MIRASYS

Mirasys Administratorhandbuch

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

1 CONTENTS

2 Übersicht über dieses Handbuch 10
3 Technischer Support 10
4 Was ist die Mirasys VMS-Software? 10
4.1 Was beinhaltet ein System? 10
4.2 VMS-Server 11
4.3 Hauptserver 11
4.4 Client-Programme 12
4.5 Netzwerkanforderungen 12
4.6 Auswahl der geeigneten Hardware 12
4.6.1 Warum Mirasys-Hardware? 13
4.6.2 Server 13
4.6.3 Beispielkonfigurationen 13
4.6.4 Client 16
4.6.5 Server- und Client-Kombinationen 17
5 Betriebssystemkompatibilität 19
6 Konfigurieren des Systems 20
7 Einloggen 20
7.1 System Manager sperren 22
7.2 Zugang zur Auswahl der Serveradresse 22
8 Management-Benutzeroberfläche 23
8.1 Menüleiste 24
8.2 Instandhaltung 24
8.3 Hilfe 24
8.4 Exportieren von Systemkamerainformationen in die CSV-Datei 24
9 System 26
9.1 Führen Sie einen der folgenden Schritte aus, um ein Werkzeug zu öffnen 27
9.2 Systemeinstellungen 28
9.2.1 Allgemeine Systemeinstellungen 29
9.2.2 Einstellungen für die Anzeige von Stationen konfigurieren 30
9.2.3 Email Einstellungen 31

9.2.4 Befehlseinstellungen 33
9.2.5 VMS-Serveradressen ändern 34
9.2.6 Systemadressen 36
9.2.7 Axis One-Click-Dispatcher-Einstellungen 38
9.2.8 VMS-Server aktualisieren 44
9.2.9 Einstellungen für die Meldung von Vorfällen 46
9.2.10 Einstellungen für Speicherschließfach 53
9.2.11 Storage Locker Einstellungen 65
9.2.12 Einstellungen für die List Management 69
9.2.13 Einstellungen für den Objektdatenspeicher 86
9.3 Sicherung 87
9.3.1 Protokolle exportieren 87
9.3.2 Backup-Einstellungen 92
9.3.3 Einstellungen zurücksetzen 94
9.4 Überwachung 98
9.4.1 Audit-Protokoll 98
9.4.2 SM-Server-Diagnose 100
9.4.3 Serverdiagnose 101
9.5 Lizenzen 105
9.5.1 So erhalten Sie einen Lizenzschlüssel 105
9.5.2 Lizenzdetails 107
9.5.3 Lizenzverwaltung 107
9.6 Wachhund 108
9.6.1 Watchdog-Einstellungen 108
9.6.2 Watchdog-Protokoll 109
9.7 Add-Ins 110
9.7.1 Mirasys Kamera-Treiber 110
9.7.2 Installieren externer Treiberpakete 134
9.7.3 Treiberinstallation und -verwendung 135
9.7.4 Installieren von Metadatentreibern 192
9.7.5 Client-Treiber installieren 192

9.7.6 Client-Plugin installieren 192
10 VMS-Servers 195
10.1 Um auf die Einstellungen zuzugreifen, führen Sie einen der folgenden Schritte aus: 195
10.2 Allgemein 195
10.2.1 Multicast-Adresse 197
10.2.2 VMS-Server-Failover-Einstellungen 197
10.2.3 Failover verzögern, um Datenverlust zu vermeiden 198
10.3 Port-Weiterleitung 199
10.3.1 Die Grundidee bei der Portweiterleitung besteht darin, dass auf einen oder mehrere VMS-Server oder Hauptserver hinter einem Router zugreifen kann, der Network Address Translation (NAT) durchführt. 199
10.3.2 Normalerweise tritt diese Situation auf, wenn sich der Client außerhalb des Netzwerks befindet und auf Server innerhalb eines Unternehmensnetzwerks zugreifen muss. 199
10.3.3 Automatische Router-Konfiguration 199
10.3.4 Einzelner Server hinter Router 200
10.3.5 Mehr als ein Server hinter dem Router 200
10.3.6 Mehr als ein Server auf mehreren Sites 201
10.4 Hardware 202
10.4.1 Video (Hardware) 204
10.4.2 Audio (Hardware) 218
10.4.3 Geräteeinstellungen 218
10.4.4 Hinzufügen von Kameras über eine CSV-Datei 219
10.5 Hinzufügen und Entfernen von VMS-Servern 223
10.5.1 So fügen Sie dem System einen Server hinzu (Aufzeichnungsserver): 223
10.5.2 So entfernen Sie einen Server aus dem System: 224
10.5.3 Verbindungsstatus: 225
10.5.4 HINWEIS: 225
10.6 Suche in den VMS Server-Einstellungen 225
10.6.1 Suche in der Registerkarte VMS Server-Einstellungen 225
10.6.2 Eingrenzung der Suche über die Registerkarte VMS Server-Einstellungen 226
10.6.3 Suche in individuellen Einstellungen 227
10.7 Kameras 228

10.7.1 Kameraeinstellungen enthalten Einstellungen für: 229
10.7.2 Kameraeinstellungen 230
10.7.3 Bewegungserkennung 240
10.7.4 VCA-Funktionen 249
10.7.5 Privatsphäre 250
10.7.6 Einstellungen für die License Plate Recognition (LPR) 254
10.7.7 Einstellungen für die Face Recognition 258
10.7.8 Einstellungen für die Object Recognition (OR) 262
10.8 VCA-Einstellungen 266
10.9 Audio 266
10.9.1 Hinzufügen, Bearbeiten und Entfernen von Audiogeräten 266
10.9.2 Audio Einstellungen 267
10.9.3 Allgemeine Einstellungen (Audio) 268
10.9.4 Audioerkennung 271
10.9.5 Planer (Audio) 272
10.10 Digitale E/A 273
10.10.1 Digitale E/A-Einstellungen 273
10.10.2 LoopBack-E/A 277
10.10.3 Logische E/A 278
10.10.4 Countdown-E/A 283
10.10.5 Geplante E/A 285
10.10.6 Eigenschaften 287
10.10.7 UniversalOutputDriver 288
10.11 Alarme (VMS-Servers) 290
10.11.1 Alarmeinstellungen 290
10.11.2 Benutzerdefinierte Alarmauslöser 309
10.12 Speicherung 316
10.12.1 Speicherplatz hinzufügen 316
10.12.2 Speichereinstellungen für Video-, Audio- und Textdaten 318
10.12.3 Automatisches Löschen von Video-, Audio- und Textdaten 319
10.12.4 Archivierung 320

10.12.5 Verwenden Sie den Betriebssystem-Cache 322
10.12.6 Aktivitätsdaten-Cache 323
10.13 Textkanaleinstellungen 324
10.13.1 So fügen Sie Textdatenkanäle hinzu: 324
10.13.2 So bearbeiten Sie Textkanäle: 326
10.13.3 So entfernen Sie alle Textkanäle, die denselben Treiber verwenden: 326
11 Profile 327
11.1 So fügen Sie ein Profil hinzu: 329
11.2 Ein bestehendes Profil duplizieren 331
11.3 Automatische Profilaktualisierungen 332
11.3.1 Automatische Profilaktualisierungen aktivieren 332
11.3.2 Automatische Profilaktualisierungen aktiviert 332
11.3.3 Automatische Profilaktualisierungen deaktiviert 332
11.4 Geräteprofil-Einstellungen 333
11.4.1 Geräte 333
11.4.2 Ausgewählte Geräteeigenschaften 334
11.4.3 Ausgewählte Gerätenodes sortieren 337
11.4.4 PTZ-Kamerasteuerungsprofil-Einstellungen 337
11.4.5 PTZ-Steuerung 337
11.4.6 Optionen des Gerätefensters für Textkanäle 338
11.4.7 Zeigen Sie die neuesten Textdaten oben an 338
11.4.8 Kopfzeile anzeigen 338
11.4.9 Benutzerdefinierte Ereignisse anzeigen 338
11.4.10 Benutzerdefinierte Ereignisse in der Textdatenliste anzeigen 338
11.4.11 Die Anzahl der Zeilen 338
11.4.12 Hinzufügen von Gerätegruppen zur Liste des ausgewählten Geräts 338
11.4.13 Alphabetisch sortieren 342
11.4.14 Client-Plugins 342
11.5 Alarme – Profileinstellungen 345
11.5.1 Bearbeiten profilspezifischer Alarmeinstellungen 345
11.5.2 So fügen Sie Alarme zu einem Profil hinzu: 345

11.5.3 So bearbeiten Sie profilspezifische Alarmbenutzerrechte: 345
11.6 Kartenprofil-Einstellungen 346
11.6.1 Hinzufügen von Karten zu Profilen 349
12 Benutzer 350
12.1 Benutzer abmelden 350
12.2 So melden Sie einen Benutzer ab: 350
12.3 Benutzer überwachen 350
12.4 Benutzergruppe 351
12.4.1 Die Benutzergruppe definiert, auf welche Mirasys VMS-Anwendungen die Benutzergruppe Zugriff hat und welche Art von Berechtigungen die Benutzergruppe in Bezug auf die Anwendungen hat. 351
12.4.2 Benutzerregeln 351
12.4.3 Erstellen einer kundenspezifischen Benutzergruppe 374
12.4.4 Zwei-Faktor-Authentifizierung 376
12.4.5 Domänenbasierte Benutzergruppen (Active Directory) 379
12.4.6 Aktive Stunden - Zeitplan für den Zugang von Benutzergruppen 381
12.5 Erstellen eines kundenspezifischen Benutzers 385
12.5.1 Identifizierung der Benutzer durch einen von der Anmelde-ID getrennten Benutzernamen 386
12.5.2 Hinzufügen eines öffentlichen Benutzernamens im System Manager 386
12.5.3 Anzeige eines öffentlichen Benutzernamens für den Benutzer in Spotter 388
12.5.4 Öffentlicher Benutzername im Spotter-Web 389
12.6 Die Benutzerkontoeinstellungen enthalten die folgenden Optionen: 389
12.7 Deaktivieren oder Aktivieren eines Benutzerkontos 390
13 ThruCast-Streaming 391
13.1 Vom Server zum Client streamen 391
13.2 Von der Kamera direkt zum Client streamen 392
13.3 Unterstützte Kameras 392
13.4 Netzwerkoptimierung 393
13.5 Multistreaming und ThruCast für Netzwerkoptimierung und -speicherung 395
13.5.1 Auswirkungen von ThruCast auf die Bildverzögerung 395
13.5.2 Von ThruCast Streaming nicht unterstützte Funktionen 395
13.5.3 Lizenzen 396
13.5.4 Mehrere Zuschauer 396

13.5.5 Client-Treiber installieren 396
13.5.6 Multi-Streaming konfigurieren 396
13.5.7 ThruCast-Standardeinstellung 397
13.6 Verwenden von ThruCast 397
14 Failover-Server 399
14.1 Failover-Funktionalität 399
14.2 Mindestanforderungen 400
14.3 VMS-Serverrollen 400
14.3.1 VMS-Serverrolle FAILOVER 400
14.3.2 VMS-Server-Rolle DEFEKT 400
14.4 Starting point 401
14.4.1 Aktivieren des VMS-Failover-Servers zum Aufzeichnungsserver 401
14.4.2 FAILOVER-Server hinzufügen 403
14.5 FAILOVER-Auslösebedingungen 406
14.6 FAILOVER-Prozess 406
14.7 MINDESTENSZENARIO FÜR FAILOVER 407
14.8 FAILOVER-SZENARIO 2 407
14.9 FAILOVER-SZENARIO 3 408
14.10 Wiederherstellen des festen Servers im System 408
14.11 Dauer der Materialkopie nach dem Failback – Testergebnisse 408
14.11.1 Testaufbau 408
14.11.2 Testergebnisse 409
15 Kurzanleitung für Mirasys VMS 409
15.1 Anmeldung bei Mirasys System Manager 410
15.2 Ändern der Sprache der Benutzeroberfläche 410
15.3 Hinzufügen von IP-Kameras zum System 412
15.3.1 Kameras einzeln hinzufügen 412
15.3.2 Mehrere Kameras gleichzeitig hinzufügen 415
15.4 Überprüfen des Referenzbildes 415
15.5 Benennen der Kameras und Konfigurieren von Auflösung und Bildrate 416
15.6 Testen der Bewegungserkennung 417

15.7 Konfigurieren der Bewegungserkennung 418
15.7.1 Bewegungserkennungsmasken bearbeiten 418
15.8 Konfigurieren von Bewegungserkennungsmasken im Kalender 420
15.9 Konfigurieren der Speichereinstellungen 421
15.10 Erstellen eines Profils für den Kunden 423
15.11 Erstellen einer Benutzergruppe für den Kunden 426
15.12 Erstellen eines Benutzerkontos für den Kunden und Hinzufügen zur Benutzergruppe des Kunden 428
15.13 Testen des Benutzerkontos 429

2 Übersicht über dieses Handbuch

Dieses Handbuch richtet sich an diejenigen, die ein Mirasys-System einrichten.
Es zeigt, wie Server zum System hinzugefügt und ihre Einstellungen geändert, Benutzerkonten und Benutzerprofile hinzugefügt und das System überwacht werden.

3 Technischer Support

Bei technischen Support- und Garantiefragen wenden Sie sich bitte an den Systemlieferanten.

4 Was ist die Mirasys VMS-Software?

Die Mirasys-Software ist ein verteiltes digitales Videoverwaltungssystem (VMS oder DVMS) für Video- und Audioüberwachungsanwendungen.
Die Software kann Echtzeit- und aufgezeichnete Video-, Audio- und Textdaten überwachen und PTZ-Kameras, E/A-Geräte und IP-Kameras steuern.
Die Software unterstützt Systeme, die aus analogen oder digitalen Überwachungskameras bestehen, und unterstützt die Erstellung analoger, digitaler oder hybrider (sowohl analoger als auch digitaler) Überwachungssysteme.
Eine zentralisierte Überwachungssystemdomäne kann aus bis zu 150 lokalen oder entfernten VMS-Servern bestehen.
Mirasys Die Software wird separat verkauft und ist Teil der Mirasys-Videoverwaltungssysteme, die sowohl aus der Software als auch aus der VMS-Serverhardware bestehen.
Bitte wenden Sie sich an Ihren Mirasys-Händler, um Informationen zu Mirasys-Software oder -Hardware zu erhalten.

4.1 Was beinhaltet ein System?

Das Mirasys-System besteht aus diesen Komponenten:

- 1-150 VMS Servers
    - **Hauptserver** (dedizierter Server – empfohlen –, einer der Videoaufzeichnungs-VMS-Server oder der einzige Server in einer Einzelserver-, nicht vernetzten Umgebung)
    - **VMS Server** („Aufzeichnungsserver“, wenn das System aus mehreren Servern besteht)
- Client-Anwendungen
    - Mirasys System Manager
    - Mirasys Spotter
    - Mirasys Spotter Web

- Mirasys Spotter Mobile

4.2 VMS-SERVER

Die VMS-Server zeichnen Video und Audio von mehreren Kameras und Audiokanälen auf und schreiben die Daten auf ein Speichergerät.
Sie können mit den Programmen System Manager und Spotter lokal oder über ein Netzwerk auf einen VMS-Server zugreifen und die Serverfunktionalität über das Spotter-Diagnose-Plugin überwachen .
Ein Server ist ein Computer mit Speicher, dem Windows-Betriebssystem und der installierten VMS-Software mit den erforderlichen Treibern.

An einen VMS-Server können mehrere Geräte angeschlossen werden:

- PTZ (Dome) Kameras und Tastaturen
- Externe Geräte, wie Sensoren, an die digitalen Eingänge
- Externe Geräte wie Türen, Lichter und Tore, die an digitale Ausgänge angeschlossen sind
- Spezielle integrierte Geräte wie Radar, IoT-Gerät oder 3rd-Party-System
- Speicher- oder Backup-Einheit (z. B. NAS, SAN oder RAID)

4.3 HAUPTSERVER

In einem vernetzten System muss einer der Server als Hauptserver eingerichtet werden.
Ein Hauptserver ist der zentrale Server eines Überwachungssystems.
Alle anderen VMS-Server stellen eine Verbindung zu ihm her, und alle Clientanwendungen kommunizieren über den Hauptserver.
Wenn der System nur einen Server enthält, dann ist dieser Server der Hauptserver.
Wenn es mehr als einen Server gibt, kann der Hauptserver frei eingestellt werden.
Es wird empfohlen, dass der Hauptserver nur für diesen Zweck in einem umfangreicheren System ein dedizierter Server ist .

HINWEIS: Auf Hauptservern muss *SQL Server Express 2014* oder ein anderer *Microsoft SQL Server 2014* installiert sein.

Der Hauptserver macht diese Dinge:

- Es überprüft die Identität aller Programme und Benutzer, die versuchen, sich am System anzumelden (Authentifizierung).
- Es speichert alle Systemkonfigurationsdaten.
- Es speichert alle Benutzerdaten.
- Es überwacht das System.

- Es synchronisiert die Uhren auf allen Servern.
- Es generiert Berichte.
- Es speichert Watchdog-Ereignisse.
- Es speichert Alarme.
- Es speichert Audit-Trails.

4.4 Client-Programme

Systemadministratoren verwenden das **System Manager**-Programm für diese Aufgaben:

- Konfigurieren der Server.
- Hinzufügen von Benutzerkonten und Benutzerprofilen.
- Überwachung des Systems.

Systembetreiber verwenden die **Spotter**-Anwendung für:

- Überwachen Sie Echtzeit- und aufgezeichnetes Video und Audio
- Steuern Sie digitale I/O-Schalter und PTZ-Kameras
- Exportieren Sie Video- und Audioclips auf lokale Medien
- Empfangen und Bearbeiten von Alarmbenachrichtigungen
- Erstellen Sie Videomatrizen mit der optionalen, separat erhältlichen Agile Video Matrix (AVM)-Software
- Verwenden Sie andere Plugins wie Grafana-Berichterstellung oder Listenverwaltung

4.5 Netzwerkanforderungen

Die Netzwerkanforderungen gelten für Systeme, bei denen Benutzer über ein Netzwerk auf die Server zugreifen.

4.6 Auswahl der geeigneten Hardware

Die Mirasys VMS-Software ist so konzipiert, dass sie auf jeder Hardware läuft. Die Mirasys VMS-Hardwarelösungen verbinden die Zuverlässigkeit der Mirasys VMS-Software mit sorgfältig ausgewählten Komponenten, die speziell für die Anforderungen von Videoüberwachungsumgebungen entwickelt wurden. Jede Hardwarekonfiguration ist auf Stabilität, Leistung und den langfristigen Einsatz in sicherheitskritischen Installationen optimiert.

Die unterstützten Betriebssysteme sind hier aufgeführt: https://documentation.mirasys.com/about-mirasys/about/supported-os

Die aktuellsten Leistungsmessungen im Zusammenhang mit unseren Software-Services finden Sie im KI-Leitfaden.

Wenn Sie Hilfe bei unserer Hardware oder bei der Auswahl Ihrer eigenen benötigen, wenden Sie sich bitte an unseren Vertrieb: https://www.mirasys.com/de/contact-us

4.6.1 Warum Mirasys-Hardware?

- Verschiedene Gehäusetypen für jeden Bedarf
- Für den Einsatz mit Mirasys VMS optimierte Hardware
- M.2-SSDs für das Betriebssystem und die Mirasys VMS-Software
- Festplatten der Enterprise-Klasse
- 5 Jahre Garantie mit Reparatur am nächsten Werktag
- Behalten Sie Ihre Festplatte 5 Jahre lang
- Mirasys ABUR-Software; USB-Stick für automatisierte Datensicherung und -wiederherstellung
- Vorinstallierte Mirasys VMS-Software mit Lizenzen

4.6.2 Server

Wenn Sie nach einer Serverlösung suchen, beachten Sie bitte Folgendes:

- Anzahl der auf dem Server laufenden Kameras
    - Bitrate
    - Codec – H.264 vs. H.265
    - Auflösung
    - FPS
- Speicherdauer für Material und Verwaltungsdaten
    - Speicherrechner
- Bedarf an VCA oder Smart Services
    - Für die Verarbeitung dieser Aufgaben ist eine Grafikkarte oder ein separater KI-Server erforderlich.

Die Anzahl der Kameras und die Speicherdauer bestimmen, für welches Servergehäuse Sie sich entscheiden können. Die Wahl des richtigen Codecs kann dazu beitragen, den Speicherbedarf zu senken, allerdings benötigt der Server dafür eine leistungsstärkere CPU. Dies ist beispielsweise bei Verwendung des H.265-Codecs der Fall, der das gleiche Material in kleinerer Dateigröße speichert, aber mehr CPU-Leistung benötigt als der ältere H.264-Codec.

4.6.3 Beispielkonfigurationen

Die in dieser Spezifikation beschriebenen Hardwarekomponenten dienen als Referenz und können je nach gewähltem Hersteller und Servermodell variieren. Es können gleichwertige oder leistungsstärkere Komponenten anderer Anbieter verwendet werden, um die angegebenen Anforderungen zu erfüllen oder zu übertreffen.

Darüber hinaus sind Speicher- und andere Hardwarekonfigurationen skalierbar. Während als einfaches Beispiel eine Konfiguration mit einer einzigen Festplatte dargestellt wird, lassen sich die Systeme auf mehrere Laufwerke erweitern, was eine höhere Kapazität, eine verbesserte Leistung und zusätzliche Redundanzoptionen wie RAID-Konfigurationen ermöglicht.

4.6.3.1 Einstiegsserver

- Geeignet für den Einsatz als Management-Server und VMS-Server.
- Bis zu 50 Kameras.

Kategorie	Empfehlung
Gehäuseform	Rack oder Tower
Prozessor	Intel 6C/8C + HT
Grafikkarte	Integriert
Arbeitsspeicher	2 × 16 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD oder 2x SSD im RAID1-Verbund – 256 GB M.2 oder größer
RAID-Controller	8 GB Cache oder mehr
RAID-Stufen	0, 1, 5, 6, 10, 50, 60
Netzwerk	1 GB Netzwerk oder schneller

4.6.3.2 Server der mittleren Leistungsklasse

- Geeignet für den Einsatz als Management-Server und VMS-Server.
- Bis zu 80 Kameras.

Kategorie	Empfehlung
Gehäuseform	Rack oder Tower
Prozessor	Intel 8C + HT
Grafikkarte	Integriert
Arbeitsspeicher	2 × 16 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	2x SSD RAID1 – 480 GB M.2 oder höher
RAID-Controller	8 GB Cache oder mehr
RAID-Stufen	0, 1, 5, 6, 10, 50, 60

Kategorie	Empfehlung
Netzwerk	1 GB Netzwerk oder schneller

4.6.3.3 Hochleistungsserver

- Geeignet für den Einsatz als VMS-Server.
- Bis zu 100+ Kameras.

Kategorie	Empfehlung
Gehäuseform	Rack oder Tower
Prozessor	Intel 16C + HT
Grafikkarte	Integriert
Arbeitsspeicher	8 × 16 GB (acht Speicherkanäle)
Betriebssystemlaufwerke	2x SSD RAID1 – 480 GB M.2 oder höher
RAID-Controller	8 GB Cache oder mehr
RAID-Stufen	0, 1, 5, 6, 10, 50, 60
Netzwerk	10 GB Netzwerk oder schneller

4.6.3.4 Smart-Server (KI)

Bei der Auswahl eines Smart-Servers hängt der Bedarf an GPU-Leistung von den Diensten ab, die auf dem Server ausgeführt werden sollen. Bei Bedarf können in der VMS-Umgebung mehrere Smart-Server eingesetzt werden.

Kategorie	Empfehlung
Gehäuseform	Rack oder Tower
Prozessor	Intel 8C + HT
Grafikkarte	NVIDIA-GPU – A2000 oder höher
Arbeitsspeicher	2 × 16 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 480 GB M.2 oder höher
Datenspeicher	1x SSD – 1 TB oder mehr
Netzwerk	1 GB Netzwerk oder schneller

4.6.4 Client

Wenn Sie nach einer Client-Lösung suchen, beachten Sie bitte Folgendes:

- Wie viele Kameras sind in der Regel auf dem Client in Betrieb?
    - Bitrate
    - Codec – H.264 vs. H.265
    - Auflösung
    - FPS
- Wird eine externe Grafikkarte benötigt?
- Gibt es mehrere VMS-Server in der Umgebung?

Wenn auf der Client-Seite viele Kameras zum Einsatz kommen, muss ausreichend CPU- und GPU-Leistung vorhanden sein, um die Dekodierung der Kamerastreams zu bewältigen. Der Einsatz einer externen GPU sollte in Betracht gezogen werden. Dasselbe gilt, wenn neuere Codecs wie H.265 verwendet werden.

4.6.4.1 Einsteiger-Client

- Bis zu 12 Streams.

Kategorie	Empfehlung
Gehäuseform	Micro
Prozessor	Intel i5/U5
Grafikkarte	Integrierte Intel-Grafikkarte
Arbeitsspeicher	2 × 8 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Netzwerk	1 GB Netzwerk

4.6.4.2 Client der mittleren Leistungsklasse

- Bis zu 12–20 Streams.

Kategorie	Empfehlung
Gehäuseform	SFF
Prozessor	Intel i5/U5 oder Intel i7/U7
Grafikkarte	Integrierte Intel-Grafikkarte oder externe Nvidia-GPU – A1000 mit 8 GB oder besser

Kategorie	Empfehlung
Arbeitsspeicher	2 × 8 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Netzwerk	1 GB Netzwerk oder schneller

4.6.4.3 High-Level-Client

- Bis zu 40+ Streams.

Kategorie	Empfehlung
Gehäuseform	Tower
Prozessor	Intel i7/U7
Grafikkarte	Externe Nvidia-GPU – Ada 2000 oder besser
Arbeitsspeicher	2 × 16 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Netzwerk	1 GB Netzwerk oder schneller

4.6.5 Server- und Client-Kombinationen

Wenn Sie nach einer Server- und Client-Lösung suchen, beachten Sie bitte Folgendes:

- Die Anzahl der auf dem Server betriebenen Kameras
    - Bitrate
    - Codec – H.264 vs. H.265-
    - Auflösung
    - FPS
- Speicherdauer für Material und Overhead
    - Speicherrechner
- Bedarf an VCA oder Smart Services
    - Für die Verarbeitung dieser Aufgaben ist eine Grafikkarte oder ein separater KI-Server erforderlich.

Die Anzahl der Kameras und die Speicherdauer bestimmen, für welches Servergehäuse Sie sich entscheiden können. Die Wahl des richtigen Codecs kann dazu beitragen, den Speicherbedarf zu senken, allerdings benötigt der

Server dafür eine leistungsstärkere CPU. Dies ist beispielsweise bei Verwendung des H.265-Codecs der Fall, der das gleiche Material in kleinerer Dateigröße speichert, aber mehr CPU-Leistung benötigt als der ältere H.264-Codec.

- Wie viele Kameras sind in der Regel auf dem Client in Betrieb?
    - Bitrate
    - Codec – H.264 vs. H.265
    - Auflösung
    - FPS
- Wird eine externe Grafikkarte benötigt?
- Gibt es mehrere VMS-Server in der Umgebung?

Wenn auf der Client-Seite viele Kameras zum Einsatz kommen, muss ausreichend CPU- und GPU-Leistung vorhanden sein, um die Dekodierung der Kamerastreams zu bewältigen. Der Einsatz einer externen GPU sollte in Betracht gezogen werden. Gleiches gilt, wenn neuere Codecs wie H.265 verwendet werden.

Wenn VCA- oder Smart-Services ausgeführt werden sollen, muss die Hardware über eine externe GPU verfügen.

4.6.5.1 Einsteiger-Kombination

Kategorie	Empfehlung

Kategorie	Empfehlung
Gehäuseform	SFF
Prozessor	Intel i5/U5
Grafikkarte	Integrierte Intel-Grafikkarte
Arbeitsspeicher	2 × 8 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Speicher	1x 4–8 TB
Netzwerk	1 GB Netzwerk

4.6.5.2 Kombination für Fortgeschrittene

Kategorie	Empfehlung
Gehäuseform	Tower

Kategorie	Empfehlung
Prozessor	Intel i5/U5 oder Intel i7/U7
Grafikkarte	Integrierte Intel-Grafikkarte oder externe Nvidia-GPU – A1000 mit 8 GB oder besser
Arbeitsspeicher	2 × 8 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Speicher	2 x 8 TB oder mehr
Netzwerk	1 GB Netzwerk

4.6.5.3 Hochkarätige Kombination

Kategorie	Empfehlung
Gehäuseform	Tower
Prozessor	Intel i7/U7
Grafikkarte	Integrierte Intel-Grafikkarte oder externe Nvidia-GPU – Ada 2000 oder besser
Arbeitsspeicher	2 × 16 GB (zwei Speicherkanäle)
Betriebssystemlaufwerke	1x SSD – 256 GB M.2 oder höher
Speicher	3 x 8 TB oder mehr
Netzwerk	1 GB Netzwerk

5 BETRIEBSSYSTEMKOMPATIBILITÄT

Mirasys VMS V9 unterstützt die folgenden Betriebssysteme:

Betriebssystem	Server mit analoger Kameraunterstützung über Aufnahmekarten	Server nur mit IP-Kameras oder angeschlossenen Videoservern (Encoder)	Gateway server	System Manager-Anwendung	Spotter-Anwendung
Windows 10	-	X	X	X	X
Windows 11	-	X	X	X	X

Windows Server 2016	-	X	X	X	X
Windows Server 2019	-	X	X	X	X

ANMERKUNGEN

Stellen Sie sicher, dass die Funktion „Desktop Experience“ für Windows-Serverbetriebssysteme aktiviert ist.

6 KONFIGURIEREN DES SYSTEMS

Nachdem Sie die Kameras und andere Geräte mit den Servern verbunden haben, konfigurieren Sie die Systemeinstellungen und fügen Sie Benutzerkonten und Benutzerprofile hinzu.

Führen Sie die folgenden Schritte aus, um das System zu konfigurieren:

1. Fügen Sie dem System Server hinzu und konfigurieren Sie deren Einstellungen.
2. Fügen Sie die richtigen Lizenzen für die Server hinzu.
3. Fügen Sie IP-Kameras und andere IP-Geräte hinzu.
4. Benutzerprofile hinzufügen.
5. Benutzerkonten hinzufügen.

Notiz: *Installieren Sie die Client-Programme auf jedem Computer, der für den Zugriff auf das System über ein Netzwerk verwendet wird*

Ein separater Installer „Nur Spotter“ wird bereitgestellt

Notiz: ***Sichern Sie nach der Konfiguration des Systems die Systemeinstellungen und alle VMS-Server-Einstellungen*** *auf der Registerkarte* ***System****.So können Sie die Einstellungen wiederherstellen, beispielsweise wenn eine Festplatte ausfällt.*

7 EINLOGGEN

Dieser Abschnitt beschreibt, wie Sie sich bei System Manager an- und abmelden.
Nur Systemadministratoren oder Benutzer mit Überwachungsrechten dürfen sich bei System Manager anmelden.

Standard-Benutzername und -Passwort

Nutzername: Admin
Password: 0308

Der Standardbenutzername und das Standardpasswort sollten auch in geschlossenen Netzwerken nicht verwendet werden.
Bitte stellen Sie sicher, dass der Standardbenutzername und das Standardpasswort nach der Installation des Systems nicht mehr verwendet werden.

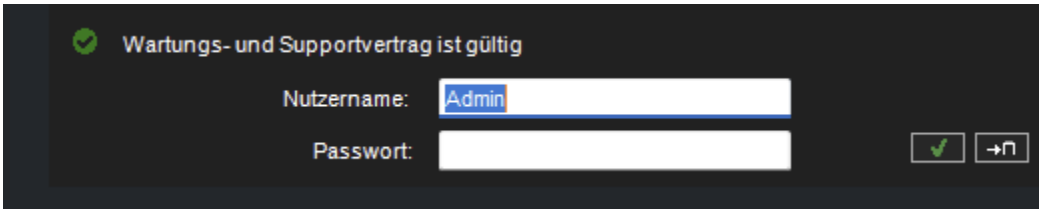
So melden Sie sich beim Systemmanager an:

Führen Sie einen der folgenden Schritte aus:

- Klicken Sie auf Start, zeigen Sie auf Programme und dann auf DVMS.
- Klicken Sie auf Start, zeigen Sie auf Programme und dann auf DVMS. Klicken Sie auf Systemmanager

In Systemen, in denen nur eine Haupt-Server-Adresse konfiguriert ist, wird der Systemmanager-Anmeldebildschirm angezeigt.
In Systemen mit mehreren Hauptserver, konfigurierten Adressen oder wenn der Benutzer in der anfänglichen Startphase die Taste „Löschen“ drückt, wird der Standortauswahlbildschirm angezeigt.

Geben Sie auf dem Anmeldebildschirm Ihren Benutzernamen in das Feld Benutzername und Ihr Kennwort in das Feld Kennwort ein.



Notiz: *Bei Benutzername und Passwort muss die Groß-/Kleinschreibung beachtet werden*

Klicken Sie auf **OK**. Der Fortschrittsbalken wird auf dem Bildschirm angezeigt, während das Programm geladen wird.

Nach dem Programmstart wird die Benutzeroberfläche angezeigt. Um abmelden oder zu zu ändern, Benutzer click in der Menüleiste Datei und dann Abmelden. So beenden Sie das Programm:

- Klicken Sie in der Menüleiste auf File und dann auf Exit
- Schließen Sie das Anwendungsfenster.

Notiz: Der Benutzer kann immer nur eine System Manager-Anwendung ausführen.
Der System Manager kann nicht gleichzeitig mit mehreren Servern verbunden sein.
Um eine Verbindung zu einem anderen Haupt-Server herzustellen, verlassen Sie den aktuellen Haupt und wählen Sie einen anderen Haupt-Server von der Site aus Auswahlbildschirm.

7.1 System Manager sperren

Sie können das Programm manuell sperren, um es zu schützen, beispielsweise wenn Sie Ihren Schreibtisch verlassen.

Um das Programm zu sperren, führen Sie einen der folgenden Schritte aus:

- Klicken Sie in der Menüleiste auf **Datei** und dann auf **Programm sperren**
- Klicken Sie in der Statusleiste auf **Programm sperren**

So entsperren Sie das Programm:

- Nach dem Sperren des Programms wird der Anmeldebildschirm angezeigt.
    - Geben Sie den Benutzernamen in das Feld **Benutzername** und das Kennwort in das Feld **Kennwort** ein.
    - Alternativ kann der Benutzer den System Manager auch direkt aus dem Sperrdialog heraus verlassen, indem er auf die Schaltfläche **Abmelden** klickt.

Beim Passwort muss die Groß-/Kleinschreibung beachtet werden

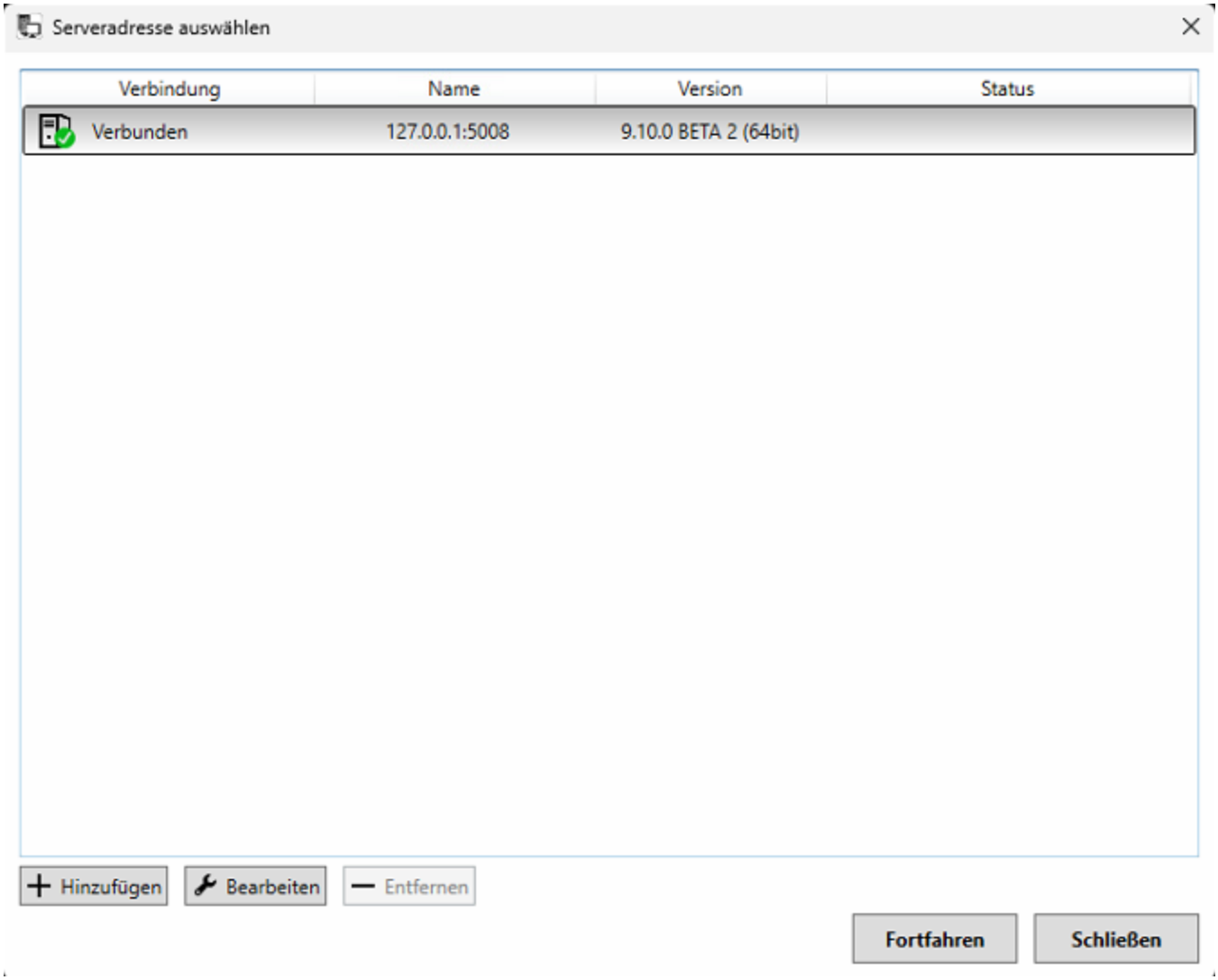
7.2 Zugang zur Auswahl der Serveradresse

In dieser Anleitung erfahren Sie, wie Sie die Serveradresse in der Client-Software bearbeiten können. Die Auswahl der Serveradresse ermöglicht es den Benutzern, neue Serveradressen hinzuzufügen, bestehende zu bearbeiten oder zu entfernen.

1. Klicken Sie mit der rechten Maustaste auf die Verknüpfung System Manager oder Spotter und wählen Sie **Als Administrator ausführen**.
2. Klicken Sie auf **Ja**, um diese Anwendung mit Administratorrechten auszuführen.
3. Danach erhalten Sie ein neues Fenster, drücken Sie die **Entf**-Taste auf der Tastatur, um das Fenster zur Auswahl der Serveradresse zu öffnen.



4. In diesem Fenster können Sie neue Serveradressen hinzufügen, bestehende Adressen bearbeiten oder entfernen.



5. Wenn alle erforderlichen Änderungen vorgenommen wurden, wählen Sie die gewünschte Serveradresse aus und klicken Sie auf **Weiter**, um die Verbindung zu diesem Server herzustellen.

8 MANAGEMENT-BENUTZEROBERFLÄCHE

Die Benutzeroberfläche von System Manager enthält diese Elemente:

8.1 MENÜLEISTE

- Datei
- Ausloggen
- Program sperren
- Importieren
- Export

8.2 INSTANDHALTUNG

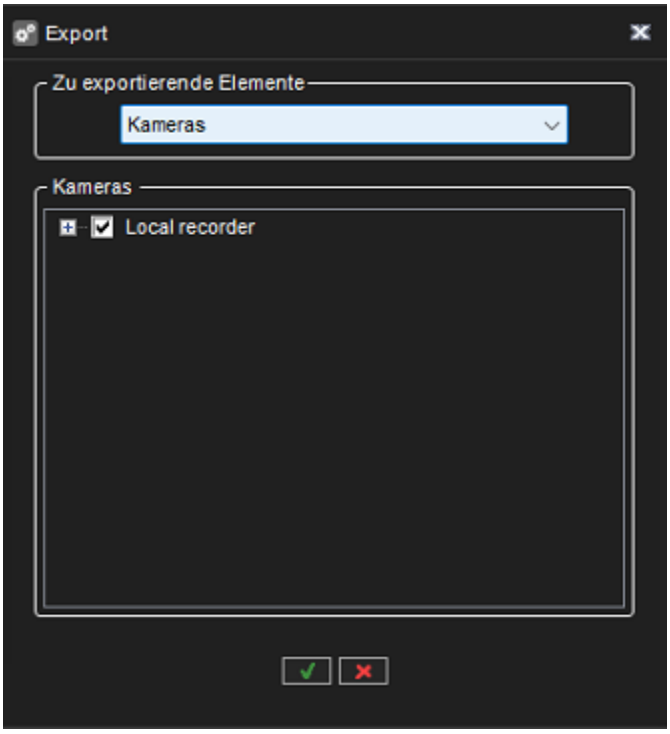
Setzen Sie den **Wartungszustand auf Ein**, um den Failover-Übergangszustand auf Aus zu steuern.

8.3 HILFE

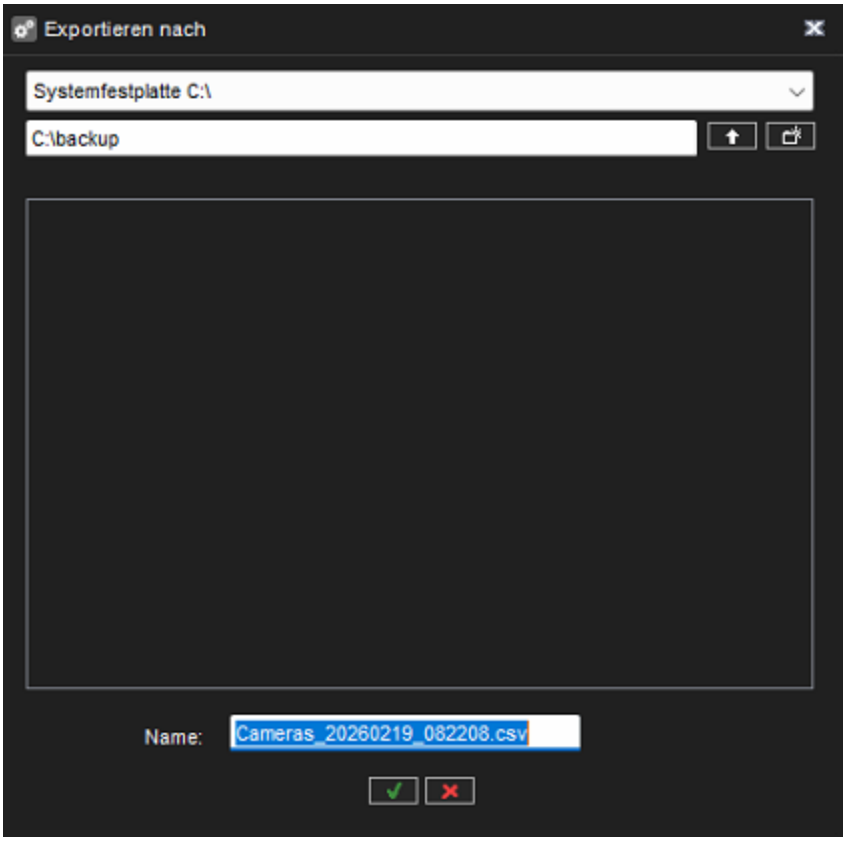
Über zeigt Informationen zur Programmversion an, **Online-Hilfe** ermöglicht den Zugriff auf die Online-Benutzerdokumentation und **Hilfethemen** ermöglicht die Verwendung des PDF-Handbuchs.

8.4 EXPORTIEREN VON SYSTEMKAMERAINFORMATIONEN IN DIE CSV-DATEI

1. Klicken Sie auf **Datei**
2. Klicken Sie auf **Export**
3. Wählen Sie die Server aus
4. Klicken Sie auf **OK**



1. Wählen Sie den Speicherort aus
2. Geben Sie den Namen der Exportdatei ein
3. Klicken Sie auf **OK**



9 SYSTEM



Auf der Registerkarte „System“ können Sie Systemeinstellungen bearbeiten und sichern, das System überwachen und diagnostische Informationen zum Kurs untersuchen.
Auf dieser Registerkarte können Sie auch Lizenzschlüssel für Server ändern, z. B. weitere Kamerakanäle hinzufügen und eine neue IP-Kamera, Metadaten, und Client-Plugin-Treiber.
Außerdem können Sie den Software-Watchdog konfigurieren.

Die Registerkarte enthält diese Werkzeuge:

- Systemeinstellungen
- Allgemeine Systemeinstellungen

- Email Einstellungen
- Befehlseinstellungen
- VMS-Serveradressen ändern
- Systemadressen
- VMS-Server aktualisieren
- Sicherung
- Protokolle exportieren
- Backup-Einstellungen
- Einstellungen zurücksetzen
- Überwachung
- SM-Server-Diagnose
- Lokale Rekorder-Diagnose
- Lizenzen
- Wachhund
- Watchdog-Einstellungen
- Watchdog-Protokolle
- Add-Ins
- Installiere Treiber
- Installieren Sie den Metadatentreiber
- Client-Treiber installieren
- Installieren Sie das Client-Plugin

9.1 Führen Sie einen der folgenden Schritte aus, um ein Werkzeug zu öffnen

- Klicken Sie auf das Tool und dann auf Bearbeiten



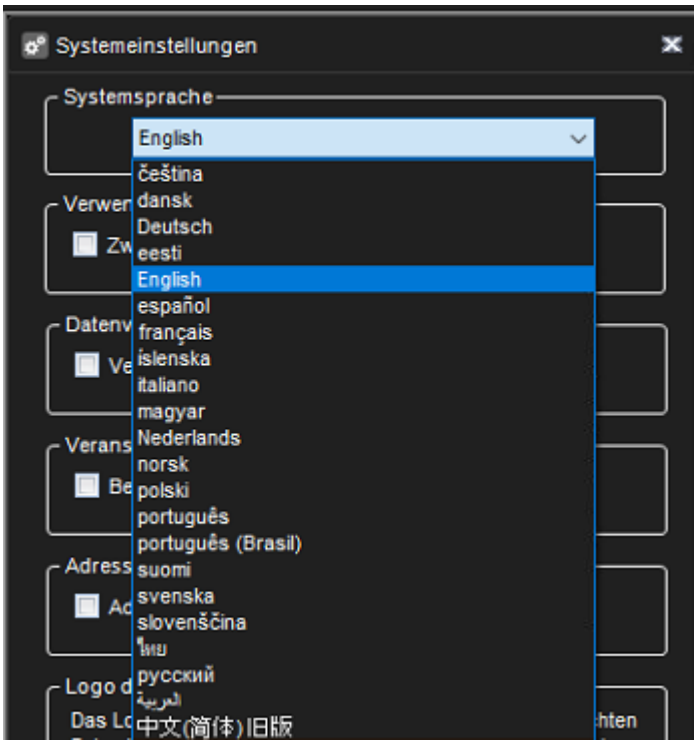
- Doppelklicken Sie auf das Werkzeug

- Ziehen Sie das Werkzeug von der Registerkarte System in den Arbeitsbereich

9.2 SYSTEMEINSTELLUNGEN



9.2.1 Allgemeine Systemeinstellungen



9.2.1.1 In diesem Bereich können Sie Folgendes steuern

- Systemsprache
- Passwortverwendung
  Sie können das System so konfigurieren, dass für alle Benutzer zwei separate Passwörter erforderlich sind. Aktivieren Sie dazu die Option „Zweites Passwort verwenden“ in den allgemeinen Systemeinstellungen.
  In diesem Modus müssen alle Benutzer zwei Passwörter angeben.
  Das standardmäßige zweite Passwort ist leer. Diese Funktion ermöglicht die Einschränkung, sodass keine einzelne Person Videos allein überprüfen kann.
  Wenn ein Passwort einer Person und das andere Passwort einer anderen Person bekannt ist, müssen beide Personen bei der Videoüberprüfung anwesend sein.
- Datenverschlüsselung
- Ereignisse (Einstellung für den Versand von Bewegungsinformationen an Clients und über Integrationen)
- Adressauswahl
- Primäres Videoclip-Logo (Logos, die an exportierte Videoclips angehängt werden)
- Sekundäres Videoclip-Logo (Logos, die an exportierte Videoclips angehängt werden)

9.2.2 Einstellungen für die Anzeige von Stationen konfigurieren

9.2.2.1 Einstellungen für die Anzeige von Stationen konfigurieren:

1. Gehen Sie zur Registerkarte **System** im System Manager
2. Doppelklicken Sie auf **Stationseinstellungen anzeigen**
3. Klicken Sie auf **Fügen Sie eine neue Spotter-Ansichtsstation hinzu**
4. Legen Sie den Namen, die Adresse und den Port für die Station fest
5. Änderungen speichern

Anzeigestationen können in den Einstellungen für Anzeigestationen erstellt, bearbeitet oder gelöscht werden.

9.2.2.2 Freigabe für Betrachtungsstationen in den Benutzerrolleneinstellungen aktivieren:

1. Gehen Sie zur Registerkarte **Benutzer** im System-Manager
2. Doppelklicken Sie auf eine Benutzergruppe
3. Klicken Sie im Abschnitt „Benutzergruppenrollen“ auf **Mirasys Spotter Enterprise Rolleneigenschaften bearbeiten**



1. Gehen Sie zur Registerkarte **Besichtigungsstationen**
2. Aktivieren Sie das Kontrollkästchen „Aktivieren Sie die Freigabe mit Anzeigestationen“ und wählen Sie aus der Liste die Anzeigestationen aus, für die der Bediener die Freigabe erteilen darf
3. Änderungen speichern

9.2.3 Email Einstellungen



Sie können E-Mail-Adressen und Gruppen angeben, die definiert werden können, um Berichte über Ereignisse zu erhalten, die im Software Watchdog angegeben sind.

9.2.3.1 So legen Sie die E-Mail-Benachrichtigungseinstellungen fest:

1. Öffnen Sie auf der Registerkarte System die E-Mail-Einstellungen

2. Geben Sie die E-Mail-Adresse des Absenders in das Feld Absender ein. Beachten Sie, dass einige E-Mail-Anwendungen so konfiguriert sind, dass sie nur Nachrichten von gültigen E-Mail-Adressen akzeptieren.
3. Geben Sie den Namen des Postausgangsservers in das Feld Postausgang (SMTP) ein. Der angegebene Server wird zum Senden aller E-Mail-Benachrichtigungen verwendet
4. Geben Sie die Anmeldeinformationen und den Port für den SMTP-Server in die entsprechenden Felder ein.
5. Legen Sie die Ereignisse fest, für die Benachrichtigungen gemäß den Anweisungen im Software Watchdog gesendet werden

Notiz: E-Mails werden nicht an alle System-E-Mail-Empfänger gesendet.

Der Administrator kann steuern, welche Watchdog-Ereignisse und -Alarme an welche E-Mail-Empfänger oder Gruppen die E-Mail gesendet wird.

9.2.3.2 So fügen Sie dem System neue E-Mail-Adressen hinzu:

1. Öffnen Sie auf der Registerkarte System die E-Mail-Einstellungen
2. Klicken Sie auf **Neue E-Mail-Adresse hinzufügen**



um eine neue Adresse hinzuzufügen.

3. Geben Sie den Namen und die E-Mail-Adresse des Empfängers in die Felder Name und Adresse ein.
4. OK klicken.

9.2.3.2.1 So fügen Sie dem System eine neue E-Mail-Gruppe hinzu

1. Öffnen Sie auf der Registerkarte System die E-Mail-Einstellungen
2. Klicken Sie auf **Neue E-Mail-Adresse hinzufügen**



um eine neue Adresse hinzuzufügen.

3. Geben Sie den Gruppennamen ein
4. OK klicken

9.2.3.3 So fügen Sie einer Gruppe einen oder mehrere Empfänger hinzu:

1. Markieren Sie die gewünschte Gruppe in der Gruppenliste
2. Markieren Sie den oder die gewünschten Empfänger in der Empfängerliste
3. Klicken Sie auf den Pfeil



um die ausgewählten Empfänger der ausgewählten Gruppe hinzuzufügen

9.2.3.4 Andere verfügbare Aktionen:

Das Bearbeiten von E-Mail-Namen, Adressen, Gruppennamen und das Entfernen von Personen aus Gruppen ist mit den Schaltflächen Bearbeiten



möglich.

Personen können mit dem Pfeil aus Gruppen entfernt werden.



Personen und Gruppen können mit der Schaltfläche



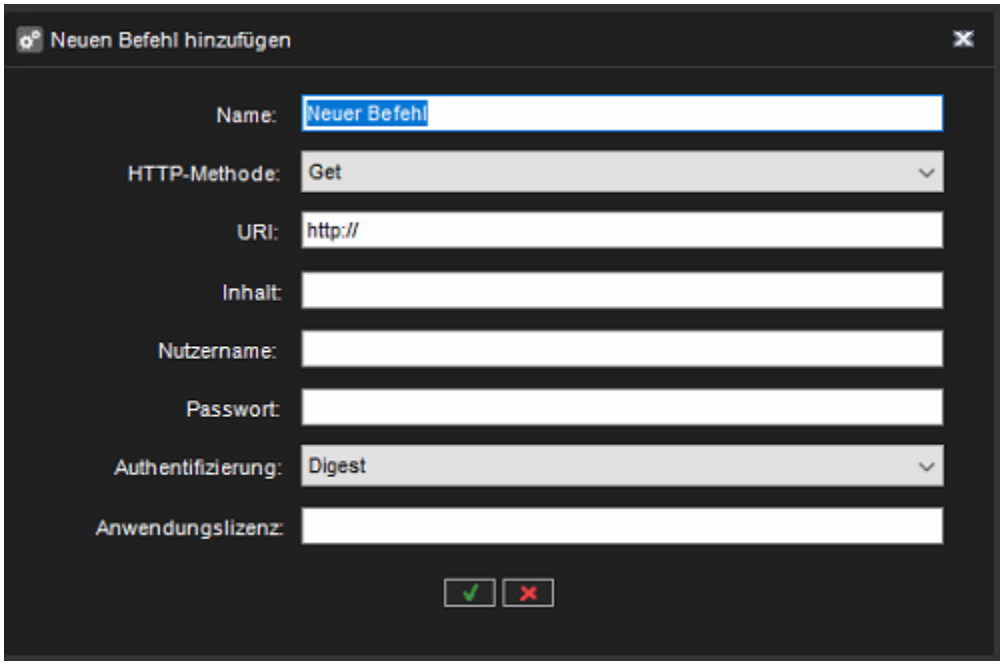
entfernt werden.
Test-E-Mails können mit Schaltfläche



a an a gesendet werden ausgewählte E-Mail-Adresse mit den im Dialogfeld E-Mail-Einstellungen definierten Einstellungen.

9.2.4 Befehlseinstellungen

Befehlseinstellungen werden für das Senden von HTTP-Befehlen verwendet

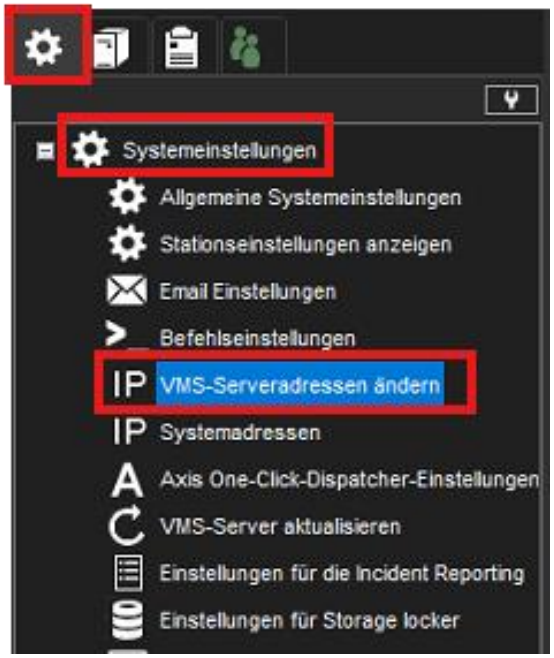


9.2.5 VMS-Serveradressen ändern

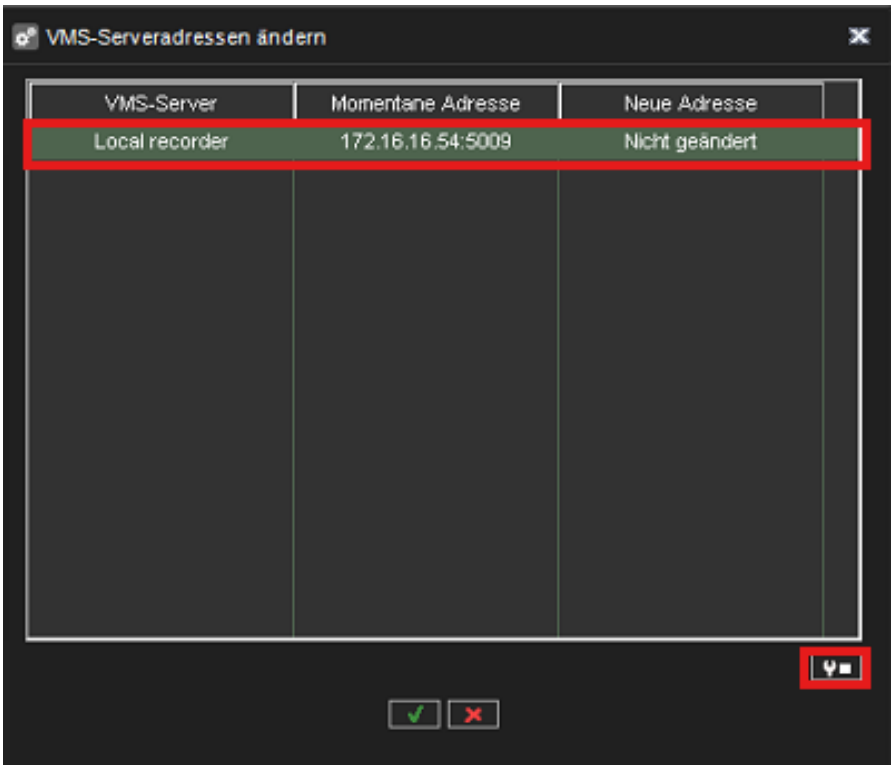
Wenn der Server als Hauptserver eines Systems fungieren soll und der Zugriff über ein Netzwerk erfolgt, müssen Sie die IP-Adresse des Servers über System Manager festlegen. IP-Adressen und DNS-Namen können im Tool **Systemadressen ändern** geändert werden.

9.2.5.1 VMS-Serveradressen ändern

1. Öffnen Sie auf der Registerkarte **System** die Option **VMS-Serveradressen ändern**.



1. Klicken Sie auf den Server und dann auf **VMS-Serveradresse ändern**.

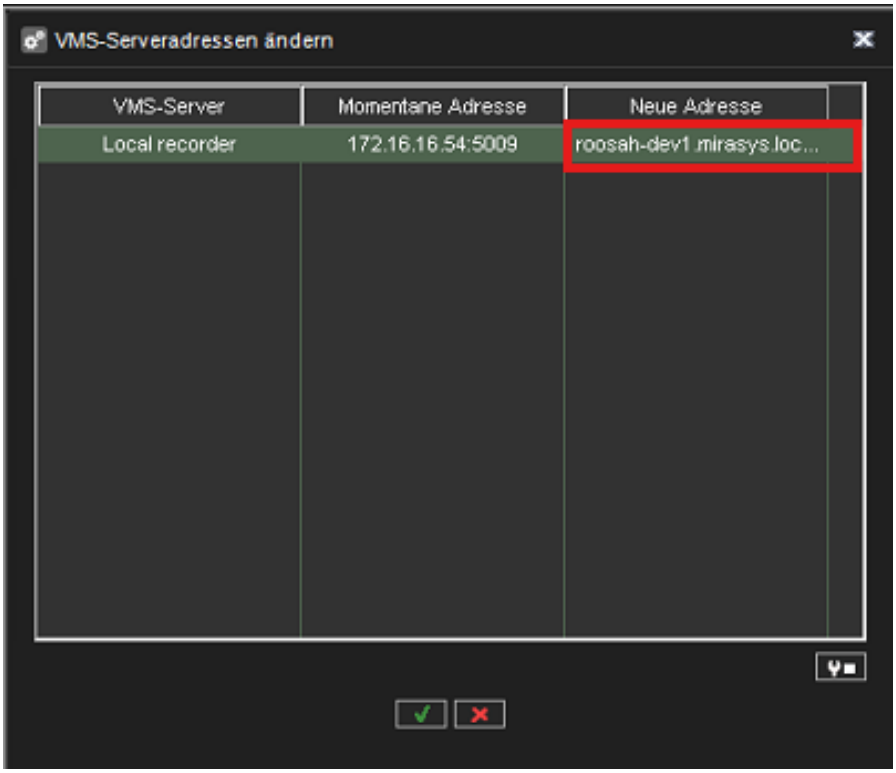


1. Geben Sie die neue IP-Adresse oder den DNS-Namen des Servers in das Feld Neue **VMS-Serveradresse** ein.

2. **OK** klicken.



Die geänderte Adresse ist im Feld „Neue Adresse“ zu sehen.

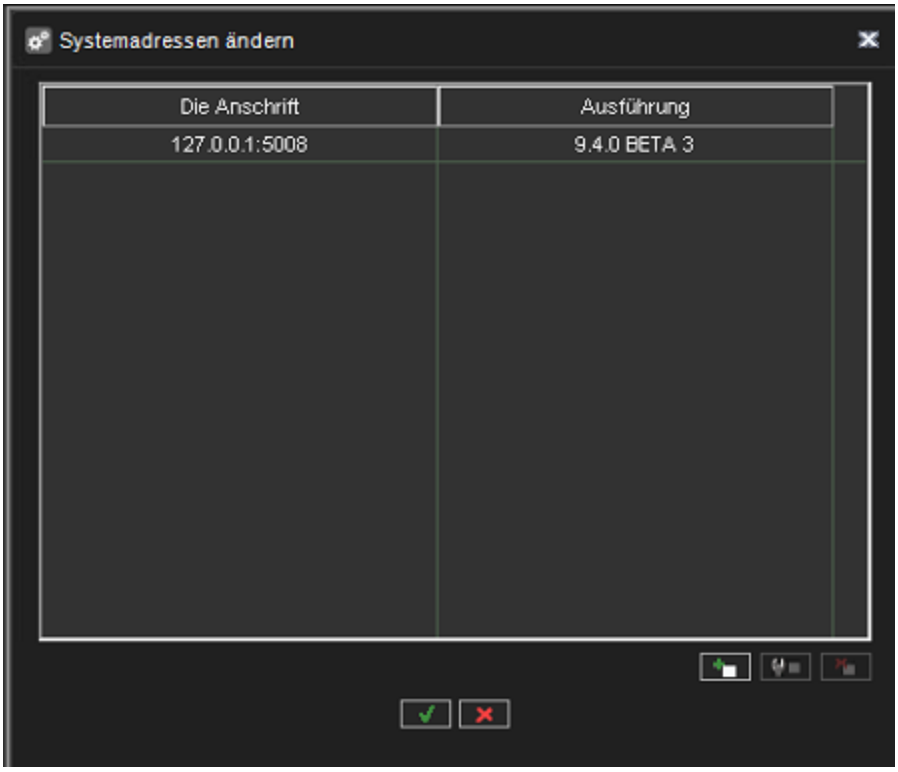


Sie müssen die lokale IP-Adresse für den Hauptserver eines Systems nur dann festlegen, wenn über ein Netzwerk auf den Server zugegriffen werden kann. Wird lokal auf den Server zugegriffen, ist es nicht erforderlich, die Adresse festzulegen.

9.2.6 Systemadressen

Der Hauptserver ist der zentrale Server eines Überwachungssystems.

Alle anderen VMS-Server verbinden sich damit und alle Client-Anwendungen kommunizieren über den Hauptserver. Während der Anmeldephase können die Clientanwendungen den Hauptserver auswählen, zu dem sie eine Verbindung herstellen.



Sie können mehrere Hauptserver-Adressen definieren, mit denen sich die Client-Anwendungen verbinden können. Die Adressen können als IP-Adressen (z. B. *http://195.168.0.1*) oder DNS-Namen (z. B. *http://www.example.com*) bereitgestellt werden.

Notiz: *Benutzer können sich mit jeder der definierten Hauptserver-Adressen verbinden, vorausgesetzt, sie haben einen kompatiblen Benutzernamen und ein kompatibles Passwort für den Hauptserver.*

9.2.6.1 So fügen Sie eine Hauptserver-Adresse hinzu

1. Öffnen Sie auf der Registerkarte System die Systemadressen
2. Klicken Sie auf **Neue Systemadresse hinzufügen**

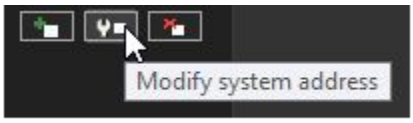


3. Geben Sie die neue Systemadresse (entweder IP-Adresse oder DNS-Name) in das Feld Hinzufügen ein.

4. OK klicken

9.2.6.2 So bearbeiten Sie eine Hauptserver-Adresse:

1. Öffnen Sie auf der Registerkarte System die Option Systemadressen.
2. Klicken Sie auf die Hauptserver-Adresse mit der geänderten IP-Adresse.



3. Klicken Sie auf Systemadresse ändern .
4. Geben Sie die neue IP-Adresse oder den DNS-Namen des DVR in das Feld Systemadresse ändern ein.
5. OK klicken

9.2.6.3 So entfernen Sie eine Hauptserver-Adresse:

1. Öffnen Sie auf der Registerkarte System die Systemadressen
2. Klicken Sie auf die Hauptserver-Adresse, die Sie entfernen möchten.
3. Klicken Sie auf Systemadresse entfernen.



9.2.7 Axis One-Click-Dispatcher-Einstellungen

9.2.7.1 Installationsschritte

Installieren Sie den O3C-Server wie im Handbuch „AXIS O3C Server Reference“ beschrieben. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

9.2.7.1.1 Wichtige Dinge:

Installieren Sie den O3C-Server wie im Handbuch „AXIS O3C Server Reference“ beschrieben. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

Wichtige Dinge:

- setup provider certificate authority:

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

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

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

9.2.7.1.1.1 Issue a server certificate:

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

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

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

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

Result:

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

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

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

9.2.7.1.2 Configure o3c-server.conf

listen_client = 172.17.102.56:80

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

stserverid = test_o3c_server

Any string

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

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

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

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

provider_name =

can be left blank

credentials = root:root

for device access requests

9.2.7.1.3 O3C-server service

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

1. Starten Sie den O3C-Serverdienst
2. Aktivieren Sie die Ein-Klick-Technologie auf der Kamera, wie in Teil 4.1 des Handbuchs beschrieben.
3. Firewalls deaktivieren oder O3C-Server zu den Ausnahmen hinzufügen

4. Registrieren Sie die Kamera wie in Teil 4.2 der Anleitung beschrieben.
    a. http://172.17.102.56/admin/dispatch.cgi?action=register&user=adp_mirasys_100&pass=GQ41lSRbbEb4w3sorkN8&mac=B8A44F17AAFA&oak=8A22D6434817&server=172.17.102.56:80
    b. where:user=adp_mirasys_100, pass=GQ41lSRbbEb4w3sorkN8 - Mirasys credentials (Provider name and password) from Axismac=B8A44F17AAFA, oak=8A22D6434817 - MAC address and OAK key from the camera
    c. Um die MAC-Adresse zu finden, verwenden Sie im Browser die folgende Zeichenfolge: http://172.17.100.84/axis-cgi/admin/param.cgi?action=list&group=Network
    d. server=172.17.102.56:80 - as "listen_client" in o3c-server.conf
5. Überprüfen Sie, ob die Kamera mit dem O3C-Server verbunden war: Rufen Sie im Browser den String auf: http://172.17.102.56:80/admin/status.cgi 172.17.102.56 - IP-Adresse des O3C-Servers
6. Und überprüfen Sie, ob ein Kommentar zum verbundenen Client wie folgt vorhanden ist: "id=4.b8a44f17aafa srcaddr=172.17.100.84:34148 accepted=1 v=2 rx=0 tx=0 connected=2022-01-10T12:45:40.875571Z

Gesamtzahl der Kunden: 1"

PS: Die Kamera versucht alle 20 Sekunden, sich mit dem Server zu verbinden

7. Überprüfen Sie, ob wir Optionen von der Kamera erhalten können: Dazu mussten die Proxy-Einstellungen für den Browser konfiguriert werden -

8. Öffnen Sie die Internetoptionen des Systems

9. Wählen Sie die Registerkarte Verbindungen -> Wählen Sie die Schaltfläche LAN-Einstellungen -> um "Proxy-Server für LAN verwenden (...)" zu aktivieren und geben Sie die Proxy-IP-Adresse und den Port ein. (im aktuellen Fall gibt es eine lokale IP-Adresse und Port 80)

10. Danach können wir die Kamerafunktionen im Browser abrufen:

- http://b8a44f17aafa/axis-cgi/param.cgi?action=list&group=root.RemoteService where b8a44f17aafa - MAC address of the camera

9.2.7.1.3.1 Filter for wireshark for Axis P1375:

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

9.2.7.2 Add Axis One-Click Camera

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



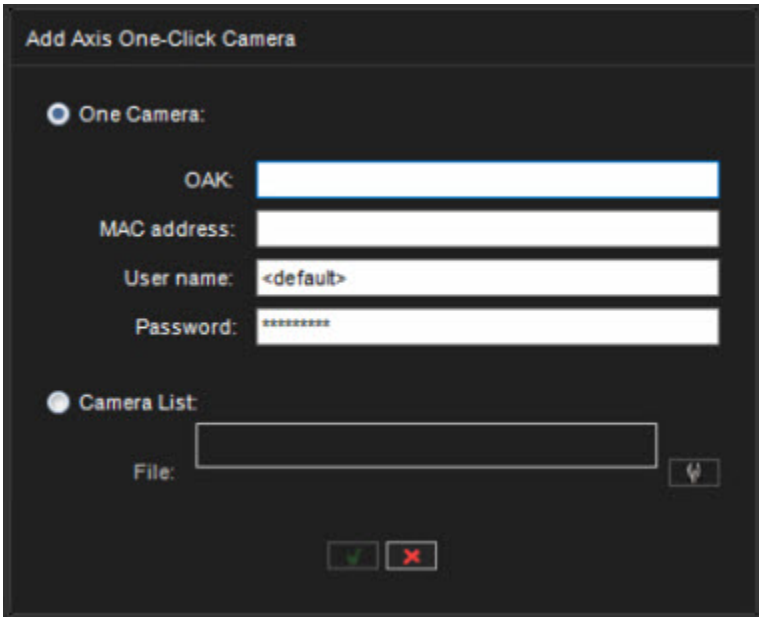
4. Open the **VMS Servers tab**

5. Click **Hardware**

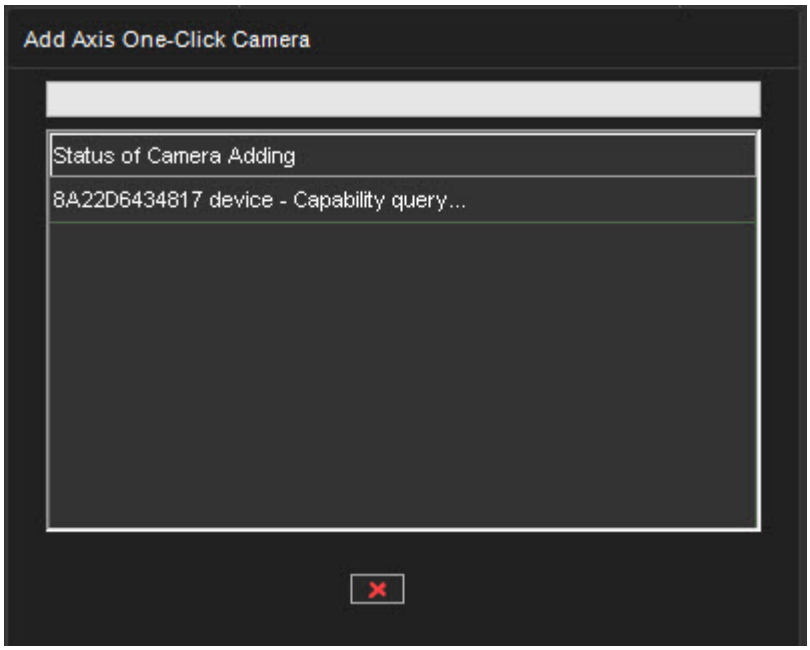
6. Click **Add Axis One-Click Camera** icon



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



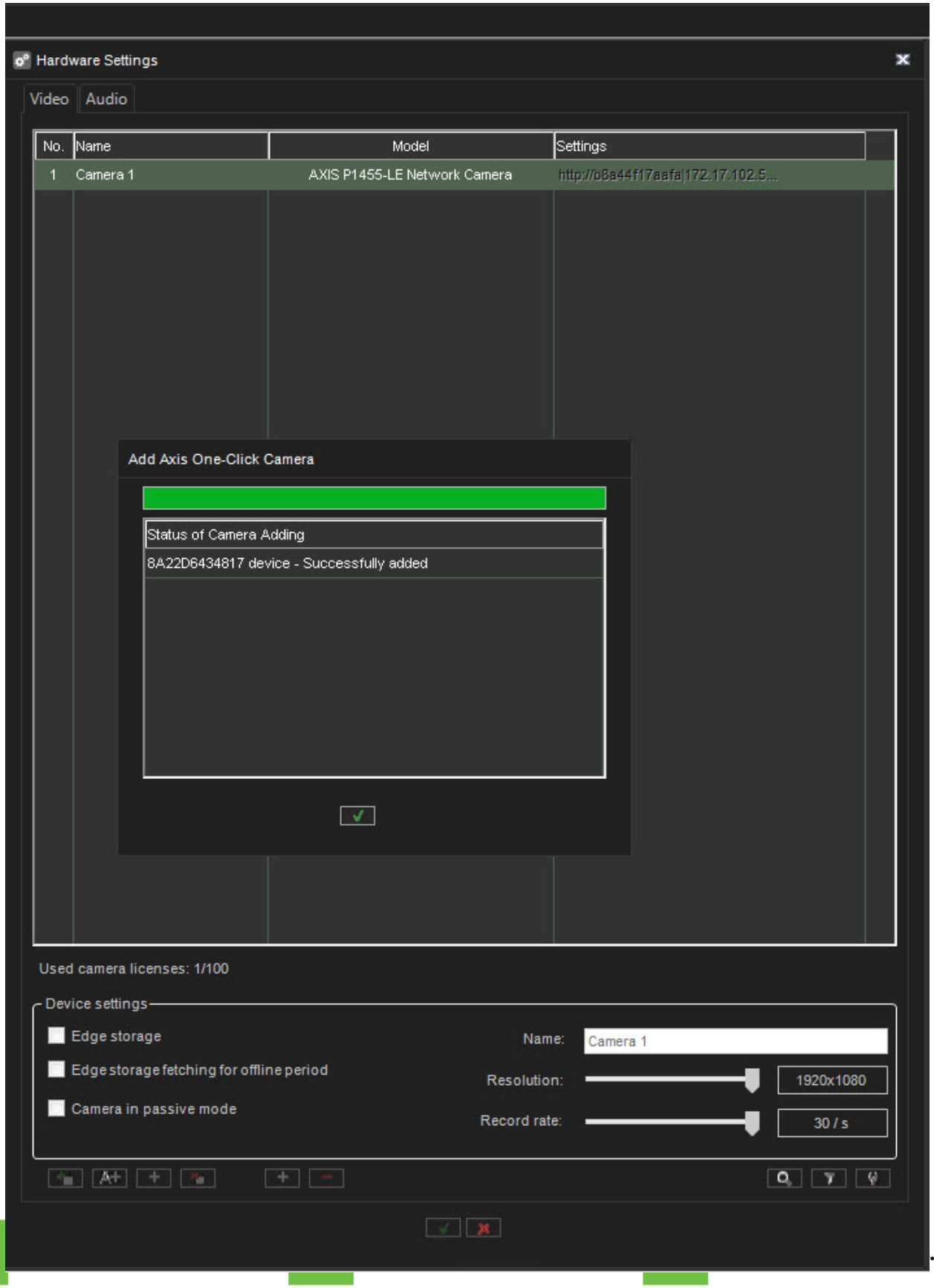
After clicking the OK, the camera query starts



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

8. Click **OK** to finalize

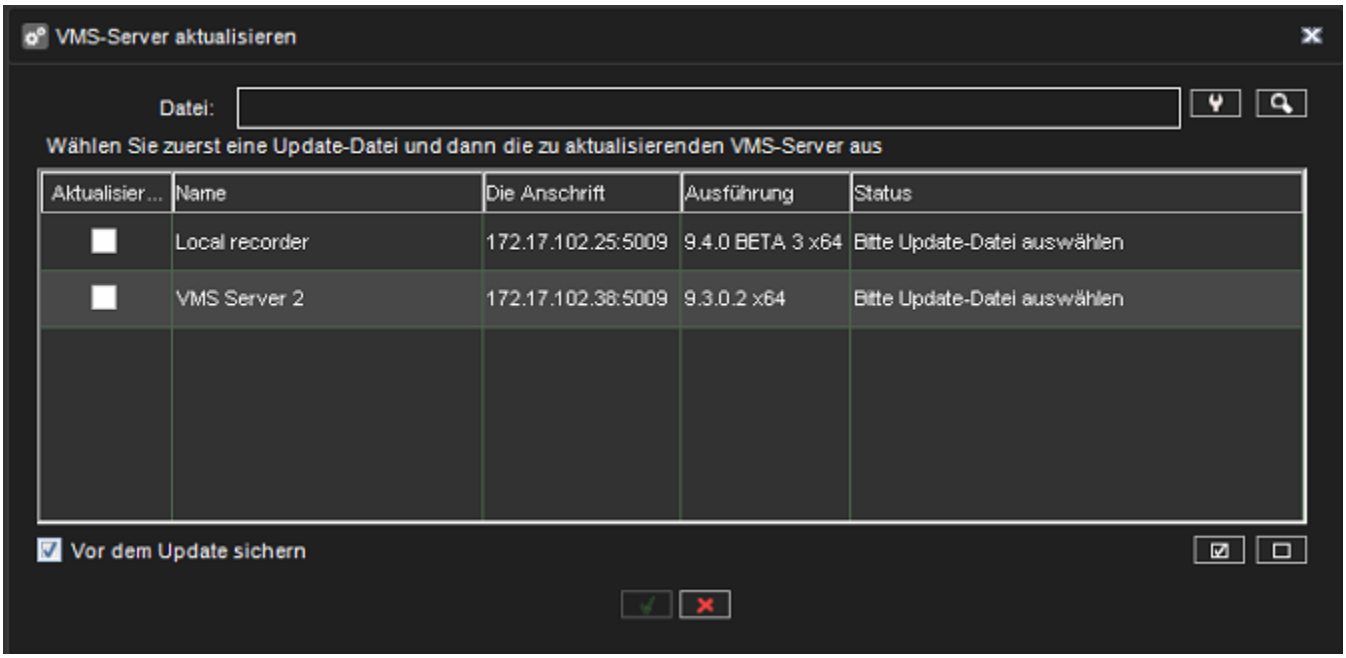
MIRASYS


Hardware Settings
Video
Audio
No.
Name
Model
Settings
1
Camera 1
AXIS P1455-LE Network Camera
http://b8a44f17aafa:172.17.102.5...
Add Axis One-Click Camera
Status of Camera Adding
8A22D6434817 device - Successfully added
Used camera licenses: 1/100
Device settings
Edge storage
Edge storage fetching for offline period
Camera in passive mode
Name:
Camera 1
Resolution:
1920x1080
Record rate:
30 / s

.com

9.2.8 VMS-Server aktualisieren

Über die Option **Update VMS Servers** ist es möglich, den lokalen Server und alle angeschlossenen VMS-Server aus der Ferne zu aktualisieren



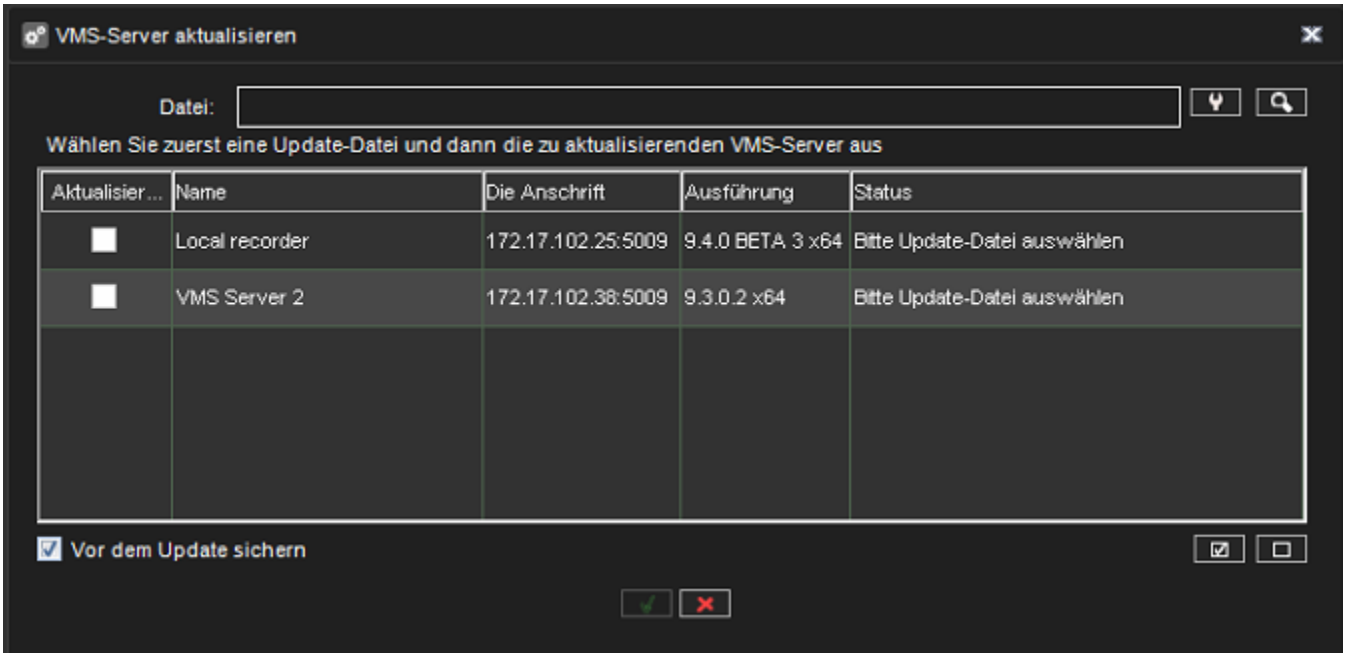
Um Server zu aktualisieren, wählen Sie zuerst die Installationsdatei mit der Schaltfläche



aus.

Die Liste wird aktualisiert, um anzuzeigen, welche Server mit der ausgewählten Installationsdatei aktualisiert werden können.

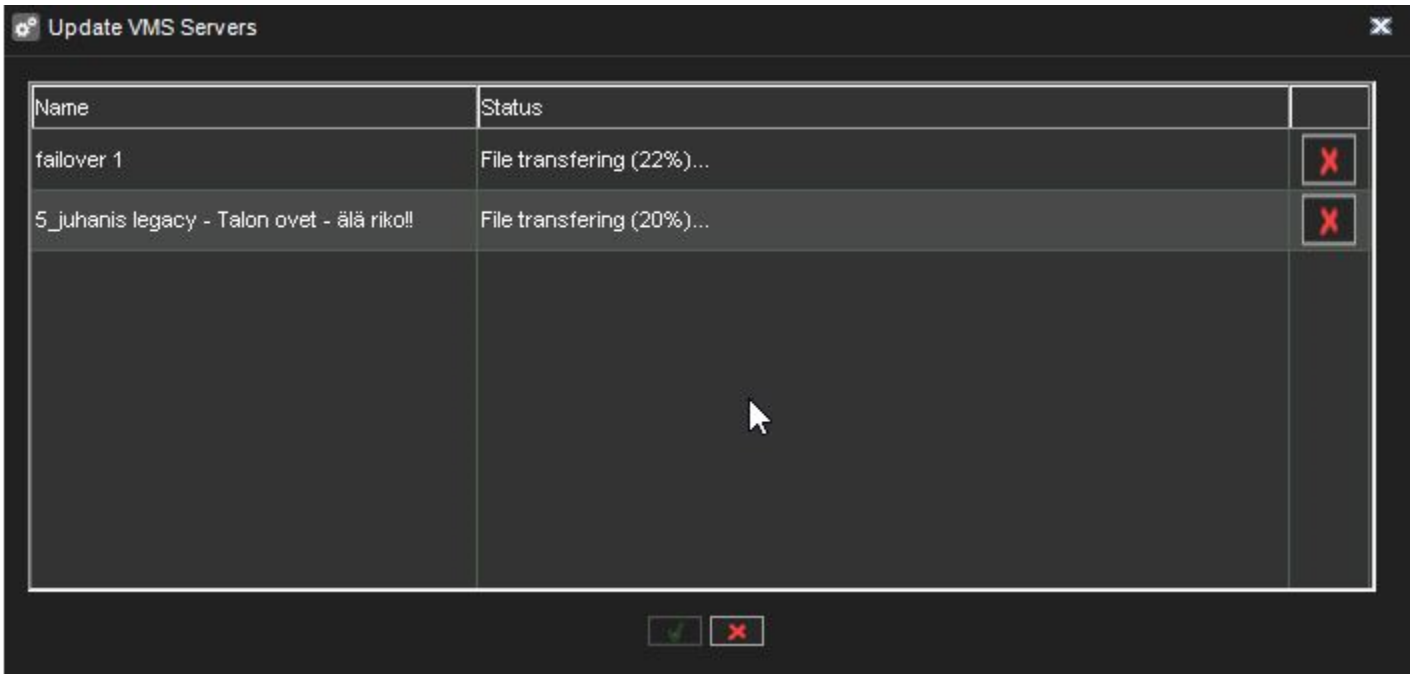
Notiz: *Bei einem Upgrade der Hauptversion, beispielsweise von VMS 6. x auf 7. x, ist es normalerweise erforderlich, zuerst die Serverlizenzen zu aktualisieren und erst danach die VMS-Software. Der Dialog „VMS-Server aktualisieren" informiert den Benutzer wenn vor dem Software-Update ein Lizenz-Upgrade erforderlich ist.*Wählen Sie als Nächstes aus, welche Server Sie aktualisieren möchten und ob Sie vor dem Update eine Sicherung durchführen möchten.



Durch Auswahl der Schaltfläche starten



Sie das Update und ein Update-Fortschrittsdialog wird angezeigt:



Dieser Dialog kann jederzeit geschlossen werden, ohne die Server-Updates zu beeinflussen.

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

Notiz:

- Der Fortschrittsdialog zeigt möglicherweise keine Statusinformationen für die Übertragung der Installationsdatei und den Aktualisierungsfortschritt an, wenn die Netzwerkverbindung langsam oder zeitweilig ist.
    - Dies ist kein Grund zur Beunruhigung; In den meisten Fällen wird das Update erfolgreich sein, es kann jedoch lange dauern (20 - 30 Minuten).
    - Es wird empfohlen, sich auf die Möglichkeit des Fernzugriffs auf solche Server vorzubereiten.
- Wenn ein lokaler Server zum Aktualisieren ausgewählt wurde, würde der Systemmanager automatisch geschlossen, nachdem dieser Dialog angezeigt wurde.
- In seltenen Fällen erfordern einige Server einen Systemneustart nach einem Remote-VMS-Softwareupdate, wenn die Verbindung zwischen dem Hauptserver und dem VMS-Server nach dem Update nicht wiederhergestellt wird.
    - Es wird empfohlen, die Verbindung zu VMS-Servern nach dem Update zu überwachen.
- Seit Version 7.4.3 unterstützt Mirasys VMS 64-Bit-Server. Das Upgrade von 32-Bit (x86) auf 64-Bit kann genau durch die Installation einer beliebigen DVMS-Version erreicht werden.
    - Nach dem Update zeigt die Systemsteuerung von Windows DVMS-x64 für 64-Bit-DVMS an.

9.2.9 Einstellungen für die Meldung von Vorfällen

In den Vorfallberichtseinstellungen definiert der Benutzer die Parameter vor, die beim Anzeigen oder Exportieren der Vorfall- oder Tagesprotokollberichte verwendet werden.

9.2.9.1 Unternehmensinformationen

- Name der Firma
- Firmenanschrift
- Firmenlogo

9.2.9.2 Berichtsnummerierung

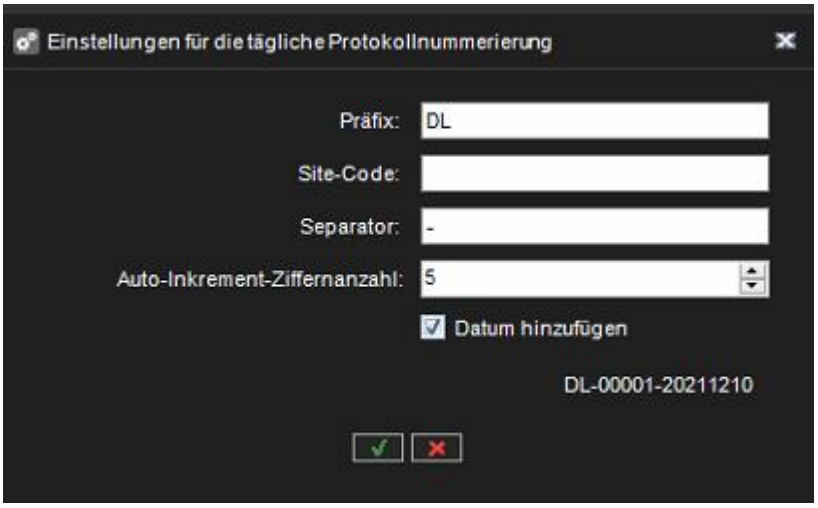
Details zur Nummerierung von Vorfällen

- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen



9.2.9.3 Details zur Nummerierung des Tagesprotokolls:

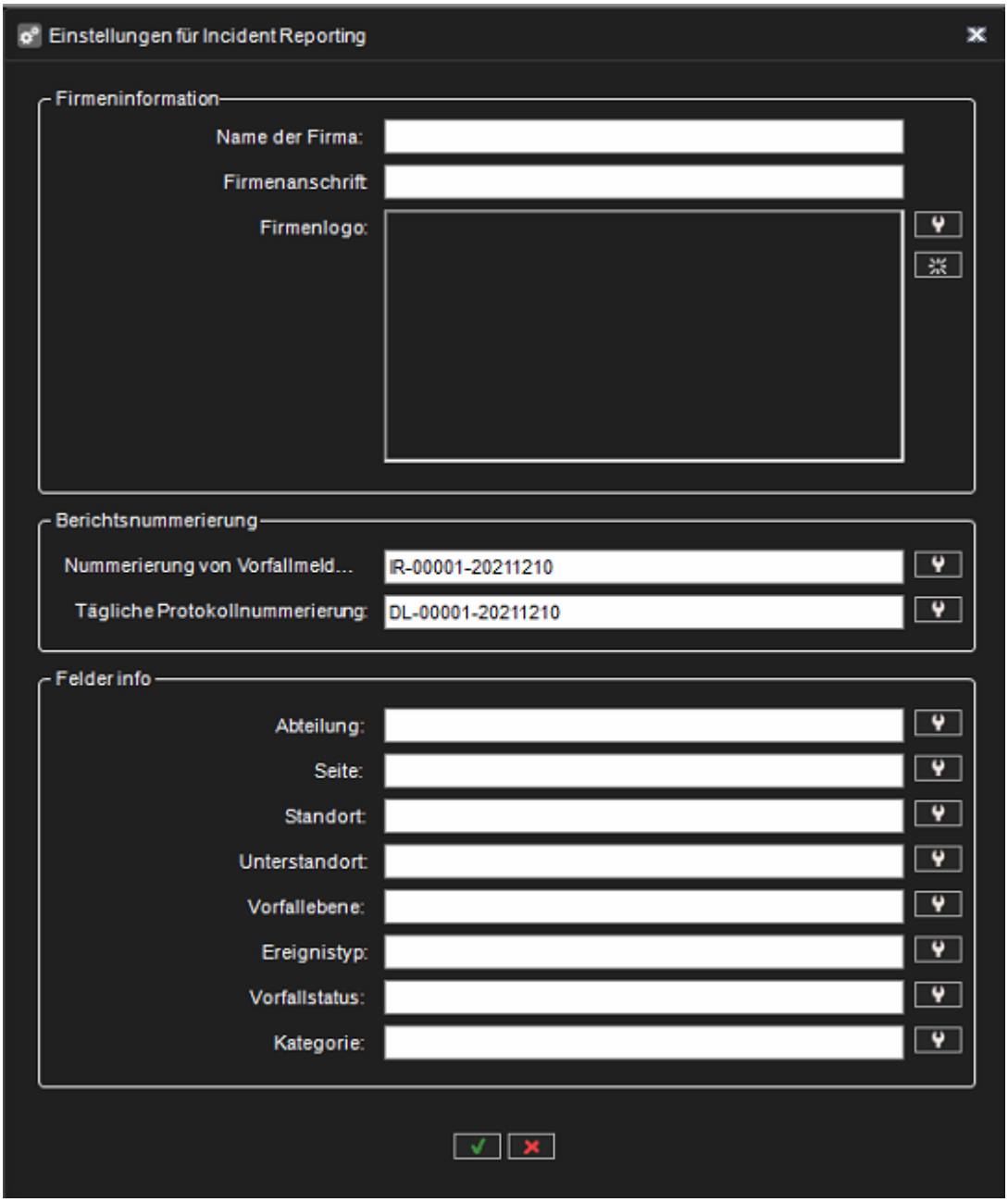
- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen



9.2.9.4 Felder info

- Abteilung
- Seite
- Standort
- Unterstandort

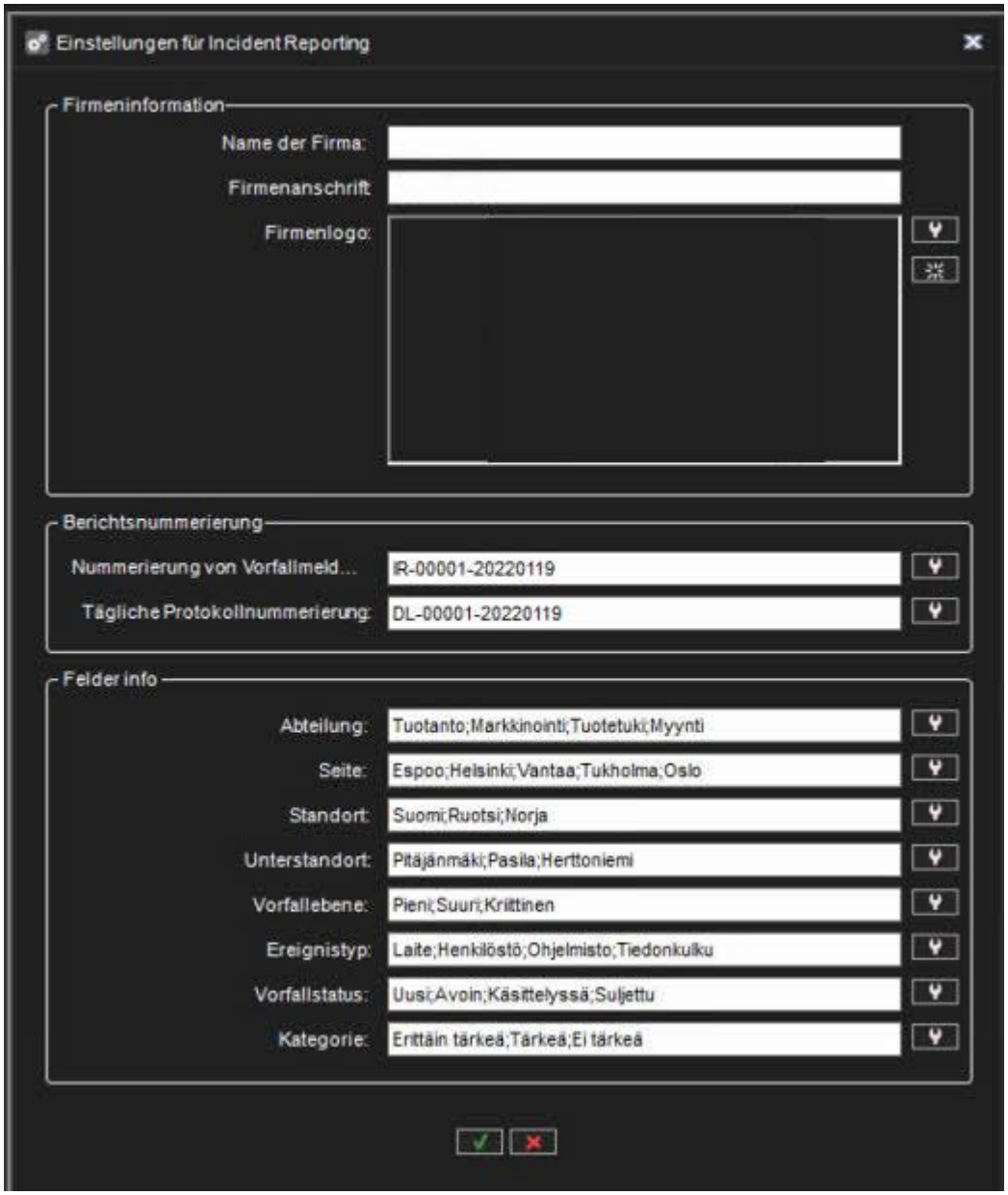
- Vorfall
- Vorfalltyp
- Vorfallstatus
- Kategorie



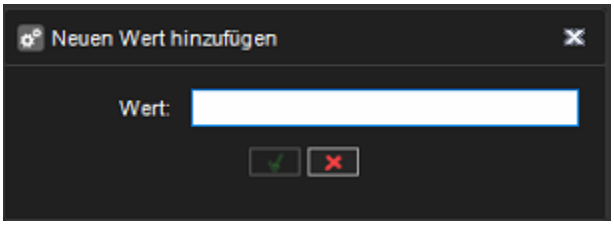
Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

9.2.9.5 Werte hinzufügen

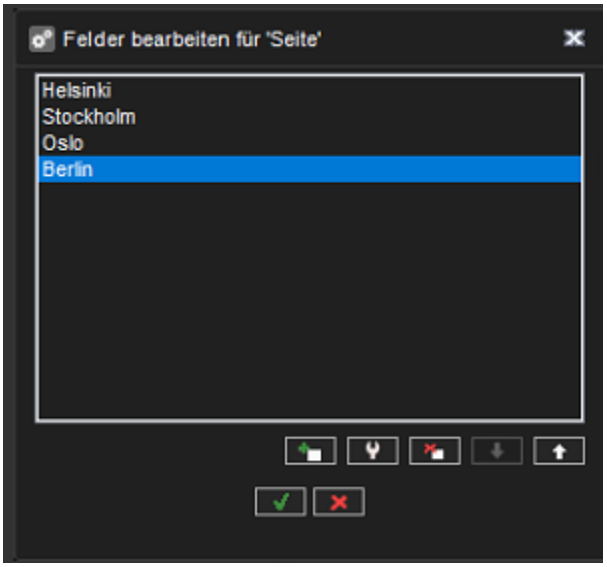
1. Wählen Sie das richtige Feld aus und klicken Sie auf **Werte aktualisieren**



1. Klicken Sie auf Wert hinzufügen
2. Geben Sie den Namen des Wertes ein
3. OK klicken

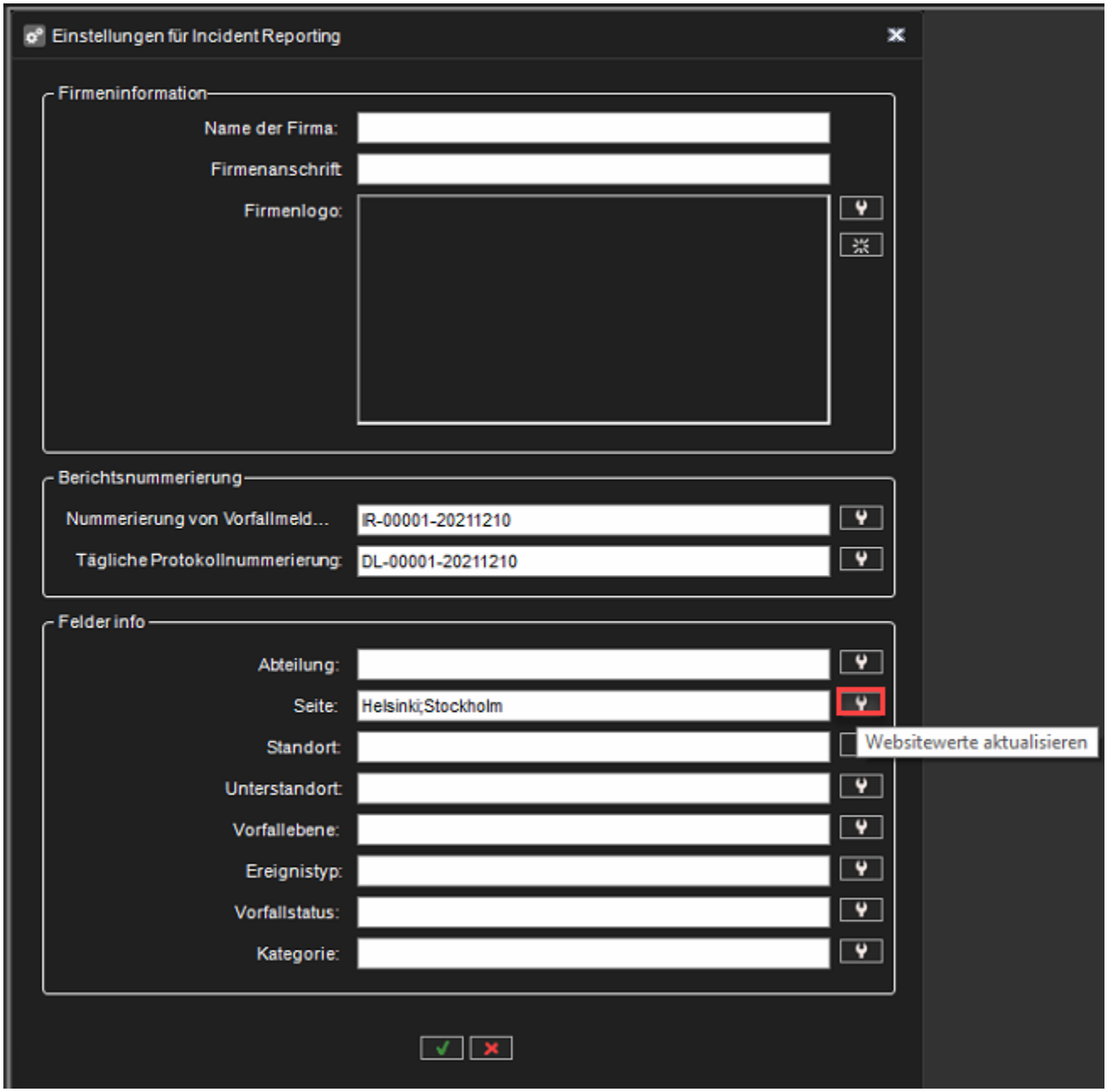


1. Neuer Mehrwert ist in der Liste zu sehen

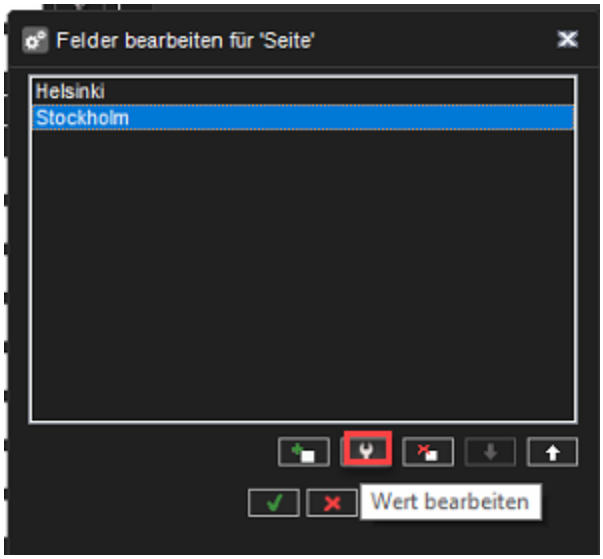


9.2.9.6 Werte bearbeiten

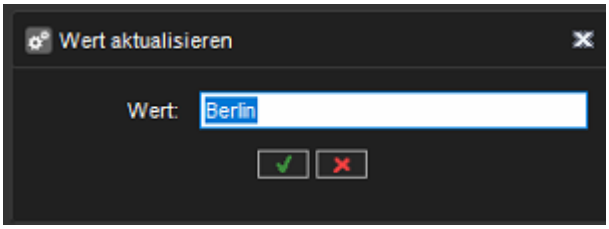
1. Klicken Sie auf das Symbol **Werte aktualisieren**



2. Wählen Sie einen Wert aus der Liste aus und klicken Sie auf Wert bearbeiten

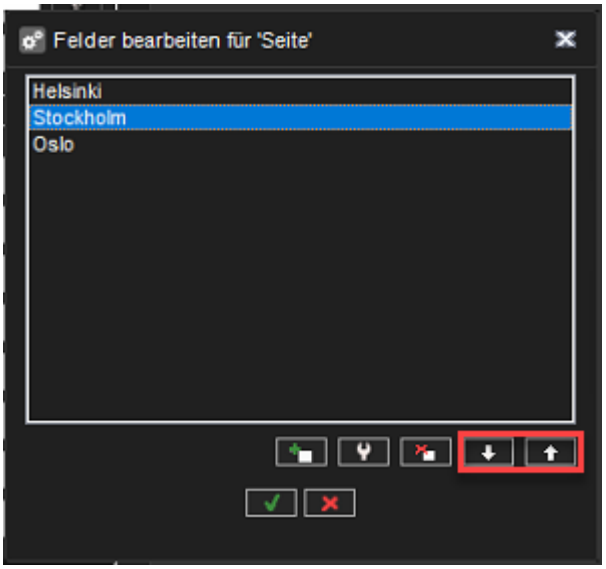


3. Geben Sie einen neuen Wertnamen ein und klicken Sie auf OK



9.2.9.7 Reihenfolge der Werte ändern

1. Wählen Sie den Wert aus und klicken Sie auf die Pfeile, um die richtige Reihenfolge der Werte festzulegen.
2. Klicken Sie auf OK um die Änderungen zu bestätigen



9.2.10 Einstellungen für Speicherschließfach

Storage Locker Settings enthält die folgenden Werte:

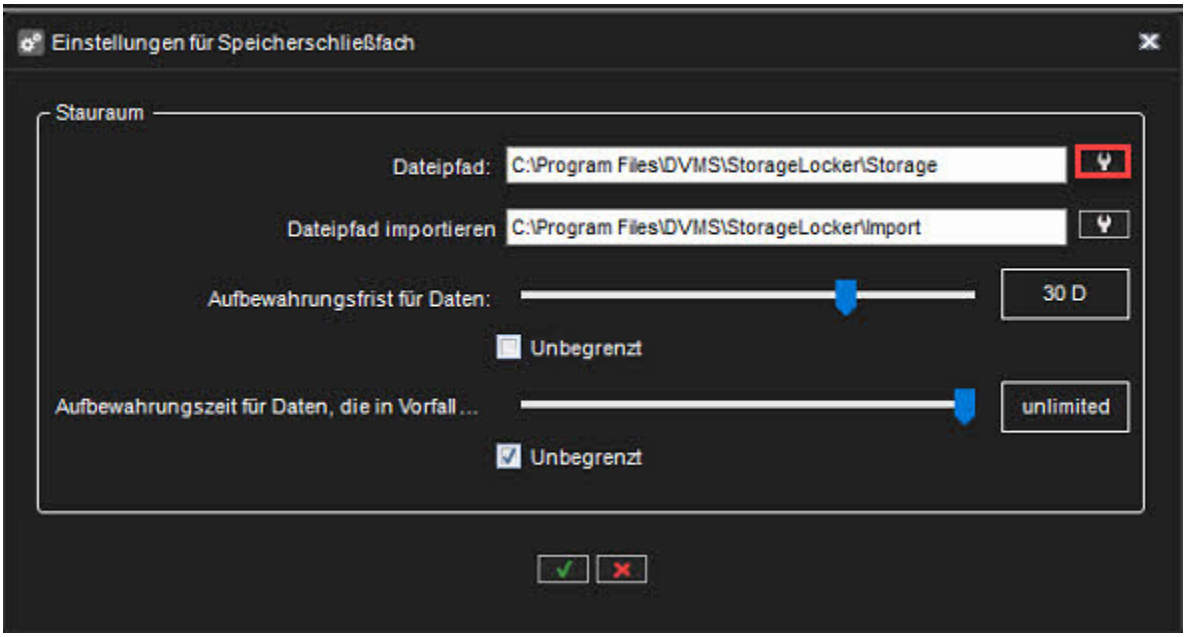
9.2.10.1 Dateipfad:

Definiert den Speicherort von Storage Locker.
Als Standardspeicherort befindet sich Storage Locker auf dem Hauptserver.

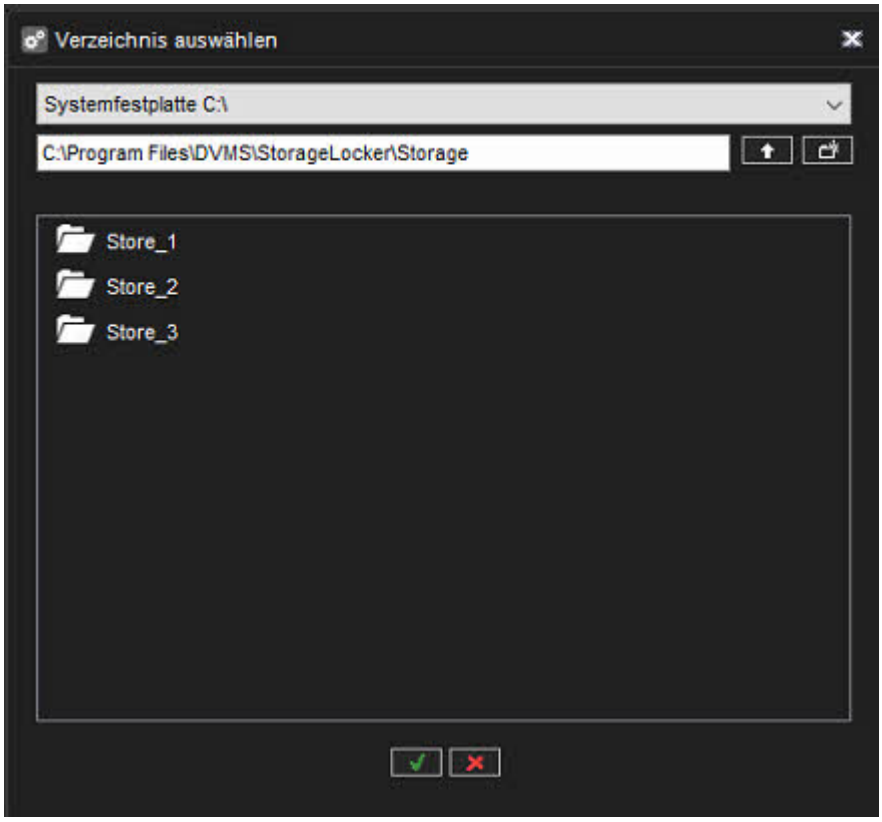
9.2.10.1.1 Dateipfad ändern

Bitte beachten Sie, dass die alten Locker-Daten des Speichers nicht an den neuen Speicherort kopiert werden

1. Klicken Sie auf Dateipfad für die Datenspeicherung festlegen



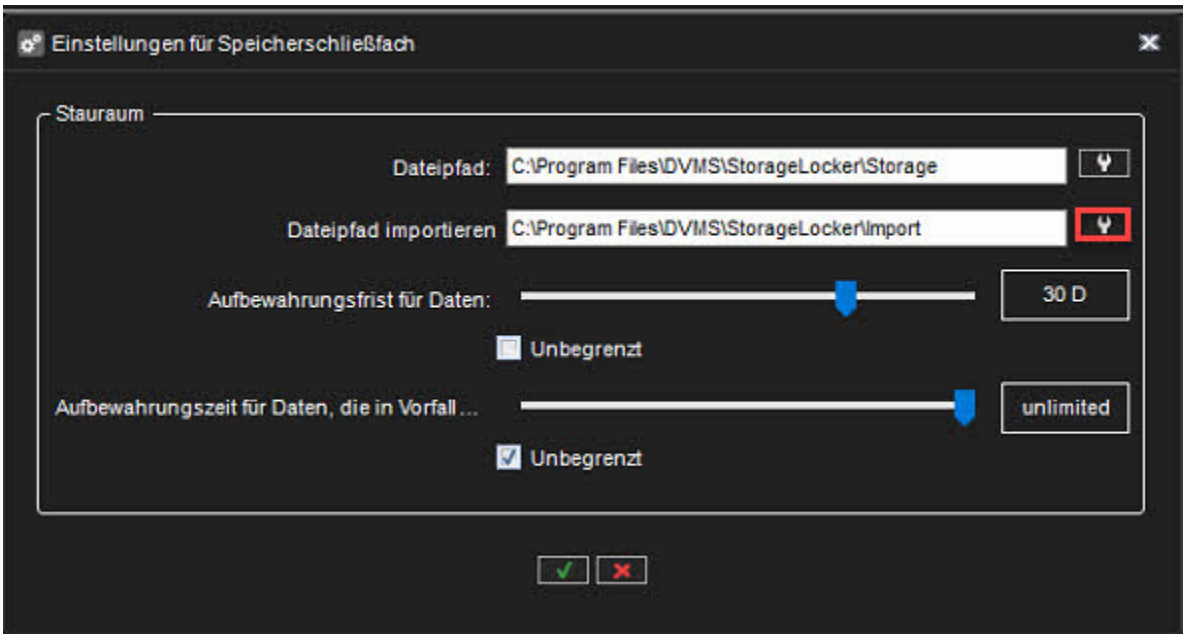
2. Wählen Sie einen neuen Standort und klicken Sie auf OK



9.2.10.2 Dateipfad importieren:

Wenn jemand Exporte hat, die zum Speicherschließfach hinzugefügt werden müssen, sollten diese Exporte in einem Ordner abgelegt werden, der in den Speicherschließfacheinstellungen als "Dateipfad importieren" definiert ist. Wie benutzt man:

- Alle Importdaten müssen sich in einem eigenen Ordner befinden, Dateien, die direkt im Importordner abgelegt werden, werden ignoriert
- Jeder Importordner kann mehrere Unterordner haben
- Bilder und Clips können in einem Ordner abgelegt werden, Storage Locker importiert sie einzeln
- SEF-Archive sollten sich in einem eigenen Ordner befinden und nicht mit anderen Daten (wie Bildern, Clips usw.)
- Importdaten sollten alle auf einmal kopiert werden, wenn etwas hinzugefügt werden soll - es sollte mit eigenem Ordner kopiert werden, Dateien, die zu bestehenden Ordnern hinzugefügt werden, werden nicht unterstützt (diese Dateien werden nicht verarbeitet)

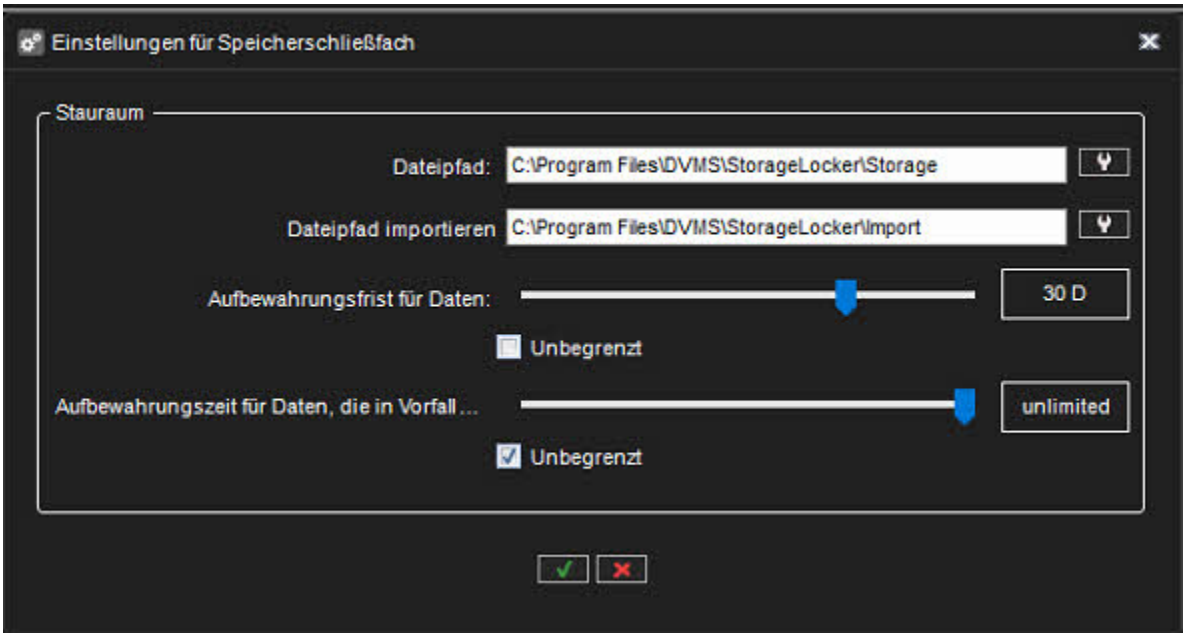


9.2.10.3 Die Aufbewahrungszeit für Daten

Die Aufbewahrungszeit für Datensätze definiert, wie lange Storage Locker Daten aufbewahrt, die in keinem Vorfallbericht verwendet werden

9.2.10.4 Die Aufbewahrungszeit für Daten, die in den Vorfallberichten verwendet werden

Die Aufbewahrungszeit für Daten, die in Vorfallberichten verwendet werden, definiert, wie lange Storage Locker Daten aufbewahrt, die in jedem Vorfallbericht verwendet werden

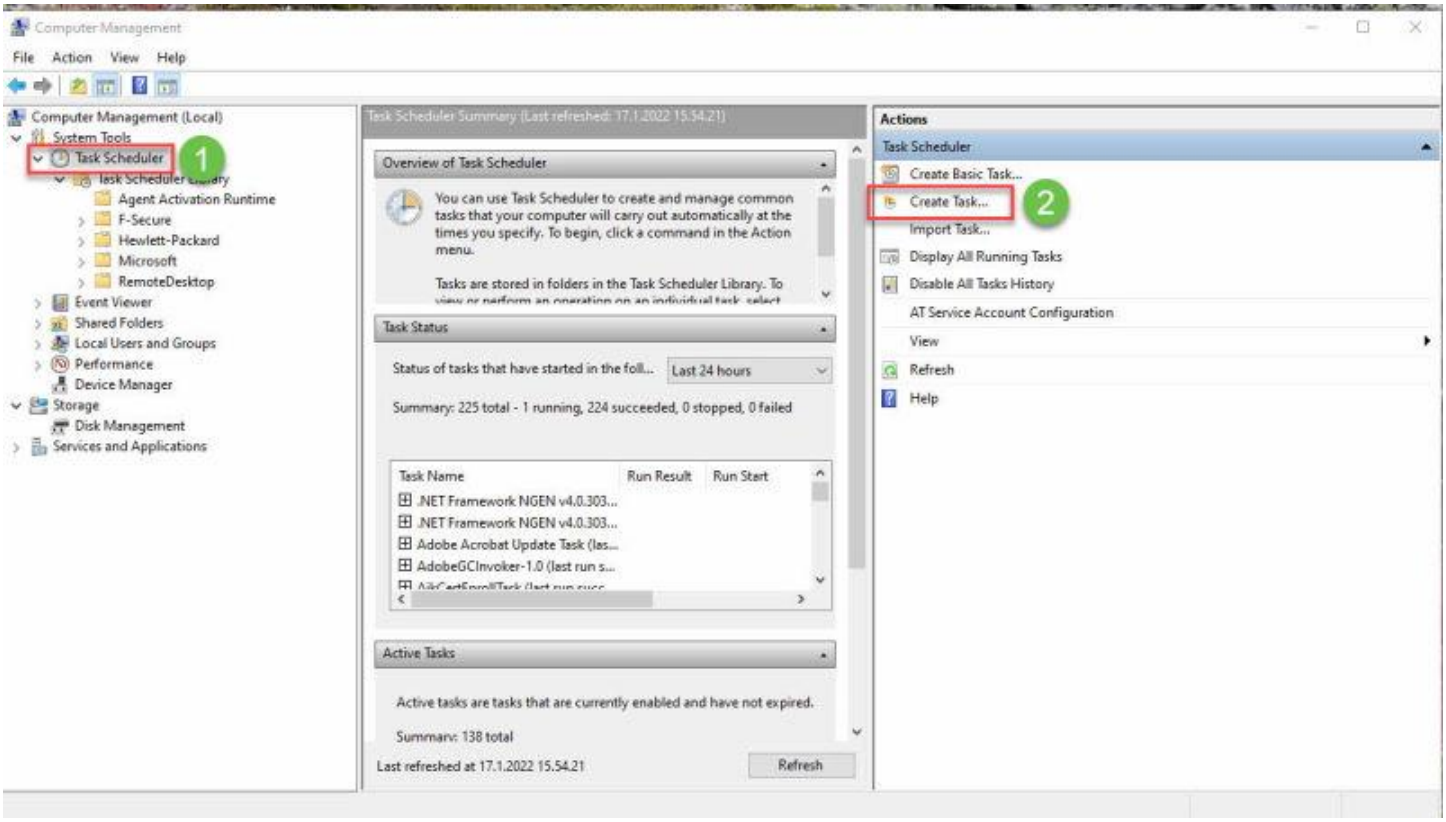


9.2.10.5 Schritte zum Zuordnen eines Netzlaufwerks, das für Storage Locker-Daten verwendet werden kann

Erstellen Sie eine Stapeldatei (siehe Details zur Stapeldatei) und speichern Sie sie am gewünschten Ort. In meinem Fall habe ich diese Batchdatei unter C:\temp mit dem Namen „SysinternalSuite.bat“ gespeichert.

- Lauf**cd C:\temp\SysinternalsSuite psexec -i -s cmd.exe /c net use S: "\\172.17.100.10\storageforvms" /user:vms sharepassword /persistent:Yes**

1. offen**Task Scheduler**
2. klicken**Create Task**

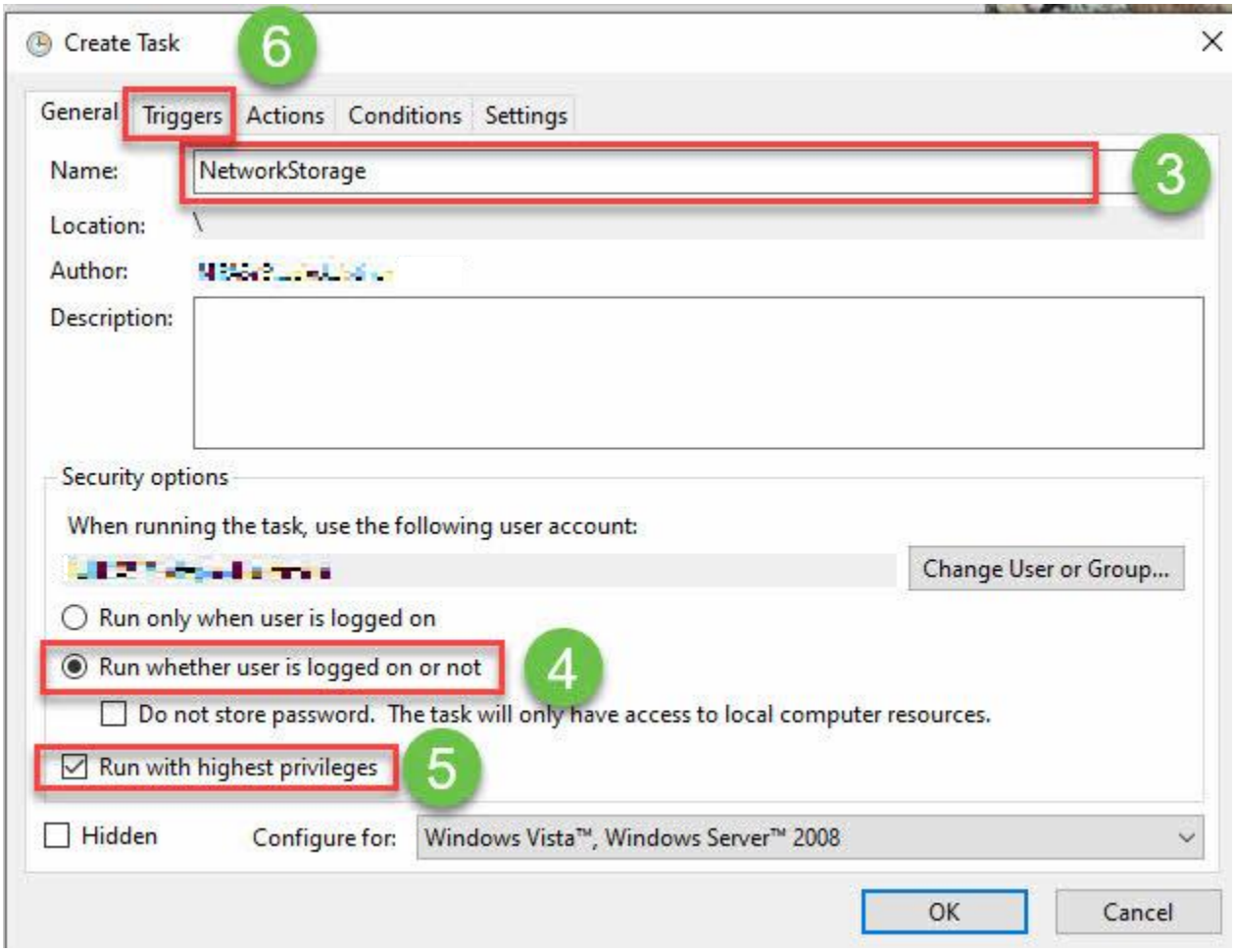


3. Name eingeben

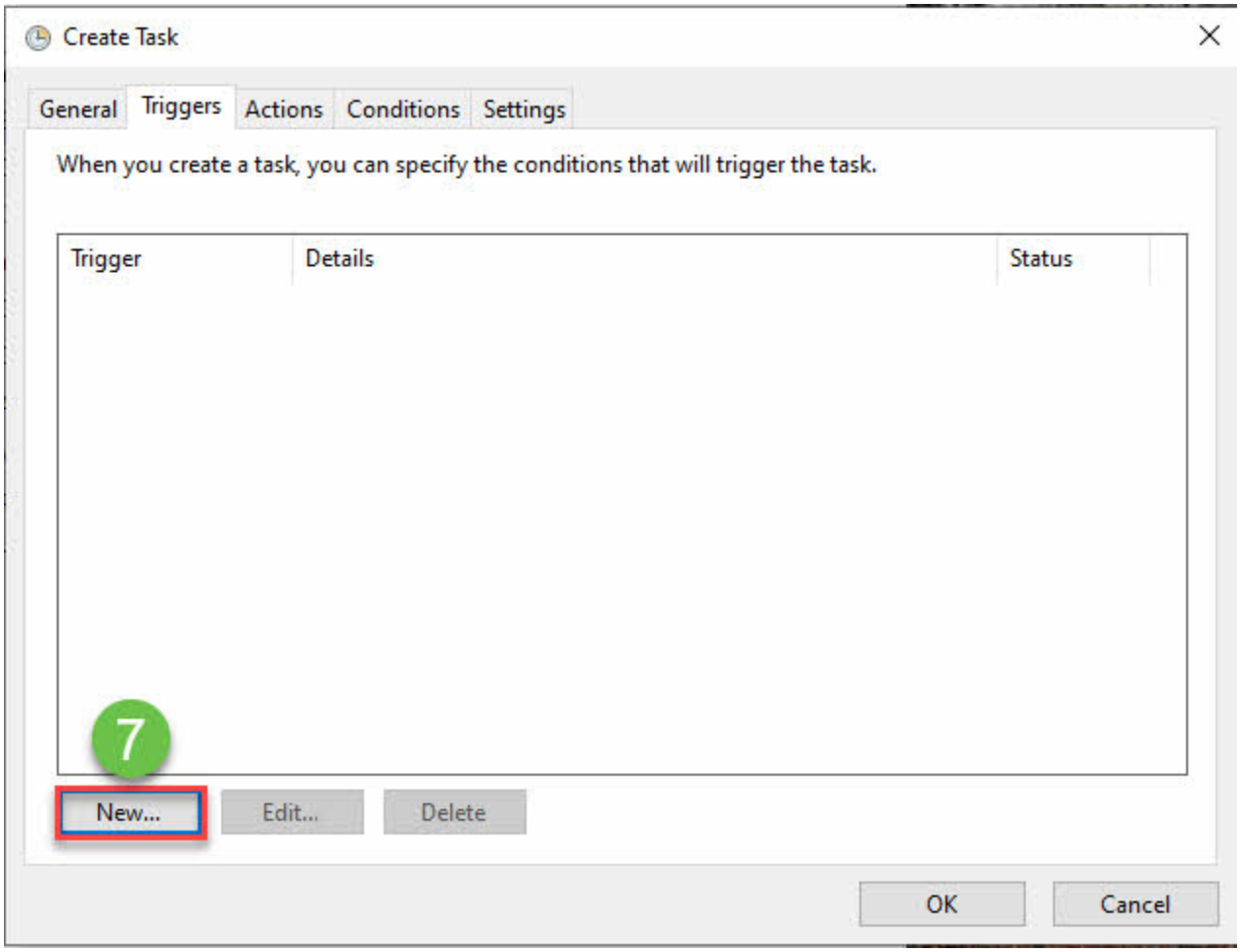
4. Ermöglichen **Run whether the user is logged on or not**

5. Ermöglichen **Run with highest privilege**

6. Offen **Triggers**

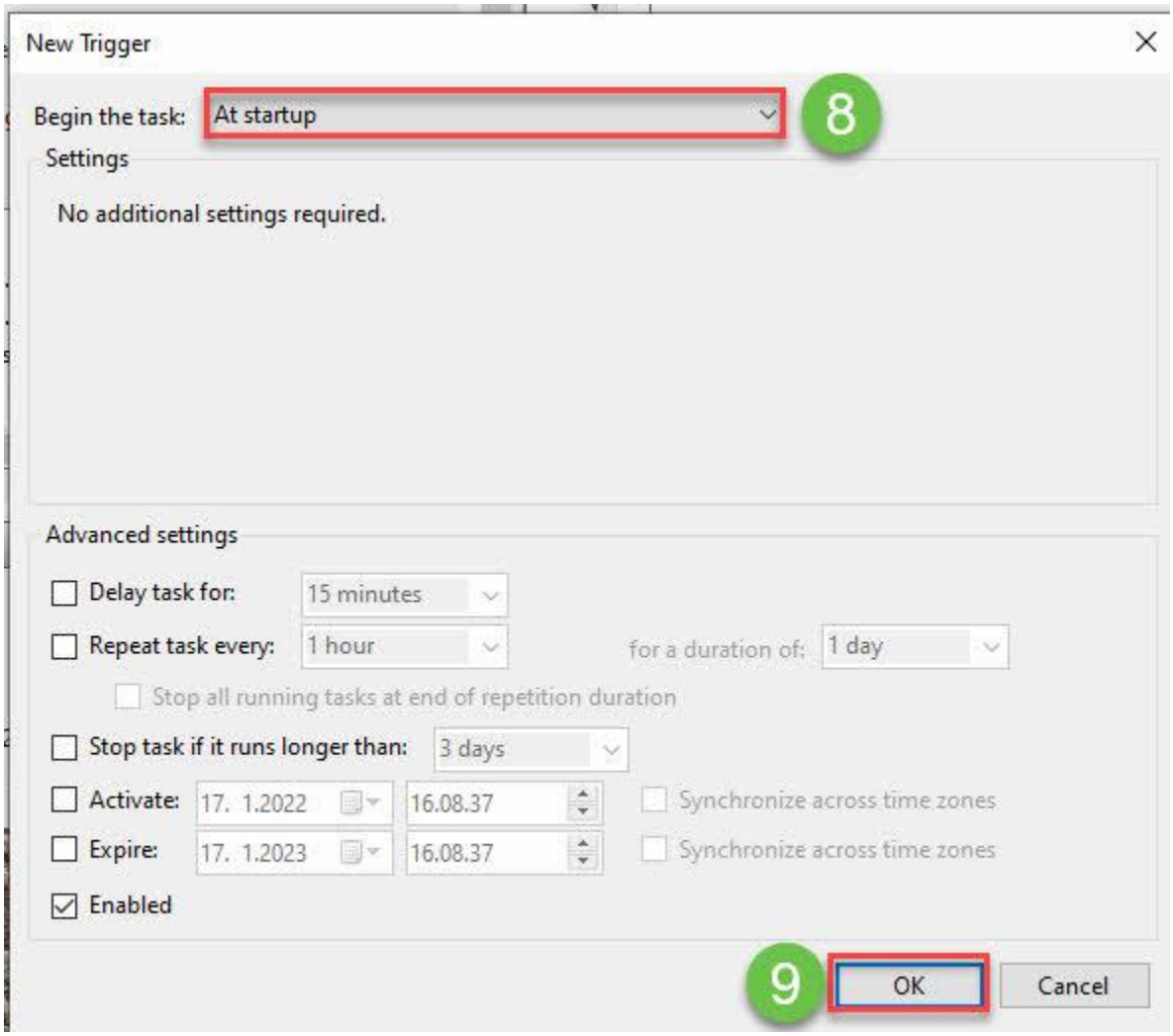


7. Klicken **New**



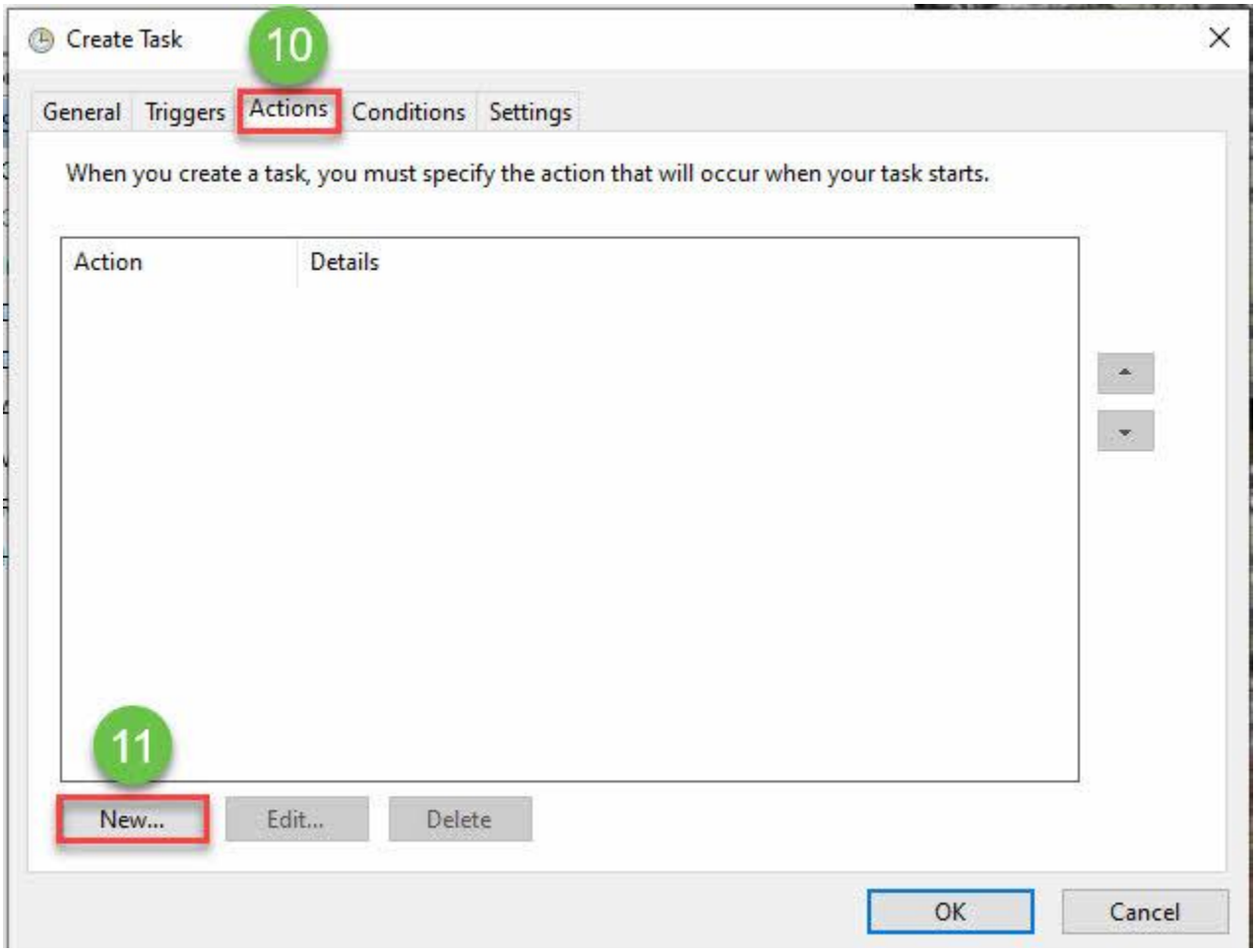
8. wählen At startup from the Begin the task dropdown list

9. Klicken**OK**



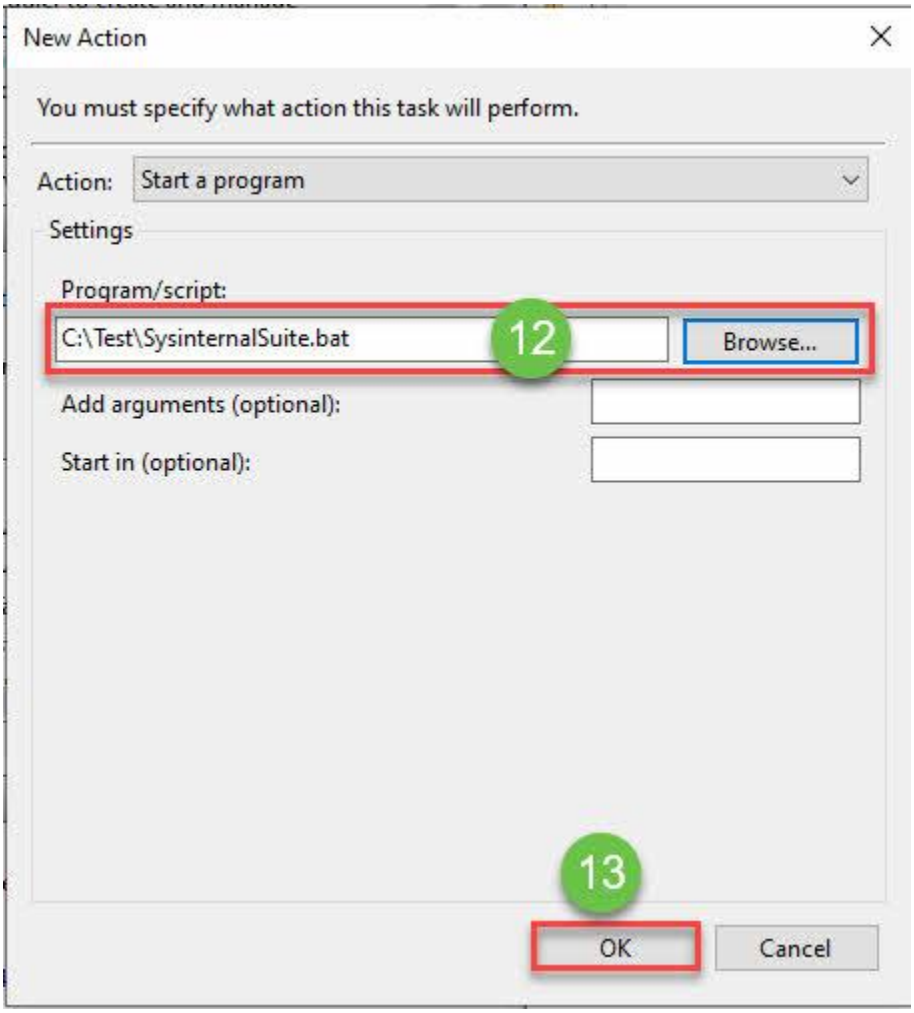
10. oppen **Actions**

11. Klicken **New**



12. Durchsuchen Sie den Speicherort des Skripts und wählen Sie Skript aus

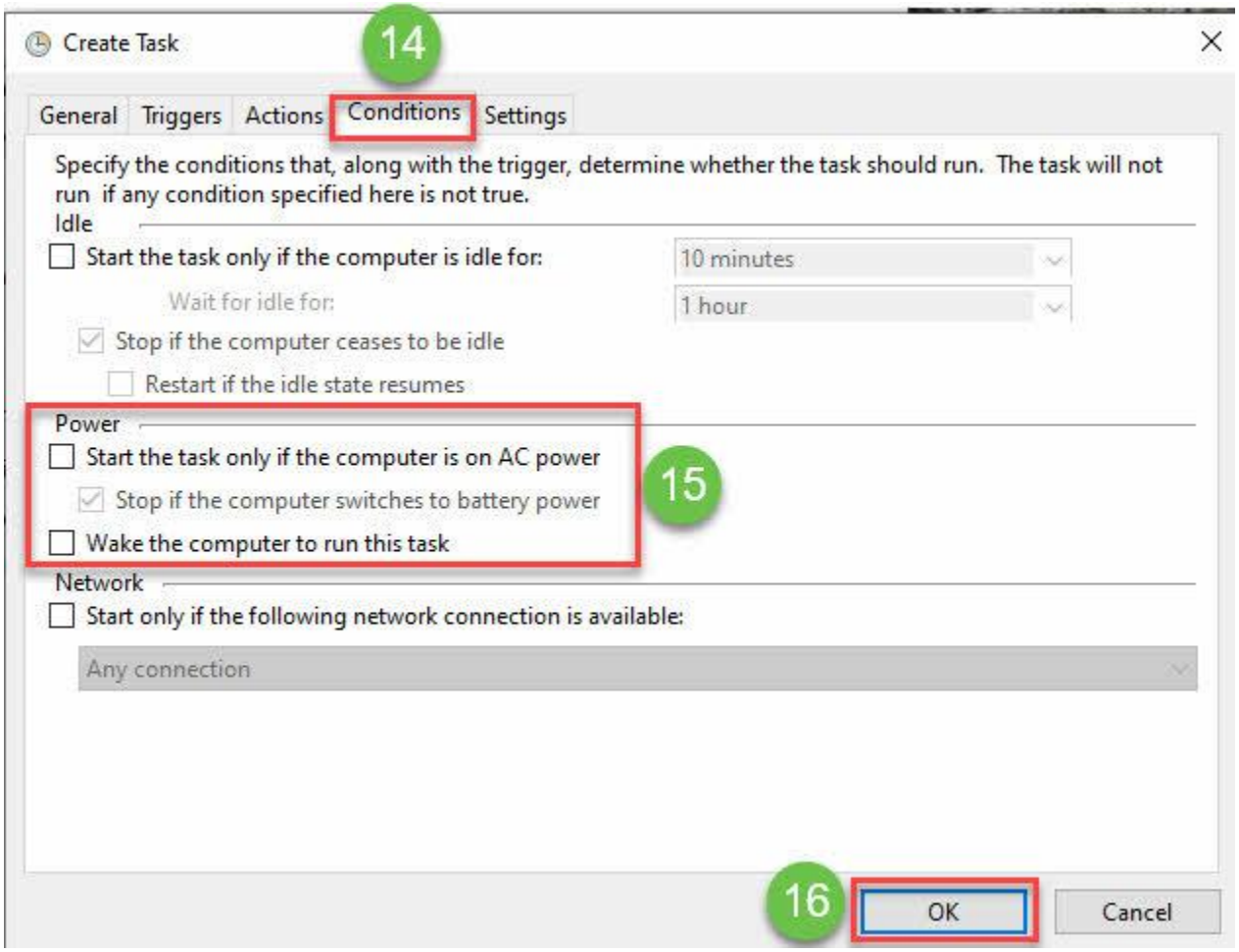
13. Klicken **OK**



14. oppen**Conditions**

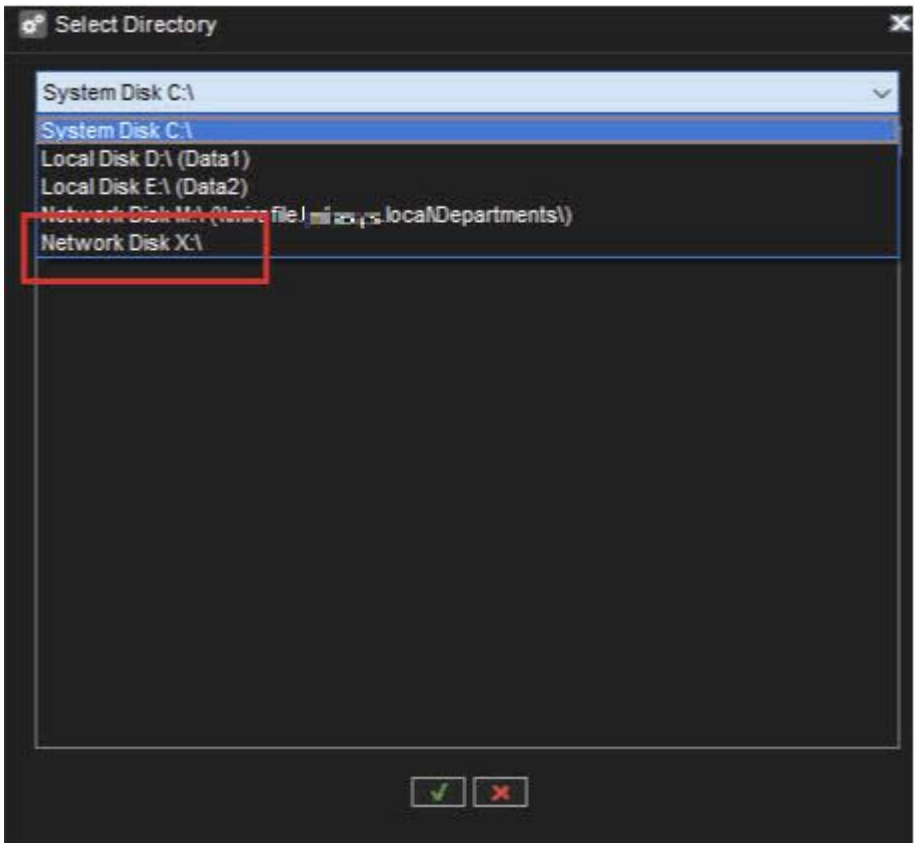
15. Deaktivieren **tart the task only if the computer is on AC power** and **Wake the computer to run this task**

16. Klicken **OK**



Beachten Sie, dass in Mein PC das neu erstellte zugeordnete Laufwerk für ALLE Benutzer dieses Systems angezeigt wird, aber sie sehen es als „Getrenntes Netzwerklaufwerk (X:)“ angezeigt.(Wenn das Laufwerk passwortgeschützt ist, wird der Benutzer aufgefordert, das Passwort einzugeben, nachdem er auf die Schaltfläche OK geklickt hat.)

