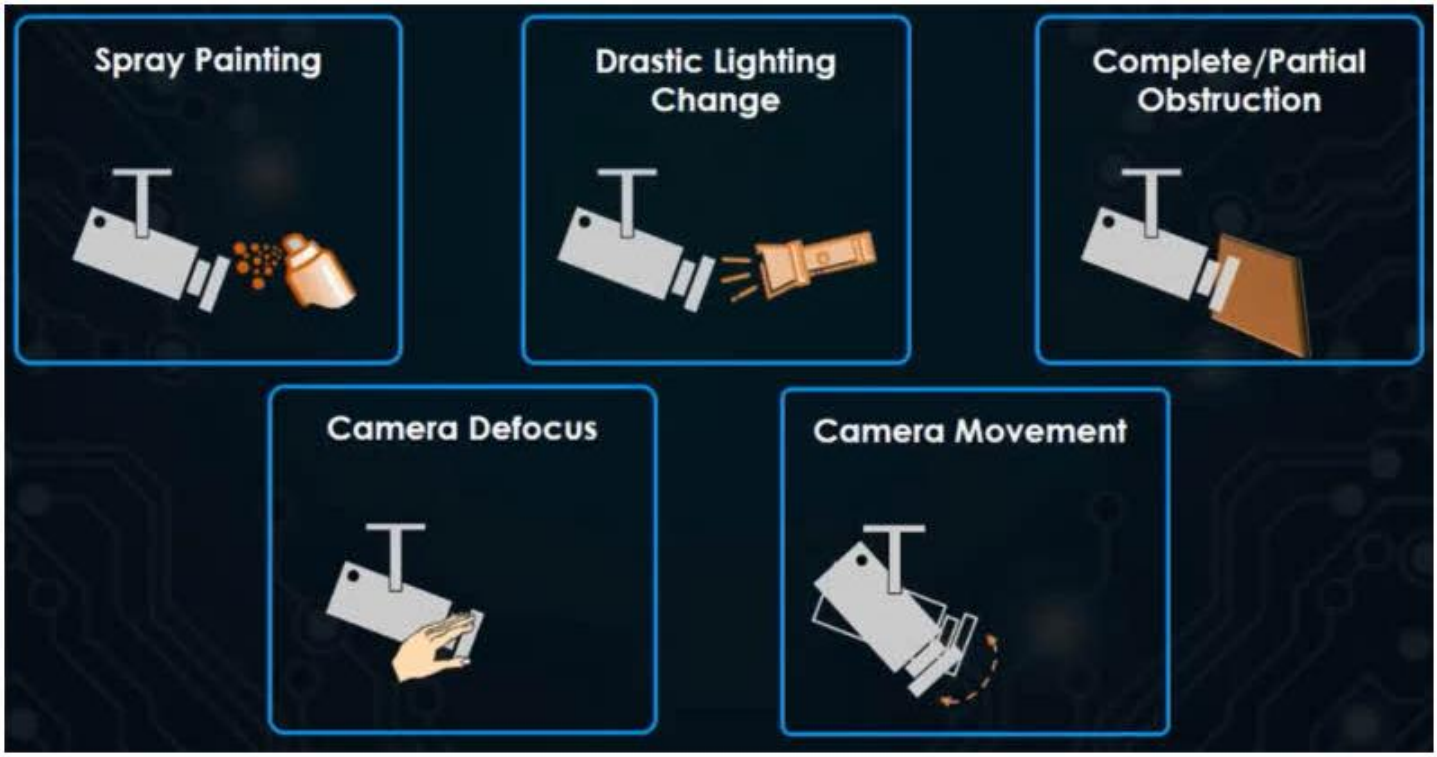
The Schedule source allows the definition of a schedule of time when the source is either on or off. The Schedule other source can be referenced by the [Source Filter] in a rule graph. Additionally, the schedule source can be used to directly control the armed state of VCA.



8.12.2.1 Properties

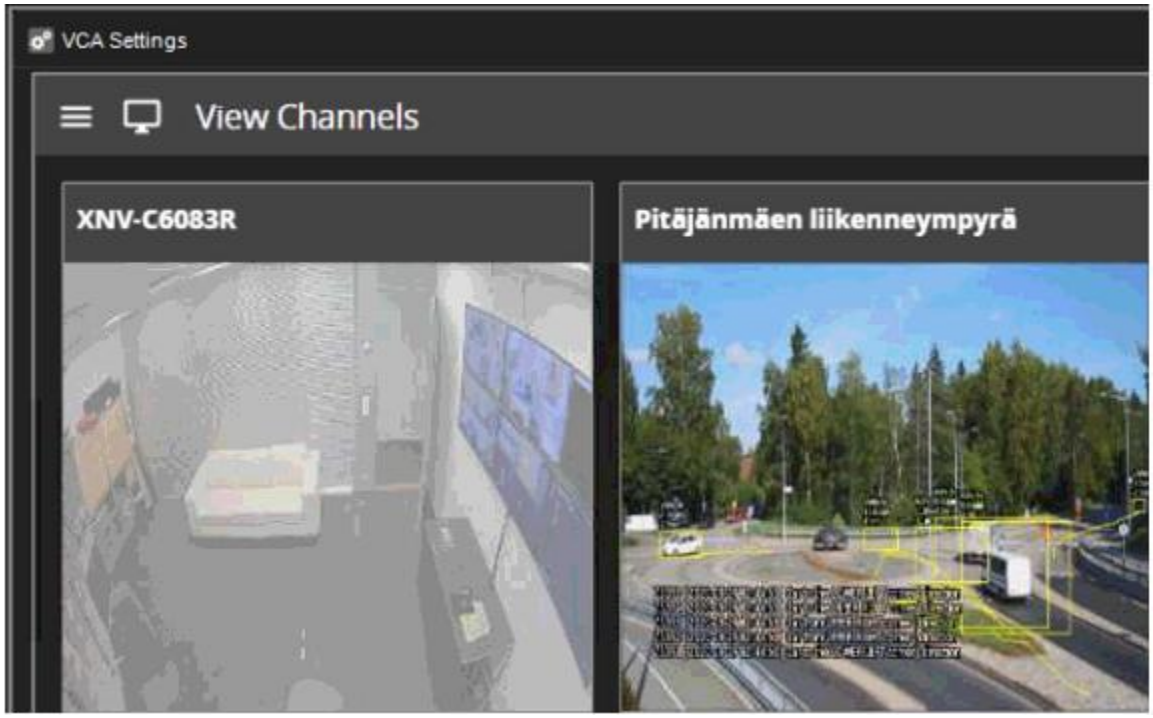
- **Schedule:** A click and drag interface which allows the definition of on periods (in green) and off periods (in grey). Each row represents one of the seven days in a week and each column represents a half hour period in that 24 hours.
- **Set Arm/Disarm:** When checked, the schedule source directly sets VCA Armed state according to the schedule defined above.

