Administratorhandbuch v9

1 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.

2 Technischer Support

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

3 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.

3.1 Was beinhaltet ein System?

Das Mirasys-System besteht aus diesen Komponenten:

- 1-150 VMS Servers
    - **Master Server** (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

3.2 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)

3.3 Master-Server

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

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

Der Master-Server 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.

3.4 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

3.5 Netzwerkanforderungen

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

4 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.

5 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.*

6 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

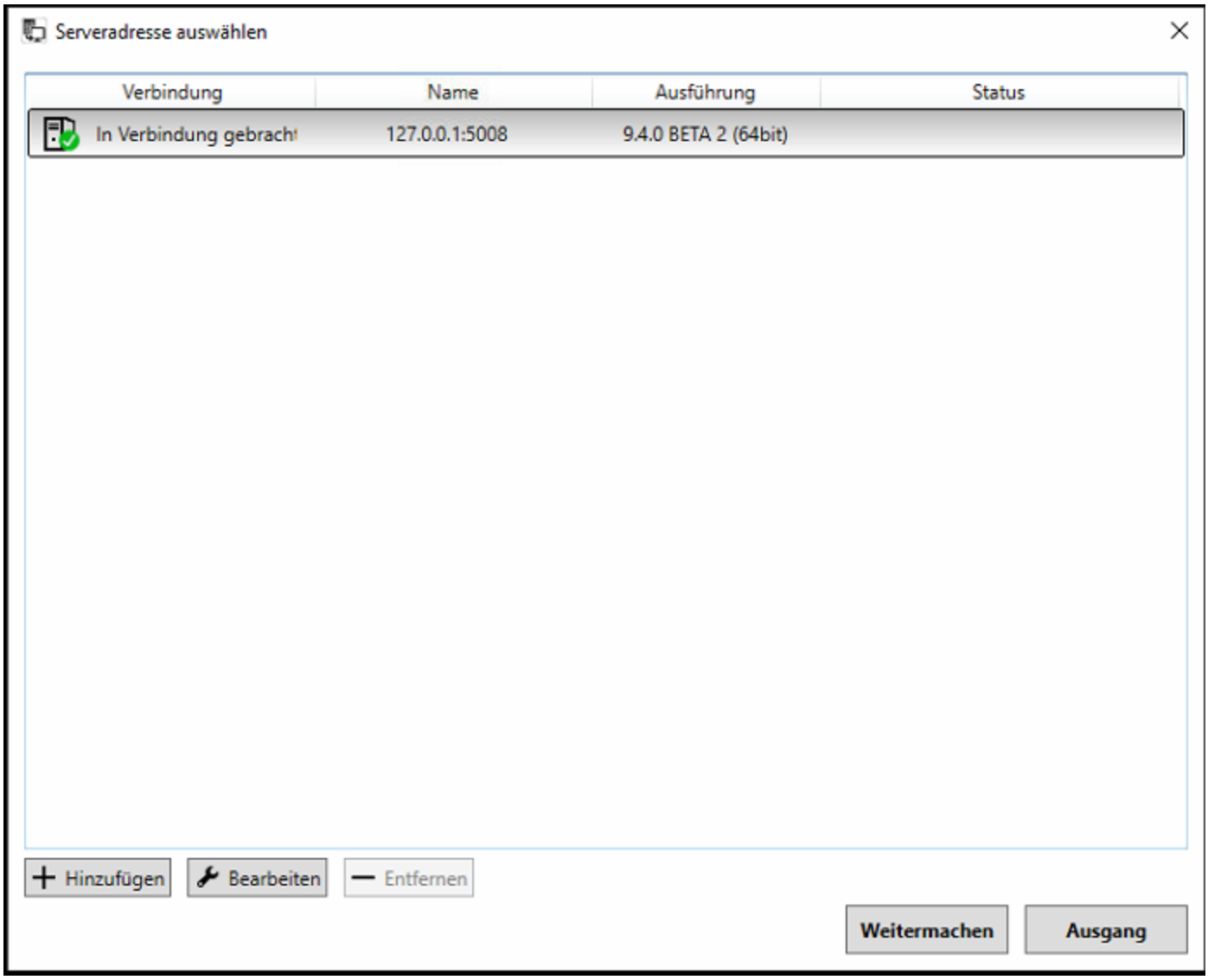
Der Standardbenutzername und das Standardpasswort sollten auch in geschlossenen Netzwerken nicht verwendet werden.
Bitte stellen Sie sicher, dass der Standardbenutzername und das Standardpasswort nach der Installation des Systems nicht mehr verwendet werden.

So melden Sie sich beim Systemmanager an:

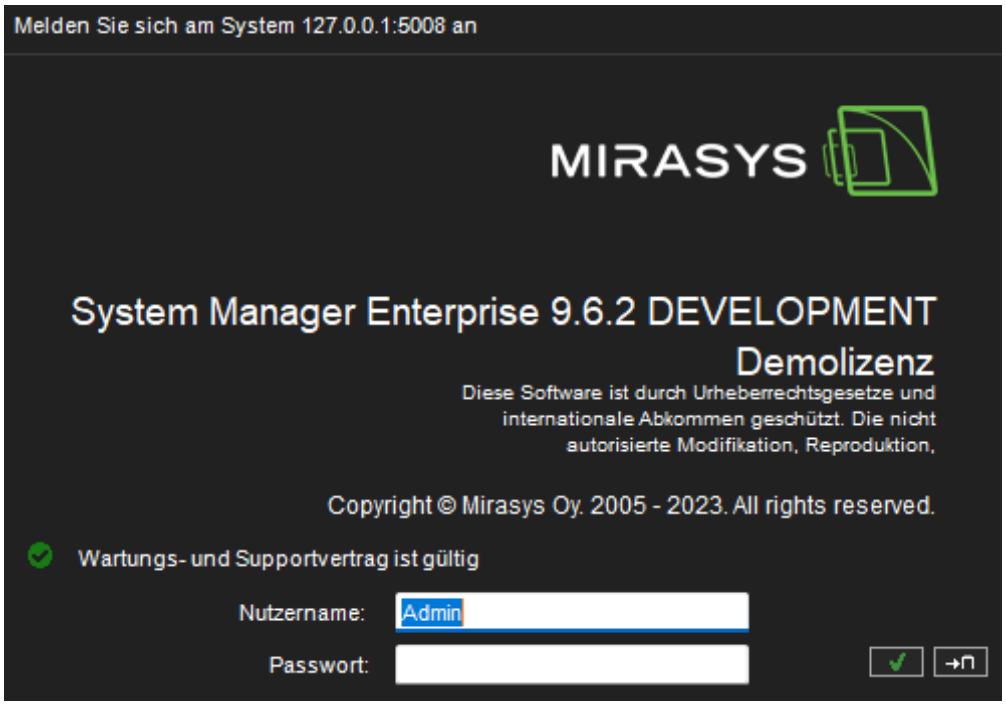
Führen Sie einen der folgenden Schritte aus:

- 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 Master-Server-Adresse konfiguriert ist, wird der Systemmanager-Anmeldebildschirm angezeigt.
In Systemen mit mehreren Mastern, konfigurierten Adressen oder wenn der Benutzer in der anfänglichen Startphase die Taste „Löschen“ drückt, wird der Standortauswahlbildschirm angezeigt .
Der Benutzer kann Master-Server-Adressen hinzufügen, entfernen oder bearbeiten oder einen Server auswählen, um sich auf diesem Bildschirm anzumelden.
Nach Auswahl eines Servers und Drücken der Schaltfläche „Weiter“ wird der Benutzer zum Anmeldebildschirm weitergeleitet.



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 Master-Server herzustellen, verlassen Sie den aktuellen Master und wählen Sie einen anderen Master-Server von der Site aus Auswahlbildschirm.

6.1 SCHLIEßANLAGENMANAGER

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 File 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. Notiz: *Beim Passwort muss die Groß-/Kleinschreibung beachtet werden*

7 MANAGEMENT-BENUTZEROBERFLÄCHE

Die System Manager-Benutzeroberfläche

Die Benutzeroberfläche von System Manager enthält diese Elemente:

7.1 MENÜLEISTE

- **Datei**
- **Ausloggen**
- **Program sperren**
- **Importieren**
- **Export**

7.2 INSTANDHALTUNG

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

7.3 HILFE

über

um Informationen über die Programmversion zu sehen.
und Sache **Hilfethemen** um die Online-Anleitung zu verwenden.

8 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

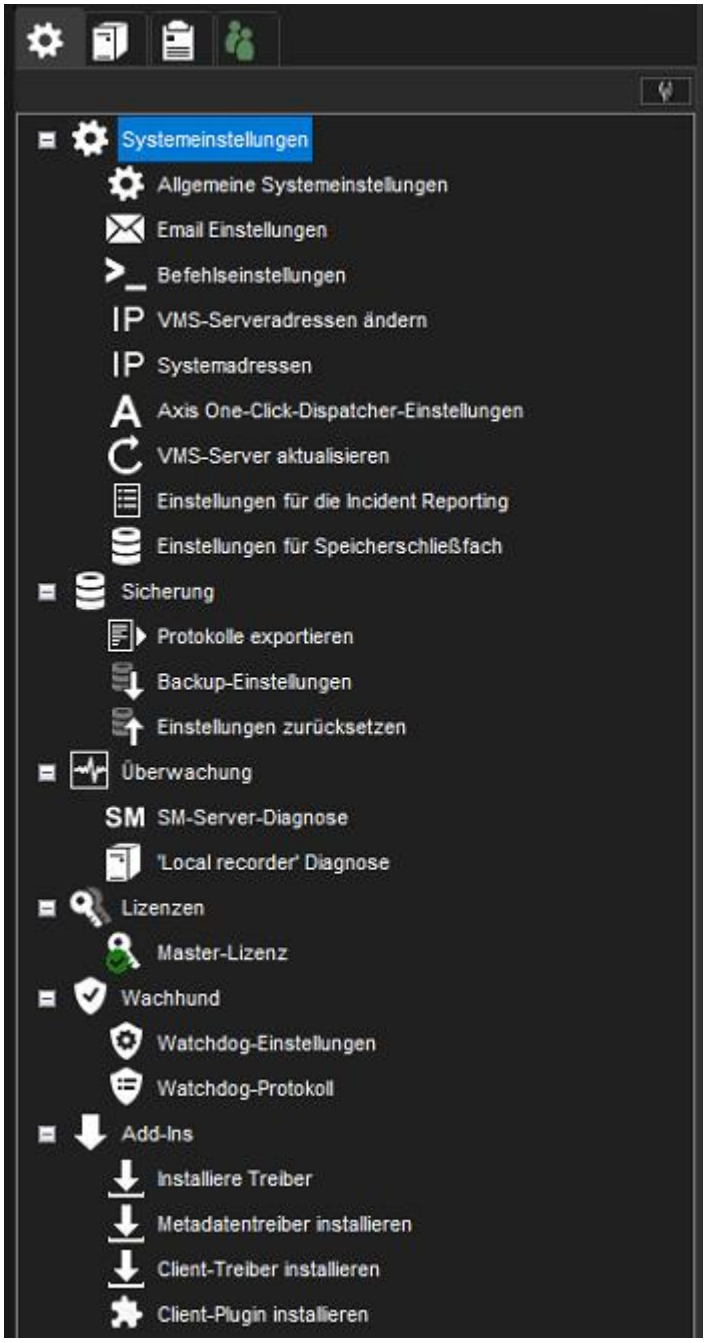
- Backup-Einstellungen
- Einstellungen zurücksetzen
- Überwachung
- SM-Server-Diagnose
- Lokale Rekorder-Diagnose
- Lizenzen
- Wachhund
- Watchdog-Einstellungen
- Watchdog-Protokolle
- Add-Ins
- Installiere Treiber
- Installieren Sie den Metadatentreiber
- Client-Treiber installieren
- Installieren Sie das Client-Plugin

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

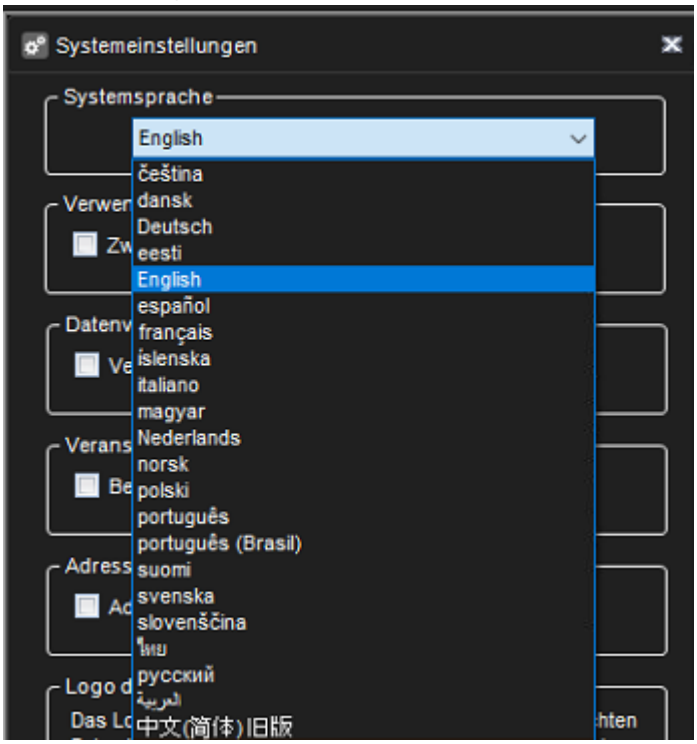
- Klicken Sie auf das Tool und dann auf Bearbeiten

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

8.2 SYSTEMEINSTELLUNGEN



8.2.1 Allgemeine Systemeinstellungen



8.2.1.1 In diesem Abschnitt können Sie Folgendes steuern:

- Systemsprache
- Die Verwendung des Passworts

Es ist möglich, das System so zu konfigurieren, dass von allen Benutzern zwei separate Passwörter verlangt werden.
Dies erfolgt durch Aktivieren der Option „Zweites Passwort in Verwendung“ in den allgemeinen Systemeinstellungen.
Wenn dieser Modus ausgewählt ist, müssen alle Benutzer zwei Passwörter eingeben Das standardmäßige zweite Passwort ist leer
Mit dieser Funktion kann eingeschränkt werden, dass keine einzelne Person Videos alleine ansehen kann.
Wenn ein Passwort einer Person und das andere Passwort einer anderen Person bekannt ist, müssen beide Personen beim Betrachten von Videos anwesend sein.

- Datenverschlüsselung

- Ereignisse (die Einstellung zum Senden von Bewegungsinformationen an Clients)
- Adressauswahl
- Primäres Videoclip-Logo (Logos, die an exportierte Videoclips angehängt sind)
- Sekundäres Videoclip-Logo (Logos, die an exportierte Videoclips angehängt sind)

8.2.2 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.

8.2.2.1 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.

8.2.2.2 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.

8.2.2.2.1 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

8.2.2.3 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

8.2.2.4 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.

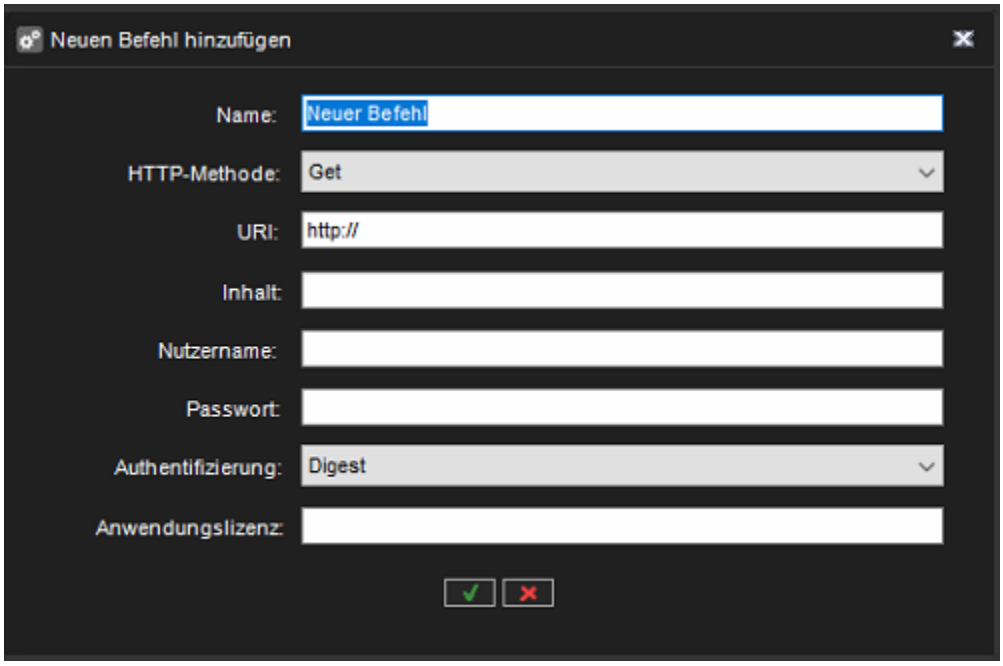
Personen und Gruppen können mit der Schaltfläche

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.

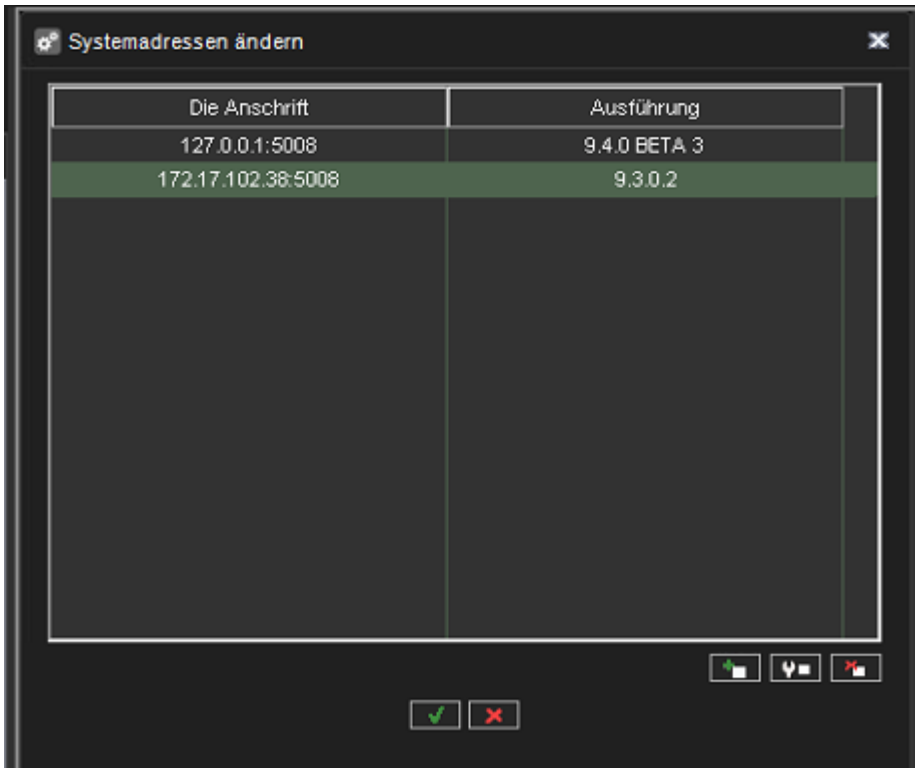
8.2.3 Befehlseinstellungen

Befehlseinstellungen werden für das Senden von HTTP-Befehlen verwendet



8.2.4 VMS-Serveradressen ändern

Wenn sich die IP-Adresse oder der DNS-Name eines Servers ändert, können Sie die neue Adresse / den neuen Namen über das **Tool VMS-Serveradressen ändern definieren.**



So ändern Sie die IP-Adresse oder den DNS-Namen eines Servers:

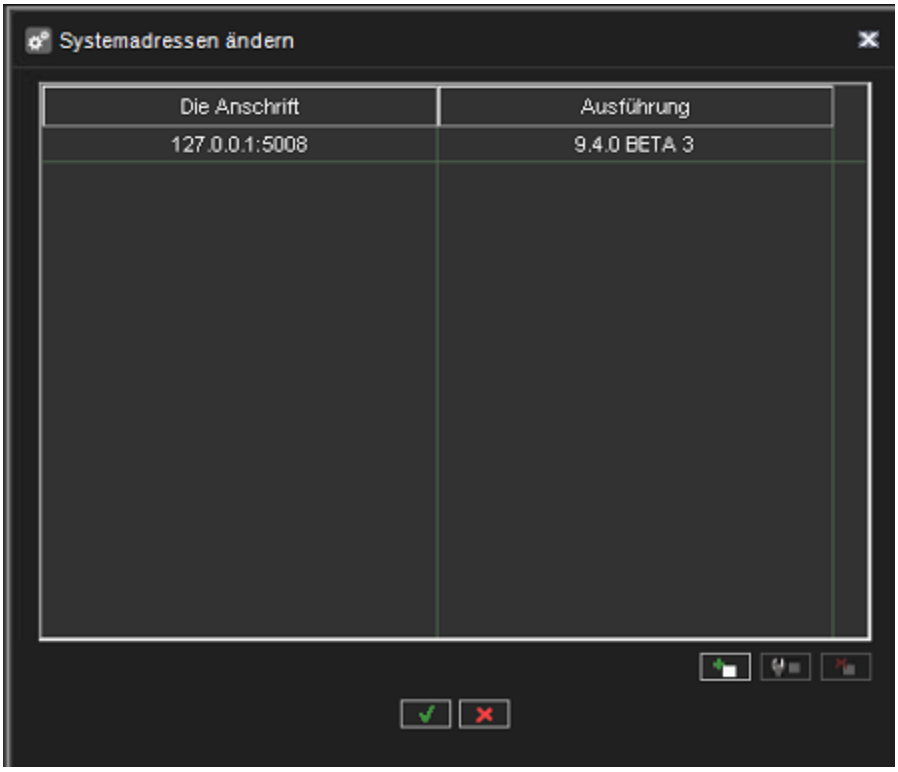
1. Öffnen Sie auf der Registerkarte System die Option VMS-Serveradressen ändern
2. Klicken Sie auf den Namen des Servers mit der geänderten IP-Adresse.
3. Klicken Sie auf **VMS-Serveradresse ändern**.

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

8.2.5 Systemadressen

Der Master Server ist der zentrale Server eines Überwachungssystems.

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



Sie können mehrere Master-Server-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 Master-Server-Adressen verbinden, vorausgesetzt, sie haben einen kompatiblen Benutzernamen und ein kompatibles Passwort für den Master-Server.*

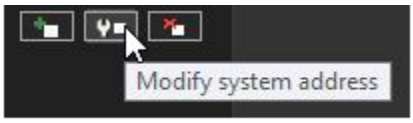
8.2.5.1 So fügen Sie eine Masterserver-Adresse hinzu

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

8.2.5.2 So bearbeiten Sie eine Master-Server-Adresse:

1. Öffnen Sie auf der Registerkarte System die Option Systemadressen.
2. Klicken Sie auf die Master-Server-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

8.2.5.3 So entfernen Sie eine Master-Server-Adresse:

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

8.2.6 Axis One-Click-Dispatcher-Einstellungen

8.2.6.1 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.

8.2.6.1.1 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)

8.2.6.1.1.1 Issue a server certificate:

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

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

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

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

Result:

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

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

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

8.2.6.1.2 Configure o3c-server.conf

listen_client = 172.17.102.56:80

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

stserverid = test_o3c_server

Any string

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

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

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

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

provider_name =

can be left blank

credentials = root:root

for device access requests

8.2.6.1.3 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

8.2.6.1.3.1 Filter for wireshark for Axis P1375:

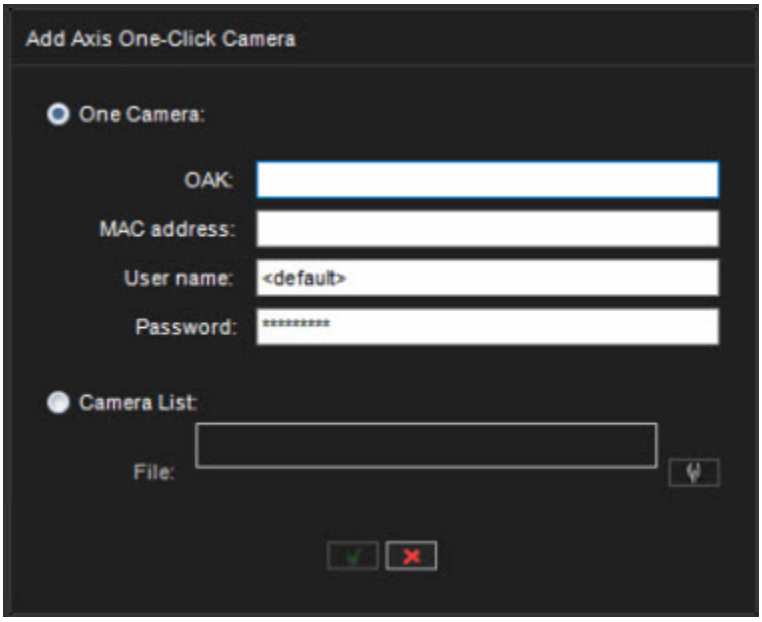
((ip.src == 172.17.100.84) && (ip.dst == 172.17.102.56)) || ((ip.src == 172.17.102.56) && (ip.dst == 172.17.100.84))

8.2.6.2 Add Axis One-Click Camera

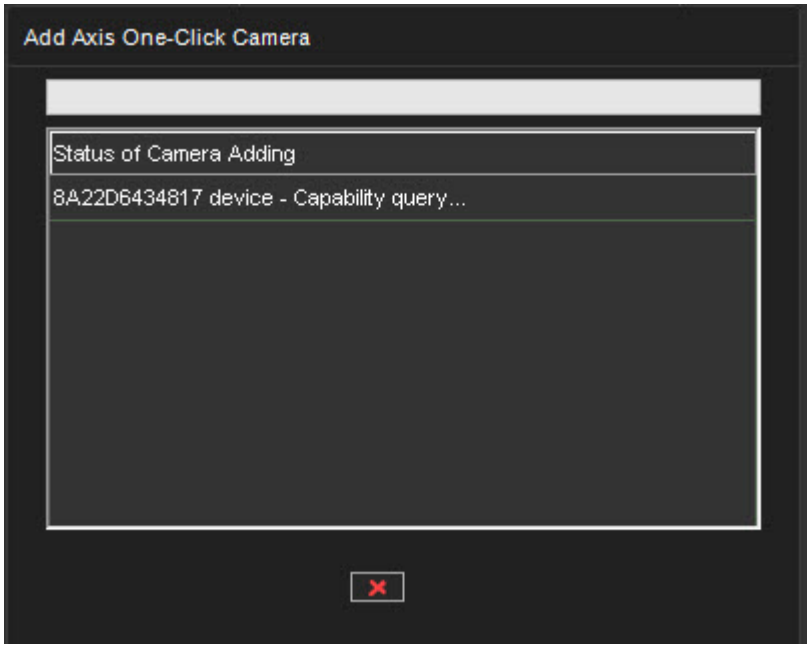
1. Open **System tab**
2. Go to **System Settings** and open **Axis one-click dispatcher settings**
3. Enter all necessary details and click **OK**

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

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

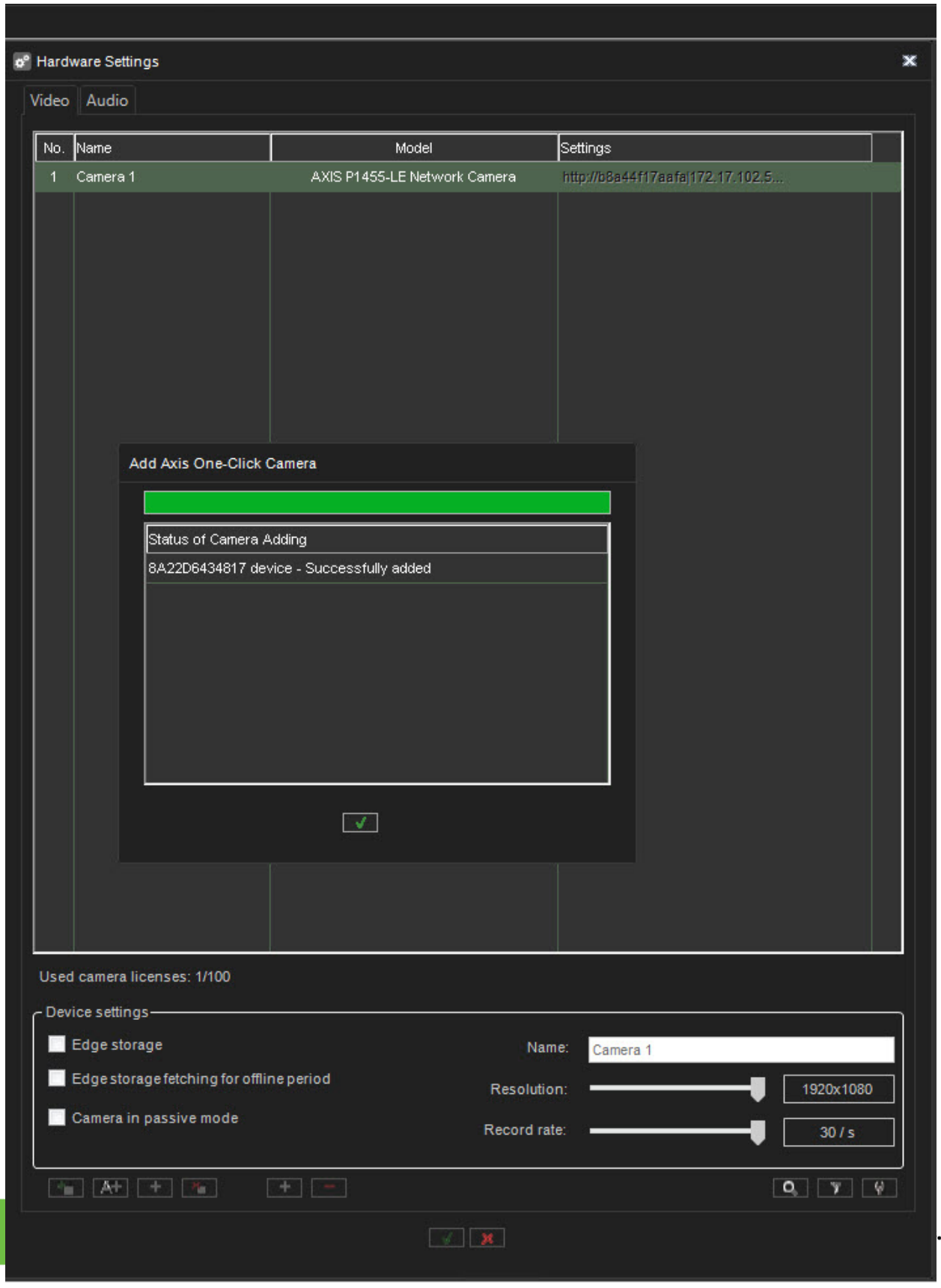


After clicking the OK, the camera query starts



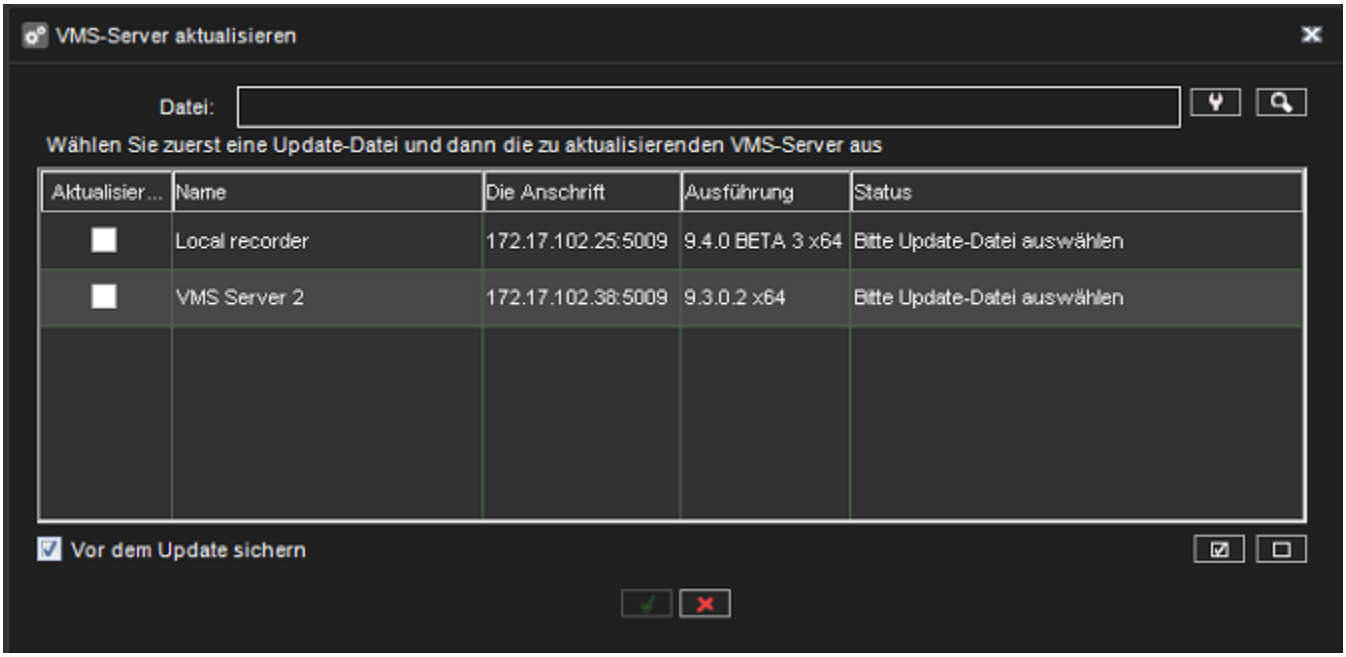
When the camera query is finished, the device will be added to the hardware list

8. Click **OK** to finalize


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

8.2.7 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

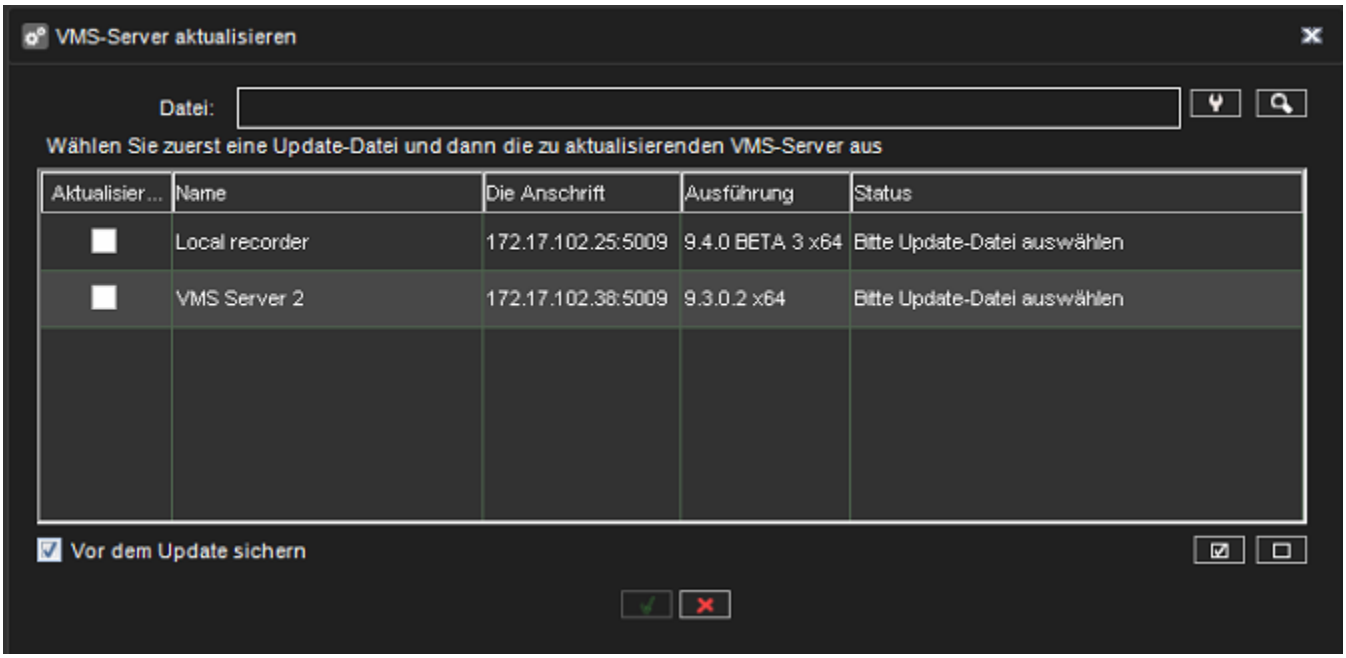


Um Server zu aktualisieren, wählen Sie zuerst die Installationsdatei mit der Schaltfläche

aus.

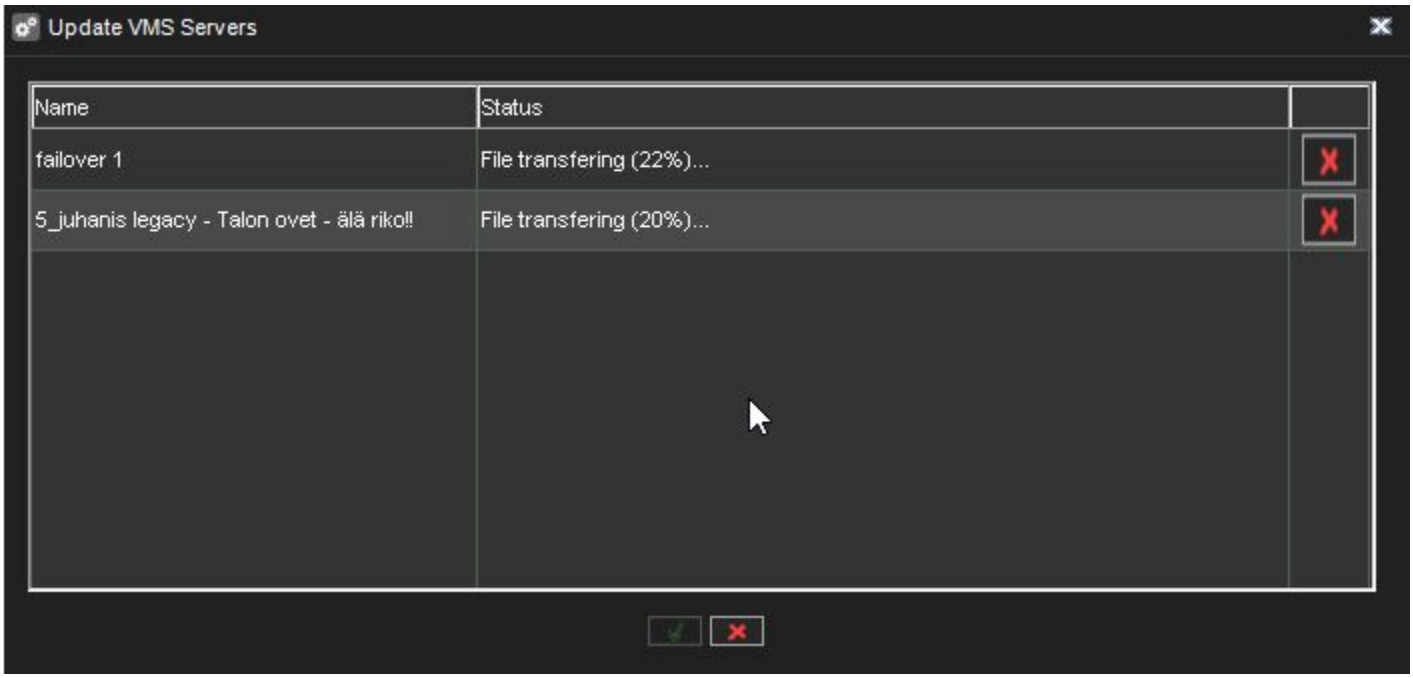
Die Liste wird aktualisiert, um anzuzeigen, welche Server mit der ausgewählten Installationsdatei aktualisiert werden können.

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.

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 Masterserver 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.

8.2.8 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.

8.2.8.1 Unternehmensinformationen

- Name der Firma
- Firmenanschrift

- Firmenlogo

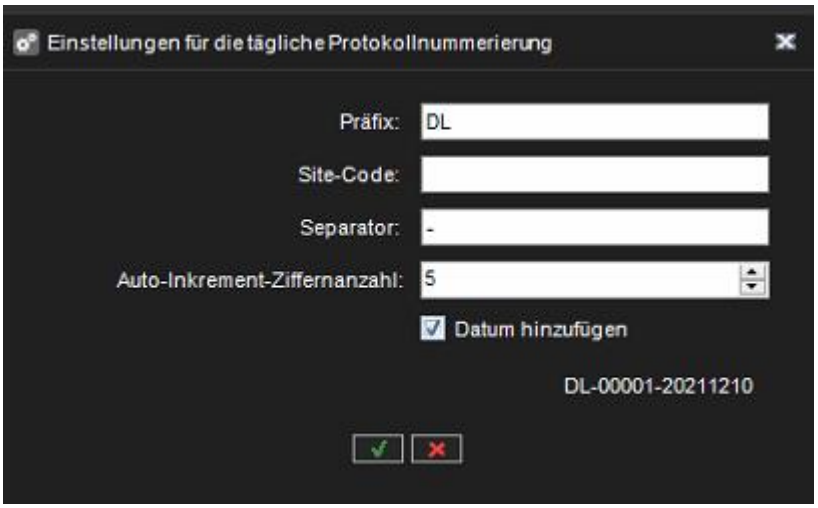
8.2.8.2 Berichtsnummerierung

Details zur Nummerierung von Vorfällen

- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen

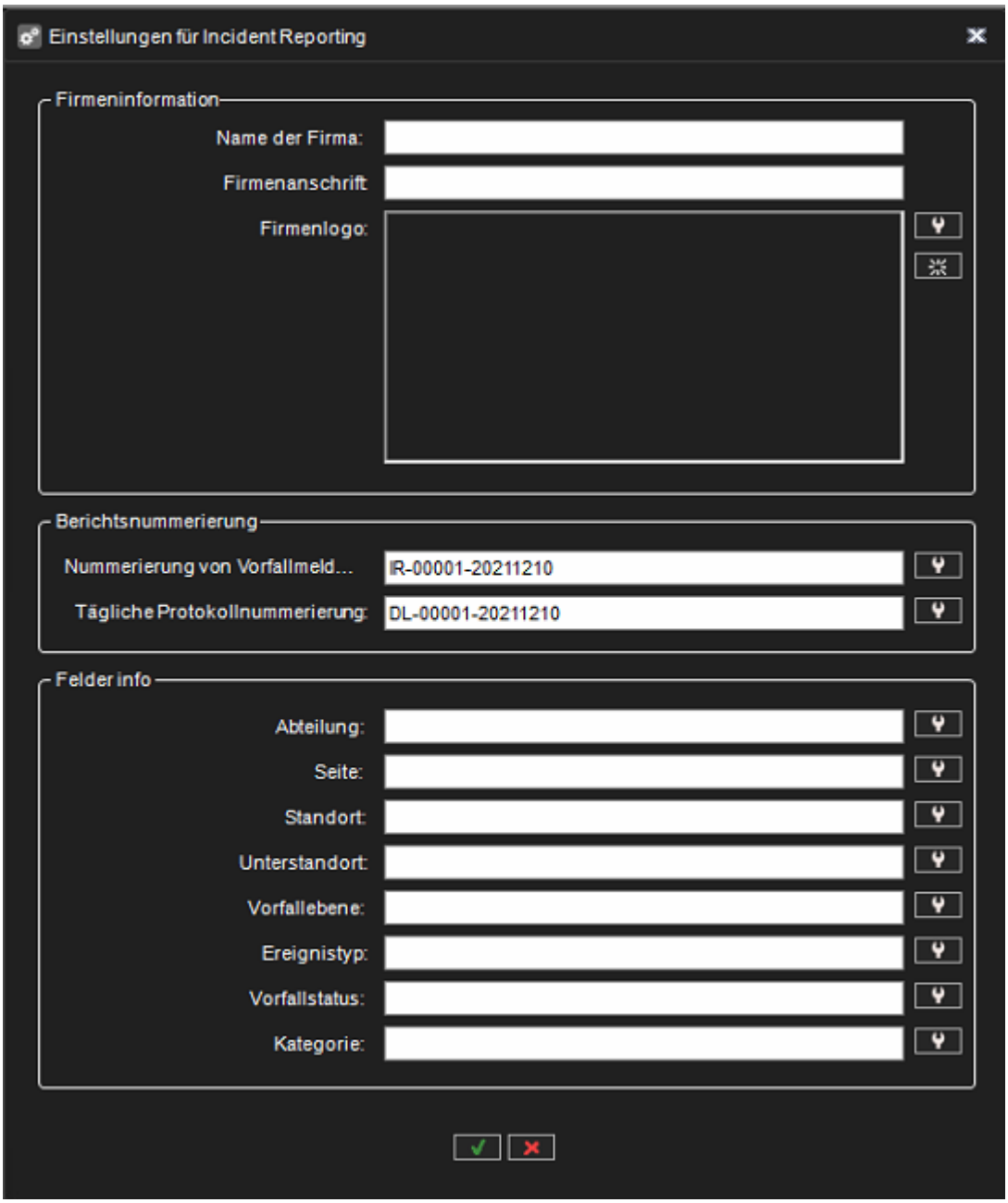
8.2.8.3 Details zur Nummerierung des Tagesprotokolls:

- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen



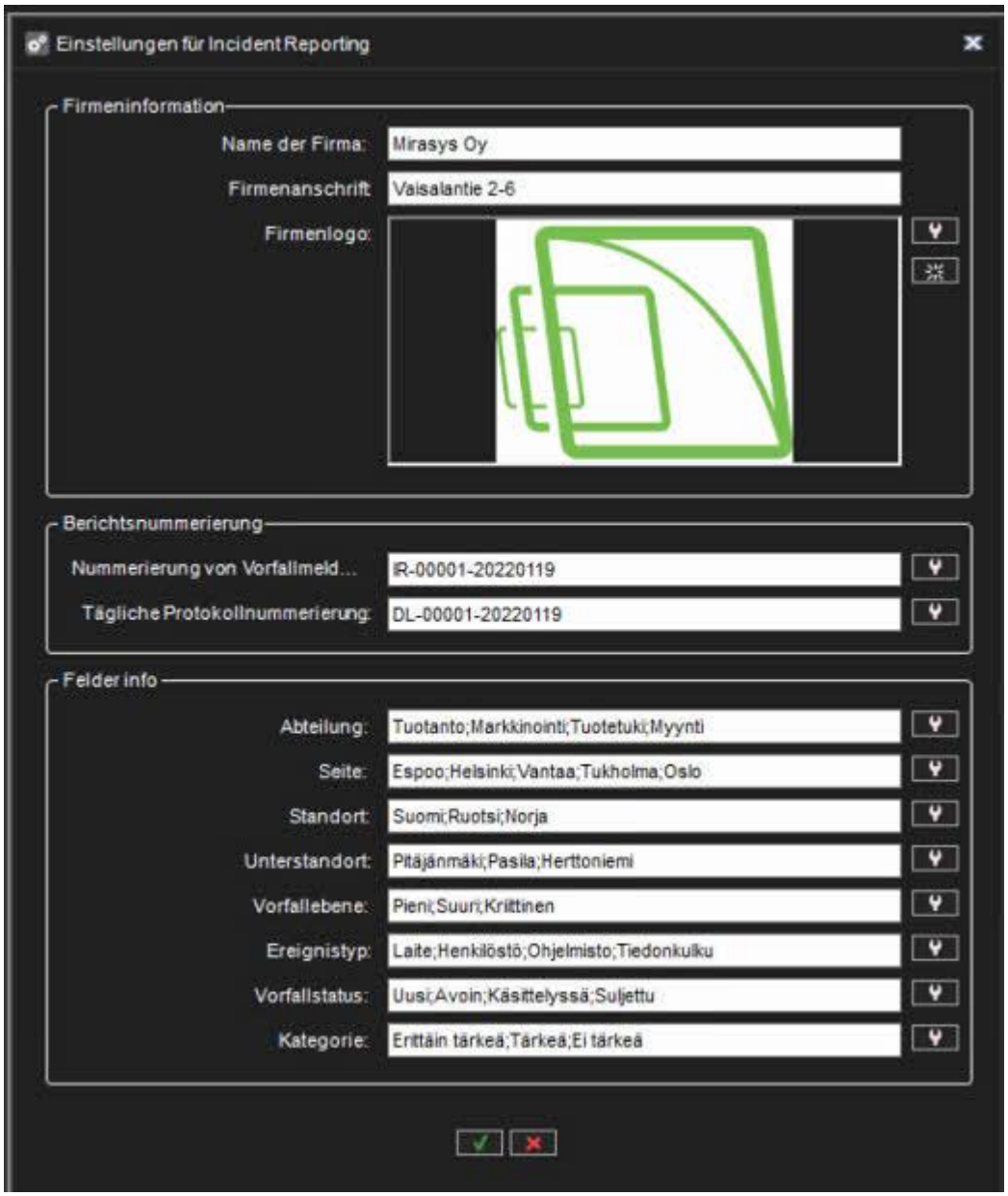
8.2.8.4 Felder info

- Abteilung
- Seite
- Standort
- Unterstandort
- Vorfall
- Vorfalltyp
- Vorfallstatus
- Kategorie



8.2.8.5 Werte hinzufügen

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

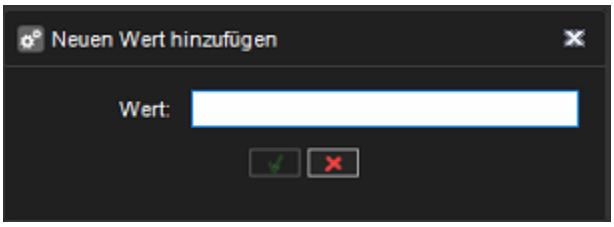


1. Klicken Sie auf Wert hinzufügen

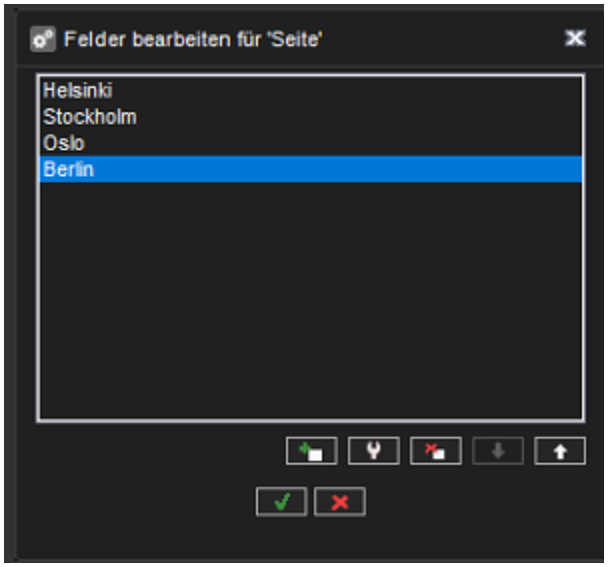
Invalid file id - f3ec2a...

2. Geben Sie den Namen des Wertes ein

3. OK klicken

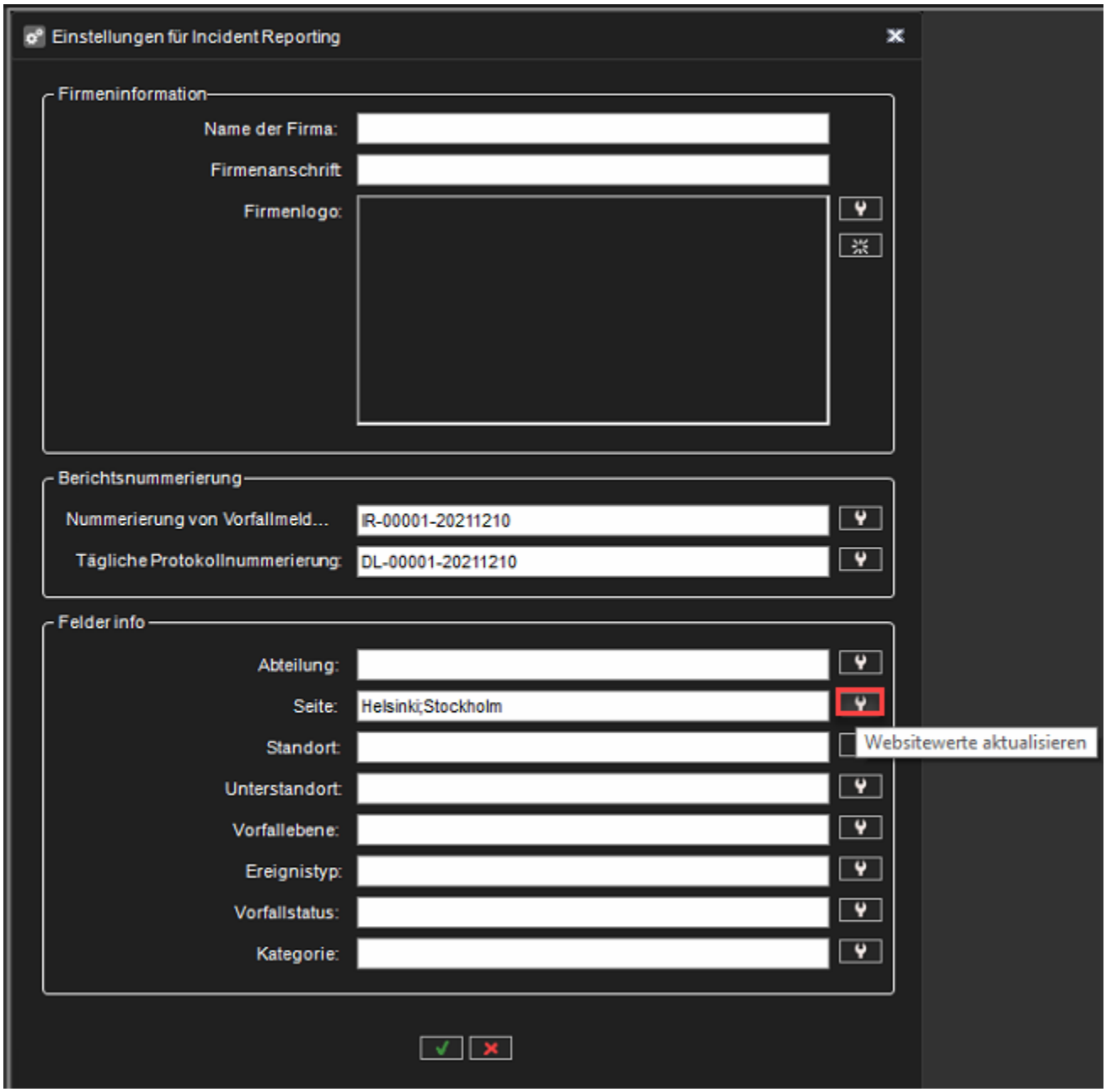


Neuer Mehrwert ist in der Liste zu sehen

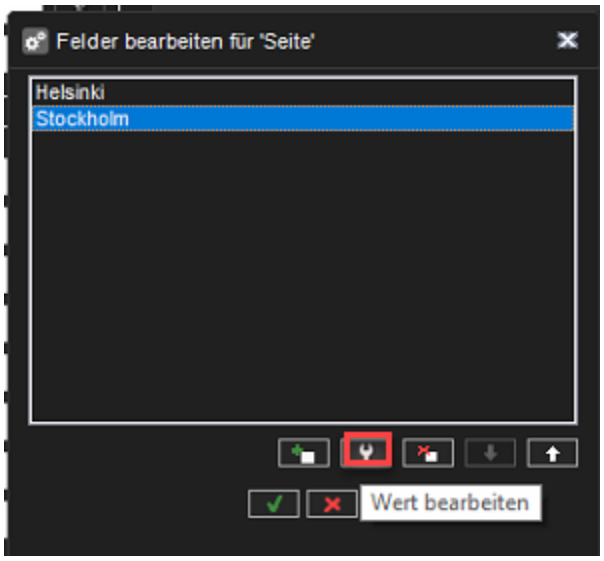


8.2.8.6 Werte bearbeiten

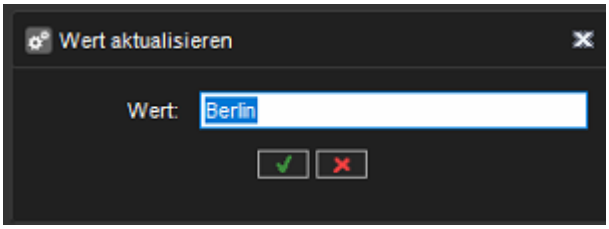
1. Klicken Sie auf das Symbol **Werte aktualisieren**



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

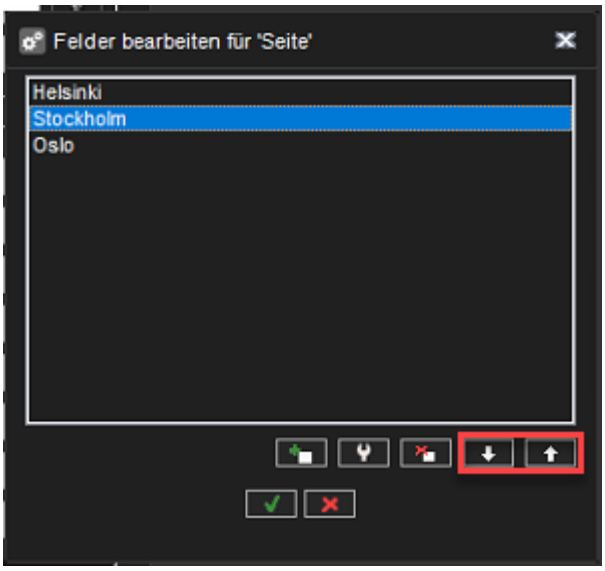


3. Geben Sie einen neuen Wertnamen ein und klicken Sie auf OK



8.2.8.7 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



8.2.9 Einstellungen für Speicherschließfach

Storage Locker Settings enthält die folgenden Werte:

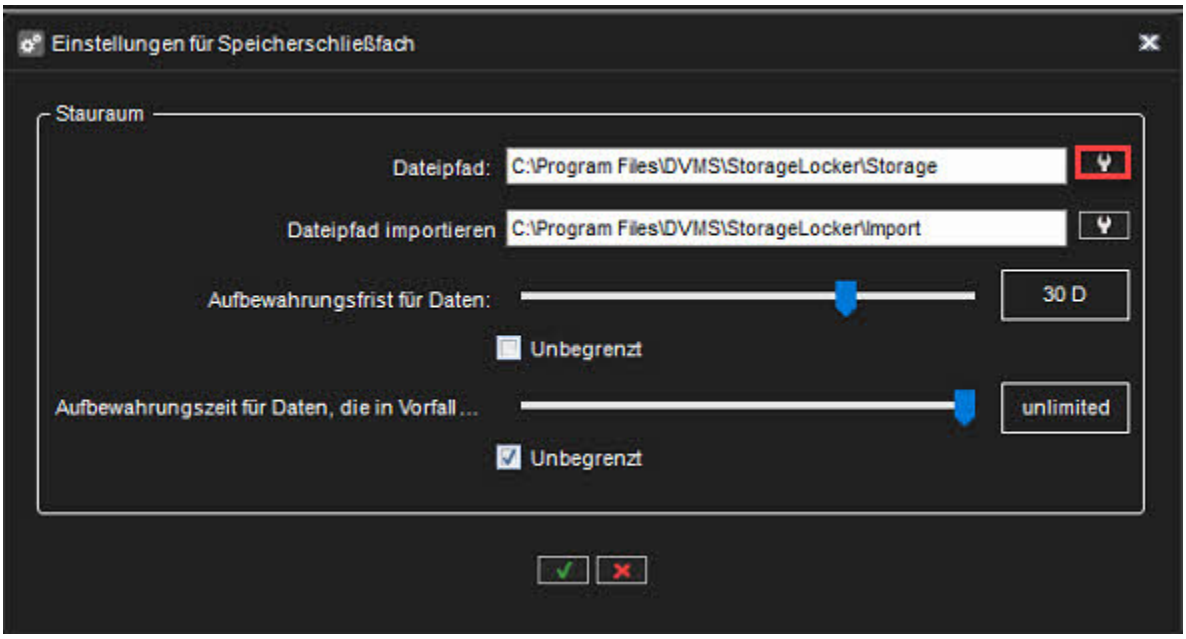
8.2.9.1 Dateipfad:

Definiert den Speicherort von Storage Locker.
Als Standardspeicherort befindet sich Storage Locker auf dem Master-Server.

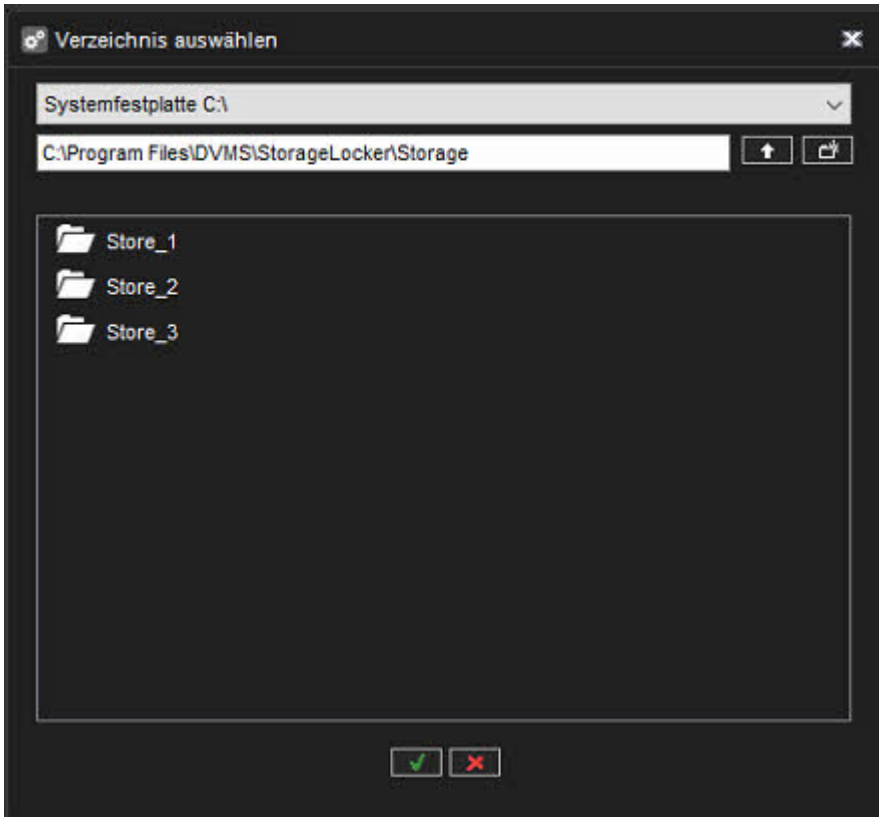
8.2.9.1.1 Dateipfad ändern

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



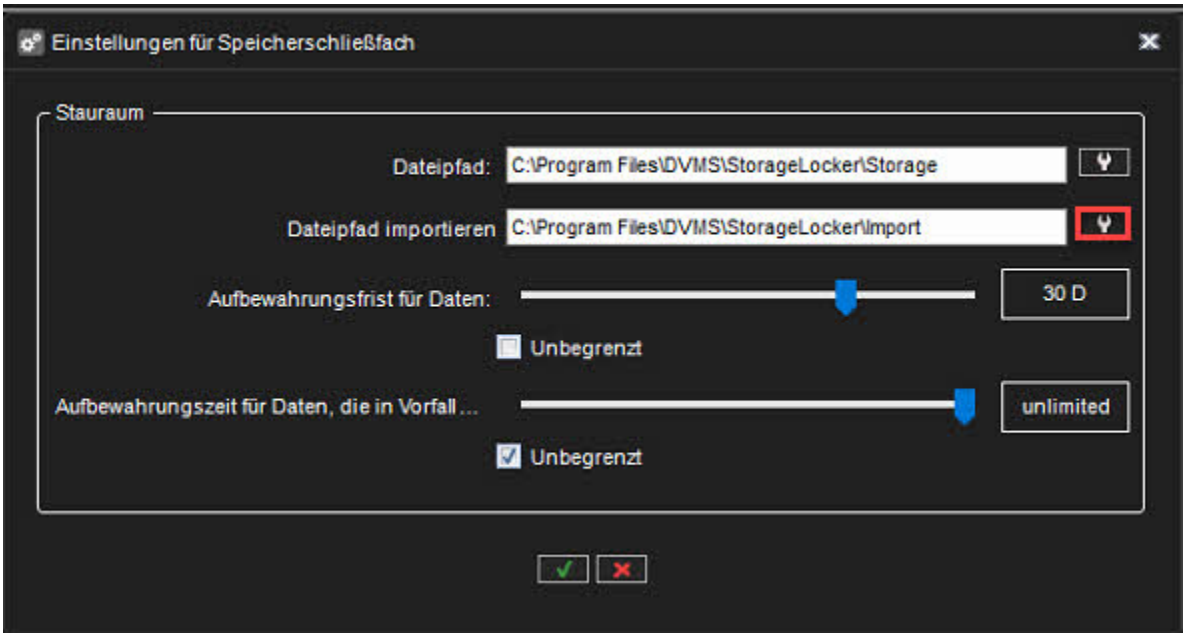
2. Wählen Sie einen neuen Standort und klicken Sie auf OK



8.2.9.2 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)

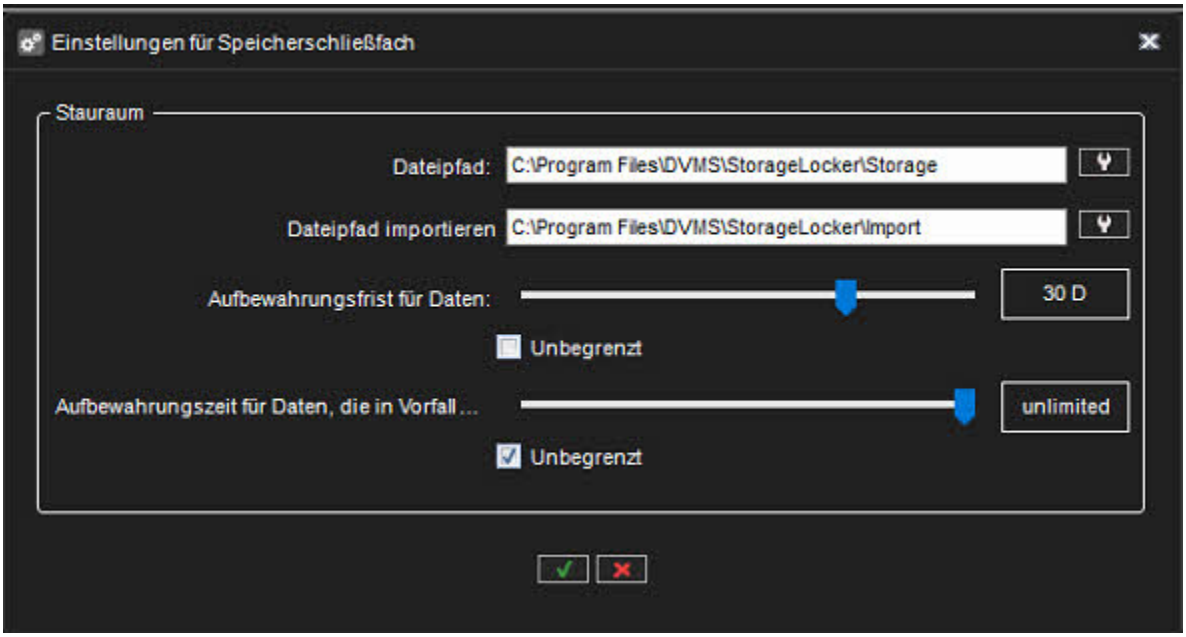


8.2.9.3 Die Aufbewahrungszeit für Daten

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

8.2.9.4 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

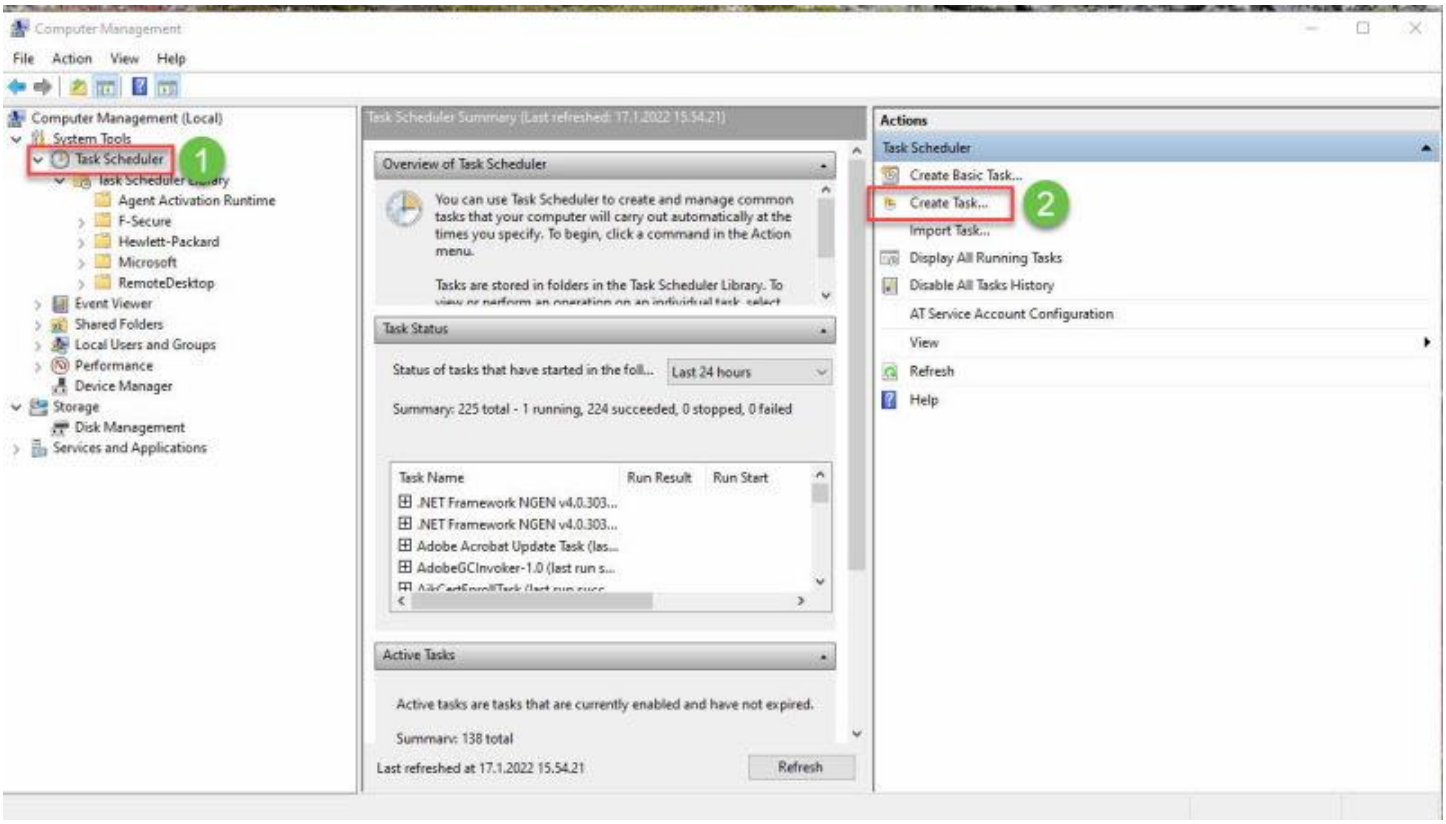


8.2.9.5 Schritte zum Zuordnen eines Netzlaufwerks, das für Storage Locker-Daten verwendet werden kann

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**

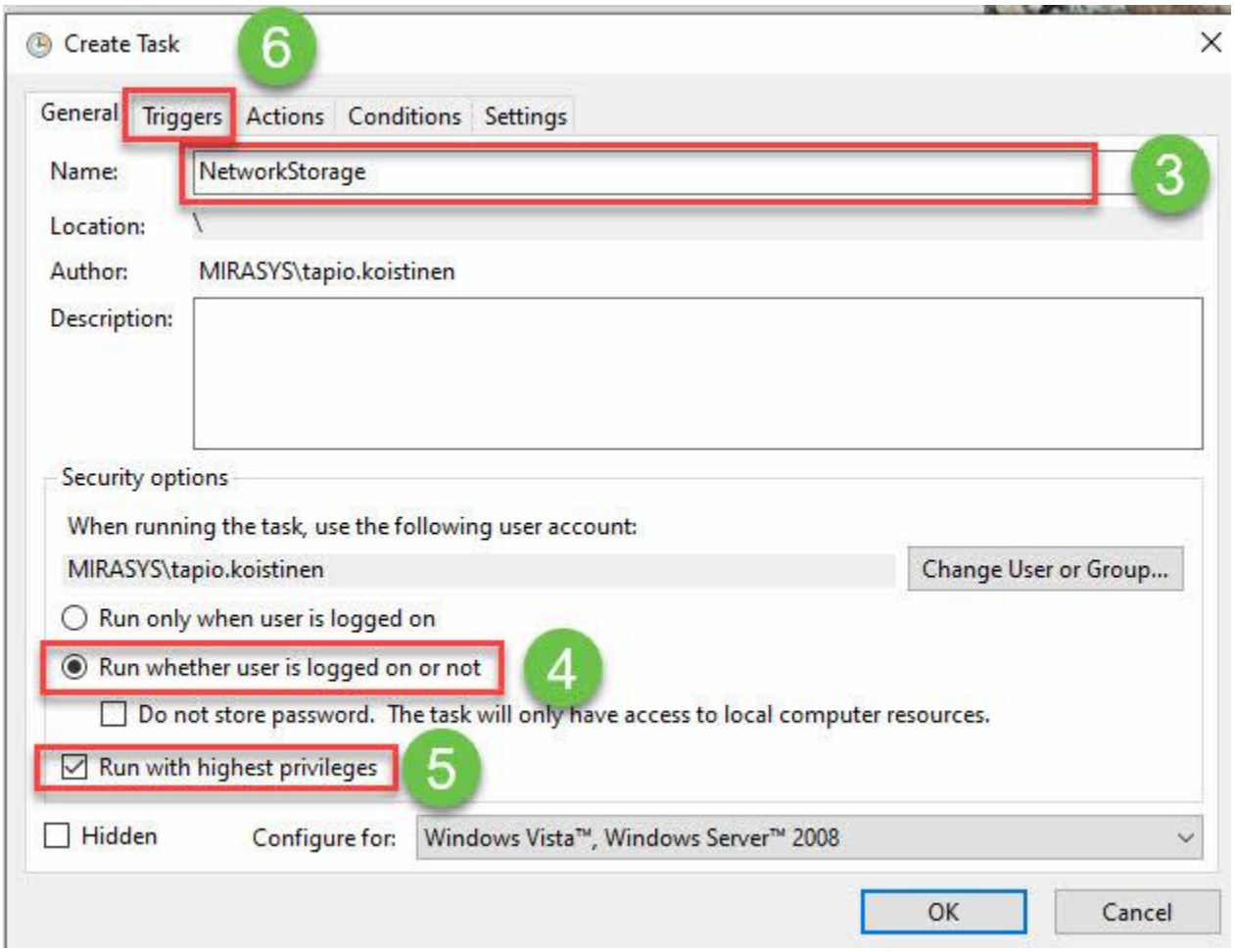


3. Name eingeben

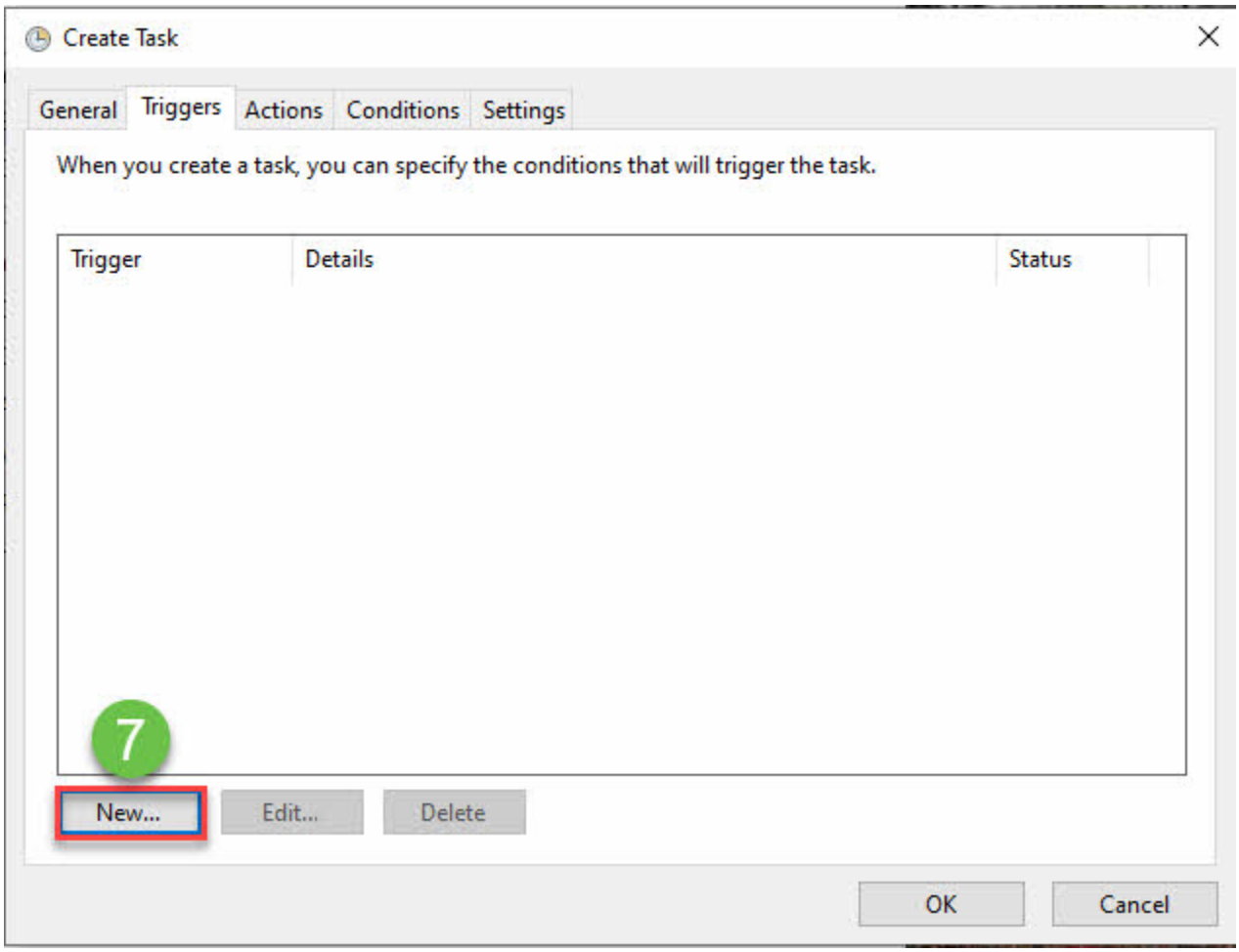
4. Ermöglichen **Run whether the user is logged on or not**

