

AXIS P3265-LVE-3 License Plate Verifier Kit

Inhalt

Funktionsweise.....	4
Das Gerät im Netzwerk ermitteln	4
Unterstützte Browser.....	4
Weboberfläche des Geräts öffnen	4
Administratorkonto erstellen	4
Sichere Kennwörter	5
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.	5
Übersicht über die Weboberfläche.....	5
Grundeinstellungen.....	6
Empfehlungen für die Kameramontage.....	6
Einrichtungsassistent.....	8
Freie Fahrt	8
Zutrittskontrolle	9
Auf die Anwendungseinstellungen zugreifen	10
Den ausgewählten Bereich anpassen	10
Region auswählen	11
Bilderfassungseinstellungen anpassen	11
Einrichten von Ereignisspeicher.....	11
Installation	13
Vorschaumodus.....	13
Ihr Gerät konfigurieren	14
Für Benutzer von AXIS Camera Station	14
AXIS License Plate Verifier einrichten.....	14
Grundlegende Einstellungen	14
Bild einstellen	14
Reduzierung der Bildverarbeitungszeit mit dem Low-Latency-Modus	14
Den Belichtungsmodus wählen	15
Tonnenverzeichnung kompensieren	15
Überprüfen der Pixelauflösung	15
Video ansehen und aufnehmen	16
Bandbreite und Speicher reduzieren.....	16
Einrichtung eines Netzwerk-Speichers	16
Video aufzeichnen und ansehen	17
Stellen Sie sicher, dass keiner das Video manipuliert hat.	17
Einrichten von Regeln für Ereignisse.....	17
Aufzeichnen von Video, wenn die Kamera ein Fahrzeugkennzeichen erkennt.....	17
Benachrichtigung bei Manipulation an Kameraobjektiv auslösen	18
Audio.....	19
Videoaufzeichnungen mit Audio ergänzen.....	19
Ihrem Produkt mithilfe von Portcast Audiofunktion hinzufügen	19
Listen verwalten	20
Erfasstes Fahrzeugkennzeichen der Liste hinzufügen.....	20
Beschreibungen zu Fahrzeugkennzeichen hinzufügen.....	20
Listennamen anpassen	21
Zulässig aufgelistete Kfz-Kennzeichen importieren	22
Kennzeichen-Listen mit anderen Kameras teilen	23
Listen planen	24
Weitere Einstellungen	25
Text-Overlay konfigurieren	25
Kennzeichen bei schlechten Lichtverhältnissen erkennen.....	25
Weniger Zeichen bei Fahrzeugkennzeichen erlauben.....	25
Nur exakte Übereinstimmungen von Nummernschildern zulassen.....	25
Bei der Übereinstimmung von Kennzeichen mehr als ein Zeichen Abweichung zulassen.....	25

Bedienern begrenzten Zugriff geben.....	26
Sichere Verbindung einrichten.....	26
Sichern und Wiederherstellen von App-Einstellungen.....	26
Alle Ereignisse löschen.....	26
Aktionen über virtuelle Ports auslösen.....	26
Anwendungsfall Einfahrt und Ausfahrt von Fahrzeugen.....	28
Eine Schranke für bekannte Fahrzeuge mittels eines Relaismoduls öffnen.....	28
Eine Schranke für bekannte Fahrzeuge mittels des E/A der Kamera öffnen.....	29
Über ein nicht autorisiertes Fahrzeug benachrichtigt werden.....	30
Anwendungsfall Zufahrtskontrolle für Fahrzeuge.....	31
Mit einer Türsteuerung verbinden.....	31
Verknüpfung mit AXIS Secure Entry.....	33
Freie Fahrt-Szenario mit Geschwindigkeitsmessung.....	35
Einrichten des Szenarios.....	35
Suche nach bestimmten Ereignissen.....	37
Suchergebnisse exportieren und freigeben.....	37
Integration.....	38
Profile verwenden, um Ereignisse auf mehrere Server zu übertragen.....	38
Ereignisinformationen an die Software anderer Hersteller per Push senden.....	38
Bilder von Nummernschildern an einen Server senden.....	39
Direkte Integration mit 2N.....	40
Integration in das Genetec Security Center.....	40
Weboberfläche.....	43
Mehr erfahren.....	44
Edge-to-Edge-Technologie.....	44
Radarkopplung.....	44
Lautsprecherkopplung.....	44
Anzeigebereich.....	44
AXIS Image Health Analytics.....	44
Technische Daten.....	45
Produktübersicht.....	45
LED-Anzeigen.....	45
Einschub für SD-Speicherkarte.....	46
Tasten.....	46
Steuertaste.....	46
Anschlüsse.....	46
Netzwerk-Anschluss.....	46
Audioanschluss.....	46
E/A-Anschluss.....	46
Fehlerbehebung.....	48
Zurücksetzen auf die Werkseinstellungen.....	48
Optionen für AXIS OS.....	48
Aktuelle AXIS OS-Version überprüfen.....	48
AXIS OS aktualisieren.....	49
Technische Probleme und mögliche Lösungen.....	49
.....	52
Leistungsaspekte.....	53
Support.....	54
Cybersicherheit.....	55
Schwachstellen-Management.....	55
Sicherheitsbenachrichtigungen.....	55
Sicherer Produktlebenszyklus.....	55