Öffnen Sie nun den System-Manager, navigieren Sie zu den Storage Locker-Einstellungen und beobachten Sie, dass das zugeordnete Laufwerk in der Liste angezeigt wird.



1. Laufwerk aus der Liste auswählen
2. Klicken **OK**



9.2.11 Storage Locker Einstellungen

Storage Locker Settings enthält die folgenden Werte:

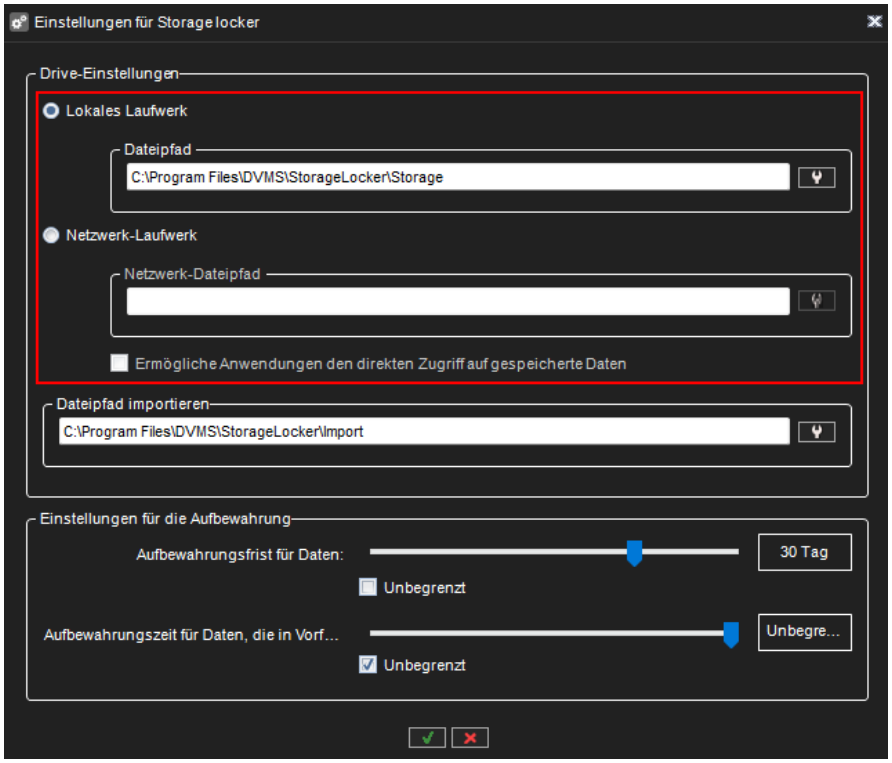
9.2.11.1 Dateipfad:

Legt den Speicherort der Storage Locker-Datei fest, der entweder ein lokales oder ein Netzwerklaufwerk sein kann. Als Standardspeicherort befindet sich der Storage Locker-Dateispeicher auf der lokalen Festplatte des Hauptserver. Ändern des Dateipfads

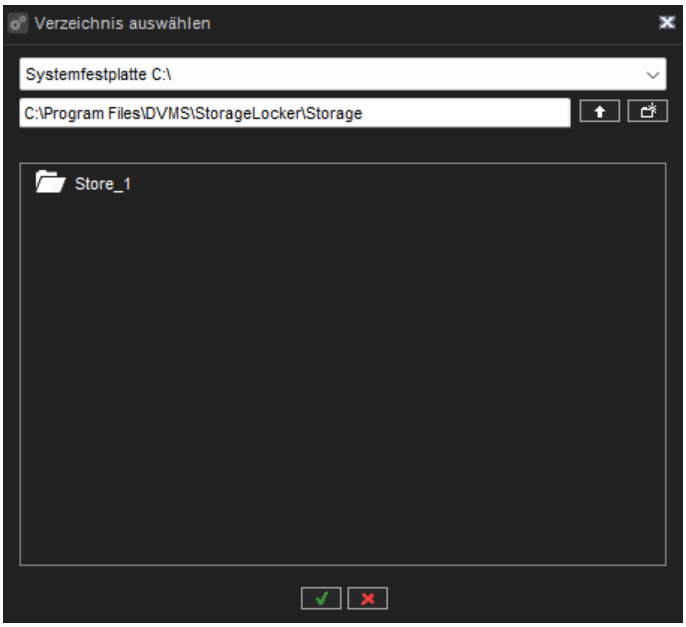
9.2.11.2 Ändern des Dateipfads

Bitte beachten Sie, dass alte Schließfachdaten nicht an den neuen Speicherort kopiert werden

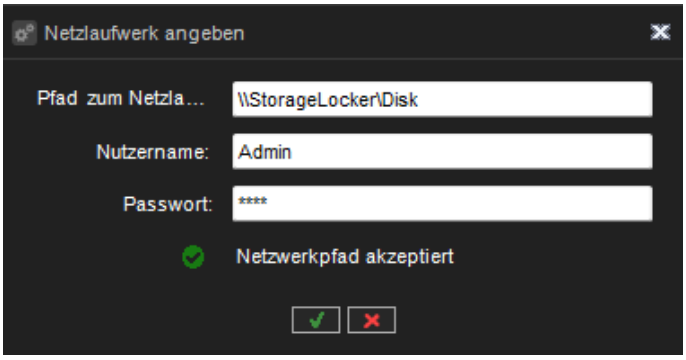
1. Wählen Sie, ob ein lokales Laufwerk oder ein Netzlaufwerk verwendet werden soll.



1. Wenn das lokale Laufwerk ausgewählt ist, klicken Sie auf Dateipfad für Datenspeicherung festlegen. Wählen Sie einen neuen Speicherort und klicken Sie auf OK.



1. Wenn ein Netzlaufwerk ausgewählt ist, klicken Sie auf Netzwerk-Dateipfad für die Datenspeicherung festlegen. Geben Sie den Netzwerkpfad, den Benutzernamen und das Passwort an und klicken Sie auf OK.

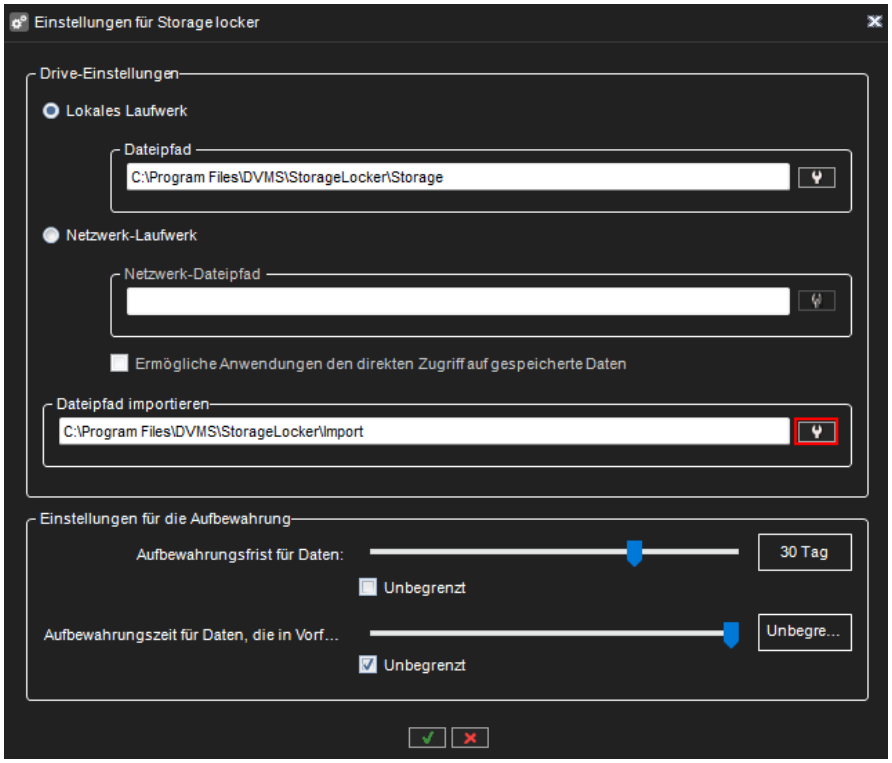


Wenn ein Netzlaufwerk für die Speicherung von Storage Locker-Daten verwendet wird, ist es möglich, Spotter-Anwendungen den direkten Zugriff auf gespeicherte Daten vom Netzlaufwerk zu gestatten, indem Sie die Option Anwendungen den direkten Zugriff auf gespeicherte Daten erlauben aktivieren.

9.2.11.3 Pfad der Importdatei

Wenn jemand Exporte hat, die zum Speicherschrank hinzugefügt werden müssen, sollten diese Exporte in einem Ordner abgelegt werden, der in den Einstellungen des Speicherschranks als "Pfad für Importdateien" definiert ist. Wie zu verwenden:

- Jede Importdatei muss sich in einem eigenen Ordner befinden, Dateien, die direkt in den Importordner gelegt werden, werden ignoriert.
- Jeder Importordner kann mehrere Unterordner haben
- Bilder und Clips können in einem Ordner abgelegt werden, Storage Locker importiert sie nacheinander
- SEF-Archive sollten sich in einem eigenen Ordner befinden und nicht mit anderen Daten (wie Bildern, Clips usw.) vermischt werden
- Importdaten sollten auf einmal kopiert werden, wenn etwas hinzugefügt wird - sollte es in einen eigenen Ordner kopiert werden, Dateien, die zu bestehenden Ordnern hinzugefügt werden, werden nicht unterstützt (diese Dateien werden nicht verarbeitet)

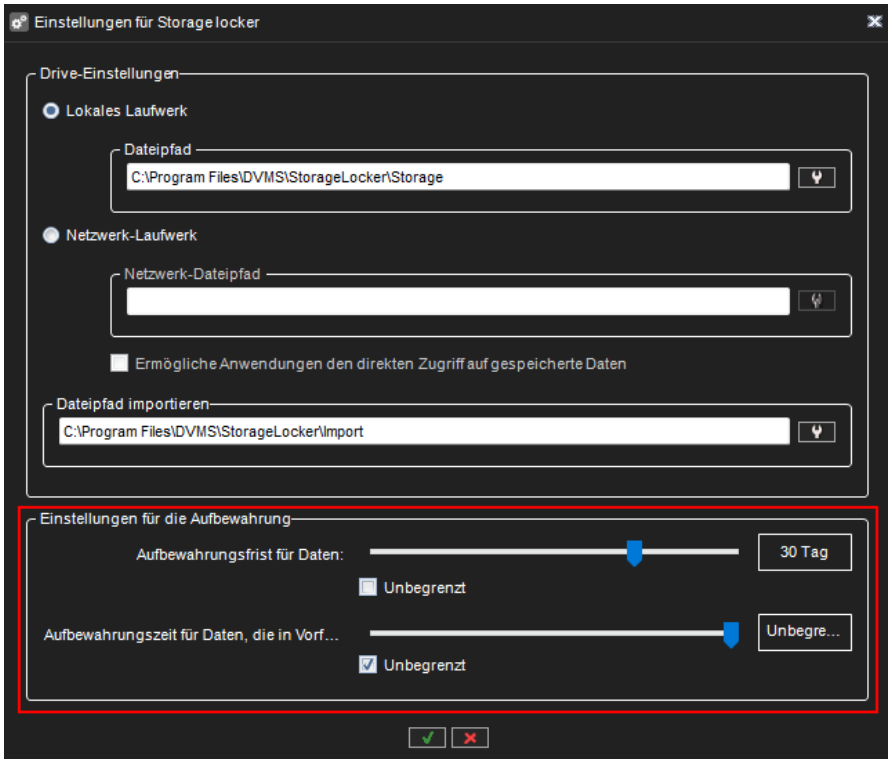


9.2.11.4 Die Aufbewahrungszeit für Daten

Die Aufbewahrungszeit für Datensätze legt fest, wie lange Storage Locker Daten aufbewahrt, die nicht in einem Vorfallsbericht verwendet werden

9.2.11.5 Die Aufbewahrungszeit für Daten, die in den Vorfallsberichten verwendet werden

Die Aufbewahrungszeit für Daten, die in Vorfallsberichten verwendet werden, legt fest, wie lange Storage Locker Daten, die in einem Vorfallsbericht verwendet werden, aufbewahrt



9.2.12 Einstellungen für die List Management

Die Listenverwaltung ermöglicht es, Identitäten und Listen zu definieren, so dass die erlaubten oder nicht erlaubten Identitäten festgelegt werden können.

Die Einstellungen definieren und verwalten die Einstellungen für die Identitäts- und Listenverwaltung. Mit den Einstellungen können Sie:

- Hinzufügen, Bearbeiten und Löschen von Identitäten mit Nummernschildern und Gesichtsbildern
- Hinzufügen, Bearbeiten und Löschen von Listen und Verwalten von Listeninhalten
- Import und Export von Listen und Identitäten
- Konfigurieren von Speichergrenzen für LPR- und FR-Ereignisdatenbanken
- Aktivieren und Definieren der Integration und ihrer Einstellungen

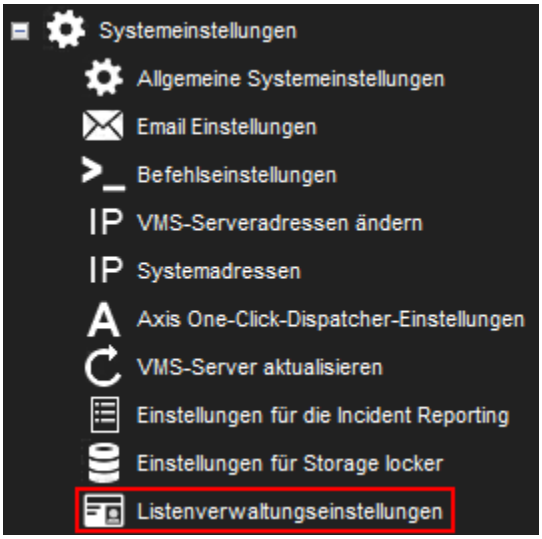
Die Systemmanager-Anwendung bietet mehrere Dialoge für den Zugriff und die Änderung von Daten und Einstellungen des Listenverwaltungsdienstes. Die Dialoge finden Sie im Abschnitt "Systemeinstellungen".

Die Integration erfordert eine LPR- und FR-Integrationslizenz.

9.2.12.1 Einstellungen für die Listenverwaltung

So öffnen Sie das Dialogfeld Einstellungen für die Listenverwaltung:

1. Gehen Sie auf die Registerkarte **System**
2. Doppelklicken Sie unter **Systemeinstellungen** auf den Baumknoten **Listenverwaltungseinstellungen**, wie in der Abbildung unten dargestellt:



1. Wenn Sie auf **Listenverwaltungseinstellungen** doppelklicken, wird der Dialog geladen, die Einstellungen werden vom Listenverwaltungsdienst angefordert und bei Erfolg angezeigt. Wenn das Laden fehlschlägt, wird dem Benutzer eine Fehlermeldung angezeigt, und der Dialog wird geschlossen.

9.2.12.2 Dialogfeld „Listenverwaltungseinstellungen“

In dem Dialog finden Sie die folgenden Registerkarten:

- **Identitäten** - Liste der Identitäten und deren Einstellungen
- **Listen** - Identitätslisten und deren Einstellungen
- **Import/Export** - Import/Export-Funktionalität zum Wiederherstellen/Speichern von Listenverwaltungsdaten im CSV-Textformat
- **Datenbankeinstellungen** - Parameter, die sich auf die Datenbank des Listenverwaltungsdienstes beziehen
- **Integrationseinstellungen** - Aktivierung der Integration und Integrationseinstellungen

Alle Änderungen, die Sie in diesen Dialogregistern vornehmen, können durch Klicken auf die Schaltfläche **OK** gespeichert werden.

Wenn Sie die Änderungen nicht behalten wollen, können Sie den Dialog mit der Schaltfläche **Schließen** oder **Abbrechen** schließen.

Nachfolgend finden Sie eine detaillierte Beschreibung der einzelnen Registerkarten.

9.2.12.2.1 Registerkarte „Identitäten”

Auf der Registerkarte **Identitäten** können Sie Operationen mit Identitäten durchführen:

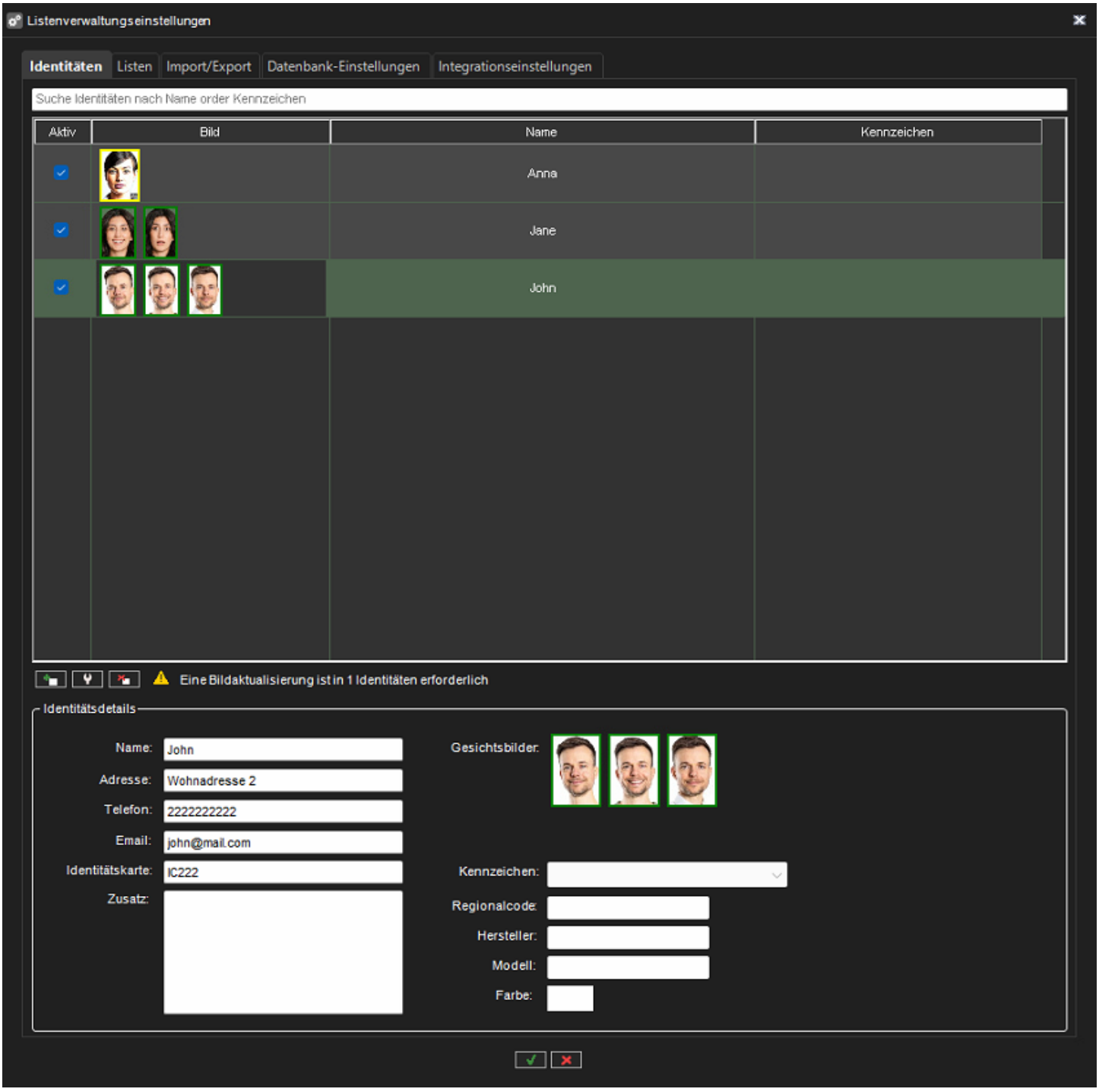


Figure 1 Registerkarte „Identitäten"

Die Auswahl von Identitäten erfolgt mit der linken Maustaste. Wenn Sie mehrere Identitäten auswählen müssen (mehrere Zeilen in der Liste), können Sie die linke Maustaste + Strg/Umschalttaste verwenden. Bei

Mehrfachauswahl können Sie die ausgewählten Identitäten in den Zustand "aktiv" oder "nicht aktiv" versetzen, indem Sie auf die Kontrollkästchen in der Spalte "Aktiv" klicken.

Oberhalb der Liste der Identitäten befindet sich das Feld **Suchen**: Wenn Sie hier etwas eingeben, wird die Liste der Identitäten automatisch gefiltert, wenn der Text in Identitätsnamen oder -kennzeichen enthalten ist.

Mit den Schaltflächen **Hinzufügen** und **Entfernen** unterhalb der Identitätsliste können Sie ausgewählte Identitäten hinzufügen oder entfernen.

Im **Bereich Identitätsdetails** können Sie detaillierte Informationen zur Identität anzeigen, aber alle diese Felder sind schreibgeschützt. Um die ausgewählte Identität zu ändern, können Sie auf die Schaltfläche **Ändern** klicken oder mit der Maustaste darauf doppelklicken.

Wenn Sie eine Identität hinzufügen oder ändern, wird das folgende Dialogfeld angezeigt:

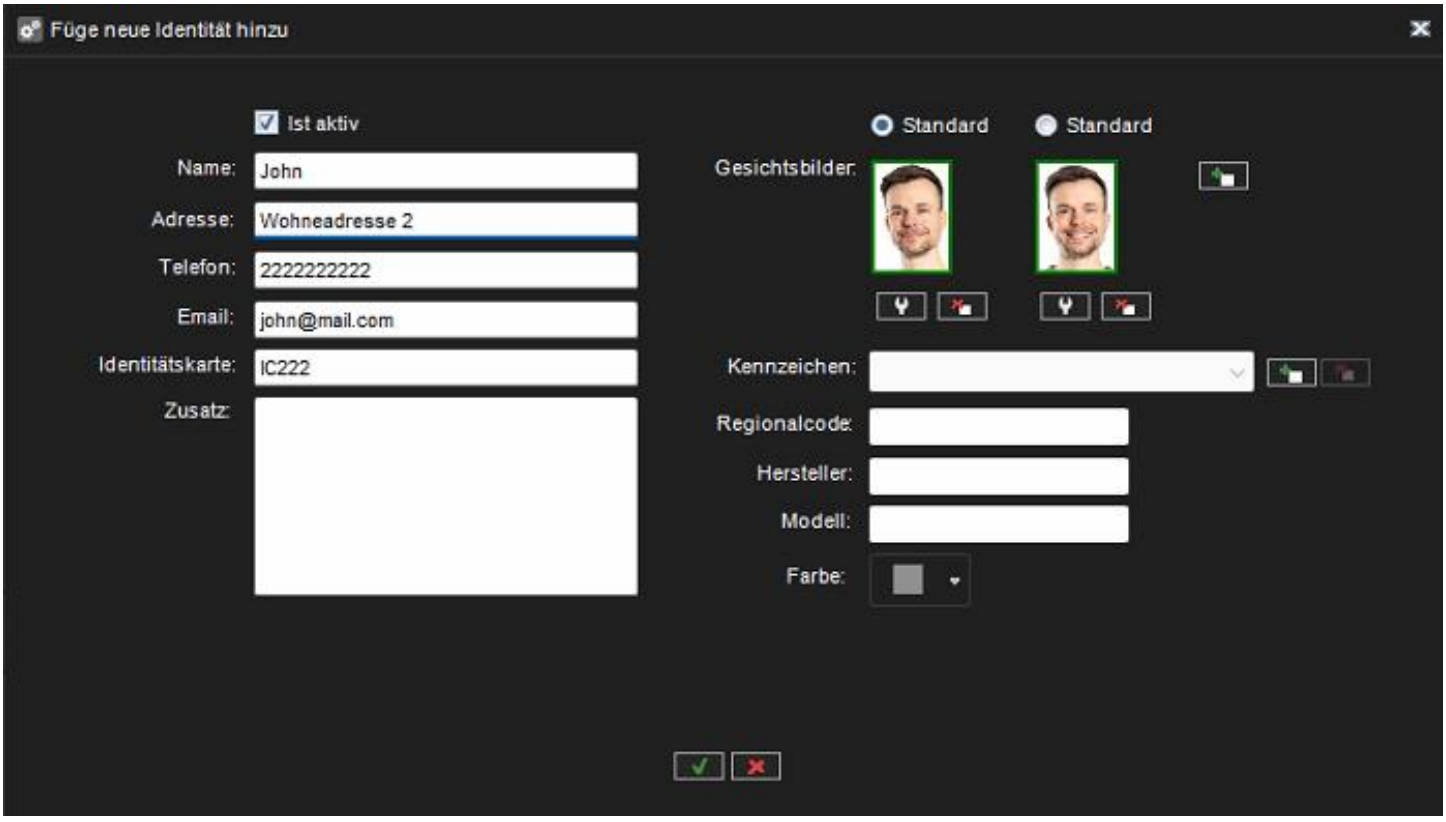


Figure 2 Dialog zum Hinzufügen/Ändern der Identität

Sie können alle Felddaten ändern oder Bilder von Gesichtern oder Fahrzeugen (Nummernschildern) hinzufügen/entfernen.

Um ein Gesichtsbild hinzuzufügen, klicken Sie auf die Schaltfläche **Fügen sie ein neues Gesichtbild hinzu** und der folgende Dialog wird geöffnet:

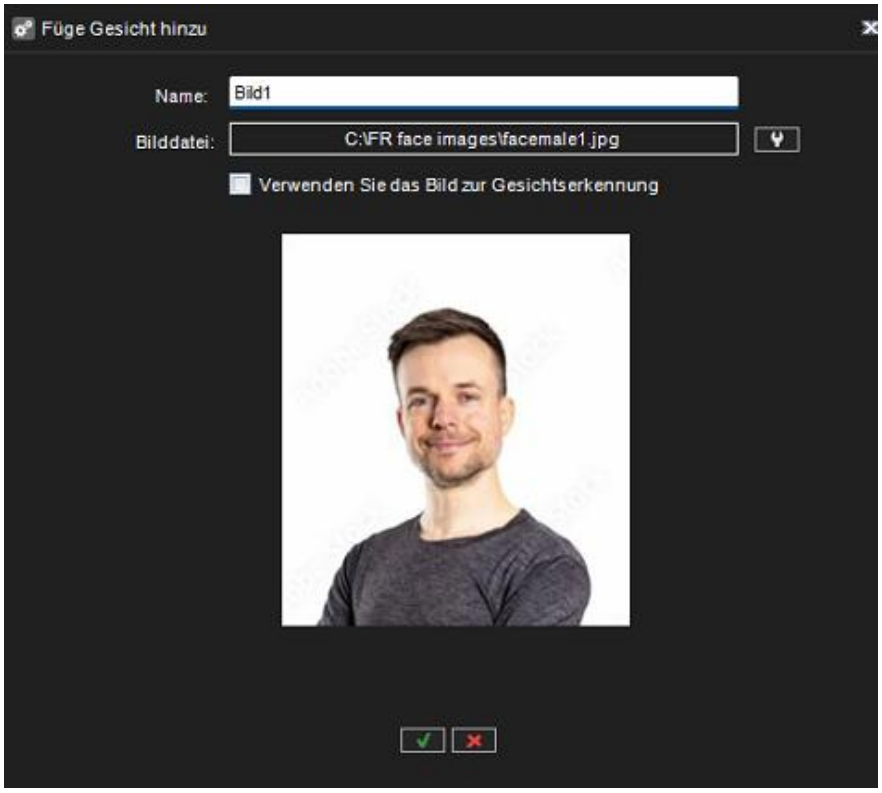


Figure 3 Dialogfeld „Füge Gesicht hinzu“

Hier können Sie einen Gesichtsbildnamen eingeben und eine Gesichtsbilddatei auswählen. Nach der Auswahl der Datei wird das Bild geladen, und die Merkmalsvektordaten des Bildes werden berechnet. Ein Bild kann für die Gesichtserkennung ausgewählt werden, indem Sie das Kontrollkästchen „Bild für Gesichtserkennung verwenden“ aktivieren. Um ein Gesichtsbild zu entfernen, klicken Sie im Dialogfeld „Identität hinzufügen/ändern“ unterhalb des Bildes auf die Schaltfläche **Ausgewähltes Gesichtsbild entfernen**.

Die maximale Anzahl von Gesichtsbildern für eine Identität beträgt 3. Alle für die Gesichtserkennung ausgewählten Gesichtsbilder werden beim Abgleich von Identitätsgesichtern verwendet. Die Verwendung mehrerer Gesichtsbilder für eine Identität kann daher die Zuverlässigkeit der Gesichtserkennung erhöhen.

Um den Vektor der Gesichtsmerkmale zu berechnen, muss mindestens ein Gesichtserkennungsdienst gestartet und im VMS registriert sein

9.2.12.2.1.1 Anforderungen an die Bildqualität von Gesichtern

Bilder, die für die Gesichtserkennung verwendet werden, müssen eine Mindestauflösung von 168 x 256 Pixel haben, um Fehlzuordnungen zu vermeiden. Die Mindestgröße des Gesichts im Bild beträgt 112 Pixel. Wenn ein Bild als zu groß erkannt wird, wird es automatisch in der Größe angepasst.

Der Qualitätswert eines Bildes wird durch eine von drei Farben in einem Umriss um das Bild herum angezeigt. Rot (niedrig) bedeutet, dass das Bild aufgrund nicht erfüllter Qualitätsanforderungen nicht akzeptiert wird. Gelb (mittel) bedeutet, dass das Bild zwar verwendet werden kann, es jedoch empfohlen wird, es durch ein Bild mit höherer Qualität zu ersetzen. Grün (hoch) bedeutet, dass das Bild die Qualitätsanforderungen erfüllt und daher verwendet werden kann. Der Qualitätswert für Gesichter wird für alle ausgewählten Bilder in den Identitätseinstellungen angezeigt, und der Benutzer erhält eine Warnmeldung, wenn mindestens eines der verwendeten Identitätsgesichtsbilder aktualisiert werden muss. Identitäten in der Identitätsliste können anhand der Bildqualität (von niedrig bis hoch oder umgekehrt) sortiert werden, indem Sie auf die Bildspalte klicken.

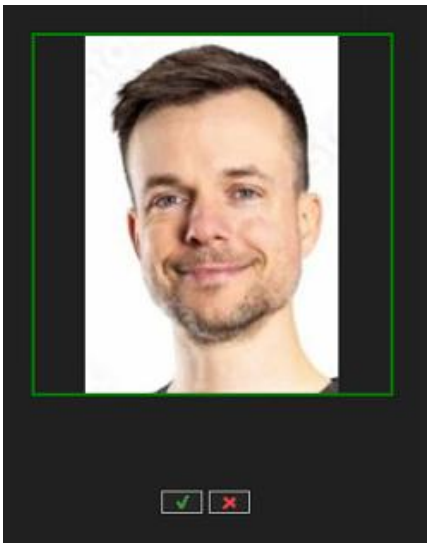


Figure 4 Gesichtsbild mit guter Qualität



Figure 5 Gesichtsbild mit mittlerer Qualität

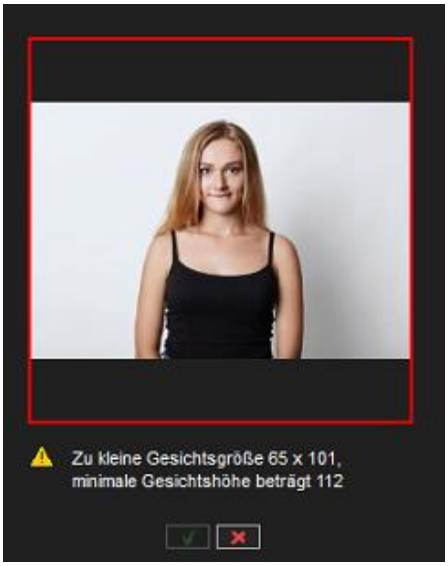


Figure 6 Gesichtsbild mit geringer Qualität

9.2.12.2.1.2 Auswahl von Bildern für FR und LPR

Der Systemadministrator kann auswählen, welche Identitätsbilder für FR und LPR verwendet werden. Es werden Bilder in hoher Qualität empfohlen, da diese zu einer genaueren Gesichtserkennung beitragen. Wenn nur die Kennzeichenerkennung verwendet wird, kann der Administrator ein beliebiges Identitätsbild auswählen. Ein Bild für die Gesichtserkennung kann ausgewählt werden, indem im Dialogfeld zum Hochladen von Identitätsbildern die Option „Bild für Gesichtserkennung verwenden“ aktiviert wird oder indem eine vorhandene Identität geändert und

auf **Ausgewähltes Identitätsbild bearbeiten** geklickt wird, wodurch das Dialogfeld für Identitätsbilder geöffnet wird, in dem dieselbe Option aktiviert werden kann.

9.2.12.2.1.3 Gesichtsbild als Standard festlegen

Eines der Gesichtsbilder für eine Identität wird als Standardbild verwendet. Ein Identitätsbild kann als Standardbild festgelegt werden, indem Sie im Dialogfeld „Identität hinzufügen/ändern“ über dem Bild auf das Optionsfeld **Standard** klicken:

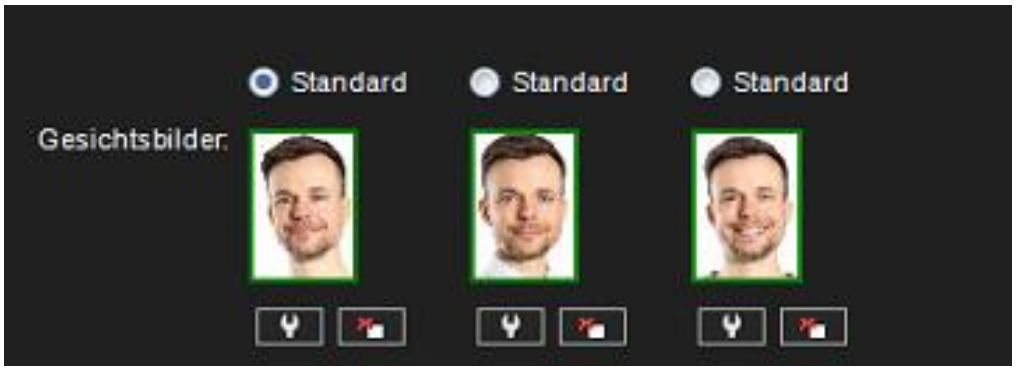


Figure 7 Ein Gesichtsfoto als Standard festlegen

9.2.12.2.1.4 Fahrzeuge hinzufügen oder entfernen

Sie können Fahrzeuge hinzufügen oder entfernen. Um ein Fahrzeug hinzuzufügen, klicken Sie auf die Schaltfläche **Neues Fahrzeug hinzufügen**, woraufhin sich der folgende Dialog öffnet:



Figure 8 Dialogfeld „Fahrzeug hinzufügen"

Im Dialogfeld **Fahrzeug hinzufügen** können Sie das Kennzeichen, die Vorwahl, den Hersteller, das Modell und die Fahrzeugfarbe eingeben. Um ein Fahrzeug zu entfernen, müssen Sie es im Kombinationsfeld auswählen und auf die Schaltfläche Ausgewähltes **Fahrzeug entfernen** klicken.

9.2.12.2.2 Registerkarte Listen

Auf der Registerkarte **Listen** können Sie Operationen mit Identitätslisten durchführen:

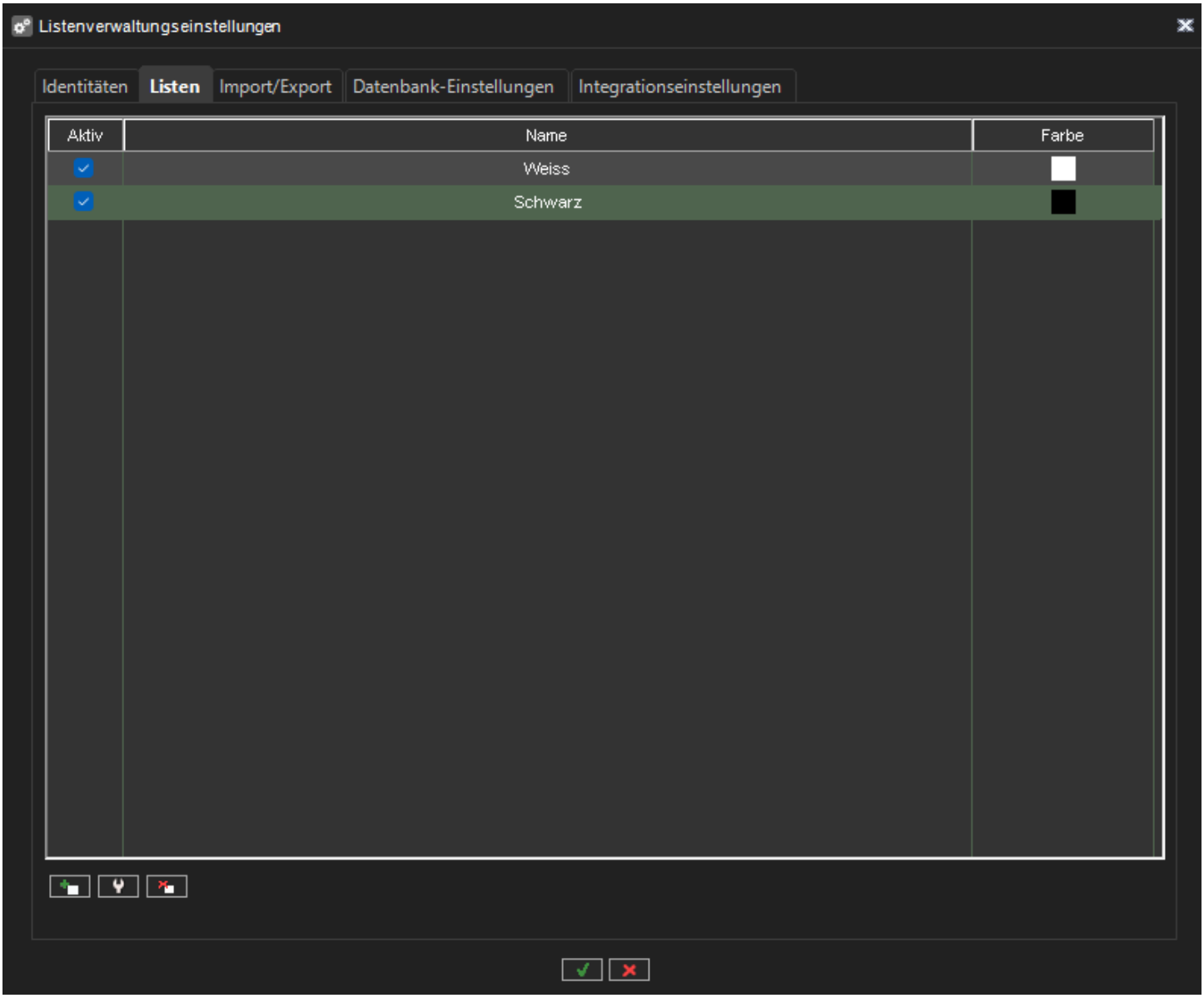


Figure 9 Registerkarte „Listen"

Die Listenauswahl erfolgt mit der linken Maustaste. Wenn Sie mehrere Listen (mehrere Zeilen) auswählen müssen, können Sie die linke Maustaste + Strg/Umschalttaste verwenden. Bei Mehrfachauswahl können Sie die ausgewählten Listen durch Anklicken der Kontrollkästchen in der Spalte **Aktiv** in den Zustand **aktiv** oder **nicht aktiv** versetzen.

Mit den Schaltflächen **Hinzufügen** und **Entfernen** unter den Listen können Sie ausgewählte Listen hinzufügen oder entfernen.

Um die ausgewählte Identitätsliste zu ändern, können Sie auf die Schaltfläche **Ändern** klicken oder mit der Maustaste darauf doppelklicken.

Wenn Sie die Identitätsliste hinzufügen oder ändern, wird das folgende Dialogfeld angezeigt:

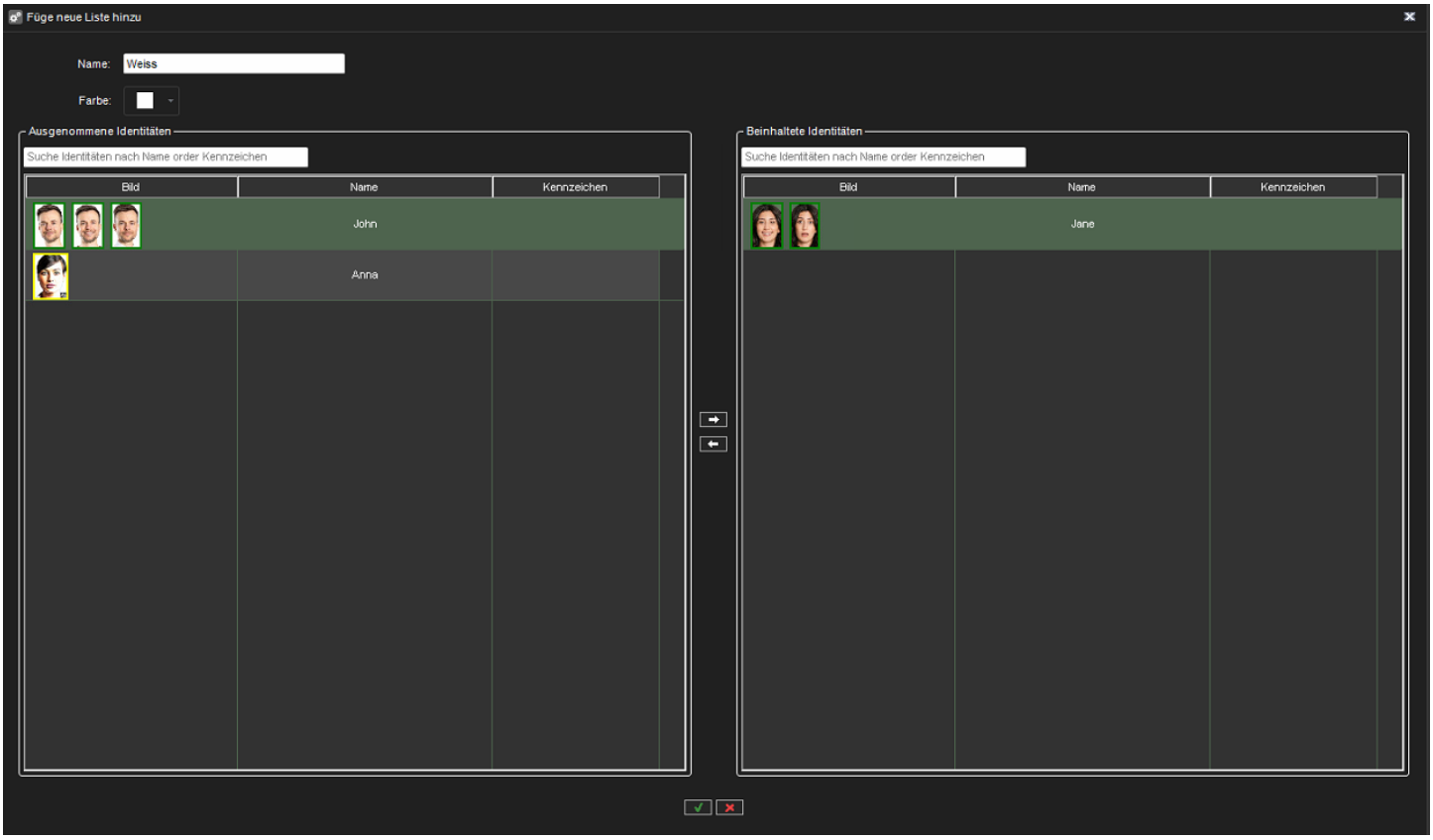


Figure 10 Dialogfeld zum Hinzufügen/Ändern von Listeneinstellungen

Sie können Identitäten in die Liste verschieben oder sie aus der Liste entfernen, den Namen der Liste und die Farbe festlegen.

9.2.12.2.3 Registerkarte „Import/Export"

Auf der Registerkarte **Import/Export** können Sie Listenverwaltungsdaten aus einer CSV-Datei importieren oder Listenverwaltungsdaten in eine CSV-Datei exportieren:

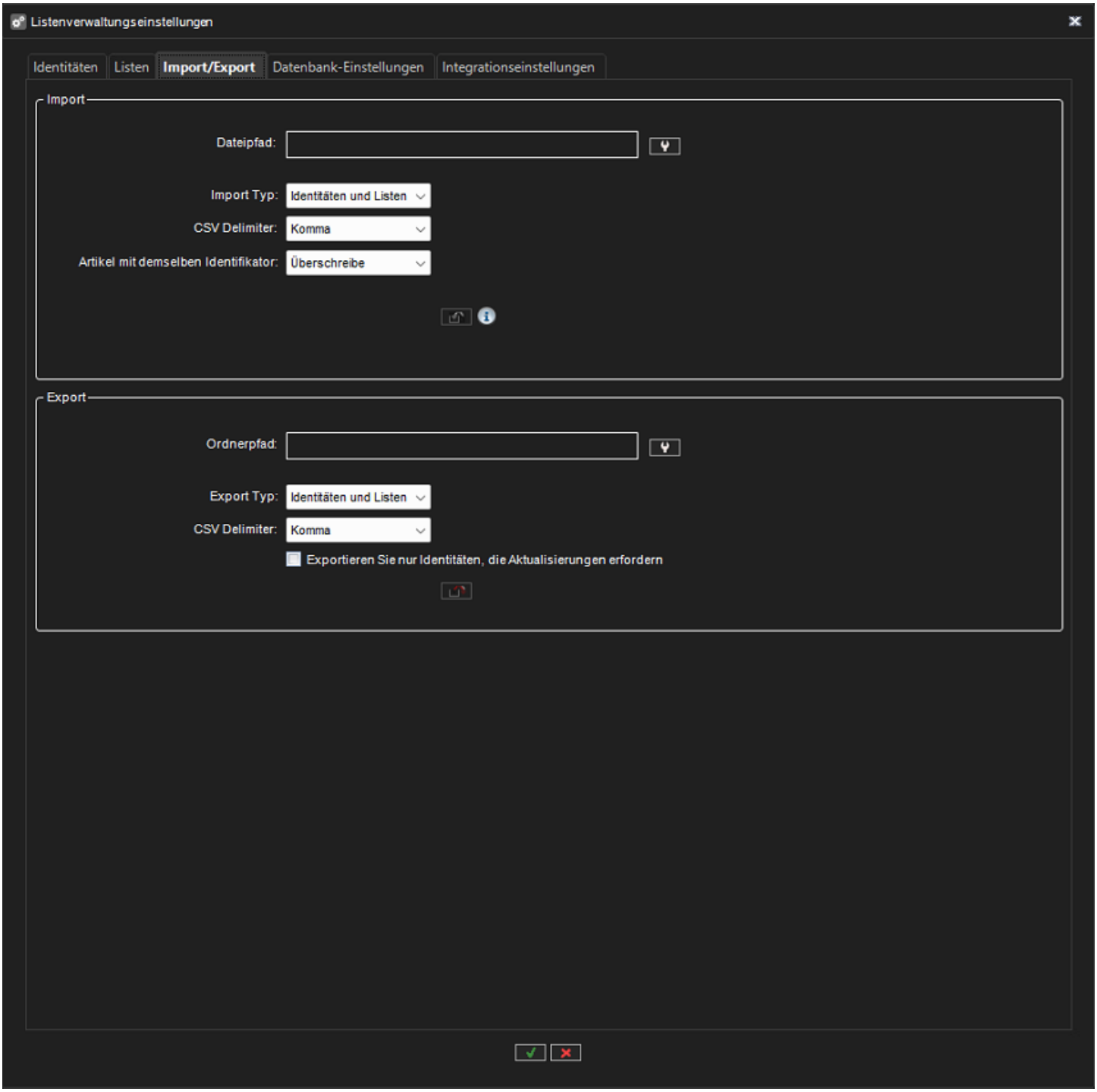


Figure 11 Registerkarte Import/Export

9.2.12.2.3.1 Parameter für den Import

Die folgenden Parameter müssen für den Importvorgang festgelegt werden:

- **Dateipfad** - Pfad zu der CSV-Datei, die die Listenverwaltungsdaten enthält
- **Importtyp** - "Nur Identitäten" oder "Identitäten und Listen"
- **CSV-Begrenzer** - "Komma" oder "Semikolon"
- **Elemente mit der gleichen Kennung** - "Überspringen", "Überschreiben" oder "Neue" Kennung für sie erstellen

Wenn die richtigen Parameter ausgewählt sind, wird die Schaltfläche **Daten aus Datei importieren** aktiviert, und der Benutzer kann den Importvorgang starten. Während des Prozesses sehen die Benutzer den Fortschritt und das Ergebnis des Imports.

9.2.12.2.3.2 Parameter für den Export

Die folgenden Parameter müssen für den Exportvorgang festgelegt werden:

- **Ordnerpfad** - Pfad zu dem Ordner, in den die Listenverwaltungsdaten exportiert werden und in dem die CSV-Datei erstellt wird
- **Exporttyp** - "Nur Identitäten" oder "Identitäten und Listen"
- **CSV-Begrenzungszeichen** - "Komma" oder "Semikolon"
- **Exportieren Sie nur Identitäten, die Aktualisierungen erfordern** - kann ein- oder ausgeschaltet werden

Wenn die richtigen Parameter ausgewählt sind, wird die Schaltfläche **Daten in Datei exportieren** aktiviert, und der Benutzer kann den Exportvorgang starten. Während des Prozesses sehen die Benutzer den Fortschritt und das Ergebnis des Exports.

Wenn das System auf eine neue Version aktualisiert wird, müssen alte Gesichtsbilder mit Kompatibilitätsproblemen, die mit FR verwendet werden, für alle Identitäten in den Einstellungen der Listenverwaltung erneut hinzugefügt werden. Der Benutzer erhält dazu eine Warnung im LMS-Installationsprogramm (die Warnung wird nur angezeigt, wenn das Upgrade Gesichtsmerkmalsvektoren aus einer älteren Version enthält). Identitätsbilder können einzeln oder in großen Mengen mithilfe des CSV-Datei-Imports und -Exports aktualisiert werden. Wenn der CSV-Import Gesichtsbilder von geringer Qualität enthält, erhält der Benutzer eine Warnung. Der Identitätsexport kann verwendet werden, um nur die Identitäten mit Bildern von geringer Qualität zu exportieren, wodurch es einfach ist, eine große Anzahl veralteter Bilder zu aktualisieren.

9.2.12.2.4 Registerkarte „Datenbankeinstellungen”

Auf der Registerkarte **Datenbankeinstellungen** können Sie die Datenbankeinstellungen für den Listenverwaltungsdienst festlegen:

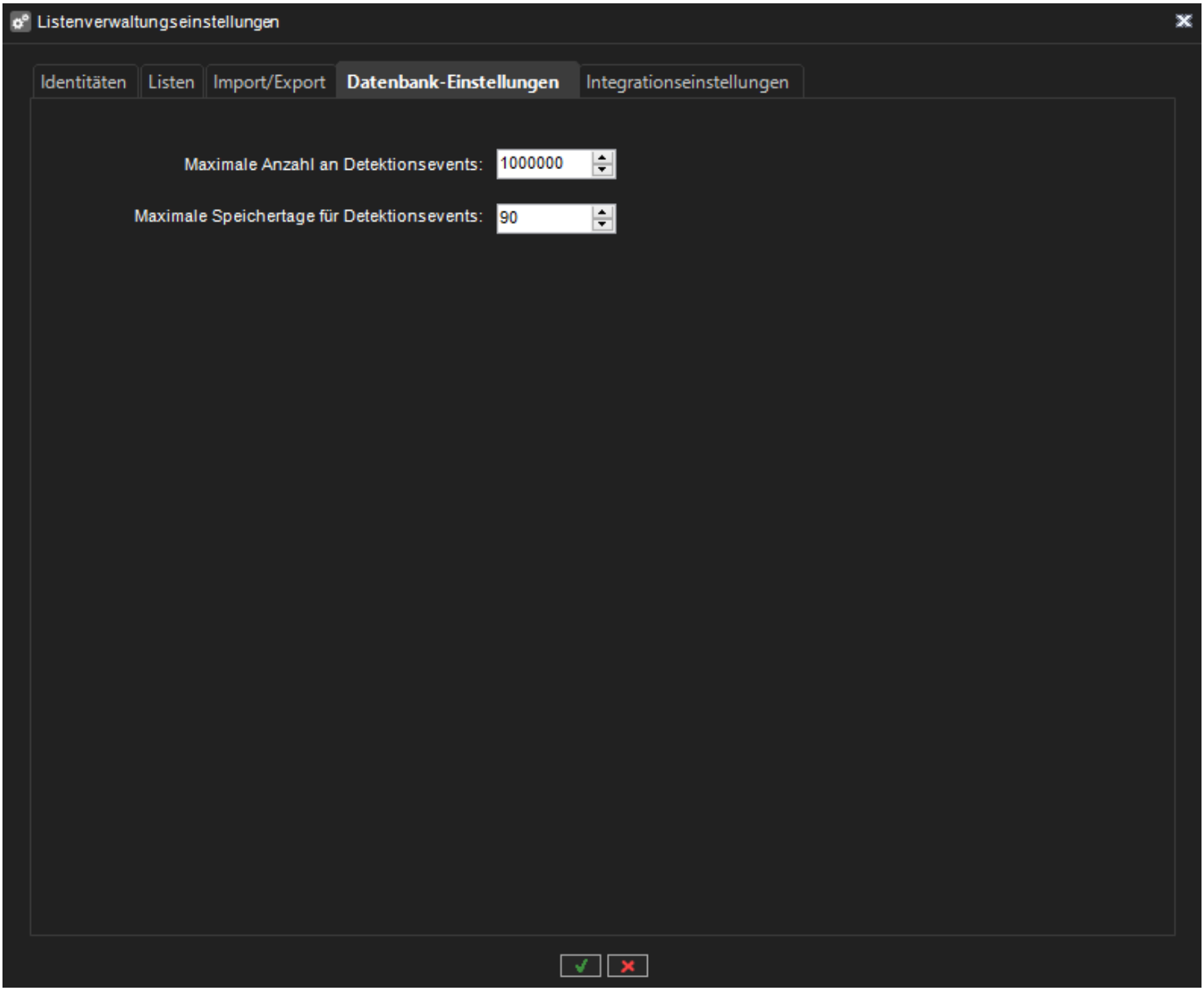


Figure 12 Registerkarte „Datenbankeinstellungen"

WARNUNG: Die Verwendung hoher Grenzwerte kann zu unbeabsichtigter Massenlöschung von Daten und einer erhöhten Systemauslastung führen. Es wird empfohlen, zunächst mit niedrigeren Grenzwerten zu beginnen und die Ergebnisse zu überprüfen, bevor umfangreichere Vorgänge ausgeführt werden.

9.2.12.2.5 Registerkarte „Integrationseinstellungen”

Auf der Registerkarte **Integrationseinstellungen** können Sie Integrationseinstellungen für den Listenverwaltungsdienst vornehmen:

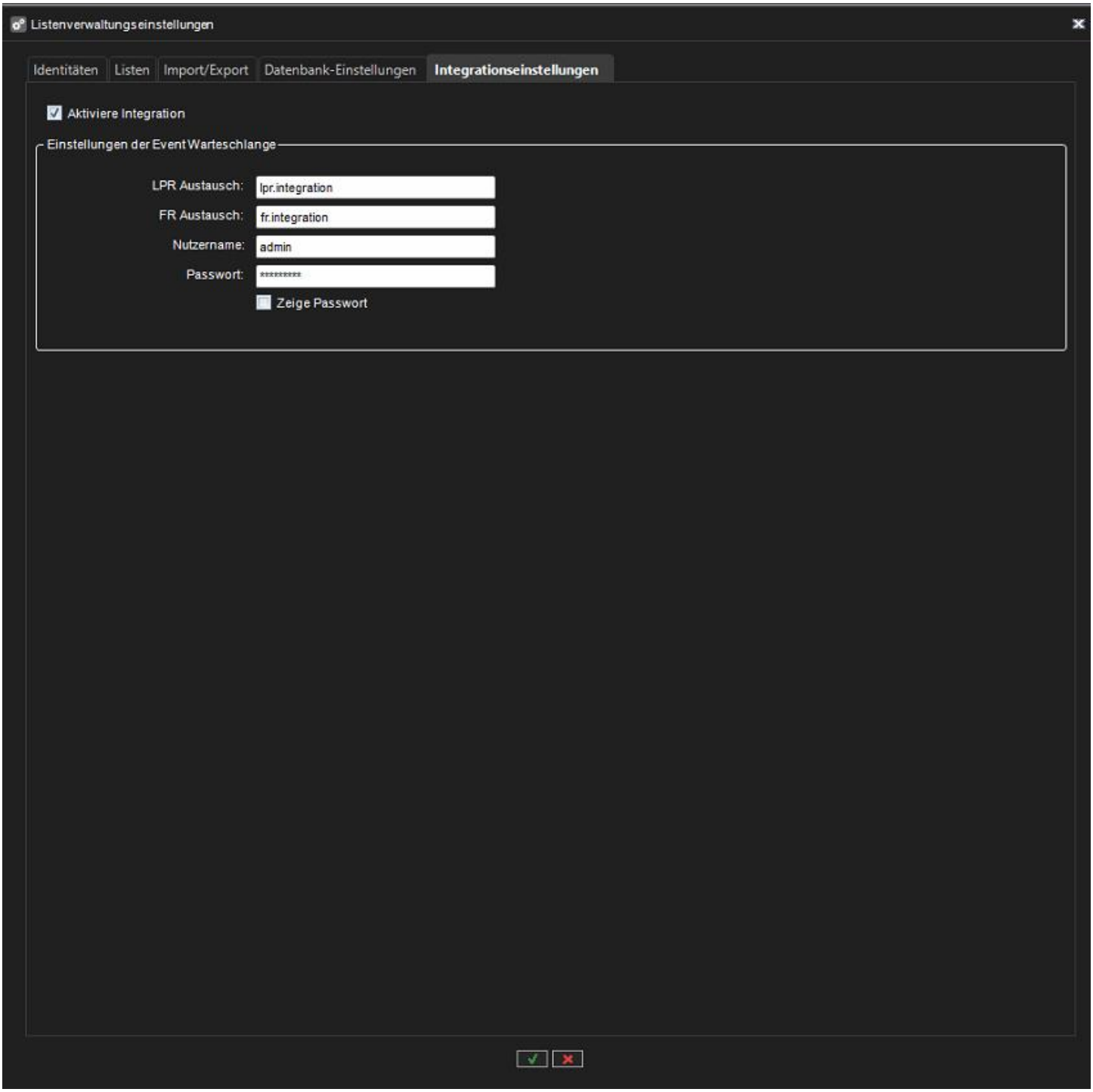


Figure 13 Registerkarte „Integrationseinstellungen"

Hier können Sie Einstellungen für die Ereigniswarteschlange festlegen und die Integrationseinstellungen aktivieren/deaktivieren. Die Registerkarte ist nicht sichtbar, wenn die Lizenz die Listenmanagement-Integration nicht aktiviert.

9.2.12.3 Benachrichtigung über die Aktualisierung von Listenverwaltungsdaten

Wenn die Listenverwaltungsdaten in einer anderen Anwendung geändert wurden, empfängt der System Manager ein Ereignis mit aktualisierten Informationen und zeigt die folgende Meldung an:

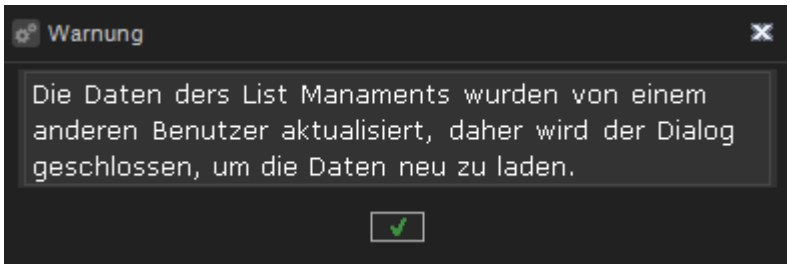
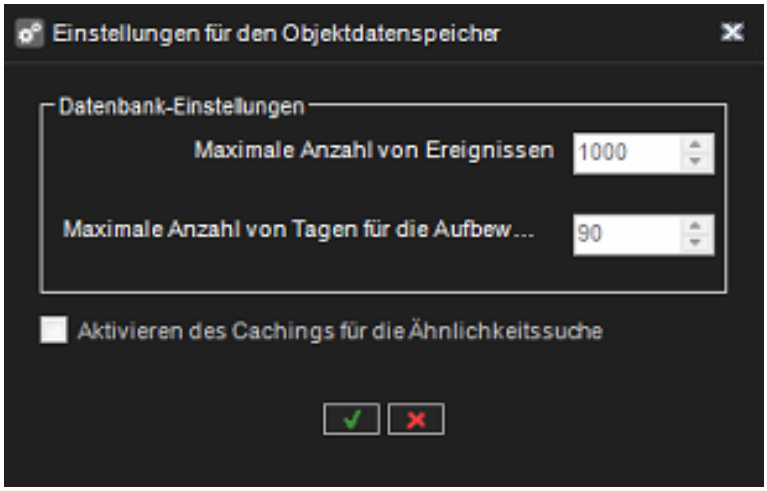


Figure 14 Warnung vor Datenaktualisierung

Wenn Sie auf die Schaltfläche **OK** des Meldungsdialogs klicken, werden alle Einstellungsdialoge geschlossen, um die Daten aus dem Listenverwaltungsdienst neu zu laden. Alle Änderungen, die nicht gespeichert wurden, gehen dabei verloren.

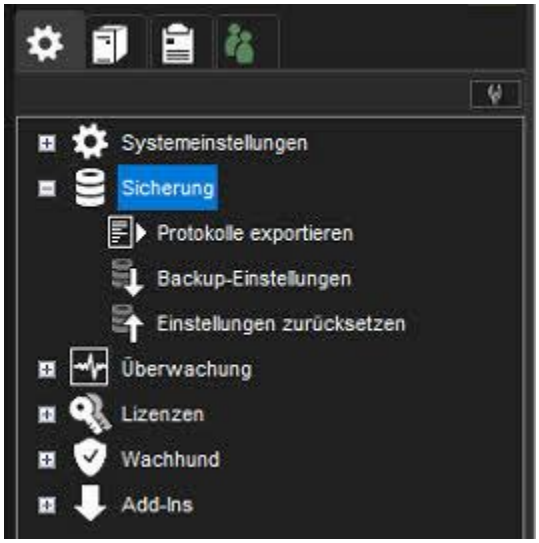
9.2.13 Einstellungen für den Objektdatenspeicher

Um die maximale Anzahl von Ereignissen, die in der Datenbank gespeichert werden sollen, und den Zeitraum, in dem diese Ereignisse aufbewahrt werden sollen, auszuwählen, gehen Sie im System-Manager zu **Systemeinstellungen** > **Einstellungen für den Objektdatenspeicher**. Hier können Sie auch das Caching für die Ähnlichkeitssuche aktivieren.



WARNUNG: Die Verwendung hoher Grenzwerte kann zu unbeabsichtigter Massenlöschung von Daten und einer erhöhten Systemauslastung führen. Es wird empfohlen, zunächst mit niedrigeren Grenzwerten zu beginnen und die Ergebnisse zu überprüfen, bevor umfangreichere Vorgänge ausgeführt werden.

9.3 SICHERUNG



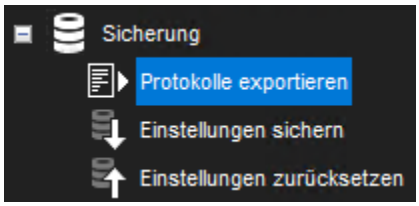
9.3.1 Protokolle exportieren

Exportieren Sie Protokolldateien und senden Sie sie an den Systemlieferanten, wenn ein Problem mit dem System auftritt.

Die Protokolldateien werden in einer komprimierten (gezippten) Datei gespeichert, die auf einem entfernbaren oder nicht entfernbaren Gerät abgelegt werden kann.

9.3.1.1 Exportieren von Protokolldateien über System Manager

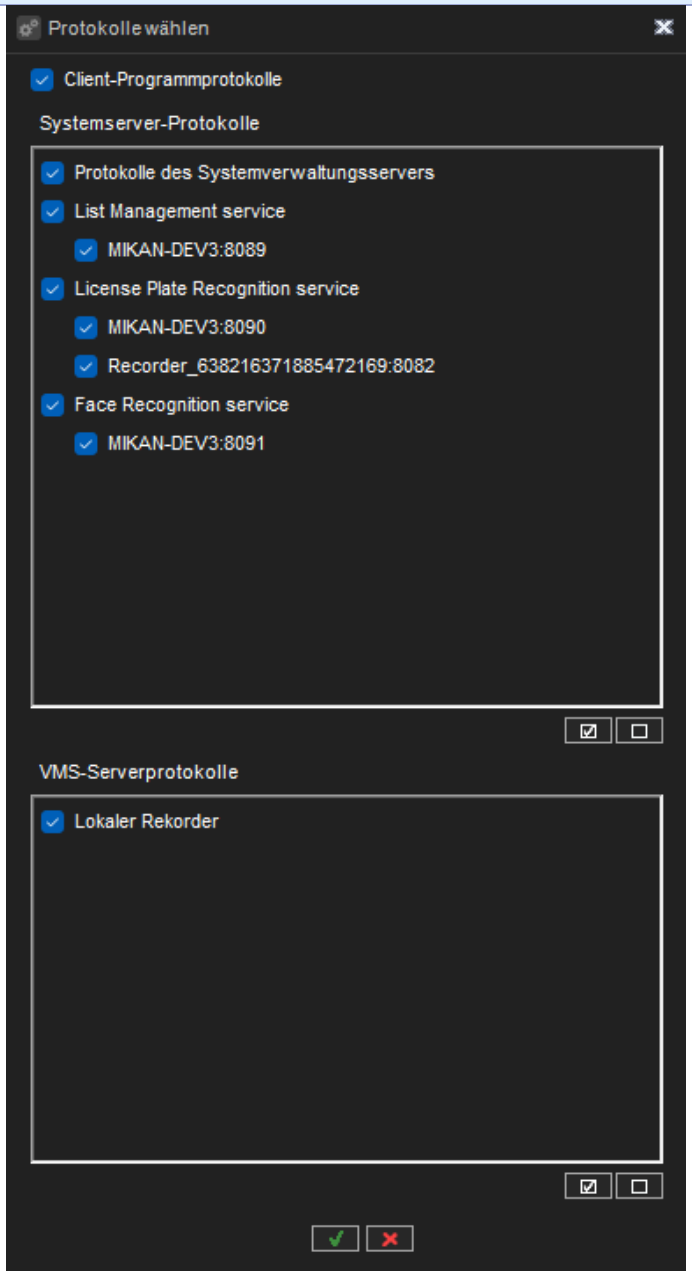
1. Öffnen Sie die Anwendung System Manager für Exportprotokolle und wählen Sie auf der Registerkarte System im Baumelement Backup den Unterpunkt Exportprotokolle.



2. Wählen Sie die Protokolle, die exportiert werden können, im Fenster Protokolle auswählen aus.

Wenn es Probleme mit einem Server gibt, wählen Sie Protokolle im Bereich System-Server-Protokolle. Wählen Sie außerdem Client-Programm-Protokolle.

Die Client-Protokolle stammen von dem Rechner, von dem aus Sie auf die Systemmanager-Anwendung zugreifen.



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

3. Click **OK**.

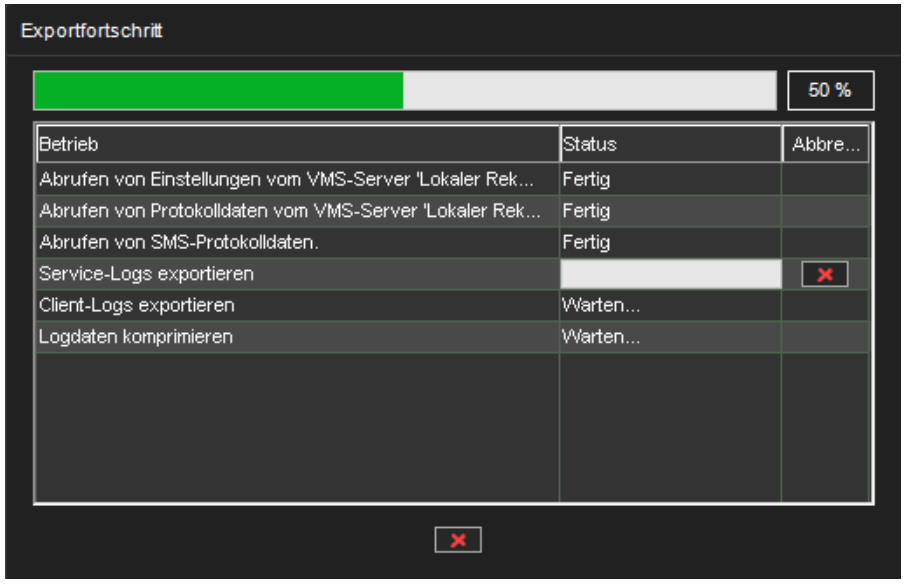
4. Select the storage device and the folder where you want to save the log files in the **Destination Directory** window.



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

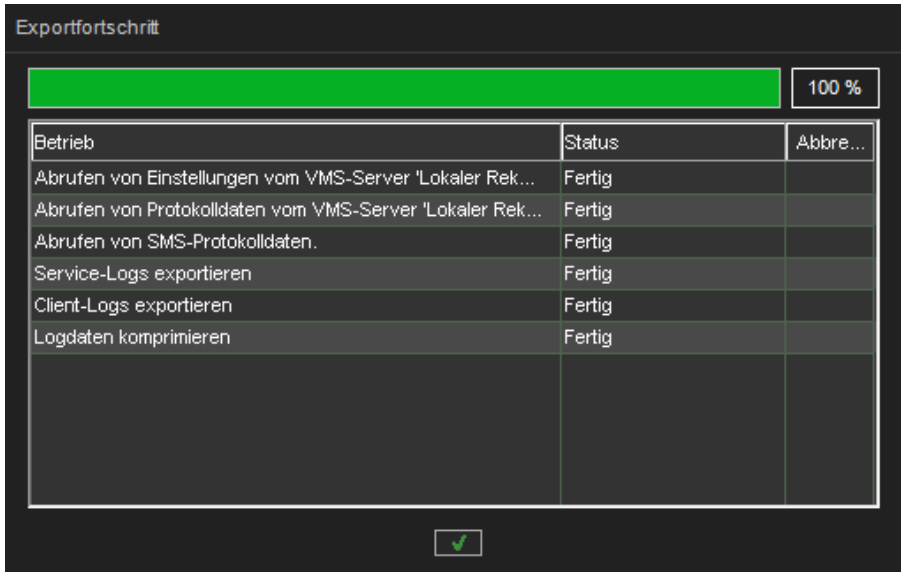
Type a name for the ZIP file in the **Name** fields and click **OK**

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



It is seems like the operation is stuck it can be cancelled.
Cancel all export by clicking on the **Cancel** button at the bottom of the window.

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



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

The typical content of logs ZIP archive is the following:



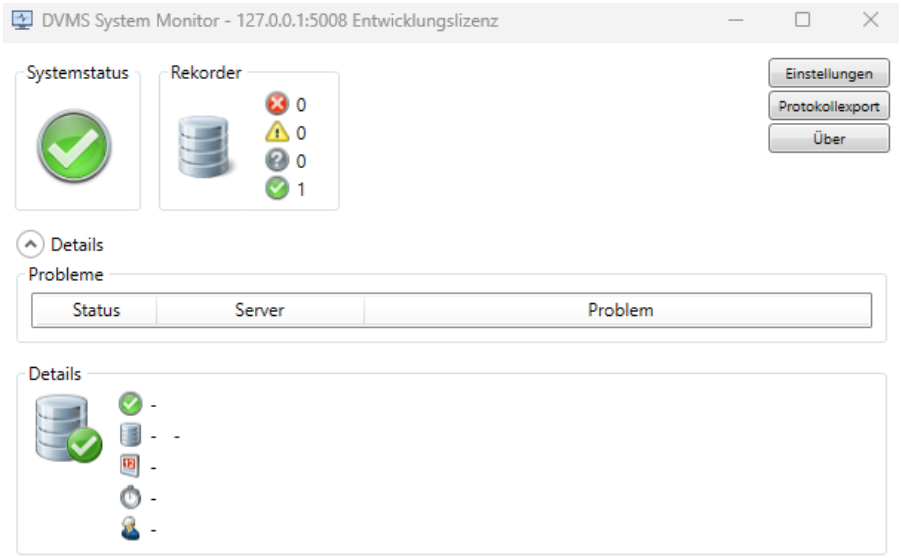
- FRService_ROMANA-DEV1_8091_Log.zip
- LMService_ROMANA-DEV1_8089_Log.zip
- LPRService_ROMANA-DEV1_8090_Log.zip
- SpotterAuditLog_9.6.0.68.txt
- SpotterAuditLog_9.6.0.70.txt
- SpotterLog_9.6.0.68.txt
- SpotterLog_9.6.0.70.txt
- SpotterLog_9.6.0.70.txt.1
- SpotterLog_9.6.0.70.txt.2
- SpotterLog_9.6.0.70.txt.3
- SpotterLog_9.6.0.70.txt.4
- SpotterLog_9.6.0.70.txt.5
- SystemManagerAuditLog.txt
- SystemManagerLog.txt
- SystemManagerLog.txt.1
- SystemManagerLog.txt.2
- SystemManagerLog.txt.3
- SystemManagerLog.txt.4
- SystemManagerLog.txt.5
- SystemManagerLog.txt.6
- SystemManagerLog.txt.7
- SystemManagerLog.txt.8
- SystemManagerLog.txt.9
- SystemManagerLog.txt.10
- SystemMonitorAuditLog.txt
- VAULog.txt
- SM_ExportServiceLog.txt
- SM_IRServerLog.txt
- SM_SLServerLog.txt
- SM_SMLog.txt.9
- SM_SMLog.txt.2
- SM_SMLog.txt.3
- SM_SMLog.txt.4
- SM_SMLog.txt.5
- SM_SMLog.txt.6
- SM_SMLog.txt.7
- SM_SMLog.txt.8
- SM_SMLog.txt
- SM_SMLog.txt.1
- SM_SMLog.txt.10
- Local recorder_ExportServiceLog.txt
- Local recorder_IRServerLog.txt
- Local recorder_ROMANA-DEV1Application.evtx
- Local recorder_ROMANA-DEV1System.evtx
- Local recorder_SLServerLog.txt
- Local recorder_CLIDVRLog.txt
- Local recorder_DVRLog.txt
- Local recorder_DVRLog.txt.1
- Local recorder_DVRLog.txt.2
- Local recorder_PerformanceLog.txt
- Local recorder_PerformanceLog.txt.1
- Local recorder_PerformanceLog.txt.2
- Local recorder_StartupLog.txt
- Local recorder_StartupLog.txt.1
- Local recorder_WDLog.txt
- Local recorder_Alarms.txt
- Local recorder_Cameras.txt
- Local recorder_CameraSets.xml
- Local recorder_DriverInfo.txt
- Local recorder_Drivers.xml
- Local recorder_PluginDrivers.xml
- Local recorder_Settings.xml

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

9.3.1.2 Export log files via System Monitor

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

1. Open System Monitor and click the **Log export** button:



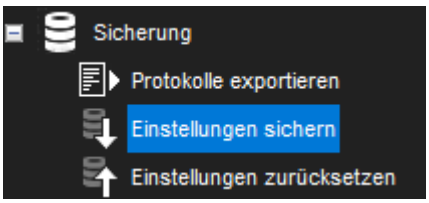
2. Choose the archive name and path for saving in the **Save as** dialog to save export archive.

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

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

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

9.3.2 Backup-Einstellungen

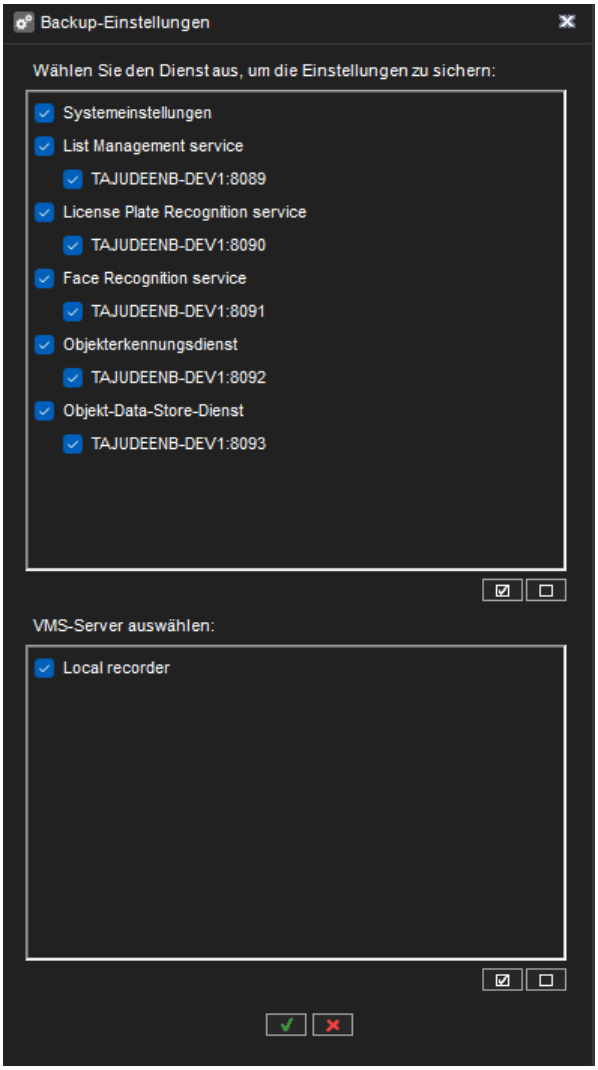


Systemeinstellungen sichern, um sie wiederherstellen zu können, wenn die Festplatte, die die Einstellungen enthält, ausfällt.

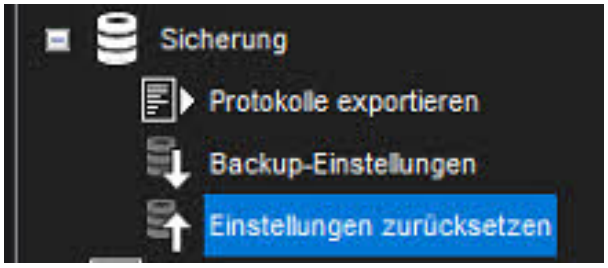
- Sie können Systemeinstellungen und Servereinstellungen sichern.
- Systemeinstellungen enthalten Daten über die Server, Profile und Benutzerkonten.
- VMS-Servereinstellungen enthalten Daten über die mit den Servern verbundene Geräte und deren Parameter.
- Sie können die Sicherungskopie auf einer Festplatte, einem Netzlaufwerk, einer CD/DVD, einer Diskette oder einem anderen entfernbaren oder nicht entfernbaren Gerät speichern.
- Sicherungsdateien haben die Dateierweiterung „.vbk“.

9.3.2.1 So sichern Sie die Einstellungen

1. Öffnen Sie auf der Registerkarte System die Sicherungseinstellungen. Das Dialogfeld Sicherungseinstellungen wird angezeigt
2. Wählen Sie die system- und serverspezifischen Einstellungen aus, die Sie sichern möchten, und klicken Sie auf OK.
3. Wählen Sie das Speichergerät und den Ordner aus, in dem Sie die Sicherungsdatei speichern möchten Um einen neuen Ordner zu erstellen, klicken Sie auf die Schaltfläche Neuer Ordner.
4. Geben Sie einen Namen für die Datei und eine Beschreibung ein und klicken Sie auf OK. Die Beschreibung ist optional. Das System erstellt die Sicherungsdatei.



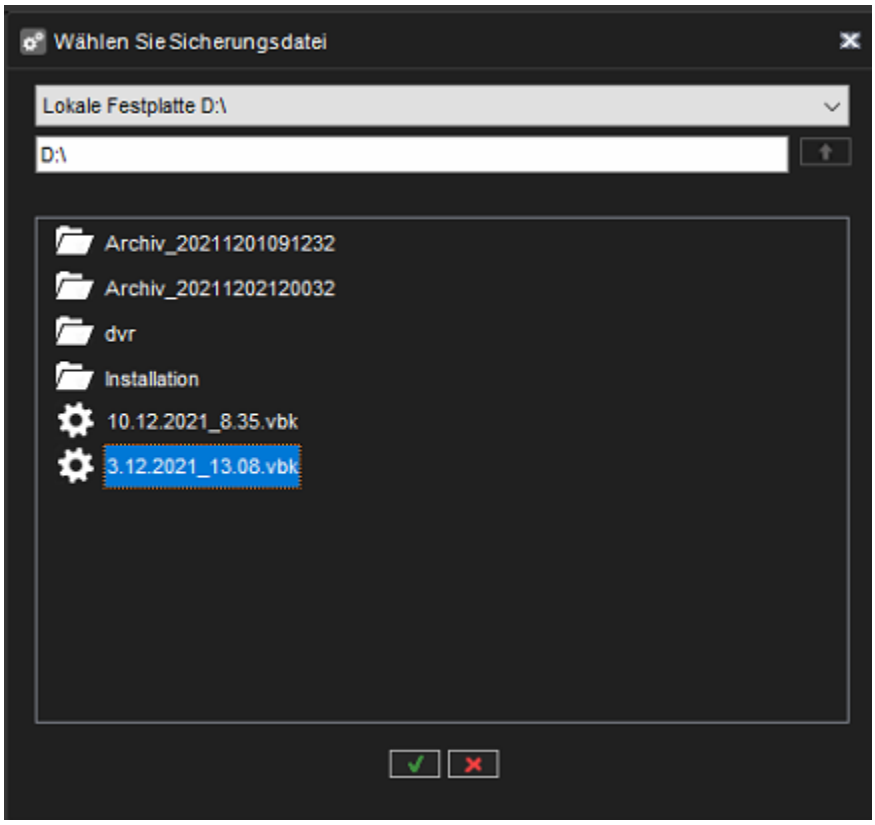
9.3.3 Einstellungen zurücksetzen



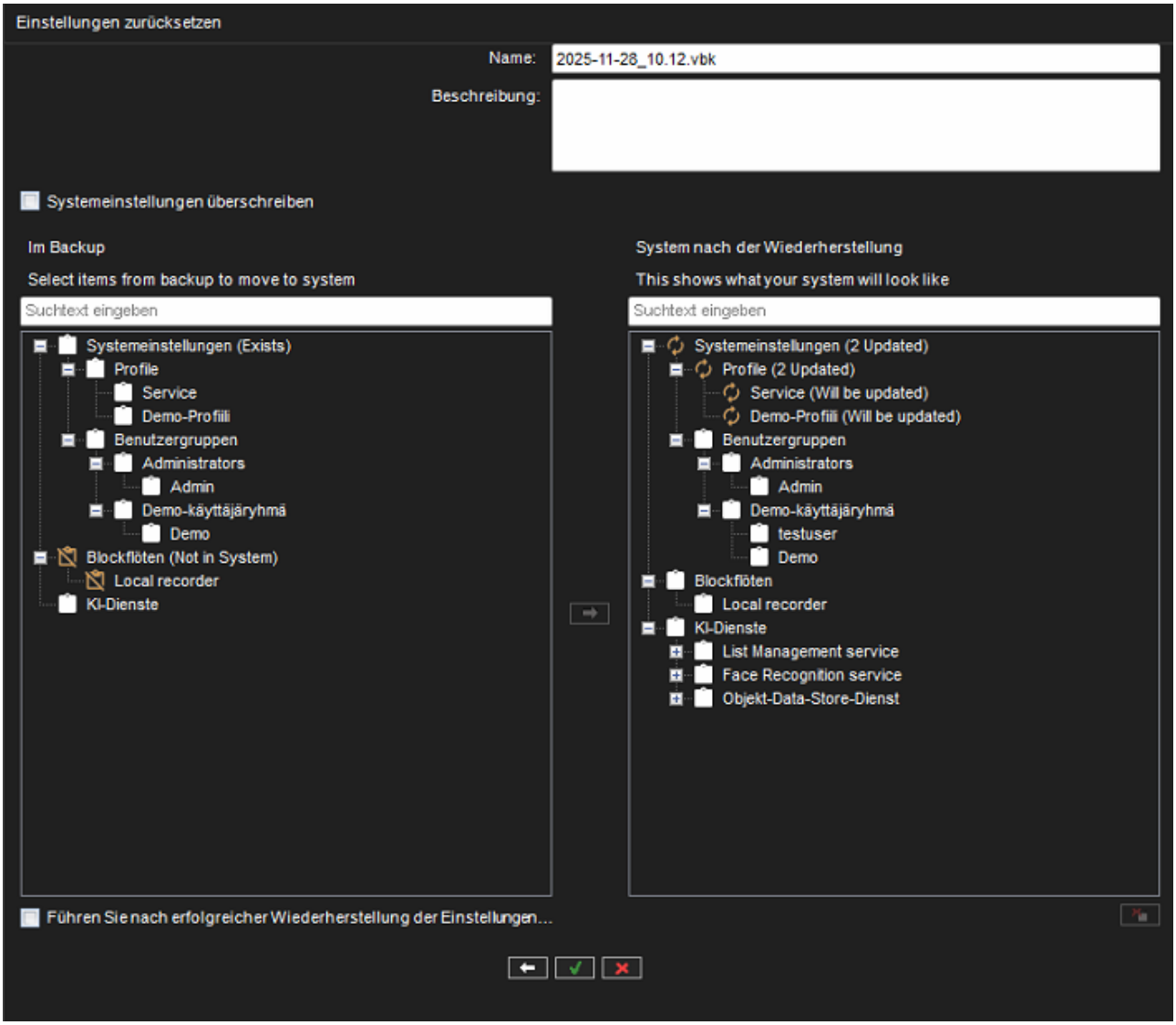
Wenn Sie eine Sicherungsdatei der System- und Servereinstellungen erstellt haben, können Sie die Einstellungen im Fehlerfall wiederherstellen.

9.3.3.1 So stellen Sie die Einstellungen wieder her

1. Öffnen Sie auf der Registerkarte **System** die **Einstellungen zum Wiederherstellen**. Das Dialogfeld „Wählen Sie Sicherungsdatei"wird angezeigt.

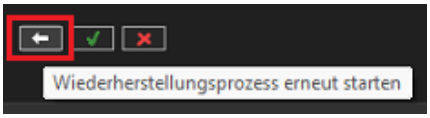


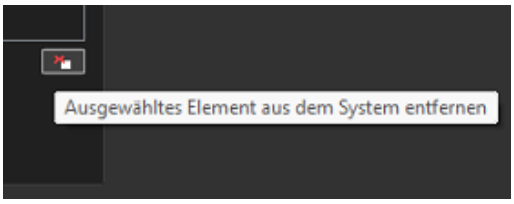
1. Suchen und wählen Sie die Sicherungsdatei (.vbk) aus und klicken **OK**. Sie auf Das System dekomprimiert die Datei und zeigt dann das Dialogfeld **Einstellungen zurücksetzen** an. Das Dialogfeld zeigt die Einstellungen und deren Beschreibung an.

2. 

Wählen Sie die Einstellungen aus, die Sie wiederherstellen möchten, und klicken Sie auf **Zum Wiederherstellen auswählen**. Das Dialogfeld zeigt, was in der Sicherung enthalten ist.

Eine vollständige Systemwiederherstellung kann durchgeführt werden, indem das Kontrollkästchen **Systemeinstellungen überschreiben** aktiviert wird. Alle vom Benutzer vorgenommenen Änderungen können durch Klicken auf **Wiederherstellungsprozess erneut starten** rückgängig gemacht werden, und eine einzelne Einstellung kann aus der Wiederherstellung entfernt werden, indem man sie im Bereich „System nach der Wiederherstellung“ auswählt und auf **Ausgewähltes Element aus dem System entfernen** klickt.





Es wird empfohlen, die Option **Führen Sie nach erfolgreicher Wiederherstellung der Einstellungen eine automatische Sicherung der Einstellungen durch** zu aktivieren, insbesondere bei der Wiederherstellung des Systems nach einem Failover.

Klicken Sie nach der Auswahl auf **OK**. Die Einstellungen werden wiederhergestellt, und es wird eine Zusammenfassung des Vorgangs angezeigt.

1. Klicken Sie auf **OK**, um die neuen Einstellungen zu übernehmen, oder auf **Wiederherstellungsprozess erneut starten**, um zum Dialogfeld „Einstellungen wiederherstellen“ zurückzukehren.

9.3.3.2 Status und Symbole der Inhalte

Der Status der Sicherungsinhalte wird im Dialogfeld „Wiederherstellungsoptionen“ neben dem Namen des Hauptordners durch ein Symbol und einen Statustext angezeigt. Die Symbole haben folgende Bedeutung:

- 

  Der Eintrag ist in der aktuellen Konfiguration bereits vorhanden, der Eintrag wird nicht aktualisiert

- 

  Der Eintrag ist in der aktuellen Konfiguration teilweise vorhanden

- 

  Der Eintrag ist in der aktuellen Konfiguration nicht vorhanden

- 

  Der Eintrag wird in der aktuellen Konfiguration aktualisiert

- 

  Der Eintrag wird zur aktuellen Konfiguration hinzugefügt

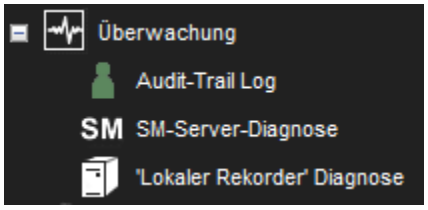
- 

  Das Element wird aus der aktuellen Konfiguration gelöscht

9.4 ÜBERWACHUNG

9.4.1 Audit-Protokoll

Das Protokoll des Audit-Trails kann verwendet werden, um Informationen über die Benutzeraktivitäten des VMS-Systems zu suchen. Der Zugriff darauf erfolgt im System-Manager auf der Registerkarte "System" unter "Überwachung".



9.4.1.1 Audit-Trail-Protokoll

Im Audit Trail Log-Dialog kann der Administrator mit verschiedenen Suchparametern nach Audit Trail-Ereignissen suchen.

Die Ergebnisse werden in einer nach Zeit geordneten Ergebnisliste aufgeführt. Gefundene Audit-Trail-Ereignisse können nach anderen Audit-Trail-Ereignis-Informationen sortiert werden, indem Sie auf die Listenüberschriften klicken.

9.4.1.2 Suchparameter

Die folgenden Suchparameter können für die Suche nach Audit-Trail-Ereignissen verwendet werden.

- **Datum** - Wählen Sie das Datum, an dem die Suche beginnen soll. Mit den Schaltflächen auf der linken und rechten Seite können Sie den Tag des Datums vergrößern oder verkleinern.
- **Zeit** - Wählen Sie die Uhrzeit des Datums, zu der die Suche beginnen soll. Mit den Schaltflächen links und rechts können Sie die Stunde der Uhrzeit erhöhen oder verringern. Die Schaltflächen nach oben und unten erhöhen bzw. verringern die Minuten der Uhrzeit um zehn.
- **Benutzer** - Benutzer, dessen Audit Trail-Ereignisse durchsucht werden sollen. Alle = Suche ohne Filterung der Benutzer.
- **Anwendung** - Zu durchsuchende Anwendung. Alle = Suche ohne Filterung der Anwendungen.
- **Max result count** - Maximale Anzahl, wie viele Audit-Trail-Ereignisse ab der Startzeit durchsucht werden sollen.
- **VMS Server** -Die Dropdown-Liste VMS-Server zeigt alle möglichen Werte für VMS-Server an, die ausgewählt werden können.

- **Endzeit-Kontrollkästchen** - Wenn dieses Kontrollkästchen aktiviert ist, können Sie das Enddatum und die Endzeit der Suche auf ähnliche Weise wie die Startzeit auswählen. Wenn es nicht markiert ist, wird die Endzeit nicht als Suchfilter verwendet (= Suche bis jetzt).
- **Audit-protokoll Veranstaltungen** - Zu durchsuchender Vorgang: Es kann keiner, einer, viele oder alle Vorgänge ausgewählt werden. Wenn keine oder alle ausgewählt sind, wird ohne Filterung der Vorgänge gesucht. Die folgenden Schaltflächen können mit Vorgängen verwendet werden:
    - Ansicht der Vorgangsliste vergrößern
    - Alle auswählen
    - Alle abwählen

9.4.1.3 Ergebnisliste

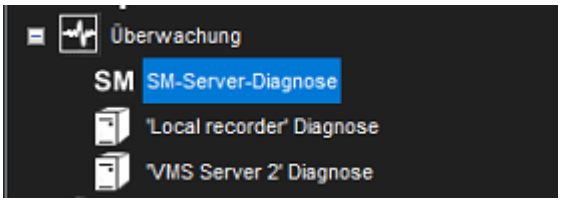
Gefundene Audit-Trail-Ereignisse werden in der Suchergebnisliste aufgeführt. Die Liste enthält Informationen zu jedem Audit-Trail-Ereignis.

- **Zeit** - Zeitpunkt der Benutzeraktion.
- **Benutzer** - Benutzername, der die Benutzeraktion durchgeführt hat.
- **Anwendung** - Anwendung, in der die Benutzeraktion durchgeführt wurde.
- **Ereignis** - Name der Benutzeraktion. Wenn sich das Ereignis auf eine Kameraprüfung bezieht und der Bediener vor dem Zugriff auf das Wiedergabematerial einen Kommentar hinzufügen muss, enthält das Ereignis den Kommentar.
- **Ereignisstatus** - ob der Vorgang erfolgreich war oder nicht.
- **Objekt** - Das Objekt hängt von der Operation selbst ab. Wenn Sie zum Beispiel eine Kamera öffnen, wird der Name dieser Kamera angezeigt.
- **VMS Server** - Zeigt an, auf welchem VMS-Server der Vorgang stattgefunden hat.

9.4.1.4 Audit-Protokoll-Export

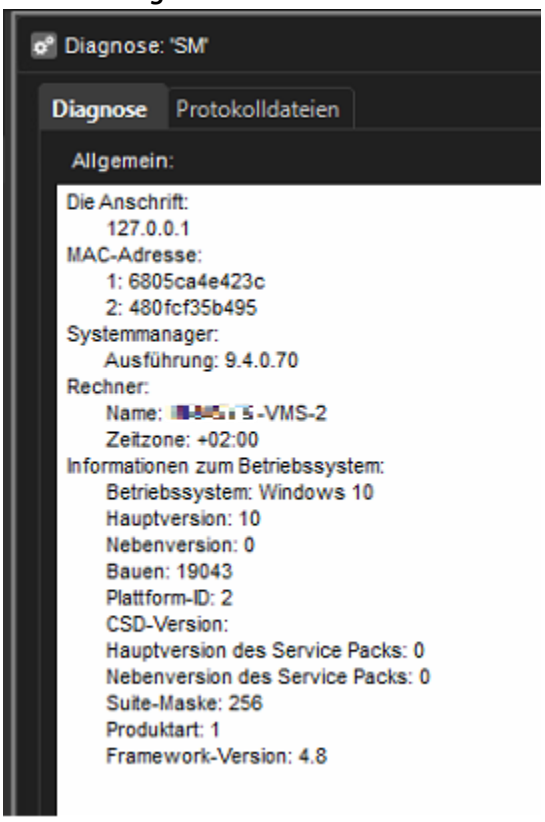
Aufgelistete Audit-Trail-Ereignisse können durch Klicken auf die Schaltfläche unter der Ergebnisliste der Audit-Trail-Ereignisse in eine PDF-Datei als Audit-Trail-Bericht exportiert werden. Der Speicherort und der Name der exportierten Datei sowie der Kommentar für den Bericht können im Dialog zum Speichern des Berichts angegeben werden. Der Titel des Audit-Protokollberichts wird aus der Exportzeit und dem Benutzer, der den Bericht exportiert hat, erstellt. Der Bericht enthält alle Audit-Protokolleinträge mit denselben Informationen, die auch in der Ergebnisliste der Audit-Trail-Ereignisse aufgeführt sind.

9.4.2 SM-Server-Diagnose



SM Server Diagnostics zeigt Informationen über den System Management Server an, der auf dem Hauptserver ausgeführt wird.

9.4.2.1 Allgemein



In SMServer Diagnostics können Sie diese Informationen überprüfen:

- SM-Serverversion
- Computername und Zeitzone
- Informationen zum Betriebssystem
- Hauptversion
- Nebenversion

- Bauen
- Plattform-ID
- CSD-Version
- Hauptversion des Service Packs
- Nebenversion des Service Packs
- Suite-Maske
- Produktart
- Framework-Version

9.4.2.2 Protokolldateien

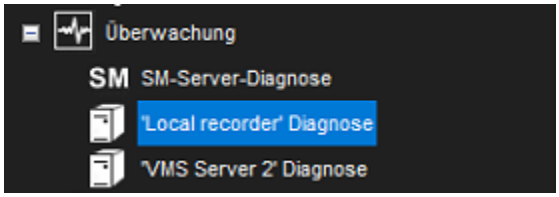
Bei Problemen mit dem System können Sie auf die Systemprotokolldateien auf der Registerkarte Protokolldateien zugreifen.

So untersuchen Sie eine Protokolldatei:

- Wählen Sie die Datei aus der Dropdown-Liste aus.

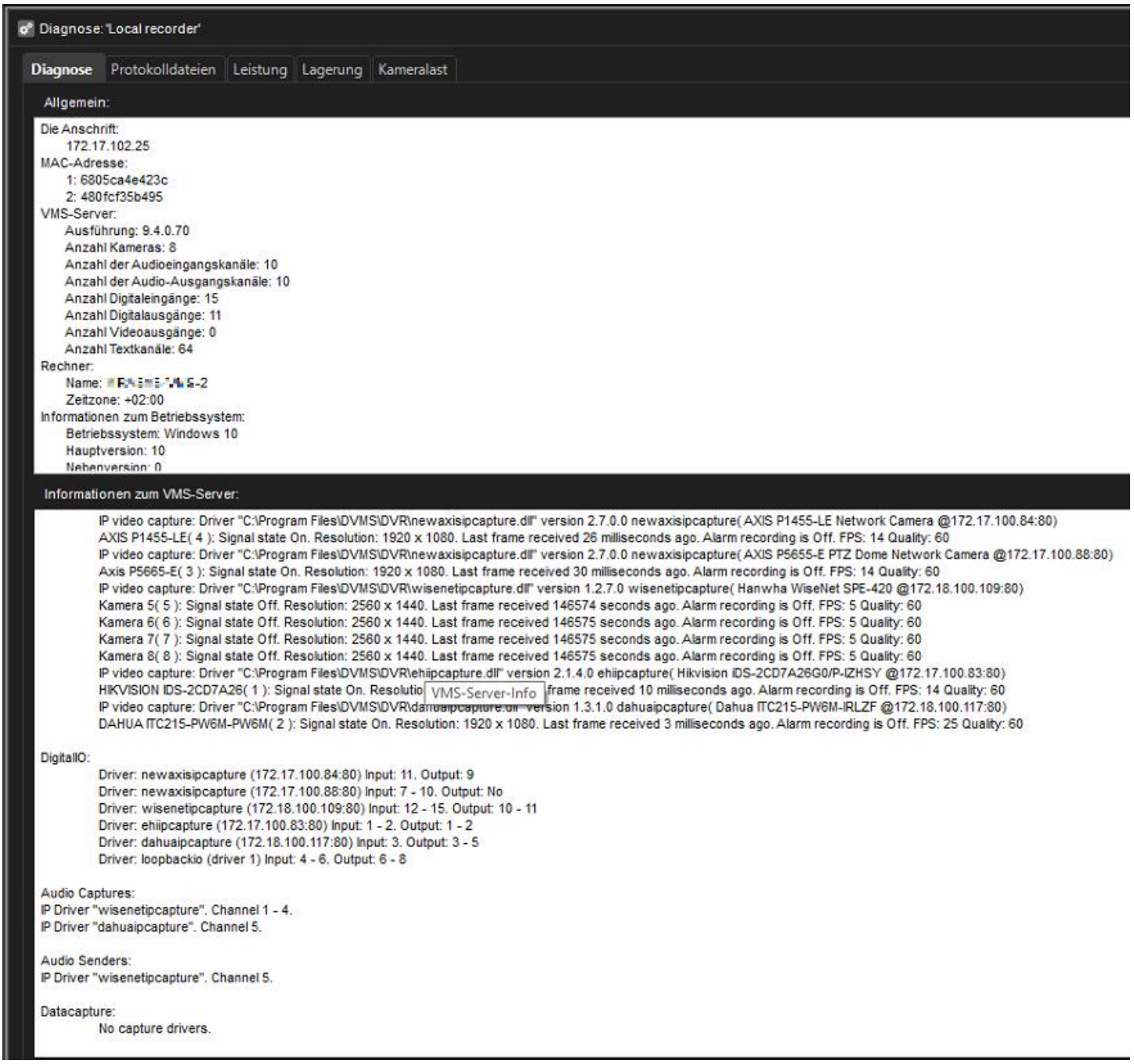
Der Inhalt wird im Inhalt der ausgewählten Protokolldatei angezeigt

9.4.3 Serverdiagnose



Die VMS-Server-Diagnose zeigt Informationen über den Server und die CPU- und Netzwerkauslastung an.

9.4.3.1 Diagnose



Die Registerkarte **Diagnose** zeigt diese Informationen:

- Informationen zum Server:
- Softwareversion

- Modell
- Anzahl der Kameras, Audiokanäle, Digitaleingänge, Digitalausgänge und Videoausgänge
- Der Name des Computers und die Zeitzone
- Informationen zum Betriebssystem
- Prozessorinformationen
- Installierte Treiber, z. B. Capture-Treiber, Videoausgabetreiber, Digitalausgabetreiber und PTZ-Treiber

9.4.3.2 Protokolldateien

Die Registerkarte Protokolldateien zeigt eine Liste der **Protokolldateien** an.

So zeigen Sie den Inhalt einer Protokolldatei an:

- Wählen Sie die Datei aus der Dropdown-Liste aus. Der Inhalt wird im Inhalt der ausgewählten Protokolldatei angezeigt

9.4.3.3 Leistung

Auf der Registerkarte **Leistung** können Sie diese überwachen:

- CPU auslastung.
- Nutzung des physischen Speichers.
- Nutzung des virtuellen Speichers.
- Netzwerktraffic.
- Benutzter Speicherplatz.

9.4.3.4 Lagerung

Auf der Registerkarte Speicher können Sie Datenträger- und Dateieigenschaften überwachen. Sie können beispielsweise den freien Speicherplatz überprüfen oder gespeicherte Daten nach Kamera und Audiokanal überwachen.

Allgemein Gesamtaufnahmekapazität. Zeigt die gesamte Speicherkapazität an, die für die Aufnahmen reserviert ist.

Belegter Speicherplatz Die Menge an Speicherplatz, die die Aufzeichnungen belegt haben.

Freier Speicherplatz. Für Aufzeichnungen ist freier Speicherplatz verfügbar.
% belegt. Der Prozentsatz der belegten Festplattenkapazität.

Durchschnittliche Speichergeschwindigkeit. Wird berechnet, indem die seit dem letzten Start des Servers gespeicherte Datenmenge durch die Betriebszeit dividiert wird.

VMS-Server-Betriebszeit Zeigt die Betriebszeit des Servers seit dem letzten Start an.

Der Zähler zeigt die Differenz zwischen der aktuellen Uhrzeit und der Startzeit in Tagen, Stunden und Minuten an.

Festplatten

Gesamtaufzeichnungskapazität. Zeigt die Speicherkapazität an, die für die Aufnahmen auf dem ausgewählten Datenträger reserviert ist.

Verwendeter Speicherplatz. Benutzter Speicherplatz auf der ausgewählten Festplatte.

Freier Speicherplatz. Auf dem ausgewählten Datenträger ist freier Speicherplatz für Aufzeichnungen verfügbar.

% verwendet. Der Prozentsatz des belegten Speicherplatzes der für die Aufzeichnungen reservierten Gesamtkapazität.

Gesamtaufzeichnungs-Cache. Zeigt die Gesamtkapazität des Caches an, der für die temporäre Speicherung von Daten verwendet wird, bevor sie dauerhaft auf eine Festplatte geschrieben werden.
Aufgrund des Caches können Video und Audio sofort aufgezeichnet werden, wenn der Server gestartet wird. Der Cache wird auch für die Aufzeichnung vor dem Ereignis verwendet.

Das System berechnet automatisch, wie viel Cache-Speicherplatz es haben muss, und weist den Speicherplatz entsprechend zu.

Verwendeter Aufzeichnungs-Cache. Temporärer Speicherplatz, der derzeit verwendet wird.

Freier Aufzeichnungscache. Temporärer Speicherplatz, der derzeit frei ist.

Kameras

Älteste Zeit. Datum und Uhrzeit des ältesten Bildes im Store.

Neueste Zeit.

Datum und Uhrzeit des neuesten Bildes im Store.

Gesamtnr. Bilder. Die Gesamtzahl der Bilder im Store.

Durchschnittliche Bildgröße. Die durchschnittliche Bildgröße.

Verwendeter Speicherplatz**. Dieser Wert zeigt, wie viel Speicherplatz die Bilder und Metadatendateien dieser Kamera beanspruchen.**

% verwendet. Dieser Wert zeigt an, wie viel Prozent des Speicherplatzes diese Kamera von der für die Aufzeichnungen reservierten Gesamtkapazität belegt hat.

Audiokanäle

Älteste Zeit. Das Datum und die Uhrzeit des ältesten Audio-Samples im Speicher.

Neueste Zeit. Das Datum und die Uhrzeit der neuesten Probe im Geschäft.
Eine Gesamtzahl von Proben. Die Gesamtzahl der Audio-Samples im Store.
Durchschnittliche Sample-Größe. Die durchschnittliche Audio-Sample-Größe.

Verwendeter Speicherplatz. Dieser Wert zeigt an, wie viel Speicherplatz die Audio-Samples und Metadatendateien des Audiokanals beanspruchen.
% verwendet. Dieser Wert zeigt an, wie viel Prozent des Speicherplatzes der Audiokanal von der für die Aufzeichnungen reservierten Gesamtkapazität belegt hat.

Textkanäle

Älteste Zeit. Das Datum und die Uhrzeit des ältesten Textdatenbeispiels im Speicher.

Neueste Zeit. Das Datum und die Uhrzeit der neuesten Probe im Geschäft.

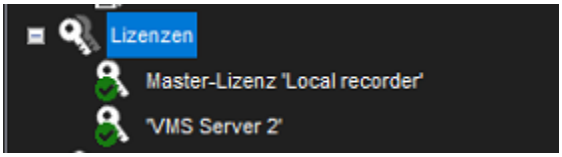
Eine Gesamtzahl von Proben. Die Gesamtzahl der Textdatenbeispiele im Speicher.

Durchschnittliche Stichprobengröße. Die durchschnittliche Stichprobengröße von Textdaten.

Verwendeter Speicherplatz. Dieser Wert zeigt, wie viel Speicherplatz die Textdatenbeispiele und Metadatendateien aus dem Textkanal beanspruchen.

% verwendet. Dieser Wert zeigt an, wie viel Prozent des Speicherplatzes der Textkanal von der für die Aufnahmen reservierten Gesamtkapazität belegt hat.

9.5 LIZENZEN



Standardmäßig unterstützt der Server ohne VMS-Lizenz nur eine IP-Kamera. Für den vollen Funktionsumfang benötigt der Server eine gültige Lizenz.
Je nach Installation müssen Sie möglicherweise die Lizenzdaten aktualisieren, wenn Sie dem System neue Funktionen oder Kameras hinzufügen.

Um einen Lizenzschlüssel zu erhalten, wenden Sie sich bitte an Ihren Lieferanten und befolgen Sie die von diesem beschriebenen Schritte zur Lizenzaktualisierung.

Sollten Sie Probleme bei der Aktualisierung der Lizenz haben, wenden Sie sich bitte an *orders@mirasys.com*.

Sie können einem Server auch weitere Kamerakanäle und Funktionen wie beispielsweise VCA-Funktionen hinzufügen, indem Sie einen neuen Lizenzschlüssel anfordern.

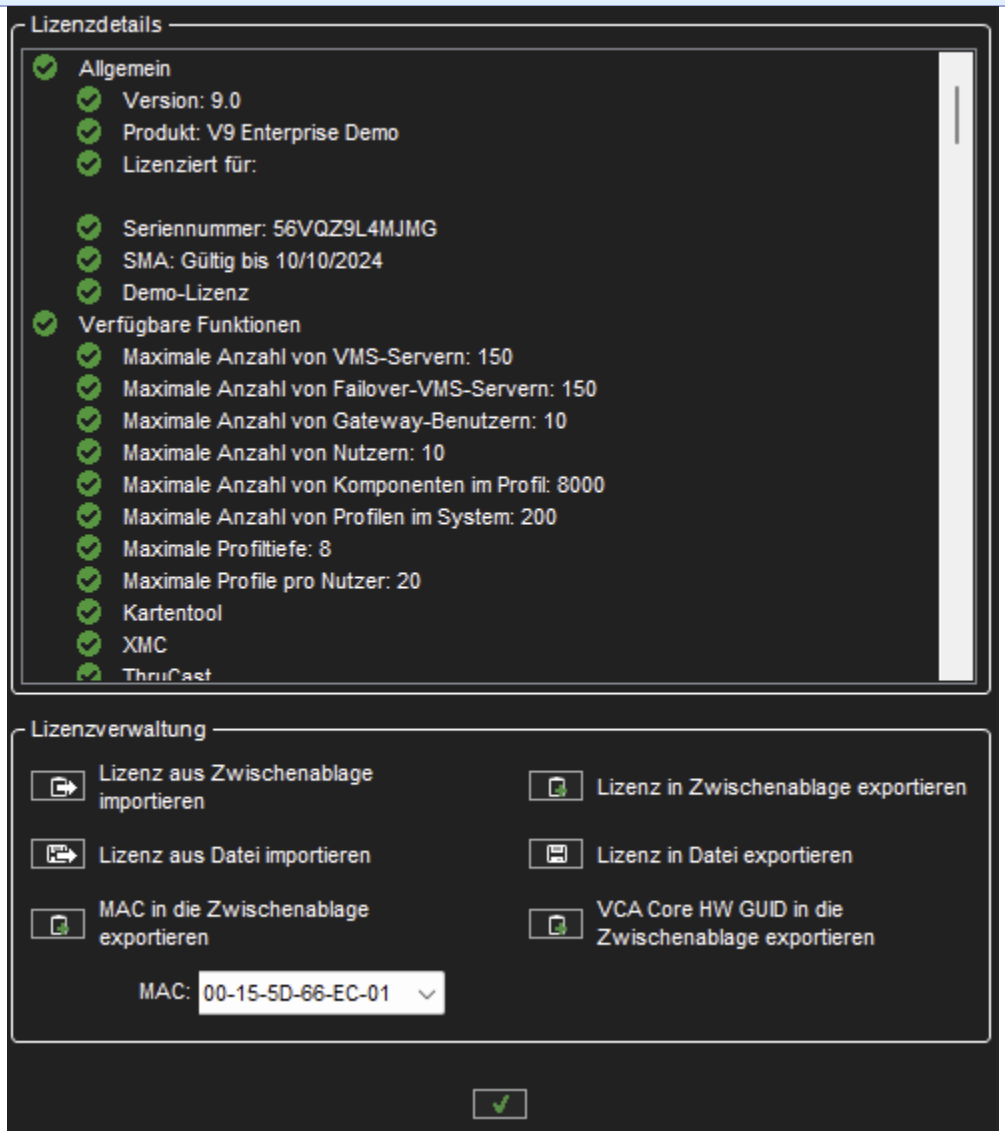
Für den Lizenzschlüssel benötigen Sie die MAC-Adresse des Servers.

9.5.1 So erhalten Sie einen Lizenzschlüssel

1. Starten Sie den System Manager. Das Dialogfeld „Lizenzinformationen“ wird automatisch angezeigt, wenn noch kein Lizenzschlüssel angegeben wurde.
2. Doppelklicken Sie auf der Registerkarte **System** unter **Lizenzen** auf den Server, den Sie aktualisieren möchten.

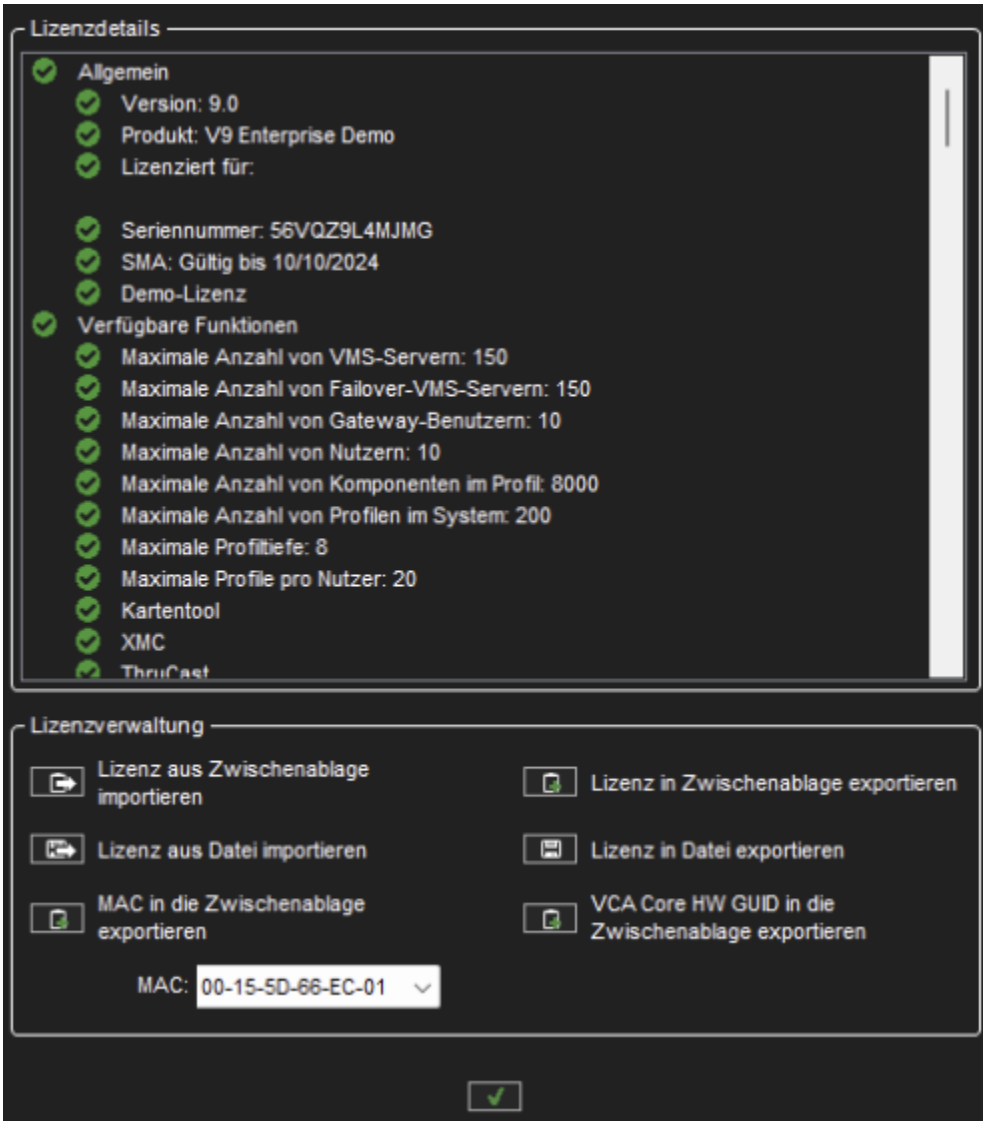
3. Kopieren Sie im Dialogfeld „Lizenzverwaltung“ die MAC-Adresse und senden Sie diese an Mirasys. Im Gegenzug erhalten Sie den Lizenzschlüssel als Textdatei.
4. Klicken Sie auf **Lizenz aus Datei importieren**.
5. Klicken Sie auf **OK**. Das System wird sofort aktualisiert.

Der standardmäßige, nicht registrierte Zustand, der die Nutzung einer IP-Kamera ermöglicht, ist zeitlich begrenzt.
Der nicht registrierte Zustand kann bis zu 60 Tage lang aktiv sein; danach ist ein gültiger Lizenzschlüssel erforderlich. Wird dem System nicht innerhalb von 60 Tagen nach der Installation ein gültiger Lizenzschlüssel hinzugefügt, wird der Betrieb des Systems eingestellt.



9.5.2 Lizenzdetails

Lizenzdetails zeigen alle unterstützten Funktionen der Lizenz.



9.5.3 Lizenzverwaltung

9.5.3.1 So importieren Sie einen Lizenzschlüssel:

1. Klicken **Sie auf Lizenz aus Datei importieren**
2. Navigieren Sie zum Speicherort der Lizenzdatei
3. **OK** klicken Die neue Lizenz wird sofort aktualisiert.

9.5.3.2 So exportieren Sie einen Lizenzschlüssel:

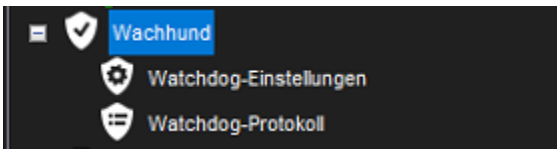
1. Klicken **Sie auf Lizenzschlüssel in Datei exportieren**, um eine Textdatei für die Lizenz zu erstellen, oder auf Lizenzschlüssel in die Zwischenablage exportieren, um **den Schlüssel in die Zwischenablage zu kopieren**.
2. Wenn Sie die Lizenz in eine Datei exportieren, legen Sie den Zielordner und den Namen der Datei fest.
3. **OK** klicken.

9.5.3.3 So exportieren Sie die VCA Core HW GUID

1. Klicken **Sie auf VCA Core HW GUID** in die Zwischenablage exportieren
2. Wählen **Sie auch die Lizenzseriennummer exportieren**
3. **OK** klicken



9.6 WACHHUND



Das System verfügt über einen Software-Watchdog (Systemüberwachungsdienst), der das System überwacht und bei Problemen bestimmte Aktionen durchführt.
Im Watchdog-Tool können Sie die Ereignisse auswählen, bei denen die Benachrichtigungsliste per E-Mail benachrichtigt wird, und auf Watchdog-Protokolle zugreifen, die enthalten die aufgetretenen Ereignisse und die durchgeführten Aktionen.

9.6.1 Watchdog-Einstellungen

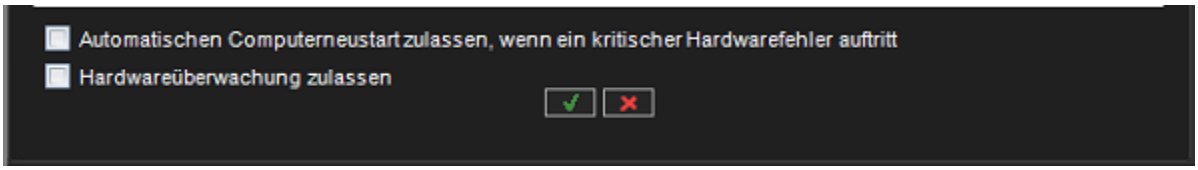
In den Watchdog-Einstellungen können Sie auswählen, welche Ereignisse einen Bericht auslösen, der an die unter E-Mail-Einstellungen
angegebenen E-Mail-Adressen gesendet wird. Sie können für jeden Server unterschiedliche Ereignisse auswählen. Alternativ können Sie dieselben Ereignisse für alle Server auswählen, indem Sie **Alle VMS-Server** auswählen aus der Dropdown-Liste auswählen.
Zusätzlich zu E-Mail-Benachrichtigungen können Benachrichtigungen über digitale Ausgänge erfolgen.
Alle Ereignistypen werden unabhängig von den E-Mail-Einstellungen in die Watchdog-Protokolle geschrieben.

9.6.1.1 So fügen Sie Ereignisse zur Benachrichtigungsliste hinzu oder entfernen sie:

1. Wählen Sie auf der Registerkarte **System** die Option **Watchdog-Einstellungen**.
2. Markieren Sie das Kontrollkästchen **Mail senden** für jeden Ereignistyp, für den eine Benachrichtigungs-E-Mail gesendet werden soll.
3. Klicken Sie auf **OK**.

9.6.1.2 Automatischer Neustart

Aktivieren Sie das Kontrollkästchen **Automatischen Computerneustart zulassen, wenn ein kritischer Hardwarefehler auftritt**, damit Ihr Computer bei hohen Hardwaretemperaturen, bei Erhalt einer Neustart-Aktion (Alarm oder Textkanal), bei einem fehlgeschlagenen Neustart des Rekorderprozesses oder bei mehreren Fehlern bei der Wiederherstellung der Verbindung zum Rekorder automatisch neu startet. Tietokonetta ei käynnistetä uudelleen kuin kerran päivässä.



Sie können bei Bedarf auch eine Hardware-Überwachung zulassen.

9.6.1.3 Digitale Ausgangsbenachrichtigungen

Benachrichtigungen über digitale Ausgabe werden serverspezifisch angelegt; Sie müssen einen bestimmten Server aus der Dropdown-Liste **VMS Server** auswählen.

So stellen Sie eine Digitalausgangsbenachrichtigung ein:

1. Wählen Sie auf der Registerkarte **System** die Option **Watchdog-Einstellungen**.
2. Wählen Sie einen Server aus der Dropdown-Liste **VMS Server** aus. Da digitale Ausgangssignale serverspezifisch sind, können Sie **Alle VMS-Server** nicht auswählen.
3. Klicken Sie auf ein Ereignis.
4. Wählen Sie den digitalen Ausgangskanal, den Sie verwenden möchten, aus dem Dropdown-Menü **In Use** aus.
5. Wenn Sie ein Pulssignal an den Ausgangskanal senden möchten, markieren Sie das Kontrollkästchen **Puls** und wählen Sie mit dem Schieberegler die Pulslänge aus.
6. Klicken Sie auf **OK**.

9.6.2 Watchdog-Protokoll

Standardmäßig zeigt das System die Watchdog-Protokolle von allen Servern an.
Sie können jedoch einen oder mehrere Server aus der Liste auf der linken Seite auswählen.

Sie können die Protokolle sortieren, indem Sie auf die Spaltenüberschriften klicken.
Um die Liste zu aktualisieren, ohne das Fenster zu schließen, klicken Sie auf die Schaltfläche **Aktualisieren**.

9.6.2.1 Zusätzliche Watchdog-Zustellungsmethoden

Die Watchdog-Funktion umfasst die folgenden Protokolle:

- TCP
- anpassbares E-Mail-Formular

Jedes Protokoll hat seinen Treiber:

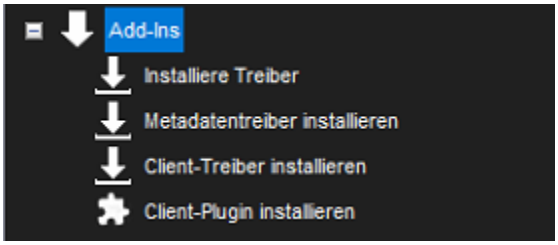
C:\Programme\DVMS\DVR\WDEventProviders\

- WDEventProviderSMTP.xml
- WDEventProviderTCP.xml

Derzeit müssen diese Dateien manuell bearbeitet werden. Jede XML-Datei enthält die Dokumentation zu den Konfigurationsoptionen.
Die neuen Konfigurationsoptionen umfassen gefilterte und bedingte Warnungen (z. B. „Warnung X nur einmal alle 60 Minuten senden“ oder „Warnung X nur senden, wenn Bedingung Y nicht innerhalb von zwei Minuten erfüllt wird“). und ein anpassbares Warnmeldungsformat.
Nachdem die Dateien bearbeitet wurden, muss Watchdog neu gestartet werden, damit die Änderungen wirksam werden.

Notiz *Diese Funktion wird nur für fortgeschrittene Benutzer empfohlen. XML-Dateien sind sehr anfällig für Rechtschreibfehler und Tippfehler bei Zeichenfolgen und Schlüsseln.*
Selbst ein winziger Fehler kann schwerwiegende Fehler verursachen. Mirasys übernimmt keine Verantwortung für XML-Fehler, die durch das Bearbeiten der Dateien verursacht werden.

9.7 ADD-INS



9.7.1 Mirasys Kamera-Treiber

Eine Liste von Mirasys Kamera-Treibern.

9.7.1.1 OnvifIPCapture

Zweck

Zur Erfassung von MJPEG-, MPEG-4-, H.264- und H.265-komprimierten Videodaten von ONVIF-kompatiblen IP-Kameras und Videoservern und zur Unterstützung der PTZ-Funktionalität dieser Geräte.

Unterstützte Kameras:

Alle ONVIF-kompatiblen IP-Geräte.
Unterstützte ONVIF-Profile: S, G, T, M

Anmerkung:

Die Edge-Storage-Funktionalität (Profil G) ist nur für einkanalige Geräte integriert.

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- H.265-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Digitale E/A
- PTZ
- Parallele Auto-Suche
- Mehrfaches Streaming
- Audio (2-Wege)
- Geräte-Bewegungserkennung
- Multicast-Streaming
- CCRiA (Kann die Auflösung im Alarmfall ändern)
- CCFiA (Kann im Alarmfall die Framerate ändern)
- Edge Storage (Video)
- Dynamische Benutzeroberfläche (seit DVMS 8.1.2)
- HTTPS-verschlüsseltes Streaming (RTSP über HTTPS-Tunneling)
- Fokus/Iris-Einstellung
- Privatsphäre-Zonen

Unterstützte Dateien

- OnvifIPCapture.dll
- OnvifIPCapture.xml
- Readme_OnvifIPCapture.txt

Letzte Version

1.9.25.0

Datum der Veröffentlichun

19.10.2026

9.7.1.2 NewAxisIPCapture

Zweck

Zur Erfassung von MJPEG-, MPEG4- und H.264-komprimierten Videodaten von Axis IP-Geräten (Kameras und Videoserver) und zur Unterstützung der PTZ-Funktionalität.

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- H.265-Videokompression
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Digitale E/A
- PTZ
- CCRiA (Kann Auflösung bei Alarm ändern)
- CCFiA (Can Change Framerate in Alarm)
- Datenschutzzonen
- Bewegungserkennung des Geräts (Firmware-Version vor 5.50)
- Audio (2-Wege)
- Mehrfaches Streaming
- Parallele Auto-Suche

- Kantenlagerung (nur Video)
- Multicast-Streaming
- Dynamische Benutzeroberfläche (seit VMS 8.1.2)
- AXIS License Plate Verifier
- Vaxtor LPR

Unterstützte Dateien

- NewAxisIPCapture.dll
- NewAxisIPCapture.xml
- Readme_NewAxisIPCapture.txt

Letzte Version

2.9.15.0

Datum der Veröffentlichun

23.10.2026

9.7.1.3 NewBoschIPCapture

Zweck

Zur Erfassung von H.265-, H.264-, MPEG-4- und MJPEG-komprimierten Videodaten von Bosch IP-Kameras und Videoservern sowie zur Unterstützung der PTZ-Funktionalität von Bosch IP-Geräten.

Unterstützte Funktionen

- Automatische Suche
- H.265-Videokomprimierung
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Mehrfaches Streaming
- Zwei-Wege-Audio (G.711Ulaw, AAC)
- Privatzonen
- Geräte-Bewegungserkennung

- Digitale E/A
- PTZ
- Parallele Auto-Suche
- Edge-Speicher
- Multicast-Streaming
- CCRiA (Kann Auflösung im Alarmfall ändern)
- CCFiA (Kann die Framerate im Alarmfall ändern)
- HTTPS-Unterstützung (außer beim Senden von Audio an die Kamera)

Unterstützte Dateien

- NewBoschIPCapture.dll
- rcpp4.dll or rcpp4x64.dll (v4.61.0.25)
- NewBoschIPCapture.xml
- Readme_NewBoschIPCapture.txt

Letzte Version

1.8.1.0

Datum der Veröffentlichung

23.09.2026

9.7.1.4 BOSCH_AutoDomeBPDrvG3

Zweck

Alter PTZ-Treiber

9.7.1.5 PelcoIPCapture

Zweck

Zur Erfassung von H.264-, MPEG-4- und MJPEG-komprimierten Videodaten von Pelco IP-Kameras und zur Unterstützung der PTZ-Funktionalität von Pelco IP-Kameras.

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung

- MJPEG-Videokomprimierung
- Digitale E/A
- PTZ
- Parallele Auto-Suche

Unterstützte Dateien

- PelcoIPCapture.dll
- PelcoIPCapture.xml
- Readme_PelcoIPCapture.txt

Letzte Version

1.8.3.5

Datum der Veröffentlichung

20.02.2019

9.7.1.6 VivotekIPCapture

Zweck

Zur Erfassung von MJPEG-, MPEG-4- und H.264-komprimierten Videodaten von Vivotek IP-Geräten (Kameras und Videoserver) und zur Unterstützung von PTZ- und IO-Funktionen von Vivotek IP-Geräten.

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- H.265-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Digitale E/A
- PTZ
- Parallele Auto-Suche
- Mehrfaches Streaming
- Kann Auflösung im Alarmfall ändern (CCRiA)

- Kann die Framerate im Alarm ändern (CCFiA)
- Dynamische Benutzeroberfläche (seit DVMS 8.1.2)
- Audio (2-Wege)

Unterstützte Dateien

- VivotekIPCapture.dll
- VivotekIPCapture.xml
- Readme_VivotekIPCapture.txt

Letzte Version

2.0.1.2

Datum der Veröffentlichung

21.10.2024

9.7.1.7 EHIIPCapture

Zweck

Zur Erfassung von H.265-, H.264-, MPEG-4- und MJPEG-komprimierten Videodaten von Hikvision-, Ernitec- und Interlogix-IP-Kameras, DVRs/NVRs und Encodern, zur Unterstützung der PTZ-Funktionalität und anderer unten beschriebener Funktionen.

Unterstützte Kameras:

- Hikvision IP-Kameras
- Hikvision DVRs/NVRs
- Hikvision Encoder
- Interlogix IP-Kameras
- Ernitec IP-Kameras

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- MJPEG-Videokomprimierung
- MPEG-4-Videokomprimierung
- H.264-Videokomprimierung

- H.265-Videokomprimierung
- Digitale E/A
- PTZ - Kontinuierliche PTZ-Bewegung wird standardmäßig für alle Kameras verwendet
- Bewegungserkennung für Geräte
- Mehrfaches Streaming
- Audio (Zweiwege)
- Edge-Speicherung (nur ISAPI-Geräte)
- Auflösung im Alarmfall ändern (CCRiA)
- Kann die Framerate im Alarmfall ändern (CCFiA)
- Multicast-Streaming
- ANPR mit Listenverwaltungsschnittstelle und separaten Parametern zum Ein- und Ausschließen von Nummernschild- und Erkennungsbildern

Unterstützte Dateien

- EHIIPCapture.dll
- EHIIPCapture.xml
- HikvisionDVRConnector.xml
- HikvisionEncoderConnector.xml
- Readme_EHIIPCapture.txt

Letzte Version

2.1.22.0

Datum der Veröffentlichung

06.02.2026

9.7.1.8 EIPCapture

Zweck

Zur Erfassung von MJPEG-, H.264- und MPEG-4-komprimierten Videodaten von e-Vision (El.MO), Dynacolor und Planet IP-Kameras und zur Unterstützung der PTZ-Funktionalität von PTZ-Kameras der genannten Hersteller.

Unterstützte Kameras:

- El.MO-Kameras der NH-Serie (e-Vision TPMX10x)

- Dynacolor HD IP-Kameras (e-Vision TDMX10x)
- Dynacolor HD WDR IP-Kameras (e-Vision TPMX20x)
- Dynacolor Kameras der V-Serie (e-Vision TPMX30x/TDMX30x)
- Dynacolor IP PTZ-Kameras (e-Vision ElDome)
- Planet ICA-HM131/HM131R/HM126/HM126R IP-Kameras
- Planet ICA-H652 IP PTZ-Kameras
- Dynacolor Full HD Quad-Stream Kameras

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- MPEG-4-Videokomprimierung
- H.264-Videokomprimierung
- Digitale E/A
- PTZ
- Parallele Auto-Suche
- Mehrfaches Streaming

Unterstützte Dateien

- EIPCapture.dll
- EIPCapture.dat
- EIPCapture.xml
- Readme_EIPCapture.txt

Letzte Version

2.3.2.5

Datum der Veröffentlichung

02.11.2016

9.7.1.9 GatewayIPCapture

Zweck

Zur Erfassung von MJPEG- und Native-komprimierten Videodaten von Gateway-Servern und zur Unterstützung von PTZ- und E/A-Funktionen.

Unterstützte Kameras:

- Alle Gateway-Server mit Promesa 3.0 oder höher

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- Native Videokompression
- Digitale E/A
- PTZ
- Parallele automatische Suche

Unterstützte Dateien

- GatewayIPCapture.dll
- GatewayIPCapture.xml
- Readme_GatewayIPCapture.txt

Letzte Version

1.0.4.0

Datum der Veröffentlichung

11.08.2016

9.7.1.10 HTTPIPCapture

Zweck

Zur Erfassung von MJPEG-komprimierten Videodaten von HTTP-IP-Geräten.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- MJPEG-Videokomprimierung

Unterstützte Dateien

- HTTPIPCapture.dll
- Readme_HTTPIPCapture.txt

Letzte Version

1.0.1.0

Datum der Veröffentlichung

07.02.2020

9.7.1.11 IPCameraCapture

Zweck

Zur Erfassung von JPEG/MPEG-4/H.264 komprimierten Video- und Audiodaten von UDP, Amano, GANZ, Ernitec, Sprinx IPE/NVC und IPN/IPX-Serie von IP-Videoservern und -Kameras Unterstützung der PTZ-Funktionalität dieser Geräte.

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Digitale E/A
- PTZ
- Kann die Framerate bei Alarm ändern (CCFiA)
- Parallele Auto-Suche
- Zwei-Wege-Audio
- Mehrfaches Streaming
- Multicast-Streaming
- Zeitsynchronisation
- Edge-Speicherung

Unterstützte Dateien

- IPCameraCapture.dll
- IPCameraCapture.xml

- Readme_IPCameraCapture.txt

Letzte Version

1.7.3.0

Datum der Veröffentlichung

20.02.2019

9.7.1.12 LGEIPCapture

Zweck

Zur Erfassung von H.264- und MJPEG-komprimierten Videodaten von LG Electronics IP-Geräten.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- MJPEG-Videokomprimierung
- H.264-Videokomprimierung
- Digitale E/A
- PTZ

Unterstützte Dateien

- LGEIPCapture.dll
- Readme_LGEIPCapture.txt

Letzte Version

1.0.6.3

Datum der Veröffentlichung

20.02.2019

9.7.1.13 NewActiIPCapture

Zweck

Zur Erfassung von MPEG4/MJPEG/H.264 komprimierten Videodaten von Acti, Messoa NIC910/930/950HPRO und Vido AU-GxxIP IP Kameras

Unterstützte Funktionen

- Automatische Suche

- Parallele automatische Suche
- Erkennung von Gerätebewegungen
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Mehrfaches Streaming
- Multicast-Streaming
- Datenschutz-Maske
- Zwei-Wege-Audio
- Digitale E/A
- PTZ
- Edge-Storage (ab Firmware 6.07.23 und höher)

Unterstützte Dateien

- AADP.dll
- ADADP.dll
- AFADP.dll
- FFMCodec.dll
- FisheyeSDK.dll
- KMpeg4.dll
- PTZParser.dll
- NewActiIPcapture.dll
- NewActiIPCapture.xml
- Readme_NewActiIPCapture.txt

Letzte Version

2.4.2.0

Datum der Veröffentlichung

29.08.2018

9.7.1.14 NewArecontIPCapture

Zweck

So erfassen Sie MJPEG/H.264-komprimierte Videodaten von Arecont IP-Kameras

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- H.264-Videokomprimierung
- Digitale E/A
- Mehrfaches Streaming
- Parallele automatische Suche
- Kann Auflösung im Alarmfall ändern (CCRiA)
- Ändern der Framerate im Alarmfall (CCFiA)
- Zwei-Wege-Audio

Unterstützte Dateien

- NewArecontIPcapture.dll
- NewArecontIPCapture.xml - example of custom parameters file
- Readme_NewArecontIPCapture.txt

Letzte Version

2.2.3.0

Datum der Veröffentlichu

15.08.2019

9.7.1.15 NewIQEyeIPCapture

Zweck

Zur Erfassung von MJPEG/H.264 komprimierten Videodaten und G.711 komprimierten Audiodaten von IQEye IP-Kameras.

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung

- H.264-Videokomprimierung
- Digitale E/A
- CCFIA (wird über die Konfigurationsdatei IQEye.xml aktiviert)
- Audio (nur G.711)

Unterstützte Dateien

- NewIQEyeIPcapture.dll
- IQEye.xml
- Readme_NewIQEyeIPCapture.txt

Letzte Version

1.4.6.0

Datum der Veröffentlichun

21.02.2014

9.7.1.16 NewMobotixIPCapture

Zweck

Zur Erfassung von MJPEG-komprimierten Videodaten von Mobotix-Kameras und zur Unterstützung der PTZ-Funktionalität

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- MxPEG-Videokomprimierung
- Digitale E/A
- PTZ
- Parallele automatische Suche
- Audio

Unterstützte Dateien

- NewMobotixIPCapture.dll
- NewMobotixIPCapture.xml

- Readme_NewMobotixIPCapture.txt

Letzte Version

1.4.2.0

Datum der Veröffentlichung

27.01.2022

9.7.1.17 NewPanasonicIPCapture

Zweck

Zur Erfassung von JPEG/MPEG4/H.264/H.265 komprimierten Videodaten von Panasonic IP-Kameras und zur Unterstützung der PTZ-Funktionalität.

Beachten Sie, dass der alte Panasonic-Treiber PanasonicIPCapture heißt.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- JPEG-Videokomprimierung
- MPEG4-Videokomprimierung
- H.264-Videokomprimierung
- E/A
- PTZ

Nur WV-Serie:

- Geräte-Bewegungserkennung
- Mehrfach-Streaming
- Multicast-Streaming
- Datenschutz-Maske
- Zwei-Wege-Audio
- CCFIA
- CCRIA
- Edge-Speicherung

- H.265-Videokompression
- Vaxtor ANPR

Unterstützte Dateien

- NewPanasonicIPcapture.dll
- NewPanasonicIPCapture.xml
- Readme_PanasonicIPCapture.txt

Letzte Version

1.6.3.0

Datum der Veröffentlichung

13.03.2025

9.7.1.18 NewSiquraIPCapture

Zweck

Zur Erfassung von MJPEG-, MPEG-4- und H.264-komprimierten Videodaten von Siqura C/S-5x/6x IP-Codecs und MD/HD-2x/6x PTZ-Kameras sowie zur Unterstützung der PTZ-Funktionalität bestimmter Siqura-Geräte.

