MIRASYS

Mirasys AI-Leitfaden

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

MIRASYS

1 CONTENTS

2 Mirasys Object Recognition (OR) 9
2.1 Objekterkennung Einführung 9
2.2 OR Service-Installation 9
2.2.1 Anforderungen 9
2.2.2 NVIDIA-Bibliotheken 10
2.2.3 OR Installation 10
2.2.4 Aktualisierung des ODS-Dienstes 11
2.2.5 ODS Installation 12
2.3 OR-Leistung 13
2.3.1 Testmaschine 13
2.3.2 Testergebnisse 14
2.3.3 Ergebnisse von Leistungstests für Personen 15
3 Mirasys List Management 16
3.1 Mirasys List Management Einleitung 16
3.2 Installation von LM Service 17
3.2.1 Voraussetzungen 17
3.2.2 Aktualisierung des List Management Service 17
3.2.3 Installation 17
3.3 PostgreSQL 15 Upgrade auf PostgreSQL 16 Version 25
3.3.1 Dieser Leitfaden gilt für 25
3.3.2 Anforderungen 26
3.3.3 Wie man ein Upgrade durchführt 26
4 Mirasys Face Recognition 40
4.1 Einführung Face Recognition 40
4.2 FR-Service-Installation 40
4.2.1 Anforderungen 41
4.2.2 NVIDIA-Bibliotheken 41
4.2.3 FR Installation 42
4.3 FR Datenschutz-Masken 50
4.4 FR-Verarbeitung, Ereignisse und Erkennung 50

4.4.1 Geräte 50
4.4.2 FR-Veranstaltungen 51
4.4.3 Visualisierung des erkannten Gesichts 51
4.5 FR Alarmauslöser und Konfiguration 51
4.5.1 Alarmauslöser 51
4.5.2 FR-Konfiguration 51
4.6 FR-Leistung 51
4.6.1 Testcomputer-Hardware 51
4.6.2 Version 9.10 51
4.6.3 Version 9.9.6 53
5 Mirasys License Plate Recognition (LPR) 54
5.1 Einführung License Plate Recognition 54
5.2 LPR-Service-Installation 54
5.2.1 Anforderungen 55
5.2.2 NVIDIA-Bibliotheken 55
5.2.3 LPR-Installation 56
5.3 LPR-Datenschutz-Masken 64
5.4 Land-Erkennung 64
5.4.1 Erkennung von Ländern mit Nummernschildern 64
5.4.2 Typen von Nummernschildern 65
5.5 LPR in Eurasien: Unterstützte Länder 65
5.5.1 Vorwahlen 65
5.5.2 Liste der unterstützten Länder in Eurasien 66
5.6 LPR auf dem amerikanischen Kontinent: Unterstützte Länder 68
5.6.1 Länder und Staaten 68
5.7 LPR-Ereignisse, Ereignisse und Erkennung 71
5.7.1 Geräte 71
5.7.2 LPR-Ereignisse 71
5.7.3 Visualisierung des erkannten Kennzeichens 71
5.8 LPR Alarmauslöser und Konfiguration 71
5.8.1 Alarmauslöser 71

5.8.2 LPR-Konfiguration....71
5.9 LPR-Leistung....71
5.9.1 Testmaschine....71
5.9.2 Durchführung des Tests....71
5.9.3 Testergebnisse....72
5.9.4 CPU....72
5.9.5 NVIDIA GPU....73
5.9.6 INTEL GPU....75
6 Easy LPR....76
6.1 Lizenzierung....76
6.2 Konfigurationsprozess....77
6.2.1 Konfigurationsprozess....77
6.2.2 Kameraspezifische Konfigurationen....77
6.3 Aktivieren von Easy LPR....80
7 Kamera-Installation LPR-Leitfaden....82
7.1 Es wird empfohlen, die Kamera in der Mitte des Fahrzeugs zu installieren....82
7.2 Wenn die Kamera am Straßenrand oder auf der Fahrbahn installiert ist, sollte der Winkel 30 Grad nicht überschreiten....83
7.3 Die Kamera sollte höher als die Scheinwerfer des Fahrzeugs angebracht werden, damit die Scheinwerfer des Fahrzeugs nicht direkt auf die Kamera gerichtet sind....84
7.4 Stellen Sie sicher, dass das Nummernschild mindestens 120 Pixel breit und mindestens 50 Pixel hoch ist. 84
7.5 Der Neigungswinkel des Kennzeichens muss innerhalb von +/- 10 Grad liegen....84
7.6 LPR-Einstellungen in der Anwendung System Manager....85
7.6.1 Festlegung der Region von Interesse....85
7.6.2 Ermöglichung der Anerkennung von Ländern....86
7.7 Allgemeine Probleme und Lösungen....86
7.7.1 Unvollständiges Nummernschild....86
7.7.2 Blickwinkel macht Nummernschilder unleserlich....87
7.7.3 Scheinwerfer anderer Fahrzeuge reflektieren vom Nummernschild....87
7.7.4 Das Nummernschild ist zu klein....87
7.7.5 Das Nummernschild ist unscharf....87

7.7.6 Das Nummernschild ist überbelichtet 87
8 Mirasys VCA-Leitfaden 88
8.1 Über Mirasys VCA 88
8.1.1 Objektverfolgung anhand von Bewegungsdaten 88
8.1.2 Zählung mittels Tripwire 88
8.1.3 Erkennung von Objektverhalten und -attributen 89
8.1.4 Verwandte Analyseoptionen 89
8.2 Kurzanleitung für VCA 89
8.3 Voraussetzungen für Mirasys VCA 90
8.3.1 VCA Core HW GUID-Datei exportieren 91
8.3.2 Aktivierung von VCA-Lizenzen 91
8.3.3 Einstellung der Auflösung und der Aufzeichnungsrate 94
8.3.4 VCA-Stream auswählen 94
8.3.5 Aktivieren des VCA-Core für die Kameras 95
8.4 Unterstützte Betriebssysteme 96
8.5 VCA-Einstellungen im System Manager 97
8.5.1 View Channels 97
8.5.2 Einstellungen 98
8.5.3 Edit Sources (Quellen bearbeiten) 99
8.5.4 Licenses (Lizenzen) 100
8.5.5 Support (Unterstützung) 100
8.6 Mirasys VCA Deep Learning 101
8.6.1 Anforderungen 101
8.6.2 Installation 101
8.7 Mirasys VCA-Lizenzserver 103
8.7.1 Port 103
8.7.2 Installation 103
8.8 Cloud-Lizenzierung 110
8.9 VCA-Kanaleinstellungen 110
8.9.1 Initialisierung 111
8.9.2 VCA Trackers 112

8.9.3 VCA-Zonen 120
8.9.4 VCA-Kalibrierung 124
8.9.5 VCA-Klassifizierung 132
8.9.6 VCA Burnt-in Anmerkungen 134
8.9.7 VCA-Regeln 136
8.9.8 VCA - Deep-Learning-Filter 177
8.10 VCA - Filter 178
8.10.1 Geschwindigkeitsfilter 179
8.10.2 VCA-Filter – Objektfilter 182
8.10.3 VCA-Filter – Farbfilter 185
8.10.4 VCA-Filter – Retrigger-Filter 189
8.10.5 VCA-Filter – Deep-Learning-Filter 190
8.11 Arten von bedingten Regeln 194
8.11.1 VCA - And 194
8.11.2 VCA - Continuously 195
8.11.3 VCA - Counter 197
8.11.4 VCA - Not 201
8.11.5 VCA - Or 202
8.11.6 VCA - Previous 204
8.11.7 VCA - Repeatedly 205
8.12 Weitere Quellen 206
8.12.1 VCA - HTTP 206
8.12.2 VCA - Schedule 206
8.13 VCA – Manipulationserkennung 208
8.13.1 So aktivieren Sie die Manipulationserkennung 208
8.13.2 So erstellen Sie einen Alarm anhand der Manipulationserkennung 210
8.14 So erstellen Sie Regeln 212
8.15 So testest du Regeln 215
8.16 So zeigen Sie VCA-Ereignisse im Mirasys Spotter an 218
8.17 So erstellen Sie einen Alarm anhand eines VCA-Ereignisses 219
8.18 Konfiguration 224

8.19 Beispiele für kombinierte Regeln 225
8.19.1 VCA - Double-Knock-Regel 225
8.19.2 Präsenz in Gebiet A oder Gebiet B 226
8.20 GPU-Leistung 227
9 Vaidio-Integration 228
9.1 Unterstützte Funktionen 229
9.2 Lizenzmodell 229
9.3 Optionale Datenbanknutzung 229
9.4 Versionskompatibilität 230
9.5 Anforderungen 230
9.5.1 Anforderungen an den Integrationsdienst 230
9.5.2 Anforderungen an das „Forensic Search“-Plugin 232
9.5.3 Vaidio-Anforderungen 232
9.6 Vaidio-Installation 232
9.6.1 Installation des Vaidio-Integrationsdienstes 233
9.6.2 Installation und Konfiguration des Forensic Search-Plugins in Spotter 243
9.7 Funktionen von Vaidio 245
9.7.1 So öffnen Sie das Plugin „Forensic Search“ 245
9.7.2 Auswahl von Kameras und Zeiträumen 246
9.7.3 Überprüfen der Suchergebnisse 246
9.7.4 Gesichtssuche (Face search) 246
9.7.5 Objektsuche (Object search) 247
9.7.6 Kfz-Kennzeichen-Suche (License plate search) 247
9.7.7 Kameraübergreifende Verfolgung (Cross-camera tracking) 248
9.7.8 Live-Monitor (Live monitor) 248
9.7.9 Wiedergabe und Storyboard 248
9.7.10 Exportieren von Videomaterial 248

MIRASYS

Tel +358 (0)9 2533 3300

Email info@mirasys.com

https://www.mirasys.com

2 MIRASYS OBJECT RECOGNITION (OR)

2.1 OBJEKTERKENNUNG EINFÜHRUNG

Die Objekterkennungssuche ermöglicht die Suche nach Merkmalen sowohl von Personen als auch von Fahrzeugen in Aufzeichnungen. Die Objekterkennungssuche verwendet die folgenden Kriterien: wo (welche Kameras), wann (Zeitintervall) und was (Personen oder Fahrzeuge und deren Merkmale).

Bei Personen wird nach der Farbe der Oberkörperbekleidung (schwarz, weiß, grau, blau, grün, rot, gelb), der Farbe der Unterkörperbekleidung (schwarz, blau, weiß, grau, braun, grün) und danach gesucht, ob die Person eine Tasche trägt (allgemein) und ob sie eine Kopfbedeckung trägt (allgemein).

Fahrzeuge können nach Typ (PKW, Motorrad, Lieferwagen, LKW, Fahrrad oder Bus) und Farbe (schwarz, blau, braun, grau, grün, orange, rot, weiß, gelb) durchsucht werden.

Die zu erkennenden Objekte können in den Einstellungen für die Objekterkennung ausgewählt werden. Die Objekterkennung erkennt nur die ausgewählten Objekte, wodurch die Ressourcennutzung effektiver wird. Die folgenden Einstellungsoptionen sind verfügbar:

- Personenattribute aktivieren
- Fahrzeugattribute aktivieren
- Identifizierung von Personenähnlichkeiten aktivieren

2.2 OR SERVICE-INSTALLATION

Für OR müssen Sie die Pakete ORService und ODSService installieren. OR übernimmt die Objekterkennung, und ODS speichert die Objekterkennungsereignisse in PostgreSQL.

2.2.1 Anforderungen

- Administratorrechte
- Object Recognition-Lizenz auf dem VMS-Server
- RTSP-Lizenzfunktion auf dem VMS-Management-Server und dem VMS-Server
- Die erforderlichen NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind installiert

Der Object Data Store Service verfügt über einen Cache für die Ähnlichkeitssuche, um die Ähnlichkeitssuche zu beschleunigen, der ein- oder ausgeschaltet werden kann.
Hinweis: Die Verwendung des Caches erhöht den Speicherverbrauch.
Sie können den Ähnlichkeitssuch-Cache bei der Installation des Dienstes aktivieren oder deaktivieren.

Die NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind nicht im OR-Installationsprogramm enthalten. Das Installationsprogramm erkennt die NVIDIA-Bibliotheksinstallationsprogramme im Unterordner „NVIDIA“ und installiert die Bibliotheken automatisch, sofern sie gefunden werden.

2.2.2 NVIDIA-Bibliotheken

Die erforderlichen NVIDIA-Bibliotheken sollten vor der Installation des OR-Dienstes installiert werden, sofern sie noch nicht vorhanden sind. Für die Installation des OR-Dienstes müssen die folgenden NVIDIA-Bibliotheken für Windows installiert sein:

- 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 für Windows 10, 11, Server 2022 und CUDA 12.0 bis 12.9 – ZIP-Paket: https://developer.nvidia.com/tensorrt/download/10x

2.2.2.1 Installation der NVIDIA-Bibliotheken

1. Laden Sie das Installationsprogramm für den Mirasys OR-Dienst herunter und speichern Sie es in einem Ordner auf Ihrem Computer
2. Erstellen Sie einen Unterordner „NVIDIA“
3. Laden Sie die oben genannten NVIDIA-Bibliotheken herunter.
4. Speichern Sie die heruntergeladenen NVIDIA-Bibliotheken im Unterordner „NVIDIA“.
5. Führen Sie das Installationsprogramm für den Mirasys OR-Dienst aus.
    a. Das Installationsprogramm für den Mirasys OR-Dienst installiert automatisch die NVIDIA-Bibliotheken, die es im Unterordner „NVIDIA“ findet, bevor der Dienst installiert wird.
6. Befolgen Sie die Installationsanweisungen, um die Installation abzuschließen.

2.2.3 OR Installation

Das Installationsprogramm enthält einen Schritt, in dem Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren müssen. Sie müssen bestätigen, dass Sie die in der Vereinbarung aufgeführten Bedingungen akzeptieren, um mit der Installation fortzufahren.

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie dieses Beispiel in den Ordner `C:\temp`.
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Klicken Sie auf **Install** (Installieren), um fortzufahren.

5. Klicken Sie auf **Next** (Weiter), um fortzufahren.
6. Aktivieren Sie das Kontrollkästchen **I accept the terms in the License Agreement** und klicken Sie auf **Next**.
7. Ändern Sie bei Bedarf den Installationsort, wenn nicht, klicken Sie auf **Next** (Weiter), um fortzufahren.
    a. Ändern Sie Dienstadresse, den HTTP-Port des Dienstes, die Adresse und den Port des Hauptservers sowie die Adresse und den Port der Ereigniswarteschlange, falls erforderlich.
    b. Ändern Sie die Dienstadresse (Service Address) so, dass sie für Client-Anwendungen erreichbar ist. Standardmäßig ist die Dienstadresse die erste erkannte IP-Adresse des Rechners.

Der HTTP-Port, auf dem der OR-Dienst gehostet wird, ist standardmäßig 8092. Ändern Sie den Port, falls der Standardport für einen anderen Zweck reserviert ist.
Der Hauptserver verwendet standardmäßig Port 8082. Legen Sie die Adresse und den Port des Hauptservers fest, damit der OR-Dienst eine Verbindung zum richtigen Hauptserver herstellen kann.
Die Ereigniswarteschlange (Event queue) verwendet standardmäßig Port 5672. Die Ereigniswarteschlange wird bei der Installation des ODS-Dienstes mitinstalliert, wobei der verwendete Port der Ereigniswarteschlange festgelegt wird. Legen Sie die Adresse der Ereigniswarteschlange auf den Rechner fest, auf dem der ODS-Dienst installiert ist.

1. Klicken Sie auf **Next** (Weiter), um fortzufahren.
2. Wählen Sie mindestens eines der Geräte aus, die für den OR verwendet werden sollen:
    - CPU
    - Intel-GPU
    - NVIDIA-GPU
3. Klicken Sie auf **Install** (Installieren), um fortzufahren, und warten Sie.

Die Installation wird einige Zeit in Anspruch nehmen, bis sie abgeschlossen ist.
Die Erstellung von Modellen kann bis zu 30 Minuten dauern. Dies hängt davon ab, wie leistungsfähig die Grafikkarte ist, die verwendet wird.

1. Klicken Sie auf **Finish** (Fertigstellen), um fortzufahren.
2. Klicken Sie auf **Close** (Schließen), um die Installation zu beenden.

2.2.4 Aktualisierung des ODS-Dienstes

Bevor Sie den Object Data Store-Dienst auf eine neuere Version aktualisieren, erstellen Sie im System Manager eine vollständige Sicherung und deinstallieren Sie den RabbitMQ-Server sowie Erlang OTP – diese können in den Windows-Einstellungen oder über die Systemsteuerung deinstalliert werden. Nach der Deinstallation der alten ODS-Version und der zusätzlichen Komponenten können Sie mit der Installation gemäß den nachstehenden

Anweisungen fortfahren. Beachten Sie, dass die Deinstallation nur einmal durchgeführt werden muss; es ist nicht erforderlich, den RabbitMQ-Server und Erlang OTP zu deinstallieren, wenn dies bereits durch den List Management Service oder in der Aktualisierungsphase des Object Data Storage Service erfolgt ist.

Die erforderliche Mindestversion von RabbitMQ ist 3.13.0. Die ODS-Installation umfasst Erlang 27.3.4.6 und RabbitMQ 4.2.0.

2.2.5 ODS Installation

Das Installationsprogramm enthält einen Schritt, in dem Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren müssen. Sie müssen bestätigen, dass Sie die in der Vereinbarung aufgeführten Bedingungen akzeptieren, um mit der Installation fortzufahren.

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie diese Datei z. B. in den Ordner „C:\temp“
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Legen Sie das Passwort für die PostgreSQL-Datenbank fest
    a. Das Standardpasswort lautet „postgres“

PostgreSQL wird zusammen mit dem ODS-Dienst installiert, sofern es nicht bereits zuvor installiert wurde.

Derzeit wird kein separater PostgreSQL-Server unterstützt, mit Ausnahme einer bestehenden Installation von PostgreSQL Version 15 oder 16

1. Klicken Sie auf **Install** (Installieren), um fortzufahren.
2. Klicken Sie auf **Next** (Weiter), um fortzufahren.
3. Ändern Sie bei Bedarf den Installationsort, wenn nicht, klicken Sie auf **Next** (Weiter), um fortzufahren.
    a. Ändern Sie die Dienstadresse, den HTTP-Port des Dienstes, die Adresse und den Port des Hauptservers sowie die Adresse und den Port der Ereigniswarteschlange, falls erforderlich.
    b. Ändern Sie die Dienstadresse (Service Address) so, dass sie für Client-Anwendungen erreichbar ist. Standardmäßig ist die Dienstadresse die erste erkannte IP-Adresse des Rechners.

Der HTTP-Port, auf dem der ODS-Dienst gehostet wird, ist standardmäßig 8093. Ändern Sie den Port, falls der Standardport für einen anderen Zweck reserviert ist.

Der Hauptserver verwendet standardmäßig Port 8082. Legen Sie die Adresse und den Port des Hauptservers fest, damit der ODS-Dienst eine Verbindung zum richtigen Hauptserver herstellen kann.
Die Ereigniswarteschlange (Event queue) verwendet standardmäßig Port 5672. Die Ereigniswarteschlange wird zusammen mit dem ODS-Dienst installiert. Ändern Sie den Port der Ereigniswarteschlange, falls der Standardport für einen anderen Zweck reserviert ist.

1. Klicken Sie auf **Next** (Weiter), um fortzufahren.
2. Klicken Sie auf **Install** (Installieren), um fortzufahren, und warten Sie.
3. Klicken Sie auf **Finish** (Fertigstellen), um fortzufahren.
4. Klicken Sie auf **Close** (Schließen), um die Installation zu beenden.

2.3 OR-Leistung

2.3.1 Testmaschine

Die Leistungstests zur Objekterkennung wurden auf einem speziellen Rechner durchgeführt, auf dem ausschließlich der Objekterkennungsdienst mit folgender Hardware läuft:

- 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.

Während des Tests wurden die folgenden Kennzahlen erfasst:

- Eingangsbildrate
- Ausgangsbildrate
- Speicherauslastung (RAM)
- CPU-Auslastung
- GPU-Auslastung für die Modellinterferenz
- GPU-Auslastung für die Videodekomprimierung
- GPU-Speicherauslastung

Die Tests wurden mit einem H.264-komprimierten Videoclip mit einer Auflösung von 1920×1080 durchgeführt.

2.3.2 Testergebnisse

2.3.2.1 Leistungstestergebnisse für Fahrzeuge

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

Streams	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	GPU Speicher
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	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	GPU Speicher
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

Streams	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	GPU Speicher
16	55	55	21%	5.5 GB	98%	7%	9.2 GB

2.3.2.2 Intel GPU: Intel UHD Graphics 750

Streams	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	Intel GPU	Intel GPU Speicher
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 Ergebnisse von Leistungstests für Personen

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

Streams	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	GPU Speicher
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	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	GPU Speicher
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	Eingangsbildrate	Ausgangsbildrate	Prozess-CPU	Prozessspeicher	NVIDIA GPU	NVIDIA decode	Intel GPU	Intel GPU Speicher
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

Diese Tests dienen lediglich als Anhaltspunkt und sind möglicherweise nicht direkt auf Produktionssysteme übertragbar.

3 MIRASYS LIST MANAGEMENT

3.1 MIRASYS LIST MANAGEMENT EINLEITUNG

List Management (LM) dient der Verarbeitung von Gesichtserkennungs- (FR) und Kennzeichenerkennungsereignissen (LPR) durch Abgleich von erkannten Gesichtern und Kennzeichen mit einer Identität und Identitätsliste. Der LM-Dienst dient zum Speichern von Identitäten und Identitätslisteninformationen, zum Empfangen und Speichern von LPR- und FR-Ereignissen, zum Senden von LPR- und FR-Ereignissen an Clients, zum Durchführen von Suchen in gespeicherten Ereignissen und zum Senden von LPR- und FR-Ereignissen an den VMS-Server zur Verarbeitung.

Der LM-Dienst hat die folgenden Fähigkeiten:

- Speichern von Identitäten und Identitätslisten in der Datenbank
- Empfangen und Speichern von LPR- und FR-Ereignissen in der Datenbank
- Abgleich von erkannten Nummernschildern und Gesichtern mit definierten Identitäten und Identitätslisten
- Suche nach LPR- und FR-Ereignissen in der Datenbank anhand von Suchparametern
- Senden von LPR- und FR-Ereignissen in Echtzeit für Clients und Rekorder
- Senden von LPR- und FR-Ereignissen an den VMS-Server zur Verarbeitung
- Benachrichtigung von Kunden und Rekordern über Änderungen in Identitäten und Identitätslisten
- Ermöglicht die Integration von Kennzeichen- und Gesichtserkennungen

Der Listenverwaltungsdienst hat ein separates Installationsprogramm, so dass er auf einem separaten Server oder auf einem VMS-Server ausgeführt werden kann.

Die Einstellungen für die Listenverwaltung (Identitäten und Identitätslisten) können in den Systemmanager-Einstellungen für die Listenverwaltung und im Plugin Spotter Smart List Management verwaltet werden.

3.2 INSTALLATION VON LM SERVICE

3.2.1 Voraussetzungen

- Administratorrechte
- LM-service ist ab Version 9.6.0 enthalten

3.2.2 Aktualisierung des List Management Service

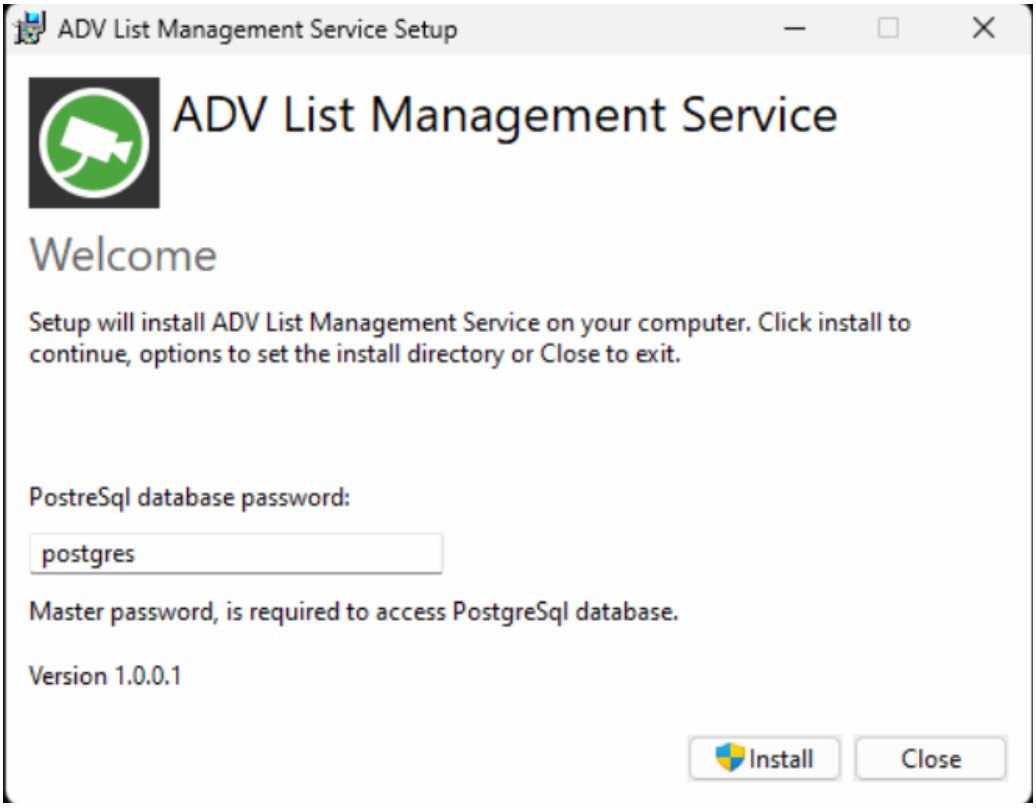
Bevor Sie den LM-Dienst auf eine neuere Version aktualisieren, erstellen Sie im System Manager eine vollständige Sicherung und deinstallieren Sie den RabbitMQ-Server sowie Erlang OTP – diese können in den Windows-Einstellungen oder über die Systemsteuerung deinstalliert werden. Nach der Deinstallation der alten LM-Version und der zusätzlichen Komponenten können Sie mit der Installation gemäß den nachstehenden Anweisungen fortfahren. Beachten Sie, dass die Deinstallation nur einmal durchgeführt werden muss; es ist nicht erforderlich, den RabbitMQ-Server und Erlang OTP zu deinstallieren, wenn dies bereits durch den List Management Service oder in der Aktualisierungsphase des Object Data Storage Service erfolgt ist.

Die erforderliche Mindestversion von RabbitMQ ist 3.13.0. Die LM-Installation umfasst Erlang 27.3.4.6 und RabbitMQ 4.2.0.

3.2.3 Installation

Das Installationsprogramm enthält einen Schritt, in dem Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren müssen. Sie müssen bestätigen, dass Sie die in der Vereinbarung aufgeführten Bedingungen akzeptieren, um mit der Installation fortzufahren.

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie dieses Beispiel in den Ordner „C:\temp“.
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Klicken Sie auf **Install**, um fortzufahren.
    a. Ändern Sie das Passwort für die PostgreSQL-Datenbank

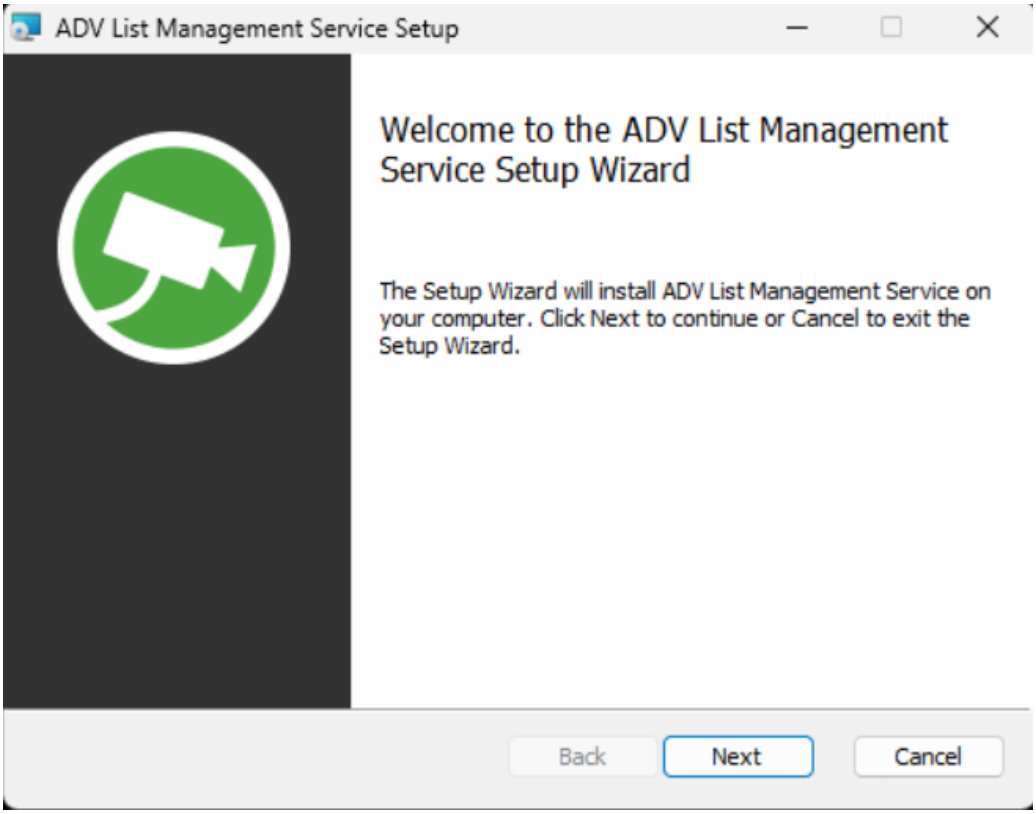


1. Warten Sie, bis PostgreSQL installiert ist.
    a. Möglicherweise müssen Sie im Laufe der Installation Firewall-Regeln anwenden.

PostgreSQL wird zusammen mit dem LM-Dienst installiert, sofern es nicht bereits zuvor installiert wurde.

Derzeit wird kein separater PostgreSQL-Server unterstützt, mit Ausnahme einer bestehenden Installation von PostgreSQL Version 15 oder 16.

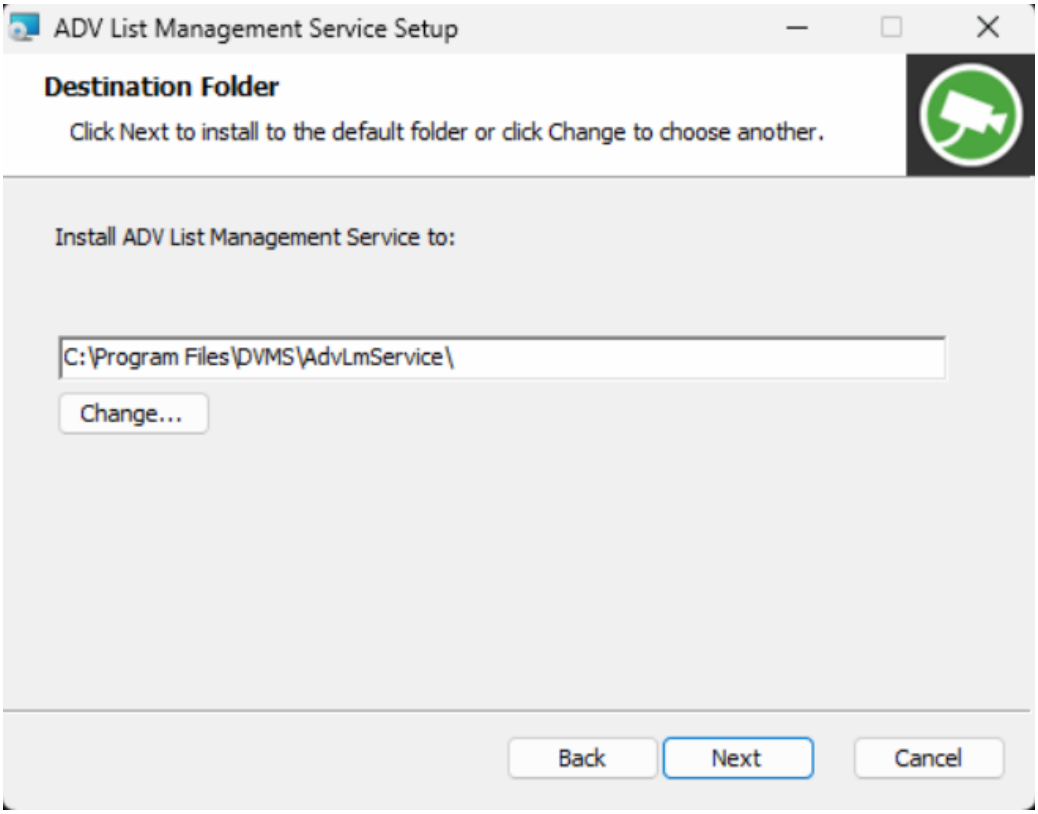
1. Klicken Sie auf **Next**, um fortzufahren.



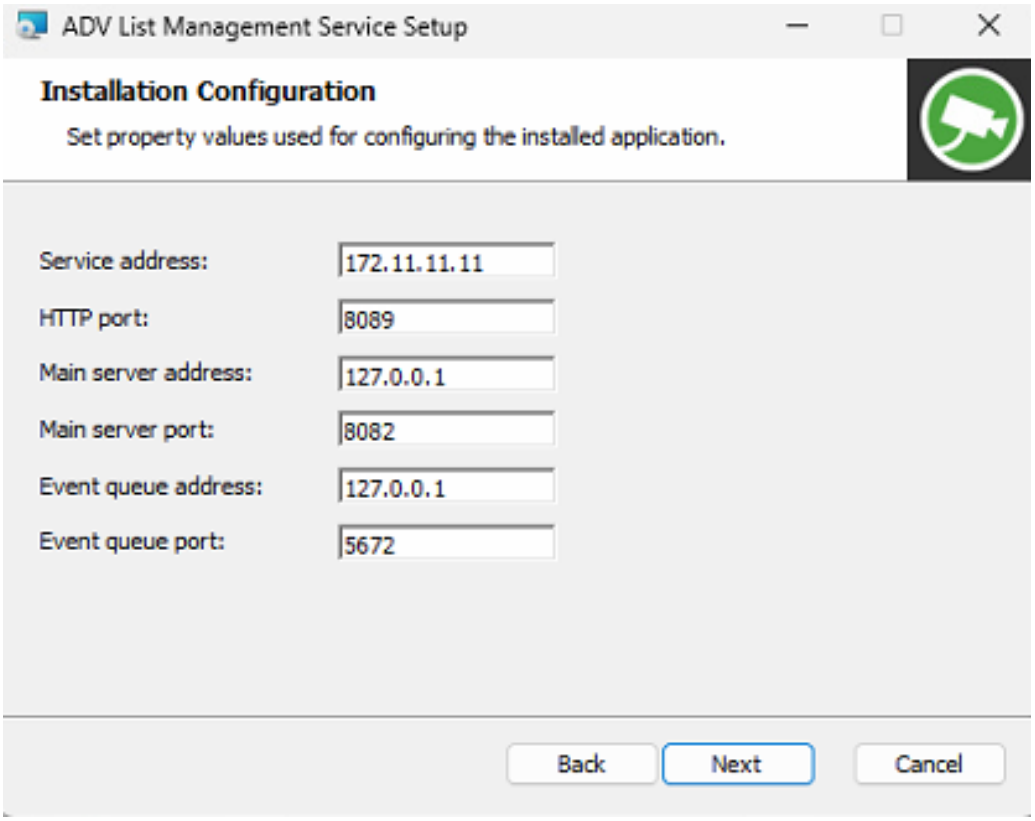
1. Aktivieren Sie das Kontrollkästchen **I accept the terms in the License agreement** („Ich akzeptiere die Bedingungen der Lizenzvereinbarung“) und klicken Sie auf **Next**



1. Ändern Sie gegebenenfalls den Installationsort; andernfalls klicken Sie auf **Next**, um fortzufahren.

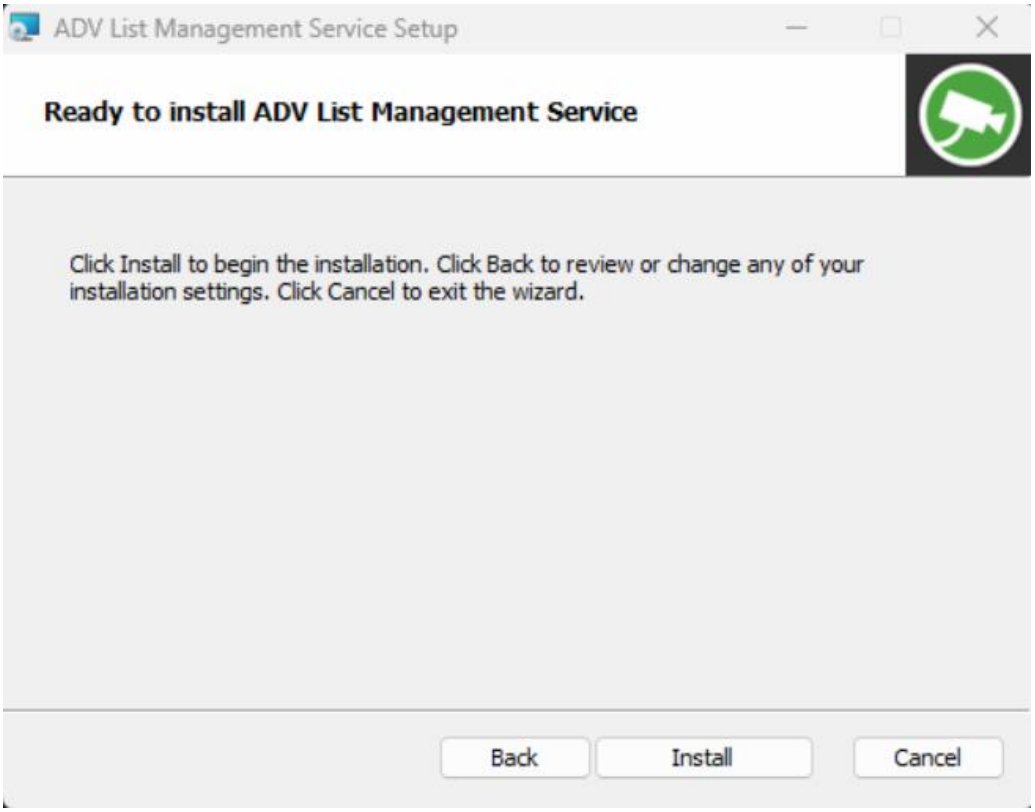


1. Ändern Sie die Ports und Adressen bei Bedarf.
    a. Wenn Sie den List Management Service auf einem anderen Server installieren, müssen Sie diese Angaben ändern.
    b. Die Adresse der Ereigniswarteschlange entspricht der Adresse, unter der der List Management Service installiert ist. Behalten Sie die Standardeinstellung bei.
    c. Ändern Sie die Dienstadresse (Service Address) so, dass sie für Client-Anwendungen erreichbar ist. Standardmäßig ist die Dienstadresse die erste erkannte IP-Adresse des Rechners.
2. Klicken Sie auf **Next**, um fortzufahren.

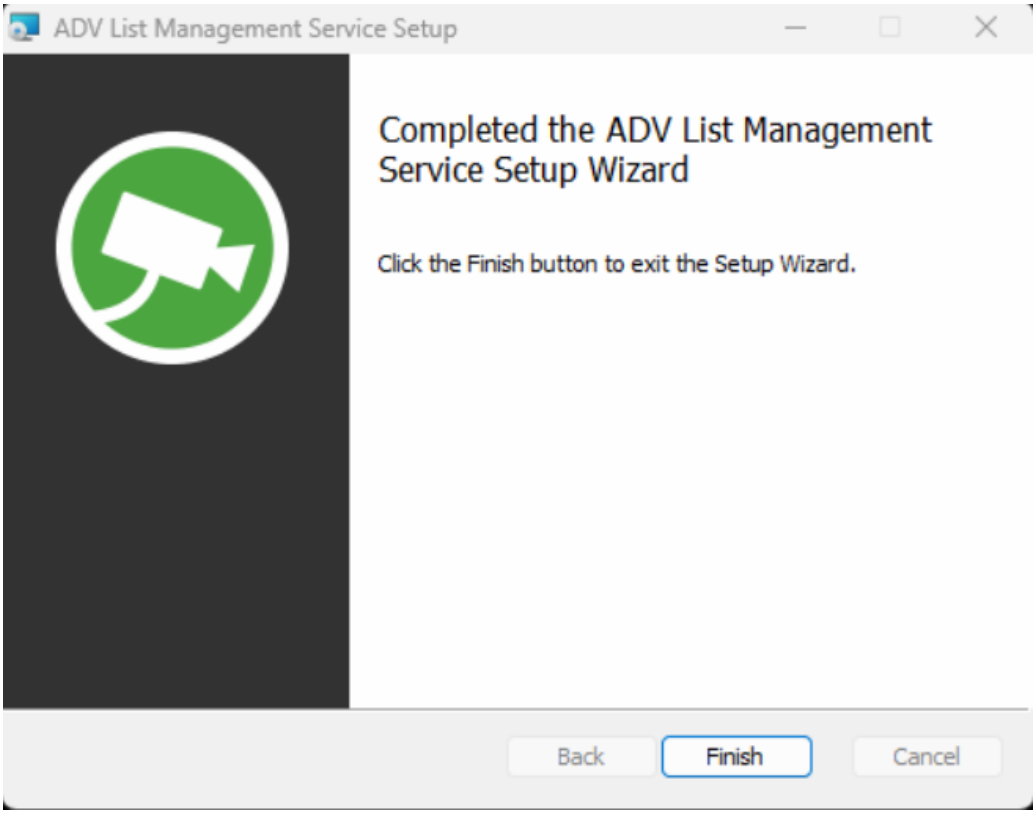


Der HTTP-Port, auf dem der LM-Dienst gehostet wird, ist standardmäßig 8089. Ändern Sie den Port, falls der Standardport für einen anderen Zweck reserviert ist.
Der Hauptserver verwendet standardmäßig Port 8082. Legen Sie die Adresse und den Port des Hauptservers fest, damit der LM-Dienst eine Verbindung zum richtigen Hauptserver herstellen kann.
Die Ereigniswarteschlange (Event queue) verwendet standardmäßig Port 5672. Die Ereigniswarteschlange wird zusammen mit dem LM-Dienst installiert. Ändern Sie den Port der Ereigniswarteschlange, falls der Standardport für einen anderen Zweck reserviert ist.

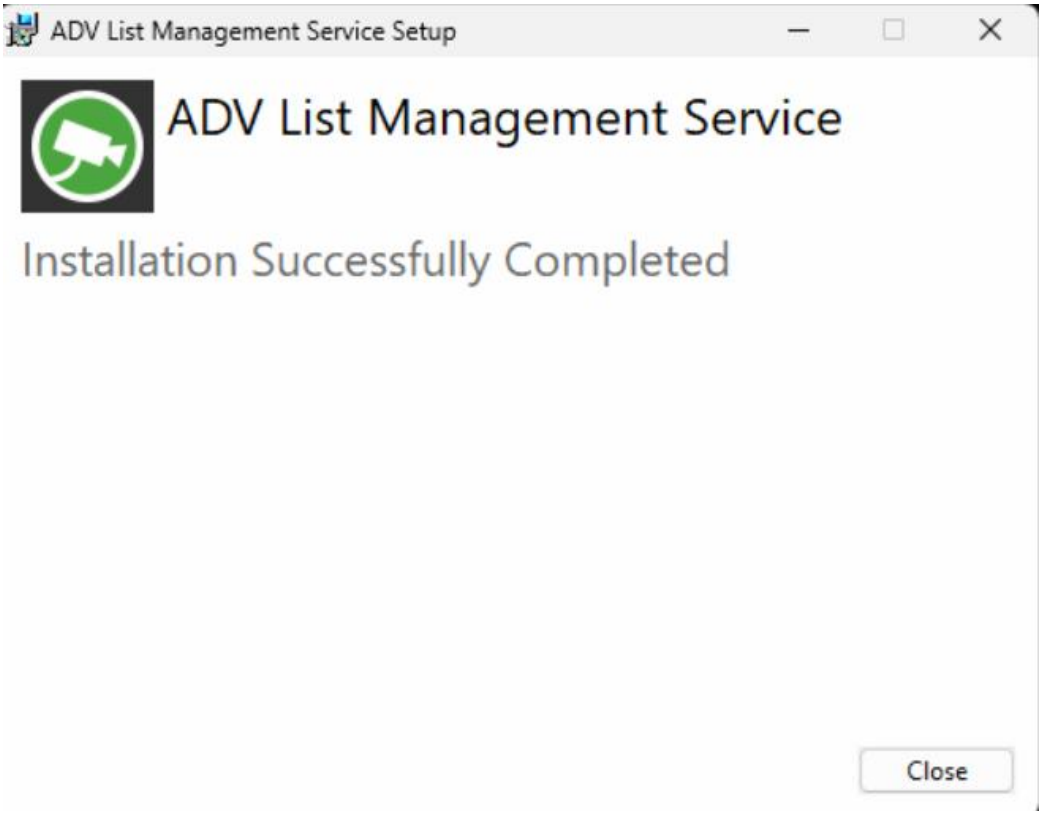
1. Klicken Sie auf **Install**, um fortzufahren.



1. Warten Sie, bis die Installation abgeschlossen ist.
    a. Möglicherweise müssen Sie im Laufe der Installation Firewall-Regeln anwenden.
    b. Das Installationsprogramm installiert den RabbitMQ-Server, der Ereignisse vom Listenverwaltungsdienst, vom Gesichtserkennungsdienst und vom Kennzeichenerkennungsdienst verarbeitet.
    c. Standardport 5672 (TCP).
2. Klicken Sie auf **Finish**, um die Installation abzuschließen.



1. Klicken Sie auf **Close**, um die Installation zu beenden.



1. Der Listenverwaltungsdienst ist nun auf dem Server installiert und einsatzbereit.
    a. Der Listenverwaltungsdienst übermittelt Daten an den VMS-Hauptserver, und Sie können den Dienst über den System-Manager konfigurieren.

3.3 PostgreSQL 15 Upgrade auf PostgreSQL 16 Version

Wenn Sie Mirasys List Management Service Version 9.6.1 oder eine frühere Version verwenden, enthält diese Version PostgreSQL 15. Bevor Sie ein Upgrade auf Mirasys List Management Service 9.6.2 oder höher durchführen und dabei Ihre aktuelle Datenbank beibehalten, müssen Sie die Datenbank zunächst auf PostgreSQL 16 migrieren.

Während des PostgreSQL-Upgrade-Prozesses speichert das System keine Daten in der Datenbank.

3.3.1 Dieser Leitfaden gilt für

- 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 Anforderungen

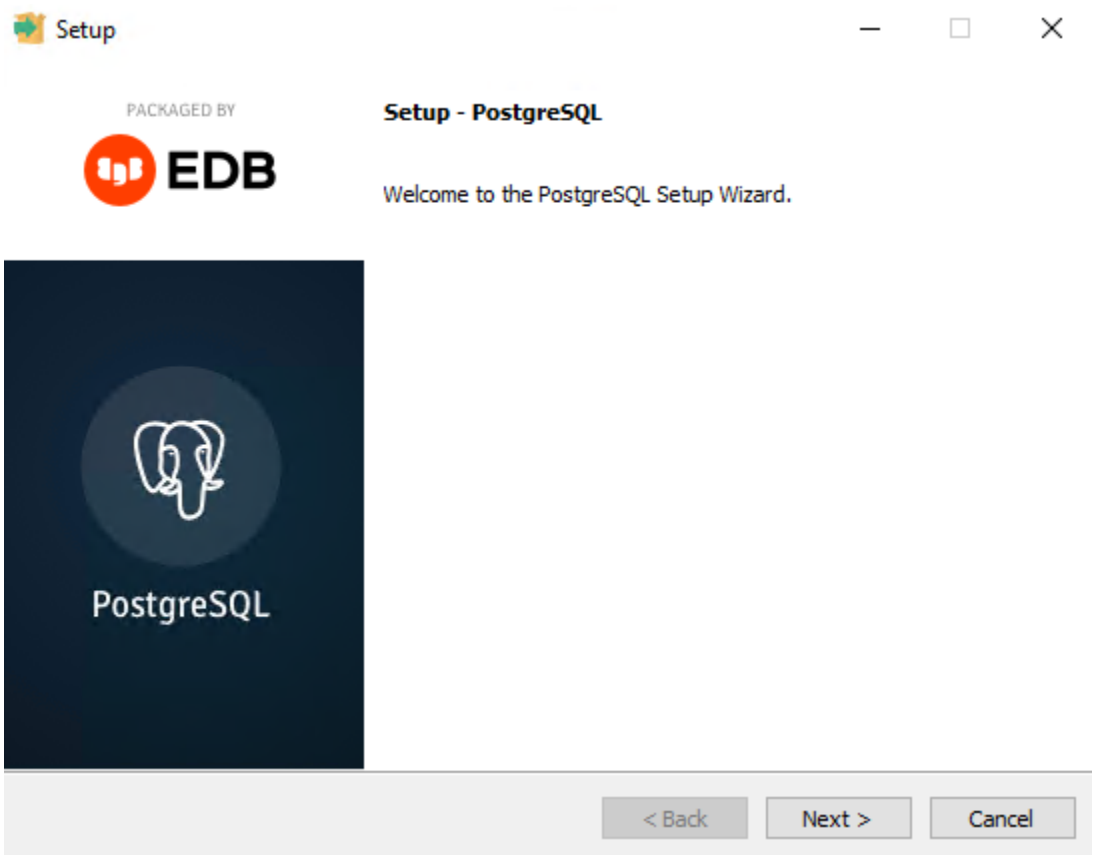
- Sicherung der Datenbank
- Notepad++
- PostgreSQL 16 Installationspaket
    - postgresql-16.1-1-windows-x64.exe
- Mirasys List Management Service 9.6.2 oder neueres Installationspaket
- Das System, auf dem Mirasys List Management Service 9.6.1 oder eine frühere Version installiert ist.

3.3.3 Wie man ein Upgrade durchführt

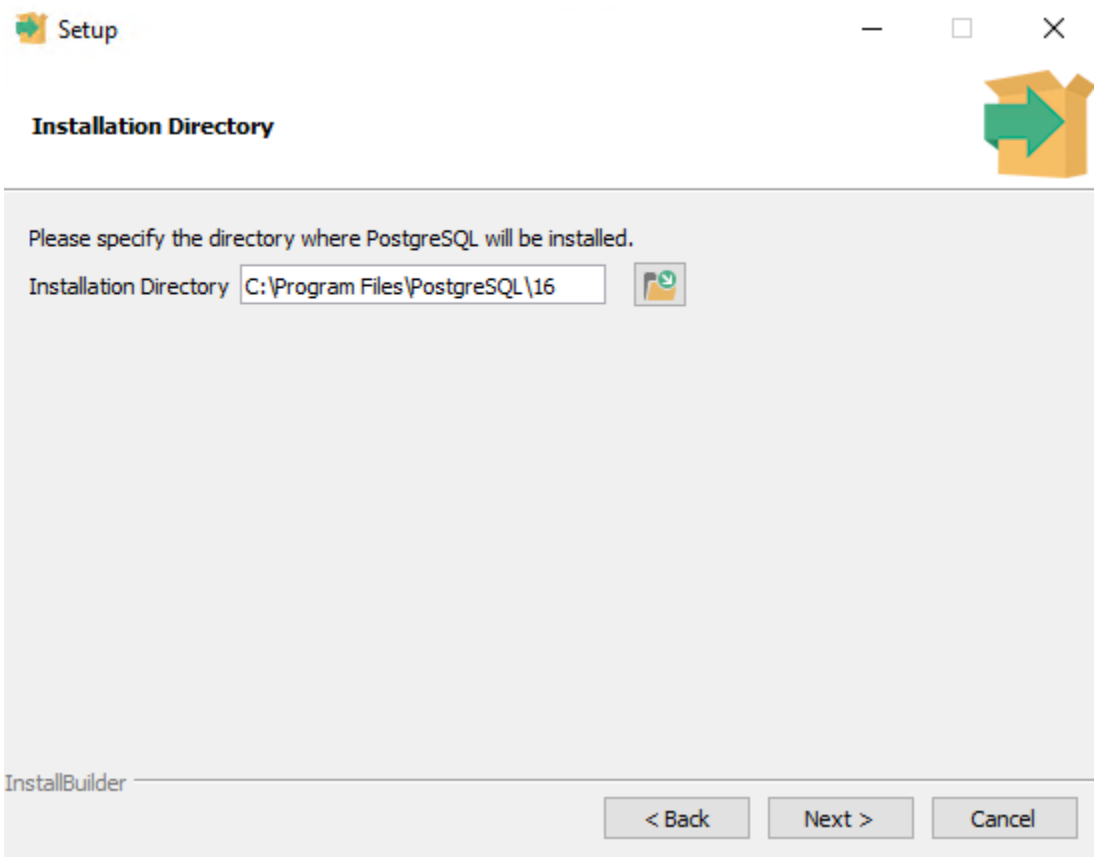
1. Beenden Sie die Dienste AdvPostgreDatabase und ADVLmService in den Windows-Diensten.
2. Ändern Sie die Startart des AdvPostgreDatabase-Dienstes auf manuell.
3. Gehen Sie zu C:\Programme\PostgreSQL\15\data und öffnen Sie die Datei postgresql.conf mit der Anwendung Notepad++.
   a. Suchen Sie die Zeile „port = 5432“ und ändern Sie diese in „port = 5433“.

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

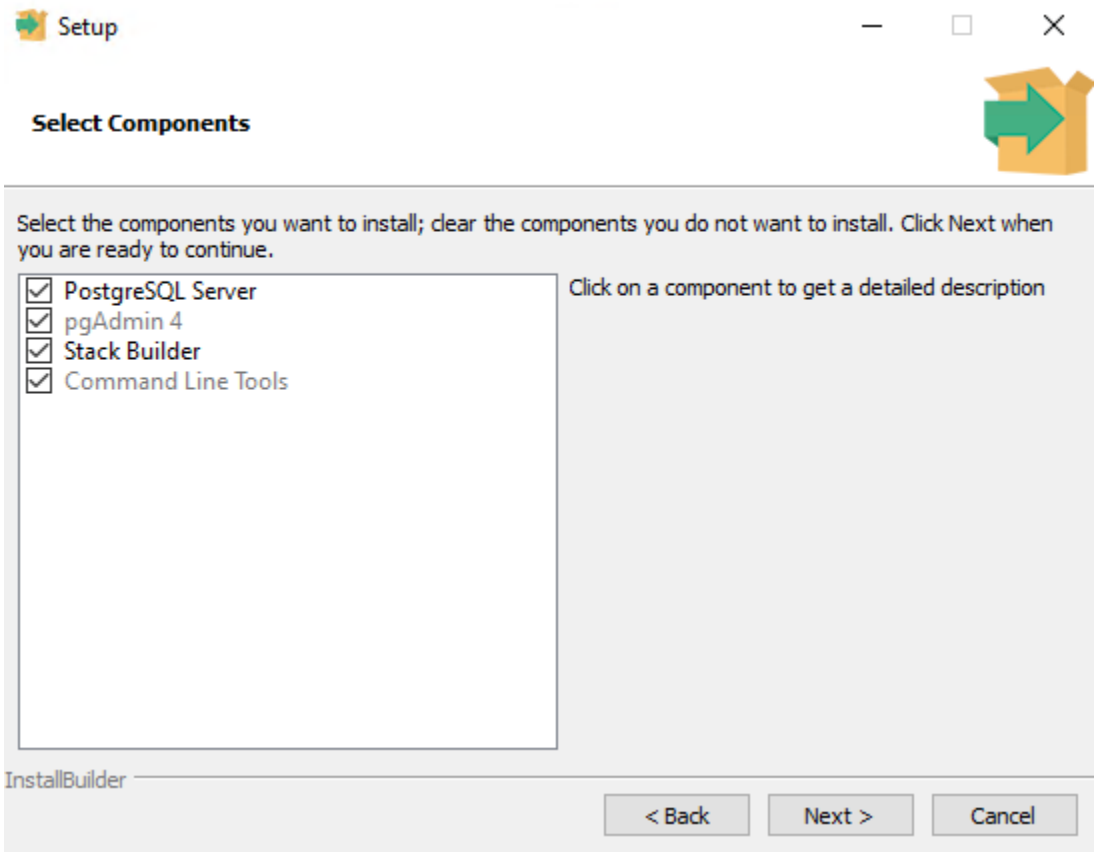
1. Speichern Sie die Konfigurationsdatei postgresql.conf.
2. Start installation of PostgreSQL 16 by double clicking PostgreSQL 16 installation package
3. Klicken Sie auf **Next** (Weiter), um fortzufahren.



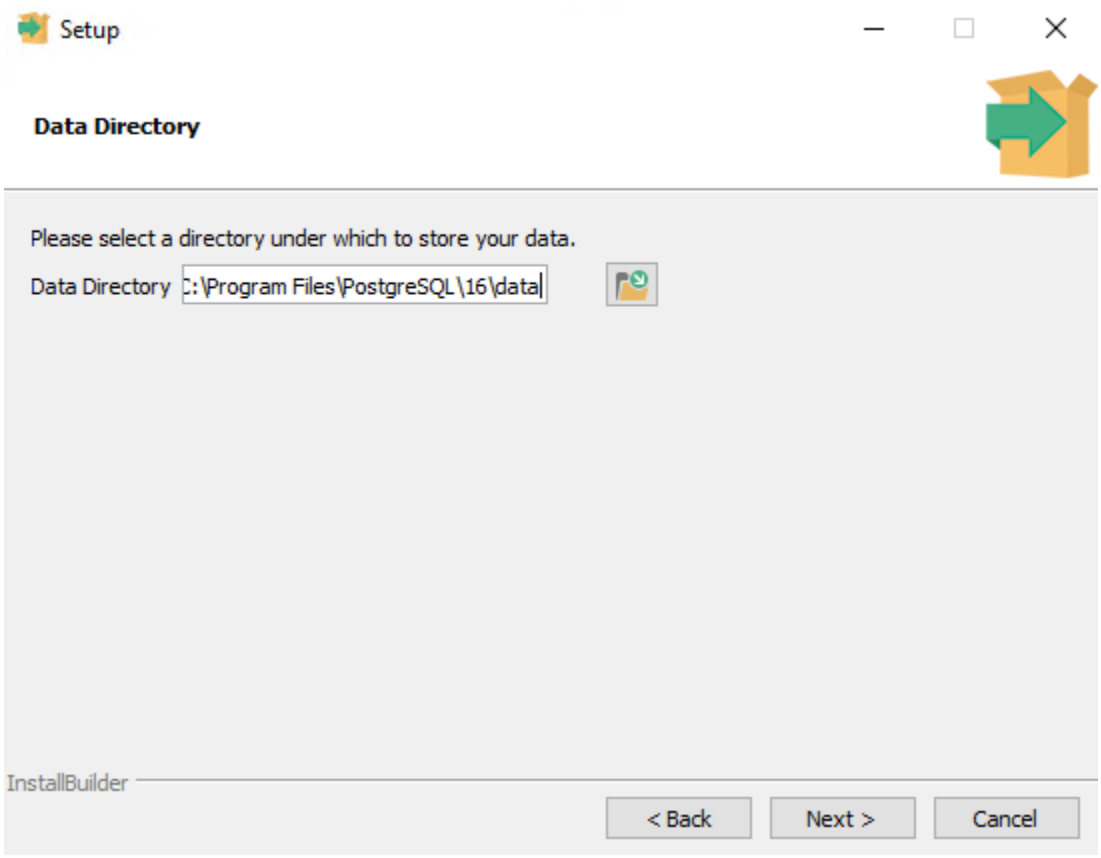
4. Verwenden Sie den Standardinstallationsort und klicken Sie auf **Next** (Weiter).



5. Mit allen Komponenten installieren.

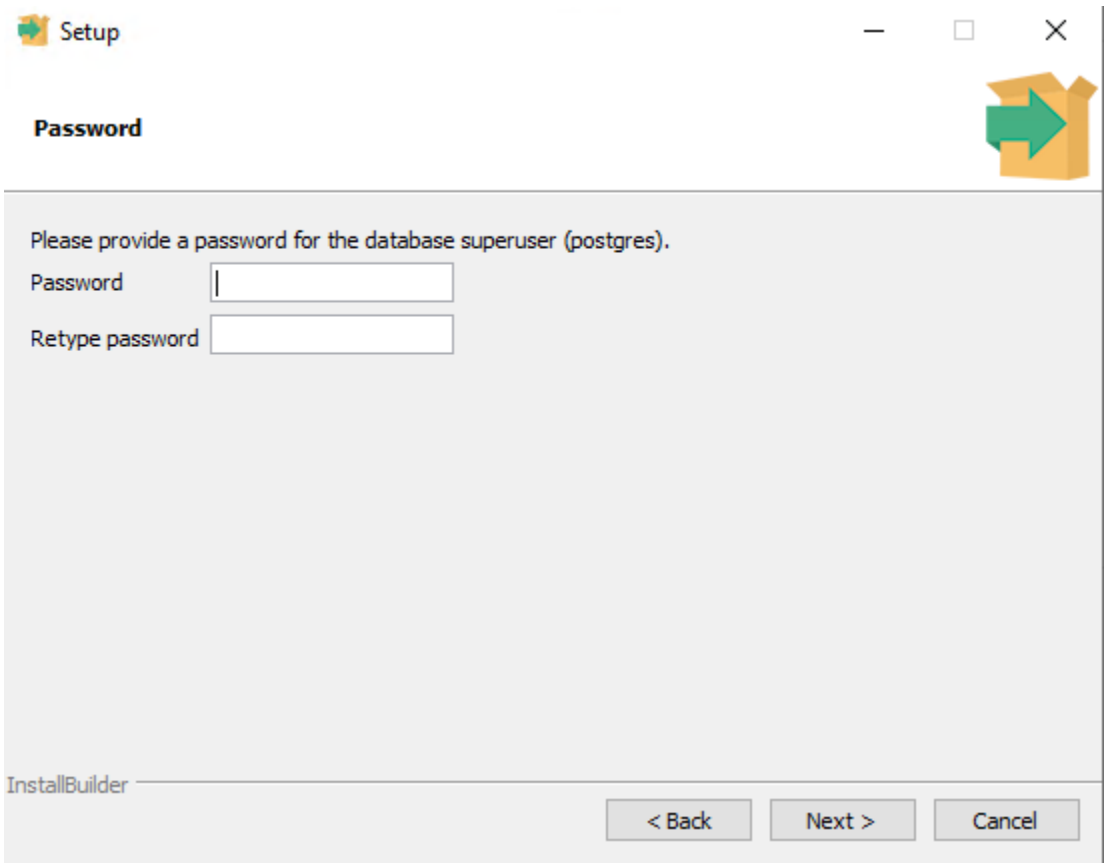


6. Verwenden Sie den Standardspeicherort des Datenverzeichnisses und klicken Sie auf **Next** (Weiter).

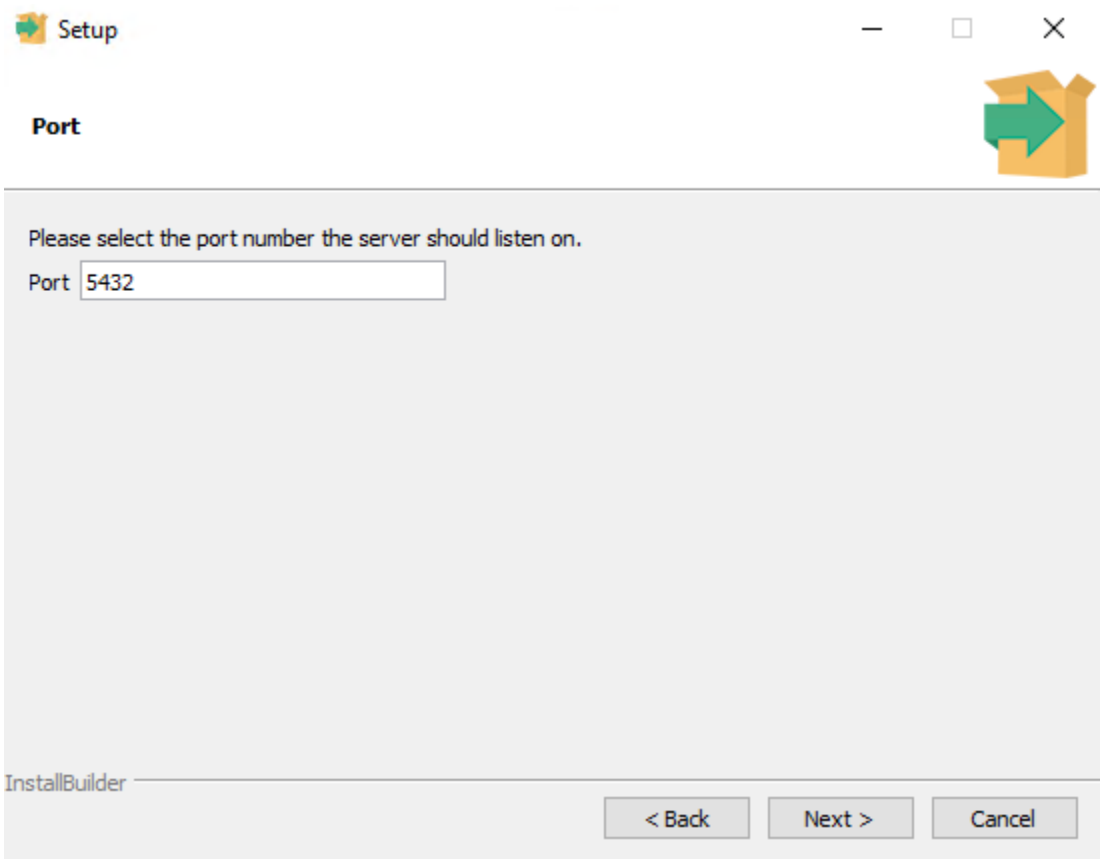


7. Geben Sie dasselbe Passwort ein, das Sie bei der Installation von Mirasys List Management Service verwendet haben.

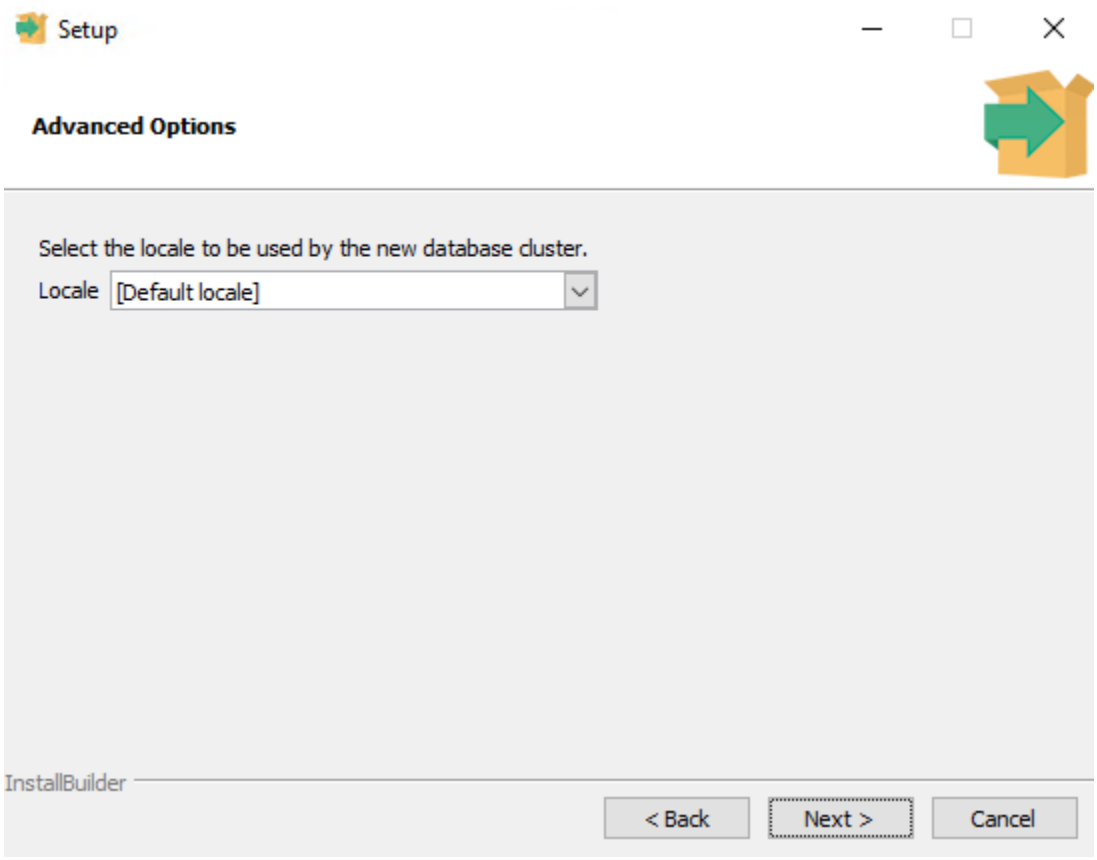
- Standard ist postgres



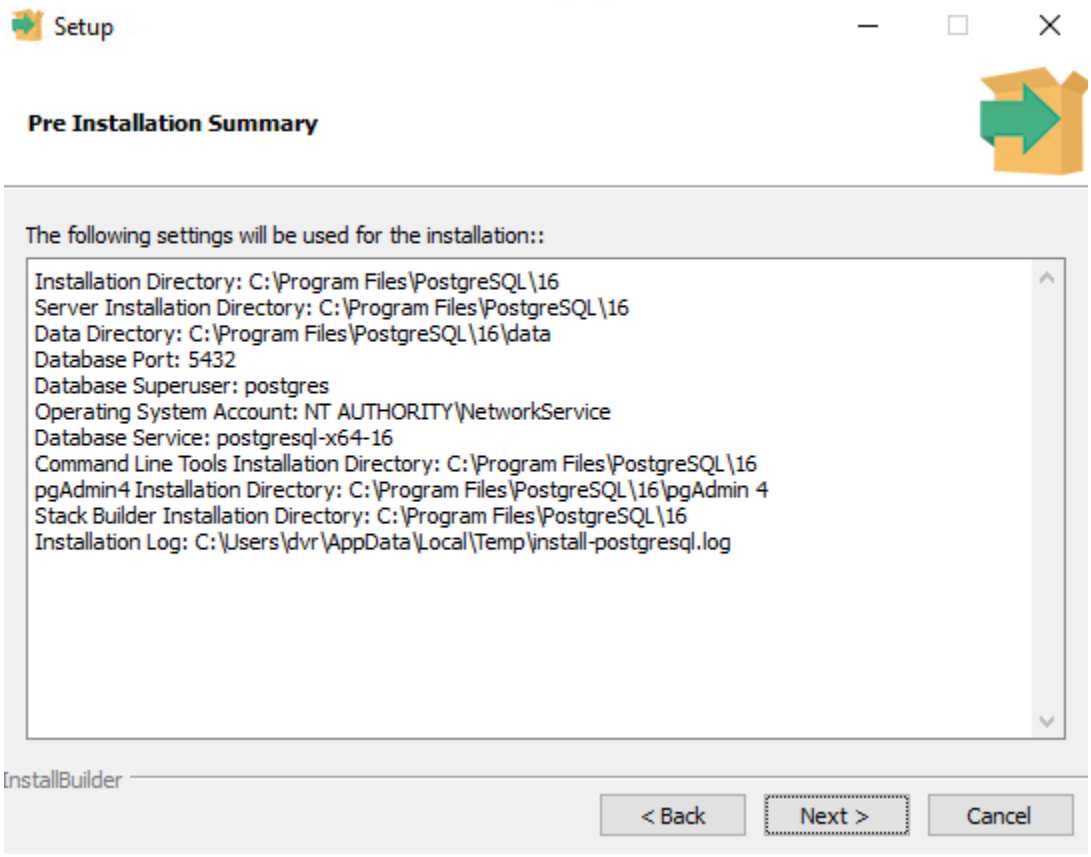
1. Verwenden Sie den Standardport 5432 und klicken Sie auf **Next** (Weiter).