5. Ermöglichen **Run with highest privilege**

6. Offen **Triggers**

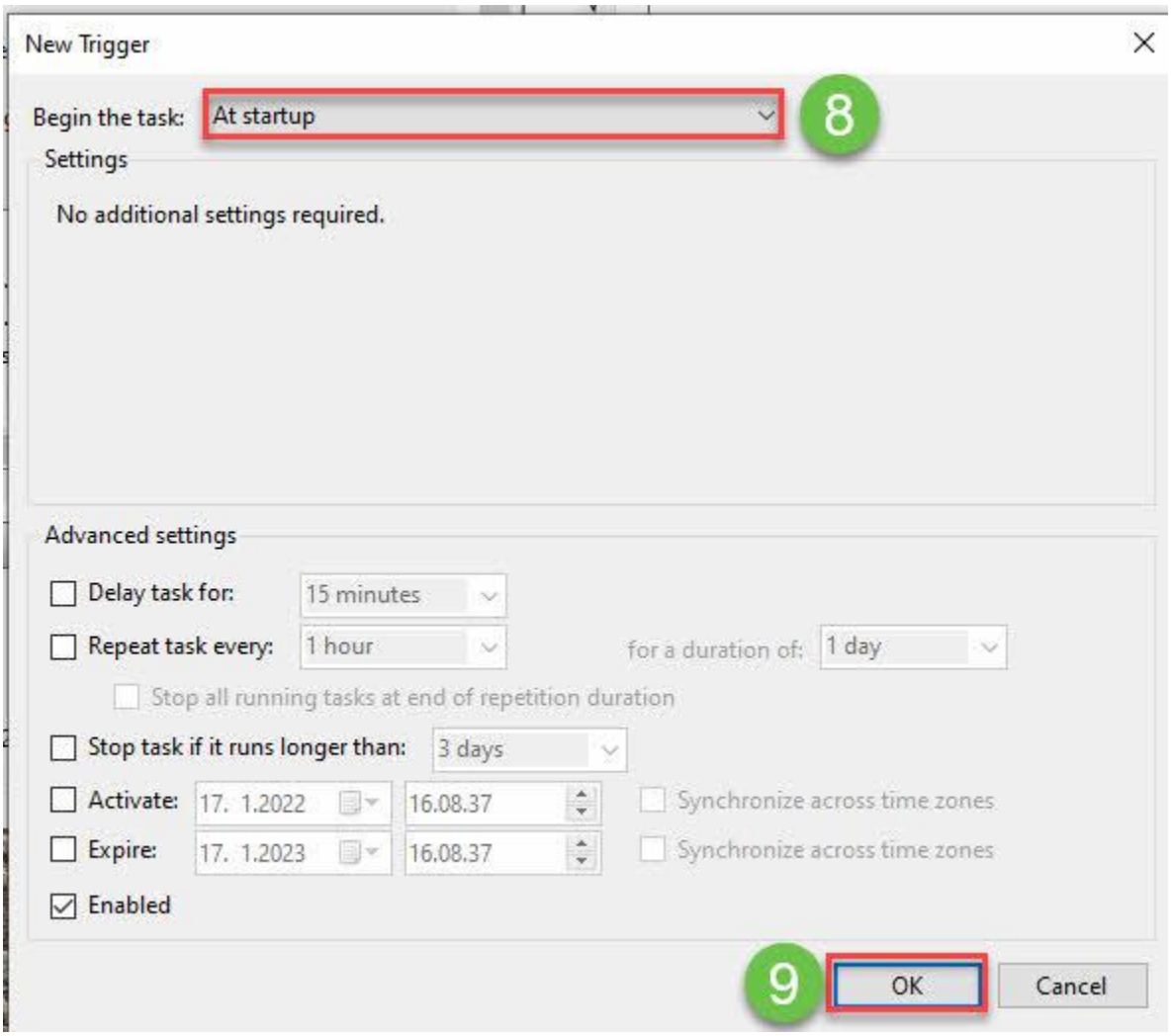


7. Klicken **New**



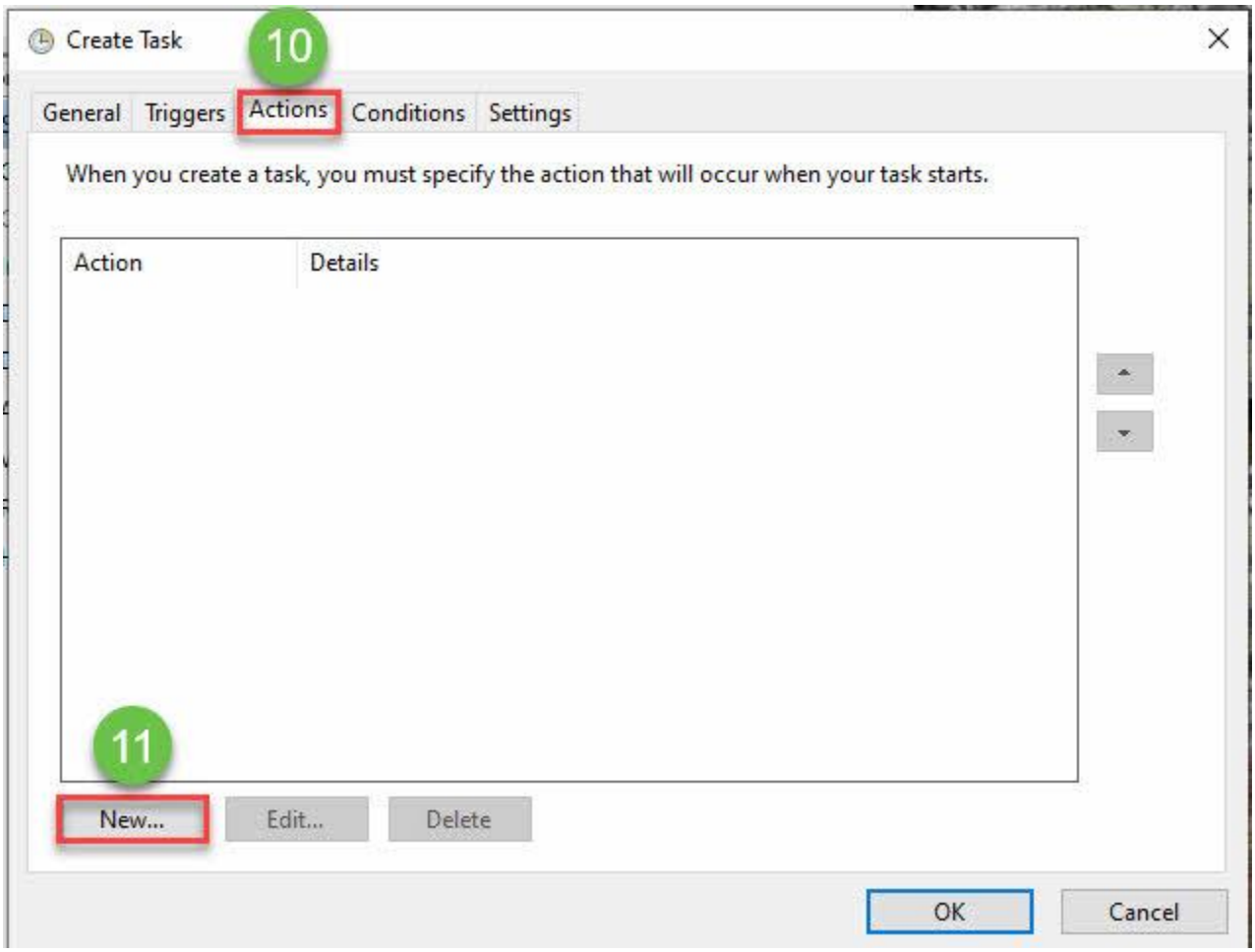
8. wählen At startup from the Begin the task dropdown list

9. Klicken**OK**



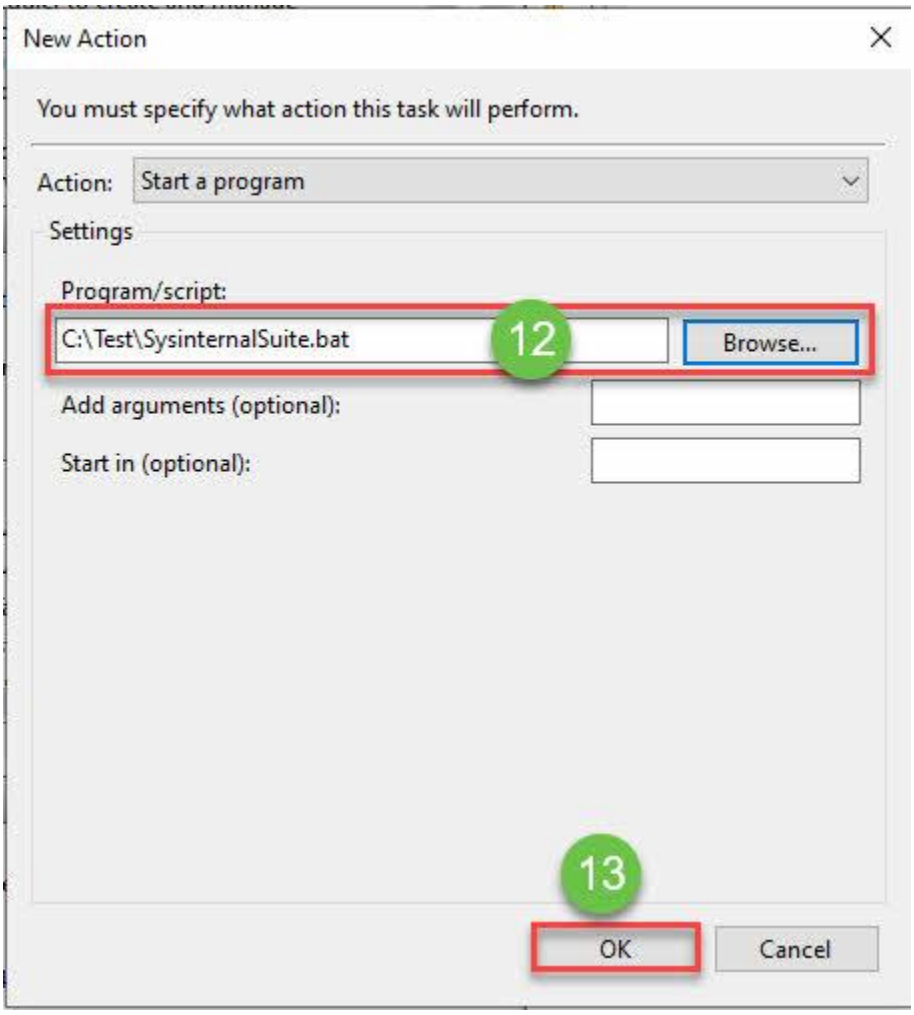
10. oppen **Actions**

11. Klicken **New**



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

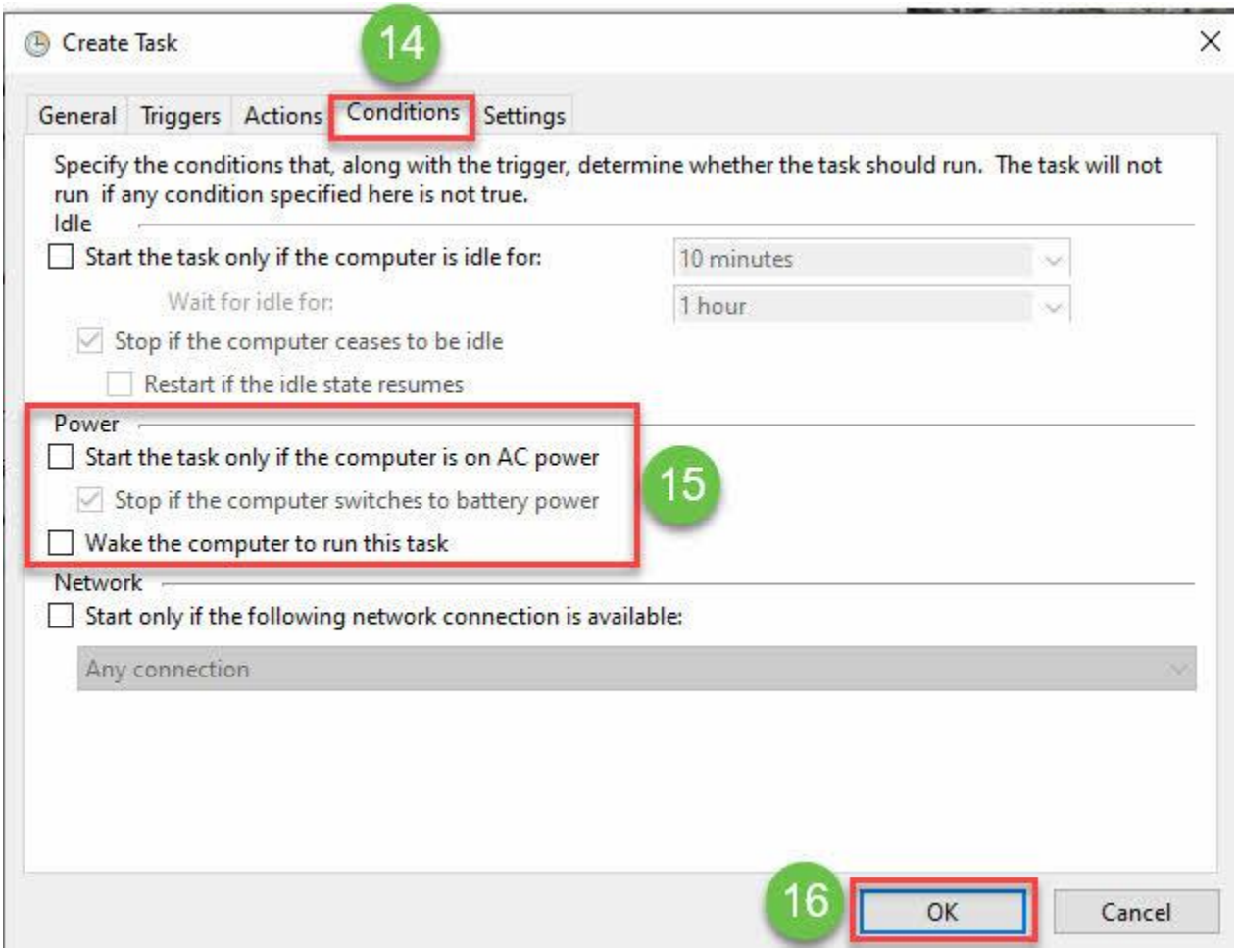
13. Klicken **OK**



14. oppen**Conditions**

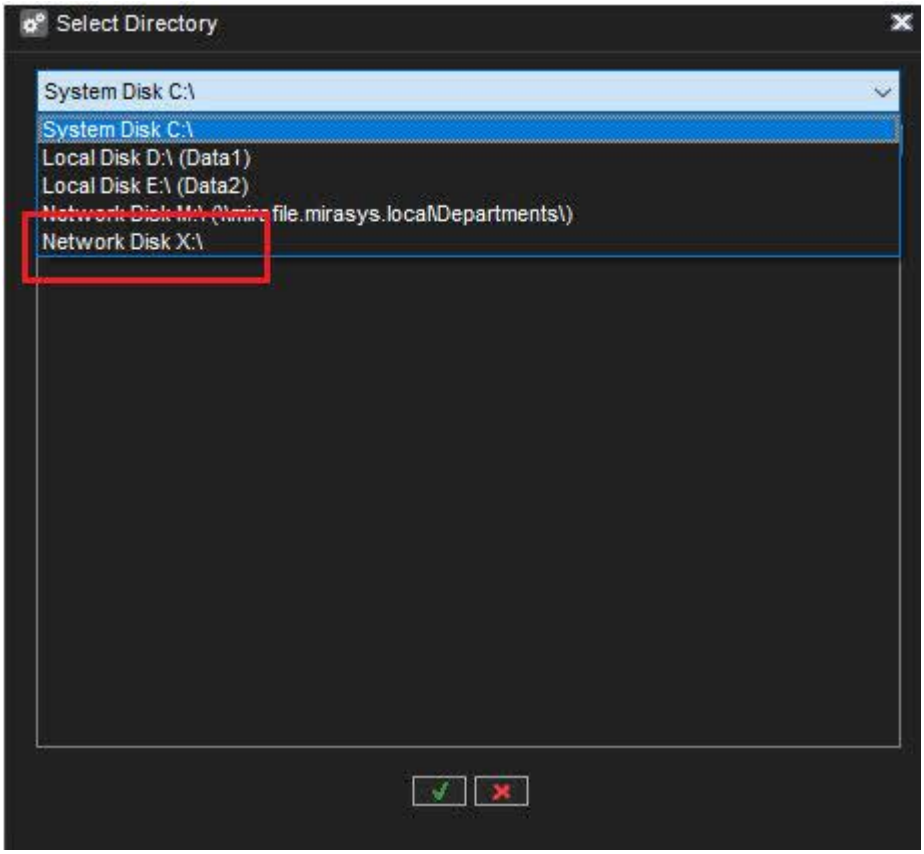
15. Deaktivieren **tart the task only if the computer is on AC power** and **Wake the computer to run this task**

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**

8.2.10 Storage Locker Einstellungen

Storage Locker Settings enthält die folgenden Werte:

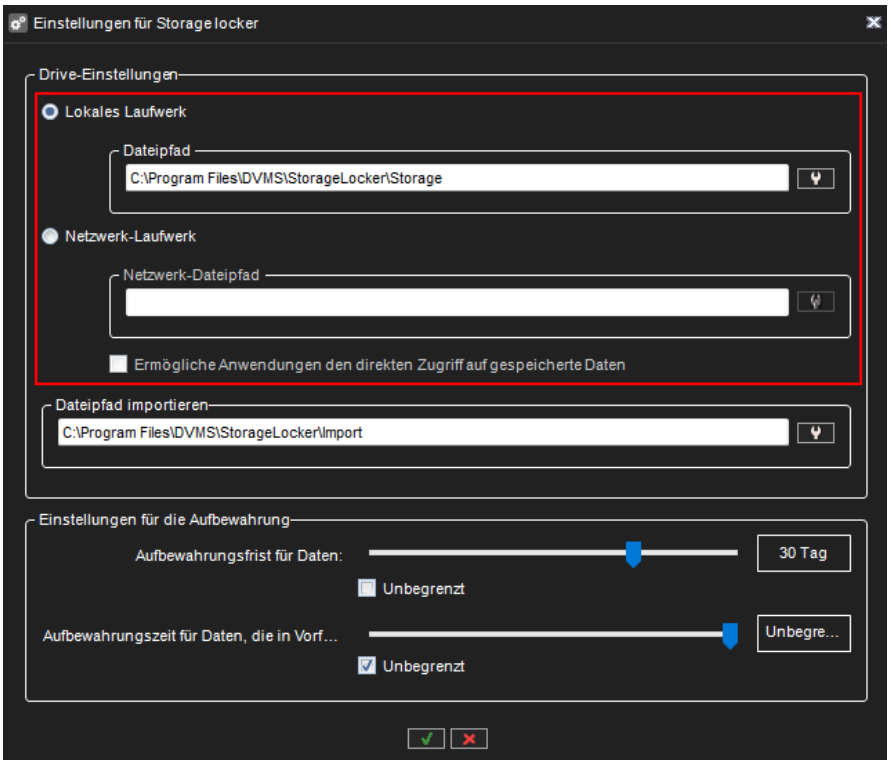
8.2.10.1 Dateipfad:

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 Master-Servers.Ändern des Dateipfads

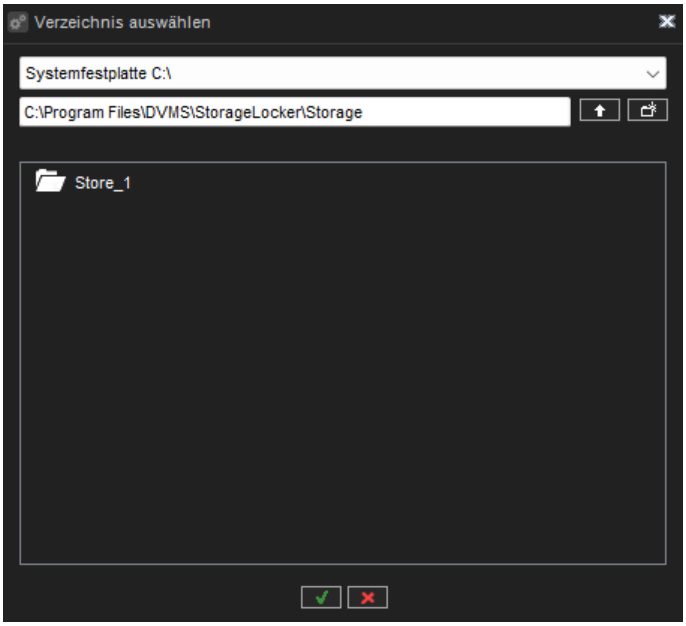
8.2.10.2 Ändern des Dateipfads

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

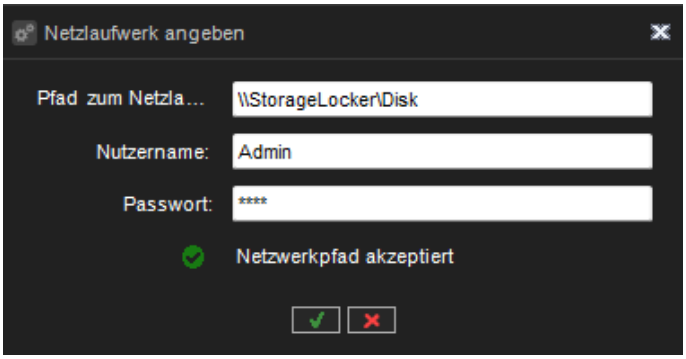
1. Wählen Sie, ob ein lokales Laufwerk oder ein Netzlaufwerk verwendet werden soll.



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.

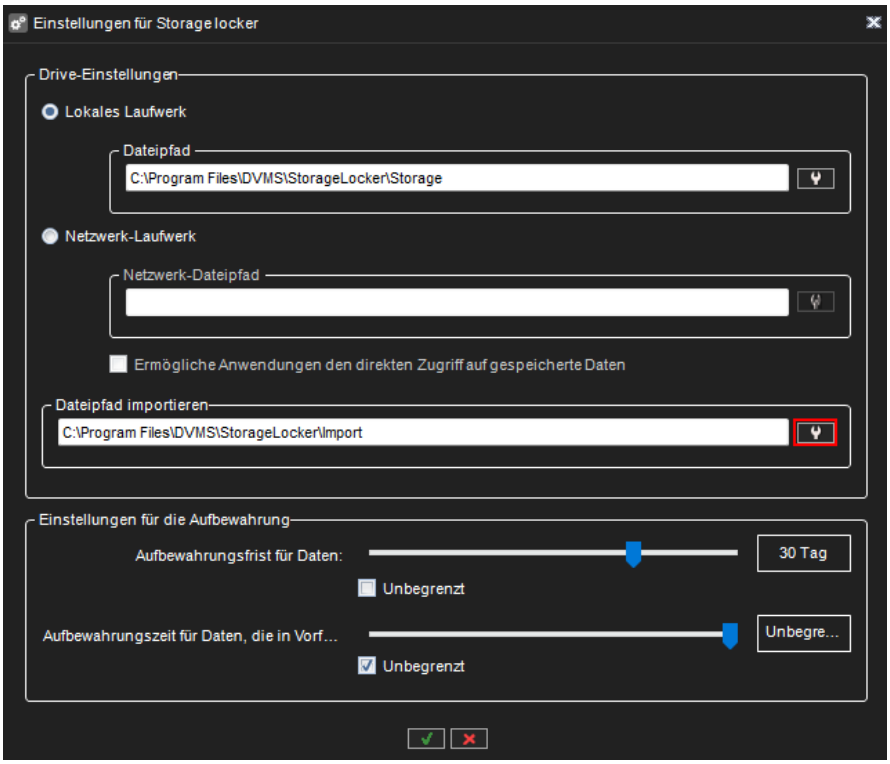


Wenn ein Netzlaufwerk für die Speicherung von Storage Locker-Daten verwendet wird, ist es möglich, Spotter-Anwendungen den direkten Zugriff auf gespeicherte Daten vom Netzlaufwerk zu gestatten, indem Sie die Option Anwendungen den direkten Zugriff auf gespeicherte Daten erlauben aktivieren.

8.2.10.3 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)

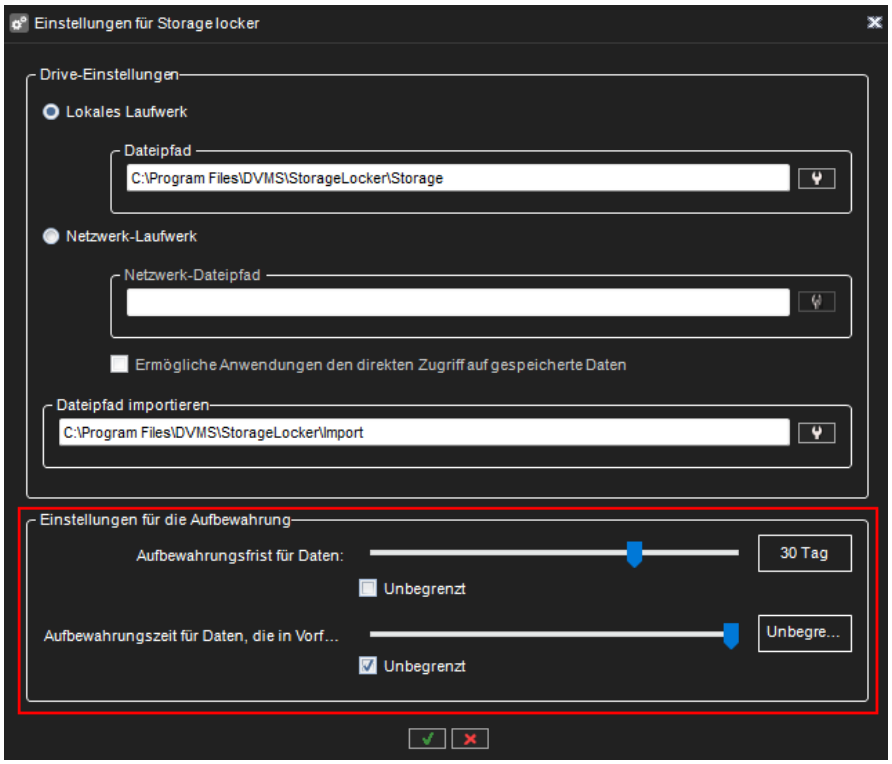


8.2.10.4 Die Aufbewahrungszeit für Daten

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

8.2.10.5 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



8.2.11 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

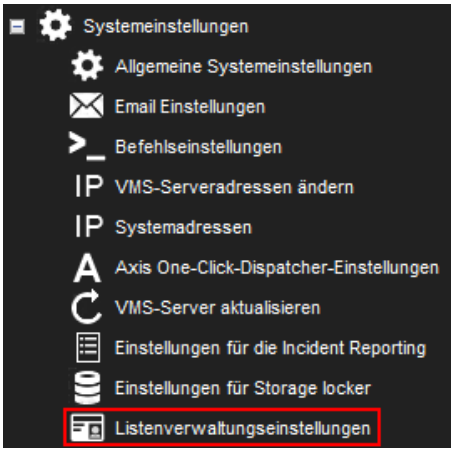
Die Systemmanager-Anwendung bietet mehrere Dialoge für den Zugriff und die Änderung von Daten und Einstellungen des Listenverwaltungsdienstes. Die Dialoge finden Sie im Abschnitt "Systemeinstellungen".

> Die Integration erfordert eine LPR- und FR-Integrationslizenz.

8.2.11.1 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.

8.2.11.1.1 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.

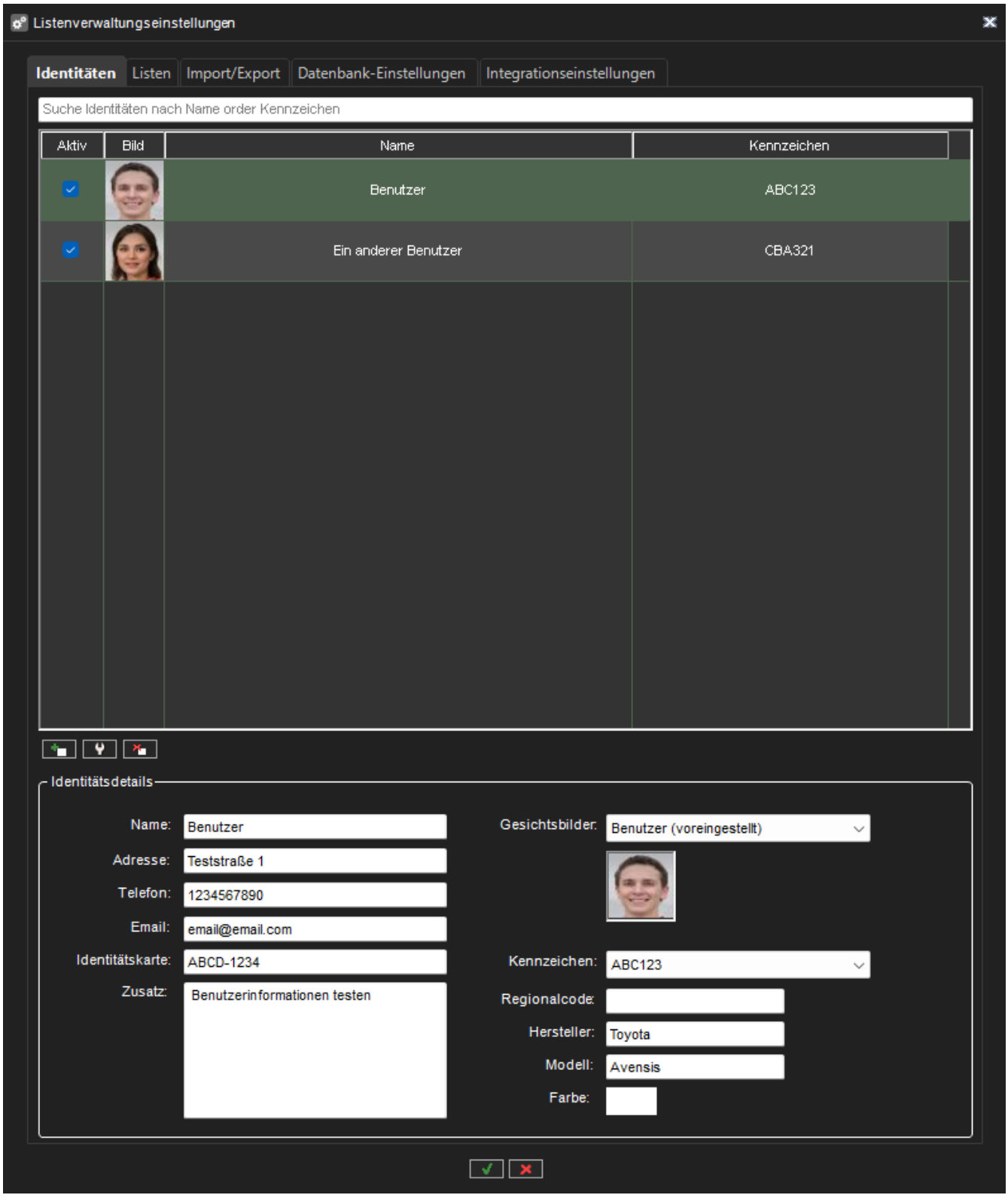
Nachfolgend finden Sie eine detaillierte Beschreibung der einzelnen Registerkarten.

8.2.11.1.1.1 Registerkarte "Identitäten

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

MIRASYS
DEEP VISION DATA COMPANY

Admin Guide V9.8.0



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

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:

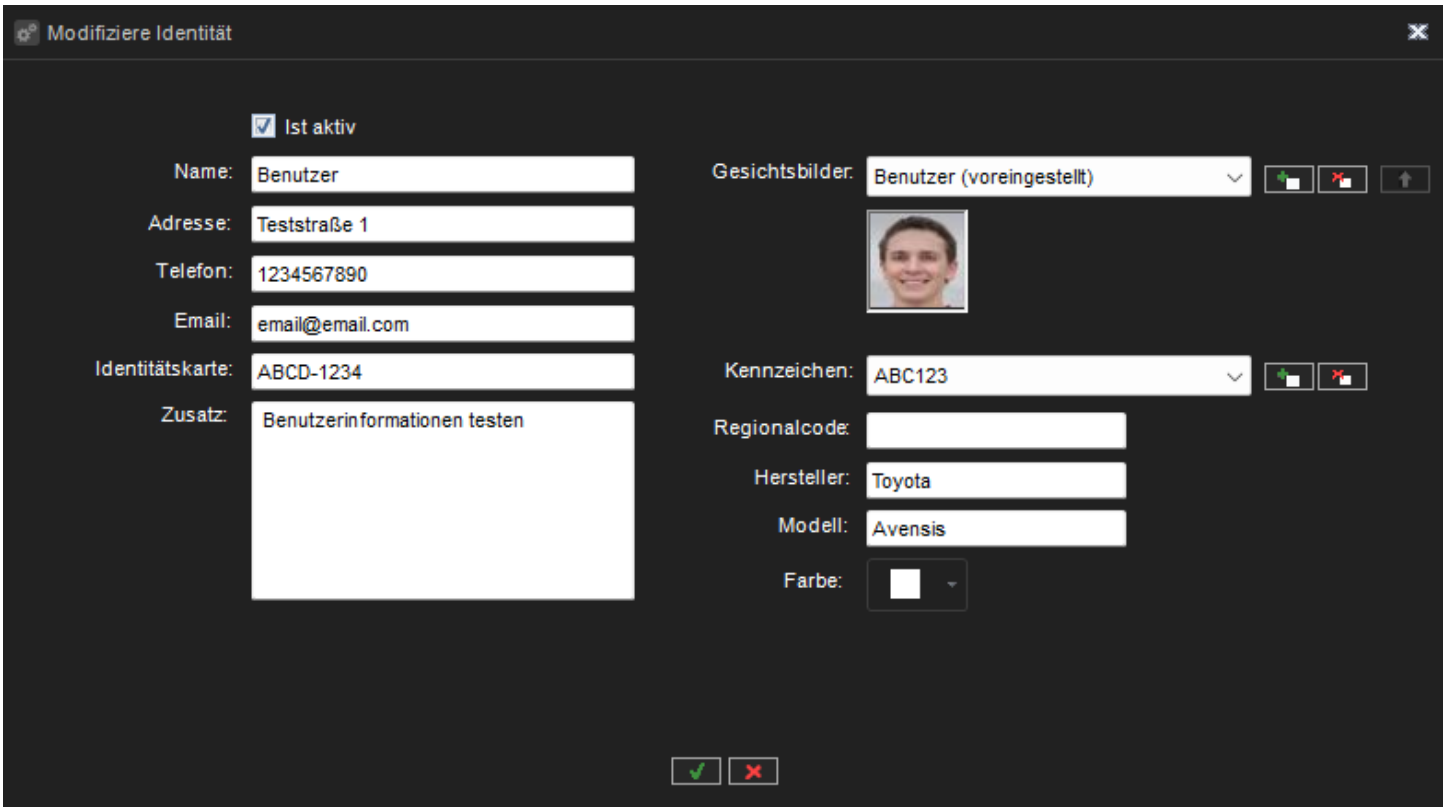


Figure 2 Dialog zum Hinzufügen/Ändern der Identität

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

Um ein Gesichtsbild hinzuzufügen, klicken Sie auf die Schaltfläche "Neues Gesichtsbild hinzufügen" und der folgende Dialog wird geöffnet:

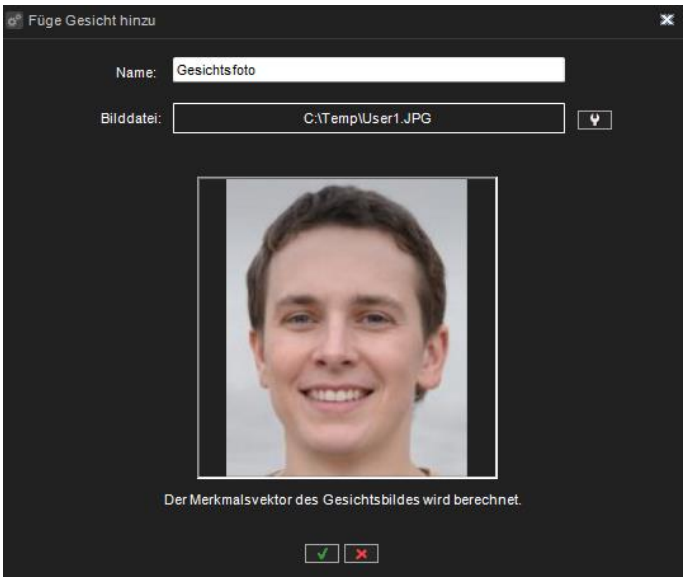


Figure 3 Dialog zum Hinzufügen/Ändern der Identität

Für eine Identität können mehrere Gesichtsbilder definiert werden. Alle Gesichtsbilder werden beim Identitätsabgleich verwendet, so dass die Verwendung mehrerer Gesichtsbilder für eine Identität die Zuverlässigkeit der Gesichtserkennung erhöhen kann.

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.

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

Um ein Gesichtsbild zu entfernen, müssen Sie es im Kombinationsfeld auswählen und auf die Schaltfläche Ausgewähltes Gesichtsbild entfernen klicken.

8.2.11.1.1.2 Gesichtsbild als Standard festlegen

Ein Gesichtsbild ist das Standardbild, das in allen Plugins und Identitätslisten als Miniaturbild verwendet wird. Um das Gesichtsbild als Standard festzulegen, müssen Sie das Gesichtsbild im

Kombinationsfeld auswählen und auf die Schaltfläche Ausgewähltes Gesichtsbild als Standard festlegen klicken:

Figure 4 Ausgewähltes Gesichtsbild als Standard festlegen

8.2.11.1.1.3 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:

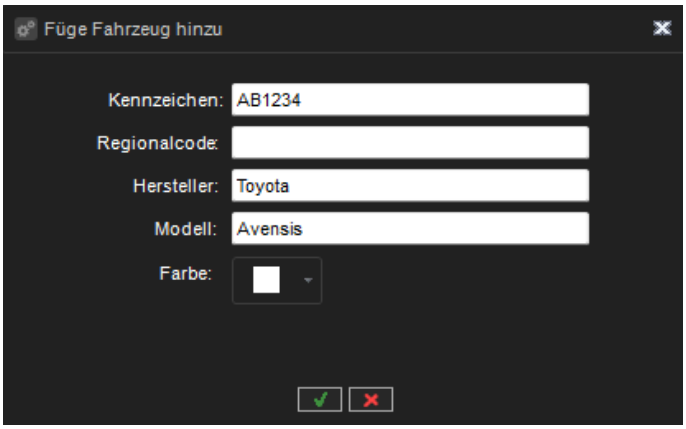


Figure 5 Dialogfeld "Fahrzeug hinzufügen

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.

8.2.11.1.1.4 Registerkarte Listen

Auf der Registerkarte Listen können Sie Operationen mit Identitätslisten durchführen:

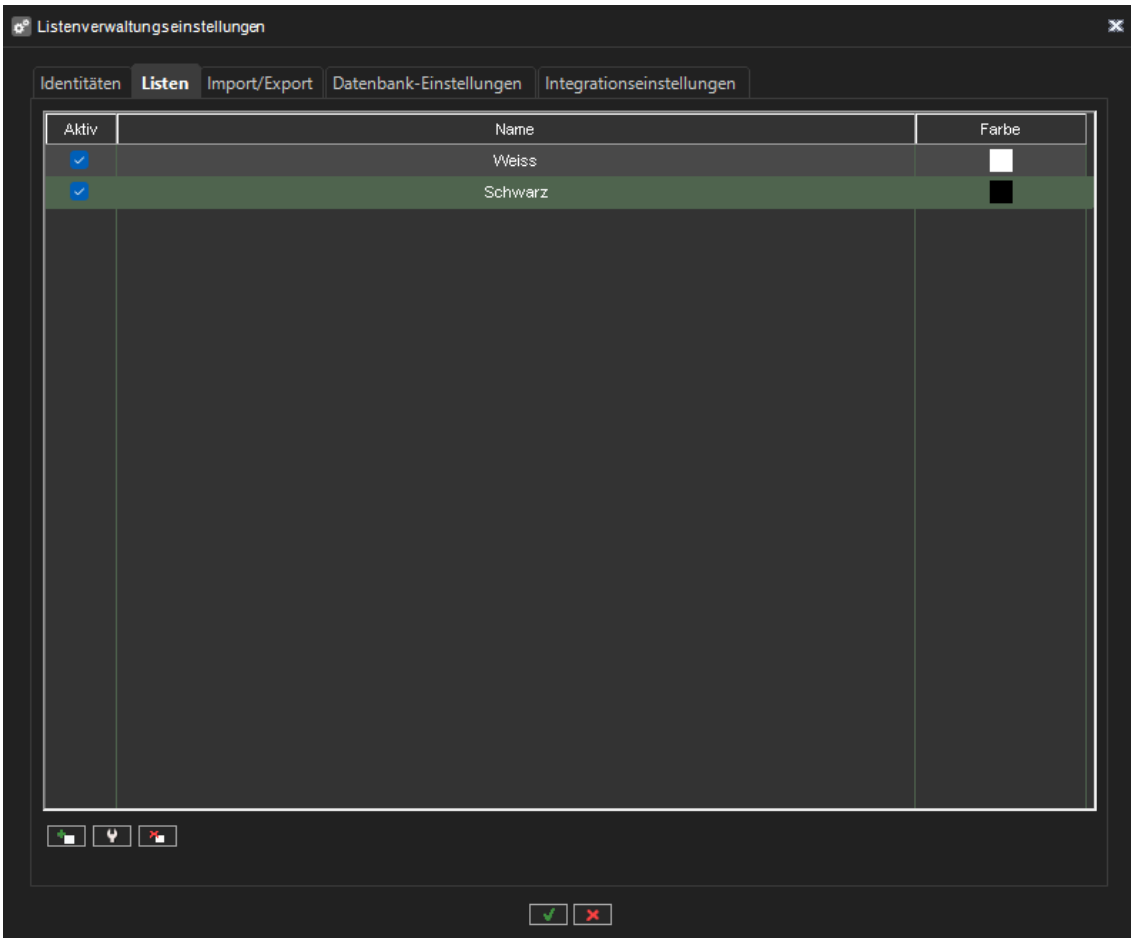


Figure 6 Registerkarte "Listen

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:

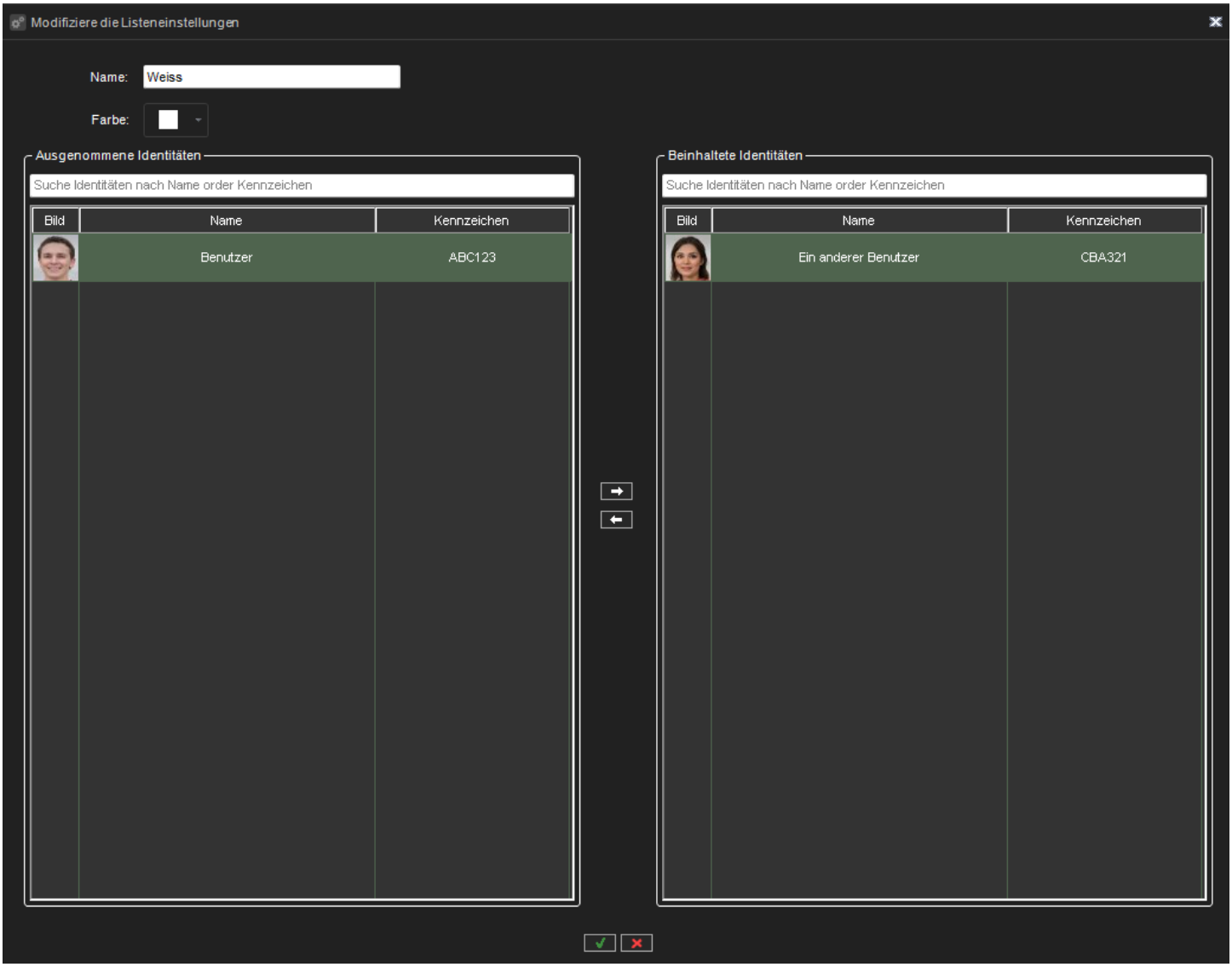


Figure 7 Dialogfeld zum Hinzufügen/Ändern von Listeneinstellungen

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

8.2.11.1.1.5 Registerkarte "Import/Export

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

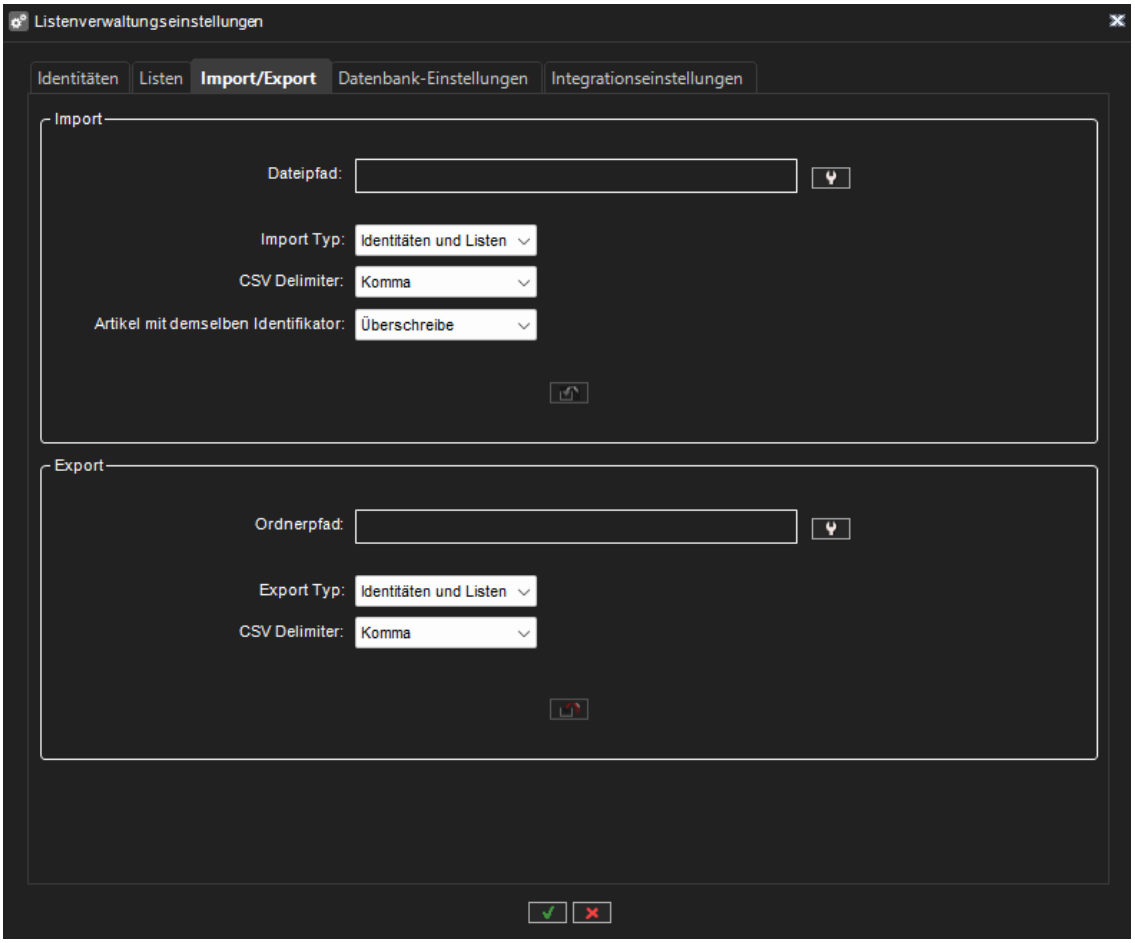


Figure 8 Registerkarte Import/Export

8.2.11.1.1.6 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.

8.2.11.1.1.7 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"

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.

Registerkarte "Datenbankeinstellungen

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

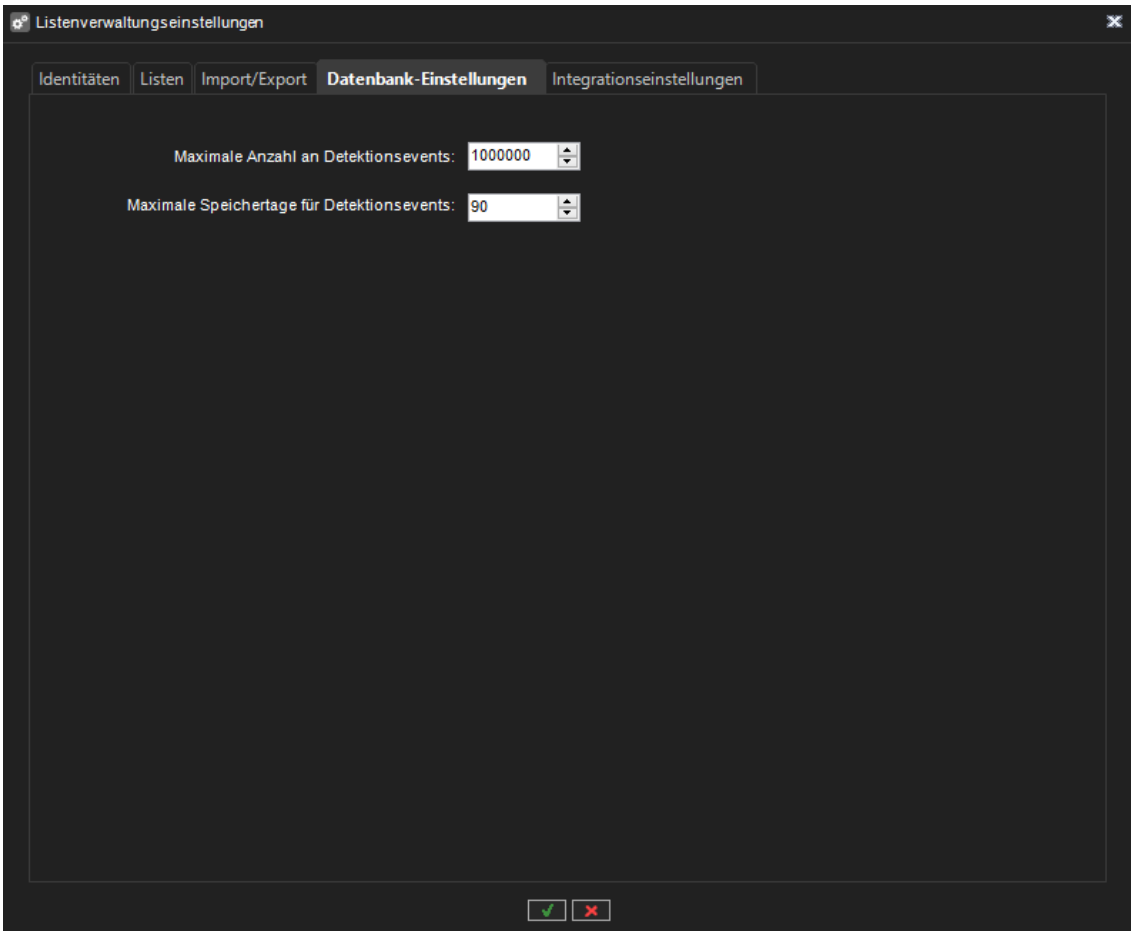


Figure 9 Registerkarte Datenbankeinstellungen

8.2.11.1.1.8 Registerkarte Integrationseinstellungen

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

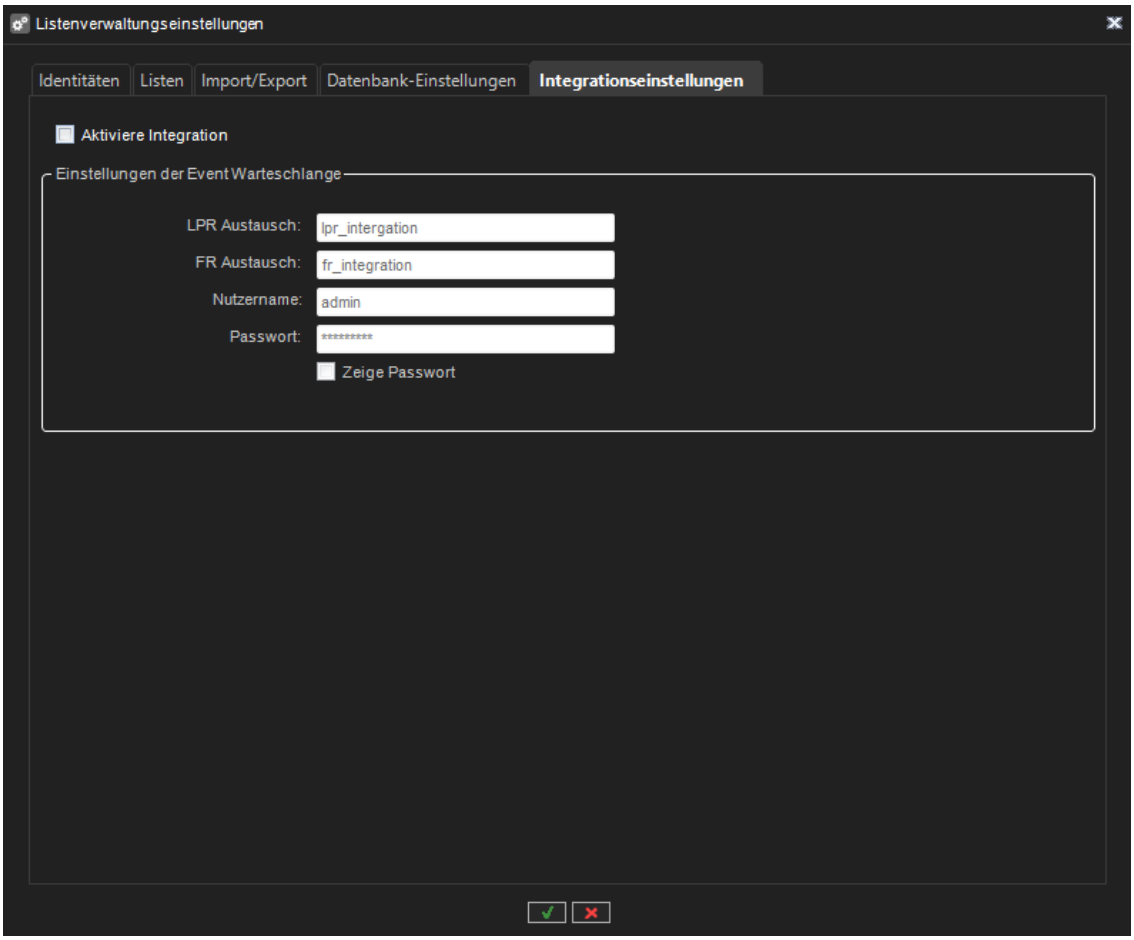


Figure 10 Registerkarte "Integrationseinstellungen

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.

8.2.11.2 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:

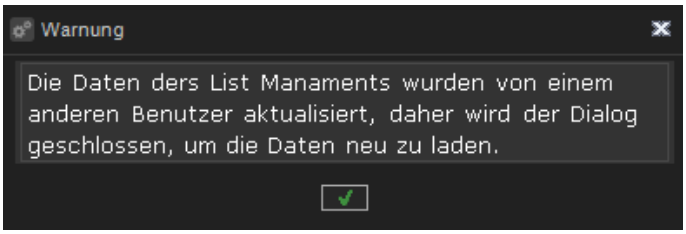
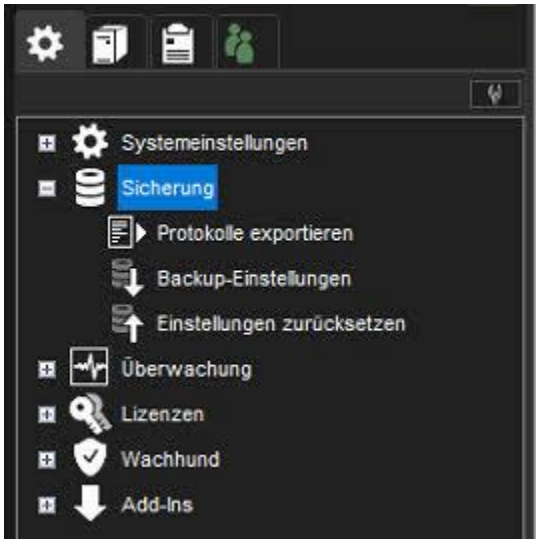


Figure 11 Warnung vor Datenaktualisierung

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.

8.3 SICHERUNG



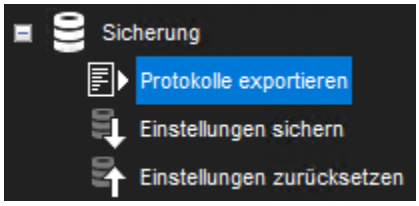
8.3.1 Protokolle exportieren

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.

8.3.1.1 Exportieren von Protokolldateien über System Manager

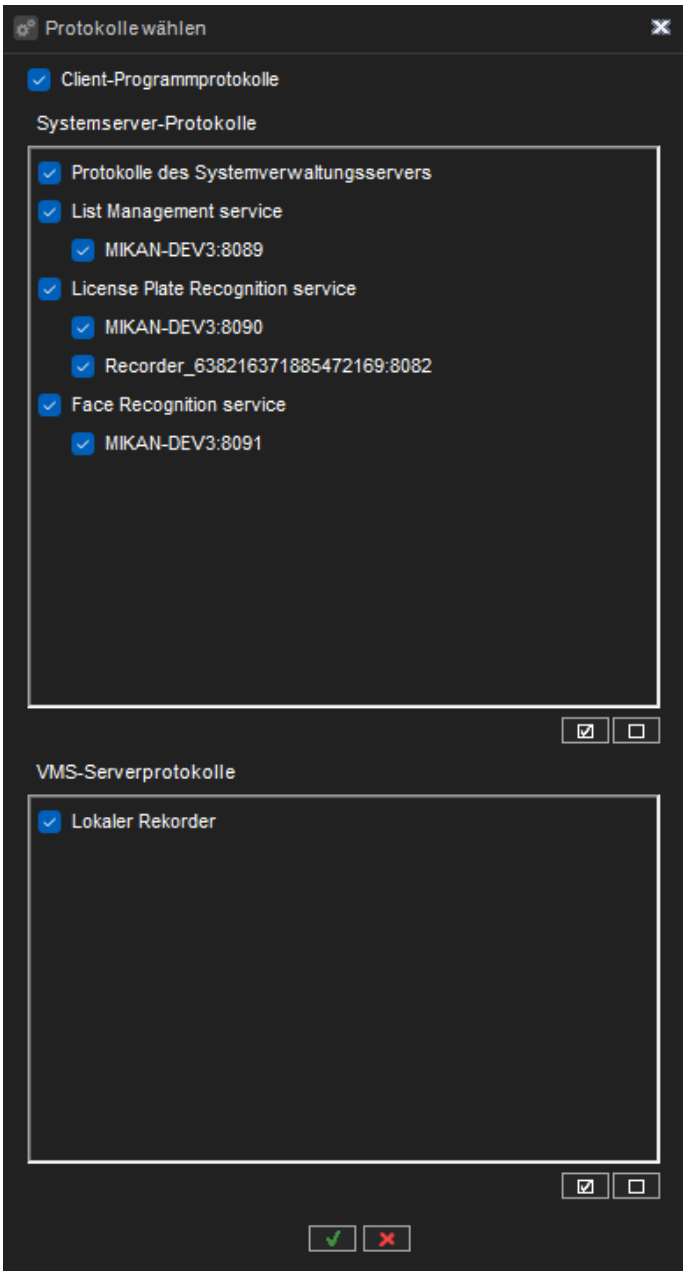
1. Öffnen Sie die Anwendung System Manager für Exportprotokolle und wählen Sie auf der Registerkarte System im Baumelement Backup den Unterpunkt Exportprotokolle.



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.

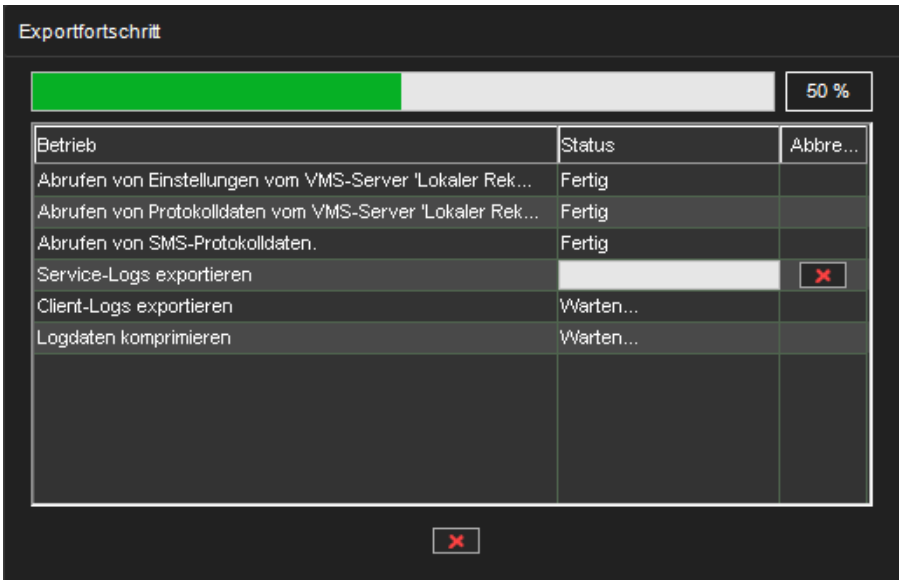
3. Click **OK**.

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.

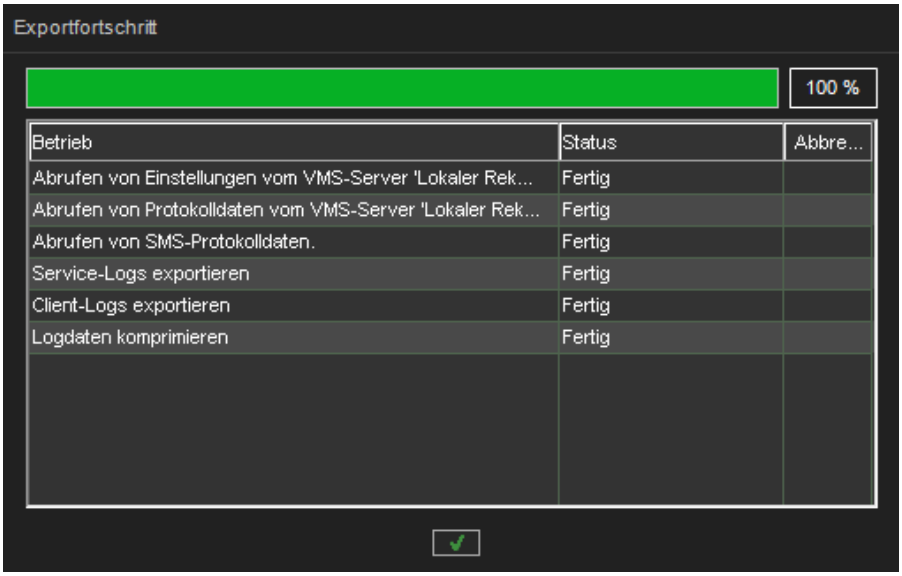
Type a name for the ZIP file in the **Name** fields and click **OK**

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:

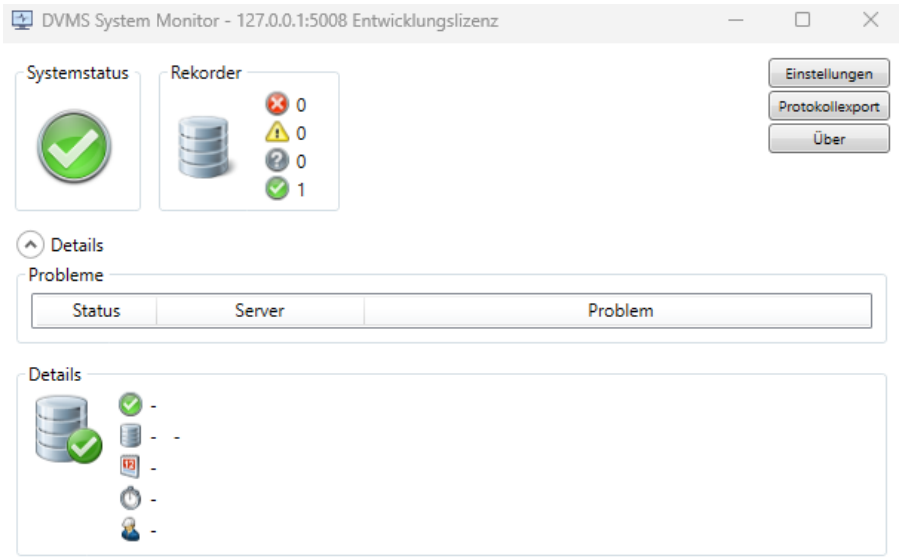
FRService_ROMANA-DEV1_8091_Log.zip
LMService_ROMANA-DEV1_8089_Log.zip
LPRService_ROMANA-DEV1_8090_Log.zip
SpotterAuditLog_9.6.0.68.txt
SpotterAuditLog_9.6.0.70.txt
SpotterLog_9.6.0.68.txt
SpotterLog_9.6.0.70.txt
SpotterLog_9.6.0.70.txt.1
SpotterLog_9.6.0.70.txt.2
SpotterLog_9.6.0.70.txt.3
SpotterLog_9.6.0.70.txt.4
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.

8.3.1.2 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:



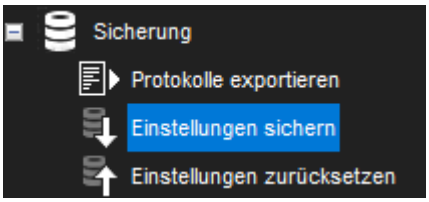
2. Choose the archive name and path for saving in the **Save as** dialog to save export archive.

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.

8.3.2 Backup-Einstellungen

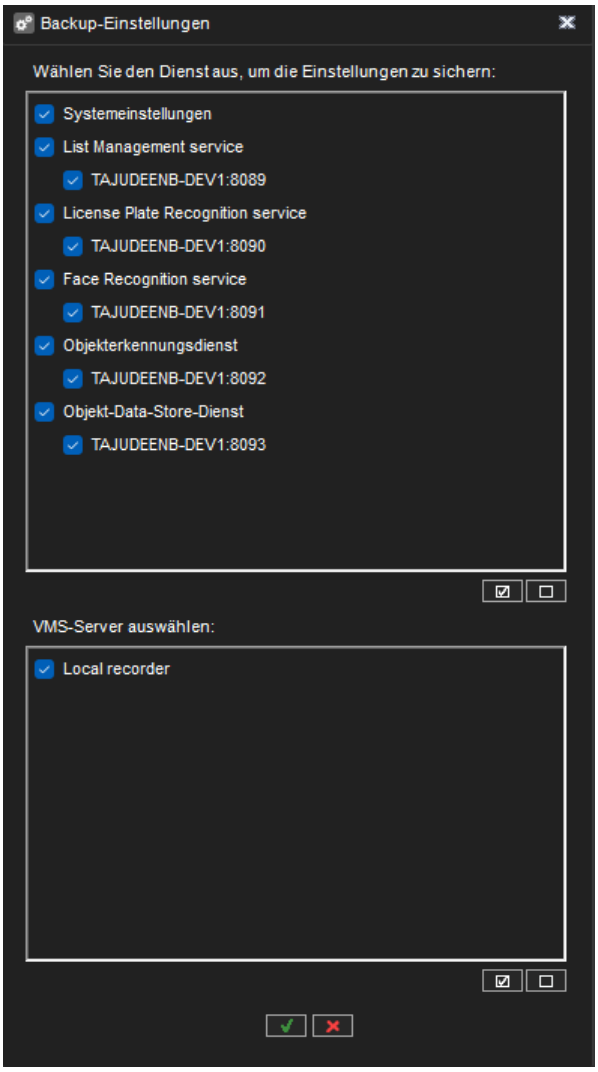


Systemeinstellungen sichern, um sie wiederherstellen zu können, wenn die Festplatte, die die Einstellungen enthält, ausfällt.

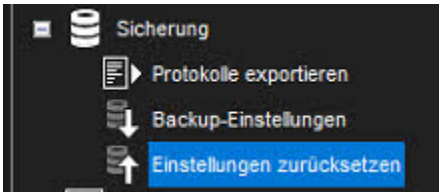
- Sie können Systemeinstellungen und Servereinstellungen sichern.
- Systemeinstellungen enthalten Daten über die Server, Profile und Benutzerkonten.
- VMS-Servereinstellungen enthalten Daten über die mit den Servern verbundene Geräte und deren Parameter.
- Sie können die Sicherungskopie auf einer Festplatte,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

8.3.2.1 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.