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- MPEG-4-Videokomprimierung
- H.264-Videokomprimierung
- E/A
- PTZ

Unterstützte Dateien

- NewSiquraIPCapture.dll
- Readme_NewSiquraIPCapture.txt

Letzte Version

1.9.5.2

Datum der Veröffentlichung

10.02.2015

9.7.1.19 NewSonyIPCapture

Zweck

Zur Erfassung von MJPEG-, MPEG-4- und H.264-komprimierten Videodaten von SONY IP-Geräten und zur Unterstützung zusätzlicher Funktionen von SONY IP-Geräten.

Unterstützte Kameras:

Alle SONY IP-Kameras (außer SNC-RZ30 und SNC-HM662 Kameras) und G5-Videoserver.

Unterstützte Funktionen

- Automatische Suche
- MJPEG-Videokomprimierung
- MPEG-4-Videokomprimierung
- H.264-Videokomprimierung
- Digitale E/A
- PTZ
- Geräte-Bewegungserkennung
- Privatzonen
- Auflösung im Alarmfall ändern (CCRiA) (nur G2-G4-Kameras)
- Änderung der Bildrate im Alarmfall (CCFiA) (nur G2-G4-Kameras)
- Parallele automatische Suche
- Mehrfaches Streaming (für G5-G7-Kameras)
- Audio (2-Wege) (für G5-G7-Kameras)
- Zeitsynchronisierung (für G5-G7-Kameras)
- Edge-Storage (für G5-G7-Kameras)
- Dynamische Benutzeroberfläche (seit DVMS 8.1.2)

Unterstützte Dateien

- NewSonyIPCapture.dll
- NewSonyIPCapture.xml

- Readme_NewSonyIPCapture.txt

Letzte Version

2.6.4.0

Datum der Veröffentlichung

22.08.2019

9.7.1.20 PSIAIPCapture

Zweck

Zur Erfassung von H.264-komprimierten Videodaten von PSIA-IP-Kameras.
Es wird die PSIA-Version 1.1 unterstützt.

Unterstützte Kameras:

PSIA-kompatible IP-Kameras

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Digitale E/A
- Parallele automatische Suche
- Dynamische Benutzeroberfläche (seit DVMS 8.1.2)

Unterstützte Dateien

- PSIAIPCapture.dll
- Readme_PSIAIPCapture.txt

Letzte Version

1.2.6.0

Datum der Veröffentlichung

03.07.2024

9.7.1.21 RTSPIPCapture

Zweck

So erfassen Sie H.265/H.264/MPEG-4/MJPEG-komprimierte Videodaten von RTSP-IP-Geräten

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- H.265-Videokomprimierung
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Multicast-Streaming (nur RTP)
- Audio-Eingang

Unterstützte Dateien

- RTSPIPCapture.dll
- RTSPIPCapture.xml
- Readme_RTSPIPCapture.txt

Letzte Version

1.6.5.0

Datum der Veröffentlichung

11.03.2026

9.7.1.22 SIPIPCapture

Zweck

Treiber für bestimmte Zenitel-Geräte, die über das SIP-Protokoll arbeiten: Zur Erfassung von H.264-komprimierten Videodaten vom SIP-Proxy

Unterstützte Funktionen

- Automatische Suche
- H.264-Videokomprimierung
- Zwei-Wege-Audio

Unterstützte Dateien

- SIPIPcapture.dll
- Readme_SIPIPCapture.txt

Letzte Version

1.0.0.0

Datum der Veröffentlichung

17.11.2016

9.7.1.23 StanleyIPCapture

Zweck

Zur Erfassung von H.264- und MJPEG-komprimierten Videodaten von Stanley IP-Kameras, zur Unterstützung von PTZ-Funktionen und anderen unten beschriebenen Funktionen.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- MJPEG-Videokomprimierung
- H.264-Videokomprimierung
- Digitale E/A
- PTZ
- Mehrfaches Streaming
- Geräte-Bewegungserkennung
- Privatzonen

Unterstützte Dateien

- StanleyIPCapture.dll
- StanleyIPCapture.xml
- Readme_StanleyIPCapture.txt

Letzte Version

1.2.1.6

Datum der Veröffentlichung

24.09.2021

9.7.1.24 WisenetIPCapture

Zweck

Zur Erfassung von H.265/HEVC-, H.264- und MJPEG-komprimierten Videodaten von Wisenet IP-Geräten und zur Bereitstellung zusätzlicher Funktionen (Digital I/O, PTZ, Privacy Masking usw.) für diese Geräte. Die SUNAPI-Spezifikation Version 2.x wird unterstützt.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- H.265/HEVC-Videokomprimierung
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Erkennung von Gerätebewegungen
- Mehrfaches Streaming
- Audio (2-Wege)
- Multicast-Streaming
- Datenschutz-Maskierung
- Digitale E/A
- PTZ
- Edge Storage (seit DVMS 8.0.0)
- Dynamische Benutzeroberfläche (seit DVMS 8.1.2)
- CCRiA (Kann die Auflösung im Alarmfall ändern)
- CCFiA (Kann die Framerate im Alarmfall ändern)
- Zeitsynchronisation
- Videoverlust-Erkennung
- Vaxtor ALPR
- WisenetRoadAI

Unterstützte Dateien

- WisenetIPCapture.dll
- WisenetIPCapture.xml
- Timezones.xml
- Readme_WisenetIPCapture.txt

Letzte Version

1.3.4.0

Datum der Veröffentlichung

23.09.2026

9.7.1.25 DahuaIPCapture

Zweck

Erfassung von mit H.265, H.264, MPEG-4 und JPEG komprimierten Videodaten von Dahua-IP-Geräten sowie Bereitstellung zusätzlicher Funktionen (Digital I/O, PTZ, Privacy Masking usw.) für diese Geräte.

Unterstützte Funktionen

- Automatische Suche
- Parallele automatische Suche
- H.265/HEVC-Videokomprimierung
- H.264-Videokomprimierung
- MPEG-4-Videokomprimierung
- MJPEG-Videokomprimierung
- Erkennung von Gerätebewegungen
- Mehrfaches Streaming
- Audio (2-Wege)
- Multicast-Streaming
- Datenschutz-Maskierung
- Digitale E/A
- PTZ

- CCFiA (Kann die Framerate im Alarmfall ändern)
- Edge Storage
- AES-256-verschlüsselter Unicast-Videostream

Unterstützte Dateien

- DahuaIPCapture.dll
- DahuaIPCapture.xml
- Readme_DahuaIPCapture.txt
- avnetsdk.dll
- d3dx9_24.dll
- dhconfigsdk.dll
- dhnetsdk.dll
- dhplay.dll
- fisheye.dll
- HWDec.dll
- Infra.dll
- Json.dll
- libcurl.dll
- libeay32.dll
- NetFramework.dll
- ssleay32.dll
- Stream.dll
- StreamConvertor.dll
- StreamSvr.dll

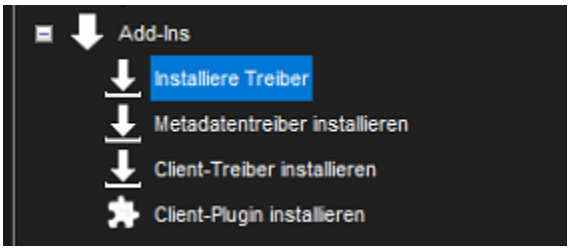
Letzte Version

1.3.8.0

Datum der Veröffentlichung

30.11.2023

9.7.2 Installieren externer Treiberpakete

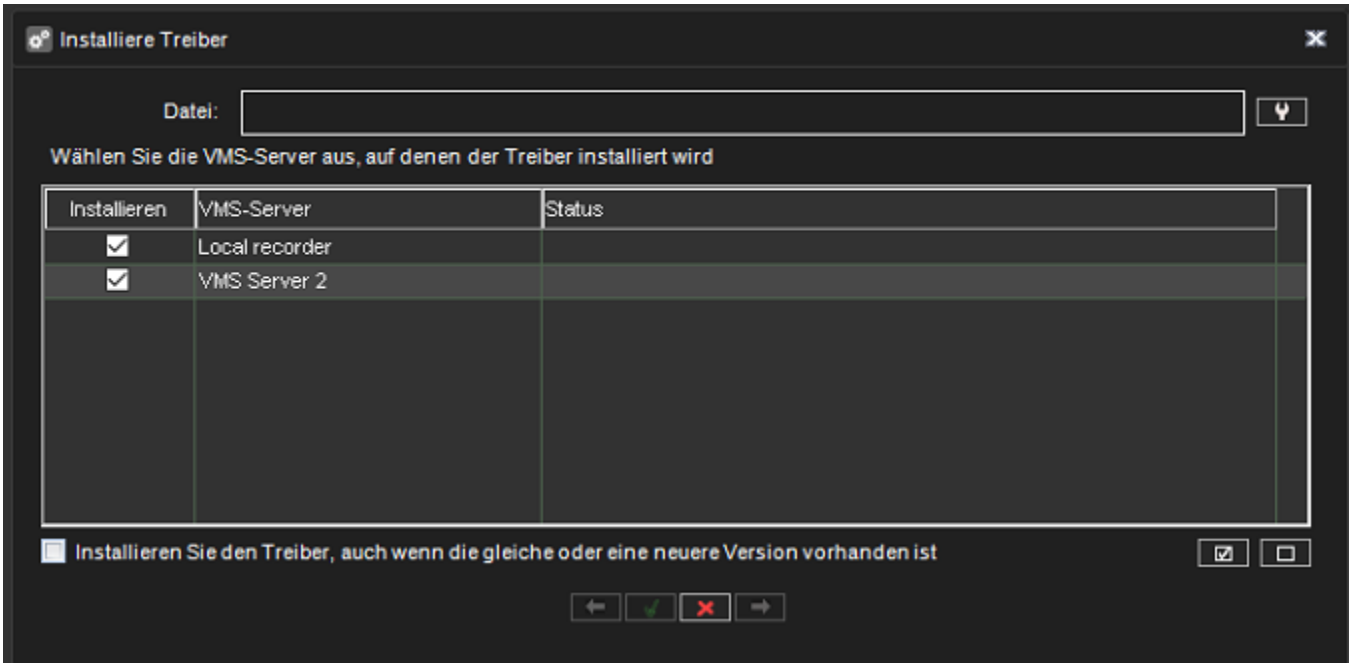


Um IP-Kameras, digitale E/A-Geräte oder Textdaten im VMS-System zu verwenden, muss der Treiber für jedes Gerät auf dem Server installiert werden.
Die Software enthält alle Treiber und Plugins, die in den vorherigen Versionen der Software enthalten waren. Jedoch Bei Bedarf können neue Treiber und Plugins manuell installiert werden.
Um einen neuen Treiber zu installieren, benötigen Sie ein gerätespezifisches Treiberinstallationspaket.
Das Treiberinstallationspaket ist ein komprimierter (gezippter) Ordner, der die Treiberdateien enthält.
Bei der Installation eines Treibers Installationspaket, vergleicht das System die Dateien im Installationspaket mit den vorhandenen Dateien auf den Servern.
Normalerweise installiert es die Dateien nur dann, wenn sie auf den Servern nicht vorhanden sind oder wenn die Dateien im Installationspaket neuer sind als die Dateien auf den Servern .
Sie können das System jedoch bei Bedarf dazu zwingen, eine beliebige Treiberversion zu installieren.

Notiz: *Wenn Sie einen bereits vorhandenen Kameratreiber aktualisieren möchten, entfernen Sie die Kamera aus dem System, bevor Sie den Treiber aktualisieren.Nach dem Entfernen der Kamera installieren Sie die Treiberdatei, danach können Sie die Kamera neu installieren.Nach der Installation eines neuen Treibers müssen Sie konfigurieren die Geräte, die den Treiber verwenden.*

So installieren Sie ein Treiberpaket:

1. Öffnen Sie auf der Registerkarte **System** unter **Add-Ins** die Option **Treiber installieren**.
2. Wählen Sie das Laufwerk aus, auf dem sich das Treiberpaket befindet, suchen Sie das Treiberpaket (.zip-Datei) und wählen Sie es aus. Das Dialogfeld **Treiber installieren**wird angezeigt.



3. Wählen Sie die Server aus, auf denen Sie den Treiber installieren möchten.

4. Wenn Sie das System zwingen möchten, die Treiberpaketversion zu installieren, wählen Sie **Treiber installieren, auch wenn dieselbe oder eine neuere Version vorhanden ist.**

5. Klicken Sie auf **Install**. Die Spalte **Status** zeigt den Text **Installed** an, wenn der Treiber erfolgreich installiert wurde. Wenn der Treiber nicht installiert ist, zeigt die Spalte eine Fehlermeldung an.

6. Klicken Sie auf **Schließen**, um das Dialogfeld zu verlassen.

Hinweise*:*

- Wenn Sie Treiber für andere Hardware als IP-Kameras aktualisieren müssen, wenden Sie sich bitte an den Systemlieferanten.
- Ein 32-Bit-System erfordert ein 32-Bit-Treiberpaket und ein 64-Bit-System erfordert ein 64-Bit-Treiberpaket.

9.7.3 Treiberinstallation und -verwendung

9.7.3.1 ArchiveCapture - Installation und Verwendung

Der Pfad für das Archiv wird in das Adressfeld (automatisches Suchfenster) eingegeben.

Die Treiberkonfiguration erfolgt über ArchiveCapture.xml:

- Schleifenfunktion
- Zeit der ursprünglichen (aufgenommenen) Bilder

- Bildrate (konfigurierbar oder Standard)
- Zeitlimits für die Aufnahme aus dem gespeicherten Archiv
- Aktivieren/Deaktivieren von Videokanälen

Die Abschnitte „Kanäle“ und „Limit“ können komplett deaktiviert werden (Attribut enabled=„0“)

Ohne ArchiveCapture.xml werden die Standardwerte verwendet.

Die Einstellungen der XML-Datei werden nur während der Archivsuche angewendet.

PAUSE, CONTINUE und NEXT_FRAME sind implementiert über `CIPVideoCapture::SetExtendedProperty`(const char* const `aProperty`, void* aValue, unsigned long `aChannelId`) wobei:
`aProperty` - Befehl, kann sein "PAUSE", "CONTINUE" and "NEXT_FRAME"
`aValue` - für zukünftige Bedürfnisse, sollte NULL sein
`aChannelId` - Kanal-ID

9.7.3.2 CanonIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber die RTSP/RTP/UDP/IP-Protokolle für den Empfang des Videostroms und des Eingangsstatus.

Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Standard-Ports sind 80,
- **RTSP**: Connection 554,
- **UDP**: Zwei sequentielle Ports pro Videostrom und zwei sequentielle Ports pro Metadatenstrom (Eingangszustände) werden in einem Portbereich von 3556 bis 4556 benötigt.

Beispiel: Wenn ein DVMS über 2 IP-Kameras verfügt, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Die Datei CanonIPCapture.xml wird zur Konfiguration des Treiberverhaltens verwendet:

- Unicast
- Multicast:Primary
- Multicast:Listener

Parameter für die PTZ-Geschwindigkeitsbegrenzung:

- PanSpeed (1 - 100%, Grenzgeschwindigkeit für gewünschten Prozentwert)
- TiltSpeed (1 - 100%, Grenzgeschwindigkeit für gewünschten Prozentwert)

- ZoomSpeed (1 - 100%, Grenzgeschwindigkeit für gewünschten Prozentwert)
- PTZQueueSize (PTZ-Warteschlangengröße, kann für langsame Kameras optimiert werden)

9.7.3.2.1 Beschränkungen

- Ältere Canon Kameras mit Firmware 1.0.3 oder früher können bei jeder Auflösungsänderung neu starten. Dies kann 1-5 Minuten dauern.
- VB-S-Kameras haben 2 H.264-Streams, die für die Aufzeichnung und die Live-Übertragung im VMS verwendet werden können. Andere Serien haben nur einen H.264-Kanal.
- VB-S-Kameras haben eine Beschränkung auf eine maximale Framerate von 15 für ausgewählte Auflösungen. Wenn eine dieser Kombinationen eingestellt ist, wird die Bildrate geändert, auch wenn die DVMS-Einstellungen anders sind:
    - 1920x1080 - Alle Größen
    - Alle Größen - 1920x1080
    - 1280x960 - 1280x960
    - 1280x720 - 1280x720
- Die Kamera der Serien VB-M, VB-H und VB-S unterscheidet sich von der herkömmlichen Bewegungserkennung. Die Erkennung erstellt ein statisches „Hintergrundbild“ und vergleicht jede Szenenänderung innerhalb des Erfassungsbereichs mit diesem Bild.
  Die Kamera sendet eine „Ereignis EIN“-Statusmeldung, wenn das Objekt in den Erfassungsbereich eintritt, und sendet einen „Ereignis AUS“-Status, wenn ein Objekt aus dem Erfassungsbereich herauskommt und die Szene wieder in das ursprüngliche „Hintergrundbild“ geändert wird.“
  Wenn der Status „Ereignis EIN“ über einen Zeitraum von 5 Minuten anhält, betrachtet die Kamera dies als einen neuen Hintergrund, sendet den Status „Ereignis AUS“ und kehrt in den Standby-Modus der Alarmerkennung zurück.
- **Unicast mode**: Der Treiber ändert die Kameraeinstellungen entsprechend den DVMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über eine Unicast-Verbindung.
- **Multicast:Primary**: Der Treiber ändert die Kameraeinstellungen entsprechend den DVMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über eine Multicast-Verbindung.
- **Multicast:Listener**: Der Treiber ändert keine Kameraeinstellungen, sondern empfängt lediglich Audio- und Videodaten von der Kamera über die Multicast-Verbindung.
- Wenn die Kamera in mehreren DVMS-Instanzen verwendet werden soll, sollte ein DVMS auf Multicast:Primary und die anderen auf Multicast:Listener eingestellt werden.
- Mehrere Multicast:Primary-Konfigurationen oder Multicast:Primary- und Unicast-Konfigurationen sind nicht zulässig; in anderen Fällen sollte die Kamera mit ständigen gleichzeitigen Einstellungsänderungen überlastet werden.

- CCFIA und CCRIA sind für die VB-M-Serie deaktiviert, da Kameras dieser Serie nach einer Änderung der Einstellungen einen Neustart erfordern.

9.7.3.3 DahuaIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Videoempfang in allen Komprimierungsmodi.

Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet. Wenn sich eine Firewall zwischen DVMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Hafen 554,
- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden in einem Portbereich von 3556 bis 4556 benötigt.

Wenn beispielsweise 4 Dahua IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.3.1 Beschränkungen

- Für mehrere Streaming-Funktionen können je nach verwendetem Gerät Einschränkungen gelten (z. B. kann die Auflösung des Extra-Streams nicht höher sein als die des Video-Mainstreams). Bitte lesen Sie das Handbuch des Geräts, um diese Einschränkungen zu erfahren.
- Die Funktion CCRiA (Can Change Resolution in Alarm) wird nicht unterstützt, da die Anwendung einer neuen Auflösung länger dauert als der Timeout für den Signalverlust.
- Kameras mit zwei abhängigen Sensoren, zum Beispiel DH-SDT4E425-8P-GB-APV1, werden nicht vollständig unterstützt.
  Unser VMS unterstützt keine unterschiedlichen Auflösungen für verschiedene Kanäle desselben Geräts. Alle Kanäle haben die gleiche Auflösungsliste, aber es können nur unterstützte Auflösungen verwendet werden. Das Gleiche gilt für die Änderung der Auflösung in der Alarmfunktionalität.
- Wenn Dahua/Stanley-Geräte die Auflösung oder Framerate nicht korrekt ändern, aktualisieren Sie sie bitte auf eine neue Firmware. Der Treiber gibt die folgende Meldung in der Datei DVRLog.txt aus:
  - „Kann keine Videokanäle für Gerät <ip>:80 konfigurieren, Ergebniscode: 12002 (Request timeout).“ „Das Gerät akzeptiert möglicherweise keine neuen Videoeinstellungen ohne korrekten Bitratenparameter. Die Kamera sendet einen falschen Bitratenbereich, und der Treiber berechnet eine inakzeptable Bitrate nach Qualität und versucht, sie sowohl im CBR- als auch im VBR-Modus anzuwenden. Es ist möglich, den Bitratenbereich mit der folgenden Option in der Datei DahuaIPCapture.xml zu überschreiben <BitrateMap enabled=„yes“ Der Treiber verfügt über eine interne Bitratenkarte für die meisten Auflösungen bis zu 1920x1080 nur für den H.264-Codec. Es ist möglich, weitere Bitraten für höhere Auflösungen und den JPEG-Codec hinzuzufügen, wie in den Beispielen im XML des Treibers gezeigt.

- Das Dahua-Gerät wird möglicherweise mit einer niedrigeren maximalen Bildrate hinzugefügt, als einige Auflösungen unterstützen. Bitte aktualisieren Sie die Firmware. Wenn dies nicht möglich ist, entfernen Sie das Dahua-Gerät aus DVMS, legen Sie die erforderlichen Videoeinstellungen über die Weboberfläche fest, und fügen Sie es erneut hinzu.
- Wenn das Dahua-Gerät viele „400“ oder „500“ HTTP-Fehler als Antwort zurückgibt, aktualisieren Sie es bitte auf eine neue Firmware. Falls das Firmware-Update nicht verfügbar ist, gibt es mehrere Parameter in der Datei DahuaIPCapture.xml:
    - `<UseEventManager>false</UseEventManager>` So deaktivieren Sie die „EventManeger“-Abfrageanforderungen
    - `<InputCheckTimeout>1000</InputCheckTimeout>` Zum Einstellen des Intervalls zwischen den Anfragen für digitale Eingänge, nur wenn die Option <UseEventManager>false</UseEventManager> deaktiviert ist
    - `<Control digitalInputs="false" motionDetection="false" />` So deaktivieren Sie die digitalen Eingänge und die Bewegungserkennung der Kamera-Hardware
- Einschränkungen der Audiofunktionalität:
    - Der Treiber verwendet die Audiofunktionalität „wie sie ist“, ohne dass die Audioparameter (wie die Ausgangsverstärkung) angepasst werden. Bitte konfigurieren Sie diese Parameter über das Web-Interface.
    - Der Treiber unterstützt die Audiokodierungen G.711 und G.726. Die AAC-Kodierung wird nicht unterstützt.
    - Bei einigen Firmware-Versionen kann es vorkommen, dass Two-Way-Audio nach einer Netzwerkunterbrechung nicht funktioniert. Bitte entfernen Sie das Gerät aus DVMS, starten Sie es neu und fügen Sie es erneut hinzu. Um diese Funktion für ein bestimmtes Gerät zu deaktivieren, setzen Sie die folgende Option: `<TwoWayAudio>NO</TwoWayAudio>`
- Einschränkungen bei der Multicast-Erfassung:
    - Die Multicast-Erfassung kann über eine XML-Konfigurationsdatei mit der Option RTPMode aktiviert werden. Diese Option wird beim Start des Streams gelesen, so dass eine Aktualisierung der Geräteeinstellungen ausreicht, um die geänderte RTPMode-Option zu aktivieren.
    - Der Benutzer sollte sicherstellen, dass nur ein Rekorder die Einstellungen von IP-Geräten ändert. Andere Rekorder, die diese Kamera verwenden, sollten keine Einstellungen ändern.
      Bitte deaktivieren Sie die Änderung der Kameraeinstellungen mit der folgenden Option
      `<ChangeSettings>false</ChangeSettings>`
      In diesem Modus ändert der Treiber die folgenden Kameraeinstellungen nicht:
      = Quality
      = Resolution
      = Framerate

- `<ChangeSettings>true</ChangeSettings>`
  Der Treiber ändert die Kameraeinstellungen entsprechend den DVMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über eine Multicast-Verbindung. Bitte konfigurieren Sie diesen Modus nur für den primären Rekorder.
- Für den sekundären Rekorder werden die folgenden Optionen genauso konfiguriert wie für den primären Rekorder:
  = Mehrere Streaming-Optionen
  = Video Codec für alle Streams
- Verschlüsseltes Streaming weist bekannte Probleme und Einschränkungen auf:
  - Der Dahua IP Capture-Treiber unterstützt den Empfang verschlüsselter Videoströme von den IP-Geräten. Die Verarbeitung des verschlüsselten Streams basiert auf 3 Dahua-Bibliotheken (NetSDK und PlaySDK von Dahua)
  - Die Stream-Verschlüsselung sollte über die Web-UI aktiviert werden, bevor sie im Mirasys VMS verwendet wird. Um sie zu aktivieren, gehen Sie zu den Geräteeinstellungen, wählen Sie die Gruppe „System“ und dann die Untergruppe „Sicherheit“ oder „Safety“ (der Name kann bei verschiedenen Geräten unterschiedlich sein). Wählen Sie im Einstellungsdialog die Registerkarte ÑSystemdienstì und aktivieren Sie das Kontrollkästchen ÑAudio- und Videoübertragungsverschlüsselungì.
  - Wenn das IP-Gerät die Stromverschlüsselung unterstützt, fügt das System den Transport „AES-256 verschlüsselt“ hinzu und wählt ihn als Standardtransport aus. Wenn Sie keine Stromverschlüsselung benötigen ñ wählen Sie einfach einen anderen Transport entsprechend Ihren Anforderungen.
  - Der AES-256-Algorithmus wird für die Stream-Verschlüsselung gemäß dem GDPR-Spezifikationsdokument von Dahua verwendet. Es wird die Key-Frame-Verschlüsselung verwendet. Mit anderen Worten:
    = Die Stream-Verschlüsselung kann für H.265-, H.264- und MPEG-4-Kodierungen verwendet werden;
    = Der MJPEG-Stream kann nicht verschlüsselt und unverändert über SDK-Bibliotheken empfangen werden.
  - MPEG-4-Verschlüsselung wird unterstützt. Es war jedoch kein Gerät verfügbar, um dies in Mirasys zu testen. Daher wurde die Implementierung auf der Grundlage der SDK-Dokumentation vorgenommen, aber nicht getestet.
  - Die Audioverschlüsselung ist über NetSDK verfügbar, wurde aber nicht in den Treiber implementiert.
  - Die Verschlüsselung wird für Multicast-Streaming nicht unterstützt.

- Für einen schnellen Start der Videoaufzeichnung im Multicast-Modus ist es möglich, Adressen und Ports auf dem Gerät und in der Treiber-XML-Datei zu konfigurieren und die Anpassung der Videoeinstellungen durch die folgende Option <ChangeSettings>false</ChangeSettings> zu deaktivieren.
- Der Zoom funktioniert bei der Stanley IPC-STAN-6100IRV Kamera möglicherweise nicht richtig. Dies ist ein Problem der Kamera-Firmware.
- Der Treiber unterstützt keinen Unicode in PTZ-Voreinstellungsnamen (Präposition).
- Bitte versuchen Sie nicht, die Kamera mit der Option <Alle Treiber> und den <Standard>-Anmeldeinformationen oder einem falschen Kennwort zu suchen - **dies kann das Benutzerkonto sperren**. Bitte fügen Sie das Gerät stattdessen mit einem einzigen „DahuaIPCapture"-Treiber hinzu.
- Dieser Treiber unterstützt nicht Windows XP.

9.7.3.4 EHIIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/HTTP/HTTPS/UDP/IP-Protokolle für den Videoempfang in allen Komprimierungsmodi. Außerdem werden HTTP/HTTPS-Protokolle für das Einstellen/Abrufen von Parametern und für Remote Stream Video verwendet. Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP/HTTPS-Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **HTTPS**: Der Standard-Port ist 443,
- **RTSP**: Hafen 554,
- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden in einem Portbereich von 3556 bis 4556 benötigt.

Wenn beispielsweise 4 Kameras in DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Die Datei EHIIPCapture.xml kann verwendet werden, um eine 360-Grad-Ansicht (Kanal) auszuwählen - bitte geben Sie die Kanalnummern an, die im folgenden Abschnitt in XML verwendet werden sollen:

```
<Channel360>1</Channel360>
<Channel360>2</Channel360>
```

Nach dem Festlegen der Kanalnummern für eine 360-Grad-Kamera muss die Kamera entfernt und wieder hinzugefügt werden, um die korrekten Funktionen für die Kanäle zu erkennen.

Für das Multicast-Streaming sind ebenfalls zwei aufeinanderfolgende Ports pro Audio- oder Videostream erforderlich, aber die Portnummern hängen von den Geräteeinstellungen oder der XML-Konfiguration ab.

Beispielsweise kann das Gerät so konfiguriert sein, dass alle Datenströme nur an einen einzigen Anschluss gesendet werden. Wenn für diese Einstellung der Anschluss 40000 angegeben ist, sollten die Anschlüsse 40000-40001 geöffnet werden.

9.7.3.4.1 Beschränkungen

- Es wird nur ein Audio-Multicast-Stream unterstützt. Eine Multicast-IP-Adresse wird für den Audiokanal und für den Videokanal verwendet, aber der Multicast-Audio-Port für denselben Stream sollte mindestens um 2 größer sein als der Video-Port, der Multicast-Video-Port für einen anderen Stream (z. B. Live) sollte mindestens um 6 größer sein als der Video-Port des vorherigen Streams (z. B. Aufnahme).
- Der Audiokanal verwendet die gleiche Multicast-IP-Adresse wie der Videostream-Empfänger. Wenn unterschiedliche Multicast-Adressen definiert sind, kann dies zu einem Konflikt in der Multicast-Konfiguration führen, die vom Videokanal (aus der Dynamic UI-Konfiguration) und dem Audiokanal (aus der XML-Datei geladen) angewendet wird.
- Sie müssen IGMP Snooping auf dem Netzwerk-Switch für die Multicast-Kommunikation aktivieren.
- Für den HTTP/HTTPS-Transport wird die folgende Logik implementiert: Das dynamische Feld RTPoverHTTP wird hinzugefügt, wenn die Kommunikation über HTTP verwendet wird oder wenn die Kommunikation über HTTPS verwendet wird. Das Gerät unterstützt die Funktion RTPoverHTTPS.
- Was das TLS-Zertifikat betrifft, so gibt die Kamera bei einer RTSP-Verbindung über HTTPS (TLS) ihr öffentliches Zertifikat während des Handshake-Verfahrens weiter. Daher müssen Clients das öffentliche Zertifikat der Kamera nicht speichern oder besitzen.
- Der Mehrfach-Streaming-Modus wird erst ab DVMS 6.1 korrekt unterstützt.
- Das Komprimierungsformat für die Aufzeichnung und das Live-Streaming sollte im Mehrfach-Streaming-Modus identisch sein.
- Die Kameras werden nach dem Ändern des Komprimierungsformats neu gestartet, so dass es etwa 30 Sekunden dauert, bis das Video nach dem Ändern des Komprimierungsformats wiederhergestellt ist.
- Bei Geräten mit zwei Streams pro Kanal („Main“ und „Sub“) hat der Remote-Stream die gleiche Auflösung wie der Aufnahmestream, so dass die Auflösungseinstellung für einen solchen Stream, bei dem es sich um eine HTTP-JPEG-Aufnahme handelt, nicht verwendet wird.
- Bei Geräten mit 3 Streams pro Kanal gibt es diese Einschränkung nicht.
- Einige Versionen der Hikvision-Firmware geben eine Liste von Auflösungen zurück, die von der Kamera nicht unterstützt werden. Diese Auflösungen können in DVMS angewendet werden, aber die Kamerabilder weisen Artefakte auf.
- Hikvision-Kameras unterstützen nur 6 RTSP-Sitzungen zur gleichen Zeit. Dies ist eine Einschränkung der Hikvision-Firmware.
- Die Bewegungserkennung sollte vor der Verwendung im DVMS manuell auf dem Gerät konfiguriert werden. Die MD-Funktionalität funktioniert möglicherweise nicht korrekt mit alten Firmware-Versionen. Bitte verwenden Sie die neueste Firmware-Version, um alle Treiberfunktionen zu nutzen.

- Der Empfang von Eingangszuständen sollte in der XML-Konfigurationsdatei aktiviert und in der Webschnittstelle des Geräts konfiguriert werden (z. B. das Senden von Eingangszuständen mit „Notify Surveillance Center“ aktivieren).
- Der dritte Stream der Hikvsion-Geräte wird als Live-Stream und der zweite als Remote-Stream verwendet.
- Die Videoverlusterkennung sollte manuell auf dem Gerät konfiguriert werden, bevor sie im DVMS verwendet wird. Sie kann auch in der Konfigurationsdatei deaktiviert/aktiviert werden.

9.7.3.5 EIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Videoempfang in allen Komprimierungsmodi.

Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Hafen 554,
- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden in einem Portbereich von 3556 bis 4556 benötigt.

Beispiel: Wenn 4 El.MO oder Dynacolor IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.5.1 Beschränkungen

- Die WinInet-Bibliothek wird zum Senden/Empfangen von HTTP-Daten zwischen DVMS und der e-Vision/Dynacolor-Kamera verwendet. Die Version 8.0 dieser Bibliothek hat eine Einschränkung: Es können nur 2 HTTP-Verbindungen gleichzeitig geöffnet werden (siehe den folgenden Artikel: http://support.microsoft.com/kb/183110).> Dieses Problem tritt auf, nachdem der Internet Explorer auf 8.0 oder höher aktualisiert wurde.
- Wenn die Webschnittstelle der Kamera auf demselben PC geöffnet wird, auf dem dieser Treiber verwendet wird, können aufgrund dieser Einschränkung einige HTTP-Anfragen nicht gesendet werden. In diesem Fall wird die Kamera möglicherweise nicht von der automatischen Suche gefunden, oder einige Funktionen funktionieren überhaupt nicht.
- Die Option „Video-OCX-Protokoll“ sollte auf „RTP über UDP“ (oder „RTP über RTSP(TCP)“ in einigen Fällen) eingestellt werden, damit der RTP/RTSP-Videostream korrekt empfangen wird. Diese Option kann nicht per CGI-Abfrage eingestellt werden. Stellen Sie sie daher vor der Verwendung der Kamera manuell über die Webschnittstelle (Registerkarte Streaming) ein.
- Die El.MO- und Dynacolor-Kameras (außer Dynacolor HD WDR IP-Kameras) haben spezifische Auflösungseinstellungen. Die Kamera kann verschiedene Auflösungen für verschiedene Codecs

unterstützen. Die Kameras der NH-Serie unterstützen beispielsweise die folgenden Auflösungen (die maximale Framerate ist in Klammern angegeben):

  - MJPEG video codec - 1280x960(12.5 fps), 640x480(25 fps);
  - MPEG4 video codec - 640x480(25 fps), 320x240(12.5 fps), 352x288(12.5 fps), 176x144(12.5 fps).

- Wenn Sie versuchen, eine nicht unterstützte Auflösung einzustellen, wird die am besten geeignete Auflösung verwendet. Detaillierte Informationen zu den von der Kamera unterstützten Auflösungen finden Sie in den Kameraeinstellungen (Seite Streaming -> Videoformat, Abschnitt „Videoauflösung“).
- Die El.MO- und Dynacolor-Kameras unterstützen nur eine oder zwei Bildraten (z. B. 25 oder 12,5 für PAL-Kameras der NH-Serie). Andere Bildwechselfrequenzen können über die Einstellung „Frame Skip“ angewendet werden. Normalerweise unterstützt die Kamera intern das Überspringen von 5, 10 und 15 Bildern. Wenn die Kamera 25 Bilder pro Sekunde für eine bestimmte Auflösung unterstützt, sendet die Kamera einen Stream mit 5, 2,5 und 1,67 Bildern pro Sekunde bei entsprechenden Einstellungen für die Bildüberspringung. Wenn Sie also versuchen, eine nicht unterstützte Framerate einzustellen, kann die tatsächliche Framerate größer sein als die in VMS verwendete. Es wird der am besten geeignete Wert verwendet.
- Der Videostream für Kameras der NH-Serie weist bei VGA-Auflösung mit den höchsten Bildraten- und Qualitätseinstellungen (sowohl für MPEG-4- als auch für MJPEG-Codecs) eine unstetige Bildrate auf. Die tatsächliche Bildrate schwankt zwischen 18 und 30 Werten, aber der Durchschnittswert der Bildrate ist um 1-2 fps niedriger als erforderlich. Dies ist ein Problem der Kamera.
- Dynacolor- und El.MO-Kameras wenden jede Anforderung von Stream-Einstellungen an, die sich in etwa 20 Sekunden ändern. Dies ist eine Funktion der Kamera.
- Die IP-PTZ-Kameras haben die folgenden Probleme:
  - Die Kamera gibt bei jedem IO-Befehl immer einen HTTP-Fehlercode 503 zurück - dies ist ein Firmware-Problem. Das IO-Modul ist bei Kameras der IP PTZ-Serie vorübergehend deaktiviert.
  - Die Kamera kehrt den „Fokus“-Befehl um: Sie führt die Aktion „Fokus nah“ für den Befehl „Fokus fern“ aus und umgekehrt. Dies ist ein Firmware-Problem.
  - Die Kamera stellt die Verbindung nach dem Abziehen des Netzwerkkabels nicht wieder her. Nachdem die Verbindung wiederhergestellt ist, sollte die Kamera manuell neu gestartet werden.
- Die HD-WDR-IP-Kameras haben die folgenden Probleme:
  - Die Kamera sendet MPEG-4-Bilder mit einer höheren Bildrate als erforderlich. Zum Beispiel kann die Kamera bei maximaler Auflösung (1280x960) bis zu 16 Bilder pro Sekunde senden, anstatt 12,5
  - Die Kamera unterstützt kein Frame Skipping für die maximale Auflösung (1280x960) für den H.264-Codec. Dies ist eine Funktion der Kamera. Daher ist nur eine Bildrate (maximal 25 oder 30 Bilder/s) für die maximale Auflösung des H.264-Codecs verfügbar.

- Die Kameras der V-Serie haben ein Problem mit dem H.264-Codec. Nach der Anwendung von 100 % Qualität für den H.264-Codec sendet die Kamera einen falschen Videostream (der VLC-Player spielt ihn nicht ab, und VMS zeigt eine Menge Frame-Skipping-Meldungen an). Dieses Problem tritt gelegentlich auf.
- Die 5-Megapixel-360∞-Fisheye-Kameras unterstützen nur Fischaugenansichten. Derzeit unterstützen sie nicht die Auswahl eines anderen Sichtbereichs.
- Mehrere Streaming-Beschränkungen:
    - Ab DVMS 6.1.1 werden mehrere Streaming-Funktionen für Full-HD Quad Stream-Kameras unterstützt. Andere Kameras werden als Single-Stream-Geräte verwendet.
    - Aufzeichnung und Live-Streams unterstützen nur H.264-Kodierung. Der Remote-Stream unterstützt sowohl MJPEG- als auch H.264-Kodierungen.
    - Die Auflösungen der verschiedenen Streams hängen voneinander ab. Für die Auflösung gilt folgende Regel: Die Auflösung eines Live-Streams kann nicht größer sein als die Auflösung eines Aufzeichnungs-Streams. Die gleiche Regel gilt für Remote- und Live-Streams. Weitere Informationen zu diesen Auflösungsbeschränkungen finden Sie im Handbuch des Geräts oder im Webinterface.

9.7.3.6 GatewayIPCapture - Installation und Verwendung

Der Treiber verwendet TCP/IP-Protokolle für den Videoempfang und das Setzen/Abrufen von Parametern in allen Komprimierungsmodi. Der Standard-Gateway-TCP-Port ist 9000. Wenn sich zwischen VMS und den Servern eine Firewall befindet, muss dieser Port geöffnet werden.

Für den Gateway-Treiber sollte ein eigenes Profil (kein Dienst) verwendet werden. Dies kann in der Datei GatewayIPCapture.xml konfiguriert werden (Profilname). Andernfalls kann die Anzahl der verwendeten Kameras falsch sein.

9.7.3.7 HTTPIPCapture - Installation und Verwendung

Der Treiber verwendet das HTTP-Protokoll, um Videoströme von IP-Geräten zu empfangen.

Der Treiber erwartet, dass die HTTP-URI zum Gerät hinzugefügt und in das Feld „IP-Adresse“ eingetragen wird.

Der erforderliche Port kann separat im Feld „Port“ oder in der HTTP-URI angegeben werden. Der HTTP-URI-Port hat eine höhere Priorität; wenn er angegeben ist, wird das DVMS-Portfeld ignoriert.

Die Stream-URI-Anforderungen: Die HTTP-URI sollte im vollständigen Format angegeben werden, z. B. http://192.168.1.70:8080/video.

Die Stream-URI kann über Player von Drittanbietern, wie VLC, überprüft werden.

9.7.3.7.1 Einschränkungen

Wenn die Kamera eine Basic-HTTP-Autorisierung erfordert, müssen der richtige Benutzername und das richtige Kennwort eingegeben werden. Andernfalls wird kein Video übertragen.

9.7.3.8 IPCameraCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Video- und Audioempfang in allen Komprimierungsmodi.

Das HTTP/HTTPS-Protokoll wird zum Einstellen/Abrufen von Parametern und für die PTZ-Funktionalität verwendet.

Wenn sich eine Firewall zwischen DVMS und den UDP-IP-Geräten befindet, müssen die folgenden RTSP/UDP/HTTP/HTTPS-Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **HTTPS**: Standardport ist 443 (wenn auf der Kamera aktiviert)
- **RTSP**: Hafen 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Audio-/Videostream werden in einem Portbereich von 3556 bis 4556 benötigt.

9.7.3.8.1 Beschränkungen

UDP-Kameras verarbeiten manchmal den PTZ-Stoppbefehl nicht. Um dieses Problem zu vermeiden, sendet der Treiber vier Stopps.

Es gibt keine Blendeneinstellungen für UDP/Amano/GANZ-Kameras. Die Firmware für UDP/Amano/GANZ-Kameras ermöglicht Änderungen der Videostandards, aber die Kameras unterstützen (im Allgemeinen) nur einen dieser Standards.

2Mpx-Kameras haben ein Problem mit MJPEG 100% Qualität - es stoppt Streaming. 2Mpx-Kameras haben unterschiedliche Auflösungen für MPEG4-Codec (keine 2Mpx).

Die IPE1100 M-Kameras haben eine Einstellung für die maximale Auflösung (SETUP > Video & Audio > Video-In > Parameter Videoauflösung). Diese Einstellung bestimmt die Liste der verfügbaren Auflösungen, z. B. ist die Mindestauflösung für 2Mpx VGA, und kleinere Auflösungen sind nicht verfügbar.

Das Aktivieren von Mehrfach- oder Multicast-Streaming-Funktionen kann die Geräteleistung verringern. Daher werden beide Videoströme mit niedrigeren Frameraten als derzeit verwendet gesendet.

Geräte der IPE-Serie senden alle Streams mit instabilen Bildraten, wenn mindestens einer dieser Streams für MJPEG-Codierung konfiguriert ist. Die Bildrate wird stabil, wenn der MJPEG-Stream gestoppt wird. Dies ist eine Funktion der Geräte der IPE-Serie.

Bei Geräten der IPN/IPX-Serie kann es vorkommen, dass die Videoeinstellungen für einen langen Zeitraum (70-90 Sekunden) gelten, wenn die Funktion für mehrfaches Streaming aktiviert ist. Bitte warten Sie, bis der Videostream beginnt, bevor Sie die Videoeinstellungen erneut ändern.

Geräte der IPN/IPX-Serie enthalten den folgenden Hinweis in der Webschnittstelle: „Wenn eine vertikale Auflösung von 1080P ausgewählt wird, können andere Videoströme keine höhere horizontale Auflösung als 1088

unterstützen.“ Das Verhalten der Kamera kann unerwartet sein, wenn der Benutzer versucht, für beide Videoströme eine Auflösung von 1080p zu verwenden.

Einschränkungen bei Multicast-Aufnahmen:Multicast capture can be enabled via an XML configuration file using the StreamingMode option. Refreshing device settings will be enough to activate the changed StreamingMode option.

- Die Treiberinstanz kann so konfiguriert werden, dass sie als primäre oder als Listener-Instanz verwendet wird. Die primäre Instanz kann IP-Geräteeinstellungen ändern und zusätzliche Funktionen nutzen. Listener-Instanzen können Video- und Audioströme per Multicast empfangen und digitale E/A-Funktionen nutzen.
- Der Benutzer sollte sicherstellen, dass nur ein Rekorder die Einstellungen von UDP IP-Geräten ändert. Andere Rekorder, die dieses Gerät verwenden, sollten sich im Zuhörermodus befinden.
- Der Multicast-Stream verwendet dieselben Einstellungen, bis er neu gestartet wird, auch wenn die Stream-Einstellungen geändert werden. Die Änderung des Stream-Status (Starten oder Stoppen) erfordert 6-10 Sekunden. Die Anwendung von Stream-Einstellungen dauert also 30-60 Sekunden.
- Bitte beachten Sie, dass der Treiber nur den Standardadapter für Multicast-Streaming verwendet. Daher funktioniert Multicast möglicherweise nicht korrekt, wenn Ihr PC mehr als eine Netzwerkkarte hat. Bitte wenden Sie sich an den Kundendienst, wenn Sie ein Problem mit der Multicast-Konfiguration haben.

Einschränkungen der Zeitsynchronisationsfunktionen:

- Die Änderung der Zeitzone hat bis zum Neustart keine Auswirkungen auf die Systemzeit. Um die korrekte Zeit anzuwenden, kann der Treiber die Kamera nach der Änderung der Zeitzoneneinstellung neu starten.
- Die Änderung der Zeitzone hat bis zum Neustart keine Auswirkungen auf die Systemzeit. Um die korrekte Zeit anzuwenden, kann der Treiber die Kamera nach der Änderung der Zeitzoneneinstellung neu starten.

Einschränkungen der Edge-Storage-Funktionalität:

- Die Edge-Storage-Funktionalität wird nur für Kameras der IPX/IPN-Serie unterstützt, und zwar ab Firmware-Version 1.8.0.4
- Die Aufzeichnung auf der SD-Karte sollte manuell über die Weboberfläche der Kamera konfiguriert werden, bevor Sie diese Funktion in VMS nutzen.
- Die IPN/IPX-Kameras erlauben nur die Aufzeichnung eines H.264-Streams auf SD-Karte. Wenn Sie die Kodierung des für die Aufzeichnung verwendeten Profils ändern, wird die Speicherung von Videomaterial auf der SD-Karte deaktiviert.
- Die IPN/IPX-Kameras ermöglichen die Suche nach aufgezeichnetem Material nur nach Ereignissen. Dies ist eine Einschränkung des SDK der Kamera. Aufgrund dieser Einschränkung können Videos, die mit den Einstellungen für kontinuierliche Aufzeichnung aufgezeichnet wurden, nicht verarbeitet werden.

- Die maximale Ereignisdauer beträgt 65 Sekunden (5 Sekunden vor der Aufzeichnung und 60 Sekunden nach der Aufzeichnung). Es gibt keine Möglichkeit, die Aufzeichnung von längeren Zeitintervallen zu konfigurieren.

9.7.3.9 LGEIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle, um Videoströme und Eingangszustände in allen Komprimierungsmodi zu empfangen. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen DVMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Die Standard-Ports sind 80 und 81,
- **RTSP**: Hafen 554,
- **UDP**: Es werden zwei sequentielle Ports pro Videostrom und zwei sequentielle Ports pro Metadatenstrom (Eingangszustände) in einem Portbereich von 3556 bis 4556 benötigt.

Wenn zum Beispiel 2 LG Electronics IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.9.1 Beschränkungen

Bei einigen LG Electronics-Geräten kann das Gerätemodell nicht empfangen werden. Bei diesen Kameras wird der Modellname als „LG Electronics IP-Kamera“ angezeigt.

Die Kamera LDW2010F-N sendet einen QCIF-Stream mit einer Auflösung von 160x112 anstelle von 176x112. Dies ist ein Merkmal der Kamera.

Die digitalen Ausgänge der LG Electronics-Geräte haben eine Besonderheit: Sie verfügen über eine Dauer-Option und können nicht über einen längeren Zeitraum geschlossen werden. Das Gerät öffnet den Ausgang automatisch, wenn die Zeitspanne abgelaufen ist.

Die SOAP-API unterstützt keine Befehle zum Umschalten von Fokus- und Blendenmodi zwischen automatischen und manuellen Werten. Wenn der Benutzer also die Blenden-/Fokuseinstellung in DVMS verwenden möchte, sollte er diesen Wert über die Weboberfläche auf manuell ändern.

9.7.3.10 NewActiIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für die Einstellung/Abruf der Parameter verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Standard-Port ist 80,
- **RTSP**: Anschluss 7070,

- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden in einem Portbereich von 3556 bis 5556 benötigt.

Die Datei NewActiIPCapture.xml wird zur Konfiguration verwendet:

1. Verhalten des Fahrers:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
2. Der Stream-Modus der Kamera und der Montagetyp (bei Fisheye-Kameras) erlauben eine Entschärfung der Kamera.

Mögliche Werte für Stream-Modi: SINGLE, DUAL, EPTZ, MD_PRESET, FISHEYE_VIEW

Mögliche Werte für Montagearten: WALL, CEILING

Die erste PTZ-Kanal-ID für ACTi-Videoserver:
Allgemeine und IP-Geräte-spezifische Konfiguration ist möglich
E.g:

```
<Device address="192.168.1.75" port="80">
<FirstPTZChannelID>2</FirstPTZChannelID>
</Device>
```

Für das Gerät 192.168.1.75:80 ist die erste PTZ-Kanal-ID die 2, die nächste (bei einem Mehrkanalgerät) die 3, usw.

9.7.3.10.1 Beschränkungen

- ACTi TCM-5311 kann den korrekten Stream nicht mehr senden, wenn die Hintergrundbeleuchtung abrupt geändert wird.
- ACTi MPEG4-Kameras benötigen eine Verzögerung zwischen der Einstellung der Parameter und dem Start des Streams (etwa 3 Sekunden).
- ACTi CAM-6510 arbeitet nicht korrekt mit 1 fps, daher ist dieser Wert für diese Kamera nicht verfügbar. Die ACTi CAM-6510 Kamera unterstützt keine Qualitätsänderung, daher ist die Qualität für alle Werte gleich.
- ACTi-Kameras haben unterschiedliche Bildraten für unterschiedliche Komprimierungsformate. Die Einstellungen werden automatisch auf den nächstgelegenen korrekten Wert umgerechnet.
- ACTi E96, B54, B55 und B56 Kameras unterstützen kein De-Warping auf der Kamera, daher hat die XML-Konfiguration keine Auswirkungen auf diese Modelle.
- ACD-Videoserver funktionieren nur mit einer PTZ-Kamera, die an jeden Kanal angeschlossen ist, mit einer Kamera-ID = 1. Der ACD2100 funktioniert beispielsweise nur mit einer Kamera, der ACD2200 mit vier

Kameras. ACD-Mehrkanalgeräte haben unterschiedliche RS485-Anschlüsse für PTZ-Kameraverbindungen, und alle Kamera-IDs müssen gleich 1 sein.

- Die tatsächliche Bildrate für ACTi-Kameras kann von den Einstellungen abweichen. Sie hängt von den Kameraeinstellungen (Objektivausgleich und Verschlusszeit) und der Beleuchtungsstärke ab.
- Videokameras unterstützen keine E/A-Funktionalität. Sie funktionieren in PAL, aber die Werkseinstellung ist NTSC. Nach Anwendung der Werkseinstellung funktioniert die Kamera nicht mehr.
- SED2100 arbeitet mit ACTi-Bibliotheken. SED2100 muss nach jeder Änderung der Parameter einen Neustart durchführen (dauert 30-60 Sekunden).
- Voreinstellungsnamen werden in einer XML-Datei gespeichert (keine Voreinstellungsverwaltung der Kamera)
- Für KCM kann die K2 Fischaugenkamera in zwei Video-Stream-Modi verwendet werden: EINZELN und EPTZ. Der Stream-Modus wird bei der Anmeldung der Kamera an DVMS erkannt, der Treiber behält diesen Modus bei. Um den Stream-Modus zu ändern, muss die Kamera aus dem DVMS entfernt werden, der Stream-Modus muss über die Weboberfläche der Kamera geändert werden, und dann kann die Kamera abonniert werden. Der Treiber stellt ihn automatisch für alle anderen KCM- und TCM-Serien im SINGLE-Video-Stream-Modus ein.
- Der ACTi-Treiber verwendet konstante Bitrateneinstellungen, die aus dem entsprechenden VMS-Qualitätswert skaliert werden:
    - CAM values: 256K, 384K, 500K, 750K, 1M, 1.5M, 2M, 2.5M, 3M
    - ACM values: 28K, 56K, 128K, 256K, 384K, 500K, 750K, 1M, 1.2M, 1.5M, 2M, 2.5M, 3M, UNLIMITED
    - TCM/KCM values: 28K, 56K, 128K, 256K, 384K, 500K, 750K, 1M, 1.2M, 1.5M, 2M, 2.5M, 3M, 3.5M, 4M, 4.5M, 5M, 5.5M, 6M, UNLIMITED
- So wird die VMS-Qualität 50% auf einen Bitratenwert von 1Mbit/sec skaliert. Die richtige DVMS-Qualität sollte so eingestellt werden, dass sie der erforderlichen Netzwerkbandbreite entspricht.
- ACTi-Videoserver haben kein internes PTZ-Protokoll; sie senden PTZ-Befehle im transparenten Modus an den COM-Port der Kamera zurück. Derzeit ist nur das PelcoD-Protokoll implementiert. Wenn eine analoge Kamera, die an einen ACTi-Videoserver angeschlossen ist, nicht mit PelcoD funktioniert, kann der Treiber nicht zur Steuerung der Kamera verwendet werden.
- Nicht alle Stream-Modi werden von den ACTi Fischaugenmodellen unterstützt. Der ACTi I51 unterstützt z. B. nur die Stream-Modi DUAL (Panorama), FISH_EYE und EPTZ. Andere Einstellungen haben keine Auswirkungen und werden im Stream-Modus verwendet, der an der Kamera eingestellt ist.
- Stream-Modus und Montageart sollten festgelegt werden, bevor die Kamera zu DVMS hinzugefügt wird. Um diese Werte zu ändern, sollte der Benutzer die Kamera aus DVMS entfernen, Änderungen in der Konfigurationsdatei vornehmen und die Kamera erneut zu DVMS hinzufügen.

- Mehrfaches Streaming für die Fischaugenkamera wird nur für diese Stream-Modi unterstützt:
    - DUAL - 2 Ströme
    - MD_PRESET - 2 Ströme in WALL Befestigungsart, 3 in CEILING
- Digitales PTZ funktioniert für die Fisheye-Kamera nur im EPTZ-Stream-Modus.
- Wenn die Auflösung oder der Stream-Modus geändert wurde, werden die Voreinstellungen für die Fisheye-Kamera ungültig; sie müssen aus DVMS entfernt und erneut zugewiesen werden.
- MPEG4 ist im DUAL-Stream-Modus deaktiviert, da es nur für den 1.
- Die Stream-Modi 6VGA und 4VGA werden nicht unterstützt.
- Die Stream-Modus-Einstellungen in der Datei NewActiIPCapture.xml gelten nur für die Fischaugen-Kameras. Die Einstellungen für den Stream-Modus anderer Kameras werden von der Kamera übernommen, wenn sie zu DVMS hinzugefügt wird. Wenn die Kamera den DUAL-Stream-Modus eingestellt hat, wird mehrfaches Streaming aktiviert, wenn SINGLE - nicht.
- Im DUAL-Stream-Modus muss die Bildrate in Stream 1 höher oder gleich hoch sein wie die in Stream 2. Andernfalls ist die Bildrate in Stream 1 auf die Bildrate in Stream 2 begrenzt. Beispiel: Die Einstellungen für die Bildrate in Stream 1 und Stream 2 sind 30 und 25. Die tatsächliche Bildrate in Stream 1 beträgt 25
- KCM/TCM-Kameras können keine Privatsphärenmasken für den zweiten Stream aktivieren. Daher werden Privatsphärenmasken nur für Single-Stream-Modi aktiviert (die Kamera sollte einen Single-Stream-Modus haben, bevor sie zu DVMS hinzugefügt wird). Bei KCM/TCM-Kameras gibt es ein allgemeines Problem im Zusammenhang mit Privatsphärenmasken und Auflösungen größer oder gleich 1920x1080: Die Privatsphärenmaske kann nur für den linken Teil des Bildschirms festgelegt werden (ACTi-Einschränkung).
- ACTi ACM-Kameras haben ein Problem mit den Privatsphärenmaskeneinstellungen. Die Position der Privatsphärenmaske ist nur bei maximaler Auflösung korrekt; bei kleineren Auflösungen kann die Position der Privatsphärenmaske von den Einstellungen abweichen.
- Die ACTi ACM-Serie kann Bewegungserkennung liefern, aber es gibt keine konfigurierbare MD auf der Webseite der Kamera. Für diese Modelle kann die „Rekorder- und Kamerahardware“ MD nicht verwendet werden.
- Multicast ist für ACTi CAM-Modelle nicht aktiviert. Alle diese Modelle arbeiten nur mit Unicast. Diese Kameras können nicht in mehreren DVMS-Instanzen verwendet werden!
- **Unicast mode**: Der Treiber ändert die Kameraeinstellungen entsprechend den DVMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über eine Unicast-Verbindung.
- **Multicast:Primary**: Der Treiber ändert die Kameraeinstellungen entsprechend den DVMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über eine Multicast-Verbindung.

- **Multicast:Listener**: Der Treiber ändert keine Kameraeinstellungen, sondern empfängt lediglich Audio- und Videodaten von der Kamera über eine Multicast-Verbindung.
- Wenn die Kamera in mehreren DVMS-Instanzen verwendet werden soll, sollte ein DVMS auf Multicast:Primary und die anderen auf Multicast:Listener eingestellt werden.
- Mehrere Multicast:Primary-Konfigurationen oder Multicast:Primary- und Unicast-Konfigurationen sind nicht zulässig; in anderen Fällen sollte die Kamera mit ständigen gleichzeitigen Einstellungsänderungen überlastet werden.
- Edge Storage wird nur für die DEBI-Serie ab Firmware 6.07.23 und höher unterstützt.
- Die Kamera ist mit UTC (GMT +00) synchronisiert, um Probleme mit der Ortszeit zu vermeiden.
- Der Modus RTP über RTSP funktioniert nicht mit den folgenden Kameraserien. Diese Kameras unterstützen diesen Modus nicht oder sind nicht vollständig getestet worden:
    - VIDO AMU-xxx
    - ACTI KCM-xxx
    - ACTI ACM-xxx

9.7.3.11 NewArecontIPCapture - Installation und Verwendung

Der Treiber für den H.264-Komprimierungsmodus verwendet RTSP/RTP/UDP/IP-Protokolle für den Videoempfang bei üblichen Bildraten. Das HTTP-Protokoll wird zum Einstellen/Abrufen von Parametern, zum Empfangen von MJPEG/H.264-Streams bei langsamen Bildraten der Kamera und zum kontinuierlichen Empfangen von MJPEG verwendet.

Wenn sich zwischen VMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream werden in einem Portbereich von 3554 bis 4556 benötigt.

Der Treiber kann mithilfe einer XML-Konfigurationsdatei konfiguriert werden, um die folgenden Parameter einzustellen:

- Innenbeleuchtungskompensationswert

Kanalspezifische Parameter:

- MaxFrameRate - maximale Bildrate bei voller Auflösung
- MaxFrameRateHalf - maximale Bildrate bei halber Auflösung

- RTP über RTSP-Transportprotokoll
- RTP-Blockgröße (falls für den jeweiligen Router erforderlich)
- BitrateMode (CBR, VBR oder Auto - die letzte Option weist den Treiber an, die Qualitätsänderung bei der Kamera zu überspringen)
- BitrateMin (Mindestbitrate für CBR)
- BirateMax (maximale Bitrate für CBR)
- KeyFrameIntervalMs (Intra-Frame-Intervall in ms, 0 - all intras)
- IndoorLightFrequency - Lichtfrequenz

9.7.3.11.1 Beschränkungen

Der Wert für die maximale Bildrate wird nach der „geheimen“ Formel von Arecont berechnet. Die tatsächliche Bildrate kann niedriger sein als angegeben - sie hängt von den Netzwerkbedingungen ab.

Einige Bildauflösungen können von den Einstellungen abweichen, z.B. 1600x1200 wird zu 1600x1184. Dies liegt daran, dass die Auflösung der Arecont-Kamera für den Vollmodus durch 32 und für den Halbmodus durch 64 teilbar sein muss.

Die maximale Auflösung von Arecont wird an der Kamera eingestellt. VMS verwendet sie und die Hälfte davon. Um die maximale Auflösung zu ändern, müssen Sie sie auf der Kamera ändern und dann eine Kamera zum VMS hinzufügen.

Arecont-Kameras haben nur zwei volle Bildauflösungen - die maximale Sensorauflösung und die Hälfte davon. Die anderen Auflösungen sind von der maximalen Auflösung abgeschnitten und werden im Treiber nicht verwendet.

AV8185 und AV8180 haben kein IO (die Angaben in der Dokumentation sind falsch).

AV3135 hat zwei Sensoren - Tag und Nacht. Beide arbeiten mit bestimmten Auflösungen. VMS zeigt Auflösungen für den Tagmodus an; die tatsächliche Bildauflösung kann von den Einstellungen abweichen.

Arecont-Kameras können die Bildauflösung dynamisch ändern. Die tatsächliche Bildauflösung kann von den Einstellungen abweichen.

DVMS unterstützt nur maximal 30 fps, so dass alle Arecont-Kameras diese Einschränkung haben (auch wenn sie mehr als 30 fps unterstützen).

Bei Arecont 4-Kanal-Kameras kann es Probleme geben, wenn H.264 + MJPEG verwendet wird. Es ist besser, ein Kompressionsformat für alle Kanäle zu verwenden.

9.7.3.12 NewAxisIPCapture - Installation und Verwendung

Der Treiber verwendet die Protokolle RTSP/HTTP/HTTPS/RTP/UDP/IP, um Audio- und Video-Multicast-Streams und H.264/MPEG-4-komprimierte Unicast-Streams zu empfangen. Das HTTP-Protokoll wird auch zum Einstellen/Abrufen von Parametern und zum Empfang von Audio- und JPEG-Videoströmen im Unicast-Modus verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP/HTTPS-Ports geöffnet sein geöffnet sein:

- **HTTP**: Der Standardport ist 80,
- **HTTPS**: Der Standardport ist 443,
- **RTSP**: Der Standardanschluss ist 554,
- **UDP**: Pro Videostream werden zwei sequentielle Ports im Portbereich 3556 bis 4556 benötigt. Wenn der Multicast-Modus aktiviert ist, sollten zwei zusätzliche sequentielle Ports pro Audio-/Videostream entsprechend der Gerätekonfiguration geöffnet werden.

Wenn beispielsweise 4 IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen. Die Ports 1024-1025 und 1028-1029 sollten zusätzlich zum Bereich 3556-4556 geöffnet werden, wenn das Gerät im Multicast-Modus verwendet wird und so konfiguriert ist, dass der Port 1024 für den Audiostrom und der Port 1028 für einen Videostrom verwendet wird.

Der Treiber kann mithilfe einer XML-Konfigurationsdatei konfiguriert werden, um die folgenden Funktionen zu aktivieren, wenn das Axis IP-Gerät diese Funktionen unterstützt:

- Multicast audio/video capture
- Axis Views

Wenn Sie Axis LPR verwenden und mehrere Netzwerkadapter haben, müssen Sie die richtige IP-Adresse (Adressen) in der Konfigurationsdatei festlegen.

9.7.3.12.1 Beschränkungen

Für die HTTPS (TLS)-Unterstützung müssen Sie das CA-Zertifikat auf dem PC-Zertifikatspeicher generieren und installieren und ein Zertifikat für jede Kamera mit Hilfe einer Anleitung von Axis generieren („HowTo. AXIS Device Manager. HTTPS certificate management“).

Der AXIS-Treiber unterstützt die Option „PTZ-Steuerungswarteschlange“ nicht. Wenn diese Option aktiviert ist, wird das AXIS Gerät als Nicht-PTZ-Gerät erkannt.

Die Privatzonen können um einige Pixel gegenüber dem in DVMS angewendeten Rechteck verschoben sein. Die Verschiebung hängt von der Bilddrehung und den Spiegeleinstellungen ab (bei einem normalen Bild nach rechts verschoben). Dies ist eine Funktion der Kamera-Firmware.

Wenn die Option „Seitenverhältniskorrektur“ auf dem Axis-Gerät aktiviert ist, kann die tatsächliche Bildauflösung von der in VMS abweichen. So beträgt die tatsächliche Auflösung beispielsweise 768x576 bei der Einstellung 704x576 oder 192x144 bei der Einstellung 176x144. Bitte deaktivieren Sie diese Option, wenn Ihr System keine Seitenverhältniskorrektur benötigt.

Wenn die Netzwerkverbindung unterbrochen wird, senden die Axis-Kameras der Serie P33 einige Sekunden Video und dann 5-10 Sekunden lang nichts mehr, nachdem die Verbindung wiederhergestellt wurde. Dieses Verhalten

wird durch die DHCP-Implementierung der Kamera verursacht. Bitte verwenden Sie eine statische IP-Adresse, um dieses Verhalten zu vermeiden.

Das IP-Gerät sollte wie folgt manuell konfiguriert werden, wenn Sie die Edge-Speicherfunktion verwenden möchten:

1. Es ist nicht möglich, die koordinierte Weltzeit (UTC) von der Kamera zu empfangen, daher sollte die Zeitzone auf „GMT+0:00“ eingestellt werden. Die Option Sommerzeit sollte ebenfalls ausgeschaltet werden.
2. Die Kameraereignisse sollten für die Videoaufzeichnung entsprechend den Benutzereinstellungen konfiguriert werden. Die Ereignisdauer sollte mindestens 3 Sekunden betragen.
3. Es wird empfohlen, die automatische SD-Reinigung zu verwenden, um den erforderlichen Speicherplatz für Videoaufnahmen zu erhalten.

Die Videoaufzeichnungen auf dem Speicher der Kamera können Lücken von bis zu 10-15 Sekunden enthalten. Dies ist eine Funktion der Kamera, verwenden Sie also bitte nicht die maximalen Einstellungen für die Videoaufzeichnung, um solche Lücken zu vermeiden.

Axis-Kameras mit mehreren Ansichten (z. B. M3007) können mithilfe der XML-Konfigurationsdatei für den Empfang von Videos aus einem bestimmten Stream konfiguriert werden. Unterschiedliche Ansichten haben unterschiedliche Fähigkeiten, so dass die Kamera erneut bei VMS angemeldet werden sollte, um die geänderten StreamConfiguration-Optionen zu nutzen.

Die Datenschutzzonen-Funktionalität kann verwendet werden, wenn der Aufzeichnungskanal die Fischaugenansicht „Übersicht“ verwendet.

Andere Ansichten unterstützen die Privacy-Masking-Funktionalität nicht, da diese Ansichten Teil der Ansicht „Übersicht“ sind.

9.7.3.12.2 Einschränkungen bei der Multicast-Erfassung

- Axis IP-Geräte unterstützen Multicast-Capture mit der Funktion Stream Profiles (Geräte mit Firmware-Version 5.0 oder höher) und können über eine XML-Datei konfiguriert werden. Ältere Geräte verwenden immer Unicast-Streaming.
- Die Unterstützung von Stream Profiles kann über die Weboberfläche überprüft werden: der Abschnitt „Video & Audio >> Stream Profiles“ sollte verfügbar sein. Der Benutzer kann ein beliebiges vorhandenes Profil für die Multicast-Streaming-Konfiguration verwenden oder das System ein neues Profil erstellen lassen. Weitere Einzelheiten finden Sie im Abschnitt „MulticastProfiles“ in der XML-Konfigurationsdatei.
- Bitte verwenden Sie nicht dasselbe Stream-Profil für verschiedene Streams - dies kann zu Konflikten bei der Anwendung der Videoeinstellungen führen.
- Die Multicast-Erfassung kann über die XML-Konfigurationsdatei mit der Option StreamingMode aktiviert werden. Diese Option wird beim Start des Streams gelesen, so dass eine Aktualisierung der Geräteeinstellungen ausreicht, um die geänderte StreamingMode-Option zu verwenden. Bitte beachten Sie,

dass DVMS seit Version 7.4.1 über eine Optimierung für den Kanalneustart verfügt, so dass in diesem Fall eine der Videooptionen für jede Kamera geändert werden muss, um den Stream neu zu starten.

- Die Treiberinstanz kann so konfiguriert werden, dass sie als primäre Instanz oder als Listener verwendet wird. Die primäre Instanz ist in der Lage, IP-Geräteeinstellungen zu ändern und zusätzliche Funktionen zu nutzen. Listener-Instanzen können Video- und Audioströme per Multicast empfangen und ermöglichen die Nutzung der digitalen E/A-Funktionalität.
- Der Listener-Recorder ändert keine Konfiguration auf der Kameraseite. Wenn z. B. kein konfiguriertes Profil auf der Kamera vorhanden ist, wird es nicht erstellt, und der Treiber kann das Video nicht empfangen. Die Kamera sollte zum primären Rekorder hinzugefügt werden, bevor sie in der Listener-Konfiguration verwendet wird.
- Die zusätzlichen Streams (Live und Remote) sind nur dann aktiv, wenn sie in Clients geöffnet sind. Um also die aktualisierten Einstellungen für das Multiple Streaming zu verwenden, müssen Sie diese Streams für den primären Rekorder starten (oder offen halten), nachdem die Stream-Einstellungen in DVMS geändert wurden. Andernfalls kann die Kamera die aktuellen Stream-Einstellungen nicht verwenden.
- Die Option Bewegungserkennung und -änderung in den Alarmfunktionen (CFiA/CRiA) kann im Multicast-Modus aufgrund der oben genannten Zeitüberschreitungsprobleme nicht verwendet werden.
- Benutzer sollten sicherstellen, dass nur ein Rekorder die Einstellungen von Axis IP-Geräten ändert. Andere Rekorder, die diese Kamera verwenden, sollten sich im Zuhörermodus befinden.
- Die Axis-Kameras unterstützen möglicherweise nicht mehr als einen Multicast-Stream, wenn die Kamera so konfiguriert ist, dass sie einen bestimmten Port für Multicasting verwendet (Einstellung „Video-Port“ ungleich Null in der Gruppe „Systemoptionen >> Netzwerk >> RTP“). Die Kamera gibt den Fehler RTSP 461 „Unsupported transport“ für den Start eines Streams zurück, wenn bereits ein Multicast-Stream gestartet ist. Bitte konfigurieren Sie die automatische Port-Auswahl (setzen Sie „Video port“ auf 0), um dieses Verhalten zu vermeiden.
- Es wird empfohlen, die IP-Adresse des Netzwerkadapters anzugeben, über den die Kamera angeschlossen ist, um Multicast-Streaming korrekt zu empfangen, falls mehr als ein Netzwerkadapter verfügbar ist.

Jedes Unicode-Zeichen wird als Symbolcode (z. B. %u0227) gespeichert und benötigt 6 Bytes. Daher kann die Länge des Unicode-Präpositionsnamens auf 11 statt auf 64 Symbole begrenzt sein.

Die Axis P1428-E Kamera unterstützt nur 2 4K (3840x2160) Streams zur gleichen Zeit. Bitte vermeiden Sie die Verwendung der 4K-Auflösung für alle Streams in der Mehrfach-Streaming-Funktion und minimieren Sie die Anzahl der Regeln, die die 4K-Auflösung für die Aufzeichnung auf der SD-Karte verwenden.

Der Treiber ermöglicht seit Version 2.5.5.0 den Wechsel zwischen den Modi „Aktiv“ und „Passiv“. Im Modus „Passiv“ ändert der Treiber keine videorelevanten Parameter, so dass in diesem Modus die folgenden Funktionen nicht funktionieren:

- Privatzonen konfigurieren

- Optionen im Alarm ändern (z. B. CFiA/CRiA-Funktionen)

Wenn die Kamera Videoparameter über RTSP- oder HTTP-Stream-URI akzeptiert, startet der Treiber den Stream ohne diese Parameter. Mit anderen Worten, es werden die über die Webschnittstelle vorgenommenen Stream-Einstellungen verwendet.

Die Anwendung von Privatsphärenmasken kann sehr lange dauern (die Erstellung jeder Zone kann bis zu einer Sekunde dauern), was den Streamstart verlangsamen kann. Um das Abonnieren von Videos zu beschleunigen, wendet der Treiber Datenschutzmasken nach dem Start des Videostreams an.

Die Treiberversionen vor 2.5.7.0 haben ein Problem mit der Erstellung von Privatsphärenmasken für Geräte mit mehreren Sensoren. Der Treiber verwendete immer die Vorlage für den ersten Kanal, so dass die Privatzonen möglicherweise falsch angezeigt wurden (z. B. auf dem falschen Kanal).

Bitte entfernen Sie die Privatzonen manuell über das Web-Interface oder setzen Sie das Gerät einfach auf die Werkseinstellungen zurück, falls Sie auf ein solches Verhalten stoßen sollten. Danach erstellt der Treiber beim nächsten Start des Videokanals Privacy Masks mit den richtigen Vorlagen.

Die Axis Zipstream-Technologie (<http://www.axis.com/global/en/technologies/zipstream)> kann mit dem Treiber verwendet werden. Der Treiber hat keine Option zur Konfiguration dieser Funktion, so dass sie manuell über das Web-Interface aktiviert werden sollte.

Bitte beachten Sie dies:

- Die über die Webschnittstelle vorgenommenen Änderungen der Videoeinstellungen (einschließlich der Axis Zipstream-Optionen) wirken sich auf die nach den Änderungen gestarteten Videostreams aus. Daher ist ein Neustart des Videostreams erforderlich, um die aktualisierten Einstellungen zu übernehmen.
- Die VMS-Software muss ein Intraframe pro Sekunde empfangen, um die Nachbearbeitung des Videostroms (VCA, Bewegungserkennung usw.) durchzuführen. Die Verwendung der Option „Dynamic GOP“ kann zu Problemen bei der Nachbearbeitung führen, daher wird die Verwendung dieser Option nicht empfohlen.The Windows XP is not supported since driver version 2.5.0.0

Die neuen Axis-Kameras (Firmware 5.50 und neuer) verwenden eine neue API für die Bewegungserkennung, die derzeit nicht vom Treiber unterstützt wird. Die VMD-Funktion wird für diese Kameras deaktiviert, bis die neue API-Unterstützung zum Treiber hinzugefügt wird.

Die native Axis-Kennzeichenerkennungsanwendung verwendet HTTP-POST-Anfragen zum Senden von ANPR-Daten. Daher startet der Treiber den HTTP-Server, um diese HTTP-POST-Nachrichten zu empfangen. Wenn der PC mehr als einen Netzwerkadapter hat, müssen Sie die korrekte IP-Adresse des Netzwerkadapters, der für die Kommunikation mit der Kamera verwendet wird, in der XML-Datei des Treibers im Parameter AxisANPR/NetworkInterface angeben. In anderen Fällen sendet die Kamera keine ANPR-Daten an den PC. Wenn Failover verwendet wird, müssen beide Adressen eingestellt werden - Hauptserver und Failover.

Axis hat die date.cgi API in die time.cgi API geändert, um die Zeit von der Kamera abzurufen oder zu setzen. Aber diese neue time.cgi API arbeitet langsam, so dass der Treiber die Zeit von der Kamera mit einer gewissen Verzögerung erhält. Außerdem hat time.cgi immer noch keine Milisekunden, so dass diese Zeitsynchronisation

nicht präzise ist. Der Treiber versucht, die Zeitdifferenz zwischen Kamera und PC mit Recorder zu berechnen, aber diese Berechnung ist nicht präzise genug. Diese Berechnung kann in der Konfigurationsdatei abgeschaltet werden, wenn die Zeit außerhalb von VMS synchronisiert wird.

Axis 360-Kameras können das De-Warping intern durchführen und es besteht die Möglichkeit, de-warped Ansichten zu verwenden als:

- streams (aufzeichnung, live oder remote), die im abschnitt ViewAreaConfiguration konfiguriert werden können
- kanäle, die im abschnitt EnableViewModes konfiguriert werden können

9.7.3.13 NewBoschIPCapture - Installation und Verwendung

Wenn sich zwischen VMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP- oder HTTPS-Ports geöffnet sein:HTTP: default port is 80,

- **HTTPS**: Der Standard-Port ist 443,
- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Pro Video-/Audio-Stream sind zwei aufeinanderfolgende Ports in einem Portbereich von 3556 bis 4556 erforderlich.

Wenn beispielsweise 4 IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Für den MPEG-4-Videostream-Empfang verwendet der Treiber die Bosch RCP+ SDK-Bibliothek. Er öffnet beliebige UDP-Ports für den Empfang von Videodaten. Der Treiber kann mithilfe einer XML-Konfigurationsdatei konfiguriert werden, um die folgenden Parameter für die Bosch IP-Geräte festzulegen:

- PTZ protocol (PelcoD, OSRD, BiCom)
- Fish-eye video channel (only one can be used)
- Jpeg stream (Recording, Live or Remote, default Remote)
- Edge storage functionality support
- Time sync (enabled / disabled)
- Control mode (active/passive)
- Transport
- Key frame interval
- Video loss check (enabled / disabled)

9.7.3.13.1 Einschränkungen

Für alle Bosch-Geräte sollten ein Benutzer und ein Passwort festgelegt sein. Andernfalls erkennen die Treiber die Kamera nicht (das Passwort sollte nicht leer sein).

Der Systemmanager kann den Treiber für ältere Versionen mit abonnierten Bosch Kameras ab VMS 7.0 auf 1.3.0.0 aktualisieren. Bei älteren VMS-Versionen sollten die Kameras aus DVMS entfernt und nach der Treiberaktualisierung wieder hinzugefügt werden.

Wenn die Kamera ohne Audiokanäle hinzugefügt wurde, sollte die Kamera auch entfernt und erneut zu DVMS hinzugefügt werden, um sie zu aktivieren.

Der Treiber entfernt oder ändert den alten BoschIPCapture-Treiber nicht, sondern verwendet die rcpp.dll wie der alte Treiber.

Um den Treiber zu installieren, sollten also keine Bosch-Kameras angeschlossen sein. Andernfalls wird die Installation des Treibers fehlschlagen.

Für NTSC-Kameras, die an die Video-Jet-Server-Serie für den MPEG-4-Codec angeschlossen sind, beträgt die maximale Auflösung 352x240 (CIF). Die D1-Auflösung funktioniert nicht, daher wird die CIF-Auflösung anstelle von D1 angezeigt.

Eine Kombination von NTSC- und PAL-Kameras, die an einen Video Jet-Server angeschlossen sind, ist nicht zulässig.

Die tatsächliche Framerate für den MJPEG-Videokanal kann niedriger sein als die in den Einstellungen angegebenen Werte.

Die Qualitätseinstellung im VMS verwendet den Bitratenwert der Kamera oder des Videoservers. Daher kann die tatsächliche Bildqualität bei unterschiedlichen Werten gleich sein (wenn das Bild die angegebenen Bitraten durchlaufen kann).

Bosch PTZ-Kameras verwenden das OSRD-Protokoll zur Steuerung der Kamera. Dieses Protokoll lässt keine Änderung der Blenden-/Fokussiergeschwindigkeit zu. Daher können Blende und Fokus mit einem vordefinierten Geschwindigkeitswert ausgeführt werden. Die Geschwindigkeitswerte können über das Web-Interface eingestellt werden. Diese Einstellungen für die VG4 AutoDome Kamera finden Sie hier: Einstellungen > Erweiterter Modus > Kamera > Objektiv > Einstellungsgruppe 1

Das OSRD-Protokoll erlaubt es nicht, Voreinstellungen zu löschen. Auch die VG4-Kamera erlaubt es nicht, eine bestehende Präposition ohne Bestätigung zu überschreiben. Die Kamera zeigt die Frage „Overwrite current scene?“ als OSD-Menü mit den Tasten [Yes] und [No] an.

Die Änderung von Fokus/Blende wird zur Bestätigung der Auswahl verwendet. Der Treiber sendet den Iris-Befehl nach dem Speichern der Voreinstellung, damit der Benutzer die Überschreibung der Voreinstellung nicht manuell bestätigen muss. Dieser Algorithmus hat ein Problem: Wenn der Präpositions-Slot leer ist (noch nicht gespeichert), wird der Text für die Irisänderung angezeigt.

Bosch Videoserver geben PTZ-Befehle an Kameras weiter, die über den seriellen Anschluss angeschlossen sind. Es gibt keine Möglichkeit, die Kennung der Kamera über die Standard-Serveroptionen zu konfigurieren. Angeschlossene Kameras müssen daher korrekt konfiguriert sein (Hardware-Einstellungen der Kamera), um die PTZ-Steuerung zu ermöglichen:

- Das PTZ-Protokoll sollte Pelco-D sein.
- Die Kennung der PTZ-Kamera sollte mit der Nummer des Videokanals übereinstimmen. Bei einer Kamera, die an den zweiten Videoeingang angeschlossen ist, sollte die Kamera-ID beispielsweise auf 2 gesetzt werden.

Die anderen Einstellungen des seriellen Ports sollten mit denen des Servers übereinstimmen (Baudrate, Paritätsbit, Stoppbit usw.).

Bosch Videoserver haben keine interne PTZ-Funktionalität. Es werden nur Befehle an die seriellen Anschlüsse mit angeschlossenen Kameras weitergeleitet. Der Treiber kann also nicht erkennen, welche Funktion an der Kamera am seriellen Anschluss angeschlossen ist und ob es sich um eine PTZ-Kamera handelt.

Aufgrund dieser Funktion werden alle Server-Videokanäle als PTZ angezeigt.

NBC255 und NVC255 haben VGA- und QVGA-Auflösungen. DVMS zeigt stattdessen D1 und CIF an. (Diese Modelle können nicht über die Geräteeigenschaften erkannt werden)

Das Mehrfach-Streaming erfolgt entsprechend den Fähigkeiten der Encoder.

Jeder Videokanal verfügt über zwei Encoder mit der Anzahl der unterstützten Auflösungen, so dass nicht alle Auflösungen für Aufnahme- und Live-Streams verfügbar sind.

Einige Auflösungen werden nur durch spezielle Kombinationen auf dem ersten und zweiten Encoder unterstützt, so dass die Auflösung des Live-Streams von den Einstellungen abweichen kann, wenn sie nicht mit der aktuellen Aufnahmeauflösung eingestellt werden kann.

Der Remote-Stream ist MJPEG; er verfügt über alle verfügbaren Auflösungen.

9.7.3.13.1.1 Einschränkungen beim Streaming

- Um die H.264-Auflösung und -Framerate für den sekundären Stream zu ändern, muss der Modus „Stream 1 kopieren“ in der Weboberfläche deaktiviert werden (Einstellungen -> Erweiterter Modus -> Kamera -> Encoder-Streams -> Stream 2 -> Die Eigenschaft „Stream 1 kopieren“ gilt NICHT für „Stream 2“);
- Es ist nicht möglich, mehrere Auflösungen anzuwenden (jeder Videokanal verfügt über zwei Encoder mit unterschiedlichen unterstützten Auflösungen);
- Der Remote-Stream ist MJPEG mit allen verfügbaren Auflösungen.
- MJPEG im Mehrfach-Streaming-Modus funktioniert nicht bei alten Serien mit Firmware 4.x
- Die Bewegungserkennung für PTZ-Kameras muss auf der Webseite der Kamera nach jeder Kamerabewegung konfiguriert werden (Einschränkung von Bosch).

- Privatzonen für PTZ-Kameras werden nicht unterstützt.
- Kameras, die über einen COM-Anschluss verfügen, werden in DVMS als PTZ-Kameras angezeigt. Sie können an die PTZ-Plattform angeschlossen werden und PTZ wird funktionieren.
- Der Treiber synchronisiert die Zeit des PCs mit der Kamera unter Verwendung der UTC-Zeit (GMT+00:00) für die Edge-Storage-Funktion. Edge-Storage wird nicht korrekt funktionieren, wenn die Zeit auf eine andere geändert wird.
- Die Edge-Storage-Funktionalität funktioniert nur bei Netzwerkausfällen zwischen Kamera und VMS.

Wenn VMS neu gestartet oder der Treiber geschlossen wurde, empfängt DVMS keine aufgezeichneten Videos von der Kamera.

Außerdem sollte die Aufzeichnung auf der Kamera konfiguriert sein, um die Edge-Storage-Funktionalität in VMS zu nutzen.

9.7.3.13.1.2 Einschränkungen bei der Multicast-Erfassung

- Die Treiberinstanz kann so konfiguriert werden, dass sie als aktive oder passive Instanz verwendet wird. Die aktive Instanz kann die IP-Geräteeinstellungen ändern und zusätzliche Funktionen nutzen. Passive Instanzen können Video- und Audioströme per Multicast empfangen und ermöglichen die Nutzung digitaler E/A-Funktionen.
- Die Passivfunktion ändert die folgenden Kameraeinstellungen nicht:
    - Codec
    - Quality
    - Resolution
    - Framerate

Die Kamera sollte dem aktiven Rekorder hinzugefügt werden, bevor sie in der passiven Konfiguration verwendet wird.

Der Benutzer sollte sicherstellen, dass nur ein Rekorder die Einstellungen der Kamera ändert. Andere Rekorder, die diese Kamera verwenden, sollten sich im passiven Modus befinden.

Wenn mehr als ein Netzwerkadapter vorhanden ist, muss die IP-Adresse des Netzwerkadapters angegeben werden, über den die Kamera angeschlossen ist, um Multicast-Streaming korrekt zu empfangen. Der in Windows als Standard markierte Netzwerkadapter wird verwendet, wenn keine Option konfiguriert ist. Für den Audiokanal sollte der Netzwerkadapter (falls mehrere Netzwerkadapter im PC verwendet werden) in der XML-Datei festgelegt werden, die dynamische Benutzeroberfläche wird nur für den Videokanal verwendet.

Die Zeitsynchronisierung ist für den passiven Speicher deaktiviert und der Edge-Speicher funktioniert möglicherweise nicht richtig.

Die Verwendung sollte die Zeitsynchronisation für den PC mit dem Aktiv-Modus-Recorder und den PC mit dem Passiv-Modus-Recorder gewährleisten.

Alte Bosch-Serien mit Firmware 4.x haben die folgende Einschränkung:

Der HTTPS-Modus funktioniert nicht

MJPEG im Multicast-Modus funktioniert nicht (nur JPEG-Anfragen über HTTP)

Privacy Zones für Firmware 6.22 werden nicht unterstützt.

Alte Bosch-Serien (wie Gen4) führen manchmal „Auto Bounding“ durch. Während dieses Prozesses ist der Stream von der Kamera nicht flüssig.

Im passiven Modus sollten alte Kameras mit MPEG4-Unterstützung auf das richtige Kompressionsformat eingestellt werden, sonst wird „Kein Signal“ angezeigt.

Die Aufzeichnung im Edge-Storage sollte im Web-Interface der Kamera auf den 1.

Die Bosch IP-Geräte geben möglicherweise keine Informationen über Audiointervalle zurück, die über RCP+-Anfragen auf dem Speicher des Geräts aufgezeichnet wurden (durch num = 90 + Kanal-ID). Dies führt dazu, dass die Audio-Edge-Funktionalität nicht korrekt funktioniert. Das Problem wurde den Bosch-Technikern gemeldet (am 20/Nov/2019), aber es gibt noch keine Lösung.

Nicht alle Bosch-Kameras können Bewegung erkennen, daher sollte auf der Webseite der Kamera geprüft werden, ob sie Bewegungserkennung unterstützt oder nicht.

9.7.3.13.1.3 So verwenden Sie die Kamera im gesicherten Modus

1. Installieren Sie ein Zertifikat auf der Kamera und dem PC mit Rekorder
2. Stellen Sie den RTP-über-HTTP-Streaming-Modus in den Kameraeinstellungen im Systemmanager ein;
3. Stellen Sie die korrekten Anmeldedaten für die Kamera ein (für das Senden von Audio an die Kamera, wenn dies nicht erforderlich ist - es können beliebige Anmeldedaten verwendet werden, die Authentifizierung erfolgt über ein Zertifikat); Audio an die Kamera ist nicht gesichert, daher sind korrekte Anmeldedaten erforderlich, um zu funktionieren.Bosch-Kameras mit H.264- und H.265-Unterstützung sollten vor dem Hinzufügen zu DVMS auf den erforderlichen Codec eingestellt werden, da einige Kameras für jeden Codec eine andere Liste der unterstützten Auflösungen / Frameraten haben.

Die von der Kamera unterstützten Auflösungen hängen vom aktuell eingestellten Codec (H.264 / H.265) ab. Die Kamera wird also mit dem aktuell eingestellten Codec hinzugefügt, DVMS wird diesen während des Hinzufügens der Kamera nicht ändern.

Die Videoverlustprüfung wird nur für Encoder mit analogen Kameras verwendet, um zu erkennen, ob die Kamera funktioniert oder nicht. Sie sollte nicht für andere Bosch Geräte verwendet werden.

Wenn der Audiocodec geändert wurde, muss die SD-Karte formatiert werden, da der Treiber versucht, den Ton mit den aktuellen Einstellungen zu empfangen. Wenn für die Kamera AAC eingestellt ist, die Aufzeichnung aber für G711 durchgeführt wurde, werden Edge-Audiodaten nicht korrekt empfangen.

Beim Streaming mit mehreren Kanälen sollten alle Kanäle denselben Codec (H.264 oder H.265) haben, da Bosch-Kameras nicht beide gleichzeitig streamen können.

Bosch Geräte verarbeiten den RTSP PAUSE-Befehl nicht korrekt (der Stream wird danach weiter gesendet).

Daher verwenden wir RTSP TEARDOWN, um den Stream anzuhalten, wenn keine Bewegung stattfindet (wenn kamerabasiertes MD verwendet wird).

9.7.3.14 NewIQEyeIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Empfang von H.264-komprimierten Video- und Audioströmen. Das HTTP-Protokoll wird für das Einstellen/Abrufen von Parametern und den kontinuierlichen Empfang von MJPEG-Streams verwendet.

Wenn sich eine Firewall zwischen DVMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Audio-/Videostream werden in einem Portbereich von 3554 bis 4556 benötigt.

9.7.3.14.1 Beschränkungen

IQEye-Kameras haben eine Auflösung und mehrere beschnittene Auflösungen. Gekürzte Auflösungen werden im Treiber nicht verwendet. Der Treiber verwendet nur den Downsampling-Prozess, um die Bildgröße zu ändern (Größe / 2, Größe / 4 und Größe / 8). Downsampling ist für Kameras aktiviert, die es unterstützen (Kameras IQ73xx, IQ04xx, IQD4xx, IQ54xx unterstützen es nicht).

Die IQ712-Kamera hat eine Beschränkung für maximale fps für MJPEG - 15 fps.

IQEye-Kameras (außer IQ73xx) haben nur eine Auflösung für H264 ñ 640x480. Die anderen können nur für MJPEG verwendet werden.

Der H.264-Codec unterstützt für alle Kameras nur die Werte 5, 10, 15 und 30 für die Bildrate. Andere Werte werden nur für MJPEG verwendet, sie werden auf die oben aufgeführten Werte skaliert, wenn der H.264-Codec aktiv ist.

Für IQA25S-Kamera für MJPEG-Codec 2560x1920 und 1280x960 Auflösungen unterstützen maximale fps Wert 7, für 640x480 und 320x240 Auflösungen - nur 10 fps max.

Für IQA25S Kamera für JPEG-Codec Auflösung max /2 sollte auf 10 fps zu arbeiten, aber es funktioniert, wie es ist - max fps ist 7, wenn höher angegeben - es 5 oder 4 fps gesetzt, ist dies ein Problem der Firmware.

Der Treiber unterstützt nur den Empfang von G.711-Audiostreams. AAC-Codec wird im Moment nicht unterstützt.

9.7.3.15 NewMobotixIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber das HTTP-Protokoll für den Videoempfang und für die Einstellung/Rücksetzung von Parametern.

Wenn sich eine Firewall zwischen DVMS und den Kameras befindet, müssen die folgenden Ports geöffnet werden: HTTP: Standard-Port ist 80.

9.7.3.15.1 Beschränkungen

Die realen FPS sind durch die Auflösungseinstellungen (Kamerafunktion) begrenzt: höhere Auflösungen haben niedrigere reale FPS-Werte. Bei einer Auflösung von 800x600 beträgt die maximale FPS beispielsweise 9 für den MJPEG-Codec.

Die Audiodaten können gemäß der HTTP-API-Dokumentation als Teil des MxPEG-Rahmens empfangen werden. Daher ist der Audiostrom für MJPEG-Streams nicht verfügbar.

Der Stream-Modus wurde von „schnell“ auf manuell geändert - diese Einstellung kann im Web-Interface geändert werden.

9.7.3.16 NewPanasonicIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber die Protokolle RTSP/RTP/UDP für den Videoempfang und HTTP/HTTPS für die Einstellung der Parameter und für die PTZ-Funktionalität.

Im H.264/MPEG4-Komprimierungsmodus verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Einstellen/Abrufen von Parametern und den kontinuierlichen Empfang von MJPEG-Streams verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Die Datei NewPanasonicIPCapture.xml wird zur Konfiguration verwendet:

- Verhalten des Fahrers:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
- Priorität der Übertragung:
    - Bitrate

- Framerate
- Beste Leistung
- Erweitertes VBR
- VBR

Minimale Bitrate (nur für den Best Effort Modus)

9.7.3.17 NewSamsungIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. HTTP/HTTPS-Protokolle werden für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **HTTPS**: Der Standard-Port ist 443,
- **RTSP**: Hafen 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Beispiel: Wenn ein VMS über 4 Samsung IP-Kameras verfügt, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Die Datei NewSamsungIPCapture.xml wird verwendet für:

1. Konfiguration des Fahrerverhaltens:
    - Unicast
    - Multicast:Primary
    - Multicast:Listener
2. Einstellungen der Videokanäle:
    - Videokanal-Protokoll (RTP over UDP, RTP over RTSP)
    - Bitrate-Modus (CBR/VBR)

9.7.3.17.1 Beschränkungen

Die Fähigkeiten von Samsung-Kameras können für frühere Firmware-Versionen nicht abgerufen werden. Alle Kamerafunktionen (mit Ausnahme des Kameramodellnamens) für diese Kameras sind im Treiber fest einprogrammiert. Daher sollten alle Kameras auf die neueste Firmware-Version aktualisiert werden.

Samsung-Kameras unterstützen die Konfiguration von Eingängen über CGI-Befehle nicht. Der Eingang ist standardmäßig als „deaktiviert“ konfiguriert. Bitte setzen Sie die Eingangskonfiguration im Web-Interface auf „NO“

(d. h. „Normal Open“), bevor Sie die Kamera zum VMS hinzufügen.Samsung camera frame rates may differ from settings (+/- 3 fps)

Treiber speichert Voreinstellungsnamen in XML-Datei (Unicode-Namen werden unterstützt)

Die Samsung PTZ-Geräte unterstützen keinen Geschwindigkeitsparameter für den Befehl „move to preset“. Daher ist die Geschwindigkeit für die Bewegung zum Preset immer gleich.

Bei Samsung-Kameras wird die Konfiguration jeder Privatzone durch eine separate Anforderung (Hinzufügen/Entfernen) vorgenommen. Um die Position der Zone zu ändern, müssen wir die vorherige Konfiguration entfernen und eine neue Position durch verschiedene Anfragen hinzufügen. Jede Anforderung zum Hinzufügen/Entfernen wird von der Kamera innerhalb von 0,6 bis 0,8 Sekunden verarbeitet. Die Aktualisierung der Positionen von 10 Privatzonen kann also bis zu 16 Sekunden dauern.

Zeitzonen für eingestellte Kameras können bei der Zeitsynchronisation falsch eingestellt sein.

Das IP-Gerät sollte vom Benutzer auf folgende Weise manuell konfiguriert werden, wenn der Benutzer die Edge-Speicherfunktion verwenden möchte:

1. Es gibt keine Möglichkeit zu wissen, ob gerade eine Datei geschrieben wird. Stellen Sie daher die Option „Post-Alarm-Dauer“ nicht auf eine lange Zeitspanne ein, da dies dazu führen kann, dass der Treiber dieses Intervall überspringt.
2. Es wird empfohlen, die Option „1 fps zwangsweise aufnehmen“ zu deaktivieren. Diese Option kann jedoch bei einigen Einstellungen des aufgezeichneten Profils deaktiviert sein (Einzelheiten finden Sie im Handbuch der Kamera). Sie können in diesem Fall ein separates Videoprofil für die Aufnahme von Videos für HD- und Full-HD-Kameras verwenden.
3. Es wird empfohlen, die automatische SD-Reinigung zu verwenden, um den erforderlichen Speicherplatz für Videoaufnahmen zu erhalten.

Samsung-Kameras der Serie 7000 haben ein Problem mit der Aufzeichnung von Videodaten nach Ereignissen. Die Kamera zeichnet nichts auf, obwohl Ereignisse, die für die Aufzeichnung konfiguriert wurden, signalisiert werden. Die Kamera beginnt mit der Aufzeichnung von Videos nach einem Neustart oder manchmal nach dem Zurücksetzen der Kameraeinstellungen auf die Werkseinstellungen. Dies ist ein Kameraproblem.

Alte Samsung-Kameramodelle wie SNP-570 und SND-460, die das STW SDK verwenden (STW-Kameras in den nächsten Hinweisen) und deren Firmware-Version älter als 1.3.5 ist, unterstützen das Abrufen der Kameraeigenschaften nicht. Diese Kameras werden als „Samsung IP-Kamera“ erkannt und funktionieren nur im PAL-Videomodus.

Samsung STW-Kameras unterstützen den Befehl „Ausgang ausschalten“ nicht. Die Ausgänge werden von der Kamera automatisch gemäß den Ausgabeeinstellungen im Web-Interface ausgeschaltet.

Samsung STW-Kameras senden MPEG-4-Streams mit 12,5 FPS für die Einstellungen 10 und 15 FPS.

Samsung STW-Kameras verringern den Videoqualitätswert für MPEG-4-Codec automatisch während der Bewegung. Dies ist eine Funktion der Kamera (laut Informationen von Samsung Techwin Support).

Die Bildrate schwankt im MPEG-4-Komprimierungsmodus für Samsung STW-Kameras. Dies wird durch den Empfang von RTP-Paketen mit falscher Sequenznummer verursacht. Dies ist ein Kameraproblem.

Ein Videostream von Samsung STW-Kameras weist FPS-Schwankungen auf, wenn die Belichtungseinstellungen für die Kamera ungültig sind. Um die Einstellungen zu korrigieren, verwenden Sie die Schaltfläche „Kamera-Setup“ auf der Seite Live-Ansicht im Web-Interface.

Samsung STW-Kameras gehen in einen deaktivierten Zustand über (HTTP-Antworten mit Statuscode 500 für alle Anfragen), nachdem die Verbindung für kurze Zeit unterbrochen und dann wiederhergestellt wurde. Das Problem wird mit einer Wahrscheinlichkeit von 30 % nur für den MJPEG-Codec reproduziert.

Die FPS-Einstellungen werden für MJPEG-Videostreams nicht korrekt angewendet. Dieses Kameraproblem tritt bei Samsung STW-Kameras mit Firmware-Version 1.3.5 oder früher auf. Daher können die tatsächlichen FPS für den MJPEG-Videostream niedriger sein als erforderlich.

Der MJPEG-Stream stoppt nach einer langen Betriebszeit (z. B. bei Tests über Nacht). Dies liegt daran, dass die Kamera HTTP-Antworten mit dem Statuscode 500 für alle Anfragen zurückgibt. In diesem Fall sollte die Kamera manuell neu gebootet werden. Dieses Problem tritt tatsächlich bei Samsung STW-Kameras auf.

Die SNP-1000A-Kamera sendet einen MJPEG-Stream mit 8-9 FPS bei 10 FPS und D1-Auflösungseinstellungen. Dies ist ein Firmware-Problem.

Die SNP-1000A-Kamera verarbeitet keine HTTP-Anfragen mehr, nachdem die Netzwerkverbindung unterbrochen und wiederhergestellt wurde (z. B. nach „Kein Signal“ während 2 Minuten). Dies liegt daran, dass die Kamera HTTP-Antworten mit dem Statuscode 403 für alle Anfragen zurückgibt. In diesem Fall sollte die Kamera manuell neu gebootet werden.

SNP-1000A- und SNC-550-Kameras unterstützen keine MPEG-4-RTP-Dienste. Für diese Kameras ist nur MJPEG-Videostream verfügbar.

Die SNP-1000A-Kamera schwenkt zwischen 0 Grad und 350 Grad. Gradwerte zwischen 351 und 359 Grad sind nicht verfügbar - dies ist eine Funktion der Kamera.

Die SNP-1000A-Kamera unterstützt keine kontinuierlichen Bewegungsbefehle. Der Treiber implementiert eine Emulation des kontinuierlichen Bewegungsmechanismus. Dieser Mechanismus reduziert die folgenden Probleme:

- Kamerabewegungen werden diskret sein.
- Der MJPEG-Stream stoppt manchmal für ein paar Sekunden, wenn sich die Kamera mit höchster Geschwindigkeit bewegt. Wahrscheinlich ist die Kamera-Firmware nicht in der Lage, den Videostream und eine Vielzahl von Bewegungsbefehlen gleichzeitig zu verarbeiten.
- Die Kamera bewegt sich fälschlicherweise in der unteren Position, wenn sie versucht, nach unten zu fahren. Die Kamera kehrt die vertikale Skala um und bewegt sich nach oben, wenn der Befehl „nach unten bewegen“ empfangen wird und die Kamera die untere Position passiert. Der nächste Befehl „Abwärtsbewegung“ wird jedoch nicht invertiert und die Kamera bewegt sich wieder in die untere Position.

Die Speicherung der Vorposition funktioniert bei der SNP-1000A-Kamera mit der aktuellen Firmware-Version nicht. Eine Aktualisierung der Firmware ist erforderlich.

Die Kameras der Serie 7002 haben eine Begrenzung für die Anzahl der aktiven Profile. Die Anzahl der aktiven Videoströme ist auf 2 begrenzt, wenn jeder von ihnen eine Auflösung von 1024x768 oder mehr verwendet. Daher kann es sein, dass die Funktion für mehrfaches Streaming bei diesen Kameras nicht korrekt funktioniert.

Der Treiber unterstützt nur G.711-Audiocodierung. Daher sollte die G.711-Kodierung manuell über das Web-Interface ausgewählt werden, wenn die Kamera mehr als eine Audiokodierung unterstützt.

VMS unterstützt keine Privatzonen für PTZ-Kameras. Die Unterstützung von Privatzonen wird also erkannt, wenn die Kamera keine Schwenk-/Neigebewegung unterstützt.

Samsung-Geräte mit WR3.0-Softwareplattformversion haben ein Problem bei der SSL-Implementierung, das die Verwendung von POST-Befehlen nicht zulässt. Daher kann die Privacy-Zones-Funktion nicht verwendet werden, wenn die HTTPS-Unterstützung aktiviert ist. Samsung hat versprochen, dieses Problem in der nächsten Firmware-Version zu beheben.

Samsung-Geräte mit WR3.0-Softwareplattformversion senden Videostreams mit niedriger Bildrate (z. B. 2-3 statt 20), wenn der Audiostream vor dem Videostream abonniert wurde. Dieses Verhalten wird durch die Implementierung des RTSP-Moduls auf der Kameraseite verursacht. Bitte speichern Sie die Kameraeinstellungen erneut, ohne sie zu ändern, um die Kamera in den normalen Streaming-Modus zu versetzen.

Bei der Verwendung von Einstellungen für konstante Bitraten (CBR) für Samsung-Geräte mit Profilunterstützung wird die VMS-Qualität anhand der folgenden Grenzwerte in Prozentwerte für die Bitrate umgerechnet:

- 2Mbps - 15Mbps für eine Auflösungsbreite von 1600px und mehr;
- 1024Kbps - 10Mbps für Auflösungsbreiten zwischen 1024px und 1600px;
- 512Kbps - 5Mbps für Auflösungsbreiten zwischen 640px und 1024px;
- 64Kbps - 2Mbps für eine Auflösungsbreite von weniger als 640px.

Die korrekte VMS-Qualität sollte so eingestellt werden, dass sie zur erforderlichen Netzwerkbandbreite passt. Andere Kameras verwenden die Standardqualitätseinstellungen, nicht die Bitrate.

Die Bitrate kann auf 6 Mbps begrenzt werden, wenn das Videoprofil im Aufnahmemodus für die interne Flash-Karte (Edge Storage) konfiguriert ist. Der Treiber ändert den Wert der GOP-Größe für Videoprofile, die im Aufnahmemodus konfiguriert sind, nicht. Um diese Einschränkung zu vermeiden, konfigurieren Sie bitte ein separates Profil für internes Aufnahmematerial über das Web-Interface der Kamera (im Abschnitt „Videoprofil“).

Für die Verwendung von VBR mit Audio und Multiple Streaming sollte die Kamera über Firmware 2.x oder höher verfügen. Mit älterer Firmware funktioniert Video für Mehrfach-Streaming nicht.

Multicast ist für Samsung-Modelle mit altem SDK (Nicht-Profil-Kameras) nicht aktiviert. Alle diese Modelle arbeiten nur mit Unicast. Diese Kameras können nicht in mehreren VMS-Instanzen verwendet werden!

Unicast mode: Der Treiber ändert die Kameraeinstellungen entsprechend den VMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über die Unicast-Verbindung.

Multicast:Primary: Der Treiber ändert die Kameraeinstellungen entsprechend den VMS-Einstellungen und empfängt Audio- und Videodaten von der Kamera über die Multicast-Verbindung.

Multicast:Listener: Der Treiber wird die folgenden Kameraeinstellungen nicht ändern:

- Qualität
- Auflösung
- Framerate

Für Multicast:Listener werden die folgenden Optionen auf die gleiche Weise konfiguriert wie für Multicast:Primary:

- Option Mehrfaches Streaming
- Videocodec für alle Streams

Wenn die Kamera in mehreren VMS-Instanzen verwendet werden soll, sollte ein VMS auf Multicast:Primary und die anderen auf Multicast:Listener eingestellt werden.

Mehrere Multicast:Primary-Konfigurationen oder Multicast:Primary- und Unicast-Konfigurationen sind nicht zulässig, da die Kamera sonst durch ständige gleichzeitige Änderungen der Einstellungen überlastet wird.

Multicast-Adresse und -Port sollten für jedes Profil auf der Webschnittstelle der Kamera eingestellt werden, andernfalls wird Multicast nicht funktionieren. Wenn Mehrfach-Streaming aktiviert ist, erstellt der Treiber ein MLIVE-Profil - Multicast-Adresse und -Port sollten auch für dieses Profil festgelegt werden.

Bereichszoom und Zentrierfunktion sind für Samsung-Kameras mit SUN API 2.0-Unterstützung verfügbar.

Die Änderung der Blende ist aufgrund von Kameraeinschränkungen langsam). Ein Klick - eine Änderung.

Wenn die Kamera bewegt (oder gezoomt) wird, werden automatische Blende und Autofokus angewendet.

Zur Unterstützung von Audio in Edge Feature ist VMS Version 7.4.3.71 oder höher erforderlich.

Die neuen Kameraserien (z. B. QNO/QNV/QND-7010R) haben Einschränkungen bei der Verwendung von 2 Megapixel und höheren Auflösungen für H.264-Streams:

- Bei Auflösungen über 2MP (2592x1520 / 2560x1440 / 2304x1296) wird die maximale Bildrate auf die Anzahl der aktiven Streams aufgeteilt:
    - 20 fps / 2 Streams = 10 fps pro Stream;
    - 20 fps / 3 Streams = 6 fps pro Stream.
- Ein Stream über 2MP + 2MP-Streams:

  - 15 fps pro Stream für Dual-Streaming-Konfigurationen (Beispiel: 2592x1520 @ 20fps + 1920x1080 @ 20fps)
  - 10 fps pro Stream für Dreifach-Streaming-Konfigurationen (Beispiel: 2592x1520 @ 20 fps + 1920x1080 @ 20 fps + 1920x1080 @ 20 fps)
- Nur 2MP (1920x1080) Streams:
  - Keine Begrenzung für 2 Streams (20 fps pro Stream)
  - 15 fps pro Stream für 3 Streams

Die Funktion zum Ändern von Optionen durch Alarm (CCFiA/CCRiA) ist für Geräte verfügbar, die einen Wechsel der Optionen schneller als 2 Sekunden ermöglichen. Die Geräte, die vor dem Jahr 2015 veröffentlicht wurden, unterstützen diese Funktion nicht.

Windows XP wird seit der Treiberversion 2.2.18.1 nicht mehr unterstützt.

9.7.3.18 NewSiquraIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern und für die PTZ-Funktionalität verwendet.

Wenn sich zwischen VMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Standard-Port ist 80,
- **RTSP**: Der Standard-Port ist Port 554,
- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden im Portbereich 3556 bis 4556 benötigt.

Beispiel: Wenn es in einem DVMS 4 Siqura-Codecs gibt, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.18.1 Beschränkungen

Der H.264-Decoder kann manchmal nicht in der Lage sein, das empfangene Bild zu dekodieren, was zu einem Fehler in der DVR-Logdatei führt.

Manchmal verarbeitet eine analoge Dome-Kamera keine PTZ-Befehle. Beispielsweise hält die Dome-Kamera manchmal nicht an, nachdem die Steuerung beendet wurde, oder sie bewegt sich nicht nach einer abrupten Richtungsänderung. Außerdem wird ein weiterer HTTP-Befehl mit denselben Parametern ignoriert, bis ein HTTP-Befehl mit anderen Parametern empfangen wird. Wahrscheinlich handelt es sich hierbei um eine Funktion des Siqura Video-Servers.

MJPEG-Videos von Siqura MD2x/HD2x-Kameras bleiben während der Live-Übertragung für einen Moment stehen. Es scheint, als ob ein Bild übersprungen wird. Das gleiche Verhalten tritt im Web-Interface auf. Dies ist ein Kameraproblem.

Siqura MD2x-Kameras mit alter Hardwarebasis unterstützen die Output-Funktionalität nicht. Der Treiber kann die Hardwareinformationen nicht erkennen, so dass die Ausgabe in jedem Fall in DVMS angezeigt wird.

Siqura-Geräte unterstützen keinen kontinuierlichen Blendenwechsel - dies ist eine Funktion der Firmware.

Alle Preset-Befehle, die im MD2x/MD6x/HD2x/HD6x-Protokoll (Dateiname „NKF - Protocol Hotkey 20090805“) als Befehle für den Zugriff auf spezielle Kamerafunktionen beschrieben sind, werden im PTZ-Modul deaktiviert. Daher wird die Anzahl der unterstützten Voreinstellungen für Siqura PTZ-Kameras weniger als 256 betragen.

Live MJPEG Encoder auf Siqura PTZ Kameras arbeiten mit niedrigerer Priorität als andere Encoder (MPEG-4 und H.264). Daher können die tatsächlichen Framerate-Werte geringer sein als für den MJPEG-HTTP-Kanal erforderlich, insbesondere bei schlechten Lichtverhältnissen.

Der Treiber speichert Voreinstellungsnamen in einer XML-Datei. Unicode-Voreinstellungsnamen werden seit Treiberversion 1.9.2.0 unterstützt.

9.7.3.19 NewSonyIPCapture - Installation und Verwendung

Der Treiber verwendet die folgenden Protokolle für den Videoempfang:

- Das HTTP/HTTPS-Protokoll wird für den Empfang von MJPEG-Video- und Bewegungserkennungsdaten verwendet;
- RTP/UDP/IP-Protokolle werden für den Empfang von MPEG-4-, H.264-Videostreams und Audiostreams verwendet;
- Das RTSP-Protokoll wird für die Steuerung des RTP-Streams für G5 (5. Generation) und neuere Geräte verwendet;
- Das HTTP-Protokoll wird zum Senden des Audiostroms an die Kamera verwendet.

Das HTTP/HTTPS-Protokoll wird auch zum Setzen/Abrufen von Parametern verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP/HTTPS-Ports
geöffnet sein:

- **HTTP**: Standard-Port ist 80,
- **HTTPS**: Der Standardanschluss ist 443,
- **RTSP**: Der Standardanschluss ist 554,
- **UDP**: zwei aufeinanderfolgende Ports pro Videostream werden im Portbereich 3556 bis 4556 benötigt.

Beispiel: Wenn 4 SONY IP-Kameras für den Empfang von MPEG-4- oder H.264-Video in einem DVMS konfiguriert sind einem DVMS, dann werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei, wird er übersprungen.

Der Treiber kann mithilfe einer XML-Konfigurationsdatei konfiguriert werden, um die Audioparameter für die SONY G5-G7 IP-Geräte einzustellen.

9.7.3.19.1 Beschränkungen

Die Kameramodelle SNC-DM160, SNC-DM110 und SNC-CM120 unterstützen eine Lichttrichterfunktion:

Der Treiber setzt den Lichttrichter immer auf den Modus „Auto“. Wenn er bei geringer Beleuchtung aktiv wird, erhöht er die Bildempfindlichkeit, schaltet aber bei einer Auflösung von 1280x960 automatisch auf eine niedrigere Auflösung von 640x480 um.

Die Aktivierungs-/Deaktivierungsverzögerung des Lichttrichters beträgt etwa 40 Sekunden.

Der Lichttrichter funktioniert nicht, wenn einer der folgenden Werte eingestellt ist:

- Die Bildgröße ist eine der folgenden:
    - JPEG - 960x720: MPEG4 - AUS
    - JPEG - 768x576: MPEG4 - AUS
    - JPEG-Beschneidung ist eingeschaltet
    - SolidPTZ ist eingeschaltet
    - Blende offen ist eingeschaltet.
- Bitte beachten Sie, dass bei ausgeschaltetem Lichttrichter die maximale Bildrate 15 fps beträgt. Weitere Einzelheiten finden Sie im Benutzerhandbuch der Kamera.

Bei hohen Bildauflösungen kann die Bildrate niedriger als gewünscht sein.

9.7.3.19.1.1 Hinweise zur Funktion Analoger Videoausgang

- Der Treiber deaktiviert die Funktion Analog Video-Out für SONY G4 IP-Kameras (4. Generation). Die Aktivierung dieser Funktion führt zu einer Einschränkung der unterstützten Codecs und Auflösungen (z. B. unterstützt die Kamera SCN-CS20 nur die Auflösung 640x480).
- Der Treiber ändert die Einstellung für den analogen Videoausgang bei G5/G6 SONY IP-Kameras nicht. Bitte beachten Sie, dass die Leistung der Kamera beeinträchtigt werden kann, wenn diese Funktion auf „Ein“ eingestellt ist.

9.7.3.19.1.2 Hinweise zur Bewegungserkennungsfunktion

- Bitte konfigurieren Sie die Bewegungserkennungszonen manuell über die Weboberfläche, bevor Sie die Bewegungserkennungstreiberfunktion verwenden.
- SONY-Kameras senden möglicherweise nicht den korrekten Stream von Bewegungsereignissen, wenn die Seite Bewegungserkennung auf der Weboberfläche der Kamera geöffnet wird. Dies bedeutet, dass die MD-Funktionalität in diesem Fall nicht korrekt funktioniert.

9.7.3.19.1.3 Andere Einschränkungen

- Die Kameras SNC-DM160, SNC-DM110 und SNC-CM120 unterstützen die Auflösungen 1280x960, 960x720 und 768x576 und werden nur mit JPEG-Komprimierung verwendet, aber diese Auflösungen werden auch mit MPEG-4 in den Kameraeinstellungen im System Manager angezeigt. Wenn eine dieser Auflösungen mit MPEG-4 ausgewählt wird, ist die tatsächliche Auflösung immer 640x480.
- Die Kameras SNC-CS20, SNC-DS60 und SNC-DS10 unterstützen nur die Auflösung 768x576 bei JPEG-Kompression, aber diese Auflösung wird im System Manager auch bei MPEG-4 angezeigt.
- Alle P-Modelle der G3-Kameras (3. Generation) haben eine maximale Framerate von 8 fps (N-Modelle 10 fps) mit H.264-Kompression, aber die Kameraeinstellungen im System Manager zeigen 25 fps als Maximum an. Da einige Kameramodelle bis zu 12 fps liefern können, verwendet der Treiber diesen Wert als maximale Framerate.
- Bei JPEG-Kompression zeigt der System Manager die Frameraten der G2-Kameras (2. Generation) mit 1 bis 25 an, die Kameras unterstützen jedoch nur 5, 6, 8, 10, 15, 20 (und 30 im NTSC-Modus) fps.
- Die Voreinstellungsfunktion und die Funktion für Privatzonen funktionieren in DVMS 5.9.8 nicht korrekt. Dieses Problem wird durch die Inkompatibilität einiger Programmschnittstellen verursacht.
- In einigen Fällen senden SONY-Kameras Videos für den MJPEG-Codec mit einer höheren Bildrate als erforderlich. Zum Beispiel sendet die SONY SNC-Z20P Kamera nach dem Zoomen einen MJPEG-Videostream mit 24-25 fps, auch wenn die Bildrate im Systemmanager auf 20 eingestellt ist. Dies ist eine Funktion der Firmware der Kamera.
- Die SONY SNC-Z20-Kamera sendet einen MJPEG-Videostrom mit einer niedrigeren Bildrate als erforderlich, wenn die maximale Auflösung und die Qualitätseinstellungen festgelegt sind. Zum Beispiel kann die maximale Bildrate bei einer Auflösung von 736x544 und einer Qualitätseinstellung von 100 % nicht höher als 3 sein. Dies ist eine Funktion der Kamera.
- Die SONY SNC-Z20-Kamera unterstützt die Funktionen Zoom und Fokus, aber nicht die Funktion Schwenken/Neigen. DVMS zeigt jedoch in jedem Fall die Schwenk-/Neigefunktion im Gerätefenster an (auch wenn die Kamera die Schwenk-/Neigefunktion nicht unterstützt und diese Funktion im Treiber deaktiviert ist). Dies ist ein VMS-Problem.
- Die SONY SNC-Z20 Kamera unterstützt keine Voreinstellungsfunktion. Aber die Schaltfläche „Voreinstellung hinzufügen“ ist in DVMS 5.4.4 für sie immer aktiviert. Dies ist ein VMS-Problem.
- Die SONY SNC-CH210 unterstützt die Auflösung 2048x1536 nur für den MJPEG-Videocodec (das Seitenverhältnis sollte auf 16:9 eingestellt werden). Für andere Codecs beträgt die maximale Auflösung 1600x1200.
- Einige G5-Kameras (5. Generation) haben eine Beschränkung für die Größe des Datenschutzrechtecks. Das Rechteck darf nicht größer als 1/16 des Kamerabildes sein:
    - 640x480 Pixel für SNC-CH220/DH220-Kameras (bezogen auf die maximale Auflösung von 1920x1080)

- 200x140 Pixel für SNC-EM520/EM521-Kameras (bezogen auf die maximale Auflösung von 800x600)So, real privacy zones may be lower than applied by users because of this camera's feature.

- SONY G5 Kameras senden HD-Videostreams mit einer Geschwindigkeit von bis zu 15 Mbps. Das Abonnieren von Videos mit HD-Auflösung

Hochqualitätsvideos für H.264/MPEG-4-Codec oder HD-Auflösungsvideos für MJPEG-Codec von mehr als einer Kamera können zu Verzögerungen im Videostrom führen. Zum Beispiel springt die tatsächliche Bildrate bei einer Einstellung von 15 fps in einem Intervall von 2..13.

- SONY G5/G6-Kameras starten ihren eigenen Video-Encoder neu, nachdem die Videooptionen geändert wurden. Dieser Vorgang dauert 3-8 Sekunden, so dass die Funktionen CCRiA und CCFiA (Ändern der Optionen durch Alarm) bei diesen Kameras nicht verwendet werden können.

Die SONY SNC-VB630-Kamera startet den H.264-Stream bei Bewegung mit 10-20 Bildern pro Sekunde statt mit 50 Bildern pro Sekunde, wenn eine Qualität von 1 % ausgewählt ist. Bitte verwenden Sie einen Qualitätswert von 2%, um dieses Verhalten zu vermeiden.

Die SONY G6-Kameras verwenden Qualitätseinstellungen (variable Bitrate), um die Qualität des H.264-Streams festzulegen. Frühere Kameragenerationen verwenden die Option Konstante Bitrate (CBR) für MPEG-4- und H.264-Kodierungen.

- Die Funktion für mehrfaches Streaming ist für SONY G5- und G6-Geräte und für DVMS Version 6.1.1 und neuer verfügbar. Ältere SONY-Geräte unterstützen diese Funktion nicht.

Die SONY G5/G6-Kameras wenden die Videoeinstellungen während mehrerer Sekunden an und können während dieses Vorgangs das Streaming anhalten. Daher kann das Starten eines Streams dazu führen, dass andere aktive Streams erneut abonniert werden.

9.7.3.19.1.4 Für SONY G5-Kameras gelten die folgenden Einschränkungen für die Funktion Mehrfach-Streaming

- Die Kameras SNC-RS44/RS46/RS84/RS86 unterstützen bis zu 3 Streams. Andere G5-Geräte unterstützen nur 2 Streams (Aufzeichnung und Live)

- Die Auflösung des zweiten Streams kann nicht größer als 640x480 sein, es sei denn, sie ist gleich der Auflösung des ersten Streams.Resolution of third stream should be equal to current resolution of first or second stream.

- Die G5-Kameras starten möglicherweise keinen Videostream, wenn MJPEG für den Live-Stream mit maximaler Auflösung ausgewählt ist. Dieses Problem wird durch ein unerwartetes Verhalten der Kamera verursacht (RTSP PLAY-Anfrage liefert Fehlercode 451). Bitte ändern Sie die Kodierung oder verringern Sie die Auflösungseinstellungen, wenn Sie dieses Problem feststellen.

- Der Treiber wählt während der Anwendung der Einstellungen automatisch die passende Auflösung, wenn die aktuelle Auflösung von der Kamera nicht unterstützt wird. Daher kann die Auflösung des Streams von den im VMS vorgenommenen Einstellungen abweichen. Bitte informieren Sie sich in der Web-Schnittstelle der Kamera über die Einschränkungen der Videoeinstellungen.

- Bei den SONY G5/G6-Kameras kann es zu Problemen bei der Kodierung/Dekodierung des G.726-Audiostreams kommen (Rauschen, kein Ton usw.). Bitte verwenden Sie den G.711-Codec, wenn Sie Probleme mit dem G.726-Codec haben.
- Die Audioausgabe (Senden an die Kamera) wird bei SONY G6-Kameras nach einem Signalverlust möglicherweise nicht wiederhergestellt.

Die Kamera gibt möglicherweise den HTTP-Fehlercode 503 zurück. Um die Funktion der Audioausgabe wiederherzustellen, starten Sie die Kamera über die Webschnittstelle neu, „System“ - „Initialisieren“ - „Neustart“.

9.7.3.19.1.5 Die Einschränkungen der SONY G7 Kamera

„Ausgabemodi":

Die SONY G7 kann in mehreren verschiedenen „Ausgabemodi“ arbeiten. Die Option „Ausgabemodus“ kann im Abschnitt „System“ - „Installation“ der Webschnittstelle geändert werden.

Bevor Sie diesen Modus ändern, sollten Sie die Kamera aus dem VMS entfernen. Nach dem Ändern des Ausgabemodus muss die Kamera erneut zum System hinzugefügt werden.

Die Funktion „Mehrfaches Streaming“ ist nur in den folgenden „Ausgabemodi“ verfügbar:

- „4K-Multi-Streaming“
- „Intelligentes Zuschneiden (FullHD)“
- „Intelligentes Zuschneiden (VGA)“Die Kamera im Ausgabemodus „HDMI“ kann nicht erkannt und hinzugefügt werden.

Die Liste der verfügbaren Videoauflösungen, Videocodecs und Bildraten ist begrenzt und hängt vom gewählten „Ausgabemodus“ und „Seitenverhältnis“ ab. Bitte fügen Sie die Kamera erneut zum VMS hinzu, nachdem Sie diesen Modus geändert haben.

- Die SONY G7-Kameras haben Bildratenwerte mit Fließkomma. Der Treiber rundet den Wert auf die nächstliegende Ganzzahl.
- Die Option „H264Quality“ ist für die SONY G7-Geräteserie nicht zulässig. Der Treiber wandelt den Wert „Qualität“ in den Bitratenwert für den H.264-Codec um.
- Bei den SONY G7-Kameras in den „4K“-Ausgabemodi kann der hochauflösende H.264-Stream vom DVMS-Videocodec nicht korrekt dekodiert werden, wenn die Option „B-Bild“ auf der Kamera aktiviert ist. Der Treiber deaktiviert diese Option standardmäßig.
- Wenn die Edge-Storage-Aufzeichnung aktiviert ist, wird die Bitrate auf 8 Mbps oder weniger für den H.264-Codec begrenzt.
- Geräte der SONY H-Serie (wie die Kamera SNC-HM662) verwenden ein anderes SDK als andere SONY G6-Kameras und können nicht mit dem nativen SONY-Treiber hinzugefügt werden. Bitte verwenden Sie stattdessen den Vivotek IP Capture-Treiber für diese Geräteserie.

- SONY SNC-EMX32R/52R-Geräte verwenden ein anderes SDK als andere SONY G6/G7-Kameras und können nicht mit dem nativen SONY-Treiber hinzugefügt werden. Bitte verwenden Sie stattdessen den BOSCH-Treiber (NewBoschIPCapture) für diese Geräteserie.

Für die Zeitsynchronisierung gelten die folgenden Regeln:

- Der Zeitsynchronisationsvorgang wird durch eine der folgenden Bedingungen ausgelöst:
- Änderung der Windows-Systemzeit;
- Wechsel der Windows-Zeitzone;
- Bei der vorherigen Zeitsynchronisierung ist ein Fehler aufgetreten;
- Die letzte erfolgreiche Synchronisierung wurde vor mehr als 30 Minuten durchgeführt.
  Diese Bedingungen werden alle 5 Minuten überprüft
- Die neue Zeit wird auf dem IP-Gerät eingestellt, wenn der Unterschied zwischen der Zeit des Geräts und der des Rekorders 10 oder mehr Sekunden beträgt.
- Die SONY HTTP API ermöglicht die Anwendung der Zeit im GMT-Format, so dass der Treiber die Zeitzoneneinstellungen auf dem IP-Gerät nicht aktualisiert
- Die Funktion zum Ändern von Optionen im Alarm (CRiA/CFA) kann nur im „aktiven“ Kontrollmodus verwendet werden. Im „Passiv“-Modus ändert der Treiber keine Optionen auf der IP-Kamera, so dass der Stream weiterläuft, ohne dass sich Auflösung oder Bildrate ändern.
- Windows XP wird seit Treiberversion 2.6.0.0 nicht mehr unterstützt.

9.7.3.20 OnvifIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:HTTP: default port is 80,

- RTSP: Der Standard-Port ist 554,
- UDP: Zwei aufeinanderfolgende Ports pro Unicast-Audio- oder Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Wenn beispielsweise 4 IP-Kameras in einem VMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Für das Multicast-Streaming sind ebenfalls zwei aufeinander folgende Ports pro Audio- oder Videostream erforderlich, aber die Anzahl der Ports hängt von den Geräteeinstellungen oder der XML-Konfiguration ab. Das Gerät kann zum Beispiel so konfiguriert sein, dass alle Streams nur an einen einzigen Port gesendet werden. Die Ports 40000-40001 sollten geöffnet werden, wenn für diese Einstellung der Port 40000 angegeben ist.

9.7.3.20.1 Beschränkungen

- Der Befehl PTZ Area Zoom wird standardmäßig mit dem Befehl PTZ Center kombiniert, sofern unterstützt
- Der PTZ-Center-Befehl wird mit geringer Genauigkeit ausgeführt, da die Genauigkeit stark vom Kameramechanismus, den vertikalen und horizontalen Blickwinkeln und den optischen Aberrationen (z. B. Verzerrungen) des aktuellen Objektivs abhängt. Es gibt derzeit keine Möglichkeit, diese Einstellungen einzugeben und zu speichern.
- Der Treiber benötigt ein Medienprofil, um Voreinstellungen vom IP-Gerät zu empfangen. Sie können also geladen werden, nachdem der Videostream abonniert wurde.
- Der Treiber verwendet Zeitstempel zur Authentifizierung auf dem Gerät gemäß den ONVIF-Spezifikationen. Daher sollten die Zeit auf dem ONVIF-kompatiblen Gerät und die Zeit auf dem PC, auf dem der VMS Recorder installiert ist, vor der Verwendung des Geräts synchronisiert werden.
- Der Treiber unterstützt keine Unicode-Positionsnamen.
- Die Mehrfach-Streaming-Funktion kann abhängig vom verwendeten Gerät Einschränkungen haben (z.B. kann die Auflösung auf Encoder1 nicht größer sein als die Auflösung auf Video-Encoder2). Bitte lesen Sie das Gerätehandbuch, um diese Einschränkungen zu erfahren.
- Geräte mit mehreren Kanälen können unterschiedliche Funktionen für verschiedene Kanäle unterstützen. Beispielsweise unterstützt der erste Kanal einen H.264- und MPEG-4-Stream mit einer Auflösung von 1920x1080 und der zweite Kanal unterstützt nur die H.264-Kodierung, aber mit einer größeren Auflösung von 4096x2160. Die VMS-Architektur erlaubt es nicht, unterschiedliche Fähigkeiten für verschiedene Kanäle zu übergeben, daher werden die Fähigkeiten aller Kanäle kombiniert (d. h. MPEG-4-Kodierung und 4096x2160-Auflösung sind für beide Kanäle im obigen Beispiel verfügbar).

Der Treiber wählt automatisch eine geeignete Option aus, wenn der Benutzer versucht, einen Optionswert anzuwenden, der vom aktuellen Videokanal nicht unterstützt wird.

- In einigen Fällen kann der Benutzer mit dem Problem „Kein Signal“ konfrontiert werden, weil das ONVIF-konforme Gerät falsch konfiguriert wurde (die Meldung „ter:Action > ter:ConfigurationConflict“ wird in der Protokolldatei angezeigt). In diesem Fall sollte der Benutzer die Einstellungen in VMS entsprechend den Fähigkeiten des Geräts korrigieren, wenn Mehrfach-Streaming aktiviert ist. Wenn die Option Mehrfaches Streaming nicht verwendet wird, nehmen Sie bitte minimale Einstellungen für zusätzliche Streams über das Web-Interface vor oder deaktivieren Sie sie ganz.
- ONVIF-konforme Geräte können möglicherweise nicht von „Single Stream“ auf „Triple Stream“ umschalten, ohne die Einstellungen für den zweiten Stream zu übernehmen. Mit anderen Worten: Der Remote-Stream wird möglicherweise nicht korrekt eingerichtet, wenn der Live-Stream nicht gestartet wurde, nachdem die Funktion „Multiple Streaming“ aktiviert wurde.
- Der Treiber wendet die Einstellungen für verschiedene Streams nacheinander an, nicht gleichzeitig. Daher kann das Starten zusätzlicher Streams mehr Zeit in Anspruch nehmen als das Starten nur des Aufzeichnungsstreams.

- Der Treiber verwendet die PTZ-Dienstversion 2.0 gemäß den ONVIF-Spezifikationen. Alte Geräte können jedoch die frühere Version 1.0 des PTZ-Dienstes verwenden, so dass der Treiber die PTZ-Funktionen nicht korrekt erkennt. Bitte verwenden Sie in diesem Fall die XML-Konfigurationsdatei, um die richtige PTZ-Service-Version anzugeben.
- Der Treiber verwendet den Pull-Point-Mechanismus, um die Zustände der digitalen Eingänge zu empfangen und den Bewegungserkennungsstrom zu überwachen. Wenn ein ONVIF-konformes Gerät diesen Mechanismus unterstützt, sollte es die Fähigkeit WSPullPointSupport in tds:GetCapabilitiesResponse gemäß Abschnitt 9.9 der ONVIF-Core-Spezifikation einstellen. Die digitalen Eingänge und die VMD-Funktionalität werden nicht erkannt, wenn diese Fähigkeit auf „nicht unterstützt“ gesetzt ist.

9.7.3.20.1.1 Einschränkungen der Audiofunktionalität

Der Treiber verwendet die Audiofunktionalität „wie sie ist“ ohne Anpassung der Audioparameter (z. B. Ausgangsverstärkung). Für die herstellerspezifischen Parameter wie „Eingangs-/Ausgangsintervall“ oder „Ausgangsdauer“ gibt es in den ONVIF-Spezifikationen keine entsprechenden Optionen. Bitte konfigurieren Sie diese Parameter vor der Verwendung der Kamera manuell über das Web-Interface.

9.7.3.20.1.2 Einschränkungen der Multicast-Erfassung

Die Multicast-Erfassung kann über die XML-Konfigurationsdatei mit der Option StreamingMode aktiviert werden. Diese Option wird beim Start des Streams gelesen, so dass eine Aktualisierung der Geräteeinstellungen ausreicht, um die geänderte StreamingMode-Option zu verwenden.

Bitte beachten Sie, dass VMS seit Version 7.4.1 über eine Optimierung für den Neustart von Kanälen verfügt, so dass es in diesem Fall erforderlich ist, eine der Videooptionen für jeden Kamerastream zu ändern, um sie neu zu starten. Die Audioeinstellungen sollten ebenfalls aktualisiert werden, um die Option zu verwenden.

Die Treiberinstanz kann so konfiguriert werden, dass sie als primäre Instanz oder als Listener verwendet wird. Die primäre Instanz ist in der Lage, die IP-Geräteeinstellungen zu ändern und zusätzliche Funktionen zu nutzen. Listener-Instanzen sind in der Lage, Video- und Audioströme per Multicast zu empfangen und ermöglichen die Nutzung der digitalen E/A- und VMD-Funktionen.

Der Treiber wählt eine Kombination von Videoquellen, Video-Encodern und Medienprofilen während der Erkennung von Fähigkeiten aus. Es ist erforderlich, dass sowohl die primäre als auch die Listener-Instanz dieselbe Kodierung auswählen, damit sie dasselbe Medienprofil auswählen können. Andernfalls wird die Listener-Treiberinstanz versuchen, ein anderes Profil zu abonnieren und einen anderen Multicast-Stream oder überhaupt keine Daten empfangen.

Der Listener-Recorder ändert keine Konfiguration auf der Seite des ONVIF-konformen Geräts. Wenn zum Beispiel kein Medienprofil auf der Kamera vorhanden ist, wird es nicht erstellt und der Treiber kann den Video- oder Audiostrom nicht empfangen. Das ONVIF-Gerät sollte vor der Verwendung in der Listener-Konfiguration zum primären Rekorder hinzugefügt werden.

Die zusätzlichen Streams (Live und Remote) sind nur dann aktiv, wenn sie in Clients geöffnet sind. Um die aktualisierten Multiple Streaming-Einstellungen zu verwenden, müssen diese Streams für den primären Rekorder

gestartet (oder geöffnet gehalten) werden, nachdem die Stream-Einstellungen im VMS geändert wurden. Andernfalls werden die neuesten Stream-Einstellungen nicht auf die Kamera angewendet.

Sie sollten sicherstellen, dass nur ein Rekorder die Einstellungen von ONVIF-kompatiblen IP-Geräten ändert. Andere Rekorder, die diese Geräte verwenden, sollten sich im Listener-Modus befinden.

Es ist erforderlich, die IP-Adresse des Netzwerkadapters anzugeben, über den die Kamera angeschlossen ist, um das Multicast-Streaming korrekt zu empfangen, falls mehr als ein Netzwerkadapter vorhanden ist. Wenn keine Option konfiguriert ist, wird der in Windows als Standard markierte Netzwerkadapter verwendet.

Der Treiber kann eine Meldung über eine ungültige Multicast-Konfiguration schreiben (z.B.: `ter:InvalidArgVal > ter:InvalidMulticastSettings`). Diese Meldung bedeutet, dass ein Fehler in der Multicast-Konfiguration vorliegt und der Video- oder Audiostream nicht gestartet werden kann.

Bitte geben Sie den Abschnitt Multicast in der XML-Konfigurationsdatei an, um das Problem zu lösen, oder passen Sie die Werte an, wenn dieser Abschnitt bereits vorhanden ist.

Einige ONVIF-konforme IP-Geräte (z. B. Axis) ermöglichen es, den Videostream beizubehalten, während der Client seine Videoparameter ändert. Infolgedessen wird ein solches Gerät den aktiven Stream für die Multicast:Listener-Instanz mit den vorherigen Einstellungen beibehalten und einen anderen Stream für die Multicast:Primary-Instanz mit den aktualisierten Einstellungen starten.

Es ist erforderlich, die Überwachung der Videooptionen auf der Hörerseite mit dem Parameter VideoSettingsMonitoringInterval zu aktivieren. Weitere Einzelheiten sind den Kommentaren in der Konfigurationsdatei zu entnehmen.

9.7.3.20.1.3 Einschränkungen der Video-Bewegungserkennung

- Das Gerät sollte den Themensatz 'tns1:VideoSource/MotionAlarm' unterstützen, um die Bewegungserkennungsfunktion zu unterstützen. Benutzerdefinierte Themensätze wie „tns1:VideoAnalytics/tnssamsung:MotionDetection“ können ebenfalls unterstützt werden, funktionieren jedoch nur bei Geräten mit einem Kanal, da diese Themensätze keine Videoquellen- oder Kanalkennungen als Quelldaten in Ereignisbenachrichtigungen enthalten.
- Es sind keine IP-Geräte-bezogenen Bewegungserkennungseinstellungen in VMS verfügbar. Daher sollten die Bewegungserkennungseinstellungen (Bereiche, Empfindlichkeit, Objektgröße usw.) auf dem IP-Gerät manuell konfiguriert werden, bevor diese Funktion im VMS verwendet wird.
- Die Bewegungserkennung kann mit Multicast-Streaming verwendet werden. Die Option „Rekorder- und Kamerahardware“ sollte sowohl auf dem primären als auch auf dem Listener-Rekorder aktiviert sein, damit der Videostream korrekt angehalten/fortgesetzt werden kann.
- Es gibt keine Möglichkeit, den Zeitpunkt der Anwendung von Video-Optionen ohne Änderung der Kamerakonfiguration zu erkennen. Der Treiber fügt die Unterstützung von CFiA/CRiA-Funktionen für alle Geräte hinzu, kann aber nicht garantieren, dass die Kamera die Optionen schnell genug per Alarm umschaltet.

Bitte probieren Sie die CFiA/CRiA-Funktion in einem Testaufbau aus, bevor Sie sie mit Sicherheitssystemen verwenden.

9.7.3.20.1.4 Sonstige Hinweise

Der Treiber verwendet seit der Treiberversion 1.5.0.0 standardmäßig den Transport „RTP over RTSP“ für das Video-/Audio-Streaming.

Die digitalen Eingänge, die vom ONVIF-konformen Gerät zurückgegeben werden, sind nach Token-Namen sortiert, um sicherzustellen, dass sie vom Gerät bei der ersten Statusabfrage nicht neu geordnet werden. Daher können die realen Eingangsnummern von den VMS-Werten abweichen (z. B. „1“, „2“, ..., „10“ wird als „1“, „10“, „2“, ..., „9“ sortiert).

Die Funktion „Optionen bei Alarm ändern“ (CRiA/CFA) kann nur im „aktiven“ Steuerungsmodus verwendet werden. Im „Passiv“-Modus ändert der Treiber keine Optionen der IP-Kamera, so dass der Stream ohne Änderung der Auflösung oder der Bildrate weiterläuft.

Windows XP wird seit Treiberversion 1.5.0.0 nicht mehr unterstützt.

9.7.3.21 PelcoIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Empfang von MPEG-4- und H.264-Videos.

Das HTTP-Protokoll wird für das Einstellen/Abrufen von Parametern, den Empfang von JPEG-Videos und für die PTZ-Funktionalität verwendet.

Wenn sich zwischen VMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP Ports geöffnet sein:

- **HTTP**: Der Standardport ist 80 für Sarix-Kameras und 49152 für Nicht-Sarix-Kameras,
- **RTSP**: Hafen 554,
- **UDP**: Pro Videostream sind zwei aufeinander folgende Ports im Portbereich 3556 bis 4556 erforderlich.
- **TCP**: 3549 ist der Standardanschluss für GENA DigitalInputs-Meldungen.

Bitte beachten Sie auch die `PelcoIPCapture.xml`, Abschnitt DigitalIOListener, Anschlusswert

Beispiel: Wenn ein VMS über 4 Pelco-Kameras verfügt, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Für Sarix, Endura und die neueste Serie der Treiber von vesrion 1.8.0.0 wird die GENA-Benachrichtigungsarchitektur verwendet. Der Treiber konfiguriert automatisch die Windows Firewall, um eingehende Verbindungen zum DigitalIOListener-Port zuzulassen. Siehe auch addFirewallRule Option.

Im Abschnitt „DigitalIOListener“ können die Optionen „address“ und „port“ verwendet werden, um die externe IP-Adresse und den Port anzugeben, falls eine Weiterleitung vom externen Netzwerk auf denselben TCP-Port erfolgt.

9.7.3.21.1 Einschränkungen

- Die Konfiguration von Qualität und Auflösung für den JPEG-Codec wird für Nicht-Sarix-Kameras nicht unterstützt. Alle JPEG-Bilder werden in 4CIF empfangen. Die SystemManager-Kameraeinstellungen werden in diesem Fall ignoriert.
- Pelco Sarix-Kameras erlauben standardmäßig den Zugriff auf sie über SOAP-Anfragen ohne Benutzerauthentifizierung. So kann jeder nicht autorisierte Benutzer Pelco Sarix-Kameras abonnieren und konfigurieren. Um ein solches Verhalten zu vermeiden, setzen Sie bitte die Einstellung „Öffentliche Benutzerzugriffsebene“ auf der Registerkarte „Benutzer“ im Web-Interface auf „Deaktiviert“.
- Die Firmware-Version kann nicht von Pelco IP-Kameras abgerufen werden. Dies ist eine Funktion der Pelco-API.
- Pelco-Kameras wenden die Einstellungen für den Videostrom etwa 30 Sekunden lang an. Daher können die Funktionen CCRiA und CCFiA nicht für Pelco IP-Kameras implementiert werden.
- Sarix MPEG-4 Encoder unterstützt keine Auflösungen über 704x576. Der Treiber setzt die Auflösung automatisch auf 704x576, wenn der Benutzer versucht, eine höhere Auflösung anzuwenden.
- Der Treiber kann von Zeit zu Zeit die Anzahl der Ein- und/oder Ausgänge der IP110-Kamera nicht empfangen. Um dieses Problem zu beheben, versuchen Sie, die Kamera aus der Kameraliste zu entfernen und sie dann wieder hinzuzufügen.
- Die tatsächliche Framerate für die JPEG-Komprimierung kann geringer sein als die erforderliche Framerate, da die Erfassung von Bildern über HTTP Verzögerungen aufweist.
- Die IO-Funktionalität für SARIX-Kameras funktioniert im Moment nicht richtig. Die Zustände der Eingänge können nicht abgefragt werden. Die Ausgabekomponente funktioniert nicht ordnungsgemäß, da die Eingangszustände unbekannt sind.
- Die Liste der unterstützten Bildwiederholraten kann für verschiedene Codecs für Sarix-Kameras unterschiedlich sein. Wenn der Benutzer versucht, einen nicht unterstützten Wert für die Bildrate anzuwenden, wird der nächsthöhere Wert für die Bildrate verwendet (z. B. wird der Wert 7,5 anstelle des nicht unterstützten Wertes 6 verwendet). Wenn der Benutzer versucht, einen höheren Wert als den maximal unterstützten Wert anzuwenden, wird automatisch der maximale Wert angewendet. Eine Liste der unterstützten Bildratenwerte finden Sie in der Webschnittstelle der Kamera.

