MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE

Table of Contents

1. Administratorhandbuch v9

Nächste

1.1. Übersicht über dieses Handbuch

Dieses Handbuch richtet sich an diejenigen, die ein Mirasys-System einrichten.

Es zeigt, wie Sie dem System Server hinzufügen und deren Einstellungen ändern, Benutzerkonten und Benutzerprofile hinzufügen und das System überwachen.

oben Vorherige Nächste

1.2. Technischer Support

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

oben Vorherige Nächste

1.3. Was ist die Mirasys VMS-Software?

Die Mirasys-Software ist ein verteiltes digitales Videomanagementsystem (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 von analogen, digitalen oder hybriden (bestehend aus analogen und digitalen) Überwachungssystemen.

Eine zentralisierte Überwachungssystemdomäne kann aus bis zu 150 lokalen oder entfernten VMS-Servern bestehen.

Die Mirasys-Software wird separat verkauft und ist Teil des Mirasys-Videomanagementsystems, das sowohl aus der Software als auch der VMS-Server-Hardware besteht.

Bitte wenden Sie sich an Ihren Mirasys-Lieferanten, um Informationen zur Mirasys-Software oder -Hardware zu erhalten.

oben Vorherige Nächste

1.3.1. 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

oben Vorherige Nächste

1.3.2. 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)

oben Vorherige Nächste

1.3.3. Master-Server

In einem vernetzten System muss einer der Server als Master-Server eingestellt werden.

Ein Master Server ist der zentrale Server eines Überwachungssystems.

Alle anderen VMS-Server verbinden sich damit und alle Client-Anwendungen kommunizieren über den Master-Server.

Wenn das System nur einen Server enthält, ist dieser Server der Master-Server.

Bei mehreren Servern kann der Master Server frei eingestellt werden.

Es wird empfohlen, dass der Master-Server allein 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.

oben Vorherige Nächste

1.3.4. 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

oben Vorherige Nächste

1.3.5. Netzwerkanforderungen

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

oben Vorherige Nächste

1.4. 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.

oben Vorherige Nächste

1.5. 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-Servereinstellungen auf der Registerkarte System.*

Auf diese Weise können Sie beispielsweise die Einstellungen wiederherstellen, wenn eine Festplattendatei

oben Vorherige Nächste

1.6. Einloggen

In diesem Abschnitt wird beschrieben, wie Sie sich bei System Manager an- und abmelden.

Nur Systemadministratoren oder Benutzer mit Überwachungsrechten dürfen sich beim System Manager anmelden.

Standard-Benutzername und -Passwort

Nutzername: Admin

Passwort: 0308

Der Standard-Benutzername und das Standard-Passwort sollten auch in geschlossenen Netzwerken nicht verwendet werden

Bitte stellen Sie sicher, dass der Standardbenutzername und das Standardkennwort nicht verwendet werden, nachdem das System installiert wurde.

So melden Sie sich beim Systemmanager an:

Führen Sie einen der folgenden Schritte aus:

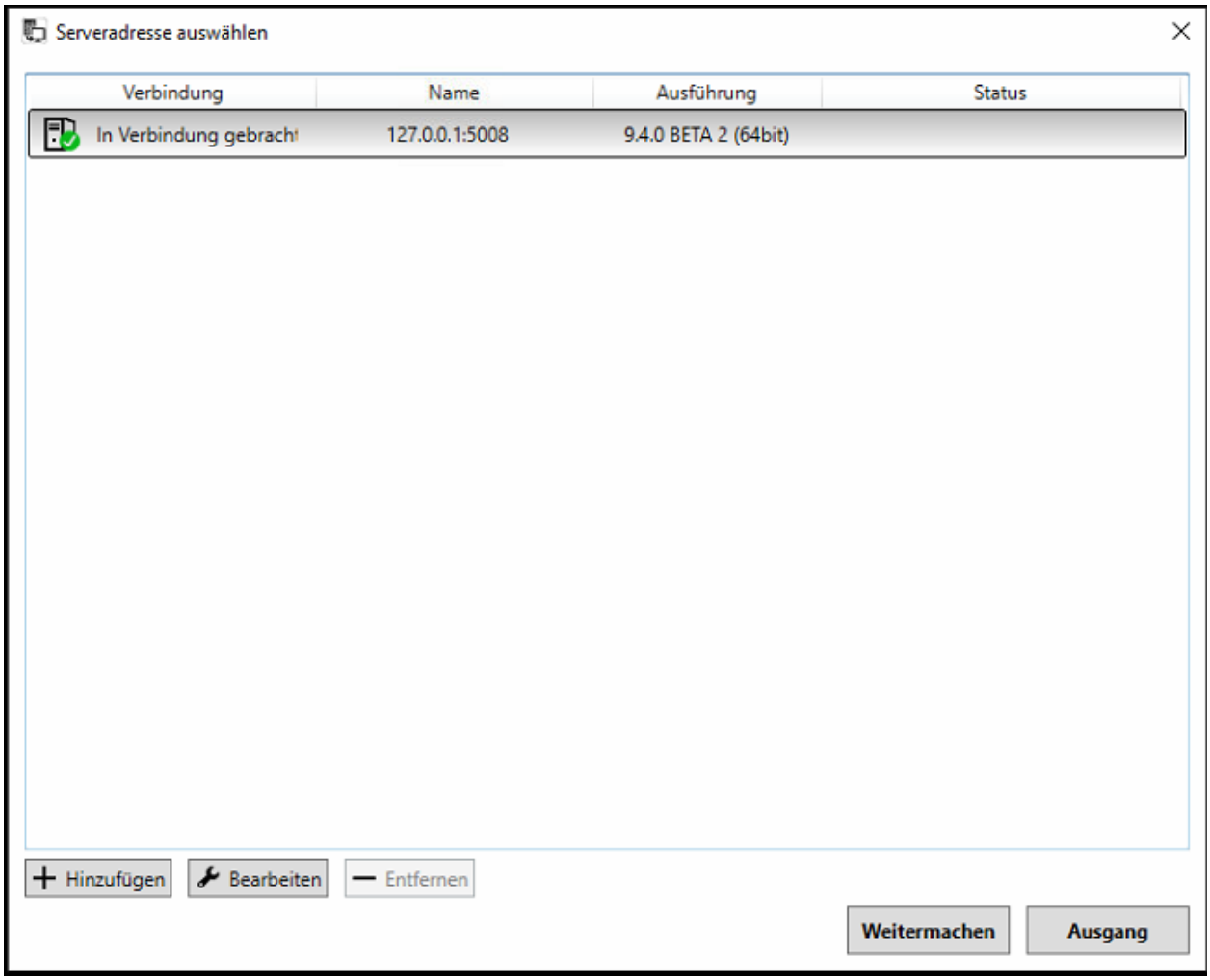
- Klicken Sie auf Start, zeigen Sie auf Programme und dann auf DVMS.
- Klicken Sie auf Start, zeigen Sie auf Programme und dann auf DVMS. Klicken Sie auf Systemmanager

Bei Systemen mit nur einer konfigurierten Master-Server-Adresse wird der Anmeldebildschirm des System-Managers angezeigt.

Bei Systemen mit mehreren Mastern, konfigurierten Adressen oder wenn der Benutzer in der ersten Startphase die Taste „Löschen“ drückt, wird der Bildschirm zur Standortauswahl angezeigt.

Der Benutzer kann Masterserveradressen hinzufügen, entfernen oder bearbeiten oder einen Server auswählen, um sich auf diesem Bildschirm anzumelden.

Nach Auswahl eines Servers und Drücken der Schaltfläche „Weiter“ gelangt ein Benutzer zum Anmeldebildschirm.



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 jeweils nur eine System Manager-Anwendung ausführen.

Es ist nicht möglich, den System Manager gleichzeitig mit mehreren Servern zu verbinden.

Um eine Verbindung zu einem anderen Master-Server herzustellen, verlassen Sie den aktuellen Master und wählen Sie einen anderen Master-Server aus dem Site-Auswahlbildschirm.

oben Vorherige Nächste

1.6.1. 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*

oben Vorherige Nächste

1.7. Management-Benutzeroberfläche

Die System Manager-Benutzeroberfläche

Die Benutzeroberfläche von System Manager enthält diese Elemente:

Menüleiste

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

Instandhaltung

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

Hilfe

über

um Informationen über die Programmversion anzuzeigen.

und dann **Hilfethemen**, um das Online-Handbuch zu verwenden.

oben Vorherige Nächste

1.8. System

Auf der Registerkarte System können Sie Systemeinstellungen bearbeiten und sichern, das System überwachen und Diagnoseinformationen zum Kurs untersuchen.

Sie können auf dieser Registerkarte auch Lizenzschlüssel für Server ändern, z. B. weitere Kamerakanäle hinzufügen und eine neue IP-Kamera, Metadaten und Client-Plugin-Treiber installieren.

Außerdem können Sie den Software-Watchdog konfigurieren.

Die Registerkarte enthält diese Werkzeuge:

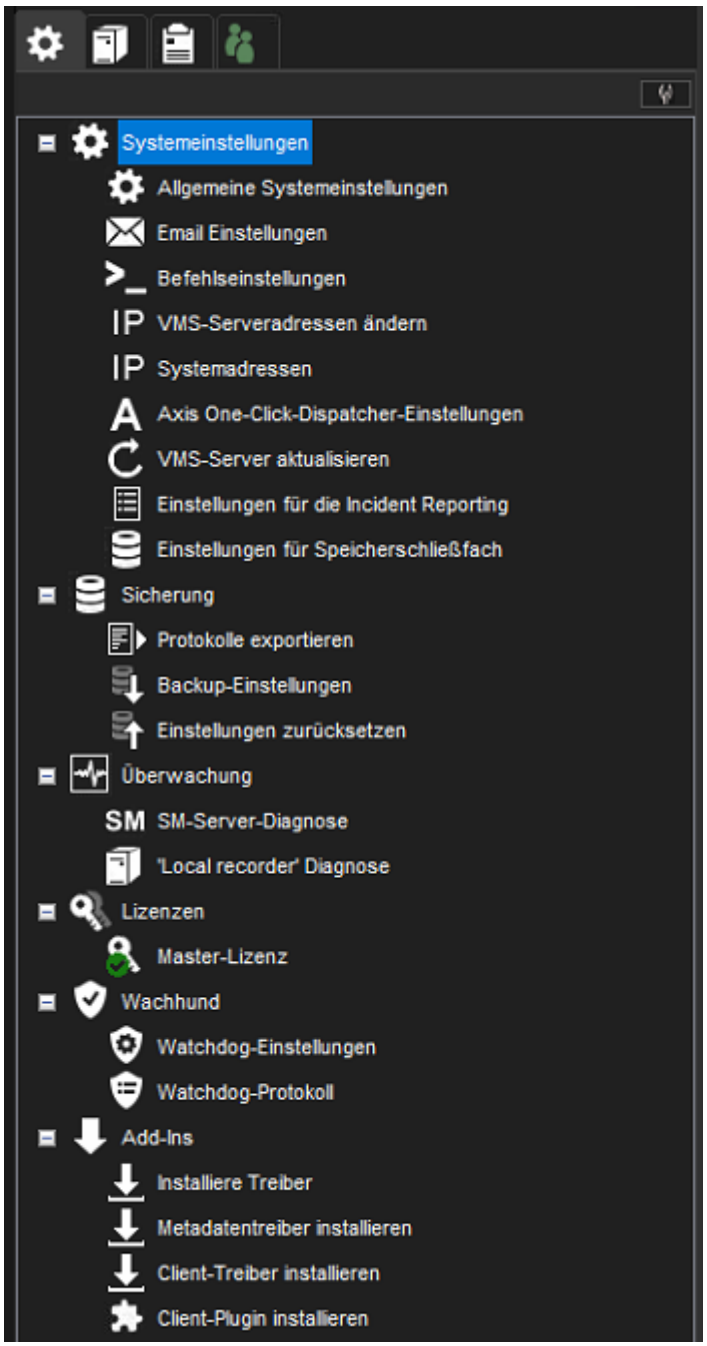
- Systemeinstellungen
- Allgemeine Systemeinstellungen
- Email Einstellungen
- Befehlseinstellungen
- VMS-Serveradressen ändern
- Systemadressen
- VMS-Server aktualisieren
- Sicherung
- Protokolle exportieren
- Backup-Einstellungen
- Einstellungen zurücksetzen
- Überwachung
- SM-Server-Diagnose
- Lokale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

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

- Klicken Sie auf das Werkzeug und dann auf Bearbeiten
- Doppelklicken Sie auf das Werkzeug
- Ziehen Sie das Werkzeug von der Registerkarte System in den Arbeitsbereich

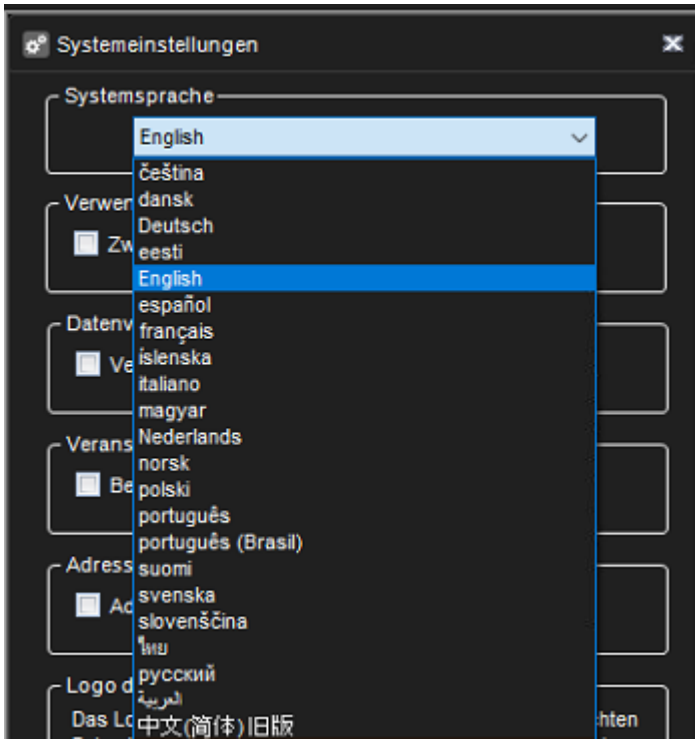
oben Vorherige Nächste

1.8.1. Systemeinstellungen



oben Vorherige Nächste

1.8.1.1. Allgemeine Systemeinstellungen



In diesem Abschnitt können Sie Folgendes steuern:

- Systemsprache
- Die Passwortnutzung

Es ist möglich, das System so zu konfigurieren, dass von allen Benutzern zwei separate Passwörter verlangt werden.

Dies geschieht durch Aktivieren der Option „Zweites Passwort verwendet“ in den allgemeinen Systemeinstellungen

Wenn dieser Modus ausgewählt ist, müssen alle Benutzer zwei Passwörter eingeben.

Das standardmäßige zweite Kennwort ist leer. Diese Funktion ermöglicht es, einzuschränken, dass keine einzelne Person Videos alleine überprüfen kann.

Wenn einer Person ein Passwort und einer anderen Person das andere Passwort bekannt ist, müssen beide Personen bei der Überprüfung von Videos vorlegen.

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

oben Vorherige Nächste

1.8.1.2. 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.

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.

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

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

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

Andere verfügbare Aktionen:

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

Mit dem Pfeil  können Personen aus Gruppen entfernt werden

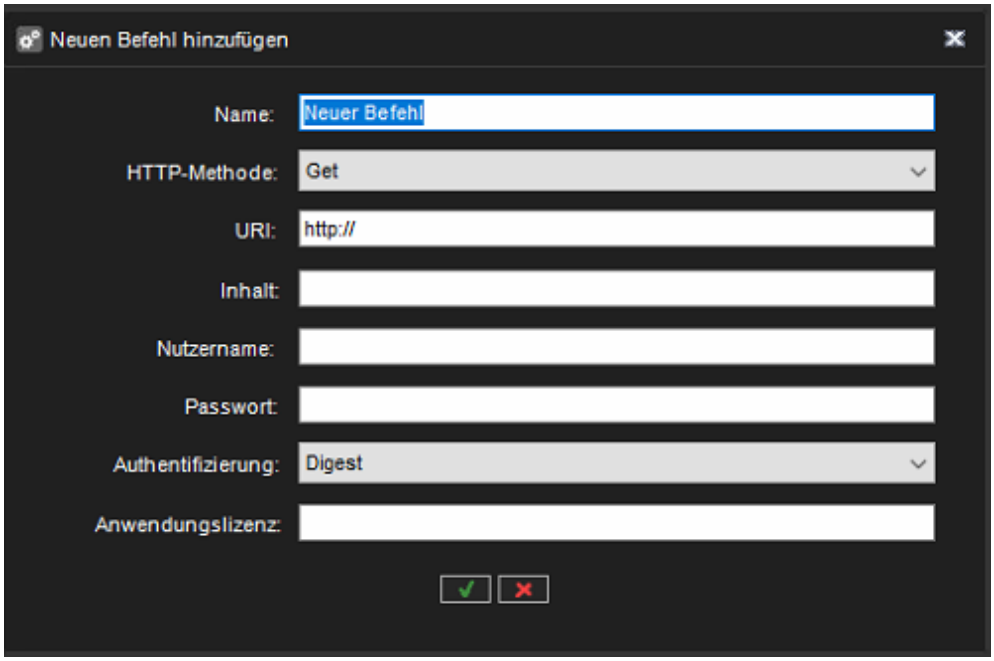
Personen und Gruppen können mit der  -Taste entfernt werden.

Test-E-Mail kann mit der Schaltfläche  a an eine ausgewählte E-Mail-Adresse gesendet werden, wobei die im E-Mail-Einstellungsdialog definierten Einstellungen verwendet werden.

oben Vorherige Nächste

1.8.1.3. Befehlseinstellungen

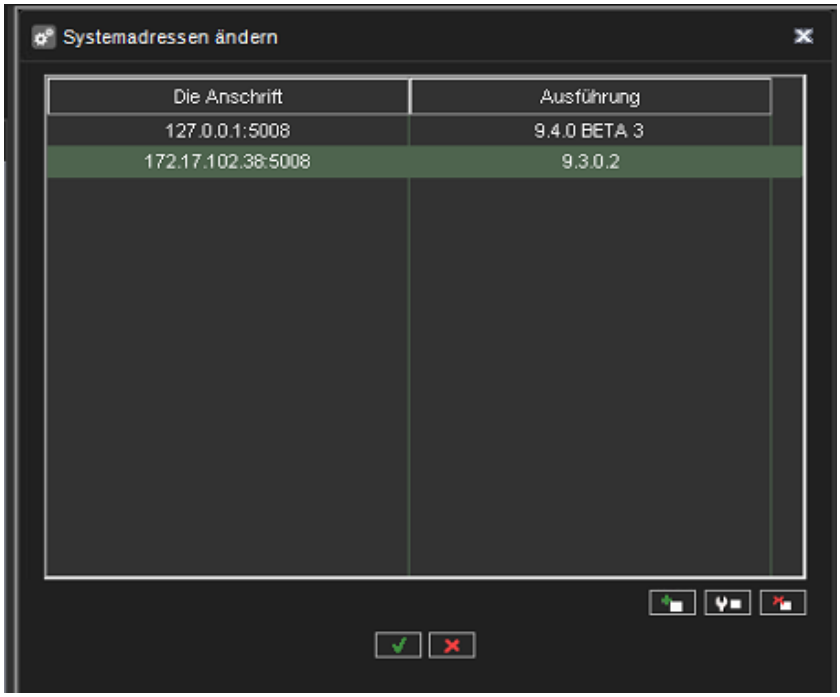
Befehlseinstellungen werden für das Senden von HTTP-Befehlen verwendet



oben Vorherige Nächste

1.8.1.4. 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:

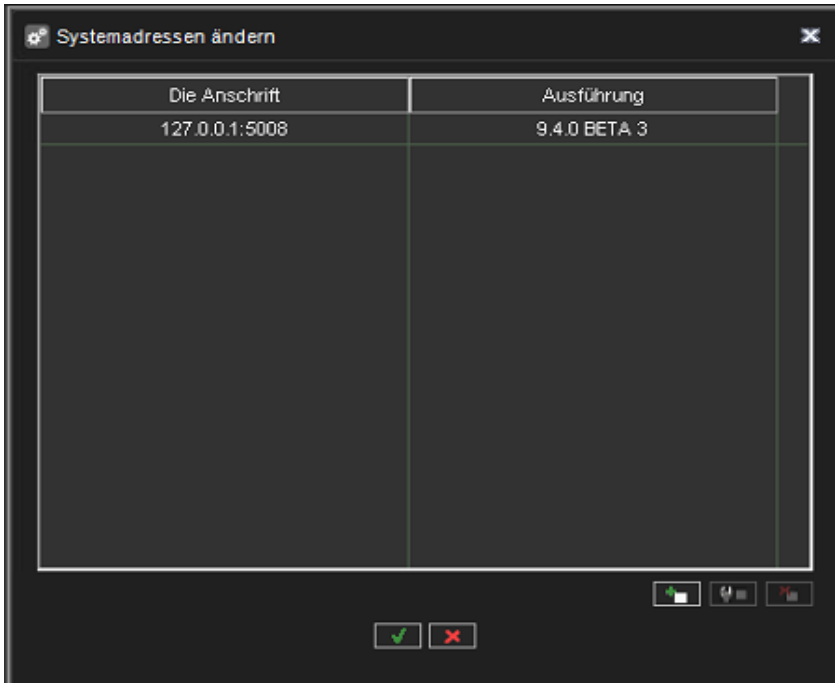
1. Öffnen Sie auf der Registerkarte System die Option VMS-Serveradressen ändern
2. Klicken Sie auf den Namen des Servers mit der geänderten IP-Adresse.
3. Klicken Sie auf **VMS-Serveradresse ändern**  .
4. Geben Sie die neue IP-Adresse oder den DNS-Namen des Servers in das Feld Neue VMS-Serveradresse ein.
5. **OK** klicken

oben Vorherige Nächste

1.8.1.5. 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 Masterserveradressen definieren, mit denen die Clientanwendungen eine Verbindung herstellen können.

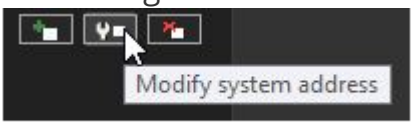
Die Adressen können als IP-Adressen (z. B. *http://195.168.0.11*) oder DNS-Namen (z. B. *http://www.example.com*) angegeben werden.

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.*

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

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

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**  .

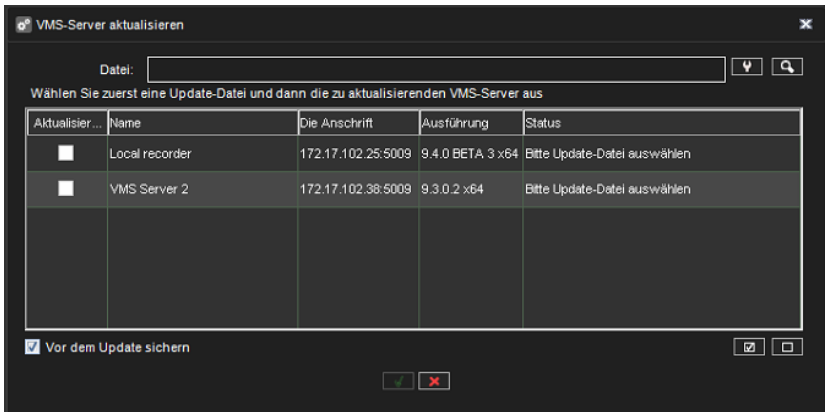
oben Vorherige Nächste

1.8.1.6. Axis One-Click-Dispatcher-Einstellungen

oben Vorherige Nächste

1.8.1.7. 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



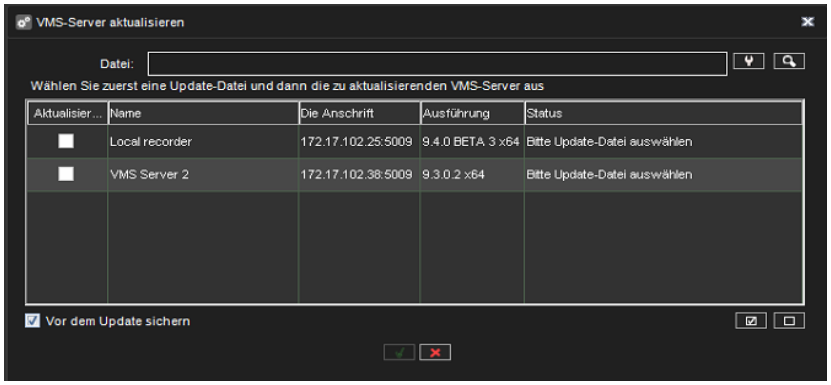
Um Server zu aktualisieren, wählen Sie zuerst die Installationsdatei mit der  -Taste aus.

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

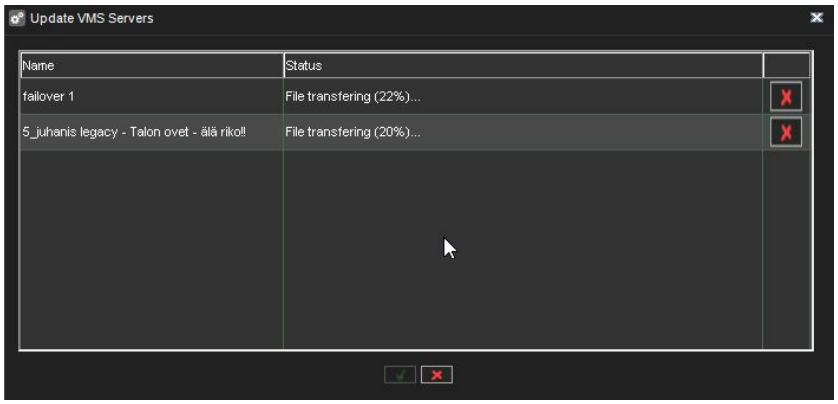
Notiz: *Bei einem Upgrade einer Hauptversion, beispielsweise von VMS 6. x auf 7. x, ist es in der Regel erforderlich, zuerst die Serverlizenzen und erst danach die VMS-Software zu aktualisieren.*

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 der Aktualisierung eine Sicherung durchführen möchten.



Durch Auswahl der Schaltfläche 1 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.

oben Vorherige Nächste

1.8.1.8. 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.

Unternehmensinformationen

- Name der Firma
- Firmenanschrift
- Firmenlogo

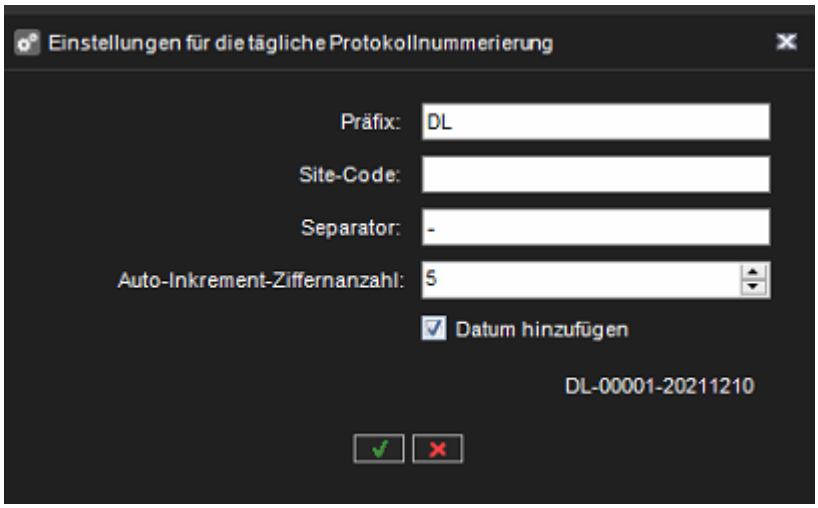
Berichtsnummerierung

Details zur Nummerierung von Vorfällen

- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen

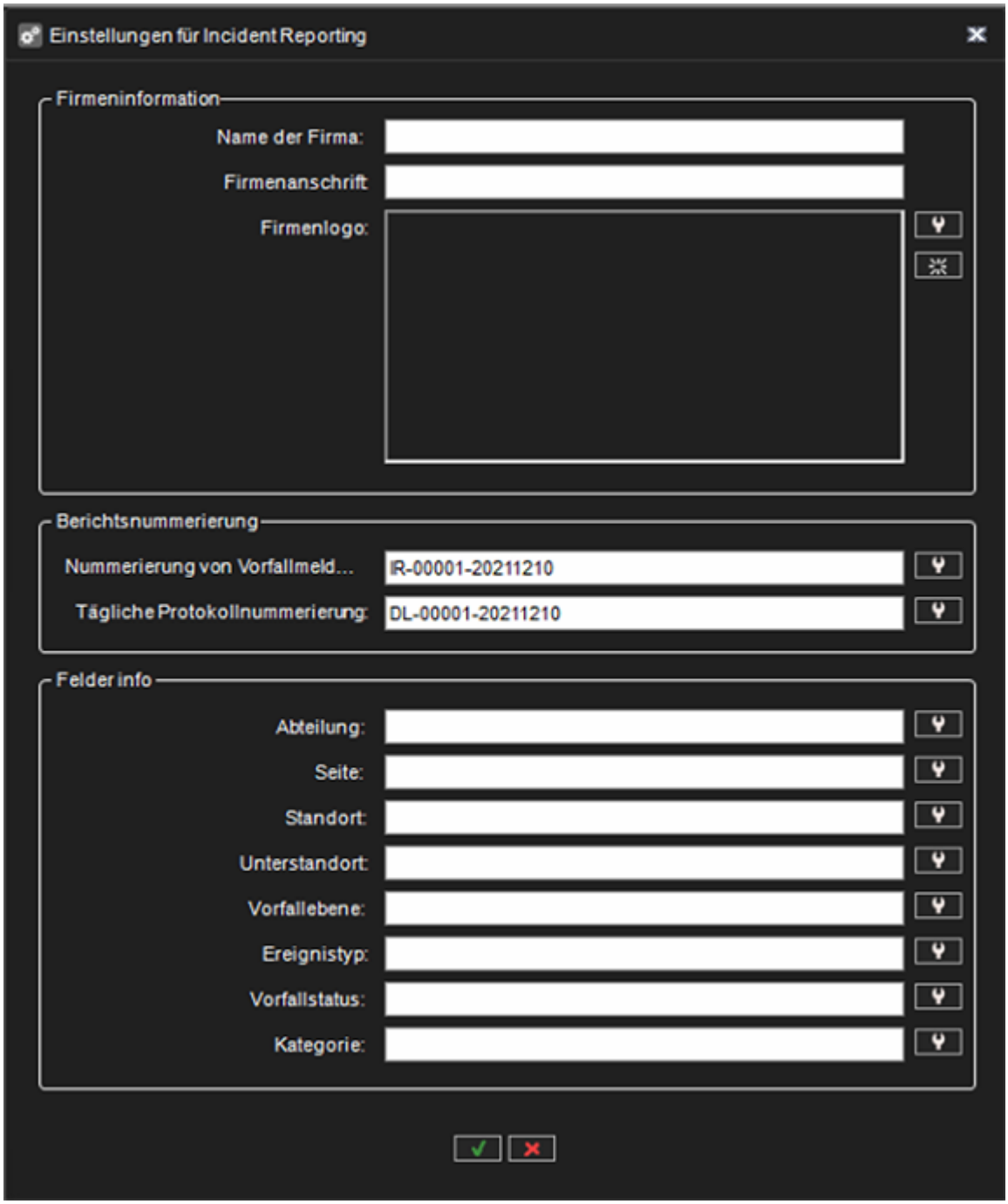
Details zur Nummerierung des Tagesprotokolls:

- Präfix
- Site-Code
- Separator
- Autoinkrementierziffern zählen



Felder info

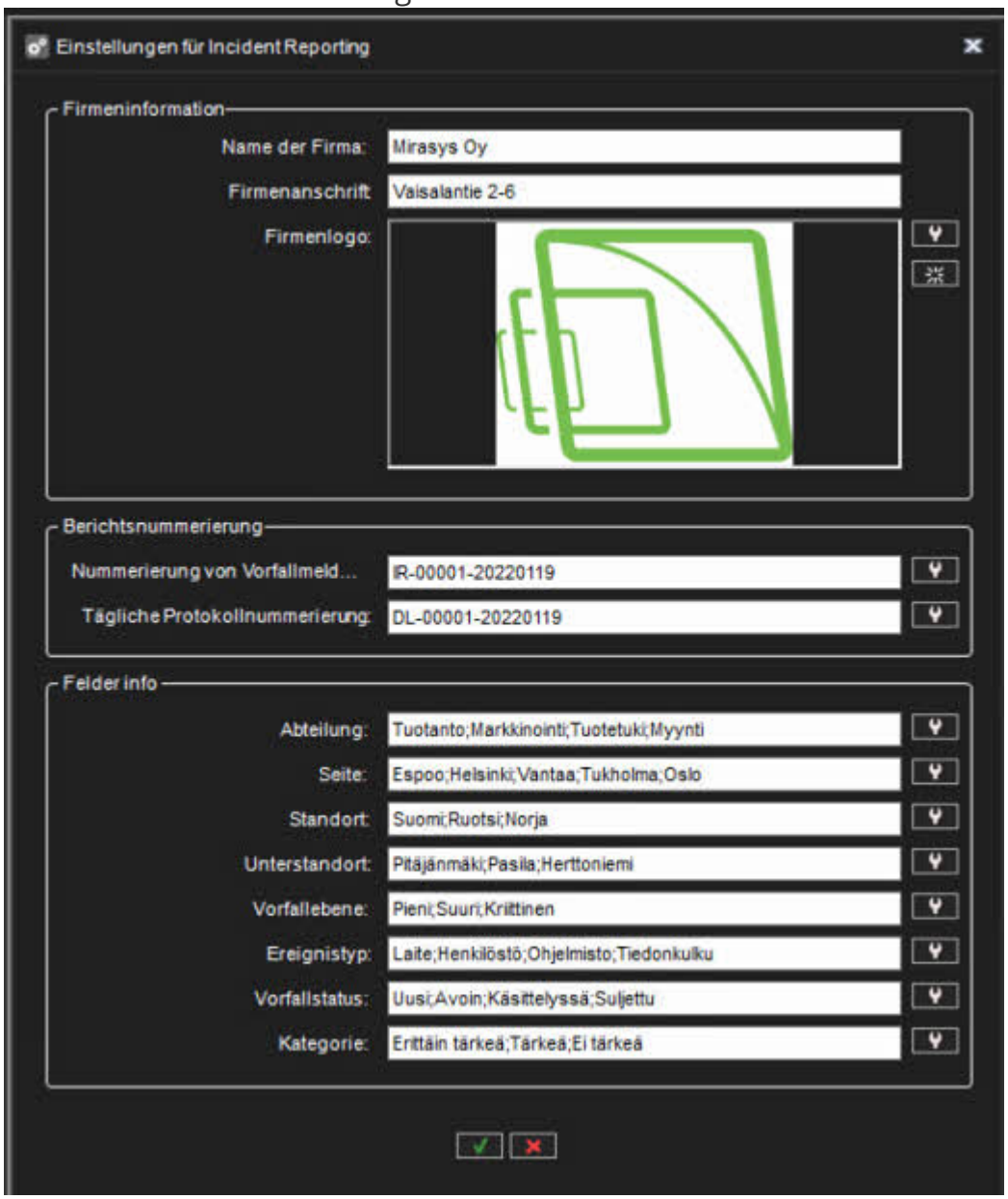
- Abteilung
- Seite
- Standort
- Unterstandort
- Vorfall
- Vorfalltyp
- Vorfallstatus
- Kategorie



oben Vorherige Nächste

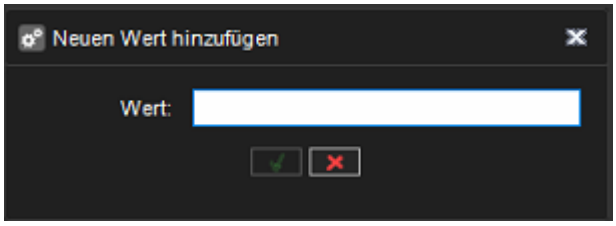
1.8.1.8.1. Werte hinzufügen

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

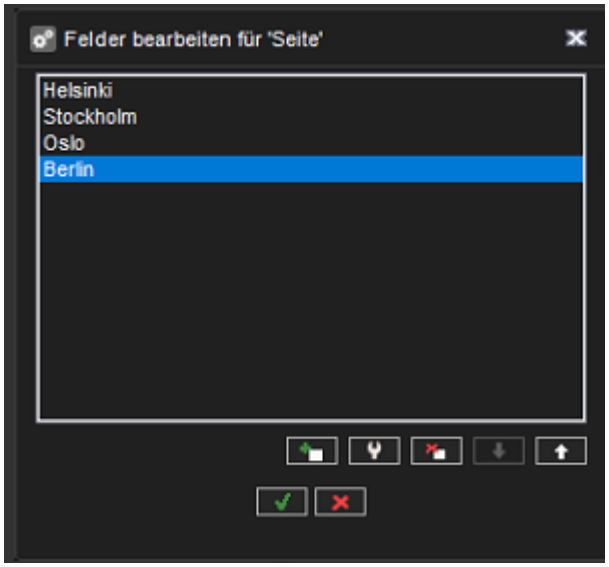


2. Klicken Sie auf Wert hinzufügen

2. Geben Sie den Namen des Wertes ein
3. OK klicken



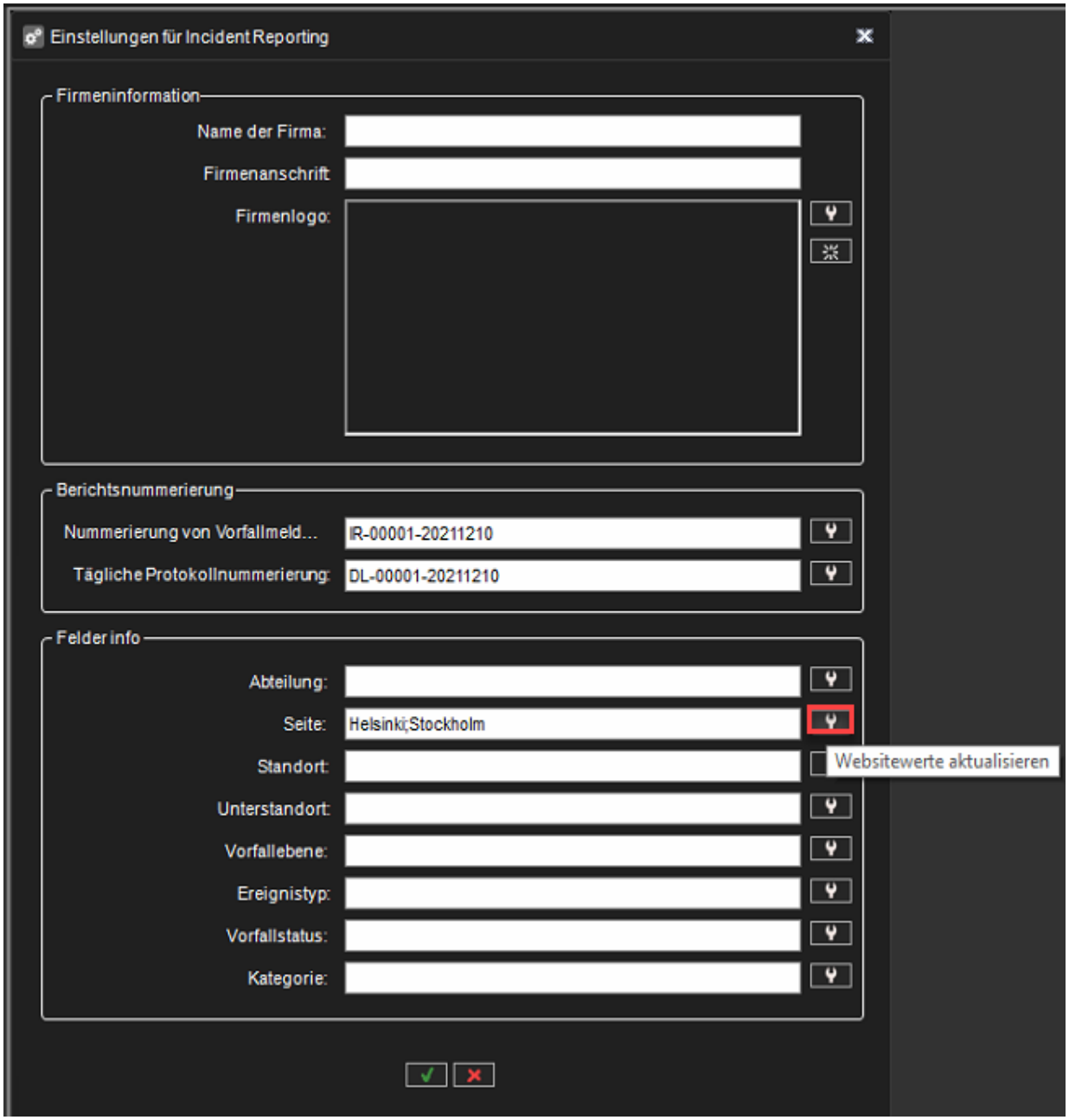
Neuer Mehrwert ist in der Liste zu sehen



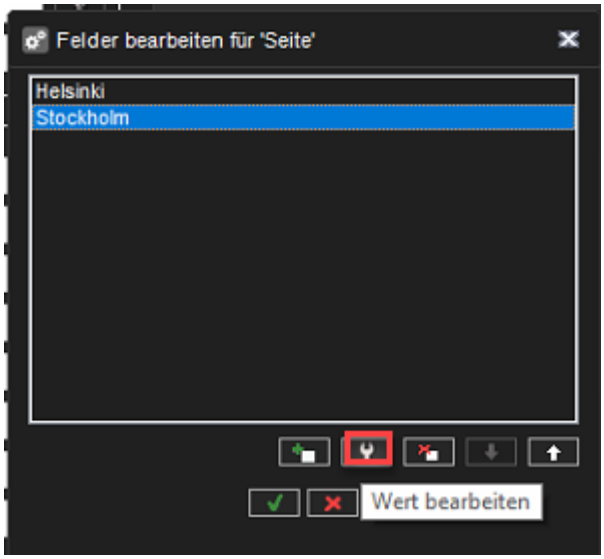
Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

1.8.1.8.2. Werte bearbeiten

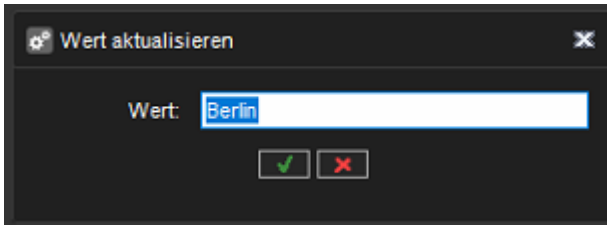
1. Klicken Sie auf das Symbol **Werte aktualisieren**



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



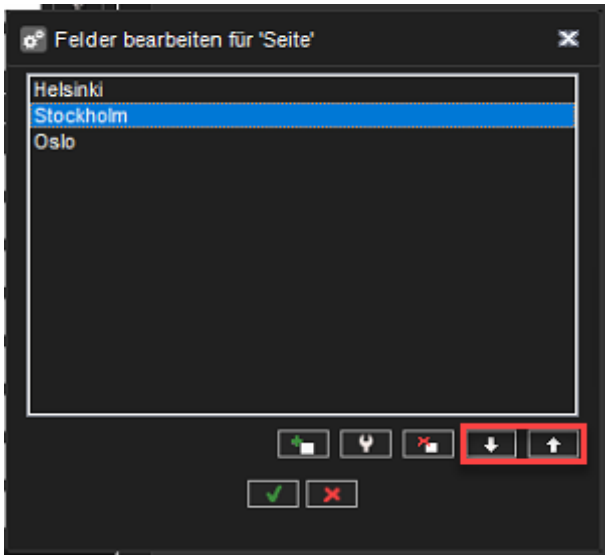
3. Geben Sie einen neuen Wertnamen ein und klicken Sie auf OK



oben Vorherige Nächste

1.8.1.8.3. 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



oben Vorherige Nächste

1.8.1.9. Einstellungen für Speicherschließfach

Storage Locker Settings enthält die folgenden Werte:

Dateipfad:

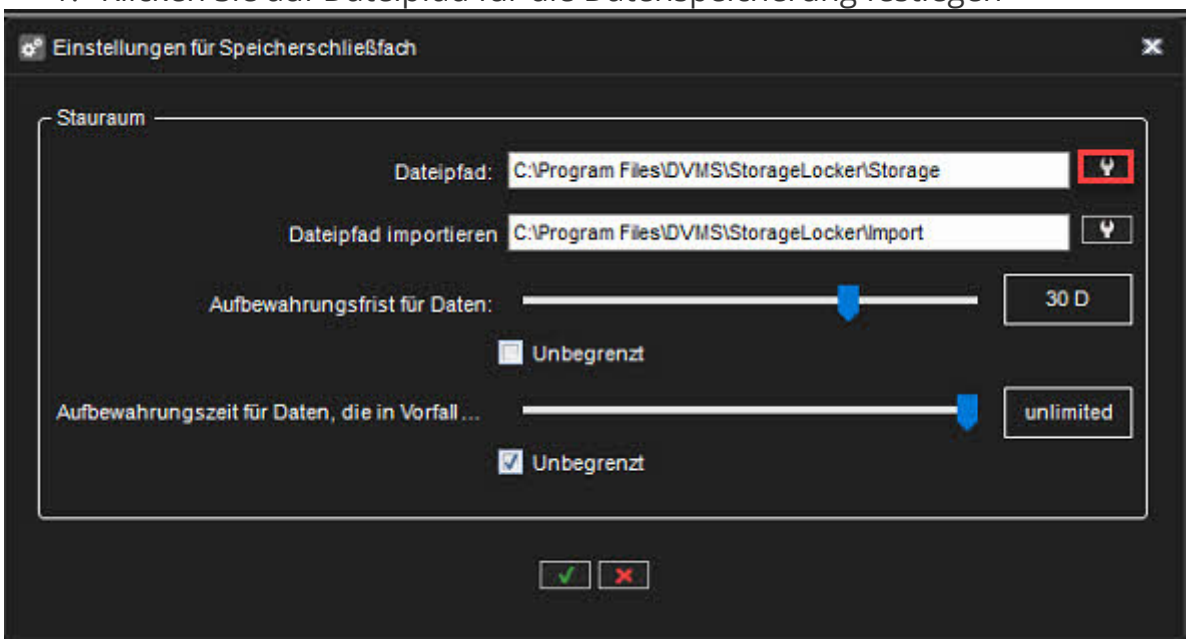
Definiert den Standort des Speicherschließfachs.

Als Standardspeicherort befindet sich Storage Locker auf dem Masterserver.

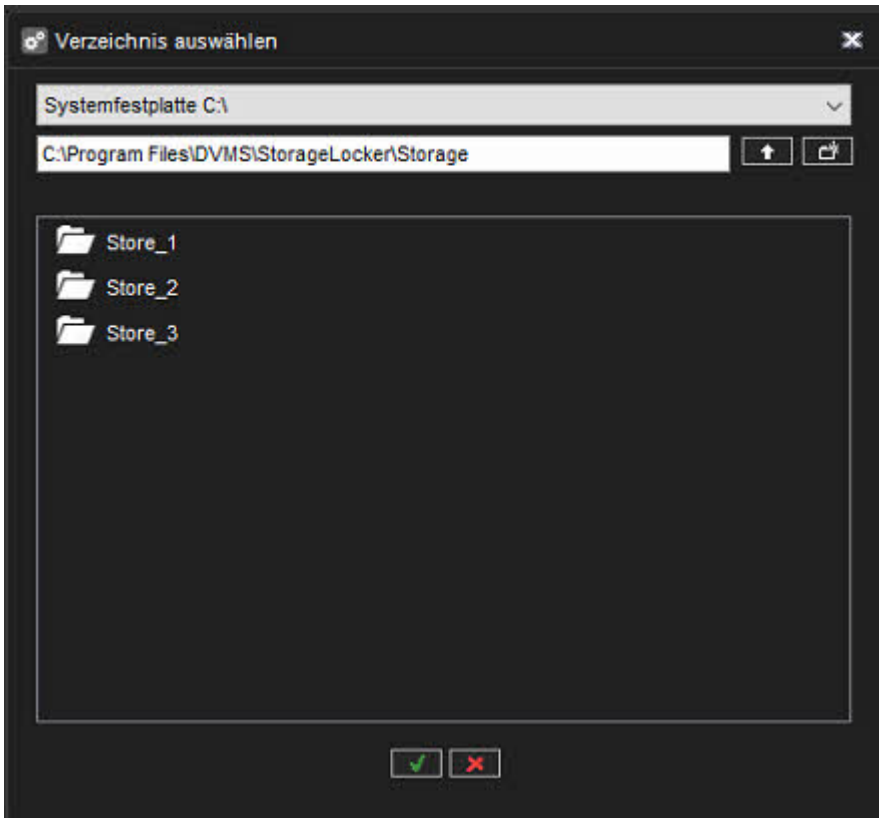
Dateipfad ändern

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



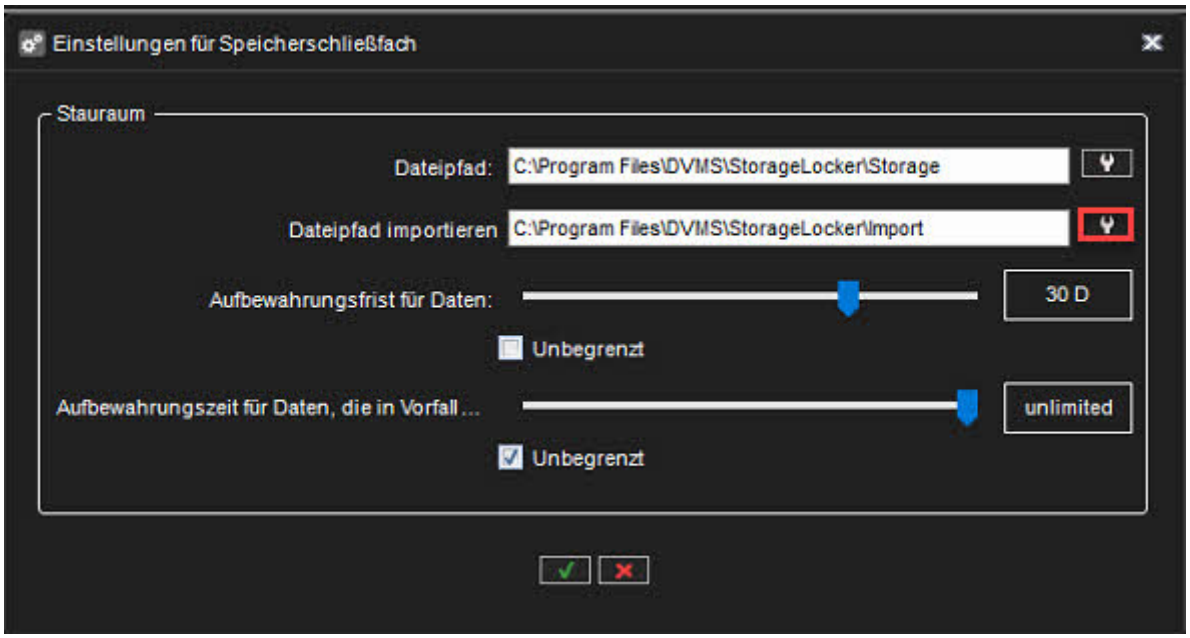
2. Wählen Sie einen neuen Standort und klicken Sie auf OK



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 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 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)

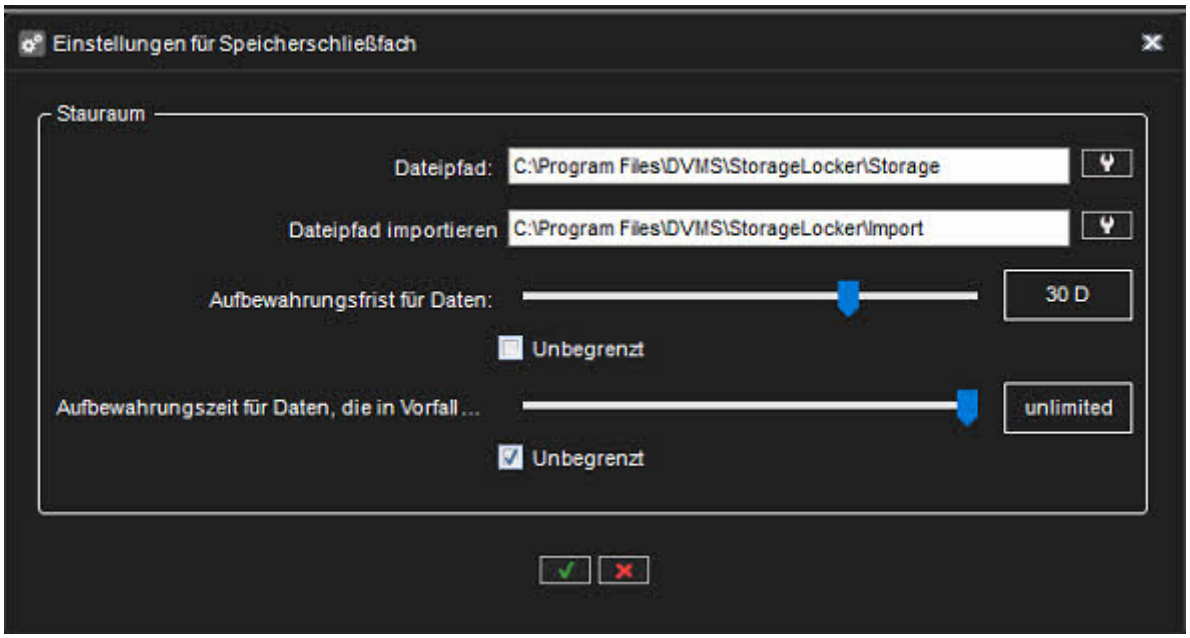


Die Aufbewahrungszeit für Daten

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

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

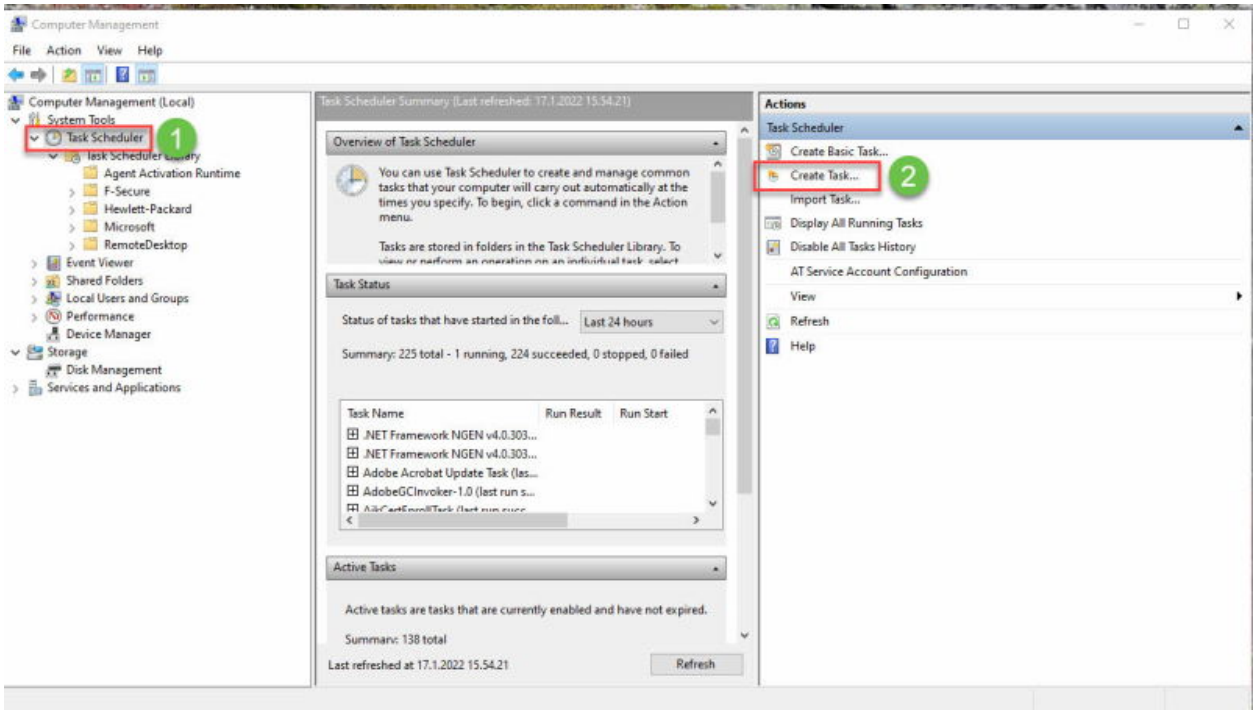


Schritte zum Zuordnen eines Netzlaufwerks, das für Storage Locker-Daten verwendet werden kann

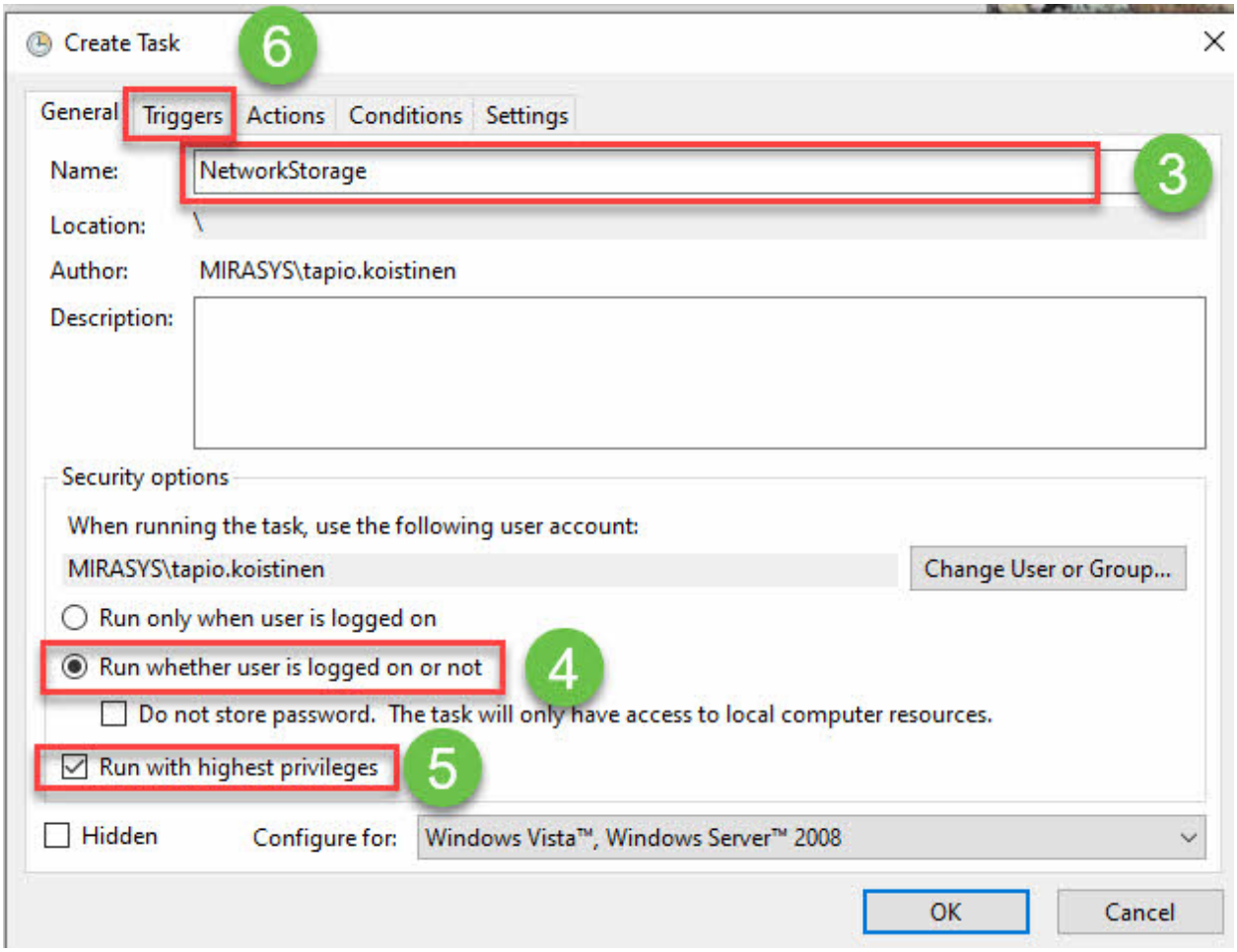
Erstellen Sie eine Stapeldatei (siehe Details zur Stapeldatei) und speichern Sie sie am gewünschten Ort. In meinem Fall habe ich diese Batchdatei unter C:\temp mit dem Namen „SysinternalSuite.bat“ gespeichert.