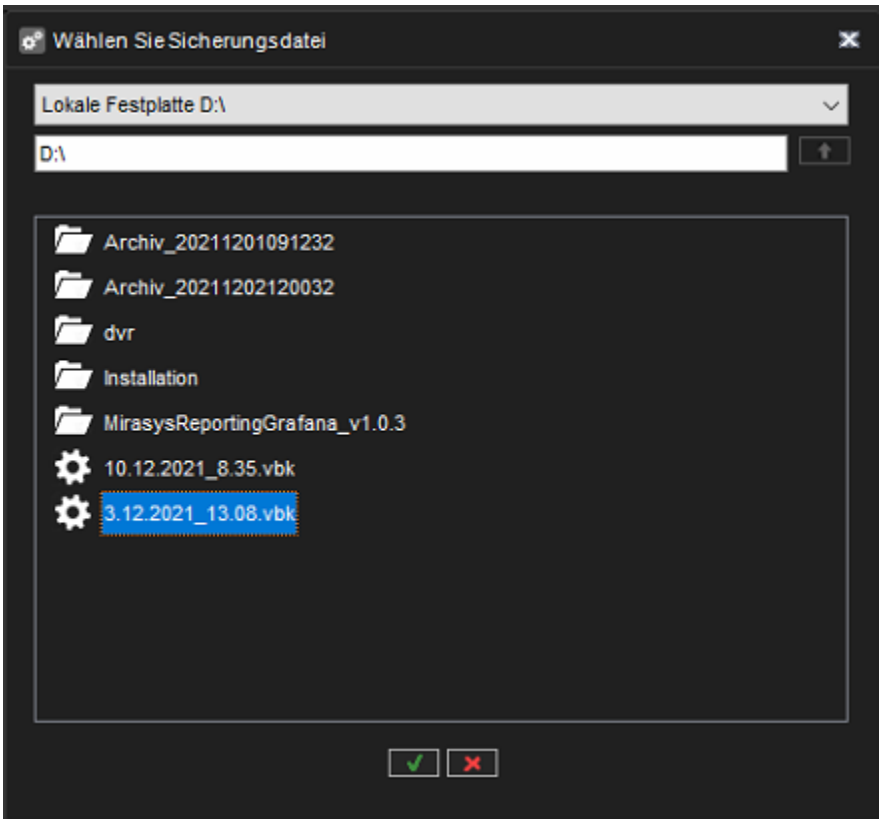
8.3.3 Einstellungen zurücksetzen



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

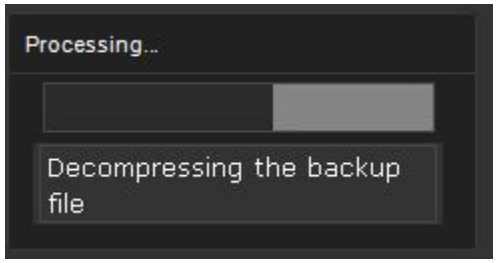
So stellen Sie die Einstellungen wieder her:

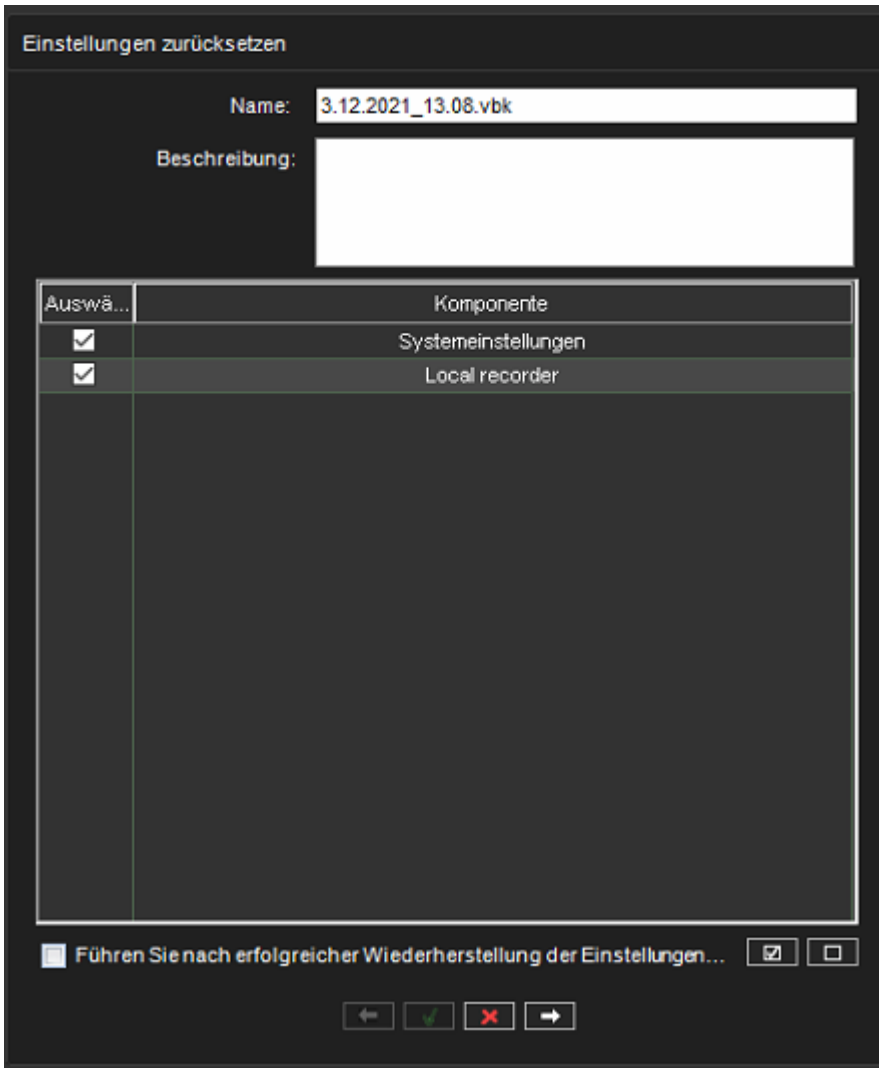
1. Öffnen Sie auf der Registerkarte System die Einstellungen zum Wiederherstellen. Das Dialogfeld Sicherungsdatei auswählen wird angezeigt



2. Suchen und wählen Sie die Sicherungsdatei (.vbk) aus und klicken Sie auf Das System dekomprimiert die Datei und zeigt dann das Dialogfeld Einstellungen wiederherstellen an.

- Die Dialogbox zeigt auch eine Beschreibung der Einstellungen





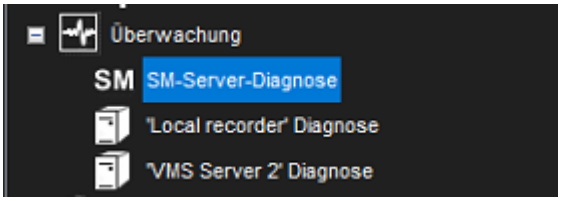
3. Wählen Sie die system- und serverspezifischen Einstellungen aus, die Sie wiederherstellen möchten, und klicken Sie auf Wiederherstellung starten. Die Einstellungen werden wiederhergestellt

4. Klicken Sie auf OK, um die neuen Einstellungen zu übernehmen, oder starten Sie den Wiederherstellungsvorgang erneut, um zum Dialog Einstellungen wiederherstellen zurückzukehren

Führen Sie nach erfolgreicher Wiederherstellung der Einstellungen eine automatische Sicherung der Einstellungen durch, insbesondere wenn das System nach einem Failover wiederhergestellt wird.

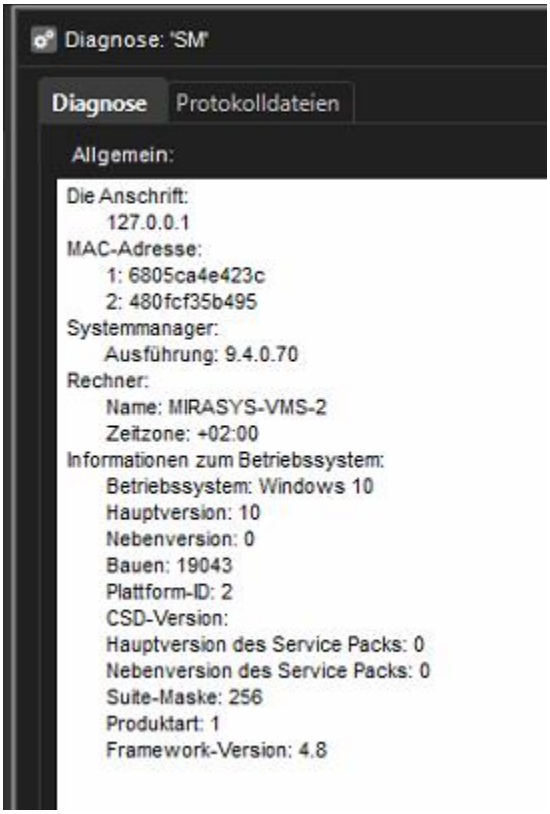
8.4 Überwachung

8.4.1 SM-Server-Diagnose



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

8.4.1.1 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

8.4.1.2 Protokolldateien

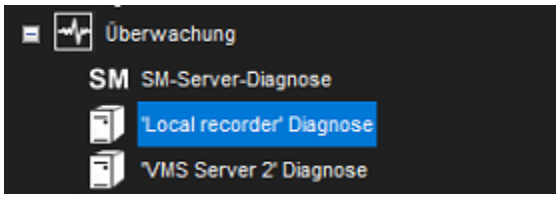
Bei Problemen mit dem System können Sie auf die Systemprotokolldateien auf der Registerkarte Protokolldateien zugreifen.

So untersuchen Sie eine Protokolldatei:

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

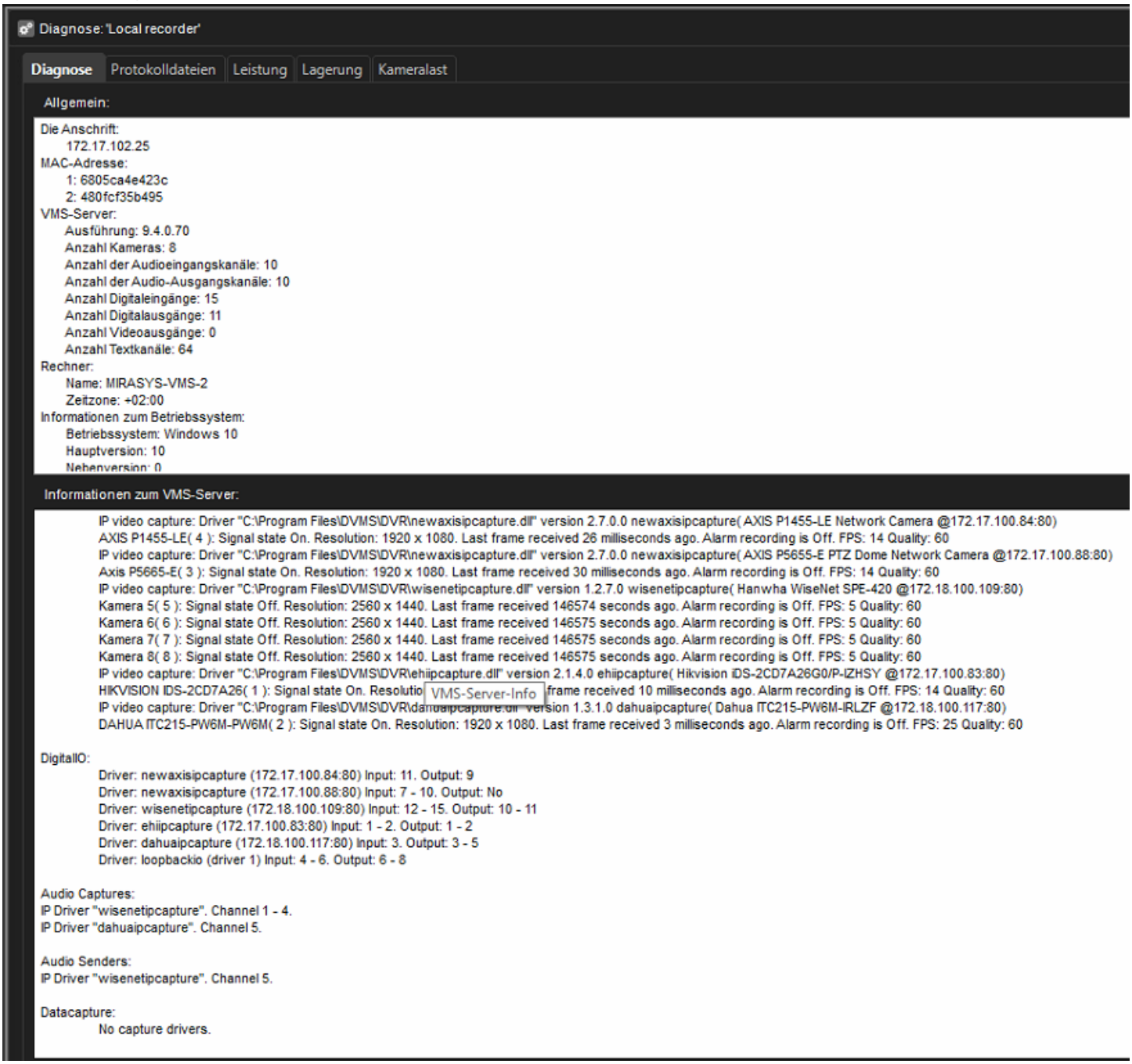
Der Inhalt wird im Inhalt der ausgewählten Protokolldatei angezeigt

8.4.2 Serverdiagnose



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

8.4.2.1 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

8.4.2.2 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

8.4.2.3 Leistung

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

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

8.4.2.4 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.

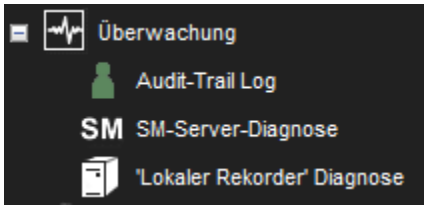
Durchschnittliche Stichprobengröße. Die durchschnittliche Stichprobengröße von Textdaten.

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.

8.4.3 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".



8.4.3.1 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.

8.4.3.2 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

8.4.3.3 Ergebnisliste

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

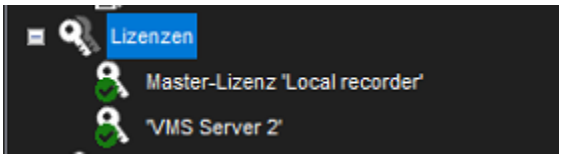
- **Zeit** - Zeitpunkt der Benutzeraktion.
- **Benutzer** - Benutzername, der die Benutzeraktion durchgeführt hat.
- **Anwendung** - Anwendung, in der die Benutzeraktion durchgeführt wurde.

- **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.

8.4.3.4 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.

8.5 LIZENZEN

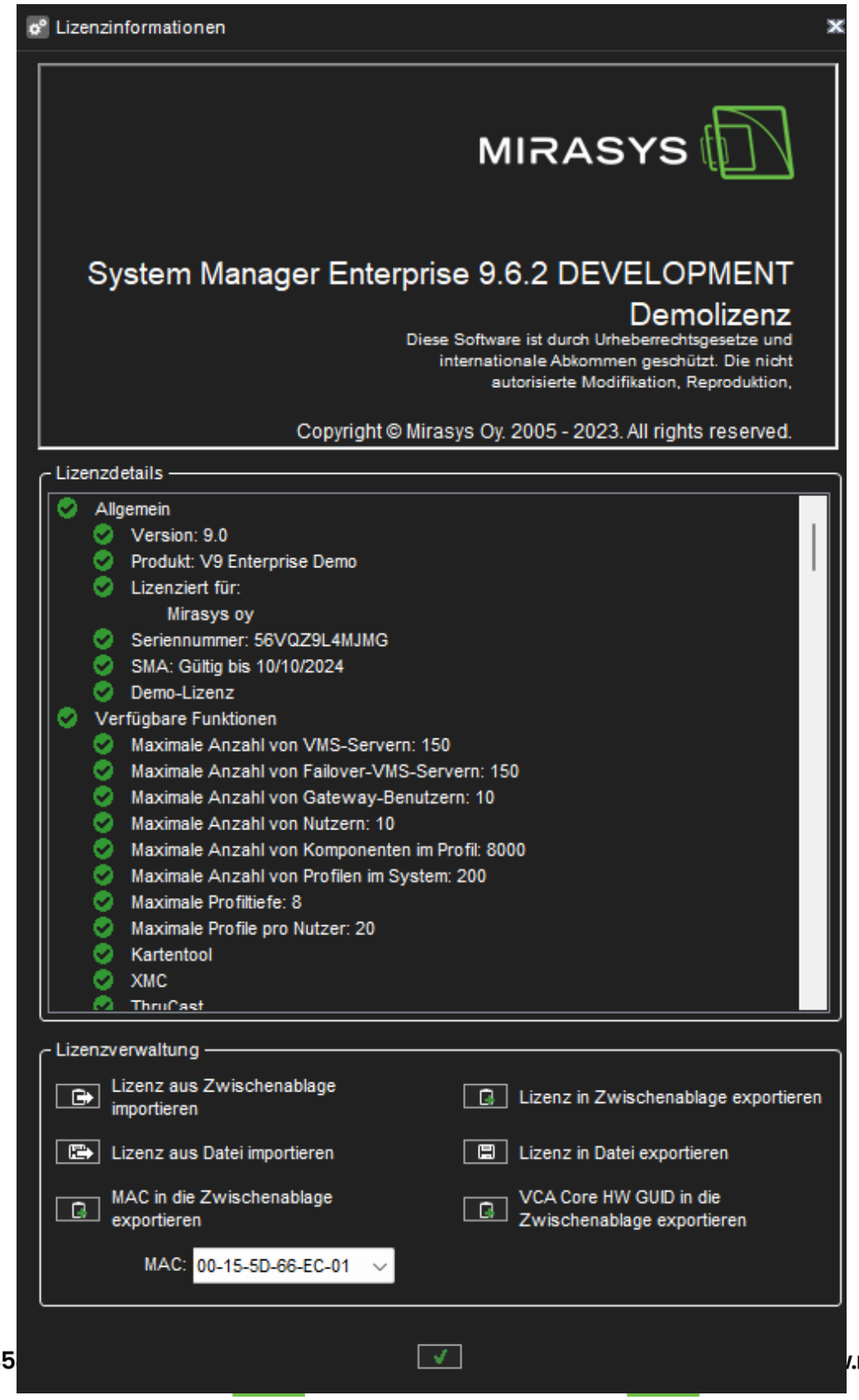


Der Server benötigt eine gültige Lizenz für die volle Funktionalität.
Je nach Installation müssen Sie möglicherweise die Lizenzinformationen aktualisieren, wenn Sie neue Funktionen oder Kameras zum System hinzufügen.
Um einen Lizenzschlüssel zu erhalten, wenden Sie sich bitte an Ihren Lieferanten und befolgen Sie das Lizenz-Upgrade-Verfahren wie folgt Details vom Anbieter.
Wenn Sie Probleme beim Upgrade der Lizenz haben, wenden Sie sich bitte an *orders@mirasys.com*
Sie können einem Server auch weitere Kamerakanäle und Funktionen wie VCA-Funktionen hinzufügen, indem Sie einen neuen Lizenzschlüssel erwerben.


Lizenzinformationen
MIRASYS
System Manager Enterprise 9.6.2 DEVELOPMENT
Demolizenz
Diese Software ist durch Urheberrechtsgesetze und internationale Abkommen geschützt. Die nicht autorisierte Modifikation, Reproduktion,
Copyright © Mirasys Oy. 2005 - 2023. All rights reserved.
Lizenzdetails
Allgemein
Version: 9.0
Produkt: V9 Enterprise Demo
Lizenziert für:
Mirasys oy
Seriennummer: 56VQZ9L4MJMG
SMA: Gültig bis 10/10/2024
Demo-Lizenz
Verfügbare Funktionen
Maximale Anzahl von VMS-Servern: 150
Maximale Anzahl von Failover-VMS-Servern: 150
Maximale Anzahl von Gateway-Benutzern: 10
Maximale Anzahl von Nutzern: 10
Maximale Anzahl von Komponenten im Profil: 8000
Maximale Anzahl von Profilen im System: 200
Maximale Profiltiefe: 8
Maximale Profile pro Nutzer: 20
Kartentool
XMC
Lizenzverwaltung
Lizenz aus Zwischenablage importieren
Lizenz in Zwischenablage exportieren
Lizenz aus Datei importieren
Lizenz in Datei exportieren
MAC in die Zwischenablage exportieren
VCA Core HW GUID in die Zwischenablage exportieren
MAC: 00-15-5D-66-EC-01

8.5.1 Lizenzdetails

Lizenzdetails zeigen alle unterstützten Funktionen der Lizenz.


Lizenzinformationen
MIRASYS
System Manager Enterprise 9.6.2 DEVELOPMENT
Demolizenz
Diese Software ist durch Urheberrechtsgesetze und internationale Abkommen geschützt. Die nicht autorisierte Modifikation, Reproduktion,
Copyright © Mirasys Oy. 2005 - 2023. All rights reserved.
Lizenzdetails
Allgemein
Version: 9.0
Produkt: V9 Enterprise Demo
Lizenziert für:
Mirasys oy
Seriennummer: 56VQZ9L4MJMG
SMA: Gültig bis 10/10/2024
Demo-Lizenz
Verfügbare Funktionen
Maximale Anzahl von VMS-Servern: 150
Maximale Anzahl von Failover-VMS-Servern: 150
Maximale Anzahl von Gateway-Benutzern: 10
Maximale Anzahl von Nutzern: 10
Maximale Anzahl von Komponenten im Profil: 8000
Maximale Anzahl von Profilen im System: 200
Maximale Profiltiefe: 8
Maximale Profile pro Nutzer: 20
Kartentool
XMC
Lizenzverwaltung
Lizenz aus Zwischenablage importieren
Lizenz in Zwischenablage exportieren
Lizenz aus Datei importieren
Lizenz in Datei exportieren
MAC in die Zwischenablage exportieren
VCA Core HW GUID in die Zwischenablage exportieren
MAC: 00-15-5D-66-EC-01

8.5.2 Lizenzverwaltung

8.5.2.1 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.

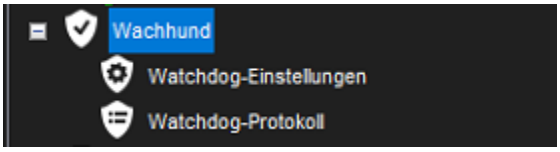
8.5.2.2 So exportieren Sie einen Lizenzschlüssel:

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.

8.5.2.3 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

8.6 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.

8.6.1 Watchdog-Einstellungen

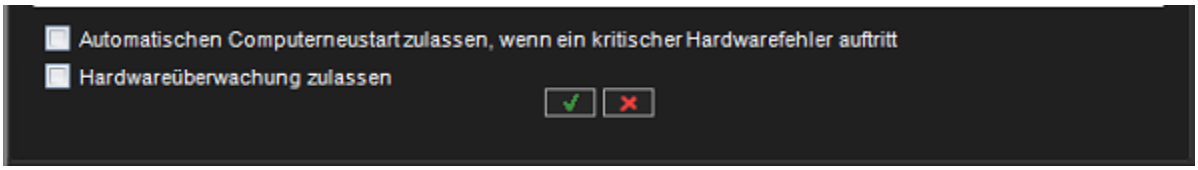
In den Watchdog-Einstellungen können Sie auswählen, welche Ereignisse einen Bericht auslösen, der an die unter E-Mail-Einstellungen
angegebenen E-Mail-Adressen gesendet wird. Sie können für jeden Server unterschiedliche Ereignisse auswählen.
Alternativ können Sie dieselben Ereignisse für alle Server 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.

8.6.1.1 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**.

8.6.1.2 Automatischer Neustart

Aktivieren Sie das Kontrollkästchen. **Ermöglichen Sie einen automatischen Neustart des Computers, wenn ein kritischer Hardwarefehler auftritt.** Um den Computer automatisch neu zu starten, wenn schwerwiegende Hardwarefehler auftreten.
Der Computer wird höchstens einmal am Tag neu gestartet. Wählen Sie **Hardwareüberwachung zulassen**.bei Bedarf



8.6.1.3 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**.

8.6.2 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**.

8.6.2.1 Zusätzliche Watchdog-Zustellungsmethoden

Die Watchdog-Funktionalität umfasst drei neue Protokolle: TCP, SMS (erfordert ein externes SMS-Modul) und anpassbares E-Mail-Formular.

Jedes neue Protokoll hat seinen Treiber:

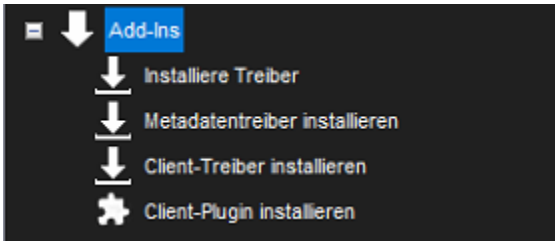
C:\Programme\DVMS\DVR\WDEventProviders\

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

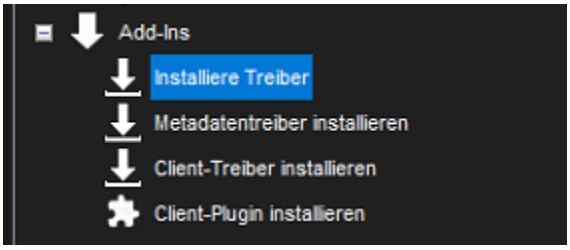
Derzeit müssen diese Dateien manuell bearbeitet werden. Jede XML-Datei enthält die Dokumentation zu den Konfigurationsoptionen.
Die neuen Konfigurationsoptionen umfassen gefilterte und bedingte Warnungen (z. B. „Warnung X nur einmal alle 60 Minuten senden“ oder „Warnung X nur senden, wenn Bedingung Y 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.

8.7 Add-Ins



8.7.1 Installieren externer Treiberpakete

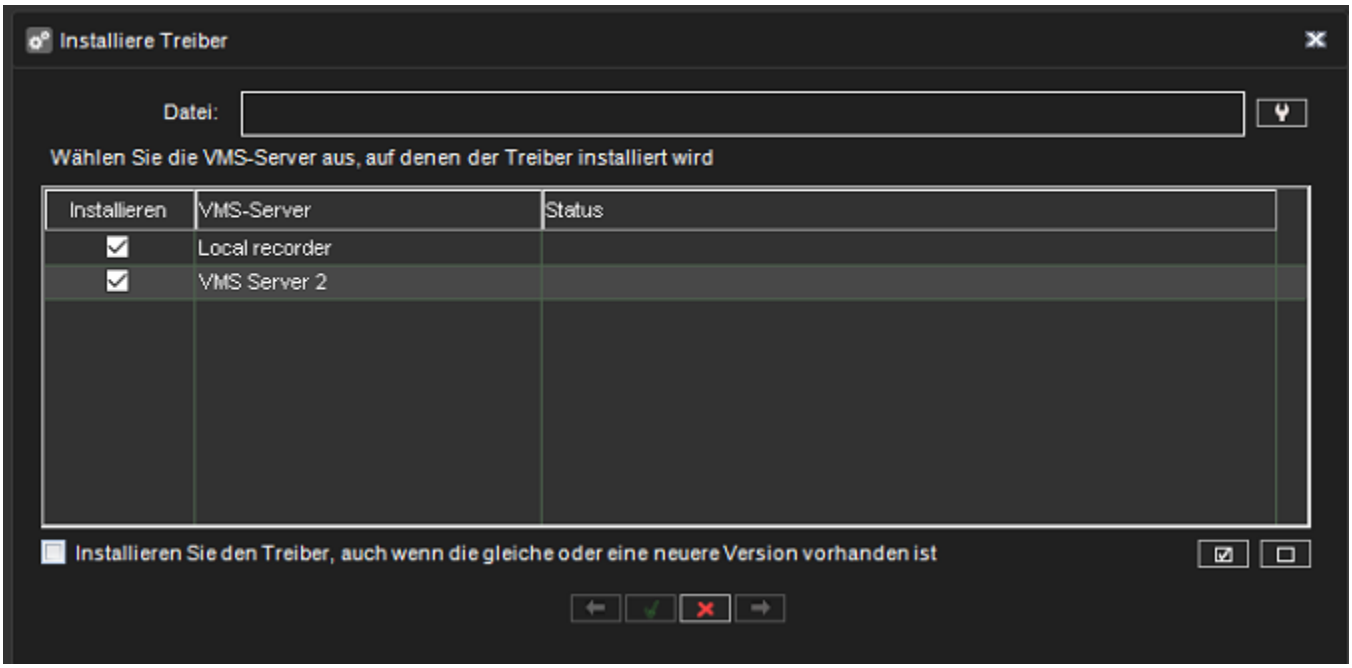


Um IP-Kameras, digitale E/A-Geräte oder Textdaten im VMS-System zu verwenden, muss der Treiber für jedes Gerät auf dem Server installiert werden.
Die Software enthält alle Treiber und Plugins, die in den vorherigen Versionen der Software enthalten waren.
Jedoch Bei Bedarf können neue Treiber und Plugins 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.

8.7.2 Installieren von Metadatentreibern

Es ist möglich, neue Metadatentreiber mit der Option **Metadatentreiber installieren** – auf der Registerkarte **System** zu aktualisieren und zu installieren.

8.7.3 Client-Treiber installieren

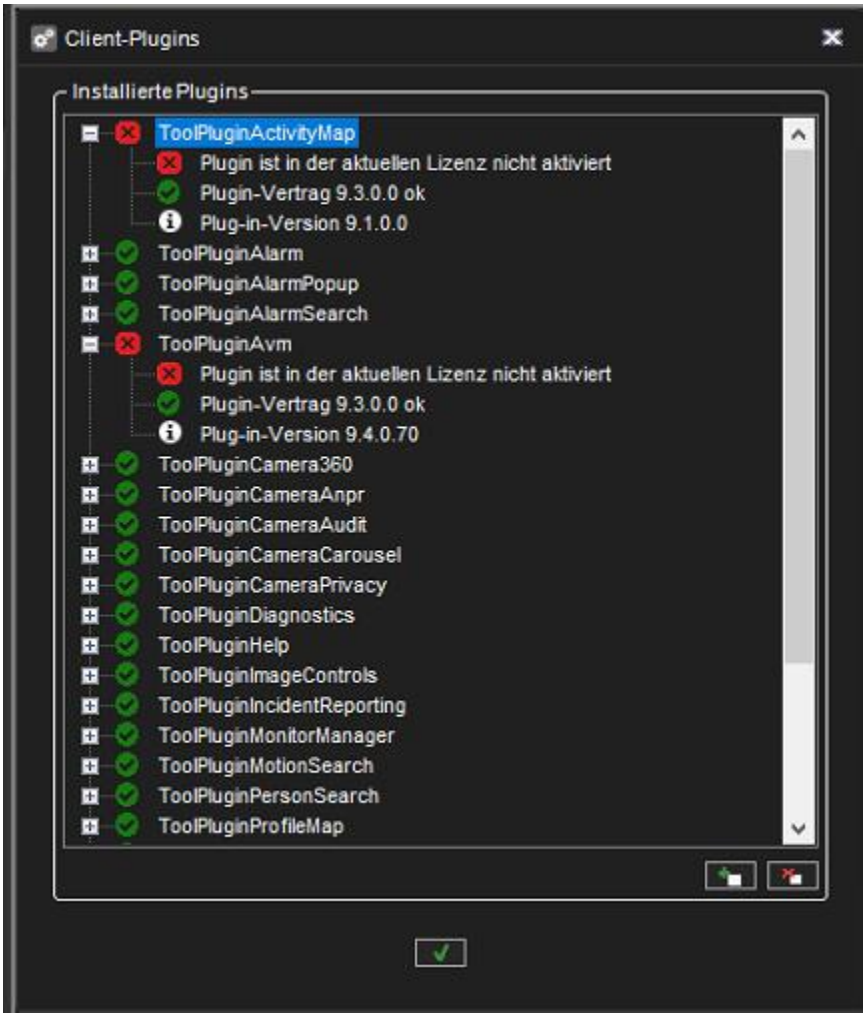
TruCast (direktes Streaming von der Kamera zum Spotter-Client) erfordert einen anderen Kameratreibertyp.

Diese werden als (verwaltete) TruCast 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.

8.7.4 Client-Plugin installieren

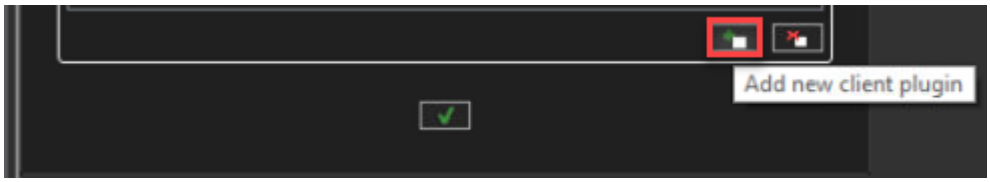
Client-Plugins für Benutzeroberflächen wie Spotter können über den System Manager installiert werden.



Die Plugin-Installation kann über die Registerkarte System unter Add-Ins geöffnet werden.

8.7.4.1 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.

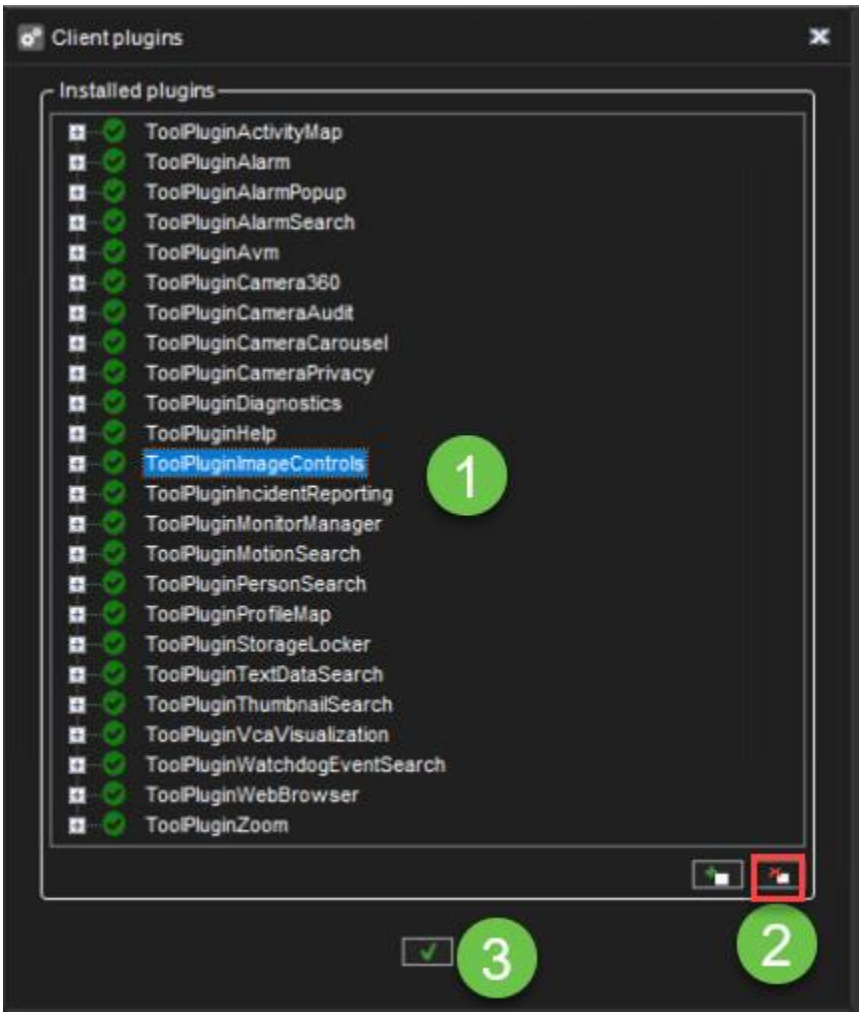
4. Wenn Sie das System zwingen möchten, die Treiberpaketversion zu installieren, wählen Sie **Treiber installieren, auch wenn dieselbe oder eine neuere Version vorhanden ist.**

5. Klick **Ok**

8.7.4.2 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**



9 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.

9.1 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**

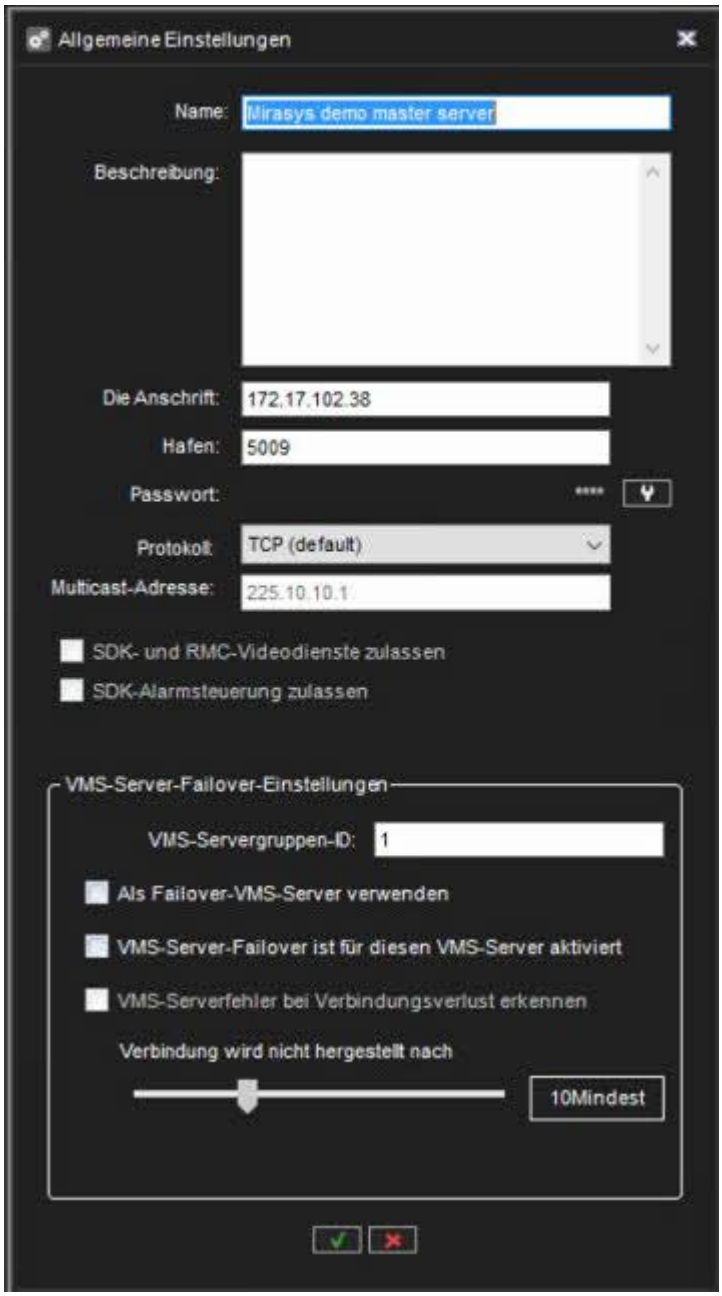
in der unteren rechten Ecke des Navigationsbereichs.

- Doppelklicken Sie auf die Einstellungen, die Sie konfigurieren möchten.
- Ziehen Sie die Einstellungen von der Registerkarte **VMS Servers** in den Arbeitsbereich.

9.2 Allgemein

- VMS-Servername
- Beschreibung

- Passwort
- Protokoll
- Multicast-Adresse
- VMS-Server-Failover-Einstellungen

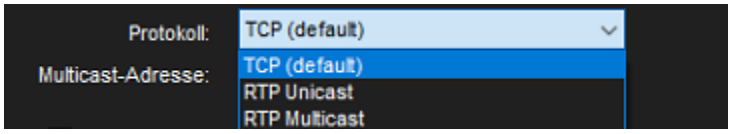


9.2.1 Multicast-Adresse

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.

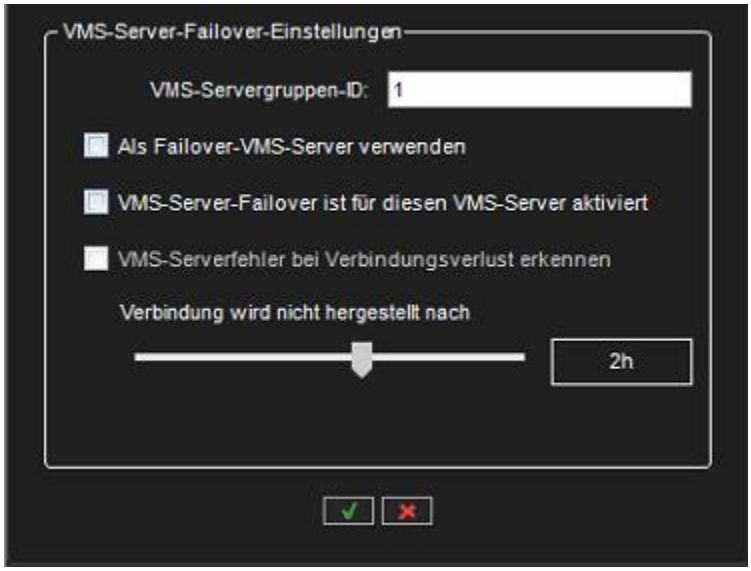
9.2.2 VMS-Server-Failover-Einstellungen

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.

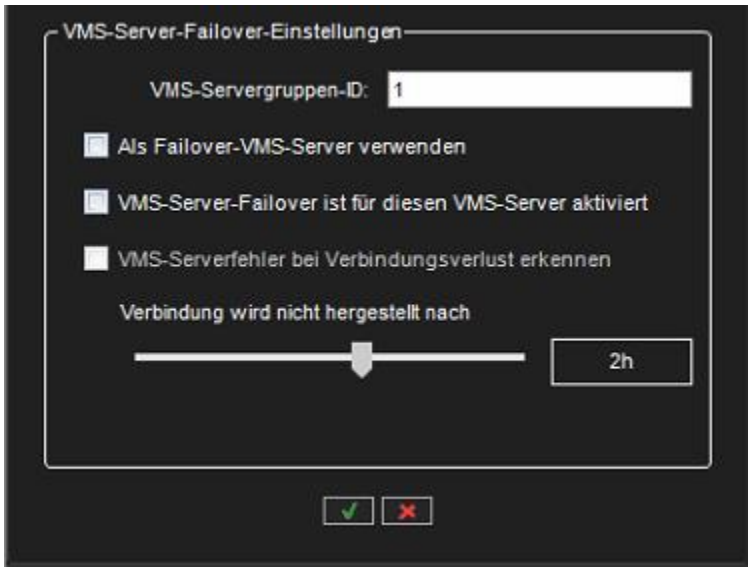
Failover-Server müssen das gleiche Dateisystem (dasselbe Laufwerk) haben Buchstaben) als VMS-Server unter Failover-Schutz, und sie können nur für Backup-Zwecke von IP-Kameras verwendet werden unzugänglich sind, wurden sie in den Ordner *„Ausgefallene VMS-Server“* verschoben.

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.



9.2.3 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.

9.3 Port-Weiterleitung

9.3.1 Die Grundidee bei der Portweiterleitung besteht darin, dass auf einen oder mehrere VMS-Server oder Master-Server hinter einem Router zugreifen kann, der Network Address Translation (NAT) durchführt.

9.3.2 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“.

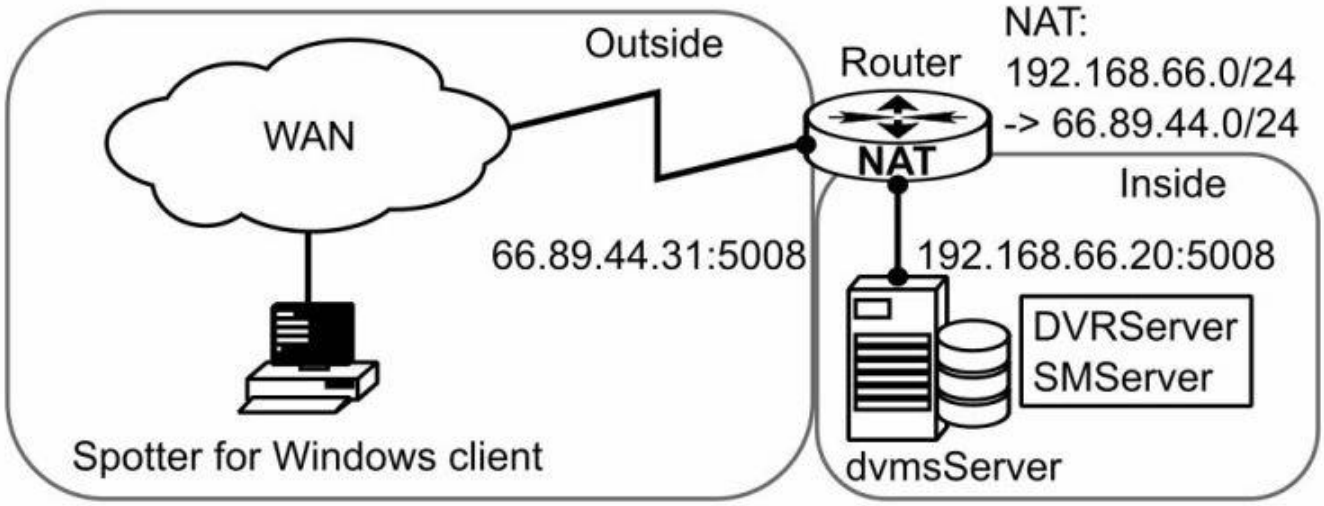
9.3.3 Automatische Router-Konfiguration

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 Master-Server ist der Port normalerweise 5008. Beim Hinzufügen neuer Server zum Master ist der Port normalerweise 5009. Wenn mehr als ein Server vor Ort ist, dann sind die Ports 5009 + 4, 5009 + 8 usw.

9.3.4 Einzelner Server hinter Router

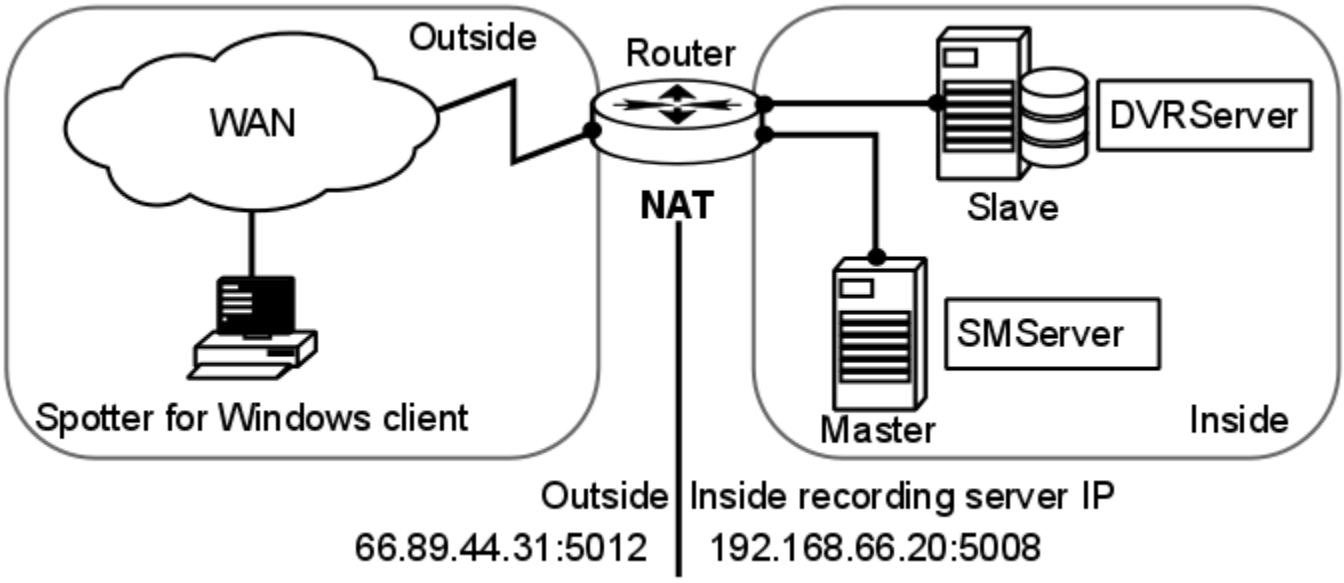
Szenario 1: Verwendung eines Systems mit **a Single Server hinter einem Router/Firewall**



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.

9.3.5 Mehr als ein Server hinter dem Router

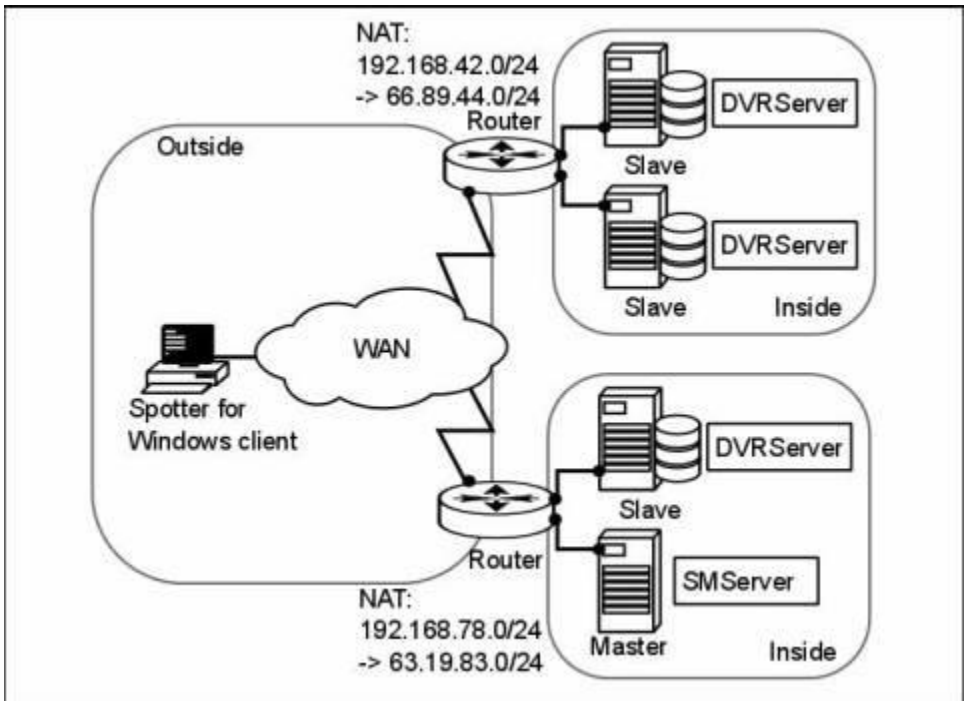
Szenario 2: Mehrere Server hinter einem einzigen Router (WAN-Adresse)



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**...

9.3.6 Mehr als ein Server auf mehreren Sites

Szenario 3: Mehr als ein Server auf mehr als einer Site

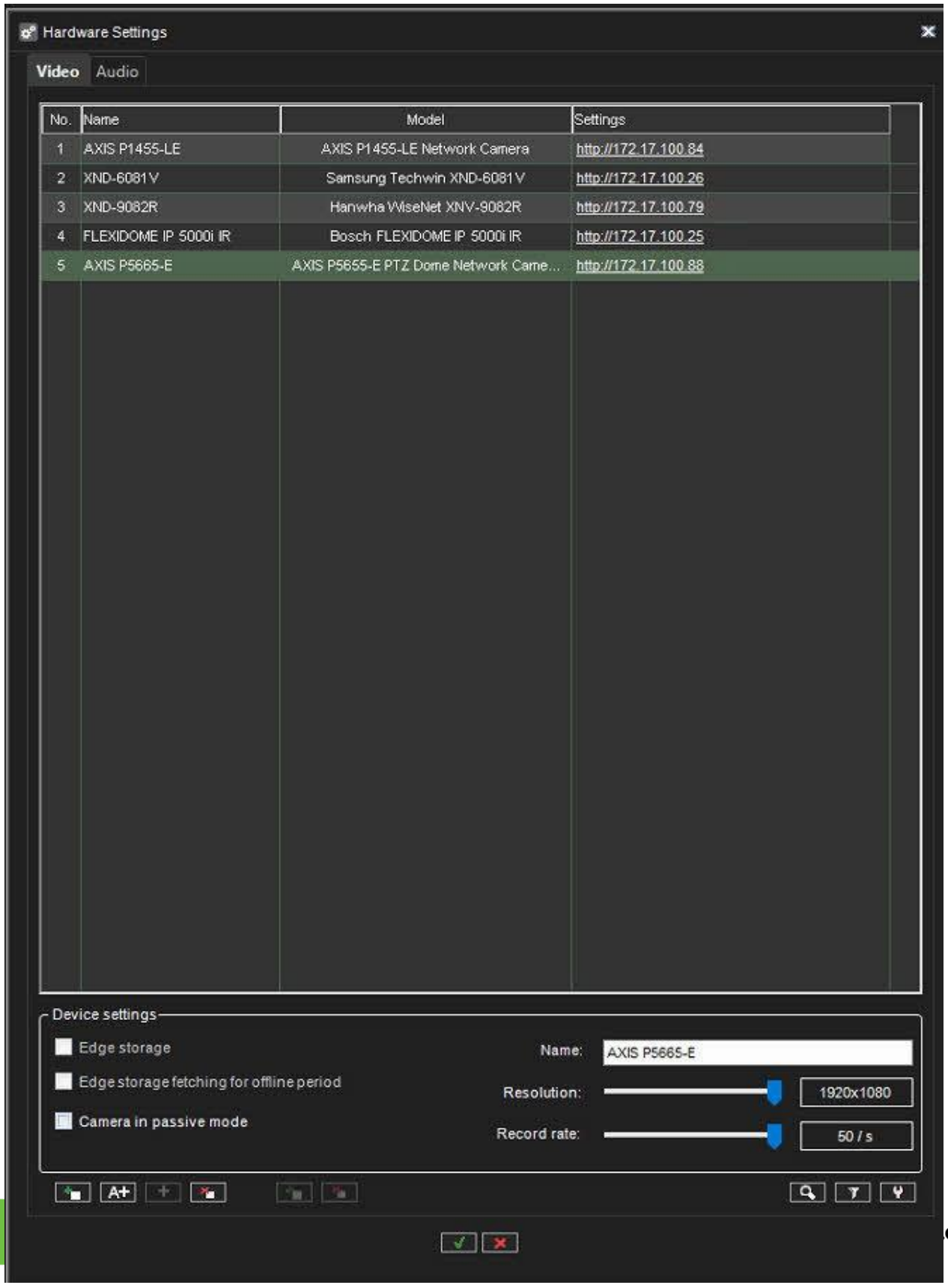


Es gilt das gleiche Prinzip wie in Szenario 2, aber diesmal muss NAT bei der Zuweisung von VMS-Servern an den Master-Server des anderen Standorts berücksichtigt werden.

9.4 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


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

9.4.1 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.

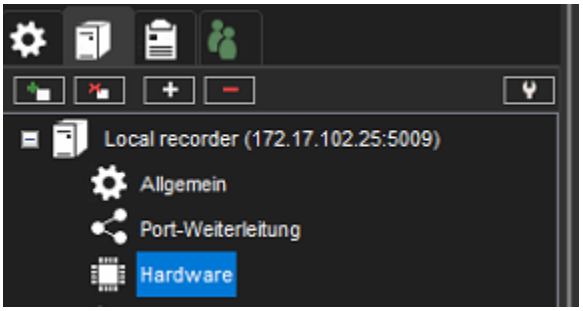
- ***Kameramodell***: Kamera nach Modellname hinzufügen. Dieser Modus wird zum Hinzufügen einer Kamera verwendet, indem ein älterer Aufnahmetreiber verwendet wird, der vordefinierte Funktionen aus der XML-Datei zur Treiberkonfiguration verwendet.
    - Das Kombinationsfeld für die Modusoption enthält 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

9.4.1.1 Gerät hinzufügen

IP-Kameras oder analoge Videoserver (Encoder) können über die Registerkarte **Video** von **Hardware-Einstellungen** verwaltet werden.



Invalid file id - 37621f...

So fügen Sie eine neue IP-Kamera hinzu, wenn die IP-Adresse bekannt ist:

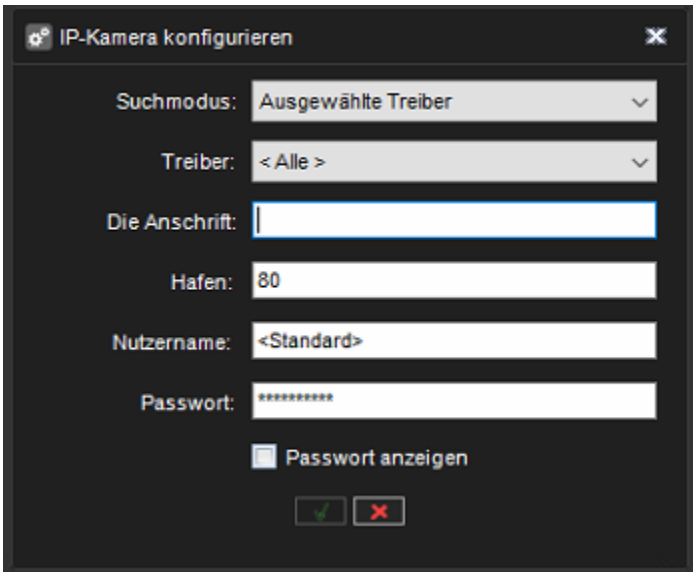
1. Klicken Sie auf der Registerkarte **Video** auf **Gerät hinzufügen**

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**.

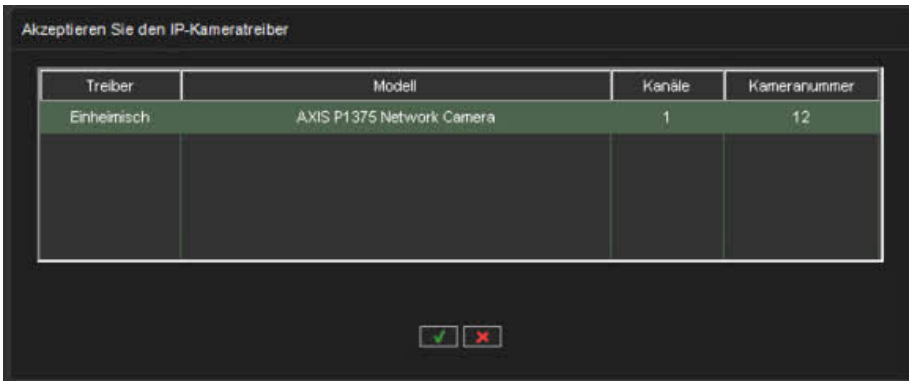


The system will now communicate with the camera and display which drivers can connect to the camera.
The camera may support **ONVIF**. In diesem Fall kann es auch der **ONVIF** -Treiber erkennen.

5. Wählen Sie einen Treiber aus der Liste aus.

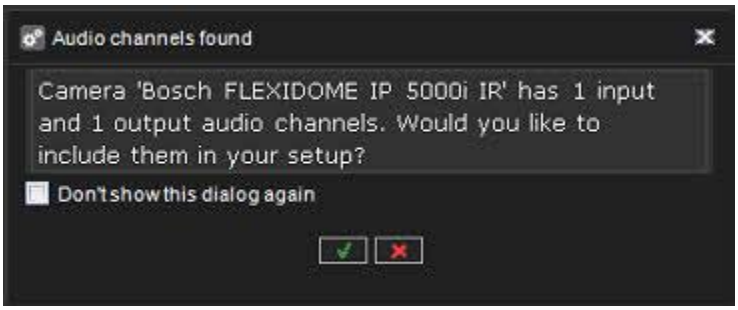
In der Regel wird empfohlen, den **Nativen** Treiber zu verwenden, falls vorhanden.
Bei Mehrkanalgeräten kann die Option **Kanäle** das Gerät mit weniger als der maximalen Anzahl von Kanälen hinzufügen.
Der Benutzer kann auch sehen, welche Kameranummer das Gerät haben wird

6. Klicken **OK**

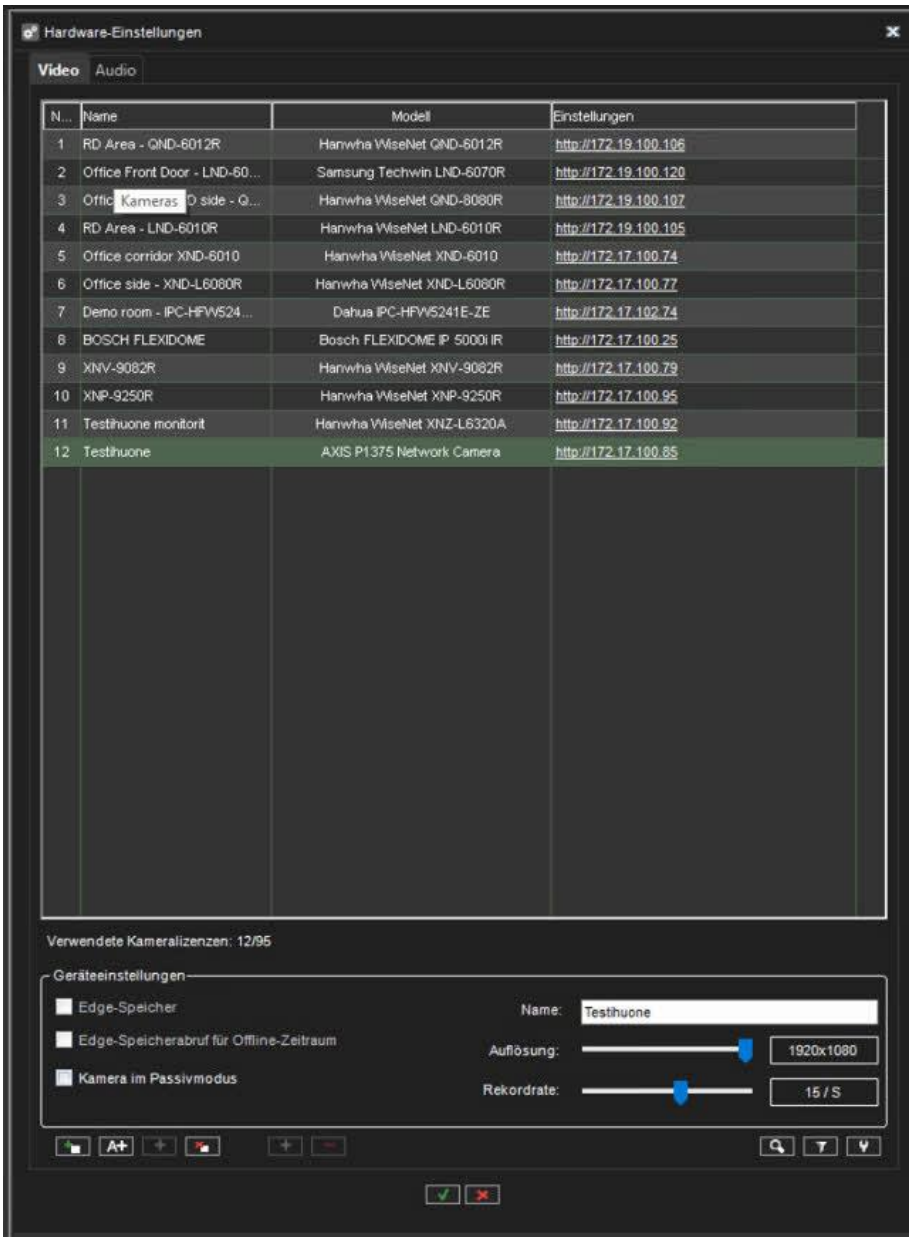


Wenn die Kamera Audiokanäle unterstützt, sehen Sie einen Dialog darüber.

7. Klicken Sie auf **OK** um auch Audiokanäle hinzuzufügen oder **X** fügen Sie nur einen Videokanal hinzu

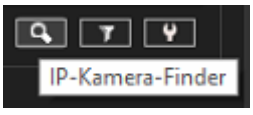


Nachdem die Kamera hinzugefügt wurde, kann das Gerät in der Liste **Hardware-Einstellungen** gefunden werden

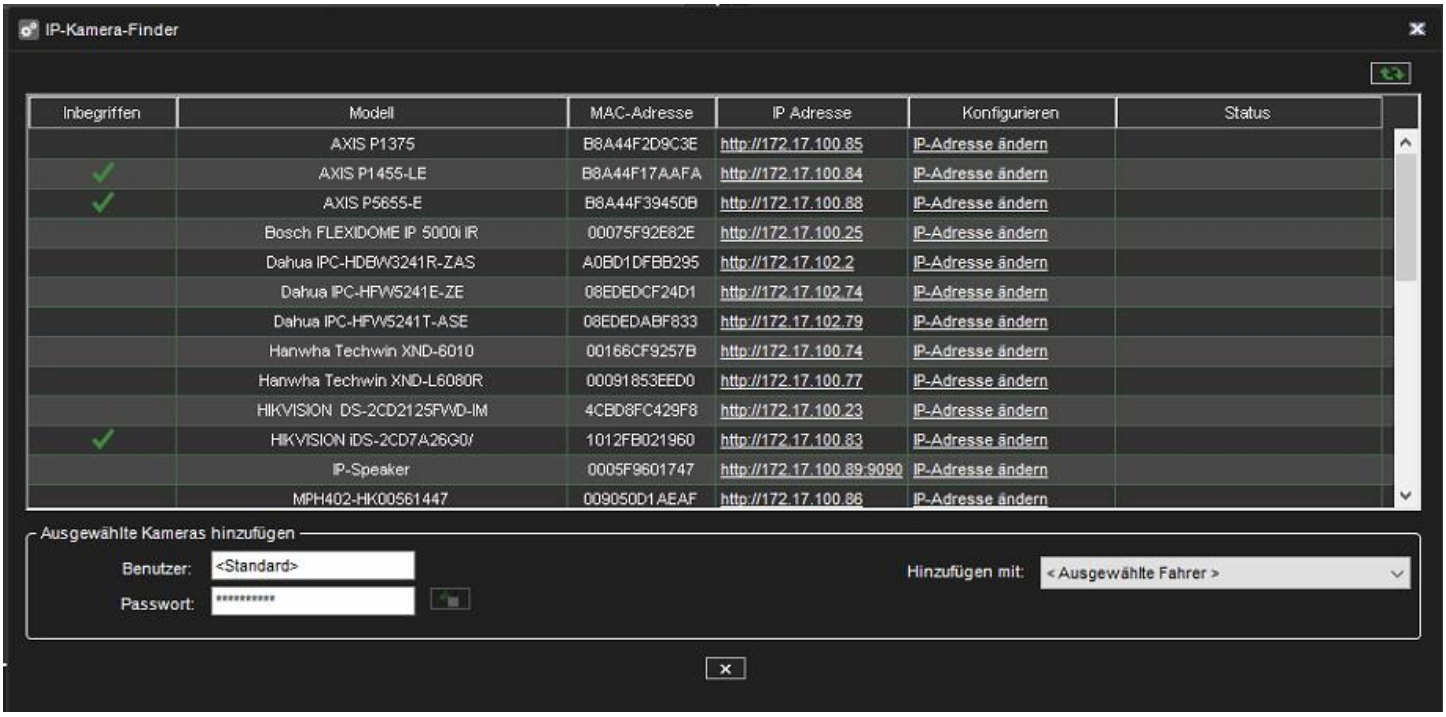


9.4.1.2 IP-Kamera-Finder

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.

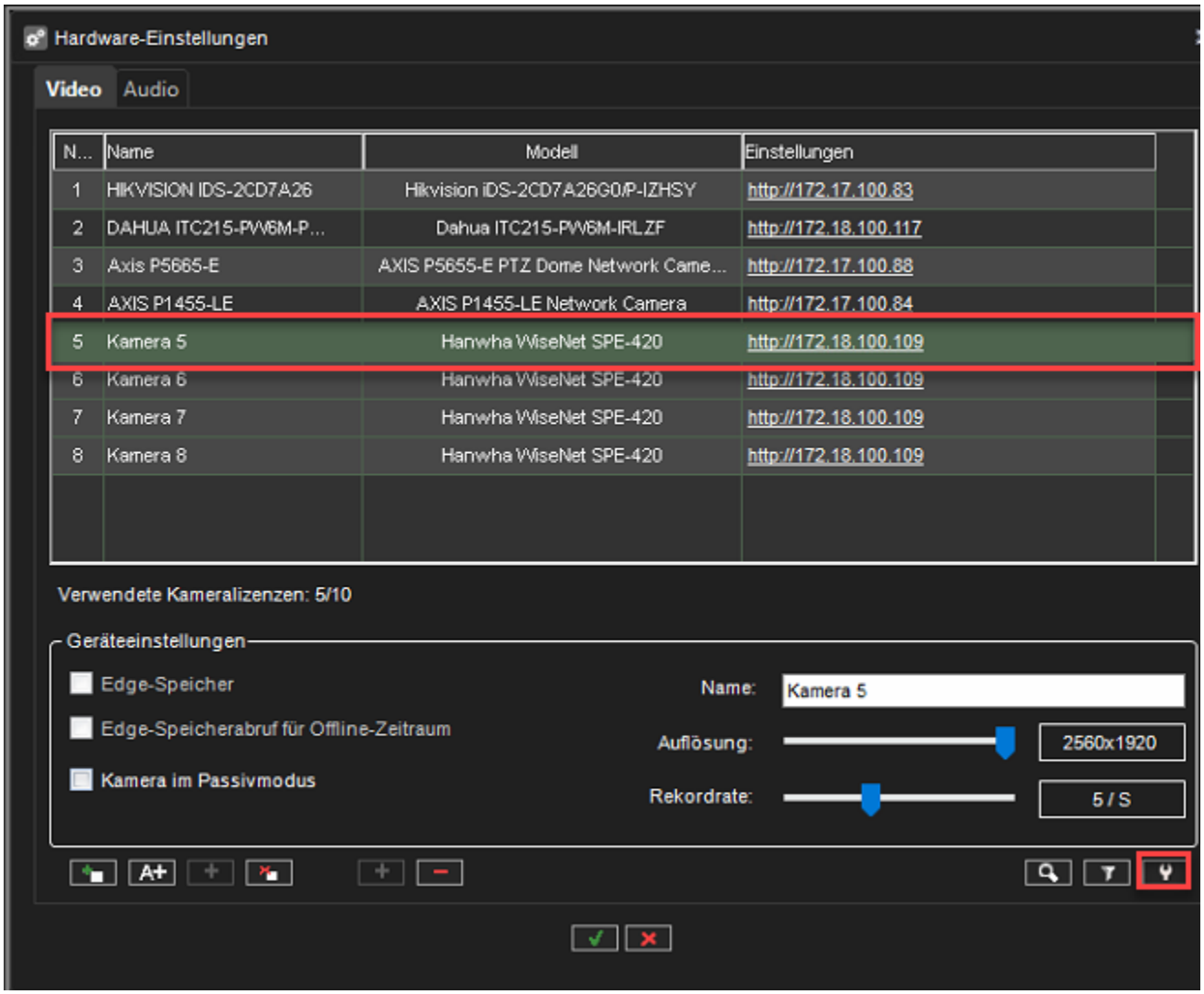
5. Klicken Sie auf **Schließen**, um den **IP-Kamerafinder** zu beenden.