Der Parameter Geschwindigkeit wird von Pelco PTZ IP-Kameras für die folgenden PTZ-Funktionen nicht unterstützt:

- Fokussieren;
- Zoomen;
- Änderung der Blende;

- Anfahren der voreingestellten Position. Der Treiber verwendet diese Funktionen also so, wie sie sind: Die Kamera verarbeitet sie in allen Fällen mit konstanter Geschwindigkeit.

Die Spectra HD-Kamera sendet den H.264-Videostrom mit einer niedrigeren Bildrate als erforderlich (z. B. 1 fps anstelle von 4 fps), wenn der Wert der Bildrate gerade ist. Die meisten ungeraden Werte (außer 1 und 25) werden korrekt verarbeitet. Dies ist ein Firmware-Problem.

Der Treiber ist nicht in der Lage, die SOAP-Antwort der Kamera zu parsen, wenn nicht standardisierte Symbole (wie Umlaute oder Hieroglyphen) in den Konfigurationsnamen verwendet werden. Die Verwendung dieser Symbole kann zu fehlerhaftem Verhalten des Treibers führen. Vermeiden Sie daher die Verwendung dieser Symbole bei der Konfiguration von Sarix-Kameras über die Webschnittstelle.

Pelco 1080p-Kameras senden möglicherweise keinen H.264-kodierten Videostrom mit 1080p-Auflösung bei niedrigen Bildraten (von 1 bis 4). Dies ist ein bekanntes Problem der Pelco-Firmware. Einzelheiten finden Sie in der Pelco Knowledge Base: <http://www.pelco.com/sites/global/en/sales-and-support/faq/faq_main.page?AID=12392>.

Um das Problem in der VMS-Software zu lösen, verwenden Sie bitte die niedrigste Qualität für diese Einstellungen.

- Der GetAlarmStates-Aufruf, der für die Abfrage der digitalen Eingänge verwendet wird, ist veraltet und wird vom Pelco-Support-Team nicht für die kommerzielle Nutzung empfohlen. Die Abfrage der digitalen Eingänge alle 2 Sekunden kann dazu führen, dass sich die Kamera nach 2-3 Tagen Betrieb aufhängt. Daher ist die Funktion der digitalen Eingänge standardmäßig deaktiviert, kann aber über die XML-Konfigurationsdatei aktiviert werden, falls sie benötigt wird. It may be required to re-add the camera after configuration file change.

Port 3549 sollte für eingehende Verbindungen in der Windows-Firewall für die DigitalIO-Funktionalität für die Serien Sarix, Endura und höher zugelassen werden. Siehe auch PelcoIPCapture.xml, Abschnitt DigitalIOListener, Port-Wert.

Ältere Versionen der Kameras haben ein Problem, wenn die Digital Outputs-Anforderungen sehr häufig gesendet werden. Wenn der Benutzer eine häufige Änderung des Ausgangs konfiguriert (häufiger als ein Wechsel pro Minute), kann die Kamera nach einigen Tagen hängen bleiben. Um dieses Problem zu vermeiden, deaktivieren Sie bitte die Funktion der digitalen Ausgänge in der Treiberkonfigurationsdatei.

Pelco Optera Serie Panorama-IP-Kameras (IMM12018, IMM12027 und IMM12036 Modelle) haben eine spezielle Implementierung von Stream Dewarping, die noch nicht in den nativen Treiber integriert wurde.

Bitte verwenden Sie stattdessen den ONVIF IP Capture-Treiber für diese Geräteserie.

9.7.3.22 PSIAIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Hafen 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Beispiel: Wenn ein VMS über 4 Kameras verfügt, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.22.1 Beschränkungen

Nur der primäre Videokanal wird unterstützt (wenn die Kamera mehrere Kanäle hat)

9.7.3.23 RTSPIPCapture - Installation und Verwendung

Der Treiber verwendet RTSP/RTP/UDP/IP-Protokolle für den Empfang von Videostreams von IP-Geräten.

Der Treiber erwartet eine RTP- oder RTSP-URI für das Hinzufügen des Geräts. Diese URI sollte in das Feld „IP-Adresse“ eingetragen werden.

Der erforderliche Port kann separat im Feld „Port“ angegeben werden oder im RTSP/RTP-URI enthalten sein. Der RTSP-URI-Port hat höhere Priorität, wenn er gesetzt ist, wird das VMS-Port-Feld ignoriert.

Die Stream-URI-Anforderungen:

- Der RTSP-URI sollte im vollständigen Format angegeben werden, z. B.: `rtsp://192.168.1.70:554/?h264x=0`
- Bei Kameras, die mehrere Videoströme senden (wie ACTi), sollte auch die korrekte Spur-ID angegeben werden: `rtsp://192.168.1.75:7070/track1`
- Die RTP-Streaming-Geräte sollten auch das richtige Präfix haben: `rtp://62.97.61.37:15000/`
- Der RTP-Dampf-URI akzeptiert auch Multicast-Adressen: `rtp://239.232.192.255:20000/`

Bitte beachten Sie, dass die Stream-URI über einen Player eines Drittanbieters, wie VLC oder QuickTime, überprüft werden kann.

Wenn sich zwischen VMS und den Kameras eine Firewall befindet, müssen die folgenden Ports geöffnet werden:

- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Für den RTSP-Modus werden zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt. Der in den Parametern angegebene Port sollte für den RTP-Streaming-Modus geöffnet werden.

Beispiel: Wenn in einem VMS 2 IP-Kameras vorhanden sind, werden die Ports 3556, 3557, 3558 und 3559 für RTSP-Sitzungen verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

Das RTSP-Streaming kann auch über die Konfigurationsdatei RTSPIPCapture.xml konfiguriert werden. Sie erlaubt es, die folgenden Optionen zu ändern:

- RTP-Videotransport. Die folgenden Typen werden unterstützt: RTPoverUDP und RTPoverRTSP `<RTPMode>RTPoverRTSP</RTPMode>`
- Deaktivierung von Keep-alive-Meldungen. Einige Geräte unterstützen die Keep-alive-Verarbeitung möglicherweise nicht, so dass sie durch die Option 0 mit der Angabe `<KeepAlive>1</KeepAlive>` deaktiviert werden kann. Diese Werte können für jedes Gerät einzeln eingestellt werden.

Die Lippensynchronisation kann mit der folgenden Option aktiviert werden: `<LogLevel>4</LogLevel>`

9.7.3.23.1 Beschränkungen

- Wenn die Kamera eine RTSP-Autorisierung erfordert, sollten der richtige Benutzername und das richtige Kennwort festgelegt werden, andernfalls wird kein Video angezeigt.
- Hinweise zum RTP-Modus:
    - Die RTP-Video-Streaming-IP-Geräte sollten in der Lage sein, SPS- und PPS-Header im Stream zu senden. Ohne diese Header ist der Treiber nicht in der Lage, den H.264-Stream korrekt zu dekodieren.
- Der Treiber ist nicht in der Lage, RTP-Streaming selbst zu starten - er verwendet nur RTP-Streams, die kontinuierlich vom Gerät erzeugt werden.
- Die Audiosynchronisierung mit RTCP funktioniert in den folgenden Fällen möglicherweise NICHT:
    - wenn das Gerät nach dem Datenpaket einen RTCP-Bericht sendet;
    - für den Modus RTP über RTSP;

Wenn die RTCP-Synchronisierung verfügbar ist, können Sie die folgenden Meldungen in der Datei DVRLog.txt finden: „`Video frame time was synchronized by RTCP successfully`“

9.7.3.23.1.1 Hinweise zum MPEG2 TS-Format

- Version 1.2.0.0 des Treibers unterstützt nur H.264 und AAC Codecs für das MPEG2 TS Format.
- Es ist nicht möglich, nur Video- oder Audiostreams zu empfangen, da diese über einen einzigen RTP-Stream übertragen werden.
- Der Audiokanal wird für alle Geräte erkannt, die das MPEG2 TS-Format (MPEG II Transport Stream) verwenden.

Bitte setzen Sie den folgenden Wert auf „false“, um Audio auf dem ausgewählten Gerät zu deaktivieren:

```
<AudioChannel>
```

```
            <Enabled>false</Enabled>

          </AudioChannel>
```

Das Betriebssystem Windows XP wird seit der Treiberversion 1.0.1.5 nicht mehr unterstützt.

9.7.3.24 SIPIPCapture - Installation und Verwendung

Beispiel für eine Zenitel-Konfiguration:

`<Zenitel PBX number>@<Zenitel Address>:<Zenitel SIP Port>@<SIPProxy_address>`
(e.g. 500@10.90.91.98:5060@10.90.91.99)

9.7.3.25 StanleyIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Hafen 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Beispiel: Wenn 4 Kameras in VMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.25.1 Beschränkungen

- Der Treiber erkennt nur die Fähigkeiten des aktuell aktivierten Profils. Wenn der Benutzer das Profil in der Weboberfläche der Kamera geändert hat, müssen die Kamerafunktionen in VMS aktualisiert werden (Neustart der automatischen Suche im Systemmanager oder erneutes Hinzufügen der Kamera).
- In VMS ist es nicht möglich, eine unterschiedliche Anzahl von Auflösungen für verschiedene Komprimierungsformate einzustellen, daher werden im Systemmanager alle unterstützten Auflösungen angezeigt. Wenn eine bestimmte Auflösung vom Komprimierungsformat nicht unterstützt wird, wird die nächstgelegene gültige Auflösung verwendet.
- Unterschiedliche Auflösungen unterstützen unterschiedliche maximale Frameraten, so dass der Treiber den nächstgelegenen gültigen Wert für die Framerate verwendet. Wenn beispielsweise die maximale Framerate für die 1080p-Auflösung 15 fps beträgt und der Benutzer in den Systemmanager-Einstellungen 30 fps angibt, legt der Treiber 15 fps für die Kamera fest.
- H.264-Videostreams haben keine Qualitätseinstellung, daher wird zur Steuerung der Streamqualität der Modus mit konstanter Bitrate (CBR) verwendet. 1 % Qualität im System Manager bedeutet minimalen Bitratenwert und 100 % Qualität bedeutet maximalen Bitratenwert.

- Bei Mehrfach-Streaming hat jeder Stream nur einen Codec und eine Auflösung. Zum Beispiel hat das erste Profil in der Kamera die folgenden Kombinationen:

-> H.264 :1920 x 1080

-> H.264 :720 x 480

-> JPEG :720 x 480

-> JPEG :352 x 240

Der erste Stream hat also den H.264-Codec und die Auflösung 1920x1080, der zweite Stream den H.264-Codec und die Auflösung 720x480, der dritte Stream den JPEG-Codec und die Auflösung 720x480. Und die vierte Kombination (JPEG-Codec und 352 x 240 Auflösung) wird wieder für den ersten Stream verwendet. Mehrfaches Streaming kann in der XML-Datei des Treibers deaktiviert werden.

Die Privatzonen können größer sein als im System Manager angezeigt, da die Stanley-Kameras feste Blöcke zur Einstellung der Maske verwenden (20 Blöcke in der Horizontalen und 12 Blöcke in der Vertikalen).

9.7.3.26 VivotekIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP-Protokoll wird für das Setzen/Abrufen von Parametern verwendet.

Wenn sich eine Firewall zwischen VMS und den Kameras befindet, müssen die folgenden RTSP/UDP/HTTP-Ports geöffnet werden:

- **HTTP**: Der Standard-Port ist 80,
- **RTSP**: Hafen 554,
- **UDP**: Zwei aufeinanderfolgende Ports pro Videostream in einem Portbereich von 3556 bis 4556 benötigt werden.

Beispiel: Wenn 4 Vivotek IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet. Wenn ein Port nicht frei ist, wird er übersprungen.

9.7.3.26.1 Beschränkungen

- Manchmal wechselt die Kamera in den „Nur HTTP“-Modus entsprechend dem Mechanismus zur Erkennung von Netzwerkfähigkeiten (kamerainterner Mechanismus). Um die Kamera wieder in den „RTP“-Modus zu versetzen, muss sie neu gebootet werden.
- Die Kamera überspringt die Kanaleinstellungen beim Wechsel vom Modus „Qualitätspriorität“ zum Modus „Bildratenpriorität“. Der Videomodus kann in der Treiber-XML-Datei eingestellt werden.

Die Standard-Ansichtsmaske für hohe Auflösung zeigt nicht das gesamte Bild an. Sie kann über das Web-Interface konfiguriert werden.

Die maximale Bildrate für hohe Auflösungen ist niedriger als angegeben.

- Befehle zum Ändern der Blende funktionieren nicht bei der getesteten SD7323-Kamera.
- AAC-Audio-Dekompression wird ab DVMS 7.4.4 oder höher unterstützt.
- Geräte der Sony H-Serie (wie die Kamera SNC-HM662) verwenden das Vivotek OEM SDK im Gegensatz zu anderen Sony G6 Kameras. Für diese Geräte sollte der Vivotek-Treiber anstelle des Sony-Treibers verwendet werden.
- Windows XP wird seit der Treiberversion 1.6.1.0 nicht mehr unterstützt.
- CCRiA- und CCFiA-Funktionen sind nur für Geräte der Serie 8xxx oder höher verfügbar
- Wenn die Auflösung durch einen Alarm geändert wird, kann der Benutzer ein ungültiges Bild sehen. Dies ist ein Geräteproblem - die Kamera sendet ein ungültiges Bild - und der Treiber kann es nicht überspringen, da alle Header in Ordnung sind.

9.7.3.27 WisenetIPCapture - Installation und Verwendung

In allen Komprimierungsmodi verwendet der Treiber RTSP/HTTP/HTTPS(TLS)/RTP/UDP/IP-Protokolle für den Videoempfang. Das HTTP/HTTPS-Protokoll wird auch zum Setzen/Abrufen von Parametern verwendet.

Wenn sich zwischen DVMS und den Kameras eine Firewall befindet, müssen die folgenden RTSP/UDP/HTTP/HTTPS-Ports geöffnet sein:

- **HTTP**: Der Standard-Port ist 80,
- **HTTPS**: Der Standard-Port ist 443,
- **RTSP**: Der Standard-Port ist 554,
- **UDP**: Zwei aufeinanderfolgende Ports (beginnend mit dem geraden Wert) pro Unicast-Audio- oder -Videostream in einem Portbereich von 3556 bis 4556.

Für die Kommunikation über HTTPS (TLS) muss RTSP über HTTP-Transport gewählt werden, der als für HTTP und für HTTPS.

Wenn zum Beispiel 4 IP-Kameras in einem DVMS vorhanden sind, werden die Ports 3556, 3557, 3558, 3559, 3560, 3561, 3562 und 3563 verwendet werden. Wenn ein Port nicht frei ist, wird das Portpaar übersprungen.

Für das Multicast-Streaming sind ebenfalls zwei aufeinander folgende Ports pro Audio- oder Videostream erforderlich, aber die Anzahl der Ports hängt von den Geräteeinstellungen oder der XML-Konfiguration ab.

Das Gerät kann z. B. so konfiguriert werden, dass alle Datenströme nur an einen einzigen Anschluss gesendet werden. Die Ports 40000-40001 sollten geöffnet werden, wenn für diese Einstellung der Port 40000 angegeben wird.

9.7.3.27.1 Beschränkungen

- Die Nummernschilderkennung wird direkt in dem auf der Kamera installierten VaxALPR-Plugin gemäß dem Handbuch „VaxALPR On-Camera Software“ konfiguriert. Software-Setup und Kamerakonfiguration. Hanwha Handbuch“. Es gibt keine Möglichkeit, die Genauigkeit der LPR über XML einzustellen.

- Es wird empfohlen, Kameras mit Whisenet 5 und Wisenet 7 Prozessoren für das Vaxtor ALPR Plugin (VaxALPR) zu verwenden.
- Bezüglich des TLS-Zertifikats: Wenn eine RTSP-Verbindung über HTTPS (TLS) hergestellt wird, gibt die Kamera ihr öffentliches Zertifikat während des Handshake-Verfahrens weiter, daher muss der Client das öffentliche Zertifikat der Kamera nicht speichern oder besitzen.
- Geben Sie keinen leeren Benutzernamen für die Autorisierung ein. Wenn der Benutzername leer ist, werden die Autorisierungs-Header nicht zu den HTTP-Anfragen hinzugefügt.
- Die Kamera kann eine nicht gedrehte Auflösung zurückgeben, wenn die Option „Fluransicht“ auf 90 oder 270 Grad eingestellt ist (z. B. 800x448 anstelle der tatsächlichen Auflösung von 448x800). In diesem Fall wird der Stream mit der korrekten (gedrehten) Auflösung empfangen.
- Datenschutzmasken werden auf der Grundlage der maximalen Auflösungsgröße gemäß den SUNAPI-Spezifikationen angewendet. Daher kann es vorkommen, dass sie nicht mit den angezeigten Positionen übereinstimmen, wenn ein beschnittenes Bild oder ein Bild mit einem anderen Seitenverhältnis verwendet wird. Dies ist ein normales Verhalten. Bitte verwenden Sie die maximale Auflösung in den Anwendungen System Manager/Spotter Admin für die Bearbeitung von Privatsphärenmasken.
- Bei der SNB-9000-Kamera (Firmware-Version 1.02_160215) können während der Anwendung der Konfiguration durch den Treiber mehrmals Privatsphärenmasken erscheinen und verschwinden. Dies ist ein kamerabezogenes Problem, das dem Hanwha Techwin-Support gemeldet wurde, der jedoch im Moment keine neue Firmware-Version plant.
- Sichtschutzmasken werden für PTZ-Geräte nicht unterstützt, da Mirasys VMS keine Möglichkeit hat, die Position der Maske mit Hilfe von Kugelkoordinaten festzulegen.
- Einige Kameras wie die PNM-9030V unterstützen Privacy Masking nur für den Übersichtskanal. Die übrigen Kanäle zeigen einen Teil des Übersichtskanals an und haben keine Möglichkeit, eigene Masken einzurichten.

Da VMS keine Möglichkeit hat, die Funktionen für jeden Videokanal einzeln einzurichten, haben alle Kamerakanäle die gleiche (maximale) Anzahl von verfügbaren Masken. Allerdings funktionieren die Masken in diesem Fall nur für den Übersichtskanal. Die Einstellungen für Privatsphärenmasken für andere Kanäle werden ignoriert.

Das Beispiel des Wisenet PNM-9030V unterstützt die Funktion der Privatsphärenmaskierung nur für den Kanal „Übersicht“.

Das Bild für die anderen Kanäle unterstützt keine Privacy-Masking-Funktion. Daher können alle Objekte, die im Bild des Kanals „Übersicht“ durch Masken verdeckt sind, auf den anderen Kanälen leicht gesehen werden.Dies ist das Konzept von Hanwha und wird in den Spezifikationen der Kamera erwähnt.

Die SNB-9000-Kamera (Firmware-Version 1.02_160215) kann den Codec nicht per SUNAPI-Aufruf ändern.

Dies ist ein kamerabezogenes Problem, das dem Hanwha Techwin-Support gemeldet wurde. Allerdings gibt es derzeit keine Pläne für die Veröffentlichung einer neuen Firmware-Version.

Bitte ändern Sie den Codec manuell über das Web-Interface, falls Sie Probleme mit der Anwendung der Videoeinstellungen haben sollten.

Die SNB-9000-Kamera ändert die Auflösung bei Alarm (CCRiA-Funktion) innerhalb von 8 Sekunden. Dieses Verhalten wird durch verschiedene Verzögerungen auf der Kameraseite während der Neuübertragung des Streams verursacht und kann auf der Treiberseite nicht verbessert werden. Die Änderung der Bildrate im Alarmfall (CCFiA) dauert aufgrund des ähnlichen Kameraverhaltens 2 Sekunden.

Bitte beachten Sie diese Einschränkungen, wenn Sie CCRiA/CCFiA-Funktionen mit dieser Kamera in Ihrem Setup verwenden möchten.

Der Treiber erlaubt nicht die Verwendung der PTZ-Funktionalität für Kameras mit „Cropped image"-Funktionen (wie SNB-9000 oder SNV-8080 Kameras).

Die Kameras mit motorisierten Fokus/Zoom-Objektiven unterstützen kein kontinuierliches Zoomen/Fokussieren wie PTZ-Kameras. Die Zoom-/Fokusänderung wird als schrittweise Einstellung im Web-Interface verwendet. Daher erfolgt die Zoom-/Fokusänderung diskret. Der Treiber sendet auch weiterhin wiederholbare Schrittbefehle, während die Zoom-/Fokustaste gedrückt wird, um eine kontinuierliche Bewegung zu emulieren.

Hanwha-Box-Kameras (mit 'B'-Zeichen im Modell, wie XNB-xxxx oder QNB-xxxx) unterstützen die Funktion Externes PTZ, die es ermöglicht, die Kamera mit der PT-Plattform zu verwenden. Leider gibt es keine Möglichkeit, über HTTP-API-Aufrufe zu erkennen, ob die Kamera mit der PT-Plattform verbunden ist oder nicht, so dass Box-Kameras mit Unterstützung der externen PTZ-Funktion als PTZ-Kameras erkannt werden. Dies ist eine Einschränkung der HTTP-API/Kamerahardware.

Die Geräte von Hanwha haben die folgenden Einschränkungen für die Namen der voreingestellten Positionen:

- Es sind nur alphanumerische Zeichen (A-Z, a-z, 0-9) erlaubt;
- Die Länge des Voreinstellungsnamens ist auf 12 Symbole begrenzt.

Als Ergebnis speichert der Treiber seit Version 1.0.2.0 die Preset-Positionen in '*.preset' XML-Dateien. Falls die Datei keine Preset-Positionen enthält, versucht der Treiber, aktuelle Informationen über Preset-Positionen aus dem Wisenet IP-Gerät zu laden.

Die Verwendung der XML-Speicherung ermöglicht auch die Verwendung von Unicode-Symbolen in voreingestellten Positionsnamen.

Der Wert für die GOV-Länge wird für das Aufnahmeprofil automatisch auf die Hälfte der aktuellen Bildrate (d. h. 2 Schlüsselbilder pro Sekunde) festgelegt und kann nicht über die Webschnittstelle oder über HTTP-API-Befehle angepasst werden. Wählen Sie ein anderes Profil als „Aufnahme"-Profil, wenn diese Einschränkung für Ihre Konfiguration nicht geeignet ist.

Das Multisensor-Wisenet IP-Gerät kann für verschiedene Kanäle unterschiedliche Auflösungsmöglichkeiten haben. Zum Beispiel unterstützt das PNM-9030V-Beispiel 6096x2540 und 2688x1120 Auflösungen für den ersten Kanal, bis zu 2592x1944 Auflösungen für die nächsten 4 Kanäle und bis zu 1920x1080 für den 6. und 7.

Leider hat das VMS keine Möglichkeit, verschiedene Auflösungen für verschiedene Kanäle festzulegen - dies ist eine Einschränkung der Softwarearchitektur. Mit anderen Worten, alle Auflösungen (6096x2540, 2688x1120 und 2592x1944) werden für alle Kanäle verfügbar sein.

Falls die gewählte Auflösung vom Kanal nicht unterstützt wird, wird stattdessen die nächsthöhere oder maximale Auflösung verwendet. In unserem Beispiel wird im Falle der Auswahl von 2592x1944 die Auflösung 2688x1120 für den ersten Kanal und 1920x1080 für den siebten Kanal verwendet.

Der Audiokanal verwendet dasselbe Videoprofil, das auch für den Empfang des Aufzeichnungsvideostroms verwendet wird.

Dies kann zu Konflikten in der Multicast-Konfiguration führen, die vom Videokanal (aus der dynamischen UI-Konfiguration) und vom Audiokanal (aus der XML-Datei geladen) angewendet wird.

Der Audiokanal ändert also die Multicast-Konfiguration nur dann, wenn sie noch nicht vom Videokanal geändert wurde. Ansonsten wird die bestehende Multicast-Konfiguration für das Multicasting des Audiostroms verwendet.

Das Videoprofil des Geräts wird für den Empfang und das Senden von Audio verwendet. Jede Änderung der Videoprofileinstellung, die zu einem Neustart der RTSP-Sitzung führt, kann auch ein erneutes Abonnieren des Audiostroms verursachen.

DVMS hat keine Möglichkeit, die Audioeinstellungen im System Manager zu konfigurieren, daher sollten diese Einstellungen über eine XML-Konfigurationsdatei konfiguriert werden.

Standardmäßig wird nur der Audio-Encoder (Option <Encoding>) angegeben: AAC für den Audioeingang und G.711 für den Audioausgang. Die anderen Audio-Optionen (einschließlich Lautstärke/Verstärkung) sind so konfiguriert, dass sie die Werte verwenden, die derzeit im Web-Interface der Kamera ausgewählt sind.

Wisenet-Kameras können eine Begrenzung der Bildrate aufweisen, die von der Anzahl der gleichzeitig gestreamten Profile abhängt:

- Die neue Q-Serie unterstützt 1920x1080 Streams mit insgesamt 45 fps. Die Kamera QND-6082R unterstützt beispielsweise bis zu 30 Bilder/s für H.264-Streams mit einer maximalen Auflösung von 1920x1080. Beim Streaming von einem einzigen Profil liefert die Kamera einen Stream mit 30 fps. Beim Streaming von 2 verschiedenen Profilen mit denselben H.264 1080p @ 30 fps Stream-Einstellungen streamt die Kamera jedoch jedes Profil nur mit 22 fps.New L-series can support 1920x1080 stream by total 30fps.
- Das Mirasys VMS hat ein Problem mit der Dekodierung von G.726-Audiostreams von verschiedenen Samples wie Wisenet XND-8080R. Das Problem wird in den nächsten Treiberversionen behoben. Bitte verwenden Sie G.711 oder AAC-Kodierung, falls Sie Probleme mit der G.726-Audiodekodierung haben.

Der Treiber unterstützt nur die neue Version der Edge-Storage-Funktion, die seit VMS Version 8.0 verfügbar ist. Die Edge-Storage-Funktion wird bei früheren DVMS-Versionen nicht erkannt.

Die Wisenet SNF-8010 Kamera hat ein Problem mit der Suche nach aufgezeichneten Datenintervallen: Sie erkennt nur Intervalle, deren Beginn und Ende innerhalb des gewünschten Zeitraums liegen. Andere Kameramuster

erkennen auch Überschneidungen (d. h. die Startzeit der Aufzeichnung liegt vor dem angeforderten Zeitraum, und die Endzeit liegt innerhalb oder nach dem Zeitraum).

Die SNF-8010-Kamera ist bereits abgekündigt (seit 2018), so dass das Problem auf der Kameraseite nicht behoben werden kann. Mirasys hat auch keine Pläne, dem Treiber eine separate Verarbeitungslogik für einzelne Modelle hinzuzufügen.

Die verschiedenen Multisensorgeräte unterstützen die Aufzeichnung von Material über eine begrenzte Anzahl von Kanälen.

Das Beispiel des PNM-9030V erlaubt beispielsweise nur die Aufzeichnung von Videos über den Kanal „Übersicht".

In diesem Fall verwendet der Treiber die Edge-Storage-Funktion nur für Kanäle, die in der Attributgruppe „Aufzeichnung" die Fähigkeit „Aufzeichnung" aufweisen.

Die SUNAPI v2.x-Spezifikationen haben die folgenden Einschränkungen für HTTP- und RTSP-Anfragen im Zusammenhang mit der Verarbeitung von Speicherfunktionen:

- Die Millisekunden sind nicht verfügbar;
- Die Zeit sollte bei allen Anfragen im lokalen Format angegeben werden (keine UTC-Unterstützung);
- Die vom Gerät zurückgegebenen Zeitintervalle sind ebenfalls in Ortszeit.

Diese Einschränkungen können die folgenden Probleme verursachen:

- Da die Zeitauflösung eine Sekunde beträgt, kann der Wechsel zwischen Aufzeichnungs- und Kantenmaterial und umgekehrt zu wiederholbaren Fragmenten führen, die nicht länger als eine Sekunde dauern, oder es können Daten fehlen, die nicht länger als eine Sekunde sind;
- Die Umrechnung zwischen Ortszeit und UTC-Zeit kann zu Problemen bei der Materialauswahl während der Umstellung auf oder von der Sommerzeit (DST) führen;
- Ein Wechsel der Zeitzone kann dazu führen, dass beim Intervallempfang ein falsches Zeitintervall gewählt wird;
- Die Wisenet-Geräte unterstützen nur eine RTSP-Verbindung für die gleichzeitige Wiedergabe. Im Falle der Verwendung eines Geräts mit mehreren Kanälen werden die verlorenen Daten also nacheinander von der SD-Karte des Geräts empfangen: alle Intervalle von allen Kanälen werden in eine einzige Warteschlange gestellt und nur dann aus der Warteschlange extrahiert, wenn gerade keine anderen Intervalle verarbeitet werden.

Der Treiber kann mit Windows 7 oder neueren Betriebssystemen verwendet werden. Ältere Betriebssysteme werden nicht unterstützt.

Für **WisenetRoadAI** ist der genaueste Erkennungsmodus **„On lost"** – er liefert die korrektesten Ergebnisse. Für eine schnellere Erkennung kann der Modus **„On reliable"** verwendet werden. In diesem Fall erfolgt die Erkennung

schneller, kann jedoch gelegentlich zu falschen Erkennungen führen. Die Modi **„On detect“** und **„On update“** werden nicht empfohlen. Das Metadatenformat sollte auf **„Onvif“** eingestellt sein (wird vom Treiber erzwungen).

Die **WisenetRoadAI**-Anwendung kann im Tab **Events** unterschiedliche Ergebnisse anzeigen, im Tab **Search** werden jedoch dieselben Ergebnisse angezeigt, wenn der Modus **„On lost“** verwendet wird.

9.7.4 Installieren von Metadatentreibern

Es ist möglich, neue Metadatentreiber mit der Option **Metadatentreiber installieren** – auf der Registerkarte **System** zu aktualisieren und zu installieren.

9.7.5 Client-Treiber installieren

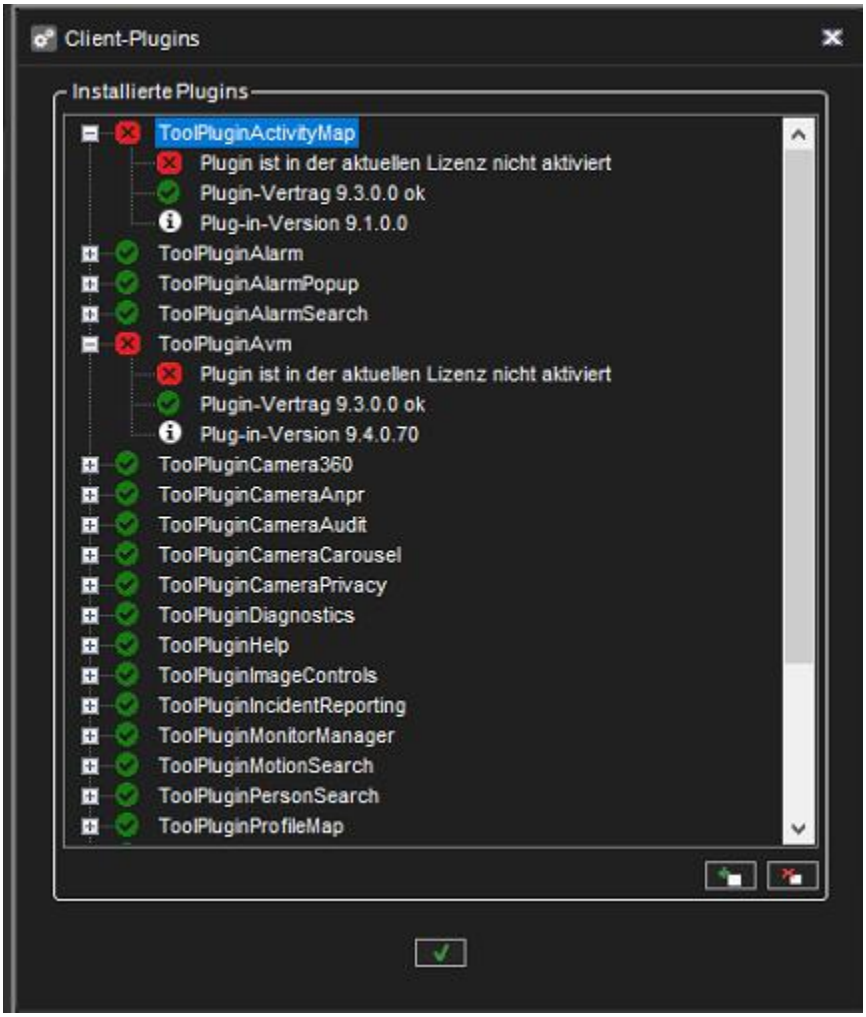
ThruCast (direktes Streaming von der Kamera zum Spotter-Client) erfordert einen anderen Kameratreibertyp.

Diese werden als (verwaltete) ThruCast Client-Treiber bezeichnet.

Die Client-Kamera-Treiber werden ähnlich wie Spotter-Plugins und Metadaten-Treiber installiert, indem die Option **Client-Treiber installieren** im Systemmanager verwendet wird.

9.7.6 Client-Plugin installieren

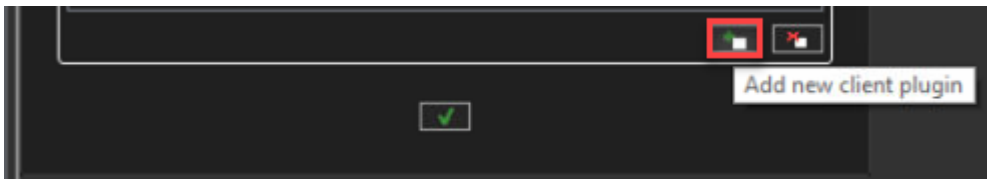
Client-Plugins für Benutzeroberflächen wie Spotter können über den System Manager installiert werden.



Die Plugin-Installation kann über die Registerkarte System unter Add-Ins geöffnet werden.

9.7.6.1 So installieren Sie ein Client-Plugin:

1. Öffnen Sie das **Client-Plugin installieren**.
2. Klicken Sie auf **Neues Client-Plugin hinzufügen**. Suchen Sie nach der richtigen Datei und wählen Sie sie aus.



3. Suchen Sie das Plugin-Paket (.zip-Datei) und wählen Sie es aus und klicken Sie auf **OK**. Die Dialogbox **Install Plugin** wird angezeigt.

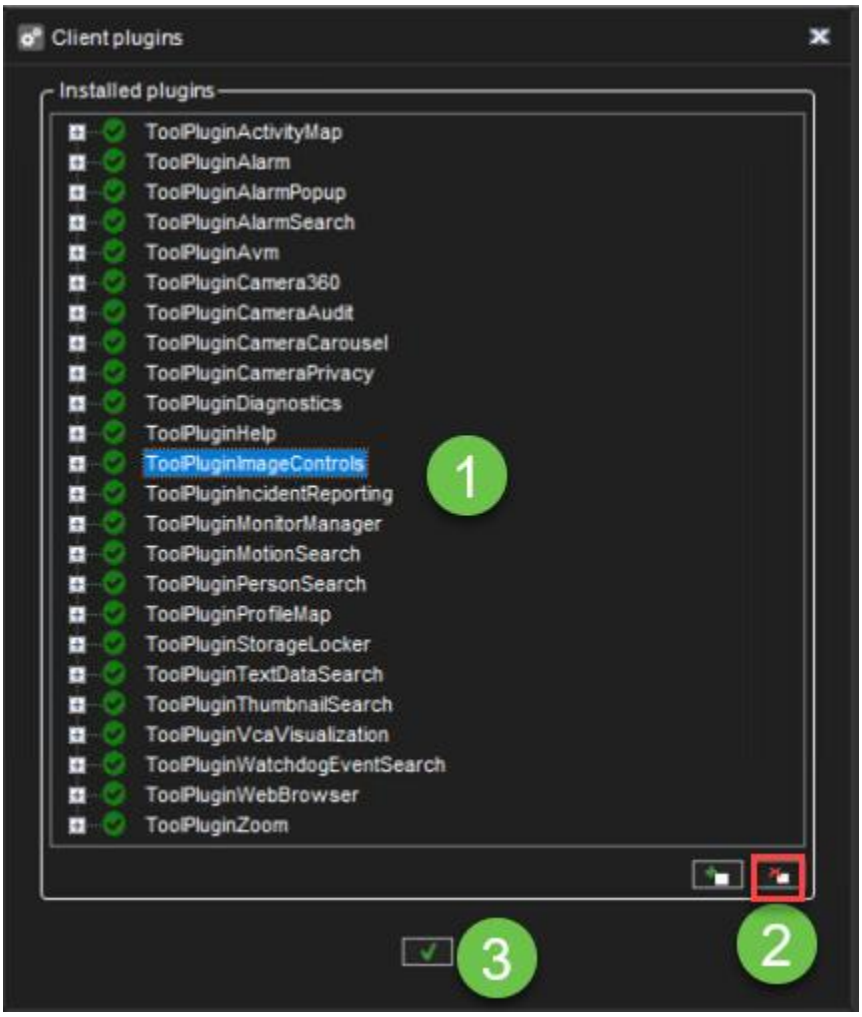
4. Wenn Sie das System zwingen möchten, die Treiberpaketversion zu installieren, wählen Sie **Treiber installieren, auch wenn dieselbe oder eine neuere Version vorhanden ist.**

5. Klick **Ok**

9.7.6.2 So entfernen Sie ein Client-Plugin:

Öffnen Sie das **Client-Plugin installieren**

1. Plug-in aus der Liste auswählen
2. Klicken **Client-Plugin entfernen**
3. Klick **Ok**



10 VMS-Servers

Auf der Registerkarte **VMS Servers** können Sie diese Einstellungen für jeden Server konfigurieren:

Symbol	Name	Beschreibung
	Allgemein	Ändern Sie den Namen und die Beschreibung des Servers. Hier finden Sie auch die IP-Adresse des Servers.
	Port-Weiterleitung	Benutzer können sehen, was die automatische Portweiterleitung als Ports für diesen Server konfiguriert hat. Die Ports können bei Bedarf geändert werden.
	Hardware	Fügen Sie IP-Kameras hinzu und wählen Sie Kamera- und Audiotreiber aus.
	Kameras	Ändern Sie Kameraparameter, Aufnahmezeitpläne und Bewegungserkennungseinstellungen.
	Audio	Ändern Sie die Audioerkennungseinstellungen und Aufnahmezeitpläne.
	Digitale E/A	Legen Sie die digitalen E/A-Einstellungen fest.
	Alarm	Richten Sie Alarmbedingungen und Alarmaktionen ein.
	Lagerung	Fügen Sie einem Server eine Festplatte hinzu und legen Sie die Speicherzeiten für Video-, Audio- und Alarmdateien fest.
	Textkanäle	Legen Sie hier die Namen und Beschreibungen von Textdatenkanälen fest.

10.1 Um auf die Einstellungen zuzugreifen, führen Sie einen der folgenden Schritte aus:

- Wählen Sie die Einstellungen aus, die Sie konfigurieren möchten (z. B. Kameras) und klicken Sie dann auf **Bearbeiten**



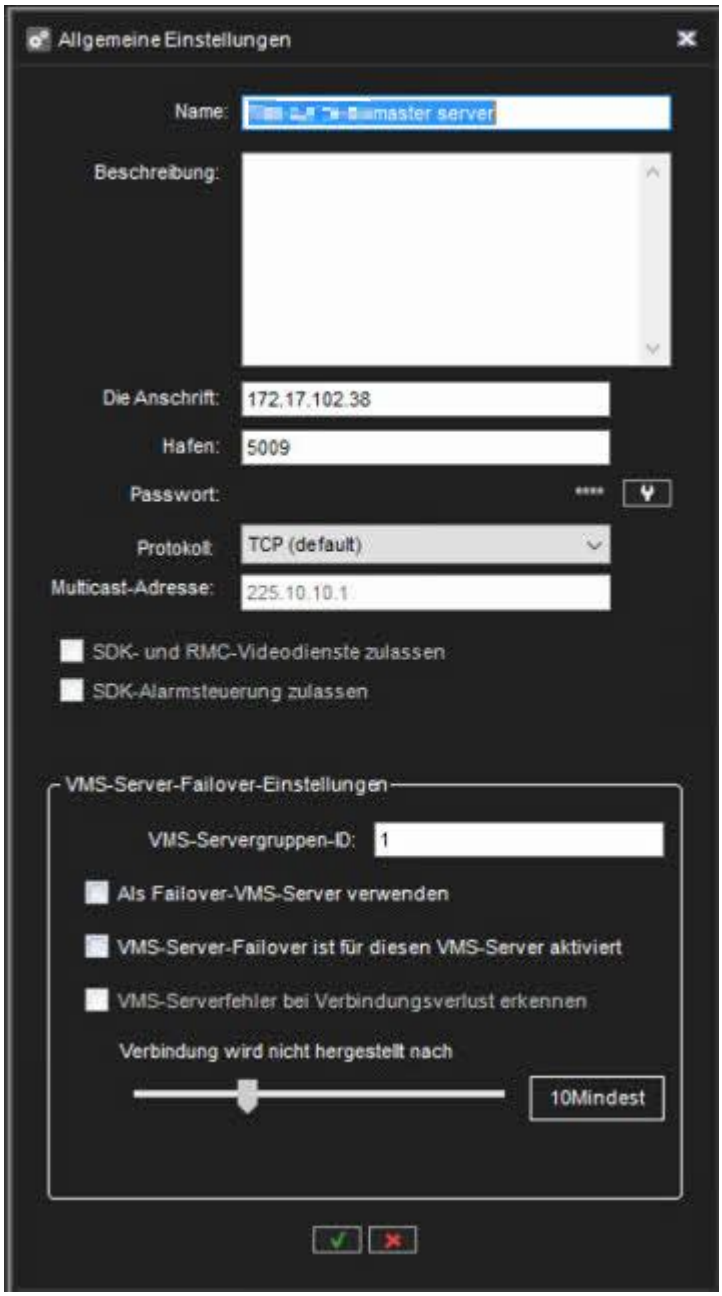
in der unteren rechten Ecke des Navigationsbereichs.

- Doppelklicken Sie auf die Einstellungen, die Sie konfigurieren möchten.
- Ziehen Sie die Einstellungen von der Registerkarte **VMS Servers** in den Arbeitsbereich.

10.2 Allgemein

- VMS-Servername
- Beschreibung

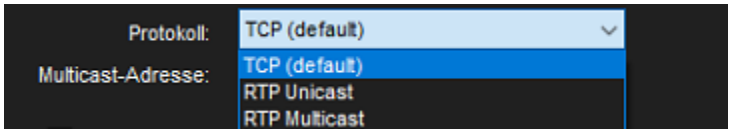
- Passwort
- Protokoll
- Multicast-Adresse
- VMS-Server-Failover-Einstellungen



10.2.1 Multicast-Adresse

Wenn ein einzelner Workstation-Stream mehrmals geöffnet wird, werden der Server – und das Netzwerk – unnötig belastet, da jeder Stream als separate Einheit behandelt wird.
Multi-Casting ermöglicht das gleichzeitige Öffnen und Senden eines einzelnen Streams an mehrere Workstations.
Bei Verwendung von Multi -casting wird der Stream für jeden Videokanal nur einmal an das LAN gesendet.
Alle Anwendungen im LAN können den einzelnen Stream empfangen, sodass die Nutzung der Netzwerkbandbreite geringer ist als beim separaten Senden eines Streams für jede Anwendung.
Die Funktion muss konfiguriert werden im System Manager und über die Netzwerkeinstellungen.
Bitte wenden Sie sich an Ihren Netzwerkinfrastrukturdienst, um Informationen zum Aktivieren der Multicasting-Unterstützung auf Netzwerkebene zu erhalten.

So konfigurieren Sie Multicasting in System Manager:



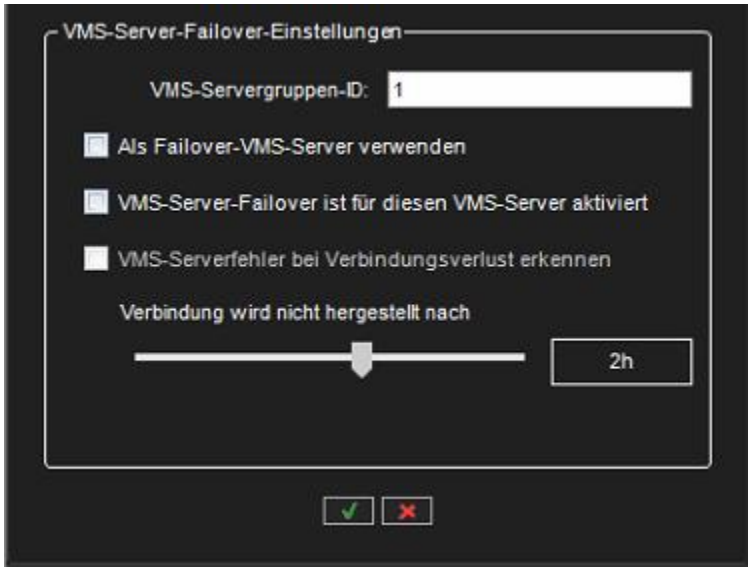
1. Ändern Sie in den allgemeinen Einstellungen des Servers das Protokoll von **TCP (Standard)** auf **RTP Multicast**.
2. Bearbeiten Sie die Multicast-Adresse.
3. Wiederholen Sie die Schritte 1-2 für alle erforderlichen Server im System. Notiz: Jede Multicast-Adresse muss separat sein.

10.2.2 VMS-Server-Failover-Einstellungen

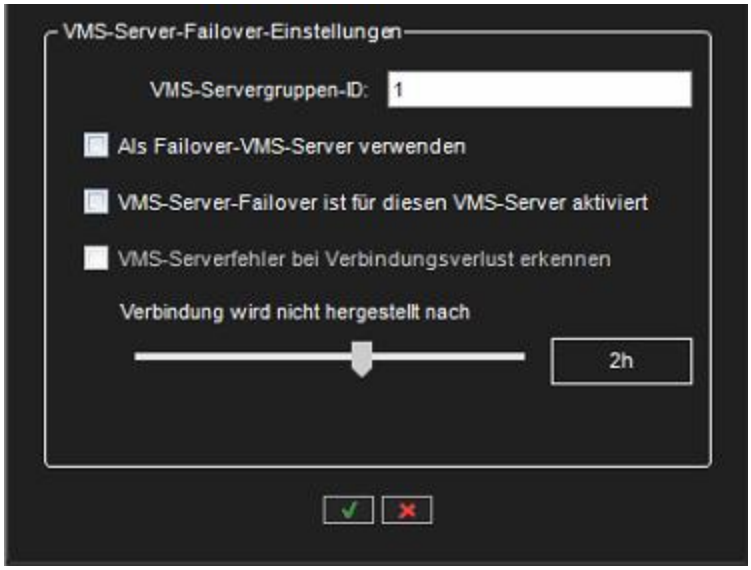
Beim Hinzufügen eines neuen Servers zum System kann dieser als Failover-Server definiert werden.
Ein Failover-Server ist ein Backup-Server, der alle Serveraufgaben übernehmen soll, von denen festgestellt wurde, dass sie unter Failover-Schutz stehen.

Failover-Server müssen das gleiche Dateisystem (dasselbe Laufwerk) haben Buchstaben) als VMS-Server unter Failover-Schutz, und sie können nur für Backup-Zwecke von IP-Kameras verwendet werden unzugänglich sind, wurden sie in den Ordner *„Ausgefallene VMS-Server“* verschoben.

Jeder verfügbare Failover-Server übernimmt die Verantwortung für den ausgefallenen Server.
Failover-Einstellungen können über die allgemeinen Einstellungen des ausgewählten Servers gesteuert werden.
Der Failover-Übergang wird durchgeführt, wenn alle Materialfestplatten defekt sind oder der Server länger als eine definierte Zeit nicht erreichbar ist.



Wenn beispielsweise unter Failover-Schutz länger als 2 Stunden nicht zugegriffen werden kann, wird die Failover-Umschaltung ausgeführt.



10.2.3 Failover verzögern, um Datenverlust zu vermeiden

Der Failover-Prozess wurde aktualisiert, um Datenverluste während des Failover-Prozesses, z. B. während der Aktualisierung des Rekorders zu verhindern.

Beim Kopieren von Material aus dem Failover-Recorder prüft der wiederhergestellte Recorder zuerst seine aufgezeichneten Daten und kopiert dann nur fehlendes Material (einschließlich Video, Audio, Textdaten, Metadaten und ANPR-Daten).

Diese Funktion kann im Dialogfeld System-Manager > VMS-Server allgemein (Kontrollkästchen Auf den Rekorder warten, um Einstellungen zu übernehmen) aktiviert werden.

Delay Failover kann nur für Rekorder ab V9.7 aktiviert werden, da Rekorder vor V9.7 keine selektive Materialkopie unterstützen und sich die Daten überschneiden.

10.3 Port-Weiterleitung

10.3.1 Die Grundidee bei der Portweiterleitung besteht darin, dass auf einen oder mehrere VMS-Server oder Hauptserver hinter einem Router zugreifen kann, der Network Address Translation (NAT) durchführt.

10.3.2 Normalerweise tritt diese Situation auf, wenn sich der Client außerhalb des Netzwerks befindet und auf Server innerhalb eines Unternehmensnetzwerks zugreifen muss.

Bei der Installation eines VMS-Servers bietet der Installer die Möglichkeit, die automatische Portweiterleitung einzuschalten. Der Standardzustand ist aus
Wenn die Portweiterleitung bei der Installation des Systems nicht aktiviert ist, kann sie über die zweite Registerkarte „VMS-Server“ aktiviert werden.
Öffnen Sie die Ansicht „Portweiterleitung“ und aktivieren Sie die Auswahl „UPnP wird verwendet“.

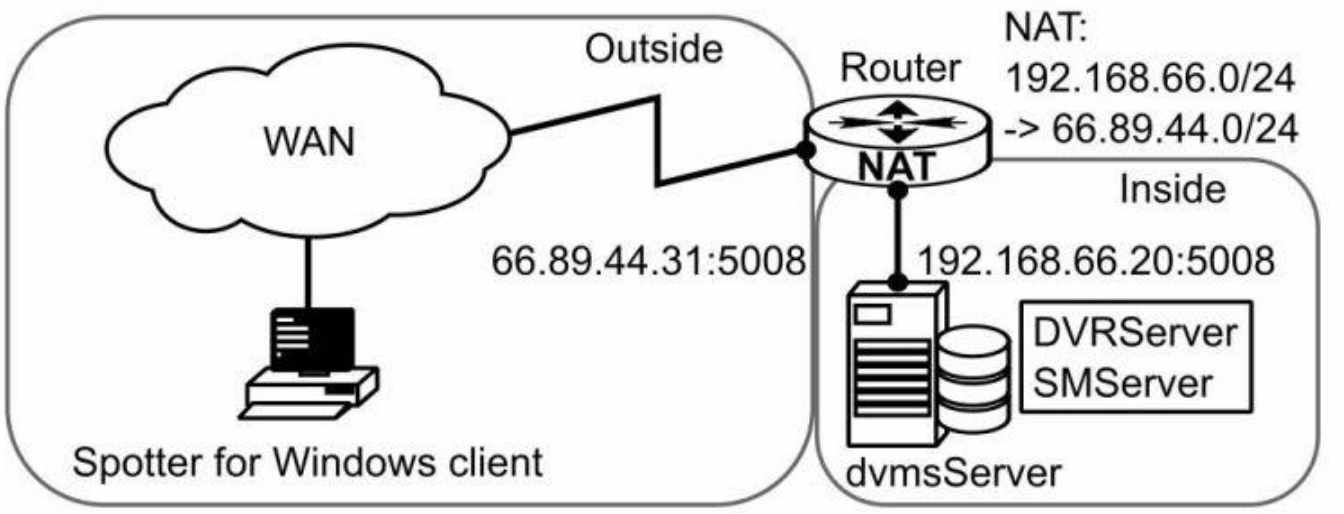
10.3.3 Automatische Router-Konfiguration

Wenn ein VMS-Server startet, versucht er, UPnP-Geräte aus dem Netzwerk zu erkennen.
Der Router muss UPnP (Universal Plug and Play) unterstützen, was auf dem Gerät aktiviert sein muss.
Der Server verfügt über eine kontinuierliche UPnP-Geräteerkennung, wenn er ausgeführt wird Wenn Netzwerkänderungen vorgenommen werden, erkennt der Server automatisch neue Router und führt eine Portweiterleitung zu ihnen durch.
Es werden nur UPnP-Geräte mit externen (WAN-)Adressen erkannt.
Wenn der Benutzer die Portweiterleitung automatisch entfernen möchte, kann er dies über den Systemmanager tun .
Danach erinnert sich der Server daran, dass die Einstellungen entfernt wurden, und leitet die Portweiterleitung nicht an diesen Router weiter.
Die Software erlaubt es nicht, die Portweiterleitungszuordnung zu löschen, wenn der Server mit einer externen Adresse zum System hinzugefügt wird.
Das Löschen der Portweiterleitungszuordnung würde dies tun Trennen Sie das System, und es wäre keine weitere Konfiguration möglich.
Wenn die Weiterleitungs-Port-Einstellungen geändert werden und die Verbindung zum Server nach einer Weile nicht wiederhergestellt wird, kann es erforderlich sein, den neu zu starten router.
Server benötigen vier Ports für die Server-zu-Server-Kommunikation. Der erste Server, der Portweiterleitung durchführt, beansprucht die Ports **5008**, **5009**, **5010** und **5011**.
Der zweite Server beansprucht die Ports 1**5012-5015**, der dritte Server die Ports 5016-5019. Und so weiter. (Vorausgesetzt, alle Ports sind verfügbar).
Der erste Port wird für die SMServer-Kommunikation verwendet (**5008, 5012, 5016…**)

Der zweite Port wird für die DVRServer-Prozesskommunikation verwendet (**5009, 5013, 5017…**)
Bei einer Verbindung zu einem Hauptserver ist der Port normalerweise 5008. Beim Hinzufügen neuer Server zum Hauptserver ist der Port normalerweise 5009. Wenn mehr als ein Server vor Ort ist, dann sind die Ports 5009 + 4, 5009 + 8 usw.

10.3.4 Einzelner Server hinter Router

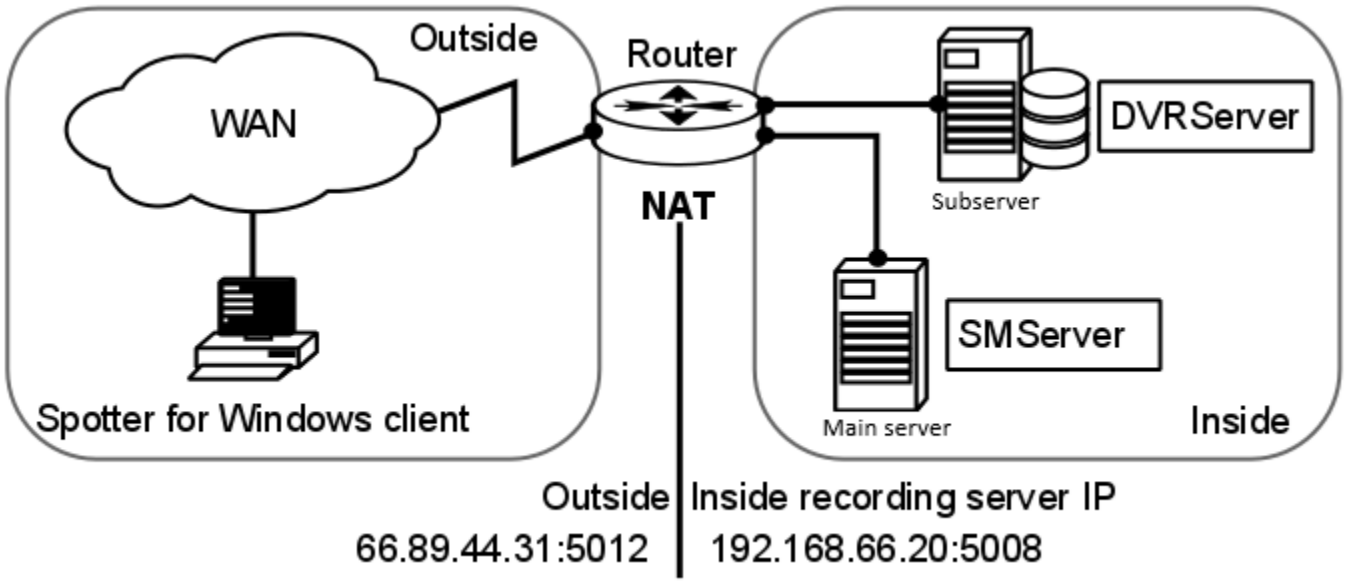
Szenario 1: Verwendung eines Systems mit **a Single Server hinter einem Router/Firewall**



Wenn der Benutzer über das WAN auf einen einzelnen Server zugreift, muss er sich mit dem VMS-Server mit der externen IP-Adresse verbinden, die der Router übersetzt hat.
Der Benutzer kann die Portweiterleitung überprüfen, welcher Port verwendet wird, aber es ist sehr wahrscheinlich Port 5008.

10.3.5 Mehr als ein Server hinter dem Router

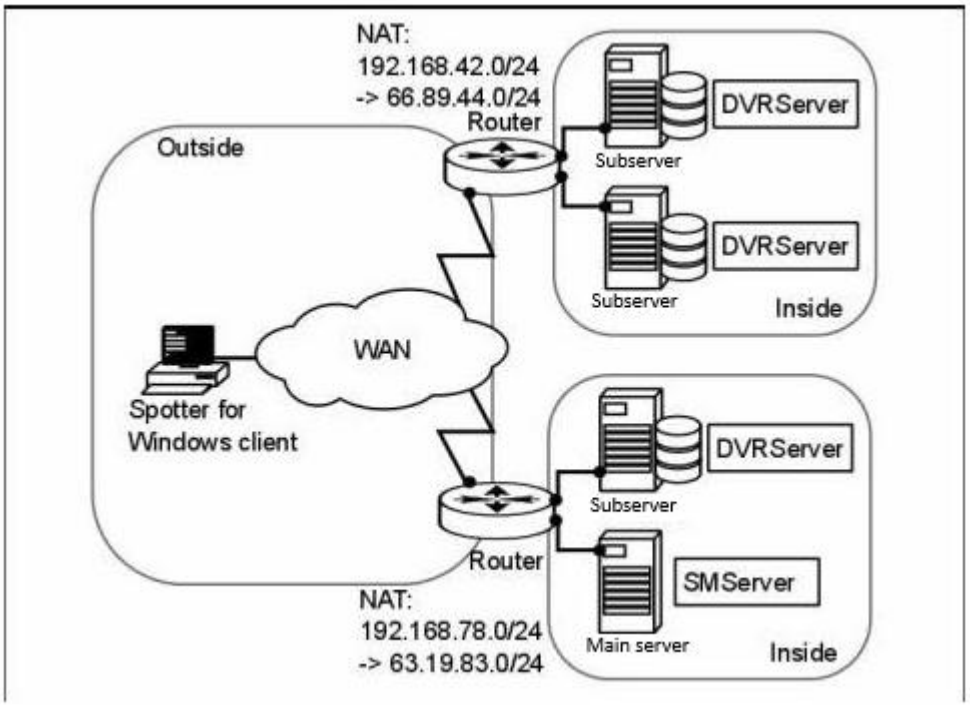
Szenario 2: Mehrere Server hinter einem einzigen Router (WAN-Adresse)



Wenn der Benutzer ein umfangreicheres System mit mehreren Servern an einem einzigen Standort konfiguriert, kann er die Server mit den externen oder internen IP-Adressen zur System Manager-Anwendung hinzufügen. ein Hinweis zeigt, dass er zwischen einer internen IP-Adresse und einer externen IP-Adresse wählen kann.
Wenn der Server aus dem WAN verwendet werden soll, dann sollte die externe IP-Adresse gewählt werden.
Die genauen Ports, auf die der Server eine Port-Weiterleitung vorgenommen hat gefunden werden, indem Sie den System Manager auf dem lokalen Server starten Die Portweiterleitung wurde durchgeführt an.
Wenn der hinzugefügte Server ein einzelner, eigenständiger Server ist, ist der Port höchstwahrscheinlich 5009.
Wenn sich mehrere Server auf derselben Site befinden, erhalten sie höchstwahrscheinlich die Ports beginnend mit **5009, 5013, 5017, 5021**...

10.3.6 Mehr als ein Server auf mehreren Sites

Szenario 3: Mehr als ein Server auf mehr als einer Site



Es gilt das gleiche Prinzip wie in Szenario 2, aber diesmal muss NAT bei der Zuweisung von VMS-Servern an den Master-Server des anderen Standorts berücksichtigt werden.

10.4 HARDWARE

Bevor Sie die Systemmanager-Anwendung verwenden, um nach der Kamera zu suchen, führen Sie bitte die folgenden Schritte aus:

- Konfigurieren Sie die IP-Adresse der Kamera
- Definieren Sie den Benutzernamen und das Passwort für die IP-Kameras
- Stellen Sie sicher, dass Zeitzone und Uhrzeit der Kamera mit denen des VMS-Servers übereinstimmen

MIRASYS


Hardware-Einstellungen 'Local recorder'
Suchtext eingeben
Video
Audio
N...
Name
Modell
Einstellungen
1
Kehä
keha_4k_25fps_h265.wmv
http://keha_4k_25fps_h265.wmv
2
London Walk
London walk.wmv
http://London walk.wmv
3
Camera 3
Hanwha Vision XNP-C6403RW
http://172.16.20.153
Verwendete Kameralizenzen: 3/20
Verwendete Gerätekanäle: 1/1
Geräteeinstellungen
Edge-Speicher
Edge-Speicherabruf für Offline-Zeitraum
Kamera im Passivmodus
360-Kamera
PTZ aktivieren
Name:
Camera 3
Auflösung:
1920x1080
Aufzeichnungsr...
25 / S
Geräteverknüpfu...
A+

Außerdem wurden unterhalb der Liste „Geräte“ im Dialogfeld „Hardwareeinstellungen“ Informationen zur Anzahl der verwendeten/gesamten Lizenzen und zu den verwendeten/gesamten Kanälen für ausgewählte Mehrkanalgeräte hinzugefügt.

10.4.1 Video (Hardware)

Beim Hinzufügen einer IP-Kamera stehen die folgenden Suchmodi zur Verfügung:

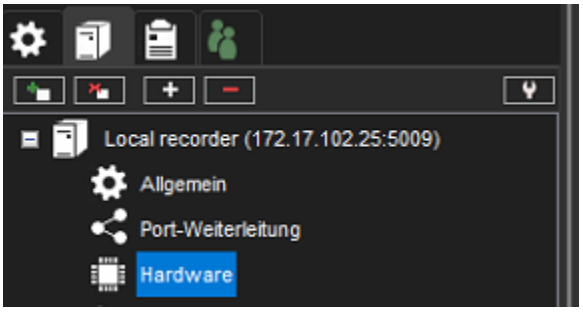
- ***Alle Fahrer***: Automatische Suche mit allen Treibern. Das System versucht, alle verfügbaren Treiber zu verwenden. Das Kombinationsfeld für die Modusoption ist deaktiviert.
- Ausgewählte Treiber: Automatische Suche nur mit bestimmten Treibern. Das System verwendet während der automatischen Suche nur die Fahrer, die über den Dialog Selected Drivers angegeben wurden.
    - Das zusätzliche Kombinationsfeld zeigt alle aktuell ausgewählten Treiber an. Ein Benutzer kann alle verwenden (unter Verwendung der Option „Alle“) oder nur einen Treiber auswählen.
- ***Derzeit aktive Fahrer***: Durchsuchen Sie die Kamera mit allen aktuell verwendeten Treibern. Wenn diese Option ausgewählt ist, verwendet das System nur Treiber, die derzeit für bereits hinzugefügte Kameras verwendet werden.
    - Wenn wir beispielsweise Kameras von Sony und Axis abonniert haben, wird die Suche nur von Sony- und Axis-Treibern durchgeführt.
    - Das Kombinationsfeld für die Modusoption enthält eine Liste der verwendeten Treiber, wenn der Benutzer einen davon verwenden möchte, und eine Option „Alle“, um alle Treiber aus dieser Liste für die Suche zu verwenden.
- ***Fahrer***: Fügen Sie eine Kamera mit einem bestimmten Treiber hinzu. Das System verwendet nur den spezifischen Treiber für die Suche.
    - Das Kombinationsfeld für die Modusoption enthält eine Liste aller installierten Treibernamen, die durchsucht werden sollen.
    - Wenn eine Suche mit angegebenen Treibern fehlschlägt, fragt das System, ob der Benutzer mit allen Treibern suchen möchte.
    - Der aktuell für die Suche verwendete Treiber sollte ebenfalls ausgeschlossen werden.
- ***Kameramodell***: Kamera nach Modellname hinzufügen. Dieser Modus wird zum Hinzufügen einer Kamera verwendet, indem ein älterer Aufnahmetreiber verwendet wird, der vordefinierte Funktionen aus der XML-Datei zur Treiberkonfiguration verwendet.
    - Das Kombinationsfeld für die Modusoption enthält eine Liste der verfügbaren Modelle.

Beim erstmaligen Hinzufügen der neuen Kamera wird standardmäßig der ***Ausgewählte Treiber*** -Modus ausgewählt.

Wenn der Dialog das nächste Mal geöffnet wird, erinnert sich das System an das vorherige Modell und die vorherige Treiberauswahl, damit der Benutzer ähnliche Kameras schneller hinzufügen kann Modus-Options-Kombinationsfeld (außer Kameras, die durch Mod hinzugefügt wurden, el natürlich).
Das System speichert die zuletzt verwendeten Optionen zum Ändern von Fällen nicht, da die Optionen nur zum Hinzufügen von Kameras verfügbar sind

10.4.1.1 Gerät hinzufügen

IP-Kameras oder analoge Videoserver (Encoder) können über die Registerkarte **Video** von **Hardware-Einstellungen** verwaltet werden.



So fügen Sie eine neue IP-Kamera hinzu, wenn die IP-Adresse bekannt ist:

1. Klicken Sie auf der Registerkarte **Video** auf **Gerät hinzufügen**

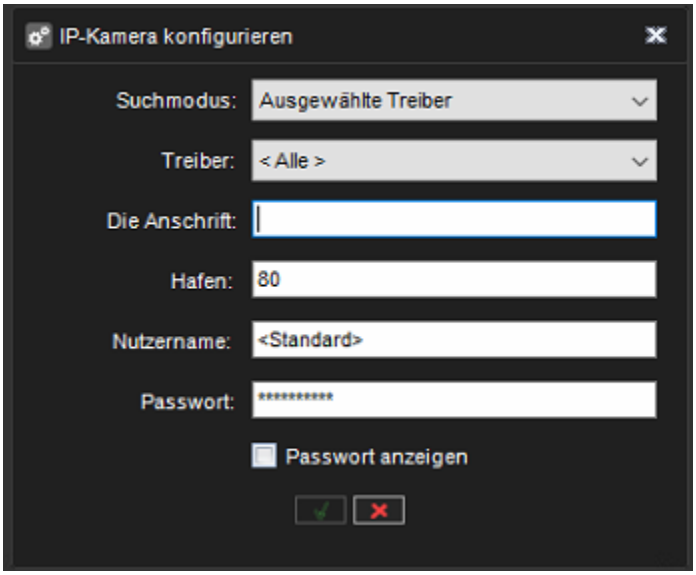


2. Geben Sie die IP-Adresse oder den DNS-Namen der Kamera oder des Videoservers ein.

- Ändern Sie bei Bedarf die Portnummer. Normalerweise wird Port 80 verwendet.

3. Geben Sie den Benutzernamen und das Kennwort für die Kamera ein.

4. Klicken Sie auf **OK**.

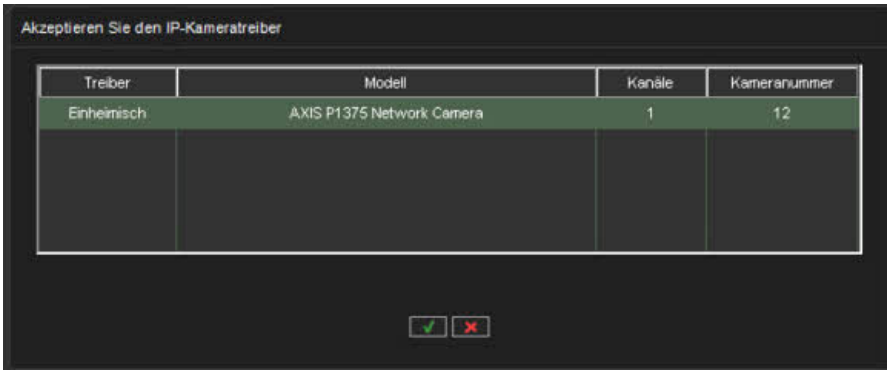


The system will now communicate with the camera and display which drivers can connect to the camera.
The camera may support **ONVIF**. In diesem Fall kann es auch der **ONVIF** -Treiber erkennen.

5. Wählen Sie einen Treiber aus der Liste aus.

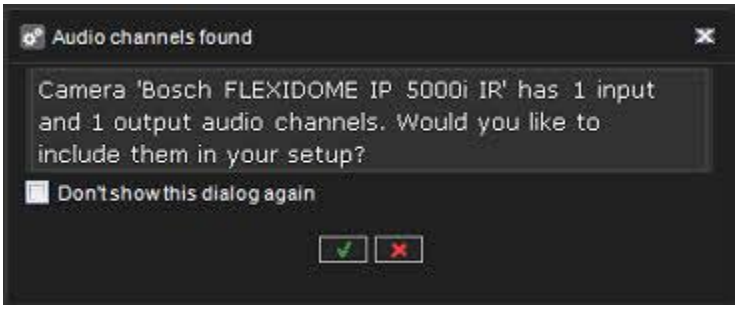
In der Regel wird empfohlen, den **Nativen** Treiber zu verwenden, falls vorhanden.
Bei Mehrkanalgeräten kann die Option **Kanäle** das Gerät mit weniger als der maximalen Anzahl von Kanälen hinzufügen.
Der Benutzer kann auch sehen, welche Kameranummer das Gerät haben wird

6. Klicken **OK**

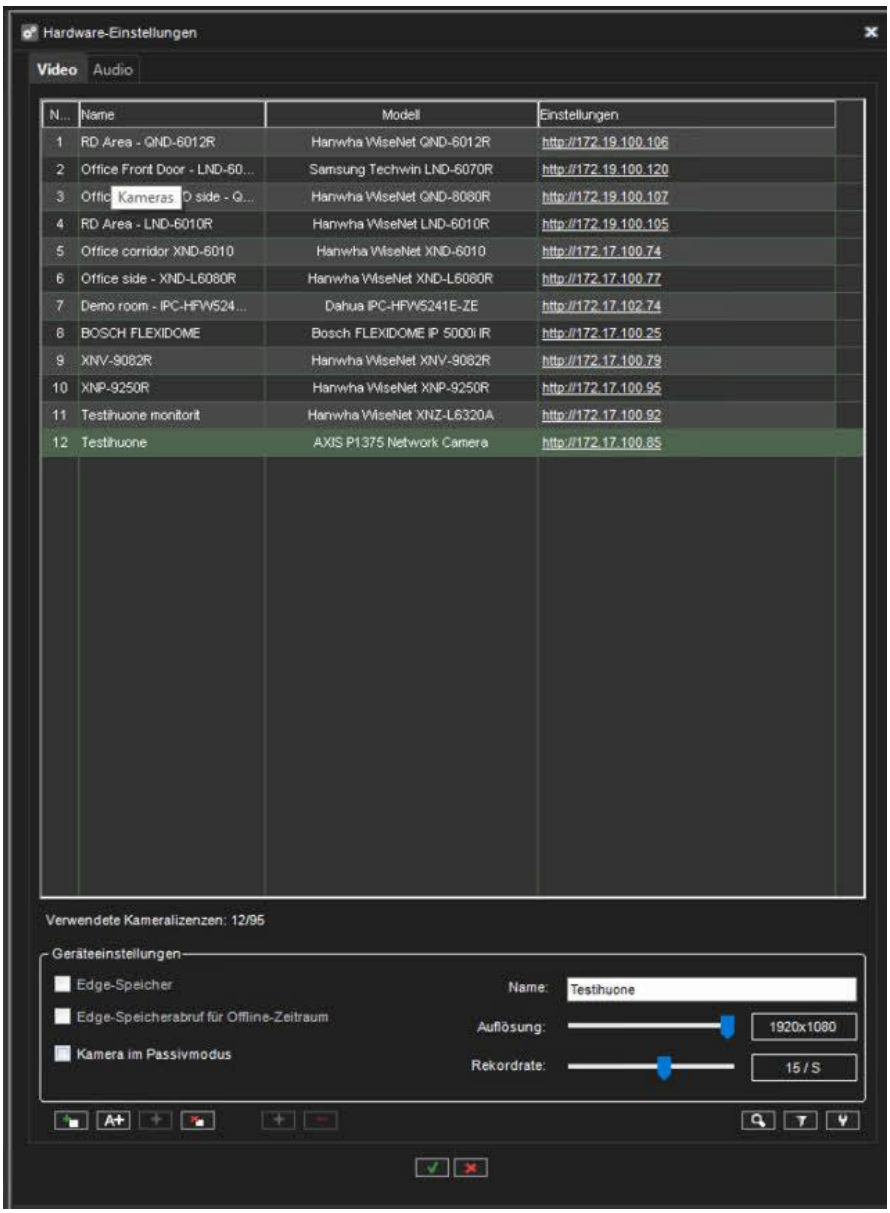


Wenn die Kamera Audiokanäle unterstützt, sehen Sie einen Dialog darüber.

7. Klicken Sie auf **OK** um auch Audiokanäle hinzuzufügen oder **X** fügen Sie nur einen Videokanal hinzu



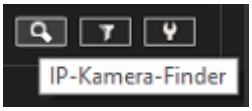
Nachdem die Kamera hinzugefügt wurde, kann das Gerät in der Liste **Hardware-Einstellungen** gefunden werden



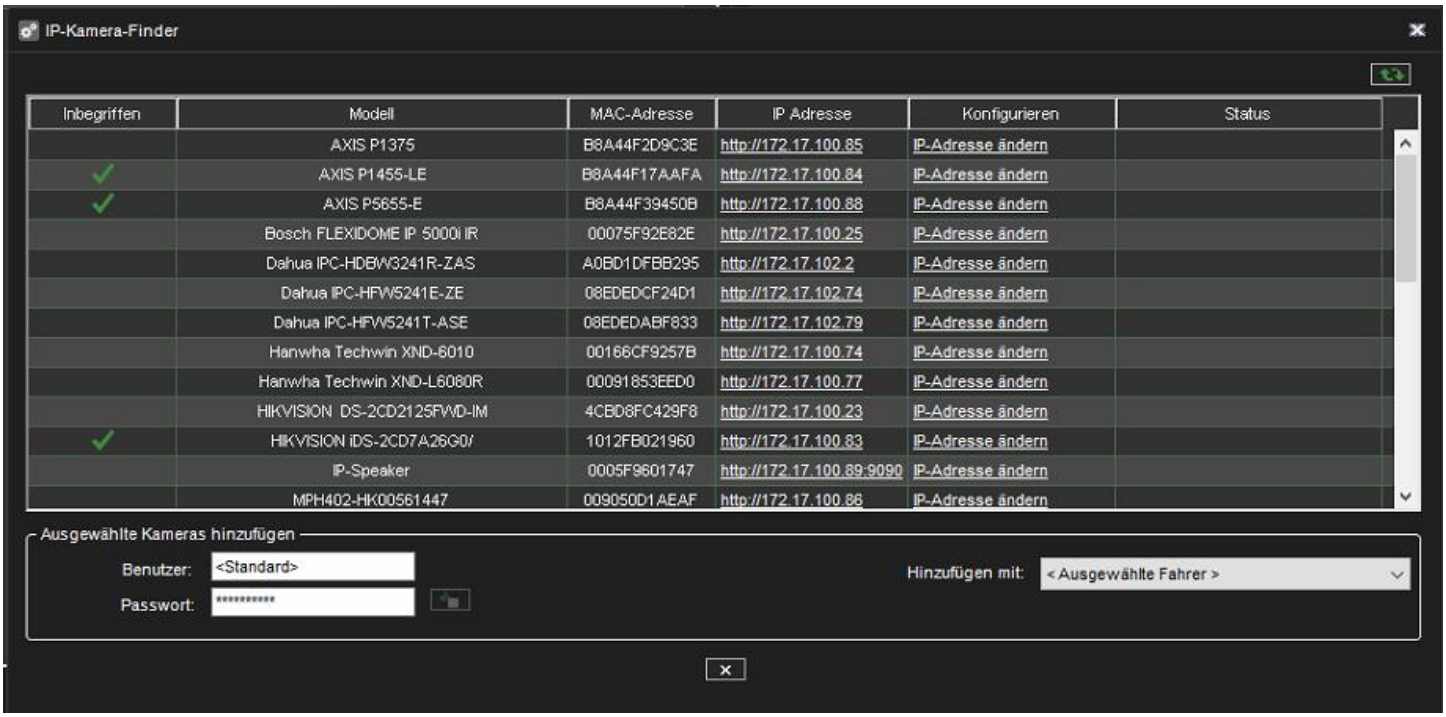
Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

10.4.1.2 IP-Kamera-Finder

1. Klicken Sie auf den **IP-Kamerafinder**



Das System scannt nun das lokale IP-Netzwerk nach aktiven IP-Adressen und kommuniziert dann mit jeder gefundenen IP-Adresse, wenn es sich um eine unterstützte IP-Kamera handelt.
Die Ergebnisliste wird nach Abschluss der Suche angezeigt.



Kameras können aus der Liste ausgewählt werden. Die Auswahl mehrerer Kameras ist mit den Tasten SHIFT oder CTRL möglich.

1. Geben Sie den Benutzernamen und das Kennwort für die Kameras ein.
2. Klicken Sie auf **Ausgewählte Kameras hinzufügen**.



3. Das System fügt dem System die ausgewählten Kameras mit dem ausgewählten Benutzernamen und Passwort hinzu.

4. Wenn das System einige der ausgewählten Kameras nicht hinzufügen kann, wird eine Fehlermeldung in der Spalte **Status** angezeigt; Sie können die Schritte 4 bis 5 für die Kameras mit den richtigen Anmeldeinformationen wiederholen.

5. Klicken Sie auf **Schließen**, um den **IP-Kamerafinder** zu beenden.

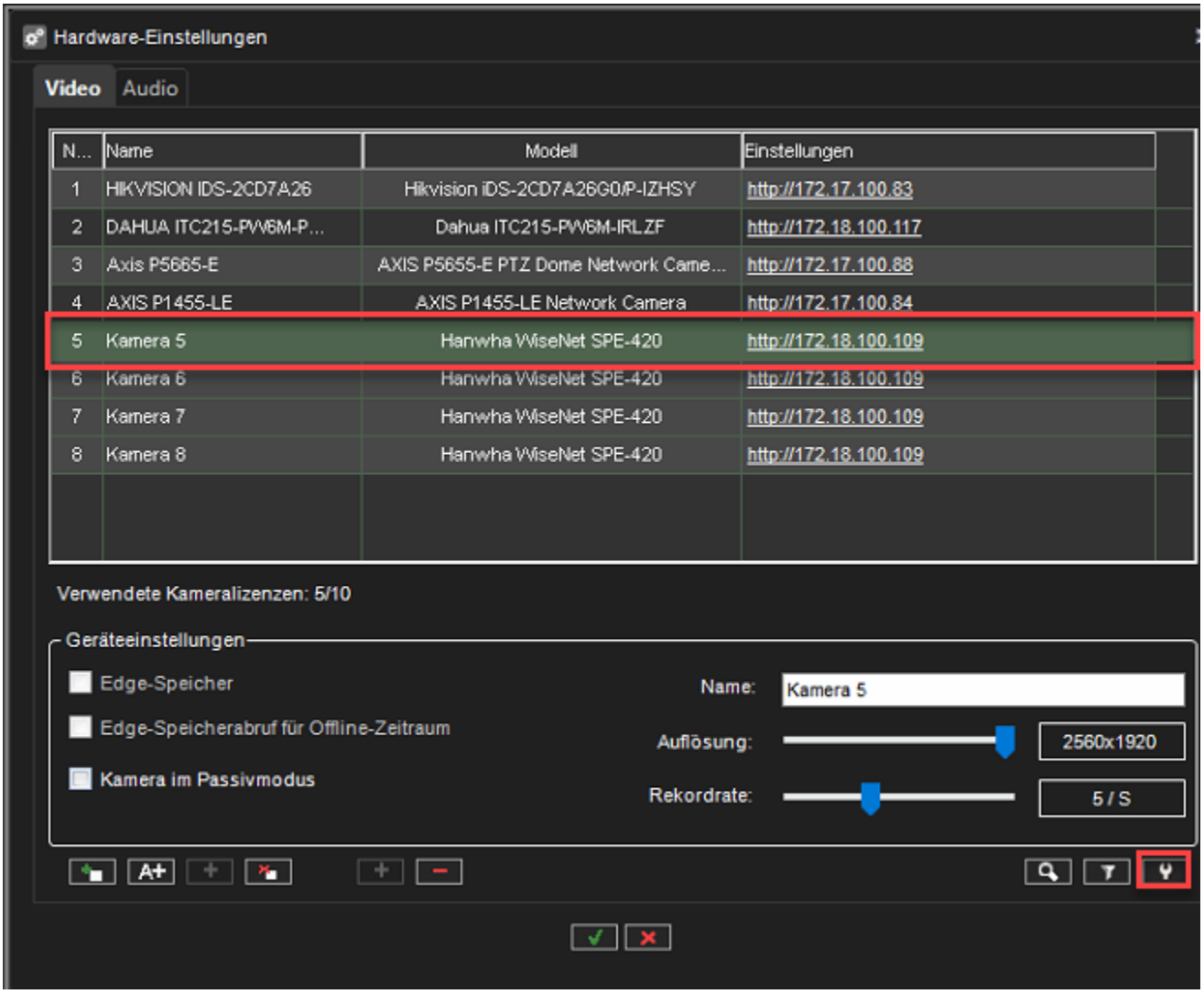
6. Speichern Sie die Hardware-Einstellungen durch Drücken von **OK** in der Liste:



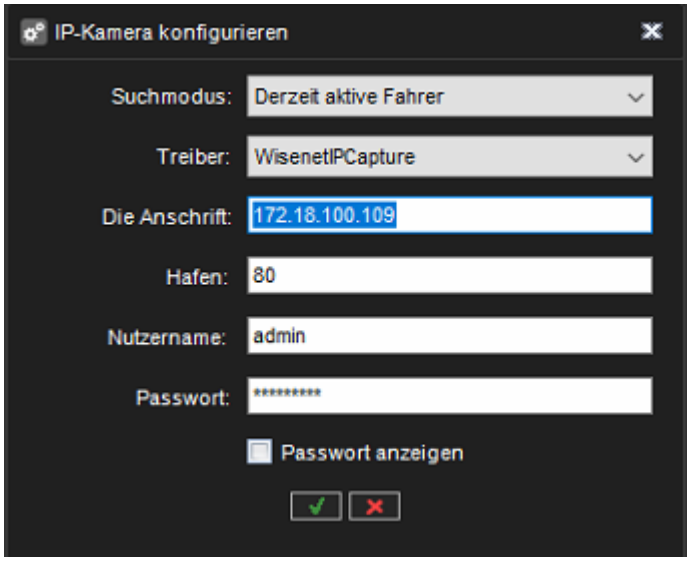
10.4.1.3 IP-Kamera bearbeiten

IP-Kamera bearbeiten ermöglicht Benutzern das Ändern von **Kameraadresse, Port, Benutzernamen oder Passwort**

1. Kamera aus der Liste auswählen
2. Klicken Sie auf **IP-Kamera bearbeiten**



1. Nehmen Sie erforderliche Änderungen vor
2. Klicken Sie auf OK, um die Änderungen zu bestätigen



10.4.1.4 Entfernen von IP-Kameras und Encodern

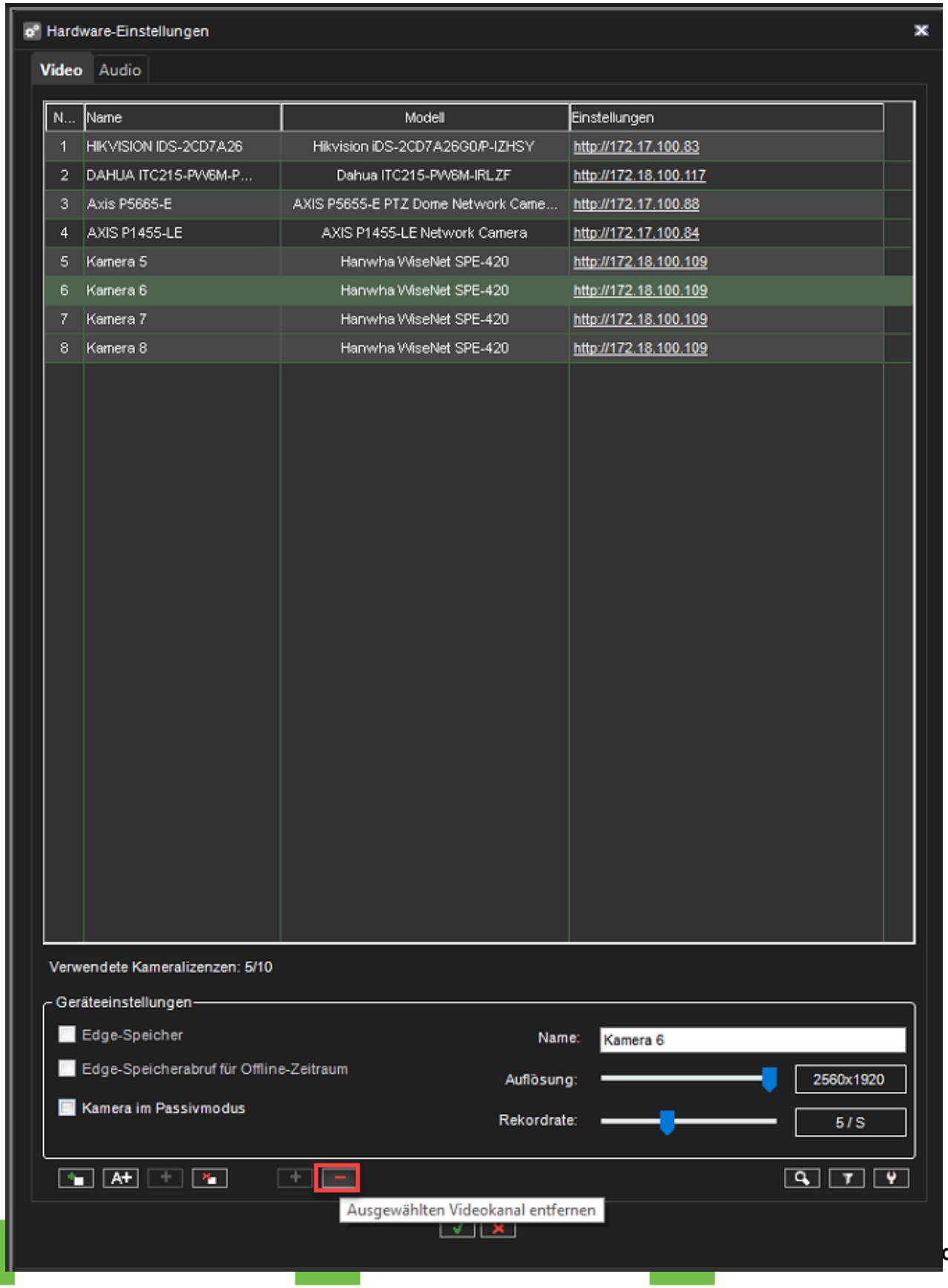
Wenn Sie den Dialog „**Hardwareeinstellungen**“ im System Manager öffnen, sehen Sie 2 Schaltflächen unter der Liste der Kameras:

- Die Schaltfläche "**Videokanal zum ausgewählten Gerät hinzufügen**"
- Die Schaltfläche „**Videokanal vom ausgewählten Gerät entfernen**“

10.4.1.4.1 So entfernen Sie eine IP-Kamera:

1. Kamera aus der Liste auf der Registerkarte **Video** auswählen
2. Klicken Sie in der unteren rechten Ecke der Registerkarte auf **Ausgewähltes Gerät entfernen**.
3. Wenn Sie aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **OK**.

MIRASYS

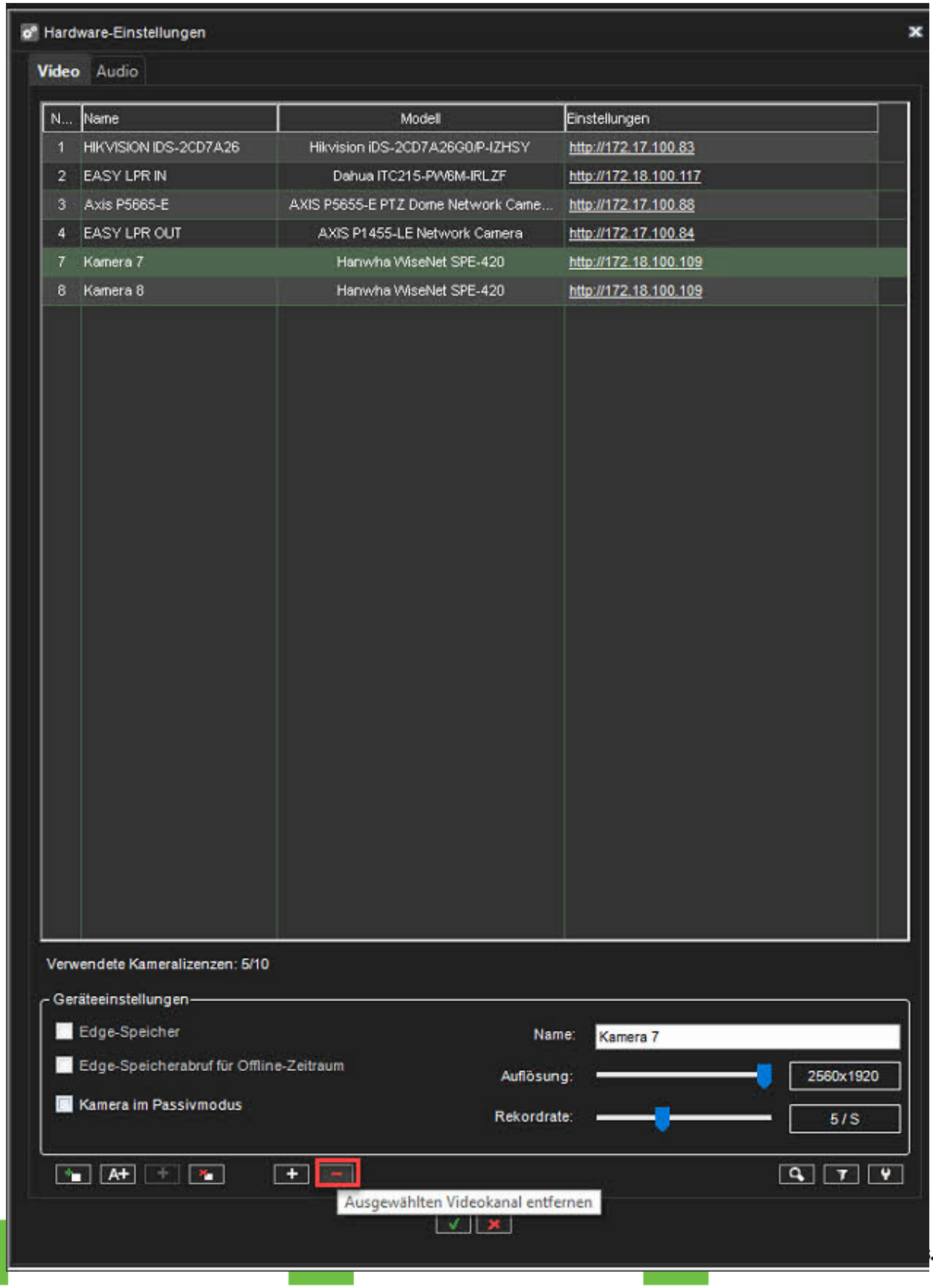

Hardware-Einstellungen
Video
Audio
N...
Name
Modell
Einstellungen
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 DAHUA ITC215-PW6M-P... Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 AXIS P1455-LE AXIS P1455-LE Network Camera http://172.17.100.84
5 Kamera 5 Hanwha WiseNet SPE-420 http://172.18.100.109
6 Kamera 6 Hanwha WiseNet SPE-420 http://172.18.100.109
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
Verwendete Kameralizenzen: 5/10
Geräteeinstellungen
Edge-Speicher
Edge-Speicherabruf für Offline-Zeitraum
Kamera im Passivmodus
Name:
Kamera 6
Auflösung:
2560x1920
Rekordrate:
5 / S
Ausgewählten Videokanal entfernen

com

10.4.1.4.2 So entfernen Sie Videokanäle vom Encoder oder Kameras mit mehreren Linsen:

1. Wählen Sie den richtigen Kanal aus der Liste
2. Klicken Sie auf **Videokanal vom ausgewählten Gerät entfernen**
3. Klicken **OK**

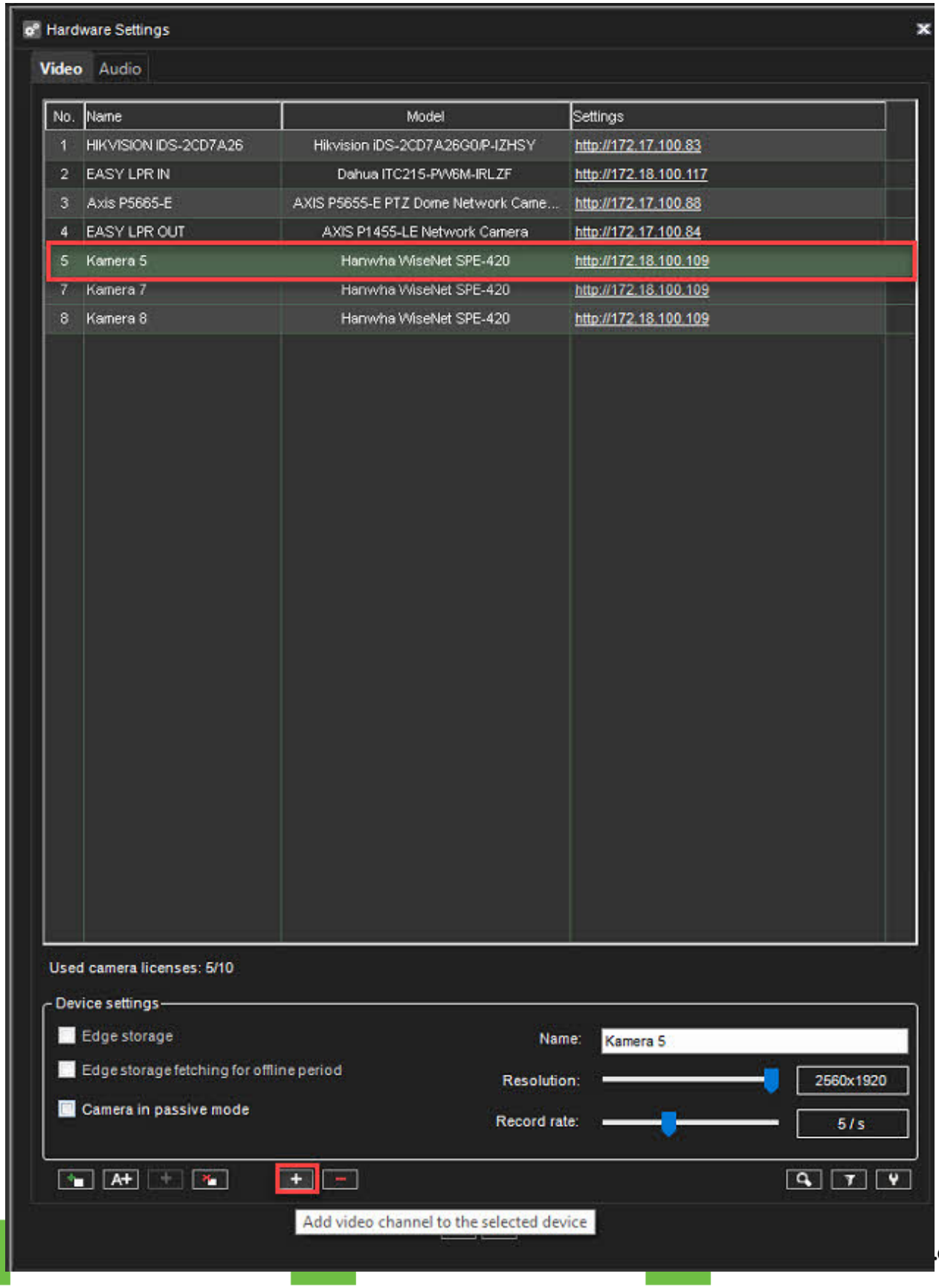
MIRASYS


Hardware-Einstellungen
Video
Audio
N...
Name
Modell
Einstellungen
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network Camera http://172.17.100.84
7 Kamera 7 Hanwha WiseNet SPE-420 http://172.18.100.109
8 Kamera 8 Hanwha WiseNet SPE-420 http://172.18.100.109
Verwendete Kameralizenzen: 5/10
Geräteeinstellungen
Edge-Speicher
Edge-Speicherabruf für Offline-Zeitraum
Kamera im Passivmodus
Name:
Kamera 7
Auflösung:
2560x1920
Rekordrate:
5 / S
A+
Ausgewählten Videokanal entfernen

10.4.1.4.3 So fügen Sie dem Encoder oder Kameras mit mehreren Objektiven Videokanäle hinzu:

1. Wählen Sie das richtige Gerät aus der Liste
2. Klicken Sie auf **Videokanal zum ausgewählten Gerät hinzufügen**
3. Klicken **OK**

MIRASYS


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

10.4.1.5 Ersetzen einer vorhandenen IP-Kamera im Mirasys VMS

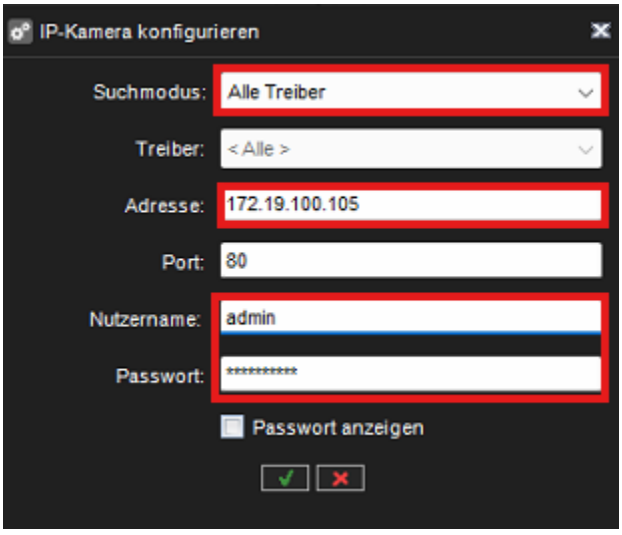
Falls die neue Kamera einen anderen Treiber verwendet als die derzeitige, muss die alte Kamera entfernt werden, bevor die neue Kamera hinzugefügt wird.

Um die vorhandene IP-Kamera durch eine neue zu ersetzen, führen Sie die folgenden Schritte aus:

- Fügen Sie die Adresse einer vorhandenen IP-Kamera für die neue IP-Kamera hinzu.
- Legen Sie für die neue IP-Kamera denselben Benutzernamen und dasselbe Passwort fest.
- Schließen Sie die Kamera an das Netzwerk an.
- Wählen Sie die Kamera aus der **Hardware**-Liste aus.
- Klicken Sie auf **IP-Kamera bearbeiten**.



1. **Suchmodus** auswählen: **Alle Treiber**
2. Überprüfen Sie, ob die Kamera die richtige IP-Adresse hat.
3. Überprüfen Sie, ob Benutzername und Passwort korrekt sind.
4. Klicken Sie auf **OK**.
5. Wählen Sie den richtigen Treiber aus der Liste **IP-Kamera-Treiber auswählen** aus.
6. Klicken Sie auf **OK**.

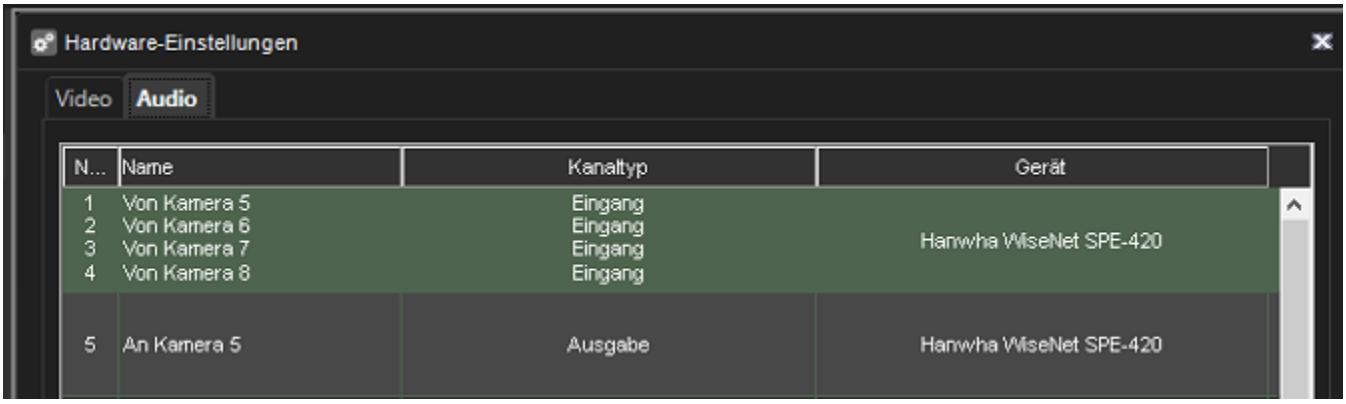


10.4.2 Audio (Hardware)

Wenn eine Kamera über kompatible IP-Audioeingangs- oder -ausgangskanäle verfügt, können Sie diese gleichzeitig hinzufügen, wenn Sie die Kamera über die automatischen Suchwerkzeuge hinzufügen.
Nachdem IP-Audioeingänge und -ausgänge für eine Kamera zum System hinzugefügt wurden, können sie bearbeitet und entfernt werden die Registerkarte **Audio**.

10.4.2.1 Angezeigte Informationen:

1. Kamera-Hardware-ID
2. Kanaltyp (Eingang)
3. Kanaltyp (Ausgabe)
4. Gerätemodell



10.4.3 Geräteeinstellungen

10.4.3.1 Edge-Speicher

Die Edge-Speicherfunktion ermöglicht eine unterbrechungsfreie Aufzeichnung bei Netzwerkausfällen. Der Rekorder überwacht den Online-/Offline-Status der Kameras und ruft Daten für den Zeitraum ab, in dem die Kameras als offline erkannt wurden. Die Informationen werden in der SQL-Datenbank gespeichert. In der Praxis kann der Videostream bei einem Netzwerkausfall auf einer SD-Speicherkarte in der Kamera gespeichert werden.

Sobald die Netzwerkverbindung wiederhergestellt wurde, wird das Video von der SD-Karte der Kamera an den Server übertragen. Bitte wenden Sie sich an die Kamera Herstellerdokumentation, um zu sehen, welche Kameras diese Funktion unterstützen.

Edge-Speicher muss in den Geräteeinstellungen aktiviert werden. Diese Funktion wird ausschließlich über das Konfigurationsdienstprogramm der Kamera konfiguriert. Anweisungen zum Aktivieren des Edge-Speichers finden Sie in der Dokumentation der Kamera.

10.4.3.2 Edge-Speicherabruf für Offline-Zeitraum

Wenn diese Option aktiviert ist, wird ein Abruf der Edge-Speicherdaten durchgeführt, wenn der Recorder für einen bestimmten Zeitraum nicht in Betrieb war; nach dem Neustart des Recorders versucht dieser, Daten von den Kameras für den Zeitraum abzurufen, in dem der Recorder ausgefallen war.

10.4.3.3 Kamera im Passivmodus

- Wenn auf mehreren Servern dieselbe Kamera konfiguriert ist, sollte einer auf **Aktiv** und die anderen auf **Passiv** eingestellt werden.
- Auf diese Weise werden nur die Einstellungen des aktiven Servers an die Kamera übermittelt.

10.4.3.4 360-Kamera

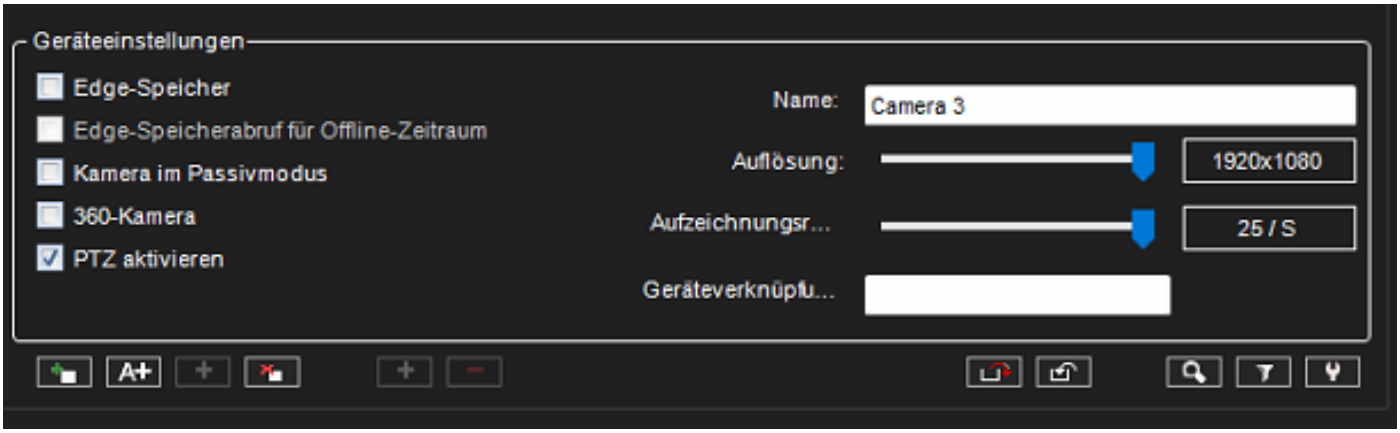
Wenn diese Einstellung aktiviert ist, wird die Kamera als 360-Grad-Kamera registriert.

10.4.3.5 PTZ aktivieren

Mit dieser Option können die PTZ-Funktionen für die Kamera ein- oder ausgeschaltet werden. Diese Einstellung ist nur sichtbar, wenn die Kamera als PTZ-Kamera erkannt wird.

10.4.3.6 Kamerainformationen

Kameraname, Auflösung, Aufnahmerate und Geräteverknüpfung können direkt über die Registerkarte **Video** eingestellt werden.



10.4.4 Hinzufügen von Kameras über eine CSV-Datei

VSM-Kameraeinstellungen können in eine CSV-Datei exportiert und aus einer CSF-Datei in VMS importiert werden. Auf diese Weise können Administratoren umfangreiche Änderungen an den Kameraeinstellungen vornehmen und die geänderten Einstellungen anschließend in das VMS-System importieren. Es ist auch möglich, mit dieser Funktion neue Kameras zu VMS hinzuzufügen.

10.4.4.1 CSV file import and export

Der System-Manager Hardware-Einstellungen verfügt über die folgenden Schaltflächen zum Exportieren von Kameraeinstellungen in eine Datei und zum Importieren von Kameraeinstellungen aus einer Datei im CSV-Format.



10.4.4.1.1 CSV-Dateiformat

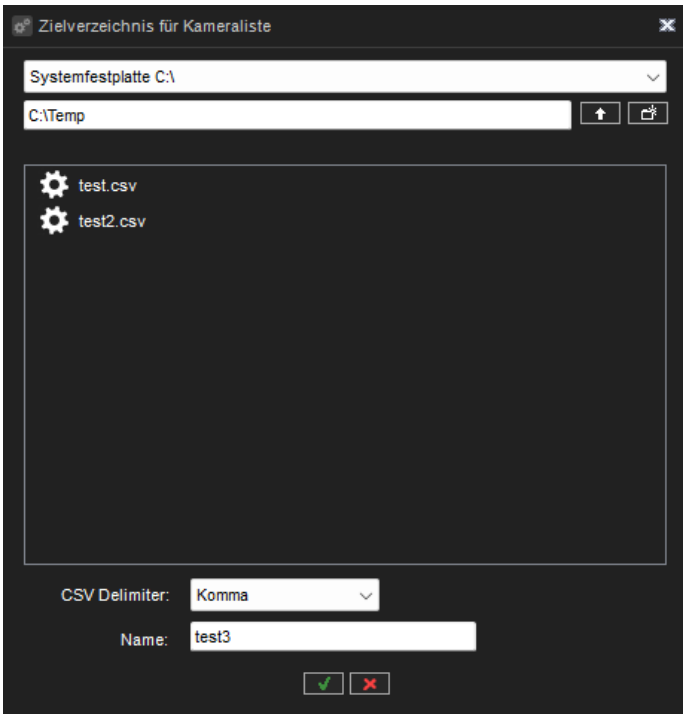
Das CSV-Dateiformat verwendet für jede Kamera die folgenden Kopfzeilen.

- **Name** - Name des Kamerakanals.
- **Nummer** - Nummer des Kamerakanals auf dem VMS-Server.
- **Beschreibung** - Beschreibung des Kamerakanals.
- **AdmDescription** - Administrative Beschreibung des Kamerakanals.
- **Adresse** - Adresse des Kamerageräts.
- **Port** - Anschluss des Kamerageräts.
- **UserName** - Benutzername für das Kameragerät.
- **Passwort** - Passwort für das Kameragerät.
- **Driver** - Treibername / native (Suche unter allen verfügbaren nativen Treibern) / onvif (Verwendung des ONVIF-Treibers). Logic verwendet den ersten Treiber, der die angegebene Zeichenkette für den Treibernamen enthält. Zum Beispiel, Achse → NewAxisIPCapture.
- **Kanal** - Verwendeter Kanal des Treibers, wenn das Gerät mehr als einen Kanal unterstützt. Bei Ein-Kanal-Geräten kann dies leer bleiben.
- **IsInUse** - Ist die Kamera in Gebrauch.
- **IsAudioInUse** - Ist Audio in Gebrauch, wenn der Treiber dies unterstützt.
- **IsIOInUse** - Ist I/O in Gebrauch. Dies hat nur beim Export von CSV-Dateien eine Bedeutung. Beim Import wird E/A automatisch verwendet, wenn das Gerät dies unterstützt.
- **Ist360** - Ist 360 Kamera.
- **Framerate** - Bilder / Sekunde des Aufnahmestroms, gerundet auf den nächsten verfügbaren Wert. Kopfzeile für andere Streams: Framerate1, Framerate2, Framerate3.
- **Auflösung** - Auflösung des Aufnahmestreams im Format Breite x Höhe (z. B. 1920x1080), gerundet auf den nächstmöglichen Wert. Für andere Streams: Auflösung1, Auflösung2, Auflösung3.
- **Codec** - Verwendeter Komprimierungscodec des Aufnahmestreams. Gerundet auf den nächsten verfügbaren Wert: JPEG, MPEG, H264, WMC9, PARSE, H265, MXPEG. Für andere Streams: Codec1, Codec2, Codec3.

- **Qualität** - Komprimierungsqualität des Aufnahmestreams, gerundet auf den nächsten verfügbaren Wert im Bereich 1-100. Für andere Streams: Qualität1, Qualität2, Qualität3.
- **Bitrate** - Bitrate des Aufnahmestreams, gerundet auf den nächstmöglichen Wert. Für andere Streams: Bitrate1, Bitrate2, Bitrate3.

10.4.4.1.2 Exportieren

Der Benutzer kann den Ordner auswählen, in den die CSV-Datei mit den Kameraeinstellungen exportiert werden soll, und einen Namen für die Datei vergeben. Sie können auch das Trennzeichen festlegen, das in der CSV-Datei verwendet wird.



Wenn der Export erfolgreich war, wird ein blinkendes grünes Symbol angezeigt. Bei einem Fehler wird ein blinkendes rotes Symbol angezeigt.

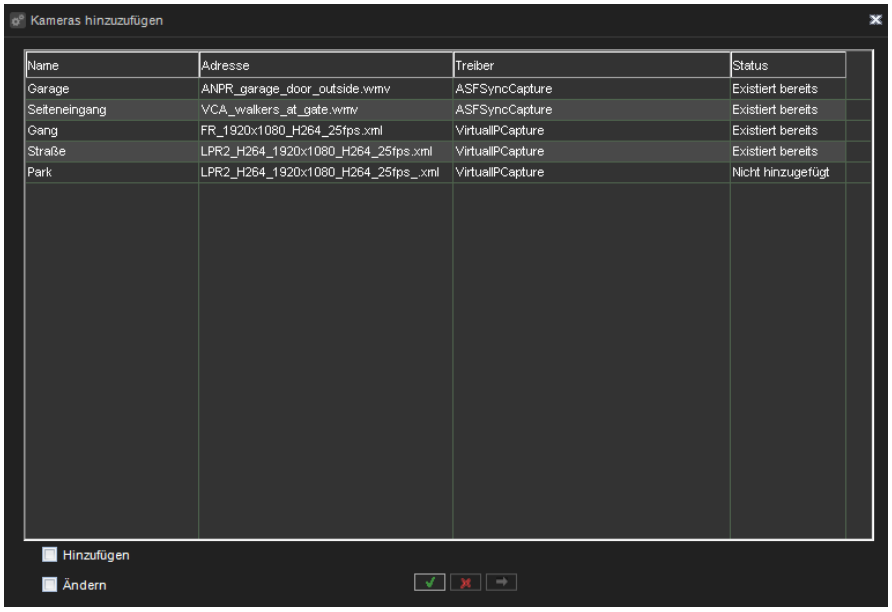
10.4.4.1.2.1 Importieren

Wenn ein Benutzer auf die Schaltfläche Importieren klickt, wird der Dialog Datei auswählen angezeigt, um die zu importierende CSV-Datei auszuwählen. Wenn die Datei ausgewählt ist, wird die Ansicht zum Hinzufügen der Kamera angezeigt, wenn das Parsen und die Validierung der CSV-Datei erfolgreich durchgeführt wurden.

Die folgenden Überprüfungsregeln werden beim Parsen importierter CSV-Dateien verwendet.

- Das Spaltenbegrenzungszeichen der CSV-Datei ist ein Komma (,) oder Semikolon (;).
- Die Reihenfolge der Kopfzeilennamen (d. h. die Spaltenreihenfolge) ist frei.
- Nicht verwendete Kopfzeilennamen (d. h. Spalten) können weggelassen werden.

- Nur der Name der Kopfzeile Adresse ist obligatorisch. Fehlt er, werden die Daten der CSV-Datei nicht akzeptiert.
- Wenn einige Eigenschaftsnamen und Daten nicht vorhanden sind, wird ein interner Standardwert verwendet.
- Bei Validierungsfehlern und -warnungen wird ein Popup-Fenster erzeugt, und weitere Informationen werden im Systemmanager-Protokoll ausgedruckt.



Kameras, die über CSV importiert werden, können als Teil des Importvorgangs in den passiven Modus versetzt werden. Systemadministratoren können diese Einstellung in der CSV-Datei festlegen.

Mehrere Streaming-Status (aktiviert oder deaktiviert) können verwendet werden, wenn dies von der Kamera unterstützt wird, ebenso wie der Bitratenmodus für die Bitrate.

Audiokanäle sollten nicht automatisch hinzugefügt werden, wenn sie beim Importieren von CSV-Dateien nicht hinzugefügt wurden.

Bitte beachten Sie, dass beim Import von Mehrkanalgeräten mit einer festgelegten Kanalnummer in der Spalte "Anzahl" für jedes Gerät eine Kanalnummer manuell definiert werden muss. Außerdem ist es notwendig, die Kanalnummer des Rekorders (aus der Spalte "Anzahl") der Kanalnummer des Geräts (Spalte "Kanal") zuzuordnen. Dieses Problem kann gelöst werden, indem die Spalten "Anzahl" und "Kanal" nicht einbezogen werden.

Nach der Validierung und dem Parsen der CSV-Datei informiert die Statusspalte darüber, ob die Kamera bereits zum System hinzugefügt wurde (bereits vorhanden) oder ob es sich um eine neue Kamera handelt (nicht hinzugefügt).

Die Kontrollkästchen Hinzufügen und Ändern werden angezeigt, wenn in der importierten CSV-Datei Änderungen an vorhandenen Kameras und neuen Kamerakonfigurationen vorgenommen wurden. Mit diesen Optionen können Sie auswählen, ob Kameras aus der CSV-Datei hinzugefügt und/oder geändert werden sollen.

Die Schaltfläche Ausführen ist aktiviert, wenn es Kameras gibt, die hinzugefügt oder geändert werden sollen. Wenn Sie auf die Schaltfläche Ausführen klicken, werden die Einstellungen aus der CSV-Datei auf die aktuellen Einstellungen angewendet (geändert und/oder hinzugefügt). Nachdem die Einstellungen übernommen wurden, wird der Status für jede Kamera aktualisiert.

Der Dialog kann nach dem Übernehmen der Einstellungen durch Klicken auf die Schaltfläche ok oder vor dem Übernehmen der Einstellungen durch Klicken auf die Schaltfläche cancel geschlossen werden.

Geänderte Kameraeinstellungen und/oder hinzugefügte Kameras werden auf den VMS-Server angewendet, sobald die Hardwareeinstellungen gespeichert sind.

10.5 Hinzufügen und Entfernen von VMS-Servern

Sie können (je nach Lizenz) 1 bis unbegrenzt viele Server in einem System haben.
Ein Server sollte nicht zu mehr als einem Hauptserver (SMServer) gehören.
Sie können für jeden Server ein Passwort angeben.
Das System fordert Sie zur Eingabe des Passworts auf, wenn jemand versucht, den Server zu einem anderen System hinzuzufügen.

10.5.1 So fügen Sie dem System einen Server hinzu (Aufzeichnungsserver):

1. Öffnen Sie die Registerkarte VMS-Server

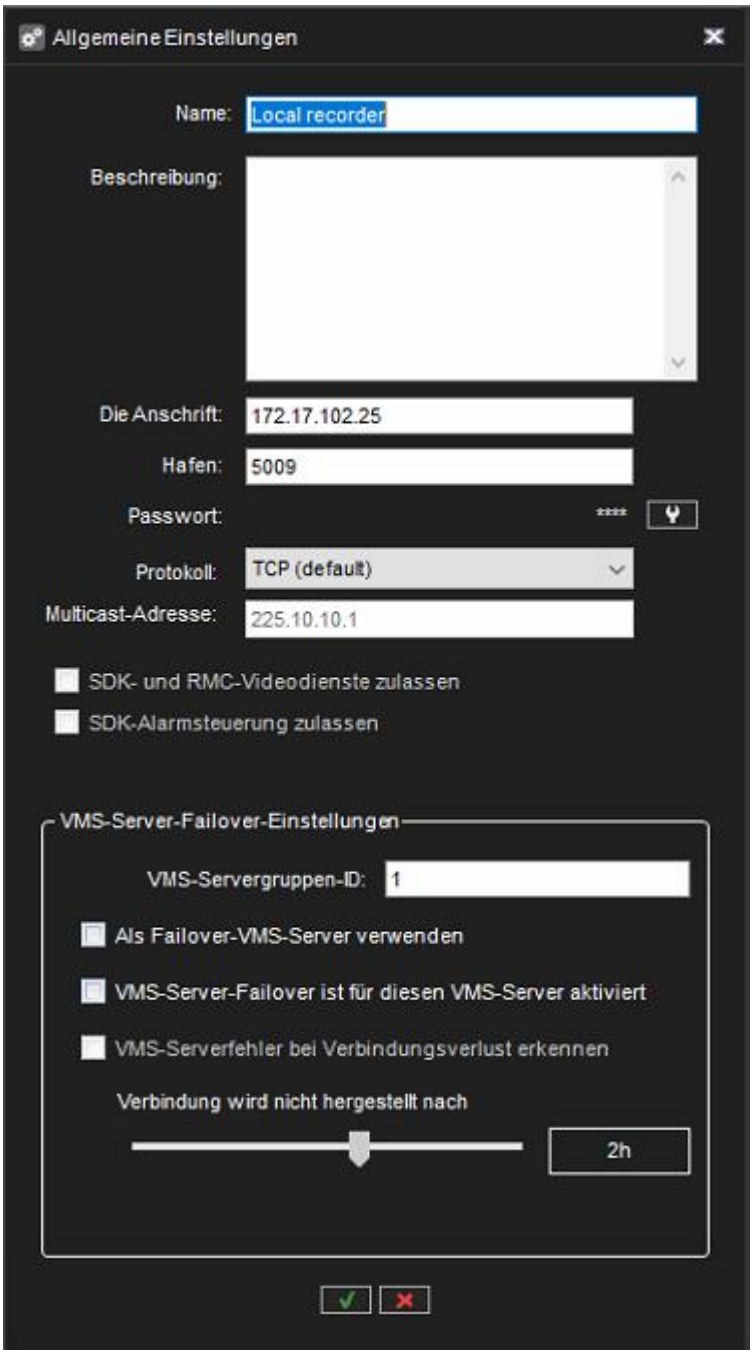


2. Klicken Sie auf VMS-Server hinzufügen



3. Das Dialogfenster **Allgemeine Einstellungen** wird angezeigt.
4. Geben Sie den Namen für den Server ein
5. Geben Sie bei Bedarf eine Beschreibung ein
6. Geben Sie die IP-Adresse oder den DNS-Namen des Servers ein.
7. Geben Sie bei Bedarf das Passwort für den Server ein
8. Klicken **OK** Der Server und die damit verbundenen Geräte (Kameras und Audiokanäle) werden der Liste hinzugefügt.

a. Notiz: *Wenn der Server passwortgeschützt ist, fordert das System zur Eingabe des Passworts auf.*



10.5.2 So entfernen Sie einen Server aus dem System:

1. Wählen Sie den Server aus, den Sie entfernen möchten.
2. Click **Remove VMS Server**

3. Klicken Sie zur Bestätigung auf **OK**.

10.5.3 Verbindungsstatus:

Wenn die Verbindung zum Server unterbrochen wird, versucht die System Manager-Anwendung automatisch, eine Verbindung zum Server herzustellen.

10.5.4 HINWEIS:

Wenn Sie Mirasys VMS als Subserver hinzugefügt haben, gehen Sie bitte wie folgt vor:

1. Ändern Sie das Admin-Benutzerkennwort mit einem Subserver System Manager
2. Deaktivieren Sie den SMServer-Dienst vom Subserver

10.6 Suche in den VMS Server-Einstellungen

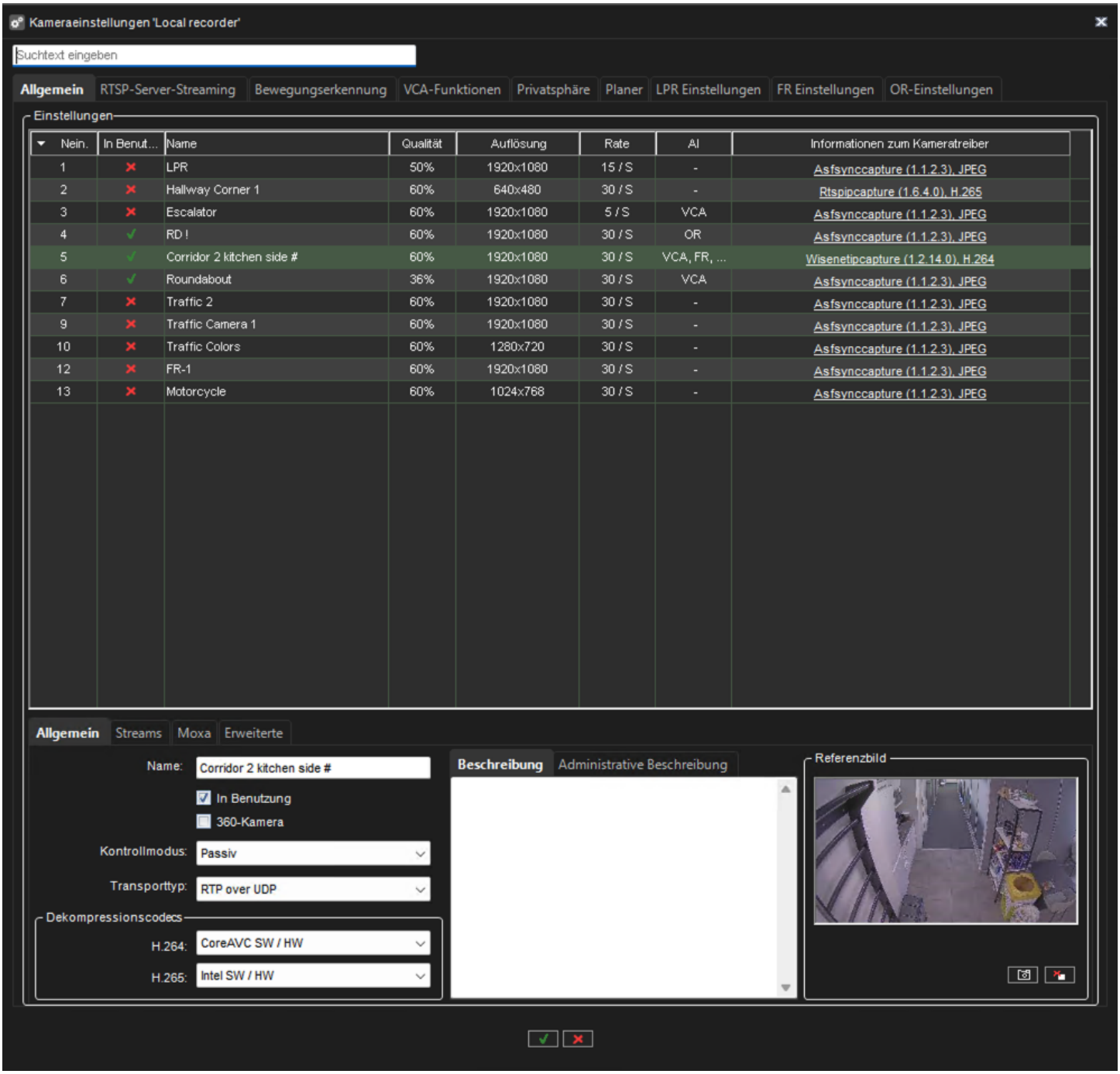
10.6.1 Suche in der Registerkarte VMS Server-Einstellungen

Auf der Registerkarte VMS-Server-Einstellungen können Sie nach einem bestimmten Gerät suchen. Wenn Sie z. B. mehrere Rekorder haben und nach einer bestimmten Kamera suchen, z. B. der "Roundabout-Kamera", und den Rekorder eingrenzen müssen, können Sie auf der Registerkarte "Rekorder" suchen, und es wird dann nur der VMS-Server angezeigt und darunter nur die Einstellungen, in denen Sie die Garage-Kamera finden können.



10.6.2 Eingrenzung der Suche über die Registerkarte VMS Server-Einstellungen

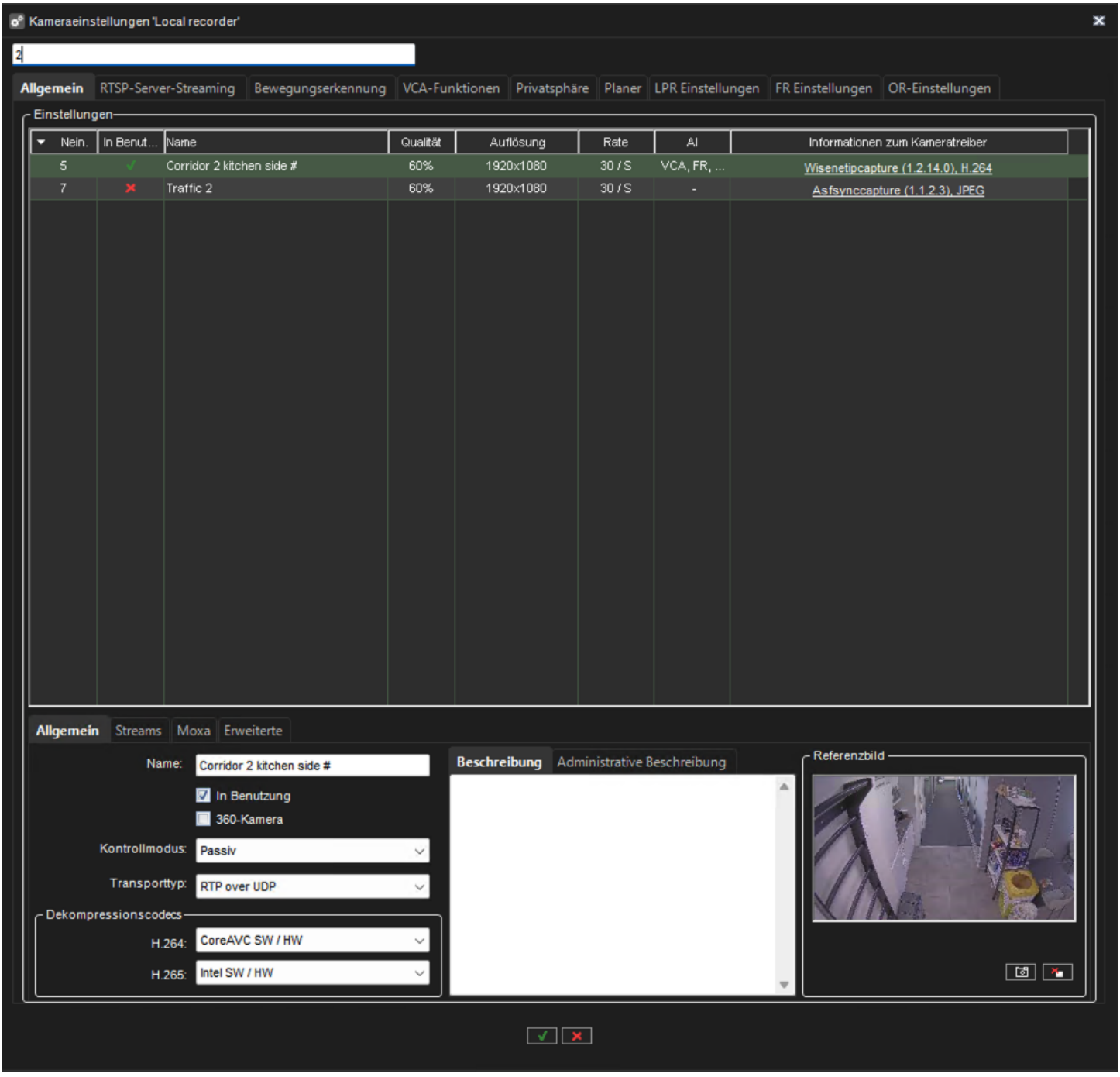
Wenn Sie z. B. die Kameraeinstellungen unter der Registerkarte Suche in den VMS Server-Einstellungen öffnen, ist die Roundabout-Kamera aus dem obigen Beispiel bereits ausgefiltert. Die Suche kann in den einzelnen Einstellungsregistern zurückgesetzt werden.



10.6.3 Suche in individuellen Einstellungen

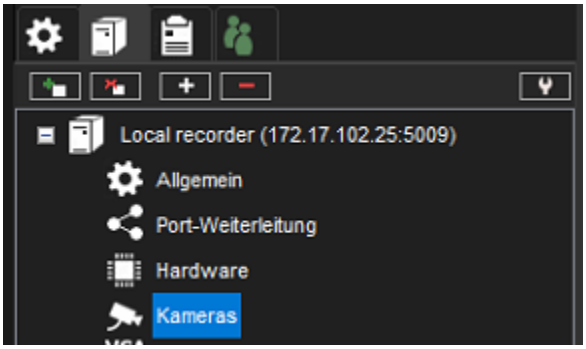
In den individuellen Einstellungen können Sie nach einem Gerät suchen. In den folgenden Einstellungen gibt es eine Suchleiste:

- Kameraeinstellungen
- Audio-Einstellungen
- Hardware-Einstellungen
- Digitale E/A-Einstellungen
- Speichereinstellungen
- Alarm-Einstellungen
- Textkanal-Einstellungen



10.7 KAMERAS

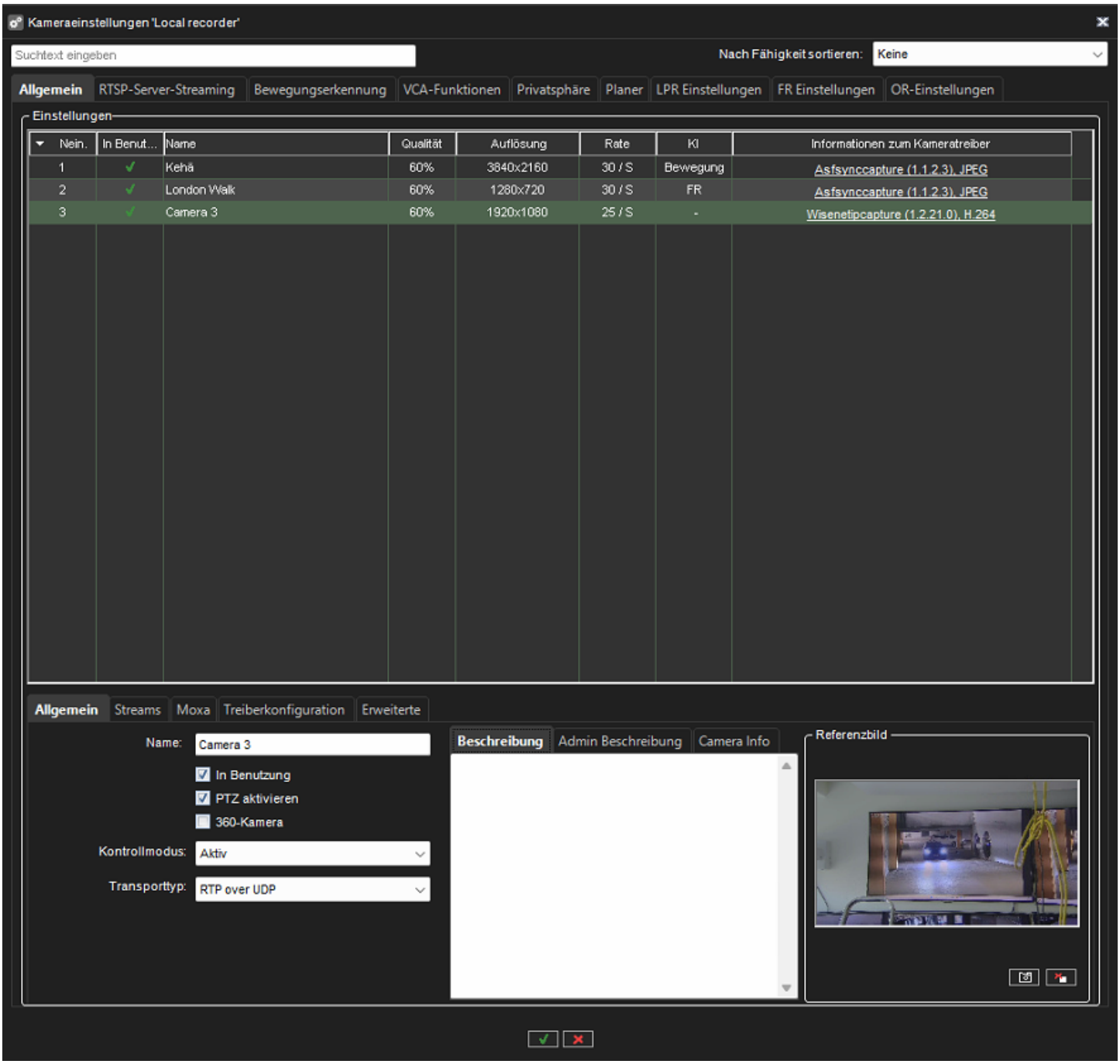
Nachdem die Kamera zum Server hinzugefügt wurde, können die Kameraeinstellungen auf der Seite **Kameras** konfiguriert werden.



10.7.1 Kameraeinstellungen enthalten Einstellungen für:

- Allgemein
- Bewegungserkennung
- VCA-Einstenllung
- Privatsphäre
- Planer

10.7.2 Kameraeinstellungen



10.7.2.1 Allgemeine Einstellungen

In den allgemeinen Einstellungen zeigen die Spalten die Kameranummer, wenn die Kamera in Gebrauch ist, den Kameranamen, die Qualität, die Auflösung und die Rate, wenn die Kamera einen AI-Dienst verwendet, welchen

Dienst und welchen Kameratreiber die Kamera verwendet. Alle Spalten können in aufsteigender oder absteigender Reihenfolge sortiert werden.

10.7.2.1.1 Name

Der Name der Kamera. Das System schlägt Namen des Typs *Kamera 1, Kamera 2* usw. vor.

10.7.2.1.2 Im Einsatz

Deaktivieren Sie dieses Kontrollkästchen, wenn keine Kamera an den Kameraeingang angeschlossen ist oder wenn Sie die Kamera deaktivieren möchten.

10.7.2.1.3 PTZ aktivieren

Mit dieser Option können die PTZ-Funktionen für die Kamera ein- oder ausgeschaltet werden. Diese Einstellung ist nur sichtbar, wenn die Kamera als PTZ-Kamera erkannt wird.

10.7.2.1.4 360 Kamera

Dies teilt dem Spotter-Client mit, dass es sich bei der Kamera um eine 360-Grad-Kamera handelt, und Spotter zeigt die Bildentzerrungsoptionen in der Kamerasymbolleiste an (sofern installiert).

10.7.2.1.5 Steuermodus

Diese Einstellung hat zwei Optionen, **Aktiv** (Standard) und **Passiv**.
Wenn mehrere Server dieselbe Kamera konfiguriert haben, sollte einer auf **Aktiv** und die anderen auf **Passiv** gesetzt werden.
Auf diese Weise werden nur die aktiven Servereinstellungen an die Kamera übermittelt .

10.7.2.1.6 Transportart

Diese Einstellung steuert, wie der Medienstream von der Kamera zum Server transportiert wird.
Die verfügbaren Optionen sind **RTP over UDP** (Standard) und **RTP over RTSP**.
Wenn die Kamera mit einer Einstellung schlecht zu funktionieren scheint (z. B. wenn es Löcher im Kameramaterial gibt oder es schwierig ist, alle Bilder von einer Kamera zu erhalten), kann die andere Einstellung verwendet werden.

10.7.2.1.7 Beschreibung

Hier können Sie eine Beschreibung der Kamera eingeben, die allen Benutzern im Spotter-Programm angezeigt wird.

10.7.2.1.8 Administrative Beschreibung

Hier können Sie eine Beschreibung der Kamera eingeben. Die Beschreibung wird im Spotter-Programm nur Systemadministratoren angezeigt.

10.7.2.1.9 Kamera-Infos

Die Registerkarte „Kamerainfo“ enthält Kontrollkästchen für die Angaben, die automatisch in die Kamerainfo aufgenommen werden sollen:

- VMS-Server

- Serverinformationen
- IP-Adresse
- Kameramodell
- Verwendete AI-Funktionen
- Auflösung
- Einstellungen der Bildrate

Die Informationen, die Sie durch Ankreuzen der Kästchen für die Kamera erhalten, werden automatisch in die Kamerabeschreibung in Spotter für diese Kamera übernommen. Standardmäßig sind alle Kästchen aktiviert.

Damit die Informationen in Spotter angezeigt werden, muss unter Benutzergruppe > Eigenschaften der Mirasys Spotter Enterprise-Rolle > Bildschirm > Bildschirmelemente die Erlaubnis erteilt werden, Kamera-Infos anzuzeigen.

10.7.2.1.10Referenzbild

Ein Referenzbild ist ein von der Kamera aufgenommenes Bild, das die Identifizierung der Kameras erleichtert.

Darüber hinaus können die Benutzer im Spotter-Programm das, was sie in der Videoansicht sehen, mit dem Referenzbild vergleichen, um sicherzustellen, dass die Kamera darauf gerichtet ist in die richtige Richtung.

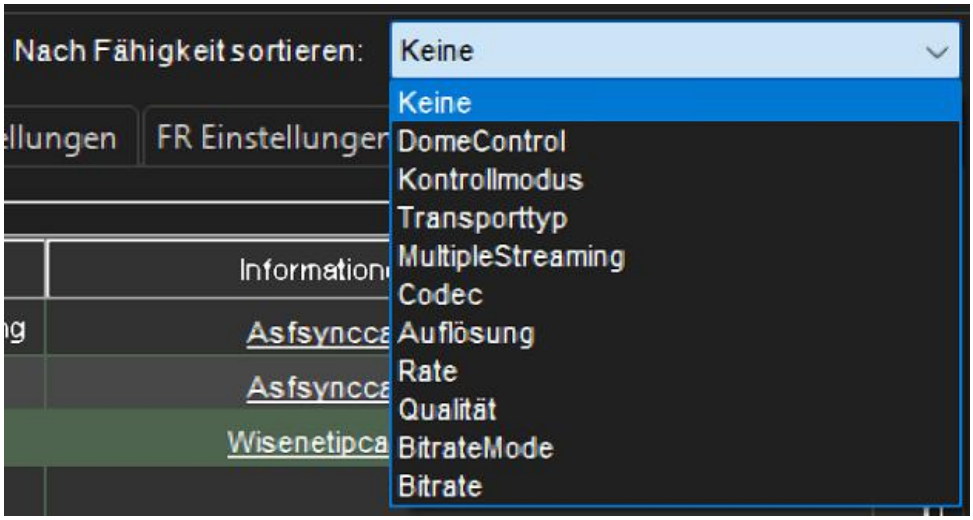
Um das aktuelle Referenzbild zu ändern, klicken Sie auf die **Schaltfläche Bild aufnehmen** . Um ein Referenzbild zu löschen, klicken Sie auf die Schaltfläche **Bild löschen**.

10.7.2.1.11Kameraeinstellungen in großen Mengen aktualisieren

Die Einstellungen können für mehrere Kameras gleichzeitig aktualisiert werden. Dazu wählen Sie mehrere Kameras aus (halten Sie die Strg-Taste gedrückt und klicken Sie auf die Kameras in der Liste) und ändern Sie die Einstellungen für eine Kamera. Die Änderungen werden auf alle ausgewählten Kameras angewendet. Kameras, die gleichzeitig aktualisiert werden, müssen über die gleichen Einstellungsmöglichkeiten verfügen. Treiber-Einstellungen können nicht gesammelt aktualisiert werden.

10.7.2.1.12Kameras nach Fähigkeiten sortieren

Kameras können in den Kameraeinstellungen nach Funktionen gruppiert werden, was die Durchführung von Massenaktualisierungen der Einstellungen erleichtert. Eine Gruppierungsbedingung kann aus dem Dropdown-Menü „Nach Fähigkeit sortieren“ ausgewählt werden, und die Kameras, die den Sortierkriterien entsprechen, werden aus der Liste ausgewählt.



10.7.2.2 Streams (Kameras)

10.7.2.2.1 Standardmäßig empfängt Mirasys VMS einen Stream in Aufzeichnungsqualität von der Kamera. Der Mirasys VMS-Server sendet den Aufzeichnungsstream standardmäßig an Mirasys Spotter



10.7.2.2.2 Codec

Der Codec wird für die Übertragung des Videos zwischen dem Server und den Client-Anwendungen und im Fall von IP-Kameras für die Übertragung des Videos zwischen der IP-Kamera und dem Server verwendet.
Im Fall von analogen Kameras ist der vom System verwendete Codec JPEG.
Bei IP-Kameras kann jeder Codec ausgewählt werden, der sowohl von der Kamera als auch von der Serversoftware unterstützt wird.
Die von der Serversoftware unterstützten Codecs sind JPEG, MPEG-4, H.264, H.265 und Mobotix MxPEG.

