Dallmeier

Dok.-Rev.: 0.3.4 | 2023-04-21



KONFIGURATION

# KAMERA-WEBINTERFACE

# DOMERA® OS

RELEASE-VERSION: 14.0.3.9

MADE IN GERMANY

See more.

# INHALT

# EINFÜHRUNG

## 1.1 GÜLTIGKEIT

Dieses Dokument ist gültig für Domera® OS in Verbindung mit folgenden Dallmeier Kameras:

| Dome-Kameras | Fisheye-Kamera | Panomera® (MK2-Modelle) |
|---|---|---|
| • RDF6800DN<br>• RDF6400DN<br>• RDF5140DN + Version E<br>• RDF5120DN + Version E | • SDF6800DN | • Panomera® S4/S8 (MK2)<br>• Panomera® W4/W8 (MK2) |

Tabelle 1-1

Zur Vereinfachung wird im Folgenden die Bezeichnung „Gerät“ oder „Kamera“ verwendet.
An Stellen, an denen zwischen den einzelnen Geräten unterschieden werden muss, werden hingegen die kompletten Produktbezeichnungen genannt.

Die Ausführungen in diesem Dokument basieren auf Domera® OS mit der Release-Version 14.0.3.9.

Abbildungen (z. B. Screenshots) in diesem Dokument können vom tatsächlichen Produkt abweichen.

## 1.2 KOMPATIBILITÄT

Die Release-Version 14.0.3.9 von Domera® OS ist mit folgender Dallmeier Hardware und Software kompatibel:

- Aufzeichnungssysteme der Generation 5 mit **SMAVIA Recording Server** Software ab Version 8.x.12* (Einschränkungen: keine Unterstützung für die Aufzeichnung von H.265-kodiertem Videomaterial sowie keine Möglichkeit einer gesicherten Verbindung und Datenübertragung mit TLS-Verschlüsselung)
- Aufzeichnungssysteme der Generation 6 mit **SMAVIA Recording Server** Software ab Version 9.x.12*
- Aufzeichnungssysteme mit **SeMSy® Recording Server** Software ab Version 10.x.3*
- **HEMISPHERE® SeMSy®** Video- und Alarm-Management-System ab Version 5.4.21
- **SeMSy® Compact** Video-Management-Software ab Version 5.3.42 für kleine und mittlere Unternehmen
- **SeMSy® Viewer** ab Software-Version 5.3.42 zur Wiedergabe und Auswertung von Backups
- **Dallmeier Device Manager** ab Software-Version 1.0.22 zur Erkennung und sicheren Verwaltung von Dallmeier VideoIP-Systemen (Kameras, Aufzeichnungssysteme etc.) im Netzwerk
- **PGuard advance** ab Software-Version 4.7.2 zur Auswertung und Verwaltung von Status-, Ereignis- und Fehlermeldungen von Dallmeier Geräten

* jeweils mit aktuellstem Service Pack

Dallmeier Kameras mit Domera® OS können zudem in ONVIF*)-konforme Video-Management-Systeme von Drittherstellern integriert werden, die die Funktionen des ONVIF Profile M, ONVIF Profile S und ONVIF Profile T sowie das Real-Time Streaming Protocol (RTSP) unterstützen.

*) Beachten Sie die Angaben zum Rechteinhaber der Marke im Copyright- und Markenhinweis auf Seite 2.

## 1.3 DOKUMENTE

Die Produktdokumentation zum jeweiligen Gerät umfasst verschiedene Dokumente, die gedruckt und/oder in digitaler Form, beispielsweise auf der Dallmeier Webseite unter https://www.dallmeier.com/, bereitgestellt werden.

Lesen Sie die gesamte Produktdokumentation zu Ihrem Gerät sorgfältig und vollständig, bevor Sie das Gerät verwenden. Beachten Sie immer die enthaltenen Anweisungen, Hinweise und Warnungen sowie die technischen Daten in der aktuell gültigen Produktspezifikation.

Bewahren Sie alle gedruckten Dokumente zu Ihrem Gerät in einem gut lesbaren Zustand und an einem geeigneten Ort auf, um ein späteres Nachschlagen zu ermöglichen. Archivieren Sie digitale Dokumente zu Ihrem Gerät (z. B. die technische Produktspezifikation) auf einem geeigneten Speichermedium.

Prüfen Sie regelmäßig die Dallmeier Webseite unter https://www.dallmeier.com/ auf mögliche Aktualisierungen der Produktdokumentation sowie auf die aktuellste Release-Version von Domera® OS (v. a. in Bezug auf Sicherheitsupdates oder -patches).

### 1.3.1 Dieses Dokument

Dieses Dokument enthält detaillierte Beschreibungen zur Konfiguration der oben aufgeführten Geräte über die webbasierte grafische Benutzeroberfläche (Graphical User Interface – GUI).
Zielgruppe dieses Dokuments ist geschultes Fachpersonal für Systemintegration (Planung und Errichtung von Videosicherheitssystemen).

### 1.3.2 Mitgeltende Dokumente

**Produktspezifikation**
Die Produktspezifikation enthält detaillierte technische Daten, Eigenschaften und Leistungsmerkmale des jeweiligen Geräts.
Zielgruppe des Dokuments ist geschultes Fachpersonal für Systemintegration (Planung und Errichtung von Videosicherheitssystemen).

**Inbetriebnahme**
Das Dokument „Inbetriebnahme“ enthält ausführliche Informationen zur fachgerechten Aufstellung, Montage, Installation, Verkabelung, Inbetriebnahme und bestimmungsgemäßen Verwendung des jeweiligen Geräts sowie Sicherheits- und Gefahrenhinweise, allgemeine technische Hinweise und Angaben zur Wartung, Prüfung und Reinigung.
Zielgruppe des Dokuments ist geschultes Fachpersonal für Systemintegration (Planung und Errichtung von Videosicherheitssystemen).

**Technische Mitteilungen**
Eine „Technische Mitteilung“ zu Domera® OS informiert über aktuelle Änderungen (Sicherheitsupdates oder -patches, Funktionserweiterungen und -verbesserungen sowie neue Features), die mit der jeweils neuesten Release-Version implementiert werden.
Zielgruppe dieser Dokumente ist geschultes Fachpersonal für Systemintegration (Planung und Errichtung von Videosicherheitssystemen).

## 1.4 DARSTELLUNGSKONVENTIONEN

Zur Verbesserung der Übersichtlichkeit und Lesbarkeit dieses Dokuments werden verschiedene Textformatierungen und Hervorhebungen verwendet:

*ACHTUNG*

*ACHTUNG* kennzeichnet Maßnahmen zur Vermeidung von Geräte- und/oder Sachschäden durch unsachgemäße Konfiguration des Geräts oder fehlerhafte Bedienung.

Handlungsanweisungen sind durch Pfeile (►) gekennzeichnet.

► Führen Sie Handlungsanweisungen stets in der beschriebenen Reihenfolge aus.

**Ausdrücke**, die fett und dunkelgrau hervorgehoben sind, beziehen sich in der Regel auf den Namen einer Anwendung, eines Produkts oder einer Funktion oder weisen auf ein Bedienelement der webbasierten grafischen Benutzeroberfläche hin (Checkbox, Drop-down-Liste, Menüpunkt, Schaltfläche etc.).

*Kursiv formatierte Absätze bieten Informationen zu Grundlagen, Besonderheiten und effizienter Vorgehensweise sowie allgemeine Empfehlungen.*

## 1.5 DISCLAIMER

Die vorliegende Dokumentation umfasst den vollen Funktionsumfang von Domera® OS.

Beachten Sie jedoch, dass

- bestimmte Funktionen und Einstellungsmöglichkeiten nur in Verbindung mit dem jeweils geeigneten Gerät zur Verfügung stehen (z. B. die Konfiguration einer integrierten IR-Beleuchtung).
- sich der Funktionsumfang Ihres Geräts immer nach der bestellten Ausstattung oder Gerätevariante richtet und vom Inhalt dieser Dokumentation abweichen kann.
- bestimmte Funktionen und Einstellungsmöglichkeiten den Erwerb einer kostenpflichtige Lizenz erfordern können.

## 1.6 RECHTLICHE HINWEISE

Beachten Sie die unten aufgeführten rechtlichen Hinweise zu dem in diesem Dokument beschriebenen Produkt bzw. der zugrunde liegenden Software:

- Dieses Produkt enthält Software, die vom OpenSSL Project für die Verwendung im OpenSSL Toolkit entwickelt wurde (http://www.openssl.org/).
- Dieses Produkt enthält von Eric Young (eay@cryptsoft.com) geschriebene kryptografische Software.
- Dieses Produkt enthält von Tim Hudson (tjh@cryptsoft.com) geschriebene Software.
- Teile dieser Software basieren auf der Arbeit der Independent JPEG Group.

Lesen und beachten Sie in diesem Zusammenhang auch die im Info-Dialog Ihres Geräts bereitgestellten Lizenztexte zu sonstigen auf Ihrem Gerät verwendeten Third-Party-Softwarekomponenten.

# VERBINDUNG & LOGIN

Die Konfiguration der Kamera erfolgt mithilfe eines gängigen Webbrowsers auf einem stationären oder mobilen Computer (Desktop-PC oder Notebook) über das lokale Netzwerk (Local Area Network – LAN).

*Alternativ können Sie die Kamera auch über ein Ethernet-Crossover-Kabel direkt mit Ihrem Desktop-PC oder Notebook verbinden und anschließend konfigurieren. Wenn Sie in diesem Fall die Kamera jedoch mit Power-over-Ethernet (PoE) betreiben wollen, ist zusätzlich ein geeigneter Single-Port-PoE-Injektor erforderlich.*

## 2.1 SYSTEMVORAUSSETZUNGEN

Die Konfiguration der Kamera stellt keine besonderen Anforderungen an die Hardware oder Software des verwendeten Client-PCs. Sie kann mit jedem modernen Desktop-PC oder Notebook durchgeführt werden. Die webbasierte grafische Benutzeroberfläche (GUI) und die integrierten Funktionen von Domera® OS sind hinsichtlich der Kamerakonfiguration unabhängig von Betriebssystem und Art des Webbrowsers. Der Download und die Installation von Browsererweiterungen bzw. Plug-ins ist nicht erforderlich.

| SYSTEMVORAUSSETZUNGEN | |
|---|---|
| **Betriebssystem (OS)** | Jedes moderne und auf dem neuesten Stand gehaltene Betriebssystem, wie beispielsweise:<br>• Linux*)<br>• macOS*)<br>• Microsoft*) Windows*) 10 oder Windows 11 |
| **Webbrowser** | Jeder moderne Desktop-Browser in seiner aktuellsten Version, wie beispielsweise:<br>• Apple*) Safari*)<br>• Google*) Chrome*)<br>• Microsoft Edge*)<br>• Mozilla*) Firefox*) |
| **Browsereinstellungen** | JavaScript*) aktiviert |
| **Browsererweiterungen/Plug-ins** | Nicht benötigt |
| **Ethernet** | 100 Mbit/s (oder mehr) |
| **Grafikkarte** | Beliebig (mit moderner Technologie) |
| **Sound** | Soundkarte oder Onboard-Soundchip (min. 16 Bit) |

Tabelle 2-1

*) Beachten Sie die Angaben zum Rechteinhaber der Marke im Copyright- und Markenhinweis auf Seite 2.

*Für eine optimale und effiziente Bedienbarkeit der webbasierten grafischen Benutzeroberfläche ist eine Computermaus mit linker und rechter Maustaste sowie einem Mausrad empfohlen.*
*Zur besseren Lesbarkeit beziehen sich die Beschreibungen in diesem Dokument hinsichtlich der Verwendung einer Computermaus nur auf Personen, die rechtshändig sind (primäre Maustaste links).*

## 2.2 VERBINDUNG HERSTELLEN

**STANDARD-IP-ADRESSE**

Die ab Werk standardmäßig eingestellte IP-Adresse einer Dallmeier Single-Sensor-Kamera ist:

`192.168.2.28`

*Die IP-Adresse, Subnetzmaske und Gateway-Adressierung des Geräts können Sie mithilfe der Client-Software **Dallmeier Device Manager** ändern.*

Um eine Verbindung zu Ihrem Gerät über einen Webbrowser herzustellen, gehen Sie wie folgt vor:

- Stellen Sie zunächst sicher, dass Ihr Client-PC und Webbrowser eine Verbindung zum Gerät über das Ethernet herstellen kann (kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung).
- Starten Sie den Webbrowser.
- Geben Sie die IP-Adresse Ihres Dallmeier Geräts in die Adresszeile des Webbrowsers ein.
- Bestätigen Sie die Eingabe.

Die Verbindung zum Gerät wird daraufhin hergestellt.

Nach erfolgreicher Verbindung zum Gerät wird aus Gründen der Systemsicherheit vor dem ersten Login ein Dialog für die Erstanmeldung angezeigt (siehe im Folgenden).

## 2.3 ERSTANMELDUNG

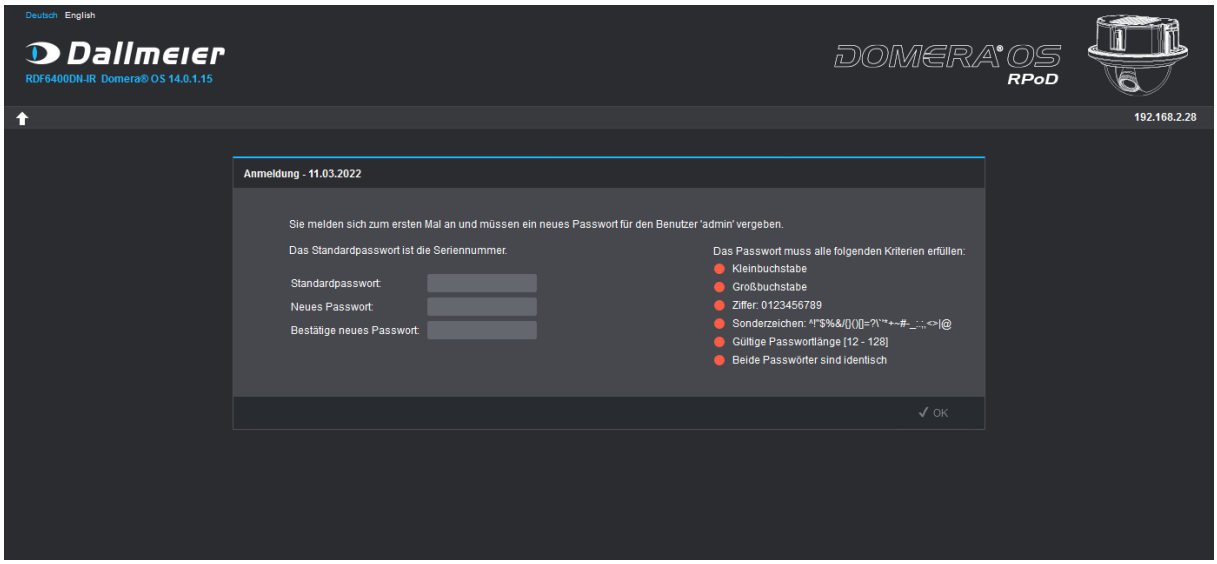


Abb. 2-1: Dialog für Erstanmeldung

> *Die Sprache der webbasierten grafischen Benutzeroberfläche kann ohne vorherige Anmeldung am Gerät in der oberen linken Ecke der Bildschirmanzeige geändert werden.*

Vor der erstmaligen Anmeldung am Gerät über einen Webbrowser müssen Sie zunächst das speziell für Ihr Gerät gültige Standardpasswort eingeben und dann ein neues Passwort für das ab Werk angelegte Administrationskonto (Benutzername: `admin`) vergeben.

Das Standardpasswort ist die vollständige Seriennummer Ihres Geräts (z. B. DHD001-23456789). Die Seriennummer befindet sich auf dem Typenschild des Geräts und lässt sich zudem mithilfe der Client-Software **Dallmeier Device Manager** ermitteln.

- ▶ Geben Sie das **Standardpasswort** (vollständige Seriennummer Ihres Geräts inkl. Bindestrich) ein.
- ▶ Geben Sie ein neues Passwort für das Standard-Administrationskonto ein (Passwortkriterien beachten) und bestätigen Sie Ihre Eingabe (die Stärke des gewählten Passworts wird bei der Eingabe angezeigt).
- ▶ Klicken Sie **OK**.

*ACHTUNG*

**Fehler bei der Anmeldung am Gerät durch falsche Eingabe von Zugangsdaten oder Gefahr von Gerätezugriff und Missbrauch des Systems durch unberechtigte Dritte**

- Notieren Sie sich alle wichtigen Zugangsdaten (Benutzernamen und Passwörter) zu Ihrem Gerät und hinterlegen Sie diese an einem sicheren Ort.
- Schützen Sie Informationen zu Benutzerkonten unbedingt vor unberechtigtem Zugriff durch Dritte.

Nach erfolgreicher Erstanmeldung am Gerät wird der Login-Dialog angezeigt (siehe im Folgenden).

## 2.4 LOGIN (ANMELDUNG)

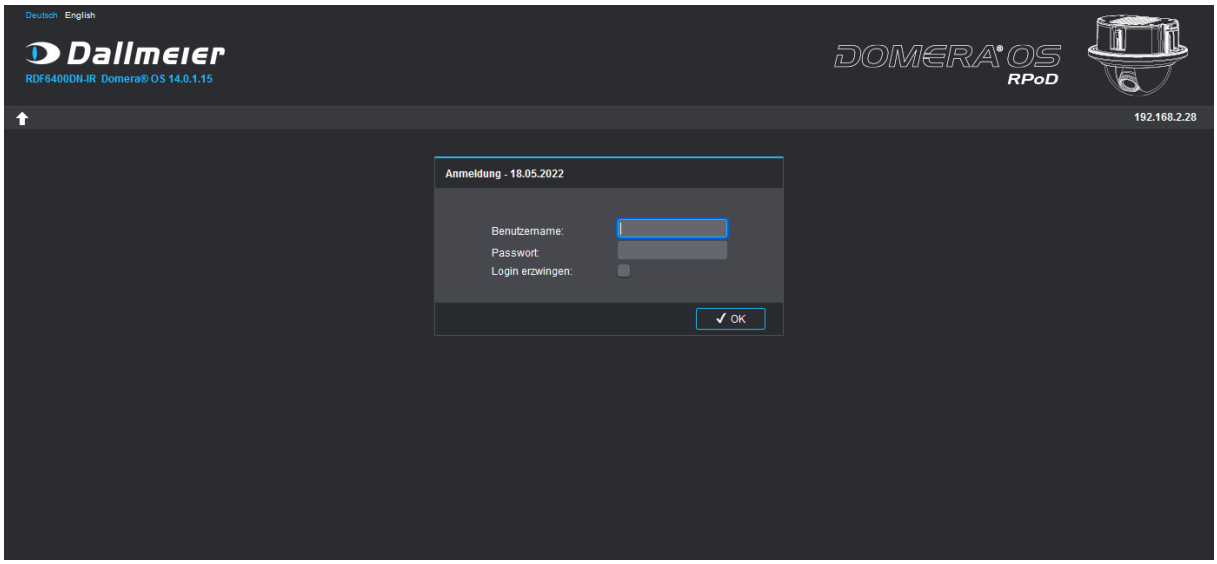


Abb. 2-2: Login-Dialog

> *Die Option **Login erzwingen** ermöglicht eine erfolgreiche Anmeldung am Gerät, auch wenn bereits ein anderer Benutzer (mit geringeren oder den gleichen Rechten) angemeldet ist.*

Die webbasierte grafische Benutzeroberfläche (Domera® OS GUI) des Konfigurations- und Live-Modus wird nur nach erfolgreicher Identifizierung als berechtigter Benutzer angezeigt.

| STANDARD-LOGIN-DATEN |
| --- |
| Der Benutzername des ab Werk angelegten Administrationskontos ist:<br><br>`admin` |

Um sich am Gerät anzumelden, fahren Sie wie folgt fort:

- Geben Sie die Zugangsdaten zu Ihrem Gerät in die Felder **Benutzername** und **Passwort** ein.
- Klicken Sie **OK**.

Nach erfolgreicher Anmeldung am Gerät wird die Benutzeroberfläche des Konfigurationsmodus angezeigt (siehe im Folgenden).

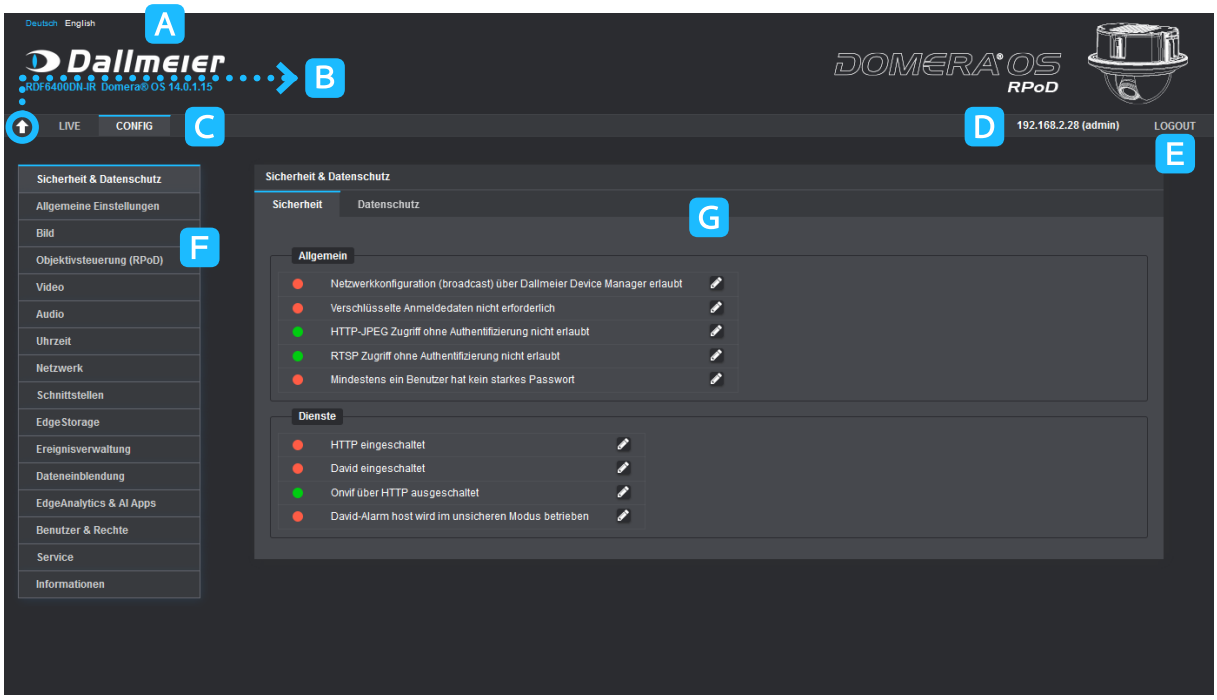


Abb. 2-3: Konfigurationsmodus

A Sprache ändern
B Titelleiste aus-/einblenden
C Umschalten zwischen Konfigurations- und Live-Modus
D IP-Adresse des Geräts und Benutzername des aktuell angemeldeten Benutzers
E Abmelden vom Gerät
F Navigationsmenü
G Bereich für Konfigurationsdialoge

- ► Konfigurieren Sie alle erforderlichen Einstellungen (siehe nachfolgende Kapitel).
- ► Klicken Sie abschließend **LOGOUT**, um sich vom Gerät korrekt abzumelden.

*Nach 5 Minuten ohne Benutzeraktion werden Sie aus Gründen der Systemsicherheit automatisch vom Gerät abgemeldet.*

# SICHERHEIT & DATENSCHUTZ

## 3.1 SICHERHEIT

Die Registerkarte **Sicherheit** ermöglicht eine schnelle Prüfung aller sicherheitsrelevanter Systemzustände. Somit können potenzielle Sicherheitslücken und kritische Schwachstellen, verursacht durch eine fehlerhafte oder unbedachte Geräte-Konfiguration, einfach ermittelt und behoben werden.
Um die erforderlichen Sicherheitsmaßnahmen in Bezug auf Cyber Security bzw. IT-Sicherheit frühestmöglich zu erkennen, wird die Übersichtsseite zur Systemsicherheit in der Regel unmittelbar nach jedem Login angezeigt.

> *Bei einem Gerätestatus-Fehler wird zunächst immer der entsprechende Fehler nach der Anmeldung auf dem Gerät angezeigt bis dieser behoben wurde – wie beispielsweise, wenn der eingetragene Zeitserver über eine längere Dauer hinweg nicht erreichbar ist.*

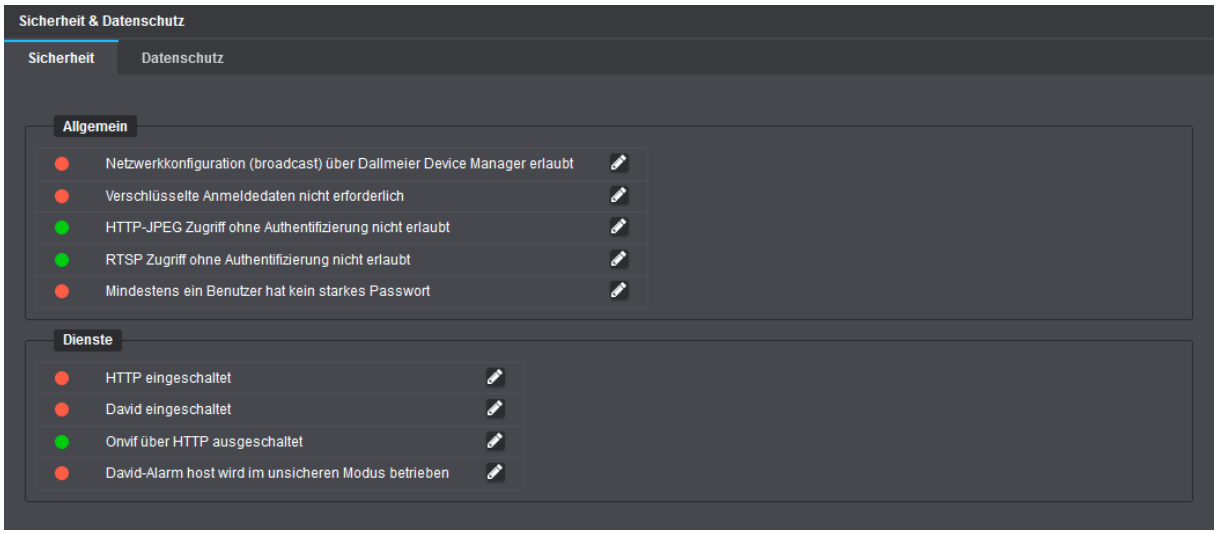


Abb. 3-1

## 3.2 DATENSCHUTZ

Die Registerkarte **Datenschutz** ermöglicht einen schnellen Zugriff auf alle datenschutzrelevanten Konfigurationsdialoge, welche die Privatsphäre und Benutzerrechte betreffen.

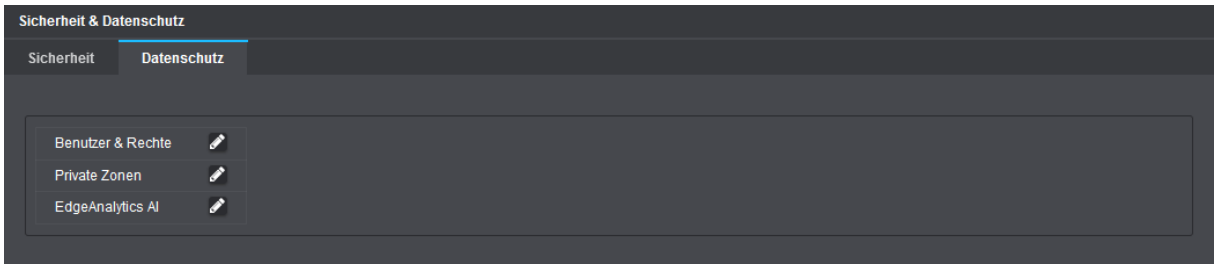


Abb. 3-2

- Klicken Sie auf das **Stift**-Symbol rechts neben der dazugehörigen Option, um den entsprechenden Konfigurationsdialog aufzurufen.

# ALLGEMEINE EINSTELLUNGEN (SPRACHE)

Die webbasierte grafische Benutzeroberfläche kann in verschiedenen Sprachen dargestellt werden.

Um die Sprache zu ändern, gehen Sie wie folgt vor:

► Klicken Sie im Navigationsmenü den Menüpunkt **Allgemeine Einstellungen**.

Die Registerkarte **Benutzeroberfläche** wird angezeigt.

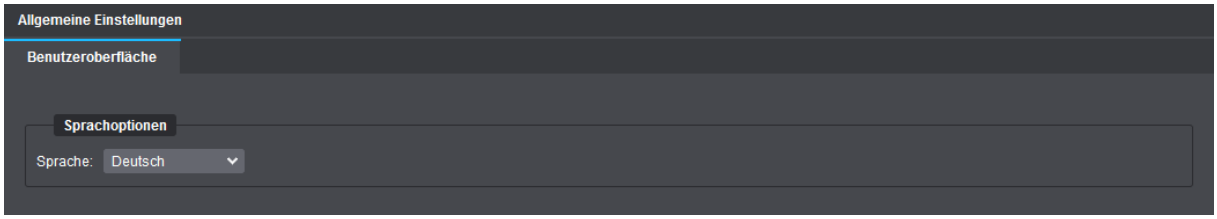


Abb. 4-1

► Wählen Sie aus der Drop-down-Liste **Sprache** die gewünschte Sprachoption.

Die Benutzeroberfläche wird daraufhin automatisch auf die gewählte Sprache umgestellt.

# BILD

Im Dialog **Bild** können der Bildaufnahmesensor konfiguriert und die Bildverarbeitungsalgorithmen an die lokale Aufnahmesituation bzw. die vorherrschenden Lichtverhältnisse der jeweiligen Szene angepasst werden. Zudem kann der automatische Tag/Nacht-Betrieb für eine optimale Belichtung sowohl bei Tag als auch in der Nacht konfiguriert werden.

- Klicken Sie im Navigationsmenü den Menüpunkt **Bild**, um den entsprechenden Dialog zu öffnen.
- Beachten Sie die nachfolgenden Erklärungen zu den verschiedenen Registerkarten und Einstellungen.

> *Sie können die im Dialog **Bild** vorgenommen Einstellungen jederzeit auf die Werkseinstellungen zurücksetzen, falls erforderlich (siehe Abschnitt „Werkseinstellungen“ auf Seite 138).*

## 5.1 VOREINSTELLUNGEN (PRESETS)

Die Registerkarte **Voreinstellungen** erlaubt die Einstellung verschiedener Belichtungsvoreinstellungen (AE Presets – Automatic Exposure Presets) für die Bilderfassung und für die Live-Vorschau auf den folgenden Registerkarten.

**Vordefinierte Presets**
Mithilfe von werkseitig vordefinierten Belichtungseinstellungen und Bildverarbeitungsalgorithmen (sogenannten Presets) kann die Kamera auf sehr einfache Weise an die meisten Lichtverhältnisse angepasst werden. So erhält man stets die bestmögliche Bildqualität. Darüber hinaus dienen Presets als nützliche Ausgangspunkte für die manuelle Feinabstimmung verschiedener Kameraparameter wie Belichtungszeit, Blende, Weißabgleich etc. Die Firmware verfügt über verschiedene Belichtungsvoreinstellungen, die für eine möglichst optimale Bilderfassung in verschiedenen Einsatzbereichen sorgen.

- **Casino (Tag)** – spezielles Preset für Szenen im Casino-Innenbereich mit hohem Kontrastumfang
- **Indoor (Tag/Nacht)** – für Szenen im Innenbereich mit mittlerem Kontrastumfang
- **Indoor HDR (Tag/Nacht)** – für Szenen im Innenbereich mit hohem Kontrastumfang
- **Low-light ICR an (Tag/Nacht)** – für Szenen mit schwacher Beleuchtung (Infrarot-Sperrfilter bleibt auch im Nachtmodus eingeschwenkt; nur für sehr spezielle Anwendungsfälle empfohlen)
- **Low-light (Tag/Nacht)** – für Szenen mit schwacher Beleuchtung
- **Outdoor (Tag/Nacht)** – für Szenen im Außenbereich mit mittlerem Kontrastumfang
- **Outdoor HDR (Tag/Nacht)** – für Szenen im Außenbereich mit hohem Kontrastumfang
- **SEDOR® Tag (Tag/Nacht)** – spezielles Preset für die SEDOR®-Videoanalyse-Software am Tag
- **SEDOR® Nacht (Tag/Nacht)** – spezielles Preset für die SEDOR®-Videoanalyse-Software bei Nacht
- **Universal (Tag/Nacht)** – für die meisten Szenen mit mittlerem Kontrastumfang geeignet
- **Universal HDR (Tag/Nacht)** – für die meisten Szenen mit hohem Kontrastumfang geeignet

**Benutzerdefinierte Presets erstellen**
Änderungen an Voreinstellungen gelten zunächst immer nur temporär (im Vorschaubild). Möchten Sie die vorgenommenen Änderungen dauerhaft übernehmen, müssen Sie diese deshalb zwingend als benutzerdefiniertes Preset speichern. Benutzerdefinierte Presets können dann beispielsweise für die **Presetautomatik** ausgewählt oder wiederum als Ausgangspunkte für weitere manuelle Anpassungen der Kameraparameter verwendet werden (erneutes Speichern oder Überschreiben erforderlich).

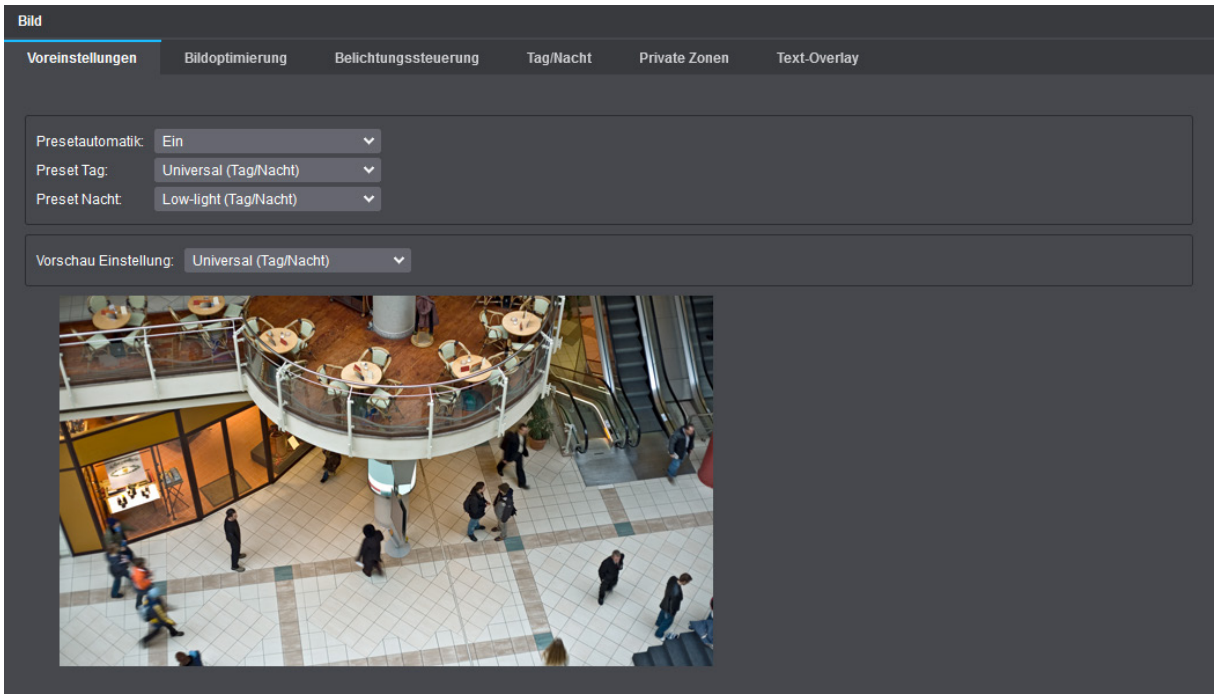


Abb. 5-1

- Wählen Sie aus der Drop-down-Liste **Vorschau Einstellung** ein vordefiniertes Preset als Ausgangspunkt für die manuelle Feinabstimmung von darauffolgenden Einstellungen.
- Nehmen Sie die erforderlichen Einstellungen auf den Registerkarten **Bildoptimierung**, **Belichtungssteuerung** und **Tag/Nacht** vor (siehe im Folgenden).

Die Option **Preset speichern** ist automatisch verfügbar, nachdem Parameter verändert wurden.

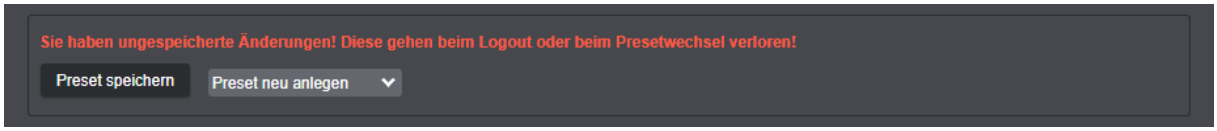


Abb. 5-2

- Klicken Sie **Preset speichern**, nachdem Sie alle notwendigen Änderungen vorgenommen haben, um ein neues benutzerdefiniertes Preset anzulegen.

Der Dialog **Preset speichern** öffnet sich.

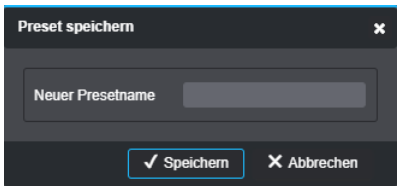


Abb. 5-3

- Geben Sie einen Namen für das Preset ein.
- Bestätigen Sie mit **Speichern**.

*Die Einstellungen der ab Werk vordefinierten Presets werden nie verändert oder überschrieben.*

Das Preset steht nun zur weiteren Verwendung zur Verfügung, zum Beispiel für die Presetautomatik (siehe im Folgenden). Damit die notwendigen Änderungen wirksam werden, muss das Preset aktiviert werden, zum Beispiel als **Preset Tag** oder **Preset Nacht**.

Die Anzahl der benutzerdefinierten Presets ist nicht beschränkt. Sie können wiederum für die Vorschau ausgewählt, weiter optimiert und wieder gespeichert werden.

**Benutzerdefinierte Presets löschen**
Zum Löschen von benutzerdefinierten Presets gehen Sie folgendermaßen vor:

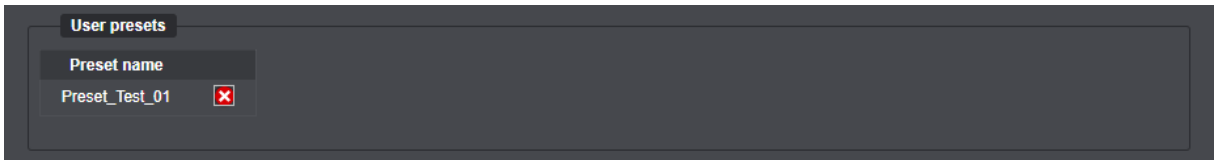


Abb. 5-4

- Klicken Sie auf das **Stift**-Symbol links neben **Presets löschen**.
- Klicken Sie auf das **Löschen**-Symbol (roter Kreis mit weißem Kreuz) rechts neben dem gespeicherten benutzerdefinierten Preset.

Das Preset ist nun gelöscht.

**Presetautomatik**
Die Funktion **Presetautomatik** schaltet das aktive Preset für die Bilderfassung um, wenn die Kamera zwischen dem Tag- und dem Nachtmodus umschaltet.

> *Verknüpft man eigens auf die jeweiligen Lichtverhältnisse zugeschnittene Presets mit der Tag/Nacht-Umschaltung, erfolgt die Bilderfassung automatisch immer mit den optimalen (gewählten) Einstellungen.*

**Vorschau Preset**
Ein Preset kann für die Live-Vorschau auf den folgenden Registerkarten eingestellt werden. Die Parameter des Preset können als Ausgangspunkte für die manuelle Feinabstimmung verwendet und dann als benutzerdefiniertes Preset gespeichert werden.

## 5.2 BILDOPTIMIERUNG

Auf der Registerkarte **Bildoptimierung** können folgende Einstellungen vorgenommen werden:

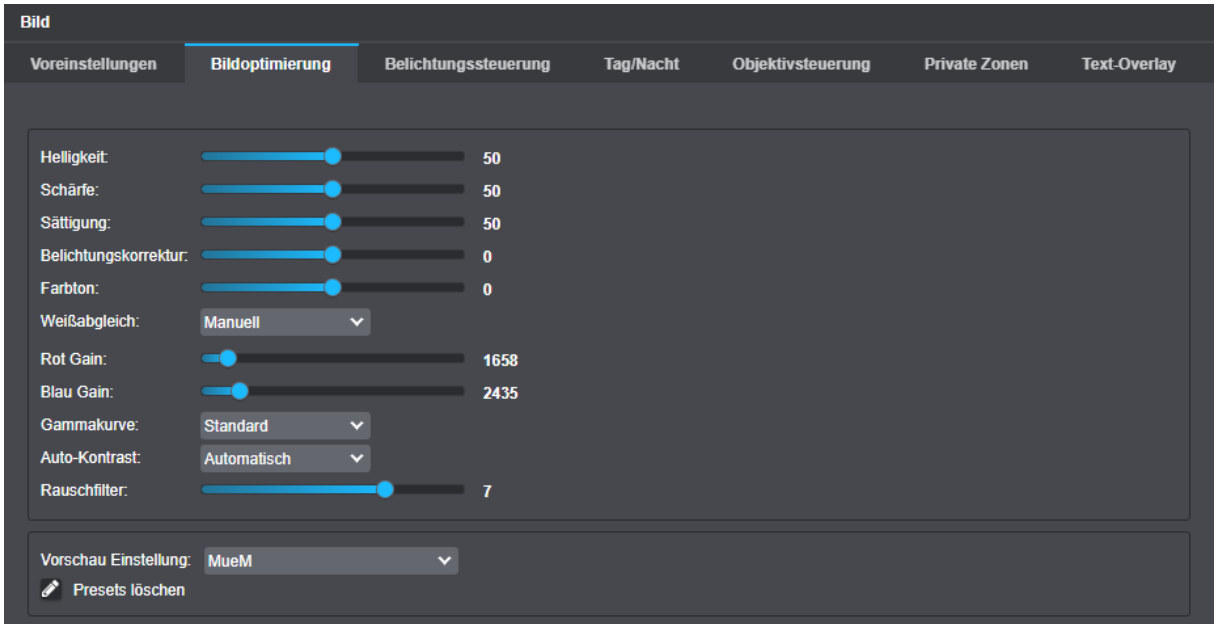


Abb. 5-5 Bildoptimierung

**Helligkeit**
Diese Einstellung bestimmt die Gesamthelligkeit im Bild durch lineare Verschiebung der Tonwerte.

> *Die Helligkeit ist eine globale Einstellung, die auf wechselnde Bildinhalte nicht reagiert.*

**Kontrast**
Diese Einstellung dient zur Anpassung der Helligkeitsunterschiede zwischen hellen und dunklen Bildbereichen.

**Schärfe**
Diese Einstellung beeinflusst den subjektiven Schärfeeindruck durch Betonung der Kantenübergänge.

> *Eine sehr starke Betonung der Kanten (hohe Schärfe) wirkt unnatürlich. Sie kann Bildartefakte (Doppelkanten) und verstärktes Bildrauschen bei schlechten Lichtverhältnissen nach sich ziehen.*

**Sättigung**
Diese Einstellung bestimmt die Farbintensität und Brillanz von Farben und somit deren wahrgenommene Intensität.

> *Die Sättigung wird automatisch gesenkt, wenn das Bildrauschen bei schlechten Lichtverhältnissen zu stark wird.*

## 5.2.1 Weißabgleich

Um unabhängig von den vorherrschenden Lichtquellen und Farbtemperaturen (gemessen in Kelvin) stets eine akkurate Farbwiedergabe zu erreichen, ist ein korrekter Weißabgleich erforderlich.

Zu diesem Zweck bietet die Kamera die folgenden Weißabgleich-Modi:

**Automatik**


Abb. 5-6

Bei dieser Einstellung wird der Weißabgleichwert mithilfe der Farbinformationen des gesamten Bildes automatisch berechnet und kontinuierlich nachgeregelt (an die Änderungen von Farbtemperaturen angepasst).
Für ein bestmögliches Ergebnis sollte sich mindestens ein weißes Objekt in der aufzunehmenden Szene befinden, das dann von der Kamera als Referenzwert für den Weißabgleich verwendet werden kann.

Die Verwendung der Einstellung „Automatik“ (ATW – Auto Tracking White Balance) ist vor allem bei Szenen mit sich ständig ändernden Lichtverhältnissen/Farbtemperaturen empfohlen, wie beispielsweise Aufnahmen im Innenraum mit künstlichen Lichtquellen und einfallendem Tageslicht.

**Manuell**


Abb. 5-7

Diese Einstellung dient zur manuellen Anpassung des Rot-, Grün- und Blauanteils im Bild. Beim manuellen Weißabgleich (MWB – Manual White Balance) können die jeweiligen Farbanteile mithilfe der Schieberegler für die Rot- und Blauverstärkung angepasst werden.

## 5.2.2 Farbtemperatur

*Diese Einstellung ist nur verfügbar im Weißabgleich-Modus **Automatik**.*

**Automatik**
Die empfohlene Einstellung zur automatischen Berechnung des Weißabgleichwerts für Szenen im Innenbereich.

**Automatik außen**
Die empfohlene Einstellung zur automatischen Berechnung des Weißabgleichwerts für Szenen im Außenbereich.

**2800 K, 4000 K, 5000 K**
Die manuelle Auswahl von voreingestellten Farbtemperaturen zur Berechnung des Weißabgleichs ist besonders für Umgebungen mit sehr geringem Weißanteil hilfreich, zum Beispiel dann, wenn grüne Spieltische in Casinos überwacht werden sollen.
Die jeweiligen Angaben in Kelvin beziehen sich auf die Beleuchtungssituation (vorherrschende Farbtempertur) am Aufstellungsort der Kamera und umfassen jeweils ein Spektrum von ±500 Kelvin um den angegebenen Wert.
2800 K entsprechen etwa dem Licht einer normalen Glühbirne, 4000 K etwa dem einer Neonröhre, und 5000 K etwa normalem, hellen Tageslicht.

## 5.2.3 Rauschfilter

Die Funktion **Rauschfilter** ist ein Filter, der während der Reduzierung des Bildrauschens die Bewegungen im Bild erkennt und verfolgt. Dadurch wird die verwischte Darstellung von bewegten Objekten (Ghosting-Effekt) wirksam minimiert.

Abb. 5-8

*Dieser Rauschfilter-Typ wird auch „MCTF - Motion Compensated Temporal Filter“ oder „3D-DNR - 3D Digital Noise Reduction“ genannt.*

Die Regelung des Filters berücksichtigt automatisch wechselnde Lichtverhältnisse. Der Filter ist bei guter Beleuchtung also kaum aktiv und wird erst bei abnehmender Helligkeit immer intensiver angewendet.

Die Stärke der Rauschreduzierung kann eingestellt werden, wobei vermehrte Ghosting-Effekte bei einer aggressiven Regelung beachtet werden müssen. Der Default-Wert von 5 ist eine guter Kompromiss zwischen Rauschreduktion und Ghosting-Effekten.

Der Filter kann mit Einstellung des Wertes 0 ausgeschaltet werden. Das Ausschalten des Filters sollte jedoch möglichst vermieden werden, da ansonsten auch kaum wahrnehmbares Microrauschen (hochfrequentes, kleinräumiges Rauschen) nicht mehr ausgefiltert würde. Dies würde die Encoderlast und die erforderliche Bandbreite merklich erhöhen.

*Um Microrauschen auszufiltern, sollte der Rauschfilter auch bei guter Beleuchtung nicht deaktiviert werden.*

## 5.3 BELICHTUNGSSTEUERUNG

Mithilfe der Belichtungssteuerung kann die automatische Belichtungsmessung der Kamera beeinflusst werden.

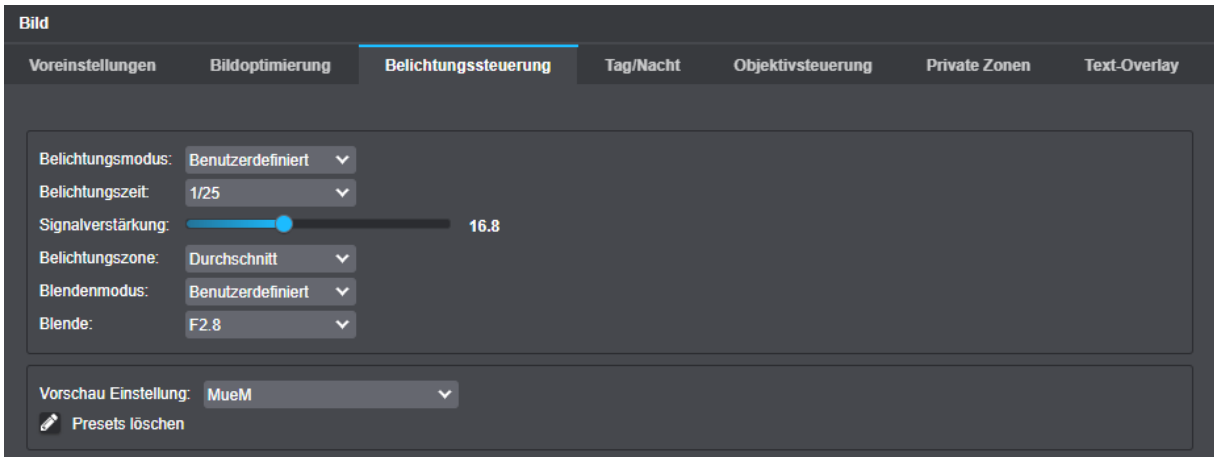


Abb. 5-9

- Beachten Sie die nachfolgenden Erklärungen.
- Stellen Sie die relevanten Optionen ein.

### 5.3.1 Belichtungsmodus

**Semi-Automatic**
Das gesamte Bild wird zur Belichtungsmessung herangezogen. Für eine korrekte Belichtung bestimmt die Kamera automatisch die beste Kombination von Belichtungszeit, Blende und Signalverstärkung. Dabei hält sie die eingestellten Maximalwerte ein.

**Benutzerdefiniert**
Das gesamte Bild wird zur Belichtungsmessung herangezogen. Für eine korrekte Belichtung werden die eingestellten Werte verwendet.

### 5.3.2 Maximale Belichtungszeit

Für eine korrekte Belichtung bestimmt die Kamera automatisch die beste Kombination von Belichtungszeit, Blende und Signalverstärkung.
Die **Maximale Belichtungszeit** definiert dabei die maximal zulässige automatische Belichtungszeit. Bei Erreichen der eingestellten maximalen Belichtungszeit wird die automatische Belichtungssteuerung (AE – Automatic Exposure) nur noch über den Blendenwert und/oder die automatische Verstärkungsregelung (AGC – Automatic Gain Control) geregelt.

### 5.3.3 Maximale Signalverstärkung

Die Option **Maximale Signalverstärkung** legt mittels Schieberegler den Wert in dB fest, mit dem die automatische Belichtungssteuerung das Signal am Sensor verstärken darf.
Höhere Werte führen zu größerem Rauschen im Bild, niedrigere Werte verringern das Rauschen.

### 5.3.4 Belichtungspriorität

Die Belichtungspriorität regelt ob der hohe, mittlere oder tiefe Tonwertbereich des Bildes bevorzugt dargestellt werden soll. Die Option **Lichter** hebt helle Bildanteile, **Mitten** die mittleren Bildanteile, und **Schatten** die tiefen Anteile des Bildes besser hervor.

### 5.3.5 Blendenmodus

**Automatisch**
Mit dieser Einstellung wird die Blendenöffnung automatisch von der Kamera geregelt (in Abhängigkeit von Belichtungszeit und Signalverstärkung).

**Benutzerdefiniert**
Diese Option dient zur manuellen Einstellung der Blendenöffnung.

## 5.4 TAG/NACHT

Dallmeier Kameras mit Domera® OS sind für eine maximale Bildqualität sowohl bei Tageslicht als auch bei schlechten Lichtverhältnissen oder sogar bei völliger Dunkelheit in der Nacht ausgelegt.

Auf der Registerkarte **Tag/Nacht** können dazu folgende Einstellungen vorgenommen werden:

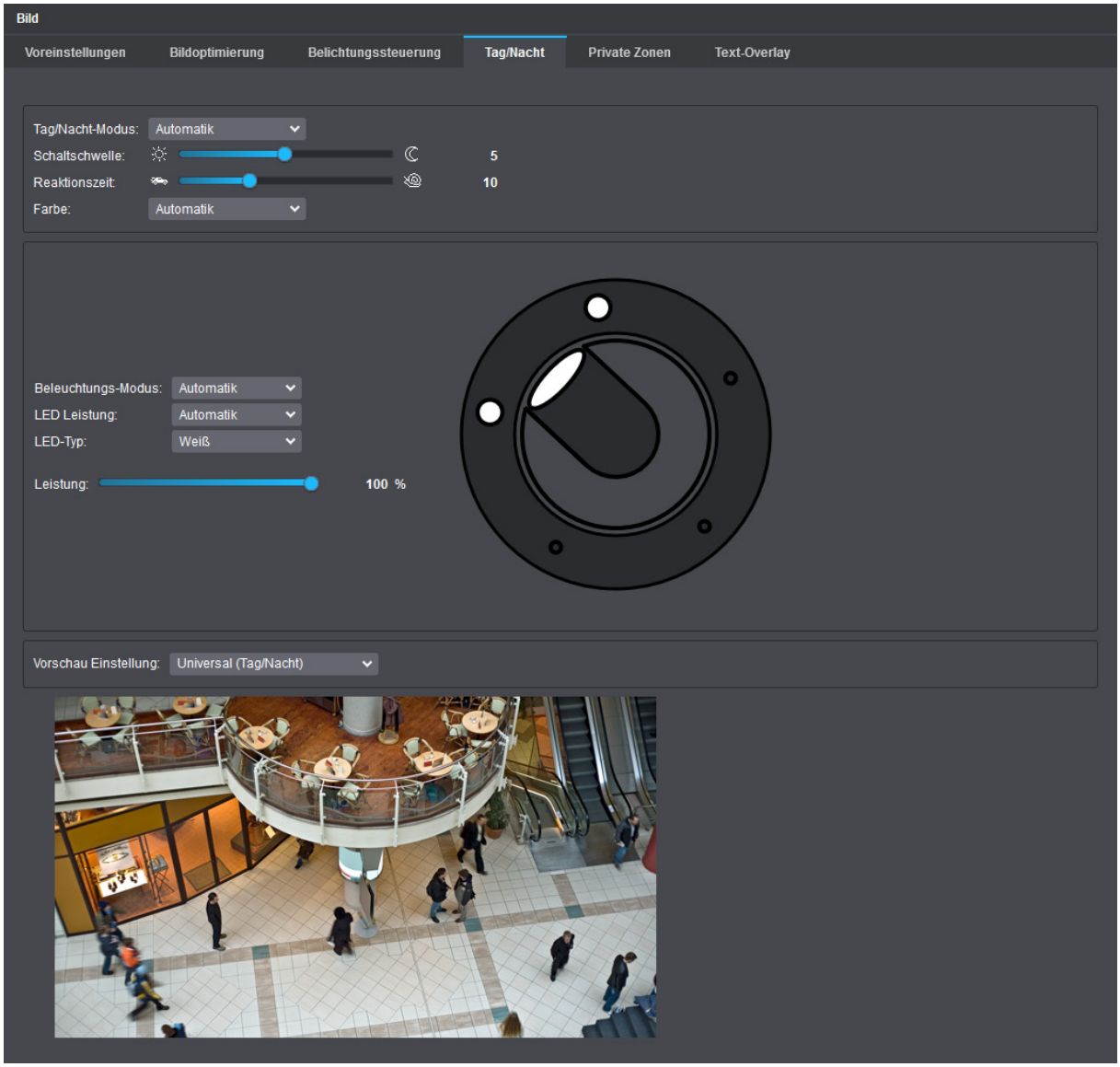


Abb. 5-10

### 5.4.1 Tag/Nacht-Modus

**Automatik**
Bei dieser Einstellung erfolgt die Tag/Nacht-Umschaltung in der Kamera automatisch in Abhängigkeit vom kontinuierlich gemessenen sichtbaren Umgebungslicht und bei Erreichen bzw. dem Unter- oder Überschreiten einer intern definierten Schaltschwelle anhand der ermittelten Werte für Belichtungszeit, Signalverstärkung und Blendenöffnung.
Bei schwachem Licht schaltet die Kamera unterhalb einer bestimmten Helligkeitsstufe in den Nachtmodus und der eingebaute Infrarot-Sperrfilter wird ausgeschwenkt (mechanisch vom Bildsensor weggeschoben), wodurch die spektrale Empfindlichkeit des Bildsensors für nahes Infrarot zunutze gemacht wird.
Sobald wieder eine bestimmte Helligkeit des sichtbaren Lichts vom integrierten Umgebungslichtsensor gemessen wird, schaltet die Kamera zurück in den Tagmodus und der Infrarot-Sperrfilter wird wieder eingeschwenkt (mechanisch vor den Bildsensor geschoben), um die im Tagmodus störenden Nahinfrarot-Wellenlängen zu blockieren (herauszufiltern) und farbgetreue Bilder zu erhalten.
Die obere Hysterese der Schaltschwelle zur automatischen Umschaltung in den Tagmodus und die Reaktionszeit vor einer tatsächlichen Tag/Nacht-Umschaltung können manuell angepasst werden (siehe Beschreibungen weiter unten).