Funktionsweise

Das Gerät im Netzwerk ermitteln

Mit AXIS IP Utility und AXIS Device Manager die Axis Geräte im Netzwerk ermitteln und ihnen unter Windows® IP-Adressen zuweisen. Beide Anwendungen sind kostenlos und können von axis.com/support heruntergeladen werden.

Weitere Informationen zum Zuweisen von IP-Adressen finden Sie unter *Zuweisen von IP-Adressen und Zugreifen auf das Gerät*.

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Andere Betriebssysteme	*	*	*	*

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
Wenn Sie die IP-Adresse nicht kennen, ermitteln Sie das Gerät im Netzwerk mithilfe von AXIS IP Utility oder AXIS Device.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Administratorkonto erstellen*, on page 4.

Eine Beschreibung aller Funktionen und Einstellungen in der Weboberfläche von Geräten mit AXIS OS finden Sie unter *Hilfe zur Weboberfläche von AXIS OS*.

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter*, on page 5.
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Konto 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*, on page 48.

Sichere Kennwörter

Wichtig

Verwenden Sie HTTPS (standardmäßig aktiviert), um Ihr Kennwort oder andere sensible Konfigurationen über das Netzwerk einzustellen. HTTPS ermöglicht sichere und verschlüsselte Netzwerkverbindungen und schützt so sensible Daten wie Kennwörter.

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.
- Ändern Sie das Kennwort regelmäßig und mindestens einmal jährlich.

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

So stellen Sie sicher, dass das Gerät über seine ursprüngliche AXIS OS-Version verfügt, bzw. übernehmen nach einem Sicherheitsangriff die volle Kontrolle über das Gerät:

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 48*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Übersicht über die Weboberfläche

In diesem Video erhalten Sie einen Überblick über die Weboberfläche des Geräts.