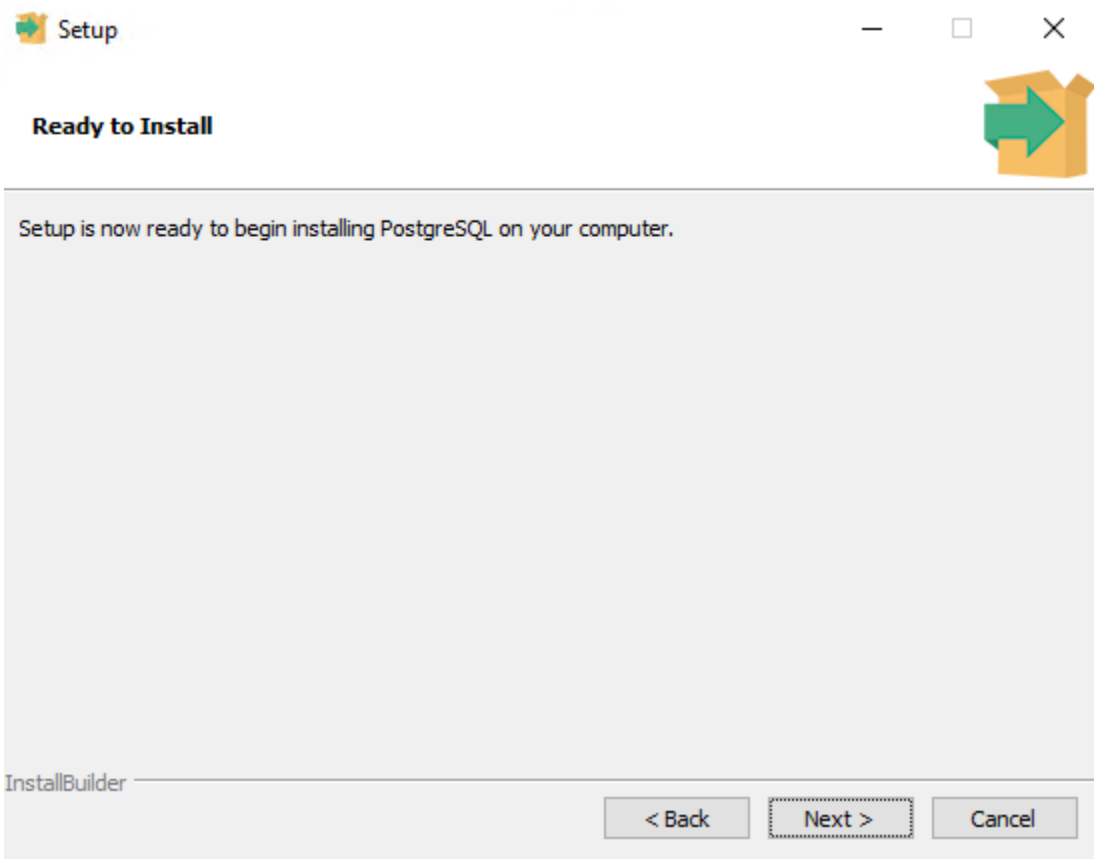
2. Verwenden Sie die standardmäßigen erweiterten Optionen und klicken Sie auf **Next** (Weiter).



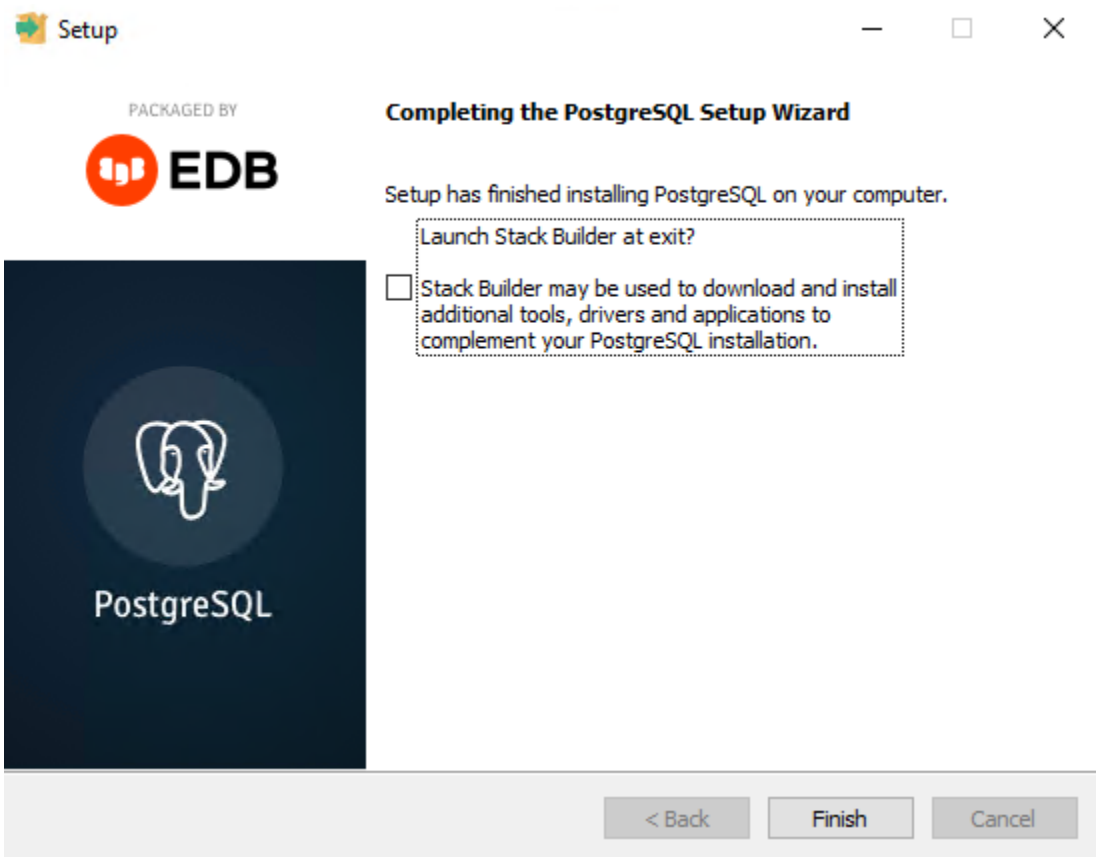
3. Sie können nun die Installationseinstellungen überprüfen. Wenn Änderungen erforderlich sind, gehen Sie zurück und ändern Sie den gewünschten Abschnitt. Andernfalls klicken Sie auf **Next** (Weiter).



4. Klicken Sie auf **Next** (Weiter) und die Installation beginnt. Dies dauert einige Zeit, warten Sie also, bis die Installation abgeschlossen ist.



5. Deaktivieren Sie die Option Launch Stack Builder und klicken Sie auf **Finish (**Fertigstellen).



6. Stoppen Sie den Dienst postgresql-x64-16 über die Windows-Dienste.
7. Ändern Sie den Starttyp von postgresql-x64-16 auf Manuell.
8. Gehen Sie zu C:\Programme\PostgreSQL\16\data und öffnen Sie die Datei postgresql.conf in Notepad++ und überprüfen Sie, ob der Port standardmäßig 5432 ist.
   a. Falls nicht, ändern Sie den Port auf 5432 und speichern Sie die Konfigurationsdatei.
9. Erlauben Sie den lokalen Zugriff, um alte und neue PostgreSQL pg_hba.conf Dateien zu bearbeiten.

   a. Die Speicherorte sind C:\Programmdateien\PostgreSQL\15\data und C:\Programmdateien\PostgreSQL\16\data

   b. Öffnen Sie die Datei pg_hba.conf an beiden Orten und ändern Sie die lokalen Verbindungen in vertrauenswürdig.

```
# 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
```

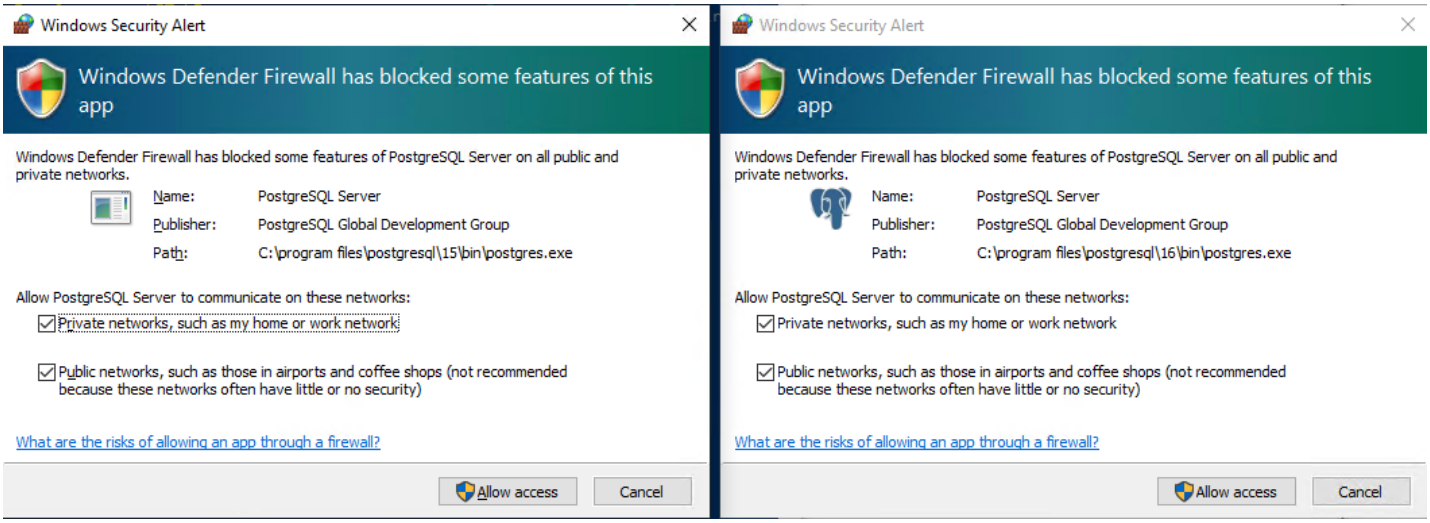
1. Speichern Sie beide Konfigurationsdateien.
2. Öffnen Sie das PowerShell-Fenster und kopieren Sie dieses Skript dorthin.

   a. Überprüfen Sie, ob die Dateipfade korrekt sind, und ändern Sie gegebenenfalls die Pfade in die korrekten Pfade.

```
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. Drücken Sie dann die **Eingabetaste** und warten Sie, bis die Aktualisierung abgeschlossen ist.

   a. Netzwerkregeln für die Firewall zulassen, wenn diese angefordert werden.



1. Vergewissern Sie sich, dass Sie ein ähnliches Ergebnis sehen, sobald die Aktualisierung abgeschlossen ist.

```
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. Suchen Sie nach Fehlern, da diese auf ein Problem hinweisen, das die Aktualisierung verhindert. Ermitteln Sie die mögliche Ursache und versuchen Sie das Upgrade erneut.
2. Schließen Sie das PowerShell-Fenster.
3. Ändern Sie pg_hba.conf wieder auf normal.

   a. Die Speicherorte sind C:\Programmdateien\PostgreSQL\15\data und C:\Programmdateien\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. Deinstallieren Sie die folgenden Anwendungen über Windows-Programme und -Funktionen

   a. ADV List Management Service

   b. PostgreSQL 15 und wählen Sie Gesamte Anwendung

      Sie brauchen sich nicht um die Warnmeldungen im Zusammenhang mit der Entfernung des Datenordners zu kümmern und klicken auf **OK**.

   c. PostgreSQL 16 und wählen Sie Gesamte Anwendung

      Sie brauchen sich nicht um die Warnmeldungen im Zusammenhang mit der Entfernung des Datenordners zu kümmern und klicken auf **OK**.

1. Jetzt können Sie den neueren Mirasys List Management Service installieren und unserer Anleitung zur Installation folgen.
2. Überprüfen Sie, ob das Upgrade erfolgreich war. Die ältere PostgreSQL-Version sollte nun auf die neuere Version aktualisiert werden, und Sie sollten in der Lage sein, sowohl die alten als auch die neuen Daten über den System Manager und Spotter zu sehen.
3. Falls gewünscht, können Sie die alte PostgreSQL-Version bereinigen, indem Sie zu C:\Programme\PostgreSQL navigieren und den Ordner „15“ löschen.

4 MIRASYS FACE RECOGNITION

4.1 EINFÜHRUNG FACE RECOGNITION

Gesichtserkennung (Face Recognition, FR) dient der Identifizierung eines menschlichen Gesichts. Sie wird im VMS-System verwendet, um Ereignisse zu erhalten, wenn Gesichter in ausgewählten Videoströmen erkannt werden, und um zu erkennen, wenn bestimmte Personen im Video zu sehen sind. Zusammen mit der Mirasys-Listenverwaltung können Sie so zum Beispiel ein automatisches Erkennungssystem für den Zutritt einer Person zu einem Gebäude einrichten. Die Gesichtserkennung und Listenverwaltung umfasst die Gesichtsverfolgung und einen Gesichtsähnlichkeitswert, um ein Gesicht einer Identität zuzuordnen. Dies geschieht, um übermäßige Gesichtserkennungsereignisse derselben Person zu vermeiden. Die maximale Anzahl von Gesichtern, die in FR aus einem Bild erkannt werden können, beträgt 20.

Beachten Sie, dass Anti-Spoofing in der aktuellen Version nicht enthalten ist.

Der FR-Dienst empfängt Videoströme, verarbeitet Bilder, erkennt Gesichter und sendet Benachrichtigungen mit Erkennungsdaten an den Listenverwaltungsdienst (LM) für den Identitäts- und Listenabgleich.

Der Gesichtserkennungsdienst hat ein separates Installationsprogramm, so dass er auf einem separaten Server oder auf einem VMS-Server ausgeführt werden kann.

Die Gesichtserkennung funktioniert mit einer Bildgröße von 168 x 256. Ist das Gesicht auf dem Bild größer, wird es vor der Identifizierung zunächst auf 168 x 256 verkleinert. Ist das Gesicht auf dem Bild kleiner, wird es ebenfalls zunächst auf die Größe 168 x 256 vergrößert. Die empfohlene Größe des Gesichts auf dem Bild beträgt mindestens 112 Pixel.

Auf der Lizenzierungsseite muss die RTSP-Streaming-Server-Funktion zum Management-Server und zu allen Servern hinzugefügt werden, auf denen die SmartFR-Funktion verwendet werden soll. Auf der Management-Server-Seite muss die gewünschte Anzahl von Kanälen für die SmartFR-Funktion hinzugefügt werden.

4.2 FR-SERVICE-INSTALLATION

Smart Services können zusammen mit der VCA-Deep-Learning-Funktion genutzt werden. In diesem Fall sollten Sie darauf achten, dass Sie die neuesten NVIDIA-Treiber verwenden und nicht die, die im CUDA-Toolkit-Paket enthalten sind. Weitere Informationen finden Sie hier.

Die NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind nicht im FR-Installationsprogramm enthalten. Das Installationsprogramm erkennt die NVIDIA-Bibliotheksinstallationsprogramme im Unterordner „NVIDIA“ und installiert die Bibliotheken automatisch, sofern sie gefunden werden.

4.2.1 Anforderungen

- Administratorrechte
- Installierter List Management Service
- Lizenz für Gesichtserkennung auf dem VMS-Management-Server
- RTSP-Lizenzfunktion auf dem VMS-Management-Server und dem VMS-Server
- Die erforderlichen NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind installiert

4.2.2 NVIDIA-Bibliotheken

Die erforderlichen NVIDIA-Bibliotheken sollten vor der Installation des FR-Dienstes installiert werden, sofern sie noch nicht vorhanden sind. Für die Installation des FR-Dienstes müssen die folgenden NVIDIA-Bibliotheken für Windows installiert sein:

- 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 für Windows 10, 11, Server 2022 und CUDA 12.0 bis 12.9 – ZIP-Paket: https://developer.nvidia.com/tensorrt/download/10x

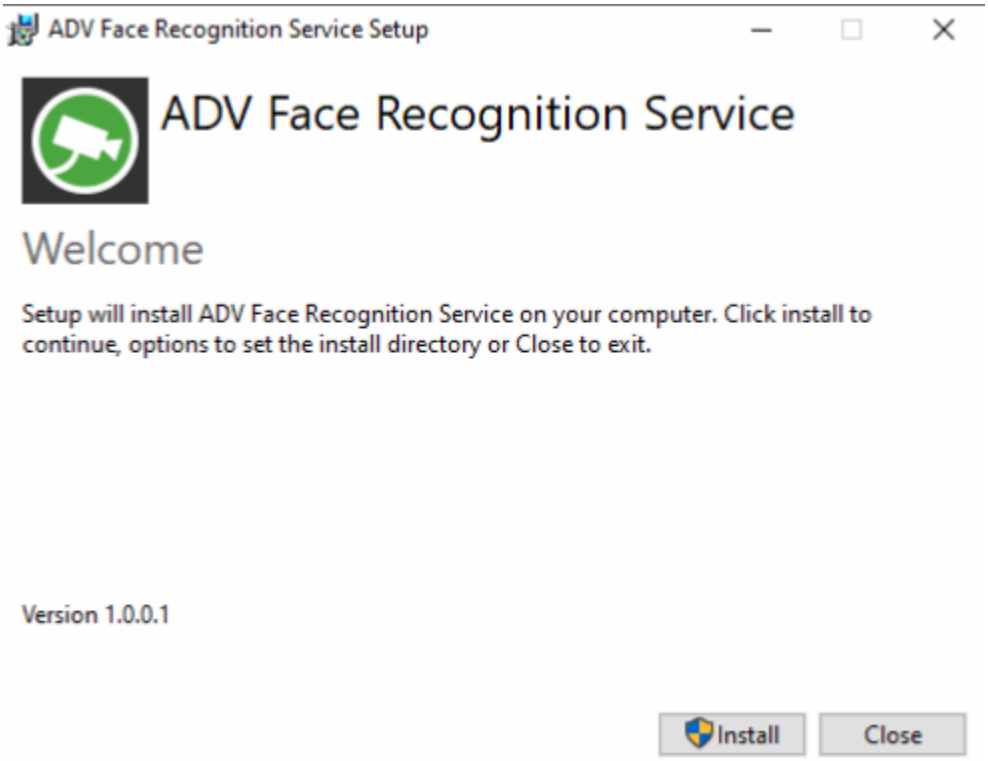
4.2.2.1 Installation der NVIDIA-Bibliotheken

1. Laden Sie das Installationsprogramm für den Mirasys FR-Dienst herunter und speichern Sie es in einem Ordner auf Ihrem Computer
2. Erstellen Sie einen Unterordner „NVIDIA“
3. Laden Sie die oben genannten NVIDIA-Bibliotheken herunter.
4. Speichern Sie die heruntergeladenen NVIDIA-Bibliotheken im Unterordner „NVIDIA“.
5. Führen Sie das Installationsprogramm für den Mirasys FR-Dienst aus.
    a. Das Installationsprogramm für den Mirasys FR-Dienst installiert automatisch die NVIDIA-Bibliotheken, die es im Unterordner „NVIDIA“ findet, bevor der Dienst installiert wird.
6. Befolgen Sie die Installationsanweisungen, um die Installation abzuschließen.

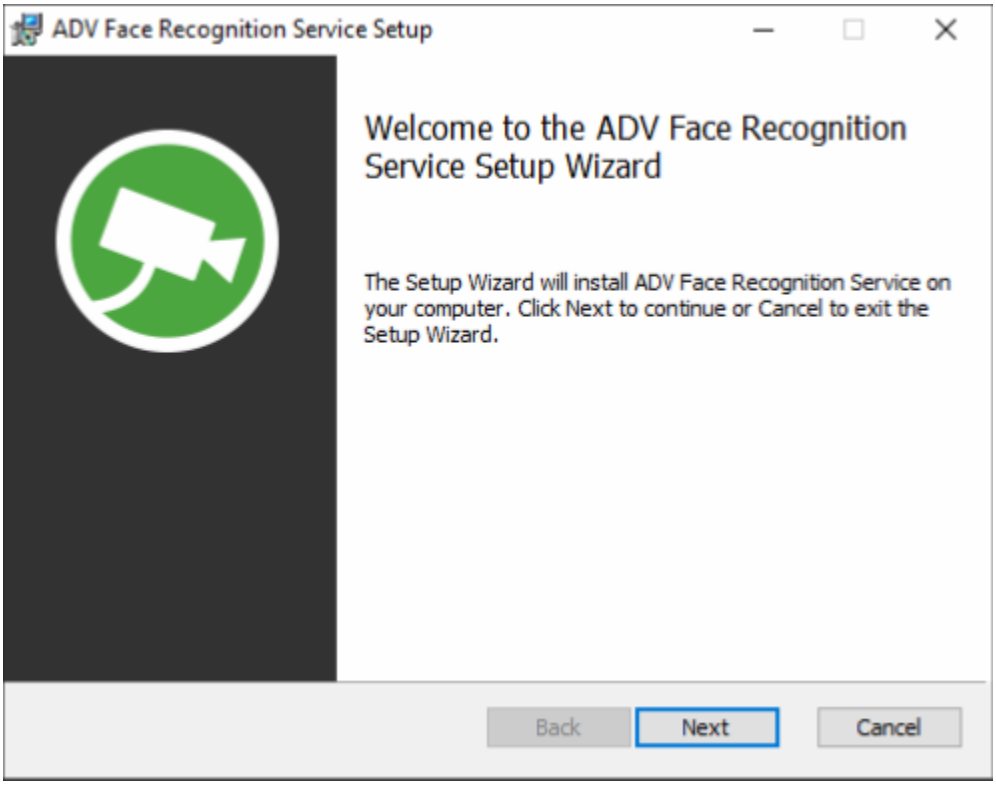
4.2.3 FR Installation

Das Installationsprogramm enthält einen Schritt, in dem Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren müssen. Sie müssen bestätigen, dass Sie die in der Vereinbarung aufgeführten Bedingungen akzeptieren, um mit der Installation fortzufahren.

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie die Dateien z. B. in den Ordner „C:\temp“.
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Klicken Sie auf **Install**, um fortzufahren.



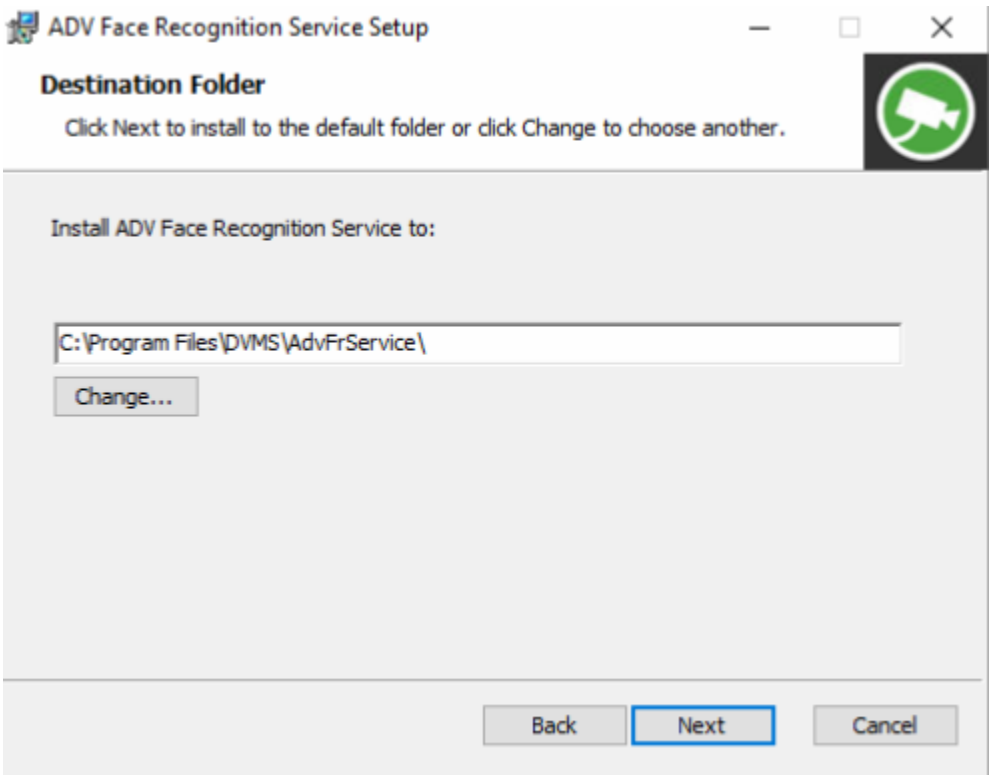
1. Klicken Sie auf **Next**, um fortzufahren.



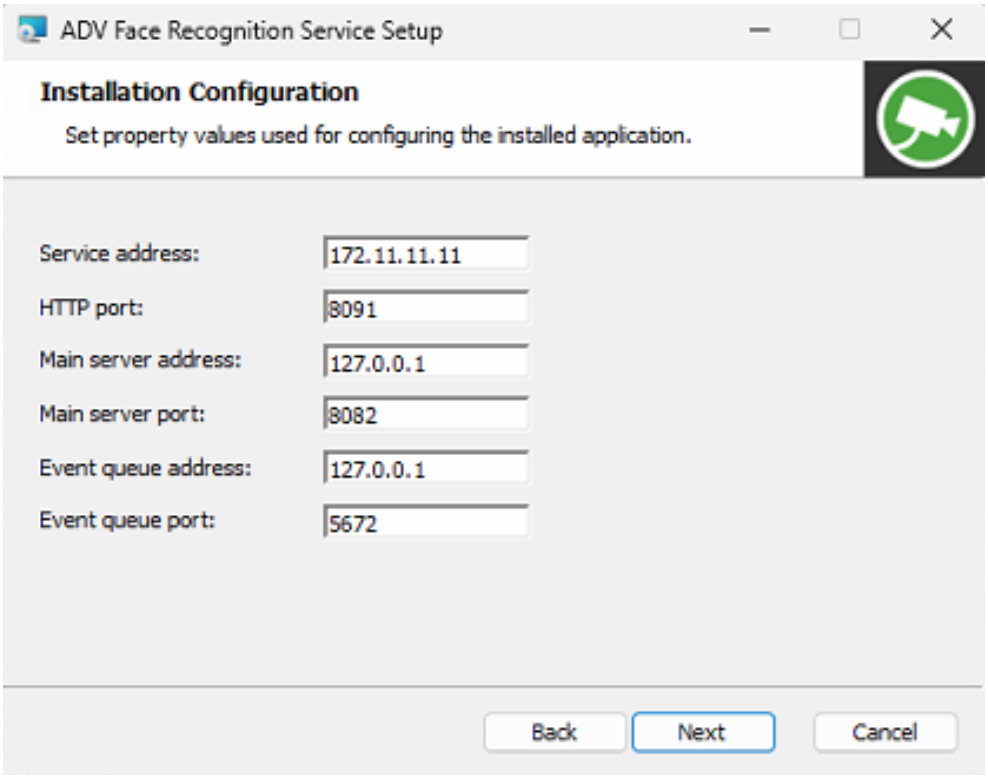
1. Aktivieren Sie das Kontrollkästchen **I accept the terms in the License Agreement** und klicken Sie auf **Next**.



1. Ändern Sie gegebenenfalls den Installationsort und klicken Sie auf **Next**, um fortzufahren.

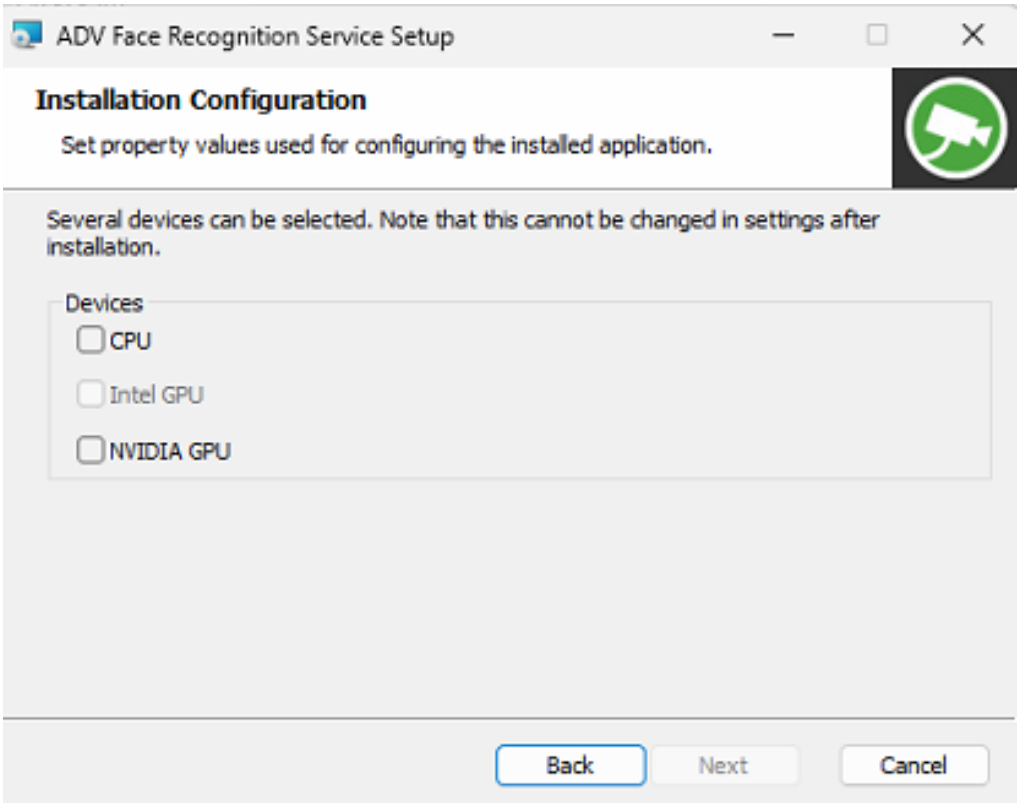


1. Ändern Sie die Ports und Adressen bei Bedarf.
    a. Wenn Sie beispielsweise den Gesichtserkennungsdienst auf einem anderen Rechner als dem VMS-Hauptserver installieren, müssen Sie die Adresse des Hauptservers durch die richtige ersetzen.
    b. Das Gleiche gilt für die Adresse der Ereigniswarteschlange. Ersetzen Sie diese Adresse durch die Serveradresse, auf der der Listenverwaltungsdienst installiert ist.
    c. Ändern Sie die Dienstadresse (Service Address) so, dass sie für Client-Anwendungen erreichbar ist. Standardmäßig ist die Dienstadresse die erste erkannte IP-Adresse des Rechners.
2. Klicken Sie auf **Next**, um fortzufahren.

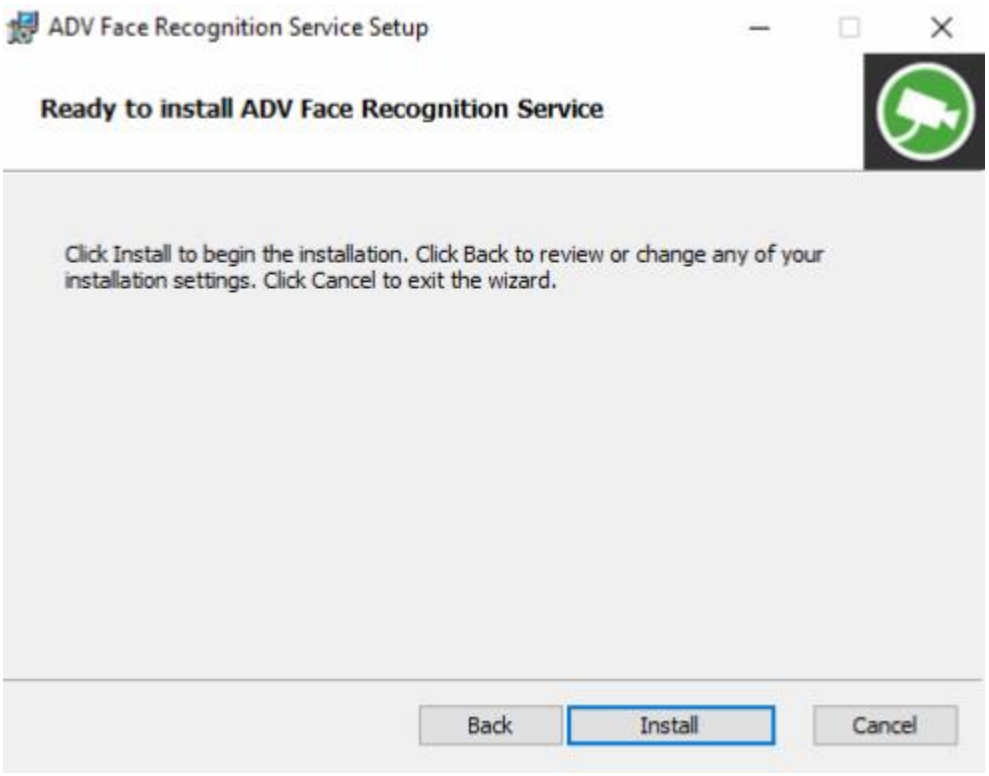


Der HTTP-Port, auf dem der FR-Dienst gehostet wird, ist standardmäßig 8091. Ändern Sie den Port, falls der Standardport für einen anderen Zweck reserviert ist.
Der Hauptserver verwendet standardmäßig Port 8082. Legen Sie die Adresse und den Port des Hauptservers fest, damit der FR-Dienst eine Verbindung zum richtigen Hauptserver herstellen kann.
Die Ereigniswarteschlange (Event queue) verwendet standardmäßig Port 5672. Die Ereigniswarteschlange wird bei der Installation des LM-Dienstes mitinstalliert, wobei der verwendete Port der Ereigniswarteschlange festgelegt wird. Legen Sie die Adresse der Ereigniswarteschlange auf den Rechner fest, auf dem der LM-Dienst installiert ist.

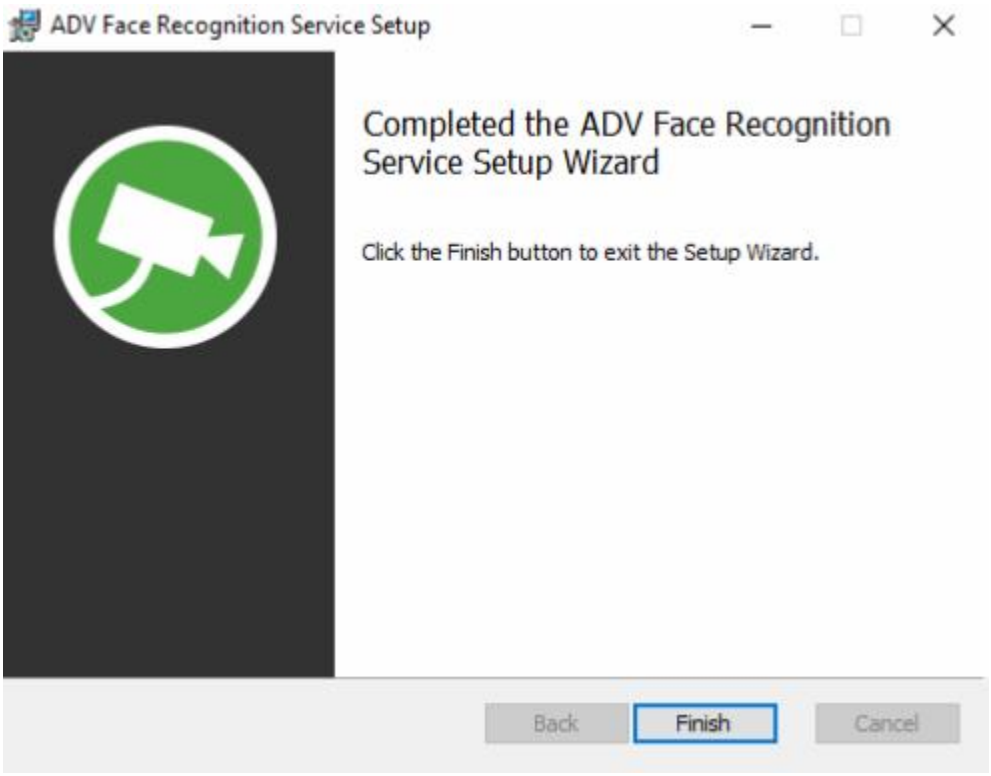
1. Wählen Sie die Geräte aus und klicken Sie auf **Next**



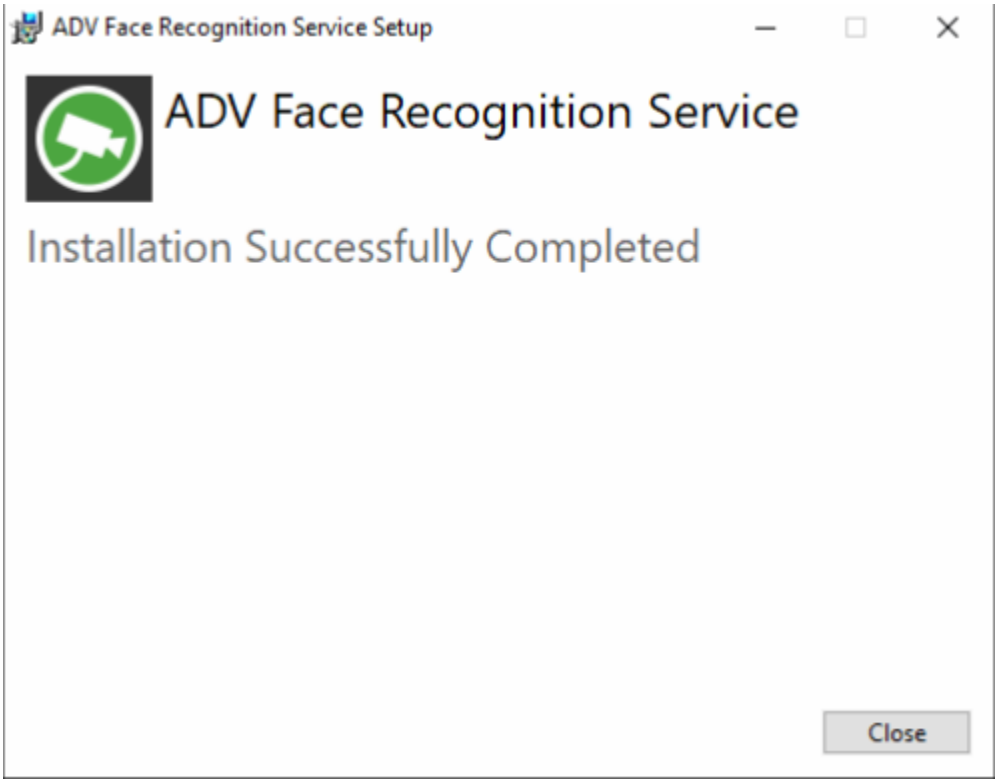
1. Klicken Sie auf **Install**, um fortzufahren, und warten Sie.
2. Die Installation dauert eine Weile, bis sie abgeschlossen ist.
3. Die Erstellung des Modells kann bis zu 30 Minuten dauern. Dies hängt davon ab, wie leistungsfähig die verwendete Grafikkarte ist.



1. Klicken Sie auf **Finish**, um fortzufahren.



1. Klicken Sie auf **Close**, um die Installation zu beenden.



1. Der Gesichtserkennungsdienst ist nun auf dem Server installiert und einsatzbereit.
    a. Der Gesichtserkennungsdienst übermittelt die Daten an den VMS-Hauptserver. Sie können den Dienst über den System Manager konfigurieren.

4.3 FR Datenschutz-Masken

Wenn für die Kamera Client-Privatsphärenmasken definiert sind, zeichnet der FR-Dienst vor der Inferenz Privatsphärenmasken auf die Eingabebilder.

- Innerhalb der Privatzone kann kein Gesicht erkannt werden.
- Vorschaubilder haben Privatzonen.

4.4 FR-Verarbeitung, Ereignisse und Erkennung

4.4.1 Geräte

Die Gesichtserkennungsverarbeitung kann mit unterschiedlicher Hardware durchgeführt werden. Unterstützte Hardware sind CPU, Intel GPU, Nvidia GPU und MAIC (Mirasys AI Card).

4.4.2 FR-Veranstaltungen

Live-FR-Ereignisse werden im Smart Recognition Plugin in Spotter angezeigt. FR-Ereignisse können mit dem Plugin Smart Search in Spotter durchsucht werden.

4.4.3 Visualisierung des erkannten Gesichts

Erkannte Gesichter können in Spotter mit dem VCA-Visualisierungs-Plugin visualisiert werden.

4.5 FR Alarmauslöser und Konfiguration

4.5.1 Alarmauslöser

Für jede Identitätsliste, die in den Einstellungen der Listenverwaltung konfiguriert ist, kann ein Alarmauslöser auf dem VMS-Server erstellt werden.

4.5.2 FR-Konfiguration

Der FR-Dienst kann in der Anwendung System Manager auf der Registerkarte FR-Einstellungen im Fenster Kameraeinstellungen konfiguriert werden.

Die FR-Einstellungen enthalten Informationen über die vom Dienst verarbeiteten Kamera-Videoströme. Jede Stream-Einstellung bezieht sich auf die Kamera und den Stream auf dem Rekorder. Jeder FR-Dienst kann seine eigenen Grenzwerte haben.

4.6 FR-Leistung

4.6.1 Testcomputer-Hardware

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

Aus Leistungsgründen wurde die Gesichtserkennung für CPU und Intel-GPU hinsichtlich Geschwindigkeit optimiert und weist eine etwas geringere Genauigkeit auf als die Erkennung für NVIDIA-GPUs. Um die beste Genauigkeit zu erzielen, sollte die NVIDIA-GPU verwendet werden.

4.6.2 Version 9.10

4.6.2.1 CPU

Streams	Größe	FPS	Process CPU	Prozess-speicher	NVIDIA decode
1	1920 x 1080	8	9%	1.8 GB	2%

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

4.6.3 Version 9.9.6

4.6.3.1 CPU

Streams	Größe	FPS	Process CPU	Prozess-speicher	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	Größe	FPS	Process CPU	Prozess-speicher	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	Größe	FPS	Process CPU	Prozess-speicher	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	Größe	FPS	Process CPU	Prozess-speicher	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 EINFÜHRUNG LICENSE PLATE RECOGNITION

Die Kennzeichenerkennung (LPR) dient zur Identifizierung eines Fahrzeugs anhand des Nummernschilds. Sie wird im VMS-System verwendet, um Ereignisse zu erhalten, wenn Nummernschilder in ausgewählten Videoströmen erkannt werden, und um zu erkennen, wenn bestimmte Fahrzeuge im Video zu sehen sind. In Verbindung mit der Mirasys-Listenverwaltung können Sie so zum Beispiel ein automatisches Erkennungssystem für die Einfahrt von Fahrzeugen in Parkhäuser einrichten.

Der LPR-Dienst empfängt Videoströme, verarbeitet Bilder, erkennt Nummernschilder und sendet Benachrichtigungen mit Erkennungsdaten an den Listenverwaltungsdienst (LM) zum Identitäts- und Listenabgleich.

Der Kennzeichenerkennungsdienst verfügt über ein separates Installationsprogramm, so dass er auf einem separaten Server oder auf einem VMS-Server ausgeführt werden kann.

5.2 LPR-SERVICE-INSTALLATION

Smart Services können zusammen mit der VCA-Deep-Learning-Funktion genutzt werden. In diesem Fall sollten Sie darauf achten, dass Sie die neuesten NVIDIA-Treiber verwenden und nicht die, die im CUDA-Toolkit-Paket enthalten sind. Weitere Informationen finden Sie hier.

Die NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind nicht im LPR-Installationsprogramm enthalten. Das Installationsprogramm erkennt die NVIDIA-Bibliotheksinstallationsprogramme im Unterordner „NVIDIA“ und installiert die Bibliotheken automatisch, sofern sie gefunden werden.

5.2.1 Anforderungen

- Administratorrechte
- Installierter List Management Service
- Lizenz für die Kennzeichenerkennung auf dem VMS-Management-Server
- RTSP-Lizenzfunktion auf dem VMS-Management-Server und dem VMS-Server
- Die erforderlichen NVIDIA-Bibliotheken (CUDA, cuDNN, TensorRT) sind installiert

5.2.2 NVIDIA-Bibliotheken

Die erforderlichen NVIDIA-Bibliotheken sollten vor der Installation des LPR-Dienstes installiert werden, sofern sie noch nicht vorhanden sind. Für die Installation des LPR-Dienstes müssen die folgenden NVIDIA-Bibliotheken für Windows installiert sein:

- 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 für Windows 10, 11, Server 2022 und CUDA 12.0 bis 12.9 – ZIP-Paket: https://developer.nvidia.com/tensorrt/download/10x

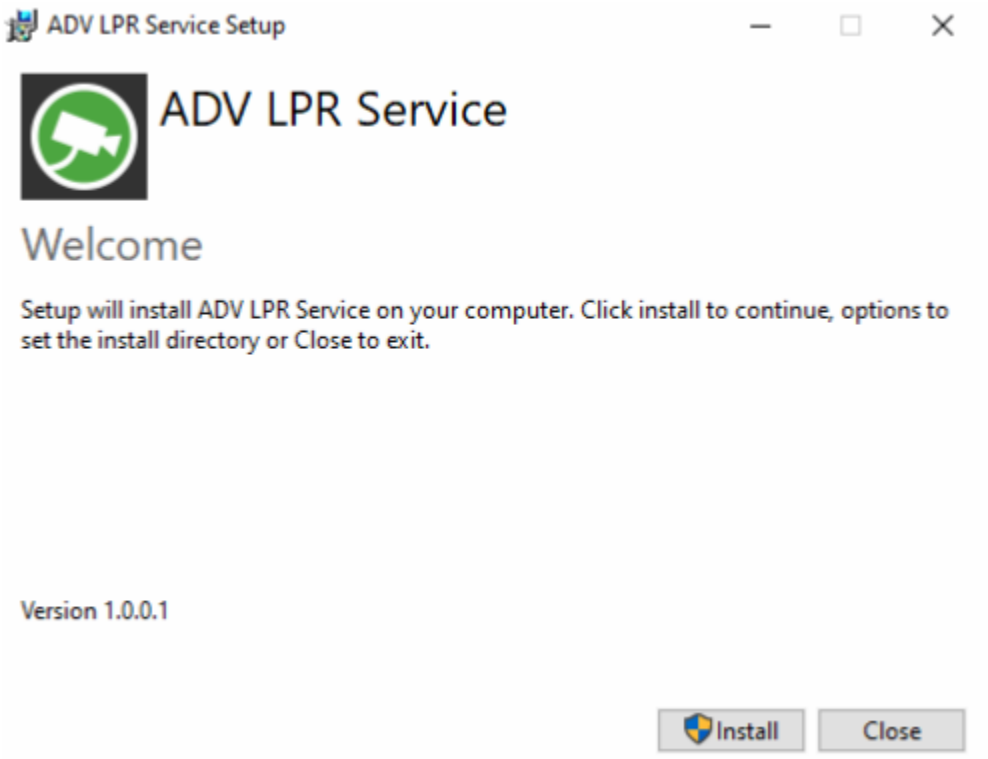
5.2.2.1 Installation der NVIDIA-Bibliotheken

1. Laden Sie das Installationsprogramm für den Mirasys LPR-Dienst herunter und speichern Sie es in einem Ordner auf Ihrem Computer
2. Erstellen Sie einen Unterordner „NVIDIA“
3. Laden Sie die oben genannten NVIDIA-Bibliotheken herunter.
4. Speichern Sie die heruntergeladenen NVIDIA-Bibliotheken im Unterordner „NVIDIA“.
5. Führen Sie das Installationsprogramm für den Mirasys LPR-Dienst aus.
    a. Das Installationsprogramm für den Mirasys LPR-Dienst installiert automatisch die NVIDIA-Bibliotheken, die es im Unterordner „NVIDIA“ findet, bevor der Dienst installiert wird.
6. Befolgen Sie die Installationsanweisungen, um die Installation abzuschließen.

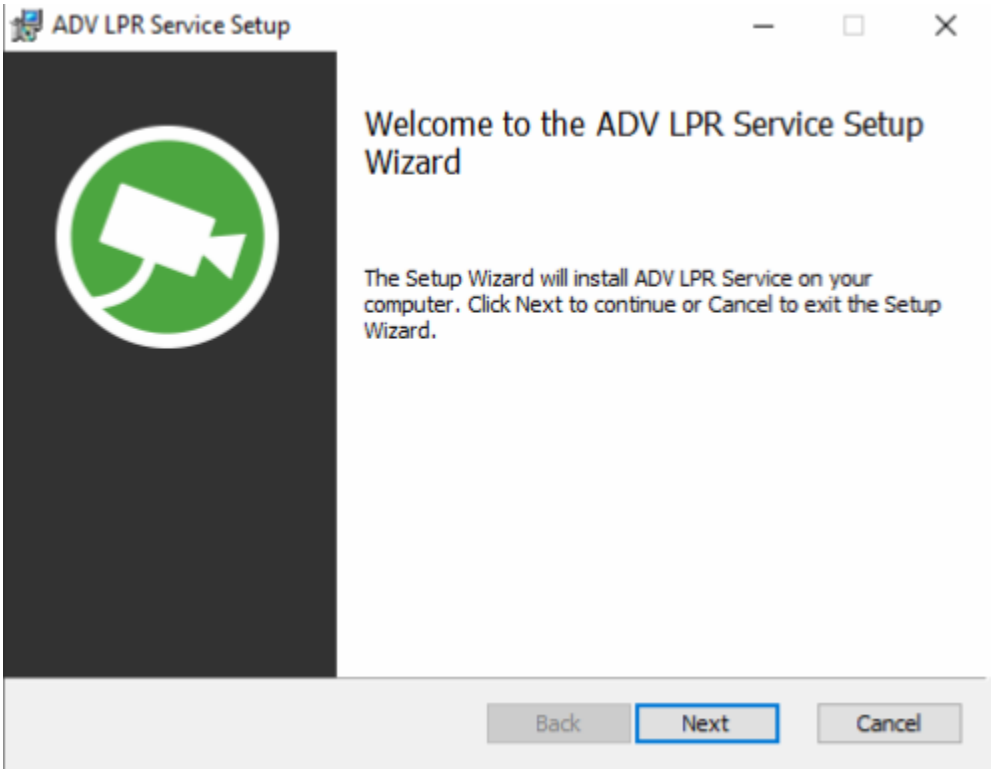
5.2.3 LPR-Installation

Das Installationsprogramm enthält einen Schritt, in dem Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren müssen. Sie müssen bestätigen, dass Sie die in der Vereinbarung aufgeführten Bedingungen akzeptieren, um mit der Installation fortzufahren.

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie die Dateien z. B. in den Ordner „C:\temp“.
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Klicken Sie auf **Install**, um fortzufahren.



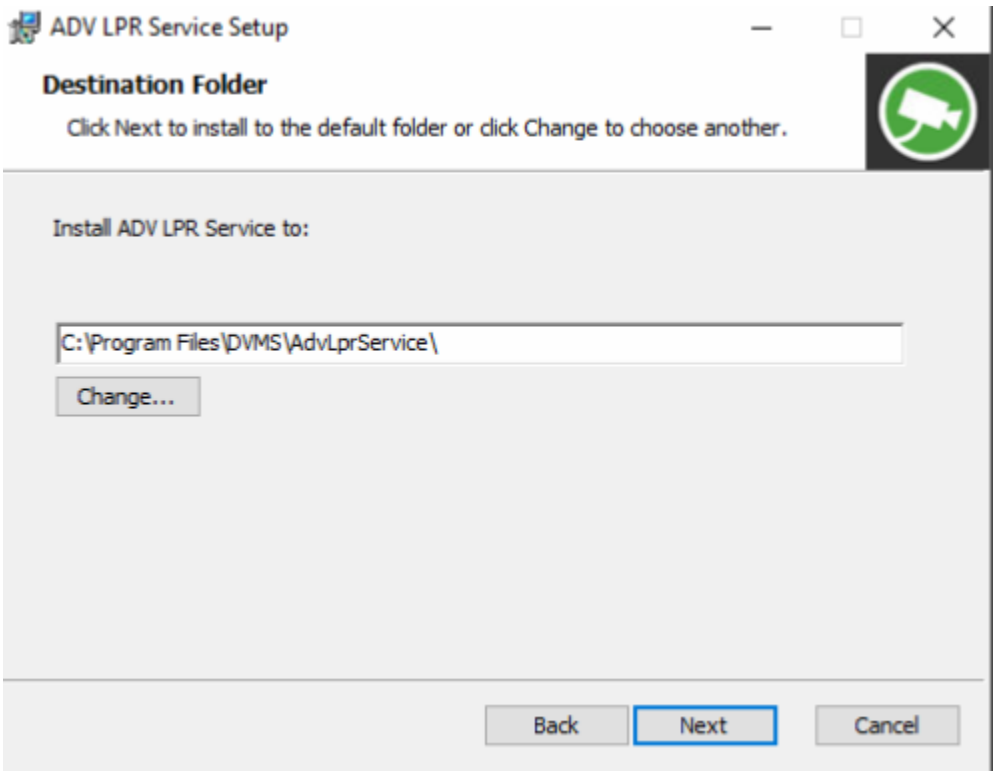
1. Klicken Sie auf **Next**, um fortzufahren.



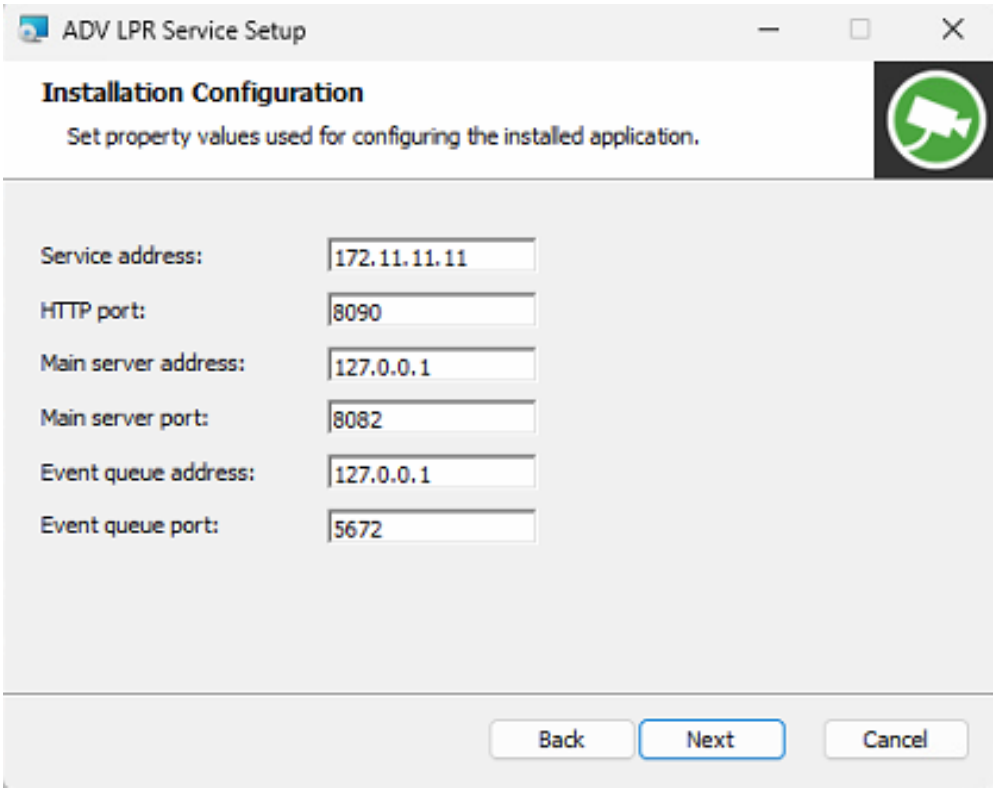
1. Aktivieren Sie das Kontrollkästchen **I accept the terms in the License Agreement** und klicken Sie auf **Next**.



1. Ändern Sie gegebenenfalls den Installationsort; andernfalls klicken Sie auf **Next**, um fortzufahren.

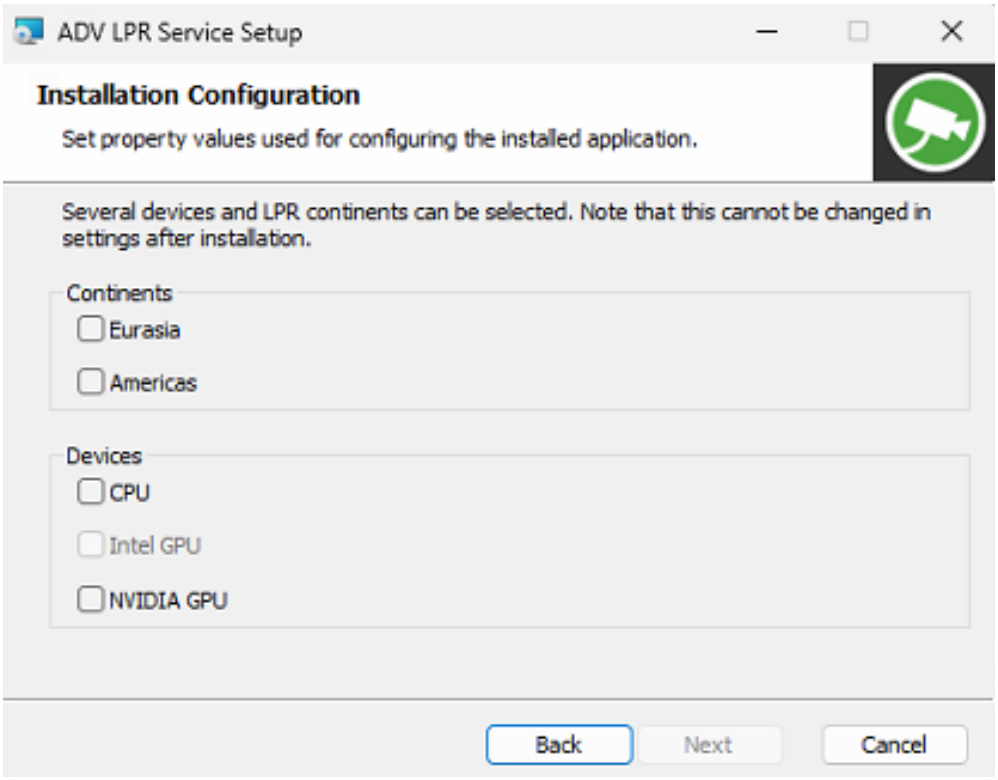


1. Ändern Sie die Ports und Adressen bei Bedarf.
    a. Wenn Sie den Dienst auf einem anderen Rechner als dem VMS-Hauptserver installieren, müssen Sie die Adresse des Hauptservers durch die richtige Adresse ersetzen.
    b. Das Gleiche gilt für die Adresse der Ereigniswarteschlange. Ersetzen Sie diese Adresse durch die Serveradresse, auf der der Listenverwaltungsdienst installiert ist.
    c. Ändern Sie die Dienstadresse (Service Address) so, dass sie für Client-Anwendungen erreichbar ist. Standardmäßig ist die Dienstadresse die erste erkannte IP-Adresse des Rechners.
2. Klicken Sie auf **Next**, um fortzufahren.

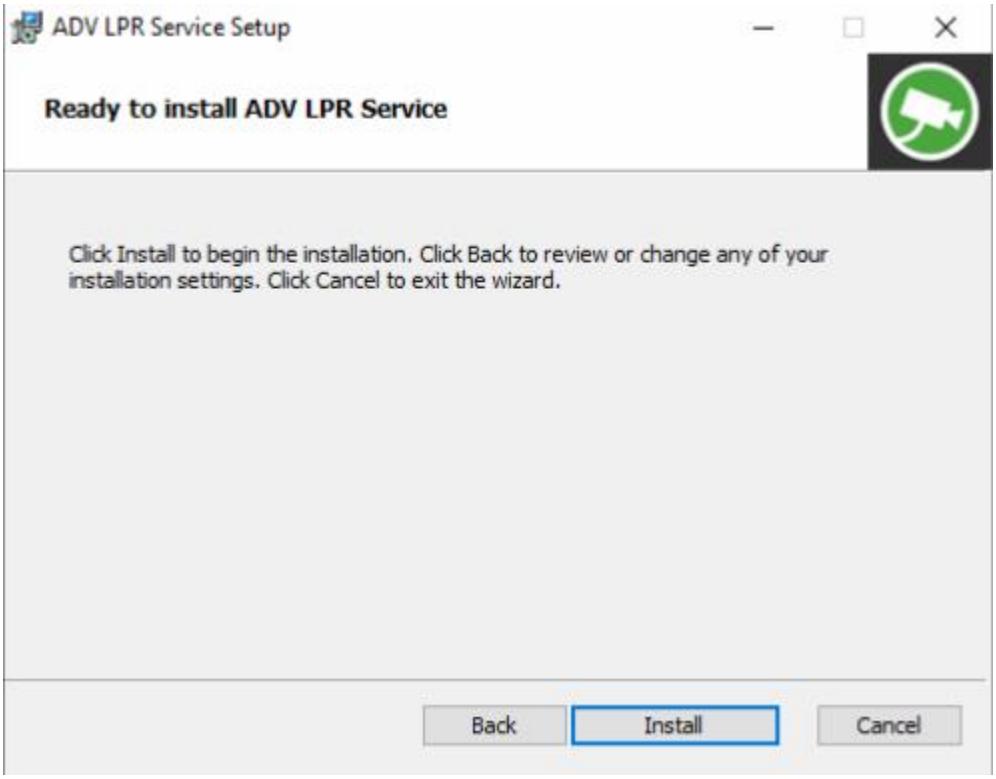


Der HTTP-Port, auf dem der LPR-Dienst gehostet wird, ist standardmäßig 8090. Ändern Sie den Port, falls der Standardport für einen anderen Zweck reserviert ist.
Der Hauptserver verwendet standardmäßig Port 8082. Legen Sie die Adresse und den Port des Hauptservers fest, damit der LPR-Dienst eine Verbindung zum richtigen Hauptserver herstellen kann.
Die Ereigniswarteschlange (Event queue) verwendet standardmäßig Port 5672. Die Ereigniswarteschlange wird bei der Installation des LM-Dienstes mitinstalliert, wobei der verwendete Port der Ereigniswarteschlange festgelegt wird. Legen Sie die Adresse der Ereigniswarteschlange auf den Rechner fest, auf dem der LM-Dienst installiert ist.

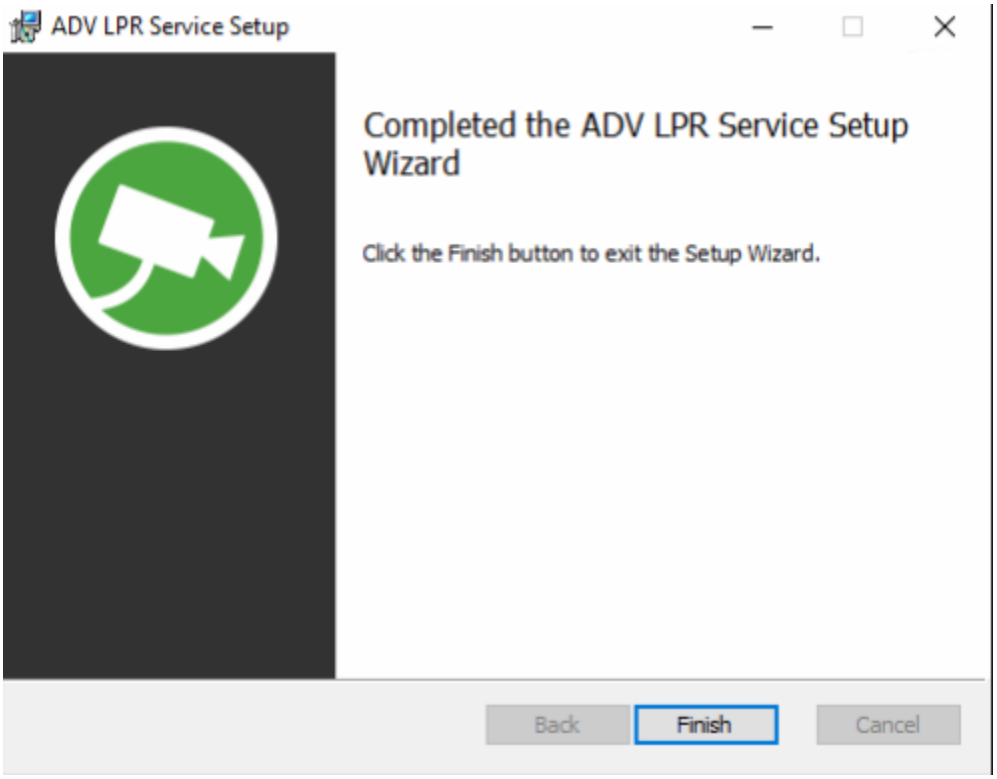
1. Wählen Sie Kontinente und Geräte aus und klicken Sie auf **Next**, um fortzufahren.



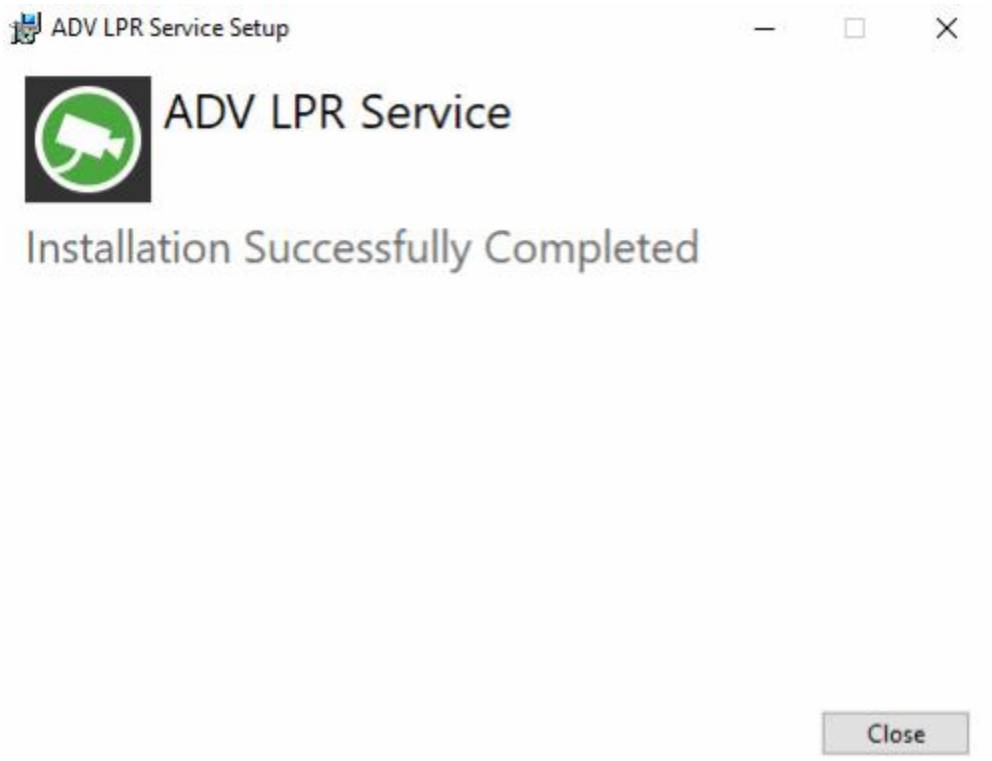
1. Klicken Sie auf **Install**, um fortzufahren, und warten Sie.
    a. Die Installation dauert eine Weile, bis sie abgeschlossen ist.
    b. Die Erstellung des Modells kann bis zu 30 Minuten dauern. Dies hängt davon ab, wie leistungsfähig die verwendete Grafikkarte ist.



1. Klicken Sie auf **Finish**, um fortzufahren.



1. Klicken Sie auf **Close**, um die Installation zu beenden.



1. Der Kennzeichenerkennungsdienst ist nun auf dem Server installiert und einsatzbereit.
    a. Der Dienst zur Kennzeichenerkennung übermittelt die Daten an den VMS-Hauptserver. Sie können den Dienst über den System Manager konfigurieren.

5.3 LPR-Datenschutz-Masken

Wenn für die Kamera Client-Privatsphärenmasken definiert sind, zeichnet der LPR-Dienst Privatsphärenmasken auf die Eingangsbilder, bevor er die Inferenz durchführt.

- Innerhalb der Privatzone kann kein Nummernschild erkannt werden.
- Thumbnail-Bilder haben Datenschutzzonen.

5.4 Land-Erkennung

Die Ländererkennung ist optional, wird aber in einigen Ländern empfohlen: Die Erkennungsgenauigkeit des Kennzeichens kann verbessert werden, wenn das Land bekannt ist.

5.4.1 Erkennung von Ländern mit Nummernschildern

Die Kennzeichenerkennung ist für Eurasien und Amerika verfügbar.

Die Ländererkennung ist optional. Sie ist nützlich in Ländern wie Finnland, wo die Buchstaben I und O den Zahlen 1 und 0 entsprechen. Wenn das Land mit hoher Sicherheit erkannt wird, können länderspezifische Regeln verwendet werden, um die Genauigkeit der Kennzeichenerkennung zu verbessern.

5.4.2 Typen von Nummernschildern

Wenn die Ländererkennung aktiviert ist, kann manchmal auch der Kennzeichentyp erkannt werden. Der Kennzeichentyp kann undefiniert oder einer der folgenden sein:

- antik
- diplomatisch
- Ausfuhr
- Militär
- provisorisch
- Vermietung
- Taxi
- Test
- Arbeit

5.5 LPR in Eurasien: Unterstützte Länder

5.5.1 Vorwahlen

In einigen Ländern sind die Nummernschilder mit Ortsvorwahlen versehen. Wenn die Ländererkennung aktiviert ist, wird auch die Vorwahl für die folgenden Länder erkannt:

- Österreich
- Deutschland
- Rumänien
- Slowenien
- Schweiz

In einem besonderen Fall kann eine Region innerhalb eines Landes erkannt werden. Die Åland-Inseln zum Beispiel haben ihre eigenen Schilder, die sich von denen in anderen Teilen Finnlands unterscheiden.

Bitte beachten Sie, dass die Genauigkeit von Land zu Land unterschiedlich ist.

Ein Kennzeichen aus nicht unterstützten Ländern kann als eines der unten aufgeführten Länder erkannt werden. Zum Beispiel können einige Kennzeichen aus Tadschikistan als Kennzeichen aus Kasachstan erkannt werden.

5.5.2 Liste der unterstützten Länder in Eurasien

- Albanien
- Andorra
- Armenien
- Österreich
- Aserbaidschan
- Weißrussland
- Belgien
- Bosnien und Herzegowina
- Bulgarien
- Kroatien
- Zypern
- Tschechische Republik
- Dänemark
- Estland
- Finnland (einschließlich Ålandinseln)
- Frankreich
- Georgien
- Deutschland
- Gibraltar
- Griechenland
- Ungarn
- Island

- Irland
- Isle of Man
- Italien
- Kasachstan
- Lettland
- Liechtenstein
- Litauen
- Luxemburg
- Malta
- Moldawien
- Monaco
- Montenegro
- Niederlande
- Nord-Mazedonien
- Norwegen
- Polen
- Portugal
- Rumänien
- Russland
- San Marino
- Serbien
- Slowakei
- Slowenien
- Spanien
- Schweden
- Schweiz

- Türkei
- Ukraine
- Vereinigtes Königreich
- Vatikan

5.6 LPR AUF DEM AMERIKANISCHEN KONTINENT: UNTERSTÜTZTE LÄNDER

Bitte beachten Sie, dass die Genauigkeit von Land zu Land unterschiedlich ist.
Ein Kennzeichen aus nicht unterstützten Ländern könnte als eines der unten aufgeführten Länder erkannt werden.

5.6.1 Länder und Staaten

Die unten aufgeführten Länder/Staaten werden unterstützt.

- Argentinien
- Bolivien
- Brasilien (altes und neues Kennzeichen)
- Kanada
- Alberta
- Britisch-Kolumbien
- Manitoba
- Ontario
- Quebec
- Saskatchewan
- Chile
- Kolumbien
- Mexiko
- Paraguay
- Peru
- Vereinigte Staaten

- Alabama
- Alaska
- Arizona
- Arkansas
- Kalifornien
- Colorado
- Connecticut
- Delaware
- District of Columbia
- Florida
- Georgien
- 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-Ereignisse, Ereignisse und Erkennung

5.7.1 Geräte

Die Verarbeitung der Nummernschilderkennung kann mit unterschiedlicher Hardware erfolgen. Unterstützte Hardware sind CPU, Intel GPU, Nvidia GPU und MAIC (Mirasys AI Card).

5.7.2 LPR-Ereignisse

Live-LPR-Ereignisse werden im Smart Recognition Plugin in Spotter angezeigt. LPR-Ereignisse können mit dem Smart Search-Plugin in Spotter gesucht werden.

5.7.3 Visualisierung des erkannten Kennzeichens

Erkannte Nummernschilder können in Spotter mit dem VCA-Visualisierungs-Plugin visualisiert werden.

5.8 LPR Alarmauslöser und Konfiguration

5.8.1 Alarmauslöser

Für jede Identitätsliste, die in den Einstellungen der Listenverwaltung konfiguriert ist, kann ein Alarmauslöser auf dem VMS-Server erstellt werden.

5.8.2 LPR-Konfiguration

Der LPR-Dienst kann in der Anwendung System Manager auf der Registerkarte LPR-Einstellungen im Fenster Kameraeinstellungen konfiguriert werden.

Die LPR-Einstellungen enthalten Informationen über die vom Dienst verarbeiteten Kamera-Videoströme. Jede Stream-Einstellung bezieht sich auf die Kamera und den Stream auf dem Rekorder. Jeder LPR-Dienst kann seine eigenen Grenzwerte haben.

5.9 LPR-Leistung

5.9.1 Testmaschine

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

5.9.2 Durchführung des Tests

- Der LPR-Dienst wird vor Beginn des Tests neu gestartet.
    - Dadurch wird Speicherplatz auf dem Testrechner freigegeben.
- Es wird HW-Videodekodierung verwendet.

- Der beste FPS-Wert ist orange markiert.
    - Dies ist der beste Wert ohne Frame-Skipping.

5.9.3 Testergebnisse

5.9.4 CPU

Streams	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	Prozess-speicher
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

Streams	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	Prozess-speicher
4	3840 x 2160	80	80	70 %		60 %	9.2 GB

5.9.5 NVIDIA GPU

Streams	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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

5.9.6 INTEL GPU

Streams	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
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	Größe	Input FPS	Output FPS	Process CPU	NVIDIA GPU	NVIDIA decode	INTEL GPU	Prozess-speicher
1	3840 x 2160	21	**21**	10 %		30 %	55 %	2.0 GB
2	3840 x 2160	39	39	27 %		60 %	98 %	5.2 GB

Diese Tests sind indikativ und möglicherweise nicht direkt auf Produktionssysteme anwendbar.