8.13 VCA - TAMPER DETECTION

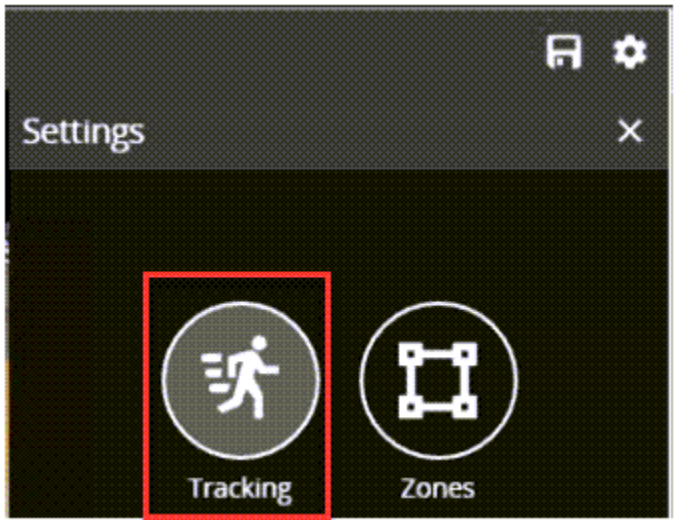


8.13.1 How to enable Tamper Detection

1. Open camera from the View Channels

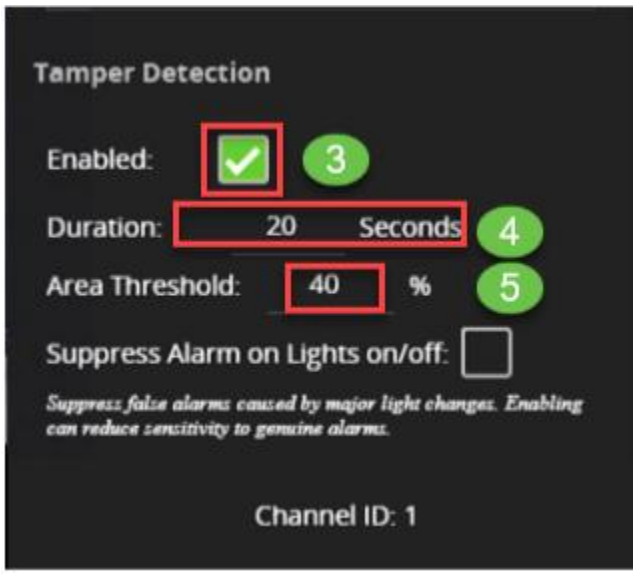


2. Open **Tracking**



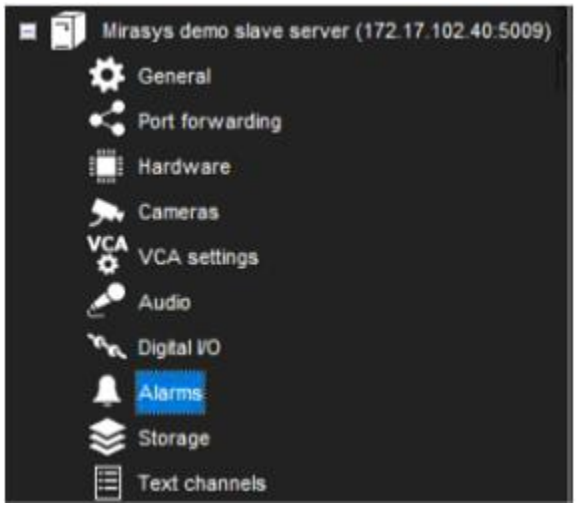
3. Enable Tamper Detection
4. Set **Duration**

5. Set **Area Threshold**

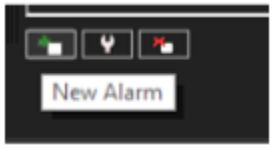


8.13.2 How to create an alarm from Tamper Detection

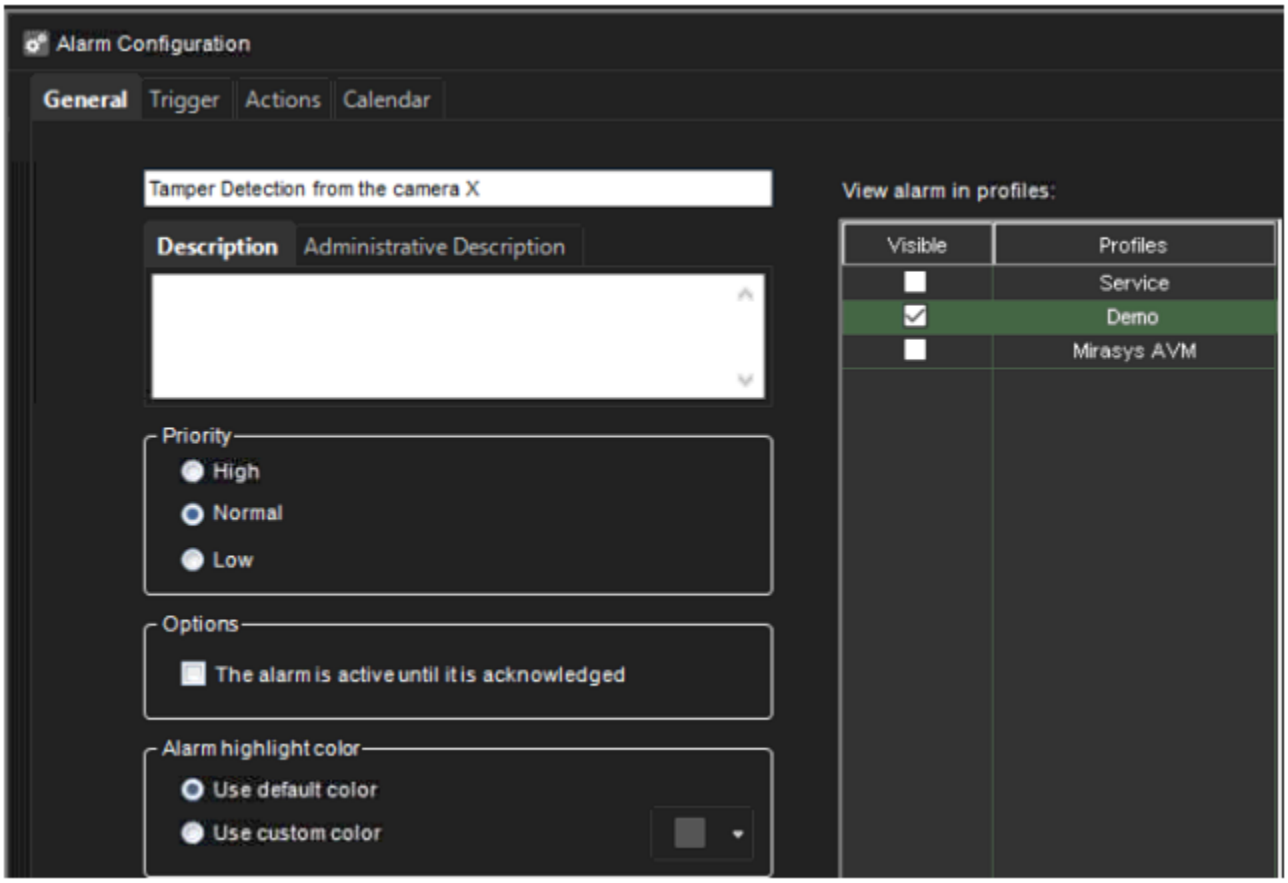
1. Open Alarms from the needed VMS server