Weboberfläche des Axis Geräts

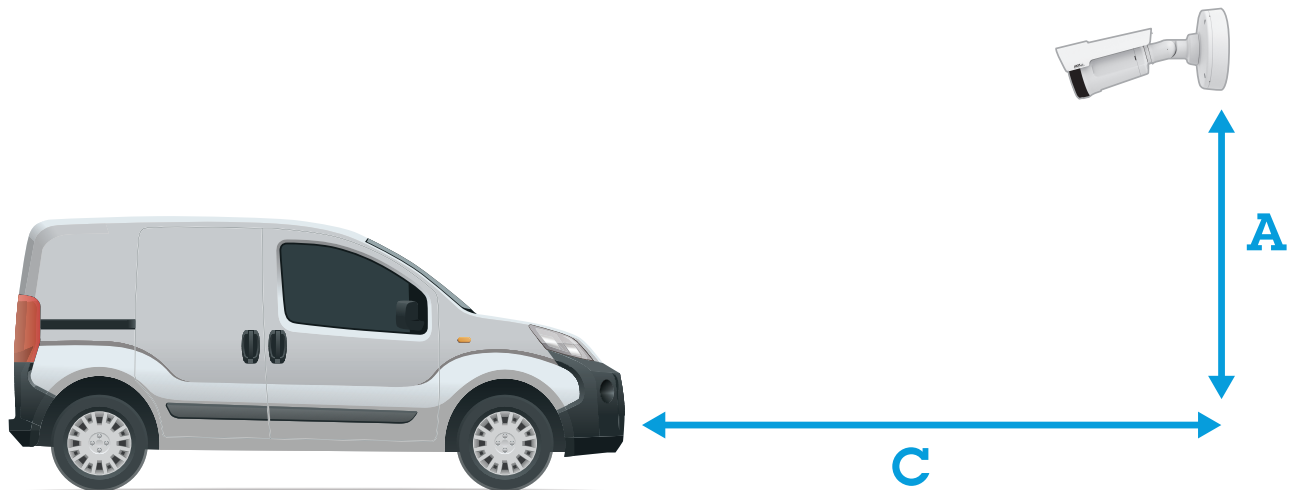
Grundeinstellungen

Diese Einrichtungsanweisungen gelten für alle Szenarios:

- 1.
- 2.
3. *Den ausgewählten Bereich anpassen, on page 10*
4. *Region auswählen, on page 11*
5. *Einrichten von Ereignisspeicher, on page 11*

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.



Zutrittskontrolle Erfassungsdistanz: 2–7 m (6,6–23 ft). Dieses Beispiel basiert auf dem AXIS P3265-LVE-3 License Plate Verifier Kit.

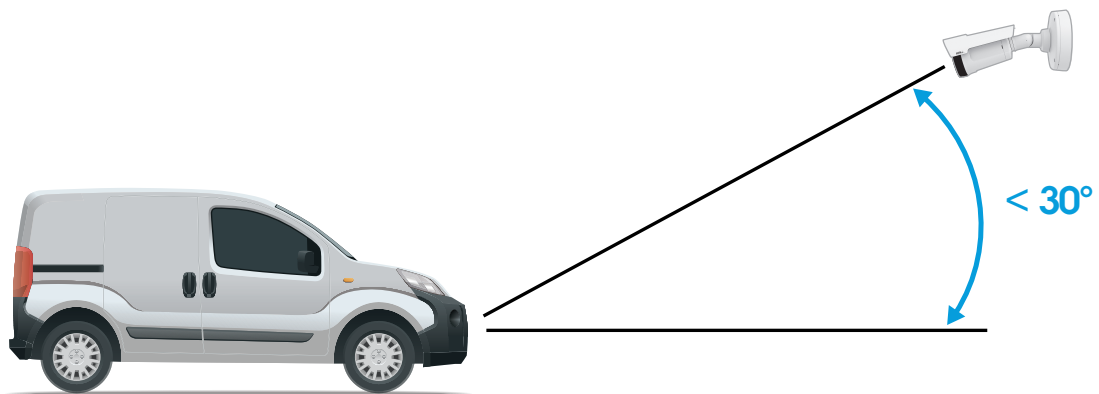
Erfassungsdistanz: (C)	Montagehöhe (A)
2,0 m (6.6 ft)	1,0 m (3.3 ft)
3,0 m (9.8 ft)	1,5 m (4.9 ft)
4,0 m (13 ft)	2,0 m (6.6 ft)
5,0 m (16 ft)	2,5 m (8.2 ft)
7,0 m (23 ft)	3,5 m (11 ft)

Freie Fahrt Erfassungsdistanz: 7–20 m (23–65 ft). Dieses Beispiel basiert auf dem AXIS P1465-LE-3 License Plate Verifier Kit.

