AXIS P1445-LE-3 License Plate Verifier Kit

Benutzerhandbuch

AXIS P1445-LE-3 License Plate Verifier Kit

Inhalt

Informationen zum Produkt 4
Erste Schritte 5
Grundeinstellungen 5
Empfehlungen für die Kameramontage 5
Einrichtungsassistent 7
Auf die Webseite des Produkts zugreifen 10
Anwendung installieren 11
Passen Sie den ausgewählten Bereich an 11
Region auswählen 12
Bilderfassungseinstellungen anpassen 12
Einrichten von Ereignisspeicher 13
Installation 14
Vorschaumodus 14
Listen verwalten 15
Erfasstes Fahrzeugkennzeichen der Liste hinzufügen 15
Beschreibungen zu Fahrzeugkennzeichen hinzufügen 15
Listennamen anpassen 15
Zulässig aufgelistete Kfz-Kennzeichen importieren 15
Listen planen 16
Weitere Einstellungen 17
Text-Overlay konfigurieren 17
Kennzeichen bei schlechten Lichtverhältnissen erkennen 17
Weniger Zeichen bei Fahrzeugkennzeichen erlauben 17
Nur exakte Übereinstimmungen von Nummernschildern zulassen 17
Bei der Übereinstimmung von Kennzeichen mehr als ein Zeichen Abweichung zulassen 17
Bedienern begrenzten Zugriff geben 18
Sichere Verbindung einrichten 18
Alle Ereignisse löschen 18
Aktionen über virtuelle Ports auslösen 18
Anwendungsfall Einfahrt und Ausfahrt von Fahrzeugen 20
Eine Schranke für bekannte Fahrzeuge mittels eines Relaismoduls öffnen 20
Eine Schranke für bekannte Fahrzeuge mittels des E/A der Kamera öffnen 21
Über ein nicht autorisiertes Fahrzeug benachrichtigt werden 22
Anwendungsfall Zufahrtskontrolle für Fahrzeuge 23
Mit einer Türsteuerung verbinden 23
Verknüpfung mit AXIS Secure Entry 25
Integration 27
Profile verwenden, um Ereignisse auf mehrere Server zu übertragen 27
Ereignisinformationen an die Software anderer Hersteller per Push senden 27
Bilder von Fahrzeugkennzeichen an einen Server senden 28
Direkte Integration mit 2N 28
Integration in das Genetec Security Center 29
Die Weboberfläche 32
Status 32
Video 33
Audio 45
Aufzeichnungen 46
Apps 47
System 48
Wartung 71
Technische Daten 73
Produktübersicht 73
LEDs 73
Einschub für SD-Speicherkarte 74
Tasten 74
Anschlüsse 74
Empfehlungen zur Reinigung 76
Fehlerbehebung 77
Für Benutzer von AXIS Camera Station 77

Inhalt

Technische Fragen, Hinweise und Lösungen 77
Zurücksetzen auf die Werkseinstellungen 79
Firmware aktualisieren 80
Leistungsaspekte 80

AXIS P1445-LE-3 License Plate Verifier Kit

Informationen zum Produkt

Informationen zum Produkt

Das AXIS P1445-LE-3 License Plate Verifier Kit besteht aus einer AXIS P1445-LE Network Camera und der vorinstallierten Anwendung AXIS License Plate Verifier, zusammen genommen eine einfache Lösung für die automatisierte Verwaltung von Einfahrts- und Ausfahrtsberechtigungen. AXIS P1445-LE-3 überprüft die Zufahrtsberechtigung zu überwachten Bereichen wie Parkplätzen über eine Freigabe- und eine Sperrliste.

Erste Schritte

Diese Setup-Anweisungen gelten für Kameras, die nicht zusammen mit AXIS License Plate Verifier verkauft werden.

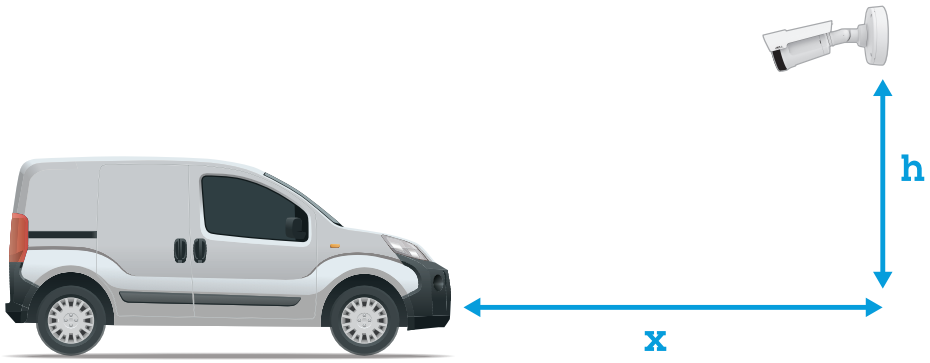
1.
2. *Anwendung installieren auf Seite 11*

Diese Setup-Anweisungen gelten für alle Szenarien:

1. *Empfehlungen für die Kameramontage auf Seite 5*
2. *Einrichtungsassistent auf Seite 7*
3. *Passen Sie den ausgewählten Bereich an auf Seite 11*
4. *Region auswählen auf Seite 12*
5. *Einrichten von Ereignisspeicher auf Seite 13*

Empfehlungen für die Kameramontage

- Beachten Sie bei der Auswahl des Montageorts, dass direkte Sonneneinstrahlung, wie zum Beispiel bei Sonnenaufgang und Sonnenuntergang, das Bild verzerren kann.
- Die Montagehöhe einer Kamera muss für das Szenario **Zutrittskontrolle** die Hälfte des Abstands zwischen Fahrzeug und Kamera betragen.
- Die Montagehöhe der Kamera für das Szenario **Freie Fahrt** (Fahrzeugkennzeichenerkennung bei langsamen Geschwindigkeiten) muss geringer als die Hälfte des Abstands zwischen Fahrzeug und Kamera sein.



Erfassungsdistanz für **Access control (Zutrittskontrolle)**: 2 bis 7 m. Dieses Beispiel basiert auf dem AXIS P3265-LVE-3 License Plate Verifier Kit.

Erfassungsdistanz: (x)	Montagehöhe (y)
2,0 m	1,0 m
3,0 m	1,5 m

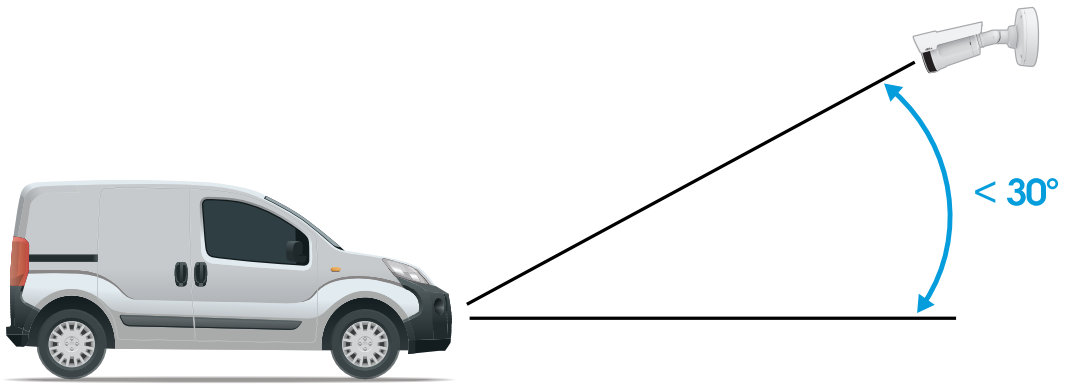
Erste Schritte

4,0 m	2,0 m
5,0 m	2,5 m
7,0 m	3,5 m

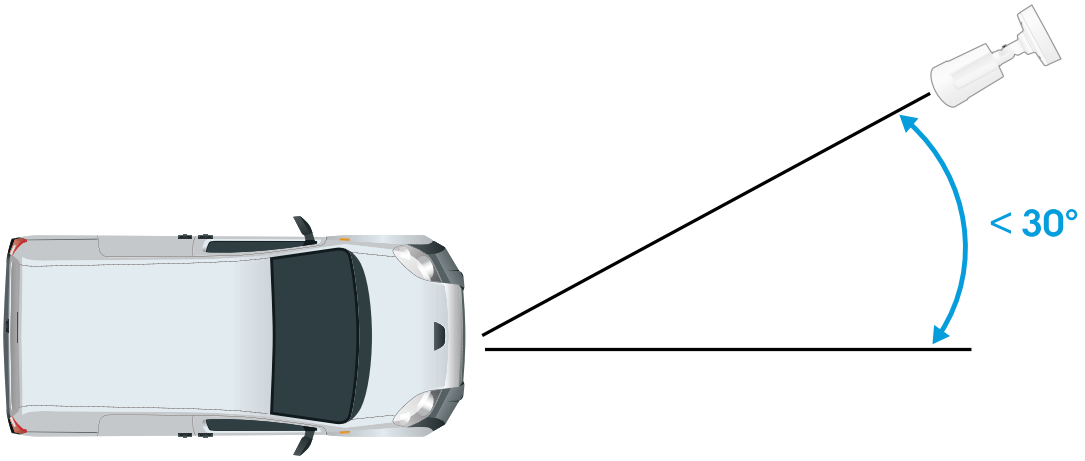
Erfassungsdistanz für **Free flow (Freie Fahrt)**: 7 bis 20 m. Dieses Beispiel basiert auf dem AXIS P1465-LE-3 License Plate Verifier Kit.

Erfassungsdistanz (x)	Montagehöhe (y)
7,0 m	3,0 m
10,0 m	4,0 m
15,0 m	6,0 m
20,0 m	10,0 m

- Der Montagewinkel der Kamera darf zu keiner Richtung hin weiter als 30° sein.

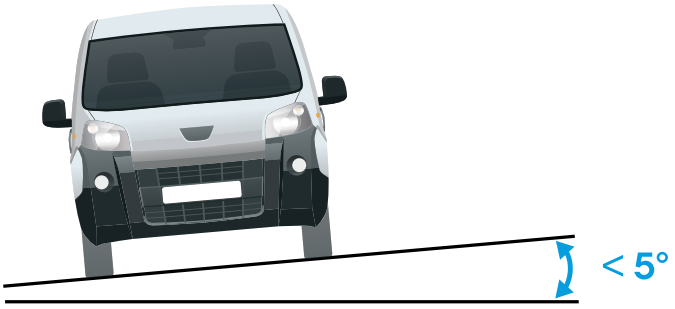


Montagewinkel von der Seite.



Montagewinkel von oben.

- Das Bild des Fahrzeugkennzeichens darf nicht um mehr als 5° horizontal geneigt sein. Falls das Bild um mehr als 5° geneigt ist, empfehlen wir für die Kamera eine Einstellung, bei der das Fahrzeugkennzeichen im Livestream horizontal dargestellt wird.



Horizontale Neigung

Einrichtungsassistent

Richten Sie beim ersten Ausführen der Anwendung mithilfe des Einrichtungsassistenten entweder **Free flow (Freie Fahrt)** oder **Access control (Zutrittskontrolle)** ein. Wenn Sie später Änderungen vornehmen möchten, ist das über die Registerkarte **Settings (Einstellungen)** unter **Setup assistant (Konfigurationsassistent)** möglich.

Freie Fahrt

Mit dieser Option kann die Anwendung Fahrzeugkennzeichen bei langsam fließendem Verkehr auf größeren Zufahrtsstraßen, in Stadtzentren und innerhalb geschlossener Bereiche wie einem Campus, Häfen oder Flughäfen erkennen und lesen. Dadurch sind eine LPR-forensische Suche und durch LPR ausgelöste Ereignisse in einem VMS möglich.

1. Wählen Sie **Freie Fahrt** und klicken Sie auf **Weiter**.
2. Wählen Sie die Bilddrehung aus, die der Montageposition der Kamera entspricht.
3. Wählen Sie die Anzahl der ausgewählten Bereiche. Beachten Sie, dass in einem Bereich Fahrzeugkennzeichen von in beide Richtungen fahrenden Fahrzeugen erkannt werden können.
4. Wählen Sie den Bereich, in dem sich die Kamera befindet.
5. Wählen Sie den Erfassungstyp.
   - Mit **Fahrzeugkennzeichen ausschneiden** wird nur das Fahrzeugkennzeichen gespeichert.
   - Mit **Fahrzeug ausschneiden** wird das gesamte erfasste Fahrzeug gespeichert.
   - Mit **Bildauflösung auf 480x270 reduziert** wird das gesamte Bild gespeichert und die Auflösung auf 480x270 reduziert.
   - Mit **Vollbild** wird das gesamte Bild in voller Auflösung gespeichert.
6. Ziehen Sie die Ankerpunkte, um den ausgewählten Bereich anzupassen. Siehe *Passen Sie den ausgewählten Bereich an auf Seite 11*.
7. Passen Sie die Richtung für den ausgewählten Bereich an. Klicken Sie auf den Pfeil und drehen Sie ihn, um die Richtung festzulegen. Die Richtung legt fest, wie die Anwendung Fahrzeuge registriert, die in den Bereich einfahren oder ihn verlassen.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie in der Auswahlliste **Protokoll** eines der folgenden Protokolle:
   - TCP
   - HTTP POST
10. Geben Sie in das Feld **Server-URL** die Server-Adresse und den Port im folgenden Format ein: `127.0.0.1:8080`
11. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein oder lassen Sie den vorgegebenen Namen stehen.
12. Wählen Sie unter **Ereignistypen** eine oder mehrere der folgenden Optionen:
    - **New (Neu)** steht für die Ersterkennung eines Fahrzeugkennzeichens.
    - **Update (Aktualisierung)** ist entweder eine Korrektur eines Zeichens auf einem zuvor erkannten Kennzeichen oder wenn eine Richtung erkannt wird, während sich das Kennzeichen bewegt und über das Bild verfolgt wird.
    - **Lost (Verloren)** ist das letzte verfolgte Ereignis des Kennzeichens, bevor es das Bild verlässt. Es enthält auch die Richtung des Kennzeichens.
13. Um die Funktion zu aktivieren, **Send event data to server (Ereignisdaten an Server senden)** auswählen.
14. Um beim Verwenden von HTTP Post die Bandbreite zu verringern, die Option **Do not to send images through HTTP POST (Keine Bilder über HTTP POST senden)** wählen.
15. Auf **Next (Weiter)** klicken.
16. Wenn Sie bereits über eine Liste mit registrierten Kennzeichen verfügen, importieren Sie diese entweder als **Sperrliste** oder als **Freigabeliste**.
17. Klicken Sie auf **Finish (Fertigstellen)**.

Zutrittskontrolle

Verwenden Sie den Setup-Assistenten für eine schnelle und einfache Konfiguration. Sie können die Anleitung mit **Überspringen** jederzeit verlassen.

1. Wählen Sie **Zutrittskontrolle** und klicken Sie auf **Weiter**.
2. Wählen Sie den Typ der zu verwendenden Zutrittskontrolle aus:
   - **Interner E/A** zur Beibehaltung der Listenverwaltung über die Kamera. Siehe *Eine Schranke für bekannte Fahrzeuge mittels des E/A der Kamera öffnen auf Seite 21*.
   - **Controller** zum Anschließen eines Türcontrollers. Siehe *Mit einer Türsteuerung verbinden auf Seite 23*.
   - **Relais** zum Anschließen an einem Relaismodul. Siehe *Eine Schranke für bekannte Fahrzeuge mittels eines Relaismoduls öffnen auf Seite 20*.
3. Wählen Sie in der Auswahlliste **Schrankenmodus** unter **Über Listen öffnen** die Option **Freigabeliste**.
4. Wählen Sie in der Auswahlliste **Fahrzeugrichtung** die Option **Ausfahrt**.
5. Wählen Sie in der Auswahlliste **ROI** den in Frage kommenden ausgewählten Bereich oder wählen Sie alle Bereiche.
6. Auf **Next (Weiter)** klicken.

Auf der Seite mit den **Image settings** (Bildeinstellungen):

1. Wählen Sie die Anzahl der ausgewählten Bereiche.
2. Wählen Sie den Bereich, in dem sich die Kamera befindet.
3. Wählen Sie den Erfassungstyp. Siehe *Bilderfassungseinstellungen anpassen auf Seite 12*.
4. Ziehen Sie die Ankerpunkte, um den ausgewählten Bereich anzupassen. Siehe *Passen Sie den ausgewählten Bereich an auf Seite 11*.
5. Passen Sie die Richtung für den ausgewählten Bereich an. Die Richtung legt fest, wie die Anwendung Fahrzeuge registriert, die in den Bereich einfahren oder ihn verlassen.
6. Klicken Sie auf **Weiter**.

Auf der Seite **Event data** (Ereignisdaten):

Hinweis

Ausführliche Einstellungen finden Sie unter: *Ereignisinformationen an die Software anderer Hersteller per Push senden auf Seite 27*.

1. Aus dem Aufklappmenü **Protocol (Protokoll)** eines der folgenden Protokolle auswählen:
   - TCP
   - HTTP POST
2. Geben Sie in das Feld **Server-URL** die Server-Adresse und den Port im folgenden Format ein: `127.0.0.1:8080`.
3. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein oder lassen Sie den vorgegebenen Namen stehen.
4. Wählen Sie unter **Ereignistypen** eine oder mehrere der folgenden Optionen:
   - **New (Neu)** steht für die Ersterkennung eines Fahrzeugkennzeichens.
   - **Update (Aktualisierung)** ist entweder eine Korrektur eines Zeichens auf einem zuvor erkannten Kennzeichen oder wenn eine Richtung erkannt wird, während sich das Kennzeichen bewegt und über das Bild verfolgt wird.
   - **Lost (Verloren)** ist das letzte verfolgte Ereignis des Kennzeichens, bevor es das Bild verlässt. Es enthält auch die Richtung des Kennzeichens.
5. Um die Funktion zu aktivieren, **Send event data to server (Ereignisdaten an Server senden)** auswählen.

6. Um beim Verwenden von HTTP Post die Bandbreite zu verringern, die Option **Do not to send images through HTTP POST (Keine Bilder über HTTP POST senden)** wählen.
7. Klicken Sie auf **Weiter**.

Auf der Seite **Import list from a .csv file** (Liste aus einer CSV-Datei importieren):

1. Wenn Sie bereits über eine Liste mit registrierten Kennzeichen verfügen, importieren Sie diese entweder als **Sperrliste** oder als **Freigabeliste**.
2. Klicken Sie auf **Finish (Fertigstellen)**.

Auf die Webseite des Produkts zugreifen

Bei unbekannter IP-Adresse den AXIS IP-, Utility- oder AXIS Device-Manager verwenden, um das Produkt im Netzwerk zu ermitteln. Beide Anwendungen sind kostenlos und können von *axis.com/support* heruntergeladen werden.

Wir empfehlen folgende Browser:

- Chrome™
- Firefox®

1. Den Browser öffnen.
2. Die IP-Adresse oder den Hostnamen des Axis Produkts in die Adresszeile des Browsers eingeben.
3. Den Benutzernamen und das Kennwort eingeben. Wenn dies der erste Zugriff auf das Produkt ist, muss zuerst das Root-Kennwort konfiguriert werden.
4. Wenn dies der erste Zugriff auf das Produkt ist, werden Sie aufgefordert, einige Grundeinstellungen vorzunehmen. Danach wird im Browser die Produktseite mit der Live-Ansicht geöffnet.

Weitere Informationen zum Ermitteln und Zuweisen von IP-Adressen bietet das Dokument *Zuweisen von IP-Adressen und Zugreifen auf das Gerät* auf der jeweiligen Produktseite auf *axis.com*

Erstellen Sie ein Administratorenkonto

Beim ersten Anmelden an Ihrem Gerät muss ein Administratorkonto erstellt werden.

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Kennwort ein. Siehe *Sichere Kennwörter auf Seite 10*.
3. Geben Sie das Kennwort erneut ein.
4. Klicken Sie auf **Add user (Benutzer hinzufügen)**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 79*.

Sichere Kennwörter

Wichtig

Das voreingestellte Kennwort wird vom Axis Gerät unverschlüsselt über das Netz gesendet. Um das Gerät zu schützen, nach dem ersten Anmelden eine sichere und verschlüsselte HTTPS-Verbindung einrichten und dann das Kennwort ändern.

Das Gerätekennwort ist der Hauptschutz für Ihre Daten und Dienste. Produkte von Axis geben keine Kennwortrichtlinien vor, da die Produkte unter den verschiedensten Bedingungen eingesetzt werden.

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

- Ein Kennwort zu verwenden, das aus mindestens acht Zeichen besteht, und das bevorzugt von einem Kennwortgenerator erzeugt wurde.
- Das Kennwort geheimzuhalten.
- Das Kennwort regelmäßig und mindestens jährlich zu ändern.

Anwendung installieren

Hinweis

Bei den Kameras P1445-LE-3, P3245-LE-3 und P1455-LE-3 wird AXIS License Plate Verifier mit der Firmware vorinstalliert.

Hinweis

Zur Installation von Anwendungen auf dem Gerät sind Administratorrechte erforderlich.

1. Die Webseite des Geräts aufrufen.
2. Die Option **Settings > Apps (Einstellungen > Apps)** aufrufen.
3. **Add (Hinzufügen)** anklicken, um die Anwendungsdatei (Format .eap) auf die Kamera hochzuladen.

Zum Aktivieren der Lizenz ist ein Lizenzschlüssel erforderlich. Dieser wird aus dem Lizenzcode und der Seriennummer des Axis Geräts generiert. Falls auf dem Computer kein Lizenzschlüssel hinterlegt ist, wie folgt vorgehen:

1. Gehen Sie auf *axis.com/support/license-key-registration#/registration*
2. Geben Sie die Seriennummer und den Lizenzcode ein.
3. Speichern Sie die Lizenzschlüsseldatei auf dem Computer. Den Speicherort der Datei ermitteln und **Activate (Aktivieren)** wählen.

Passen Sie den ausgewählten Bereich an

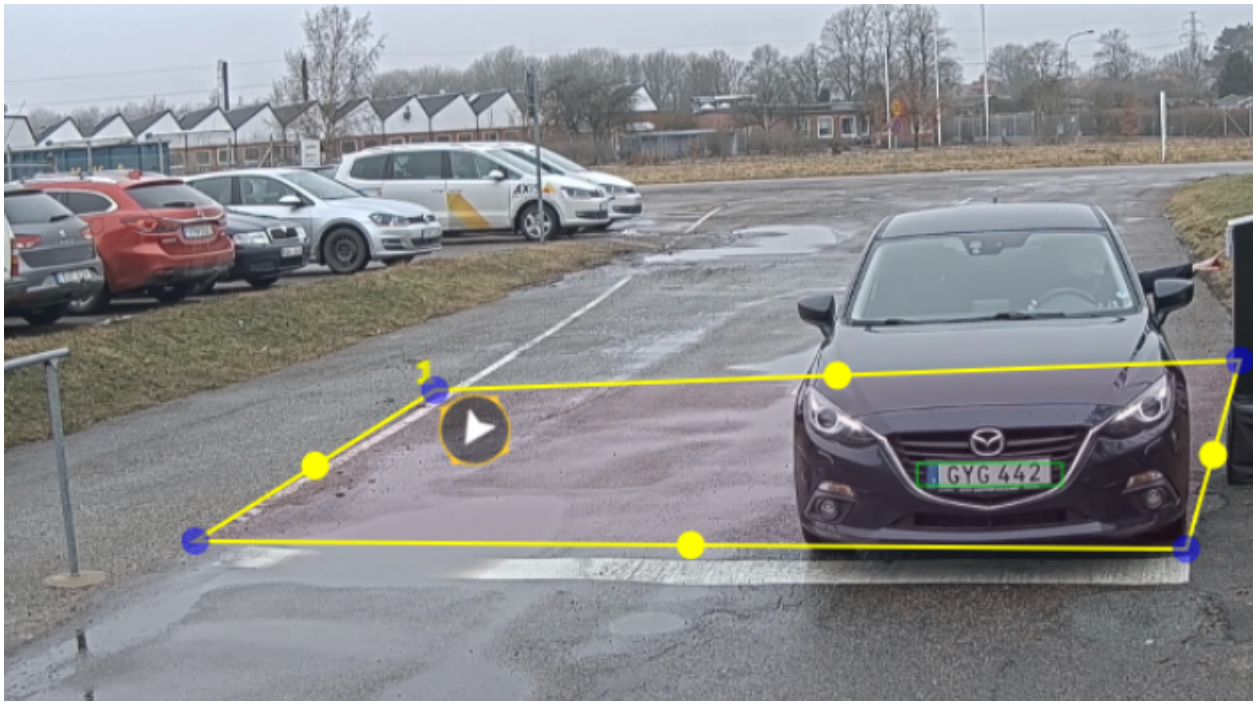
Der ausgewählte Bereich ist der Bereich in der Live-Ansicht, in dem die Anwendung nach Fahrzeugkennzeichen sucht. Legen Sie den ausgewählten Bereich aus Leistungsgründen so klein wie möglich an. Passen Sie die Konfiguration für den ausgewählten Bereich an:

1. Wechseln Sie zu **Settings (Einstellungen)**.
2. Klicken Sie auf **Edit area of interest (Ausgewählten Bereich bearbeiten)**.
3. Um die Verifizierung und die erfassten Bilder zu verbessern, gehen Sie zu **Zoom** und stellen den Schieber gemäß Ihren Anforderungen ein.
4. Damit die Kamera die Fahrzeuge automatisch fokussiert, klicken Sie auf **Autofocus (Autofokus)**. Um den Fokus manuell einzustellen, gehen Sie zu **Focus (Fokus)** und stellen ihn mit dem Schieber ein.
5. Klicken Sie auf einen beliebigen Bereich und ziehen Sie ihn an die Stelle, an der die Nummernschilder am besten sichtbar sind, um den ausgewählten Bereich zu verschieben. Wenn der ausgewählte Bereich außerhalb der Live-Ansicht liegt, springt er automatisch wieder auf die Standardposition zurück. Nach dem Speichern der Einstellungen sicherstellen, dass der Interessensbereich in der gewählten Position angezeigt wird.
6. Um den ausgewählten Bereich anzupassen, klicken Sie auf eine beliebige Stelle im Bereich und ziehen Sie die blau markierten Ankerpunkte.
   - Um den ausgewählten Bereich zurückzusetzen, klicken Sie mit der rechten Maustaste in den Bereich und wählen Sie **Reset (Zurücksetzen)**.
   - Um Ankerpunkte hinzuzufügen, klicken Sie auf einen der gelben Ankerpunkte. Der Ankerpunkt wird jetzt blau dargestellt und kann verändert werden. Neben dem blauen Ankerpunkt werden automatisch neue gelbe Punkte hinzugefügt. Die maximale Anzahl blauer Ankerpunkte beträgt acht.