6. Speichern Sie die Hardware-Einstellungen durch Drücken von **OK** in der Liste:

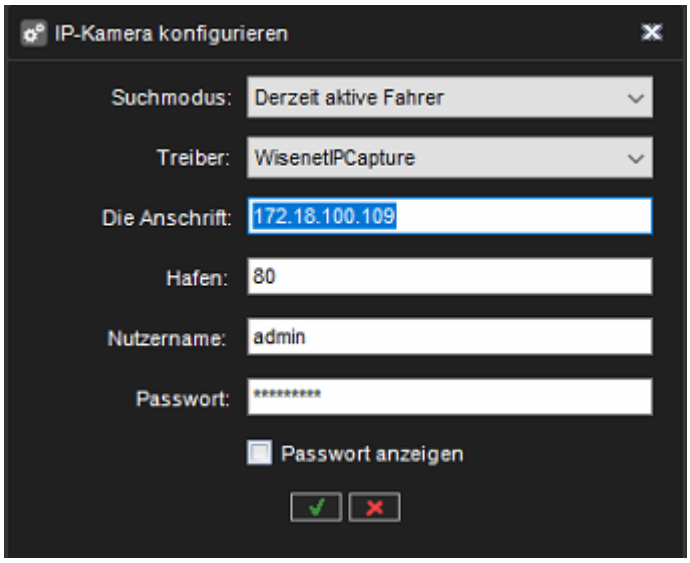
9.4.1.3 IP-Kamera bearbeiten

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



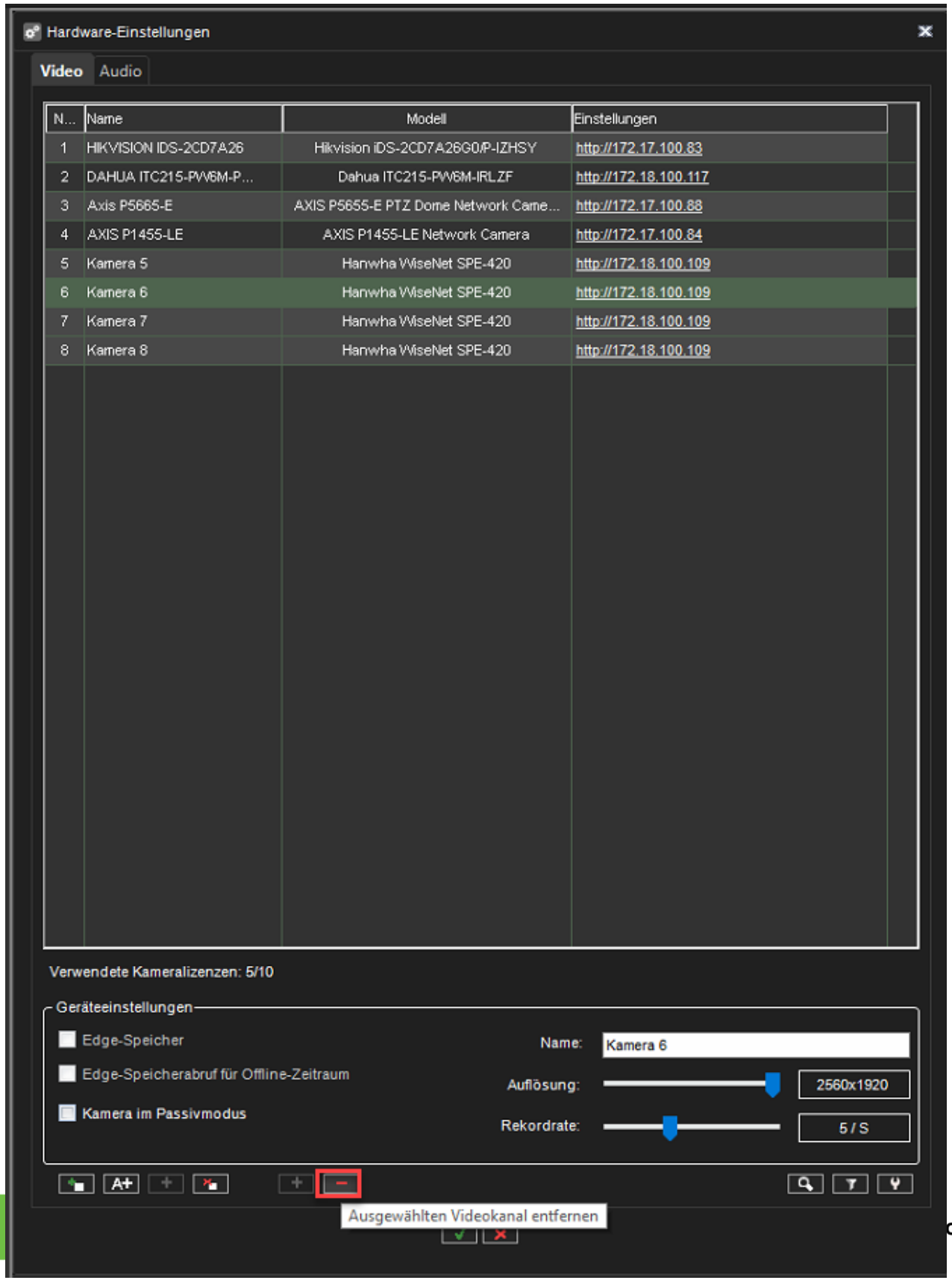
9.4.1.4 Entfernen von IP-Kameras und Encodern

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**“

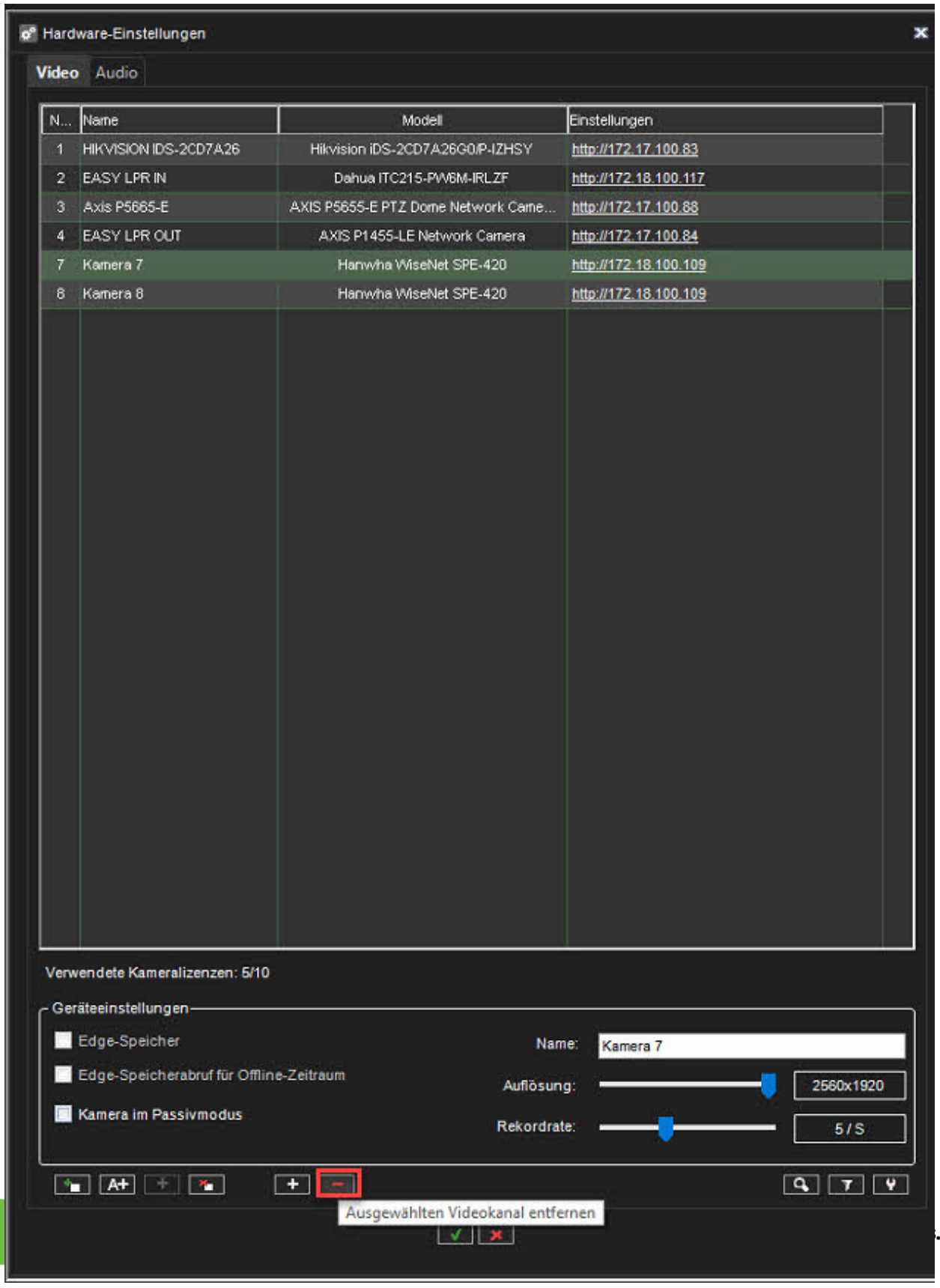
9.4.1.4.1 So entfernen Sie eine IP-Kamera:

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**.


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

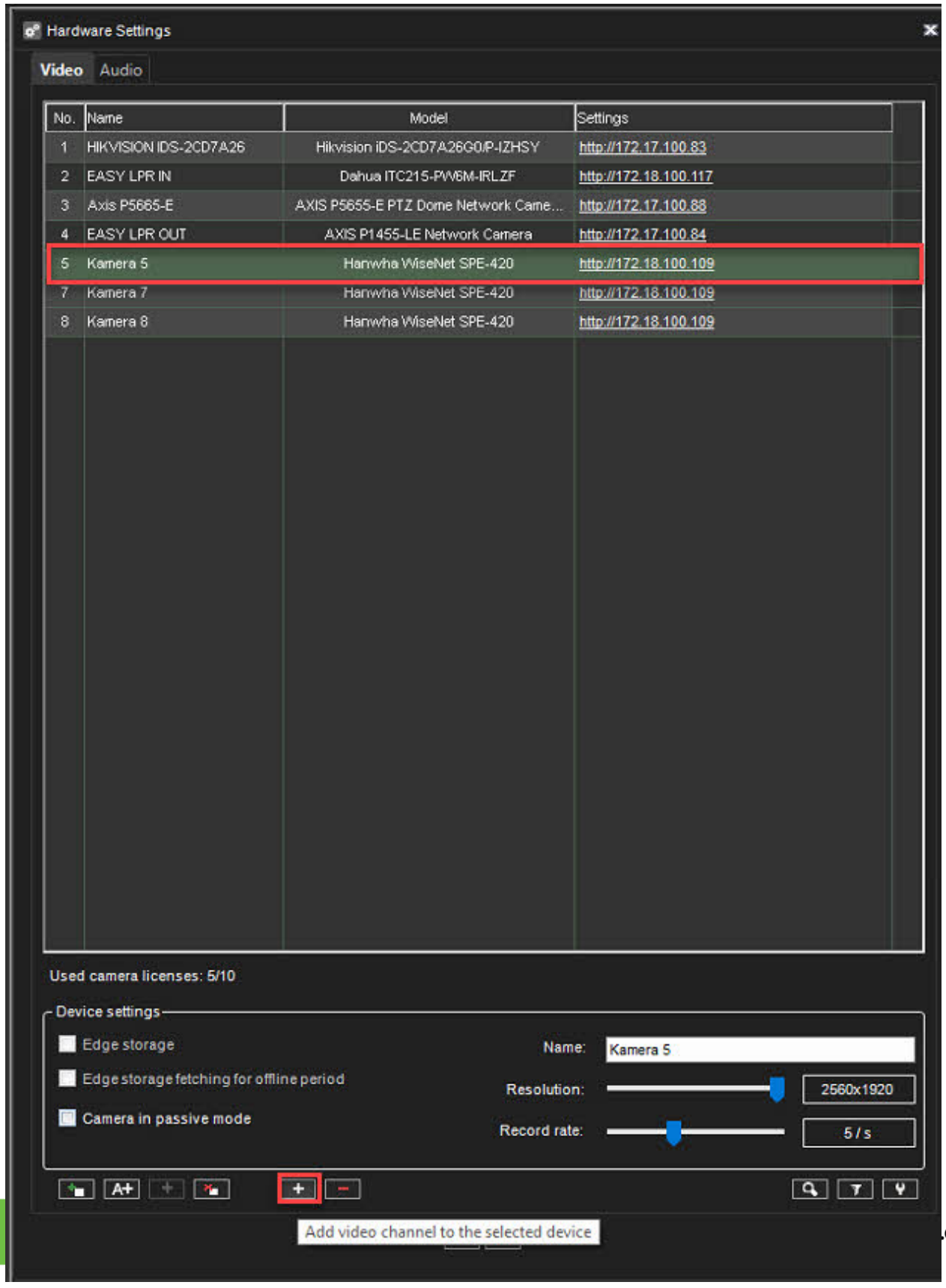
9.4.1.4.2 So entfernen Sie Videokanäle vom Encoder oder Kameras mit mehreren Linsen:

1. Wählen Sie den richtigen Kanal aus der Liste
2. Klicken Sie auf **Videokanal vom ausgewählten Gerät entfernen**
3. Klicken **OK**


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
Ausgewählten Videokanal entfernen

9.4.1.4.3 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**

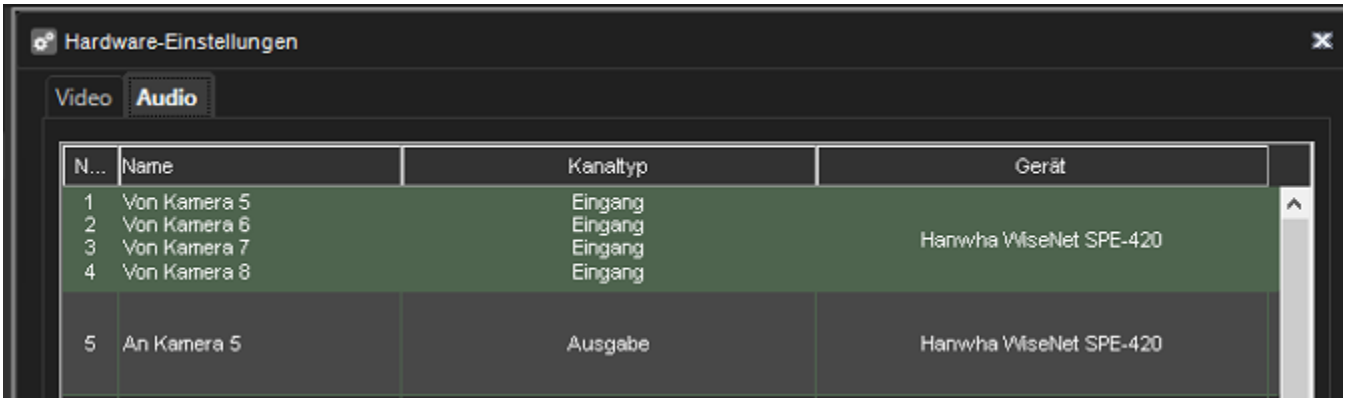

Hardware Settings
Video
Audio
No.
Name
Model
Settings
1 HIKVISION IDS-2CD7A26 Hikvision iDS-2CD7A26G0/P-IZHSY http://172.17.100.83
2 EASY LPR IN Dahua ITC215-PW6M-IRLZF http://172.18.100.117
3 Axis P5665-E AXIS P5655-E PTZ Dome Network Came... http://172.17.100.88
4 EASY LPR OUT AXIS P1455-LE Network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

9.4.2 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**.

9.4.2.1 Angezeigte Informationen:

1. Kamera-Hardware-ID
2. Kanaltyp (Eingang)
3. Kanaltyp (Ausgabe)
4. Gerätemodell



9.4.3 Geräteeinstellungen

9.4.3.1 Edge-Speicher

Die Edge-Speicherfunktionalität ermöglicht eine unterbrechungsfreie Aufzeichnung bei Netzwerkausfällen. In der Praxis kann bei einem Netzwerkausfall der Video-Feed 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.

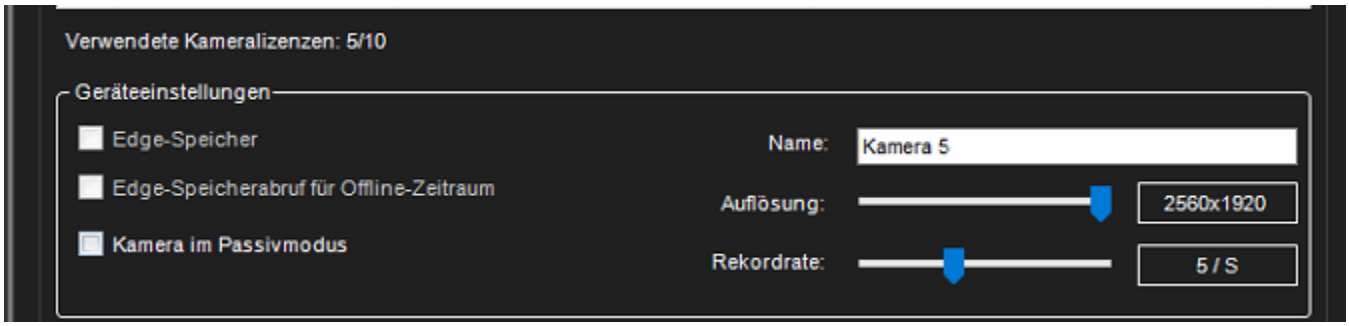
9.4.3.2 Edge-Speicherabruf für Offline-Zeitraum

9.4.3.3 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.

9.4.3.4 Kamerainformationen

Kameraname, Auflösung und Aufnahmerate können direkt über die Registerkarte **Video** eingestellt werden



9.4.4 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.

9.4.4.1 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.

9.4.4.1.1 CSV-Dateiformat

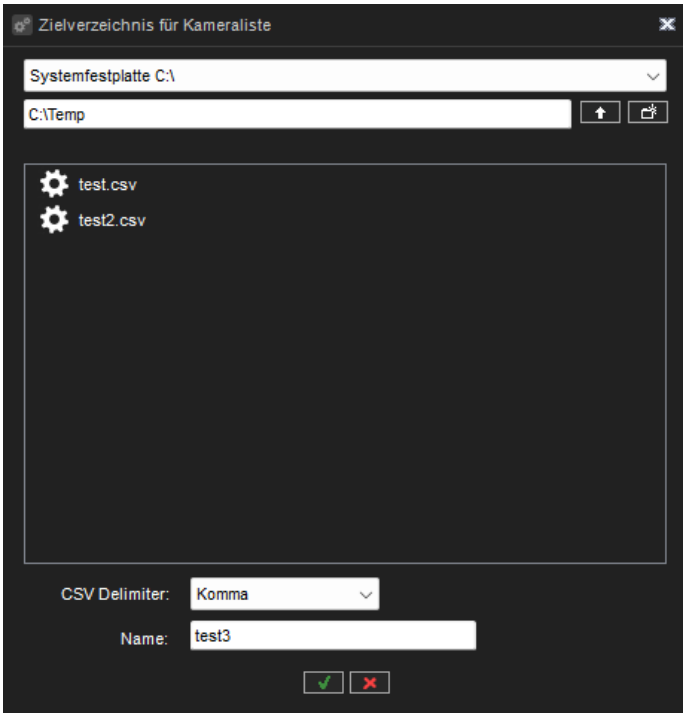
Das CSV-Dateiformat verwendet für jede Kamera die folgenden Kopfzeilen.

- **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.

9.4.4.1.2 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.



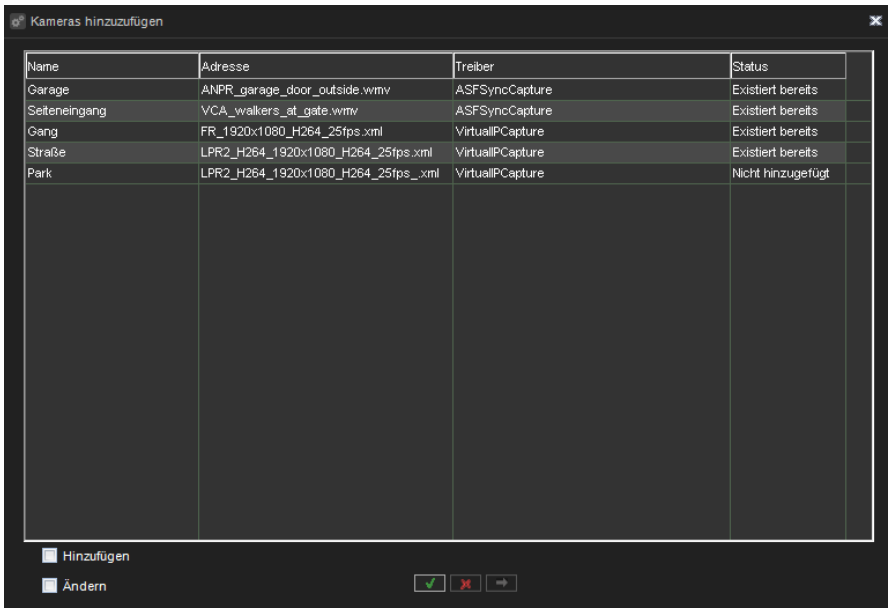
Wenn der Export erfolgreich war, wird ein blinkendes grünes Symbol angezeigt. Bei einem Fehler wird ein blinkendes rotes Symbol angezeigt.

9.4.4.1.2.1 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.

9.5 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 Master Server (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.

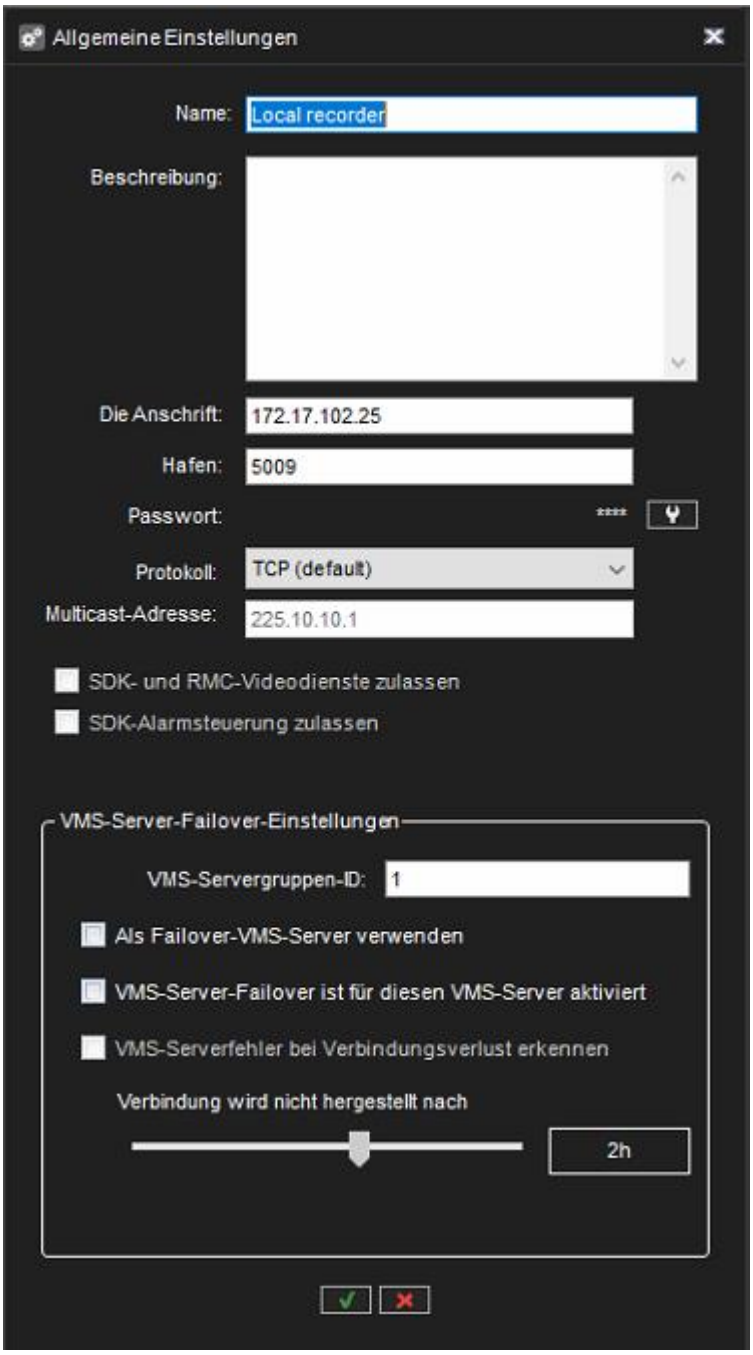
9.5.1 So fügen Sie dem System einen Server hinzu (Aufzeichnungsserver):

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.*



9.5.2 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**.

9.5.3 Verbindungsstatus:

Wenn die Verbindung zum Server unterbrochen wird, versucht die System Manager-Anwendung automatisch, eine Verbindung zum Server herzustellen.

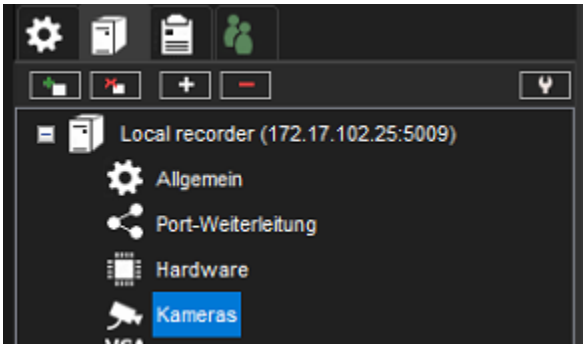
9.5.4 HINWEIS:

Wenn Sie Mirasys VMS als Slave-Server hinzugefügt haben, gehen Sie bitte wie folgt vor:

1. Ändern Sie das Admin-Benutzerkennwort mit einem Slave-Server System Manager
2. Deaktivieren Sie den SMServer-Dienst vom Slave-Server

9.6 KAMERAS

Nachdem die Kamera zum Server hinzugefügt wurde, können die Kameraeinstellungen auf der Seite **Kameras** konfiguriert werden.

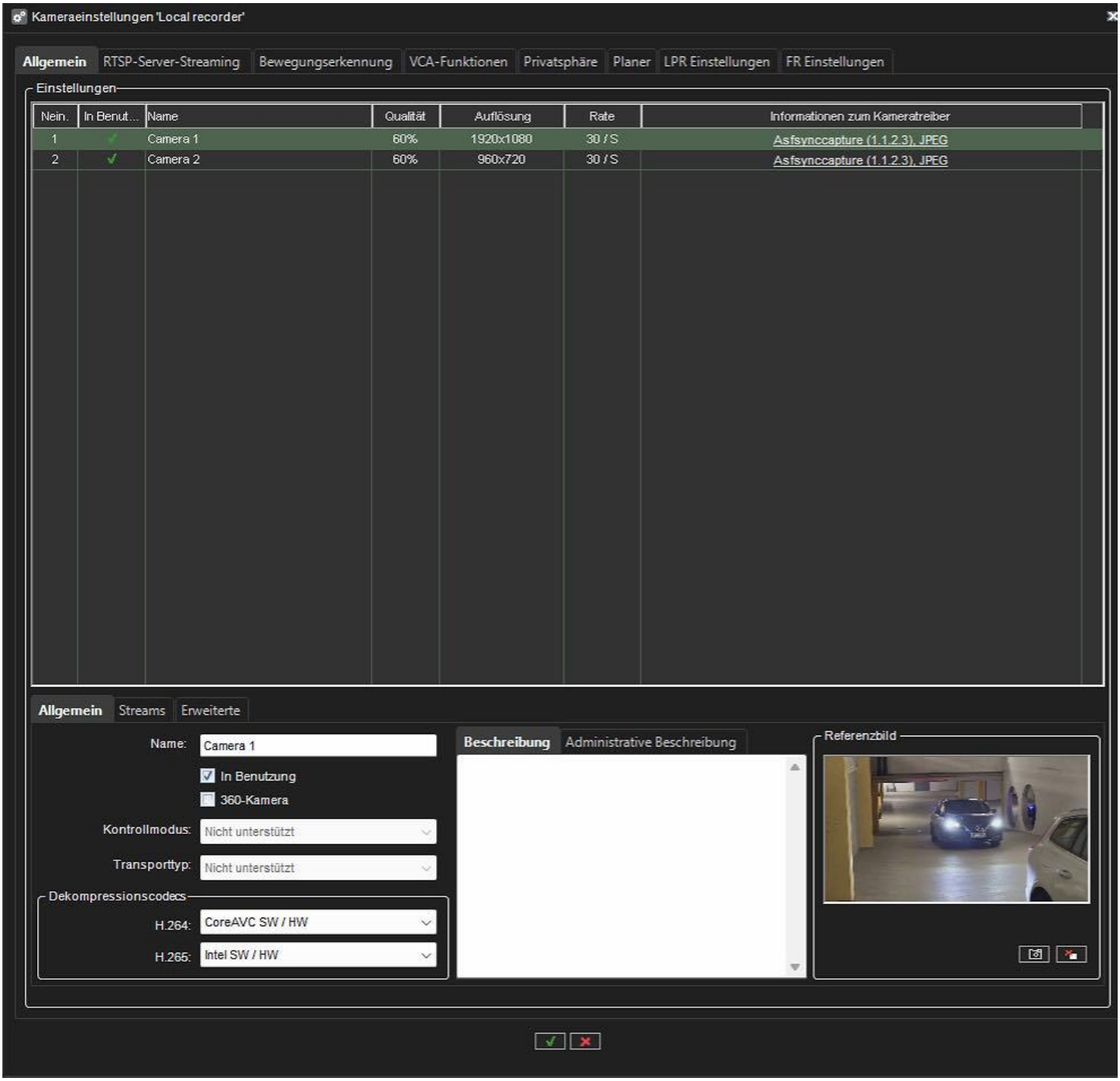


9.6.1 Kameraeinstellungen enthalten Einstellungen für:

- Allgemein
- Bewegungserkennung
- VCA-Einstenllung
- Privatsphäre

- Planer

9.6.2 Kameraeinstellungen



9.6.2.1 Allgemeine Einstellungen

9.6.2.1.1 Name

Der Name der Kamera. Das System schlägt Namen des Typs *Kamera 1, Kamera 2* usw. vor.

9.6.2.1.2 Im Einsatz

Deaktivieren Sie dieses Kontrollkästchen, wenn keine Kamera an den Kameraeingang angeschlossen ist oder wenn Sie die Kamera deaktivieren möchten.

9.6.2.1.3 360 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).

9.6.2.1.4 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 .

9.6.2.1.5 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.

9.6.2.1.6 Dekomprimierungscodecs.

Codecs werden zum Kodieren und Dekodieren von Videodaten verwendet

9.6.2.1.7 Beschreibung

Hier können Sie eine Beschreibung der Kamera eingeben, die allen Benutzern im Spotter-Programm angezeigt wird.

9.6.2.1.8 Administrative Beschreibung.

Hier können Sie eine Beschreibung der Kamera eingeben. Die Beschreibung wird im Spotter-Programm nur Systemadministratoren angezeigt.

9.6.2.1.9 Reference image

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**.

9.6.2.2 Streams (Kameras)

9.6.2.2.1 Standardmäßig empfängt Mirasys VMS einen Stream in Aufzeichnungsqualität von der Kamera. Der Mirasys VMS-Server sendet den Aufzeichnungsstream standardmäßig an Mirasys Spotter

9.6.2.2.2 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.

9.6.2.2.3 Bitrate mode.

Diese Einstellung steuert, ob die variable Bitrate (VBRMax) oder die konstante Bitrate (CBR) verwendet wird.

9.6.2.2.4 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.

9.6.2.2.5 Auflösung

Bei automatisch konfigurierten IP-Kameras werden genau die vom Kameramodell unterstützten Bildauflösungen angezeigt.

9.6.2.2.6 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)

9.6.2.2.7 Multi-Streaming (Kameras)

Multi-Streaming ermöglicht separate Feeds von einer einzelnen Kamera.

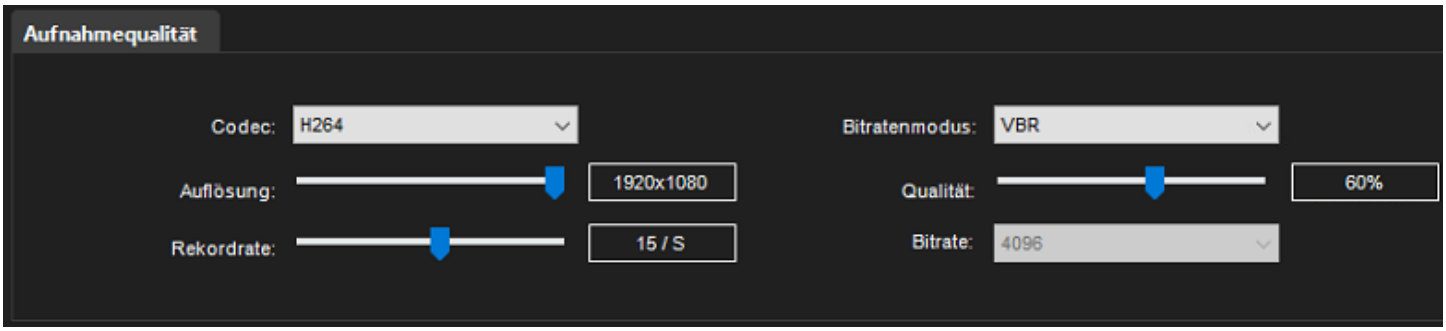
Die Funktion ermöglicht die Verwendung separater Streams zum Aufzeichnen und Anzeigen.

Die Funktion ist nur verfügbar, wenn die Kamera und der Treiber dies unterstützen.

9.6.2.2.7.1 Aufnahmequalität

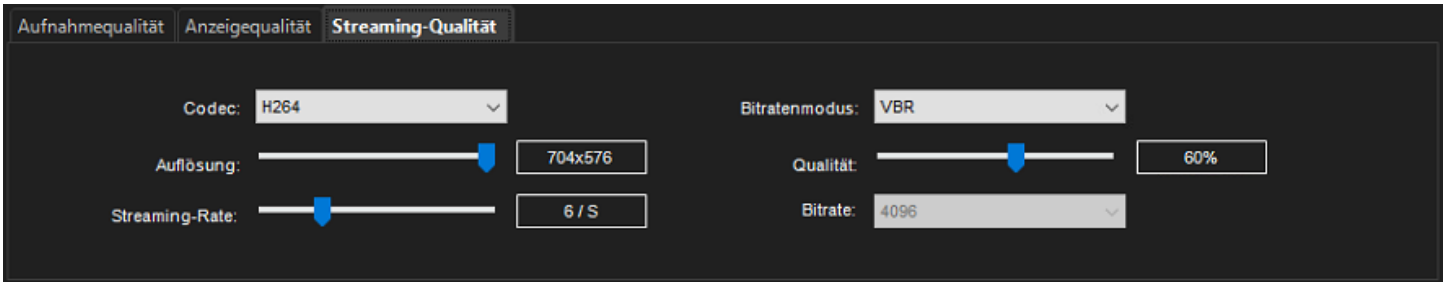
Standardmäßig empfängt Mirasys VMS einen Stream in Aufzeichnungsqualität von der Kamera.

Der Mirasys VMS-Server sendet den Aufzeichnungsstream standardmäßig an den Mirasys Spotter



9.6.2.2.7.2 Anzeigequalität

9.6.2.2.7.3 Streaming-Qualität



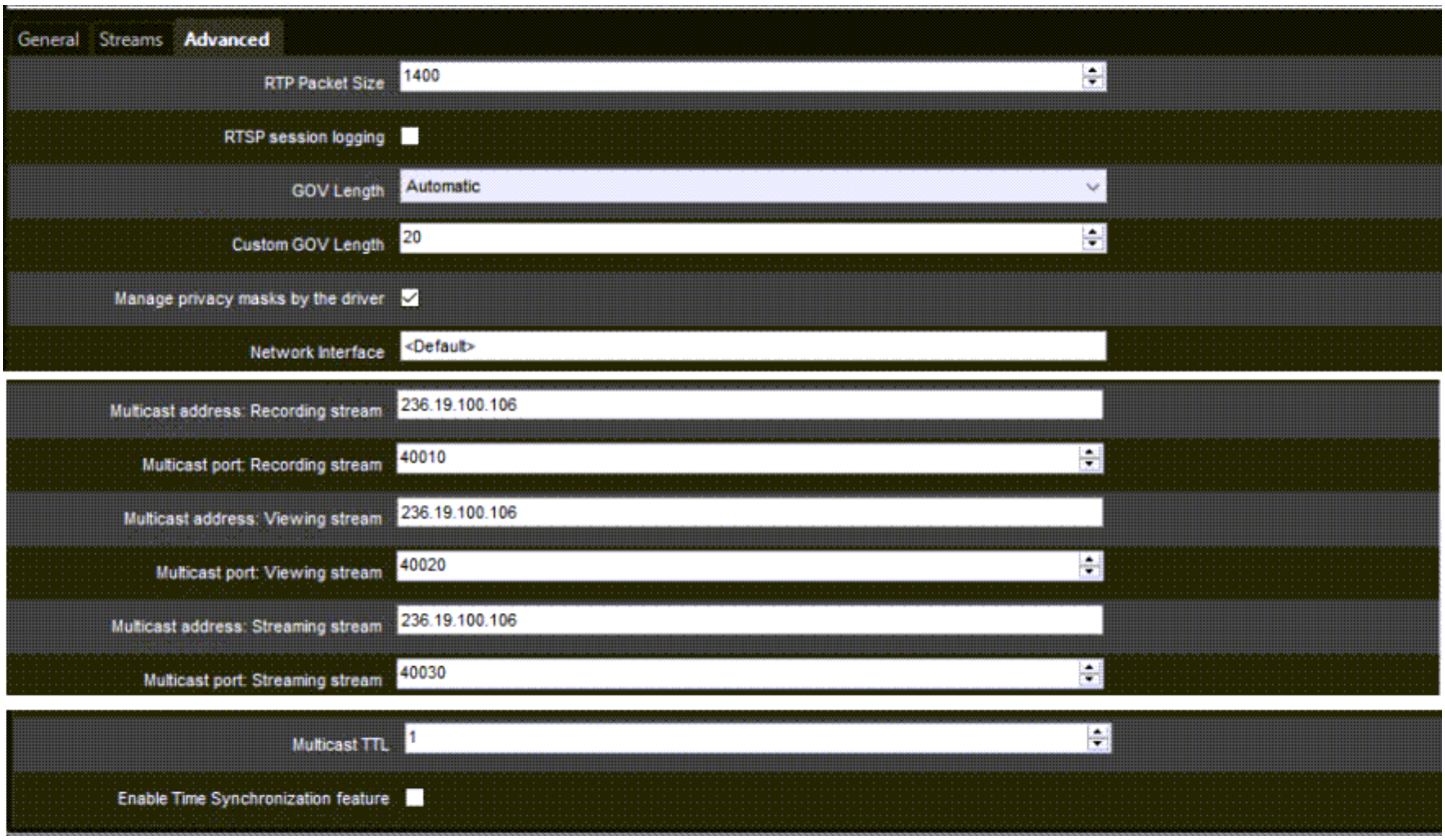
9.6.2.3 Fortschrittlich

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.

9.6.2.3.1 Konfigurierbare Werte

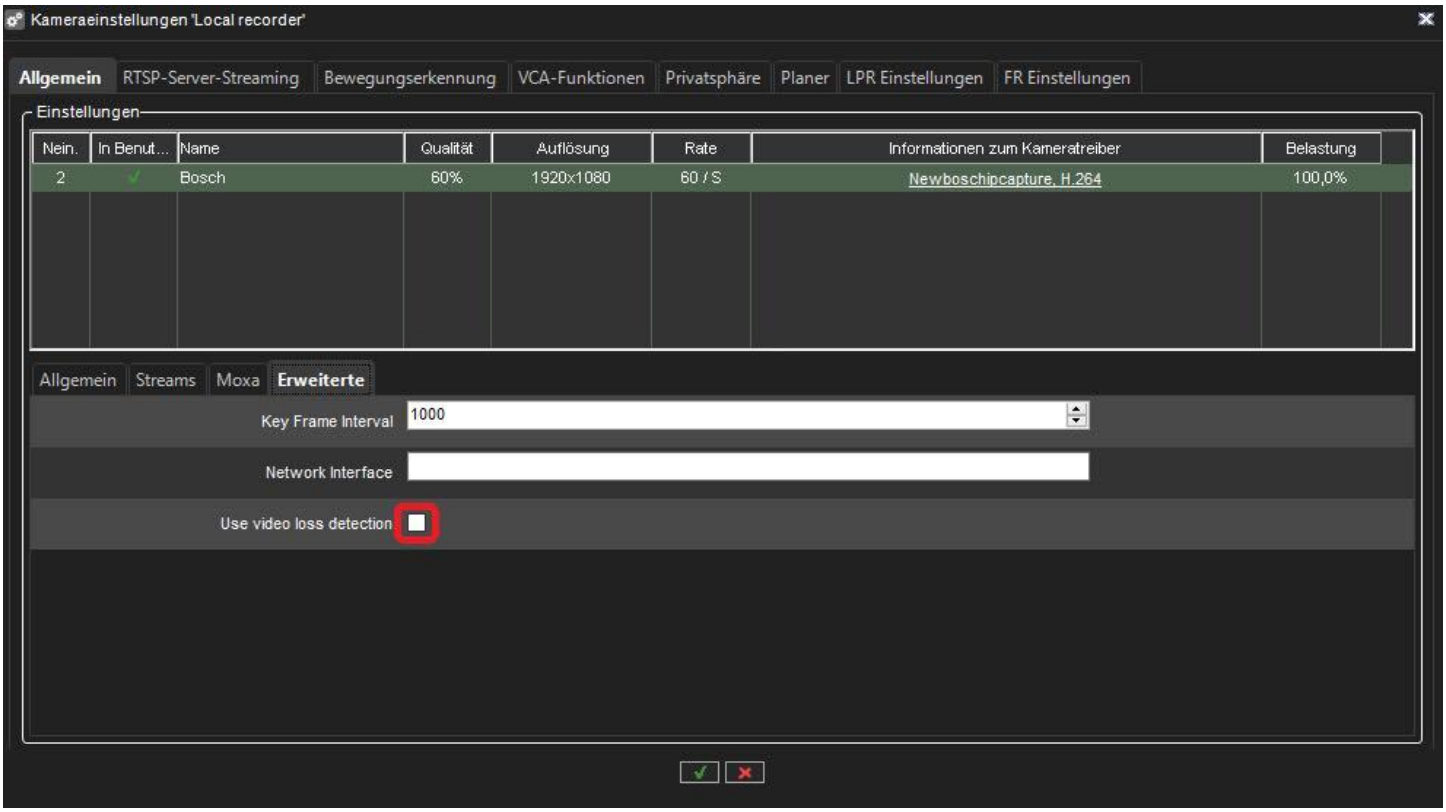
- RTP-Paketgröße

- 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



9.6.2.3.2 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.



9.6.2.4 Moxa-Einstellungen

9.6.2.4.1 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.

9.6.2.4.2 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.

9.6.2.4.2.1 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".

9.6.2.4.2.2 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.

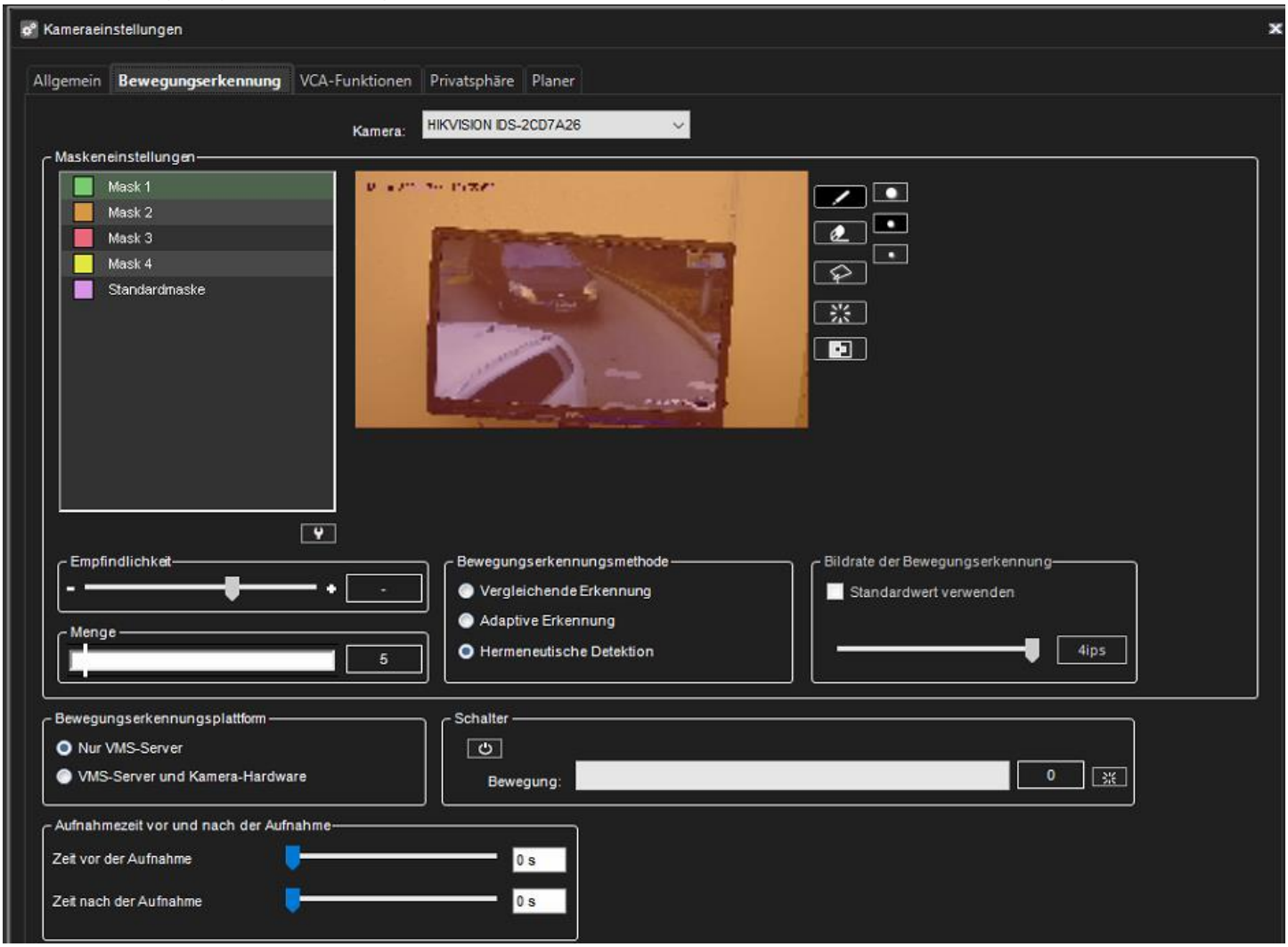
Parität - Wert aus der folgenden Aufzählung:

- { "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".

9.6.3 Bewegungserkennung



9.6.3.1 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.

9.6.3.2 Methoden zur Bewegungserkennung

9.6.3.2.1 Vergleichende Erkennung

Vergleicht ein Bild mit dem Bild davor. Wenn die Unterschiede die eingestellten Grenzen überschreiten, erkennt das System Bewegung.
Sie können die vergleichende Bewegungserkennung unter den meisten Bedingungen verwenden. Wenn sich jedoch viel im Hintergrund bewegt, z. B. Regen, sich bewegende Blätter oder Änderungen der Lichtverhältnisse, Verwenden Sie die adaptive Bewegungserkennung.

9.6.3.2.2 Adaptive Erkennung

Vergleicht jedes Bild mit einem Hintergrundbild. Das System lernt automatisch das Hintergrundbild und die dazugehörige Bewegung.
So interpretiert das System z. B. sich bewegende Blätter nicht als Bewegung.
Ändert sich außerdem mehr als die Hälfte der Pixel in einem Bild, folgert das System daraus, dass die Die Lichtverhältnisse haben sich geändert.
Infolgedessen wird das Referenzbild zurückgesetzt und erneut mit dem Lernen begonnen.

9.6.3.2.3 Hermeneutische Entdeckung

Ist ein ausgeklügeltes Bewegungserkennungssystem für schwierige Wetterbedingungen (z. B. starker Regen, „lautes" Hintergrundbild usw.) und Situationen, in denen externe Tools zur Analyse von Videoinhalten (VCA) verwendet werden.
Es sollte beachtet werden, dass die hermeneutische Erkennung mehr Verarbeitungsressourcen erfordert als die anderen Erkennungsmethoden.

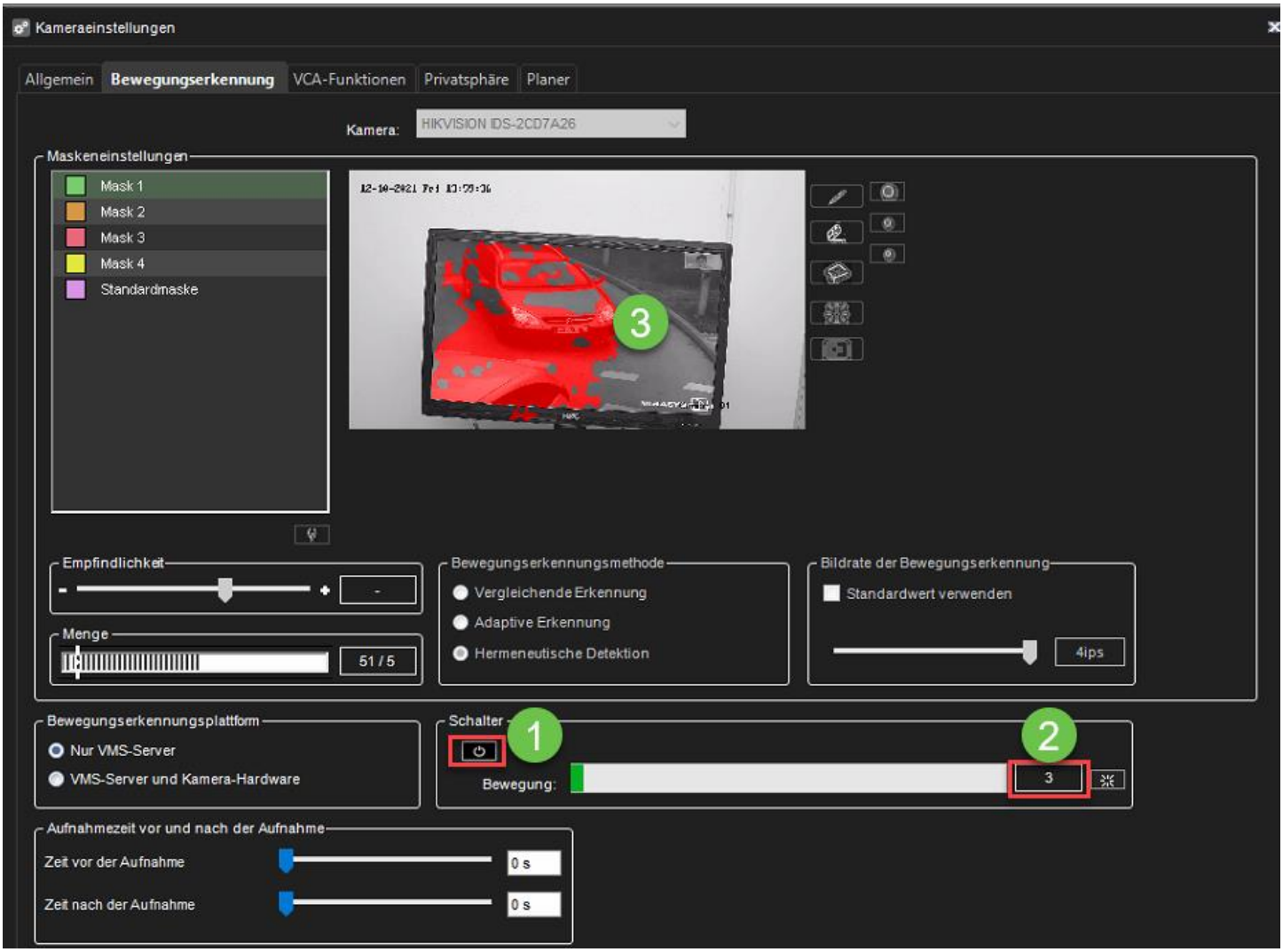
9.6.3.3 Bildrate der Bewegungserkennung

Definiert die bei der Bewegungserkennung verwendete Bildrate.
Es wird allgemein empfohlen, die Standardbildrate zu verwenden.
Bei IP-Kameras verwendet die Bewegungserkennung Intra-Frames und stimmt mit der Intra-Frame-Rate überein.
In der Regel ist dies ein Bild pro Sekunde.

9.6.3.4 Schalter

1. Ermöglichen**Schalter**
2. Überprüfen Sie die Bewegungswerte

3. Das Kamerabild zeigt an, welcher Bereich des Kamerabildes eine Bewegungserkennungsaufzeichnung verursacht

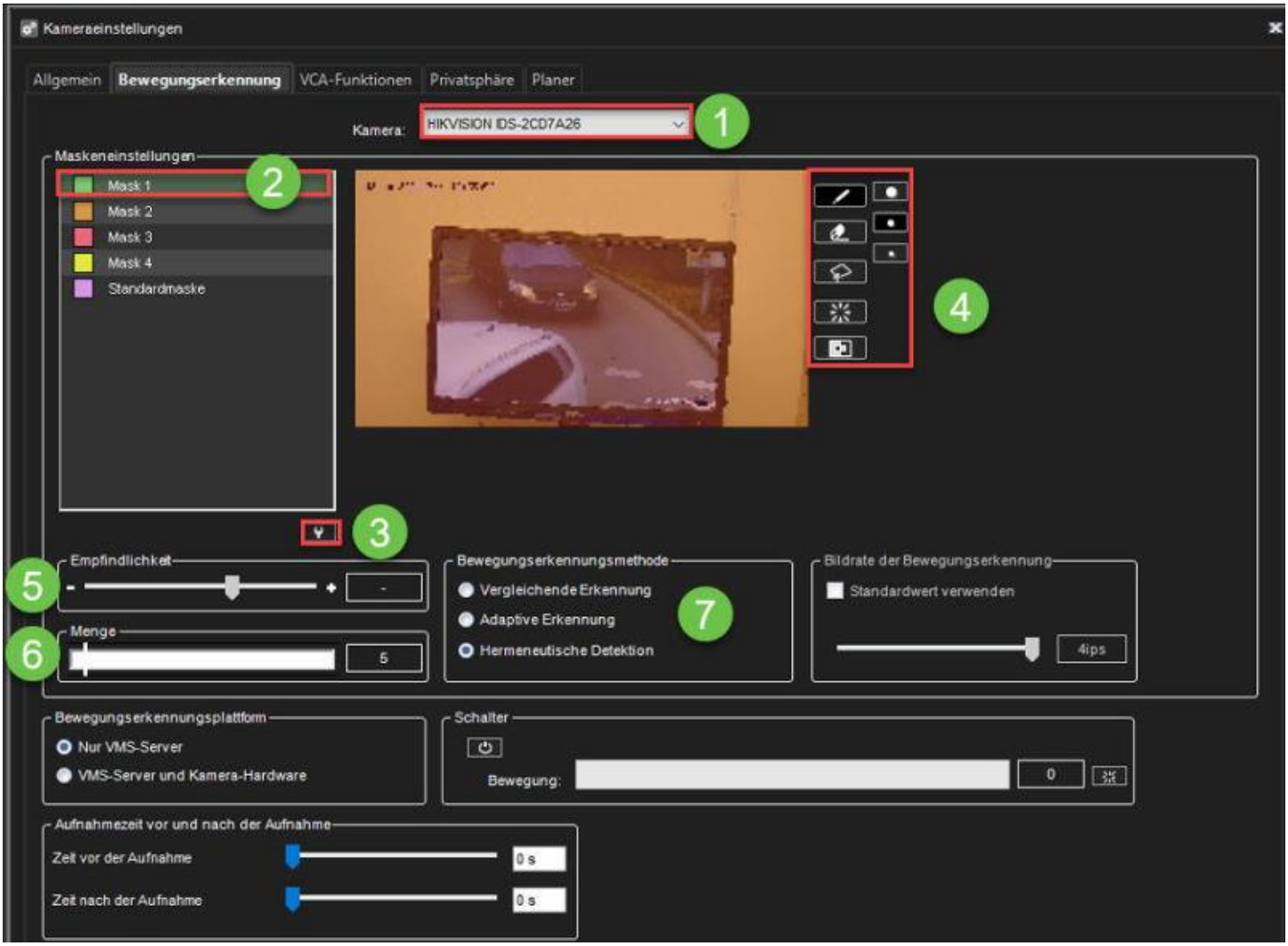


9.6.3.5 Vor- und Nachaufzeichnungszeit

Die Vor- und Nachaufzeichnung von Bewegungen wird verwendet, um Material vor und nach der Bewegung aufzuzeichnen.
Jede Maske kann separat konfiguriert werden.
Die Werte reichen von 0s bis 60 Minuten.

9.6.3.6 Bearbeiten einer Maske

1. Wählen Sie auf der Registerkarte **Bewegungserkennung** die Kamera aus der Kameraliste aus.
2. Klicken Sie auf die Maske, die Sie bearbeiten möchten.
3. Um den Namen der Maske zu ändern, klicken Sie auf **Maskennamen ändern** und geben Sie einen neuen Namen für die Maske ein.



1. Zeichnen Sie mit den in der folgenden Tabelle aufgeführten Zeichenwerkzeugen die Bereiche rot, in denen das System Bewegungen erkennen soll, und entfernen Sie das Rot aus den Bereichen, in denen die Bewegung ignoriert werden soll.
2. Stellen Sie die Erkennungsempfindlichkeit ein.
3. Stellen Sie die minimale Bewegungsmenge ein.
4. Wählen Sie die Bewegungserkennungsmethode aus: vergleichende, adaptive oder hermeneutische Bewegungserkennung.

Erkannte Bewegung wird im Bild rot angezeigt und der Zähler erhöht sich bei jeder erkannten Bewegung.

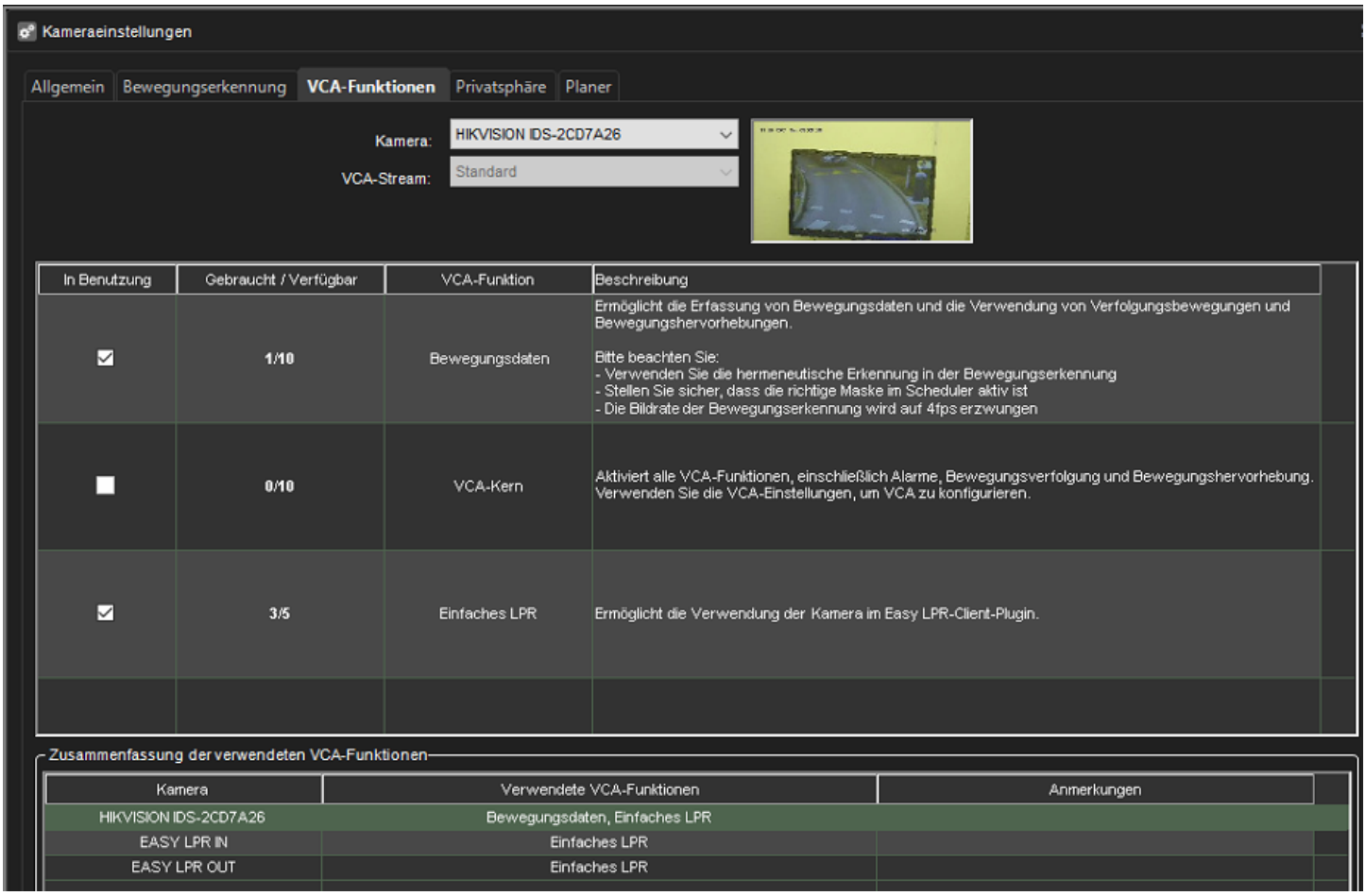
9.6.3.6.1 Zeichenutensilien:

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).
Invalid file id - c81910...	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).

9.6.4 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.

9.6.5 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.

9.6.5.1 Privatzone auf der Kamera

9.6.5.1.1 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**.

9.6.5.1.2 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**.

9.6.5.1.3 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**

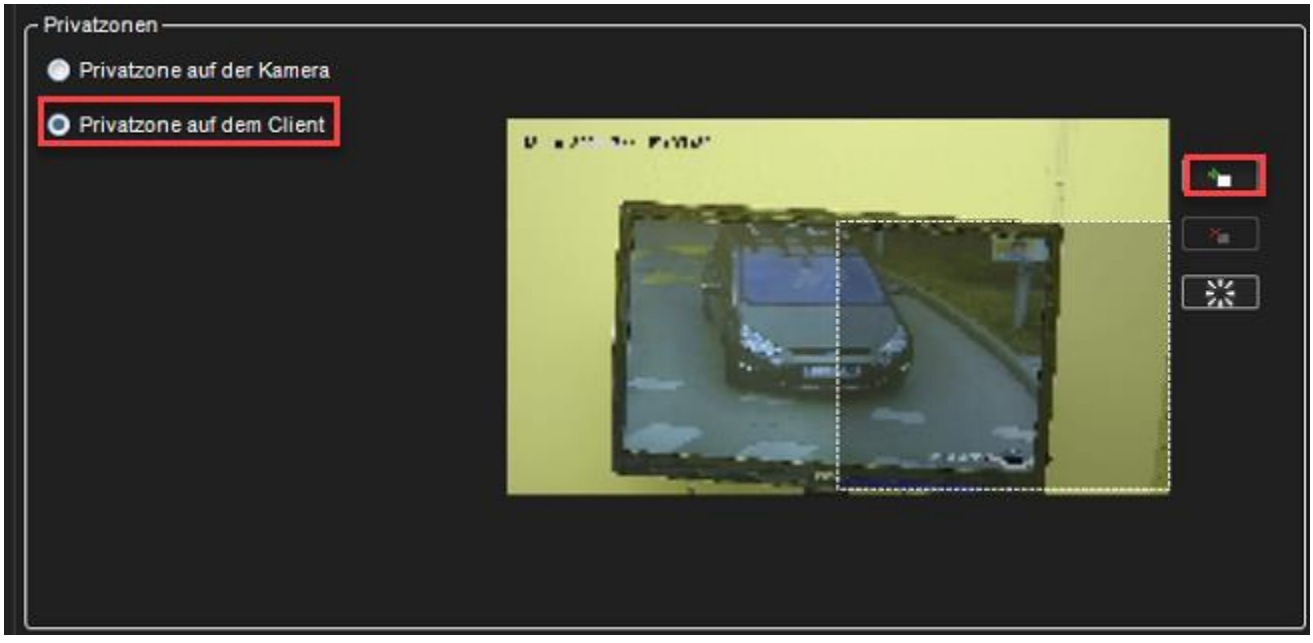
Privatzone hinzufügen.

9.6.5.2 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.

9.6.5.2.1 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**.



9.6.5.2.2 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**.

9.6.5.3 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.

9.6.5.3.1 Gesichter verwischen

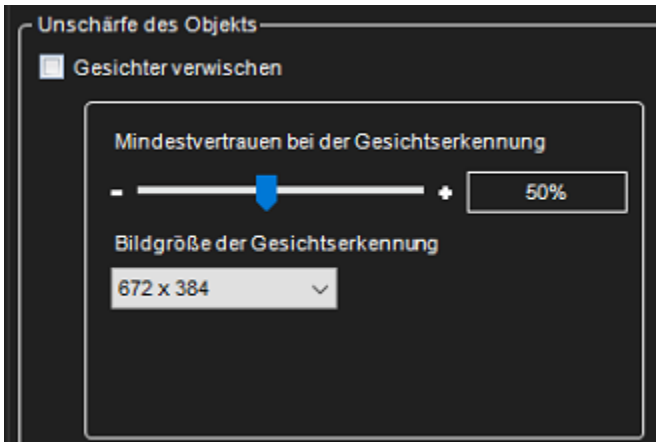
9.6.5.3.1.1 Mindestvertrauen bei der Gesichtserkennung

9.6.5.3.1.2 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



9.6.5.3.2 Verwischen Sie sich bewegende Objekte

9.6.5.3.2.1 Empfindlichkeit der Bewegungserkennung

Wie empfindlich Pixel im Bild als Bewegungspixel
erkannt werden

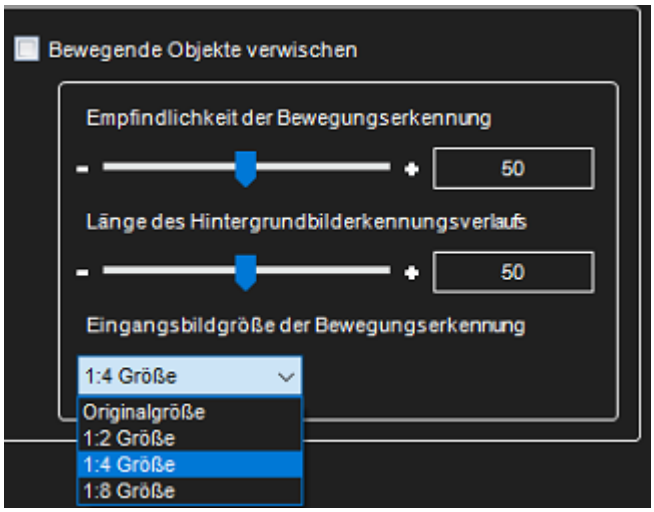
9.6.5.3.2.2 Länge des Hintergrundbilderkennungsverlaufs

Wie schnell stationäre Objekte als Hintergrund erkannt werden

9.6.5.3.2.3 Eingangsbildgröße der Bewegungserkennung

Die kleinere Größe ist schneller zu verarbeiten, liefert aber die schlechteren Ergebnisse.

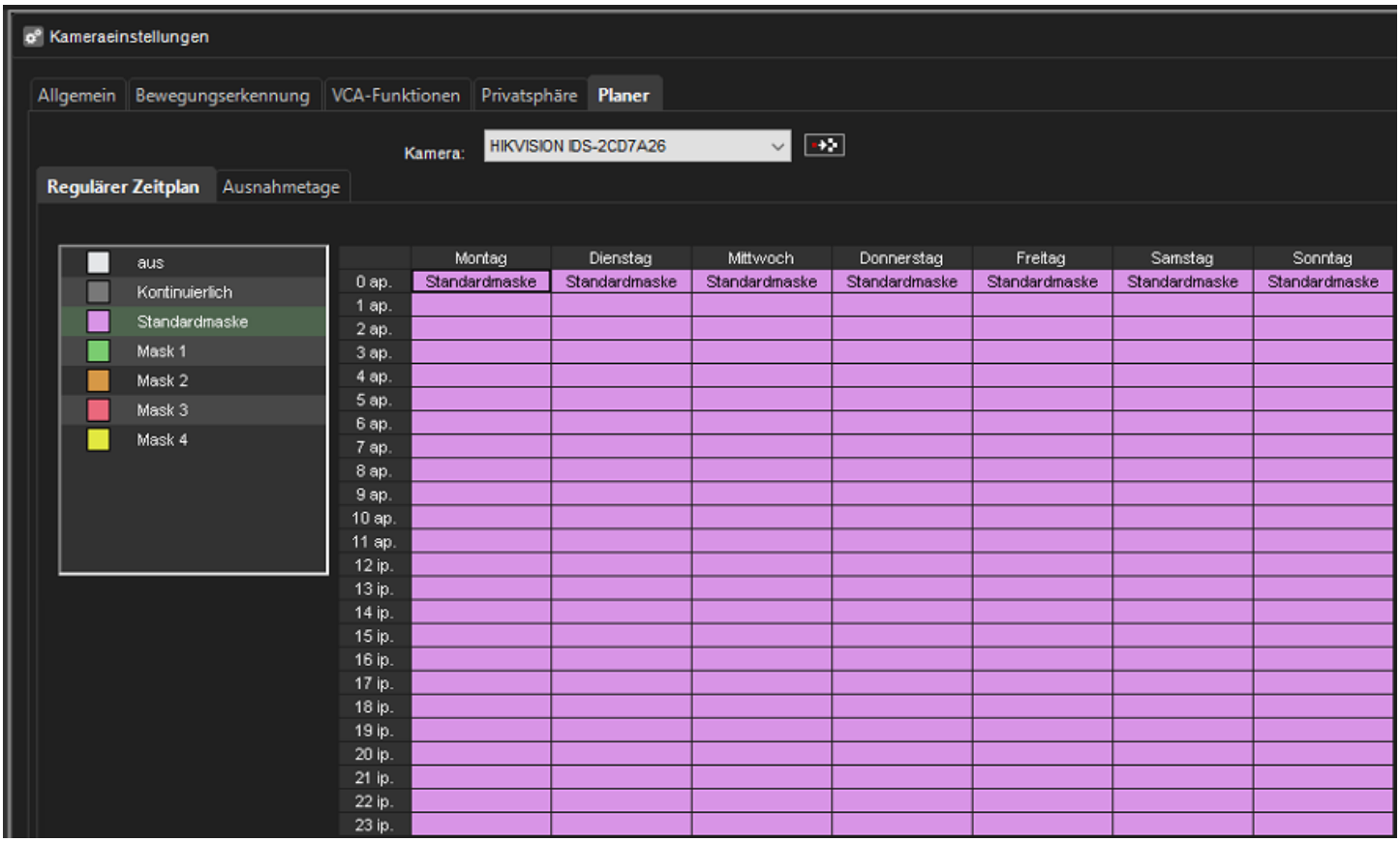
- Originalgröße
- 1:2 Größe
- 1:4 Größe
- 1:8 Größe



9.6.6 Planer

Der Planer definiert, welche Maske auf jeder Kamera verwendet wird und welche Tage und Stunden für die Maske aktiv sind.

Standardmäßig wird ein Video aufgezeichnet, wenn das System eine Bewegung in der Standardmaske erkennt. Die Standardmaske ist rund um die Uhr aktiv.



Sie können jedoch für jede Stunde der Woche unterschiedliche Optionen festlegen. Um den Zeitplan zu ändern, klicken Sie auf die Maske, die Sie aktivieren möchten, und klicken Sie dann auf die geplante Stunde, in der Sie sie verwenden möchten.

Spitze *Um mehr als eine Stunde gleichzeitig zu ändern, ziehen Sie mit der Maus.*

Um alle Stunden der Woche zu ändern, klicken Sie auf die Zelle über der Stundenspalte (auf der linken Seite der Überschriftenzeile des Wochentags).

Diese Optionen sind verfügbar:

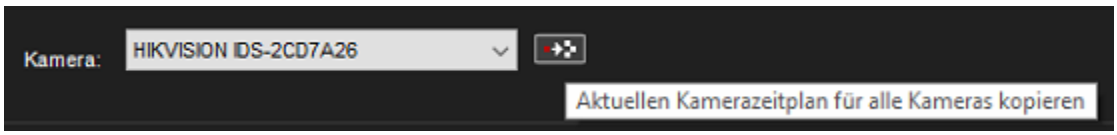
- **aus** Video wird nicht aufgezeichnet. Mögliche Alarme werden jedoch aufgezeichnet. Alarme werden in **Alarmeinstellungen** konfiguriert.
- **Kontinuierlich** Die Kamera nimmt alle Bilder auf. Diese Option verbraucht viel Speicherplatz.

- **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.

So kopieren Sie den aktuellen Zeitplan 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.

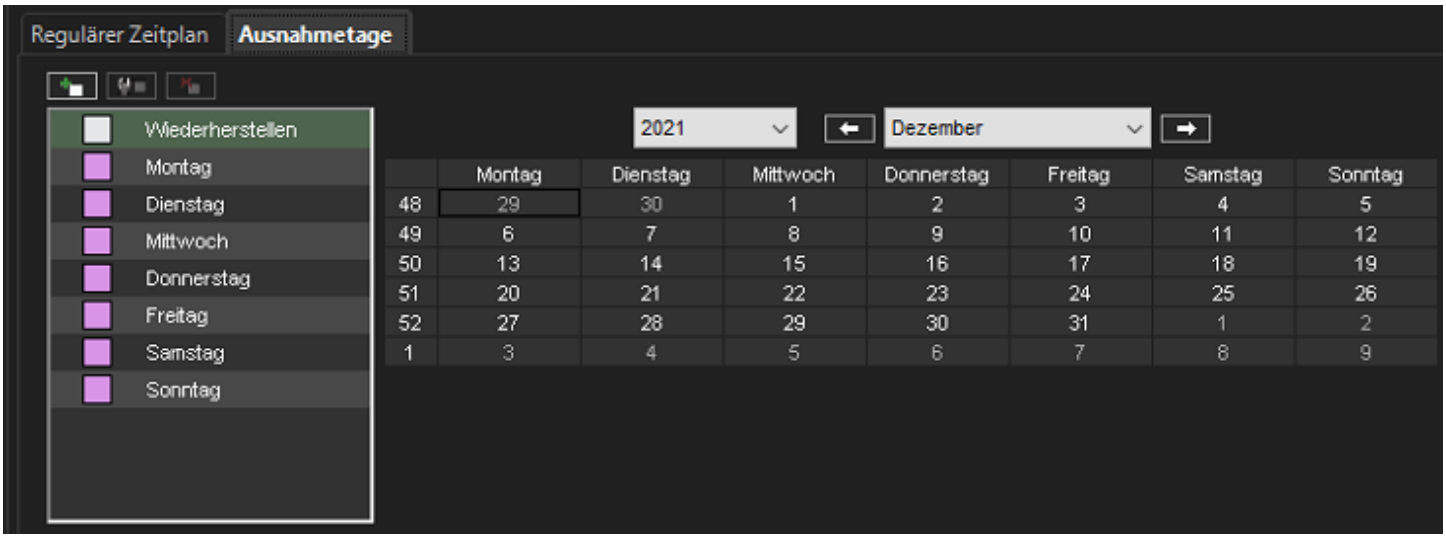


9.6.6.1 Mit den Einstellungen für Ausnahmetage können Sie Feiertage im Kalender festlegen.

9.6.6.1.1 So legen Sie einen Zeitplan für Ausnahmetage fest:

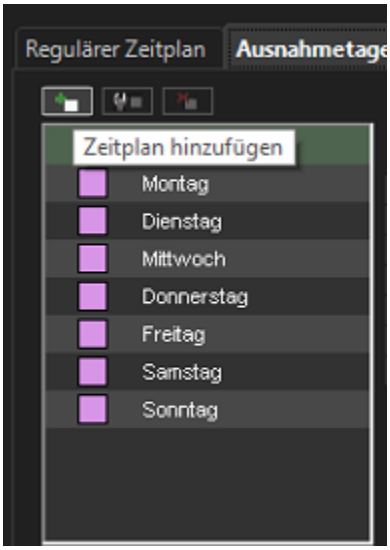
Sie können einen Tagesplan aus dem **regulären Plan** anwenden oder einen **Ausnahmeplan mit Tagen** verwenden.

1. Wählen Sie auf der Registerkarte **Ausnahmetage** das Jahr und den Monat aus.
2. Klicken Sie im linken Bereich auf den Zeitplan, den Sie anwenden möchten, und klicken Sie dann im Kalender auf den Feiertag.



9.6.6.1.2 So fügen Sie einen benutzerdefinierten Zeitplan hinzu:

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**

9.6.6.1.3 So bearbeiten Sie einen benutzerdefinierten Zeitplan:

1. Wählen Sie den Zeitplan aus und klicken Sie auf **Zeitplan bearbeiten**.
2. Bearbeiten Sie den Zeitplan und klicken Sie auf **OK**.

9.6.6.1.4 So löschen Sie einen benutzerdefinierten Zeitplan:

- Wählen Sie den Zeitplan im linken Bereich aus und klicken Sie auf **Zeitplan löschen**.

9.6.6.1.5 So stellen Sie den ursprünglichen Zeitplan wieder her:

Klicken Sie auf **Wiederherstellen** und dann auf den Tag, den Sie wiederherstellen möchten.

9.6.7 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.

9.6.7.1 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.