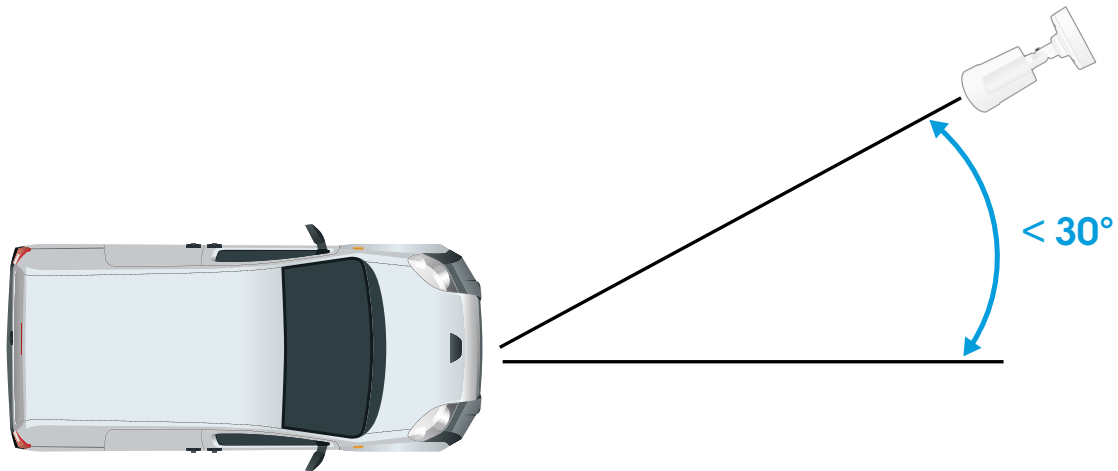
Erfassungsdistanz (C)	Montagehöhe (A)
7,0 m (23 ft)	3,0 m (9.8 ft)

10,0 m (33 ft)	4,0 m (13 ft)
15,0 m (49 ft)	6,0 m (19.5 ft)
20,0 m (65 ft)	10,0 m (33 ft)

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

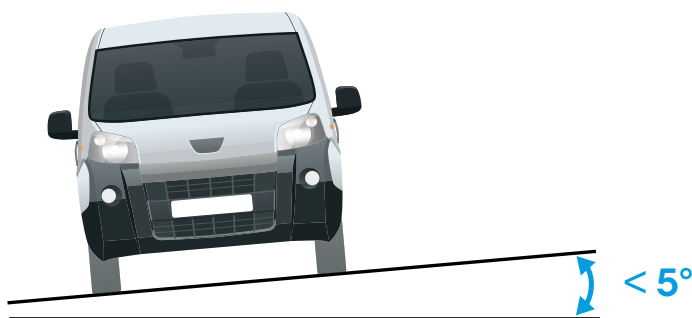


Montagewinkel von der Seite



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.



Drehwinkel.

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, gehen Sie zu **Settings** (Einstellungen) > **Maintenance** (Wartung) und klicken Sie unter **Setup assistant** (Einrichtungsassistent) auf Start.

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 **Free flow** (Freie Fahrt) und klicken Sie auf **Next** (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 **License plate crop** (Kennzeichen-Ausschnitt) wird nur das Kennzeichen gespeichert.
 - Mit **Vehicle crop** (Fahrzeugausschnitt) 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.
6. Ziehen Sie die Ankerpunkte, um den ausgewählten Bereich anzupassen. Siehe *Den ausgewählten Bereich anpassen, on page 10*.
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. Aus dem Aufklappmenü **Protocol** (Protokoll) eines der folgenden Protokolle auswählen:
 - TCP
 - HTTP POST

10. Geben Sie in das Feld **Server URL (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. 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.
 - **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. Klicken Sie auf **Next (Weiter)**.
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 (Fertig)**.

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, on page 29*.
 - **Controller** zum Anschließen eines Türcontrollers. Siehe .
 - **Relais** zum Anschließen an einem Relaismodul. Siehe .
3. Wählen Sie in der Auswahlliste **Schrankenmodus** unter **Über Listen öffnen** die Option **Freigabeliste**.
4. Im Aufklappmenü **Vehicle direction (Fahrzeugrichtung)** **Out (Ausfahrt)** wählen.
5. Wählen Sie in der Auswahlliste **ROI** den in Frage kommenden ausgewählten Bereich oder wählen Sie alle Bereiche.
6. Klicken Sie auf **Next (Weiter)**.