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

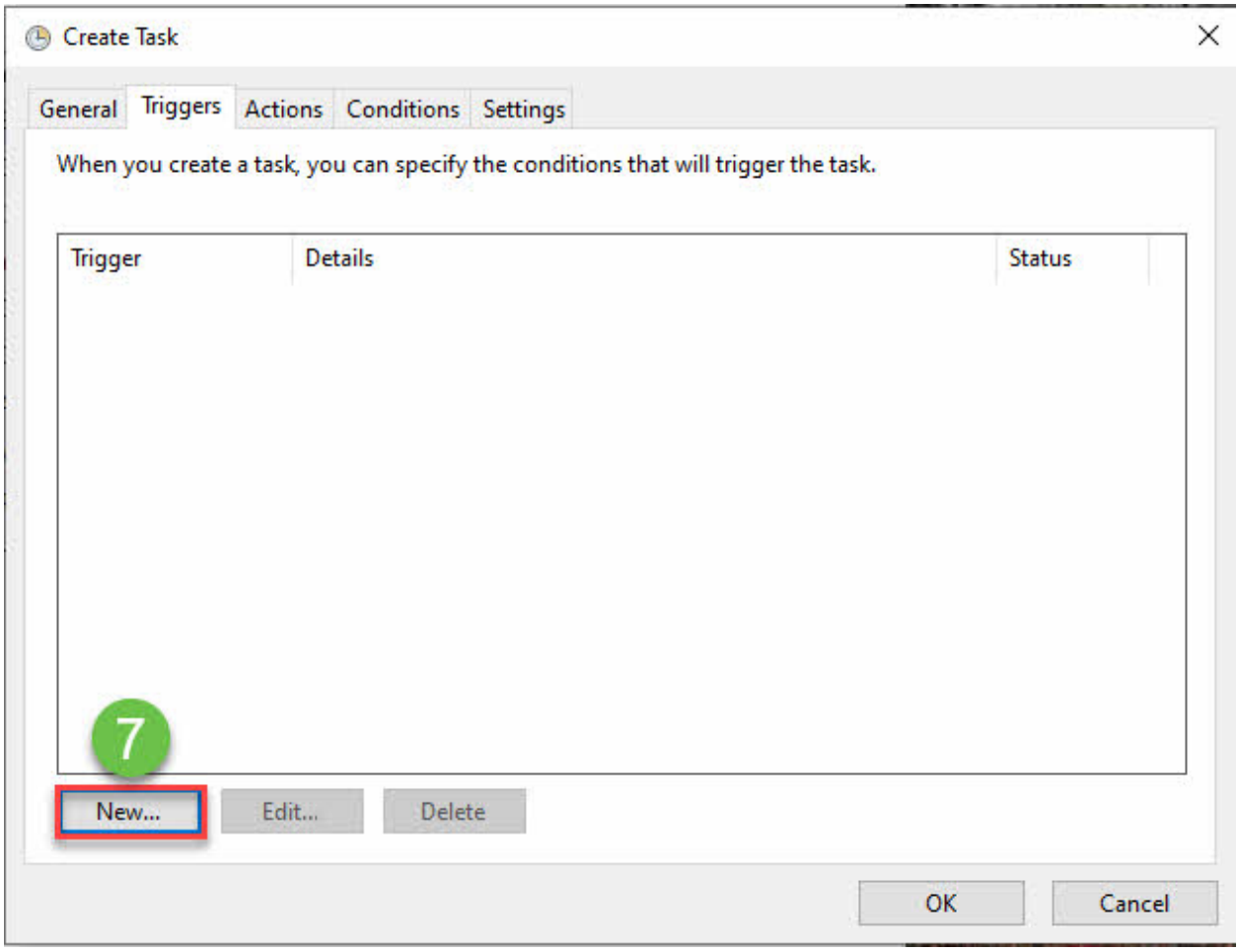
1. offen**Task Scheduler**
2. klicken**Create Task**



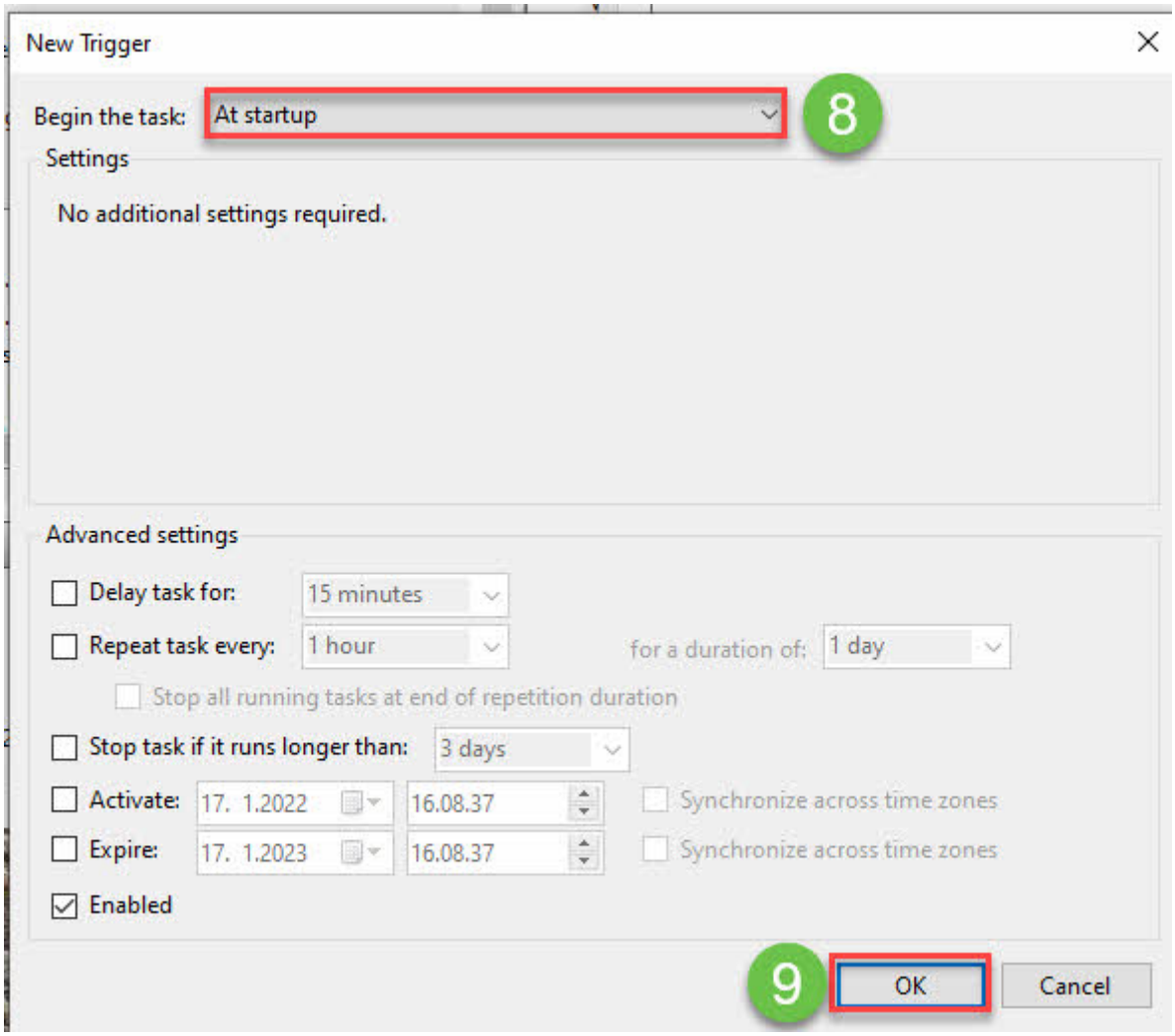
3. Name eingeben
4. Ermöglichen**Run whether the user is logged on or not**
5. Ermöglichen**Run with highest privilege**
6. Offen**Triggers**



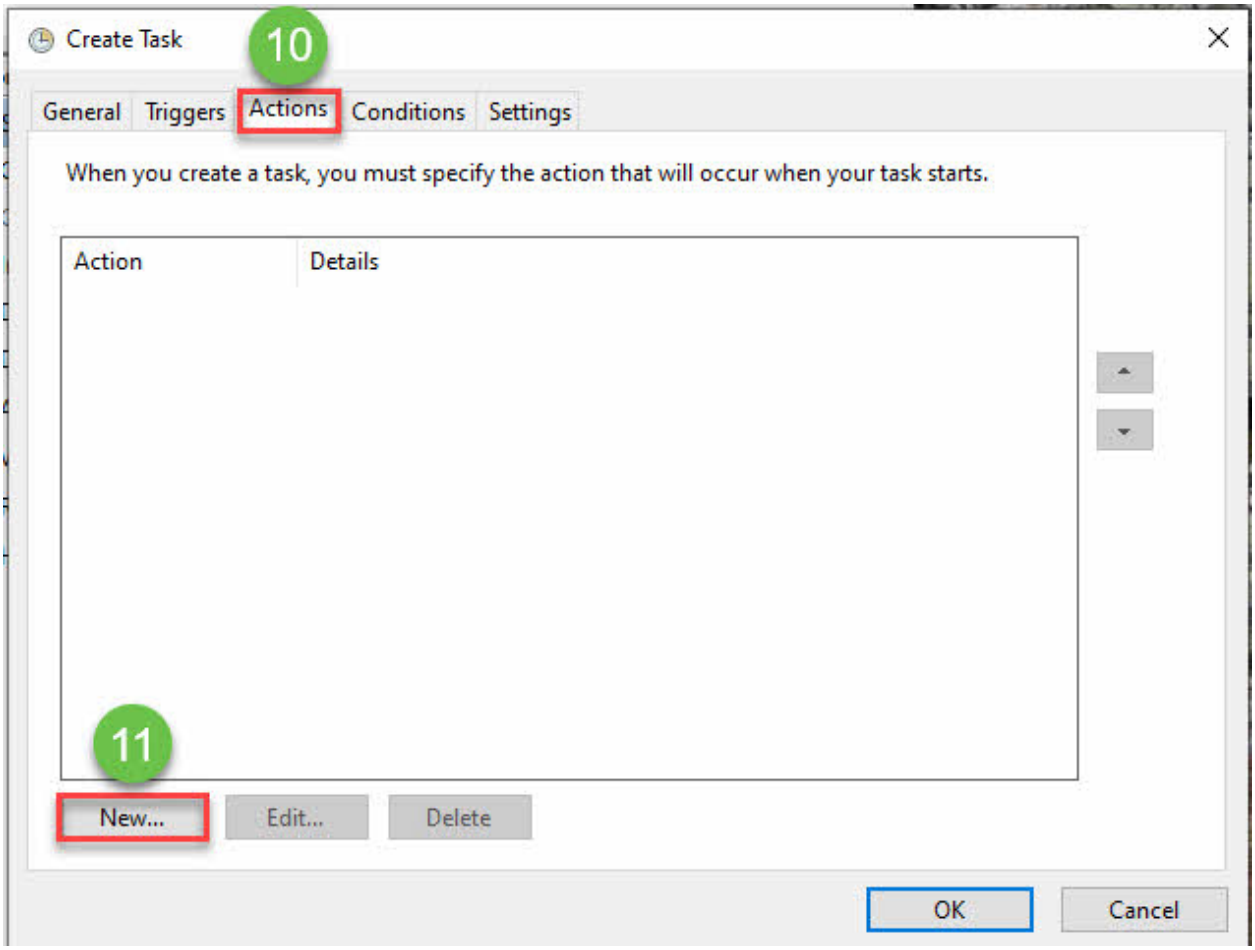
7. Klicken**New**



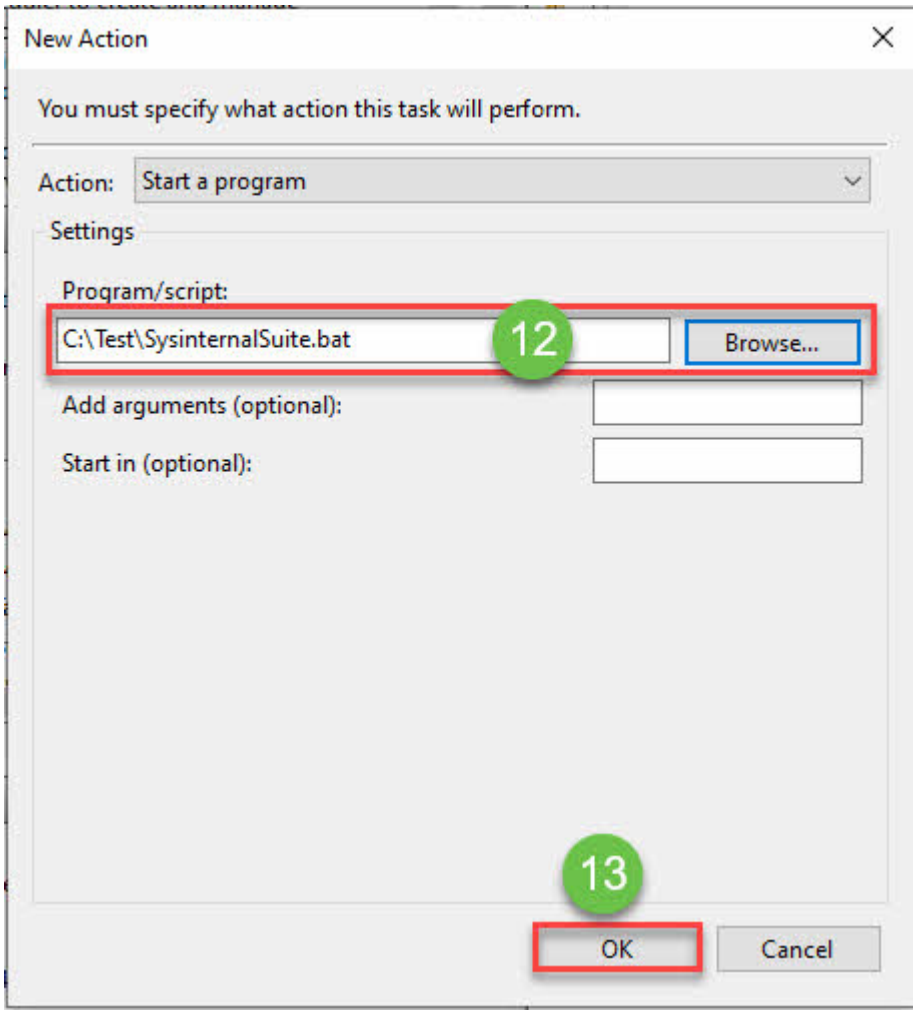
8. wählen At startup from the Begin the task dropdown list
9. Klicken**OK**



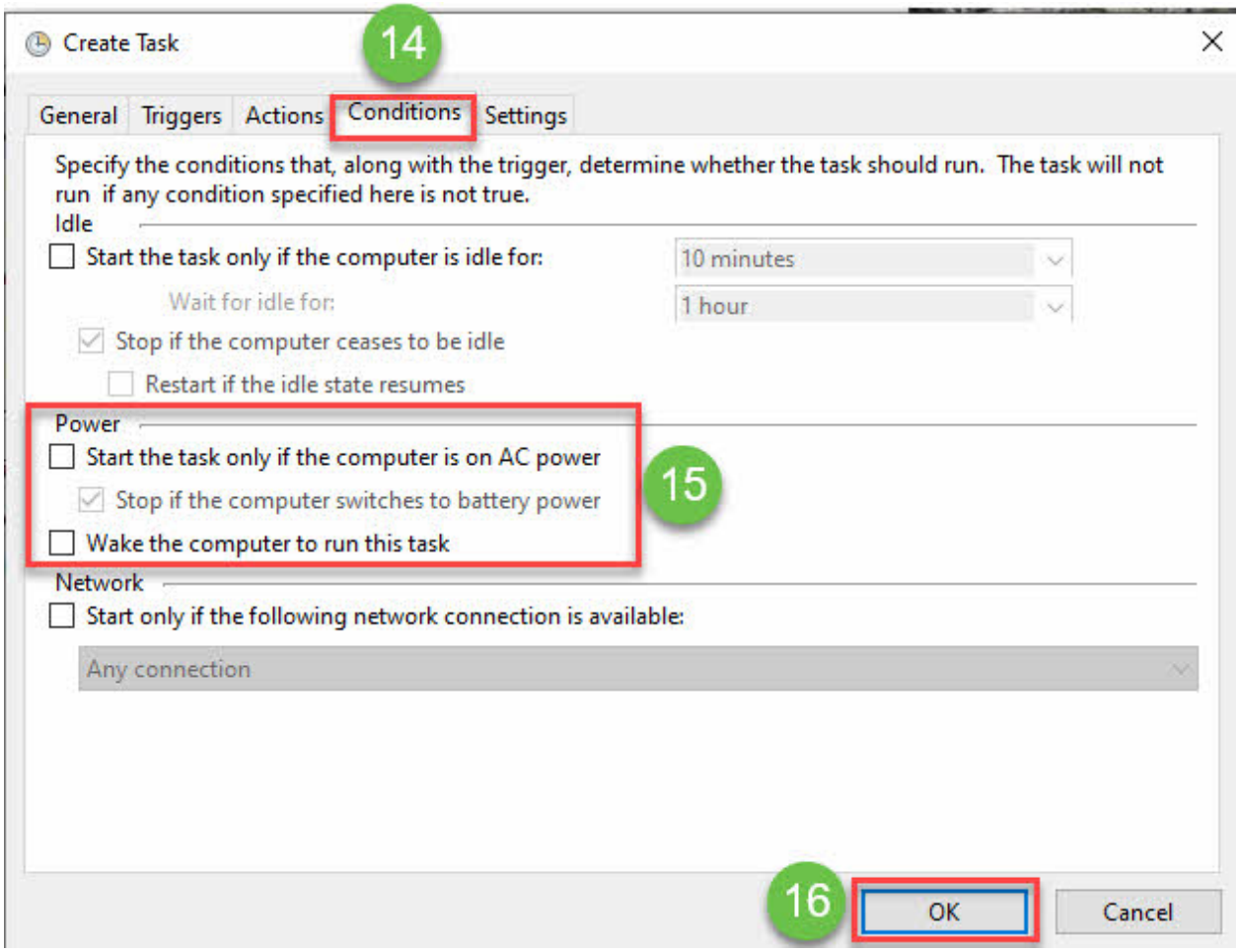
10. oppen**Actions**
11. Klicken**New**



12. Durchsuchen Sie den Speicherort des Skripts und wählen Sie Skript aus
13. Klicken **OK**

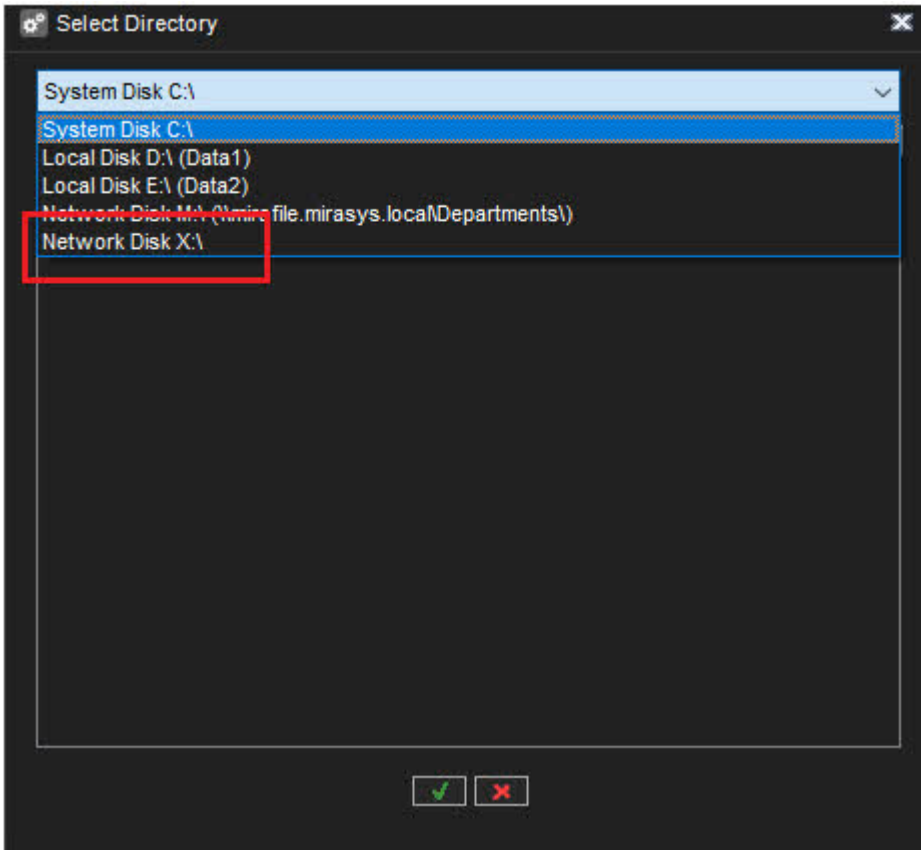


14. oppen**Conditions**
15. Deaktivieren**tart the task only if the computer is on AC power** and **Wake the computer to run this task**
16. Klicken **OK**



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.)

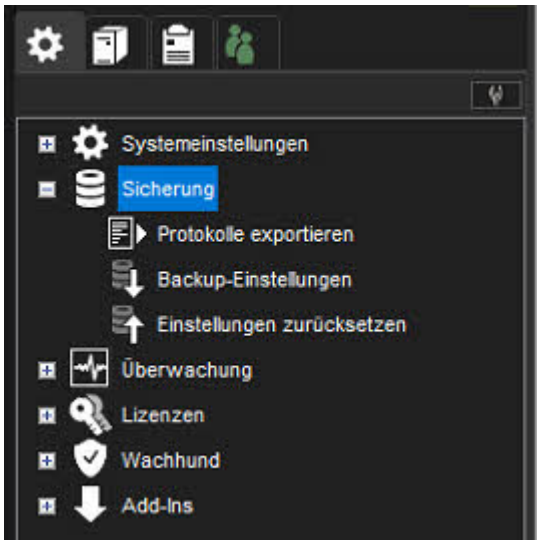
Öffnen Sie nun den System-Manager, navigieren Sie zu den Storage Locker-Einstellungen und beobachten Sie, dass das zugeordnete Laufwerk in der Liste angezeigt wird.



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

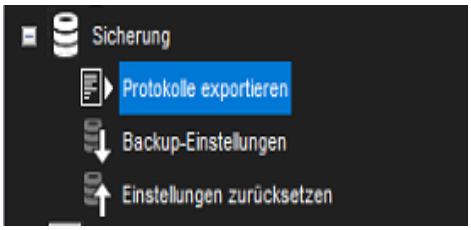
oben Vorherige Nächste

1.8.2. Sicherung



oben Vorherige Nächste

1.8.2.1. Protokolle exportieren



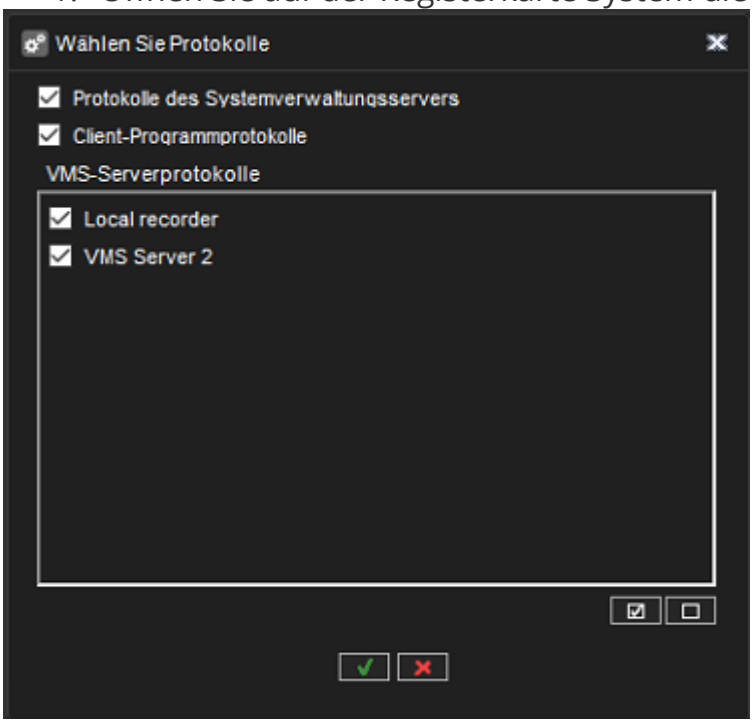
Bei Problemen mit dem System können Sie Protokolldateien exportieren und an den Systemlieferanten senden.

Dies sind die Protokolldaten auf dem Anzeigefeld, der Diskette oder der Diskette und der Ausgabesignalleiste.

Protokolldateien werden in einer komprimierten (gezippten) Datei gespeichert.

So exportieren Sie Protokolldateien:

1. Öffnen Sie auf der Registerkarte System die Option Protokolle exportieren

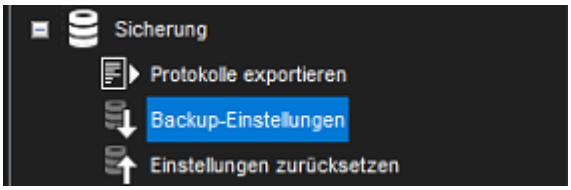


2. Wählen Sie die zu exportierenden Protokolle aus und klicken Sie auf OK. Bei Problemen mit einem Server wählen Sie die Protokolle dieses Servers aus. Wählen Sie außerdem die Protokolle des System Management Servers und des Client-Programms aus
    b. Beachten Sie, dass die Client-Protokolle von dem Computer stammen, auf dem Sie auf die Systemmanageranwendung zugreifen.

3. Wählen Sie das Speichergerät und den Ordner aus, in dem Sie die Protokolldateien speichern möchten. Um einen neuen Ordner zu erstellen, klicken Sie auf die Schaltfläche Neuer Ordner
4. Geben Sie einen Namen für die ZIP-Datei ein und klicken Sie auf OK. Das System exportiert die Dateien in eine ZIP-Datei. Senden Sie die ZIP-Datei an den Systemlieferanten

oben Vorherige Nächste

1.8.2.2. Backup-Einstellungen



Sichern Sie die Systemeinstellungen, um sie wiederherstellen zu können, wenn die Festplatte die Einstellungsdateien enthält.

Sie können Systemeinstellungen und Servereinstellungen sichern.

Systemeinstellungen enthalten Daten zu den Servern, Profilen und Benutzerkonten.

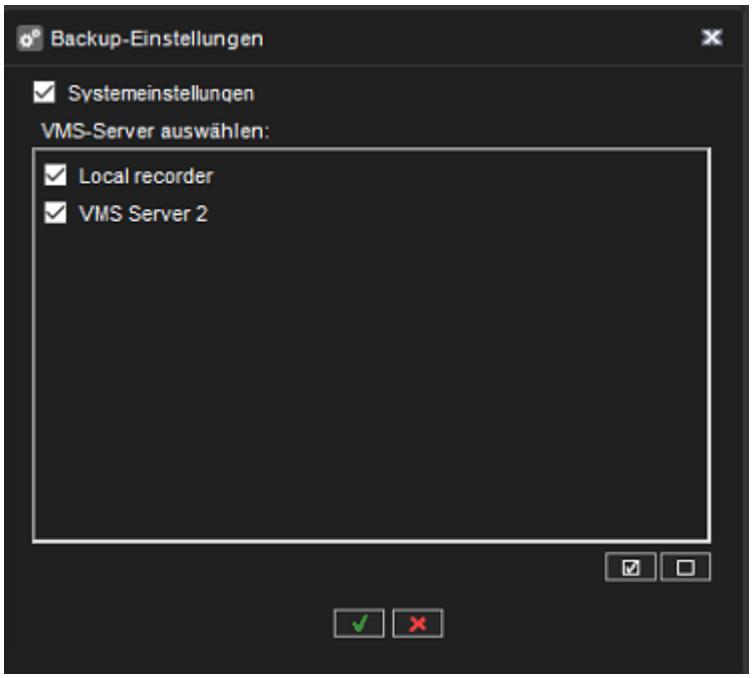
Die VMS-Servereinstellungen enthalten Daten über die mit den Servern verbundenen Geräte und deren Parameter.

Sie können die Sicherungskopie auf einer Festplatte, einem Netzlaufwerk, einer CD/DVD, einer Diskette oder einem anderen austauschbaren oder nicht austauschbaren Gerät speichern.

Backup-Dateien haben die Dateierweiterung „.vbk“.

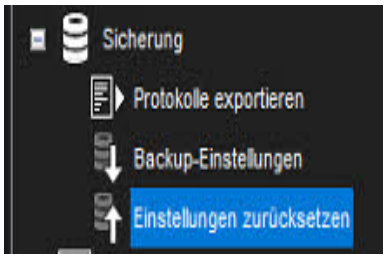
So sichern Sie die Einstellungen:

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.
1. 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.
2. 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.



oben Vorherige Nächste

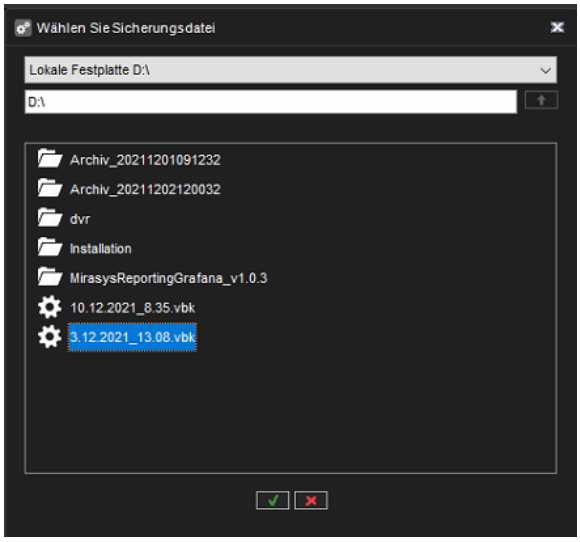
1.8.2.3. Einstellungen zurücksetzen



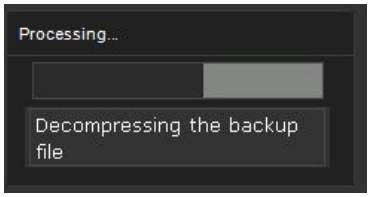
Wenn Sie eine Sicherungsdatei der System- und Servereinstellungen erstellt haben, können Sie die Einstellungen im Fehlerfall wiederherstellen.

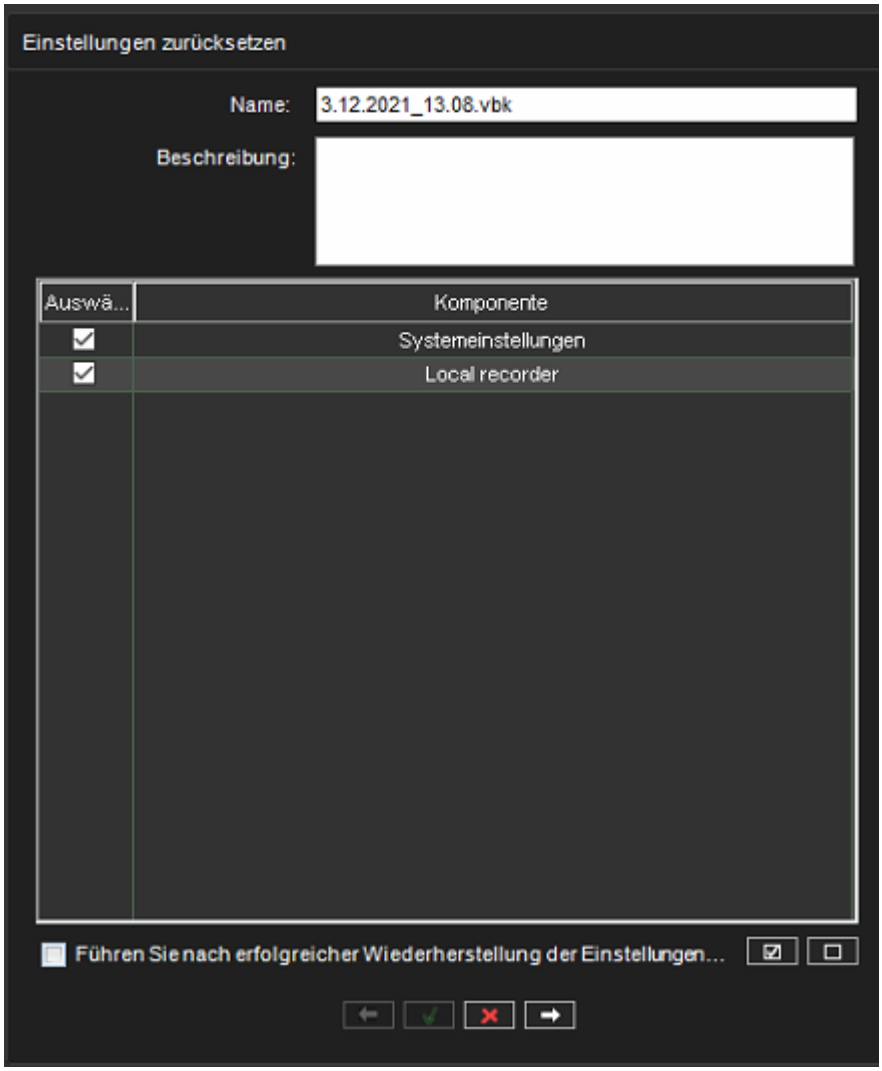
So stellen Sie die Einstellungen wieder her:

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.
    b. 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

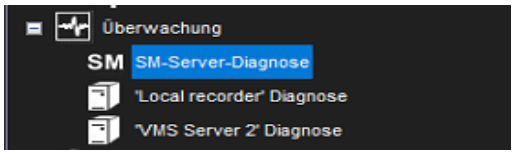
Führen Sie nach erfolgreicher Wiederherstellung der Einstellungen eine automatische Sicherung der Einstellungen durch, insbesondere wenn das System nach einem Failover wiederhergestellt wird.

oben Vorherige Nächste

1.8.3. Überwachung

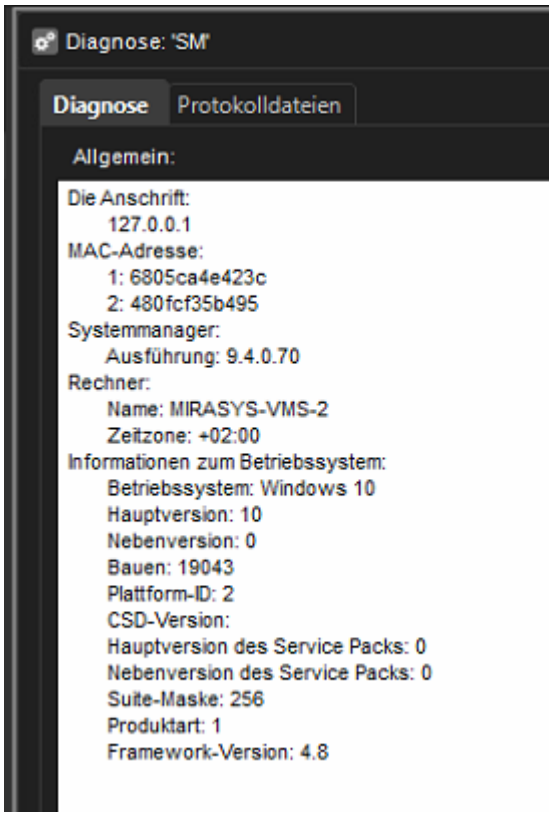
oben Vorherige Nächste

1.8.3.1. SM-Server-Diagnose



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

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

Protokolldateien

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

So untersuchen Sie eine Protokolldatei:

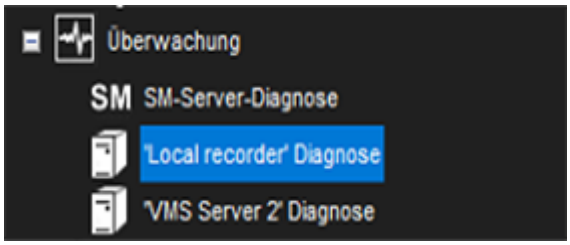
- Wählen Sie die Datei aus der Dropdown-Liste aus.

Der Inhalt wird im Inhalt der ausgewählten Protokolldatei angezeigt

oben Vorherige Nächste

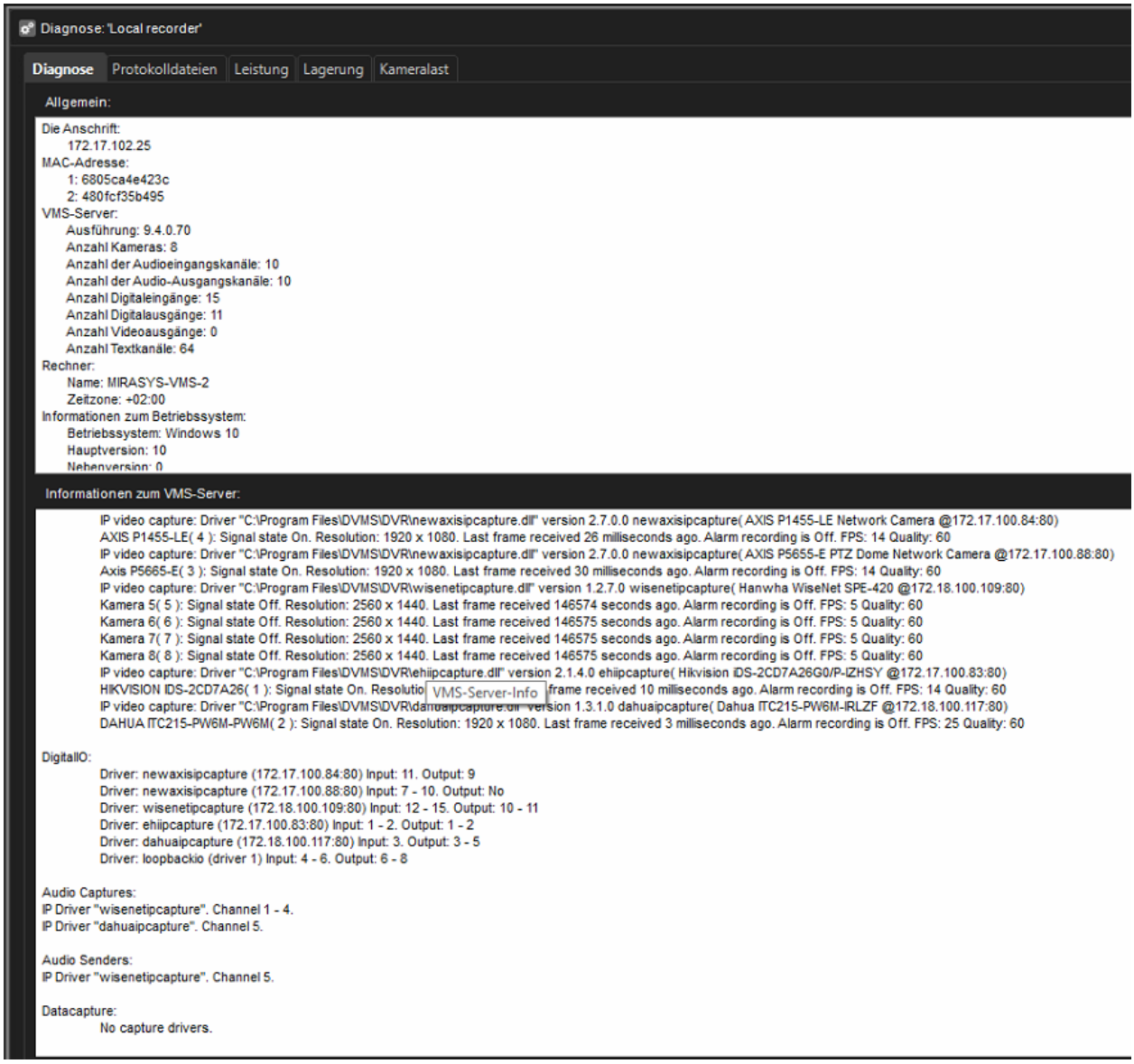
1.8.3.2. Serverdiagnose

Serverdiagnose



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

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

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

Leistung

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

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

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 verwendet haben.

Freiraum Für Aufnahmen steht freier Speicherplatz zur Verfügung.

% Gebraucht Der Prozentsatz der Kapazität des Datenträgers, der verwendet wird.

Durchschnittliche Speichergeschwindigkeit Berechnet durch Division der seit dem letzten Serverstart gespeicherten Datenmenge durch die Betriebszeit.

Betriebszeit des VMS-Servers 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

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

Belegter Speicherplatz Verwendeter Aufnahmespeicher auf der ausgewählten Festplatte.

Freiraum Auf dem ausgewählten Datenträger steht freier Speicherplatz für Aufnahmen zur Verfügung.

% Gebraucht Der Prozentsatz des belegten Speicherplatzes an der Gesamtkapazität, der für die Aufzeichnungen reserviert ist.

Gesamter Aufzeichnungs-Cache. Zeigt die Gesamtkapazität des Caches an, der für die temporäre Speicherung von Daten verwendet wird, bevor diese dauerhaft auf eine Festplatte geschrieben werden.

Durch den Cache können Video und Audio beim Starten des Servers sofort aufgezeichnet werden. 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 Aufnahme-Cache Temporärer Raum, der derzeit genutzt wird.

Kostenloser Aufnahme-Cache Temporärer Speicherplatz, der derzeit frei ist.

Kameras

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

Neueste Zeit Datum und Uhrzeit des neuesten Bilds im Store.

Total no. of images Die Gesamtzahl der Bilder im Store.

Durchschnittliche Bildgröße Die durchschnittliche Bildgröße.

Belegter Speicherplatz Dieser Wert zeigt an, wie viel Speicherplatz die Bilder und Metadatendateien dieser Kamera belegen.

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

Audiokanäle

Älteste Zeit. Datum und Uhrzeit des ältesten gespeicherten Audiobeispiels.

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

Eine Gesamtzahl von Proben Die Gesamtzahl der Audio-Samples im Speicher.

Durchschnittliche Stichprobengröße Die durchschnittliche Audio-Sample-Größe.

Belegter Speicherplatz Dieser Wert zeigt an, wie viel Speicherplatz die Audiosamples und Metadatendateien des Audiokanals belegen.

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

Textkanäle

Älteste Zeit. Datum und Uhrzeit der ältesten gespeicherten Textdatenprobe.

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

Eine Gesamtzahl von Proben Die Gesamtzahl der im Speicher befindlichen Textdatenproben.

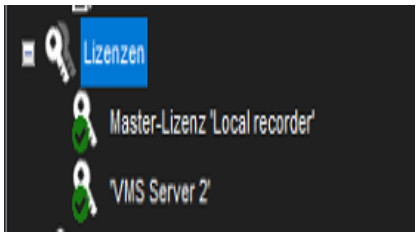
Durchschnittliche Stichprobengröße Die durchschnittliche Stichprobengröße für Textdaten.

Belegter Speicherplatz Dieser Wert zeigt an, wie viel Platz die Textdatenproben und Metadatendateien aus dem Textkanal belegen.

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

oben Vorherige Nächste

1.8.4. Lizenzen



Der Server benötigt für den vollen Funktionsumfang eine gültige Lizenz.

Je nach Installation müssen Sie möglicherweise die Lizenzinformationen aktualisieren, wenn Sie dem System neue Funktionen oder Kameras hinzufügen.

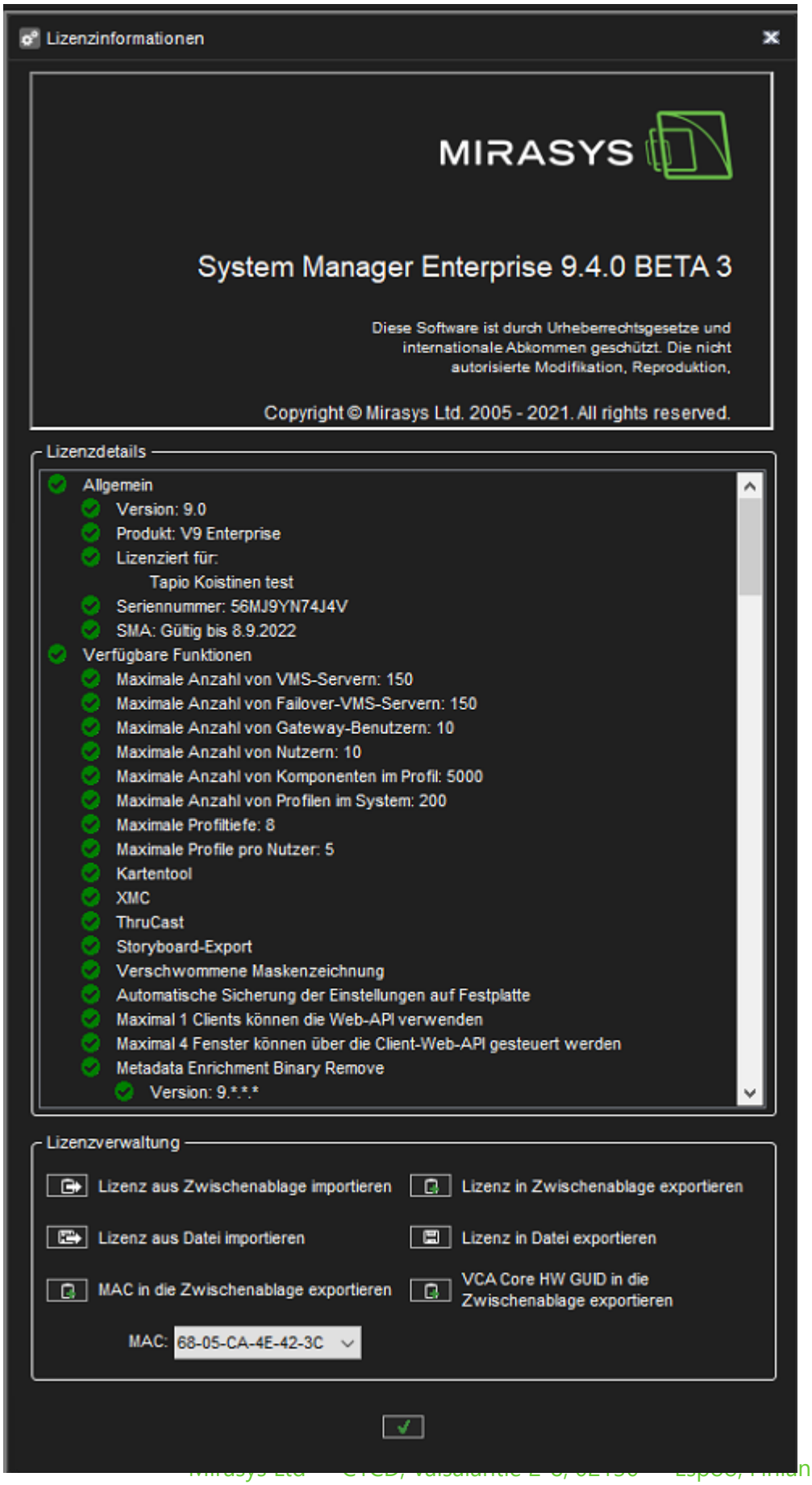
Um einen Lizenzschlüssel zu erhalten, wenden Sie sich bitte an Ihren Lieferanten und befolgen Sie das vom Lieferanten beschriebene Lizenz-Upgrade-Verfahren.

Bei Problemen beim Upgrade der Lizenz wenden Sie sich bitte an *order@mirasys.com*

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

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE

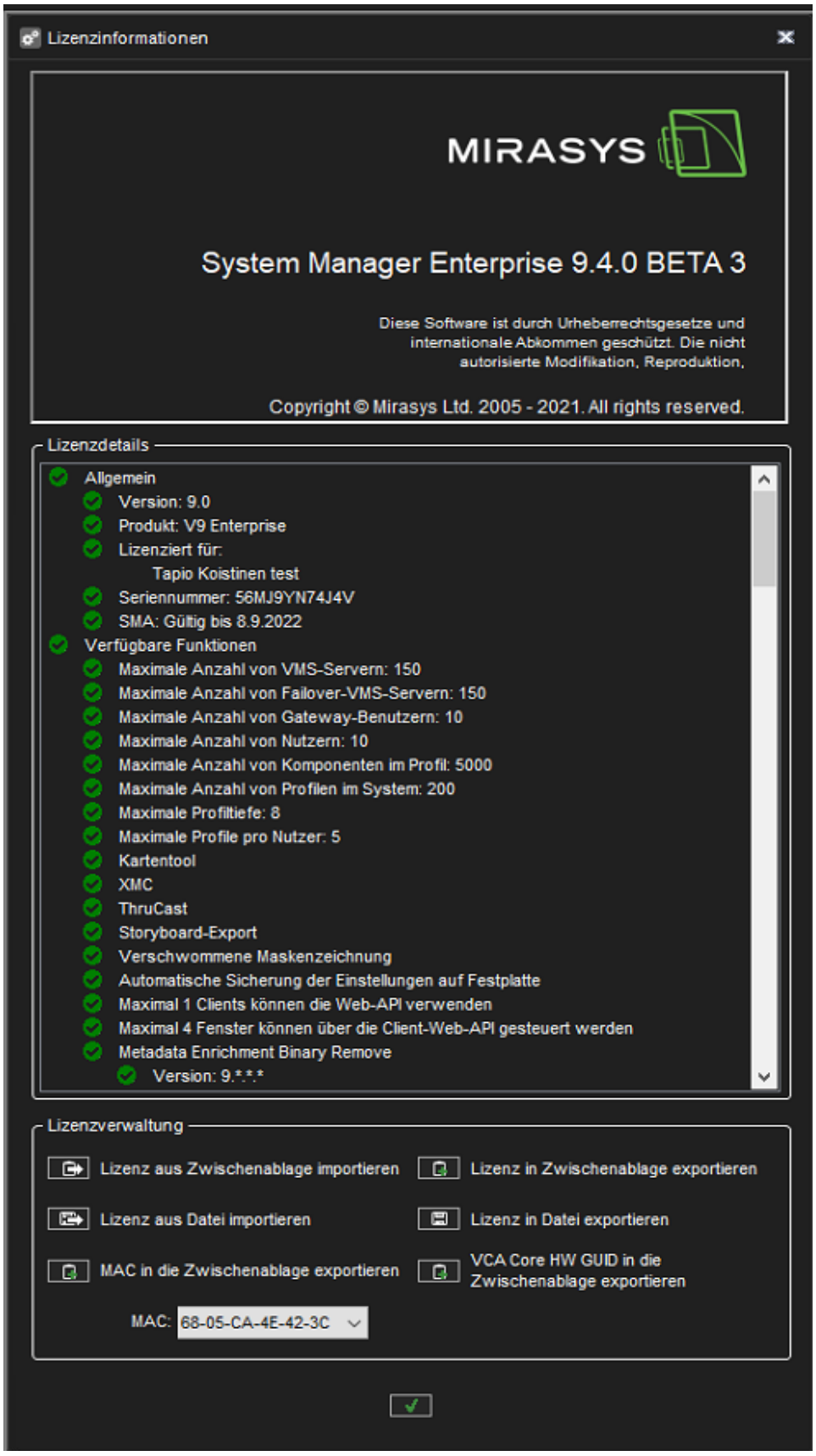


1.8.4.1. Lizenzdetails

Lizenzdetails zeigen alle unterstützten Funktionen der Lizenz.

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE



1.8.4.2. Lizenzverwaltung

So importieren Sie einen Lizenzschlüssel:

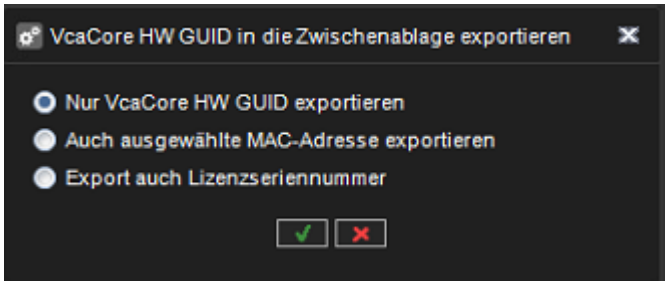
1. Klicken **Sie auf Lizenz aus Datei importieren**
2. Navigieren Sie zum Speicherort der Lizenzdatei
4. **OK** klicken Die neue Lizenz wird sofort aktualisiert.

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.

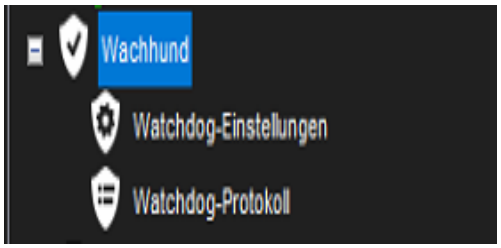
So exportieren Sie die VCA Core HW GUID

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



oben Vorherige Nächste

1.8.5. Wachhund



Das System verfügt über einen Software-Watchdog (System Monitoring Service), der das System überwacht und bei Problemen gezielt Aktionen ausführt.

Im Watchdog-Tool können Sie die Ereignisse auswählen, bei denen die Benachrichtigungsliste per E-Mail benachrichtigt wird, und auf Watchdog-Protokolle zugreifen, die aufgetretene Ereignisse und durchgeführte Aktionen enthalten.

oben Vorherige Nächste

1.8.5.1. Watchdog-Einstellungen

In den Watchdog-Einstellungen können Sie auswählen, welche Ereignisse einen Bericht auslösen, der an die in den E-Mail-Einstellungen angegebenen E-Mail-Adressen gesendet wird

Sie können für jeden Server verschiedene Ereignisse auswählen.

Alternativ können Sie für alle Server dieselben Ereignisse auswählen, indem Sie **Alle VMS-Server** aus der Dropdown-Liste auswählen.

Neben E-Mail-Benachrichtigungen können Benachrichtigungen über digitale Ausgänge erfolgen.

Alle Ereignistypen werden unabhängig von den E-Mail-Einstellungen in die Watchdog-Logs geschrieben.

So fügen Sie Ereignisse zur Benachrichtigungsliste hinzu oder entfernen sie:

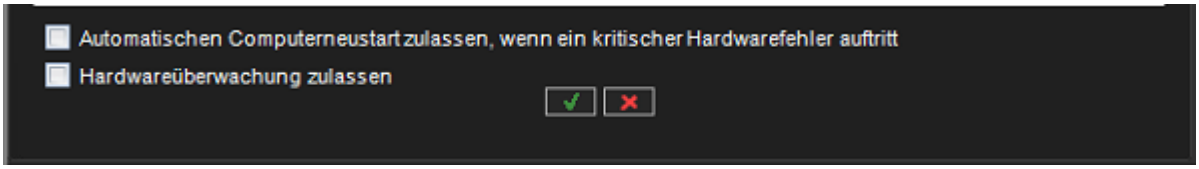
1. Wählen Sie auf der Registerkarte **System** die Option **Watchdog-Einstellungen**.
2. Markieren Sie das Kontrollkästchen **Mail senden** für jeden Ereignistyp, für den eine Benachrichtigungs-E-Mail gesendet werden soll.
3. Klicken Sie auf **OK**.

Automatischer Neustart

Aktivieren Sie das Kontrollkästchen. **Automatischen Neustart des Computers zulassen, wenn ein kritischer Hardwarefehler auftritt,** um den Computer neu zu starten, wenn schwerwiegende Hardwarefehler automatisch auftreten.

Der Computer wird nicht mehr als einmal täglich neu gestartet.

Wählen Sie **Hardwareüberwachung zulassen**.bei Bedarf



Digitale Ausgangsbenachrichtigungen

Neben E-Mail-Benachrichtigungen können Benachrichtigungen über digitale Ausgänge erfolgen.

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**.

oben Vorherige Nächste

1.8.5.2. Watchdog-Protokoll

Standardmäßig zeigt das System die Watchdog-Protokolle von allen Servern an.

Sie können jedoch einen oder mehrere Server aus der Liste links 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**.

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.

Zu den neuen Konfigurationsoptionen gehören gefilterte und bedingte Warnungen (d. h. „Warnung X nur einmal alle 60 Minuten senden“ oder „Warnung X nur senden, wenn Bedingung Y nicht in zwei Minuten erfüllt wird“) und anpassbares Warnmeldungsformat.

Nachdem die Dateien bearbeitet wurden, muss Watchdog neu gestartet werden, damit die Änderungen wirksam werden.

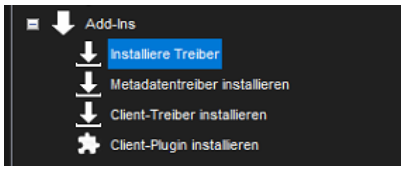
Notiz *Diese Funktion wird nur für fortgeschrittene Benutzer empfohlen. XML-Dateien sind sehr anfällig für Rechtschreibfehler und falsch eingegebene Zeichenfolgen und Schlüssel.*

Selbst ein winziger Fehler kann fatale Fehler verursachen. Mirasys übernimmt keine Verantwortung für XML-Fehler, die durch das Bearbeiten der Dateien verursacht werden.

1.8.6. Add-Ins

oben Vorherige Nächste

1.8.6.1. Installieren externer Treiberpakete



Um IP-Kameras, digitale I/O-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.

Bei Bedarf können jedoch 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 Treiberinstallationspakets vergleicht das System die Dateien im Installationspaket mit den vorhandenen Dateien auf den Servern.