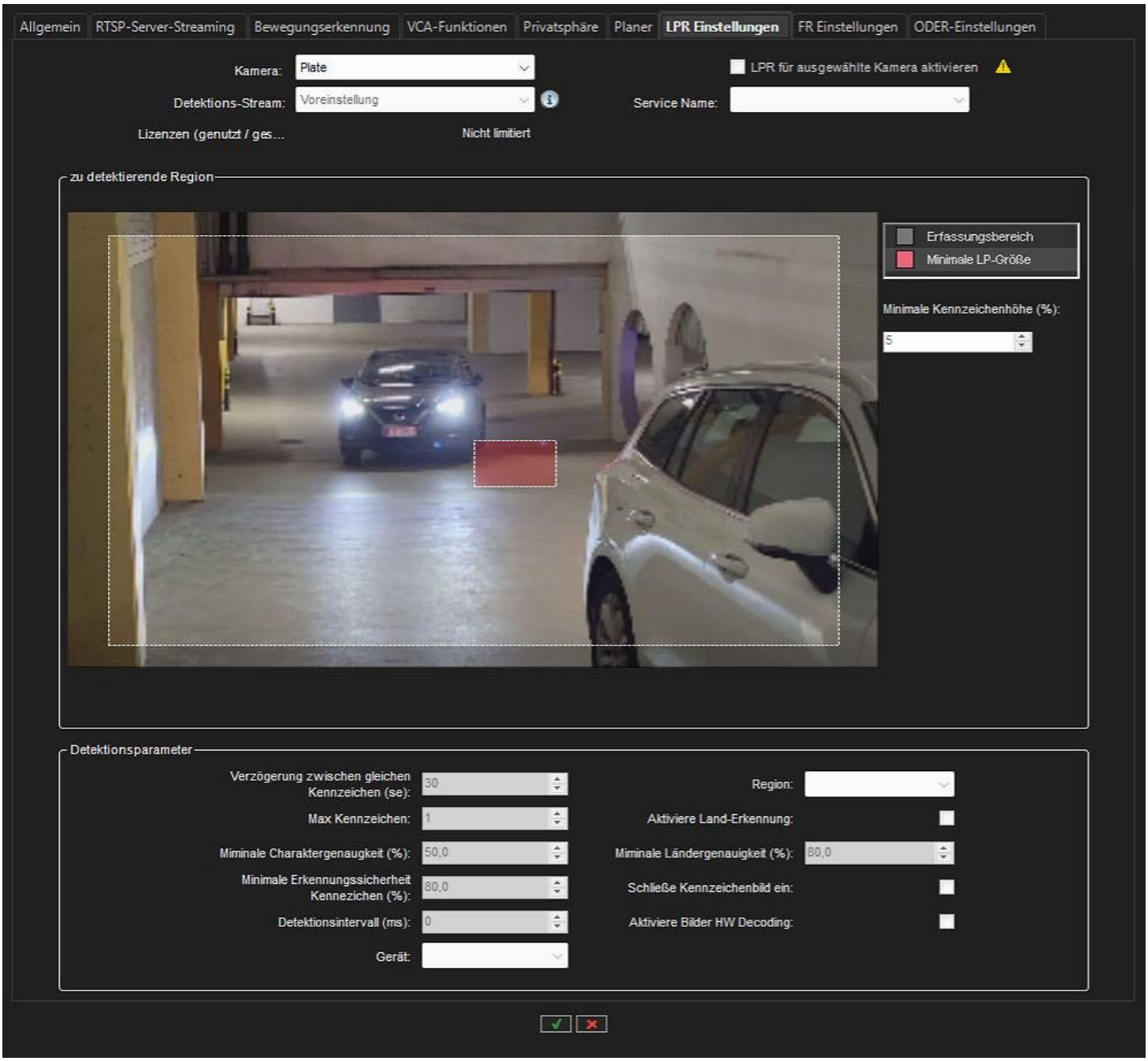
9.6.7.1.1 Kamera auswählen, streamen und LPR aktivieren

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.

9.6.7.2 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.
- **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).

9.6.7.3 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.

9.6.7.4 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.

9.6.8 Einstellungen für die Face Recognition (FR)

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.

9.6.8.1 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.

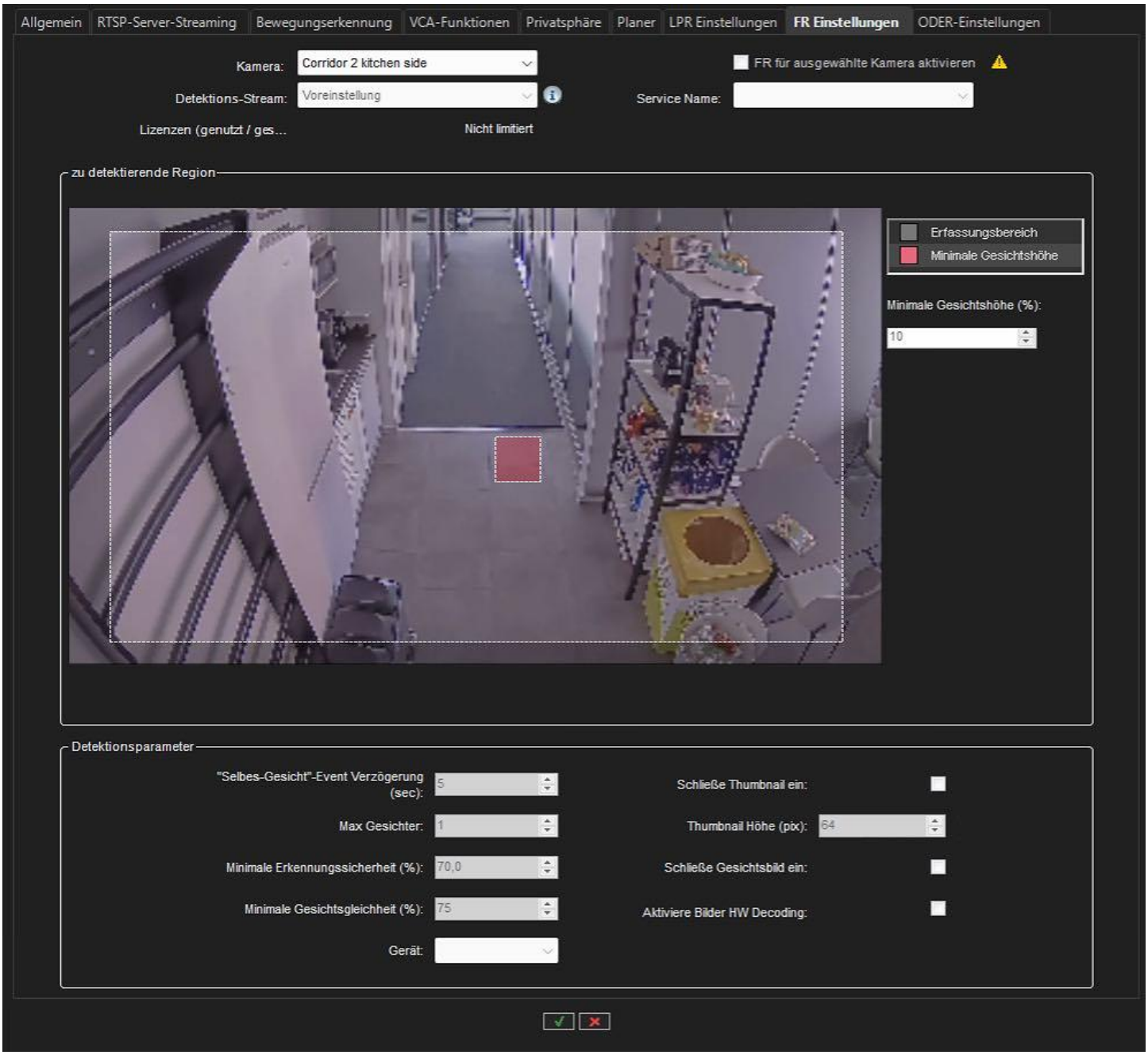
Wenn Ihre Lizenz die Smart FR-Funktion nicht unterstützt, wird die Registerkarte FR-Einstellungen ausgeblendet.

9.6.8.1.1 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.

9.6.8.2 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.



9.6.8.3 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 5 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).

9.6.8.4 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.

9.6.8.5 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.

9.6.9 Einstellungen für die Object Recognition (OR)

Systemadministrator-Einstellungen, die es Operatoren ermöglichen, die Objekterkennung in der Spotter Smart Search zu nutzen.

9.6.9.1 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.

9.6.9.1.1 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.

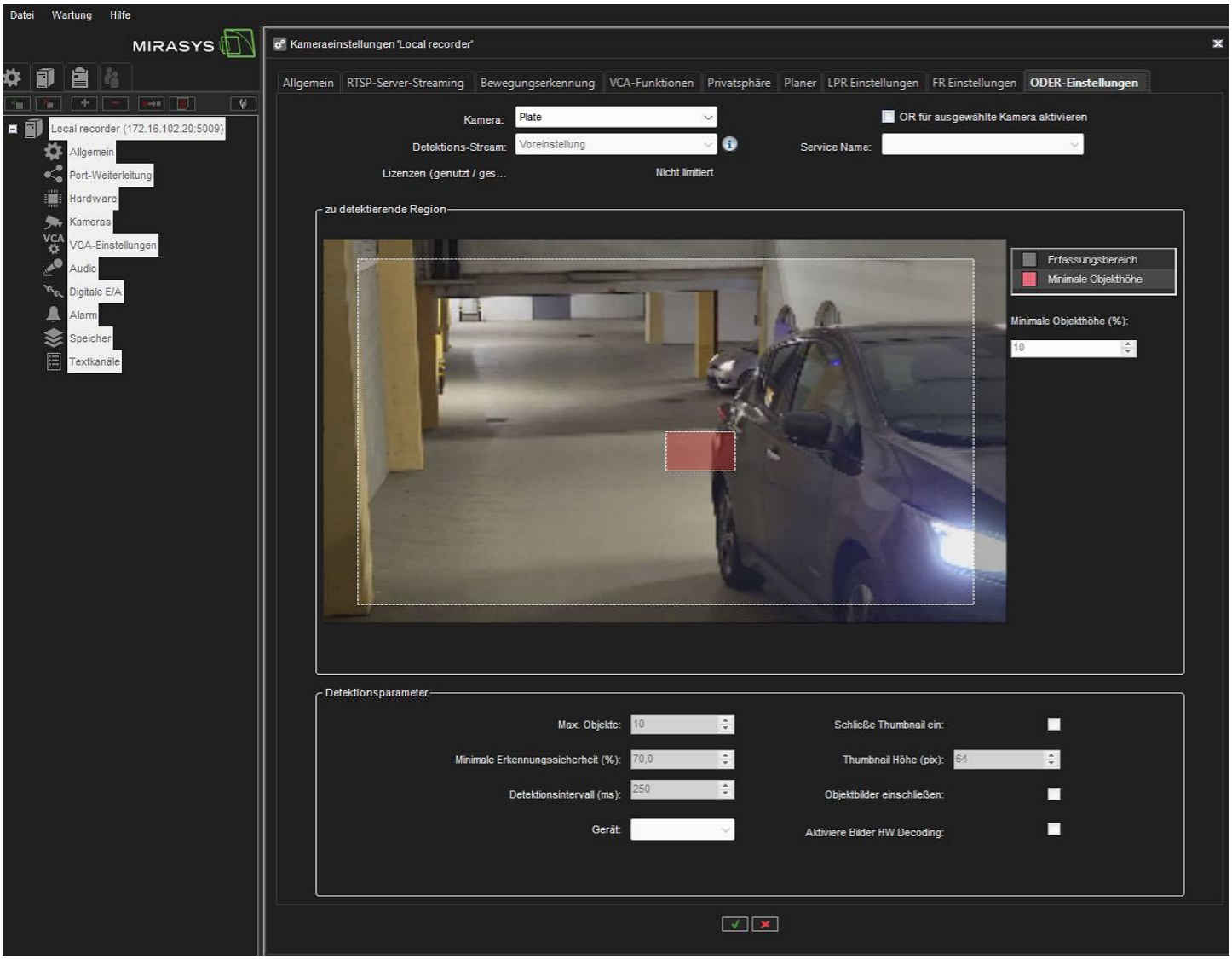
4. Wenn das Kontrollkästchen OR für ausgewählte Kamera aktivieren nicht markiert ist, ist das Dropdown-Menü Dienst deaktiviert.
5. Das Textfeld Lizenz zeigt die Anzahl der verwendeten Lizenzen und die maximale Anzahl von Lizenzen an.

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.

9.6.9.1.2 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.



9.6.9.1.3 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.

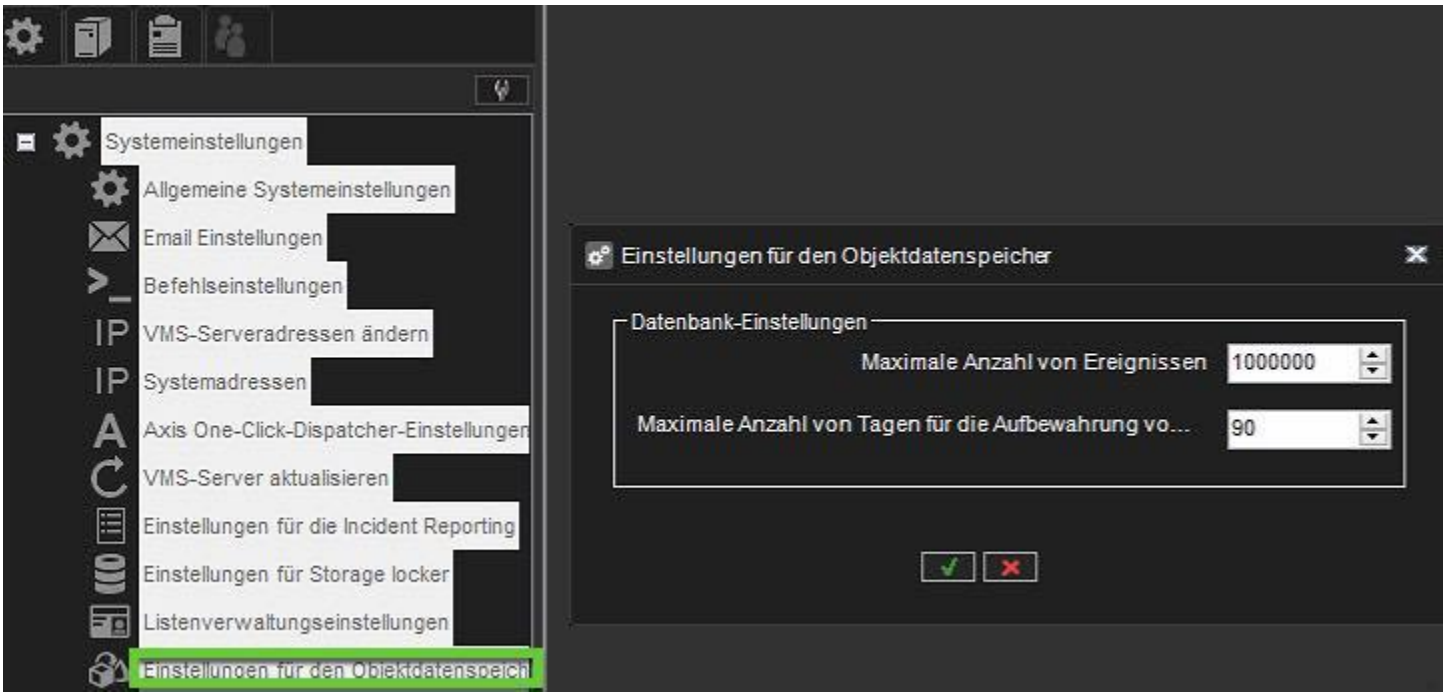
Thumbnail höhe (px) - die Höhe des Thumbnail-Bildes in Pixeln. NUR aktiviert, wenn das Kästchen Miniaturbild einschließen markiert ist. Der Wert sollte zwischen 32 und 128 Pixeln liegen.

Objektbilder einschließen - schließt Objektbilder in die zurückgegebenen Daten ein oder nicht.

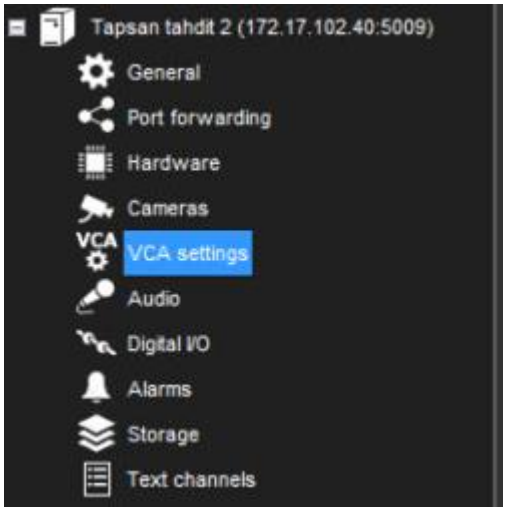
Aktiviere Bilder HW-Dekodierung - aktivieren Sie die Dekodierung der eingegebenen Bilder mit der am besten geeigneten Computerplattform (CUDA, DXVA oder DirectX).

9.6.9.2 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 > Objektdatenspeichereinstellungen.



9.7 VCA-EINSTELLUNGEN



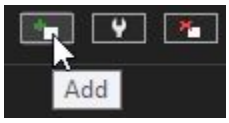
9.8 Audio

9.8.1 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.

9.8.1.1 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.*

9.8.1.2 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**.

9.8.1.3 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.

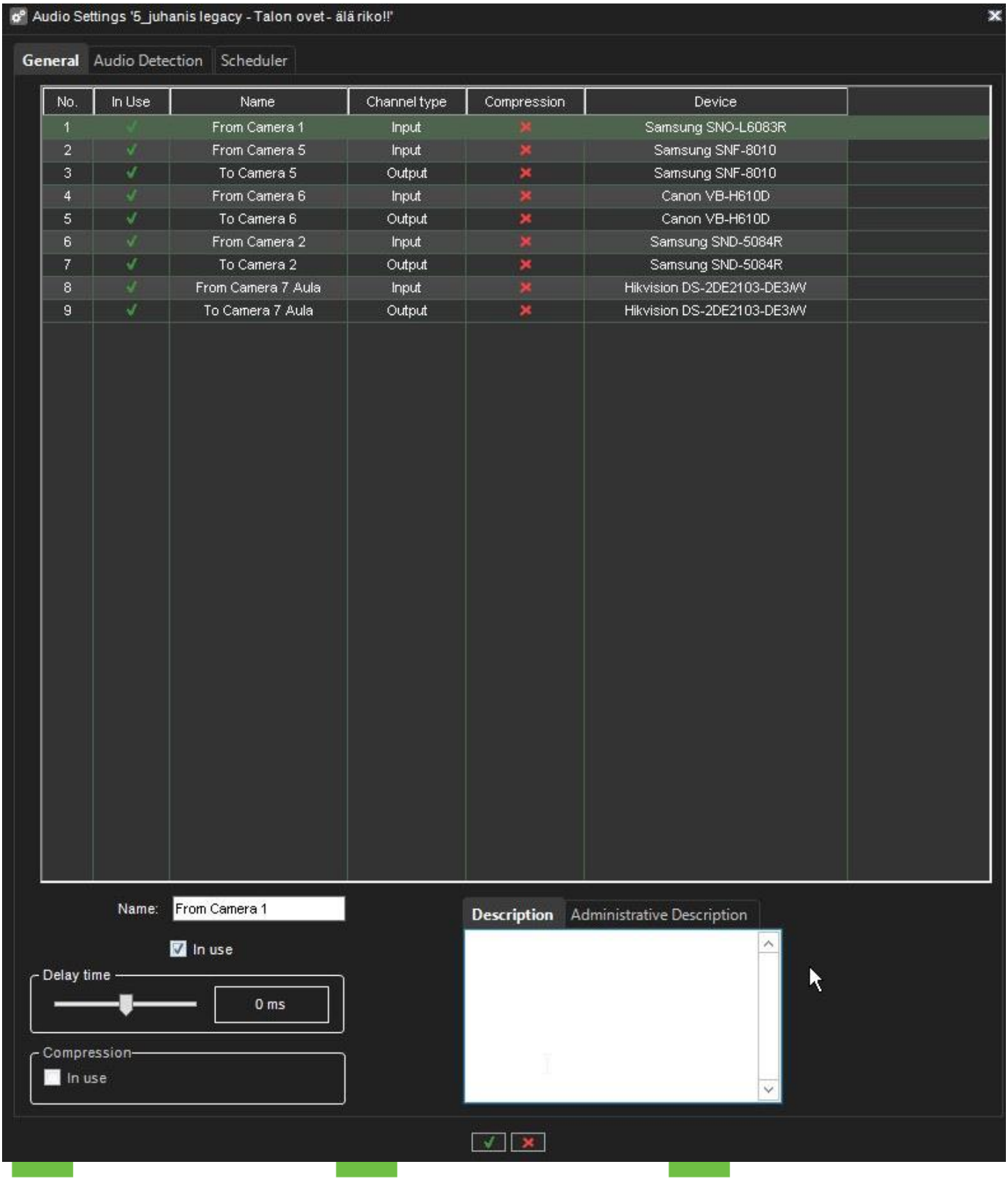
9.8.2 Audio Einstellungen

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.

9.8.3 Allgemeine Einstellungen (Audio)


Audio Settings '5_juhanis legacy - Talon ovet - älä riko!!'
General
Audio Detection
Scheduler
No.
In Use
Name
Channel type
Compression
Device
1 From Camera 1 Input Samsung SNO-L6083R
2 From Camera 5 Input Samsung SNF-8010
3 To Camera 5 Output Samsung SNF-8010
4 From Camera 6 Input Canon VB-H610D
5 To Camera 6 Output Canon VB-H610D
6 From Camera 2 Input Samsung SND-5084R
7 To Camera 2 Output Samsung SND-5084R
8 From Camera 7 Aula Input Hikvision DS-2DE2103-DE3/W
9 To Camera 7 Aula Output Hikvision DS-2DE2103-DE3/W
Name:
From Camera 1
In use
Delay time
0 ms
Compression
In use
Description
Administrative Description

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**.

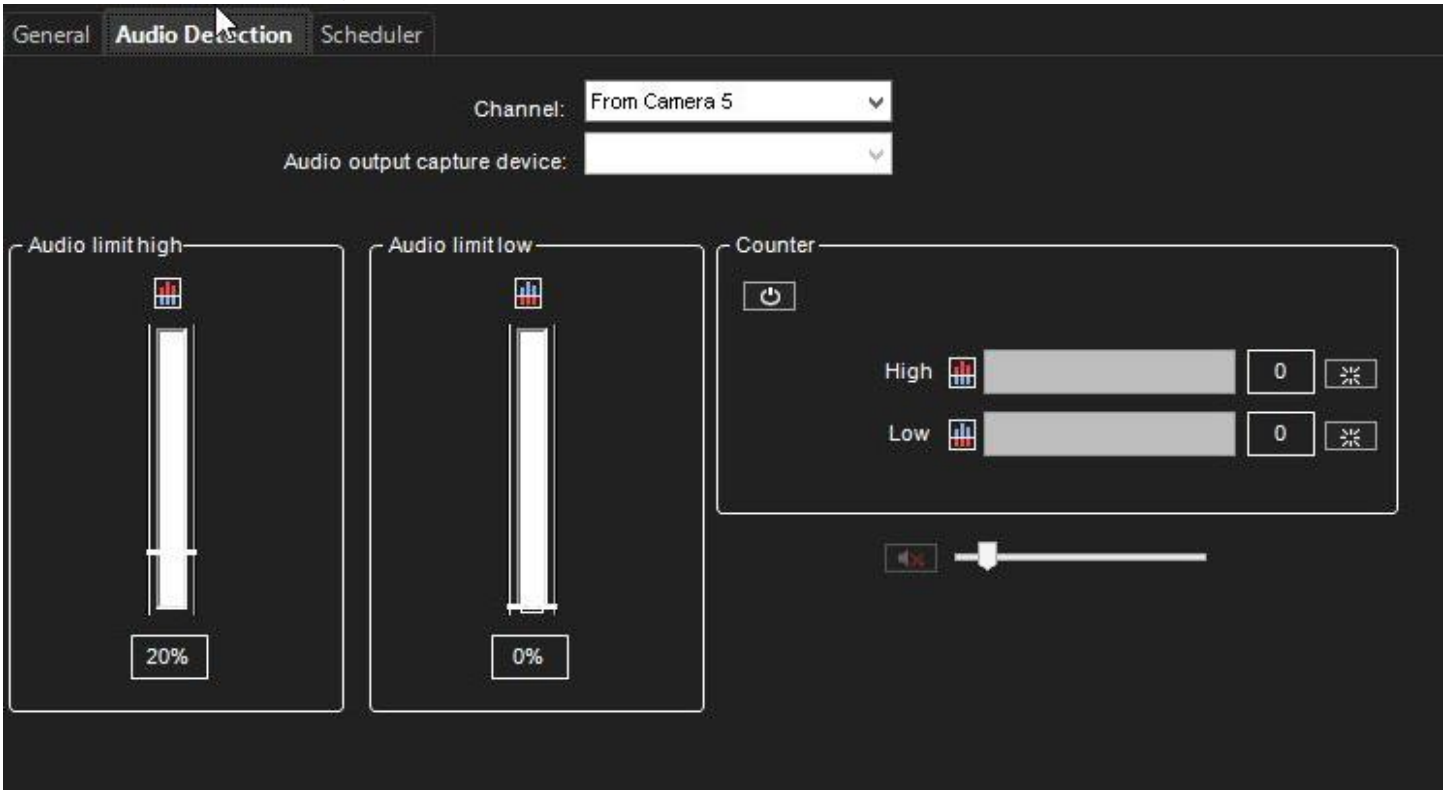
Allgemeine Einstellungen ändern:

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.

9.8.4 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.

9.8.5 Planer (Audio)

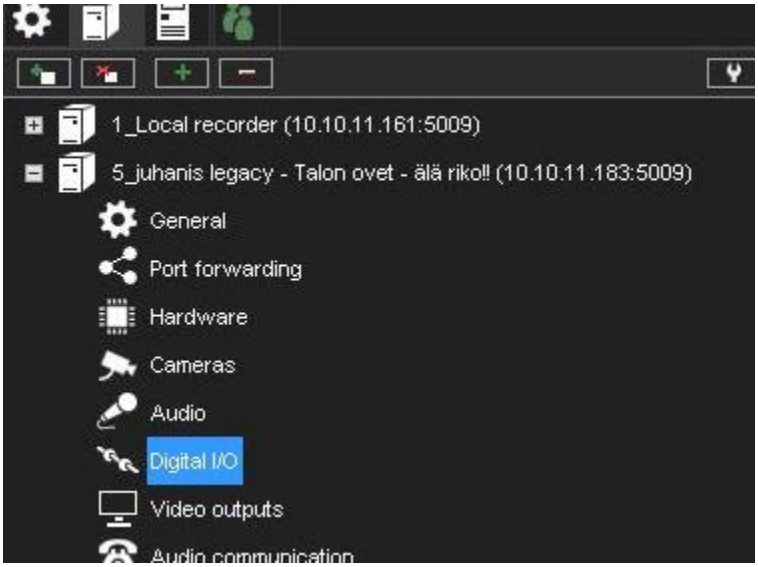
Standardmäßig wird Audio aufgezeichnet, wenn der erkannte Audiopegel die Standarderkennungsgrenze (**Audio limit high**) überschreitet.

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.

9.9 Digitale E/A

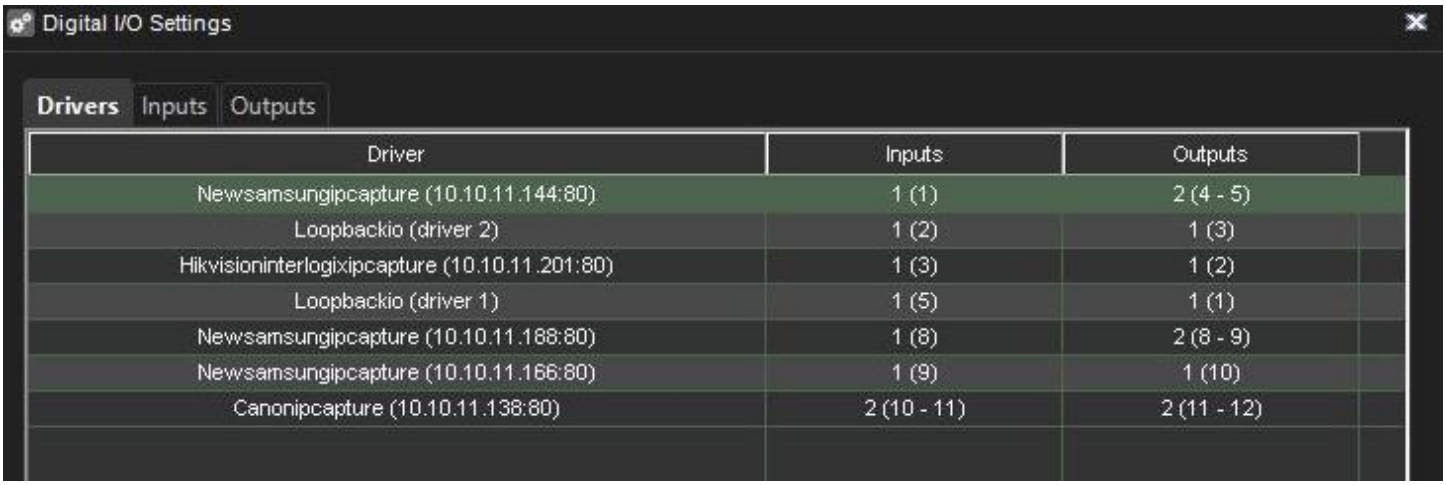


9.9.1 Digitale E/A-Einstellungen

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.

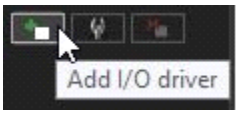
9.9.1.1 Treiber

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.

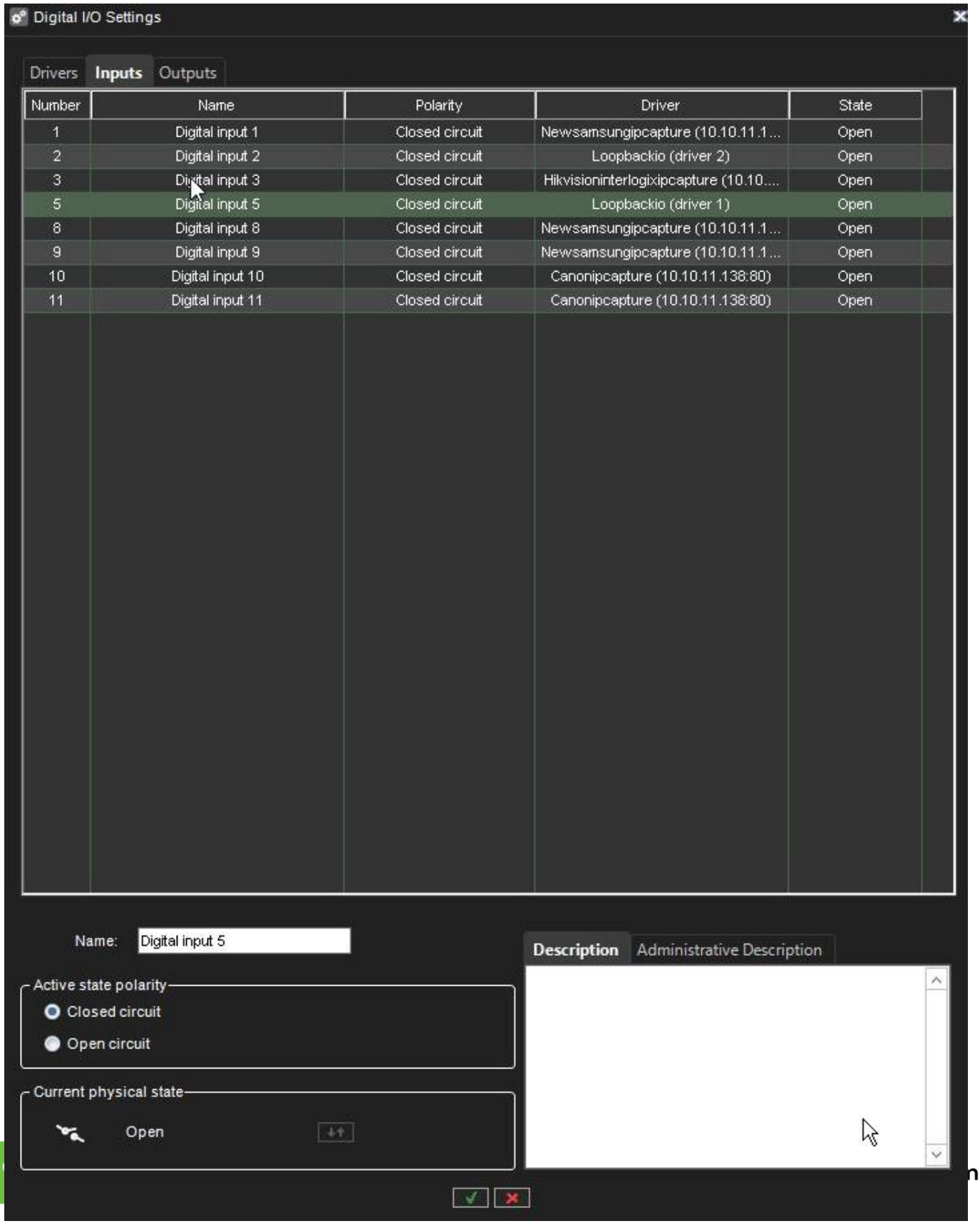
3. Doppelklicken Sie auf den Gerätetreiber, den Sie bearbeiten möchten.
4. Bearbeiten Sie die Geräteeinstellungen in der Liste **Eigenschaften**.
5. Um die Einstellungen zu speichern, klicken Sie auf **OK**.

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.

9.9.1.2 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.


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.

9.9.1.3 Digitale Ausgänge

Wählen Sie bei digitalen Ausgängen, ob ein Relais geöffnet oder geschlossen ist (Polarität), wenn der Ausgang ausgelöst wird.

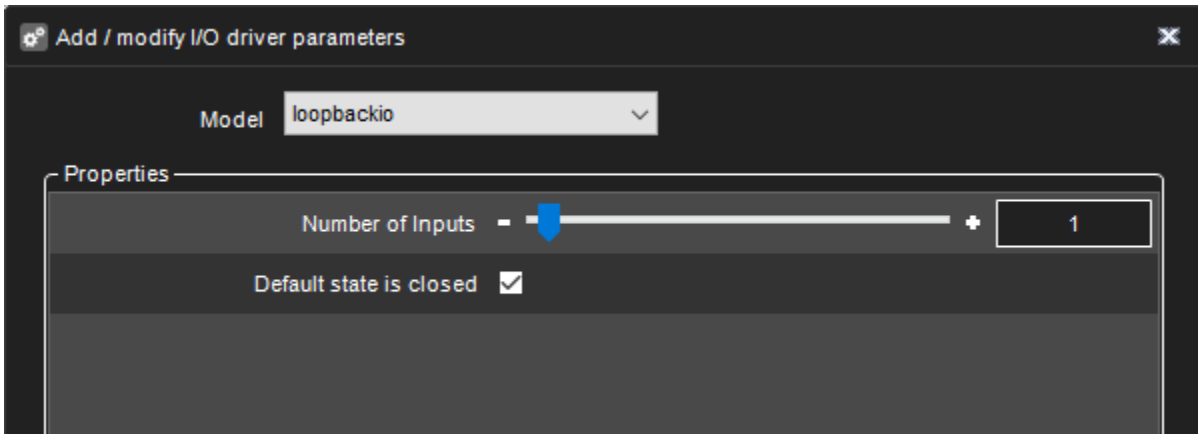
Name Um einen Ausgang umzubenennen, wählen Sie den Ausgang aus und geben Sie dann einen neuen Namen für den Ausgang in **Name**.
Polarität des aktiven Zustands ein. Wählen Sie den Ausgang und wählen Sie dann, ob der Ausgang geschlossen oder geöffnet ist, wenn er aktiviert wird.
Aktueller physikalischer 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)**.

9.9.2 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.



9.9.3 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.

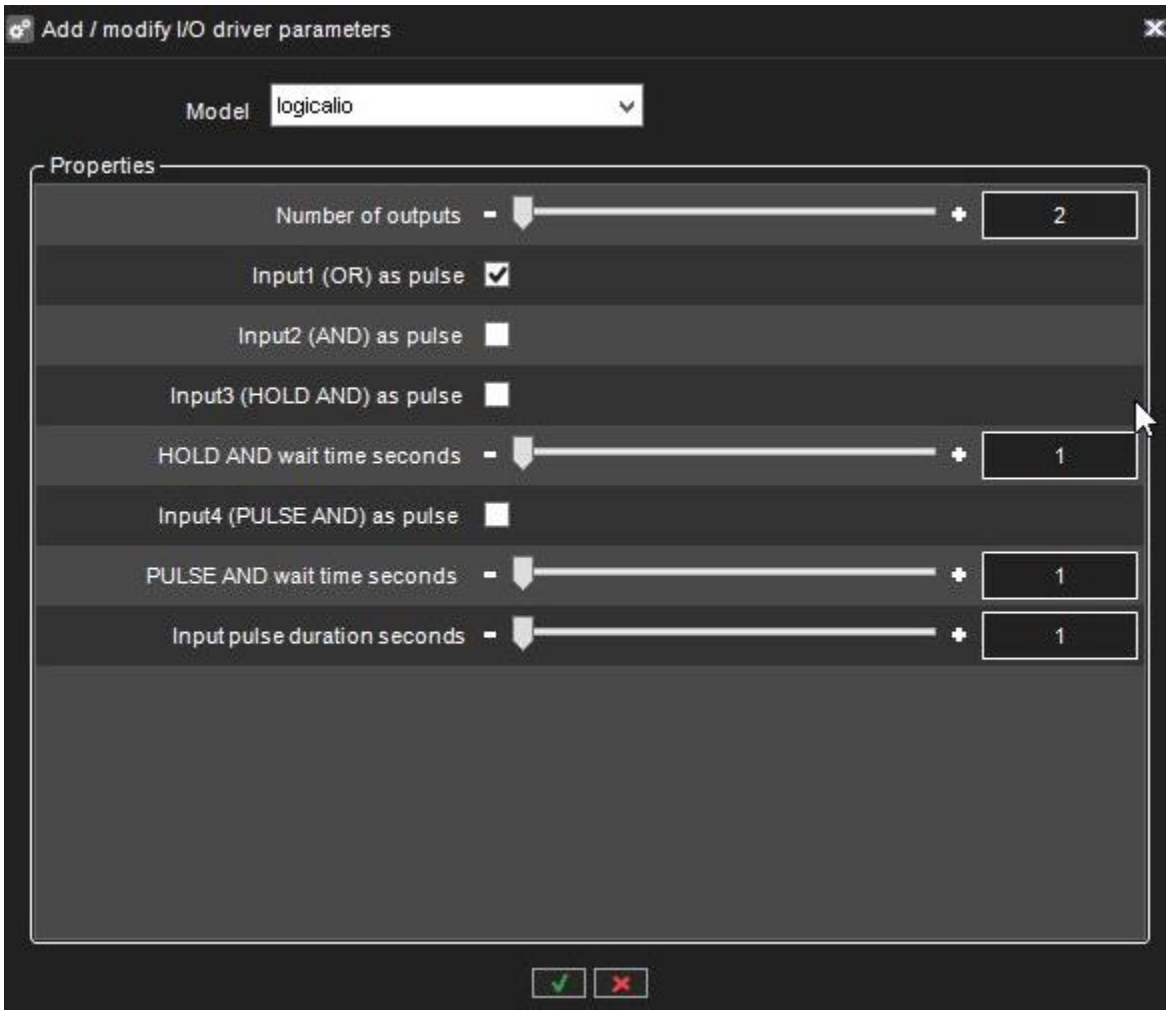
Ein anderes Beispiel könnte sein, dass ein Eingangs-„Tor" mit zwei Türen das Öffnen der zweiten Tür nur zulässt, wenn die erste geschlossen ist.

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.

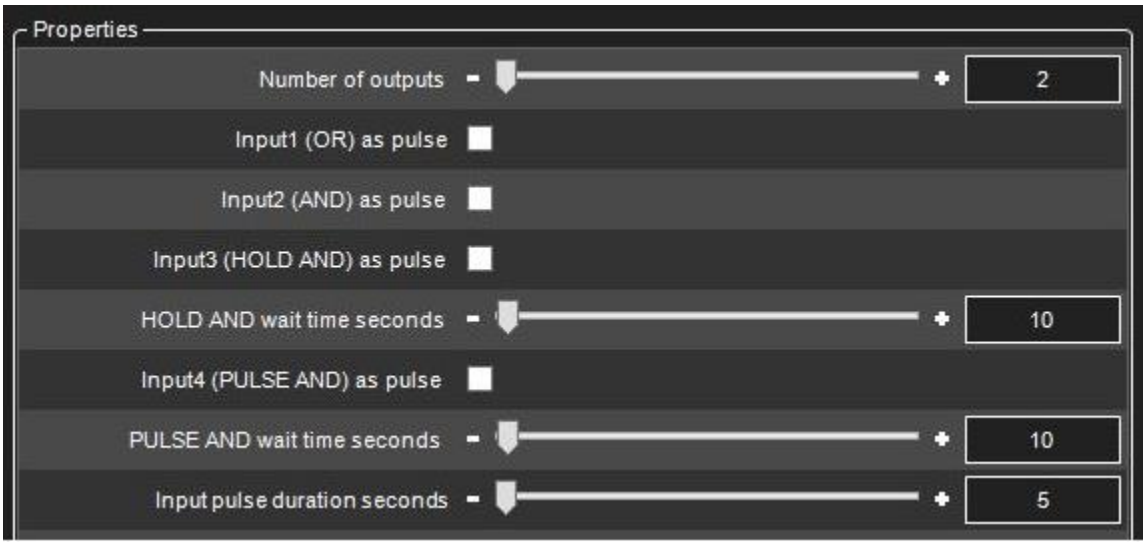
Die Mindestanzahl beträgt zwei, die Höchstzahl 32.



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:

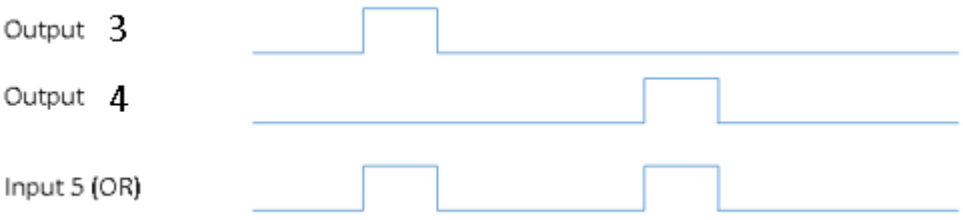


Das Beispiel hat 2 Ausgänge, die die Operanden sind. Diese sind in der IO-Liste als Ausgänge 3 und 4 zu sehen.

Die automatisch erstellten 4 Eingänge werden in der Liste als Eingänge 5, 6, 7 und 8 angezeigt.

9.9.3.1 „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.

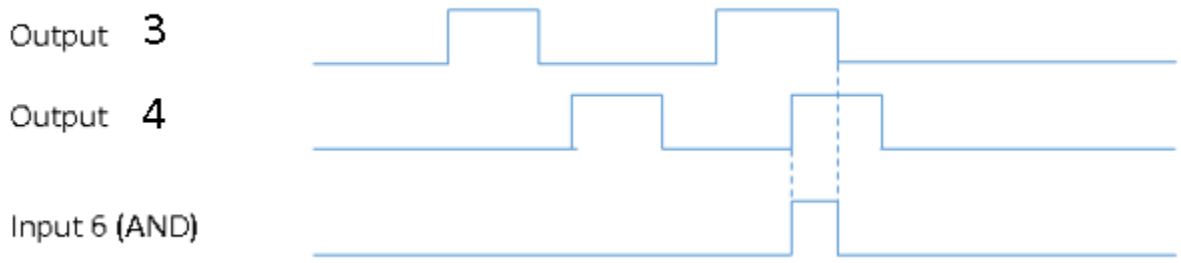


In unserem Beispiel ist Eingang 5 das ODER-Signal. Wenn entweder Ausgang 3 ODER Ausgang 4 eingeschaltet ist, wird als Ergebnis Eingang 5 eingeschaltet.

Der Eingang bleibt so lange eingeschaltet, wie einer der Ausgänge eingeschaltet bleibt. (Es sei denn, der Pulsmodus ist ausgewählt, siehe unten für Details)

9.9.3.2 „UND"-Eingang

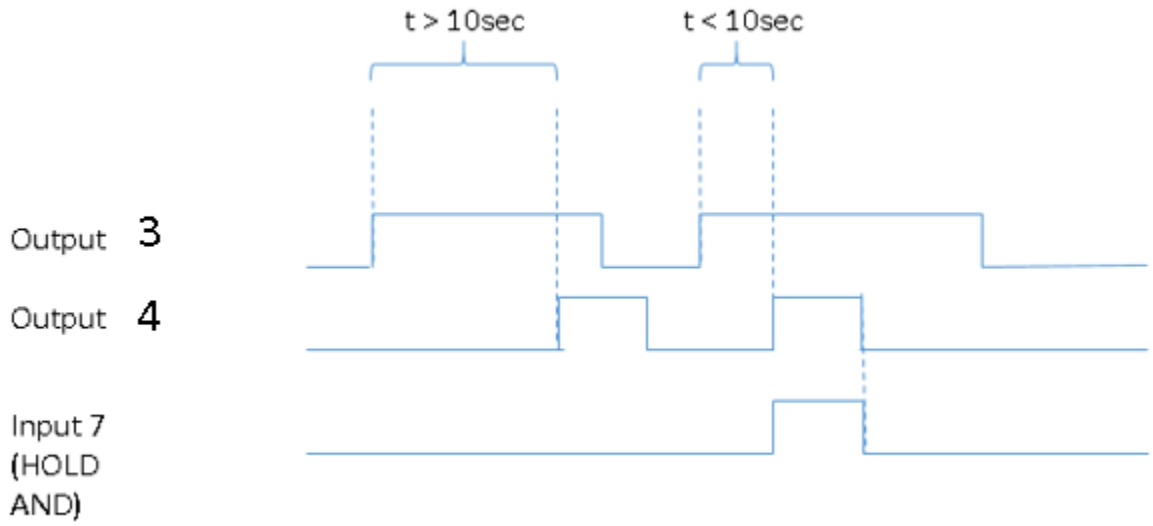
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.



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

9.9.3.3 "HOLD AND" Input

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



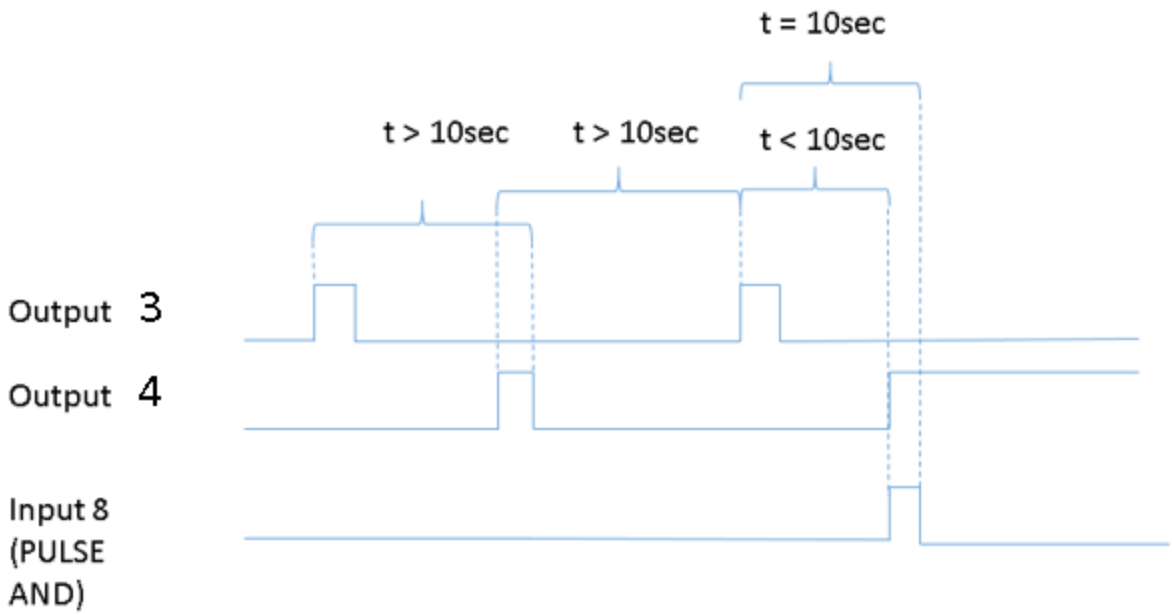
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

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

9.9.3.4 "PULSE AND" Input

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

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

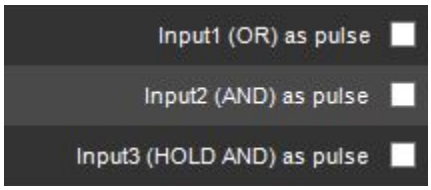


Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

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

9.9.3.5 Pulse Mode For Inputs

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



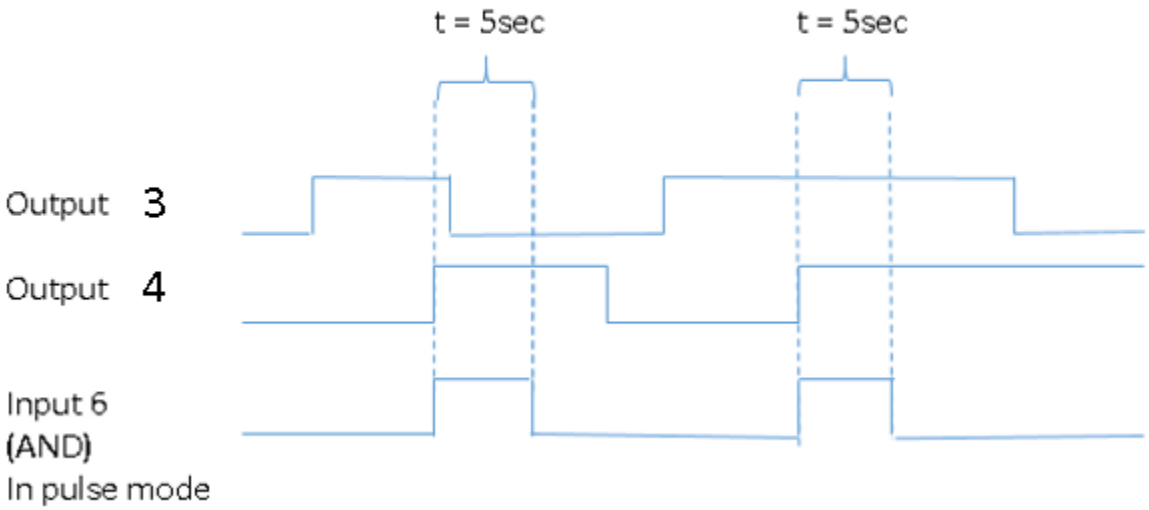
and

The pulse duration can also be adjusted.

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

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

It would mean behaviour like this:



9.9.4 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.

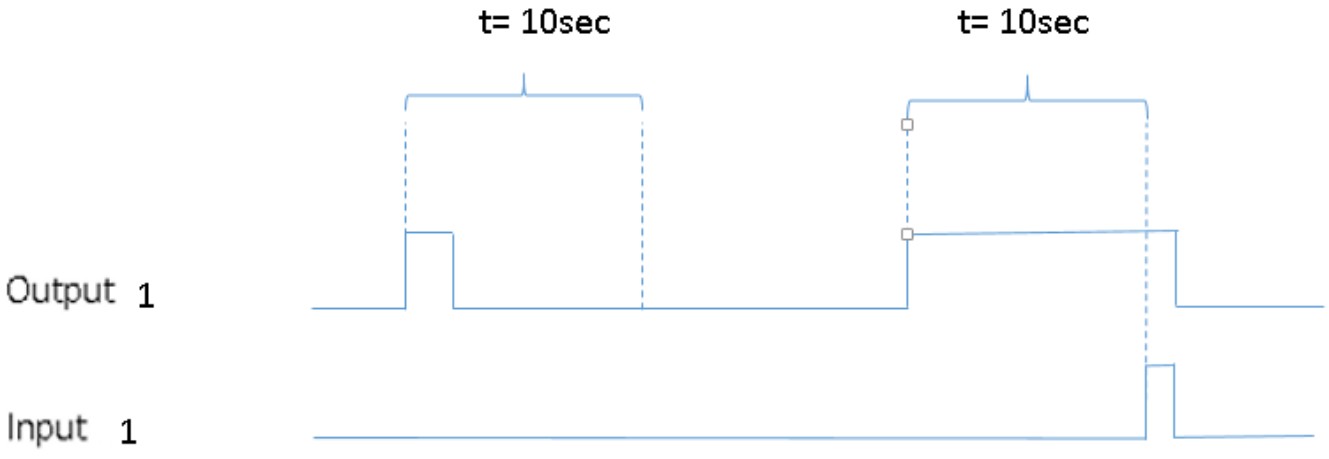
Eine Lizenz steuert logische E/A und Countdown-E/A. Wenn die Lizenz nicht vorhanden ist, schlägt das Erstellen neuer E/A fehl.

9.9.4.1 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.



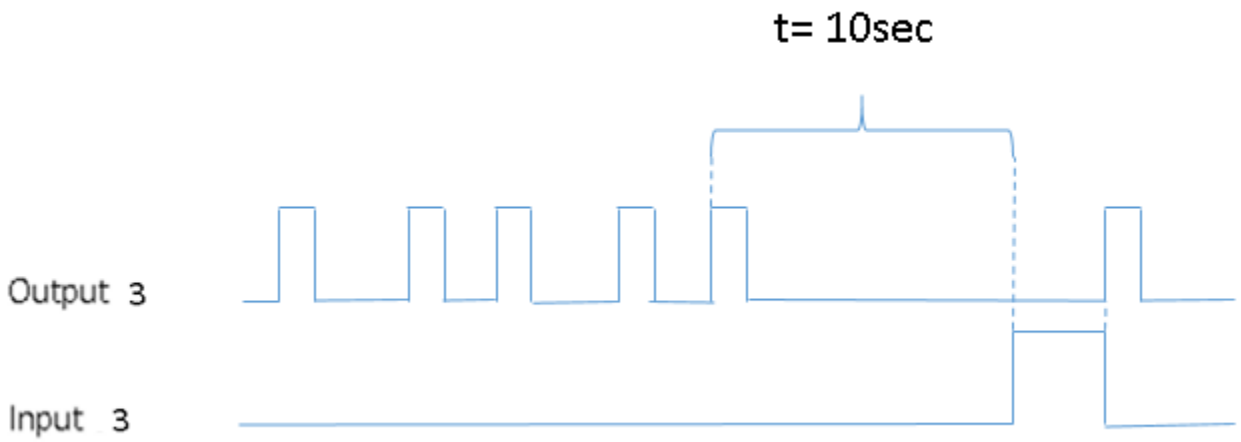
Beim Erstellen eines neuen Countdown-E/A sind die ersten beiden Eingangs-Ausgangspaare von diesem Typ.

9.9.4.2 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.

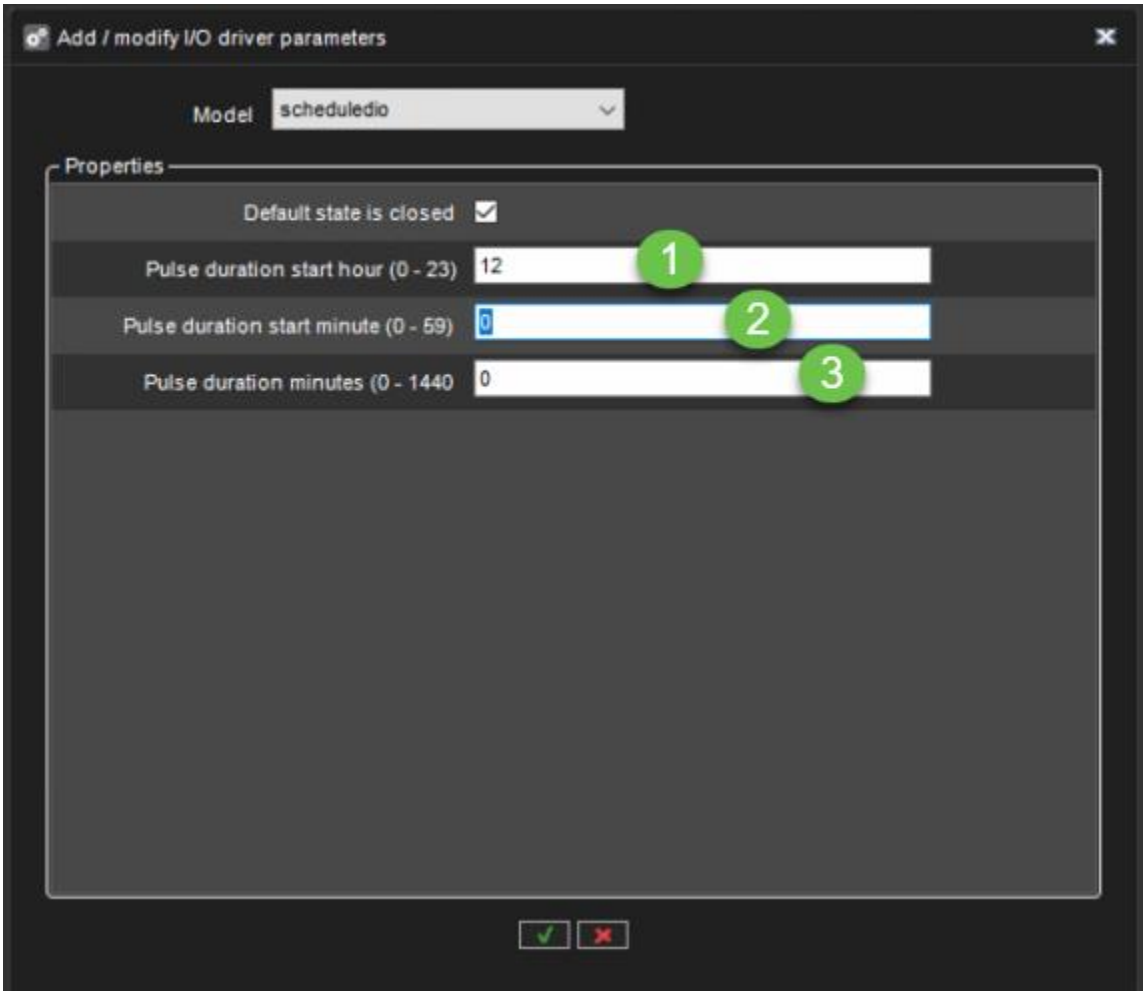
9.9.5 Geplante E/A

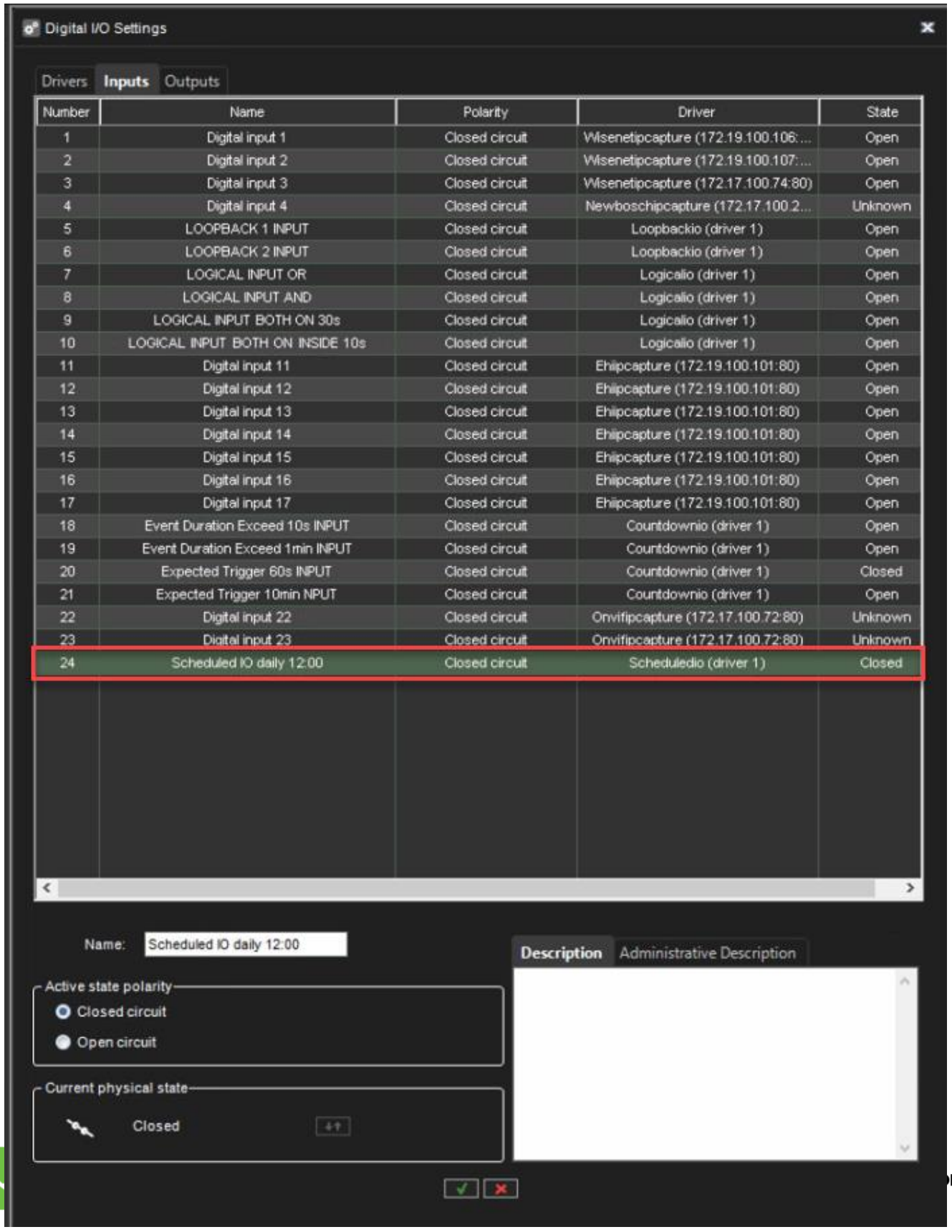
9.9.5.1 Mit Scheduled IO ist es möglich, einen Zeitplan für jeden digitalen Ausgang zu erstellen, der mit dem VMS-Server verbunden ist.

9.9.5.2 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

9.9.6 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)

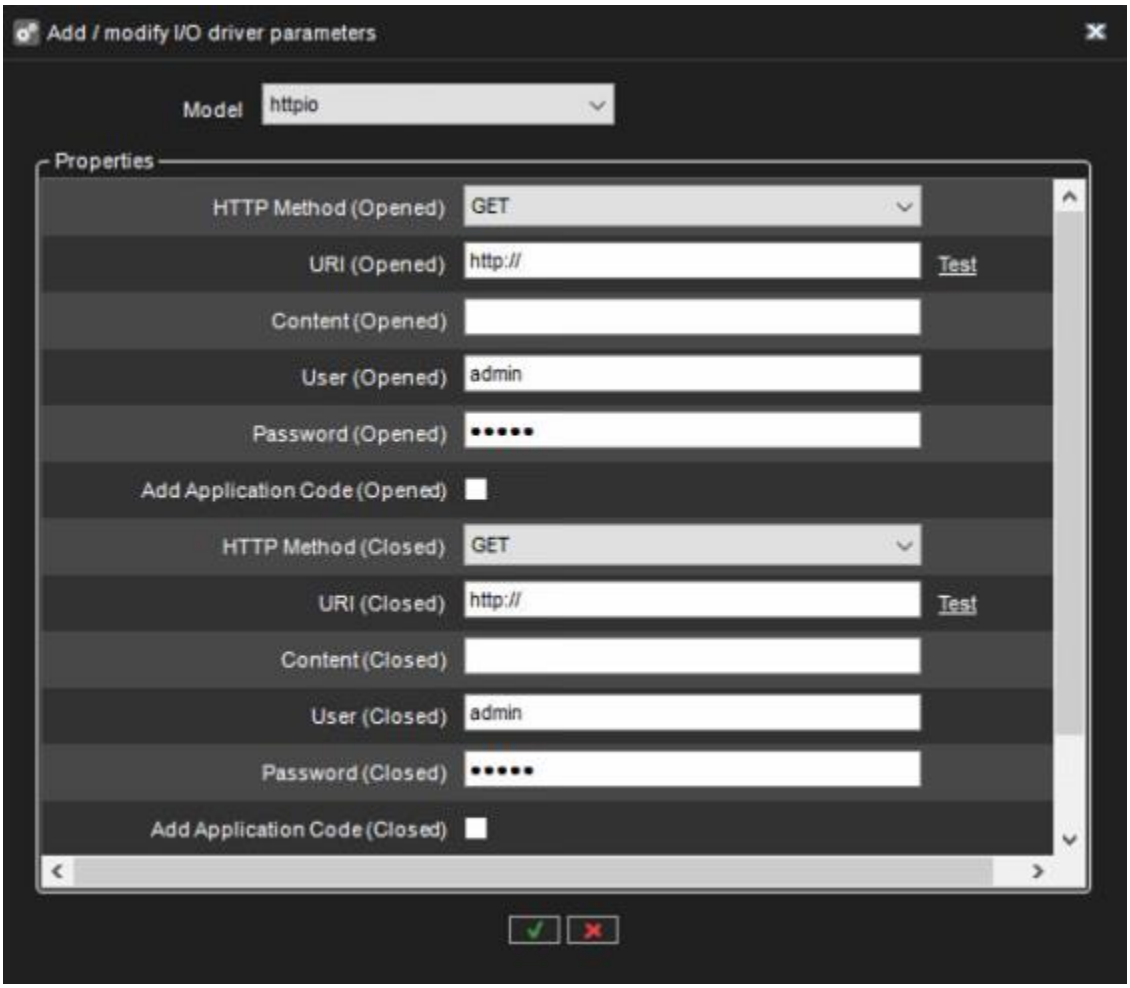
Content(Closed)

User(Closed)

Password(Closed)

Authentication

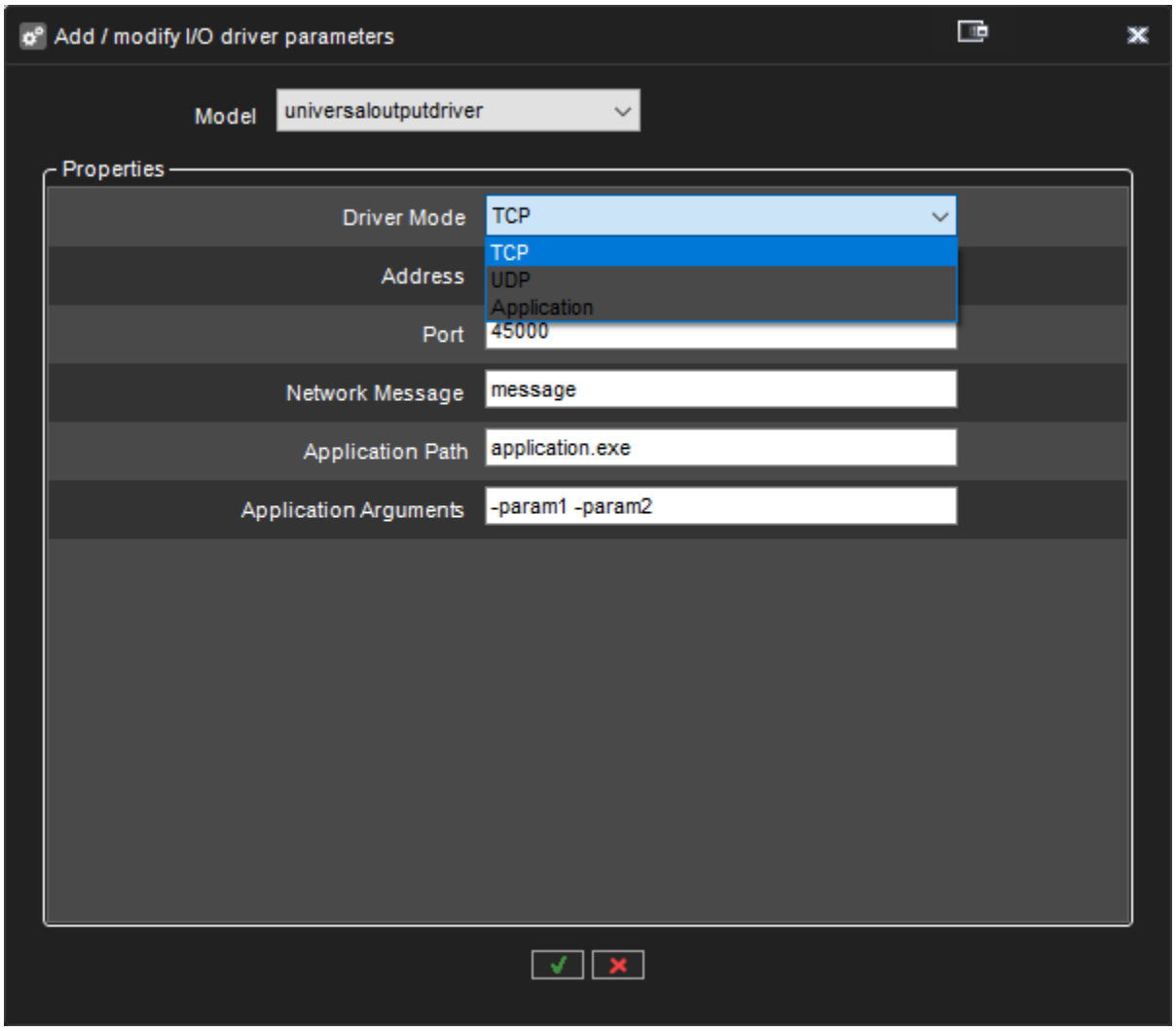
- BASIC
- DIGEST



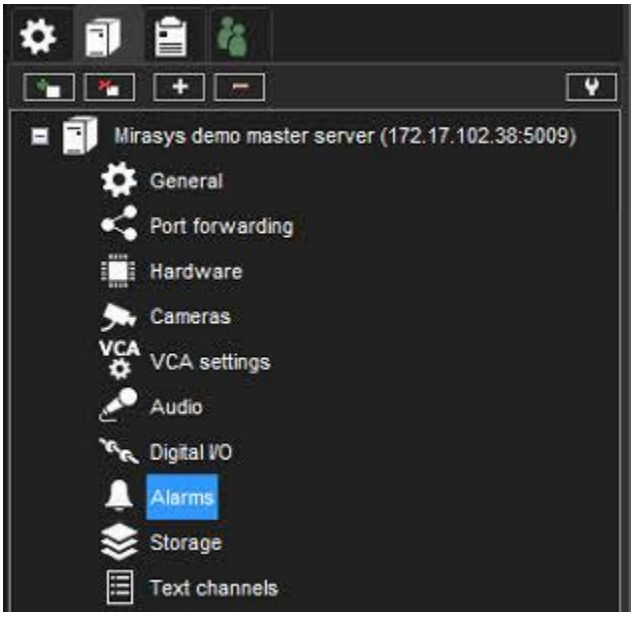
9.9.7 UniversalOutputDriver

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.


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

9.10 Alarm (VMS-server)



9.10.1 Alarmeinstellungen

Die Alarmmanagement-Tools ermöglichen die Erstellung serverspezifischer Alarme basierend auf verschiedenen Auslösern basierend auf Bewegung, Schallpegel oder bestimmten Textdatenauslösern.

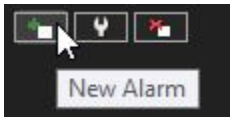
Darüber hinaus können die Trigger kundenspezifische Trigger von Drittanbietern beinhalten.

Alarme können über den Bildschirm **Alarme** auf der Registerkarte **VMS-Server** erstellt, bearbeitet und gelöscht werden.

9.10.2 Hinzufügen eines neuen Weckers

9.10.2.1 Allgemein

1. Klicken Sie auf Neuer Alarm

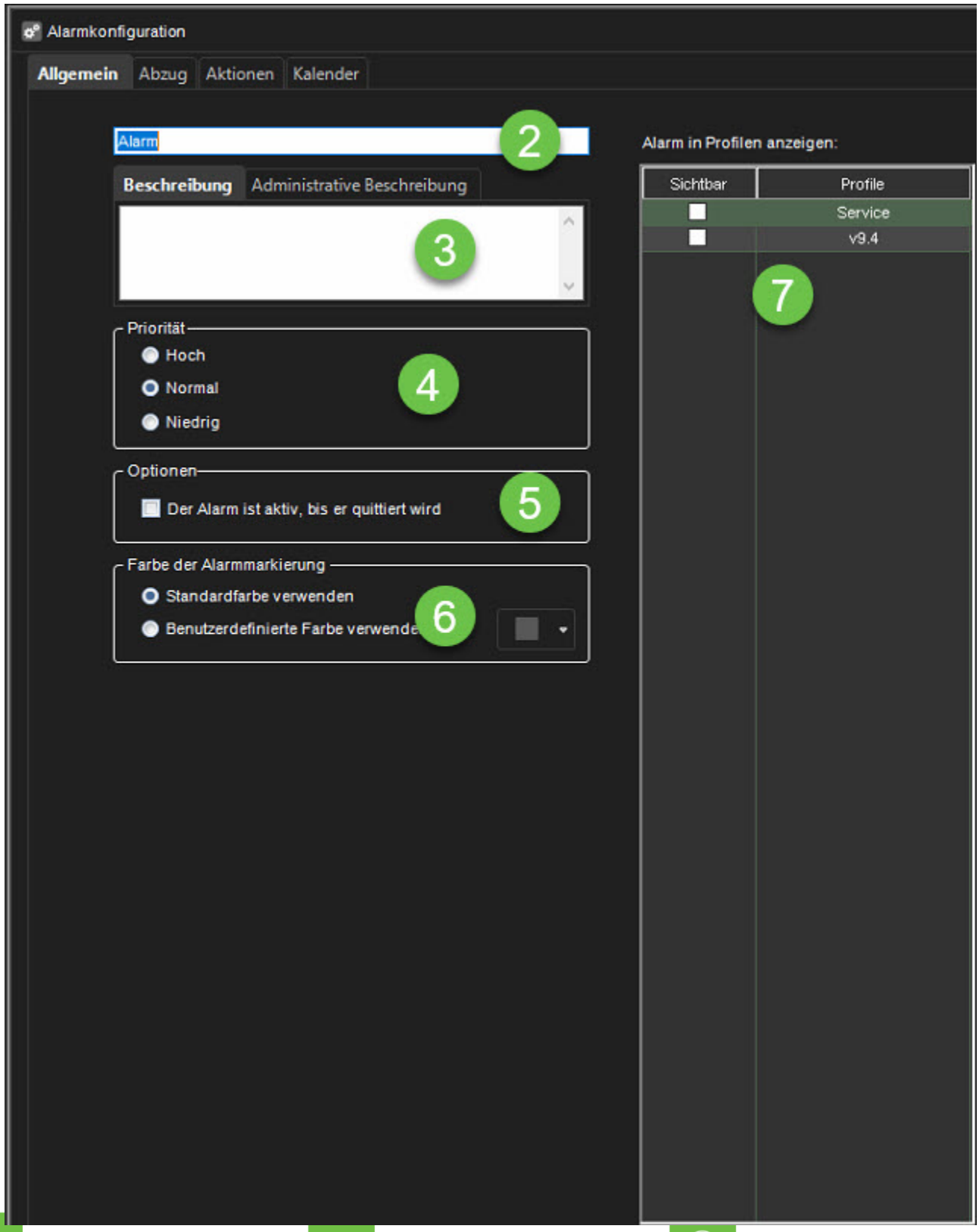


in der linken unteren Ecke des Bildschirms Alarme.