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, on page 11*.
4. Ziehen Sie die Ankerpunkte, um den ausgewählten Bereich anzupassen. Siehe *Den ausgewählten Bereich anpassen, on page 10*.
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, siehe *Ereignisinformationen an die Software anderer Hersteller per Push senden*, on page 38.

1. Aus dem Aufklappmenü **Protocol (Protokoll)** eines der folgenden Protokolle auswählen:
 - TCP
 - HTTP POST
2. Geben Sie in das Feld **Server URL (Server-URL)** die Server-Adresse und den Port im folgenden Format 127.0.0.1:8080 ein.
3. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein oder lassen Sie den vorgegebenen Namen stehen.
4. 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.
 - **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** (Fertig).

Auf die Anwendungseinstellungen zugreifen

1. Wechseln Sie zu der Weboberfläche der Kamera zu **Apps**, starten Sie die Anwendung und klicken Sie auf **Öffnen**.

Den ausgewählten Bereich anpassen

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. **Settings (Einstellungen)** aufrufen.
2. Klicken Sie auf **Image (Bild)**.
3. Klicken Sie auf 1:1, um den Bereich zu vergrößern, in dem Sie den Datenaustausch überwachen oder die Zutrittskontrolle verwalten möchten.
4. Um die Erkennung und die aufgenommenen Bilder zu verbessern, klicken Sie auf **AF**.
5. Um die Kamera automatisch auf die Fahrzeuge fokussieren zu lassen, klicken Sie auf **AF**. Um den Fokus manuell einzustellen, passen Sie ihn mit dem Schieber an.
6. Klicken Sie auf **Area of interest (Ausgewählter Bereich)**, um ihn im Ansichtsbereich anzuzeigen.
7. Um den ausgewählten Bereich zu verschieben, klicken Sie auf eine beliebige Stelle in diesem Bereich, um ihn auszuwählen, und ziehen Sie ihn an die Stelle, an der die Nummernschilder am besten sichtbar sind. Nach dem Speichern der Einstellungen sicherstellen, dass der Interessensbereich in der gewählten Position angezeigt wird.

8. Um den ausgewählten Bereich anzupassen, klicken Sie auf eine beliebige Stelle in diesem Bereich, um ihn auszuwählen, und ziehen Sie die blau hervorgehobenen Ankerpunkte.
 - Um den ausgewählten Bereich zurückzusetzen, klicken Sie auf die Schaltfläche „Reset (Zurücksetzen)“ in der unteren linken Ecke neben dem Zahlensymbol.
 - Um Ankerpunkte hinzuzufügen, klicken Sie auf einen der dunklen Ankerpunkte. Der Ankerpunkt wird jetzt gelb dargestellt und kann verändert werden. Neben dem gelben Ankerpunkt werden automatisch neue dunkle Punkte hinzugefügt. Die maximale Anzahl gelber Ankerpunkte beträgt acht.
9. Klicken Sie auf einen beliebigen Bereich außerhalb des ausgewählten Bereichs, um Ihre Änderungen zu speichern.
10. Um im **Event log (Ereignisprotokoll)** korrekte Rückmeldungen zur Fahrtrichtung zu erhalten, drehen Sie den Pfeil in die Fahrtrichtung.
 - 10.1. Klicken Sie auf das Pfeil-Symbol.
 - 10.2. Wählen Sie den Ankerpunkt aus und drehen Sie den Pfeil, sodass in die Fahrtrichtung zeigt.
 - 10.3. 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 **Richtung** angezeigt.

11. Um zu überprüfen, ob Ihr ausgewählter Bereich groß genug ist, um optimale Ergebnisse zu erzielen, verwenden Sie den Pixelzähler.
 - Um den Pixelzähler anzuzeigen, klicken Sie auf das Taschenrechner-Symbol.
 - Um den Bereich des Pixelzählers in voller Größe anzupassen, ziehen Sie die untere rechte Ecke des gelb markierten Bereichs.
 - Um den Pixelzählerbereich zu verschieben, klicken Sie auf eine beliebige Stelle innerhalb des Bereichs und ziehen Sie ihn an die gewünschte Position.
- Um einen zweiten ausgewählten Bereich hinzuzufügen, klicken Sie auf + neben 1.
- Bei Verwendung einer eigenständigen Kamera können mit der App die empfohlenen Einstellungen für die Nummernschilderkennung festgelegt werden.
 1. Klicken Sie auf das Zauberstab-Symbol, und die Einstellungen werden für die Nummernschilderkennung optimiert.
 2. Klicken Sie auf die Menüschaltfläche neben dem Zauberstab, um die eingestellten Werte anzuzeigen.