10.7.2.2.3 Bitrate mode.

Diese Einstellung steuert, ob die variable Bitrate (VBRMax) oder die konstante Bitrate (CBR) verwendet wird.

10.7.2.2.4 Qualität

Stellen Sie diesen Wert zwischen 0%-100% ein. Ein höherer Wert bedeutet eine bessere Bildqualität, aber auch eine große Bilddatengröße.

Um die Bilddatengröße zu verringern, stellen Sie den Wert niedriger ein. Eine niedrigere Einstellung des Werts verringert jedoch auch die Qualität der Bilder.

50 % sind in der Regel ausreichend. Wählen Sie für drahtlose Verbindungen und Verbindungen mit geringer Bandbreite 0 % aus.

10.7.2.2.5 Auflösung

Bei automatisch konfigurierten IP-Kameras werden genau die vom Kameramodell unterstützten Bildauflösungen angezeigt.

10.7.2.2.6 Rekordrate

Die Aufzeichnungsrate definiert, wie viele Frames die Kamera an das VMS sendet und wie viele Frames aufgezeichnet werden.

Die maximale Rate hängt vom Videostandard und vom Kameratyp ab.

Multiple Streaming (Multi-Streaming)

Mehrfach-Streaming (Multi-Streaming)

10.7.2.2.7 Multi-Streaming (Kameras)

Multi-Streaming ermöglicht separate Feeds von einer einzelnen Kamera.

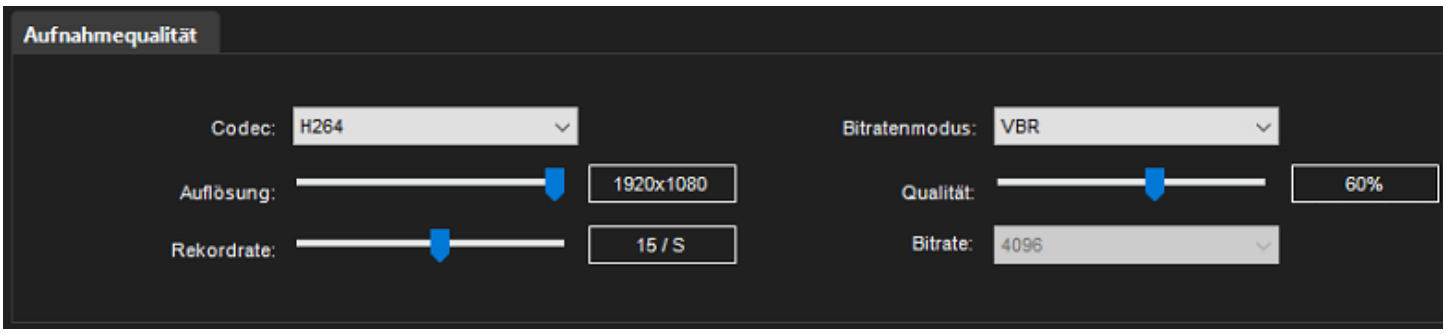
Die Funktion ermöglicht die Verwendung separater Streams zum Aufzeichnen und Anzeigen.

Die Funktion ist nur verfügbar, wenn die Kamera und der Treiber dies unterstützen.

10.7.2.2.7.1 Aufnahmequalität

Standardmäßig empfängt Mirasys VMS einen Stream in Aufzeichnungsqualität von der Kamera.

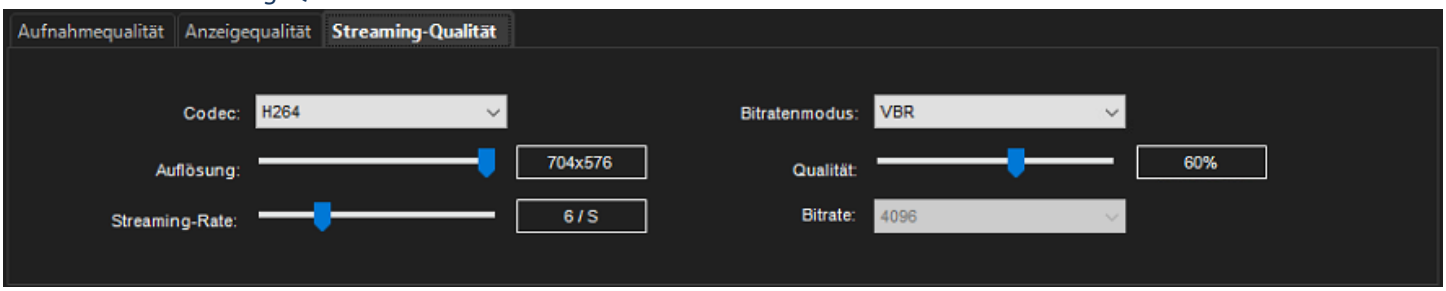
Der Mirasys VMS-Server sendet den Aufzeichnungsstream standardmäßig an den Mirasys Spotter



10.7.2.2.7.2 Anzeigequalität



10.7.2.2.7.3 Streaming-Qualität



10.7.2.3 Moxa-Einstellungen

10.7.2.3.1 Moxa PTZ-Bearbeitung aktivieren

In den Eigenschaften der System Manager-Rolle / VMS-Server-Einstellungen kann die Bearbeitung der Moxa-PTZ-Einstellungen für die Benutzergruppe ausgewählt werden. Wenn Moxa-PTZ-Steuerung aktivieren nicht ausgewählt ist, sind die Moxa-PTZ-Einstellungen unter Kameraeinstellungen sichtbar, können aber nicht geändert werden.

10.7.2.3.2 Moxa PTZ-Einstellungen

In den Kameraeinstellungen ist eine zusätzliche Registerkarte für Moxa-Einstellungen für Kameras verfügbar, für die Moxa-PTZ-Treibereinstellungen konfiguriert wurden oder wenn die Moxa-Bearbeitung für die Benutzergruppe aktiviert ist.

10.7.2.3.2.1 Gerät

Aktivieren Sie die Moxa PTZ-Einstellungen für die Kamera

Wenn die Kamera keine PTZ-Einstellungen hat, öffnen Sie die Registerkarten Gerät und PTZ-Steuerung mit den Standardwerten.

Wenn die Kamera über Moxa-PTZ-Einstellungen verfügt und Aktivieren nicht ausgewählt ist, werden beim Speichern der Einstellungen die Moxa-PTZ-Einstellungen von der Kamera entfernt

Adresse geben Sie die IP- oder DNS-Adresse des MOXA-Geräts ein.

Portindex ist der Index des seriellen Ports (1 - 255) im MOXA-Gerät, an dem die PTZ-Kamera angeschlossen ist.

Timeout/ms ist der Timeout in Millisekunden für die Kommunikation mit dem MOXA-Gerät (5000 ms als Standard)

Protokoll ist das Kommunikationsprotokoll mit der PTZ-Kamera aus der folgenden Aufzählung:

- { "PelcoD", "BoschOSRD" }
    - Standardwert ist "PelcoD".

10.7.2.3.2.2 PTZ-Steuerung

Kameraindex - Adresse der analogen PTZ-Kamera, die in der Kamera eingestellt ist (normalerweise sind es Hardware-Jumper) (0 - 255)

Baudrate - Baudrate der seriellen Schnittstelle in Bits pro Sekunde. MOXA unterstützt die folgenden Baudraten:

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

Datenbits - (Byte) - Wert aus dem folgenden Satz:

- {5, 6, 7, 8 }
- Der Standardwert ist 8.

Stoppbit - (Byte) - Wert aus dem folgenden Satz:

- { 1, 2 }
- Standardwert ist 1.

Parität - Wert aus der folgenden Aufzählung:

- { "None" = 0, "Even" = 1, "Odd" = 2, "Mark" = 3, "Space" = 4 }
- Standardwert ist "Keine".

Flusskontrolle - Wert aus der folgenden Aufzählung:

- { "Keine" = 0, "RTS / CTS" = 1, "XON / XOFF" = 2, "Beide" = 3 }
- Standardwert ist "Keine".

10.7.2.4 Erweiterte

Diese Registerkarte enthält Optionen für erweiterte Kameraeinstellungen.

10.7.2.4.1 Dekomprimierungscodecs

Codecs werden zum Kodieren und Dekodieren von Videodaten verwendet

10.7.2.4.2 Geräteverknüpfung

Im Textfeld „Geräteverknüpfung“ kann eine Taste für eine Kamera festgelegt werden. Der in den Kameraeinstellungen festgelegte Shortcut wird als Standard-Shortcut verwendet.

10.7.2.5 Treiberkonfiguration

Diese Registerkarte enthält kamera- oder treiberspezifische einzigartige Einstellungen. Ein Treiber-Update kann dieser Registerkarte zusätzliche Werte bringen.
Die Auswahl mehrerer Kameras ist mit der SHIFT- oder CTRL-Taste möglich.
Bitte beachten Sie, dass Sie bei Auswahl von mehr als einer Kamera keine Parameter einstellen können, die nicht von allen ausgewählten Kameras unterstützt werden.

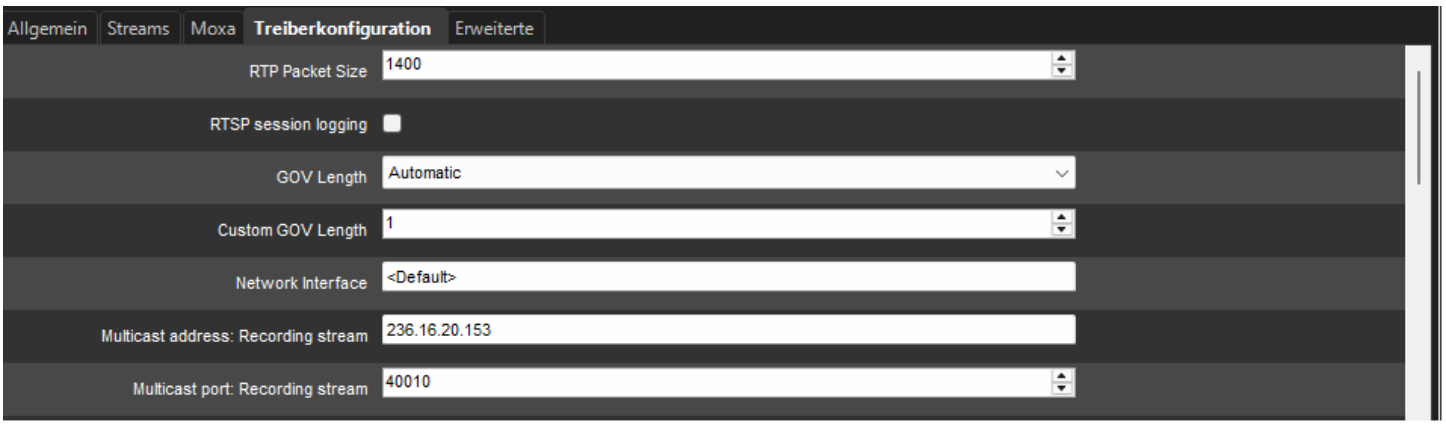
10.7.2.5.1 Konfigurierbare Werte

- RTP-Paketgröße
- RTSP-Sitzungsprotokollierung
- GOV-Länge
- Benutzerdefinierte GOV-Länge
- Datenschutzmaske durch den Fahrer verwalten
- Netzwerkschnittstelle
- Multicast-Adresse: Aufnahmestream
- Multicast-Port: Aufnahmestream
- Multicast-Adresse: Stream ansehen
- Multicast-Port: Stream ansehen
- Multicast-Adresse: Streaming-Stream
- Multicast-Port: Streaming-Stream
- Multicast-TTL
- Enable Time Synchronization feature
- Enable 3-Axis PTZ
- Enable simple focus after zooming
- PTZ OSD menu confirmation timeout
- Minimum Pan/Tilt speed (percent)

- Maximum Pan/Tilt speed (percent)
- Minimum Zoom speed (percent)
- Maximum Zoom speed (percent)
- Enable PTZ log

Die Einstellung der Schwenk-/Neige- und Zoomgeschwindigkeit ist für die folgenden Kameratreiber möglich:

- ONVIF
- Bosch
- Hanwha
- Axis



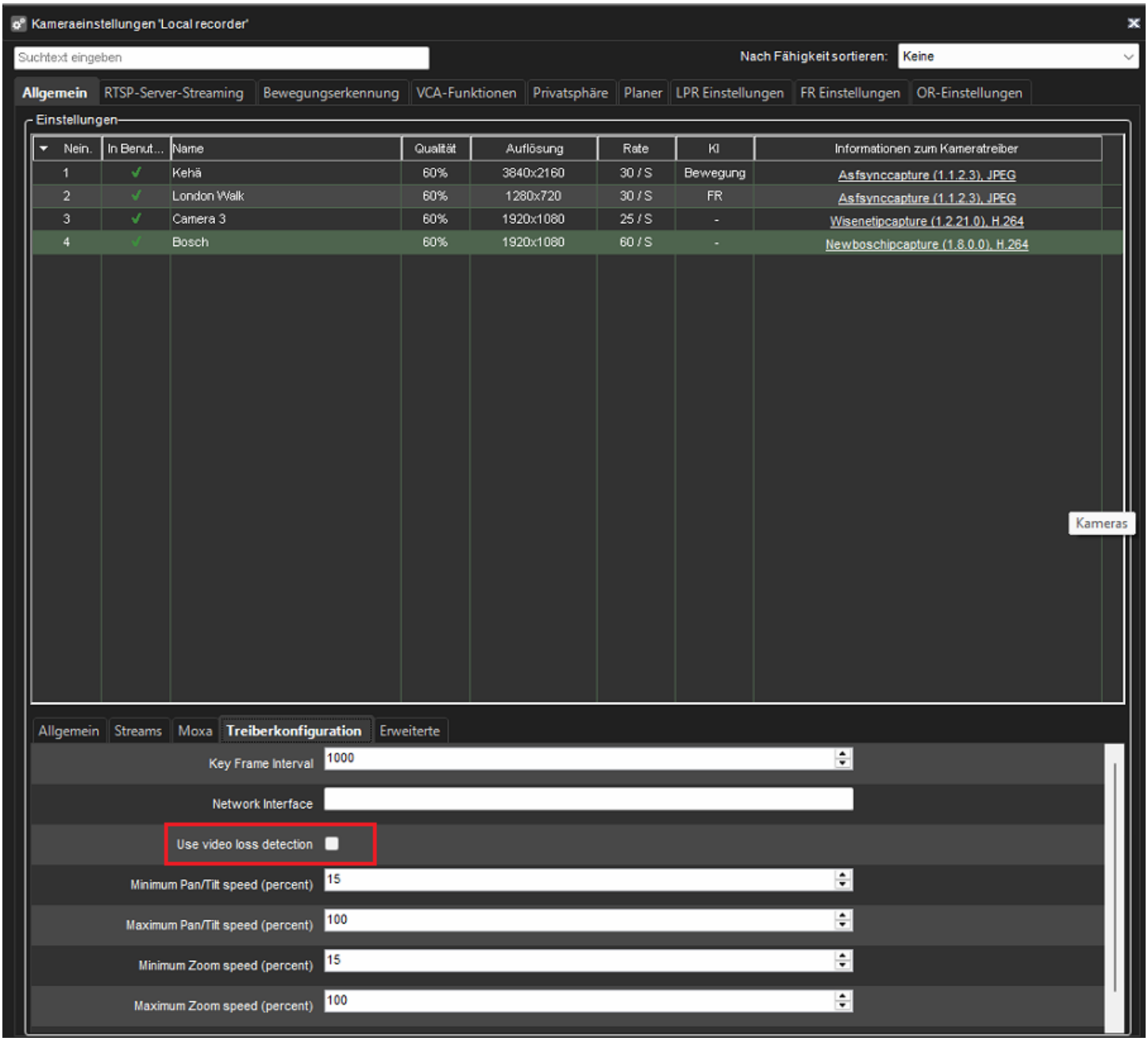




10.7.2.5.2 Ereignis "Signalverlust" im nativen Bosch-Treiber

Benutzer haben jetzt die Möglichkeit, bei der Verwendung von Bosch-Treibern ein "Signalverlust-Ereignis" im nativen Bosch-Treiber zu aktivieren. Diese Funktion ist besonders nützlich für die Überwachung der Signalintegrität und die Sicherstellung einer konsistenten Überwachung. Diese Einstellung ist im System Manager einstellbar. Wenn ein Benutzer diese Option auf "wahr" setzt, bleibt sie auch nach VMS- oder Treiberaktualisierungen erhalten. Dadurch wird sichergestellt, dass die Benutzerpräferenzen für die Überwachung

von Signalereignissen konsistent beibehalten werden, ohne dass die Einstellungen nach einer Aktualisierung neu konfiguriert werden müssen.



10.7.3 Bewegungserkennung

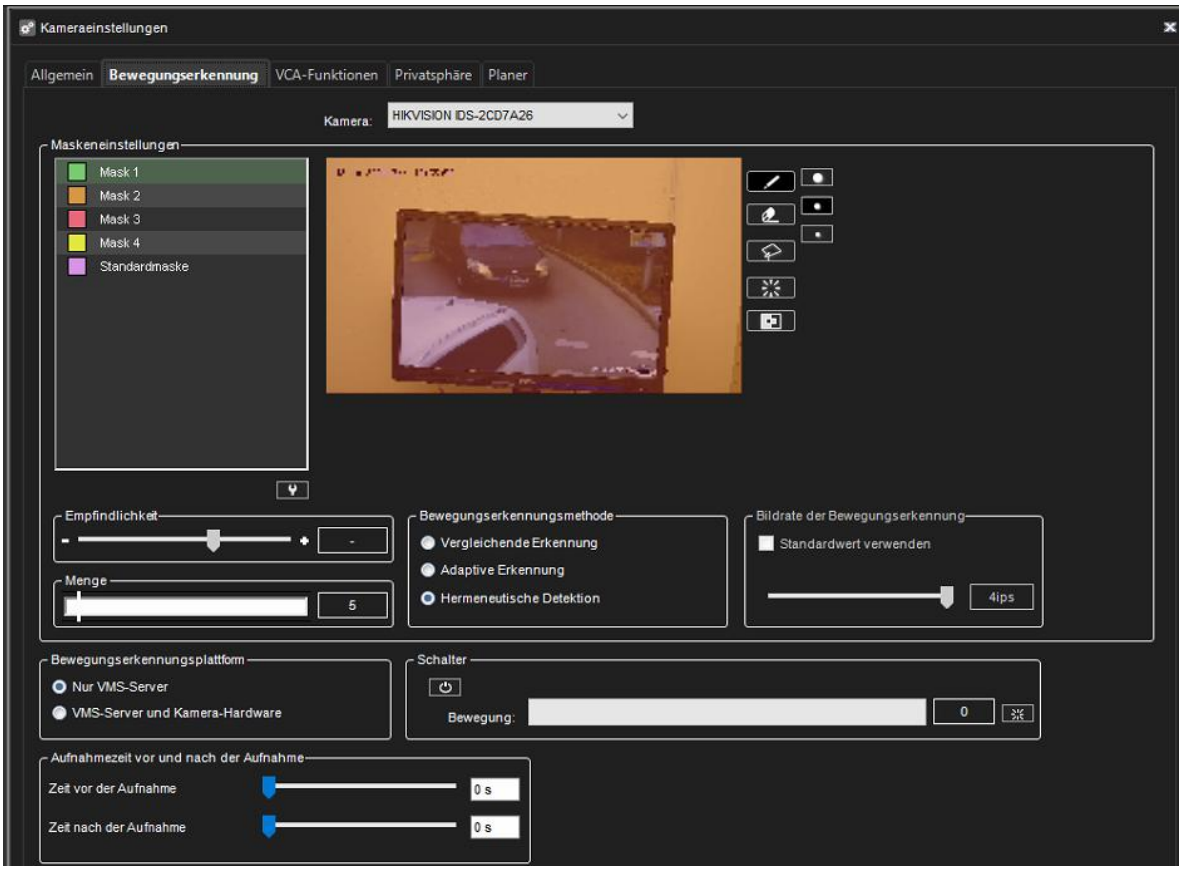
Mit unserer Bewegungserkennungsfunktion können Sie festlegen, welche Aufzeichnungen in unserem Dateisystem gespeichert werden und zur Auslösung von Alarmen verwendet werden können.

Um mit der Bewegungserkennung zu beginnen, müssen Sie Bewegungsmasken konfigurieren, die dann verwendet werden, um zu definieren, ob eine Bewegung auf der Kamera oder im Videostream erkannt wird.

Mithilfe des Schedulers können Sie entscheiden, welche Bewegungsmasken bei der Speicherung von Aufzeichnungen im Dateisystem verwendet werden sollen.

Die durch die Bewegungserkennung erhaltenen Informationen können in den Alarmeinstellungen verwendet werden, um Alarme auszulösen. In den Einstellungen für die Alarmauslösung legen Sie fest, welche Bewegungsmaske für die Bewegungserkennung als Alarmauslöser verwendet werden soll.

Um auf die Konfiguration der Bewegungserkennung im System Manager zuzugreifen, gehen Sie zu VMS Server Settings > Camera Settings > Motion Detection.



10.7.3.1 Empfindlichkeit und Quantität

Das System erkennt Bewegung, wenn:

- Pixel ändern sich mehr als das eingestellte Limit (Empfindlichkeit).
- Die angegebene Pixelanzahl ändert sich (Menge).

Wenn im Bild viele Hintergrundgeräusche vorhanden sind, z. B. Änderungen der Lichtverhältnisse, verringern Sie die Empfindlichkeit, indem Sie den Schieberegler nach links ziehen, oder erhöhen Sie die Mengenbegrenzung, indem Sie den Schieberegler nach rechts ziehen.

10.7.3.2 Methoden zur Bewegungserkennung

10.7.3.2.1 Vergleichende Erkennung

Die vergleichende Erkennung vergleicht ein Bild mit dem vorherigen Bild und kann unter den meisten Bedingungen eingesetzt werden.

Wenn die Unterschiede die eingestellten Grenzwerte überschreiten, erkennt das System eine Bewegung.

> Bei viel Bewegung im Hintergrund, z. B. bei Regen, sich bewegenden Blättern oder wechselnden Lichtverhältnissen, sollten Sie die adaptive Bewegungserkennung verwenden.

10.7.3.2.2 Adaptive Erkennung

Die adaptive Erkennung vergleicht jedes Bild mit einem Hintergrundbild.

Das System lernt automatisch das Hintergrundbild und interpretiert z. B. bewegte Blätter nicht als Bewegung.

Wenn sich mehr als die Hälfte der Pixel in einem Bild ändert, schließt das System daraus, dass sich die Lichtverhältnisse geändert haben, und setzt das Referenzbild zurück und beginnt erneut mit dem Lernen.

10.7.3.2.3 Hermeneutische Entdeckung

Die hermeneutische Erkennung ist ein ausgeklügeltes Bewegungserkennungssystem für schwierige Wetterbedingungen wie starken Regen, „verrauschte“ Hintergrundbilder und Situationen, in denen externe Video-Content-Analysetools (VCA) verwendet werden.

> Die hermeneutische Erkennung erfordert mehr Verarbeitungsressourcen als die anderen Erkennungsmethoden.

10.7.3.3 Bildrate der Bewegungserkennung

Mit der Bildrate für die Bewegungserkennung wird die für die Bewegungserkennung verwendete Bildrate festgelegt.

Es wird im Allgemeinen empfohlen, die Standard-Bildrate zu verwenden.

Bei IP-Kameras verwendet die Bewegungserkennung Intra-Frames und entspricht der Intra-Frame-Rate. Normalerweise ist dies ein Bild pro Sekunde.

10.7.3.4 Bewegungserkennungsplattform

10.7.3.4.1 Nur VMS-Server

Der VMS-Server empfängt alle Videobilder von der Kamera. Der VMS-Server nutzt die konfigurierten Bewegungsmasken oder führt entsprechend den Einstellungen des Zeitplaners eine kontinuierliche Aufzeichnung durch.

10.7.3.4.2 VMS-Server und Kamera-Hardware

Der VMS-Server empfängt jene Videobilder von der Kamera, in denen die Bewegungserkennung der Kamera eine Bewegung festgestellt hat. Der VMS-Server nutzt die konfigurierten Bewegungsmasken oder die kontinuierliche Aufzeichnung entsprechend den Einstellungen des Zeitplaners:

- Bewegungserkennungsmasken: Sowohl die Kameras als auch die Bewegungserkennung des VMS-Servers werden genutzt, um zu verhindern, dass Videos aufgezeichnet werden, wenn Streams zur Anzeige in Client-Anwendungen geöffnet werden.
- Kontinuierliche Aufzeichnung: Es wird ausschließlich die Bewegungserkennung der Kamera verwendet. Beachten Sie, dass das Video, das zur Anzeige an die Client-Anwendungen weitergeleitet wird, ebenfalls aufgezeichnet wird.

10.7.3.5 Konfiguration der Bewegungserkennung

Um auf die Konfiguration der Bewegungserkennung im System Manager zuzugreifen, gehen Sie zu VMS Servereinstellungen > Kameraeinstellungen > Bewegungserkennung.

1. Wählen Sie die Kamera im Dropdown-Menü Kamera aus.
2. Wählen Sie unter Maskeneinstellungen die Maske aus, die Sie konfigurieren möchten.
   Sie können den Namen der Maske ändern.
   Klicken Sie auf Maskenname ändern und geben Sie einen neuen Namen für die Maske ein.
   Bitte beachten Sie, dass die Standardmaskenkonfiguration nicht geändert werden kann.
3. Zeichnen Sie die Maske über das Bild, um festzulegen, für welchen Bereich der Bewegungserkennungs-Feed berechnet werden soll. Verwenden Sie die Zeichenwerkzeuge auf der rechten Seite der Ansicht und malen Sie mit den Zeichenwerkzeugen die Bereiche rot an, in denen das System Bewegungen erkennen soll, und entfernen Sie das Rot aus den Bereichen, in denen Bewegungen ignoriert werden sollen.

10.7.3.5.1 Zeichenutensilien

Werkzeug	Name	Beschreibung
	Bleistift	Verwenden Sie zum Einstellen des Bewegungserkennungsbereichs. Wählen Sie die Stiftgröße aus, indem Sie auf eine der Schaltflächen für die Werkzeuggröße klicken (groß, mittel, klein).

	Radiergummi	Verwenden Sie diese Option, um ausgewählte Bereiche zu löschen, die Sie nicht einschließen möchten. Wählen Sie die Radiergummigröße aus, indem Sie auf eine der Schaltflächen für die Werkzeuggröße klicken (groß, mittel, klein).
	Lasso	Wählen Sie mit geraden Linien Bereiche aus. Wenn das Stiftwerkzeug ausgewählt ist, fügt die Verwendung dieses Werkzeugs ausgewählten Bereichen hinzu. Wenn das Radiergummi-Werkzeug ausgewählt ist, wird dieses Werkzeug aus der Auswahl entfernt. Klicken Sie auf das Bild, bei dem Sie die Auswahl beginnen möchten. Klicken Sie erneut auf die Stelle, an der Sie die Linie verankern möchten, und ändern Sie die Richtung. Um die Auswahl abzuschließen, klicken Sie auf den Startpunkt. Der ausgewählte Bereich wird rot gestrichen oder die rote Farbe wird entfernt.
	Füllen/Löschen	Wenn das Stiftwerkzeug ausgewählt ist, wird durch Klicken auf diese Schaltfläche der gesamte Bildbereich ausgewählt. Wenn das Radiergummi-Werkzeug ausgewählt ist, wird durch Klicken auf diese Schaltfläche alle Auswahlen entfernt.
	Umkehren	Kehrt ausgewählte und nicht ausgewählte Bereiche um. Manchmal ist es einfacher, den Bereich auszuwählen, den Sie nicht maskieren möchten, und dann die Auswahl umzukehren.
	Werkzeuggröße	Klicken Sie auf eine der Schaltflächen, um die Größe des Bleistifts oder Radierers auszuwählen (groß, mittel, klein).

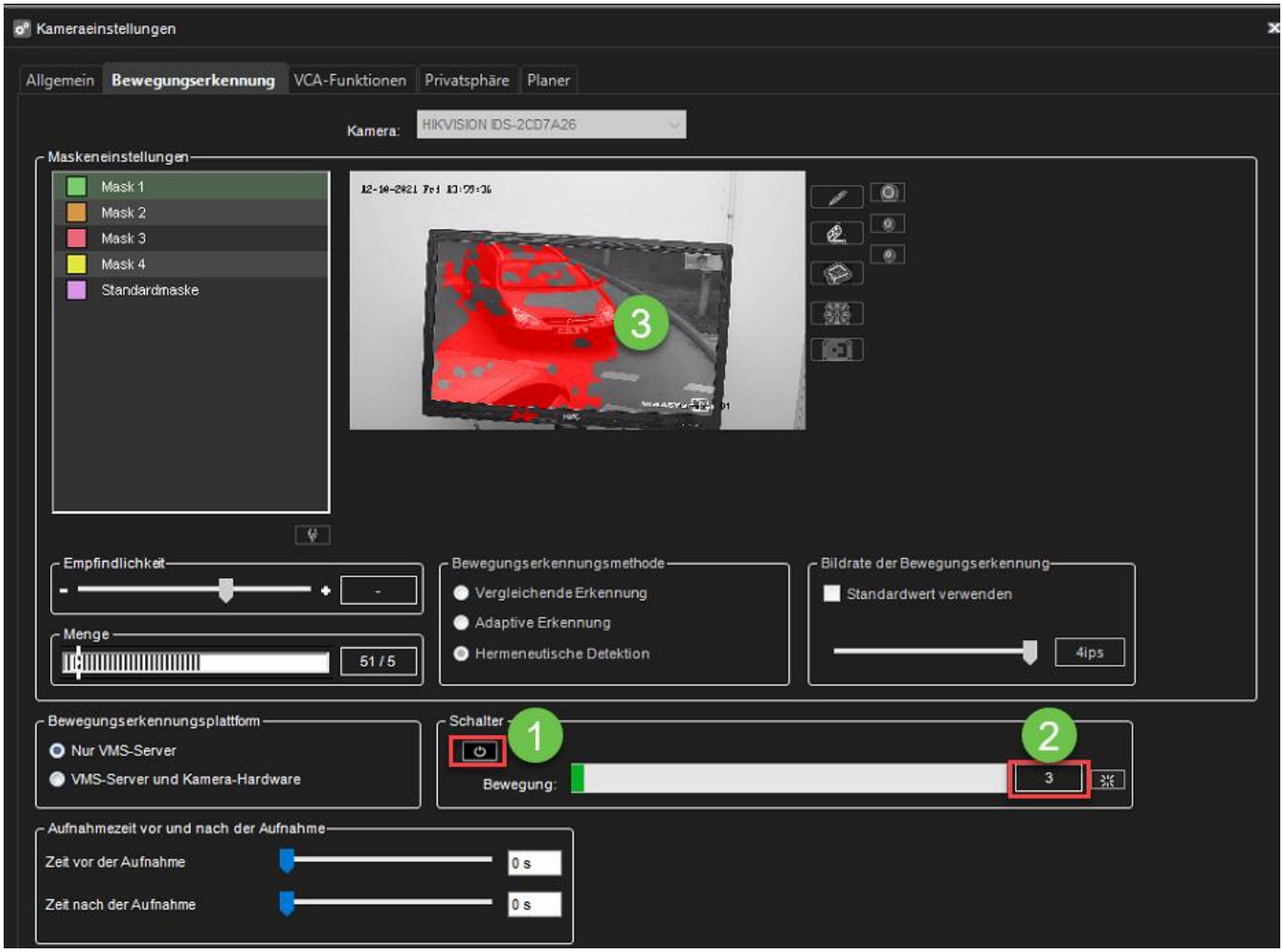
1. Stellen Sie die Erkennungsempfindlichkeit mit dem Schieberegler ein.
2. Stellen Sie mit dem Schieberegler die Mindestmenge an Bewegung ein.
3. Wählen Sie die Bewegungserkennungsmethode. Sie können zwischen vergleichender, adaptiver oder hermeneutischer Bewegungserkennung wählen. Eine ausführlichere Beschreibung dieser Optionen finden Sie auf der vorherigen Seite.
4. Wählen Sie entweder den Standardwert für die Bewegungserkennungs-Bildrate oder verwenden Sie den Schieberegler.
5. Wählen Sie die Bewegungserkennungsplattform, entweder nur den VMS Server oder den VMS Server und die Kamerahardware.
6. Sobald die Konfiguration abgeschlossen ist, müssen die Bewegungserkennungsmasken mit Hilfe des Zeitplaners in Betrieb genommen werden. Um auf die Konfiguration der Bewegungserkennung im System Manager zuzugreifen, gehen Sie zu VMS Server Settings > Camera Settings > Scheduler. Eine Anleitung zur Verwendung des Schedulers finden Sie im nächsten Dokument.

10.7.3.5.2 Schalter

Um die Bewegungserkennung zu testen, können Sie den Zähler verwenden. Wenn Sie den Zähler aktivieren, wird das Video von der Kamera gestreamt und die Bewegungserkennung wird berechnet. Das Ergebnis der Bewegungserkennung wird oben auf dem Bild angezeigt. Der Zählerwert erhöht sich jedes Mal, wenn eine Bewegung erkannt wird, je nach Ihrer Konfiguration.

So verwenden Sie den Zähler:

1. Ermöglichen **Schalter**
2. Überprüfen Sie die Bewegungswerte
3. Das Kamerabild zeigt an, welcher Bereich des Kamerabildes eine Bewegungserkennungsaufzeichnung verursacht



10.7.3.5.3 Vor- und Nachaufzeichnungszeit

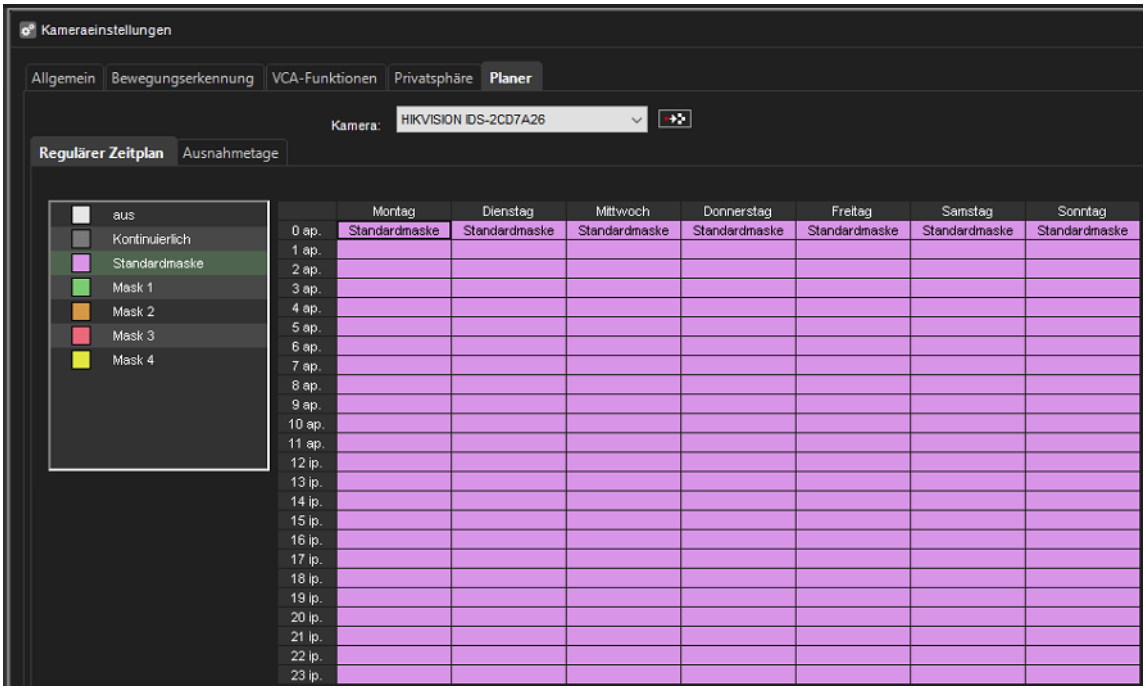
Wenn Sie Material vor und nach der Bewegung aufzeichnen möchten, verwenden Sie die Vor- und Nachaufzeichnung von Bewegung.

- Jede Maske kann separat konfiguriert werden.
- Die Werte reichen von 0s bis 60 Minuten.

- Mit der Schaltfläche Vor- und Nachaufzeichnungszeit für alle Kameras kopieren können Sie die ausgewählten Werte auf alle Kameras übertragen.

10.7.3.6 Planer

Der Planer legt fest, welche Bewegungsmaske für jede Kamera zu welcher Zeit verwendet wird. Sie können aktive Tage für eine Bewegungsmaske auswählen, oder, noch genauer, aktive Stunden. Standardmäßig wird das Video aufgezeichnet, wenn das System eine Bewegung in der Standardmaske erkennt. Die Standardmaske ist standardmäßig 24/7 aktiv.



Für jede Stunde der Woche können Sie verschiedene Optionen einstellen, z. B. die Verwendung unterschiedlicher Bewegungserkennungsmasken am Tag und in der Nacht. Der Planer bietet die folgenden Optionen:

- **aus**
  Video wird nicht aufgezeichnet. Mögliche Alarme werden jedoch aufgezeichnet. Alarme werden in **Alarmeinstellungen** konfiguriert.
- **Kontinuierlich**
  Die Kamera nimmt alle Bilder auf. Diese Option verbraucht viel Speicherplatz.
- **Standardmaske**
  Die Kamera zeichnet Videos mit der Standard-Bewegungserkennungsmaske und den Standard-Bewegungserkennungsparametern auf.
- **Benutzerdefinierte Maske.**
  Die Kamera nimmt Videos mit einer benutzerdefinierten Maske auf. Jede Kamera kann bis zu vier benutzerdefinierte Masken haben.

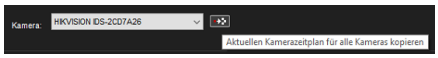
10.7.3.6.1 So verwenden Sie den Scheduler

1. Legen Sie den regulären Wochenplan auf der Registerkarte Regulärer Zeitplan fest.
2. Legen Sie bei Bedarf Feiertagszeitpläne auf der Registerkarte Feiertage fest.
3. Um den Zeitplan zu ändern, klicken Sie auf die Bewegungsmaske, die Sie auswählen möchten.
4. Klicken Sie auf die geplante Stunde, in der die Bewegungsmaske verwendet werden soll.
    - Um mehrere Stunden gleichzeitig zu ändern, ziehen Sie mit der Maus oder klicken Sie auf die erste Zelle, halten Sie die UMSCHALTTASTE gedrückt und klicken Sie dann auf die letzte Zelle.
    - Um alle Stunden in einer Spalte oder einer Zeile zu ändern, klicken Sie auf die Spalten- oder Zeilenüberschrift.
    - Um alle Stunden der Woche zu ändern, klicken Sie auf die Zelle über der Stundenspalte (auf der linken Seite der Wochentagsüberschriftenzeile).
5. Klicken Sie auf das Symbol „Speichern“ ✔ at am unteren Rand der Seite, um alle Kameraeinstellungen zu speichern.

10.7.3.6.2 Kopieren eines Zeitplans für alle Kameras

Sie können den aktuell ausgewählten Aufnahmezeitplan für alle Kameras im System kopieren.

1. Klicken Sie auf Zeitplan kopieren.



2. Die Standardmaske ist rund um die Uhr aktiv.

10.7.3.6.3 Einstellung von Ausnahmetagen für Feiertage

Sie können alternative Aufzeichnungszeitpläne für Feiertage verwenden und einen Tageszeitplan aus dem regulären Zeitplan anwenden oder einen Zeitplan für Ausnahmetage verwenden.

10.7.3.6.3.1 Hinzufügen eines Zeitplans für Ausnahmetage

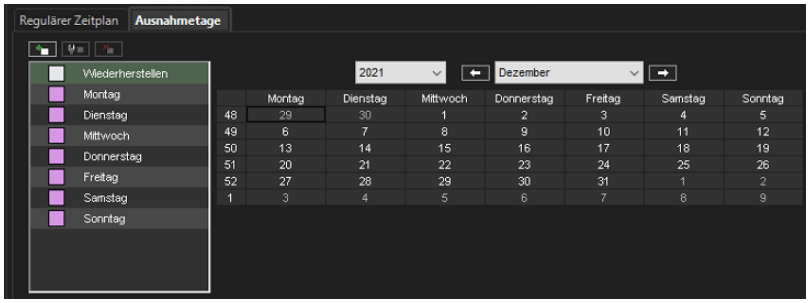
1. Klicken Sie auf **Zeitplan hinzufügen**



1. Geben Sie einen Namen für den Zeitplan ein.
2. Klicken Sie auf die Maske, die Sie anwenden möchten, und klicken Sie dann auf die Stunden, auf die Sie die Maske anwenden möchten.
3. Klicken **OK**.

10.7.3.6.3.2 Zeitpläne für Ausnahmetage verwenden

1. Klicken Sie auf die Registerkarte Ausnahmetage.
2. Wählen Sie das Jahr und den Monat aus.
3. Klicken Sie im linken Bereich auf den Zeitplan, den Sie anwenden möchten.
4. Klicken Sie auf den Feiertag im Kalender.



10.7.3.6.3.3 Bearbeiten eines benutzerdefinierten Zeitplans

1. Wählen Sie den Zeitplan aus.
2. Klicken Sie auf Zeitplan bearbeiten.
3. Nehmen Sie die Änderungen vor, die Sie vornehmen möchten.
4. Klicken Sie auf OK.

10.7.3.6.3.4 Löschen eines benutzerdefinierten Zeitplans

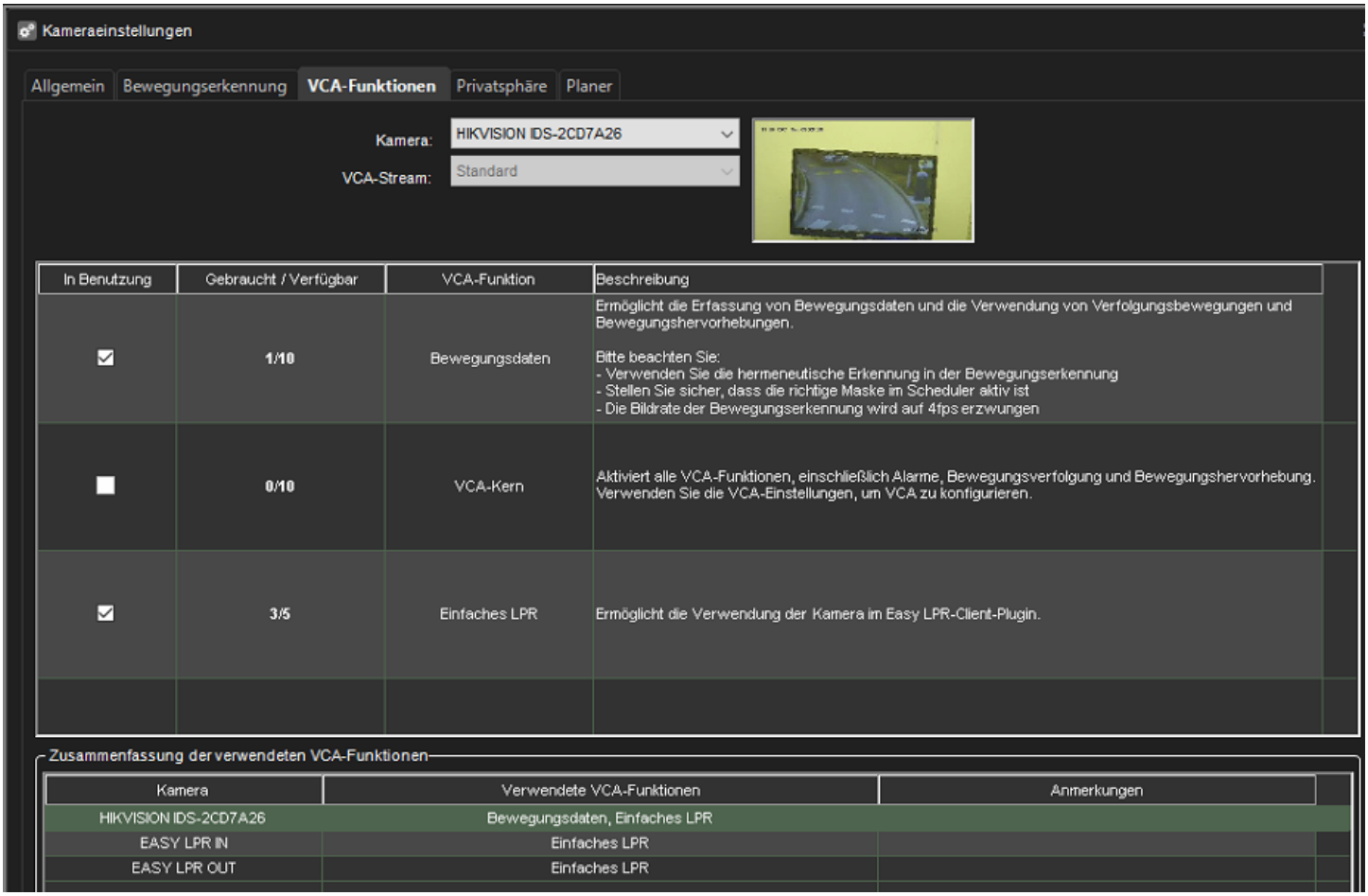
1. Wählen Sie den Zeitplan im linken Fensterbereich aus.
2. Klicken Sie auf Zeitplan löschen.
3. Bestätigen Sie, dass der Zeitplan gelöscht werden soll.

10.7.3.6.4 Wiederherstellen des ursprünglichen Zeitplans

1. Klicken Sie auf Wiederherstellen
2. Klicken Sie auf den Tag, den Sie wiederherstellen möchten.
3. Klicken Sie zum Speichern auf ✔.

10.7.4 VCA-Funktionen

Wenn die Softwarelizenz Video Content Analytics (VCA)-Funktionalität umfasst, kann sie kameraspezifisch auf der Registerkarte **VCA-Funktionen** verwaltet werden.
Je nach Lizenz können bestimmte VCA-Funktionalitäten auf der Registerkarte aktiviert oder deaktiviert werden. Dies ist möglich um zu steuern, welcher Stream (in einer konfigurierten Kamera zur Verwendung mehrerer Streamings) für VCA verwendet wird.
Dies wird über das Pulldown-Menü unter der Kameraauswahl erreicht (siehe folgendes Bild).



Die Registerkarte VCA-Funktionen

Im Primärzustand enthält die Registerkarte die folgenden VCA-Funktionen:

- **Bewegungsdaten:** Internal VCA-Bewegungsdaten, die Datenerfassung, Bewegungsverfolgung und Bewegungshervorhebung ermöglichen. Visualisiert in **Mirasys Spotter**.
- **VCA Core:** ermöglicht die volle VCA-Funktionalität. Konfiguriert über die VCA-Einstellungen im Systemmanager.

- **Easy LPR**: Ermöglicht die Verwendung der Kamera im Easy LPR Client-Plugin

Bitte beachten Sie, dass die VCA-Funktionen nur verfügbar sind, wenn sie über die Lizenz aktiviert sind.

10.7.5 Privatsphäre

Unter dem Datenschutz-Menü können Sie die Privatzonen der Kamera und die Gesichts- und Bewegungsunschärfe-Funktionalität steuern.
Zu beachten: Der Inhalt der Privatleben-Funktionalitäten ist (für den Benutzer) nur verfügbar, wenn sie für die Kamera definiert sind.
(Dh wenn die kamera nicht hat, z.b. Wenn die Gesichtsunschärfe definiert ist, dürfen diese Kameras die Gesichter nicht unscharf machen – selbst wenn die Benutzergruppe des Endbenutzers die Berechtigungsstufe so eingestellt hätte, dass nur unverschwommene Materialien angezeigt werden.
Dies gilt auch beim Exportieren der Materialien.

10.7.5.1 Privatzone auf der Kamera

10.7.5.1.1 Datenschutzzone hinzufügen

1. Wählen Sie auf der Registerkarte **Privatzonen** die Kamera aus der Kameraliste aus.
2. Wählen Sie **Privacy-Zone an der Kamera**
3. Klicken Sie auf **Privatzone hinzufügen**.
4. Malen Sie die Privatzone auf die Kameraansicht. Die neu erstellte Zone wird halbtransparent hellgrau dargestellt. Sie können die Zone durch Ziehen in der Größe ändern und verschieben.
5. Wiederholen Sie die Schritte 1 bis 3, um so viele private Zonen wie erforderlich zu erstellen.
6. Klicken Sie auf **OK**.



10.7.5.1.2 Entfernen der Privatzone

So entfernen Sie Privatzonen:

1. Wählen Sie auf der Registerkarte **Privatzonen** die Kamera aus der Kameraliste aus.
2. Klicken Sie in der Kameraansicht auf eine Privatzone.
3. Klicken Sie auf **Privatzone entfernen** oder **Alle Privatzonen entfernen**.
4. Klicken Sie auf **OK**.

10.7.5.1.3 ONVIF Profile T Unterstützung der Maskierung der Privatsphäre

Unser ONVIF-Treiber wurde aktualisiert, um automatisch zu erkennen, ob ein Profil T Gerät die Einrichtung von Privatzonen unterstützt. Diese Funktion bietet eine bessere Kontrolle über Videoüberwachungsinhalte und ermöglicht es den Benutzern, die Privatzonenmaskierung der Kamera für unser VMS im Systemmanager hinzuzufügen, zu entfernen oder zu ändern.

Weitere Informationen finden Sie unter **Administratorhandbuch > VMS Server > Kameras > Privatsphäre**

Privatzone hinzufügen.

10.7.5.2 Privatzone auf dem Client

Auf dem Spotter-Client: Diese Datenschutzzonen sind nur auf dem Anzeige-Client implementiert. Dadurch kann das vollständige Video aufgezeichnet und exportiert werden, aber die Bereiche mit Datenschutzabschirmung sind nur für Benutzer zugänglich, die dazu berechtigt sind.

10.7.5.2.1 Datenschutzzone hinzufügen

1. Wählen Sie auf der Registerkarte **Privatzonen** die Kamera aus der Kameraliste aus.

2. Wählen Sie **Privacy-Zone auf dem Client**
3. Klicken Sie auf **Privatzone hinzufügen**.
4. Malen Sie die Privatzone auf die Kameraansicht. Die neu erstellte Zone wird halbtransparent hellgrau dargestellt. Sie können die Zone durch Ziehen in der Größe ändern und verschieben.
5. Wiederholen Sie die Schritte 1 bis 3, um so viele private Zonen wie erforderlich zu erstellen.
6. Klicken Sie auf **OK**.



10.7.5.2.2 Entfernen der Privatzone

So entfernen Sie Privatzonen:

1. Wählen Sie auf der Registerkarte **Privatzone** die Kamera aus der Kameraliste aus.
2. Klicken Sie in der Kameraansicht auf eine Privatzone.
3. Klicken Sie auf **Privatzone entfernen** oder **Alle Privatzonen entfernen**.
4. Klicken Sie auf **OK**.

10.7.5.3 Unschärfe von Objekten

Die Einstellungen „Gesichter unkenntlich machen“ und „Bewegte Objekte unkenntlich machen“ können als zusätzlicher Datenschutz eingerichtet werden ausreichende Berechtigungen.)
Die Unschärfe funktioniert nicht auf der Spotter-Seite – oder für den Export des Videomaterials für die Kameras, wenn sie nicht auf der Seite des Systemadministrators ausgewählt wurden.
Höhere Auflösungen, die für die Algorithmen verwendet werden, bedeuten eine höhere Genauigkeit für die Algorithmen – aber auch eine höhere CPU Ladungen.

10.7.5.3.1 Gesichter verwischen

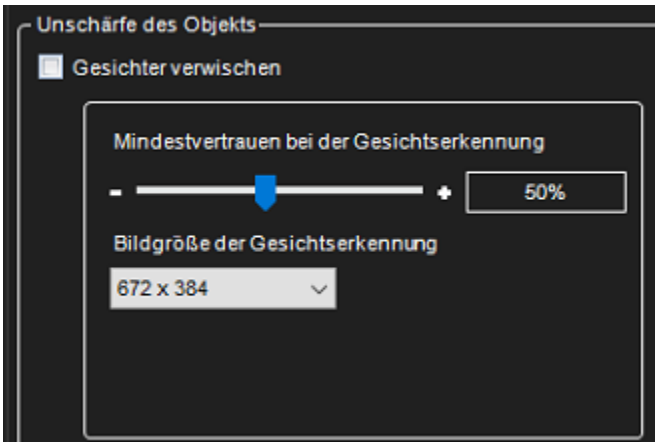
10.7.5.3.1.1 Mindestvertrauen bei der Gesichtserkennung

10.7.5.3.1.2 Bildgröße der Gesichtserkennung

Bei einem kleinen Wert für die Gesichtserkennungsgröße muss das Gesicht einer Person näher an der Kamera sein. Die Gesichtserkennung wird schneller.

Verwendung eines größeren Werts für die Gesichtserkennungsgröße. das Gesicht einer Person wird weiter von der Kamera entfernt erkannt.

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



10.7.5.3.2 Verwischen Sie sich bewegende Objekte

10.7.5.3.2.1 Empfindlichkeit der Bewegungserkennung

Wie empfindlich Pixel im Bild als Bewegungspixel
erkannt werden

10.7.5.3.2.2 Länge des Hintergrundbilderkennungsverlaufs

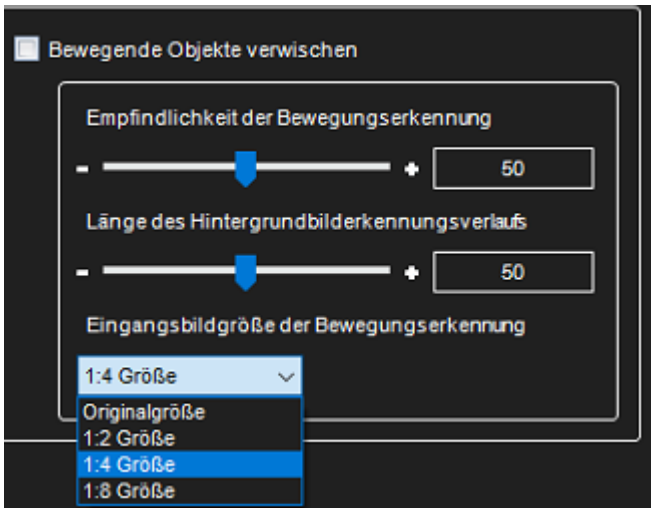
Wie schnell stationäre Objekte als Hintergrund erkannt werden

10.7.5.3.2.3 Eingangsbildgröße der Bewegungserkennung

Die kleinere Größe ist schneller zu verarbeiten, liefert aber die schlechteren Ergebnisse.

- Originalgröße
- 1:2 Größe

- 1:4 Größe
- 1:8 Größe



10.7.6 Einstellungen für die License Plate Recognition (LPR)

Systemadministrator-Einstellungen, die es Betreibern ermöglichen, die Nummernschilderkennung in Spotter Smart Search und Spotter Smart Recognition zu nutzen.

> Für die Smart LPR-Funktion ist eine RTSP-Server-Streaming-Lizenz erforderlich.

10.7.6.1 Einstellungen für die License Plate Recognition

Die Einstellungen für die Nummernschilderkennung finden Sie im Systemmanager auf der Registerkarte VMS-Server > Kameras.

Wechseln Sie im Fenster Kameraeinstellungen zur Registerkarte LPR-Einstellungen.

> Wenn Ihre Lizenz die Smart LPR-Funktion nicht unterstützt, wird die Registerkarte LPR-Einstellungen ausgeblendet.

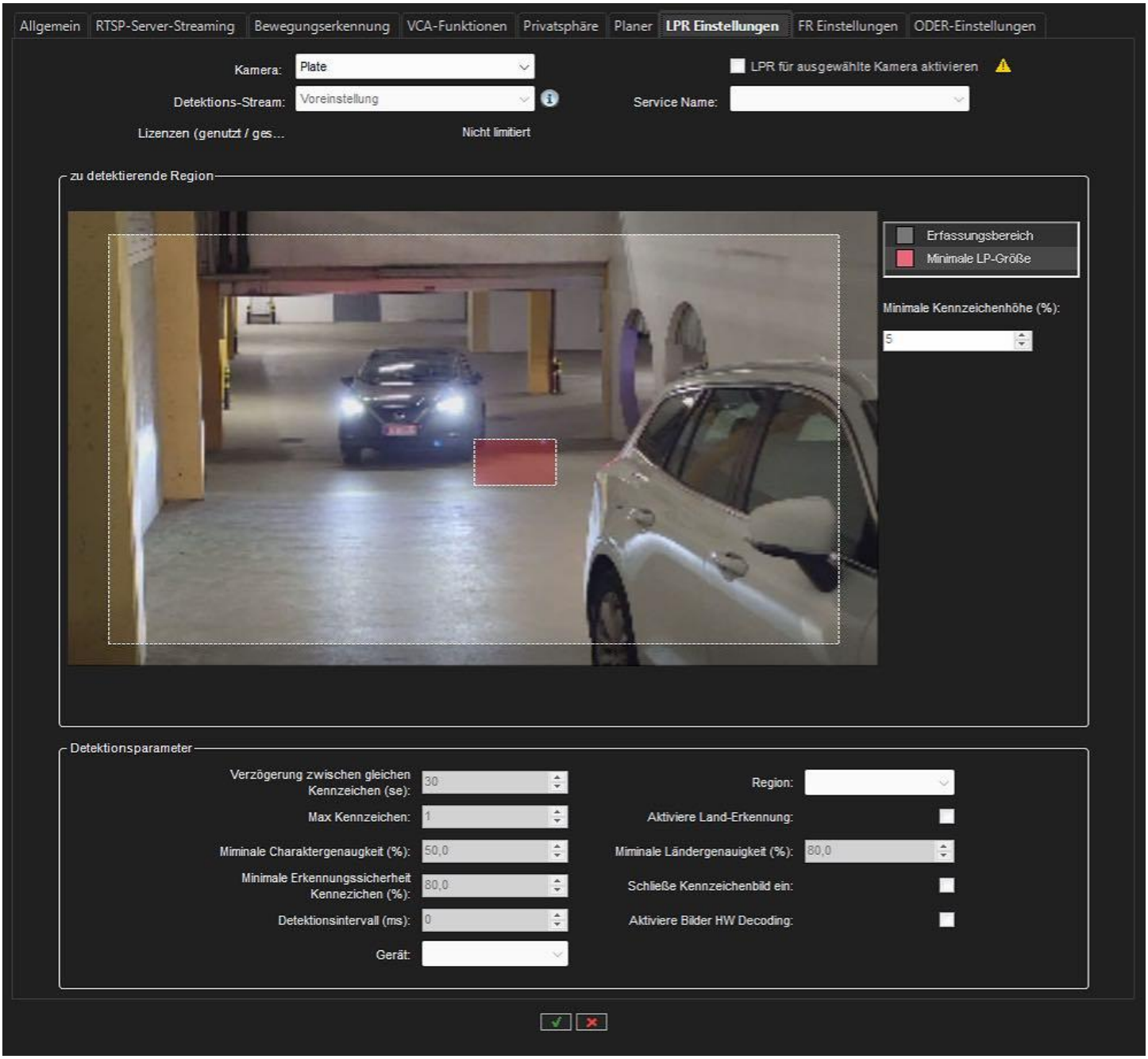
10.7.6.1.1 Kamera auswählen, streamen und LPR aktivieren

1. Wählen Sie die Kamera aus dem Dropdown-Menü in LPR
2. Wenn es mehr als einen Stream gibt, können Sie den Stream auswählen. Wenn nur ein Stream vorhanden ist, gibt es einen Standardstream wie in der Abbildung oben, und das Dropdown-Menü ist deaktiviert.
3. Sie können erst dann einen Dienst auswählen, wenn Sie den Dienst durch Anklicken des Kästchens LPR für ausgewählte Kamera aktivieren aktiviert haben.

4. Wenn das Kontrollkästchen LPR für die ausgewählte Kamera aktivieren nicht markiert ist, ist das Dropdown-Menü Dienst deaktiviert.
5. Das Textfeld Lizenz zeigt die Anzahl der verwendeten Lizenzen und die maximale Anzahl der Lizenzen an.

10.7.6.2 Erkennungsparameter

Nachdem die Kamera, ihr Stream und der LPR-Erkennungsdienst ausgewählt wurden, können die Kennzeichenerkennungseinstellungen angepasst werden. Die Kennzeichenerkennungseinstellungen befinden sich im Gruppenfeld Erkennungsparameter auf der Registerkarte LPR-Einstellungen im Fenster Kameraeinstellungen.



Die Kennzeichenerkennungseinstellungen werden für die Konfiguration des Kennzeichenerkennungsdetektors verwendet.

- **Bereich von Interesse** - Definieren Sie den Bereich, in dem die Erkennungen durchgeführt werden.
- **Verzögerung bei gleichem Kennzeichen** - die Anzahl der Sekunden, die vergehen sollen, bevor das gleiche Kennzeichen zweimal gelesen wird.

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

- **Max plates** - maximale Anzahl der zu erkennenden Platten. Erkannte Kennzeichen werden in absteigender Reihenfolge nach der Kennzeichenkonfidenznummer sortiert.
- **Minimale Zeichenkonfidenz** - Konfidenzniveau für die Erkennung von Plattenzeichen. Gültige Werte liegen zwischen 25% und 95%.
- **Minimale Kennzeichenkonfidenz** - Konfidenzniveau des Erkenners. Gültige Werte liegen im Bereich von 25% - 95%.
- **Minimale Plattenhöhe** - minimale Plattenhöhe in %. Gültige Werte liegen im Bereich von 1% - 50%. Der Standardwert ist 5%.
- **Erkennungsintervall -** die Anzahl der Millisekunden, die beschreibt, wie oft die Kennzeichenerkennung durchgeführt wird: wenn es z.B. 250ms ist, dann wird die Kennzeichenerkennung 4 mal in einer Sekunde durchgeführt (auch wenn die Bildrate des Videostroms viel höher ist, wie 30 fps).
- **Gerät** - wird für die Inferenz verwendet. Die verfügbaren Geräte hängen von der Hardware des aktuellen Dienstes ab.
- **Region** - Das Erkennungsmodell (Eurasien oder Amerika), das für die Erkennung verwendet werden soll.
- **Minimum country confidence** - Konfidenzniveau des Ländererkenners. Gültige Werte liegen zwischen 25% und 95%.
- **Ländererkennung aktivieren** - Aktivieren oder Deaktivieren der Ländererkennung. Die Aktivierung der Ländererkennung kann in einigen Fällen die Kennzeichenerkennung verbessern.
- **Kennzeichenbilder einbeziehen** - Kennzeichenbilder in die zurückgegebenen Daten einbeziehen oder nicht.
- **Bilder HW-Dekodierung aktivieren** - aktiviert die Dekodierung von Eingabebildern mit der am besten geeigneten Computerplattform (CUDA, DXVA oder DirectX).

10.7.6.3 Einstellungen speichern

1. Klicken Sie auf die Schaltfläche OK mit dem grünen Häkchensymbol am unteren Rand des Fensters Kameraeinstellungen.
2. Klicken Sie auf die Schaltfläche Abbrechen mit dem roten Kreuzsymbol, um das Speichern der LPR-Einstellungen abzubrechen und zu den Einstellungswerten zurückzukehren, die nach dem Öffnen der Anwendung System-Manager geladen wurden.
3. Die LPR-Einstellungen für die ausgewählte Kamera werden nach dem Einschalten anderer Kameras, Streams oder Registerkarten vorübergehend gespeichert.

Wenn Sie die Stream-Einstellungen für die ausgewählte Kamera und den ausgewählten Erkennungs-Stream löschen möchten, wählen Sie im Feld Dienstname Combobx für die ausgewählte Kamera und den ausgewählten Erkennungs-Stream "Keine" aus.

10.7.6.4 Einfluss auf die Einstellungen

Die folgenden Aktionen wirken sich unabhängig von den Aktionen auf der Registerkarte LPR-Einstellungen auf die Diensteinstellungen aus:

- **Löschen eines Rekorders**: Beim Löschen eines Rekorders werden alle Streams in den Einstellungen aller LPR-Dienste, die mit dem entfernten Rekorder gearbeitet haben, gelöscht und die LPR-Einstellungen gespeichert.
- **Löschen einer Kamera**: Beim Löschen einer Kamera wird der Stream in den Einstellungen aller LPR-Dienste, die mit dieser Kamera gearbeitet haben, und beim Speichern der LPR-Einstellungen gelöscht. Es gibt eine Regel - eine Kamera mit einem Stream kann nur von einem LPR-Dienst verwendet werden, aber ein LPR-Dienst kann mit mehreren Kameras arbeiten.
- **Ändern der Bildgröße und des Kompressionstyps auf der Unterregisterkarte Streams der Registerkarte Allgemein**: Wenn Sie die Auflösung oder den Kompressionstyp für die Kamera und den Stream ändern, die in den Einstellungen eines beliebigen LPR-Dienstes enthalten sind, werden die Einstellungen des LPR-Dienstes geändert und gespeichert, wenn das Fenster Kameraeinstellungen geschlossen wird.
- **Ändern der RTSP-Streaming-Einstellungen in der Gruppe "Streaming-Einstellungen" auf der Registerkarte "RTSP-Server-Streaming"**: Wenn Sie das "Kennwort", den "Benutzernamen", den "RTSP-Port" und den "Streaming-Modus" (Sicherheitstyp) für die ausgewählte Kamera und den Stream ändern, die in den Einstellungen eines beliebigen LPR-Dienstes enthalten sind, werden die Einstellungen des LPR-Dienstes geändert und gespeichert, wenn das Fenster "Kameraeinstellungen" geschlossen wird.
- **Ändern der Bildgröße in der Gruppe "Geräteeinstellungen" auf der Registerkarte "Video" im Fenster "Hardware-Einstellungen"**: Wenn Sie die Auflösung für die ausgewählte Kamera ändern (hier ist es möglich, die Auflösung nur für den Aufzeichnungs-Stream zu ändern), die in den Einstellungen eines beliebigen LPR-Dienstes vorhanden ist, werden die Einstellungen des LPR-Dienstes geändert und gespeichert, wenn das Fenster "Hardware-Einstellungen" geschlossen wird.
- **Ändern der Kamera durch Klicken auf die Schaltfläche IP-Kamera bearbeiten auf der Registerkarte Video im Fenster Hardware-Einstellungen**: Wenn Sie die Kamera durch Klicken auf die Schaltfläche IP-Kamera bearbeiten ändern, werden die Auflösung und der Kompressionstyp für die neue Kamera (nur für Aufzeichnungs-Stream) in den Einstellungen des LPR-Dienstes neu geschrieben, wo die Kamera-ID angezeigt wird.

10.7.7 Einstellungen für die Face Recognition

Systemadministrator-Einstellungen, die es Bedienern ermöglichen, die Gesichtserkennung in Spotter Smart Search und Spotter Smart Recognition zu nutzen.

Für diese Funktion ist eine **RTSP-Server-Streaming-Lizenz** erforderlich.

10.7.7.1 Einstellungen für die Face Recognition

Die Einstellungen für die Gesichtserkennung finden Sie im System Manager auf der Registerkarte **VMS Server** > **Kameras**.

Gehen Sie im Fenster Kameraeinstellungen auf die Registerkarte **FR-Einstellungen**.

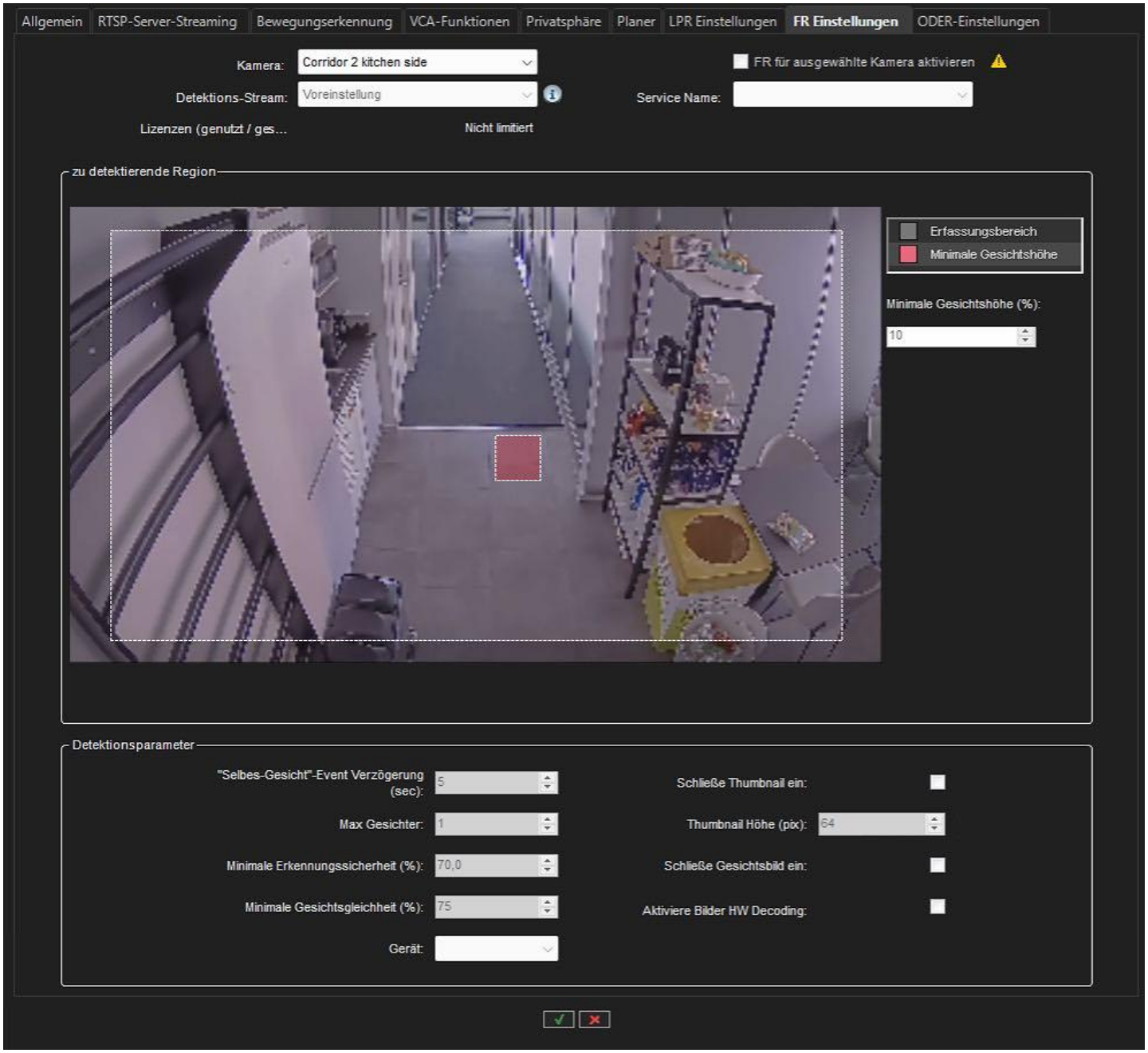
> Wenn Ihre Lizenz die **Smart FR**-Funktion nicht unterstützt, wird die Registerkarte F**R-Einstellungen** ausgeblendet.

10.7.7.1.1 Kamera auswählen, streamen und FR aktivieren

1. Wählen Sie die **Kamera** aus dem Dropdown-Menü in FR
2. Wenn es mehr als einen **Stream** gibt, können Sie den Stream auswählen. Wenn nur ein Stream vorhanden ist, gibt es einen Standard-Stream, wie in der Abbildung oben, und das Dropdown-Menü ist deaktiviert.
3. Sie können einen Dienst erst auswählen, nachdem Sie den Dienst durch Anklicken des Kästchens **FR für ausgewählte Kamera aktivieren** aktiviert haben.
4. Wenn das Kästchen **FR für ausgewählte Kamera aktivieren** nicht angekreuzt ist, ist das Dropdown-Menü Dienst deaktiviert.
5. Das Textfeld Lizenz zeigt die Anzahl der verwendeten Lizenzen und die maximale Anzahl der Lizenzen an.

10.7.7.2 Face detection Einstellungen

Nachdem die Kamera, ihr Stream und der FR-Erkennungsdienst ausgewählt wurden, können die Einstellungen für die Gesichtserkennung angepasst werden. Die Einstellungen für die Gesichtserkennung finden Sie im Gruppenfeld Erkennungsparameter auf der Registerkarte FR-Einstellungen im Fenster Kameraeinstellungen.



10.7.7.3 Erkennungsparameter

Die Gesichtserkennungseinstellungen werden für die Konfiguration des Gesichtserkennungsdetektors verwendet.

Bereich von Interesse - Definieren Sie den Bereich, in dem die Erkennungen durchgeführt werden.

Max faces - maximale Anzahl der Gesichter, die im Bild erkannt werden sollen. Der Wert sollte zwischen 1 und 20 liegen.

Mindestvertrauen - Vertrauensniveau des Erkenners. Wenn das Vertrauen für das erkannte Gesicht unter diesem Schwellenwert liegt, wird das Gesicht ignoriert. Gültige Werte liegen zwischen 25% und 95%.

Minimale Gesichtshöhe - minimale Gesichtshöhe in %. Gültige Werte liegen zwischen 5 und 50%%. Standardwert 10%.

Minimale Gesichtsähnlichkeit - Wenn die Ähnlichkeit größer oder gleich diesem Wert ist, handelt es sich um dasselbe Gesicht. Der Wert sollte zwischen 50% und 95% liegen.

Verzögerung bei Ereignissen mit demselben Gesicht - die Anzahl der Sekunden, die vergehen sollten, bevor ein Ereignis mit demselben Gesicht auftritt.

Gerät - wird für die Inferenz verwendet. Die verfügbaren Geräte hängen von der Hardware des aktuellen Dienstes ab.

Thumbnail height - die Höhe des Thumbnail-Bildes in Pixeln. Der Wert sollte zwischen 32 und 128 Pixeln liegen.

Miniaturbild einschließen - schließt das Miniaturbild der Erkennungsquelle in die zurückgegebenen Daten ein oder nicht.

Gesichtsbilder einschließen - schließt Gesichtsbilder in die zurückgegebenen Daten ein oder nicht.

Enable images HW decoding - Aktiviert die Dekodierung von Eingabebildern mit der am besten geeigneten Computerplattform (CUDA, DXVA oder DirectX).

10.7.7.4 Einstellungen speichern

1. Klicken Sie auf die Schaltfläche **OK** mit dem grünen Häkchen am unteren Rand des Fensters **Kameraeinstellungen**, um zu speichern.
2. Klicken Sie auf die Schaltfläche **Abbrechen** mit dem roten Kreuzsymbol, um das Speichern der FR-Einstellungen abzubrechen und zu den Einstellungswerten zurückzukehren, die nach dem Öffnen der Anwendung **System Manager** geladen wurden.

Wenn Sie Stream-Einstellungen für die ausgewählte Kamera und den ausgewählten Erkennungs-Stream löschen, sollte in der Combobox für den **Dienstnamen** der Wert "Kein" ausgewählt sein.

10.7.7.5 Beeinflussung der Einstellungen

Die folgenden Aktionen wirken sich unabhängig von den Aktionen auf der Registerkarte FR-Einstellungen auf die Diensteinstellungen aus:

- **Löschen eines Rekorders**: Beim Löschen eines Rekorders werden alle Streams in den Einstellungen aller FR-Dienste, die mit dem entfernten Rekorder gearbeitet haben, gelöscht und die FR-Einstellungen gespeichert.

- **Löschen einer Kamera**: Beim Löschen einer Kamera wird der Stream in den Einstellungen aller FR-Dienste, die mit dieser Kamera gearbeitet haben, gelöscht und die FR-Einstellungen gespeichert. Es gibt eine Regel - eine Kamera mit einem Stream kann nur von einem FR-Dienst verwendet werden, aber ein FR-Dienst kann mit mehreren Kameras arbeiten.
- **Ändern der Bildgröße und des Kompressionstyps auf der Unterregisterkarte Streams der Registerkarte Allgemein**: Wenn Sie die Auflösung oder den Kompressionstyp für die Kamera und den Stream ändern, die in den Einstellungen eines beliebigen FR-Dienstes vorhanden sind, werden die Einstellungen des FR-Dienstes geändert und gespeichert, wenn das Fenster **Kameraeinstellungen** geschlossen wird.
- **Ändern der RTSP-Streaming-Einstellungen in der Gruppe Streaming-Einstellungen auf der Registerkarte RTSP-Server-Streaming**: Wenn Sie das "Kennwort", den "Benutzernamen", den "RTSP-Port" und den "Streaming-Modus" (Sicherheitstyp) für die ausgewählte Kamera und den Stream ändern, die in den Einstellungen eines beliebigen FR-Dienstes enthalten sind, werden die Einstellungen des FR-Dienstes geändert und gespeichert, wenn das Fenster **Kameraeinstellungen** geschlossen wird.
- **Ändern der Bildgröße in der Gruppe Geräteeinstellungen auf der Registerkarte Video im Fenster Hardware-Einstellungen**: Wenn Sie die Auflösung für die ausgewählte Kamera ändern (hier ist es möglich, die Auflösung nur für den **Aufzeichnungs**-Stream zu ändern), die in den Einstellungen eines beliebigen FR-Dienstes vorhanden ist, werden die Einstellungen des FR-Dienstes geändert und gespeichert, wenn das Fenster **Hardware-Einstellungen** geschlossen wird.
- **Ändern der Kamera durch Klicken auf die Schaltfläche IP-Kamera bearbeiten auf der Registerkarte Video im Fenster Hardware-Einstellungen**: Wenn Sie die Kamera durch Klicken auf die Schaltfläche IP-Kamera bearbeiten ändern, werden die Auflösung und der Kompressionstyp für die neue Kamera (nur für den **Aufzeichnungs**-Stream) in den Einstellungen des FR-Dienstes neu geschrieben, wo die Kamera-ID angezeigt wird; die Einstellungen des FR-Dienstes werden geändert und gespeichert, wenn das Fenster **Hardware-Einstellungen** geschlossen wird.

10.7.8 Einstellungen für die Object Recognition (OR)

Systemadministrator-Einstellungen, die es Operatoren ermöglichen, die Objekterkennung in der Spotter Smart Search zu nutzen.

10.7.8.1 Object Recognition Settings

Die Einstellungen für die Objekterkennung finden Sie im Systemmanager auf der Registerkarte VMS Server > Kameras.

Gehen Sie im Fenster Kameraeinstellungen auf die Registerkarte OP-Einstellungen.

> Wenn die Benutzerlizenz die Objekterkennungsfunktion nicht unterstützt, wird die Registerkarte OR-Einstellungen ausgeblendet.

10.7.8.1.1 Kamera auswählen, streamen und aktivieren ODER

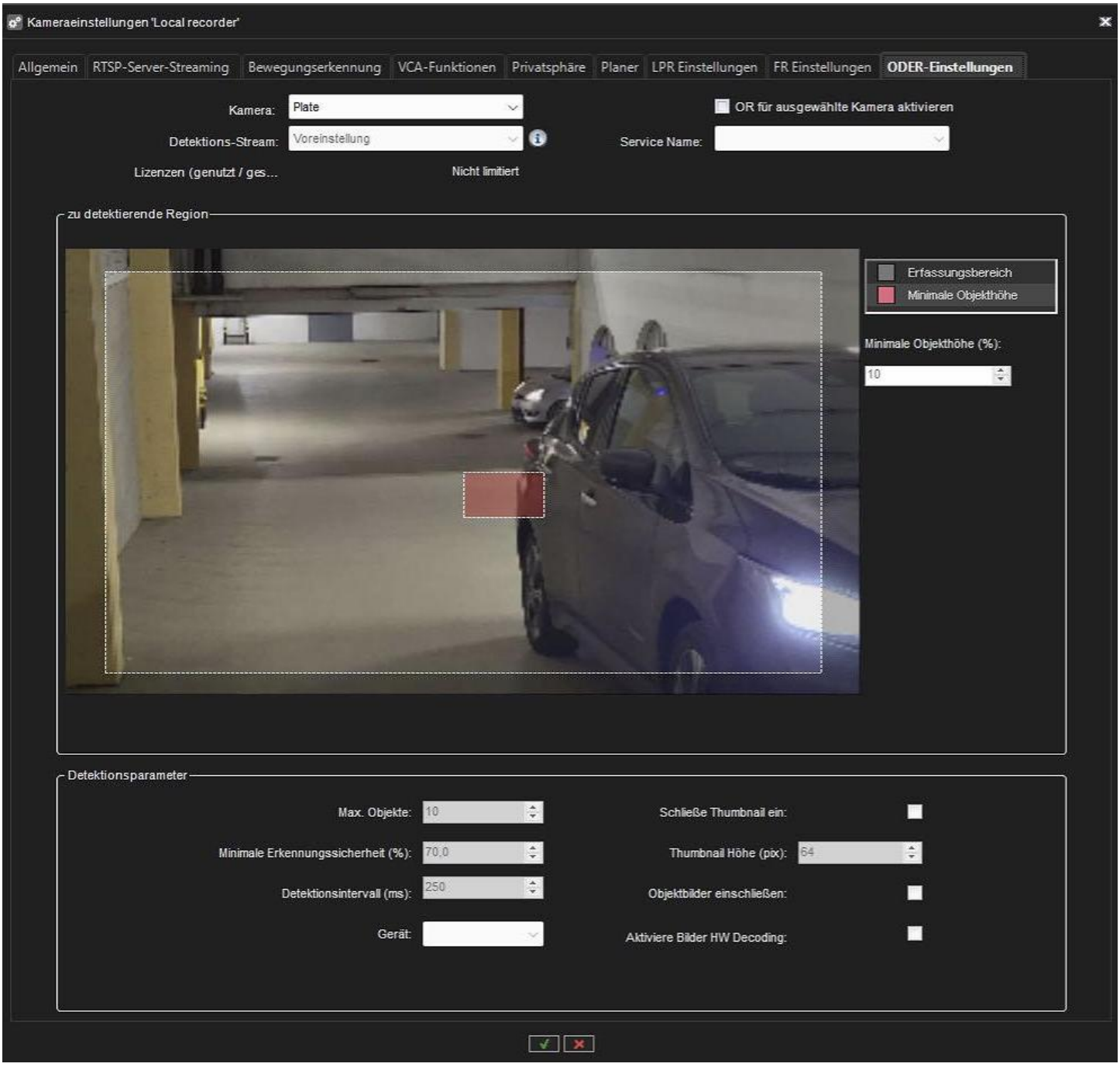
1. Wählen Sie die Kamera aus dem Dropdown-Menü in ODER
2. Wenn es mehr als einen Stream gibt, können Sie den Stream auswählen. Wenn nur ein Stream vorhanden ist, gibt es einen Standardstream wie in der Abbildung oben, und das Dropdown-Menü ist deaktiviert.
3. Sie können einen Dienst erst auswählen, nachdem Sie den Dienst durch Anklicken des Kästchens OR für ausgewählte Kamera aktivieren aktiviert haben.
4. Wenn das Kontrollkästchen OR für ausgewählte Kamera aktivieren nicht markiert ist, ist das Dropdown-Menü Dienst deaktiviert.
5. Das Textfeld Lizenz zeigt die Anzahl der verwendeten Lizenzen und die maximale Anzahl von Lizenzen an.

Wenn die Kamera den ODER-Dienst nicht unterstützt oder kein Dienst für sie aktiv ist, kann der Dienst nicht aktiviert werden.
Das gelbe Symbol zeigt dies an, und wenn der Benutzer den Mauszeiger darüber bewegt, erscheint ein Tooltip mit dem Text Für diese Kamera ist kein OR-Dienst aktiv.

10.7.8.1.2 Erfassungsbereich / Minimale Objektgröße

Ein Bild im Erkennungsbereich wird sofort hochgeladen, nachdem die aktuelle Kamera in der Kamera-Kombibox ausgewählt wurde. Die minimale Objektgröße kann auf zwei Arten angepasst werden:

- Anpassen des Prozentsatzes in Min. Objekthöhe (%)
- Stellen Sie ihn im Rahmen mit dem angezeigten Quadrat für Mindestobjektgröße ein. Das Quadrat hat die gleiche Farbe wie im Selektor rechts neben dem Rahmen.
- Die Mindestgröße kann nicht weniger als 10% betragen.



10.7.8.1.3 Erkennungsparameter

Max objects - maximale Anzahl der zu erkennenden Objekte im Bild. Der Wert sollte zwischen 1 und 100 liegen.

Minimale Erkennungssicherheit (%) - Vertrauensniveau des Erkenners. Liegt das Vertrauen in das erkannte Objekt unter diesem Schwellenwert, wird das Objekt ignoriert. Gültige Werte liegen zwischen 25% und 95%.

Detektionsintervall (ms) - die Anzahl der Millisekunden, die beschreibt, wie oft die Objekterkennung durchgeführt wird: wenn sie z. B. 250 ms beträgt, wird die Objekterkennung 4 Mal in einer Sekunde durchgeführt (auch wenn die Bildrate des Videostroms viel höher ist, z. B. 30 fps).

Gerät - wird für die Inferenz verwendet. Die verfügbaren Geräte hängen von der Hardware des aktuellen Dienstes ab.

Schließe Thumbnail ein - schließt das Thumbnail der Erkennungsquelle in die zurückgegebenen Daten ein oder nicht.

Thumbnail höhe (px) - die Höhe des Thumbnail-Bildes in Pixeln. NUR aktiviert, wenn das Kästchen Miniaturbild einschließen markiert ist. Der Wert sollte zwischen 32 und 128 Pixeln liegen.

Objektbilder einschließen - schließt Objektbilder in die zurückgegebenen Daten ein oder nicht.

Aktiviere Bilder HW-Dekodierung - aktivieren Sie die Dekodierung der eingegebenen Bilder mit der am besten geeigneten Computerplattform (CUDA, DXVA oder DirectX).

WARNUNG: Die Verwendung hoher Grenzwerte kann zu unbeabsichtigter Massenlöschung von Daten und einer erhöhten Systemauslastung führen. Es wird empfohlen, zunächst mit niedrigeren Grenzwerten zu beginnen und die Ergebnisse zu überprüfen, bevor umfangreichere Vorgänge ausgeführt werden.

Die Einstellungen für den Objektdatenspeicher finden Sie im System Manager unter **Systemeinstellungen** > **Einstellungen für den Objektdatenspeicher**.

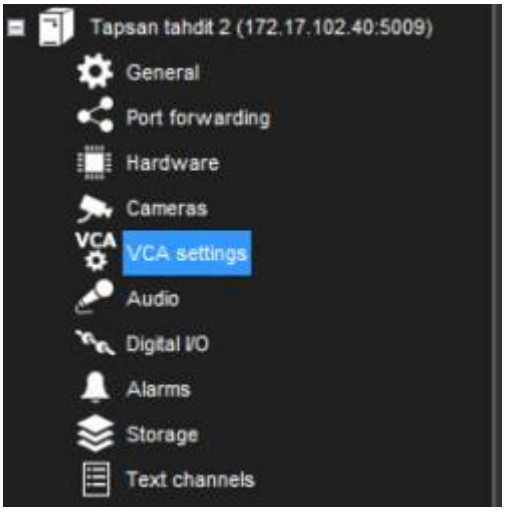
10.7.8.1.4 Empfohlene Konfiguration für OR-Einstellungen

Für OR werden die folgenden Streaming- und Erkennungseinstellungen empfohlen:

- Verwenden Sie CBR (Constant Bit Rate) für Streams – mit CBR erhält OR ein vollständiges Bild bzw. einen I-Frame, der nur die geänderten Bilder enthält. Dadurch funktioniert das System besser und liefert bessere Ergebnisse. Beachten Sie, dass es erforderlich sein kann, die Streaming-Bitrate zu begrenzen, um eine Beeinträchtigung der Netzwerkleistung zu vermeiden.
- Das Erkennungsintervall sollte vorzugsweise 2000 ms oder 1000 ms pro Kamera betragen, bei bis zu 10–15 Objekten.
- Die Höhe der Miniaturansichten sollte auf 64 px oder weniger eingestellt werden. Größere Werte können den Speicherplatz stark belasten.
- Beachten Sie bei der Festlegung der minimalen Objekthöhe, dass größere Werte für klare Bilder am besten geeignet sind.

Die Verwendung der empfohlenen Einstellungen trägt zur Optimierung der OR-Leistung bei. Beispielsweise können die Festplatten- und GPU-Auslastung deutlich gesenkt werden, wenn OR korrekt konfiguriert ist.

10.8 VCA-Einstellungen



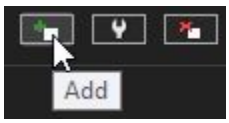
10.9 Audio

10.9.1 Hinzufügen, Bearbeiten und Entfernen von Audiogeräten

Das System unterstützt drei grundlegende Arten von Audiokomponenten: unidirektionale analoge und IP-Audiokanäle, bidirektionale IP-Audiokanäle und einen einzelnen Audiokommunikationskanal.

10.9.1.1 So konfigurieren Sie Audiogeräte:

1. Öffnen Sie die **VMS-Server** tab.
2. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Hardware** aus dem Menü.
3. Öffnen Sie die Registerkarte **Audio**.
4. Wählen Sie die **Hinzufügen**-Option



5. Wählen Sie den Capture-Treiber aus der Liste aus.
6. Wählen Sie eine dieser Optionen:

1. **Mono** Wählen Sie diese Option, um zwei Monokanäle zu verwenden.

2. **Stereo** Wählen Sie diese Option, um zwei Monokanäle zu einem Stereokanal zu kombinieren.

1. Klicken Sie auf **OK**.

Notiz *IP-kamerabasierte IP-Audioeingangs- und -ausgangskanäle werden dem System hauptsächlich über die automatischen Kamerasuchtools hinzugefügt.Falls ein IP-kamerabasierter Audiokanal nicht über die Kamerasuchtools hinzugefügt werden kann oder wenn der Kanal verspätet hinzugefügt wird, folgen Sie den Anweisungen Befolgen Sie die Anweisungen oben, um den Audiokanal hinzuzufügen.*

10.9.1.2 So bearbeiten Sie ein Audiogerät:

1. Öffnen Sie die **VMS-Server** tab.
2. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Hardware** aus dem Menü.
3. Öffnen Sie die Registerkarte **Audio**.
4. Wählen Sie den Audiokanal aus.
5. Click **Edit Audio Channel**



in the lower right corner of the tab. Das Dialogfeld**Audio konfigurieren** wird angezeigt.

6. Bearbeiten Sie die Informationsfelder.
7. Klicken Sie auf **OK**.

10.9.1.3 So entfernen Sie ein Audiogerät:

1. Öffnen Sie die **VMS-Server** tab.
2. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Hardware** aus dem Menü.
3. Öffnen Sie die Registerkarte **Audio**.
4. Wählen Sie den Audiokanal aus.
5. Klicken Sie auf **Letzten Audiokanal aus der Liste entfernen**



in der unteren rechten Ecke der Registerkarte.
Hinweis: *Sie können ein Audiogerät nicht aus der Mitte der Liste entfernen; nur das zuletzt hinzugefügte Audiogerät kann entfernt werden.*

6. Das letzte Audiogerät in der Liste wird vom Server entfernt.

10.9.2 Audio Einstellungen

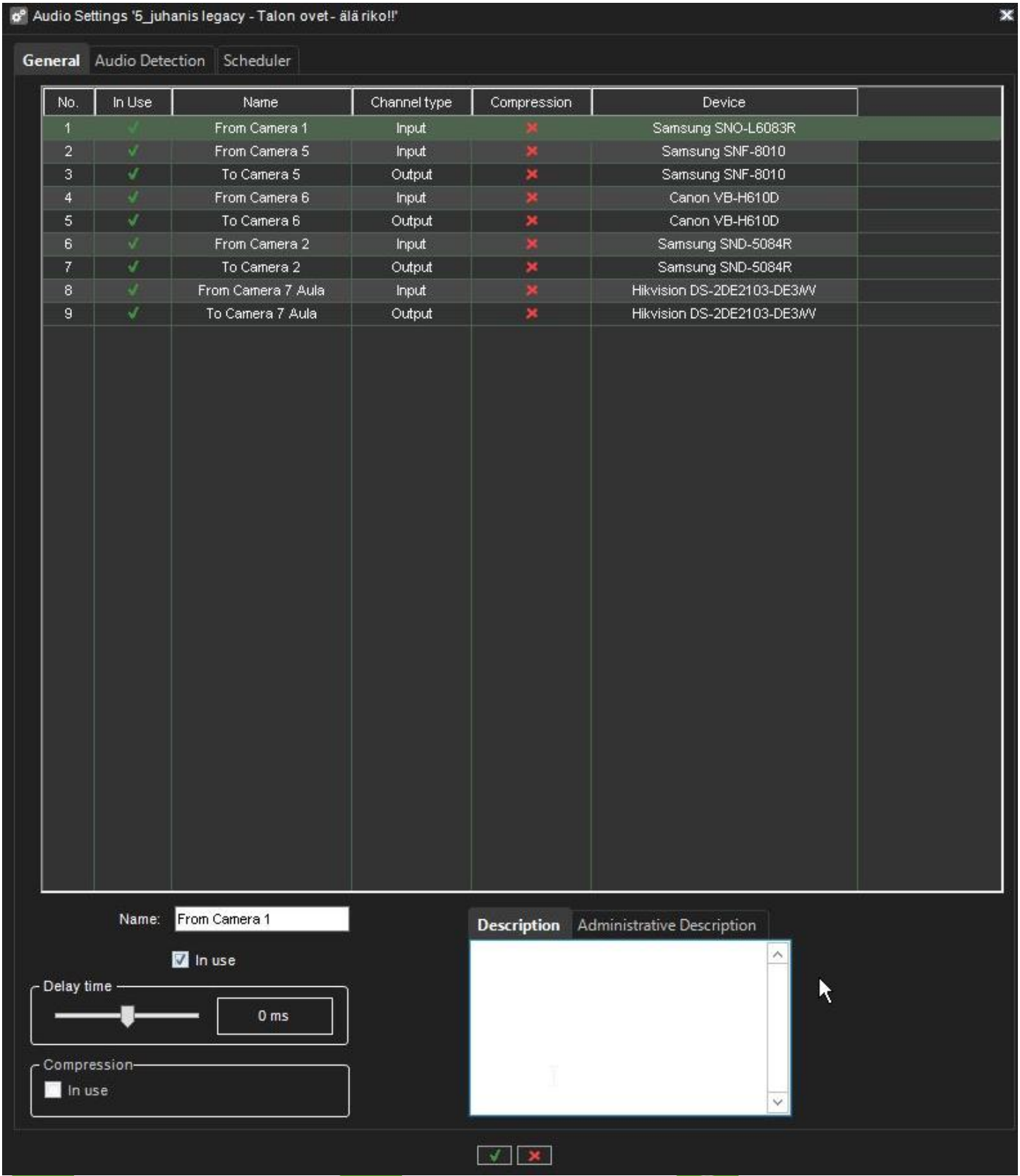
Das System unterstützt drei grundlegende Arten von Audiokomponenten:

- **Einweg-Analog- und IP-Audiokanäle:** Dazu gehören hauptsächlich kamerabasierte und separate Mikrofone.
- **Zwei-Wege-IP-Audiokanäle:** Zwei-Wege-IP-Audiokanäle erfordern eine IP-Kamera mit einem Audioeingangs- und -ausgangskanal.
    - Zweiwege-IP-Audiokanäle werden für die Kommunikation zwischen dem Kamerastandort und einem Spotter-Client verwendet.
    - Es kann immer nur ein Spotter-Client für die Kommunikation verwendet werden, aber andere Clients im System können den Kanal abhören und bei Bedarf die Kommunikation übernehmen.
    - Die gesamte Kommunikation, die über einen Zweiwege-IP-Audiokanal läuft, wird im System aufgezeichnet.
- **Ein einzelner Audiokommunikationskanal:** Ein älteres Kommunikationsmodell. Jedes System enthält einen Kommunikationskanal.
    - Der Nachteil bei der Verwendung des Audiokommunikationskanals besteht darin, dass das Signal den Server umgeht, was bedeutet, dass die Kommunikation nicht im System aufgezeichnet wird.

10.9.3 Allgemeine Einstellungen (Audio)



MIRASYS



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

Die Registerkarte **Allgemein** auf der Seite **Audio** listet die Grundeinstellungen aller Audiokanäle auf:

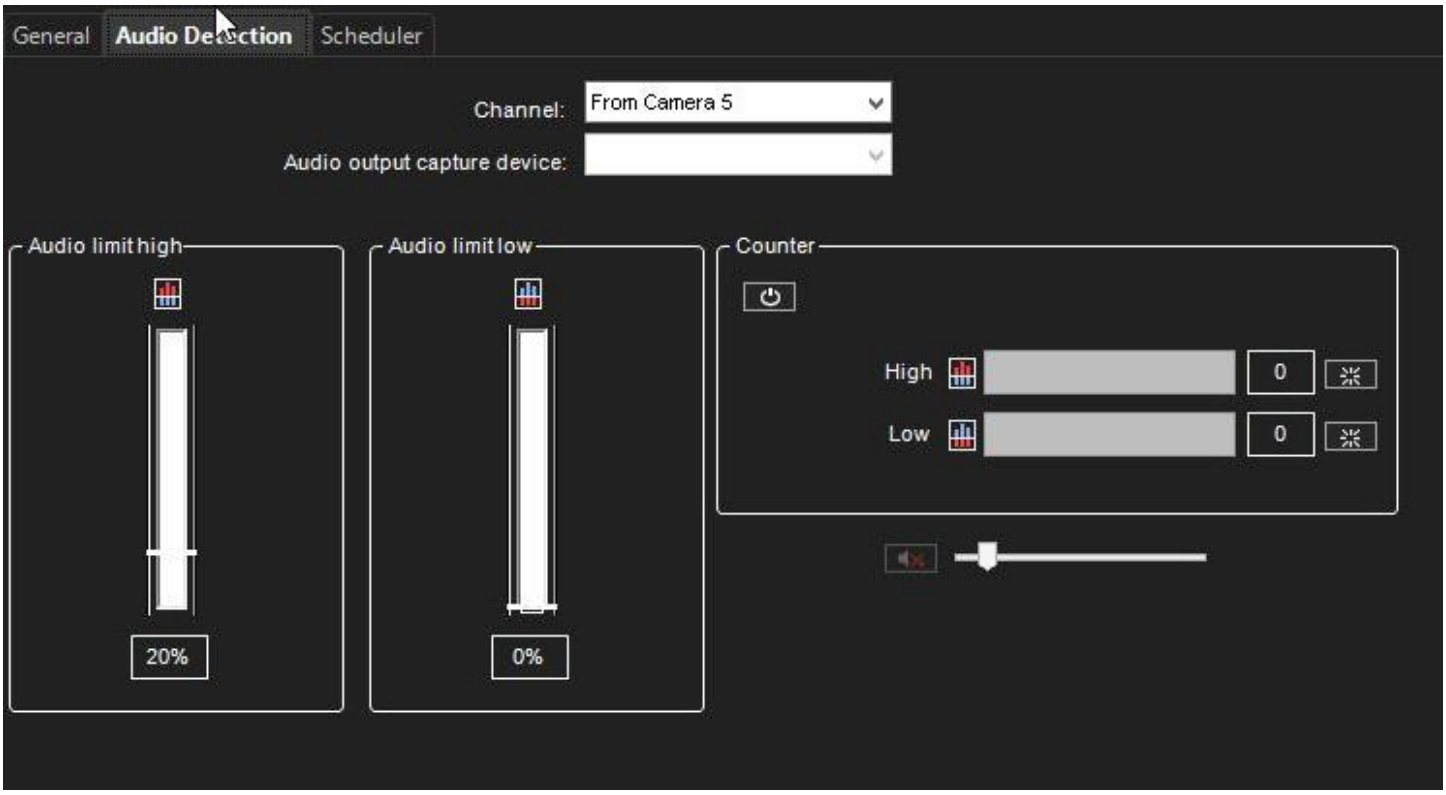
- **Nein** Die Nummer des Kanals.
- **In Benutzung** Zeigt an, ob ein Kanal aktiviert oder deaktiviert ist.
- **Name** Der Name des Kanals.
- **Mono / Stereo**. Zeigt an, ob ein Kanal ein Mono- oder Stereokanal ist.
- **Kompression** Zeigt an, ob die Komprimierung ein- oder ausgeschaltet ist. Ein Häkchen bedeutet, dass Komprimierung verwendet wird.
- **Capture-Treiber**. Zeigt an, welcher Capture-Treiber verwendet wird. Wählen Sie den Treiber in **Hardware-Einstellungen**.

Allgemeine Einstellungen ändern:

1. Wählen Sie den Kanal aus der Liste aus.
2. Im unteren Teil des Fensters können Sie diese Einstellungen ändern:

1. **Name** Der Name des Kanals.
2. **Im Einsatz**. Wählen Sie , um den Kanal zu aktivieren. Deaktivieren Sie das Kontrollkästchen, um den Kanal zu deaktivieren.
3. **Verzögerungszeit**. Stellt die Verzögerungszeit beim Synchronisieren des Audiostreams mit anderen Geräten ein.
4. Die Verzögerungszeit kann verwendet werden, um die Audio- und Videostream-Synchronisation zu optimieren, um beispielsweise eine bessere Lippensynchronisation zu ermöglichen.
5. **Kompression** Wählen Sie diese Option, um die Komprimierung zu verwenden. Komprimierte Audiodateien benötigen weniger Speicherplatz, aber die Audioqualität ist etwas geringer. Deaktivieren Sie das Kontrollkästchen, um keine Komprimierung zu verwenden.
6. **Beschreibung** Hier können Sie eine Beschreibung des Kanals eingeben, die den Benutzern im Spotter-Programm angezeigt wird.
7. **Administrative Beschreibung**. Hier können Sie eine Beschreibung des Kanals eingeben, die im Spotter-Programm nur Systemadministratoren angezeigt wird.

10.9.4 Audioerkennung



Legen Sie auf der Registerkarte **Audioerkennung** auf der Seite **Audio** die oberen und unteren Grenzwerte für die Audioerkennung fest.
Das System zeichnet Audio auf, wenn der Audiopegel den oberen Grenzwert überschreitet.
Zusätzlich können Sie das System so einstellen, dass es einen Alarm ausgibt, wenn der Audiopegel überschritten wird die obere Grenze oder unterschreitet die untere Grenze.

So legen Sie die Grenzen fest:

1. Wählen Sie den Audiokanal aus der Liste aus.
2. Klicken Sie auf **Audiozähler ein-/ausschalten**.
    a. Das System zeigt den Audiopegel in den Anzeigen **Audio Limit High** und **Audio Limit Low** an, und die Zähler erhöhen sich jedes Mal, wenn die Audioerkennung aktiviert wird.
    b. Der obere Zähler erhöht sich, wenn der Audiopegel den oberen Grenzwert überschreitet. Der untere Zähler erhöht sich, wenn der Audiopegel unter die untere Grenze fällt.
3. Stellen Sie den oberen Grenzwert so ein, dass der Audiopegel unter normalen Bedingungen unter dem Grenzwert bleibt.
    a. Die Audioerkennung wird aktiviert, wenn der Pegel den Grenzwert überschreitet.

4. Stellen Sie den unteren Grenzwert so ein, dass der Audiopegel unter normalen Bedingungen über dem Grenzwert bleibt.
    a. Die Audioerkennung wird aktiviert, wenn der Pegel unter den Grenzwert fällt.
5. Um die Zähler zurückzusetzen, klicken Sie auf die Reset-Schaltflächen.
6. Schalten Sie die Zähler aus, indem Sie auf die Schaltfläche **Audiozähler ein-/ausschalten** klicken.
7. Um die Einstellungen zu speichern, klicken Sie auf **OK**.

Sie können die Lautstärke des Audios einstellen und auch den Audiokanal stumm schalten.

Diese Einstellungen werden nicht gespeichert; sie ändern nur die Audiowiedergabe in den Audioeinstellungen.

- **Stumm** Schaltet den Audiokanal stumm.
- **Lautstärke anpassen**. Passt die Audiolautstärke an.

10.9.5 Planer (Audio)

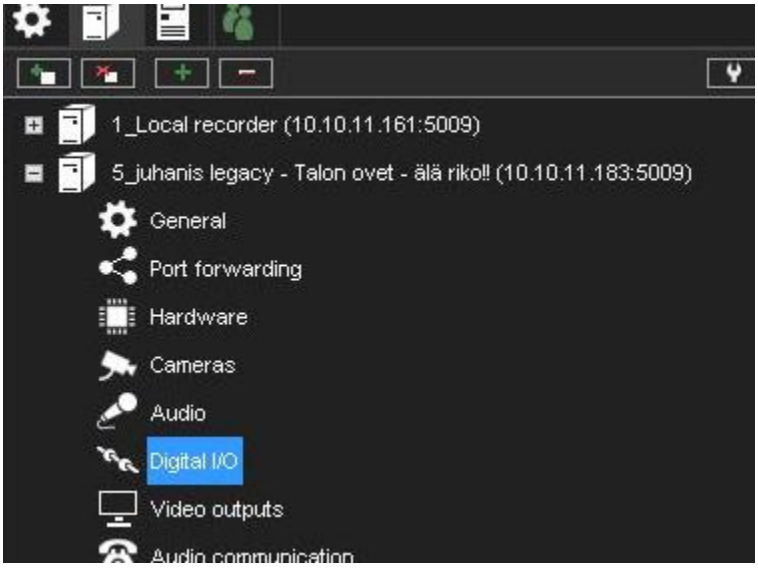
Standardmäßig wird Audio aufgezeichnet, wenn der erkannte Audiopegel die Standarderkennungsgrenze (**Audio limit high**) überschreitet.

Ähnlich wie beim Videoplaner ist es möglich, die Audioaufzeichnung mit den folgenden Optionen sowohl für reguläre Wochen als auch für Feiertage zu steuern.

1. **aus** Audio wird nicht aufgezeichnet. Mögliche Alarme werden jedoch aufgezeichnet.
2. **Kontinuierlich** Alle Audiodaten werden aufgezeichnet.
3. **Audioerkennung.** Audio wird aufgezeichnet, wenn der gemessene Audiopegel den Grenzwert überschreitet **Der Audiopegel ist hoch.**
    a. Legen Sie den Grenzwert in den Audioeinstellungen fest

Die Funktionalität dieser Ansicht ähnelt der des Video-Schedulers.

10.10 DIGITALE E/A

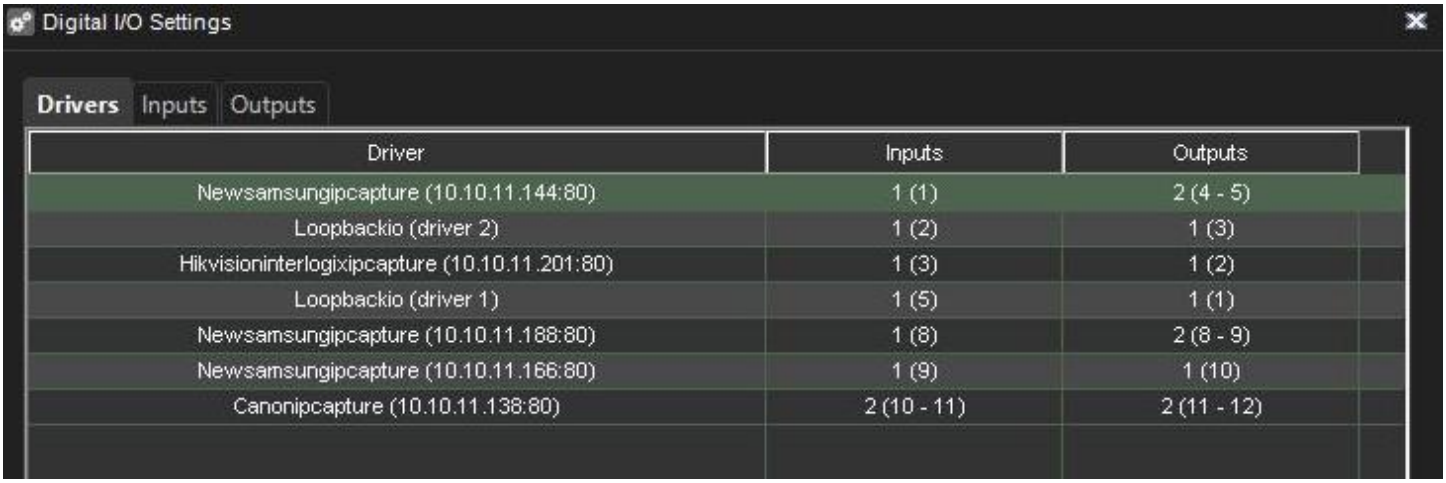


10.10.1 Digitale E/A-Einstellungen

In **Digitale E/A**-Einstellungen können Sie digitale Eingabe- und Ausgabegeräte hinzufügen und die Eingabe- und Ausgabeeinstellungen konfigurieren.
In diesen Abschnitten wird beschrieben, wie digitale E/A-Geräte eingerichtet werden.

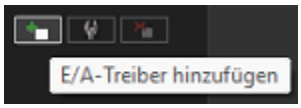
10.10.1.1 Treiber

Zusätzlich zu den im System enthaltenen standardmäßigen digitalen E/A-Treibern können dem System neue Treiber hinzugefügt werden, indem sie als Plugins installiert werden.
Sobald ein E/A-Gerätetreiber zum System hinzugefügt wurde, kann das Gerät konfiguriert und über die Registerkarte **Treiber** verwendet werden.



So verwenden Sie einen E/A-Gerätetreiber:

1. Installieren Sie bei Bedarf das Gerätetreiberpaket.
2. Öffnen Sie die **VMS-Server** tab.
3. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Digital I/O** aus dem Menü.
4. Klicken Sie in der unteren rechten Ecke des Bildschirms auf **E/A-Treiber hinzufügen**.



5. Wählen Sie den Treiber aus dem Dropdown-Menü **Model** aus.
6. Konfigurieren Sie die Geräteeinstellungen in der Liste **Eigenschaften**.
7. Um die Einstellungen zu speichern, klicken Sie auf **OK**.

Notiz *Nach der Konfiguration eines digitalen E/A-Gerätetreibers müssen Sie möglicherweise die Ein- und/oder Ausgänge konfigurieren.*

So bearbeiten Sie die Einstellungen des E/A-Gerätetreibers:

1. Öffnen Sie die **VMS-Server** tab.
2. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Digital I/O** aus dem Menü.
3. Doppelklicken Sie auf den Gerätetreiber, den Sie bearbeiten möchten.
4. Bearbeiten Sie die Geräteeinstellungen in der Liste **Eigenschaften**.
5. Um die Einstellungen zu speichern, klicken Sie auf **OK**.

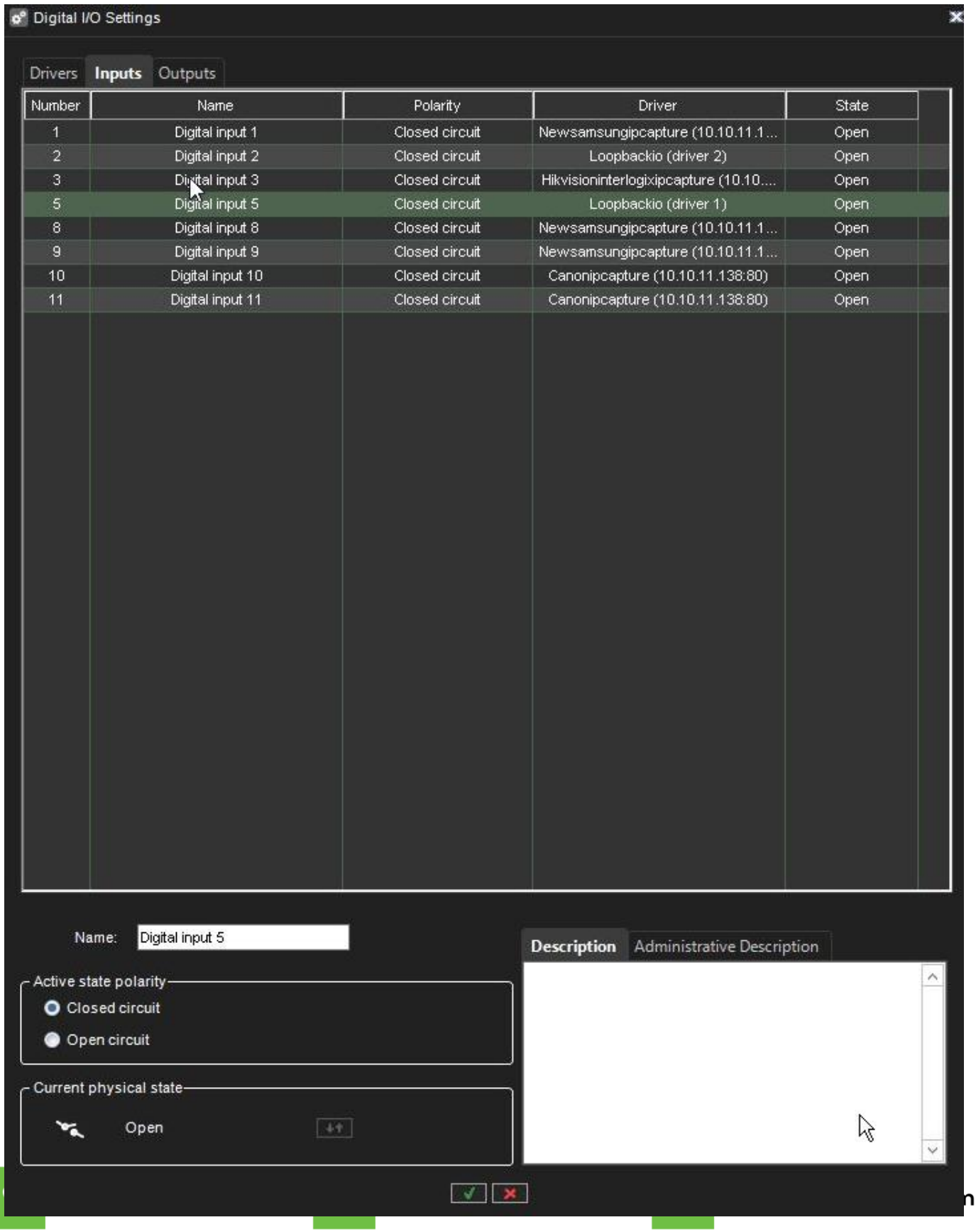
So löschen Sie einen E/A-Gerätetreiber:

1. Öffnen Sie die **VMS-Server** tab.
2. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Digital I/O** aus dem Menü.
3. Klicken Sie auf den E/A-Gerätetreiber, den Sie löschen möchten.
4. Klicken Sie auf **E/A-Treiber löschen** in der unteren rechten Ecke des Bildschirms.
5. Klicken Sie auf **Ok**, um das Löschen zu bestätigen.

10.10.1.2 Digitale Eingänge

Sie können digitale Eingänge verwenden, um Alarme zu aktivieren.
Legen Sie in den digitalen Eingangseinstellungen die Polarität der Eingänge fest. Legen Sie die Alarmaktionen in den Alarmeinstellungen fest.

MIRASYS


Digital I/O Settings
Drivers
Inputs
Outputs
Number
Name
Polarity
Driver
State
1
Digital input 1
Closed circuit
Newsamsungipcapture (10.10.11.1...
Open
2
Digital input 2
Closed circuit
Loopbackio (driver 2)
Open
3
Digital input 3
Closed circuit
Hikvisioninterlogixipcapture (10.10....
Open
5
Digital input 5
Closed circuit
Loopbackio (driver 1)
Open
8
Digital input 8
Closed circuit
Newsamsungipcapture (10.10.11.1...
Open
9
Digital input 9
Closed circuit
Newsamsungipcapture (10.10.11.1...
Open
10
Digital input 10
Closed circuit
Canonipcapture (10.10.11.138:80)
Open
11
Digital input 11
Closed circuit
Canonipcapture (10.10.11.138:80)
Open
Name:
Digital input 5
Description
Administrative Description
Active state polarity
Closed circuit
Open circuit
Current physical state
Open

Name Um einen Eingang umzubenennen, wählen Sie den Eingang aus und geben Sie dann einen neuen Namen für den Eingang in **Name.Polarität des aktiven Zustands ein.** Wählen Sie den Eingang und dann aus, ob der Eingang aktiviert wird, wenn der Stromkreis geöffnet oder geschlossen wird.
Aktueller physikalischer Zustand. Zeigt den Status eines Relais in Echtzeit an (**Open** oder **Closed**).
Beschreibung Hier können Sie eine Beschreibung der ausgewählten Eingabe eingeben, die allen Benutzern im Spotter-Programm angezeigt wird.
Administrative Beschreibung. Hier können Sie eine Beschreibung der ausgewählten Eingabe eingeben, die im Spotter-Programm nur für Systemadministratoren angezeigt wird.

10.10.1.3 Digitale Ausgänge

Wählen Sie bei digitalen Ausgängen, ob ein Relais geöffnet oder geschlossen ist (Polarität), wenn der Ausgang ausgelöst wird.

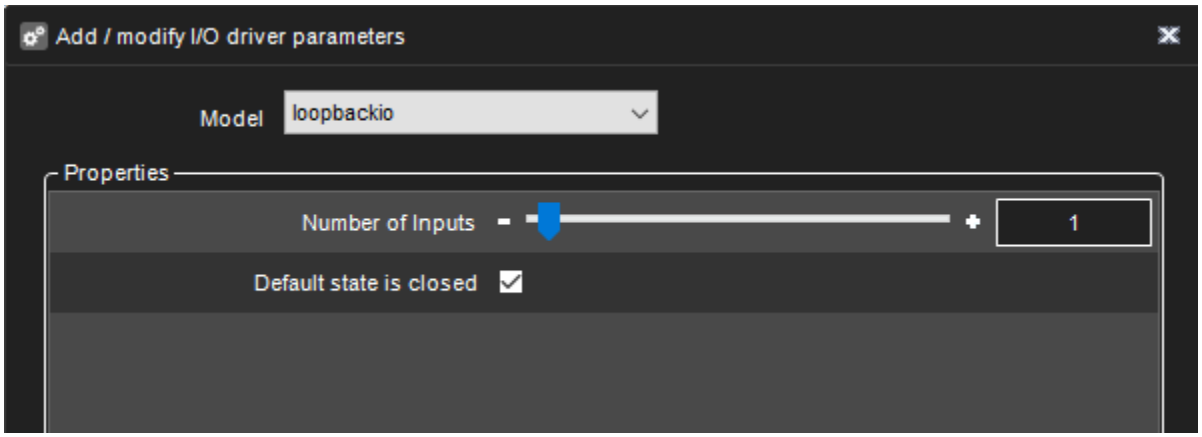
Name Um einen Ausgang umzubenennen, wählen Sie den Ausgang aus und geben Sie dann einen neuen Namen für den Ausgang in **Name**.
Polarität des aktiven Zustands ein. Wählen Sie den Ausgang und wählen Sie dann, ob der Ausgang geschlossen oder geöffnet ist, wenn er aktiviert wird.
Aktueller physikalischer Zustand. Zeigt den Status eines Relais in Echtzeit an (**Open** oder **Closed**).
Beschreibung Hier können Sie eine Beschreibung der ausgewählten Ausgabe eingeben, die allen Benutzern im Spotter-Programm angezeigt wird.
Administrative Beschreibung. Hier können Sie eine Beschreibung der ausgewählten Ausgabe eingeben, die im Spotter-Programm nur für Systemadministratoren angezeigt wird.

Um einen Digitalausgang zu testen, klicken Sie auf die Schaltfläche **Change State (Toggle)**.

10.10.2 LoopBack-E/A

Mit dem LoopBack I/O können Sie virtuelle I/O-Geräte erstellen, bei denen der Eingang direkt mit dem Ausgang verbunden ist.

Mit diesem Treiber können Sie in der Spotter-Anwendung Schaltflächen erstellen, um Alarme manuell auszulösen.



10.10.3 Logische E/A

Mit Logical I/O ist es möglich, Aktionen basierend auf den ODER- und UND-Operatoren zu erstellen.

Der I/O-Treiber emuliert einen externen I/O, der mit ihm selbst verbunden ist. Beispiel:

Wenn der Kunde beispielsweise bestätigen möchte, dass ein Ereignis der automatischen Nummernschilderkennung (ANPR) ausgelöst wird, wenn sich ein Auto vor der Kamera befindet, kann die logische I/O verwendet werden, um eine „Regel“ zu erstellen, die nur zu einer Aktion führt wenn VCA ein Auto erkennt UND gleichzeitig ein ANPR-Leseereignis stattfindet.

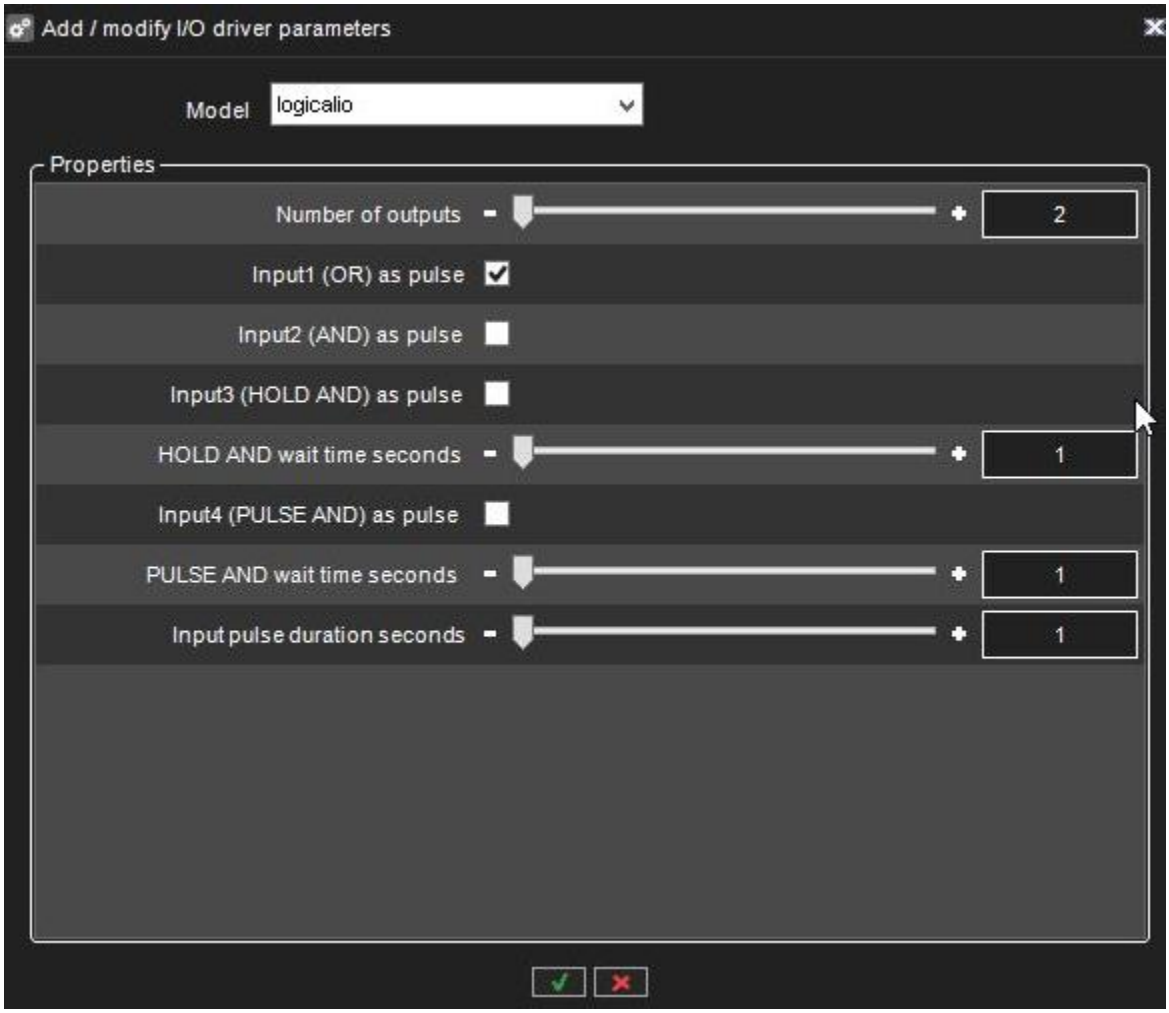
Ein anderes Beispiel könnte sein, dass ein Eingangs-„Tor“ mit zwei Türen das Öffnen der zweiten Tür nur zulässt, wenn die erste geschlossen ist.

Logische E/A können über dieselbe Schnittstelle wie der Rest der digitalen E/A im System Manager bedient werden.

Eine Lizenz steuert logische E/A und Countdown-E/A. Wenn die Lizenz nicht vorhanden ist, schlägt das Erstellen neuer E/A fehl.

Wenn ein neuer logischer E/A hinzugefügt wird, ist die erste Option im Dialog, wie viele Ausgangszustände als Operanden bei der UND/ODER-Entscheidung verwendet werden.

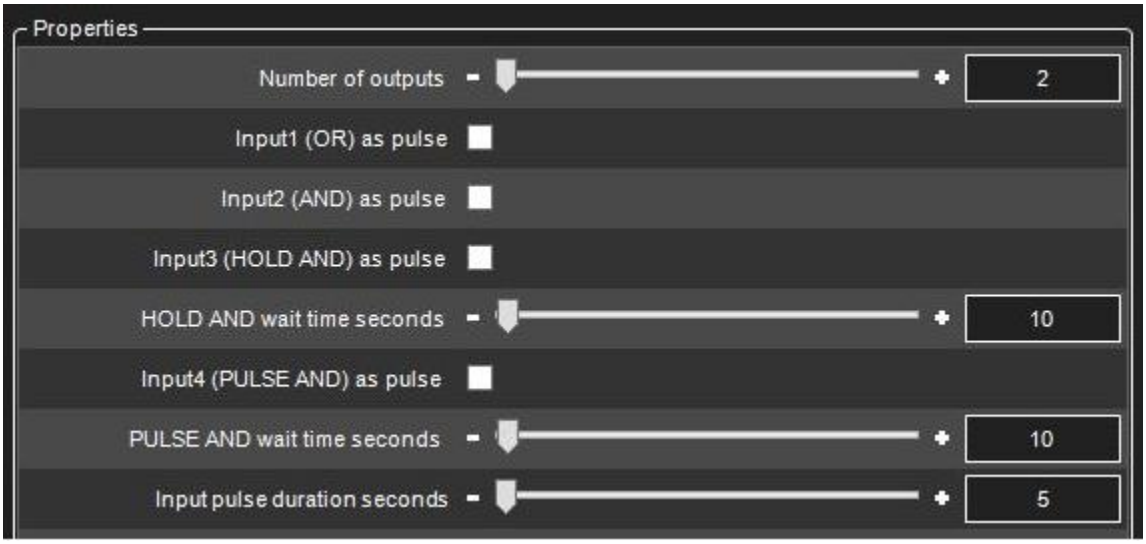
Die Mindestanzahl beträgt zwei, die Höchstzahl 32.



Alle logischen I/Os generieren automatisch vier Eingänge, die verwendet werden können.

Eingang	Typ
1	ODER
2	UND
3	HALTEN UND
4	IMPULS UND

In den folgenden Abschnitten werden die verschiedenen Eingänge anhand des folgenden Beispiels genauer beschrieben:

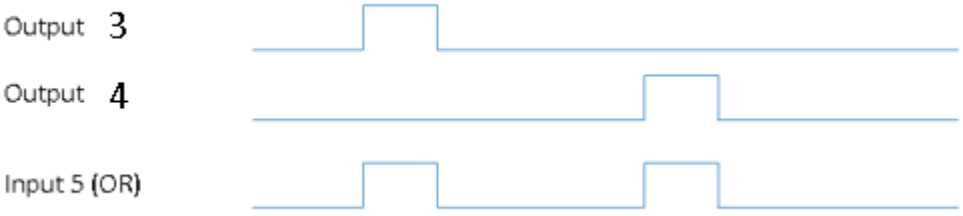


Das Beispiel hat 2 Ausgänge, die die Operanden sind. Diese sind in der IO-Liste als Ausgänge 3 und 4 zu sehen.

Die automatisch erstellten 4 Eingänge werden in der Liste als Eingänge 5, 6, 7 und 8 angezeigt.

10.10.3.1 „ODER"-Eingang

Der erste Eingang, den der logische E/A erzeugt, ist ein ODER-Signal. Wenn einer der Ausgänge eingeschaltet ist, wird der ODER-Eingang eingeschaltet.

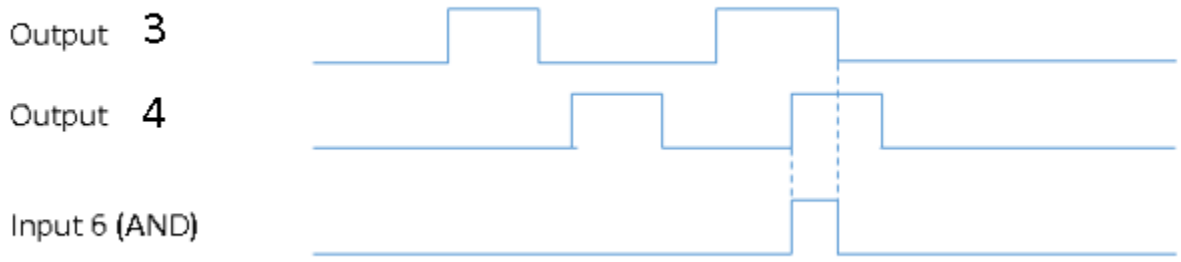


In unserem Beispiel ist Eingang 5 das ODER-Signal. Wenn entweder Ausgang 3 ODER Ausgang 4 eingeschaltet ist, wird als Ergebnis Eingang 5 eingeschaltet.

Der Eingang bleibt so lange eingeschaltet, wie einer der Ausgänge eingeschaltet bleibt. (Es sei denn, der Pulsmodus ist ausgewählt, siehe unten für Details)

10.10.3.2 „UND"-Eingang

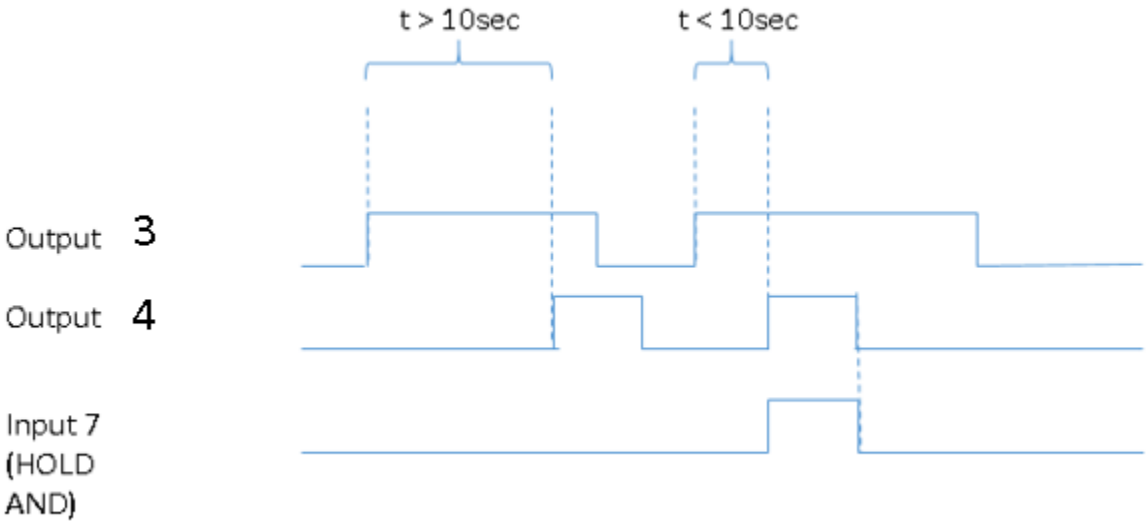
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.



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

10.10.3.3 "HOLD AND" Input

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



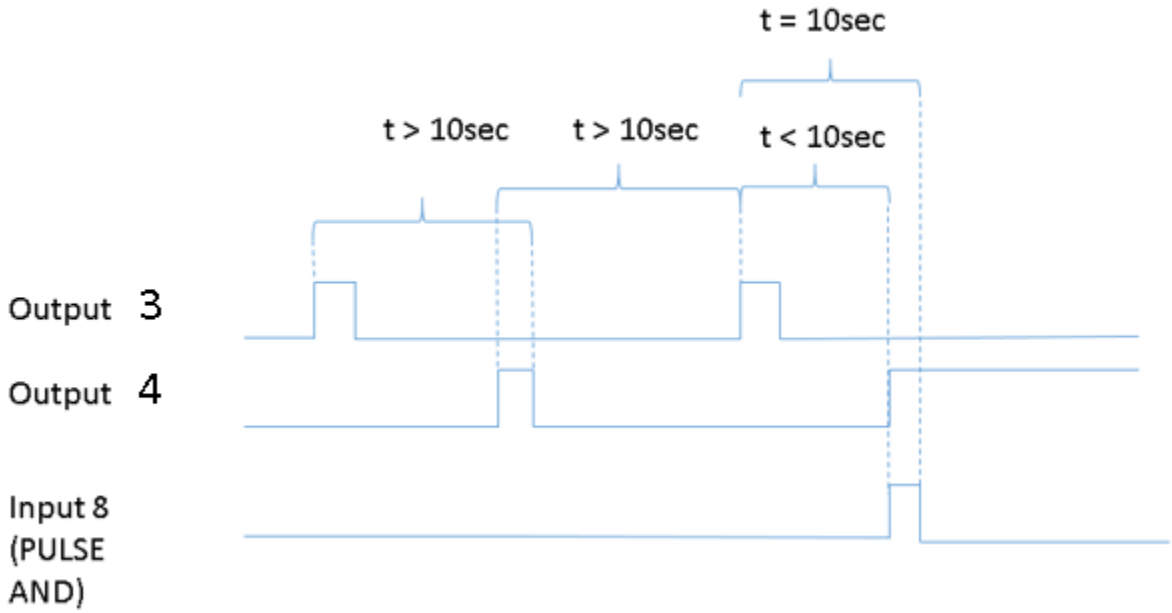
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

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

10.10.3.4 "PULSE AND" Input

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

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

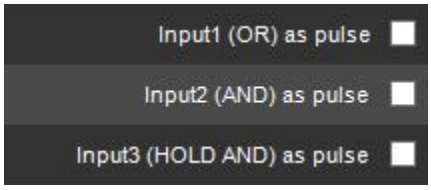


Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

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

10.10.3.5 Pulse Mode For Inputs

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



and



The pulse duration can also be adjusted.

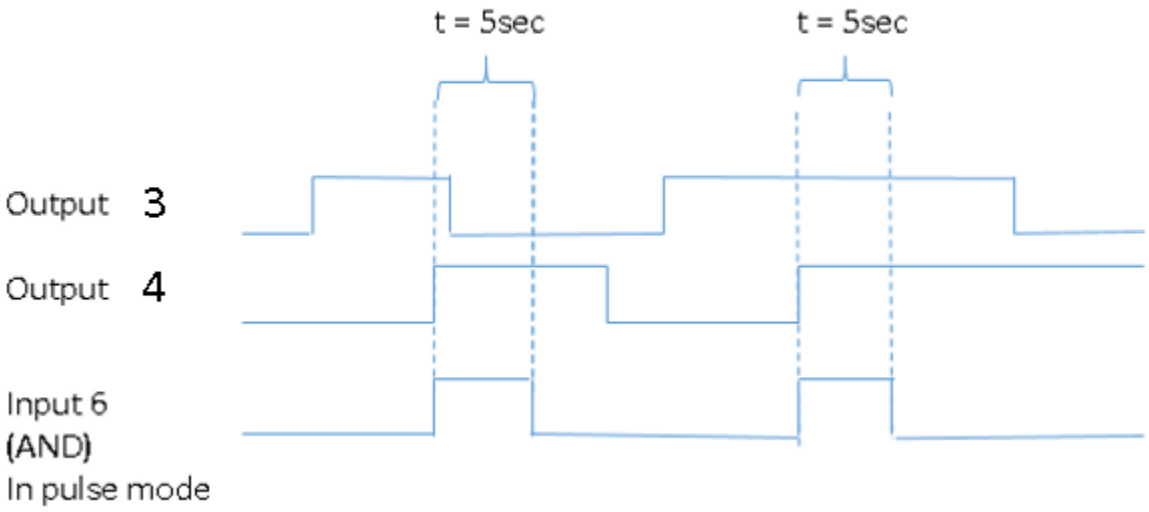


If the pulse mode is in use, the input will turn off after the set pulse duration.

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



It would mean behaviour like this:



10.10.4 Countdown-E/A

Mit Countdown I/O ist es möglich, Aktionen basierend darauf zu erstellen, ob einige Ereignisse in einem definierten Zeitraum eintreten oder nicht.

Wenn im System Manager ein neuer Countdown-E/A erstellt wird, erstellt dieser automatisch 4 Eingänge und 4 Ausgänge.

Countdown I/O hat zwei grundlegende Modi. Die ersten beiden Ein-/Ausgangspaare sind vom Typ 1, die letzten beiden Paare vom Typ 2.

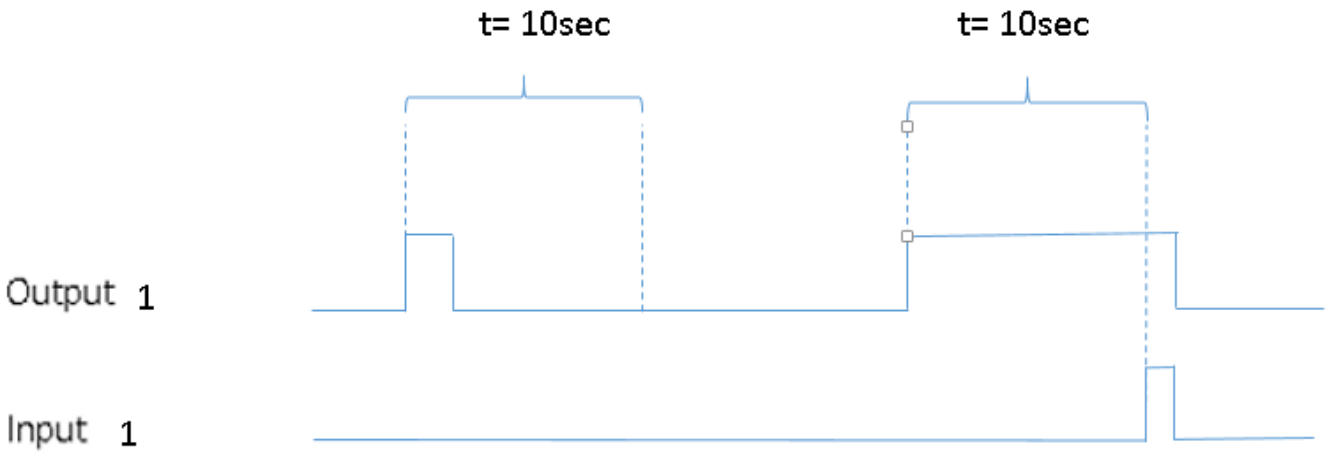
Eine Lizenz steuert logische E/A und Countdown-E/A. Wenn die Lizenz nicht vorhanden ist, schlägt das Erstellen neuer E/A fehl.

10.10.4.1 Ereignisdauer überschritten Modus (Typ 1)

Erstens ist es möglich, einen Alarm auszulösen, wenn ein Ereignis länger dauert als die geplante Dauer.

Nehmen wir zum Beispiel an, die Zeit beträgt 10 Sekunden. Wird Ausgang eins ausgelöst und bleibt kürzer als die definierte Dauer aktiv, erfolgt kein Alarm.

Wird der Ausgang ausgelöst und bleibt länger als die definierte Dauer aktiv, erfolgt ein Alarm.



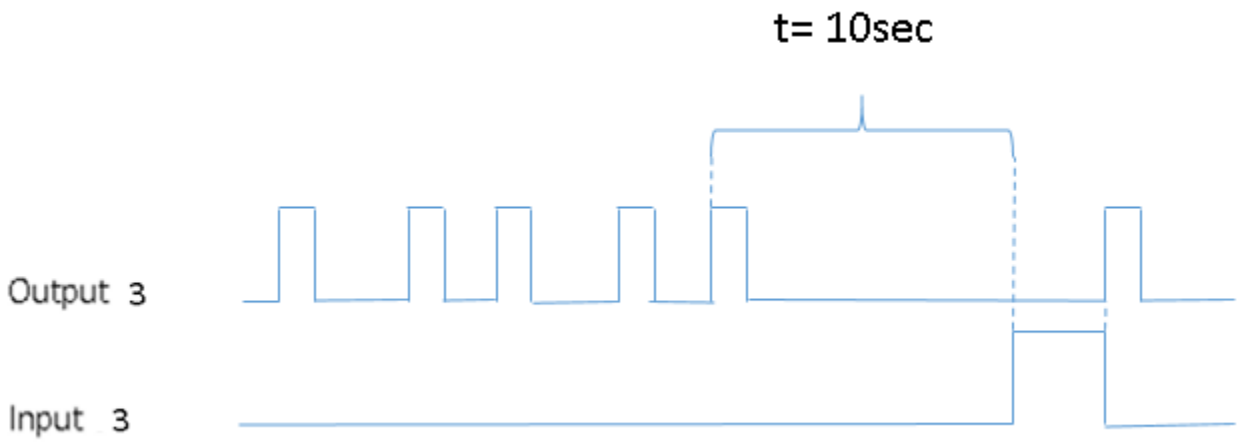
Beim Erstellen eines neuen Countdown-E/A sind die ersten beiden Eingangs-Ausgangspaare von diesem Typ.

10.10.4.2 Erwarteter Triggermodus (Typ 2)

Zweitens ist es möglich, einen Alarm auszulösen, wenn ein erwarteter Impuls nicht innerhalb der definierten Zeit empfangen wird.

Zum Beispiel beträgt die Zeit 10 Sekunden, und wir erwarten, dass der normale Betrieb alle 2-3 Sekunden Impulse von Ausgang 3 erhält.

Wenn der Impuls länger als 10 Sekunden fehlt, wird der Eingangszustand auf aktiv geändert. Es bleibt aktiv, bis der nächste Ausgangstrigger empfangen wird.