2. Geben Sie den Namen des neuen Alarms in das Feld **Name** ein.
3. Geben Sie die **Beschreibung** und **Verwaltungsbeschreibung** des neuen Alarms in die entsprechenden Felder unter dem Feld **Name** ein.
4. 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.
5. 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.
6. **Alarm-Hervorhebungsfarbe** ermöglicht Administratoren, eine benutzerdefinierte Farbe für jeden Alarm separat zu definieren.
7. Wählen Sie im Menü **Alarme in Profilen anzeigen** die Profile aus, in denen der Alarm verwendet werden soll. *Notiz: Alarme können auch über die Registerkarte **Profile** zu Profilen hinzugefügt werden.*

MIRASYS
DEEP VISION DATA COMPANY

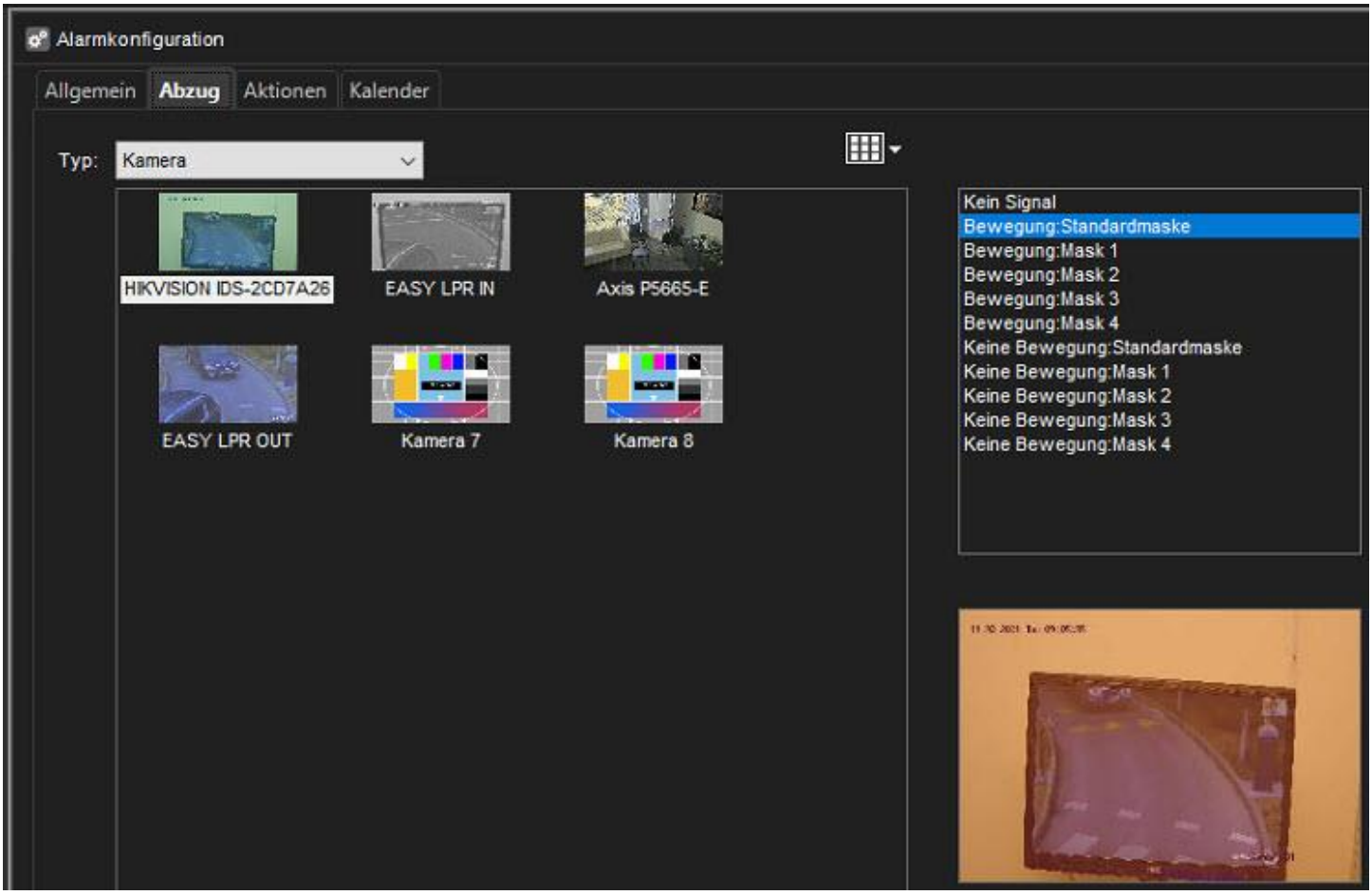
Admin Guide V9.8.0



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

9.10.2.2 Absuz

8. Öffnen Sie die Registerkarte **Trigger**. Die Registerkarte **Trigger** wird verwendet, um die Trigger zu definieren, die das Alarmereignis starten.



9. Wählen Sie den Triggertyp aus dem Dropdown-Menü **Type** aus.

- Kamera
- Audio
- Metadaten
- Textdaten
- Digitale Eingabe

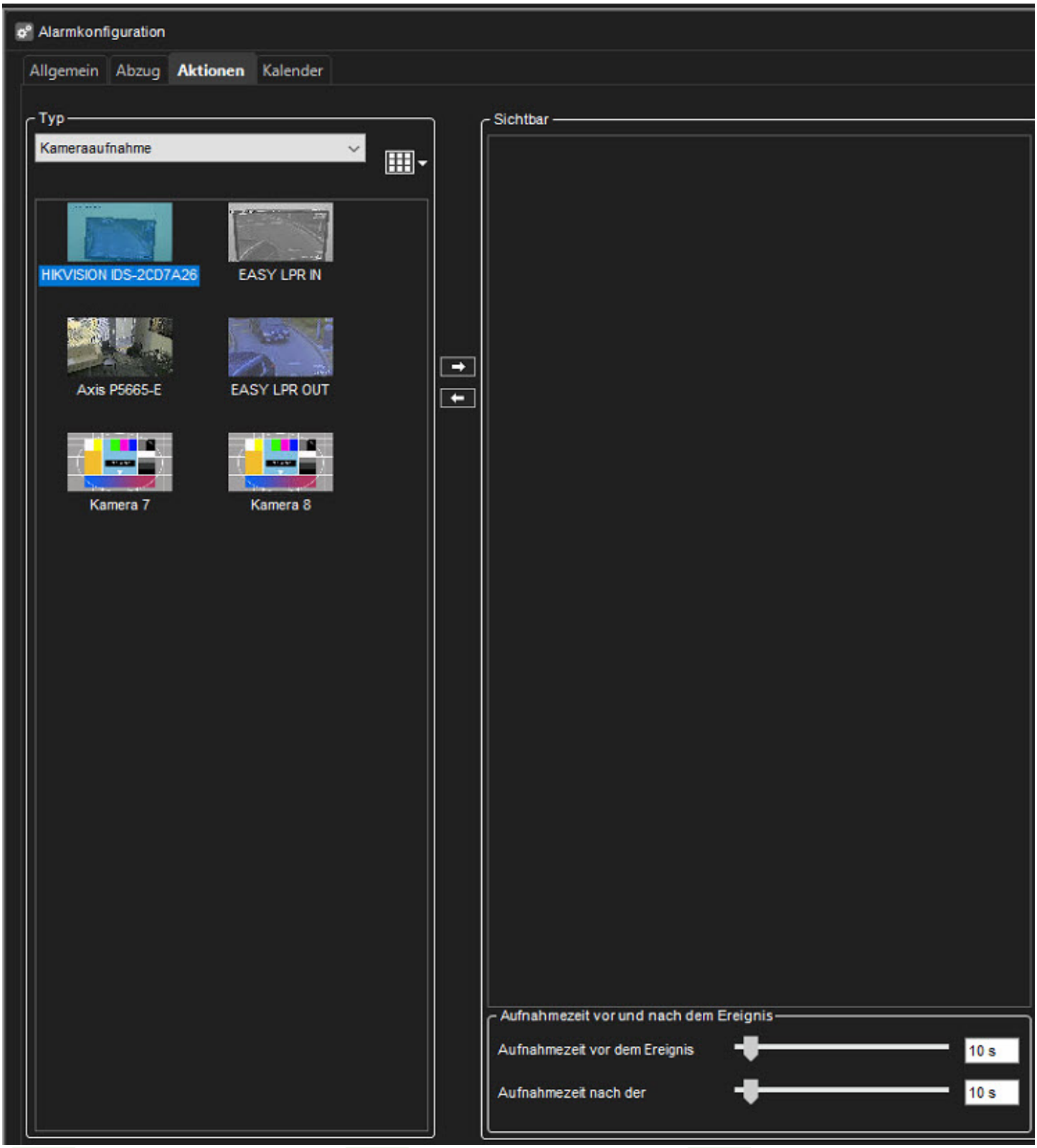
10. Wählen Sie das Gerät, das den Alarm auslösen soll, aus der Geräteliste unter dem Dropdown-Menü **Typ** aus.

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.

9.10.2.3 Aktionen

12. Öffnen Sie die Registerkarte **Aktionen**. Die Registerkarte **Aktionen** wird verwendet, um die Aktionen zu definieren, die der Alarm ausführt, wenn er ausgelöst wird.


Alarmkonfiguration
Allgemein
Abzug
Aktionen
Kalender
Typ
Kameraaufnahme
HIKVISION IDS-2CD7A26
EASY LPR IN
Axis P5665-E
EASY LPR OUT
Kamera 7
Kamera 8
Sichtbar
Aufnahmezeit vor und nach dem Ereignis
Aufnahmezeit vor dem Ereignis
10 s
Aufnahmezeit nach der
10 s

13. Wählen Sie den Aktionstyp aus dem Dropdown-Menü **Typ** aus. Der Aktionstyp definiert die grundlegende Funktionalität des Alarms.

9.10.2.4 Aktionstypen und Einstellungen

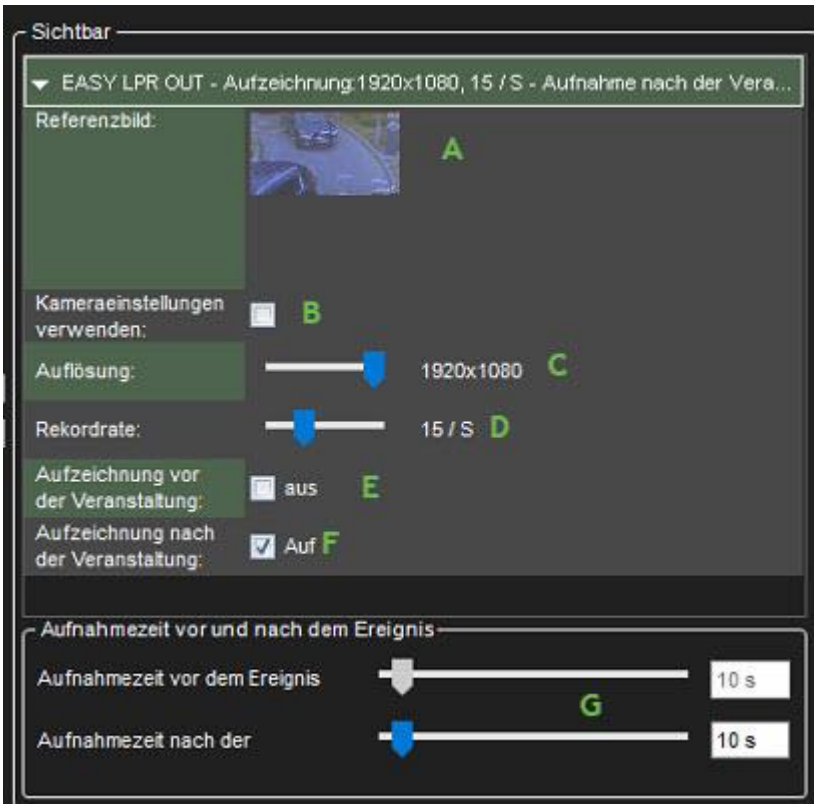
Die folgende Liste enthält die Standardaktionstypen und ihre Parameter. Einige der oben aufgeführten Aktionstypen sind möglicherweise nicht auf allen Systemen verfügbar.

Notiz: *Zusätzlich zu den Standardaktionen kann das System Alarmaktionen enthalten, die über Module von Drittanbietern installiert werden.*

9.10.2.4.1 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.



Die Aktion umfasst die folgenden Felder und Parameter:

A) Referenzbild. Dieses statische Feld enthält das Referenzbild (Image) der Kamera.

B) Kameraeinstellungen verwenden. Durch Aktivieren dieses Kontrollkästchens wird die Alarmaufzeichnung mit der kameraspezifischen Einstellung für Auflösung und Aufzeichnungsrate durchgeführt.

C) Auflösung. Verwenden Sie den Schieberegler, um die Auflösung einer IP-Kamera während der Alarmaufzeichnung zu ändern. Der Schieberegler ist nur für IP-Kameras aktiv.

D) 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.

E)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.

F)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.

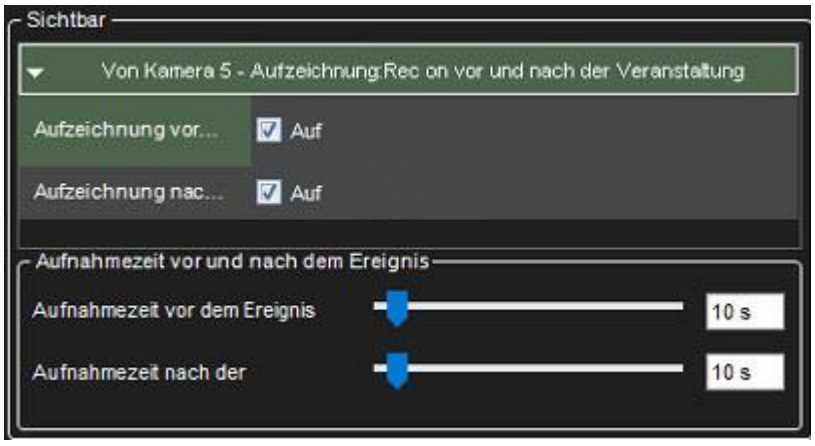
G)Aufnahmezeit vor und nach dem Ereignis Diese Schieberegler können verwendet werden, um die Aufzeichnungsdauer vor und nach dem Ereignis für die Aktion einzustellen. Die Schieberegler sind nur aktiv, wenn die Aufzeichnung vor und/oder nach dem Ereignis aktiviert wurde.

Anmerkung *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.*

9.10.2.4.2 Audio 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:

E)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.

F)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.

G)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.

Notiz: *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.*

9.10.2.4.3 Digitaler 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.

Notiz: *Auch wenn die Schieberegler* ***Aufnahmezeit vor und nach dem Ereignis*** *für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.*

9.10.2.4.4 PTZ (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:

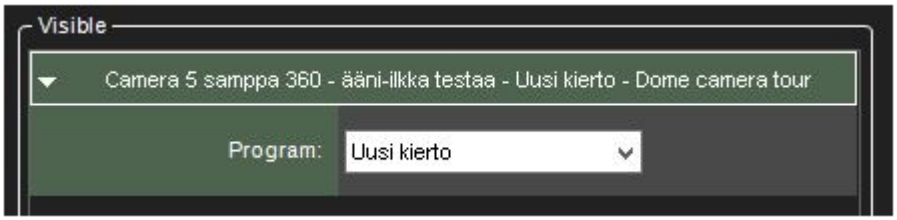
- **Position** Verwenden Sie das Dropdown-Menü, um die voreingestellte Position auszuwählen, in die sich die PTZ-Kamera während des Alarms bewegt.

Notiz: *Auch wenn die Schieberegler* ***Aufnahmezeit vor und nach dem Ereignis*** *für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.*

9.10.2.4.5 PTZ (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.



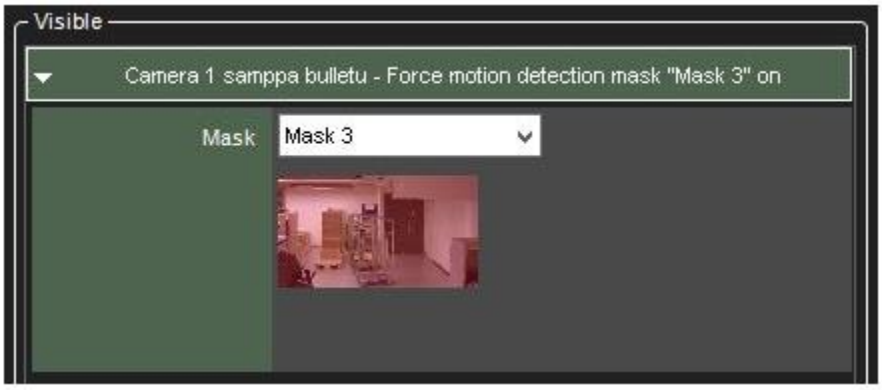
Die Aktion umfasst die folgenden Felder und Parameter:

- **Program** Verwenden Sie das Dropdown-Menü, um die PTZ-Kameratour auszuwählen, die beginnt, wenn der Alarm ausgelöst wird.

Notiz *Auch wenn die Schieberegler* ***Aufnahmezeit vor und nach dem Ereignis*** *für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.*

9.10.2.4.6 Stellen 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:

- **Masken** Verwenden Sie das Dropdown-Menü, um die Bewegungserkennungsmaske auszuwählen, die während des Alarms verwendet wird.

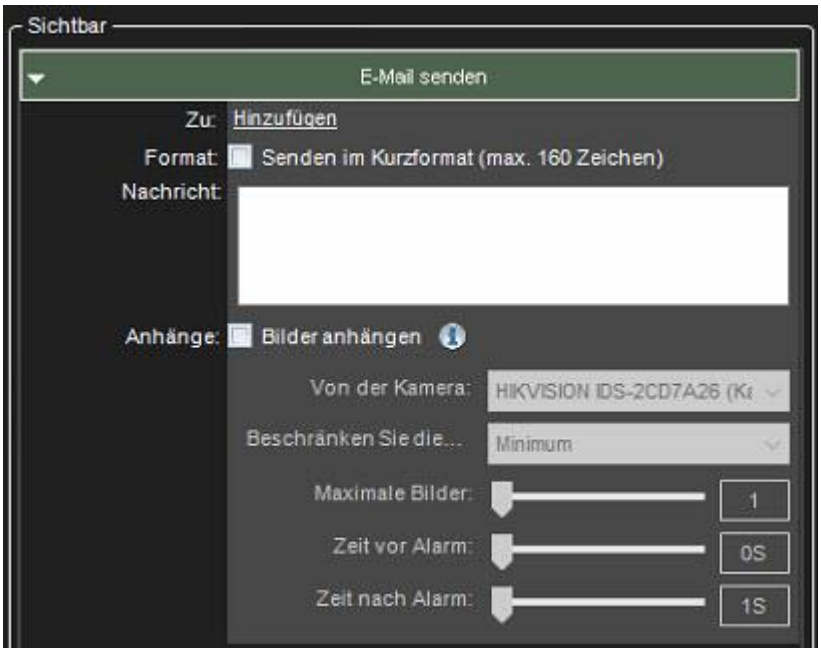
Notiz: *Auch wenn die Schieberegler 2Vor- und Nachaufzeichnungsdauer2 für den Aktionstyp angezeigt werden, haben sie keinen Einfluss auf die Funktionalität der Aktion.*

9.10.2.4.7 E-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.

Notiz:

- 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:

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).

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.

Notiz:

- *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.

9.10.2.4.8 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.

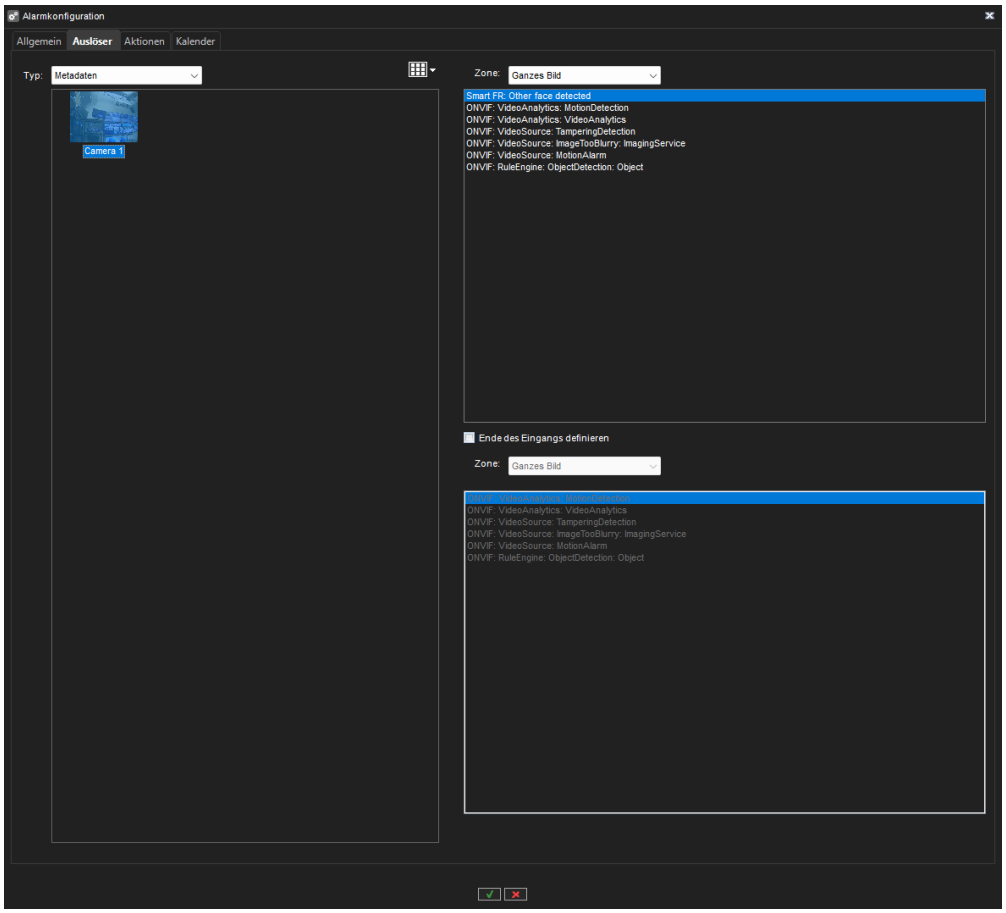
9.10.2.5 ONVIF profile M

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.

9.10.2.5.1 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.



9.10.2.5.2 Einen ONVIF-Alarm auslösen

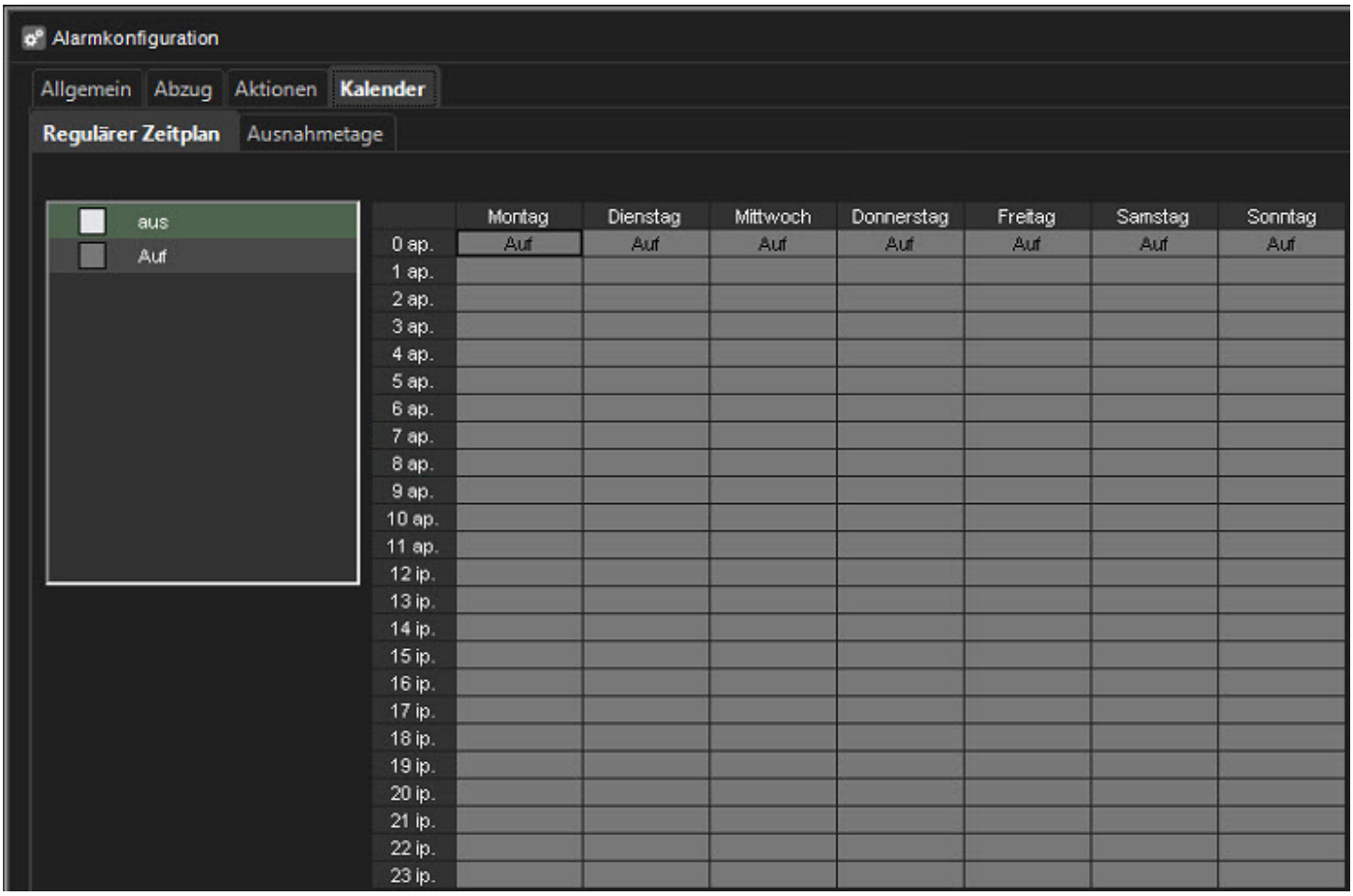
Die Gerätealarme/-auslöser selbst sollten über die Webschnittstelle des Geräts konfiguriert werden, da der System Manager keine Benutzeroberfläche für ihre Konfiguration hat. Diese Konfiguration sollte durchgeführt werden, bevor Sie das Gerät zu VMS hinzufügen, oder die Gerätefunktionen sollten im System 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.

9.10.2.6 Kalender

1. Definieren Sie das, wenn der Alarm aktiv ist
2. Klicken **OK**



9.10.3 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.

9.10.3.1 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.

9.10.3.2 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.

9.10.3.3 So 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.

9.10.3.4 So 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

9.10.3.5 So 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.

9.10.4 Löschen eines Alarms

9.10.4.1 Deleting an Alarm

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. Der Alarm wird aus dem System gelöscht.

9.11 Lagerung

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.

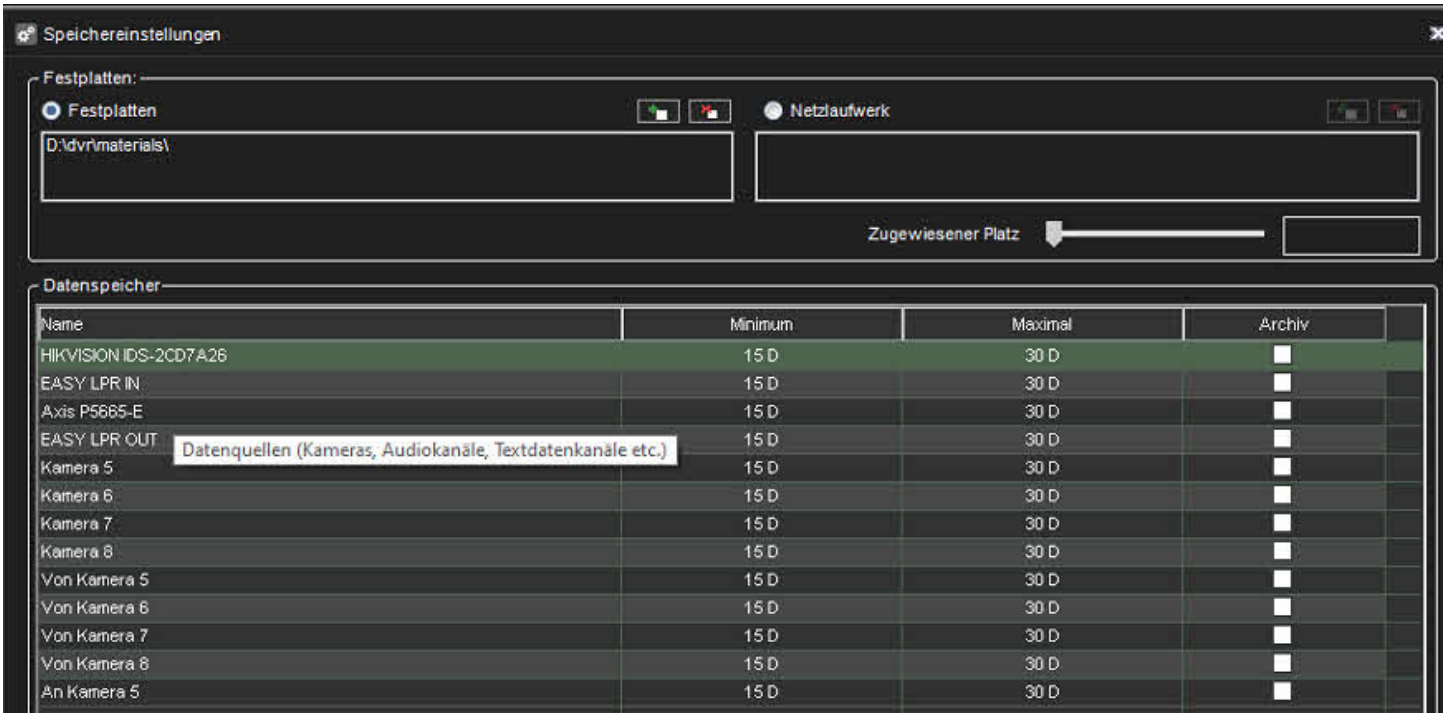
Die Speichereinstellungen werden auch verwendet, um die automatische Archivierungsfunktion zu konfigurieren, die es ermöglicht, täglich oder wöchentlich Sicherungskopien der serverspezifischen Video-, Audio- und Textdaten zu erstellen.

Video-, Audio-, Textdaten und Alarmaufzeichnungen werden aufbewahrt, bis ihr definiertes **Maximum**-Datum überschritten oder der zugewiesene Speicherplatz erschöpft ist.

9.11.1 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.

9.11.1.1 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**.

9.11.1.2 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.

9.11.1.3 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.

9.11.2 Speichereinstellungen für Video-, Audio- und Textdaten

9.11.2.1 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.

9.11.2.2 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.*

9.11.2.3 Alarmgrenzen

9.11.2.3.1 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.

9.11.2.3.2 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.

9.11.2.3.2.1 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.

9.11.2.3.2.2 % 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.

9.11.3 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.*

9.11.4 Archivierung

Sie können das System so einstellen, dass Video-, Audio- und Textdaten täglich oder wöchentlich automatisch archiviert werden.

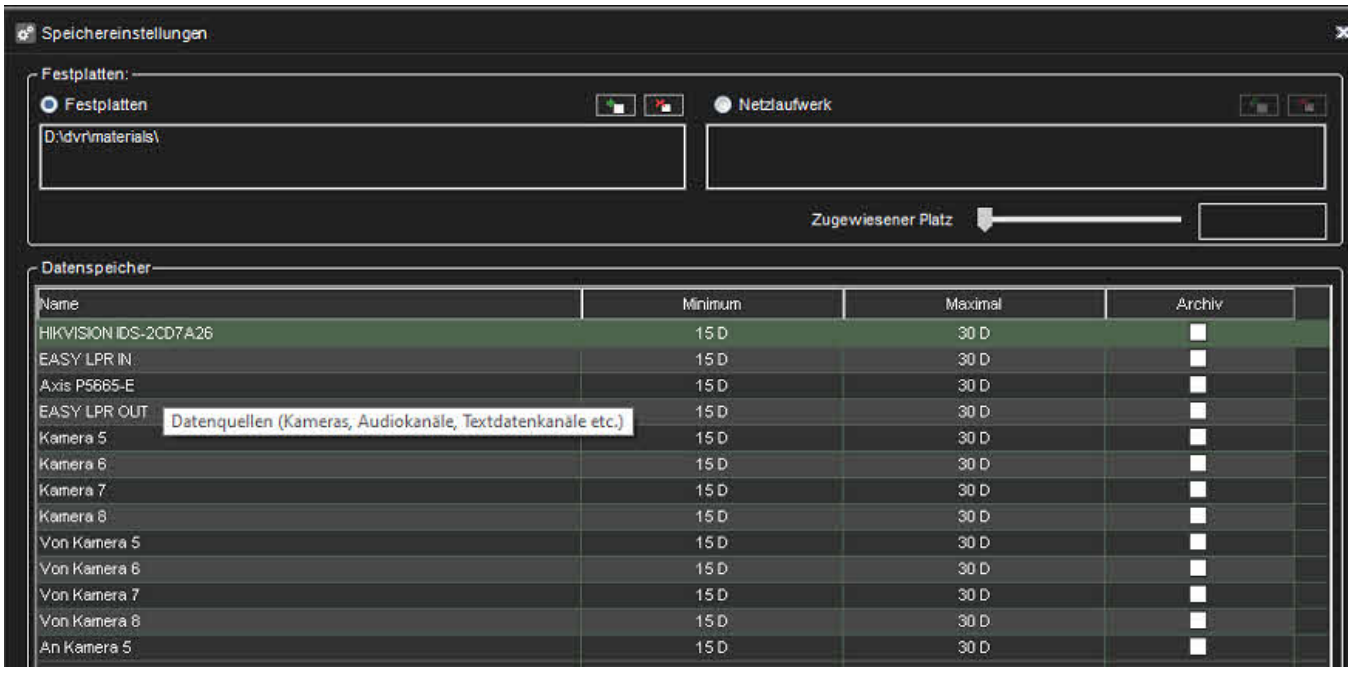
Die Archivdateien können automatisch auf den Festplatten des Servers oder einem Netzlaufwerk erstellt werden.

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.*

9.11.4.1 So legen Sie einen automatischen Archivierungszeitplan fest:

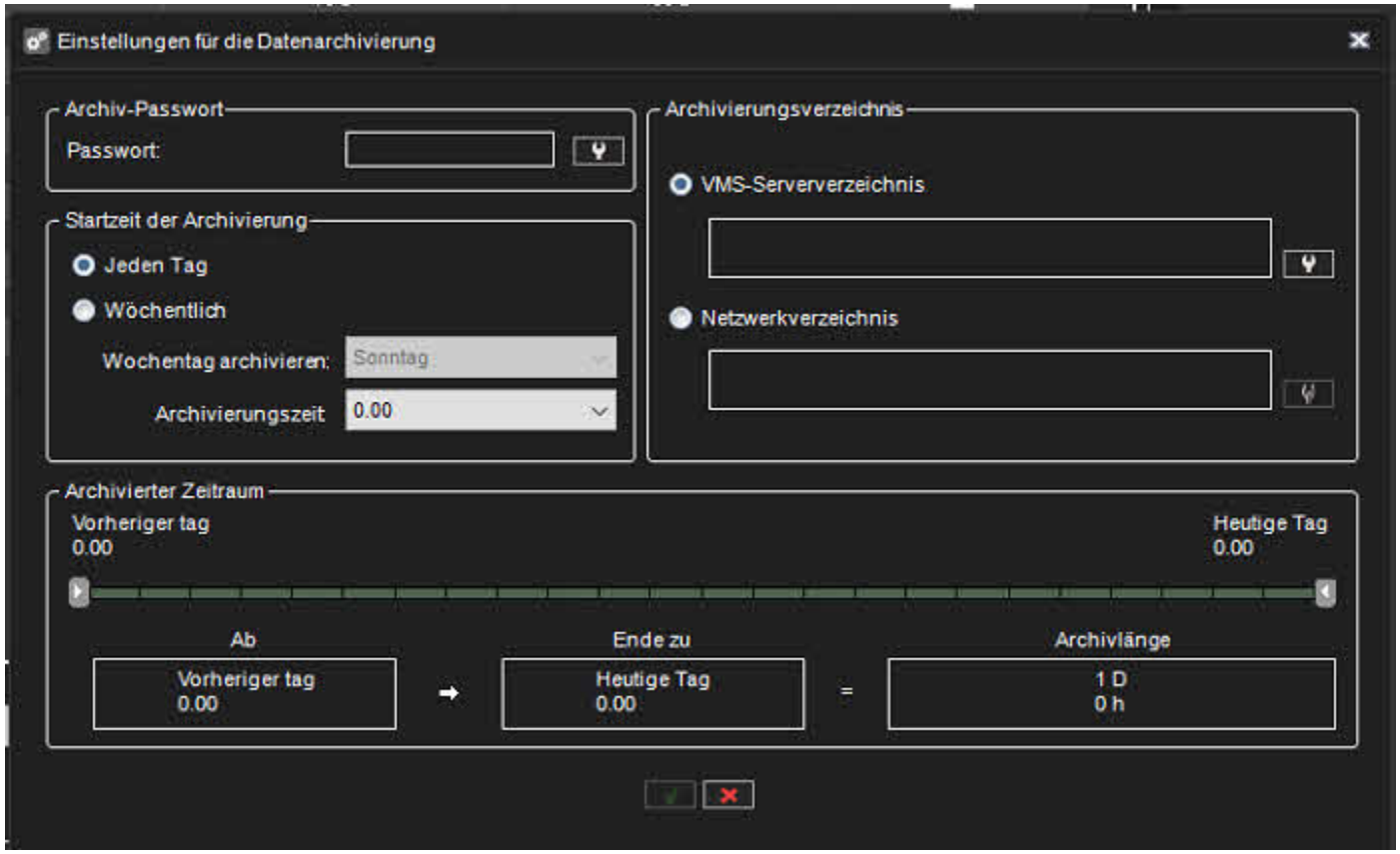
1. Klicken Sie im Bereich **Datenspeicherung** auf die Geräte, die Sie in den automatischen Archivierungsprozess einbeziehen möchten.
   Hinweis Wählen Sie benachbarte Geräte oder Ordner aus, halten Sie die UMSCHALTTASTE gedrückt und klicken Sie dann auf das erste und letzte Gerät, das Sie auswählen 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



9.11.5 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.

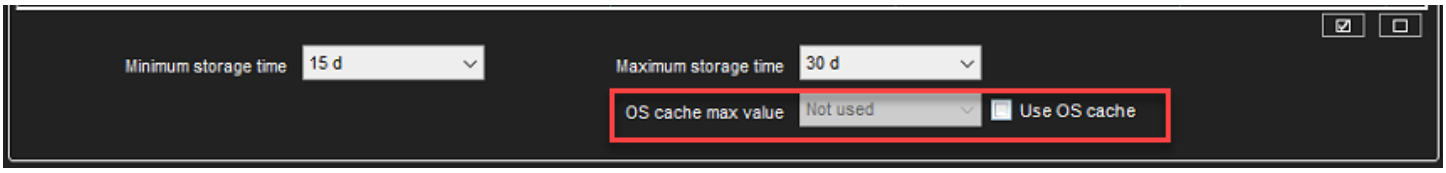
Der letzte hilft, mit instabiler Last auf der Festplatte umzugehen und die am häufigsten verwendeten Teile der Daten zwischenzuspeichern.

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.



9.12 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.

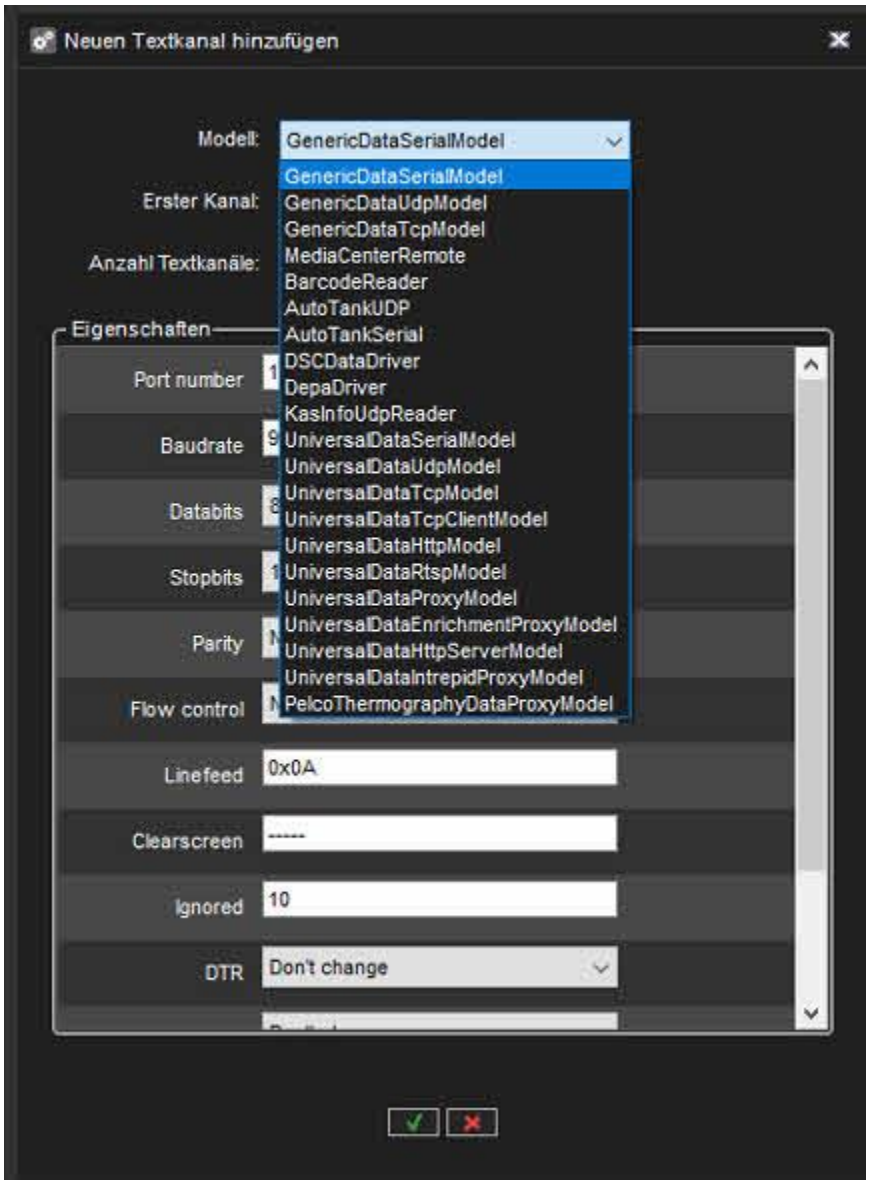
Ein zusätzliches Dokument für UniversalData-Treiber kann von unserem Extranet heruntergeladen werden oder wenden Sie sich an den Support. Dieser Treiber eröffnet endlose Möglichkeiten für die Integration in Systeme von Drittanbietern.

9.12.1 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.

9.12.2 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.*

9.12.3 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.*

10 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 Master-Servers vorgibt.

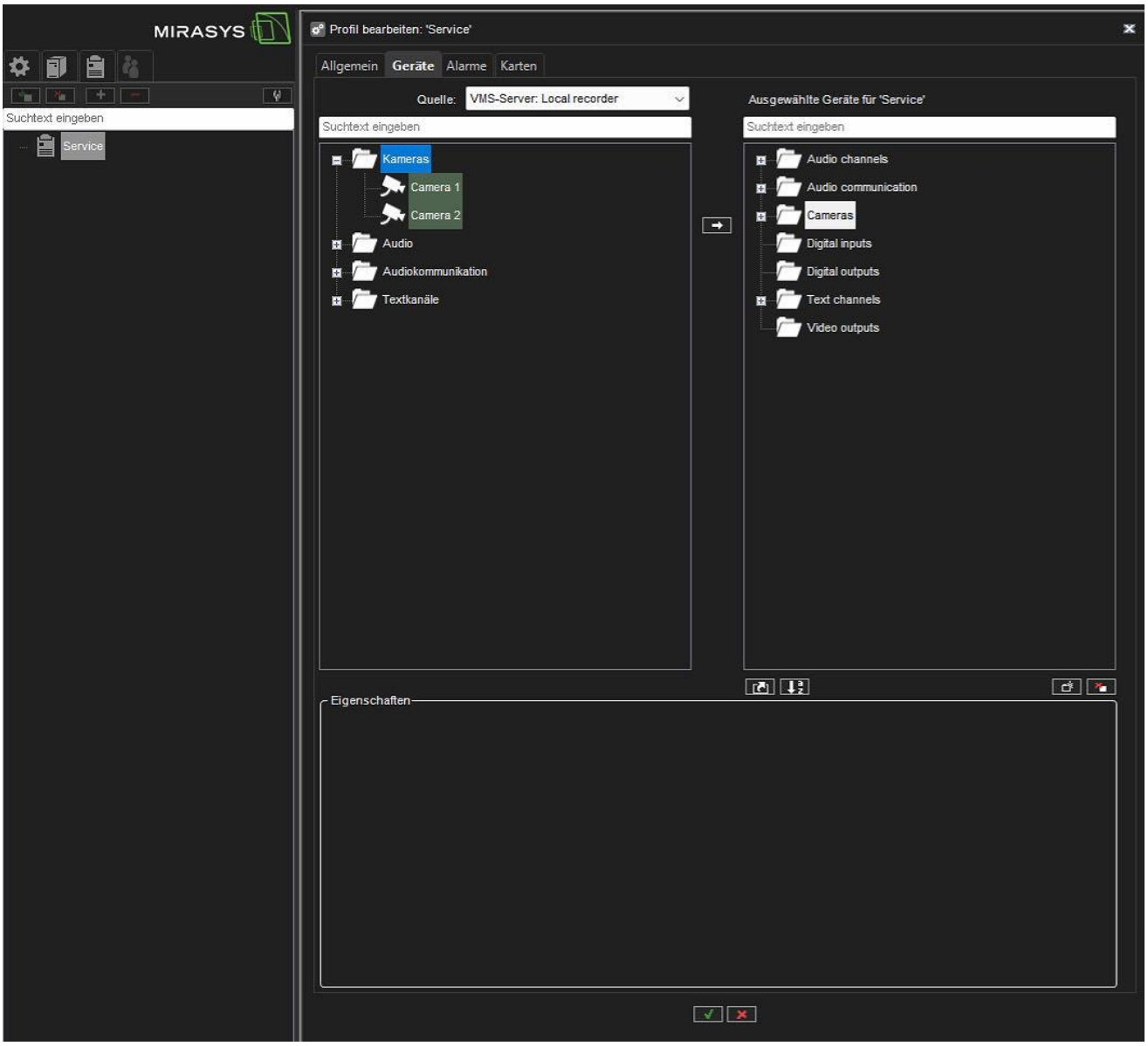
Die Geräte sind nach Gerätetyp gruppiert. Beispielsweise befinden sich alle Kameras in einer Gruppe und alle Audiokanäle in einer anderen Gruppe.

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.



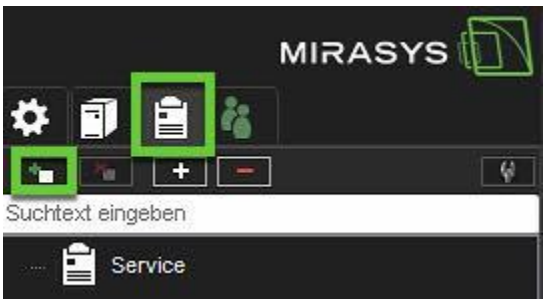
Sie können das Standardprofil als solches verwenden oder frei bearbeiten, zum Beispiel Kameras am genauen Standort gruppieren. Oder Sie können neue Profile hinzufügen. Ein Profil kann Geräte von verschiedenen Servern enthalten.

Sie können einem Profil bis zu 2.000 Gruppen und Geräte hinzufügen. Außerdem können Sie die Geräte beliebig in Gruppen einteilen.

10.1 Erstellen eines kundenspezifischen Profils

10.1.1 So fügen Sie ein Profil hinzu:

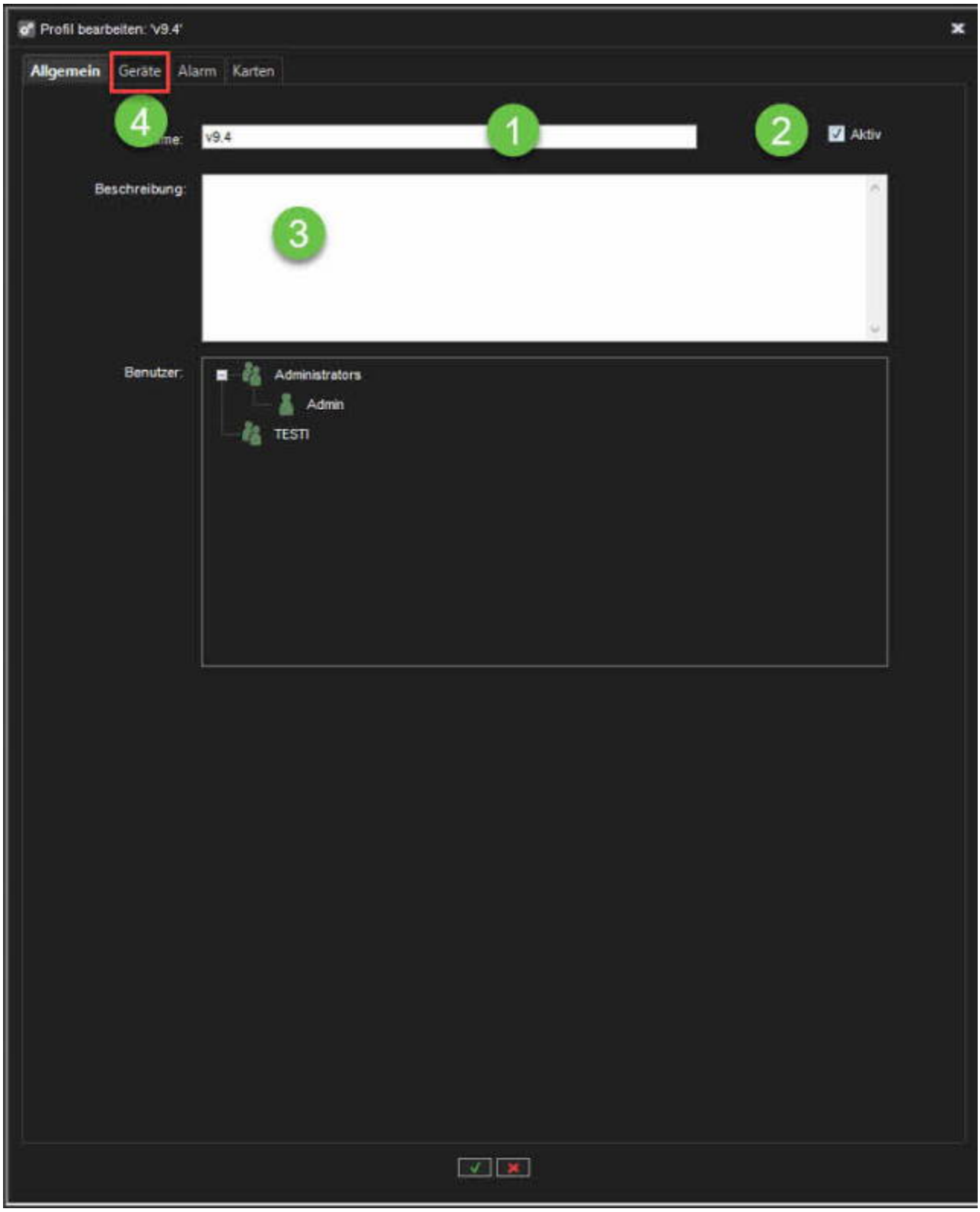
1. Klicken Sie auf **Profil hinzufügen**



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
DEEP VISION DATA COMPANY

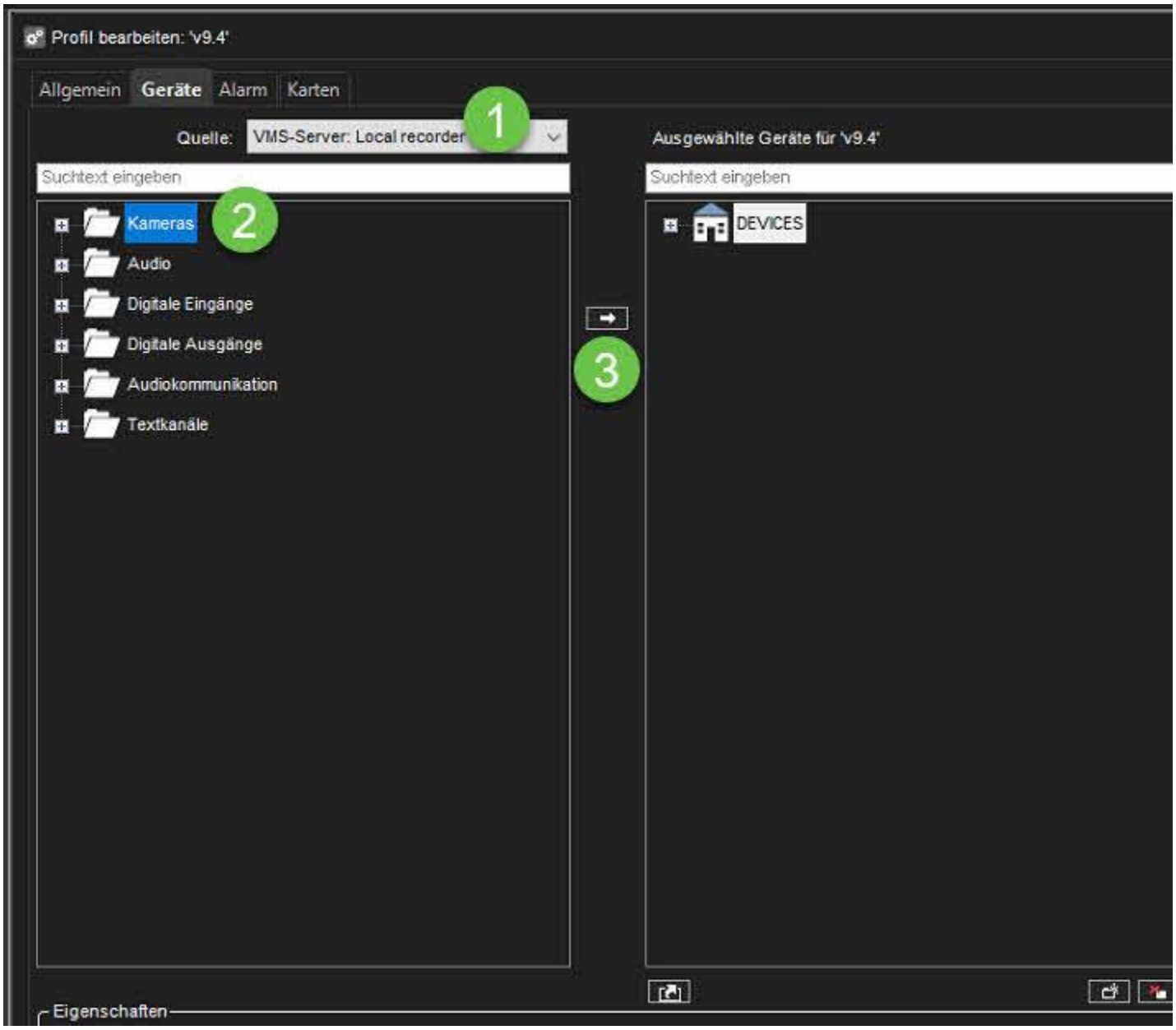
Admin Guide V9.8.0



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

10.1.1.1 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**



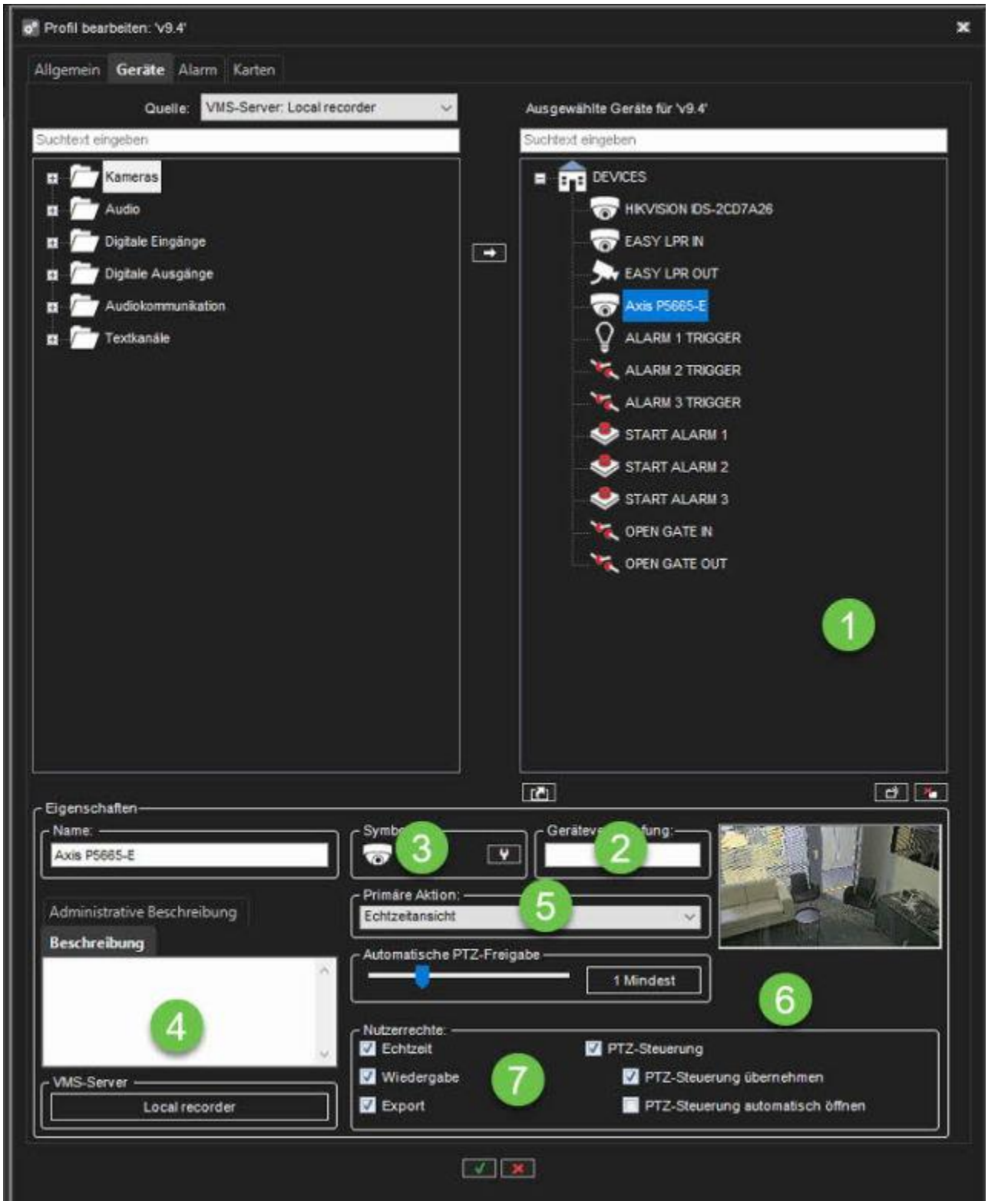
10.1.1.2 Ausgewählte Geräteeigenschaften

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

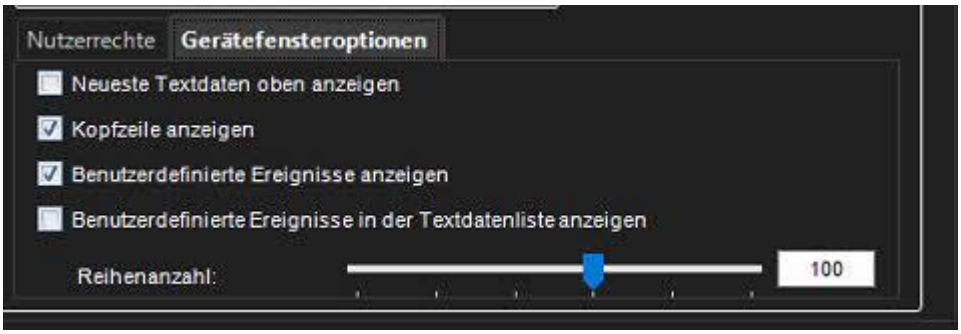
MIRASYS
DEEP VISION DATA COMPANY

Admin Guide V9.8.0



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

10.1.1.3 Optionen des Gerätefensters für Textkanäle



In den Gerätefensteroptionen können Sie auswählen, wie Benutzern Textdaten angezeigt werden. Diese Optionen sind verfügbar:

10.1.1.3.1 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.

10.1.1.3.2 Kopfzeile anzeigen

Wählen Sie diese Option, um die vom Textdatenerfassungstreiber angegebenen Identifikationsdaten anzuzeigen.

10.1.1.3.3 Benutzerdefinierte Ereignisse anzeigen

Wählen Sie diese Option aus, um vom Textdatenerfassungstreiber festgelegte benutzerdefinierte Ereignisse anzuzeigen.

10.1.1.3.4 Benutzerdefinierte Ereignisse in der Textdatenliste anzeigen

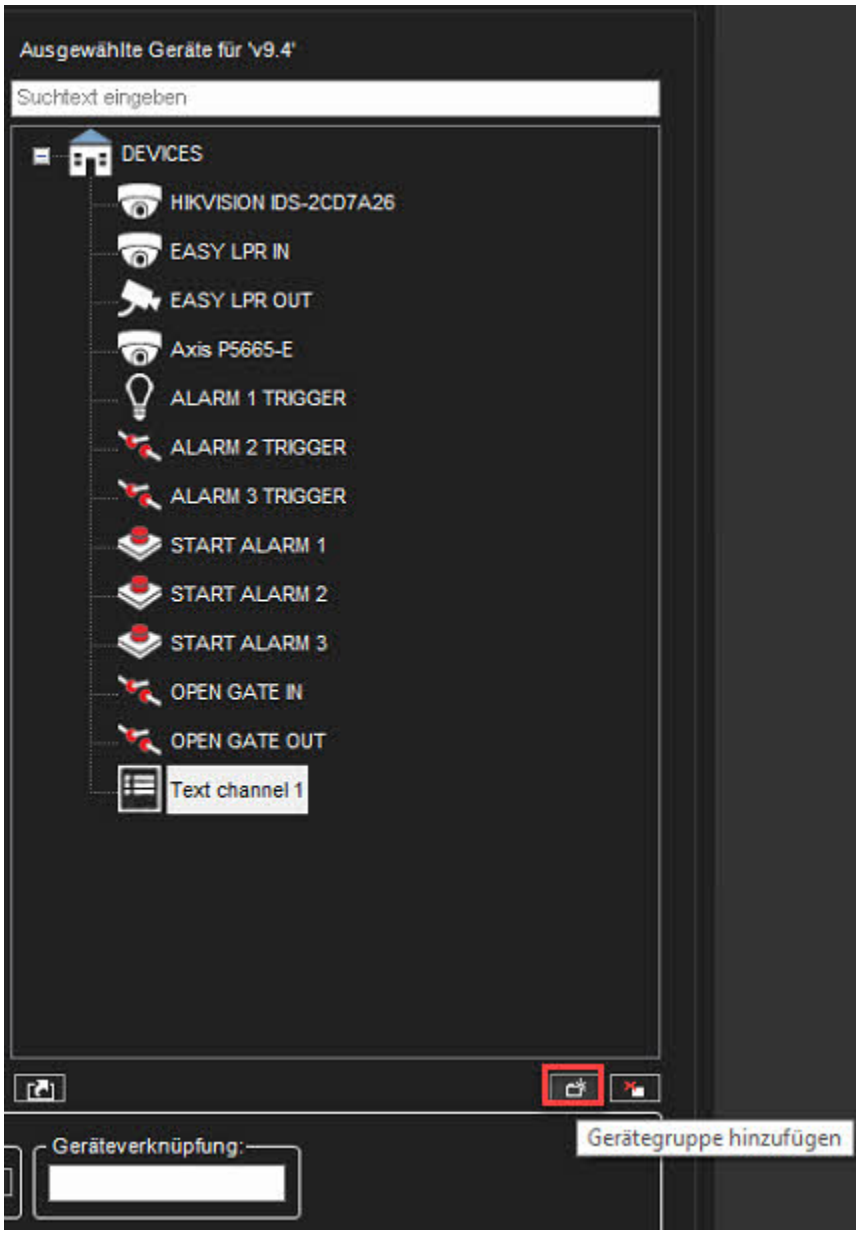
Wählen Sie diese Option, um benutzerdefinierte Ereignisse in der Textdatenliste (anstelle der benutzerdefinierten Ereignisliste) anzuzeigen.

10.1.1.3.5 Die Anzahl der Zeilen

Geben Sie die Anzahl der Zeilen an, die höchstens in der Textdatenliste angezeigt werden.

10.1.1.4 Hinzufügen von Gerätegruppen zur Liste des ausgewählten Geräts

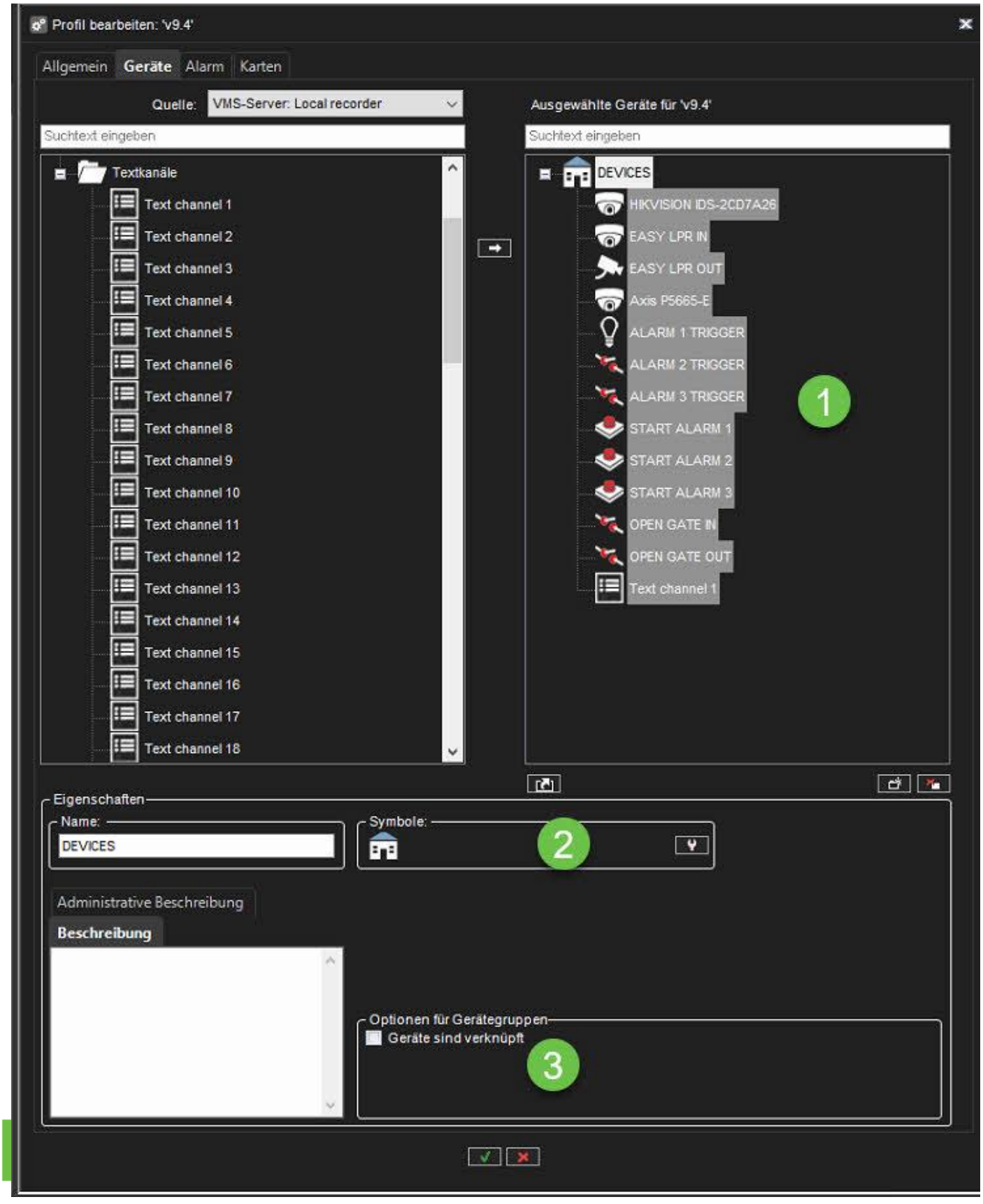
1. Klicken Sie unter dem Bereich **Ausgewählte Geräte** auf **Gerätegruppe hinzufügen**. Eine neue Gerätegruppe wird angezeigt.



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*

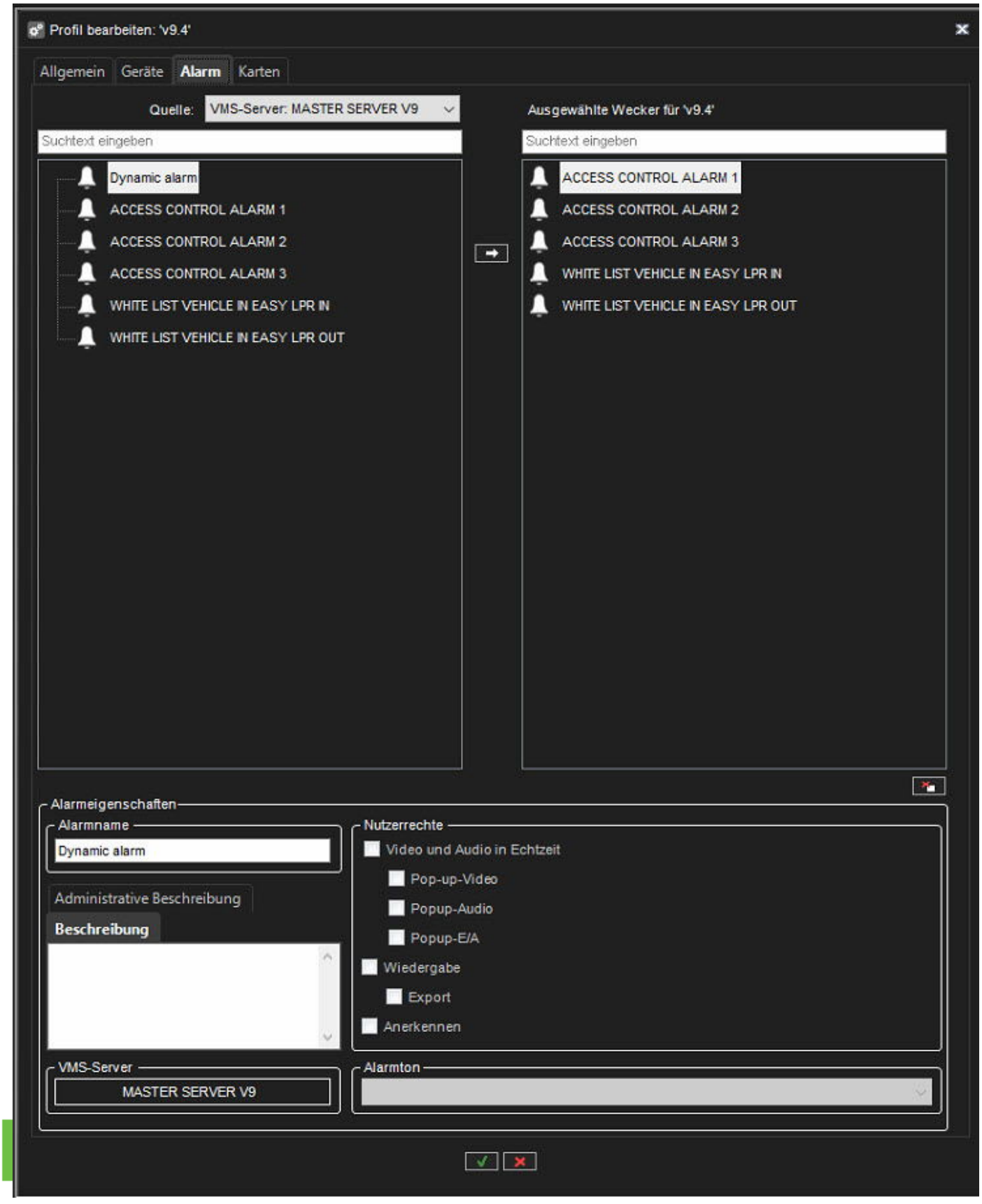
1. Klicken Sie auf die Gerätegruppe und geben Sie einen Namen dafür ein

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).


Profil bearbeiten: 'v9.4'
Allgemein
Geräte
Alarm
Karten
Quelle:
VMS-Server: Local recorder
Suchtext eingeben
Textkanäle
Text channel 1
Text channel 2
Text channel 3
Text channel 4
Text channel 5
Text channel 6
Text channel 7
Text channel 8
Text channel 9
Text channel 10
Text channel 11
Text channel 12
Text channel 13
Text channel 14
Text channel 15
Text channel 16
Text channel 17
Text channel 18
Ausgewählte Geräte für 'v9.4'
Suchtext eingeben
DEVICES
HIKVISION IDS-2CD7A26
EASY LPR IN
EASY LPR OUT
Axis P5665-E
ALARM 1 TRIGGER
ALARM 2 TRIGGER
ALARM 3 TRIGGER
START ALARM 1
START ALARM 2
START ALARM 3
OPEN GATE IN
OPEN GATE OUT
Text channel 1
1
Eigenschaften
Name:
DEVICES
Symbole:
2
Administrative Beschreibung
Beschreibung
Optionen für Gerätegruppen
Geräte sind verknüpft
3

10.1.2 Alarm

10.1.2.1 Bearbeiten profilspezifischer Alarmeinstellungen


Profil bearbeiten: 'v9.4'
Allgemein
Geräte
Alarm
Karten
Quelle:
VMS-Server: MASTER SERVER V9
Suchtext eingeben
Dynamic alarm
ACCESS CONTROL ALARM 1
ACCESS CONTROL ALARM 2
ACCESS CONTROL ALARM 3
WHITE LIST VEHICLE IN EASY LPR IN
WHITE LIST VEHICLE IN EASY LPR OUT
Ausgewählte Wecker für 'v9.4'
Suchtext eingeben
ACCESS CONTROL ALARM 1
ACCESS CONTROL ALARM 2
ACCESS CONTROL ALARM 3
WHITE LIST VEHICLE IN EASY LPR IN
WHITE LIST VEHICLE IN EASY LPR OUT
Alarmeigenschaften
Alarmname
Dynamic alarm
Administrative Beschreibung
Beschreibung
Nutzerrechte
Video und Audio in Echtzeit
Pop-up-Video
Popup-Audio
Popup-E/A
Wiedergabe
Export
Anerkennen
VMS-Server
MASTER SERVER V9
Alarmton

Auf der Registerkarte **Alarme** können Sie die Alarme auswählen, die Sie in ein Profil aufnehmen möchten, und die profilspezifischen Benutzerrechte der Alarme bearbeiten.

10.1.2.2 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.*

10.1.2.3 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**.

10.1.2.3.1 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.

10.1.3 Karten

10.1.3.1 Hinzufügen von Karten zu Profilen

10.1.3.1.1 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. 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.