6 EASY LPR

Die Easy LPR-Integration bietet Ihnen die Möglichkeit, die von der Kamera erfassten Kennzeichen an das Mirasys VMS zu übermitteln und die Kennzeichenlisten der Kamera zu aktualisieren.

Hier finden Sie eine Anleitung zur Verwendung dieses Spotter-Plugins.

Weitere Informationen zu den unterstützten Kameras finden Sie hier.

6.1 LIZENZIERUNG

Für das Plugin ist keine separate Lizenz erforderlich. Die Mirasys-VMS-Serverlizenz legt fest, wie viele ANPR-Kanäle hinzugefügt werden können.

Der Name der Funktion lautet **Anpr Channels Limit**, und der Name des steuerbaren Werts lautet **Nutzungslimit**.



6.2 KONFIGURATIONSPROZESS

6.2.1 Konfigurationsprozess

1. Konfigurieren Sie die LPR-Funktionalität für die verwendeten Kameras (weitere Informationen finden Sie auf der Website des Herstellers)
2. Überprüfen Sie, ob die Kennzeichen auf der Kameraseite korrekt erkannt werden.
3. Fügen Sie Kameras zum Mirasys VMS hinzu.
    a. Verwenden Sie einen nativen Kameratreiber.
4. Überprüfen Sie, ob die Mirasys VMS-Lizenz LPR-Kameras unterstützt.
5. Aktivieren Sie Easy LPR (eine ausführliche Anleitung dazu finden Sie hier)

Hier finden Sie die Liste der unterstützten Kameras. In dieser Liste sind die getesteten ANPR-/LPR-Kameras aufgeführt.
Je nach API des Kameraherstellers müssen möglicherweise Änderungen an der XML-Datei der Kamera vorgenommen werden.

6.2.2 Kameraspezifische Konfigurationen

Falls es keine herstellerspezifischen Anweisungen gibt, können Sie die folgenden Anweisungen befolgen:
Aktivieren von Easy LPR

6.2.2.1 Axis und Axis License Plate Verifier

- Stellen Sie sicher, dass die neueste Version der Axis License Plate Verifier-Software auf der Kamera installiert ist.
- Stellen Sie sicher, dass der Axis License Plate Verifier lizenziert ist und ordnungsgemäß funktioniert.
- Stellen Sie sicher, dass Sie den neuesten Axis-Treiber für VMS verwenden.

Damit der Axis License Plate Verifier Daten an den VMS-Server sendet, muss die XML-Datei des Treibers bearbeitet werden.

- Öffnen Sie die Datei „NewAxisIPCapture.xml“ und bearbeiten Sie sie mit dem Notepad.
    - Standardpfad: C:\Program Files\DVMS\DVR
- Suchen Sie diesen Abschnitt:

```
<!-- Axis License Plate Verifier configuration -->
 <AxisANPR>
```

```
      <!-- 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 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>
    </AxisANPR>
```

- In diesem Abschnitt müssen Sie den Abschnitt <NetworkInterface></NetworkInterface> bearbeiten.
- Fügen Sie dort die IP-Adresse des VMS-Servers ein und, falls ein Failover vorhanden ist, auch diese.
    - Wiederholen Sie diesen Vorgang für alle erforderlichen Server.
    - Bitte beachten Sie, dass diese Angaben bei Treiber- oder VMS-Updates überschrieben werden.
- Nun können Sie diese Datei speichern, die Datei im DVR-Ordner ersetzen und den DVRServer-Dienst neu starten.

6.2.2.2 Hanwha Wisenet und Vaxtor

- Stellen Sie sicher, dass die neueste Vaxtor-LPR-Software auf der Kamera installiert ist.
- Stellen Sie sicher, dass Vaxtor LPR lizenziert ist und ordnungsgemäß funktioniert.
- Stellen Sie sicher, dass Sie den neuesten Hanwha Wisenet-Treiber für VMS verwenden.

Damit Vaxtor Daten an den VMS-Server sendet, muss die XML-Datei des Treibers bearbeitet werden.

- Öffnen Sie die Datei „WisenetIPCapture.xml“ und bearbeiten Sie sie mit dem Notepad.
    - Standardpfad: C:\Program Files\DVMS\DVR
- Suchen Sie diesen Abschnitt:

```
<!-- 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 diesem Abschnitt müssen Sie den Abschnitt <NetworkInterface></NetworkInterface> bearbeiten.
- Fügen Sie dort die IP-Adresse des VMS-Servers ein und, falls ein Failover vorhanden ist, fügen Sie auch diese hinzu.
    - Wiederholen Sie diesen Vorgang für alle erforderlichen Server.
    - Bitte beachten Sie, dass diese Angaben bei Treiber- oder VMS-Updates überschrieben werden.
- Nun können Sie diese Datei speichern, die Datei im DVR-Ordner ersetzen und den DVRServer-Dienst neu starten.

6.2.2.3 Panasonic und Vaxtor

- Stellen Sie sicher, dass die neueste Vaxtor-LPR-Software auf der Kamera installiert ist.
- Stellen Sie sicher, dass Vaxtor LPR lizenziert ist und ordnungsgemäß funktioniert.
- Stellen Sie sicher, dass Sie den neuesten Panasonic-Treiber für das VMS verwenden.

Damit Vaxtor Daten an den VMS-Server sendet, muss die XML-Datei des Treibers bearbeitet werden.

- Öffnen Sie die Datei „NewPanasonicIPCapture.xml“ und bearbeiten Sie diese mit Notepad.
    - Standardpfad: C:\Program Files\DVMS\DVR
- Suchen Sie diesen Abschnitt:

```
  <!-- 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 diesem Abschnitt müssen Sie den Abschnitt <NetworkInterface></NetworkInterface> bearbeiten.
- Fügen Sie dort die IP-Adresse des VMS-Servers ein und, falls ein Failover vorhanden ist, auch diese.

- Wiederholen Sie diesen Vorgang für alle erforderlichen Server.
- Bitte beachten Sie, dass diese Angaben bei Treiber- oder VMS-Updates überschrieben werden.

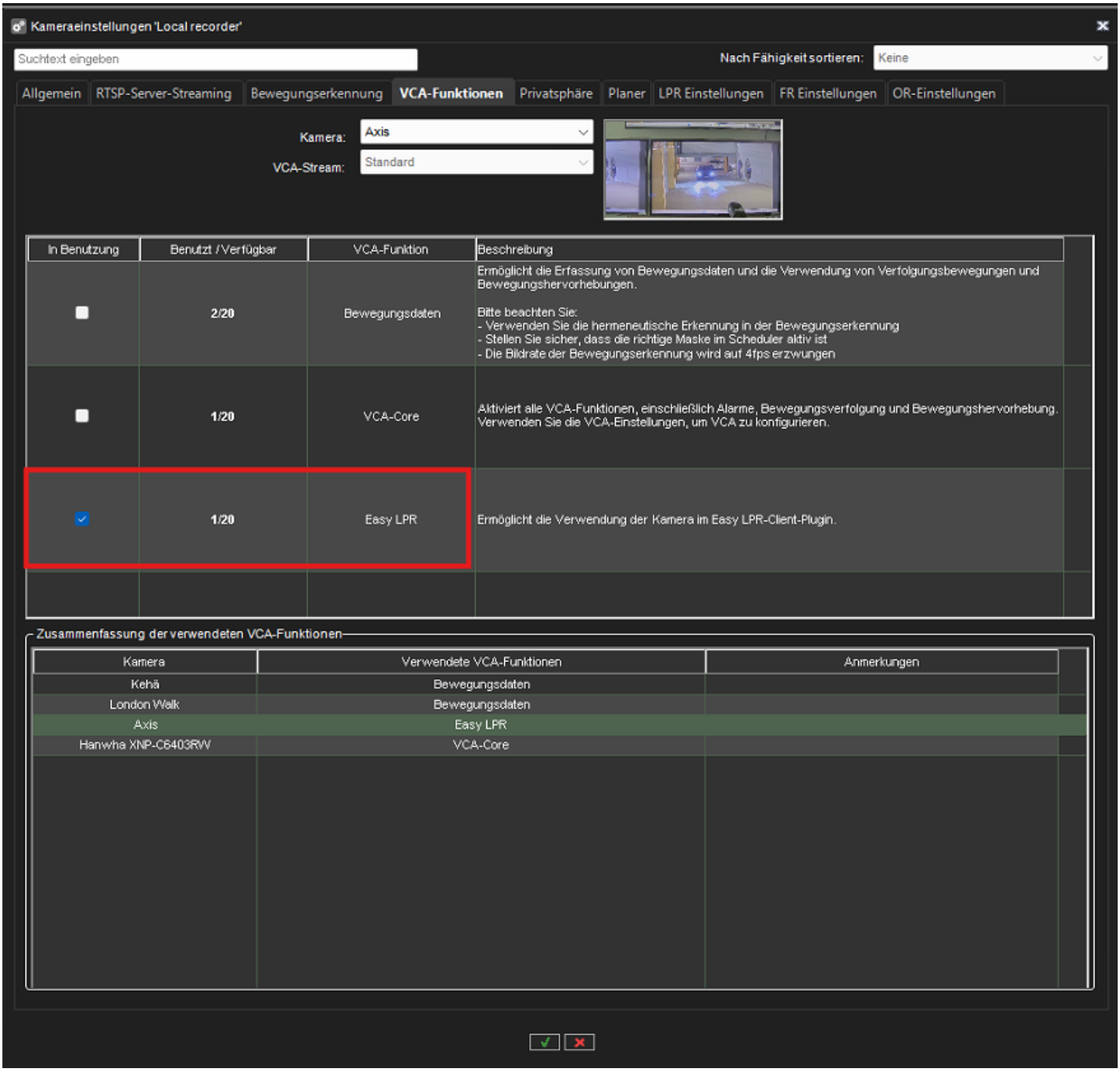
- Nun können Sie diese Datei speichern, die Datei im DVR-Ordner ersetzen und den DVRServer-Dienst neu starten.

6.3 AKTIVIEREN VON EASY LPR

1. Öffnen Sie **VMS-Server**
2. Öffnen Sie **Kameras**



1. Klicken Sie auf **VCA-Funktionen**
1. Wählen Sie die LPR-Kamera
1. **Easy LPR** aktivieren
1. Klicken Sie auf **Speichern**

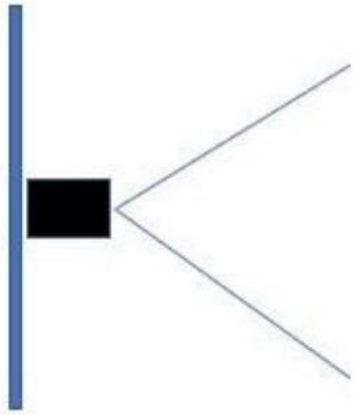


Wenn die ausgewählte Kamera Easy LPR nicht unterstützt, ist die Option, sie als „In Benutzung“ zu kennzeichnen, deaktiviert.

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

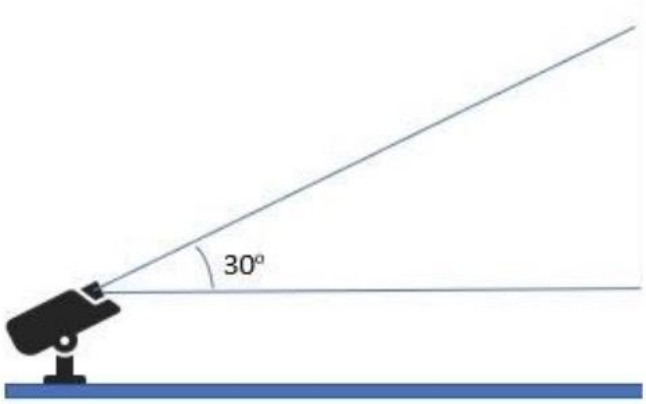
7 KAMERA-INSTALLATION LPR-LEITFADEN

7.1 ES WIRD EMPFOHLEN, DIE KAMERA IN DER MITTE DES FAHRZEUGS ZU INSTALLIEREN.



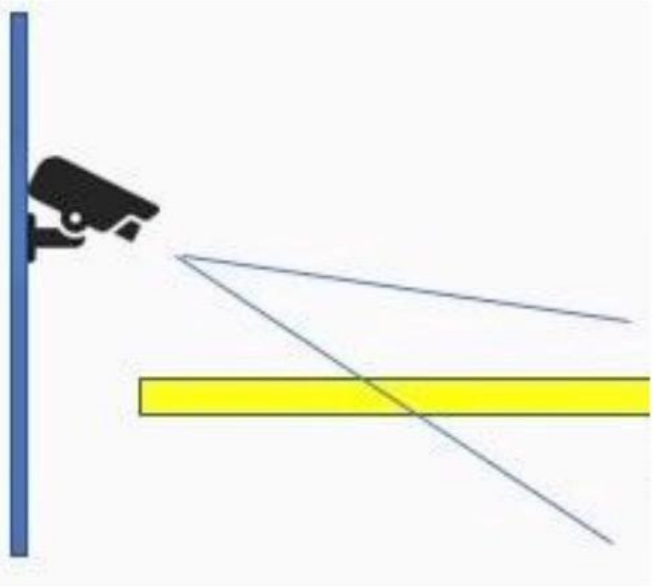


7.2 WENN DIE KAMERA AM STRAßENRAND ODER AUF DER FAHRBAHN INSTALLIERT IST, SOLLTE DER WINKEL 30 GRAD NICHT ÜBERSCHREITEN.





7.3 Die Kamera sollte höher als die Scheinwerfer des Fahrzeugs angebracht werden, damit die Scheinwerfer des Fahrzeugs nicht direkt auf die Kamera gerichtet sind.





7.4 Stellen Sie sicher, dass das Nummernschild mindestens 120 Pixel breit und mindestens 50 Pixel hoch ist.



Höhe mindestens 50 Pixel

Breite mindestens 120 Pixel

7.5 Der Neigungswinkel des Kennzeichens muss innerhalb von +/- 10 Grad liegen.



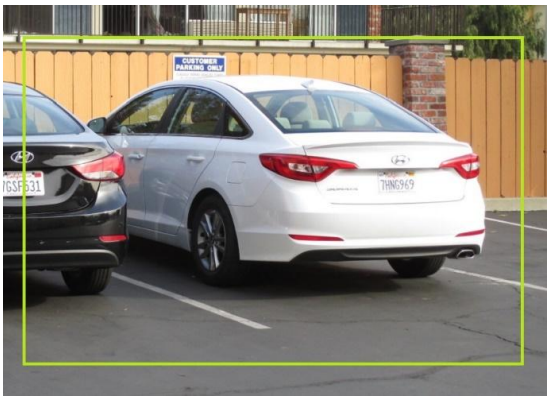


7.6 LPR-Einstellungen in der Anwendung System Manager

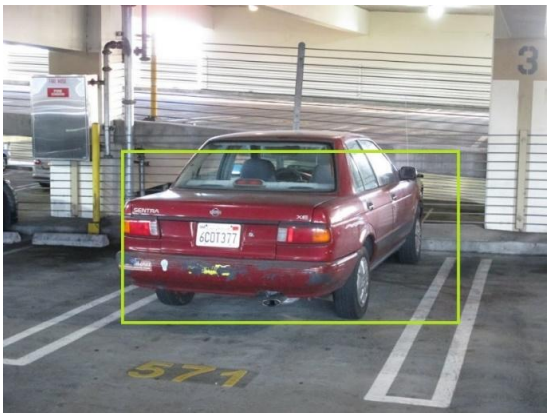
Stellen Sie sicher, dass die richtige Region (Amerika/Eurasien) ausgewählt ist.

7.6.1 Festlegung der Region von Interesse

Die Region von Interesse wird verwendet, um zu definieren, wo die Erkennung Nummernschilder findet.



Lassen Sie einen gewissen Spielraum zu der Region von Interesse, um nicht teilweise sichtbare Platten zu erkennen.



Das gesamte Nummernschild befindet sich innerhalb des interessierenden Bereichs, und das Nummernschild wird erkannt.



Das Nummernschild befindet sich nicht vollständig innerhalb des interessierenden Bereichs, und das Nummernschild wird nicht erkannt.

7.6.2 Ermöglichung der Anerkennung von Ländern

In vielen Ländern ähnelt der Buchstabe O der Zahl 0, und der Buchstabe I sieht genauso aus wie die Zahl 1. Die Aktivierung der Ländererkennung verbessert die Erkennungsgenauigkeit in diesen Fällen.



Das Format für das brasilianische Kfz-Kennzeichen ist beispielsweise "abc1d23".

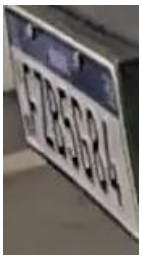
7.7 Allgemeine Probleme und Lösungen

7.7.1 Unvollständiges Nummernschild



Lösung: Legen Sie den Interessenbereich nicht zu nahe an den Bildgrenzen fest.

7.7.2 Blickwinkel macht Nummernschilder unleserlich



Lösung 1: Bewegen Sie die Kamera an einen besseren Ort.

Lösung 2: Stellen Sie den Bereich von Interesse so ein, dass das Schild erkannt wird, wenn es aus einem besseren Winkel sichtbar ist.

7.7.3 Scheinwerfer anderer Fahrzeuge reflektieren vom Nummernschild



Lösung 1: Bringen Sie die Kamera an einen besseren Ort.

Lösung 2: Stellen Sie den Interessenbereich so ein, dass das Kennzeichen auch dann erkannt wird, wenn die Scheinwerfer anderer Fahrzeuge nicht in die Richtung des Kennzeichens zeigen.

7.7.4 Das Nummernschild ist zu klein



Lösung 1: Bewegen Sie die Kamera an einen besseren Ort oder zoomen Sie hinein.

Lösung 2: Stellen Sie den Bereich von Interesse so ein, dass das Kennzeichen erkannt wird, wenn sich das Fahrzeug näher an der Kamera befindet.

Lösung 3: Erhöhen Sie den Wert für die Mindesthöhe des Kennzeichens in den LPR-Einstellungen, damit die Erkennung kleiner Kennzeichen ignoriert wird.

7.7.5 Das Nummernschild ist unscharf



Lösung 1: Passen Sie die Schärfe an und verlängern Sie die Verschlusszeit in den Einstellungen der Kamera.

Lösung 2: Erhöhen Sie die Beleuchtung des Bereichs.

7.7.6 Das Nummernschild ist überbelichtet



Lösung 1: Passen Sie die Bildeinstellungen der Kamera an.

Lösung 2: Überprüfen Sie den Installationsort der Kamera und verschieben Sie sie höher, damit die Scheinwerfer nicht von der Platte reflektiert werden.

8 MIRASYS VCA-LEITFADEN

8.1 ÜBER MIRASYS VCA

Mirasys VCA (Video Content Analytics) umfasst eine Reihe von Echtzeit-Videoanalyselösungen, die mithilfe fortschrittlicher Bildverarbeitungsalgorithmen Videomaterial in verwertbare Informationen umwandeln. Das Herzstück des Produkts ist eine hochentwickelte Engine zur Objekterkennung und -verfolgung, die bewegliche und stationäre Ziele kontinuierlich verfolgt.

Die Tracking-Engine zeichnet sich durch eine integrierte Robustheit gegenüber störenden Umgebungsbedingungen wie wechselnder Beleuchtung, sich bewegendem Laub, plätscherndem Wasser usw. aus.

Mirasys VCA ist ein Oberbegriff für eine Reihe von Zusatzmodulen für die Videoanalyse, die unter anderem folgende Funktionen umfassen:

- Fähigkeit, aggressives Verhalten zu erkennen.
- Fähigkeit, Stürze zu erkennen.
- Fähigkeit, das Überqueren von Fahrbahnen zu erkennen.
- Fähigkeit, wiederholtes Verhalten zu erkennen.
- Fähigkeit, Personen mit erhobenen Händen zu erkennen.
- Die Deep-Learning-Objekt-Tracker-Klassen zum Auslösen von Alarmen umfassen nun Personen, Busse, Motorräder, Fahrräder, PKWs, Transporter, LKWs, Gabelstapler und Taschen.
- Unterstützung für verschiedene mögliche Ereigniszustände: Start (Standard), Ein, Stopp. Beachten Sie, dass die Zustände „Ein“ und „Stopp“ nur verfügbar sind, wenn sie in den VCA-Core-Konfigurationsdateien definiert sind.

Weitere Funktionen sind:

8.1.1 Objektverfolgung anhand von Bewegungsdaten

Hervorhebung und Verfolgung von Objekten anhand von Bewegungsdaten mit automatischer Zoomfunktion.

Die Bewegungsdaten werden durch eine serverbasierte, hermeneutische Bewegungserkennung generiert.

8.1.2 Zählung mittels Tripwire

Neben der Funktion zur Verfolgung von Objekten in Bewegung bietet das System eine Linienzählung für an der Decke montierte Kameras sowie eine clientbasierte Visualisierung der Zählwerte über den Spotter-Client.

8.1.3 Erkennung von Objektverhalten und -attributen

Zur kontinuierlichen Verfolgung und Klassifizierung von sich bewegenden und stationären Zielen und Merkmalen steht eine umfassende Palette regelbasierter Filter zur Verfügung, darunter „Betreten“, „Verlassen“, „Erscheinen“, „Verschwinden“, „stillstehende Objekte“, Richtungsbeschränkungen, Objektzählung, Herumlungern, Objekttyp und Objektgeschwindigkeit.

Es werden mehrere Filter und Regeln für beliebige Kombinationen mehrerer überlappender Erkennungszonen unterstützt, zusätzlich zu einer fortschrittlichen Personenverfolgungs-Engine, die für die Verfolgung von Personen in unübersichtlichen Innenräumen wie beispielsweise im Einzelhandel optimiert ist. Enthält spezielle, hochpräzise Zählfunktionen, die für den Einsatz in belebten Umgebungen optimiert sind.

8.1.4 Verwandte Analyseoptionen

Erhältlich als eigenständige Anwendungen, Produkte oder über projektbezogene Integrationen:

- Kamerabasierte (integrierte, Edge-)Analysen unterstützen ausgewählte Kamerahersteller und deren Funktionen über herstellerspezifische Integrationsschnittstellen.
- Audioanalyse-Technologien beziehen sich auf Software zur Extraktion von Informationen und Bedeutungen aus Audiosignalen, wie beispielsweise die Erkennung von Glasbruchgeräuschen usw.
- Gesichtserkennungstechnologien beziehen sich auf Software oder Kamerafunktionen zur automatischen Identifizierung oder Überprüfung der Identität, des Alters, des Geschlechts usw. einer Person anhand von Videomaterial.
- Technologien zur Kennzeichenerkennung (ANPR/LPR) beziehen sich auf Software oder Kamerafunktionen zur automatischen Identifizierung von Fahrzeug- oder Containernummern.

8.2 KURZANLEITUNG FÜR VCA

Mirasys VMS 9.10.0 enthält VCA-Deep-Learning-Analysedateien für die VCA-KI-Erkennung V2.2.5, für die eine NVIDIA-GPU sowie GPU-Treiber des NVIDIA CUDA Toolkits 11.8 erforderlich sind. Das NVIDIA CUDA Toolkit v11.8 kann von der NVIDIA-Website heruntergeladen werden: https://developer.nvidia.com/cuda-11-8-0-download-archive

Damit Sie schnell loslegen können, haben wir nachfolgend die wichtigsten Themen aufgelistet. Bitte führen Sie die folgenden Schritte für jeden Server durch:

1. Entscheiden Sie, welche VCA-Funktionen Ihren Anforderungen entsprechen. Lassen Sie sich beraten oder wenden Sie sich an Ihren Mirasys-Ansprechpartner.
2. Erwerben und installieren Sie ein Mirasys-VMS-System sowie den dazugehörigen Softwarelizenzschlüssel mit den erforderlichen Funktionen.
3. Fügen Sie die Videokameras hinzu, die Sie für VCA verwenden möchten, konfigurieren Sie diese und aktivieren Sie die VCA-Funktion in den Kameraeinstellungen.

4. Aktivieren Sie den hermeneutischen Bewegungserkennungsmodus für jede Kamera, die für VCA verwendet wird.
5. Exportieren Sie die VCA-Core-HW-GUID, fordern Sie den VCA-Aktivierungslizenzcode bei Mirasys an und aktivieren Sie Mirasys VCA mit diesen Lizenzen.
6. Kalibrieren Sie jede Kamera in den VCA-Einstellungen, falls eine Objektklassifizierung erforderlich ist.
7. Konfigurieren Sie den Erfassungsbereich und die Regeln für jede Kamera.
8. Konfigurieren Sie bei Bedarf Alarme auf der Grundlage der VCA-Ereignisse.
9. Überprüfen Sie die Visualisierung der VCA-Funktionalität mithilfe der Anwendung „Spotter for Windows“.

Um die HWGUID für die VCA-Lizenz zu erhalten, muss in den Kameraeinstellungen des System Managers eine Kamera aktiviert werden, damit die VCA-Engine gestartet wird. Sobald die VCA läuft, kann die VCA-HWGUID im Lizenzdialog des VMS-Servers im System Manager abgerufen werden.

Die VCA-Engine wird auf dem VMS-Server gestartet, sobald mindestens eine Kamera in den Kameraeinstellungen des System Managers für die Nutzung von VCA konfiguriert wurde. Beim allerersten Start der VCA-Engine werden die NVIDIA-Bibliotheken kompiliert, sofern Deep Learning verwendet wird. Dies kann sehr lange dauern und hängt von der verwendeten Hardware ab. Während der Kompilierung ist die VCA-Funktion nicht verfügbar.
Es wird dringend empfohlen, nach der Aktivierung der VCA zu warten, bis die NVIDIA-Bibliotheken kompiliert sind, bevor weitere Vorgänge auf dem VMS-Server durchgeführt werden.

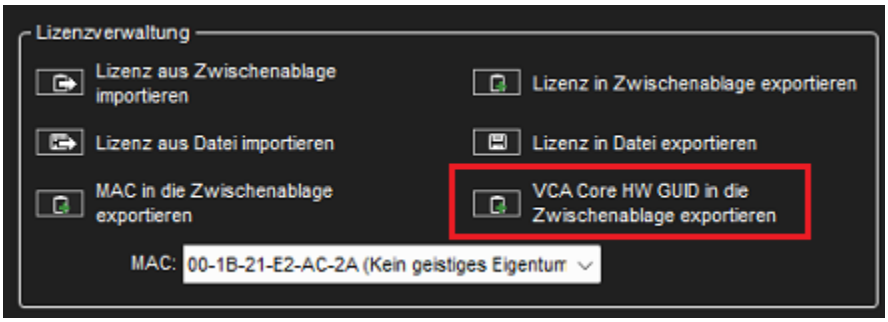
8.3 Voraussetzungen für Mirasys VCA

- VCA Core HW GUID-Datei exportieren
- VCA-Lizenz aktivieren
- Bewegungserkennungsmethode einrichten
- VCA Core für die Kameras aktivieren
- NVIDIA-GPU und CUDA Toolkit 11.8 – GPU-Treiber

Mirasys VMS 9.10.0 enthält VCA-Deep-Learning-Analysedateien für die VCA-KI-Erkennung V2.2.5, für die eine NVIDIA-GPU sowie GPU-Treiber des CUDA Toolkits 11.8 erforderlich sind. Das NVIDIA CUDA Toolkit v11.8 kann von der NVIDIA-Website heruntergeladen werden:
https://developer.nvidia.com/cuda-11-8-0-download-archive

8.3.1 VCA Core HW GUID-Datei exportieren

1. Wechseln Sie zur Registerkarte **System**
2. Öffnen Sie **Lizenzen**
3. Doppelklicken Sie auf die Lizenz
4. Wählen Sie die Option **VCA Core HW GUID in die Zwischenablage exportieren**



1. Wählen Sie die Option **Export auch Lizenzserienummer**
2. Klicken Sie auf **OK**



1. Fügen Sie den Inhalt der Zwischenablage in das Textdokument ein
2. Senden Sie es an Mirasys, um die VCA-Lizenz zu erhalten

VcaCore Hw Guid: C1092267BD20344A5853FFD2BEA65406C1884F6FA19B503395E85F8545F75E2D

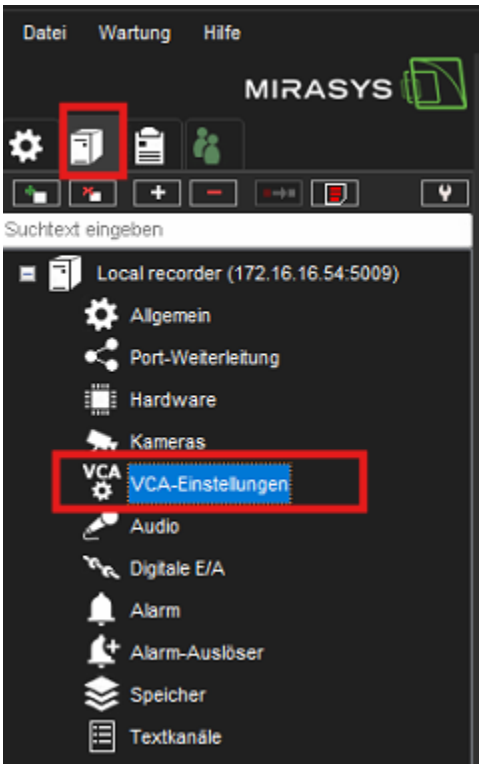
Seriennummer der Lizenz: YL9QMELM9QK5

Um die HWGUID für die VCA-Lizenz zu erhalten, muss in den Kameraeinstellungen des System Managers eine Kamera aktiviert werden, damit die VCA-Engine gestartet wird. Sobald die VCA läuft, kann die VCA-HWGUID im Lizenzdialog des VMS-Servers im System Manager abgerufen werden.

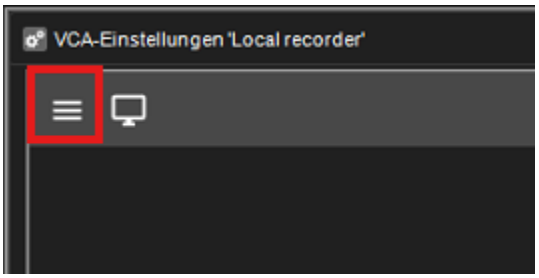
8.3.2 Aktivierung von VCA-Lizenzen

1. Wechseln Sie zur Registerkarte **VMS-Server**

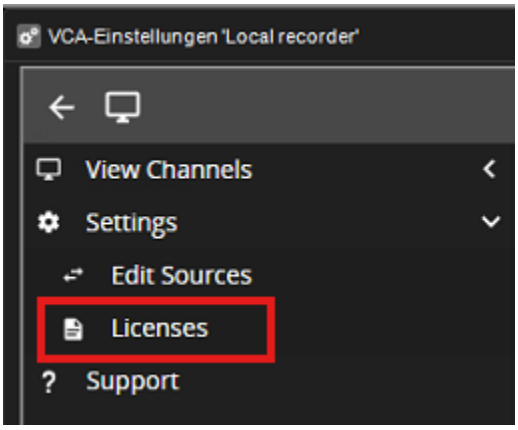
2. Öffnen Sie die **VCA-Einstellungen**



1. Klicken Sie auf das Symbol **Einstellungen** in der oberen linken Ecke



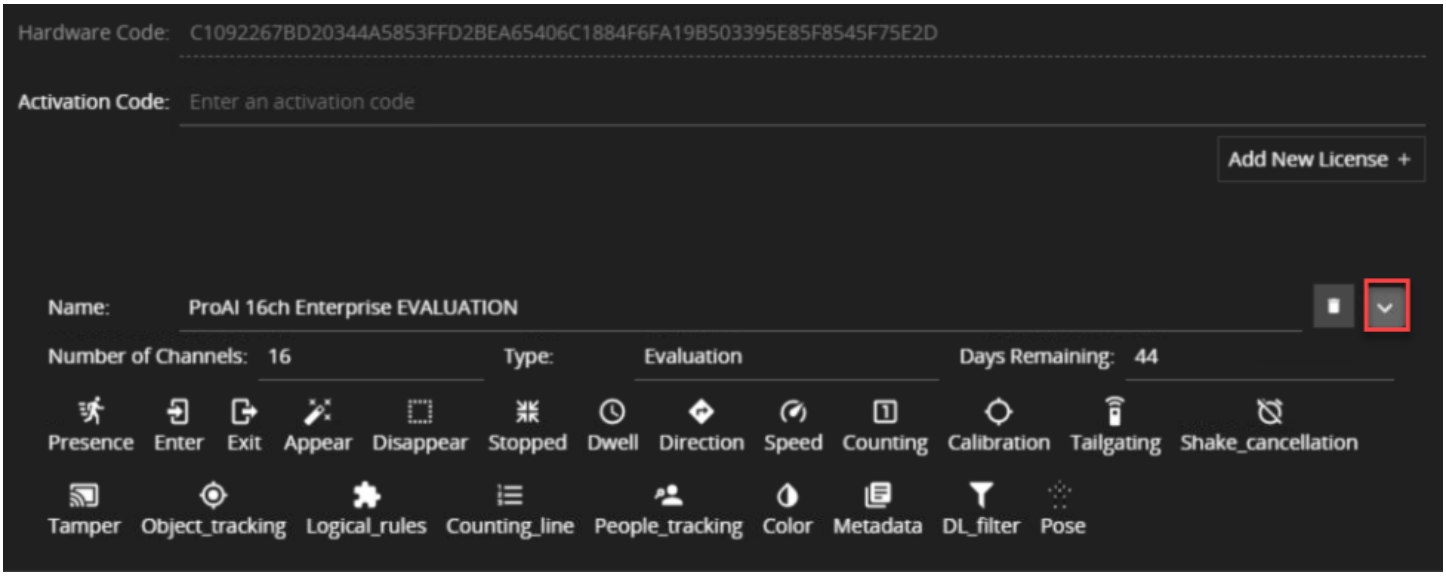
4.Wählen Sie die Option **Licenses** (Lizenzen) aus



1. Fügen Sie die Lizenz, die Sie von Mirasys erhalten haben, in das Feld **Activation code** (Aktivierungscode) ein
2. Klicken Sie auf **Add New License** (Neue Lizenz hinzufügen)

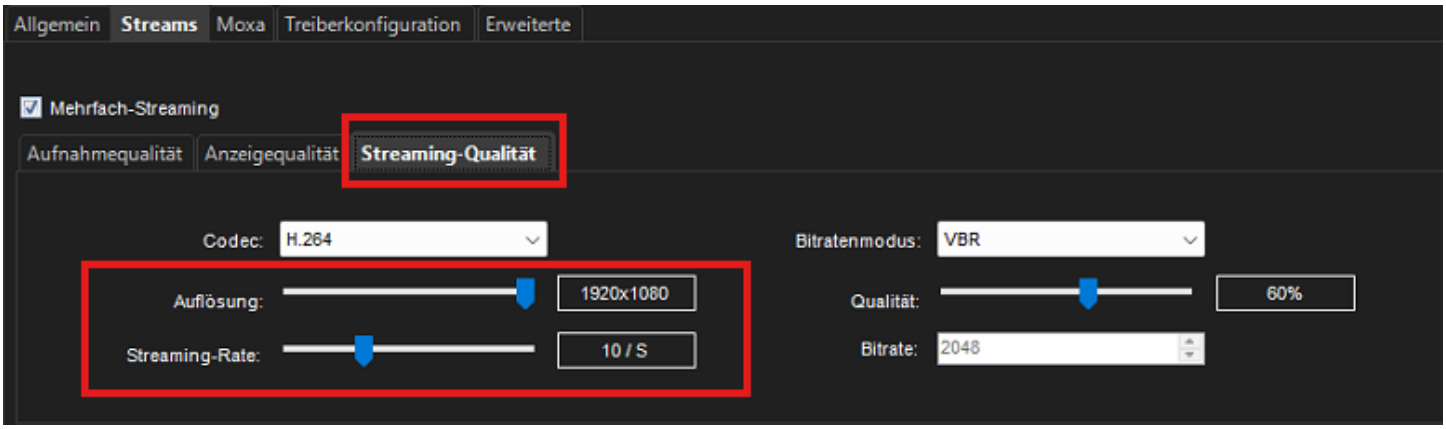


1. Sobald die Lizenz hinzugefügt wurde, werden Ihnen allgemeine Informationen zur Lizenz und zu den unterstützten Funktionen angezeigt



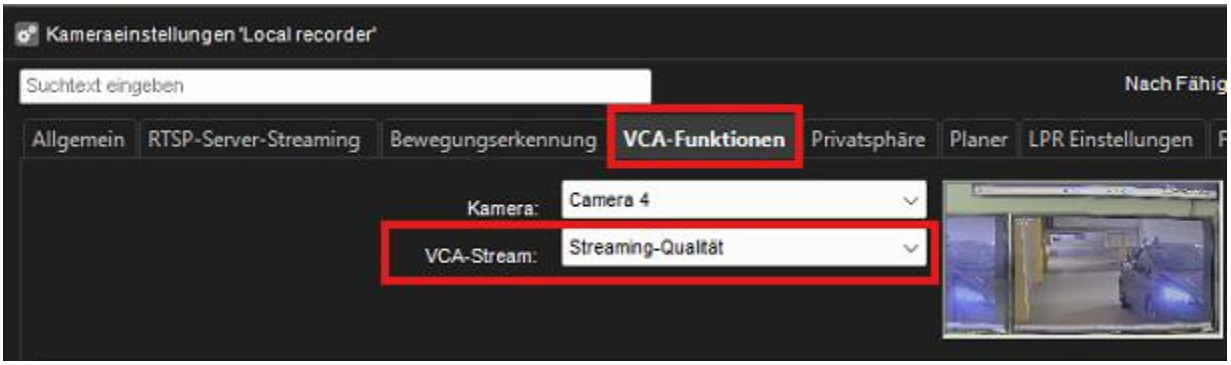
8.3.3 Einstellung der Auflösung und der Aufzeichnungsrate

1. Aktivieren Sie das Mehrfach-Streaming für die Kameras, die für Mirasys VCA verwendet werden.
2. Stellen Sie die **Auflösung der Streaming-Qualität** auf 640x480 ein.
3. Stellen Sie die **Streaming-Rate der Streaming-Qualität** auf 15 Bilder pro Sekunde ein.



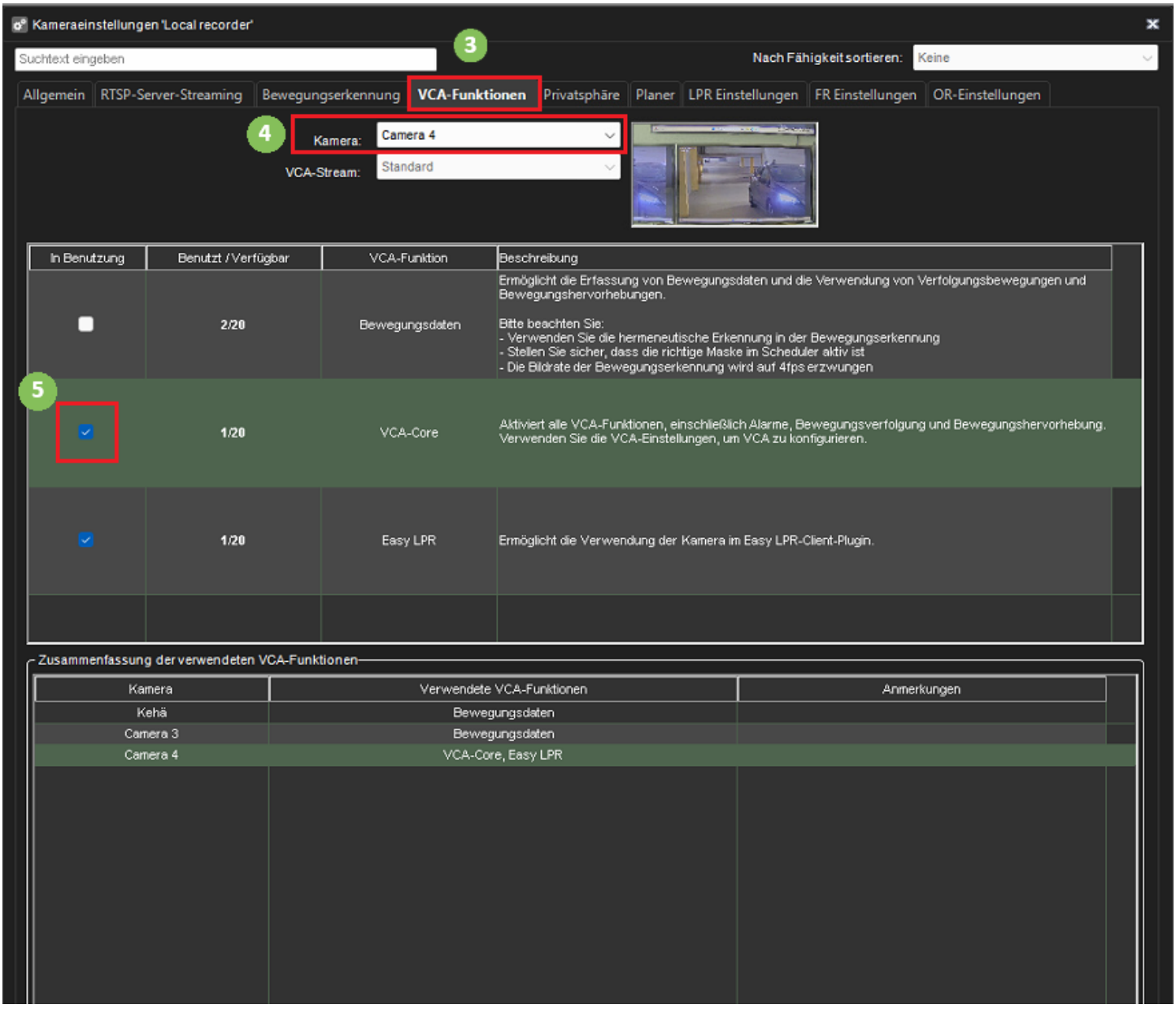
8.3.4 VCA-Stream auswählen

1. Öffnen Sie die Registerkarte **VCA-Funktionen**
2. Wählen Sie eine Kamera aus der Liste aus
3. Öffnen Sie die Dropdown-Liste **VCA-Stream** und wählen Sie die **Streaming-Qualität** aus



8.3.5 Aktivieren des VCA-Core für die Kameras

1. Wechseln Sie zur Registerkarte **VMS-Server**
2. Öffnen Sie **Kameras**
3. Wählen Sie **VCA-Funktionen**
4. Wählen Sie eine Kamera aus
5. Aktivieren Sie **In Benutzung**
6. Klicken Sie auf **OK**



8.4 Unterstützte Betriebssysteme

Mirasys nutzt für die Video-Content-Analyse (VCA) eine Drittanbieterlösung, die in das Mirasys VMS integriert ist.

Die offiziell unterstützten Betriebssysteme sind:

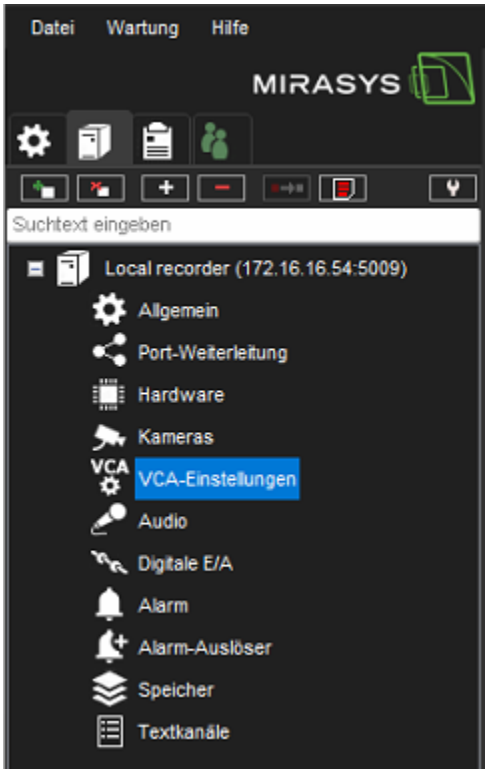
- Windows 11 / Server 2016 (oder höher)
- Ubuntu 22.04 LTS Desktop / Server (oder höher)

Mit diesen Betriebssystemen erzielen Sie die beste Leistung.

Sie können für den Mirasys-VMS-Server jedoch auch jedes andere neuere Betriebssystem oder Server-Betriebssystem verwenden.

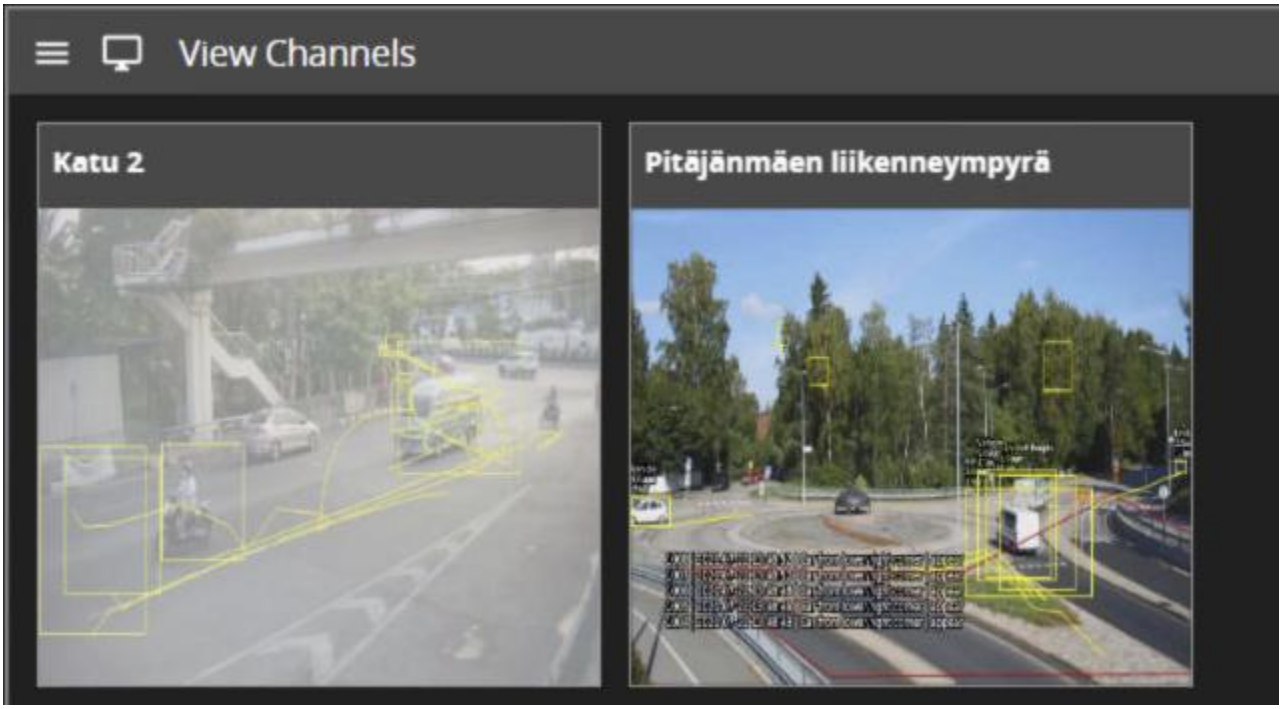
8.5 VCA-Einstellungen im System Manager

1. Wechseln Sie zur Registerkarte **VMS-Server**
2. Öffnen Sie die **VCA-Einstellungen**



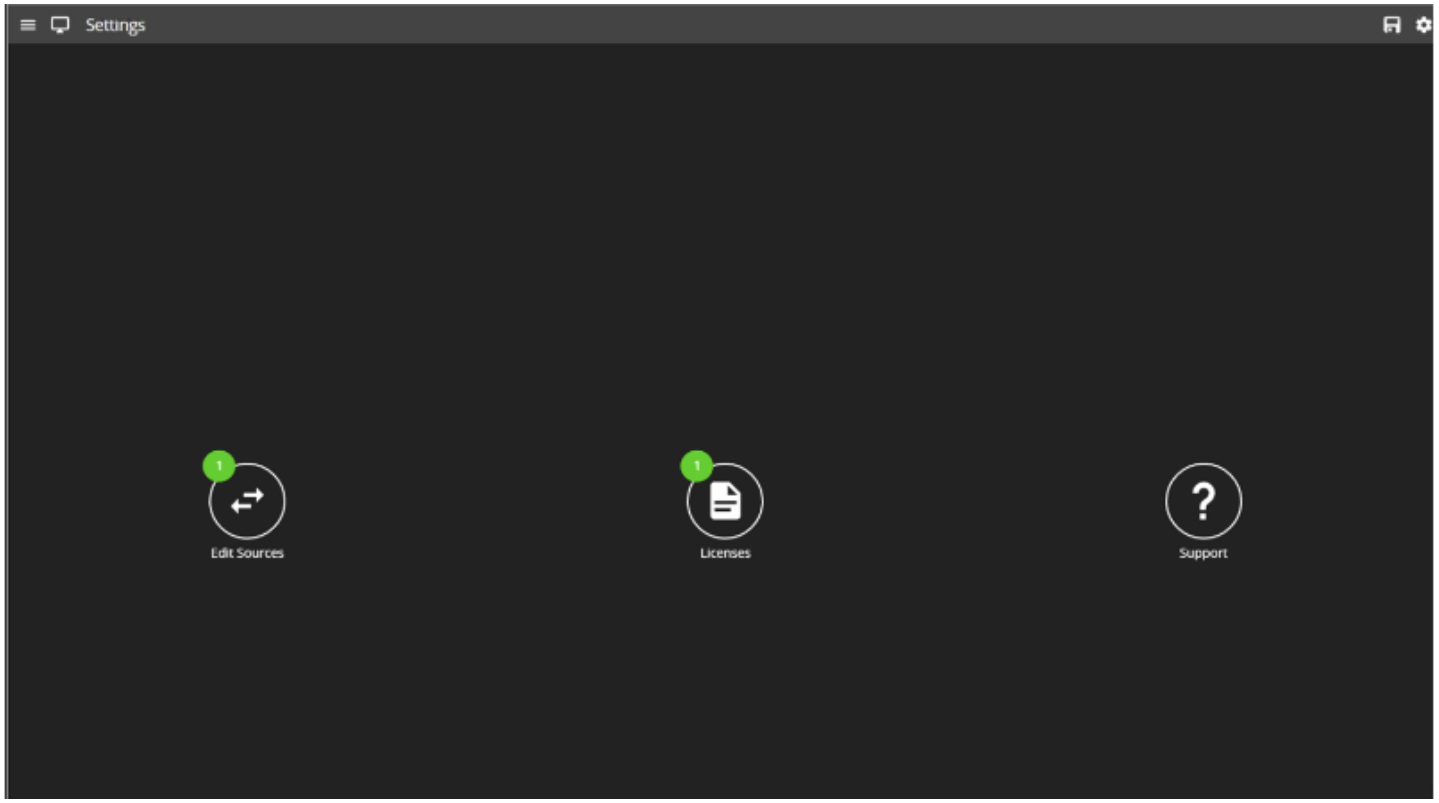
8.5.1 View Channels

Unter „View Channels“ werden alle Kameras angezeigt, für die **VCA-Core** aktiviert ist.



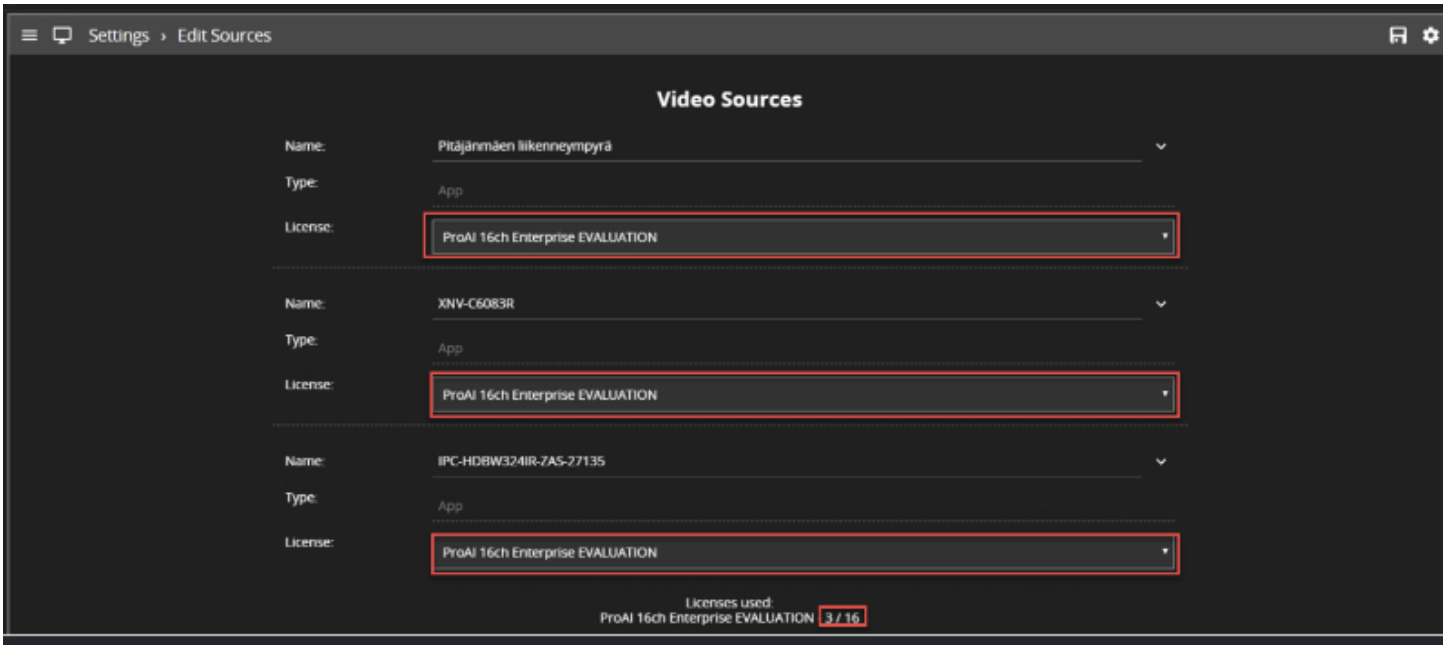
8.5.2 Einstellungen

- Edit Sources (Quellen bearbeiten)
- Licenses (Lizenzen)
- Support (Unterstützung)



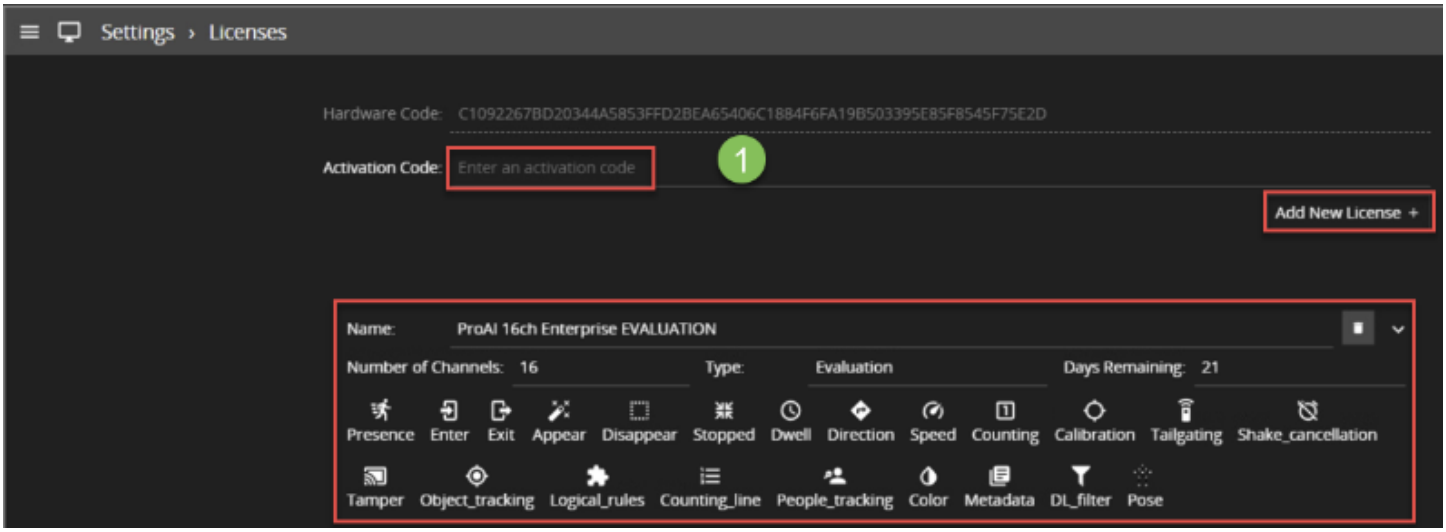
8.5.3 Edit Sources (Quellen bearbeiten)

Unter „Edit Sources“ wird angezeigt, welche Kameras für den VCA-Kern verwendet wurden.
Benutzer können außerdem den Typ der VCA-Lizenz sowie die Anzahl der für die VCA-Lizenz genutzten Kanäle einsehen.



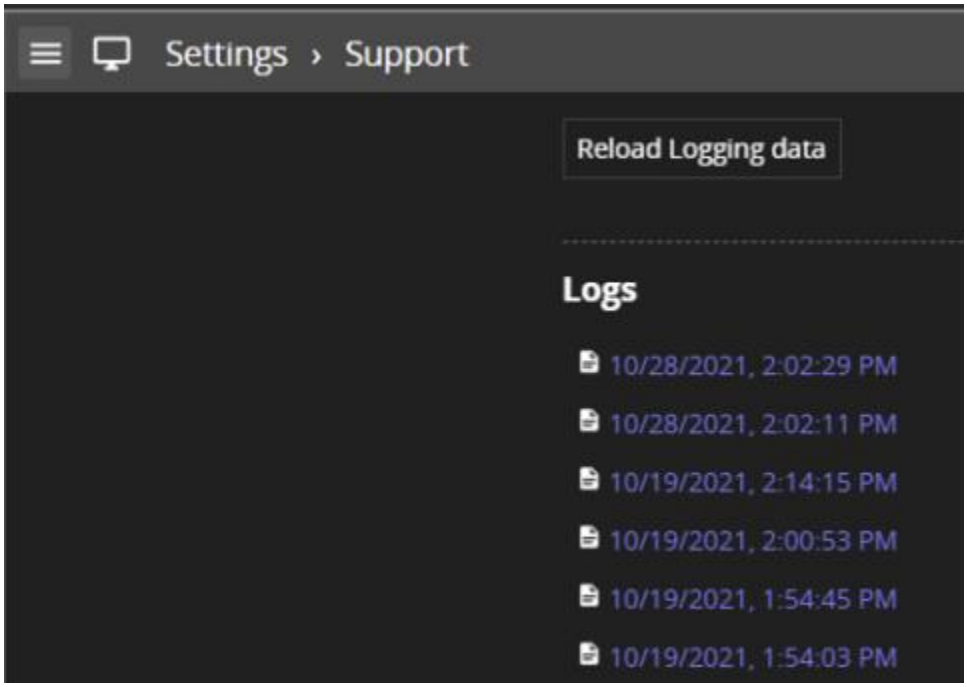
8.5.4 Licenses (Lizenzen)

Unter „Licenses“ werden der aktuelle Lizenztyp und die enthaltenen Funktionen angezeigt
Benutzer können weitere VCA-Lizenzen hinzufügen.



8.5.5 Support (Unterstützung)

Der Support zeigt Protokolle aus dem Mirasys VCA an, und Benutzer können Protokolle herunterladen.



8.6 MIRASYS VCA DEEP LEARNING

8.6.1 Anforderungen

- NVIDIA-GPU mit CUDA-Kernen
    - Eine NVIDIA-GPU mit CUDA Compute Capability 7.5 oder höher
    - Die Anzahl der Deep-Learning-Kanäle, die auf dem System genutzt werden können, hängt von den CUDA-Kernen der GPU ab
- Die neuesten NVIDIA-Grafiktreiber (mindestens 460.73 oder höher)
- CUDA Toolkit
- Mirasys VMS 9.4 oder neuer
- Deep-Learning-Objektdateien

8.6.2 Installation

1. Installieren Sie die neuesten Nvidia-Treiber auf dem System
2. Laden Sie das **Mirasys VCA Deep Learning**-Paket aus dem Mirasys-Extranet herunter
3. Entpacken Sie das Paket
4. Navigieren Sie zum Ordner **CUDA Toolkit**

5. Installieren Sie das **CUDA Toolkit** mit allen Funktionen
    a. Eine detaillierte Installationsanleitung finden Sie hier.
    b. Einige Funktionen werden nicht installiert, da Microsoft Visual Studio nicht zur Installation benötigt wird, aber das Toolkit enthält Beispieldateien
    c. Wenn Sie Mirasys VMS bereits installiert haben, müssen die VMS-Dienste vor dem Kopieren der Dateien gestoppt werden.
6. Dienste anhalten: **WDServer**, **DVRServer** und **SMServer**
    a. Dies ist nicht erforderlich, wenn Sie Version 9.6 oder neuer verwenden
7. Kopieren Sie den Inhalt des Ordners **VCA Deep Learning files** in den Pfad **C:\Program Files\DVMS\DVR\vca\bin**
    a. Dies ist nicht erforderlich, wenn Sie Version 9.6 oder neuer verwenden
    b. Dieser Pfad ist der Standardinstallationsort von Mirasys VMS: Wenn Sie Mirasys VMS an einem anderen Ort installiert haben, kopieren Sie die Dateien dorthin.
8. Starten Sie die Dienste **WDServer**, **DVRServer** und **SMServer**.
    a. Dies ist nicht erforderlich, wenn Sie Version 9.6 oder neuer verwenden

Sie haben nun die Installation abgeschlossen und können mit der Deep-Learning-Verfolgung beginnen.

Die VCA-Engine wird auf dem VMS-Server gestartet, sobald mindestens eine Kamera in den Kameraeinstellungen des System Managers für die Nutzung der VCA konfiguriert wurde. Beim allerersten Start der VCA-Engine werden die NVIDIA-Bibliotheken kompiliert, was sehr lange dauern kann. Die Dauer der Kompilierung hängt von der verwendeten Hardware ab. Während der Kompilierung ist die VCA nicht funktionsfähig.
Es wird dringend empfohlen, nach der Aktivierung der VCA zu warten, bis die NVIDIA-Bibliotheken kompiliert sind, bevor weitere Vorgänge auf dem VMS-Server durchgeführt werden.

Die Lizenzierung erfolgt über die lokale VCA-Deep-Learning-Lizenzierung oder über den Lizenzserver (virtuelle Umgebung oder, falls Sie die Lizenzen zentral verwalten möchten). Um die HWGUID für die VCA-Lizenz zu erhalten, muss in den Kameraeinstellungen des System Managers eine Kamera aktiviert werden, damit die VCA-Engine ausgeführt wird. Sobald die VCA läuft, kann die VCA-HWGUID im Lizenzdialog des VMS-Servers im System Manager abgerufen werden.

In manchen Fällen funktioniert die Erkennung möglicherweise nicht einwandfrei. Versuchen Sie bitte, die Bildqualität zu verbessern oder das Kamerabild näher an den gewünschten Erkennungsbereich heranzuzoomen.

Die Modelle wurden mit Farbbildern trainiert; bei der Verwendung von Schwarz-Weiß-Bildern oder Wärmebildern funktioniert die Erkennung daher unter Umständen nicht einwandfrei. Um dieses Problem zu beheben, können Sie versuchen, den Deep-Learning-Filter in Verbindung mit dem Objekt-Tracker zu verwenden.

8.7 MIRASYS VCA-LIZENZSERVER

Dieser Lizenzserver ermöglicht die Nutzung von VCA in virtuellen Maschinen oder die zentrale Verwaltung der Lizenzen für alle Server. Dazu müssen Sie den Mirasys VCA-Lizenzserver auf einer physischen Hardware installieren und lizenzieren.
Dieser Server kann dann Lizenzen an virtuelle Maschinen vergeben.

Diese Funktion wird ab Version 9.4 unterstützt.

Installieren Sie keine weiteren Dienste auf dem Lizenzserver. Dies kann zu Problemen bei der Lizenzierung führen.

Sie müssen den VCA-Lizenzserver nicht installieren, wenn Sie den Beispiel-Master als Lizenzserver verwenden und es sich dabei um einen physischen Server handelt. In diesem Fall ist VCA in den VMS enthalten, und Sie können Lizenzen über den System Manager – VCA-Einstellungen installieren. Verbinden Sie anschließend jeden Server mit der IP-Adresse dieses Hauptservers.

Es wird empfohlen, dieselbe VMS-Version zu verwenden, wenn ein Server als VCA-Lizenzserver fungiert.

Der VCA-Lizenzserver muss auf einem separaten physischen Rechner installiert werden und darf nicht auf demselben Rechner installiert werden, auf dem VMS installiert ist, da dies zu einer Überschneidung der VCA-Funktionen führen würde.

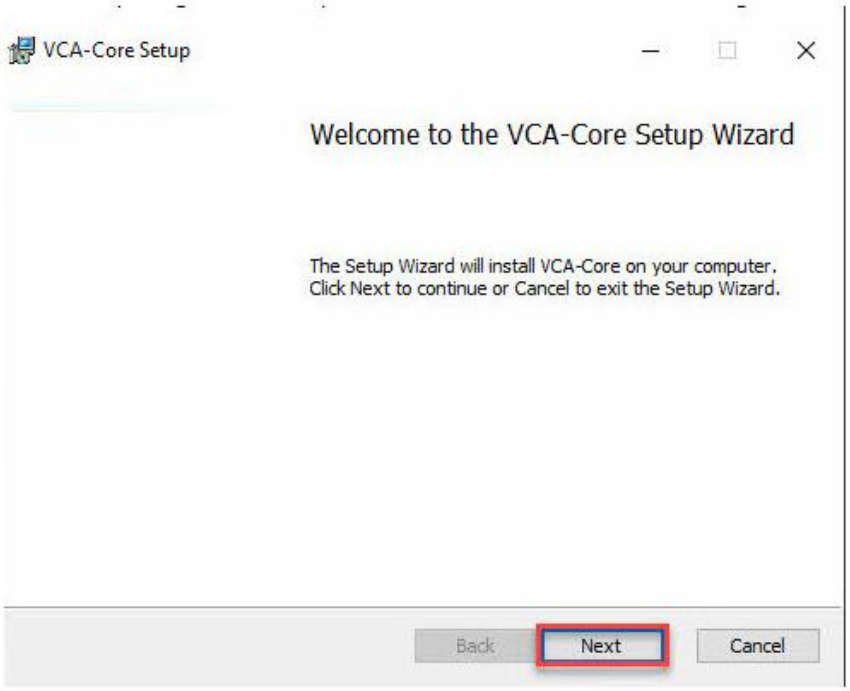
8.7.1 Port

- 8080, TCP für die Verwaltung des VCA-Lizenzservers
- 15769, TCP für den VCA-Lizenzport

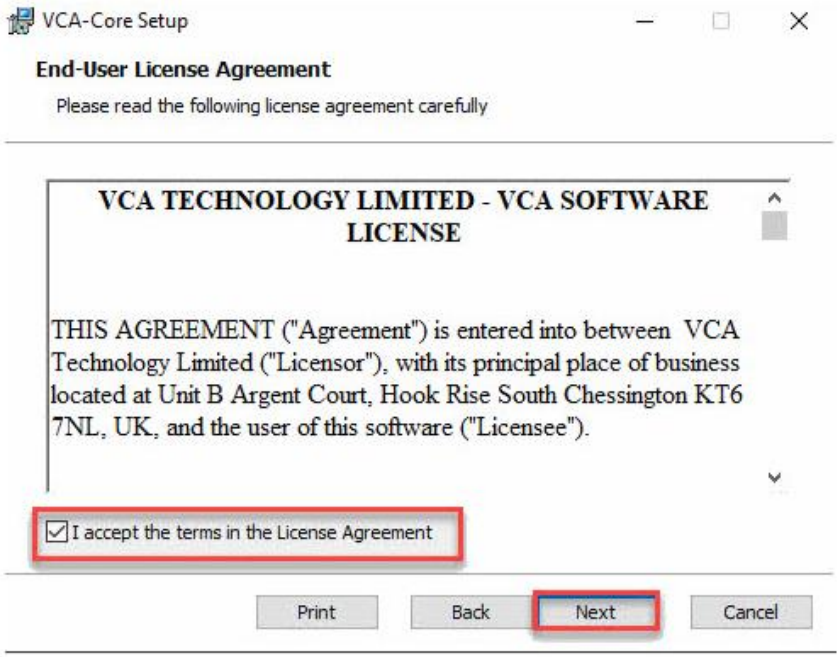
8.7.2 Installation

1. Laden Sie das neueste Mirasys VCA-Lizenzserver-Paket aus dem Mirasys-Extranet herunter

2. Entpacken Sie das ZIP-Paket an einem Ort Ihrer Wahl und starten Sie die Installation durch Doppelklick auf die Installationsdatei
3. Klicken Sie auf **Next**, um fortzufahren



1. Akzeptieren Sie die **Endbenutzer-Lizenzvereinbarung** und klicken Sie auf **Next**

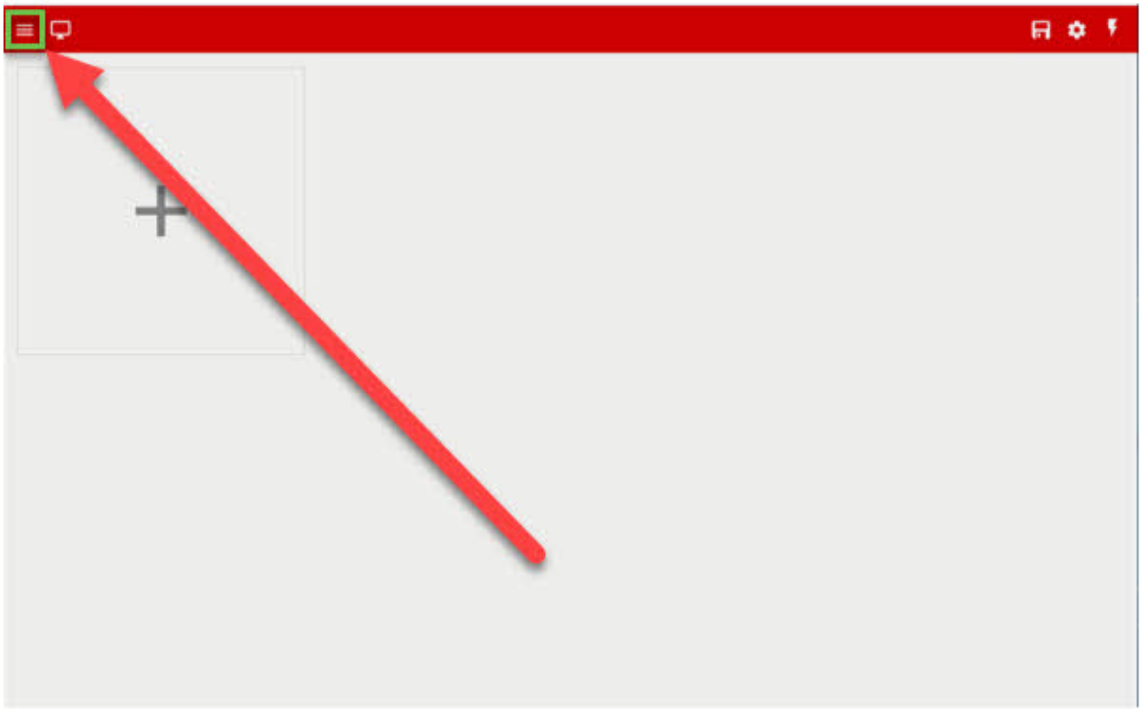


1. Befolgen Sie die Anweisungen, bis die Installation abgeschlossen ist

8.7.2.1 Nutzung und Lizenzierung

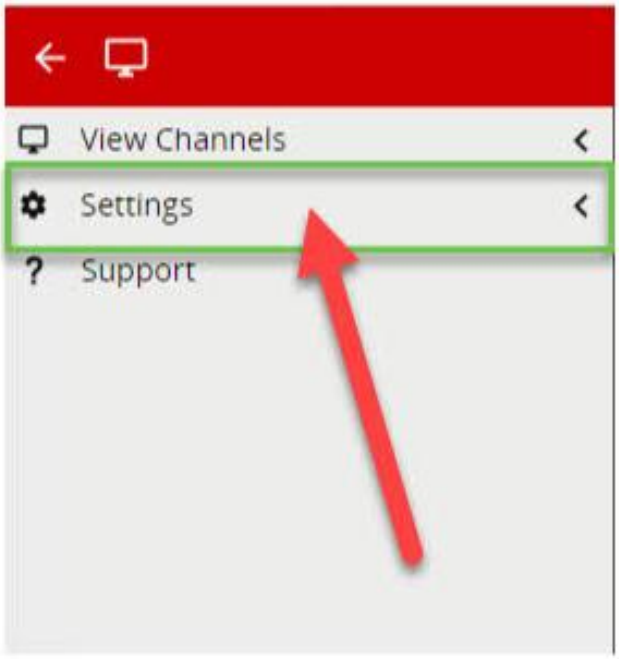
Um sich beim Mirasys VCA-Lizenzserver anzumelden, müssen Sie den Browser verwenden und die Website http://localhost:8080/ aufrufen.
Der Standard-Benutzername lautet **admin** und das Standard-Passwort ist **admin**.