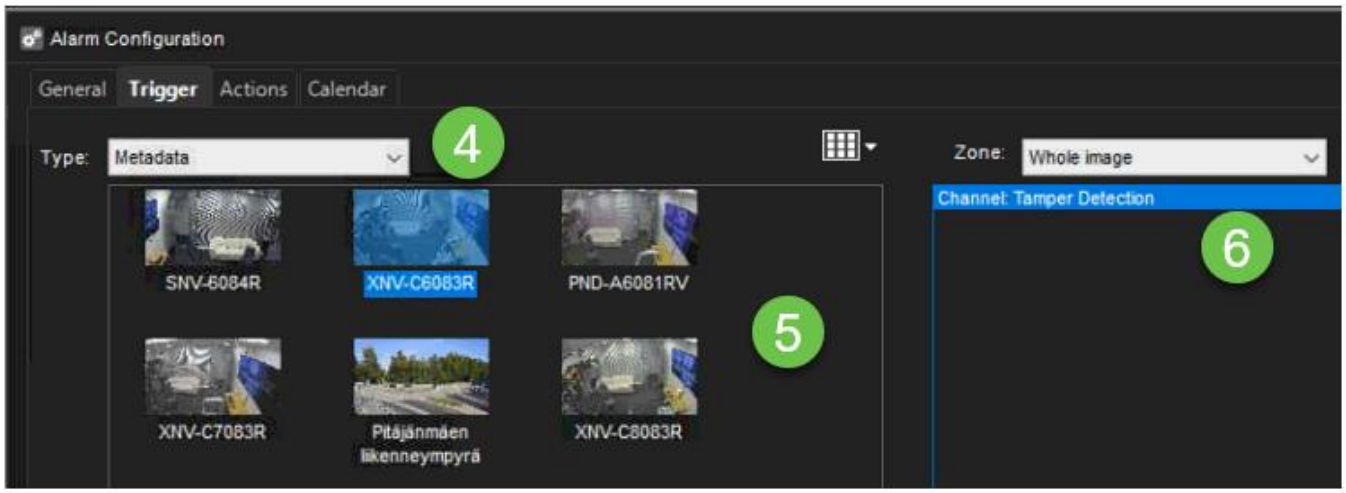
2. Click **New Alarm**



3. Enter the name of the alarm



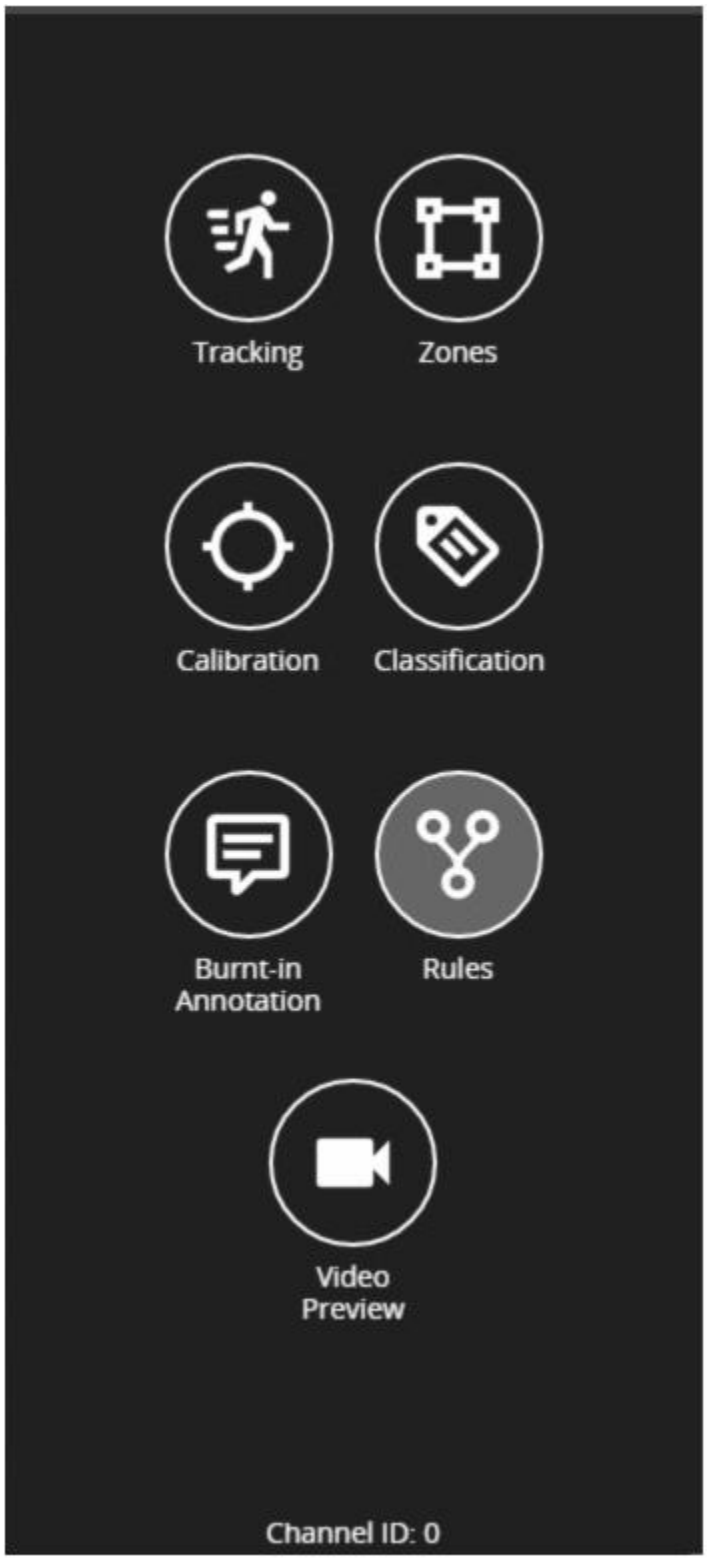
4. Select Trigger **Metadata**
5. Select camera from the list
6. Select Tamper Detection