**Tag – ICR ein**
Bei dieser Einstellung arbeitet die Kamera unabhängig vom gemessenen Umgebungslicht immer im Tagmodus. Der Infrarot-Sperrfilter bleibt dabei ständig eingeschwenkt.

**Nacht – ICR aus**
Bei dieser Einstellung arbeitet die Kamera unabhängig vom gemessenen Umgebungslicht immer im Nachtmodus. Der Infrarot-Sperrfilter bleibt dabei ständig ausgeschwenkt.

**Automatik – ICR ein**
Diese Einstellung entspricht der oben beschriebenen Einstellung **Automatik**, der Infrarot-Sperrfilter bleibt jedoch auch im Nachtmodus durchgehend eingeschwenkt (vor dem Bildsensor positioniert).

*Diese Einstellmöglichkeit ist nur für sehr spezielle Anwendungsszenarien vorgesehen.*

### 5.4.2 Schaltschwelle

Diese Einstellung dient zur Anpassung der oberen Hysterese für das Zurückschalten in den Tagmodus, um ein zu häufiges Umschalten der Kamera zwischen Tag- und Nachtbetrieb zu vermeiden.
Der eingestellte Wert (Standard: **5**) gibt an, um wie viel heller das aktuell vom integrierten Umgebungslichtsensor gemessene sichtbare Licht sein muss als der letzte bekannte Helligkeitswert vor dem Umschalten in den Nachtmodus, bevor die Kamera wieder in den Tagmodus zurückschaltet.

**Geringerer Wert**
Die Kamera schaltet vergleichsweise früh wieder in den Tagmodus zurück. Das bedeutet, dass zwischen dem letzten bekannten Helligkeitswert vor dem Umschalten in den Nachtmodus und dem aktuell vom integrierten Umgebungslichtsensor gemessenen sichtbaren Licht nur eine relativ geringe Differenz bestehen muss.

**Höherer Wert**
Die Kamera schaltet erst relativ spät wieder in den Tagmodus zurück.

### 5.4.3 Reaktionszeit

Diese Funktion dient zur weiteren Feineinstellung der automatischen Tag/Nacht-Umschaltung.
Die Reaktionszeit in Sekunden (Standard: **10**) definiert dabei die Verzögerungszeit vor der eigentlichen Tag/Nacht-Umschaltung bei Unter- bzw. Überschreiten der intern definierten Schaltschwelle.

Beispiel:
Wird die Kamera tagsüber in einem Raum mit einem Fenster zu einer Verkehrsstraße betrieben, kann es bei Vorbeifahren eines großen Lastkraftwagens zu einer kurzfristigen starken Verdunkelung des gesamten Innenraums kommen. In der Folge würde die Kamera normalerweise bei Unterschreiten der internen Schaltschwelle sofort in den Nachtmodus schalten und kurz darauf wieder zurück in den Tagmodus.
Im umgekehrten Fall würde es hingegen nachts immer wieder zu einem ungewollten kurzfristigen Umschalten in den Tagmodus und zurück kommen, sobald das Scheinwerferlicht vorbeifahrender Autos in den Innenraum strahlt.

Mithilfe der Reaktionszeit kann die automatische Tag/Nacht-Umschaltung also je nach Bedarf entsprechend verzögert werden.

### 5.4.4 Farbe

**Automatik**
Bei dieser Einstellung schaltet die Kamera im Nachtmodus automatisch in den Graustufen- bzw. Schwarz-Weiß-Modus und im Tagmodus wieder in den Farbmodus.

**Ein**
Bei dieser Einstellung arbeitet die Kamera sowohl im Tag- als auch im Nachtmodus immer im Farbmodus.

*Bei Einsatz von Infrarotlicht im Nachtmodus (Infrarot-Sperrfilter ist ausgeschwenkt) kann das Vorhandensein von noch sichtbarem Restlicht in der erfassten Szene je nach Entfernung und Oberflächenbeschaffenheit der abgebildeten Objekte (Reflexionsgrad) unter Umständen zu Falsch- bzw. Fehlfarben in den ausgegebenen Bildern führen.*

**Aus**
Bei dieser Einstellung arbeitet die Kamera sowohl im Tag- als auch im Nachtmodus immer im Schwarz-Weiß-Modus (jegliche Farbinformationen aus der erfassten Szene sind dabei unwiederbringlich verloren).

*Ohne die vorliegenden Farbinformationen im generierten Bild kann die Gesamtbildqualität bei Szenen mit nur sehr unzureichender Beleuchtung im Tagmodus möglicherweise verbessert werden (z. B. durch Vermeidung von störendem Farbrauschen).*

### 5.4.5 Beleuchtungs-Modus

Mithilfe dieser Einstellung können Sie die integrierte Infrarot(IR)- oder Weißlicht-LED-Beleuchtung Ihrer Kamera konfigurieren.
Die IR-Beleuchtung erfolgt beispielsweise mittels halbdiskreter 850 nm Hochleistungs-LEDs.

Es stehen drei Beleuchtungs-Modi zur Verfügung:

**Automatik**
Die gewählte Beleuchtungsart (IR oder Weißlicht; siehe Drop-down-Liste **LED-Typ**) wird automatisch aktiviert, sobald die Kamera vom Tag- in den Nachtmodus wechselt, und wieder deaktiviert, wenn die Kamera erneut im Tagmodus arbeitet.
Die LED-Leistung kann dabei je nach Bedarf manuell geregelt werden.

**Immer an**
Die gewählte Beleuchtungsart bleibt unabhängig von der jeweiligen Betriebsart (Tag- oder Nachtmodus) immer aktiviert.
Die LED-Leistung kann dabei je nach Bedarf manuell geregelt werden.

**Immer aus**
Die integrierten Beleuchtungs-LEDs (IR oder Weißlicht) bleiben unabhängig von der jeweiligen Betriebsart (Tag- oder Nachtmodus) immer deaktiviert.

## 5.5 PRIVATE ZONEN

Zum Schutz der Privatsphäre und zur Einhaltung von Datenschutzgesetzen und Regelungen, die eine gezielte Überwachung und/oder Aufzeichnung bestimmter sensibler Bereiche verbieten, ermöglicht die Funktion **Private Zonen** ein Ausblenden (Maskieren) frei wählbarer Zonen in der erfassten Szene mithilfe verschiedener Maskierungswerkzeuge.
Die Maskierung kann dabei mit schwarzen Rechtecken oder Polygonen erfolgen.

> *Die Anzahl möglicher privater Zonen ist modellabhängig (beachten Sie die Produktspezifikation zu Ihrem Gerät).*
> *Die gesamte Fläche aller privaten Zonen kann bis zu 100% des Gesamtbildes betragen.*

- Wählen Sie die Registerkarte **Private Zonen**.

**Rechteck zeichnen**

- Klicken Sie auf die Schaltfläche **Rechteck zeichnen**.
- Positionieren Sie den Mauszeiger an der Stelle, an der Sie mit dem Zeichnen beginnen wollen.
- Ziehen Sie mit gedrückter linker Maustaste ein Rechteck über den relevanten Bildbereich.
- Lassen Sie die Maustaste los, um das Zeichnen des Rechtecks abzuschließen.

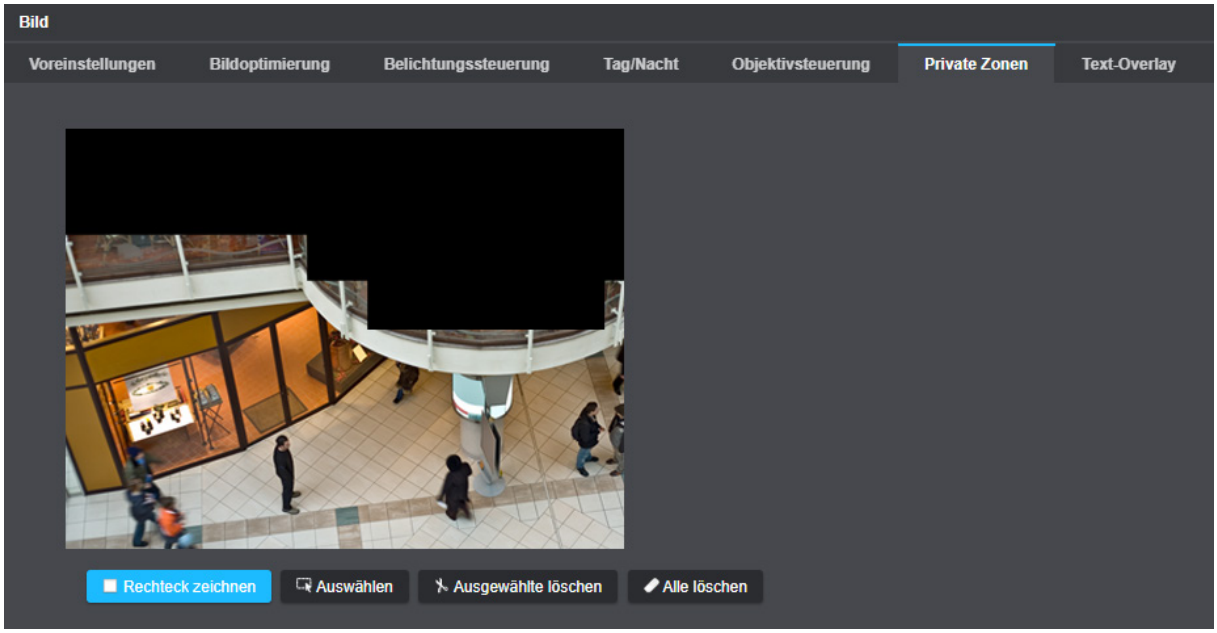


Abb. 5-11

Der gewählte Bildbereich wird als private Zone maskiert.

- Verfahren Sie entsprechend für die Definition weiterer privater Zonen.

> *Das Verschieben von definierten privaten Zonen durch Drag&Drop wird unterstützt.*

**Polygon zeichnen**

- Klicken Sie auf die Schaltfläche **Polygon zeichnen**.
- Positionieren Sie den Mauszeiger an der Stelle, an der Sie mit dem Zeichnen beginnen wollen.
- Legen Sie jeweils per Linksklick mit der Maus die Ecken eines Polygons (Vielecks) fest, das als private Zone definiert werden soll.
- Schließen Sie per Rechtsklick mit der Maus die Erstellung des Vielecks ab (Rechtsklick = letzter Eckpunkt).

**Private Zonen löschen**

Um private Zonen zu löschen, gehen Sie folgendermaßen vor:

- Markieren Sie die erforderliche private Zone und klicken Sie auf die Schaltfläche **Ausgewählte löschen**.

Die ausgewählte Zone ist nun gelöscht.

- Klicken Sie auf die Schaltfläche **Alle löschen**, um alle privaten Zonen auf einmal zu löschen.

## 5.6 TEXT-OVERLAY

Auf der Registerkarte **Text-Overlay** können verschiedene Texteinblendungen definiert und konfiguriert werden, die dann im Live-Bild oder bei der Wiedergabe des aufgezeichneten Videomaterials dauerhaft angezeigt werden.

> *Die jeweiligen Zeichenfolgen werden fest in das Vidobild eingefügt. Sie können nicht nachträglich ausgeblendet bzw. entfernt werden.*

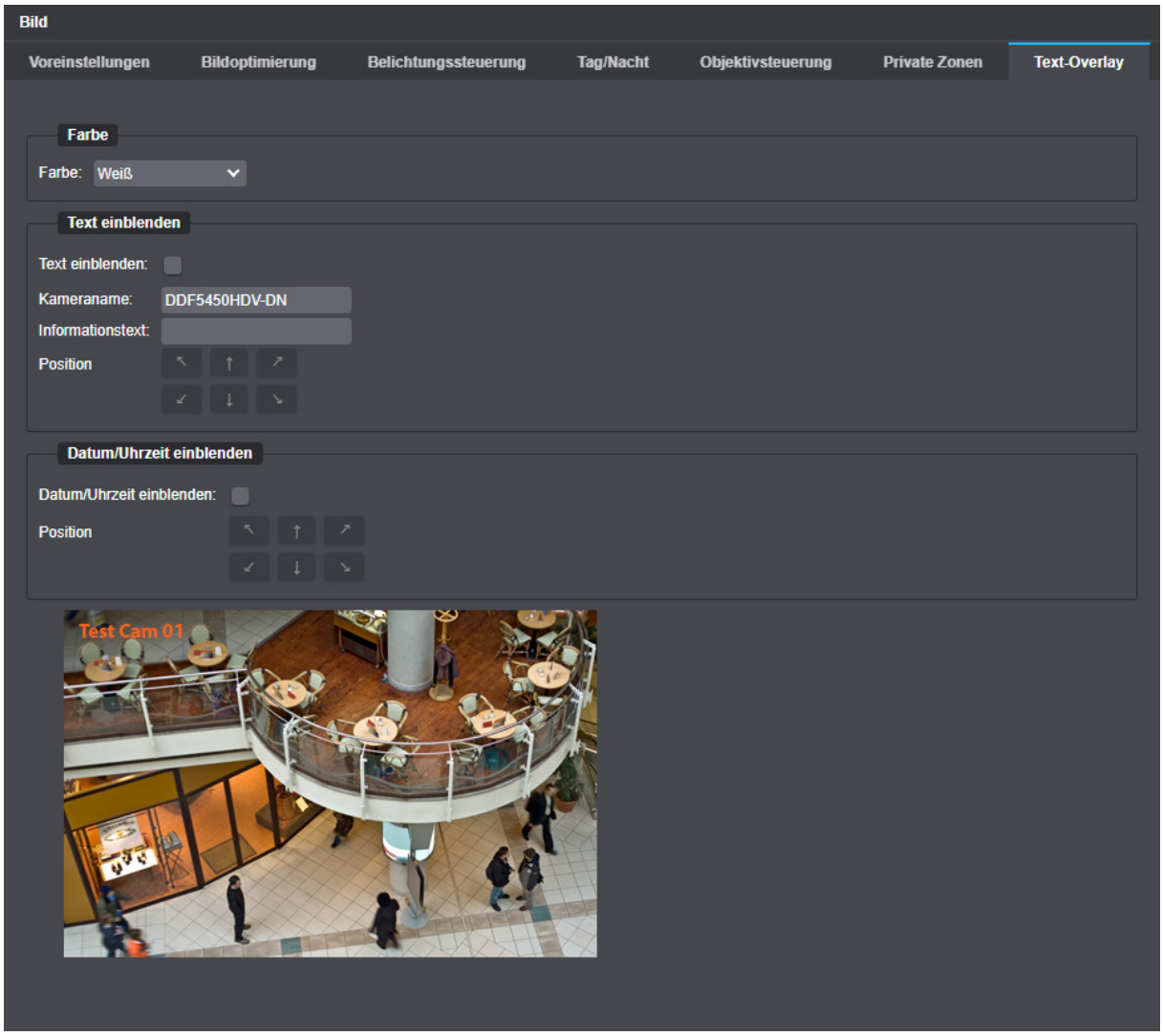


Abb. 5-12

### Farbe

- Wählen Sie zunächst aus der Drop-down-Liste **Farbe** eine globale Farbe aus, die für die erfasste Szene und die Positionen der jeweiligen Texteinblendungen geeignet ist, damit die Zeichenfolgen später so gut wie möglich zu erkennen bzw. lesbar sind.

**Text einblenden**

- Aktivieren Sie die Checkbox **Text einblenden**.
- Wählen Sie aus der Drop-down-Liste **Einblendemodus** zwischen den möglichen Texteinblendungen **Kameraname**, **Informationstext** oder **Typ und Seriennummer** Ihrer Kamera.
- Ändern Sie gegebenenfalls die Bezeichnung der Kamera im Feld **Kameraname** oder geben Sie einen **Informationstext** in das entsprechende Feld ein.
- Legen Sie die Position der zuvor gewählten Texteinblendung mit den entsprechenden Pfeil-Buttons fest.

**Datum/Uhrzeit einblenden**

- Aktivieren Sie die Checkbox Datum/Uhrzeit **einblenden**, wenn Sie die zum Zeitpunkt der jeweiligen Bilderzeugung vorliegende Systemzeit der Kamera in das Videobild einblenden möchten.
- Legen Sie die Position der eingeblendeten Systemzeit mit den entsprechenden Pfeil-Buttons fest.

# OBJEKTIVSTEUERUNG (RPOD)

Mit Domera® OS erfolgt die Positionierung (Ausrichtung) der Objektiv-/Sensoreinheit sowie die Einstellung von Zoom (Brennweite) und Fokus dank der integrierten **PTRZ (Pan Tilt Roll Zoom)**-Funktion des **Dallmeier RPoD** (Remote Positioning Dome) bequem über das Netzwerk im Webbrowser.

*ACHTUNG*

**Beschädigung der Kamera-Kardanik und des Objektivs**

Die kardanische Aufhängung der Kamera und das P-Iris Varifokal-Objektiv sind mit hochpräzisen Schrittmotoren ausgestattet. Versuchen Sie daher unter keinen Umständen, die Ausrichtung der Objektiv-/Sensoreinheit oder den Zoom und den Fokus manuell an der Kamera-Hardware einzustellen.

- Klicken Sie im Navigationsmenü den Menüeintrag **Objektivsteuerung (RPoD)**, um den entsprechenden Dialog zu öffnen.

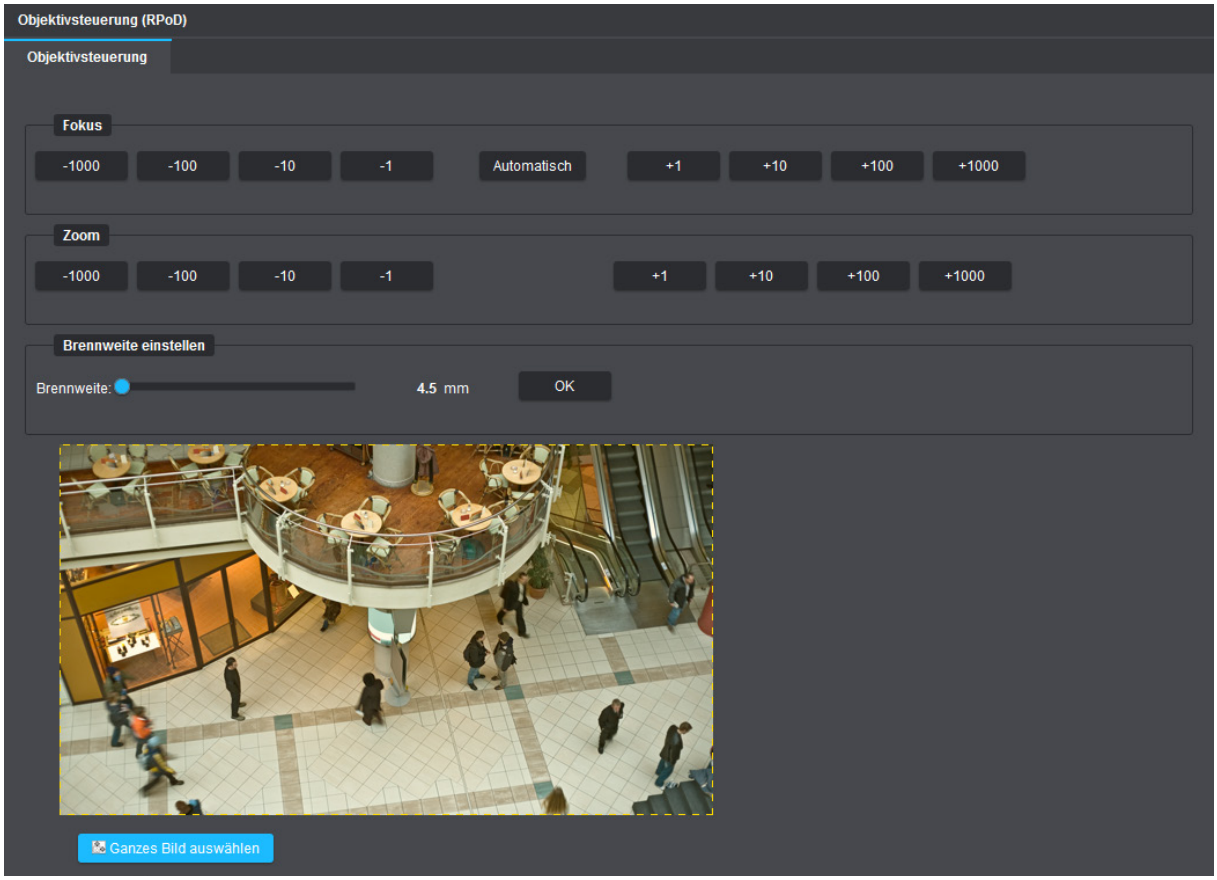


Abb. 6-1

## Fokus

Fokussierung Fernbereich (**+**) / Nahbereich (**–**) mit One-Push Autofokus* (Schaltfläche **Automatisch**)

* Für optimale Ergebnisse beim One-Push Autofokus wählt P-Iris automatisch die größtmögliche Blendenöffnung (kleinstmögliche Blendenzahl) und damit eine anfänglich minimale Schärfentiefe, um später unter allen Lichtverhältnissen eine hervorragende Abbildungsqualität und maximale Schärfeausdehnung im Objektraum zu erhalten. Nach einer kurzen Zeit ohne Benutzeraktion wird die Blende des P-Iris-Objektivs wieder auf den ursprünglichen Blendenwert zurückgesetzt.

### Zoom

Zoom In (**+**) / Zoom Out (**–**)
Anpassung des Bildausschnitts durch Veränderung der Brennweite in einzelnen variablen Schritten

### Brennweite einstellen

Anpassung des Bildausschnitts durch Verstellen der Brennweite anhand fester Werte (Stufenzoom mit mehreren werksseitig vordefinierten Brennweiten)

- Wählen Sie eine vordefinierte **Brennweite** mithilfe des entsprechenden Schiebereglers.
- Bestätigen Sie mit **OK**.

*Reduzieren Sie ggf. die Encoding-Datenrate (Bitrate), um mögliche Verzögerungen (längere Reaktionszeiten) bei der browserbasierten Objektivsteuerung zu minimieren.*

### Positioning

Dieser Dialogbereich dient zur elektronischen Positionierung (Ausrichtung) der Objektiv-/Sensoreinheit über das Netzwerk.

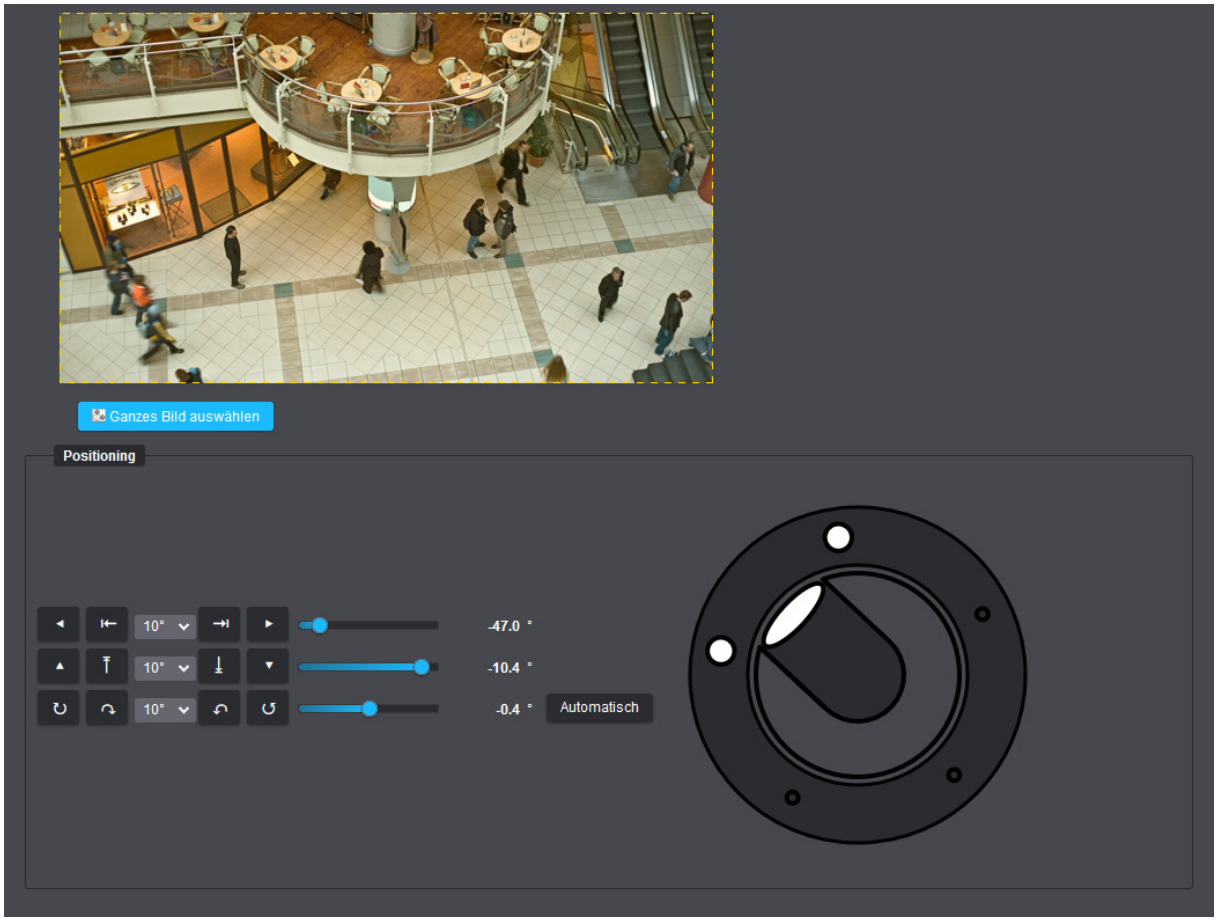


Abb. 6-2

*Bewegen Sie den Mauszeiger über die verfügbaren Schaltflächen, um die jeweilige Funktionsbeschreibung (Tooltip) anzuzeigen.*
*Änderungen an der elektronischen Positionierung (Pan, Tilt, Roll) werden zur Veranschaulichung und besseren Bedienbarkeit entsprechend grafisch dargestellt.*

# VIDEO

Der Dialog **Video** dient zur Konfiguration der Sensor- und Encodereinstellungen.

- ▶ Klicken Sie im Navigationsmenü den Menüeintrag **Video**, um den entsprechenden Dialog zu öffnen.
- ▶ Beachten Sie die nachfolgenden Erklärungen zu den verschiedenen Einstellungen.

## 7.1 SENSOREINSTELLUNGEN

Die Registerkarte **Sensoreinstellungen** umfasst die grundlegenden Konfigurationseinstellungen, die für alle verfügbaren Streams Ihrer Kamera gleichermaßen wirksam sind (siehe Abschnitt „Stream-/Encoder-einstellungen“ auf Seite 38).

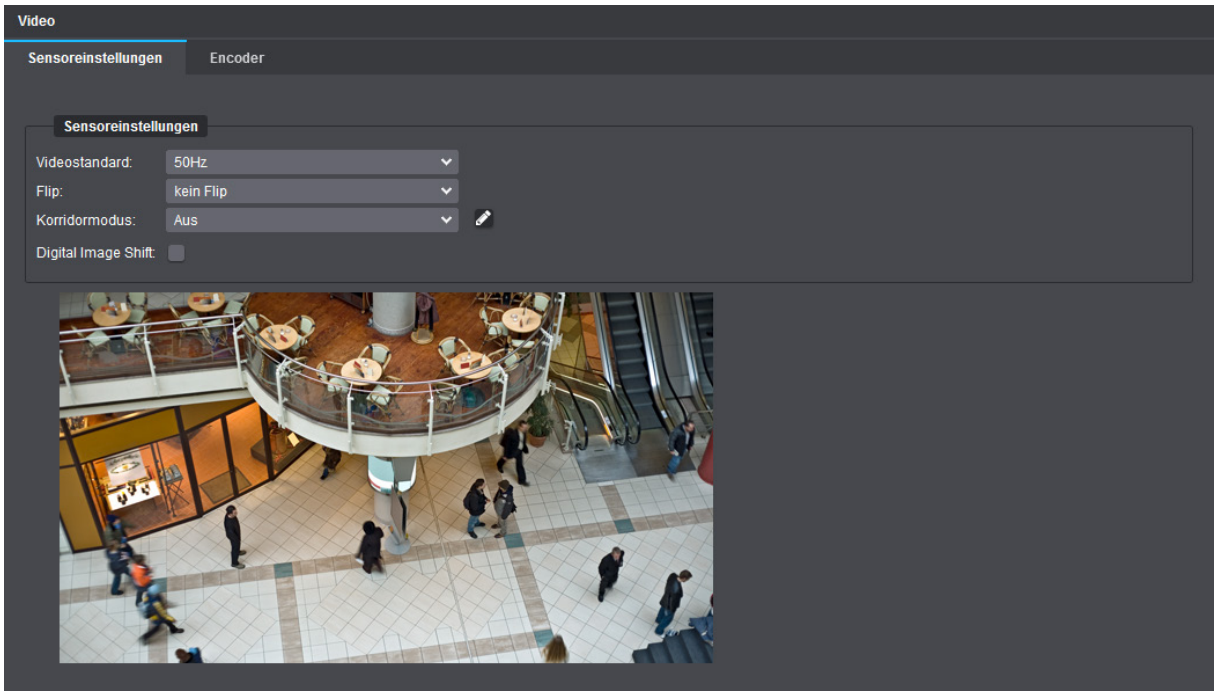


Abb. 7-1

**Videostandard** (Frequenzeinstellung)
Für eine korrekte Bilderfassung und Signalverarbeitung muss die Frequenzeinstellung auf Ihrer Kamera mit der Frequenz des Stromnetzes (Netzfrequenz) in Ihrem Land bzw. Ihrer Region übereinstimmen:

- **50 Hz** (verwendet in PAL-Ländern wie z. B. in Europa, Australien und vielen Ländern Afrikas und Asiens)
- **60 Hz** (verwendet in NTSC-Ländern wie z. B. in den USA und Japan)

Die gewählte Frequenzeinstellung beeinflusst u. a. die jeweils einstellbaren Bildraten (**Bilder/Sekunde**) für die einzelnen verfügbaren Streams auf der Registerkarte **Encoder** (z. B. 25/50 fps@50 Hz oder 30/60 fps@60 Hz) sowie einige der einstellbaren Werte für die **Belichtungszeit** (z. B. 1/50 s@50 Hz oder 1/60 s@60 Hz) auf der Registerkarte **Belichtungssteuerung** im Dialog **Bild**.

Beachten Sie, dass eine inkorrekte Einstellung dieses Parameters zu einem typischen störenden 50/60 Hz-Videoflimmern (Bildflackern) führen kann, z. B. bei Verwendung künstlicher, fluoreszierender Lichtquellen wie Leuchtstofflampen, die mit Wechselstrom (AC – „Alternating Current“) betrieben werden.

### Flip

Mithilfe der **Flip**-Funktion kann das Bild in der Kamera an der horizontalen Achse (**vertikaler** Flip), an der vertikalen Achse (**horizontaler** Flip) oder an beiden Achsen gleichzeitig gespiegelt werden. Dies ermöglicht Ihnen flexible Lösungen für die Montage der Kamera auf einem Tisch, an einer Decke oder an einer Wand.

### Korridormodus

*Der **Korridormodus** ist nicht für Fisheye-Kameramodelle verfügbar.*

Der **Korridormodus** eignet sich insbesondere für die Videoabsicherung vertikal ausgerichteter Szenen wie langgestreckte Räume (Gänge, Flure, Korridore), Straßen und Gehwege, Bahnsteige oder Zaunanlagen (Perimeterschutz).
Zunächst wird die Kamera bzw. die Objektiv-/Sensoreinheit bei der Installation physisch so gedreht, dass die Szene nicht wie üblich in einem Seitenverhältnis von 16:9 bzw. 4:3 (Querformat) erfasst wird, sondern in einem Seitenverhältnis von 9:16 bzw. 3:4, also im Hochformat. Somit kann die volle verfügbare Sensorauflösung ausschließlich für wichtige Bildbereiche genutzt werden. Eine Encodierung, Netzwerkübertragung, Aufzeichnung und spätere Decodierung überflüssiger Informationen an den Bildseiten wird vermieden.
Bei der Auswertung des Videomaterials (Live-Ansicht oder Playback/Wiedergabe) werden die Bilder dann entsprechend der zuvor gewählten Einstellung automatisch für den Operator richtig gedreht angezeigt.

Beispiel:

Abb. 7-2:
Auflösung Full HD,
Sensor-Seitenverhältnis 16:9,
keine physische Kameradrehung,
Korridormodus > Aus

Abb. 7-3:
Auflösung Full HD,
Sensor-Seitenverhältnis 9:16,
physische Kameradrehung um 90°,
Korridormodus > Aus

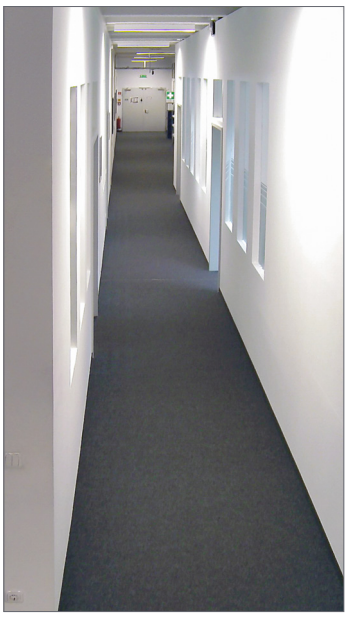

Abb. 7-4:
Auflösung Full HD,
Sensor-Seitenverhältnis 9:16,
physische Kameradrehung um 90°,
Korridormodus > Rotation um 90°

## Digital Image Shift

*Die Funktion **Digital Image Shift** ist nicht für Dome-Kameras mit motorgetriebener Kardanik verfügbar („Remote Positioning Dome“ oder kurz: RPoD).*

In der Regel wird nur ein bestimmter Bereich aus der Mitte des Bildsensors effektiv zur Bilderfassung genutzt, niemals jedoch die gesamte verfügbare Sensorfläche. Je nach gewählter Ausgabeauflösung für **Stream 1** (siehe Abschnitt „Stream-/Encodereinstellungen“ auf Seite 38) bleibt daher normalerweise eine definierte Anzahl von Sensorpixeln an den Rändern des Bildsensors unberücksichtigt.

Die Funktion **Digital Image Shift** ermöglicht es, den erfassten Bildausschnitt über den Webbrowser geringfügig nachzujustieren, indem der auszulesende Pixelbereich in horizontaler und/oder vertikaler Richtung abweichend von der Mitte des Bildsensors digital verschoben wird.

Die Verwendung dieser Funktion mithilfe der entsprechenden Schieberegler ist vor allem dann hilfreich, wenn Sie nach der Montage und Ausrichtung der Kamera feststellen, dass der erfasste Bildausschnitt der zu beobachtenden Szene nicht exakt Ihren Anforderungen entspricht. Eine manuelle Feinjustierung der Blickrichtung der Objektiv-/Sensoreinheit direkt an der Kamera ist demnach nicht erforderlich.

## 7.2 STREAM-/ENCODEREINSTELLUNGEN

Auf der Registerkarte **Encoder** werden die jeweiligen Encodereinstellungen für die einzelnen verfügbaren Streams festgelegt.

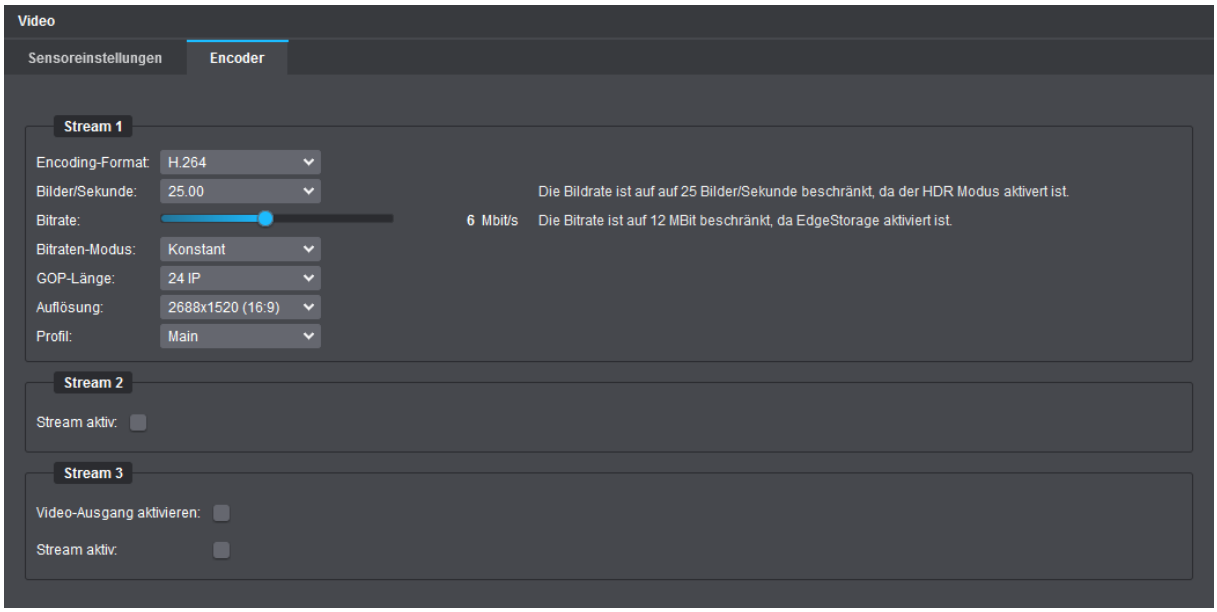


Abb. 7-5

> *Die auf den folgenden Seiten beschriebenen Einstellungen **Bitrate**, **Bitraten-Modus** und **GOP-Länge** sind nicht verfügbar, wenn das **Encoding-Format** > **MJPEG** gewählt ist.*

### Encoding-Format

Das **Encoding-Format** bestimmt jeweils den Videocodec (**H.264**, **H.265** oder **MJPEG**), der zum Encodieren der einzelnen Streams verwendet wird.

### Bilder/Sekunde

Die Einstellung **Bilder/Sekunde** bestimmt die Bildrate (in fps) und legt die Anzahl der Bilder (Frames) fest, die pro Sekunde hintereinander produziert werden.
Je höher die Bildrate, desto flüssiger die Videowiedergabe. Eine höhere Bildrate erfordert jedoch immer auch eine höhere Netzwerkbandbreite (Übertragungskapazität) und mehr Speicherplatz für die Aufzeichnung von Videomaterial.
Eine Bildrate von 25 fps (in PAL-Ländern bzw. in Ländern mit einer Netzfrequenz von 50 Hz) oder 30 fps (in NTSC-Ländern bzw. in Ländern mit einer Netzfrequenz von 60 Hz) entspricht beispielsweise den Anforderungen an Echtzeit-Anwendungen (Real-Time Video).

### JPEGQuality

Diese Einstellung ist nur verfügbar, wenn das **Encoding-Format** > **MJPEG** (Motion JPEG) ausgewählt ist. Bei der Verwendung des Formats **MJPEG** wird jedes erzeugte Einzelbild unabhängig voneinander als separates JPEG-Bild komprimiert. Der Schieberegler **JPEGQuality** bestimmt dabei die Qualität der JPEG-Bilder, die je nach eingestellter Bildrate nacheinander generiert werden. Je höher der eingestellte Wert ist, desto geringer ist die Komprimierungsrate und desto höher ist die Qualität der einzelnen Bilder, aber desto höher ist auch der Bandbreiten- und Speicherplatzbedarf.

### Bitrate

Die Encoding-Bitrate bestimmt die Anzahl der Bits pro Sekunde, die für die Codierung der erzeugten Videodaten verwendet werden. Je mehr Bits dem Video-Encoder pro Sekunde bereitgestellt werden, um die Bildinhalte in komprimierter Form abzubilden, desto höher ist in der Regel die spätere Bildqualität. Eine höhere Video-Bitrate erfordert jedoch immer auch eine höhere Netzwerkbandbreite (Übertragungskapazität) für die paketweise Übertragung der Daten und mehr Speicherplatz für die Datenaufzeichnung.

Geringere Bitrate = Höhere Bildkompression
= Kleinere Datenmenge
= Geringere Bildqualität und Detailwiedergabe
= Geringerer Bandbreiten- und Speicherplatzbedarf

Höhere Bitrate = Geringere Bildkompression
= Größere Datenmenge
= Höhere Bildqualität und Detailwiedergabe
= Höherer Bandbreiten- und Speicherplatzbedarf

### Bitraten-Modus

Der **Bitraten-Modus** ermöglicht die Einstellung einer konstanten Bitrate oder einer variablen Bitrate für die Video-Codierung, jeweils auch mit einer Prioritätseinstellung für die Bildqualität (siehe im Folgenden).

#### Konstante Bitrate

Bei einer konstanten Bitrate erfolgt die Video-Codierung immer mit der eingestellten Bitrate, auch wenn sie für Szenen mit wenig Bildveränderungen nicht erforderlich ist.
Wenn die eingestellte Bitrate für Szenen mit vielen Bildveränderungen nicht ausreicht, wird die Bildqualität angepasst.
Konstante Bitraten erlauben eine genauere Berechnung der erforderlichen Netzwerkbandbreite (Übertragungskapazität) und Speicherkapazität (für die Aufzeichnung).

#### Variable Bitrate

Bei einer variablen Bitrate wird die Bitrate dynamisch an die Bildveränderungen angepasst. Für Szenen mit wenig Bildveränderungen wird sie gesenkt, für Szenen mit vielen Bildveränderungen erhöht.

> *Der Schieberegler **Bitrate** wird in diesem Fall erweitert und erlaubt die Einstellung einer Bitraten-Untergrenze. Diese wird auch für Szenen ohne Bildveränderungen nicht unterschritten.*

Für Szenen mit sehr vielen Bildveränderungen kann die Bitrate kurzzeitig über den eingestellten Wert angehoben werden. Wenn die verfügbare Gesamt-Bitrate nicht für alle Streams/Encoder ausreicht, wird die Bildqualität angepasst.
Variable Bitraten ermöglichen eine höhere Bildqualität bei gleichzeitig besserer Ausnutzung der verfügbaren Netzwerkbandbreite (Übertragungskapazität) und Speicherkapazität (für die Aufzeichnung).

#### Prioritätseinstellung für die Bildqualität

Die Modi **Konstant QK** und **Variabel QK** (QK = Quality Keep) sind eine Variation der oben beschriebenen Bitraten-Modi. Wenn die eingestellte Bitrate (**Konstant QK**) oder die verfügbare Gesamt-Bitrate für alle Streams/Encoder (**Variabel QK**) für Szenen mit sehr vielen Bildveränderungen nicht ausreicht, wird statt der Bildqualität die Bildrate (fps) angepasst.

### GOP-Länge

[Standardeinstellung: **24 IP**]

Die Kodierung eines Videostreams mit **H.264** (MPEG-4 Part 10 / AVC – Advanced Video Coding) oder **H.265** (MPEG-H Part 2 / HEVC – High Efficiency Video Coding) erfolgt durch die Einteilung von Bildern im MPEG-Datenstrom in sogenannte „Group of Pictures" (GOP) oder Bild(er)gruppen definierter Länge (**GOP-Länge**).

Eine GOP beginnt mit einem I-Frame (Intra-Frame bzw. Key-Frame), das alle generierten Bildinformationen enthält und als Referenz für die nachfolgenden Bilder innerhalb einer GOP dient.
Das I-Frame ist unabhängig von vorherigen und nachfolgenden Bildern des Videostreams und wird ähnlich dem JPEG-Verfahren mit einer relativ geringen Kompressionsrate komprimiert.
Nach einem I-Frame folgen je nach eingestellter **GOP-Länge** ein oder mehrere P-Frames (Predicted Frames), die nur die Bewegungsvorhersagen und Differenzinformationen zu den vorherigen Bildern (I-Frame oder P-Frames) beinhalten (Long-Term Prediction).
Die Kompressionsrate bei P-Frames ist wesentlich höher als bei einem I-Frame, da Änderungen zu vorhergehenden Referenzbildern nur als Bewegungsvektoren kodiert werden müssen.
Die erforderliche Bitrate für P-Frames verringert sich also, sodass bei gegebener Gesamt-Encoding-Bitrate mehr Bits für das I-Frame zur Verfügung stehen. Somit kann die Qualität des I-Frames, wie beispielsweise die Detailwiedergabe, bei einer höheren **GOP-Länge** gesteigert werden.
Bei Szenen mit wenigen Bewegungsänderungen kann eine höhere **GOP-Länge** vorteilhaft sein, da die Kompressionseffizienz gesteigert wird.
Bei Szenen mit vielen Bewegungsänderungen kann eine hohe Anzahl von P-Frames jedoch die Bildqualität negativ beeinflussen, da die Bewegungsvorhersagen (Motion Predictions) immer ungenauer werden.

Je kleiner die **GOP-Länge** (d.h. mehr I-Frames, weniger P-Frames),

- desto weniger effektiv ist die Kompression.
- desto höher ist die Bildqualität.
- desto geringer ist die CPU-Auslastung während der Encodierung und Decodierung.
- desto höher sind die Anforderungen an Netzwerkbandbreite und Speicherplatz.
- desto flüssiger ist die Wiedergabe beim schnellen Vor- und Zurückspulen.

Je größer die **GOP-Länge** (d.h. weniger I-Frames, mehr P-Frames),

- desto effektiver ist die Kompression.
- desto geringer ist möglicherweise die Bildqualität bei Szenen mit vielen Bewegungsänderungen.
- desto höher ist die CPU-Auslastung während der Encodierung und Decodierung.
- desto geringer sind die Anforderungen an Netzwerkbandbreite und Speicherplatz.
- desto ruckeliger/abgehackter ist die Wiedergabe beim schnellen Vor- und Zurückspulen.

Die GOP endet vor dem nächsten I-Frame.
Aus den Bildern einer GOP werden später auf Decoder-Seite die sichtbaren Einzelbilder generiert.

> *Die **GOP-Länge: 1 I** (nur I-Frames) kennzeichnet eine sehr niedrige Kompressionsrate (ähnlich MJPEG). Sie sollte daher nur in sehr speziellen Ausnahmefällen verwendet werden, da der Bandbreiten- und Speicherplatzbedarf signifikant steigt.*
> *Beachten Sie auch, dass viele P-Frames innerhalb einer GOP (große **GOP-Länge**) möglicherweise zu Verzögerungen beim Einstieg in einen Stream oder zu Frame-Drops beim Rückwärts-Abspielen auf einigen Decodern führen können.*

### Auflösung

Diese Einstellung definiert die Ausgabeauflösung der generierten Bilder (Anzahl Bildpunkte bzw. Pixel in horizontaler und vertikaler Richtung).
Je nach Kameramodell und verbautem Bildsensor werden dabei verschiedene Ausgabeauflösungen unterstützt.

> *Detaillierte Informationen zu den verfügbaren Ausgabeauflösungen finden Sie in der Produktspezifikation des jeweiligen Kameramodells.*

### Weitwinkel

Diese Einstellung ist nur verfügbar, wenn die Ausgabeauflösung für **Stream 1** nicht auf die maximal nutzbare Sensorauflösung Ihres Kameramodells eingestellt ist.

Grundsätzlich wird der Bildwinkel in der geometrischen Optik durch das Aufnahmeformat (Format der Bildebene) und die eingestellte Brennweite am Objektiv bestimmt. Je nach gewählter Ausgabeauflösung für **Stream 1** und der damit ausgelesenen Sensorfläche (Aufnahmeformat) ändert sich daher in der Regel der Bildwinkel trotz gleichbleibender Brennweite und folglich auch der abgebildete Bildausschnitt der zu beobachtenden Szene.
Standardmäßig entspricht die Auflösung der ausgegebenen Bilder (gewählte Ausgabeauflösung) der Auflösung der verwendeten Sensorfläche (Anzahl ausgelesener Sensorpixel in horizontaler und vertikaler Richtung).
Die Funktion **Weitwinkel** hingegen bewirkt, dass auch bei niedrigeren Auflösungseinstellungen immer die gleiche Sensorfläche zur Bilderfassung verwendet wird wie bei der maximal verfügbaren Auflösung; in diesem Fall werden die ausgelesenen Sensorpixel jedoch nachträglich mittels „Downscaling“ auf die gewählte Zielauflösung herunterskaliert (siehe Beispiel unten). Da das Aufnahmeformat (die genutzte Sensorfläche) somit immer gleich bleibt, ändert sich auch der Bildwinkel bei gegebener Brennweite nicht mehr – unabhängig von der gewählten Ausgabeauflösung. Auf diese Weise kann der gleiche Bildausschnitt wie bei maximaler Auflösung auch mit einer geringeren Ausgabeauflösung abgebildet werden.

**Beispiel für Dome-Kamera RDF6400DN bei gegebener (gleichbleibender) Brennweite:**

Auflösung an **Stream 1**: 2688 × 1520 (maximal verfügbare Sensorauflösung)
Checkbox **Weitwinkel**: Nicht verfügbar, da der größtmögliche Bildwinkel bei gegebener Brennweite bereits vorliegt.
Ausgelesene Sensorpixel: 2688 × 1520
Ausgabeauflösung: 2688 × 1520

Auflösung an **Stream 1**: 720p (1280 × 720)
Checkbox **Weitwinkel**: Verfügbar aber **deaktiviert** -> Downscaling Off
Ausgelesene Sensorpixel: 1280 × 720
Ausgabeauflösung: 1280 × 720
-> Der Bildwinkel verkleinert sich im Vergleich zum Bildwinkel, der bei maximaler Auflösung vorliegt.

Auflösung an **Stream 1**: 720p (1280 × 720)
Checkbox **Weitwinkel**: Verfügbar und **aktiviert** -> Downscaling On
Ausgelesene Sensorpixel: **2688 × 1520**
Ausgabeauflösung: 1280 × 720
-> Der Bildwinkel entspricht dem Bildwinkel, der bei maximaler Auflösung vorliegt.

### Profil

Diese Einstellung ist nur für die Encodierung mit **H.264** verfügbar.

Das Profil **High** ist das am weitesten verbreitete und zugleich das effizienteste und leistungsfähigste **H.264**-Encodierungsprofil.
Im Gegensatz zum Profil **Main** verwendet es wesentlich komplexere Encodierungstechniken und ermöglicht dadurch sowohl einen etwas geringeren Bandbreitenbedarf für die Datenübertragung als auch einen etwas geringeren Speicherplatzbedarf für die Aufzeichnung von Videomaterial bei einer ebenso hohen Bildqualität.
Allerdings erfordert das Profil **High** mehr Prozessorkapazität bzw. CPU-Rechenleistung für die spätere Decodierung des Streams bzw. des aufgezeichneten Videomaterials als das Profil **Main**.

> *Das gewählte **H.264**-Encodierungsprofil muss auf Decoder-Seite unterstützt werden. In Verbindung mit Systemen und Applikationen von Dallmeier ist grundsätzlich das Profil **High** empfohlen.*

### Stream aktiv

Je nach Bedarf können mehrere Streams auf der Kamera aktiviert werden, die jeweils über unabhängige Einstellungsprofile verfügen. So kann beispielsweise ein Stream mit hoher Qualität und Bildrate für die Aufzeichnung konfiguriert werden, während ein anderer Stream für die bandbreitenschonende Live-Ansicht im lokalen Netzwerk optimiert wird.

# AUDIO

LIZENZ-CODE ERFORDERLICH

**Für dieses Feature ist der Erwerb eines Lizenz-Codes und ggf. zusätzlicher Hardware erforderlich.**

Weitere Informationen finden Sie in der Produktspezifikation zu Ihrer Kamera auf der Dallmeier Webseite unter https://www.dallmeier.com/.

Um einen gültigen Lizenz-Code für dieses Feature zu erwerben, wenden Sie sich an Ihren Dallmeier Vertriebspartner.

*Die Nutzung von Videosicherheitssystemen in Verbindung mit Audioübertragung und -aufzeichnung ist in der Regel streng reglementiert (v. a. in öffentlichen Bereichen). Informieren Sie sich vor dem Einsatz der bereitgestellten Audiofunktionen über die regional geltenden Gesetze, Vorschriften und Bestimmungen in Bezug auf Datenschutz und Persönlichkeitsrechte und stellen Sie deren Einhaltung sicher.*

Im Dialog **Audio** können Sie die Audioeinstellungen Ihrer Kamera nach Bedarf konfigurieren.

- Klicken Sie im Navigationsmenü den Menüeintrag **Audio**, um den entsprechenden Dialog zu öffnen.
- Beachten Sie die nachfolgenden Erklärungen zu den verschiedenen Registerkarten und Einstellungen.

## 8.1 AUDIOEINGANG

Der Audioeingang an der Kamera (Line-In oder integriertes Mikrofon, falls vorhanden) ermöglicht u. a. folgende Anwendungsszenarien:

- Übermittlung von individuellen Anliegen per Audio an den Operator (Bediener) des Videosicherheitssystems durch Personen, die sich vor oder in der Nähe der Kamera befinden, beispielsweise um Zutritt zu bestimmten Bereichen zu erhalten oder um auf besondere Vorkommnisse oder Zwischenfälle in der unmittelbaren Umgebung hinzuweisen, die sich nicht direkt im Sichtfeld der Kamera abspielen
- Audiovisuelle Aufzeichnung bei Vernehmungen von Zeugen oder Befragungen von mutmaßlichen Straftätern zusätzlich zu schriftlichen Protokollen für eine umfassendere Beweiserhebung bei Gerichtsverhandlungen
- Audiovisuelle Protokollierung bei der Aufnahme bzw. Einweisung von Patienten in forensisch-psychiatrische Ambulanzen oder für richterliche Entscheidungen hinsichtlich einer einstweiligen Anordnung der vorläufigen Unterbringung in einer psychiatrischen Einrichtung oder der Sicherungsverwahrung
- Bild- und Tonaufzeichnungen von Kundgebungen zu behördlichen Schulungszwecken
- Video- und Audiomitschnitte von Live-Events, Konferenzen, Vorträgen uvm.

Die Vielfalt an Anwendungsmöglichkeiten ist nahezu unbegrenzt – klären Sie jedoch unbedingt vorab, ob und unter welchen Bedingungen die Übertragung/Aufzeichnung von Audioinhalten zulässig ist!