7. Klicken Sie auf einen beliebigen Bereich außerhalb des ausgewählten Bereichs, um Ihre Änderungen zu speichern.
8. Um im **Event log (Ereignisprotokoll)** korrekte Rückmeldungen zur Fahrtrichtung zu erhalten, drehen Sie den Pfeil in die Fahrtrichtung.
   8.1 Klicken Sie auf das Pfeil-Symbol.
   8.2 Wählen Sie den Ankerpunkt aus und drehen Sie den Pfeil, sodass in die Fahrtrichtung zeigt.
   8.3 Um die Änderungen zu speichern, außerhalb des zu wählenden Bereichs klicken.

Beachten Sie, dass in einem Bereich Fahrzeugkennzeichen von in beide Richtungen fahrenden Fahrzeugen erkannt werden können. Die Rückmeldungen zur Fahrtrichtung werden in der Spalte **Direction (Richtung)** angezeigt.

- Um einen zweiten ausgewählten Bereich hinzuzufügen, wählen Sie **2** im Auswahlmenü **Area of interest (Ausgewählter Bereich)**.



Beispiel mit einem ausgewählten Bereich.

Hinweis

- Bei Verwendung einer eigenständigen Kamera können mit der App die empfohlenen Einstellungen für die Nummernschilderkennung festgelegt werden.

  Klicken Sie auf **Recommended LPR settings (Empfohlene LPR-Einstellungen)**. In der Tabelle werden die aktuellen und die empfohlenen Einstellungen unterschiedlich dargestellt.

  Klicken Sie auf **Update settings (Einstellungen aktualisieren)**, damit die App ihre empfohlenen Werte ändert.

Region auswählen

1. Wechseln Sie zu **Settings (Einstellungen)** > **Image (Bild)**.
2. Wählen Sie in der Auswahlliste **Region** Ihre Region aus.

Bilderfassungseinstellungen anpassen

1. Wechseln Sie zu **Settings (Einstellungen)** > **Image (Bild)**.
2. Um die Auflösung von erfassten Bildern zu ändern, wechseln Sie zu **Auflösung**.
3. Um die Drehung des erfassten Bilds zu ändern, wechseln Sie zu **Bilddrehung**.
4. Um die Speicherungsart der erfassten Bilder zu ändern, wechseln Sie zu **Save full frame (Vollbild speichern)**:
   - Mit **Fahrzeugkennzeichen ausschneiden** wird nur das Fahrzeugkennzeichen gespeichert.
   - Mit **Fahrzeug ausschneiden** wird das gesamte erfasste Fahrzeug gespeichert.
   - Mit **Frame downsized 480x270 (Bildauflösung auf 480x270 reduziert)** wird das gesamte Bild gespeichert und die Auflösung auf 480x270 reduziert.
   - Mit **Full frame (Vollbild)** wird das gesamte Bild in voller Auflösung gespeichert.

Einrichten von Ereignisspeicher

Ein Ereignis besteht aus dem erfassten Bild, dem Fahrzeugkennzeichen, der Nummer des ausgewählten Bereichs, der Fahrzeugrichtung, dem Zugang sowie Datum und Uhrzeit.

Anhand des Anwendungsfalls in diesem Beispiel wird erklärt, wie Ereignisse mit zulässigen Fahrzeugkennzeichen 30 Tage lang gespeichert werden können.

Erforderlich:

- Physisch installierte und an das Netzwerk angeschlossene Kamera
- AXIS License Plate Verifier ist auf dem aktuellen Stand und wird auf der Kamera ausgeführt.
- Interner Speicher oder eine in der Kamera installierte SD-Karte.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Events (Ereignisse)**.
2. Wählen Sie unter **Save events (Ereignisse speichern)**die Option **Allowlisted (Als zulässig geführt)**.
3. Unter **Delete events after (Ereignisse löschen nach)30 days (30 Tage)** wählen.

Hinweis

Um eine eingelegte SD-Karte zu erkennen, wenn die App läuft, müssen Sie die App neu starten. Wenn eine SD-Karte in der Kamera installiert ist, wählt die App automatisch die SD-Karte als Standardspeicher aus.
AXIS License Plate Verifier verwendet den internen Speicher der Kameras, um bis zu 1.000 Ereignisse zu speichern, wobei der Ausschnitt des Fahrzeugkennzeichens als Rahmen dient. Wenn Sie größere Bilder verwenden, variiert die Anzahl der Ereignisse, die Sie speichern können.
Um die Aufnahmeeinstellungen zu ändern, wechseln Sie zu **Settings > Image** (Einstellungen > Bild). Auf einer SD-Karte können bis zu 100.000 Ereignisse beliebiger Bildtypen gespeichert werden.

Installation

Vorschaumodus

Der Vorschaumodus eignet sich optimal für Monteure für die Feinjustierung der Kameraansicht während der Installation. Für den Zugriff auf die Kameraansicht im Vorschaumodus ist keine Anmeldung erforderlich. Sie ist ab dem Einschalten des Geräts nur für eine begrenzte Zeit in der Werkseinstellung verfügbar.

Dieses Video zeigt, wie der Vorschaumodus verwendet wird.

Listen verwalten

Erfasstes Fahrzeugkennzeichen der Liste hinzufügen

Ein Fahrzeugkennzeichen kann nach der Erfassung durch die Anwendung direkt einer Liste hinzugefügt werden.

1. Klicken Sie auf die Registerkarte **Event log** (Ereignisprotokoll).
2. Rufen Sie **Latest Event** (Letztes Ereignis) auf.
3. Klicken Sie neben dem hinzuzufügenden Fahrzeugkennzeichen auf **Der Liste hinzufügen**.
4. Wählen Sie im Auswahlmenü die Liste, der das Fahrzeugkennzeichen hinzugefügt werden soll.
5. Klicken Sie auf **Append** (Anhängen).

Beschreibungen zu Fahrzeugkennzeichen hinzufügen

So fügen Sie in der Liste eine Beschreibung zu einem Fahrzeugkennzeichen hinzu:

- Wechseln Sie zu **List management (Listenverwaltung)**.
- Wählen Sie das Fahrzeugkennzeichen aus, das Sie bearbeiten möchten, und klicken Sie auf das Stiftsymbol.
- Geben Sie die relevanten Informationen in das Feld **Description (Beschreibung)** oben in der Liste ein.
- Klicken Sie zum Speichern auf das Laufwerkssymbol.

Listennamen anpassen

Sie können den Namen jeder einzelnen Liste so ändern, dass dieser Ihrem speziellen Anwendungsfall entspricht.

1. Wechseln Sie zu **List management (Listenverwaltung)**.
2. Wechseln Sie zum Listenmenü der Liste, die Sie ändern möchten.
3. Wählen Sie **Umbenennen** aus.
4. Geben Sie den Namen der Liste ein.

Der neue Listenname wird in allen vorhandenen Konfigurationen aktualisiert.

Zulässig aufgelistete Kfz-Kennzeichen importieren

Sie können zulässige Fahrzeugkennzeichennummern aus einer .csv-Datei auf dem Computer importieren. Zusätzlich zum Fahrzeugkennzeichen können Sie in der CSV-Datei zu jedem Fahrzeugkennzeichen auch Kommentare hinzufügen.

Die Struktur der CSV-Datei muss wie folgt aussehen: `Fahrzeugkennzeichen, Datum, Beschreibung`

Beispiel

Nur Fahrzeugkennzeichen: `AXIS123`

Fahrzeugkennzeichen + Beschreibung: `AXIS123,,John Smith`

Fahrzeugkennzeichen + Datum + Beschreibung: `AXIS123,2022-06-08,John Smith`

1. Gehen Sie zu **Listenverwaltung**.
2. Gehen Sie zum Kontextmenü neben **Freigabeliste** und wählen Sie **Aus Datei importieren**.

3. Wählen Sie auf dem Computer eine CSV-Datei aus.
4. **OK** anklicken.
5. Überprüfen Sie, ob die importierten Fahrzeugkennzeichen in der **Freigabeliste** angezeigt werden.

Kennzeichen-Listen mit anderen Kameras teilen

Sie können die Kennzeichen-Listen für andere Kameras im Netzwerk freigeben. Bei der Synchronisation werden alle aktuellen Listen mit Fahrzeugkennzeichen der anderen Kameras überschrieben.

1. Wechseln Sie zu **List management (Listenverwaltung)**.
2. Geben Sie unter **Kamerasynchronisierung** die IP-Adresse, den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **+**.
4. Klicken Sie auf **Kamerasynchronisierung**.
5. Überprüfen Sie, ob Datum und Uhrzeit unter **Letzte Synchronisierung** entsprechend aktualisiert werden.

Listen planen

Listen können so geplant werden, dass sie nur zu bestimmten Zeiten an bestimmten Wochentagen aktiv sind. Liste planen:

- Wechseln Sie zu **List management (Listenverwaltung)**.
- Wechseln Sie zum Menü der Liste, die Sie planen möchten.
- Wählen Sie **Schedule (Zeitplan)** im Popup-Menü aus.
- Wählen Sie Start- und Endzeit sowie den Tag aus, an dem die Liste aktiv sein soll.
- Klicken Sie auf die Schaltfläche neben **Enabled (Aktiviert)**.
- Klicken Sie auf **Save (Speichern)**.

Weitere Einstellungen

Text-Overlay konfigurieren

Ein Text-Overlay zeigt die folgenden Ereignisinformationen in der Live-Ansicht an: `Wochentag, Monat, Uhrzeit, Jahr, Fahrzeugkennzeichen`.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Image (Bild)**.
2. Aktivieren Sie **Text-Overlay**.
3. Stellen Sie für die **Overlay-Dauer** einen Wert zwischen 1 und 9 Sekunden ein.
4. Wählen Sie entweder Datum, Uhrzeit und Fahrzeugkennzeichen (**Datum/Uhrzeit + FK**) oder nur das Fahrzeugkennzeichen (**FK**.
5. Stellen Sie sicher, dass das Overlay in der Live-Ansicht angezeigt wird.

Kennzeichen bei schlechten Lichtverhältnissen erkennen

Jede Erfassung erhält durch den Algorithmus eine Punktzahl, die als Empfindlichkeitswert (Confidence-Parameter) bezeichnet wird. Erfassungen mit einer niedrigeren Punktzahl als der ausgewählte Wert werden in der Ereignisliste nicht angezeigt.

Bei Szenen mit dunklen Lichtbedingungen können Sie den Empfindlichkeitswert niedriger einstellen.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Detection parameters (Erfassungsparameter)**.
2. Passen Sie den Schieber unter **Empfindlichkeitswert** an. Um Fehlerfassungen zu vermeiden, wird empfohlen, den Grenzwert schrittweise um 0,05 zu verringern.
3. Stellen Sie sicher, dass der Algorithmus die Fahrzeugkennzeichen wie erwartet erfasst.

Weniger Zeichen bei Fahrzeugkennzeichen erlauben

In der Anwendung ist standardmäßig eine zur Erfassung eines Fahrzeugkennzeichens erforderliche Mindestanzahl an Zeichen festgelegt. Die standardmäßige Mindestanzahl an Zeichen beträgt fünf. Sie können die Anwendung so konfigurieren, dass Fahrzeugkennzeichen mit weniger Zeichen erfasst werden.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Detection parameters (Erfassungsparameter)**.
2. Geben Sie im Feld **Mindestanzahl an Zeichen** die Mindestanzahl an Zeichen ein, die zugelassen werden sollen.
3. Stellen Sie sicher, dass die Anwendung die Kennzeichen wie erwartet erfasst.

Nur exakte Übereinstimmungen von Nummernschildern zulassen

Der Abgleichalgorithmus erlaubt automatisch eine Abweichung von einem Zeichen beim Abgleich des erkannten Kennzeichens mit der Erlaubnis- oder Blockliste. Für einige Szenarien müssen jedoch alle Zeichen des Fahrzeugkennzeichens genau überstimmen.

1. Wechseln Sie zu **List management (Listenverwaltung)**.
2. Klicken Sie hier, um **Strikter Abgleich** zu aktivieren.
3. Stellen Sie sicher, dass die Anwendung die Fahrzeugkennzeichen wie erwartet abgleicht.

Weitere Einstellungen

Bei der Übereinstimmung von Kennzeichen mehr als ein Zeichen Abweichung zulassen

Der Abgleichalgorithmus erlaubt automatisch eine Abweichung von einem Zeichen beim Abgleich des erkannten Kennzeichens mit der Erlaubnis- oder Blockliste. Sie können jedoch mehr als ein Zeichen Abweichung zulassen.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Detection parameters (Erfassungsparameter)**.
2. Wählen Sie unter **Zulässige Zeichenabweichung** die Anzahl an Zeichen auf, die sich unterscheiden dürfen.
3. Stellen Sie sicher, dass die Anwendung die Fahrzeugkennzeichen wie erwartet abgleicht.

Bedienern begrenzten Zugriff geben

Bediener können über eine URL begrenzten Zugriff auf die App erhalten. Auf diese Weise haben sie nur Zugriff auf das **Event log (Ereignisprotokoll)** und die **List management (Listenverwaltung)**. Die URL finden Sie unter **Settings > User rights (Einstellungen > Benutzerrechte)**.

Sichere Verbindung einrichten

Richten Sie zum Schutz der Kommunikation und Daten zwischen Geräten, z. B. zwischen Kamera und Tür-Steuerung mithilfe von Zertifikaten eine sichere Verbindung mit HTTPS ein.

1. Wechseln Sie zu **Settings (Einstellungen)** > **Security (Sicherheit)**.
2. Aktivieren Sie HTTPS über die Option **HTTPS aktivieren**.
3. Wählen Sie entweder **Selbstsigniert** oder **CA-signiert**.

Hinweis

Weitere Informationen zu HTTPS und zu dessen Nutzung finden Sie auf .

Alle Ereignisse löschen

Nachdem Sie die App eingerichtet haben, kann es sinnvoll sein, die Aufzeichnungen von Bildern oder erfassten Kennzeichen während des Setups zu löschen.

So löschen Sie alle Bilder und Kennzeichen aus der Datenbank:

Wechseln Sie zu **Settings > Maintenance (Einstellungen > Wartung)**.

- Klicken Sie auf **Clear all recognition results auf (Alle Erkennungsergebnisse löschen)**.
- Klicken Sie auf **Yes (Ja)**.

Aktionen über virtuelle Ports auslösen

Virtuelle Ports können zusammen mit der Zutrittskontrolle verwendet werden, um Aktionen jeglicher Art auszulösen. In diesem Beispiel wird die gemeinsame Einrichtung von AXIS License Plate Verifier und der E/A-Eingänge zum Anzeigen eines Text-Overlays mithilfe eines virtuellen Ports.

Voraussetzungen:

- Physisch installierte und an das Netzwerk angeschlossene Kamera.
- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
- Kabel zwischen Schranke und E/A-Port der Kamera angeschlossen.
- Die Grundeinstellungen wurden vorgenommen. Siehe *Grundeinstellungen auf Seite 5*.

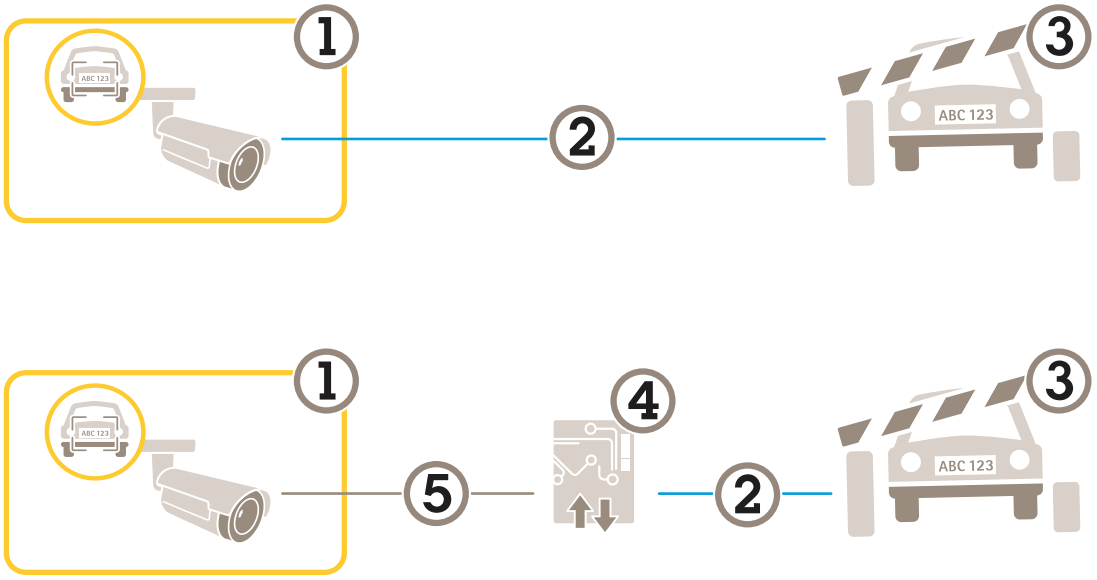
Weitere Einstellungen

1. Gehen Sie auf die Webseite der Anwendung und wählen Sie die Registerkarte **Einstellungen**.
2. Gehen Sie zu **Zutrittskontrolle**.
3. Wählen Sie unter **Zutrittskontrolle** in der Auswahlliste **Typ** die Option **Interner E/A**.
4. Wählen Sie die **E/A-Ausgangsnr.**.
5. Wählen Sie in der Auswahlliste **Virtueller Port** einen Port aus.
6. Wählen Sie im Auswahlmenü **Schrankenmodus** die Option **Für alle öffnen**.
7. Wählen Sie im Auswahlmenü **Fahrzeugrichtung** die Option **Jede**.
8. Wählen Sie in der Auswahlliste **ROI** den in Frage kommenden ausgewählten Bereich oder wählen Sie alle Bereiche.
9. Wechseln Sie zu die Webseite der Kamera zu **System > Ereignisse**.
10. Klicken Sie auf **Regel hinzufügen**.
11. Wählen Sie unter **Condition (Bedingung)** die Option **Virtual input is active (Virtueller Eingang ist aktiv)** und die von Ihnen ausgewählte Portnummer aus.
12. Wählen Sie unter **Action (Aktion)** die Option **Use overlay text (Overlay-Text verwenden)** aus.
13. Wählen Sie **Videokanäle**.
14. Geben Sie den anzuzeigenden Text ein.
15. Fügen Sie die Dauer des Textes hinzu.
16. Klicken Sie auf **Save (Speichern)**.
17. Rufen Sie **Video > Overlays** auf.
18. Rufen Sie **Overlays** auf.
19. Wählen Sie im Auswahlmenü die Option **Text** und klicken Sie auf **+**.
20. Geben Sie `#D` ein oder wählen Sie den Modifikator in der Auswahlliste **Modifikatoren**.
21. Überprüfen Sie, ob das Text-Overlay angezeigt wird, wenn ein Fahrzeug in der Live-Ansicht in den Interessensbereich einfährt.

Anwendungsfall Einfahrt und Ausfahrt von Fahrzeugen

In diesem Anwendungsfall gleicht die Anwendung das von der Kamera erfasste Fahrzeugkennzeichen mit einer in der Kamera gespeicherten Liste berechtigter oder nicht berechtigter Kennzeichen ab.

In diesem Anwendungsfall muss die Anwendung in eine Kamera mit E/A-Unterstützung oder einem angeschlossenen E/A-Relaismodul zum Öffnen und Schließen der Schranke integriert sein.



Zwei Einrichtungsmöglichkeiten für den Anwendungsfall Einfahrt und Ausfahrt von Fahrzeugen

1 *Axis Kamera mit AXIS License Plate Verifier*
2 *E/A-Kommunikation*
3 *Schranke*
4 *E/A-Relaismodul von Axis*
5 *IP-Kommunikation*

Eine Schranke für bekannte Fahrzeuge mittels eines Relaismoduls öffnen

In diesem Anwendungsbeispiel wird erklärt, wie AXIS License Plate Verifier zusammen mit einem Relaismodul eingerichtet wird, um eine Schranke für ein bekanntes Fahrzeug zu öffnen, das durch eine bestimmte Region of Interest (ROI) in, sagen wir, einen Parkplatz fährt.

Erforderlich:

- Physisch installierte und an das Netzwerk angeschlossene Kamera.
- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
- Die Kabel zwischen Schranke und Relaismodul sind angeschlossen.
- Die Grundeinstellungen wurden vorgenommen. Siehe *Grundeinstellungen auf Seite 5*.

1. Wechseln Sie zu die Webseite der Kamera, wählen Sie **Einstellungen** und öffnen Sie AXIS License Plate Verifier.
2. Die Webseite des Relaismoduls aufrufen und sicherstellen, dass der Relaisport an den E/A-Port der Kamera angeschlossen ist.
3. Kopieren Sie die IP-Adresse des Relaismoduls.

4. Gehen Sie zurück zu AXIS License Plate Verifier.
5. Wechseln Sie zu **Settings (Einstellungen) > Access control (Zutrittskontrolle)**.
6. Wechseln Sie zu **Type (Typ)** und wählen Sie in der Auswahlliste **Relay (Relais)**.
7. Wählen Sie in der Auswahlliste **E/A-Ausgang** den an die Schranke angeschlossenen E/A-Port aus.
8. Wählen Sie in der Auswahlliste **SchrankenmodusÜber Listen öffnen** und überprüfen Sie dann die **Freigabeliste**.
9. Wählen Sie in der Auswahlliste **FahrzeugrichtungEinfahrt**.
10. Legen Sie über die Auswahlliste **ROI** den ausgewählten Bereich fest, der die Fahrspur abdeckt.
11. Geben Sie folgende Informationen ein:
    - die IP-Adresse des Relaismoduls im Format `192.168.0.0`
    - den Benutzernamen für das Relaismodul
    - das Kennwort für das Relaismodul
12. Um die Verbindung zu überprüfen, klicken Sie auf **Connect (Verbinden)**.
13. Um die Verbindung zu aktivieren, klicken Sie auf **Integration einschalten**.
14. Wechseln Sie zu die Registerkarte **Listenverwaltung**.
15. Geben Sie das Fahrzeugkennzeichen in das Feld **Freigabeliste** ein.

Hinweis

Die physischen Eingangsanschlüsse 1 bis 8 am Relaismodul entsprechen den Eingangsanschlüssen 1 bis 8 in der Auswahlliste. Hinweis: Die Relaisports 1 bis 8 am Relaismodul entsprechen den Ports 9 bis 16 in der Auswahlliste. Dies ist selbst dann der Fall, wenn das Relaismodul nur über 8 Ports verfügt.

16. Überprüfen Sie, ob die Anwendung das Fahrzeugkennzeichen in der Freigabeliste als bekanntes Fahrzeug identifiziert und die Schranke wie erwartet öffnet.

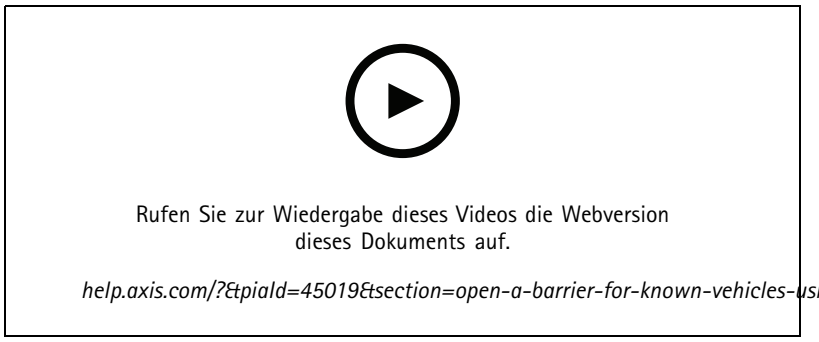
Eine Schranke für bekannte Fahrzeuge mittels des E/A der Kamera öffnen

In diesem Beispiel wird das Einrichten von AXIS License Plate Verifier zum Öffnen einer Schranke für bekannte Fahrzeuge, die z. B. auf einen Parkplatz fahren, über den E/A-Port der Kamera erläutert.

Anforderungen:

- Eine physisch installierte und an das Netzwerk angeschlossene Kamera.
- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
- Kabel zwischen Schranke und E/A-Port der Kamera angeschlossen.
- Grundeinstellungen vorgenommen. Siehe *Grundeinstellungen auf Seite 5*.

Anwendungsfall Einfahrt und Ausfahrt von Fahrzeugen



Eine Schranke für bekannte Fahrzeuge mittels des E/A der Kamera öffnen

1. Wechseln Sie zu die Webseite der Anwendung, wählen Sie die Registerkarte **Ereignisprotokoll** und fügen Sie die entsprechenden Fahrzeugkennzeichen einer Liste hinzu. Siehe *Erfasstes Fahrzeugkennzeichen der Liste hinzufügen auf Seite 15*.
2. Um die Listen direkt zu bearbeiten, Wechseln Sie zur Registerkarte **List management (Listenverwaltung)**.
3. Geben Sie die zugelassenen Fahrzeugkennzeichen in das Feld **Freigabeliste** ein.
4. Wechseln Sie zur Registerkarte **Settings (Einstellungen)**.
5. Wählen Sie unter **Zutrittskontrolle** in der Auswahlliste **Typ** die Option **Interner E/A**.
6. Wählen Sie die **E/A-Ausgangsnr.**.
7. Wählen Sie in der Auswahlliste **SchrankenmodusÜber Listen öffnen** und überprüfen Sie dann die **Freigabeliste**.
8. Wählen Sie in der Auswahlliste **FahrzeugrichtungEinfahrt**.
9. Wählen Sie in der Auswahlliste **ROI** den in Frage kommenden ausgewählten Bereich oder wählen Sie alle Bereiche.
10. Überprüfen Sie, ob die Anwendung das Fahrzeugkennzeichen in der Freigabeliste als bekanntes Fahrzeug identifiziert und die Schranke wie erwartet öffnet.

Hinweis

Sie können den Namen jeder einzelnen Liste so ändern, dass dieser Ihrem speziellen Anwendungsfall entspricht.

Über ein nicht autorisiertes Fahrzeug benachrichtigt werden

In diese Beispiel wird erläutert, welche Einstellungen in der Anwendung vorzunehmen sind, um in der Kamera ein Ereignis zu erstellen, das eine Benachrichtigung auslöst.

Anforderungen:

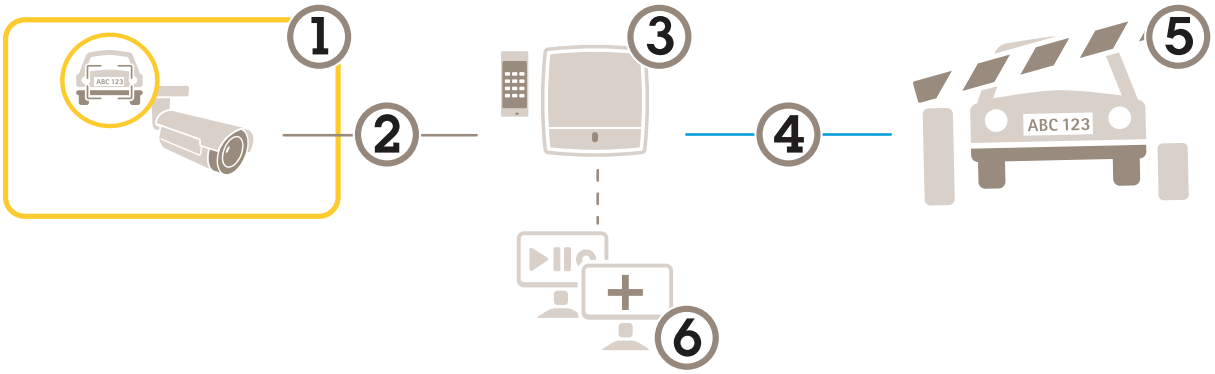
- Die Grundeinstellungen wurden vorgenommen. Siehe *Grundeinstellungen auf Seite 5* .