Normalerweise werden die Dateien nur dann installiert, 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 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.*

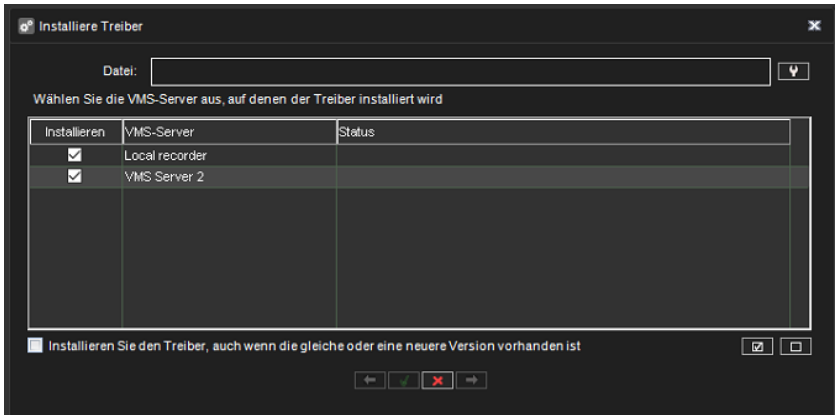
Installieren Sie nach dem Entfernen der Kamera die Treiberdatei. Danach können Sie die Kamera neu installieren.

Nach der Installation eines neuen Treibers müssen Sie die Geräte konfigurieren, 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.

oben Vorherige Nächste

1.8.6.2. Installieren von Metadatentreibern

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

oben Vorherige Nächste

1.8.6.3. Client-Treiber installieren

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

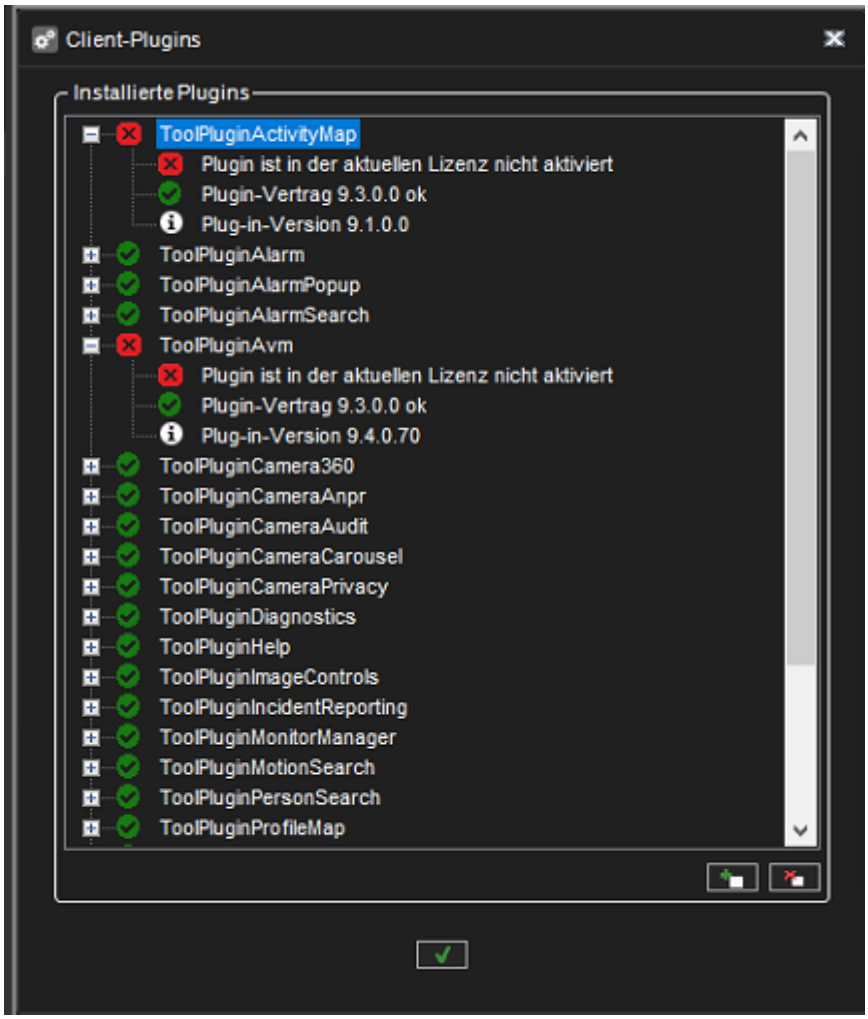
Diese werden als (verwaltete) TruCast Client-Treiber bezeichnet.

Die Client-Kamera-Treiber werden ähnlich wie Spotter-Plugins und Metadaten-Treiber installiert, indem die Option **Client-Treiber installieren** im Systemmanager verwendet wird.

oben Vorherige Nächste

1.8.6.4. Client-Plugin installieren

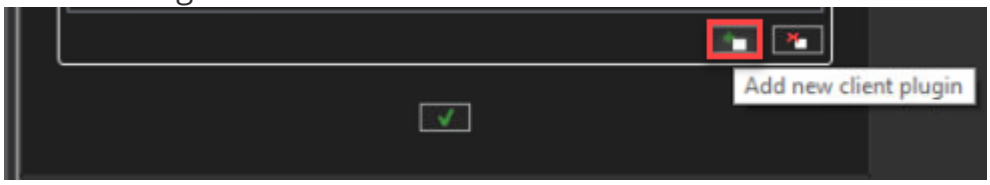
Client-Plugins für Benutzeroberflächen wie Spotter können über den System Manager installiert werden.



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

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.

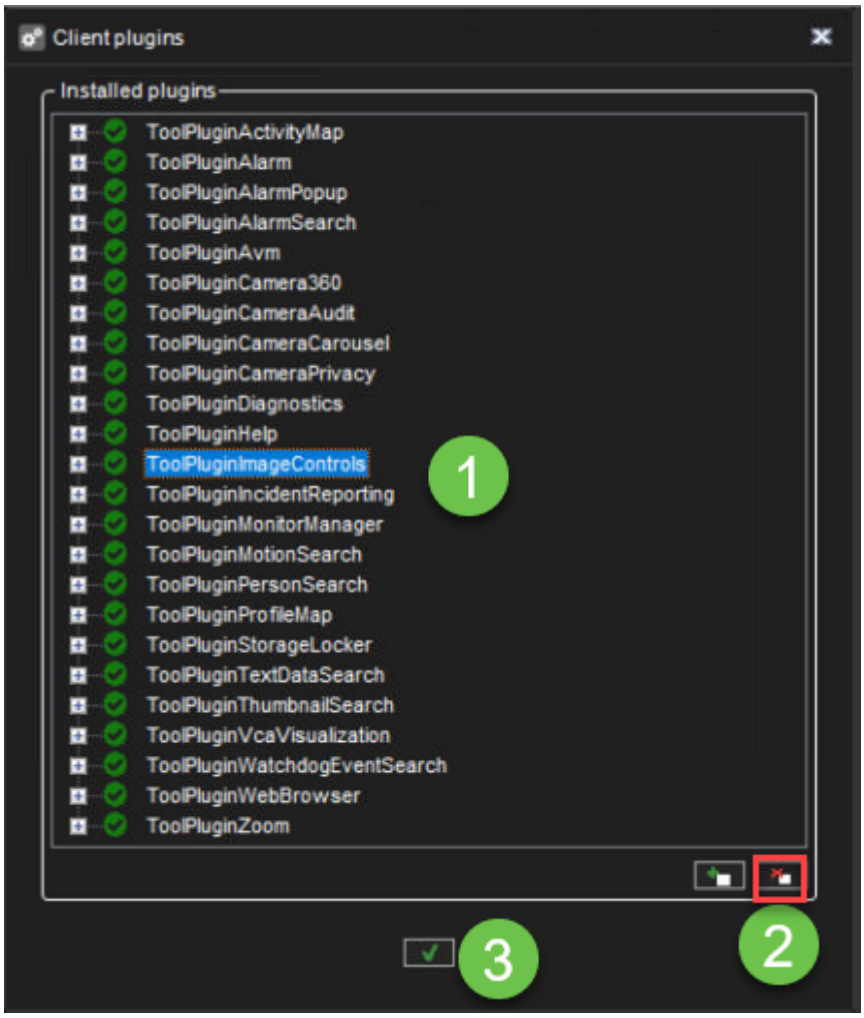


3. Suchen Sie das Plugin-Paket (.zip-Datei) und wählen Sie es aus und klicken Sie auf **OK**. Die Dialogbox **Install Plugin** wird angezeigt.
4. Wenn Sie das System zwingen möchten, die Treiberpaketversion zu installieren, wählen Sie **Treiber installieren, auch wenn dieselbe oder eine neuere Version vorhanden ist.**
5. Klick **Ok**

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**



Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

1.9. VMS-Server

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.

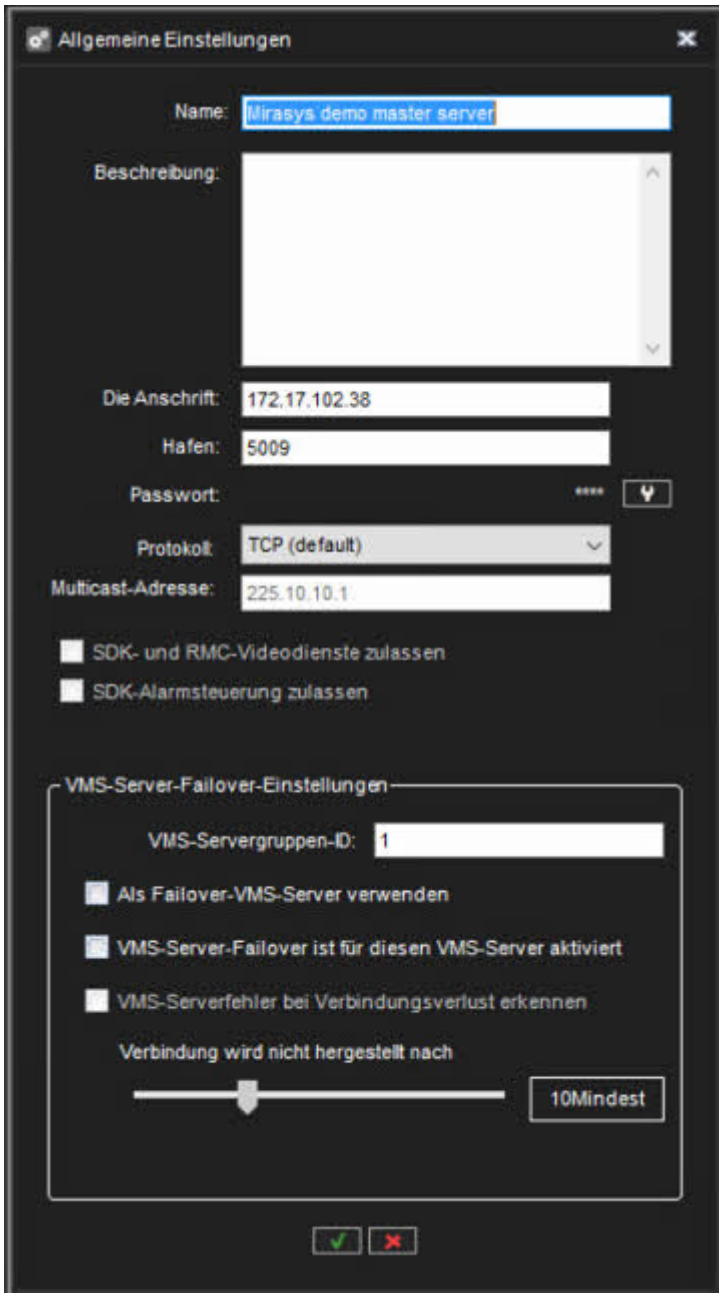
Um auf die Einstellungen zuzugreifen, führen Sie einen der folgenden Schritte aus:

- 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.

oben Vorherige Nächste

1.9.1. Allgemein

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



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.

Multicasting ermöglicht das gleichzeitige Öffnen und Senden eines einzelnen Streams an mehrere Workstations.

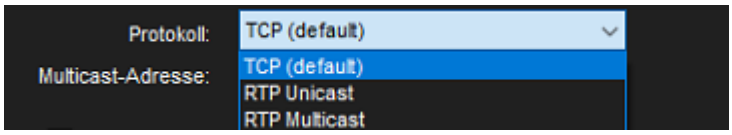
Bei Verwendung von Multicasting wird der Stream für jeden Videokanal nur einmal an das LAN gesendet.

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 im System Manager und über die Netzwerkeinstellungen konfiguriert werden.

Bitte wenden Sie sich an Ihren Netzwerkinfrastrukturdienst, um Informationen zur Aktivierung 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.

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 Server-Aufgaben übernimmt, die unter Failover-Schutz stehen.

Failover-Server müssen dasselbe Dateisystem (gleiche Laufwerksbuchstaben) haben wie die VMS-Server unter Failover-Schutz und können nur für Sicherungszwecke von IP-Kameras verwendet werden.

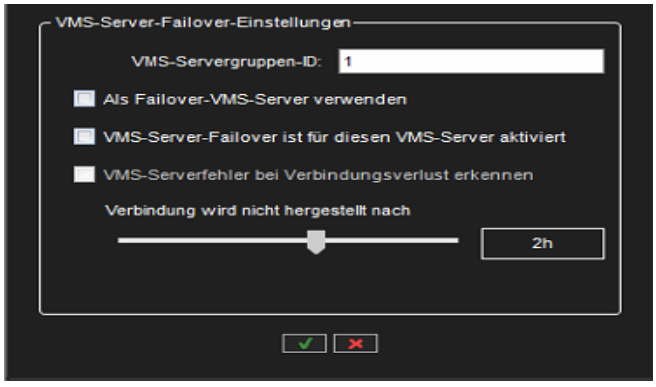
Im Standby-Modus werden Failover-Server in einem separaten Ordner in der Liste *VMS Server* angezeigt.

Wenn ein VMS-Server als defekt oder unzugänglich eingestuft wird, wurde er in den Ordner *„Broken VMS Servers“* verschoben.

Jeder verfügbare Failover-Server übernimmt die Verantwortung des ausgefallenen Servers.

Failover-Einstellungen können über die allgemeinen Einstellungen des ausgewählten Servers gesteuert werden.

Der Failover-Übergang wird durchgeführt, wenn alle Materialplatten 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.

oben Vorherige Nächste

1.9.2. Port-Weiterleitung

***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.**

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“.

oben Vorherige Nächste

1.9.2.1. 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, das auf dem Gerät aktiviert sein muss.

Der Server verfügt während der Ausführung über eine kontinuierliche UPnP-Geräteerkennung. Wenn also 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 merkt sich der Server, dass die Einstellungen entfernt wurden, und leitet 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 des Port-Forward-Mappings würde das System trennen und es wäre keine weitere Konfiguration möglich.

Wenn die Forward-Port-Einstellungen geändert werden und die Verbindung zum Server nach einiger Zeit nicht wiederhergestellt wurde, muss der Router möglicherweise neu gestartet werden.

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 **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...**)

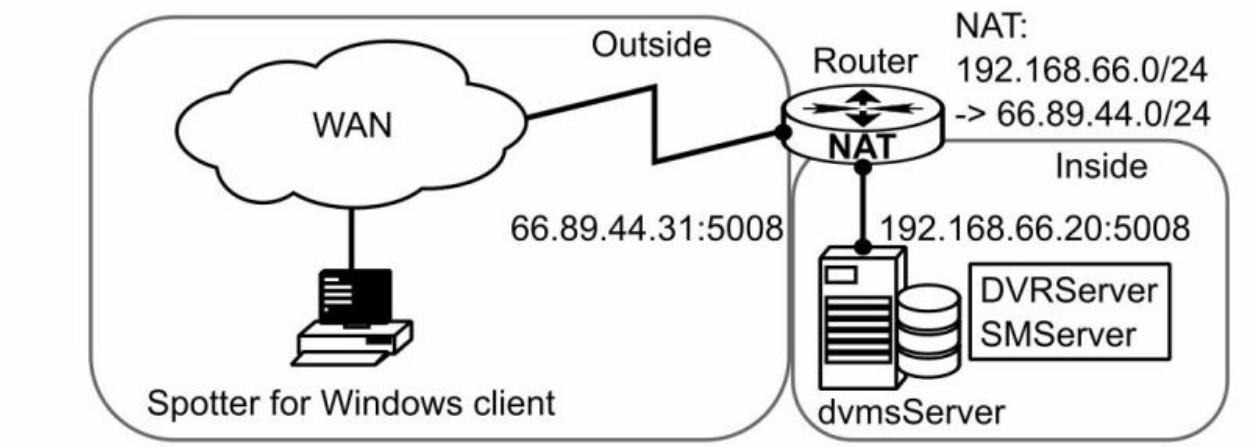
Der zweite Port wird für die DVRServer-Prozesskommunikation verwendet (**5009, 5013, 5017...**)

Wenn Sie eine Verbindung zu einem Master-Server herstellen, ist der Port normalerweise 5008. Beim Hinzufügen neuer Server zum Master ist der Port normalerweise 5009. If there are more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.

oben Vorherige Nächste

1.9.2.2. Einzelner Server hinter Router

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



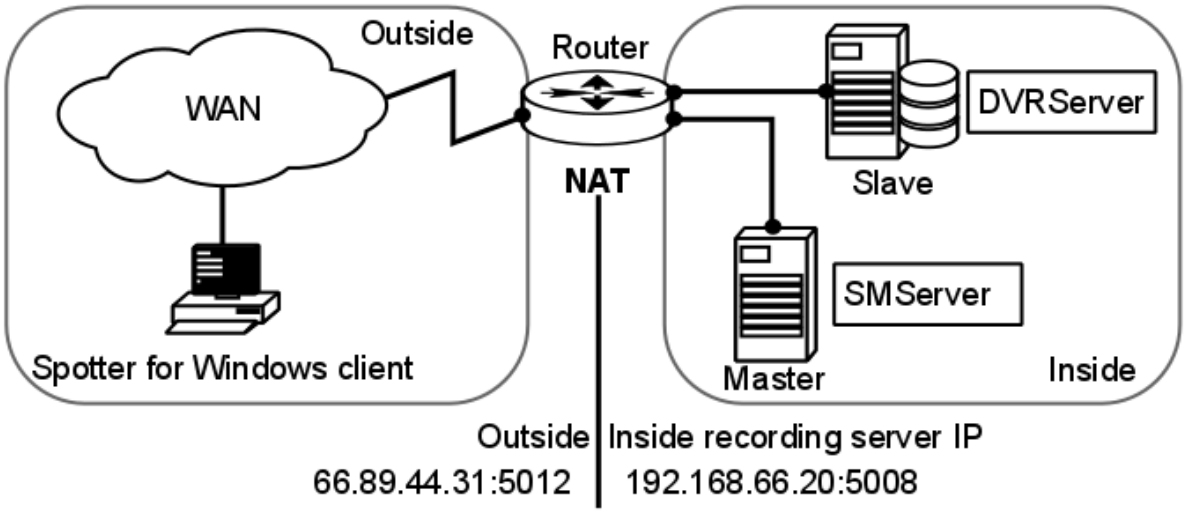
Wenn der Benutzer über das WAN auf einen einzelnen Server zugreift, muss er sich mit der externen IP-Adresse, die der Router übersetzt hat, mit dem VMS-Server verbinden.

Der Benutzer kann die Portweiterleitung überprüfen, was der verwendete Port ist, aber es ist sehr wahrscheinlich Port 5008.

oben Vorherige Nächste

1.9.2.3. 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.

Wenn der Server beim Hinzufügen eines neuen VMS-Servers eine automatische Portweiterleitung durchgeführt hat, zeigt ein Hinweis an, dass er zwischen einer internen IP-Adresse und einer externen IP-Adresse wählen kann.

Soll der Server aus dem WAN genutzt werden, dann sollte die externe IP-Adresse gewählt werden.

Die genauen Ports, zu denen der Server die Portweiterleitung durchgeführt hat, können durch Starten des System Managers auf dem lokalen Server ermittelt werden.

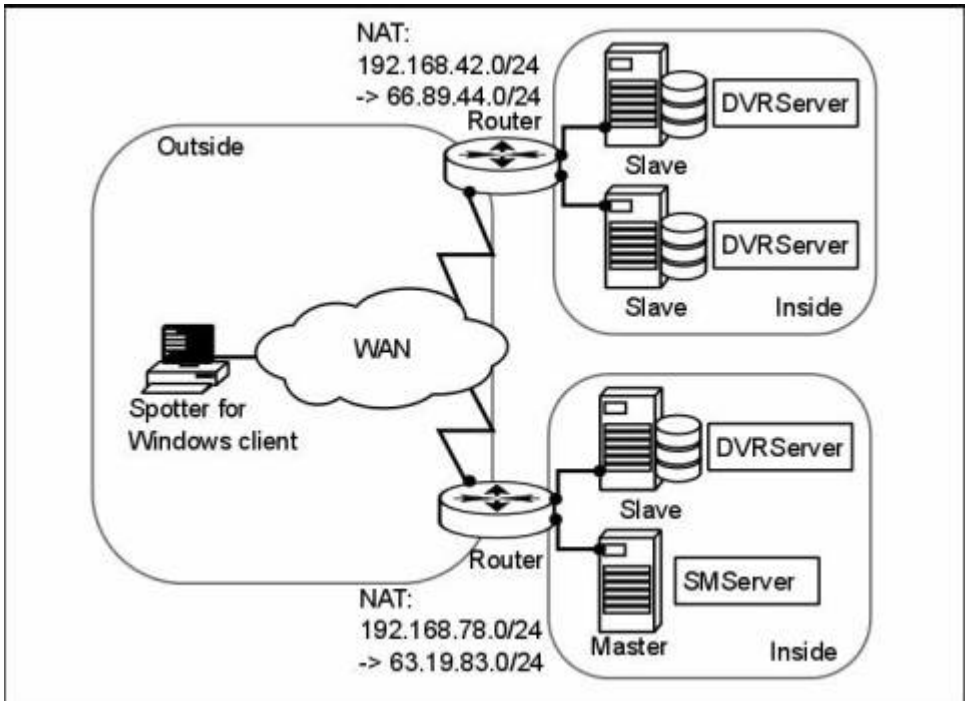
Beim Hinzufügen eines Servers zu einem Masterserver, wenn er sich nicht am lokalen Standort befindet (kann die lokale IP-Adresse nicht verwenden), muss der Benutzer die externe IP-Adresse und den ersten Port kennen, an den die Portweiterleitung durchgeführt wurde.

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, die mit **5009, 5013, 5017, 5021**... beginnen.

1.9.2.4. Mehr als ein Server auf mehreren Sites

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



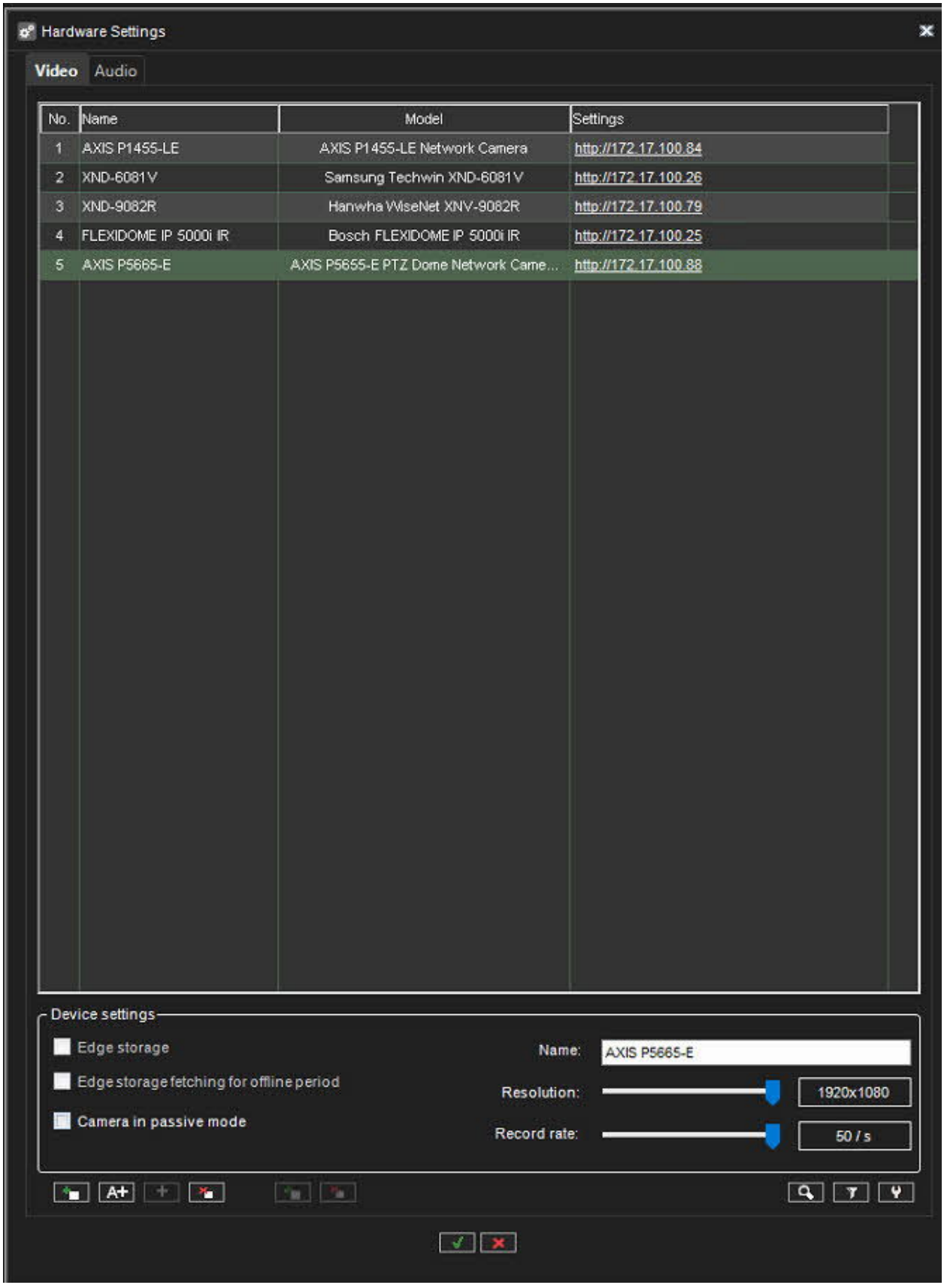
Es gilt das gleiche Prinzip wie in Szenario 2, aber diesmal muss NAT bei der Zuweisung von VMS-Servern an den Master-Server des anderen Standorts berücksichtigt werden.

oben Vorherige Nächste

1.9.3. 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



oben Vorherige Nächste

1.9.3.1. Video

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.

Beim nächsten Öffnen des Dialogs merkt sich das System die vorherige Modell- und Treiberauswahl, damit der Benutzer ähnliche Kameras schneller hinzufügen kann.

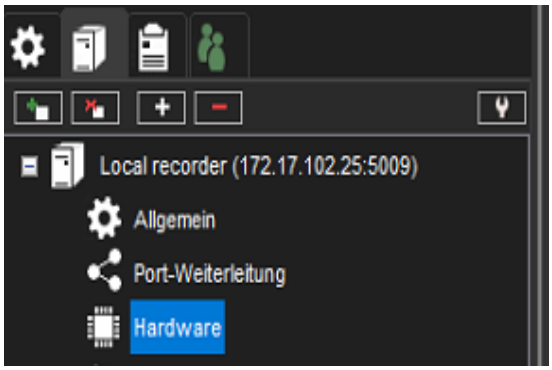
Wenn Sie die vorhandene Kamera mit der Schaltfläche Ändern öffnen, wird ein Dialog mit dem Kombinationsfeld Aktuell aktiver Fahrer-Suchmodus und Fahrername im Modus-Optionsfeld angezeigt (außer natürlich Kameras, die von Mod hinzugefügt wurden).

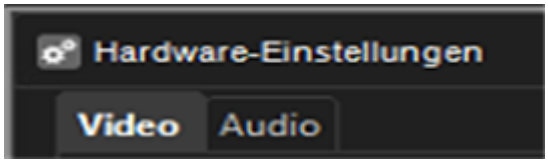
Das System speichert die zuletzt verwendeten Optionen zum Ändern von Fällen nicht, da die Optionen nur zum Hinzufügen von Kameras verfügbar sind

oben Vorherige Nächste

1.9.3.1.1. Gerät hinzufügen

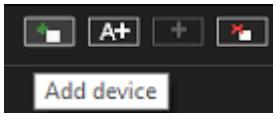
IP-Kameras oder analoge Videoserver (Encoder) können über die Registerkarte **Video** von **Hardware-Einstellungen** verwaltet werden.



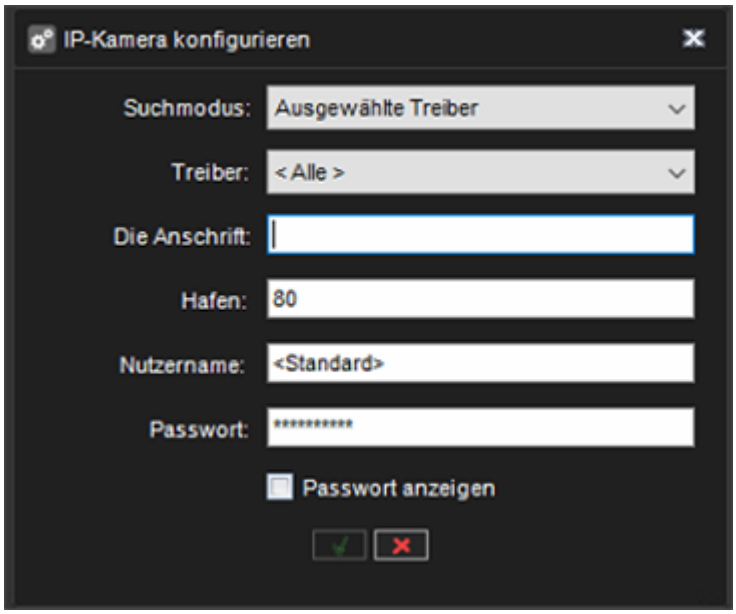


So fügen Sie eine neue IP-Kamera hinzu, wenn die IP-Adresse bekannt ist:

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



2. Geben Sie die IP-Adresse oder den DNS-Namen der Kamera oder des Videoservers ein.
    - Ändern Sie bei Bedarf die Portnummer. Normalerweise wird Port 80 verwendet.
3. Geben Sie den Benutzernamen und das Kennwort für die Kamera ein.
4. Klicken Sie auf **OK**.



Das System kommuniziert nun mit der Kamera und zeigt an, welche Fahrer sich mit der Kamera verbinden können.

Die Kamera unterstützt möglicherweise **ONVIF**. In diesem Fall kann es auch der **ONVIF** -Treiber erkennen.

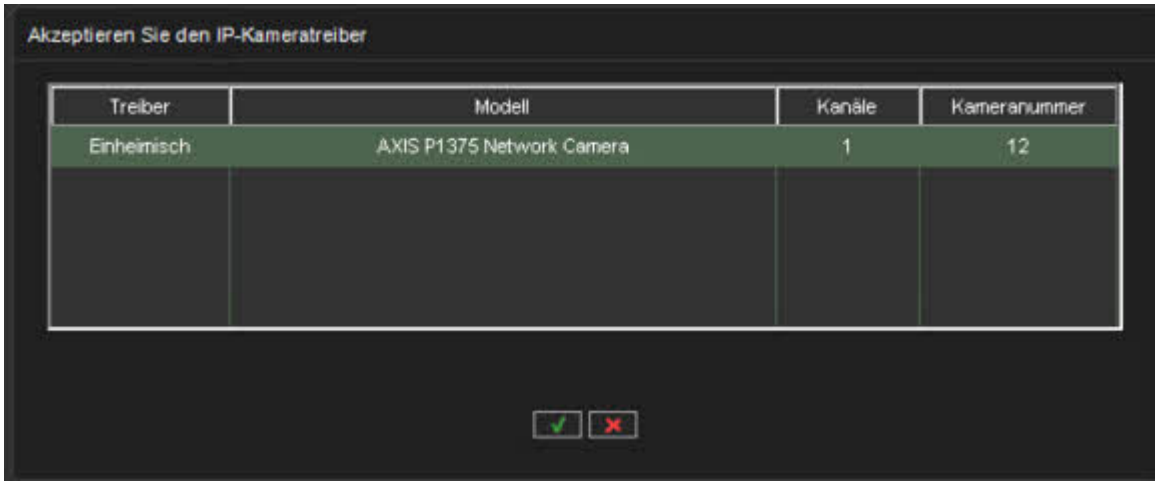
5. Wählen Sie einen Treiber aus der Liste aus.

In der Regel wird empfohlen, den **Native** -Treiber zu verwenden, falls vorhanden.

Bei Mehrkanalgeräten kann die Option **Channels** das Gerät mit weniger als der maximalen Anzahl von Kanälen hinzufügen.

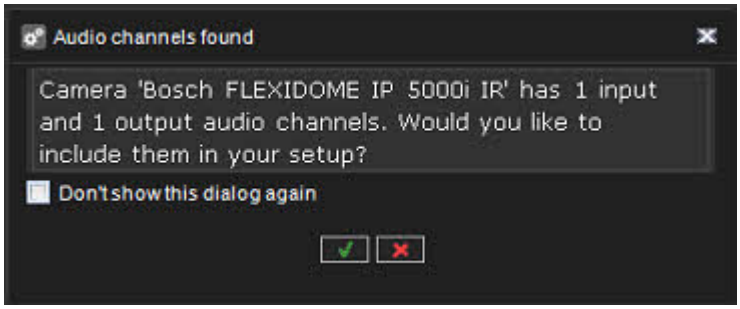
Der Benutzer kann auch sehen, was die Kameranummer des Geräts sein wird

6. Klicken **OK**

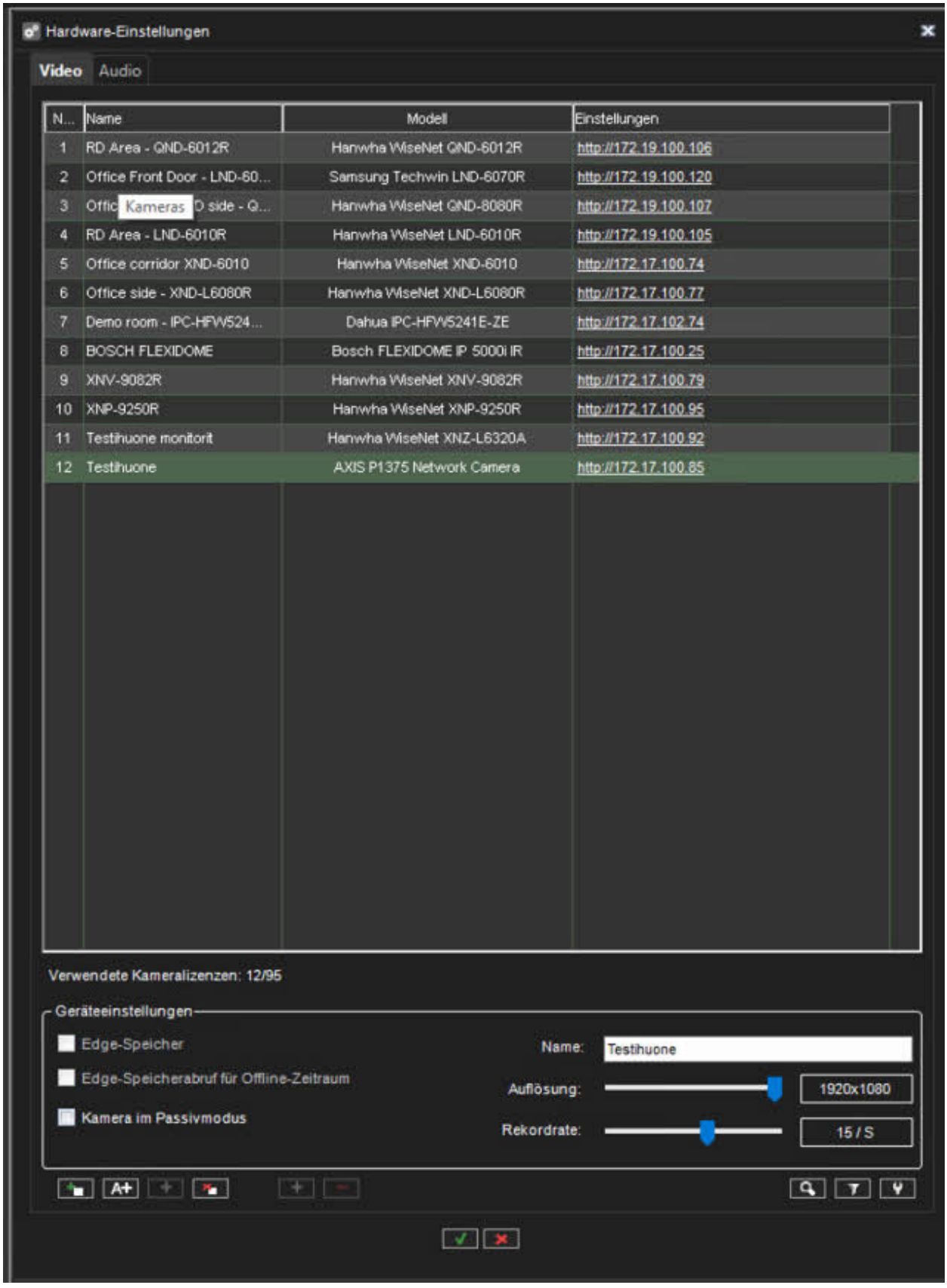


Wenn die Kamera Audiokanäle unterstützt, sehen Sie einen Dialog darüber.

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



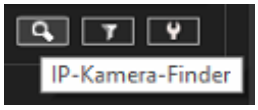
Nachdem die Kamera hinzugefügt wurde, kann das Gerät in der Liste **Hardware-Einstellungen** gefunden werden



oben Vorherige Nächste

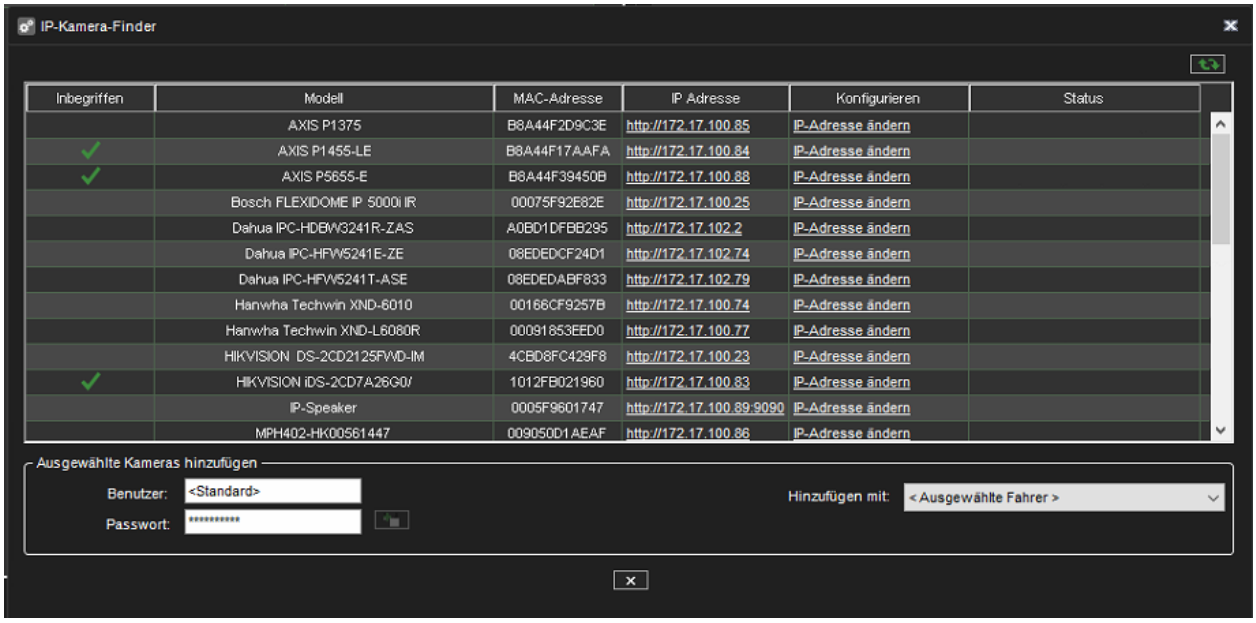
1.9.3.1.2. IP-Kamera-Finder

1. Klicken Sie auf den **IP-Kamerafinder**



Das System durchsucht 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 resultierende Liste wird angezeigt, nachdem die Suche abgeschlossen ist.



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.

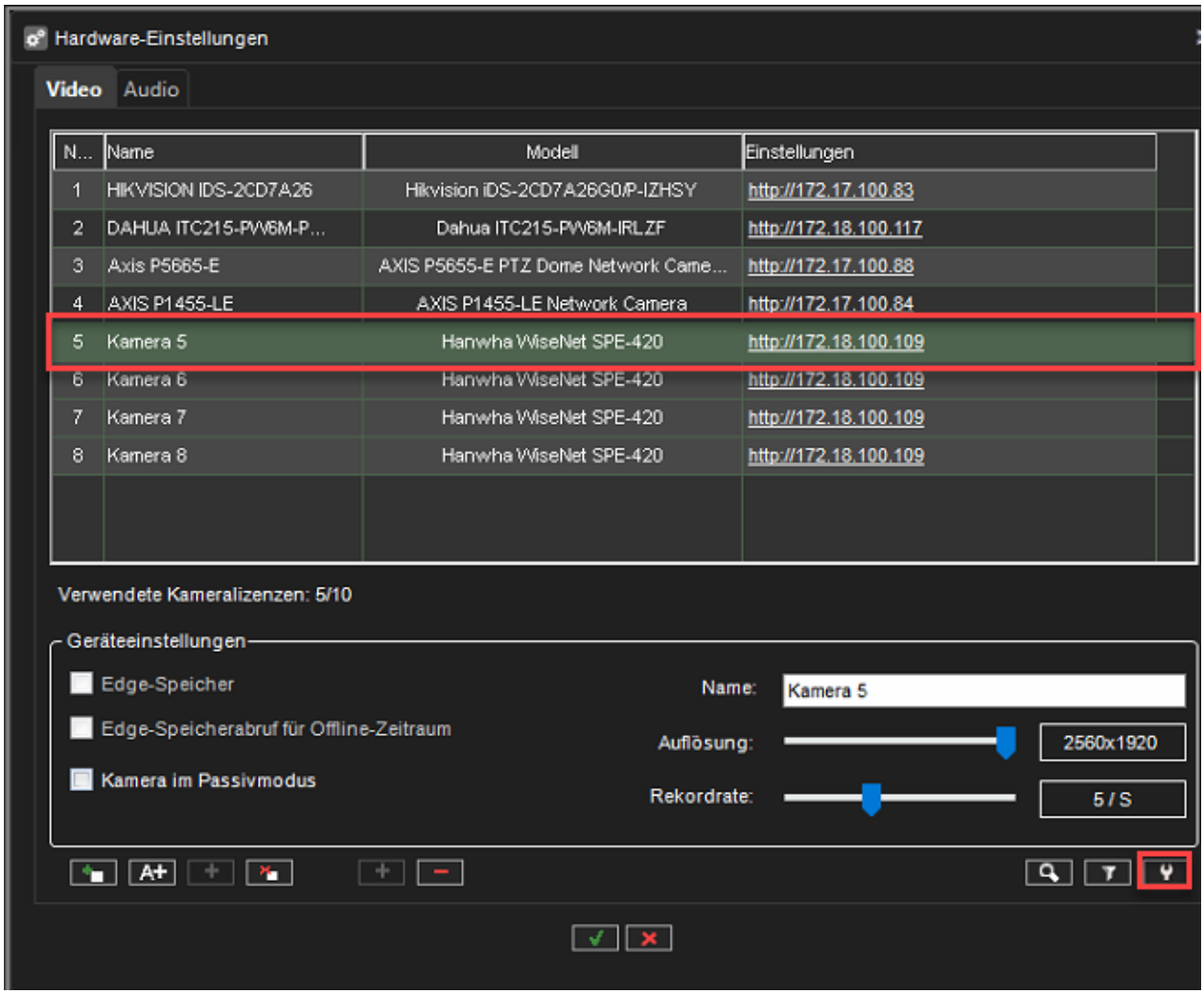
4. Wenn das System einige der ausgewählten Kameras nicht hinzufügen kann, wird eine Fehlermeldung in der Spalte **Status** angezeigt; Sie können die Schritte 4 bis 5 für die Kameras mit den richtigen Anmeldeinformationen wiederholen.
5. Klicken Sie auf **Schließen**, um den **IP-Kamerafinder** zu beenden.
6. Speichern Sie die Hardware-Einstellungen durch Drücken von **OK** in der Liste:

oben Vorherige Nächste

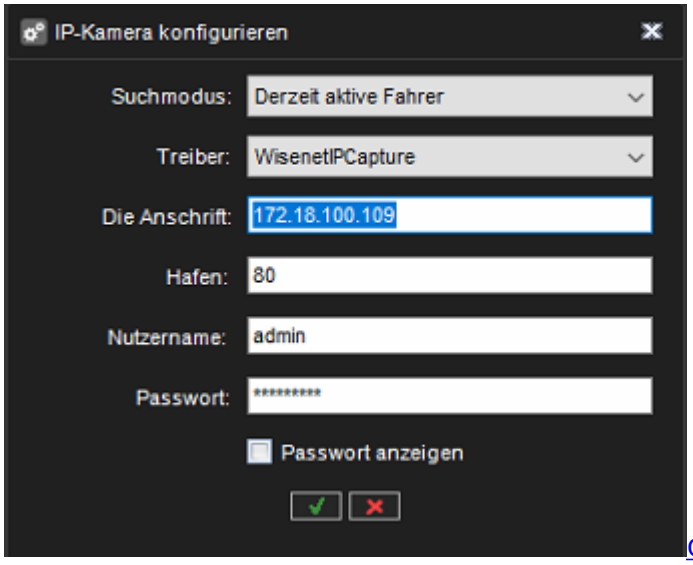
1.9.3.1.3. IP-Kamera bearbeiten

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



oben Vorherige Nächste

1.9.3.1.4. Entfernen von IP-Kameras und Encodern

Wenn Sie den Dialog „**Hardwareeinstellungen**“ im System Manager öffnen, sehen Sie 2 Schaltflächen unter der Liste der Kameras:

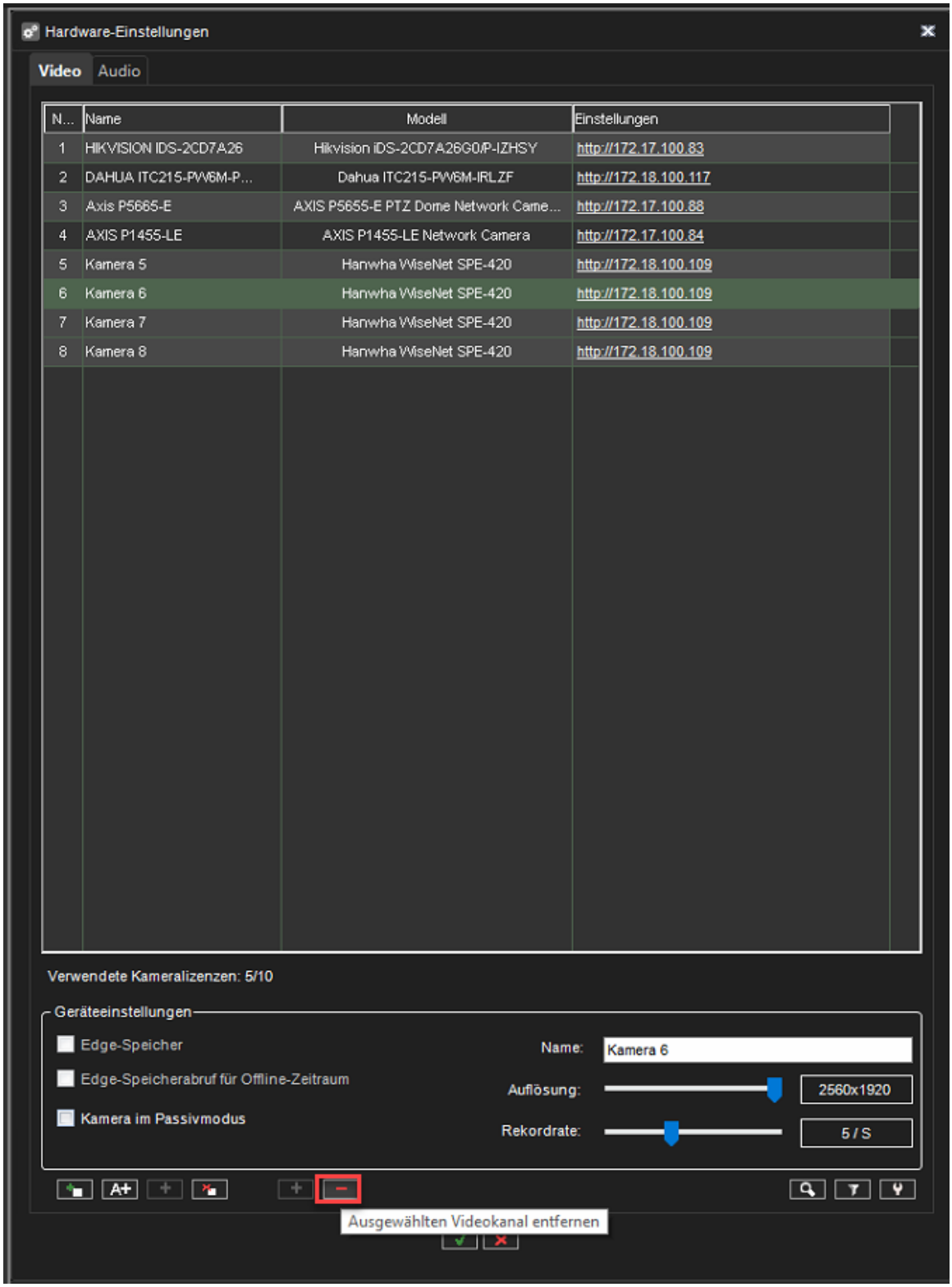
- Die Schaltfläche "**Videokanal zum ausgewählten Gerät hinzufügen**"
- Die Schaltfläche „**Videokanal vom ausgewählten Gerät entfernen**“

So entfernen Sie eine IP-Kamera:

1. Kamera aus der Liste auf der Registerkarte **Video** auswählen
2. Klicken Sie in der unteren rechten Ecke der Registerkarte auf **Ausgewähltes Gerät entfernen**.
3. Wenn Sie aufgefordert werden, den Löschvorgang zu bestätigen, klicken Sie auf **OK**.

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE

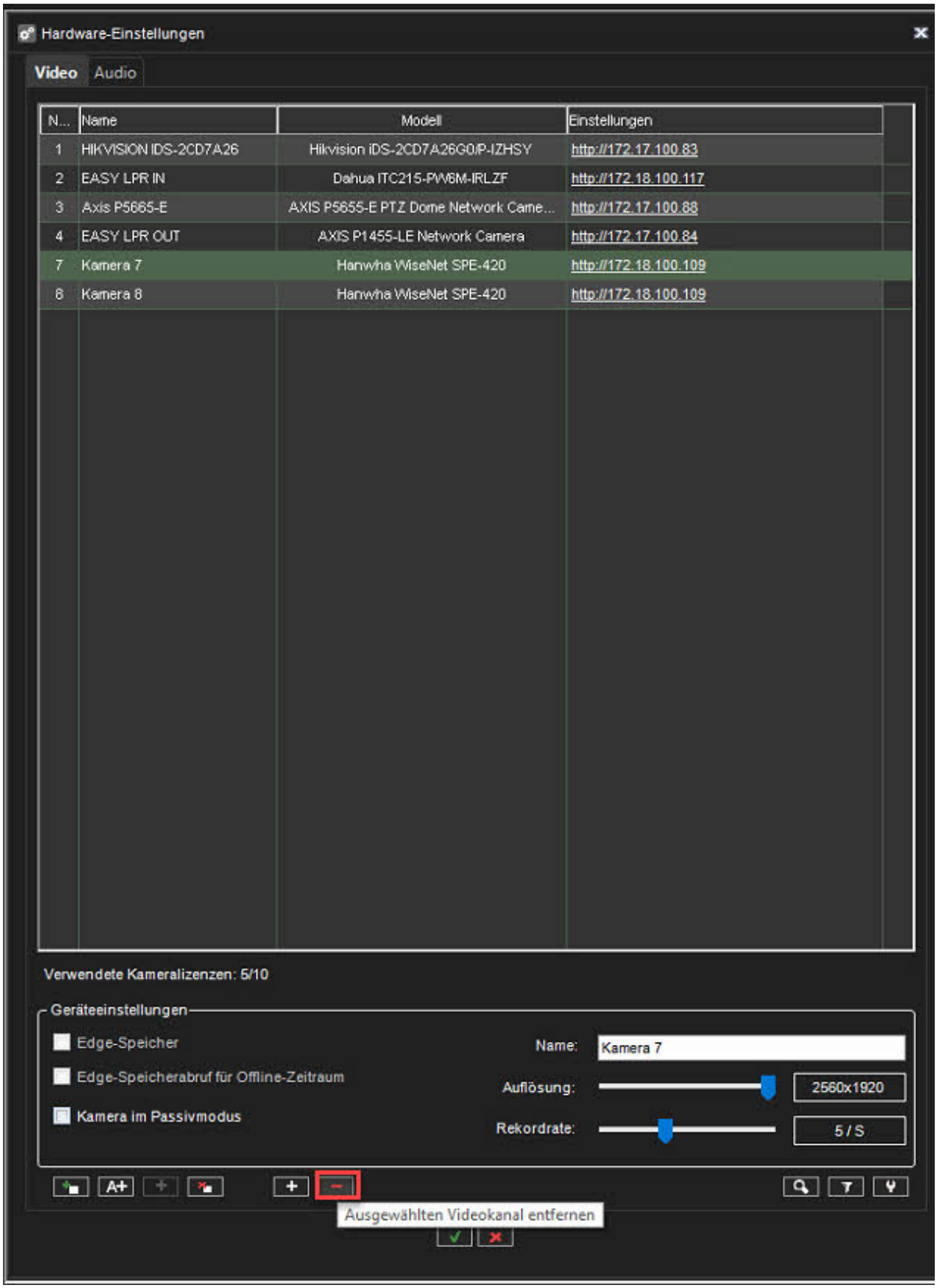


So entfernen Sie Videokanäle vom Encoder oder Kameras mit mehreren Linsen:

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

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE



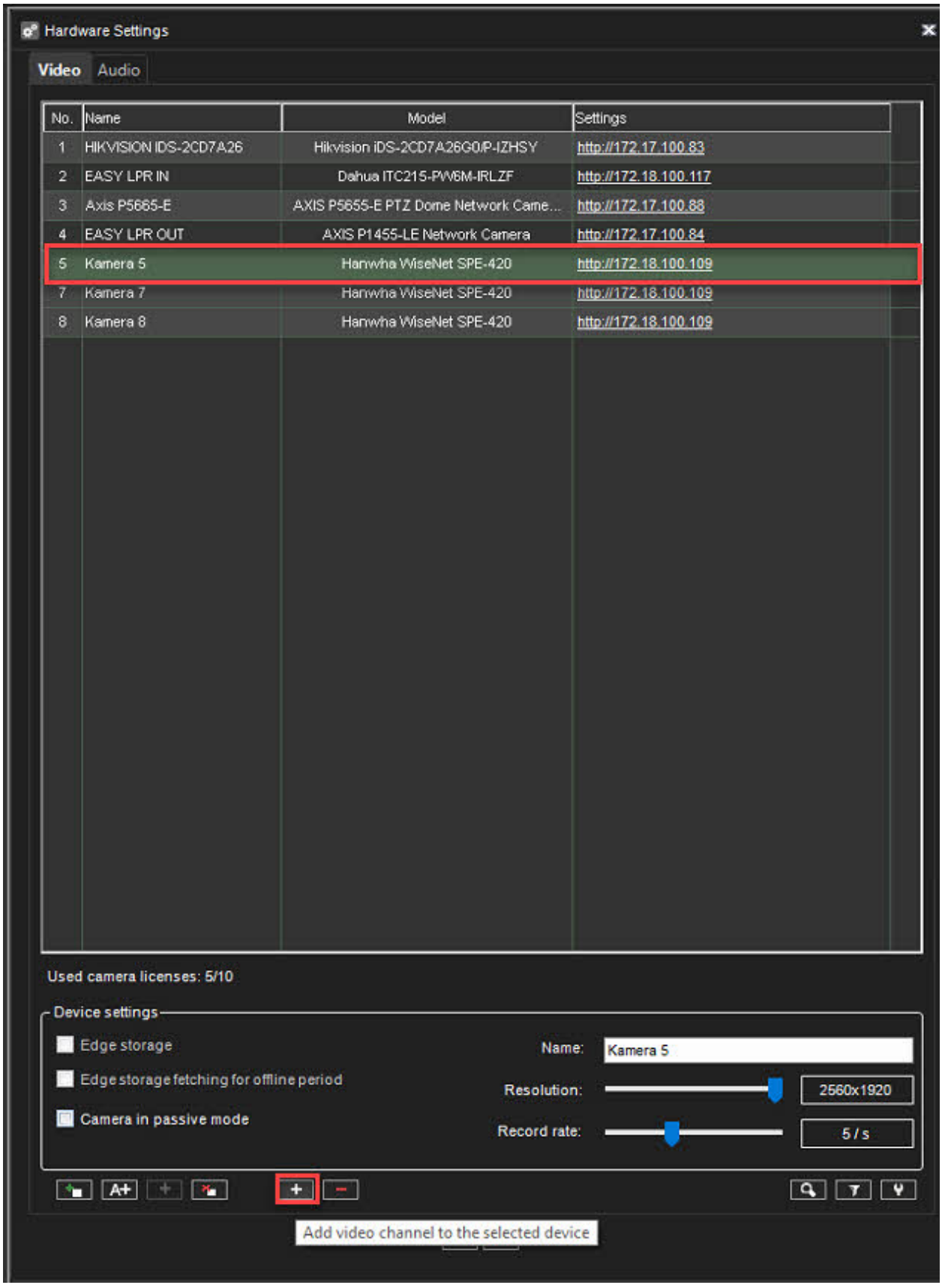
Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

So fügen Sie dem Encoder oder Kameras mit mehreren Objektiven Videokanäle hinzu:

1. Wählen Sie das richtige Gerät aus der Liste
2. Klicken Sie auf **Videokanal zum ausgewählten Gerät hinzufügen**
3. Klicken **OK**

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE



Mirasys Ltd - C1CD, Vaisalantie 2-8, 02130 - Espoo, Finland
Tel +358 (0)9 2533 3300 - info@mirasys.com - www.mirasys.com

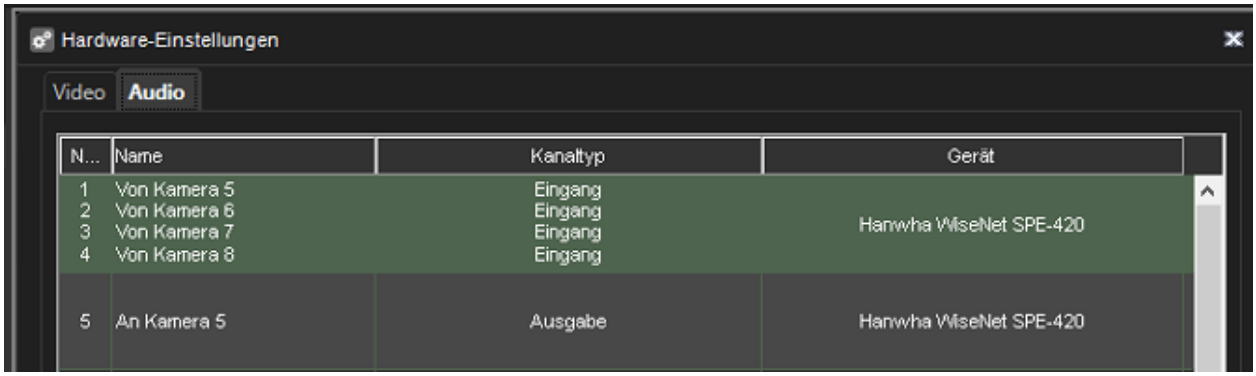
1.9.3.2. Audio

Wenn eine Kamera über kompatible IP-Audio-Eingangs- oder -Ausgangskanäle verfügt, können Sie diese gleichzeitig hinzufügen, wenn Sie die Kamera über die automatischen Suchwerkzeuge hinzufügen.