8.14 How to create rules

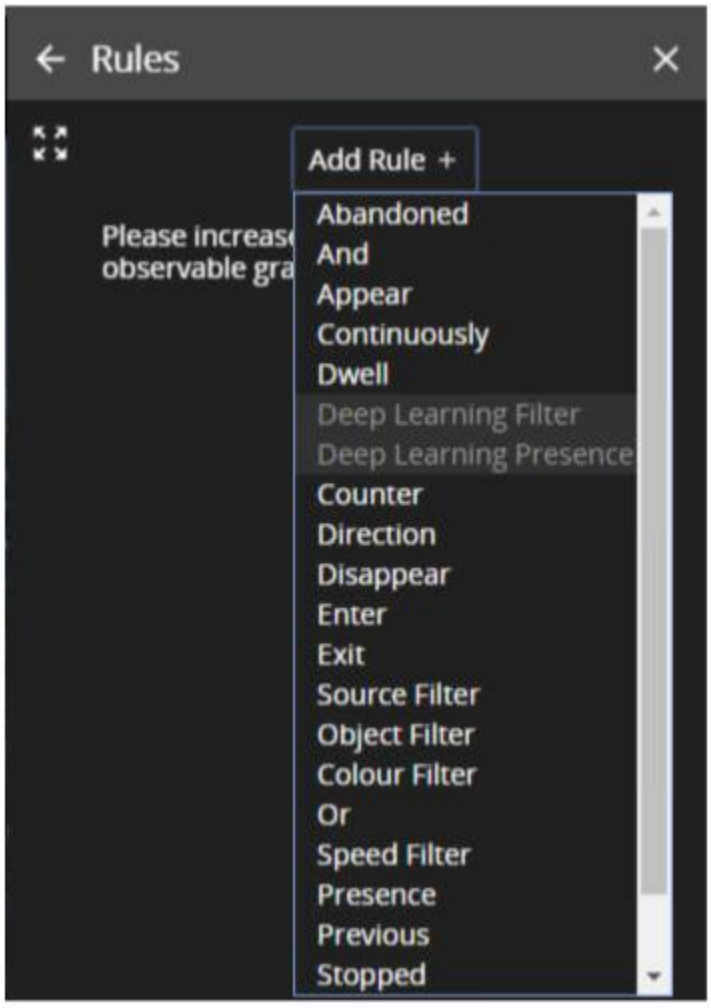
1. Click **Rules**

MIRASYS

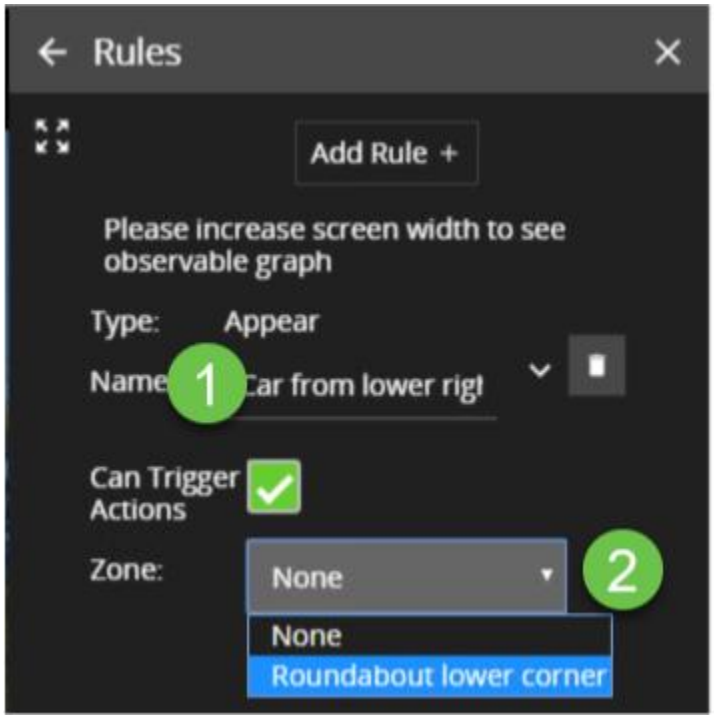


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

2. Click **Add Rule**
3. Select rule from the list

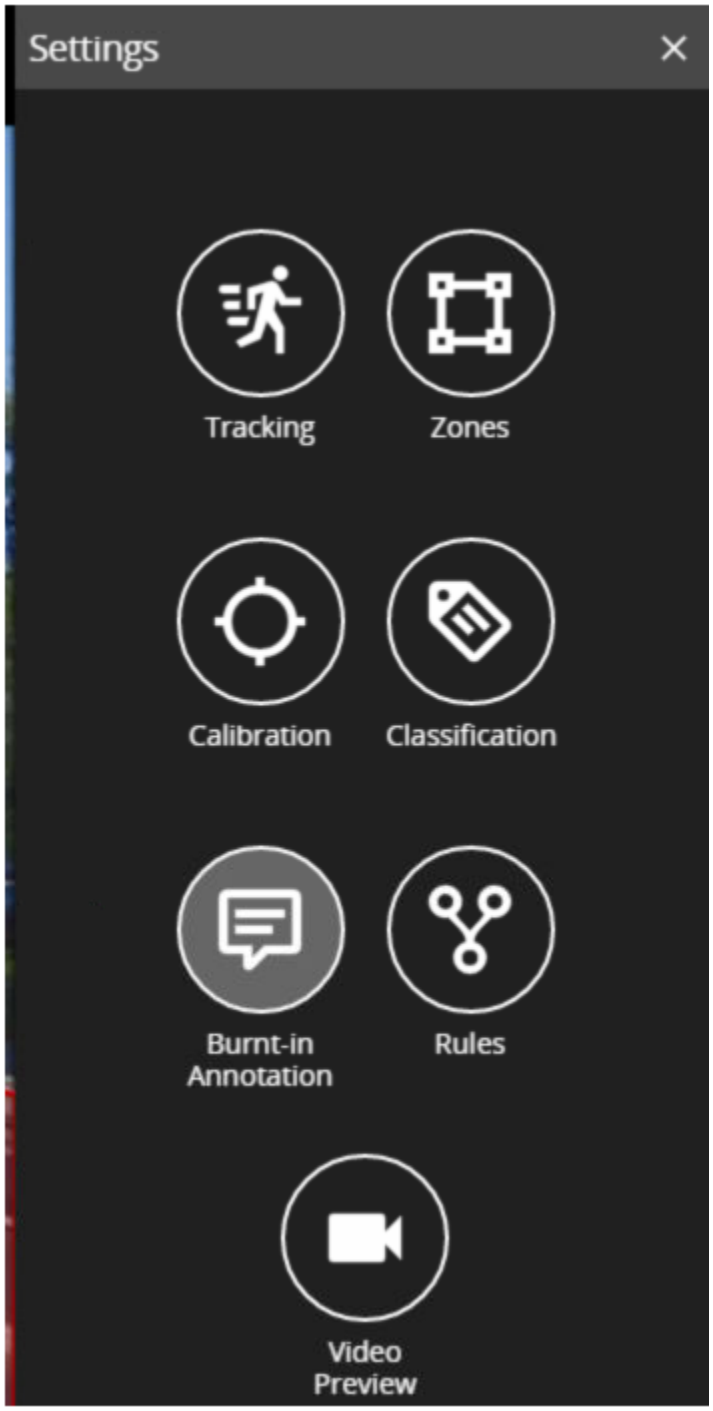


4. Set the name for the rule
5. Select zone



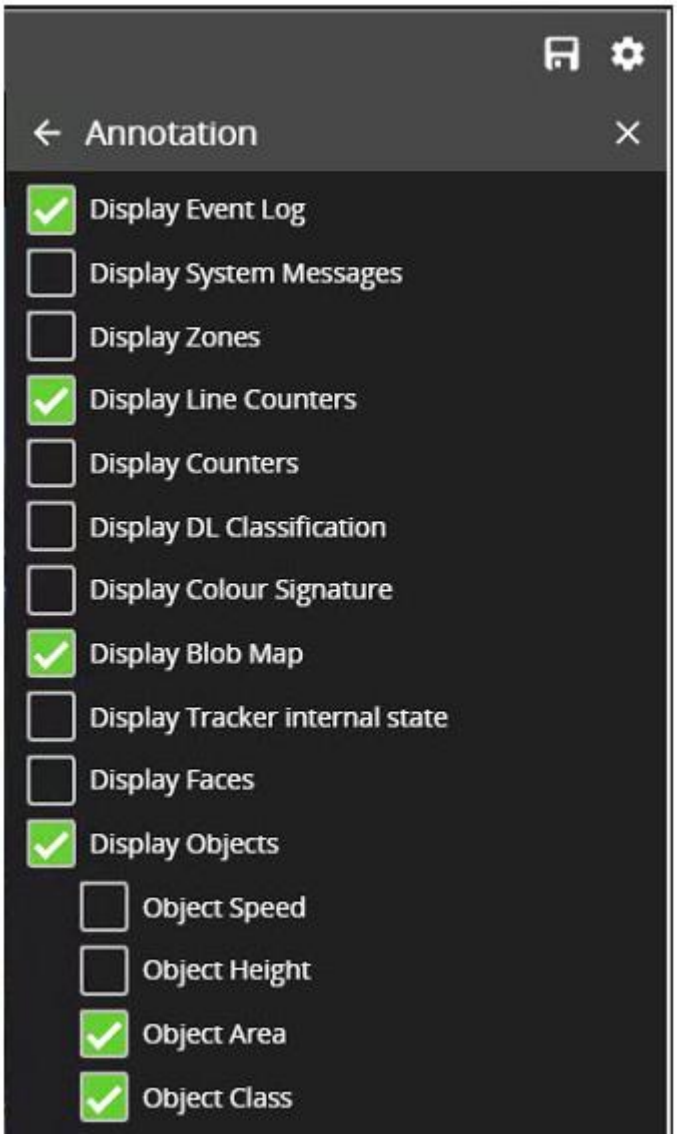
8.15 How to test rules

1. Open **Burnt-in Annotation**

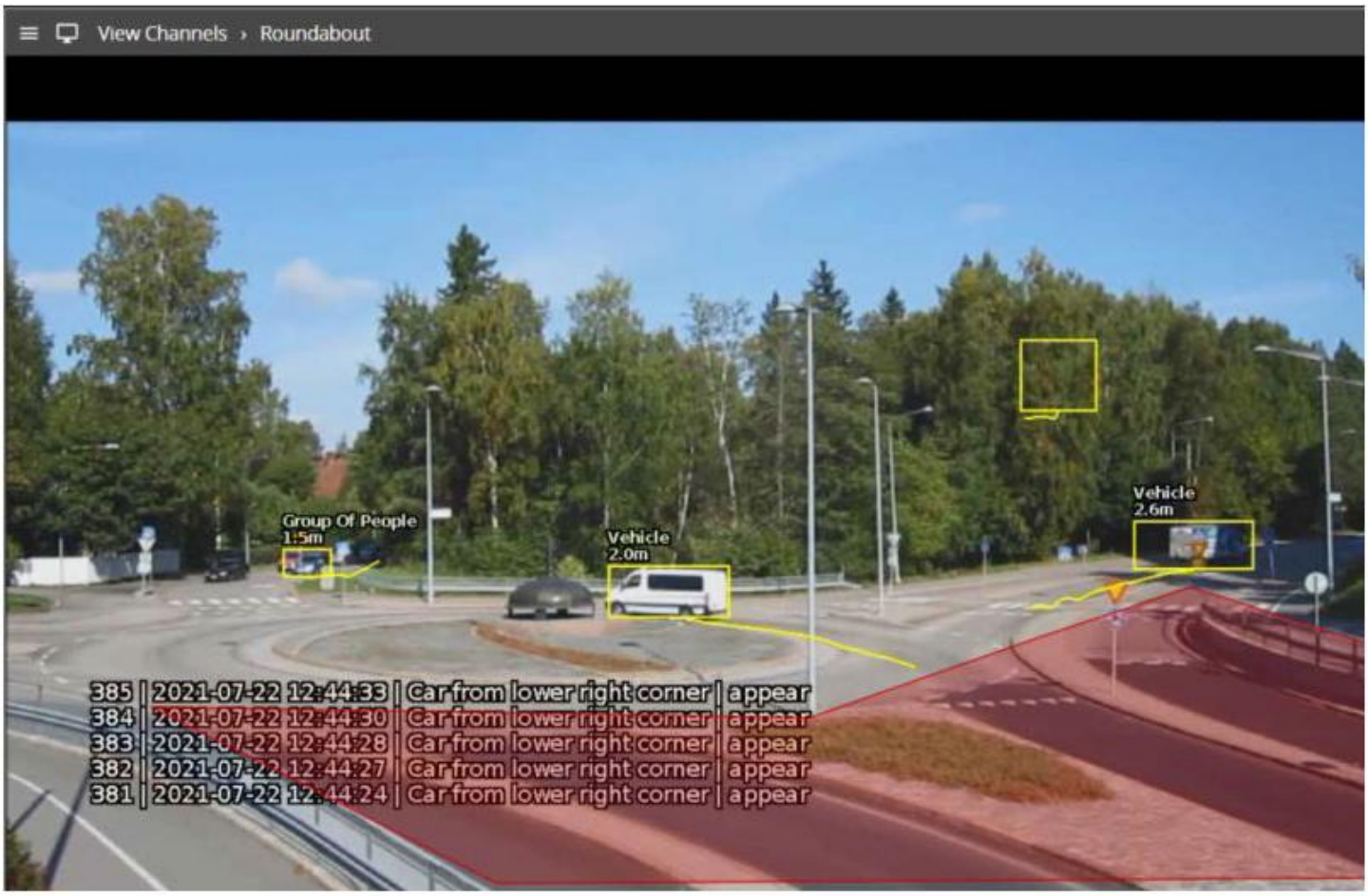


2. Enable **Event Log**
3. Enable **Display Line Counters**

4. Enable **Display Blob Map**
5. Enable **Display Objects**
    a. Enable **Object Area**
    b. Enable **Object Class**