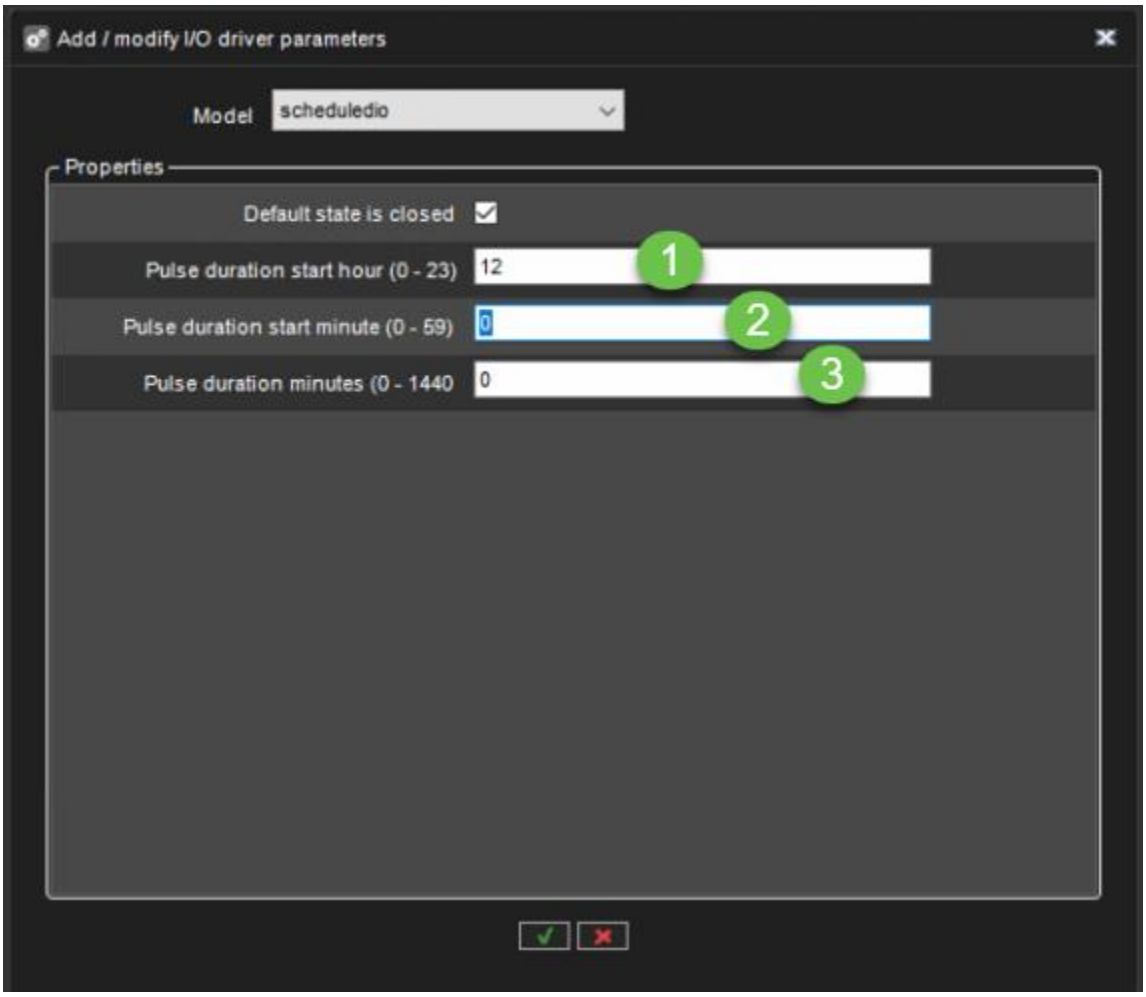
Beim Erstellen eines neuen Countdown-E/A ist das letzte Eingangs-Ausgangs-Paar von diesem Typ.

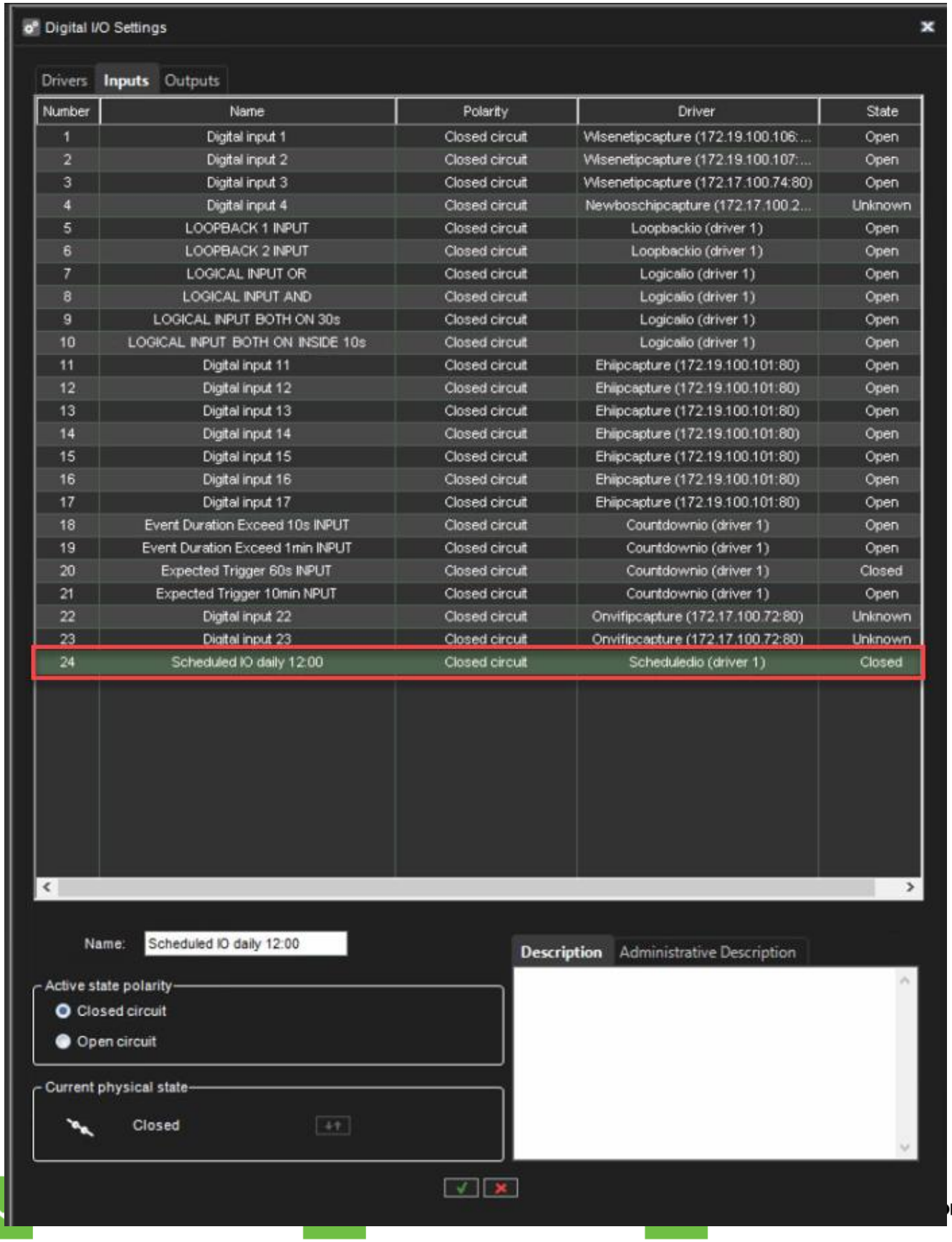
10.10.5 Geplante E/A

10.10.5.1 Mit Scheduled IO ist es möglich, einen Zeitplan für jeden digitalen Ausgang zu erstellen, der mit dem VMS-Server verbunden ist.

10.10.5.2 Es können nur die gleichen digitalen Ausgänge des VMS-Servers geplant werden.

1. Stellen Sie die Pulsdauer ein, beginnen Sie eine Stunde
2. Startminute der Pulsdauer einstellen
3. Stellen Sie die Pulsdauer in Minuten ein




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

10.10.6 Eigenschaften

HTTP-Methode (geöffnet)

- GET
- PUT
- POST
- DELETE

URL(geöffnet)

Inhalt (geöffnet)

User(Opened)

Password(Opened)

HTTP Method(Closed)

- GET
- PUT
- POST
- DELETE

URL(Closed)

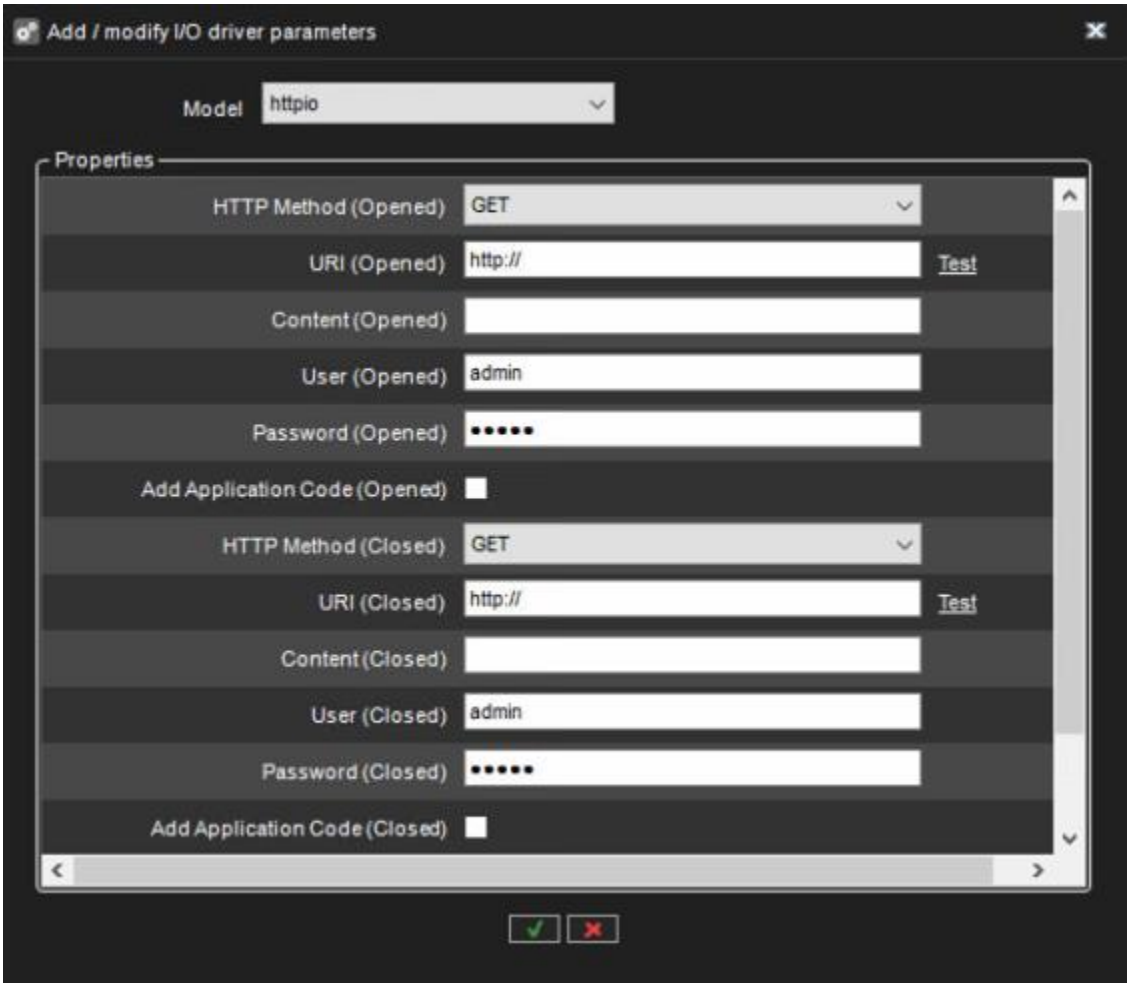
Content(Closed)

User(Closed)

Password(Closed)

Authentication

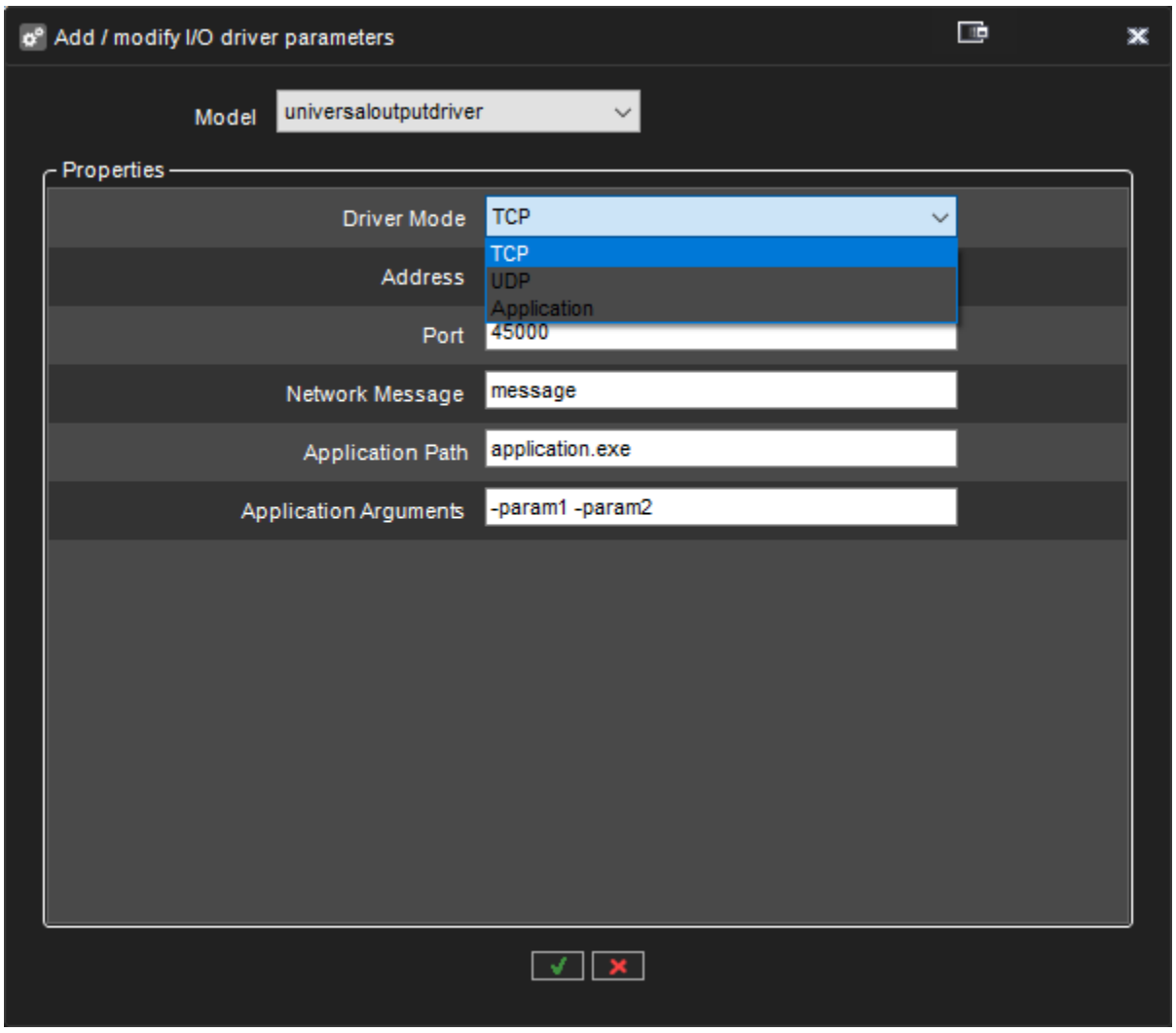
- BASIC
- DIGEST



10.10.7 UniversalOutputDriver

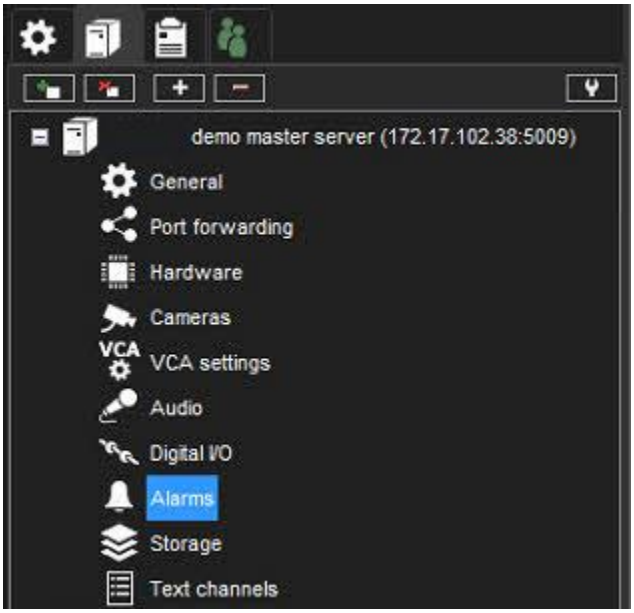
Mit diesem Treiber können Sie Daten an Drittsysteme senden oder Anwendungen auf dem Server oder entfernten Systemen starten.

Weitere Informationen zu diesem Treiber finden Sie in unserem Extranet oder wenden Sie sich an den Support.



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

10.11 Alarme (VMS-Servers)



10.11.1 Alarmeinstellungen

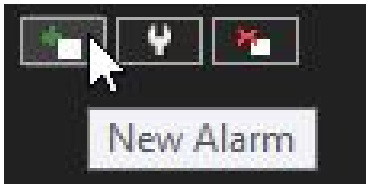
Die Alarmmanagement-Tools ermöglichen die Erstellung serverspezifischer Alarme basierend auf verschiedenen Auslösern basierend auf Bewegung, Schallpegel oder bestimmten Textdatenauslösern.

Darüber hinaus können die Trigger kundenspezifische Trigger von Drittanbietern beinhalten.

Alarme können über den Bildschirm **Alarme** auf der Registerkarte **VMS-Server** erstellt, bearbeitet und gelöscht werden.

10.11.1.1 Alarme hinzufügen, löschen, ändern und kopieren

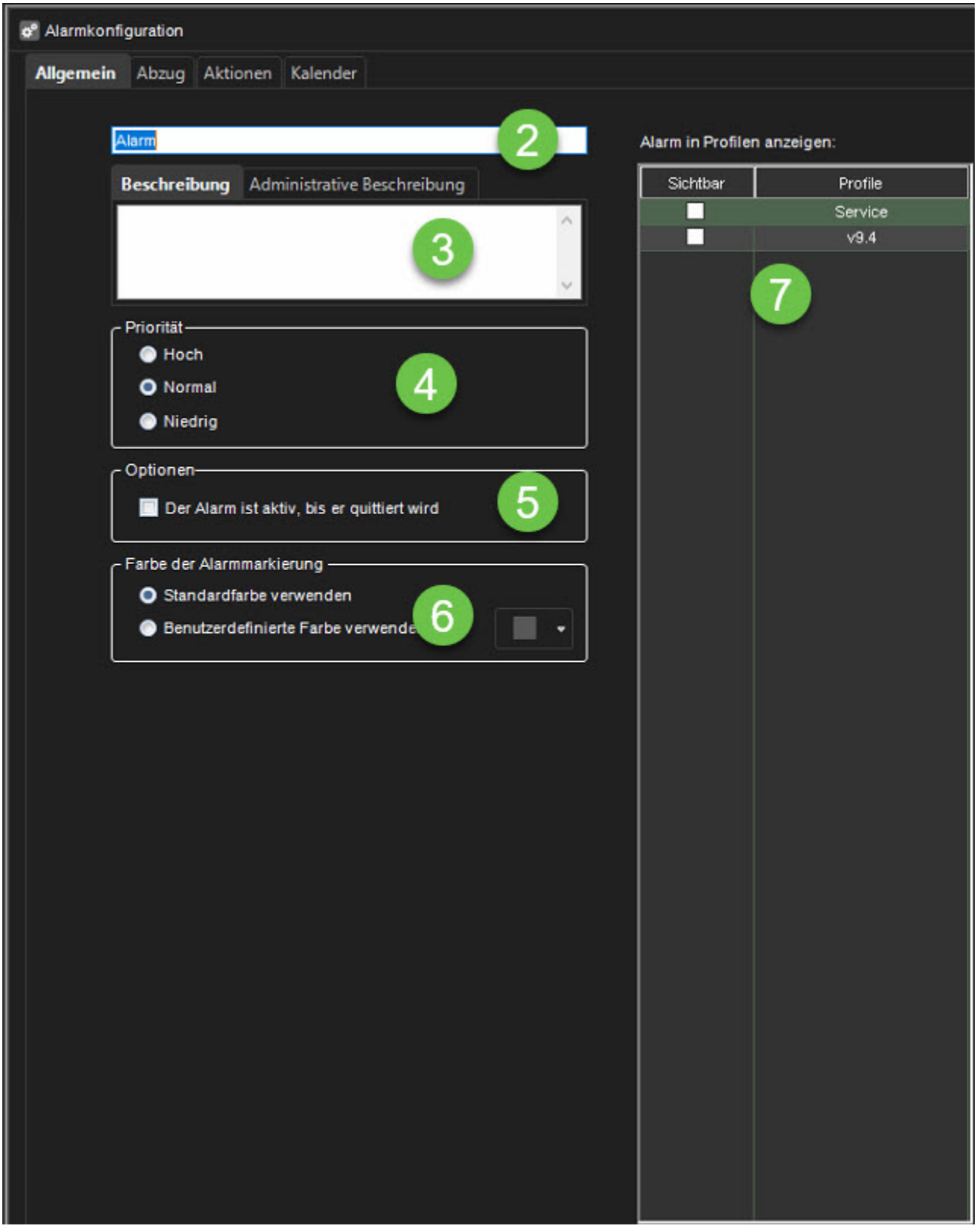
1. Klicken Sie auf **Neuer Alarm** in der linken unteren Ecke des Bildschirms Alarme.



1. Geben Sie den Namen des neuen Alarms in das Feld **Name** ein.
2. Geben Sie die **Beschreibung** und **Verwaltungsbeschreibung** des neuen Alarms in die entsprechenden Felder unter dem Feld **Name** ein.
3. Wählen Sie aus, ob der Alarm **hoch**, **durchschnittlich** oder **niedrig Priorität** hat. Die Priorität wird verwendet, um die Reihenfolge festzulegen, in der Alarme bei mehreren gleichzeitigen Alarmen ausgeführt werden.

4. Wählen Sie **Der Alarm ist aktiv, bis er bestätigt wird**, um den Alarm als kontinuierlich zu erstellen; Wenn die Option ausgewählt ist, wird der Alarm fortgesetzt, bis ein Benutzer ihn über die **Spotter**-Anwendung bestätigt.
5. **Alarm-Hervorhebungsfarbe** ermöglicht Administratoren, eine benutzerdefinierte Farbe für jeden Alarm separat zu definieren.
6. Wählen Sie im Menü **Alarme in Profilen anzeigen** die Profile aus, in denen der Alarm verwendet werden soll.

MIRASYS

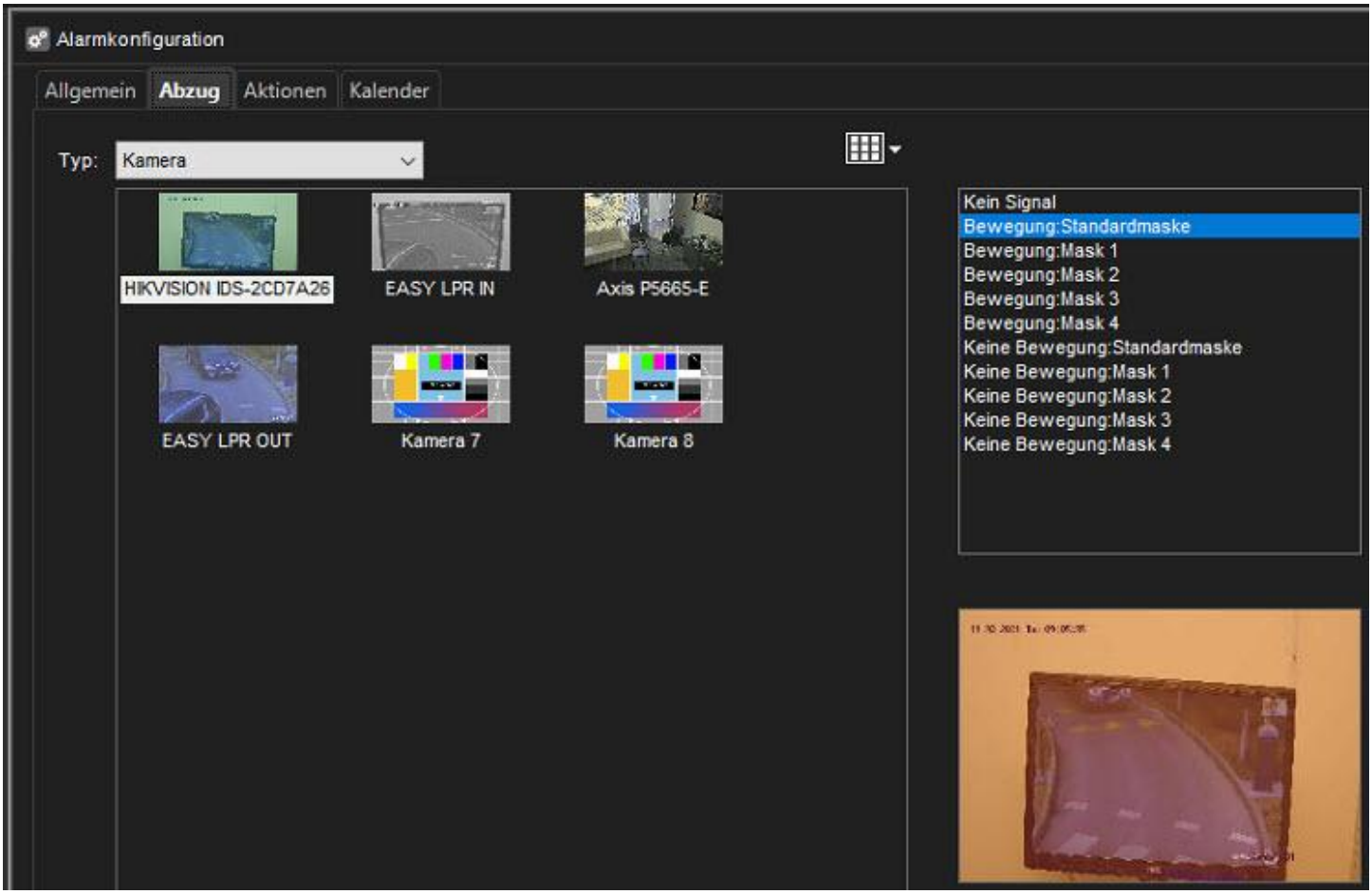


Tel +358 (0)9 2533 3300
Email info@mirasys.com
https://www.mirasys.com

Alarme können auch über die Registerkarte **Profile** zu Profilen hinzugefügt werden.

10.11.1.1.1Auswählen des Auslösers

1. Öffnen Sie die Registerkarte **Trigger**. Die Registerkarte **Trigger** wird verwendet, um die Trigger zu definieren, die das Alarmereignis starten.



1. Wählen Sie den Triggertyp aus dem Dropdown-Menü **Type** aus.

- Kamera
- Audio
- Metadaten
- Textdaten
- Digitale Eingabe

10. Wählen Sie das Gerät, das den Alarm auslösen soll, aus der Geräteliste unter dem Dropdown-Menü **Typ** aus.

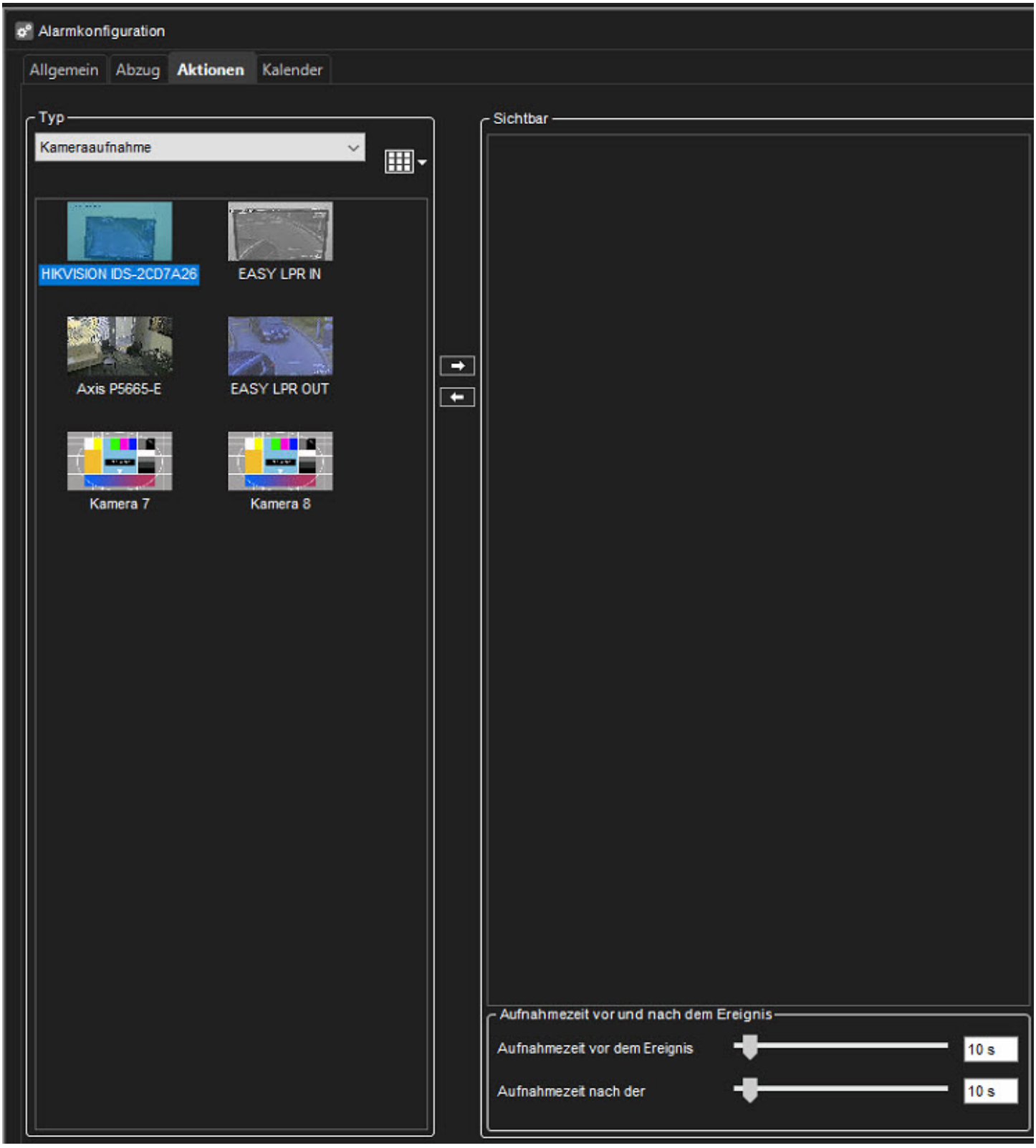
11. Wählen Sie die auslösende Bedingung aus der Bedingungsliste auf der rechten Seite des Bildschirms aus.

- Bei kamerabasierten Auslösern können Sie die Maske auswählen, die bei der Bewegungserkennung verwendet wird, um den Alarm auszulösen.
- Bei audiobasierten Auslösern können Sie den Alarm so einstellen, dass er basierend auf einem hohen oder niedrigen Audiopegel ausgelöst wird.
- Für textdatenbasierte (z. B. VCA, Metadaten usw.) Trigger können Sie den Alarm so einstellen, dass er basierend auf einer Textdatenzeichenfolge ausgelöst wird.
  Zusätzlich können Sie einen optionalen Alarmende-Trigger festlegen, indem Sie **Beendigungseingang definieren** markieren und eine Zeichenfolge auswählen zum Beenden des Alarms.
- Bei digitaleingangsbasierten Triggern wird der Alarm basierend auf der Polaritätsänderung des Eingangs ausgelöst.

10.11.1.1.2Aktionen

12. Öffnen Sie die Registerkarte **Aktionen**. Die Registerkarte **Aktionen** wird verwendet, um die Aktionen zu definieren, die der Alarm ausführt, wenn er ausgelöst wird.

MIRASYS



Tel +358 (0)9 2533 3300

Email info@mirasys.com

https://www.mirasys.com

13. Wählen Sie den Aktionstyp aus dem Dropdown-Menü **Typ** aus. Der Aktionstyp definiert die grundlegende Funktionalität des Alarms.

1. Legen Sie bei Bedarf auf der Registerkarte **Kalender** den Zeitplan für den Alarm fest.
2. Klicken Sie auf **OK**.
3. Klicken Sie in der Alarmliste auf **OK**, um die Änderungen zu speichern.

10.11.1.1.3Löschen eines Alarms

1. Wählen Sie auf der Registerkarte **VMS-Server** den Server aus
2. Doppelklicken Sie auf **Alarme**
3. Wählen Sie den Alarm aus, den Sie löschen möchten, indem Sie auf seinen Namen klicken
4. Klicken Sie auf **Alarm entfernen** in der linken unteren Ecke des Bildschirms **Alarme**



5. Klicken Sie in der Alarmlistenansicht auf **OK**, um die Änderungen zu speichern

10.11.1.1.4 Einen Alarm ändern

1. Gehen Sie zu den **Alarmen**
2. Wählen Sie den Alarm aus, den Sie bearbeiten möchten
3. Klicken Sie auf **Alarm bearbeiten**



4. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **OK**
5. Klicken Sie in der Alarmlistenansicht auf **OK**, um die Änderungen zu speichern

10.11.1.1.5Alarme kopieren und einfügen

Eine vorhandene Alarmkonfiguration kann kopiert und eingefügt werden, um einen neuen, ähnlichen Alarm zu erstellen. Der Benutzer muss lediglich den Namen, die Beschreibung und den Auslöser für die neue Kopie definieren, wodurch die Alarmkonfiguration schnell und effizient erfolgt.

1. Gehen Sie zu den **Alarmen**

2. Wählen Sie den zu kopierenden Alarm aus
3. Klicken Sie auf **Alarm kopieren**



1. Legen Sie den Namen, die Beschreibung und den Auslöser für den neuen Alarm fest
2. Klicken Sie auf **OK**
3. Klicken Sie in der Alarmlistenansicht auf **OK**, um die Änderungen zu speichern

10.11.1.2 Aktionstypen und Einstellungen

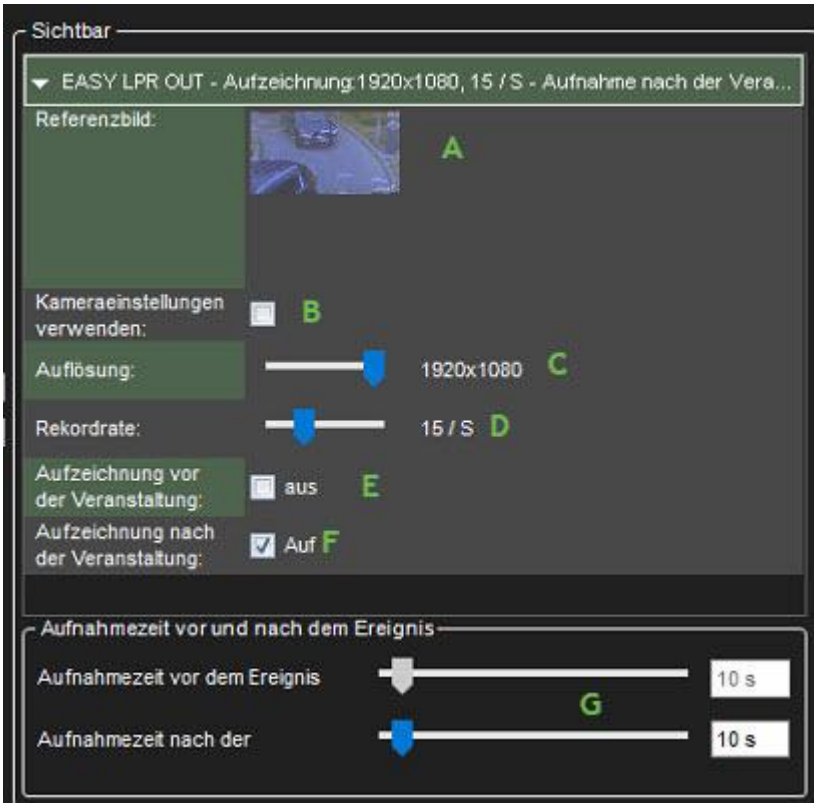
Die folgende Liste enthält die Standardaktionstypen und ihre Parameter. Einige der oben aufgeführten Aktionstypen sind möglicherweise nicht auf allen Systemen verfügbar.

> Zusätzlich zu den Standardaktionen kann das System Alarmaktionen enthalten, die über Module von Drittanbietern installiert werden.

10.11.1.2.1 Kameraaufnahme

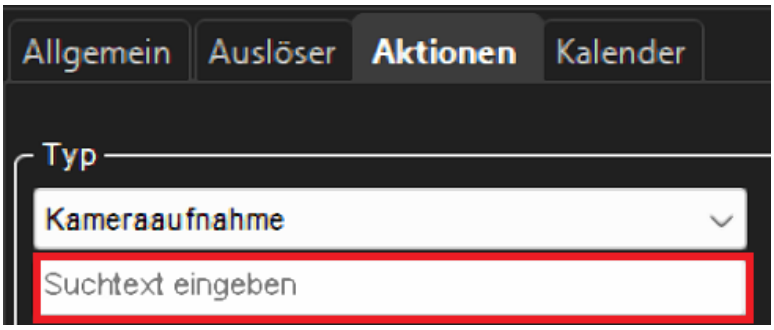
Die Kameraaufzeichnung ist die Standardaktion für Kameras. Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, werden die durch den Alarmtyp definierten Aufnahmeeinstellungen anstelle der Standardeinstellungen der Kamera verwendet.

Wenn in **Spotter** Alarm-Popup-Fenster für das Benutzerprofil aktiviert sind, werden Geräte, die mit der Aktion **Kameraaufzeichnung** verwendet werden, in der Alarm-Popup-Ansicht angezeigt, wenn der Alarm ausgelöst wird.



10.11.1.2.2Suche nach Aktionen

Um nach einer Aktion zu suchen, geben Sie den Namen der gesuchten Aktion in die Suchleiste ein.



Die Aktion umfasst die folgenden Felder und Parameter:

10.11.1.2.2.1 Referenzbild

Dieses statische Feld enthält das Referenzbild (Image) der Kamera (A).

10.11.1.2.2.2 Kameraeinstellungen verwenden

Durch Aktivieren dieses Kontrollkästchens wird die Alarmaufzeichnung mit der kameraspezifischen Einstellung für Auflösung und Aufzeichnungsrate durchgeführt (B).

10.11.1.2.2.3 Auflösung

Verwenden Sie den Schieberegler, um die Auflösung einer IP-Kamera während der Alarmaufzeichnung zu ändern. Der Schieberegler ist nur für IP-Kameras aktiv (C).

10.11.1.2.2.4 Aufzeichnungsrate

Verwenden Sie den Schieberegler, um die IPS-Rate der Kamera während der Alarmaufzeichnung zu ändern. Der Schieberegler ist inaktiv, wenn das Kontrollkästchen **Kameraeinstellungen verwenden** markiert ist (D).

10.11.1.2.2.5 Aufzeichnung vor der Veranstaltung

Markieren Sie dieses Kontrollkästchen, um die Aufzeichnung vor dem Ereignis einzuschalten. Die Dauer der Aufzeichnung vor der Veranstaltung kann mit dem Schieberegler **Aufzeichnung vor der Veranstaltung** eingestellt werden (E).

10.11.1.2.2.6 Aufzeichnung nach der Veranstaltung

Aktivieren Sie dieses Kontrollkästchen, um die Aufzeichnung nach der Veranstaltung aktivieren. Die Dauer der Aufzeichnung nach der Veranstaltung kann mit dem Schieberegler **Aufzeichnung nach der Veranstaltung** eingestellt werden (F).

10.11.1.2.2.7 Aufnahmezeit vor und nach dem Ereignis

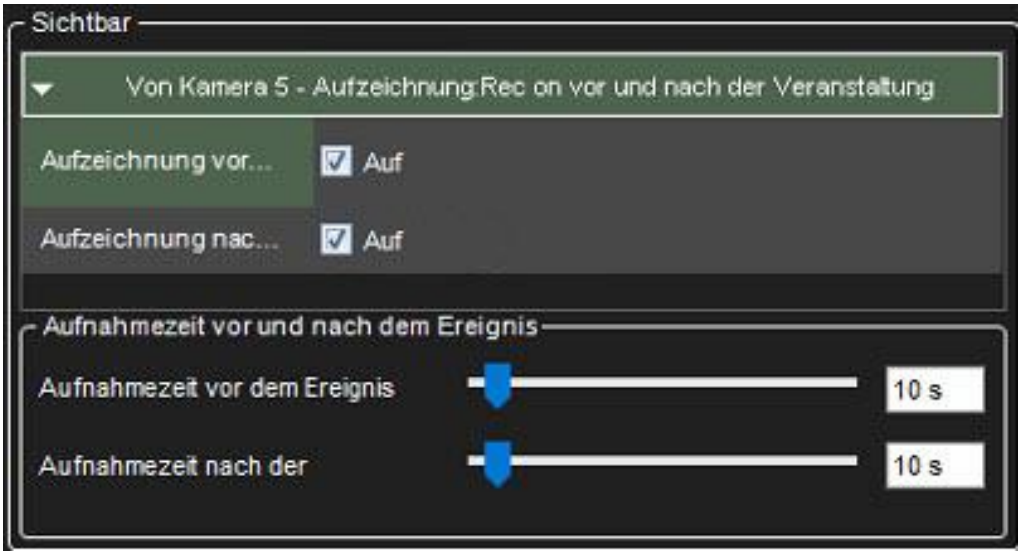
Diese Schieberegler können verwendet werden, um die Aufzeichnungsdauer vor und nach dem Ereignis für die Aktion einzustellen. Die Schieberegler sind nur aktiv, wenn die Aufzeichnung vor und/oder nach dem Ereignis aktiviert wurde (G).

Alle Geräte (Kameras und Mikrofone) sind mit dem Alarm verbunden und haben ihre Aufzeichnung vor und nach dem Ereignis aktiviert, um die gleiche Aufzeichnungsdauer vor und nach dem Ereignis zu teilen.

10.11.1.2.3Audio Aufnahme

Die Audioaufzeichnung ist die Standardaktion für Mikrofone. Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, werden die vom Alarmtyp definierten Aufnahmeeinstellungen anstelle der Standardeinstellungen des Mikrofons verwendet.

Wenn in **Spotter** Alarm-Popup-Fenster für das Benutzerprofil aktiviert sind, werden Geräte, die mit der Aktion **Audioaufnahme** verwendet werden, in der Alarm-Popup-Ansicht angezeigt, wenn der Alarm ausgelöst wird.



Die Aktion umfasst die folgenden Felder und Parameter:

10.11.1.2.3.1 Aufzeichnung vor der Veranstaltung

Markieren Sie dieses Kontrollkästchen, um die Aufzeichnung vor dem Ereignis einzuschalten. Die Dauer der Aufzeichnung vor der Veranstaltung kann mit dem Schieberegler **Aufzeichnung vor der Veranstaltung** eingestellt werden.

10.11.1.2.3.2 Aufzeichnung nach der Veranstaltung

Aktivieren Sie dieses Kontrollkästchen, um die Aufzeichnung nach der Veranstaltung aktivieren. Die Dauer der Aufzeichnung nach der Veranstaltung kann mit dem Schieberegler **Aufzeichnung nach der Veranstaltung** eingestellt werden.

10.11.1.2.3.3 Aufnahmezeit vor und nach dem Ereignis

Diese Schieberegler können verwendet werden, um die Aufzeichnungsdauer vor und nach dem Ereignis für die Aktion einzustellen. Die Schieberegler sind nur aktiv, wenn die Aufzeichnung vor und/oder nach dem Ereignis aktiviert wurde.

> Alle Geräte (Kameras und Mikrofone), die mit dem Alarm verbunden sind und deren Aufzeichnung vor und nach dem Ereignis aktiviert ist, um die gleiche Aufzeichnungsdauer vor und nach dem Ereignis zu teilen.

10.11.1.2.4Digitaler Ausgang

Der **digitale Ausgang** ist die Standardaktion für digitale E/A-Geräte. Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, wird das E/A-Gerät aktiviert.

Auch wenn die Schieberegler **Aufnahmezeit vor und nach dem Ereignis** für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.

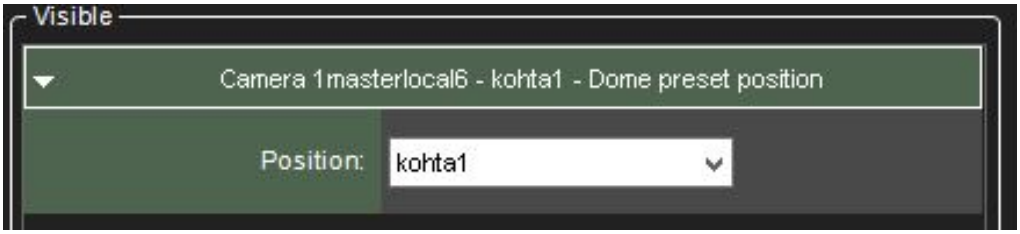
10.11.1.2.5PTZ (Dome) Voreingestellte Position

Die Aktion **PTZ voreingestellte Position** kann verwendet werden, um eine PTZ-Kamera auf eine bestimmte voreingestellte Position einzustellen.

Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, bewegt sich die PTZ-Kamera automatisch in die ausgewählte voreingestellte Position.

Informationen zum Festlegen von voreingestellten PTZ-Kamerapositionen finden Sie im Mirasys VMS Spotter-Benutzerhandbuch.

Es sollte beachtet werden, dass diese Aktion die PTZ-Kamera in eine voreingestellte Position bewegt, aber nicht dazu führt, dass der Video-Feed von der PTZ-Kamera in der Alarmansicht in der Client-Anwendung angezeigt wird, es sei denn, es wurden andere Alarmaktionen wie **Kameraaufzeichnung** durchgeführt für die PTZ-Kamera ausgewählt.



Die Aktion umfasst die folgenden Felder und Parameter:

10.11.1.2.5.1 Position

Verwenden Sie das Dropdown-Menü, um die voreingestellte Position auszuwählen, in die sich die PTZ-Kamera während des Alarms bewegt.

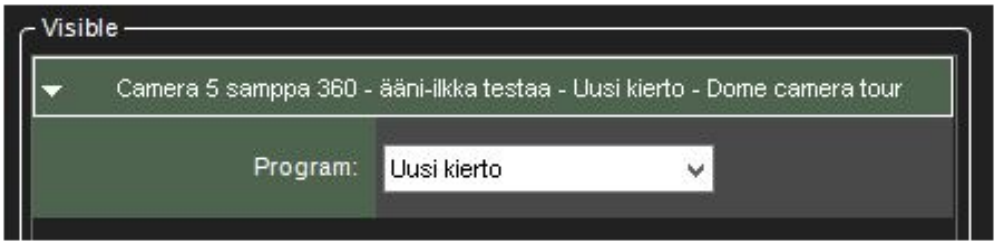
Auch wenn die Schieberegler **Aufnahmezeit vor und nach dem Ereignis** für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.

10.11.1.2.6PTZ (Dome) Kameratour

Die Aktion **PTZ-Kameratour** kann verwendet werden, um eine PTZ-Kamera so einzustellen, dass sie eine vorprogrammierte PTZ-Kameratour startet. Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, wird

die ausgewählte PTZ-Kameratour gestartet. Informationen zum Festlegen von voreingestellten PTZ-Kameratour finden Sie im *Mirasys VMS Spotter-Benutzerhandbuch.*

Es sollte beachtet werden, dass diese Aktion die PTZ-Kameratour startet, aber nicht dazu führt, dass der Video-Feed von der PTZ-Kamera in der Alarmansicht in der Client-Anwendung angezeigt wird, es sei denn, andere Alarmaktionen, wie z. B. **Kameraaufzeichnung,** wurden für ausgewählt PTZ-Kamera.



Die Aktion umfasst die folgenden Felder und Parameter:

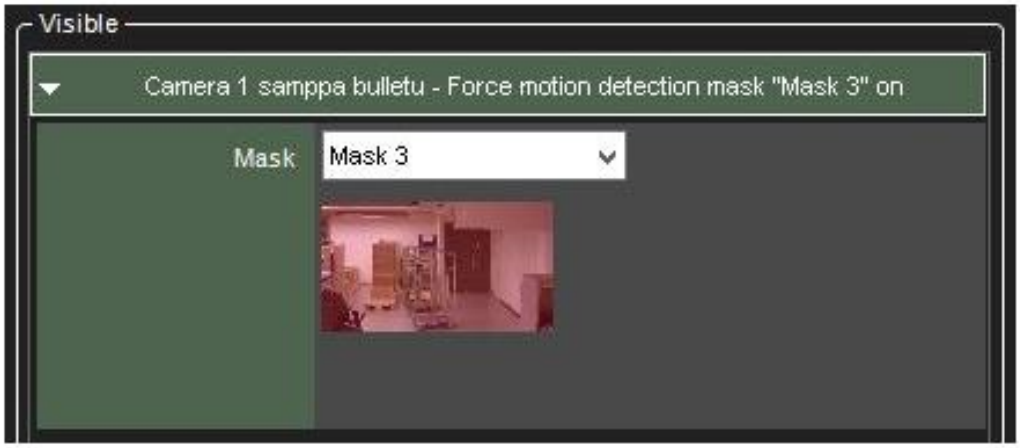
10.11.1.2.6.1 Program

Verwenden Sie das Dropdown-Menü, um die PTZ-Kameratour auszuwählen, die beginnt, wenn der Alarm ausgelöst wird.

> Auch wenn die Schieberegler **Aufnahmezeit vor und nach dem Ereignis** für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.

10.11.1.2.7Stellen Sie die Bewegungserkennungsmaske ein

Die Aktion **Stellen Sie die Bewegungserkennungsmaske ein** kann die Bewegungserkennungsmaske ändern, die von einer bestimmten Kamera während des Alarms verwendet wird. Wenn der Alarm auftritt, wird die für die bezeichnete Kamera verwendete Bewegungserkennungsmaske in die alarmspezifische Maske geändert. Nach Ende des Alarms stellt das System die Standardmaske wieder her.



Die Aktion umfasst die folgenden Felder und Parameter:

10.11.1.2.7.1 Masken

Verwenden Sie das Dropdown-Menü, um die Bewegungserkennungsmaske auszuwählen, die während des Alarms verwendet wird.

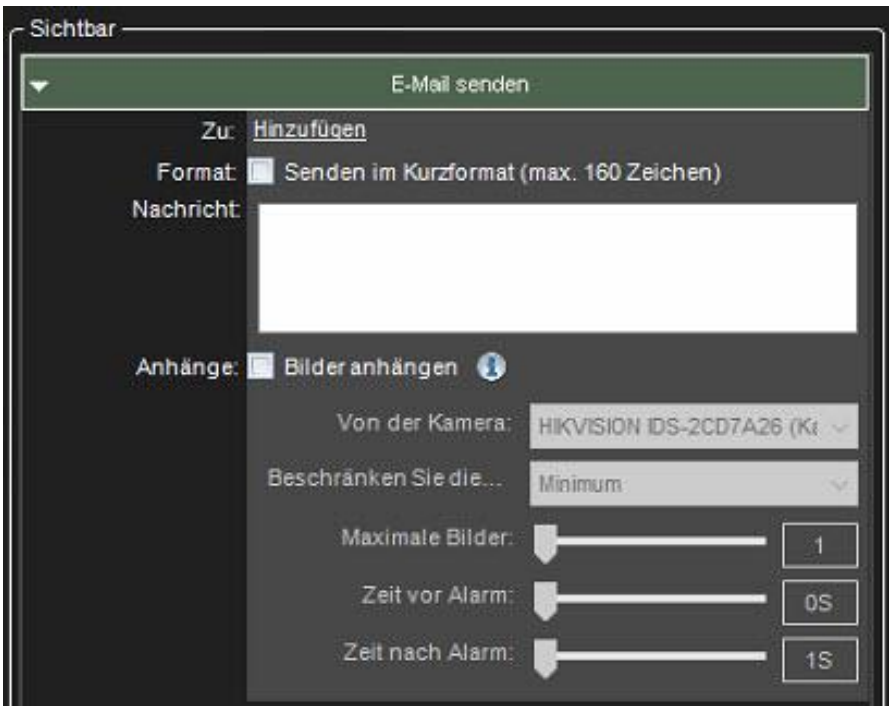
> Auch wenn die Schieberegler 2Vor- und Nachaufzeichnungsdauer2 für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.

10.11.1.2.8E-Mail senden

Die Aktion **E-Mail senden** kann zum Senden von E-Mails an beliebige E-Mail-Adressen oder Gruppen verwendet werden, die in den **E-Mail-Einstellungen** auf der Registerkarte **System** konfiguriert wurden.

Sie können auswählen, welcher Empfänger oder welche Gruppe den Alarm erhalten soll.

Sie können auch ein oder mehrere unskalierte oder verkleinerte Bilder in die Alarm-E-Mail einfügen. Deaktivieren Sie dazu die Option **Im Kurzformat senden** und aktivieren Sie die Option **Bilder anhängen**



Danach können Sie eine Kamera, die Größe für die Bildskalierung, die gewünschte Anzahl von Bildern und den Zeitraum, aus dem die Bilder abgerufen werden, auswählen.

- Die Anzahl der Bilder in dieser Konfiguration ist die maximal gelieferte Menge. Möglicherweise kommen weniger Bilder an.
- Das Anhängen von Bildern an Alarm-E-Mails kann zu hohem Datenverkehr führen, daher wird empfohlen, die Konfigurationseinstellungen zu testen, um die optimale Einstellung zu finden.
- Wenn Sie Probleme haben, dass mit den Standardeinstellungen keine Bilder ankommen, wird empfohlen, mehr als ein Bild für die Einstellung „Maximale Bilder“ auszuwählen und die Schieberegler leicht anzupassen, um eine längere Zeit zu haben, in der die Bilder abgerufen werden.

Die Aktion umfasst die folgenden Felder und Parameter:

10.11.1.2.8.1 Format

Definiert das Nachrichtenformat als kurz oder normal.

Eine Kurznachricht enthält nur bis zu 160 Zeichen und kann keinen zusätzlichen Nachrichtentext oder Bildanhänge enthalten (siehe unten).

10.11.1.2.8.2 Nachricht

Dieses Feld enthält die Nachricht, die an die Empfänger gesendet wird, wenn der Alarm auftritt. Das Nachrichtenfeld ist nur aktiv, wenn das E-Mail-Format auf lang eingestellt ist.

Im Gegensatz zu anderen Alarmaktionen kann die Aktion **E-Mail senden** nur einmal für jeden Alarm ausgewählt werden. Nach der Auswahl verschwindet die Aktion aus der Liste der verfügbaren Aktionen. Die Nachricht enthält den Alarmnamen im Titel.

10.11.1.2.9Einstellungen für alle Alarmaktionen gleichzeitig anpassen

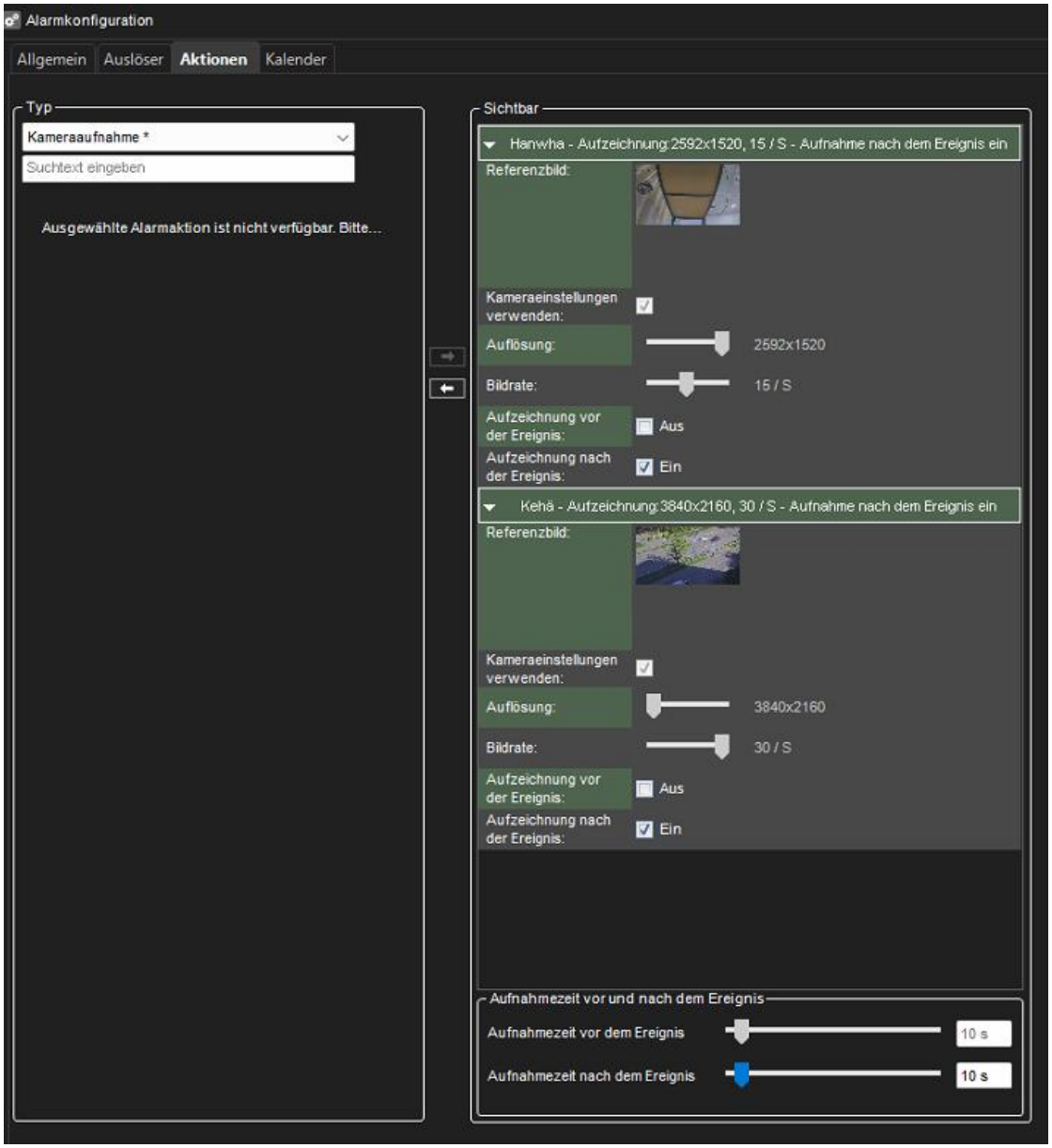
Die Einstellungen für mehrere Alarmaktionen können gleichzeitig in der Alarmkonfiguration angepasst werden. Diese Option beschleunigt die Konfiguration, wenn Alarme ähnliche Aktionen haben, da die Einstellungen nicht für jede Aktion separat angepasst werden müssen. In der Abbildung unten können beispielsweise die Einstellungen für die Alarmaktion für beide ausgewählten Kameras gleichzeitig angepasst werden.

Um Einstellungen für mehrere Aktionen gleichzeitig anzupassen, müssen alle ausgewählten Aktionen denselben Aktionstyp haben.

10.11.1.2.10 Einstellungen für alle Alarmaktionen gleichzeitig anpassen:

1. Öffnen **Alarme**
2. Öffnen Sie die Registerkarte **Aktionen** in der Alarmkonfiguration

3. Wählen Sie den richtigen Aktionstyp aus dem Dropdown-Menü aus und fügen Sie die gewünschten Aktionen hinzu
4. Wählen Sie die hinzugefügten Aktionen aus der Liste aus (Sie können mehrere auswählen, indem Sie die Strg-Taste gedrückt halten, während Sie auf die Elemente klicken)
5. Passen Sie die Einstellungen einer der ausgewählten Aktionen an: Die gleichen Änderungen werden automatisch auf alle ausgewählten Aktionen angewendet



10.11.1.2.11 Alarme deaktivieren

Die Aktion **Alarme deaktivieren** kann verwendet werden, um Deaktivierungsalarme basierend auf einem Alarm zu senden. Die Konfiguration kann so erfolgen, dass alle Alarme deaktiviert sind, Alarme mit niedriger und mittlerer Priorität oder Alarme mit niedriger Priorität.

Mit dieser Option können bestimmte Alarme aktiv bleiben, während andere unterdrückt werden.

Die Alarme werden nur deaktiviert, solange der Alarm, der sie deaktiviert, aktiv ist.

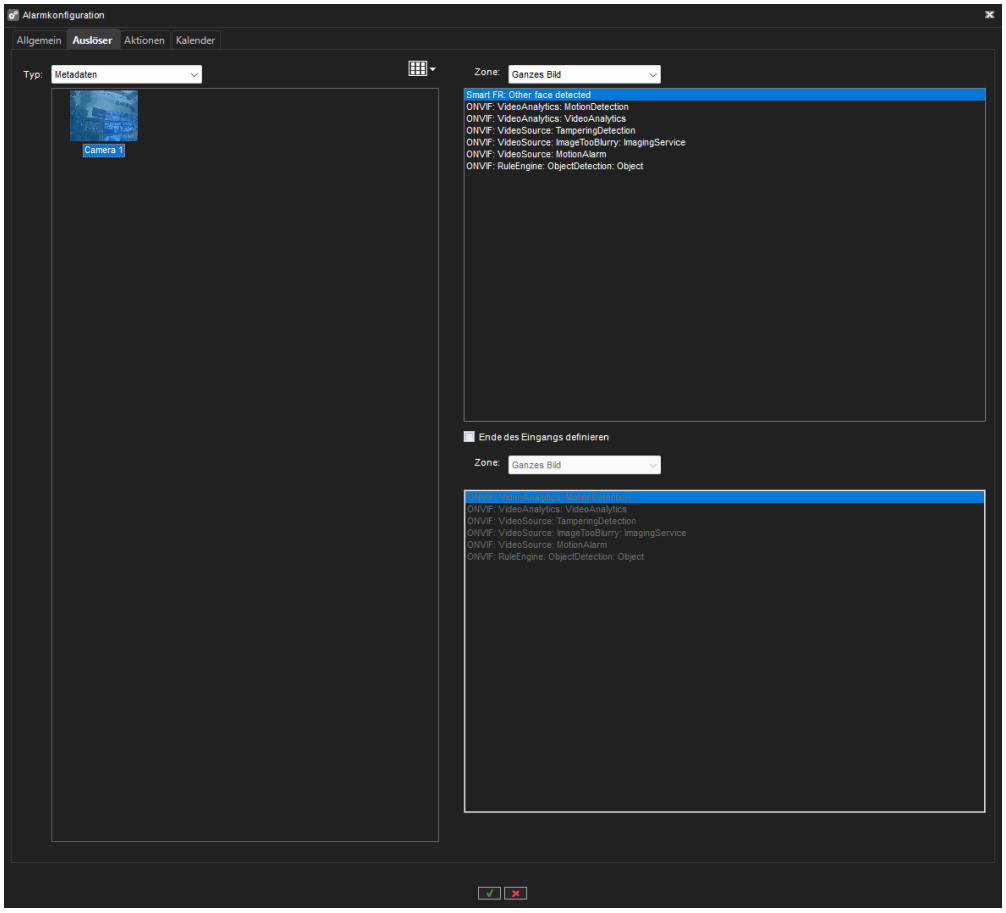
10.11.1.3 ONVIF Profile M

Unser System unterstützt jetzt das ONVIF-Profil M. Mit diesem wichtigen Update kann unser VMS effektiv auf Alarmauslöser unterstützender Kameras reagieren und so die Sicherheit und Reaktionsfähigkeit Ihrer Überwachungseinrichtung verbessern.

Um eine nahtlose Integration und Konformität zu gewährleisten, haben wir diese Funktion mit führenden Kameramarken, darunter Axis, Bosch und Hanwha, eingehend getestet.

10.11.1.3.1 ONVIF Alarm

Sobald Sie ein Gerät hinzugefügt haben, das das ONVIF-Profil M unterstützt, müssen Sie keine besonderen Schritte unternehmen, um diese Auslöser zu aktivieren oder zu deaktivieren. Sie werden automatisch zu den Metadatenauslösern der Kamera hinzugefügt. In der Alarmkonfiguration im System-Manager wird dies auf der Registerkarte Auslöser angezeigt und als ONVIF aufgeführt. Sie können diese zum Erstellen neuer Alarme verwenden.



10.11.1.3.2Einen ONVIF-Alarm auslösen

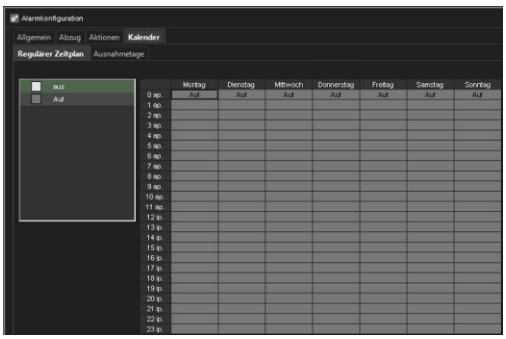
Die Gerätealarme/-auslöser selbst sollten über die Webschnittstelle des Geräts konfiguriert werden, da der System Manager keine Benutzeroberfläche für ihre Konfiguration hat. Diese Konfiguration sollte durchgeführt werden, bevor Sie das Gerät zu VMS hinzufügen, oder die Gerätefunktionen sollten im System Manager aktualisiert werden, um die Änderungen am Gerät zu verstehen.

1. System Manager starten.
2. Fügen Sie ein Gerät mit ONVIF Profil M Unterstützung hinzu.
3. Gehen Sie zur Registerkarte VMS-Server.
4. Wählen Sie die Menüpunkt **Alarm**.
5. Wählen Sie einen **Neuen Alarm**.
6. Die Registerkarte **Allgemein** wird geöffnet, in der Sie dem Alarm einen Namen geben und auswählen können, welche Profile den Alarm verwenden sollen.

7. Gehen Sie zur Registerkarte **Auslöser**.
8. Wählen Sie als Typ **Metadaten**.
9. Wählen Sie den Typ der ONVIF-Metadaten, die Sie zur Auslösung des Alarms verwenden möchten.
10. Gehen Sie auf die Registerkarte **Aktionen** und wählen Sie die gewünschte Aktion für den Alarm aus.
11. Gehen Sie auf die Registerkarte **Kalender** und wählen Sie aus, welche Tage/Stunden für den Alarm aktiviert sind. Standardmäßig ist der Alarm für jeden Tag 24 Stunden lang aktiv.
12. Klicken Sie abschließend auf OK am unteren Rand.

10.11.1.4 Alarme Kalender

1. Definieren Sie das, wenn der Alarm aktiv ist
2. Klicken **OK**



10.11.1.4.1 Ausnahmetage

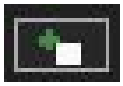
Alarmspezifische Feiertagszeitpläne können Zeitpläne für bestimmte Daten erstellen oder ein bestimmtes Datum festlegen, um einen Alarmzeitplan zu verwenden, der für einen anderen Wochentag entwickelt wurde. Auf die Unterregisterkarte **Ausnahmetage** über die Registerkarte **Kalender** des Alarms zugegriffen werden.

10.11.1.4.2 So stellen Sie ein bestimmtes Datum so ein, dass es mit dem Zeitplan eines anderen Wochentags funktioniert

1. Wählen Sie den Wochentag aus der Zeitplanliste auf der linken Seite des Bildschirms aus.
2. Wählen Sie das gewünschte Jahr und den gewünschten Monat aus den Dropdown-Menüs über dem Kalender aus.
3. Klicken Sie auf ein Datum im Kalender, um den Zeitplan hinzuzufügen.

10.11.1.4.3 So erstellen Sie einen benutzerdefinierten Zeitplan

1. Klicken Sie oben links auf dem Bildschirm auf Hinzufügen



2. Geben Sie den Namen des Ferienzeitplans in das Feld **Zeitplanname** ein.
3. Um den Zeitplan zu erstellen, wählen Sie **Aus** aus der Liste **Ein/Aus** auf der linken Seite des Bildschirms und markieren Sie die Stunden, zu denen der Alarm für den Tag ausgeschaltet ist.
4. Klicken Sie auf **OK**, um den Zeitplan zu speichern.
5. Wählen Sie das gewünschte Jahr und den gewünschten Monat aus den Dropdown-Menüs über dem Kalender aus.
6. Klicken Sie auf ein Datum im Kalender, um den Zeitplan hinzuzufügen.

10.11.1.4.4So bearbeiten Sie einen benutzerdefinierten Zeitplan

1. Wählen Sie den benutzerdefinierten Zeitplan aus der Zeitplanliste auf der linken Seite des Bildschirms aus.
2. Klicken Sie oben links auf dem Bildschirm auf Bearbeiten



3. Bearbeiten Sie den Zeitplan.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

10.11.1.4.5So löschen Sie einen benutzerdefinierten Zeitplan

1. Wählen Sie den benutzerdefinierten Zeitplan aus der Zeitplanliste auf der linken Seite des Bildschirms aus.
2. Klicken Sie oben links auf dem Bildschirm auf Entfernen



10.11.1.4.6So stellen Sie den ursprünglichen Zeitplan wieder her

1. Klicken Sie in der Zeitplanliste auf der linken Seite des Bildschirms auf **Wiederherstellen**.
2. Klicken Sie im Kalender auf den Tag, den Sie wiederherstellen möchten.

10.11.2 Benutzerdefinierte Alarmauslöser

Systemadministratoren können benutzerdefinierte Alarmauslöser unter System Manager > VMS Servers > Alarmauslöser erstellen. Auf dieser Registerkarte können Sie alle erstellten benutzerdefinierten Alarmauslöser in Tabellenform nach Auslösername, Typ, eindeutiger ID und Kamera anzeigen.

10.11.2.1 Benutzerdefinierte Web-API-Alarmauslöser

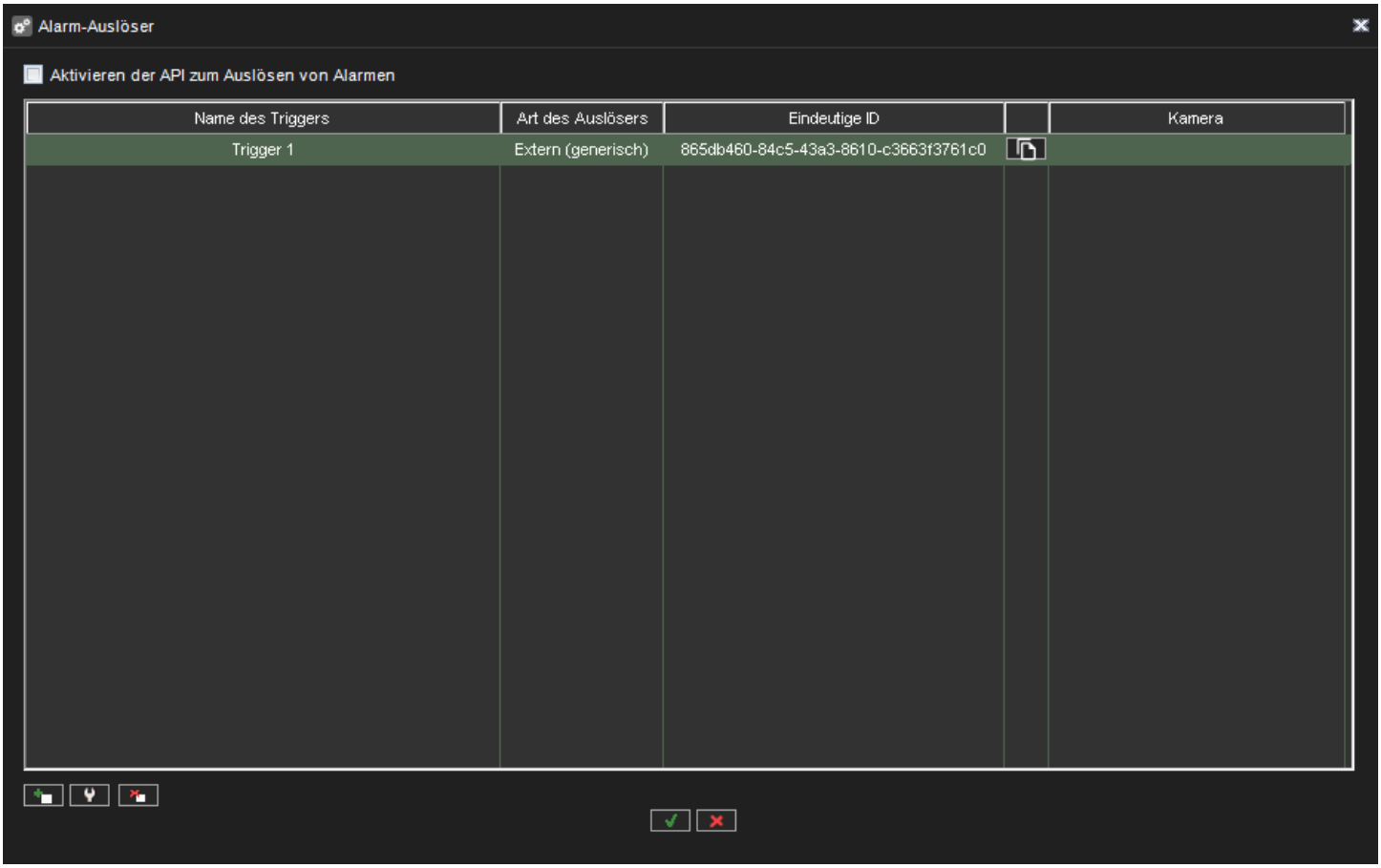
Wenn Sie Mirasys Alarm API zur Integration in unser System verwenden, können Systemadministratoren benutzerdefinierte Alarmauslöser unter System Manager > VMS Servers > Alarm Triggers erstellen.

Auf dieser Registerkarte können Sie alle erstellten benutzerdefinierten Alarmauslöser in Tabellenform nach Auslösername, Typ, eindeutiger ID und Kamera anzeigen.

Wenn Sie die **Alarmauslöser-API** im Fenster Alarmauslöser aktivieren, werden alle Alarmauslöser angezeigt, die von der Mirasys Alarm-API erstellt wurden.

10.11.2.1.1 Einen Alarmauslöser erstellen

1. Um einen Alarm zu erstellen, gehen Sie zu **VMS Servers** und wählen Sie Recorder.
2. Öffnen Sie **Alarmauslöser**.
3. Klicken Sie auf das grüne + Zeichen unten links im Fenster, um einen **API Trigger hinzuzufügen**. Ein neuer Dialog zum **Hinzufügen eines neuen Alarmauslösers** wird geöffnet.
4. Wählen Sie den Triggertyp **Mirasys Alarm API.**
5. Schreiben Sie den **Triggernamen** in das freie Textfeld.
6. Wählen Sie den Typ aus, der entweder **allgemeiner Alarm** oder **Kanal** ist.
    - Für **Kanal** definieren Sie bitte den Kanalbereich.
7. Klicken Sie auf **Speichern**. Das System generiert eine eindeutige ID für den Trigger, die in der Tabelle **Alarmauslöser** angezeigt wird.
8. Klicken Sie auf das grüne Häkchen, um die Einstellungen der **Alarmauslöser** zu **speichern**.



10.11.2.1.2Bearbeiten eines Alarmauslösers

1. Um einen Alarmauslöser zu ändern, gehen Sie zu **VMS Servers** und wählen Sie Recorder. Unter **Alarme** öffnen Sie **Alarmauslöser**.
2. Wählen Sie den Auslöser, den Sie ändern möchten, aus der Liste aus.
3. Klicken Sie auf die Schaltfläche **Ändern**.
4. Sie können den Triggernamen ändern und Kanal oder allgemeiner Alarm auswählen. Für Kanal definieren Sie bitte den Kanalbereich. Das System wird eine eindeutige ID für den Auslöser generieren.
5. Klicken Sie auf **Änderungen speichern**.

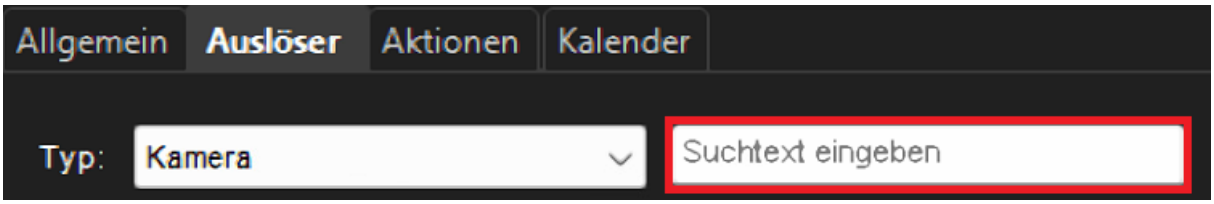
10.11.2.1.3Löschen eines Alarmauslösers

1. Um einen Alarmauslöser zu löschen, gehen Sie zu **VMS Servers** und wählen Sie Recorder. Unter **Alarme** öffnen Sie **Alarmauslöser.**

2. Wählen Sie einen Alarm aus der Auslöserliste.
3. Klicken Sie auf die Schaltfläche **Löschen**.
4. Bestätigen Sie den Löschvorgang im Bestätigungsmodal.

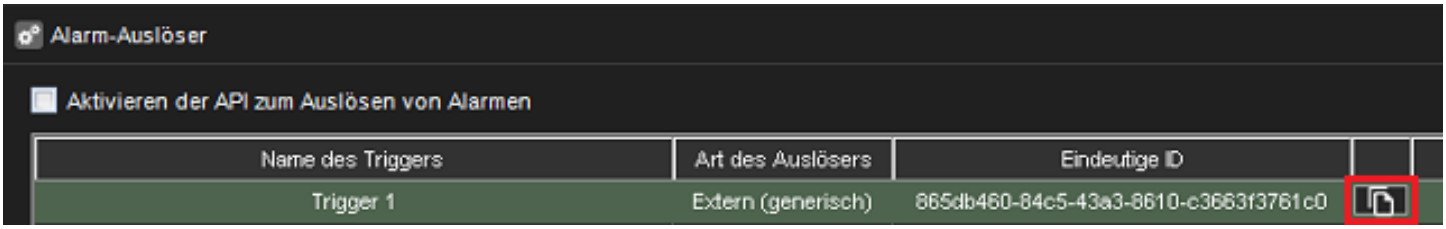
10.11.2.1.4Auslöser suchen

1. Gehen Sie zu **Alarme** und doppelklicken Sie auf einen Alarm
2. Öffnen Sie die Registerkarte **Auslöser**
3. Geben Sie den Namen des gesuchten Auslösers in die Suchleiste ein



10.11.2.1.5Kopieren einer Alarmauslöser-ID

1. Gehen Sie zur Registerkarte **VMS-Server** im System-Manager
2. Doppelklick auf **Alarmauslöser**
3. Klicken Sie auf die Schaltfläche **Kopieren** neben der ID des Auslösers



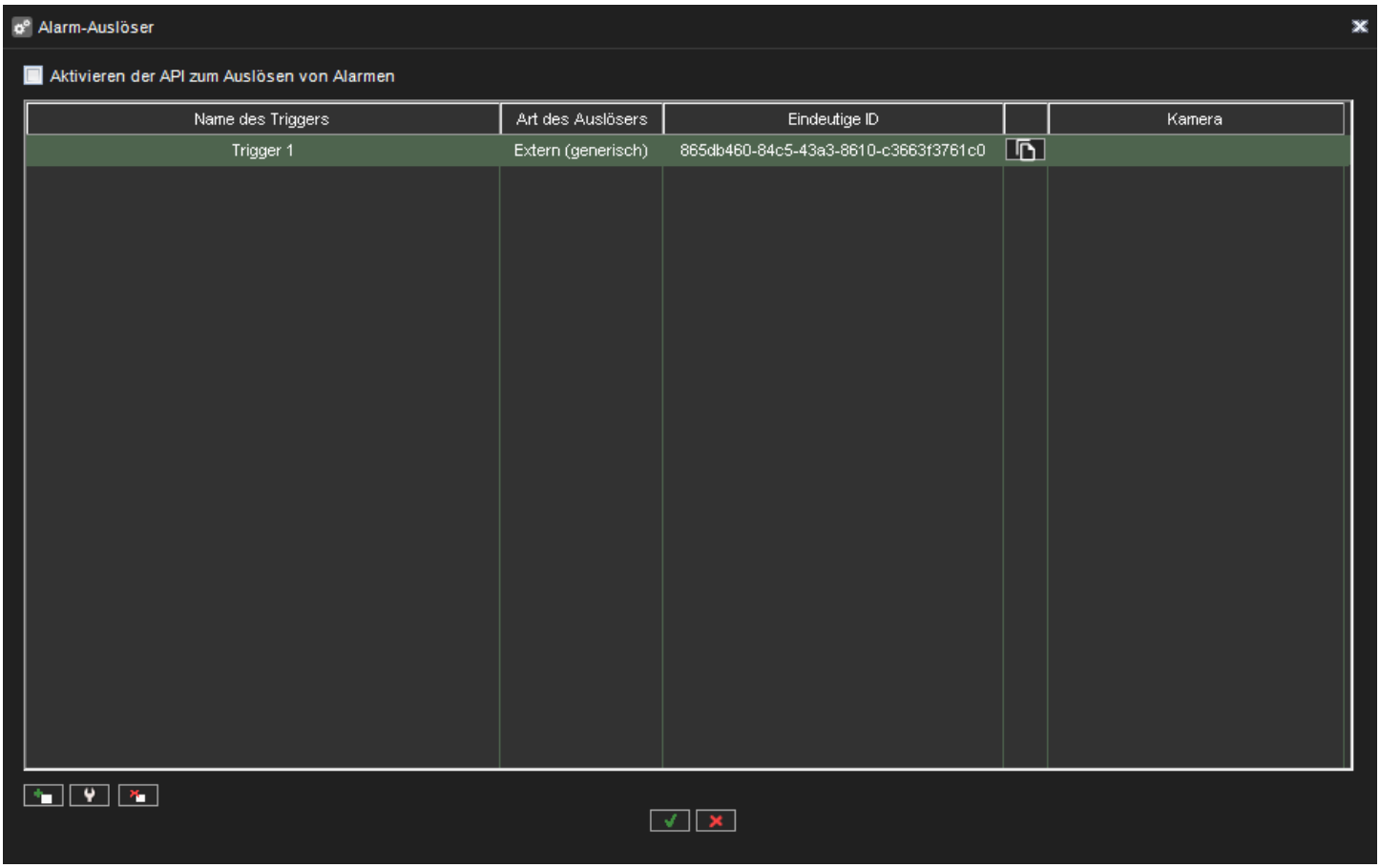
Die Auslöser-ID kann auch beim Hinzufügen oder Ändern eines Auslösers kopiert werden, indem Sie den Text im ID-Feld markieren und Strg + C drücken oder mit der rechten Maustaste auf den Text klicken und „Kopieren“ auswählen.

Die ID wird in die Zwischenablage kopiert und kann so einfach in externe Anwendungen eingefügt werden.

10.11.2.2 ONVIF Profil M Benutzerdefinierte Alarmauslöser

Bei der Verwendung von ONVIF-Profil-M-konformen Geräten können Systemadministratoren in unserem VMS Alarmauslöser auf der Grundlage der auf der Kameraseite verfügbaren Metadaten erstellen.

Gehen Sie zu System Manager > VMS-Server > Alarmauslöser

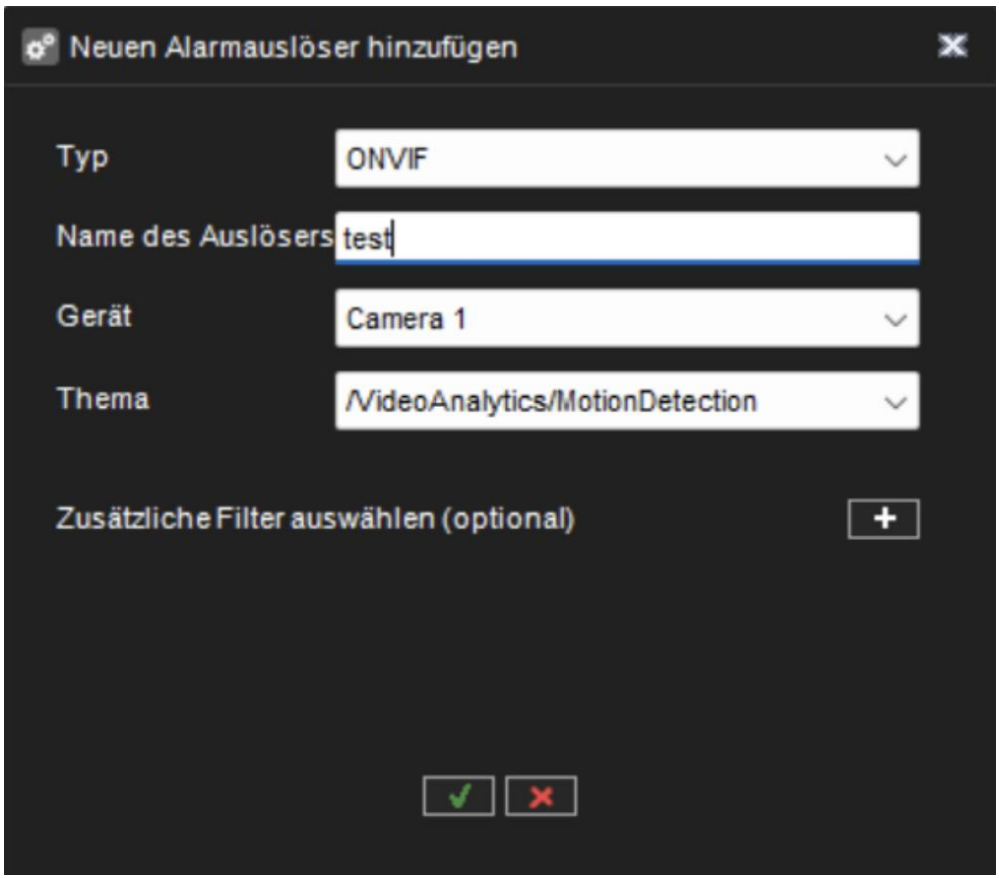


10.11.2.2.1Einen Alarmauslöser erstellen

1. Öffnen Sie Alarmauslöser. Es wird eine Tabelle mit Ihren benutzerdefinierten Alarmauslösern angezeigt.
2. Klicken Sie auf das +-Zeichen in der unteren linken Ecke, um einen Alarmauslöser hinzuzufügen.

Dadurch wird das Dialogfeld **Neuen Alarmauslöser hinzufügen** geöffnet.

3. Wählen Sie den **Auslösertyp** ONVIF.
4. Schreiben Sie den **Namen des Auslösers**, den Sie für den Auslöser gewählt haben.
5. Wählen Sie im Dropdown-Menü **Gerät** eine Kamera aus.
6. Wählen Sie im Dropdown-Menü ein **Thema** für den Auslöser, z. B. Bewegungserkennung.



7. **Wählen Sie zusätzliche Filter** aus, indem Sie auf das +-Zeichen klicken.

10.11.2.2.2Filter nach Quelle und Parameter

Wir empfehlen dringend, optionale Filter nach Quelle und Parameter auszuwählen, um festzulegen, welche Alarme empfangen werden sollen.

In den Feldern Filter nach Quelle und Parameter können Systemadministratoren so viele Filter hinzufügen, wie sie möchten.

Um eine **Quelle hinzuzufügen**, klicken Sie auf das +-Zeichen. Wählen Sie die Quelle aus den verfügbaren Quellen im Dropdown-Menü **Namen**. Definieren Sie den **Wert**. Definieren Sie die **Operation**.

Um einen **Parameter hinzuzufügen**, klicken Sie auf das + Zeichen. Wählen Sie den Parameter aus den verfügbaren Parametern im Dropdown-Menü Namen aus. Definieren Sie den **Wert**. Definieren Sie die **Operation**. Wählen Sie **Größer oder gleich** oder **Kleiner oder gleich** unter Operation, um einen Wertebereich zu definieren.

Um Quellen und Parameter zu entfernen, befindet sich rechts neben jeder Zeile ein rotes --Zeichen. Klicken Sie zum Entfernen.

Klicken Sie auf ✓ zum **Speichern**. Sie kehren zum Dialogfeld Neuen Alarmauslöser hinzufügen zurück.

Wenn Sie den Wert nicht eingegeben haben, ist die Funktion Speichern ✓ deaktiviert.

1. Klicken Sie auf ✓ zum Speichern.

10.11.2.2.3Bearbeiten eines Alarmauslösers

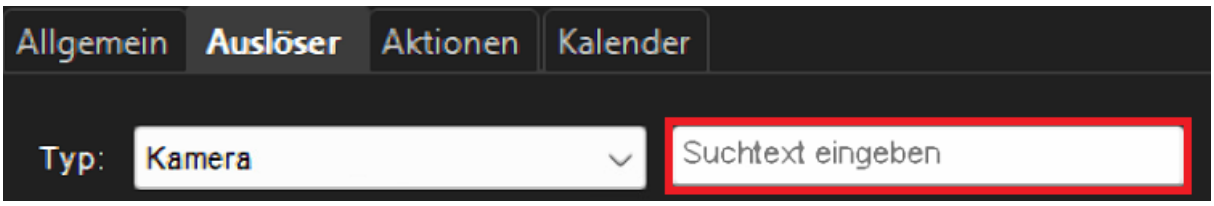
1. Um einen Alarmauslöser zu ändern, gehen Sie zu **VMS Servers**, wählen Sie Recorder und öffnen Sie unter Alarme den Punkt **Alarmauslöser**.
2. Wählen Sie den Auslöser, den Sie ändern möchten, aus der Liste aus.
3. Klicken Sie auf die Schaltfläche **Ändern** unten links (Schraubenschlüssel-Symbol).
4. Siehe oben unter Erstellen eines Alarmauslösers, um zu erfahren, wie Sie Änderungen vornehmen können.
5. Klicken Sie auf ✓, um die Änderungen zu **speichern**.

10.11.2.2.4Löschen eines Alarmauslösers

1. Um einen Alarmauslöser zu löschen, gehen Sie zu **VMS Servers** und wählen Sie Recorder.
2. **Alarmauslöser** öffnen.
3. Wählen Sie einen Alarm aus der Auslöserliste aus.
4. Klicken Sie auf die rote X-Schaltfläche unten links, um zu **löschen.**
5. Bestätigen Sie die Löschung im Bestätigungsmodal.

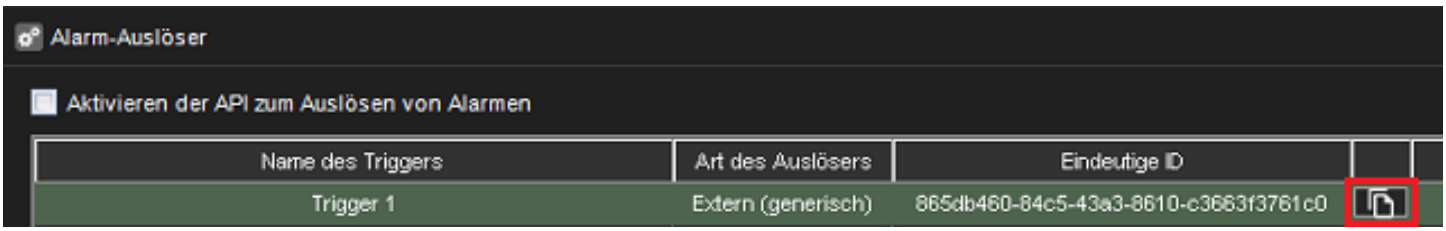
10.11.2.2.5Auslöser suchen

1. Gehen Sie zu **Alarme** und doppelklicken Sie auf einen Alarm
2. Öffnen Sie die Registerkarte **Auslöser**
3. Geben Sie den Namen des gesuchten Auslösers in die Suchleiste ein



10.11.2.2.6Kopieren einer Alarmauslöser-ID

1. Gehen Sie zur Registerkarte **VMS-Server** im System-Manager
2. Doppelklick auf **Alarmauslöser**
3. Klicken Sie auf die Schaltfläche **Kopieren** neben der ID des Auslösers



Die Auslöser-ID kann auch beim Hinzufügen oder Ändern eines Auslösers kopiert werden, indem Sie den Text im ID-Feld markieren und Strg + C drücken oder mit der rechten Maustaste auf den Text klicken und „Kopieren“ auswählen.

Die ID wird in die Zwischenablage kopiert und kann so einfach in externe Anwendungen eingefügt werden.

10.12 Speicherung

In den Speichereinstellungen können Sie die Speicherzeit der aufgezeichneten Video-, Audio- und Textdaten sowie Alarmdaten festlegen.

Darüber hinaus können Sie nach dem Hinzufügen einer Festplatte zu einem Server diese über die Speichereinstellungen als zusätzlichen Datenspeicher festlegen.

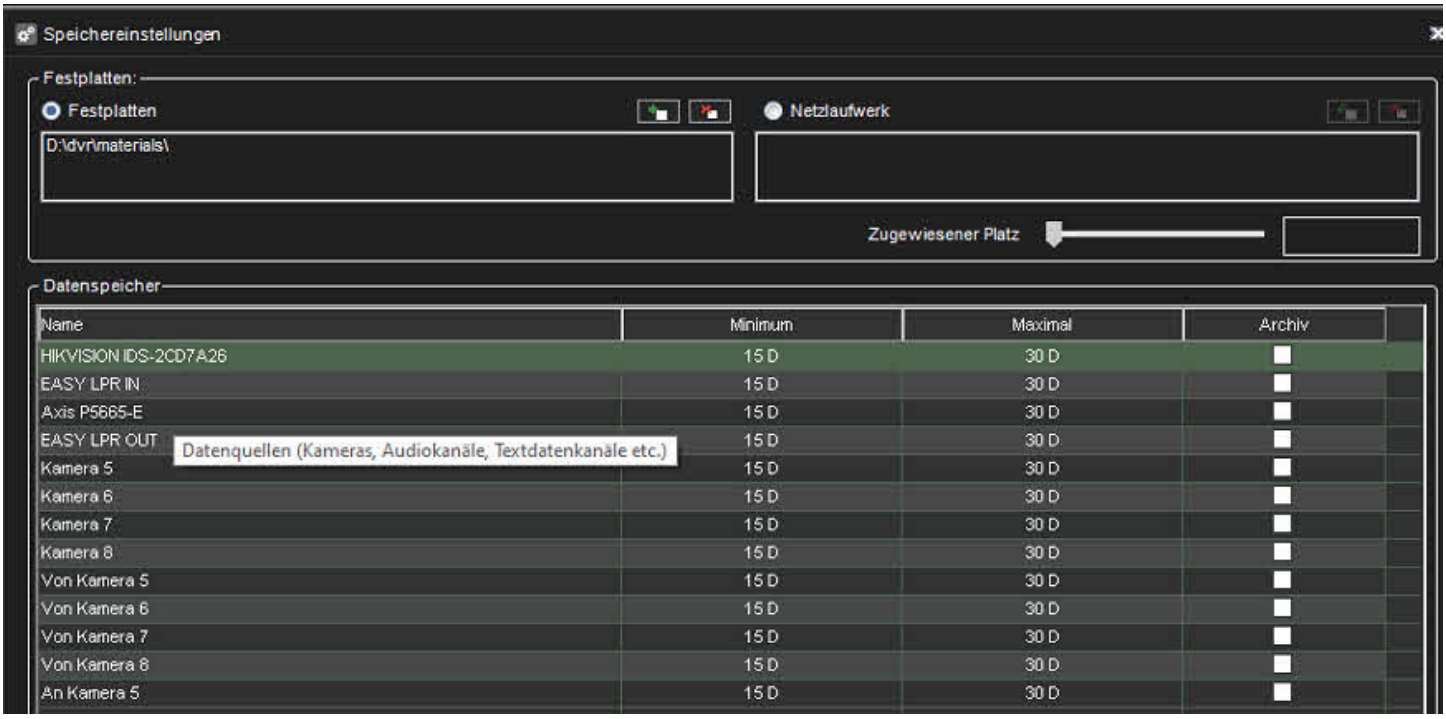
Die Speichereinstellungen werden auch verwendet, um die automatische Archivierungsfunktion zu konfigurieren, die es ermöglicht, täglich oder wöchentlich Sicherungskopien der serverspezifischen Video-, Audio- und Textdaten zu erstellen.

Video-, Audio-, Textdaten und Alarmaufzeichnungen werden aufbewahrt, bis ihr definiertes **Maximum**-Datum überschritten oder der zugewiesene Speicherplatz erschöpft ist.

10.12.1 Speicherplatz hinzufügen

Wenn zusätzlicher Speicherplatz benötigt wird, können Sie neue Festplatten hinzufügen oder ein Netzlaufwerk für die Datenspeicherung (z. B. NAS-Unterstützung) zuordnen.

Wie im Bild zu sehen, können mehrere Netzwerkspeicherlaufwerke und lokale Laufwerke gleichzeitig verwendet werden.



Notiz: *Beim Hinzufügen von Speicherlaufwerken zum alten Mirasys-Dateisystem (VMS-Serverversion 7.5.x oder früher) wird empfohlen, dass die Speicherlaufwerke alle die gleiche Kapazität haben, und jede einzelne Festplatte sollte weniger als 10 TB groß sein, und die Gesamtgröße pro VMS Server sollte weniger als 25 TB groß sein.*

Die Verwendung mehrerer Speicherplatten hat den Vorteil, dass das Schreiben von Material auf alle Laufwerke verteilt werden kann, wodurch es unwahrscheinlicher wird, dass ein Verlust eines einzelnen Materiallaufwerks große Teile des gespeicherten Materials auslöscht.

10.12.1.1 So fügen Sie eine Festplatte hinzu:

1. Installieren Sie die neue Festplatte.
2. Klicken Sie in Speichereinstellungen auf Festplatte hinzufügen.



Das Dialogfeld Datenträger hinzufügen wird angezeigt.Die Minimaler freier Speicherplatz auf der neuen Diskettenbox zeigt, wie viel freien Speicherplatz die neue Diskette haben muss.

3. Wählen Sie die Festplatte aus der Liste aus und klicken Sie auf **OK**.

10.12.1.2 So ordnen Sie ein Netzlaufwerk zu:

1. Aktivieren Sie in **Speichereinstellungen** das Kontrollkästchen **Netzlaufwerk**.

2. Klicken Sie bei Bedarf auf Netzlaufwerk definieren



um den Konfigurationsbildschirm für Netzlaufwerke zu öffnen.

3. Geben Sie den Benutzernamen und das Passwort des Netzlaufwerks in die Felder **Benutzername** und **Passwort** ein.
4. Geben Sie den Speicherort des Netzlaufwerks in das Feld **Netzlaufwerkspfad** ein.
5. Klicken **OK**
6. Verwenden Sie den Schieberegler **Zugewiesener Speicherplatz**, um den Speicherplatz einzustellen, der auf dem Netzlaufwerk für die Datenspeicherung reserviert ist.

10.12.1.3 So ordnen Sie mehrere Netzlaufwerke zu:

1. Installieren und konfigurieren Sie den Netzwerkspeicher so, dass er als lokal zugeordnetes Laufwerk funktioniert (verwenden Sie beispielsweise iSCSI-Initiator oder ähnliches).
2. Klicken Sie in Speichereinstellungen auf Festplatte hinzufügen



Das Dialogfeld Datenträger hinzufügen wird angezeigt.

3. Die Speichergröße kann für iSCSI-Festplatten nicht konfiguriert werden.
4. Klicken Sie auf OK, um die Einstellungen zu speichern. Wiederholen Sie dies für andere Festplatten.

10.12.2 Speichereinstellungen für Video-, Audio- und Textdaten

10.12.2.1 Minimum

Um Aufzeichnungen von einem oder mehreren Video-, Audio- oder Textdatenkanälen zu priorisieren, stellen Sie sicher, dass die Mindestwerte für andere Kanäle ausreichend niedrig sind.

Stellen Sie dann den Wert für den oder die Kanäle mit hoher Priorität höher ein.

Wenn Sie **Automatisch** wählen, löscht das System Aufnahmen von Kanälen, die den meisten Speicherplatz beanspruchen.

10.12.2.2 Maximal

Das System prüft die Aufzeichnungen täglich und löscht diejenigen, die älter als die maximale Anzahl von Tagen sind.

Wenn Sie **Automatisch** wählen, werden die Aufnahmen nur gelöscht, wenn der freie Speicherplatz nicht ausreicht.

Notiz: *Wenn die Mindestwerte für einige Kanäle zu hoch sind, während sie gleichzeitig für andere Kanäle nicht eingestellt sind, löscht das System Aufzeichnungen von den Kanälen ohne eingestelltes Minimum.*

10.12.2.3 Alarmgrenzen

10.12.2.3.1 Minimum

Das System löscht Alarme, die älter als der Mindestwert sind.

Wenn Sie **Automatisch** wählen, werden die Aufnahmen nur gelöscht, wenn der freie Speicherplatz nicht ausreicht.

10.12.2.3.2 Maximal

Das System prüft die Alarmaufzeichnungen täglich und löscht sie, die älter als die maximale Anzahl an Tagen sind.

Wenn Sie **Automatisch** wählen, werden die Aufnahmen nur gelöscht, wenn der freie Speicherplatz nicht ausreicht.

10.12.2.3.2.1 Log-Einträge

Dieser Wert gibt an, wie viele Alarmereignisse maximal im Alarmprotokoll gespeichert werden.

Das System prüft stündlich die Anzahl der Logeinträge und löscht bei Überschreitung die ältesten Einträge.

10.12.2.3.2.2 % maximal

Dieser Wert gibt an, wie viel Speicherplatz Alarmaufzeichnungen vom gesamten Speicherplatz verwenden dürfen.

Solange nicht der gesamte Speicherplatz belegt ist, können Alarmaufzeichnungen mehr Speicherplatz als diesen Wert beanspruchen.

Das System löscht zuerst die ältesten Alarmaufzeichnungen, bevor es andere Video- oder Audioaufzeichnungen löscht, wenn der gesamte Speicherplatz belegt ist.

10.12.3 Automatisches Löschen von Video-, Audio- und Textdaten

Nach Überschreiten der definierten maximalen Speicherzeit werden gespeicherte Video-, Audio-, Text- und Alarmdaten automatisch gelöscht – die maximale Speicherzeit für Daten, die das System täglich prüft.

Da die Größe eines gespeicherten Datenstroms aufgrund von Bewegungen im Videobild, Änderungen der Audiopegel oder der Anzahl von Textdatenereignissen erheblich variieren kann, kann es schwierig sein, den Speicherplatzbedarf genau vorherzusagen.

Daher kann es das System manchmal für erforderlich halten, freien Speicherplatz zu gewährleisten, indem es altes Material unabhängig von der maximalen Speicherzeit automatisch löscht.

Wenn Daten gelöscht werden müssen, um freien Speicherplatz zu gewährleisten, läuft der Löschvorgang nach folgendem Muster ab:

In einfachen Worten läuft dieser Aufbewahrungsprozess so ab, wenn FS eine neue kostenlose Datei benötigt:

1. Überprüfen Sie die Alarmquote. Wenn die Alarmmaterialdateien mehr zählen als die Quote (% von allen Daten), bereinigen wir die älteste Alarmdatei und verwenden sie wieder

2. Überprüfen Sie die Mindesteinstellungen für Alarmdaten – wenn Alarmkanäle Daten enthalten, die die Mindestalarmeinstellungen überschreiten – nehmen wir die älteste Datei von diesen, bereinigen sie und verwenden sie erneut
3. Überprüfen Sie die Mindesteinstellungen für alle Materialkanäle (Video, Audio, Daten) – wenn einige Kanäle Daten enthalten, die die Mindesteinstellungen überschreiten – nehmen wir die älteste Datei von diesen, bereinigen sie und verwenden sie wieder
4. Überprüfen Sie die älteste Datei von Kanälen mit automatischen Min-Einstellungen, wenn sie vorhanden sind. Wenn ja, nehmen wir die älteste Datei von diesen, bereinigen sie und verwenden sie erneut
5. Wenn immer noch nichts gefunden wird – wir nehmen einfach die älteste Datei aus allen Kanälen (Material und Alarm), bereinigen sie und verwenden sie erneut

Außerdem haben wir eine Hintergrundaufgabe, die Materialdateien gemäß den maximalen Einstellungen bereinigt.

Die Startperiode wird von allen Kanälen (Material und Alarm) auf eine minimale maximale Einstellung eingestellt.

Notiz: *Um sicherzustellen, dass die Notwendigkeit einer automatischen Löschung aufgrund von Speicherplatzmangel minimiert wird, ist es gut, die Festplattennutzung regelmäßig zu überwachen und die maximale Speicherzeit und den zugewiesenen Speicherplatz zu ändern.*

Es ist ratsam, manuelle oder automatische Archivierungstools zu verwenden, um sicherzustellen, dass keine relevanten Daten bei Speicherplatzproblemen gelöscht werden.

Hinweis *Sie können ein Watchdog-Ereignis festlegen, das Sie benachrichtigt, wenn der Speicherplatz knapp wird.*

10.12.4 Archivierung

Sie können das System so einstellen, dass Video-, Audio- und Textdaten täglich oder wöchentlich automatisch archiviert werden.

Die Archivdateien können automatisch auf den Festplatten des Servers oder einem Netzlaufwerk erstellt werden.

Die Archivdateien können auf jedem Spotter-Client geöffnet werden.

Notiz: *Archivdateien können sehr groß sein und daher den Speicherplatz schnell füllen. Archivdateien sollten regelmäßig von den Serverfestplatten oder Netzlaufwerken kopiert und entfernt werden, auf denen sie automatisch gespeichert werden.*

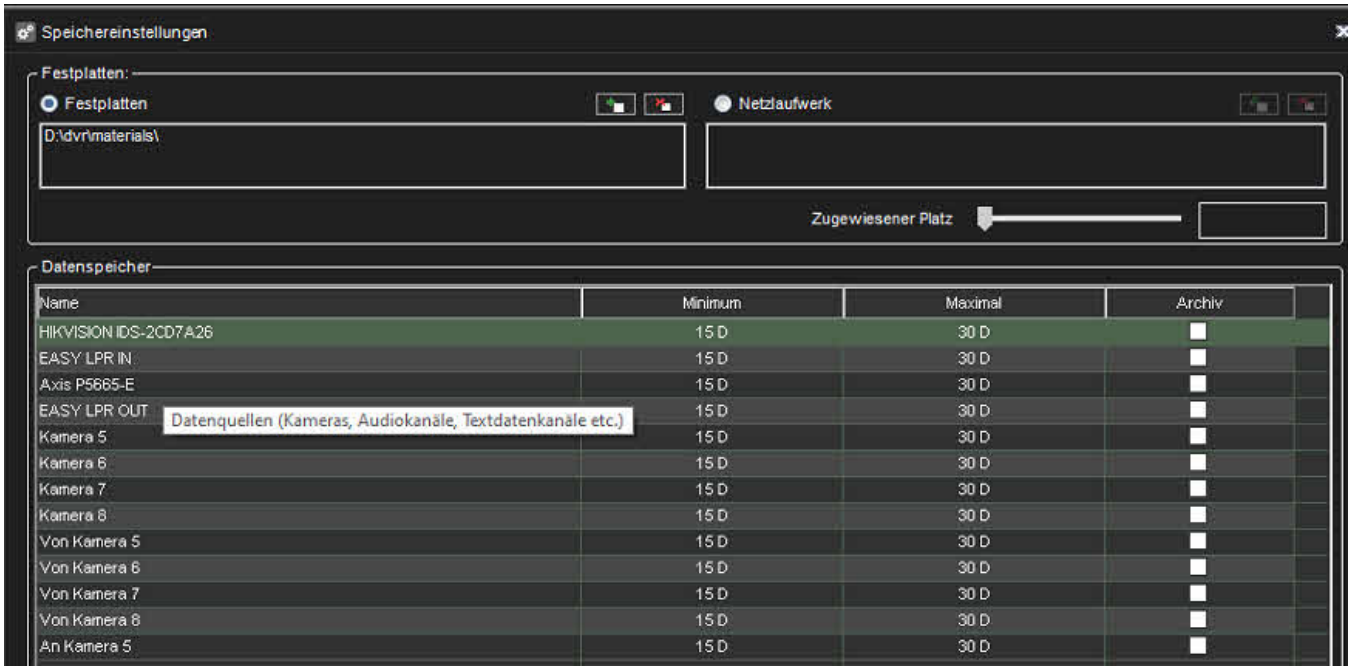
10.12.4.1 So legen Sie einen automatischen Archivierungszeitplan fest:

1. Klicken Sie im Bereich **Datenspeicherung** auf die Geräte, die Sie in den automatischen Archivierungsprozess einbeziehen möchten.
   Hinweis Wählen Sie benachbarte Geräte oder Ordner aus, halten Sie die UMSCHALTTASTE gedrückt und klicken Sie dann auf das erste und letzte Gerät, das Sie auswählen möchten.
   a. Um ein Gerät zu einer Auswahl hinzuzufügen oder aus einer Auswahl zu entfernen, halten Sie die STRG-Taste gedrückt und klicken Sie dann auf das Gerät, das Sie hinzufügen oder entfernen

möchten.

Hinweis: *Durch Auswählen einer Gerätegruppe (Ordner) wird auch deren Inhalt ausgewählt.*

2. Markieren Sie das Kontrollkästchen **Archiv**.

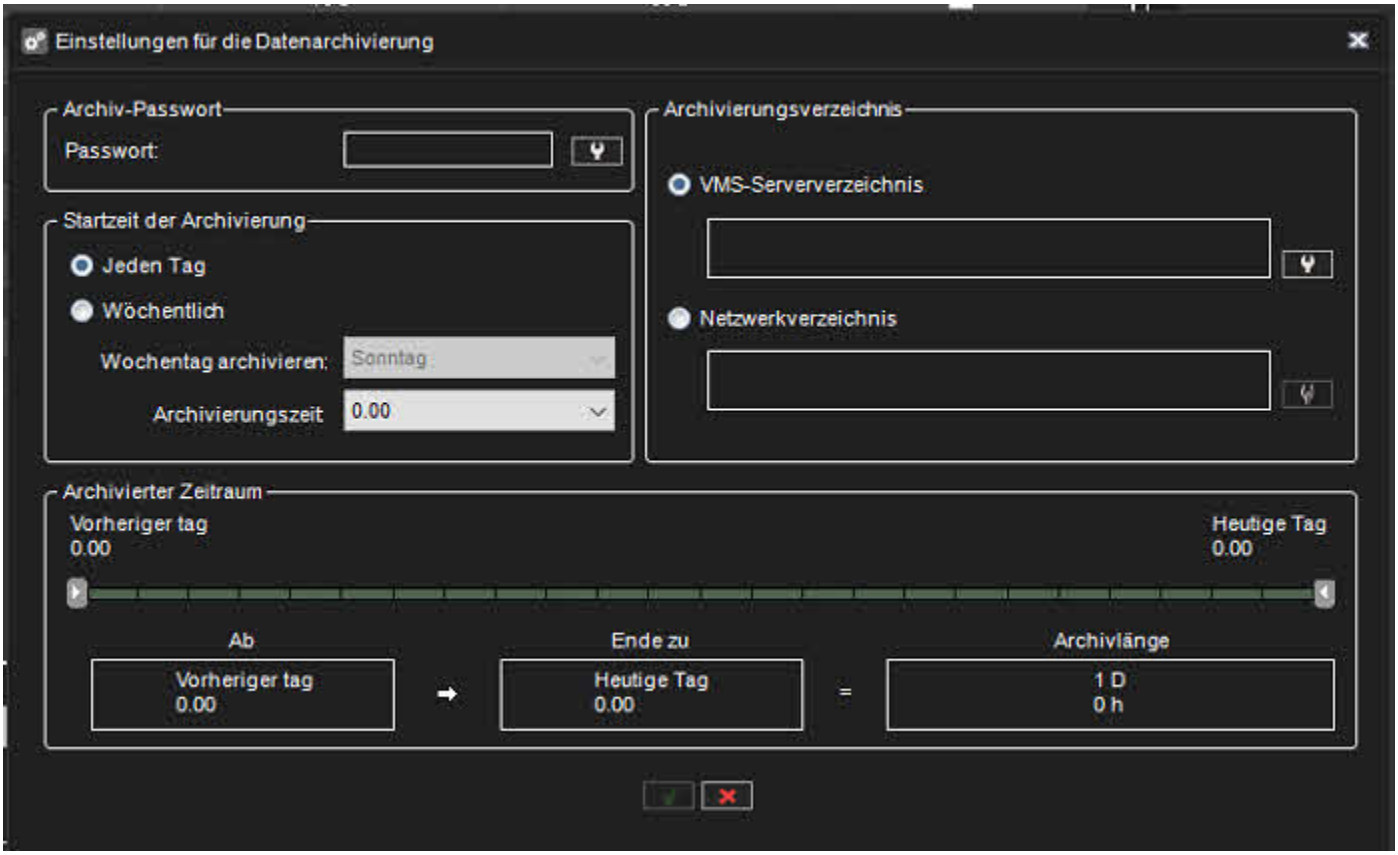


3. Klicken Sie auf **Archiveinstellungen ändern**



4. Legen Sie das Archivpasswort fest, indem Sie auf **Archivpasswort ändern** klicken
5. Wählen Sie aus, ob das Archiv täglich oder wöchentlich erstellt werden soll, indem Sie **Täglich oder Einmal pro Woche** auswählen
6. Wenn Sie die tägliche Archivierung festlegen, verwenden Sie das Dropdown-Menü **Archivierungszeit**, um die Uhrzeit auszuwählen, zu der die Archivdateien erstellt werden.

7. Wenn Sie die wöchentliche Archivierung festlegen, verwenden Sie die Dropdown-Menüs **Archivierungs-Wochentag** und **Archivierungszeit**, um das Datum und die Uhrzeit auszuwählen, an denen die Archivdateien erstellt werden.
8. Verwenden Sie den Schieberegler **Archivierter Zeitraum**, um den Zeitraum festzulegen, der in den Archivdateien verwendet wird.
9. Wählen Sie aus, ob die Archive auf einem lokalen Laufwerk (auf dem Server) oder einem Netzlaufwerk erstellt werden sollen, indem Sie das **VMS-Serververzeichnis** oder **Netzwerkverzeichnis** auswählen.
10. Klicken Sie auf die Schaltfläche **Verzeichnis** wechseln oder **Netzlaufwerk** wechseln, um das Verzeichnis zum Speichern der Archive festzulegen.
11. Klicken Sie auf **OK**, um den Archivierungszeitplan festzulegen



10.12.5 Verwenden Sie den Betriebssystem-Cache

DVMS 8. x und neuer haben die Möglichkeit, die Verwendung des Betriebssystem-Cache beim Zugriff auf die physische Festplatte zu aktivieren.

DVMS 9.4 und neuer haben die Möglichkeit, die maximale OS-Cache-Größe festzulegen.

Jede Software kann im Direktzugriffsmodus auf die Festplatte zugreifen, wenn das Betriebssystem kein Caching verwendet und den Betriebssystem-Cache verwendet.

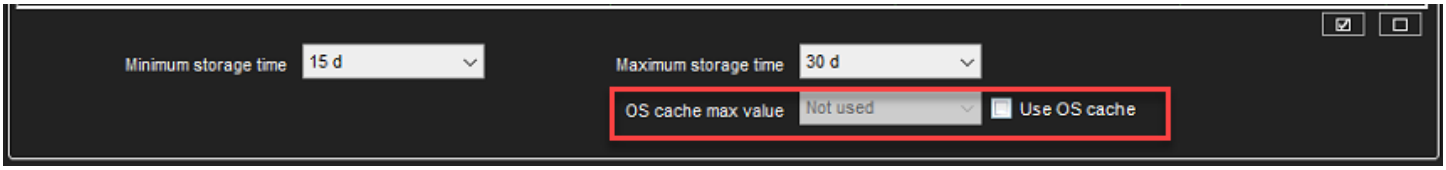
Der letzte hilft, mit instabiler Last auf der Festplatte umzugehen und die am häufigsten verwendeten Teile der Daten zwischenzuspeichern.

Windows Server- und Windows-Desktopversionen haben unterschiedliche Prioritäten für Anwendungen – Windows-Dienste priorisieren Hintergrunddienste und Desktopversionen priorisieren UI-Anwendungen.

Außerdem verwendet Windows Server mehr Systemressourcen, um z. HDD-Zugriff und kann dafür bis zu 90 % des Arbeitsspeichers verwenden.

Um Situationen zu vermeiden, in denen der gesamte RAM vom Dateisystem-Cache belegt ist, verfügt DVMS 9.4 und neuer über eine Option, um die maximale Größe des Betriebssystem-Cache zu begrenzen.

Die Einstellung für den maximalen OS-Cache ist bis zum Neustart des PCs gültig, sodass sie bei jedem Start des Rekorders festgelegt werden.

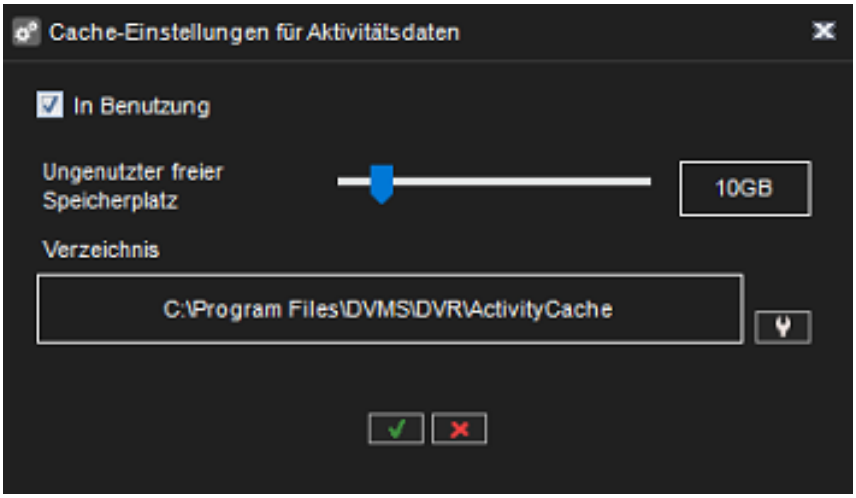


10.12.6 Aktivitätsdaten-Cache

Sie können die Einstellungen für den Aktivitätsdaten-Cache bearbeiten, indem Sie auf **Einstellungen für den Aktivitäts-Cache bearbeiten** klicken.



Im Einstellungsdialog müssen Sie zunächst das Kontrollkästchen **In Benutzung** aktivieren, um die Funktion zu aktivieren. Anschließend können Sie die Einstellungen anpassen.



Sie können die folgenden Einstellungen bearbeiten:

- **Ungenutzter freier Speicherplatz**: Legen Sie mithilfe des Schiebereglers fest, wie viel Speicherplatz frei bleiben soll (Standard: 10 GB)
- **Verzeichnis**: Wählen Sie das Verzeichnis aus, in dem die Cache-Dateien gespeichert werden sollen

Um die Änderungen zu übernehmen, klicken Sie im Dialogfeld „Cache-Einstellungen für den Aktivitätsdaten“ und in der Ansicht „Speichereinstellungen“ auf **OK**.

10.13 TEXTKANALEINSTELLUNGEN

Die Server können Textdaten von Geräten wie Kassen oder Tankstellenpumpen empfangen.

Der Treiber legt fest, welche Textdaten aufgezeichnet werden und was den Benutzern angezeigt wird. Es gibt auch benutzerdefinierte Ereignisse und Suchkriterien an.

Zusätzlich zu den in der Software enthaltenen Standard-Textdatentreibern können neue Treiber installiert werden.

In-Text-Kanaleinstellungen können Sie den Namen eines Textkanals ändern und seine Beschreibung hinzufügen oder bearbeiten.

In den **Profileinstellungen** können Sie die Benutzerrechte und die Gerätefensteroptionen für jeden Kanal und jedes Profil einstellen.

Ein zusätzliches Dokument für UniversalData-Treiber kann von unserem Extranet heruntergeladen werden oder wenden Sie sich an den Support. Dieser Treiber eröffnet endlose Möglichkeiten für die Integration in Systeme von Drittanbietern.

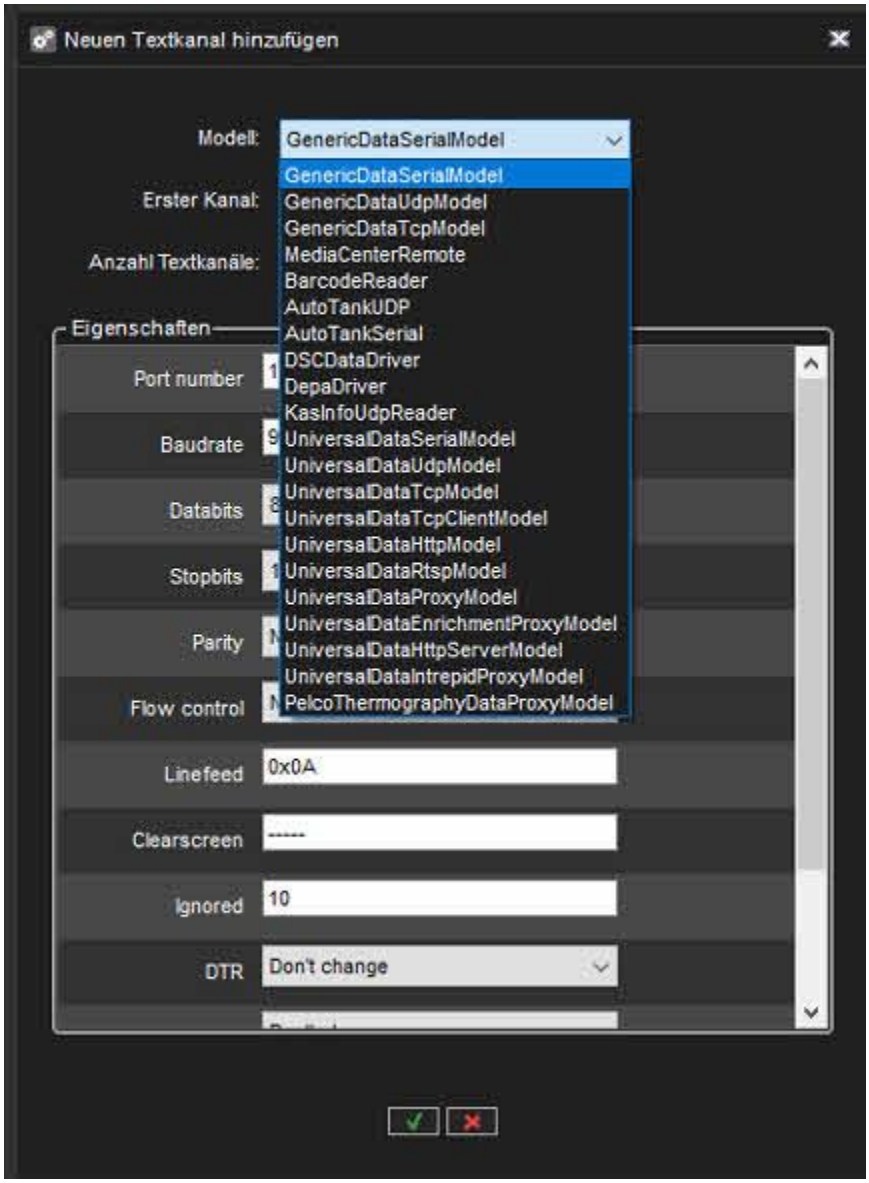
10.13.1 So fügen Sie Textdatenkanäle hinzu:

1. Klicken Sie auf Kanäle hinzufügen



in der unteren rechten Ecke des Bildschirms Textkanaleinstellungen.

2. Wählen Sie den Textdatenkanaltreiber aus dem Dropdown-Menü Model aus.



3. Verwenden Sie die **Nr. von Datenkanälen** Schieberegler, um die Anzahl der Kanäle auszuwählen, die Sie erstellen möchten.

4. Tragen Sie die treiberspezifischen Informationen in die Felder in der Liste **Eigenschaften** ein.
5. Klicken Sie auf **OK**, um die Kanäle zu speichern.

10.13.2 So bearbeiten Sie Textkanäle:

1. So bearbeiten Sie den Namen und die Beschreibung eines Textdatenkanals:
    a. Wählen Sie einen Textdatenkanal aus der Kanalliste aus.
    b. Geben Sie einen Namen für den Kanal in das Feld Name ein.
    c. Geben Sie eine allgemeine Beschreibung und eine administrative Beschreibung des Kanals in die entsprechenden Felder ein.
        i. Alle Benutzer können die allgemeine Beschreibung sehen, während nur Systemadministratoren die administrative Beschreibung sehen können.
    d. Markieren Sie das Kontrollkästchen **In use**, um den Kanal als aktiv zu setzen, oder deaktivieren Sie das Kontrollkästchen, um den Kanal als inaktiv zu setzen.
2. So bearbeiten Sie die Konfigurationseinstellung eines Textdatenkanals:
    a. Wählen Sie einen Textdatenkanal aus der Kanalliste aus.
    b. Click Modify channels



    c. Bearbeiten Sie die treiberspezifischen Informationen in den Feldern in der Liste **Eigenschaften**.
    d. Klicken Sie auf **OK**, um die Änderungen zu speichern.

Notiz: *Beim Bearbeiten der Konfigurationseinstellungen eines Textdatenkanals werden die Einstellungen für alle Textdatenkanäle geändert, die den genauen Treiber verwenden.*

10.13.3 So entfernen Sie alle Textkanäle, die denselben Treiber verwenden:

1. Wählen Sie einen Textdatenkanal aus der Kanalliste aus.
2. Klicken Sie auf Kanäle **löschen**



in der unteren rechten Ecke des Bildschirms Textkanaleinstellungen.

3. Alle Textdatenkanäle, die denselben Treiber wie der ausgewählte Textdatenkanal verwenden, werden entfernt.

Notiz: Um Textdatenkanäle zu entfernen, ohne alle Kanäle zu löschen, die den spezifischen Treiber verwenden, klicken Sie auf Ändern von Kanälen



und *geben Sie die neue Anzahl von Textdatenkanälen mit* ***Nr. von Kanälen*** *Slider.*

11 PROFILE

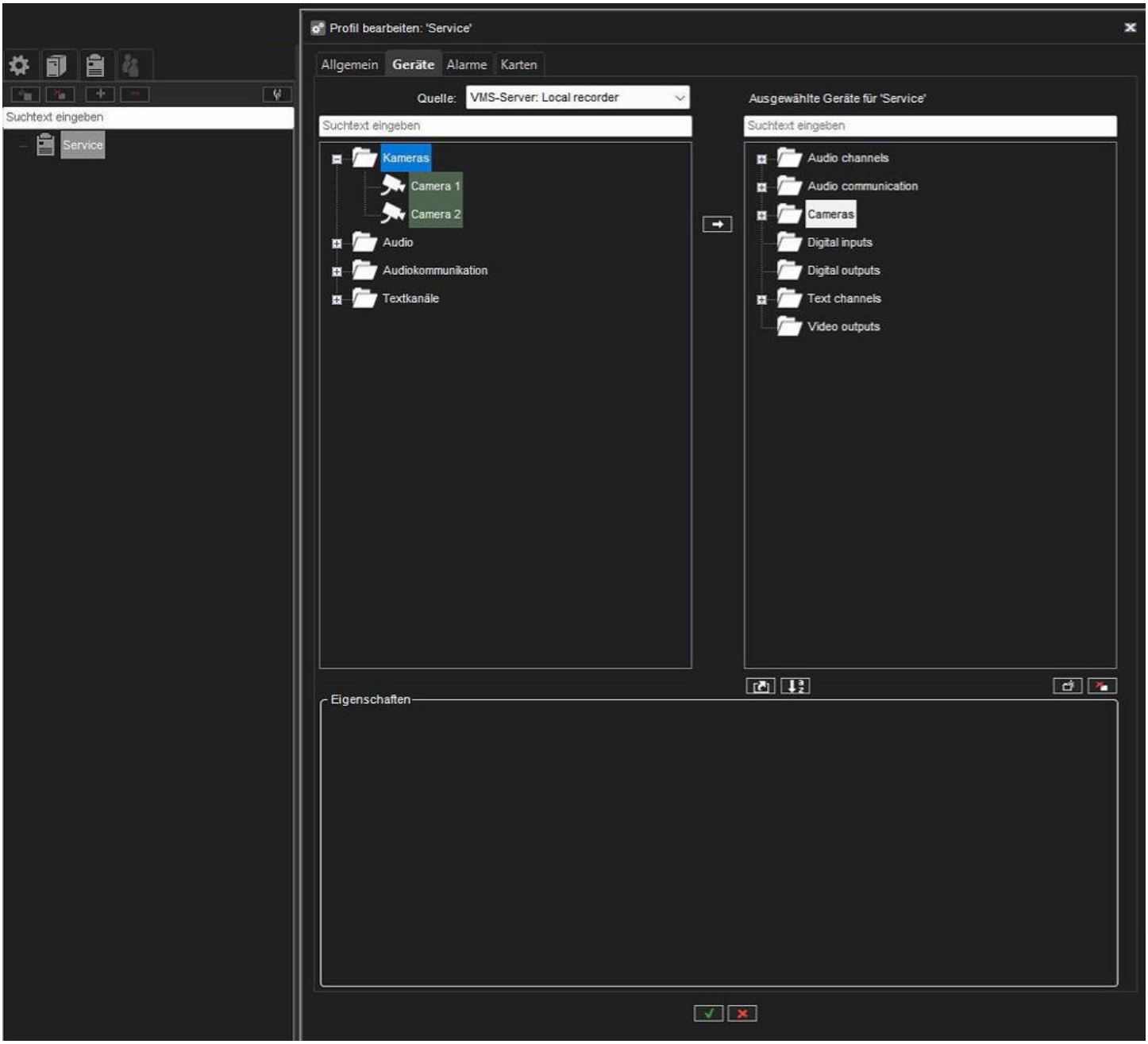
Profile definieren, auf welche VMS-Komponenten der Benutzer Zugriff hat und welche Art von Benutzerrechten der Benutzer für die Komponenten hat. Das System hat ein Standardprofil, Service. Das Standardprofil enthält die Geräte, die der Lizenzschlüssel des Hauptservers vorgibt.

Die Geräte sind nach Gerätetyp gruppiert. Beispielsweise befinden sich alle Kameras in einer Gruppe und alle Audiokanäle in einer anderen Gruppe.

Ein *profile* setzt die Rechte eines Benutzers im System. Jeder Benutzer kann 1 bis 5 Profile haben, die diese *Geräte enthalten*:

- Kameras (feste Kameras und PTZ-Kameras)
- Audiokanäle
- Audiokommunikationskanal
- Digitaleingänge (Alarmeingänge)
- Digitale Ausgänge (Steuerausgänge)
- Videoausgänge
- Textkanäle
- Alarm
- Plugin-Instanzen
- Startseiten des Webbrowsers

Um den Inhalt eines Profils zu sehen, doppelklicken Sie auf das Profil und der Inhalt wird auf dem Hauptbildschirm geladen.



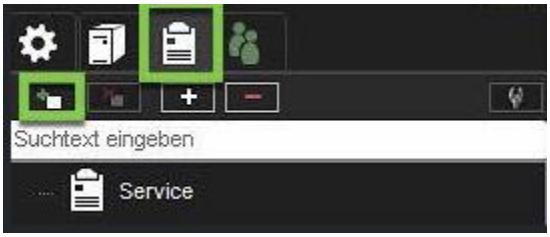
Sie können das Standardprofil als solches verwenden oder frei bearbeiten, zum Beispiel Kameras am genauen Standort gruppieren. Oder Sie können neue Profile hinzufügen. Ein Profil kann Geräte von verschiedenen Servern enthalten.

Sie können einem Profil bis zu 2.000 Gruppen und Geräte hinzufügen. Außerdem können Sie die Geräte beliebig in Gruppen einteilen.

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

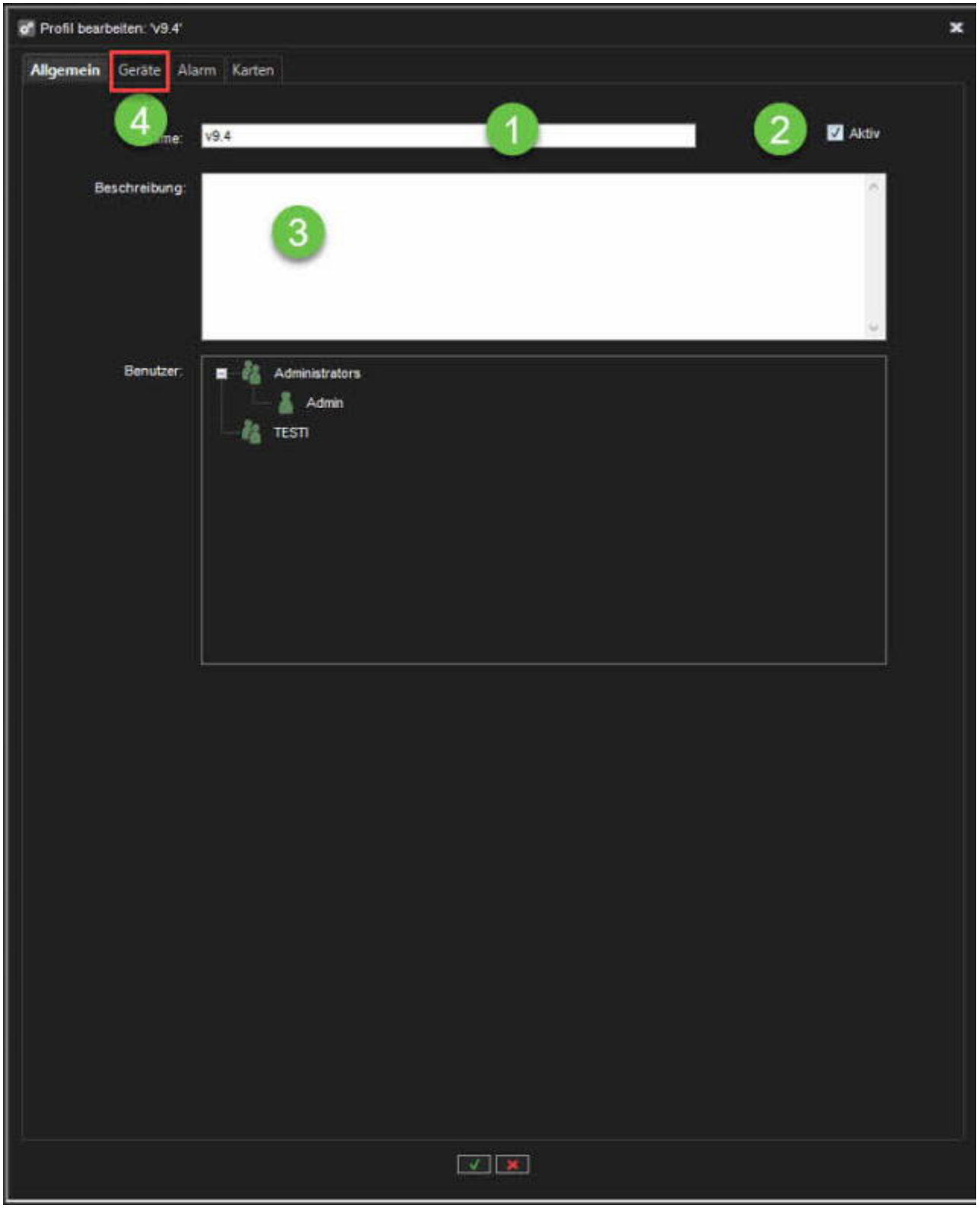
11.1 So fügen Sie ein Profil hinzu:

1. Klicken Sie auf **Profil hinzufügen**



1. Legen Sie den Namen des Profils fest
2. Profilstatus setzen: **Aktiv** oder **Deaktiviert**
3. Legen Sie die Beschreibung fest, falls erforderlich. Die Beschreibung wird nur im System Manager angezeigt
4. Öffnen Sie **Geräte**

MIRASYS



Tel +358 (0)9 2533 3300

Email info@mirasys.com

https://www.mirasys.com

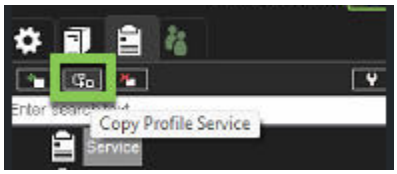
11.2 Ein bestehendes Profil duplizieren

Sie können ein bestehendes Profil in System Manager kopieren, um die Erstellung neuer Profile auf der Grundlage bestehender Profile zu erleichtern.

Das kopierte Profil enthält identische Geräte-, Alarm- und Karteneinstellungen.

Bitte beachten Sie, dass allgemeine Einstellungen wie Beschreibung und Benutzergruppen nicht übernommen werden.
Das neue Profil ist standardmäßig aktiv und kann bearbeitet und gelöscht werden.
Nur Systemadministratoren mit der Fähigkeit „Profil hinzufügen können“ in der Systemmanagerrolle können das Profil kopieren.

1. Wählen Sie ein Profil in System Manager > Profile.
2. Klicken Sie auf die Schaltfläche „Profil kopieren“, die sich zwischen „Profil hinzufügen“ und „Profil entfernen“ befindet.



Bitte beachten Sie, dass diese Schaltfläche nur aktiv ist, wenn ein Profil ausgewählt ist.

3. Wenn Sie auf „Profil kopieren“ klicken, wird ein neues Profil erstellt, dessen Geräte-, Alarm- und Karteneinstellungen mit denen des kopierten Profils identisch sind.



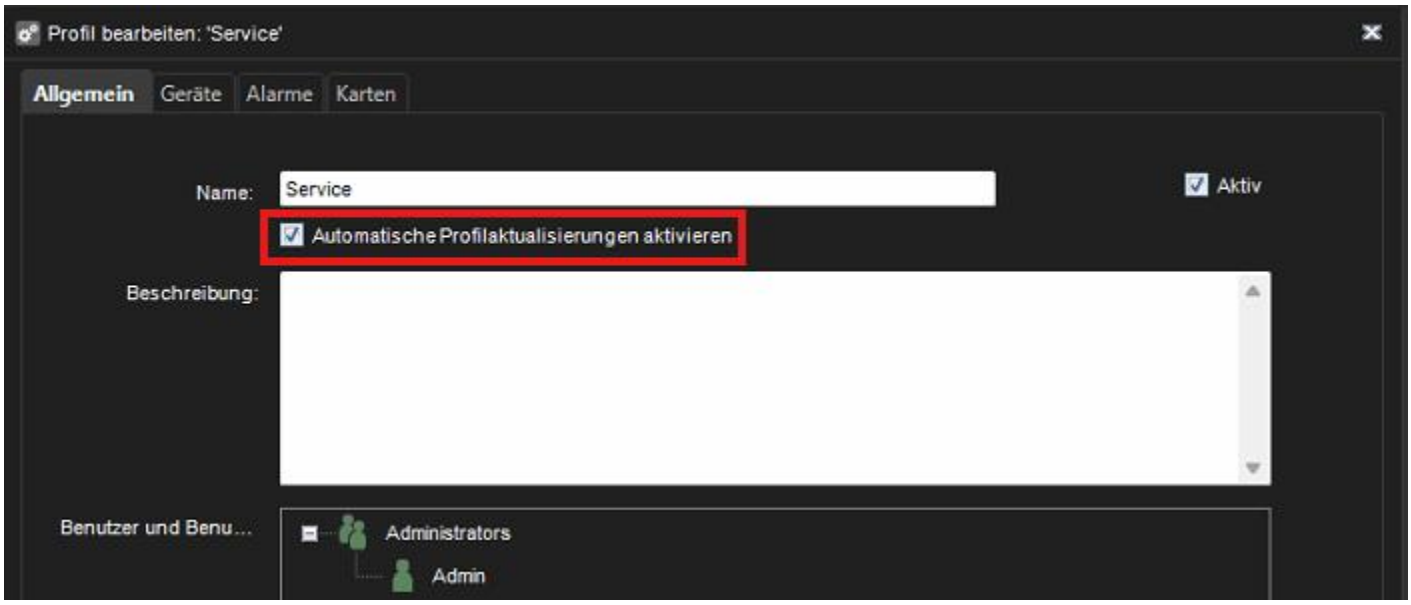
Die neue Profilkopie steht unter dem kopierten Profil mit einer Nummer hinter dem Namen: Wenn der Profilname „Service“ lautet, wird die Kopie „Service 1“ sein. Wenn es bereits ein Profil „Service 1“ gibt, heißt es „Service 2“ usw.

4. In den allgemeinen Einstellungen kann der Name bearbeitet werden, das Profil kann aktiviert oder deaktiviert werden und eine Beschreibung kann hinzugefügt werden. Die neue Profilkopie ist standardmäßig aktiv.
5. Klicken Sie auf ✓ zum Speichern. Das Profil ist nun in SM > Benutzergruppen sichtbar und kann zu Benutzergruppen hinzugefügt werden.

11.3 AUTOMATISCHE PROFILAKTUALISIERUNGEN

11.3.1 Automatische Profilaktualisierungen aktivieren

Auf der Registerkarte **Allgemein** eines Profils befindet sich die Option **Automatische Profilaktualisierungen aktivieren**. Diese Einstellung ist standardmäßig aktiviert.



Im Folgenden wird das Verhalten der Einstellung im aktivierten bzw. deaktivierten Zustand beschrieben.

11.3.2 Automatische Profilaktualisierungen aktiviert

Das heißt, das Kontrollkästchen der Einstellung ist angekreuzt.

Profilknoten werden automatisch aus dem Profil entfernt, wenn das verknüpfte Gerät entfernt wird.

11.3.3 Automatische Profilaktualisierungen deaktiviert

Das heißt, das Kontrollkästchen für diese Einstellung ist nicht aktiviert.

Wenn ein Systemadministrator die Einstellung deaktiviert und das Profil somit „sperrt“, werden nur manuelle Änderungen in den Profileinstellungen des System Managers übernommen.

Profilknoten werden nicht automatisch entfernt, wenn verknüpfte Geräte entfernt werden, und Profile können defekte Verknüpfungen zu Geräten enthalten.

Profilknoten können nur manuell in den Profileinstellungen des System-Managers oder, im Falle von Alarmen, in den Alarmeinstellungen hinzugefügt oder entfernt werden.

11.3.3.1 Beschädigte Profilknoten

Alle Anwendungen funktionieren unabhängig von beschädigten Profilknoten einwandfrei. Auch das Sichern und Wiederherstellen des Systems funktioniert normal.

Beschädigte Profilknoten sind für Benutzer nicht zugänglich und werden in keiner Anwendung – mit Ausnahme der Profileinstellungen des System Managers – im Profilbaum angezeigt. Obwohl die Knoten nicht angezeigt werden, bleiben sie in den Systemdaten erhalten.