Nachdem dem System IP-Audioeingänge und -ausgänge für eine Kamera hinzugefügt wurden, können sie über die Registerkarte **Audio** bearbeitet und entfernt werden.

Angezeigte Informationen:

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



oben Vorherige Nächste

1.9.3.3. Geräteeinstellungen

Edge-Speicher

Die Edge-Speicherfunktionalität ermöglicht eine unterbrechungsfreie Aufzeichnung bei Netzwerkausfällen. In der Praxis kann bei In-Netzwerk-Blackout der Video-Feed auf einer SD-Speicherkarte der Kamera gespeichert werden.

Sobald die Netzwerkverbindung wiederhergestellt ist, wird das Video von der SD-Karte der Kamera an den Server übertragen.

Bitte lesen Sie in der Dokumentation des Kameraherstellers nach, welche Kameras diese Funktion unterstützen.

Edge Storage muss in den Geräteeinstellungen aktiviert sein.

Diese Funktion wird ausschließlich über das Konfigurationsdienstprogramm der Kamera konfiguriert.

Anweisungen zum Aktivieren des Edge-Speichers finden Sie in der Dokumentation der Kamera.

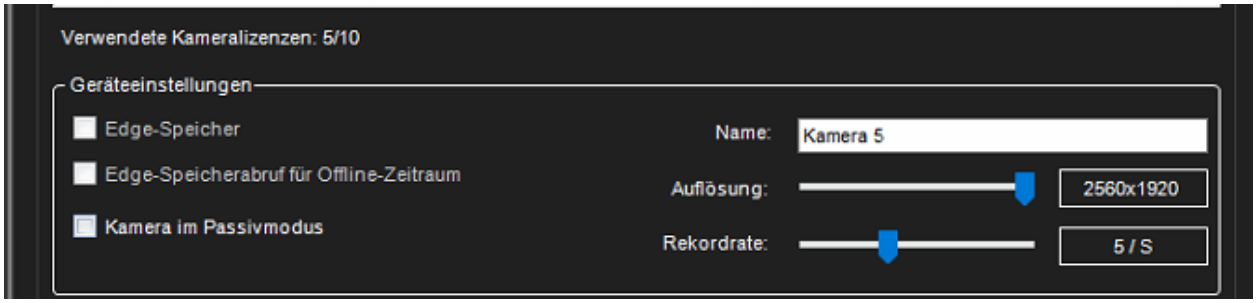
Edge-Speicherabruf für Offline-Zeitraum

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.

Kamerainformationen

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



oben Vorherige Nächste

1.9.4. Hinzufügen und Entfernen von VMS-Servern

Sie können (je nach Lizenz) von 1 bis zu einer unbegrenzten Anzahl von Servern in einem System haben.

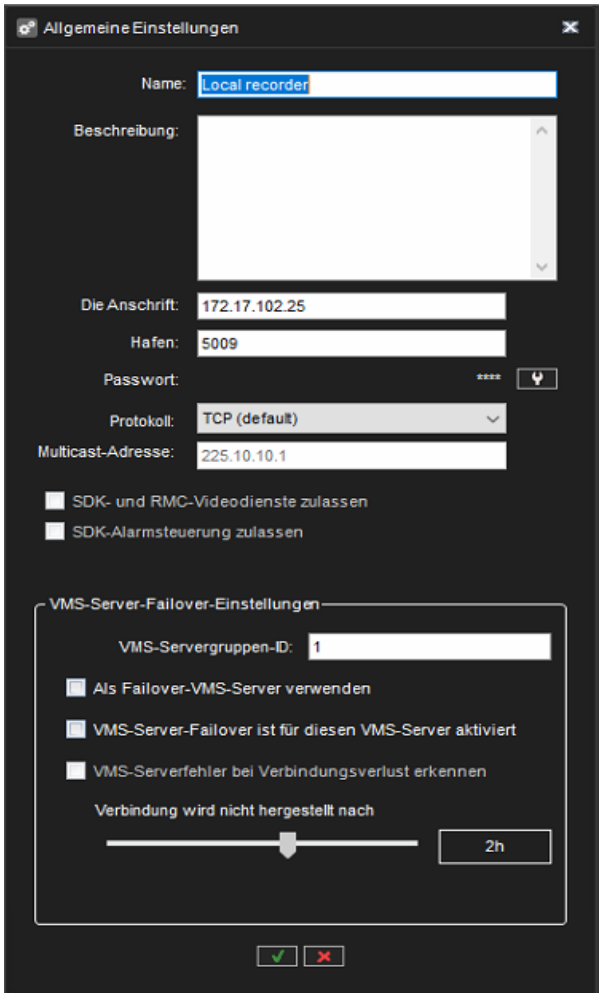
Ein Server sollte nicht zu mehr als einem Master Server (SMServer) gehören.

Sie können für jeden Server ein Kennwort angeben.

Das System fordert zur Eingabe des Kennworts auf, wenn jemand versucht, den Server zu einem anderen System hinzuzufügen.

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

1. Öffnen Sie die Registerkarte **VMS-Server** 
2. Klicken Sie **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.*



So entfernen Sie einen Server aus dem System:

1. Wählen Sie den Server aus, den Sie entfernen möchten.
2. Klicken Sie auf **VMS-Server**  . entfernen
3. Klicken Sie zur Bestätigung auf **OK**.

Verbindungsstatus:

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

HINWEIS:

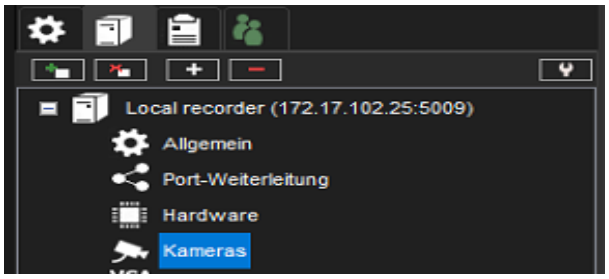
Wenn Sie Mirasys VMS als Slave-Server hinzugefügt haben, gehen Sie bitte wie folgt vor:

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

oben Vorherige Nächste

1.9.5. Kameras

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

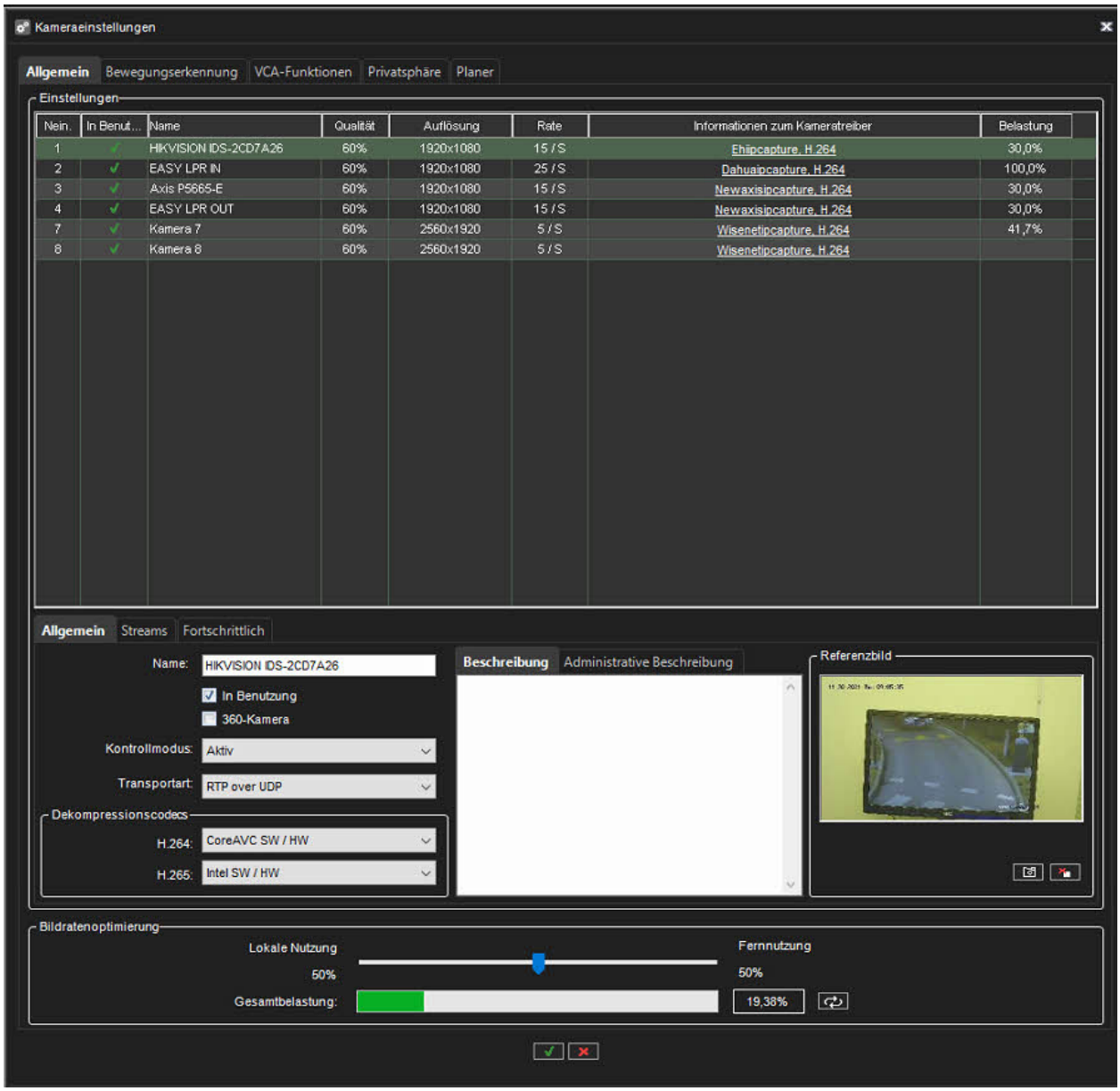


Kameraeinstellungen enthalten Einstellungen für:

- Allgemein
- Bewegungserkennung
- VCA-Einstenllung
- Privatsphäre
- Planer

oben Vorherige Nächste

1.9.5.1. Kameraeinstellungen



oben Vorherige Nächste

1.9.5.1.1. Allgemeine Einstellungen

Name

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

Im Einsatz

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

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).

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 .

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.

Dekomprimierungscodecs.

Codecs werden zum Kodieren und Dekodieren von Videodaten verwendet

Beschreibung

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

Administrative Beschreibung.

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

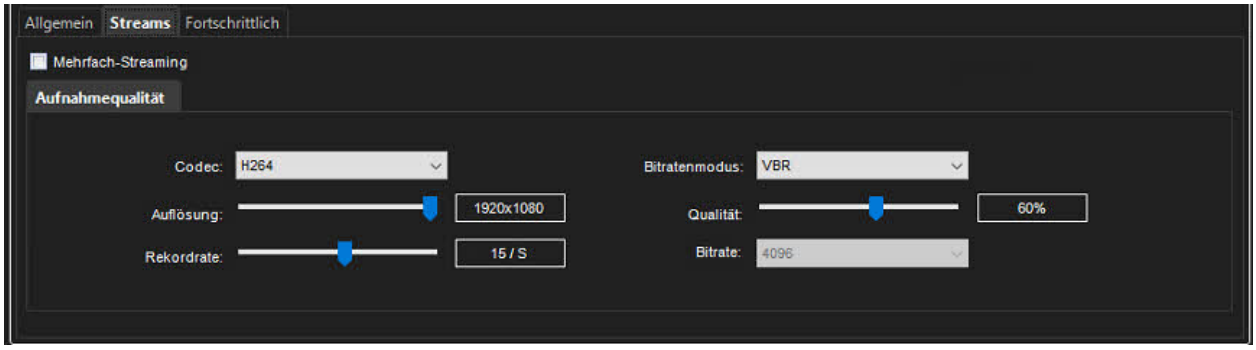
Reference image

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**.

oben Vorherige Nächste

1.9.5.1.2. Streams

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



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.

Bitrate mode.

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

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.

Auflösung

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

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)

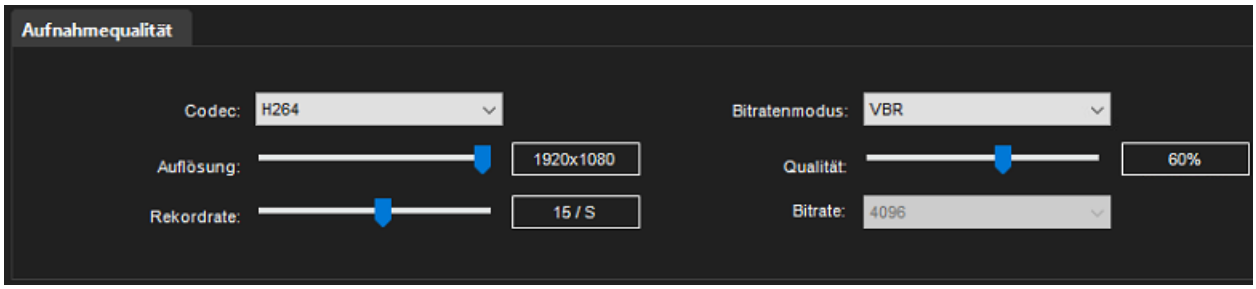
oben Vorherige Nächste

1.9.5.1.2.1. Multi-Streaming

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.

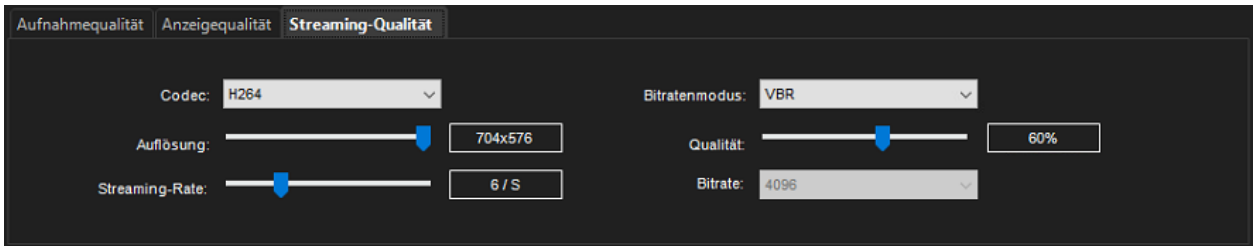
Aufnahmequalität

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



Anzeigequalität

Streaming-Qualität



oben Vorherige Nächste

1.9.5.1.3. Fortschrittlich

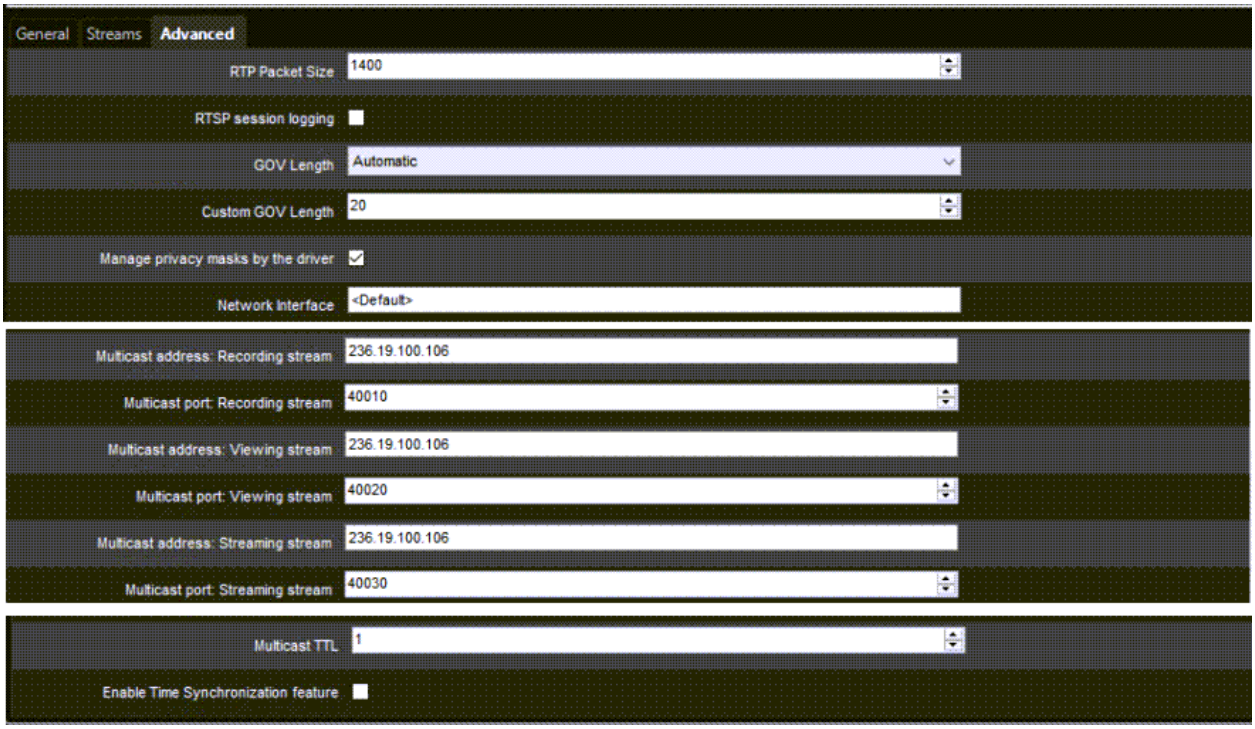
Diese Registerkarte enthält kamera- oder treiberspezifische einzigartige Einstellungen. Ein Treiberupdate kann dieser Registerkarte zusätzliche Werte bringen.

Die Auswahl mehrerer Kameras ist mit den Tasten SHIFT oder CTRL möglich.

Bitte beachten Sie, dass Sie bei Auswahl mehrerer Kameras nicht Parameter einstellen können, die nicht von allen ausgewählten Kameras unterstützt werden.

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



oben Vorherige Nächste

1.9.5.1.4. Bildratenoptimierung

Der Schieberegler soll die Last abschätzen, wenn der Server sowohl als Aufzeichnungsserver als auch als Client-Workstation verwendet wird.

Die Standardannahme für die lokale/remote Nutzung beträgt 50 %.

Wenn dies die Anzahl der Kameras oder die Verwendung der gewünschten Kameraeinstellungen einschränkt, kann der Schieberegler in Richtung 100 % gezogen werden, um alle gewünschten Kameras mit den gewünschten Einstellungen hinzuzufügen.

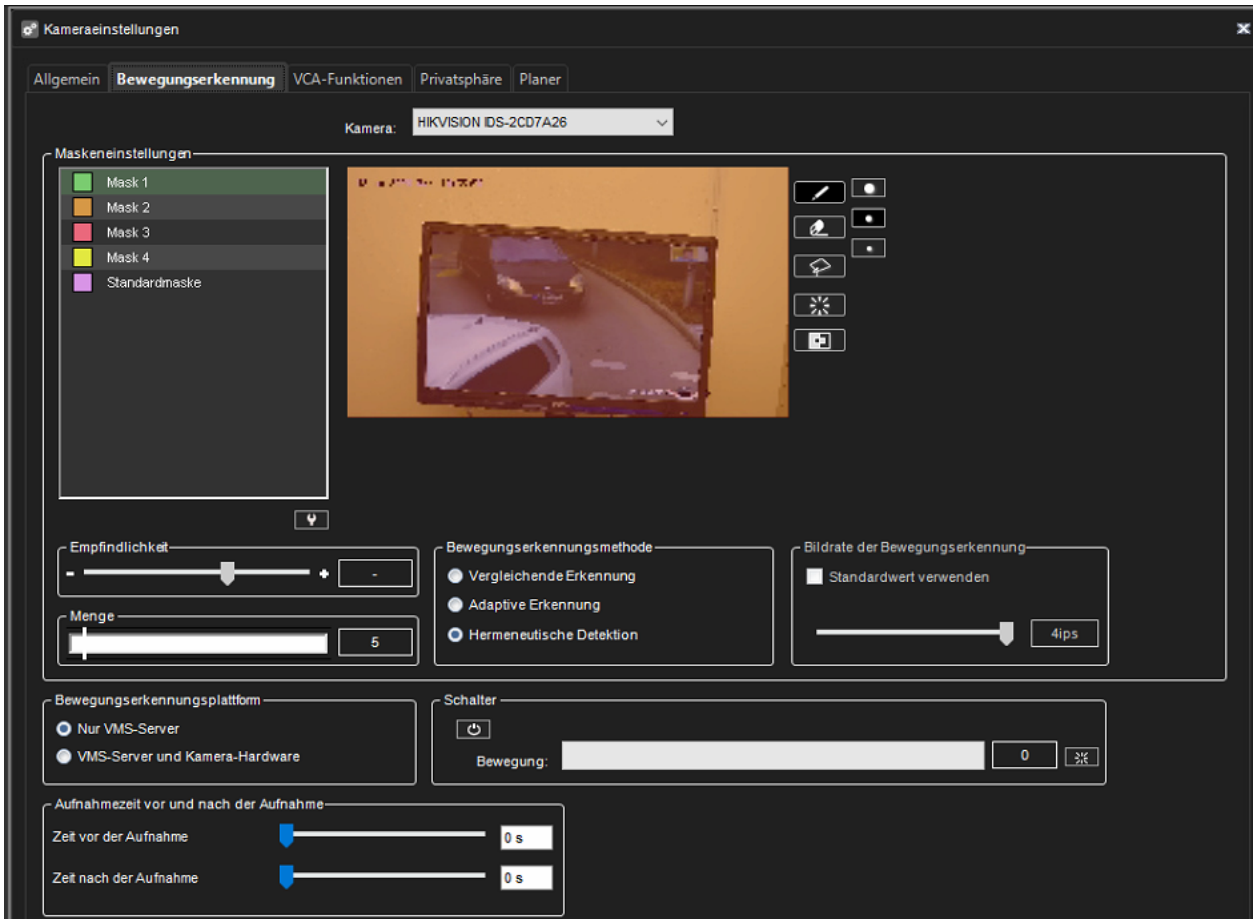
Es sollte jedoch darauf geachtet werden, den Server in einer solchen Situation nicht zu überlasten.

Nachdem Sie festgelegt haben, ob die Bildraten für die lokale oder die Remote-Anzeige optimiert werden sollen, klicken Sie auf **Optimieren.**

Das System setzt die Aufzeichnungsraten auf die höchstmöglichen Werte.

oben Vorherige Nächste

1.9.5.2. Bewegungserkennung



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.

Methoden zur Bewegungserkennung

Vergleichende Erkennung

Vergleicht ein Bild mit dem Bild davor. Überschreiten die Differenzen die eingestellten Grenzen, erkennt das System Bewegung.

Sie können die vergleichende Bewegungserkennung unter den meisten Bedingungen verwenden.

Wenn jedoch im Hintergrund viel Bewegung stattfindet, z. B. Regen, sich bewegende Blätter oder Änderungen der Lichtverhältnisse, verwenden Sie die adaptive Bewegungserkennung.

Adaptive Erkennung

Vergleicht jedes Bild mit einem Hintergrundbild. Das System lernt automatisch das Hintergrundbild und die dazugehörige Bewegung.

So interpretiert das System beispielsweise sich bewegende Blätter nicht als Bewegung.

Wenn sich außerdem mehr als die Hälfte der Pixel in einem Bild ändern, schließt das System daraus, dass sich die Lichtverhältnisse geändert haben.

Als Ergebnis setzt es das Referenzbild zurück und beginnt erneut, es zu lernen.

Hermeneutische Entdeckung

Ist ein ausgeklügeltes Bewegungserkennungssystem für herausfordernde Wetterbedingungen (z. B. starker Regen, „lautes“ Hintergrundbild usw.) und Situationen, in denen externe Tools zur Analyse von Videoinhalten (VCA) verwendet werden.

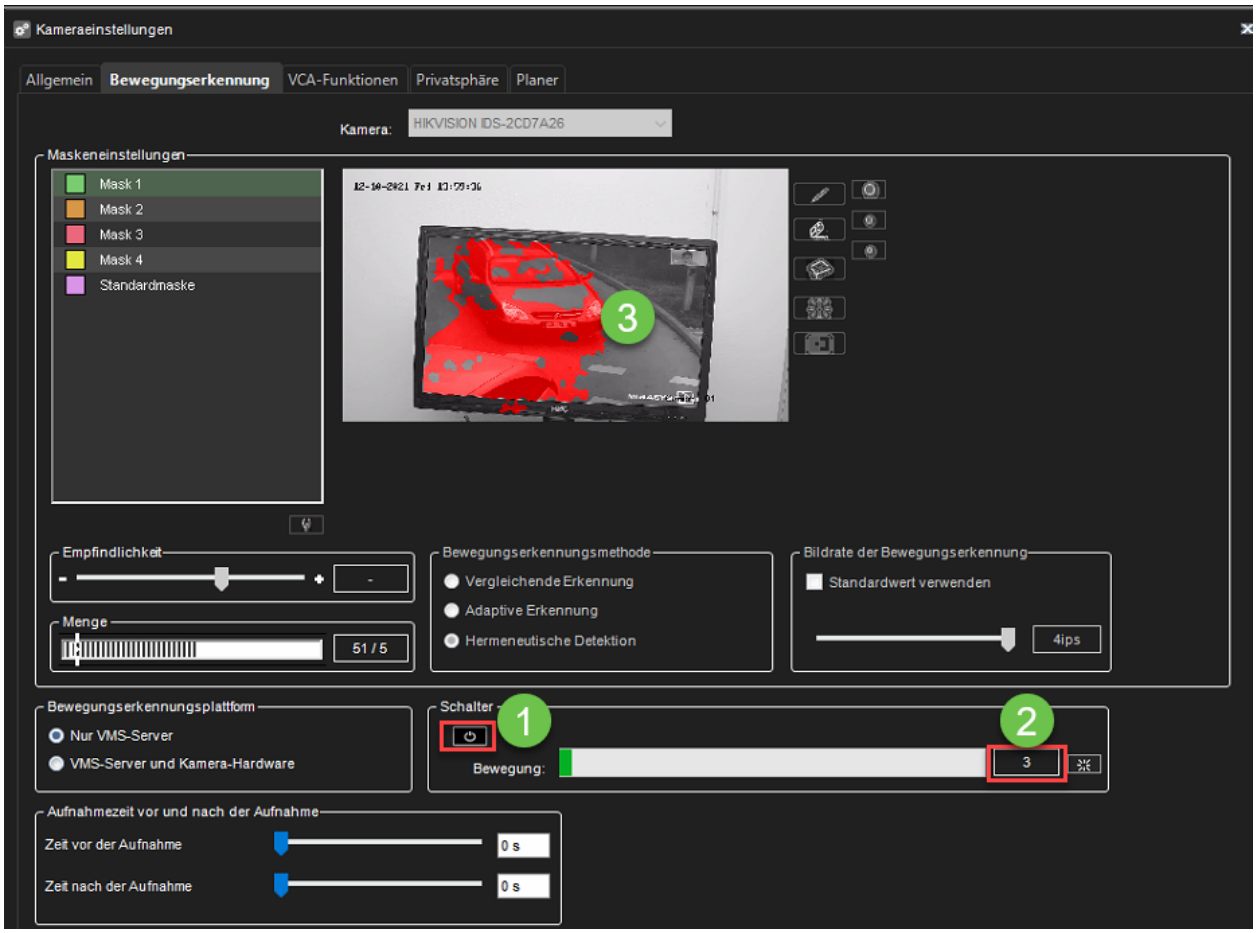
Es sollte beachtet werden, dass die hermeneutische Erkennung mehr Verarbeitungsressourcen erfordert als die anderen Erkennungsmethoden.

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.

Schalter

1. Ermöglichen**Schalter**
2. Überprüfen Sie die Bewegungswerte
3. Das Kamerabild zeigt an, welcher Bereich des Kamerabildes eine Bewegungserkennungsaufzeichnung verursacht



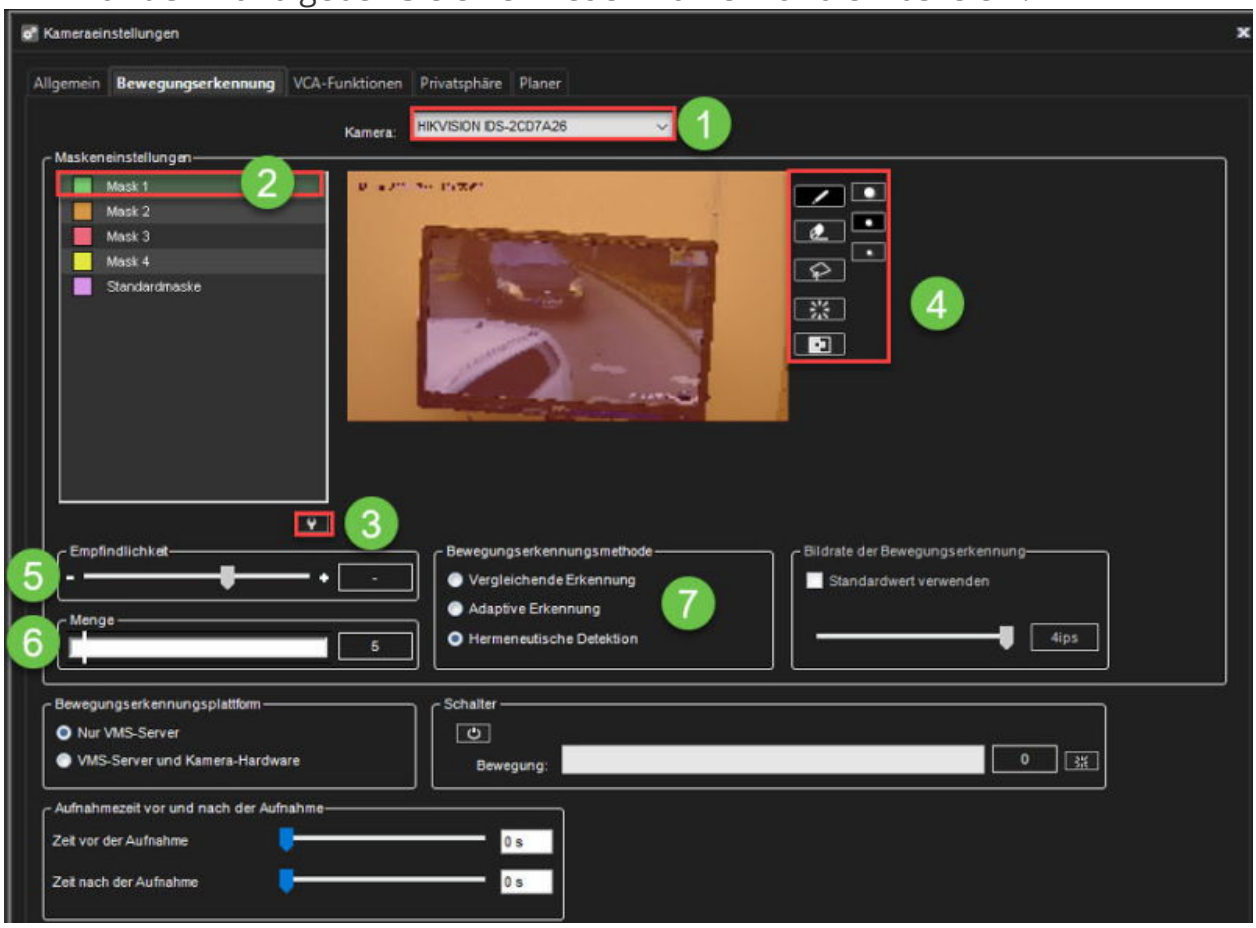
Pre- and Post- recording time

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.

oben Vorherige Nächste

1.9.5.2.1. 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.



4. 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.
5. Stellen Sie die Erkennungsempfindlichkeit ein.
6. Stellen Sie die minimale Bewegungsmenge ein.
7. 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.

Zeichenutensilien:

Werkzeug	Name	Beschreibung
	Bleistift	Verwenden Sie zum Einstellen des Bewegungserkennungsbereichs. Wählen Sie die Stiftgröße aus, indem Sie auf eine der Schaltflächen für die Werkzeuggröße klicken (groß, mittel, klein).
	Radiergummi	Verwenden Sie diese Option, um ausgewählte Bereiche zu löschen, die Sie nicht einschließen möchten. Wählen Sie die Radiergummigröße aus, indem Sie auf eine der Schaltflächen für die Werkzeuggröße klicken (groß, mittel, klein).
	Lasso	Wählen Sie mit geraden Linien Bereiche aus. Wenn das Stiftwerkzeug ausgewählt ist, fügt die Verwendung dieses Werkzeugs ausgewählten Bereichen hinzu. Wenn das Radiergummi-Werkzeug ausgewählt ist, wird dieses Werkzeug aus der Auswahl entfernt. Klicken Sie auf das Bild, bei dem Sie die Auswahl beginnen möchten. Klicken Sie erneut auf die Stelle, an der Sie die Linie verankern möchten, und ändern Sie die Richtung. Um die Auswahl abzuschließen, klicken Sie auf den Startpunkt. Der ausgewählte Bereich wird rot gestrichen oder die rote Farbe wird entfernt.
	Füllen/Löschen	Wenn das Stiftwerkzeug ausgewählt ist, wird durch Klicken auf diese Schaltfläche der gesamte Bildbereich ausgewählt. Wenn das Radiergummi-Werkzeug ausgewählt ist, wird durch Klicken auf diese Schaltfläche alle Auswahlen entfernt.
	Umkehren	Kehrt ausgewählte und nicht ausgewählte Bereiche um. Manchmal ist es einfacher, den Bereich auszuwählen, den Sie nicht maskieren möchten, und dann die Auswahl umzukehren.
	Werkzeuggröße	Klicken Sie auf eine der Schaltflächen, um die Größe des Bleistifts oder Radierers auszuwählen (groß, mittel, klein).

oben Vorherige Nächste

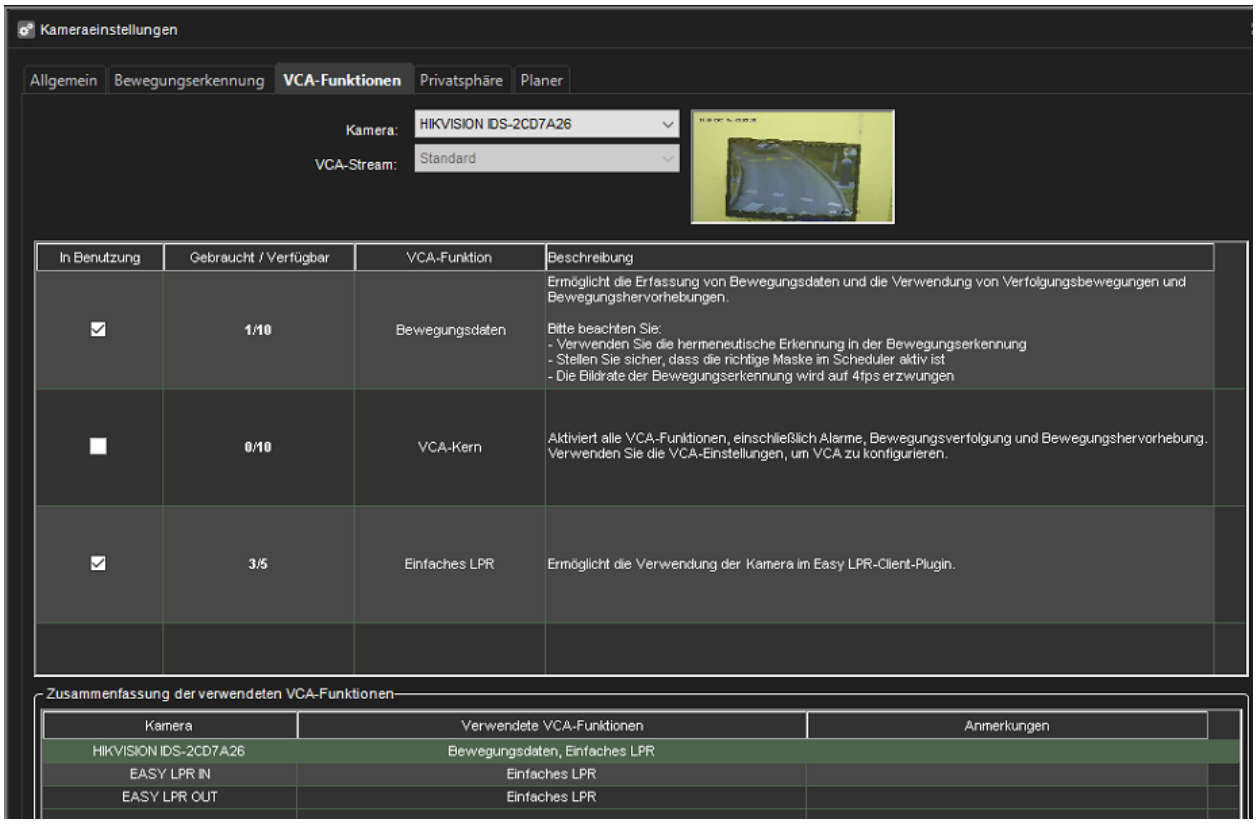
1.9.5.3. VCA-Funktionen

Wenn die Softwarelizenz Video Content Analytics (VCA)-Funktionalität beinhaltet, kann sie kameraspezifisch auf der Registerkarte **VCA Funktionalität** verwaltet werden.

Je nach Lizenz können auf der Registerkarte bestimmte VCA-Funktionalitäten aktiviert oder deaktiviert werden.

Es ist möglich zu steuern, welcher Stream (in einer konfigurierten Kamera, um mehrere Streams zu verwenden) für VCA verwendet wird.

Dies wird über das Pulldown-Menü unter der Kameraauswahl erreicht (siehe folgende Abbildung)



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.

oben Vorherige Nächste

1.9.5.4. Privatsphäre

Unter dem Datenschutz-Menü können Sie die Privatzonen der Kamera und die Gesichts- und Bewegungsunschärfe-Funktionalität steuern.

Zu beachten: Der Inhalt der Datenschutzfunktionen ist (für den Benutzer) nur verfügbar, wenn er für die Kamera definiert ist.

(D. h., wenn die Kamera z. B. keine Gesichtsunschärfe definiert hat, dürfen die Gesichter dieser Kamera nicht unscharf werden – selbst wenn die Benutzergruppe des Endbenutzers die Berechtigungsstufe so eingestellt hat, dass nur unverwackeltes Material angezeigt wird.

Dies gilt auch beim Export der Materialien.

oben Vorherige Nächste

1.9.5.4.1. Privatzone auf der Kamera

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**.

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**.

oben Vorherige Nächste

1.9.5.4.2. Privatzone auf dem Client

Auf dem Spotter-Client: Diese Privatzonen werden nur auf dem Viewer-Client implementiert.

Auf diese Weise kann das gesamte Video aufgezeichnet und exportiert werden, die datenschutzgeprüften Bereiche sind jedoch nur für Benutzer zugänglich, die dazu berechtigt sind.

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**.

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**.

oben Vorherige Nächste

1.9.5.4.3. Unschärfe von Objekten

Als zusätzliche Privatsphäre können die Einstellungen „Gesichter verwischen“ und „Bewegte Objekte verwischen“ eingerichtet werden.

Wenn die gesichts- oder bewegungsbasierte Unschärfe für eine Kamera aktiviert ist, stehen diese auch auf der Spotter-Seite zur Verfügung (sofern der Benutzer über ausreichende Berechtigungen verfügt).

Die Unschärfe wird auf Spotterseite nicht funktionieren - oder beim Export des Videomaterials für die Kameras, wenn diese nicht auf der Systemadministratorseite ausgewählt wurden.

Höhere Auflösungen, die für die Algorithmen verwendet werden, bedeuten eine höhere Genauigkeit der Algorithmen – aber auch höhere CPU-Last.

Gesichter verwischen

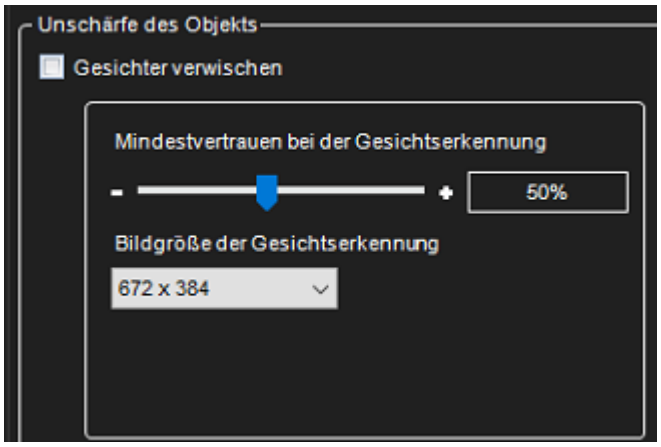
Mindestvertrauen bei der Gesichtserkennung

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



Verwischen Sie sich bewegende Objekte

Empfindlichkeit der Bewegungserkennung

Wie empfindlich Pixel im Bild als Bewegungspixel erkannt werden

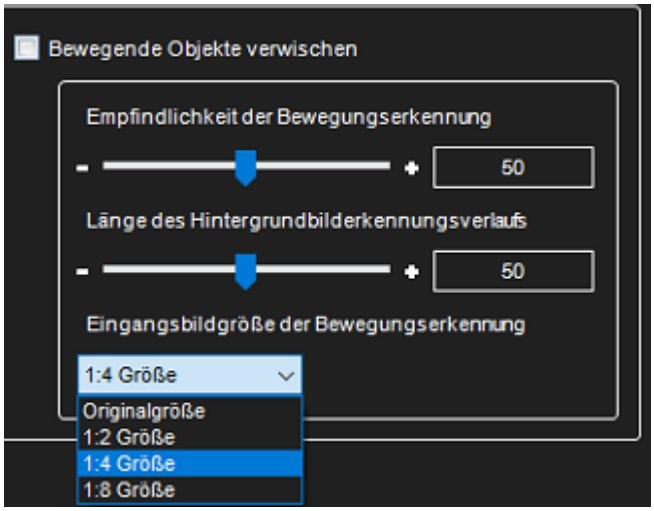
Länge des Hintergrundbilderkennungsverlaufs

Wie schnell stationäre Objekte als Hintergrund erkannt werden

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

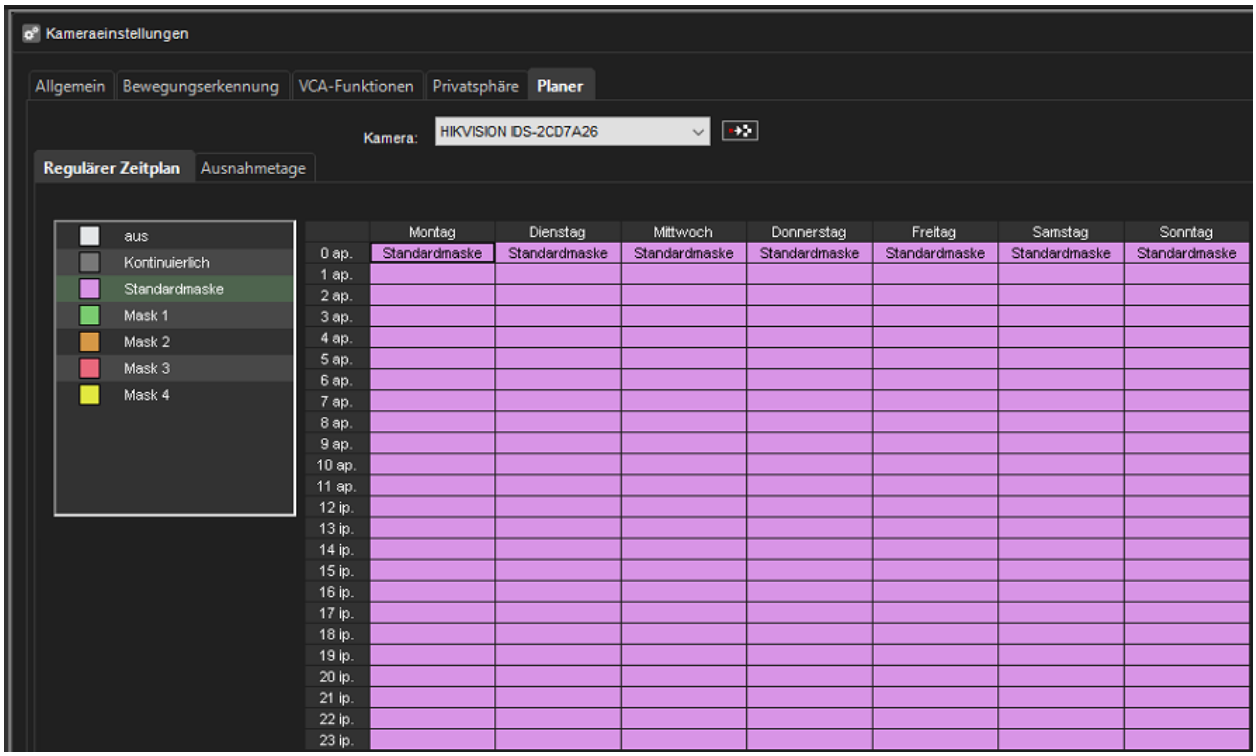


oben Vorherige Nächste

1.9.5.5. Planer

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

Standardmäßig wird 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. Verwenden Sie beispielsweise tagsüber und nachts unterschiedliche Bewegungserkennungsmasken.

Stellen Sie zuerst den regulären Wochenplan auf der Registerkarte **Regulärer Zeitplan** und dann, falls erforderlich, Ferienpläne auf der Registerkarte **Feiertage** ein.

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.*

Sie können auch auf die erste Zelle klicken, die UMSCHALTTASTE gedrückt halten und dann auf die letzte Zelle klicken.

Um alle Stunden in einer Spalte oder Zeile zu ändern, klicken Sie auf die Spalten- oder Zeilenüberschrift.

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

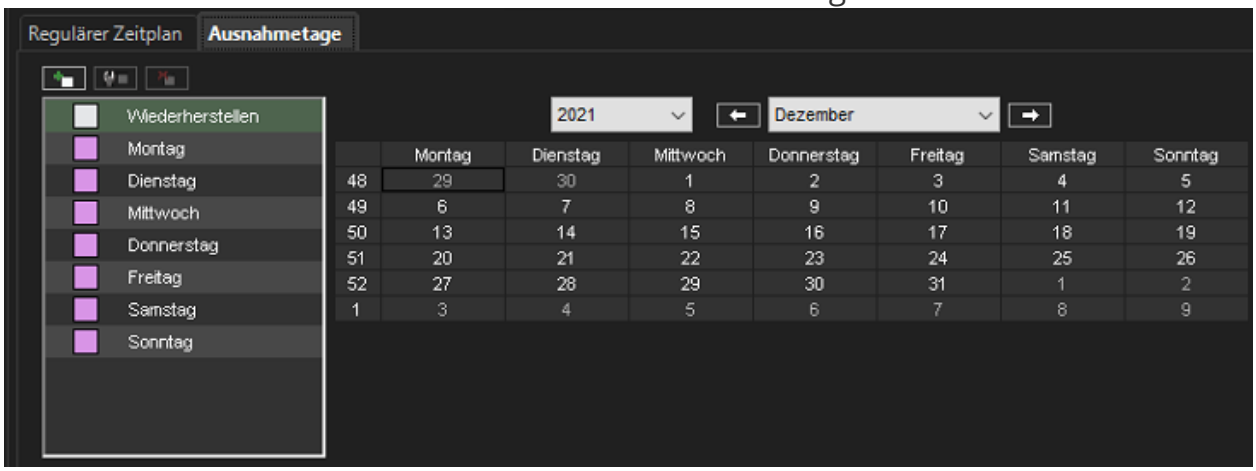
Mit den Einstellungen für Ausnahmetage können Sie Feiertage im Kalender festlegen.

So legen Sie einen Zeitplan für Ausnahmetage fest:

Sie können für Feiertage unterschiedliche Aufzeichnungszeitpläne verwenden.

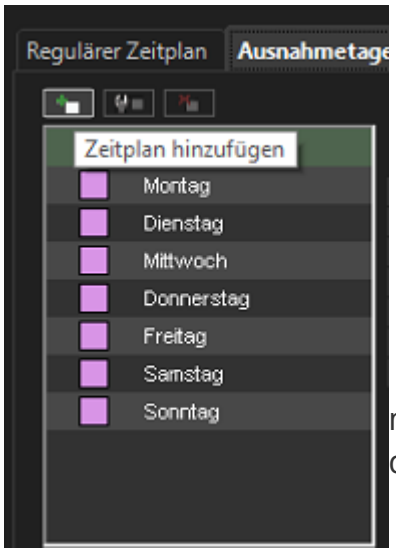
Sie können einen Tagesplan aus dem **regulären Plan** anwenden oder einen **Ausnahmeplan mit Tagen** verwenden.

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.



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**

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**.

So löschen Sie einen benutzerdefinierten Zeitplan:

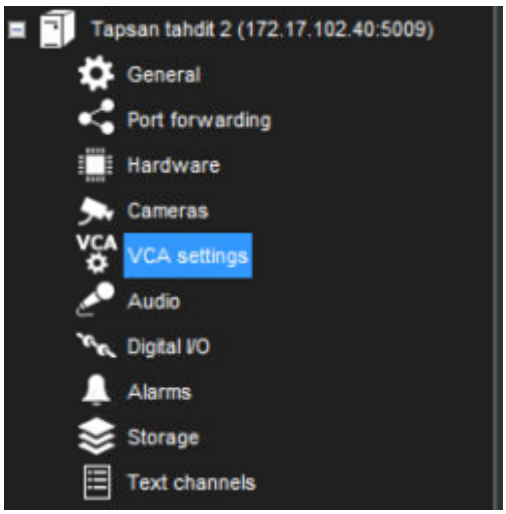
- Wählen Sie den Zeitplan im linken Bereich aus und klicken Sie auf **Zeitplan löschen**.

So stellen Sie den ursprünglichen Zeitplan wieder her:

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

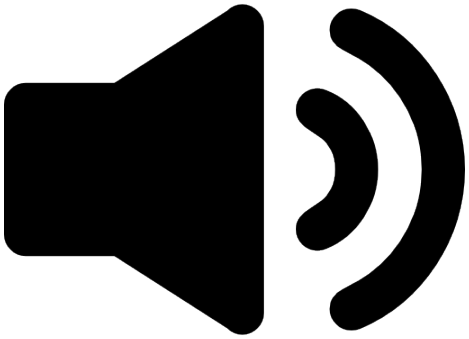
oben Vorherige Nächste

1.9.6. VCA-Einstellungen



oben Vorherige Nächste

1.9.7. Audio

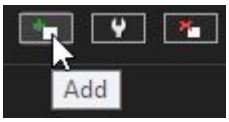


oben Vorherige Nächste

1.9.7.1. 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.

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.
7. Klicken Sie auf **OK**.

Notiz *IP-kamerabasierte IP-Audio-Eingangs- und -Ausgangskanäle werden dem System hauptsächlich über die automatischen Kamerasuchwerkzeuge hinzugefügt.*

Wenn ein IP-Kamera-basierter Audiokanal nicht über die Kamerasuchwerkzeuge hinzugefügt werden kann oder der Kanal verspätet hinzugefügt wird, befolgen Sie die obigen Anweisungen, um den Audiokanal hinzuzufügen.

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. Klicken Sie in der unteren rechten Ecke der Registerkarte auf **Audiokanal bearbeiten**  . Das Dialogfeld **Audio konfigurieren** wird angezeigt.
6. Bearbeiten Sie die Informationsfelder.
7. Klicken Sie auf **OK**.

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.

oben Vorherige Nächste

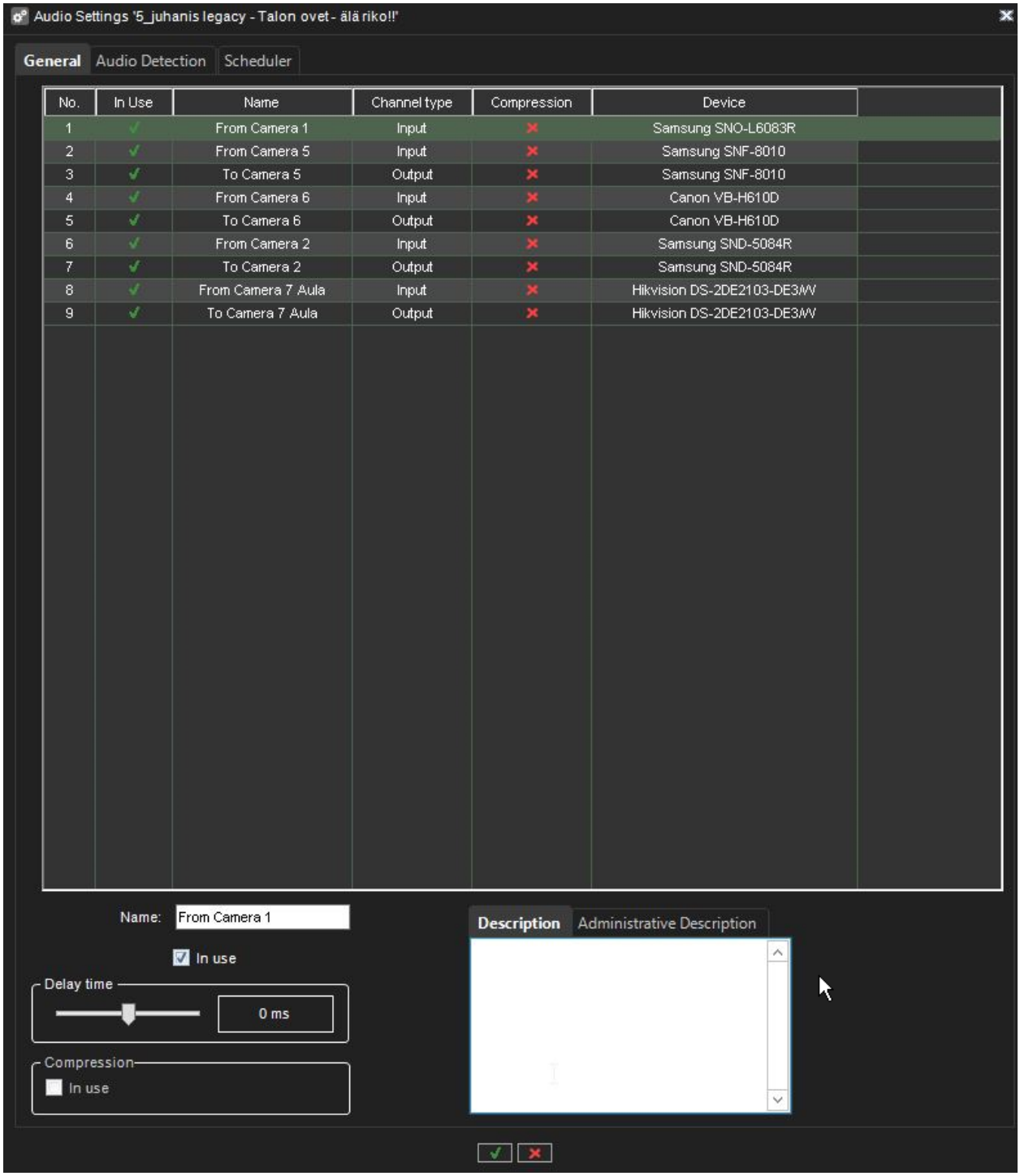
1.9.7.2. Audio Einstellungen

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.

oben Vorherige Nächste

1.9.7.3. Allgemeine Einstellungen



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.

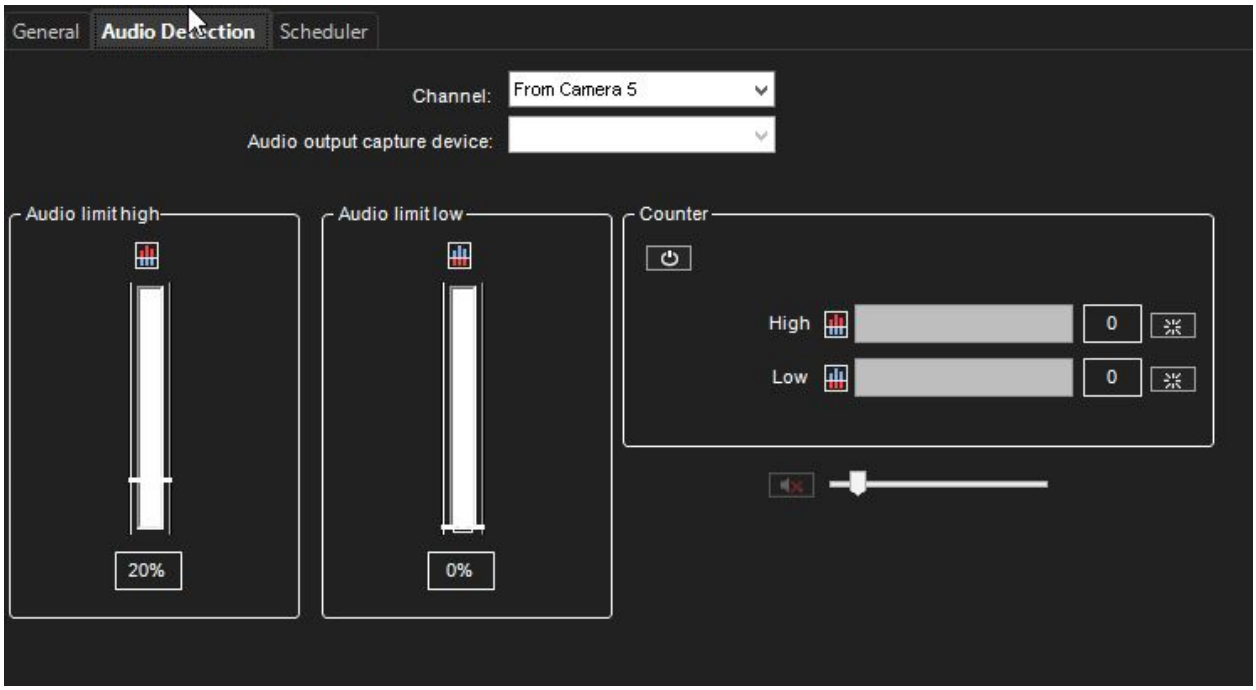
- **Kompression** Zeigt an, ob die Komprimierung ein- oder ausgeschaltet ist. Ein Häkchen bedeutet, dass Komprimierung verwendet wird.
- **Capture-Treiber**. Zeigt an, welcher Capture-Treiber verwendet wird. Wählen Sie den Treiber in **Hardware-Einstellungen**.