1. Wechseln Sie zu **List management (Listenverwaltung)**.
2. Geben Sie das Fahrzeugkennzeichen in das Feld **Sperrliste** ein.
3. Wechseln Sie zu die Webseite der Kamera.
4. Wechseln Sie zu **Einstellungen** > **Ereignisse** und erstellen Sie eine Aktionsregel, wobei die Anwendung als Bedingung und die Benachrichtigung als Aktion einzugeben ist.
5. Überprüfen, ob die Anwendung das hinzugefügte Fahrzeugkennzeichen als nicht berechtigt identifiziert und die Aktionsregel erwartungsgemäß angewendet wird.

Anwendungsfall Zufahrtskontrolle für Fahrzeuge

In diesem Anwendungsfall der Zufahrtskontrolle kann die Anwendung an eine Netzwerk-Türsteuerung von Axis angeschlossen werden und mithilfe von Zufahrtsregeln und Zeitplänen für Zufahrtszeiten nicht nur den Fahrzeugverkehr der Mitarbeiter sondern auch den der Besucher Lieferanten einfach verwalten.

Als Absicherung ein Zugangssystem mit Türsteuergerät und Kartenlesegerät einsetzen. Zum Einrichten des Türsteuergeräts und des Kartenlesegeräts, siehe die Benutzerdokumentation auf *axis.com*



1 *Axis Kamera mit AXIS License Plate Verifier*
2 *IP-Kommunikation*
3 *Axis Netzwerk-Türcontroller mit Kartenlesegerät*
4 *E/A-Kommunikation*
5 *Schranke*
6 *Optionale Software anderer Hersteller*

Mit einer Türsteuerung verbinden

In diesem Beispiel wird die Kamera an eine Netzwerk-Türsteuerung angeschlossen. Sie wird also als Sensor eingesetzt. Die Kamera sendet die Informationen an die Steuerung, die diese dann analysiert und entsprechende Ereignisse auslöst.

Hinweis

Um auf alle Parameter zugreifen zu können, beim Wechsel zwischen AXIS License Plate Verifier und AXIS Entry Manager die Webseiten aktualisieren.

Erforderlich:

- Die Kamera und die Türsteuerung sind physisch installiert und an das Netzwerk angeschlossen
- AXIS License Plate Verifier ist auf dem aktuellen Stand und ist auf dem aktuellen Stand und wird auf der Kamera ausgeführt.
- Grundeinstellungen vorgenommen. Siehe *Grundeinstellungen auf Seite 5*.

Anwendungsfall Zufahrtskontrolle für Fahrzeuge

So nehmen Sie die Anwendung mit AXIS A1001 Door Controller in Betrieb.

Hardwarekonfiguration in AXIS Entry Manager

1. AXIS Entry Manager aufrufen und unter **Setup** eine neue Hardwarekonfiguration starten.
2. In der Hardwarekonfiguration die Netzwerk-Türsteuerung umbenennen auf „Eingangssteuerung".
3. **Next (Weiter)** anklicken.
4. In **Configure locks connected to this controller (An diese Steuerung angeschlossene Schlösser konfigurieren)** die Option **Door monitor (Türmonitor)** deaktivieren.
5. **Next (Weiter)** anklicken.
6. In **Configure readers connected to this controller (An diese Steuerung angeschlossene Lesegeräte konfigurieren)** die Option **Exit reader (Ausgangslesegerät)** deaktivieren.
7. **Finish (Fertigstellen)** anklicken.

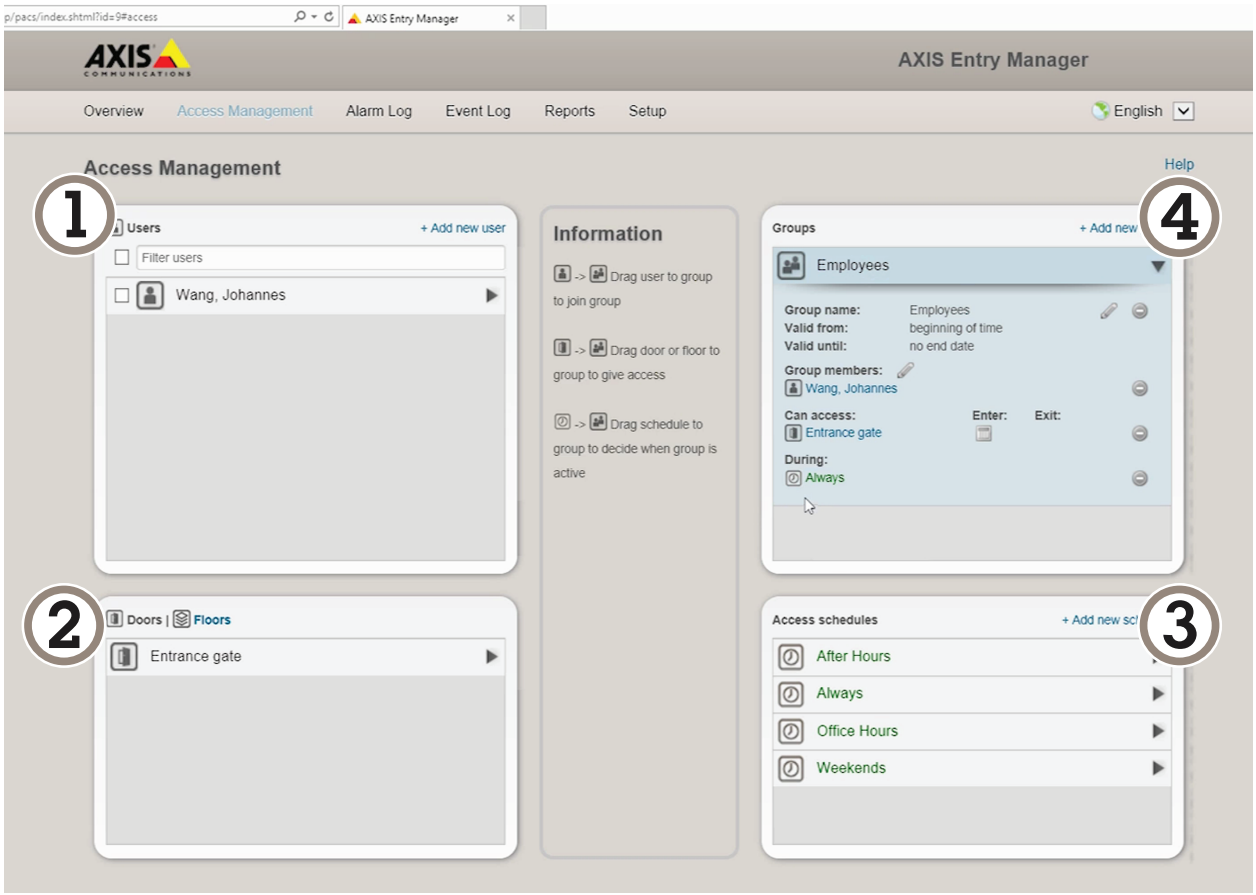
Konfiguration in AXIS License Plate Verifier

1. Wechseln Sie zur Webseite von AXIS License Plate Verifier.
2. Wechseln Sie zu **Settings (Einstellungen) > Access control (Zutrittskontrolle)**.
3. Wechseln Sie zu **Type (Typ)** und wählen Sie in der Auswahlliste **Controller**.
4. Geben Sie folgende Informationen ein:
   - die IP-Adresse des Controllers im Format `192.168.0.0`
   - den Benutzernamen für die Steuerung
   - das Kennwort für die Steuerung
5. Klicken Sie auf **Connect (Verbinden)**.
6. Bei erfolgreichem Verbindungsaufbau wird im Aufklappmenü **Network Door Controller name (Bezeichnung der Netzwerktürsteuerung)** „Eingangssteuerung" angezeigt. „Eingangssteuerung" wählen.
7. Im Aufklappmenü **Reader name (Bezeichnung des Lesegeräts)** das an die Türsteuerung „Eingangssteuerung" angeschlossene Lesegerät auswählen, zum Beispiel „Eingangslesegerät". Die Namen lassen sich in AXIS Entry Manager ändern.
8. Um die Verbindung zu aktivieren, wählen Sie **Turn on integration (Integration einschalten)**.
9. Geben Sie das Fahrzeugkennzeichen eines Benutzers in das Testfeld ein oder verwenden Sie die Standardeinstellungen und klicken Sie auf **Test integration (Integration testen)**. Überprüfen, ob der Test erfolgreich abgeschlossen wurde.

Benutzer, Gruppen, Türen und Zeitpläne in AXIS Entry Manager konfigurieren

1. Rufen Sie AXIS Entry Manager auf.
2. Wechseln Sie zu **Access Management (Zutrittsverwaltung)**.

3. Wechseln Sie zu **Doors > Add identification type** (Türen > Identifizierungstyp hinzufügen).
4. Wählen Sie in der Auswahlliste **Erforderliche Berechtigungsnachweise** die Option **Nur Fahrzeugkennzeichen**.
5. Um Nutzungszeiten für die Identifikationsart vorzugeben, legen Sie für die Tür per Drag and Drop einen **Zeitplan** fest.
6. Fügen Sie Benutzer hinzu sowie für jeden Benutzer den Berechtigungsnachweis **Fahrzeugkennzeichen**.
7. Klicken Sie erneut auf **Berechtigungsnachweis hinzufügen** und geben Sie das Fahrzeugkennzeichen ein.
8. Klicken Sie auf **Neue Gruppe hinzufügen** und geben Sie die entsprechenden Informationen ein.
9. Um einer Gruppe Benutzer hinzuzufügen, ziehen Sie per Drag and Drop **Benutzer** in die Benutzergruppe.
10. Um Benutzern Zutritt zu gewähren, ziehen Sie per Drag and Drop die **Tür** in die Benutzergruppe.
11. Um Zutrittszeiten vorzugeben, ziehen Sie per Drag and Drop einen **Zeitplan** in die Benutzergruppe.



Übersicht über die Benutzeroberfläche von AXIS Entry Manager.

1 *Benutzer*
2 *Türen*
3 *Zeitpläne*
4 *Benutzergruppen*

Verknüpfung mit AXIS Secure Entry

Dieses Beispiel beschreibt, wie Sie eine Axis Türsteuerung in AXIS Camera Station und AXIS Secure Entry mit AXIS Licence Plate Verifier verknüpfen.

Erforderlich:

- Kamera und Türsteuerung fertig installiert und mit dem Netzwerk verbunden.
- AXIS License Plate Verifier ist auf dem aktuellen Stand und wird auf der Kamera ausgeführt.
- AXIS Camera Station Client Version 5.49.449 oder höher.
- Die Grundeinstellungen wurden vorgenommen. Siehe *Grundeinstellungen auf Seite 5*.

AXIS Camera Station: siehe *Leser hinzufügen*.

AXIS License Plate Verifier:

1. Wechseln Sie zu der Registerkarte **Settings (Einstellungen)** zu **Configuration wizard (Konfigurationsassistent)**, und klicken Sie auf **Start**.
2. Wählen Sie die Option **Access Control (Zutrittskontrolle)**.
3. Wählen Sie Option **Secure Entry (Sicherer Zugang)**, and click **Next**.

AXIS Camera Station:

4. Geben Sie die in der Geräteliste unter **AXIS Camera Station > Configuration > Other Devices (AXIS Camera Station > Konfiguration > Andere Geräte)** angegebene IP-Adresse der Türsteuerung ein.
5. Wechseln Sie zu **AXIS Camera Station > Configuration > Encrypted communication (AXIS Camera Station > Konfiguration > Verschlüsselte Kommunikation)**, um einen Authentifizierungsschlüssel hinzufügen.
6. Wechsel Sie zu **External Peripheral Authentication Key (Authentifizierungsschlüssel für externe Peripheriegeräte)**, und klicken Sie auf **Show authentication key (Authentifizierungsschlüssel anzeigen)**.
7. Klicken Sie auf **Copy key (Schlüssel kopieren)**.

AXIS License Plate Verifier:

8. Gehen Sie im Konfigurationsassistenten zu **Authentifizierungsschlüssel** und fügen sie dort den kopierten Schlüssel ein.
9. Klicken Sie auf **Connect (Verbinden)**.
10. Wählen Sie im Auswahlmenü unter **Türsteuerung** die gewünschte Türsteuerung.
11. Wählen Sie im Auswahlmenü unter **Name des Lesers** den gewünschten Leser.
12. Aktivieren Sie die Option **Turn on integration (Integration aktivieren)**.
13. Klicken Sie auf **Next (Weiter)**.
14. Passen Sie den ausgewählten Bereich an. Siehe hierzu *Passen Sie den ausgewählten Bereich an auf Seite 11*.
15. Doppelklicken Sie auf **Next (Weiter)** und dann auf **Finish (Fertigstellen)**.

Integration

Profile verwenden, um Ereignisse auf mehrere Server zu übertragen

Mit Profilen können Sie ein Ereignis mit unterschiedlichen Protokollen gleichzeitig an verschiedene Server übertragen. Profile verwenden:

1. Wählen Sie ein Profil aus dem Drop-Down Menü **Profiles (Profile)**.
2. Regel konfigurieren Siehe *Ereignisinformationen an die Software anderer Hersteller per Push senden auf Seite 27*.
3. Klicken Sie auf Save (Speichern).
4. Wählen Sie ein neues Profil aus dem Drop-Down Menü **Profiles (Profile)**.

Ereignisinformationen an die Software anderer Hersteller per Push senden

Hinweis

Die Anwendung sendet die Ereignisinformationen im Format JSON. Für weitere Informationen *melden Sie sich mit Ihrem MyAxis Konto an*, rufen Sie die *AXIS VAPIX-Bibliothek* auf und wählen Sie AXIS License Plate Verifier.

Mit dieser Funktion lässt sich Software anderer Hersteller integrieren. Dabei werden die Ereignisdaten per Push mittels TCP oder HTTP POST übertragen.

Bevor Sie beginnen:

- Die Kamera muss physisch installiert und an das Netzwerk angeschlossen sein.
- AXIS License Plate Verifier muss auf dem aktuellen Stand sein und auf der Kamera ausgeführt sein.

1. Wechseln Sie zu **Integration** > **Push events (Ereignisse per Push senden)**.
2. Aus dem Aufklappmenü **Protocol (Protokoll)** eines der folgenden Protokolle auswählen:
   - TCP
   - HTTP POST
   - Geben Sie den Benutzernamen und das Kennwort ein.
3. Geben Sie in das Feld **Server URL** die Server-Adresse und den Port im folgenden Format ein: `127.0.0.1:8080`
4. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein oder lassen Sie den vorgegebenen Namen stehen.
5. Wählen Sie unter **Ereignistypen** eine oder mehrere der folgenden Optionen:
   - **New (Neu)** steht für die Ersterkennung eines Fahrzeugkennzeichens.
   - **Update (Aktualisierung)** ist entweder eine Korrektur eines Zeichens auf einem zuvor erkannten Kennzeichen oder wenn eine Richtung erkannt wird, während sich das Kennzeichen bewegt und über das Bild verfolgt wird.
   - **Lost (Verloren)** ist das letzte verfolgte Ereignis des Kennzeichens, bevor es das Bild verlässt. Es enthält auch die Richtung des Kennzeichens.
6. Um die Funktion zu aktivieren, **Send event data to server (Ereignisdaten an Server senden)** auswählen.
7. Um beim Verwenden von HTTP POST die Bandbreite zu verringern, können Sie die Option **Do not to send images through HTTP POST (Keine Bilder über HTTP POST senden)** wählen.
8. Klicken Sie auf **Save (Speichern)**.

Hinweis

Um Ereignisse per HTTP POST zu übertragen, können Sie anstelle eines Benutzernamens und Kennworts eine Autorisierungsleiste verwenden. Gehen Sie zum Feld **Auth-Header (Autorisierungsleiste)** und fügen Sie einen Pfad zu einer Authentifizierungs-API hinzu.

Bilder von Fahrzeugkennzeichen an einen Server senden

Über diese Funktion können Sie Bilder der Fahrzeugkennzeichen über FTP auf einen Server übertragen.

Bevor Sie beginnen:

- Die Kamera muss physisch installiert und an das Netzwerk angeschlossen sein.
- AXIS License Plate Verifier muss auf dem aktuellen Stand sein und auf der Kamera ausgeführt sein.

1. Gehen Sie zu **Integration** > **Ereignisse per Push senden**.
2. Wählen Sie in der Auswahlliste **Protokoll** die Option **FTP**.
3. Geben Sie in das Feld **Server-URL** die Server-Adresse im folgenden Format ein: `ftp://10.21.65.77/LPR`.
4. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein. Für die Bilder wird ein Ordner mit diesem Namen erstellt. Bilder werden im folgenden Format erstellt: timestamp_area of interest_direction_carID_license plate text_country.jpg.
5. Geben Sie den Benutzernamen und das Kennwort für den FTP-Server ein.
6. Wählen Sie die Pfad- und Namensmodifikatoren für die Dateinamen aus.
7. Klicken Sie auf **Done (Fertig)**.
8. Unter **Event types (Ereignistypen)** eine oder mehrere der folgenden Optionen wählen:
   - **New (Neu)** steht für die Ersterkennung eines Fahrzeugkennzeichens.
   - **Update (Aktualisierung)** ist entweder eine Korrektur eines Zeichens auf einem zuvor erkannten Kennzeichen oder wenn eine Richtung erkannt wird, während sich das Kennzeichen bewegt und über das Bild verfolgt wird.
   - **Verloren** ist das letzte verfolgte Ereignis des Fahrzeugkennzeichens, bevor es das Bild verlässt. Es enthält auch die Richtung des Kennzeichens.

   Hinweis

   Die Richtung ist nur im Dateinamen enthalten, wenn **Verloren** oder **Aktualisieren** ausgewählt wurde.
9. Um die Funktion zu aktivieren, wählen Sie **Ereignisdaten an Server senden**.
10. Klicken Sie auf **Save (Speichern)**.

Hinweis

Beachten Sie, dass das Bild je nach ausgewähltem Aufnahmemodus anders aussehen kann, siehe *Bilderfassungseinstellungen anpassen auf Seite 12*.

Hinweis

Wenn Push-Ereignisse fehlschlagen, sendet die App die ersten fehlgeschlagenen Ereignisse (bis zu 100) erneut an den Server. Bei der Verwendung von FTP für Push-Ereignisse an einen Windows-Server sollten Sie %c nicht zur Benennung von Bildern nutzen, die Datum und Uhrzeit enthalten. Dies liegt daran, dass Windows die durch die Funktion %c für Datum und Uhrzeit eingestellte Benennung nicht akzeptiert. Beachten Sie, dass dies bei der Verwendung eines Linux-Servers kein Problem ist.

Direkte Integration mit 2N

In diesem Beispiel wird die direkte Integration mit einem 2N-IP-Gerät beschrieben.

Richten Sie ein Konto auf Ihrem 2N-Gerät ein:

1. Gehen Sie zu 2N IP Verso.
2. Gehen Sie zu **Dienste** > **HTTP-API** > **Konto 1**.
3. Wählen Sie **Konto aktivieren**.
4. Wählen Sie **Zugriff auf Kamera**.
5. Wählen Sie **Fahrzeugkennzeichenerkennung**.
6. Kopieren Sie die IP-Adresse.

In der App AXIS License Plate Verifier:

1. Gehen Sie zu **Integration** > **Direkte Integration**.
2. Fügen Sie dem 2N-Gerät die IP-Adresse oder URL hinzu.
3. Wählen Sie **Verbindungstyp**.
4. Wählen Sie, wofür die **Schranke verwendet wird**.
5. Geben Sie Ihren Benutzernamen und das Kennwort ein.
6. Klicken Sie auf **Integration aktivieren**.
7. Klicken Sie auf **Save (Speichern)**.

So überprüfen Sie, ob die Integration funktioniert:

1. Gehen Sie zu 2N IP Verso.
2. Gehen Sie zu **Status** > **Ereignisse**.

Integration in das Genetec Security Center

Dieses Beispiel beschreibt die direkte Integration in das Genetec Security Center.

Im Genetec Security Center:

1. Gehen Sie zu **Übersicht**.
2. Stellen Sie sicher, dass **Datenbank**, **Verzeichnis** und **Lizenz** online sind. Ist dies nicht der Fall, führen Sie alle Genetec- und SQLEXPRESS-Dienste unter Windows ausführen.
3. Gehen Sie zu **Konfigurationstool für Genetec > Plugins**.
4. Klicken Sie auf **Entität hinzufügen**.
5. Gehen Sie zu **Plugin** und wählen Sie **LPR-Plugin**.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie auf **Weiter**.
9. Wählen Sie das hinzugefügte LPR-Plugin und gehen Sie zu **Datenquellen** .

Unter **ALPR liest API**:

10. Markieren Sie **Aktiviert**.

11. Geben Sie in **Name** Folgendes ein: **Plugin REST API**.
12. Geben Sie im **API-Pfadpräfix** Folgendes ein: **lpr**.
13. Wählen Sie in **REST-Port443**.
14. Geben Sie im **WebSDK-Host** Folgendes ein: **localhost**.
15. Wählen Sie im **WebSDK-Port443**.
16. Markieren Sie **Selbstsignierte Zertifikate zulassen**.

Unter **Datenquelle für Security Center-Ereignisse**:

17. Markieren Sie **Aktiviert**.
18. Geben Sie in **NameSecurity Center Lpr-Ereignisse** ein.
19. Wählen Sie unter im Auswahlmenü unter **Verarbeitungsfrequenz** die Option **5 Sek.**.
20. Wechseln Sie zur Registerkarte **Data sinks (Datensenken)**.
21. Klicken Sie auf **+**.
22. Wählen Sie als **Typ** die Option **Datenbank**.
23. **Datenbank auswählen und konfigurieren:**.
    - Markieren Sie **Aktiviert**.
    - Markieren Sie in **Quelle** die Optionen **REST-API des Plugin** und **Native ALPR-Ereignisse**.
    - Geben Sie in **NameLese-DB** ein.
    - Markieren Sie unter **Einschließen** die Optionen **Lesen**, **Treffer** und **Bilder**.
    - Wechseln Sie zur Registerkarte **Resources (Ressourcen)**.
    - Klicken Sie auf **Datenbank löschen** und dann auf **Datenbank erstellen**.

API-Benutzer erstellen:

24. Wechseln Sie zu **Config Tool > User Management (Konfigurationstool >Benutzerverwaltung)**.
25. Klicken Sie auf **Entität hinzufügen**.
26. Wählen Sie **Benutzer**.
27. Geben Sie einen Benutzernamen und ein Kennwort ein. Lassen Sie die anderen Felder unverändert.
28. Wählen Sie den hinzugefügten Benutzer aus, und wechseln Sie zur Registerkarte **Privileges (Berechtigungen)**.
29. Markieren Sie diese Option, um alles unter **Anwendungsberechtigungen** zu erlauben.
30. Markieren Sie diese Option, **Drittanbieter-ALPR liest API** zu erlauben.
31. Klicken Sie auf **Apply (Übernehmen)**.

In der App **AXIS License Plate Verifier**:

1. Wechseln Sie zur Registerkarte **Integration**.
2. Wählen Sie in der Auswahlliste **Genetec Security Center**.
3. Geben Sie in **URL/IP** Ihre Adresse gemäß dieser Vorlage ein: `https://server-address/api/V1/lpr/lpringestion/reads`.

4. Geben Sie Ihren Genetec-Benutzernamen und das Kennwort ein.
5. Klicken Sie auf **Integration aktivieren**.
6. Gehen Sie zur Registerkarte **Einstellungen**.
7. Unter **Sicherheit > HTTPS**.
8. Wählen Sie je nach Einstellungen im Genetec Security Center **Selbstsigniert** oder **CA-signiert**.

Im Genetec Security Center:

1. Gehen Sie zu **Genetec Security Desk**.
2. Klicken Sie unter **Prüfung** auf **Lesen**.
3. Gehen Sie zur Registerkarte **Lesen**.
4. Filtern Sie das Ergebnis wie gewünscht.
5. Klicken Sie **Bericht erstellen**.

Hinweis

Sie können sich auch die Genetec-Dokumentation zum Integrieren von Plugins von Drittanbieter-ALPR durchlesen. *Das ist hier möglich (Registrierung erforderlich).*

Die Weboberfläche

Um die Weboberfläche des Geräts aufzurufen, müssen Sie die IP-Adresse des Geräts in einen Webbrowser eingeben.

Hinweis

Die in diesem Abschnitt beschriebenen Funktionen und Einstellungen werden von Gerät zu Gerät unterschiedlich unterstützt.

Dieses Symbol zeigt an, dass die Funktion oder Einstellung nur für einige Geräte verfügbar ist.

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Die Sprache ändern.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

- Informationen zum angemeldeten Benutzer.
- **Change account (Konto wechseln)**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
- **Log out (Abmelden)**: Melden Sie sich vom aktuellen Konto ab.

Das Kontextmenü enthält:

- **Analytics data (Analysedaten)**: Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.
- **Feedback**: Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.
- **Rechtliches**: Lassen Sie sich Informationen zu Cookies und Lizenzen anzeigen.
- **Info**: Lassen Sie sich Geräteinformationen anzeigen, einschließlich Firmwareversion und Seriennummer.
- **Legacy device interface (Frühere Benutzeroberfläche)**: Wechseln Sie zur früheren Weboberfläche des Geräts.

Status

Zeitsynchronisierungsstatus

Zeigt Informationen zur NTP-Synchronisierung an, z. B. ob das Gerät mit einem NTP-Server synchronisiert ist und wie lange es noch bis zur nächsten Synchronisierung dauert.

NTP settings (NTP-Einstellungen): Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Date and time (Datum und Uhrzeit)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich Firmwareversion und Seriennummer.

Upgrade firmware (Firmwareaktualisierung): Aktualisieren Sie die Firmware auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie eine Firmwareaktualisierung durchführen können.

RAM-Auslastung: Prozent des verwendeten RAM.

CPU-Auslastung: Prozent des verwendeten CPU.

GPU-Auslastung: Prozent des verwendeten GPU.

GPU-Busauslastung: Prozent des verwendeten GPU-Bus.

Dekodierung: Aktueller Status des Decodierungsvorgangs, *ausgeführt* oder *angehalten*.

IP-Adresse: Die IP-Adresse des Geräts.

Datum und Uhrzeit: Datum und Uhrzeit des Geräts.