In den Profileinstellungen des System Managers werden folgende Informationen zu beschädigten Verknüpfungen angezeigt:

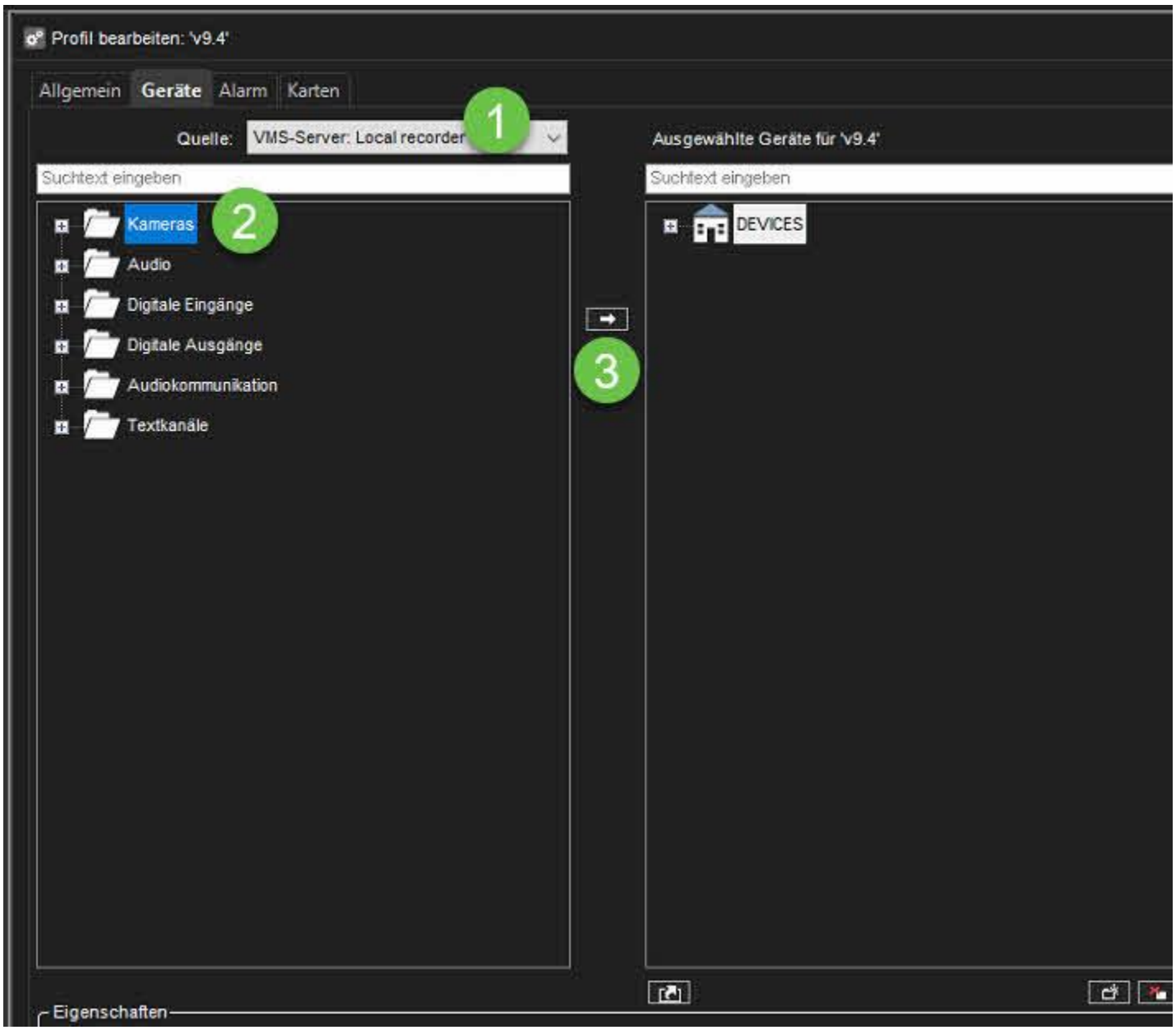
- Name und Adresse des Aufzeichnungsgeräts
- Gerätename
- Hinweis, dass die Verbindung zum Gerät unterbrochen ist

Wenn ein verbundenes Gerät erneut hinzugefügt wird, wird die Verbindung zwischen dem Profilknoten und dem Gerät wiederhergestellt. Alle Clients erhalten wieder Zugriff auf den Profilknoten und das Gerät.

11.4 Geräteprofil-Einstellungen

11.4.1 Geräte

1. Wählen Sie aus der Dropdown-Liste Quelle **VMS-Server oder ein anderes Profil** aus
2. Wählen Sie die benötigten Komponenten oder Gerätegruppen aus dem linken Feld aus
3. Klicken Sie auf **Hinzufügen**
4. Um die Eigenschaften ausgewählter Komponenten zu ändern, gehen Sie bitte zu **Ausgewählte Geräte**

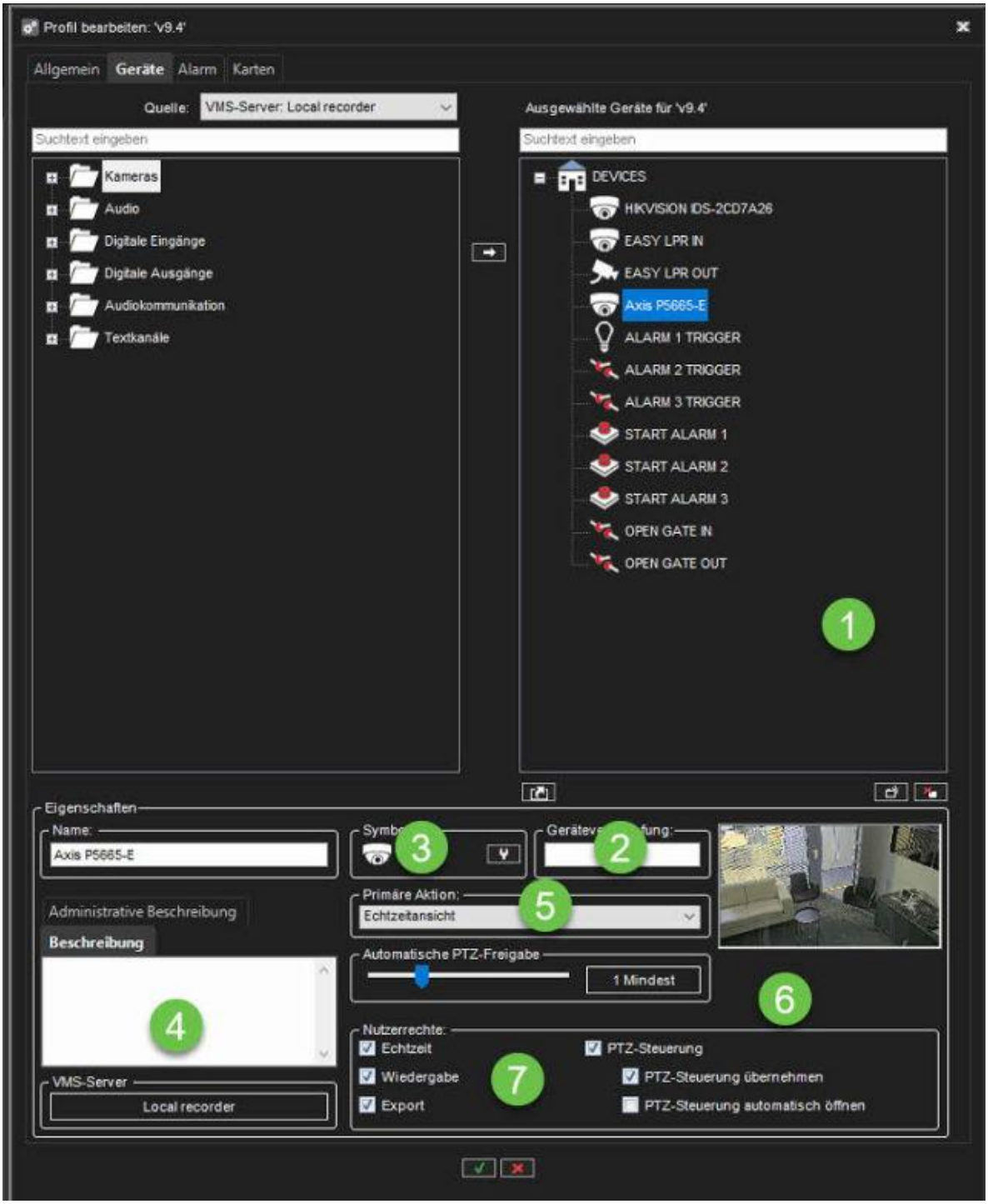


11.4.2 Ausgewählte Geräteeigenschaften

1. Komponente aus der Liste des ausgewählten Geräts auswählen
2. Legen Sie **Geräteverknüpfung** fest
3. Ändern Sie das Gerätesymbol, indem Sie auf **Symbol ändern** klicken
4. Legen Sie **Beschreibung und Administrative Beschreibung fest, falls erforderlich**

5. Wählen Sie die **Primäre Aktion**, wählen Sie die Aktion aus, die ausgeführt wird, wenn ein Benutzer in Spotter auf das Gerät doppelklickt.
6. Set **Automatische PTZ-Auslösung** (nur für die PTZ-Kameras)
7. Legen Sie Benutzerrechte für die Komponente fest
    a. **Echtzeit**
    b. **Wiedergabe**
    c. **Export**
    d. **PTZ-Steuerung** (nur für die PTZ-Kameras)
        i. **PTZ-Steuerung übernehmen**
        ii. **PTZ-Steuerung automatisch öffnen**
8. Klicken Sie auf **OK**, um die Profilerstellung abzuschließen

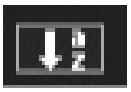
MIRASYS



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

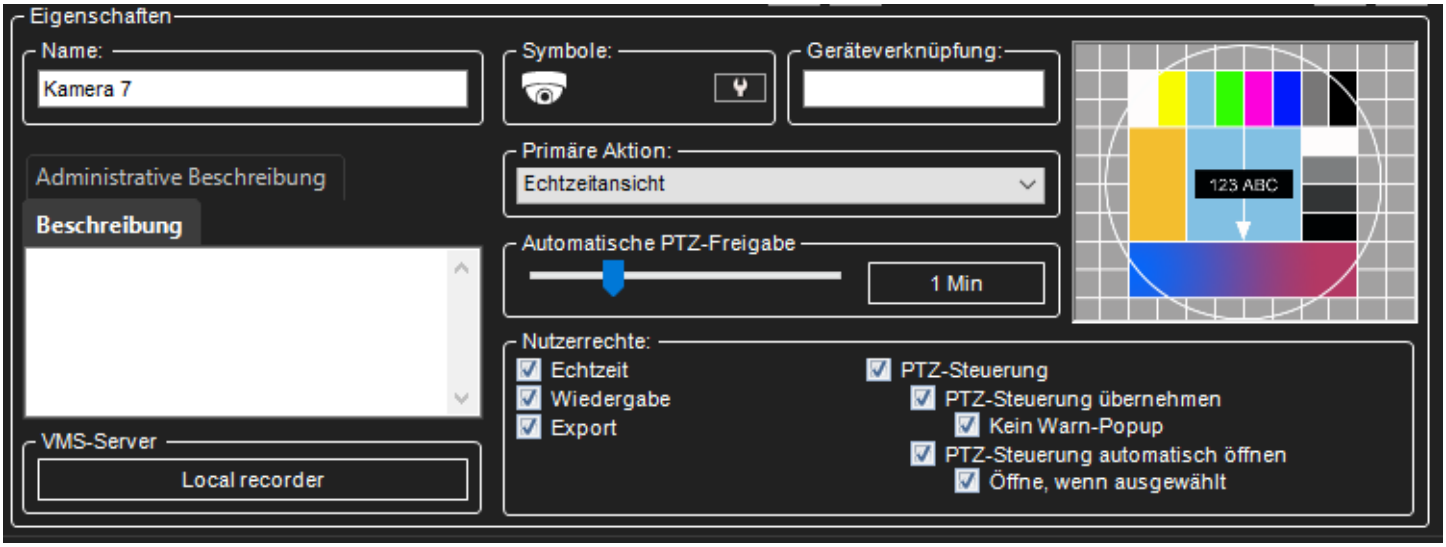
11.4.3 Ausgewählte Gerätenodes sortieren

Die alphanumerische Sortierung (a -> z) der ausgewählten Ordnerprofilknoten wird durch Drücken der Sortiertaste ausgeführt, durch erneutes Drücken wird die umgekehrte Sortierung (z -> a) ausgeführt.



11.4.4 PTZ-Kamerasteuerungsprofil-Einstellungen

In den System-Manager-Kameraprofileinstellungen in den Benutzerrechten der Dome-Kamera wurde die Option **Öffnen, wenn ausgewählt** hinzugefügt.

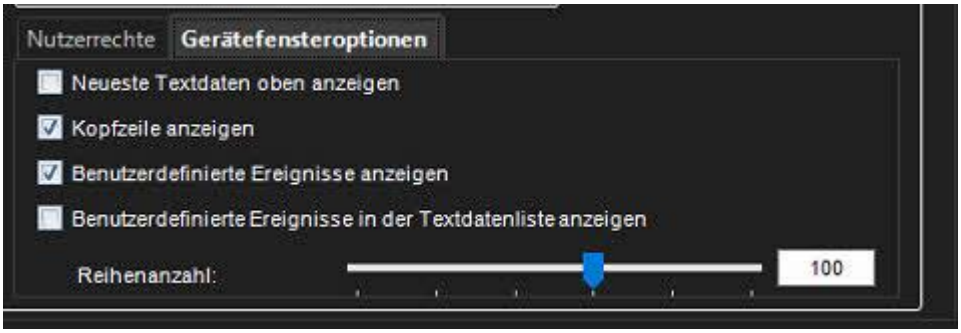


Wenn Öffnen bei Auswahl ausgewählt ist, wird die Steuerung der Dome-Kamera automatisch aktiviert, wenn die Dome-Kameraansicht im Spotter ausgewählt wird.

11.4.5 PTZ-Steuerung

- Automatische Dome-Freigabe
    - Werte: 1 min, 2 min, 3 min, 4 min, 5 min, 10 min, 15 min, 30 min, 45 min, 1 h, 2 h, 4 h, 8 h, 12 h, 1 d
- PTZ-Steuerung übernehmen
    - Kein Warnungs-Popup
- PTZ-Steuerung automatisch öffnen
    - Öffne, wenn ausgewählt

11.4.6 Optionen des Gerätefensters für Textkanäle



In den Gerätefensteroptionen können Sie auswählen, wie Benutzern Textdaten angezeigt werden. Diese Optionen sind verfügbar:

11.4.7 Zeigen Sie die neuesten Textdaten oben an.

Standardmäßig werden die neuesten Textdaten am Ende der Textdatenliste hinzugefügt. Wählen Sie diese Option, um stattdessen die neuesten Textdaten oben in der Textdatenliste anzuzeigen.

11.4.8 Kopfzeile anzeigen

Wählen Sie diese Option, um die vom Textdatenerfassungstreiber angegebenen Identifikationsdaten anzuzeigen.

11.4.9 Benutzerdefinierte Ereignisse anzeigen

Wählen Sie diese Option aus, um vom Textdatenerfassungstreiber festgelegte benutzerdefinierte Ereignisse anzuzeigen.

11.4.10 Benutzerdefinierte Ereignisse in der Textdatenliste anzeigen

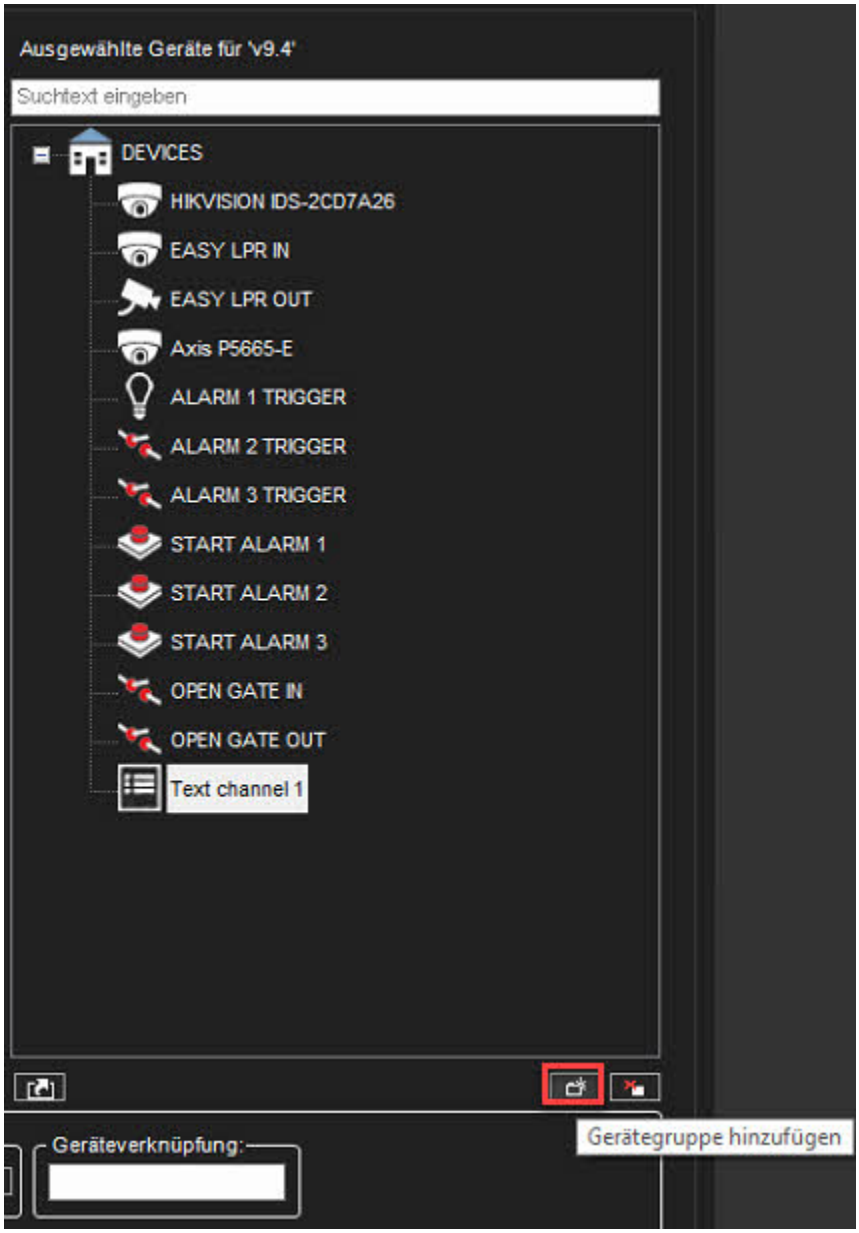
Wählen Sie diese Option, um benutzerdefinierte Ereignisse in der Textdatenliste (anstelle der benutzerdefinierten Ereignisliste) anzuzeigen.

11.4.11 Die Anzahl der Zeilen

Geben Sie die Anzahl der Zeilen an, die höchstens in der Textdatenliste angezeigt werden.

11.4.12 Hinzufügen von Gerätegruppen zur Liste des ausgewählten Geräts

1. Klicken Sie unter dem Bereich **Ausgewählte Geräte** auf **Gerätegruppe hinzufügen**. Eine neue Gerätegruppe wird angezeigt.

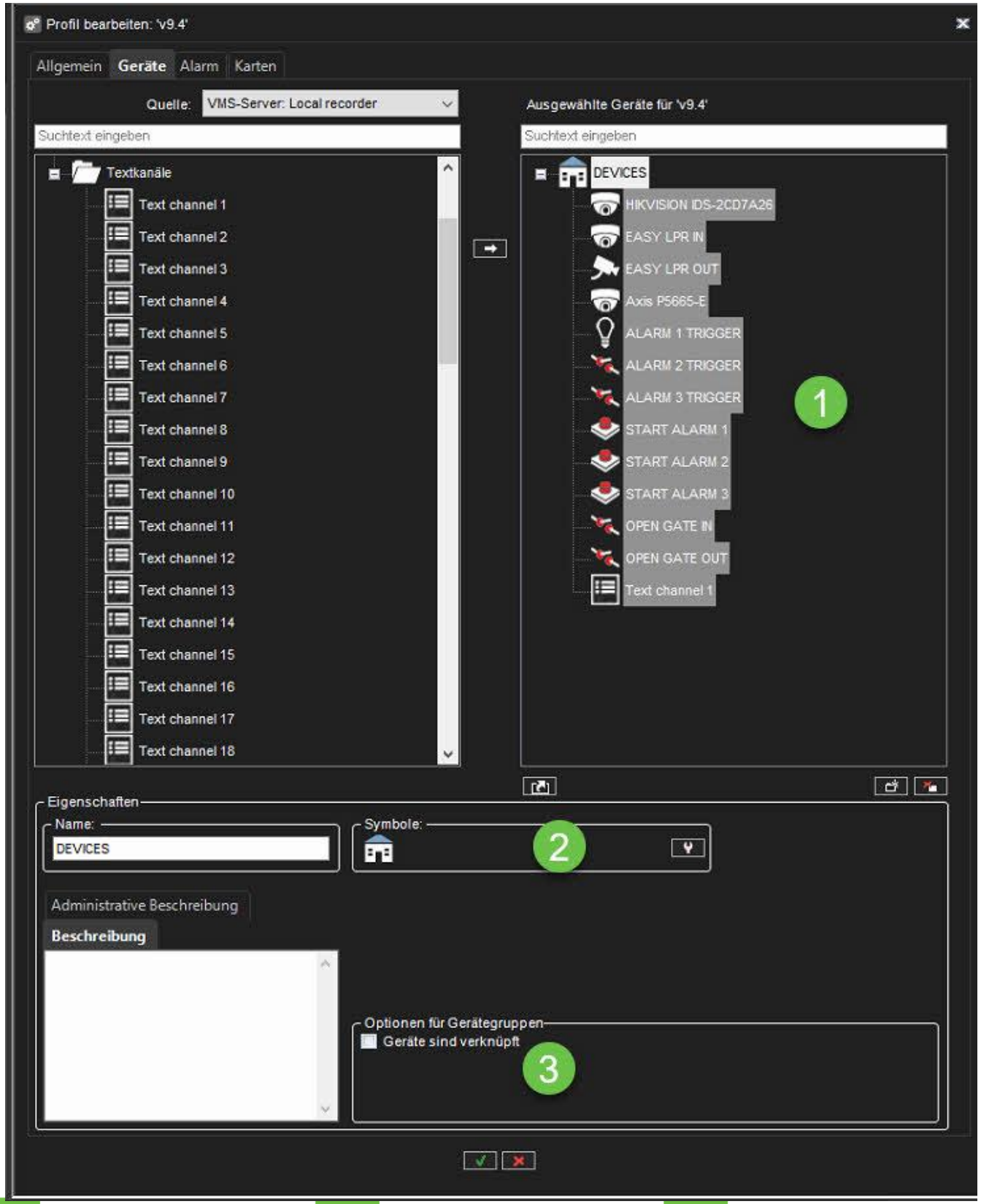


Notiz: Eine neue Gerätegruppe wird immer unter der ausgewählten Gerätegruppe hinzugefügt. Um eine Gerätegruppe zur obersten Ebene hinzuzufügen, stellen Sie sicher, dass keine der vorhandenen Gerätegruppen ausgewählt ist

1. Klicken Sie auf die Gerätegruppe und geben Sie einen Namen dafür ein
2. Um das für die Gerätegruppe verwendete Symbol zu ändern, klicken Sie auf **Symbol ändern** . Wählen Sie dann das Symbol aus, das Sie verwenden möchten.
3. Geben Sie eine Beschreibung der Gerätegruppe in **Beschreibung** ein.

4. Legen Sie bei Bedarf Gerätegruppenoptionen fest (**Geräte sind verknüpft,** um automatisch alle Geräteansichten derselben Gruppe zu öffnen, wenn der Benutzer eine der Geräteansichten öffnet).

MIRASYS



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

11.4.13 Alphabetisch sortieren

Sortierregeln:

- in den Ordner oder die Stammverzeichnisebene, in dem/der sich die aktuell ausgewählte Komponente befindet (jedoch nicht in Unterordner)
- in die ausgewählten Ordner (jedoch nicht in Unterordner)
- wenn kein Profilknoten ausgewählt ist, werden Stammknoten sortiert (jedoch keine Unterordner)
- wenn mehrere Ordner derselben Ebene ausgewählt sind, werden alle ausgewählten Ordner sortiert (jedoch keine Unterordner)

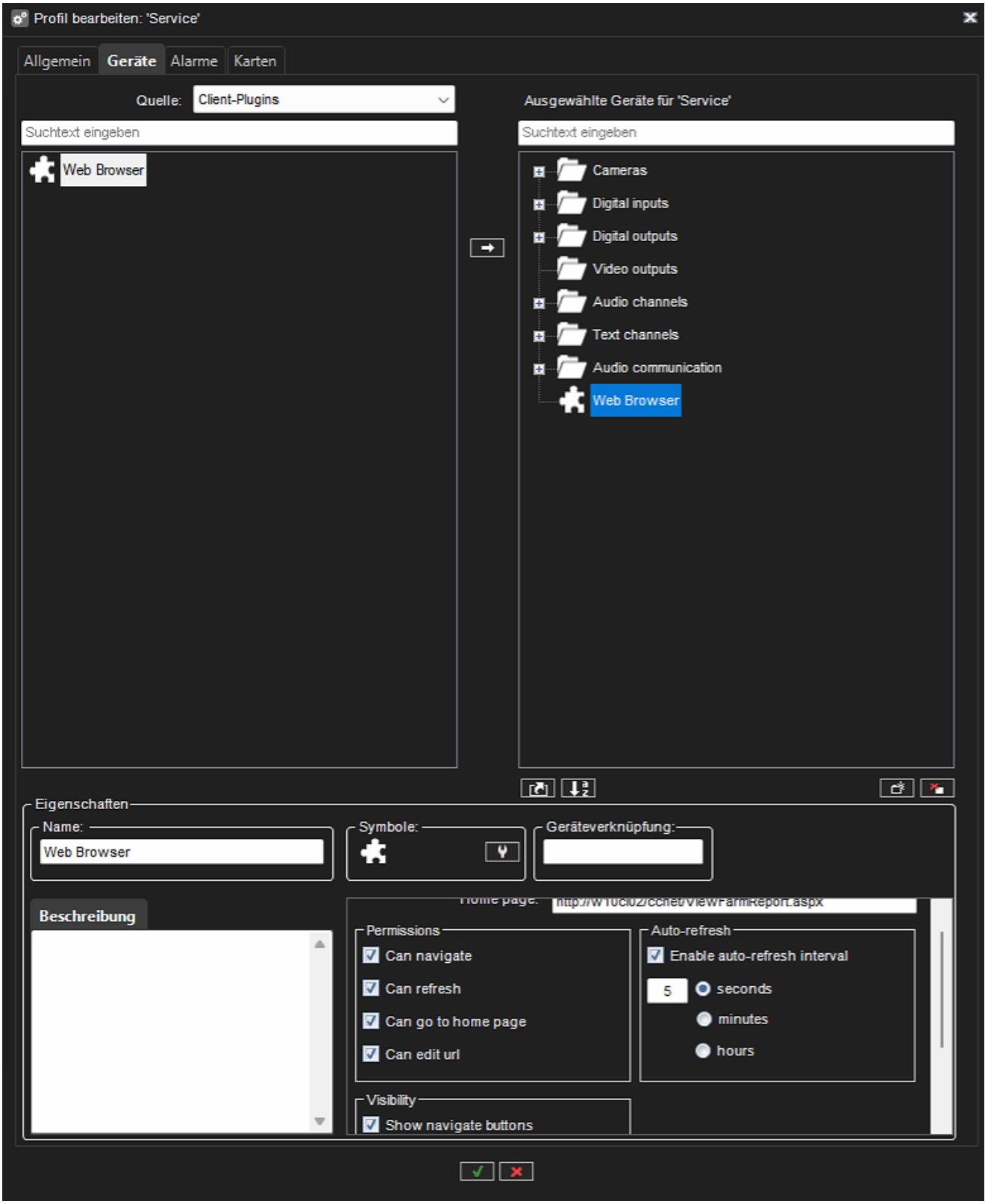
11.4.14 Client-Plugins

11.4.14.1 Webbrowser-Plugin

Der Webbrowser wird unter Systemmanager > Profile > Profil auswählen und öffnen > Geräte konfiguriert.

1. Um Webseiten als Kanäle hinzuzufügen, ändern Sie die Quelle in Client-Plugins. Wählen Sie das Webbrowser-Plugin und fügen Sie es zu Geräte hinzu.
2. Wählen Sie den Webbrowser aus und fügen Sie den Namen und ggf. eine Beschreibung hinzu und ändern Sie das Symbol, falls gewünscht.
3. Fügen Sie unter Startseite die Adresse der Webseite hinzu.
4. Legen Sie die Berechtigungen fest:
    - Kann navigieren
    - Kann aktualisieren
    - Kann zur Startseite wechseln
    - Kann URL bearbeiten
5. Sie können ein automatisches Aktualisierungsintervall aktivieren und das Intervall entweder in Sekunden, Minuten oder Stunden festlegen.
6. Klicken Sie auf ✓ zum Speichern.

MIRASYS



Tel +358 (0)9 2533 3300

Email info@mirasys.com

https://www.mirasys.com

11.4.14.2 VLC Player-Plugin

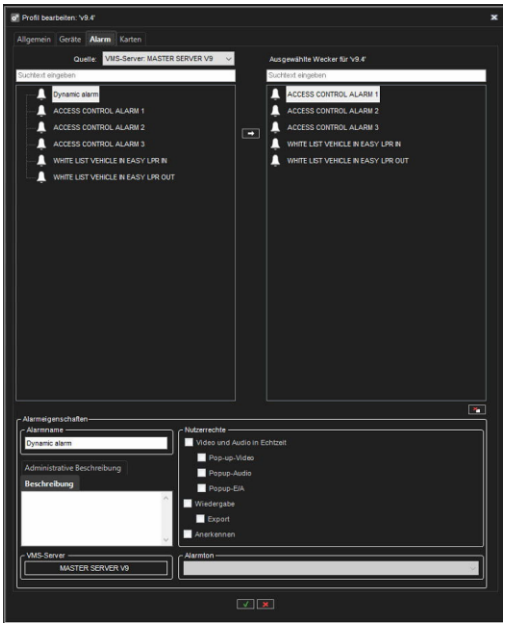
Die Konfiguration des VLC-Players erfolgt im Systemmanager > Profile > Profil auswählen und öffnen > Geräte.

So konfigurieren Sie das VLC Player-Plugin:

1. Klicken Sie in den Profileinstellungen auf die Registerkarte Geräte.
2. Wählen Sie Client-Plugins aus dem Dropdown-Menü Service.
3. Wählen Sie VLC Player.
4. Klicken Sie auf den nach rechts zeigenden Pfeil ➡️ , um den VLC Player zur Profilstruktur hinzuzufügen.
5. Benennen Sie die Player-Instanz unter Eigenschaften.
6. Fügen Sie bei Bedarf eine Beschreibung hinzu.
7. Wählen Sie bei Bedarf unter Icons ein Symbol für den Player aus.
8. Fügen Sie bei Bedarf eine Geräteverknüpfung hinzu.
9. Geben Sie die URL des VLC Players ein, den Sie abspielen möchten.
10. Aktivieren Sie das Kontrollkästchen URL anzeigen, wenn Sie die URL in Spotter anzeigen lassen möchten.
11. Aktivieren Sie das Kontrollkästchen Automatisch abspielen, wenn Sie möchten, dass der VLC Player die URL abspielt, wenn er in Spotter geöffnet wird.
12. Klicken Sie auf ✓ zum Speichern.

11.5 ALARME – PROFILEINSTELLUNGEN

11.5.1 Bearbeiten profilspezifischer Alarmeinstellungen



Auf der Registerkarte **Alarme** können Sie die Alarme auswählen, die Sie in ein Profil aufnehmen möchten, und die profilspezifischen Benutzerrechte der Alarme bearbeiten.

Der Auslösertyp für Alarmauslöser, die vom Systemadministrator für ONVIF-Profil M-konforme Geräte erstellt werden, und für die Alarmauslösungs-Web-API ist Extern.

11.5.2 So fügen Sie Alarme zu einem Profil hinzu:

1. Öffnen Sie die Registerkarte **Alarme**.
2. Wählen Sie einen Server aus dem Dropdown-Menü **Quelle** aus. Die verfügbaren Alarme werden im linken Bereich angezeigt.
3. Wählen Sie den Alarm oder die Alarme aus, die Sie hinzufügen möchten, und klicken Sie dann auf den Rechtspfeil. Sie können Alarme auch aus dem linken Bereich nach rechts ziehen.
4. Speichern Sie das Profil, indem Sie auf **OK** klicken.

Notiz: *Sie können Alarme auch über den Bildschirm zum Erstellen/Bearbeiten von Alarmen zu Profilen hinzufügen.*

11.5.3 So bearbeiten Sie profilspezifische Alarmbenutzerrechte:

1. Öffnen Sie die Registerkarte **Alarme**.
2. Klicken Sie im Bereich **Ausgewählte Alarme** auf einen Alarm.

3. Stellen Sie die Benutzerrechte für jeden Alarm ein. Die Einstellungen der Benutzerrechte befinden sich unten rechts auf der Registerkarte **Alarme**.
    a. Sie können individuelle Rechte für jeden Alarm festlegen oder mehrere Alarme auswählen (indem Sie die Umschalt- oder Steuerungstaste gedrückt halten, während Sie Alarme auswählen) und die gleichen Optionen für mehrere Alarme festlegen.
4. Damit der Computer bei einem Alarm einen Ton abspielt, wählen Sie **Alarmton** und dann den wiedergegebenen Ton. Um die Sounds zu testen, wählen Sie den Sound aus der Liste aus und klicken Sie auf **Play**.
5. Speichern Sie die Einstellungen durch Klicken auf **OK**.

Die Benutzerrechte umfassen:

- **Echtzeit-Video und -Audio**. Wählen Sie diese Option, damit die Benutzer Alarmvideos oder -audios in Echtzeit sehen können.
- **Pop-up video**. Wählen Sie diese Option aus, damit Benutzer automatisch Alarmvideos erhalten.
- **Pop-up audio**. Wählen Sie diese Option aus, damit Benutzer automatisch Alarmtöne erhalten.
- **Wiedergabe** Wählen Sie diese Option, um das Alarmvideo des Benutzers abzuspielen.
- **Export** Wählen Sie diese Option, damit die Benutzer Alarmvideos auf lokalen Medien speichern können.
- **Anerkennen** Wählen Sie diese Option, damit die Benutzer Alarme bestätigen können.

11.5.3.1 Einen Alarm aus einem Profil löschen

1. Öffnen Sie die Registerkarte **Alarme**.
2. Klicken Sie im Bereich Ausgewählte Alarme auf einen Alarm.
3. Klicken Sie auf **Alarm löschen**.



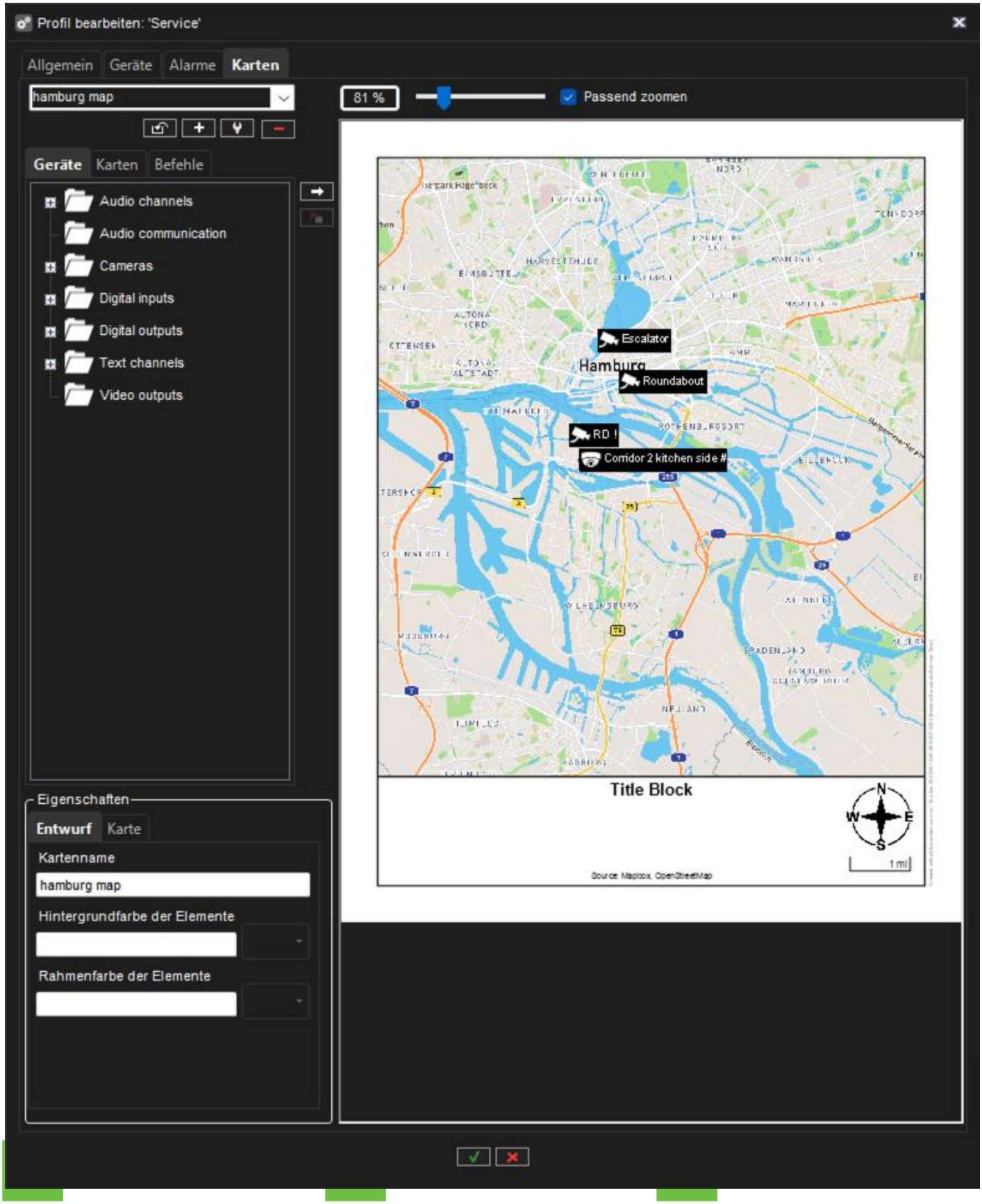
Wenn einem Alarm ein Auslöser oder keine Aktionen zugeordnet sind, bleibt er zwar auf der Registerkarte „Alarme“ des Profils sichtbar, erscheint jedoch nicht mehr in den Alarmeinstellungen des Rekorders. Durch das Ändern der Alarmeinstellungen wird deren Konfiguration, einschließlich der Profile, gelöscht.

11.6 KARTENPROFIL-EINSTELLUNGEN

Derzeit unterstützen wir beim Hinzufügen einer Karte die folgenden Formate:

- JPG / JPEG (Joint Photographic Experts Group)
- BMP (Bitmap)
- PDF (Portable Document Format)
- SVG (Skalierbare Vektorgrafik)
- PNG (Tragbare Netzwerkgrafiken)

MIRASYS


Profil bearbeiten: 'Service'
Allgemein
Geräte
Alarme
Karten
hamburg map
81 %
Passend zoomen
Geräte
Karten
Befehle
Audio channels
Audio communication
Cameras
Digital inputs
Digital outputs
Text channels
Video outputs
Escalator
Hamburg
Roundabout
RD !
Corridor 2 kitchen side #
Title Block
N
W
E
S
1 mi
Source: Mapbox, OpenStreetMap
Eigenschaften
Entwurf
Karte
Kartenname
hamburg map
Hintergrundfarbe der Elemente
Rahmenfarbe der Elemente

11.6.1 Hinzufügen von Karten zu Profilen

11.6.1.1 So fügen Sie eine Karte hinzu:

1. Klicken Sie auf die Schaltfläche **Level ändern** und wählen Sie dann die Gerätegruppe aus, der Sie eine Karte hinzufügen möchten. Die Geräte, die zur ausgewählten Gruppe gehören, werden im linken Bereich angezeigt.
    a. Untergruppen werden ebenfalls angezeigt. Sie können auch auf die Untergruppensymbole im linken Bereich doppelklicken, um zu einer niedrigeren Ebene zu wechseln.
2. Klicken Sie auf **Karte hinzufügen** und suchen Sie das Bild, das Sie als Karte verwenden möchten.
3. Standardmäßig ist die Option Anpassen über der Karte aktiviert. Sie können die Option Anpassen durch Zoomen auch deaktivieren und den Zoom mit dem Schieberegler über der Karte manuell anpassen.
4. Wählen Sie im linken Bereich die Geräte und Gerätegruppen aus, die Sie der Karte hinzufügen möchten, und klicken Sie auf den Pfeil **Zur Karte hinzufügen**.
    a. Elemente, die sich bereits auf der Karte befinden, werden im linken Bereich abgeblendet angezeigt. Wenn Sie der Karte Untergruppensymbole hinzufügen, fungieren die Symbole als Links zu den Untergruppenkarten.
    b. Benutzer können zu einer Karte einer niedrigeren Ebene wechseln, indem sie auf das Untergruppensymbol doppelklicken.

Hinweis Um mehr als ein Gerät gleichzeitig auszuwählen, halten Sie die SHIFT- oder CTRL-Taste gedrückt.

1. Wählen Sie ein Gerät oder eine Gerätegruppe aus der Karte aus und dann können Sie unter **Geräteeigenschaften** diese Optionen festlegen:
2. Bei Kameras können Sie die Richtung auswählen, in die das Kamerasymbol zeigt.
3. Standardmäßig wird das Namensschild jedes Geräts auf der Karte angezeigt. Deaktivieren Sie das Kontrollkästchen **Label**, um ein Durcheinander der Etiketten zu vermeiden. Der Name wird stattdessen als Popup-Label angezeigt.
4. Wenn Sie mehrere Gerätesymbole auf engstem Raum unterbringen müssen, können Sie Ortsmarken verwenden.
5. Aktivieren Sie das Kontrollkästchen **Ortsmarke**. Auf der Karte werden eine Ortsmarke (x) und eine Verbindungslinie angezeigt. Ziehen Sie die Ortsmarke (x) an die richtige Position des Geräts.
6. Ziehen Sie dann das Symbol an eine geeignete Position auf der Karte.

11.6.1.2 So entfernen Sie eine Sitemap

- Zeigen Sie die Karte an, die Sie entfernen möchten, und klicken Sie auf **Karte entfernen**

11.6.1.3 So entfernen Sie ein Symbol von der Karte

- Wählen Sie das Symbol aus und klicken Sie auf **Entfernen**

12 Benutzer

Alle Benutzer gehören einer Benutzergruppe (siehe unten) an, über die ihre Nutzungsrechte definiert und verwaltet werden.

Der Administrator kann neue Benutzergruppen hinzufügen, unterschiedliche Nutzungsrechte für die Gruppen festlegen und Benutzer hinzufügen.

Das System unterstützt die Integration von Benutzerrechten auf Domänenebene (LDAP), wodurch Benutzer aus Domänengruppen synchronisiert werden können.

Jede Benutzergruppe muss über mindestens ein Profil verfügen, das die Geräte der Benutzergruppe im System festlegt.

Eine Benutzergruppe kann höchstens fünf Profile haben.

Ein Benutzername und ein Passwort schützen alle Benutzerkonten.

12.1 Benutzer abmelden

Wenn Sie über Administratorrechte verfügen, können Sie einen Benutzer vom Spotter-Programm abmelden.

12.2 So melden Sie einen Benutzer ab:

Klicken Sie mit der rechten Maustaste auf den Benutzernamen auf der Registerkarte Benutzer und klicken Sie auf **Benutzer abmelden.**

HINWEIS: Bitte ändern Sie immer das Admin-Benutzerkennwort, nachdem Sie die Installation abgeschlossen haben.
Sie sollten niemals Standardpasswörter im Mirasys VMS-System belassen.

12.3 Benutzer überwachen

Die Registerkarte **Benutzer** zeigt an, ob Benutzer am System angemeldet sind:

Symbol	Beschreibung
	(Grün). Der Benutzer ist angemeldet. Klicken Sie auf das Pluszeichen (+), um den Namen des Programms anzuzeigen, bei dem der Benutzer angemeldet ist, und die IP-Adresse des Computers des Benutzers. Zusätzlich werden Datum und Uhrzeit der Anmeldung angezeigt.
	(Rot). Der Benutzer ist nicht angemeldet.
	(Grau) Das Benutzerkonto ist deaktiviert.

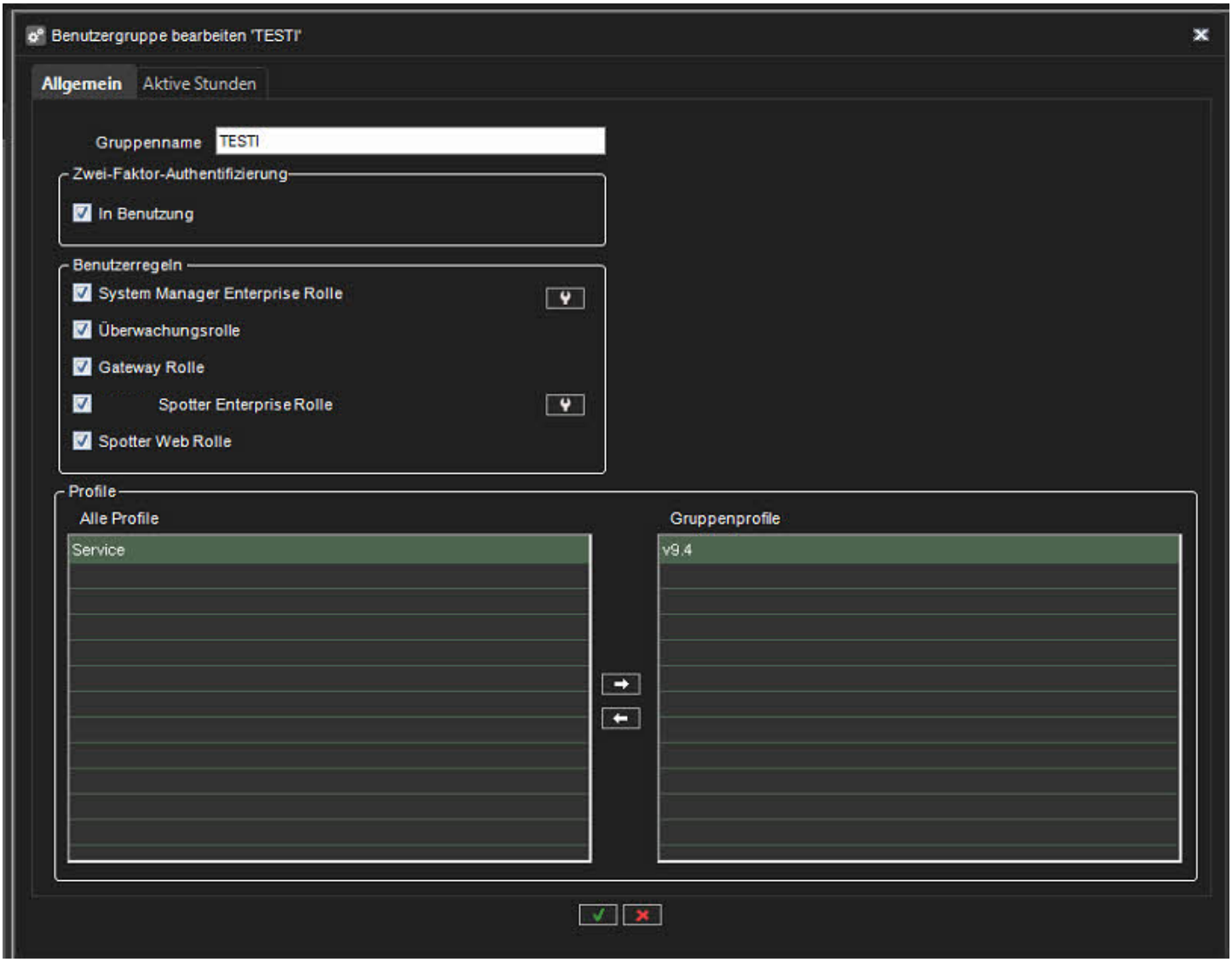
12.4 BENUTZERGRUPPE

12.4.1 Die Benutzergruppe definiert, auf welche Mirasys VMS-Anwendungen die Benutzergruppe Zugriff hat und welche Art von Berechtigungen die Benutzergruppe in Bezug auf die Anwendungen hat.

12.4.2 Benutzerregeln

Das System unterstützt die folgenden Arten von Benutzerrollen (definiert durch Benutzergruppen):

- **Rolle des Systemmanagers:** Administratoren dürfen sich beim System Manager anmelden und alle Einstellungen ändern, z. B. Kameraeinstellungen ändern oder neue Profile oder Benutzerkonten hinzufügen.
- **Überwachungsrolle:** Benutzer mit Überwachungsrechten dürfen sich beim System Manager anmelden und das System auf der Registerkarte **System** überwachen, aber sie dürfen die Einstellungen nicht ändern.
- **Gateway-Rolle: ist diese Rolle aktiv, kann die Benutzergruppe auf das DVMS-Gateway zugreifen**
- **Mirasys Spotter Enterprise-Rolle:** Endbenutzer können sich bei Spotter anmelden, jedoch nicht bei System Manager.
- **Spotter Web role:** Endbenutzer können sich bei Spotter Web anmelden



12.4.2.1 Unternehmensrolle Systemmanager

Es ist möglich, für verschiedene Benutzergruppen explizite Berechtigungen für den Systemmanager zu setzen.

Dies ermöglicht beispielsweise die Implementierung von Funktionalitäten, um verschiedene Benutzergruppen für die Hardwarewartung und Benutzerverwaltung zuzulassen, was für große Systeme hilfreich ist.

Um die Funktionalität zu aktivieren - aktivieren Sie das Kontrollkästchen "Systemmanager-Unternehmensrolle" für die Benutzergruppe und klicken Sie auf das Symbol "Schraubenschlüssel", um die Details für diese Gruppe zu bearbeiten.



12.4.2.1.1 System

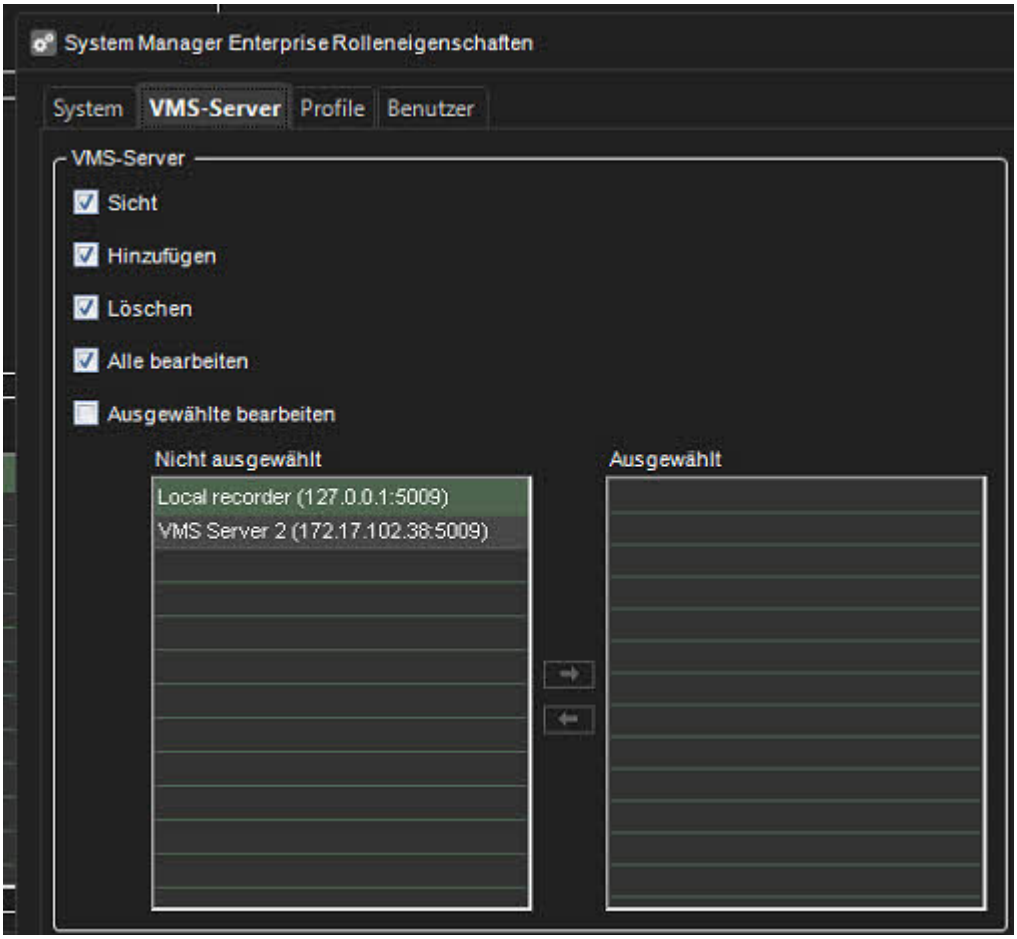


Die System-Tab-Berechtigungen können für eine Benutzergruppe aktiviert oder deaktiviert werden, indem beispielsweise die Systemeinstellungen deaktiviert werden, werden die Systemeinstellungen für alle Benutzer in der Benutzergruppe ausgeblendet

12.4.2.1.2 VMS Servers

Die Registerkarte VMS-Server ermöglicht einer Benutzergruppe Berechtigungen zum Anzeigen, Hinzufügen, Löschen und Bearbeiten entweder aller oder nur ausgewählter VMS-Server, die notiert werden sollen: Wenn "Ausgewählte bearbeiten" aktiviert ist, ermöglicht das darunter liegende Shuttle-Kästchen die Definition, welche spezifischen Server diese Benutzergruppe hat Zugriff auf.

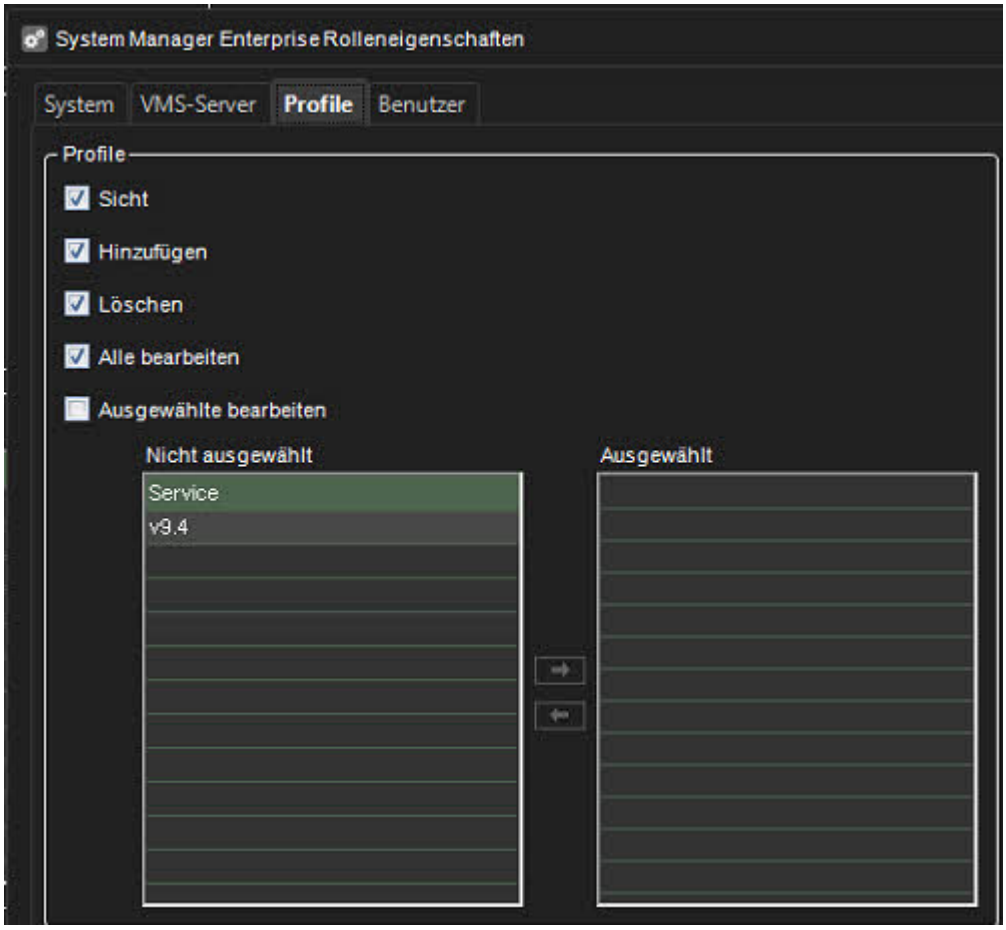
Dies ist in großen Installationen praktisch, wenn bestimmte Benutzergruppen mit bestimmten Servern arbeiten (z. B. wenn es separate Wartungsgruppen für verschiedene Standorte gibt - und die Aufzeichnungsserver standortspezifisch sind.)



12.4.2.1.3 Profiles

Die Registerkarte Profile/Berechtigungen, die für die Benutzergruppe festgelegt werden können:

„Ausgewählte bearbeiten“ ermöglicht Ihnen zu entscheiden, für welche Profile die Funktionalität gilt (ähnlich wie bei der Berechtigungskonfiguration „Server“).



12.4.2.1.4 Benutzer

Die Benutzerregisterkarten/Berechtigungen, die für die Benutzergruppe festgelegt werden können:



„Alle bearbeiten“ oder „Ausgewählte bearbeiten“ muss für eine Benutzergruppe aktiviert sein, damit Benutzer sie hinzufügen und/oder löschen können (diese Optionen werden automatisch deaktiviert, wenn „Alle bearbeiten“ oder „Ausgewählte bearbeiten“ deaktiviert ist).

This functionality affects VMS Servers, Profiles and Users tabs

12.4.2.2 Überwachungsrolle

Die Benutzer mit der Rolle Überwachung haben die Berechtigung:

12.4.2.2.1 System

- Protokolle exportieren
- SM-Server- und VMS-Server-Diagnose
- Lizenzen
- Watchdog-Protokoll

12.4.2.2.2 Profiles

Kann den Inhalt der Profile anzeigen

12.4.2.2.3 Benutzer

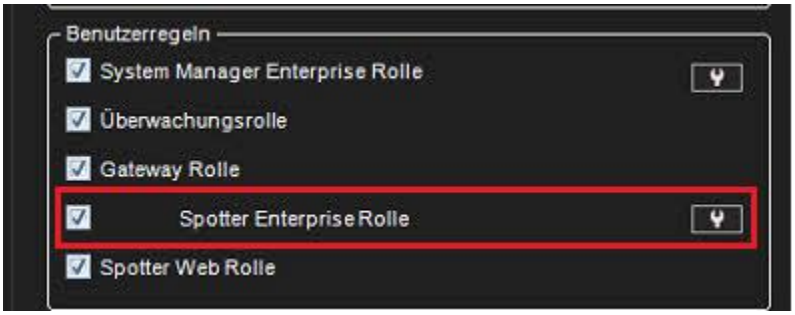
Kann die Systembenutzergruppen und -benutzer anzeigen

12.4.2.3 Gateway-Rolle

Gateway-Rolle ermöglicht die alte Spotter Mobile-Nutzung

12.4.2.4 Mirasys Spotter Enterprise Rolle

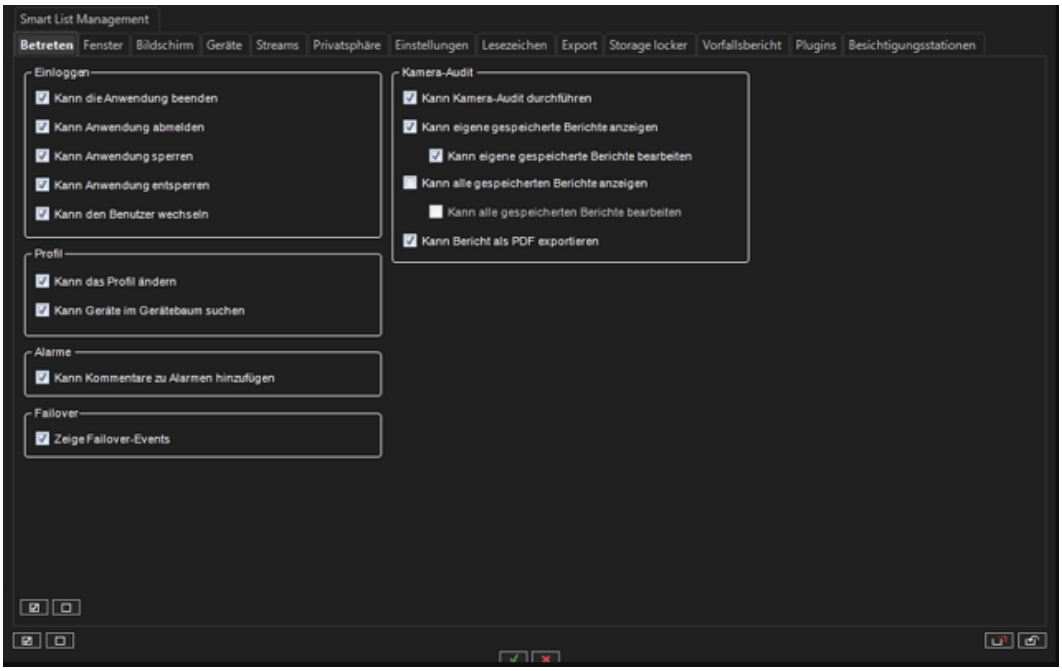
Benutzerdefinierte Benutzerrolleneigenschaften können bearbeitet werden, indem Sie auf die Schaltfläche zum Bearbeiten der benutzerdefinierten Rolleneigenschaften klicken.



Die benutzerdefinierten **Spotter**-Rollen können mit fast hundert verschiedenen Optionen (ohne Plugin-spezifische Anpassungen) angepasst werden.

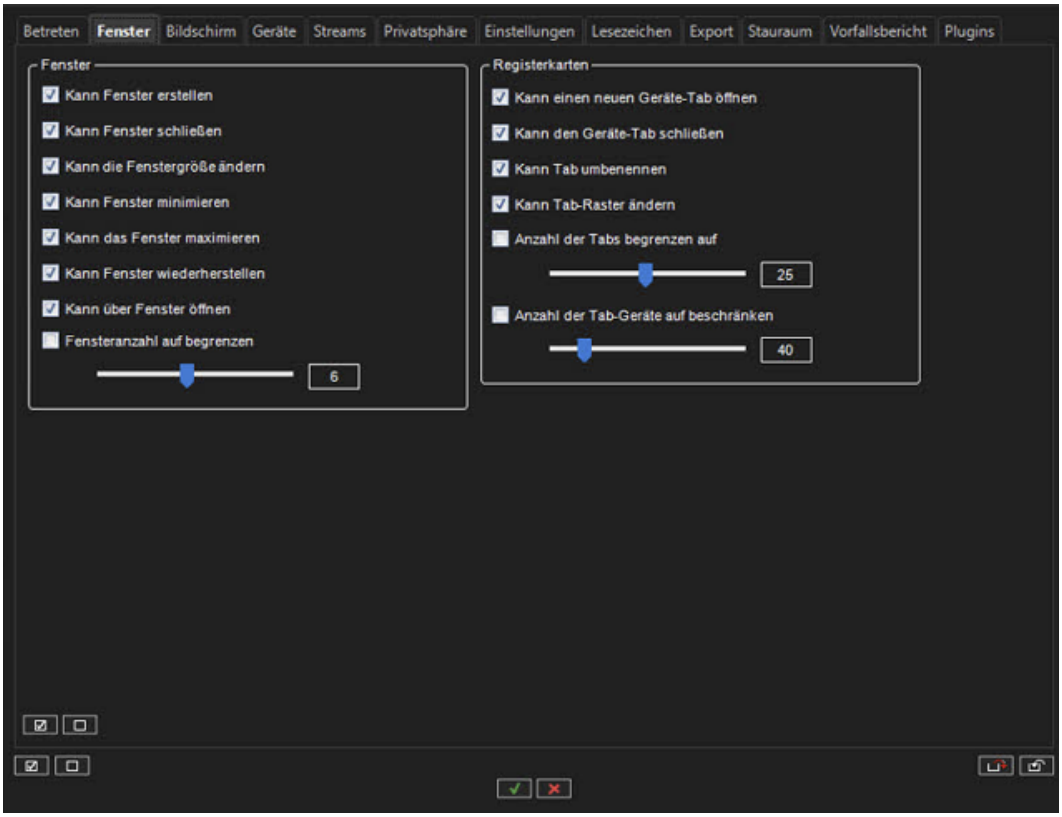
12.4.2.4.1 Betreten

Die Registerkarte Zugriff der Rollenanpassung enthält Optionen für den Anwendungszugriff und den Zugriff auf Profile und Alarmkommentare.



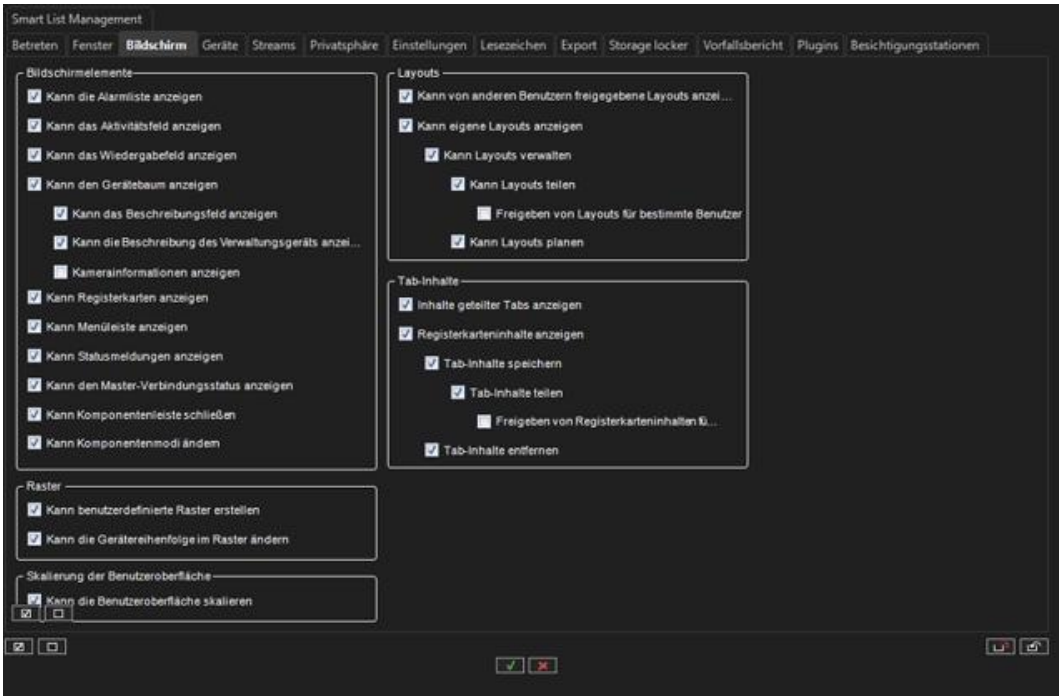
12.4.2.4.2 Fenster

Die Registerkarte „Fenster“ enthält Optionen für die Spotter-Fensterverwaltung und die Registerkartenverwaltung.



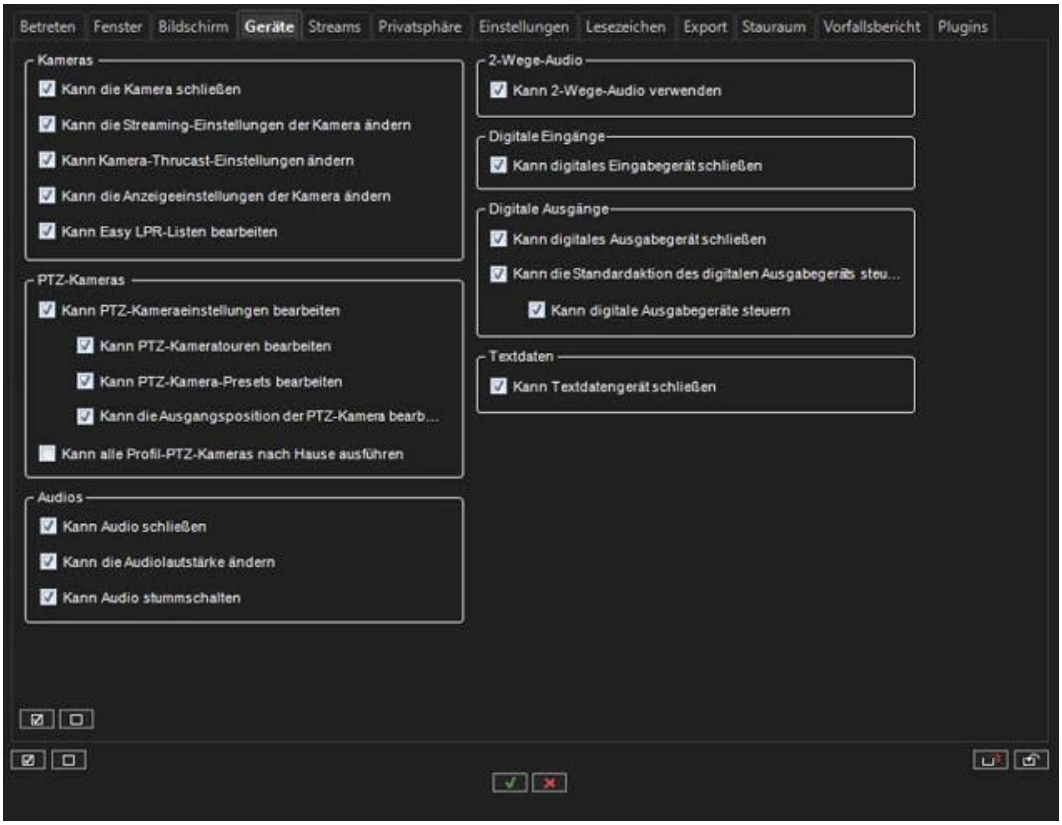
12.4.2.4.3 Bildschirm

Die Registerkarte Bildschirm enthält Optionen für den Zugriff auf verschiedene Bildschirmelemente und Layouts, Lesezeichen, Kameraraster und gespeicherte Kameraregisterkarten.



12.4.2.4.4 Geräte

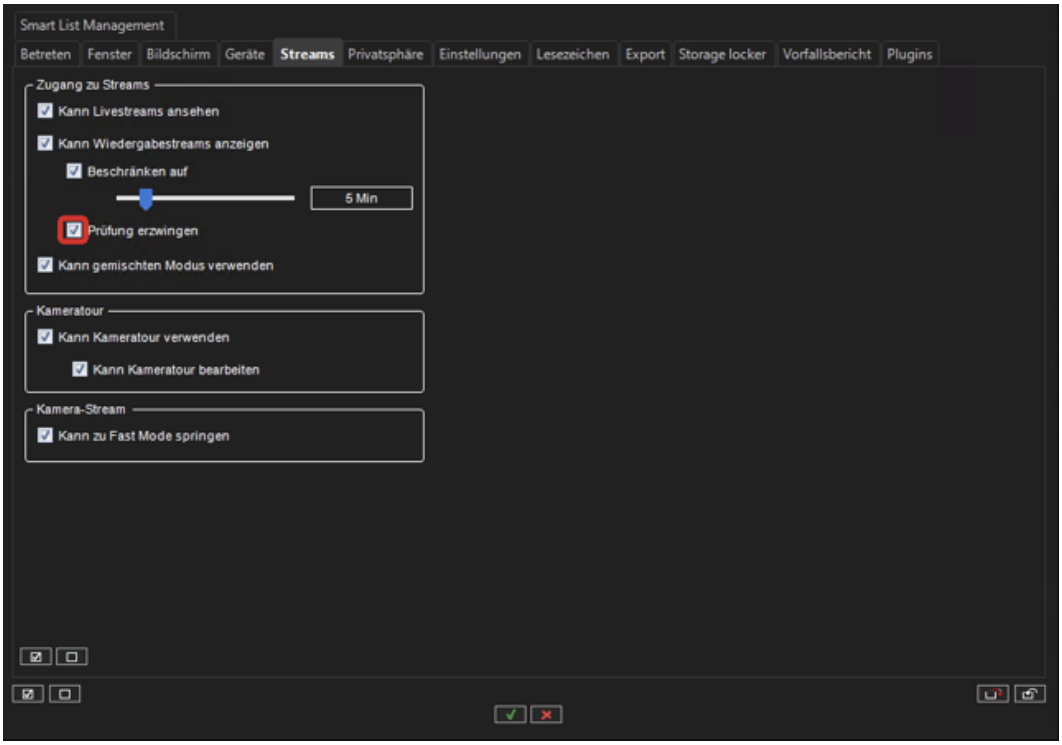
Die Registerkarte Geräte enthält Optionen zur Mediensteuerung.



12.4.2.4.5 Streams

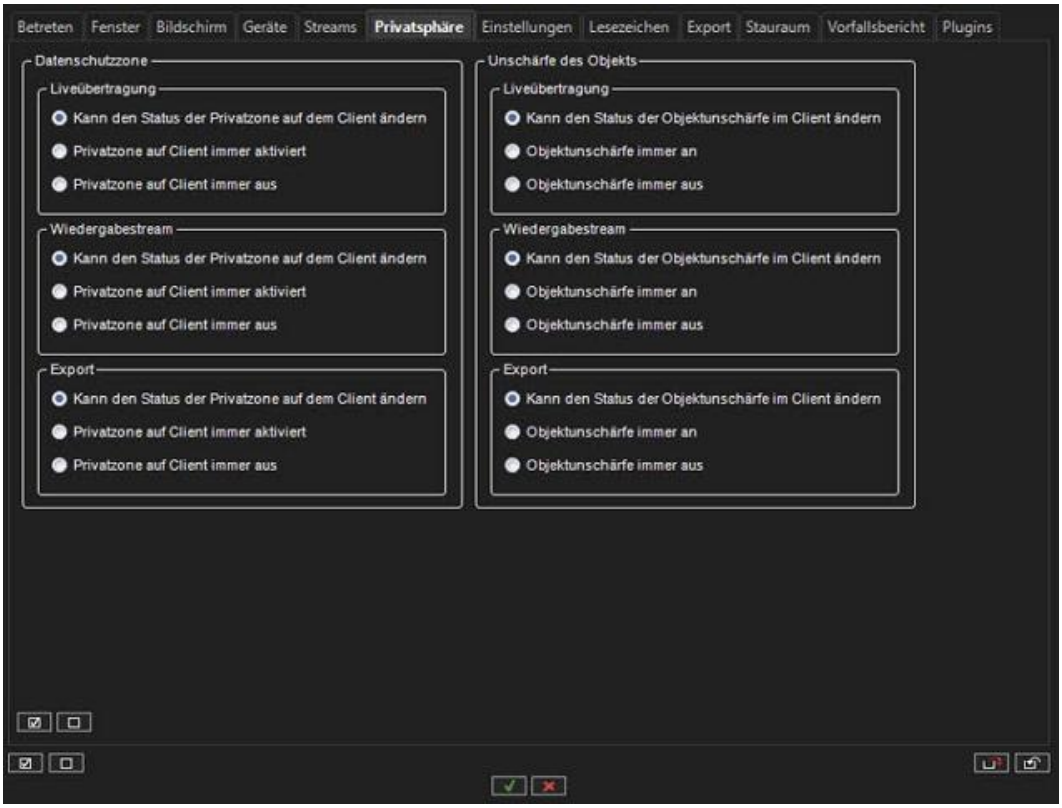
Die Registerkarte „Streams“ enthält Optionen für den Stream-Zugriff und -Export.

Auf der Video Wall kann der Bediener nun erzwingen, dass ein Benutzer vor der Verwendung des Wiedergabemodus einen Kommentar hinzufügt, um anzugeben, warum der Wiedergabemodus verwendet wird, bevor er in den Wiedergabemodus wechseln kann. Der Playback-Kommentar wird dem Audit-Protokoll hinzugefügt.



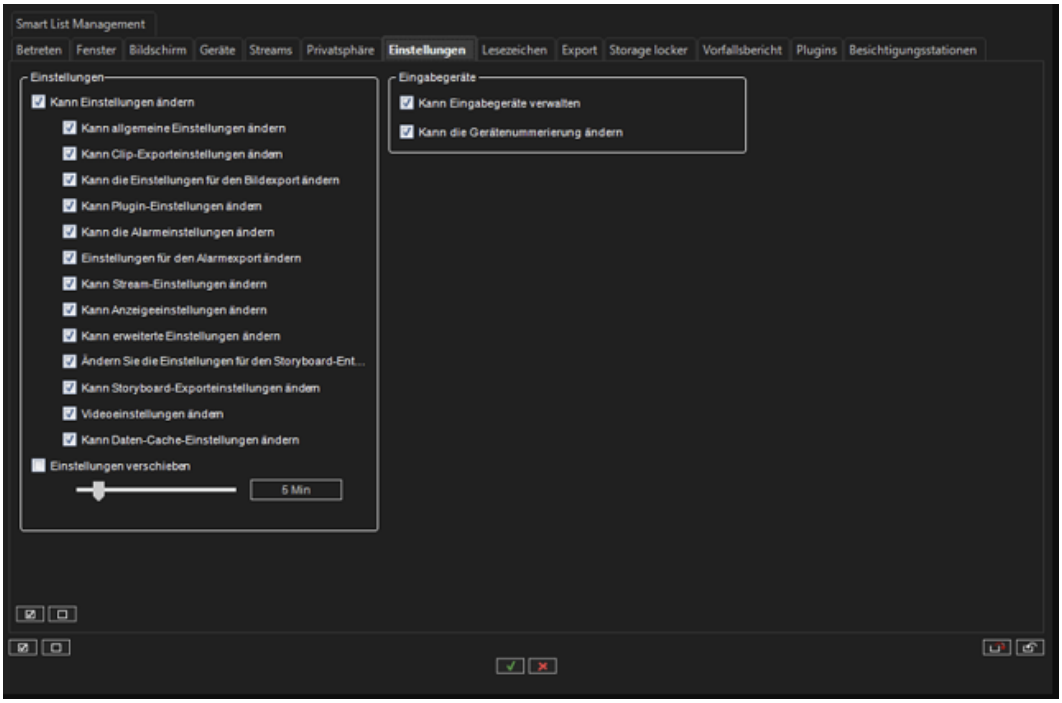
12.4.2.4.6 Privatsphäre

Die Registerkarte Privatsphäre enthält Optionen für den Datenschutz.



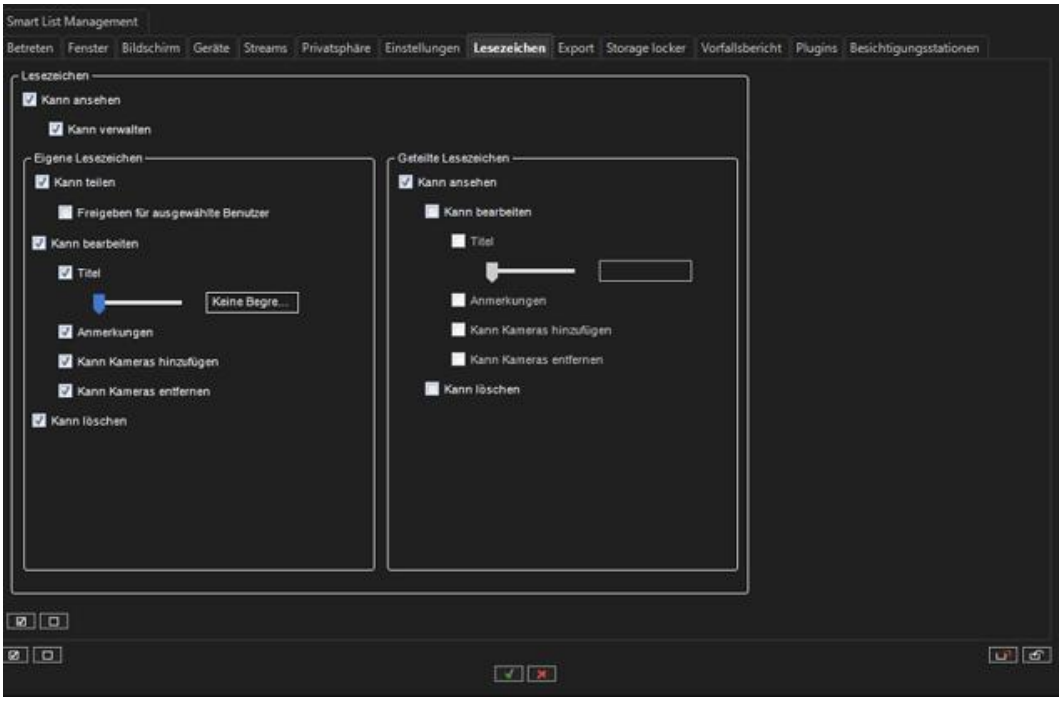
12.4.2.4.7 Einstellungen

Die Registerkarte Einstellungen enthält Optionen für Spotter-Einstellungen.



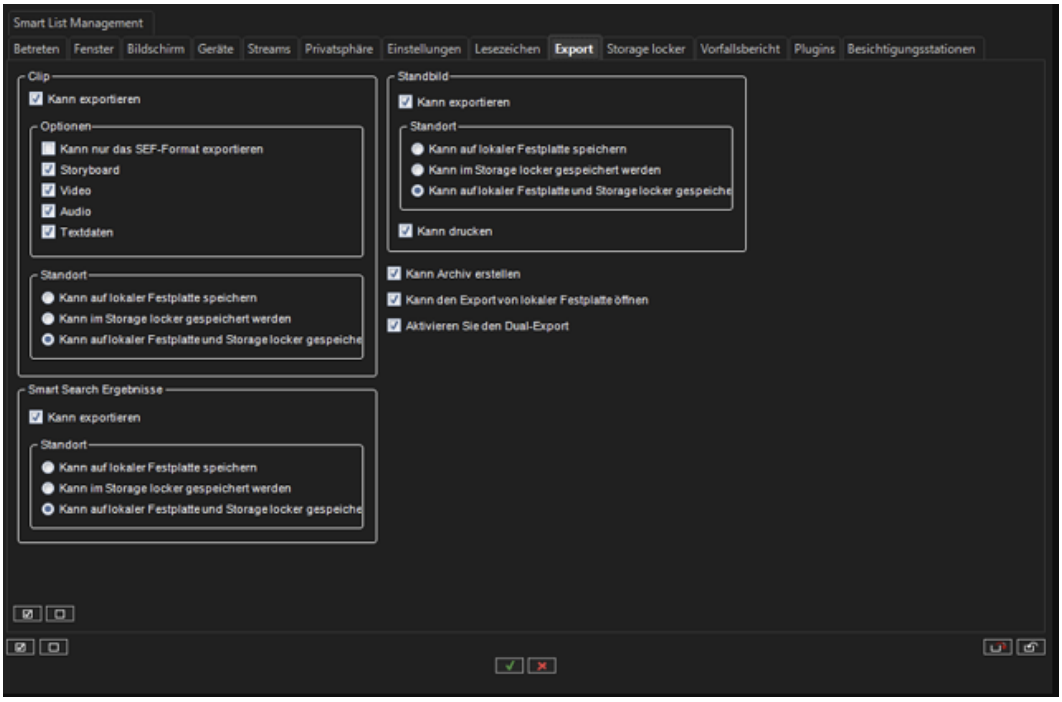
12.4.2.4.8 Lesezeichen

Die Registerkarte „Lesezeichen“ enthält Optionen für Lesezeichen



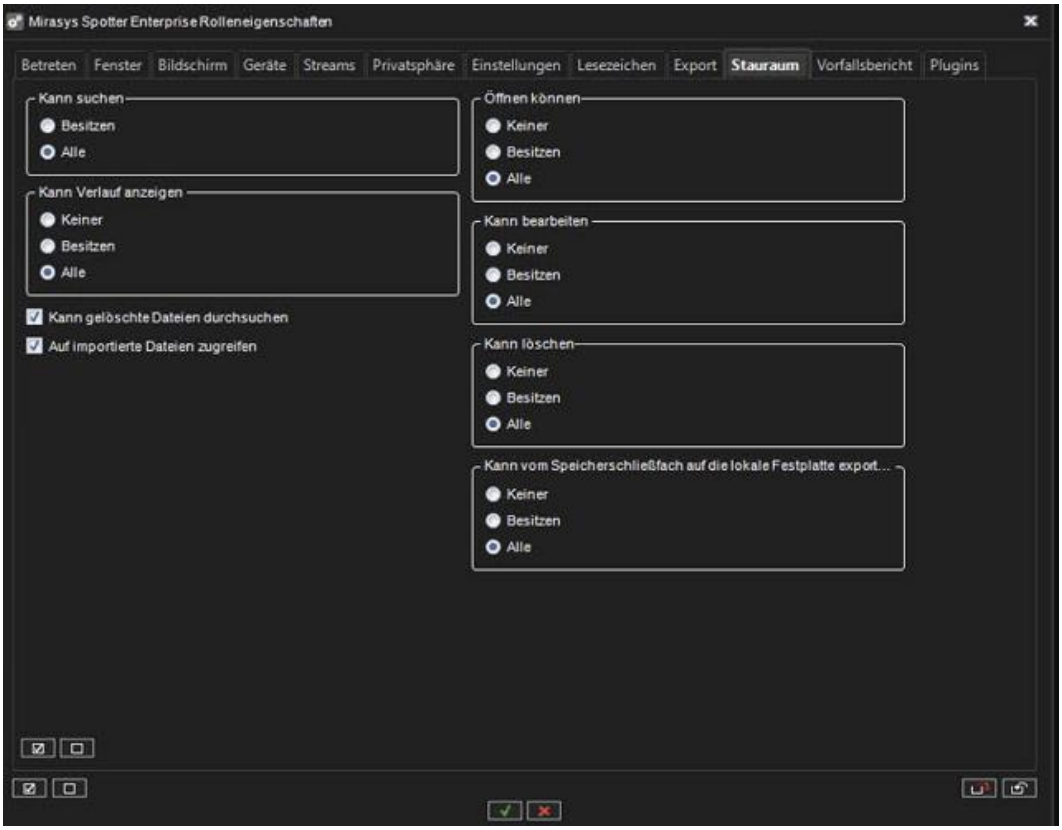
12.4.2.4.9 Export

Die Registerkarte Export enthält Optionen für Exportfunktionen



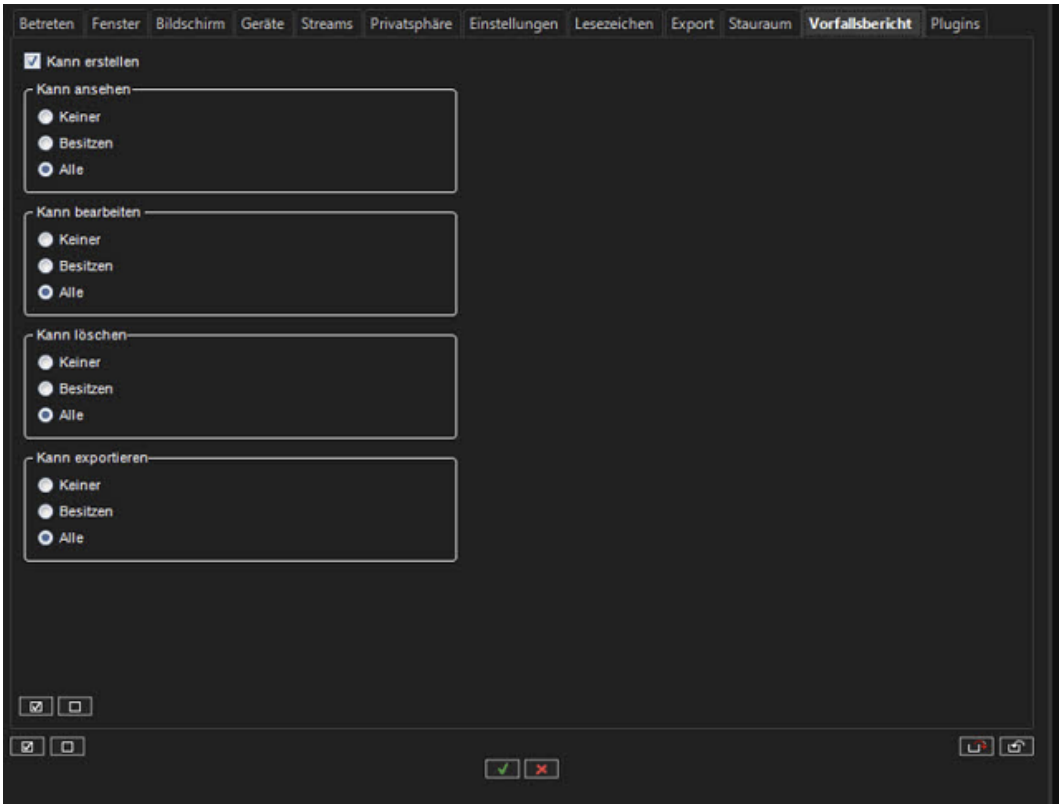
12.4.2.4.10Storage Locker

Die Registerkarte „Stauraum“ enthält Optionen für das Plug-in „Storage Locker“.



12.4.2.4.11Vorfallsbericht

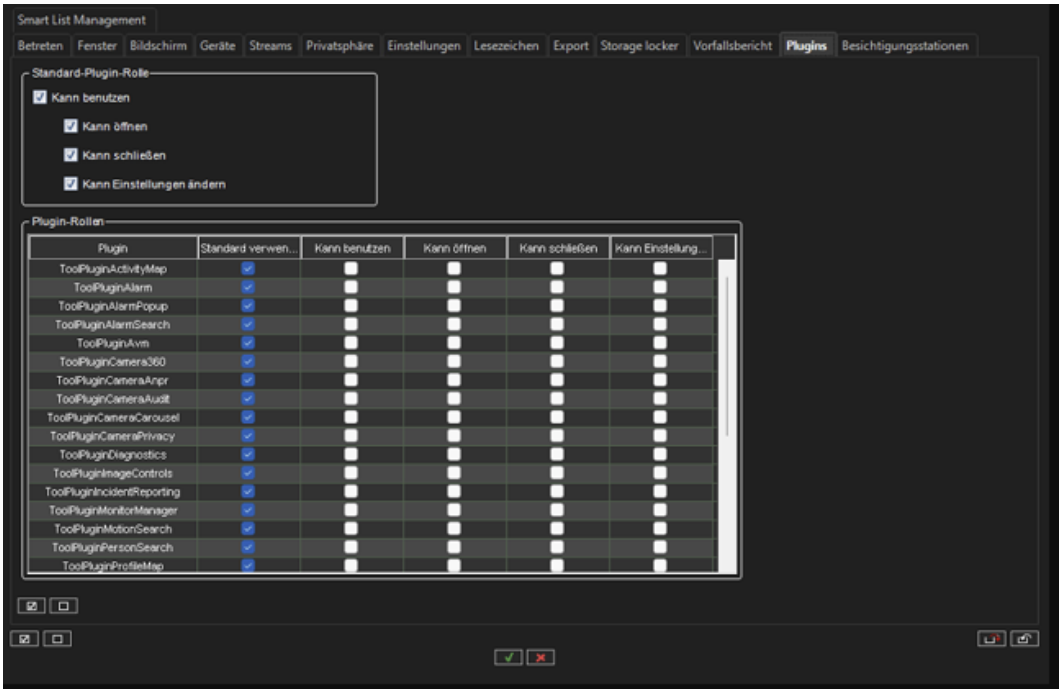
Die Registerkarte „Vorfallsbericht“ enthält Optionen für das Plug-in „Incident Reporting“.



12.4.2.4.12Plugins

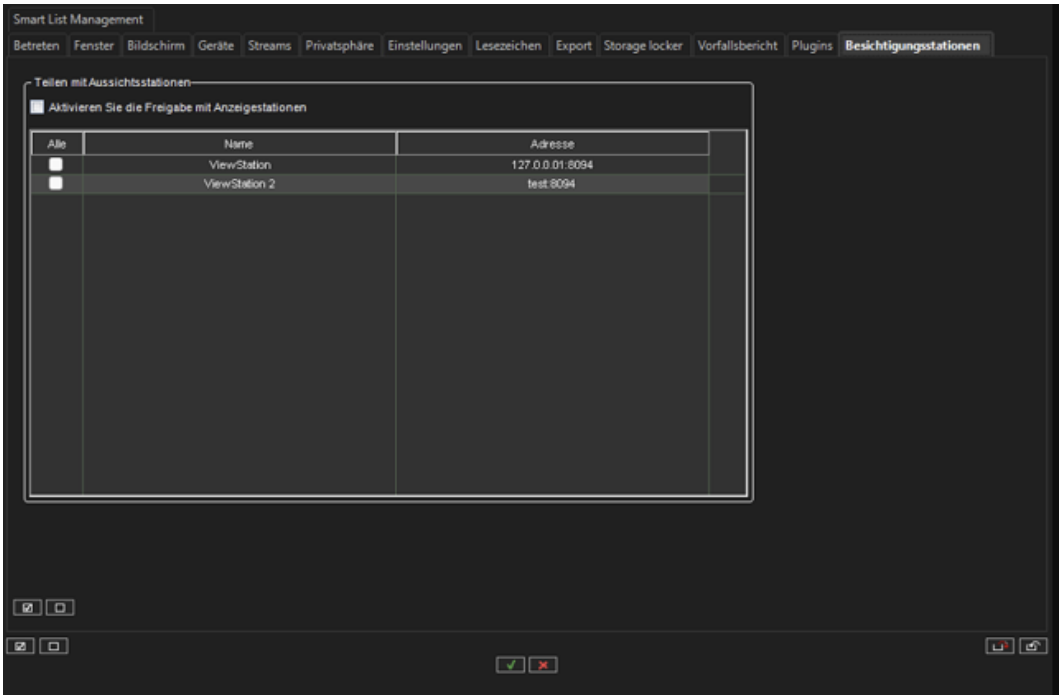
Die Registerkarte Plugins enthält Optionen für Spotter-Plugins.

Jedes Plugin-Verhalten kann entweder standardmäßig oder benutzerdefiniert sein. Das Standardverhalten kann über die Steuerelemente „Standard-Plugin-Rolle“ gesteuert werden.



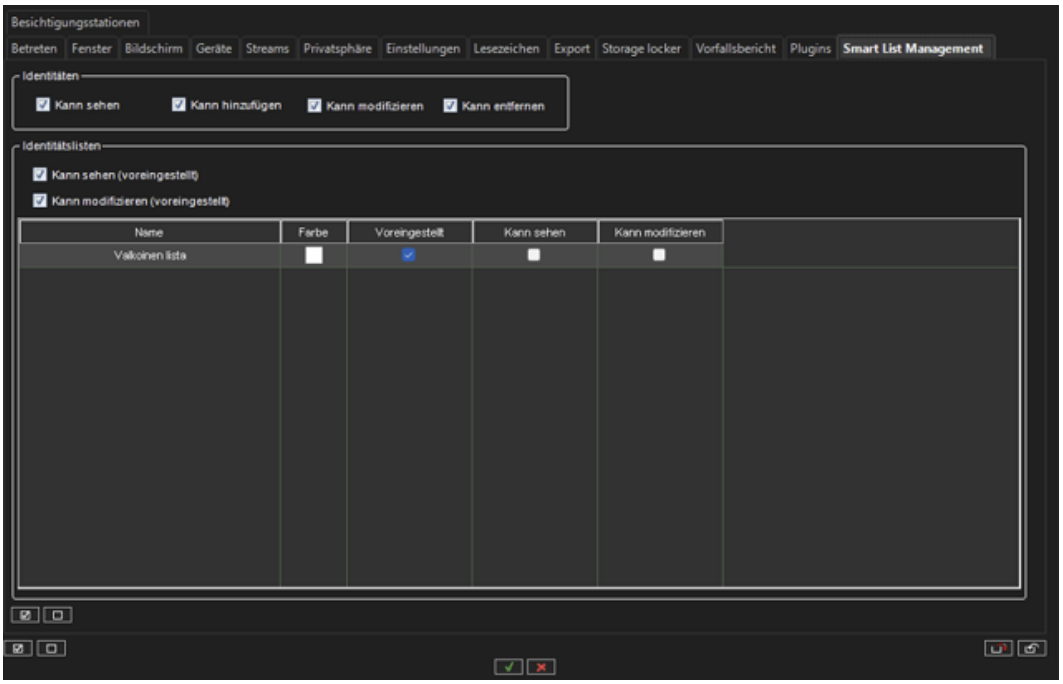
12.4.2.4.13Besichtigungsstationen

Die Registerkarte „Anzeigestationen“ enthält Optionen zum Anzeigen von Stationen.



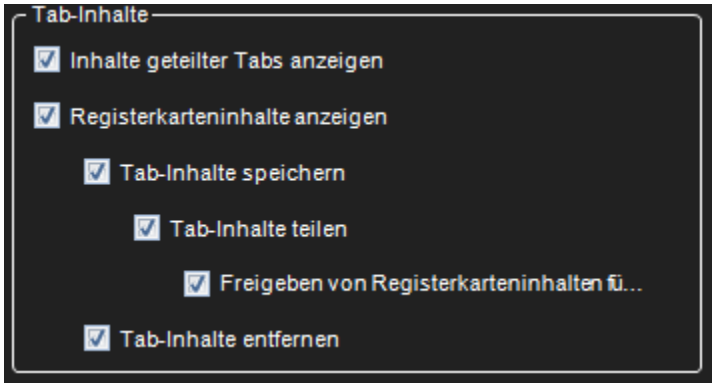
12.4.2.4.14Smart List Management

Die Registerkarte „Smart List Management“ enthält Optionen für das Plugin „Smart List Management“.



12.4.2.4.15Freigabe von Registerkarteninhalten für ausgewählte Benutzer

1. Gehen Sie in der Desktop-Anwendung System Manager unter Eigenschaften der Mirasys Spotter-Rolle auf die Registerkarte Inhalt.
2. Aktivieren Sie das Kontrollkästchen Inhalt der Registerkarte für bestimmte Benutzer freigeben, um die Funktion zu aktivieren.



12.4.2.4.16Freigabe für bestimmte Benutzer

12.4.2.4.16.1 Lesezeichen für bestimmte Benutzer freigeben

1. Gehen Sie im Menü auf der linken Seite auf die Registerkarte Benutzer und Benutzergruppen.
2. Öffnen Sie die Benutzergruppe "Administratoren" durch Doppelklick auf die Gruppe Administrotors im linken Menü.
3. Klicken Sie auf das Symbol rechts neben der Mirasys Spotter Enterprise-Rolle unter Benutzergruppenrollen, um die Eigenschaften der Mirasys Spotter Enterprise-Rolle zu bearbeiten.
4. Hier können Sie unter der Registerkarte Lesezeichen auswählen, ob Sie Lesezeichen für bestimmte Benutzer freigeben möchten, indem Sie auf An ausgewählte Benutzer freigeben klicken..

12.4.2.4.16.2 Share layouts with specified users

1. Gehen Sie im Menü auf der linken Seite auf die Registerkarte Benutzer und Benutzergruppen.
2. Öffnen Sie die Benutzergruppe "Administratoren" durch Doppelklick auf die Gruppe Administrotors im linken Menü.
3. Klicken Sie auf das Symbol rechts neben der Mirasys Spotter Enterprise-Rolle unter Benutzergruppenrollen, um die Eigenschaften der Mirasys Spotter Enterprise-Rolle zu bearbeiten.
4. Hier können Sie den Inhalt der Registerkarte auswählen, indem Sie auf der Registerkarte Bildschirm unter Registerinhalte auf Layoutinhalte für bestimmte Benutzer freigeben klicken..

12.4.2.4.16.3 Freigabe von Registerkarteninhalten für bestimmte Benutzer

1. Gehen Sie im Menü auf der linken Seite auf die Registerkarte Benutzer und Benutzergruppen.

2. Öffnen Sie die Benutzergruppe "Administratoren" durch Doppelklick auf die Gruppe Administrotors im linken Menü.
3. Klicken Sie auf das Symbol rechts neben der Mirasys Spotter Enterprise-Rolle unter Benutzergruppenrollen, um die Eigenschaften der Mirasys Spotter Enterprise-Rolle zu bearbeiten.
4. Hier können Sie den Inhalt der Registerkarte für ausgewählte Benutzer freigeben, indem Sie auf Registerinhalte für bestimmte Benutzer freigeben unter Registerinhalte.

12.4.2.4.17Direkter Alarm-Export in einen bestimmten Ordner

Wenn Systemadministratoren diese Funktion aktivieren und konfigurieren, ist es möglich, einen Alarm direkt aus der Alarmtabelle in Spotter in einen bestimmten Ordner der Alarmsuche zu exportieren.

1. Klicken Sie auf das Schraubenschlüssel-Symbol unter der Registerkarte Benutzer und Benutzergruppen im Menü auf der linken Seite, um zu Benutzergruppe bearbeiten zu gelangen, und klicken Sie dann auf den Schraubenschlüssel neben Mirasys Spotter Enterprise plus, um zur Registerkarte Einstellungen der Spotter-Rolle zu gelangen.
2. Aktivieren Sie das Kontrollkästchen für Alarm-Exporteinstellungen ändern unter Einstellungen ändern.

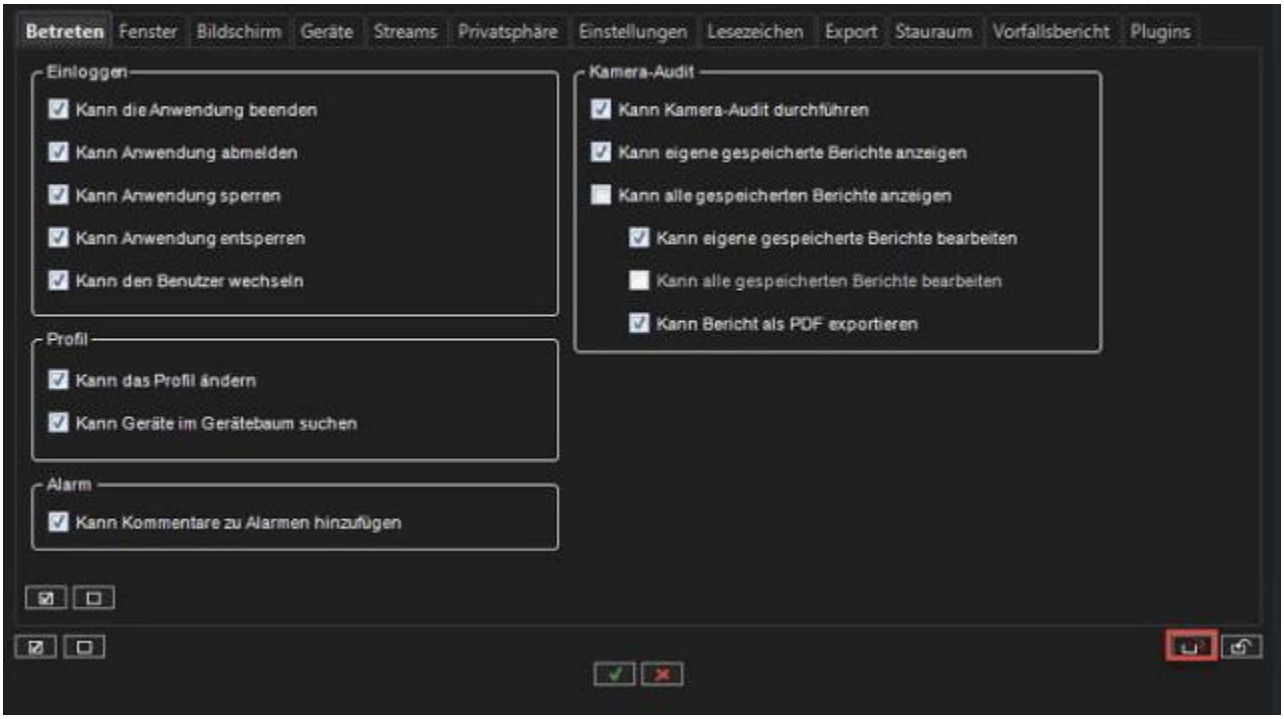
12.4.2.5 Spotter Web role (Benutzerregeln)

Spotter Web-Rolle ermöglicht neue Spotter Web- und Spotter Mobile-Nutzung

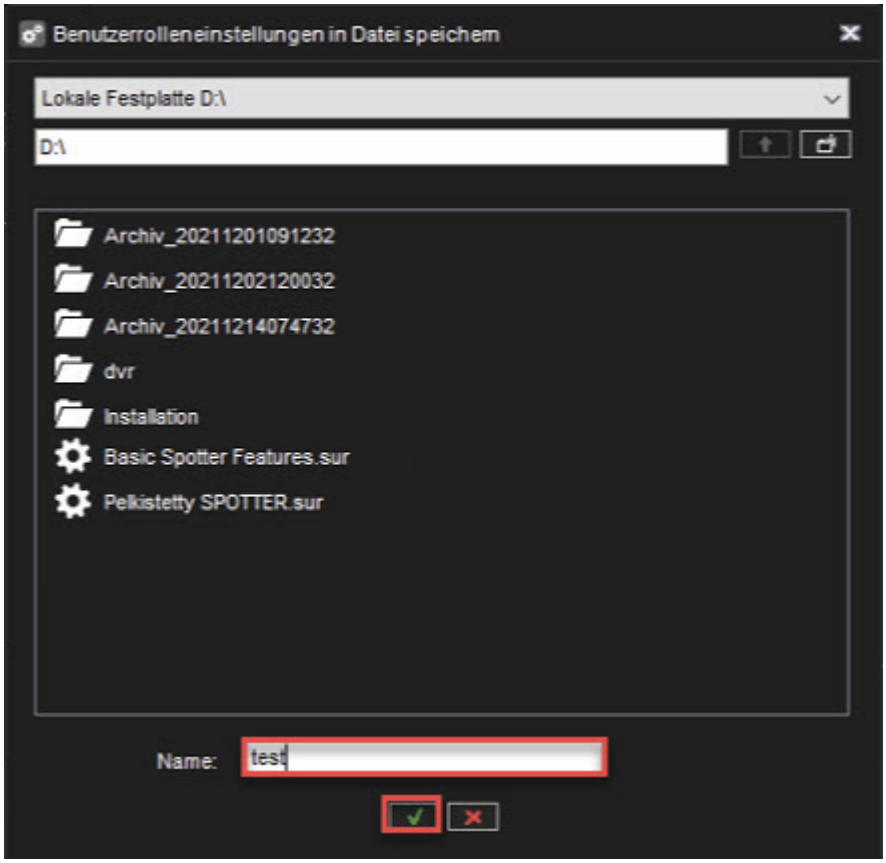
12.4.2.6 Exportieren und Importieren von Benutzerrolleneinstellungen

12.4.2.6.1 Benutzerrolleneinstellungen werden exportiert

- Klicken Sie auf **Benutzerrolleneinstellungen in Datei** exportieren

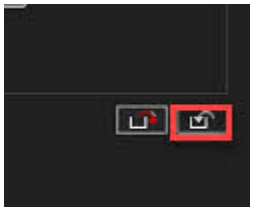


1. Ziel aussuchen
2. Legen Sie den Namen der Datei fest
3. Klicken **OK**

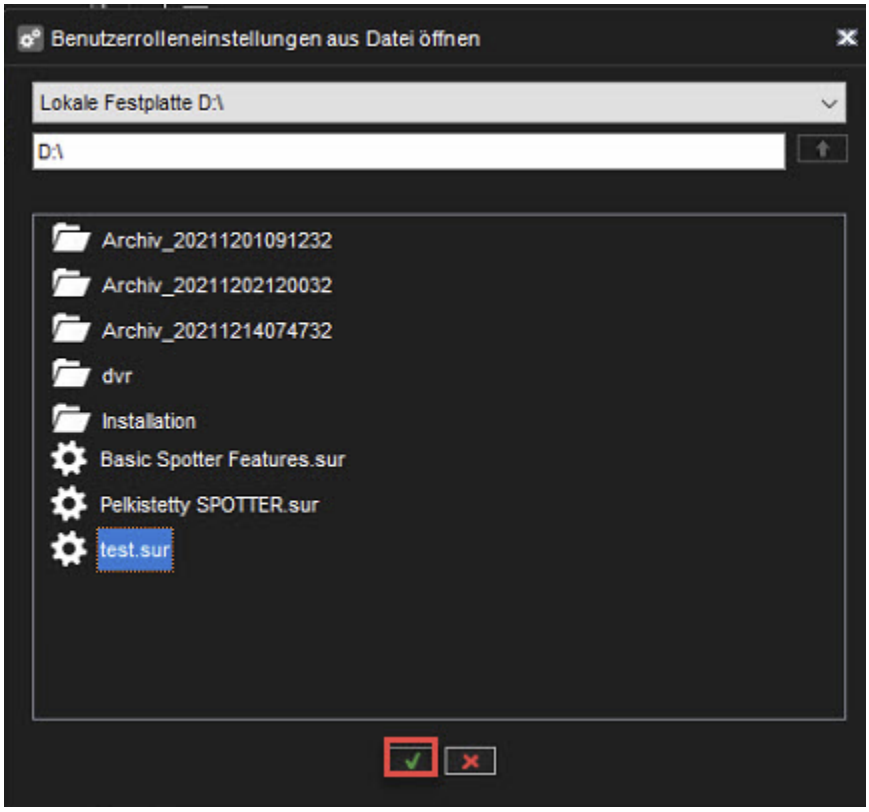


12.4.2.6.2 Importieren von Benutzerrolleneinstellungen

1. Klicken Sie auf **Benutzerrolleneinstellungen aus der Datei importieren**



2. Datei auswählen (.sur)
3. Klicken **OK**



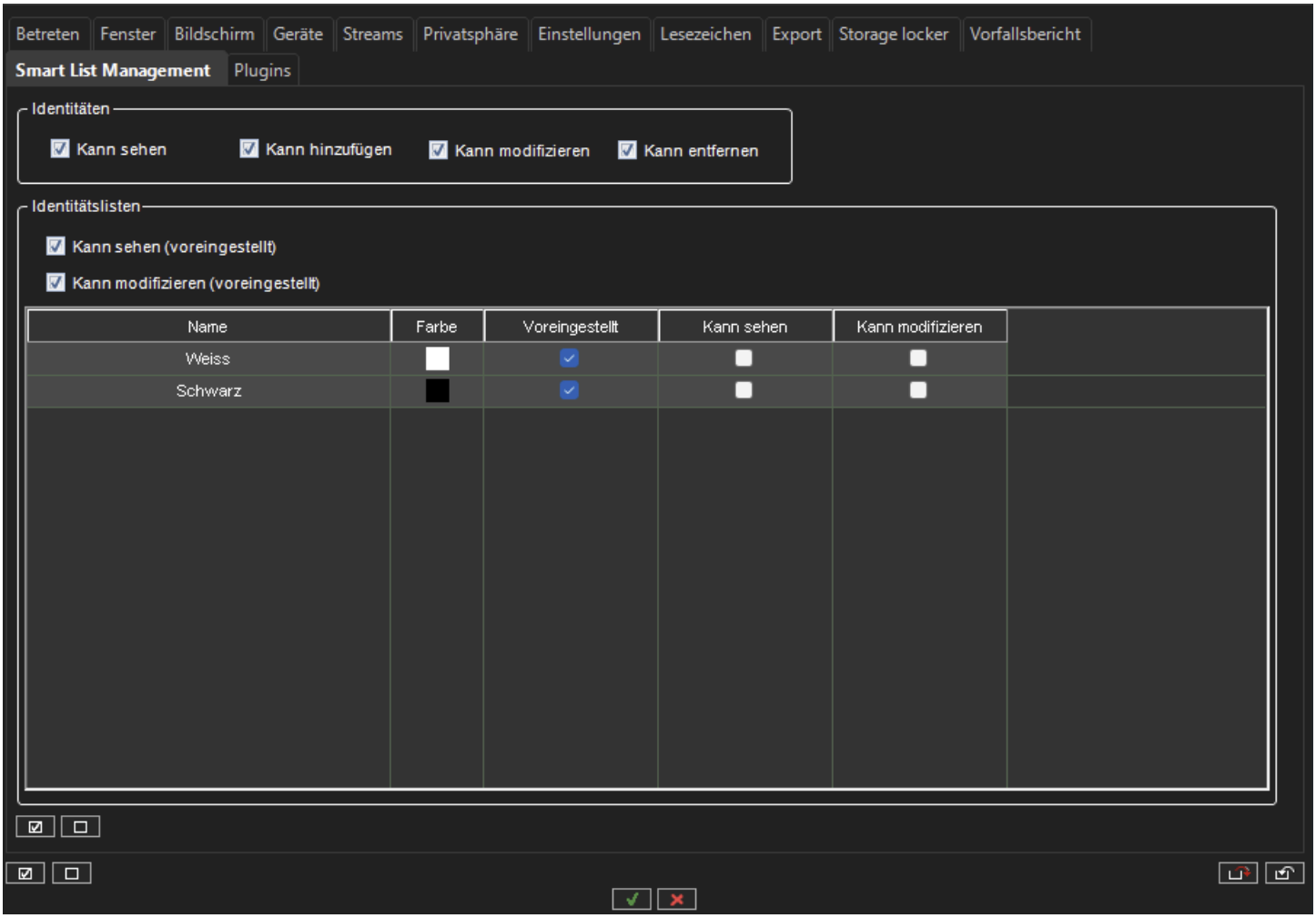
12.4.2.7 Benutzerrollen für die Listenverwaltung

Das Plugin zur Verwaltung von Spotter-Listen kann in den Einstellungen der Spotter-Benutzerrolle aktiviert werden, wo es auch möglich ist, die Berechtigungen zur Verwaltung von Identitäten und Identitätslisten einzuschränken.

12.4.2.7.1 Eigenschaften der intelligenten Listenverwaltung

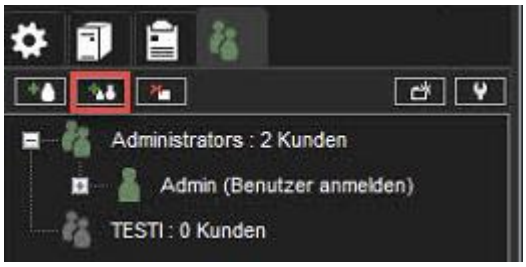
Die Registerkarte "Intelligente Listenverwaltung" enthält Rolleneigenschaften, die sich auf die Funktionen der intelligenten Listenverwaltung beziehen:

- Möglichkeit, Identitäten anzuzeigen, hinzuzufügen, zu ändern und zu entfernen.
- Möglichkeit zum Anzeigen und Ändern von Identitätslisten (Standardeigenschaften und Eigenschaften für jede Liste separat).



12.4.3 Erstellen einer kundenspezifischen Benutzergruppe

1. Klicken Sie **Benutzergruppe hinzufügen**



2. Geben Sie einen Namen für die Gruppe in das Feld **Gruppenname** ein

3. Aktivieren Sie bei Bedarf die **Zwei-Faktor-Authentifizierung**

4. Wählen Sie die **Benutzerrollen** für die Gruppe aus.

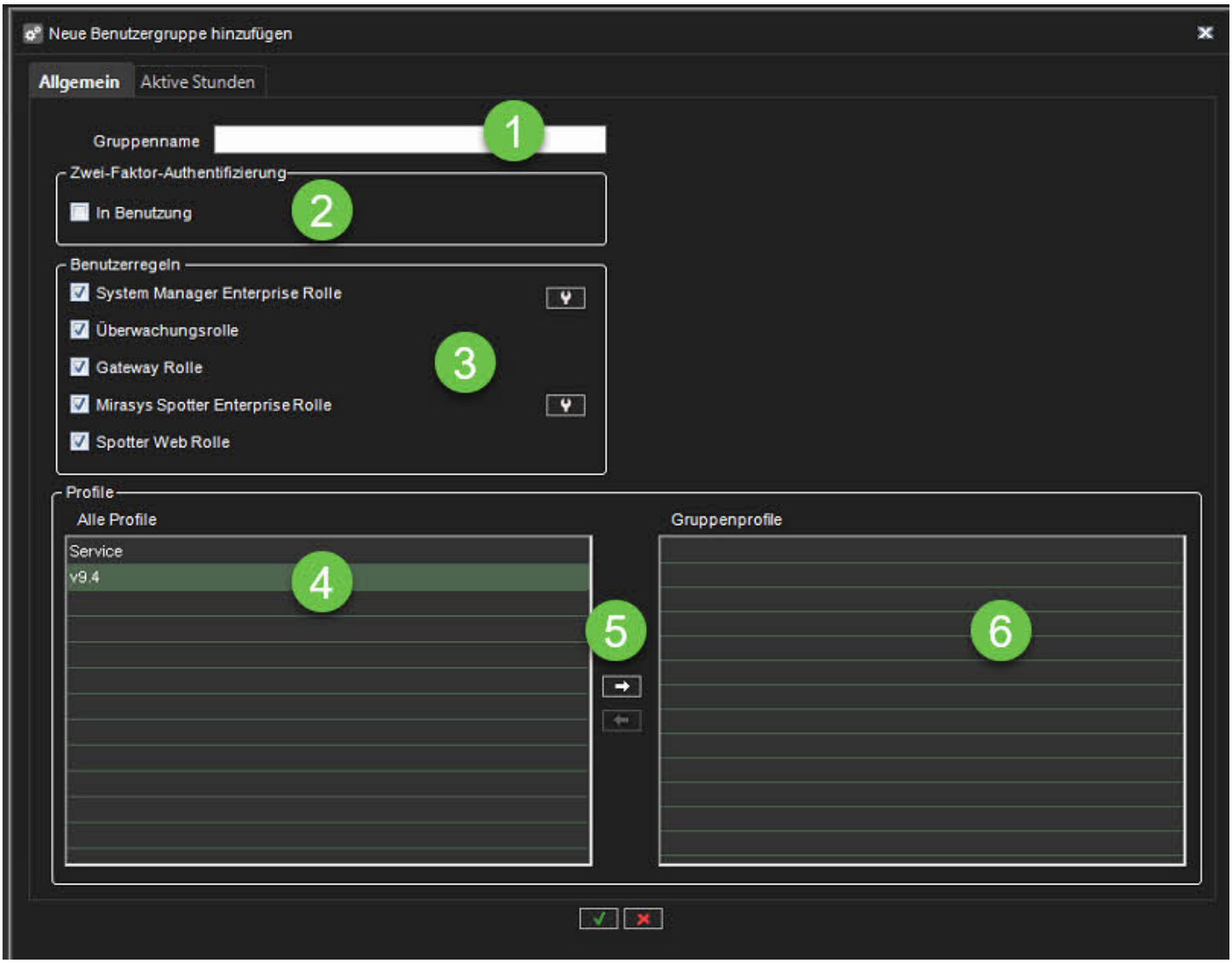
5. Wählen Sie das **Profil** oder **Profile** aus, das Sie der Benutzergruppe zuweisen möchten.

6. Klicken Sie auf die Schaltfläche mit dem Pfeil nach rechts oder ziehen Sie die Profile aus dem linken Bereich in das Feld mit den Gruppenprofilen

7. Überprüfen Sie, ob die richtigen Profile gefunden wurden

8. Klicken Sie auf **Ok**, um die Erstellung der Benutzergruppe zu bestätigen

HInweis: *Um mehr als ein Profil gleichzeitig auszuwählen, halten Sie die UM SHIFT- oder CTRL-Taste gedrückt.*



12.4.3.1 Bearbeiten einer Benutzergruppe

So bearbeiten Sie eine Benutzergruppe (ob system- oder domänen**basiert):**

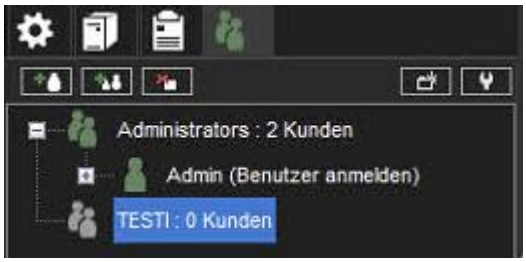
1. Öffnen Sie die Registerkarte **Benutzer**.
2. Klicken Sie auf die Benutzergruppe, die Sie bearbeiten möchten.
3. Sie können die folgenden Einstellungen bearbeiten:
    a. Geben Sie einen Namen für die Gruppe in das Feld **Gruppenname** ein.
    b. Wählen Sie die Benutzerrollen für die Gruppe aus.
    c. Wählen Sie das oder die Profile aus, die Sie der Benutzergruppe zuweisen möchten. Klicken Sie auf die rechte Pfeilschaltfläche oder ziehen Sie die Profile aus dem linken Bereich nach rechts.
4. Klicken Sie auf **OK**, um die Änderungen zu speichern.

- **Hinweis:** *Um mehr als ein Profil gleichzeitig auszuwählen, halten Sie die UM SHIFT- oder CTRL-Taste gedrückt.*

12.4.3.2 Löschen einer Benutzergruppe

So löschen Sie eine Benutzergruppe (ob system- oder domänen**basiert):**

1. Öffnen Sie die Registerkarte **Benutzer**.
2. Klicken Sie auf die Benutzergruppe, die Sie löschen möchten. Beachten Sie, dass Sie die Standardgruppe **Administrators** nicht löschen können.



1. Klicken Sie oben links auf **Benutzergruppe löschen**.
2. Klicken Sie auf **OK** , um die Gruppe zu löschen.

Notiz *Domänenbasierte (LDAP) Benutzergruppen können nicht über System Manager gelöscht werden. Beim Löschen wird eine LDAP-Gruppe aus System Manager entfernt, aber die Domänengruppe ist davon nicht betroffen.*

12.4.4 Zwei-Faktor-Authentifizierung

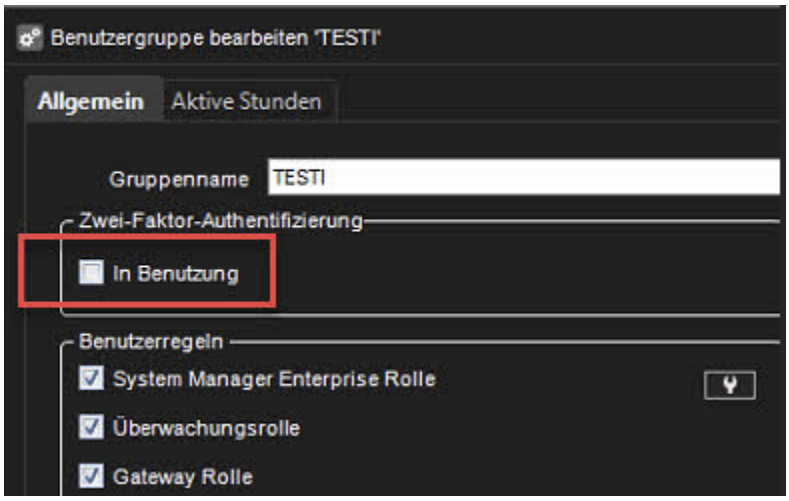
Die Zwei-Faktor-Authentifizierung ist eine Funktion zur Verbesserung der Identifizierung des Benutzers, indem der Benutzername und das Kennwort sowie ein Code von einem externen physischen Gerät angefordert werden.

Dies macht es praktisch unmöglich, z.B. bestimmte Benutzergruppen (z. B. Systemadministratoren), um gemeinsame Zugangsdaten zu verwenden.

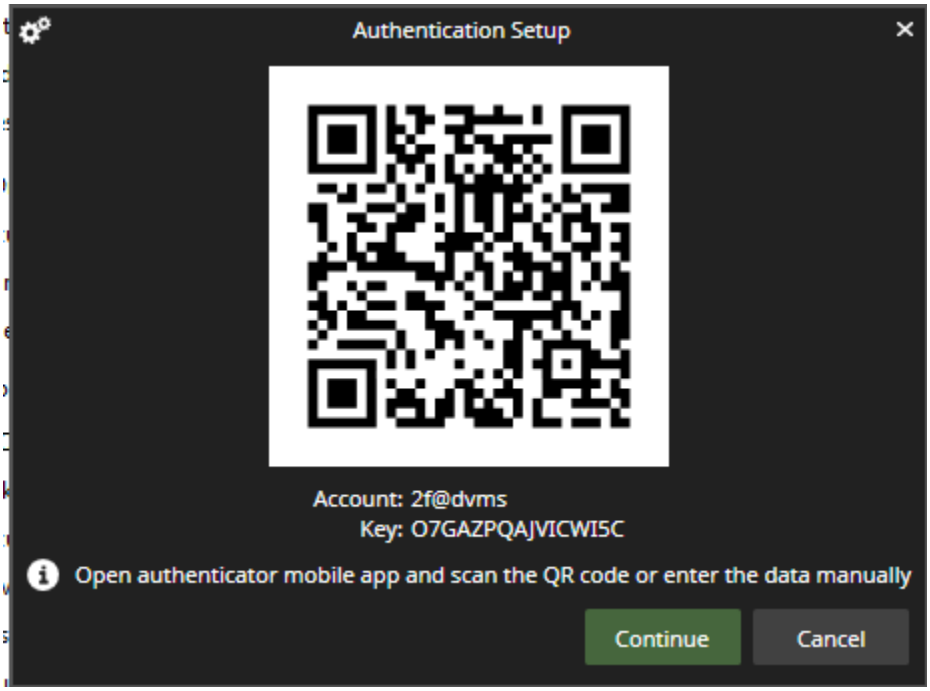
(Die Verwendung gemeinsamer Zugangsdaten würde es fast unmöglich machen, später z. B. bestimmte Benutzeraktionen aus den Audit-Logs zu überwachen.)

12.4.4.1 Aufstellen:

1. Der Admin aktiviert die 2-Faktor-Authentifizierung für die jeweilige Benutzergruppe.



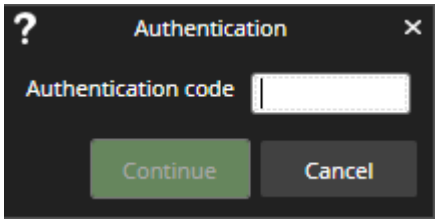
2. Beim erstmaligen Einloggen des Benutzers in der Gruppe wird der Benutzer aufgefordert, den 2-Faktor-Authentifizierungs-Client (z. B. Authy, Google Authenticator, MS Authenticator (kostenlos erhältlich)) auf seinem mobilen Gerät zu verwenden bzw. zu installieren .
3. Das VMS und der Authentifizierungsclient werden dann mit der Software mit VMS synchronisiert.
4. Dies geschieht, indem der vom VMS generierte „geheime Schlüssel“ per QR-Code an die Authentifizierungssoftware übertragen oder direkt in die Software eingetippt wird.
   Beispiel unten:



5. Danach generiert der Authentifizierungsclient automatisch neue Einmalpasswörter.
    a. (Die Passwörter ändern sich regelmäßig und werden synchron gehalten, da die VMS-Uhren und die Authentifizierungs-App die gleiche Zeit haben.
    b. Beachten Sie, dass dies keine direkte Datenkommunikationsverbindung zwischen der Software erfordert.)

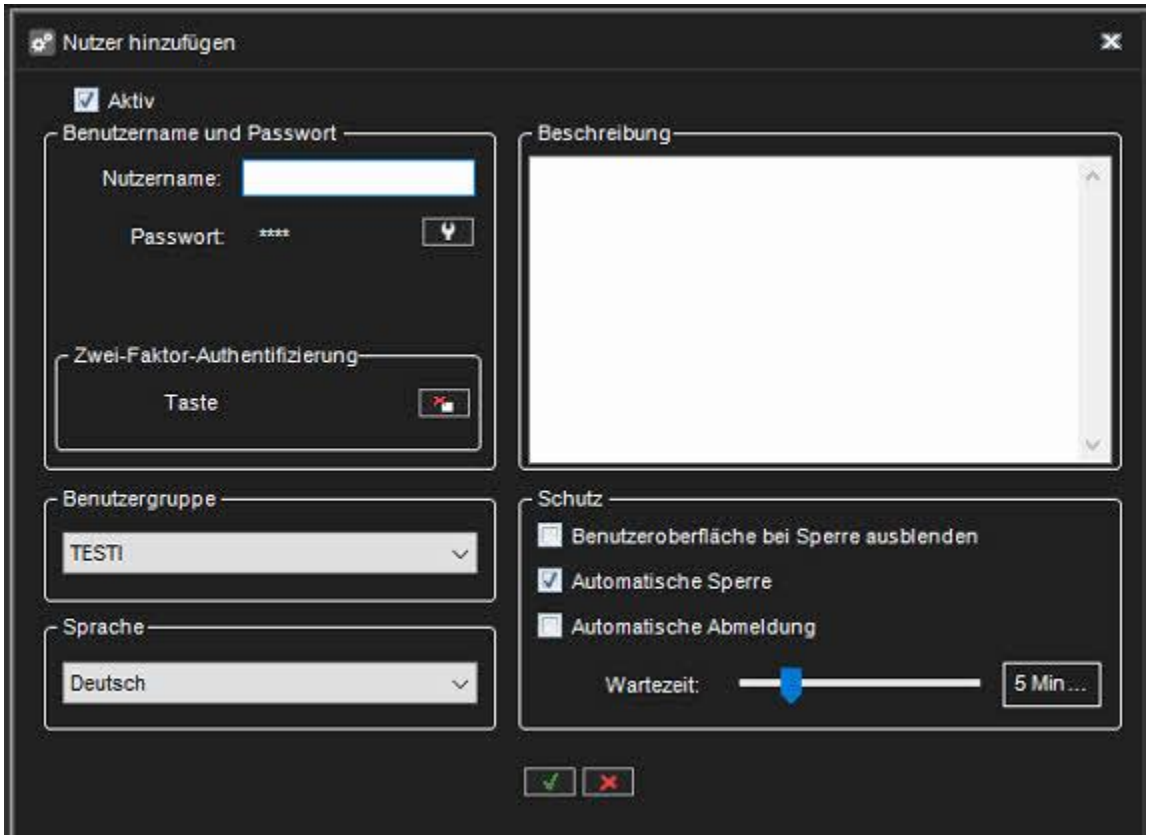
12.4.4.2 Anmeldung:

1. Der Benutzer stellt VMS die Standard-Anmeldeinformationen zur Verfügung (Benutzername, Passwort)
2. Das VMS fordert für jede Anmeldung einen Authentifizierungscode von der Authentifizierungs-App an.
3. Der Benutzer gibt das Einmalpasswort aus der Authentifizierungs-App an. Der Benutzer gibt sie in den VMS-Client ein.



12.4.4.3 Instandhaltung:

1. Wenn der Benutzer seinen geheimen 2-Faktor-Schlüssel vergisst, kann der Administrator den Schlüssel dann über den Systemmanager zurücksetzen.
2. Nach dem Zurücksetzen des 2-Faktor-Geheimschlüssels muss der Benutzer den privaten Schlüssel bei der nächsten Anmeldung aktualisieren. (Siehe Schritt 2).



12.4.5 Domänenbasierte Benutzergruppen (Active Directory)

Das System unterstützt die Integration von Benutzerrechten auf Domänenebene (Microsoft Active Directory, LDAP), wodurch Benutzer aus Domänengruppen synchronisiert werden können.

Domänenbasierte Benutzer können sich mit ihren Domänenbenutzernamen und Passwörtern beim VMS-System anmelden.

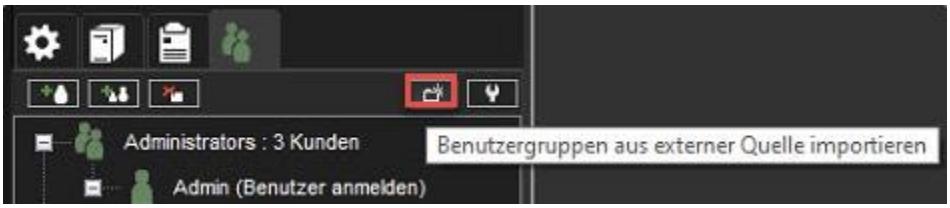
Standardmäßig werden Benutzergruppenrechte alle 30 Minuten mit ihrer übergeordneten Domäne synchronisiert.

Bitte wenden Sie sich an Ihren Systemlieferanten, wenn Sie das Standardintervall ändern müssen.

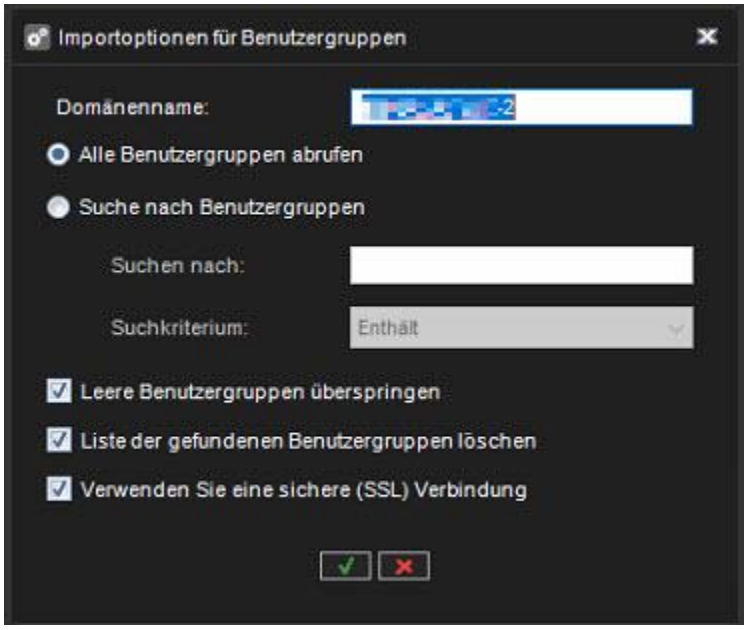
Diese Funktion erfordert ein Lizenzupdate.

12.4.5.1 Hinzufügen einer neuen domänenbasierten Benutzergruppe zum System

1. Klicken Sie in der oberen linken Ecke der Registerkarte **Benutzer** auf **Benutzergruppen aus einer externen Quelle importieren.**
   Der Hauptserver muss mit einer Domäne verbunden sein, damit die Schaltfläche angezeigt wird.
   Wenn der Server nicht mit einer Domäne verbunden ist, ist die Schaltfläche nicht sichtbar.



1. Geben Sie den Namen der Domäne in das Dialogfeld **Domänenname** ein.
2. Wählen Sie aus, ob Sie alle Benutzergruppen abrufen oder nach bestimmten Gruppen suchen möchten. Wenn Sie nach bestimmten Gruppen nach Namen suchen möchten, können Sie ein Suchkriterium hinzufügen, das darauf basiert, dass die Textzeichenfolge dem Gruppennamen entspricht, im Gruppennamen enthalten ist oder der Gruppenname in der Textzeichenfolge beginnt oder endet.
3. Wählen Sie aus, ob offene Benutzergruppen übersprungen oder eingeschlossen werden sollen.
4. Wählen Sie aus, ob vorherige Suchergebnisse gelöscht oder beibehalten werden sollen.
5. Aktivieren Sie **Sichere (SSL)-Verbindung verwenden**. Wenn benötigt
6. Klicken Sie auf **Ok**.
7. Wählen Sie im Fenster **Benutzergruppen importieren** die Benutzergruppen aus, die Sie aus der Domäne importieren möchten.
8. Klicken Sie auf **Ok**, um die ausgewählten Gruppen zu importieren.
9. Bearbeiten Sie die importierten Benutzergruppen, um ihre Benutzerrollen wie unten beschrieben festzulegen.



12.4.6 Aktive Stunden - Zeitplan für den Zugang von Benutzergruppen

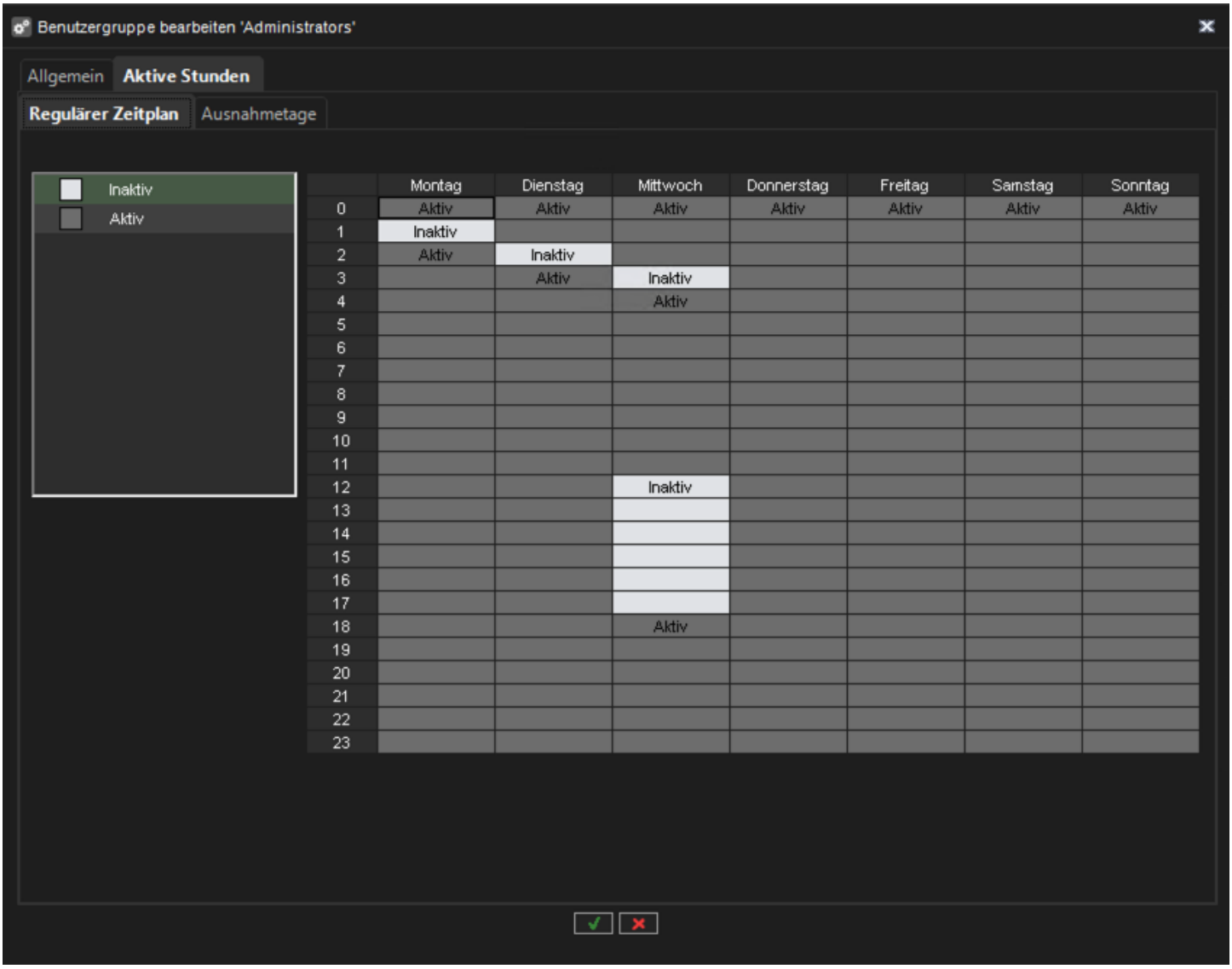
Sie können die Tage und Stunden festlegen, an denen eine bestimmte Benutzergruppe auf Spotter zugreifen kann, um z. B. den Zugriff der Bediener auf Spotter außerhalb der Arbeitszeiten zu kontrollieren.

Gehen Sie zu System-Manager > Benutzer und Benutzergruppen, um den Zugriffszeitplan für Benutzergruppen zu konfigurieren.

12.4.6.1 Regelmäßiger Zeitplan

Auf der Registerkarte Regelmäßiger Zeitplan können Sie einen wöchentlichen Zeitplan festlegen, der bestimmt, wann die Benutzergruppe Spotter verwenden kann oder wann dies verhindert wird.

1. Klicken Sie auf die Benutzergruppe, die Sie bearbeiten möchten.
2. Klicken Sie auf die Registerkarte Aktive Stunden.
3. Standardmäßig sind alle Stunden des Tages aktiv.
4. Um den Zugriff während bestimmter Stunden zu verhindern:
    a. Wählen Sie Inaktiv links neben dem Wochenplan.
    b. Klicken Sie auf die Stunden, in denen die Benutzergruppe keinen Zugriff auf Spotter haben soll (=Inaktiv).



1. Um eine inaktive Stunde wieder in eine aktive zu ändern, wählen Sie links neben dem Wochenplan die Option Aktiv und klicken Sie auf die Stunde, in der sich die Benutzergruppe bei Spotter anmelden können soll.
2. Wenn der reguläre Zeitplan fertiggestellt ist, klicken Sie auf das grüne Häkchen, um zu speichern.

Wenn ein Bediener einer Benutzergruppe versucht, sich während einer inaktiven Zeit bei Spotter anzumelden, kann er sich nicht anmelden, und es wird die Meldung Unautorisierter Benutzer angezeigt.

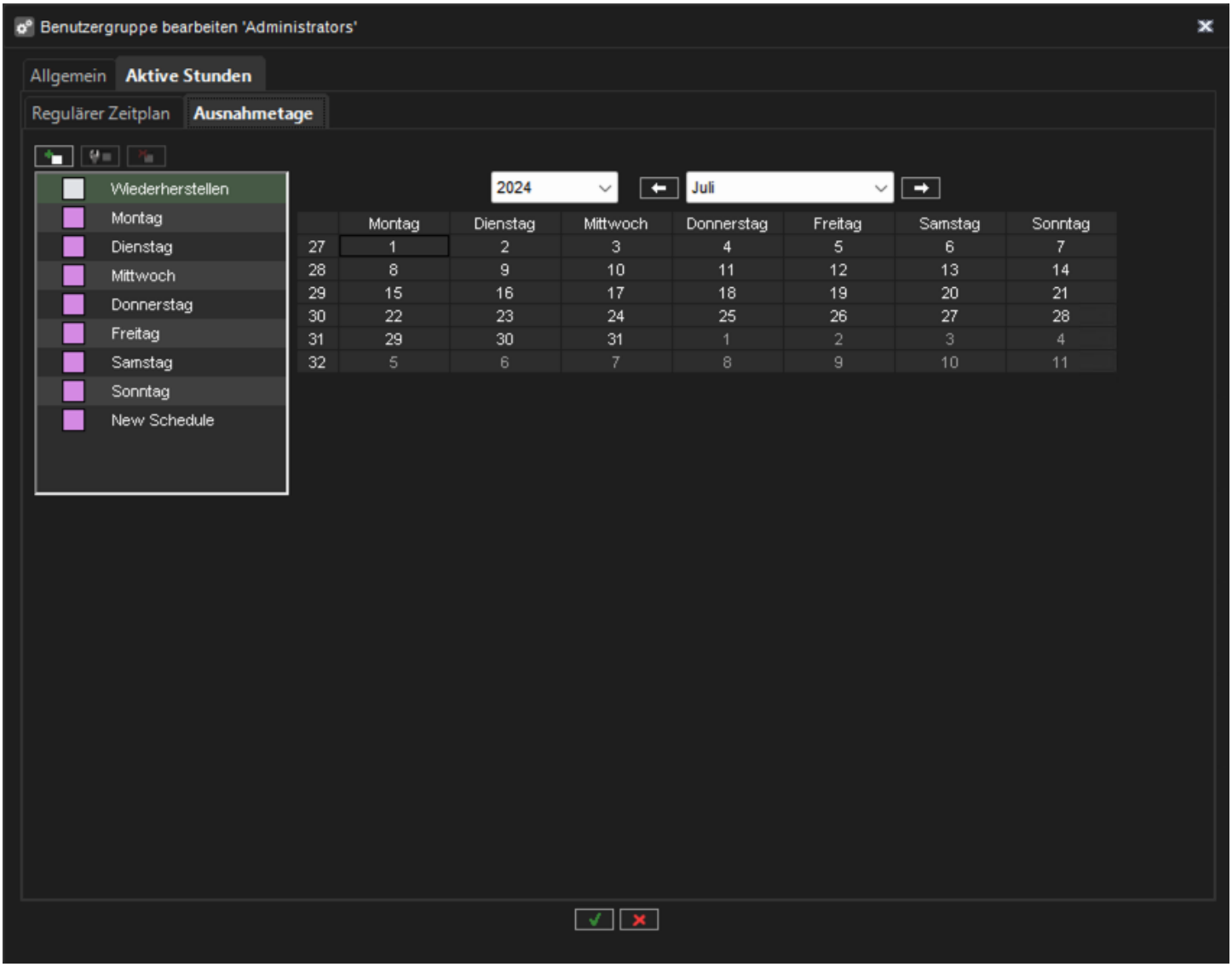


12.4.6.2 Ausnahmetage

Wenn Sie an einem bestimmten Datum einen anderen Zeitplan verwenden möchten, können Sie den regulären Zeitplan für dieses Datum auf der Registerkarte Ausnahmetage überschreiben

Ihr regulärer Terminplan ist für alle Wochentage links im Kalender für Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag und Sonntag verfügbar.