8.7.2.1.1 Auf der Startseite gelangst du über das Hamburger-Menü zu den Einstellungen.

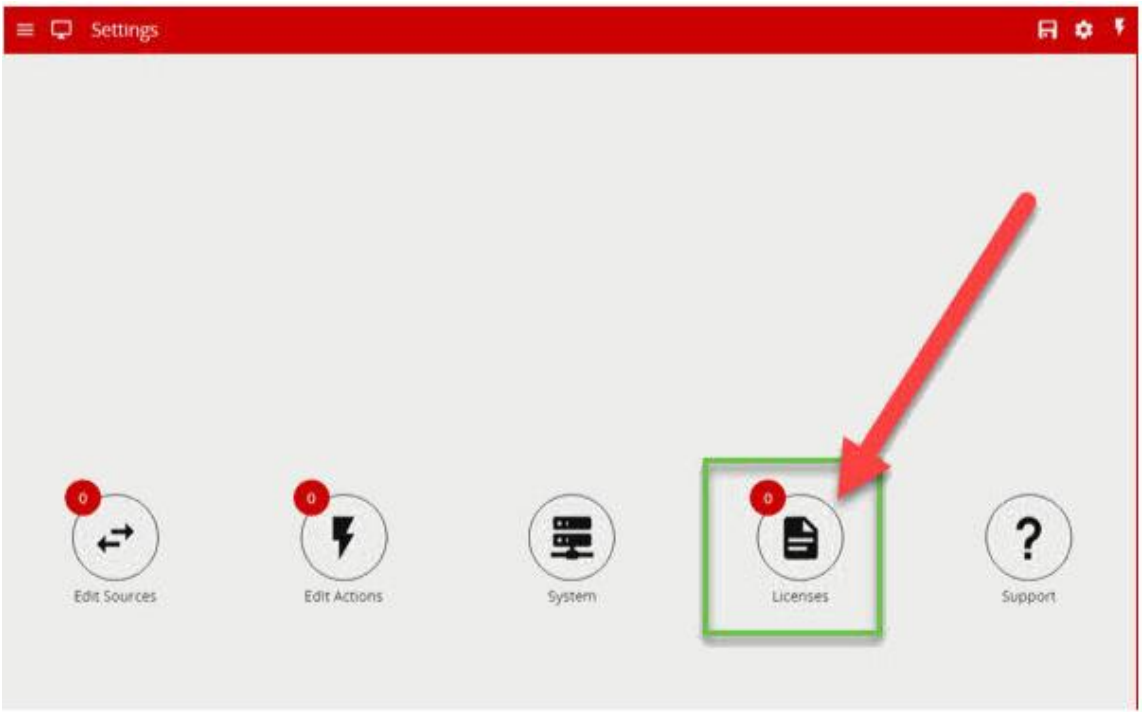


8.7.2.1.2 Hinzufügen der Lizenz

1. **Einstellungen** öffnen



1. **Lizenzen** öffnen

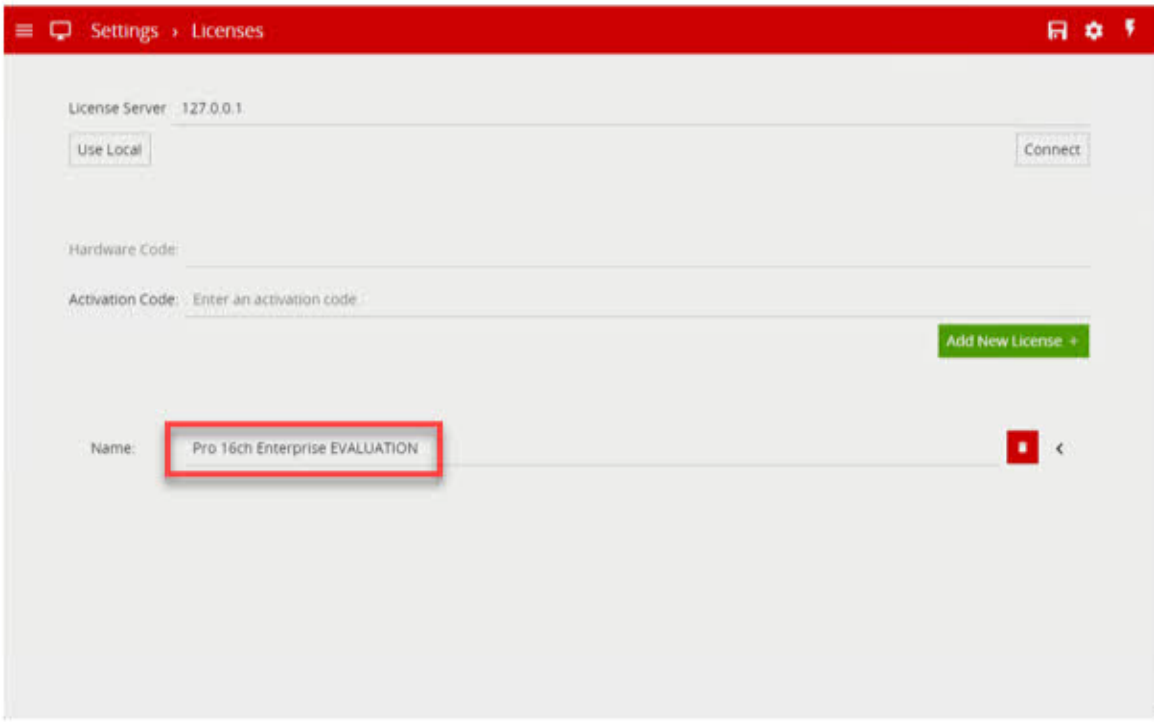


1. Kopieren Sie den Hardware-Code und senden Sie ihn an Mirasys, um die Lizenzdaten zu erhalten.

2. Wenn Sie den Aktivierungscode von Mirasys erhalten haben, fügen Sie den Code in das Feld **Activation Code** ein und klicken Sie auf **Add New License**

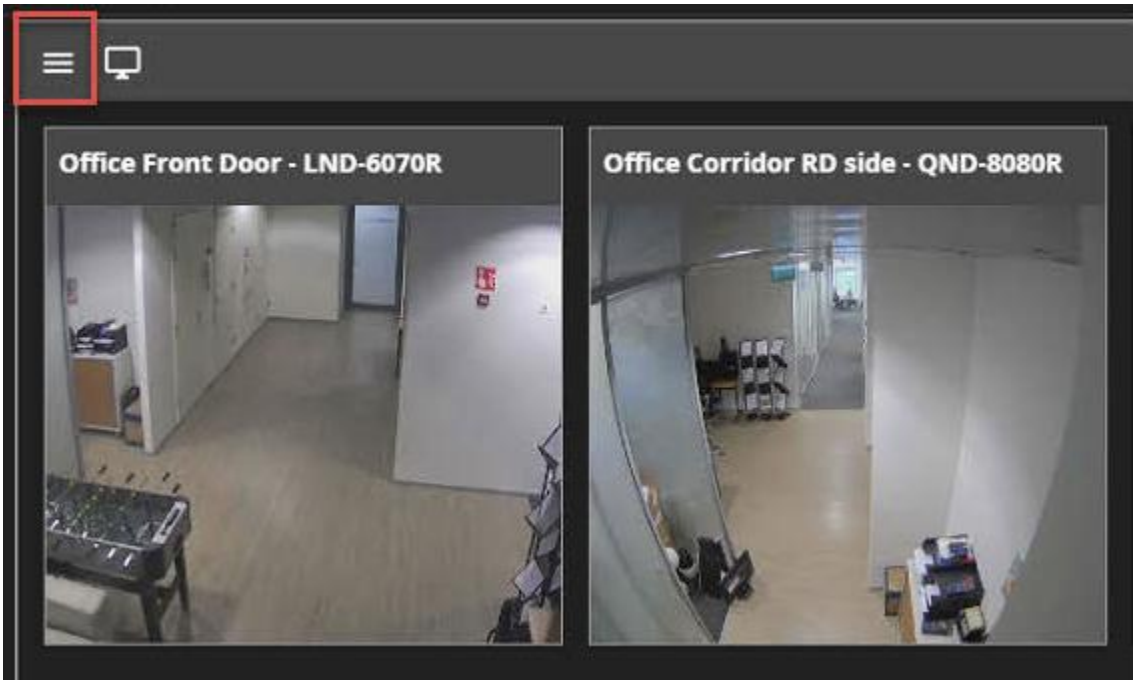


1. Sobald Sie die gewünschten Lizenzen zum System hinzugefügt haben, können Sie auf der Mirasys-VMS-Seite fortfahren.

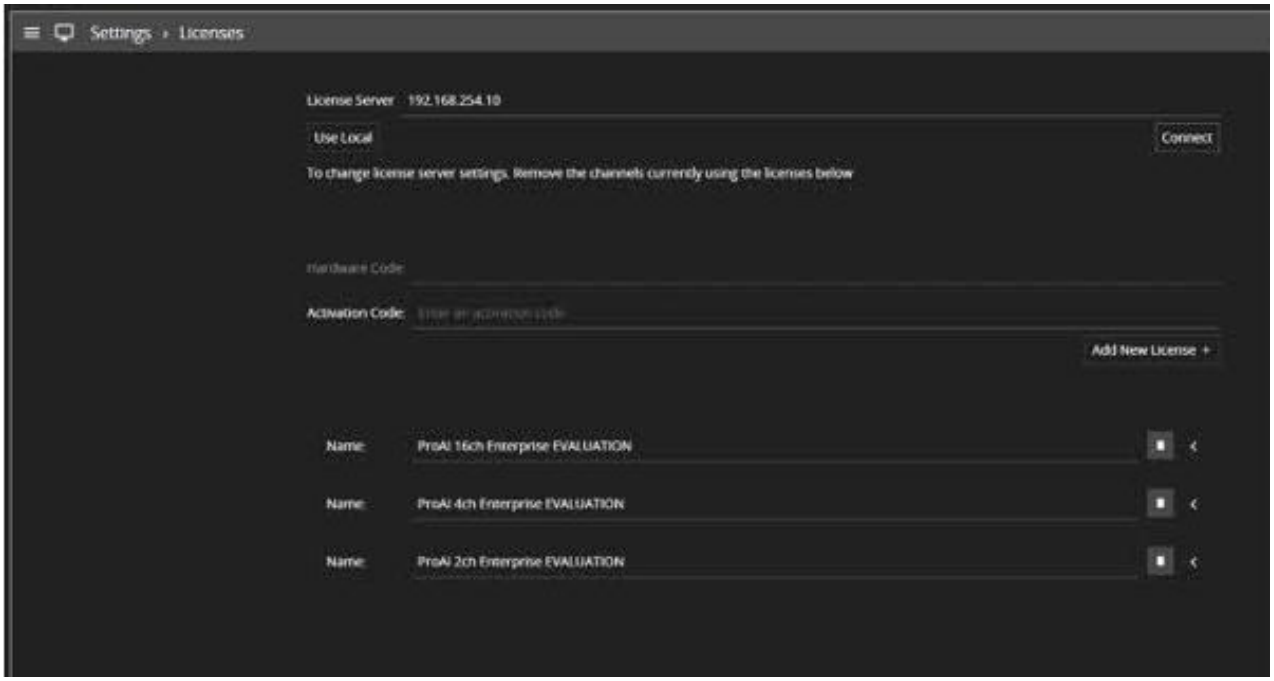


8.7.2.2 Konfiguration des Mirasys VMS

1. Öffnen Sie den System Manager, wechseln Sie zum Server-Bereich und wählen Sie **VCA-Einstellungen**
2. Daraufhin öffnet sich ein neues Fenster, in dem Sie ein ähnliches Burger-Menü wie zuvor finden



1. In diesem Menü finden Sie die Einstellungen, über die Sie die DNS- oder IP-Adresse des Lizenzservers festlegen können

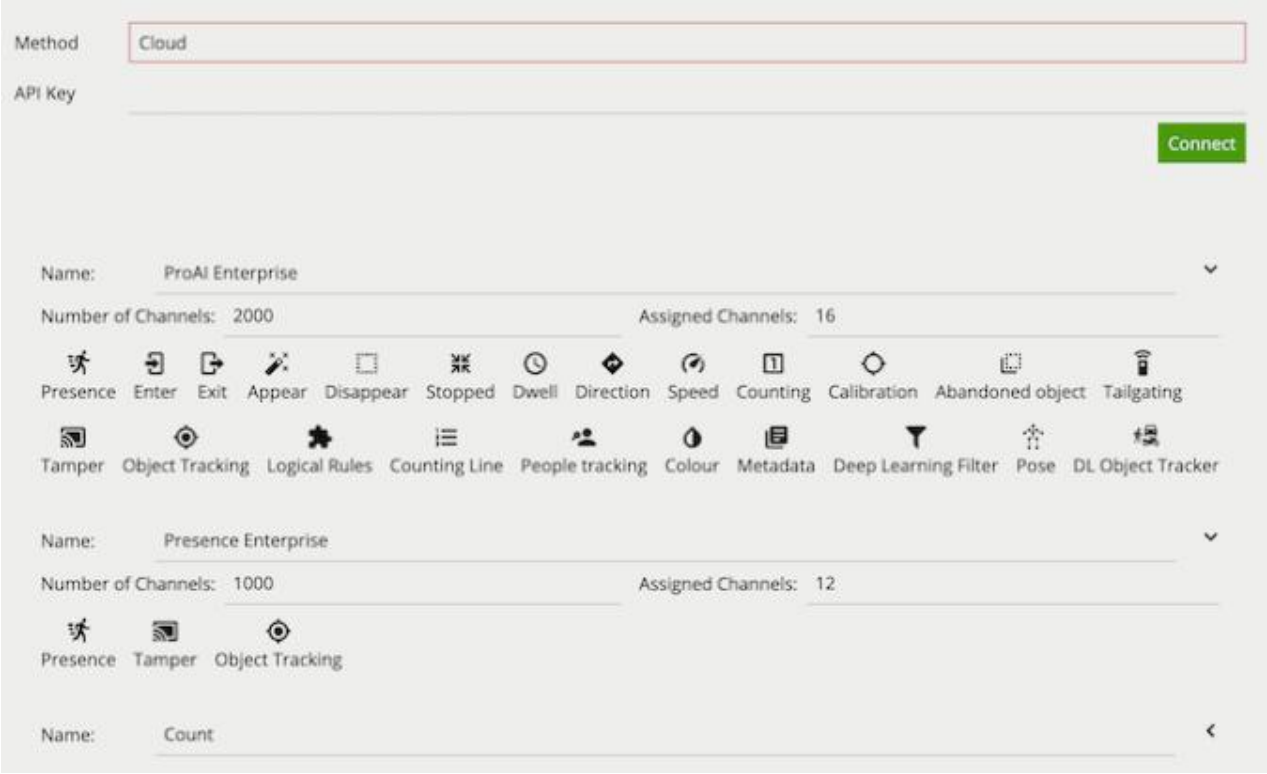


1. Wenn Sie die Adresse des Lizenzservers eingeben müssen, können Sie hier auf **Connect** klicken

Wenn die Verbindung erfolgreich hergestellt wurde, werden hier die Lizenzen des Mirasys VCA-Lizenzservers angezeigt.

Anschließend können Sie zu den VCA-Einstellungen und -Quellen wechseln, um dem gewünschten Kamerakanal die gewünschte Lizenz zuzuweisen.

8.8 CLOUD-LIZENZIERUNG



Sobald ein gültiger API-Schlüssel angegeben und die Verbindung zum Cloud-Lizenzierungsserver hergestellt wurde, wird der diesem API-Schlüssel zugeordnete Lizenzpool angezeigt.

Bei Verwendung der Cloud-Lizenzierung wird der für VCAserver verfügbare Lizenzpool über ein Cloud-Portal verwaltet.

- **Methode**: Wechselt zwischen Cloud-Lizenzierung und einem Lizenzserver.
- **API-Schlüssel**: Ein Autorisierungstoken, das mit einem Cloud-Lizenzierungskonto verknüpft ist.
- **Verbinden**: Verbindet diese Instanz von VCAserver mit den Cloud-Lizenzierungsservern.
- Die Liste der installierten Lizenzen und deren Funktionen wird darunter angezeigt.

Bei Neuinstallationen muss dem Cloud-Lizenzierungskonto eine Lizenz zum Lizenzpool hinzugefügt werden, bevor ein Benutzer Quellen hinzufügen kann.

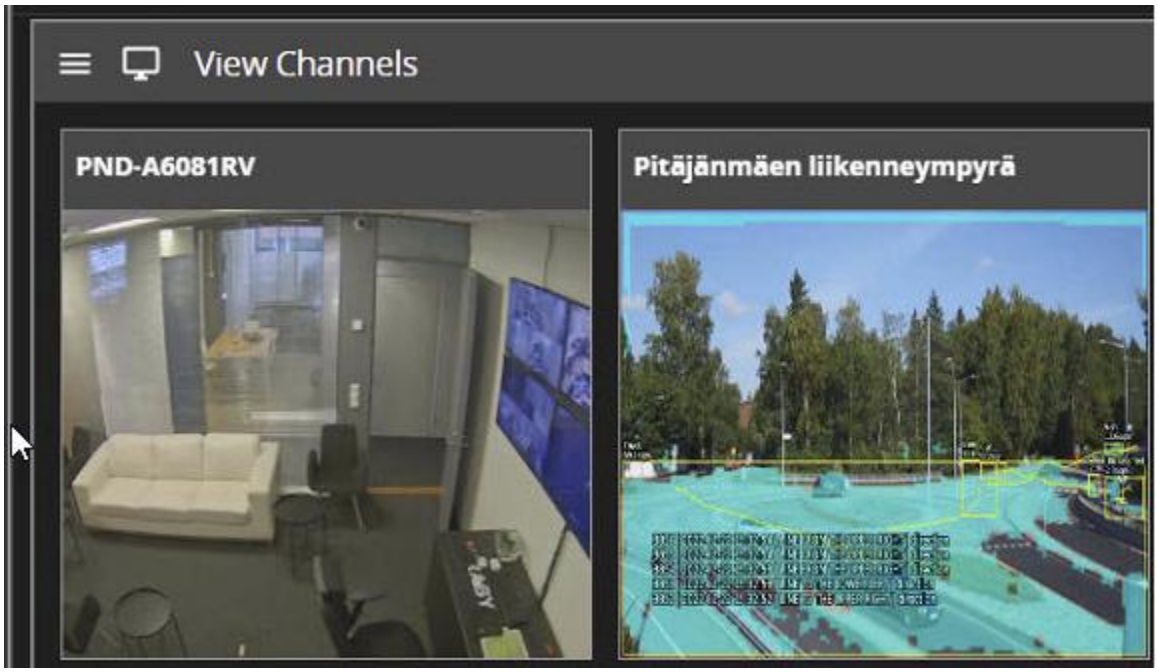
8.9 VCA-KANALEINSTELLUNGEN

Die VCA-Kanaleinstellungen enthalten alle Konfigurationen für Videokanäle, auf denen VCACore aktiviert ist.

- Verfolgung

- Zonen
- Kalibrierung
- Klassifizierung
- Eingebrannte Anmerkungen
- Regeln
- Videovorschau
- Deep Learning

Sie können die gewünschte Kamera unter **VCA-Einstellungen** öffnen, indem Sie darauf klicken.



8.9.1 Initialisierung

Wenn der Benutzer einen Tracker auswählt, ist eine Initialisierungsphase erforderlich. Diese hängt vom ausgewählten Tracker ab.

Objekt-Tracker: Nach der Auswahl muss der Tracker die Szene „erlernen“, um den Hintergrund von sich bewegenden Objekten im Vordergrund zu unterscheiden.

Während des Erlernens der Szene wird in der Live-Ansicht die folgende Meldung angezeigt, und es werden in dieser Zeit keine Objekte verfolgt.

DL People Tracker & DL Object Tracker: Bei der ersten Auswahl führt die DL-Engine einen Modellgenerierungsprozess durch. Dadurch werden die DL-Modelle für die Ausführung auf der verfügbaren GPU-Hardware optimiert.

Unabhängig davon, welcher Tracker ausgewählt wird, werden das DL People Tracker-Modell, das DL Object Tracker-Modell und das DL Filter-Modell in einem Durchgang optimiert.

Dieser Vorgang kann bis zu 10 Minuten pro Modell dauern und sich je nach GPU-Konfiguration verlängern. Nach Abschluss des Vorgangs werden die optimierten Modelle im Konfigurationsordner gespeichert.

Der Vorgang muss nicht erneut ausgeführt werden, es sei denn, die GPU-Hardware wird gewechselt. Während der Optimierung wird in der Live-Ansicht eine Meldung angezeigt, und während dieser Zeit werden keine Objekte verfolgt.

Bitte beachten Sie: Der DL-Filter erfordert denselben Initialisierungsvorgang, zeigt jedoch keine Meldung an.

Nach der Initialisierung beginnt VCAserver mit der Analyse des Videostreams mit dem ausgewählten Tracker. Die für diesen Tracker spezifischen Einstellungen werden ebenfalls unterhalb der Auswahloption für die Tracker-Engine angezeigt.

Unabhängig vom ausgewählten Tracker kann jedes verfolgte Objekt durch die verfügbaren Regeln geleitet werden. In einigen Fällen sind bestimmte Regeln oder Algorithmen jedoch nur mit einem bestimmten Tracker verfügbar. Beispielsweise sind der Deep-Learning-Filter sowie die Regeln für verlassene und entfernte Objekte nur mit dem Object Tracker verfügbar.

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

Der Objekt-Tracker ist eine bewegungsbasierte Erkennungs-Engine. Anhand der im Bild erkannten Veränderungen unterteilt der Algorithmus das Bild in Vordergrund und Hintergrund und verfolgt dabei jedes Objekt im Vordergrund, dessen Bewegung einen festgelegten Schwellenwert überschreitet. Der Objekt-Tracker verfügt über folgende Einstellungen:

8.9.2.1.1 Verweildauer für stationäre Objekte

Die Verweildauer für stationäre Objekte legt fest, wie lange ein Objekt von der Engine verfolgt wird, sobald es zum Stillstand gekommen ist.
Da Objekte, die zum Stillstand kommen, nach einer bestimmten Zeit in die Szene „eingebunden“ werden müssen,

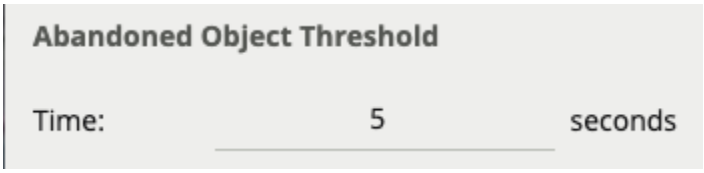
vergisst die Tracking-Engine Objekte, die nach Ablauf der Verweildauer für stationäre Objekte zum Stillstand gekommen sind.



Die Standardeinstellung beträgt 60 Sekunden.

8.9.2.1.2 Schwellenwert für zurückgelassene/entfernte Objekte

This threshold amount of time an object must be classed as abandoned or removed before an Abandoned / Removed rule will trigger.

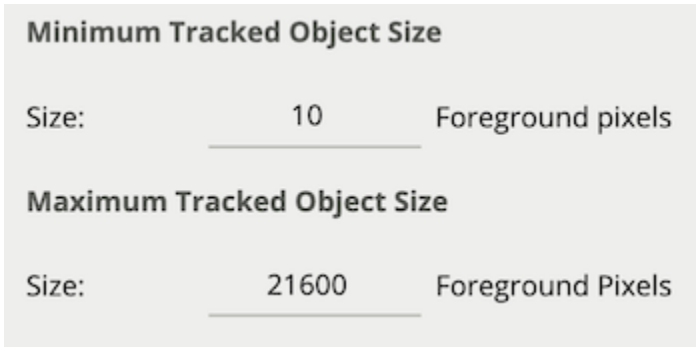


Die Standardeinstellung beträgt 5 Sekunden.

8.9.2.1.3 Mindestgröße des zu verfolgenden Objekts

Die **Minimale Größe des zu verfolgenden Objekts** legt fest, wie groß das kleinste Objekt sein muss, das für die Verfolgung in Betracht gezogen wird.

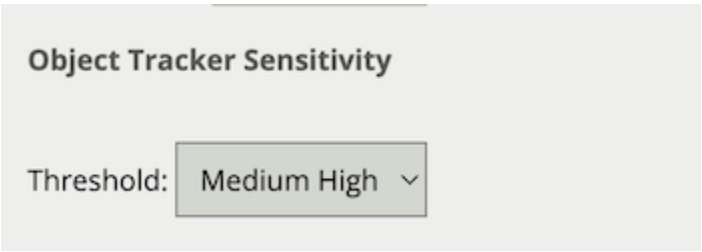
Für die meisten Anwendungen wird die Standardeinstellung von 10 empfohlen. In bestimmten Situationen, in denen eine höhere Empfindlichkeit erforderlich ist, kann der Wert manuell festgelegt werden.
Niedrigere Werte ermöglichen es der Engine zwar, kleinere Objekte zu verfolgen, können jedoch die Anfälligkeit für Fehlalarme erhöhen.



8.9.2.1.4 Empfindlichkeit des Objekt-Trackers

Mit dem Wert für die Empfindlichkeit des Objekt-Trackers lässt sich der Objekt-Tracker so einstellen, dass Bewegungen unterhalb eines bestimmten Schwellenwerts ignoriert werden.
In Kombination mit der eingeblendeten Blob-Map-Annotation, die den Bereich der Szene visualisiert, in dem der

Objekt-Tracker Bewegungen erkennt, kann dieser Wert angepasst werden, um Umgebungsrauschen herauszufiltern.



Die Standardeinstellung ist 4.

8.9.2.1.5 Erkennung von Szenenwechseln (Objekt-Tracker)

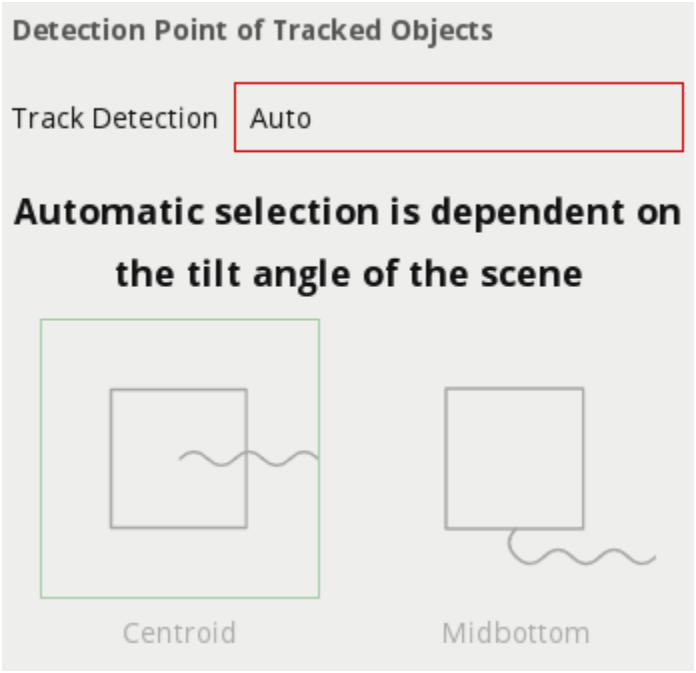
Erfahren Sie mehr über die Erkennung von Szenenwechseln.

8.9.2.1.6 Erkennungspunkt von verfolgten Objekten

Für jedes verfolgte Objekt wird ein Punkt verwendet, um die Position des Objekts zu bestimmen und zu prüfen, ob es eine Zone schneidet und eine Regel auslöst. Dieser Punkt wird als Erkennungspunkt bezeichnet.
Es gibt 3 Modi, die den Erkennungspunkt relativ zum Objekt definieren:

Automatisch

Im automatischen Modus wird der Erkennungspunkt automatisch basierend auf der Konfiguration des Kanals festgelegt.
Er wählt „Centroid“ (Mittelpunkt), wenn die Kamera von oben kalibriert ist, oder „Mid-bottom“ (Mitte unten), wenn die Kamera seitlich kalibriert oder nicht kalibriert ist.



Schwerpunkt

In diesem Modus wird der Erkennungspunkt zwangsläufig auf den Schwerpunkt des Objekts festgelegt.



Mitte unten

In diesem Modus wird der Erkennungspunkt zwangsläufig auf die Mitte der Unterkante des verfolgten Objekts festgelegt.
Normalerweise ist dies der Bodenkontaktpunkt des Objekts (der Schnittpunkt des Objekts mit der Bodenebene).



8.9.2.1.7 Manipulationserkennung (Objekt-Tracker)
Erfahren Sie mehr über die Manipulationserkennung.

8.9.2.1.8 Intervall für die Signalsignalisierung bei Signalverlust
Siehe Intervall für die Signalsignalisierung bei Signalverlust

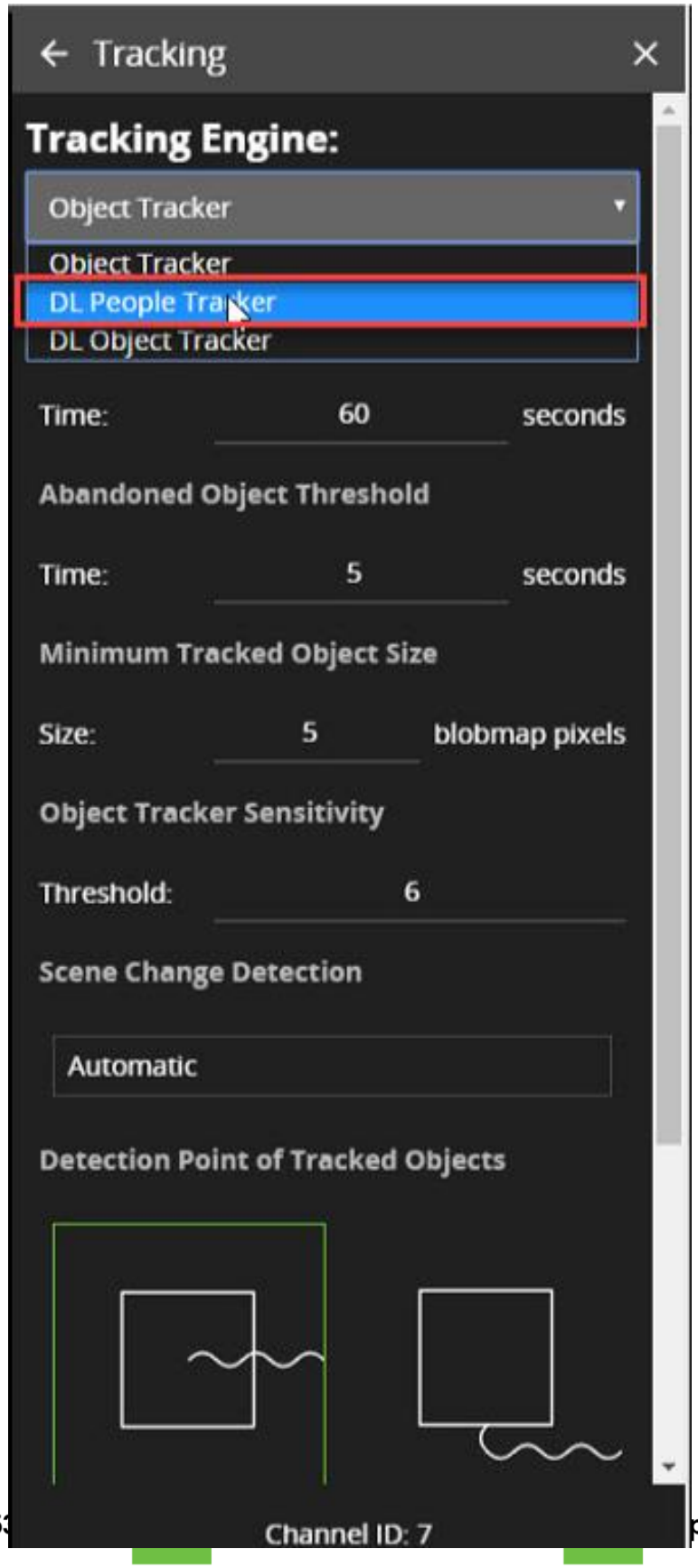
8.9.2.2 VCA Deep Learning People Tracker
Die Deep-Learning-Personenerkennung wurde entwickelt, um Personen in Situationen zu verfolgen, in denen sich das Kamerasichtfeld relativ nah befindet.
Der Deep Learning People Tracker basiert auf der Pose-Estimation-Technologie und liefert die Position einer Person im Sichtfeld sowie zusätzliche Metadaten zu Schlüsselpunkten an den Körperteilen.
Die Hardwareanforderungen für diesen Algorithmus finden Sie unter Deep Learning-Anforderungen.

Der Deep Learning People Tracker verfügt über die folgenden Einstellungen:

8.9.2.2.1 Manipulationserkennung (DLPT)
Erfahren Sie mehr über die Manipulationserkennung.

8.9.2.2.2 Intervall für Signalverlustmeldung
Siehe „Intervall für Signalverlustmeldung“

8.9.2.2.3 DL People Tracker aktivieren
1. **View Channels** öffnen
2. Kamera auswählen
3. **Tracking** öffnen
4. Öffnen Sie die **Tracking-Engine** über das Dropdown-Menü und wählen Sie **DL People Tracker** aus


Tracking
Tracking Engine:
Object Tracker
Object Tracker
DL People Tracker
DL Object Tracker
Time: 60 seconds
Abandoned Object Threshold
Time: 5 seconds
Minimum Tracked Object Size
Size: 5 blobmap pixels
Object Tracker Sensitivity
Threshold: 6
Scene Change Detection
Automatic
Detection Point of Tracked Objects
Channel ID: 7

8.9.2.3 VCA Deep Learning Object Tracker

Der Deep-Learning-Objekt-Tracker wurde für die präzise Erkennung und Verfolgung von Personen, Fahrzeugen und wichtigen Objekten in schwierigen Umgebungen entwickelt, in denen bewegungsbasierte Verfolgungsmethoden an ihre Grenzen stoßen würden.
Nachfolgend finden Sie eine Liste der Objekte, die vom Deep-Learning-Objekt-Tracker erkannt werden:

Klassenname	Beschreibung
`person`	Eine Person oder ein Objekt, das von einer Person bewegt wird (z. B. ein Fahrrad)
`motorcycle`	Ein Motorrad
`bicycle`	Ein Fahrrad
`cyclist`	Eine Person auf einem Fahrrad kann als zwei separate Objekte erfasst werden
`bus`	Ein Bus
`car`	Ein Auto
`van`	Ein Kleinbus, einschließlich Minivans und Minibusse
`truck`	Ein Lkw, einschließlich Lastkraftwagen und Nutzfahrzeuge,
`forklift`	Ein Gabelstapler
`bag`	Ein Rucksack oder eine Reisetasche (Sporttasche)

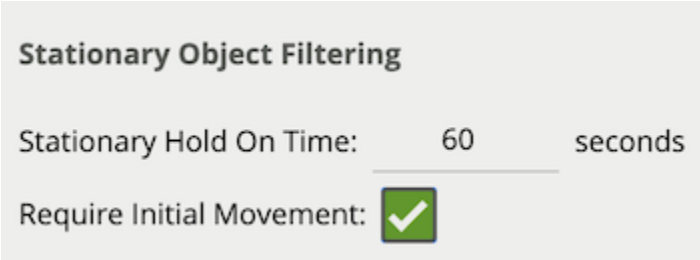
Der Deep-Learning-Objekt-Tracker basiert auf einem Klassifizierungs- und Erkennungsmodell und ermittelt die Position eines Objekts im Sichtfeld. Die Hardwareanforderungen für diesen Algorithmus finden Sie unter Deep-Learning-Anforderungen.

Der Deep-Learning-Objekt-Tracker verfügt über folgende Einstellungen:

8.9.2.3.1 Filterung stationärer Objekte

Siehe Haltezeit für stationäre Objekte.

Zusätzlich zur „Haltezeit für stationäre Objekte“ steht die Einstellung „Anfängliche Bewegung erforderlich“ zur Verfügung, die verhindert, dass Objekte verfolgt werden, die sich nicht bewegt haben.



8.9.2.3.2 Erkennungspunkt der verfolgten Objekte

Siehe Erkennungspunkt der verfolgten Objekten.

8.9.2.3.3 Manipulationserkennung (DLOT)

Erfahren Sie mehr über die Manipulationserkennung.

8.9.2.3.4 Intervall für die Signalsignalisierung

Siehe „Intervall für die Signalsignalisierung“

8.9.2.4 VCA Deep Learning Skeleton Tracker

Der Deep-Learning-Skeleton-Tracker verfolgt Personen in Situationen, in denen sich das Kamerasichtfeld relativ nah befindet.

Der Deep-Learning-Skeleton-Tracker basiert auf der Pose-Estimation-Technologie und liefert die Position einer Person im Sichtfeld sowie zusätzliche Metadaten zu Schlüsselpunkten an den Körperteilen. Die Hardwareanforderungen für diesen Algorithmus finden Sie unter Deep-Learning-Anforderungen.

Der Deep-Learning-Skeleton-Tracker verfügt über folgende Einstellungen:

- Manipulationserkennung (DLST)

8.9.2.5 VCA Hand Object Interaction Tracker

> **Die letzte Version, die den „Hand Object Interaction Tracker“ enthält, ist 9.6.2**. Diese Funktion wurde in späteren Versionen entfernt.

Der Hand-Objekt-Interaktions-Tracker (HOI-Tracker) dient zur Erkennung von Händen und den von ihnen gehaltenen Objekten. Für eine optimale Erkennung benötigt der HOI-Tracker ein Blickfeld von oben und aus relativer Nähe. Nachfolgend finden Sie eine Liste der Objekte, die vom Hand-Objekt-Interaktions-Tracker erkannt werden:

Klassenname	Beschreibung
hand	eine Hand
object	Ein Objekt, das von einem Handobjekt gehalten wird

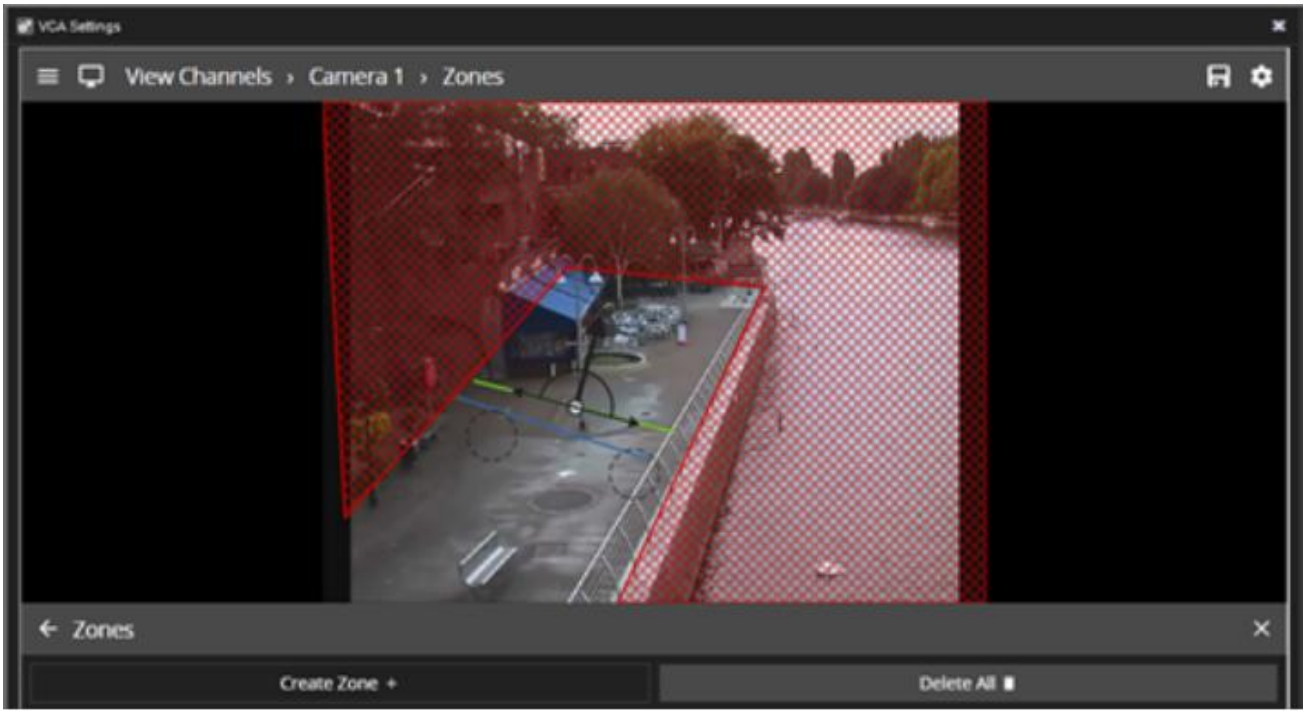
Der Hand-Objekt-Interaktions-Tracker basiert auf einem Klassifizierungs- und Erkennungsmodell, das die Position eines Objekts im Sichtfeld ermittelt. Die Hardwareanforderungen für diesen Algorithmus finden Sie unter Deep-Learning-Anforderungen

Der Hand-Objekt-Interaktions-Tracker verfügt über folgende Einstellungen:

- Erkennungspunkt der verfolgten Objekte (HOI)
- Manipulationserkennung (HOI)
- Intervall für die Signalsignalisierung bei Signalverlust (HOI)

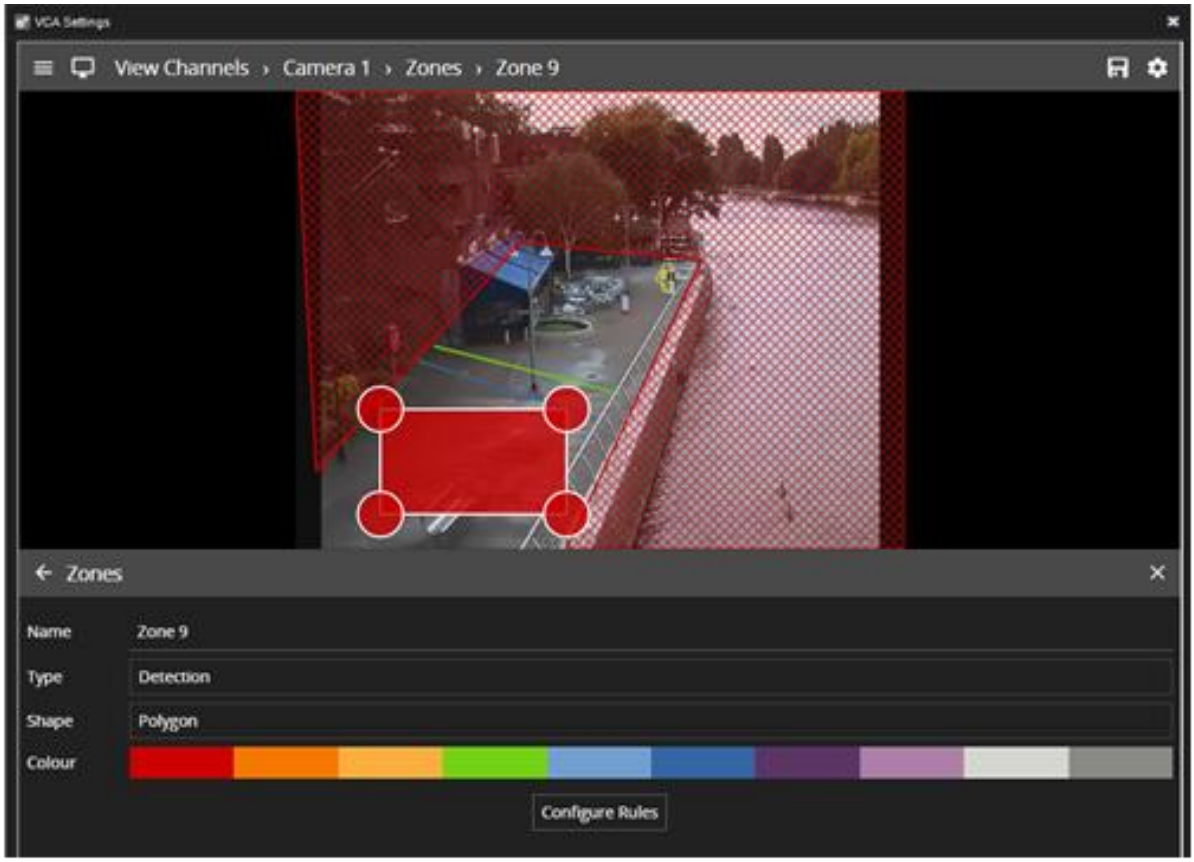
8.9.3 VCA-Zonen

Zonen sind die Erfassungsbereiche, in denen VCAcore arbeitet.
Um ein bestimmtes Verhalten zu erkennen, muss eine Zone konfiguriert werden, um den Bereich festzulegen, in dem eine Regel gilt.



8.9.3.1 Zonenspezifische Einstellungen

Das Menü zur Zonenkonfiguration enthält eine Reihe von zonenspezifischen Konfigurationsparametern:



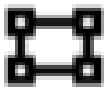
- **Name**: Der Name der Zone, der in Ereignisbenachrichtigungen angezeigt wird.
- **Type** (Typ): Der Typ der Zone. Mögliche Optionen:
- **Detection** (Erkennung): Eine Zone, die verfolgte Objekte erkennt und auf die Regeln angewendet werden können.
- **Non-detection** (Nicht-Erkennung): Eine Zone, die einen Bereich festlegt, der von der VCAcore-Analyse ausgeschlossen werden soll.
    - In Nicht-Erkennungszonen werden keine Objekte erkannt.
    - Nützlich, um Bereiche mit potenziellen Fehlalarmen aus einer Szene auszuschließen (z. B. sich bewegende Bäume, blinkende Lichter usw.).
- **Shape** (Form): Die Form der Zone. Kann eine der folgenden sein:
    - **Polygon**: Ein polygonaler Erkennungsbereich mit mindestens drei Knoten. Regeln gelten für den gesamten Bereich.
    - **Line** (Linie): Eine ein- oder mehrsegmentige Linie mit mindestens zwei Knoten. Die Regeln gelten für die Länge der Linie.

- **Colour** (Farbe): Die Farbe der Zone.
- **Configure Rules (**Regeln konfigurieren): Eine Schaltfläche, um direkt zur Seite für die Regelkonfiguration zu gelangen

8.9.3.2 Eine Zone hinzufügen

Zonen können auf verschiedene Arten hinzugefügt werden:

1. Doppelklicken Sie an einer beliebigen Stelle auf die Videoanzeige.
2. Klicken Sie im Menü „Zone settings“ auf die Schaltfläche „Create Zone“.
3. Klicken Sie mit der rechten Maustaste oder tippen Sie und halten Sie die Finger gedrückt, um das Kontextmenü anzuzeigen, und wählen Sie das Symbol zum Hinzufügen einer Zone aus.



8.9.3.2.1 Das Kontextmenü

Durch einen Rechtsklick oder durch langes Drücken (auf Mobilgeräten) wird ein Kontextmenü angezeigt, das auf den aktuellen Kontext zugeschnittene Befehle enthält.



Die folgenden Aktionen sind über das Kontextmenü verfügbar:

Fügt eine neue Zone hinzu

Löscht eine vorhandene Zone

Fügt einen Knoten zu einer Zone hinzu

Löscht einen vorhandenen Knoten aus einer Zone



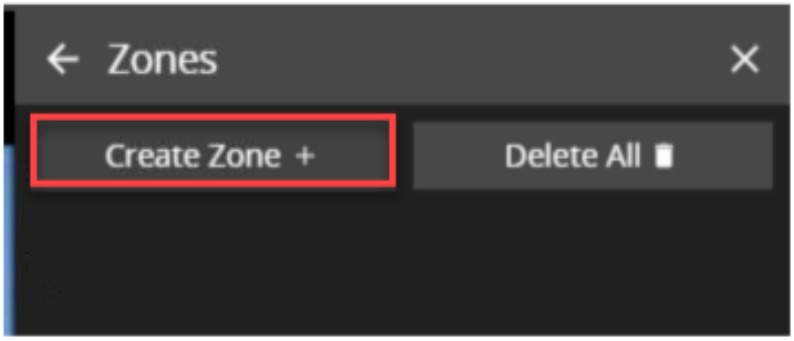




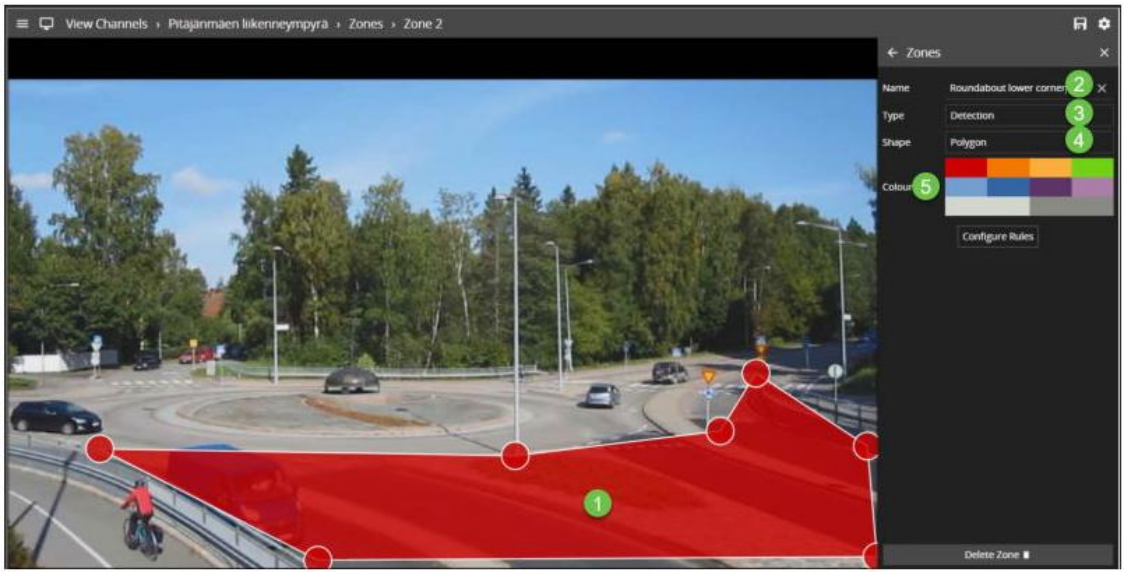


8.9.3.3 Eine Zone erstellen

Klicken Sie auf das Symbol **Create Zone**



1. Zeichne einen Bereich und lege die Position auf dem Bild fest
2. Lege den Namen des Bereichs fest
3. Lege den Erkennungsmodus fest
4. Lege die Form fest
5. Lege die Farbe fest



8.9.3.4 Positionierung von Zonen

Um die Position einer Zone zu ändern, klicken Sie auf die Zone und ziehen Sie sie an die gewünschte Stelle. Um die Form einer Zone zu ändern, ziehen Sie die Knoten, um die gewünschte Form zu erstellen. Neue Knoten können durch Doppelklicken auf den Rand der Zone oder durch Klicken auf das Symbol „Knoten hinzufügen“ im Kontextmenü hinzugefügt werden.

8.9.3.5 Zone löschen

Zonen können auf folgende Weise gelöscht werden:

- Wählen Sie die Zone aus und klicken Sie im Menü der Zoneneinstellungen auf die Schaltfläche **Delete Zone**.
- Wählen Sie die Zone aus, rufen Sie das Kontextmenü auf und wählen Sie das Symbol zum Löschen der Zone

8.9.4 VCA-Kalibrierung

Eine Kamerakalibrierung ist erforderlich, damit VCAcore Objekte in verschiedene Objektklassen einordnen kann. Sobald ein Kanal kalibriert wurde, kann VCAcore reale Objekteigenschaften wie Geschwindigkeit, Höhe und Fläche ermitteln und Objekte entsprechend klassifizieren.

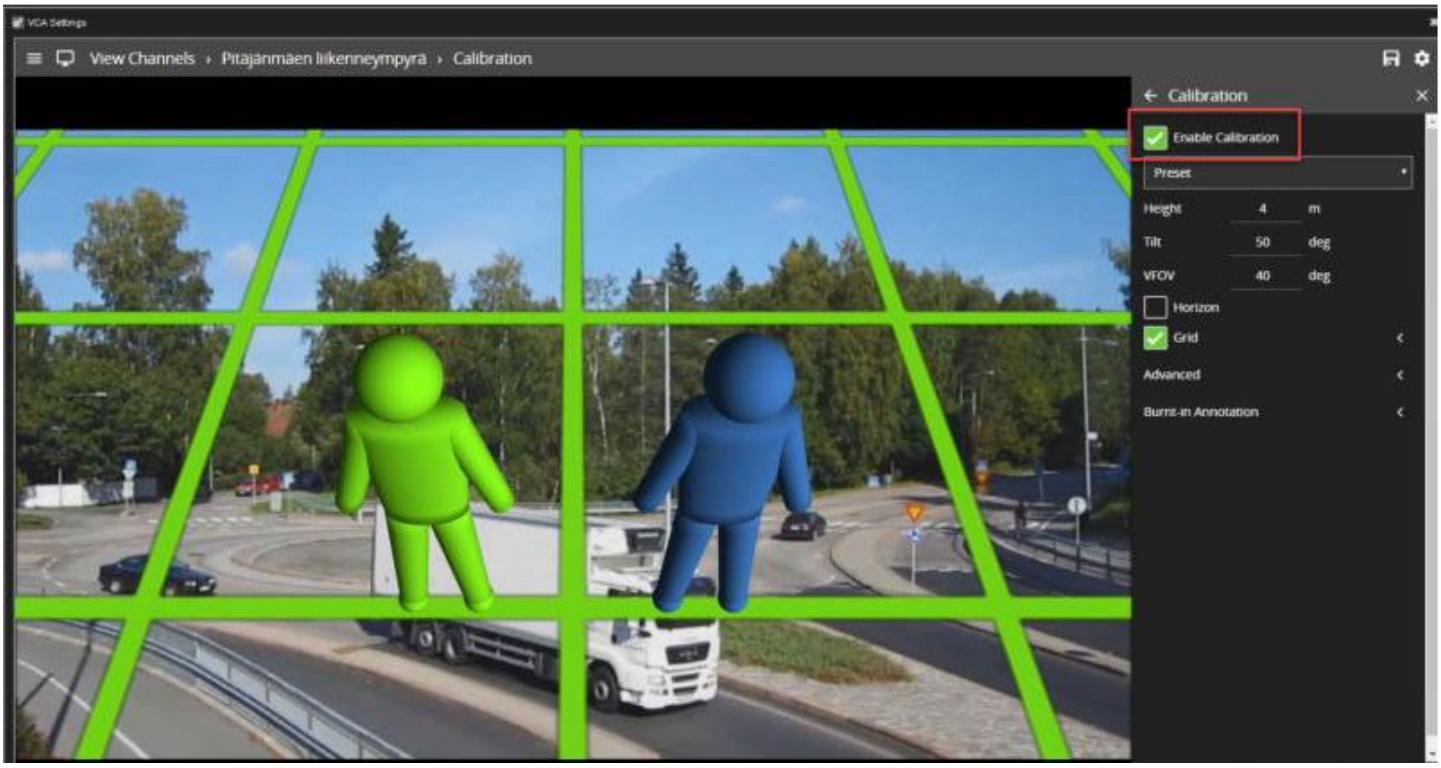
Bei Verwendung der Deep-Learning-Verfolgung ist keine Kalibrierung erforderlich, wohl aber bei Verwendung von normalem VCA oder Deep-Learning-Filtern.

8.9.4.1 Die Kamerakalibrierung gliedert sich in folgende Unterthemen:

1. Kalibrierung aktivieren
2. Kalibrierungssteuerung
3. Kalibrierung eines Kanals
4. Erweiterte Kalibrierungsparameter

8.9.4.2 Kalibrierung aktivieren

Standardmäßig ist die Kalibrierung deaktiviert.
Um die Kalibrierung für einen Kanal zu aktivieren, aktivieren Sie das Kontrollkästchen **Enable Calibration**.



8.9.4.3 Kalibrierungssteuerung

8.9.4.3.1 3D-Grafiküberlagerung

Während des Kalibrierungsvorgangs müssen die Merkmale im Videobild mit einer 3D-Grafiküberlagerung abgeglichen werden.
Die 3D-Grafiküberlagerung besteht aus einem grünen Raster, das die Grundebene darstellt.
Auf der Grundebene befinden sich mehrere 3D-Mimics (menschenähnliche Figuren), die die Abmessungen einer Person mit den aktuellen Kalibrierungsparametern darstellen.
Die Kalibrierungs-Mimics dienen zur Überprüfung der Größe einer Person in der Szene und sind 1,8 Meter groß.
Die Mimics können in der Szene verschoben werden, um sie an Personen (oder Objekte mit bekannter, vergleichbarer Höhe) anzupassen.

8.9.4.3.2 Maussteuerung

Die Kalibrierungsparameter lassen sich wie folgt mit der Maus einstellen:

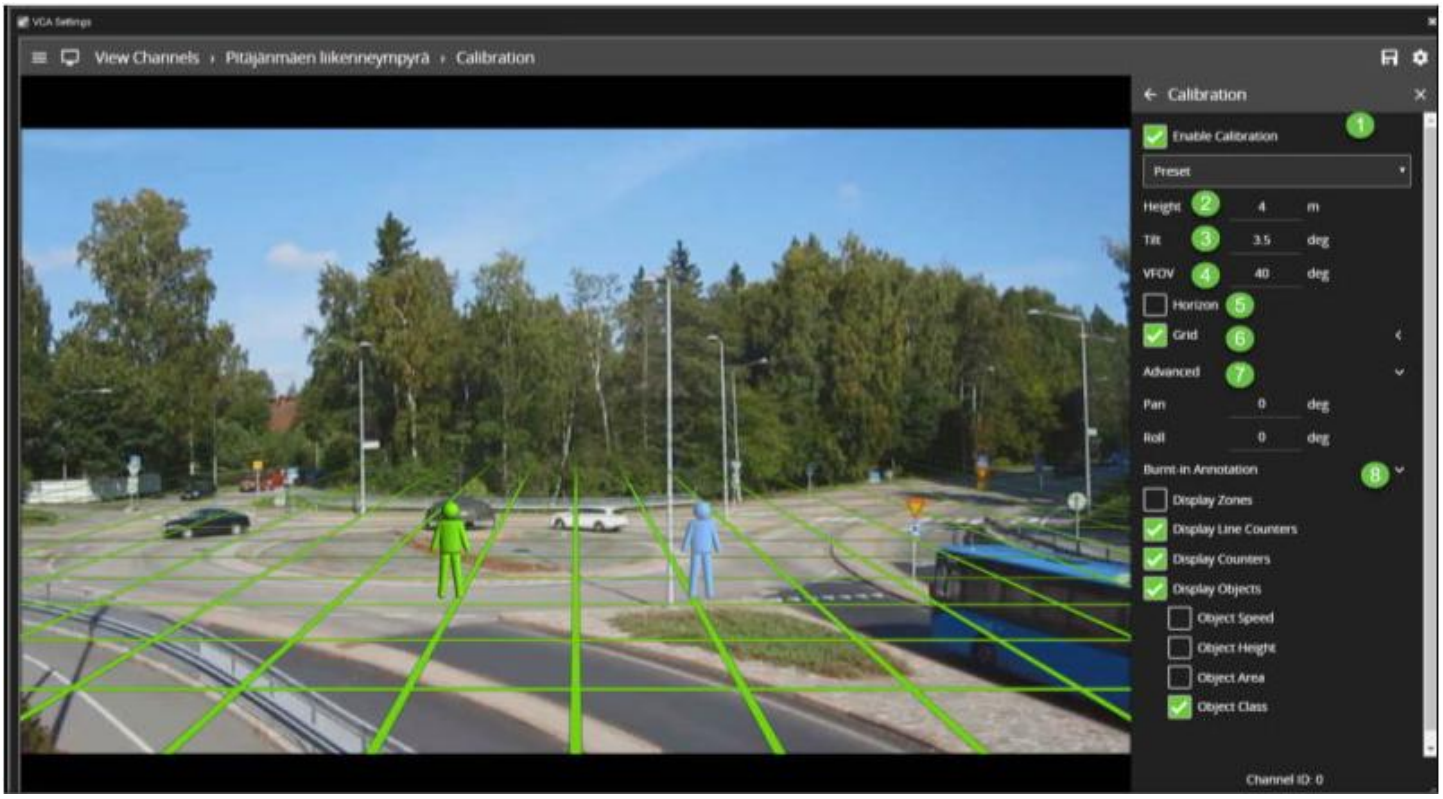
- Klicken Sie auf die Grundebene und ziehen Sie sie, um den Neigungswinkel der Kamera zu ändern.
- Verwenden Sie das Mausrad, um die Kamerahöhe einzustellen. – Ziehen Sie den Schieberegler, um das vertikale Sichtfeld zu ändern.

Hinweis: Die Schieberegler im Bedienfeld können ebenfalls zur Einstellung des Neigungswinkels und der Höhe der Kamera verwendet werden.

8.9.4.3.3 Elemente des Bedienfelds

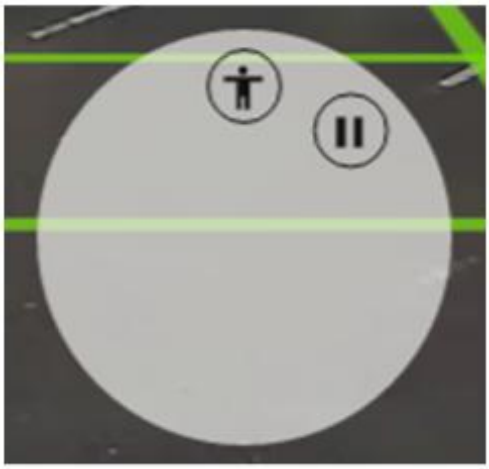
Das Bedienfeld (im obigen Bild auf der rechten Seite zu sehen) enthält die folgenden Steuerelemente:

1. **Height** (Höhe): Passt die Höhe der Kamera an
2. **Tilt** (Neigung): Passt den Neigungswinkel der Kamera an
3. **VFOV**: Passt das vertikale Sichtfeld der Kamera an. Hinweis: Ein korrekter Wert für das vertikale Sichtfeld der Kamera ist für eine genaue Kalibrierung und Klassifizierung unerlässlich.
4. **Horizon** (Horizont): Aktiviert/deaktiviert die Horizontanzeige. Nützlich, um die Kamera in einer tiefen Szene am Horizont auszurichten.
5. **Grid** (Raster): Aktiviert/deaktiviert die Anzeige des Bodenraster. Über die Schaltfläche zum Ein- und Ausblenden (<) werden zusätzliche Einstellungen angezeigt, mit denen Farbe, Deckkraft und Größe des Bodenraster angepasst werden können.
6. **Advanced** (Erweitert): Zeigt erweiterte Einstellungen zur Steuerung der Schwenk- und Neigebewegung der Kamera an.
7. **Burnt-in Annotation** (Eingebrannte Anmerkung): Zeigt die Steuerelemente für die eingebrannte Anmerkung zur Vereinfachung an.

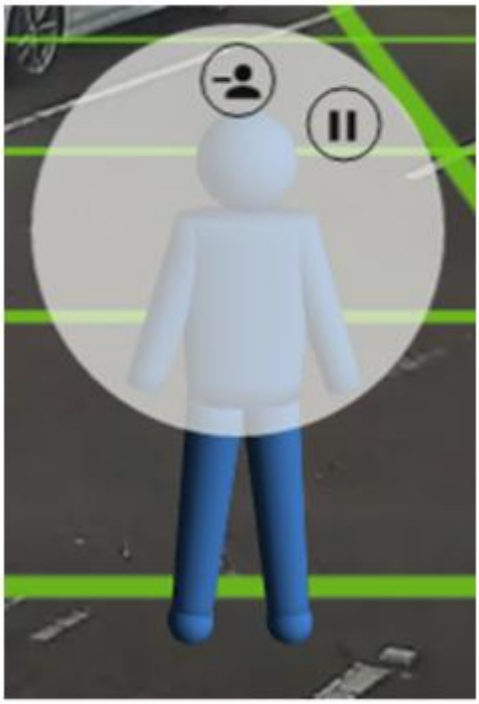


8.9.4.3.4 Kontextmenü-Einträge

Durch einen Rechtsklick mit der Maus (oder durch Tippen und Halten auf einem Tablet) auf das Raster wird das Kontextmenü angezeigt:



Wenn Sie dieselbe Aktion auf einem Mimic-Display ausführen, wird das Mimic-Kontextmenü angezeigt:



Die folgenden Aktionen sind über das Kontextmenü verfügbar:

1. 
2. 
3. 
4. 

1. Halten Sie das Video an. Durch das Anhalten des Videos lassen sich die Mimikbewegungen leichter an Objekten in der Szene ausrichten.
2. Das Video wird fortgesetzt, nachdem es zuvor angehalten wurde.
3. Fügt der Grundebene einen zusätzlichen Mimic hinzu.
4. Entfernt das aktuell ausgewählte Mimic von der Grundebene.

8.9.4.4 Kalibrierung eines Kanals

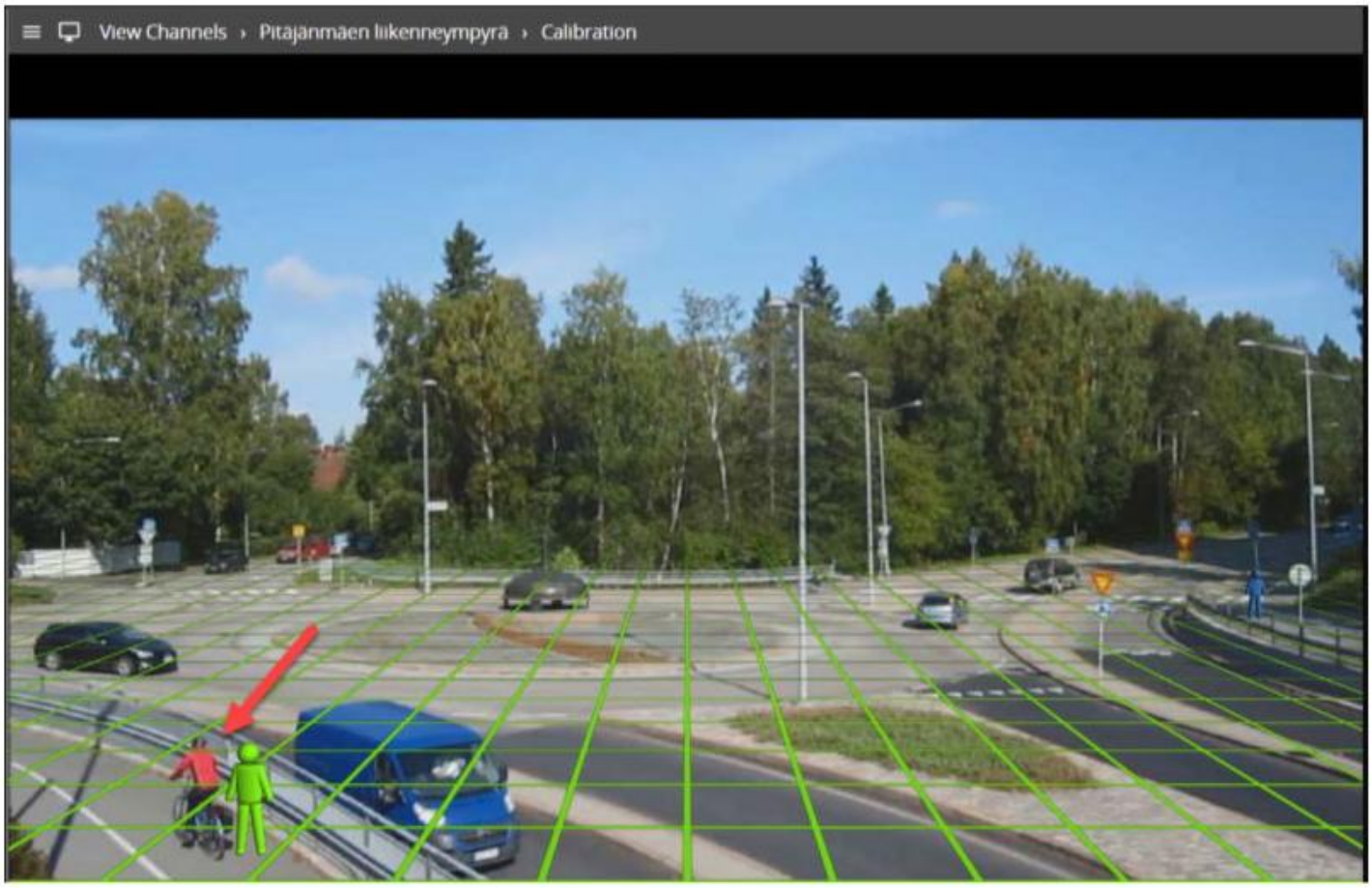
Die Kalibrierung eines Kanals ist erforderlich, um Objektparameter wie Höhe, Fläche, Geschwindigkeit und Klassifizierung zu schätzen.

Sind die Höhe, der Neigungswinkel und das vertikale Sichtfeld entsprechend der Installation bekannt, können diese einfach als Parameter in die entsprechenden Felder im Bedienfeld eingegeben werden.

Sind diese Parameter jedoch nicht eindeutig bekannt, bietet dieser Abschnitt eine Schritt-für-Schritt-Anleitung zur Kalibrierung eines Kanals.

8.9.4.4.1 Schritt 1: Personen in der Szene finden

Suche in der Szene nach Personen oder Objekten in Menschengröße.
Versuche, eine Person in der Nähe der Kamera und eine Person, die weiter von der Kamera entfernt ist, zu finden. Es ist hilfreich, das Video mithilfe der Wiedergabe-/Pause-Taste anzuhalten, damit die Mimik-Elemente präzise platziert werden können. Platziere die Mimik-Elemente auf oder in der Nähe der Personen:



8.9.4.4.2 Schritt 2: Geben Sie das vertikale Sichtfeld der Kamera ein

Die Ermittlung des korrekten vertikalen Sichtfelds ist für eine genaue Kalibrierung wichtig.
Die folgende Tabelle enthält vorberechnete Werte für das vertikale Sichtfeld bei verschiedenen Sensorgrößen.

	Brennweite(mm)	1	2	3	4	5	6	7	8	9	10	15	20	30	40	50
CCD-Größe (in)	CCD-Höhe(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

Falls die Tabelle die entsprechenden Parameter nicht enthält, lässt sich das vertikale Sichtfeld abschätzen, indem man die Bildränder oben und unten betrachtet.
Beachten Sie, dass es ohne das korrekte vertikale Sichtfeld unter Umständen nicht möglich ist, die Mimik der Personen an verschiedenen Positionen in der Szene aufeinander abzustimmen.

8.9.4.4.3 Schritt 3: Geben Sie die Kamerahöhe ein

Wenn die Kamerahöhe bekannt ist, geben Sie sie direkt ein. Wenn die Höhe nicht bekannt ist, schätzen Sie sie so gut wie möglich und geben Sie sie direkt ein.

8.9.4.4.4 Schritt 4: Passen Sie den Neigungswinkel und die Kamerahöhe an

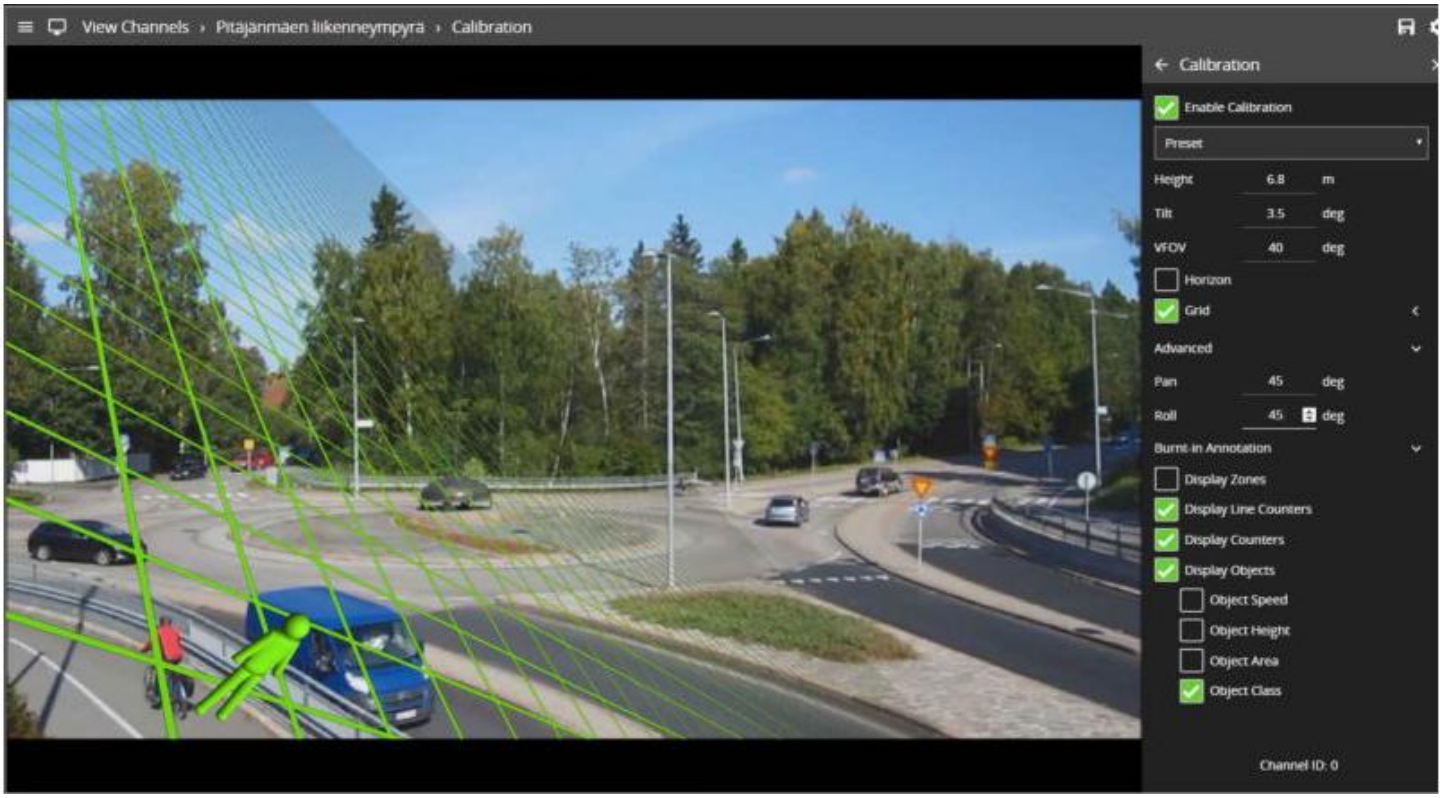
Passen Sie den Neigungswinkel der Kamera (und gegebenenfalls die Höhe) so lange an, bis beide Mimics ungefähr die gleiche Größe haben wie eine reale Person an dieser Position in der Szene.
Klicken und ziehen Sie die Grundebene, um den Neigungswinkel zu ändern, und verwenden Sie das Mausrad oder das Bedienfeld, um die Kamerahöhe anzupassen.
Das Ziel ist es, sicherzustellen, dass die an verschiedenen Stellen auf dem Raster platzierten Mimics mit Personen oder Objekten in Menschengröße in der Szene übereinstimmen.
Sobald die Parameter angepasst wurden, spiegelt die Objektbeschriftung die Änderungen wider und klassifiziert die Objekte entsprechend.