Region auswählen

1. Wechseln Sie zu **Settings (Einstellungen) > Recognition (Erkennung)**.
2. Im Aufklappmenü **Region** auswählen.

Bilderfassungseinstellungen anpassen

1. Wechseln Sie zu **Settings (Einstellungen) > Image (Bild)**.
2. Um die Auflösung der erfassten Bilder zu ändern, gehen Sie zu **Image resolution (Bildauflösung)**
3. Um die Drehung des erfassten Bildes zu ändern, gehen Sie zu **Rotation (Drehung)**

Einrichten von Ereignisspeicher

Ein Ereignis besteht aus dem erfassten Bild, dem Fahrzeugkennzeichen, der Nummer des ausgewählten Bereichs, der Fahrtrichtung, 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.

Anforderungen:

- Physisch installierte und an das Netzwerk angeschlossene Kamera
 - AXIS License Plate Verifier wird auf der Kamera ausgeführt.
 - Interner Speicher oder eine in der Kamera installierte SD-Karte.
1. Gehen Sie zu **Settings (Einstellungen) > Storage (Speicher)**.
 2. Wählen Sie unter **Retain events (Ereignisse speichern)** die Option **Allowlisted (Als zulässig geführt)**.
 3. Wählen Sie unter **Retention period (Speicherdauer)** die Option **30 days (30 Tage)**.
 4. Um die Speicherungsart der erfassten Bilder zu ändern, wechseln Sie zu **Save full frame (Vollbild speichern)**:
 - Mit **License plate crop (Kennzeichen-Ausschnitt)** wird nur das Kennzeichen gespeichert.
 - Mit **Vehicle crop (Fahrzeugausschnitt)** 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.

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.

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.

Ihr Gerät konfigurieren

Für Benutzer von AXIS Camera Station

AXIS License Plate Verifier einrichten

Wenn ein Gerät mit einem Netzwerk AXIS License Plate Verifier konfiguriert wird, wird es in diesem Bereich als externe Datenquelle im Video Management System 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. Das Zusatzgerät zur AXIS Camera Station hinzufügen. 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 hierzu *Datensuche*.
 9. Klicken Sie auf , um die Suchergebnisse in eine txt-Datei zu exportieren.

Grundlegende Einstellungen

Montageposition festlegen

1. Wechseln Sie zu **Video > Installation > Montageposition**.
2. Klicken Sie auf **Ändern**.
3. Wählen Sie eine Montageposition aus und klicken Sie auf **Save and restart (Speichern und neu starten)**.

Netzfrequenz einstellen

1. Gehen Sie auf **Video > Installation > Netzfrequenz**.
2. Wählen Sie eine Netzfrequenz aus und klicken Sie auf **Speichern und neu starten**.

Bild einstellen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts.

Reduzierung der Bildverarbeitungszeit mit dem Low-Latency-Modus

Sie können die Bildverarbeitungszeit Ihres Livestreams durch Einschalten des Low-Latency-Modus optimieren. Die Verzögerung in Ihrem Livestream wird damit auf ein Minimum reduziert. Wenn Sie den Low-Latency-Modus verwenden, ist die Bildqualität geringer als gewöhnlich.

1. **System > Plain config (System > Einfache Konfiguration)** aufrufen.
2. Wählen Sie in der Dropdown-Liste die Option **ImageSource (Bildquelle)** aus.

3. Gehen Sie auf **ImageSource/I0/Sensor > Low latency mode (Low-Latency-Modus)**, und wählen Sie **On (Ein)**.
4. **Save (Speichern)** anklicken.