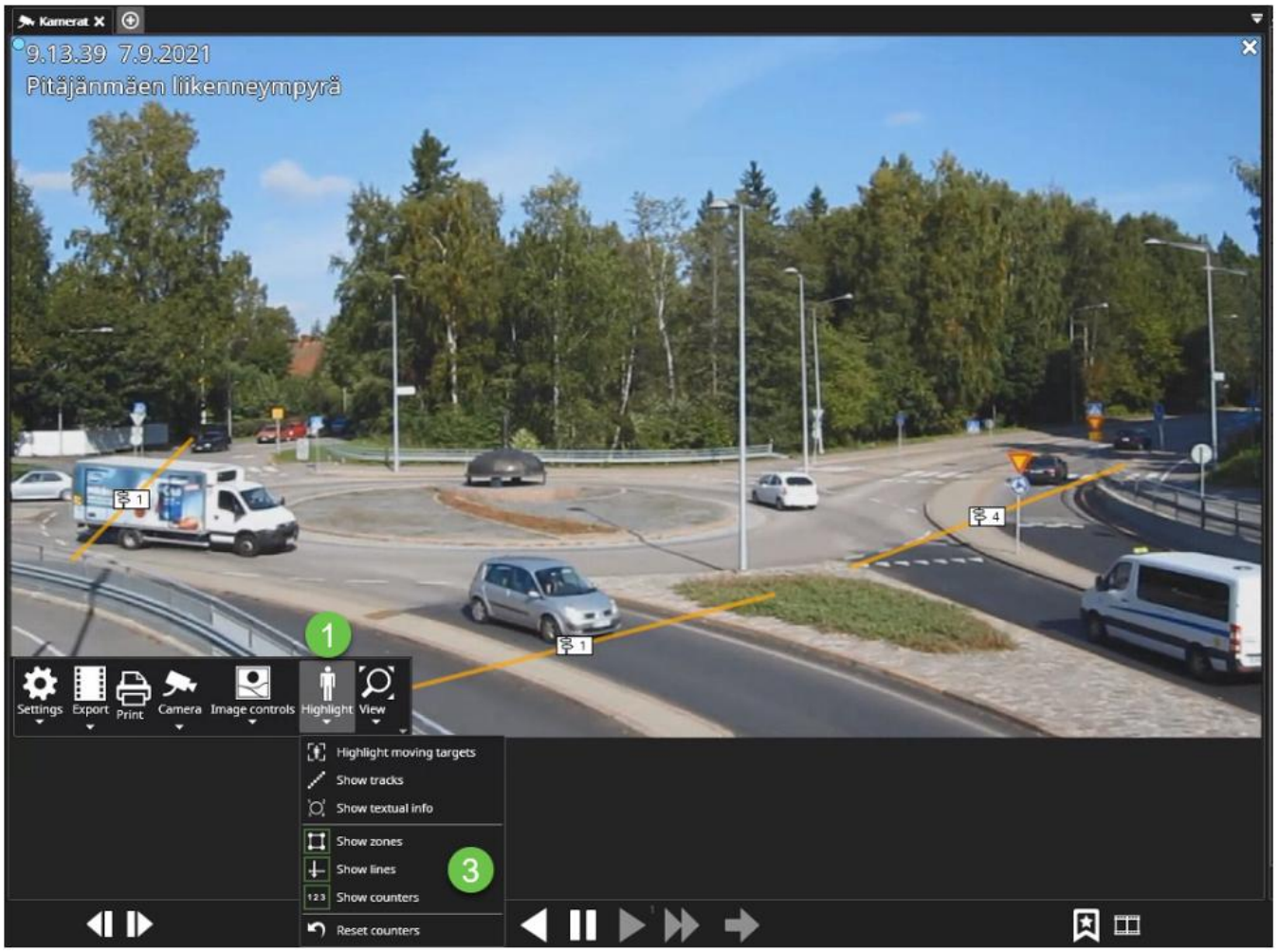


Open the correct camera and check that triggered events can be seen



8.16 How to view VCA events in the Mirasys Spotter

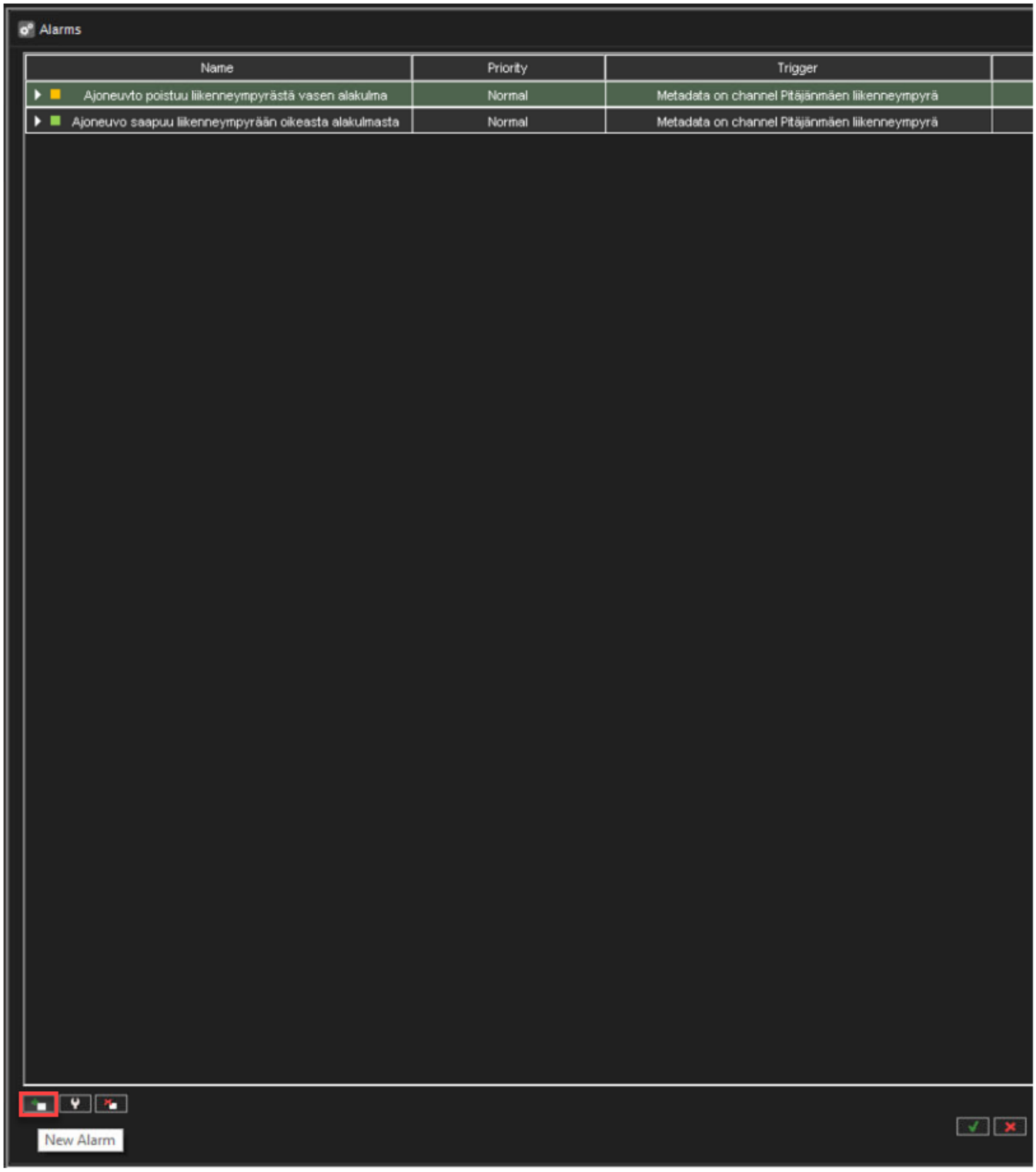
1. Open camera to the real-time view
2. Open camera toolbar and click **Highlight**
3. Enable needed options(**Show zone**s, **Show lines** or **Show counters**

1. 

8.17 How to create an alarm from VCA event

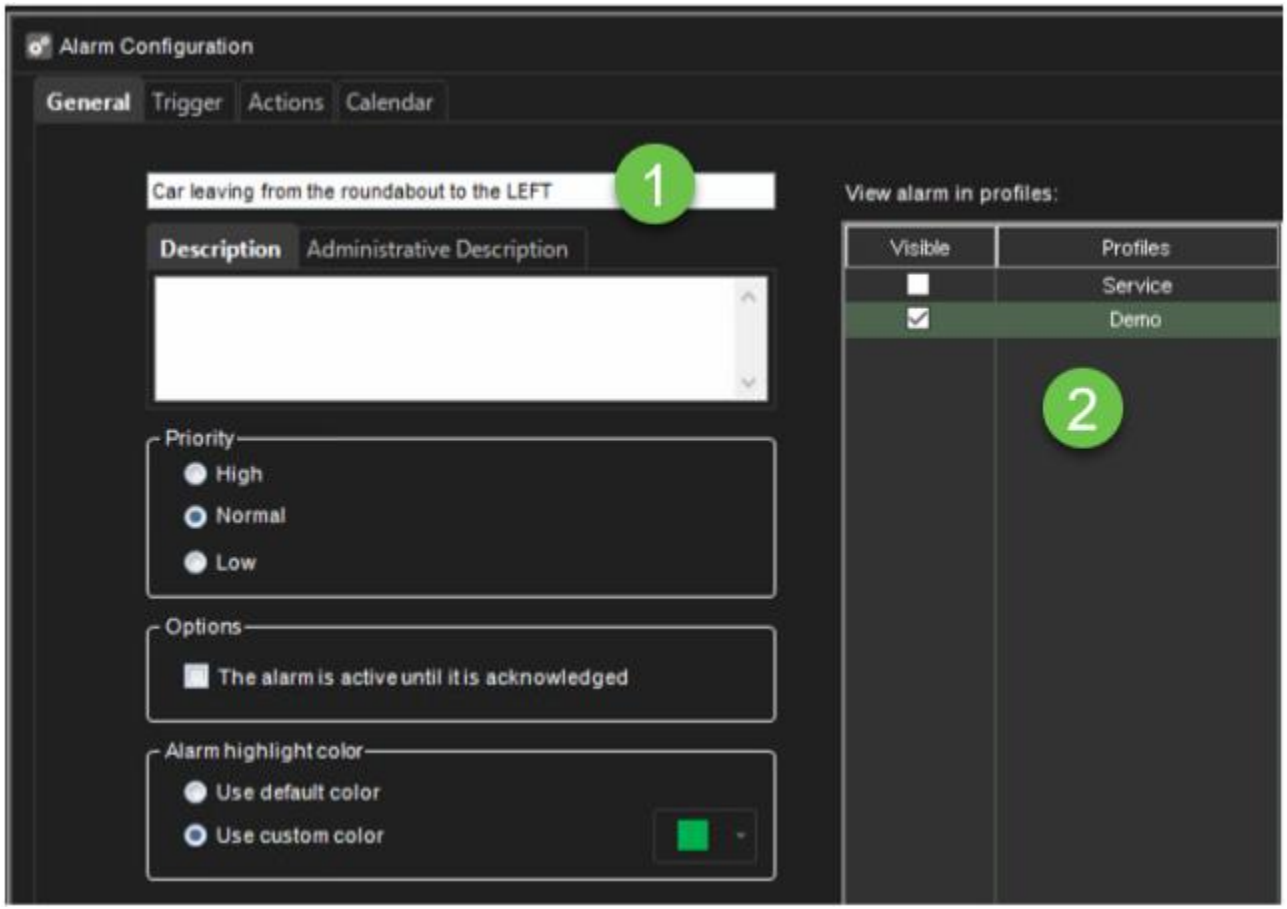
1. Go to the **VMS servers** tab
2. Click **Alarms**
3. Click **New Alarm**