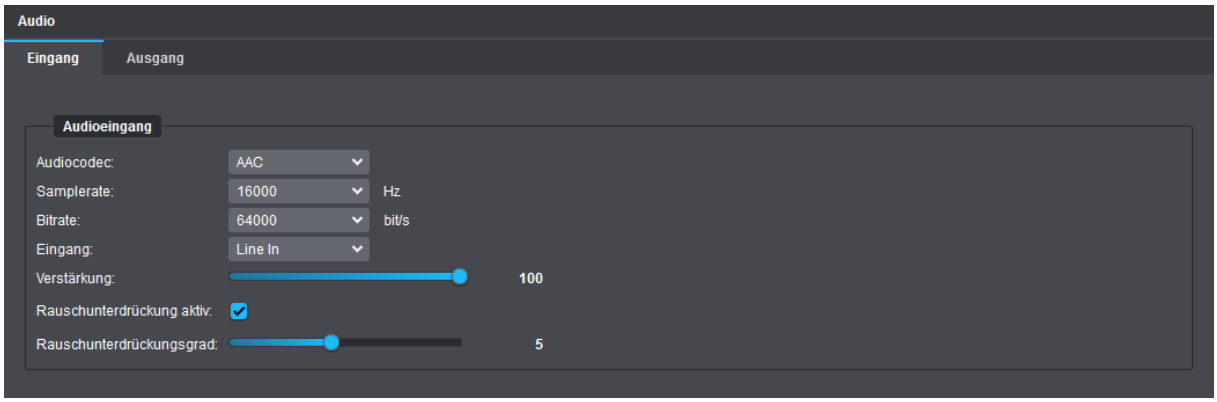


Abb. 8-1

### Audio-Codec

Diese Einstellung legt den Codec fest, der für die Codierung der Audiodaten (Audiodatenkompression) nach der Digitalisierung der eingehenden analogen Audiosignale (Analog-Digital-Wandlung) verwendet wird. Die folgenden Audioc-Codecs stehen dabei zur Auswahl:

- **G.711**
  Der Audio-Codec **G.711** ist in erster Linie für die **Codierung und Übertragung von Sprachdaten** bzw. Voice-over-IP (kurz: VoIP) **in ISDN-Qualität** vorgesehen und benötigt im Vergleich zu anderen Audio-Codecs nur relativ wenig CPU-Rechenleistung. Für die Kompression und Übertragung von hochwertigen Audiodaten wie beispielsweise Musik und Sound-Clips ist der **Sprachcodec G.711** hingegen nur bedingt geeignet.
  Die Datenkompression bei **G.711** entsteht ausschließlich durch Digitalisierung des analogen Audiosignals mittels Pulse Code Modulation (PCM) und Kompandierung (nach **A-LAW**- oder **µ-LAW**-Verfahren). Die Sample- bzw. Abtastrate für die zeitliche Diskretisierung im ersten Schritt der Analog-Digital-Wandlung beträgt **8 kHz** (8000 Samples pro Sekunde oder eine Messung alle 0,125 Millisekunden), die anschließende Quantisierung erfolgt nichtlinear mit **8 Bit**, was insgesamt zu einer Datenrate von **64 kBit/s** führt (8 kHz Abtastfrequenz × 8 Bit pro Abtastung).
  Die tatsächliche Datenübertragungsrate (benötigte Bandbreite) bei **G.711** nach der Codierung inklusive Overhead liegt bei etwa **80 kBit/s** bis **128 kBit/s**.
  Für die Codierung der Audiodaten können Sie je nach Land zwischen einem der beiden nachfolgenden Kompandierungsverfahren mit unterschiedlicher Quantisierungskennlinie wählen:

  - **A-LAW** (PCMA; verwendet in Europa und den meisten anderen Ländern)
  - **µ-LAW** (PCMU oder mu-law; üblicherweise verwendet in Nordamerika und Japan)

  Der Audio-Codec **G.711** empfiehlt sich generell nur für Anwendungen, bei denen die Übermittlung von Informationen mittels **Sprache in einfacher ISDN-Qualität** vorgesehen ist.

- **AAC** – Advanced Audio Coding
  Der Audio-Codec **AAC** eignet sich neben der **Codierung und Übertragung von gesprochenen Inhalten in hochwertiger Sprachqualität** insbesondere für die effiziente Komprimierung anspruchsvoller Audiodaten wie etwa Musik und Sounds in hoher klanglicher Präzision, Differenziertheit und Klanggüte (Wiedergabetreue).
  Die nach der Digitalisierung erzeugten Quelldaten werden durch ausgefeilte und komplexe Codierungsverfahren so reduziert, dass die Datenreduktion (Audiodatenkompression) bei der späteren Ausgabe vom menschlichen Gehör (psychoakustisch) nahezu nicht wahrnehmbar ist.
  Die Sample- bzw. Abtastrate und die Audio-Bitrate können nach Bedarf eingestellt werden (siehe im Folgenden).

### Samplerate

Diese Einstellung ist nur für den Audio-Codec **AAC** verfügbar.
Die Sample- bzw. Abtastrate definiert, wie oft pro Sekunde die kontinuierlichen Spannungsänderungen des eingehenden elektrischen Signals (analoges Audiosignal) für die Digitalisierung gemessen bzw. abgetastet werden (z. B. 48000 Mal pro Sekunde = 48 kHz).
Je höher die eingestellte Abtastrate für die zeitliche Diskretisierung ist, desto genauer kann das ursprüngliche analoge Signal digital abgebildet werden und desto besser (transparenter) ist später die Audioqualität bei gleicher Bitraten-Einstellung (siehe unten), aber umso höher ist auch die benötigte CPU-Rechenleistung für die darauffolgende Audiodatenkompression.

### Bitrate

Diese Einstellung ist nur für den Audio-Codec **AAC** verfügbar.
Der Begriff **Bitrate** beschreibt grundsätzlich das Verhältnis einer digitalen Datenmenge zu einer bestimmten Zeiteinheit und wird üblicherweise in Bit pro Sekunde angegeben (abgekürzt als Bit/s bzw. bit/s oder im Englischen als bps für „bit per second“), wobei oft das SI-Präfix Kilo vorangestellt wird (1 kBit/s = 1.000 Bit/s).
Die Audio-Bitrate gibt in diesem Zusammenhang die Anzahl von Bits an, mit denen der Audio-Encoder der Kamera die erzeugten digitalen Audiodaten pro Sekunde codiert, bevor diese Daten schließlich in komprimierter Form paketweise in das Netzwerk übertragen werden.
Je höher die eingestellte Audio-Bitrate bei gleichen Quelldaten und unveränderter Sample- bzw. Abtastrate (siehe oben) ist, desto besser ist in der Regel die spätere Audio-Ausgabequalität aufgrund der geringeren Kompressionsrate, aber desto höher ist auch der Bandbreitenbedarf für die Übertragung der codierten Audiodaten und der erforderliche Speicherplatz für die Aufzeichnung (bei gleicher Titel-/Spurlänge und identischem Original-Audioinhalt).
Allerdings hängt die Ausgabequalität von digitalem Audiomaterial nach einer Audiodatenkompression nicht zwangsläufig nur von der Höhe der gewählten Encoding-Bitrate ab, sondern immer auch von der Gesamtkomplexität und Dynamik des ursprünglichen Audiosignals bzw. der darin enthaltenen Frequenzspektren. Je komplexer das eigentliche analoge Signal ist, desto mehr Bitrate sollte dem Audio-Encoder für die Codierung bereitgestellt werden. Für weniger anspruchsvolle Audioinhalte können niedrigere Bitraten ausreichen, ohne dass die Qualität wahrnehmbar beeinträchtigt wird.

*Für eine hochwertige Audioübertragung und -aufzeichnung in DVD-Qualität werden eine **Samplerate** von **48 kHz** und eine **Bitrate** von **96 kBit/s** empfohlen.*

### Eingang

Diese Einstellung ermöglicht es zwischen einem integrierten **Mikrofon** mit niedrigem Pegel (falls hardwareseitig vorhanden) und einem angeschlossenen **Line-In**-Gerät mit relativ hohem Pegel wie beispielsweise einem externen Mikrofon mit Vorverstärker* zu wählen, wodurch eine korrekte Pegelverarbeitung der eingehenden analogen Audiosignale sichergestellt wird.

* Ein Mikrofon-Preamp hebt ein Mikrofonsignal auf Line-Pegel.

*Die Drop-down-Liste **Eingang** wird nur dann in der Registerkarte angezeigt, wenn Ihre Kamera über ein integriertes Mikrofon verfügt (ab Werk oder später nachgerüstet).*

### Verstärkung

Dieser Schieberegler dient zur Regelung der Signalverstärkung des eingehenden analogen Audiosignals vor der eigentlichen Digitalisierung und Codierung.

### Rauschunterdrückung

Diese Einstellung dient zur Minderung von möglichem Hintergrundrauschen im Ausgangssignal. Beachten Sie jedoch, dass ein zu hoch eingestellter **Rauschunterdrückungsgrad** zu Qualitätsverlust im verbleibenden Audiosignal führen kann.

#### Grundlegende Abfolge der Verarbeitung eingehender analoger Audiosignale

Eingehende analoge Audiosignale (z. B. Sprache) an der Kamera über Hardware-Audioeingang (Line-In) oder integriertes Mikrofon* -> A/D-Wandlung (Abtastung, Quantisierung) -> Codierung bzw. Audiodatenkompression mittels Audio-Codec -> Paketweise Übertragung (Streaming) der komprimierten Audiodaten in das Netzwerk.

* Schalldruckschwankungen werden mittels Mikrofon zunächst in elektrische Spannungsänderungen (analoge Audiosignale) umgesetzt.

## 8.2 AUDIOAUSGANG

Der analoge Audioausgang an der Kamera ermöglicht es dem Operator (Bediener) des Videosicherheitssystems, im Bedarfsfall aktiv, reaktionsschnell und situationsspezifisch mit Personen zu kommunizieren, die sich vor oder in der Nähe der Kamera befinden.

So sind u. a. die folgenden Anwendungsszenarien denkbar:

- Einzelne Besucher individuell und persönlich begrüßen und willkommen heißen
- Personen gezielt vor potentiellen Gefahrensituationen warnen (z. B. bei stärker werdender Auslastung von Engstellen auf Veranstaltungsgeländen durch erhöhtes Personenaufkommen)
- Spezifische akustische Hinweise bei unbewusstem oder vorsätzlichem Fehlverhalten von Personen vor Ort ausgeben, um Situation angemessen aufzulösen (z. B. bei unbefugtem Betreten gesicherter Bereiche oder dem Zurücklassen von abgelegtem Gepäck, Aktentaschen und anderen Gegenständen)
- Personengruppen oder Einzelpersonen frühzeitig auf mögliche verdächtige Handlungen aufmerksam machen (z.B. bei Herumlungern)

▶ Wählen Sie die Registerkarte **Ausgang**.

### 8.2.1 Lautstärke und Audio-Codec

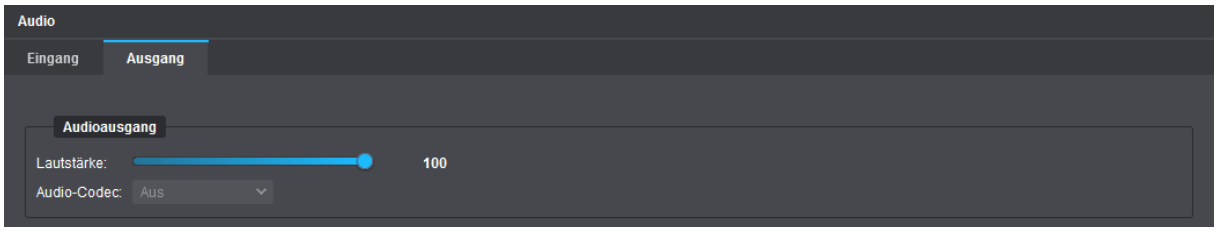


Abb. 8-2

**Lautstärke**
Dieser Schieberegler dient zur Regelung der Lautstärke bei der Ausgabe von decodierten Audiodaten als analoge Audiosignale auf einem angeschlossenen Lautsprecher mit integriertem Verstärker.

**Audio-Codec**
Empfangene Audiodaten (**G.711 A-LAW**/**µ-LAW** oder **AAC**) können von der Kamera in Echtzeit decodiert und anschließend als analoge Audiosignale über die hardwareseitig vorhandene Audio-Out-Schnittstelle ausgegeben werden (z. B. auf einem angeschlossenen Lautsprecher mit integriertem Verstärker).
Das **HEMISPHERE® SeMSy® Video Management System** oder **SeMSy® Compact** übertragen die Audiosignale (z. B. eingehend über den Mikrofonanschluss des Client-PCs) in digitalisierter Form mithilfe des Dallmeier Video-(**DaVid**-)Protokolls an die Kamera. Hierbei sind keine manuellen Einstellungen im Audio-Client (Audio-Decoder) der Kamera erforderlich, da die Auswahl des geeigneten Codecs automatisch erfolgt.

**Grundlegende Abfolge der Verarbeitung empfangener Audiodaten (über LAN zur Kamera gesendet)**

Client-Anwendung (z. B. **SeMSy® Compact**) sendet codierte Audiodaten paketweise über das Netzwerk an die Kamera -> Decodierung der komprimierten Audio-Datenströme mit passendem Audio-Codec -> D/A-Wandlung -> Ausgabe der analogen Audiosignale auf einem angeschlossenen Lautsprecher mit integriertem Verstärker.

## 8.2.2 Audiodatei

Neben der gezielten, vom Operator (Bediener) des Videosicherheitssystems manuell initiierten Audioausgabe über die hardwareseitig vorhandene Audio-Out-Schnittstelle an der Kamera (z. B. für individuelle Begrüßungen von Besuchern direkt über den Client-PC in der Sicherheitszentrale mittels Mikrofon und **SeMSy® Compact**) ermöglicht die Kamera auch die automatische, ereignisgesteuerte Wiedergabe von zuvor auf die Kamera hochgeladenen Audiosequenzen, um beispielsweise Eindringlinge automatisiert vor dem Betreten gesicherter Bereiche zu warnen.

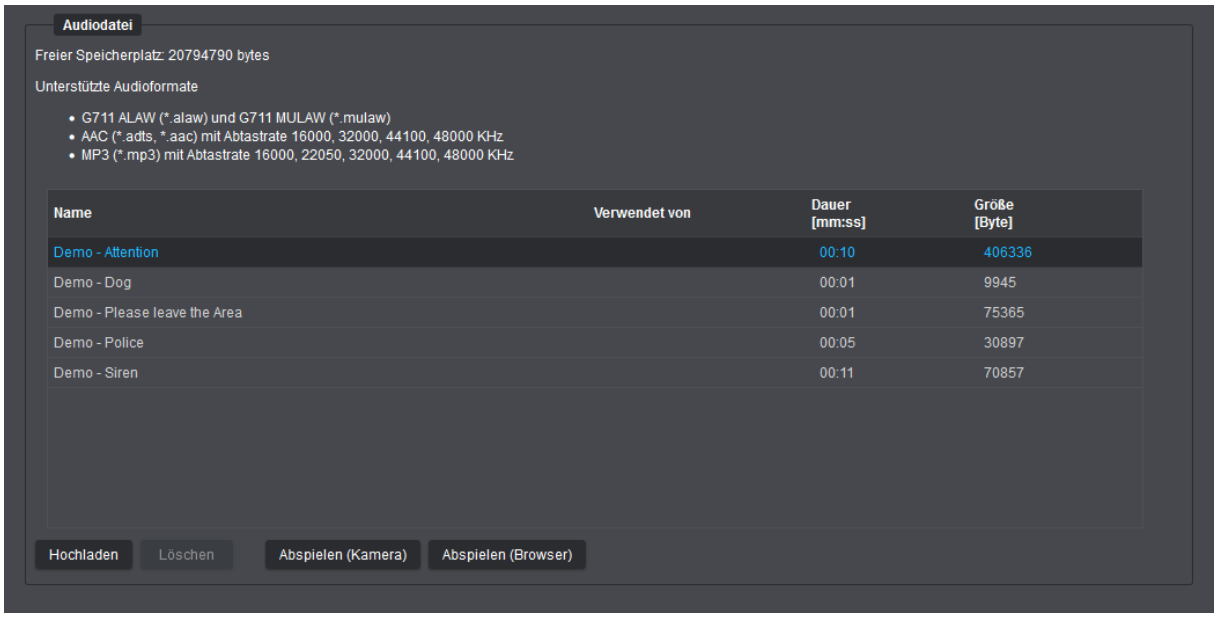


Abb. 8-3

Der Dialogbereich **Audiodatei** dient zum Hochladen und Verwalten von Audiosequenzen, wie z. B. eingesprochene automatische Begrüßungstexte und anderweitige häufig benötigte Durchsagen, Signal- und Alarmtöne oder jegliche sonstige Art von Sprach-, Musik- und Toneinspielungen.

Die Wiedergabe von Audiosequenzen über die Audio-Out-Schnittstelle an der Kamera kann dann entweder manuell durch Klicken der Schaltfläche **Abspielen (Kamera)** gestartet werden oder automatisch durch Eintreten eines oder mehrerer der folgenden Ereignisse ausgelöst werden:

- Zustandsänderung eines Kontakt-Eingangs an der Kamera
- Ereignis auf Basis von **EdgeAnalytics** erkannt:
  - Line Crossing (Objekt hat eine virtuelle Linie überquert)
  - Intrusion Detection (Objekt hat einen sensitiven Bereich betreten/verlassen)
  - Loitering (Erkennung von herumlungernden Personen wurde begonnen oder beendet)

Für Testzwecke können Audiosequenzen auch direkt im Webbrowser abgespielt werden (Schaltfläche **Abspielen (Browser)** klicken).

> *Ab Werk sind bereits verschiedene Audiosequenzen auf die Kamera hochgeladen. Diese können nicht gelöscht werden. Beachten Sie zudem vor dem Upload von Audiodateien die Angaben im Kameradialog zu den aktuell unterstützten Audio-Codecs und Container- bzw. Datei-Formaten sowie zu den gegebenenfalls möglichen Qualitätsstufen (Sample- bzw. Abtastraten).*

# DATUM & UHRZEIT

Die Systemzeit der Kamera kann entweder manuell eingestellt oder mit einem NTP-Zeitserver synchronisiert werden.

## 9.1 MANUELLE KONFIGURATION

*Beachten Sie, dass eine manuelle Konfiguration nicht möglich ist, wenn die Synchronisation mit einem NTP-Zeitserver eingeschaltet ist.*

- Klicken Sie im Navigationsmenü den Menüeintrag **Uhrzeit**.

Die Registerkarte **Uhrzeit** wird angezeigt.

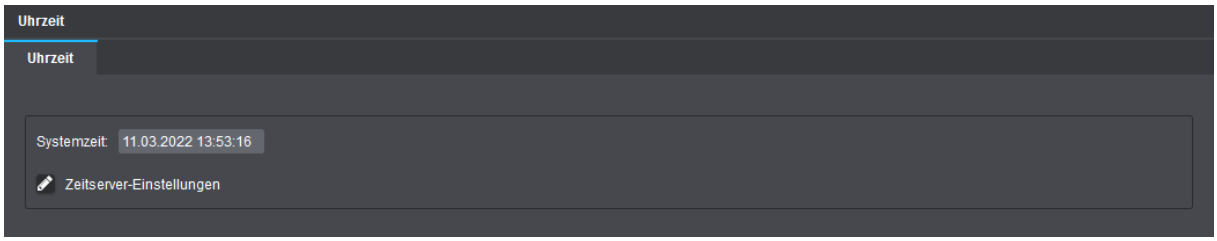


Abb. 9-1

- Klicken Sie in das Feld **Systemzeit**.
- Nehmen Sie die erforderlichen Einstellungen vor.
- Bestätigen Sie abschließend mit **Fertig**.

Die eingestellte Zeit wird daraufhin als neue Systemzeit übernommen.

## 9.2 ZEITSERVER-EINSTELLUNGEN

Beschreibungen zu den **Zeitserver-Einstellungen** finden Sie im Abschnitt „Zeitserver“ auf Seite 57.

# NETZWERK

## 10.1 GRUNDLEGENDE EINSTELLUNGEN

Die Netzwerkeinstellungen des Geräts können manuell konfiguriert oder von einem DHCP-Server (Dynamic Host Configuration Protocol Server) automatisch zugewiesen werden.

*ACHTUNG*

**Netzwerkkonflikte aufgrund ungültiger oder nicht korrekter IP-Adresse**

Um Netzwerkkonflikte zu vermeiden, sollten Sie vorab klären, ob die vorgesehenen Netzwerkeinstellungen zulässig sind. Insbesondere die Vergabe einer bereits belegten IP-Adresse kann zu Fehlfunktionen führen.

▶ Klicken Sie **Netzwerk** > **Grundlegende Einstellungen**.

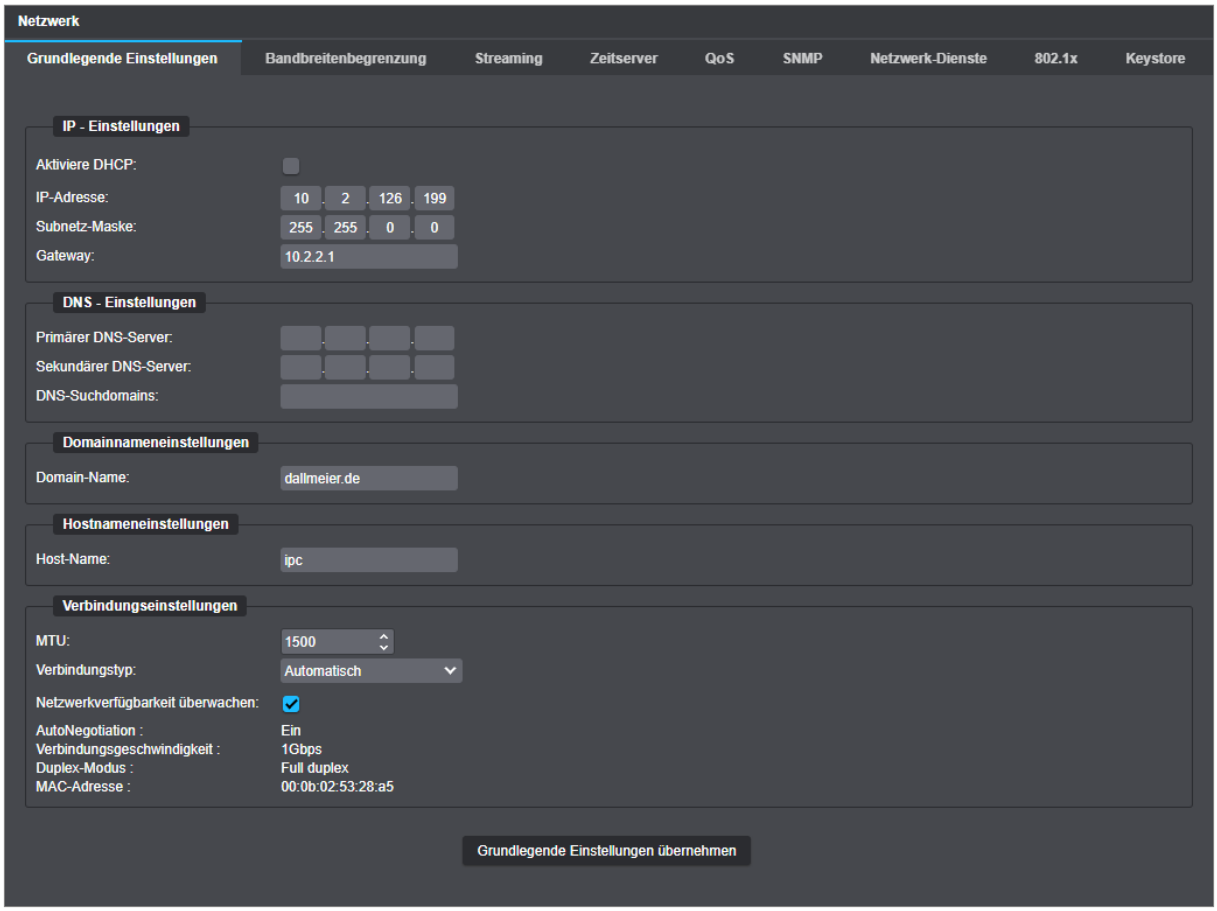


Abb. 10-1

### Werkseinstellungen

| | |
|---|---|
| Aktiviere DHCP: | `deaktiviert` |
| IP-Adresse: | `192.168.2.28` |
| Subnetz-Maske: | `255.255.255.0` |
| Gateway: | `192.168.2.1` |

**ACHTUNG**

**Netzwerkverbindungsfehler durch fehlerhafte Konfigurationseinstellungen**

Durch fehlerhafte Einstellungen kann das Gerät möglicherweise nicht mehr über das Netzwerk erreichbar sein.

- Kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung.
- Notieren Sie sich zu Zwecken der Problembehebung vor Änderung der Konfiguration die **MAC-Adresse** sowie alle neuen Einstellungen.

---

- Beachten Sie die nachfolgenden Erklärungen.
- Konfigurieren Sie die erforderlichen Netzwerkeinstellungen.
- Klicken Sie auf **Grundlegende Einstellungen übernehmen**, um die Einstellungen zu übernehmen.

*Die Schaltfläche **Grundlegende Einstellungen übernehmen** wird erst aktiv, wenn alle notwendigen Daten eingegeben sind.*

### IP-Settings

**Aktiviere DHCP**

Siehe „Automatisches Zuweisen der Netzwerkeinstellungen durch DHCP“ auf Seite 53.

**IP-Adresse**

Manuelle Eingabe der (statischen) IP-Adresse für die Kamera.

**Subnetz-Maske**

Manuelle Eingabe der Subnetz-Maske, in dem sich das Gerät befindet. Anhand der IP-Adresse und Subnetz-Maske kann festgestellt werden, ob sich Netzwerkgeräte im selben Teilnetz befinden und direkt miteinander kommunizieren können oder ob diese in verschiedenen Netzwerken liegen und ein Router den Datenverkehr zwischen den Netzwerkgeräten regeln muss.

**Gateway**

Manuelle Eingabe des Standard-Routers (Default-Gateway). Diese Angabe ist notwendig, um aus verschiedenen Subnetzen auf die Kamera zugreifen zu können.

### DNS-Settings, Domainname-Settings und Hostname-Settings

Da IP-Adressen relativ schwer zu merken sind, können Sie auf IP-Geräte auch mithilfe von sogenannten Host-Namen verweisen, was Ihnen ein wesentlich leichteres Auffinden von IP-Geräten bzw. Hosts im lokalen Netzwerk (LAN) erlaubt.

Das Mapping (die Namensauflösung) von Host-Namen in die jeweils zugehörigen IP-Adressen wird vom sogenannten Domain Name Service durchgeführt (DNS-Server erforderlich).
Darüber hinaus kann die Namensauflösung von IP-Adressen, also die Umsetzung der Host-Namen zu IP-Adressen, direkt in der Hosts-Datei auf Ihrem lokalen Rechner hinterlegt und gespeichert werden.

Der **Host-Name** (oder zutreffender der kurze Host-Name) bestimmt den eigentlichen Rechner- bzw. Gerätenamen (z. B. `myhostname`).
Der **Domain-Name** ist üblicherweise die Netzwerk-Domäne innerhalb des lokalen Netzwerks (LAN) Ihres Unternehmens bzw. Ihrer Abteilung (z. B. `example.com` oder `intranet.example.com`).

Host-Namen werden durch spezielle DNS-Server (besser bekannt als Name-Server) aufgelöst.
Die Auflösung von Host-Namen in IP-Adressen erfordert die Zuweisung eines primären Name-Servers (**Primärer DNS-Server,** z. B. `ns1.example.com`) und aus Gründen der Ausfallsicherheit und Verfügbarkeit die Zuweisung eines sekundären Name-Servers (Sekundärer DNS-Server, z. B. `ns2.example.com`).

Um sich beispielsweise mit dem IP-Gerät mithilfe seines langen Host-Namens bzw. vollständigen Domain-Namens (Fully Qualified Domain Name, kurz FQDN) zu verbinden, können Sie ganz einfach `myhostname.example.com` verwenden.
Je nach Einstellungen des DNS-Servers bzw. der Hosts-Datei können Sie zur Verbindung mit dem IP-Gerät auch nur dessen kurzen Host-Namen (hier: `myhostname`) verwenden.

**DNS-Suchdomains** (max. 5 erlaubt, durch Leerzeichen getrennt) sind dann hilfreich, wenn sich beispielsweise ein definierter Alarm-Host oder NTP-Zeitserver nicht in der von Ihnen angegebenen Netzwerk-Domäne (**Domain-Name**) befindet.

### Link-Settings

Unter **Link-Setting**s lassen sich diverse Einstellungen in Bezug auf das Netzwerkprotokoll treffen sowie die aktuellen Werte für Verbindungsgeschwindigkeit, Duplex-Modus und MAC-Adresse ablesen.

#### MTU

Die MTU bestimmt die maximale Paketgröße von TCP/IP-Paketen, die vom Gerät versendet werden (Standard: 1500 Byte, Maximalgröße für Ethernet-Standard). Eine große MTU liefert normalerweise den besten Datendurchsatz, eine kleinere MTU führt hingegen zu stärkerer Paket-Fragmentierung sein. Stark fragmentierte Pakete werden unter Umständen von Routern oder Firewalls nicht weitergeleitet.

#### Verbindungstyp

Diese Einstellung bestimmt die Übertragungsrate und den Duplex-Modus zwischen dem Network Interface Controller (NIC) der Kamera und dem des verbundenen Ethernet-Netzwerkports eines Routers, Hubs oder Switches. Die Einstellung **Automatisch** (Autonegotiation) ist für die meisten Anwendungsfälle die empfohlene Einstellung.
Das Autonegotiation-Verfahren erlaubt es zwei miteinander verbundenen Netzwerkkomponenten oder einem Endgerät, die maximal mögliche Übertragungsgeschwindigkeit und das Duplex-Verfahren selbstständig auszuhandeln und zu konfigurieren.

#### MAC-Adresse

Hier wird die Hardware-Adresse (physikalische Adresse) der Kamera angezeigt. Die MAC-Adresse dient der eindeutigen Identifikation des Geräts im Netzwerk und kann nicht geändert werden.

**Automatisches Zuweisen der Netzwerkeinstellungen durch DHCP**
Um die Netzwerkeinstellungen automatisch von einem DHCP-Server zuweisen zu lassen, gehen Sie folgendermaßen vor:

- Stellen Sie sicher, dass ein aktiver DHCP-Server in Ihrem lokalen Netzwerk (LAN) erreichbar ist.

> *Kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung.*

- Aktivieren Sie die Checkbox **Aktiviere DHCP**.

Die IP-Adresse, Subnetz-Maske und Gateway-Adresse können dann nicht mehr manuell festgelegt werden, sondern werden nach Speicherung der Netzwerkeinstellungen vom zentralen DHCP-Server automatisch zugewiesen.

> *Um vom DHCP-Server empfangene Einstellungen zu ignorieren, können Sie die entsprechenden Checkboxen unter **DNS-Settings**, **Domainname-Settings** oder **Hostname-Settings** deaktivieren und die erforderlichen Werte eingeben.*

- Falls erforderlich, konfigurieren Sie die verfügbaren DNS-Einstellungen (siehe Abschnitt „DNS-Settings, Domainname-Settings und Hostname-Settings“ auf Seite 51).
- Bestätigen Sie abschließend mit **OK**.

Die Verbindung zum Gerät wird daraufhin beendet und die neuen Netzwerkeinstellungen werden vom DHCP-Server automatisch zugewiesen (Lease-Dauer beachten).

> *Nach Änderung der Netzwerkeinstellungen müssen Sie sich erneut mit dem Gerät verbinden (mit neu zugewiesener IP-Adresse):*

Die neu zugewiesene IP-Adresse kann mithilfe der MAC-Adresse des Geräts in der Dallmeier Software PService oder auf dem DHCP-Server ermittelt werden.
PService muss im gleichen LAN ausgeführt werden, in dem sich das Gerät befindet.

**Manuelle Zuweisung der Netzwerkeinstellungen**

- Beachten Sie zunächst die festgelegten und gültigen IP-Adressbereiche in Ihrem Netzwerk.

> *Kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung.*

- Stellen Sie sicher, dass die Checkbox **Aktiviere DHCP** deaktiviert ist.
- Geben Sie die **IP-Adresse** ein, die Sie dem Gerät zuweisen möchten.
- Geben Sie die **Subnetz-Maske** ein.

- Geben Sie die **Gateway**-Adresse ein.
- Falls erforderlich, konfigurieren Sie die verfügbaren DNS-Einstellungen (siehe Abschnitt „DNS-Settings, Domainname-Settings und Hostname-Settings“ auf Seite 51).
- Bestätigen Sie abschließend mit **OK**.

Die Verbindung zum Gerät wird daraufhin beendet und die neuen Netzwerkeinstellungen werden übernommen.

*Nach Änderung der Netzwerkeinstellungen müssen Sie sich erneut mit dem Gerät verbinden (mit neu zugewiesener IP-Adresse).*

## 10.2 BANDBREITENBEGRENZUNG

Die Bandbreitenbegrenzung legt eine Obergrenze in Mbit/s für die Datenübertragungsrate der einzelnen Streams der Kamera fest.

Die Begrenzung der Bandbreite (maximal zulässige Bitraten-Spitzen) kann hilfreich sein, um Videoartefakte oder Frame-Drops (Verlust einzelner Bilder) zu verhindern, die durch Paketverluste bei Verbindungen mit geringen Bandbreiten auftreten können.

- Klicken Sie **Netzwerk** > **Bandbreitenbegrenung**.

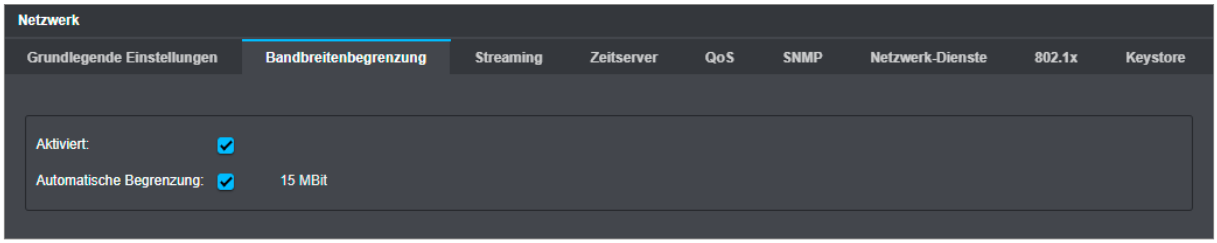


Abb. 10-2

- Klicken Sie die Checkbox **Aktiviert**, um die Bandbreitenbegrenzung zu aktivieren.
- Beachten Sie die folgenden Optionen.

**Manuelle Einstellung**
Legen Sie den Wert für die Spitzenbandbreite mit dem dazugehörigen Schieberegler fest.
Bestätigen Sie mit **OK**.

**Automatische Einstellung**
Wenn die Checkbox **Automatisches Limit** aktiviert ist, wählt die Kamera automatisch die maximal zulässige Spitzenbitrate aus und berücksichtigt dabei die höchste gewählte Bitrate, so dass eine reibungslose Liveübertragung gewährleistet ist.

- Aktivieren Sie die Chebox **Automatisches Limit**.
- Bestätigen Sie mit **OK**.

## 10.3 STREAMING

Der (statische) Video Server ermöglicht eine kontinuierliche Übertragung (Streaming) der erzeugten Videodaten in das Netzwerk, ohne dass die Daten aktiv von einer Applikation angefordert werden.

- Klicken Sie **Netzwerk** > **Streaming**.

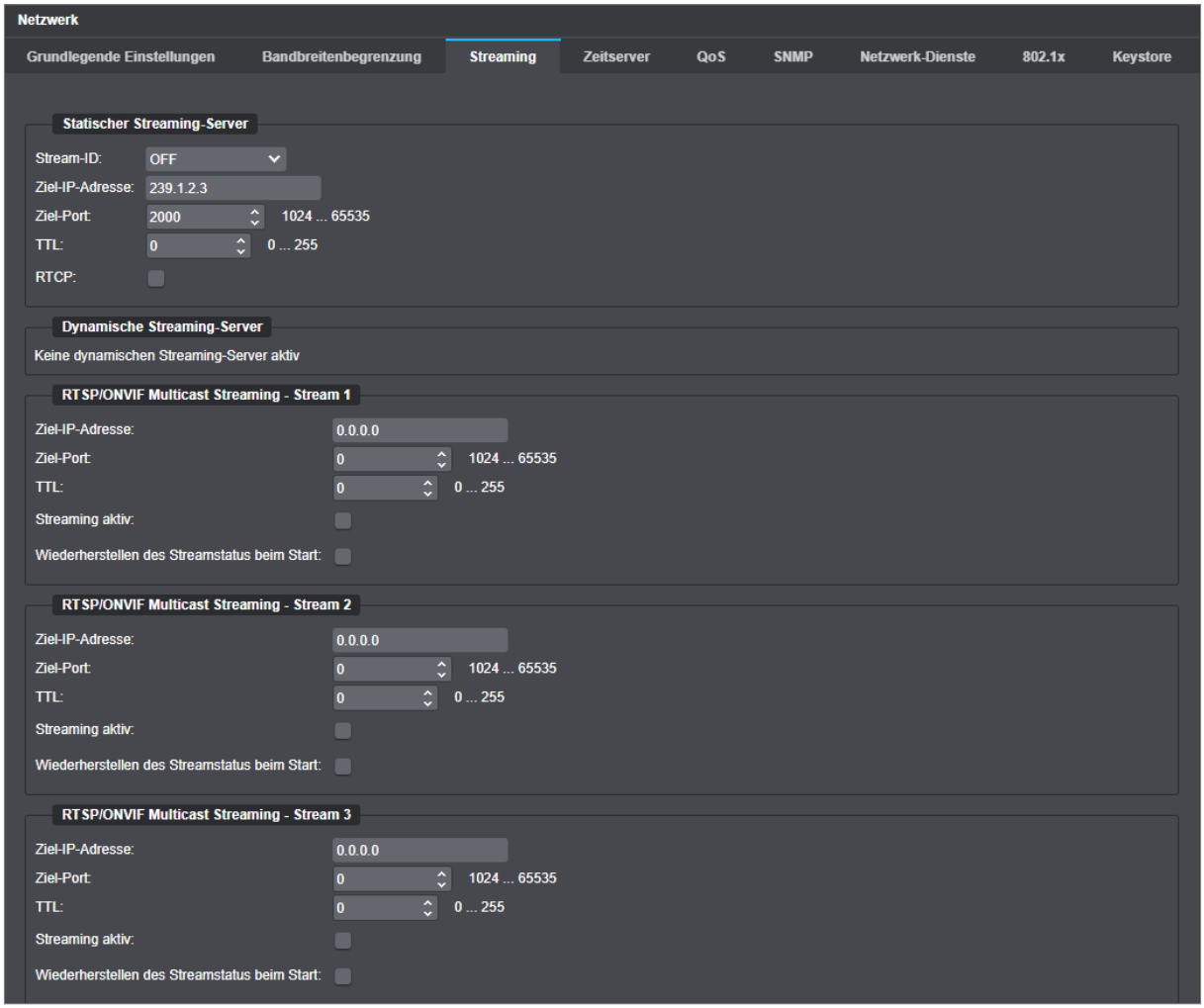


Abb. 10-3

### Statischer Streaming-Server

- Beachten Sie die nachfolgenden Erklärungen.
- Wählen Sie einen Encoder aus der Drop-down-Liste **Stream-ID**.
- Geben Sie die **Ziel-IP-Adresse** ein.
- Geben Sie im Feld **Ziel-Port** die Portnummer des Dienstes ein, der die IP-Datenpakete erhalten soll.
- Geben Sie den TTL-Wert für IP-Pakete im Feld **TTL** ein.
- Aktivieren Sie die Checkbox **RTCP**, falls erforderlich.
- Bestätigen Sie abschließend mit **OK**.

Je nach Typ der verwendeten Ziel-IP-Adresse ändert sich das Übertragungsverfahren beziehungsweise die Verteilung der Datenpakete im Netzwerk:

**Ziel-IP-Adresse (Multicast)**
Mithilfe der Multicast-Technologie kann ein einzelner Stream für mehrere Ziele oder Empfänger im Netzwerk repliziert werden, ohne dass der Quell-Host mehrere Kopien desselben Streams für die unterschiedlichen Ziel-Hosts erstellen muss. Der Netzwerkdatenverkehr kann somit wesentlich optimiert und die Performance-Auslastung des sendenden Hosts erheblich reduziert werden.

*Bevor Sie IP-Multicasting nutzen können, müssen Sie sicherstellen, dass die empfangenden Hosts und die lokalen Router/Switches in Ihrem Netzwerk IP-Multicasting unterstützen und korrekt konfiguriert sind.*

- Kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung.

Bei Multicast-Übertragungen werden die Datenpakete mit einer speziellen IP-Multicast-Gruppenadresse versehen und über eine sogenannte Punkt-zu-Mehrpunkt-Verbindung an eine Gruppe von Empfängern (Multicast-Gruppe) versendet.
Im Gegensatz zu Unicast müssen die Datenpakete nur einmal vom Quell-Host versendet werden; die Vervielfältigung der Pakete und Weiterleitung an die einzelnen Mitglieder der Gruppe (Ziel-Hosts) wird von speziell konfigurierten (Multicast-fähigen) Routern/Switches ausgeführt.
Um periodisch festzustellen, ob registrierte Mitglieder einer Multicast-Gruppe noch aktiv sind, müssen Multicast-Switches verwendet werden, die IGMP-Snooping (in IPv4) oder MLD-Snooping (in IPv6) unterstützen. Dadurch kann die Auslastung des Netzwerks weiter reduziert werden, da Multicast-Datagramme nur an diejenigen Empfänger weitergeleitet werden, die sie empfangen möchten (also ihre Multicast-Gruppenzugehörigkeit zyklisch bekanntgeben).

Eine Gruppe von Endpunkten (Multicast-Gruppe) wird durch eine einzelne IP-Multicast-Gruppenadresse identifiziert: Multicast verwendet den Adressbereich der Klasse D von 224.0.0.0 bis 239.255.255.255 (ausgedrückt als 224.0.0.0/4 in im Netzwerk-Prefix oder der CIDR-Notation – Classless Inter-Domain Routing).

*Beachten Sie, dass bestimmte Multicast-Adressbereiche für spezielle Zwecke reserviert sind. Für den lokalen Einsatz wird die Verwendung der Adressen im Bereich von 239.0.0.0 bis 239.255.255.255 empfohlen, da dieser Adressbereich als nicht öffentlich gekennzeichnet ist und nicht ins Internet weitergeleitet (geroutet) wird.*

Die Adressangaben sind unverbindlich. Beachten Sie daher immer die aktuellen Spezifikationen und Richtlinien zu den einzelnen Adressbereichen.

- Kontaktieren Sie gegebenenfalls die für Ihre Netzwerkadministration zuständige Person für weitere Informationen und zu Ihrer Unterstützung.

*Beschreibungen zu Multicast und empfohlene Switche für Dallmeier Systeme finden Sie in den Dallmeier Whitepapers „Switch-Basics“ und „Switch-Whitelist“ auf der Dallmeier Webseite unter https://www.dallmeier.com/.*

**Ziel-IP-Adresse (Unicast)**
Die Datenpakete werden mit einer bestimmten IP-Adresse und Portnummer versehen und über eine Punkt-zu-Punkt-Verbindung an genau einen Empfänger (Client) versendet.

Der Empfänger erhält die Datenpakete nur, wenn der entsprechende Anwendungsdienst über die festgelegte Portnummer erreichbar ist.

**TTL**
Der TTL-Wert (Time To Live) legt die Lebensdauer eines IP-Pakets fest.
Jeder Router, den ein IP-Paket passiert, verringert den TTL-Wert um 1.
Wenn der Wert 0 (Null) erreicht ist, wird das IP-Paket verworfen.
Zum einen wird dadurch verhindert, dass IP-Pakete aufgrund von Routing-Fehlern endlos im Netzwerk kreisen, zum anderen, dass IP-Pakete die Grenzen des LAN (Local Area Network) durchbrechen und in das WAN (Wide Area Network) gesendet werden (TTL = 1).

Je nach Anforderung kann ein TTL-Wert von 1 – 255 eingegeben werden. Bei Eingabe von 0 (Null) werden die Default-Werte verwendet (TTL = 1 bei Multicast, TTL = 64 bei Unicast).

**RTCP**
Das Real-Time Transport Control Protocol (RTCP) ist eine Erweiterung des Real-Time Transport Protocol (RTP) und dient unter anderem zur Übermittlung von periodischen Statusinformationen, wie beispielsweise Zeitstempel der übertragenen Videoströme.

## 10.4 ZEITSERVER

*Beachten Sie, dass der von Ihnen angegebene NTP-Zeitserver ständig über das Netzwerk erreichbar sein muss.*

- Klicken Sie **Netzwerk** > **Zeitserver**.

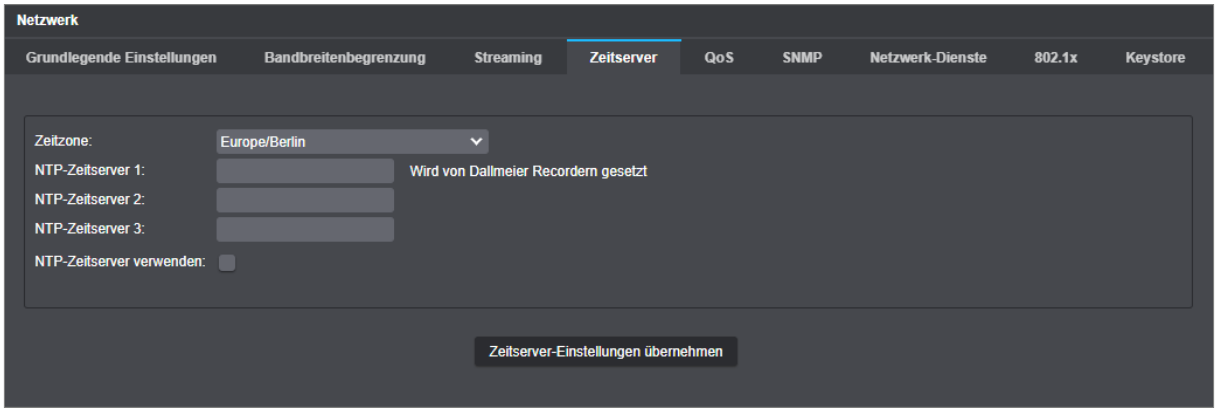


Abb. 10-4

- Legen Sie die **Zeitzone** fest.
- Geben Sie die IP-Adresse des **NTP-Zeitserver** ein.
- Aktivieren Sie die Checkbox **NTP-Zeitserver** verwenden.
- Bestätigen Sie mit **Zeitserver-Einstellungen übernehmen**.

*Die Schaltfläche **Zeitserver-Einstellungen übernehmen** wird erst aktiv, wenn alle notwendigen Daten eingegeben sind.*

Die Synchronisation mit dem angegebenen NTP-Zeitserver wird aktiviert.

## 10.5 QUALITY OF SERVICE

Die Funktion **Quality of Service** kennzeichnet die Datenpakete des Videostroms mit einem speziellen DSCP-Code.
Während der Übertragung über das Netzwerk erkennen die Switches diese Datenpakete und weisen ihrer Übertragung die höchste Priorität zu. Bei Lastspitzen reduziert ein Switch die Bandbreite für andere Datenpakete (E-Mail, VoIP, FTP, etc.) und erhöht automatisch die Bandbreite für den Videostream. Dadurch wird ein Datenstau vermieden und alle Datenpakete erreichen den Client zur reibungslosen Darstellung des Videostroms nahezu in Echtzeit.

*Beachten Sie, dass die bevorzugte Übertragung von Videostreams andere Dienste (E-Mail, VoIP, FTP usw.) erheblich stören kann.*
*Die Nutzung von **Quality of Service** sollte immer mit der für Ihre Netzwerkadministration zuständigen Person besprochen werden.*

### UDP Video und Audio QoS DSCP Setup

Der DSCP-Code identifiziert den Datentyp und das Weiterleitungsverhalten des Switches. Ein höherer DSCP-Code bedeutet daher keine höhere Priorität, sondern identifiziert einen anderen Datentyp mit einem anderen Weiterleitungsverhalten. In Verbindung mit Cisco Catalyst Switches beispielsweise muss für Videostreams immer der DSCP-Code 32 verwendet werden.

► Klicken Sie **Netzwerk** > **QoS**.

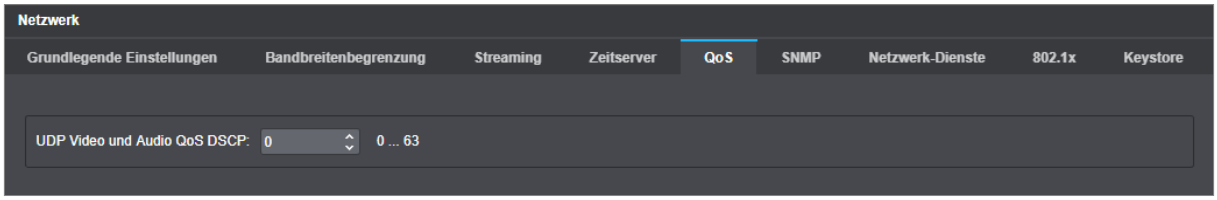


Abb. 10-5

► Geben Sie den korrekten **UDP Video- und Audio-QoS-DSCP-Code** ein (siehe oben).

## 10.6 SNMP

Das Simple Network Management Protocol (SNMP) ist ein Netzwerkpotokoll zur Überwachung und Steuerung von Netzwerkelementen mithilfe eines Netzwerk-Management-Systems (NMS). Das Protokoll wird aktuell in drei verschiedenen Versionen unterstützt.

- Klicken Sie **Netzwerk** > **SNMP**.

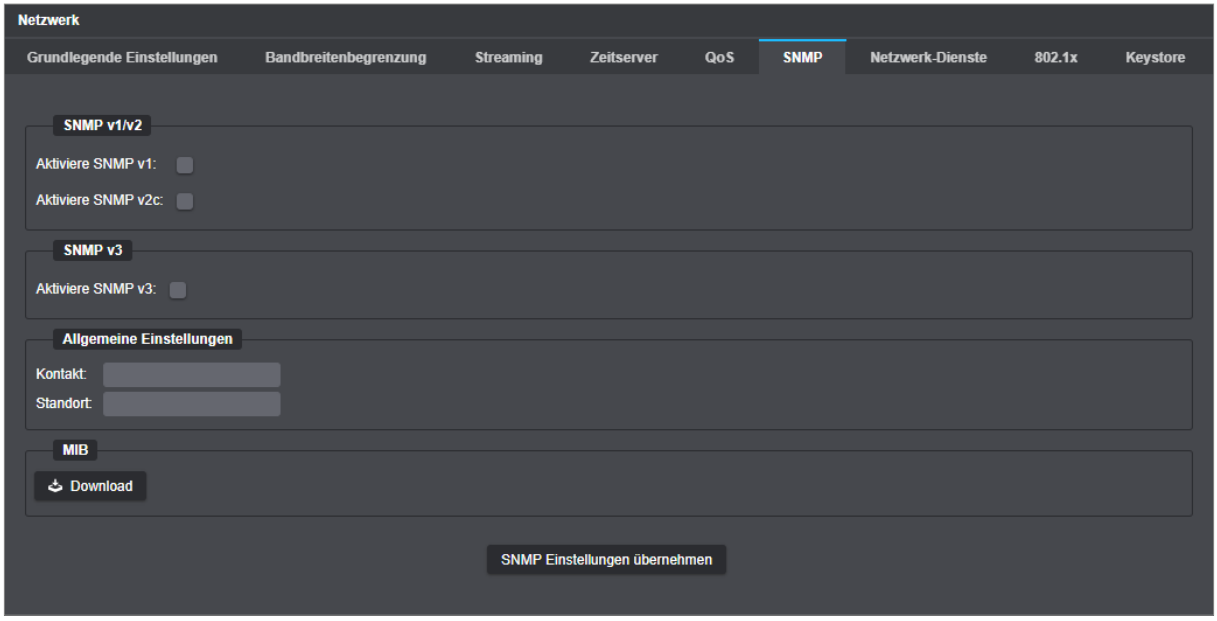


Abb. 10-6

- Nehmen Sie die notwendigen Einstellungen vor (siehe unten).
- Bestätigen Sie mit **SNMP Einstellungen übernehmen**.

> *Die Schaltfläche **SNMP Einstellungen übernehmen** wird erst aktiv, wenn alle notwendigen Daten eingegeben sind.*

> *Die gewählte SNMP-Version muss mit derjenigen Ihres verwendeten Netzwerk-Management-Systems (NMS) übereinstimmen.*

### SNMP v1/v2c

SNMP v1/v2c sind zwar verbreitet, bieten aber keine ausreichende Sicherheit, und sollten somit nach Möglichkeit nicht verwendet werden.

> *Beachten Sie, dass Community-Strings (die als eine Art Passwort dienen) bei SNMP v1/v2c im Klartext übertragen werden und von jedem im Netzwerk „mitgehört“ werden können.*

- Aktivieren Sie die Checkbox der erforderlichen SNMP-Version.
- Geben Sie den zu verwendenden **Community**-String (Default: public) in das entsprechende Feld ein.

### SNMP v3

SNMP v3 bietet als Sicherheitsmaßnahmen eine SNMP-Benutzer- und Passwortabfrage, sowie eine Verschlüsselung der Daten bei der Übertragung.

- ► Aktivieren Sie die Checkbox **Aktiviere SNMP v3**.
- ► Geben Sie den zu verwendenden SNMP-Benutzernamen in das Feld **User** ein.
- ► Wählen Sie die erforderliche Authentifizierungsart aus der Drop-down-Liste **Authentifizierung** aus (siehe unten).
- ► Wählen Sie die erforderliche Verschlüsselungsart aus der Drop-down-Liste **Verschlüsselung** aus (siehe unten).

**Authentifizierung**

Es stehen drei Authentifizierungsarten zur Auswahl:

- **OFF**
  Keine Authentifizierung (nur Angabe des SNMP-Benutzernamens erforderlich)
- **MD5**
  Hash-Authentifizierung (HMAC) mit Message-Digest Algorithm 5 (Passwort mindestens 8 Zeichen)
- **SHA**
  Hash-Authentifizierung (HMAC) mit Secure Hash Algorithm (Passwort mindestens 8 Zeichen)

**Verschlüsselung**

Es kann aus drei Arten zur Übertragungsverschlüsselung der Daten gewählt werden:

- **OFF**
  Keine Übertragungsverschlüsselung der Daten
- **DES**
  Data Encryption Standard (Passwort der Verschlüsselung mindestens 8 Zeichen)
- **AES**
  Advanced Encrpytion Standard (Passwort der Verschlüsselung mindestens 8 Zeichen)

### Allgemeine Einstellungen

Diese Sektion dient zur Angabe der Kontaktperson (E-Mail-Adresse) und des Standorts (z. B. 3. Stock) des zu verwaltenden SNMP-Agenten (dieses Gerät).

- ► Geben Sie die entsprechenden Informationen in die Felder **Kontakt** und **Standort** ein.

**Benutze INFORM für TRAP**

Falls der Adressat der SNMP-Nachricht eine Rückmeldung über deren Eingang senden soll, kann von TRAP auf INFORM umgestellt werden.

- ► Aktivieren Sie die Checkbox **Benutze INFORM für TRAP**, falls erforderlich.

### Trap Optionen

Folgende SNMP-Status-Meldungen (Traps) können selbständig von der Kamera zum Server geschickt werden:

- **Cold start**
  Meldung, wenn der SNMP-Agent startet
- **Warm start**
  Meldung, wenn der SNMP-Agent die Konfiguration neu lädt
- **Shutdown**
  Meldung, wenn der SNMP-Agent gestoppt wird
- **Authentification failure**
  Meldung, wenn der Zugriff auf den SNMP-Agent ohne Berechtigung versucht wird
- **Link up**
  Meldung, wenn das Netzwerk nach Ausfall wieder verfügbar ist
- **LLDP**
  Meldung bei jeder Änderung der über LLDP/CDP erkannten Netzwerkteilnehmer

Zudem können die folgenden Informationen über das Gerät abgefragt werden:

- IP-MIB: Internet protocol (IP-Konfiguration)
- HOST-RESOURCES-MIB: hrSystemUptime (System Uptime)
- HOST-RESOURCES-MIB: hrSystemDate (Systemzeit/-datum)
- UCD-SNMP-MIB: Memory Statistics (RAM-Auslastung)
- UCD-SNMP-MIB: CPU Statistics (CPU-Auslastung)
- UCD-SNMP-MIB: Load Average Information (durchschnittliche CPU-Auslastung)

### MIB

Um Informationen über weitere mögliche Abfragen zu erhalten, kann die MIB-Datei heruntergeladen werden.