8.9.4.4.5 Schritt 5: Überprüfung der Einrichtung

- Sobald die Szene kalibriert ist, ziehen Sie Mimics an verschiedene Stellen in der Szene oder fügen Sie sie dort hinzu und überprüfen Sie, ob sie in derselben Größe/Höhe erscheinen wie eine reale Person.
- Vergewissern Sie sich, dass die von der VCAcore-Annotation gemeldete Höhe und Fläche in etwa korrekt sind.
- Beachten Sie, dass die Einstellungen für die eingeblendeten Anmerkungen im Bedienfeld verwendet werden können, um die verschiedenen Arten von Anmerkungen zu aktivieren und zu deaktivieren.
- Wiederholen Sie Schritt 4, bis die Kalibrierung akzeptabel ist.

8.9.4.5 Erweiterte Kalibrierungsparameter

Die erweiterten Kalibrierungsparameter ermöglichen es, die Grundebene zu schwenken und zu neigen, ohne die Kamerakalibrierungsparameter zu beeinflussen.
Dies kann hilfreich sein, um den Kalibrierungsaufbau zu visualisieren, wenn die Szene eine Schwenk- oder Neigebewegung gegenüber der Kamera aufweist.



Hinweis: Die erweiterten Parameter für Schwenken und Neigen beeinflussen lediglich die Ausrichtung der 3D-Grundebene, damit diese bequemer an die Videoszene angepasst werden kann; sie haben keinen Einfluss auf die Kalibrierungsparameter.

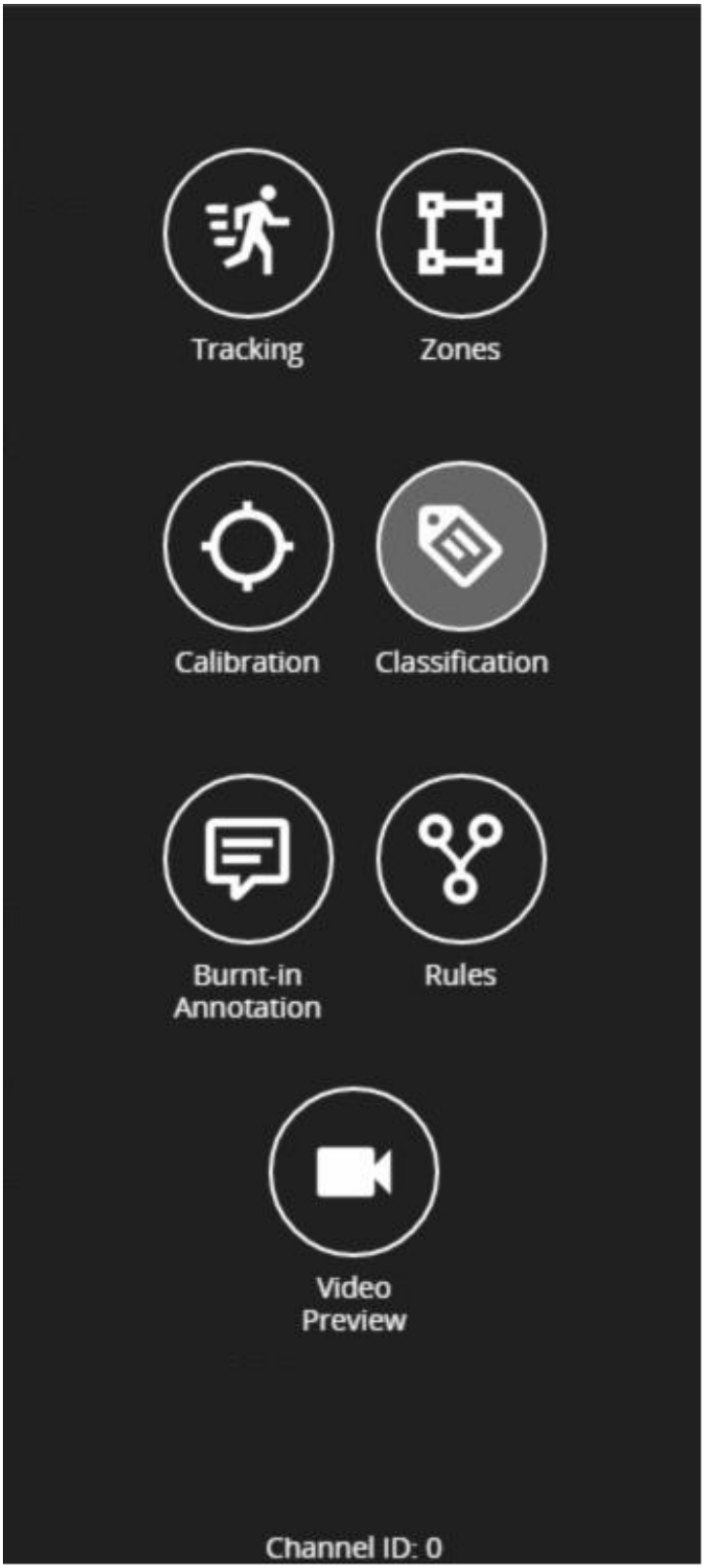
8.9.5 VCA-Klassifizierung

VCAcore kann eine Klasse für sich bewegende Objekte entweder mithilfe seiner Deep-Learning-Modelle oder anhand von Eigenschaften definieren, die aus einem Objekt in einer kalibrierten Szene extrahiert wurden.

Beide Klassifizierungsmethoden werden über Filter in der Regeloberfläche angewendet.

Klassifizierungsfilter ermöglichen es, ein Objekt, das eine Regel ausgelöst hat, anhand seiner vorhergesagten Klasse zu bewerten und bei Bedarf herauszufiltern.

MIRASYS



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

8.9.5.1 Objektklassifizierung

Sobald eine Kameraansicht kalibriert wurde, werden für jedes in dieser Ansicht erkannte Objekt verschiedene Eigenschaften ermittelt, darunter die Objektfläche und die Geschwindigkeit.

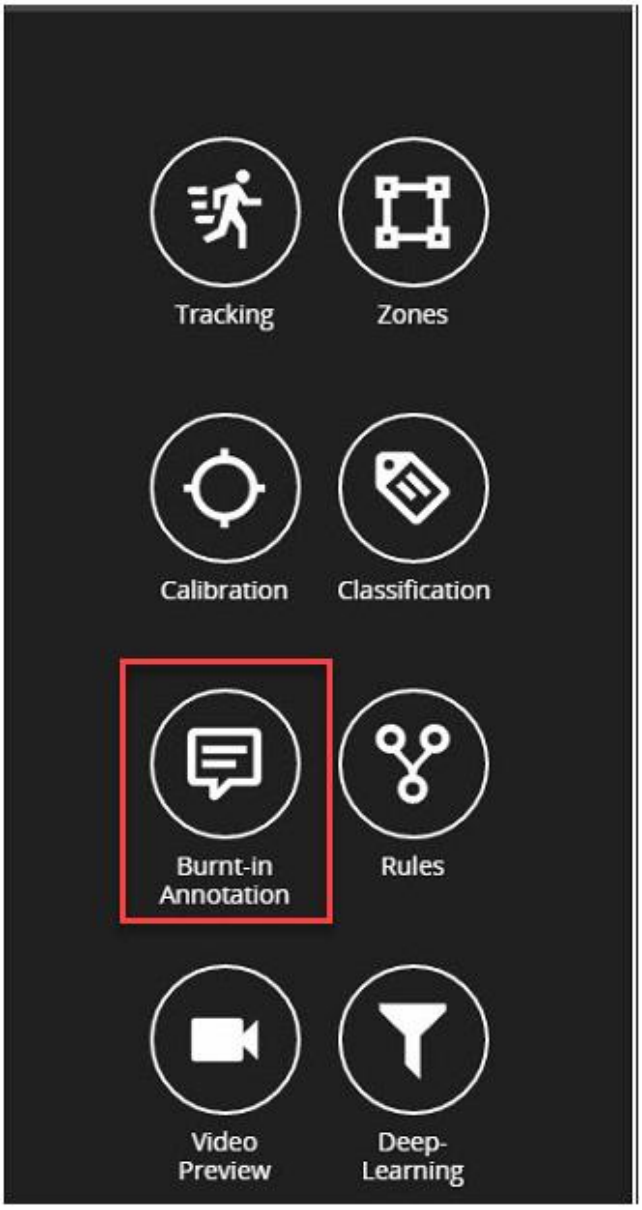
Die Objektklassifizierung von VCAserver erfolgt durch den Abgleich dieser Eigenschaften mit einer Reihe konfigurierbarer Objektklassifikatoren.

VCAserver ist bereits mit den gängigsten Objektklassifikatoren vorinstalliert, die in den meisten Fällen nicht angepasst werden müssen.

8.9.6 VCA Burnt-in Anmerkungen

Mit fest burnt-in Anmerkungen können VCAserver-Metadaten in den Rohvideostream eingeblendet werden.

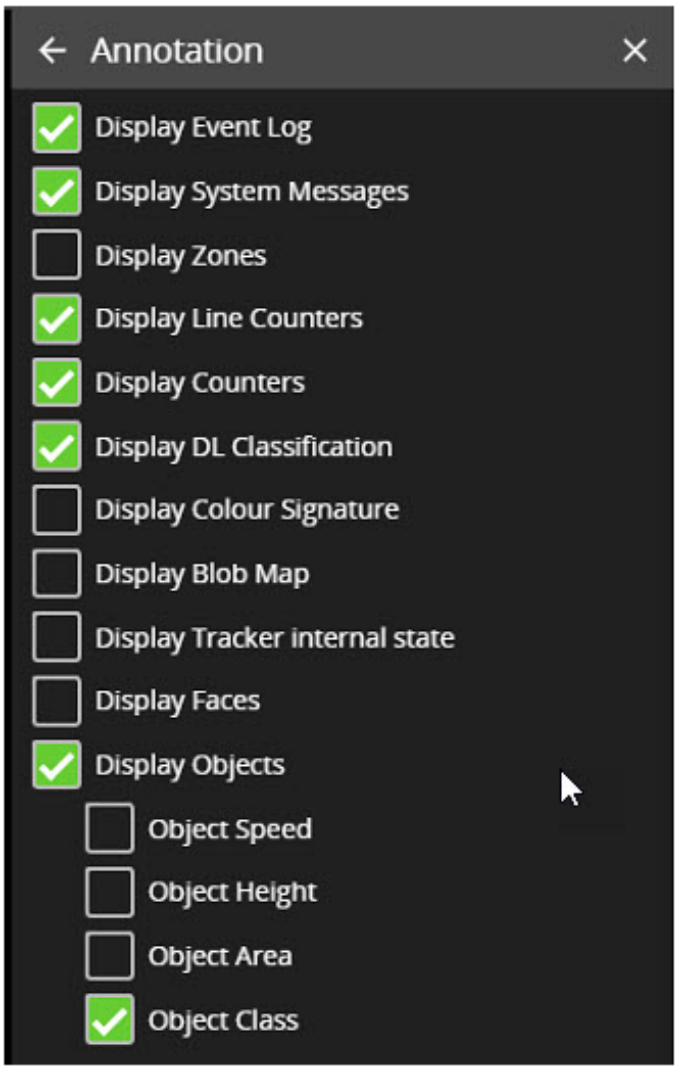
Über die Einstellungen für fest burnt-in Anmerkungen wird gesteuert, welche VCAserver-Metadaten (Objekte, Ereignisse usw.) in den Videostream eingeblendet werden.



Hinweis:

- Um Objektparameter wie Geschwindigkeit, Größe, Fläche und Klassifizierungen anzuzeigen, muss der Kanal zunächst kalibriert werden.
- Um DL-Klassifizierungsanmerkungen anzuzeigen, muss für den Kanal eine aktive Deep-Learning-Filterregel konfiguriert oder der DL People Tracker aktiviert sein.
- Um Farbsignatur-Anmerkungen anzuzeigen, muss für den Kanal eine aktive Farbfilterregel konfiguriert sein.

- Einige Anmerkungen gelten nur für bestimmte Tracker; in solchen Fällen ist der erforderliche Tracker in Klammern angegeben.



8.9.7 VCA-Regeln

Die Regeln von VCAcore dienen dazu, bestimmte Ereignisse in einem Videostream zu erkennen.
Es gibt drei Regeltypen, die zur Erkennung von Ereignissen und zum Auslösen von Aktionen genutzt werden können:

8.9.7.1 Basis-Eingaben / Regel:

Ein Algorithmus, der ausgelöst wird, wenn ein bestimmtes Verhalten oder Ereignis beobachtet wird, z. B. Anwesenheit. Basis-Eingaben können zum Auslösen einer Aktion verwendet werden.

8.9.7.2 Filter:

Ein Filter, der ausgelöst wird, wenn das Objekt, das die Eingangsregel / logische Regel ausgelöst hat, die Filteranforderungen erfüllt, z. B. sich mit einer bestimmten Geschwindigkeit bewegt. Filter können verwendet werden, um eine Aktion auszulösen.allen

8.9.7.3 Bedingte Regel:

Eine logische Verknüpfung zwischen einem oder mehreren Eingängen, um die Erkennung komplexerer Verhaltensweisen zu ermöglichen, z. B. UND.
Bedingte Regeln können verwendet werden, um eine Aktion auszulösen.
In VCAcore können Regelkonfigurationen so einfach sein wie einzelne Basiseingänge, die an eine Zone angehängt sind und zum Auslösen einer Aktion dienen.

Alternativ können Regeln mithilfe von bedingten Regeln und Filtern zu komplexeren logischen Regelkonfigurationen kombiniert werden.

Das übergeordnete Ziel der Regeln in VCAcore ist es, die Generierung fehlerhafter Warnmeldungen zu vermeiden, indem Funktionen bereitgestellt werden, die verhindern, dass unerwünschtes Verhalten eine Aktion auslöst.

- VCA – Grundlegende Eingaben
- VCA – Aggressives Verhalten
- VCA – Zurückgelassene und entfernte Objekte
- VCA – Erscheinen und Verschwinden
- VCA – Betreten und Verlassen
- VCA – Richtung
- VCA – Richtungswechsel
- VCA – Verweilen
- VCA – Fallen
- VCA – Anwesenheit
- VCA – Zu dichtes Auffahren
- VCA – Anhalten
- VCA – Zählreihe
- VCA – Bedingte Regeln
- VCA – Zähler
- VCA – Objekt-Spuren

- VCA – Objektanzeige

8.9.7.4 VCA – Grundlegende Eingaben

Eine einfache Eingabe oder Regel kann nur dazu verwendet werden, eine Aktion auszulösen oder als Eingabe für einen anderen Regeltyp zu dienen.
Einfache Eingaben erfordern immer eine Zone und möglicherweise einige zusätzliche Parameter.
Eine einfache Eingabe kann für sich allein verwendet werden, um eine Aktion auszulösen, wird jedoch häufig als Eingabe für andere Filter oder bedingte Regeln genutzt.

8.9.7.5 VCA – Aggressives Verhalten

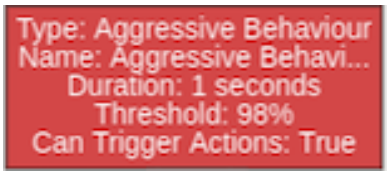
Eine Regel, die ausgelöst wird, wenn im Sichtfeld aggressives Verhalten über einen längeren Zeitraum als den festgelegten Wert festgestellt wird.

Aggressives Verhalten erfordert keine Zone und läuft unabhängig vom Tracker. Die Aktivierung dieses Algorithmus durch Hinzufügen dieser Regel wirkt sich auf die Kanalkapazität aus, da der Algorithmus zusätzlich zu dem für die ausgewählten Kanäle festgelegten Tracker ausgeführt wird.

Für diese Funktion ist eine separate VCAbehaviour-Lizenz erforderlich.



8.9.7.5.1 Grafische Ansicht



8.9.7.5.2 Formularansicht



8.9.7.5.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	“Aggressive #”
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Duration (Dauer)	Zeitraum, bevor ein aggressives Verhalten die Regel auslöst	1 to 60 seconds

8.9.7.6 VCA – Zurückgelassene und entfernte Gegenstände

Die Regel für zurückgelassene und entfernte Objekte wird ausgelöst, wenn ein Objekt in einem definierten Bereich zurückgelassen wurde – beispielsweise wenn eine Person eine Tasche auf einem Bahnsteig zurücklässt – oder wenn ein Objekt aus einem definierten Bereich entfernt wurde.
Die Regel für zurückgelassene Objekte verfügt über eine Dauer-Eigenschaft, die festlegt, wie lange ein Objekt bereits zurückgelassen oder entfernt sein muss, damit die Regel ausgelöst wird.

Nachfolgend finden Sie ein Beispielszenario, in dem eine Tasche in einem definierten Bereich zurückgelassen wird, wodurch die Regel ausgelöst wird.

MIRASYS



Nachfolgend finden Sie ein ähnliches Beispielszenario, bei dem die Tasche aus dem definierten Bereich entfernt wird, wodurch die Regel ausgelöst wird

MIRASYS

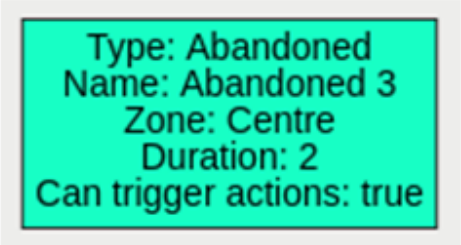


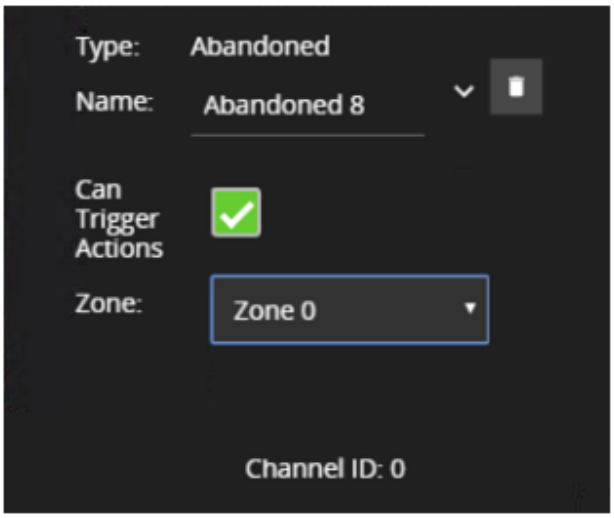
Tel +358 (0)9 2533 3300

Email info@mirasys.com

https://www.mirasys.com

Hinweis: Der zur Erkennung zurückgelassener und entfernter Objekte verwendete Algorithmus ist in beiden Fällen derselbe und kann daher nicht zwischen zurückgelassenen und entfernten Objekten unterscheiden. Dies liegt daran, dass der Algorithmus lediglich analysiert, wie sich Pixelblöcke im Verhältnis zu einem Hintergrundmodell verändern, das im Laufe der Zeit erstellt wird.



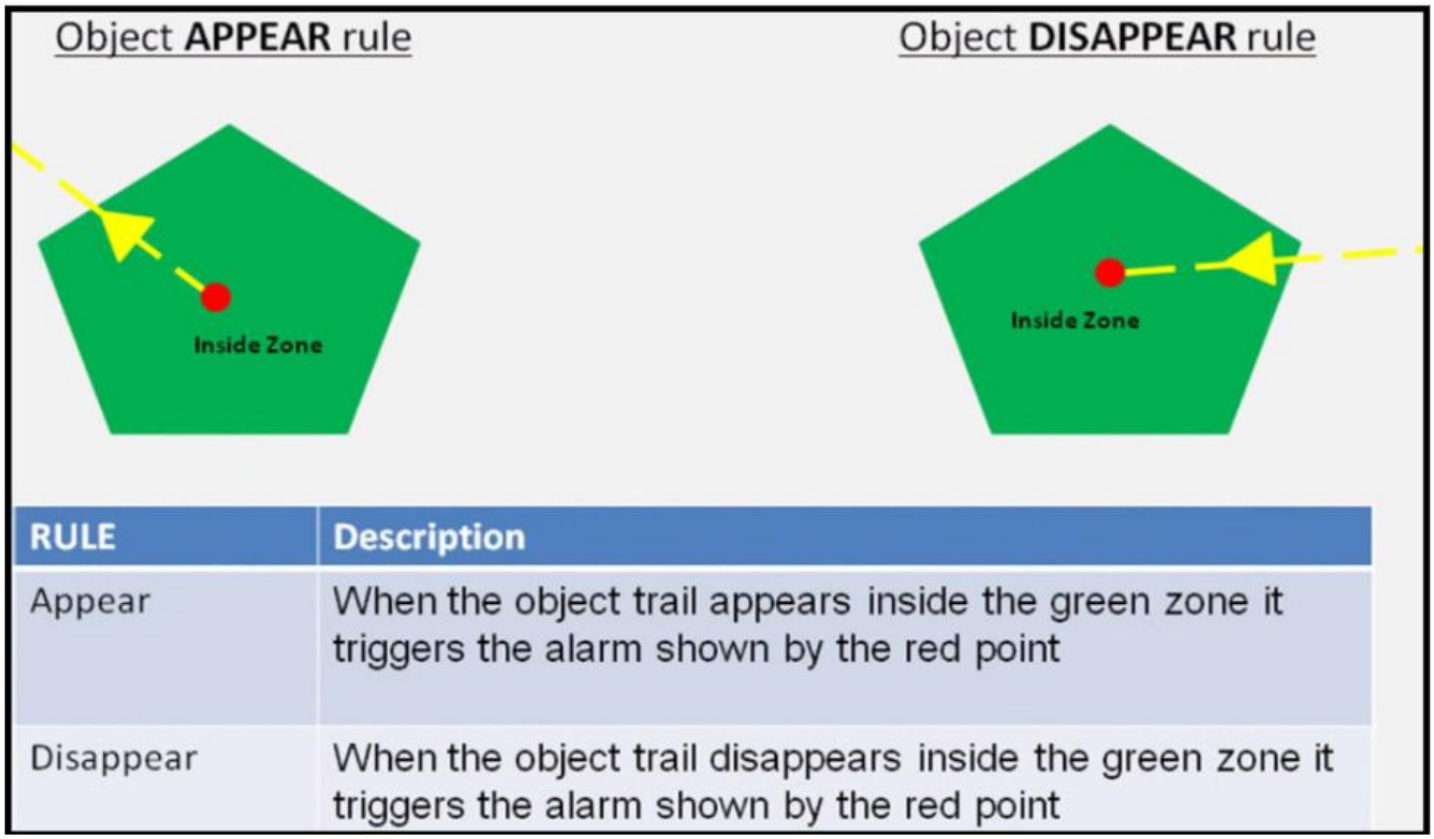


Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Abandoned #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Duration (Dauer)	Zeitraum, in dem ein Objekt bereits zurückgelassen oder entfernt worden sein muss, bevor die Regel ausgelöst wird	0
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

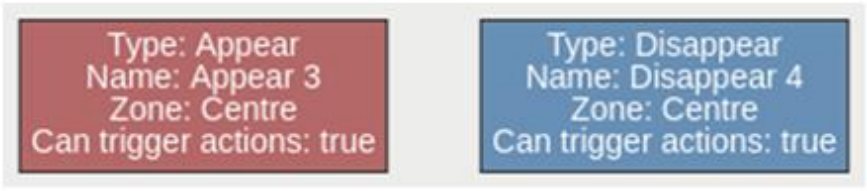
8.9.7.7 VCA – Erscheinen und Verschwinden

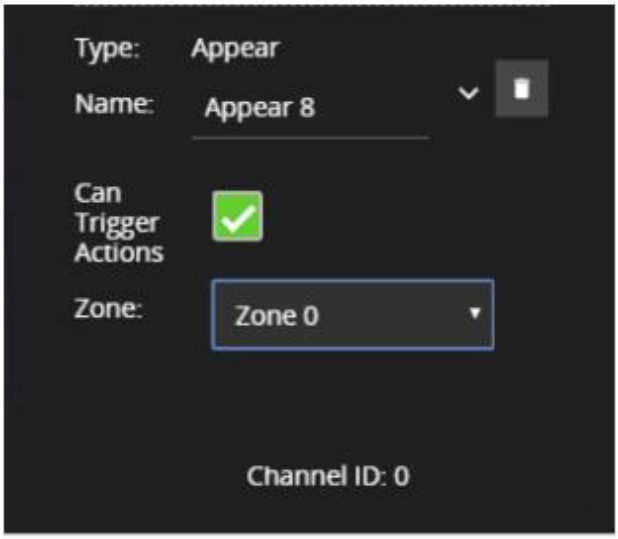
Die „Erscheinen“-Regel erkennt Objekte, deren Verfolgung innerhalb einer Zone beginnt, z. B. eine Person, die aus einer Tür in die Szene tritt.

Umgekehrt erkennt die „Verschwinden“-Regel Objekte, deren Verfolgung innerhalb einer Zone endet, z. B. eine Person, die durch eine Tür die Szene verlässt.
Hinweis: Die „Erscheinen“- und „Verschwinden“-Regeln unterscheiden sich von den „Eintritt“- und „Austritt“-Regeln, wie in den Beschreibungen der „Eintritt“- und „Austritt“-Regeln erläutert.



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





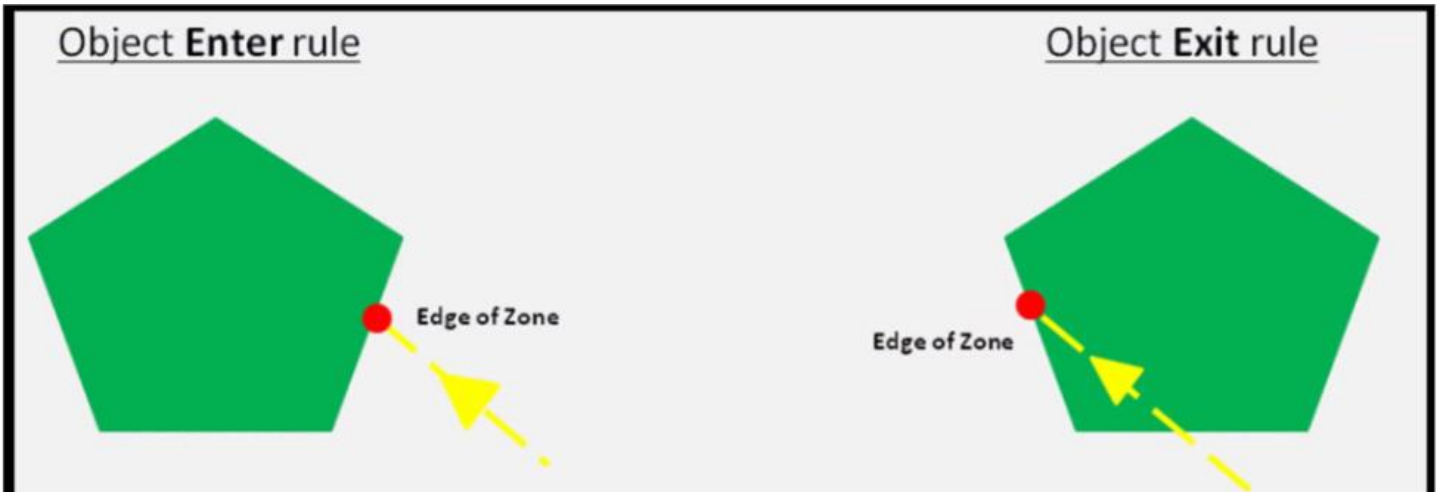
8.9.7.7.1 Konfiguration für Appear

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Appear #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.7.2 Konfiguration für Disappear

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Disappear #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.8 VCA – Ein- und Ausstieg

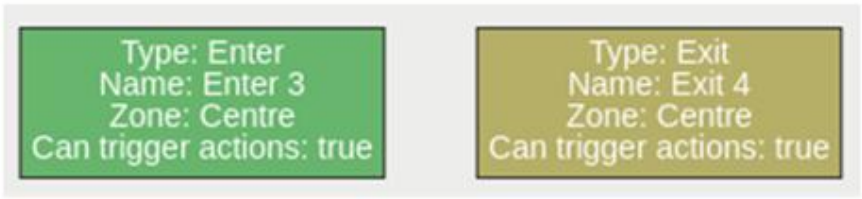


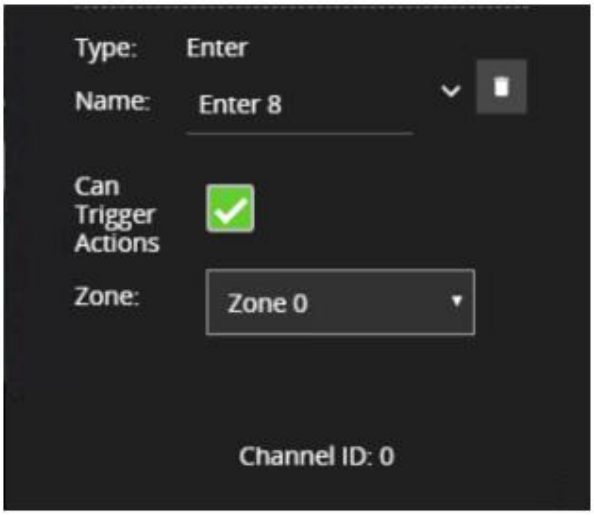
RULE	Description
Enter	When the object trail crosses from the outside to the inside of the green zone it triggers the alarm shown by the red point
Exit	When the object trail crosses from the inside to the outside of the green zone it triggers the alarm shown by the red point

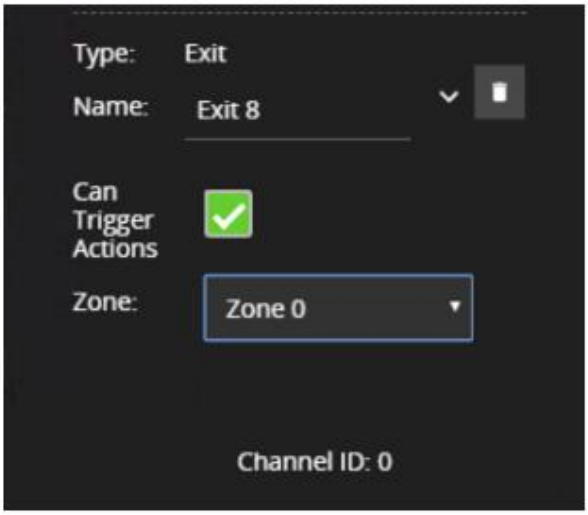
Die „Enter“-Regel erkennt, wenn Objekte eine Zone betreten.
Mit anderen Worten: wenn Objekte von außerhalb einer Zone in das Innere einer Zone gelangen.
Umgekehrt erkennt die „Exit“-Regel, wenn ein Objekt eine Zone verlässt: wenn es die Grenze einer Zone von innen nach außen überschreitet.

Hinweis: „Enter“- und „Exit“-Regeln unterscheiden sich wie folgt von „Appear“- und „Disappear“-Regeln:

1. Während die „Enter“-Regel bereits verfolgte Objekte erkennt, die die Zonengrenze von außen nach innen überqueren, erkennt die „Appear“-Regel Objekte, die innerhalb einer Zone verfolgt werden (z. B. durch eine Tür in die Szene erscheinen).
2. Während die „Exit“-Regel bereits verfolgte Objekte erkennt, die die Zonengrenze von innen nach außen überqueren, erkennt die „Disappear“-Regel Objekte, die innerhalb der Zone nicht mehr verfolgt werden (z. B. durch eine Tür die Szene verlassen).







8.9.7.8.1 Konfiguration für Enter

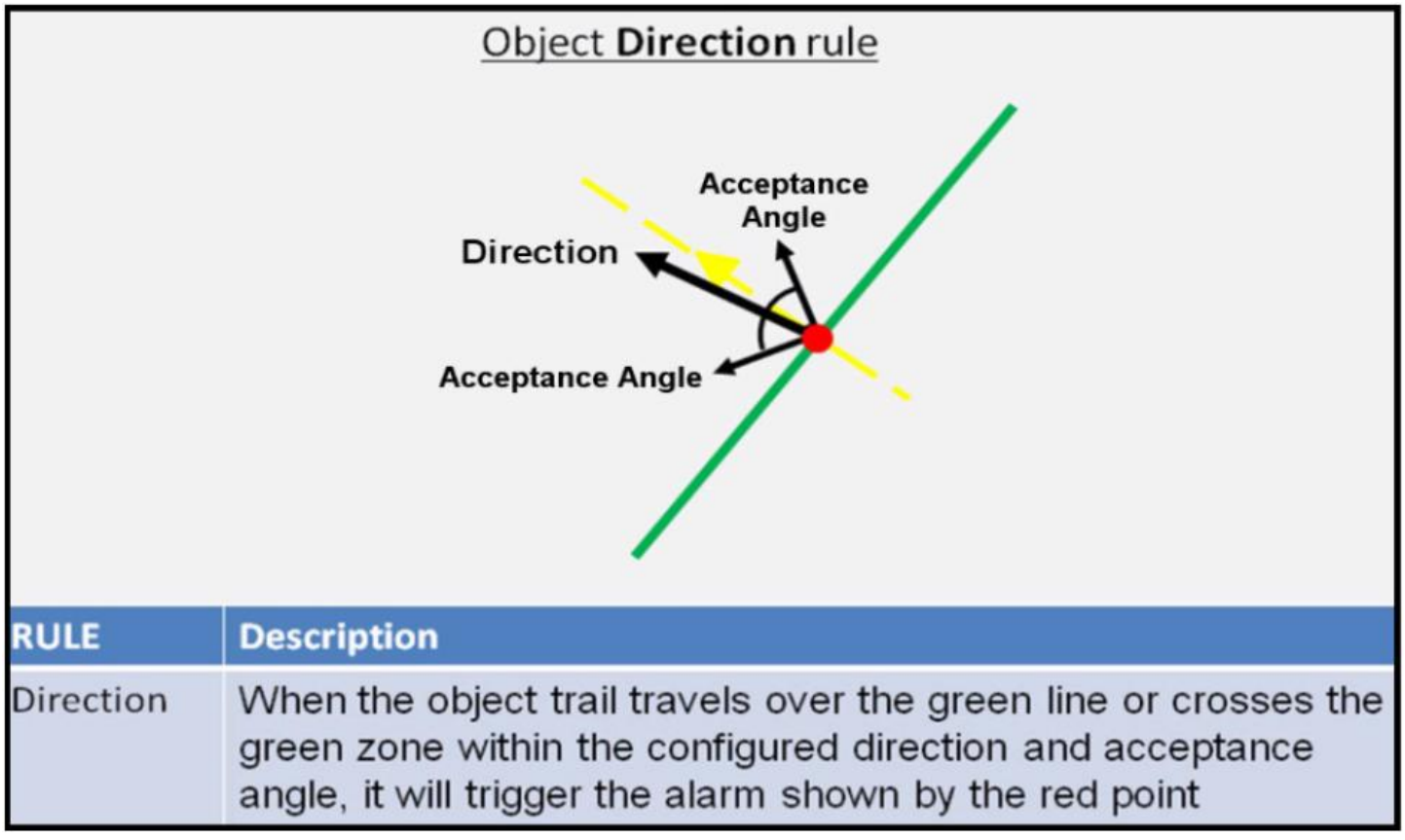
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Enter #"
Zone	Die Zone, der diese Regel zugeordnet ist	None

Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.8.2 Konfiguration für Exit

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Exit #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

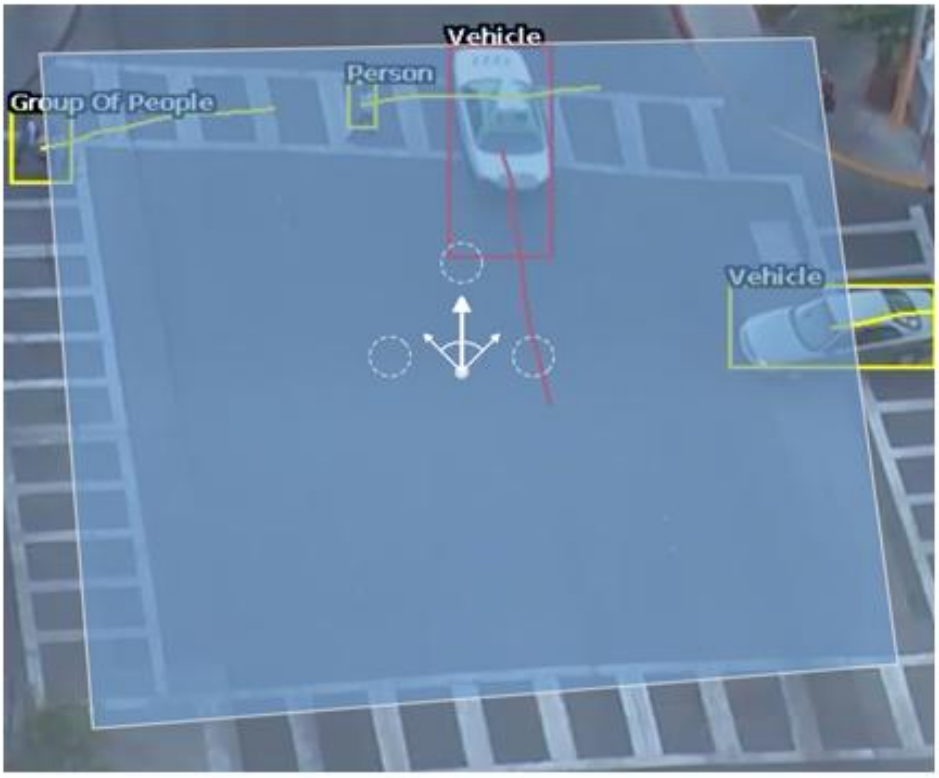
8.9.7.9 VCA – Richtung



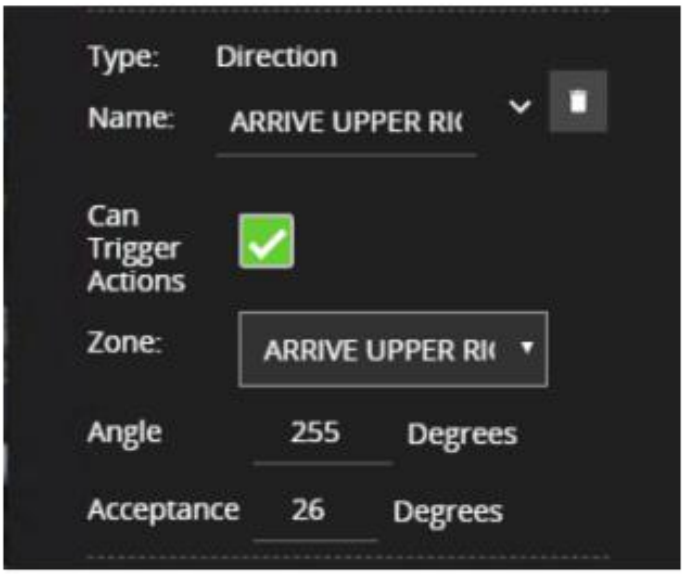
Die Richtungsregel erkennt Objekte, die sich in eine bestimmte Richtung bewegen.
Konfigurieren Sie die Richtung und den Erfassungswinkel, indem Sie die Pfeile auf dem Steuerelement für die Richtung verschieben.
Die Hauptrichtung wird durch den großen Pfeil in der Mitte angezeigt.
Der Erfassungswinkel ist der Winkel zwischen den beiden kleineren Pfeilen.

Objekte, die sich in der konfigurierten Richtung (innerhalb der Grenzen des Erfassungswinkels) durch eine Zone oder über eine Linie bewegen, lösen die Regel aus und lösen ein Ereignis aus.
Die folgende Abbildung veranschaulicht, wie das weiße Auto, das sich in der konfigurierten Richtung bewegt, die Regel auslöst, während die anderen Objekte dies nicht tun.

MIRASYS



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



8.9.7.9.1 Konfiguration für Richtung

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Direction #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Winkel	Primärer Richtungswinkel, 0–359. 0 als Referenz nach oben.	0
Annahme	Zulässige Abweichung auf jeder Seite der Hauptrichtung, bei der die Regel weiterhin ausgelöst wird	0

8.9.7.10 VCA – Richtungswechsel

Die Regel „Richtungsüberschreitung“ wurde entwickelt, um Fehlalarme zu reduzieren, die bei einfachen Anwendungsfällen mit Linienüberschreitungen häufig auftreten. Die Richtungsüberschreitung ist für die Verwendung mit einer Zone anstelle einer Linie konzipiert und führt eine Reihe zusätzlicher Prüfungen durch, wenn ein Objekt diese Zone sowohl betritt als auch verlässt.

Damit ein Objekt die Regel „Richtungsüberschreitung“ auslöst, muss es:

- die Zone in einer Richtung betreten, die innerhalb des Akzeptanzwinkels liegt.
- einer der angegebenen Objektklassen zugeordnet sein.
- die Zone in einer Richtung verlassen, die innerhalb des Akzeptanzwinkels liegt.

Konfigurieren Sie die Richtung und den Akzeptanzwinkel, indem Sie die Pfeile auf dem Steuerelement für die Richtung verschieben. Die Hauptrichtung wird durch den großen zentralen Pfeil angezeigt. Der Akzeptanzwinkel ist der Winkel zwischen den beiden kleineren Pfeilen.

Die folgende Abbildung veranschaulicht, wie das weiße Auto, das sich in der konfigurierten Richtung bewegt, die Regel auslöst, während die anderen Objekte dies nicht tun.



8.9.7.10.1 Grafische Ansicht

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 Formularansicht



8.9.7.10.3 Konfiguration

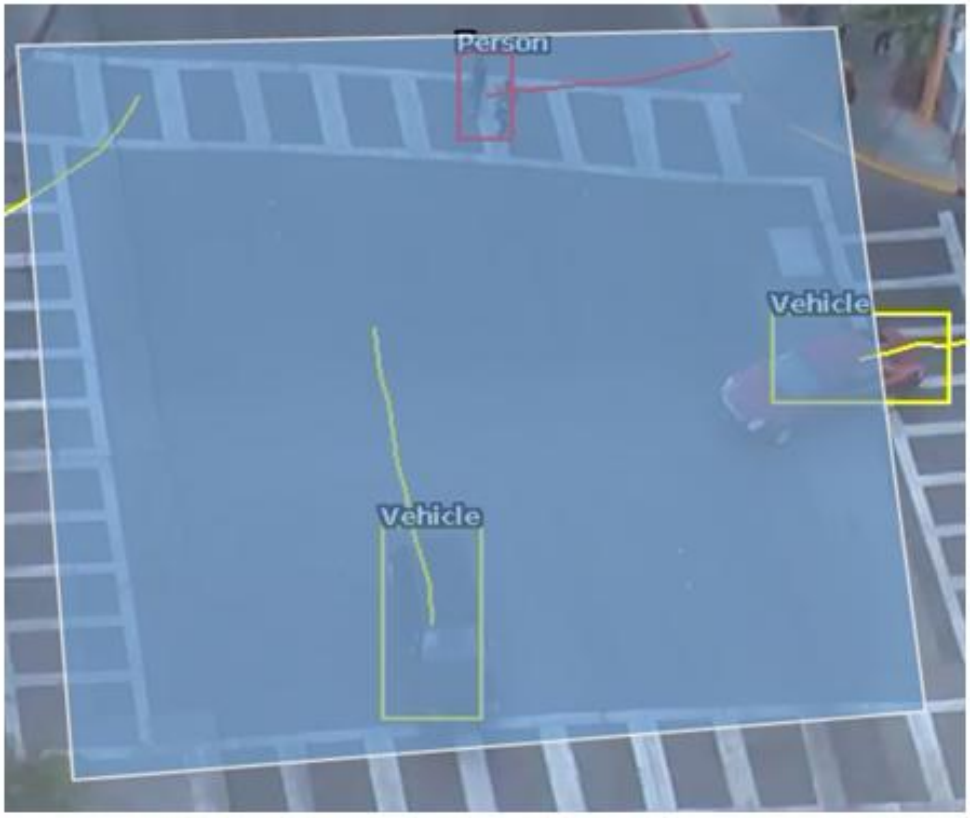
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	“Directional #”

Merkmal	Beschreibung	Standardwert
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Zone	Die Zone, der diese Regel zugeordnet ist	None
Angle (Winkel)	Primärer Richtungswinkel, 0–359. 0 als Referenz nach oben.	0
Annahme	Zulässige Abweichung auf jeder Seite der Hauptrichtung, bei der die Regel weiterhin ausgelöst wird	0
Klassen	Die Objektklassen, die einen Alarm auslösen dürfen	None

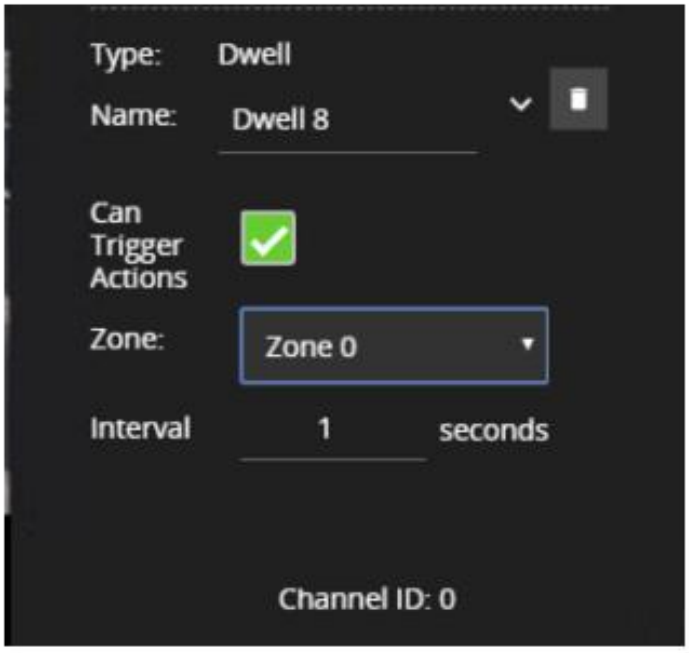
8.9.7.11 VCA – Dwell

Eine Verweildauerregel wird ausgelöst, wenn sich ein Objekt für eine bestimmte Zeit in einer Zone aufgehalten hat. Der Parameter „Intervall“ gibt die Zeit an, die das Objekt in der Zone verweilen muss, bevor ein Ereignis ausgelöst wird.
Die folgende Abbildung zeigt, wie die in der Zone erkannte Person rot hervorgehoben wird, da sie sich bereits für die gewünschte Zeit in der Zone aufgehalten hat.
Die beiden Fahrzeuge haben sich noch nicht lange genug in der Zone aufgehalten, um die Verweildauerregel auszulösen.

MIRASYS



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



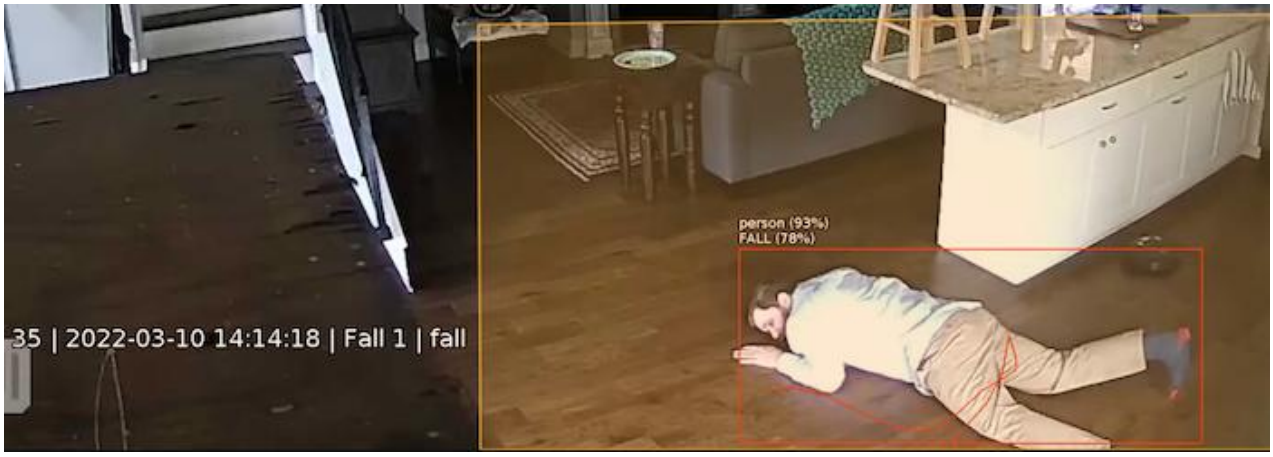
8.9.7.11.1 Konfiguration für Dwell

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Direction #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Intervall	Zeitdauer in Sekunden	1

8.9.7.12 VCA - Fallen

Die Sturzregel erkennt, wenn sich ein Objekt, das vom Deep Learning People Tracker als Person klassifiziert wurde, im gestürzten Zustand befindet.

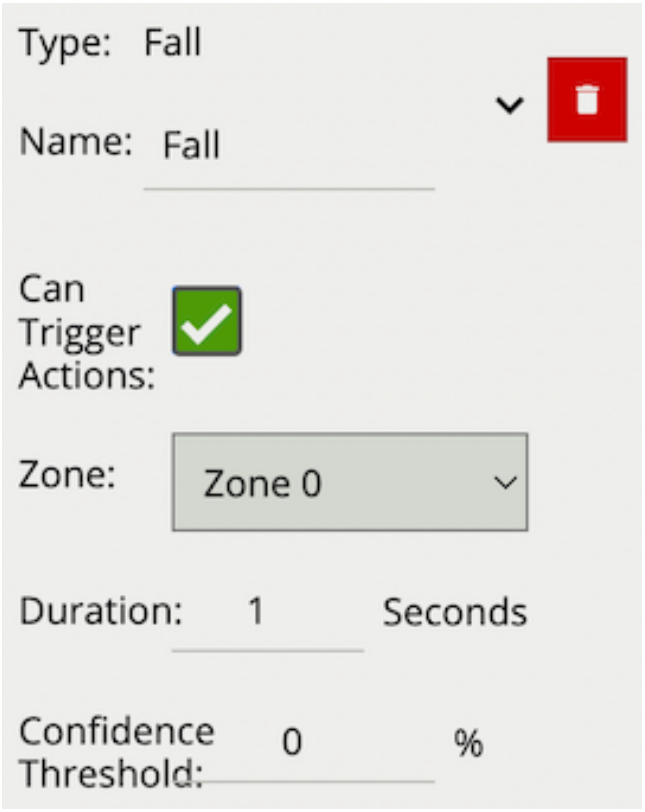
Wenn die Sturzregel zu einer Kanalkonfiguration hinzugefügt wird, läuft der Sturzerkennungsalgorithmus im Hintergrund, was zu einer zusätzlichen Belastung der GPU führt. Derzeit ist diese Regel nur bei Verwendung des Deep Learning People Trackers verfügbar.



8.9.7.12.1 Grafische Ansicht



8.9.7.12.2 Formularansicht



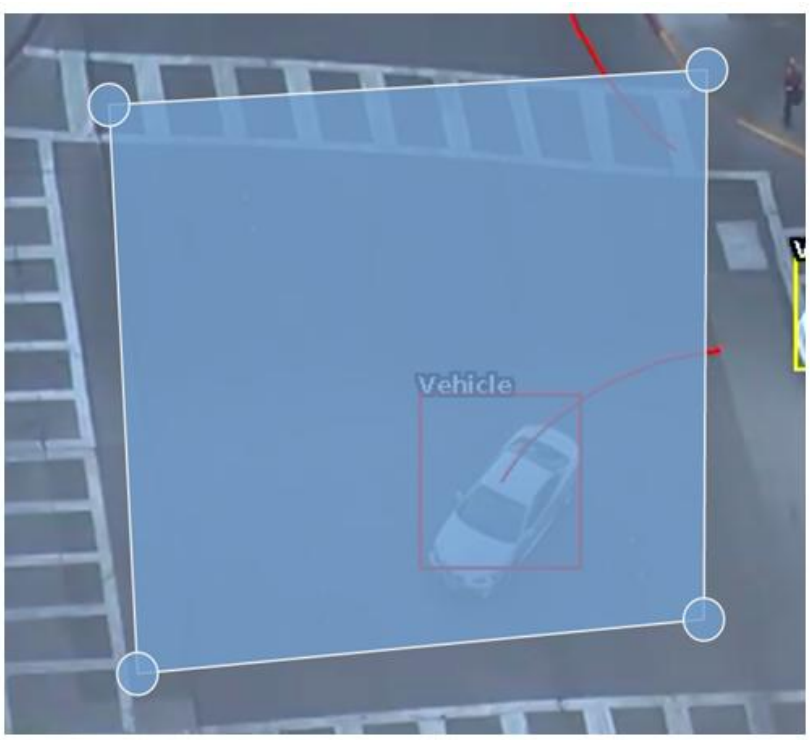
8.9.7.12.3 Konfiguration

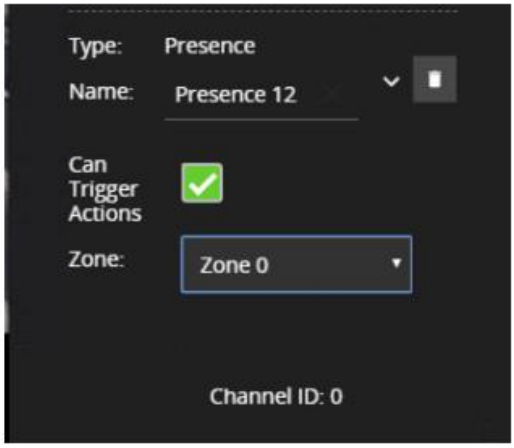
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Fall #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Duration (Dauer)	Zeitraum, den ein Objekt bereits gefallen sein muss, bevor die Regel ausgelöst wird	1 to 60 seconds
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Confidence Threshold (Konfidenzschwelle)	Die für die Auslösung der Regel erforderliche Algorithmus-Zuverlässigkeit (in Prozent)	0

8.9.7.13 VCA – Anwesenheit

Eine Regel, die ein Ereignis auslöst, wenn ein Objekt zum ersten Mal in einer bestimmten Zone erkannt wird. Hinweis: Die „Presence“-Regel umfasst eine Vielzahl unterschiedlicher Verhaltensweisen; so wird sie

beispielsweise unter denselben Umständen ausgelöst wie die „Enter“- und die „Appear“-Regel.
Welche Regel am besten geeignet ist, hängt vom jeweiligen Szenario ab.





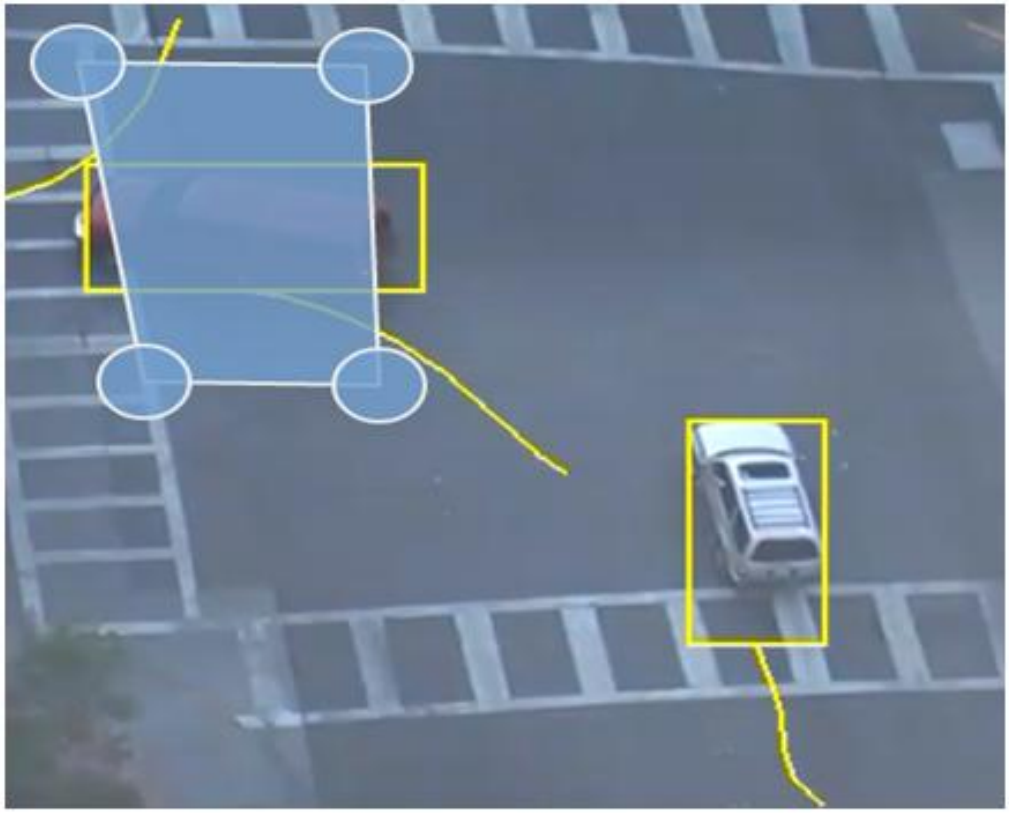
8.9.7.13.1 Konfiguration Anwesenheit

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Deep Learning Presence #"

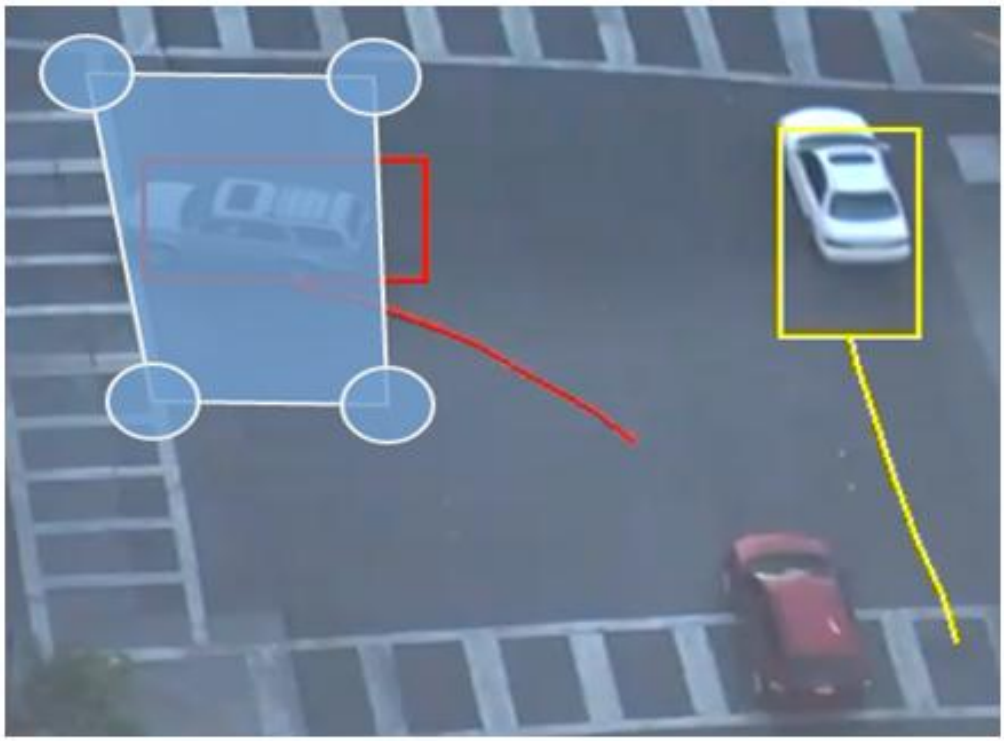
Zone	Die Zone, der diese Regel zugeordnet ist	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.14 VCA - zu dichtes Auffahren

Die Regel zur Erkennung von zu dichtem Auffahren erkennt Objekte, die kurz nacheinander eine Zone durchqueren oder eine Linie überqueren.
In diesem Beispiel ist Objekt 1 gerade dabei, eine Erkennungslinie zu überqueren. Ein weiteres Objekt (Objekt 2) folgt dicht dahinter.
Der Schwellenwert für die Erkennung von zu dichtem Auffahren ist auf 5 Sekunden eingestellt.
Das heißt, jedes Objekt, das die Linie innerhalb von 5 Sekunden nach einem Objekt überquert, das die Linie bereits überquert hat, löst die Regel zur Erkennung von zu dichtem Auffahren aus.



Objekt 2 überquert die Linie innerhalb von 5 Sekunden nach Objekt 1. Dies löst den Filter für zu geringen Abstand aus und löst ein Ereignis aus.





8.9.7.14.1 Konfiguration

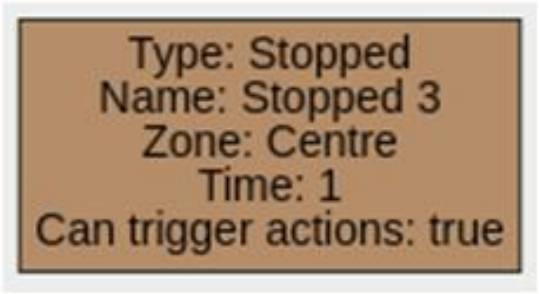
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Tailgating #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Duration (Dauer)	Zeitraum, den ein Objekt bereits gefallen sein muss, bevor die Regel ausgelöst wird	0

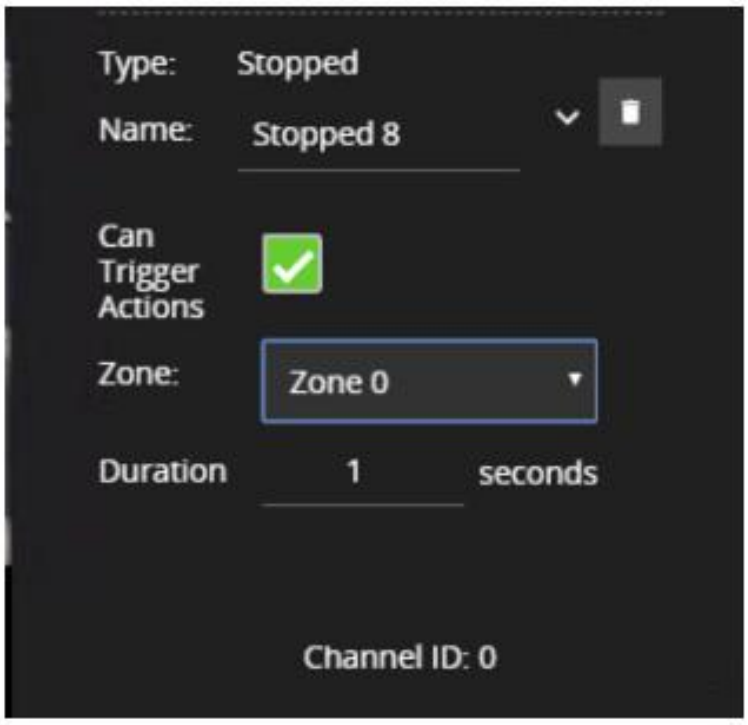
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.15 VCA - Angehalten

Die Regel „Stillstand“ erkennt Objekte, die sich länger als die festgelegte Zeit innerhalb einer Zone nicht bewegen. Für die Regel „Stillstand“ muss zunächst eine Zone ausgewählt werden, bevor die Zeitdauer konfiguriert werden kann.

Hinweis: Die Regel „Stillstand“ erkennt keine zurückgelassenen Objekte. Sie erkennt nur Objekte, die sich zu einem bestimmten Zeitpunkt bewegt haben und dann stillstehen.





8.9.7.15.1 Konfiguration Angehalten

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Stopped #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Time (Zeit)	Zeitraum, bevor ein stillstehendes Objekt die Regel auslöst	0
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.16 VCA- Zählzeile

Die letzte Version, die die „Line Counter"-Regel enthält, ist 9.6.2. Anstelle des „Line Counter" wird empfohlen, die Regeln „Direction" und „Directional Crossing" in Verbindung mit Zählern zu verwenden, da diese Optionen eine größere Flexibilität und Kompatibilität mit Trackern bieten.

Eine Zählzeile (Line Counter) ist ein Erkennungsfilter, der für die richtungsabhängige Objektzählung (z. B. von Personen oder Fahrzeugen) in belebteren Erkennungsszenarien optimiert ist.

Beispiele für solche Anwendungen sind unter anderem:

- Personenzählung mit Überkopfkameras im Einzelhandel.
- Fahrzeugzählung mit Überkopfkameras auf öffentlichen Straßen.

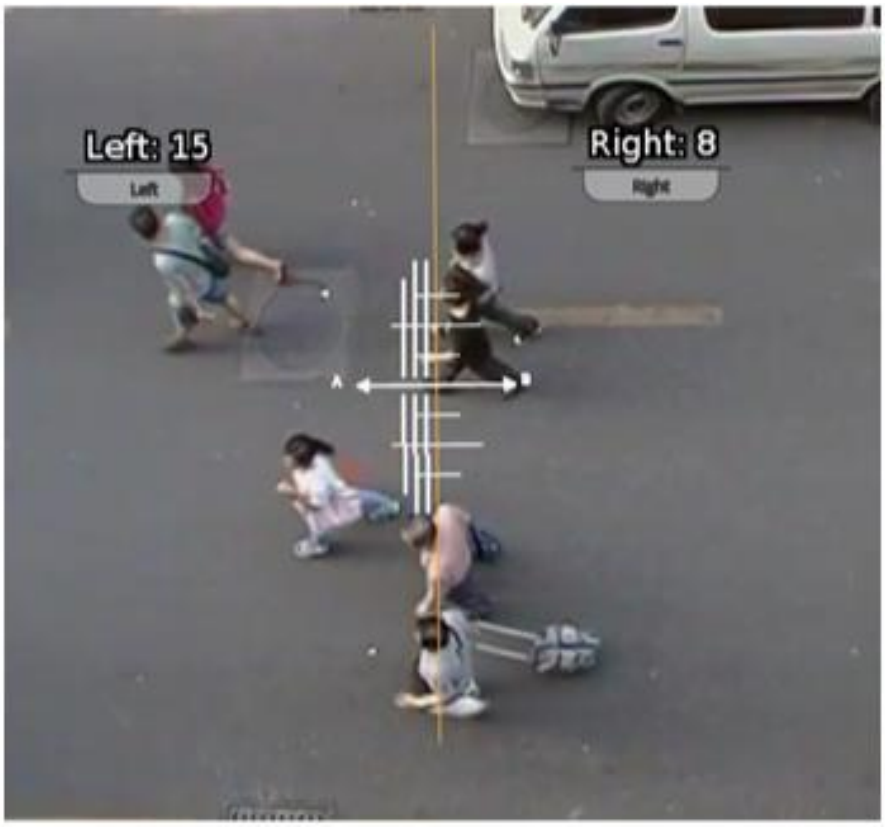
In bestimmten Situationen, wie beispielsweise an Eingängen mit Überkopfkameras, liefert die Zähllinie in der Regel genauere Ergebnisse als die oben genannten Zähler, die mit einer Anwesenheitsregel verknüpft sind.

Jedes Mal, wenn ein Objekt die Linie in der konfigurierten Richtung überquert, wird ein Ereignis ausgelöst.
Wenn mehrere Objekte gleichzeitig die Linie überqueren, werden entsprechend mehrere Ereignisse ausgelöst.
Diese Ereignisse können direkt zum Auslösen von Aktionen verwendet werden, sofern die Eigenschaft „Kann Aktionen auslösen" aktiviert ist.
Zähllinien werden an Zonen angehängt, die mit einer Linienform konfiguriert sind.
Weitere Informationen finden Sie unter **Zonen**.

Wenn eine Zählzeile mit einer Zone konfiguriert wird, die nicht als Linienform definiert ist, wird die Zoneigenschaft automatisch geändert (die Form der Zone kann erst wieder geändert werden, wenn die Zählzeile nicht mehr auf die betreffende Zone verweist).

Zählzeilen haben eine festgelegte Richtung, die durch den Pfeil in der Benutzeroberfläche angezeigt wird (Richtung A oder B); die Richtung dieses Pfeils wird durch die konfigurierte Zone bestimmt.
Jede Instanz der Regel zählt in einer einzigen Richtung. Um in beide Richtungen zu zählen, muss eine zweite Zählregel zur gleichen Zone hinzugefügt werden, wobei die entgegengesetzte Richtung ausgewählt wird.
Zur Veranschaulichung ist unten ein Beispiel-Regeldiagramm einer mit einem Zähler konfigurierten Zwei-Wege-Zählregel dargestellt.

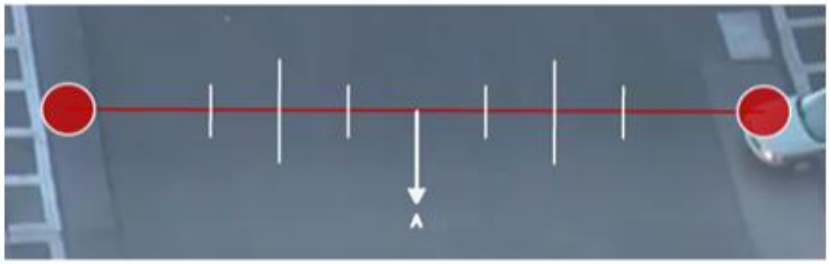
HINWEIS: Die maximale Anzahl an Zählregelfiltern, die pro Videokanal angewendet werden können, beträgt 5.



8.9.7.16.1 Kalibrierung der Zählzeile

Um genaue Zählwerte zu erhalten, muss die Zählzeile kalibriert werden.
Im Gegensatz zur Objektverfolgungsfunktion kann dies nicht allgemein für die gesamte Szene mithilfe des 3D-Kalibrierungswerkzeugs durchgeführt werden.
Der Grund dafür ist, dass die Zählzeile nicht immer auf der Bodenebene platziert ist; sie kann an jeder beliebigen Stelle in der Szene in beliebiger Ausrichtung platziert werden.

Beispielsweise könnte eine Zählzeile bei einer seitlichen Kameraansicht vertikal ausgerichtet werden.
Anstelle des 3D-Kalibrierungswerkzeugs verfügt die Zählzeile über eine eigene Kalibrierungseinstellung.
Zwei Balken, die in gleichem Abstand zur Mitte der Zeile liegen, stellen die Breite des erwarteten Objekts dar.
Dadurch kann die Zählzeile Störsignale ausblenden und auch mehrere Objekte zählen.