MIRASYS

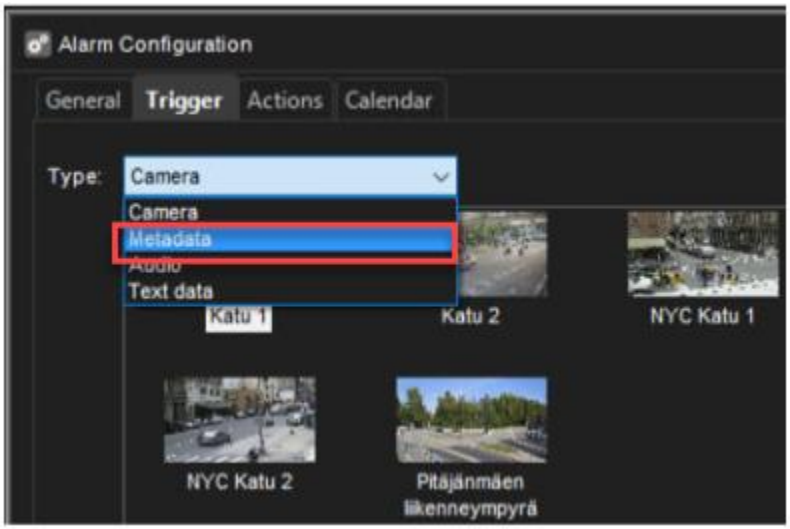


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

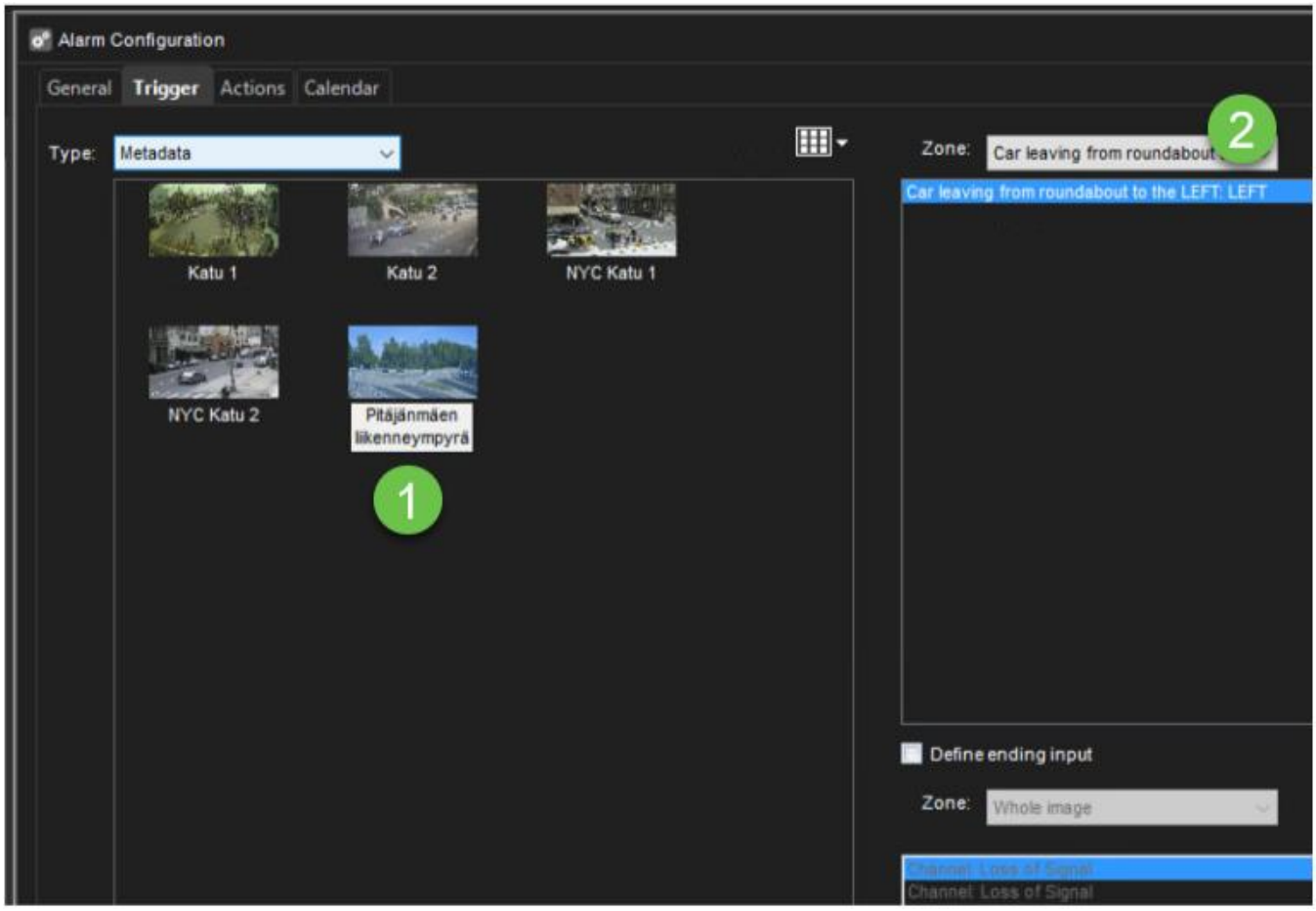
4. Enter the name of the alarm
5. Select the **View alarm in profiles**
6. Go to the **Trigger** tab