Ongoing recordings (Laufende Aufzeichnungen)

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter *Aufzeichnungen auf Seite 46*

Anzeige des Speicherorts der Aufzeichnung.

Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

View details (Details anzeigen): Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port und PID/Process für jeden Client an.

Video

Klicken Sie darauf, um den Live-Videostream wiederzugeben.

Klicken Sie darauf, um den Live-Videostream einzufrieren.

Klicken Sie darauf, um vom Live-Videostream eine Momentaufnahme anzufertigen. Die Datei wird im Ordner Downloads des Rechners gespeichert. Die Bilddatei trägt den Namen [snapshot_JJJJ_MM_TT_HH_MM_SS.jpg]. Die tatsächliche Größe des Schnappschusses hängt von der Komprimierung ab, die von der Engine des jeweiligen Browsers angewendet wird, auf dem der Schnappschuss empfangen wird. Daher kann die Größe des Schnappschusses von der eigentlichen Komprimierungseinstellung abweichen, die im Axis Gerät konfiguriert ist.

Klicken Sie darauf, um sich die E/A-Ausgangsports anzeigen zu lassen. Verwenden Sie den Schalter, um den Schaltkreis eines Ports zu öffnen oder zu schließen, z. B. um Zusatzausrüstung zu testen.

Klicken Sie darauf, um die IR-Beleuchtung manuell ein- oder auszuschalten.

Klicken Sie darauf, um das sichtbare Weißlicht manuell ein- oder auszuschalten.

Klicken Sie darauf, um auf die Steuerelemente auf dem Bildschirm zuzugreifen:

- **Voreingestellte Steuerelemente**: Aktivieren Sie diese Option, um die auf dem Bildschirm verfügbaren Steuerelemente zu verwenden.
- **Benutzerdefinierte Steuerelemente**: Klicken Sie auf + **Benutzerdefinierte Steuerelemente** hinzufügen, um dem Bildschirm Steuerelemente hinzuzufügen.

Startet die Waschanlage. Zu Beginn der Abfolge wird die Kamera in die Waschposition gefahren. Nach Abschluss der Abfolge wird die Kamera in ihre vorherige Position zurückgefahren. Dieses Symbol wird nur angezeigt, wenn die Waschanlage angeschlossen und konfiguriert ist.

Startet den Wischer.

Klicken Sie und wählen Sie eine vordefinierte Position aus, um zu dieser vordefinierten Position in der Live-Ansicht zu wechseln. Oder klicken Sie auf **Setup**, um zur Seite mit der vordefinierten Position zu wechseln.

Fügt einen Fokusabrufbereich hinzu oder entfernt diesen. Bei Hinzufügen eines Fokusabrufbereichs speichert die Kamera die Fokuseinstellungen des spezifischen Schwenk-/Neigungsbereichs. Wenn die Kamera sich in der Live-Ansicht in einen als Fokusabrufbereich definierten Bereich begibt, dann ruft die Kamera die gespeicherten Fokusdaten ab. Es muss lediglich die Hälfte des Bereichs abgedeckt werden, um die Fokusdaten abzurufen.

Klicken Sie, um eine Guard-Tour auszuwählen, und klicken Sie dann auf **Start**, um die Guard-Tour wiederzugeben. Oder klicken Sie auf **Setup**, um zur Seite mit der Guard-Tour Position zu wechseln.

Klicken Sie darauf, um für einen ausgewählten Zeitraum die Heizung manuell einzuschalten.

Klicken Sie darauf, um die ständige Aufzeichnung eines Live-Videostreams zu starten. Klicken Sie erneut, um die Aufzeichnung anzuhalten. Wenn eine Aufzeichnung läuft, wird sie nach einem Neustart automatisch fortgesetzt.

Klicken Sie darauf, um sich den für das Gerät konfigurierten Speicher anzeigen zu lassen. Melden Sie sich als Administrator an, um den Speicher zu konfigurieren.

Klicken Sie darauf, um auf weitere Einstellungen zuzugreifen:

- **Video format (Videoformat)**: Wählen Sie das Codierungsformat aus, das in der Live-Ansicht verwendet werden soll.
- **Client stream information (Informationen über den Client-Stream)**: Aktivieren Sie diese Option, um dynamische Informationen über den vom Browser zur Anzeige der Live-Ansicht verwendeten Videostream anzuzeigen. Die Bitrate-Informationen unterscheiden sich aufgrund unterschiedlicher Informationsquellen von den in einem Text-Overlay angezeigten Informationen. Die Bitrate in den Informationen zum Clientstream ist die Bitrate der letzten Sekunde und stammt vom Codierungstreiber des Geräts. Die Bitrate im Overlay ist die durchschnittliche Bitrate der letzten 5 Sekunden und stammt vom Browser. Beide Werte decken nur den Rohvideostream ab und nicht die zusätzliche Bandbreite, die bei der Übertragung über das Netzwerk via UDP/TCP/HTTP erzeugt wird.
- **Adaptiver Videostream**: Aktivieren Sie diese Option, um die Bildauflösung zur Erhöhung der Benutzerfreundlichkeit an die tatsächliche Bildschirmauflösung des Clients anzupassen und eine mögliche Überlastung der Client-Hardware zu vermeiden. Der adaptive Videostream wird nur eingesetzt, wenn die Wiedergabe des Live-Videostreams über die Weboberfläche in einem Browser erfolgt. Wenn adaptiver Videostream aktiviert ist, beträgt die maximale Bildrate 30 Bilder pro Sekunde. Wenn Sie bei aktiviertem adaptivem Stream eine Momentaufnahme erstellen, wird die vom adaptiven Videostream ausgewählte Bildauflösung verwendet.

- **Nivellierraster**: Klicken Sie auf , um sich das Nivellierraster anzeigen zu lassen. Mithilfe des Rasters können Sie entscheiden, ob das Bild horizontal ausgerichtet ist. Klicken Sie auf , um es auszublenden.
- **Pixel counter (Pixelzähler)**: Klicken Sie auf , um den Pixelzähler anzuzeigen. Das Feld auf den ausgewählten Bereich platzieren und die Größe durch Ziehen anpassen. Die Größe des Felds in Pixeln lässt sich auch über die Felder **Width (Breite)** und **Height (Höhe)** definieren.
- **Refresh (Aktualisieren)**: Klicken Sie auf , um das Standbild der Live-Ansicht zu aktualisieren.
- **PTZ-Steuerelemente** : Aktivieren Sie diese Ansicht, um die PTZ-Steuerelemente in der Live-Ansicht anzuzeigen.

1:1 Klicken Sie darauf, um sich die Live-Ansicht mit voller Auflösung anzeigen zu lassen. Wenn die volle Auflösung größer als die Bildschirmgröße ist, navigieren Sie unter Verwendung des kleineres Bilds im Bild.

Klicken Sie darauf, um sich den Live-Videostream im Vollbildmodus anzeigen zu lassen. Drücken Sie DIE ABBRUCHTASTE, um den Vollbildmodus zu verlassen.

Installation

Capture mode (Aufnahmemodus) : Ein Aufnahmemodus ist eine voreinstellte Konfiguration, um festzulegen, wie die Kamera Bilder aufnehmen soll. Eine Änderung des Aufnahmemodus kann sich auf viele anderen Einstellungen, wie Sichtbereiche und Privatzonenmasken, auswirken.

Mounting position (Montageposition) : Die Bildausrichtung kann sich je nach Installation der Kamera ändern.

Power line frequency (Netzfrequenz): Wählen Sie die in Ihrer Region verwendete Frequenz aus, um Bildflimmern zu minimieren. In Amerika wird in der Regel eine Frequenz von 60 Hz verwendet. Auf allen anderen Kontinenten wird in der Regel eine Frequenz von 50 Hz verwendet. Wenden Sie sich bei Fragen zur Netzfrequenz an Ihr Stromversorgungsunternehmen.

Drehen: Wählen Sie die bevorzugte Bildausrichtung aus.

Zoom: Stellen Sie mithilfe des Schiebereglers die Zoomstufe ein.

Focus (Fokus): Stellen Sie mithilfe des Schiebereglers den Fokus manuell ein.

AF: Klicken Sie auf diese Option, damit sich die Kamera selbsttätig auf den ausgewählten Bereich fokussiert. Wird kein Autofokus-Bereich gewählt, fokussiert die Kamera auf die ganze Szene.

Autofokusbereich: Klicken Sie auf , um den Autofokusbereich zu sehen. Dieser Bereich sollte der ausgewählte Bereich sein.

Reset focus (Fokus zurücksetzen): Klicken Sie darauf, um den Fokus an die Originalposition zurückkehren zu lassen.

Hinweis

In kalten Umgebungen kann es einige Minuten dauern, bis Zoom und Fokus verfügbar sind.

Bildkorrektur

Die Weboberfläche

Wichtig

Wir raten davon ab, mehrere Funktionen zur Bildkorrektur gleichzeitig zu verwenden, da dies zu Leistungsproblemen führen kann.

Barrel distortion correction (BDC) (Korrektur der Tonnenverzeichnung) : Aktivieren Sie diese Option, um bei Tonnenverzeichnung ein gerades Bild zu erhalten. Bei der Tonnenverzeichnung handelt es sich um einen Objektiveffekt, durch den das Bild nach außen gewölbt wirkt. Der Zustand ist besser zu erkennen, wenn aus dem Bild herausgezoomt wird.

Crop (Ausschneiden) : Stellen Sie mithilfe des Schiebereglers die Korrekturstufe ein. Bei einem niedrigeren Wert wird die Bildbreite zu Lasten der Höhe und Auflösung des Bildes beibehalten. Bei einem höheren Wert werden die Höhe und Auflösung des Bildes zu Lasten der Bildbreite beibehalten.

Remove distortion (Verzerrung entfernen) : Stellen Sie mithilfe des Schiebereglers die Korrekturstufe ein. Beim Zusammenziehen wird die Bildbreite zu Lasten der Höhe und Auflösung des Bildes beibehalten. Beim Aufblasen werden die Höhe und Auflösung des Bildes zu Lasten der Bildbreite beibehalten.

Bildstabilisierung : Aktivieren Sie diese Option für eine glattere und ruhigere Bildabfolge mit weniger Unschärfe. Wir empfehlen die Verwendung der Funktion Bildstabilisierungvon in Umgebungen, in denen das Gerät exponiert angebracht und Vibrationen, z. B. durch Wind oder Straßenverkehr, ausgesetzt ist.

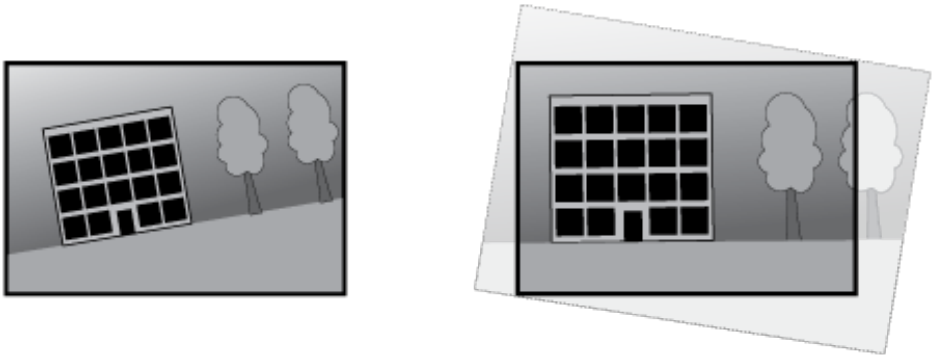
Focal length (Brennweite) : Passen Sie mithilfe des Schiebereglers die Brennweite an. Ein höherer Wert führt zu einer höheren Vergrößerung mit einen engeren Blickwinkel, während ein niedrigerer Wert zu einer niedrigeren Vergrößerung mit einem breiterem Blickwinkel führt.

Stabilizer margin (Stabilisierungsmarge) : Mit dem Schieberegler die Größe der Stabilisierungsmarge festlegen. Diese legt das zu stabilisierende Vibrationsniveau fest. Wenn das Produkt in einer Umgebung mit vielen Vibrationen installiert ist, bewegen Sie den Schieberegler in Richtung **Max.**. Dadurch wird eine kleinere Szene erfasst. Bewegen Sie den Schieberegler in Richtung **Min.** bei weniger Vibrationen.

Straighten image (Bild ausrichten) : Aktivieren Sie diese Option und richten Sie mithilfe des Schiebereglers das Bild durch Drehen gerade aus und schneiden es digital zu. Die Funktion ist hilfreich, wenn es die Kamera bei der Installation nicht gerade ausgerichtet werden kann. Idealerweise sollte das Bild während der Installation gerade ausgerichtet werden.

: Klicken Sie darauf, um sich ein Unterstützungsraster im Bild anzeigen zu lassen.

: Klicken Sie darauf, um das Raster auszublenden.



Bild, bevor es gerade ausgerichtet wurde und danach.

Bild

Darstellung

Szeneprofil : Wählen Sie ein Szeneprofil für Ihr Überwachungsszenario aus. Ein Szene-Profil optimiert die Bildeinstellungen einschließlich Farbstufe, Helligkeit, Schärfe, Kontrast und lokaler Kontrast für eine bestimmte Umgebung oder zu einem bestimmten Zweck.

- **Forensisch**: Zu Überwachungszwecken geeignet.
- **Innenbereich** : Für den Innenbereich geeignet.
- **Außenbereich** : Für den Außenbereich geeignet.
- **Lebhaft**: Zu Demonstrationszwecken nützlich.
- **Verkehrsübersicht**: Für die Überwachung des Fahrzeugverkehrs geeignet.

Saturation (Sättigung): Stellen Sie mithilfe des Schiebereglers die Farbintensität ein. Sie können z. B. ein Bild in Graustufen erstellen.

Contrast (Kontrast): Passen Sie mithilfe des Schiebreglers den Unterschied zwischen hell und dunkel an.

Helligkeit: Stellen Sie mithilfe des Schiebereglers die Lichtstärke ein. Dadurch lassen sich Objekte leichter erkennen. Helligkeit wird nach der Bildaufnahme angewendet und hat keine Auswirkungen auf die Bilddaten. Um mehr Details aus dunklen Bereichen zu erhalten, ist es normalerweise besser, die Verstärkung oder die Belichtungszeit zu erhöhen.

Schärfe: Stellen mithilfe des Schiebereglers den Randkontrast ein, um Objekte in einem Bild schärfer darzustellen. Wenn Sie die Schärfe erhöhen, kann dies zu einer höherem Bitrate und einem höheren Bedarf an Speicherplatz führen.

Großer Dynamikbereich

WDR : Aktivieren Sie diese Option, um sowohl helle als auch dunkle Bereiche im Bild darzustellen.

Lokaler Kontrast : Stellen Sie mithilfe des Schiebereglers den Kontrast des Bildes ein. Bei einem höheren Wert wird der Kontrast zwischen dunklen und hellen Bereichen größer.

Farbtonzuordnung : Passen Sie mithilfe des Schiebereglers das auf das Bild angewendete Tone-Mapping an. Bei einem Korrekturwert von „0" erfolgt lediglich eine normale Gammakorrektur, ein größerer Wert erhöht dagegen die Sichtbarkeit der dunkelsten und hellsten Bildbereiche.

Weißabgleich

Wenn die Kamera die Farbtemperatur der Lichtquelle erfasst, kann sie das Bild so anpassen, dass die Farben natürlicher dargestellt werden. Sollte dies nicht ausreichen, können Sie eine geeignete Lichtquelle aus der Liste wählen.

Die Einstellung Automatischer Weißabgleich verringert durch allmähliches Anpassen das Risiko von Farbflimmern. Wenn die Beleuchtung geändert oder die Kamera das erste Mal hochgefahren wird, kann die Anpassung an die veränderten Lichtverhältnisse bis zu 30 Sekunden dauern. Befindet sich in einer Szene mehr als eine Art von Lichtquelle, also wenn sie sich in ihrer Farbtemperatur unterscheiden, dann wird die stärkere Lichtquelle als Bezugswert für den Algorithmus zum Ermitteln des Weißabgleichs verwendet. Dieses Verhalten kann übersteuert werden. Dazu wird ein fester Weißabgleichswert gewählt, welcher der als Bezugswert bevorzugten Lichtquelle entspricht.

Lichtverhältnisse:

- **Automatisch**: Automatisches Identifizieren und Ausgleichen der Lichtquellenfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen verwendet werden kann.
- **Automatisch – Außenbereiche** : Automatisches Identifizieren und Ausgleichen der Lichtquellenfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen im Außenbereich verwendet werden kann.
- **Benutzerdefiniert – Innenbereiche** : Fester Farbausgleichswert für Innenräume mit Kunstlichtquelle, ausgenommen fluoreszierendes Licht, und geeignet für normale Farbtemperaturen von etwa 2800 K.
- **Benutzerdefiniert – Außenbereiche** : Fester Farbausgleichswert für sonniges Wetter und eine Farbtemperatur von etwa 5.500 K.

- **Fest – Fluoreszierend 1**: Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 4000 K.
- **Fest – Fluoreszierend 2**: Fester Farbausgleichswert für fluoreszierendes Licht mit einer Farbtemperatur von etwa 3.000 K.
- **Fest – Innenbereich**: Fester Farbausgleichswert für Innenräume mit Kunstlichtquelle, ausgenommen fluoreszierendes Licht, und geeignet für normale Farbtemperaturen von etwa 2800 K.
- **Fest – Außenbereich 1**: Fester Farbausgleichswert für sonniges Wetter und eine Farbtemperatur von etwa 5.500 K.
- **Fest – Außenbereich 2**: Fester Farbausgleichswert für bewölktes Wetter und eine Farbtemperatur von etwa 6.500 K.
- **Street light – mercury (Straßenbeleuchtung – Quecksilber)** : Fester Farbausgleichswert zur Kompensation des ultravioletten Anteil von häufig als Straßenbeleuchtung eingesetzten Quecksilberdampfleuchten.
- **Street light – sodium (Straßenbeleuchtung – Natriumdampflampen)** : Fester Farbausgleichswert, der den Gelb-Gelbanteil von häufig als Straßenbeleuchtung eingesetzten Natriumdampfleuchten ausgleicht.
- **Aktuelle Einstellung beibehalten**: Behält die aktuelle Einstellung bei und nimmt keinen Lichtausgleich vor.
- **Manuell** : Legen Sie den Weißabgleich mit Hilfe eines weißen Objekts fest. Ziehen Sie dazu einem Kreis zu einem Objekt, das von der Kamera als weiß interpretiert werden soll (zum Beispiel ein weißes Blatt Papier) in die Mitte des Live-Bildes. Stellen Sie mit den Schiebereglern für **Rotabgleich** und **Blauabgleich** den Weißabgleich manuell ein.

Tag-/Nachtmodus

IR-Sperrfilter:

- **Auto**: Wählen Sie diese Option aus, damit sich der Infrarot-Filter automatisch ein- und ausschaltet. Wenn sich die Kamera im Tag-Modus befindet, wird der Infrarot-Sperrfilter eingeschaltet, der die eingehende IR-Beleuchtung blockiert. Im Nachtmodus wird der Infrarot-Sperrfilter ausgeschaltet und die Lichtempfindlichkeit der Kamera wird erhöht.
- **Ein**: Wählen Sie diese Option, um den Infrarot-Sperrfilter zu aktivieren. Das Bild ist in Farbe, aber mit verringerter Lichtempfindlichkeit.
- **Aus**: Wählen Sie diese Option, um den Infrarot-Sperrfilter zu deaktivieren. Das Bild wird schwarzweiß dargestellt und die Lichtempfindlichkeit erhöht.

Grenzwert: Stelle Sie mithilfe des Schiebereglers ein, bei welchem Lichtgrenzwert die Kamera vom Tag-Modus in den Nachtmodus wechseln soll.

- Verschieben Sie den Schieberegler in Richtung **Hell**, um den Grenzwert für den IR-Sperrfilter zu verringern. Die Kamera wechselt früher in den Nachtmodus.
- Verschieben Sie den Schiebregler in Richtung **Dunkel**, um den Grenzwert für den IR-Sperrfilter zu erhöhen. Die Kamera wechselt später in den Nachtmodus.

IR light (Infrarotlicht)

Wenn Ihr Gerät nicht über eine integrierte Beleuchtung verfügt, sind diese Steuerelemente nur verfügbar, wenn ein unterstützendes Axis Zubehör angeschlossen ist.

Allow illumination (Beleuchtung zulassen): Aktivieren Sie diese Option, damit die Kamera im Nachtmodus auf die integrierte Beleuchtung zurückgreift.

Beleuchtung synchronisieren: Aktivieren Sie diese Option, um die Beleuchtung automatisch mit dem Umgebungslicht zu synchronisieren. Die Tag/Nacht-Synchronisierung funktioniert nur, wenn der IR-Sperrfilter auf **Auto** oder **Aus** gestellt ist.

Automatic illumination angle (Automatischer Beleuchtungswinkel) : Aktivieren Sie diese Option, um den automatischen Beleuchtungswinkel zu verwenden.

Illumination angle (Beleuchtungswinkel) : Mithilfe des Schiebereglers können Sie den Beleuchtungswinkel manuell einstellen, z. B. wenn sich der Winkel vom Sichtwinkel der Kamera unterscheiden muss. Bei großem Sichtwinkel der Kamera kann der Beleuchtungswinkel kleiner (mehr teleobjektivartig) eingestellt werden. Dies führt zu dunklen Bildecken.

IR wavelength (Infrarot-Wellenlänge) : Wählen Sie die gewünschte Wellenlänge für das IR-Licht aus.

White light (Sichtbares Weißlicht) :

Allow illumination (Beleuchtung zulassen) : Aktivieren Sie Option, damit diese Kamera im Nachtmodus sichtbares Weißlicht verwenden kann.

Synchronize illumination (Beleuchtung synchronisieren) : Aktivieren Sie diese Option, um das sichtbare Weißlicht automatisch mit dem Umgebungslicht zu synchronisieren.

Exposure (Belichtung)

Wählen Sie einen Belichtungsmodus, sich rasch verändernde unregelmäßige Bildeffekte zu verringern, zum Beispiel durch unterschiedliche Lichtquellen verursachtes Flimmern. Wir empfehlen dem automatischen Belichtungsmodus oder dieselbe Frequenz wie Ihr Stromnetz.

Exposure mode (Belichtungsmodus):

- **Automatic (Automatisch)**: Die Kamera stellt Blende, Verstärkung und Verschlusszeit selbsttätig ein.
- **Automatic aperture (Automatische Blendeneinstellung)** : Die Kamera stellt Blende und Verstärkung selbsttätig ein. Die Verschlusszeit ist vorgegeben.
- **Automatische Verschlusseinstellung** : Die Kamera stellt die Verschlusszeit und die Verstärkung automatisch ein. Die Blende ist vorgegeben.
- **Aktuelle Einstellung beibehalten**: Behält die aktuellen Belichtungseinstellungen bei.
- **Flimmerfrei** : Die Kamera stellt unter Verwendung folgender Verschlusszeiten Blende und Verstärkung automatisch ein: 1/50 s (50 Hz) und 1/60 s (60 Hz).
- **Flimmerfrei 50 Hz** : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/50 s der Blende und Verstärkung selbsttätig ein.
- **Flimmerfrei 60 Hz** : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/60 s der Blende und Verstärkung selbsttätig ein.
- **Flimmerreduziert** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden (50 Hz) und 1/120 Sekunden (60 Hz) einsetzen.
- **Flimmerreduziert 50 Hz** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden einsetzen.
- **Flimmerreduziert 60 Hz** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/120 Sekunden einsetzen.
- **Manuell** : Die Blendenöffnung, Verstärkung und Verschlusszeit sind vorgegeben.

Exposure zone (Belichtungsbereich) : Verwenden Sie Belichtungsbereiche, um die Belichtung in einem ausgewählten Teil der Szene zu optimieren, z. B. dem Bereich vor einer Eingangstür.

Hinweis

Die Belichtungsbereiche beziehen sich auf das Originalbild (nicht gedreht); die Bereichsnamen gelten für das Originalbild. Wenn zum Beispiel der Videostream um 90° gedreht wird, dann wird der **Obere** Bereich zum **Unteren** Bereich des Streams und der **linke** Bereich zum **rechten** Bereich.

- **Automatisch**: Für die meisten Situationen geeignet.
- **Mitte**: Damit wird anhand eines einen fest definierten Bereichs in der Bildmitte die Belichtung berechnet. Dieser Bereich hat in der Live-Ansicht eine feste Größe und Position.
- **Full (Gesamt)** : Damit wird anhand der kompletten Live-Ansicht die Belichtung berechnet.
- **Upper (Oben)** : Damit wird anhand eines festgelegten Bereichs im oberen Teil des Bildes die Belichtung berechnet.
- **Lower (Unten)** : Damit wird anhand eines festgelegten Bereichs im unteren Teil des Bildes die Belichtung berechnet.
- **Left (Links)** : Damit wird anhand eines festgelegten Bereichs im linken Teil des Bildes die Belichtung berechnet.
- **Right (Rechts)** : Damit wird anhand eines festgelegten Bereichs im rechten Teil des Bildes die Belichtung berechnet.
- **Genau**: Damit wird anhand eines Bereichs mit festgelegter Größe und Position die Belichtung berechnet.
- **Benutzerdefiniert**: Damit wird anhand eines Ausschnitts der Live-Ansicht die Belichtung berechnet. Sie können Größe und Position des Bereichs anpassen.

Maximale Verschlusszeit: Wählen Sie die Verschlusszeit für beste Bildqualität. Zu lange Verschlusszeiten (längere Belichtung) können Bewegungsunschärfe erzeugen, wobei zu kurze Verschlusszeiten die Bildqualität beeinträchtigen können. Die maximale Verschlusszeit verbessert das Bild mittels maximaler Verstärkung.

Maximale Verstärkung: Wählen Sie die passende maximale Verstärkung aus. Wenn Sie die maximale Verstärkung erhöhen, wird die Detailschärfe dunkler Bilder verbessert, jedoch auch den Rauschpegel erhöht. Mehr Rauschen kann einem erhöhten Bedarf an Bandbreite und Speicherplatz zur Folge haben. Bei Einstellung einer hohen maximalen Verstärkung kann die Bildqualität bei extrem unterschiedlichen Lichtverhältnissen (Tag/und Nacht) sehr unterschiedlich ausfallen. Die maximierte Verstärkung verbessert das Bild mittels maximierter Verschlusszeit.

Motion-adaptive exposure (Bewegungsadaptive Belichtung) : Wählen Sie diese Option, um die Bewegungsunschärfe bei schlechten Lichtverhältnissen zu verringern.

Balance zwischen Bewegungsunschärfe und Rauschen: Passen Sie mithilfe des Schiebereglers an, ob Bewegungsschärfe oder geringes Rauschen Vorrang hat. Um geringere Bandbreite und geringes Rauschen auf Kosten den Bewegungsschärfe zu bevorzugen, schieben Sie den Schieberegler in Richtung **Geringes Rauschen**. Um Bewegungsschärfe auf Kosten geringer Bandbreite und geringen Rauschens zu bevorzugen, schieben den Schieberegler in Richtung **Geringe Bewegungsunschärfe**.