8.9.7.16.1.1 So kalibrieren Sie die Zählzeile:

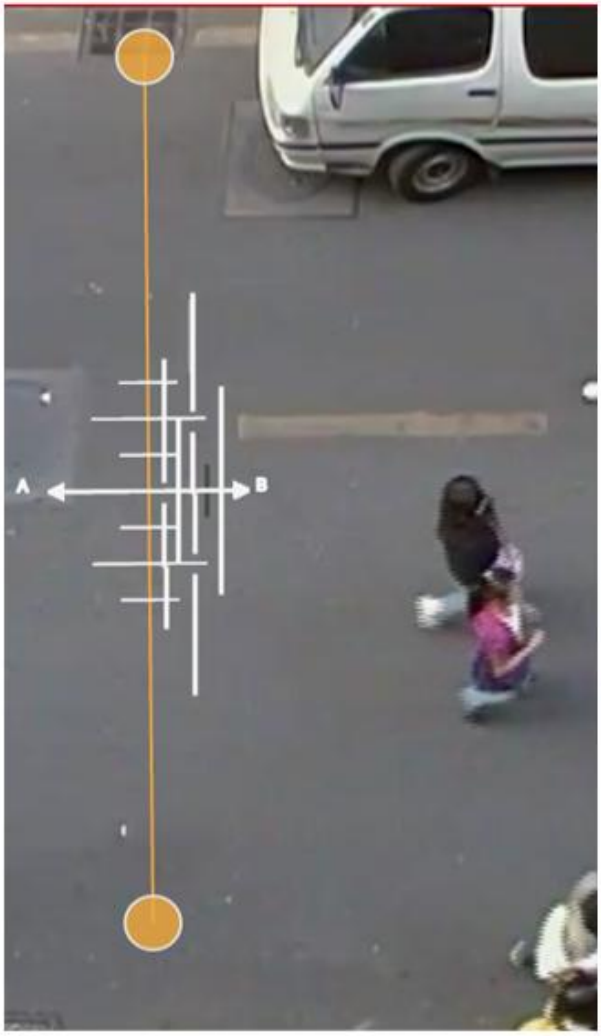
1. Wählen Sie die Regel „Line Counter“ aus.
2. Aktivieren Sie die Option „Breitenkalibrierung aktivieren“.
3. Ziehen Sie die Kalibrierungsmarkierungen, um den Abstand zwischen ihnen so anzupassen, dass er in etwa der Größe der zu zählenden Objekte entspricht. Alternativ können Sie den Schieberegler „Breite“ verschieben, um das gleiche Ergebnis zu erzielen.
4. Die Kalibrierungsbreite wird innerhalb der Zählzeilenlinie angezeigt und kann direkt bearbeitet werden, um die Kalibrierungsbreite zu ändern.
5. Die kleinen Markierungen auf beiden Seiten der großen Markierungen zeigen die minimale und maximale Breite an, die als ein einzelnes Objekt gezählt wird.

HINWEIS: Wenn der Schieberegler „Breite“ auf Null gesetzt ist, wird das Kontrollkästchen „Breitenkalibrierung aktivieren“ automatisch deaktiviert.

8.9.7.16.1.2 Rückmeldung zur Kalibrierung der Zählzeile

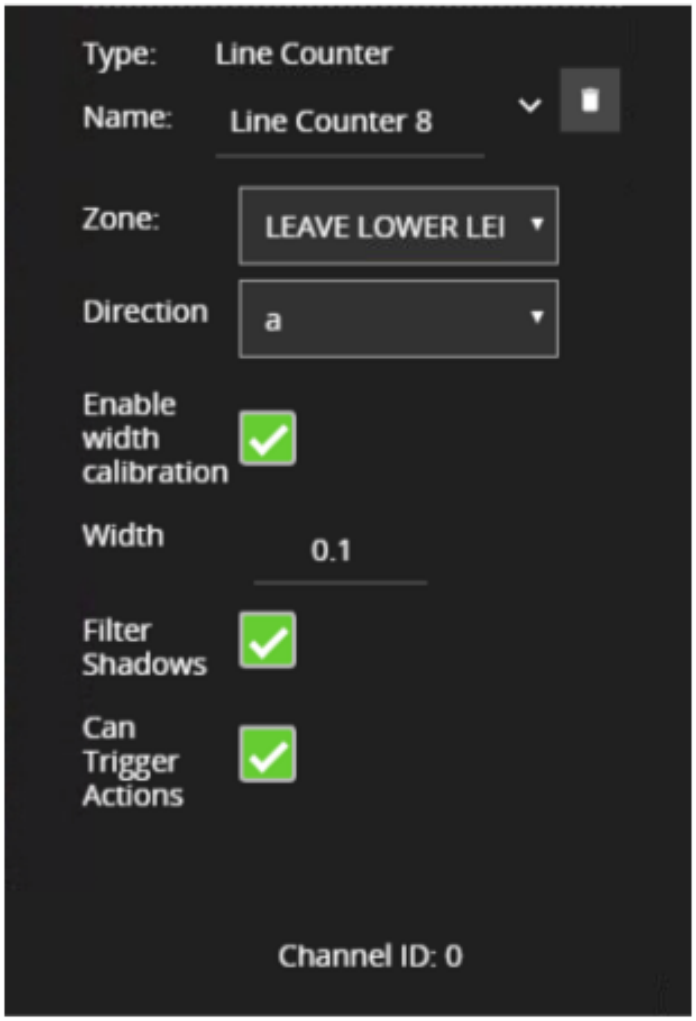
Damit der Benutzer die Kalibrierung der Zählzeile genauer konfigurieren kann, werden die Breiten der erkannten Objekte als Überlagerung neben der Zählzeile angezeigt, wenn Objekte diese passieren.
Standardmäßig ist diese Anzeigeoption aktiviert. Sollte sie jedoch nicht erscheinen, stellen Sie sicher, dass die Option in den Einstellungen für „Eingebrannte Anmerkungen“ aktiviert ist.

Die Kalibrierungsrückmeldung wird auf der Seite „Zonenkonfigurationen“ als schwarze und weiße Linien auf beiden Seiten der Zählzeile dargestellt. Jede Linie steht für ein vom Zählalgorithmus erkanntes Objekt. Die Breite der Linie zeigt die Breite des von der Linie erkannten Objekts an. Für jede Richtung werden die letzten Erkennungen angezeigt, wobei die aktuellste am nächsten an der Zählzeile erscheint.



8.9.7.16.2 Schattenfilter

Die Zählzeile verfügt über einen Schattenfilter, der dazu dient, die Auswirkungen von Objektschatten auf den Zählalgorithmus zu beseitigen.
Schatten können zu ungenauen Zählergebnissen führen, indem sie ein Objekt größer erscheinen lassen, als es tatsächlich ist, oder indem sie zwei oder mehr Objekte miteinander verbinden.
Wenn Schatten zu ungenauen Zählungen führen, sollte der Schattenfilter aktiviert werden, indem das Kontrollkästchen „Schattenfilter“ für die Linie aktiviert wird.
Es wird empfohlen, den Schattenfilter nur zu aktivieren, wenn tatsächlich Schatten vorhanden sind, da der Algorithmus bestimmte Teile eines Objekts fälschlicherweise als Schatten interpretieren kann, was zu schlechteren Zählergebnissen führen kann.
Dies gilt insbesondere für Objekte, die im Vergleich zum Hintergrund einen geringen Kontrast aufweisen (z. B. Personen in schwarzen Mänteln vor einem schwarzen Teppich).



Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Stopped #"
Zone	Die Zone, der diese Regel zugeordnet ist	None
Direction (Richtung)	Zählen in Richtung „A“ oder „B“ aktivieren (eine Richtung pro Zählzeile)	None
Enable Width Calibration (Breitenkalibrierung aktivieren)	Breitenkalibrierung für eine genauere Zählung	None
Width (Breite)	Kalibrierungswert für die Breite	0
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active

8.9.7.17 VCA - Bedingte Regeln

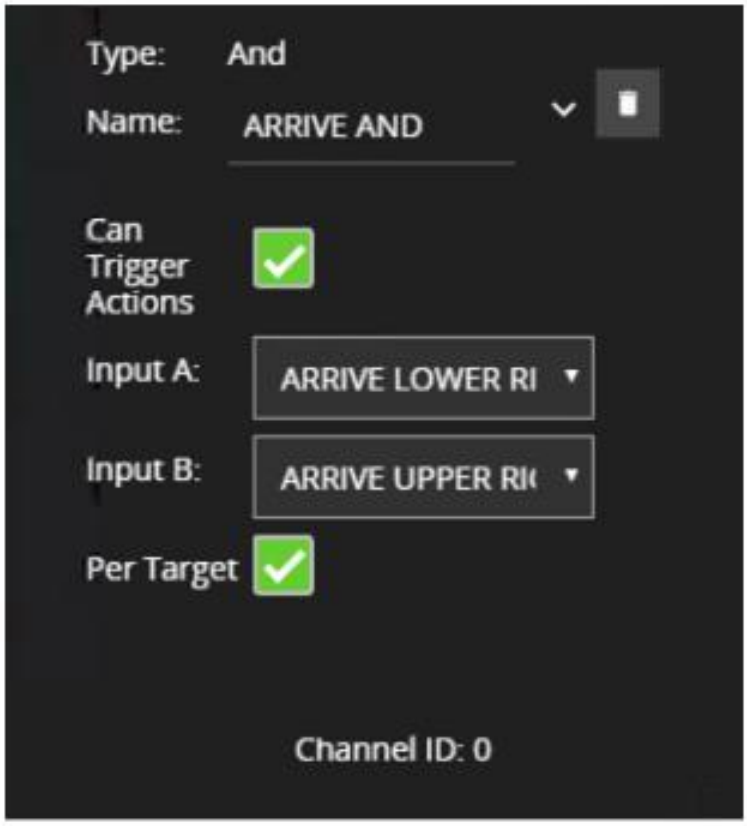
Eine bedingte Eingabe ist, ähnlich wie ein Filter, eine Eingabe, die allein keine Aktion auslösen kann.
Sie benötigt die Eingabe einer anderen Basiseingabe, einer bedingten Regel oder eines Filters, um sinnvoll zu sein.
Ein Beispiel hierfür ist die UND-Regel. Die UND-Regel benötigt zwei zu vergleichende Eingaben, um zu funktionieren.

8.9.7.17.1 Die vollständige Liste der bedingten Regeln lautet wie folgt:

- And
- Continuously
- Counter
- Or
- Previous

8.9.7.17.2 And

Ein logischer Operator, der zwei Regeln miteinander verknüpft und nur dann Ereignisse auslöst, wenn beide Eingaben wahr sind.



Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"And #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input A (Eingabe A)	Die erste Eingabe	None
Input B (Eingabe B)	Die zweite Eingabe	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active

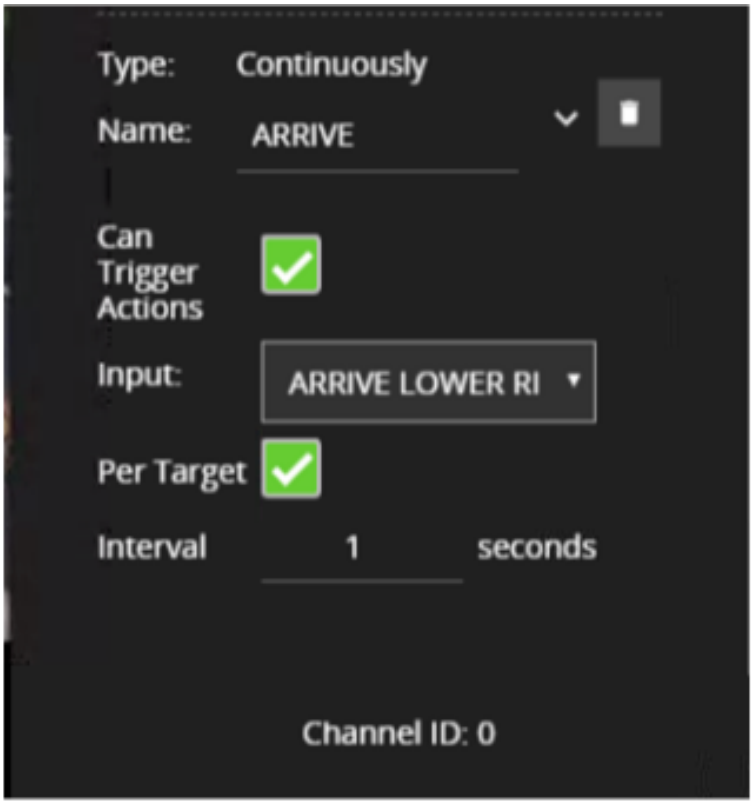
Betrachtet man eine Szene mit zwei Präsenzregeln, die mit zwei separaten Zonen verknüpft sind und durch eine UND-Regel verbunden sind, so erläutert die folgende Tabelle das Verhalten der Eigenschaft „Per Target“. Beachten Sie, dass sich „Objekt“ hier auf ein verfolgtes Objekt bezieht, wie es von der VCA-Tracking-Engine erkannt wird.

State (Zustand)	Per Target (Pro Ziel)	Outcome (Ergebnis)
Object A in Input A, Object B in input B	On	Es wurden zwei Ereignisse generiert, eines für jedes Objekt
Object A in Input A, Object B in input B	Off	Es wurde nur ein Ereignis generiert

Zudem ist zu beachten, dass die Regel, wenn sie bei deaktiviertem „Per Target“ ausgelöst wird, erst dann erneut ausgelöst wird, wenn sie „zurückgesetzt“ wird, d. h. wenn die AND-Bedingung nicht mehr erfüllt ist.

8.9.7.17.3 Continuously

Ein logischer Operator löst Ereignisse aus, wenn seine Eingabe über einen vom Benutzer festgelegten Zeitraum hinweg ununterbrochen vorliegt.



Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Continuously #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Per Target (Pro Ziel)	Pro erfasstem Objekt wird ein Ereignis ausgelöst. Weitere Informationen finden Sie in der folgenden Beschreibung	Active
Interval (Intervall)	Die Zeit in Millisekunden	1000 ms

Betrachtet man eine Szene mit einer Zone, einer dieser Zone zugeordneten Anwesenheitsregel und einer an diese Anwesenheitsregel angehängten „Continuously“-Regel, so generiert die Regel bei aktivierter Eigenschaft „Per Target“ für jedes verfolgte Objekt, das sich kontinuierlich in der Zone aufhält, ein Ereignis.

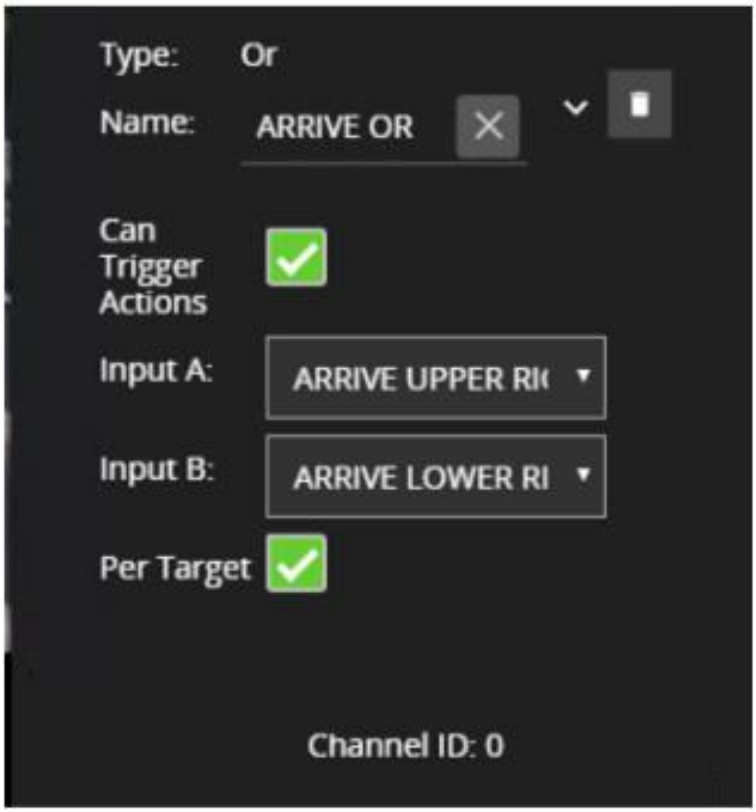
Ist diese Eigenschaft deaktiviert, wird von der Regel nur ein einziges Ereignis generiert, selbst wenn sich mehrere verfolgte Objekte in der Zone befinden.
Wenn „Per Target“ deaktiviert ist, generiert die Regel zudem nur dann Ereignisse, wenn eine Zustandsänderung vorliegt – d. h. wenn sich die Regelbedingung von „wahr“ auf „falsch“ oder umgekehrt ändert.

8.9.7.17.3.1 Wenn „Per Target“ deaktiviert ist, ändert sich der Status, wenn:

1. Eine beliebige Anzahl von Objekten betritt den betreffenden Bereich und verbleibt dort
2. Alle Objekte verlassen den betreffenden Bereich

8.9.7.17.4 Or

Ein logischer Operator, der zwei Regeln miteinander verknüpft und Ereignisse auslöst, wenn eine der beiden Eingaben wahr ist.



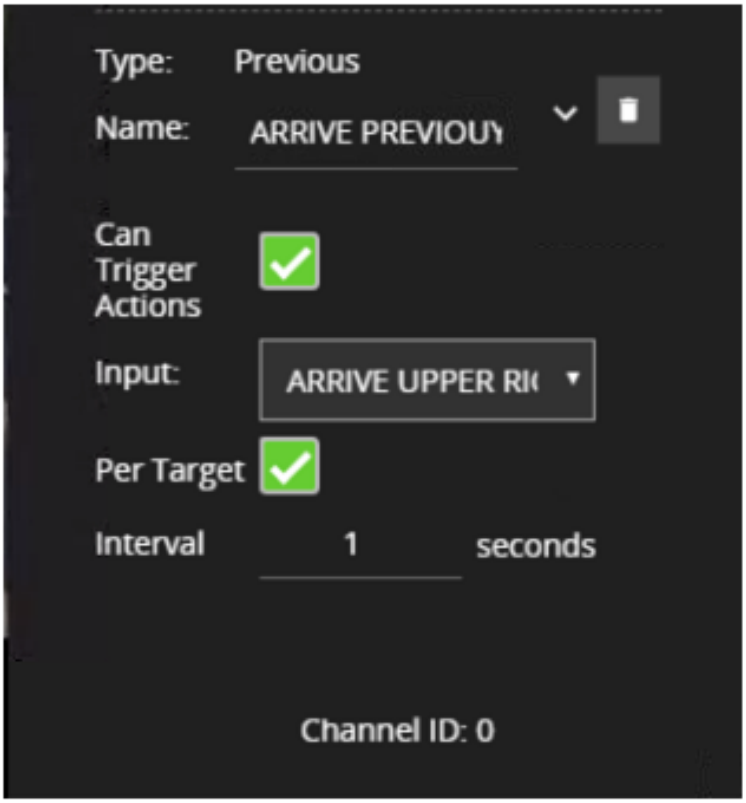
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Or #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input A (Eingabe A)	Die erste Eingabe	None
Input B (Eingabe B)	Die zweite Eingabe	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active

Betrachtet man eine Szene mit zwei Präsenzregeln, die mit zwei separaten Zonen verknüpft sind und durch eine ODER-Regel verbunden sind, so erläutert die folgende Tabelle das Verhalten der Eigenschaft „Pro Ziel“.

State (Zustand)	Per Target (Pro Ziel)	Outcome (Ergebnis)
Object A in Input A, No object in input B	On	Es wurden zwei Ereignisse generiert, eines für jedes Objekt
No object in Input A, Object B in input B	On	Es wurde nur ein Ereignis generiert (für Objekt B)
Object A in Input A, No object in input B	On	Es wurde nur ein Ereignis generiert (für Objekt A)
Object A in Input A, No object in input B	Off	Es wurde nur ein Ereignis generiert
No object in Input A, Object B in input B	Off	Es wurde nur ein Ereignis generiert
Object A in Input A, No object in input B	Off	Es wurde nur ein Ereignis generiert

8.9.7.17.5 Previous

Ein logischer Operator wird bei Eingangsereignissen ausgelöst, die zu einem bestimmten Zeitpunkt innerhalb eines vergangenen Zeitfensters aktiv waren.
Dieses Fenster wird durch den Zeitraum zwischen dem aktuellen Zeitpunkt und dem Zeitraum vor dem aktuellen Zeitpunkt (der durch den Wert des Intervallparameters festgelegt wird) definiert.



Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Previous #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Per Target (Pro Ziel)	Pro erfasstem Objekt wird ein Ereignis ausgelöst. Weitere Informationen finden Sie in der folgenden Beschreibung	Active
Interval (Intervall)	Die Zeit in Millisekunden	1000 ms

8.9.7.18 VCA - Zähler

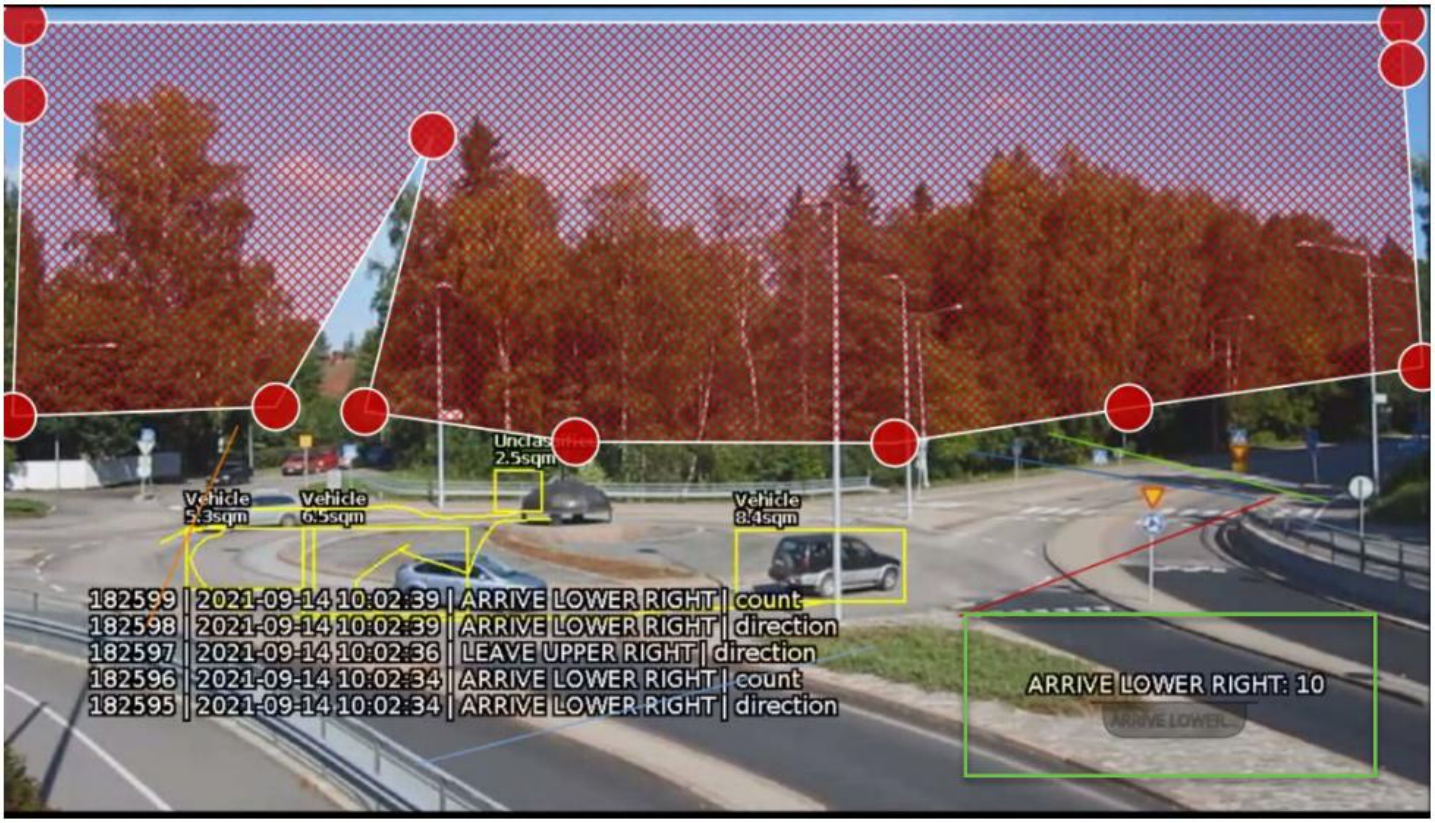
Diese Zähler sind nur in der VCA-Konfiguration sichtbar. Informationen zur Verwendung der Zähler im Spotter finden Sie im Spotter-Handbuch.
Die Zähler können so konfiguriert werden, dass sie zählen, wie oft eine Regel ausgelöst wird, beispielsweise die Anzahl der Personen, die eine Linie überqueren.

Die Zählerregel ist für zwei Anwendungsarten ausgelegt:

- Increment/Decrement: (Inkrementieren/Dekrementieren): Hierbei wird ein Zähler durch die angehängten Regeln erhöht (+1 pro Regelauslösung) und durch andere angehängte Regeln verringert (-1 pro Regelauslösung).
- Occupancy (Belegung): Hierbei gibt der Zähler die Anzahl der Objekte wieder, die derzeit die angehängten Regeln auslösen.

Jedem der drei Eingänge eines Zählers können mehrere Regeln zugewiesen werden.
Dadurch kann beispielsweise die Belegung von zwei Anwesenheitsregeln in einem einzigen Zähler oder die Aktivitäten mehrerer Ein- und Ausgangstüren in einem einzigen Zähler erfasst werden. Zur Veranschaulichung ist unten ein Beispiel für ein Regeldiagramm aufgeführt.
Grundsätzlich sollte ein einzelner Zähler nicht sowohl für die Belegungserfassung als auch für die Inkrementierung/Dekrementierung verwendet werden.

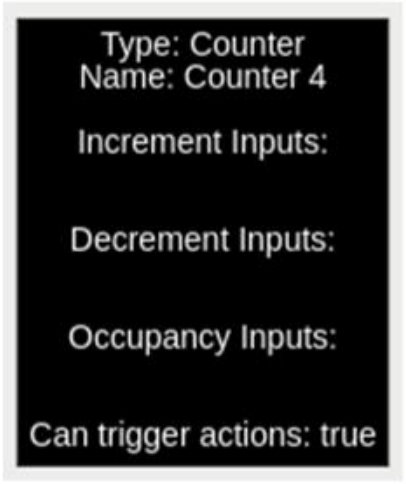
Hinweis: Von einem Zähler erzeugte Ereignisse lösen den Deep-Learning-Filter nicht aus, selbst wenn dieser auf dem Kanal aktiviert ist.

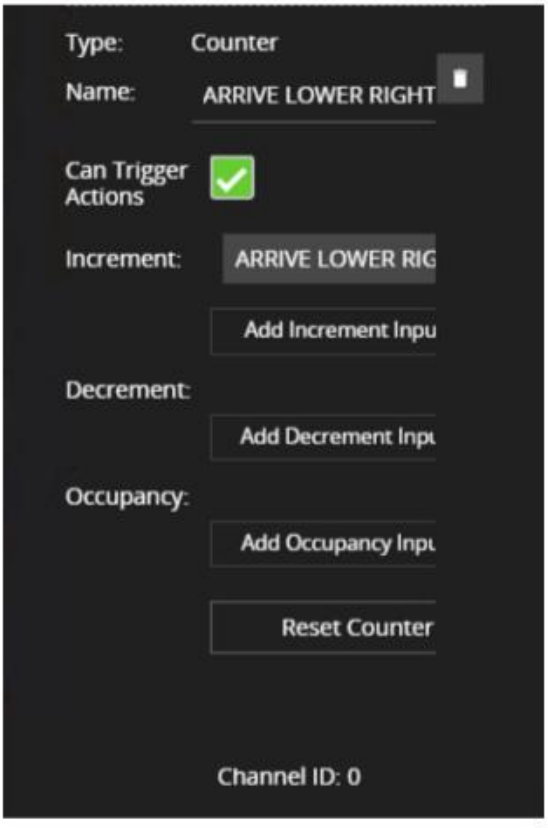


8.9.7.18.1 Zähler positionieren

Nach dem Hinzufügen wird ein Zählerobjekt im Videostream wie unten dargestellt angezeigt.
Der Zähler kann neu positioniert werden, indem man den „Griff“ unterhalb des Zählernamens anklickt und den Zähler an die gewünschte Stelle verschiebt.


Counter 0: 144
handle


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

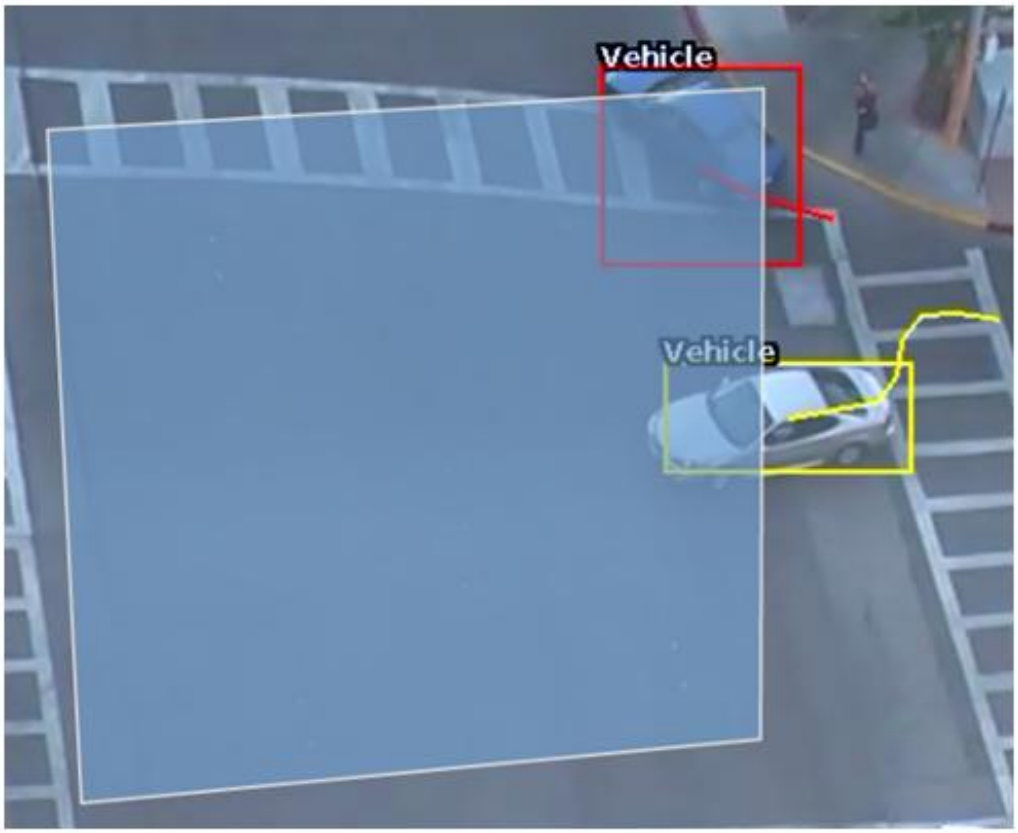

Type: Counter
Name: ARRIVE LOWER RIGHT
Can Trigger Actions
Increment:
ARRIVE LOWER RIG
Add Increment Inpu
Decrement:
Add Decrement Inpu
Occupancy:
Add Occupancy Inpu
Reset Counter
Channel ID: 0

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Counter #"
Increment (Inkrement)	Die Regel, die bei ihrer Auslösung den Zähler um eins erhöht	None
Decrement (Verringerung)	The rule which, when triggered, will subtract one from the counter	None
Occupancy (Auslastung)	Setzt den Zähler auf die aktuelle Anzahl der aktiven Auslöser der Regel*	None
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Reset Counter (Zähler zurücksetzen)	Eine Schaltfläche, mit der der Zählerstand auf 0 zurückgesetzt werden kann	None

- Wenn beispielsweise eine Anwesenheitsregel als Belegungsziel festgelegt ist und diese Anwesenheitsregel derzeit von zwei Objekten ausgelöst wird, zeigt der Zähler den Wert „2“ an.

8.9.7.19 VCA- Objektspuren

Die Spur zeigt den Verlauf des Objekts an.
Je nach Kalibrierung kann die Spur vom Schwerpunkt oder vom unteren Mittelpunkt des Objekts ausgehend gezeichnet werden.
(Weitere Informationen finden Sie unter „Erweiterte Einstellungen“).
Die Spur ist entscheidend dafür, wie eine Regel ausgelöst wird.
Der Schnittpunkt des Spurpunkts mit einer Zone oder Linie bestimmt, ob eine Regel ausgelöst wird oder nicht.
Das folgende Bild veranschaulicht diesen Punkt: Die Spur des blauen Fahrzeugs schneidet die Erkennungszone und wird rot dargestellt.
Umgekehrt schneidet das weiße Fahrzeug zwar die Erkennungszone, seine Spur jedoch (noch) nicht; daher hat es die Regel nicht ausgelöst und wird gelb dargestellt.



8.9.7.20 VCA - Objektanzeige

Sobald Regeln konfiguriert sind, werden sie in Echtzeit auf den Kanal angewendet, sodass ein Feedback über ihre Funktionsweise möglich ist.
Objekte, die eine Regel ausgelöst haben, werden mit einem Begrenzungsrahmen und einer Spur gekennzeichnet. Objekte können in zwei Zuständen dargestellt werden:

1. **Nicht alarmiert**: Standardmäßig gelb dargestellt. Ein erkanntes Objekt, das keine Kriterien erfüllt, löst keine Regel aus und löst kein Ereignis aus.
2. **Alarmiert**: Standardmäßig rot dargestellt. Ein erkanntes Objekt, das eine oder mehrere Regeln ausgelöst hat. Löst ein Ereignis aus.

Wie unten zu sehen ist, werden bei Auslösung eines Ereignisses in den Standardeinstellungen Details zum Ereignis in der unteren Hälfte des Videostreams angezeigt.
Objektklassen-Markierungen werden in diesem Beispiel generiert durch

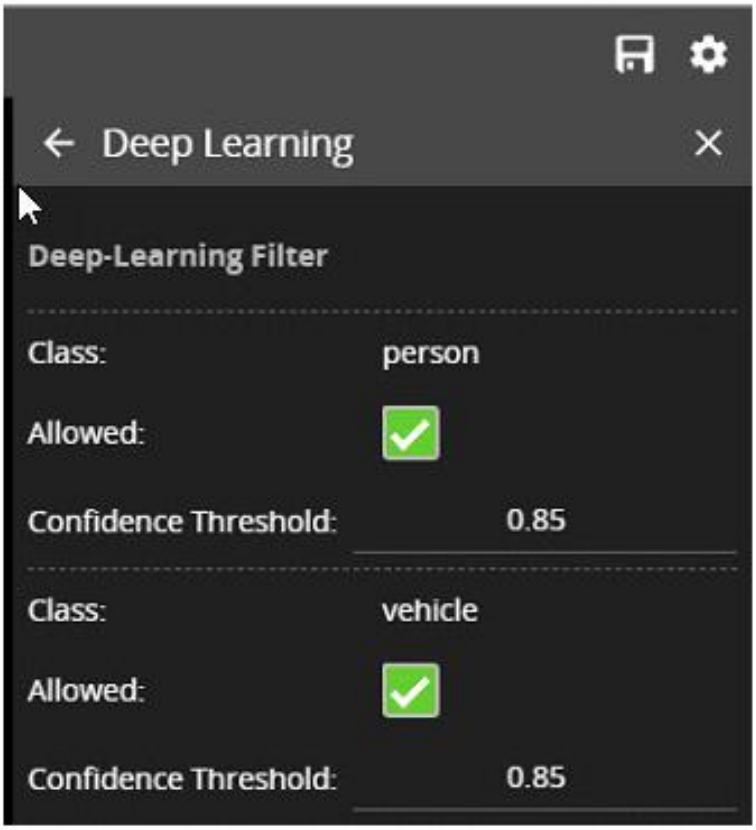


8.9.8 VCA - Deep-Learning-Filter

VCAserver unterstützt auch die Klassifizierung mithilfe des Deep-Learning-Filters. In diesem Fall kann ein Objekt, das eine Regel ausgelöst hat, mithilfe des Deep-Learning-Filters analysiert werden, woraufhin eine vorhergesagte Klasse und ein Konfidenzniveau zurückgegeben werden. Die verfügbaren Objektklassen werden durch das Modell definiert.

Auf VCAserver kann der Deep-Learning-Filter GPU-Beschleunigung nutzen; siehe **Deep-Learning-Anforderungen** für die Hardwareanforderungen.

Ohne GPU-Beschleunigung nutzt der Deep-Learning-Filter die CPU. Die Aktivierung des Deep-Learning-Filters auf mehreren Kanälen, die ein hohes Ereignisvolumen generieren (mehr als 1 pro Sekunde), kann zu einer schlechten Systemleistung führen und wird daher nicht empfohlen.



Jede der möglichen Objektklassen verfügt über zusätzliche Parameter:

Zulässig: Gibt an, ob dieser Objekttyp den Filter passieren darf. Ist diese Option deaktiviert, lösen Objekte, die diesem Typ zugeordnet werden, keine Aktionen aus.

Vertrauensschwelle: Ein Wert (0,0 – 1,0), der das für die Klassifizierung erforderliche Mindestvertrauensniveau angibt. Objekte mit einem Klassifizierungswert unterhalb dieses Mindestwerts werden herausgefiltert und lösen keine Aktionen aus.

8.10 VCA - Filter

Ein Filter kann keine Aktion eigenständig auslösen, da er zur Auslösung eine weitere Basiseingabe, einen Filter oder eine Bedingungsregel benötigt.

- VCA-Filter – Geschwindigkeitsfilter
- VCA-Filter – Objektfilter
- VCA-Filter – Farbfilter
- VCA-Filter – Retrigger-Filter

- VCA-Filter – Deep-Learning-Filter

8.10.1 Geschwindigkeitsfilter

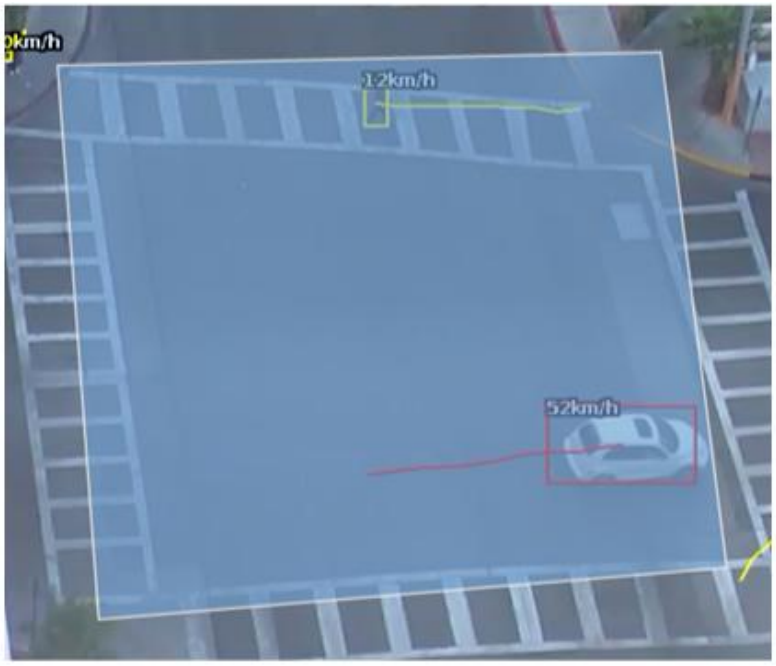
Mit dem Geschwindigkeitsfilter lässt sich überprüfen, ob sich die Geschwindigkeit eines Objekts, das einen Eingang ausgelöst hat, innerhalb des durch eine Unter- und Obergrenze definierten Geschwindigkeitsbereichs bewegt.

> Der Kanal muss kalibriert werden, damit der Geschwindigkeitsfilter verfügbar ist.

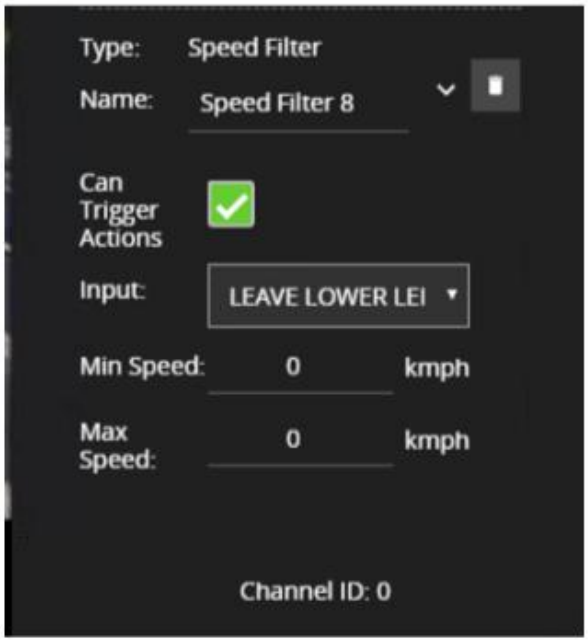
Häufig wird diese Regel mit einer Anwesenheitsregel kombiniert; zur Veranschaulichung ist unten ein Beispiel für einen Regelgraphen dargestellt.

Die folgende Abbildung zeigt, wie eine solche Regelkombination bei einem Auto ausgelöst wird, das sich mit 52 km/h bewegt, während eine Person, die sich mit 12 km/h bewegt, außerhalb des konfigurierten Bereichs (25–100 km/h) liegt und die Regel daher nicht auslöst.

MIRASYS



Type: Speed
Name: Speed 3
Min Speed: 50
Max Speed: 200
Can trigger actions: true

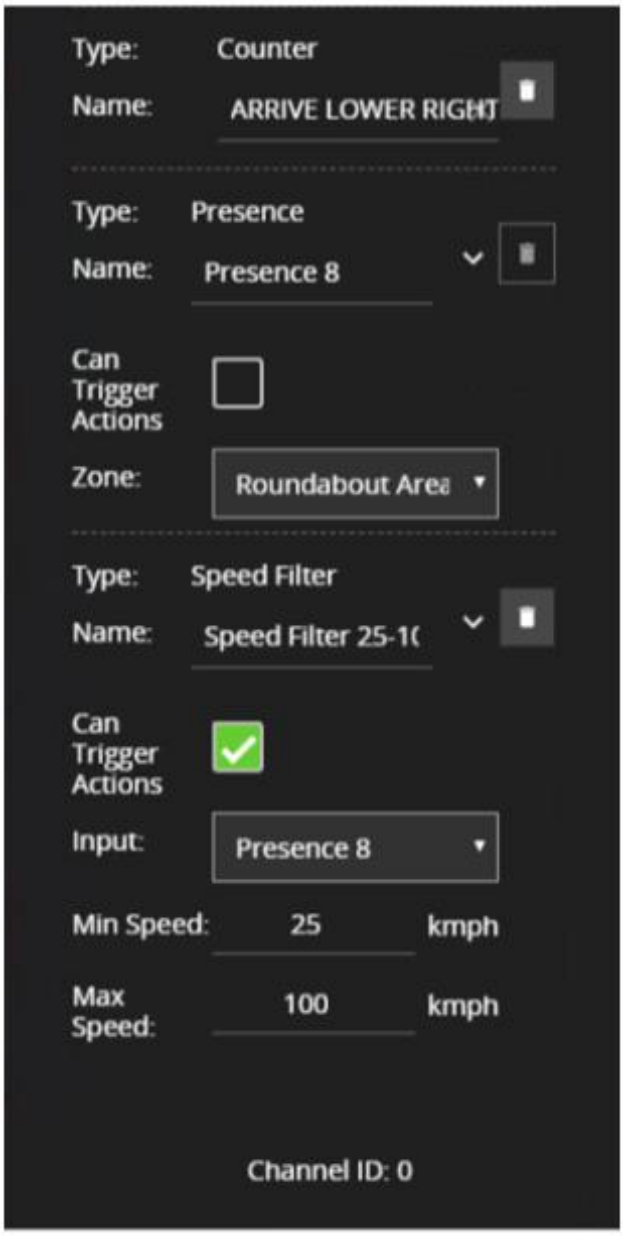


Tel +358 (0)9 2533 3300 Email info@mirasys.com https://www.mirasys.com

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Speed #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Min Speed (Mindestgeschwindigkeit)	Die Mindestgeschwindigkeit (km/h), mit der sich ein Objekt bewegen muss, damit die Regel ausgelöst wird	0
Max Speed (Höchstgeschwindigkeit)	Die Höchstgeschwindigkeit (km/h), bei der ein Objekt die Regel auslöst	0

8.10.1.1 Typische Kombination logischer Regeln

Die folgende logische Regel prüft, ob ein Objekt, das die der Zone „Centre“ zugeordnete Anwesenheitsregel auslöst, gleichzeitig mit einer Geschwindigkeit zwischen 25 und 100 km/h fährt, wie in der Geschwindigkeitsregel „Speed Filter 25-100 km/h“ festgelegt.
Nur der Geschwindigkeitsfilter ist auf „Kann Aktionen auslösen“ gesetzt, was bedeutet, dass nur dieser Bestandteil der logischen Regel als Quelle für Aktionen zur Verfügung steht. Darüber hinaus hat jede vom Geschwindigkeitsfilter generierte Aktivität den Ereignistyp „Anwesenheit“.



8.10.2 VCA-Filter – Objektfilter

Der Objektklassifizierungsfilter ermöglicht es, Objekte herauszufiltern, die eine Regel auslösen, wenn sie nicht einer bestimmten Klasse zugeordnet sind (z. B. Person, Fahrzeug).

Der Objektklassifizierungsfilter muss mit einer oder mehreren anderen Regeln kombiniert werden, um zu verhindern, dass unerwünschte Objekte einen Alarm auslösen. Zur Veranschaulichung ist unten ein Beispiel für ein Regeldiagramm aufgeführt.

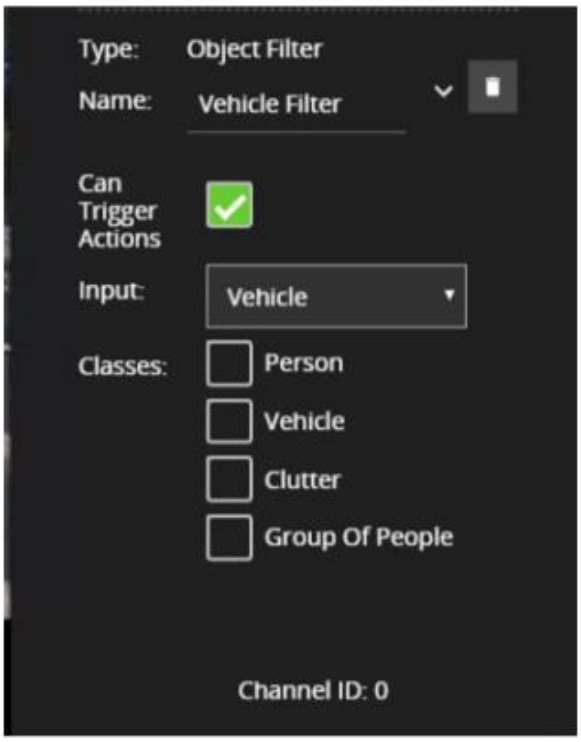


Das vorherige Bild veranschaulicht, wie der mit der Klasse „Fahrzeug“ konfigurierte Objektklassifizierungsfilter ausschließlich Fahrzeugobjekte einbezieht.

Die Person in diesem Bereich wird herausgefiltert, da die Klasse „Person“ in der Filterliste nicht ausgewählt ist.

Der Kanal muss kalibriert werden, damit der Objektklassifizierungsfilter verfügbar ist.





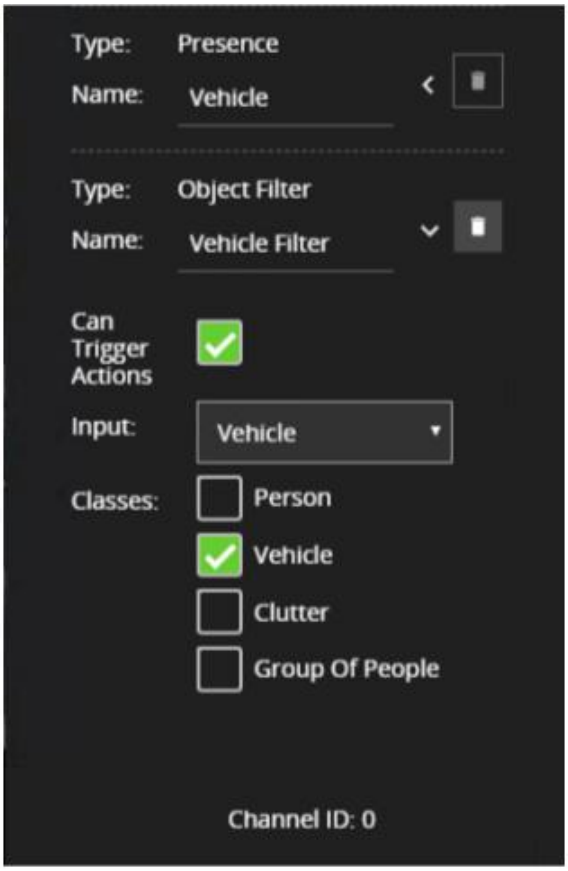
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Object Filter #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Classes (Klassen)	Die Objektklassen, die einen Alarm auslösen dürfen	None

8.10.2.1 Typische Kombination logischer Regeln

Die folgende logische Regel prüft, ob das Objekt, das die der Zone „Centre“ zugeordnete Anwesenheitsregel auslöst, auch als „Fahrzeug“ klassifiziert ist, wie im Objektfilter „Fahrzeugfilter“ festgelegt.

Nur der Objektfilter ist auf „Kann Aktionen auslösen“ gesetzt, was bedeutet, dass nur dieser Bestandteil der logischen Regel als Quelle für Aktionen zur Verfügung steht.

Zudem hat jede vom Geschwindigkeitsfilter generierte Aktivität den Ereignistyp „Anwesenheit“.



8.10.3 VCA-Filter – Farbfilter

Der Farbfilter nutzt den „Colour Signature“-Algorithmus und ermöglicht es, Objekte danach herauszufiltern, ob sie eine bestimmte Farbkomponente enthalten.

Der „Colour Signature“-Algorithmus ist dafür zuständig, jedes Pixel eines erkannten Objekts einer von 10 Farbklassen zuzuordnen.

Mit dem Farbfilter können Sie eine oder mehrere dieser Farbklassen auswählen; der Filter wird ausgelöst, wenn das Zielobjekt aus einer oder mehreren der ausgewählten Farben besteht.

Das folgende Bild zeigt ein Beispiel für ein verfolgtes Objekt, bei dem die Anmerkungen zur Farbsignatur aktiviert sind.
Hier werden die vier Farben, die mehr als 5 % des Objekts ausmachen, durch das am Objekt angeheftete Farbfeld dargestellt.

In diesem Fall wird eine Person in der Szene verfolgt, die hochsichtbare Sicherheitskleidung trägt. Der Farbfilter ist so eingestellt, dass er bei Gelb ausgelöst wird, wodurch die Person erkannt, der Schatten jedoch ignoriert wird.

In der Regel wird der Farbklassifizierungsfilter mit einer oder mehreren weiteren Regeln kombiniert, um zu verhindern, dass unerwünschte Objekte einen Alarm auslösen. Zur Veranschaulichung ist unten ein Beispiel für ein Regeldiagramm dargestellt.



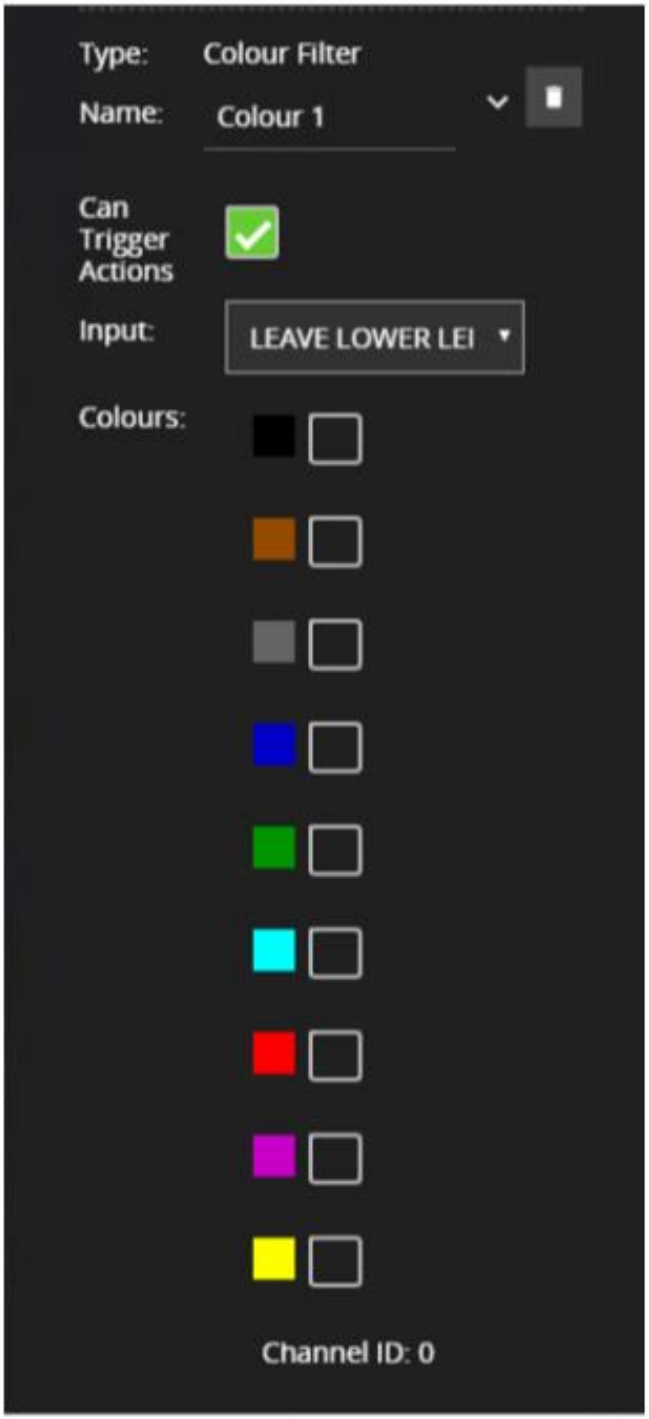
Das vorherige Bild veranschaulicht, wie der mit der Klasse „Fahrzeug“ konfigurierte Objektklassifizierungsfilter ausschließlich Fahrzeugobjekte einbezieht.

Die Person in diesem Bereich wird herausgefiltert, da die Klasse „Person“ in der Filterliste nicht ausgewählt ist.

Damit der Farbfilter funktioniert, muss die Farbsignatur für den Kanal aktiviert sein.

MIRASYS

Type: Colour Filter
Name: Colour Filter 1
Can trigger actions: true



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

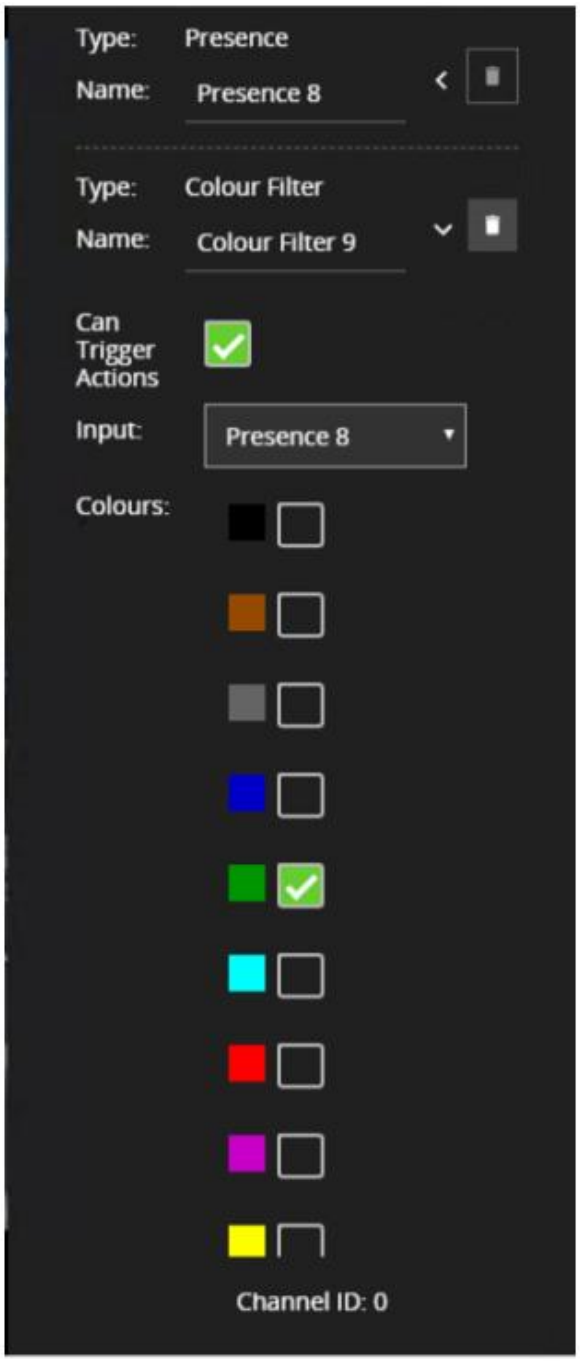
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Object Filter #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Colours (Farben)	Die Farben, die einen Alarm auslösen dürfen	All Unchecked

8.10.3.1 Typische Kombination logischer Regeln

Die folgende logische Regel prüft, ob das Objekt, das die Anwesenheitsregel „Zuglinie an Zone ‚Centre' angebunden" auslöst, auch die Farbe „Grün" als eine der vier prozentual am häufigsten vorkommenden Farben enthält.

Nur der Farbfilter ist auf „Kann Aktionen auslösen" gesetzt, was bedeutet, dass nur dieser Bestandteil der logischen Regel als Quelle für Aktionen zur Verfügung steht.

Zudem hat jede vom Geschwindigkeitsfilter generierte Aktivität den Ereignistyp „Anwesenheit".

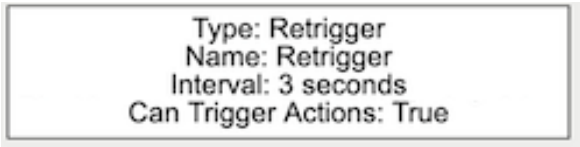


8.10.4 VCA-Filter – Retrigger-Filter

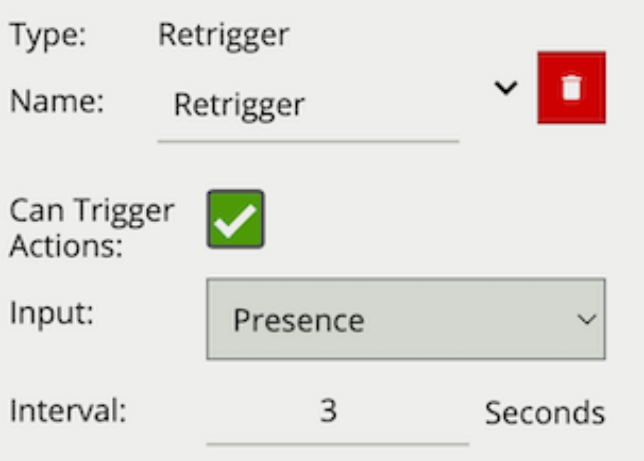
Der Retrigger-Filter fungiert als Ereignisdurchlass, der nur dann ein Ereignis generiert, wenn der Eingang innerhalb des festgelegten Zeitraums zuvor noch nicht ausgelöst wurde.

In der Regel wird der Retrigger-Filter am Ende einer Regelkombination angewendet, um zu verhindern, dass doppelte Alarme gesendet werden. Dies ermöglicht eine feinere Steuerung als die Option „Event Retrigger Time“. Ereignisse, die vom Retrigger-Filter erzeugt werden, haben denselben Ereignistyp wie die Eingangsregel.

8.10.4.1 Grafische Ansicht



8.10.4.2 Formularansicht



8.10.4.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Retrigger #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Interval (Intervall)	Zeitraum, in dem das eingehende Ereignis kein weiteres Ereignis auslösen kann	3

8.10.5 VCA-Filter – Deep-Learning-Filter

Der Deep-Learning-Filter ermöglicht es, Objekte herauszufiltern, die eine Regel auslösen, wenn sie vom Deep-Learning-Modell nicht einer bestimmten Klasse zugeordnet werden. Die verfügbaren Objektklassen werden durch das Modell definiert.

Die Einstellungen für den Deep-Learning-Filter werden auf der Seite „Deep Learning“ konfiguriert.

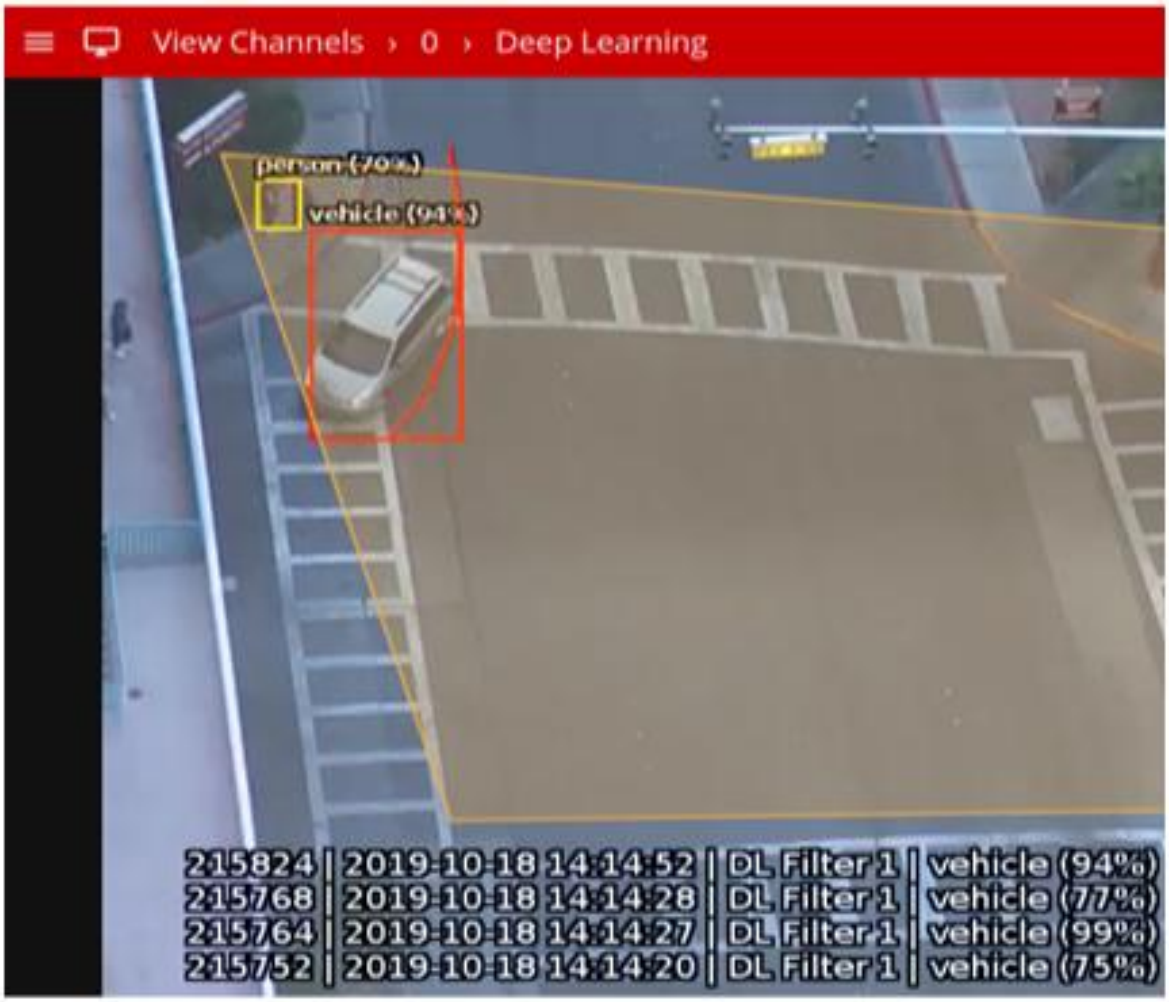
Auf VCAserver kann der Deep-Learning-Filter GPU-Beschleunigung nutzen; siehe Deep-Learning-Anforderungen für die Hardwareanforderungen.

Ohne GPU-Beschleunigung nutzt der Deep-Learning-Filter die CPU. Die Aktivierung des Deep-Learning-Filters auf mehreren Kanälen, die ein hohes Ereignisvolumen generieren (mehr als 1 pro Sekunde), **kann zu einer schlechten Systemleistung führen und wird daher nicht empfohlen.**

8.10.5.1 Regelkombinationen und Objektklassenparameter

In der Regel wird der Deep-Learning-Filter mit einer oder mehreren anderen Regeln kombiniert, um zu verhindern, dass unerwünschte Objekte einen Alarm auslösen. Zur Veranschaulichung finden Sie unten ein Beispiel für ein Regeldiagramm. Bitte beachten Sie, dass der Deep-Learning-Filter nicht als Eingabe für andere Regeltypen verwendet werden kann. Daher muss er die letzte Regel in einem Diagramm sein.

MIRASYS





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

Jede der möglichen Objektklassen verfügt über zusätzliche Parameter:

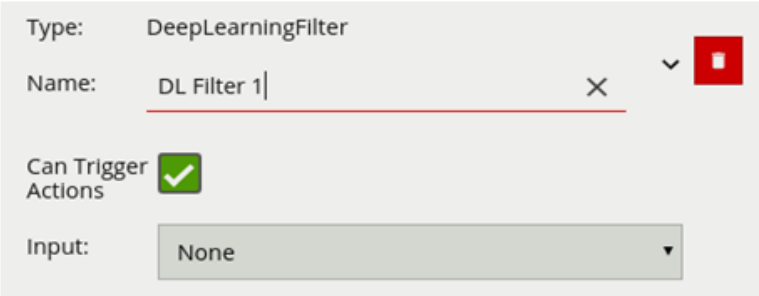
Zulässig: Gibt an, ob dieser Objekttyp den Filter passieren darf. Ist diese Option deaktiviert, lösen Objekte, die diesem Typ zugeordnet werden, keine Aktionen aus.

Vertrauensschwelle: Ein Wert (0,0 – 1,0), der das für die Klassifizierung erforderliche Mindestvertrauensniveau angibt. Objekte mit einem Klassifizierungswert unterhalb dieses Mindestwerts werden herausgefiltert und lösen keine Aktionen aus.

Das vorherige Bild veranschaulicht, wie der Deep-Learning-Filter, der nur auf die Fahrzeugklasse (Vertrauensschwelle 0,5) konfiguriert ist, ausschließlich auf das Fahrzeugobjekt reagiert.

Die Person in diesem Bereich wird herausgefiltert, da die Einstellung „Personenklasse zulässig“ auf der Deep-Learning-Konfigurationsseite nicht aktiviert ist.



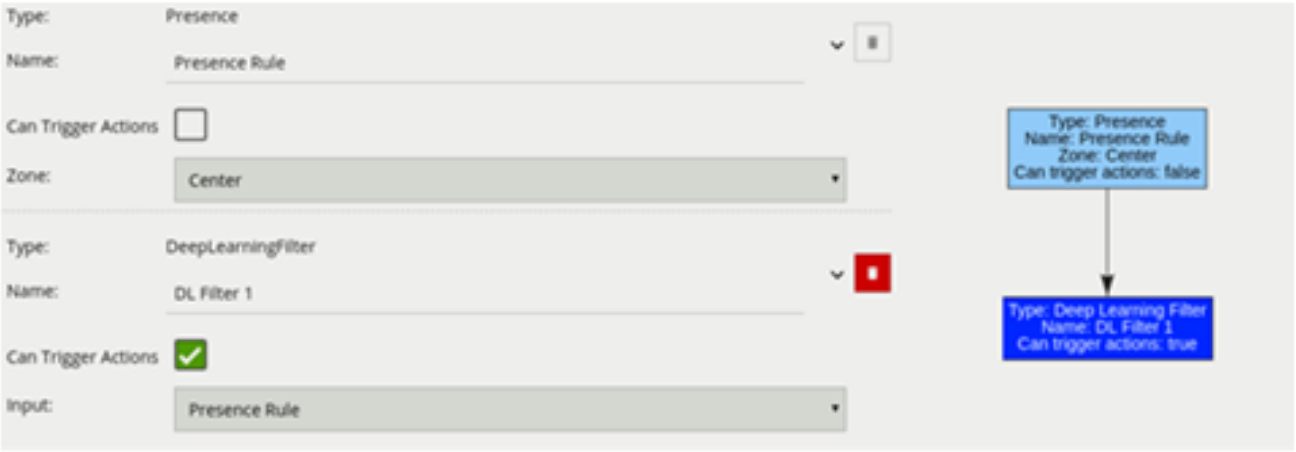


Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"DL Filter #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None

8.10.5.2 Typische Kombination logischer Regeln

Die folgende logische Regel prüft, ob das Objekt, das die der Zone „Centre“ zugewiesene Anwesenheitsregel auslöst, zu einer der relevanten Klassen gehört, die auf der Einstellungsseite für Deep Learning definiert sind (siehe Abbildung der Einstellungsseite oben).
Nur der Deep-Learning-Filter ist auf „Kann Aktionen auslösen“ gesetzt, was bedeutet, dass nur dieser Bestandteil der logischen Regel als Quelle für Aktionen zur Verfügung steht.

Zudem erhält jede vom Geschwindigkeitsfilter generierte Aktivität den Ereignistyp „Anwesenheit“.



8.11 Arten von bedingten Regeln

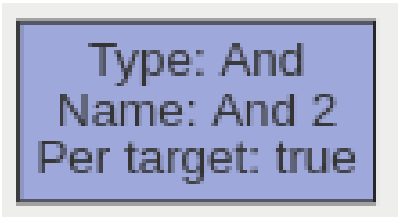
Die derzeit unterstützten bedingten Regeln sowie eine detaillierte Beschreibung der einzelnen Regeln.

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

8.11.1 VCA - And

Ein logischer Operator, der zwei Regeln miteinander verknüpft und nur dann Ereignisse auslöst, wenn beide Eingaben wahr sind.

8.11.1.1 Grafische Ansicht



8.11.1.2 Formularansicht



8.11.1.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"And #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input A (Eingabe A)	Die erste Eingabe	None
Input B (Eingabe B)	Die zweite Eingabe	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active

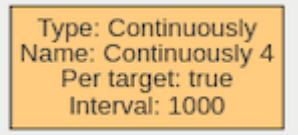
Betrachtet man eine Szene mit zwei Präsenzregeln, die mit zwei separaten Zonen verknüpft sind und durch eine AND-Regel verbunden sind, so erläutert die folgende Tabelle das Verhalten der Eigenschaft „Per Target“. Beachten Sie, dass sich „Objekt“ hier auf ein verfolgtes Objekt bezieht, wie es von der VCA-Tracking-Engine erkannt wird.

State (Zustand)	Per Target (Pro Ziel)	Outcome (Ergebnis)
Object A in Input A, Object B in input B	On	Es wurden zwei Ereignisse generiert, eines für jedes Objekt
Object A in Input A, Object B in input B	Off	Es wurde nur ein Ereignis generiert

8.11.2 VCA - Continuously

Ein logischer Operator, der Ereignisse auslöst, wenn sein Eingangssignal über einen vom Benutzer festgelegten Zeitraum hinweg ununterbrochen anliegt.

8.11.2.1 Grafische Ansicht



8.11.2.2 Formularansicht



8.11.2.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Continuously #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active
Interval (Intervall)	Die Zeit in Millisekunden	1

Betrachtet man eine Szene mit einer Präsenzregel, die einer Zone zugeordnet ist, und einer daran angehängten „Kontinuierlich"-Regel: Wenn die Eigenschaft **Per Target** aktiviert ist, generiert die Regel für jedes verfolgte Objekt, das sich kontinuierlich in der Zone aufhält, ein Ereignis. Ist sie deaktiviert, wird von der Regel nur ein einziges Ereignis generiert, selbst wenn sich mehrere verfolgte Objekte in der Zone befinden. Wenn **Per Target** deaktiviert ist, generiert die Regel zudem nur dann Ereignisse, wenn sich der Status ändert, d. h. wenn sich die Regelbedingung von „wahr" auf „falsch" oder umgekehrt ändert. Wenn **Per Targe**t deaktiviert ist, ändert sich der Status, wenn:

- beliebig viele Objekte die betreffende Zone betreten und in der Zone verbleiben
- **alle** Objekte die betreffende Zone verlassen

8.11.3 VCA - Counter

Zähler können so konfiguriert werden, dass sie zählen, wie oft eine Regel ausgelöst wird. Zum Beispiel die Anzahl der Personen, die eine Linie überqueren. Die Zählerregel ist für zwei Anwendungsarten ausgelegt:

- **Increment/Decrement** (Inkrementieren/Dekrementieren): Dabei wird ein Zähler durch die zugewiesene(n) Regel(n) erhöht (+1 bei jeder Regelauslösung) und durch eine andere zugewiesene Regel (-1 bei jeder Regelauslösung) verringert.
- **Occupancy** (Belegung): Hierbei gibt der Zähler die Anzahl der Objekte wieder, die derzeit die angehängte(n) Regel(n) auslösen.

edem der drei Eingänge eines Zählers können mehrere Regeln zugewiesen werden. So kann beispielsweise die Belegung zweier Anwesenheitsregeln in einem einzigen Zähler erfasst werden oder die Aktivitäten mehrerer Ein- und Ausgangstüren in einem einzigen Zähler. Zur Veranschaulichung ist unten ein Beispiel für ein Regeldiagramm dargestellt.

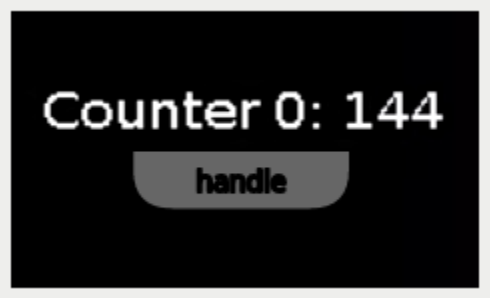
Generell sollte ein einzelner Zähler nicht sowohl für die Belegungserfassung als auch für die Inkrementierung/Dekrementierung verwendet werden.