7. Select **Type**: **Metadata**

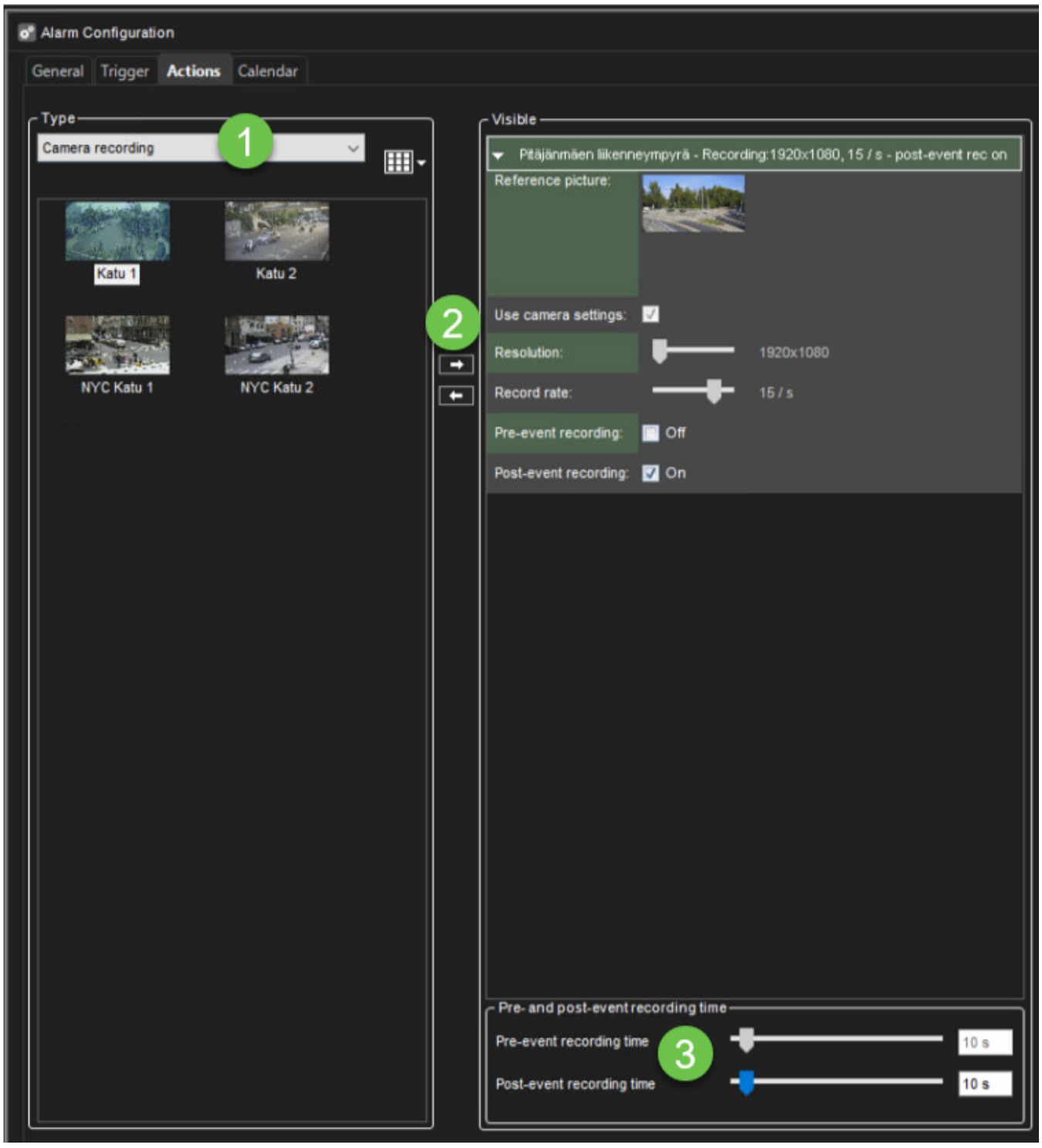


8. Select the correct camera from the list
9. Select zone
10. Go to the **Actions** tab



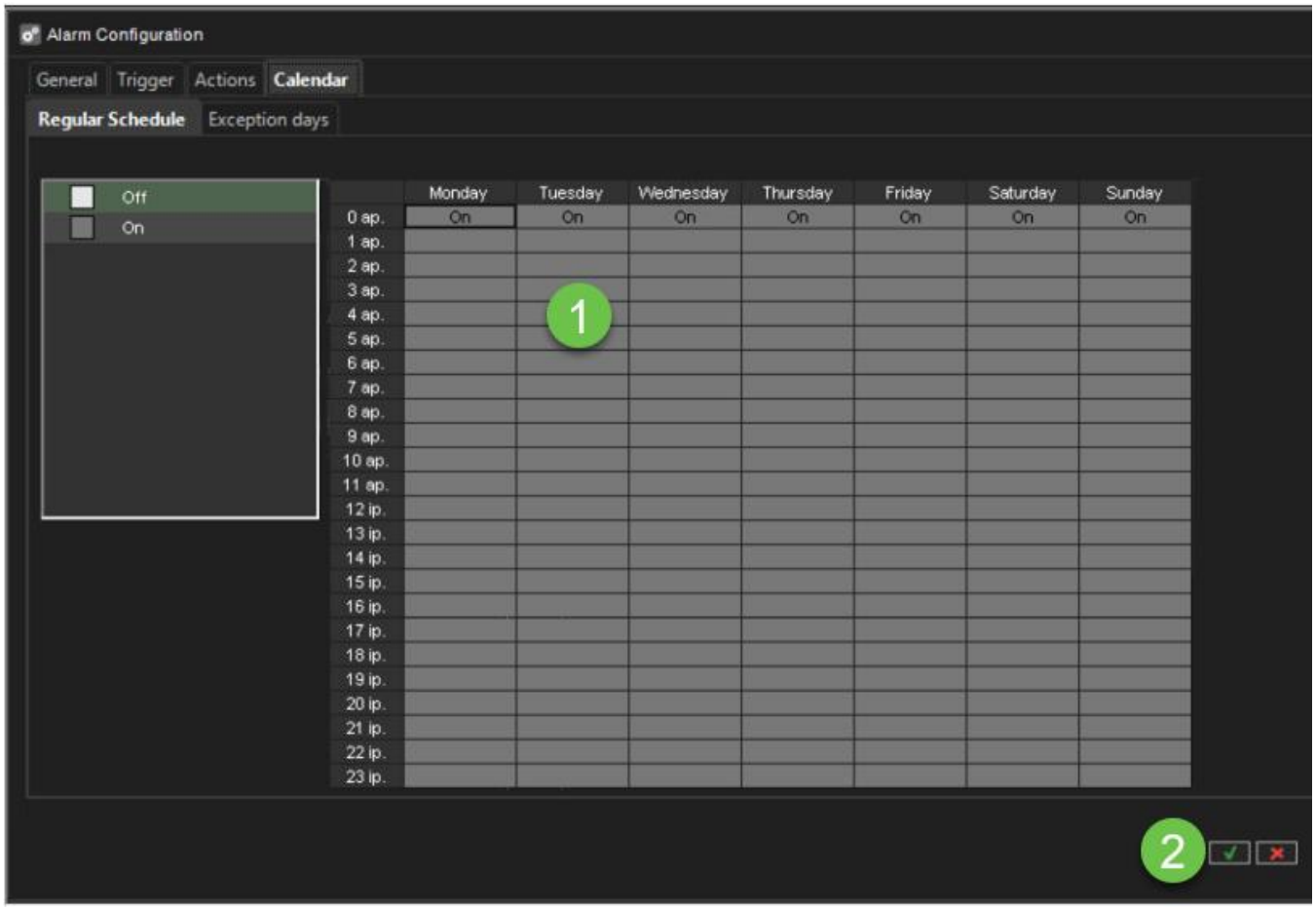
11. Select needed actions
12. Add them to the Visible list
13. Set Pre - and post-event recording time, if needed
14. Go to the **Calendar** tab

MIRASYS

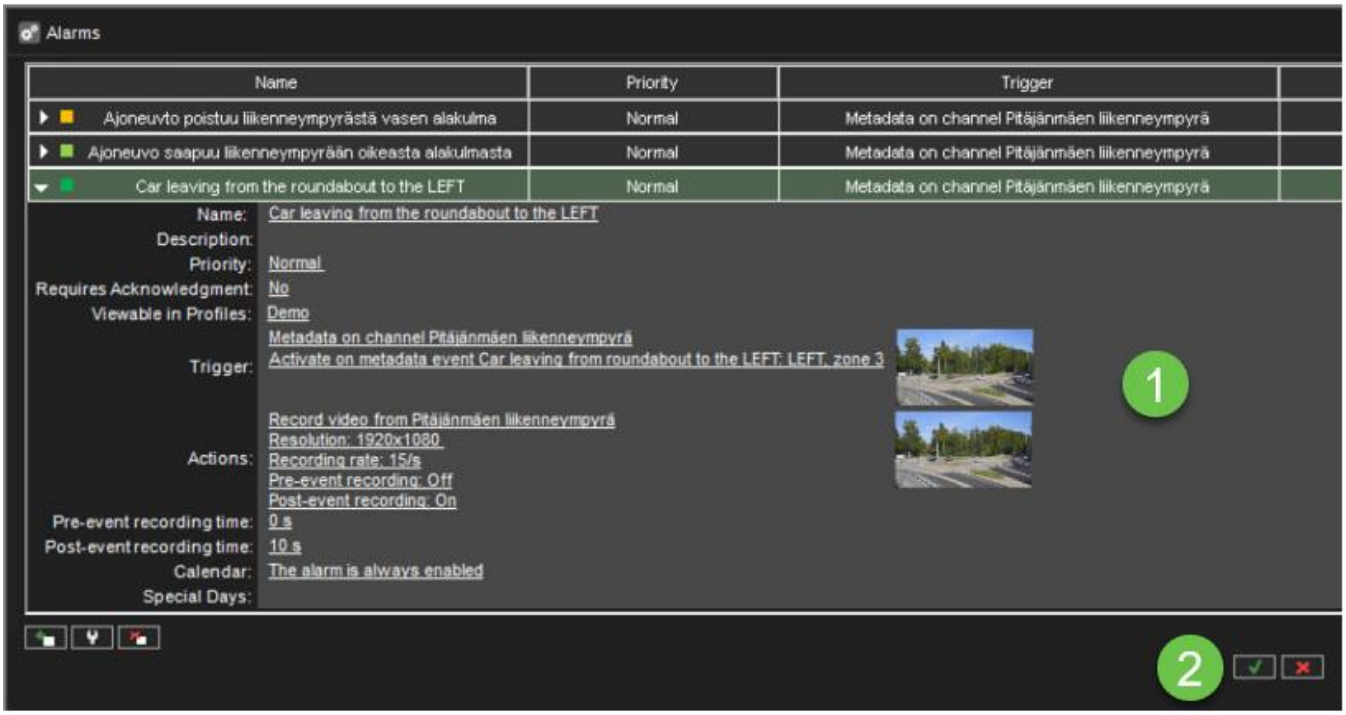


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

15. Set alarm schedule
16. Click OK

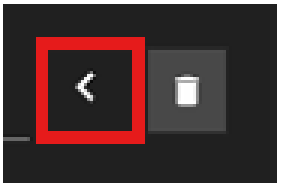


17. Check alarm configuration
18. Click OK to finalize alarm creation



8.18 CONFIGURATION

1. Open System Manager
2. Select **VCA Settings** for the desired server
3. Click the **Menu** button in the top left corner
4. Select **Settings**
5. Select **Edit Sources**
6. Click **Add Other Source +**
7. Select **Schedule**
8. Give a name for the schedule and click the arrow icon to open the details of the source



1. Select the day and time for activation

2. Go to **Rules** from View Channels by clicking on the desired camera
3. Select **Add Rule +** and select Counter from the dropdown menu
4. Add the schedule you created earlier by clicking **Add Reset Input +**

The VCA Counter is reset when this input is activated.