Den Belichtungsmodus wählen

Verwenden Sie Belichtungsmodi zur Verbesserung der Bildqualität bestimmter Überwachungsszenen. Mit den Belichtungsmodi können Sie Blendenöffnung, Verschlusszeit und Verstärkung steuern. Gehen Sie auf **Video > Bild > Belichtung** und wählen Sie zwischen folgenden Belichtungsmodi:

- Wählen Sie für die meisten Fälle **Automatische Beleuchtung**.
- Für Umgebungen mit einem gewissen Anteil Kunstlicht, wie etwa fluoreszierendes Licht, den Modus **"Flimmerfrei"** wählen.
Die der Netzfrequenz entsprechende Frequenz wählen.
- Für Umgebungen mit einem gewissen Anteil Kunstlicht und hellem Licht, wie etwa fluoreszierendes Licht nachts im Außenbereich oder Sonne tags, den Modus **"Flimmerreduziert"** wählen.
Die der Netzfrequenz entsprechende Frequenz wählen.
- Um die aktuellen Belichtungseinstellungen beizubehalten, wählen Sie den Modus **Aktuelle beibehalten**.

Tonnenverzeichnung kompensieren

Tonnenverzeichnung ist ein Phänomen, bei dem gerade Linien zum Bildrand hin zunehmend verzerrt dargestellt werden. Tonnenverzeichnung wird oft durch ein breites Sichtfeld hervorgerufen. Die Korrektur der Tonnenverzeichnung gleicht diesen Effekt aus.

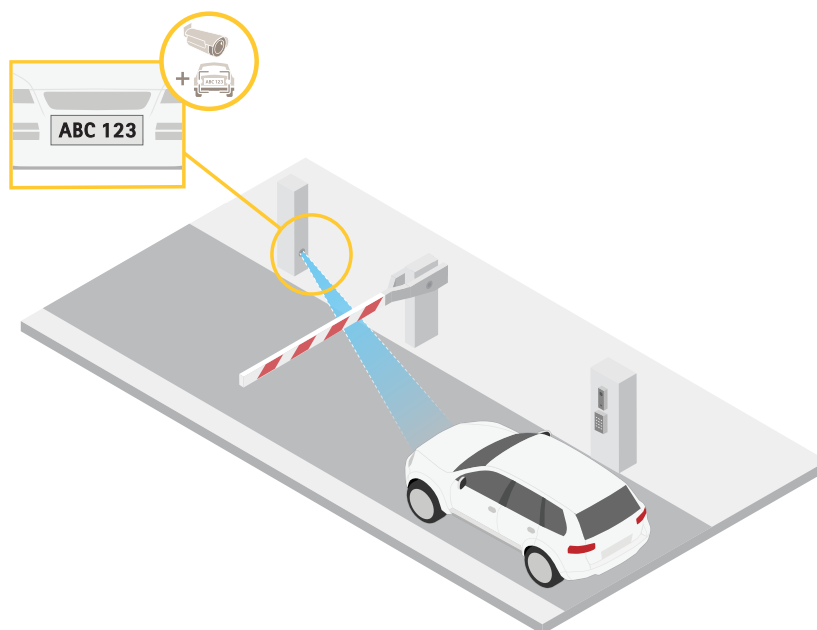
Hinweis

Die Korrektur der Tonnenverzeichnung beeinträchtigt die Bildauflösung und das Sichtfeld.

1. Gehen Sie zu **Video > Installation > Bildkorrektur**.
2. Aktivieren Sie **Barrel distortion correction (BDC) (Korrektur der Tonnenverzeichnung (BDC))**.

Überprüfen der Pixelauflösung

Überprüfen Sie mithilfe des Pixelzählers, ob ein definierter Teil des Bilds genügend Pixel enthält, um z. B. ein Autokennzeichen zu erkennen.



1. Gehen Sie auf **Video > Bild**.

2. Klicken Sie auf .
3. Klicken Sie für Pixel counter (Pixelzähler) auf .
4. Passen Sie in der Live-Ansicht der Kamera Größe und Position des Rechtecks um den ausgewählten Bereich herum an, z. B. dort, wo Autokennzeichen voraussichtlich erscheinen werden.
5. Sie können die Pixelanzahl für jede Seite des Rechtecks sehen und entscheiden, ob die Werte für Ihre Anforderungen ausreichen.