► Klicken Sie **Download**, um die MIB-Datei herunterzuladen, falls erforderlich.

## 10.7 NETZWERK-DIENSTE

### Werkseinstellungen

ONVIF: deaktiviert
RTSP: deaktiviert

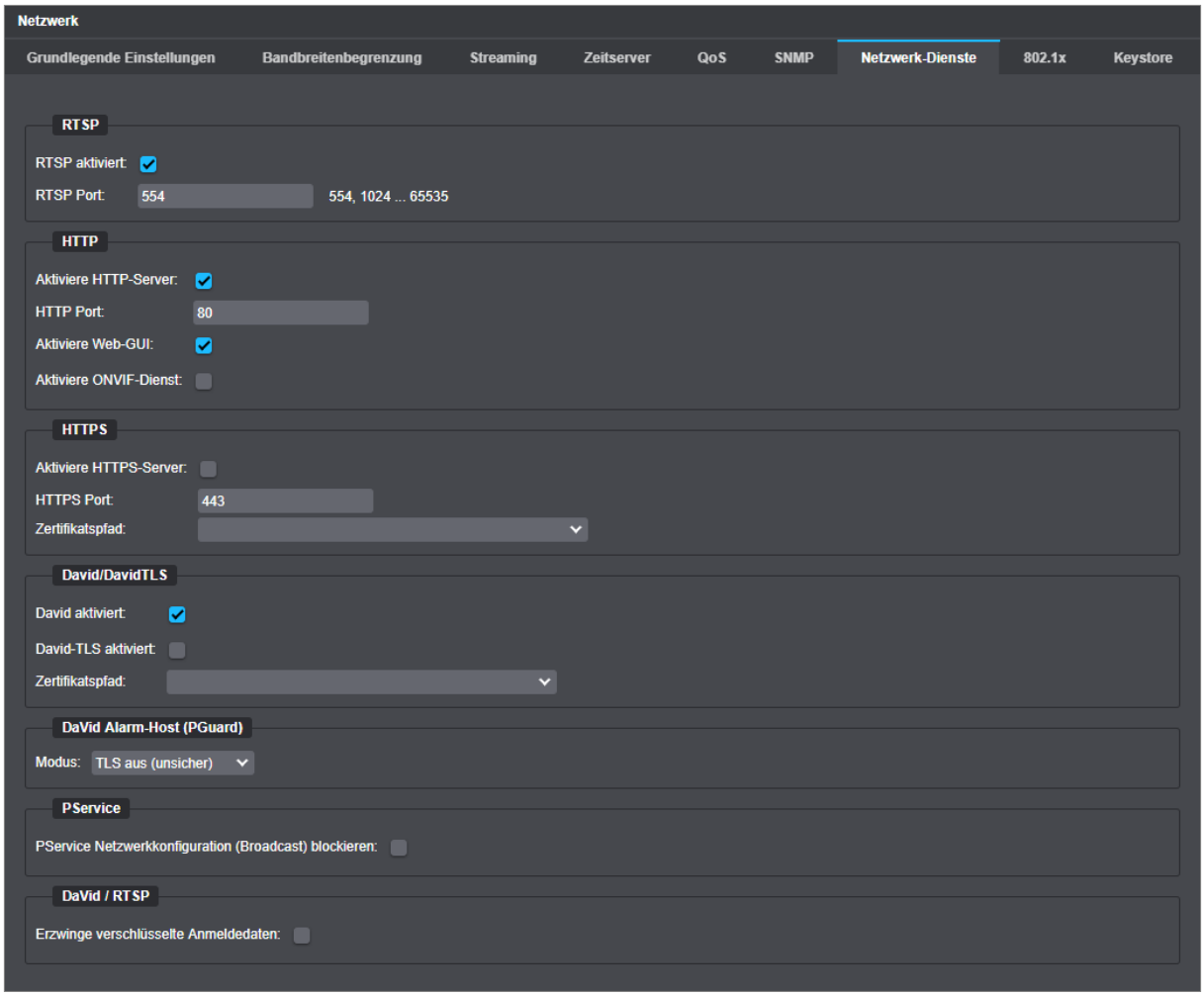


Abb. 10-7

- Beachten Sie die nachfolgenden Erklärungen.
- Aktivieren Sie die relevanten Checkboxen.
- Geben Sie gegebenenfalls den notwendigen Port ein.

*Netzwerk-Dienste werden nach Aktivierung der entsprechenden Checkbox sofort aktiv.*

### ONVIF

ONVIF (Open Network Video Interface Forum) ist eine standardisierte Schnittstelle für netzwerkbasierte Videogeräte. Das ONVIF-Protokoll ermöglicht die Konfiguration des Gerätes und die Abfrage des Video-Streams durch einen beliebigen Client, unabhängig von proprietären Protokollen des Herstellers.

Die Checkbox unter **ONVIF** aktiviert die entsprechende Schnittstelle für den Zugriff durch externe Clients.

### RTSP

Das Real Time Streaming Protocol (RTSP) dient zur Steuerung der kontinuierlichen Übertragung von Multimedia-Inhalten über IP-basierte Netzwerke (Media-Streams).
RTSP nutzt dazu eine direkte (bidirektionale) Kommunikation mit dem RTSP-Streaming-Server der Kamera, einerseits zur Ermittlung des geeigneten Übertragungsprotokolls für die RTP-Datenübermittlung (UDP oder TCP), andererseits zur Übertragung von Steuerungsaktionen von IP-basierten RTSP-fähigen Applikationen (Player), wie beispielsweise zum Starten und Stoppen von Videoübertragungen.
Die Kodierung, Paketierung und der Transport der Datenströme vom Server zum Client erfolgt dabei (unidirektional) über das Real-Time Transport Protocol (RTP).
Normalerweise werden die RTP-Übertragungen der Streaming-Inhalte über UDP (User Datagram Protocol) realisiert, die RTSP-Übertragungen hingegen über eine TCP-Verbindung (TCP = Transmission Control Protocol).

**RTP-Übertragungen über UDP:**
UDP ist ein sogenanntes unzuverlässiges und verbindungsloses Protokoll. Vor der Datenübertragung wird keine Verbindung zum Empfänger/Client aufgebaut. Der Empfänger/Client sendet keine Bestätigung über den Empfang der Daten. Während der Übertragung über UDP können Paketverluste (z. B. Fehlen einzelner Bilder) auftreten. Verlorene Pakete werden nicht erneut gesendet.
UDP-Pakete von außen (Internet) ins lokale Netzwerk werden im Normalfall von Internet-Routern/Firewalls pauschal blockiert.
UDP erlaubt flüssige und schnelle Datenübertragungen mit relativ geringen Verzögerungen (Delays) bzw. ohne zeitlichen Versatz der IP-Pakete (engl. Jitter).
Für jede RTSP/RTP-Übertragung über UDP müssen drei Ports geöffnet sein, ein statischer Port für die RTSP-Steuerbefehle (Standard-Portnummer: 554) und zwei dynamische Ports für den RTP-Datenstrom.

**RTP/RTSP-Übertragungen über TCP:**
TCP ist ein sogenanntes zuverlässiges und verbindungsorientiertes Protokoll. Vor der Datenübertragung wird eine Verbindung zum Empfänger/Client aufgebaut. Der Empfänger/Client sendet eine Bestätigung über den Empfang jedes IP-Pakets. Während der Datenübertragung über TCP können normalerweise keine Paketverluste auftreten (außer im Falle eines Pufferüberlaufs in der Kamera bei dauerhafter Netzwerküberlastung), jedoch ist die Datenübertragung unter Umständen langsamer als über UDP.
Normalerweise muss für Datenübertragungen von RTP/RTSP/TCP-Paketen vom Internet ins lokale Netzwerk nur der RTSP-Port am Internet-Router bzw. an der Firewall geöffnet sein.
RTSP erlaubt es, die Übertragung von RTP-Streams in die bestehende RTSP/TCP-Verbindung einzubetten, es ist also keine gesonderte UDP-Übertragung oder ein zusätzlicher Port für den RTP-Datenstrom notwendig.

Der Standard-Port für RTSP-Übertragungen von Streaming-Daten (Live-Audio und Live-Video) ist 554. Alternativ kann dieser Port einen Wert im Bereich von 1024 – 65535 erhalten.

Befinden sich mehrere Kameras im gleichen Subnetz (hinter dem selben NAT-Router), müssen Sie jeder Kamera einen eigenen, einmalig auftretenden internen RTSP-Port zuweisen, wenn Sie auf den RTSP-Server der jeweiligen Kamera mithilfe von Port-Forwarding von extern (WAN) zugreifen möchten (eventuell nicht notwendig falls der NAT-Router Port-Redirection unterstützt).

Informationen zu RTSP-Requests für den Zugriff auf den jeweiligen Stream finden Sie im Abschnitt „RTSP-Applikation“ auf Seite 146.

### HTTP/HTTPS

Neben HTTP wird auch das Kommunikationsprotokoll HTTPS (HyperText Transfer Protocol Secure) unterstützt, um Daten sicher und vor dem Zugriff Dritter geschützt zu übertragen.
HTTPS dient zum einen der Identitäts-Authentifizierung von zwei Verbindungspartnern beim Aufbau der Kommunikation mithilfe von Zertifikaten und zum anderen der Verschlüsselung von Nutzdaten (Payload), also der zwischen den beiden Kommunikationspartnern zu transportierenden Video- und Audiodatenpakete.

Für einer HTTPS-Konfiguration muss zuvor ein gültiges HTTPS-Zertifikat erstellt werden (siehe Abschnitt „Keystore“ auf Seite 66).

Der Standard-Port für HTTPS-Verbindungen ist 443.

> *Für weiterführende Information und zur Unterstützung bei der Erstellung und Einbindung eines gültigen TLS-Zertifikats, wenden Sie sich an die für Ihre Netzwerkadministration zuständige Person.*

### DaVid/DaVidTLS

Es besteht die Möglichkeit das DaVid-Protokoll zu verwenden und den Datenverkehr mittels Transport Layer Security (TLS) zu verschlüsseln.
Für die Verschlüsselung muss zuvor ein Zertifikatspfad im Keystore erstellt werden (siehe Abschnitt „Keystore“ auf Seite 66).

- Aktivieren Sie die Checkbox **David aktiviert**, falls erforderlich.
- Wählen Sie den **Zertifikatspfad** für die Verschlüsselung aus der entsprechenden Drop-down-Liste.
- Aktivieren Sie die Checkbox **David-TLS**, falls erforderlich.

### DaVid Alarm Host (PGuard)

Das Verhalten des Systems bei der TLS-Verschlüsselung beim Senden von ereignisgesteuerten Nachrichten an einen Alarm-Host über das DaVid-Protokoll kann über die Drop-down-Liste gesteuert werden.

- Wählen Sie den gewünschten TLS-Modus aus der Drop-down-Liste **Modus** aus.

### Dallmeier Device Manager

**Dallmeier Device Manager** ist ein Tool für die Fernkonfiguration von Dallmeier Netzwerkgeräten.
Es scannt das Netzwerk, erkennt die vorhandenen Netzwerkgeräte und bietet unter anderem eine Funktion für die Änderung der Netzwerkeinstellungen an.

Die Einstellung **Dallmeier Device Manager Netzwerkkonfiguration (Broadcast) blockieren** verhindert die Änderung der Netzwerkeinstellungen mit **Dallmeier Device Manager**.

### DaVid/RTSP

- Um die Verschlüsselung von Anmeldeinformationen zu erzwingen, die über das Dallmeier Video- (**DaVid**-)Protokoll gesendet werden, aktivieren Sie die Checkbox **Erzwinge verschlüsselte Anmededaten**.

> *Beachten Sie, dass diese Einstellung nicht die Anmeldung an der Benutzeroberfläche des Geräts über einen Webbrowser verschlüsselt.*

## 10.8 802.1X

IEEE 802.1X beschreibt einen Standard für die portbasierte Netzwerkzugriffskontrolle und stellt sicher, dass neu angeschlossene Netzwerkgeräte nur nach einer erfolgreichen Authentifizierung Zugang zum entsprechend abgesicherten lokalen Netzwerk (LAN) erhalten.
DOMERA® OS unterstützt ausschließlich das sichere und zertifikatsbasierte Authentifizierungsverfahren über **EAP-TLS** (Extensible Authentication Protocol über eine gesicherte TLS-Verbindung).
Der Authentifizierungsprozess schließt drei Elemente ein: den Supplikanten (hier: die Kamera), der auf das Netzwerk zugreifen will, den Authentifikator (z. B. ein IEEE 802.1X-fähiger Managed Switch), der den Zugang zum Netzwerk über die einzelnen Netzwerk-Ports (z. B. physische Ethernet-Schnittstellen) kontrolliert und den zentralen Authentifizierungsserver (RADIUS-Server), der die übermittelten Authentifizierungdaten eines neu angeschlossenen Supplikanten überprüft und, falls diese gültig sind, dessen Identität verifiziert.

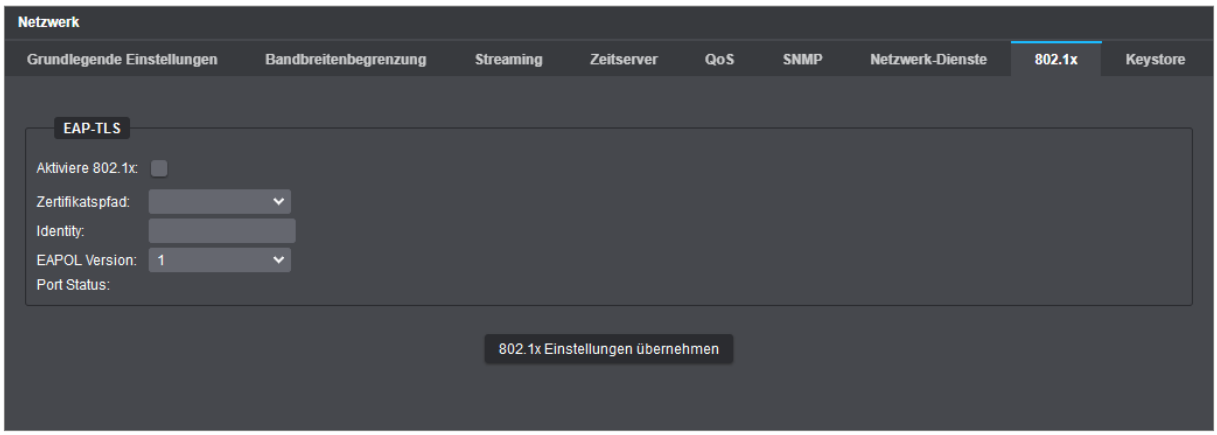


Abb. 10-8

- Aktivieren Sie die Checkbox **Aktiviere 802.1x**.
- Wählen Sie den **Zertifikatspfad**, der das signierte digitale Client-Zertifikat für die Authentifizierung beim Authentifizierungsserver enthält (für Beschreibungen zur Zertifikatsverwaltung, siehe Abschnitt „Keystore“ auf Seite 66).
- Geben Sie die EAP-Identität der Kamera in das Eingabfeld **Identity** ein, falls diese Angabe für einen korrekten Authentifizierungsprozess bei Ihrem RADIUS-Server erforderlich ist.

  Inwieweit die Angabe einer EAP-Identität erforderlich ist und wie die genaue Form eines solchen Identity-Strings auszusehen hat (z. B. gleich dem „Common Name“ im signierten Client-Zertifikat), hängt von der Konfiguration Ihres RADIUS-Servers ab.

- Wählen Sie diejenige **EAPOL Version**, die auch Ihr Authentikator (IEEE 802.1X-fähiger Switch) verwendet, damit die Authentifizierungdaten später korrekt übermittelt werden.
- Bestätigen Sie Ihre Eingaben abschließend mit **802.1x Einstellungen übernehmen**.

## 10.9 KEYSTORE

Die Registerkarte **Keystore** dient zur Anzeige und Verwaltung von Netzwerkzertifikaten.

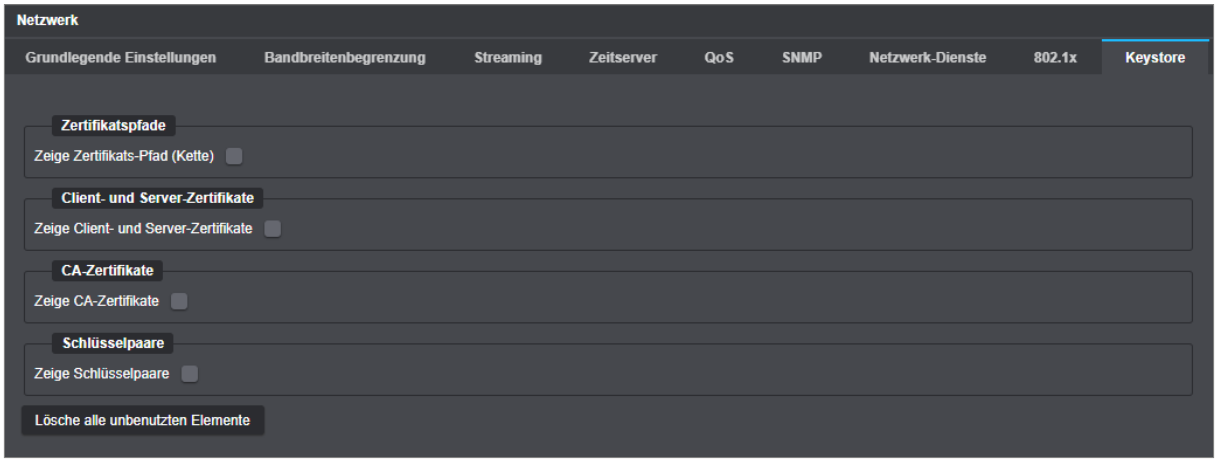


Abb. 10-9

### 10.9.1 Allgemeine Funktionen

Die folgenden allgemeinen Funktionen verhalten sich bei allen verfügbaren Optionen gleich:

**Info**

- Wählen Sie einen Listeneintrag.
- Klicken Sie **Info**, um den Dialog mit Zusatzinformationen zum gewählten Eintrag zu öffnen.

**Lösche [Element]**

> *Beachten Sie, dass die „Löschen"-Aktion sofort ausgeführt wird und keine vorherige Abfrage zur Bestätigung erfolgt.*

- Wählen Sie einen Listeneintrag.
- Klicken Sie **Lösche [Element]**, um den ausgewählten Eintrag aus der jeweiligen Liste zu entfernen.

**Lösche alle [Elemente]**

*Beachten Sie, dass die „Löschen“-Aktion sofort ausgeführt wird und keine vorherige Abfrage zur Bestätigung erfolgt.*

- Klicken Sie **Lösche alle [Elemente]**, um alle Eintrage aus der jeweiligen Liste zu entfernen.

**Lösche alle unbenutzten [Elemente]**

*Beachten Sie, dass die „Löschen“-Aktion sofort ausgeführt wird und keine vorherige Abfrage zur Bestätigung erfolgt.*

- Klicken Sie **Lösche alle unbenutzten [Elemente]**, um alle Eintrage aus der jeweiligen Liste zu entfernen, die gerade keine Verwendung haben.

## 10.9.2 Zertifikate und Schlüssel verwalten

### Zertifikatspfade

- Aktivieren Sie die Checkbox **Zeige Zertifikats-Pfad (Kette)**.

Eine Liste der Zertifikats-Pfade mit Zusatzinformationen und die Schaltflächen zur Verwaltung werden angezeigt.

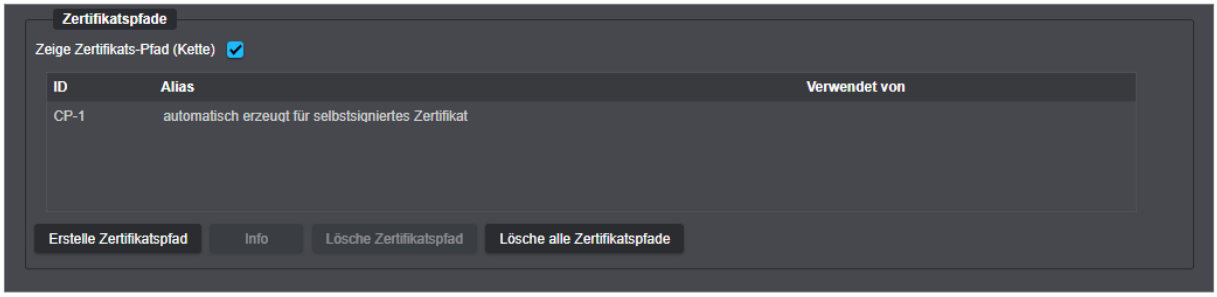


Abb. 10-10

**Erstelle Zertifikatspfad**

- Klicken Sie **Erstelle Zertifikatspfad**, um den entsprechenden Dialog zu öffnen.

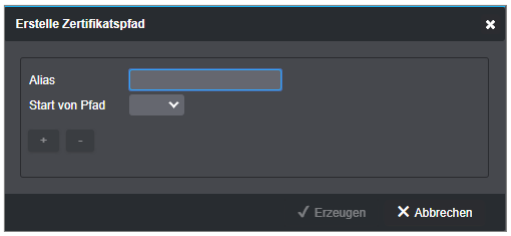


Abb. 10-11

- Geben Sie ein **Alias** ein.
- Wählen Sie aus der Drop-down-Liste **Start von Pfad** den Beginn der Kette aus.
- Erstellen Sie mithilfe der Buttons **+** und **–** den erforderlichen Pfad.
- Bestätigen Sie mit **Erzeugen**.

Der Pfad ist nun erstellt und wird in der Liste angezeigt.

### Client- und Server-Zertifikate

- Aktivieren Sie die Checkbox **Zeige Client- und Server-Zertifikate**.

Eine Liste der Client- und Server-Zertifikate und die Schaltflächen zur Verwaltung werden angezeigt.

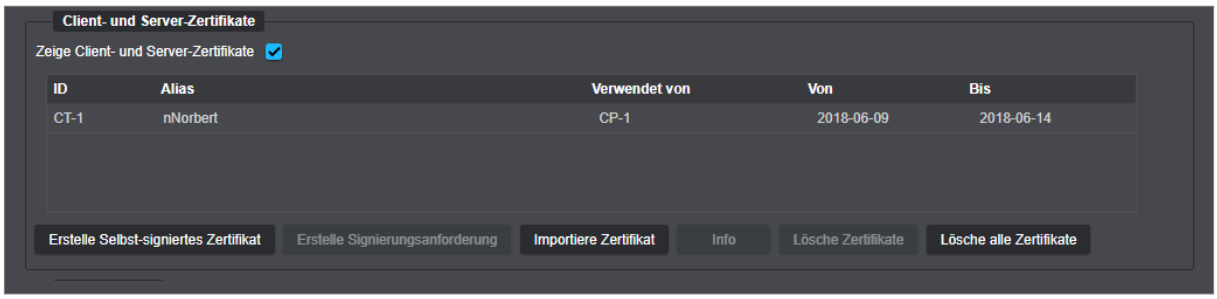


Abb. 10-12

### Selbst signiertes Zertifikat erstellen

- Klicken Sie **Erstelle Selbst-signiertes Zertifikat**, um den entsprechenden Dialog zu öffnen.

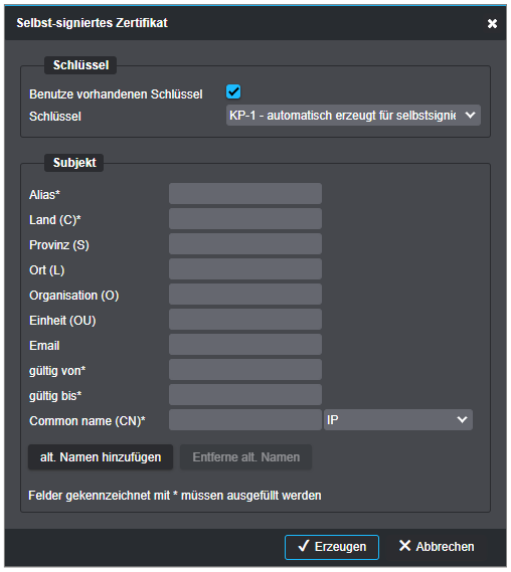


Abb. 10-13

- Aktivieren Sie die Checkbox **Benutze vorhandenen Schlüssel**, falls erforderlich.

- Geben Sie die erforderlichen Daten unter **Subjekt** an.
- Bestätigen Sie mit **Erzeugen**.

Das selbst-signierte Zertifikat ist erstellt und wird in der Liste angezeigt. Es kann nun verwendet werden.

### Erstelle Signierungsanforderung

Um eine Signierungsanforderung zu erzeugen, gehen Sie folgendermaßen vor:

- Markieren Sie das erforderliche Zertifikat.
- Klicken Sie **Erstelle Signierungsanforderung**, um den Dialog **Zertifikats-Signierungsanforderung** zu öffnen.

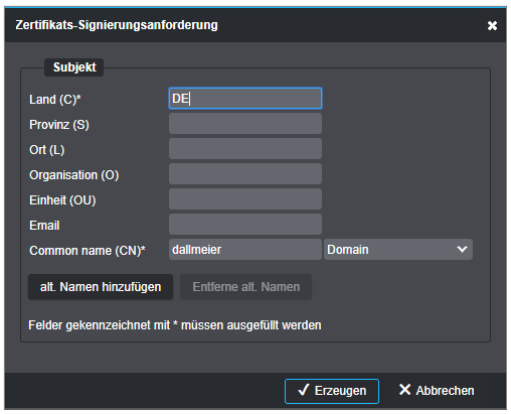


Abb. 10-14

- Geben Sie die erforderlichen Daten ein.
- Klicken Sie **Erzeugen**, um die Erstellung der Signierungsanforderung abzuschließen.
- Senden Sie die erzeugte Datei (**csr.pem**) zur Signatur an die Zertifizierungsstelle (Certificate Authority, CA) in Ihrem Unternehmen oder an eine vertrauenswürdige Drittanbieter-Zertifizierungsstelle.
  Nach Erhalt des von der Zertifizierungsstelle digital signierten Zertifikats (jetzt CA-Zertifikat) können Sie dieses importieren (siehe im Folgenden).

### Importiere Zertifikat

- Klicken Sie **Importiere Zertifikat**, um den Import-Dialog zu öffnen.

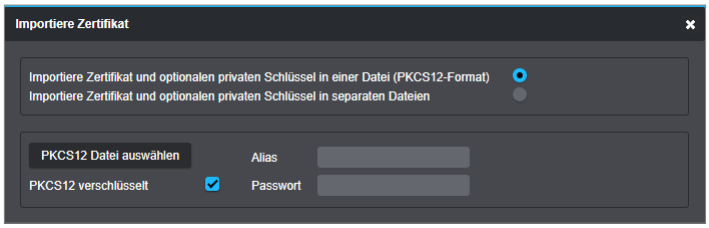


Abb. 10-15

Zertifikate und optionale private Schlüssel können entweder in einer Datei (**PKCS12-Format**) oder in separaten Dateien bereitgestellt sein.

- Wählen Sie mithilfe der Radiobuttons das vorliegende Bereitstellungsformat.

> *Die entsprechenden Optionen werden erst angezeigt, wenn der dazugehörige Radiobutton aktiviert ist.*

**Import aus einer Datei im PKCS12-Format**

- Klicken Sie **PKCS12 Datei auswählen**.
- Geben Sie mithilfe des Datei-Explorers den Dateipfad an.
- Geben Sie ein **Alias** ein, falls erforderlich.
- Aktivieren Sie die Checkbox **PKCS12 verschlüsselt**, falls erforderlich.
- Geben Sie das entsprechende **Passwort** ein, falls erforderlich.
- Bestätigen Sie mit **OK**.

**Import aus separaten Dateien**

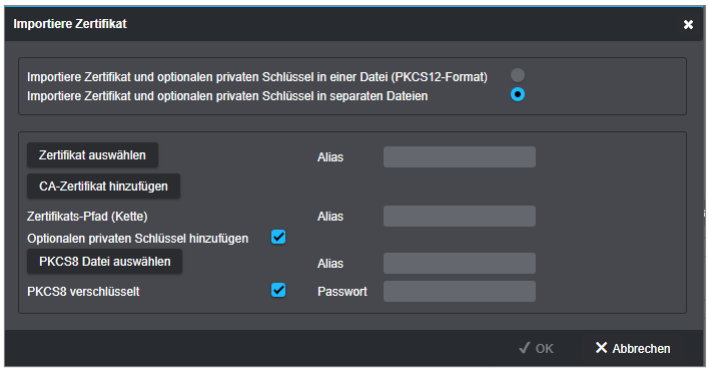


Abb. 10-16

- Klicken Sie **Zertifikat auswählen**.
- Geben Sie mithilfe des Datei-Explorers den Dateipfad an.
- Klicken Sie **CA-Zertifikat hinzufügen**.

Die Schaltfläche **CA-Zertifikat auswählen** wird eingeblendet.

- Klicken Sie **CA-Zertifikat auswählen**.
- Geben Sie mithilfe des Datei-Explorers den Dateipfad an.
- Aktivieren Sie die Checkbox **Optionalen privaten Schlüssel hinzufügen**, falls erforderlich.
- Klicken Sie **PKCS8 Datei auswählen**.
- Geben Sie mithilfe des Datei-Explorers den Dateipfad an.
- Aktivieren Sie gegebenenfalls die Checkbox **PKCS8 verschlüsselt**.
- Geben Sie das erforderliche **Passwort** ein.
- Bestätigen Sie mit **OK**.

### CA-Zertifikate

- Aktivieren Sie die Checkbox **Zeige CA-Zertifikate**.

Eine Liste der CA-Zertifikate und die Schaltflächen zur Verwaltung werden angezeigt.

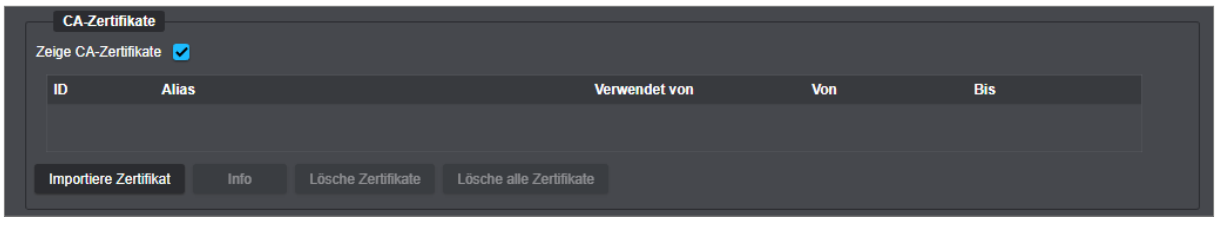


Abb. 10-17

- Klicken Sie **Importiere Zertifikat**, um den entsprechenden Dialog zu öffnen.

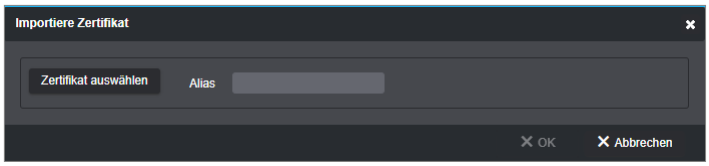


Abb. 10-18

- Klicken Sie **Zertifikat auswählen**.
- Geben Sie mithilfe des Datei-Explorers den Dateipfad an.
- Geben Sie ein **Alias** ein, falls erforderlich.
- Bestätigen Sie mit **OK**.

Das Zertifikat ist nun importiert und wird in der Liste angezeigt.

### Schlüsselpaare

- Aktivieren Sie die Checkbox **Zeige Schlüsselpaare**.

Eine Liste der Schlüsselpaare und die Schaltflächen zur Verwaltung werden angezeigt.

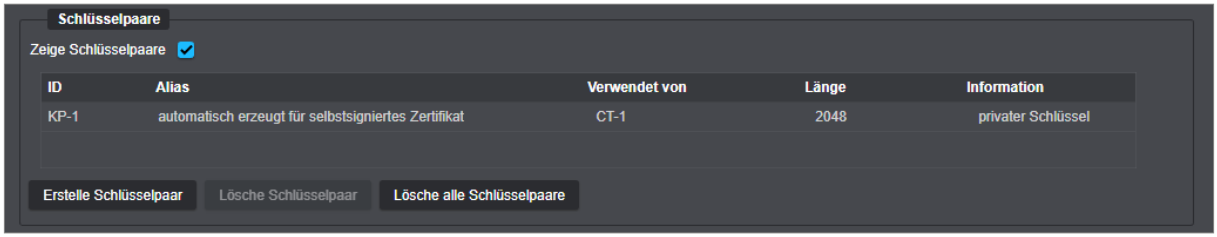


Abb. 10-19

#### Erstelle Schlüsselpaar

Um ein Schlüsselpaar zu erzeugen, gehen Sie folgendermaßen vor:

- Klicken Sie **Erstelle Schlüsselpaar**, um den entsprechenden Dialog zu öffnen.

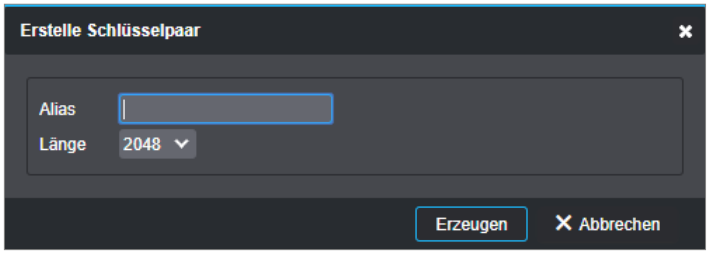


Abb. 10-20

- Geben Sie die erforderlichen Daten ein.
- Klicken Sie **Erzeugen**, um die Erstellung des Schlüsselpaars abzuschließen.

Das Schlüsselpaar ist nun erstellt und wird in der Liste angezeigt. Es kann nun verwendet werden.

# SCHNITTSTELLEN

Im Dialog **Schnittstellen** können die hardwareseitig vorhandenen Relais-Ausgänge und Kontakt-Eingänge auf den entsprechenden Registerkarten konfiguriert werden.

- Klicken Sie im Navigationsmenü den Menüpunkt **Schnittstellen**.

## 11.1 RELAIS-AUSGÄNGE

- Wählen Sie die Registerkarte **Relais-Ausgänge**.

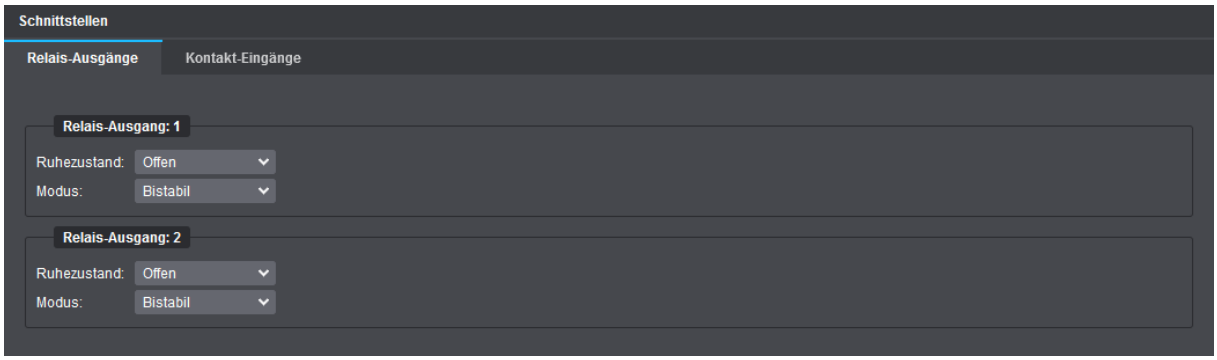


Abb. 11-1

- Wählen Sie aus der Drop-down-Liste **Ruhezustand** den erforderlichen Grundzustand (**Offen** oder **Geschlossen**) für den jeweiligen Relais-Ausgang.
- Wählen Sie aus der Drop-down-Liste **Modus** den erforderlichen Betriebsmodus für den jeweiligen Relais-Ausgang.

Die folgenden zwei Relais-Betriebsmodi stehen zur Verfügung:

### Bistabil

Im Modus **Bistabil** ändert sich der Zustand eines Relais-Ausgangs nur durch einen neu ausgelösten Ereignis-Handler oder durch einen Programmbefehl.

> *Wenn ein Relais-Ausgang im Modus **Bistabil** arbeitet und ein Ereignis-Handler erstellt wird, der den Relais-Ausgang dazu veranlasst, vom Ruhezustand in den aktiven Zustand zu schalten, muss ein separater Ereignis-Handler konfiguriert werden, um den Relais-Ausgang wieder in seinen Ruhezustand zurückzuschalten (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).*

### Monostabil

Im Modus **Monostabil** ändert sich der Zustand eines Relais-Ausgangs durch einen Ereignis-Handler nur für eine bestimmte Zeitspanne.
Der Konfigurationsdialog wird um das Eingabefeld **Dauer** erweitert, das es erlaubt, einen Timer in Millisekunden (ms) einzustellen.
Nach Ablauf der eingestellten Zeit wird der Relais-Ausgang wieder automatisch in den zuvor festgelegten **Ruhezustand** geschaltet.

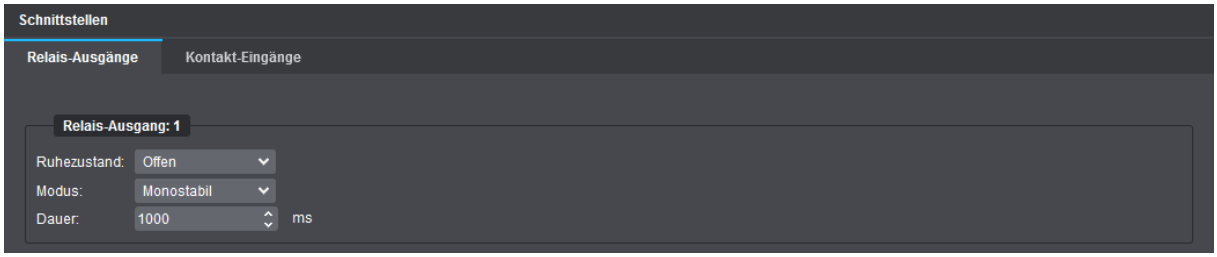


Abb. 11-2

- Geben Sie die erforderliche Ablaufzeit in Millisekunden (ms) in das Eingabefeld **Dauer** ein.

## 11.2 KONTAKT-EINGÄNGE

- Wählen Sie die Registerkarte **Kontakt-Eingänge**.

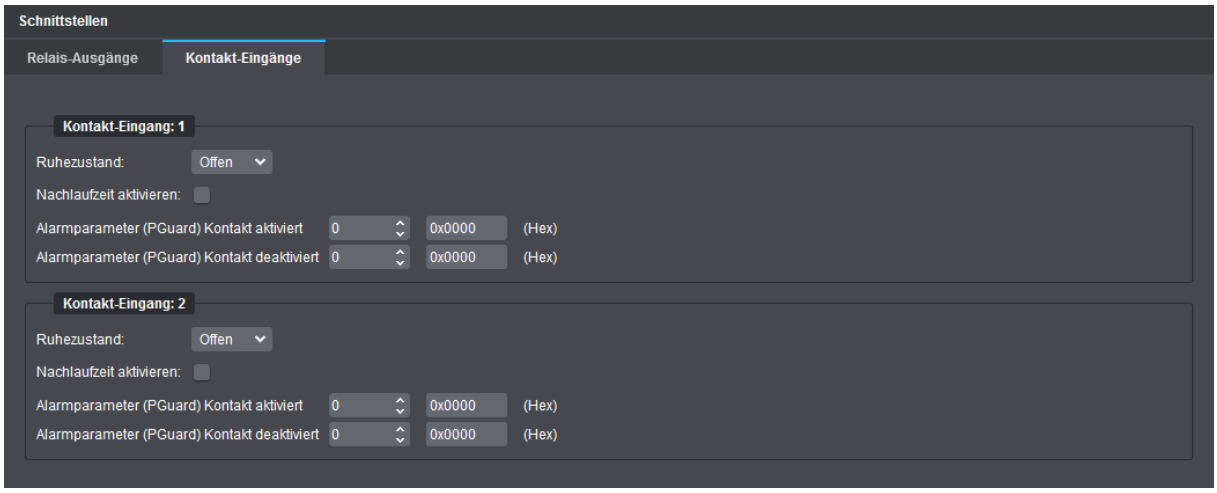


Abb. 11-3

- Wählen Sie aus der Drop-down-Liste **Ruhezustand** den erforderlichen Grundzustand (**Offen** oder **Geschlossen**) für den jeweiligen Kontakt-Eingang.

### Nachlaufzeit aktivieren

Die Funktion **Nachlaufzeit aktivieren** ermöglicht es, eine zeitliche Verzögerung festzulegen, bis die Zustandsänderung eines Kontakt-Eingangs intern verarbeitet wird. Dadurch kann beispielsweise verhindert werden, dass unerwünschte Ereignismeldungen versendet werden, wenn ein Kontakt-Eingang geöffnet und innerhalb einer sehr kurzen Zeit wieder geschlossen wird.

► Aktivieren Sie die Checkbox **Nachlaufzeit aktivieren**, falls erforderlich.

Das Eingabefeld **Dauer** wird eingeblendet.


Abb. 11-4

► Geben Sie die erforderliche Nachlaufzeit in Millisekunden (ms) in das Eingabefeld **Dauer** ein.

### Alarmparameter (PGuard) Kontakt aktiviert/deaktiviert

Ein Alarmparameter ist ein Parameter, der als Zusatzinformation an einen **Dallmeier Video-(DaVid-) Protokoll**-fähigen Alarm-Host (z. B. **PGuard advance** – Dallmeier Client-Software zur Auswertung und Verwaltung von Ereignismeldungen) gesendet wird, wenn der entsprechende hardwareseitig vorhandene Kontakt-Eingang [1–2] aktiviert oder deaktiviert (in den jeweils zuvor festgelegten **Ruhezustand** versetzt) wird.

Als Zusatzparameter können je nach Anforderung Werte von **1**–**65535** eingegeben werden.

Für das Versenden von Alarmparametern bei Zustandsänderung der Kontakt-Eingänge [1–2] müssen Sie einen Ereignis-Handler des Aktionstyps **DaVid Alarm-Host (PGuard)** mit dem entsprechenden Ereignis-Auslöser **Kontakt-Eingang [1–2] aktiviert/deaktiviert** konfigurieren.
Weitere Informationen dazu finden Sie im Abschnitt „PGuard-Nachrichten“ auf Seite 93.

# EDGESTORAGE

Die Funktion **EdgeStorage** erlaubt die verlustfreie Aufzeichnung eines Dallmeier VideoIP-Systems im Fall des temporären Ausfalls der IT-Infrastruktur oder des Aufzeichnungssystems.

Dallmeier IP-Kameras sind mit einem RAM-Speicher ausgestattet. Dieser interne Speicher wird von **EdgeStorage** für die Speicherung der Aufnahmen zur verlustfreien Überbrückung eines Netzwerkausfalls verwendet.

Wenn lange Netzwerkausfälle erwartet werden, kann der interne Speicher von Dallmeier IP-Kameras erweitert werden.

- ► Klicken Sie im Navigationsmenü den Menüpunkt **EdgeStorage**, um den entsprechenden Dialog zu öffnen.

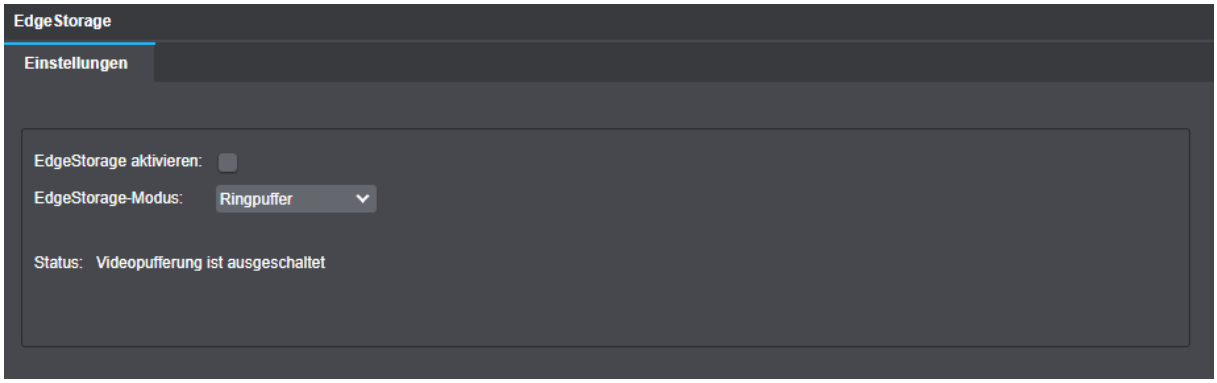


Abb. 12-1

- ► Aktivieren Sie die Checkbox **EdgeStorage aktivieren**.
- ► Wählen Sie aus der Drop-down-Liste **EdgeStorage-Modus** den erforderlichen Speichermodus.

Die folgenden Speichermodi stehen zur Verfügung:

**Ringpuffer**
Sobald der Speicher voll ist, wird damit begonnen, die ältesten Bilder zu überschreiben.

**Linearer Puffer**
Sobald der Speicher voll ist, wird nicht mehr weiter aufgezeichnet.

> *Mithilfe der **Ereignisverwaltung** und **PGuard-Nachrichten** können Sie sich über eine Änderung des EdgeStorage-Status informieren lassen. Weitere Informationen dazu finden Sie im Kapitel „Ereignisverwaltung“ auf Seite 76.*

# EREIGNISVERWALTUNG

Mit der **Ereignisverwaltung** von Domera® OS können verschiedene **Regeln** definiert werden, nach denen die Kamera automatisch bestimmte Aktionen ausführt, wenn eine zuvor festgelegte Bedingung erfüllt ist (z. B. Wiedergabe einer Audiosequenz, wenn eine Person eine virtuelle Linie im Bild überquert hat).

*Eine einzelne Regel kann mehrere unterschiedliche Kamera-Aktionen gleichzeitig initiieren.*

Für komplexere Regeln lassen sich mehrere Bedingungen mit den logischen Operatoren AND oder OR kombinieren und über Bedingungsgruppen verschachtelte Bedingungen formulieren.

*Bei der Erstellung von Regeln erfolgt keine Plausibilitätsprüfung der Abfragelogik verknüpfter (kombinierter) oder verschachtelter Bedingungen.*

Ergänzend zu Aktionsregeln wird die Konfiguration diverser **Ereignis-Handler** für das gezielte automatische Versenden von **PGuard-Nachrichten** anhand bestimmter Auslösekriterien unterstützt (z. B. das bevorstehende Gültigkeitsende eines digitalen Zertifikats).

## 13.1 REGELN

- Klicken Sie im Navigationsmenü den Menüeintrag **Ereignisverwaltung**, um den entsprechenden Dialog zu öffnen.

Die Registerkarte **Regeln** wird angezeigt.

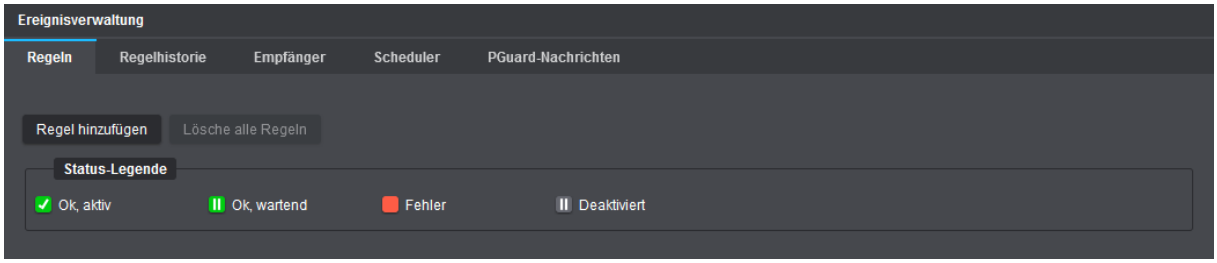


Abb. 13-1

- Klicken Sie **Regel hinzufügen**.

*Alle im Folgenden durchgeführten Benutzeraktionen zur Erstellung von Regeln sind stets sofort und ohne weitere manuelle Bestätigungsschritte wirksam.*

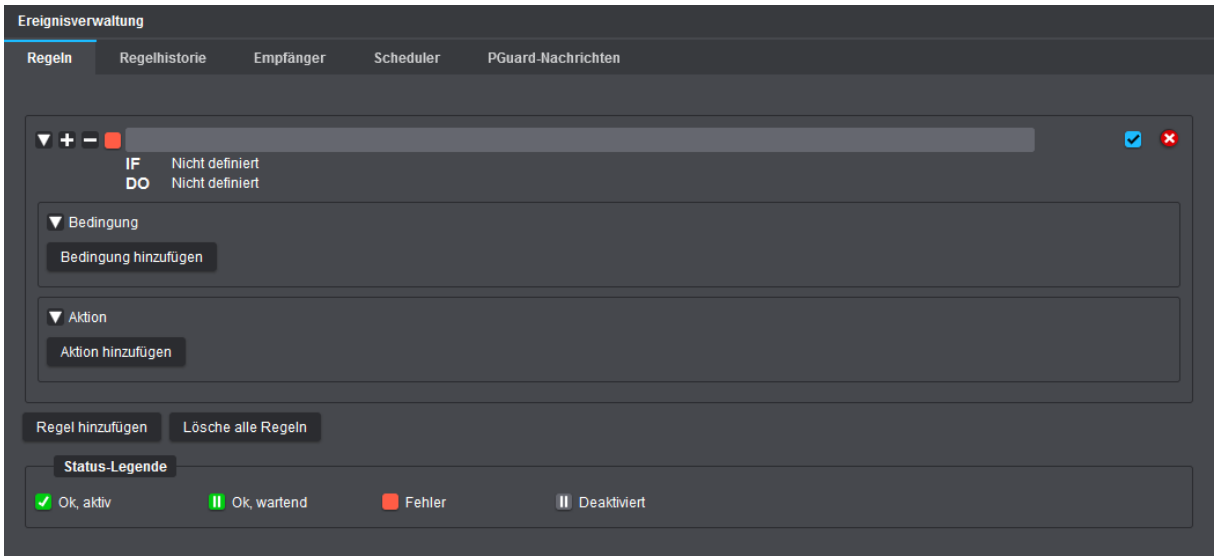


Abb. 13-2

**Funktionsbeschreibung Symbolschaltflächen (Icon-Buttons)**

- Stammstrukturknoten eines Elements (Regel, Bedingung oder Aktion) einklappen/reduzieren
- Stammstrukturknoten eines Elements ausklappen/erweitern
- Alle Elemente (inkl. untergeordnete Strukturknoten) einer Regel ausklappen/erweitern
- Alle Elemente einer Regel einklappen/reduzieren
- Element löschen

**Beschreibung Status-Legende**

- Einzelne Aktion korrekt konfiguriert oder einzelne Bedingung ist gerade erfüllt („true“) oder gesamte Regel wird gerade ausgeführt
- Einzelne Bedingung oder gesamte Regel korrekt konfiguriert > Kamera wartet bis Bedingung „true“ ist
- Element nicht oder fehlerhaft konfiguriert
- Einzelne Bedingung/Aktion oder gesamte Regel durch Abwählen der entsprechenden Checkbox deaktiviert

- Geben Sie im angezeigten Eingabefeld einen beschreibenden Namen für die neue Regel ein.
- Klicken Sie **Bedingung hinzufügen** und konfigurieren Sie die erforderlichen Parameter (siehe Abschnitt „Bedingungen“ auf Seite 78).
- Klicken Sie **Aktion hinzufügen** und konfigurieren Sie die erforderlichen Parameter (siehe Abschnitt „Aktionen“ auf Seite 81).

### 13.1.1 Bedingungen

Im Rahmen einer Regel können folgende *Stateless*-Bedingungen und *Stateful*-Bedingungen definiert sein:

**Line crossed** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn ein neues Objekt die ausgewählte virtuelle Linie im Bild überquert hat (virtueller Stolperdraht).

> *Mit der Funktion **Klassenfilter** können einzelne Objektklassen als auslösende Elemente gezielt aus- oder abgewählt werden, so dass die Bedingung später nur für bestimmte Objekttypen als erfüllt betrachtet wird.*

**Intrusion area entered** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn ein neues Objekt in den ausgewählten Intrusion-Bereich entweder ganz oder teilweise eingedrungen ist.

> *Mit der Funktion **Klassenfilter** können einzelne Objektklassen als auslösende Elemente gezielt aus- oder abgewählt werden, so dass die Bedingung später nur für bestimmte Objekttypen als erfüllt betrachtet wird.*

**Intrusion area exited** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn das Objekt, das zuvor in den ausgewählten Intrusion-Bereich eingedrungen ist, diesen Bereich wieder verlassen hat.

> *Mit der Funktion **Klassenfilter** können einzelne Objektklassen als auslösende Elemente gezielt aus- oder abgewählt werden, so dass die Bedingung später nur für bestimmte Objekttypen als erfüllt betrachtet wird.*

**Intrusion area occupied by object** [„*Stateful* Condition“, zustandsbehaftet]
Bedingung ist erfüllt („true“), solange sich mindestens ein Objekt im ausgewählten Intrusion-Bereich befindet.
Bedingung ist nicht oder nicht mehr erfüllt („false“), wenn sich kein Objekt im ausgewählten Intrusion-Bereich befindet oder alle zuvor detektierten Objekte im ausgewählten Intrusion-Bereich „verloren“ gehen oder statisch werden.

> *Mit der Funktion **Klassenfilter** können einzelne Objektklassen als auslösende Elemente gezielt aus- oder abgewählt werden, so dass die Bedingung später nur für bestimmte Objekttypen als erfüllt betrachtet wird.*

**Loitering started** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn sich eine neue Person entweder ganz oder teilweise über einen ungewöhnlich langen Zeitraum im ausgewählten Loitering-Bereich aufhält (Start von Herumlungern jeweils erfüllt, wenn der gewählte Level hinsichtlich der Mindestaufenthaltsdauer überschritten wird).

**Loitering ended** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn diejenige Person, die zuvor das Loitering-Start-Ereignis im ausgewählten Loitering-Bereich ausgelöst hat, diesen Bereich wieder verlassen hat.

**Loitering** [„*Stateful* Condition“, zustandsbehaftet]
Bedingung ist erfüllt („true“), solange sich mindestens eine Person entweder ganz oder teilweise über einen ungewöhnlich langen Zeitraum im ausgewählten Loitering-Bereich aufhält (nachdem der gewählte Level hinsichtlich der Mindestaufenthaltsdauer überschritten wurde).
Bedingung ist nicht oder nicht mehr erfüllt („false“), wenn sich keine Person im ausgewählten Loitering-Bereich befindet oder alle zuvor detektierten Personen im ausgewählten Loitering-Bereich „verloren“ gehen.

**Digital input state** [„*Stateful* Condition“, zustandsbehaftet]
Bedingung ist erfüllt („true“), solange der ausgewählte Kontakt-Eingang (1 – 2) an der Kamera-Hardware oder der ausgewählte virtuelle Eingang (Virtual 1 – 4) den angegebenen Input-Status aufweist.

**Digital input transition** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn der ausgewählte Kontakt-Eingang (1 – 2) an der Kamera-Hardware oder der ausgewählte virtuelle Eingang (Virtual 1 – 4) in den angegebenen Input-Status übergeht.

**Day/Night state** [„*Stateful* Condition“, zustandsbehaftet]
Bedingung ist erfüllt („true“), solange die Kamera im angegebenen Tag/Nacht-Modus arbeitet.