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.

oben Vorherige Nächste

1.9.7.4. Audioerkennung



Legen Sie auf der Registerkarte **Audio Detection** auf der Seite **Audio 2**die oberen und unteren Grenzwerte für die Audioerkennung fest.

Das System zeichnet Audio auf, wenn der Audiopegel den oberen Grenzwert überschreitet.

Darüber hinaus können Sie das System so einstellen, dass es einen Alarm ausgibt, wenn der Audiopegel den oberen Grenzwert überschreitet oder unter den unteren Grenzwert fällt.

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.

oben Vorherige Nächste

1.9.7.5. Planer (Audio)

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

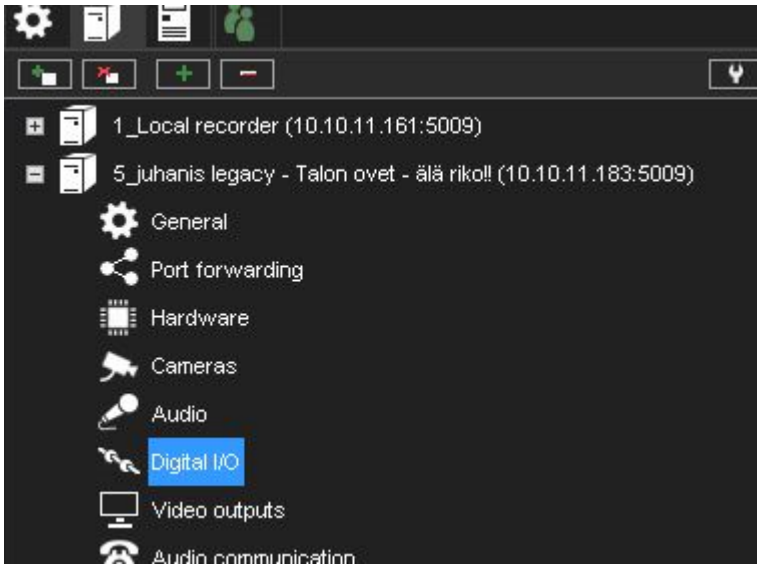
Ähnlich wie beim Videoplaner ist es möglich, die Audioaufzeichnung mit den folgenden Optionen sowohl für reguläre Wochen als auch für Feiertage zu steuern.

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. Set the limit on the Audio Settings

Die Funktionalität dieser Ansicht ähnelt der des Video-Schedulers.

oben Vorherige Nächste

1.9.8. Digitale E/A



oben Vorherige Nächste

1.9.8.1. Digitale E/A-Einstellungen

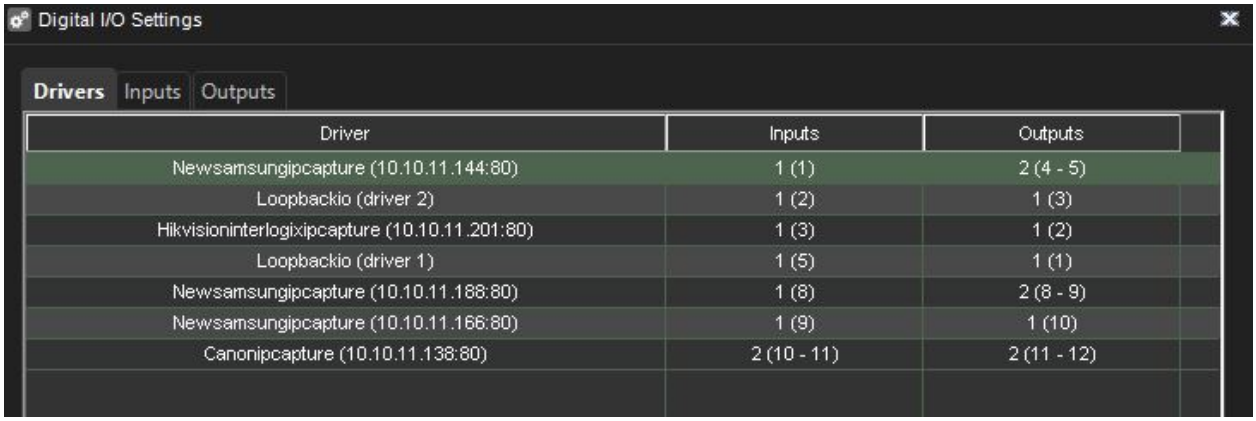
In den Einstellungen **Digital I/O** können Sie digitale Eingabe- und Ausgabegeräte hinzufügen und die Eingabe- und Ausgabeeinstellungen konfigurieren.

In diesen Abschnitten wird beschrieben, wie Sie digitale E/A-Geräte einrichten.

Treiber

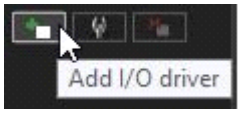
Zusätzlich zu den im System enthaltenen standardmäßigen digitalen E/A-Treibern können dem System neue Treiber hinzugefügt werden, indem sie als Plugins installiert werden.

Nachdem dem System ein E/A-Gerätetreiber hinzugefügt wurde, kann das Gerät über die Registerkarte **Treiber** konfiguriert und verwendet werden.



So verwenden Sie einen E/A-Gerätetreiber:

1. Installieren Sie bei Bedarf das Gerätetreiberpaket.
2. Öffnen Sie die **VMS-Server** tab.



4. Wählen Sie den richtigen Server aus und öffnen Sie die Seite **Digital I/O** aus dem Menü.
3. Klicken Sie in der unteren rechten Ecke des Bildschirms auf **E/A-Treiber hinzufügen**.
4. Wählen Sie den Treiber aus dem Dropdown-Menü **Model** aus.
5. Konfigurieren Sie die Geräteeinstellungen in der Liste **Eigenschaften**.
6. 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**.

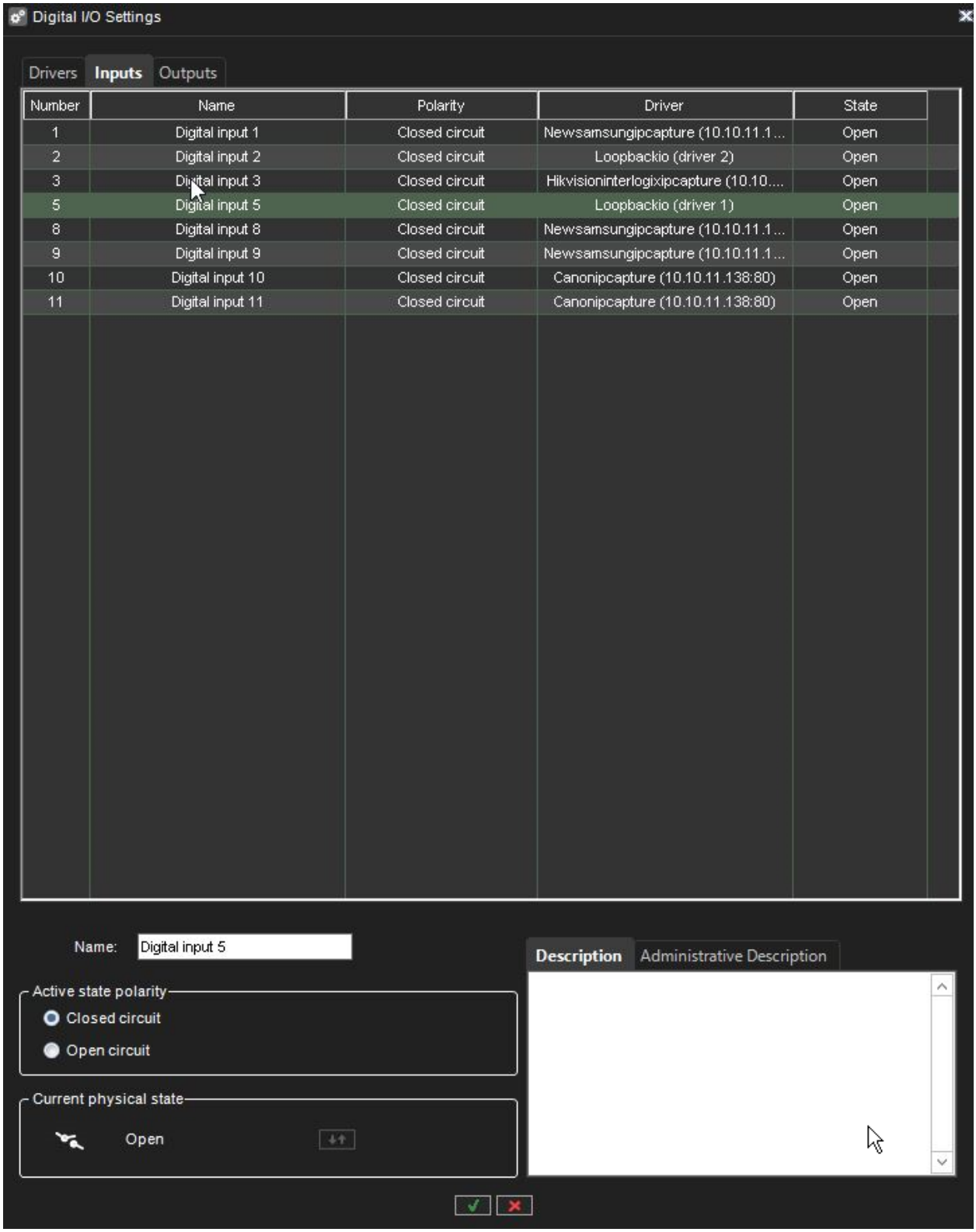
So löschen Sie einen E/A-Gerätetreiber:

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.

Digitale Eingänge

Sie können digitale Eingänge verwenden, um Alarme zu aktivieren.

Stellen Sie in den Digitaleingangseinstellungen die Polarität der Eingänge ein. Legen Sie die Alarmaktionen in den Alarmeinstellungen fest.



Name Um einen Eingang umzubenennen, wählen Sie den Eingang aus und geben dann einen neuen Namen für den Eingang in **Name ein.**

Aktive Statuspolarität. Wählen Sie den Eingang und wählen Sie 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.

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 dann einen neuen Namen für den Ausgang in **Name** ein.

Aktive Statuspolarität. Wählen Sie den Ausgang aus und wählen Sie dann aus, ob der Ausgang geschlossen oder geöffnet ist, wenn er aktiviert ist.

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.

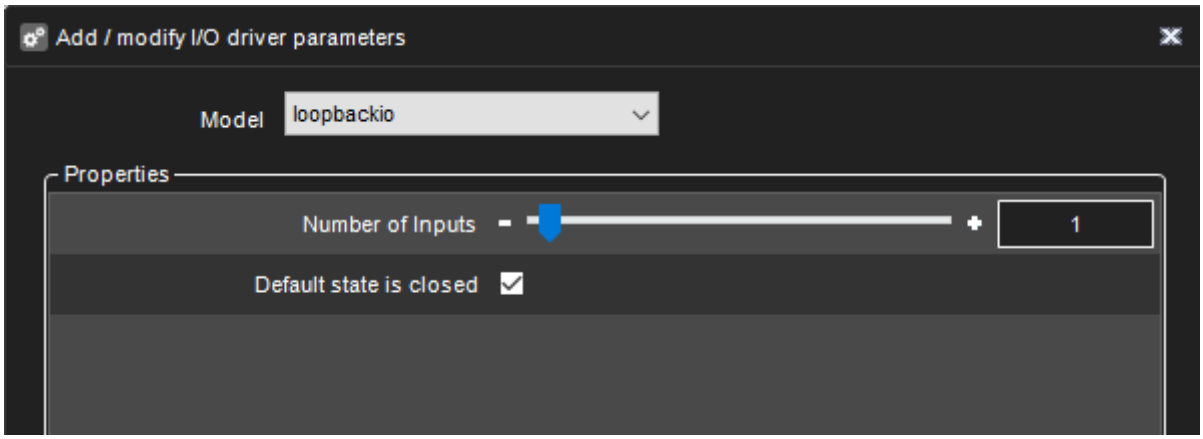
Um einen Digitalausgang zu testen, klicken Sie auf die Schaltfläche **Change State (Toggle)**.

oben Vorherige Nächste

1.9.8.2. 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.



oben Vorherige Nächste

1.9.8.3. 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.

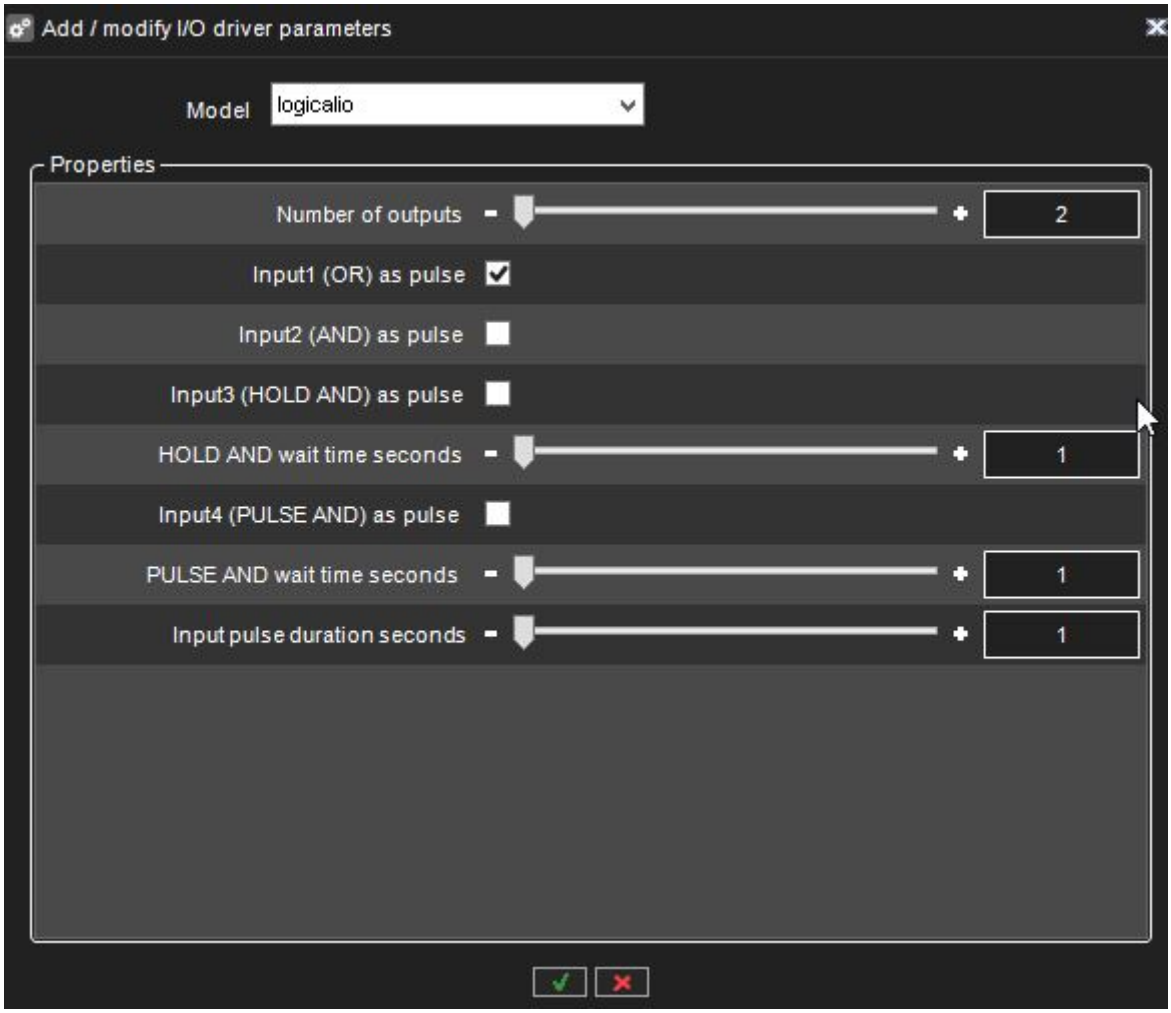
Ein anderes Beispiel könnte sein, dass ein Eingangs-„Tor“ mit zwei Türen das Öffnen der zweiten Tür nur zulässt, wenn die erste geschlossen ist.

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.

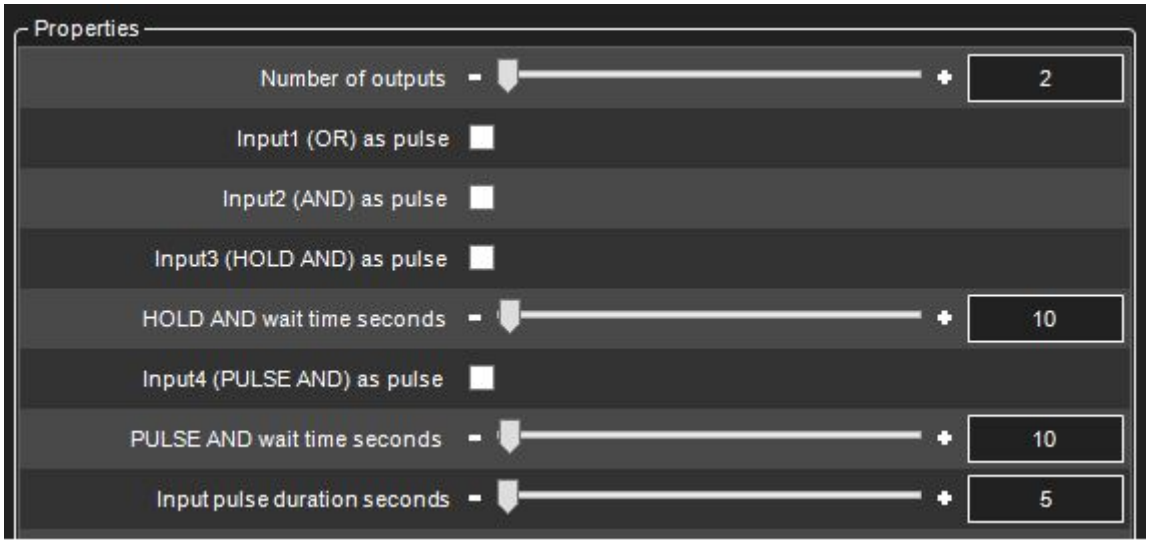
Die Mindestanzahl beträgt zwei, die Höchstzahl 32.



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:

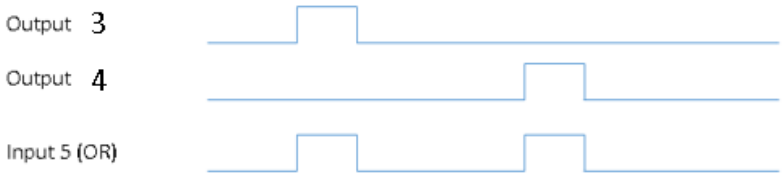


Das Beispiel hat 2 Ausgänge, die die Operanden sind. Diese sind in der IO-Liste als Ausgänge 3 und 4 zu sehen.

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

„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.

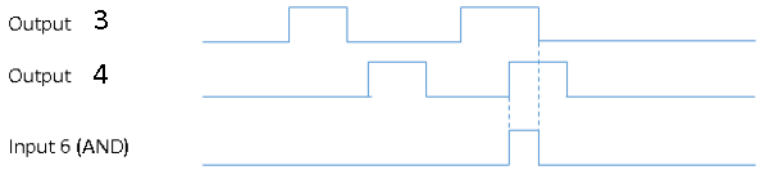


In unserem Beispiel ist Eingang 5 das ODER-Signal. Wenn entweder Ausgang 3 ODER Ausgang 4 eingeschaltet ist, wird als Ergebnis Eingang 5 eingeschaltet.

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

„UND“-Eingang

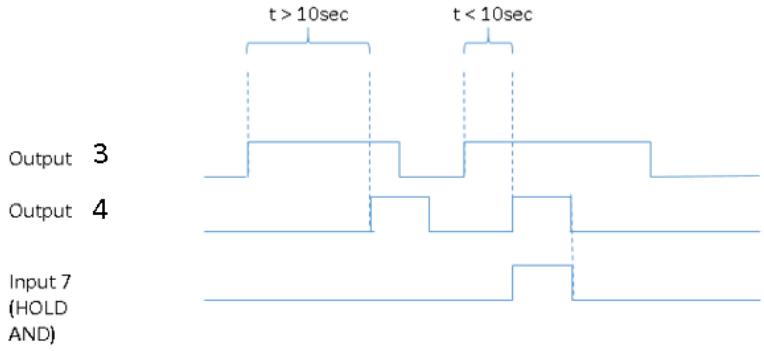
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.



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

"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.



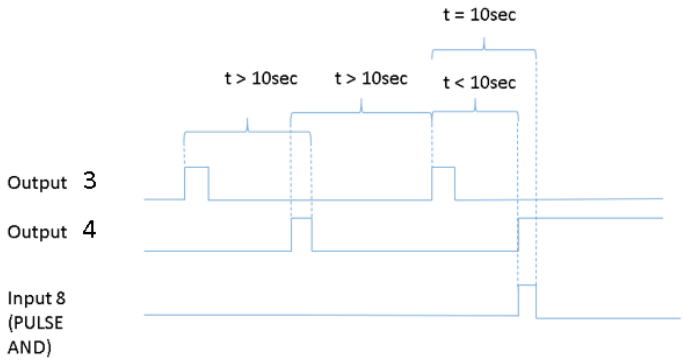
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

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

"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.

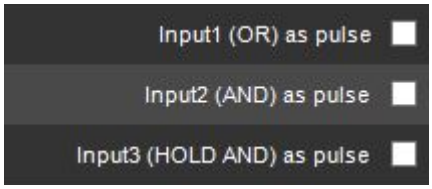


Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

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

Pulse Mode For Inputs

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



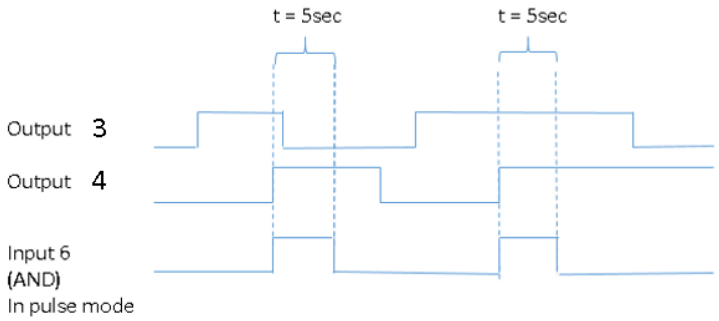
and

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:



oben Vorherige Nächste

1.9.8.4. 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.

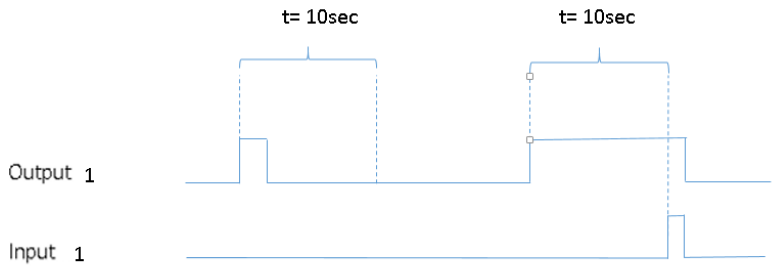
Eine Lizenz steuert logische E/A und Countdown-E/A. Wenn die Lizenz nicht vorhanden ist, schlägt das Erstellen neuer E/A fehl.

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.



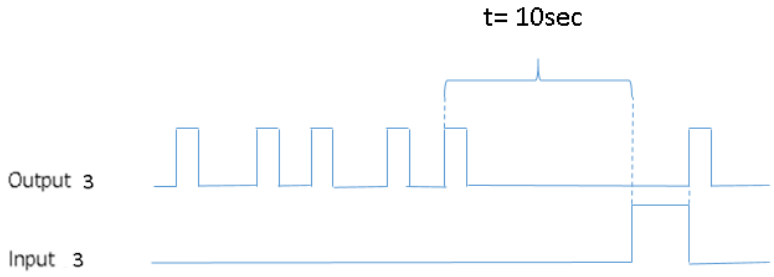
Beim Erstellen eines neuen Countdown-E/A sind die ersten beiden Eingangs-Ausgangspaare von diesem Typ.

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.

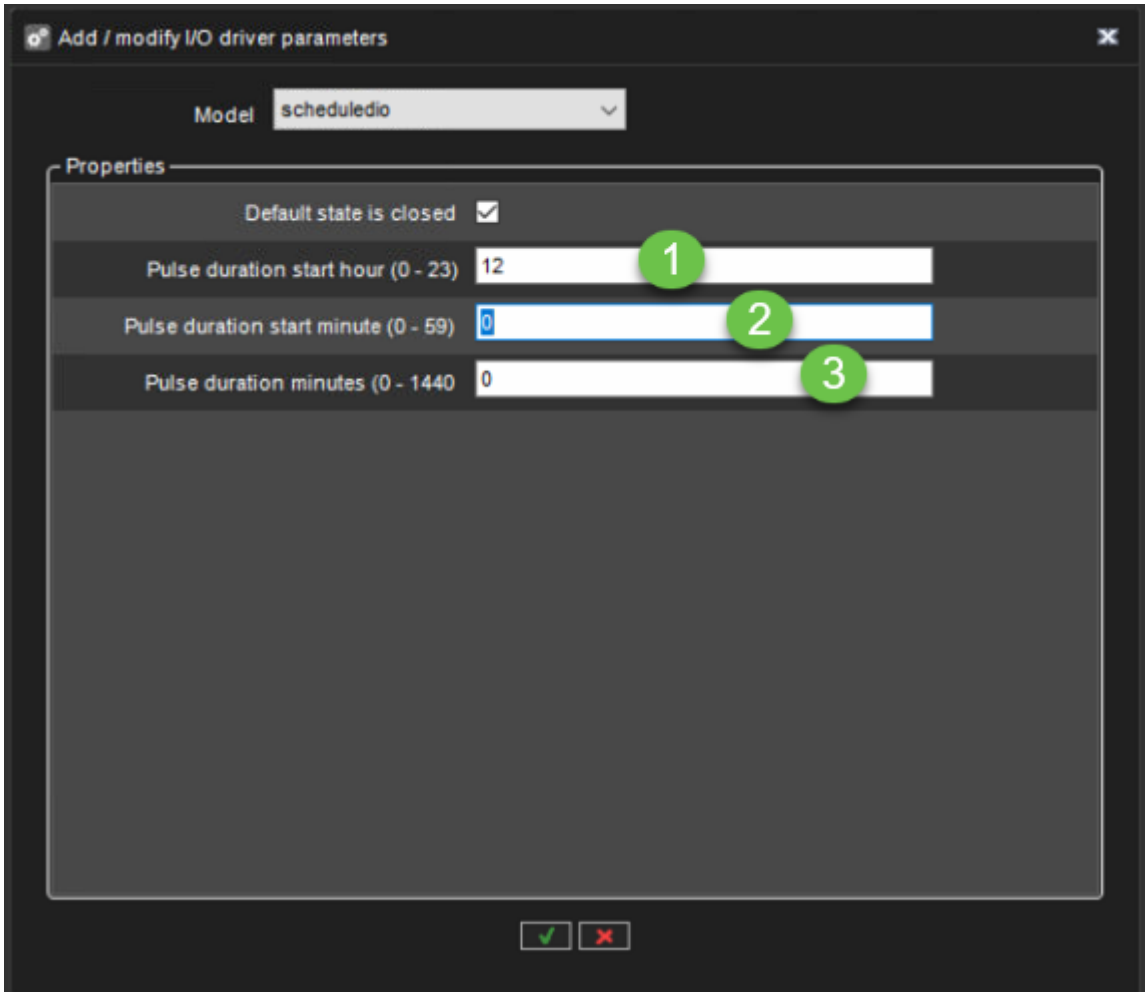
oben Vorherige Nächste

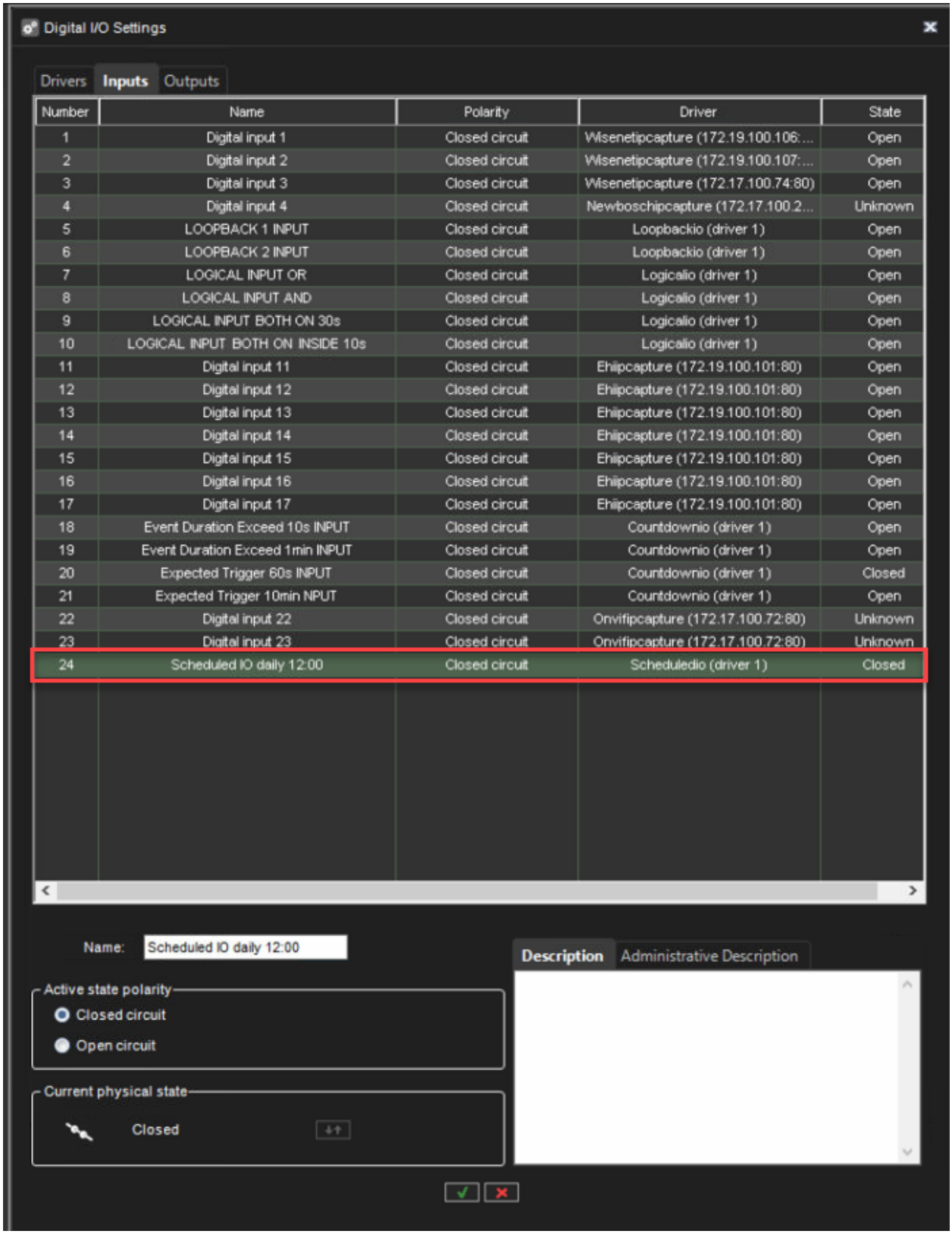
1.9.8.5. Geplante E/A

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

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





oben Vorherige Nächste

1.9.8.6. HTTP-E/A

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)

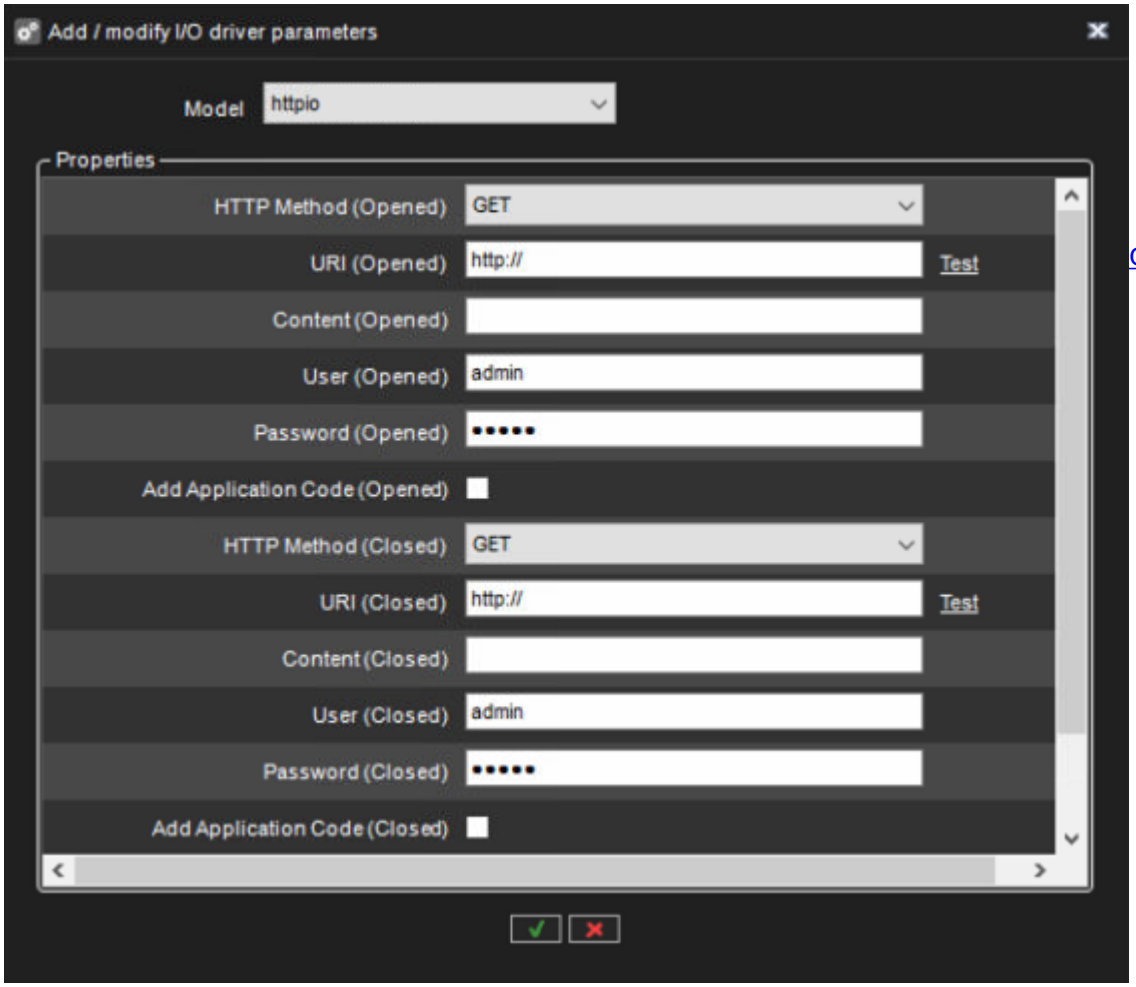
Content(Closed)

User(Closed)

Password(Closed)

Authentication

- BASIC
- DIGEST



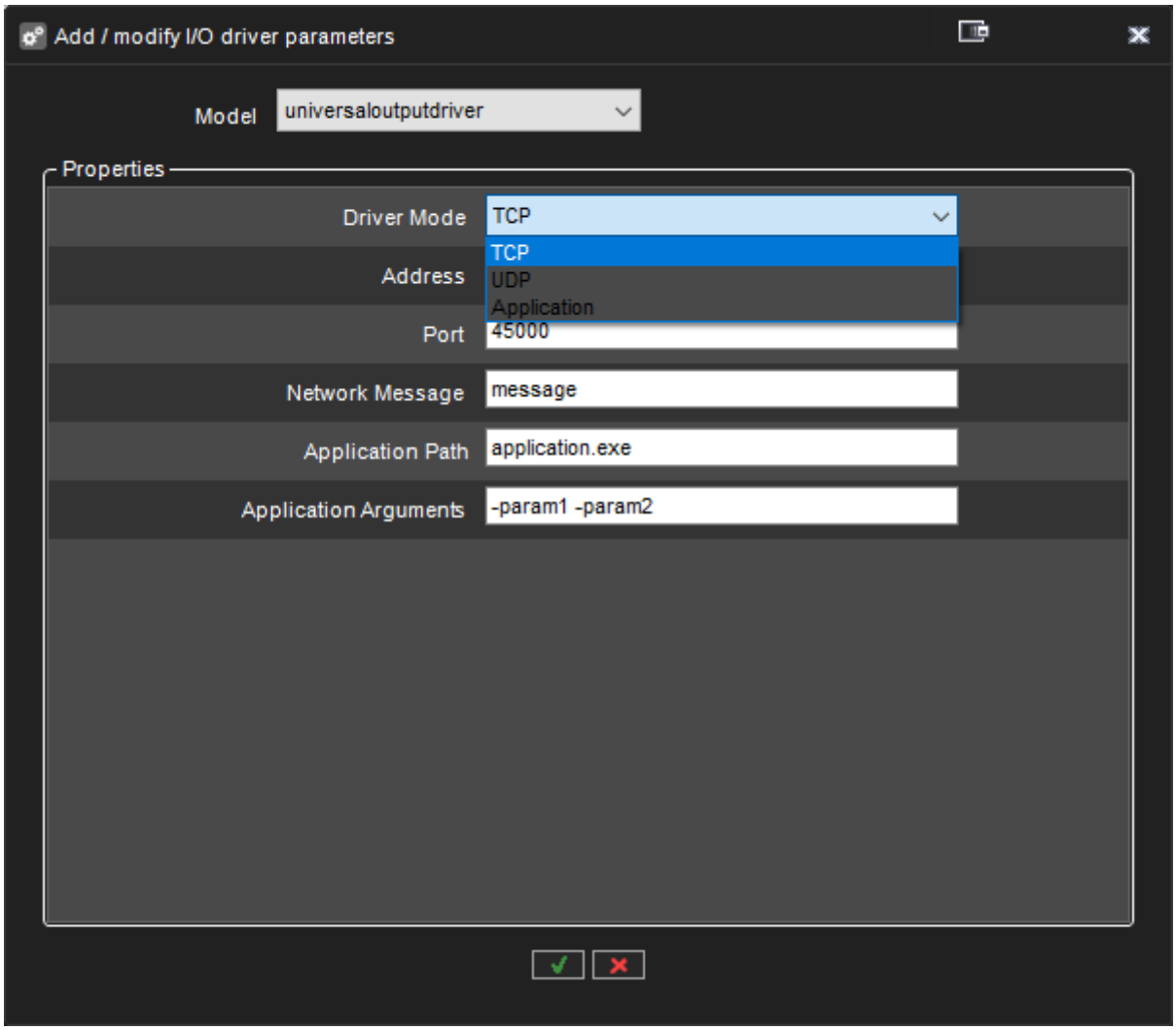
oben

Vorherige Nächste

1.9.8.7. UniversalOutputDriver

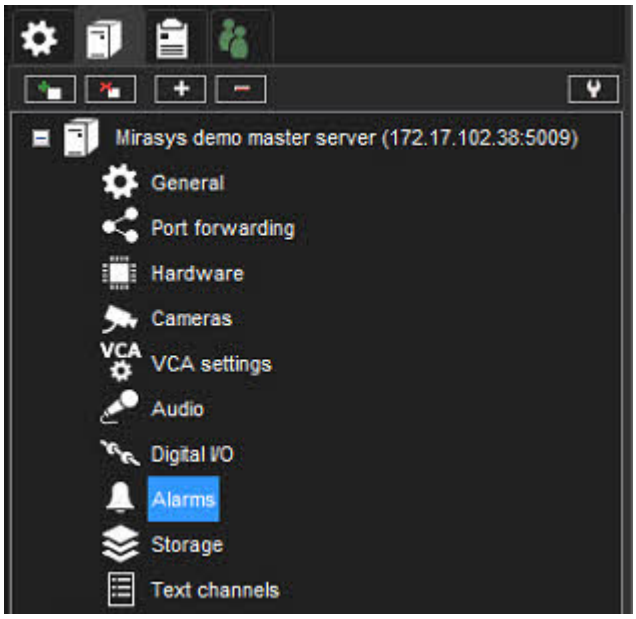
Mit diesem Treiber können Sie Daten an Drittsysteme senden oder Anwendungen auf dem Server oder entfernten Systemen starten.

Weitere Informationen zu diesem Treiber finden Sie in unserem Extranet oder wenden Sie sich an den Support.



oben Vorherige Nächste

1.9.9. Alarm



Alarmeinstellungen

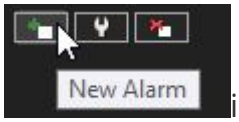
Die Alarmmanagement-Tools ermöglichen die Erstellung serverspezifischer Alarme basierend auf verschiedenen Auslösern basierend auf Bewegung, Schallpegel oder bestimmten Textdatenauslösern.

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.

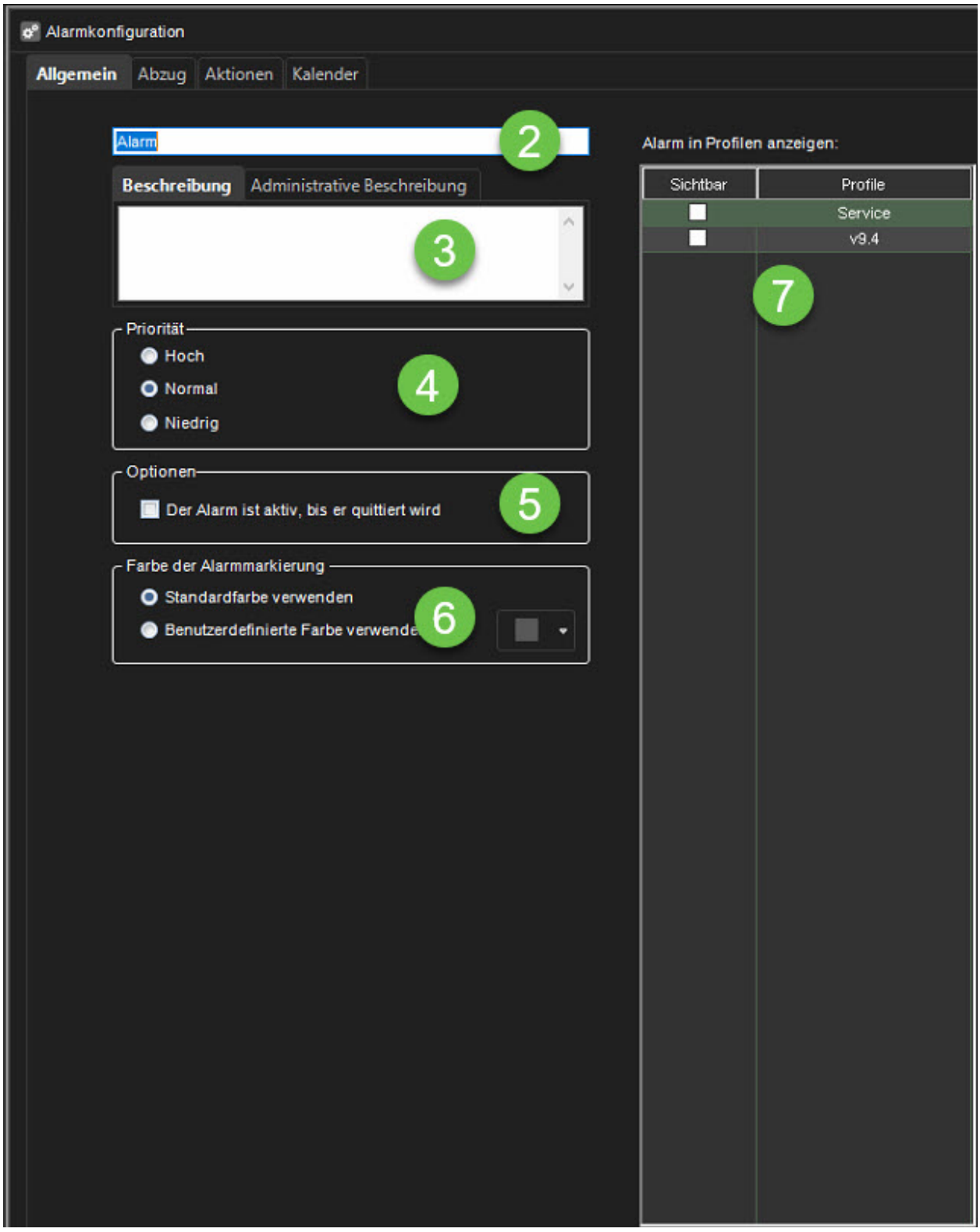
Hinzufügen eines neuen Weckers

Allgemein

1. Klicken Sie auf **Neuer Alarm** 

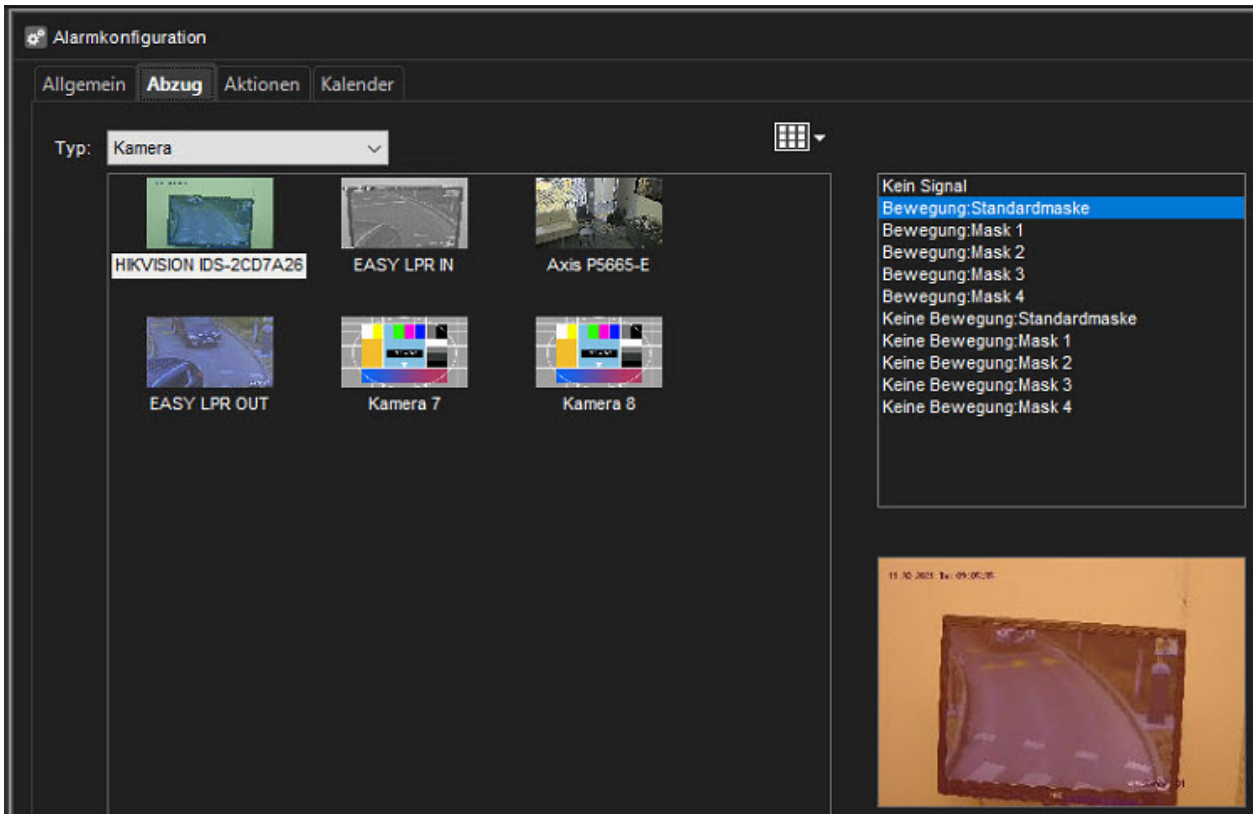
in der linken unteren Ecke des Bildschirms **Alarme**.
2. Geben Sie den Namen des neuen Alarms in das Feld **Name** ein.
3. Geben Sie die **Beschreibung** und **Verwaltungsbeschreibung** des neuen Alarms in die entsprechenden Felder unter dem Feld **Name** ein.

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.*



Absuz

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

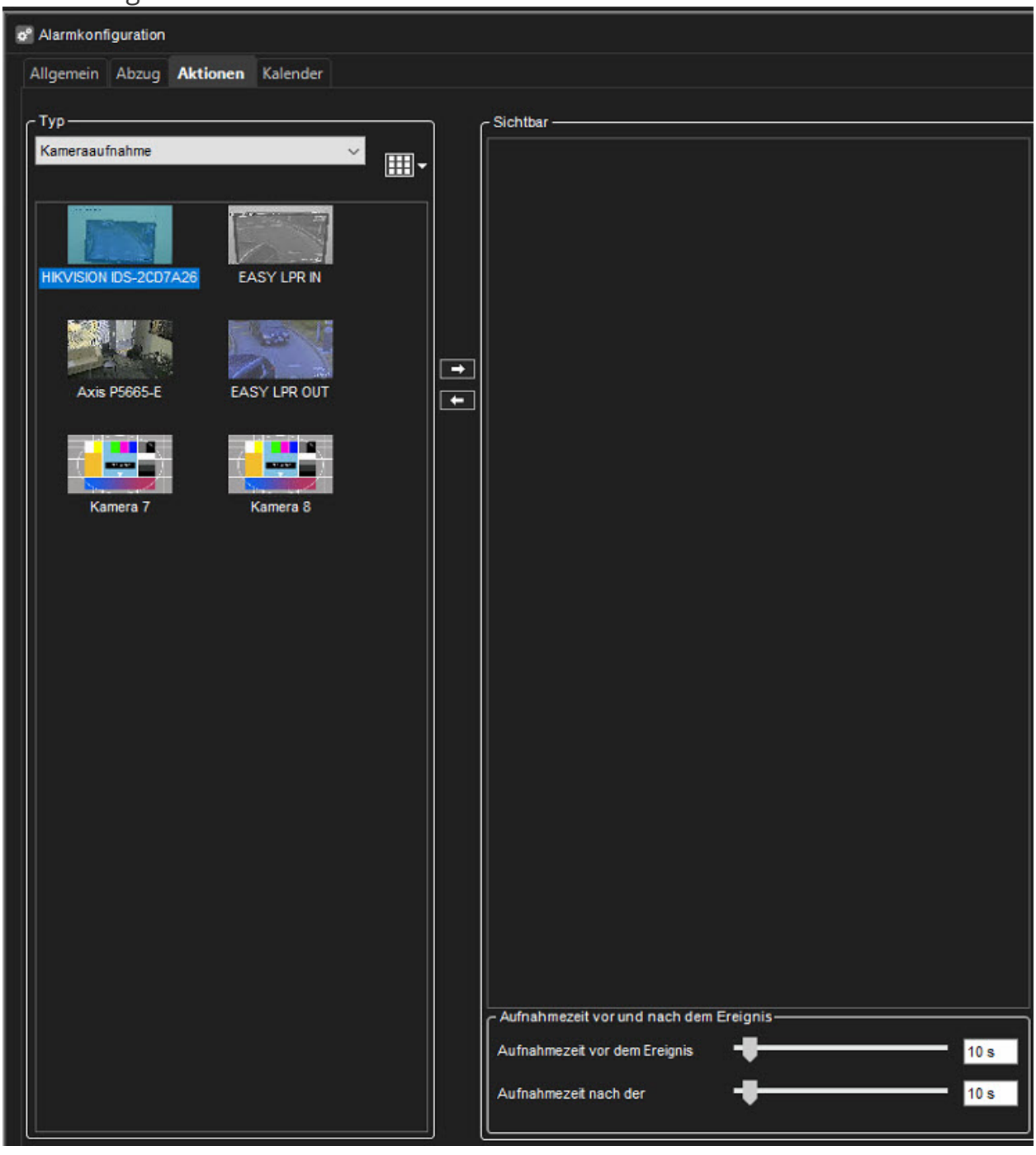


9. Wählen Sie den Triggertyp aus dem Dropdown-Menü **Type** aus.
    i. Kamera
    j. Audio
    k. Metadaten
    l. Textdaten
    m. Digitale Eingabe
10. Wählen Sie das Gerät, das den Alarm auslösen soll, aus der Geräteliste unter dem Dropdown-Menü **Typ** aus.
11. Wählen Sie die auslösende Bedingung aus der Bedingungsliste auf der rechten Seite des Bildschirms aus.
    i. Bei kamerabasierten Auslösern können Sie die Maske auswählen, die bei der Bewegungserkennung verwendet wird, um den Alarm auszulösen.
    j. Bei audiobasierten Auslösern können Sie den Alarm so einstellen, dass er basierend auf einem hohen oder niedrigen Audiopegel ausgelöst wird.
    k. 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.

l. Bei digitaleingangsbasierten Triggern wird der Alarm basierend auf der Polaritätsänderung des Eingangs ausgelöst.

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.



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

Aktionstypen und Einstellungen

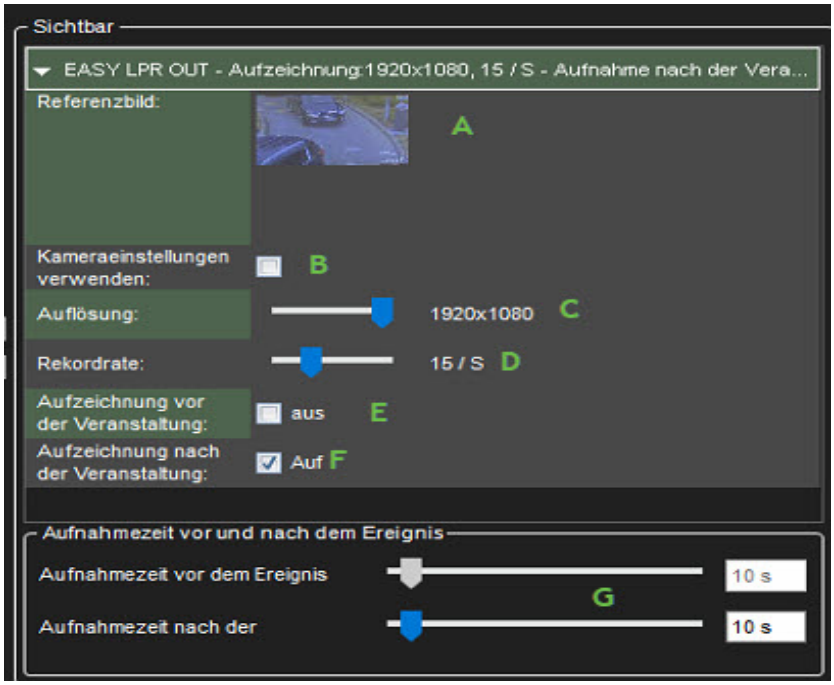
Die folgende Liste enthält die Standardaktionstypen und ihre Parameter. Einige der oben aufgeführten Aktionstypen sind möglicherweise nicht auf allen Systemen verfügbar.

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

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.

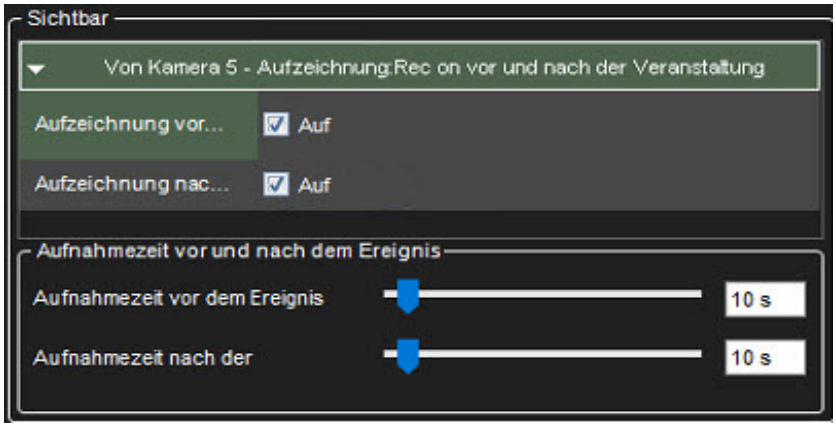
G)Aufnahmezeit vor und nach dem Ereignis Diese Schieberegler können verwendet werden, um die Aufzeichnungsdauer vor und nach dem Ereignis für die Aktion einzustellen. Die Schieberegler sind nur aktiv, wenn die Aufzeichnung vor und/oder nach dem Ereignis aktiviert wurde.

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.*

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.*

Digitaler Ausgang

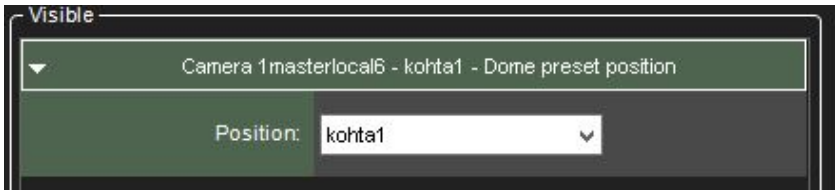
Der **digitale Ausgang** ist die Standardaktion für digitale E/A-Geräte. Wenn ein Alarm ausgelöst wird, der diesen Aktionstyp enthält, wird das E/A-Gerät aktiviert.

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.*

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:

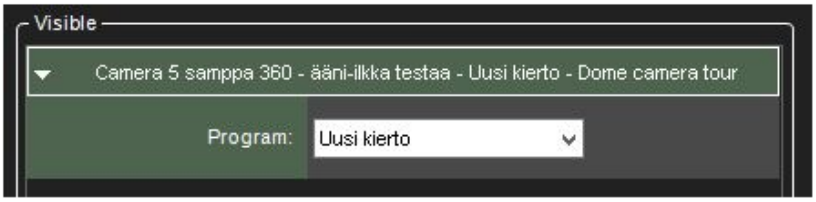
- **Position** Verwenden Sie das Dropdown-Menü, um die voreingestellte Position auszuwählen, in die sich die PTZ-Kamera während des Alarms bewegt.

***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.*

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.



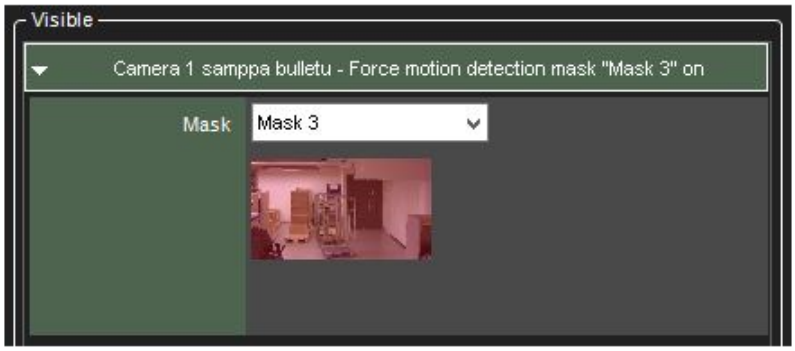
Die Aktion umfasst die folgenden Felder und Parameter:

- **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.*

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.*

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.