Hinweis

Sie können die Belichtung entweder durch Einstellen der Belichtungszeit oder der Verstärkung verändern. Die Erhöhung der Belichtungszeit führt dies zu mehr Bewegungsunschärfe und die Erhöhung der Verstärkung zu mehr Rauschen. Wenn Sie **Blur-noise trade-off (Kompromiss zwischen Unschärfe und Rauschen)** in Richtung **Low noise (Geringes Rauschen)** einstellen, wird die automatische Belichtung bei erhöhter Belichtung eher längeren Belichtungszeiten Vorrang geben und umgekehrt, wenn Sie den Kompromiss in Richtung **Low motion blur (Geringe Bewegungsunschärfe)** anpassen. Bei schwachem Licht erreichen sowohl die Verstärkung und die Belichtungszeit letztendlich ihren jeweiligen Maximalwert und es wird keiner der beiden mehr bevorzugt.

Blendenöffnung arretieren : Aktivieren Sie diese Option, um die mithilfe des Schiebereglers der **Blendenöffnung** eingestellte Blendenöffnung zu halten. Aktivieren Sie diese Option, um der Kamera zu erlauben, den Bildfokus automatisch an die Blendenöffnung anzupassen. Sie können z. B. die Öffnung für Szenen mit konstanten Lichtverhältnissen feststellen.

Blendenöffnung : Passen Sie mithilfe des Schiebereglers die Blendenöffnung an, d. h. wie viel Licht durch das Objektiv gelassen wird. Bewegen Sie den Schieberegler in Richtung **Öffnen**, damit mehr Licht in den Sensor gelangen kann, um bei schwachen Lichtverhältnissen ein helleres Bild zu erzeugen. Eine große Blendenöffnung reduziert auch die Schärfentiefe, d.h. dass sich nahe der Kamera oder weit von ihr entfernt befindliche Objekte nur unscharf erfasst werden. Bewegen Sie den Schieberegler in Richtung **Geschlossen**, damit ein das Bild stärker fokussiert werden kann.

Belichtungsgrad: Stellen Sie mithilfe des Schiebereglers die Bildbelichtung ein.

Defog (Entnebelung) : Aktivieren Sie diese Option, damit Nebelwetter erkannt wird und zur Erzeugung eines deutlicheres Bilds Nebeleffekte erfasst und entfernt wird.

Hinweis

Wir raten Ihnen davon ab, bei Szenen mit geringem Kontrast, großen Unterschieden in den Lichtverhältnissen oder bei leicht unscharfem Autofokus **Entnebelung** zu aktivieren. Dies kann die Bildqualität beispielsweise durch erhöhten Kontrast beeinflussen. Bei aktivierter Entnebelung kann sich außerdem zu große Helligkeit negativ auf die Bildqualität auswirken.

Optik

Temperaturkompensation: Aktivieren Sie diese Funktion, wenn die Fokusposition anhand der Temperatur in der Optik korrigiert werden soll.

IR compensation (IR-Kompensation) : Aktivieren Sie diese Funktion, wenn die Fokusposition bei ausgeschalteten Infrarot-Sperrfilter und nicht leuchtendem Infrarotlicht korrigiert werden soll.

Zoom und Fokus kalibrieren: Klicken Sie hier, um die Optik sowie die Zoom- und Fokuseinstellungen auf die Werkseinstellungen zurückzusetzen. Dies ist erforderlich, wenn die Kalibrierung der Optik während des Transports verloren gegangen ist oder das Gerät extremen Vibrationen ausgesetzt war.

Videostream

Allgemein

Auflösung: Wählen Sie eine für die zu überwachende Szene geeignete Bildauflösung. Eine höhere Auflösung erfordert mehr Bandbreite und Speicherplatz.

Bildrate: Um Bandbreitenprobleme im Netzwerk zu vermeiden oder den Speicherbedarf zu reduzieren, kann die Bildrate auf eine feste Größe begrenzt werden. Wird die Bildrate bei Null belassen, wird die unter den aktuellen Bedingungen höchstmögliche Bildrate zugelassen. Höhere Bildraten erfordern mehr Bandbreite und Speicherkapazität.

Komprimierung: Stellen Sie mithilfe des Schiebereglers die Bildkomprimierung ein. Höhere Komprimierung hat eine niedrigere Bitrate und eine geringere Bildqualität zur Folge. Eine niedrigere Komprimierung verbessert die Bildqualität, benötigt jedoch beim Aufzeichnen eine höhere Bandbreite und mehr Speicher.

Signiertes Video : Aktivieren Sie diese Option, um Videos die Funktion Signiertes Video hinzuzufügen. Signiertes Video schützt durch das Hinzufügen von kryptografischen Signaturen das Video vor Manipulation.

Zipstream

Zipstream ist eine Technologie zur Bitratenreduzierung, um die Videoüberwachung zu optimieren. Sie reduziert in Echtzeit die durchschnittliche Bitrate eines H.264- oder H.265-Streams. Bei Szenen mit mehreren Interessensbereichen wendet Axis Zipstream eine hohe Bitrate an, z.B. bei Szenen mit sich bewegenden Objekten. Ist die überwachte Szene eher statisch, wendet Zipstream eine niedrigere Bitrate an und reduziert so den Bedarf an Speicherplatz. Weitere Informationen finden Sie unter *Reduzierung der Bitrate mit Axis Zipstream*

Strength (Stärke) der Bitrate-Verringerung wählen:

- **Off (Aus)**: Keine Reduzierung der Bitrate.
- **Low (Niedrig)**: Bei den meisten Szenen keine sichtbaren Qualitätseinbußen. Dies ist die Standardoption, die bei allen Szenentypen zur Reduzierung der Bitrate verwendet werden kann.
- **Mittel**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und leicht verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **High (Hoch)**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen). Diese Stufe wird für mit der Cloud verbundene Geräte und Geräte empfohlen, die auf lokalen Speicher zurückgreifen.
- **Höher**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **Extreme (Extrem)**: Sichtbarer Effekt in den meisten Szenen: Die Bitrate wird für den kleinsten Speicher optimiert.

Optimize for storage (Für Speicherung optimieren): Aktivieren Sie dies, um die Bitrate zu minimieren und dabei die Qualität zu erhalten. Die Optimierung wird nicht auf den im Webclient angezeigten Videostream angewendet. Dies kann nur verwendet werden, wenn Ihr VMS B-Rahmen unterstützt. Durch Aktivieren von **Optimize for storage** (Speicheroptimierung) wird auch **Dynamic GOP** aktiviert.

Dynamische FPS (Bilder pro Sekunde): Aktivieren Sie diese Option, damit sich die Bandbreite je nach Aktivitätsniveau der Szene ändern kann. Mehr Aktivität erfordert mehr Bandbreite.

Unterer Grenzwert: Geben Sie einen Wert ein, um je nach Bewegung in der Szene die Bildrate zwischen der Mindestanzahl an Bildern pro Sekunde und den Standardanzahl an Bilder pro Sekunde anzupassen. Wir empfehlen, bei Szenen mit sehr geringer Bewegung, bei denen die Anzahl an Bilder pro Sekunde auf 1 oder niedriger fallen können, einen unteren Grenzwert anzugeben.

Dynamic GOP (Group of Pictures): Aktivieren Sie diese Option, um das Intervall zwischen I-Frames anhand des Aktivitätsniveaus der Szene dynamisch anzupassen.

Oberer Grenzwert: Geben Sie eine maximale GOP-Länge ein, das heißt die maximale Anzahl von P-Frames zwischen zwei I-Frames. Ein I-Frame ist ein Einzelbild, das unabhängig von anderen Einzelbildern dekodierbar ist.

P-Frames: Ein P-Frame ist ein vorhersagbares Einzelbild, das nur die Bildänderungen gegenüber dem vorangehenden Einzelbild anzeigt. Geben Sie die gewünschte Anzahl von P-Frames ein. Je höher die Anzahl, desto weniger Bandbreite ist erforderlich. Tritt aber im Netzwerk ein Datenstau auf, könnte es zu einer merklichen Verschlechterung der Videoqualität kommen.

Bitrate control (Bitratensteuerung)

- **Average (Durchschnitt)**: Wählen Sie diese Option, um die Bitrate automatisch über einen längeren Zeitraum anzupassen und je nach verfügbaren Speicher die bestmögliche Bildqualität zu liefern.
  - Klicken Sie darauf, um die Zielbitrate anhand des verfügbaren Speichers, der Aufbewahrungszeit und des Bitratenlimits zu berechnen.
  - **Zielbitrate**: Geben Sie die gewünschte Zielbitrate ein.
  - **Aufbewahrungszeit**: Geben Sie die Aufbewahrungszeit für Aufzeichnungen in Tagen ein.
  - **Speicher**: Zeigt den für den Videostream nutzbaren geschätzten Speicherplatz an.
  - **Maximale Bitrate**: Aktivieren Sie diese Option, um eine Bitratengrenze festzulegen.
  - **Bitratengrenze**: Geben Sie eine Bitratengrenze ein, die über der Zielbitrate liegt.
- **Maximum**: Wählen Sie diese Option, um die maximale Sofort-Bitrate des Videostreams auf Grundlage der Netzwerkbandbreite festzulegen.
  - **Maximum**: Geben Sie die maximale Bitrate ein.
- **Variable**: Wählen Sie diese Option, damit sich die Bitrate je nach Aktivitätsniveau der Szene anpasst. Mehr Aktivität erfordert mehr Bandbreite. Diese Option wird für die meisten Situationen empfohlen.

Ausrichtung

Spiegelung: Aktivieren Sie diese Option, um das Bild zu spiegeln.

Audio

Einschließen: Aktivieren Sie diese Option, um Audio im Videostream zu verwenden.

Source (Quelle) : Wählen die zu verwendende Audioquelle.

Stereo : Aktivieren Sie diese Option, um sowohl integriertes Audio als auch Audio von einem externen Mikrofon zu verwenden.

Overlays

+ : Klicken Sie darauf, um ein Overlay hinzuzufügen. Wählen Sie in der Auswahlliste den Typ des Overlays aus:

- **Text**: Wählen Sie diese Option, um einen Text anzeigen zu lassen, der in das Live-Ansichtsbild integriert und in allen Ansichten, Aufzeichnungen und Schnappschüssen sichtbar ist. Sie können einen eigenen Text eingeben und Sie können auch vorkonfigurierte Modifikatoren verwenden, um z. B. Uhrzeit, Datum und Bildrate automatisch anzeigen zu lassen.
  - : Klicken Sie darauf, um den Datumsmodifikator `%F` hinzufügen und das Format JJJJ-MM-TT anzuzeigen.
  - : Klicken Sie darauf, um den Uhrzeitmodifikator `%X` hinzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
  - **Modifikatoren**: Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel `%a` den Wochentag an.
  - **Größe**: Wählen Sie die gewünschte Schriftgröße.
  - **Darstellung**: Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
  - : Wählen Sie die Position des Overlays im Bild.
- **Bild**: Wählen Sie diese Option, um ein statisches Bild über dem Videostream zu zeigen. Sie können .bmp-, .png-, .jpeg- oder .s jpeg-Dateien verwenden.
  Um ein Bild hochzuladen, klicken Sie auf **Bilder**. Bevor Sie ein Bild hochladen, können Sie folgende Optionen festlegen:
  - **An Auflösung anpassen**: Wählen Sie diese Option, um das Overlay-Bild automatisch an die Videoauflösung anzupassen.
  - **Transparenz verwenden**: Wählen Sie den Hexadezimal-RGB-Wert für diese Farbe und geben Sie diesen ein. Verwenden Sie das Format RRGGBB. Beispiele für Hexadezimalwerte: FFFFFF für Weiß, 000000 für Schwarz, FF0000 für Rot, 6633FF für Blau und 669900 für Grün. Nur bei .bmp-Bildern.
- **Streaming-Indikator** : Wählen Sie diese Option, um eine Animation über dem Videostream zu einzublenden. Die Animation zeigt an, dass der Videostream live ist, selbst wenn die Szene aktuell bewegungsfrei ist.
  - **Darstellung**: Wählen Sie die Farbe der Animation und des Hintergrunds, zum Beispiel rote Animation auf durchsichtigem Hintergrund (Standardeinstellung).
  - **Größe**: Wählen Sie die gewünschte Schriftgröße.
  - : Wählen Sie die Position des Overlays im Bild.

Sichtbereiche

+ : Klicken Sie darauf, um einen Sichtbereich zu erstellen.

Klicken Sie auf den Sichtbereich, um auf die Einstellungen zuzugreifen.

Name: Geben Sie einen Namen für den Sichtbereich ein. Die maximale Länge liegt bei 64 Zeichen.

Seitenverhältnis: Wählen Sie das gewünschte Seitenverhältnis. Die Auflösung wird automatisch angepasst.

PTZ: Aktivieren Sie diese Option, um die Funktionen Schwenken, Neigen und Zoomen im Sichtbereich zu verwenden.

Privatzonenmasken

+ : Klicken Sie darauf, um eine neue Privatzonenmaske zu erstellen.

Privacy masks (Privatzonenmasken): Klicken Sie darauf, um die Farbe aller Privatzonenmasken zu ändern oder um alle Privatzonenmasken dauerhaft zu löschen.

Maske x: Klicken Sie darauf, um die Maske umzubenennen, zu deaktivieren oder dauerhaft zu löschen.

Audio

Geräteinstellungen

Input (Eingang): Audioeingang ein- oder ausschalten. Zeigt die Eingangsart an.

Allow stream extraction (Videostream-Extraktion erlauben) : Aktivieren Sie diese Option, um eine Videostream-Extraktion zuzulassen.

Input type (Eingangsart) : Wählen Sie die Art des Eingangs aus, z. B. interner Mikrofon- oder Line-Eingang.

Power type (Spannungsart) : Wählen Sie die Art der Eingangsstromversorgung aus.

Apply changes (Änderungen übernehmen) : Wenden Sie Ihre Auswahl an.

Separate gain controls (Separate Verstärkungsregler) : Aktivieren Sie diese Option, um die Verstärkung für die verschiedenen Eingangsarten separat einzustellen.

Automatic gain control (Automatische Verstärkungsregelung) : Aktivieren Sie dieses Option, damit die Verstärkung dynamisch an Klangänderungen angepasst wird.

Verstärkung: Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Mikrofonsymbol.

Ausgang: Zeigt die Ausgangsart an.

Verstärkung: Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Lautsprechersymbol.

Videostream

Encoding (Codierung): Wählen Sie die Codierung für das Streaming der Eingangsquelle aus. Diese Kodierung steht nur bei aktiviertem Audioeingang zur Auswahl. Klicken Sie auf **Enable audio input (Audioeingang aktivieren)**, falls der Audioeingang deaktiviert ist.

Audioclips

Add clip (Clip hinzufügen): Fügen Sie einen neuen Audioclip hinzu. Sie können Dateien wie .au, .mp3, .opus, .vorbis, .wav verwenden.

Audio-Clip abspielen.

Audio-Clip anhalten.

Das Kontextmenü enthält:

- **Rename (Umbenennen)**: Namen des Audio-Clip ändern.
- **Create link (Link erstellen)**: Erstellen Sie eine URL, über die der Audioclip auf dem Gerät abgespielt wird. Legen Sie für den Clip die Lautstärke und die Anzahl der Wiederholungen fest.
- **Herunterladen**: Laden Sie den Audioclip auf Ihren Computer herunter.
- **Löschen**: Entfernen Sie den Audioclip vom Gerät.

Aufzeichnungen

Klicken Sie darauf, um die Aufzeichnungen zu filtern.

Von: Zeigt Aufzeichnungen, die nach einem bestimmten Zeitpunkt gemacht wurden.

Bis: Zeigt Aufzeichnungen, die bis zu einem bestimmten Zeitpunkt gemacht wurden.

Source (Quelle) : Zeigt Aufzeichnungen auf Grundlage der Quelle. Die Quelle bezieht sich auf den Sensor.

Event (Ereignis): Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Storage (Speicher): Zeigt Aufzeichnungen nach Speichertyp.

Ongoing recordings (Laufende Aufzeichnungen): Anzeige aller laufenden Kamera-Aufzeichnungen.

Starten einer Kamera-Aufzeichnung.

Wählen Sie das Speichermedium, auf dem die Aufzeichnung gespeichert werden soll.

Beenden einer Kamera-Aufzeichnung.

Ausgelöste Aufzeichnungen können entweder manuell gestoppt oder durch Ausschalten der Kamera beendet werden.

Fortlaufende Aufzeichnungen laufen so lange weiter, bis sie manuell gestoppt werden. Bei Ausschalten der Kamera wird die Aufzeichnung nach dem Wiedereinschalten fortgesetzt.

Die Aufzeichnung wiedergeben.

Abspielen der Aufzeichnung anhalten.

Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

Set export range (Exportbereich festlegen): Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten.

Encrypt (Verschlüsseln): Legen Sie mit dieser Option ein Kennwort für exportierte Aufzeichnungen fest. Die exportierte Datei kann ohne das Kennwort nicht geöffnet werden.

Klicken Sie auf , um eine Aufzeichnung zu löschen.

Export (Exportieren): Exportieren der ganzen Aufzeichnung oder eines Teils davon.

Apps

Add app (App hinzufügen): Installieren einer neuen App.

Find more apps (Weitere Apps finden): Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet.

Allow unsigned apps (Unsignierte Apps erlauben): Aktivieren Sie diese Option, um die Installation unsignierter Apps zu ermöglichen.

Allow root-privileged apps (Apps mit Root-Berechtigungen zulassen): Aktivieren Sie diese Option, um Apps mit Root-Berechtigungen uneingeschränkten Zugriff auf das Gerät zu ermöglichen.

Sehen Sie sich die Sicherheitsupdates in den AXIS OS und ACAP-Apps an.

Hinweis

Bei gleichzeitiger Ausführung mehrerer Apps kann die Leistung des Geräts beeinträchtigt werden.

Verwenden Sie den Schalter neben dem App-Namen, um diese zu starten oder anzuhalten.

Open (Öffnen): Auf die Anwendungseinstellungen zugreifen. Die verfügbaren Einstellungen sind anwendungsabhängig. Für einige Anwendungen stehen keine Einstellmöglichkeiten zur Verfügung.

Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

- **Open-source license (Open-Source-Lizenz)**: Anzeigen von Informationen über die in der App genutzten Open-Source-Lizenzen.
- **App log (App-Protokoll)**: Ereignisprotokoll der App anzeigen. Das Protokoll ist hilfreich, wenn Sie sich an den Support wenden müssen.
- **Lizenz mit Schlüssel aktivieren**: Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Verwenden Sie diese Option, wenn Ihr Gerät keinen Internetzugang besitzt.
  Falls Sie keinen Lizenzschlüssel besitzen, gehen Sie zu *axis.com/products/analytics*. Um einen Lizenzschlüssel zu erzeugen, benötigen Sie einen Lizenzcode und die Seriennummer Ihres Axis Produkts,
- **Lizenz automatisch aktivieren**: Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Gehen Sie über diese Option, wenn Ihr Gerät über einen Internetzugang verfügt. Sie benötigen einen Lizenzschlüssel, um die Lizenz zu aktivieren.
- **Deactivate the license (Lizenz deaktivieren)**: Deaktivieren Sie die Lizenz, um sie durch eine andere Lizenz zu ersetzen, z. B. wenn Sie von einer Testlizenz zu einer vollständigen Lizenz wechseln. Wenn Sie die Lizenz deaktivieren, wird sie damit auch vom Gerät entfernt.
- **Settings (Einstellungen)**: Darüber werden die Parameter konfiguriert.
- **Delete (Löschen)**: Darüber löschen Sie die App dauerhaft vom Gerät. Die Lizenz muss zuerst deaktiviert werden, da sie andernfalls weiterhin aktiv ist.

System

Uhrzeit und Standort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

Wir empfehlen Ihnen, Datum und Uhrzeit des Geräts mit einem NTP-Server zu synchronisieren.

Synchronization (Synchronisierung): Wählen Sie eine Option zur Synchronisierung von Datum und Uhrzeit des Geräts aus.

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server))**: Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP))**: Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server)**: Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server))**: Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Benutzerdefinierte Datum und Uhrzeit**: Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie auf **Get from system (Vom System abrufen)**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

Time zone (Zeitzone): Wählen Sie die zu verwendende Zeitzone aus. Die Zeit wird automatisch bei Sommer- und Standardzeit angepasst.

Hinweis

Die Einstellungen für Datum und Uhrzeit werden vom System für alle Aufzeichnungen, Protokolle und Systemeinstellungen verwendet.

Gerätestandort

Den Gerätestandort eingeben. Das Videoverwaltungssystem kann mit dieser Information das Gerät auf eine Karte setzen.

- **Latitude (Breite)**: Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Longitude (Länge)**: Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Heading (Ausrichtung)**: Die Ausrichtung des Geräts laut Kompass eingeben. Der Wert 0 steht für: genau nach Norden.
- **Label (Bezeichnung)**: Eine aussagekräftige Bezeichnung für das Gerät eingeben.
- **Save (Speichern)**: Klicken Sie hier, um den Gerätestandort zu speichern.

Netzwerk

IPv4

Assign IPv4 automatically (IPv4 automatisch zuweisen): Wählen Sie diese Option, damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der IP-Adresse (DHCP).

IP address (IP-Adresse): Geben Sie für das Gerät eine eindeutige IP-Adresse ein. Statische IP-Adressen können innerhalb von isolierten Netzwerken zufällig zugewiesen werden, sofern jede Adresse eindeutig ist. Zur Vermeidung von Konflikten empfehlen wir Ihnen, sich vor dem Zuweisen einer statischen IP-Adresse an den Netzwerkadministrator zu wenden.

Subnet mask (Subnetzmaske): Geben Sie die Subnetzmaske ein, um festzulegen, welche Adressen sich im lokalen Netzwerk befinden. Jede Adresse außerhalb des lokalen Netzwerks wird über den Router geleitet.

Router: Geben Sie die IP-Adresse des Standardrouters (Gateway) ein, um Geräten zu verbinden, die in verschiedenen Netzwerken und Netzwerk-Segmenten verwendet werden.

Fallback to static IP address if DHCP isn't available (Fallback zu statischer IP-Adresse, wenn DHCP nicht verfügbar ist): Wählen Sie aus, ob Sie eine statische IP-Adresse hinzufügen möchten, die als Reserve verwendet werden soll, wenn DHCP nicht verfügbar ist und keine IP-Adresse automatisch zugewiesen werden kann.

Hinweis

Wenn DHCP nicht verfügbar ist und das Gerät eine statische Fallback-Adresse verwendet, wird die statische Adresse mit einem begrenzten Bereich konfiguriert.

IPv6

IPv6 automatisch zuweisen: Wählen Sie diese Option, um IPv6 einzuschalten und damit der Netzwerk-Router dem Gerät automatisch eine IP-Adresse zuweisen kann.

Host-Name

Assign hostname automatically (Host-Namen automatisch zuweisen): Wählen Sie diese Option aus, damit der Netzwerkrouter dem Gerät automatisch einen Host-Namen zuweisen kann.

Host-Name: Geben Sie den Host-Namen manuell ein, um ihn als alternative Möglichkeit für den Zugriff auf das Gerät zu verwenden. Der Server-Bericht und das Systemprotokoll verwenden den Host-Namen. Zugelassene Zeichen sind A–Z, a–z, 0–9 und -.

DNS servers (DNS-Server)

Assign DNS automatically (DNS automatisch zuweisen): Wählen Sie diese Option, damit der DHCP-Server dem Gerät automatisch Domains für die Suche und DNS-Server-Adressen zuweisen kann. Für die meisten Netzwerke empfehlen wir eine automatische Zuweisung der DNS-Server-Adresse (DHCP).

Search domains (Suchdomains): Wenn Sie einen Host-Namen verwenden, der nicht vollständig qualifiziert ist, klicken Sie auf **Add search domain (Suchdomain hinzufügen)** und geben Sie eine Domain ein, in der nach dem vom Gerät verwendeten Host-Namen gesucht werden soll.

DNS servers (DNS-Server): Klicken Sie auf **Add DNS server (DNS-Server hinzufügen)** und geben Sie die IP-Adresse des DNS-Servers ein. Dadurch werden in Ihrem Netzwerk Host-Namen in IP-Adressen übersetzt.

HTTP und HTTPS

HTTPS ist ein Protokoll, das Verschlüsselung für Seitenanforderungen von Benutzern und für die vom Webserver zurückgegebenen Seiten bereitstellt. Der verschlüsselte Austausch von Informationen wird durch die Verwendung eines HTTPS-Zertifikats geregelt, das die Authentizität des Servers gewährleistet.

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie für die Erstellung und Installation von Zertifikaten zu **System > Security (System > Sicherheit)**.

Zugriff zulassen über: Wählen Sie aus, ob Sie einem Benutzer erlauben wollen, eine Verbindung mit dem Gerät über die Protokolle **HTTP**, **HTTPS** oder **HTTP and HTTPS (HTTP und HTTPS)** herzustellen.

Hinweis

Wenn Sie auf verschlüsselte Internetseiten über HTTPS gehen, kann es zu Beeinträchtigungen der Leistung kommen, insbesondere wenn Sie eine Seite zum ersten Mal aufrufen.

HTTP port (HTTP-Port): Geben Sie den zu verwendenden HTTP-Port ein. Das Gerät lässt Port 80 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

HTTPS port (HTTPS-Port): Geben Si den zu verwendenden HTTPS-Port ein. Das Gerät lässt Port 443 oder jeden Port im Bereich 1024-65535 zu. Wenn Sie als Administrator angemeldet sind, können Sie auch einen beliebigen Port im Bereich 1-1023 eingeben. Wenn Sie einen Port in diesem Bereich verwenden, erhalten Sie eine Warnung.

Zertifikat: Wählen Sie ein Zertifikat, um HTTPS für das Gerät zu aktivieren.

Protokolle zur Netzwerkerkennung

Bonjour®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

Bonjour-Name: Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.

UPnP®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

UPnP-Name: Geben Sie den im Netzwerk anzuzeigenden Namen an. Der Standardname setzt sich aus dem Namen des Geräts und seiner MAC Adresse zusammen.

WS-Erkennung: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

Cloud-Anbindung mit einem Mausklick

One-Click Cloud Connect (O3C) stellt in Verbindung mit einem O3C-Dienst einen einfachen und sicheren Internetzugang zu Live-Video und aufgezeichneten Videos von jedem Standort aus bereit. Weitere Informationen finden Sie unter *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (O3C zulassen):

- **One-click**: Dies ist die Standardeinstellung. Halten Sie die Steuertaste am Gerät gedrückt, um über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sie müssen das Gerät innerhalb von 24 Stunden nach dem Drücken der Steuertaste beim O3C-Dienst registrieren. Andernfalls wird sich das Gerät vom O3C-Dienst getrennt. Nach der Registrierung des Geräts ist **Always (Immer)** aktiviert und das Gerät bleibt mit dem O3C-Dienst verbunden.
- **Immer**: Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Nach der Registrierung bleibt das Gerät mit dem O3C-Dienst verbunden. Verwenden Sie diese Option, wenn die Steuertaste am Gerät außer Reichweite ist.
- **Nein**: Deaktiviert den O3C-Dienst.