**Day/Night transition** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn die Kamera in den angegebenen Tag/Nacht-Modus übergeht.

**Tamper** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn die Kamera die ausgewählte Sabotagehandlung oder den ausgewählten Manipulationsversuch an der Kamera erkannt hat.

**EdgeStorage** [„*Stateless* Condition“, zustandslos]
Bedingung ist jeweils genau dann einmal erfüllt („true“), wenn die entsprechende ausgewählte **EdgeStorage**-Statusänderung eintritt (siehe nachfolgende Erläuterungen):

- **MediumOK**
  Fehlerfreie Speicherkarte nach Kamera-Neustart gefunden oder
  Speicherkarte arbeitet nach einem temporären Fehler im laufenden Betrieb wieder fehlerfrei.

- **MediumError**
  Speicherkarte wurde im laufenden Betrieb entfernt oder Speicherkarte ist fehlerhaft.

- **NoMedium**
  Keine Speicherkarte nach Kamera-Neustart gefunden.

- **BufferingStarted**
  Netzwerkverbindung zu Dallmeier Aufzeichnungssystem unterbrochen >
  Speicherung (Pufferung) von Audio-, Video- und Metadaten auf Speicherkarte gestartet.

- **BufferingFinished**
  Netzwerkverbindung zu Dallmeier Aufzeichnungssystem wiederhergestellt >
  Speicherung (Pufferung) von Audio-, Video- und Metadaten auf Speicherkarte beendet.

- **DeliveringStarted**
  Übertragung der gespeicherten Daten an Dallmeier Aufzeichnungssystem gestartet (SmartBackfill).

- **DeliveringFinished**
  Übertragung der gespeicherten Daten an Dallmeier Aufzeichnungssystem abgeschlossen.

- **BufferFull** („Linearer Puffer“)
  Speicherkarte ist voll > Speicherung (Pufferung) von Daten auf Speicherkarte gestoppt.

- **BufferOverwriting** („Ringpuffer“)
  Speicherkarte ist voll > Überschreiben der ältesten Daten im Ringspeicher (erneut) gestartet.

**Certificate expiry** [„*Stateless* Condition“, zustandslos]
Bedingung ist genau dann einmal erfüllt („true“), wenn der ausgewählte Schwellenwert in Tagen vor Ablauf der Gültigkeit eines digitalen Zertifikats erreicht ist.

**Service interval** [„*Stateless* Condition“, zustandslos]
Bedingung ist zu einem der folgenden Zeitpunkte vor Ablauf der Software-Wartungslizenz für die Kamera genau einmal erfüllt („true“):

- 60 Tage vor Serviceintervall-Ende
- 30 Tage vor Serviceintervall-Ende
- 0 Tage vor Serviceintervall-Ende

**Scheduler** [„*Stateful* Condition“, zustandsbehaftet]
Bedingung ist erfüllt („true“), solange sich der ausgewählte Zeitplaner (regelmäßig wiederkehrender 7-Tage-Wochenzeitplan) gemäß seinen Einstellungen zu festgelegten Uhrzeiten und Ausnahmen im hier angegebenen Status **Inaktiv** oder **Aktiv** befindet (siehe Abschnitt „Scheduler“ auf Seite 92).

### 13.1.2 Aktionen

Im Rahmen einer Regel können folgende Kamera-Aktionen initiiert werden:

**Digitaler Ausgang**
Diese Aktion ändert (*oder* belässt) den aktuellen Schaltzustand des ausgewählten Relais-Ausgangs an der Kamera-Hardware auf

- aktiv, wenn eine *Stateless*-Bedingung „true“ wird.
- aktiv, wenn eine *Stateful*-Bedingung „true“ wird.
- aktiv, solange eine *Stateful*-Bedingung „true“ ist.

> *Aktivieren Sie für „Stateless“-Bedingungen ggf. die Funktion **Monostable for stateless**, damit der Relais-Ausgang nach Ablauf der eingestellten Zeit wieder automatisch in seinen Ruhezustand zurückfällt.*

- inaktiv (Ruhezustand), wenn sich eine *Stateful*-Bedingung von „true“ zu „false“ ändert.
- inaktiv (Ruhezustand), solange eine *Stateful*-Bedingung „false“ ist.

**Beleuchtung**
Diese Aktion schaltet (*oder* belässt) die Weißlicht-LED-Beleuchtung der Kamera

- für die eingestellte **Dauer** ein (Standardwert: 30 Sekunden), wenn eine *Stateless*-Bedingung „true“ wird.
- ein, wenn eine *Stateful*-Bedingung „true“ wird.
- durchgehend eingeschaltet, solange eine *Stateful*-Bedingung „true“ ist.
- aus, wenn sich eine *Stateful*-Bedingung von „true“ zu „false“ ändert und die eingestellte Ablaufzeit (Schieberegler **Dauer**) verstrichen ist.

▶ Wählen Sie aus der Drop-down-Liste **Kameramode** eine der folgenden drei Optionen:

**Farbe**
Befindet sich die Kamera bei Aktivierung der Weißlicht-LEDs im Nachtmodus und gleichzeitig im Schwarz-Weiß-Modus, schaltet die Kamera automatisch in den Farbmodus, auch wenn die eigentliche Umschaltschwelle vom Nacht- in den Tagmodus noch nicht erreicht sein sollte.
Dies kann möglicherweise dazu führen, dass die Kamera unter bestimmten Bedingungen häufig zwischen dem Schwarz-Weiß- und dem Farbmodus umschaltet.

**Schwarz/weiß**
Befindet sich die Kamera bei Aktivierung der Weißlicht-LEDs im Nachtmodus, bleibt die Kamera ungeachtet des nun sichtbaren (weißen) Umgebungslichts weiterhin im Schwarz-Weiß-Modus, auch wenn die eigentliche Umschaltschwelle vom Nacht- in den Tagmodus bereits erreicht sein sollte.

**Beibehalten**
Mit dieser Option behält die Kamera bei Aktivierung der Weißlicht-LEDs genau den Modus bei, der sich aus dem zu diesem Zeitpunkt gemessenen sichtbaren Umgebungslicht und der über die Drop-down-Liste **Farbe** auf der Registerkarte **Tag/Nacht** im Dialog **Bild** gewählten Einstellung ergibt.

▶ Aktivieren Sie ggf. die Checkbox **Blinklicht**, um blinkende Weißlicht-LEDs anstelle von LED-Dauerlicht zu verwenden.

### MQTT client

Diese Aktion sendet spezielle MQTT-Nachrichten an einen eigens dafür betriebenen Message-Broker (MQTT-Server) in Ihrem Netzwerk, wenn eine Bedingung „true“ wird.

Weiterführende Informationen zu **MQTT** finden Sie im Abschnitt „Empfänger“ auf Seite 86.

- ► Wählen Sie einen zuvor auf der Registerkarte **Empfänger** definierten MQTT-Empfänger-Host (Broker) aus.
- ► Geben Sie im Feld **Topic** eine Zeichenfolge im UTF-8-Format ein (z. B.: LineCrossed), die der Message-Broker später zum thematischen Filtern von MQTT-Nachrichten für jeden verbundenen MQTT-Client verwendet (bei Topics wird zwischen Groß- und Kleinschreibung unterschieden).

### HEMISPHERE-MQTT client

Diese Aktion sendet, abhängig von der jeweiligen Bedingung, spezielle MQTT-Nachrichten mit den ausgewählten Topics (z. B. **People counting**) an den angegebenen ActiveMQ-Broker in Ihrer **Dallmeier HEMISPHERE®**-Umgebung (ASA-MQTT).

Weiterführende Informationen zu **MQTT** finden Sie im Abschnitt „Empfänger“ auf Seite 86.

*Diese Aktion kann nur in Verbindung mit mindestens einer der folgenden „Stateless Conditions“ verwendet werden:*

- ***Line crossed***
- ***Intrusion area entered***
- ***Intrusion area exited***
- ***Loitering started***
- ***Loitering ended***
- ***Tamper***

- ► Wählen Sie einen zuvor auf der Registerkarte **Empfänger** definierten MQTT-Broker (ASA).
- ► Wählen Sie die erforderlichen MQTT-Topics, die versendet werden sollen.

### HTTP client

Diese Aktion sendet spezielle Nachrichten in Form von HTTP-Anfragen (Requests) an den ausgewählten Webserver in Ihrem Netzwerk bzw. an eine darauf laufende Webanwendung (Webservice), wenn eine Bedingung „true“ wird.
Die übermittelten HTTP-Nachrichten können dann wiederum dazu verwendet werden, bestimmte Nachfolgeaktionen über den adressierten Webservice auszulösen (z. B. das Anlegen oder Aktualisieren eines Datensatzes).

Weiterführende Informationen zu **HTTP** finden Sie im Abschnitt „Empfänger“ auf Seite 86.

- ▶ Wählen Sie einen zuvor auf der Registerkarte **Empfänger** definierten HTTP-Empfänger-Host aus.
- ▶ Wählen Sie aus der Drop-down-Liste **Methode** die erforderliche Anfrage-Methode des HTTP-Requests (**GET**, **PUT**, **POST**).
- ▶ Geben Sie den Pfad zum laufenden Webservice und anschließend den entsprechenden Abfrageteil ein, wie beispielsweise:

```
/api/CreateEvent?Ressource=CameraEvent&type=LineCrossed
```

*Die korrekte Anfrage-Methode des jeweiligen HTTP-Requests (**GET**, **PUT**, **POST**) sowie den genauen Pfad und Abfrageteil entnehmen Sie der Dokumentation zu dem von Ihnen verwendeten Webservice.*

### Audioausgabe

Diese Aktion startet (*und* wiederholt ggf.) die Wiedergabe einer auf die Kamera hochgeladenen Audiosequenz,

- wenn eine *Stateless*-Bedingung „true“ wird.
- wenn eine *Stateful*-Bedingung „true“ wird.
- solange eine *Stateful*-Bedingung „true“ ist (nur, falls **Wiederhole Audiosequenz** aktiviert ist).

*Eine gestartete Audiosequenz wird immer bis zum Ende abgespielt (unabhängig von ihrer Gesamtlänge), auch wenn eine Bedingung während der Audiowiedergabe wieder „false“ wird.*

- ▶ Beachten Sie die Erläuterungen zu den einzelnen Audioausgabeparametern auf der folgenden Seite und nehmen Sie die erforderlichen Einstellungen vor.

**Minimale Wiederholzeit**
Dieser Parameter legt die Zeit in Sekunden fest, die nach dem Abspielen der ausgewählten Audiosequenz vergehen muss, bevor weitere als erfüllt („true“) betrachtete Bedingungen innerhalb der Regel berücksichtigt werden, um dieselbe Audiosequenz erneut abzuspielen.

Beispiel:
Bedingung = **Line crossed** OR **Intrusion area entered**; Minimale Wiederholzeit = **10 Sekunden**

1. Person 1 überquert virtuelle Linie > Audiosequenz wird bis zum Ende abgespielt > Minimale Wiederholzeit von **10 Sekunden** startet nach Audioausgabe.
2. Person 2 überquert virtuelle Linie bei **5 Sekunden** nach Audioausgabe > Audiosequenz wird ***nicht*** abgespielt.
3. Auto 1 fährt in Intrusion-Bereich nach weiteren **3 Sekunden** > Audiosequenz wird ***nicht*** abgespielt.
4. Person 3 überquert virtuelle Linie bei **11 Sekunden** nach Audioausgabe > Audiosequenz wird erneut bis zum Ende abgespielt > Minimale Wiederholzeit von **10 Sekunden** startet erneut nach zweiter Audioausgabe.
5. Auto 2 fährt in Intrusion-Bereich nach weiteren **3 Sekunden** > Audiosequenz wird ***nicht*** abgespielt.
6. Auto 3 fährt in Intrusion-Bereich bei **11 Sekunden** nach zweiter Audioausgabe > Audiosequenz wird erneut bis zum Ende abgespielt.

**Wiederhole Audiosequenz**
Dieser Parameter ist nur bei *Stateful*-Bedingungen wirksam und legt fest, ob und ggf. in welchen Zeitabständen die ausgewählte Audiosequenz wiederholt (in einer Audioschleife) abgespielt werden soll, bis die entsprechende *Stateful*-Bedingung nicht mehr erfüllt ist bzw. wieder „false“ wird.
Die eingestellte **Wiederholzeit** bestimmt dabei die Länge der Wiederholpausen zwischen dem Ende einer vollständig abgespielten Audiosequenz und dem erneuten Start der Audiosequenz.

**Unterdrücke kurze Bedingungen**
Dieser Parameter gibt an, wie lange eine Bedingung mindestens erfüllt sein muss, bevor die ausgewählte Audiosequenz abgespielt wird. Bei aktivierter Option werden alle *Stateless*-Bedingungen unterdrückt und *Stateful*-Bedingungen müssen mindestens für die Dauer des eingestellten Unterdrückungsintervalls erfüllt sein, damit die Audiosequenz abgespielt wird.

### DaVid notification
Diese Aktion sendet eine DaVid-Meldung in Form einer wählbaren (und später intern verwendeten) Benachrichtungs-ID an ein System, das sich aktiv über das DaVid-Protokoll mit der Kamera verbunden hat (z. B. ein Dallmeier Aufzeichnungssystem).
Das mit der Kamera verbundene DaVid-Protokoll-fähige System kann dann wiederum so konfiguriert werden, dass es abhängig von der empfangenen DaVid-Message-ID bzw. dem jeweils zugeordneten Namen bestimmte Nachfolgeaktionen ausführt (z. B. Schalten eines am Dallmeier Aufzeichnungssystem vorhandenen Relais).

// Setup-Beispiel an Dallmeier Aufzeichnungssystem **IPS 10 000 MK2** //
Recorder-Hauptmenü > **Schnittstellen** > **Relais OUT** > Relais-Nr. aus entspr. Drop-down-Liste auswählen > Option **Kamera-Ereignis mit Timer** aus Drop-down-Liste **Funktion** auswählen > Kamera mit Domera® OS hinzufügen > Relevante Namen der **Benachrichtigungsereignisse** auswählen.

### Email

Diese Aktion versendet je nach zutreffender Bedingung entsprechende Ereignismeldungen als E-Mail via SMTP (Simple Mail Transfer Protocol) bzw. ESMTP (Extended SMTP) über das ausgewählte E-Mail-Konto an einen oder mehrere eingetragene E-Mail-Empfänger.

Informationen zum Anlegen eines E-Mail-Kontos (Account), über das die Ereignismeldungen versendet werden, finden Sie im Abschnitt „Empfänger“ auf Seite 86.
Wenn Sie mehrere E-Mail-Konten auf der Registerkarte **Empfänger** eingerichtet haben, können Sie auswählen, welches Konto beim Senden der E-Mail-Nachricht verwendet werden soll.

- Wählen Sie ein zuvor auf der Registerkarte **Empfänger** definiertes **Konto** für den E-Mail-Versand aus.
- Geben Sie im Feld **An** den oder die Empfänger der E-Mail-Nachricht ein.

> *Trennen Sie mehrere Empfänger durch ein Leerzeichen, ein Komma, ein Semikolon oder einen Zeilenumbruch.*

- Geben Sie **Betreff** und **Text** der E-Mail-Nachricht ein.

Im Text der E-Mail-Nachricht werden neben einem beliebigen freien Text folgende Variablen unterstützt:

- **{rule}**
  Name der ausgeführten Regel
- **{event}**
  Auslösendes Ereignis innerhalb der Regel (zutreffende Bedingung)
- **{hostname}**
  Host-Name der Kamera (siehe Dialog **Netzwerk** > Registerkarte **Grundlegende Einstellungen**)
- **{ip}**
  IP-Adresse der Kamera
- **{cameraName}**
  Name der Kamera (siehe Dialog **Allgemeine Einstellungen**)
- **{location}**
  Standort der Kamera (siehe Dialog **Allgemeine Einstellungen** > Registerkarte **Standort**)
- **{timestamp}**
  Zeitstempel des Ereignisses

- Aktivieren Sie bei Bedarf die Checkbox **Bild hinzufügen**, um das zum Zeitpunkt des Ereignisses aktuelle Live-Bild an die E-Mail-Nachricht anzuhängen.

> *Testen Sie die Richtigkeit Ihrer Eingaben mit der Schaltfläche **Test**, bevor Sie die Regel im Live-Betrieb Ihrer Kamera anwenden.*

## 13.2 REGELHISTORIE

Die Registerkarte **Regelhistorie** listet alle Regeln nach Datum/Uhrzeit auf, die die Kamera aufgrund einer zutreffenden Bedingung abgearbeitet hat.

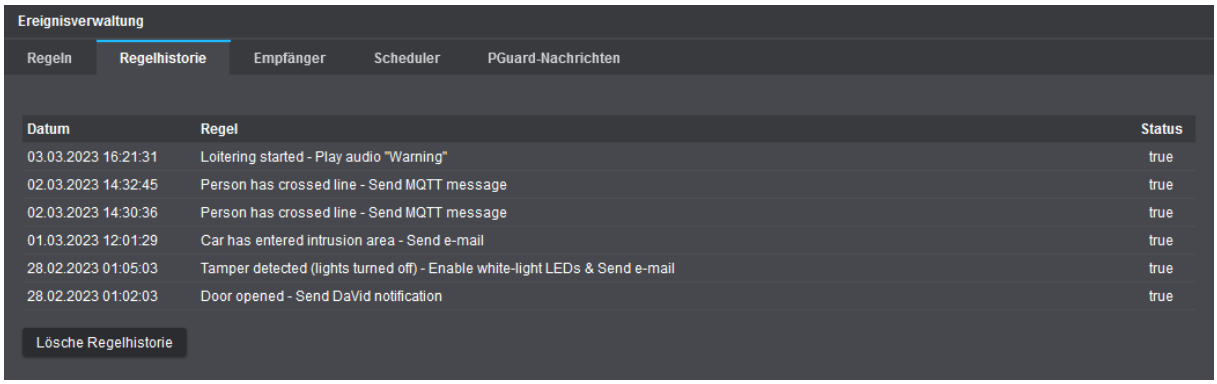


Abb. 13-3

## 13.3 EMPFÄNGER

Auf der Registerkarte Empfänger können Sie je nach Anforderung einen oder mehrere **HTTP**-, **MQTT**-, **ONVIF-MQTT**- und **E-Mail**-Empfänger definieren, die die von der Kamera generierten Ereignisse jeweils entsprechend der ausgewählten Kamera-Aktion und dem daraus abgeleiteten Kommunikationsprotokoll in geeigneter Weise verarbeiten.

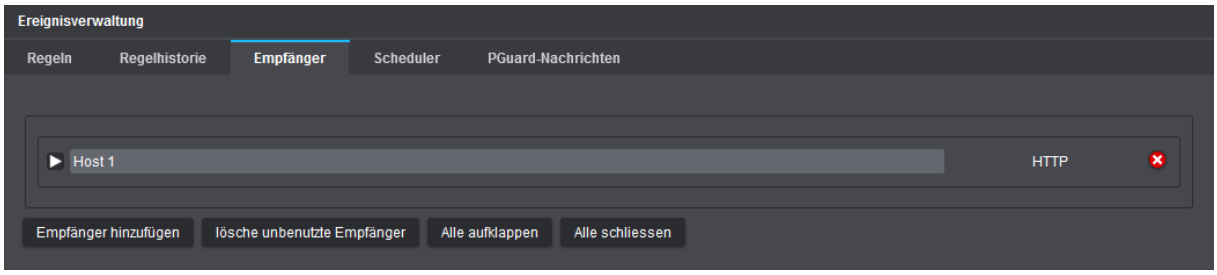


Abb. 13-4

- Beachten Sie zunächst die Erläuterungen zu den einzelnen Empfängertypen auf den folgenden Seiten.
- Klicken Sie **Empfänger hinzufügen**.
- Wählen Sie aus der Drop-down-Liste **Empfänger** den erforderlichen Empfängertyp und bestätigen Sie mit **OK**.
- Konfigurieren Sie die erforderlichen Parameter für den jeweiligen Empfänger.

*Konfigurierte Empfänger, die später von einer Regel in Verwendung sind, können nicht gelöscht werden.*

### 13.3.1 HTTP

Dieser Empfängertyp ermöglicht es Ihnen, einen HTTP-Server in Ihrem Netzwerk anzugeben, der die von der Kamera generierten HTTP-Requests entgegennimmt und standardmäßig über Port 80 (bei einer unverschlüsselten Verbindung mittels HTTP) bzw. über Port 443 (bei einer verschlüsselten TLS-Verbindung mittels HTTPS) an den entsprechenden Dienst (Webservice) ausliefert.


Abb. 13-5

- Geben Sie im angezeigten Eingabefeld einen beschreibenden Namen für den HTTP-Empfänger-Host ein.
- Geben Sie im Feld **URI** die Adresse (gemäß folgender Syntax) ein, unter der Ihr Webservice im Netzwerk erreichbar ist:

  - Schema bzw. Typ des Protokolls (http oder https) für die Kommunikation zwischen Kamera und Webserver; gefolgt von einem Doppelpunkt (:)
  - Host des Rechners bzw. Webservers, auf dem Ihr Webservice läuft; eingeleitet durch zwei Schrägstriche (//): Hier kann entweder die IP-Adresse angegeben werden oder, falls Sie in den Netzwerkeinstellungen der Kamera erreichbare DNS-Server zur Namensauflösung eingetragen haben, der entsprechend registrierte Fully Qualified Domain Name (FQDN) des Webservers, wie z. B. web1.example.com
  - Portnummer mit vorangestelltem Doppelpunkt (:), über die der Webservice auf Ihrem HTTP-Server erreichbar ist (nur optional, falls abweichend von Standard-HTTP-Port 80 bzw. Standard-HTTPS-Port 443)

  Beispiel für unverschlüsselte Verbindung (**http**) über Nicht-Standardport **8080**:

  ```
  http://192.0.2.1:8080
  ```

  Beispiel für verschlüsselte TLS-Verbindung (**https**) über Nicht-Standardport **8443**:

  ```
  https://192.0.2.1:8443
  ```

  Die o. g. IP-Adresse ist nur beispielhaft und muss mit der IP-Adresse bzw. dem FQDN des Webservers ersetzt werden, auf dem Ihr Webservice läuft.

- Geben Sie die Anmeldedaten für die Anmeldung beim Webservice in die Felder **Benutzername** und **Passwort** ein, falls eine Client-Authentifizierung gegenüber dem Webservice erforderlich ist.

**Smart-Filter** (Standardwert: 30 Sekunden)
Dieser Parameter legt die Zeit in Sekunden fest, die nach dem Versenden eines HTTP-Requests vergehen muss, bevor weitere als erfüllt („true“) betrachtete Bedingungen innerhalb einer Regel berücksichtigt werden, um erneut einen HTTP-Request zu versenden (entspricht Beispiel unter **Minimale Wiederholzeit** für die Kamera-Aktion **Audioausgabe**; siehe Abschnitt „Minimale Wiederholzeit“ auf Seite 84).

### 13.3.2 MQTT

Dieser Empfängertyp ermöglicht es Ihnen, einen sogenannten Message-Broker bzw. MQTT-Server in Ihrem Netzwerk anzugeben. In seiner Rolle als zentraler Vermittler nimmt ein Message-Broker die von der Kamera (Publishing-Client) generierten MQTT-Nachrichten entgegen, filtert die Nachrichten intern nach den gekennzeichneten Topics (Themen, zu denen die Nachrichten veröffentlicht werden sollen) und sendet schließlich die in den MQTT-Nachrichten enthaltenen Daten und Informationen an all jene MQTT-Clients (Subscriber) in Ihrem Netzwerk, die zuvor genau die in der Kamera definierten Topics beim Message-Broker abonniert haben.
MQTT (Message Queuing Telemetry Transport) basiert auf dem Publish-Subscribe-Modell.
Bei der Machine-to-Machine-Kommunikation (M2M) besteht also keine direkte Verbindung zwischen den einzelnen IoT-Geräten („IoT“ steht für „Internet of Things“ – auf Deutsch: „Internet der Dinge“).
Die Übertragung der MQTT-Nachrichten erfolgt mittels TCP/IP über den Standardport 1883 bei einer unverschlüsselten Verbindung oder über den Standardport 8883 bei einer verschlüsselten TLS-Verbindung (abhängig von der Konfiguration Ihres MQTT-Servers).

Mithilfe von MQTT-Nachrichten sind beispielsweise folgende Anwendungsszenarien denkbar:

- Automatisierte Erstellung von Analyse-Dashboards für die grafische Visualisierung von **EdgeAnalytics**-Events der Kamera auf Basis von MQTT-Topics und den darin enthaltenen Daten (Telemetrieereignisse)
- Auslösen von Aktionen auf einem anderen IoT-Gerät (Subscriber) im Netzwerk, wenn die Daten im gesendeten MQTT-Topic der Kamera (Publisher) einen bestimmten Wert enthalten

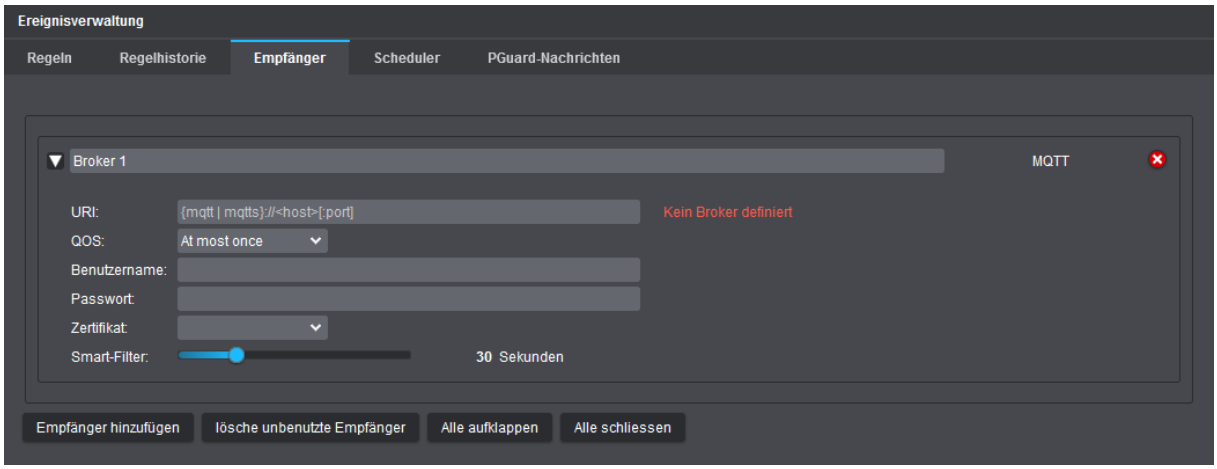

Abb. 13-6

- Geben Sie im angezeigten Eingabefeld einen beschreibenden Namen für den MQTT-Empfänger-Host ein.
- Geben Sie im Feld **URI** die Ziel-IP-Adresse Ihres MQTT-Servers (Schema/Protokoll und IP-Adresse des Rechners, auf dem die MQTT-Messaging-Server-Anwendung läuft) sowie die Portnummer mit vorangestelltem Doppelpunkt (:) ein, über die der Message-Broker erreichbar ist (siehe Beispiele unten):

  Beispiel für unverschlüsselte Verbindung (**mqtt**) über Standardport **1883**:

  ```
  mqtt://192.0.2.2:1883
  ```

  Beispiel für verschlüsselte TLS-Verbindung (**mqtts**) über Standardport **8883**:

  ```
  mqtts://192.0.2.2:8883
  ```

  Die o. g. IP-Adresse ist nur beispielhaft und muss mit der IP-Adresse des Rechners ersetzt werden, auf dem Ihr MQTT-Broker läuft.

- Wählen Sie aus der Drop-down-Liste **QoS** (Quality of Service) einen der folgenden QoS-Level (Stufe der Dienstqualität bzw. der Zuverlässigkeit für die Message-Zustellung beim Broker):

  - **At most once** (QoS der Stufe 0 – höchstens einmalige Zustellung; Standardeinstellung):
    - Garantiert, dass die Kamera die MQTT-Nachricht nur genau einmal versendet, es erfolgt jedoch keine Bestätigung vom Broker (Server) über den Empfang der Nachricht
    - Keine Garantie, dass die Nachricht erfolgreich beim Broker zugestellt wird
    - Kein erneuter Sendeversuch bzw. Retry seitens der Kamera (z. B. wenn Broker vorübergehend nicht erreichbar/ausgefallen ist), da die Nachricht nach dem Versenden nicht weiter in der Kamera aufbewahrt wird („Fire and forget"- bzw. „Abschicken und vergessen"-Methode)
    - Keine Erstellung und Übertragung von Duplikaten der ursprünglichen Nachricht
    - Schnellste, jedoch auch unzuverlässigste Art der MQTT-Nachrichtenübermittlung, aber mit geringstem Ressourcenverbrauch

  - **At least once** (QoS der Stufe 1 – mindestens einmalige Zustellung):
    - Garantiert, dass die MQTT-Nachricht der Kamera mindest einmal beim Broker zugestellt wird
    - Die Nachricht wird zunächst mit einer eindeutigen Nachrichtennummer (Packet Identifier) versehen, dann lokal auf der Kamera gespeichert (Outbound-Queue) und schließlich in regelmäßigen Zeitabständen wiederholt versendet, bis der Broker den Empfang der Nachricht mit einem sogenannten PUBACK-Paket inkl. passendem Packet Identifier quittiert
    - Übertragung von Duplikaten der ursprünglichen Nachricht möglich (z. B. wenn die Rückantwort des MQTT-Servers durch Verbindungsengpässe zuvor verloren ging)
    - Bester Kompromiss zwischen Zuverlässigkeit der MQTT-Nachrichtenübermittlung und Ressourcenverbrauch

  - **Exactly once** (QoS der Stufe 2 – genau einmalige Zustellung):
    - Garantiert, dass die MQTT-Nachricht der Kamera genau einmal beim Broker zugestellt wird
    - Zustellgarantie erfolgt durch mindestens vierstufigen Handshake zwischen Kamera und Broker
    - Zuverlässigste Art der MQTT-Nachrichtenübermittlung, aber auch ressourcenintensivste und langsamste QoS-Stufe aufgrund des relativ hohen Overheads

  *Beachten Sie, dass die eingestellte QoS-Stufe von Ihrem MQTT-Broker unterstützt werden muss.*

- Falls für den Verbindungsaufbau mit dem Message-Broker eine Client-Authentifizierung erforderlich ist, gehen Sie folgendermaßen vor:
  Geben Sie die Anmeldedaten für die Anmeldung beim MQTT-Server in die Felder **Benutzername** und **Passwort** ein und/oder wählen Sie zusätzlich/alternativ aus der Drop-down-Liste **Zertifikat** ein gültiges Client-Authentifizierungszertifikat aus, das auf Ihrer Kamera gespeichert ist (muss zuvor vom Message-Broker bereitgestellt und in den Keystore der Kamera importiert werden).

  *Die konkrete Vorgehensweise bezüglich der Authentifizierung gegenüber dem Broker ist abhängig von der Konfiguration Ihres MQTT-Servers.*
  *Beachten Sie, dass MQTT-Authentifizierungsdaten (Benutzername und Passwort) bei einer unverschlüsselten Verbindung im Klartext übertragen werden.*

Der **Smart-Filter** entspricht in seiner Funktion dem gleichen Parameter wie beim Empfängertyp **HTTP**.

### 13.3.3 ONVIF-MQTT

Bei diesem Empfängertyp handelt es sich um einen eigenständigen MQTT-Publishing-Client auf der Kamera, der nach den Vorgaben der ONVIF*)-Spezifikation (ONVIF Profile M) für die Verarbeitung von Analyse-Metadaten arbeitet. Sobald über das Netzwerk eine Verbindung zum angegebenen MQTT-Broker hergestellt wurde, empfängt der ONVIF-MQTT-Publishing-Client auf der Kamera zunächst alle von der Kamera generierten **EdgeAnalytics**-Ereignisse (Intrusion, Line Crossing, Loitering etc.), verarbeitet diese, kennzeichnet sie automatisch mit den entsprechenden Topics und sendet sie schließlich als spezielle MQTT-Nachrichten an den verbundenen MQTT-Broker.
Beachten Sie, dass dieser Empfängertyp nicht explizit für MQTT-Kamera-Aktionen innerhalb von Regeln ausgewählt werden kann, sondern als eigenständiger Prozess (ONVIF-MQTT-Publishing-Service) auf der Kamera ausgeführt wird, sobald die erforderlichen Daten vollständig und korrekt konfiguriert sind.

*) Beachten Sie die Angaben zum Rechteinhaber der Marke im Copyright- und Markenhinweis auf Seite 2.

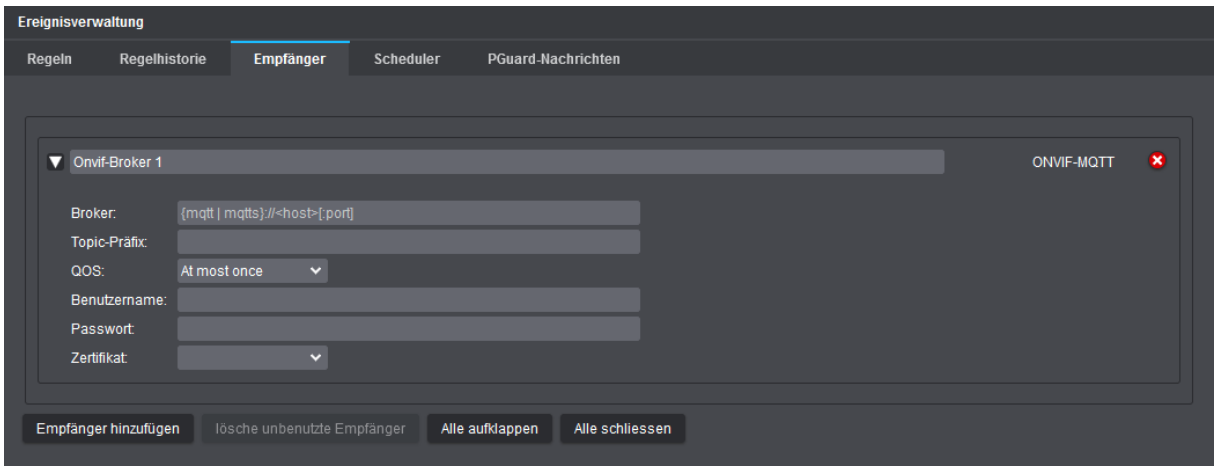

Abb. 13-7

Der Dialog zur Anbindung eines MQTT-Brokers entspricht im Wesentlichen dem Dialog des im vorherigen Abschnitt beschriebenen Empfängertyps **MQTT** (siehe Abschnitt „MQTT“ auf Seite 88).
Das Feld **Broker** ist hierbei identisch mit dem entsprechenden Feld **URI**.

**Topic-Präfix**
Das sogenannte **Topic-Präfix** ist die eindeutige Kennung der Kamera innerhalb eines veröffentlichten Topics (**EdgeAnalytics**-Themas).
Stellen Sie sicher, dass dieser Identifier nur einmal vergeben wird, da MQTT-Clients (Subscriber) andernfalls falsche Daten erhalten oder der MQTT-Broker möglicherweise die Verbindung verweigert.
Verwenden Sie beispielsweise entweder den Namen der Kamera (ohne Leerzeichen) oder die IP-Adresse der Kamera, wobei die Eindeutigkeit der Kennung im gesamten MQTT-Umfeld unbedingt gegeben sein muss.

## 13.3.4 E-Mail

Dieser Empfängertyp ermöglicht es Ihnen, einen E-Mail-Account anzugeben, der die von der Kamera generierten E-Mail-Nachrichten empfängt, um diese daraufhin an den oder die in der jeweiligen Regel eingetragenen E-Mail-Empfänger zu versenden.

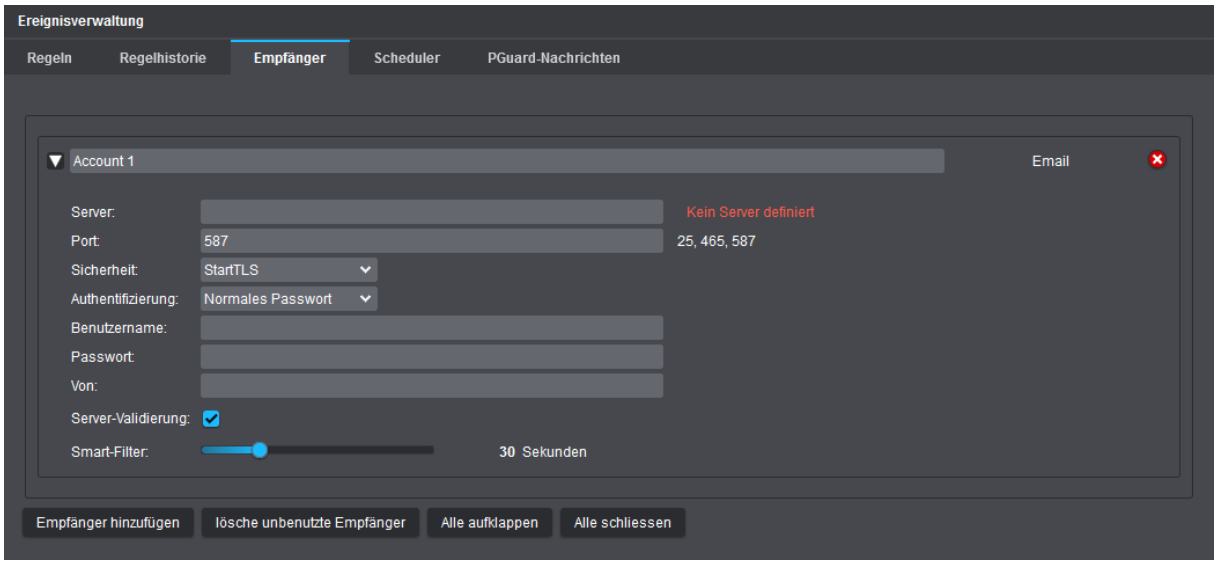


Abb. 13-8

- Geben Sie im angezeigten Eingabefeld einen beschreibenden Namen für den E-Mail-Account ein.
- Geben Sie im Feld **Server** die IP-Adresse des Rechners bzw. Mailservers ein, auf dem Ihr Postausgangsserver (SMTP) läuft, oder, falls Sie in den Netzwerkeinstellungen der Kamera erreichbare DNS-Server zur Namensauflösung eingetragen haben, den entsprechend registrierten Fully Qualified Domain Name (FQDN) des Mailservers, wie z. B. mx1.example.com.
- Geben Sie im Feld **Port** die Portnummer ein, unter der Ihr Postausgangsserver (SMTP) Verbindungen entgegennimmt (SMTP-Standardport: **25**, **456** oder **587**).
- Wählen Sie aus der Drop-down-Liste **Sicherheit** eine Methode zum Schutz der Authentifizierungsdaten und E-Mail-Nachrichten während ihrer Übertragung aus, z. B. eine zertifikatsbasierte verschlüsselte Verbindung mit **STARTTLS** (Port **587**) oder eine zertifikatsbasierte verschlüsselte Verbindung mit **SSL/TLS** (Port **465**).
- Geben Sie die erforderlichen Authentifizierungsdaten in die Felder **Benutzername** und **Passwort** ein, falls eine Authentifizierung gegenüber dem Mailserver erforderlich ist.
- Geben Sie im Feld **Von** die E-Mail-Adresse ein, die als Absenderadresse für die von der Kamera generierten E-Mail-Nachrichten verwendet werden soll.
- Deaktivieren Sie ggf. die Checkbox **Server-Validierung**, falls eine Gültigkeitsprüfung des Mailserver-Zertifikats nicht anwendbar/erforderlich ist.
  Bei der Validierung eines Mailservers wird vor dem eigentlichen E-Mail-Versand clientseitig geprüft, ob das vom Server übermittelte SSL/TLS-Zertifikat gültig ist. Ein Server-Zertifikat ist beispielsweise dann ungültig, wenn es abgelaufen ist, einen ungültigen Vertrauenspfad aufweist (Zertifikatskette ist unvollständig oder enthält ungültige Zertifikate) oder wenn der oben eingetragene Hostname bzw. FQDN des Mailservers nicht mit dem im Zertifikat angegebenen Hostnamen übereinstimmt.

> *Die korrekten Einstellungen hängen von der Konfiguration Ihres Mailservers ab. Wenden Sie sich ggf. an die für Ihre Netzwerkadministration zuständige Person oder an Ihren E-Mail-Anbieter, um weitere Informationen und Unterstützung zu erhalten.*

Der **Smart-Filter** entspricht in seiner Funktion dem gleichen Parameter wie beim Empfängertyp **HTTP**.

## 13.4 SCHEDULER

Auf der Registerkarte **Scheduler** können verschiedene wöchentlich wiederkehrende Zeitpläne erstellt werden, um diese dann innerhalb einer Regel als Bedingung für die Ausführung von Kamera-Aktionen zu definieren.

> *Sofern keine Ausnahmen für bestimmte Kalendertage festgelegt sind, gilt der jeweilige 7-Tage-Wochenzeitplan immer ganzjährig (und für künftige Kalenderjahre).*

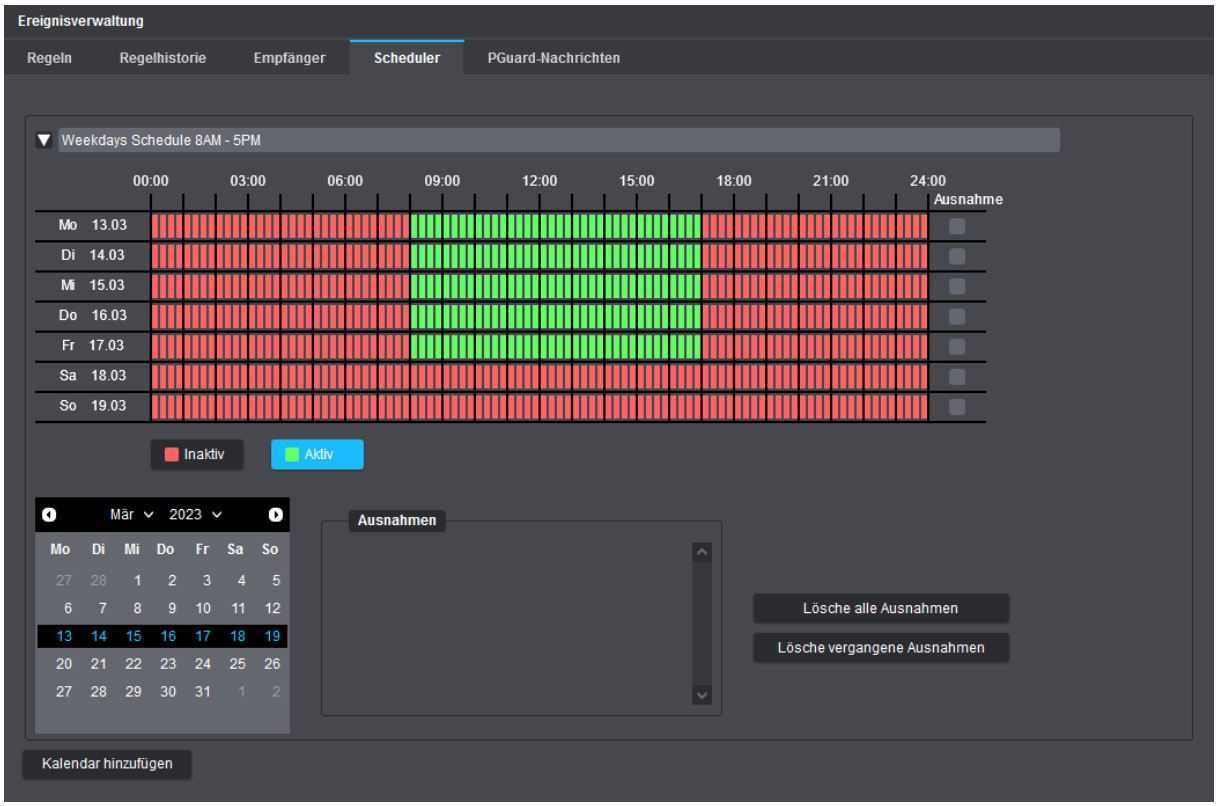


Abb. 13-9

- Geben Sie im angezeigten Eingabefeld einen beschreibenden Namen für den wiederkehrenden Wochenzeitplan ein.
- Klicken Sie je nach Anforderung auf die Schaltfläche **Inaktiv** (rot) oder **Aktiv** (grün) und markieren Sie die relevanten Zeitbereiche im Wochenplan mit gedrückter linker Maustaste (der kleinste wählbare Zeitbereich ist 15 Minuten).

Im obigen Beispiel (Abb. 13-9) wurde ein wiederkehrender Wochenzeitplan erstellt, der ganzjährig (ohne Ausnahmen) für Werktage in der Zeit von 08:00 bis 17:00 Uhr als aktiv markiert ist.
Wenn Sie später innerhalb einer Regel einen wiederkehrenden Wochenzeitplan als Bedingung definieren, können Sie wählen, ob Kamera-Aktionen nur in den als aktiv markierten Zeitbereichen oder nur in den als inaktiv markierten Zeitbereichen ausgeführt werden sollen.
Sie können mehrere Zeitpläne erstellen, z. B. einen für Wochentage und einen für Wochenenden, jeweils mit Ausnahmen für bestimmte Kalendertage, wie etwa für gesetzliche Feiertage, Betriebsferien oder Zeiten, in denen Wartungsarbeiten geplant sind. Um Ausnahmen hinzuzufügen, wählen Sie zunächst das entsprechende Datum im Kalender aus, aktivieren das Kontrollkästchen **Ausnahme** rechts neben dem Zeitblock für den Kalendertag und passen dann den betreffenden Zeitbereich nach Bedarf an.

## 13.5 PGUARD-NACHRICHTEN

### 13.5.1 Ereignis-Handler erstellen

Auf der Registerkarte **PGuard-Nachrichten** können Sie verschiedene **Ereignis-Handler** definieren, die bei Eintreten bestimmter Ereignisse automatisch **PGuard-Nachrichten** über das **Dallmeier Video**-Protokoll (kurz: **DaVid**) an einen eingetragenen Alarm-Host (**PGuard**) versenden.

> *Für die Auswertung und Verwaltung der gesendeten **PGuard-Nachrichten** muss die Software **PGuard advance** von Dallmeier auf dem jeweiligen Client-PC (Alarm-Host) installiert und gestartet sein.*

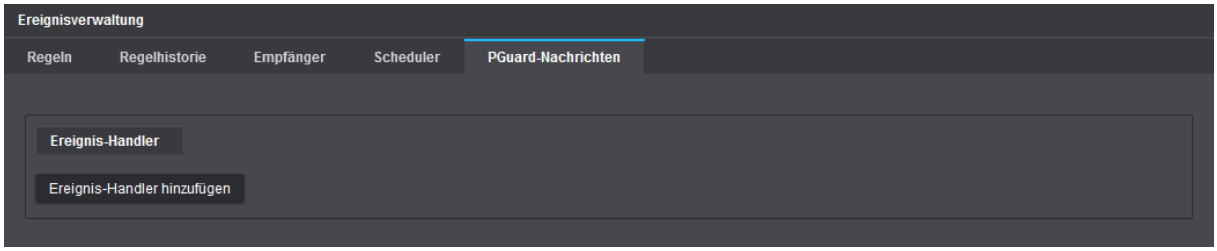


Abb. 13-10

- Klicken Sie **Ereignis-Handler hinzufügen**, um den entsprechenden Dialog zu öffnen.

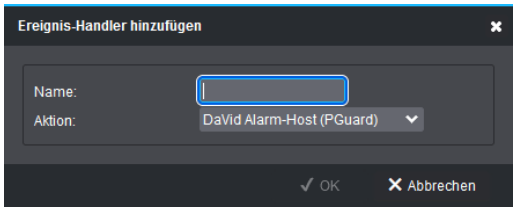


Abb. 13-11

- Geben Sie im Eingabefeld **Name** einen aussagekräftigen und eindeutigen Namen für den neuen Ereignis-Handler ein.
- Bestätigen Sie mit **OK**.

Der neue Ereignis-Handler wird daraufhin erstellt und kann nun konfiguriert werden (siehe im Folgenden).

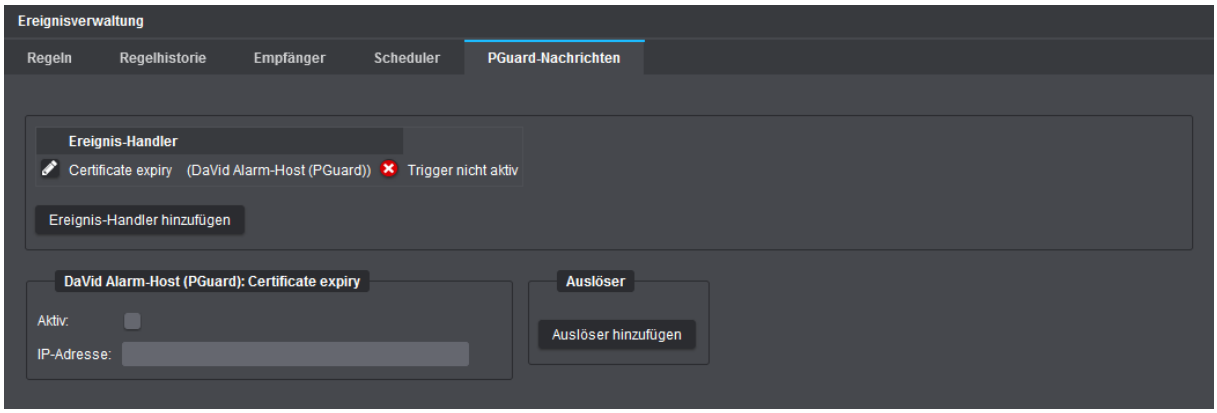


Abb. 13-12

- Stellen Sie zunächst sicher, dass sich Ihre Kamera und der jeweilige Alarm-Host im selben LAN befinden oder über ein Gateway miteinander kommunizieren können.
- Geben Sie die **IP-Adresse** des Alarm-Hosts ein, an den die **PGuard-Nachrichten** bei Eintreten bestimmter Ereignisse gesendet werden sollen.
- Klicken Sie **Auslöser hinzufügen**, um den Dialog **Ereignis-Auslöser hinzufügen** zu öffnen.

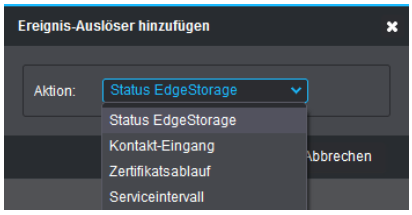


Abb. 13-13

- Wählen Sie aus der Drop-down-Liste **Aktion** einen Ereignis-Auslöser (Trigger).

Die folgenden Ereignis-Auslöser stehen zur Auswahl (für detaillierte Beschreibungen siehe Abschnitte weiter unten):

- **Status EdgeStorage**
- **Kontakt-Eingang**
- **Zertifikatsablauf**
- **Serviceintervall**

- Bestätigen Sie mit **OK**.
- Konfigurieren Sie die Auslöser-Parameter, sofern vorhanden.
- Fügen Sie dem Ereignis-Handler bei Bedarf weitere Auslöser hinzu.
- Aktivieren Sie die Checkbox **Aktiv**, um den Ereignis-Handler zu aktivieren.

### Status EdgeStorage

Bei diesem Ereignis-Auslöser wird immer dann eine **PGuard-Nachricht** an den Alarm-Host gesendet, wenn sich der **EdgeStorage**-Status ändert (siehe Kapitel „EdgeStorage“ auf Seite 75).

Folgende Statusänderungen werden über das **DaVid**-Protokoll gesendet:

- **MediaOK**
  Fehlerfreie Speicherkarte nach Kamera-Neustart gefunden oder
  Speicherkarte arbeitet nach einem temporären Fehler im laufenden Betrieb wieder fehlerfrei.

- **MediaErr**
  Speicherkarte wurde im laufenden Betrieb entfernt oder Speicherkarte ist fehlerhaft.

- **NoMedia**
  Keine Speicherkarte nach Kamera-Neustart gefunden.

- **Buffering**
  Netzwerkverbindung zu Dallmeier Aufzeichnungssystem unterbrochen >
  Speicherung (Pufferung) von Audio-, Video- und Metadaten auf Speicherkarte gestartet.

- **NoBuffering**
  Netzwerkverbindung zu Dallmeier Aufzeichnungssystem wiederhergestellt >
  Speicherung (Pufferung) von Audio-, Video- und Metadaten auf Speicherkarte beendet.

- **Delivering**
  Übertragung der gespeicherten Daten an Dallmeier Aufzeichnungssystem gestartet (SmartBackfill).

- **NoDelivering**
  Übertragung der gespeicherten Daten an Dallmeier Aufzeichnungssystem abgeschlossen.

- **BufferFull** („Linearer Puffer“)
  Speicherkarte ist voll > Speicherung (Pufferung) von Daten auf Speicherkarte gestoppt.

- **BufferOverwriting** („Ringpuffer“)
  Speicherkarte ist voll > Überschreiben der ältesten Daten im Ringspeicher (erneut) gestartet.

### Kontakt-Eingang

Bei diesem Ereignis-Auslöser wird immer dann eine **PGuard-Nachricht** an den Alarm-Host gesendet, wenn der ausgewählte **Kontakt-Eingang 1** oder **Kontakt-Eingang 2** an der Kamera-Hardware den jeweils angegebenen Status **Aktiviert** oder **Inaktiviert** (Ruhezustand) annimmt.

> *Detaillierte Beschreibungen zur Konfiguration der Kontakt-Eingänge Ihrer Kamera finden Sie im Abschnitt „Kontakt-Eingänge“ auf Seite 73.*

### Zertifikatsablauf

Bei diesem Ereignis-Auslöser werden wiederholt **PGuard-Nachrichten** an den Alarm-Host gesendet, bevor ein vorhandenes digitales Zertifikat auf der Kamera abläuft.
Die Meldungen werden in Abständen von 30, 10, 5, 3, 2, 1 und 0 Tagen vor dem Ablaufdatum gesendet.

**Serviceintervall**

Bei diesem Ereignis-Auslöser werden wiederholt **PGuard-Nachrichten** an den Alarm-Host gesendet, bevor die Software-Wartungslizenz für die Kamera abläuft.
Die Meldungen werden in Abständen von 60, 30 und 0 Tagen vor dem Ablaufdatum gesendet.

> *Details zu Ablaufdatum und -zeit der aktuellen Software-Wartungslizenz für Ihre Kamera (**Serviceintervall-Ende**) finden Sie z. B. im Kamera-Dialog **Informationen** auf der Registerkarte **Allgemeine Informationen** (siehe Abschnitt „Allgemeine Informationen“ auf Seite 142).*

## 13.5.2 Ereignis-Handler bearbeiten

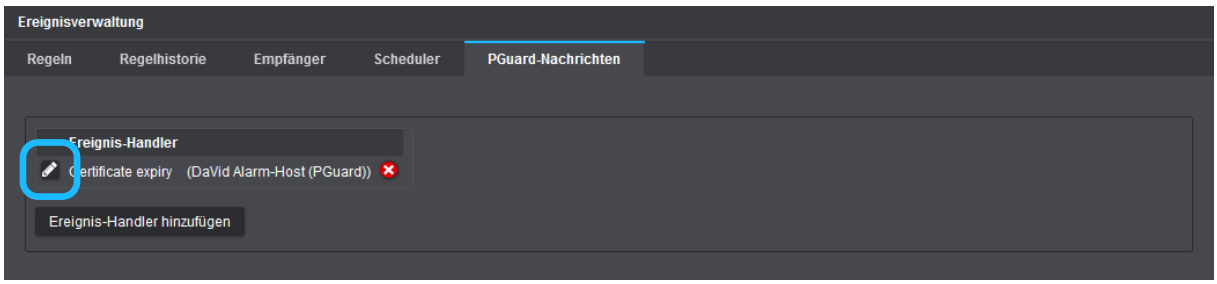


Abb. 13-14

- Klicken Sie zum Bearbeiten eines gespeicherten Ereignis-Handlers auf das **Stift**-Symbol links neben dem Namen des Ereignis-Handlers.
- Nehmen Sie die erforderlichen Änderungen vor.