Alarme deaktivieren

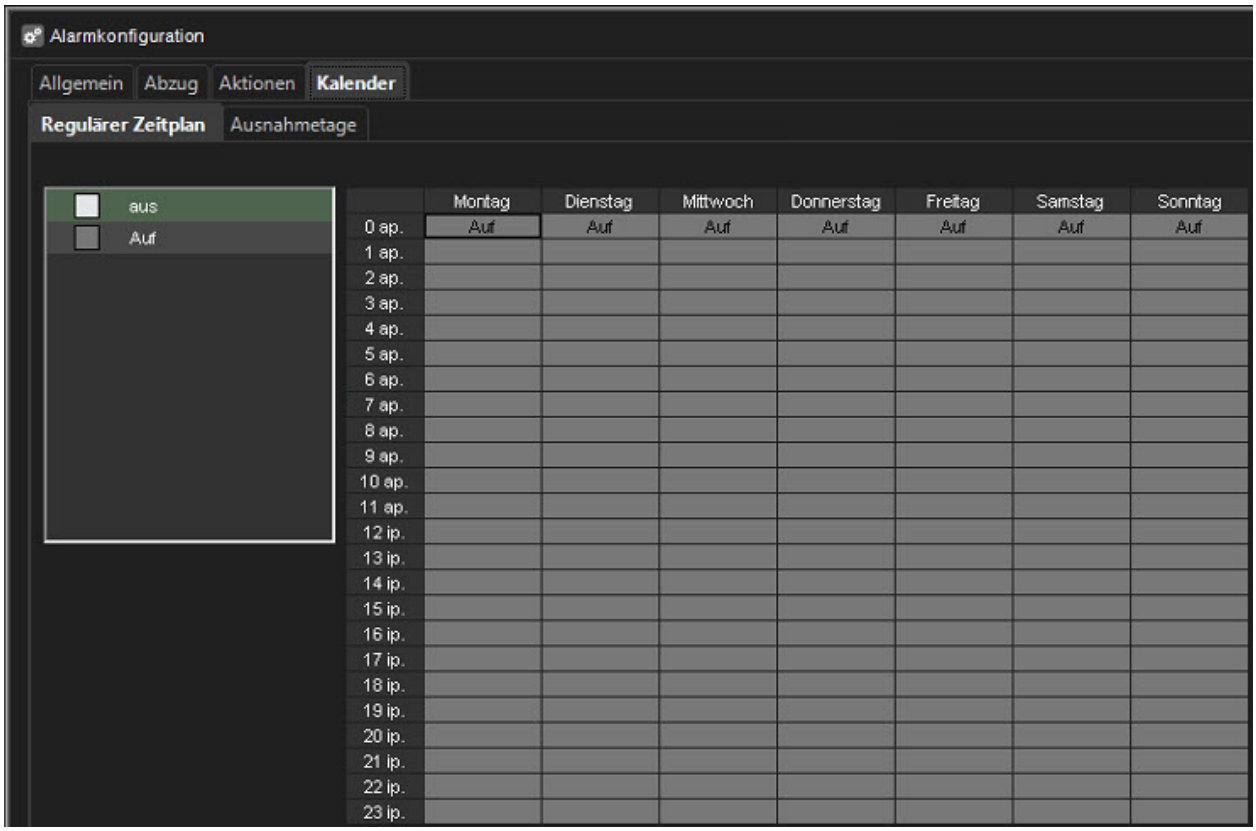
Die Aktion **Alarme deaktivieren** kann verwendet werden, um Deaktivierungsalarme basierend auf einem Alarm zu senden. Die Konfiguration kann so erfolgen, dass alle Alarme deaktiviert sind, Alarme mit niedriger und mittlerer Priorität oder Alarme mit niedriger Priorität.

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.

Kalender

14. Definieren Sie das, wenn der Alarm aktiv ist
15. Klicken **OK**



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.

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.

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.

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.

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**  .

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.

Löschen eines Alarms

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.

oben Vorherige Nächste

1.9.10. 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.

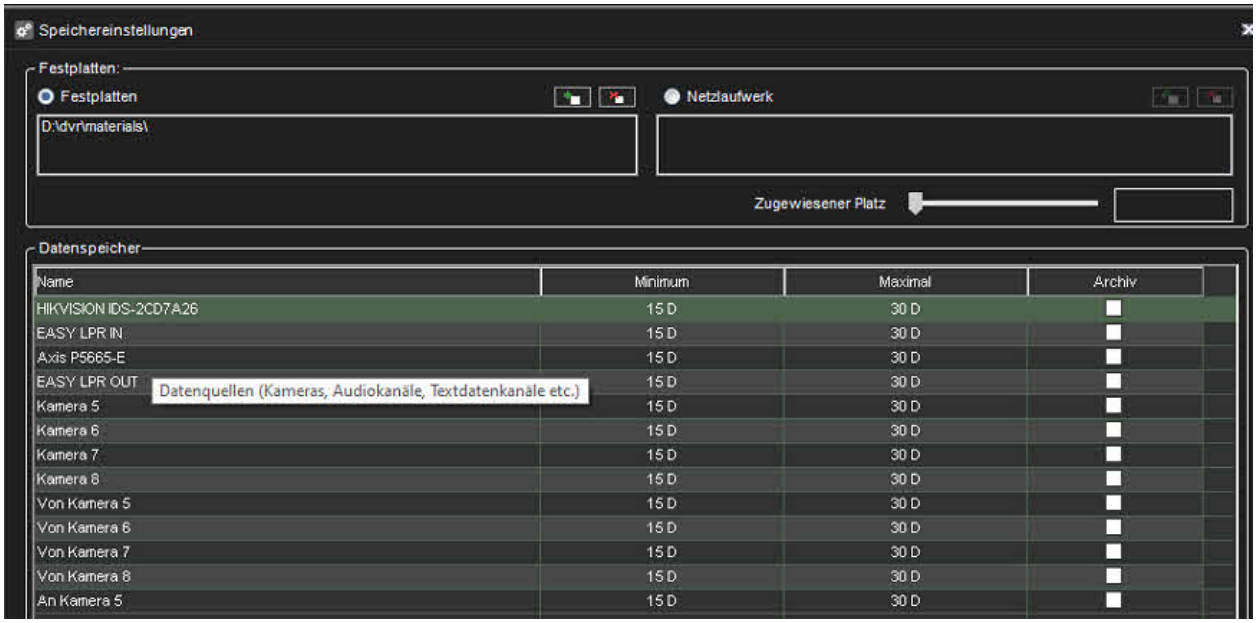
Die Speichereinstellungen werden auch verwendet, um die automatische Archivierungsfunktion zu konfigurieren, die es ermöglicht, täglich oder wöchentlich Sicherungskopien der serverspezifischen Video-, Audio- und Textdaten zu erstellen.

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

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.

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.
    a. 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**.

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.

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.

Speichereinstellungen für Video-, Audio- und Textdaten

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.

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.*

Alarmgrenzen

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.

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.

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.

% 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.

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.*

Archivierung

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

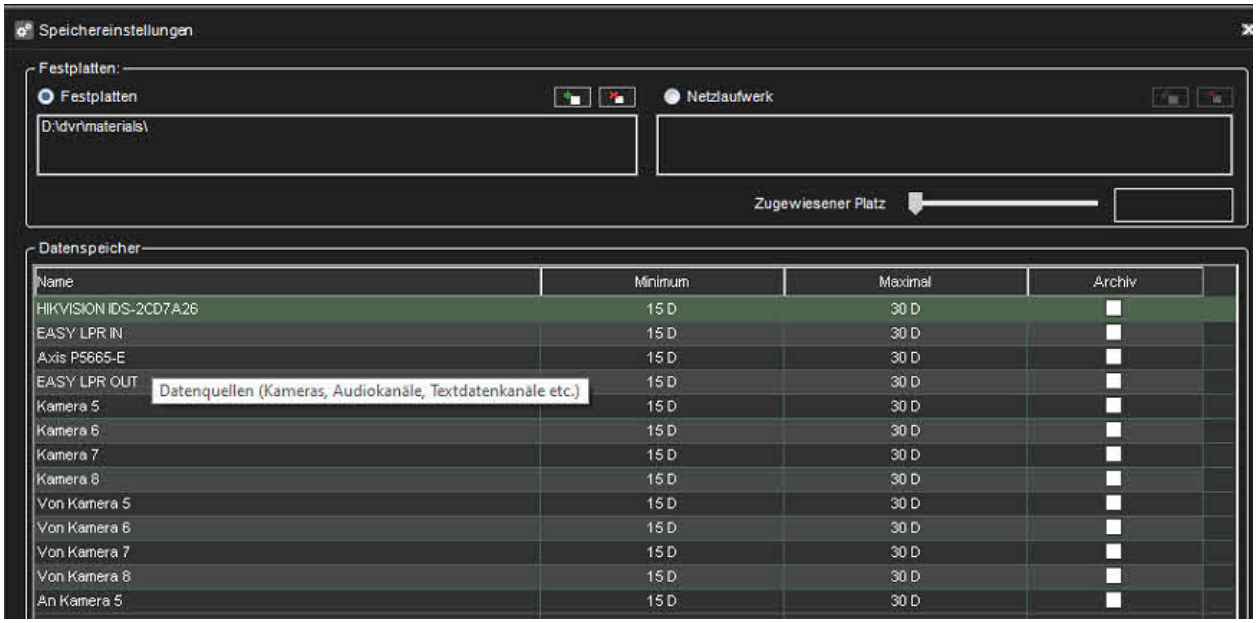
Die Archivdateien können automatisch auf den Festplatten des Servers oder einem Netzlaufwerk erstellt werden.

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.*

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**.

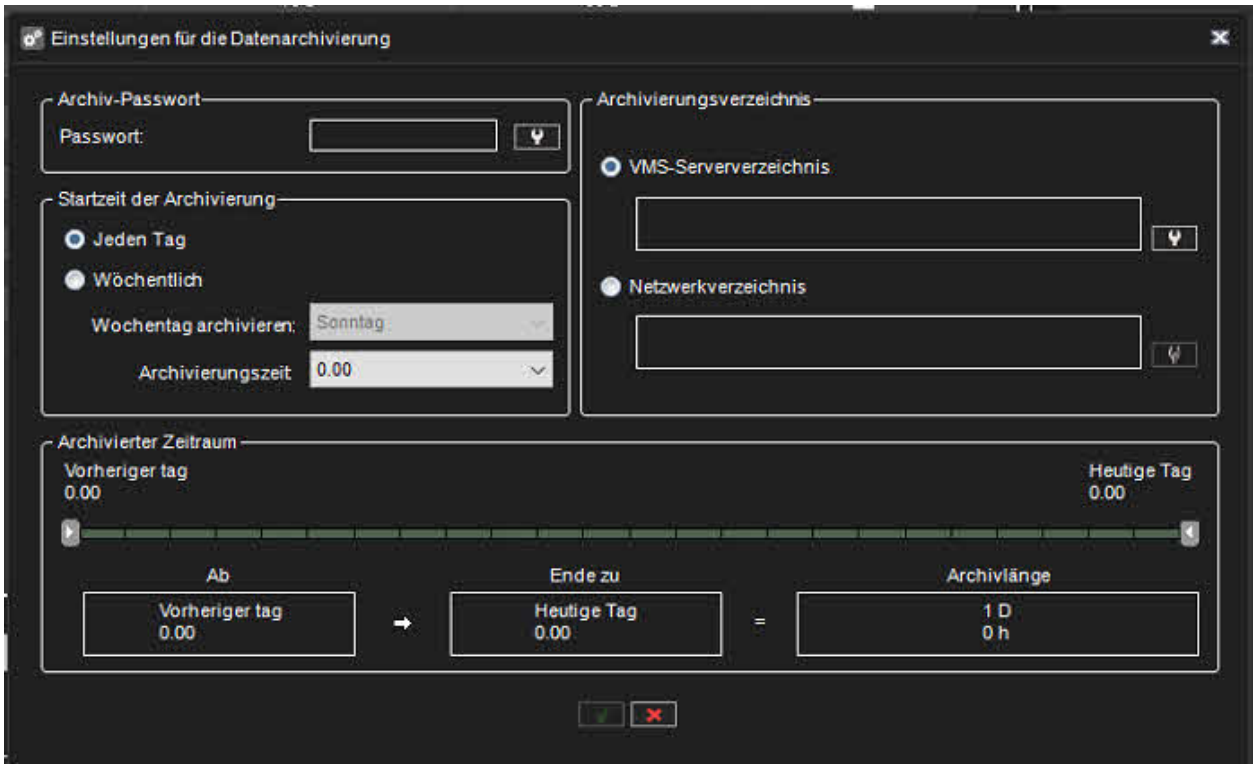


3. Klicken Sie auf **Archiveinstellungen ändern**

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

MIRASYS
DEEP VISION DATA COMPANY

Administrator Guide V9 - DE



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.

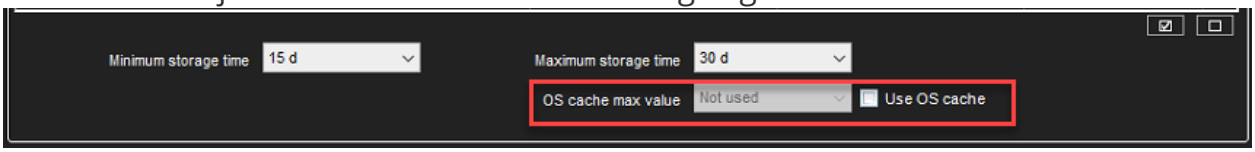
Der letzte hilft, mit instabiler Last auf der Festplatte umzugehen und die am häufigsten verwendeten Teile der Daten zwischenzuspeichern.

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.



oben Vorherige Nächste

1.9.11. Textkanäle

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.

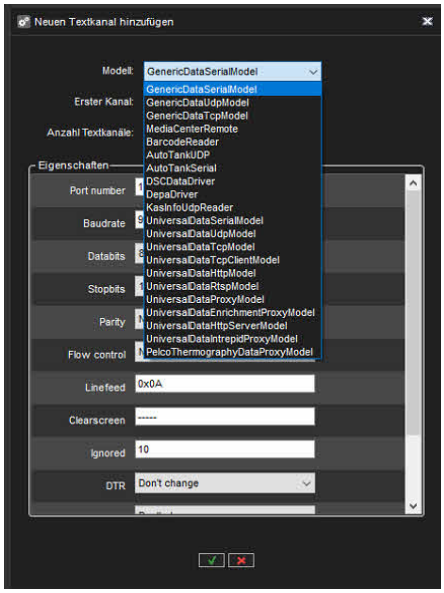
In-Text-Kanaleinstellungen können Sie den Namen eines Textkanals ändern und seine Beschreibung hinzufügen oder bearbeiten.

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.

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.

So bearbeiten Sie Textkanäle:

1. So bearbeiten Sie den Namen und die Beschreibung eines Textdatenkanals:
1. Wählen Sie einen Textdatenkanal aus der Kanalliste aus.
2. Geben Sie einen Namen für den Kanal in das Feld Name ein.
3. Geben Sie eine allgemeine Beschreibung und eine administrative Beschreibung des Kanals in die entsprechenden Felder ein.
    a. Alle Benutzer können die allgemeine Beschreibung sehen, während nur Systemadministratoren die administrative Beschreibung sehen können.
4. 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:
1. Wählen Sie einen Textdatenkanal aus der Kanalliste aus.
2. Click **Modify channels**  .
3. Bearbeiten Sie die treiberspezifischen Informationen in den Feldern in der Liste **Eigenschaften**.
4. 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.*

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.*

oben Vorherige Nächste

1.10. 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.

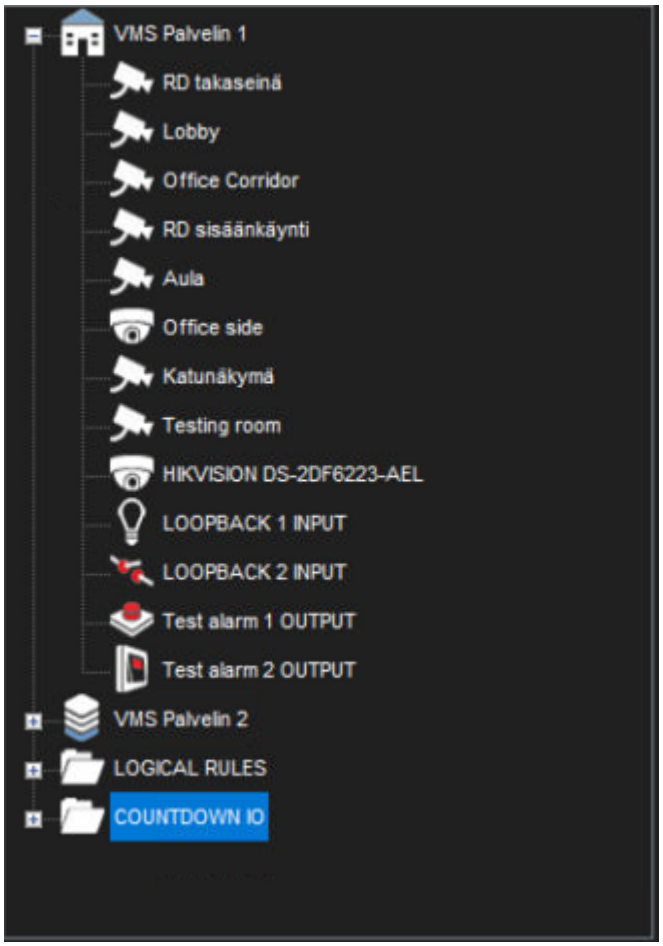
Sie können das Standardprofil als solches verwenden oder frei bearbeiten, zum Beispiel Kameras am genauen Standort gruppieren.

Oder Sie können neue Profile hinzufügen. Ein Profil kann Geräte von verschiedenen Servern enthalten.

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

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

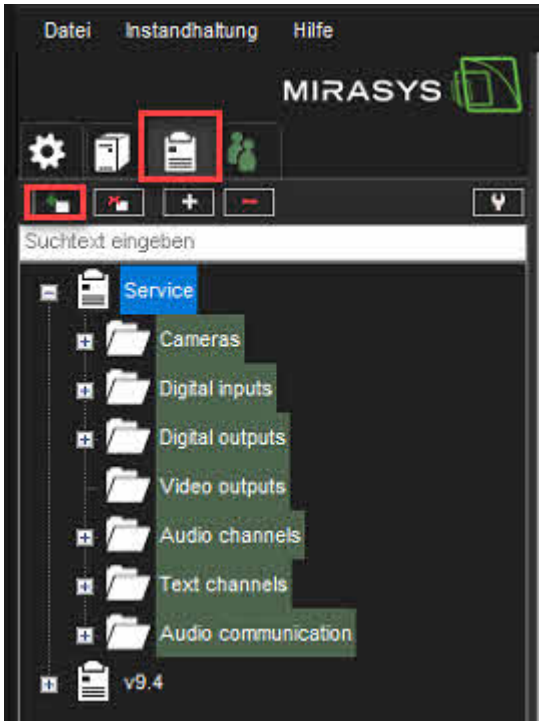


oben Vorherige Nächste

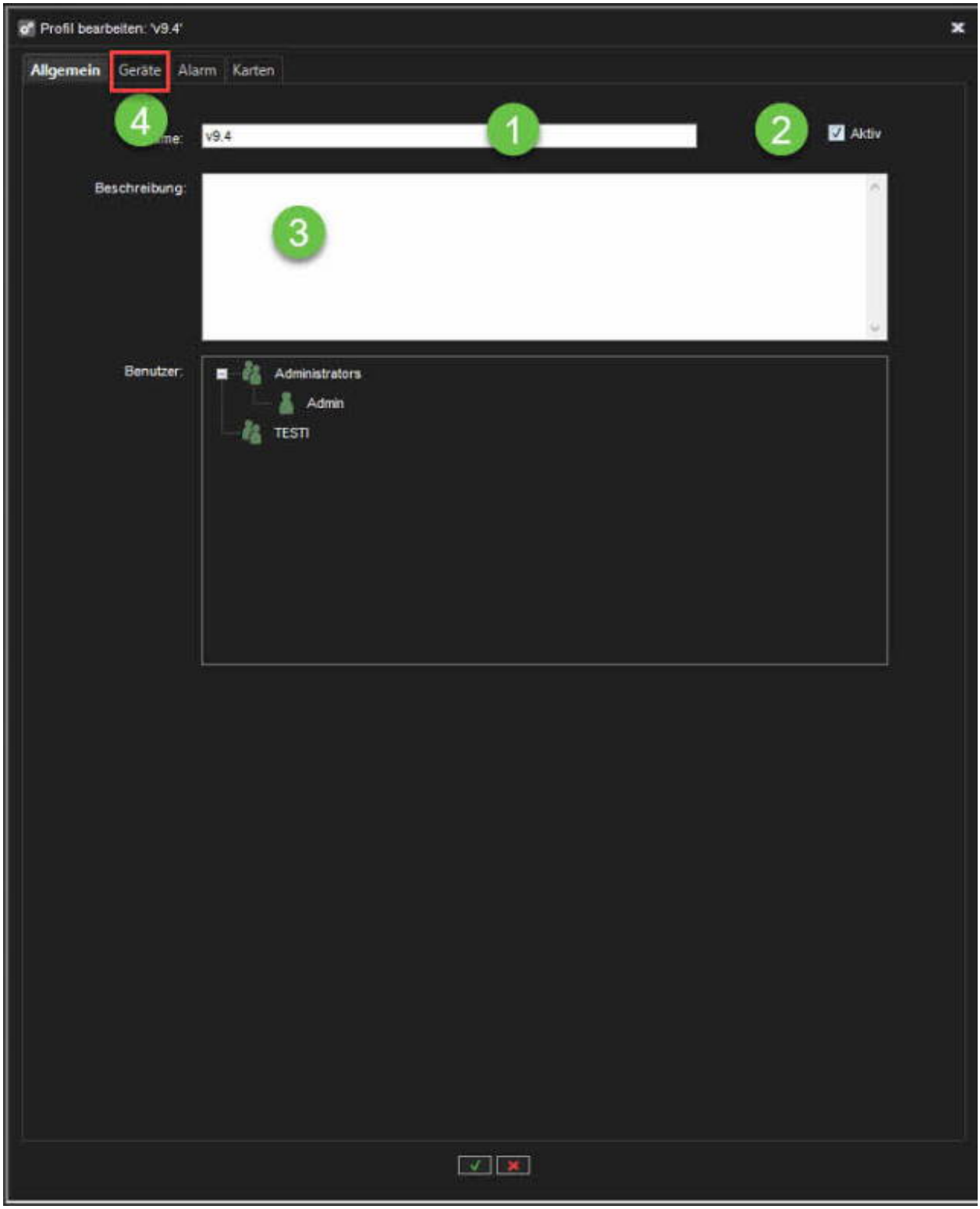
1.10.1. Erstellen eines kundenspezifischen Profils

So fügen Sie ein Profil hinzu:

1. Klicken Sie auf **Profil hinzufügen**



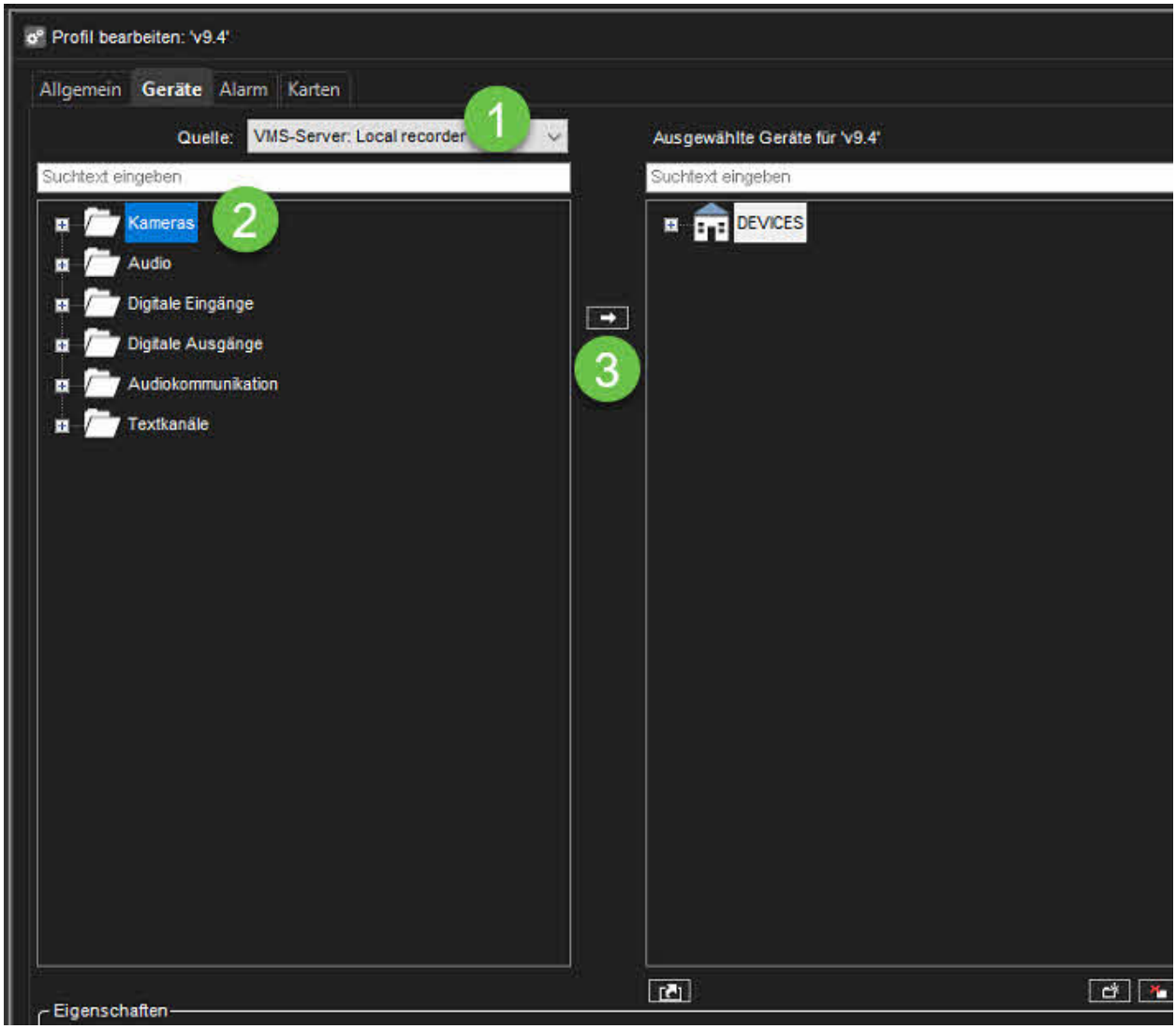
1. Legen Sie den Namen des Profils fest
2. Profilstatus setzen: **Aktiv** oder **Deaktiviert**
3. Legen Sie die Beschreibung fest, falls erforderlich. Die Beschreibung wird nur im System Manager angezeigt
4. Öffnen Sie **Geräte**



Geräte

1. Wählen Sie aus der Dropdown-Liste Quelle **VMS-Server oder ein anderes Profil** aus

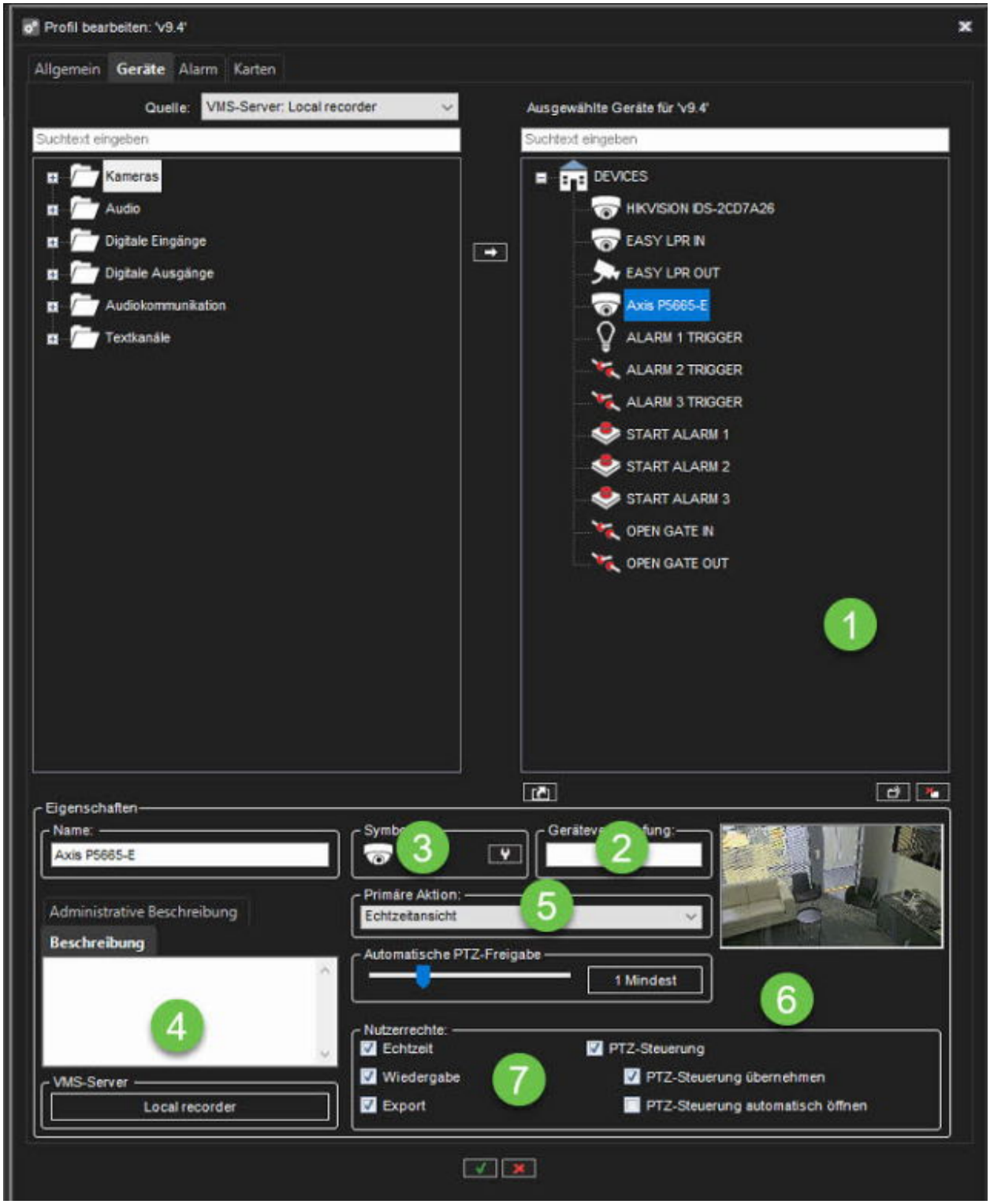
2. Wählen Sie die benötigten Komponenten oder Gerätegruppen aus dem linken Feld aus
3. Klicken Sie auf **Hinzufügen**
4. Um die Eigenschaften ausgewählter Komponenten zu ändern, gehen Sie bitte zu **Ausgewählte Geräte**



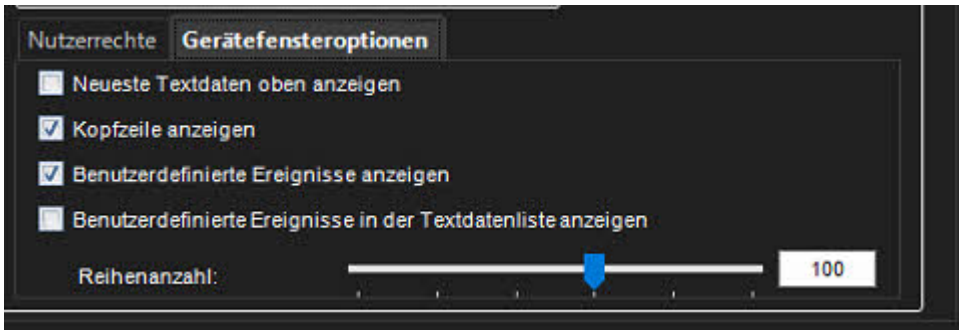
Ausgewählte Geräteeigenschaften

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



Optionen des Gerätefensters für Textkanäle



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

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.

Kopfzeile anzeigen

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

Benutzerdefinierte Ereignisse anzeigen

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

Benutzerdefinierte Ereignisse in der Textdatenliste anzeigen

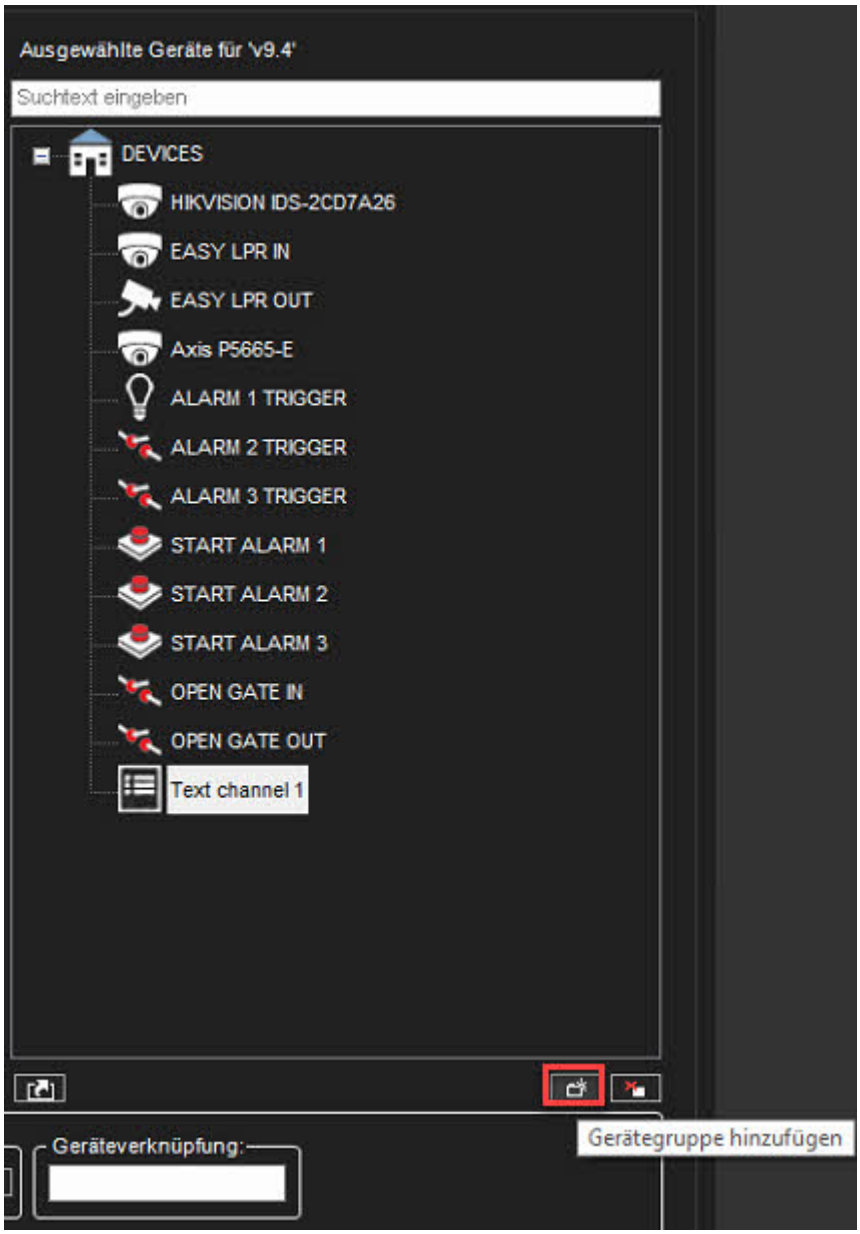
Wählen Sie diese Option, um benutzerdefinierte Ereignisse in der Textdatenliste (anstelle der benutzerdefinierten Ereignisliste) anzuzeigen.

Die Anzahl der Zeilen

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

Hinzufügen von Gerätegruppen zur Liste des ausgewählten Geräts

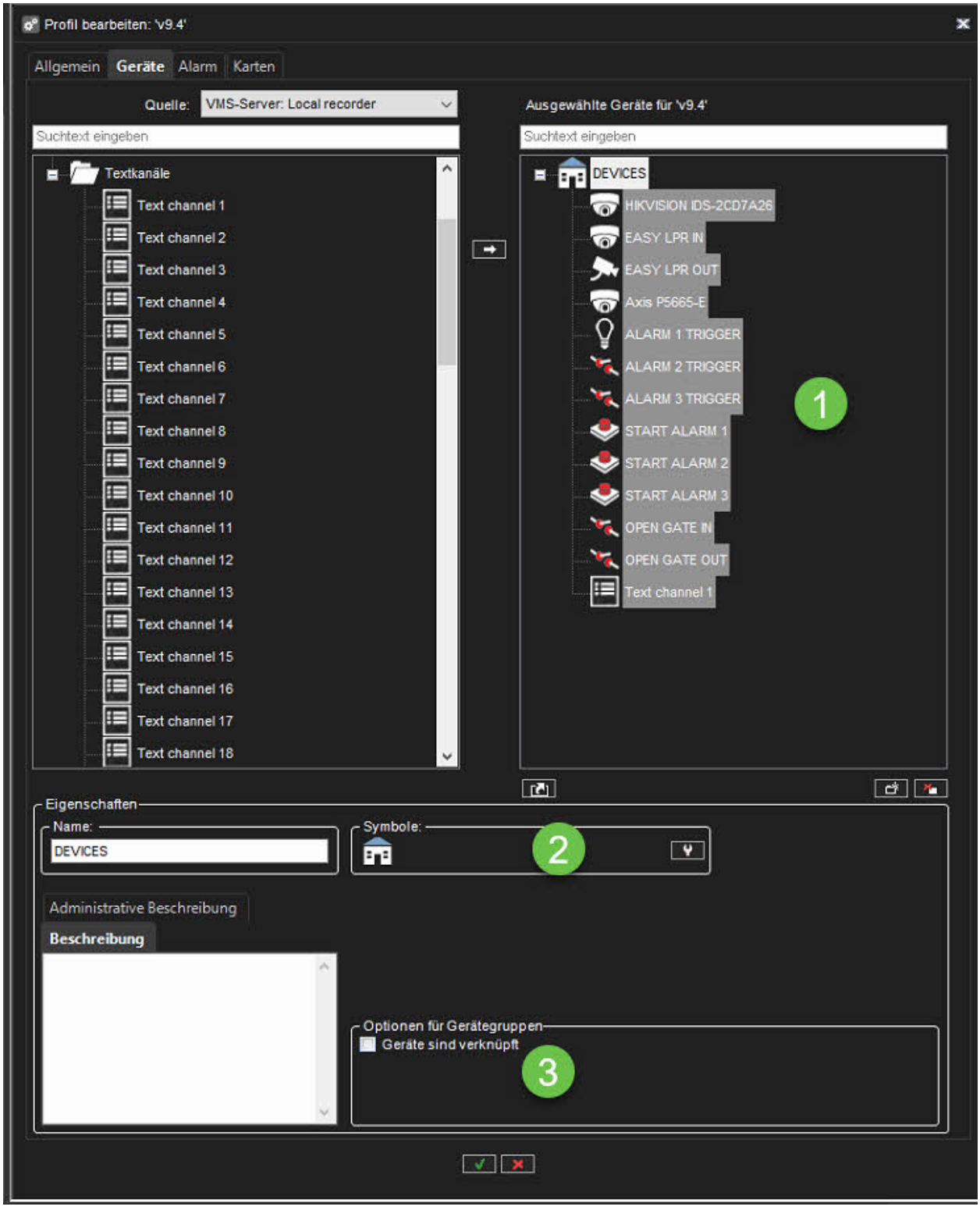
1. Klicken Sie unter dem Bereich **Ausgewählte Geräte** auf **Gerätegruppe hinzufügen**. Eine neue Gerätegruppe wird angezeigt.



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*

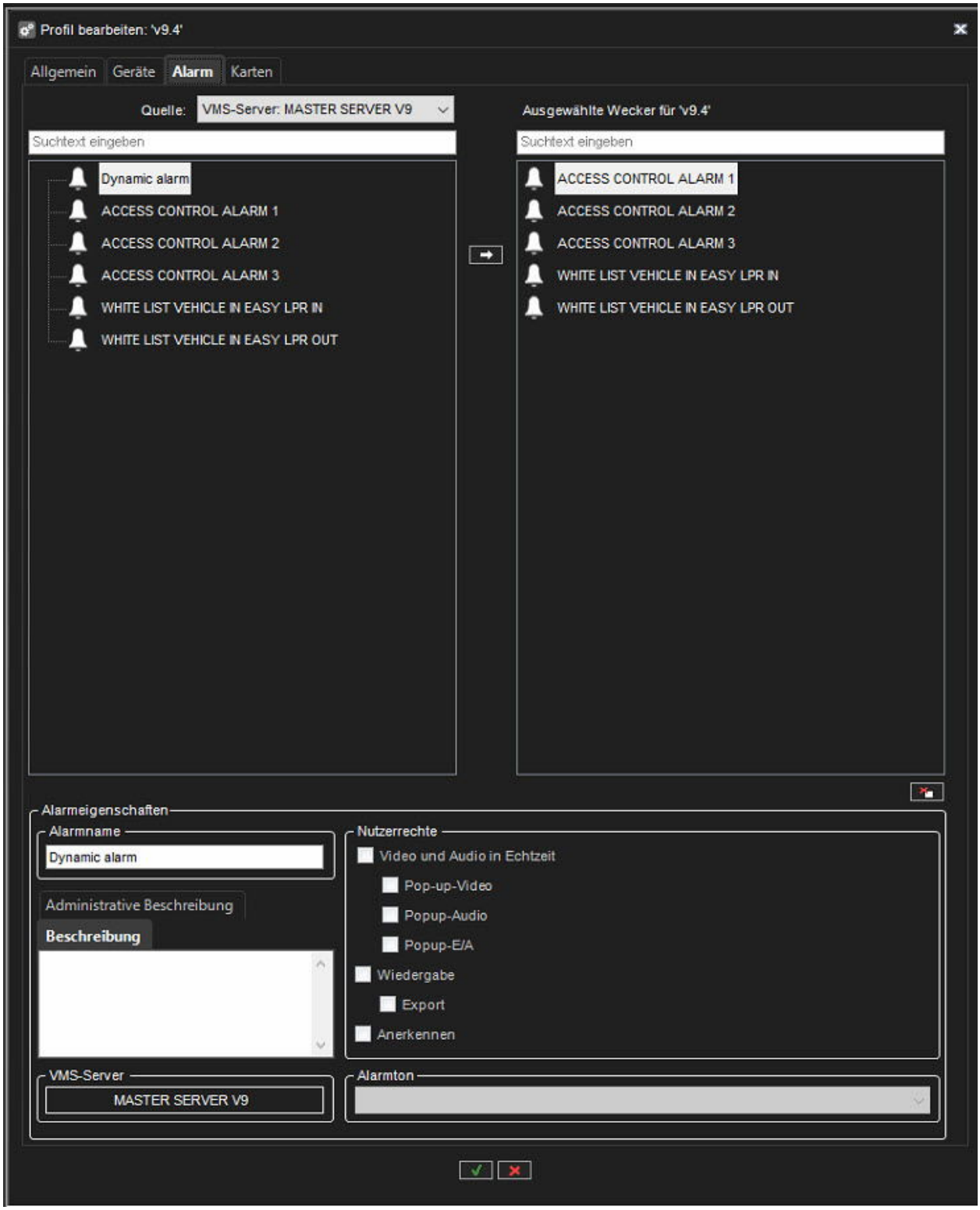
1. Klicken Sie auf die Gerätegruppe und geben Sie einen Namen dafür ein
2. Um das für die Gerätegruppe verwendete Symbol zu ändern, klicken Sie auf **Symbol ändern** . Wählen Sie dann das Symbol aus, das Sie verwenden möchten.
3. Geben Sie eine Beschreibung der Gerätegruppe in **Beschreibung** ein.

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).



Alarm

Bearbeiten profilspezifischer Alarmeinstellungen



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

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.*

So bearbeiten Sie profilspezifische Alarmbenutzerrechte:

1. Öffnen Sie die Registerkarte **Alarme**.
2. Klicken Sie im Bereich **Ausgewählte Alarme** auf einen Alarm.
3. Stellen Sie die Benutzerrechte für jeden Alarm ein. Die Einstellungen der Benutzerrechte befinden sich unten rechts auf der Registerkarte **Alarme**.
    a. Sie können individuelle Rechte für jeden Alarm festlegen oder mehrere Alarme auswählen (indem Sie die Umschalt- oder Steuerungstaste gedrückt halten, während Sie Alarme auswählen) und die gleichen Optionen für mehrere Alarme festlegen.
4. Damit der Computer bei einem Alarm einen Ton abspielt, wählen Sie **Alarmton** und dann den wiedergegebenen Ton. Um die Sounds zu testen, wählen Sie den Sound aus der Liste aus und klicken Sie auf **Play**.
5. Speichern Sie die Einstellungen durch Klicken auf **OK**.

Die Benutzerrechte umfassen:

- **Echtzeit-Video und -Audio**. Wählen Sie diese Option, damit die Benutzer Alarmvideos oder -audios in Echtzeit sehen können.
- **Pop-up video**. Wählen Sie diese Option aus, damit Benutzer automatisch Alarmvideos erhalten.
- **Pop-up audio**. Wählen Sie diese Option aus, damit Benutzer automatisch Alarmtöne erhalten.

- **Wiedergabe** Wählen Sie diese Option, um das Alarmvideo des Benutzers abzuspielen.
- **Export** Wählen Sie diese Option, damit die Benutzer Alarmvideos auf lokalen Medien speichern können.
- **Anerkennen** Wählen Sie diese Option, damit die Benutzer Alarme bestätigen können.

Karten

Hinzufügen von Karten zu Profilen

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.

So entfernen Sie eine Sitemap:

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

So entfernen Sie ein Symbol von der Karte:

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

oben Vorherige Nächste

1.11. 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.

Benutzer abmelden

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

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.

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.

oben Vorherige Nächste

1.11.1. Benutzergruppe

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.

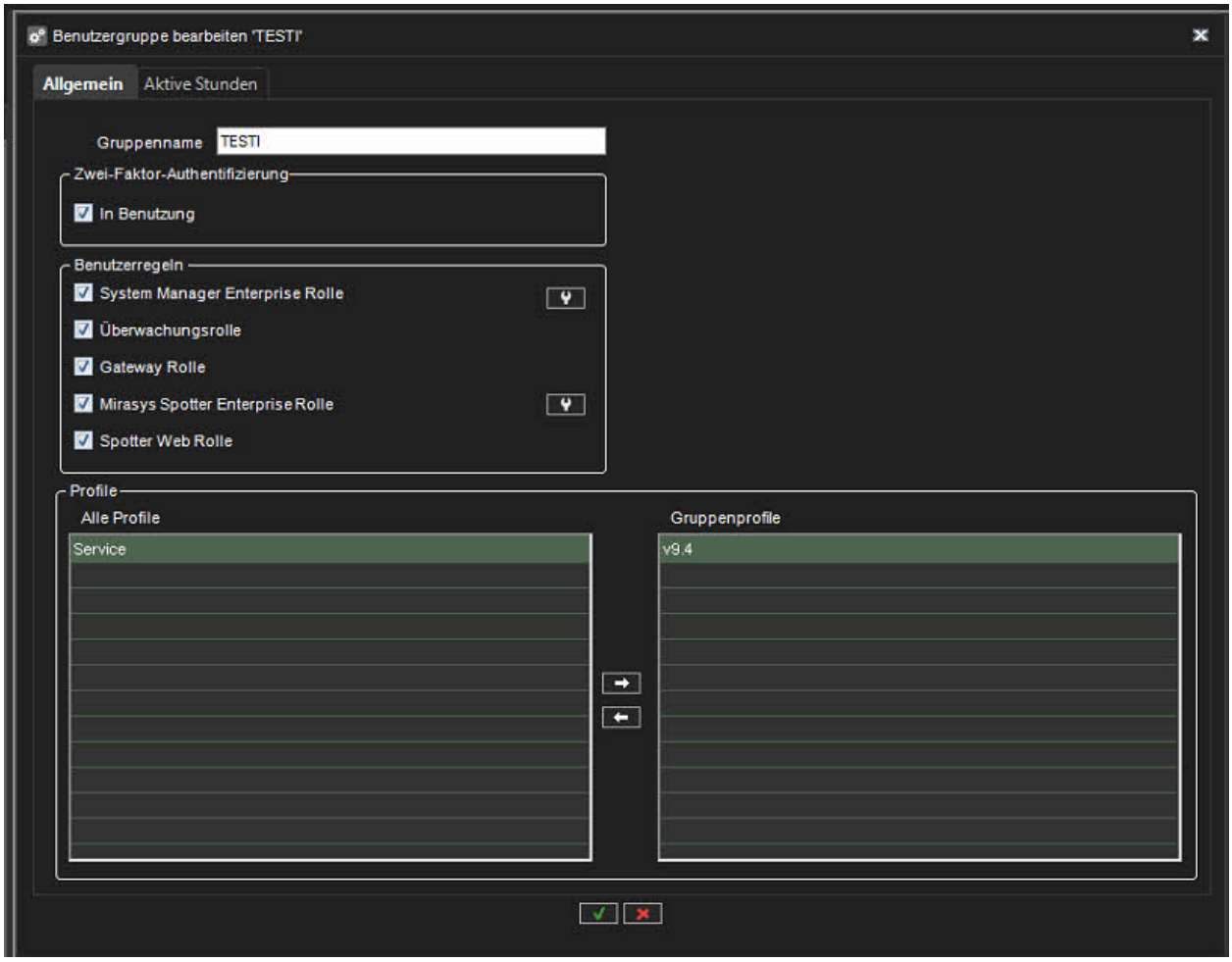
oben Vorherige Nächste

1.11.1.1. Benutzerregeln

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



oben Vorherige Nächste

1.11.1.1.1. 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.

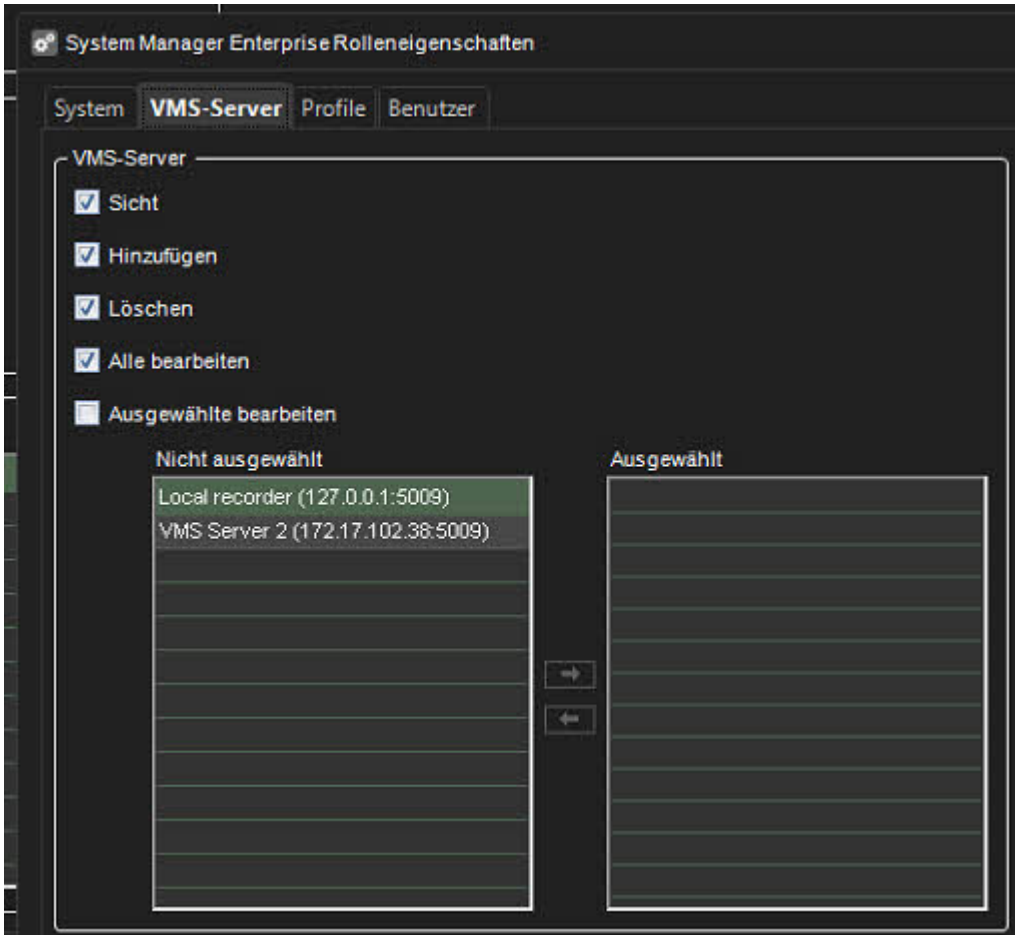
System

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

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.

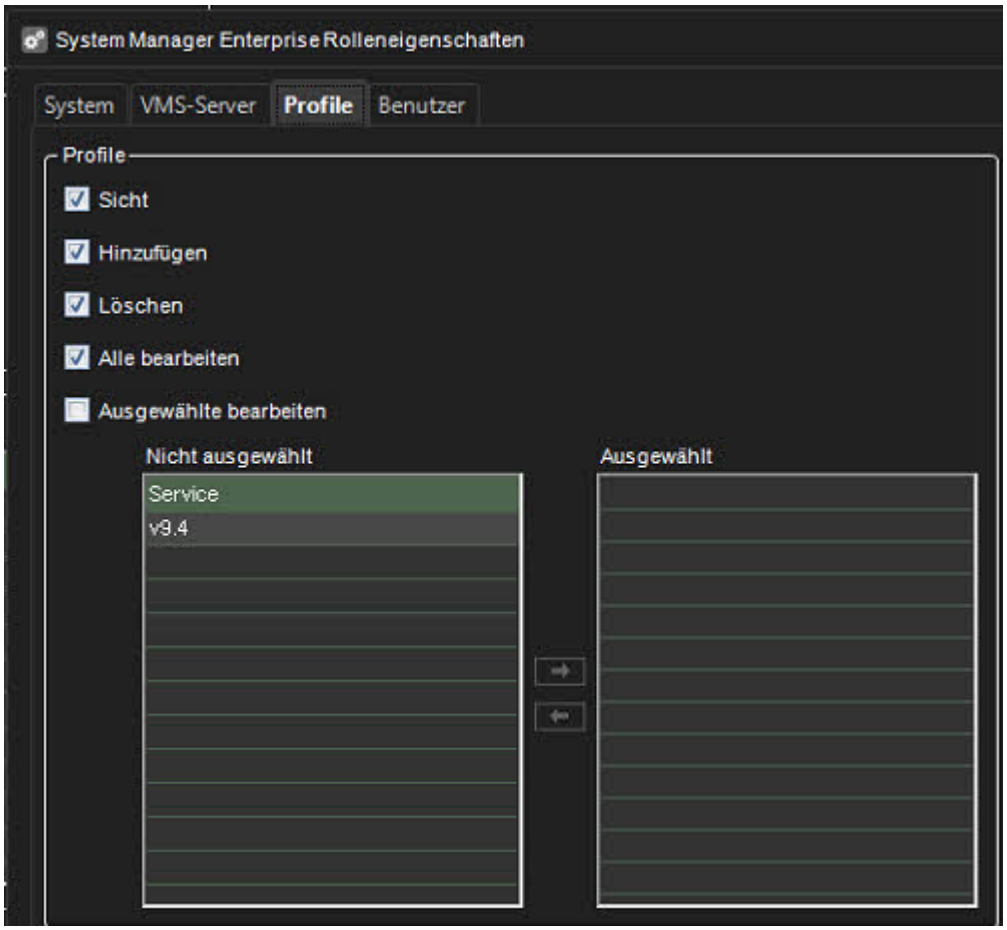
Dies ist in großen Installationen praktisch, wenn bestimmte Benutzergruppen mit bestimmten Servern arbeiten (z. B. wenn es separate Wartungsgruppen für verschiedene Standorte gibt - und die Aufzeichnungsserver standortspezifisch sind.)



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“).



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

oben Vorherige Nächste

1.11.1.1.2. Überwachungsrolle

Die Benutzer mit der Rolle Überwachung haben die Berechtigung:

System

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

Profiles

Kann den Inhalt der Profile anzeigen

Benutzer

Kann die Systembenutzergruppen und -benutzer anzeigen

oben Vorherige Nächste

1.11.1.1.3. Gateway-Rolle

Gateway-Rolle ermöglicht die alte Spotter Mobile-Nutzung

oben Vorherige Nächste

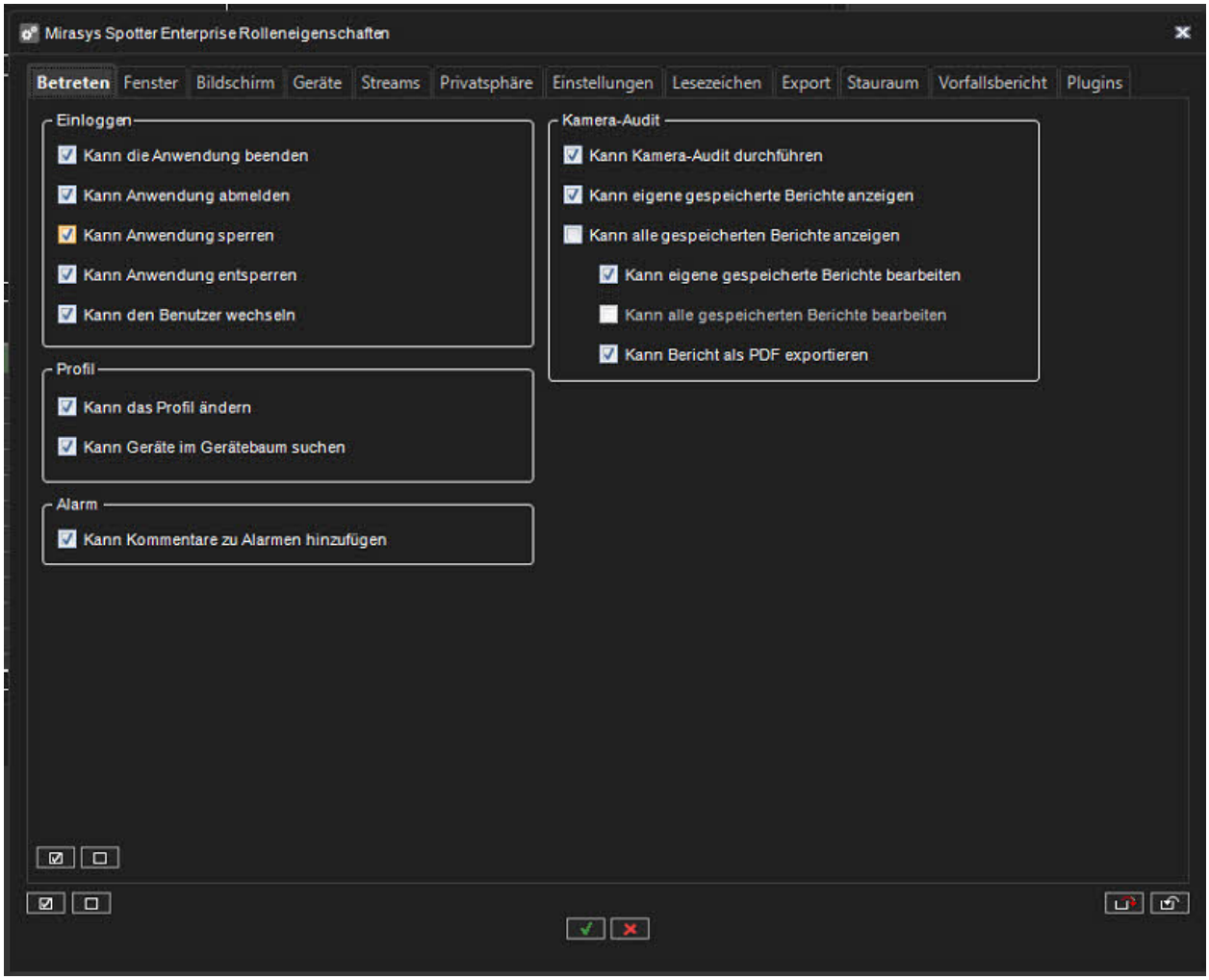
1.11.1.1.4. Mirasys Spotter Enterprise Rolle

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.