Proxy settings (Proxy-Einstellungen): Geben Sie falls erforderlich die Proxyeinstellungen ein, um eine Verbindung zum Proxy-Server herzustellen.

Host: Geben Sie die Adresse des Proxy-Servers ein.

Port: Geben Sie die Nummer der für den Zugriff verwendeten Ports an.

Anmeldung und **Kennwort**: Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.

Authentication method (Authentifizierungsmethode):

- **Basic (Einfach)**: Diese Methode ist das am besten geeignete Authentifizierungsschema für HTTP. Sie ist nicht so sicher wie die **Digest**-Methode, da sie den Benutzernamen und das Kennwort unverschlüsselt an den Server sendet.
- **Digest**: Diese Methode ist sicherer, da das Kennwort hier stets verschlüsselt im Netzwerk übermittelt wird.
- **Auto**: Bei dieser Option kann das Gerät die Authentifizierungsmethode automatisch je nach unterstützten Methoden auswählen. Die Methode **Digest** wird gegenüber der Methode **Einfach** bevorzugt.

Besitzerauthentifizierungsschlüssel (OAK): Klicken Sie auf **Schlüssel abrufen**, um den Besitzerauthentifizierungsschlüssel abzurufen. Dies ist nur dann möglich, wenn das Gerät ohne Firewall oder Proxy mit dem Internet verbunden ist.

SNMP

Simple Network Management Protocol (SNMP) ermöglicht die Remoteverwaltung von Netzwerk-Geräten.

SNMP: Wählen Sie die zu verwendende SNMP-Version.

- **v1 und v2c**:
  - **Lese-Community**: Geben Sie den Namen der Community mit ausschließlich Lesezugriff auf alle unterstützten SNMP-Objekte an. Der Standardwert ist **public (öffentlich)**.
  - **Write community (Schreib-Community)**: Geben Sie den Namen der Community mit Lese- oder Schreibzugriff auf alle unterstützten SNMP-Objekte (außer schreibgeschützte Objekte) an. Der Standardwert ist **schreiben**.
  - **Traps aktivieren**: Aktivieren Sie die Option, um Trap-Berichte zu erhalten. Traps werden vom Gerät bei wichtigen Ereignissen und Statusänderungen zum Versenden von Meldungen verwendet. In der Weboberfläche können Sie Traps für SNMP v1 und v2c einrichten. Traps werden automatisch deaktiviert, wenn Sie zu SNMP v3 wechseln oder SNMP deaktivieren. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Trap-Adresse**: Geben Sie die IP-Adresse oder den Host-Namen des Verwaltungsservers ein.
  - **Trap-Community**: Geben Sie die Trap-Community ein, die das Gerät zum Versenden einer Trap-Meldung an das Verwaltungssystem verwenden soll.
  - **Traps**:
  - **Kaltstart**: Versendet eine Trap-Nachricht, wenn das Gerät hochgefahren wird.
  - **Warmstart**: Versendet eine Trap-Nachricht, wenn Sie eine SNMP-Einstellung ändern.
  - **Verbindungsaufbau**: Versendet eine Trap-Meldung, wenn der Status eines Links von Down zu Up wechselt.
  - **Authentifizierung fehlgeschlagen**: Versendet eine Trap-Meldung, wenn ein Authentifizierungsversuch fehlschlägt.

Hinweis

Alle Axis Video MIB-Traps sind aktiviert, wenn Sie SNMP v1- und v2c-Traps aktivieren. Weitere Informationen finden Sie unter *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden.

Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.

- **Kennwort für das Konto "initial"**: Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

Sicherheit

Zertifikate

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten verwendet. Das Gerät unterstützt zwei Zertifikattypen:

- **Client-/Serverzertifikate**
  Ein Client-/Serverzertifikat identifiziert das Axis Produkt und kann selbstsigniert oder von einer Zertifizierungsstelle (Certificate Authority, CA) ausgegeben worden sein. Ein selbstsigniertes Zertifikat bietet begrenzten Schutz und kann vor Erhalt eines CA-Zertifikats verwendet werden.
- **CA-Zertifikate**
  CA-Zertifikate werden zum Authentifizieren von Peer-Zertifikaten verwendet, um zum Beispiel die Identität eines Authentifizierungsservers zu überprüfen, wenn das Gerät mit einem durch IEEE 802.1X geschützten Netzwerk verbunden ist. Auf dem Gerät sind mehrere CA-Zertifikate vorinstalliert.

Folgende Formate werden unterstützt:

- Zertifikatsformate: .PEM, .CER und .PFX
- Formate von privaten Schlüssel: PKCS#1 und PKCS#12

Wichtig

Wenn Sie das Gerät auf die Werkseinstellungen zurücksetzen, werden alle Zertifikate gelöscht. Vorinstallierte CA-Zertifikate werden neu installiert.

Die Zertifikate in der Liste filtern.

Add certificate (Zertifikat hinzufügen): Klicken Sie, um ein Zertifikat hinzuzufügen.

- **More (Mehr)** : Weitere Felder anzeigen, die Sie ausfüllen oder auswählen müssen.
- **Secure keystore (Sicherer Schlüsselspeicher)**: Wählen Sie **Secure element (Sicheres Element)** oder **Trusted Platform Module 2.0** zum sicheren Speichern des privaten Schlüssels aus. Weitere Informationen zum zu wählenden sicheren Schlüsselspeicher finden Sie unter *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Schlüsseltyp)**: Wählen Sie in der Dropdown-Liste zum Schutz des Zertifikats den Standard- oder einen anderen Verschlüsselungsalgorithmus aus.

Das Kontextmenü enthält:

- **Certificate information (Zertifikatsinformationen)**: Lassen Sie sich die Eigenschaften eines installierten Zertifikats anzeigen.
- **Zertifikat löschen**: Löschen Sie das Zertifikat.
- **Signierungsanforderung erstellen**: Erstellen Sie eine Anforderung zur Zertifikatsignierung, um sie an eine Registrierungsstelle zu senden und ein digitales Zertifikat zu erhalten.

Secure keystore (Sicherer Schlüsselspeicher) :

- **Secure element (CC EAL6+)**: Wählen Sie diese Option aus, um sicheres Element für sicheren Schlüsselspeicher zu verwenden.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2)**: Wählen Sie diese Option aus, um TPM 2.0 für sicheren Schlüsselspeicher zu verwenden.

IEEE 802.1x

IEEE 802.1x ist ein IEEE-Standard für portbasierte Netzwerk-Zugriffskontrolle, die eine sichere Authentifizierung für drahtgebundene und drahtlose Netzwerk-Geräte bereitstellt. IEEE 802.1x basiert auf EAP (Extensible Authentication Protocol).

Zum Zugriff auf ein mit IEEE 802.1x geschütztes Netzwerk müssen sich die Netzwerk-Geräte authentifizieren. Die Authentifizierung erfolgt durch einen Authentifizierungsserver, üblicherweise ein RADIUS-Server (zum Beispiel FreeRADIUS und Microsoft Internet Authentication Server).

Zertifikate

Wenn die Konfiguration ohne CA-Zertifikat erfolgt, ist die Validierung des Serverzertifikats deaktiviert und das Gerät versucht, sich selbst zu authentifizieren, unabhängig vom aktuellen Netzwerk.

Bei Verwendung eines Zertifikats bei der Implementierung von Axis authentifizieren sich das Gerät und der Authentifizierungsserver mithilfe von digitalen Zertifikaten über EAP-TLS (Extensible Authentication Protocol – Transport Layer Security).

Damit das Gerät auf ein netzwerkgeschütztes Netzwerk zugreifen darf, müssen Sie ein signiertes Clientzertifikat auf dem Gerät installieren.

Client certificate (Clientzertifikat): Wählen Sie ein Clientzertifikat aus, um IEEE 802,1x zu verwenden. Der Authentifizierungsserver verwendet das Zertifikat zur Validierung der Identität des Clients.

CA certificate (CA-Zertifikat): Wählen Sie CA-Zertifikate zur Validierung der Identität des Authentifizierungsservers. Wenn kein Zertifikat ausgewählt sind, versucht das Gerät, sich selbst zu authentifizieren, unabhängig vom Netzwerk, mit dem es verbunden ist.

EAP-Identität: Geben Sie die mit dem Clientzertifikat verknüpfte Identität des Benutzers ein.

EAPOL-Version: Wählen Sie die in dem Netzwerk-Switch verwendete EAPOL-Version.

IEEE 802.1x verwenden: Wählen Sie diese Option aus, um das IEEE 802.1x-Protokoll zu verwenden.

Brute-Force-Angriffe verhindern

Blocken: Aktivieren Sie diese Option, um Brute-Force-Angriffe zu blockieren. Ein Brute-Force-Angriff versucht über Trial-and-Error, Zugangsdaten oder Verschlüsselungsschlüssel zu erraten.

Blockierdauer: Geben Sie ein, wie viele Sekunden ein Brute-Force-Angriff blockiert werden soll.

Blockierbedingungen: Geben Sie die Anzahl der pro Sekunde zulässigen Authentifizierungsfehler ein, bevor blockiert wird. Sie können die Anzahl der zulässigen Fehler sowohl auf Seiten- als auch auf Geräteebene festlegen.

IP address filter (IP-Adressfilter)

Use filter (Filter verwenden): Wählen Sie diese Option, um zu filtern, welche IP-Adressen auf das Gerät zugreifen dürfen.

Policy (Richtlinie): Wählen Sie, ob Sie den Zugriff für bestimmte IP-Adressen **Allow (erlauben)** oder **Deny (verweigern)** möchten.

Addresses (Adressen): Geben Sie die IP-Nummern ein, denen der Zugriff auf das Gerät erlaubt oder verweigert wird. Sie können auch das CIDR-Format verwenden.

Spezifisch signiertes Firmwarezertifikat

Zum Installieren von Test-Firmware oder anderer benutzerdefinierter Firmware von Axis auf dem Gerät benötigen Sie ein individuell signiertes Firmwarezertifikat. Das Zertifikat prüft, ob die Firmware sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Firmware kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Benutzersignierte Firmwarezertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

Install (Installieren): Klicken Sie, um das Zertifikat zu installieren. Sie müssen das Zertifikat installieren, bevor Sie die Firmware installieren.

Konten

Accounts (Konten)

+ **Add account (Konto hinzufügen)**: Klicken Sie, um ein neues Konto hinzuzufügen. Es können bis zu 100 Konten hinzugefügt werden.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

New password (Neues Kennwort): Geben Sie ein Kennwort für den Kontonamen ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.

Repeat password (Kennwort wiederholen): Geben Sie das gleiche Kennwort erneut ein.

Privileges (Rechte):

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener)**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**einstellungen.
  - Apps werden hinzugefügt.
- **Betrachter**: Hat Zugriff auf:
  - Einen Videostream ansehen und Schnappschüsse machen.
  - Aufzeichnungen ansehen und exportieren.
  - Schwenken, Neigen und Zoomen; mit PTZ-Benutzerzugriff.

⋮ Das Kontextmenü enthält:

Update account (Konto aktualisieren): Bearbeiten Sie die Eigenschaften des Kontos.

Delete account (Konto löschen): Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

Anonymous access (Anonymer Zugriff)

Allow anonymous viewing (Anonymes Betrachten zulassen): Aktivieren Sie diese Option, damit Personen als Betrachter auf das Gerät zugreifen können, ohne sich mit einem Benutzerkonto anmelden zu müssen.

Allow anonymous PTZ operating (Anonyme PTZ-Benutzung zulassen): Aktivieren Sie diese Option. damit anonyme Benutzer das Bild schwenken, neigen und zoomen können.

SSH accounts (SSH-Konten)

+ **Add SSH account (SSH-Konto hinzufügen)**: Klicken Sie, um ein neues SSH-Konto hinzuzufügen.

- **Restrict root access (Root-Zugriff beschränken)**: Aktivieren, um die Funktion einzuschränken, die einen Root-Zugriff erfordert.
- **Enable SSH (SSH aktivieren)**: Den SSH-Dienst aktivieren.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

Neues Kennwort: Geben Sie ein Kennwort für das Konto ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.

Repeat password (Kennwort wiederholen): Geben Sie das gleiche Kennwort erneut ein.

Comment (Anmerkung): Geben Sie eine Anmerkung ein (optional).

Das Kontextmenü enthält:

Update SSH account (SSH-Konto aktualisieren): Bearbeiten Sie die Eigenschaften des Kontos.

Delete SSH account (SSH-Konto löschen): Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

OpenID Configuration (OpenID-Konfiguration)

Wichtig

Geben Sie die richtigen Werte ein, um sicherzustellen, dass Sie sich erneut am Gerät anmelden können.

Client ID (Client-ID): Geben Sie den OpenID-Benutzernamen ein.

Outgoing Proxy (Ausgehender Proxy): Geben Sie die Proxyadresse für die OpenID-Verbindung ein, um einen Proxyserver zu verwenden.

Admin claim (Administratorenforderung): Geben Sie einen Wert für die Administratorrolle ein.

Provider URL (Provider-URL): Geben Sie den Weblink für die API-Endpunkt-Authentifizierung ein. Das Format muss https://[insert URL]/.well-known/openid-configuration sein

Operator claim (Bedienerforderung): Geben Sie einen Wert für die Bedienerrolle ein.

Require claim (Anspruchanforderung): Geben Sie die Daten ein, die im Token enthalten sein sollen.

Viewer claim (Betrachterforderung): Geben Sie den Wert für die Betrachterrolle ein.

Remote user (Remote-Benutzer): Geben Sie einen Wert zur Identifizierung von Remote-Benutzern ein. Dadurch wird der aktuelle Benutzer auf der Weboberfläche des Geräts angezeigt.

Scopes (Bereiche): Optionale Bereiche, die Teil des Tokens sein können.

Client secret (Kundengeheimnis): Geben Sie das OpenID-Kennwort ein.

Save (Speichern): Klicken Sie hier, um die OpenID-Werte zu speichern.

Enable OpenID (OpenID aktivieren): Die aktuelle Verbindung aktivieren und die Geräteauthentifizierung über die Provider-URL zulassen.

Ereignisse

Regeln

Eine Aktionsregel definiert die Bedingungen, die dazu führen, dass das Produkt eine Aktion ausführt. Die Liste zeigt alle derzeit konfigurierten Regeln für das Produkt.

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

+ **Add a rule (Regel hinzufügen)**: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

Wait between actions (Wartezeit zwischen den Aktionen): Geben Sie die an (hh:mm:ss), wie viel Zeit mindestens zwischen Regelaktivierungen vergehen muss. Es ist sinnvoll, wenn die Regel beispielsweise durch Tag-Nacht-Bedingungen aktiviert wird, damit nicht aufgrund kleiner Änderungen der Lichtverhältnisse bei Sonnenaufgang und -untergang die Regel wiederholt aktiviert wird.

Bedingung: Wählen Sie eine Bedingung aus der Liste aus. Eine Bedingung muss erfüllt sein, damit das Gerät eine Aktion ausführen kann. Wenn mehrere Bedingungen festgelegt wurden, müssen zum Auslösen der Aktion alle dieser Bedingungen erfüllt sein. Informationen zu bestimmten Bedingungen finden Sie unterunter *Erste Schritte mit Regeln für Ereignisse*.

Die Bedingung als Auslöser verwenden: Wählen Sie diese Option aus, damit diese erste Bedingung nur als Startauslöser funktioniert. Damit bleibt die Regel nach Aktivierung so lange aktiv, wie alle anderen Bedingungen erfüllt sind, unabhängig vom Status der ersten Bedingung. Wenn diese Option nicht ausgewählt ist, ist die Regel nur aktiv, wenn alle Bedingungen erfüllt sind.

Bedingungen umkehren: Wählen Sie diese Option, wenn die Bedingung im Gegensatz zu Ihrer Auswahl stehen soll.

+ **Bedingung hinzufügen**: Klicken Sie darauf, um eine zusätzliche Bedingung hinzuzufügen.

Aktion: Wählen Sie eine Aktion aus der Liste aus und geben Sie die erforderlichen Informationen ein. Informationen zu bestimmten Aktionen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Empfänger

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis

Sie können bis zu 20 Empfänger erstellen.

+ **Einen Empfänger hinzufügen**: Klicken Sie darauf, um einen Empfänger hinzuzufügen.

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

- **FTP**
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Geben Sie die vom FTP-Server verwendete Portnummer ein. Der Standardport ist 21.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem FTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
  - **Use passive FTP (Passives FTP verwenden)**: Normalerweise fordert das Produkt den FTP-Zielserver zum Öffnen der Datenverbindung auf. Normalerweise initiiert das Gerät die FTP-Steuerung und die Datenverbindungen zum Zielserver. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielserver eine Firewall eingerichtet ist.
- **HTTP**

- **URL**: Geben Sie die Netzwerkadresse des HTTP-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise http://192.168.254.10/cgi-bin/notify.cgi.
- **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
- **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
- **Proxy**: Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTP-Server ein Proxyserver erforderlich ist.

- **HTTPS**
  - **URL**: Geben Sie die Netzwerkadresse des HTTPS-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Server-Zertifikat validieren)**: Wählen Sie diese Option, um zu überprüfen, ob das Zertifikat von HTTPS-Server erstellt wurde.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Proxy**: Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTPS-Server ein Proxyserver erforderlich ist.
- **Network storage (Netzwerk-Speicher)**
  Darüber können Sie einen Netzwerk-Speicher wie NAS (Network Attached Storage) hinzufügen und als Empfänger für zu speichernde Dateien verwenden. Die Dateien werden im Format Matroska (MKV) gespeichert.
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen der Netzwerk-Speicher ein.
  - **Freigabe**: Geben Sie den Namen der Freigabe auf dem Host ein.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
- **SFTP**
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Geben Sie die vom SFTP-Server verwendete Portnummer ein. Der Standardport ist 22.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem SFTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Öffentlicher SSH-Host-Schlüsseltyp (MD5)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine hexadezimale Zeichenfolge mit 32 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Öffentlicher SSH-Host-Schlüsseltyp (SHA256)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine Base64-kodierte Zeichenfolge mit 43 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
- **SIP or VMS (SIP oder VMS)** :
  SIP: Wählen Sie diese Option, um einen SIP-Anruf zu starten.
  VMS: Wählen Sie diese Option, um einen VMS-Anruf zu starten.
  - **From SIP account (Von SIP-Konto)**: Wählen Sie die entsprechende Option aus der Liste aus.
  - **To SIP address (An SIP-Adresse)**: Geben Sie die entsprechende SIP-Adresse ein.
  - **Test**: Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.
- **E-Mail**
  - **Send email to (E-Mail senden an)**: Geben Sie die gewünschte(n) E-Mail-Versandadresse(n) ein. Trennen Sie mehrere Adressen jeweils mit einem Komma.

- **E-Mail senden von**: Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.
- **Benutzername**: Geben Sie den Benutzernamen für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **Kennwort**: Geben Sie das Kennwort für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **Email server (SMTP) (E-Mail-Server (SMTP))**: Geben Sie den Namen des SMTP-Servers ein. Zum Beispiel smtp.gmail.com, smtp.mail.yahoo.com.
- **Port**: Geben Sie die Portnummer des SMTP-Servers ein. Zulässig sind Werte zwischen 0 und 65535. Der Standardport ist 587.
- **Verschlüsselung**: Um die Verschlüsselung zu verwenden, wählen Sie SSL bzw. TLS.
- **Server-Zertifikate validieren**: Wenn Sie eine Verschlüsselung verwenden, wählen Sie diese Option zur Überprüfung der Identität des Geräts. Das Zertifikat kann ein eigensigniertes oder ein von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat sein.
- **POP authentication (POP-Authentifizierung)**: Aktivieren Sie diese Option, um den Namen des POP-Servers einzugeben, z.B. pop.gmail.com.

Hinweis

Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, geplante E-Mails erhalten usw. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, damit Ihr E-Mail-Konto nicht gesperrt wird oder die erwarteten E-Mails nicht verloren gehen.

- **TCP**
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Geben Sie die Nummer des für den Zugriff auf den Server verwendeten Ports ein.

Test: Klicken auf dieses Feld, um die Einrichtung zu überprüfen.

⋮ Das Kontextmenü enthält:

Empfänger anzeigen: Klicken Sie darauf, um die Details zu den Empfängern zu sehen.

Empfänger kopieren: Klicken Sie darauf, um einen Empfänger zu kopieren. Beim Kopieren können Sie Änderungen am neuen Empfänger vornehmen.

Empfänger löschen: Klicken Sie darauf, um den Empfänger dauerhaft zu löschen.

Zeitpläne

Zeitpläne und Impulse können als Bedingungen in Regeln verwendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Zeitpläne und Impulse sowie Informationen zur Konfigurierung auf.

+ **Zeitplan hinzufügen**: Klicken Sie hier, um einen Zeitplan oder Impuls zu erstellen.

Manuelle Auslöser

Mithilfe des manuellen Auslösers können Sie eine Regel manuell auslösen. Der manuelle Auslöser kann beispielsweise zum Validieren von Aktionen beim Installieren und Konfigurieren des Produkts verwendet werden.

MQTT

MQTT (Message Queuing Telemetry Transport) ist ein Standardprotokoll für das Internet der Dinge (IoT). Es wurde für eine vereinfachte IoT-Integration entwickelt und wird in einer Vielzahl von Branchen zum Anschließen von Remote-Geräten mit kleinem Code-Footprint und minimaler Netzwerkbandbreite verwendet. Der MQTT-Client in der Axis Geräte-Firmware kann die Integration der im Gerät erzeugten Daten und Ereignisse in Systeme vereinfachen, bei denen es sich nicht um Video Management Software (VMS) handelt.

Richten Sie das Gerät als MQTT-Client ein. Die MQTT-Kommunikation basiert auf zwei Entitäten, den Clients und dem Broker. Die Clients können Nachrichten senden und empfangen. Der Broker ist für das Routing von Nachrichten zwischen den Clients zuständig.

Weitere Informationen zu MQTT finden Sie im *AXIS OS Portal*.

ALPN

Bei ALPN handelt es sich um eine TLS/SSL-Erweiterung, mit der während der Handshake-Phase der Verbindung zwischen Client und Server ein Anwendungsprotokoll ausgewählt werden kann. Au diese Weise können Sie die MQTT-Datenverkehr über denselben Port zulassen, der für andere Protokolle wie HTTP verwendet wird. In einigen Fällen ist möglicherweise kein dedizierter Port für die MQTT-Kommunikation vorhanden. Eine Lösung besteht in diesem Fall in der Verwendung von ALPN, um die von den Firewalls erlaubte Verwendung von MQTT als Anwendungsprotokoll auf einem Standardport zu nutzen.

MQTT-Client

Verbinden: Aktivieren oder deaktivieren Sie den MQTT-Client.

Status: Zeigt den aktuellen Status des MQTT-Clients an.

Broker

Host: Geben Sie den Host-Namen oder die Adresse des MQTT-Servers ein.

Protokoll: Wählen Sie das zu verwendende Protokoll aus.

Port: Geben Sie die Portnummer ein.

- 1883 ist der Standardwert für **MQTT über TCP**
- 8883 ist der Standardwert für **MQTT über SSL**
- 80 ist der Standardwert für **MQTT über WebSocket**
- 443 ist der Standardwert für **MQTT über WebSocket Secure**

ALPN protocol (ALPN-Protokoll): Geben Sie den Namen des ALPN-Protokolls ein, den Sie vom Anbieter Ihres MQTT-Brokers erhalten haben. Dies gilt nur für MQTT über SSL und MQTT über WebSocket Secure.

Username (Benutzername): Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll.

Kennwort: Geben Sie ein Kennwort für den Benutzernamen ein.

Client-ID: Geben Sie eine Client-ID ein. Die Client-ID wird an den Server gesendet, wenn der Client eine Verbindung herstellt.

Sitzung bereinigen: Steuert das Verhalten bei Verbindung und Trennungszeit. Wenn diese Option ausgewählt ist, werden die Statusinformationen beim Verbinden und Trennen verworfen.

Keep alive interval (Keep-Alive-Intervall): Hiermit kann der Client erkennen, wann der Server nicht mehr verfügbar ist, ohne auf das lange TCP/IP-Timeout warten zu müssen.

Timeout (Zeitüberschreitung): Das Zeitintervall in Sekunden, in dem eine Verbindung hergestellt werden kann. Standardwert: 60

Device topic prefix (Themenpräfix des Geräts): Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registrierkarte **MQTT Client** und in den Veröffentlichungsbedingungen auf der Registrierkarte **MQTT-Veröffentlichung** verwendet.

Reconnect automatically (Automatisch wiederverbinden): Gibt an, ob der Client nach einer Trennung der Verbindung die Verbindung automatisch wiederherstellen soll.

Nachricht zum Verbindungsaufbau

Gibt an, ob eine Nachricht gesendet werden soll, wenn eine Verbindung hergestellt wird.

Nachricht senden: Aktivieren Sie diese Option, damit Nachrichten versendet werden.

Standardeinstellung verwenden: Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

Beibehalten: Wählen Sie diese Option, um den Status des Clients bei diesem **Thema** beizubehalten.

QoS: Ändern Sie die QoS-Ebene für den Paketfluss.

Nachricht zum letzten Willen und Testament

Mit Letzter Wille und Testament (LWT) kann ein Client bei der Verbindung mit dem Broker ein Testament zusammen mit seinen Zugangsdaten bereitstellen. Wenn der Kunde die Verbindung irgendwann später auf nicht ordnungsgemäße Weise abbricht (vielleicht weil seine Stromquelle deaktiviert ist), kann er den Broker eine Nachricht an andere Kunden übermitteln lassen. Diese LWT-Nachricht hat dieselbe Form wie eine normale Nachricht und wird über die gleiche Mechanik geroutet.

Nachricht senden: Aktivieren Sie diese Option, damit Nachrichten versendet werden.

Standardeinstellung verwenden: Deaktivieren Sie diese Option, um Ihre eigene Standardnachricht eingeben zu können.

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

Beibehalten: Wählen Sie diese Option, um den Status des Clients bei diesem **Thema** beizubehalten.

QoS: Ändern Sie die QoS-Ebene für den Paketfluss.

MQTT publication (MQTT-Veröffentlichung)

Use default topic prefix (Standard-Themenpräfix verwenden): Wählen Sie diese Option aus, um das Standard-Themenpräfix zu verwenden, das im Gerätethemenpräfix auf der Registerkarte **MQTT client (MQTT-Client)** definiert ist.

Include topic name (Themanamen einschließen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

Include topic namespaces (Themen-Namespaces einschließen): Wählen Sie diese Option aus, um Namespaces des ONVIF-Themas im MQTT-Thema einzuschließen.

Include serial number (Seriennummer hinzufügen): Wählen Sie diese Option, um die Seriennummer des Geräts in die MQTT-Nutzlast einzuschließen.

+ **Bedingung hinzufügen**: Klicken Sie darauf, um eine Bedingung hinzuzufügen.