10.1.3.1.2 So entfernen Sie eine Sitemap:

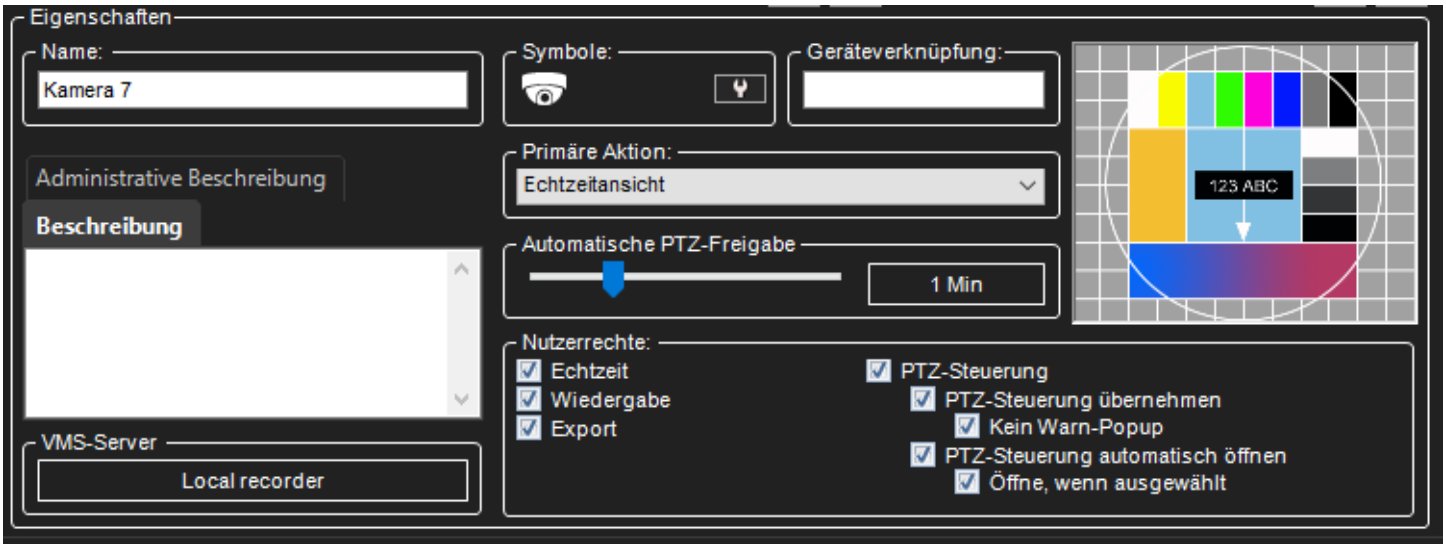
- Zeigen Sie die Karte an, die Sie entfernen möchten, und klicken Sie auf **Karte entfernen**

10.1.3.1.3 So entfernen Sie ein Symbol von der Karte:

- Wählen Sie das Symbol aus und klicken Sie auf **Entfernen**

10.2 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 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.

11.1 Benutzer abmelden

Wenn Sie über Administratorrechte verfügen, können Sie einen Benutzer vom Spotter-Programm abmelden.

11.2 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.

11.3 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.

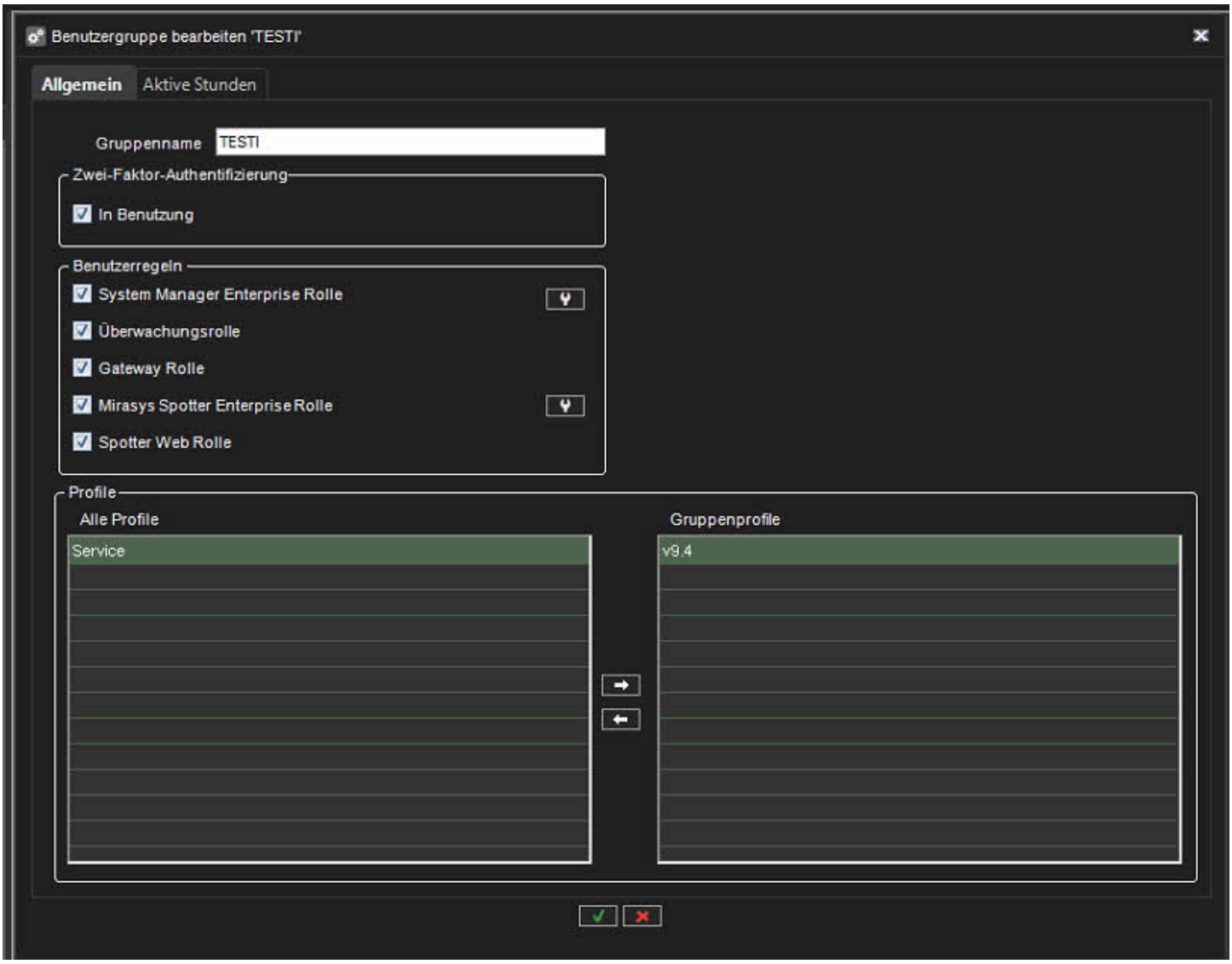
11.4 Benutzergruppe

11.4.1 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.

11.4.2 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



11.4.2.1 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.

11.4.2.1.1 System

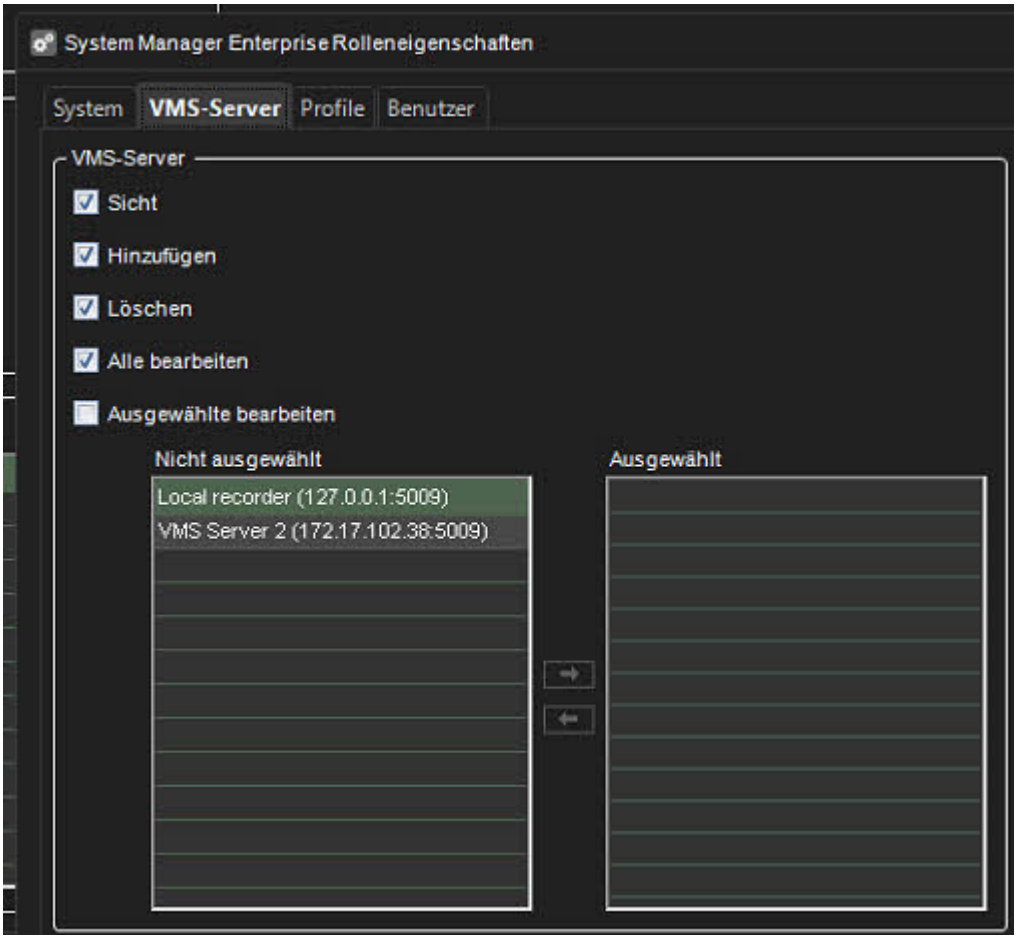
Die System-Tab-Berechtigungen können für eine Benutzergruppe aktiviert oder deaktiviert werden, indem beispielsweise die Systemeinstellungen deaktiviert werden, werden die Systemeinstellungen für alle Benutzer in der Benutzergruppe ausgeblendet

11.4.2.1.2 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.

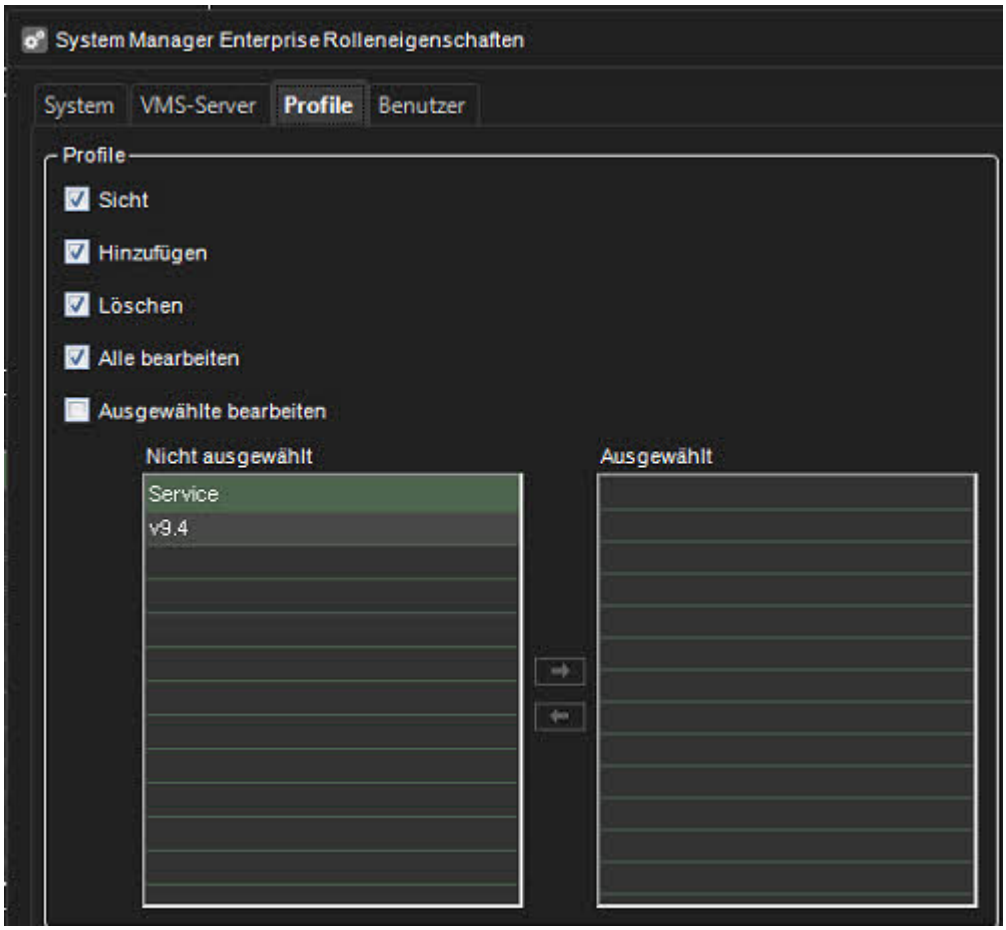
Dies ist in großen Installationen praktisch, wenn bestimmte Benutzergruppen mit bestimmten Servern arbeiten (z. B. wenn es separate Wartungsgruppen für verschiedene Standorte gibt - und die Aufzeichnungsserver standortspezifisch sind.)



11.4.2.1.3 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“).



11.4.2.1.4 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

11.4.2.2 Überwachungsrolle

Die Benutzer mit der Rolle Überwachung haben die Berechtigung:

11.4.2.2.1 System

- Protokolle exportieren
- SM-Server- und VMS-Server-Diagnose
- Lizenzen
- Watchdog-Protokoll

11.4.2.2.2 Profiles

Kann den Inhalt der Profile anzeigen

11.4.2.2.3 Benutzer

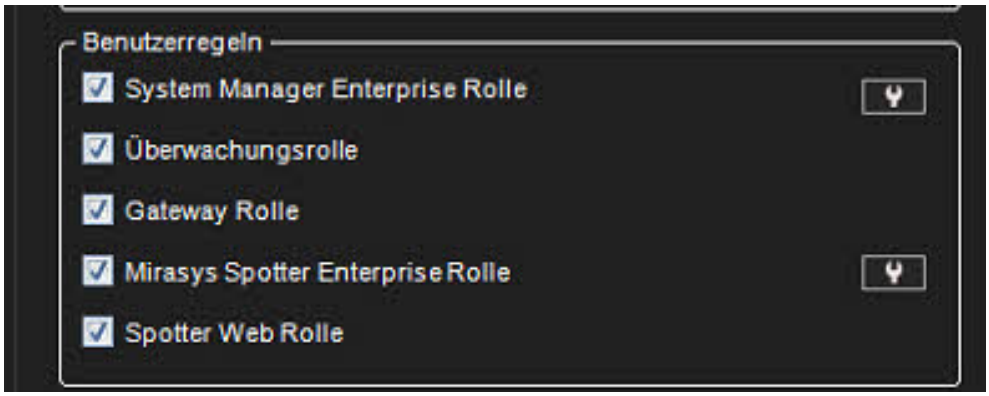
Kann die Systembenutzergruppen und -benutzer anzeigen

11.4.2.3 Gateway-Rolle

Gateway-Rolle ermöglicht die alte Spotter Mobile-Nutzung

11.4.2.4 Mirasys Spotter Enterprise Rolle

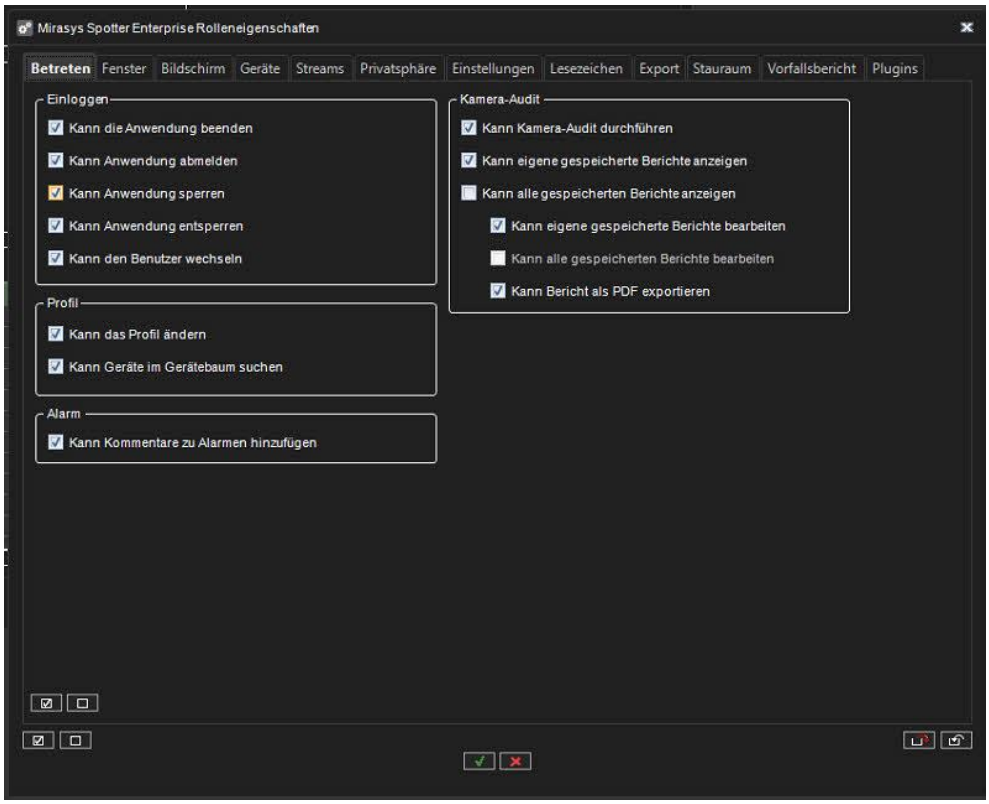
Benutzerdefinierte Benutzerrolleneigenschaften können bearbeitet werden, indem Sie auf die Schaltfläche zum Bearbeiten der benutzerdefinierten Rolleneigenschaften klicken.



Die benutzerdefinierten **Spotter**-Rollen können mit fast hundert verschiedenen Optionen (ohne Plugin-spezifische Anpassungen) angepasst werden.

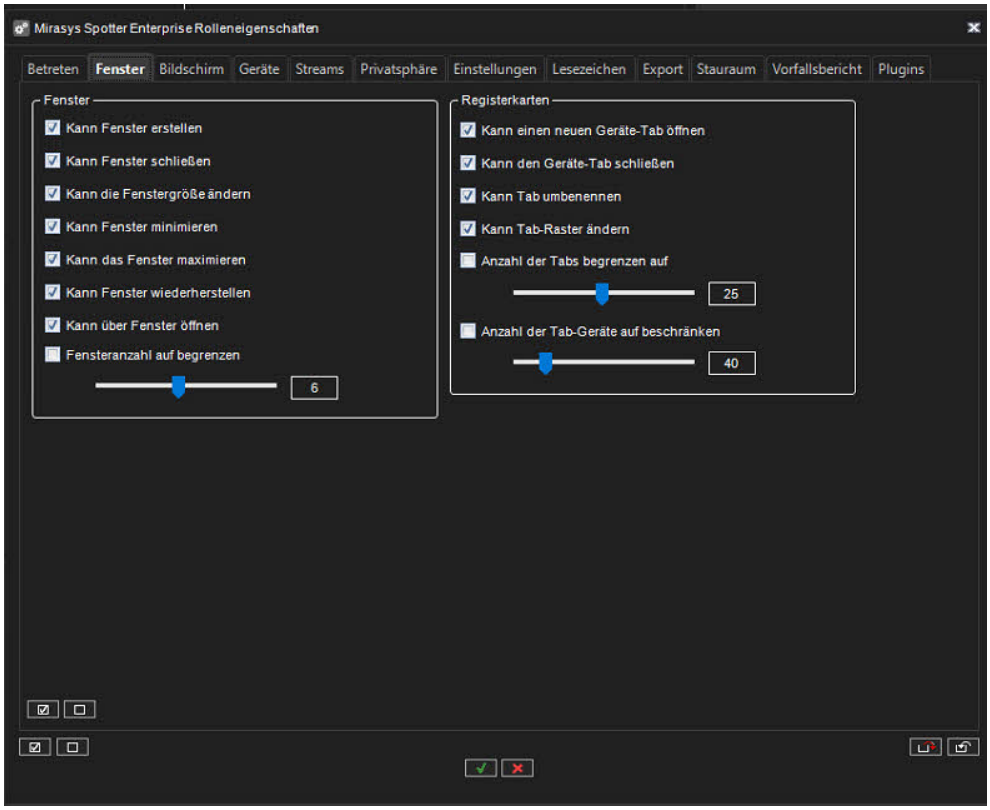
11.4.2.4.1 Access

Die Registerkarte Zugriff der Rollenanpassung enthält Optionen für den Anwendungszugriff und den Zugriff auf Profile und Alarmkommentare.



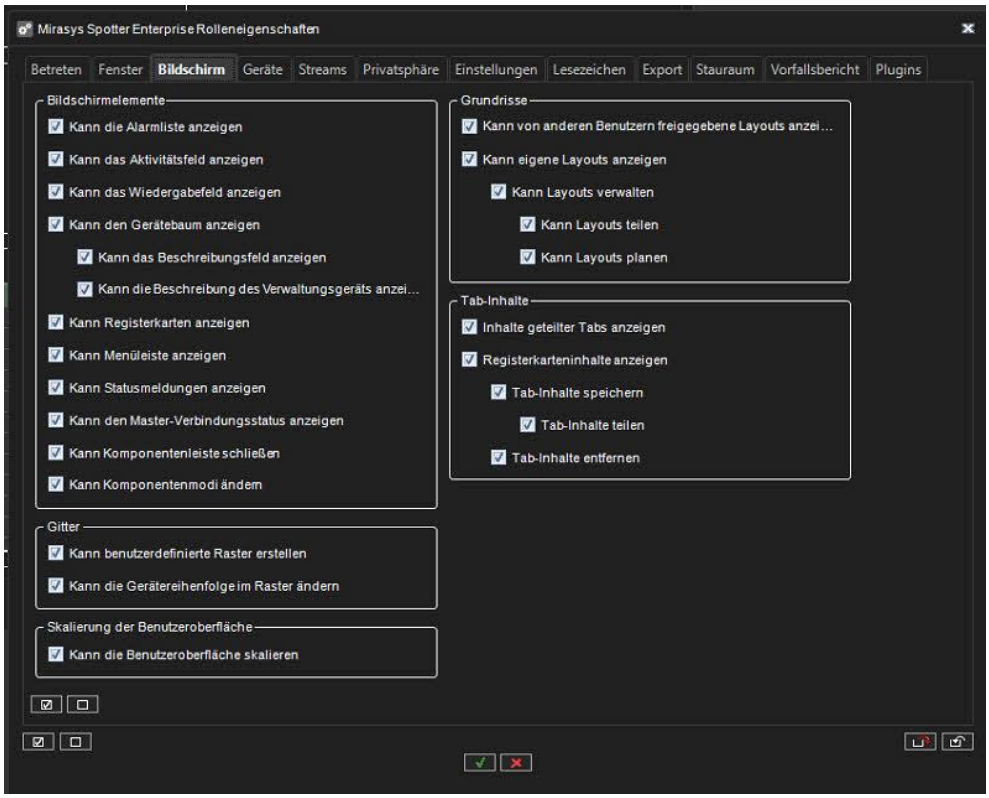
11.4.2.4.2 Fenster

Die Registerkarte „Fenster“ enthält Optionen für die Spotter-Fensterverwaltung und die Registerkartenverwaltung.



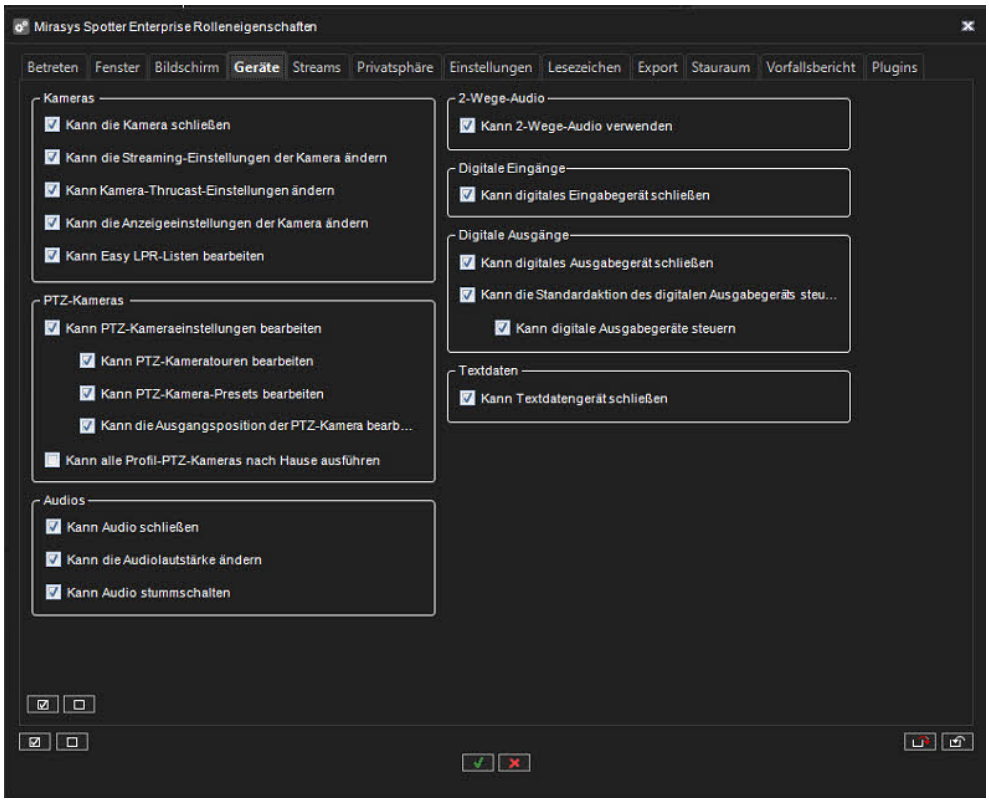
11.4.2.4.3 Bildschirm

Die Registerkarte Bildschirm enthält Optionen für den Zugriff auf verschiedene Bildschirmelemente und Layouts, Lesezeichen, Kameraraster und gespeicherte Kameraregisterkarten.



11.4.2.4.4 Geräte

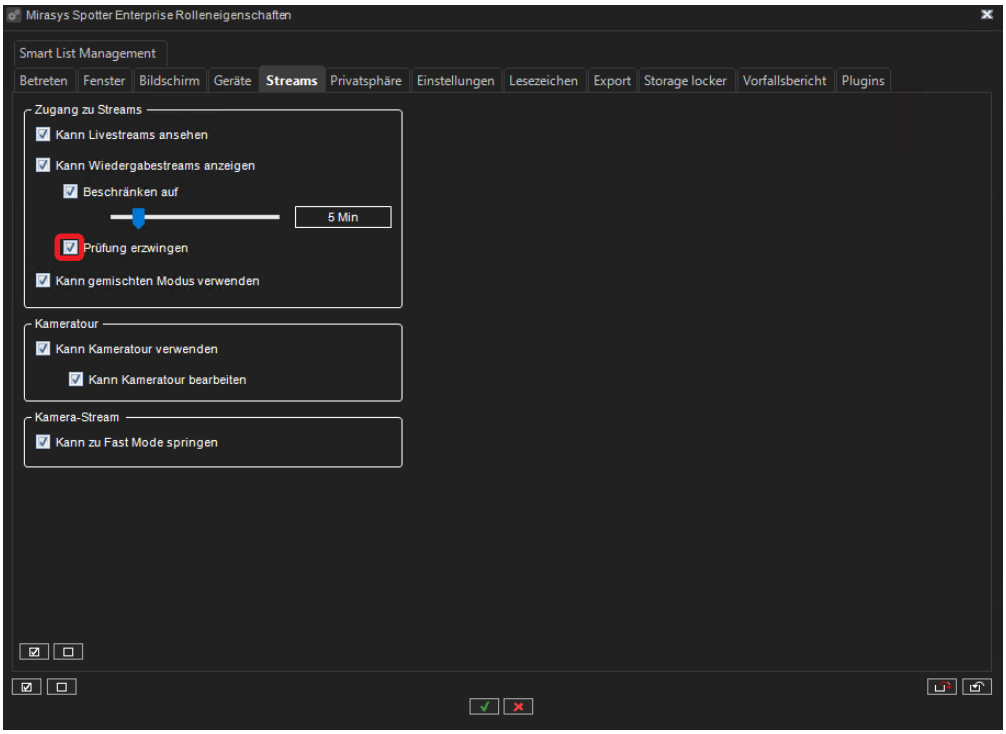
Die Registerkarte Geräte enthält Optionen zur Mediensteuerung.



11.4.2.4.5 Streams

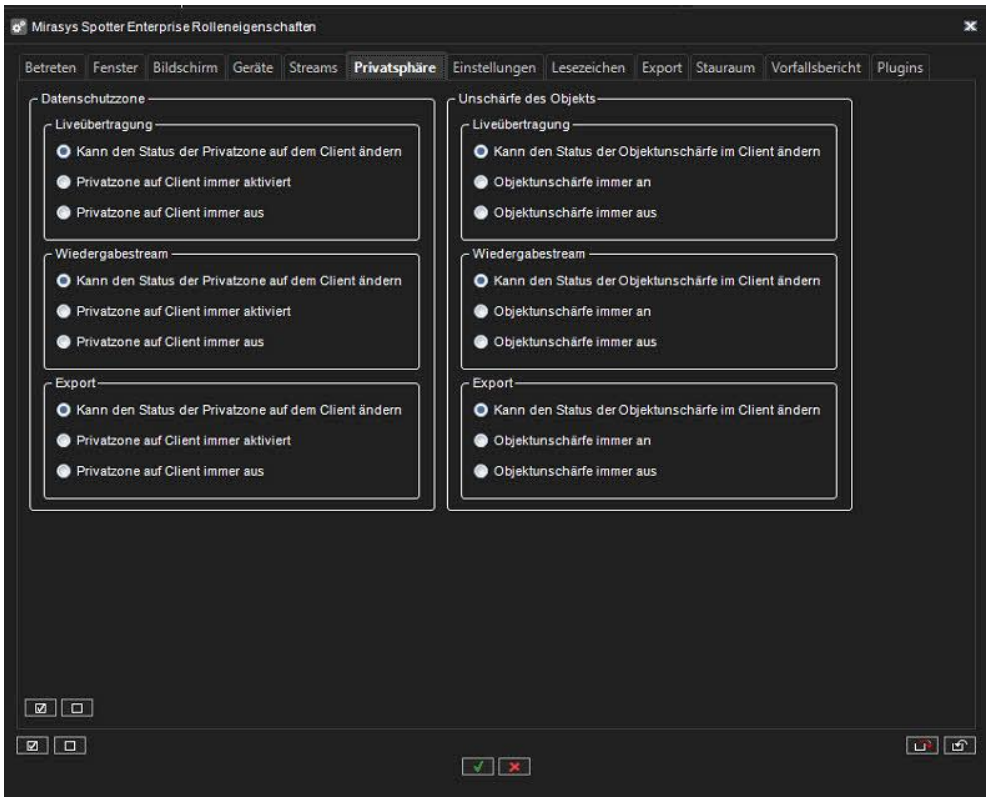
Die Registerkarte „Streams“ enthält Optionen für den Stream-Zugriff und -Export.

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.



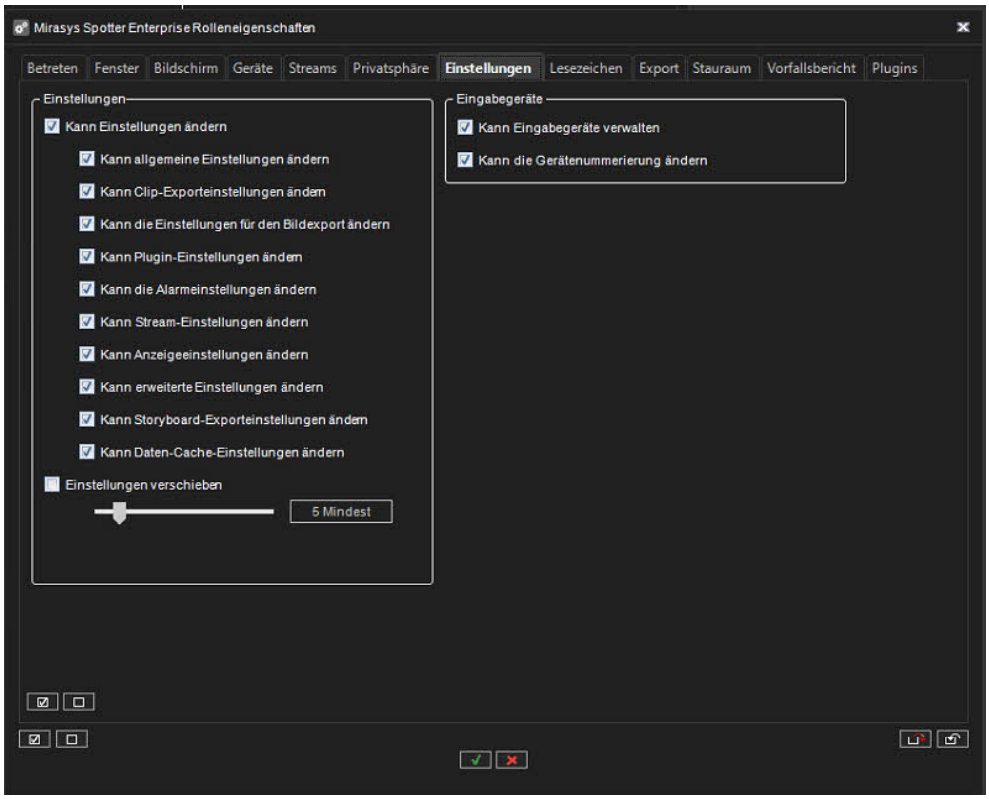
11.4.2.4.6 Privatsphäre

Die Registerkarte Privatsphäre enthält Optionen für den Datenschutz.



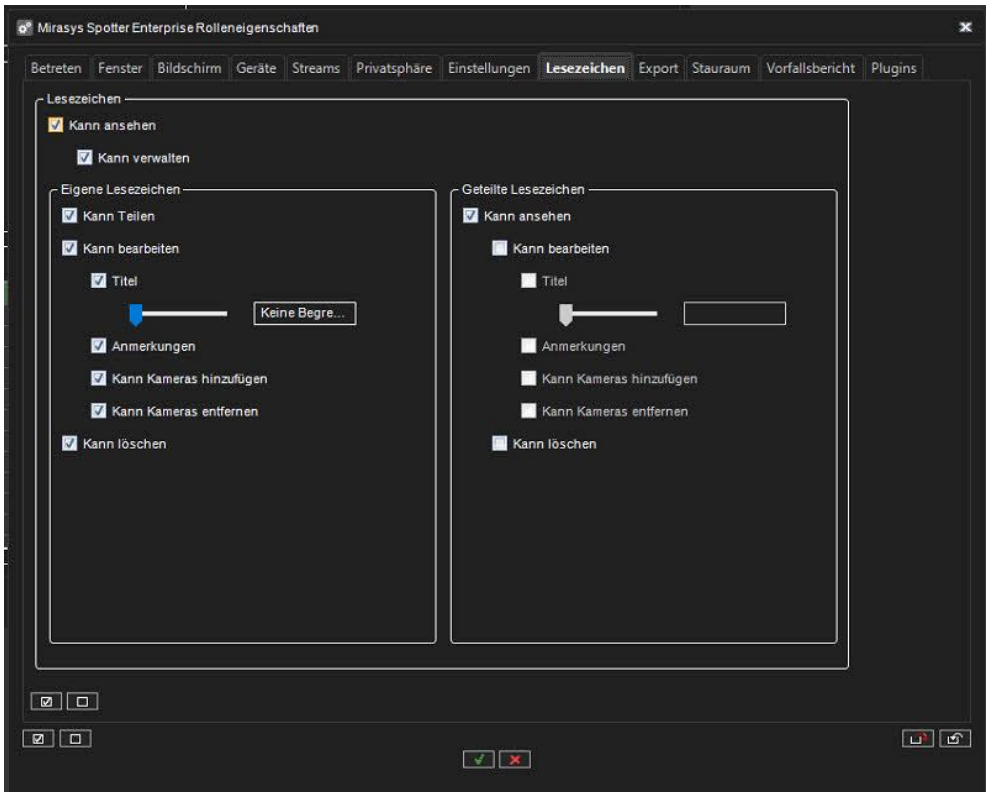
11.4.2.4.7 Einstellungen

Die Registerkarte Einstellungen enthält Optionen für Spotter-Einstellungen.



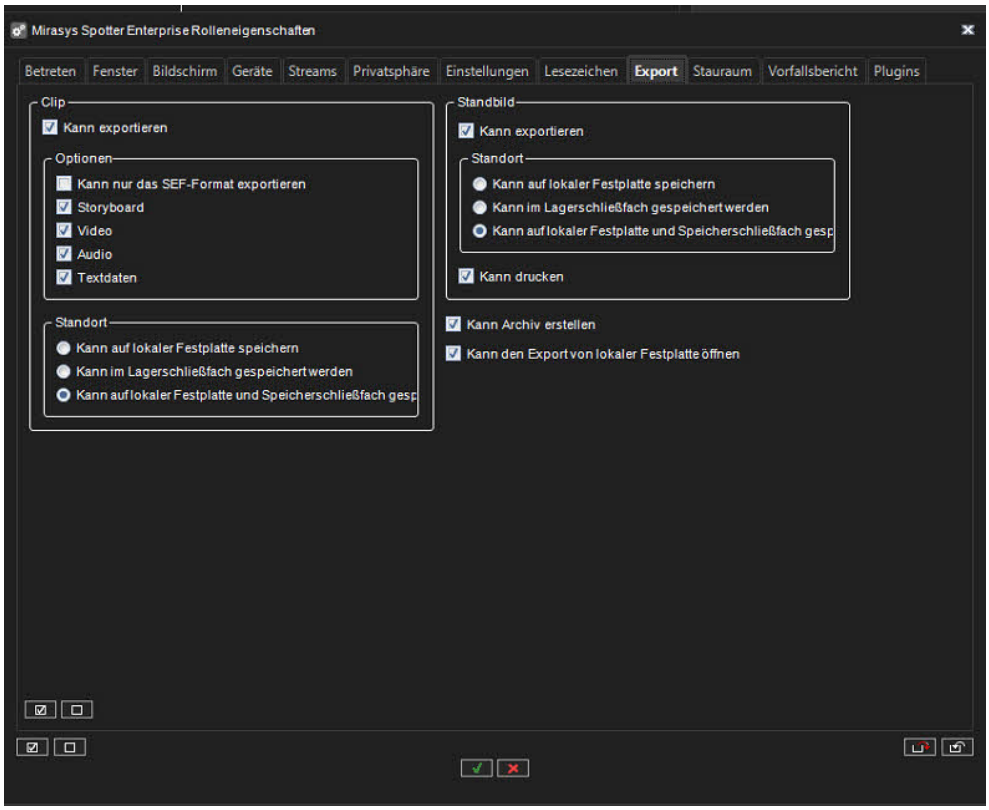
11.4.2.4.8 Lesezeichen

Die Registerkarte „Lesezeichen“ enthält Optionen für Lesezeichen



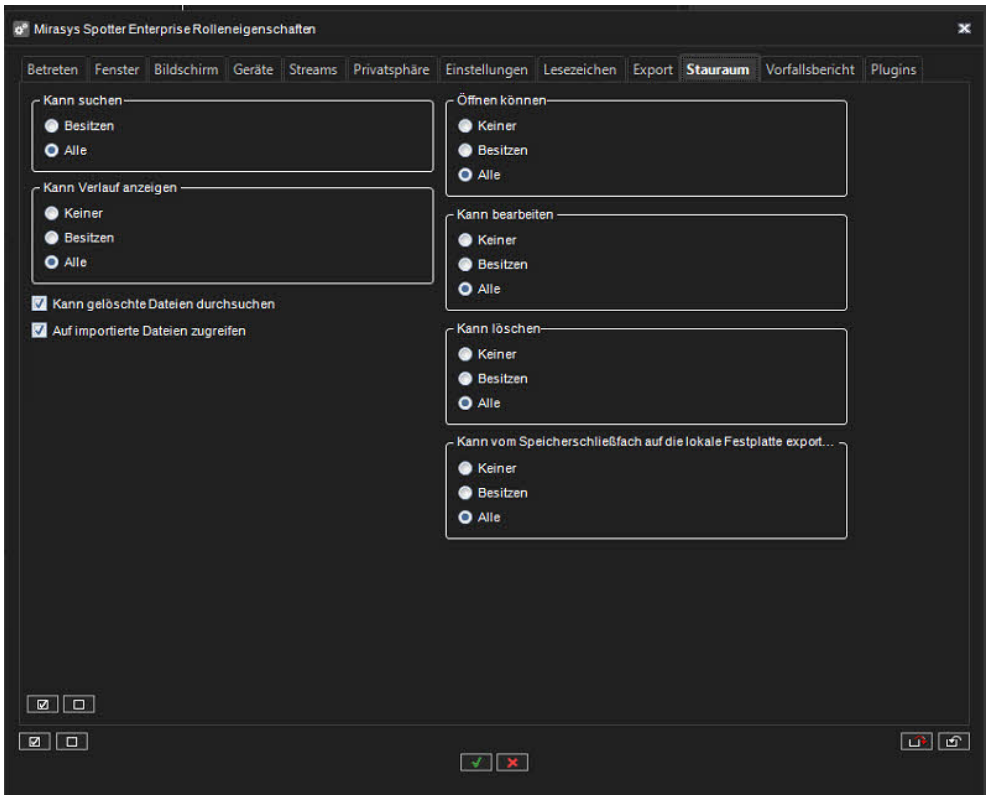
11.4.2.4.9 Export

Die Registerkarte Export enthält Optionen für Exportfunktionen



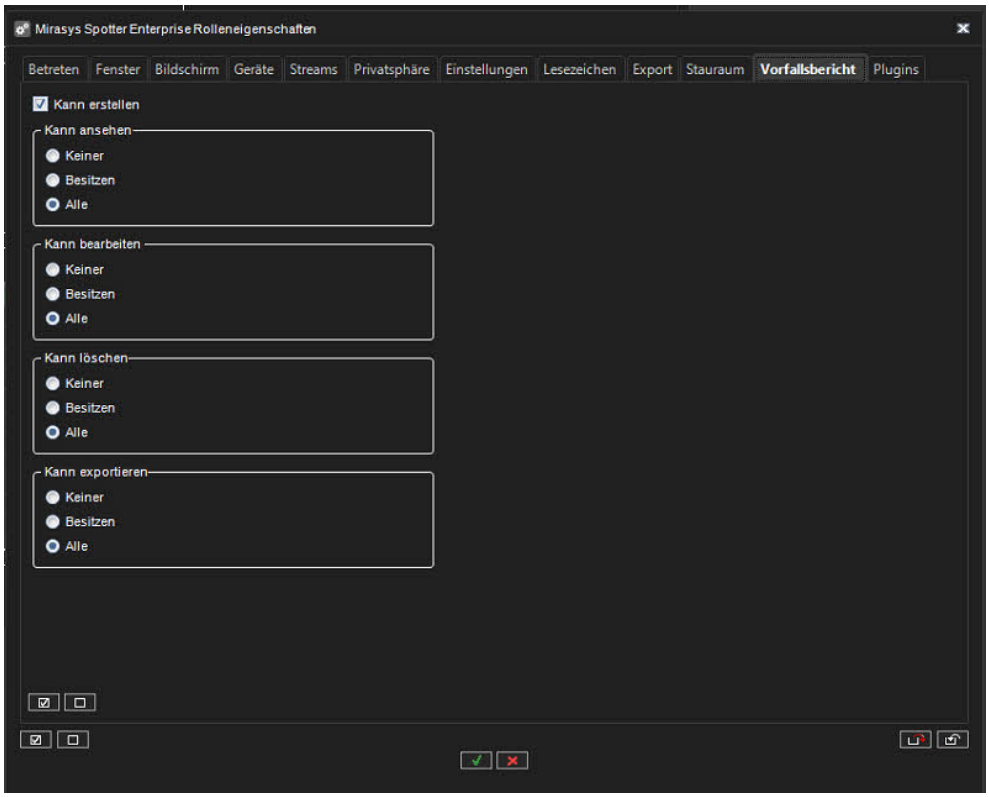
11.4.2.4.10 Storage Locker

Die Registerkarte „Stauraum“ enthält Optionen für das Plug-in „Storage Locker“.



11.4.2.4.11 Vorfallsbericht

Die Registerkarte „Vorfallsbericht“ enthält Optionen für das Plug-in „Incident Reporting“.



11.4.2.4.12 Plugins

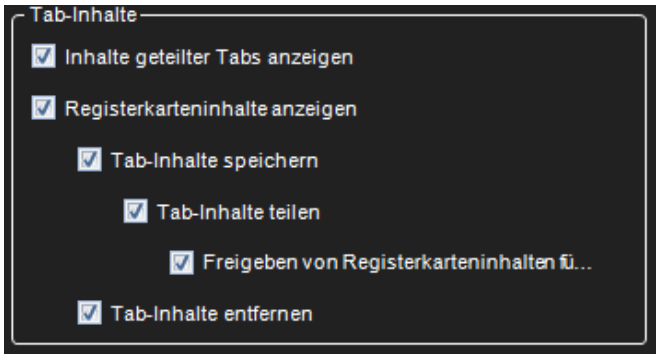
Die Registerkarte Plugins enthält Optionen für Spotter-Plugins.

Invalid file id - cfda42...

Jedes Plugin-Verhalten kann entweder standardmäßig oder benutzerdefiniert sein. Das Standardverhalten kann über die Steuerelemente „Standard-Plugin-Rolle“ gesteuert werden.

11.4.2.4.13 Freigabe 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.



11.4.2.4.14 Freigabe für bestimmte Benutzer

11.4.2.4.14.1 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..

11.4.2.4.14.2 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..

11.4.2.4.14.3 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.

11.4.2.4.15 Direkter 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.

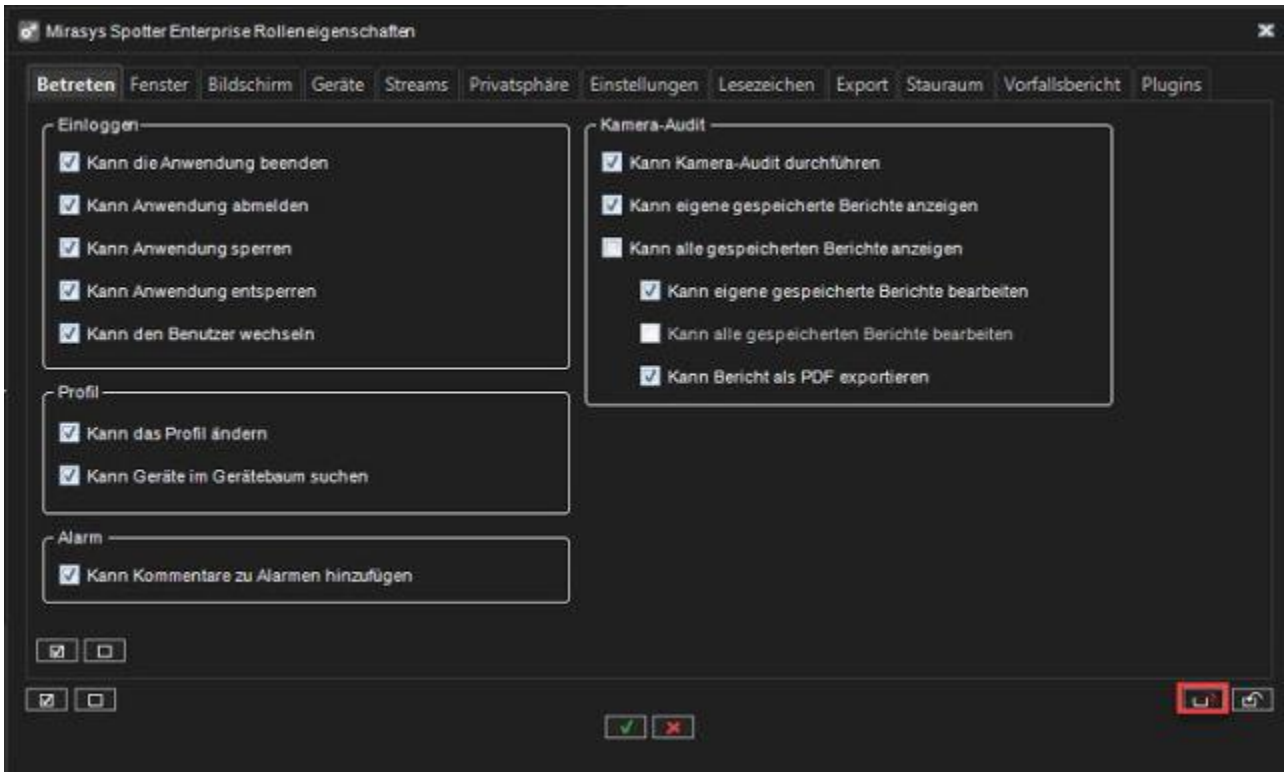
11.4.2.5 Spotter Web role (Benutzerregeln)

Spotter Web-Rolle ermöglicht neue Spotter Web- und Spotter Mobile-Nutzung

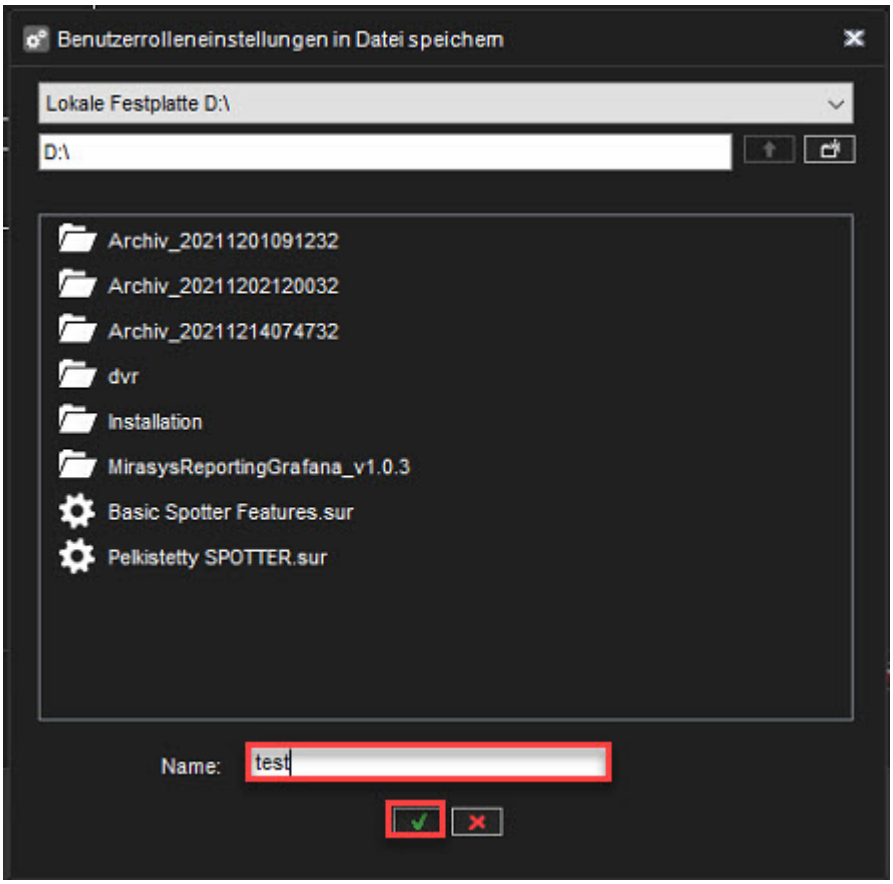
11.4.2.6 Exportieren und Importieren von Benutzerrolleneinstellungen

11.4.2.6.1 Benutzerrolleneinstellungen werden exportiert

- Klicken Sie auf **Benutzerrolleneinstellungen in Datei** exportieren

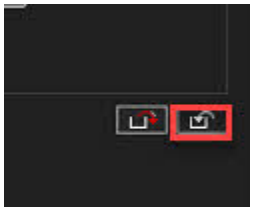


1. Ziel aussuchen
2. Legen Sie den Namen der Datei fest
3. Klicken **OK**

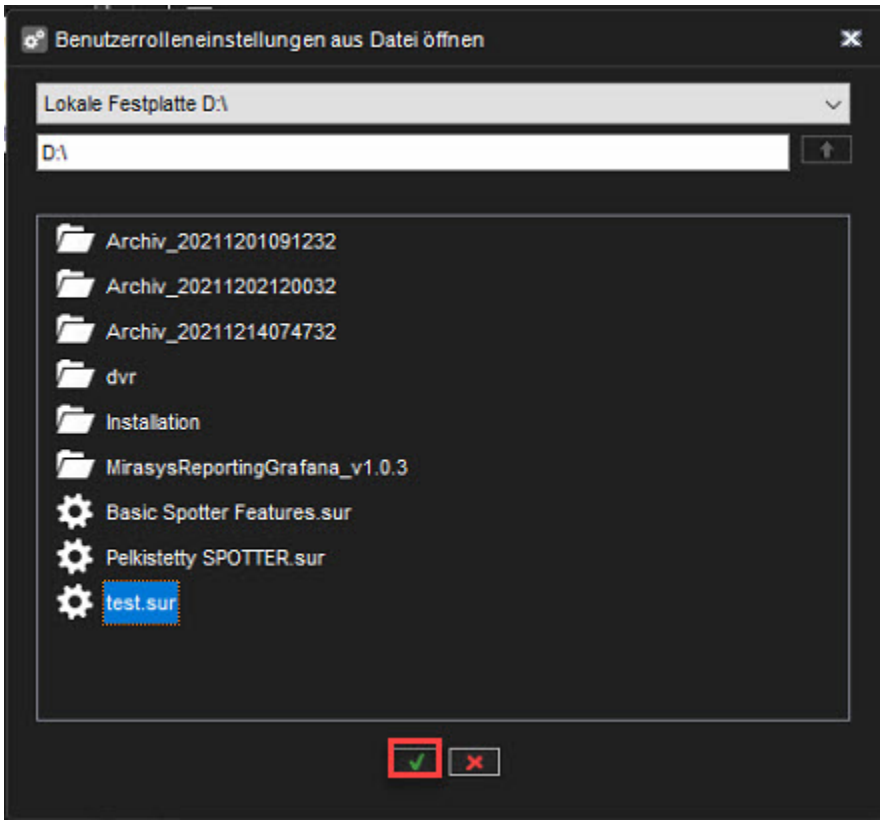


11.4.2.6.2 Importieren von Benutzerrolleneinstellungen

1. Klicken Sie auf **Benutzerrolleneinstellungen aus der Datei importieren**



2. Datei auswählen (.sur)
3. Klicken **OK**



11.4.2.7 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.

11.4.2.7.1 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).

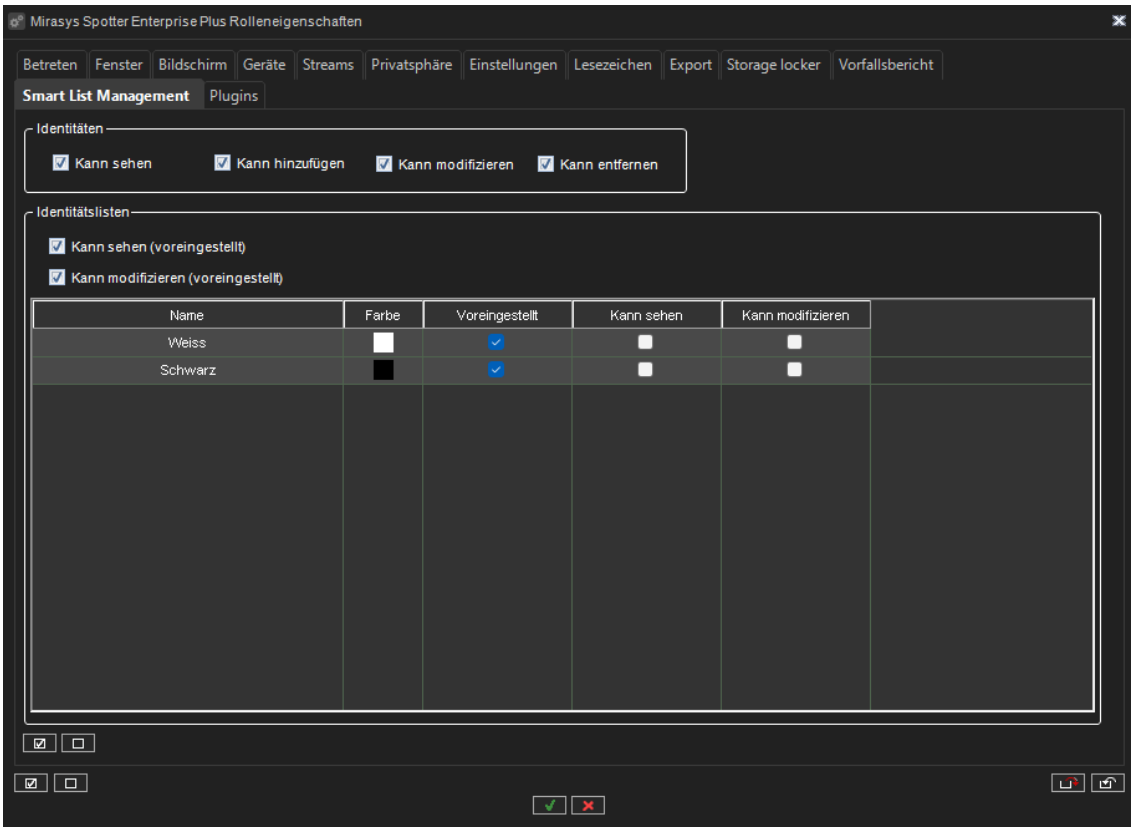


Figure 12 "Registerkarte "Intelligente Listenverwaltung

11.4.3 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.

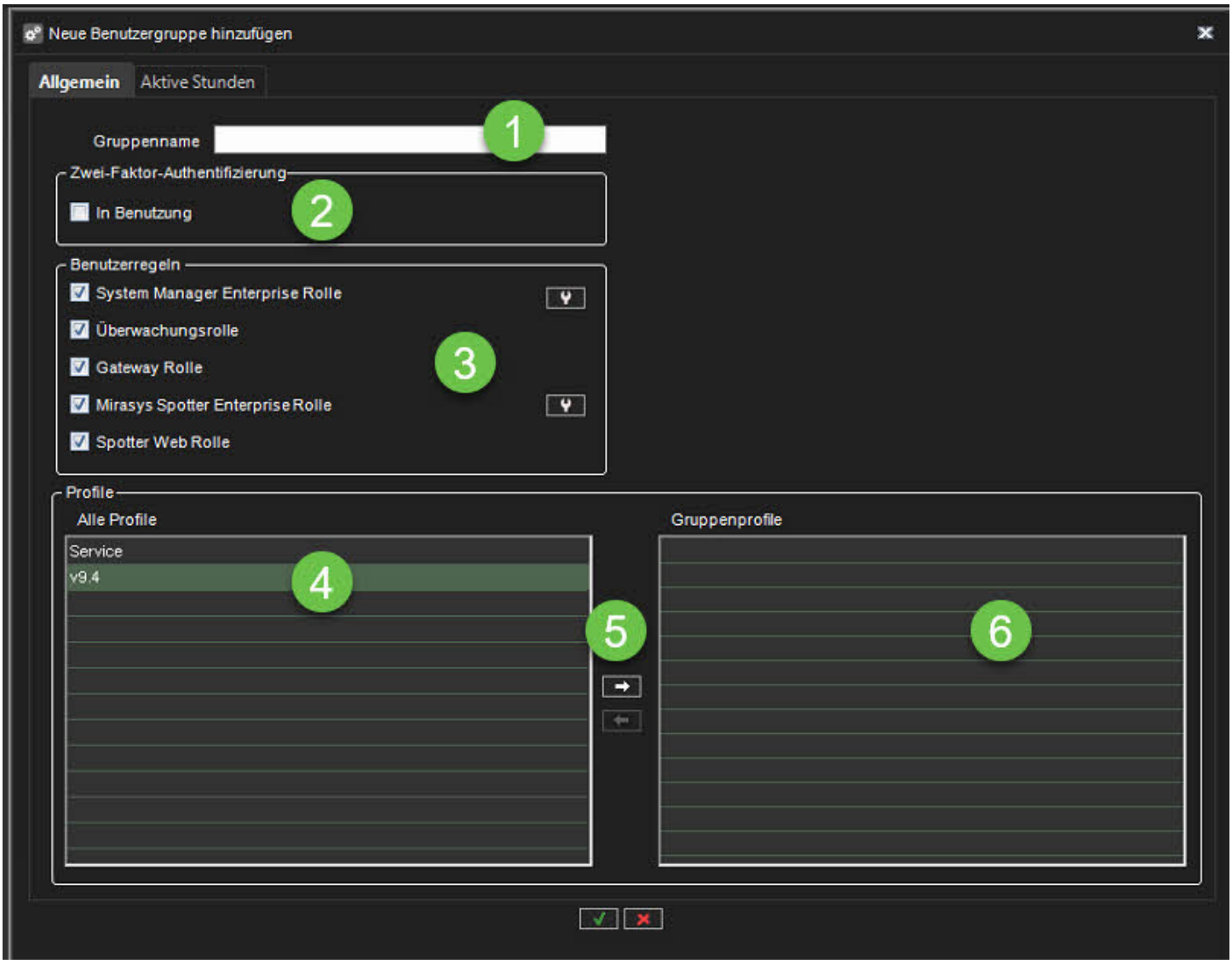
5. Wählen Sie das **Profil** oder **Profile** aus, das Sie der Benutzergruppe zuweisen möchten.

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.*



11.4.3.1 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.*

11.4.3.2 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.*

11.4.4 Zwei-Faktor-Authentifizierung

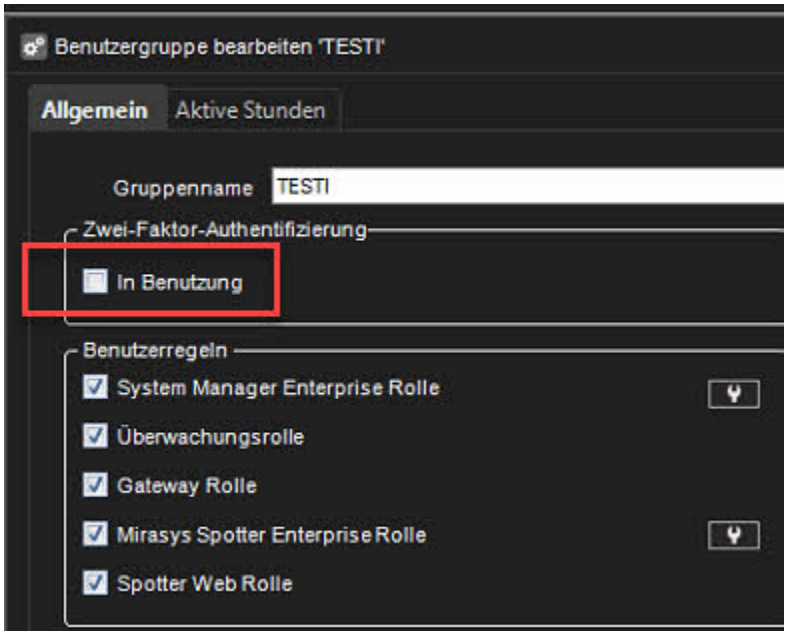
Die Zwei-Faktor-Authentifizierung ist eine Funktion zur Verbesserung der Identifizierung des Benutzers, indem der Benutzername und das Kennwort sowie ein Code von einem externen physischen Gerät angefordert werden.

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.)

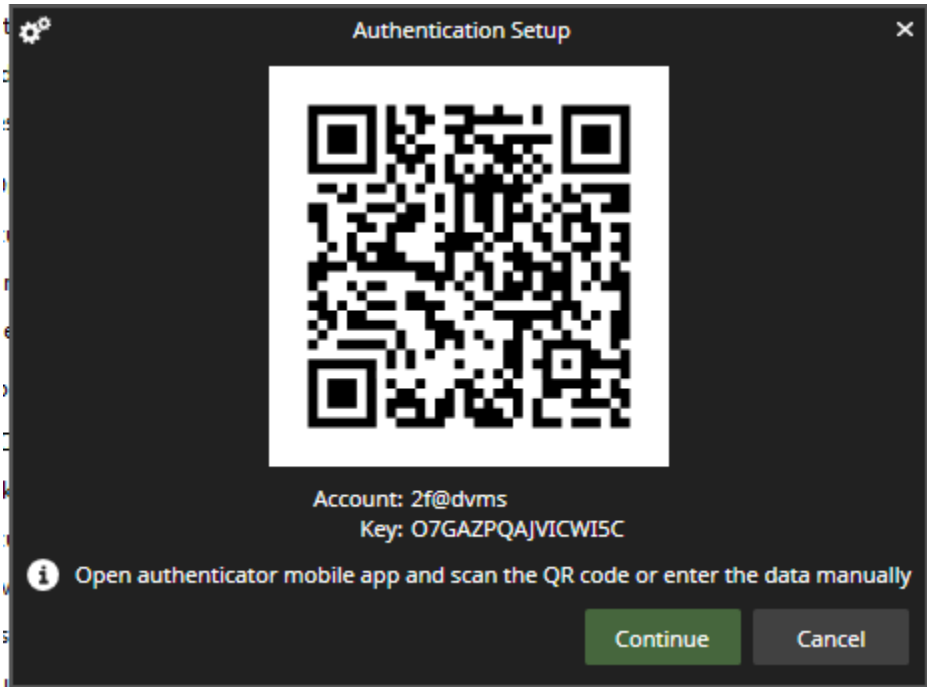
11.4.4.1 Aufstellen:

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:

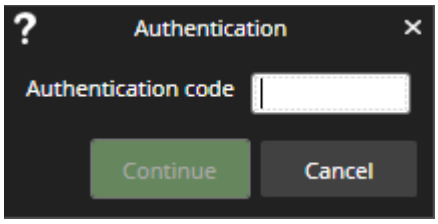


5. Danach generiert der Authentifizierungsclient automatisch neue Einmalpasswörter.
    a. (Die Passwörter ändern sich regelmäßig und werden synchron gehalten, da die VMS-Uhren und die Authentifizierungs-App die gleiche Zeit haben.
    b. Beachten Sie, dass dies keine direkte Datenkommunikationsverbindung zwischen der Software erfordert.)

11.4.4.2 Anmeldung:

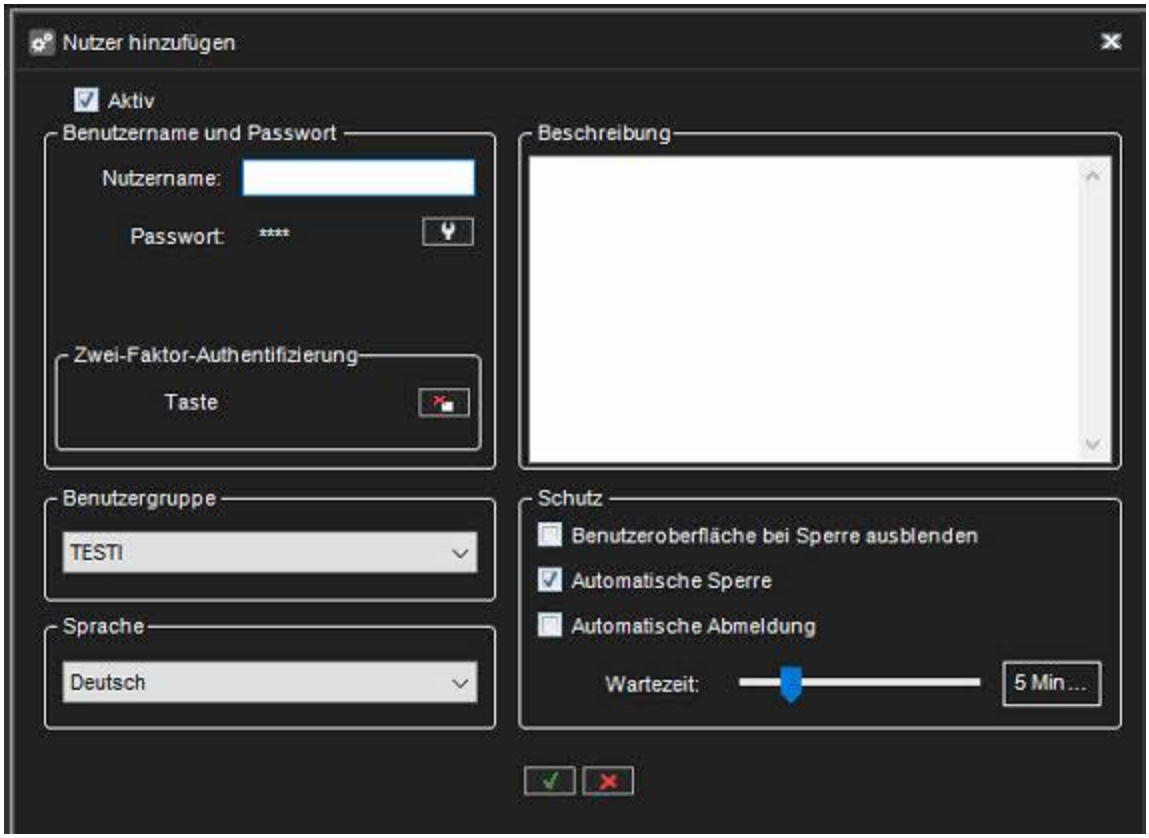
1. Der Benutzer stellt VMS die Standard-Anmeldeinformationen zur Verfügung (Benutzername, Passwort)
2. Das VMS fordert für jede Anmeldung einen Authentifizierungscode von der Authentifizierungs-App an.

3. Der Benutzer gibt das Einmalpasswort aus der Authentifizierungs-App an. Der Benutzer gibt sie in den VMS-Client ein.



11.4.4.3 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).



11.4.5 Domänenbasierte Benutzergruppen (LDAP)

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.

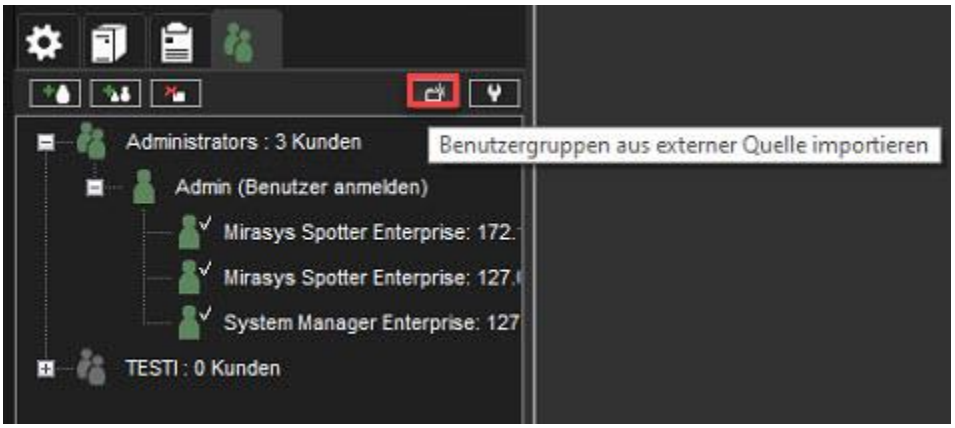
Diese Funktion erfordert ein Lizenzupdate.

11.4.5.1 So fügen Sie dem System eine neue domänenbasierte Benutzergruppe hinzu:

1. Klicken Sie in der oberen linken Ecke der Registerkarte **Benutzer** auf **Benutzergruppen aus einer externen Quelle importieren**

Der Master-Server 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.



2. Geben Sie den Namen der Domäne in das Dialogfeld **Domänenname** ein.

3. 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.

4. Wählen Sie aus, ob offene Benutzergruppen übersprungen oder eingeschlossen werden sollen.

5. Wählen Sie aus, ob vorherige Suchergebnisse gelöscht oder beibehalten werden sollen.

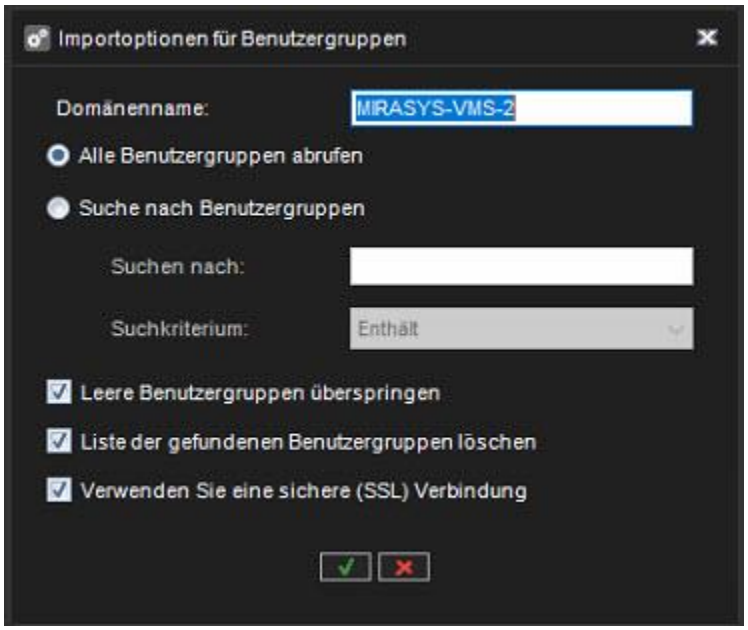
6. Aktivieren Sie **Sichere (SSL)-Verbindung verwenden**. Wenn benötigt

7. Klicken Sie auf **Ok**.

8. Wählen Sie im Fenster **Benutzergruppen importieren** die Benutzergruppen aus, die Sie aus der Domäne importieren möchten.

9. Klicken Sie auf **Ok**, um die ausgewählten Gruppen zu importieren.

10. Bearbeiten Sie die importierten Benutzergruppen, um ihre Benutzerrollen wie unten beschrieben festzulegen.



11.5 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.

11.5.1 Identifizierung der Benutzer durch einen von der Anmelde-ID getrennten Benutzernamen

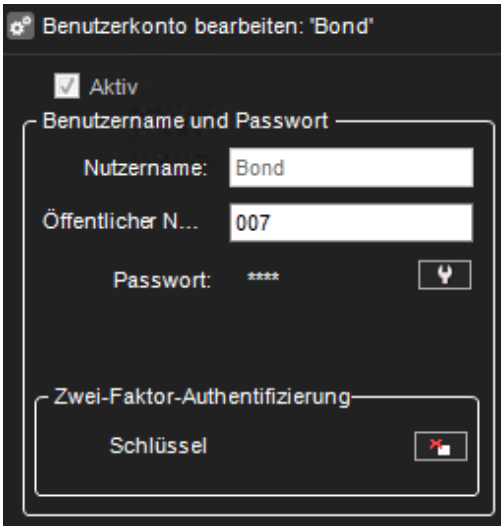
Um die Sicherheit der Plattform zu verbessern, können die Benutzer durch einen separaten Benutzernamen identifiziert werden, damit die Anmelde-ID des Benutzers nicht angezeigt wird.