## 13.5.3 Ereignis-Handler löschen

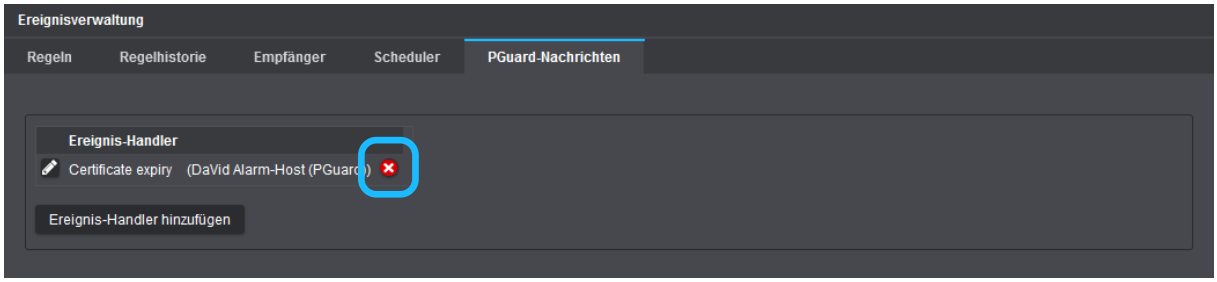


Abb. 13-15

- Klicken Sie zum Löschen eines gespeicherten Ereignis-Handlers auf das **Löschen**-Symbol (roter Kreis mit weißem Kreuz) rechts neben dem Aktionstyp des Ereignis-Handlers.
- Bestätigen Sie mit **OK**.

# DATENEINBLENDUNG

Die Funktion **Dateneinblendung** ermöglicht die Einbettung von externen Texten und Schnittstellen-Daten in den Video-Stream.
Externe Daten können beispielsweise von Kassensystemen, Geldausgabeautomaten (GAA) oder Zutrittskontrollsystemen (ZuKo-Systeme) über das Dallmeier Video-(**DaVid**-)Protokoll direkt an die Kamera übertragen werden.

Je nach Client-Anwendung bzw. -Gerät werden die eingebetteten Daten dann direkt im Videobild eingeblendet oder im Info-Bereich (Einblendungen) des entsprechenden Kamera-Splits mit dem Videobild angezeigt (z. B. bei der Auswertung mit **SeMSy® Compact**).

Vor der Einbettung in den Video-Stream können die empfangenen Daten gefiltert werden. Zudem kann die Position der Dateneinblendung direkt im Videobild festgelegt werden.

*ACHTUNG*

**Fehler bei der Dateneinblendung im Videobild aufgrund von inkompatibler Hardware**

Beachten Sie, dass die Einblendung und Positionierung der eingebetteten Daten direkt im Videobild nur in Verbindung mit folgenden Dallmeier Geräten genutzt werden kann:

- DIS-2/M DecoderPro HD
- DIS-2/M Multi-D HD
- WSD-2 HD

Die eingebetteten Daten werden in Verbindung mit den o. g. Geräten direkt im Live-Bild auf einem angeschlossenen Monitor eingeblendet.

Eine Aufzeichnung der eingebetteten Daten muss jedoch immer gesondert konfiguriert werden.
Aktivieren Sie dazu die Option **SW Kontakt** bzw. **Feldkontakt** in den Aufzeichnungseinstellungen (Ereignisaufzeichnung) der entsprechenden Spur.
Detaillierte Informationen dazu finden Sie beispielsweise in den Produktdokumentationen folgender Dallmeier Aufzeichnungssysteme:

- DIS-2/M Multi-D HD
- DIS-2/M NSU
- WSD-2 HD

## 14.1 DAUER

- Klicken Sie **Dateneinblendung** > **Anzeige**.

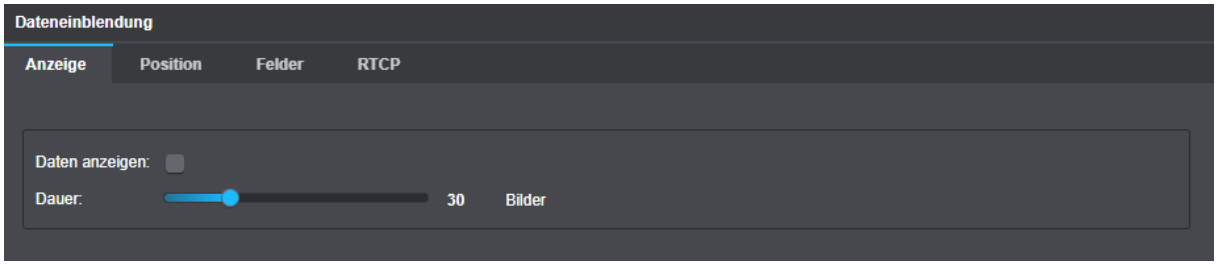


Abb. 14-1

- Aktivieren Sie die Einblendung mit der Checkbox **Daten anzeigen**.
- Wählen Sie die **Dauer** für die spätere Dateneinblendung.

Die empfangenen Daten werden in das zum Zeitpunkt des Datenempfangs aktuelle Bild (Frame) eingebettet und verbleiben für die gewählte **Dauer** (Anzahl Bilder).

## 14.2 POSITION

Um keine wichtigen Bildausschnitte zu verdecken, kann der Anzeigenbereich für die direkte Dateneinblendung im Videobild positioniert werden.

- Klicken Sie **Dateneinblendung** > **Position**.

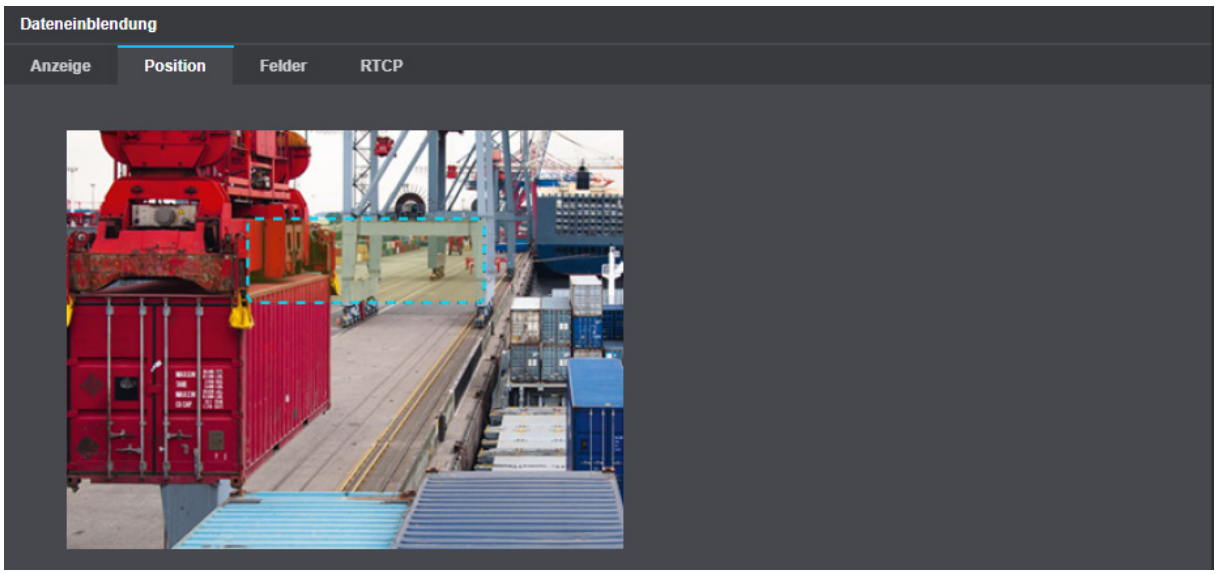


Abb. 14-2

- Markieren Sie den Anzeigenbereich durch Aufziehen eines Rechtecks.

*Beachten Sie, dass das Seitenverhältnis und die Größe (Auflösung) der tatsächlichen Bildschirmanzeige vom verwendeten Client abhängen.*

## 14.3 FELDER

Die empfangenen Daten können vor der Einbettung in den Video-Stream gefiltert werden.

*Die Filterung (Auswahl) wirkt sich nur auf empfangene Daten aus, also Daten die tatsächlich von externen Geräten an die Kamera übertragen wurden.*

▶ Klicken Sie **Dateneinblendung** > **Felder**.

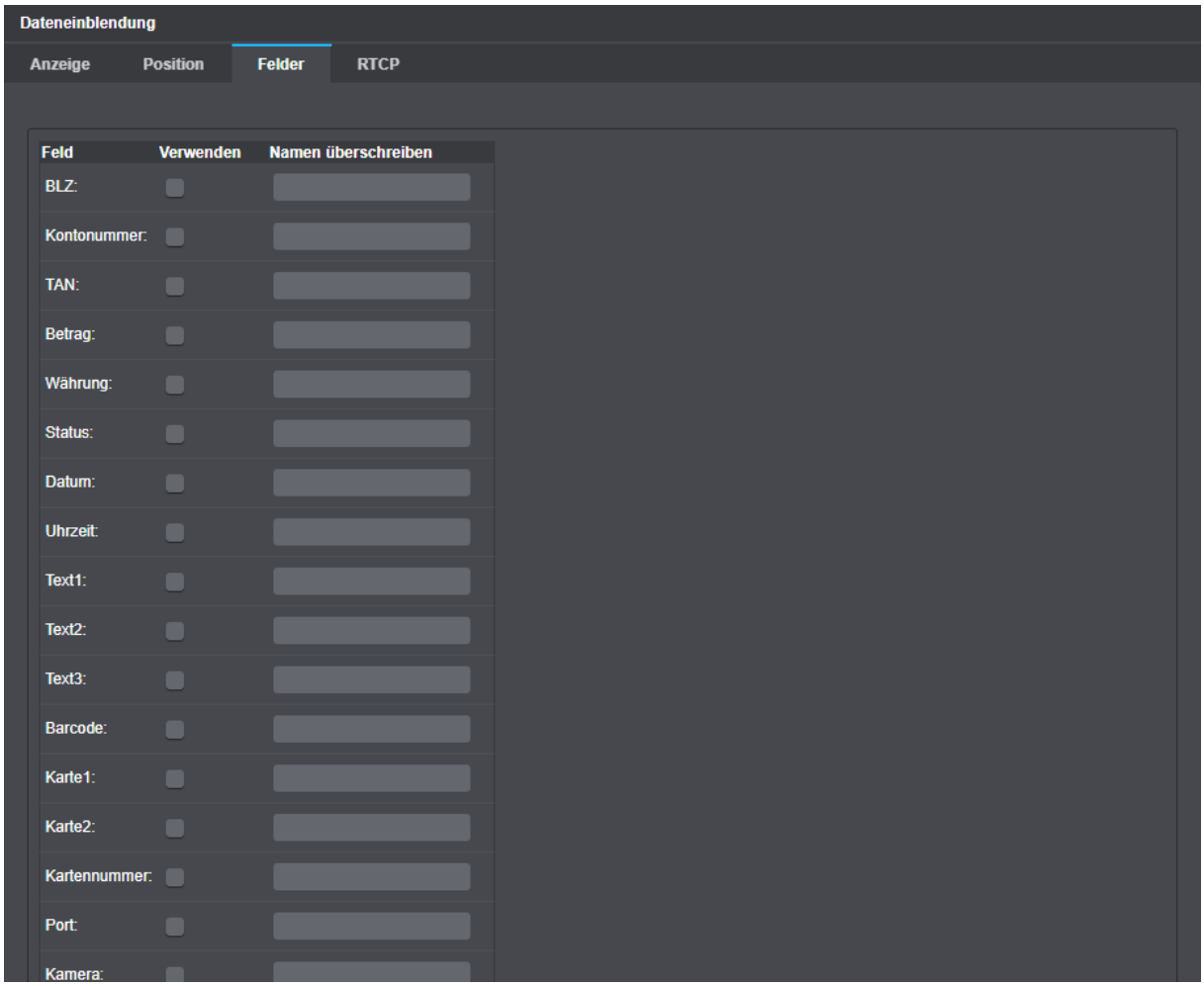


Abb. 14-3

▶ Wählen Sie alle relevanten Daten durch Aktivierung der entsprechenden Checkbox.

*Die Daten werden mit einem voreingestellten Text (Spalte **Feld**) angezeigt. Dieser kann durch einen neuen Text in der Spalte **Name überschreiben** ersetzt werden.*

*Wenn Streaming über RTCP aktiviert ist (siehe „Streaming“ auf Seite 55) muss die Versendung der Daten über RTCP ebenfalls aktiviert werden (**Dateneinblendung** > **RTCP**).*

# EDGEANALYTICS & AI APPS

Mit Domera® OS stehen ab Werk (je nach Kameramodell) zwei grundlegend unterschiedlich konzipierte Lösungen und Verfahren zur Videoinhaltsanalyse direkt auf der Kamera als sogenannte **EdgeAnalytics**-Anwendungen zur Verfügung:

**VCA Motion Detection** -> siehe „VCA Motion Detection“ auf Seite 103
Konventionelle Bewegungserkennung von Objekten mit einfacher Objektklassifizierung (dieses **EdgeAnalytics**-Verfahren ist in der Regel bereits ab Werk standardmäßig aktiviert)

**EdgeAnalytics AI Object Detection App** -> siehe „Edge Analytics AI Object Detection App“ auf Seite 116
KI-gestützte Objekterkennung (unabhängig von Bewegungen im Bild) mit erweiterter hochpräziser Objektklassifizierung auf Basis modernster Deep-Learning-Techniken und eines zuvor intensiv trainierten künstlichen neuronalen Netzes (nach Ablauf eines 30-tägigen Testzeitraums ist der Erwerb eines gültigen Lizenz-Codes für die weitere Nutzung dieses **EdgeAnalytics**-Verfahrens erforderlich)

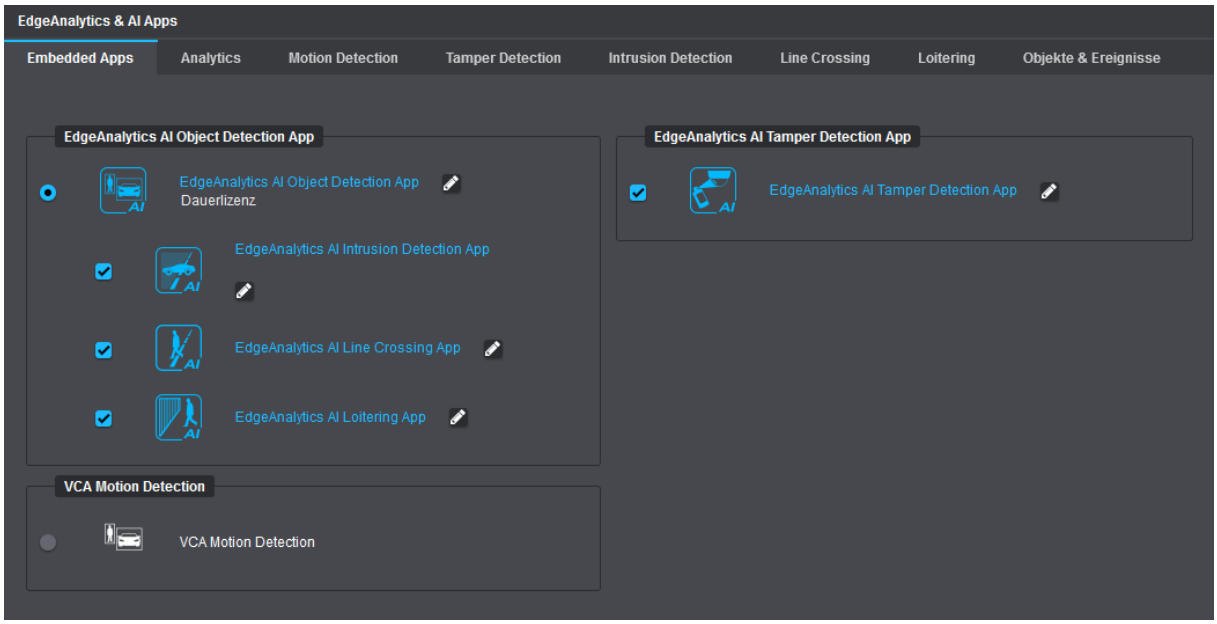


Abb. 15-1

Je nach Bedarf können zudem verschiedene Analyse-Zusatzanwendungen auf der Kamera aktiviert werden, die jeweils auf Grundlage der generierten Analysedaten des zuvor gewählten **EdgeAnalytics**-Verfahrens arbeiten (siehe im Folgenden).

*Für bestmögliche Analyseergebnisse auch bei anspruchsvollen Szenenbedingungen ist die **EdgeAnalytics AI Object Detection App** mit KI-gestützter Objekterkennung und erweiterter Objektklassifizierung empfohlen.*

In Verbindung mit **VCA Motion Detection** zur allgemeinen Bewegungserkennung von Objekten (Motion Detection) mit virtueller Bewegungsverfolgung (Virtual Motion Tracking) und einfacher Objektklassifizierung können folgende Analyse-Zusatzanwendungen aktiviert und dann auf den entsprechenden Registerkarten individuell konfiguriert werden:

- **VCA Intrusion Detection** -> siehe „Intrusion Detection“ auf Seite 121
  Automatische Generierung von Ereignissen, sobald erkannte Objekte in frei definierbare sensitive Bereiche im Bild eindringen oder diese wieder verlassen; beispielsweise verwendbar zur Außenhautabsicherung kritischer Infrastrukturen oder zur Gelände- und Freiflächensicherung

- **VCA Line Crossing** -> siehe „Line Crossing“ auf Seite 123
  Automatische Generierung von Ereignissen, sobald erkannte Objekte frei definierbare virtuelle Linien im Bild überqueren (virtueller Stolperdraht); beispielsweise verwendbar zur Perimeterabsicherung (Zaunüberwachung, Absicherung gegen Übersteigen)

In Verbindung mit der **EdgeAnalytics AI Object Detection App** zur KI-gestützten Objekterkennung mit erweiterter hochpräziser Objektklassifizierung können standardmäßig folgende Analyse-Zusatzanwendungen aktiviert und dann auf den entsprechenden Registerkarten individuell konfiguriert werden:

- **EdgeAnalytics AI Intrusion Detection App** -> siehe „Intrusion Detection“ auf Seite 121
  Automatische Generierung von Ereignissen, sobald relevante Objekte in frei definierbare sensitive Bereiche im Bild eindringen oder diese wieder verlassen; beispielsweise verwendbar zur Außenhautabsicherung kritischer Infrastrukturen oder zur Gelände- und Freiflächensicherung

- **EdgeAnalytics AI Line Crossing App** -> siehe „Line Crossing“ auf Seite 123
  Automatische Generierung von Ereignissen, sobald relevante Objekte frei definierbare virtuelle Linien im Bild überqueren (virtueller Stolperdraht); beispielsweise verwendbar zur Perimeterabsicherung (Zaunüberwachung, Absicherung gegen Übersteigen)

- **EdgeAnalytics AI Loitering App** -> siehe „Loitering“ auf Seite 125
  Automatische Generierung von Ereignissen, sobald sich Personen für einen ungewöhnlich langen (einstellbaren) Zeitraum in frei definierbaren sensitiven Bereichen im Bild aufhalten (Herumlungern); beispielsweise verwendbar zur Gebäude- und Eingangssicherung

**EdgeAnalytics AI Tamper Detection App** -> siehe „Tamper Detection“ auf Seite 127
Mit der **EdgeAnalytics AI Tamper Detection App** steht Ihnen bei Bedarf und unabhängig vom zuvor gewählten **EdgeAnalytics**-Verfahren eine weitere spezielle **EdgeAnalytics**-Anwendung zur Verfügung, die automatisch nachfolgend genannte Sabotagehandlungen oder Manipulationsversuche an der Kamera erkennt und entsprechende Ereignisse generiert:

- **Licht aus/an**-Erkennung, sobald sich die durchschnittliche Beleuchtungsstärke der erfassten Szene schlagartig verändert, wie beispielsweise bei:

  - abrupter Änderung des Raumlichts (durch Sabotage einer Lichtquelle)
  - Besprühen oder Verdecken der Kamera bzw. der Dome-Bubble
  - starker Blendung des Objektivs bzw. Bildsensors durch eine externe sehr helle Lichtquelle (z. B. Laser)

- **Bild zu unscharf** (z. B. durch Vernebeln der Kamera oder unbefugtes Defokussieren)

- **Globale Szenenänderung** (z. B. durch Verdrehen oder Verdecken der Kamera)

### Speicherung, Weiterverarbeitung und Auswertung von Kamera-Analysedaten

Die generierten Kamera-Analysedaten (detektierte Objekte, identifizierte Objektklassen, Bewegungsereignisse, erkannte Manipulationsversuche an der Kamera etc.) werden in Form von Metadaten (Zusatzinformationen zu den Videodaten, wie z. B. Position und Lage eines erkannten Objekts, Objekttyp, Bewegungsrichtung sowie Zeitstempel des Ereignisses) in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.

Für die korrekte Speicherung, Weiterverarbeitung und spätere Auswertung der Kamera-Analysedaten ist zum Zeitpunkt der Erstellung dieses Dokuments auf Folgendes zu achten:

Auf dem jeweiligen **Dallmeier Aufzeichnungssystem** muss

- in den Aufnahmeeinstellungen zur entsprechenden Kamera die Checkbox **EdgeAnalytics AI (VCA) verwenden** auf der Registerkarte **Encoder-Einstellungen** aktiviert sein (oder, je nach Version Ihrer Dallmeier Recording Server Software, die Checkbox **Bildverarbeitung am Recorder** auf der Registerkarte **Qualität** deaktiviert sein),
- in den Aufnahmeeinstellungen zur entsprechenden Kamera die Checkbox **Datenbank verwenden** zur Speicherung von Kamera-Analysedaten (Metadaten) in der Recorder-Datenbank aktiviert sein und
- in den globalen Recorder-Aufnahmeeinstellungen **Suchkriterien** die Checkbox **Bewegungskoordinaten** und die Checkbox **Sedor data** aktiviert sein.

Für die gezielte spätere Suche nach bestimmten Ereignissen und Objektklassen sowie die effiziente Auswertung von Vorfällen auf Basis der Kamera-Analysedaten steht Ihnen dann z. B. die Dallmeier Video-Management-Software **SeMSy® Compact** mit der Funktion **SmartFinder** zur Verfügung.

*Beachten Sie in diesem Zusammenhang auch die Ausführungen in den aktuellen Dokumentationen zu Ihrem Dallmeier Aufzeichnungssystem und zu **SeMSy® Compact**.*

### Ereignisgesteuerte Kamera-Aktionen auf Basis von **EdgeAnalytics**-Events

**EdgeAnalytics**-Events (z. B. generierte Ereignisse der **EdgeAnalytics AI Intrusion Detection App**) können bei Bedarf als Auslöser für eine Vielzahl von intelligenten Kamera-Aktionen verwendet werden (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).

## 15.1 VCA MOTION DETECTION

Das **EdgeAnalytics**-Verfahren **VCA Motion Detection** zur konventionellen Bewegungserkennung von Objekten mit einfacher Objektklassifizierung ist in der Regel bereits werkseitig auf der Kamera aktiviert. Bei diesem klassischen Verfahren der Videoinhaltsanalyse (**Video Content Analysis** oder kurz: **VCA**) direkt auf der Kamera werden Objekte in der erfassten Szene ausschließlich anhand von Bewegungen erkannt. Je nach Anforderung und Kamerakonfiguration können die sich im Bild bewegenden Objekte zusätzlich auf Basis einer allgemeinen, einfachen Analyse charakteristischer Merkmale automatisch klassifiziert und damit einem bestimmten Objekttyp (Person, Fahrzeug oder, falls nicht zutreffend, Unclassified) zugeordnet werden.
Solange keine Analyse-Zusatzanwendungen (**VCA Intrusion Detection** und/oder **VCA Line Crossing**) auf der Kamera aktiviert sind, werden lediglich die aktuellen Tracking-Koordinaten von erkannten Objekten inklusive der zugehörigen Zeitstempel und ggf. der jeweiligen Objektklasse von identifizierten Objekten kontinuierlich in Form von Metadaten an das jeweilige Dallmeier Aufzeichnungssystem gesendet, bis das jeweilige Objekt nicht mehr gültig ist.

- Aktivieren Sie das **EdgeAnalytics**-Verfahren **VCA Motion Detection**, falls noch nicht aktiv.

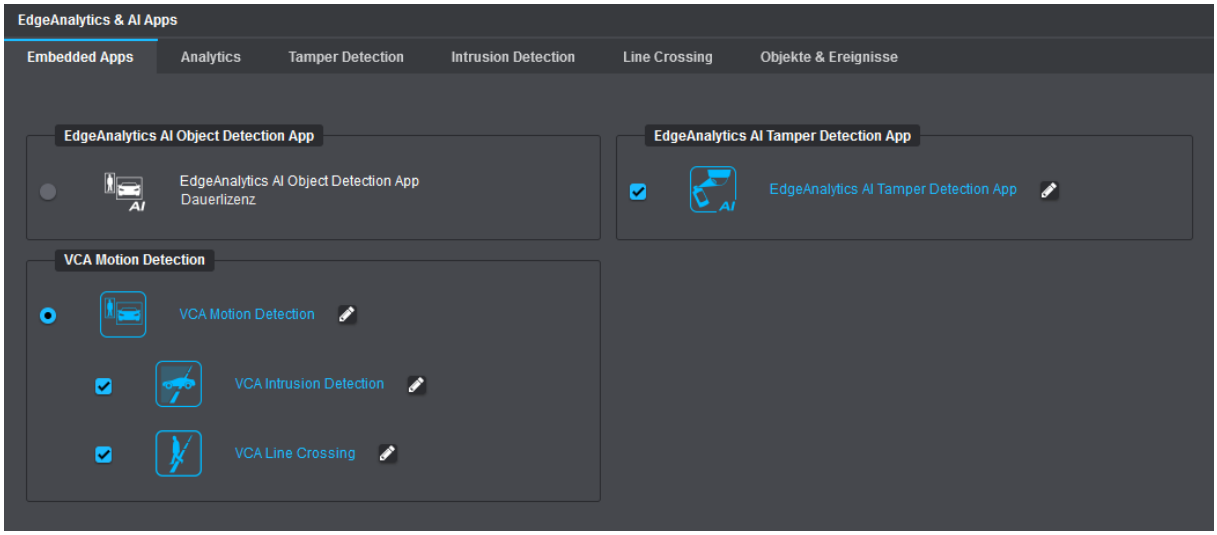


Abb. 15-2

- Klicken Sie auf das **Stift**-Symbol rechts neben dem Eintrag **VCA Motion Detection** oder wählen Sie die Registerkarte **Analytics**, um die Einstellungen des **EdgeAnalytics**-Verfahrens zu bearbeiten (siehe im Folgenden).

### 15.1.1 Allgemeine Einstellungen

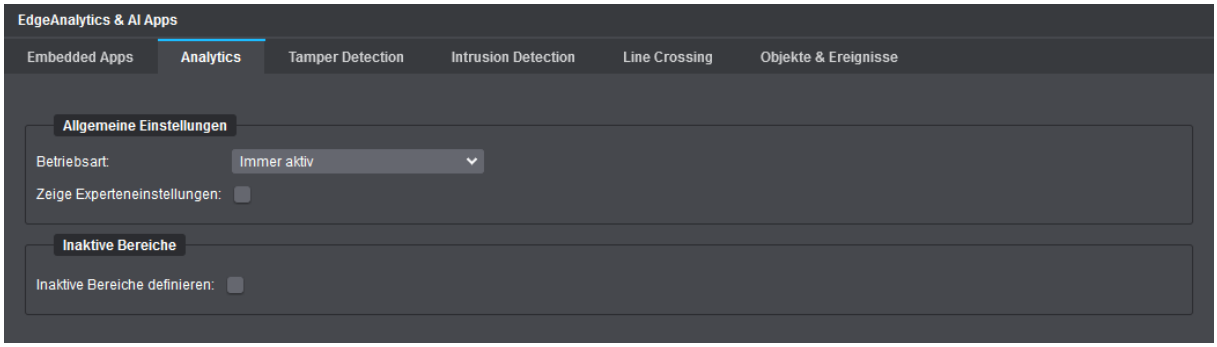


Abb. 15-3

**Betriebsart**

- Wählen Sie aus der Drop-down-Liste **Betriebsart** zwischen den folgenden Optionen:

- **Immer aktiv**
  Standardeinstellung (empfohlen)

- **Auf Anforderung durch Recorder**
  Die Videoinhaltsanalyse auf der Kamera (**EdgeAnalytics**) startet nur auf Anforderung mittels **DaVid**-Protokoll durch ein entsprechend konfiguriertes Dallmeier Aufzeichnungssystem.

**Zeige Experteneinstellungen**

- Aktivieren Sie die Checkbox **Zeige Experteneinstellungen**, um die verfügbaren Experteneinstellungen zur **VCA Motion Detection** anzuzeigen (siehe Abschnitt „Experteneinstellungen“ auf Seite 105).

## 15.1.2 Experteneinstellungen

Die **Experteneinstellungen VCA Motion Detection** bieten spezielle Einstellmöglichkeiten zur detaillierten Anpassung der Videoanalyse-Algorithmen. Sie werden erst angezeigt, wenn die entsprechende Checkbox unter **Allgemeine Einstellungen** (siehe oben) aktiviert wurde.
In den Experteneinstellungen können u. a. die Einstellungen zur Objekt- und Bewegungserkennung im Hinblick auf die Szenenbedingung (grundlegende Lichtverhältnisse in der erfassten Szene), die Kameraperspektive (Blickrichtung der Kamera nach der Installation) und die wesentlichen Objektmerkmale (minimal erforderliche und maximal gültige Objektgröße im Bild) vorgenommen werden.

> *Für bestmögliche Analyseergebnisse im Live-Betrieb sollten Sie alle Einstellungen, die Sie ändern, stets erneut auf der Registerkarte **Objekte & Ereignisse** überprüfen, z. B. hinsichtlich Anzahl, Plausibilität und Relevanz erkannter Objekte und Ereignisse (siehe Abschnitt „Objekte & Ereignisse“ auf Seite 129).*

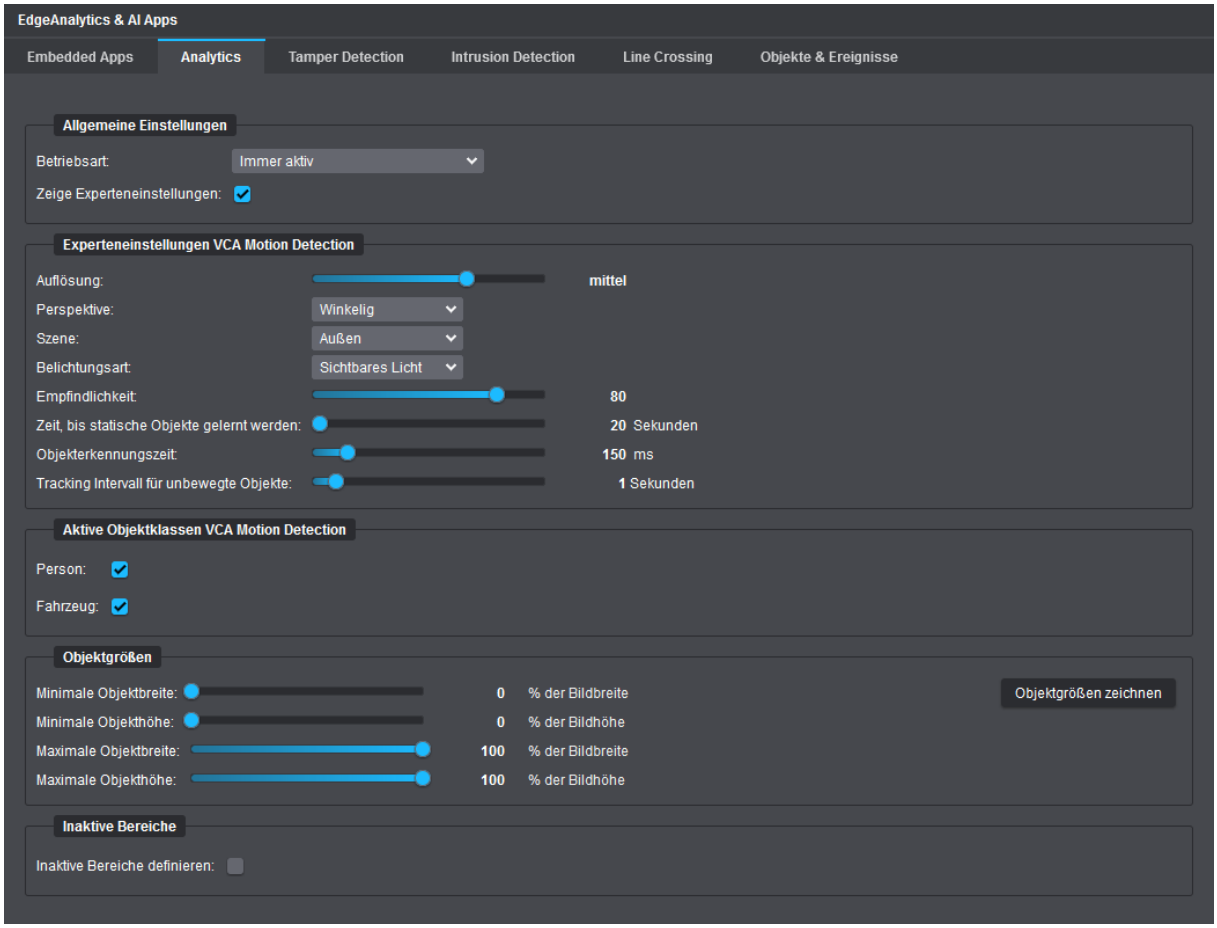


Abb. 15-4

**Auflösung**
Diese Einstellung bestimmt, mit welcher Bildauflösung das **EdgeAnalytics**-Verfahren intern arbeiten soll (Standardeinstellung: **mittel**). Die zu wählende Einstellung hängt hierbei von Art und Entfernung der zu beobachtenden Objekte, ihrer Geschwindigkeit sowie der vorherrschenden Szenerie ab.
Bei einer höheren Analyse-Auflösung können kleinere Objekte besser detektiert und präziser klassifiziert werden, die Analyse erfolgt jedoch mit weniger Bildern pro Sekunde, da die CPU-Auslastung der Kamera steigt. Je höher die Analyse-Bildrate (Bilder/Sekunde) ist, desto genauer erfolgt hingegen die virtuelle Bewegungsverfolgung von erkannten Objekten.

Die folgende Tabelle gibt Ihnen einen allgemeinen Überblick über die in der Regel empfohlenen Analyse-Auflösungen für verschiedene Szenenbedingungen und Objektgrößen (gilt jedoch ausschließlich für das **EdgeAnalytics**-Verfahren **VCA Motion Detection**):

| SZENENBEDINGUNG / OBJEKTGRÖSSEN | EMPFOHLENE ANALYSE-AUFLÖSUNG |
|---|---|
| **Innenbereich – Mittelgroße/große Objekte** | sehr klein |
| **Innenbereich – Kleine Objekte** | klein |
| **Außenbereich – Mittelgroße/große Objekte** | klein |
| **Außenbereich – Kleine Objekte** | mittel |

Tabelle 15-1

Die folgende Tabelle gibt Ihnen einen allgemeinen Überblick über die in der Regel empfohlenen Analyse-Bildraten für verschiedene Videoanalyseanwendungen (gilt jedoch ausschließlich für das **EdgeAnalytics**-Verfahren **VCA Motion Detection**):

| VIDEOANALYSEANWENDUNG | EMPFOHLENE ANALYSE-BILDRATE (BILDER/SEKUNDE) |
|---|---|
| **Allgemeine Bewegungserkennung von Objekten mit virtueller Bewegungsverfolgung** | 10–20 (min. 8) |
| **Intrusion Detection** | 5–15 (min. 5) |
| **Tamper Detection** | 5–15 (min. 5) |

Tabelle 15-2

Die Angaben zur aktuellen Analyse-Bildrate (Bilder/Sekunde) und zur gegenwärtig verursachten CPU-Auslastung durch die laufende Videoinhaltsanalyse finden Sie auf der Registerkarte **Objekte & Ereignisse** im Dialogbereich **Statistik** (siehe Abschnitt „Objekte & Ereignisse“ auf Seite 129).

- Stellen Sie die erforderliche **Auflösung** für die Analyse mit dem entsprechenden Schieberegler ein.

**Perspektive**
Diese Einstellung bestimmt, welche Kameraperspektive (Blickrichtung der Kamera nach der Installation) von den Videoanalyse-Algorithmen bei der Verarbeitung der Bilddaten berücksichtigt werden soll.

► Wählen Sie aus der Drop-down-Liste **Perspektive** die zutreffende Kameraperspektive aus:

- **Horizontal**: Waagrechter Blick auf die Szene bei relativ geringer Kamera-Montagehöhe
- **Von oben**: Senkrechter Blick auf die Szene von oben;
  in der Regel gut geeignet für die Erkennung der Bewegungsrichtung von Objekten
- **Winkelig**: Schräger Blick auf die Szene von oben mit einer Kameraneigung von ca. 30° und einer Kamera-Montagehöhe von ca. 2,5 – 3,0 m;
  empfohlen beispielsweise für **Intrusion Detection**

**Szene**
Diese Einstellung bestimmt, welche Szenenbedingung (grundlegende Lichtverhältnisse in der erfassten Szene) von den Videoanalyse-Algorithmen bei der Verarbeitung der Bilddaten berücksichtigt werden soll.

► Wählen Sie aus der Drop-down-Liste **Szene** die zutreffende Szenenbedingung aus:

- **Außen**: Empfohlene Einstellung für Szenen im Außenbereich
- **Innen**: Empfohlene Einstellung für Szenen im Innenbereich

**Belichtungsart**
Diese Einstellung bestimmt, welche Art der Belichtung in der erfassten Szene von den Videoanalyse-Algorithmen bei der Verarbeitung der Bilddaten berücksichtigt werden soll.

► Wählen Sie die zutreffende **Belichtungsart** aus der entsprechenden Drop-down-Liste aus:

- **Sichtbares Licht**: Geeignet beispielsweise im reinen Tag-Betrieb der Kamera
- **Infrarotes Licht**: Geeignet beispielsweise im reinen Nacht-Betrieb der Kamera bei eingeschalteten IR-LEDs
- **Automatik**: Die Videoanalyse-Algorithmen versuchen automatisch zu erkennen, um welche Art der Belichtung es sich in der erfassten Szene handelt.

**Empfindlichkeit**
Diese Einstellung definiert die Empfindlichkeit der Bewegungserkennung.

Je höher der eingestellte Wert ist, desto höher ist die Empfindlichkeit und desto schneller werden Bewegungen in der erfassten Szene als solche erkannt, d. h. umso geringfügiger müssen beliebige Veränderungen zwischen aufeinanderfolgenden Einzelbildern (engl. *frames*) ausfallen, um diese Veränderungen als neue Objekte zu definieren.

Empfohlene Empfindlichkeitswerte für verschiedene Situationen:

- **60**: Bei Situationen mit störendem Lichtflackern in der erfassten Szene (z. B. durch Glühbirnen).
- **70**: Bei starkem Bildrauschen durch hohe Signalverstärkung oder bei kontinuierlich kleinen Veränderungen im Bild (z. B. durch Regen, Schneefall oder sich im Wind bewegende Äste und Blätter eines Baums).
- **80**: Dies ist die Standardeinstellung und eignet sich für die meisten Anwendungsfälle.
- **90**: Bei Szenen mit geringem Kontrast (z. B. durch geringe Signalverstärkung) oder bei Aufnahmen mit dunklen oder grauen Objekten in der Nacht.
- **95**: Bei Szenen mit sehr geringem Kontrast (z. B. durch Nebel) oder bei Aufnahmen mit kaum sichtbaren Objekten in der Nacht.

▶ Legen Sie die erforderliche **Empfindlichkeit** mit dem entsprechenden Schieberegler fest.

**Zeit, bis statische Objekte gelernt werden**
Diese Einstellung legt die Zeit in Sekunden fest, die vergehen muss, bis detektierte Objekte, die sich nicht mehr im Bild bewegen, als Teil des Hintergrunds und nicht mehr als Objekte betrachtet werden (z. B. ein geparktes Fahrzeug).
Nach Ablauf der eingestellten Zeit werden die zugehörigen objektbezogenen Metadaten (z. B. aktuelle Tracking-Koordinaten inklusive Zeitstempel) nicht mehr weiter generiert und versendet.

Die Standardeinstellung ist **20 Sekunden**.

▶ Stellen Sie die erforderliche Ablaufzeit mit dem verfügbaren Schieberegler ein.

**Objekterkennungszeit**
Diese Einstellung gibt die Zeit in Millisekunden an, wie lange eine neu detektierte beliebige Bildveränderung in der erfassten Szene mindestens andauern muss, bis diese Veränderung als neues gültiges Objekt definiert wird.

Die Standardeinstellung ist **150 ms**.

▶ Stellen Sie die erforderliche minimale Gültigkeitsdauer mit dem verfügbaren Schieberegler ein.

**Tracking-Intervall für unbewegte Objekte**
Diese Einstellung bestimmt das Zeitintervall in Sekunden zwischen dem wiederholten Versenden von (statischen) Tracking-Koordinaten von detektierten Objekten, die sich bereits nicht mehr im Bild bewegen, bevor diese Objekte schließlich als Teil des Hintergrunds betrachtet werden (siehe Abschnitt „Zeit, bis statische Objekte gelernt werden“ auf Seite 108).
Mithilfe dieser Einstellung kann die Anzahl von redundanten Metadaten reduziert werden, die für eine spätere Auswertung nicht zwingend notwendig sind.

Beispiel:
Nachdem ein Fahrzeug geparkt wurde, wird es zunächst weiterhin als Objekt betrachtet. Die sich nicht mehr verändernden Tracking-Koordinaten des geparkten Fahrzeugs werden jedoch nach wie vor periodisch im jeweils eingestellten Zeitintervall in Form von Metadaten an das jeweilige Dallmeier Aufzeichnungssystem gesendet, bis das geparkte Fahrzeug nicht mehr länger als Objekt, sondern als Teil des Hintergrunds betrachtet wird.

- Stellen Sie das erforderliche Zeitintervall mit dem verfügbaren Schieberegler ein.

> *Ist das **Tracking-Intervall für unbewegte Objekte** auf **0 Sekunden** eingestellt (dies entspricht der Standardeinstellung), werden die statischen Tracking-Koordinaten eines Objekts zusammen mit jedem erzeugten Einzelbild (Frame) an das jeweilige Dallmeier Aufzeichnungssystem gesendet.*

### 15.1.2.1 Aktive Objektklassen VCA Motion Detection

Mithilfe der automatischen Objektklassifizierung können sich bewegende Objekte auf Basis einer allgemeinen, einfachen Analyse von charakteristischen Merkmalen automatisch klassifiziert und damit einem bestimmten Objekttyp (Person, Fahrzeug oder, falls nicht zutreffend, Unclassified) zugeordnet werden.
Die erkannten Objektzusatzinformationen werden in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.
Bei der späteren Auswertung von Ereignissen (z. B. mit **SeMSy® Compact**) können die Suchergebnisse dann speziell nach relevanten Objekttypen bzw. Objektklassen gefiltert werden.

- Um die automatische Objektklassifizierung einzuschalten, aktivieren Sie die entsprechenden Checkboxen **Person** und/oder **Fahrzeug**.

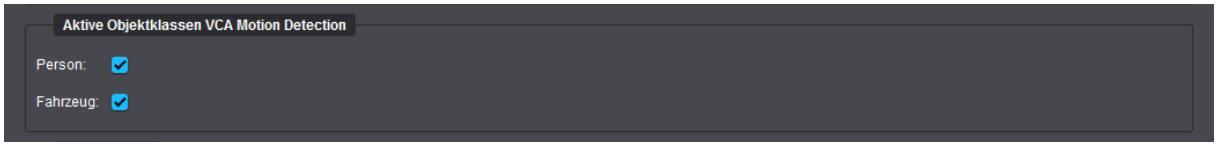


Abb. 15-5

Ein detektiertes Objekt wird in der Regel zunächst als unbekanntes Objekt betrachtet.
Die Genauigkeit der Zuordnung eines detektierten Objekts zu seinem korrekten Objekttyp steigt mit der Dauer der Analyse des jeweiligen Objekts.
Wenn beispielsweise ein Lieferwagen vom Bildrand her langsam in die Szene hineinfährt, kann das neu detektierte Objekt zunächst vorübergehend fälschlicherweise als „Person“ interpretiert werden.
Mit fortschreitender Analysedauer, d. h. sobald sich der Lieferwagen weiter in die Szene hineinbewegt, wird jedoch der richtige Objekttyp „Fahrzeug“ als solcher erkannt.
Beachten Sie also, dass sich die Klasse eines erkannten Objekts im Laufe seiner Analyse unter Umständen ändern kann.

*Mit aktivierter Objektklassifizierung steigt die CPU-Auslastung der Kamera.*

### 15.1.2.2 Objektgrößen

Die Einstellung der minimal erforderlichen und maximal gültigen Objektgröße prozentual in Bezug auf die Gesamtbildbreite/-höhe bestimmt, ab und bis zu welcher Größe ein Objekt als solches betrachtet wird. Objekte, die kleiner oder größer sind als die festgelegten Grenzwerte, werden automatisch von der Analyse ausgeschlossen.
Die Funktion **Objektgrößen zeichnen** erleichtert dabei das Abschätzen von gültigen Objektdimensionen in der erfassten Szene.

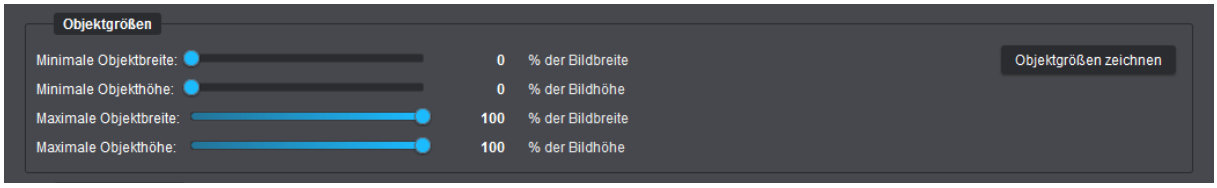


Abb. 15-6

**Minimale Objektbreite/-höhe**

- Legen Sie die minimal erforderliche Objektbreite/-höhe prozentual in Bezug auf die Gesamtbildbreite/-höhe mit den entsprechenden Schiebereglern fest.

**Maximale Objektbreite/-höhe**

- Legen Sie die maximal gültige Objektbreite/-höhe prozentual in Bezug auf die Gesamtbildbreite/-höhe mit den entsprechenden Schiebereglern fest.

Empfehlungen:

- Für eine zuverlässige Objekterkennung sowie eine möglichst genaue virtuelle Objektverfolgung sollte die Größe von Objekten mindestens 5–10 % des Gesamtbilds betragen.
- Für die Erkennung von Personen mit durchschnittlicher Größe sollte die Größe von Objekten bzw. von Personen ca. 10–20 % des Gesamtbilds betragen.
- Die Größe eines Objekts sollte in der Regel nicht mehr als 40 % des Gesamtbilds betragen.
- Objekte (Personen) sollten sich der Kamera nicht näher als bis zu 3 Meter nähern.

*Die o. g. Empfehlungen gelten ausschließlich für das **EdgeAnalytics**-Verfahren **VCA Motion Detection**.*

### Objektgrößen zeichnen

- Klicken Sie auf die Schaltfläche **Objektgrößen zeichnen** (Abb. 15-6), um im daraufhin angezeigten Vorschaubild mit Ihrer Maus die minimal erforderlichen und maximal gültigen Größen für Objekte in der erfassten Szene zu definieren.

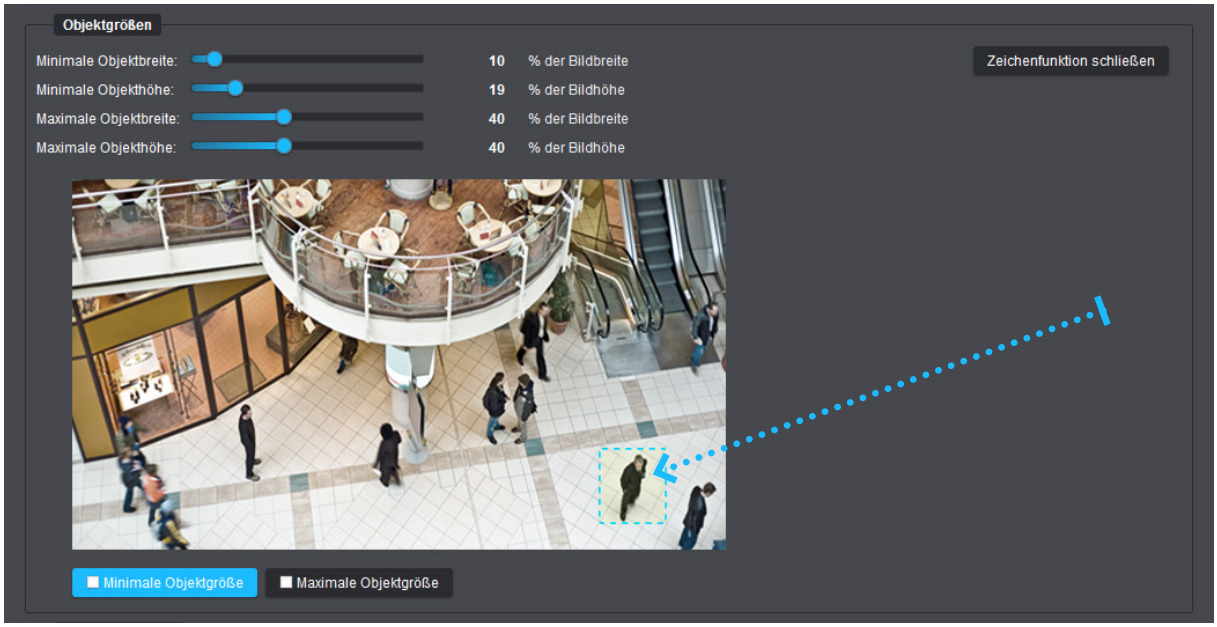


Abb. 15-7

- Klicken Sie auf die Schaltfläche **Minimale Objektgröße**.
- Positionieren Sie den Mauszeiger an der Stelle, an der Sie mit dem Zeichnen beginnen wollen.
- Ziehen Sie mit gedrückter linker Maustaste ein Rechteck in der erforderlichen Größe auf (siehe Pfeil in Abb. 15-7).
- Lassen Sie die Maustaste los, um das Zeichnen des Rechtecks abzuschließen.
- Klicken Sie auf die Schaltfläche **Maximale Objektgröße** und wiederholen Sie die letzten Schritte.

Die Werte der jeweiligen Schieberegler werden entsprechend der gezeichneten Objektgrößen automatisch angepasst.

- Klicken Sie auf die Schaltfläche **Zeichenfunktion schließen**, um die Zeichenfunktion zu beenden.

*Verwenden Sie reale Objekte als Größenreferenz beim Zeichnen der Rechtecke.*

### 15.1.3 Inaktive Bereiche

Mithilfe der Funktion **Inaktive Bereiche** können einzelne oder mehrere frei definierbare Bereiche im Bild generell von der Videoinhaltsanalyse ausgeschlossen werden.
Auf diese Weise lassen sich zum einen die Anzahl nicht relevanter Objekte und Ereignisse (z. B. bedingt durch vorbeigehende Fußgänger oder durchfahrende Fahrzeuge an den Bildrändern sowie aufgrund kontinuierlicher Bewegung von Wolken, Vegetation und Gewässer) auf ein Minimum reduzieren und zum anderen die Prozessorauslastung auf der Kamera (gegenwärtig verursachte CPU-Auslastung durch die laufende Videoinhaltsanalyse) senken.

Zur Erstellung und Bearbeitung inaktiver Bereiche im Bild stehen nach Aktivierung der Checkbox **Inaktive Bereiche definieren** eine Live-Vorschau (Bildrate 1 fps) sowie verschiedene Werkzeuge zur Verfügung.

Inaktive Bereiche werden im Vorschaubild rot maskiert.
Alle gemachten Änderungen werden stets verzögerungsfrei und ohne weitere Benutzeraktion übernommen.

Zur Erstellung inaktiver Bereiche im Bild gehen Sie folgendermaßen vor:

- Aktivieren Sie die Checkbox **Inaktive Bereiche definieren**.
- Wählen Sie das erforderliche Werkzeug zum Zeichnen, Bearbeiten oder Löschen von inaktiven Bereichen (siehe im Folgenden).

**Polygon zeichnen**

- Klicken Sie auf die Schaltfläche **Polygon zeichnen**.
- Legen Sie jeweils per Linksklick mit der Maus die Ankerpunkte (Ecken) eines Polygons (Vielecks) fest, das als inaktiver Bereich definiert werden soll.
- Schließen Sie per Rechtsklick mit der Maus oder mit der **Enter**-Taste auf Ihrer Tastatur die Erstellung des Vielecks ab (es wird kein weiterer Ankerpunkt gesetzt).

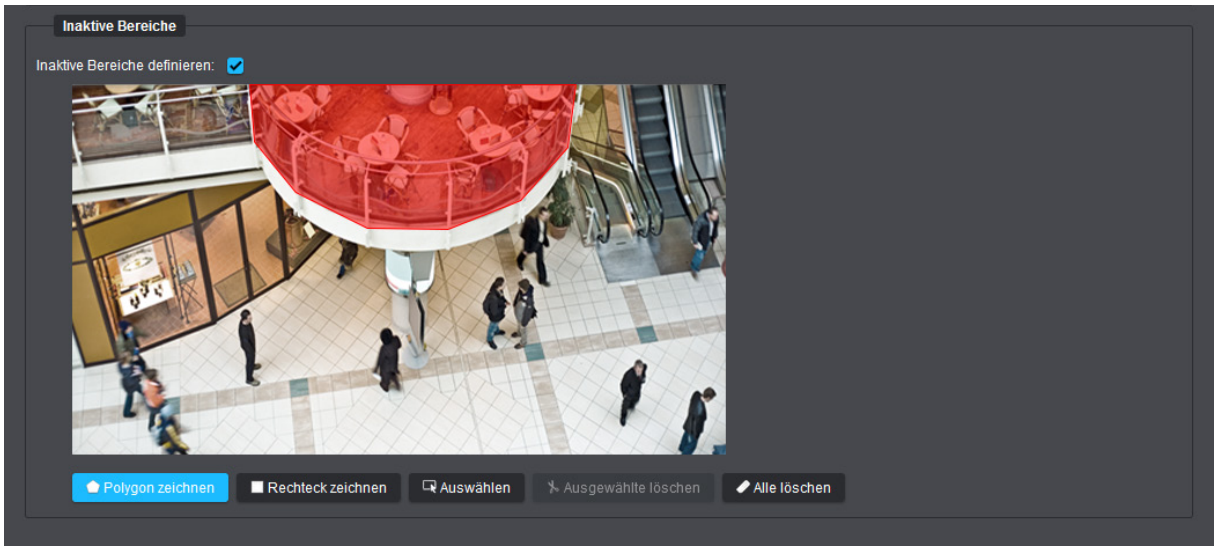


Abb. 15-8

*Sie können mehrere polygonale Bereiche im Bild als inaktiv definieren.*
*Die Ankerpunkte (Ecken) eines eingezeichneten Polygons können nachträglich bearbeitet werden (siehe Abschnitt „Auswählen/Bearbeiten“ auf Seite 115).*

**Rechteck zeichnen**

- Klicken Sie auf die Schaltfläche **Rechteck zeichnen**.
- Legen Sie mit gedrückter linker Maustaste einen rechteckigen Bereich im Bild als inaktiv fest (Maustaste abschließend loslassen).