Retain (Beibehalten): Definiert, welche MQTT-Meldungen als beibehalten gesendet werden.

- **None (Keine)**: Alle Melden werden als nicht beibehalten gesendet.
- **Property (Eigenschaft)**: Es werden nur statusbehaftete Meldungen als beibehalten gesendet.
- **Alle**: Es werden nur statuslose Meldungen als beibehalten gesendet.

QoS: Wählen Sie die gewünschte Stufe für die MQTT-Veröffentlichung.

MQTT-Abonnements

+ **Abonnement hinzufügen**: Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

Abonnementfilter: Geben Sie das MQTT-Thema ein, das Sie abonnieren möchten.

Themenpräfix des Geräts verwenden: Fügen Sie den Abonnementfilter als Präfix zum MQTT-Thema hinzu.

Abonnementart:

- **Statuslos**: Wählen Sie diese Option, um MQTT-Meldungen in statuslose Meldungen zu konvertieren.
- **Statusbehaftet**: Wählen Sie diese Option, um MQTT-Meldungen in Bedingungen zu konvertieren. Als Status wird der Nutzlast verwendet.

QoS: Wählen Sie die gewünschte Stufe für das MQTT-Abonnement.

Speicher

Network storage (Netzwerk-Speicher)

Ignore (Ignorieren): Aktivieren Sie diese Option, um den Netzwerk-Speicher zu ignorieren.

Add network storage (Netzwerk-Speicher hinzufügen): Klicken Sie auf diese Option zum Hinzufügen einer Netzwerk-Freigabe, auf der Sie Aufzeichnungen speichern können.

- **Adresse**: Geben Sie die IP-Adresse des Host-Servers, in der Regel ein NAS (Network Attached Storage), ein. Wir empfehlen Ihnen, den Host für eine statische IP-Adresse zu konfigurieren (nicht DHCP, da sich eine dynamische IP-Adresse ändern kann) oder DNS zu verwenden. Namen des Typs Windows SMB/CIFS werden nicht unterstützt.
- **Netzwerk-Freigabe**: Geben Sie den Namen des freigegebenen Speicherorts auf dem Host-Server ein. Mehrere Axis Geräte können dieselbe Netzwerk-Freigabe verwenden, da jedes Gerät einen eigenen Ordner erhält.
- **User (Benutzer)**: Wenn der Server eine Anmeldung erfordert, geben Sie den Benutzernamen ein. Zur Anmeldung an einem bestimmten Domainserver geben Sie `DOMAIN\Benutzername` ein.
- **Kennwort**: Wenn der Server eine Anmeldung erfordert, geben Sie das Kennwort ein.
- **SMB-Version**: Wählen Sie die SMB-Speicherprotokollversion für die Verbindung mit dem NAS. Wenn Sie **Auto** wählen, versucht das Gerät, eine der sicheren Versionen SMB zu installieren: 3.02, 3.0 oder 2.1. Wählen Sie 1.0 oder 2.0 zur Herstellung einer Verbindung zu älteren NAS, die höhere Versionen nicht unterstützen. Weitere Informationen zur SMB-Unterstützung in Axis Geräten finden Sie *hier*.
- **Freigabe hinzufügen, auch wenn der Verbindungstest fehlschlägt**: Wählen Sie diese Option, um die Netzwerk-Freigabe hinzuzufügen, auch wenn während des Verbindungstests ein Fehler erkannt wurde. Bei dem Fehler kann es beispielsweise sein, dass Sie kein Kennwort eingegeben haben, obwohl für den Server ein Kennwort erforderlich ist.

Remove network storage (Netzwerk-Speicher entfernen): Klicken Sie hier, um die Verbindung zur Netzwerk-Freigabe zu trennen, zu lösen oder zu entfernen. Dadurch werden alle Einstellungen für die Netzwerk-Freigabe entfernt.

Unbind (Lösen): Klicken Sie hier, um die Netzwerk-Freigabe zu lösen und zu trennen.
Bind (Zuweisen): Klicken Sie hier, um die Netzwerk-Freigabe zuzuweisen und zu verbinden.

Unmount (Trennen): Klicken Sie hier, um die Netzwerk-Freigabe zu trennen.
Mount (Einbinden): Klicken Sie hier, um die Netzwerk-Freigabe einzubinden.

Write protect (Schreibschutz): Aktivieren Sie diese Option, damit nicht mehr auf die Netzwerk-Freigabe geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte Netzwerk-Freigabe kann nicht formatiert werden.

Retention time (Aufbewahrungszeit): Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Datenmenge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn der Netzwerk-Speicher voll ist, werden alte Aufzeichnungen gelöscht, bevor der ausgewählte Zeitraum verstrichen ist.

Tools (Werkzeuge)

- **Test connection (Verbindung testen)**: Prüfen Sie die Verbindung zur Netzwerk-Freigabe.
- **Format (Formatieren)**: Formatieren Sie die Netzwerk-Freigabe, wenn zum Beispiel schnell alle Daten gelöscht werden müssen. CIFS ist die verfügbare Dateisystemoption.

Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Integrierter Speicher

Wichtig

Gefahr von Datenverlust und Beschädigung von Aufzeichnungen. Die SD-Karte darf nicht entfernt werden, während das Gerät in Betrieb ist. Trennen Sie die SD-Karte, bevor Sie sie entfernen.

Trennen: Klicken Sie hier, um die SD-Karte sicher zu entfernen.

Schreibschutz: Aktivieren Sie diese Option, damit nicht mehr auf die SD-Karte geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte SD-Karte kann nicht formatiert werden.

Autoformat (Automatisch formatieren): Aktivieren Sie diese Option, um eine neu eingesetzte SD-Karte automatisch zu formatieren. Sie wird als Dateisystem ext4 formatiert.

Ignorieren: Aktivieren Sie diese Option, um die Speicherung der Aufzeichnungen auf der SD-Karte zu beenden. Wenn Sie die SD-Karte ignorieren, erkennt das Gerät nicht mehr, dass die Karte vorhanden ist. Diese Einstellung steht nur Administratoren zur Verfügung.

Aufbewahrungszeit: Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Datenmenge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn die SD-Karte voll ist, werden alte Aufzeichnungen gelöscht, bevor der ausgewählte Zeitraum verstrichen ist.

Werkzeuge

- **Überprüfen**: Überprüfen Sie die SD-Speicherkarte auf Fehler. Diese Funktion steht nur für das Dateisystem ext4 zur Verfügung.
- **Reparieren**: Beheben Sie Fehler im Dateisystem ext4. Um eine SD-Karte mit dem Dateisystem VFAT zu reparieren, werfen Sie die SD-Karte aus und setzen Sie sie einem Computer ein, bevor Sie die Festplattenreparatur durchführen.
- **Format (Formatieren)**: Formatieren Sie die SD-Karte zum Beispiel, wenn das Dateisystem geändert oder alle Daten schnell gelöscht werden sollen. Die beiden verfügbaren Dateisysteme sind VFAT und ext4 Das Format ext4 wird wegen des Schutzes vor Datenverlust beim Auswerfen der Karte oder bei plötzlichem Stromausfall empfohlen. Sie benötigen jedoch einen externen ext4-Treiber oder eine Anwendung, um unter Windows® auf das Dateisystem zuzugreifen.
- **Encrypt (Verschlüsseln)**: Verwenden Sie dieses Tool, um die SD-Karte zu formatieren und die Verschlüsselung zu aktivieren. **Encrypt (Verschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Verschlüsselung mit **Encrypt** sind alle auf der SD-Karte gespeicherten Daten mittels Verschlüsselung geschützt.
- **Decrypt (Entschlüsseln)**: Verwenden Sie dieses Tool, um die SD-Karte ohne Verschlüsselung zu formatieren. **Decrypt (Entschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Entschlüsselung mit **Decrypt** sind die auf der SD-Karte gespeicherten Daten nicht mehr mittels Verschlüsselung geschützt.
- **Change password (Kennwort ändern)**: Andern Sie das zum Verschlüsseln der SD-Karte erforderliche Kennwort.

Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Wear trigger (Auslöser für Abnutzung): Legen Sie einen Wert für die Abnutzung der SD-Speicherkarte fest, bei dem eine Aktion ausgelöst werden soll. Der Abnutzungsgrad reicht von 0 bis 200 %. Eine neue SD-Karte, die noch nie verwendet wurde, hat einen Abnutzungsgrad von 0 %. Ein Abnutzungsgrad von 100 % gibt an, dass die zu erwartende Lebensdauer der SD-Karte bald abläuft. Wenn der Abnutzungsgras 200% erreicht, besteht ein hohes Risiko einer Fehlfunktion der SD-Karte. Wir empfehlen Ihnen, den Auslöser für Abnutzung auf 80 bis 90 % einzustellen. Dadurch haben Sie Zeit, Aufzeichnungen herunterzuladen und die SD-Karte zu ersetzen, bevor sie möglicherweise abgebnutzt ist. Mit dem Auslöser für Abnutzung können Sie ein Ereignis einrichten und sich eine Benachrichtigung senden lassen, wenn der Abnutzungsgrad den von Ihnen festgelegten Wert erreicht.

Integrierter Speicher

Festplatte

- **Frei**: Freier Platz auf dem Datenträger.
- **Status**: Ob das Laufwerk bereitsteht ist oder nicht.
- **File system (Dateisystem)**: Das von der Festplatte verwendete Dateisystem.
- **Encrypted (Verschlüsselt)**: Ob das Laufwerk verschlüsselt ist oder nicht.
- **Temperatur**: Die aktuelle Temperatur der Hardware.
- **Allgemeiner Zustandstest**: Das Ergebnis nach Überprüfung des Datenträgerzustands.

Werkzeuge

- **Überprüfen**: Überprüfen Sie das Speichergerät auf Fehler und versuchen Sie es automatisch zu reparieren.
- **Reparieren**: Reparieren Sie das Speichergerät. Während der Reparatur werden laufende Aufzeichnungen unterbrochen. Das Reparieren eines Speichergeräts kann zu einem Datenverlust führen.
- **Formatieren**: Löschen Sie alle Aufzeichnungen und formatieren Sie das Speichergerät. Wählen Sie ein Dateisystem.
- **Encrypt (Verschlüsseln)**: Gespeicherte Daten verschlüsseln.
- **Decrypt (Entschlüsseln)**: Gespeicherte Daten entschlüsseln. Alle Dateien auf dem Speichergerät werden vom System gelöscht.
- **Change password (Kennwort ändern)**: Ändern Sie das Kennwort für die Festplattenverschlüsselung. Das Ändern des Kennworts beeinträchtigt laufende Aufzeichnungen nicht.
- **Werkzeug verwenden**: Klicken Sie hier, um das ausgewählte Werkzeug ausführen zu können.

Unmount (Trennen) : Klicken Sie, bevor Sie das Gerät vom System trennen. Dies beendet alle laufenden Aufzeichnungen.

Write protect (Schreibschutz): Aktivieren Sie dies, um das Speichergerät gegen Überschreiben zu schützen.

Autoformat (Automatisch formatieren) : Das Laufwerk wird automatisch mit dem ext4-Dateisystem formatiert.

SIP

Settings (Einstellungen)

Das Session Initiation Protocol (SIP) wird für die Kommunikation zwischen Benutzern verwendet. Die Sitzungen können Audio- und Videoelemente enthalten.

SIP aktivieren: Markieren Sie diese Option, um SIP-Anrufe zu starten und zu empfangen.

Eingehende Anrufe zulassen: Wählen Sie diese Option, um eingehende Anrufe von anderen SIP-Geräten zuzulassen.

Call handling (Anrufbearbeitung)

- **Calling timeout (Zeitüberschreitung bei Anruf)**: Legen Sie die maximale Dauer eines Anrufversuchs fest, wenn niemand antwortet.
- **Incoming call duration (Dauer des eingehenden Anrufs)**: Legen Sie die maximale Dauer für einen eingehenden Anruf (maximal 10 Minuten) fest.
- **End calls after (Anrufe beenden nach)**: Legen Sie die maximale Anrufdauer (maximal 60 Minuten) fest. Wählen Sie **Infinite call duration (Unendliche Anrufdauer)**, wenn Sie die Dauer eines Anrufs nicht begrenzen möchten.

Ports

Eine Portnummer muss zwischen 1024 und 65535 liegen.

- **SIP-Port**: Der für die SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Die Standardportnummer ist 5060. Bei Bedarf eine andere Portnummer eingeben.
- **TLS_Port**: Der für verschlüsselte SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Die Standardportnummer ist 5061. Bei Bedarf eine andere Portnummer eingeben.
- **RTP-Startport**: Der Netzwerkport, der für den ersten RTP-Medienstream in einem SIP-Anruf verwendet wird. Der Standardstartport ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern.

NAT-Traversal

NAT (Network Address Translation) verwenden, wenn sich das Gerät in einem privaten Netzwerk befindet und auch von außerhalb verfügbar sein soll.

Hinweis

NAT-Traversal muss vom Router unterstützt werden. Der Router muss außerdem UPnP® unterstützen.

Die Protokolle von NAT Traversal können einzeln oder in verschiedenen Kombinationen verwendet werden, die sich nach der Netzwerkumgebung richten.

- **ICE**: Das Protokoll ICE (Interactive Connectivity Establishment) erhöht die Chancen, den effizientesten Kommunikationspfad zwischen gleichrangigen Geräten zu finden. Mit dem Aktivieren von STUN und TURN werden die Chancen des ICE-Protokolls nochmals verbessert.
- **STUN**: STUN (Session Traversal Utilities for NAT) ist ein Client-Server-Netzwerkprotokoll, an dem das Gerät erkennt, ob sie sich hinter einer NAT oder Firewall befinden. Zudem werden mit diesem Protokoll öffentlich verortete IP-Adressen (NAT-Adressen) und Portnummern abgerufen, die von NAT für Verbindungen mit Remote-Hosts zugewiesen wurden. Die STUN-Server-Adresse eingeben, zum Beispiel eine IP-Adresse.
- **TURN**: TURN (Traversal Using Relays around NAT) ist ein Protokoll, mit dem Geräte hinter einem NAT-Router oder einer Firewall über TCP oder UDP Daten von anderen Hosts empfangen können. Geben Sie die TURN-Server-Adresse und die Anmeldedaten ein.

Audio und Video

- **Audio-Codec-Priorität**: Wählen Sie mindestens einen Audiocodec, um SIP-Anrufe in der gewünschten Audioqualität zu ermöglichen. Ändern Sie die Prioritätsreihenfolge per Drag & Drop.

Hinweis

Die gewählten Codecs müssen mit dem Codec des Anrufempfängers übereinstimmen, da dieser für den Anruf entscheidend ist.

- **Audioausrichtung**: Wählen Sie zulässige Audiorichtungen.
- **H.264-Paketierungsmodus**: Wählen Sie den zu verwendenden Paketierungsmodus aus.
  - **Auto**: (Empfohlen) Das Gerät entscheidet, welcher Paketierungsmodus verwendet wird.
  - **Keinen**: Es wird kein Paketierungsmodus festgelegt. Dieser Modus wird häufig als Modus **0** bezeichnet.
  - **0**: Nicht-verschachtelter Modus.
  - **1**: Modus für eine einzelne NAL-Einheit.
- **Videoausrichtung**: Wählen Sie zulässige Videorichtungen.

Zusätzliches

- **Wechsel von UDP zu TCP**: Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll (User Datagram Protocol) auf das Protokoll TCP (Transmission Control Protocol) zu wechseln. Mit einem Wechsel wird Fragmentierung vermieden und der Wechsel kann stattfinden sofern eine Anfrage innerhalb von 200 Bytes der maximalen Übertragungseinheit (MTU) liegt oder größer als 1300 Byte ist.
- **Über Umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Kontakt umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Alle ... am Server registrieren**: Legen Sie fest, wie oft sich das Gerät am SIP-Server für SIP-Konten registrieren soll.
- **DTMF-Nutzlasttyp**: Ändert den Standard-Nutzlasttyp für DTMF.

Accounts (Konten)

Alle aktuellen SIP-Konten sind unter **SIP accounts (SIP-Konten)** aufgeführt. Der farbige Kreis zeigt den Status von registrierten Konten an.

Das Konto wurde erfolgreich beim SIP-Server registriert.

Es liegt bei diesem Konto ein Problem vor. Mögliche Gründe: Autorisierungsfehler, falsche Kontendaten oder der SIP-Server kann das Konto nicht ermitteln.

Ein **Peer-to-peer (Standard)** Konto ist ein automatisch erstelltes Konto. Sobald mindestens ein weiteres Konto erstellt ist, kann das automatisch erstellte Konto gelöscht werden und das neu eingerichtete Konto als Standardkonto gewählt werden. Das Standardkonto wird immer für Anrufe über die programmierbare Schnittstelle VAPIX® Application Programming Interface (API) verwendet, wenn kein SIP-Senderkonto angegeben ist.

Add account (Konto hinzufügen): Klicken Sie darauf, um ein neues SIP-Konto zu erstellen.

- **Active (Aktiv)**: Wählen Sie diese Option, um das Konto nutzen zu können.
- **Als Standard setzen**: Mit dieser Option dieses Konto als Standardkonto verwenden. Es muss ein und nur ein Standardkonto vorhanden sein.
- **Answer automatically (Automatisch annehmen)**: Einen eingehenden Anruf automatisch annehmen.
- **Prioritize IPv6 over IPv4 (IPv6 über IPv4 bevorzugen)** : Wählen Sie diese Option aus, um IPv6-Adressen gegenüber IPv4-Adressen zu bevorzugen. Dies ist nützlich, wenn Verbindungen zu Peer-to-Peer-Konten oder Domänennamen hergestellt werden, die sowohl in IPv4- als auch in IPv6-Adressen auflösen. IPv6 kann nur für Domänennamen priorisiert werden, die IPv6-Adressen zugeordnet sind.
- **Name**: Geben Sie einen beschreibenden Namen ein. Das kann zum Beispiel ein Vor- und Nachname, eine Funktion oder ein Standort sein. Der Name muss nicht eindeutig sein.
- **Benutzer-ID**: Geben Sie die dem Axis Gerät zugeordnete eindeutige Telefonnummer oder Durchwahl an.
- **Peer-to-Peer**: Für Direktanrufe an ein anderes SIP-Gerät im lokalen Netzwerk.
- **Registriert**: Für Anrufe an SIP-Geräte außerhalb des lokalen Netzwerks über einen SIP-Server.
- **Domain**: Sofern verfügbar, geben Sie den Domainnamen ein. Dieser wird bei Anrufen bei anderen Konten als Teil der SIP-Adresse angezeigt.
- **Kennwort**: Geben Sie zum Authentifizieren am SIP-Server das dem SIP-Konto zugeordnete Kennwort ein.
- **Authentifizierungs-ID**: Geben Sie die Authentifizierungs-ID für den SIP-Server ein. Wenn diese mit der Benutzer-ID identisch ist, muss sie nicht gesondert eingegeben werden.
- **Anrufer-ID**: Der dem Empfänger der von diesem Gerät aus getätigten Anrufe angezeigte Name.
- **Registrierungsstelle**: Geben Sie die IP-Adresse der Registrierungsstelle ein.
- **Übertragungsmodus**: Den SIP-Übertragungsmodus für das Konto wählen: UPD, TCP oder TLS.
- **TLS version** (nur mit Übertragungsmodus TLS): Wählen Sie die zu verwendende TLS-Version. Die Versionen **v1.2** und **v1.3** sind die sichersten. **Automatic (Automatisch)** wählt die sicherste Version aus, die das System verarbeiten kann.
- **Media encryption (Medienverschlüsselung)** (nur mit Übertragungsmodus TLS): Die Art der Verschlüsselung für Medien (Audio und Video) für SIP-Anrufe wählen.
- **Zertifikat** (nur mit Übertragungsmodus TLS): Ein Zertifikat wählen.
- **Server-Zertifikat überprüfen** (nur mit Übertragungsmodus TLS): Markieren Sie diese Option, um das Server-Zertifikat zu überprüfen.
- **Sekundärer SIP-Server**: Aktivieren Sie diese Option, damit bei fehlgeschlagener Registrierung am primären SIP-Server das Gerät versucht, sich am sekundären SIP-Server zu registrieren.
- **SIP secure (SIP-Secure)**: Diese Option zum Verwenden von Secure Session Initiation Protocol (SIPS) wählen. SIPS verwendet zum Verschlüsseln den Übertragungsmodus TLS.
- **Proxys**
  - **Proxy**: Klicken Sie darauf, um einen Proxy hinzuzufügen.
  - **Priorisieren**: Klicken Sie darauf, um Proxys zu priorisieren, wenn Sie zwei oder mehrere davon haben.
  - **Server-Adresse**: Geben Sie die IP-Adresse des primären SIP-Servers ein.
  - **Username (Benutzername)**: Falls verlangt, einen Benutzernamen für den SIP-Proxyserver eingeben.
  - **Kennwort**: Geben Sie das Kennwort für den SIP-Proxyserver ein, falls erforderlich.
- **Video**
  - **Sichtbereich**: Wählen Sie den für Videoanrufe zu verwendenden Sichtbereich. Ohne Auswahl wird die Standardansicht verwendet.

- **Auflösung**: Wählen Sie die für Videoanrufe zu verwendende Auflösung. Die Auflösung wirkt sich auf die erforderliche Bandbreite aus.
- **Bildrate**: Wählen Sie die Bildrate für Videoanrufe auf. Die Bildrate wirkt sich auf die erforderliche Bandbreite aus.
- **H.264 profile (Profil H.264)**: Wählen Sie das Profil aus, das für Videoanrufe verwendet werden soll.

Test call (Testanruf)

SIP account (SIP-Konto): Wählen Sie das Konto, von dem aus der Testanruf durchgeführt werden soll.

SIP-Adresse: Geben Sie eine SIP-Adresse ein und klicken Sie auf , um einen Testanruf zu tätigen und sicherzustellen, dass das Konto funktioniert.

Videostreamprofile

Ein Videostreamprofil besteht aus einer Gruppe von Einstellungen, die sich auf den Videostream auswirken. Videostreamprofile können in verschiedenen Situationen verwendet werden, z. B. bei der Erstellung von Ereignissen und der Verwendung von Aufzeichnungsregeln.

Add stream profile (Videostreamprofil hinzufügen): Klicken Sie, um ein neues Videostreamprofil zu erstellen.

Preview (Vorschau): Vorschau des Videostreams mit den ausgewählten Einstellungen des Videostreamprofils. Die Vorschau wird aktualisiert, wenn Sie die Einstellungen auf der Seite ändern. Wenn Ihr Gerät unterschiedliche Sichtbereiche hat, können Sie den Sichtbereich in der Dropdown-Ansicht in der unteren linken Ecke des Bildes ändern.

Name: Fügen Sie einen Namen für Ihr Profil hinzu.

Description (Beschreibung): Fügen Sie eine Profilbeschreibung hinzu.

Video codec (Video-Codec): Wählen Sie den Video-Codec aus, der für das Profil verwendet werden soll.

Resolution (Auflösung): Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Frame rate (Bildrate): Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Compression (Komprimierung): Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Zipstream : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Optimize for storage (Für Speicherung optimieren) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Dynamic FPS (Dynamische Bilder pro Sekunde) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Dynamic GOP (Dynamic Group of Pictures) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Mirror (Spiegelung) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

GOP length (GOP-Länge) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Bitrate control (Bitratensteuerung): Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

Include overlays (Overlays einbeziehen): Wählen Sie den Typ der einzubeziehenden Overlays aus. Weitere Informationen zum Hinzufügen von Overlays finden Sie unter *Overlays auf Seite 44*.

Include audio (Audio einbeziehen) : Siehe *Videostream auf Seite 42* für eine Beschreibung dieser Einstellung.

ONVIF

ONVIF-Konten

ONVIF (Open Network Video Interface Forum) ist ein globaler Schnittstellenstandard, der Endbenutzern, Integratoren, Beratern und Herstellern die Nutzung der Vorteile von Netzwerk-Videotechnologie erleichtert. ONVIF sorgt für die Kompatibilität zwischen Produkten unterschiedlicher Hersteller, erhöhte Flexibilität, verringerte Kosten und zukunftssichere Systeme.

Beim Erstellen eines ONVIF-Kontos wird automatisch die ONVIF-Kommunikation aktiviert. Verwenden Sie den Kontonamen und das Kennwort für sämtliche ONVIF-Kommunikation mit dem Gerät. Weitere Informationen finden Sie auf den Seiten für die Axis Developer Community auf *axis.com*.

Add accounts (Konten hinzufügen): Klicken Sie darauf, um ein neues ONVIF-Konto hinzuzufügen.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

Neues Kennwort: Geben Sie ein Kennwort für das Konto ein. Kennwörter müssen aus 1 bis 64 Zeichen bestehen. Für das Kennwort sind nur die druckbaren Zeichen des ASCII-Codes (Code 32 bis 126), also Buchstaben, Ziffern, Satzzeichen sowie einige Sonderzeichen zulässig.

Repeat password (Kennwort wiederholen): Geben Sie das gleiche Kennwort erneut eingeben.

Rolle:

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener)**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**einstellungen.
  - Apps werden hinzugefügt.
- **Media account (Medienkonto)**: Erlaubt nur Zugriff auf den Videostream.

Das Kontextmenü enthält:

Update account (Konto aktualisieren): Bearbeiten Sie die Eigenschaften des Kontos.

Delete account (Konto löschen): Das Konto löschen. Das Root-Konto kann nicht gelöscht werden.

ONVIF-Medienprofile

Ein ONVIF-Medienprofil besteht aus einem Satz von Konfigurationen, mit deren Hilfe Sie die Medienstreameinstellungen ändern können.

Medienprofil hinzufügen: Klicken Sie darauf, um ein neues ONVIF-Medienprofil hinzuzufügen.

profile_x: Klicken Sie auf ein Profil, um es zu bearbeiten.

Analytische Metadaten

Metadatenproduzenten

Listet die Apps auf, die Metadaten streamen, sowie die Kanäle, die sie verwenden.

Producer (Produzent): Die App, die Metadaten erzeugt. Unterhalb der App befindet sich eine Liste der Metadatentypen, die die App vom Gerät streamt.

Kanal: Der Kanal, den die App verwendet. Wählen Sie diese Option, um den Metadatenstream zu aktivieren. Deaktivieren Sie diese Option aus Gründen der Kompatibilität oder Ressourcenverwaltung.

Melder

Kameramanipulation

Der Manipulationsmelder der Kamera generiert einen Alarm, wenn sich die Szene ändert, beispielsweise wenn das Objektiv abgedeckt, besprüht oder stark defokussiert ist, und die in **Trigger delay (Verzögerung beim Auslösen)** festgelegte Zeit verstrichen ist. Der Manipulationsmelder wird nur aktiviert, wenn die Kamera mindestens 10 Sekunden lang nicht bewegt wurde. In dieser Zeit richtet der Melder ein Szenemodell ein, um durch einen Vergleich Manipulationen in aktuellen Bildern zu erkennen. Stellen Sie zur ordnungsgemäßen Einrichtung des Szenemodells sicher, dass die Kamera fokussiert ist, die Lichtbedingungen stimmen und die Kamera nicht auf eine konturlose Szene wie etwa eine leere Wand gerichtet ist. Die Funktion Kamera-Manipulation kann auch als Bedingung für das Auslösen von Aktionsregeln verwendet werden.