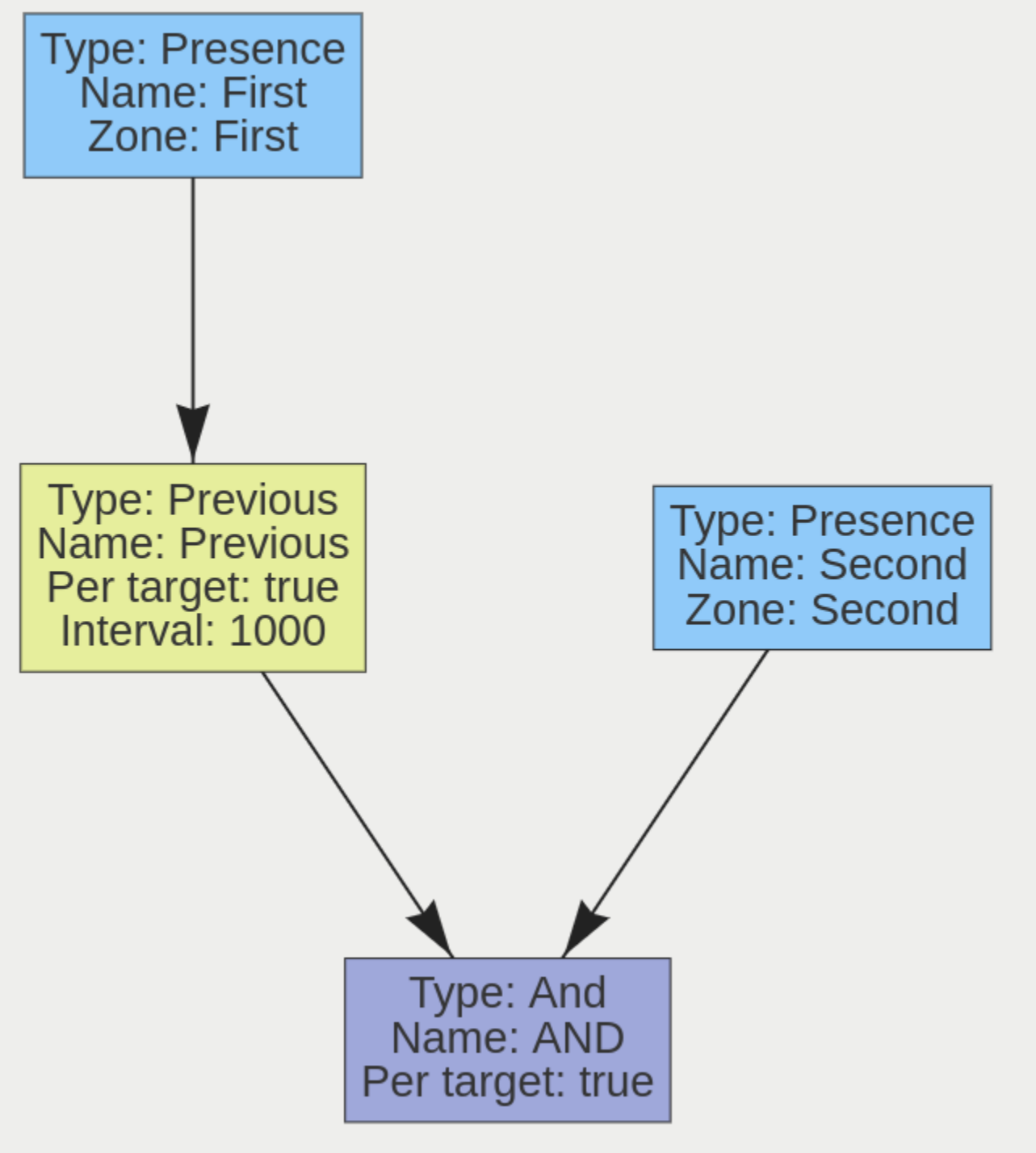
All these steps are done in the **VCA Settings** menu.

8.19 Combined Rule Examples

- Double-knock Rule
- Presence in A or B

8.19.1 Double-knock Rule

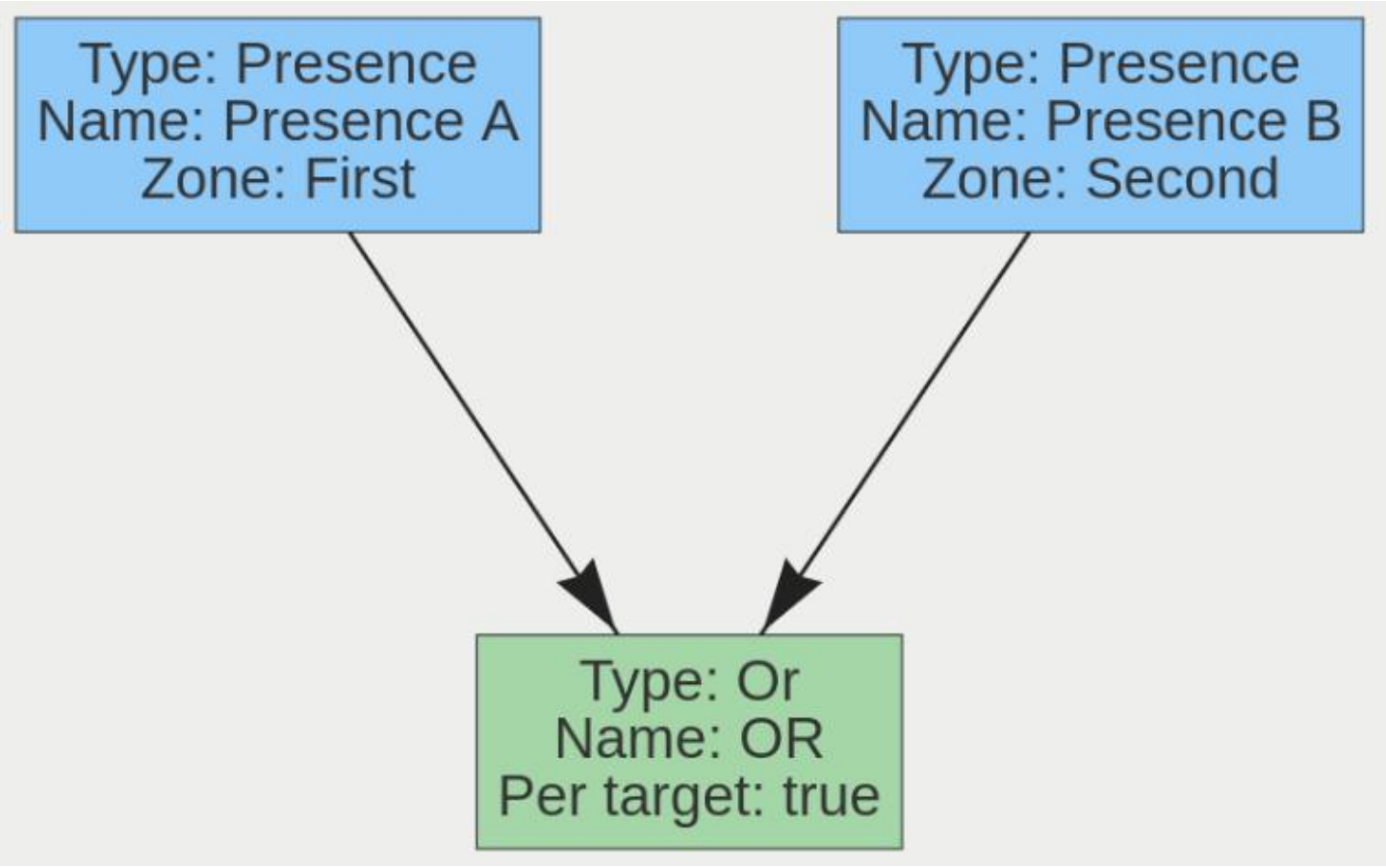
The "double-knock" logical rule triggers when an object enters a zone which had previously entered another defined, zone within a set period of time. The interval on the Previous rule decides how much time can elapse between the object entering the first and second zone. The graph for a double-knock 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.

8.19.2 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.

8.20 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