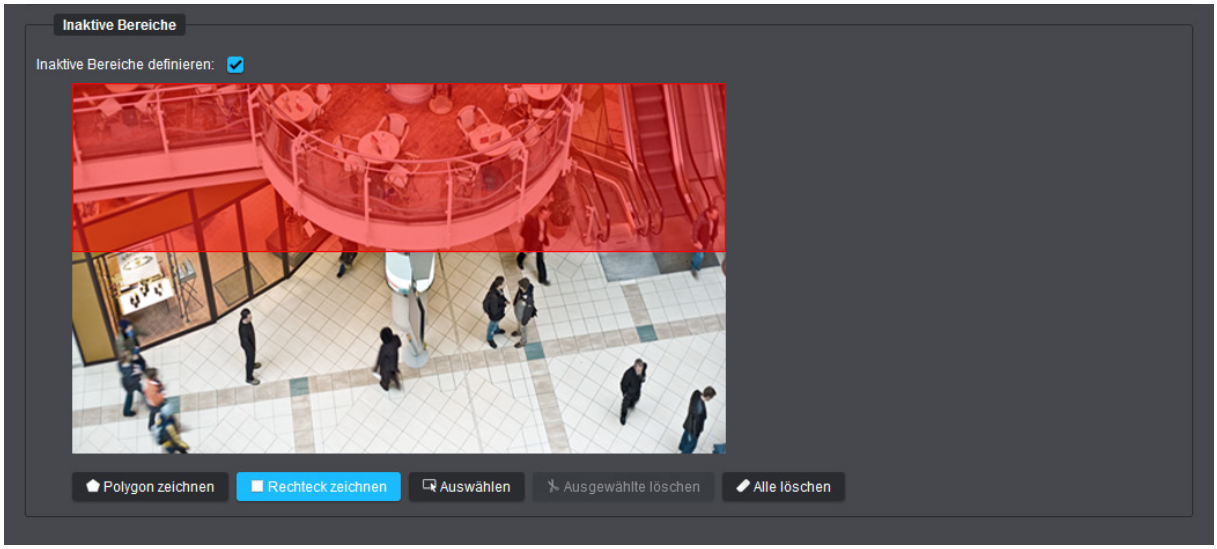


Abb. 15-9

*Sie können mehrere rechteckige Bereiche im Bild als inaktiv definieren.*
*Die Ankerpunkte (Ecken) eines eingezeichneten Rechtecks können nachträglich bearbeitet werden (siehe Abschnitt „Auswählen/Bearbeiten“ auf Seite 115).*

**Auswählen/Bearbeiten**

- Klicken Sie auf die Schaltfläche **Auswählen**.
- Klicken Sie mit der linken Maustaste auf einen inaktiven Bereich, um diesen auszuwählen.

Der gewählte inaktive Bereich wird an seinen Ankerpunkten (Ecken) mit kleinen weißen Kreisen markiert.

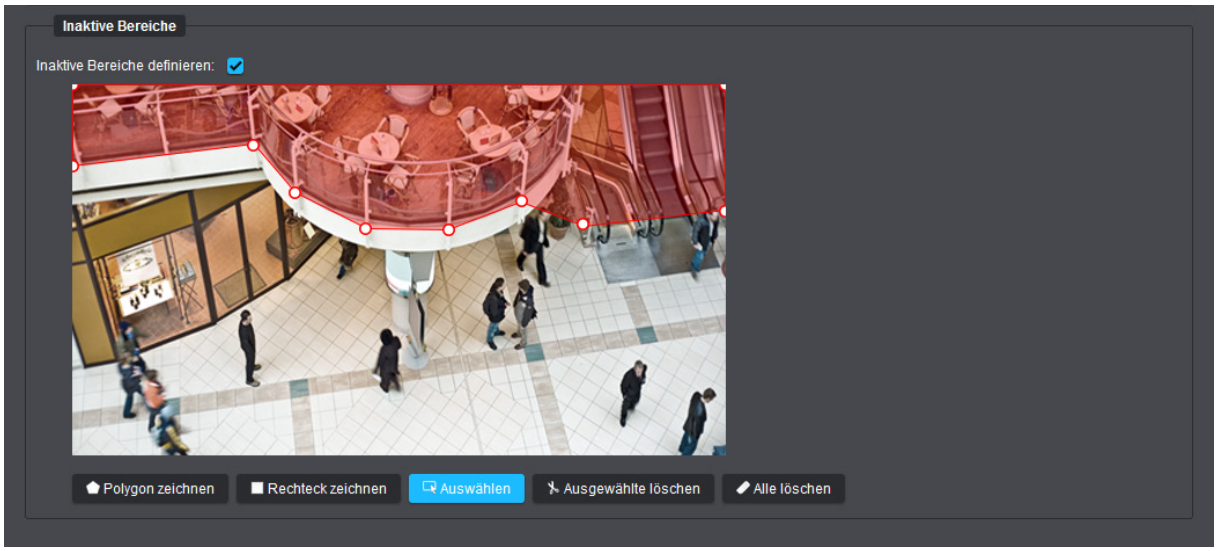


Abb. 15-10: Zur Bearbeitung ausgewähltes Polygon (erkennbar an den weißen Ankerpunkten)

- Verschieben Sie die weißen Kreise mit gedrückter linker Mautaste, um den definierten inaktiven Bereich zu ändern (es können neue Ankerpunkte mit der linken Maustaste hinzufügt, aber keine bestehenden Ankerpunkte gelöscht werden).

Zum Löschen von inaktiven Bereichen verfahren Sie wie folgt:

**Alle löschen**

- Klicken Sie auf die Schaltfläche **Alle löschen**, um alle definierten inaktiven Bereiche zu löschen.

**Ausgewählte löschen**

- Klicken Sie auf die Schaltfläche **Auswählen**.
- Klicken Sie mit der linken Maustaste auf einen eingezeichneten inaktiven Bereich, um diesen auszuwählen (**Strg**-Taste auf Ihrer Tastatur gedrückt halten, um mehrere auszuwählen).
- Klicken Sie auf die Schaltfläche **Ausgewählte löschen** oder drücken Sie die **Entf**-Taste auf Ihrer Tastatur, um alle zuvor ausgewählten markierten Bereiche zu löschen.

## 15.2 EDGE ANALYTICS AI OBJECT DETECTION APP

LIZENZ-CODE ERFORDERLICH

**Für die Nutzung dieses Features ist nach Ablauf eines 30-tägigen Testzeitraums* der Erwerb eines gültigen Lizenz-Codes erforderlich.**

Weitere Informationen finden Sie in der Produktspezifikation zu Ihrer Kamera auf der Dallmeier Webseite unter https://www.dallmeier.com/.

Um einen gültigen Lizenz-Code für dieses Feature zu erwerben, wenden Sie sich an Ihren Dallmeier Vertriebspartner.

* Die Ablaufzeit des Testzeitraums beginnt erst, wenn die Funktion zum ersten Mal aktiviert wird. Sobald die Funktion während des Testzeitraums deaktiviert oder die Kamera von der Stromversorgung getrennt wird, wird die Ablaufzeit des 30-tägigen Testzeitraums pausiert.

Als logische und konsequente Weiterentwicklung der klassischen Bewegungserkennung mit einfacher Objektklassifizierung (siehe Abschnitt „VCA Motion Detection“ auf Seite 103) verwendet die zukunftsorientierte **EdgeAnalytics AI Object Detection App** mit KI-gestützter Objekterkennung ein auf Basis modernster Deep-Learning-Techniken intensiv trainiertes künstliches neuronales Netz, um die erfasste Szene unabhängig von Bewegungen im Bild zu analysieren und erkannte Objekte verschiedenster Art (Person, Zweirad, Auto uvm.) äußerst präzise, zuverlässig und in Echtzeit zu klassifizieren.

► Aktivieren Sie die **EdgeAnalytics AI Object Detection App**.

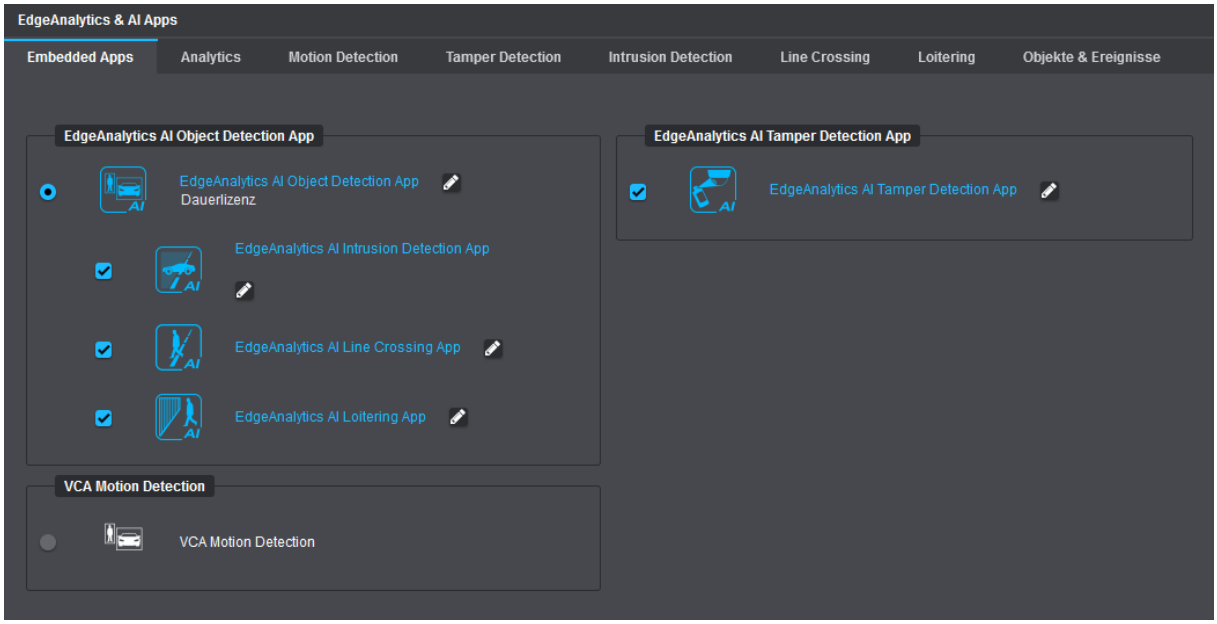


Abb. 15-11

► Klicken Sie auf das **Stift**-Symbol rechts neben dem Eintrag **EdgeAnalytics AI Object Detection App** oder wählen Sie die Registerkarte **Analytics**, um die Einstellungen des **EdgeAnalytics**-Verfahrens zu bearbeiten (siehe im Folgenden).

## 15.2.1 Allgemeine Einstellungen

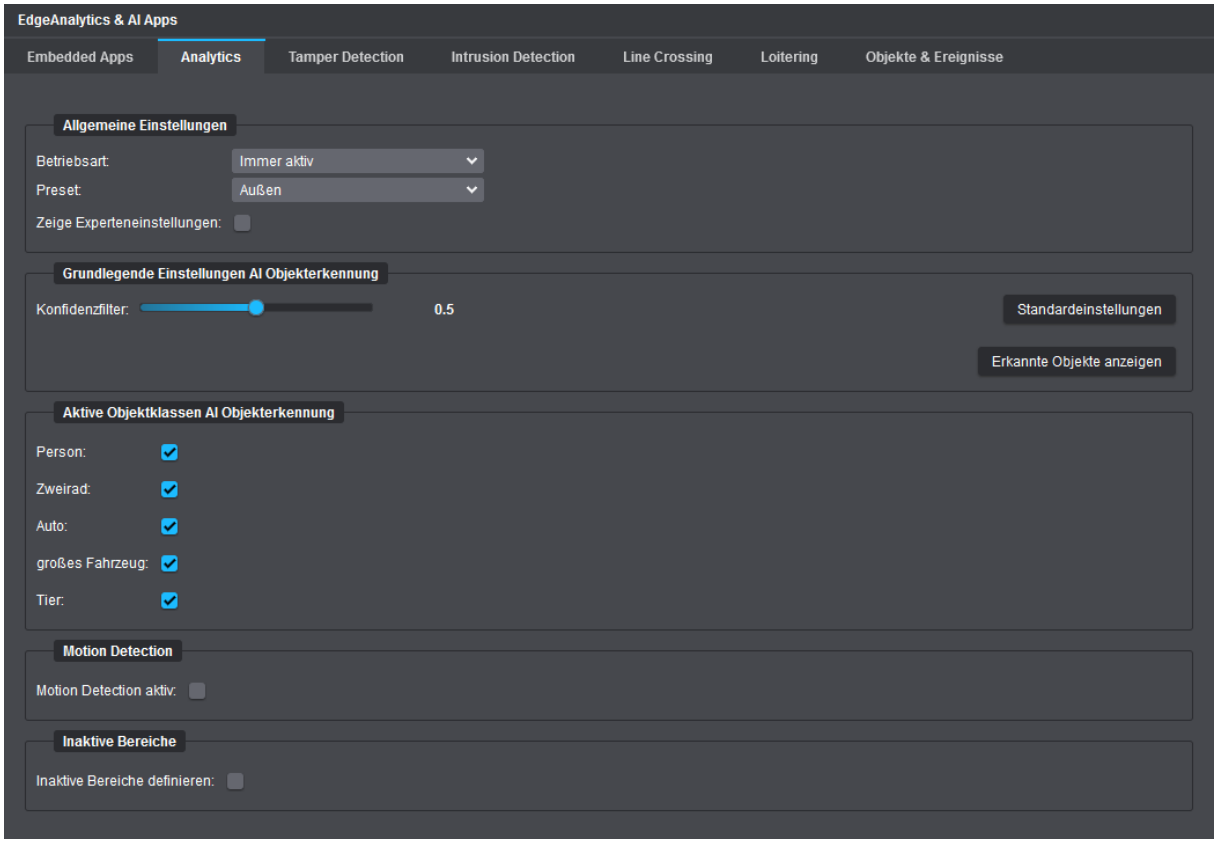


Abb. 15-12

**Betriebsart**

▶ Wählen Sie aus der Drop-down-Liste **Betriebsart** zwischen den folgenden Optionen:

- **Immer aktiv**
  Standardeinstellung (empfohlen)

- **Auf Anforderung durch Recorder**
  Die Videoinhaltsanalyse auf der Kamera (**EdgeAnalytics**) startet nur auf Anforderung mittels **DaVid**-Protokoll durch ein entsprechend konfiguriertes Dallmeier Aufzeichnungssystem.

**Preset**

Diese Einstellung bestimmt, welche Szenenbedingung (grundlegende Lichtverhältnisse in der erfassten Szene) von den Videoanalyse-Algorithmen bei der Verarbeitung der Bilddaten berücksichtigt werden soll.

▶ Wählen Sie aus der Drop-down-Liste **Preset** die zutreffende Szenenbedingung aus:

- **Außen**: Empfohlene Einstellung für Szenen im Außenbereich
- **Innen**: Empfohlene Einstellung für Szenen im Innenbereich

**Zeige Experteneinstellungen**

▶ Aktivieren Sie die Checkbox **Zeige Experteneinstellungen**, um die verfügbaren Experteneinstellungen zur **EdgeAnalytics AI Object Detection App** anzuzeigen (siehe Abschnitt „Experteneinstellungen“ auf Seite 119).

**Konfidenzfilter**
Der für jeden Objekt-Begrenzungsrahmen („Bounding Box“) angezeigte Konfidenz- bzw. Vertrauenswert gibt an, wie sicher die KI-gestützte Objekterkennung ist bzw. wie sehr sie sich selbst vertraut, die Objektklasse eines erkannten Objekts korrekt interpretiert zu haben.
Die jeweiligen Werte können dabei zwischen 0 (kein Vertrauen in die Erkennung) und 1 (hohes Vertrauen) liegen. Je höher der Konfidenzwert ist, desto überzeugter ist die Analyse-Engine also von der Richtigkeit seiner eigenen Ergebnisse.
Mithilfe der Funktion **Konfidenzfilter** können erkannte Objekte, deren Konfidenzwerte unter dem eingestellten Schwellwert liegen, automatisch verworfen werden.

Die Standardeinstellung ist **0.5**.

- Klicken Sie auf die Schaltfläche **Erkannte Objekte anzeigen**, um die Objektanzeige zu aktivieren.
- Legen Sie den erforderlichen Schwellwert mit dem Schieberegler **Konfidenzfilter** fest.

*Beachten Sie, dass erkannte Objekte, deren Konfidenzwerte nur geringfügig unter dem eingestellten Schwellwert liegen, nicht unmittelbar verworfen werden.*

**Aktive Objektklassen AI Objekterkennung**
Mithilfe der automatischen KI-gestützten Objektklassifizierung können Objekte im Bild unabhängig von Bewegungen äußerst präzise und zuverlässig klassifiziert und damit einem bestimmten Objekttyp (Person, Zweirad, Auto etc.) zugeordnet werden.
Die erkannten Objektzusatzinformationen werden in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.
Bei der späteren Auswertung von Ereignissen (z. B. mit **SeMSy® Compact**) können die Suchergebnisse dann speziell nach relevanten Objekttypen bzw. Objektklassen gefiltert werden.

- Um die automatische Objektklassifizierung einzuschalten, aktivieren Sie die entsprechende Checkbox hinter dem jeweiligen Objekttyp.

*Mit aktivierter Objektklassifizierung steigt die CPU-Auslastung der Kamera.*

**Motion Detection**
Diese Einstellung dient zur zusätzlichen Aktivierung einer konventionellen Bewegungserkennung von Objekten im Bild, die im Wesentlichen nach dem gleichen Prinzip arbeitet wie das herkömmliche **EdgeAnalytics**-Verfahren **VCA Motion Detection**.
Nach Aktivierung der Funktion wird eine neue Registerkarte mit der Bezeichnung **Motion Detection** angezeigt, auf der die Empfindlichkeit der Bewegungserkennung nach Bedarf angepasst werden kann.
Je empfindlicher die Einstellung gewählt wird (Standardeinstellung: **normal**), desto schneller werden Bewegungen in der erfassten Szene als solche erkannt, d. h. umso geringfügiger müssen beliebige Veränderungen zwischen aufeinanderfolgenden Einzelbildern (engl. *frames*) ausfallen, um diese Veränderungen als neue, nicht klassifizierte Objekte zu definieren.

**Inaktive Bereiche**
Beschreibungen zu dieser Funktion finden Sie im Abschnitt „Inaktive Bereiche“ auf Seite 113.

## 15.2.2 Experteneinstellungen

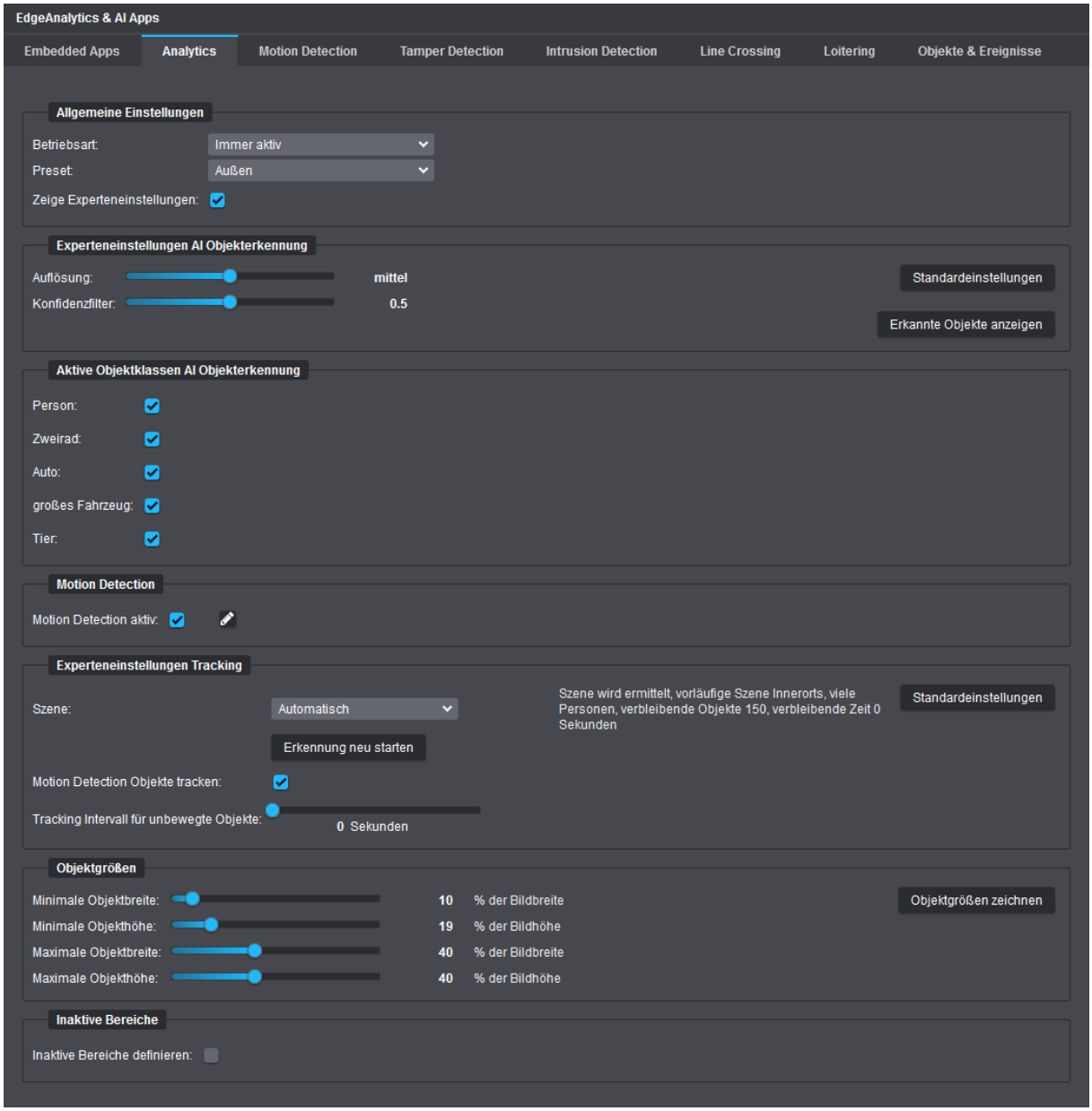


Abb. 15-13

### Auflösung

Diese Einstellung bestimmt, mit welcher Bildauflösung das **EdgeAnalytics**-Verfahren intern arbeiten soll (Standardeinstellung: **mittel**). Die zu wählende Einstellung hängt hierbei von Art und Entfernung der zu beobachtenden Objekte, ihrer Geschwindigkeit sowie der vorherrschenden Szenerie ab.
Bei einer höheren Analyse-Auflösung können kleinere Objekte besser detektiert und präziser klassifiziert werden, die Analyse erfolgt jedoch mit weniger Bildern pro Sekunde, da die CPU-Auslastung der Kamera steigt. Je höher die Analyse-Bildrate (Bilder/Sekunde) ist, desto genauer erfolgt hingegen die virtuelle Bewegungsverfolgung von erkannten Objekten.
Die Angaben zur aktuellen Analyse-Bildrate (Bilder/Sekunde) und zur gegenwärtig verursachten CPU-Auslastung durch die laufende Videoinhaltsanalyse finden Sie auf der Registerkarte **Objekte & Ereignisse** im Dialogbereich **Statistik** (siehe Abschnitt „Objekte & Ereignisse“ auf Seite 129).

- Stellen Sie die erforderliche **Auflösung** für die Analyse mit dem entsprechenden Schieberegler ein.

**Szene**
Diese Einstellung legt fest, welche Bedingungen in der erfassten Szene hinsichtlich der typischen maximalen Bewegungsgeschwindigkeiten verschiedener Objektklassen (Person, Fahrzeug, Tier) sowie der ggf. zu erwartenden Personendichte von den Videoanalyse-Algorithmen bei der Verarbeitung der Bilddaten berücksichtigt werden sollen.

- Wählen Sie aus der Drop-down-Liste **Szene** zwischen den folgenden Optionen:

- **Automatisch** (Standardeinstellung)
  Bei dieser Einstellung wird versucht, die vorherrschende Szenerie und die darin üblicherweise vorkommenden Objektklassen, deren objektspezifische maximale Bewegungsgeschwindigkeiten sowie ggf. die zu erwartende Personendichte möglichst genau maschinell zu ermitteln.
- **Autobahn**
- **Außerorts**
- **Innerorts, viele Personen**
- **Innerorts**
- **Benutzerdefiniert**
  Diese Einstellung ermöglicht die individuelle manuelle Anpassung der jeweiligen maximalen Bewegungsgeschwindigkeiten für die einzelnen Objektklassen.

**Motion Detection Objekte tracken**
Diese Einstellung ist nur verfügbar, wenn die Einstellung **Motion Detection aktiv** eingeschaltet ist (siehe Abschnitt „Motion Detection“ auf Seite 118).
Mithilfe dieser Einstellung werden auch für unbekannte Objekte, die keiner der möglichen Objektklassen zugeordnet werden können, oder für Objekte, die sich im Bild bewegen, Tracking-Koordinaten in Form von Metadaten generiert.

**Tracking-Intervall für unbewegte Objekte**
Diese Einstellung bestimmt das Zeitintervall in Sekunden zwischen dem wiederholten Versenden von (statischen) Tracking-Koordinaten erkannter Objekte, die sich nicht im Bild bewegen.
Mithilfe dieser Einstellung kann die Anzahl von redundanten Metadaten reduziert werden, die für eine spätere Auswertung nicht zwingend notwendig sind.

Beispiel:
Die sich nicht verändernden Tracking-Koordinaten eines geparkten Fahrzeugs werden periodisch nur im jeweils eingestellten Zeitintervall in Form von Metadaten an das jeweilige Dallmeier Aufzeichnungssystem gesendet.

- Stellen Sie das erforderliche Zeitintervall mit dem verfügbaren Schieberegler ein.

> *Ist das **Tracking-Intervall für unbewegte Objekte** auf **0 Sekunden** eingestellt (dies entspricht der Standardeinstellung), werden die statischen Tracking-Koordinaten eines Objekts zusammen mit jedem erzeugten Einzelbild (Frame) an das jeweilige Dallmeier Aufzeichnungssystem gesendet.*

**Objektgrößen**
Beschreibungen zu dieser Funktion finden Sie im Abschnitt „Objektgrößen“ auf Seite 111.

## 15.3 INTRUSION DETECTION

Die Analyse-Zusatzanwendung **Intrusion Detection** ermöglicht die automatische Generierung von Ereignissen, sobald erkannte Objekte in frei definierbare sensitive Bereiche im Bild eindringen oder diese wieder verlassen.

Typische Anwendungen:
- Außenhautabsicherung kritischer Infrastrukturen
- Gelände- und Freiflächensicherung
- Gebäude- und Eingangssicherung
- Beobachtung von Halte- und Parkverbotszonen sowie Feuerwehrzufahrten, Rettungswegen o. ä.

Zur Erstellung und Bearbeitung aktiver sensitiver Bereiche im Bild stehen eine Live-Vorschau (Bildrate 1 fps) sowie verschiedene Werkzeuge und Feineinstellungen zur Verfügung.

Aktive sensitive Bereiche werden im Vorschaubild rot maskiert.
Alle gemachten Änderungen werden stets verzögerungsfrei und ohne weitere Benutzeraktion übernommen.

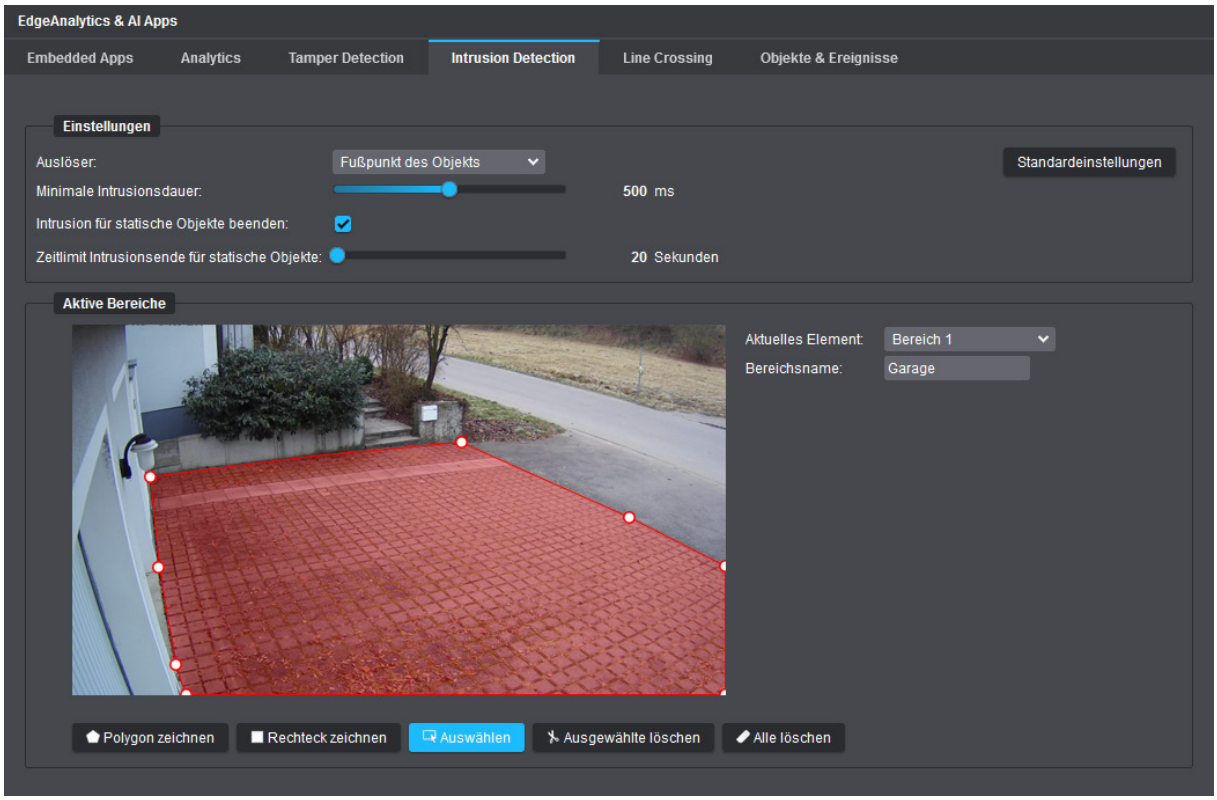


Abb. 15-14

- Definieren Sie die erforderlichen aktiven sensitiven Bereiche im Bild, in denen die Analyse-Zusatzanwendung **Intrusion Detection** ausgeführt werden soll.

Die Erstellung und Bearbeitung aktiver sensitiver Bereiche im Bild (max. 4 Intrusion-Bereiche möglich) entspricht der Vorgehensweise zur Festlegung global inaktiver Bereiche der Videoinhaltsanalyse (siehe Abschnitt „Inaktive Bereiche“ auf Seite 113).

- Vergeben Sie für jeden eingezeichneten Intrusion-Bereich einen eindeutigen Bereichsnamen (jeweiligen eingezeichneten Bereich vorher mit Auswahlwerkzeug markieren).

Im oben gezeigten Beispiel (Abb. 15-14) wurde die Garagenzufahrt mithilfe des **Polygon**-Werkzeugs als aktiver sensitiver Bereich definiert. Sobald ein Objekt in diesen Bereich eindringt (oder diesen wieder verlässt), wird automatisch ein entsprechendes Ereignis generiert und in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.
Die jeweiligen Intrusion-Ereignisse können zudem als Auslösebedingungen für verschiedene intelligente Kamera-Aktionen verwendet werden (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).

**Auslöser**
Diese Einstellung bestimmt, ob bereits der Fußpunkt von Objekten in einem aktiven sensitiven Bereich als neues Ereignis gewertet werden soll, erst das Zentrum bzw. der Mittelpunkt von Objekten, oder ob eine benutzerdefinierte prozentuale Mindestüberlappung von Objekten mit einem aktiven sensitiven Bereich dafür bestehen muss (Standardeinstellung = Fußpunkt).

- Wählen Sie den erforderlichen **Auslöser** aus der entsprechenden Drop-down-Liste.

**Schwellwert**
Diese Einstellung ist nur verfügbar, wenn zuvor als **Auslöser** die Option **Überlappung des Objekts** gewählt wurde (siehe oben).
Der Schwellwert legt fest, wie viel Prozent eines Objekts mindestens in einen aktiven sensitiven Bereich eindringen muss (oder den Bereich wieder verlassen muss), um ein neues Ereignis zu generieren.

- Legen Sie den erforderlichen **Schwellwert** mit dem entsprechenden Schieberegler fest.

**Minimale Intrusionsdauer**
Diese Einstellung gibt die Zeit in Millisekunden an, wie lange ein detektiertes Objekt mindestens in einem aktiven sensitiven Bereich verbleiben muss, bis ein Intrusion-Start-Ereignis generiert wird (nach einem Intrusion-Start-Ereignis wird alle 3 Sekunden ein Intrusion-Continued-Ereignis erzeugt, bis das Objekt den Bereich wieder verlässt, was wiederum ein abschließendes Intrusion-End-Ereignis erzeugt).

Die Standardeinstellung ist **500 ms**.

- Stellen Sie die erforderliche minimale Intrusion-Dauer mit dem verfügbaren Schieberegler ein.

**Intrusion für statische Objekte beenden**
Ist diese Einstellung aktiviert und wird ein Objekt, das zuvor in einen aktiven sensitiven Bereich eingedrungen ist, nach einer Weile statisch (z. B. nachdem ein Fahrzeug geparkt wurde), so wird nach einer einstellbaren Ablaufzeit (siehe unten) ein einmaliges Intrusion-End-Ereignis generiert.

**Zeitlimit Intrusionsende für statische Objekte**
Diese Einstellung ist nur verfügbar, wenn zuvor die Einstellung **Intrusion für statische Objekte beenden** aktiviert wurde (siehe oben).

Die Standardeinstellung ist **20 Sekunden**.

- Stellen Sie die erforderliche Ablaufzeit mit dem verfügbaren Schieberegler ein.

**Standardeinstellungen**
- Klicken Sie auf die Schaltfläche **Standardeinstellungen**, wenn Sie die Standardeinstellungen wiederherstellen möchten.

## 15.4 LINE CROSSING

Die Analyse-Zusatzanwendung **Line Crossing** ermöglicht die automatische Generierung von Ereignissen, sobald erkannte Objekte frei definierbare virtuelle Linien im Bild überqueren (virtueller Stolperdraht). Sobald ein entsprechendes Ereignis vorliegt, wird es in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.
Die jeweiligen Line-Crossing-Ereignisse können zudem als Auslösebedingungen für verschiedene intelligente Kamera-Aktionen verwendet werden (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).

Typische Anwendungen:
- Perimeterabsicherung (Zaunüberwachung, Absicherung gegen Übersteigen)

Zur Erstellung und Bearbeitung von virtuellen Linien im Bild stehen eine Live-Vorschau (Bildrate 1 fps) sowie verschiedene Werkzeuge und Feineinstellungen zur Verfügung.

Virtuelle Linien werden im Vorschaubild rot dargestellt.
Es können bis zu vier virtuelle Linien in Form von Polylinien im Bild eingezeichnet werden.
Eine Polylinie kann aus max. 3 verbundenen Liniensegmenten bzw. max. 4 Ankerpunkten bestehen.
Alle gemachten Änderungen werden stets verzögerungsfrei und ohne weitere Benutzeraktion übernommen.

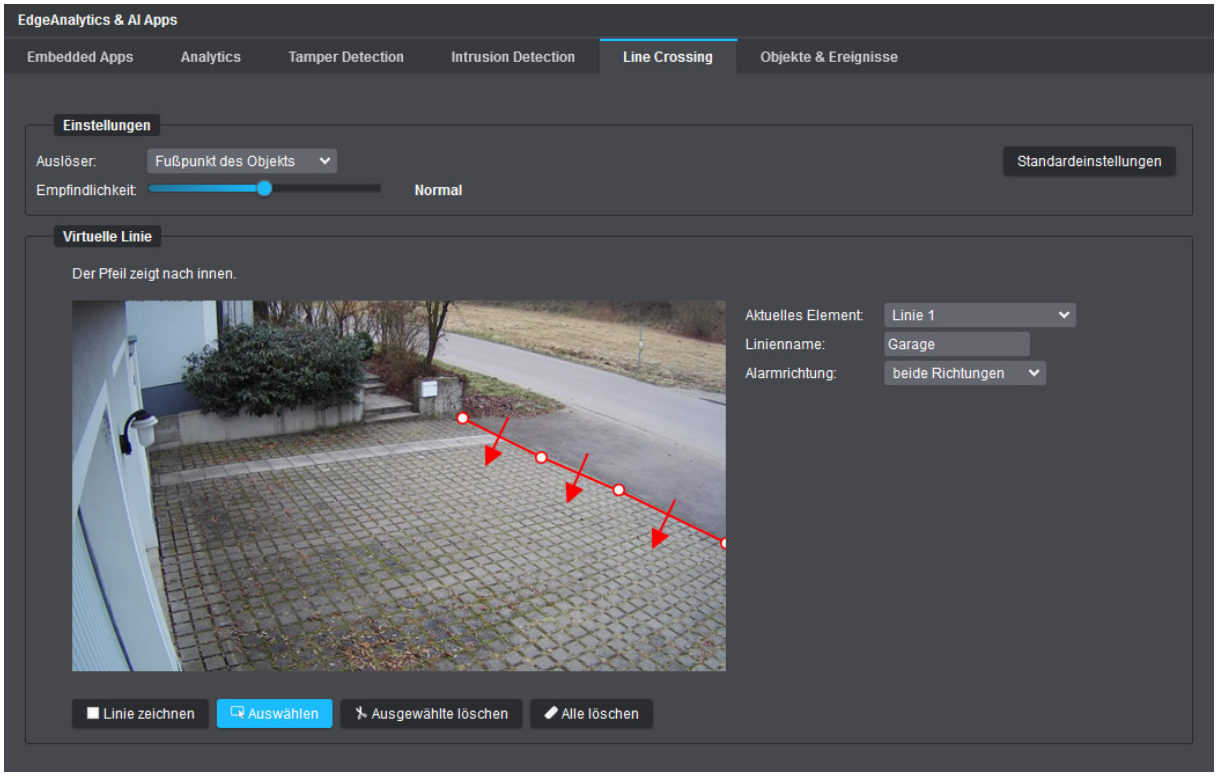


Abb. 15-15

- ▶ Legen Sie den Startpunkt einer neuen Polylinie mit der linken Maustaste im Vorschaubild fest.
- ▶ Ziehen Sie den Mauszeiger an die nächste Position im Vorschaubild und klicken Sie erneut mit der linken Maustaste in das Bild, um den nächsten Ankerpunkt der Polylinie zu definieren (nach min. 2 festgelegten Ankerpunkten können Sie die Zeichenfunktion per Rechtsklick mit der Maus beenden).
- ▶ Wiederholen Sie bei Bedarf die letzten Schritte, um weitere virtuelle Linien hinzuzufügen (Sie können bis zu vier virtuelle Linien im Bild erstellen, falls erforderlich).

**Virtuelle Linie bearbeiten**

- Klicken Sie auf die Schaltfläche **Auswählen**.
- Klicken Sie mit der linken Maustaste auf eine eingezeichnete Polylinie, um diese auszuwählen.

Die gewählte Polylinie wird an ihren Ankerpunkten mit kleinen weißen Kreisen markiert.

- Vergeben Sie einen eindeutigen Liniennamen.
- Wählen Sie die Alarmrichtung für die virtuelle Linie (die Pfeile einer Polylinie zeigen immer nach innen).
- Verschieben Sie ggf. die Ankerpunkte mit gedrückter linker Mautaste (es können neue Ankerpunkte hinzufügt werden, wenn die maximale Anzahl von 4 Ankerpunkten noch nicht erreicht ist, aber es können keine bestehenden Ankerpunkte gelöscht werden).
- Wiederholen Sie die letzten Schritte für jede eingezeichnete Polylinie.

Zum Löschen von Polylinien verfahren Sie wie folgt:

**Alle löschen**

- Klicken Sie auf die Schaltfläche **Alle löschen**, um alle definierten virtuellen Linien zu löschen.

**Ausgewählte löschen**

- Klicken Sie auf die Schaltfläche **Auswählen**.
- Klicken Sie mit der linken Maustaste auf eine eingezeichnete Polylinie, um diese auszuwählen (**Strg**-Taste auf Ihrer Tastatur gedrückt halten, um mehrere auszuwählen).
- Klicken Sie auf die Schaltfläche **Ausgewählte löschen** oder drücken Sie die **Entf**-Taste auf Ihrer Tastatur, um alle zuvor ausgewählten Polylinien zu löschen.

**Auslöser**

Diese Einstellung bestimmt, ob bereits der Fußpunkt von Objekten auf eingezeichneten virtuellen Linien als neues Ereignis gewertet werden soll oder ob mindestens das Zentrum bzw. der Mittelpunkt von Objekten die virtuellen Linien überqueren muss (Standardeinstellung = Fußpunkt).

- Wählen Sie den erforderlichen **Auslöser** aus der entsprechenden Drop-down-Liste.

**Empfindlichkeit**

Je höher die eingestellte Empfindlichkeit ist, desto schneller wird ein neues Ereignis ausgelöst, sobald ein Objekt eine virtuelle Linie überquert. Eine sehr niedrige Empfindlichkeit verhindert zum Beispiel, dass viele unerwünschte Ereignisse erzeugt werden, wenn Objekte die eingezeichneten virtuellen Linien beim Vorbeigehen oder -fahren lediglich für einen sehr kurzen Moment bis zu einem gewissen Grad überqueren.

Die Standardeinstellung ist **Unempfindlich**.

- Stellen Sie die erforderliche **Empfindlichkeit** mit dem entsprechenden Schieberegler ein.

**Standardeinstellungen**

- Klicken Sie auf die Schaltfläche **Standardeinstellungen**, wenn Sie die Standardeinstellungen wiederherstellen möchten.

## 15.5 LOITERING

*Die Analyse-Zusatzanwendung **Loitering** ist nur verfügbar in Verbindung mit der **EdgeAnalytics AI Object Detection App**.*

Die Analyse-Zusatzanwendung **Loitering** ermöglicht die automatische Generierung von Ereignissen, sobald sich Personen für einen ungewöhnlich langen (einstellbaren) Zeitraum in frei definierbaren sensitiven Bereichen im Bild aufhalten (Herumlungern).
Sobald ein entsprechendes Ereignis vorliegt, wird es in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.
Die jeweiligen Loitering-Ereignisse können zudem als Auslösebedingungen für verschiedene intelligente Kamera-Aktionen verwendet werden (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).

Typische Anwendungen:
- Außenhautabsicherung kritischer Infrastrukturen
- Gelände- und Freiflächensicherung
- Gebäude- und Eingangssicherung

Zur Erstellung und Bearbeitung aktiver sensitiver Bereiche im Bild stehen eine Live-Vorschau (Bildrate 1fps) sowie verschiedene Werkzeuge und Feineinstellungen zur Verfügung.

Aktive sensitive Bereiche werden im Vorschaubild rot maskiert.
Alle gemachten Änderungen werden stets verzögerungsfrei und ohne weitere Benutzeraktion übernommen.

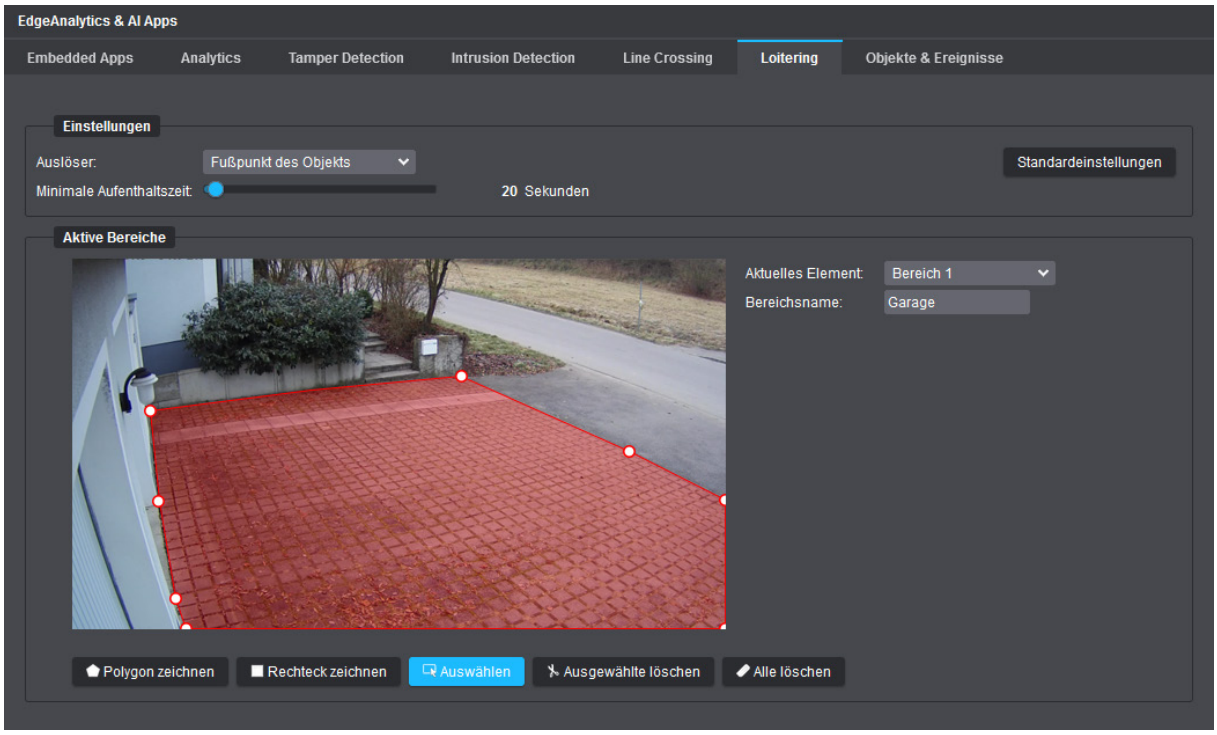


Abb. 15-16

- Definieren Sie die erforderlichen aktiven sensitiven Bereiche im Bild, in denen die Analyse-Zusatzanwendung **Loitering** ausgeführt werden soll.

Die Erstellung und Bearbeitung aktiver sensitiver Bereiche im Bild (max. 3 Loitering-Bereiche möglich) entspricht der Vorgehensweise zur Festlegung global inaktiver Bereiche der Videoinhaltsanalyse (siehe Abschnitt „Inaktive Bereiche“ auf Seite 113).

- Vergeben Sie für jeden eingezeichneten Bereich einen eindeutigen Bereichsnamen (jeweiligen eingezeichneten Bereich vorher mit Auswahlwerkzeug markieren).

**Auslöser**
Diese Einstellung bestimmt, ob bereits der Fußpunkt einer Person in einem aktiven sensitiven Bereich als neues Ereignis gewertet werden soll, erst das Zentrum bzw. der Mittelpunkt einer Person, oder ob eine benutzerdefinierte prozentuale Mindestüberlappung einer Person mit einem aktiven sensitiven Bereich dafür bestehen muss (Standardeinstellung = Fußpunkt).

- Wählen Sie den erforderlichen **Auslöser** aus der entsprechenden Drop-down-Liste.

**Schwellwert**
Diese Einstellung ist nur verfügbar, wenn zuvor als **Auslöser** die Option **Überlappung des Objekts** gewählt wurde (siehe oben).
Der Schwellwert legt fest, wie viel Prozent einer Person sich mindestens in einem aktiven sensitiven Bereich aufhalten muss, um ein neues Loitering-Start-Ereignis zu generieren.

- Legen Sie den erforderlichen **Schwellwert** mit dem entsprechenden Schieberegler fest.

**Minimale Aufenthaltszeit**
Diese Einstellung gibt die Zeit in Sekunden an, wie lange eine detektierte Person mindestens in einem aktiven sensitiven Bereich verweilen muss, bis ein Loitering-Start-Ereignis generiert wird (nach einem Loitering-Start-Ereignis wird alle 3 Sekunden ein Loitering-Continued-Ereignis erzeugt, bis die Person den Bereich wieder verlässt, was wiederum ein abschließendes Loitering-End-Ereignis erzeugt).

Die Standardeinstellung ist **20 Sekunden**.

- Stellen Sie die erforderliche minimale Aufenthaltszeit mit dem verfügbaren Schieberegler ein.

**Standardeinstellungen**
- Klicken Sie auf die Schaltfläche **Standardeinstellungen**, wenn Sie die Standardeinstellungen wiederherstellen möchten.

## 15.6 TAMPER DETECTION

Die **EdgeAnalytics AI Tamper Detection App** bietet spezielle Analyse- und Event-Processing-Funktionen, die nach der Aktivierung automatisch verschiedene Sabotagehandlungen oder Manipulationsversuche an der Kamera erkennen können (siehe Abschnitte weiter unten).
Sobald ein entsprechendes Ereignis vorliegt, wird es in Form von Metadaten in Echtzeit an das jeweilige Dallmeier Aufzeichnungssystem zur Speicherung und Weiterverarbeitung gesendet.

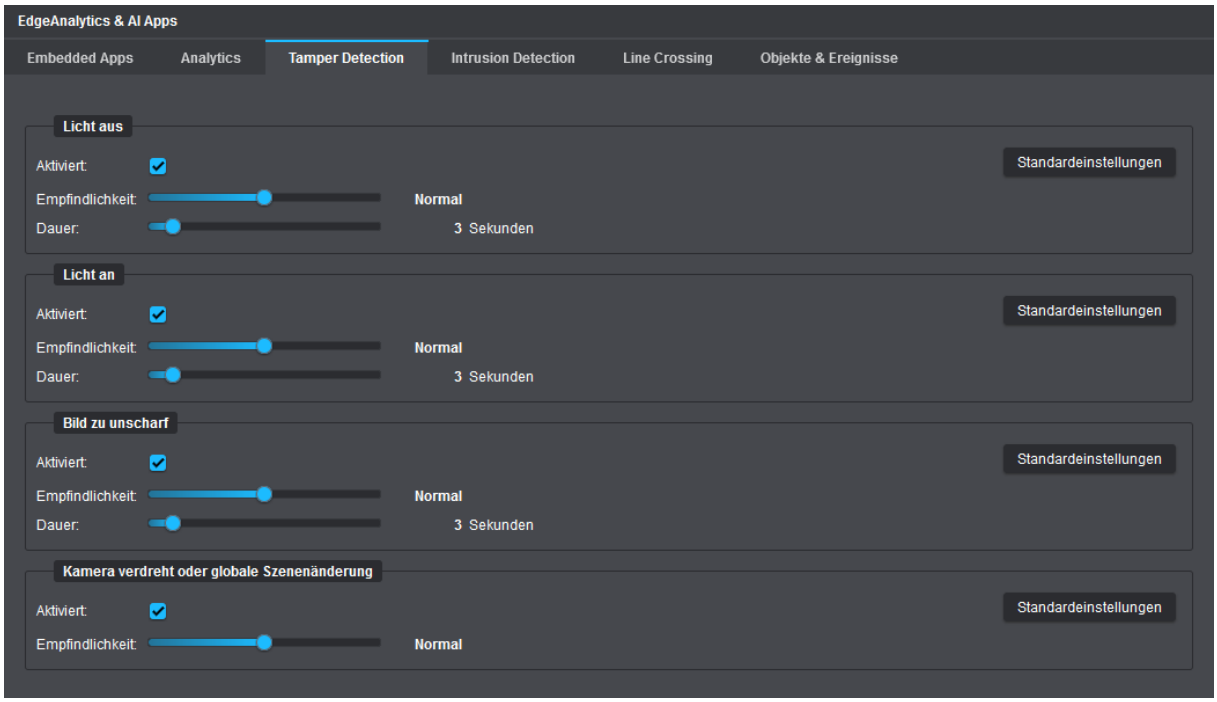


Abb. 15-17

### Licht aus

Generiert automatisch ein neues Ereignis, sobald sich die durchschnittliche Beleuchtungsstärke der erfassten Szene schlagartig verringert, wie beispielsweise bei:

- abrupter Änderung des Raumlichts durch Ausschalten oder Sabotage einer Lichtquelle
- Besprühen oder Verdecken der Kamera bzw. der Dome-Bubble

**Empfindlichkeit**
Diese Einstellung bestimmt, wie stark sich die Beleuchtungsstärke der erfassten Szene schlagartig ändern muss, um ein neues Ereignis zu generieren. Je höher die eingestellte Empfindlichkeit, desto geringer muss die schlagartige Änderung der Beleuchtungsstärke sein.

Die Standardeinstellung ist **Normal**.

- ▶ Stellen Sie die erforderliche **Empfindlichkeit** mit dem entsprechenden Schieberegler ein.

**Dauer**
Diese Einstellung gibt die Zeit an, wie lange die schlagartige Änderung der Beleuchtungsstärke andauern muss, bis ein entsprechendes neues Ereignis generiert wird.

- ▶ Stellen Sie die erforderliche **Dauer** mit dem entsprechenden Schieberegler ein (die Standardeinstellung ist **3 Sekunden**).

### Licht an

Generiert automatisch ein Ereignis, sobald sich die durchschnittliche Beleuchtungsstärke der erfassten Szene schlagartig erhöht, wie beispielsweise bei:

- abrupter Änderung des Raumlichts durch Anschalten einer Lichtquelle
- starker Blendung des Objektivs bzw. Bildsensors durch eine externe sehr helle Lichtquelle (z. B. Laser)

**Empfindlichkeit und Dauer**

Siehe Beschreibungen im Abschnitt „Licht aus“ auf Seite 127.

### Bild zu unscharf

Generiert automatisch ein Ereignis, sobald das Bild plötzlich unscharf und verschwommen wird (z. B. durch absichtliches Vernebeln der Kamera oder unbefugtes Defokussieren des Objektivs).

**Empfindlichkeit**

Diese Einstellung bestimmt, wie stark sich das Bild zur ursprünglich erfassten Szene verändern muss, um ein neues Ereignis zu generieren. Je höher die eingestellte Empfindlichkeit, desto weniger muss sich das Bild verändern.

Die Standardeinstellung ist **Normal**.

► Stellen Sie die erforderliche **Empfindlichkeit** mit dem entsprechenden Schieberegler ein.

**Dauer**

Diese Einstellung gibt die Zeit an, wie lange die Änderung andauern muss, bis ein entsprechendes neues Ereignis generiert wird.

► Stellen Sie die erforderliche **Dauer** mit dem entsprechenden Schieberegler ein (die Standardeinstellung ist **3 Sekunden**).

### Kamera verdreht oder globale Szenenänderung

Generiert automatisch ein Ereignis bei einer abrupten Szenenänderung, wie z. B. durch Verdrehen oder Verdecken der Kamera oder wenn plötzlich große Objekte im Nahbereich der Kamera sichtbar werden.

**Empfindlichkeit**

Diese Einstellung bestimmt, wie schnell eine Manipulation an der Kamera als solche erkannt wird. Je höher die eingestellte Empfindlichkeit, desto weniger muss beispielsweise das Objektiv der Kamera verdeckt werden, um das als neues Ereignis zu interpretieren.
Beachten Sie jedoch, dass eine hohe Empfindlichkeitseinstellung hier auch zu vielen nicht relevanten Ereignissen führen kann, beispielsweise durch wetterbedingte Kameraschwankungen bei einer Außenmontage der Kamera auf einem hohen Mast. Regeln Sie in diesem Fall die Empfindlichkeitseinstellung nach unten.

Die Standardeinstellung ist **Normal**.

► Stellen Sie die erforderliche **Empfindlichkeit** mit dem entsprechenden Schieberegler ein.

*Klicken Sie auf die Schaltfläche **Standardeinstellungen** hinter der jeweiligen Funktion, wenn Sie die zugehörigen Standardeinstellungen wiederherstellen möchten.*

## 15.7 OBJEKTE & EREIGNISSE

Auf der Registerkarte **Objekte & Ereignisse** können die Einstellungen zur Videoinhaltsanalyse vor dem Live-Betrieb der Kamera ausführlich getestet werden.