Verzögerung beim Auslösen: Geben Sie ein, wie lange die Manipulationsbedingungen gegeben sein müssen, bevor der Alarm ausgelöst wird. So können falsche Alarme bei bekannten Bedingungen, die das Bild beeinträchtigen, verhindert werden.

Auslösen bei dunklem Bild: Es ist schwer möglich einen Alarm zu generieren, wenn das Kameraobjektiv besprüht wird, denn dieses Ereignis ist unmöglich von anderen Situationen zu unterscheiden, in denen der gleiche Effekt auftritt, also wenn sich etwa die Lichtverhältnisse ändern. Aktivieren Sie diese Einstellung, um in allen Fällen, in denen sich das Bild verdunkelt, Alarme zu erzeugen. Wenn das Gerät ausgeschaltet ist, erzeugt es keinen Alarm, wenn sich das Bild verdunkelt.

Hinweis

Zur Erfassung von Manipulationsversuchen in statischen und nicht überfüllten Szenen.

Audioerkennung

Diese Einstellungen sind für jeden Audioeingang verfügbar.

Lautstärke: Die Lautstärke kann auf einen Wert von 0 bis 100 festgelegt werden, wobei 0 die empfindlichste und 100 die unempfindlichste Einstellung ist. Richten Sie die Lautstärke mithilfe der Aktivitätsanzeige als Richtwert ein. Beim Erstellen von Ereignissen kann der Schallpegel als Bedingung verwendet werden. Sie können wählen, ob eine Aktion ausgelöst werden soll, wenn der Schallpegel den eingestellten Wert übersteigt, unter- oder überschreitet.

Stoßerkennung

Stoßmelder: Aktivieren Sie diese Option, damit ein Alarm erzeugt wird wenn das Gerät von einem Objekt getroffen oder manipuliert wird.

Empfindlichkeitsstufe: Bewegen Sie den Schieberegler, um die Empfindlichkeitsstufe einzustellen, bei der das Gerät einen Alarm erzeugen soll. Bei einem niedrigen Wert erzeugt das Gerät nur bei starkem Schlag einen Alarm. Bei einem hohen Wert erzeugt das Gerät schon bei leichter Manipulation einen Alarm.

Videoausgang

Energieeinstellungen

Energieeinstellungen

Delayed shutdown (Verzögerte Abschaltung) : Aktivieren Sie dies, wenn Sie eine Verzögerung vor dem Ausschalten der Stromversorgung festlegen möchten.

Delay time (Verzögerungszeit) : Legen Sie eine Verzögerung von 1 bis 60 Minuten fest.

Power saving mode (Energiesparmodus) : Aktivieren Sie diese Option, um das Gerät in den Energiesparmodus zu schalten. Wenn Sie den Energiesparmodus aktivieren, ist die Reichweite der IR-Beleuchtung herabgesetzt.

Set power configuration (Energieversorgungskonfiguration einstellen): Ändern Sie die Energieversorgungskonfiguration, indem Sie eine andere PoE-Klasse aus den Optionen auswählen. Klicken Sie auf **Save and restart (Speichern und Neustart)**, um die Änderung zu speichern.

Hinweis

Wenn Sie die Stromversorgung auf PoE Klasse 3 festlegen, wird das Profil **Low power profile (Niedrigspannung)** empfohlen, wenn Ihr Gerät über diese Option verfügt.

Zubehör

E/A-Ports

Schließen Sie externe Geräte über digitale Eingänge an, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können, wie etwa PIR-Sensoren, Tür- oder Fensterkontakte und Glasbruchmelder.

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

Port

Name: Bearbeiten Sie den Text, um den Port umzubenennen.

Direction (Richtung): gibt an, dass es sich bei dem Port um einen Eingangsport handelt. gibt an, dass es sich um einen Ausgangsport handelt. Wenn der Port konfigurierbar ist, können Sie auf die Symbole klicken, um zwischen Eingang und Ausgang zu wechseln.

Normal state (Normalzustand): Klicken Sie auf für einen geöffneten Schaltkreis" und auf für einen geschlossenen Schaltkreis.

Current state (Aktueller Status): Zeigt den aktuellen Status der Ports an. Der Ein- oder Ausgang wird aktiviert, wenn der aktuelle Zustand vom Normalzustand abweicht. Ein Eingang am Gerät ist offen, wenn er getrennt ist oder eine Spannung von mehr als 1 V Gleichstrom anliegt.

Hinweis

Der Schaltkreis des Ausgangs ist während eines Neustarts offen. Nach abgeschlossenem Neustart nimmt der Schaltkreis wieder die normale Position an. Wenn die Einstellungen auf dieser Seite geändert werden, nehmen die Schaltkreise der Ausgänge wieder ihre jeweiligen normalen Positionen an, wobei es unerheblich ist, ob aktive Auslöser vorliegen.

Supervised (Überwacht) : Aktivieren Sie diese Option, um Aktionen zu erkennen und auszulösen, wenn jemand die Verbindung zu digitalen E/A-Geräten manipuliert. Sie können nicht nur erkennen, ob ein Eingang geöffnet oder geschlossen ist, sondern auch, ob jemand diesen manipuliert hat (d. h. abgeschnitten oder gekürzt). Zur Überwachung der Verbindung ist im externen E/A-Kreis zusätzliche Hardware (Abschlusswiderstände) erforderlich.

Edge-to-Edge

Koppelung

Mit der Kopplung können kompatible Netzwerk-Lautsprecher oder Mikrofone von Axis so eingesetzt werden, als seien sie Teil der Kamera. Nach den Kopplung fungiert der Netzwerk-Lautsprecher als Audioausgabegerät, mit dem Audioclips abgespielt und Audio über die Kamera übertragen kann. Das Netzwerkmikrofon nimmt Geräusche aus der Umgebung auf und stellt sie als Audioeingabegerät zur Verfügung, das in Medienstreams und Aufnahmen verwendet werden kann.

Wichtig

Um diese Funktion mit einer Video Management Software (VMS) verwenden zu können, koppeln Sie zuerst die Kamera mit dem Lautsprecher oder Mikrofon und fügen dann Ihrer VMS die Kamera hinzu.

Legen Sie in der Ereignisregel ein Limit für „Zwischen Aktionen warten (hh:mm:ss)" fest, wenn Sie ein mit dem Netzwerk gekoppeltes Audiogerät in einer Ereignisregel mit „Audioerfassung" als Bedingung und „Wiedergabe von Audio-Clips" als Aktion verwenden. Damit wird eine Rückkopplungsschlaufe vermieden, wenn das erfassende Mikrofon Audio vom Lautsprecher mit aufnimmt.

Adresse: Geben Sie den Host-Namen oder die IP-Adresse des Netzwerk-Lautsprechers ein.

Username (Benutzername): Geben Sie den Benutzernamen ein.

Password (Kennwort): Geben Sie ein Benutzerkennwort ein.

Speaker pairing (Lautsprecher-Kopplung): Wählen Sie diese Option, um einen Netzwerk-Lautsprecher zu koppeln.

Microphone pairing (Mikrofon-Kopplung): Wählen Sie diese Option, um ein Mikrofon zu koppeln.

Clear fields (Felder löschen): Klicken Sie hier, um alle Felder zu löschen.

Connect (Verbinden): Klicken Sie hier, um eine Verbindung mit dem Lautsprecher oder Mikrofon herzustellen.

Protokolle

Protokolle und Berichte

Berichte

- **View the device server report (Geräteserver-Bericht anzeigen)**: Zeigt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugangsprotokoll wird automatisch dem Server-Bericht angefügt.
- **Download the device server report (Bericht zum Geräteserver herunterladen)**: Dabei wird eine .zip-Datei mit dem vollständigen Server-Bericht als Textdatei im Format UTF-8 sowie einem Schnappschuss der aktuellen Live-Ansicht erstellt. Schließen Sie beim Kontakt mit dem Support stets die ZIP-Datei des Server-Berichts ein.
- **Download the crash report (Absturzbericht herunterladen)**: So wird ein Archiv mit ausführlichen Informationen zum Produktstatus heruntergeladen. Der Absturzbericht enthält die im Server-Bericht enthaltenen Informationen sowie ausführliche Debug-Informationen. Dieser Bericht enthält möglicherweise vertrauliche Daten wie z. B. Netzwerk-Traces. Es kann einige Minuten dauern, bis der Bericht generiert wird.

Protokolle

- **Systemprotokoll sehen**: Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **View the access log (Zugangsprotokoll anzeigen)**: Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekennwort verwendet wurde.

Netzwerk-Trace

Wichtig

Eine Datei zum Netzwerk-Trace enthält möglicherweise vertrauliche Informationen wie Zertifikate oder Kennwörter.

Ein Netzwerk-Trace hilft durch die Aufzeichnung von Aktivitäten im Netzwerk beim Beheben von Problemen.

Trace time (Trace-Dauer): Geben Sie die Dauer des Trace in Sekunden oder Minuten an und klicken Sie auf **Download (Herunterladen)**.

Remote-Systemprotokoll

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.

+ **Server**: Klicken Sie, um einen neuen Server hinzuzufügen.

Host: Geben Sie den Host-Namen oder die IP-Adresse des Servers ein.

Format: Wählen Sie das zu verwendende syslog-Nachrichtenformat aus.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokoll): Wählen Sie das zu verwendende Protokoll und den zu verwendenden Port aus:

- UDP (Standardport ist 514)
- TCP (Standardport ist 601)
- TLS (Standardport ist 6514)

Schweregrad: Wählen Sie aus, welche Nachrichten gesendet werden sollen, wenn diese ausgelöst werden.

CA-Zertifikat einrichten: Sehen Sie sich die aktuellen Einstellungen an oder fügen Sie ein Zertifikat hinzu.

Direktkonfiguration

Direktkonfiguration ist für fortgeschrittene Benutzer mit Erfahrung bei der Konfiguration von Axis Geräten vorgesehen. Die meisten Parameter können auf dieser Seite eingestellt und bearbeitet werden.

Wartung

Neustart: Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.

Wiederherstellen: Setzten Sie die *meisten Einstellungen* auf die Werkseinstellungen zurück. Anschließend müssen Sie Gerät und Apps neu konfigurieren, nicht vorinstallierte Apps neu installieren sowie Ereignisse und PTZ-Voreinstellungen neu erstellen.

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

- Boot-Protokoll (DHCP oder statisch)
- Statische IP-Adresse
- Standardrouter
- Subnetzmaske
- Einstellungen für 802.1X
- Einstellungen für O3C

Werkseinstellungen: Setzten Sie *alle* Einstellungen werden auf die Werkseinstellungen zurück. Anschließend müssen Sie die IP-Adresse zurücksetzen, um auf das Gerät zugreifen zu können.

Hinweis

Sämtliche Firmware des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Firmware auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper "Signierte Firmware, sicherer Start und Sicherheit von Privatschlüsseln" auf *axis.com*.

Firmwareaktualisierung: Aktualisieren Sie auf eine neue Firmwareversion. Neue Firmwareversionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu *axis.com/support*.

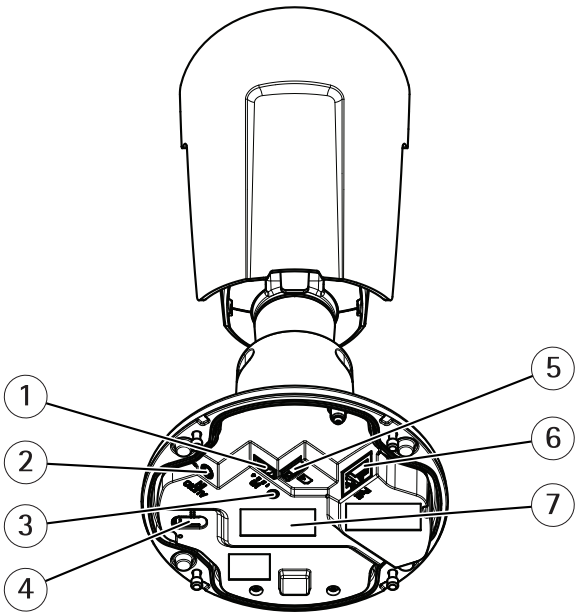
Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standardaktualisierung**: Aktualisieren Sie auf die neue Firmwareversion.
- **Werkseinstellungen**: Aktualisieren und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen Firmwareversion zurückkehren.
- **Automatisches Zurücksetzen**: Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige Firmwareversion zurückgesetzt.

Firmware zurücksetzen: Gehen Sie auf die vorherige Firmwareversion zurück.

Technische Daten

Produktübersicht



1 *E/A-Anschluss*
2 *Audioanschluss*
3 *LED-Statusanzeige*
4 *Steuertaste*
5 *Einschub für microSD-Karte*
6 *Netzwerk-Anschluss*
7 *Teilenummer (P/N) und Seriennummer (S/N)*

LEDs

LED-Statusanzeige	Bedeutung
Leuchtet nicht	Anschluss und Normalbetrieb.
Grün	Leuchtet bei Normalbetrieb nach Abschluss des Startvorgangs 10 Sekunden dauerhaft grün.
Gelb	Leuchtet beim Start. Blinkt während Firmware-Aktualisierung und Wiederherstellung der Werkseinstellungen.
Gelb/rot	Blinkt gelb/rot, wenn die Netzwerk-Verbindung nicht verfügbar ist oder unterbrochen wurde.
Rot	Aktualisierung der Firmware fehlgeschlagen.

Einschub für SD-Speicherkarte

HINWEIS

- Gefahr von Schäden an der SD-Karte. Benutzen Sie beim Einsetzen oder Entfernen der SD-Karte keine scharfen Werkzeuge oder Gegenstände aus Metall und wenden Sie keine übermäßige Kraft an. Setzen Sie die Karte mit den Fingern ein und entnehmen Sie diese auf die gleiche Weise.
- Gefahr von Datenverlust und beschädigten Aufzeichnungen. Entfernen Sie vor dem Herausnehmen die SD-Karte von der Weboberfläche des Geräts. Die SD-Karte darf nicht entfernt werden, während das Produkt in Betrieb ist.

Dieses Gerät unterstützt Karten des Typs microSD/microSDHC/microSDXC.

Empfehlungen zu SD-Karten finden Sie auf *axis.com*.

Die Logos microSD, microSDHC und microSDXC sind Marken von SD-3C, LLC. microSD, microSDHC und microSDXC sind in den USA und/oder anderen Ländern Marken oder eingetragene Marken von SD-3C, LLC.

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 79*.

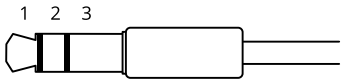
Anschlüsse

Netzwerk-Anschluss

RJ45-Ethernetanschluss mit Power over Ethernet (PoE).

Audioanschluss

- **Audioeingang** – 3,5 mm, für ein Monomikrofon oder ein Monosignal (der linke Kanal wird von einem Stereosignal genutzt).



Audioeingang

1 Spitze	2 Ring	3 Hülse
Unsymmetrisches Mikrofon (mit oder ohne Elektretspeisung) oder Leitung	Elektretspeisung, sofern ausgewählt	Erdung

E/A-Anschluss

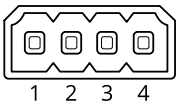
Über den E/A-Anschluss wird Zusatzausrüstung in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösungen, Alarmbenachrichtigungen und anderen Funktionen angeschaltet. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende Schnittstellen bereit:

Digitaleingang – Zum Anschluss von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können wie etwa PIR-Sensoren, Tür- und Fensterkontakte sowie Glasbruchmelder.

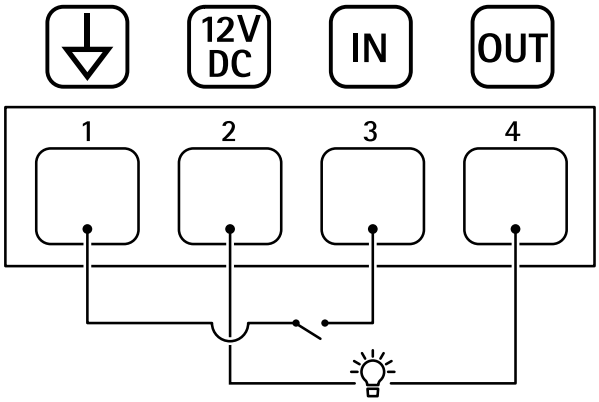
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

Technische Daten

4-poliger Anschlussblock



Beispiel



1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V, max. 25 mA*
3 *Digitaleingang*
4 *Digitalausgang*

Empfehlungen zur Reinigung

Fehlerbehebung

Unbekannte Fahrzeuge werden als akzeptiert gekennzeichnet

Wenn der Antrag Fahrzeuge mit Fahrzeugkennzeichen zulässt, die nicht auf der Zulassungsliste stehen, ist ein wahrscheinlicher Grund dafür, dass der Vergleich eine Abweichung von einem Zeichen zulässt.
Zum Beispiel, wenn **AXI S1234** sich in der Genehmigungsliste befindet, die der Antrag akzeptiert **AXI SI234**.
Gleichermaßen, wenn **AXIS 1234** sich in der Freigabeliste befindet, die der Antrag akzeptiert **AXI 1234**.

Gehen Sie zu *Weitere Einstellungen auf Seite 17*, um die zulässigen Zeichen festlegen.

Die Verbindung zwischen Anwendung und Steuergerät oder Relaismodul arbeitet nicht

Sicherstellen, dass das Steuergerät oder Relaismodul Datenaustausch über HTTP zulässt. Das Benutzerhandbuch des entsprechenden Geräts erläutert das Bearbeiten dieser Einstellung.

Für Benutzer von AXIS Camera Station

AXIS License Plate Verifier einrichten

Wenn ein Gerät mit einem Netzwerk AXIS License Plate Verifier, wird es in diesem Bereich als externe Datenquelle in der AXIS Camera Station betrachtet. Sie können eine Ansicht mit der Datenquelle verbinden, nach vom Gerät erfassten Fahrzeugkennzeichen suchen und das entsprechende Bild anzeigen.

Hinweis

- Dafür ist AXIS Camera Station 5.38 oder höher erforderlich.
- AXIS License Plate Verifier erfordert eine Lizenz.

1. Laden Sie die Anwendung und installieren Sie sie auf Ihrem Gerät.
2. Konfigurieren Sie die Anwendung. Siehe *AXIS License Plate Verifier Benutzerhandbuch*.
3. Bei einer vorhandenen Installation von AXIS Camera Station erneuern Sie das für die Kommunikation mit dem Client verwendete Serverzertifikat. Siehe *Zertifikat erneuern*.
4. Aktivieren Sie die Zeitsynchronisierung, um den Server von AXIS Camera Station als NTP-Server zu verwenden. Siehe dazu *Server-Einstellungen*.
5. Fügen Sie das Gerät zu AXIS Camera Station hinzu. Siehe dazu *Geräte hinzufügen*.
6. Wenn das erste Ereignis empfangen wird, wird unter **Konfiguration > Geräte > externe Datenquelle** automatisch eine Datenquelle hinzugefügt.
7. Verbinden Sie die Datenquelle mit einer Ansicht. Siehe dazu *Externe Datenquellen*.
8. Suchen Sie nach Fahrzeugkennzeichen, die vom Gerät erfasst wurden. Siehe dazu *Datensuche*.
9. Klicken Sie auf , um die Suchergebnisse in eine txt-Datei zu exportieren.

Technische Fragen, Hinweise und Lösungen

Falls Sie hier nicht das Gesuchte finden, bitte den Bereich „Fehlerbehebung" unter *axis.com/support* aufrufen.

Fehlerbehebung

Probleme beim Aktualisieren der Firmware

Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche Firmwaredatei hochgeladen wurde. Überprüfen, ob der Name der Firmwaredatei dem Gerät entspricht und erneut versuchen.
Probleme nach dem Aktualisieren von Firmware	Bei nach dem Aktualisieren von Firmware auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurückrollen.

Probleme beim Einstellen der IP-Adresse

Das Gerät befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein): • Wenn Folgendes angezeigt wird: `Reply from (Antwort von)<IP address>: bytes=32; time=10...` dies bedeutet, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut. • Wenn Folgendes angezeigt wird: `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell `http` oder `https` in die Adressleiste des Browsers eingeben. Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 79*.
Die IP-Adresse wurde von DHCP geändert	Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Gerät mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Ermitteln Sie das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde). Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen dazu finden Sie auf *axis.com/support*.
Zertifikatfehler beim Verwenden von IEEE 802.1X	Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **Einstellungen > System > Datum und Uhrzeit**.

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

Für den externen Zugriff auf das Gerät wird die Verwendung einer der folgenden Anwendungen für Windows® empfohlen:

- AXIS Companion: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Video Management Software: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

Auf *axis.com/vms* finden Sie Anweisungen und die Download-Datei.

Fehlerbehebung

Probleme beim Videostreaming	
Auf Multicast H.264 kann nur von lokalen Clients zugegriffen werden	Prüfen Sie, ob der Router Multicasting unterstützt und ob die Routereinstellungen zwischen dem Client und dem Gerät konfiguriert werden müssen. Möglicherweise müssen Sie den TTL-Wert (Time To Live) erhöhen.
Multicast H.264 wird im Client nicht angezeigt	Prüfen Sie mit dem Netzwerkadministrator, ob die vom Axis Gerät verwendeten Multicast-Adressen für das Netzwerk gültig sind. Prüfen Sie gemeinsam mit dem Netzwerkadministrator, ob eine Firewall die Wiedergabe verhindert.
Schlechte Bildqualität bei der Wiedergabe mit H.264	Stellen Sie sicher, dass die Grafikkarte den aktuellen Treiber verwendet. Die aktuellen Treiber können in der Regel von der Webseite des Herstellers heruntergeladen werden.
Abweichende Farbsättigung zwischen H.264 und Motion JPEG	Die Einstellungen des Grafikadapters ändern. Weitere Informationen bietet die Dokumentation des Adapters.
Bildrate niedriger als erwartet	• Siehe *Leistungsaspekte auf Seite 80*. • Verringern Sie die Anzahl der auf dem Clientcomputer ausgeführten Anwendungen. • Begrenzen Sie die Anzahl der gleichzeitigen Anzeigen. • Prüfen Sie mit dem Netzwerkadministrator, ob ausreichend Bandbreite verfügbar ist. • Die Bildauflösung verringern. • Die maximale Bildrate hängt von der Netzfrequenz (60/50 Hz) des Axis Geräts ab.

Verbindung über Port 8883 mit MQTT über SSL kann nicht hergestellt werden	
Die Firewall blockiert den Datenverkehr über Port 8883, da er als ungesichert eingestuft wird.	In einigen Fällen stellt der Server/Broker möglicherweise keinen bestimmten Port für die MQTT-Kommunikation bereit. Möglicherweise kann MQTT über einen Port verwendet werden, der normalerweise für HTTP/HTTPS-Datenverkehr verwendet wird. • Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll. • Wenn der Server/Broker ALPN unterstützt, kann darüber verhandelt werden, ob MQTT über einen offenen Port (wie z. B. 443) verwendet werden soll. Prüfen Sie mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

Hinweis

Die Kamera wurde mit AXIS License Plate Verifier vorkonfiguriert. Nach dem Zurücksetzen auf die Werkseinstellungen muss der Lizenzschlüssel erneut installiert werden. Siehe .

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 73*.
3. Halten Sie die Steuertaste etwa 15 bis 30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse `192.168.0.90`.

5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.

   Die Installations- und Verwaltungstools finden auf den Supportseiten unter *axis.com/support*.

Die Parameter können auch über die Weboberfläche des Geräts auf die Werkseinstellungen zurückgesetzt werden. Gehen Sie zu **Wartung** > **Werkseinstellungen** und klicken Sie auf **Standardeinstellungen**.

Firmware aktualisieren

Wichtig

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Firmware gespeichert (sofern die Funktionen als Teil der neuen Firmware verfügbar sind). Es besteht diesbezüglich jedoch keine Garantie seitens Axis Communications AB.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

Beim Aktualisieren mit der aktuellen Firmware im aktiven Track werden auf das Gerät die neuesten verfügbaren Funktionen versorgt. Lesen Sie vor der Aktualisierung der Firmware stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise dazu. Die aktuelle Version der Firmware und die Versionshinweise finden Sie auf *axis.com/support/firmware*.

1. Die Firmware können Sie auf *axis.com/support/firmware* kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Navigieren Sie zu **Maintenance > Firmware upgrade (Wartung > Firmwareaktualisierung)** und klicken Sie auf **Upgrade (Aktualisieren)**.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Mithilfe des AXIS Device Managers lassen sich mehrere Geräte gleichzeitig aktualisieren. Weitere Informationen dazu finden Sie auf *axis.com/products/axis-device-manager*.

Leistungsaspekte

Achten Sie beim Einrichten Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die Leistung auswirken. Einige Faktoren wirken sich auf die erforderliche Bandbreite (die Bitrate) aus, andere auf die Bildrate und einige sowohl auf die Bandbreite als auch die Bildrate. Wenn die CPU-Auslastung ihre Grenze erreicht, wirkt sich dies ebenfalls auf die Bildrate aus.

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Hohe Bildauflösung und geringe Komprimierung führen zu Bildern mit mehr Daten, die wiederum mehr Bandbreite erfordern.
- Durch Drehen des Bildes in der GUI kann sich die CPU-Auslastung des Geräts erhöhen.
- Der Zugriff von vielen Clients des Typs Motion JPEG oder Unicast H.264 beeinflusst die Bandbreite.
- Die gleichzeitige Wiedergabe verschiedener Videostreams (Auflösung, Komprimierung) durch mehrere Clients beeinflusst sowohl die Bildrate als auch die Bandbreite.

  Wo immer möglich, identisch konfigurierte Videostreams verwenden, um eine hohe Bildrate zu erhalten. Videostreamprofile werden verwendet, um identische Videostreams sicherzustellen.
- Der gleichzeitige Zugriff auf Videostreams des Typs Motion JPEG und H.264 beeinflusst sowohl die Bildrate als auch die Bandbreite.
- Die intensive Verwendung von Ereignissen beeinflusst die CPU-Auslastung, die sich wiederum auf die Bildrate auswirkt.
- Die Verwendung von HTTPS kann, besonders beim Streaming im Format Motion JPEG, die Bildrate reduzieren.

Fehlerbehebung

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Die Wiedergabe auf schlecht arbeitenden Clientcomputern verringert die wahrgenommene Leistung und beeinflusst die Bildrate.
- Mehrere gleichzeitig ausgeführte ACAP-Anwendungen (AXIS Camera Application Platform) können die Bildrate und die allgemeine Leistung beeinflussen.

Benutzerhandbuch
AXIS P1445-LE-3 License Plate Verifier Kit
© Axis Communications AB, 2018 - 2023
Vers. M24.2
Datum: September 2023
Teil-Nr. T10126900