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.

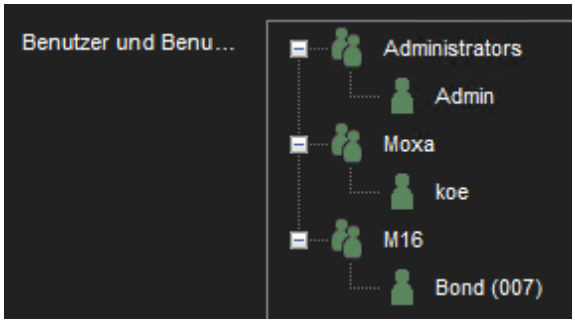
11.5.2 Hinzufügen eines öffentlichen Benutzernamens im System Manager

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:

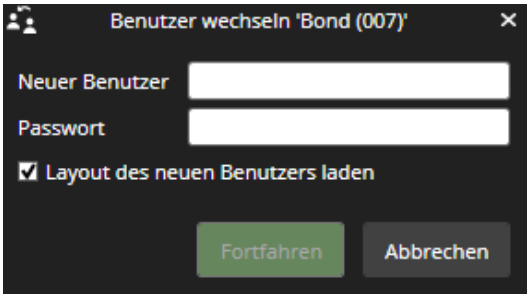
Dieser Name wird in der Benutzerliste des System Managers angezeigt:



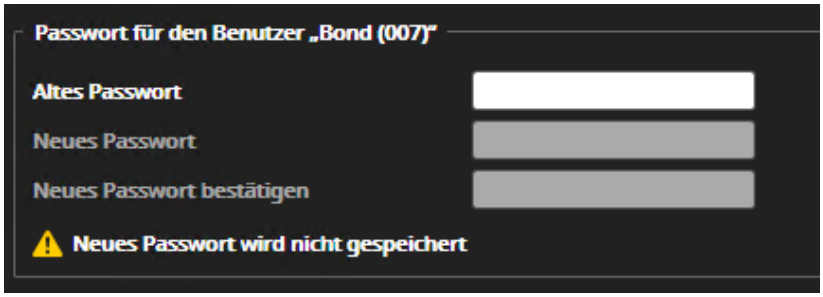
Und auch als angemeldeter Benutzer:

11.5.3 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:



11.5.4 Öffentlicher Benutzername im Spotter-Web

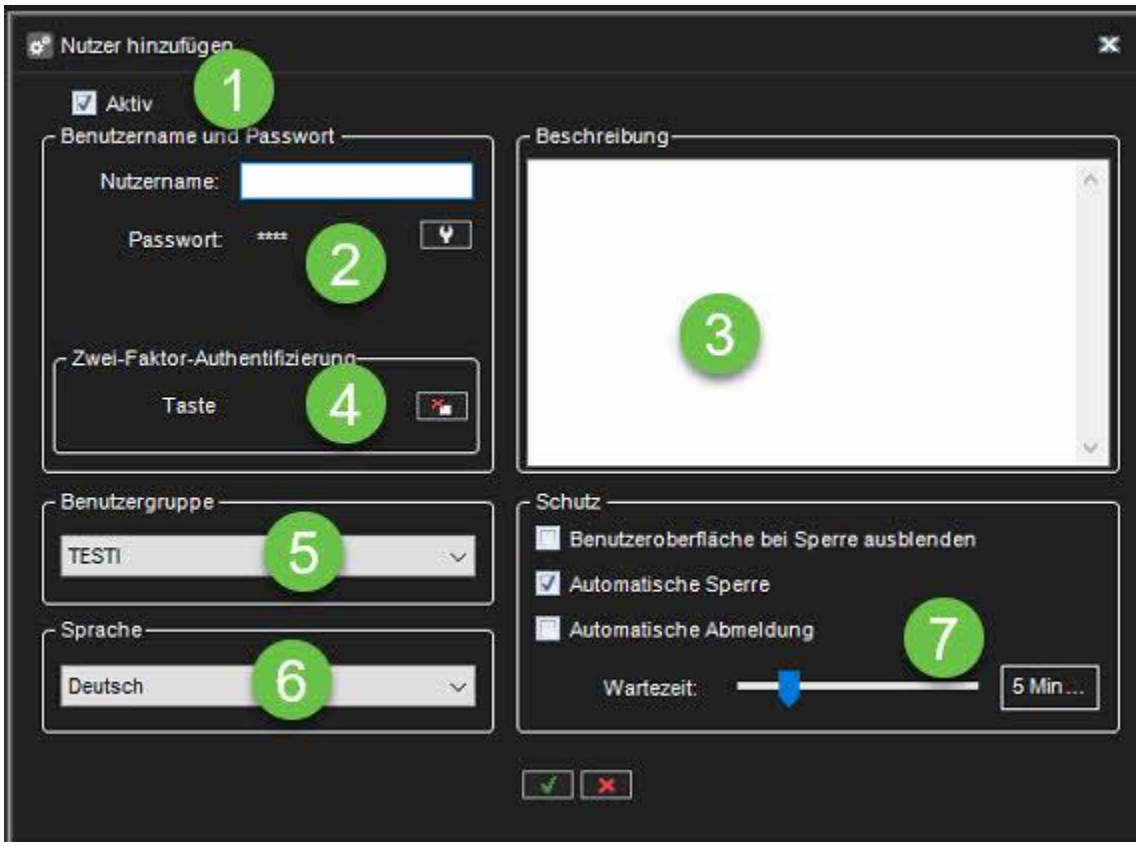
Der öffentliche Benutzername wird in Spotter Web in der oberen rechten Ecke angezeigt, wenn er im System Manager definiert wurde.

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.

11.6 Die Benutzerkontoeinstellungen enthalten die folgenden Optionen:

- Kontostatus
- Passwort
- Zwei-Faktor-Authentifizierung Schlüsselverwaltung, siehe mehr von Zwei-Faktor-Authentifizierung
- Benutzergruppe
- Sprache
- Schutzeinstellungen



11.7 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.*

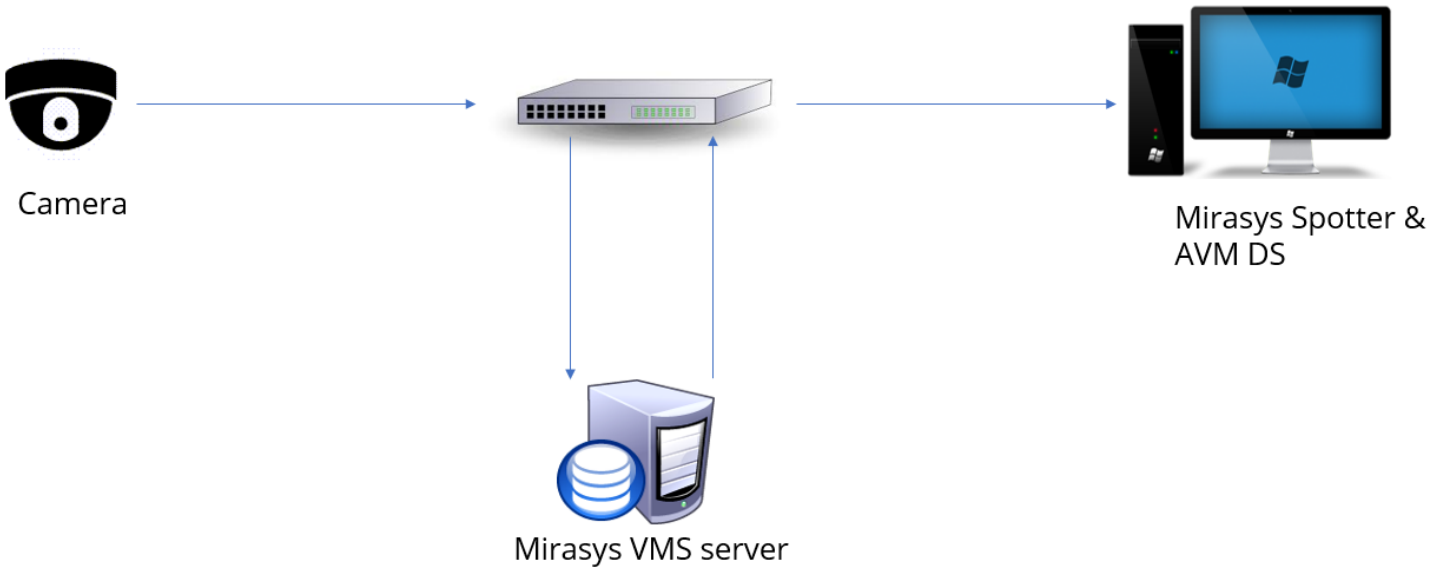
12 TruCast

TruCast ist die Funktion zum direkten Kamera-Videostreaming in Mirasys VMS.

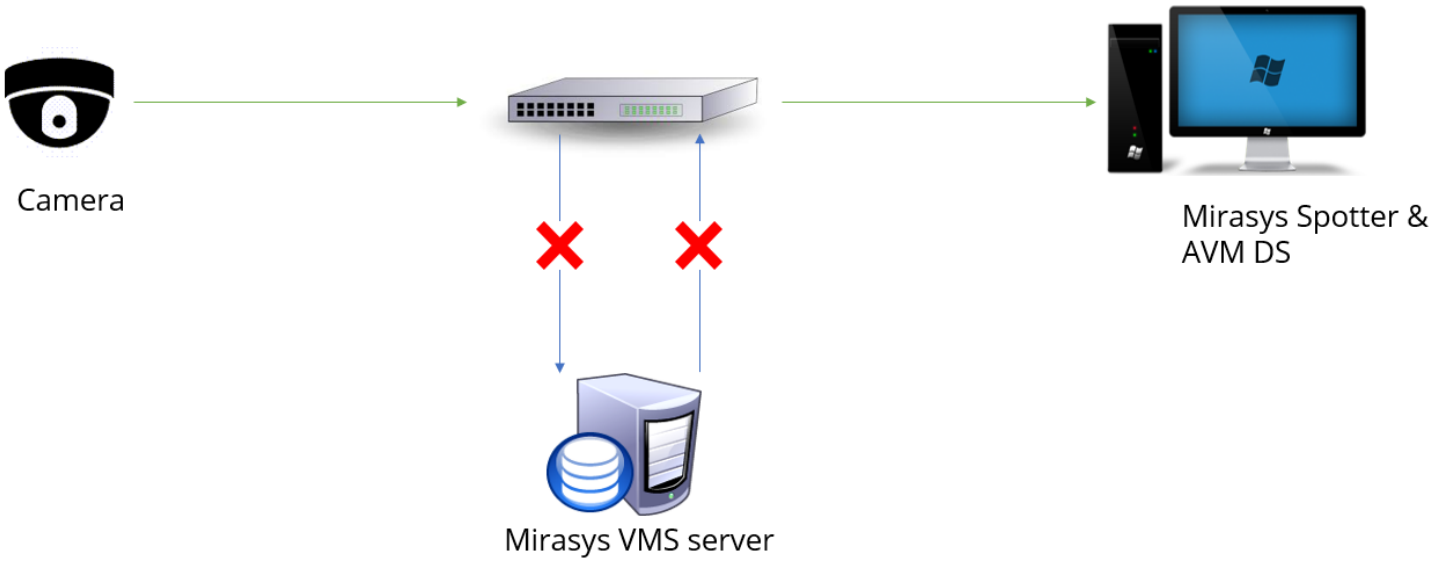
Bei TruCast kommt der Videostream direkt von der Kamera zum Viewing-Client, der Spotter für Windows-Anwendung.

In einem Standard-Streaming-Szenario kommt der Stream zum Client vom VMS-Server.

12.1 Vom Server zum Client streamen



12.2 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.

12.3 Unterstützte Kameras

TruCast 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 TruCast-Treiber für Kameras, die nicht in der Liste der unterstützten Kameras aufgeführt sind.

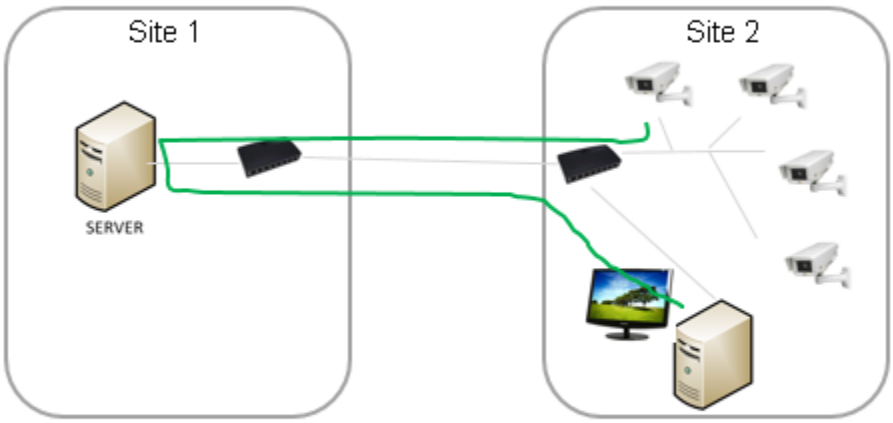
Die Verwendung des ONVIF-Treibers erfordert, dass die Kamera mit dem ONVIF-Treiber zum VMS-System hinzugefügt wird, nicht mit dem nativen Treiber der Kamera.

12.4 Netzwerkoptimierung

TruCast kann verwendet werden, um die Netzwerklast in bestimmten Szenarien zu reduzieren.

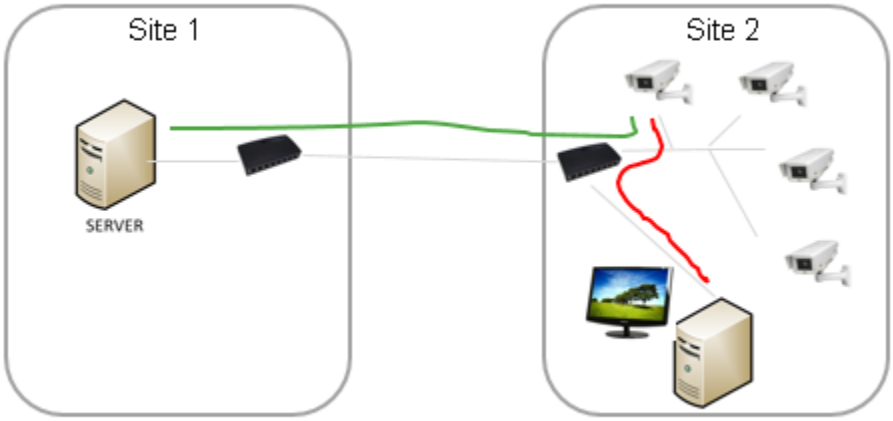
Die Lastreduzierung erfolgt hauptsächlich, wenn sich der Server außerhalb des Standorts (remote) und der Viewing-Client vor Ort (lokal zu den Kameras) befindet.

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 TruCast, 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.

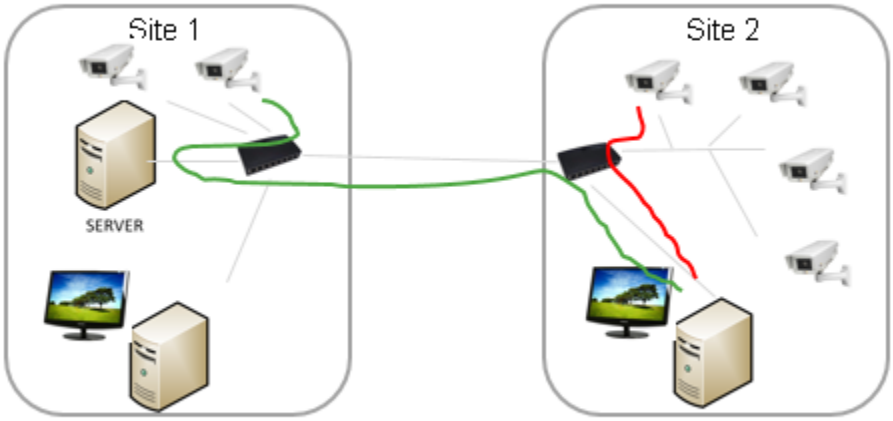
Wenn der Stream mit TruCast direkt von der Kamera konsumiert wird, wird der Verkehr zwischen den beiden Standorten reduziert.



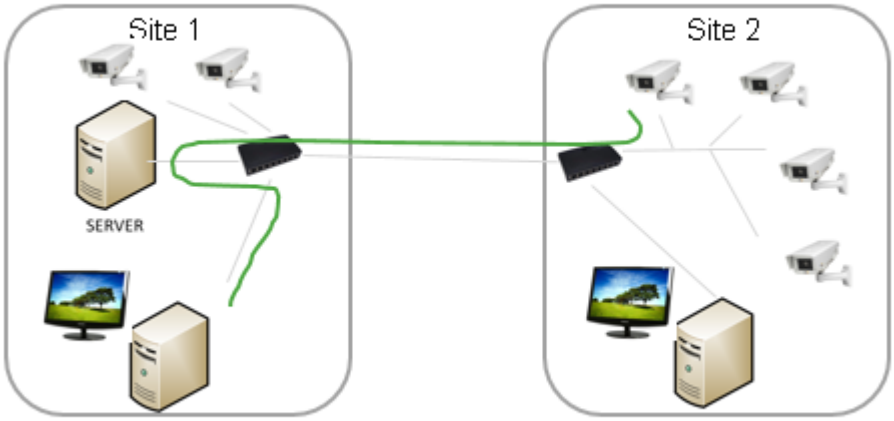
In Beispielszenario 2 befinden sich Kameras an zwei Standorten und anzeigende Clients an zwei Standorten.

Für den Site 2-Anwender ist der Einsatz von TruCast für die Kameras vor Ort sinnvoller.

Der Benutzer kann wählen, ob TruCast für alle Kameras oder nur für die Kameras vor Ort verwendet werden soll.



Für den Benutzer von Site 1 reduziert die Verwendung von TruCast nur den Datenverkehr vom Server zur nächsten Netzwerkverbindung.



Benutzer haben die vollständige Kontrolle darüber, welche Kameras typischerweise von TruCast verwendet werden.

Die Einstellung wird für jede Kamera und jeden Benutzer gespeichert und in Spotter-Layouts gespeichert.

12.5 Multistreaming und TruCast für Netzwerkoptimierung und -speicherung

Da es auch möglich ist, für TruCast einen anderen Stream als den Aufzeichnungsstream zu verwenden, sollte dies bei der Planung der Netzwerkkapazität berücksichtigt werden.

Beispielsweise können Benutzer Live-Bilder mit TruCast 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.

12.5.1 Auswirkungen von TruCast auf die Bildverzögerung

Da der TruCast-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.

12.5.2 Von TruCast Streaming nicht unterstützte Funktionen

TruCast unterstützt keine PTZ-Steuerung oder Audio

Außerdem unterstützt TruCast derzeit nur Live-Bilder. Die Wiedergabe (aufgezeichnete Bilder) wird derzeit immer vom Server empfangen.

12.5.3 Lizenzen

TruCast erfordert die VMS-Lizenz, damit die TruCast-Funktion und die TruCast-Client-Treiberkennungen verwendet werden.

Diese TruCast-Treiberlizenzen und die TruCast-Funktion sind in der Produktversion Mirasys V9 immer aktiviert.

12.5.4 Mehrere Zuschauer

Da jeder TruCast-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.

12.5.5 Client-Treiber installieren

Vor der Verwendung von TruCast 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 TruCast bereit.

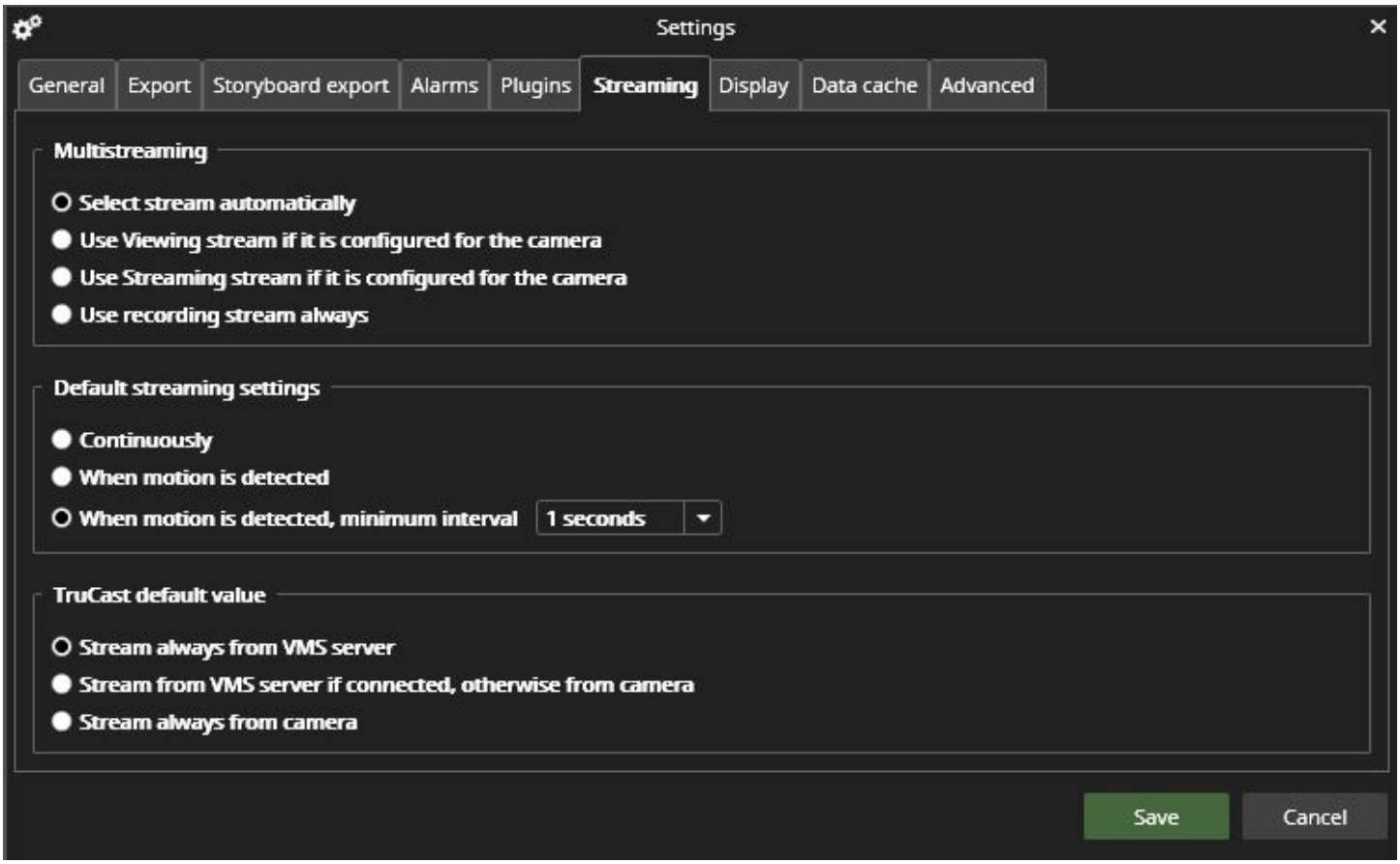
Bitte beachten Sie, dass nur die Kameras, deren Client-Treiber installiert wurde, als TruCast aktiviert angezeigt werden.

12.5.6 Multi-Streaming konfigurieren

TruCast 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 TruCast-Anzeige verwendet.



12.5.7 TruCast-Standardeinstellung

Die Standardeinstellung für alle Kameras, die noch nicht für TruCast verwendet wurden, kann in den Spotter-Einstellungen - Streaming - TruCast-Standardwert definiert werden.

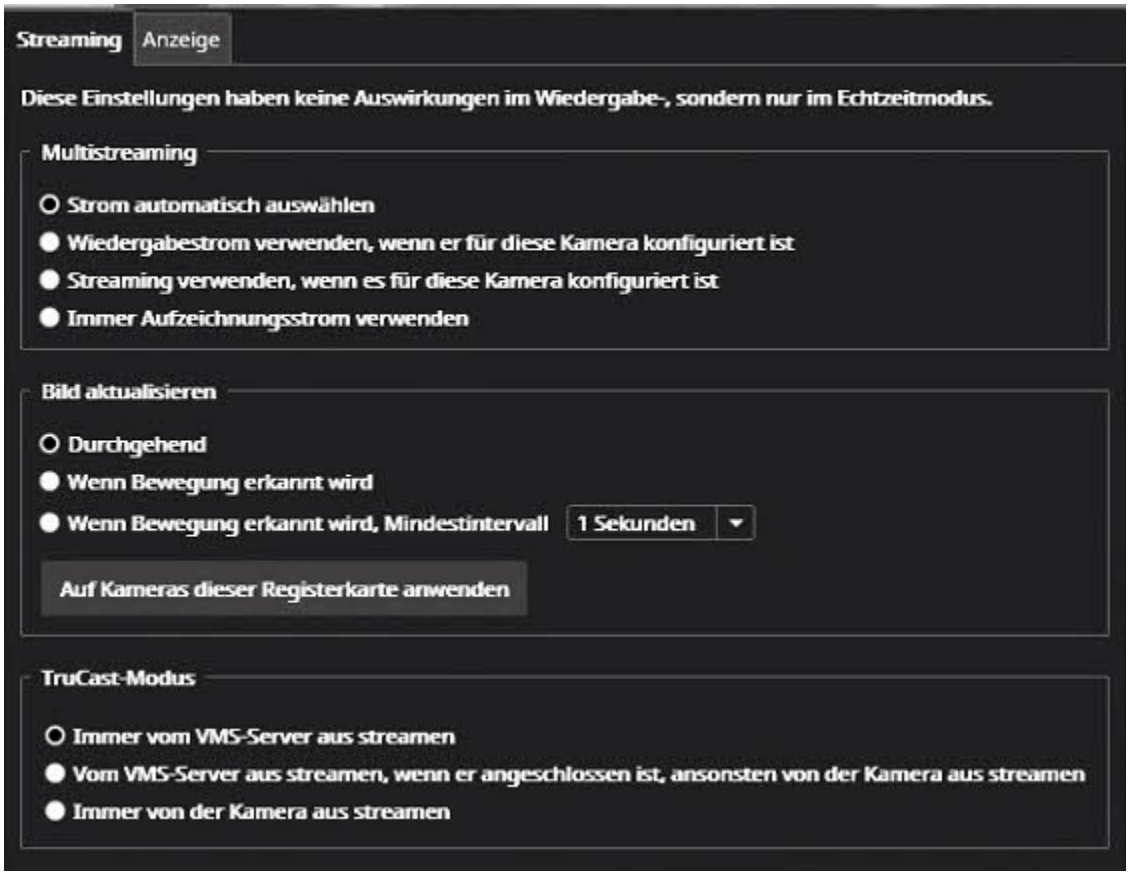
Die möglichen Werte sind

- Immer vom VMS-Server streamen
- Streamen Sie normal vom VMS-Server, wechseln Sie jedoch zu TruCast, wenn die Verbindung zum Server unterbrochen wird
- Immer mit TruCast streamen

12.6 Verwenden von TruCast

Der Benutzer kann die Kameras mit TruCast Capability über die Kamera-Symbolleiste – Einstellungen – sehen.

Für Kameras mit TruCast ist die Einstellung verfügbar.



Bei Kameras ohne TruCast ist der untere Teil des Dialogs deaktiviert.

Die Einstellung wird für jede Kamera separat gespeichert.

Wenn TruCast aktiv ist, wird oben über der Kamera im Gerätebaum ein kleiner Pfeil angezeigt.

13 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.

Analoge Kameras, die an die Capture-Karte eines Servers angeschlossen sind, werden nicht an den Failover-Server übertragen. Beim Wechsel werden nur zuvor zugewiesene IP-Kameras neu zugewiesen.

13.1 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 Master-Server 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 Master-Server, einem VMS-Server für die Videoaufzeichnung und einem Standby-Failover-Server.

Die Failover-Migration wird unter den folgenden Bedingungen ausgelöst:

- Der Master Server hat die Verbindung zu einem VMS Server verloren und das vom Administrator eingestellte Timeout ist erreicht
- Ein VMS-Server hat dem Master-Server 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 Master-Server 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.

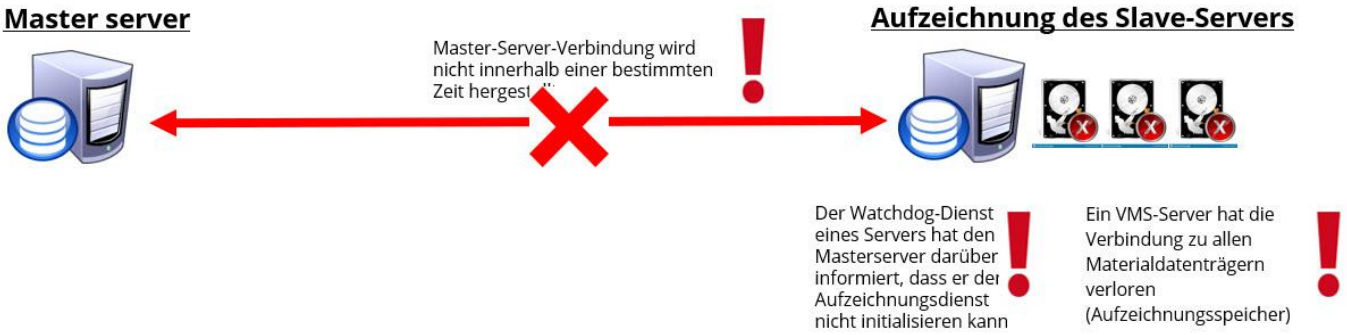
13.2 Mindestanforderungen

- **Master-Server auf separatem PC installiert**
    - Die Lizenz muss eine automatische Sicherungsfunktion enthalten
    - Die Lizenz muss einen oder mehrere Failover-Server enthalten
- **1 Slave-Server für Aufzeichnung**

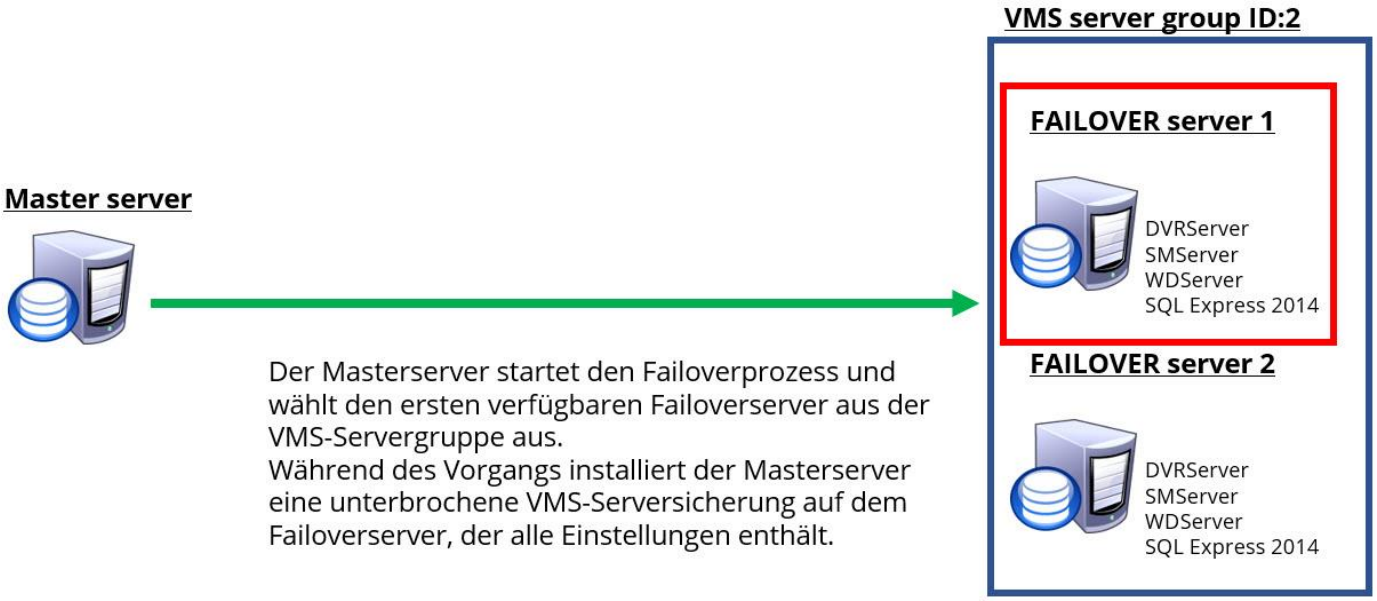
1 Standby-Failover-Server

- Die Lizenz muss mindestens die gleiche Anzahl an Videokanälen enthalten wie der Aufzeichnungs-Slave-Server
- Materialfestplatte gleicher Größe und zugewiesene Laufwerksbuchstaben

13.3 FAILOVER-AUSLÖSEBEDINGUNGEN



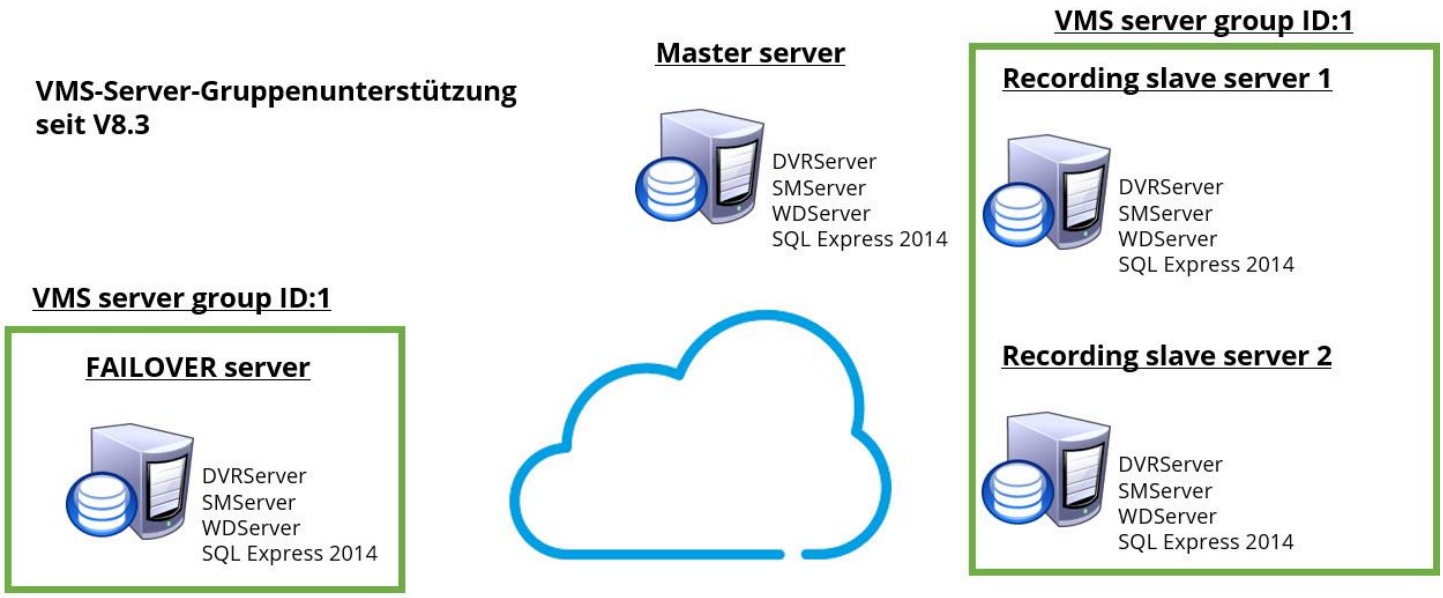
13.4 FAILOVER-PROZESS



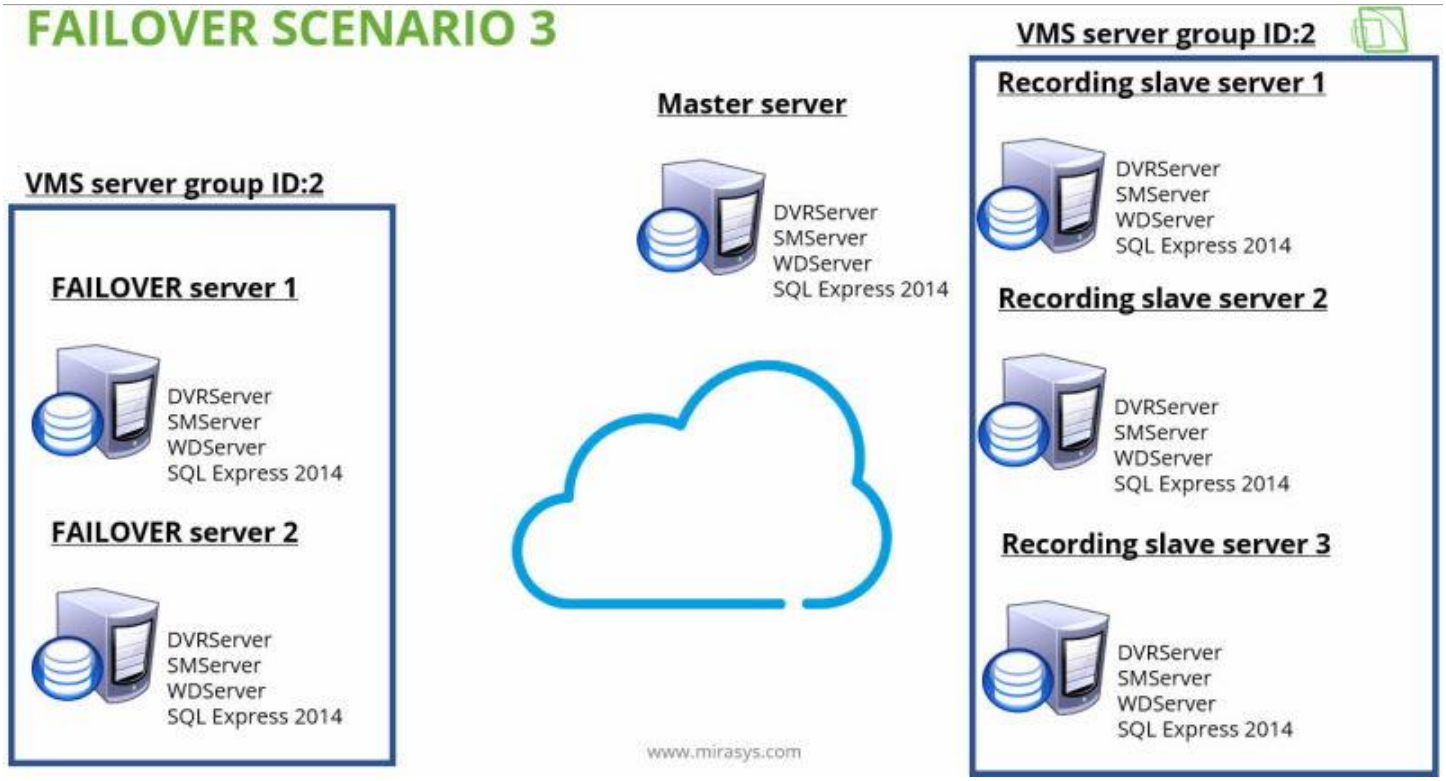
13.5 MINDESTENSZENARIO FÜR FAILOVER

13.6 FAILOVER-SZENARIO 2

VMS-Server-Gruppenunterstützung seit V8.3



13.7 FAILOVER-SZENARIO 3



13.8 VMS-SERVERROLLEN

13.8.1 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.

13.8.2 VMS-Server-Rolle DEFEKT

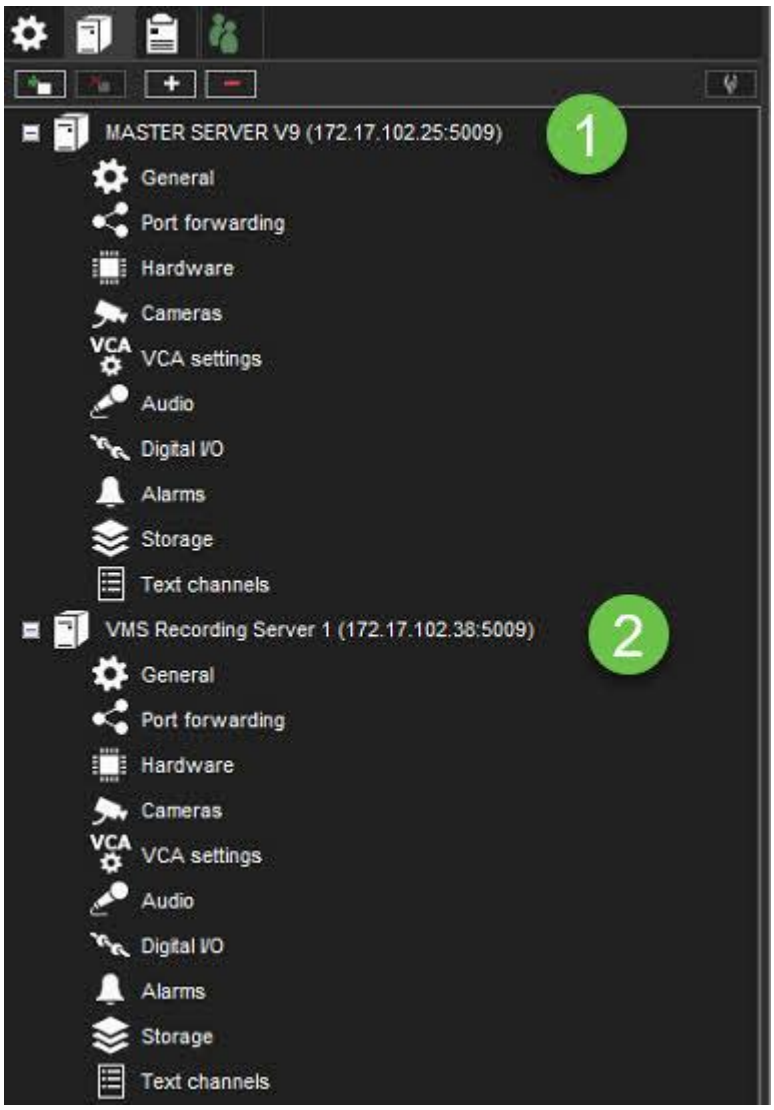
Die Gruppe Defekte VMS-Server zeigt den Verbindungsstatus an; die Einstellungen auf defekten Servern können nicht geändert werden.

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.

13.9 Starting point

Der Master-Server und 1 Aufzeichnungs-Slave-Server wurden dem System hinzugefügt



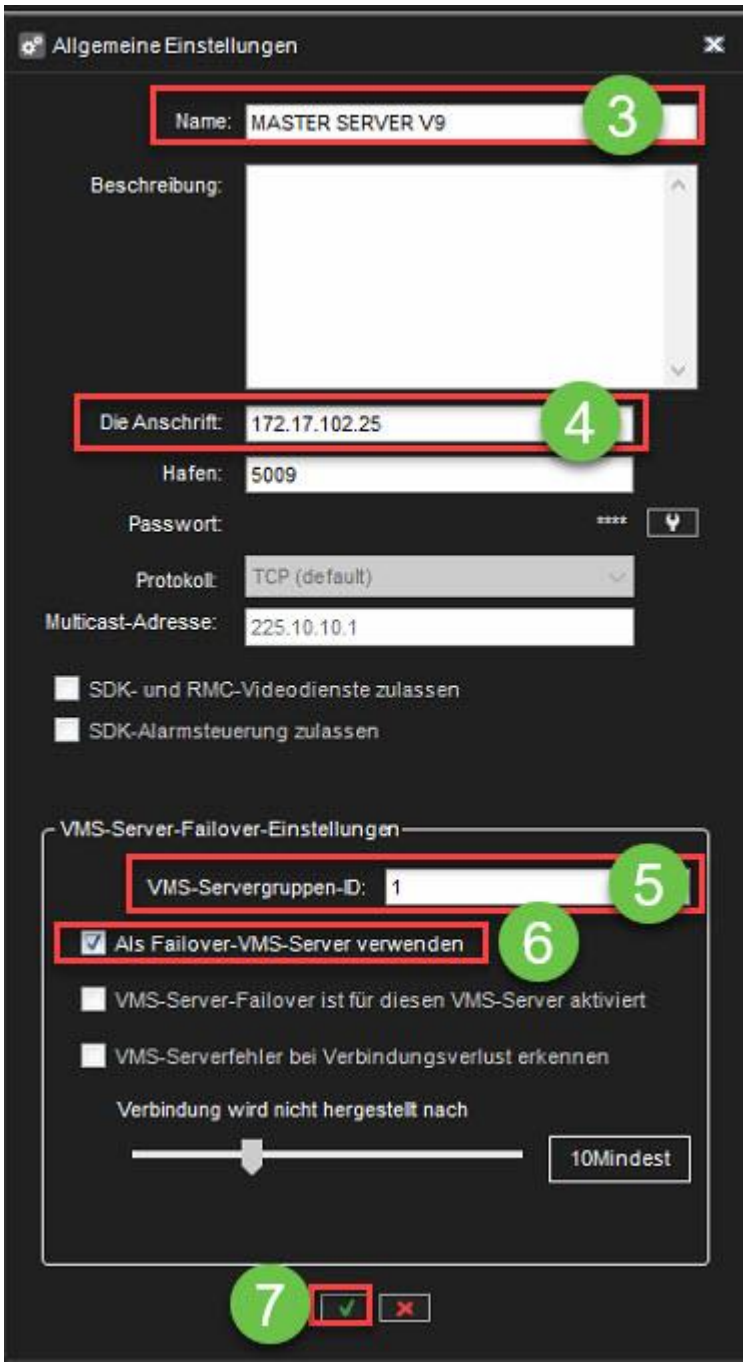
13.9.1 Aktivieren des VMS-Failover-Servers zum Aufzeichnungsserver

1. Öffnen Sie die Registerkarte **VMS-Server**
2. Wählen Sie den Slave-Server 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**

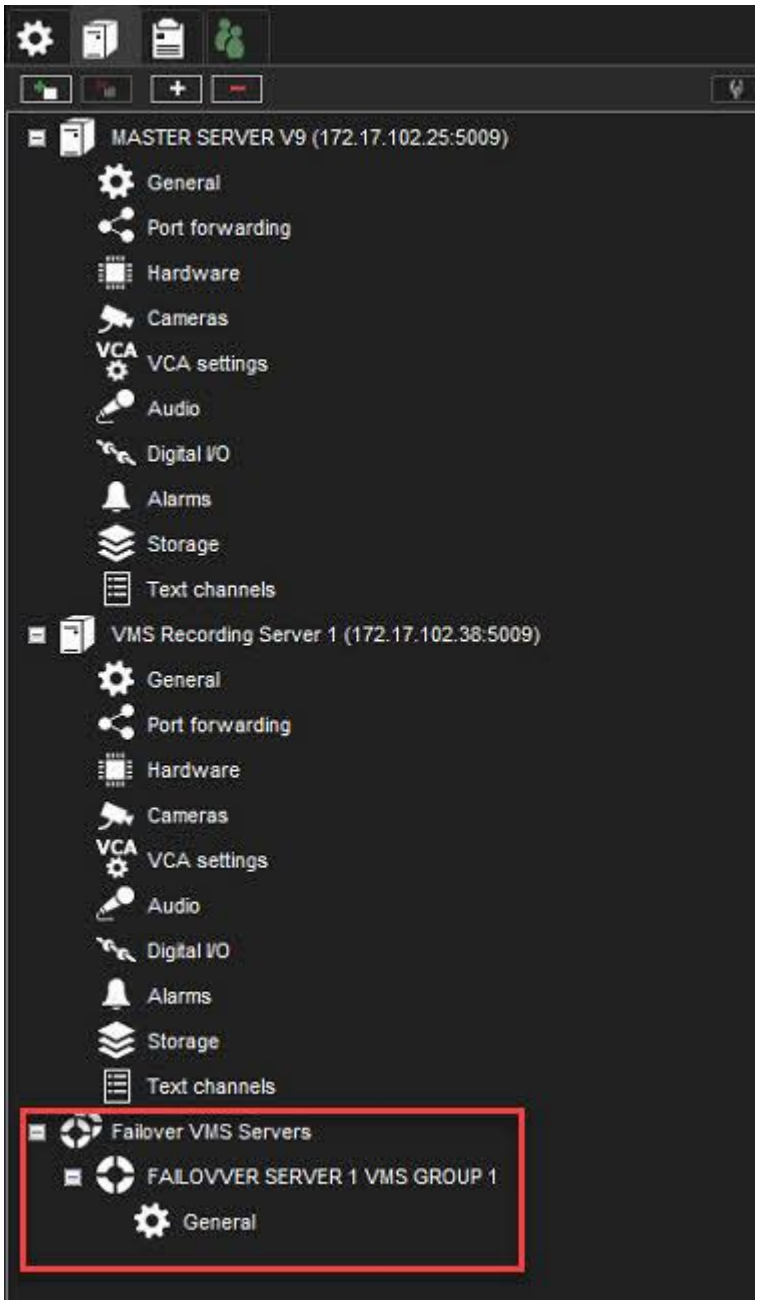
13.9.2 FAILOVER-Server hinzufügen

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



13.10 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 Mirasys Face Recognition

14.1 Einführung Face Recognition

Gesichtserkennung (Face Recognition, FR) dient der Identifizierung eines menschlichen Gesichts. Sie wird im VMS-System verwendet, um Ereignisse zu erhalten, wenn Gesichter in ausgewählten Videoströmen erkannt werden, und um zu erkennen, wenn bestimmte Personen im Video zu sehen sind. Zusammen mit der Mirasys-Listenverwaltung können Sie so zum Beispiel ein automatisches Erkennungssystem für den Zutritt einer Person zu einem Gebäude einrichten.

Beachten Sie, dass Anti-Spoofing in Version 9.6 nicht enthalten ist.

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

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

14.2 FR Datenschutz-Masken

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

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

14.3 FR-Verarbeitung, Ereignisse und Erkennung

14.3.1 Geräte

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

14.3.2 FR-Veranstaltungen

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

14.3.3 Visualisierung des erkannten Gesichts

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

14.4 FR Alarmauslöser und Konfiguration

14.4.1 Alarmauslöser

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

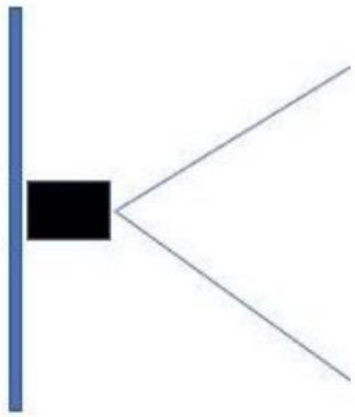
14.4.2 FR-Konfiguration

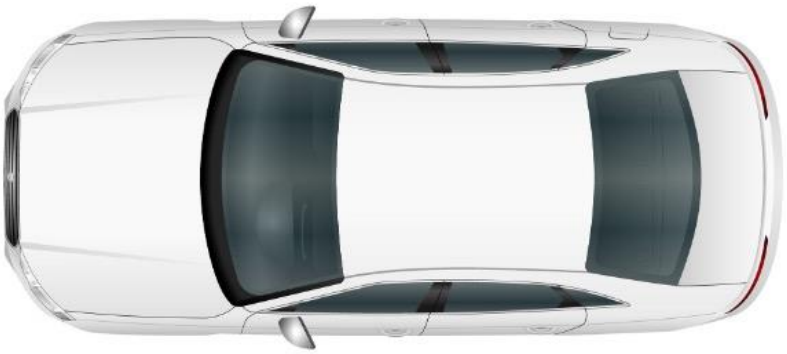
Der FR-Dienst kann in der Anwendung System Manager auf der Registerkarte FR-Einstellungen im Fenster Kameraeinstellungen konfiguriert werden.

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

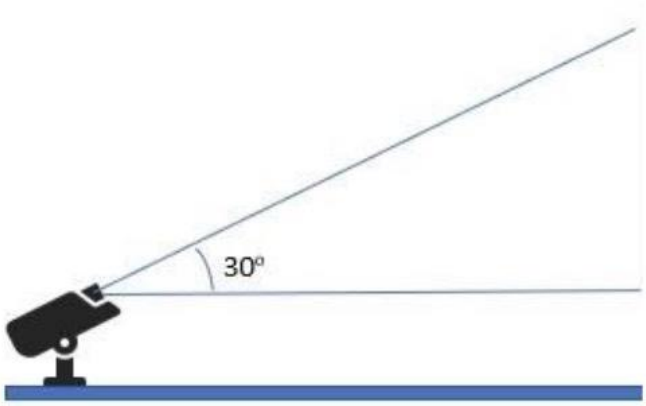
15 KAMERA-INSTALLATION LPR-LEITFADEN

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

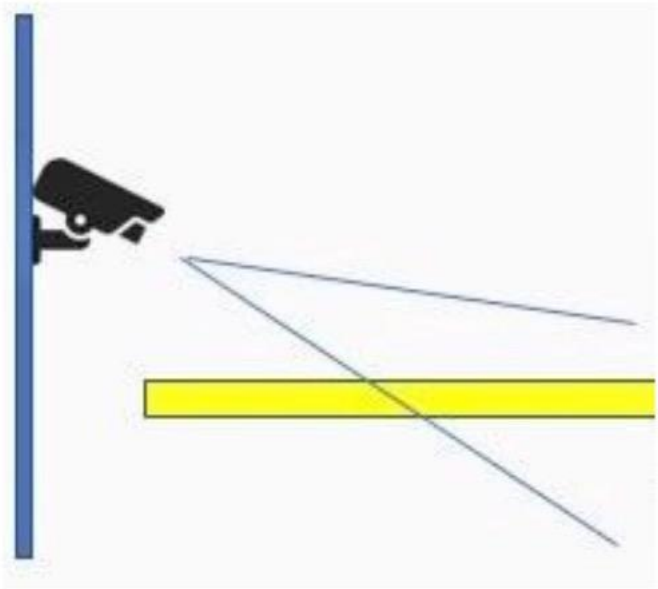




15.2 Wenn die Kamera am Straßenrand oder auf der Fahrbahn installiert ist, sollte der Winkel 30 Grad nicht überschreiten.



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



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

Höhe mindestens 50 Pixel

Breite mindestens 120 Pixel

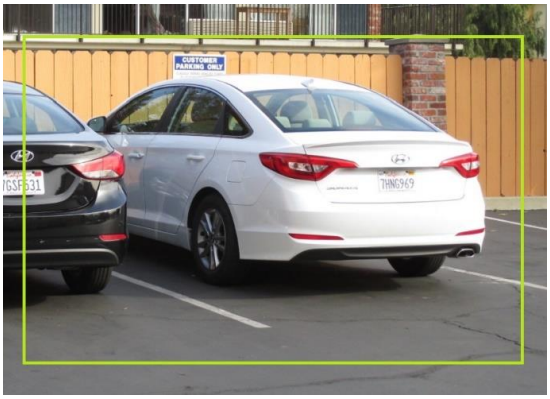
15.5 Der Neigungswinkel des Kennzeichens muss innerhalb von +/- 10 Grad liegen.

15.6 LPR-Einstellungen in der Anwendung System Manager

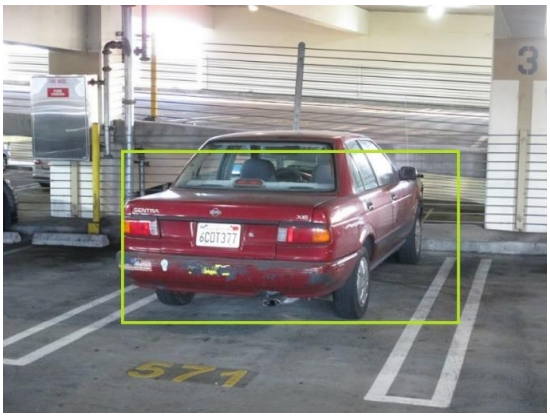
Stellen Sie sicher, dass die richtige Region (Amerika/Eurasien) ausgewählt ist.

15.6.1 Festlegung der Region von Interesse

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



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



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

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

15.6.2 Ermöglichung der Anerkennung von Ländern

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

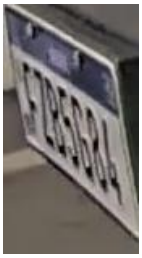
Das Format für das brasilianische Kfz-Kennzeichen ist beispielsweise "abc1d23".

15.7 Allgemeine Probleme und Lösungen

15.7.1 Unvollständiges Nummernschild

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

15.7.2 Blickwinkel macht Nummernschilder unleserlich



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

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

15.7.3 Scheinwerfer anderer Fahrzeuge reflektieren vom Nummernschild

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

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

15.7.4 Das Nummernschild ist zu klein

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

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

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

15.7.5 Das Nummernschild ist unscharf

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

Lösung 2: Erhöhen Sie die Beleuchtung des Bereichs.

15.7.6 Das Nummernschild ist überbelichtet

Lösung 1: Passen Sie die Bildeinstellungen der Kamera an.

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

16 Mirasys License Plate Recognition (LPR)

16.1 Einführung License Plate Recognition

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

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

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

16.2 LPR-Datenschutz-Masken

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

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

16.3 Land-Erkennung

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

16.3.1 Erkennung von Ländern mit Nummernschildern

Die Kennzeichenerkennung ist für Eurasien und Amerika verfügbar.

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

16.3.2 Typen von Nummernschildern

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

- antik
- diplomatisch
- Ausfuhr

- Militär
- provisorisch
- Vermietung
- Taxi
- Test
- Arbeit

16.4 LPR in Eurasien: Unterstützte Länder

16.4.1 Vorwahlen

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

- Österreich
- Deutschland
- Rumänien
- Slowenien
- Schweiz

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

Bitte beachten Sie, dass die Genauigkeit von Land zu Land unterschiedlich ist.
Ein Kennzeichen aus nicht unterstützten Ländern kann als eines der unten aufgeführten Länder erkannt werden. Zum Beispiel können einige Kennzeichen aus Tadschikistan als Kennzeichen aus Kasachstan erkannt werden.

16.4.2 Liste der unterstützten Länder in Eurasien

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

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

- Slowenien
- Spanien
- Schweden
- Schweiz
- Türkei
- Ukraine
- Vereinigtes Königreich
- Vatikan

16.5 LPR auf dem amerikanischen Kontinent: Unterstützte Länder

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

16.5.1 Länder und Staaten

Die unten aufgeführten Länder/Staaten werden unterstützt.

- Argentinien
- Bolivien
- Brasilien (altes und neues Kennzeichen)
- Kanada
- Alberta
- Britisch-Kolumbien
- Manitoba
- Ontario

- Quebec
- Saskatchewan
- Chile
- Kolumbien
- Mexiko
- Paraguay
- Peru
- Vereinigte Staaten
    - Alabama
    - Alaska
    - Arizona
    - Arkansas
    - Kalifornien
    - Colorado
    - Connecticut
    - Delaware
    - District of Columbia
    - Florida
    - Georgien
    - Hawaii
    - Idaho
    - Illinois

- Indiana
- Iowa
- Kansas
- Kentucky
- Louisiana
- Maine
- Maryland
- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio

- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee
- Texas
- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

- Uruguay
- Venezuela

16.6 LPR-Ereignisse, Ereignisse und Erkennung

16.6.1 Geräte

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

16.6.2 LPR-Ereignisse

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

16.6.3 Visualisierung des erkannten Kennzeichens

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

16.7 LPR Alarmauslöser und Konfiguration

16.7.1 Alarmauslöser

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

16.7.2 LPR-Konfiguration

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

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

17 Easy LPR

17.1 EASY LPR-Hauptfunktionen

- Live-Überwachung von einer Kamera gleichzeitig
- Kennzeichensuche von einer Kamera gleichzeitig
- Nummernlistenverwaltung
    - Schwarze Liste
    - Weiße Liste
- Kennzeichenlisten importieren und exportieren

- Hochladen der Kennzeichenliste zu den Kameras
- Digitale Ausgangssteuerung basierend auf:
    - Anderes Schild erkannt
    - Schwarzes Listenschild erkannt
    - Weißes Listenschild erkannt

Überprüfen Sie die unterstützten Kameras in der Liste der unterstützten Kameras.

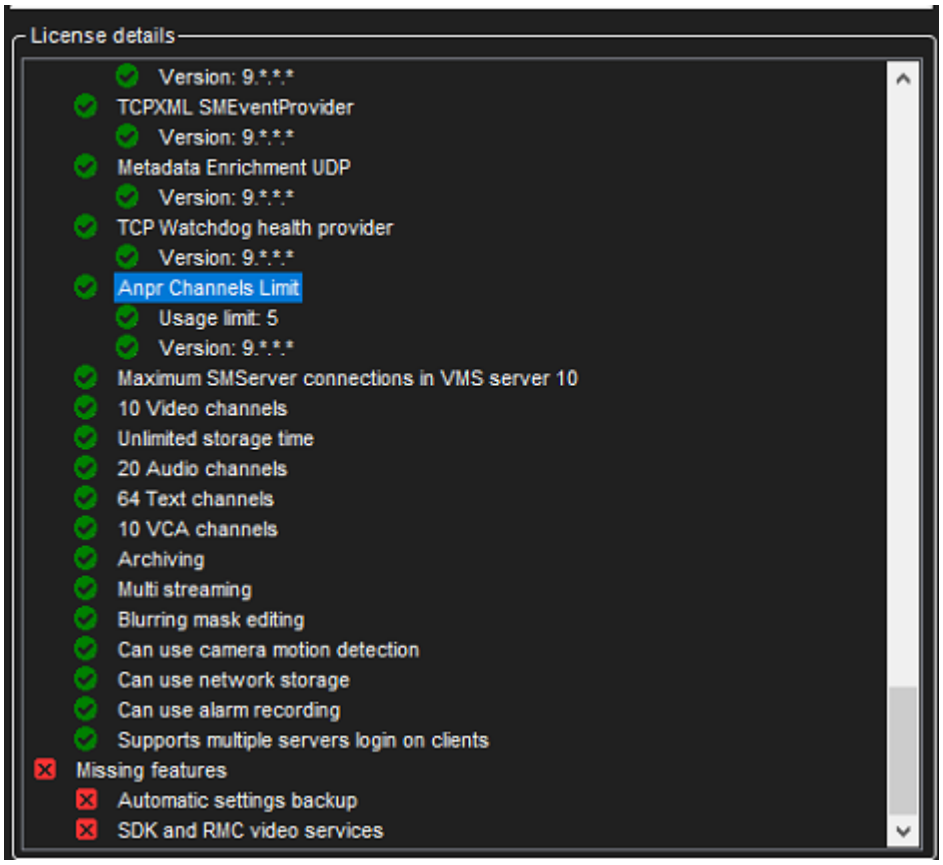
17.2 Konfigurationsprozess

1. Konfigurieren Sie die LPR-Funktionalität für die verwendeten Kameras. Weitere Informationen finden Sie auf der Website des Herstellers
2. Kameras zum Mirasys VMS hinzufügen
3. Überprüfen Sie, ob die Mirasys VMS-Lizenz LPR-Kameras unterstützt
4. Einfaches Easy LPR aktivieren

17.3 Lizenzierung

Die Mirasys VMS-Serverlizenz definiert, wie viele ANPR-Kanäle hinzugefügt werden können.

Der Name der Funktion lautet **Anpr Channels limit** and controlable value name **Usage limit**



17.4 Aktivieren von Easy LPR

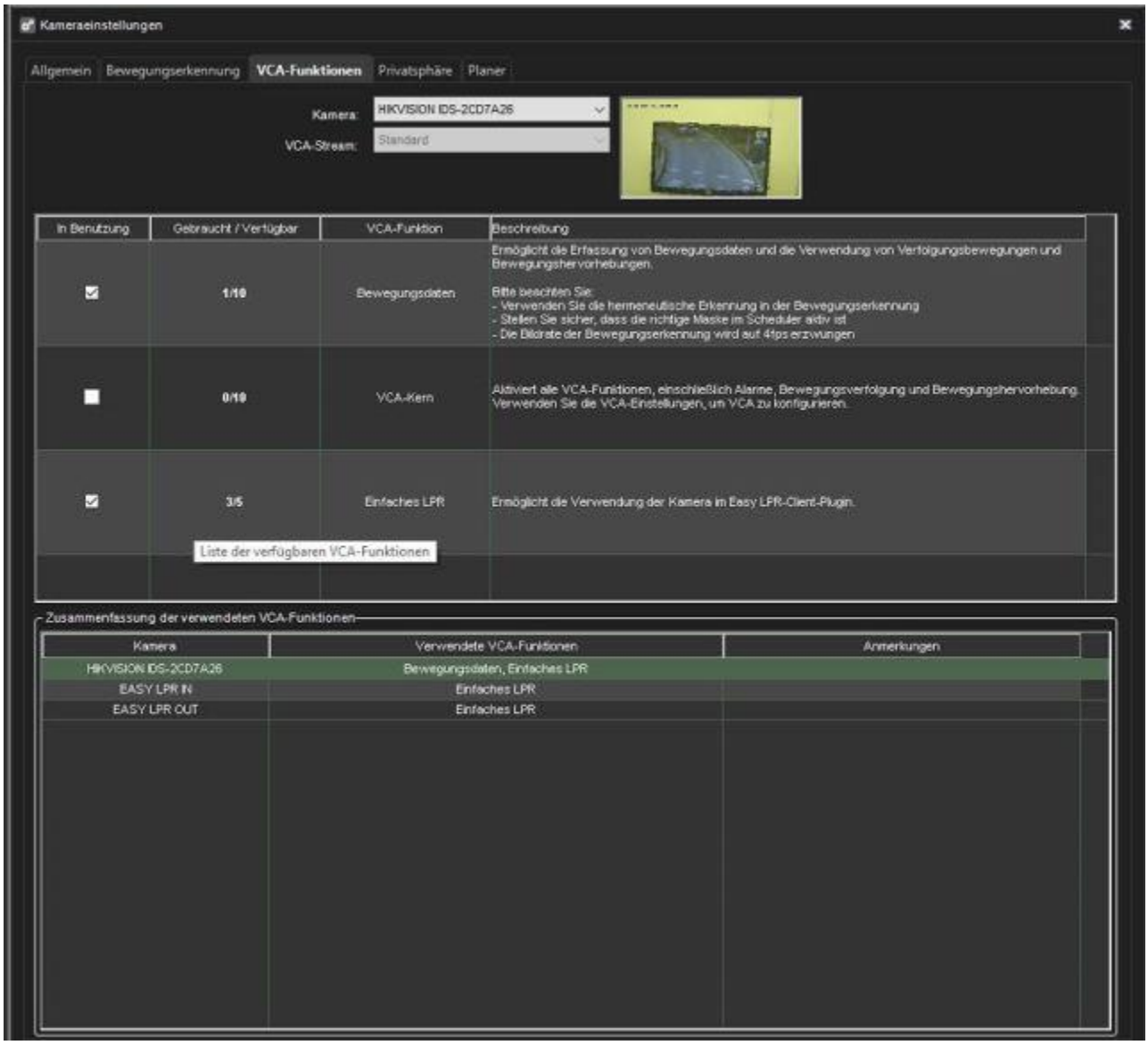
1. Öffnen Sie **VMS-Server**
2. Öffnen Sie **Kameras**

3. Klicken Sie auf **VCA-Funktionen**

4. Wählen Sie die LPR-Kamera

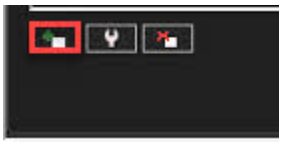
5. **Easy LPR** aktivieren

6. Klicken Sie auf **Speichern**



17.5 Erstellen eines Alarms aus einem Easy LPR-Ereignis

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



4. Geben Sie alle erforderlichen Informationen in der Registerkarte **Allgemein** ein

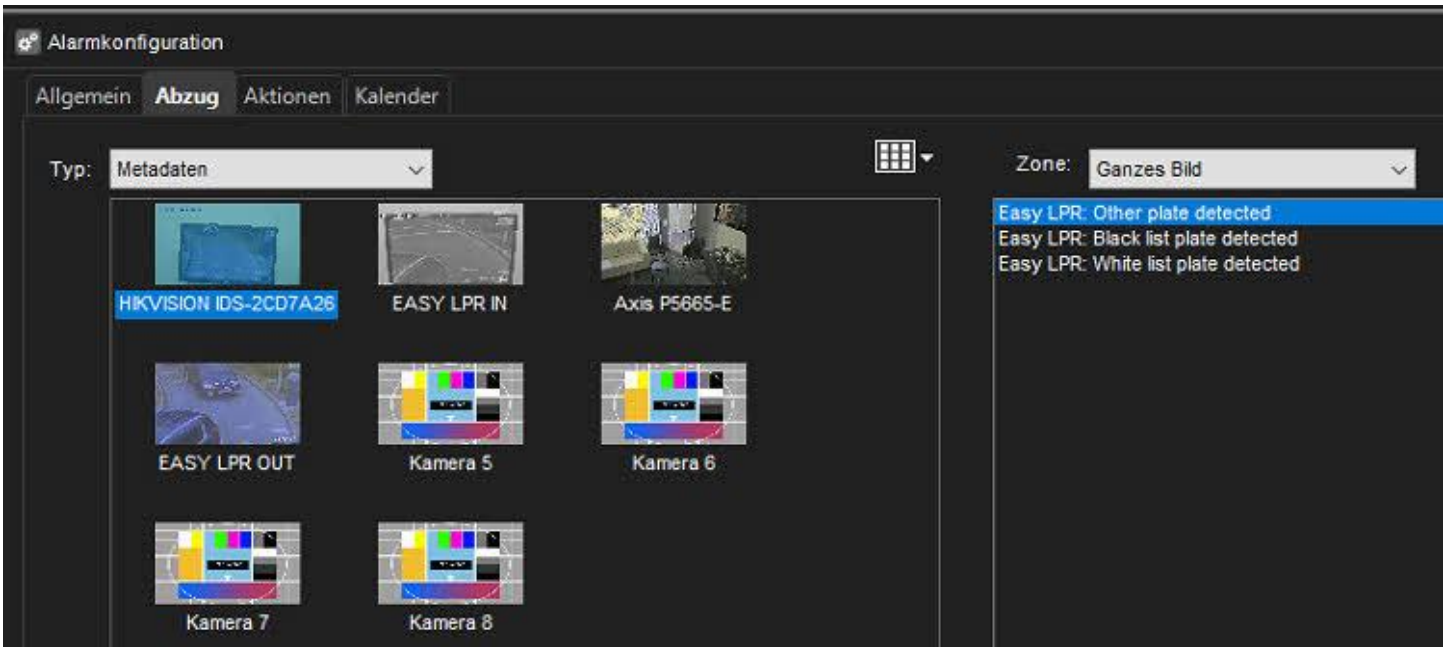
5. Öffnen Sie **Abzug** Tag

6. Triggertyp auswählen **Metadaten**

7. Wählen Sie die LPR-Kamera

8. Wählen Sie das richtige Ereignis aus:

- **Easy LPR: Andere Platte erkannt**
- **Easy LPR: Schwarzes Listenschild erkannt**
- **Easy LPR: Weiße Liste-Kennzeichen erkannt**



9. Geben Sie die Aktionen der Alarme ein

10. Kalender einstellen

11. Überprüfen Sie die Gesamtansicht des Alarms

12. Klicken Sie auf **OK** um eine Alarmerstellung zu bestätigen

18 MIRASYS LIST MANAGEMENT

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

Der LM-Dienst hat die folgenden Fähigkeiten:

- Speichern von Identitäten und Identitätslisten in der Datenbank
- Empfangen und Speichern von LPR- und FR-Ereignissen in der Datenbank
- Abgleich von erkannten Nummernschildern und Gesichtern mit definierten Identitäten und Identitätslisten
- Suche nach LPR- und FR-Ereignissen in der Datenbank anhand von Suchparametern
- Senden von LPR- und FR-Ereignissen in Echtzeit für Clients und Rekorder

- Senden von LPR- und FR-Ereignissen an den VMS-Server zur Verarbeitung
- Benachrichtigung von Kunden und Rekordern über Änderungen in Identitäten und Identitätslisten
- Ermöglicht die Integration von Kennzeichen- und Gesichtserkennungen

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

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

19 Mirasys Objektintunnistus (OR)

19.1 Objektintunnistus Johdanto

Objektintunnistushaku antaa operaattoreille mahdollisuuden etsiä tallenteista sekä henkilöiden että ajoneuvojen ominaisuuksia. Objektintunnistushaku etsii seuraavilla kriteereillä: missä (mitkä kamerat), milloin (aikaväli) ja mitä (ihmiset tai ajoneuvot ja niiden ominaisuudet).

Henkilöiden osalta haettavissa olevat attribuutit ovat ylävartalon vaatteiden väri (musta, valkoinen, harmaa, sininen, vihreä, punainen, keltainen), alavartalon vaatteiden väri (musta, sininen, valkoinen, harmaa, ruskea, vihreä), onko henkilöllä laukku (yleinen) ja onko hänellä päähine (yleinen).

Ajoneuvot voidaan tutkia tyypin (henkilöauto, moottoripyörä, pakettiauto, kuorma-auto, polkupyörä tai linja-auto) ja värin (musta, sininen, ruskea, harmaa, vihreä, oranssi, punainen, valkoinen ja keltainen) mukaan.

19.2 OR Service-Installation

Für OR müssen Sie die Pakete ORService und ODSService installieren.

19.2.1 Anforderungen

- Administratorrechte

- Object Recognition-Lizenz auf dem VMS-Server

19.2.2 Installation

1. Laden Sie die neueste Version aus dem Extranet herunter.
2. Entpacken Sie dieses Beispiel in den Ordner C:\temp.
3. Starten Sie die Installation durch Doppelklick auf die Installationsdatei.
4. Klicken Sie auf Installieren, um fortzufahren.
5. Klicken Sie auf Weiter, um fortzufahren.
6. Ändern Sie bei Bedarf den Installationsort, wenn nicht, klicken Sie auf Weiter, um fortzufahren.
7. Ändern Sie den HTTP-Port des Dienstes, die Adresse und den Port des Hauptservers (Master) sowie die Adresse und den Port der Ereigniswarteschlange, falls erforderlich.

Der HTTP-Port ist standardmäßig 8092
Der Hauptserver (Master) verwendet standardmäßig Port 8082
Die Ereignis-Warteschlange verwendet standardmäßig Port 5672. Die Ereignis-Warteschlange wird mit dem ODSService-Paket installiert.

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

Die Installation wird einige Zeit in Anspruch nehmen, bis sie abgeschlossen ist.

Die Erstellung von Modellen kann bis zu 30 Minuten dauern. Dies hängt davon ab, wie leistungsfähig die Grafikkarte ist, die verwendet wird.

1. Klicken Sie auf Fertig stellen, um fortzufahren.
2. Klicken Sie auf Schließen, um die Installation zu beenden.

Der Objekterkennungsdienst ist nun auf dem Server installiert und einsatzbereit.