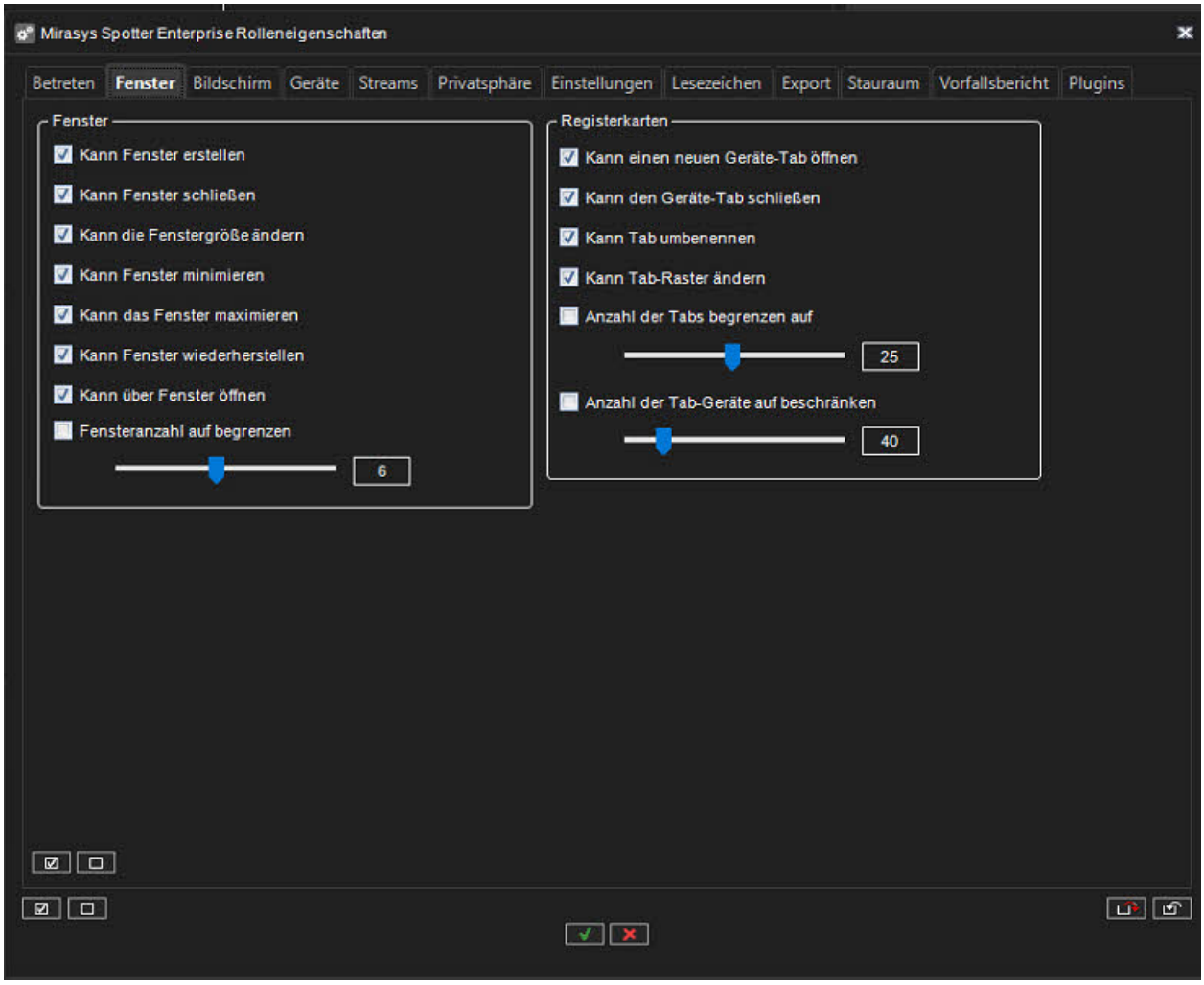
Access

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



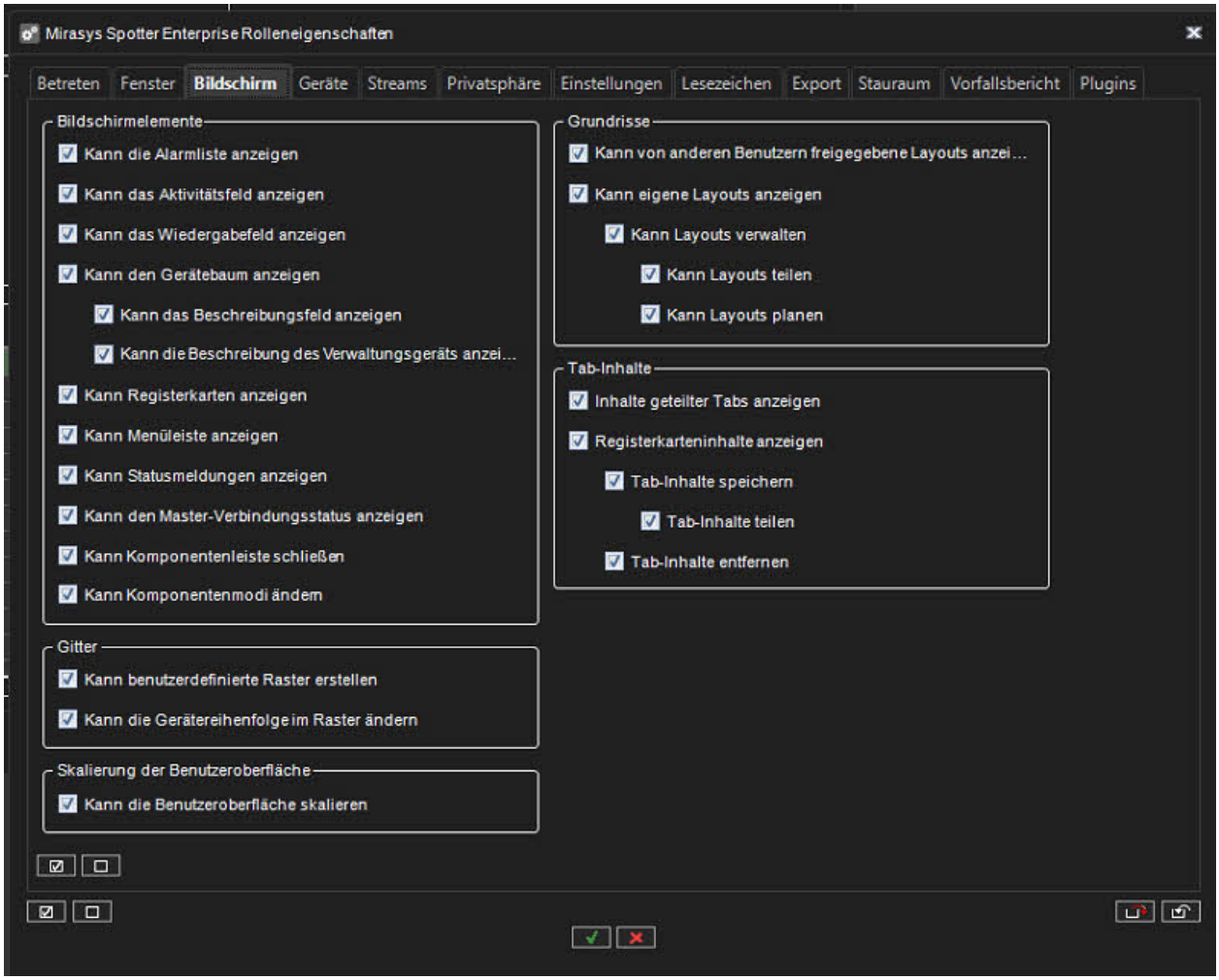
Fenster

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



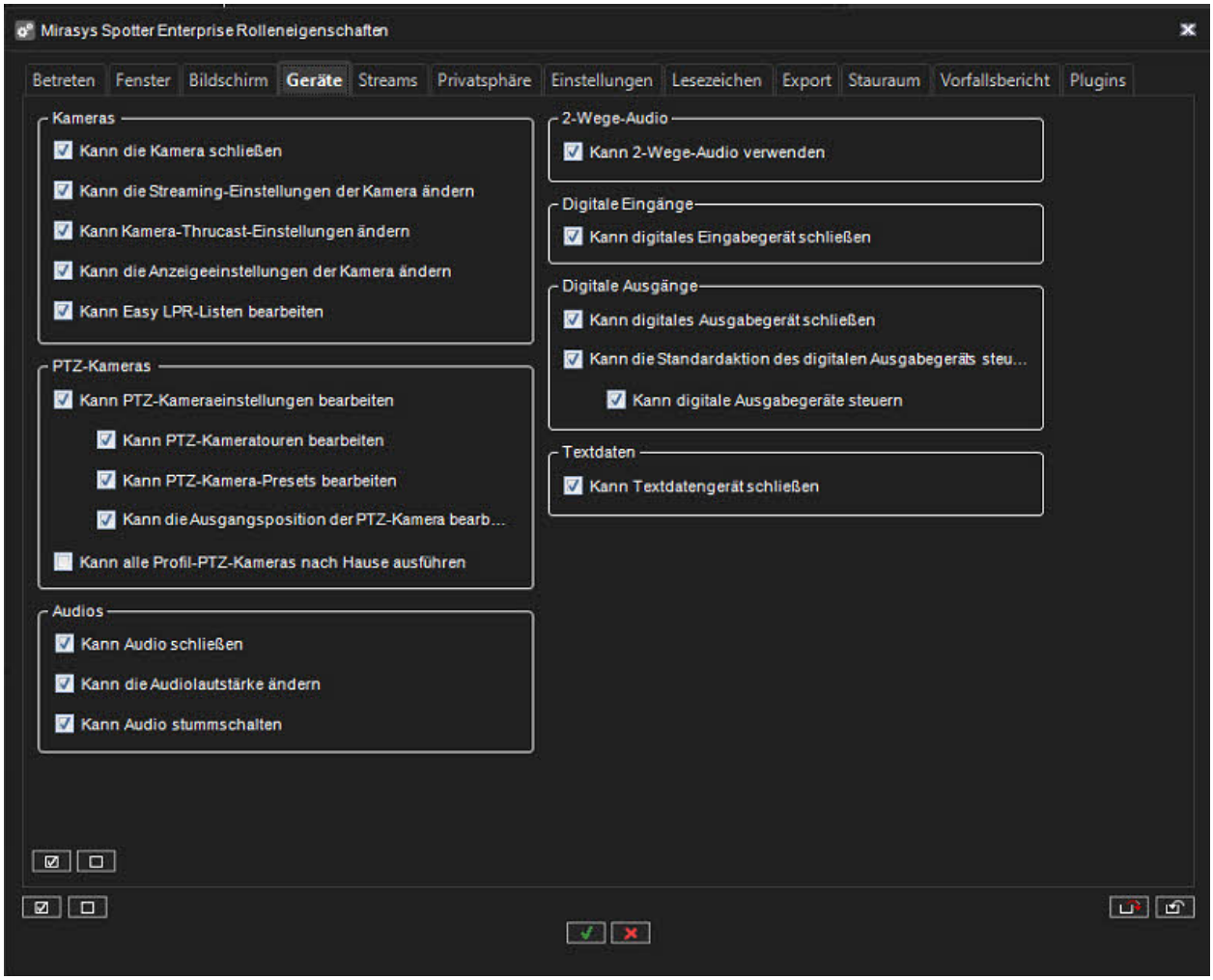
Bildschirm

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



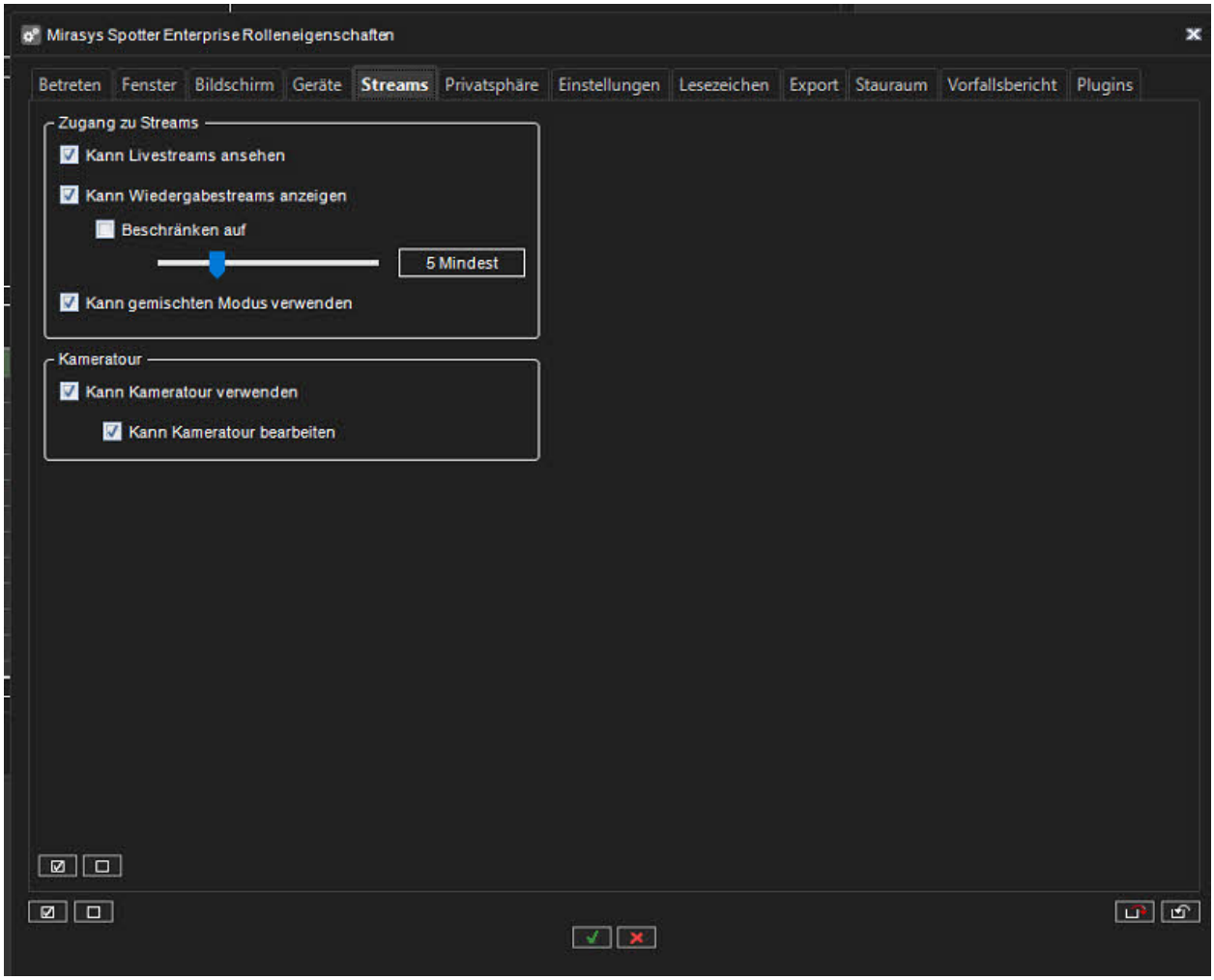
Geräte

Die Registerkarte Geräte enthält Optionen zur Mediensteuerung.



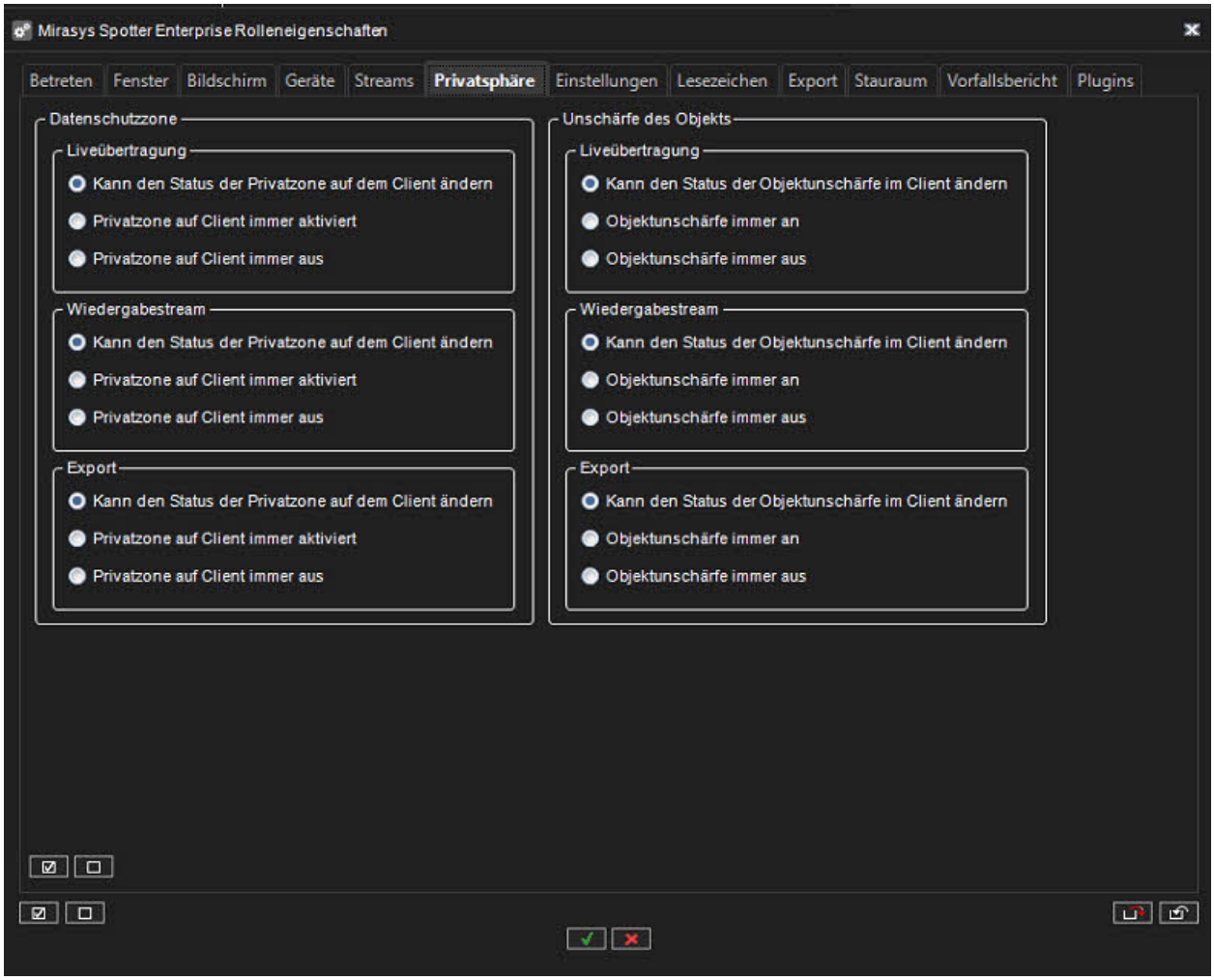
Streams

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



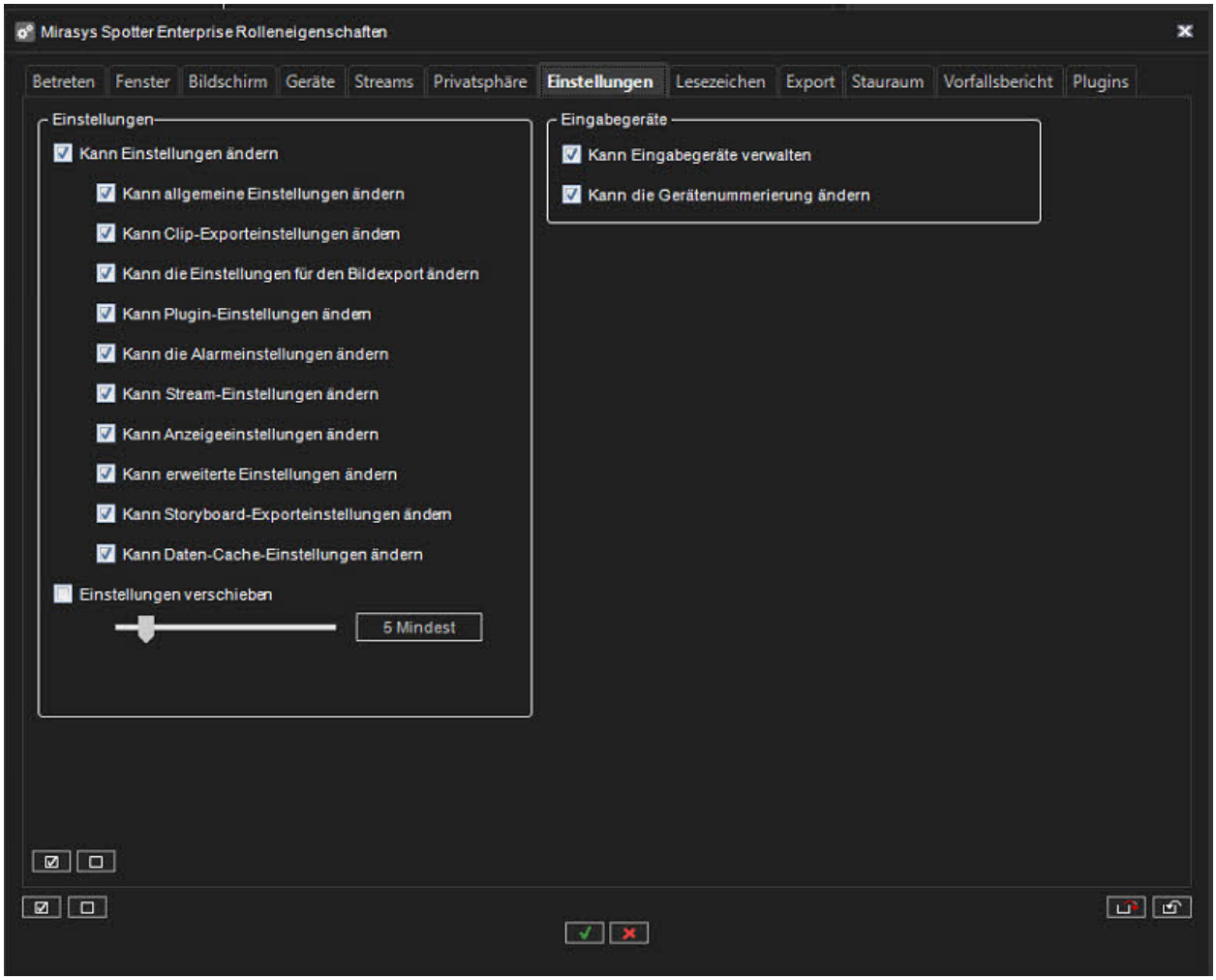
Privatsphäre

Die Registerkarte Privatsphäre enthält Optionen für den Datenschutz.



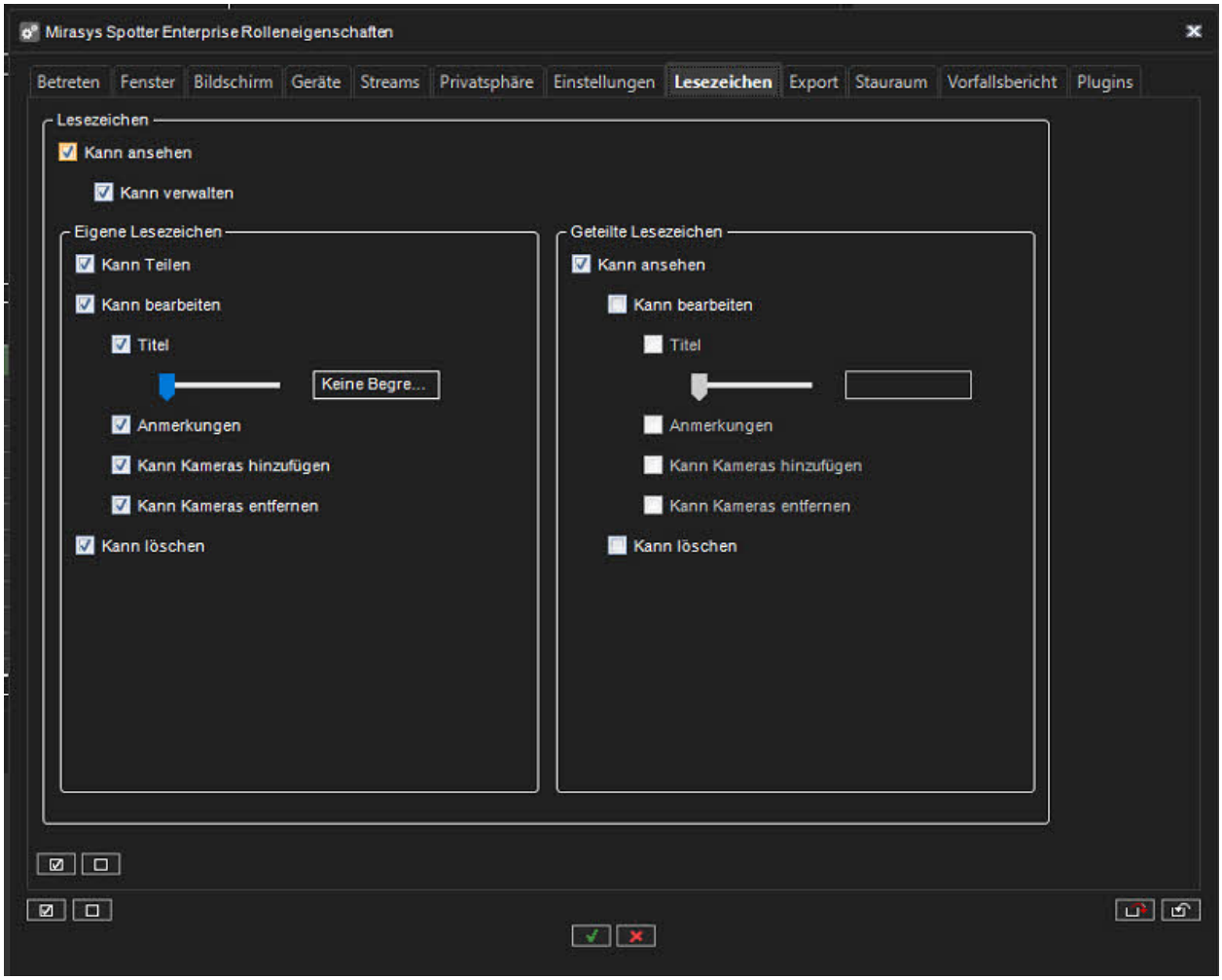
Einstellungen

Die Registerkarte Einstellungen enthält Optionen für Spotter-Einstellungen.



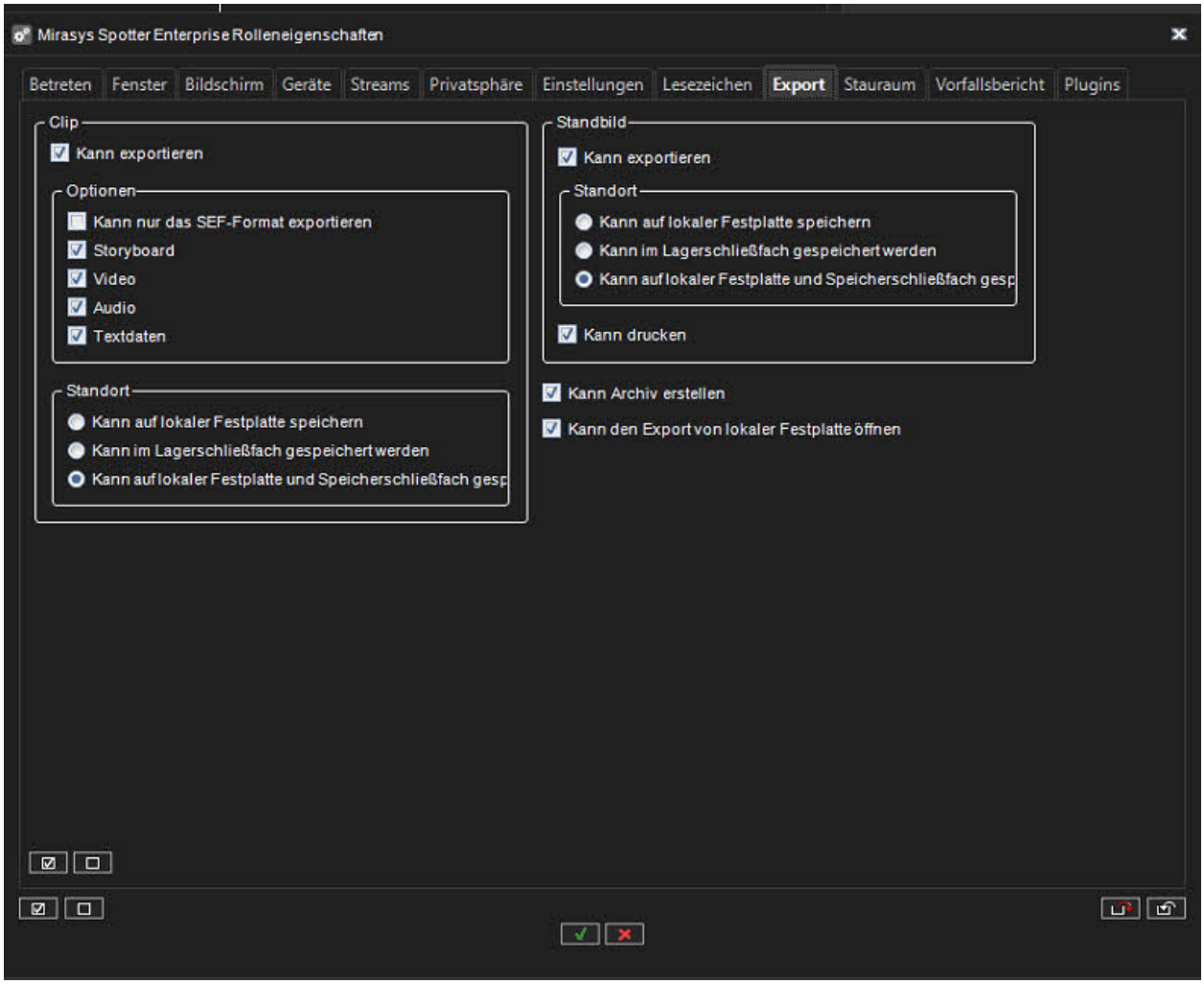
Lesezeichen

Die Registerkarte „Lesezeichen“ enthält Optionen für Lesezeichen



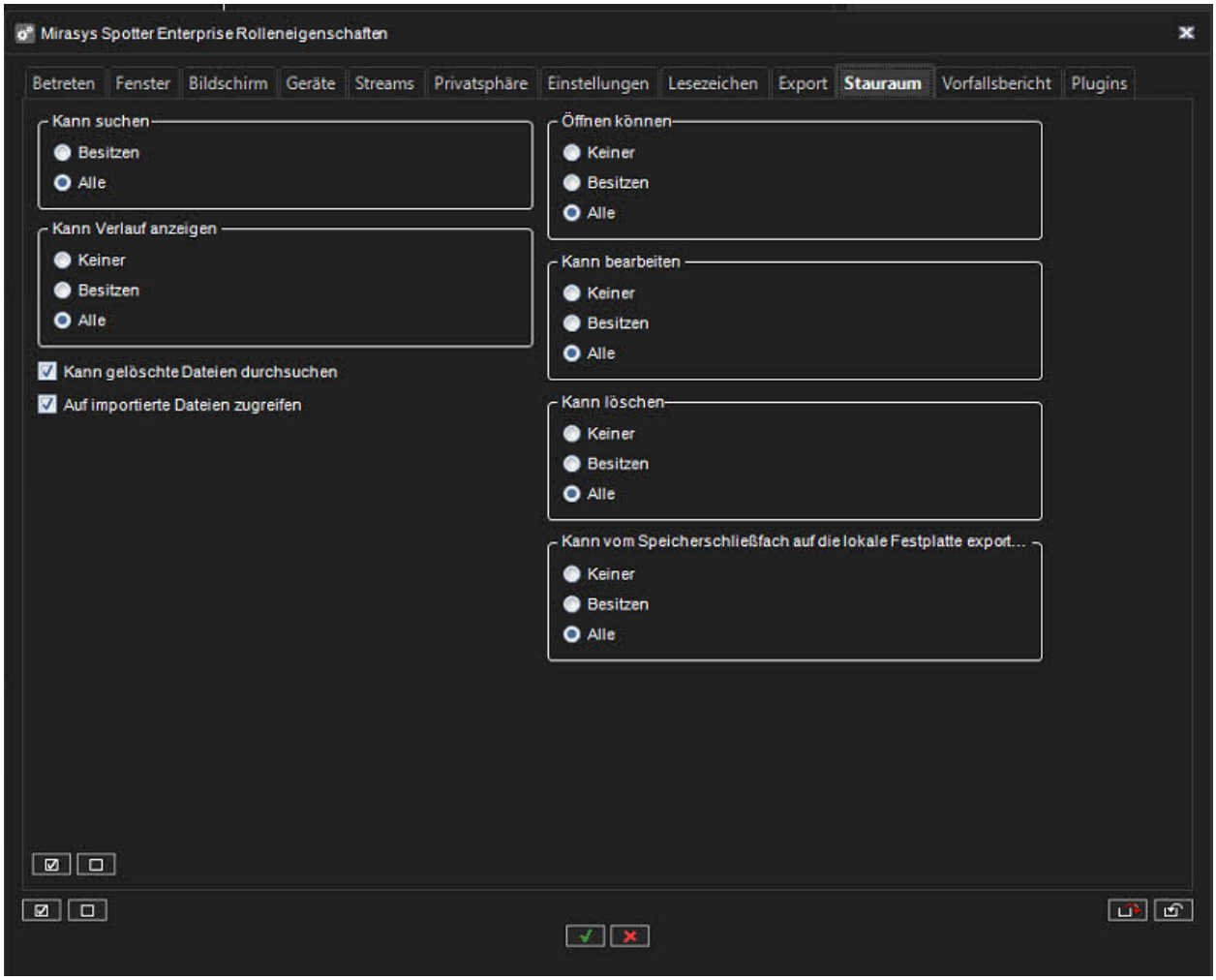
Export

Die Registerkarte Export enthält Optionen für Exportfunktionen



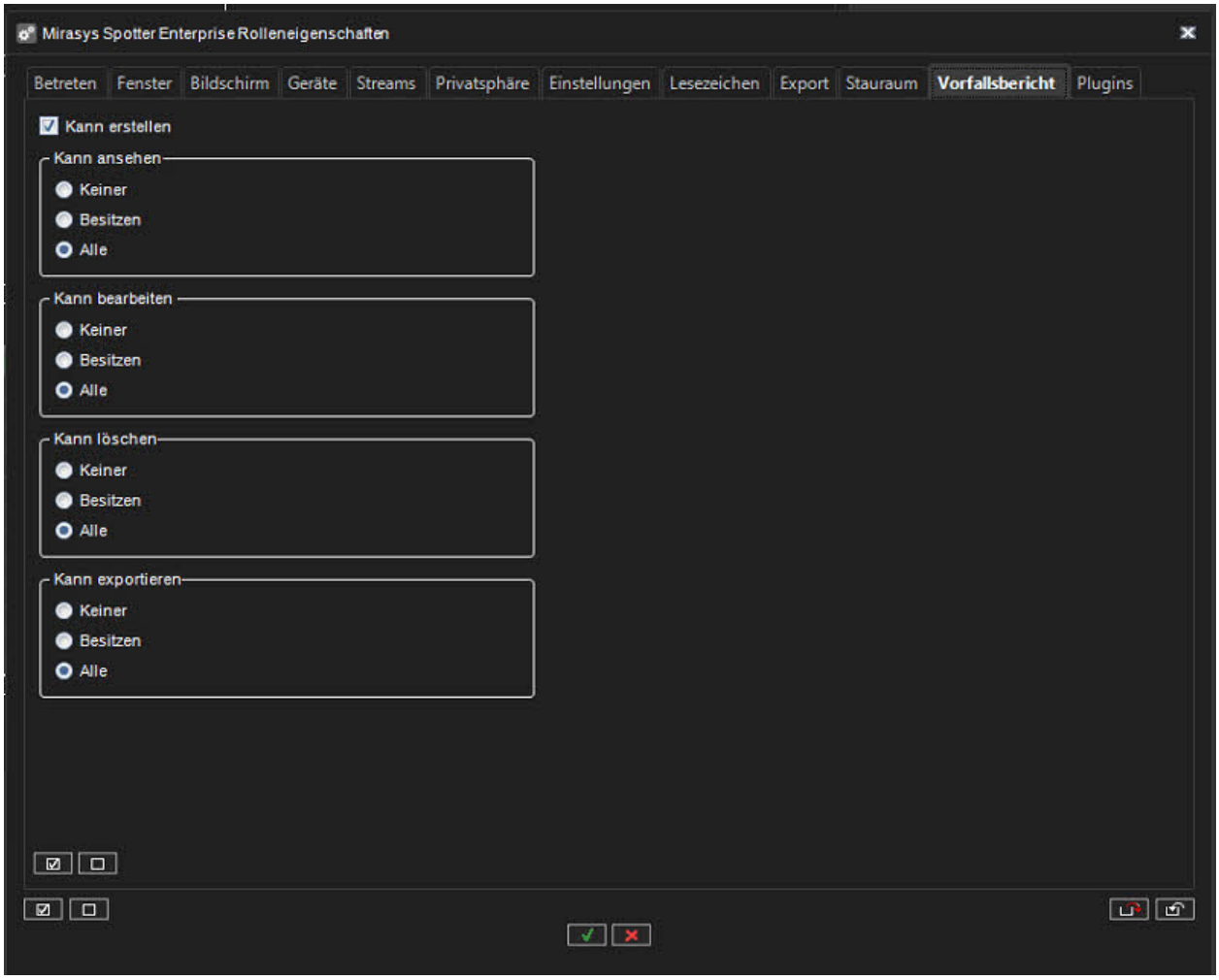
Storage Locker

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



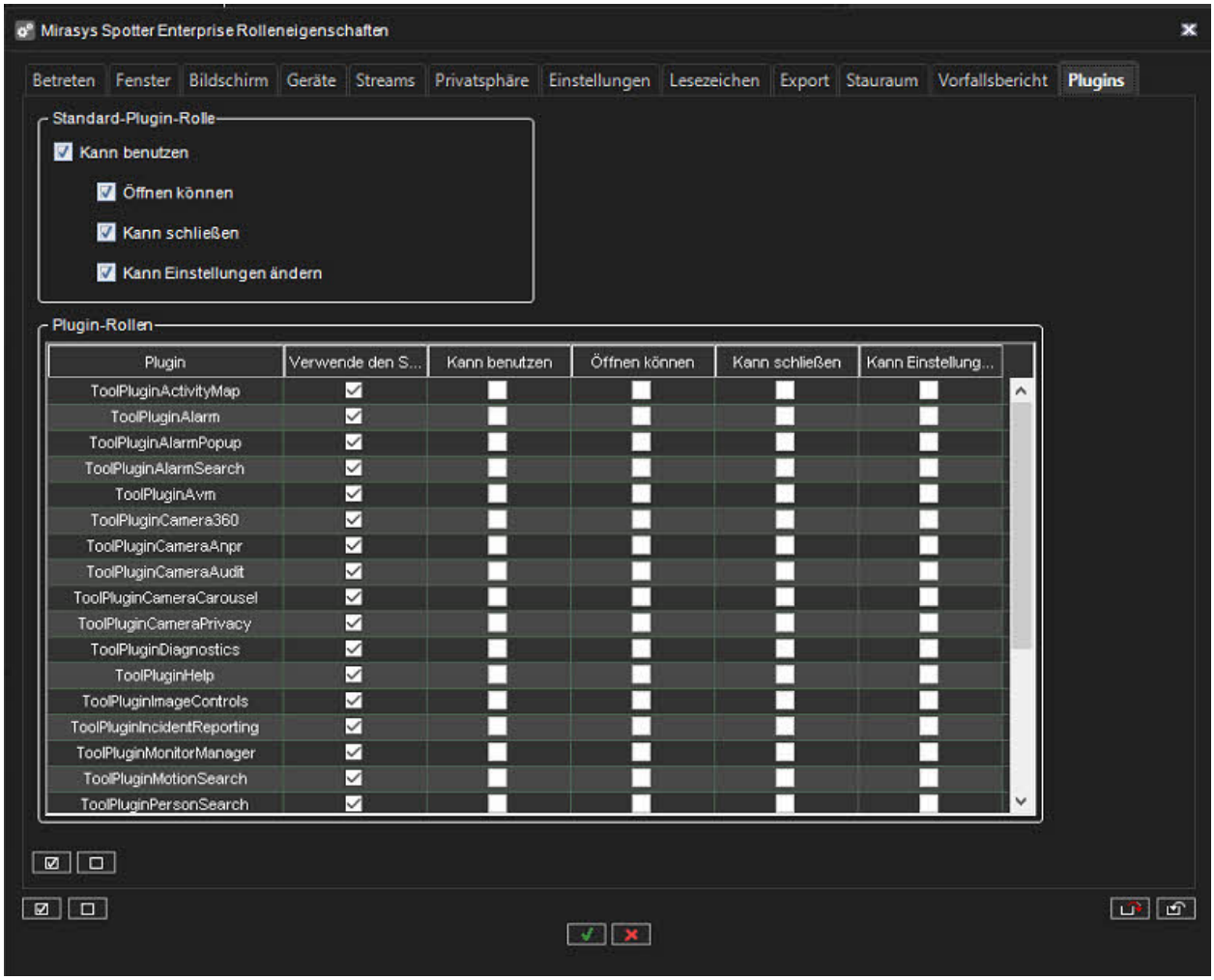
Vorfallsbericht

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



Plugins

Die Registerkarte Plugins enthält Optionen für Spotter-Plugins.



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

oben Vorherige Nächste

1.11.1.1.5. Spotter Web role

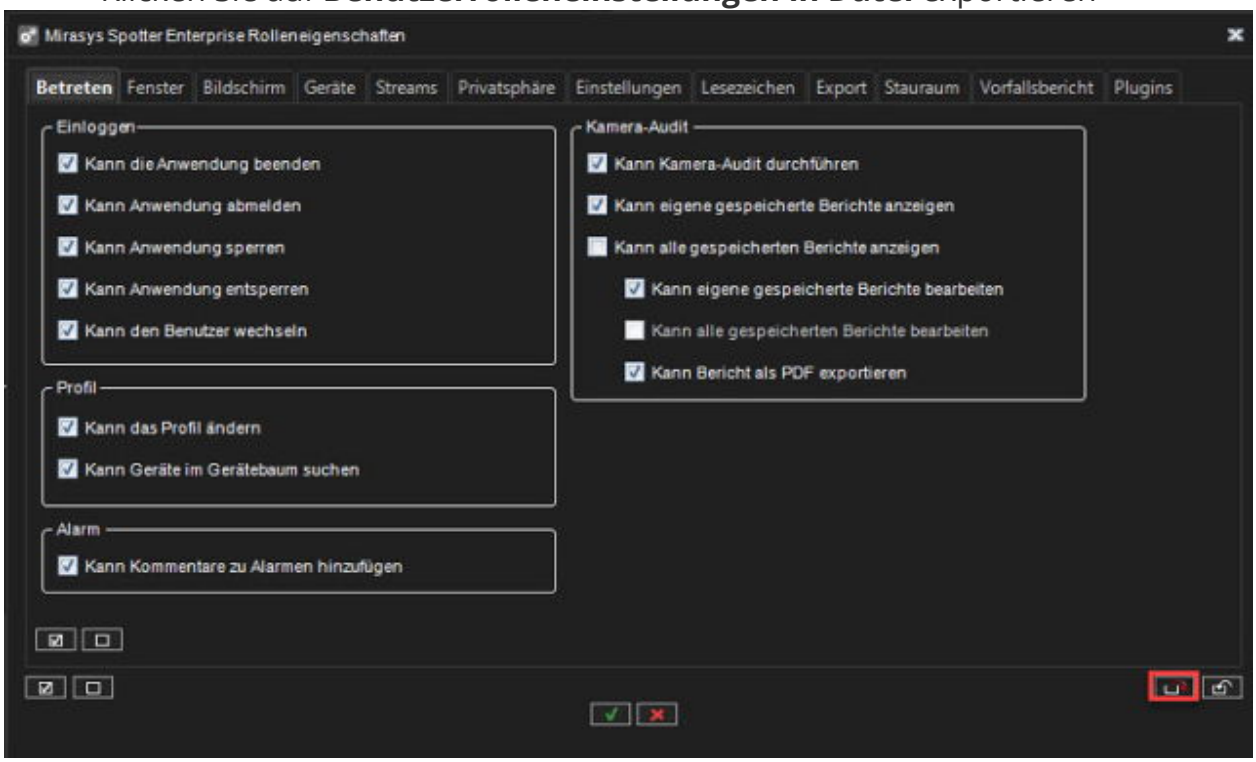
Spotter Web-Rolle ermöglicht neue Spotter Web- und Spotter Mobile-Nutzung

oben Vorherige Nächste

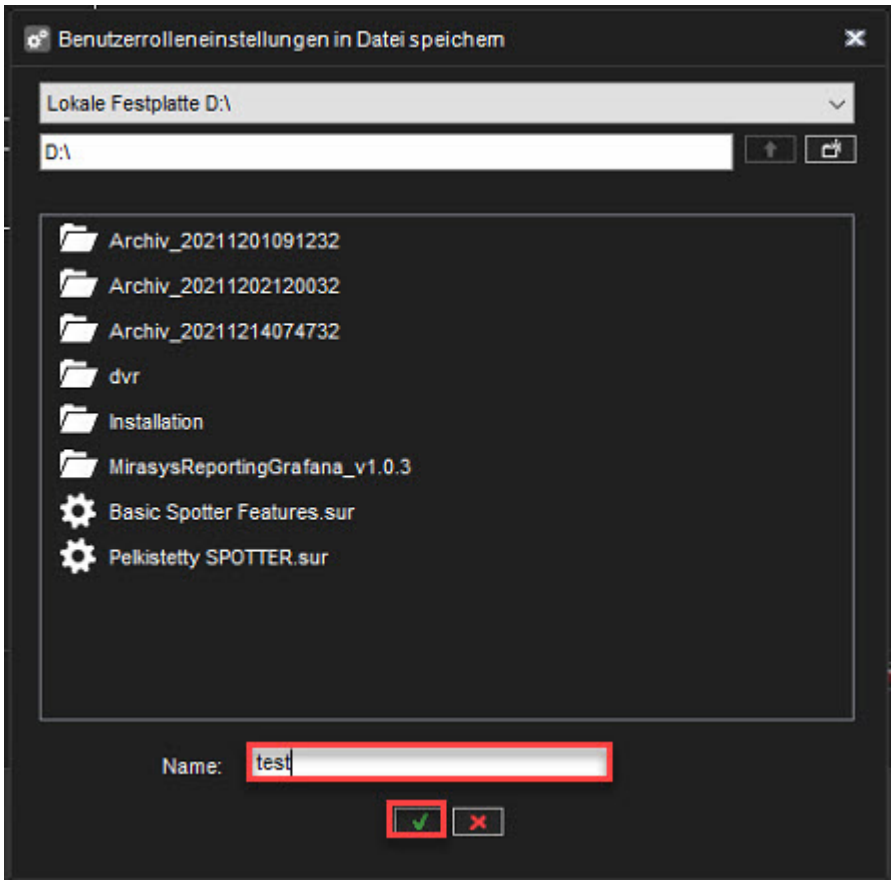
1.11.1.1.6. Exportieren und Importieren von Benutzerrolleneinstellungen

Benutzerrolleneinstellungen werden exportiert

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

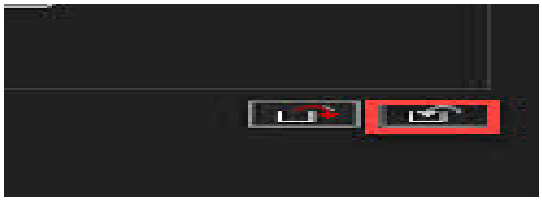


2. Ziel aussuchen
3. Legen Sie den Namen der Datei fest
4. Klicken **OK**

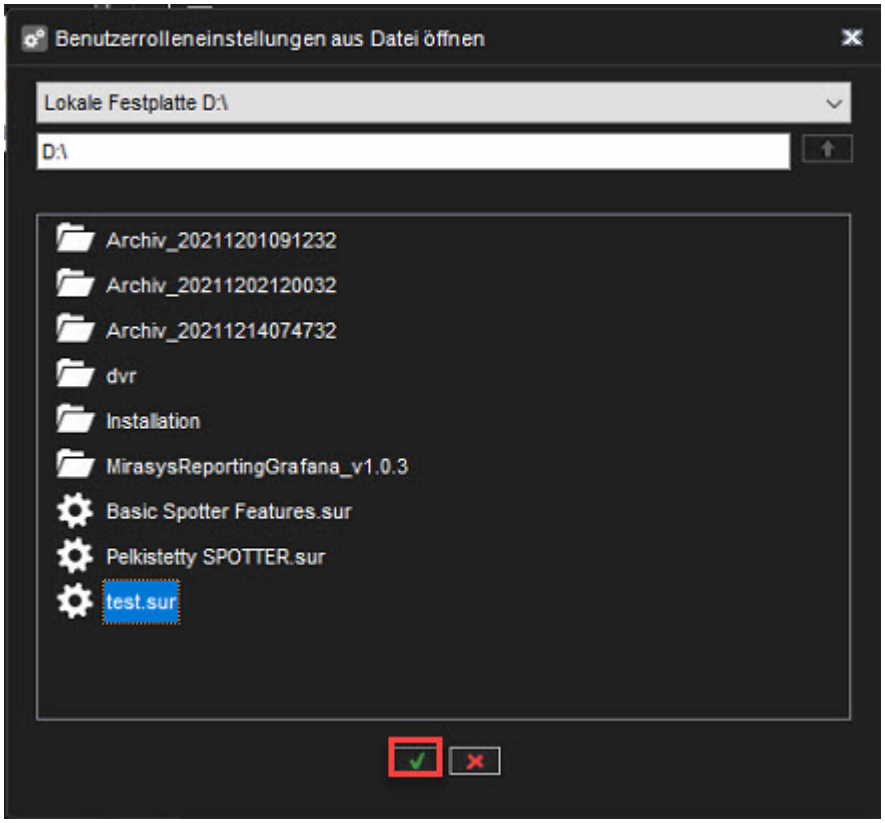


Importieren von Benutzerrolleneinstellungen

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



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



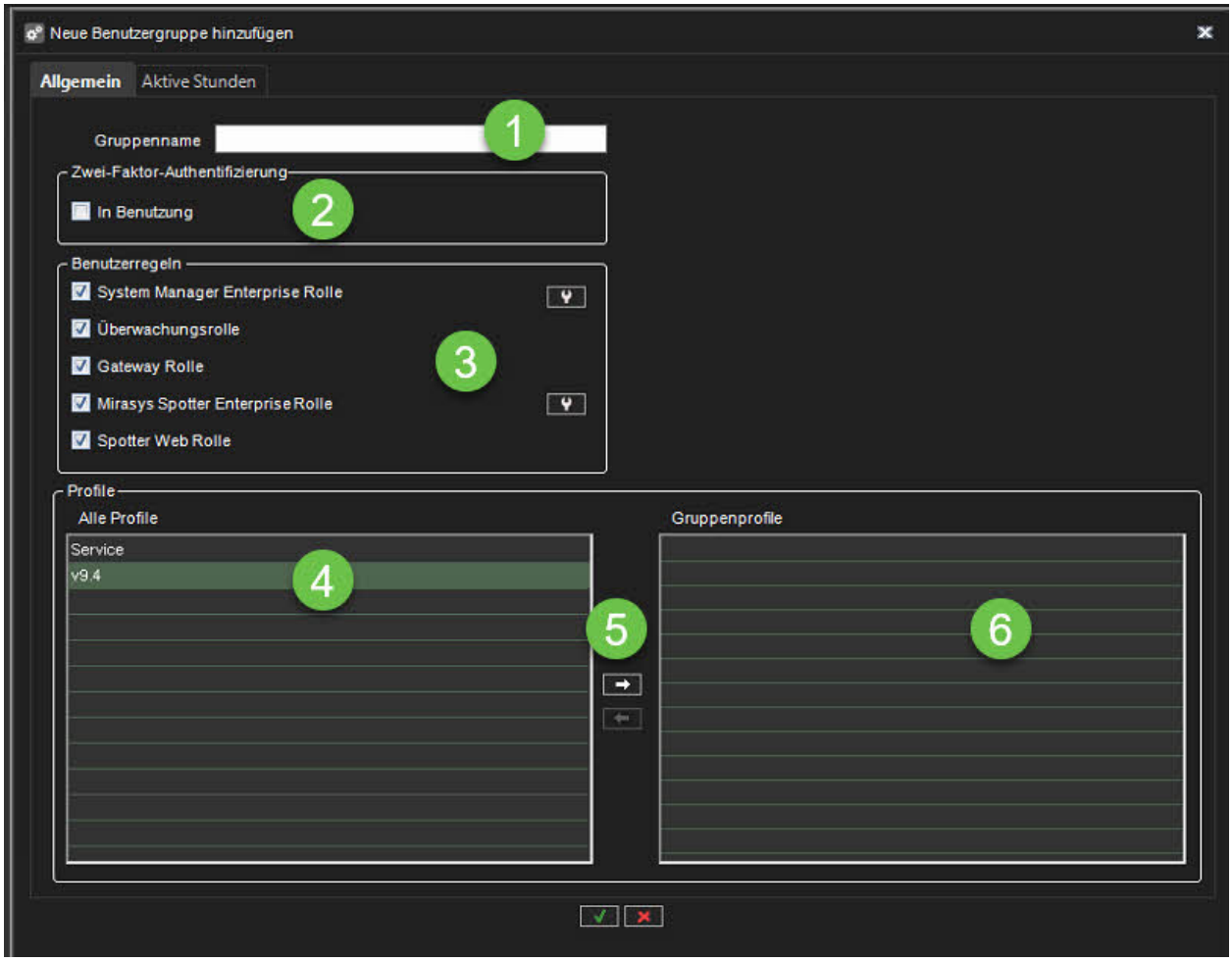
oben Vorherige Nächste

1.11.1.2. Erstellen einer kundenspezifischen Benutzergruppe

1. Klicken Sie **Benutzergruppe hinzufügen**

1. Geben Sie einen Namen für die Gruppe in das Feld **Gruppenname** ein
2. Aktivieren Sie bei Bedarf die **Zwei-Faktor-Authentifizierung**
3. Wählen Sie die **Benutzerrollen** für die Gruppe aus.
4. Wählen Sie das **Profil** oder **Profile** aus, das Sie der Benutzergruppe zuweisen möchten.
5. 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
6. Überprüfen Sie, ob die richtigen Profile gefunden wurden
7. 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.*



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.*

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.

3. Klicken Sie oben links auf **Benutzergruppe löschen**.
4. 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.*

oben Vorherige Nächste

1.11.1.3. Zwei-Faktor-Authentifizierung

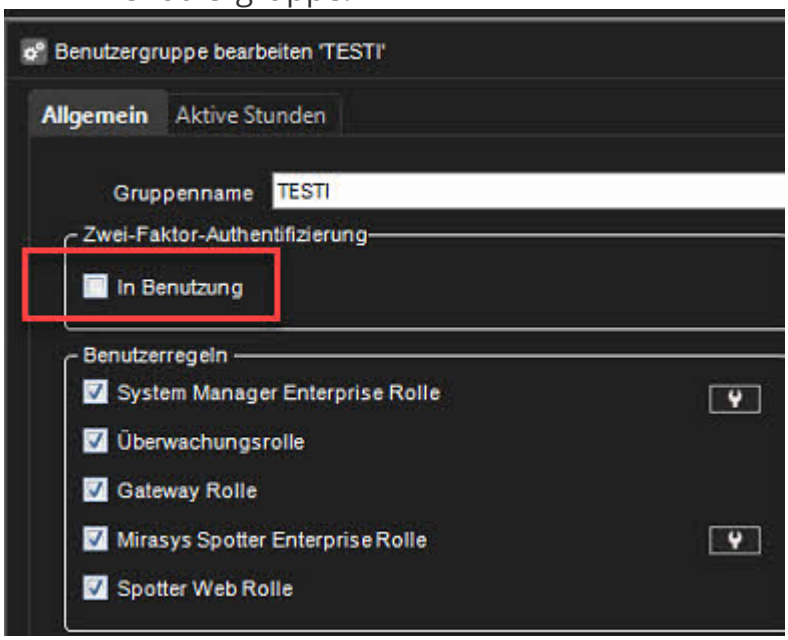
Die Zwei-Faktor-Authentifizierung ist eine Funktion zur Verbesserung der Identifizierung des Benutzers, indem der Benutzername und das Kennwort sowie ein Code von einem externen physischen Gerät angefordert werden.

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.)