Der Schwellenwertoperator des Zählers ermöglicht es dem Benutzer, zu begrenzen, wann ein Zähler ein Ereignis generiert. Basierend auf dem ausgewählten Verhalten und einem definierten Schwellenwert kann der Zähler so konfiguriert werden, dass er nur in bestimmten Szenarien Ereignisse sendet. Zu den Schwellenwertoperatoren gehören:

- Greater than or equal to (Größer als oder gleich)
- Less than or equal to (Kleiner als oder gleich)
- Greater than (Größer als)
- Less than (Kleiner als)
- Equal to (Gleich)
- Not Equal to (Nicht gleich)
- None (Keine)

8.11.3.1 Positionszähler

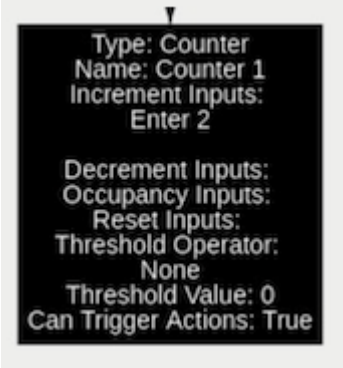
Nach dem Hinzufügen wird ein Zählerobjekt im Videostream wie unten dargestellt angezeigt. Der Zähler kann verschoben werden, indem man den „Griff“ unterhalb des Zählernamens anklickt und den Zähler an die gewünschte Stelle zieht.



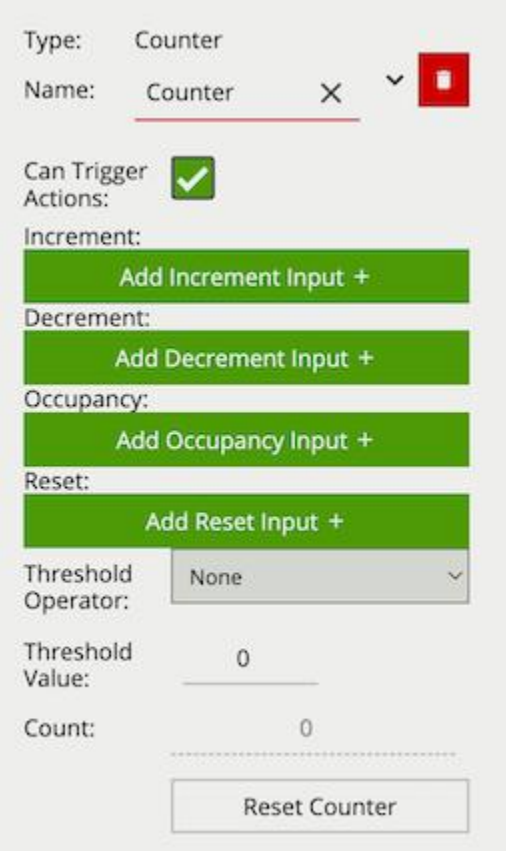
Ein Rechtsklick mit der Maus (oder ein Tippen und Halten auf einem Tablet) auf das Raster öffnet das Kontextmenü.



8.11.3.2 Grafische Ansicht



8.11.3.3 Formularansicht



8.11.3.4 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Counter #"
Increment (Inkrement)	Die Regel, die bei ihrer Auslösung den Zähler um eins erhöht	None
Decrement (Dekrementieren)	Die Regel, die bei ihrer Auslösung den Zählerstand um eins verringert	None
Occupancy (Auslastung)	Setzt den Zähler auf die aktuelle Anzahl der aktiven Auslöser der Regel	None
Reset (Zurücksetzen)	Setzt den `count` auf `0` zurück, wenn die zugewiesene(n) Regel(n) ausgelöst wird/werden	None
Threshold Operator (Schwellenwertoperator)	Legt fest, wann ein Zähler basierend auf dem Schwellenwert Ereignisse auslöst	None

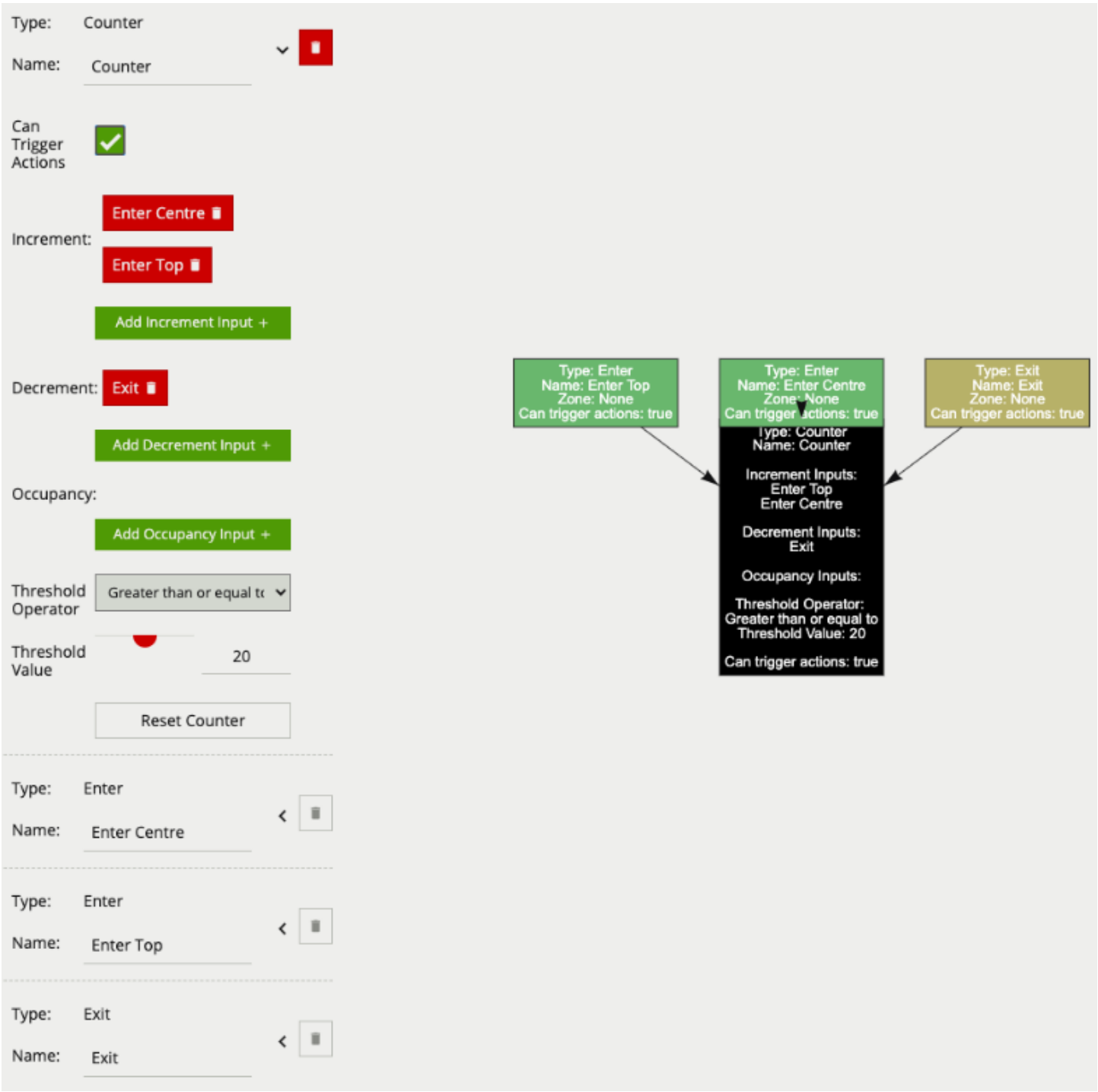
Merkmal	Beschreibung	Standardwert
Threshold Value (Schwellenwert)	Der Wert, den der Schwellenwertoperator zur Festlegung des Verhaltens verwendet	0
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Reset Counter (Zähler zurücksetzen)	Eine Schaltfläche, mit der der Zählerstand auf 0 zurückgesetzt werden kann	None

Wenn beispielsweise eine Anwesenheitsregel als Belegungsziel festgelegt ist und derzeit zwei Objekte diese Anwesenheitsregel auslösen, zeigt der Zähler den Wert 2 an.

8.11.3.5 Typische Kombination logischer Regeln

Das folgende Zählerbeispiel erhöht einen Zähler auf Grundlage von zwei Eintrittsregeln – **Enter Centre** und **Enter Top** –, die jeweils den Zonen **Centre** und **Top** zugeordnet sind. Das bedeutet, dass der Zähler um +1 erhöht wird, sobald eine dieser Eintrittsregeln ausgelöst wird. Der Zähler wird zudem auf Grundlage der Austrittsregel **Exit** verringert, die jedes Mal, wenn ein Objekt die Zone **Centre** verlässt, 1 vom Zähler abzieht. Der Schwellenwertoperator und der Schwellenwert begrenzen den Zähler so, dass er nur dann Ereignisse generiert, wenn der Zählerstand über 20 liegt.

Nur die Zählerregel **Counter** ist auf **Can Trigger Actions gesetzt**, was bedeutet, dass nur diese Komponente der logischen Regel als Quelle für Aktionen verfügbar ist. In diesem Fall löst eine Aktion, die diese Regel als Quelle verwendet, jedes Mal aus, wenn sich der Zählerstand ändert.



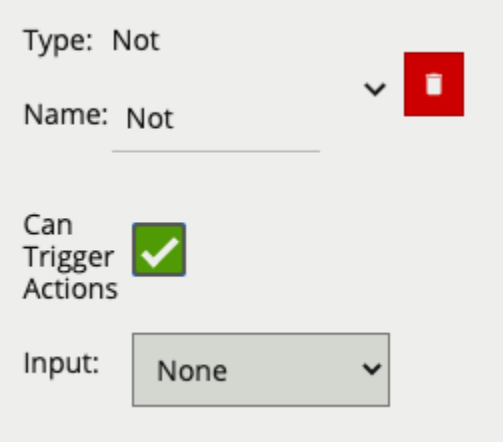
8.11.4 VCA - Not

Ein logischer Operator, der ein Ereignis auslöst, wenn die Eingaberegel falsch wird.

8.11.4.1 Grafische Ansicht



8.11.4.2 Formularansicht



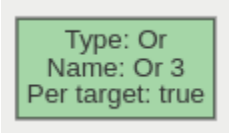
8.11.4.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Not #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Die Eingaberegel	None

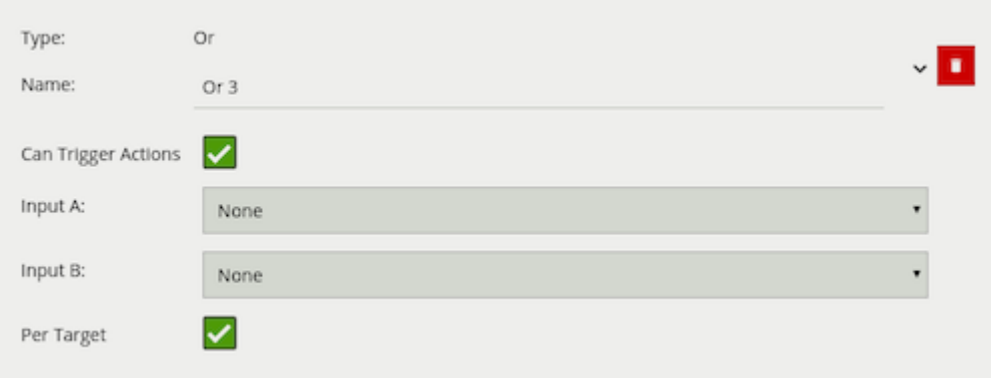
8.11.5 VCA - Or

Ein logischer Operator, der zwei Regeln miteinander verknüpft und Ereignisse auslöst, wenn eine der beiden Eingaben wahr ist.

8.11.5.1 Grafische Ansicht



8.11.5.2 Formularansicht



8.11.5.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Not #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input A (Eingabe A)	Die erste Eingabe	None
Input B (Eingabe B)	Die zweite Eingabe	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active

Betrachtet man eine Szene mit zwei Präsenzregeln, die mit zwei separaten Zonen verknüpft sind und durch eine ODER-Regel verbunden sind, so erläutert die folgende Tabelle das Verhalten der Eigenschaft **Per Target**.

State (Zustand)	Per Target (Pro Ziel)	Outcome (Ergebnis)
Object A in Input A, No object in input B	On	Es wurden zwei Ereignisse generiert, eines für jedes Objekt
No object in Input A, Object B in input B	On	Es wurde nur ein Ereignis generiert (für Objekt B)
Object A in Input A, No object in input B	On	Es wurde nur ein Ereignis generiert (für Objekt A)
Object A in Input A, No object in input B	Off	Es wurde nur ein Ereignis generiert
No object in Input A, Object B in input B	Off	Es wurde nur ein Ereignis generiert

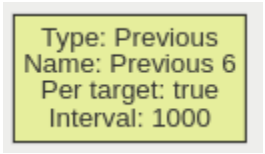
State (Zustand)	Per Target (Pro Ziel)	Outcome (Ergebnis)
Object A in Input A, No object in input B	Off	Es wurde nur ein Ereignis generiert

Zudem ist zu beachten, dass die Regel, wenn sie bei deaktiviertem **Per Target** ausgelöst wird, erst dann erneut ausgelöst wird, wenn sie „zurückgesetzt“ wird, d. h. wenn die ODER-Bedingung nicht mehr erfüllt ist.

8.11.6 VCA - Previous

Ein logischer Operator, der bei Eingangsereignissen ausgelöst wird, die zu einem bestimmten Zeitpunkt innerhalb eines vergangenen Zeitfensters aktiv waren. Dieses Fenster erstreckt sich von der aktuellen Zeit bis zu dem Zeitraum vor der aktuellen Zeit (der durch den Wert „Intervall“ festgelegt wird).

8.11.6.1 Grafische Ansicht



8.11.6.2 Formularansicht



8.11.6.3 Konfiguration

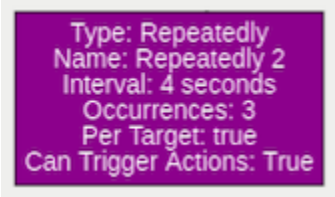
Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Previous #"
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Eingaberegel	None
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active
Interval (Intervall)	Die Zeit in Millisekunden	1

8.11.7 VCA - Repeatedly

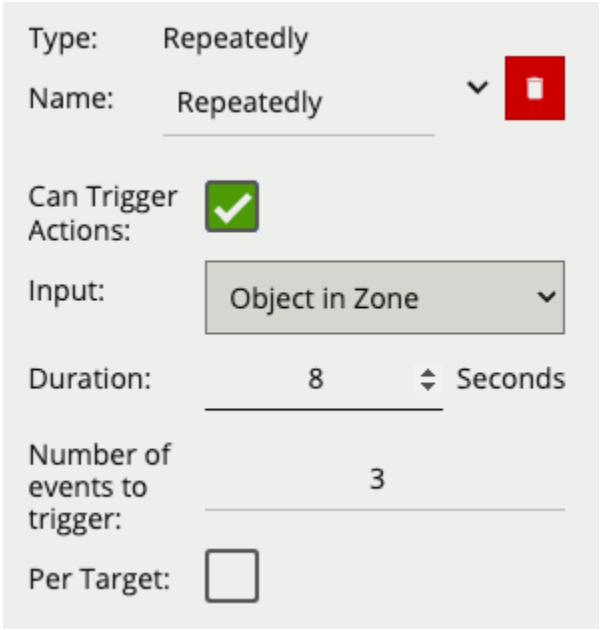
Ein logischer Operator, der ausgelöst wird, wenn eine Eingaberegel innerhalb eines definierten Zeitraums eine bestimmte Anzahl von Malen ausgelöst wird. Der Zeitraum wird als Zeitfenster berechnet, das von jedem Eingabeereignis ausgeht. Wenn beispielsweise eine „Repeatedly"-Regel so konfiguriert ist, dass sie ein Ereignis generiert, wenn die Eingaberegel innerhalb von acht Sekunden dreimal ausgelöst wird, und diese Eingaberegel innerhalb von acht Sekunden viermal ausgelöst wird, wird die „Repeatedly"-Regel sowohl nach dem dritten als auch nach dem vierten Auslösen der Eingaberegel ausgelöst. Dies liegt daran, dass die ersten drei Auslösungen (Ereignisse 1–3) innerhalb eines 8-Sekunden-Fensters stattfanden und zudem die zweite Gruppe (Ereignisse 2–4) ebenfalls innerhalb ihres eigenen 8-Sekunden-Fensters auftrat.

Die Option **Per Target** legt fest, dass es sich um dasselbe verfolgte Objekt handeln muss, das die Eingabe auslöst.

8.11.7.1 Grafische Ansicht



8.11.7.2 Formularansicht



8.11.7.3 Konfiguration

Merkmal	Beschreibung	Standardwert
Name	Ein vom Benutzer festgelegter Name für diese Regel	"Previous #"

Merkmal	Beschreibung	Standardwert
Can Trigger Actions (Kann Aktionen auslösen)	Gibt an, ob durch diese Regel ausgelöste Ereignisse Aktionen auslösen	Active
Input (Eingabe)	Eingaberegel	None
Duration (Dauer)	Der Zeitpunkt, zu dem die „Anzahl der auszulösenden Ereignisse“ ausgelöst werden muss	3
Number of Events to Trigger (Anzahl der auszulösenden Ereignisse)	Die Anzahl der Eingaben, die zum Auslösen erforderlich sind	4
Per Target (Pro Ziel)	Pro verfolgtem Objekt ein Ereignis auslösen	Active

8.12 Weitere Quellen

- HTTP
- Schedule (Zeitplan)

8.12.1 VCA - HTTP

Die HTTP-Quelle erstellt einen beliebigen REST-API-Endpunkt mit einer Statusvariablen, die auf „true“ oder „false“ gesetzt werden kann. Dadurch wird ein virtueller digitaler Eingang erstellt, den Systeme von Drittanbietern aktivieren oder deaktivieren können. Die HTTP-Quelle kann über den [Quellenfilter] in einem Regelgraphen referenziert werden.

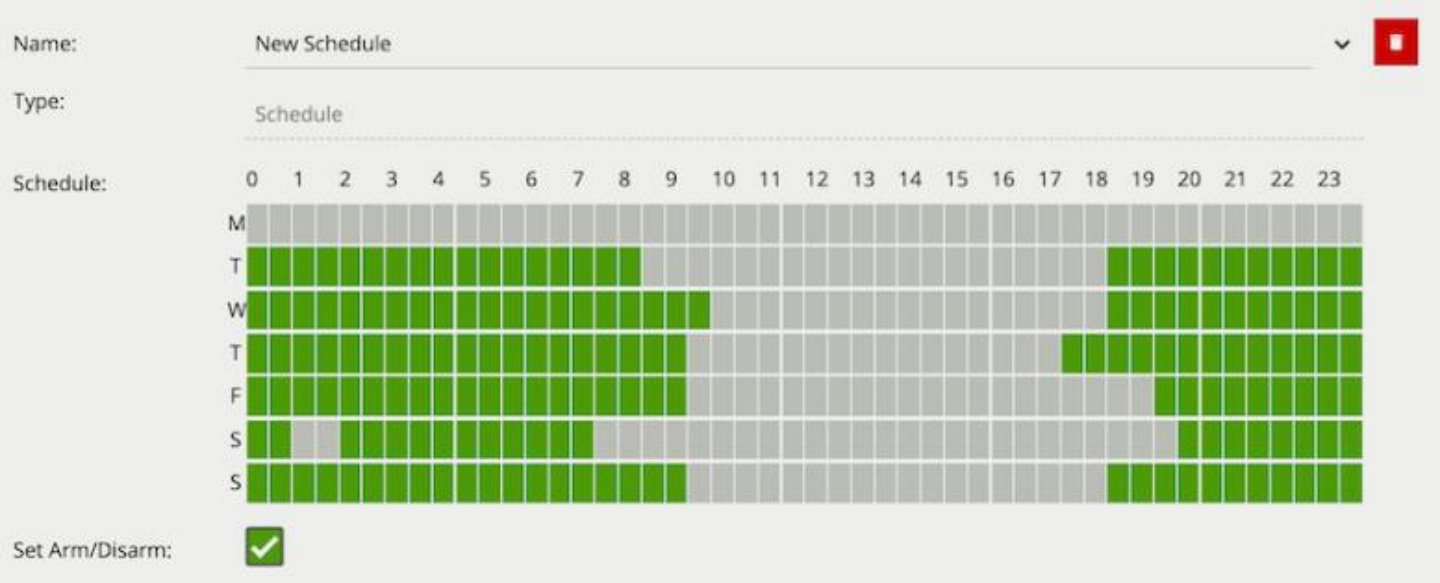


8.12.1.1 Eigenschaften

- **Endpoint URL**: Der REST-API-Endpunkt, der die Statusvariable definiert.

8.12.2 VCA - Schedule

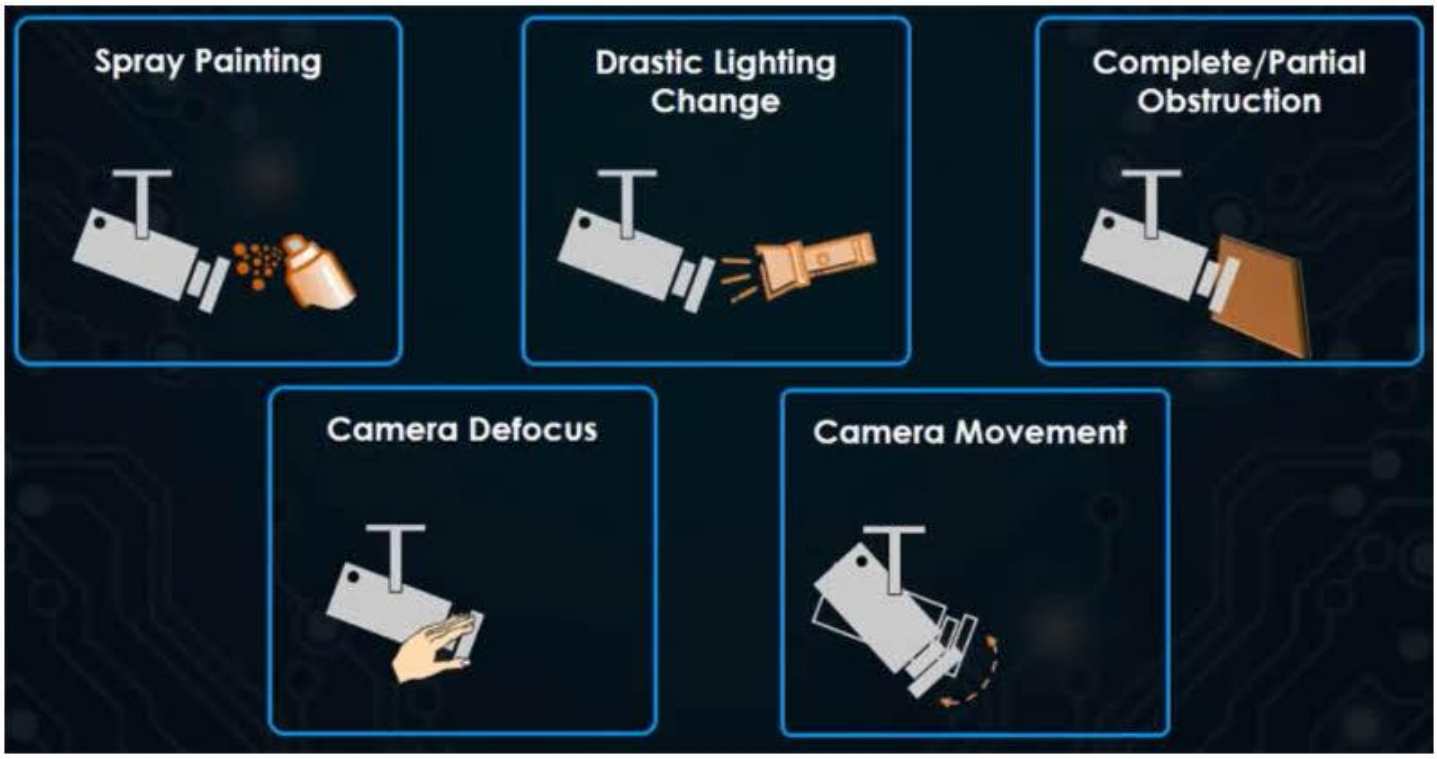
Die Zeitplanquelle ermöglicht die Festlegung eines Zeitplans, nach dem die Quelle ein- oder ausgeschaltet wird. Auf die Zeitplanquelle kann über den [Quellenfilter] in einem Regelgraphen verwiesen werden. Darüber hinaus kann die Zeitplanquelle dazu verwendet werden, den aktivierten Zustand des VCA direkt zu steuern.



8.12.2.1 Eigenschaften

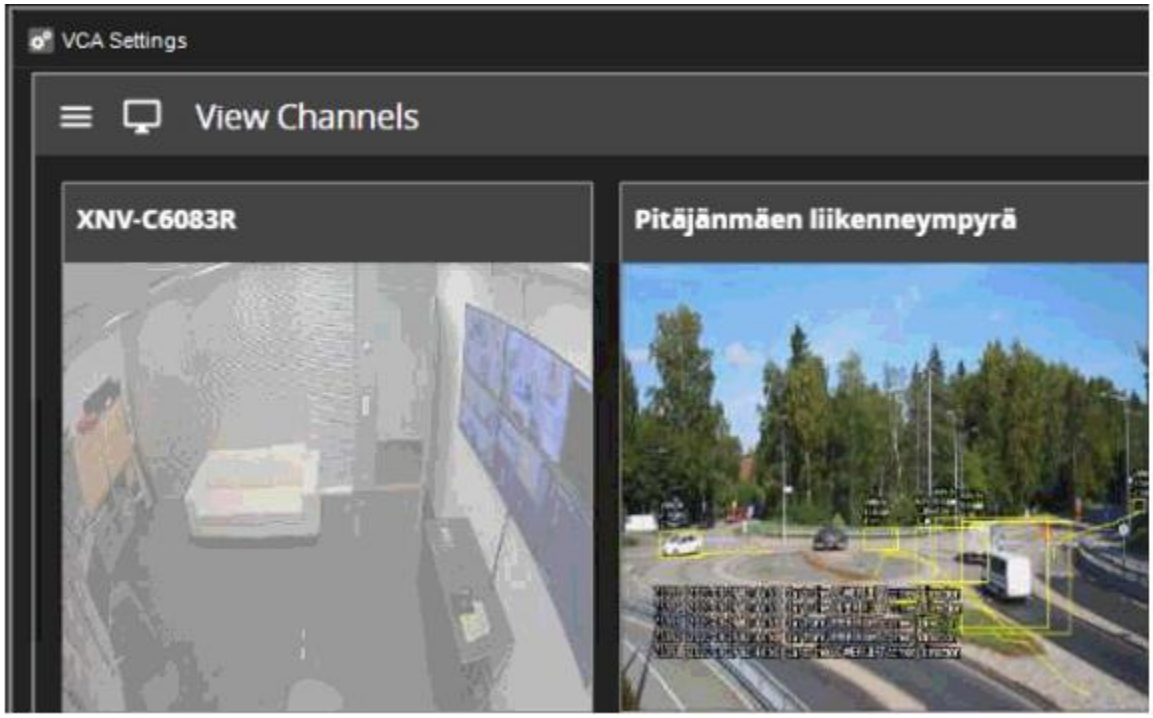
- **Schedule** (Zeitplan): Eine Drag-and-Drop-Oberfläche, über die Aktivierungs- (grün) und Deaktivierungszeiten (grau) festgelegt werden können. Jede Zeile steht für einen der sieben Wochentage, jede Spalte für einen halbstündigen Zeitraum innerhalb dieser 24 Stunden.
- **Set Arm/Disarm** (Aktivieren/Deaktivieren): Wenn diese Option aktiviert ist, legt die Zeitplanquelle den VCA-Aktivierungsstatus direkt gemäß dem oben definierten Zeitplan fest.

8.13 VCA – MANIPULATIONSERKENNUNG

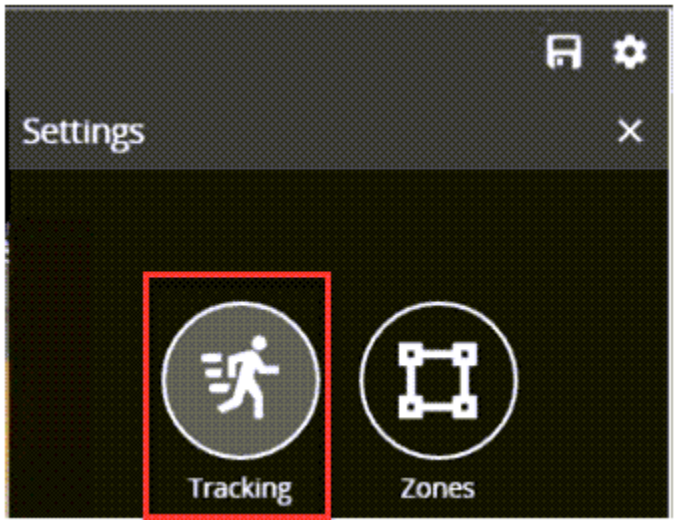


8.13.1 So aktivieren Sie die Manipulationserkennung

1. Öffnen Sie die Kamera über die Kanalansicht

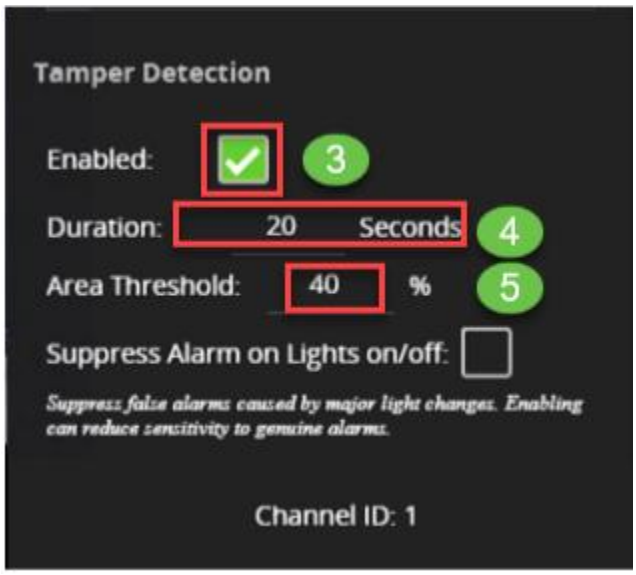


2. **Tracking** öffnen



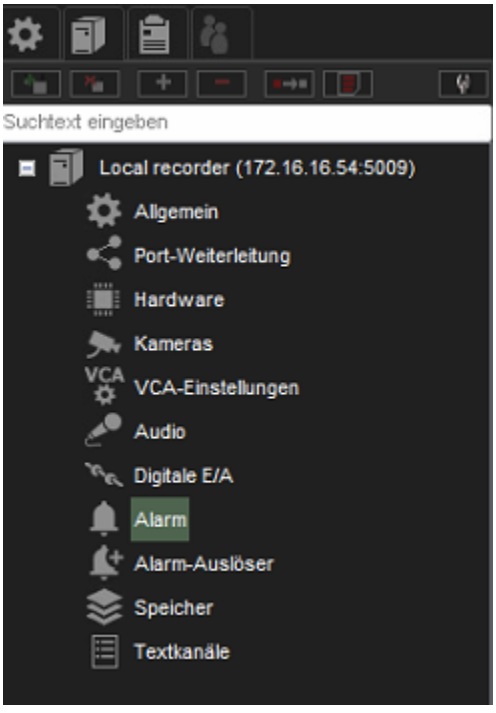
3. **Tamper Detection** (Manipulationserkennung) aktivieren
4. **Duration** (Dauer) festlegen

5. **Area Threshold (**Bereichsschwellenwert) festlegen

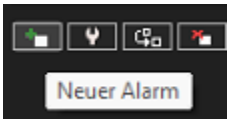


8.13.2 So erstellen Sie einen Alarm anhand der Manipulationserkennung

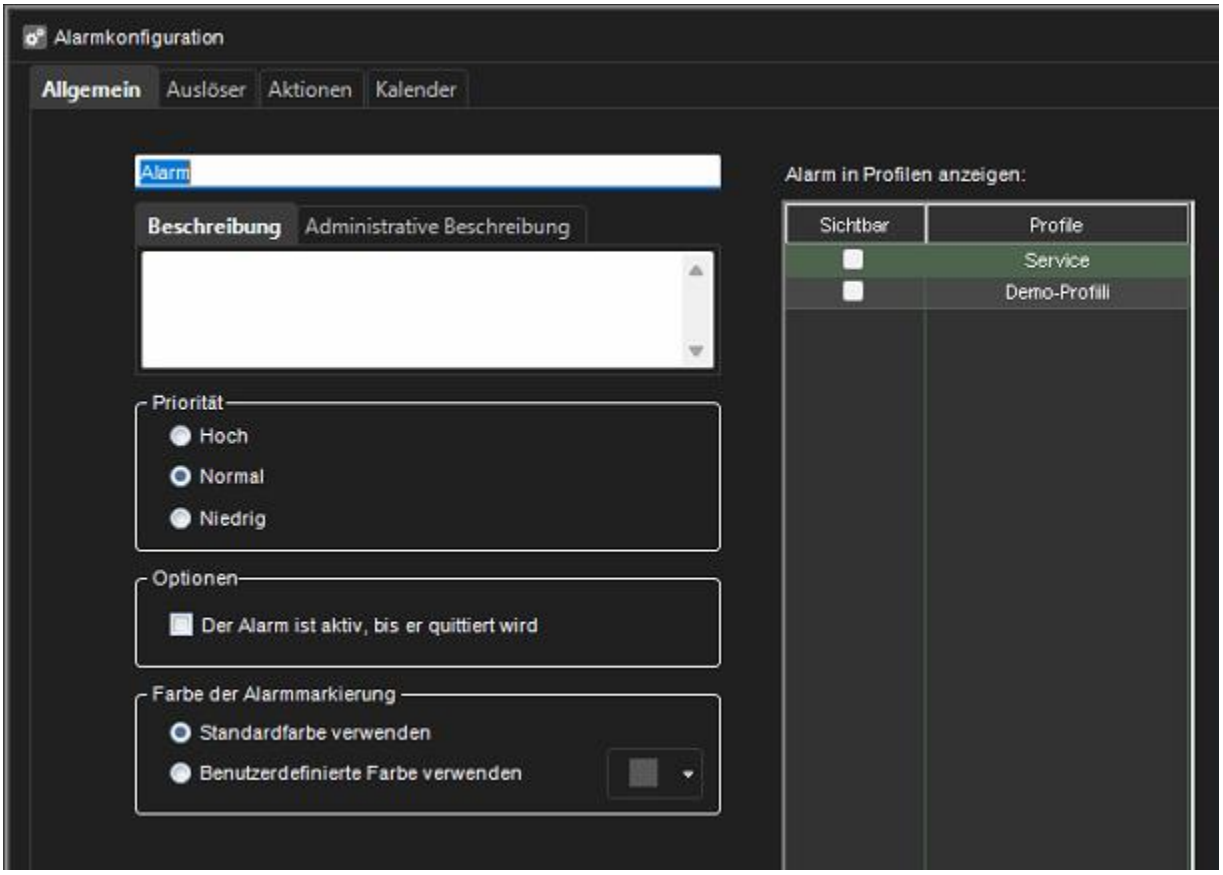
1. Offene **Alarme** vom gewünschten VMS-Server



2. Klicken Sie auf **Neuer Alarm**

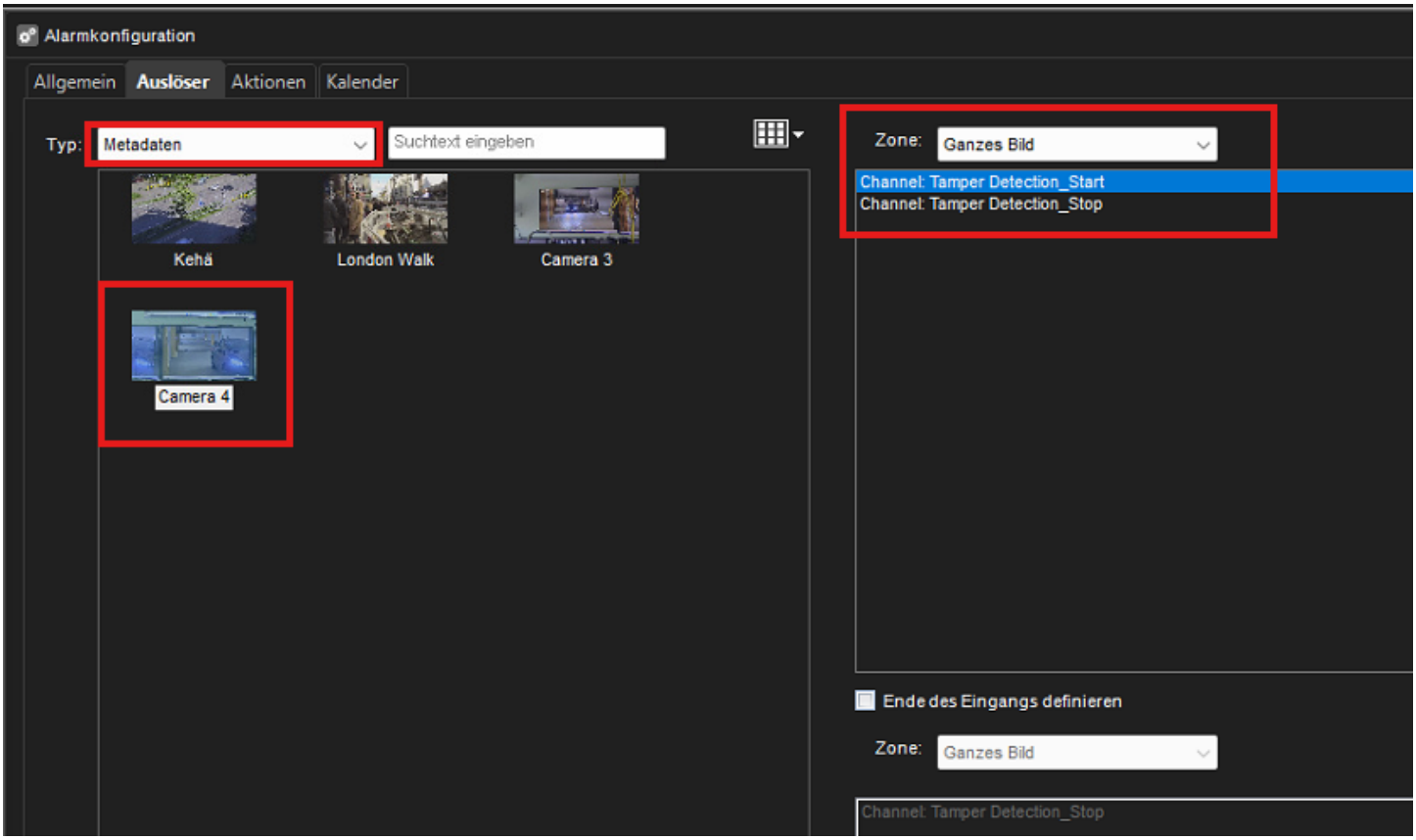
1. 

Geben Sie den Namen des Alarms ein

2. 

Metadaten des Triggers auswählen

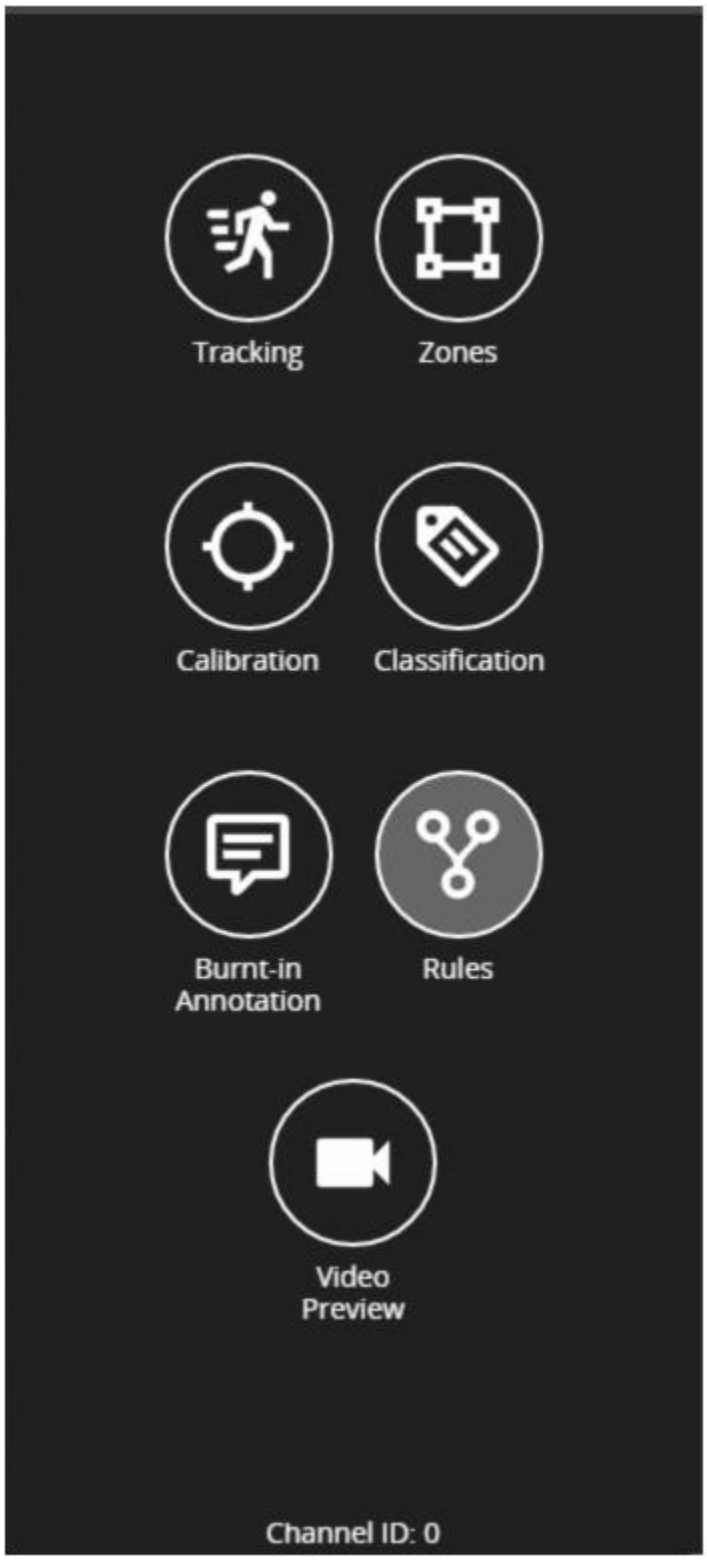
3. Wähle eine Kamera aus der Liste aus
4. **Tamper Detection** (Manipulationserkennung) auswählen



8.14 So erstellen Sie Regeln

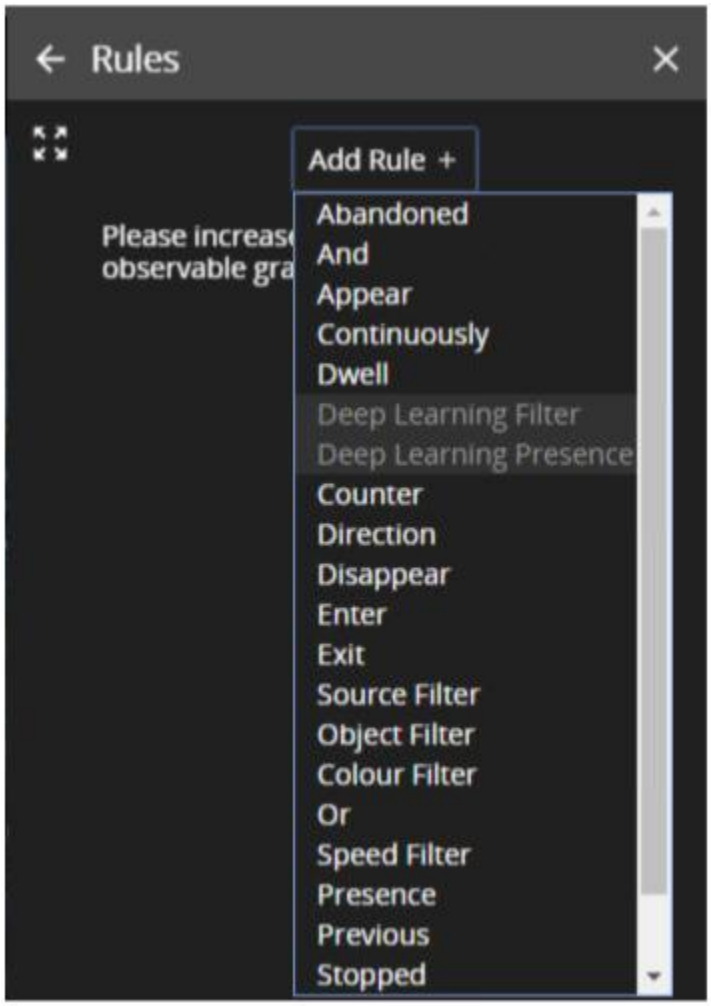
1. Klicken Sie auf **Rules**

MIRASYS

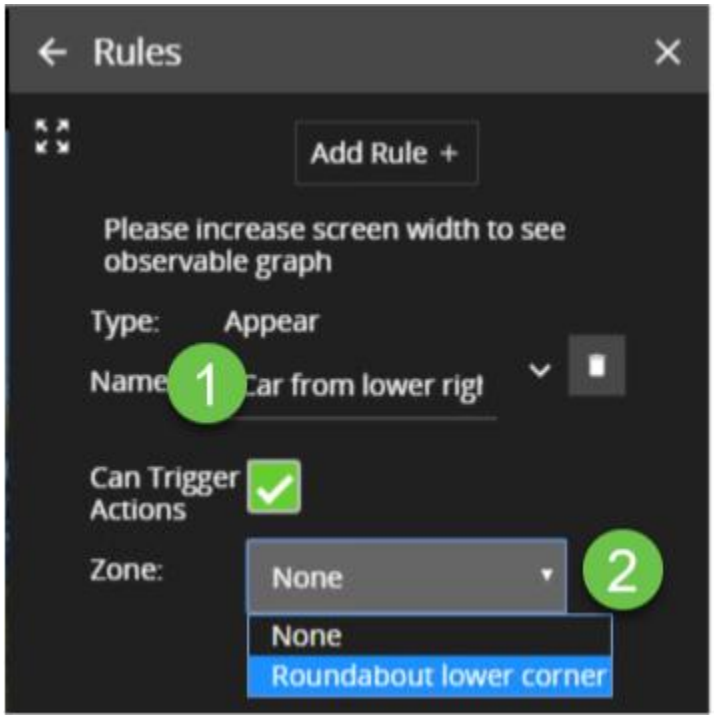


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

2. Klicken Sie auf **Add Rule**
3. Wählen Sie eine Regel aus der Liste aus

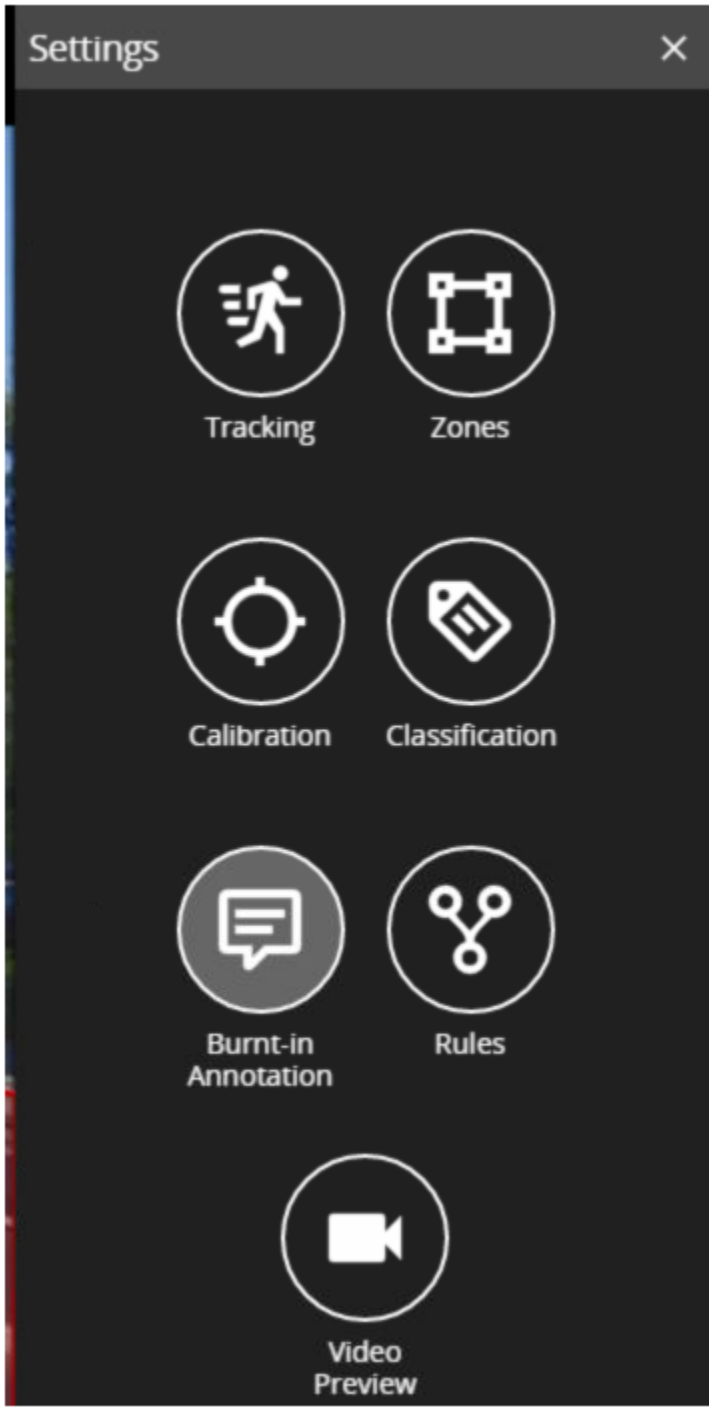


4. Legen Sie den Namen für die Regel fest
5. Zone auswählen



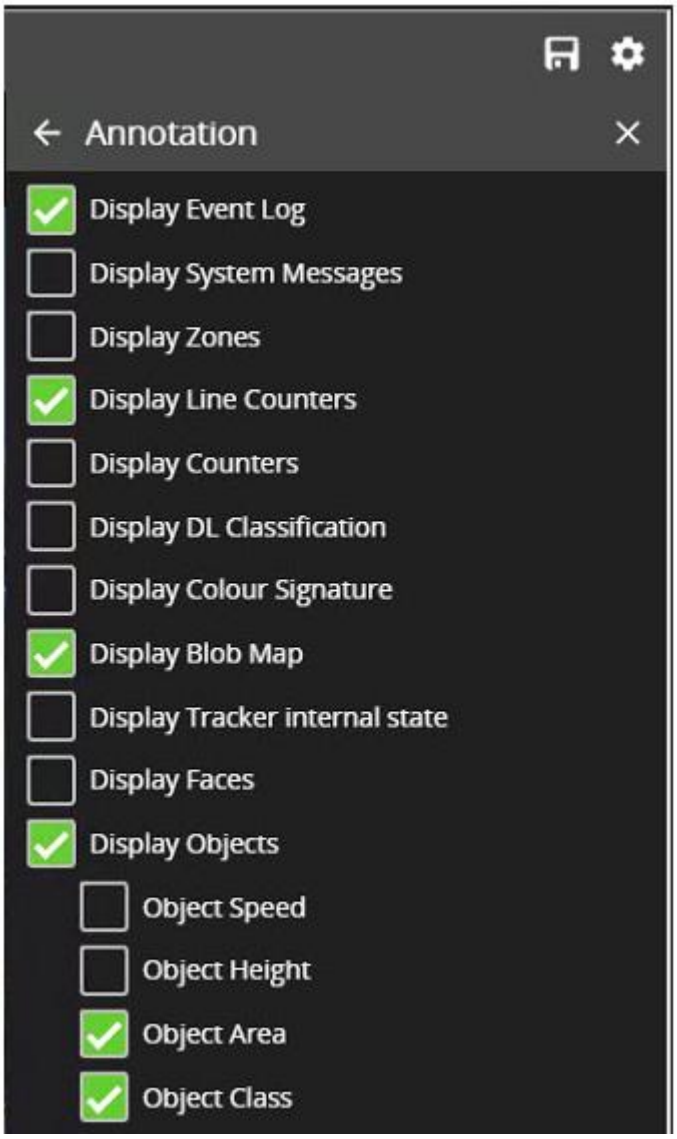
8.15 So testest du Regeln

1. **Burnt-in Annotation** öffnen

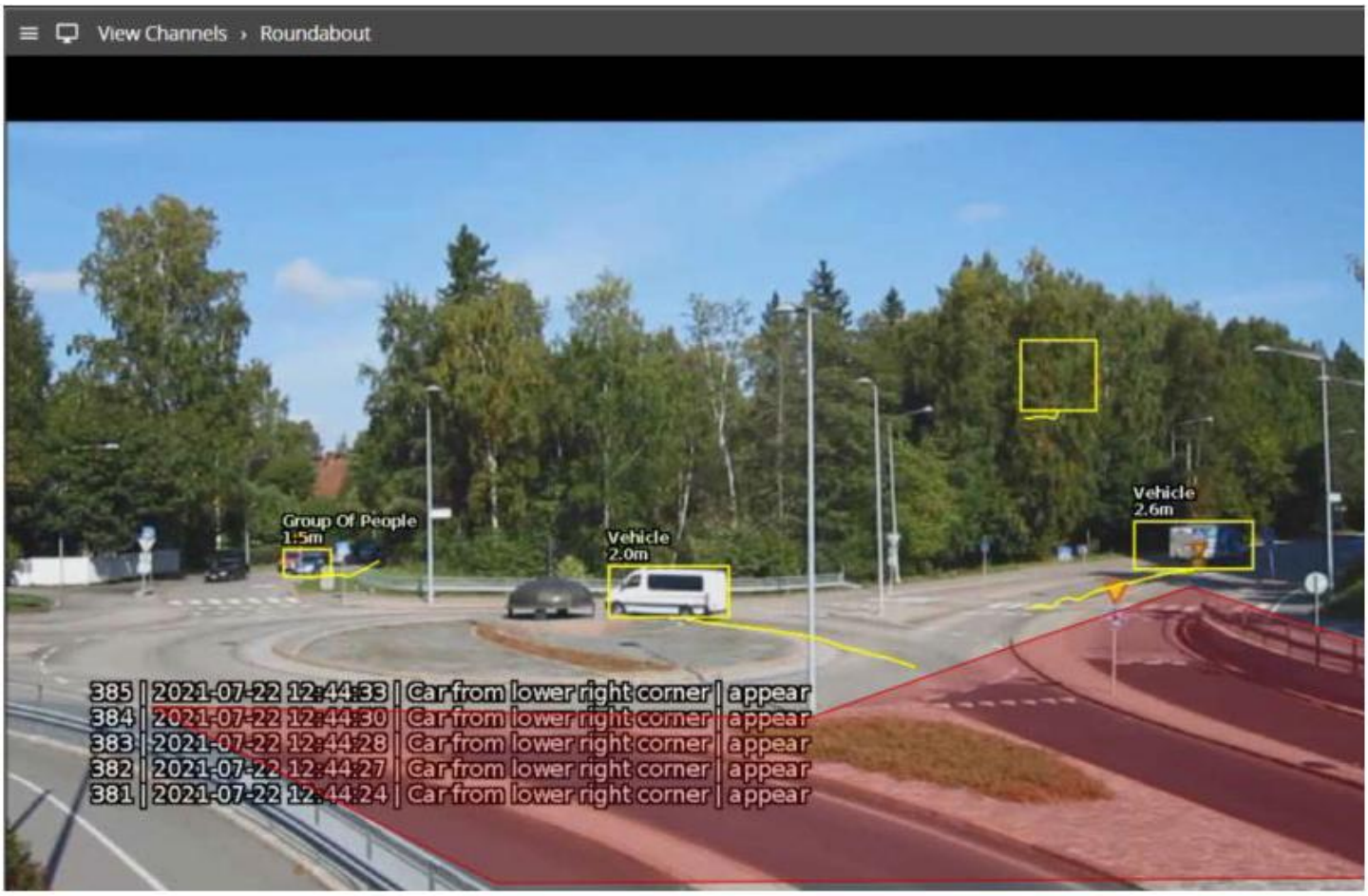


2. **Event Log** aktivieren
3. **Display Line Counters** aktivieren

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

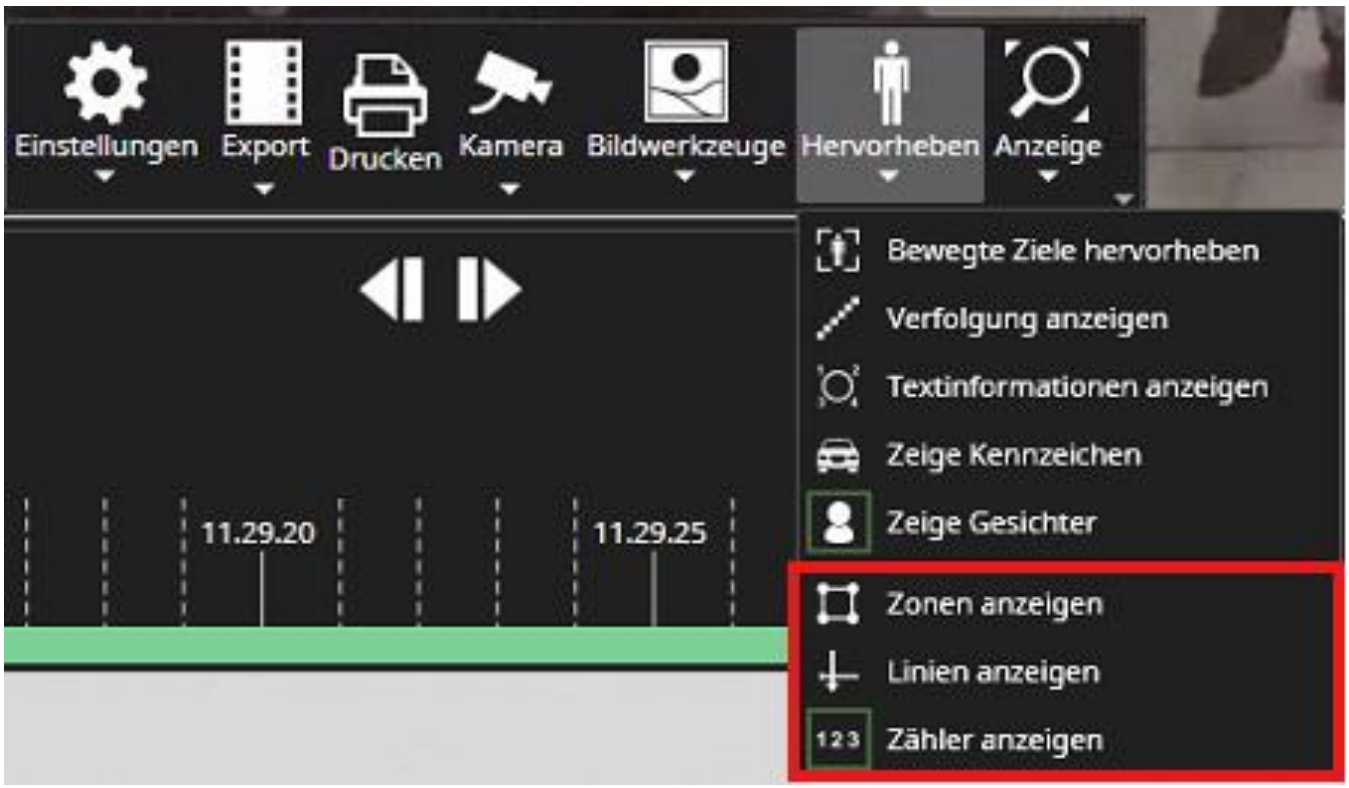


Öffnen Sie die richtige Kamera und überprüfen Sie, ob die ausgelösten Ereignisse angezeigt werden



8.16 So zeigen Sie VCA-Ereignisse im Mirasys Spotter an

1. Öffnen Sie die Kameraansicht in Echtzeit
2. Öffnen Sie die Kamera-Symbolleiste und klicken Sie auf **Hervorheben**
3. Aktivieren Sie die gewünschten Optionen (**Zonen anzeigen**, **Linien anzeigen** oder **Zähler anzeigen**)

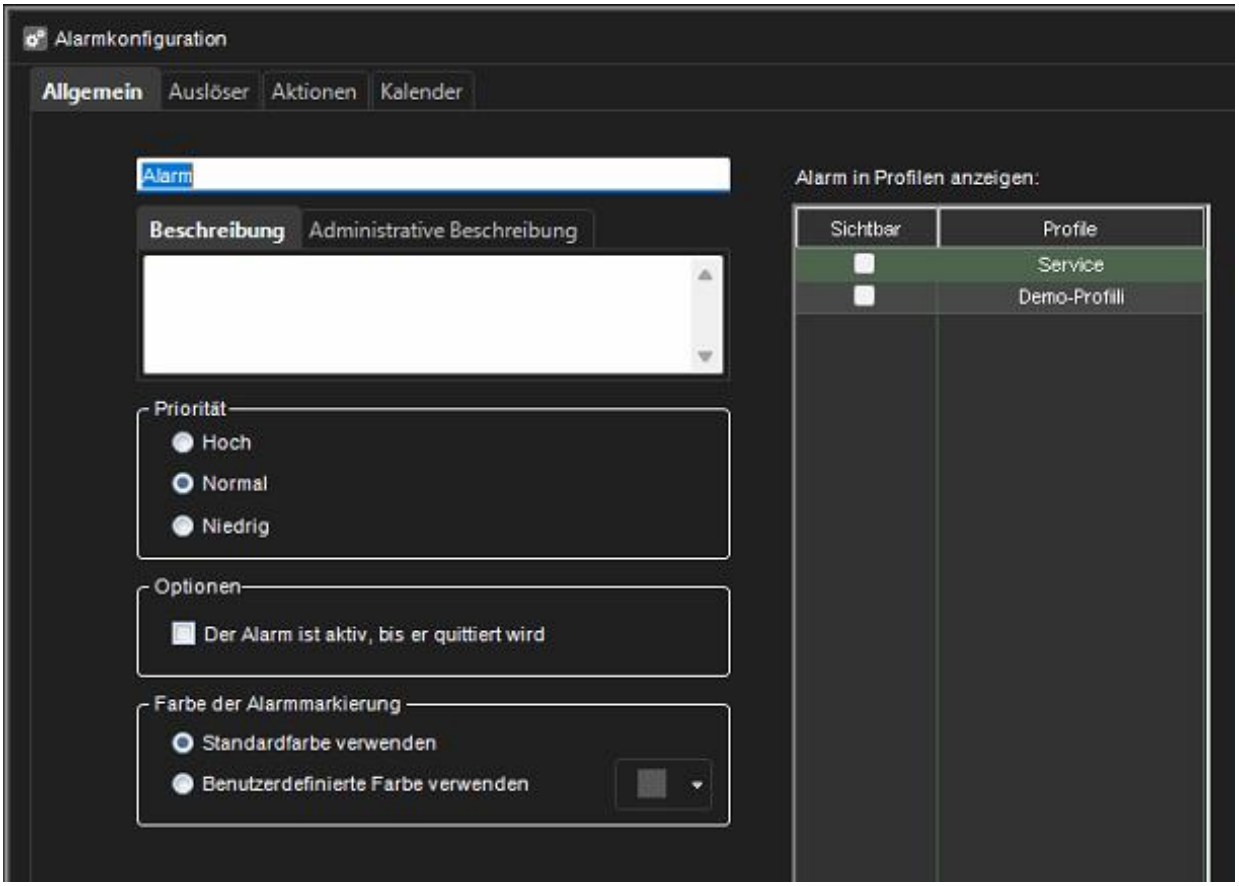


8.17 So erstellen Sie einen Alarm anhand eines VCA-Ereignisses

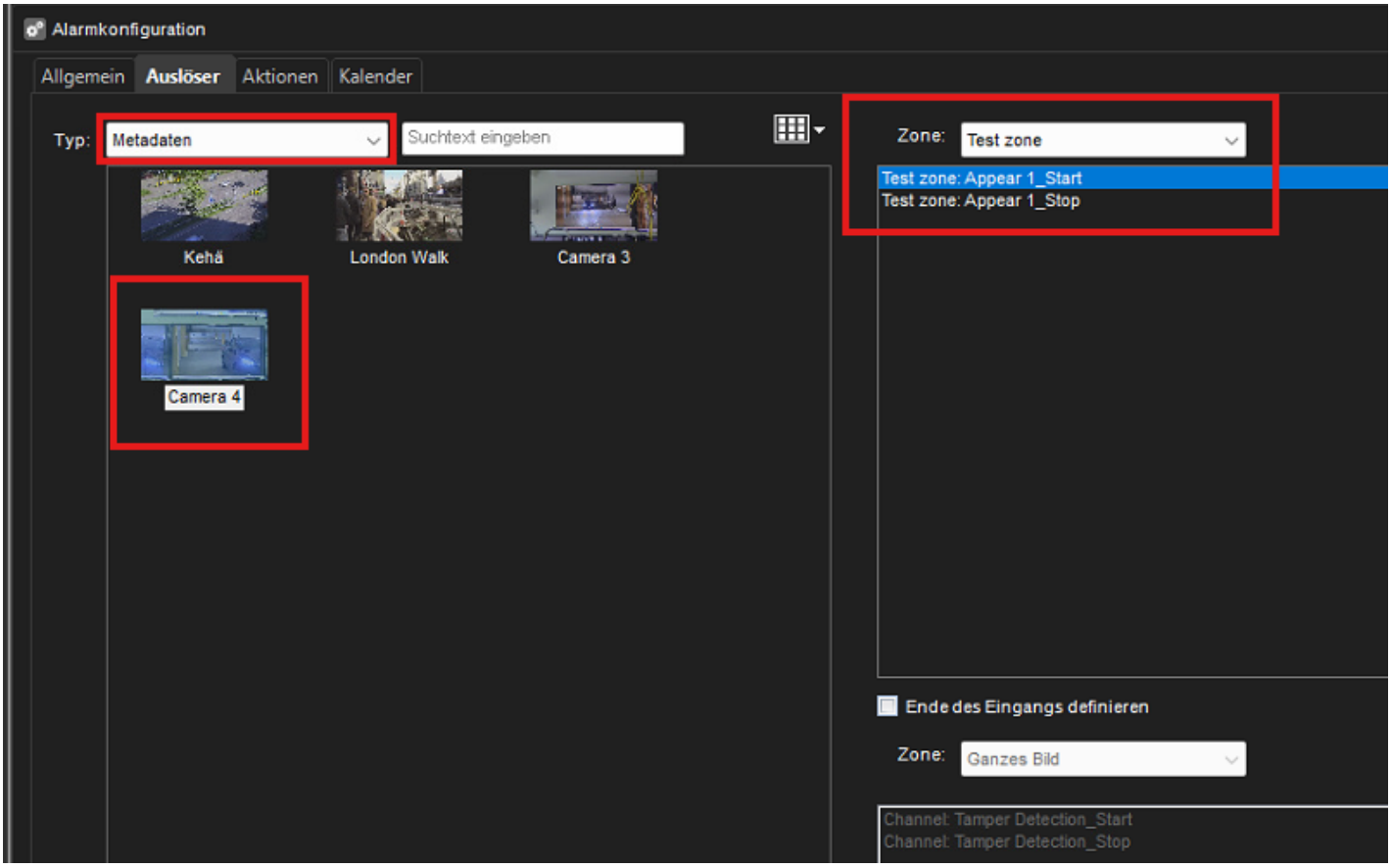
1. Wechseln Sie zur Registerkarte **VMS-Server**
2. Klicken Sie auf **Alarme**
3. Klicken Sie auf **Neuer Alarm**
4. 