1. Wählen Sie den Monat und das Jahr aus.
2. Wählen Sie den Tag rechts neben dem Zeitplan aus, um den Zeitplan eines anderen Tages zu verwenden, und klicken Sie dann auf das Datum, für das Sie den Zeitplan eines anderen Tages verwenden möchten.



1. Um einen Ausnahmetag zu entfernen, wählen Sie Wiederherstellen und klicken Sie auf das Datum.
2. Klicken Sie auf das grüne Häkchen, um zu speichern.

12.4.6.2.1 Einen neuen Ausnahmetagesplan erstellen

Sie können Ihren Ausnahmeplan auch erstellen, indem Sie auf das +-Zeichen oben links im Plan klicken.

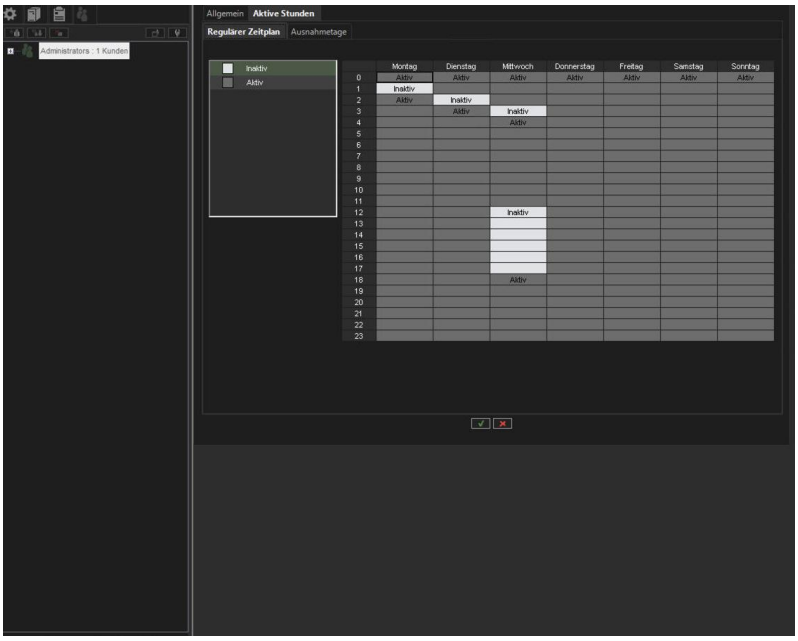
In diesem Ausnahmeplan können Sie auswählen, welche Stunden eine Ausnahme vom regulären Zeitplan sein sollen (Ein) oder nicht (Aus).

1. Wählen Sie "Ein" oder "Aus" und klicken Sie auf die Stunden, in denen der reguläre Zeitplan nicht verwendet wird oder verwendet werden soll.
2. Sie können den Zeitplan unter dem Namen Zeitplan benennen.
3. Speichern Sie es, indem Sie auf das grüne Kontrollkästchen klicken.

Es ist nun bereit für die Verwendung an Ausnahmetagen.

Der Ausnahmeplan kann über das Menü bearbeitet und gelöscht werden:





12.5 Erstellen eines kundenspezifischen Benutzers

So fügen Sie dem System einen neuen Benutzer hinzu:

1. Öffnen Sie die Registerkarte **Benutzer**.
2. Klicken Sie auf den Namen der Benutzergruppe, zu der Sie den Benutzer hinzufügen möchten.
    a. Beachten Sie, dass Sie Benutzer nur zu systemeigenen Gruppen hinzufügen können, nicht zu domänenbasierten Gruppen.
3. Klicken Sie auf Benutzer hinzufügen in der oberen linken Ecke der Registerkarte Benutzer. Das Dialogfeld Benutzer hinzufügen wird angezeigt.

4. Mach Folgendes:
    a. Geben Sie einen Namen für das Konto in das Feld **Benutzername** ein.
    b. Um dem Konto ein Passwort hinzuzufügen, klicken Sie auf **Passwort ändern** und geben Sie das Passwort zweimal ein.
    c. Geben Sie eine optionale Beschreibung zum Benutzerkonto ein.
    d. Wählen Sie über das Pulldown-Menü die Benutzergruppe aus, der Sie den Benutzer zuordnen möchten.
    e. Wählen Sie die Sprache der Benutzeroberfläche für den Benutzer aus.
    f. Legen Sie Schutzeinstellungen für die Programme fest:
        i. **Benutzeroberfläche auf Schloss ausblenden**
        ii. **AutomatischeSperre**
        iii. **Automatische Abmeldung**
        iv. **Wartezeit**: Wenn der Benutzer das Programm für die angegebene Zeit nicht verwendet, wird das Programm gesperrt oder der Benutzer abgemeldet.

Hinweis: Benutzer können ihre Passwörter und die Sprache der Benutzeroberfläche im Spotter-Programm ändern.

12.5.1 Identifizierung der Benutzer durch einen von der Anmelde-ID getrennten Benutzernamen

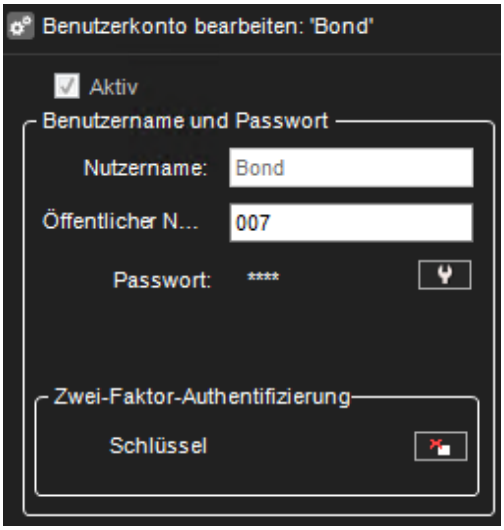
Um die Sicherheit der Plattform zu verbessern, können die Benutzer durch einen separaten Benutzernamen identifiziert werden, damit die Anmelde-ID des Benutzers nicht angezeigt wird.

Der Systemadministrator kann in den Benutzereinstellungen des Systemmanagers einen öffentlichen Namen für Benutzer festlegen. Der öffentliche Nutzername sollte eindeutig sein. Dies ist nicht zwingend erforderlich, und das Feld kann auch leer gelassen werden.

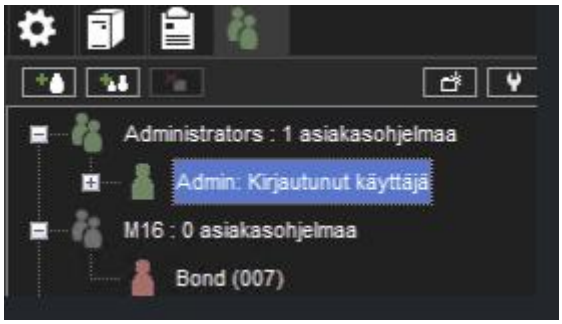
Wie bisher verwendet der Benutzer den Login-Benutzernamen, um sich bei einer beliebigen Anwendung anzumelden. Wenn ein öffentlicher Benutzername für den Benutzer eingegeben wurde, wird dieser öffentliche Benutzername in der Client-Benutzeroberfläche angezeigt.

12.5.2 Hinzufügen eines öffentlichen Benutzernamens im System Manager

1. Gehen Sie in der System Manager Desktop-Anwendung zu Benutzereinstellungen und klicken Sie auf Bearbeiten.
2. Im Feld **Öffentlicher Name** kann der Systemadministrator einen öffentlichen Namen für einen Benutzer angeben:



Dieser Name wird in der Benutzerliste des System Managers angezeigt:

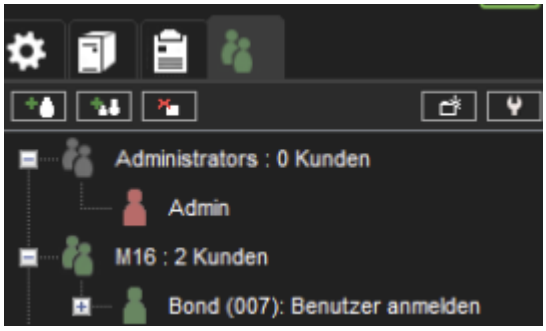


Dieser Name wird in der Benutzerliste des System Managers angezeigt:



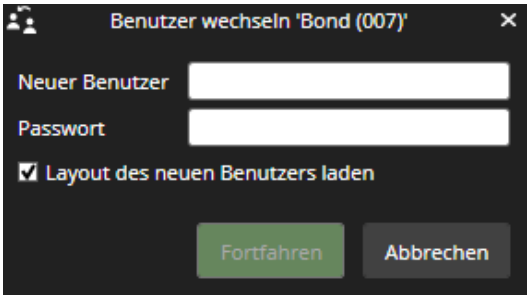
Und auch als angemeldeter Benutzer:



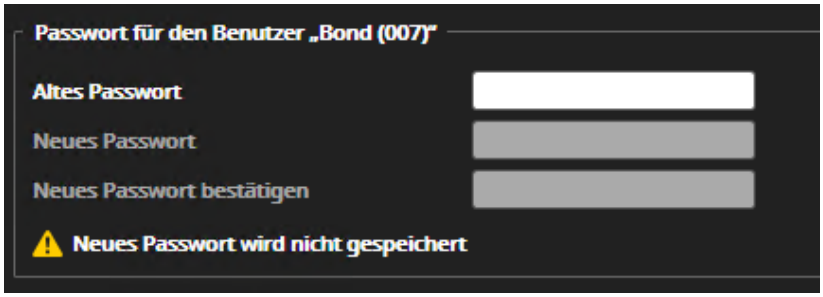


12.5.3 Anzeige eines öffentlichen Benutzernamens für den Benutzer in Spotter

Wenn für einen Benutzer in System Manager ein öffentlicher Benutzername festgelegt ist, wird der öffentliche Benutzername zusammen mit der Benutzeridentität in Benutzer wechseln angezeigt:



Die Benutzer können auch ihren öffentlichen Benutzernamen sehen, wenn sie ihr Passwort ändern:



12.5.4 Öffentlicher Benutzername im Spotter-Web

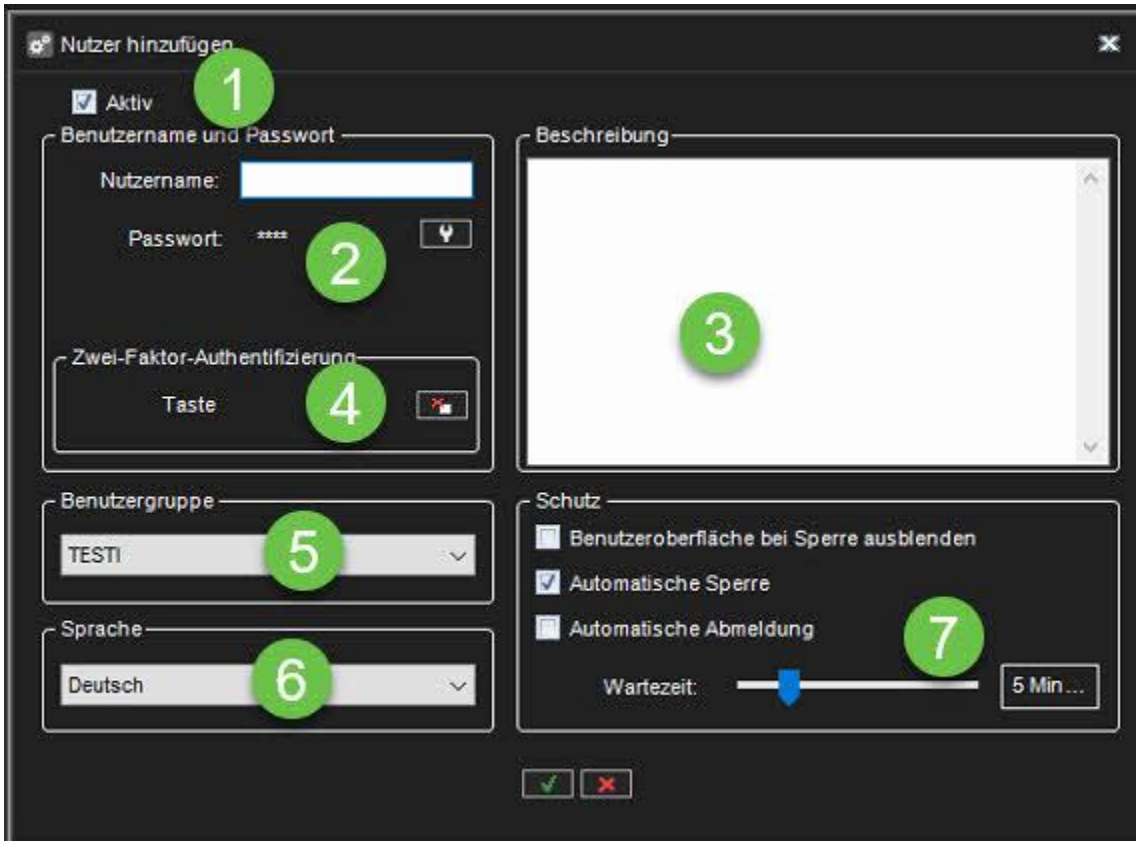
Der öffentliche Benutzername wird in Spotter Web in der oberen rechten Ecke angezeigt, wenn er im System Manager definiert wurde.

Wurde der öffentliche Name nicht definiert, wird der Anmeldename des Benutzers angezeigt.

Wenn der öffentliche Name des Benutzers im System Manager geändert wird, wird der Spotter Web-Benutzer abgemeldet und muss sich erneut anmelden. Nach der Anmeldung wird auf dem Hauptbildschirm ein neuer öffentlicher Name angezeigt. Wurde er im System Manager entfernt, gilt derselbe Vorgang, und nach der Anmeldung wird der Anmeldename des Benutzers angezeigt.

12.6 Die Benutzerkontoeinstellungen enthalten die folgenden Optionen:

- Kontostatus
- Passwort
- Zwei-Faktor-Authentifizierung Schlüsselverwaltung, siehe mehr von Zwei-Faktor-Authentifizierung
- Benutzergruppe
- Sprache
- Schutzeinstellungen



12.7 Deaktivieren oder Aktivieren eines Benutzerkontos

Wenn Sie verhindern möchten, dass sich ein Benutzer am System anmeldet, das Benutzerkonto jedoch für eine spätere Verwendung behalten möchten, können Sie das Konto deaktivieren.

Wenn der Benutzer wieder berechtigt ist, sich am System anzumelden, können Sie das Konto aktivieren.

So deaktivieren oder aktivieren Sie ein Benutzerkonto:

1. Wählen Sie auf der Registerkarte **Benutzer** das Benutzerkonto aus
2. Klicken Sie auf **Benutzerkonto bearbeiten**
3. Führen Sie einen der folgenden Schritte aus:

- **Um das Konto zu deaktivieren, deaktivieren Sie das Kontrollkästchen Active**.
- Um das Konto zu aktivieren, aktivieren Sie das Kontrollkästchen **Active**.

1. Klicken Sie auf **OK**.

Hinweis: *Domänenbasierte (LDAP) Benutzer können mit System Manager nicht gelöscht oder entfernt werden.*

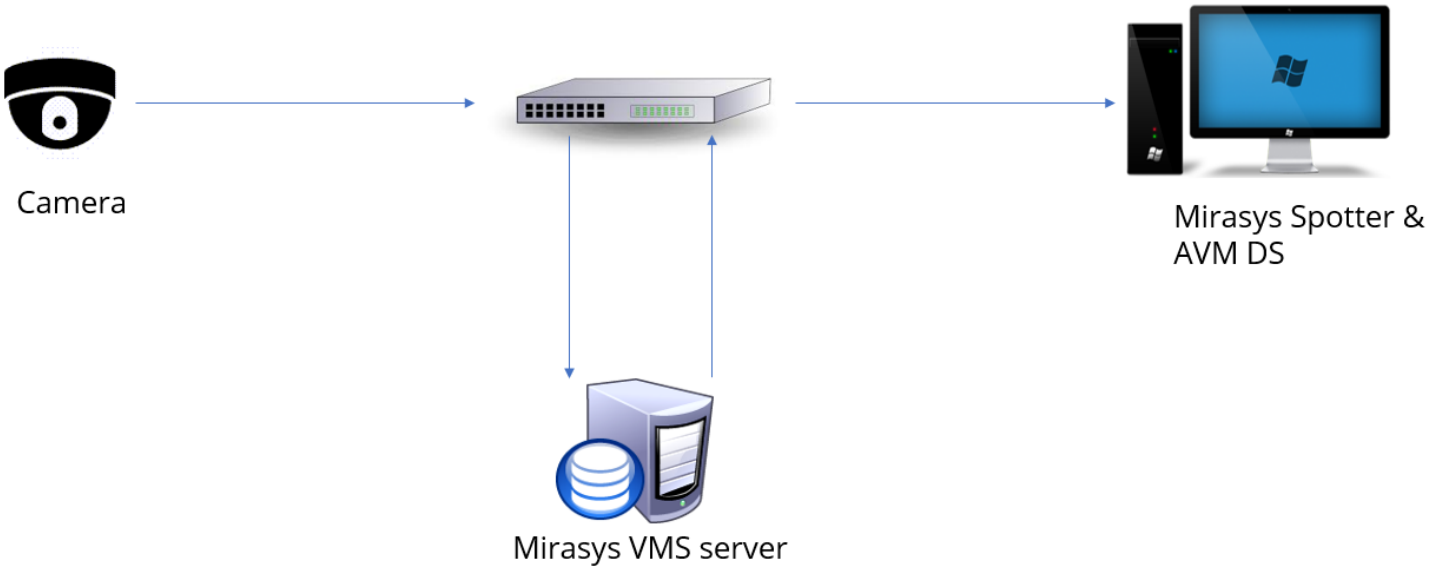
13 ThruCast-Streaming

ThruCast ist die Funktion zum direkten Kamera-Videostreaming in Mirasys VMS.

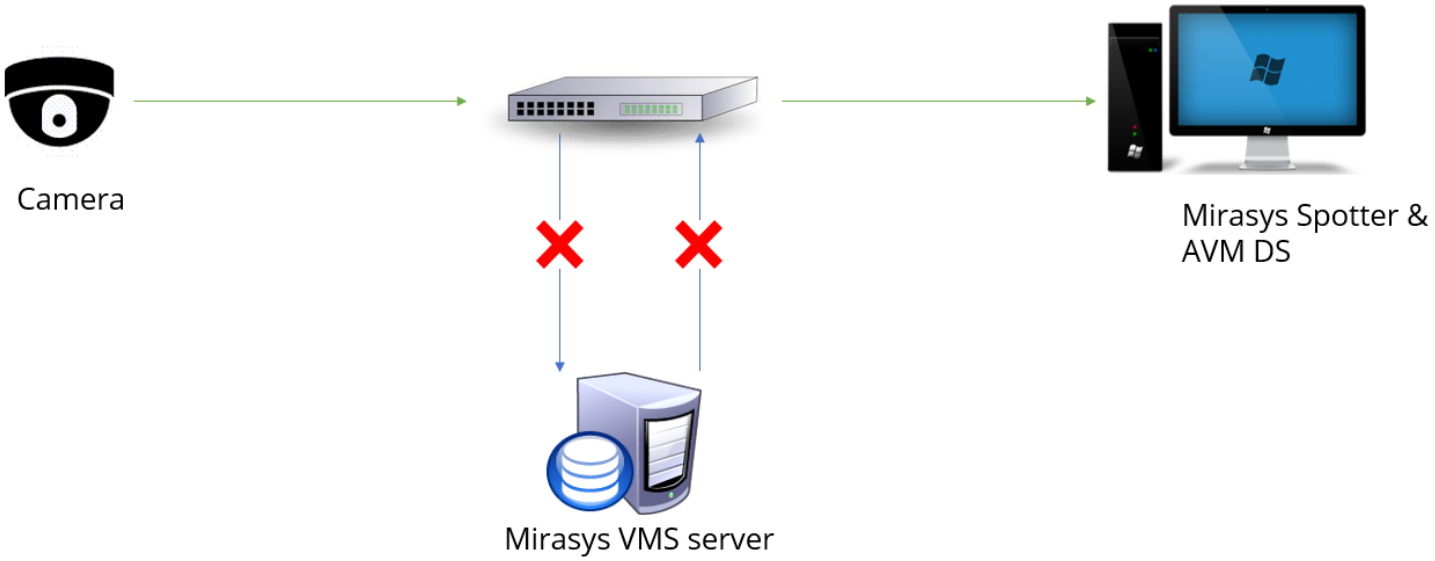
Bei ThruCast kommt der Videostream direkt von der Kamera zum Viewing-Client, der Spotter für Windows-Anwendung.

In einem Standard-Streaming-Szenario kommt der Stream zum Client vom VMS-Server.

13.1 Vom Server zum Client streamen



13.2 Von der Kamera direkt zum Client streamen



Es ist möglich, den direkten Stream von der Kamera zum Client zu erhalten, wenn die VMS-Serververbindung in Ordnung ist. Dies kann nützlich sein, wenn Benutzer die Netzwerkauslastung optimieren möchten.

13.3 Unterstützte Kameras

ThruCast erfordert einen separaten Kamera-Capture-Treiber für den Client.

Derzeit existieren Treiber für folgende Kamerahersteller:

- Acti
- Axis
- Bosch
- Dahua
- Hikvision
- Lilin
- Samsung
- Sony
- Stanley
- ONVIF

Verwenden Sie den ONVIF ThruCast-Treiber für Kameras, die nicht in der Liste der unterstützten Kameras aufgeführt sind.

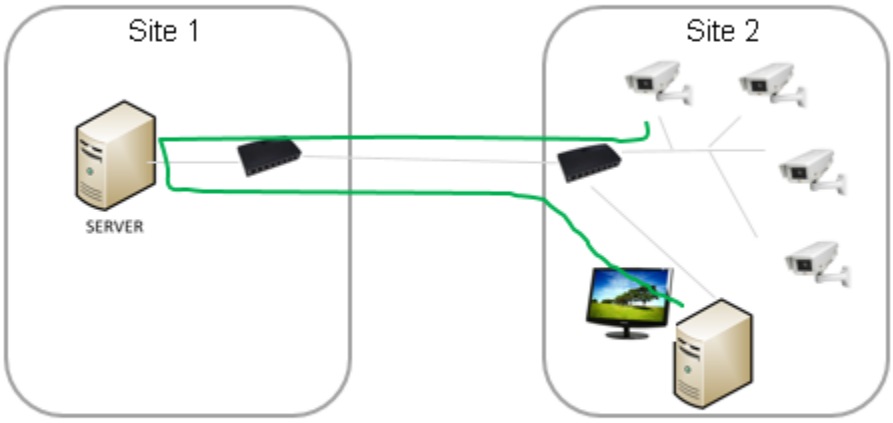
Die Verwendung des ONVIF-Treibers erfordert, dass die Kamera mit dem ONVIF-Treiber zum VMS-System hinzugefügt wird, nicht mit dem nativen Treiber der Kamera.

13.4 NETZWERKOPTIMIERUNG

ThruCast kann verwendet werden, um die Netzwerklast in bestimmten Szenarien zu reduzieren.

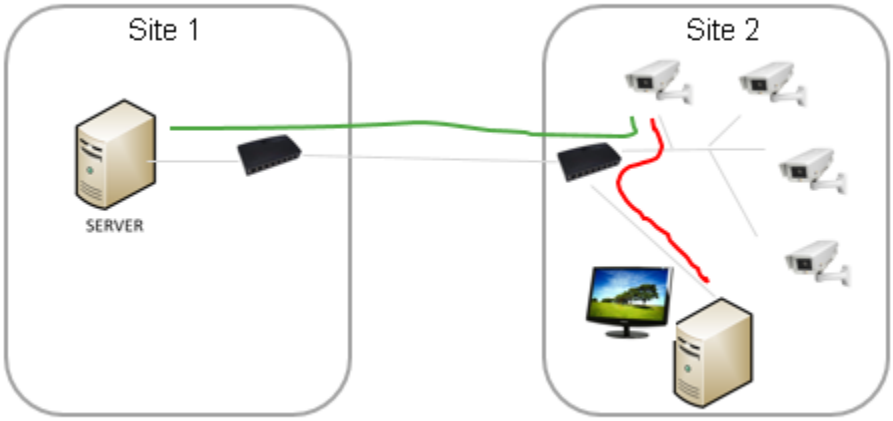
Die Lastreduzierung erfolgt hauptsächlich, wenn sich der Server außerhalb des Standorts (remote) und der Viewing-Client vor Ort (lokal zu den Kameras) befindet.

In Beispielszenario 1 haben wir zwei Standorte, an denen die Aufzeichnung außerhalb des Standorts erfolgt und der Viewing-Client vor Ort ist. Im folgenden Diagramm erfolgt die Anzeige ohne ThruCast, und das Video geht zuerst zum Server und dann vom Server zum Anzeige-Client.



Bei dieser Lösung wird der Verkehr zwischen den beiden Standorten erhöht.

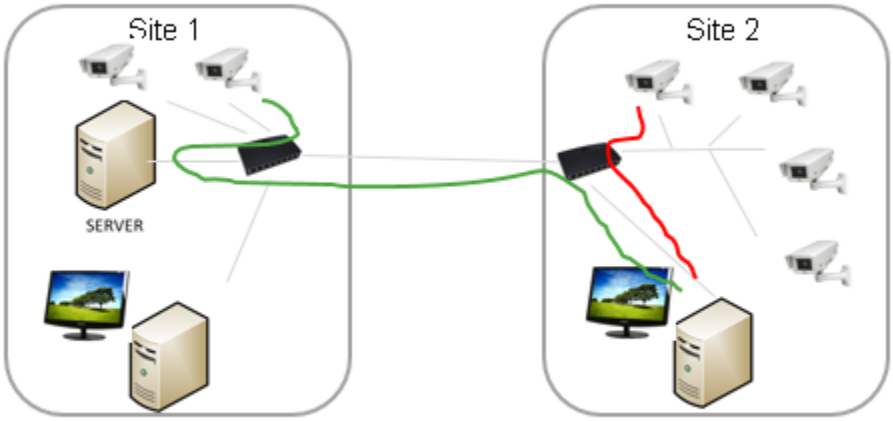
Wenn der Stream mit ThruCast direkt von der Kamera konsumiert wird, wird der Verkehr zwischen den beiden Standorten reduziert.



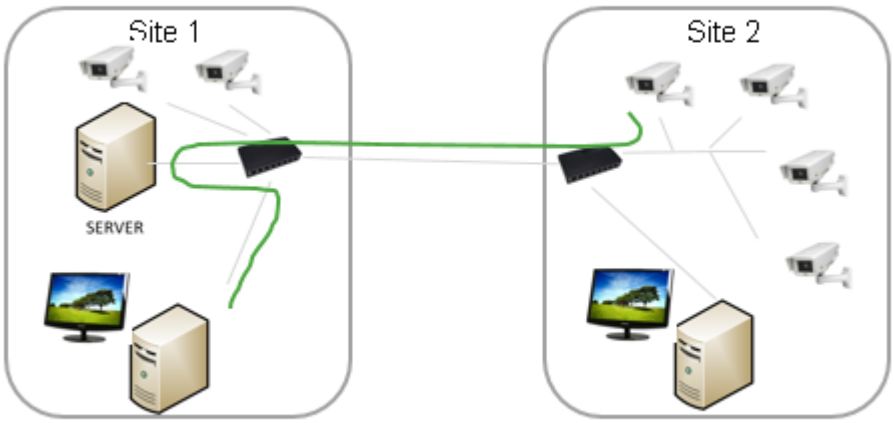
In Beispielszenario 2 befinden sich Kameras an zwei Standorten und anzeigende Clients an zwei Standorten.

Für den Site 2-Anwender ist der Einsatz von ThruCast für die Kameras vor Ort sinnvoller.

Der Benutzer kann wählen, ob ThruCast für alle Kameras oder nur für die Kameras vor Ort verwendet werden soll.



Für den Benutzer von Site 1 reduziert die Verwendung von ThruCast nur den Datenverkehr vom Server zur nächsten Netzwerkverbindung.



Benutzer haben die vollständige Kontrolle darüber, welche Kameras typischerweise von ThruCast verwendet werden.

Die Einstellung wird für jede Kamera und jeden Benutzer gespeichert und in Spotter-Layouts gespeichert.

13.5 Multistreaming und ThruCast für Netzwerkoptimierung und -speicherung

Da es auch möglich ist, für ThruCast einen anderen Stream als den Aufzeichnungsstream zu verwenden, sollte dies bei der Planung der Netzwerkkapazität berücksichtigt werden.

Beispielsweise können Benutzer Live-Bilder mit ThruCast mit einer höheren Bildrate (z. B. 25 fps) anzeigen und immer mit einer niedrigeren Bildrate (z. B. acht fps) aufnehmen.

Dies reduziert den Speicher- und Netzwerkbedarf erheblich.

13.5.1 Auswirkungen von ThruCast auf die Bildverzögerung

Da der ThruCast-Stream nicht zum VMS-Server und zurück wandert, ist die Verzögerung von der Kamera zum Client etwas geringer, aber der Unterschied zum vom Server empfangenen Stream ist nicht groß, nur wenige Millisekunden.

Der Unterschied in der Zweistrom-Mode ist im wirklichen Leben kompliziert zu beobachten.

13.5.2 Von ThruCast Streaming nicht unterstützte Funktionen

ThruCast unterstützt keine PTZ-Steuerung oder Audio

Außerdem unterstützt ThruCast derzeit nur Live-Bilder. Die Wiedergabe (aufgezeichnete Bilder) wird derzeit immer vom Server empfangen.

13.5.3 Lizenzen

ThruCast erfordert die VMS-Lizenz, damit die ThruCast-Funktion und die ThruCast-Client-Treiberkennungen verwendet werden.

Diese ThruCast-Treiberlizenzen und die ThruCast-Funktion sind in der Produktversion Mirasys V9 immer aktiviert.

13.5.4 Mehrere Zuschauer

Da jeder ThruCast-Viewer einen individuellen neuen Stream von der Kamera zum Client öffnet, sollten Anwender testen, wie viele Streams zuverlässig von den verwendeten Kameras geöffnet werden können. In der Praxis funktionieren normalerweise 3-5 Streams ok.

13.5.5 Client-Treiber installieren

Vor der Verwendung von ThruCast müssen die erforderlichen Client-Treiber mit der System Manager-Anwendung installiert werden, wenn sie nicht mit der ursprünglichen Systeminstallation installiert wurden.

Die Client-Treiberpakete sind im gesamten Setup-Paket von Mirasys verfügbar. Sie werden mit der Dateinamenerweiterung „.sdi“ benannt.

Diese Treiber werden auf der ersten Seite der System Manager-Anwendung installiert, „Client-Treiber installieren“.

Die neuen Treiber können hinzugefügt werden, indem Sie auf die Schaltfläche „Neuen Client-Treiber installieren“ klicken und die SDI-Pakete auswählen.

Klicken Sie anschließend auf die Schaltfläche „OK“.

Nach der Installation der Treiber müssen diese noch auf die anzeigenden Spotter-Clients heruntergeladen werden. Dies geschieht, wenn der Spotter vom Desktop aus neu gestartet wird.

Nachdem Spotter die neuen Treiber heruntergeladen hat, ist das System für die Verwendung von ThruCast bereit.

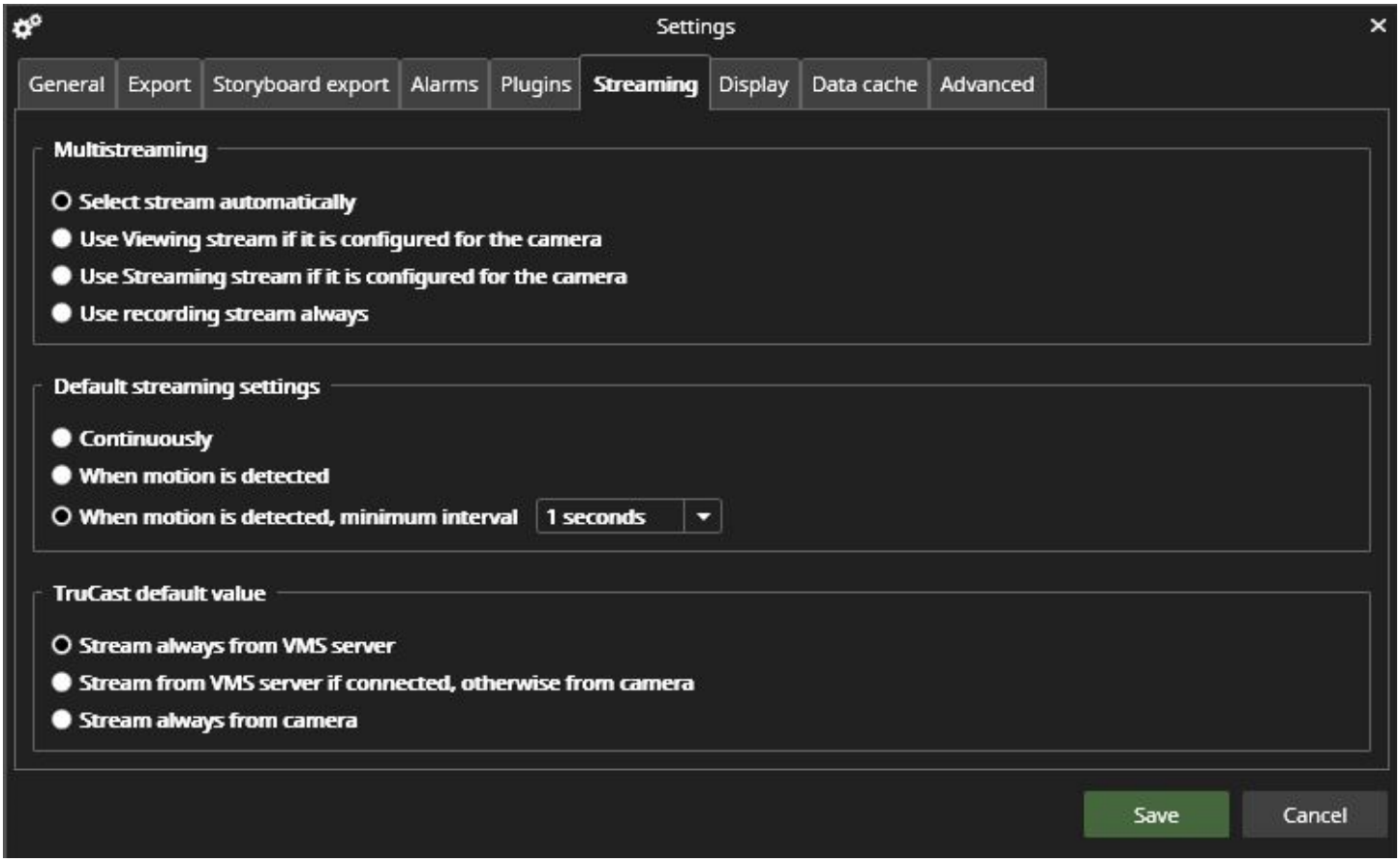
Bitte beachten Sie, dass nur die Kameras, deren Client-Treiber installiert wurde, als ThruCast aktiviert angezeigt werden.

13.5.6 Multi-Streaming konfigurieren

ThruCast kann jeden Stream von der Kamera, der Aufzeichnung, Live-Anzeige oder Remote-Streams verwenden.

Das Multi-Streaming wird normalerweise im System Manager - Kameras aktiviert und konfiguriert.

In den Spotter-Client-Einstellungen - Streaming - Multi-Streaming kann der Benutzer auswählen, welcher der Streams zum Anzeigen verwendet wird. Dieselbe Einstellung wird für die Standard- und ThruCast-Anzeige verwendet.



13.5.7 ThruCast-Standardeinstellung

Die Standardeinstellung für alle Kameras, die noch nicht für ThruCast verwendet wurden, kann in den Spotter-Einstellungen - Streaming - ThruCast-Standardwert definiert werden.

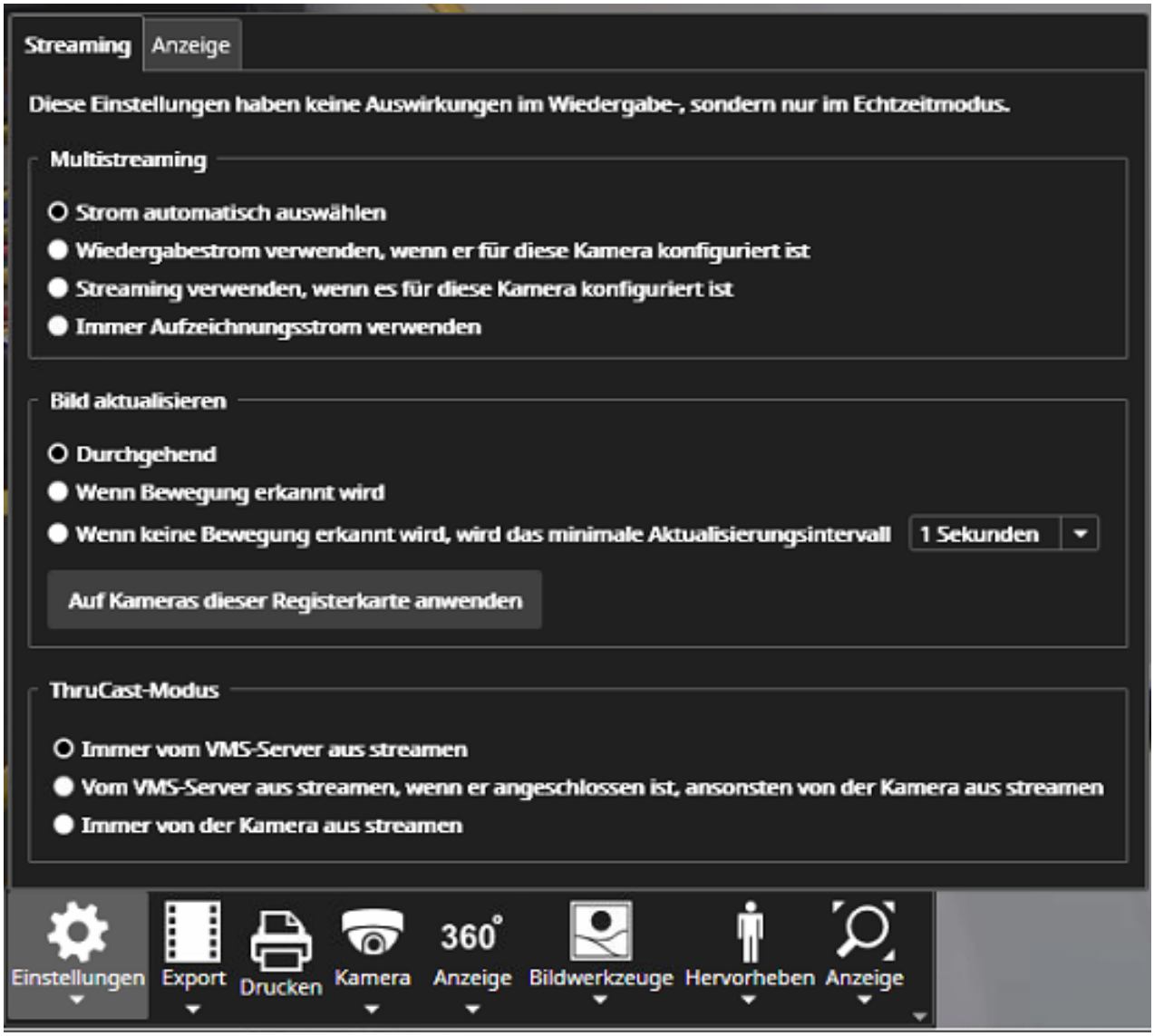
Die möglichen Werte sind

- Immer vom VMS-Server streamen
- Streamen Sie normal vom VMS-Server, wechseln Sie jedoch zu ThruCast, wenn die Verbindung zum Server unterbrochen wird
- Immer mit ThruCast streamen

13.6 Verwenden von ThruCast

Der Benutzer kann die Kameras mit ThruCast Capability über die Kamera-Symbolleiste – Einstellungen – sehen.

Für Kameras mit ThruCast ist die Einstellung verfügbar.



Bei Kameras ohne ThruCast ist der untere Teil des Dialogs deaktiviert.

Die Einstellung wird für jede Kamera separat gespeichert.



Wenn ThruCast aktiv ist, wird oben über der Kamera im Gerätebaum ein kleiner Pfeil angezeigt.

14 Failover-Server

Mirasys VMS unterstützt Failover-Videoserver als Mirasys VMS-Option.

Failover-Server sind VMS-Server im passiven Standby-Modus, bis das System erkennt, dass einer der aktiven Videoaufzeichnungs-VMS-Server ausgefallen ist; An dieser Stelle tritt ein Failover-Server an die Stelle des defekten Servers.

Der ausgefallene Server kann repariert und als neuer Failover-Server ersetzt werden, während der an seine Stelle getretene Failover-Server als aktiver Server weiterarbeiten kann.

***Hinweis**: Wenn ein Failover-Server einen aktiven Server ersetzt, sind alle nicht integrierten Spotter-Plugins (wie Grafana oder List Management Application) nicht im Switch enthalten und müssen nach einer Serverwiederherstellung manuell neu installiert werden.*

Aufzeichnungs- und Failover-Server sollten ein ähnliches Hardware-Setup aufweisen und die Zuweisungen von Laufwerksbuchstaben und Versionsnummern gemeinsam nutzen.

14.1 Failover-Funktionalität

Beim Hinzufügen eines neuen Servers zum System kann der Administrator auswählen, ob der hinzugefügte Server ein Standardserver oder ein Failover-Server ist.

Es kann eine beliebige Anzahl von Failover-Servern (0-n) geben.

Wenn der Server der Standardserver ist, kann der Administrator wählen, ob dieser bestimmte Server zur Failover-Überwachung hinzugefügt wird, d. h. bei einem Serverausfall (Hardware oder Software) wird dieser Server auf den verfügbaren Failover-Server migriert.

Es ist wichtig zu beachten, dass der Hauptserver auf einer anderen Hardware installiert werden muss als auf derjenigen, die mit Aufzeichnungslizenzen oder Failover-Lizenzen betrieben wird.

Das minimale Hardware-Setup besteht aus drei Servern: einem Hauptserver, einem VMS-Server für die Videoaufzeichnung und einem Standby-Failover-Server.

Die Failover-Migration wird unter den folgenden Bedingungen ausgelöst:

- Der Hauptserver hat die Verbindung zu einem VMS Server verloren und das vom Administrator eingestellte Timeout ist erreicht
- Ein VMS-Server hat dem Hauptserver mitgeteilt, dass die Verbindung zu allen Materialplatten (Aufzeichnungsspeicher) auf dem Server fehlgeschlagen ist
    - Eine manuelle Datenwiederherstellung von Serverfestplatten kann versucht werden, wenn die Festplatten noch funktionsfähig sind
- Der Watchdog-Dienst eines Servers hat den Hauptserver darüber informiert, dass er den Aufzeichnungsdienst nicht initialisieren kann

Die Aufzeichnung erfolgt kontinuierlich, nachdem der Failover-Server übernommen wurde, um das System betriebsbereit zu halten.

Die einzige Ausnahme ist die Timeout-Zeit zwischen Trennen und Failover-Trigger. Der Administrator konfiguriert dies.

Nachdem ein Failover-Server die Aufzeichnungsrolle eines ausgefallenen Servers übernommen hat, wird automatisch eine Systemsicherung erstellt, um eine neue Baseline festzulegen.

Während des Failover-Wiederherstellungsprozesses und der folgenden Systemsicherung:

- Benutzer können keine manuellen Sicherungsvorgänge durchführen
- Alle folgenden defekten Server werden einer Failover-Warteschlange hinzugefügt

Die Failover-Warteschlange wird behandelt, nachdem die Failover-Wiederherstellung abgeschlossen wurde.

14.2 Mindestanforderungen

- **Hauptserver auf separatem PC installiert**
    - Die Lizenz muss eine automatische Sicherungsfunktion enthalten
    - Die Lizenz muss einen oder mehrere Failover-Server enthalten
- **1 Subserver für Aufzeichnung**

1 Standby-Failover-Server

- Die Lizenz muss mindestens die gleiche Anzahl an Videokanälen enthalten wie der Aufzeichnungs-Subserver
- Materialfestplatte gleicher Größe und zugewiesene Laufwerksbuchstaben

14.3 VMS-Serverrollen

14.3.1 VMS-Serverrolle FAILOVER

Um einen Server als Failover-Server einzurichten, muss ein freier Failover-Lizenzplatz verfügbar sein.

Wenn ein Server als Failover-Server hinzugefügt wird, versetzt der System Manager den Server in den Standby-Modus.

Die Gruppe Failover-VMS-Server zeigt Serververbindungsstatus und allgemeine Servereinstellungen, wenn die Verbindung verfügbar ist.

14.3.2 VMS-Server-Rolle DEFEKT

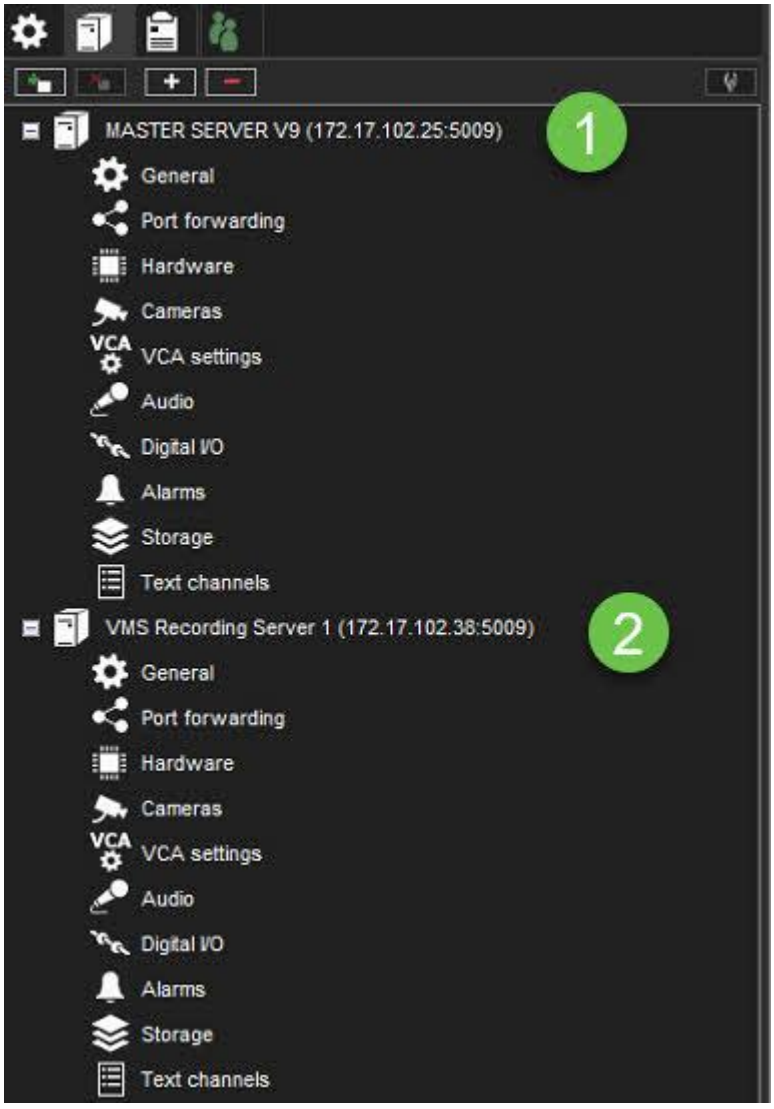
Die Gruppe Defekte VMS-Server zeigt den Verbindungsstatus an; die Einstellungen auf defekten Servern können nicht geändert werden.

Benutzer können jedoch Serverprotokolle exportieren, wenn eine Verbindung zu einem defekten Server besteht.

Um einen defekten Server, der durch einen Failover-Server ersetzt wurde, wieder ins System zu bekommen, muss dieser zunächst manuell entfernt und anschließend als neuer Server wieder hinzugefügt werden.

14.4 STARTING POINT

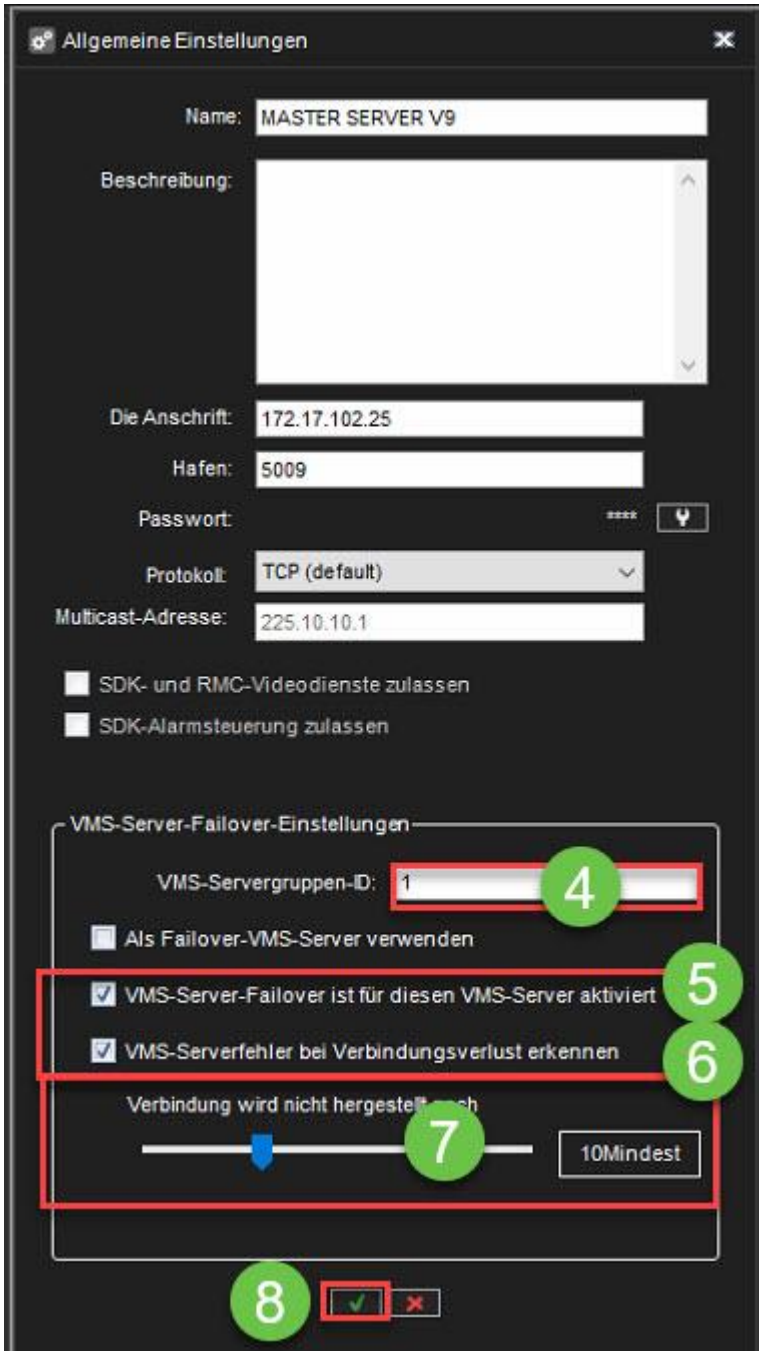
Der Hauptserver und 1 Aufzeichnungs-Subserver wurden dem System hinzugefügt



14.4.1 Aktivieren des VMS-Failover-Servers zum Aufzeichnungsserver

1. Öffnen Sie die Registerkarte **VMS-Server**
2. Wählen Sie den Subserver aus der Liste aus

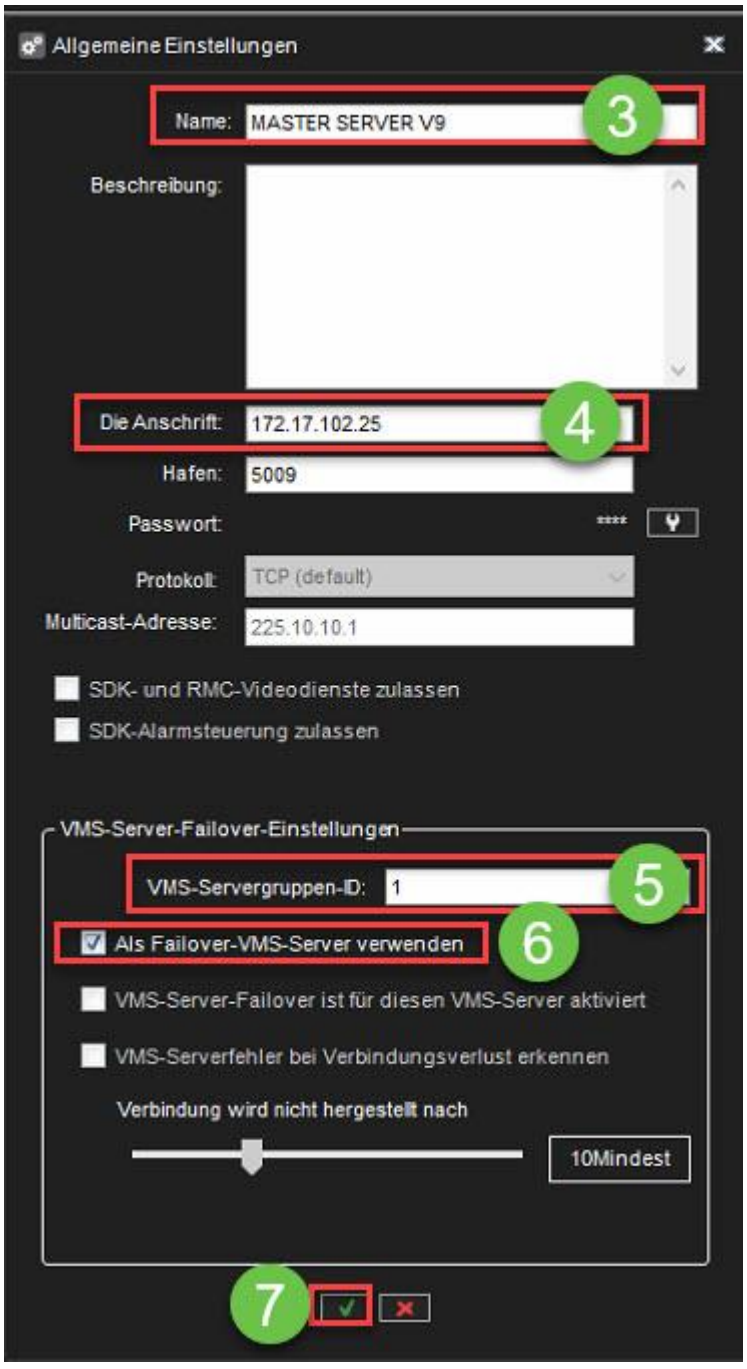
3. Klicken Sie auf **Allgemein**
4. Definieren Sie **VMS-Servergruppen-ID (Standard 1)**
5. Aktivieren **VMS-Server-Failover ist für diesen VMS-Server aktiviert**
6. Aktivieren Sie **Erkennen von VMS-Serverfehlern bei Verbindungsverlust**
7. **Definieren Sie den Wert Verbindung wird nicht aufgebaut nach**
8. Klicken **OK**



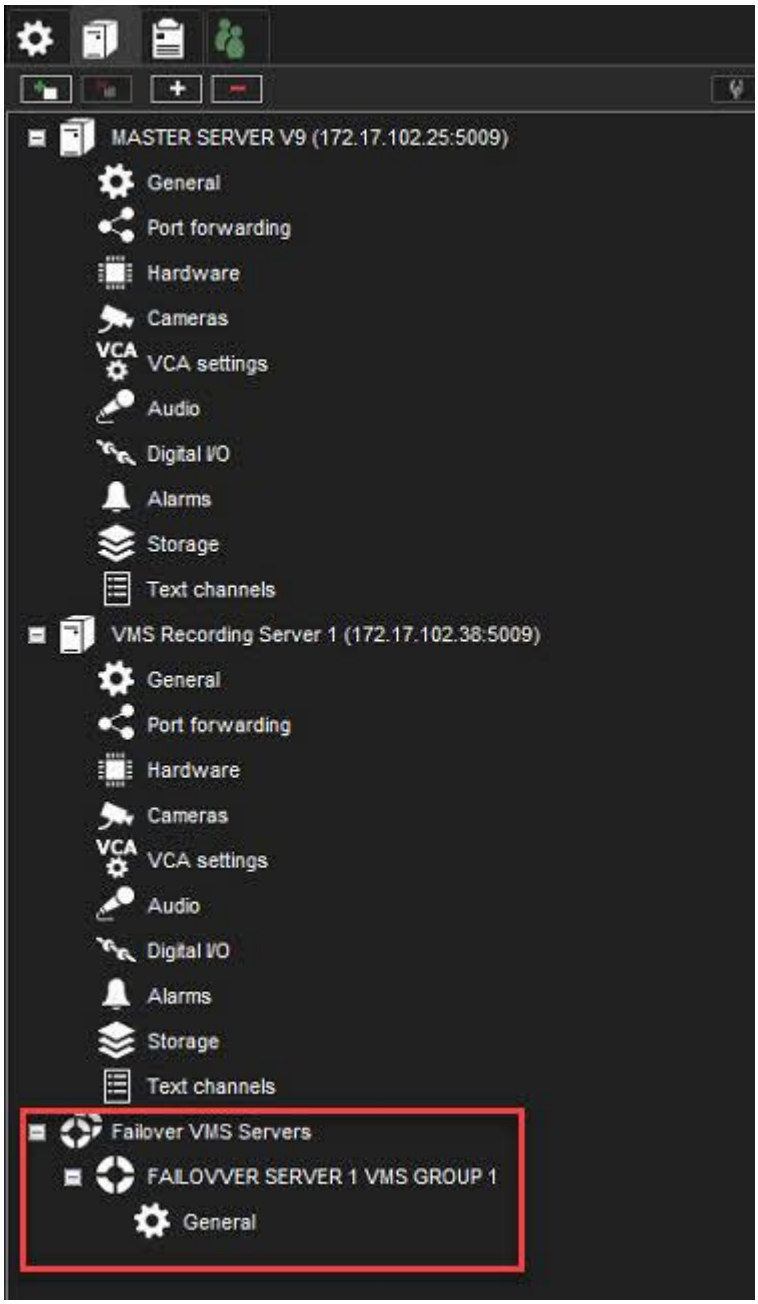
14.4.2 FAILOVER-Server hinzufügen

1. Öffnen Sie die Registerkarte **VMS-Server**
2. Klicken Sie auf **VMS-Server hinzufügen**
3. Legen Sie den Namen für den Server fest

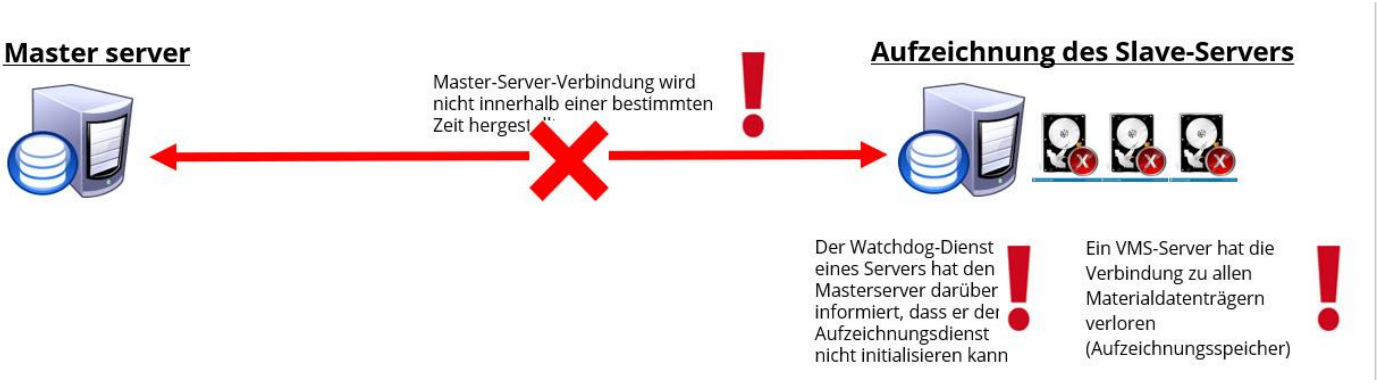
4. Stellen Sie die IP-Adresse des Servers ein
5. Definieren Sie die **VMS-Servergruppen-ID**
6. Aktivieren **Als Failover-VMS-Server verwenden**
7. Click **OK**



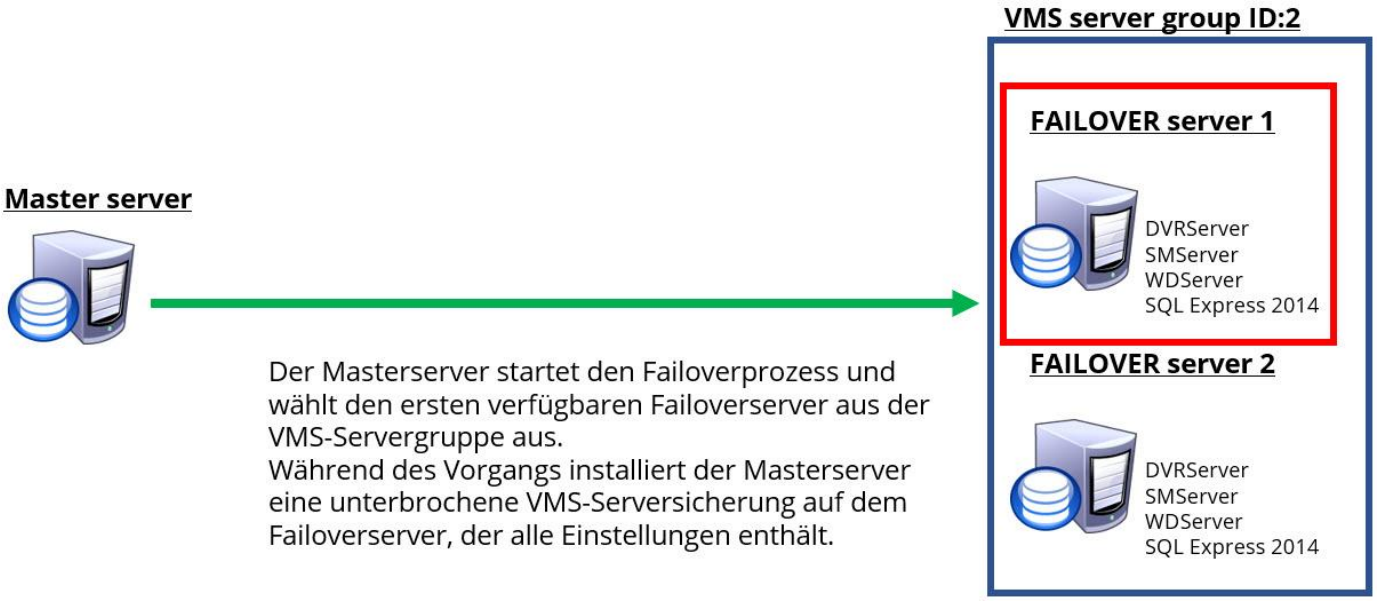
Nach dem Hinzufügen zeigt die Registerkarte VMS-Server die Zeile **Failover VMS Server** an



14.5 FAILOVER-AUSLÖSEBEDINGUNGEN



14.6 FAILOVER-PROZESS



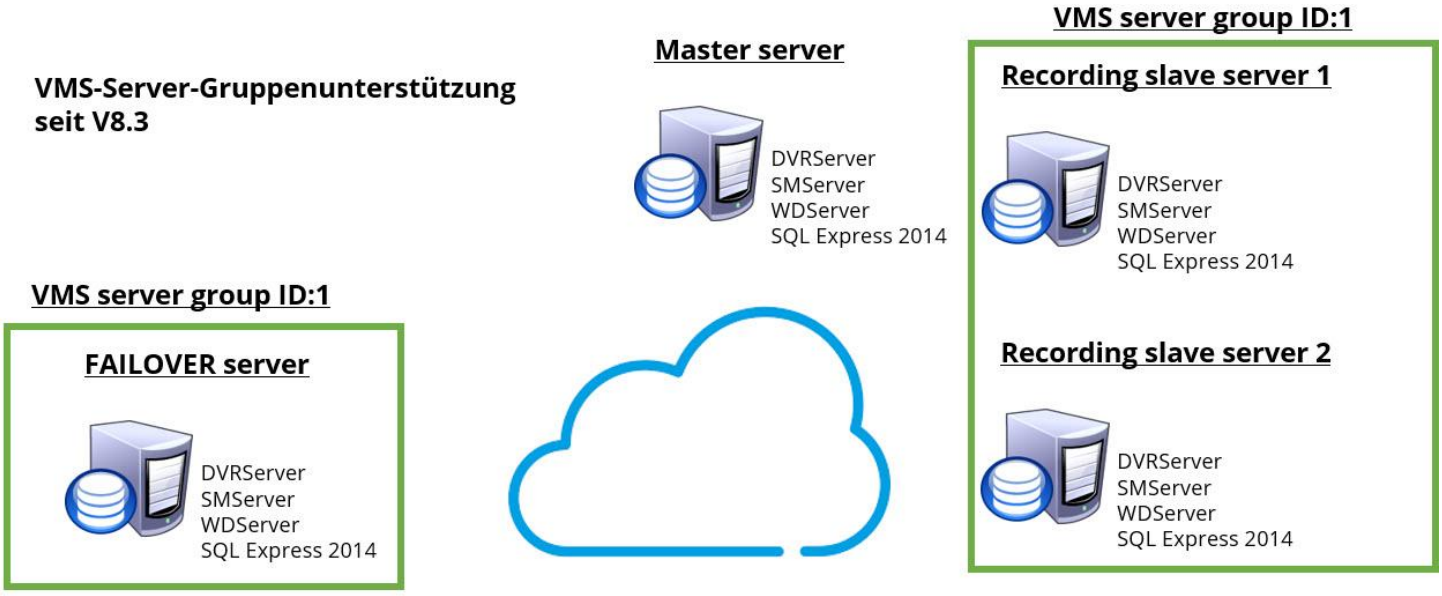
Der Masterserver startet den Failoverprozess und wählt den ersten verfügbaren Failoverserver aus der VMS-Servergruppe aus.
Während des Vorgangs installiert der Masterserver eine unterbrochene VMS-Serversicherung auf dem Failoverserver, der alle Einstellungen enthält.

14.7 MINDESTENSZENARIO FÜR FAILOVER

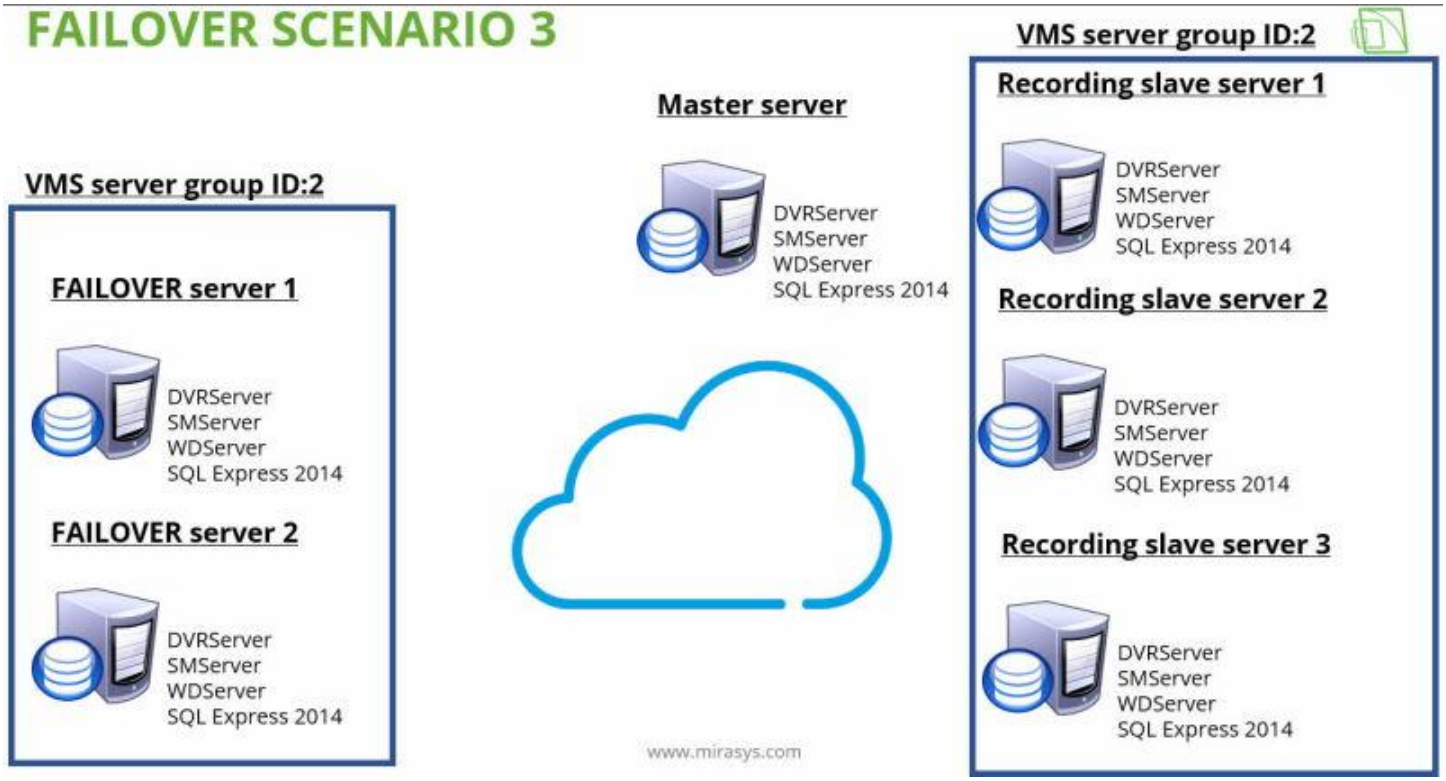


14.8 FAILOVER-SZENARIO 2

VMS-Server-Gruppenunterstützung seit V8.3



14.9 FAILOVER-SZENARIO 3



14.10 Wiederherstellen des festen Servers im System

Die Gruppe Defekte VMS-Server zeigt den Verbindungsstatus an; die Einstellungen auf defekten Servern können nicht geändert werden.

Benutzer können jedoch Serverprotokolle exportieren, wenn eine Verbindung zu einem defekten Server besteht.

Um einen defekten Server, der durch einen Failover-Server ersetzt wurde, wieder ins System zu bekommen, muss dieser zunächst manuell entfernt und anschließend als neuer Server wieder hinzugefügt werden.

14.11 Dauer der Materialkopie nach dem Failback – Testergebnisse

Diese Seite enthält Informationen zum Test der Materialkopie beim Failover des VMS-Servers. Der Test wurde durchgeführt, um die Zeit zu messen, die für das Kopieren der gespeicherten Daten nach einem Failback vom Failover-Server auf den VMS-Server benötigt wird. Die Testergebnisse bieten eine Grundlage für die Abschätzung der Dauer der Materialkopie nach einem Failback.

14.11.1 Testaufbau

Bei der Durchführung der Tests wurden die folgenden VMS-Server verwendet:

- Haupt-VMS-Server – Rechter Windows-11-Rechner mit 64 GB RAM

- Ausgefallener VMS-Server – Virtuelle Maschine mit Windows 11 und 24 GB RAM
- Failover-VMS-Server – Virtuelle Maschine mit Windows 11 und 24 GB RAM

Der ausgefallene VMS-Server verwendete Kameraemulatoren, um die gespeicherten Daten in jedem Testszenario ähnlich zu halten. Die Server nutzten das dedizierte Laufwerk (Laufwerk D:\) für die Speicherung, und das Laufwerk wurde vor der Ausführung jedes Testszenarios gelöscht. Die verwendeten Server waren an ein 1-GB-Netzwerk angeschlossen.

14.11.2 Testergebnisse

Die Dauer des Materialkopiervorgangs wurde aus den Protokollen des VMS-Servers (C://Program Files/DVMS/DVR/Logs/DVRl.og.txt) erfasst.

Die folgende Tabelle enthält Informationen zu den Testergebnissen der Materialkopie mit folgenden Angaben:

- Dauer des Failovers
- Anzahl der verwendeten Kameras
- Größe des Materials, das auf den ausgefallenen Server zurückkopiert wurde
- Dauer in Minuten für eine Materialkopie vom Failover-Server auf den VMS-Server

Dauer des Failovers	**Kopieren von Material**									
	1 Kamera		**5 Kameras**		**10 Kameras**		**15 Kameras**		**20 Kameras**	
	GB	**Minuten**	**GB**	**Minuten**	**GB**	**Minuten**	**GB**	**Minuten**	**GB**	**Minuten**
1 Stunde	1,4	6	7	13	14	20	22	33	29	40
5 Stunden	7	13	35	65	70	130	105	185	140	250
10 Stunden	14	26	70	130	140	260	210	390	280	500
15 Stunden	22	39	105	195	210	390	315	575	420	750

15 KURZANLEITUNG FÜR MIRASYS VMS

1. Anmeldung bei Mirasys System Manager
2. Ändern der Sprache der Benutzeroberfläche
3. Hinzufügen von IP-Kameras zum System
4. Überprüfen des Referenzbildes

5. Benennen der Kameras und Konfigurieren von Auflösung und Bildrate
6. Testen der Bewegungserkennung
7. Konfigurieren der Bewegungserkennung
8. Konfigurieren von Bewegungserkennungsmasken im Kalender
9. Konfigurieren der Speichereinstellungen entsprechend den Kundenanforderungen
10. Erstellen eines Profils für den Kunden
11. Erstellen einer Benutzergruppe für den Kunden
12. Erstellen eines Benutzerkontos für den Kunden und Hinzufügen zur Benutzergruppe des Kunden
13. Testen des Benutzerkontos in Mirasys Spotter

15.1 Anmeldung bei Mirasys System Manager

1. Starten Sie den System Manager über das Symbol auf dem Desktop

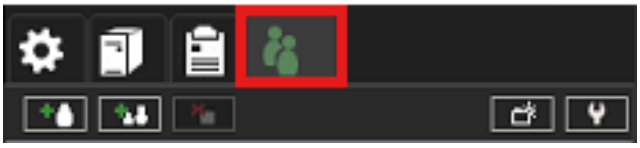


1. Melden Sie sich beim System Manager an: Benutzername: Admin, Passwort: 0308

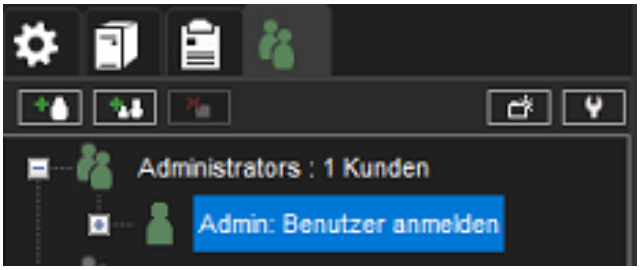


15.2 Ändern der Sprache der Benutzeroberfläche

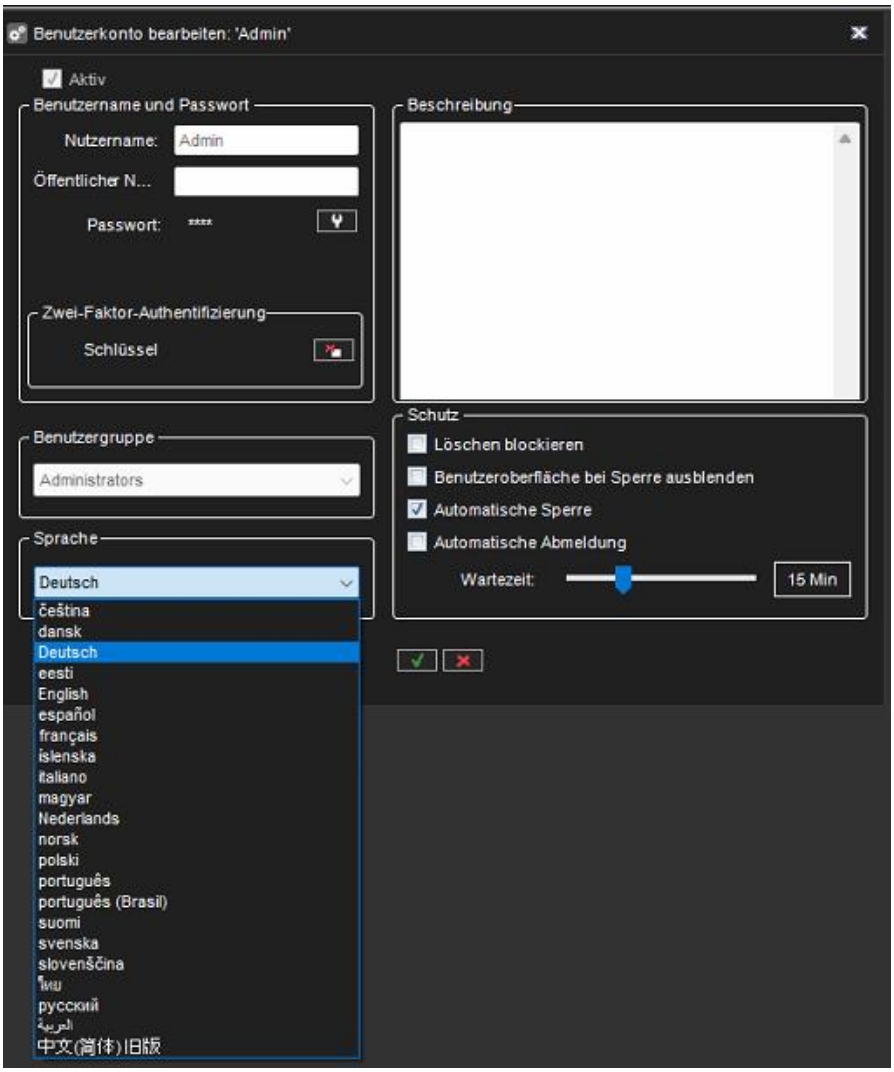
1. Wechseln Sie zur Registerkarte **Benutzer und Benutzergruppen**



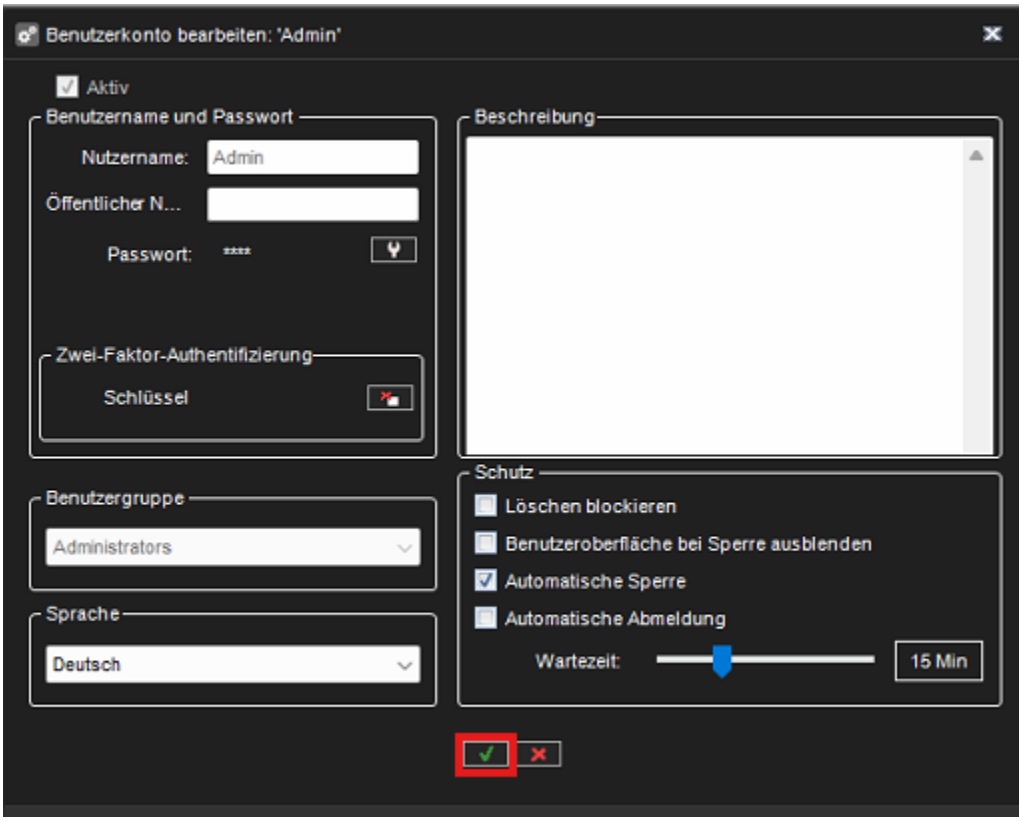
1. Doppelklicken Sie auf den Benutzer **Admin**



1. Wählen Sie „Deutsch“ aus dem Dropdown-Menü aus



1. Bestätigen Sie die Änderungen, indem Sie auf **OK** klicken



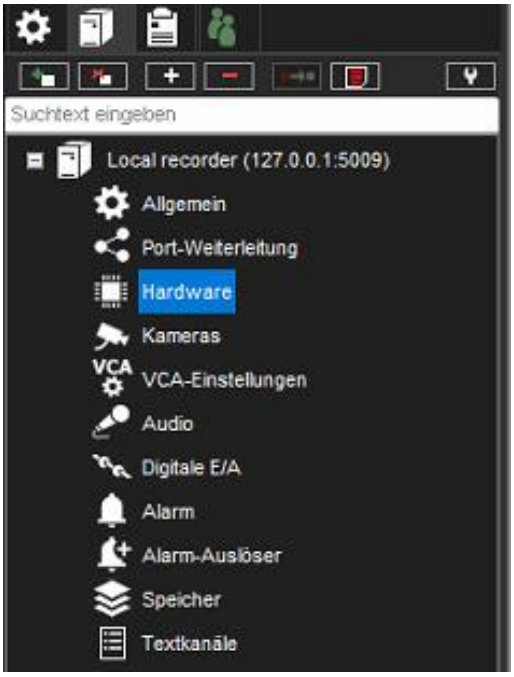
15.3 Hinzufügen von IP-Kameras zum System

Bevor Sie IP-Kameras zum Mirasys VMS-System hinzufügen, überprüfen Sie bitte Folgendes:

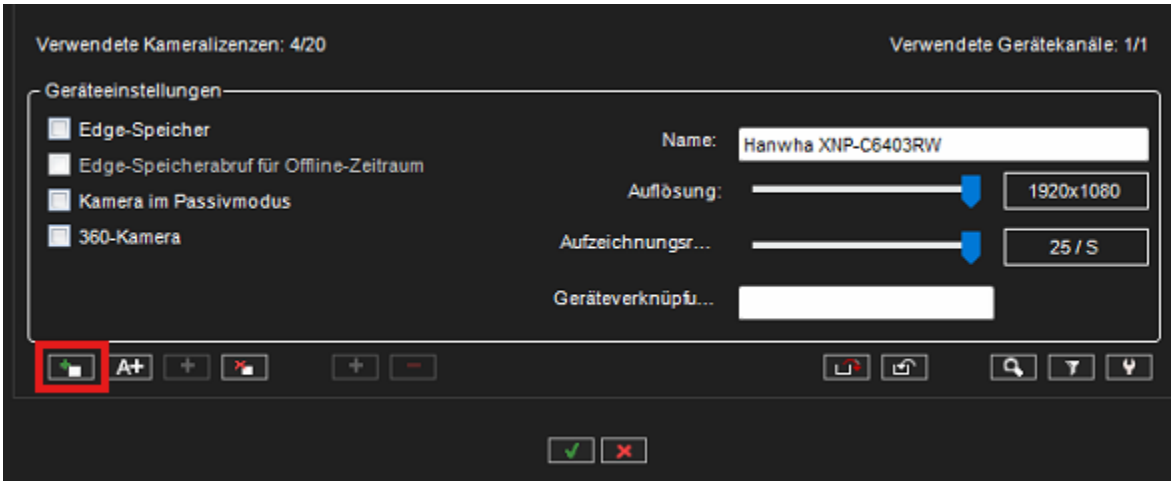
- Stellen Sie sicher, dass Sie die IP-Adressen, Benutzernamen und Passwörter für die Kameras haben, die Sie hinzufügen möchten.
- Vergewissern Sie sich, dass sich der Computer, auf dem die Mirasys VMS-Software installiert ist, im selben Netzwerk wie die IP-Kameras befindet.
- Vergewissern Sie sich, dass die Zeitzone, das Datum und die Uhrzeit auf den IP-Kameras mit denen auf dem Computer übereinstimmen, auf dem die Mirasys VMS-Software installiert ist.

15.3.1 Kameras einzeln hinzufügen

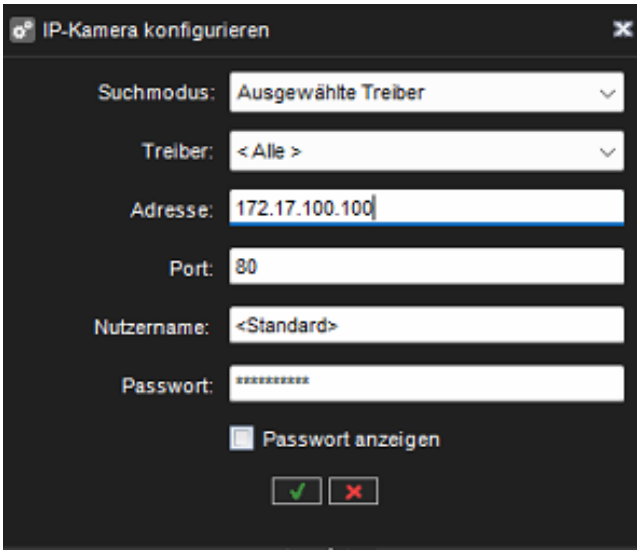
1. Wechseln Sie zur Registerkarte **VMS-Server**
2. Öffnen Sie **Hardware**



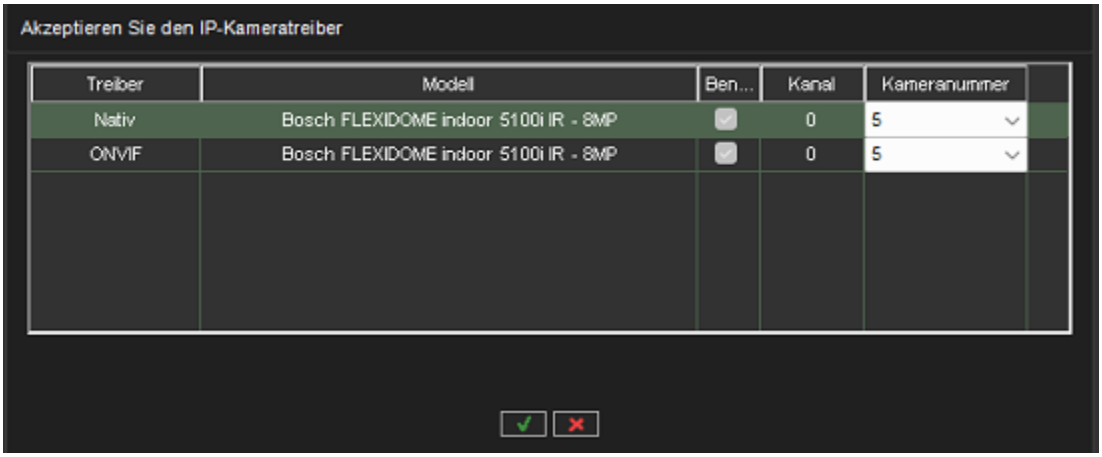
1. Wählen Sie unten links **Gerät hinzufügen**



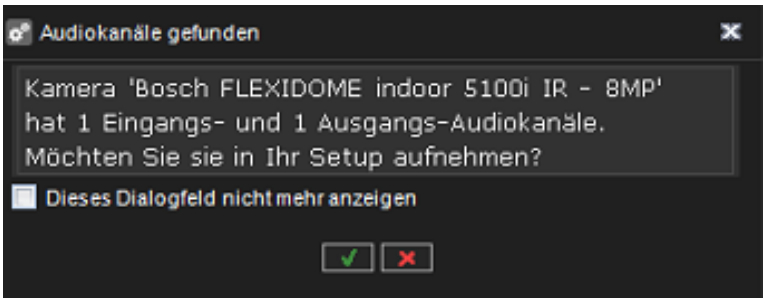
1. Geben Sie die folgenden Informationen ein:
    - IP-Adresse
    - Benutzername
    - Passwort
2. Klicken Sie auf **OK**, um mit dem Hinzufügen einer Kamera zu beginnen



1. Sobald die Kamera erkannt wurde, wählen Sie den **nativen** Treiber aus, falls die Software mehrere Treiber für die Kamera anbietet.
2. Klicken Sie anschließend auf **OK**, um fortzufahren.



1. Der Dialog „Audiokanäle“ wird angezeigt, wenn die Kamera Audiokanäle unterstützt. Wählen Sie **OK** (✓) oder **Abbrechen** (×), je nachdem, ob Sie Audiokanäle aktivieren möchten.



15.3.2 Mehrere Kameras gleichzeitig hinzufügen

Der Kameratreiber muss die Funktion „Autosearch“ unterstützen (siehe die Readme-Datei im ZIP-Paket des Kameratreibers)

1. Wählen Sie **IP-Kamera-Finder**



1. Wählen Sie Kameras aus der Liste aus (Umschalttaste), indem Sie sie markieren
2. Geben Sie den Benutzernamen und das Passwort ein
3. Um Kameras hinzuzufügen, klicken Sie auf **Ausgewählte Kameras hinzufügen**

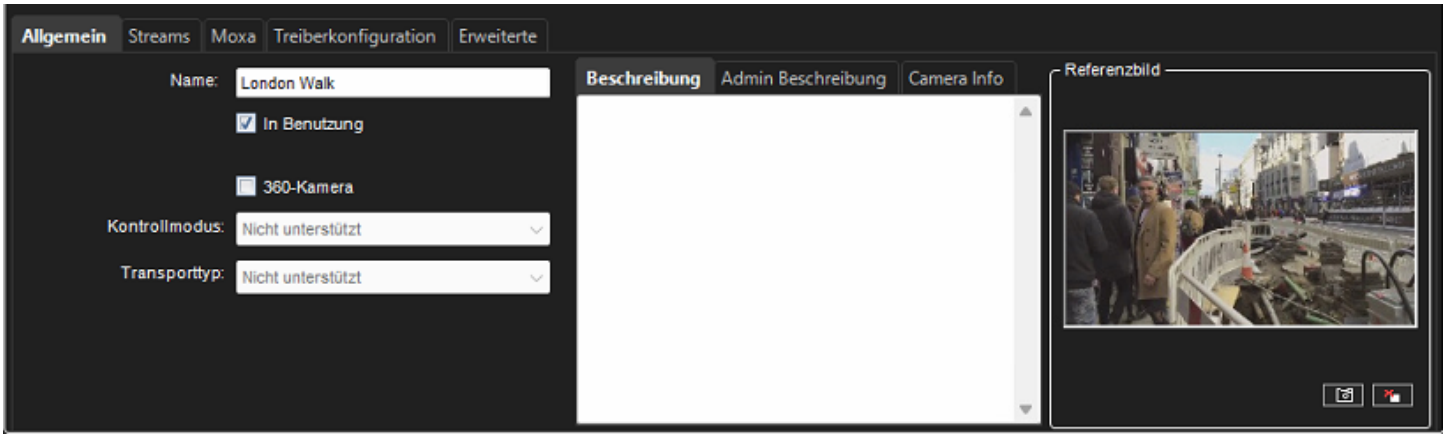


15.4 Überprüfen des Referenzbildes

1. Gehen Sie zu **System Manager** > **VMS-Server** > **Kameras**

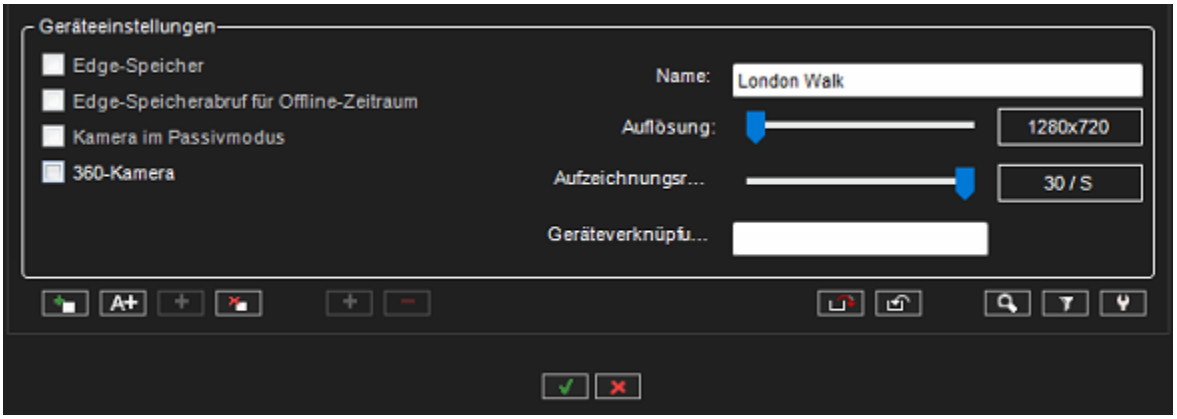


1. Wählen Sie eine Kamera aus der Liste aus
2. Vergewissern Sie sich, dass ein Referenzbild von der Kamera empfangen wird
3. Führen Sie diesen Vorgang für alle Kameras durch



15.5 Benennen der Kameras und Konfigurieren von Auflösung und Bildrate

1. Gehen Sie zu **VMS-Server** > **Hardware**
2. Wählen Sie eine Kamera aus der Liste aus
3. Legen Sie den Namen, die Auflösung und die Aufzeichnungsrate fest
4. Klicken Sie auf **OK**, um die Änderungen zu bestätigen

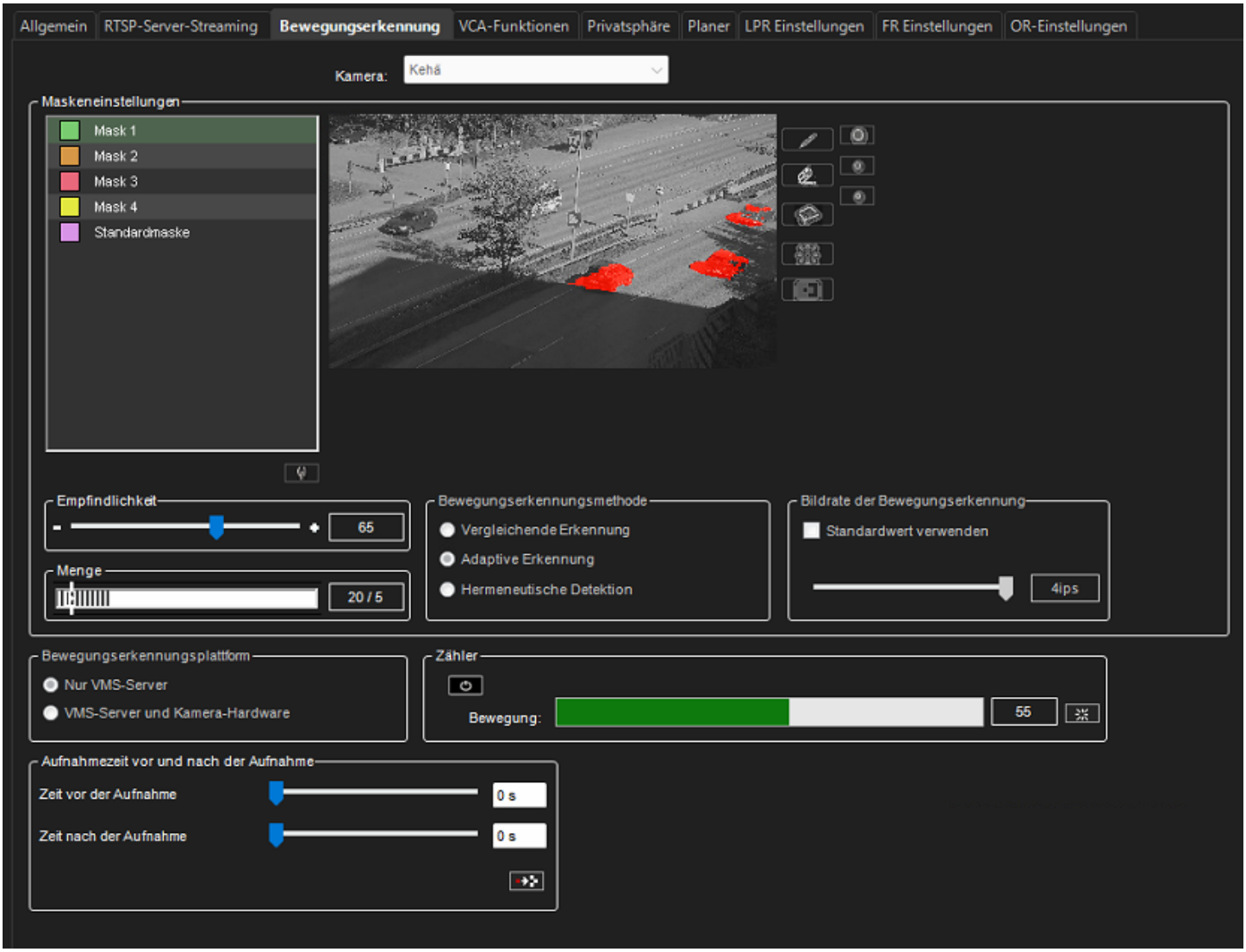


Sie können den Kameranamen, die Auflösung und die Aufzeichnungsrate auch an folgender Stelle ändern:

System Manager > **VMS-Server** > **Kameras** > **Streams**

15.6 Testen der Bewegungserkennung

1. Gehen Sie zu **VMS-Server** > **Kameras**
2. Wechseln Sie zur Registerkarte **Bewegungserkennung**
3. **Zähler** starten
4. Wenn der Zähler aktiv ist, werden in dem Bildfenster die Bereiche, in denen eine Bewegung erkannt wird, rot angezeigt.
5. Wenn der **Schwellenwert** (Anzahl der veränderten Pixel) überschritten wird, nimmt die Mirasys VMS-Software auf. Standard: 5 %
6. Durch Anpassen der Empfindlichkeit und des Schwellenwerts kann jede Kamera individuell konfiguriert werden

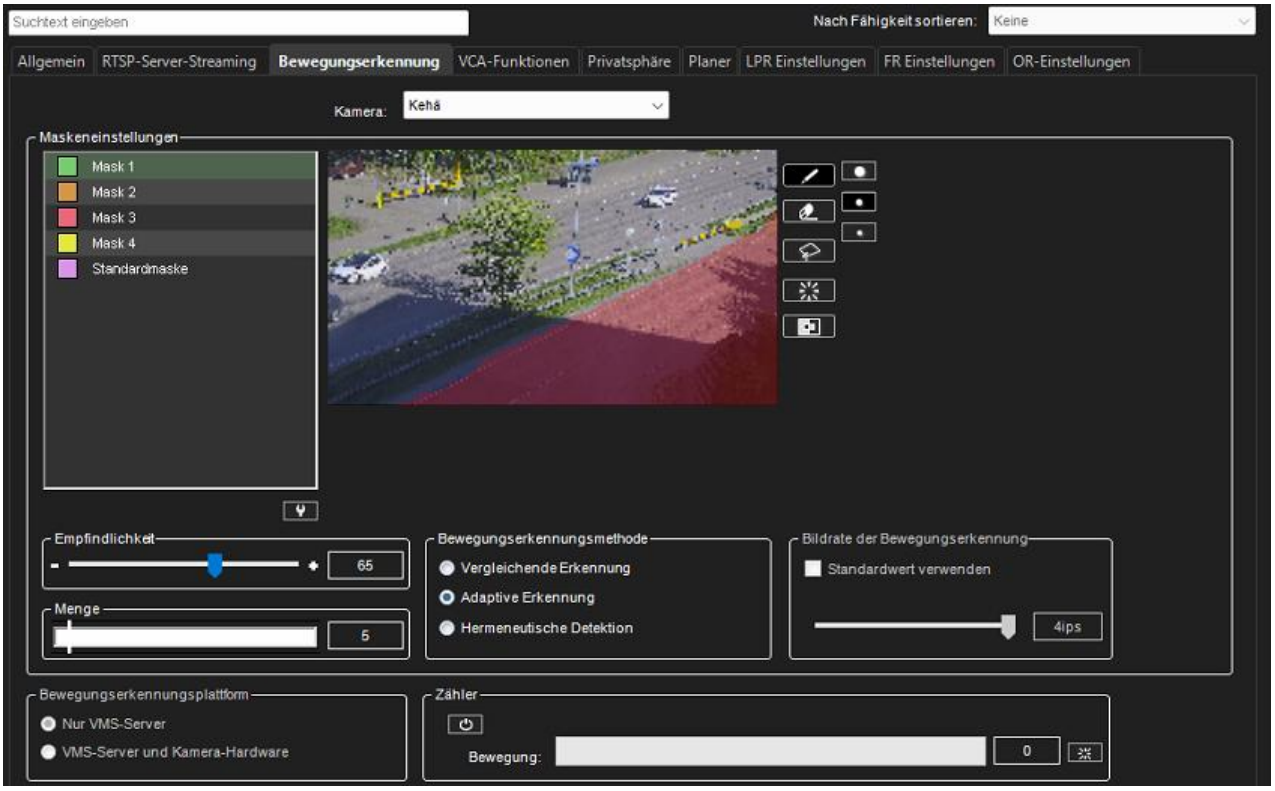


15.7 KONFIGURIEREN DER BEWEGUNGSERKENNUNG

Es ist wichtig, alle Bereiche aus dem Bildausschnitt auszuschließen, in denen die Bewegungserkennung keine Aufzeichnung auslösen soll.

15.7.1 Bewegungserkennungsmasken bearbeiten

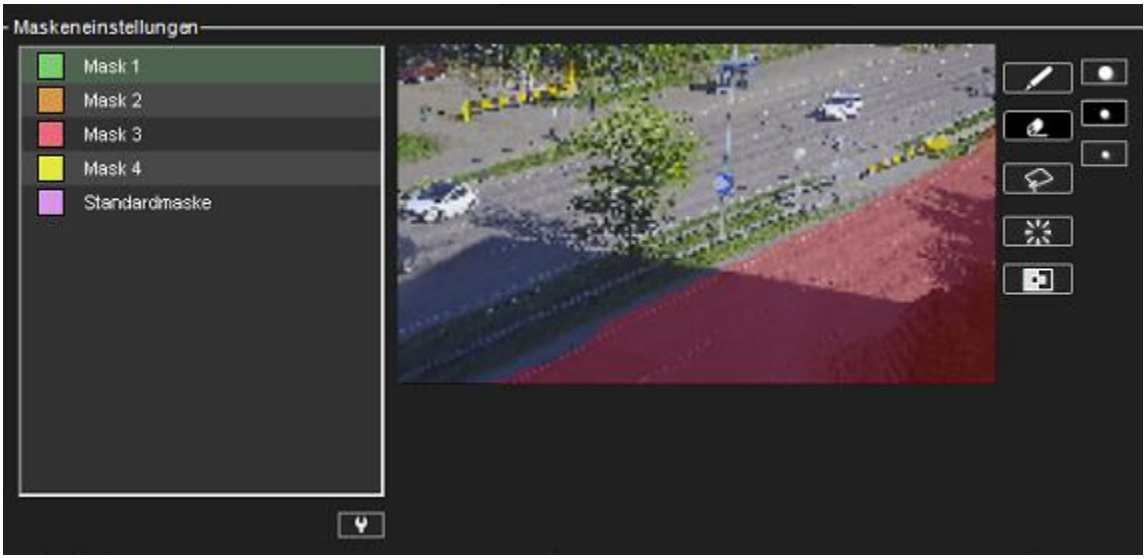
1. Gehen Sie zu **System Manager** > **VMS-Server** > **Kameras** > **Bewegungserkennung**
2. Wählen Sie eine Kamera aus der Liste aus
3. Vergewissern Sie sich, dass die Bewegungserkennungsmethode auf **Adaptive Erkennung** eingestellt ist
4. Wählen Sie **Mask 1**



1. **Radiergummi** auswählen



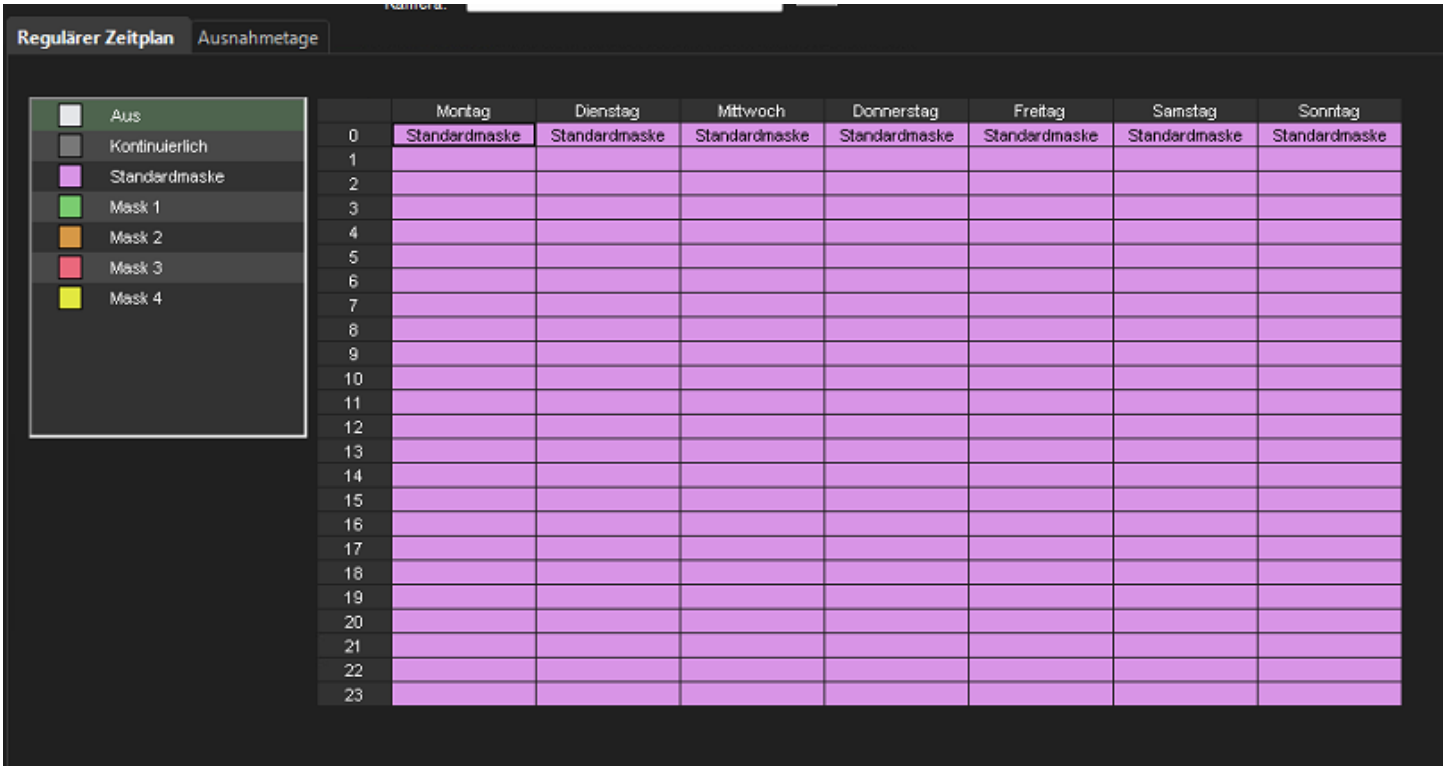
1. Entfernen Sie alle Bereiche aus dem Bildausschnitt, in denen keine Aufzeichnung ausgelöst werden soll. Bewegungen innerhalb des markierten Bereichs werden aufgezeichnet, sobald der Schwellenwert für die Bewegungserkennung überschritten wird.



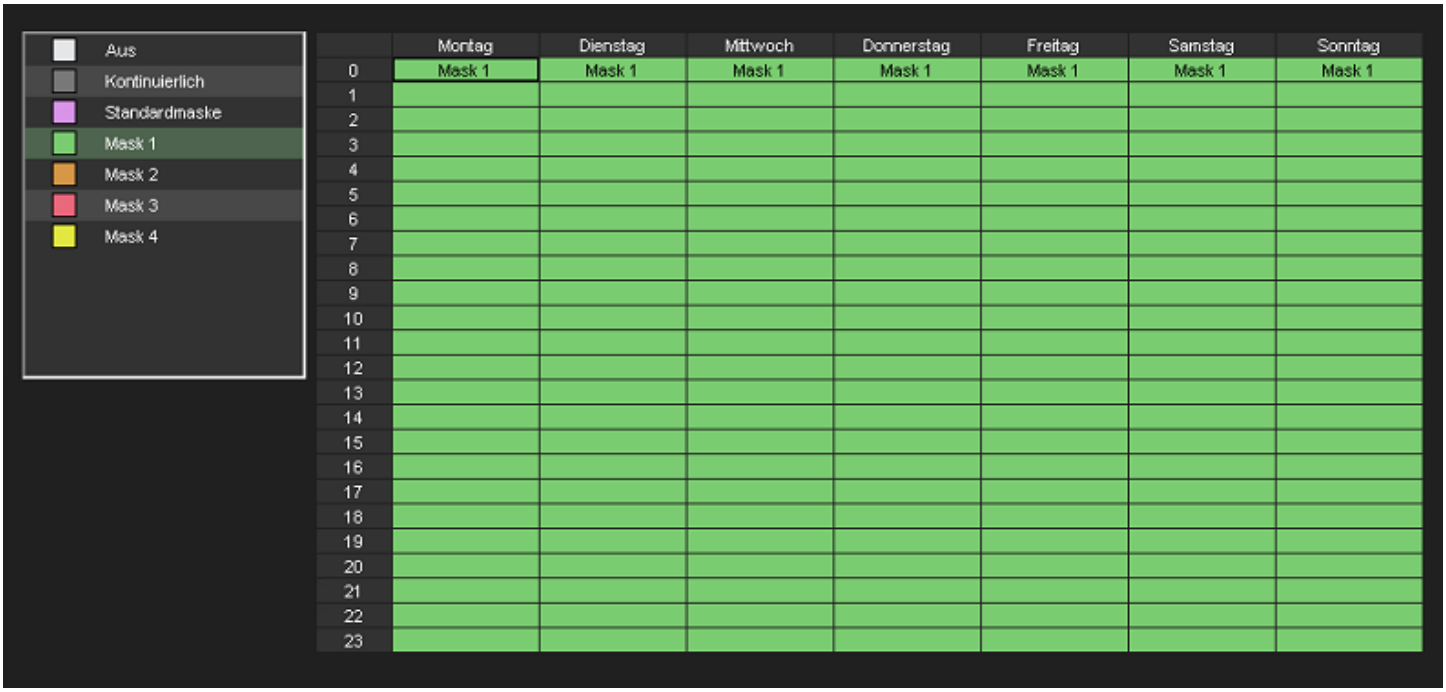
15.8 Konfigurieren von Bewegungserkennungsmasken im Kalender

Sobald die Einstellungen für die Bewegungserkennung konfiguriert sind, wechseln Sie zur Registerkarte **Planer**.

Standardmäßig verwendet die Mirasys VMS Software für alle Kameras die Standardmaske, was bedeutet, dass Bewegungen an beliebiger Stelle im Bildausschnitt eine Aufzeichnung auslösen.

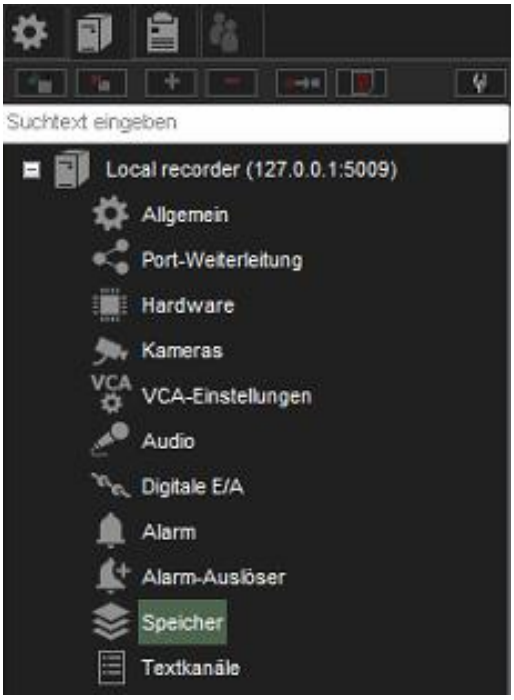


1. Wählen Sie eine Kamera aus
2. Wählen Sie **Mask 1** (zuvor bearbeitete Maske)
3. Wählen Sie die obere linke Ecke aus (wählen Sie die gesamte Woche aus), indem Sie mit der linken Maustaste klicken
4. Sie können auch den genauen Tag und die Uhrzeit auswählen, indem Sie die linke Maustaste gedrückt halten
5. Bestätigen Sie die Änderung, indem Sie unten auf **OK** klicken
6. Wiederholen Sie diese Schritte für jede Kamera, die angepasst werden muss

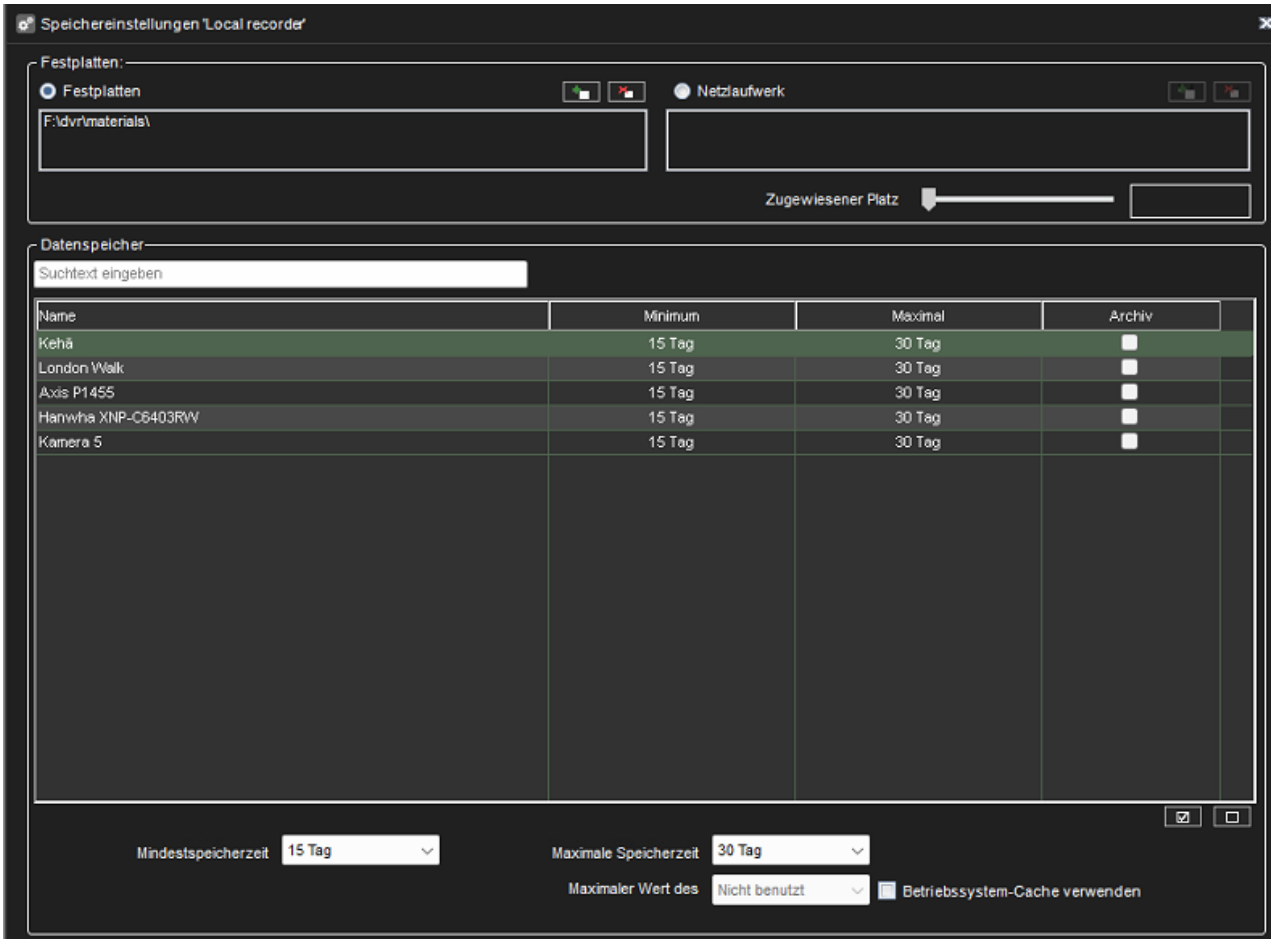


15.9 Konfigurieren der Speichereinstellungen

1. Gehen Sie zu **System Manager** > **VMS-Server** > **Speicher**



1. Wählen Sie eine oder mehrere Kameras aus (Umschalt+Klick)
2. **Mindetspeicherzeit** festlegen → Die Daten werden mindestens x Tage lang aufbewahrt, sofern auf der Festplatte genügend Speicherplatz vorhanden ist
3. **Maximale Speicherzeit** festlegen → Die Mirasys VMS-Software löscht automatisch Aufzeichnungen, die älter als die festgelegte maximale Speicherdauer sind
4. Klicken Sie auf **OK**, um die Einstellungen zu bestätigen

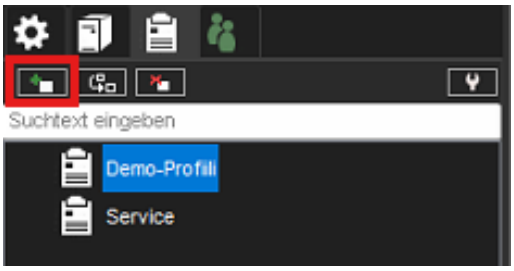


15.10 Erstellen eines Profils für den Kunden

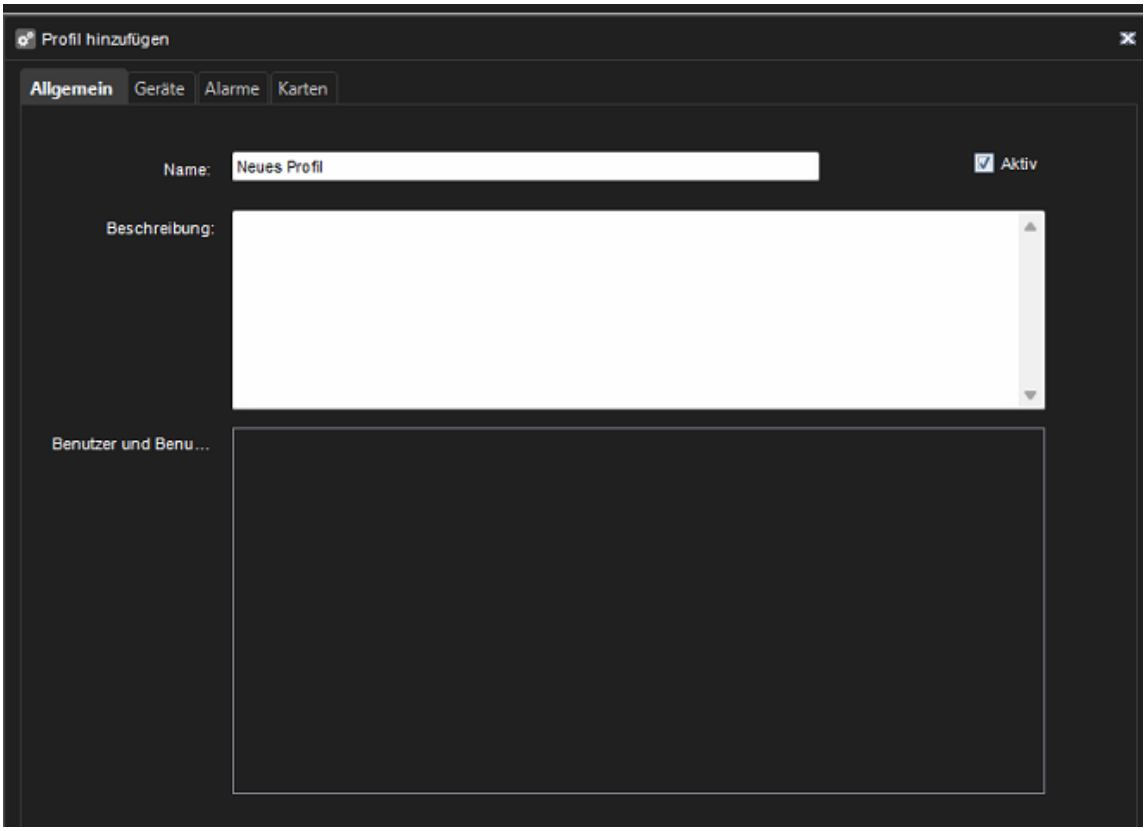
Ein Profil legt fest, welche Kameras oder Geräte der Endkunde in der Spotter-Software sieht.

Es ist wichtig, dass das Profil des Kunden nur die erforderlichen Komponenten enthält.

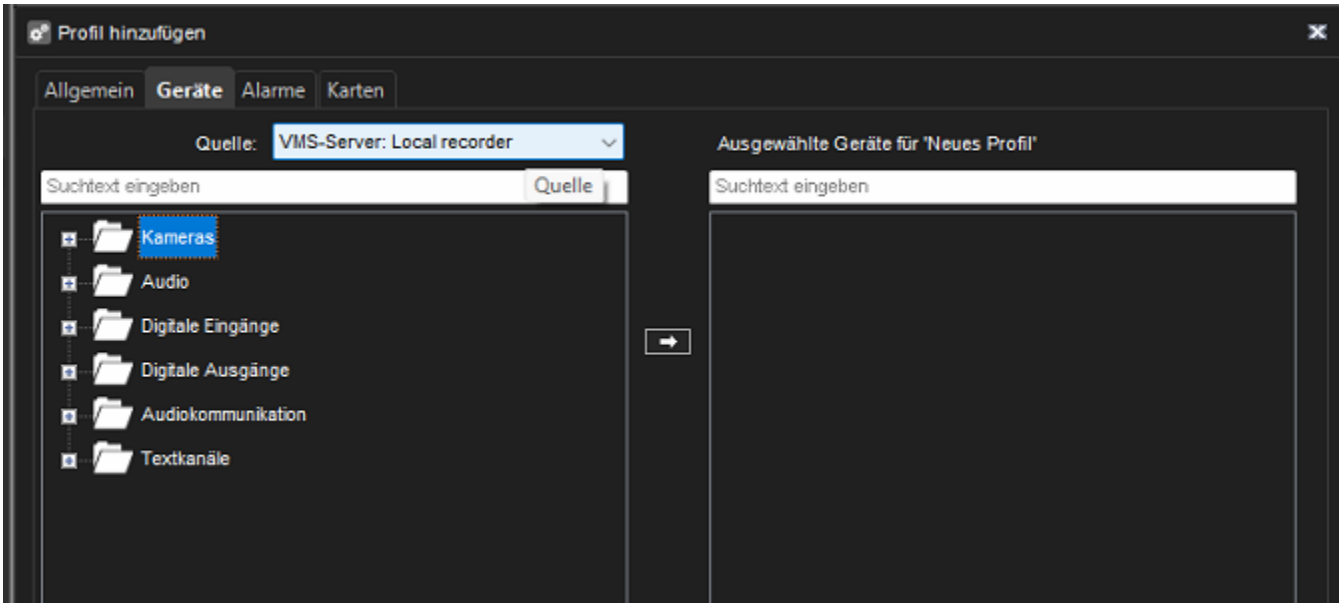
1. Gehen Sie zu **System Manager** > **Profile**
2. Wählen Sie **Profil hinzufügen**



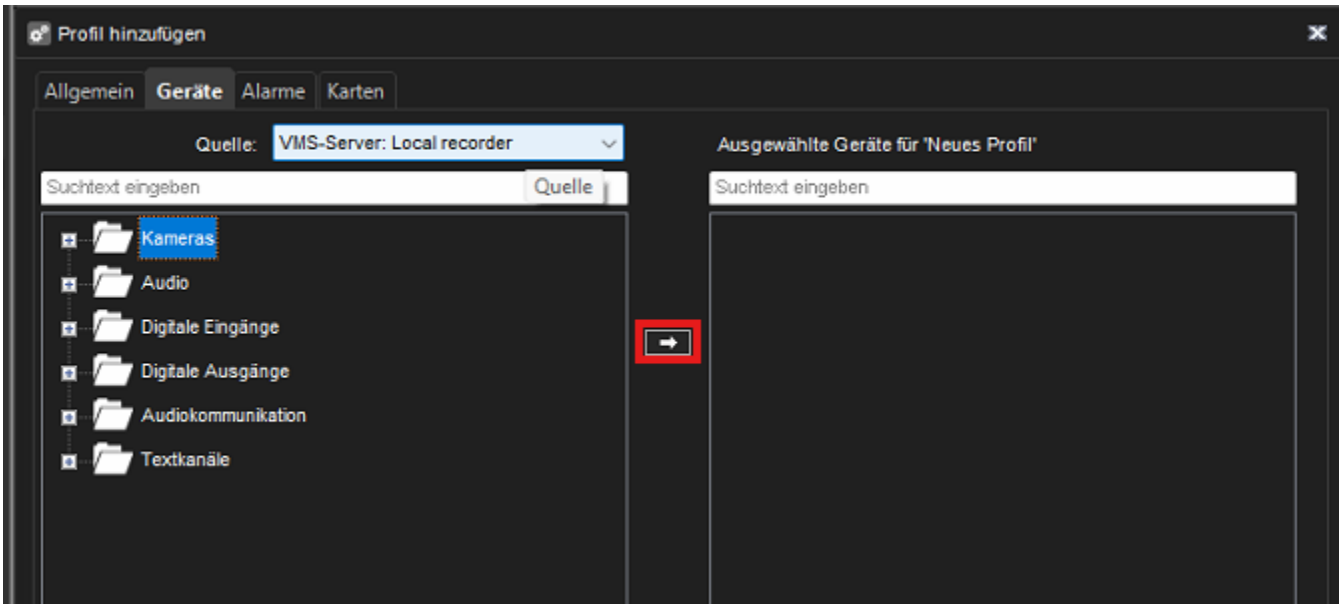
1. Geben Sie einen Profilnamen ein



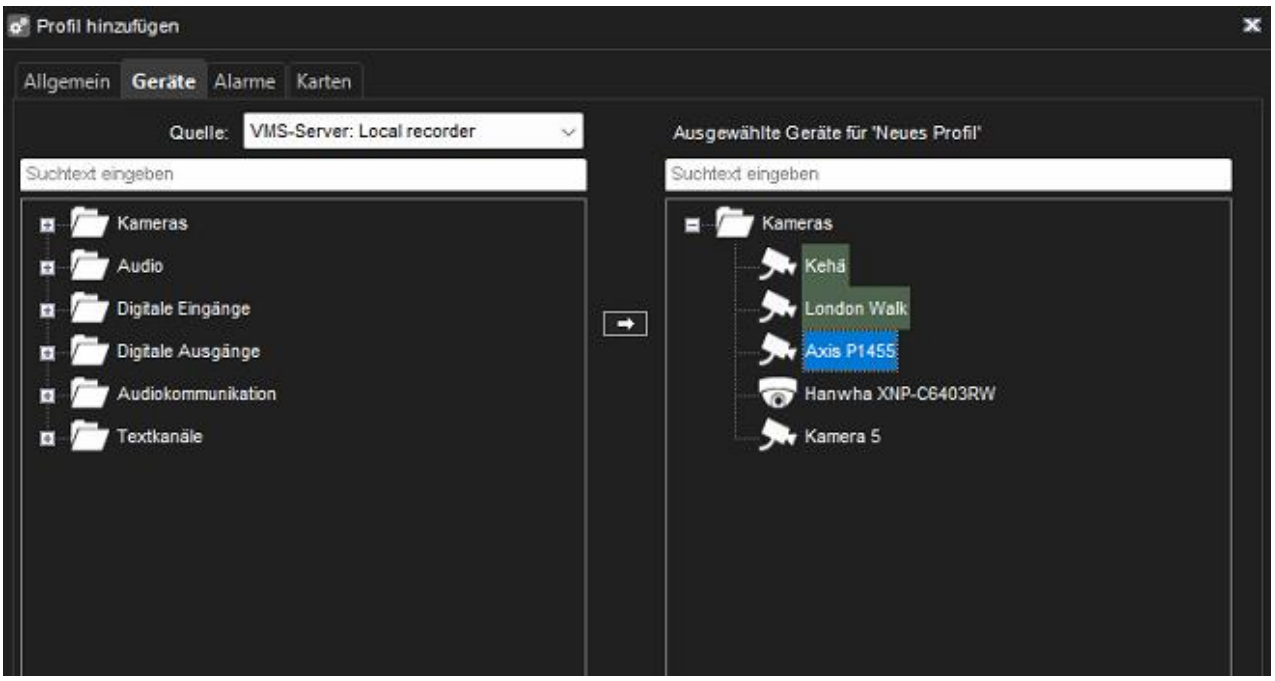
1. Wechseln Sie zur Registerkarte **Geräte**
2. Stellen Sie als Quelle „VMS-Server: Local Recorder“ ein



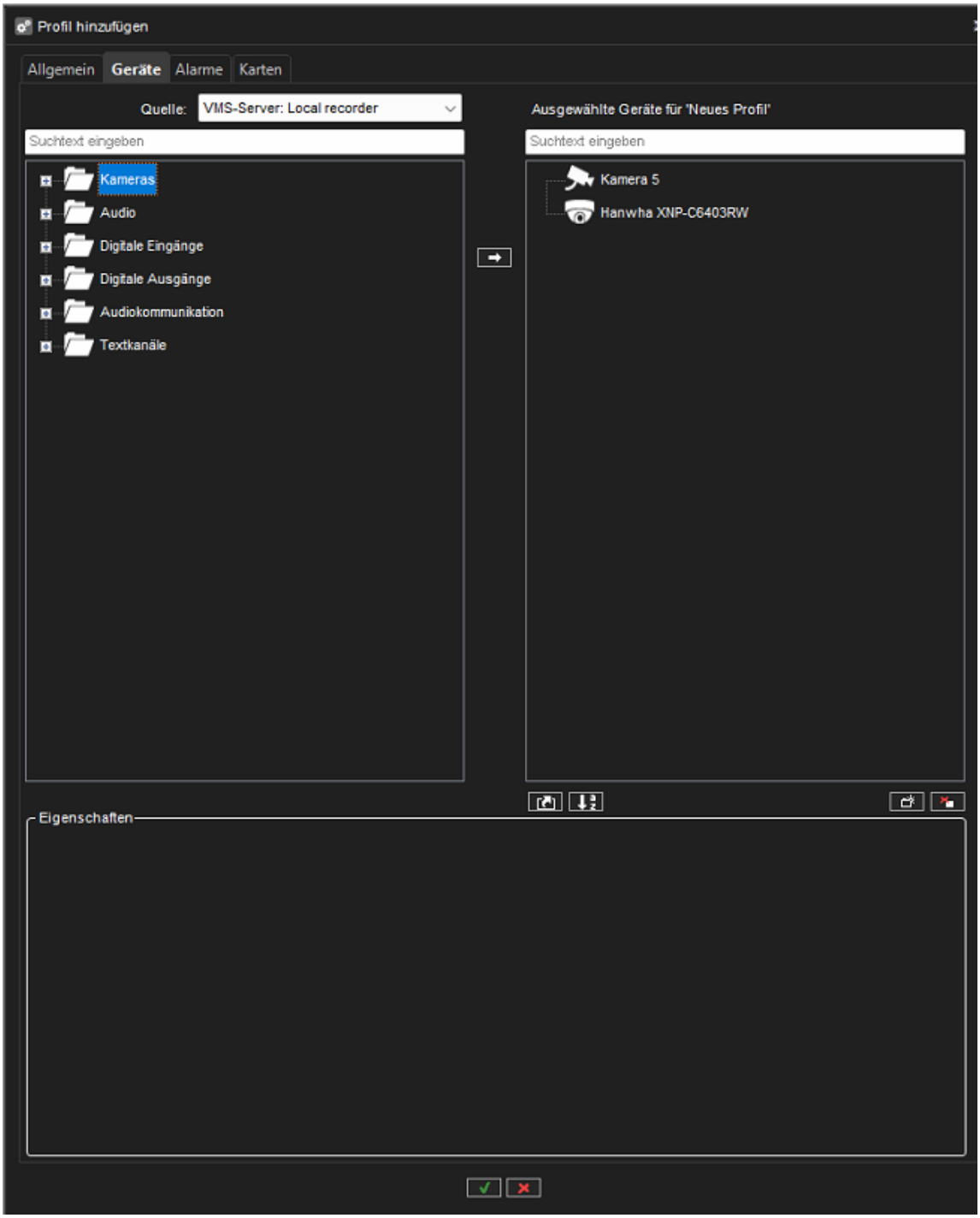
1. Wählen Sie den Ordner **Kameras** aus und klicken Sie auf die Schaltfläche **Hinzufügen**



1. Wählen Sie in der Liste „Ausgewählte Geräte“ die Kameras aus, die nicht mit dem System verbunden sind



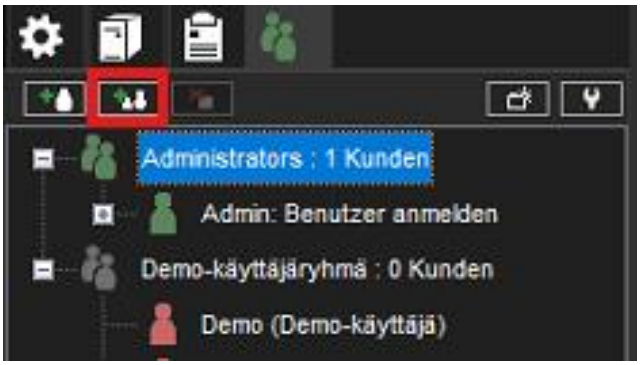
1. Bestätigen Sie die Änderungen, indem Sie auf **OK** klicken



15.11 Erstellen einer Benutzergruppe für den Kunden

Die Benutzergruppe legt fest, welche Anwendungen der Endbenutzer nutzen darf.

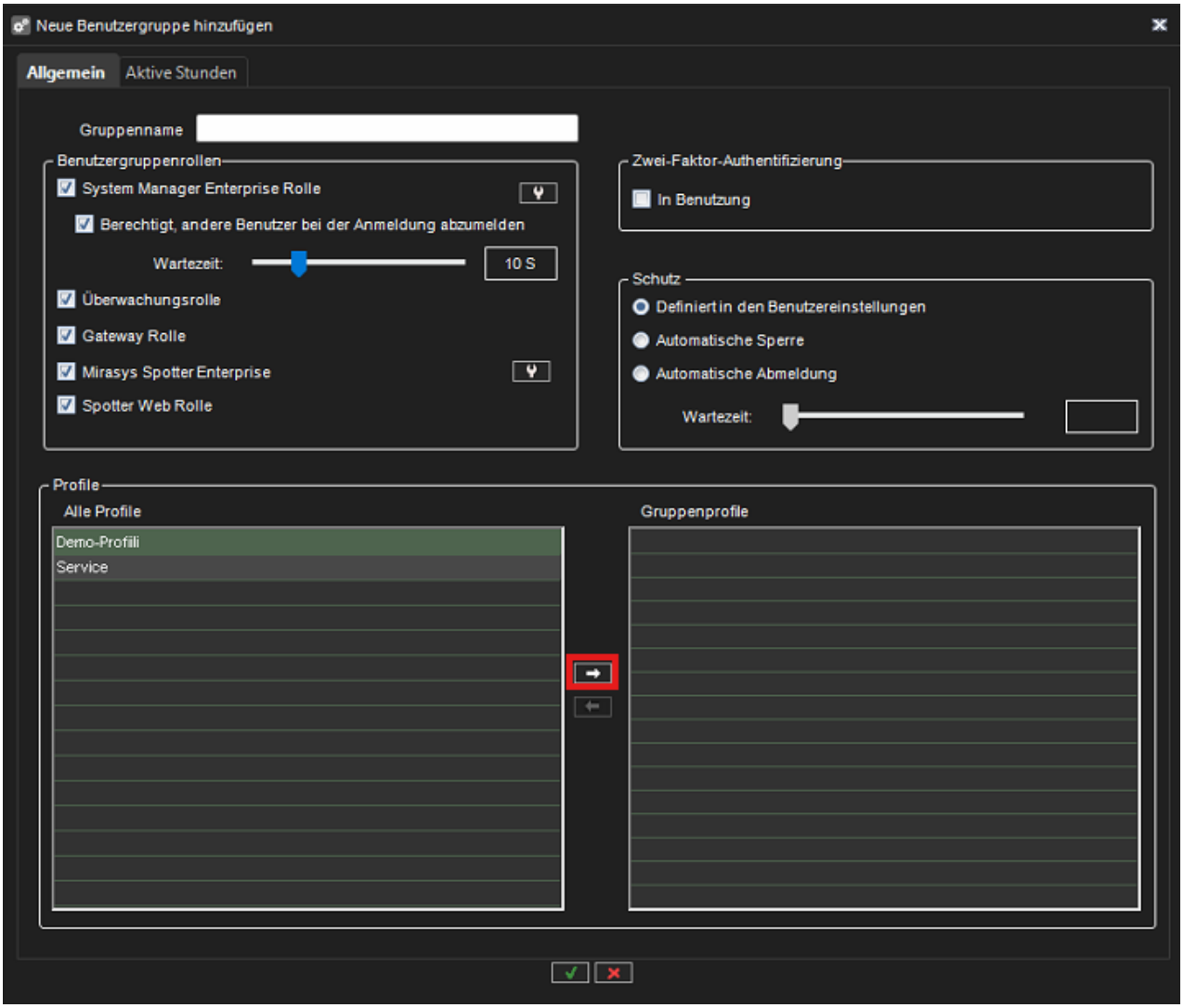
1. Gehen Sie zu **System Manager** > **Benutzer und Benutzergruppen**
2. Wählen Sie **Benutzergruppe hinzufügen**



1. Geben Sie einen Namen für die Gruppe ein
2. Aus Benutzerrollen entfernen

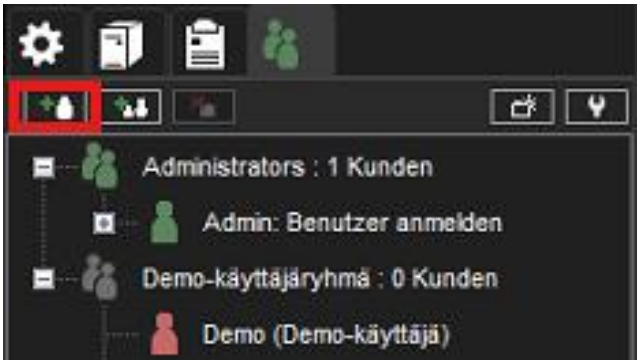
- **Rolle System Manager Enterprise** (Anmeldung bei System Manager und vollständige Verwaltung)
- **Rolle Überwachung** (Anmeldung bei System Manager und Systemüberwachung)

1. Wählen Sie das zuvor erstellte Profil aus dem Menü **Alle Profile** aus und klicken Sie auf **Profil für Benutzergruppe auswählen**
2. Bestätigen Sie die Änderungen, indem Sie auf **OK** klicken

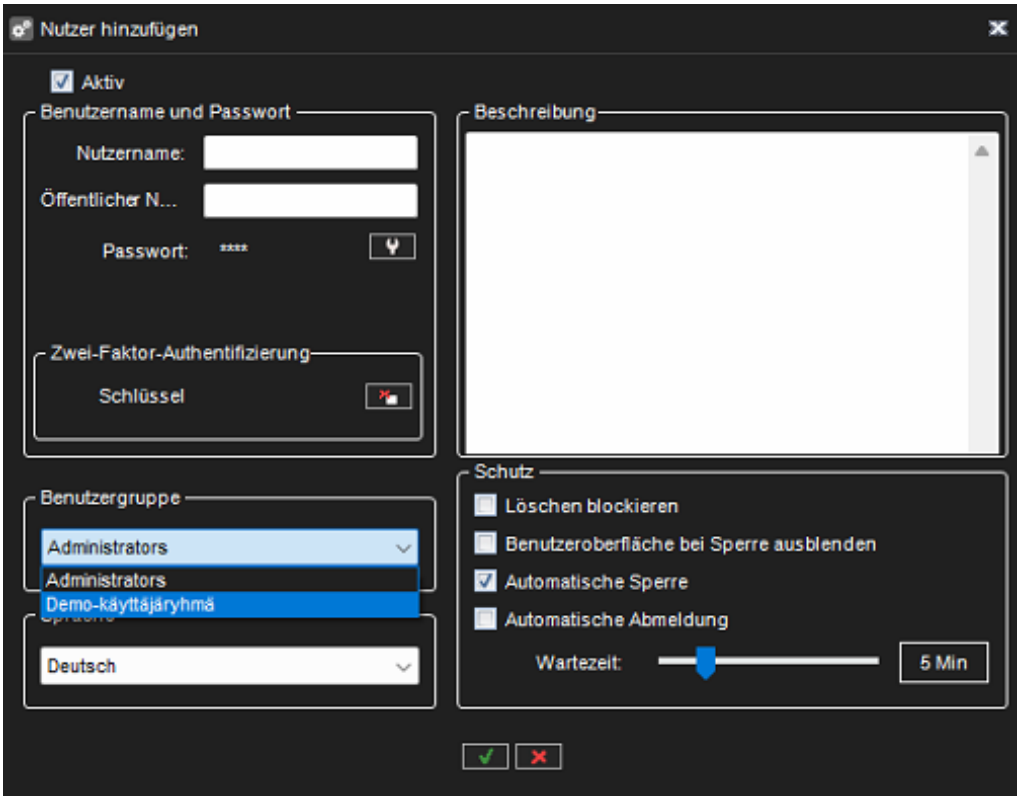


15.12 Erstellen eines Benutzerkontos für den Kunden und Hinzufügen zur Benutzergruppe des Kunden

1. Gehen Sie zu **System Manager** > **Benutzer und Benutzergruppen**
2. Klicken Sie auf **Benutzer hinzufügen**



1. Geben Sie den **Benutzernamen** ein (die Anmelde-ID des Kunden)
2. Geben Sie das **Passwort** ein
3. Wählen Sie die **Benutzergruppe** aus (eine zuvor für den Kunden erstellte Benutzergruppe)
4. Bestätigen Sie mit **OK**



15.13 Testen des Benutzerkontos

1. Öffnen Sie die Spotter-Anwendung vom Desktop aus



1. Geben Sie den **Benutzernamen** und das **Passwort** ein und klicken Sie auf **Fortfahren**



1. Der Kunde sollte die Kameras sehen können, die bei der Erstellung des Profils festgelegt wurden