> *Für bestmögliche Analyseergebnisse im Live-Betrieb sollten Sie alle Einstellungen, die Sie ändern, stets erneut auf der Registerkarte **Objekte & Ereignisse** überprüfen, z. B. hinsichtlich Anzahl, Plausibilität und Relevanz erkannter Objekte und Ereignisse.*

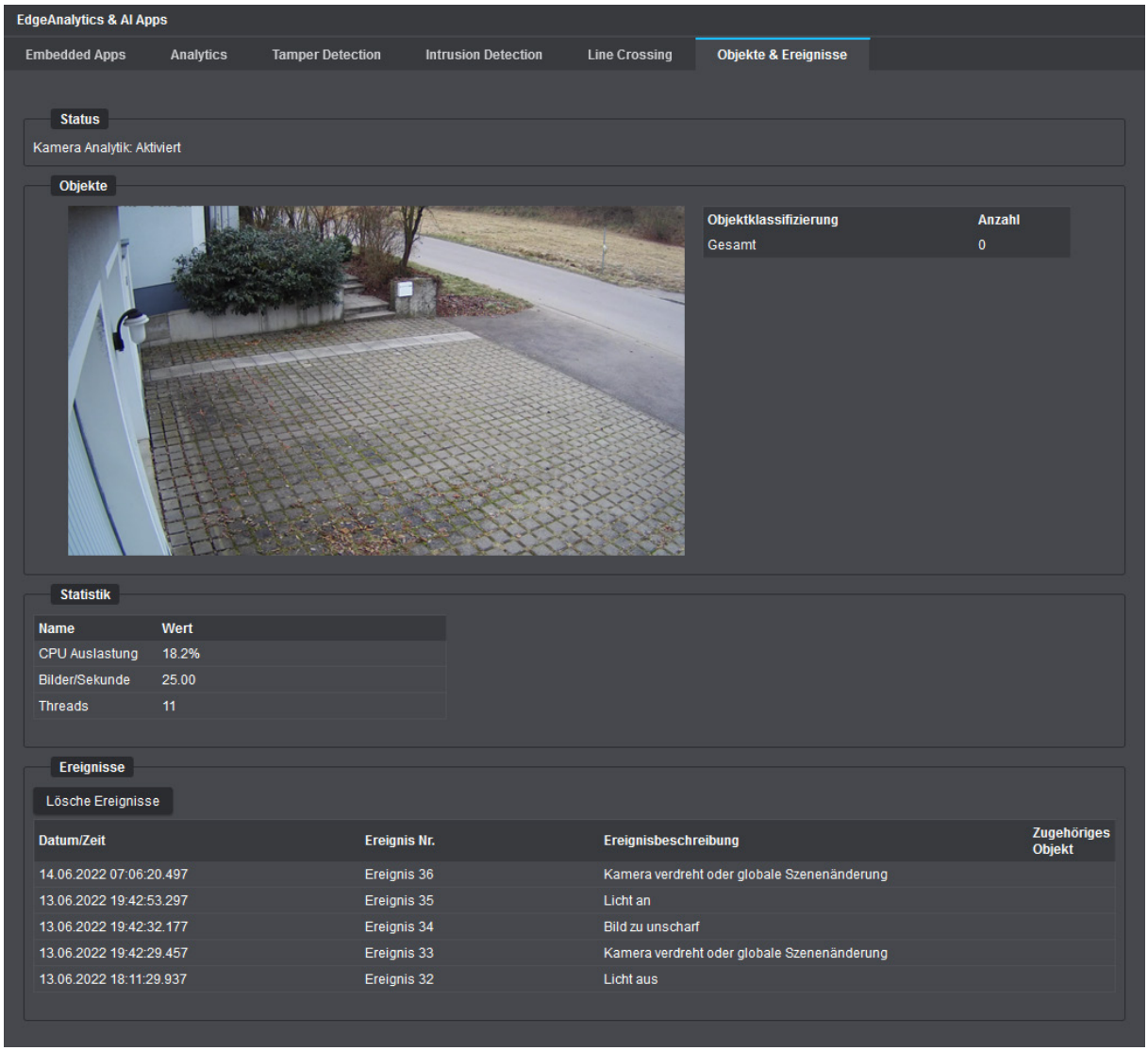


Abb. 15-18

### Objekte

In diesem Dialogbereich werden in einer Live-Vorschau (Bildrate 1 fps) alle im Bild detektierten Objekte mit farbigen Objekt-Begrenzungsrahmen („Bounding Boxes“) markiert und solange virtuell im Bild verfolgt, bis sie von der Kamera nicht mehr als Objekte wahrgenommen werden.
Je nach identifiziertem Objekttyp (Person, Fahrzeug etc.) werden dabei unterschiedliche Rahmenfarben zur Objektmarkierung verwendet.

### Statistik

In diesem Dialogbereich werden folgende Angaben bereitgestellt:

- Gegenwärtig verursachte CPU-Auslastung durch die laufende Videoinhaltsanalyse
- Aktuelle Analyse-Bildrate (Bilder/Sekunde)

> *Beachten Sie in diesem Zusammenhang die Erläuterungen zur Analyse-Auflösung und Analyse-Bildrate (Bilder/Sekunde) im Abschnitt „Auflösung“ auf Seite 106.*

### Ereignisse

In diesem Dialogbereich werden die letzten 20 Ereignisse aufgelistet, die von den Analyse-Zusatzanwendungen auf der Kamera erzeugt wurden (z. B. **Intrusion Detection**, **Line Crossing** oder **Tamper Detection**). Jeder Ereigniseintrag beinhaltet u. a. den genauen Ereigniszeitstempel (Datum/Zeit des Ereignisses) sowie eine kurze Ereignisbeschreibung.

# BENUTZER & RECHTE

Die Konfiguration der Kamera ist nur für authentifizierte und autorisierte Benutzer zugänglich.
Mit der Benutzer- und Rechteverwaltung der Kamera können Sie mehreren Benutzergruppen unterschiedliche Zugriffs- und Konfigurationsrechte zuweisen und jeder Gruppe einzelne Benutzer zuordnen.

- Klicken Sie im Navigationsmenü den Menüeintrag **Benutzer & Rechte**, um den entsprechenden Dialog zu öffnen.

Die Registerkarte **Benutzerverwaltung** wird angezeigt.

## 16.1 BENUTZERVERWALTUNG

Die Anmeldung am Gerät erfordert immer die Eingabe eines Benutzernamens in Kombination mit einem Passwort. Ein starkes und sicheres Passwort ist dabei unerlässlich. Es sollte komplex sein, aus einer beliebigen Zeichenfolge bestehen und lang sein. Verwenden Sie keine persönlichen Informationen, gebräuchliche Ausdrücke (real existierende Wörter) oder Namen als Teil eines Passworts.
Aus Sicherheitsgründen müssen Passwörter mindestens 12 Zeichen lang sein (maximal zulässig sind 128 Zeichen) und alle folgenden Kriterien erfüllen (aus folgenden Zeichen bestehen):

- Kleinbuchstabe
- Großbuchstabe
- Ziffer: 0123456789
- Sonderzeichen: ^!”$%&/{}()[]=?\`’*+~#-_:.;,<>|@

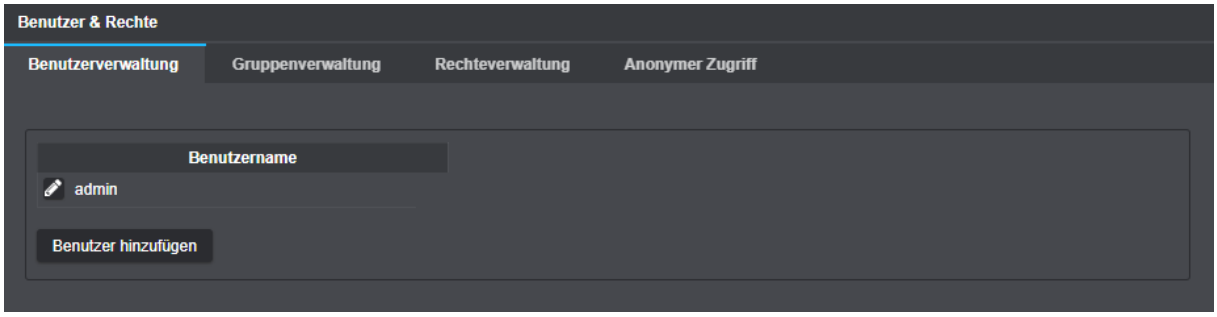


Abb. 16-1

**Benutzer hinzufügen**

- Klicken Sie **Benutzer hinzufügen**.
- Geben Sie einen eindeutigen Benutzernamen ein (dieser kann später nicht mehr geändert werden).
- Geben Sie ein starkes und sicheres Passwort ein (Passwortkriterien beachten) und bestätigen Sie dieses im entsprechenden Feld (beide eingegebenen Passwörter müssen identisch sein).
- Klicken Sie abschließend **OK**.

**Benutzer(-passwort) ändern oder Benutzer löschen**

- Klicken Sie auf das **Stift**-Symbol links neben einem Benutzer, um das zugehörige Passwort zu ändern oder klicken Sie auf das **Löschen**-Symbol (roter Kreis mit weißem Kreuz) rechts neben einem Benutzer, um den entsprechenden Benutzer zu löschen.

Der Benutzer **admin** (das Administrationskonto ab Werk) kann nicht gelöscht werden.

## 16.2 GRUPPENVERWALTUNG

Jeder Benutzer kann individuell einer Benutzergruppe als Mitglied zugeordnet werden und besitzt dann die Rechte (Privilegien) der jeweiligen Benutzergruppe.

- Wählen Sie die Registerkarte **Gruppenverwaltung**.

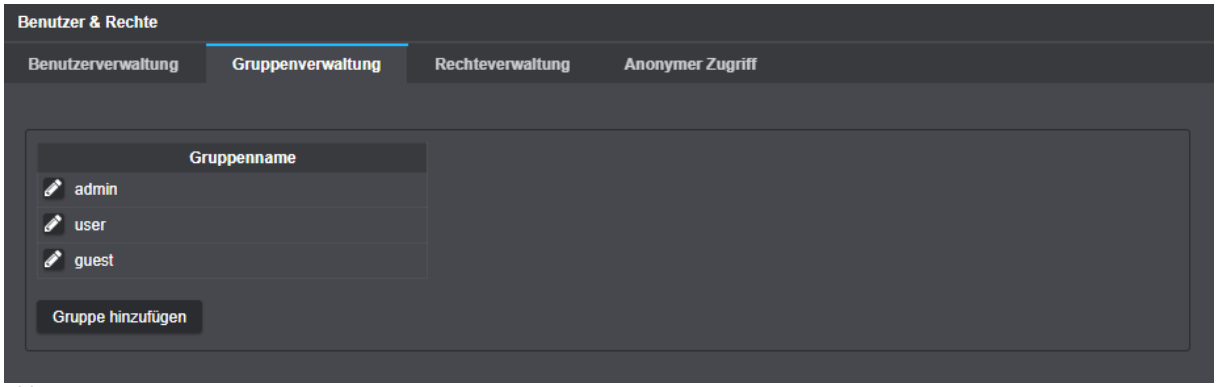


Abb. 16-2

### Gruppe hinzufügen

- Klicken Sie **Gruppe hinzufügen**.
- Geben Sie einen eindeutigen Gruppennamen ein (dieser kann später nicht mehr geändert werden).
- Bestätigen Sie abschließend mit **OK**.

### Mitglieder einer Gruppe verwalten

- Klicken Sie auf das **Stift**-Symbol links neben einer Gruppe, um die Mitglieder der Gruppe zu verwalten.

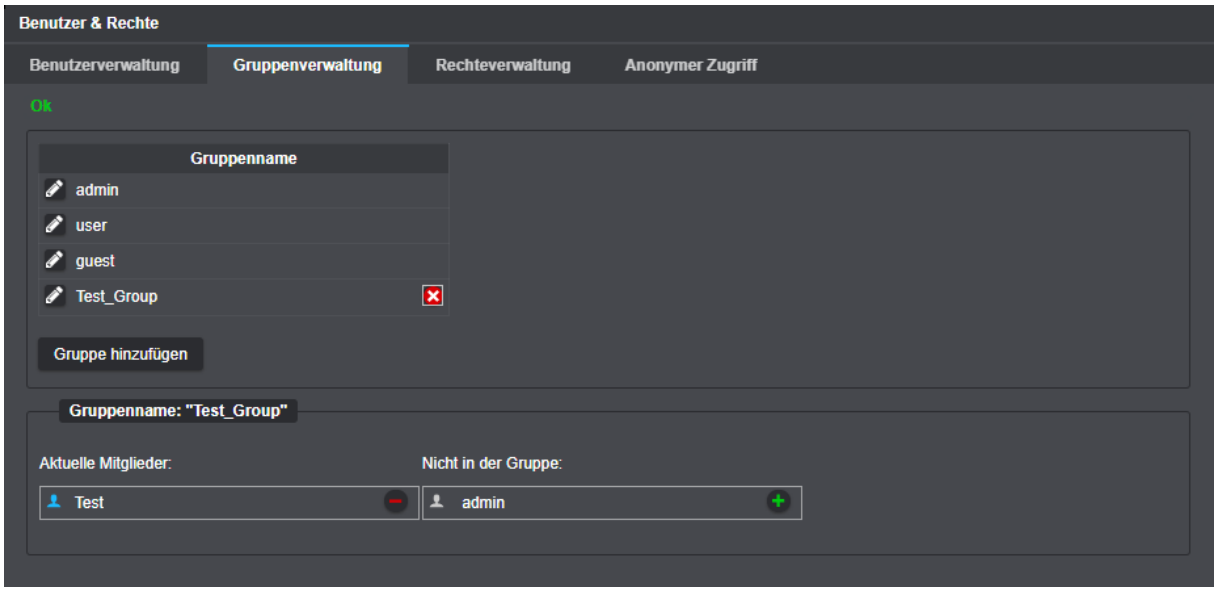


Abb. 16-3

- Klicken Sie den **+** Button (grün, rechte Spalte), um den betreffenden Benutzer der Gruppe zuzuordnen.
- Klicken Sie den **–** Button (rot, linke Spalte), um den Benutzer aus der Gruppe zu entfernen.

### Gruppe löschen

- Klicken Sie auf das **Löschen**-Symbol (roter Kreis mit weißem Kreuz) rechts neben einer Gruppe, um die entsprechende Gruppe zu löschen (die Gruppen **admin**, **user** und **guest** können nicht gelöscht werden).

## 16.3 RECHTEVERWALTUNG

Jeder Benutzergruppe, und damit den zugeordneten Benutzern/Mitgliedern der Gruppe, können individuelle Rechte (Privilegien) zugewiesen werden.

- Wählen Sie die Registerkarte **Rechteverwaltung**.

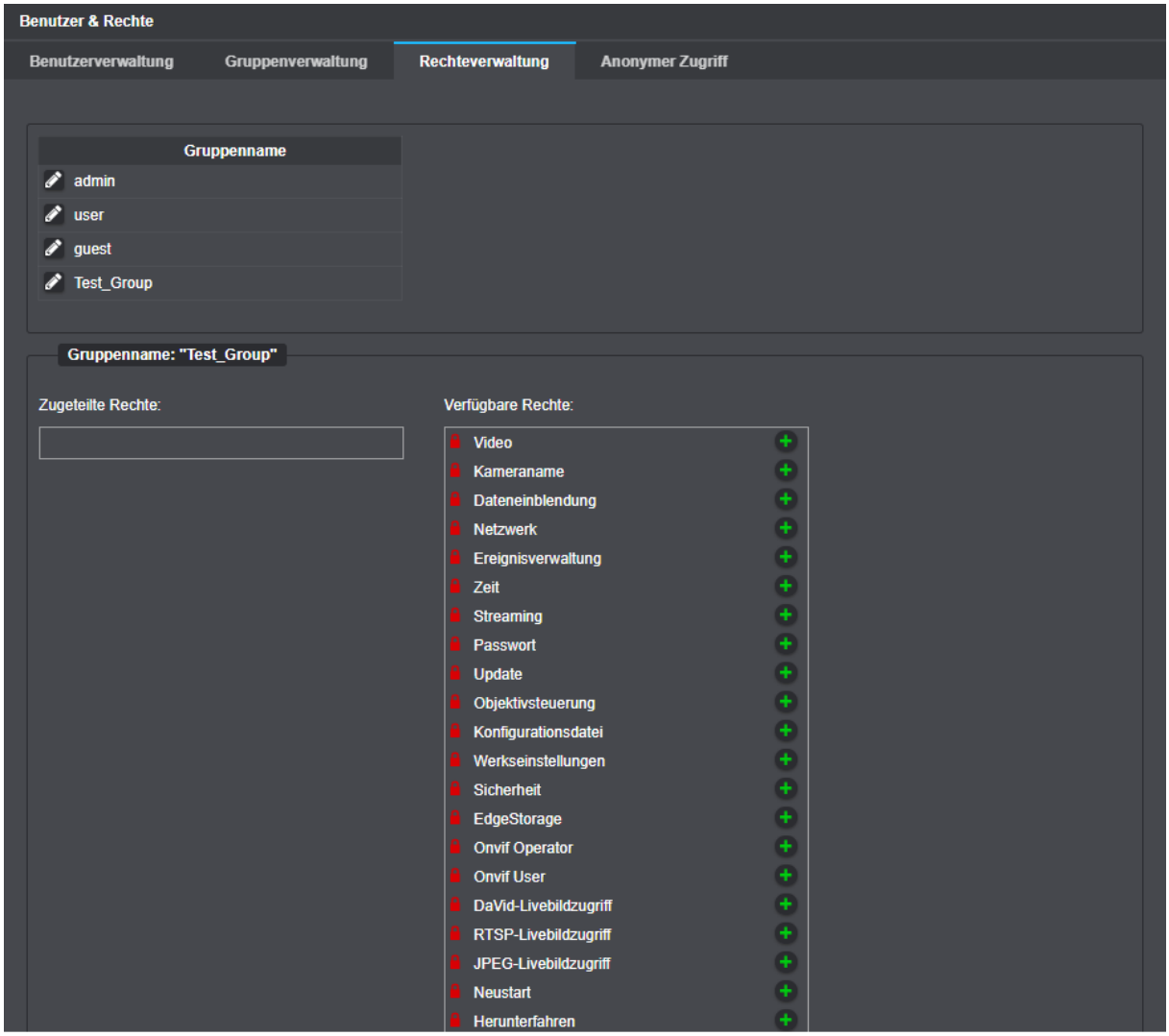


Abb. 16-4

- Klicken Sie auf das **Stift**-Symbol links neben einer Gruppe, um die Rechte (Privilegien) der betreffenden Gruppe zu bearbeiten.
- Klicken Sie den **+** Button (grün, rechte Spalte), um der Gruppe ein Recht zuzuweisen.
- Klicken Sie den **–** Button (rot, linke Spalte), um der Gruppe ein zugewiesenes Recht zu entziehen.

Die Rechte der Benutzergruppe **admin** können nicht eingeschränkt werden.

## 16.4 ANONYMER ZUGRIFF

Auf der Registerkarte **Anonymer Zugriff** werden Einstellungen für die Bildübertragung ohne vorherige Authentifizierung eines Benutzers vorgenommen (siehe Kapitel „Bildübertragung“ auf Seite 145).

- Wählen Sie die Registerkarte **Anonymer Zugriff**.

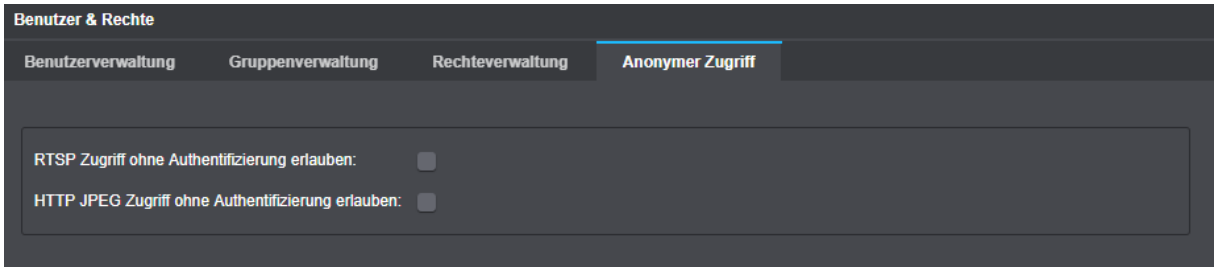


Abb. 16-5

- Aktivieren Sie die erforderlichen Checkboxen.

# SERVICE

▶ Klicken Sie im Navigationsmenü den Menüpunkt **Service**.

Der Dialog **Service** wird angezeigt.

## 17.1 KONFIGURATIONSDATEI

### 17.1.1 Export

Die Gerätekonfiguration kann (vollständig oder in Teilen) exportiert und zur späteren Wiederverwendung als .cfg-Datei gespeichert werden.

*ACHTUNG*

**IP-Adresskonflikte durch fehlerhafte Netzwerkeinstellungen**

Wenn Sie die gespeicherte Konfigurationsdatei später in andere Kameras (desselben Typs) in Ihrem bestehenden Netzwerk importieren möchten, dann dürfen Sie die **Netzwerkeinstellungen** nicht in die .cfg-Datei exportieren, um IP-Adressduplikate zu vermeiden.

▶ Wählen Sie die Registerkarte **Konfigurationsdatei**.

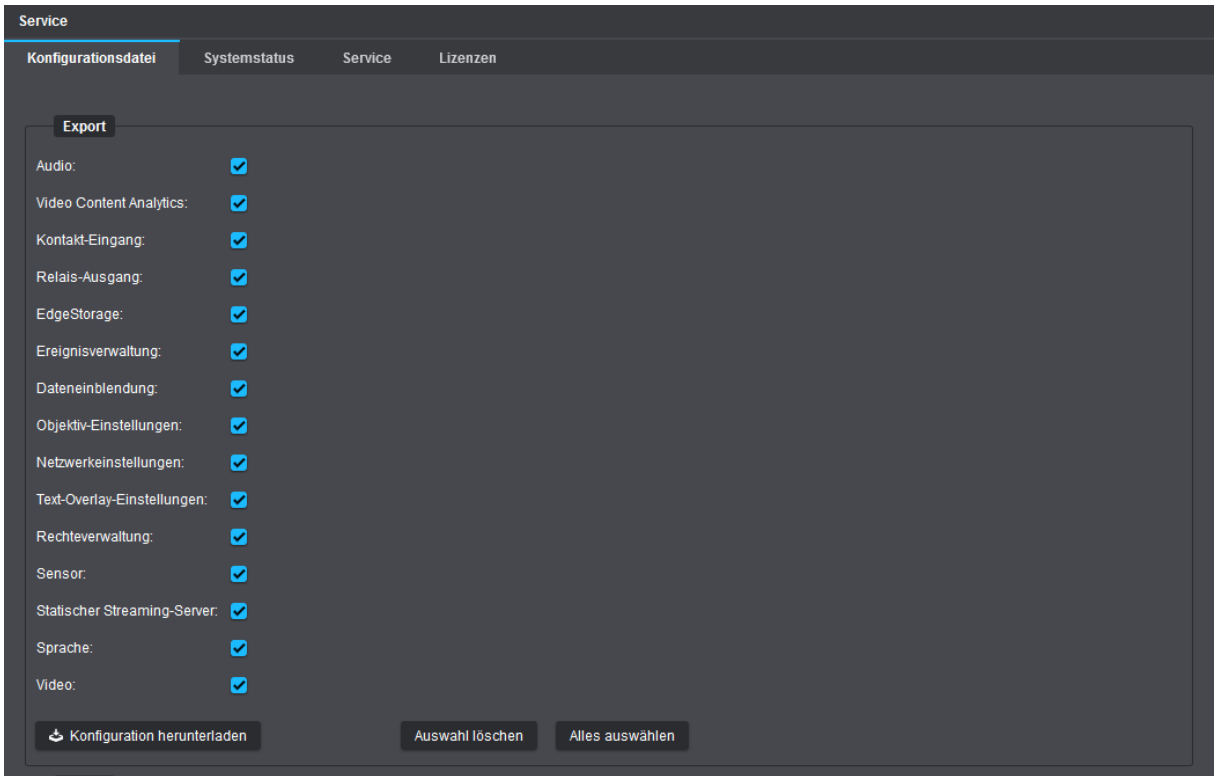


Abb. 17-1

► Wählen Sie unter dem Bereich **Export** die erforderlichen Einstellungen aus, die in die Konfigurationsdatei exportiert werden sollen, indem Sie die entsprechenden Kontrollkästchen aktivieren, wie z. B.:

**Audio**
Exportiert die Audioeinstellungen (siehe Kapitel „Audio“ auf Seite 43).

**Video Content Analytics**
Exportiert die Einstellungen zur Video-Content-Analyse (siehe Kapitel „Edge Analytics & AI Apps“ auf Seite 100).

**Kontakt-Eingang**
Exportiert die Schnittstellen-Einstellungen für die Kontakt-Eingänge (siehe Abschnitt „Kontakt-Eingänge“ auf Seite 73).

**Relais-Ausgang**
Exportiert die Schnittstellen-Einstellungen für die Relais-Ausgänge (siehe Abschnitt „Relais-Ausgänge“ auf Seite 72).

**EdgeStorage**
Exportiert die EdgeStorage-Einstellungen (siehe Kapitel „EdgeStorage“ auf Seite 75).

**Ereignisverwaltung**
Exportiert die Einstellungen zur Ereignisverwaltung (siehe Kapitel „Ereignisverwaltung“ auf Seite 76).

**Dateneinblendung**
Exportiert die Einstellungen zur Einbettung von externen Texten und Schnittstellendaten (siehe Kapitel „Dateneinblendung“ auf Seite 97).

**Objektiv-Einstellungen**
Exportiert die Einstellungen für

- Tag-/Nachtmodus (siehe Abschnitt „Tag/Nacht“ auf Seite 25),
- Blendenmodus und Blende (siehe Abschnitt „Belichtungssteuerung“ auf Seite 23).

**Netzwerkeinstellungen**
Exportiert die Netzwerkeinstellungen (siehe Kapitel „Netzwerk“ auf Seite 50).

**Text-Overlay-Einstellungen**
Exportiert die Einstellungen zur Texteinblendung im Bild (siehe Abschnitt „Text-Overlay“ auf Seite 31).

**Rechteverwaltung**
Exportiert die Einstellungen zur Benutzer- und Rechteverwaltung (siehe Kapitel „Benutzer & Rechte“ auf Seite 131).

**Sensor**
Exportiert die Einstellungen für

- Kamera-Presets (siehe Abschnitt „Voreinstellungen (Presets)“ auf Seite 17),
- Bildoptimierung (siehe Abschnitt „Bildoptimierung“ auf Seite 20),
- Korridormodus (siehe Abschnitt „Sensoreinstellungen“ auf Seite 35).

**Statischer Streaming-Server**
Exportiert die Einstellungen für den statischen Streaming-Server (siehe Abschnitt „Streaming“ auf Seite 55).

**Sprache**
Exportiert die Spracheinstellung (siehe Kapitel „Allgemeine Einstellungen (Sprache)“ auf Seite 16).

**Video**
Exportiert die Sensor- und die Stream-/Encodereinstellungen (siehe Kapitel „Video“ auf Seite 35). Beachten Sie jedoch, dass die Einstellung zum **Korridormodus** nur durch Auswahl des Kontrollkästchens **Sensor** exportiert wird.

- Klicken Sie **Konfiguration herunterladen**.
- Wählen Sie den gewünschten Speicherort aus und bestätigen Sie mit **OK**.

*Für eine spätere leichtere Zuordnung der Konfigurationsdatei besteht der Dateiname standardmäßig aus der Produktbezeichnung und IP-Adresse Ihres Geräts. Wenn Sie keinen anderen Pfad/Ordner zum Speichern heruntergeladener Dateien angeben, wird die .cfg-Datei im Standard-Download-Ordner gespeichert, den Sie in Ihrem Webbrowser definiert haben.*

## 17.1.2 Import

Das Importieren von Konfigurationsdateien spart Zeit bei der Konfiguration größerer Anlagen zur Videosicherheit und -überwachung, bei denen viele baugleiche Dallmeier Kameras zum Einsatz kommen.

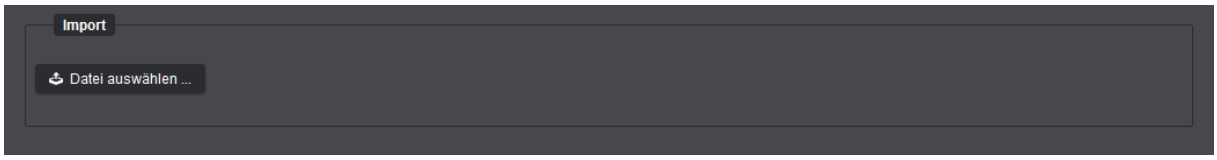


Abb. 17-2

- Klicken Sie **Datei auswählen** unter dem Bereich **Import**.
- Suchen und wählen Sie mit dem angezeigten Datei-Explorer die zu importierende Konfigurationsdatei mit der Dateiendung .cfg.
- Klicken Sie **Öffnen** und bestätigen Sie mit **OK**.

Die Konfiguration wird nun auf die Kamera übertragen.

## 17.2 SYSTEMSTATUS

Das Gerät kann jederzeit, falls erforderlich, auf die Werkseinstellungen zurückgesetzt werden oder im unwahrscheinlichen Fall eines Systemfehlers bzw. unbeabsichtigten Systemverhaltens neu gestartet werden.

- Wählen Sie die Registerkarte **Systemstatus**.

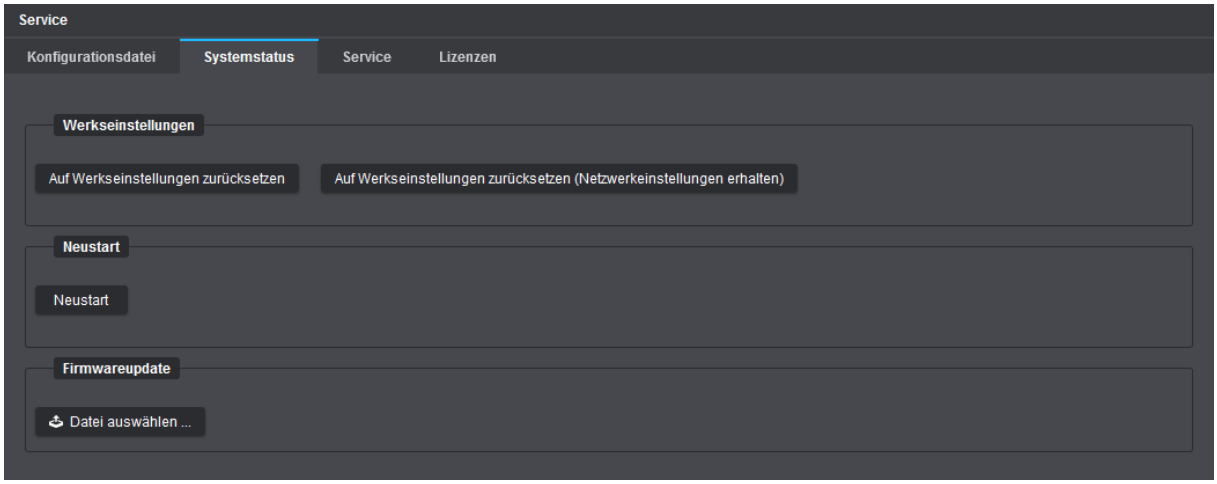


Abb. 17-3

### 17.2.1 Werkseinstellungen

- Klicken Sie **Auf Werkseinstellungen zurücksetzen**, um alle werkseitigen Standardeinstellungen wiederherzustellen, angelegte Benutzerkonten zu löschen und das Administrationskennwort sowie die Netzwerkeinstellungen (IP-Adresse, Gateway, Subnetz-Maske etc.) zurückzusetzen, ...

  oder

- klicken Sie **Auf Werkseinstellungen zurücksetzen (Netzwerkeinstellungen erhalten)**, um alle werkseitigen Standardeinstellungen wiederherzustellen, jedoch ohne die angelegten Benutzerkonten zu löschen oder das Administrationskennwort und die Netzwerkeinstellungen zurückzusetzen.

> *Bei Zurücksetzen auf die Werkseinstellungen behalten Lizenzen ihre Gültigkeit (bis zu Ihrem Ablauf).*

### 17.2.2 Neustart

- Klicken Sie **Neustart**, um das Gerät, z. B. im Falle eines unerwarteten Systemverhaltens, neu zu starten.

### 17.2.3 Firmwareupdate

- Prüfen Sie regelmäßig die Dallmeier Webseite unter https://www.dallmeier.com/ auf die aktuellste Release-Version von Domera® OS (v. a. in Bezug auf Sicherheitsupdates oder -patches).
- Klicken Sie **Datei auswählen**, um eine für Ihr Produktmodell gültige Update-Datei (mit der Dateiendung .bin) auf die Kamera zu übertragen und den Update-Vorgang zu starten.

## 17.3 SERVICE

Die Registerkarte **Service** dient ausschließlich für spezielle Servicezwecke und ermöglicht Ihnen bei Bedarf, die Support-Informationen zu Ihrem Gerät als .dat-Datei für den Dallmeier Support herunterzuladen.

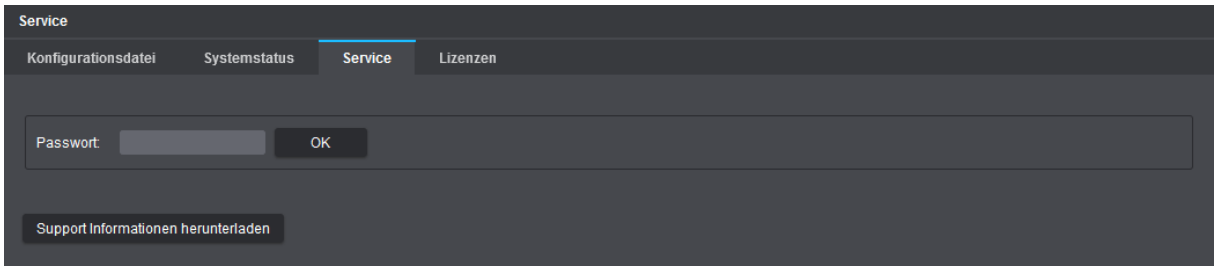


Abb. 17-4

- Klicken Sie **Supportinformationen herunterladen**.
- Wählen Sie den gewünschten Speicherort aus und bestätigen Sie mit **OK**.
- Kontaktieren Sie gegebenenfalls den Dallmeier Support zur weiteren Vorgehensweise.

*Für eine spätere leichtere Zuordnung der Support-Datei besteht der Dateiname standardmäßig aus der Produktbezeichnung und IP-Adresse Ihres Geräts.*
*Wenn Sie keinen anderen Pfad/Ordner zum Speichern heruntergeladener Dateien angeben, wird die .dat-Datei im Standard-Download-Ordner gespeichert, den Sie in Ihrem Webbrowser definiert haben.*

## 17.4 LIZENZEN

Auf der Registerkarte **Lizenzen** können Sie mögliche Zusatzfunktionen für Ihre Kamera freischalten oder die Laufzeit der Software-Wartungslizenz für Ihre Kamera verlängern.

Informationen zu den verfügbaren Zusatzfunktionen und Software-Wartungslizenzen finden Sie in der Produktspezifikation Ihrer Kamera auf der Dallmeier Webseite unter https://www.dallmeier.com/.

Um einen gültigen Lizenz-Code für eine bestimmte Zusatzfunktion oder zur Verlängerung der Software-Wartungslizenz zu erwerben, wenden Sie sich an Ihren Dallmeier Vertriebspartner.

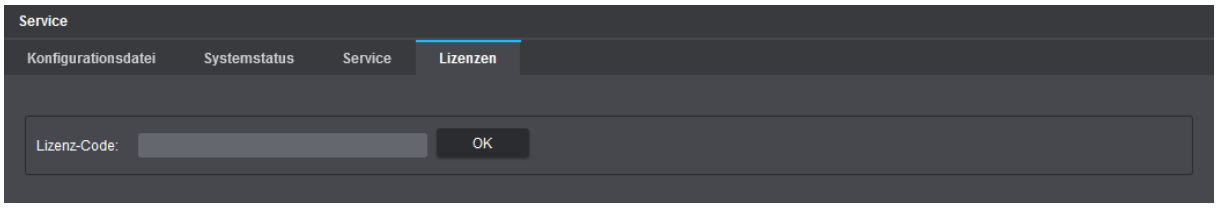


Abb. 17-5

- Geben Sie einen gültigen **Lizenz-Code** ein.
- Bestätigen Sie mit **OK**.

Je nach eingegebenem Lizenz-Code wird daraufhin entweder die entsprechende Zusatzfunktion auf Ihrer Kamera freigeschaltet und kann anschließend unmittelbar genutzt werden, oder die Software-Wartungslizenz verlängert sich abhängig vom erworbenen Service-Paket automatisch um die gewählte Dauer.

> *Informationen zu aktiven Lizenzen auf Ihrer Kamera sowie Details zu Ablaufdatum und -zeit der Software-Wartungslizenz (**Serviceintervall-Ende**) finden Sie im Dialog **Informationen** auf der Registerkarte **Allgemeine Informationen** (siehe Abschnitt „Allgemeine Informationen“ auf Seite 142).*

- Beachten Sie die Hinweise zu Software-Wartungslizenzen auf der folgenden Seite.

## Wichtige Hinweise zu Software-Wartungslizenzen

Kameras mit Domera® OS werden standardmäßig mit einer kostenfreien Software-Wartungslizenz ausgeliefert, die einen Zeitraum von 12 Monaten abdeckt. Diese Gültigkeitsdauer kann entweder bereits bei der Kamerabestellung oder zu einem späteren Zeitpunkt durch Eingabe eines erworbenen Lizenz-Codes für Software-Wartung verlängert werden.

**Lückenlose Lizenzierungshistorie**
Entscheidend für die Berechtigung zur Aktualisierung Ihrer Kamera ist eine lückenlose Lizenzierungshistorie für Software-Wartung (kontinuierlich fortlaufende Software-Wartungslizenzen auf Ihrer Kamera).

Ein Beispiel:
Ihre Kamera soll auf eine neue Version von Domera® OS aktualisiert werden, die im dritten Betriebsjahr der Kamera veröffentlicht wird.
In diesem Fall ist eine fortlaufende Lizenzierung ohne Unterbrechung für Jahr 1 (kostenfreie Lizenz), Jahr 2 (erste Lizenz) und Jahr 3 (zweite Lizenz) erforderlich.

**Freigabedatum der Update-Datei**
Entscheidend für die Berechtigung zur Aktualisierung Ihrer Kamera ist das Freigabedatum der Update-Datei. Es muss innerhalb eines lückenlosen Lizenzierungszeitraums liegen.

Ein Beispiel:
Eine Kamera mit Software-Wartungslizenzen, die nur Jahr 1 + Jahr 2 abdecken, kann auch im Jahr 3 des Kamerabetriebs noch aktualisiert werden, wenn die Update-Datei vor dem Ablaufdatum der Lizenz für Jahr 2 freigegeben wurde.

*Die Laufzeit der kostenfreien Software-Wartungslizenz ab Werk beginnt erst ab einer Betriebsdauer Ihrer Kamera von 500 Stunden.*
*Details zu Ablaufdatum und -zeit der aktuellen Software-Wartungslizenz können über den* ***Dallmeier Device Manager*** *abgerufen werden.*

# INFORMATIONEN

Im Dialog **Informationen** werden verschiedene Informationen zum Gerät angezeigt.

► Klicken Sie im Navigationsmenü den Menüpunkt **Informationen**.

## 18.1 ALLGEMEINE INFORMATIONEN

Auf der Registerkarte **Allgemeine Informationen** werden Ihnen die wesentlichen allgemeinen Geräteinformationen angezeigt.

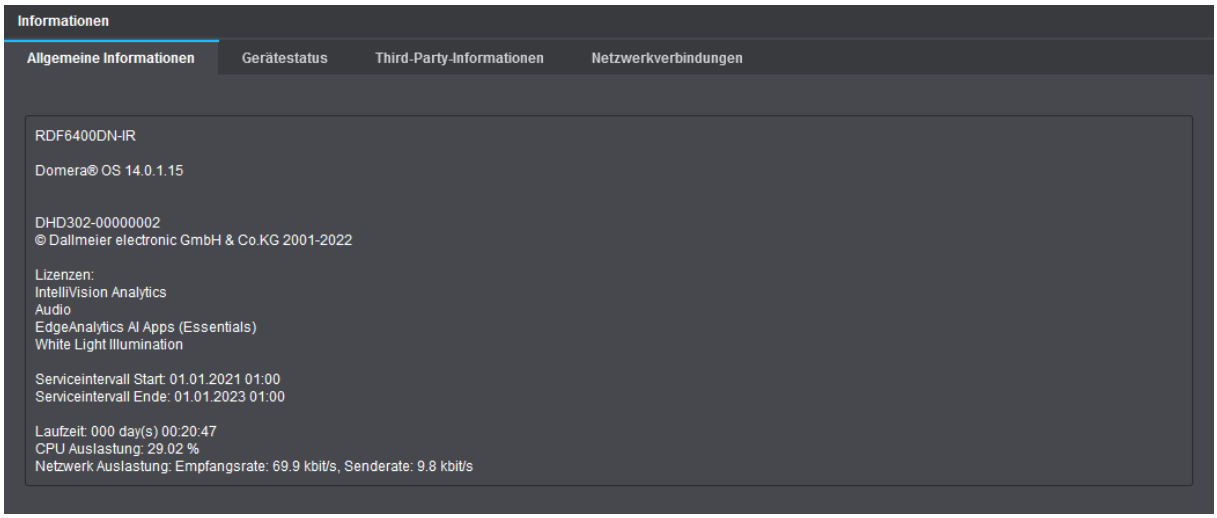


Abb. 18-1

Die folgenden Gerätedaten werden bereitgestellt:

- Bezeichnung des Produktmodells
- Versionsnummer des installierten Domera® OS
- Seriennummer des Geräts
- Aktuell über Lizenzen freigeschaltene Zusatzfunktionen (inklusive eines möglichen Ablaufdatums)
- Serviceintervall mit Start- und Enddatum (Gültigkeit der Software-Wartungslizenz)
- Laufzeit (vergangene Zeit seit dem letzten Systemstart des Geräts)
- CPU-Auslastung des Geräts
- Netzwerkauslastung des Geräts (aktuelle Empfangs- und Senderate)

> *Mithilfe der **Ereignisverwaltung** auf der Kamera und der Dallmeier Client-Software **PGuard advance** können Sie sich rechtzeitig vor Ablauf des Serviceintervalls der Software-Wartungslizenz automatisch benachrichtigen lassen (siehe Abschnitt „PGuard-Nachrichten“ auf Seite 93).*

## 18.2 GERÄTESTATUS

Auf der Registerkarte **Gerätestatus** werden Informationen über den allgemeinen Status des Geräts und, falls vorhanden, Hinweise zu erforderlichen Sicherheitsmaßnahmen in Bezug auf Cyber Security bzw. IT-Sicherheit angezeigt.

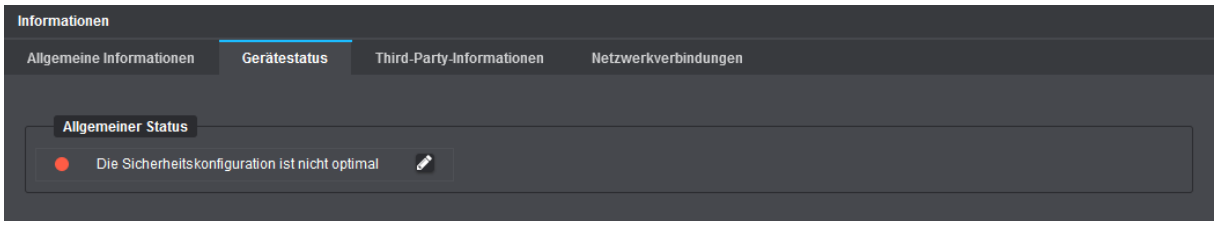


Abb. 18-2

## 18.3 THIRD-PARTY-INFORMATIONEN

Auf der Registerkarte **Third-Party-Informationen** werden Informationen über die auf dem Gerät verwendeten Software-Lizenzen von Drittanbietern angezeigt.

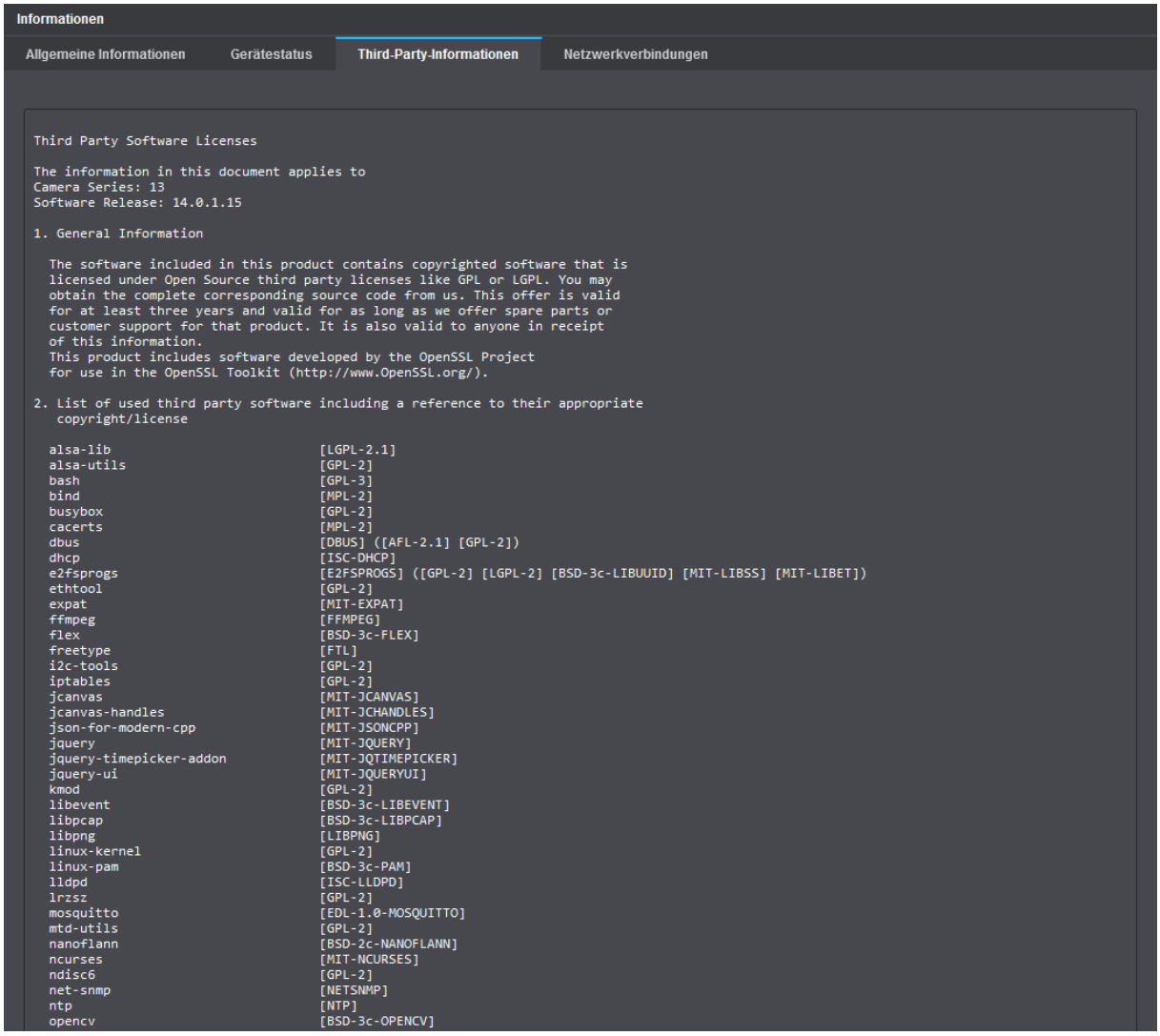


Abb. 18-3

## 18.4 NETZWERKVERBINDUNGEN

Auf der Registerkarte **Netzwerkverbindungen** werden detaillierte Informationen zu den gerade aktiven Netzwerkverbindungen angezeigt, die derzeit zur Kamera bestehen.

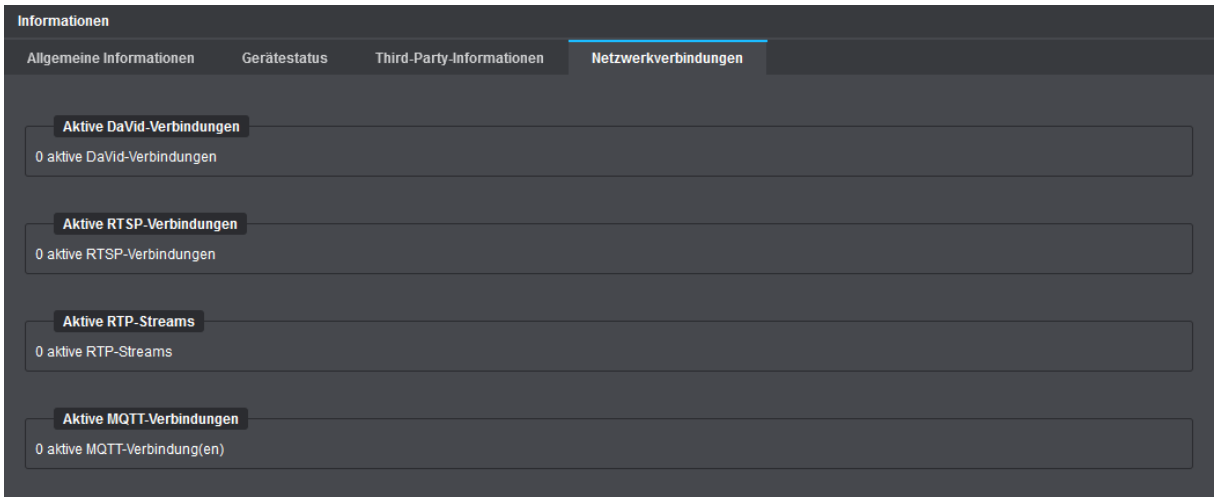


Abb. 18-4

# BILDÜBERTRAGUNG

Die Kamera kann als aktives Netzwerkelement zur kontinuierlichen Übertragung der erzeugten Videodaten (Unicast- oder Multicast-Streaming) ohne vorherige Anforderung durch einen Client konfiguriert werden (siehe Abschnitt „Streaming“ auf Seite 55).
Darüber hinaus kann die Kamera als passives Netzwerkelement von externen Clients und Applikationen dazu veranlasst werden, die Übertragung der erzeugten Videodaten über verschiedene Transport-, Übertragungs- und Steuerungsprotokolle zu initiieren.

## 19.1 EINZELBILDER (JPEG)

Aktuelle Videodaten können als Einzelbilder (JPEG) mit jedem beliebigen Webbrowser angezeigt werden.

| | |
|---|---|
| Transportprotokoll: | TCP |
| Übertragungsprotokoll: | HTTP |
| Port: | 80 |

Beachten Sie, dass

- der abgefragte Stream aktiviert sein muss (**Stream 1** ist immer aktiviert).
- der abgefragte Stream auf **MJPEG** eingestellt sein muss (andernfalls wird unabhängig vom abgefragten Stream nur ein anamorphes Miniatur-/Vorschaubild mit einem Seitenverhältnis von 4:3 und einer Größe von 640 × 480 Pixel angezeigt, das in der Breite gestaucht und in der Höhe gestreckt wirkt).

Beachten Sie zudem, dass entweder

- die Berechtigung **JPEG-Livebildzugriff** für einen bestimmten Benutzer gewährt sein muss, um den Zugriff auf die Einzelbilder nur mit vorheriger Benutzerauthentifizierung zu erlauben (siehe Abschnitt „Rechteverwaltung“ auf Seite 133), ...

  oder

- die Checkbox **HTTP JPEG Zugriff ohne Authentifizierung erlauben** aktiviert sein muss, wenn die Anzeige der Einzelbilder ohne Benutzerauthentifizierung gewährt werden soll (siehe Abschnitt „Anonymer Zugriff“ auf Seite 134).

Verwenden Sie einen der folgenden HTTP-Requests für den jeweils erforderlichen Stream:

```
[Stream 1]: http://192.168.2.28/live/image0.jpg
[Stream 2]: http://192.168.2.28/live/image1.jpg
[Stream 3]: http://192.168.2.28/live/image2.jpg
```

Die oben genannte Standard-IP-Adresse ist nur beispielhaft und muss mit der IP-Adresse Ihrer Kamera ersetzt werden.

Das angezeigte Einzelbild (JPEG) kann jederzeit manuell aktualisiert werden (z. B. mit der F5-Taste auf Ihrer Tastatur). Der jeweilige HTTP-Request kann außerdem in eine HTML-(JavaScript-)Seite eingebunden werden, die das Bild automatisch aktualisiert.

## 19.2 RTSP-APPLIKATION

Das Live-Video kann von externen RTSP-fähigen Applikationen (z. B. Playern) aktiv angefordert und die Übermittlung der Streaming-Inhalte mithilfe von RTSP gesteuert werden (Start und Stopp).
Beachten Sie dazu den Abschnitt „Netzwerk-Dienste“ auf Seite 62.

| | |
|---|---|
| Transportprotokoll: | TCP/UDP |
| Übertragungsprotokoll: | RTP |
| Steuerungsprotokoll: | RTSP |
| Port: | 554 (Standardeinstellung) |

**RTSP und RTP über HTTP Tunneling**

| | |
|---|---|
| Übertragungsprotokoll: | HTTP |
| Port: | 80 |

Beachten Sie, dass

- der angeforderte Stream aktiviert sein muss (**Stream 1** ist immer aktiviert).
- der **RTSP**-Server in der Kamera aktiviert sein muss (siehe Abschnitt „Netzwerk-Dienste“ auf Seite 62).

Beachten Sie zudem, dass entweder

- die Berechtigung **RTSP-Livebildzugriff** für einen bestimmten Benutzer gewährt sein muss, um den Zugriff auf das Live-Video nur mit vorheriger Benutzerauthentifizierung zu erlauben (siehe Abschnitt „Rechteverwaltung“ auf Seite 133), ...

  oder

- die Checkbox **RTSP Zugriff ohne Authentifizierung erlauben** aktiviert sein muss, wenn die Anzeige des Live-Videos ohne Benutzerauthentifizierung gewährt werden soll (siehe Abschnitt „Anonymer Zugriff“ auf Seite 134).

Verwenden Sie einen der folgenden RTSP-Requests für den jeweils erforderlichen Stream:

```
[Stream 1]: rtsp://192.168.2.28:554/encoder1
[Stream 2]: rtsp://192.168.2.28:554/encoder2
[Stream 3]: rtsp://192.168.2.28:554/encoder3
```

Die oben genannte Standard-IP-Adresse ist nur beispielhaft und muss mit der IP-Adresse Ihrer Kamera ersetzt werden.

Achten Sie darauf, dass nach einer Änderung der Standard-RTSP-Port-Nummer **554** (siehe Abschnitt „Netzwerk-Dienste“ auf Seite 62), diese auch im RTSP-Request explizit geändert werden muss.

Beispiel für **Stream 1** mit neuer RTSP-Port-Nummer **1024**:

```
[Stream 1]: rtsp://192.168.2.28:1024/encoder1
```

Die verfügbaren Streams 1 bis 3 können von drei Applikationen simultan abgefragt werden.
Damit kann eine sogenannte „Dual- oder Tri-Streaming“-Funktionalität realisiert werden (bis zu drei Streams mit unterschiedlicher Qualität).

Wenn mehrere Applikationen die Daten eines einzelnen Streams abfragen, steigt die Netzwerkauslastung und somit die erforderliche Bandbreite proportional an.
In diesem Fall sollte eine Multicast-Konfiguration vorgezogen werden, da diese nur die Bandbreite für einen Stream erfordert.

HEADQUARTERS

**Dallmeier electronic GmbH & Co.KG**
Bahnhofstr. 16
93047 Regensburg
Germany

tel +49 941 8700 0
fax +49 941 8700 180
mail info@dallmeier.com

https://www.dallmeier.com/