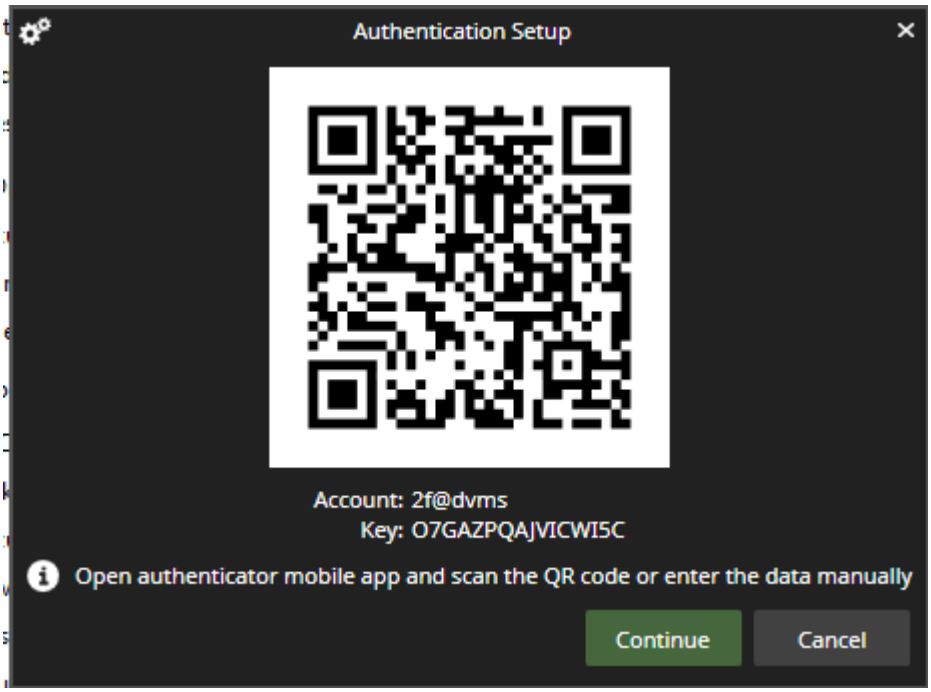
Aufstellen:

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.

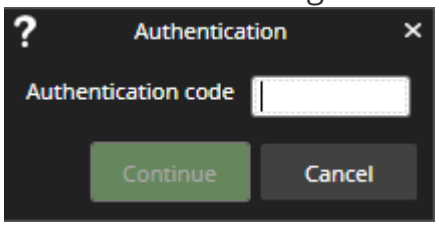
Beispiel unten:



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.)

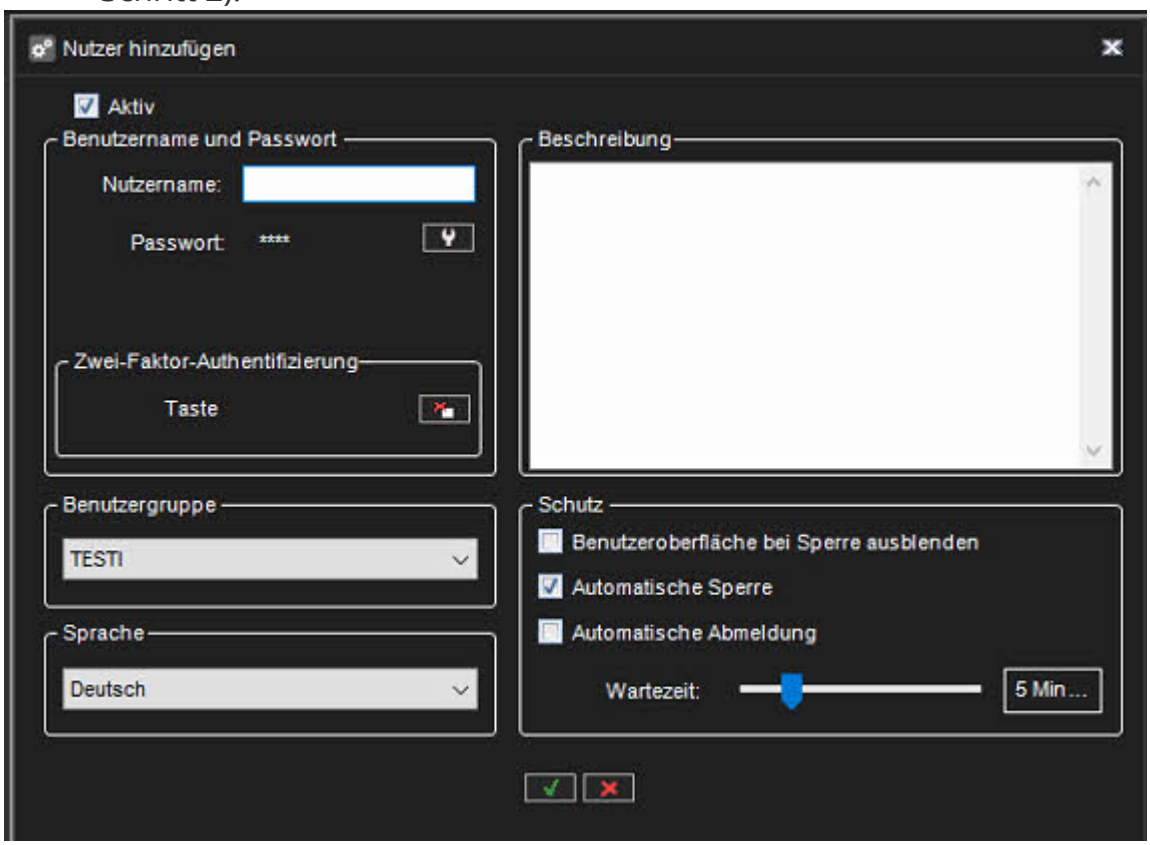
Anmeldung:

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.



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).



oben Vorherige Nächste

1.11.1.4. Domänenbasierte Benutzergruppen (LDAP)

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.

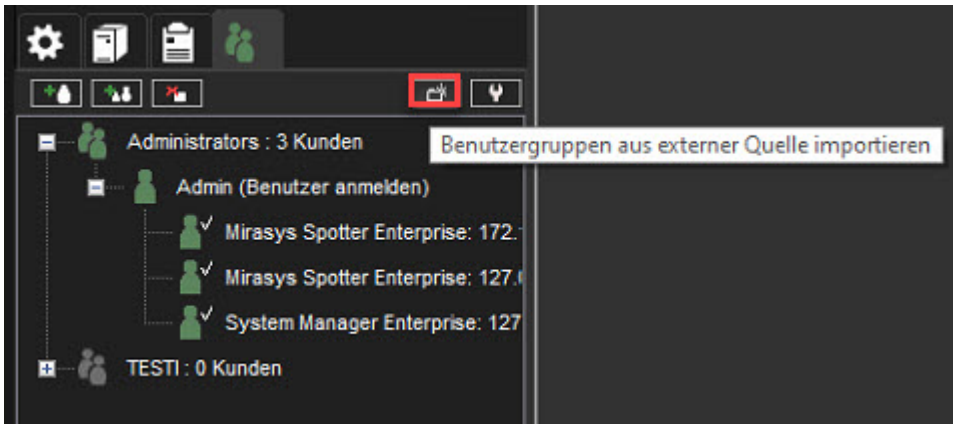
Diese Funktion erfordert ein Lizenzupdate.

So fügen Sie dem System eine neue domänenbasierte Benutzergruppe hinzu:

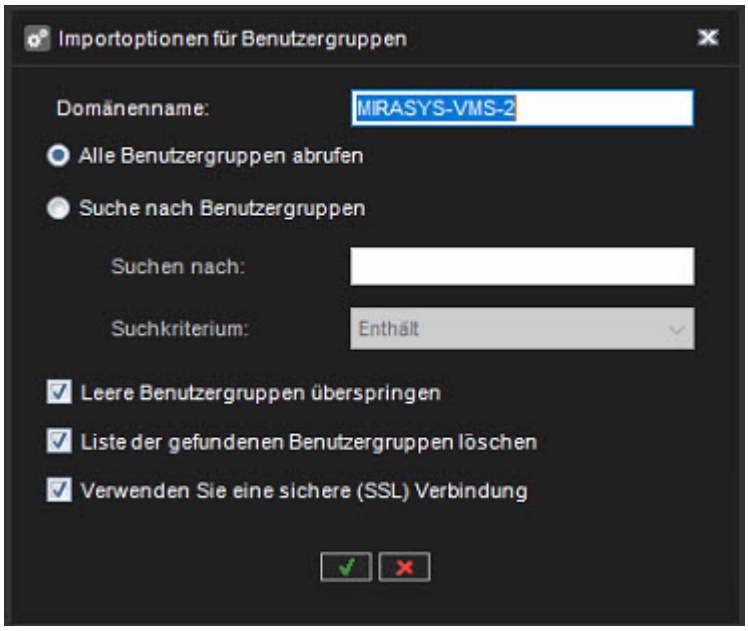
1. Klicken Sie in der oberen linken Ecke der Registerkarte **Benutzer** auf **Benutzergruppen aus einer externen Quelle importieren**

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.
    a. 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.



oben Vorherige Nächste

1.11.2. 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.

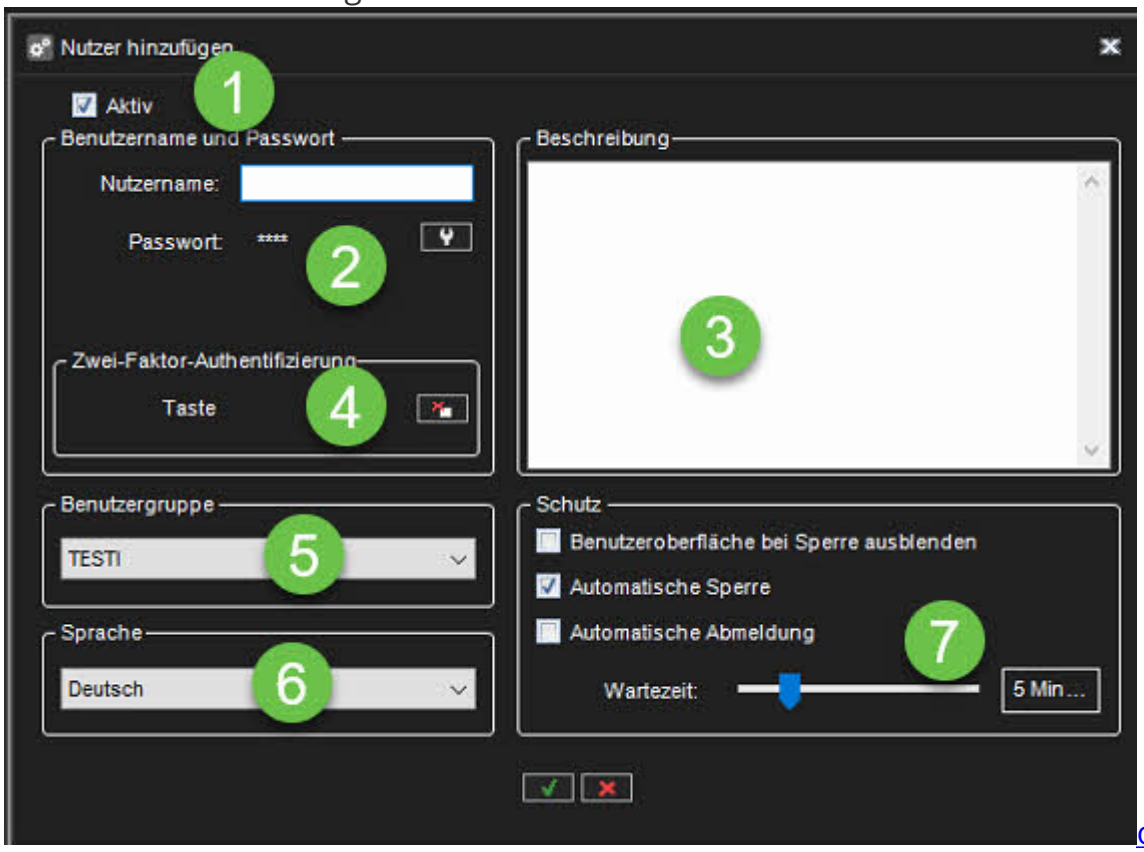
Hinweis: Benutzer können ihre Passwörter und die Sprache der Benutzeroberfläche im Spotter-Programm ändern.

oben Vorherige Nächste

1.11.3. Benutzerkontoeinstellungen

Die Benutzerkontoeinstellungen enthalten die folgenden Optionen:

- Kontostatus
- Passwort
- Two-factor authentication key management, see more from Two-factor authentication
- Benutzergruppe
- Sprache
- Schutzeinstellungen



oben
Vorherige Nächste

1.11.4. Deaktivieren oder Aktivieren eines Benutzerkontos

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**.

3. Klicken Sie auf **OK**.

Hinweis: *Domänenbasierte (LDAP) Benutzer können mit System Manager nicht gelöscht oder entfernt werden.*

oben Vorherige Nächste

1.12. TruCast

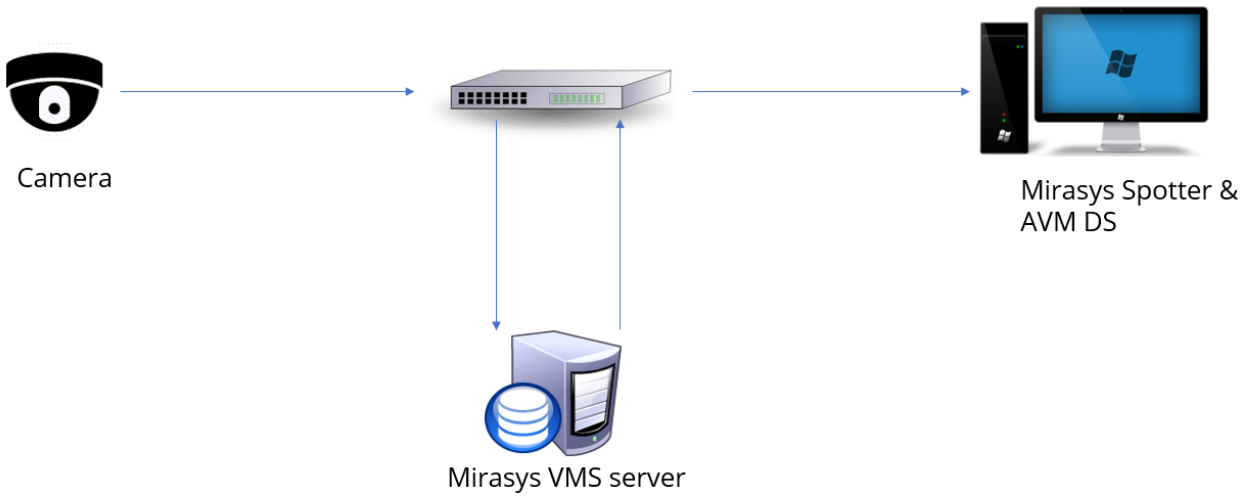
TruCast

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

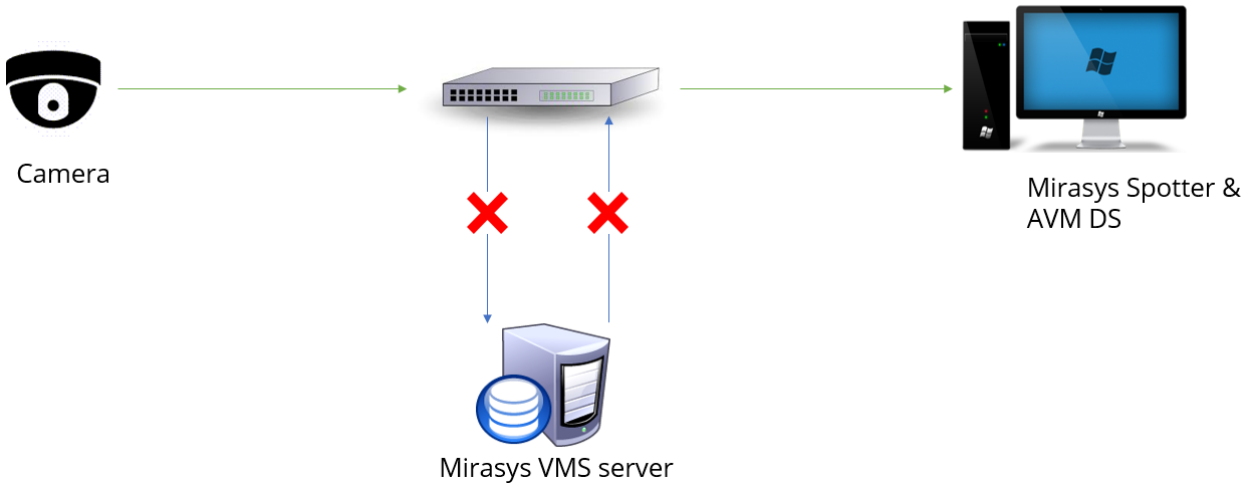
Bei TruCast kommt der Videostream direkt von der Kamera zum Viewing-Client, der Spotter für Windows-Anwendung.

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

Vom Server zum Client streamen



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.

oben Vorherige Nächste

1.12.1. Unterstützte Kameras

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.

oben Vorherige Nächste

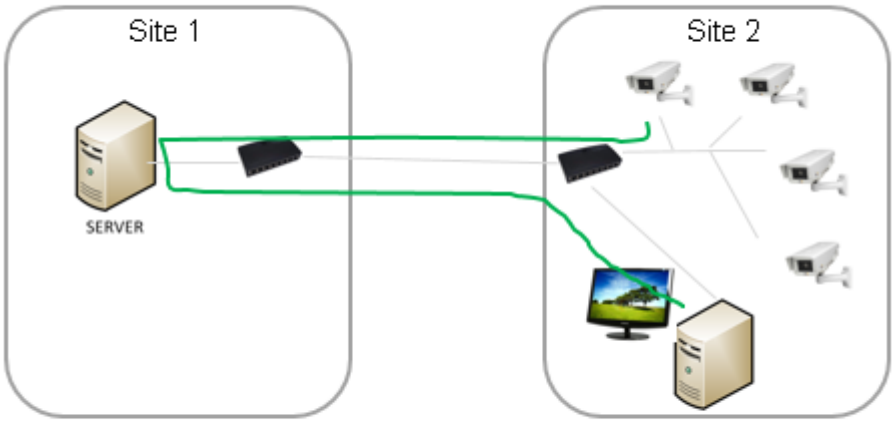
1.12.2. Netzwerkoptimierung

Netzwerkoptimierung

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

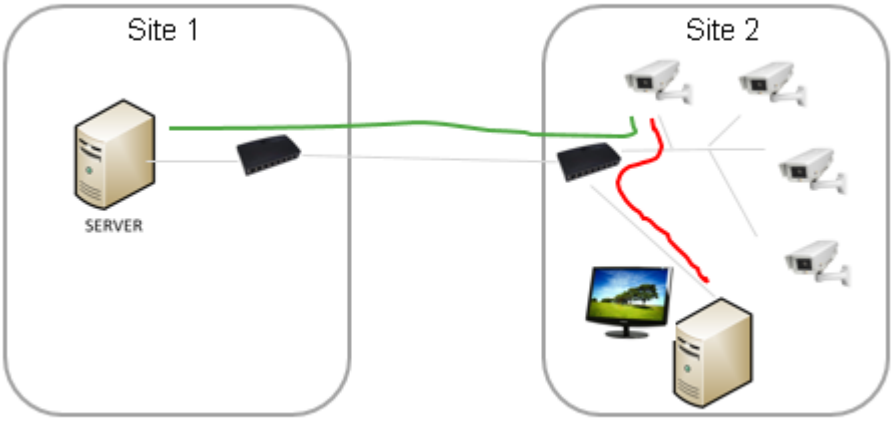
Die Lastreduzierung erfolgt hauptsächlich, wenn sich der Server außerhalb des Standorts (remote) und der Viewing-Client vor Ort (lokal zu den Kameras) befindet.

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.

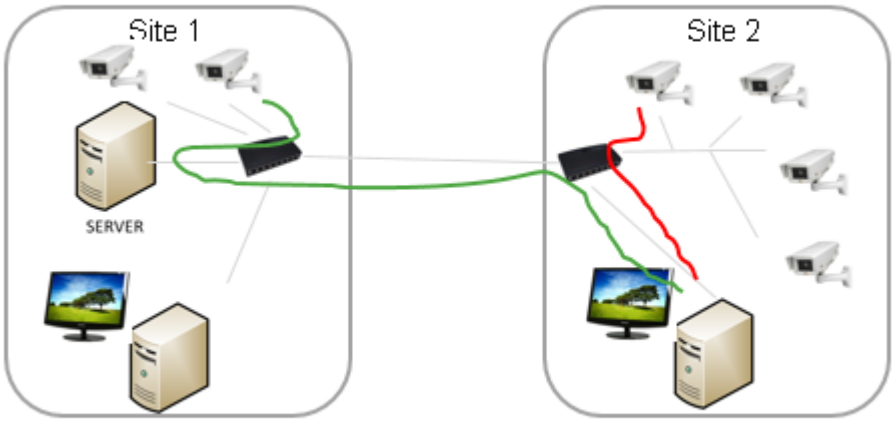
Wenn der Stream mit TruCast direkt von der Kamera konsumiert wird, wird der Verkehr zwischen den beiden Standorten reduziert.



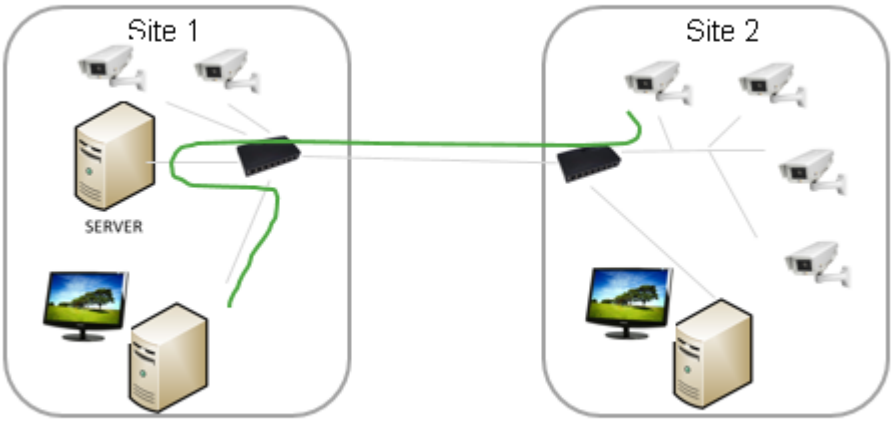
In Beispielszenario 2 befinden sich Kameras an zwei Standorten und anzeigende Clients an zwei Standorten.

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.

oben Vorherige Nächste

1.12.3. 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.

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.

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.

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.

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.

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.

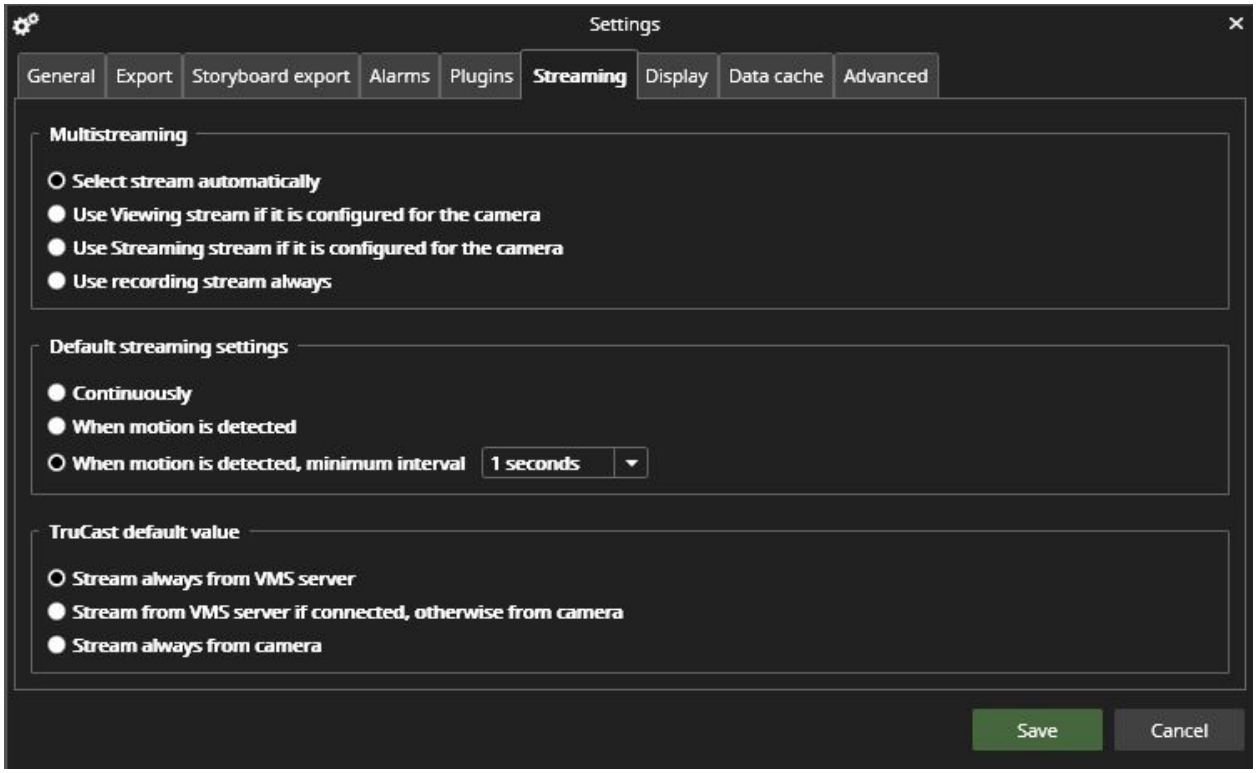
Bitte beachten Sie, dass nur die Kameras, deren Client-Treiber installiert wurde, als TruCast aktiviert angezeigt werden.

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.



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

oben Vorherige Nächste

1.12.4. Verwenden von TruCast

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.

oben Vorherige Nächste

1.13. 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.

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.

oben Vorherige Nächste

1.13.1. Mindestanforderungen

Mindestanforderungen

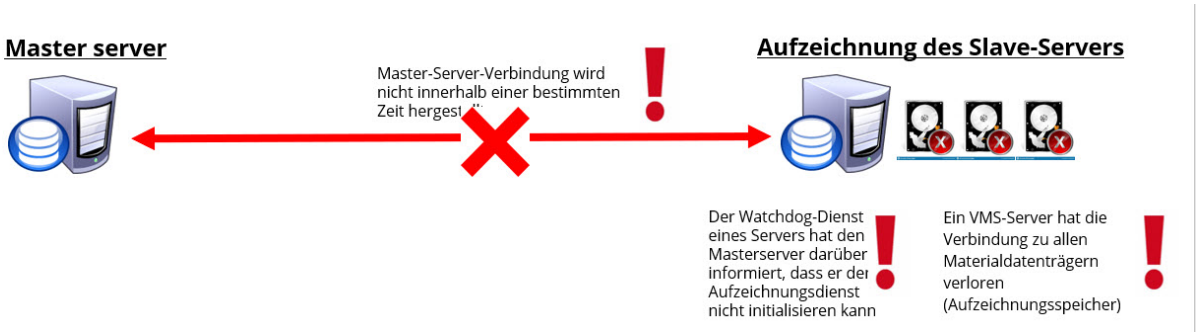
- **Master-Server auf separatem PC installiert**
  - Die Lizenz muss eine automatische Sicherungsfunktion enthalten
  - Die Lizenz muss einen oder mehrere Failover-Server enthalten
- **1 Slave-Server für Aufzeichnung**

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

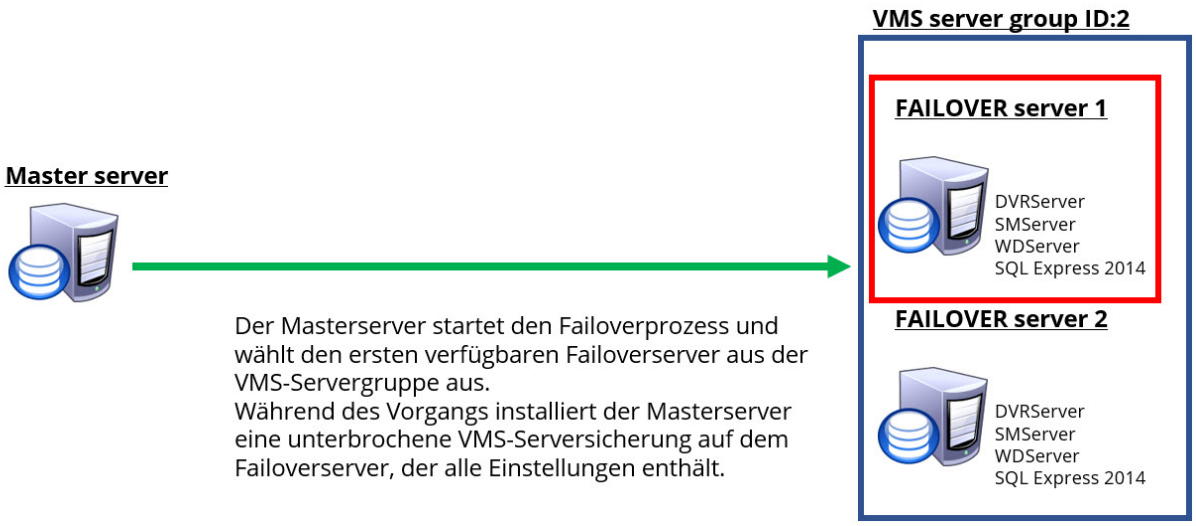
oben Vorherige Nächste

1.13.2. FAILOVER-Auslösebedingungen



oben Vorherige Nächste

1.13.3. FAILOVER-Prozess

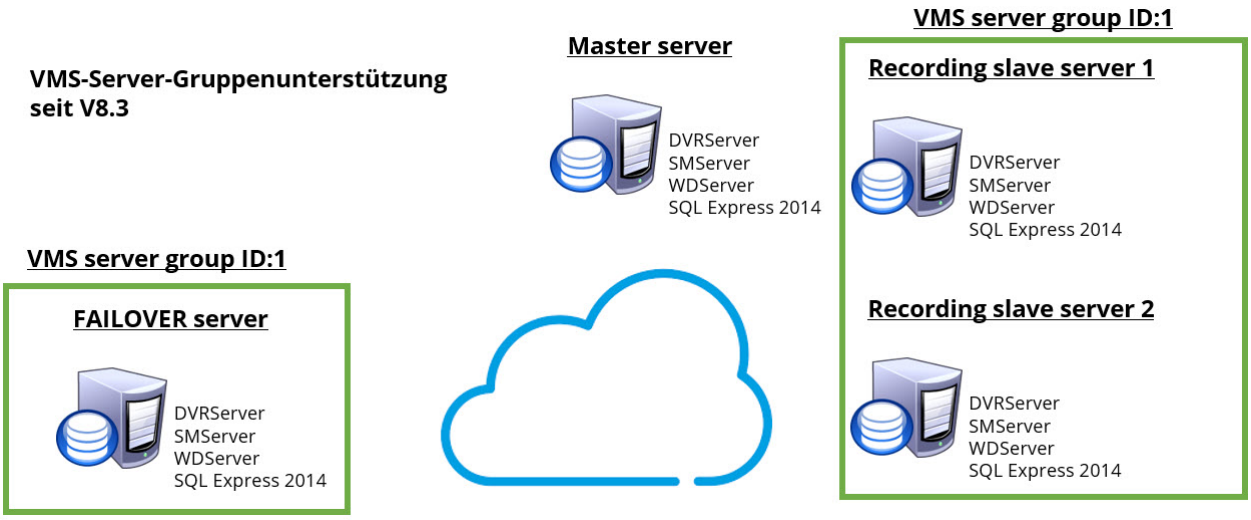


oben Vorherige Nächste

1.13.4. MINDESTENSZENARIO FÜR FAILOVER

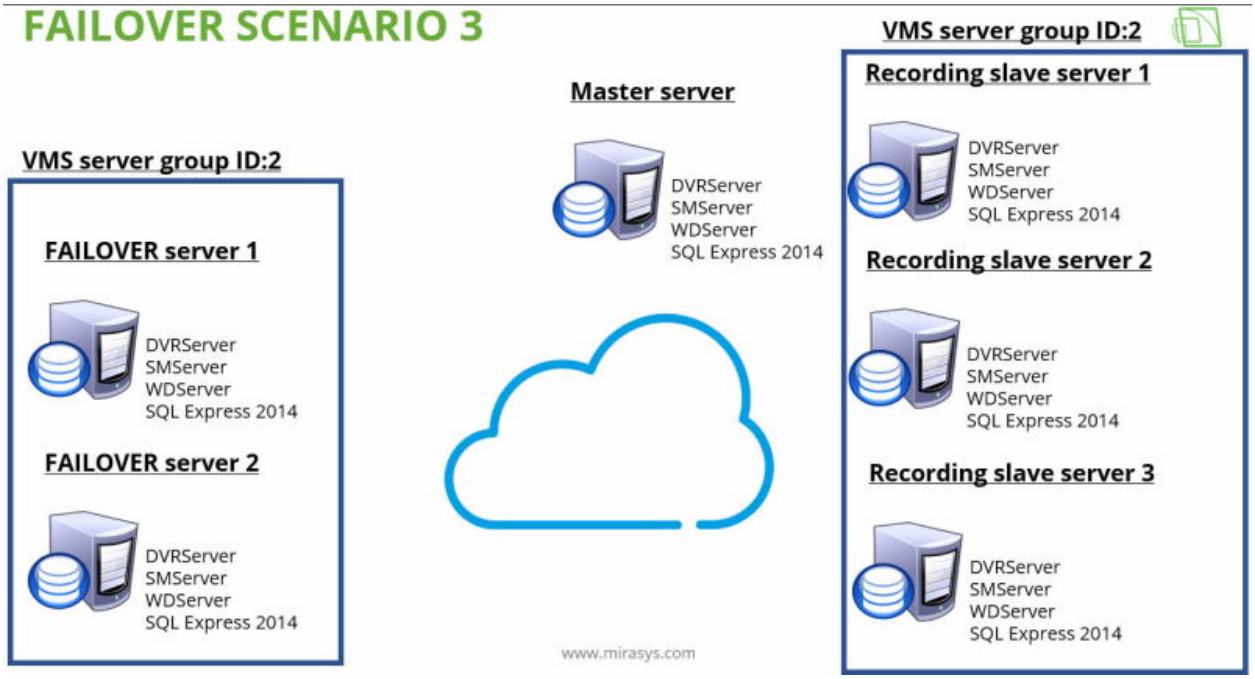
oben Vorherige Nächste

1.13.5. FAILOVER-SZENARIO 2



oben Vorherige Nächste

1.13.6. FAILOVER-SZENARIO 3



oben Vorherige Nächste

1.13.7. VMS-Serverrollen

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.

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.

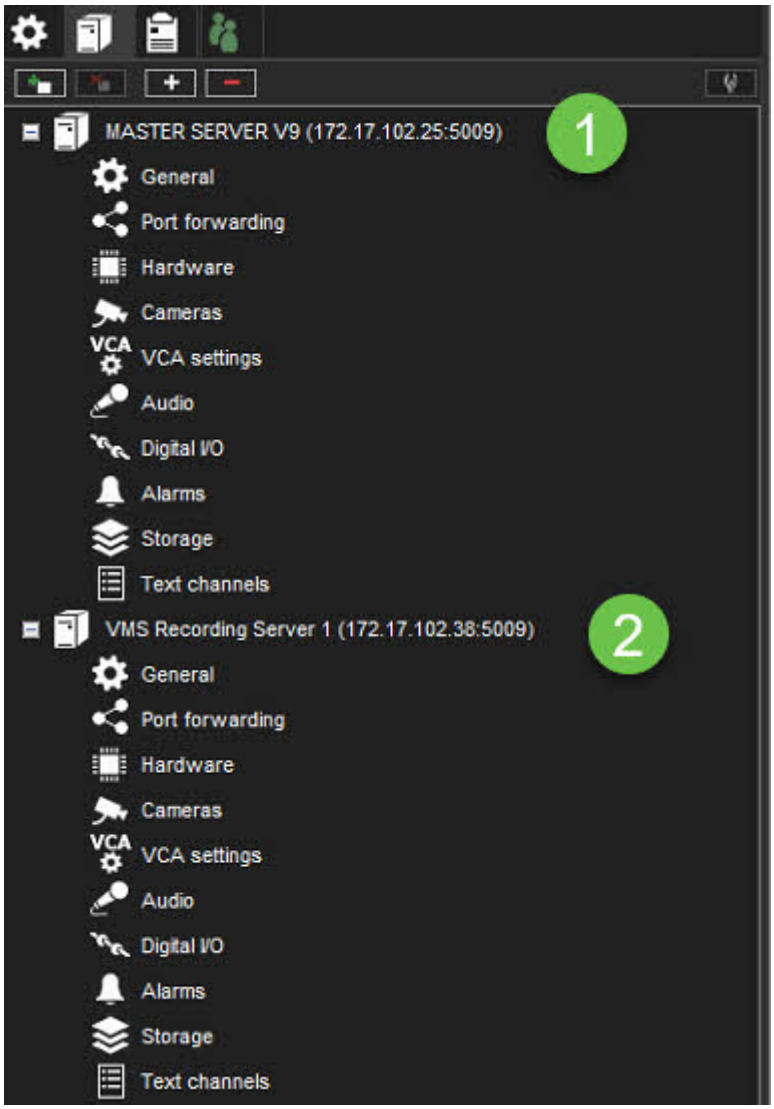
Um einen defekten Server, der durch einen Failover-Server ersetzt wurde, wieder ins System zu bekommen, muss dieser zunächst manuell entfernt und anschließend als neuer Server wieder hinzugefügt werden.

oben Vorherige Nächste

1.13.8. Aufbau eines Failover-Systems

Starting point

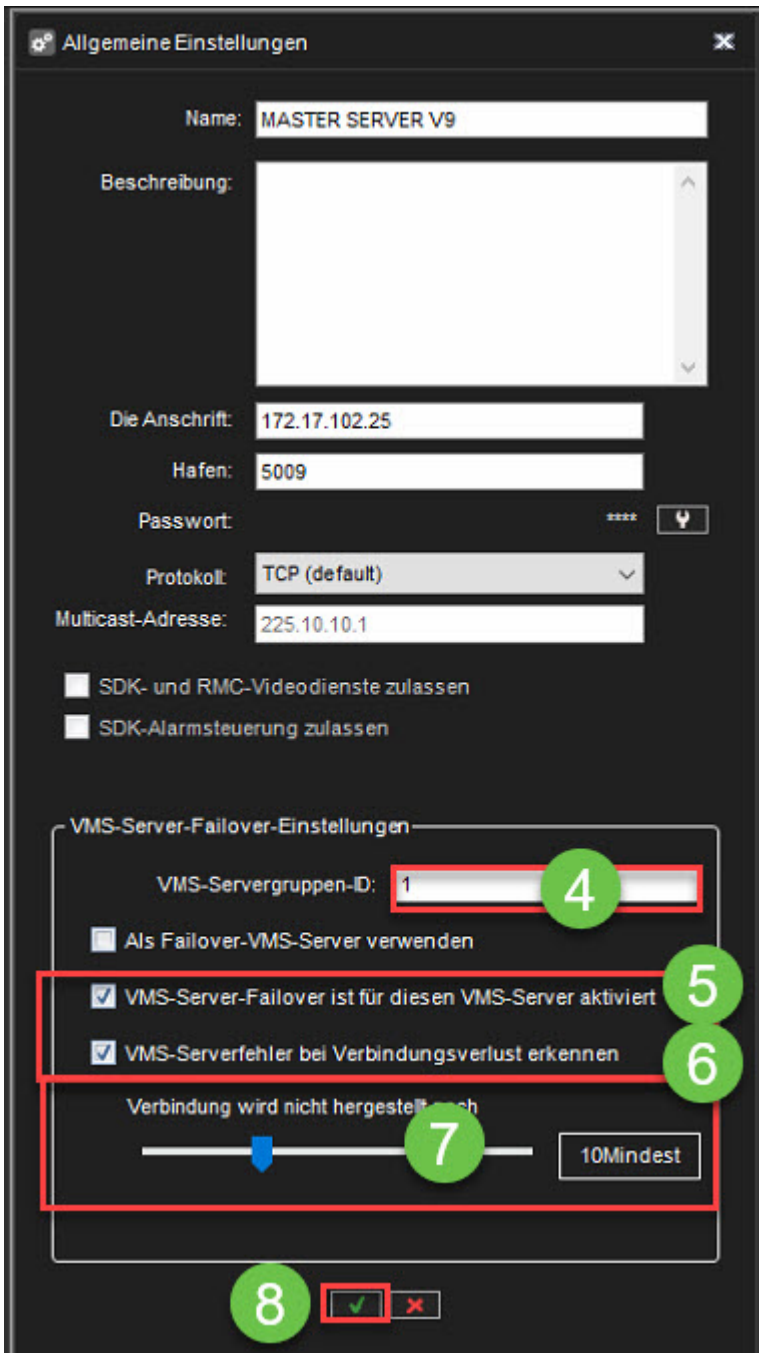
Der Master-Server und 1 Aufzeichnungs-Slave-Server wurden dem System hinzugefügt



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**

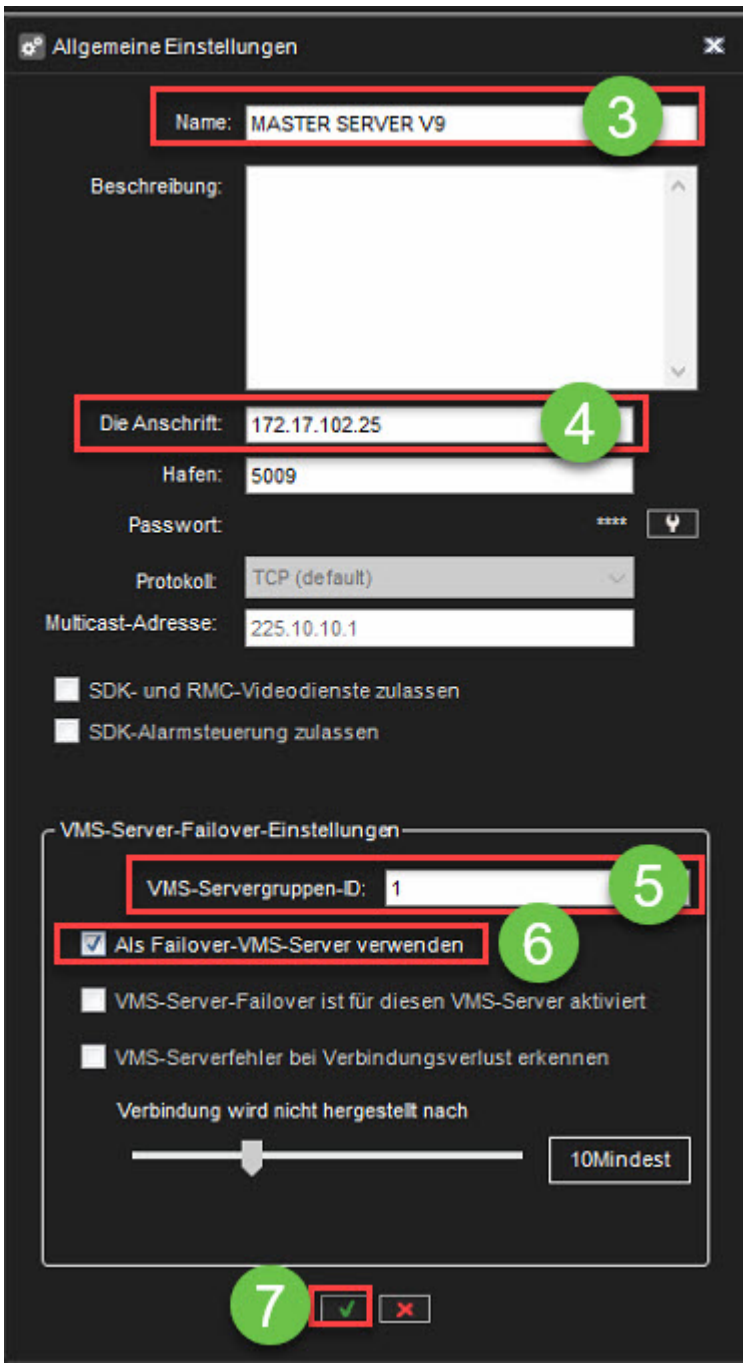
4. Definieren Sie **VMS-Servergruppen-ID (Standard 1)**
5. Aktivieren **VMS-Server-Failover ist für diesen VMS-Server aktiviert**
6. Aktivieren Sie **Erkennen von VMS-Serverfehlern bei Verbindungsverlust**
7. **Definieren Sie den Wert Verbindung wird nicht aufgebaut nach**
8. Klicken **OK**



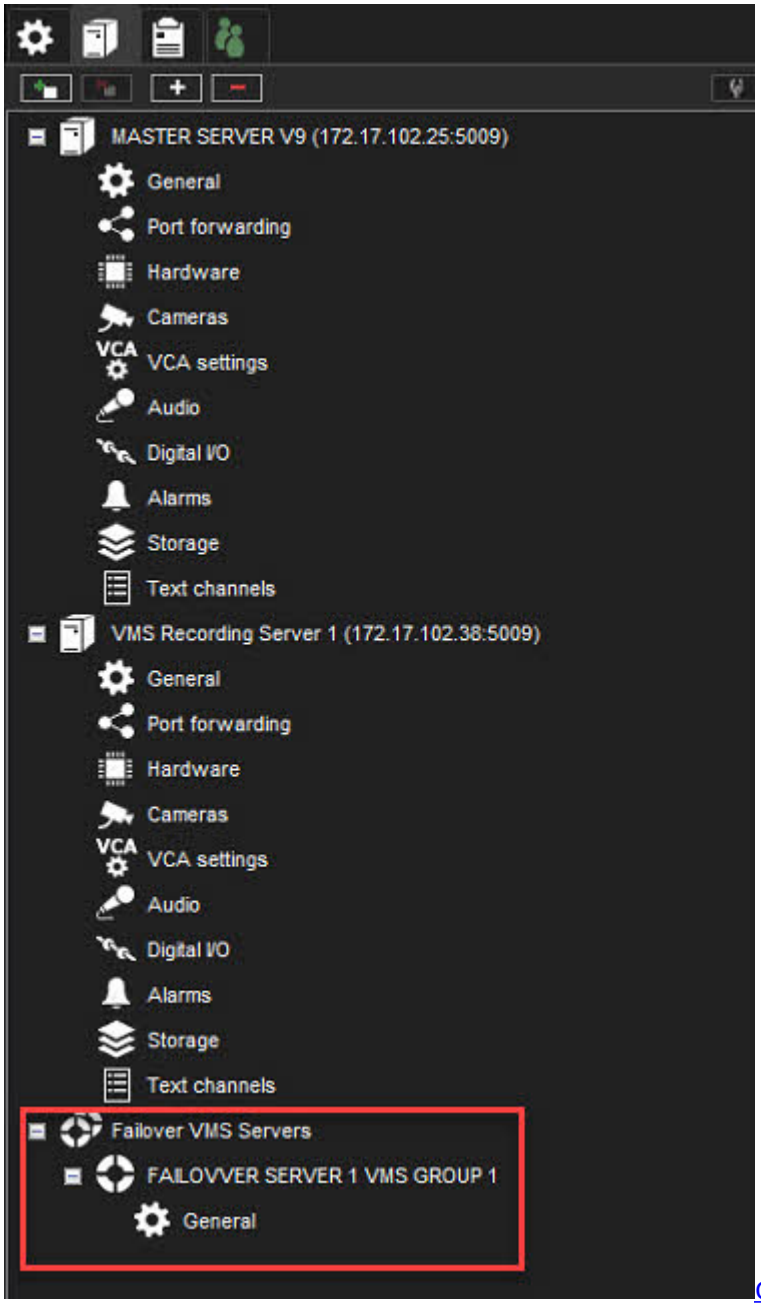
FAILOVER-Server hinzufügen

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



oben Vorherige Nächste

1.13.9. 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.

oben Vorherige Nächste

1.14. Easy LPR

EASY LPR ist eine kamerabasierte LPR-Erkennung. Unterstützte Kameras sind:

- Hikvision 7-series LPR cameras
- Axis cameras, which support Vaxtor VaxALPR, version 2.2-20 and AXIS License Plate Verifier version 2.1-0
- Dahua ITC215-PW6M-IRLZF, firmware 2.625

❗

Bitte prüfen Sie, ob Ihr Mirasys VMS mindestens über diese Treiberversionen verfügt:

- **AxisIPCapture64bit_v2.8.1.0**
- **Dahua IP Capture driver 1.3.1.0 (64bit)**
- **EHIIPCapture64bit_v2.1.4.0**

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

oben Vorherige Nächste

1.14.1. Konfigurationsprozess

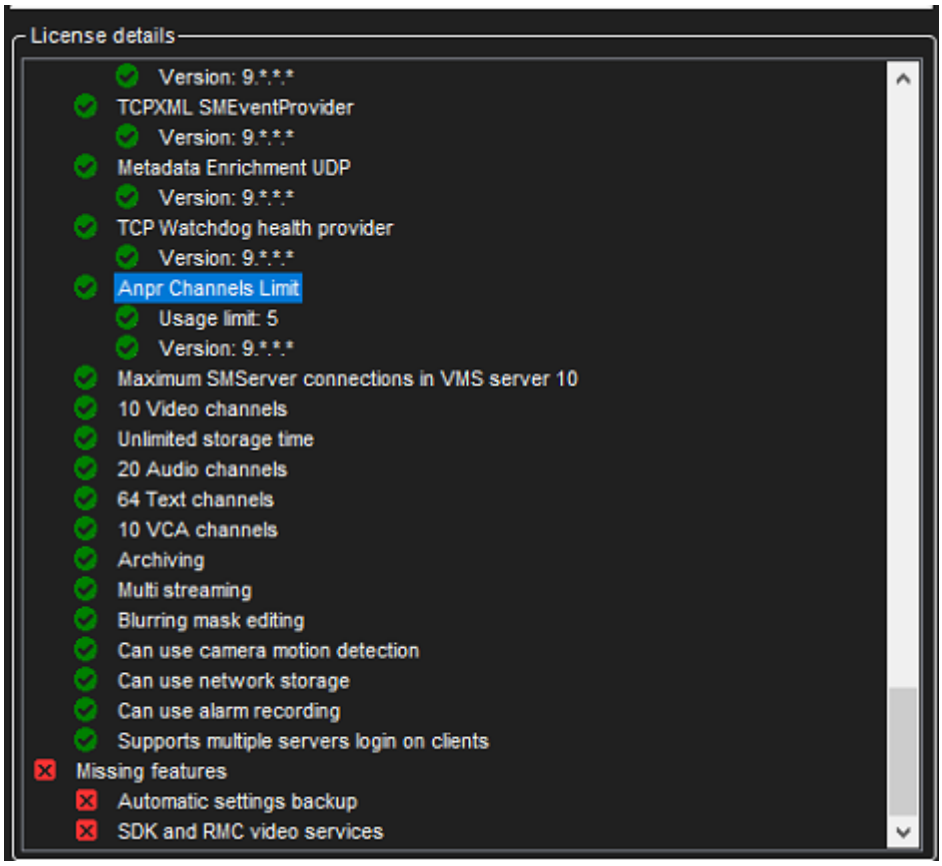
1. Konfigurieren Sie die LPR-Funktionalität für die verwendeten Kameras. Weitere Informationen finden Sie auf der Website des Herstellers
2. Kameras zum Mirasys VMS hinzufügen
3. Überprüfen Sie, ob die Mirasys VMS-Lizenz LPR-Kameras unterstützt
4. Einfaches Easy LPR aktivieren

oben Vorherige Nächste

1.14.2. 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**

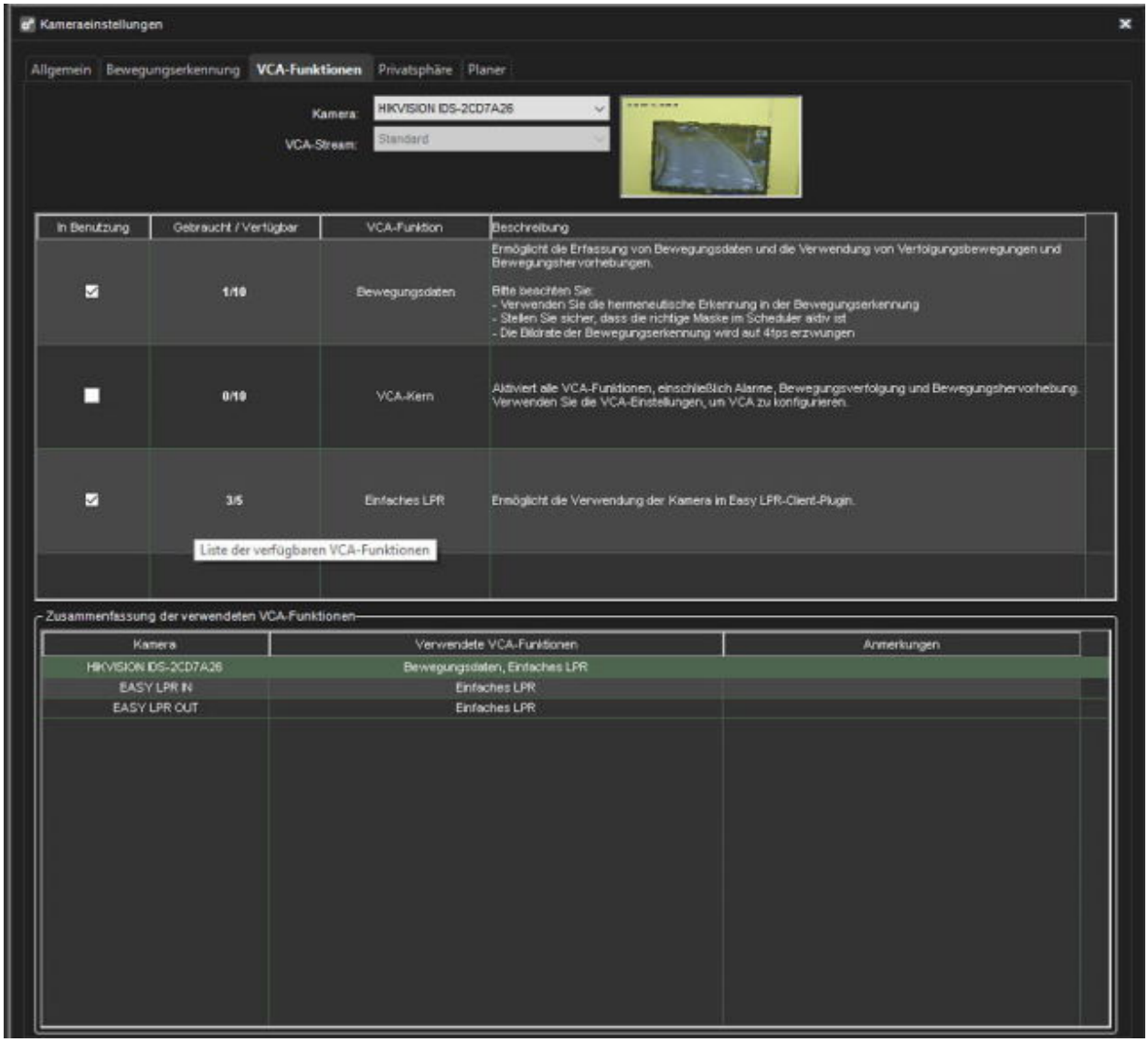


oben Vorherige Nächste

1.14.3. 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**

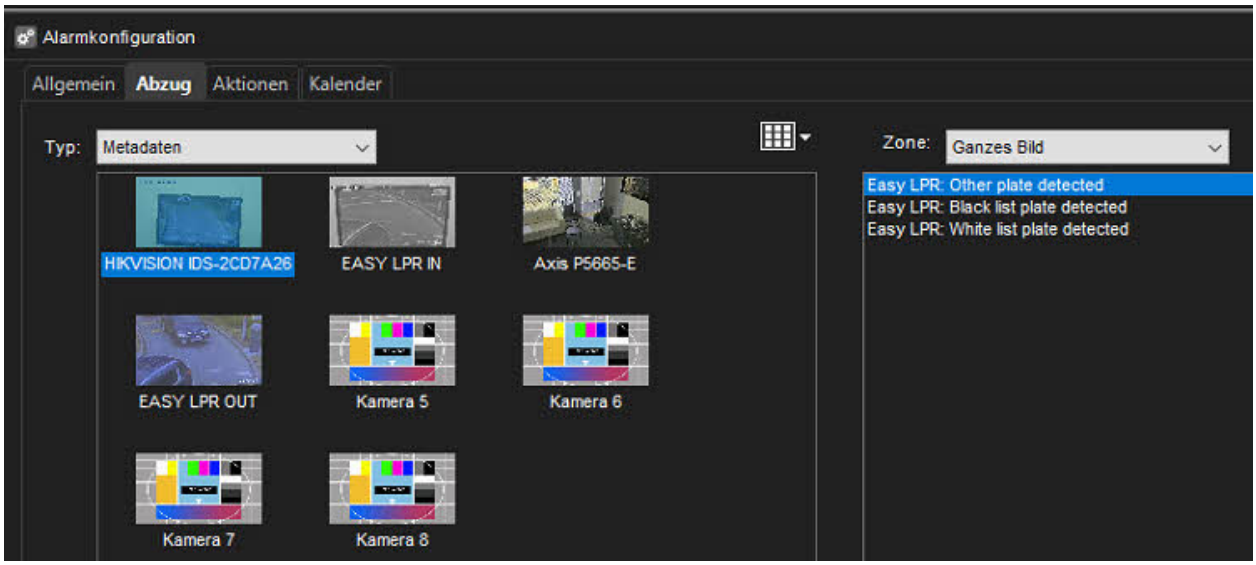


oben Vorherige Nächste

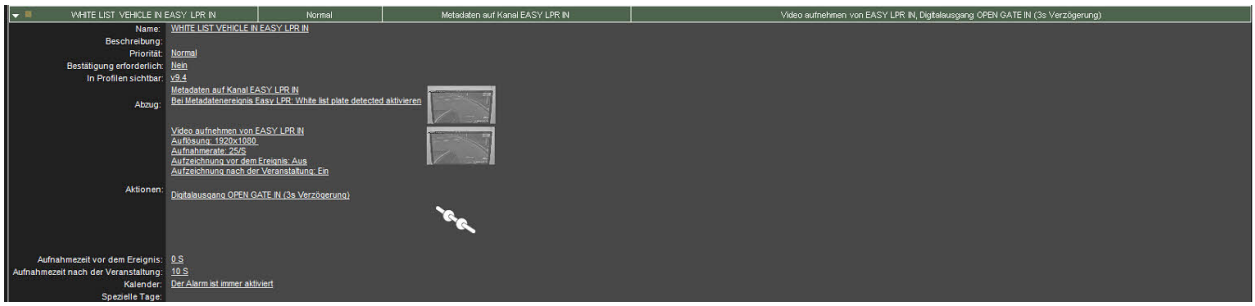
1.14.4. Erstellen eines Alarms aus einem Easy LPR-Ereignis

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:
    d. **Easy LPR: Andere Platte erkannt**
    e. **Easy LPR: Schwarzes Listenschild erkannt**
    f. **Easy LPR: Weiße Liste-Kennzeichen erkannt**



8. Geben Sie die Aktionen der Alarme ein
9. Kalender einstellen
10. Überprüfen Sie die Gesamtansicht des Alarms
11. Klicken Sie auf **OK** um eine Alarmerstellung zu bestätigen



oben Vorherige