Geben Sie den Namen des Alarms ein

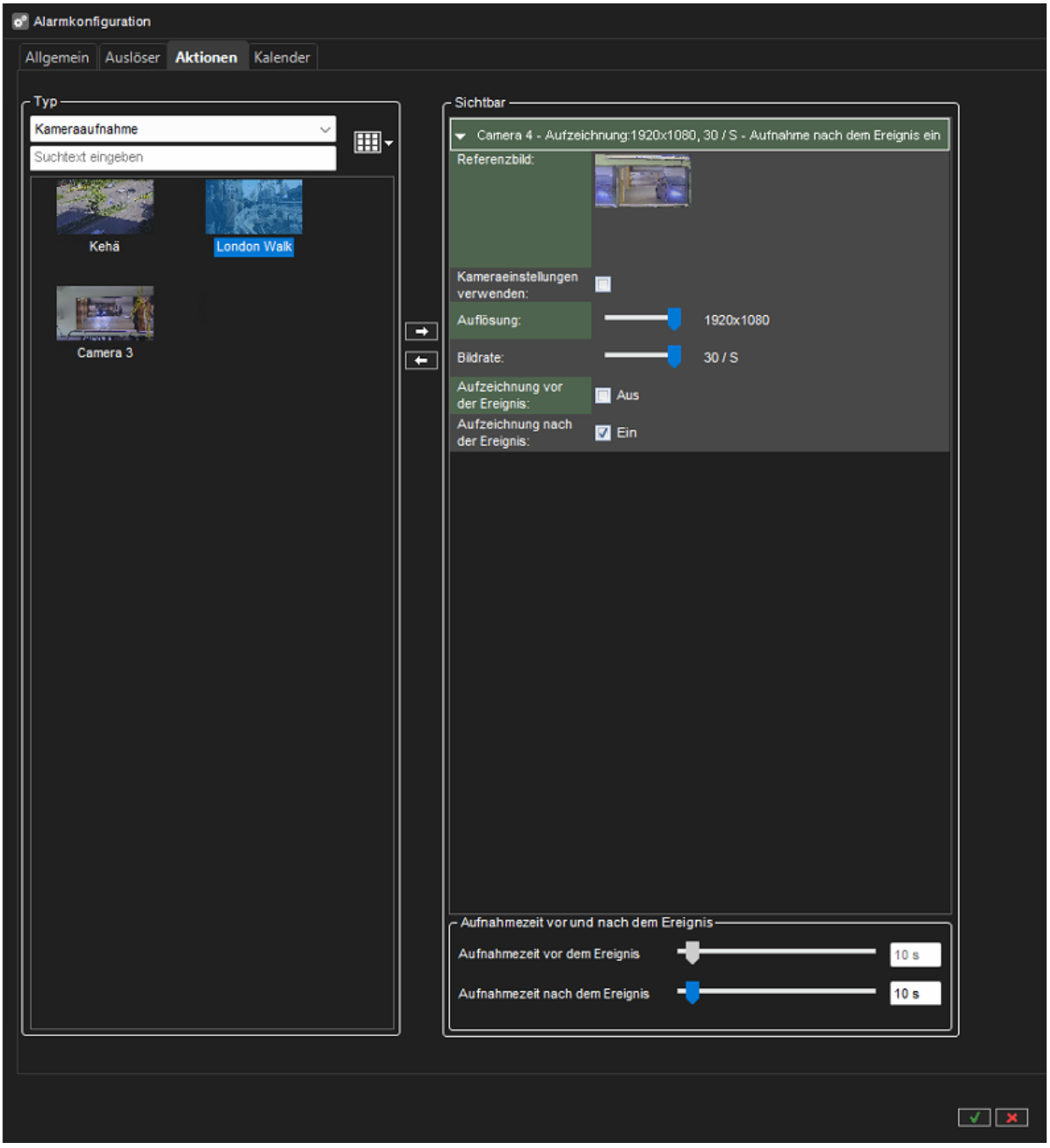
5. Wählen Sie **Alarm in Profilen anzeigen**



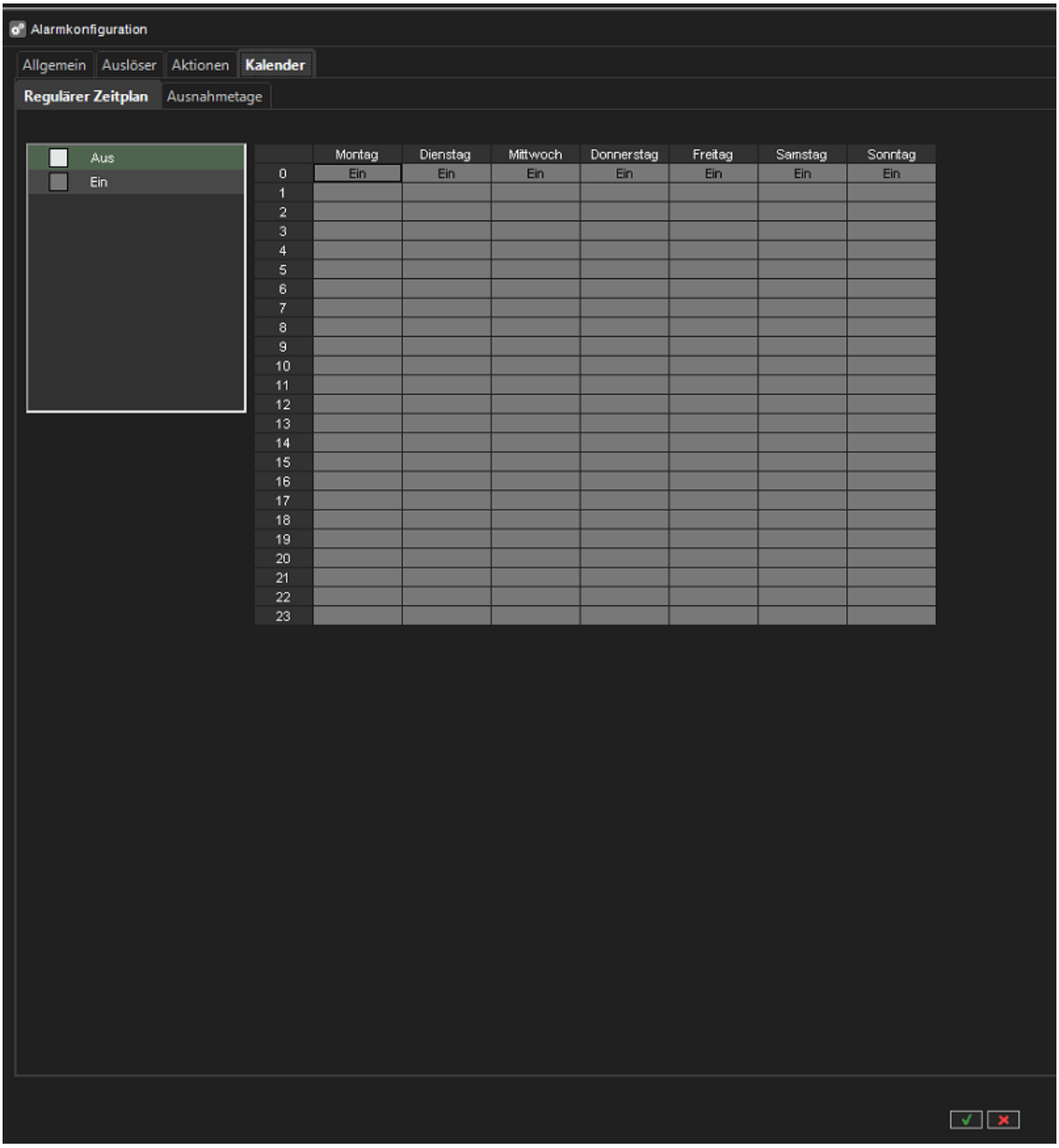
1. Wechseln Sie zur Registerkarte **Auslöser**
2. Typ auswählen: **Metadaten**
3. Wählen Sie die richtige Kamera aus der Liste aus
4. Wählen Sie eine Zone aus



1. Wechseln Sie zur Registerkarte **Aktionen**
2. Wählen Sie die erforderlichen Aktionen aus
3. Fügen Sie sie der Liste „Sichtbar“ hinzu
4. Legen Sie bei Bedarf die Aufzeichnungsdauer vor und nach dem Ereignis fest

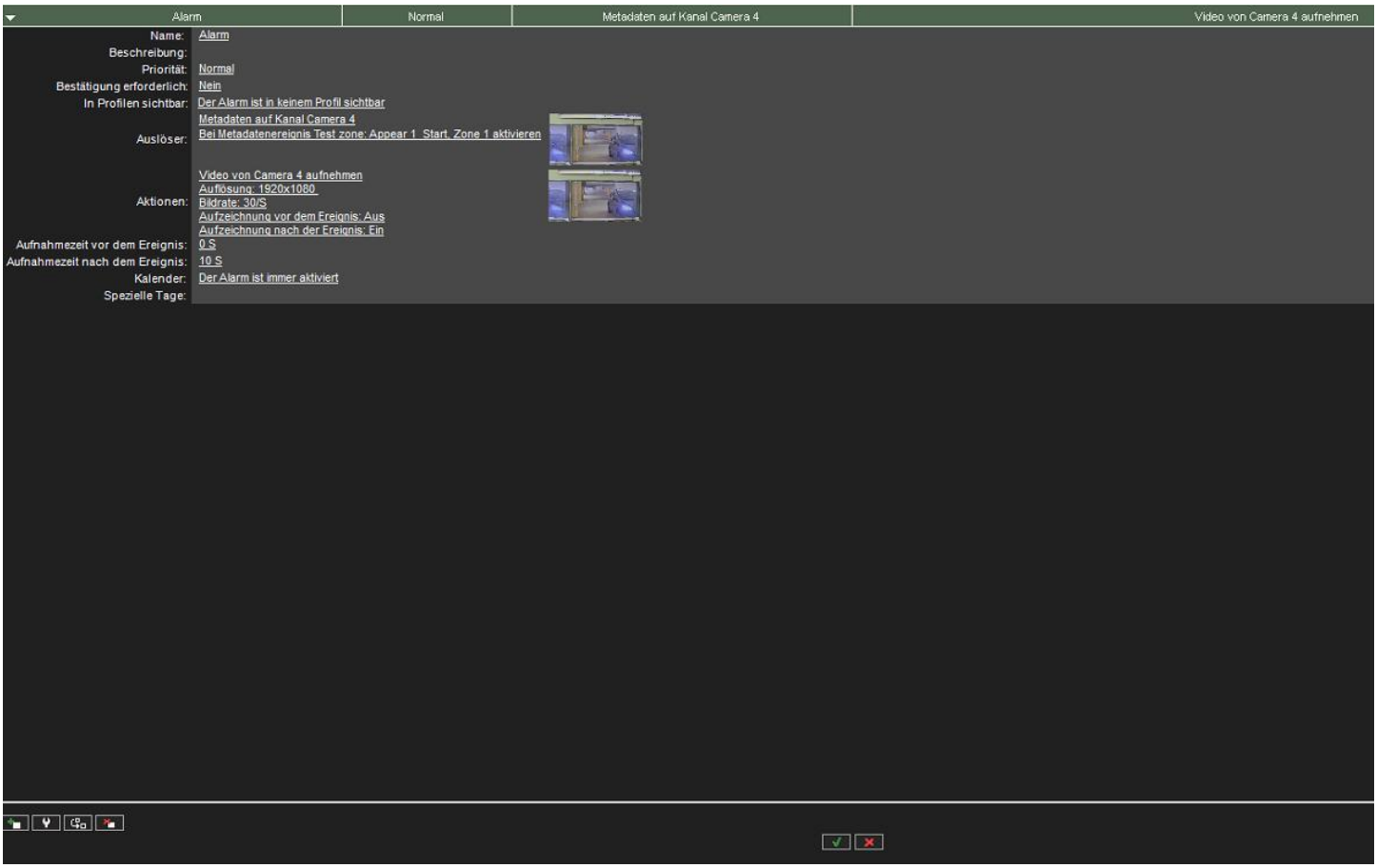


1. Wechseln Sie zur Registerkarte **Kalender**
2. Zeitplan für Alarm einstellen
3. Auf **OK** klicken



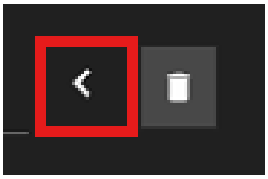
4. Alarmkonfiguration überprüfen

5. Klicken Sie auf **OK**, um die Erstellung des Alarms abzuschließen



8.18 KONFIGURATION

1. System Manager öffnen
2. Gewünschten Server auswählen **VCA-Einstellungen**
3. Klicken Sie auf die **Menü**-Schaltfläche in der oberen linken Ecke
4. Wählen Sie **Settings**
5. Wählen Sie **Edit Source**
6. Wählen Sie **Add Other Source +**
7. Wählen Sie **Schedule**
8. Geben Sie einen Namen für den Zeitplan ein und klicken Sie auf das Pfeilsymbol, um die Details der Quelle zu öffnen



1. Wählen Sie den Tag und die Uhrzeit für die Aktivierung aus
2. Gehen Sie zu den **Rules** unter „Kanäle anzeigen“, indem Sie auf die gewünschte Kamera klicken
3. Wählen Sie **Add Rule +** und wählen Sie „Counter“ aus dem Dropdown-Menü aus
4. Fügen Sie den zuvor erstellten Zeitplan hinzu, indem Sie auf **Add Reset Input +** klicken

Der VCA-Zähler wird zurückgesetzt, wenn dieser Eingang aktiviert wird.

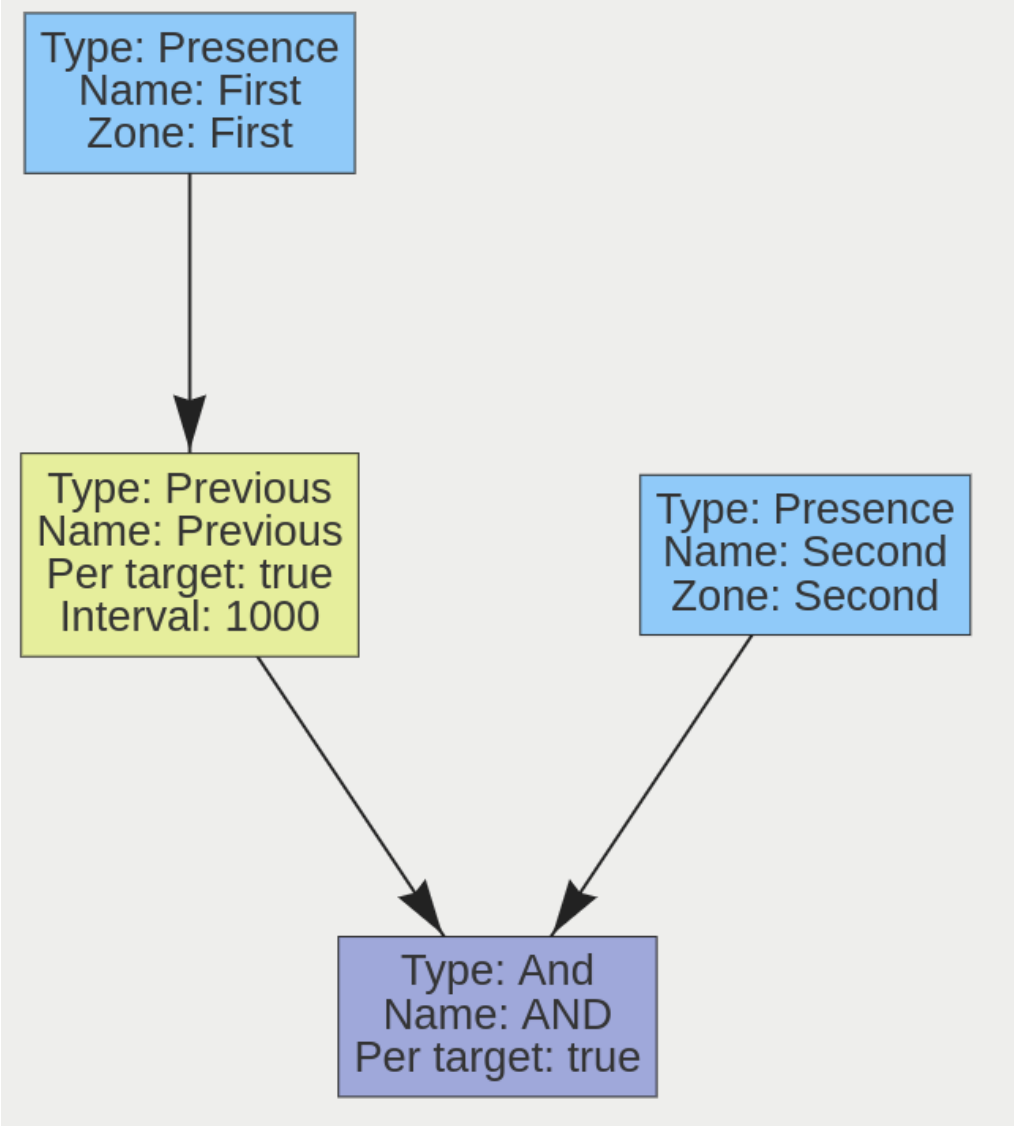
Alle diese Schritte werden im Menü **VCA-Einstellungen**.

8.19 Beispiele für kombinierte Regeln

- Double-Knock-Regel
- Präsenz in Gebiet A oder Gebiet B

8.19.1 VCA - Double-Knock-Regel

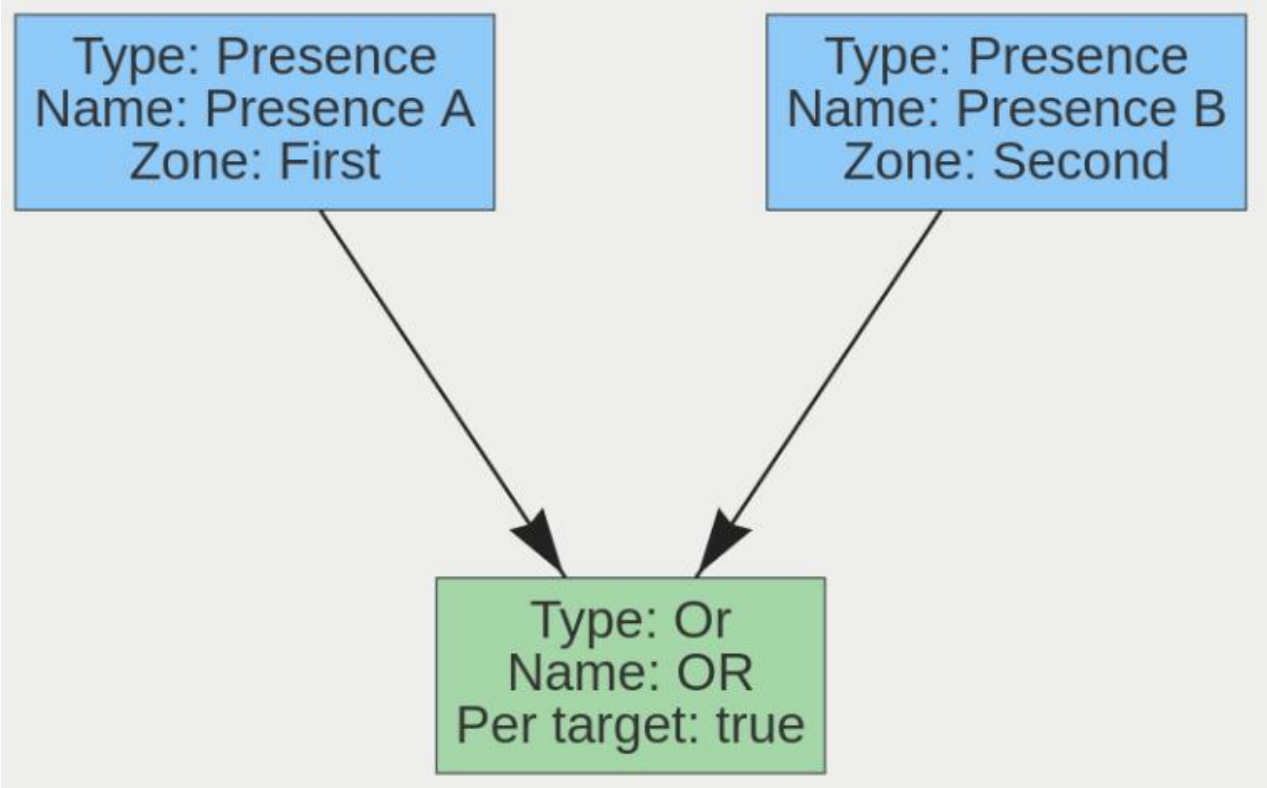
Die logische Regel „Double-Knock“ wird ausgelöst, wenn ein Objekt eine Zone betritt, das zuvor innerhalb eines festgelegten Zeitraums eine andere definierte Zone betreten hat. Das Intervall in der vorherigen Regel legt fest, wie viel Zeit zwischen dem Betreten der ersten und der zweiten Zone durch das Objekt vergehen darf. Das Diagramm für eine logische „Double-Knock“-Regel sieht wie folgt aus:



Die Regel lässt sich wie folgt interpretieren: „Ein Objekt befindet sich in Zone 2 und befand sich in den letzten 1000 Millisekunden in Zone 1“. Diese Regel kann als zuverlässige Methode zur Erkennung des Betretens eines Bereichs verwendet werden. Da das Objekt zwei Zonen in einer bestimmten Reihenfolge betreten muss, können damit Fehlalarme vermieden werden, die bei einer einfachen Anwesenheitsregel auftreten können.

8.19.2 Präsenz in Gebiet A oder Gebiet B

Diese Regel wird ausgelöst, wenn sich ein Objekt entweder in Zone A oder in Zone B befindet. Der Ablauf ist wie folgt:



Ein typischer Anwendungsfall für diese Regel ist, wenn mehrere Bereiche bestehen, in denen der Zugang verboten ist, diese Bereiche jedoch nicht ohne Weiteres durch eine einzige Zone abgedeckt werden können. Es können zwei Zonen erstellt werden, denen jeweils eine eigene Anwesenheitsregel zugeordnet wird; diese können dann mithilfe einer Or-Regel kombiniert werden.

8.20 GPU-Leistung

Hier finden Sie eine grundlegende Erklärung dazu, wofür die CPU verwendet wird. Die CPU wird für Folgendes genutzt:

- Dekodierung des eingehenden RTSP-Streams
- Kodierung aller ausgehenden, mit Anmerkungen versehenen RTSP-Streams
- Anpassung der Bildgröße vor der Weiterleitung an die Analyse-Engine
- Vorverarbeitung, bevor das Bild zur Verarbeitung durch den DL-Tracker an die GPU weitergeleitet wird

Die ersten drei Punkte werden derzeit für alle Tracker durchgeführt, sowohl für den Standard-Bewegungsobjekt-Tracker als auch für die DL-Tracker.

Der letzte Punkt wird bei Verwendung der DL-Tracker ausgeführt und erfordert zusätzliche Ressourcen der CPU. Infolgedessen verringert sich die Anzahl der Kanäle, die auf einer bestimmten CPU unterstützt werden können, wenn DL-Tracker verwendet werden.

Diese Tabelle gibt einen Überblick darüber, wie VCA mit einer GPU abschneiden kann. Verschiedene Szenarien können die Leistung beeinflussen.

GPU	CUDA-Kerne	Tensor-Kerne	Speicher	Prozessortaktfrequenz	Speicherbandbreite (GB/sec)	Tatsächliche Kanäle DLOT-getestet
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**

9 VAIDIO-INTEGRATION

Die **Vaidio-Integration** ermöglicht es einem Mirasys-VMS-Bediener, die forensische Suche mit Vaidio AI direkt aus Spotter heraus durchzuführen. Sie besteht aus zwei unabhängig voneinander bereitgestellten Komponenten, die über eine HTTP-REST-API miteinander kommunizieren: dem Integrationsdienst und dem Plugin für die forensische Suche. Die folgende Tabelle enthält weitere Details zu den Komponenten.

Komponente	Beschreibung	Ausführungsumgebung	Technologie
Integration Service	A standalone Windows service that exposes a REST API and proxies requests through to a Vaidio appliance.	A DVMS/VMS, a Spotter, or its own dedicated machine.	Self-contained .NET 9, installed by a Windows MSI.

Komponente	Beschreibung	Ausführungsumgebung	Technologie
Plugin „Forensic Search“	Ein Spotter-Plugin, das dem Spotter-Client die Registerkarte „Forensische Suche“ hinzufügt.	Im Spotter-Client, zusammen mit den anderen Spotter-Plugins.	.NET Framework 4.8: Das Plugin wird als separates .spi-Paket bereitgestellt, das im System Manager auf dem VMS-System installiert werden kann.

9.1 Unterstützte Funktionen

In der Benutzeroberfläche des Spotter-Plugins (Registerkarten):

- **Gesichtssuche –** Suche nach einem Gesicht in aufgezeichnetem Material (anhand eines hochgeladenen Bildes oder eines erkannten Deskriptors).
- **Objektsuche –** Suche nach Objekten und ähnlichen Objekten.
- **Kennzeichensuche –** Suche nach aufgezeichneten Kennzeichen.
- **Kameraübergreifende Verfolgung –** Verfolgung einer Person über mehrere Kameras hinweg.
- **Live-Anzeige –** Aktuelle Gesichter/Kennzeichen, sobald sie erkannt werden.

9.2 Lizenzmodell

Ein funktionsfähiges System benötigt zwei unabhängige Lizenzen:

1. **Die Lizenz für den Integrationsdienst** – schaltet die Dienst-API frei und ist an den Rechner des Dienstes gebunden.
2. **Die Lizenz für das Forensic-Search-Plugin** – die VMS-Hauptlizenz muss die Lizenz für das **Deep Vision Data-Plugin** enthalten, da das Plugin sonst in Spotter überhaupt nicht geladen wird.

9.3 Optionale Datenbanknutzung

Der Integrationsdienst unterstützt die optionale Installation einer Datenbank, die bei der Installation ausgewählt werden kann:

	Ohne Datenbank	Mit einer Datenbank
Umfasst	Nur Forensic Search	Forensic Search plus Identitätsabgleich – Persistenz der Personenidentität
Back-up-Speicher	Keine	Eine lokale PostgreSQL-16-Datenbank

	Ohne Datenbank	Mit einer Datenbank
Installieren	Derselbe Installer, Kontrollkästchen deaktiviert (Standardeinstellung)	Derselbe Installer, Kontrollkästchen angekreuzt – er installiert oder erkennt PostgreSQL 16, anschließend den Dienst
Abwägung	Am einfachsten, am kleinsten, keine Datenbank, die betrieben oder gesichert werden muss	Fügt eine zustandsbehaftete Abhängigkeit hinzu, die Sie bereitstellen, sichern und sichern müssen

Das Installationsprogramm des Integrationsdienstes enthält PostgreSQL und installiert es nur, wenn das Kontrollkästchen **Identitätsabgleich-Datenbank installieren** aktiviert ist (oder bei einer automatischen Installation der Parameter `InstallDatabase=1`übergeben wird). Forensic Search greift in keinem Fall auf die Datenbank zu, sodass bei einer Ausführung ohne Datenbank lediglich die Identitätsabgleich-Funktion ausfällt, nicht jedoch die Funktionen von Forensic Search.

> Die meisten Bereitstellungen erfolgen **ohne Datenbank**. Entscheiden Sie sich nur dann für eine Bereitstellung **mit Datenbank**, wenn die dauerhafte Speicherung von Personenidentitäten ausdrücklich erforderlich ist.

9.4 VERSIONSKOMPATIBILITÄT

Das „Forensic Search"-Plugin funktioniert nur mit derselben Version des Integrationsdienstes. Bei einer Versionsinkongruenz zeigt das „Forensic Search"-Plugin beim Öffnen eine entsprechende Meldung an.

> Aktualisieren Sie den Dienst auf die entsprechende Version, bevor Sie ein neueres Plugin einführen.

9.5 ANFORDERUNGEN

9.5.1 Anforderungen an den Integrationsdienst

9.5.1.1 Anforderungen an den Host

- **Betriebssystem**: Windows 10 x64 / Windows Server 2016 oder höher.
- **.NET**: Für den Dienst ist kein .NET erforderlich, da er eigenständig ist (enthält eine eigene .NET 9-Laufzeitumgebung). .NET Framework 4.8 muss vorhanden sein, jedoch nur für das Installationsprogramm selbst; auf jedem DVMS/VMS-Rechner ist es bereits installiert.
- **Benutzerrechte**: Die Installation erfolgt pro Rechner und erfordert erweiterte Rechte (Administrator / UAC). Der Dienst läuft standardmäßig als „LocalSystem".

- **Speicherplatz**: ca. 200 MB für den eigenständigen Dienst und ca. 400 MB zusätzlich, wenn Sie die Datenbank (PostgreSQL) installieren. Das Installationsprogramm selbst ist ca. 420 MB groß, da das PostgreSQL-Redistributable immer darin eingebettet ist.

9.5.1.2 Netzwerk und Konnektivität

- **Eingehender Datenverkehr**: Der Dienst lauscht auf TCP 5194 (alle Schnittstellen). Das Installationsprogramm eröffnet dafür automatisch eine Firewall-Regel für eingehenden Datenverkehr (die bei der Deinstallation wieder entfernt wird). Spotter-Clients, auf denen das Plugin läuft, müssen `<http://<service-host>>:5194` erreichen können.

- **Ausgehende Verbindungen zu Vaidio**: Der Dienst muss die API der Vaidio-Appliance erreichen können. Verwenden Sie den Vaidio-API-Port (in der Regel :80, Pfad `/ainvr/api/...`) – achten Sie darauf, nicht die Admin-Weboberfläche unter :8000 zu verwenden (der Aufruf von `:8000` führt zu HTML- und JSON-Parsing-Fehlern).

- **Ausgehende Verbindung zu PostgreSQL (nur für die Datenbankkonfiguration)**: standardmäßig localhost:5432.

- Der Dienst läuft über reines HTTP auf Port 5194. Um TLS zu verwenden oder ihn über das lokale Netzwerk hinaus verfügbar zu machen, setzen Sie einen Reverse-Proxy ein und/oder schränken Sie den Firewall-Bereich ein.

9.5.1.3 Anforderungen an den Betreiber bei der Installation

Der Betreiber, der den Dienst installiert, benötigt Folgendes:

- Administratorrechte auf dem Zielrechner.

- Die Vaidio-Adresse, den Port, den Benutzernamen und das Passwort.

- Optional eine `.lic`-Lizenzdatei für diesen Rechner. Der Assistent zeigt die Hardware-ID des Rechners auf der Lizenzseite an, sodass diese abgefragt werden kann; dieser Schritt kann übersprungen werden. Ohne Lizenz lässt sich der Dienst zwar installieren und ausführen, gibt jedoch bei funktionsfähigen Endpunkten den HTTP-Status 423 zurück.

- Nur für die Datenbankkonfiguration: das Passwort des PostgreSQL-Superusers, mit dem die Bereitstellung erfolgen soll. Auf einem Rechner, auf dem PostgreSQL bereits installiert ist, ist dies das vorhandene Superuser-Passwort dieser Instanz.

Der Betreiber muss Folgendes nicht mehr bereitstellen:

- Die API-Schlüssel. Ein Admin-Schlüssel und ein Benutzer-Schlüssel, die das Plugin und andere API-Clients vorlegen, werden vom Installationsprogramm generiert und auf der Seite zur Dienstkonfiguration mit „Kopieren“-Schaltflächen angezeigt. Sie können weiterhin bearbeitet werden, falls der Kunde eigene Werte verwenden möchte. Ein leerer Schlüssel würde bei jeder Anfrage einen HTTP-Fehler 401 zur Folge haben, daher lässt das Installationsprogramm diese Felder niemals leer.

- Der Proxy-Sicherheitsschlüssel wird automatisch generiert, wenn das Feld leer ist. Er wird vom Server selbst ausgestellt: Der Server fügt ihn in die von ihm ausgegebenen Proxy-URLs ein und validiert eingehende Anfragen anhand seiner eigenen Kopie, sodass niemand außerhalb des Servers ihn jemals kennen muss. Eine manuelle Einstellung ist möglich, aber nicht erforderlich.

9.5.2 Anforderungen an das „Forensic Search“-Plugin

- Ein Spotter-Client der entsprechenden VMS-Version (V9.10 oder V10).
- Das signierte `ToolPluginIntegrationServer.spi`-Paket, das von Mirasys bezogen wird.
- Eine VMS-Hauptserverlizenz, die die Lizenz für das „Deep Vision Data Plugin“ enthält. Ohne diese Lizenz ist die Registerkarte „Forensic Search“ nicht verfügbar.
- Netzwerkzugriff auf den Dienst (eingehend).
- Der Dienst muss mindestens auf dem gleichen Stand wie das Plugin sein, andernfalls wird die Registerkarte mit der Meldung „Integrationsserver aktualisieren“ gesperrt. Installieren oder aktualisieren Sie den Dienst auf die entsprechende Version, bevor Sie das Plugin bereitstellen.

Beachten Sie, dass es zwei verschiedene Lizenzen gibt: **(1)** Die VMS-Hauptserverlizenz muss die Lizenz für das Deep Vision Data Plugin enthalten, damit das Plugin geladen wird; **(2)** die `.lic`-Datei des Integrationsdienstes schaltet die API des Dienstes frei. Beide sind für ein funktionsfähiges System erforderlich.

9.5.3 Vaidio-Anforderungen

- Eine erreichbare Vaidio-Appliance, deren API für den Service-Host freigegeben ist.
- Die API-Basisauthentifizierung muss in Vaidio aktiviert sein (**System** → **Einstellungen**), und es muss ein spezielles Konto mit Administratorrechten für den Integrationsserver angelegt worden sein.
- Ein einzelner Standard-NVR. Die Verwendung mehrerer NVRs wird nicht unterstützt bzw. kann nicht garantiert werden.
- Vaidio-Lizenzfunktionen, die die vom Plugin bereitgestellten Funktionen abdecken: FR (Gesichtserkennung), LPR (Kennzeichenerkennung), Alter und Geschlecht, Marke und Modell sowie kamerübergreifende Personenverfolgung. Das Verhalten bei Fehlen einiger dieser Funktionen wurde nicht getestet. Das Produkt stellt die von Vaidio bereitgestellten Funktionen zur Verfügung; es fügt keine eigenen Analysen hinzu.
- Getestete Vaidio-Versionen: 6.2.0, 7.1.0, 9.0.0, 9.1.0. Neuere Versionen sollten funktionieren, solange die öffentliche Vaidio-API kompatibel bleibt.

9.6 VAIDIO-INSTALLATION

Diese Seite enthält Anleitungen für zwei Installationen:

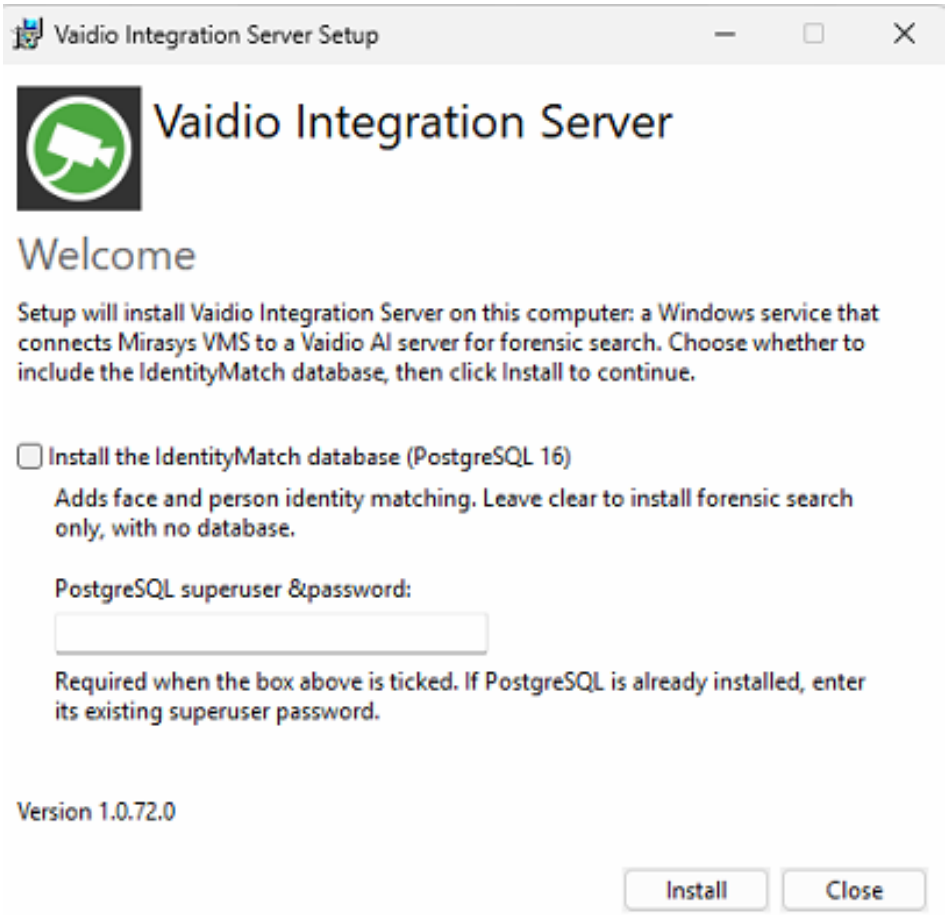
- **Der Integrationsdienst**
    - Läuft auf einem Windows-Rechner, der auf Vaidio zugreifen kann, verfügt über einen Einrichtungsassistenten und ein Kontrollkästchen zum Einbinden der IdentityMatch-Datenbankinstallation.
    - Fordern Sie die signierte Datei `VaidioIntegrationServiceSetup.exe` bei Mirasys an.
- **Das Forensic Search-Plugin**
    - Ein separates, optionales Plugin-Paket (`.spi`), das in Spotter installiert wird.
    - Fordern Sie das signierte `ToolPluginIntegrationServer.spi`-Paket bei Mirasys an.

Sie benötigen nicht beide Installationsprogramme auf demselben Rechner. In einer typischen Umgebung wird der Dienst auf einem Rechner (dem DVMS oder einem dedizierten Rechner) ausgeführt, während das Plugin auf dem Spotter-Client jedes Bedieners verwendet wird.

9.6.1 Installation des Vaidio-Integrationsdienstes

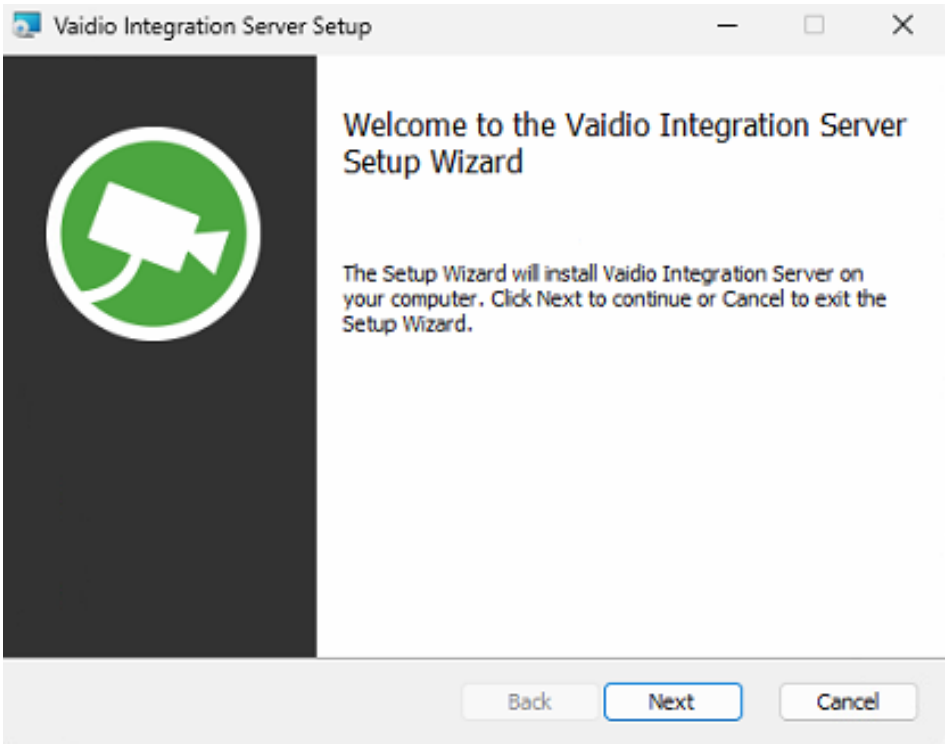
Bitte lesen Sie die Vaidio-Anforderungen durch, bevor Sie mit der Installation beginnen.

1. Klicken Sie mit der rechten Maustaste auf die Datei `VaidioIntegrationServiceSetup.exe` und wählen Sie **Als Administrator ausführen**.
2. Lassen Sie das Kontrollkästchen deaktiviert und klicken Sie auf **Installieren**, wenn keine Datenbankinstallation erforderlich ist. Wenn Sie die Datenbank installieren möchten, aktivieren Sie das Kontrollkästchen **IdentityMatch-Datenbank installieren (PostgreSQL 16)**, legen Sie das Superuser-Passwort für PostgreSQL fest und klicken Sie auf **Installieren**.
    a. Um sicherzustellen, dass Sie die für Ihre Anforderungen geeignete Option auswählen, lesen Sie bitte die Anweisungen zur optionalen Datenbanknutzung, bevor Sie mit der Installation fortfahren.
        i. Wenn Sie die Datenbankinstallation ausgewählt haben, finden Sie die Dokumentation hier.

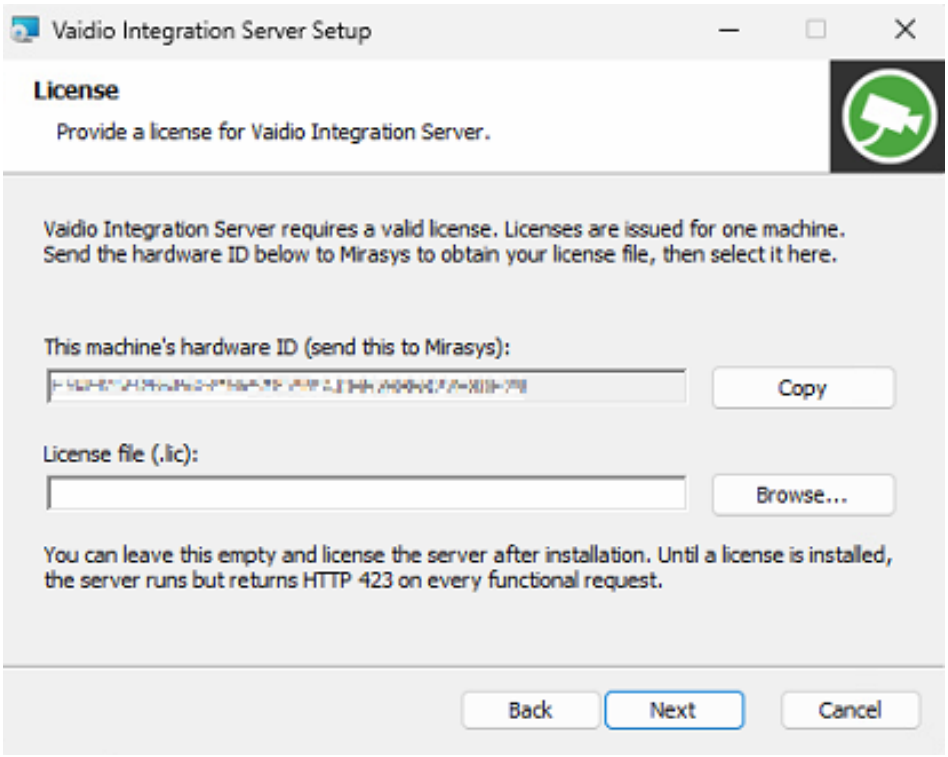


Wenn Sie auswählen, die Datenbank in die Installation einzubeziehen, bleibt der Fortschrittsbildschirm einige Minuten lang stehen, während PostgreSQL installiert wird. Das Installationsprogramm von PostgreSQL zeigt keine Informationen an und kann daher keinen Fortschritt anzeigen. **Brechen Sie die Installation nicht ab,** da ein Abbruch die PostgreSQL-Installation nicht stoppt und eine PostgreSQL-Installation zurückbleibt, die Sie manuell entfernen müssen.

1. Klicken Sie auf **Weiter**.

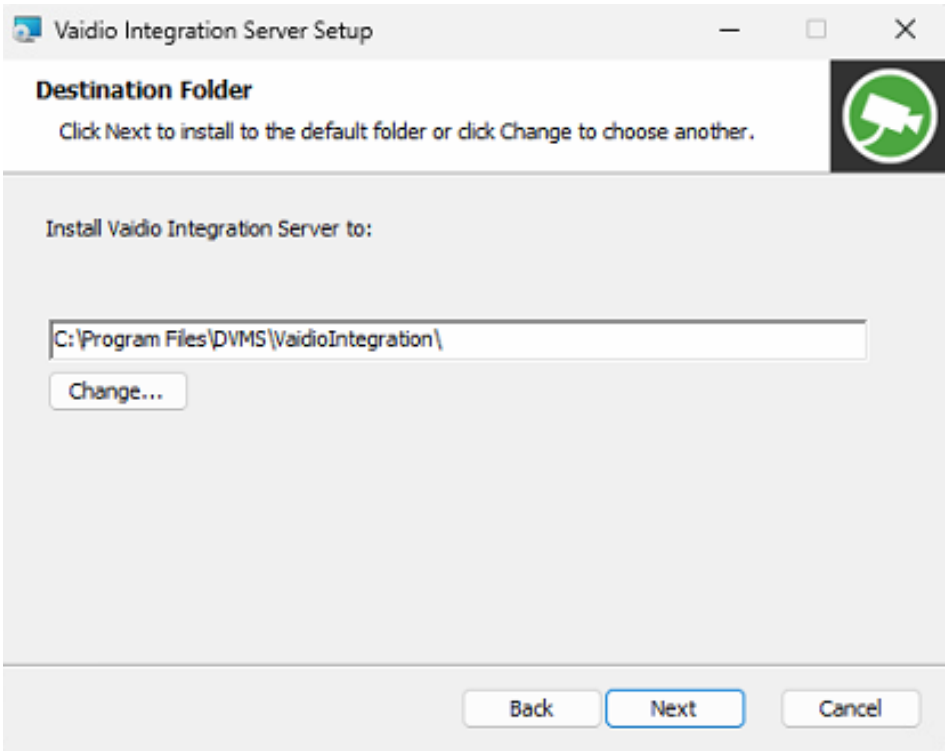


1. Wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
    a. Wenn Sie die Bedingungen nicht akzeptieren, können Sie die Installation nicht fortsetzen.
2. Führen Sie optional die Serverlizenzierung durch (dies kann auch nach der Installation erfolgen) und klicken Sie auf **Weiter**.
3.
    a. Auf dem Lizenzierungsbildschirm wird die Hardware-ID des Computers angezeigt, und Sie können die Lizenzdatei (`.lic`) auswählen.

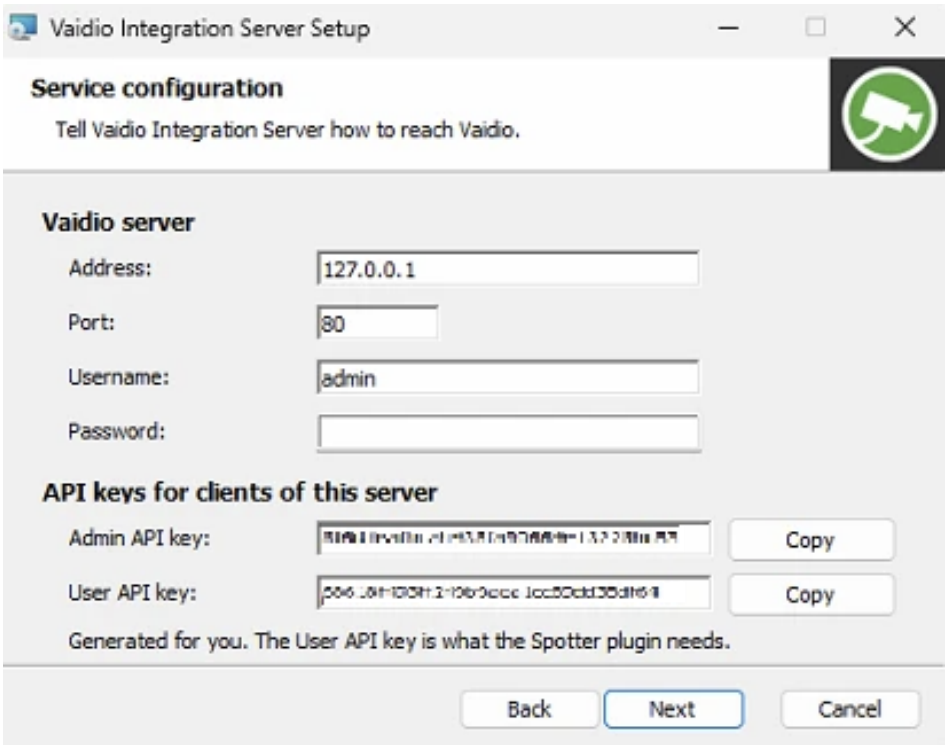


Lesen Sie die Anweisungen zur Lizenzaktivierung, falls Sie diese erst nach der Installation durchführen möchten.

1. Ändern Sie gegebenenfalls den Installationsort und klicken Sie auf **Weiter**.
    a. Der Standardinstallationsort lautet `C:\Program Files\DVMS\VaidioIntegration`.

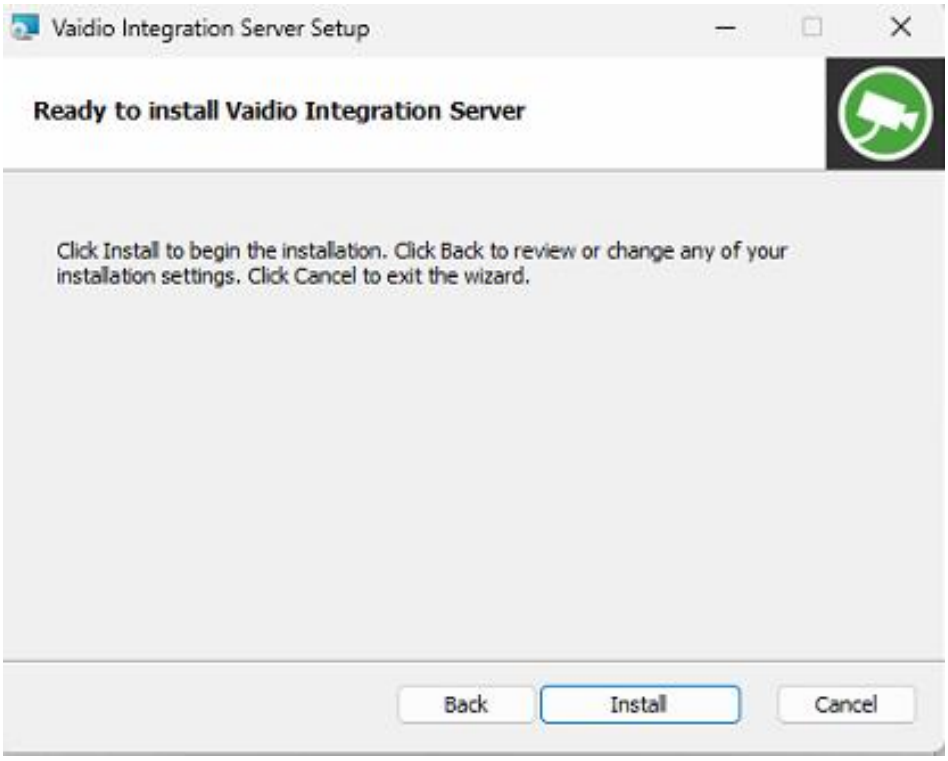


1. Geben Sie optional die Konfigurationsdaten ein (dies ist auch nach der Installation möglich) und klicken Sie auf **Weiter**.
    a. Vaidio-Adresse und -Port (voreingestellt: `127.0.0.1` und `80`)
    b. Vaidio-Benutzername und -Passwort
    c. Der Admin-API-Schlüssel und der Benutzer-API-Schlüssel

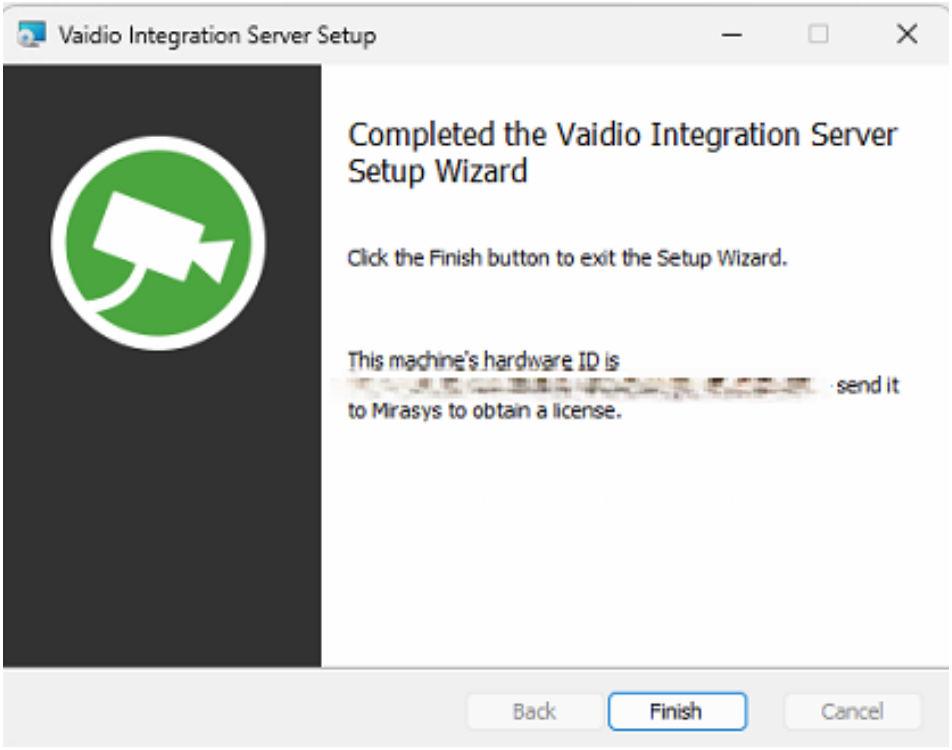


Wenn Sie die Konfigurationsdetails leer lassen, wird ein funktionsfähiger, noch nicht konfigurierter Server installiert: Der Dienst wird gestartet, öffnet seinen Port und meldet, was noch fehlt.
Weitere Informationen finden Sie unter Konfiguration nach der Installation, falls Sie die Konfiguration nach der Installation abschließen möchten.

1. Klicken Sie auf **Installieren**.



1. Klicken Sie auf **Fertig stellen**.



Nachdem die Installation abgeschlossen ist, können Sie die Installation überprüfen, um sicherzustellen, dass alles ordnungsgemäß funktioniert.

9.6.1.1 Hinzufügen der Datenbank (IdentityMatch)

Wenn Sie sich dafür entscheiden, die Datenbank in die Installation einzubeziehen (siehe Schritt 2 unter Installation des Vaidio-Integrationsdienstes), beachten Sie bitte Folgendes:

- Wenn PostgreSQL 15/16 bereits vorhanden ist, wird es erkannt und weiterverwendet; in diesem Fall muss `DB_PASSWORD` dem bestehenden Superuser-Passwort dieser Instanz entsprechen. Andernfalls wird das eingebettete PostgreSQL 16 als Dienst `AdvPostgreSql16` auf Port :5432 installiert.
- Das Installationsprogramm richtet eine Anwendungsrolle mit minimalen Berechtigungen (`vaidio`) ein, die Eigentümerin einer dedizierten Datenbank (`vaidiointegration`) ist. Sie geben lediglich das Superuser-Passwort (`DB_PASSWORD`) an; das Passwort für die Anwendungsrolle wird generiert und ausschließlich in die Verbindungszeichenfolge geschrieben.
- IdentityMatch und die Datenbank sind aktiviert; der Dienst erstellt sein Schema beim ersten Start.

Die PostgreSQL-Instanz wird möglicherweise gemeinsam mit anderen Mirasys-Diensten genutzt. Die `vaidio`-Anwendungsrolle hat nur Zugriff auf die Datenbank dieses Produkts, wodurch der Schadensumfang begrenzt wird. Konfigurieren Sie den Dienst nicht so, dass er sich als PostgreSQL-Superuser anmeldet.

`DB_HOST/DB_PORT` sind standardmäßig auf `localhost:5432` gesetzt; diese Einstellungen sollten nur überschrieben werden, wenn PostgreSQL remote betrieben wird.

9.6.1.2 Konfiguration nach der Installation

Ein nicht konfigurierter Server antwortet:

- GET /_health → **503 Unhealthy**, wobei jede fehlende Einstellung und der vollständige Pfad der zu bearbeitenden Datei aufgeführt werden.
- Jeder funktionsfähige Endpunkt → **503**, mit derselben Erklärung im Textkörper.
- GET /api/v1/version → **200** (das Plugin meldet also „nicht konfiguriert“ statt einer Versionsinkongruenz).

So schließen Sie die Konfiguration nach der Installation ab:

1. Gehen Sie zum **Startmenü → Mirasys → Vaidio-Integrationskonfiguration bearbeiten**. Dadurch wird die Datei `appsettings.Production.json` mit erhöhten Rechten im Notepad geöffnet. Sie benötigen diese Verknüpfung: Die Datei ist nur für SYSTEM und Administratoren lesbar, sodass ein normal gestarteter Notepad (selbst von einem Administrator) die Fehlermeldung „Zugriff verweigert“ anzeigt. In der Datei wird jede Einstellung in einem Kommentar am Anfang erläutert.

2. Speichern Sie die Datei und starten Sie anschließend den Dienst `ADVVaidioIntegration` über `services.msc` neu.
3. Gehen Sie zum **Startmenü → Mirasys → Vaidio Integration Health** (oder `<http://localhost:5194/_health`), um den Vorgang zu überprüfen.

Die Konfigurationsdatei ist im JSON-Format, wobei Kommentare und abschließende Kommas zulässig sind. Wenn Sie die Datei fehlerhaft belassen, startet der Server dennoch, ignoriert die Datei und meldet die Zeile und Spalte des Syntaxfehlers unter `/_health`.

9.6.1.3 Überprüfen Sie die Installation

Überprüfen Sie nach der Installation die folgenden Punkte, um sicherzustellen, dass die Installation ohne Probleme abgeschlossen wurde:

- Der Dienst `ADVVaidioIntegration` („ADV Vaidio Integration Service“) läuft (automatischer Start, LocalSystem).
- Die Dateien befinden sich unter `C:\Program Files\DVMS\VaidioIntegration`.
- Der Dienst lauscht auf Port 5194, und die eingehende Firewall-Regel „ADV Vaidio Integration Service (TCP 5194)“ ist vorhanden.
- `GET <http://localhost:5194/_health>` → `200 Healthy`, sobald Vaidio erreichbar ist und eine Lizenz vorhanden ist. (Ohne Lizenz geben funktionsfähige Endpunkte den Status 423 zurück; die Endpunkte für Status, Version und Lizenz reagieren weiterhin.)

9.6.1.4 Verbindung zu Vaidio herstellen

Die Verbindung zu Vaidio erfolgt ausschließlich über die Konfiguration (wird bei der Installation über die oben genannten Eigenschaften festgelegt oder durch Bearbeiten der Dienstkonfigurationsdatei und einen Neustart):

```
"Vaidio": { "Server": {
  "BaseUrl": "http://<vaidio-host>/",   // API port (:80, /ainvr/api). NOT :8000.
  "Username": "admin",
  "Password": "<password>"
}}
```

Verbindung überprüfen: Bei aktivierter Lizenz gibt der Aufruf von `GET /api/v1/forensic-search/cameras` die Vaidio-Kameras zurück, und der Aufruf von `GET /api/v1/license` zeigt Vaidio `IsValid: true` an, wenn die Authentifizierung bei Vaidio erfolgreich war.

9.6.1.5 Lizenz aktivierung

Eine Lizenz ist über die Hardware-ID an den Rechner gebunden und muss daher für jeden Rechner einzeln generiert werden (ausgestellt von Mirasys). So weisen Sie eine Lizenz zu:

1. **Rufen Sie die Hardware-ID ab**. Die ID ist an verschiedenen Stellen zu finden:

•

- Auf dem Lizenzbildschirm des Installationsprogramms (siehe Schritt 5 bei der Installation des Vaidio-Integrationsdeinstes), wo sie kopiert werden kann;
- In der Datei `C:\Program Files\DVMS\VaidioIntegration\License\hardware-id.txt`, die der Dienst bei jedem Start neu schreibt;
- `"C:\Program Files\DVMS\VaidioIntegration\Mirasys.IntegrationServer.exe" --hardware-id`, wodurch die ID ausgegeben wird und das Programm beendet wird;
- `GET <http://<host>>:5194/api/v1/license/hardware-id`, wofür der Admin-API-Schlüssel erforderlich ist.

Die Hardware-ID kann nicht zum Erstellen einer Lizenz verwendet werden.

1. **Senden Sie die Hardware-ID an Mirasys**, um eine `license.lic`-Datei zu erhalten.
2. **Wenden Sie die Lizenz an**. Dazu gibt es mehrere Möglichkeiten:
   - auf der Seite „Lizenz“ des Installationsprogramms, indem Sie die `.lic`-Datei auswählen
   - bei der Installation über `LICENSE_FILE=...`
   - indem Sie die Datei unter `C:\Program Files\DVMS\VaidioIntegration\License\license.lic` ablegen und den Dienst neu starten
   - indem Sie sie zur Laufzeit hochladen (Admin-API-Schlüssel): `POST /api/v1/license` (Multipart-Datei, `.lic`, ≤1 MB) (kein Neustart erforderlich)

Solange keine gültige Lizenz vorliegt, geben funktionsfähige Endpunkte den **HTTP-Status 423** zurück.

> Der Upload-Endpunkt wird abgelehnt, wenn der Dienst mit einem benutzerdefinierten Lizenzpfad konfiguriert ist. Legen Sie die Datei in diesem Fall manuell unter dem konfigurierten Pfad ab. Der Standardpfad lautet `License/license.lic`.

9.6.1.6 Kameras in Vaidio importieren (optional)

Der Dienst kann Kameras aus einem Mirasys-VMS-Kameraexport (CSV) in Vaidio massenweise registrieren. Dies ist ein Vorgang, für den ein Admin-Schlüssel erforderlich ist:

- `GET /api/v1/system/test-connection` – Funktionsprüfung des Dienstes (Benutzerschlüssel).
- `POST /api/v1/system/cameras/bulk-add` – CSV-Datei hochladen (`multipart/form-data`, `text/csv`; Admin-Schlüssel).

Die CSV-Spalten entsprechen dem Mirasys-VMS-Export (`Camera.Address`, `Camera.Port`, `Camera.Username`, `Camera.Password`, `Camera.Install.CameraType` = `RTSP` oder `Onvif`, `Camera.Name`, `StreamUrl`, `Camera.Description`, `Camera.Install.Manufacturer/Model`, `Camera.Location.Longitude/Latitude`). RTSP-

Kameras verwenden `StreamUrl` als Quelle; ONVIF-Kameras erhalten die RTSP-URI über das ONVIF-Protokoll. Überspringen Sie diesen Schritt, wenn die Kameras des Kunden bereits in Vaidio registriert sind.

9.6.1.7 Kamerakonfiguration und Zuordnung

Die von Vaidio verwendeten Kameras müssen ebenfalls im Mirasys VMS konfiguriert werden. Für jede integrierte Kamera muss die Kamerakonfiguration im Mirasys VMS mit der in Vaidio konfigurierten Kamera übereinstimmen. Der Kameraname und die Details zum Videostream müssen übereinstimmen, damit die Integration eine Vaidio-Erkennung der richtigen Mirasys VMS-Kamera und -Aufzeichnung zuordnen kann.

Für Spotter-Funktionen, die VMS-Aufzeichnungen nutzen, ist eine korrekte Kameratoeweisung erforderlich, darunter:

- Öffnen eines forensischen Suchergebnisses in der Wiedergabe
- Anzeigen der zu einer Erkennung gehörenden Aufzeichnung
- Erstellen und Überprüfen von Storyboards
- Verfolgen von Erkennungen über mehrere Kameras hinweg
- Exportieren von Videoclips
- Exportieren von Schnappschüssen oder anderem Beweismaterial
- Öffnen synchronisierter Aufzeichnungen von zugehörigen Kameras

Vaidio stellt die Metadaten für die KI-Erkennung und die forensische Suche bereit, während das Mirasys-VMS das aufgezeichnete Videomaterial für die Wiedergabe, die Erstellung von Storyboards und den Export bereitstellt.

> Wenn eine Kamera in Vaidio vorhanden ist, aber in Mirasys VMS nicht korrekt konfiguriert wurde, wird die Erkennung möglicherweise dennoch im Plugin „Forensic Search“ angezeigt, Spotter kann die entsprechende Aufzeichnung jedoch möglicherweise nicht finden oder öffnen.

9.6.2 Installation und Konfiguration des Forensic Search-Plugins in Spotter

Das `.spi`-Paket wird im System Manager installiert, und die Spotter-Clients erkennen es automatisch. Anschließend kann es auf den Dienst verwiesen werden.

Beim Öffnen der Registerkarte überprüft das Plugin die Serverversion und zeigt eine Upgrade-Meldung an, falls der Server zu alt ist. Andernfalls stellt es über die konfigurierte Adresse und den API-Schlüssel eine Verbindung zur REST-API des Dienstes her.

9.6.2.1 Installieren Sie das Plugin-Paket (System Manager)

> Die Installation ist nur einmal pro System erforderlich, nicht einmal pro Client.

1. Laden Sie die Datei `ToolPluginIntegrationServer.spi` von Mirasys herunter und kopieren Sie sie auf den Rechner, auf dem System Manager ausgeführt wird.
2. Öffnen Sie in System Manager die Registerkarte **System** und wählen Sie **Client-Plugin installieren**.
3. Klicken Sie auf **Neues Client-Plugin hinzufügen**.
4. Wählen Sie die `.spi`-Datei aus. System Manager überprüft die Signatur des Pakets und lädt es in den SMServer-Plugin-Speicher hoch.
5. **Forensic Search** wird nun in der Liste der installierten Plugins angezeigt.

Spotter-Clients laden das Plugin bei Bedarf vom SMServer herunter, sodass die Benutzer lokal nichts installieren müssen. Ein bereits ausgeführter Client muss neu gestartet werden, bevor die Registerkarte angezeigt wird.

Wenn das Paket abgelehnt wird, ist die Datei beschädigt oder unvollständig. Fordern Sie eine neue Kopie an, anstatt es erneut mit derselben Datei zu versuchen.

9.6.2.2 Richten Sie das Plugin auf den Dienst aus (zentralisierte Einstellungen im System Manager)

Das Plugin liest seine Verbindungsdaten aus den zentralisierten Einstellungen von Spotter, die einmalig im **System Manager** konfiguriert werden:

1. Stellen Sie sicher, dass **Forensic Search** im System Manager installiert bzw. registriert ist (starten Sie den SMServer neu, falls es nicht angezeigt wird).
2. Öffnen Sie die Registerkarte **Profile** → wählen Sie das aktuelle Profil aus.
3. Ändern Sie auf der Registerkarte **Geräte** die Quelle auf „Client-Plugins“, wählen Sie links **Forensic Search** und rechts eine Gerätegruppe aus und fügen Sie diese dem Profil hinzu.

Forensic Search muss auf der zweiten Ebene des Profilbaums als direktes untergeordnetes Element des Ordners `Plugins` abgelegt werden. Es darf sich **nicht** in einem Unterordner befinden.

1. Klicken Sie auf die Schaltfläche „→“, füllen Sie die Einstellungsfelder aus und klicken Sie auf **OK**.

Feld	Wert
Adresse	Hostname oder IP-Adresse des Diensthosts, z. B. `192.168.49.183` (ohne `<http://>`oder sonstige Präfixe).
Port	`5194` (die Standard-Portnummer des Dienstes).
API-Schlüssel	Der Standard-API-Schlüssel für Benutzer (der bei der Installation als `USER_API_KEY` festgelegte Wert). Verwenden Sie den Admin-Schlüssel nur, wenn Administratorvorgänge erforderlich sind.

Es reicht aus, die Verbindung einmal zu konfigurieren. Jeder Spotter-Client in diesem Profil übernimmt dann die zentralen Einstellungen.

Zu den API-Schlüsseln: In älteren Dokumentationen wurden feste Standardschlüssel veröffentlicht. Diese sind inzwischen **veraltet und unsicher** (da sie nun öffentlich zugänglich sind). Verwenden Sie die Schlüsselwerte, die der Betreiber bei der Installation festgelegt hat.

9.7 FUNKTIONEN VON VAIDIO

Das Plugin bietet folgende Hauptfunktionen:

- Gesichtssuche
- Objektsuche und Suche nach ähnlichen Objekten
- Kennzeichensuche
- kamerübergreifende Verfolgung
- Live-Überwachung
- Wiedergabe der Suchergebnisse
- Erstellung von Storyboards
- Export von Videos und Schnappschüssen

Weitere Informationen zu den einzelnen Funktionen finden Sie weiter unten auf dieser Seite.

9.7.1 So öffnen Sie das Plugin „Forensic Search“

1. Starten Sie Spotter
2. Öffnen Sie **Forensic Search** unter „Plugins“
3. Wählen Sie die gewünschte Suchfunktion aus
4. Wählen Sie die Kameras, den Zeitbereich und weitere verfügbare Suchkriterien aus
5. Starten Sie die Suche

Beim Öffnen des Plugins wird die Verbindung zum Integrationsdienst überprüft und sichergestellt, dass die Versionen des Plugins und des Dienstes kompatibel sind. Wenn das Plugin keine Verbindung zum Integrationsdienst herstellen kann oder die Versionen nicht übereinstimmen, wird eine Fehlermeldung angezeigt.

9.7.2 Auswahl von Kameras und Zeiträumen

Forensische Suchvorgänge werden anhand von aufgezeichnetem Videomaterial und Metadaten durchgeführt, die über das angeschlossene Vaidio-System verfügbar sind. Vor dem Start einer Suche kann der Bediener eine oder mehrere Kameras, eine Start- und Endzeit sowie suchartenspezifische Kriterien auswählen. Durch die Einschränkung der Kameraauswahl und des Zeitraums lässt sich die Anzahl der Ergebnisse reduzieren und die Suchleistung verbessern.

Die Suchergebnisse hängen von den für die ausgewählten Kameras konfigurierten Analysen ab. Für die Suche nach Kfz-Kennzeichen muss beispielsweise die Kennzeichenerkennung für die entsprechenden Kameras aktiviert sein.

9.7.3 Überprüfen der Suchergebnisse

Suchergebnisse werden als erkannte Ereignisse oder übereinstimmende Objekte angezeigt. Je nach Suchtyp kann ein Ergebnis Folgendes enthalten:

- Ein Miniaturbild
- Datum und Uhrzeit der Erkennung
- Kameraname
- Informationen zur Übereinstimmung oder Ähnlichkeit
- Objektklassifizierung
- Kfz-Kennzeichen
- Zusätzliche Vaidio-Metadaten

Durch Auswahl eines Ergebnisses kann der Bediener die zugehörige Aufzeichnung in Spotter überprüfen. Die Aufzeichnung wird zum Zeitpunkt der Erkennung oder kurz davor geöffnet, sodass der Bediener das Ereignis im Kontext untersuchen kann.

9.7.4 Gesichtssuche (Face search)

Die Gesichtssuche kann verwendet werden, um Auftritte einer Person in aufgezeichneten Videos zu lokalisieren. Eine Suche kann anhand eines hochgeladenen Referenzbildes, eines in einem bestehenden Suchergebnis erkannten Gesichts oder eines von der Integration unterstützten erkannten Gesichtsdeskriptors gestartet werden.

Der Bediener wählt das Referenzgesicht, die Kameras und den Zeitbereich aus und startet anschließend die Suche. Die Ergebnisse zeigen Gesichter an, die Vaidio als visuell ähnlich zum ausgewählten Referenzgesicht erkennt. Der Bediener kann ein Ergebnis auswählen, um:

- das erkannte Gesicht anzuzeigen
- die Kamera und den Erkennungszeitpunkt einzusehen
- die entsprechende Aufzeichnung zu öffnen
- das erkannte Gesicht als Grundlage für eine weitere Suche zu verwenden

- die kamerübergreifende Verfolgung zu starten, sofern diese unterstützt wird

Die Genauigkeit der Gesichtssuche wird durch Bildqualität, Kamerawinkel, Beleuchtung, Entfernung, Gesichtsbedeckungen und die Auflösung der Quelle beeinflusst. Die Ergebnisse der Gesichtssuche sollten als Hilfsmittel bei Ermittlungen und nicht als alleinige Grundlage für die Identifizierung einer Person herangezogen werden.

9.7.5 Objektsuche (Object search)

Die Objektsuche kann verwendet werden, um Personen, Fahrzeuge oder andere unterstützte Objektkategorien in aufgezeichneten Videos zu lokalisieren. Die verfügbaren Objekttypen und Filter hängen von der Vaidio-Analytics-Konfiguration und den vom Plugin bereitgestellten Optionen ab.

Beispiele hierfür sind Personen, PKWs, Transporter, Busse, LKWs, Motorräder und Fahrräder. Je nach Konfiguration stehen möglicherweise zusätzliche Filter für Objektfarbe, Kleidungsfarbe, Fahrzeugtyp, Bewegungsrichtung, Kamera und Erkennungszeit zur Verfügung.

Der Bediener wählt die gewünschten Kriterien, Kameras und den Zeitbereich aus und startet die Suche. Durch Auswahl eines Ergebnisses wird die entsprechende Mirasys-VMS-Aufzeichnung in Spotter geöffnet.

9.7.5.1 Suche nach ähnlichen Objekten (Similar-object search)

Ein erkanntes Objekt kann als Referenz für die Suche nach optisch ähnlichen Objekten verwendet werden. Nachdem beispielsweise ein Fahrzeug von einer Kamera erfasst wurde, kann der Bediener dieses Fahrzeug als Referenz für eine neue Suche über andere Kameras und Zeiträume hinweg nutzen. Die Ähnlichkeitsergebnisse werden von der KI generiert und sollten anhand der Originalaufnahmen überprüft werden.

9.7.6 Kfz-Kennzeichen-Suche (License plate search)

Die Kfz-Kennzeichen-Suche dient dazu, Fahrzeuge anhand der von Vaidio erfassten Kennzeicheninformationen zu lokalisieren. Der Benutzer kann ein vollständiges oder teilweises Kfz-Kennzeichen eingeben und die zu durchsuchenden Kameras sowie den Zeitbereich auswählen. Die unterstützten Abgleichoptionen hängen vom Plugin und der Vaidio-Konfiguration ab.

Die Ergebnisse können den erkannten Kennzeichentext, Datum und Uhrzeit der Erfassung, den Kameranamen, eine Miniaturansicht des Fahrzeugs oder des Kennzeichens sowie einen Link zur entsprechenden Aufzeichnung enthalten.

Die Erkennungsgenauigkeit wird durch die Kameraposition, Bewegungsunschärfe, die Sichtbarkeit des Kennzeichens, die Beleuchtung, die Wetterbedingungen und das Kennzeichenformat beeinflusst. Das Personal sollte das erkannte Kennzeichen durch Überprüfung der Originalaufzeichnung bestätigen

9.7.7 Kameraübergreifende Verfolgung (Cross-camera tracking)

Die kameraübergreifende Verfolgung kann genutzt werden, um eine Person über mehrere Kameras hinweg zu verfolgen. Die Verfolgung kann in der Regel ausgehend von einem Ergebnis der Gesichts- oder Objektsuche gestartet werden.

Der Bediener wählt eine erkannte Person aus und startet eine kamerenübergreifende Suche. Vaidio sucht daraufhin innerhalb des ausgewählten Zeitraums nach ähnlichen Erkennungen von anderen Kameras. Die Ergebnisse können chronologisch dargestellt werden und den Kameranamen, den Erkennungszeitpunkt, eine Miniaturansicht des Motivs, Ähnlichkeitsinformationen sowie den Zugriff auf die zugehörige Aufzeichnung enthalten.

Die kamerübergreifende Verfolgung basiert auf visueller Ähnlichkeit und Erkennungsmetadaten. Es kann nicht garantiert werden, dass alle Ergebnisse dieselbe Person darstellen. Die Bediener sollten die gesamte Sequenz und die Quellaufnahmen überprüfen, um die Genauigkeit sicherzustellen.

9.7.8 Live-Monitor (Live monitor)

Der Live-Monitor zeigt kürzlich erkannte Gesichter und Kennzeichen von Kameras an, die an das Vaidio-System angeschlossen sind. Er kann verwendet werden, um aktuelle Erkennungsergebnisse zu beobachten, ohne wiederholt eine Suche im Archiv durchführen zu müssen. Zu den angezeigten Informationen gehören:

- Kürzlich erkannte Gesichter
- Kürzlich erkannte Kennzeichen
- Kameraname
- Erkennungszeitpunkt
- Miniaturansicht der Erkennung
- Erkannter Kennzeichentext

9.7.9 Wiedergabe und Storyboard

Die Suchergebnisse können auch dazu verwendet werden, relevante Ereignisse in einem Storyboard zusammenzufassen. Ein Storyboard hilft dem Bediener dabei, ausgewählte Erkennungen und Aufzeichnungen in einer chronologischen Untersuchungssequenz zu ordnen. Die Storyboard-Funktionalität hängt von der korrekten Kameratoeweisung, der Verfügbarkeit von Aufzeichnungen, der Spotter-Version und den Berechtigungen des Bedieners ab.

9.7.10 Exportieren von Videomaterial

Relevantes Videomaterial kann nach der Überprüfung eines Suchergebnisses exportiert werden. Das „Forensic Search“-Plugin identifiziert das Ereignis und öffnet die zugehörige Mirasys-VMS-Aufzeichnung. Der eigentliche Videoexport erfolgt über die Standard-Exportfunktion von Spotter.

1. Wählen Sie ein Suchergebnis aus.

2. Öffnen Sie die entsprechende Aufzeichnung in Spotter.
3. Bestätigen Sie die Start- und Endzeit des gewünschten Materials.
4. Verwenden Sie die Exportfunktion von Spotter, um den Export zu erstellen.
5. Wählen Sie das verfügbare Exportformat und den Speicherort aus.
6. Schließen Sie den Export ab.

Je nach Spotter-Konfiguration und Benutzerberechtigungen kann der Export Videos von einer oder mehreren Kameras, ein ausgewähltes Zeitintervall, unterstützte Beweismittel- oder Standard-Videoformate, Schnappschüsse sowie zugehörige Verifizierungsinformationen umfassen.

Die Verfügbarkeit des Exports wird durch VMS-Berechtigungen gesteuert. Benutzer ohne Exportberechtigung können Ergebnisse einsehen, aber keine Aufzeichnungen exportieren.