Video ansehen und aufnehmen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts. Weitere Informationen zum Streamen und Speichern finden Sie unter .

Bandbreite und Speicher reduzieren

Wichtig

Eine Reduzierung der Bandbreite kann zum Verlust von Details im Bild führen.

1. Gehen Sie auf **Video > Videostream**.
2. Klicken Sie in der Live-Ansicht auf .
3. Wählen Sie **Videoformat AV1** aus, wenn Ihr Gerät dies unterstützt. Andernfalls wählen Sie **H.264**.
4. Gehen Sie auf **Video > Videostream > Allgemein** und erhöhen Sie die **Komprimierung**.
5. Gehen Sie zu **Video > Stream > Zipstream (Video > Videostream > Zipstream)** und führen Sie eine oder mehrere der folgenden Schritte durch:

Hinweis

Die Einstellungen **Zipstream** werden für alle Video-Encoder außer MJPEG verwendet.

- Wählen Sie die **Strength (Stärke)** des Zipstreams aus, die Sie verwenden möchten.
- Aktivieren Sie **Optimize for storage (Speicher optimieren)**. Dies kann nur verwendet werden, wenn die Video Management Software B-Rahmen unterstützt.
- Aktivieren Sie **Dynamische FPS**.
- Aktivieren Sie **Dynamisches GOP** und wählen Sie eine hohe **Obere Grenze** als Wert für die GOP-Länge.

Hinweis

Die meisten Webbrowser unterstützen nicht das Dekodieren von H.265. Aus diesem Grund unterstützt das Gerät es auf dessen Weboberfläche nicht. Stattdessen können Sie auf ein Video Management System oder eine Anwendung zurückgreifen, die das Decodieren von H.265 unterstützt.

Einrichtung eines Netzwerk-Speichers

Um Aufzeichnungen im Netzwerk zu speichern, müssen Sie Ihren Netzwerk-Speicher einrichten.

1. Gehen Sie auf **System > Storage (System > Speicher)**.
2. Klicken Sie unter **Network storage (Netzwerk-Speicher)** auf  **Add network storage (Netzwerk-Speicher hinzufügen)**.
3. Geben Sie die IP-Adresse des Host-Servers an.
4. Geben Sie unter **Network share (Netzwerk-Freigabe)** den Namen des freigegebenen Speicherorts auf dem Host-Server ein.
5. Geben Sie den Benutzernamen und das Kennwort ein.
6. Wählen Sie die SMB-Version aus oder lassen Sie **Auto** stehen.

7. Wählen Sie **Add share without testing (Freigabe ohne Test hinzufügen)**, wenn vorübergehende Verbindungsprobleme auftreten oder die Freigabe noch nicht konfiguriert ist.
8. Klicken Sie auf **Hinzufügen**.

Video aufzeichnen und ansehen

Video direkt von der Kamera aufzeichnen

1. Gehen Sie auf **Video > Videostream**.
2. Um eine Aufzeichnung zu starten, klicken Sie auf .

Wenn Sie noch keinen Speicher eingerichtet haben, klicken Sie auf  und . Anweisungen zum Einrichten des Netzwerk-Speichers finden Sie unter *Einrichtung eines Netzwerk-Speichers, on page 16*

3. Um die Aufzeichnung anzuhalten, klicken Sie erneut auf .

Video ansehen

1. Gehen Sie auf **Recordings (Aufzeichnungen)**.
2. Klicken Sie auf  für Ihre Aufzeichnung in der Liste.

Stellen Sie sicher, dass keiner das Video manipuliert hat.

Mit einem signierten Video können Sie sicherstellen, dass das von der Kamera aufgezeichnete Video von niemanden manipuliert wurde.

1. Wechseln Sie zu **Video > Stream > General (Allgemein)** und aktivieren Sie **Signed Video (Signiertes Video)**.
2. Nehmen Sie Videos direkt auf dem Gerät auf oder verwenden Sie AXIS Camera Station Pro oder eine andere kompatible Video Management Software. Anweisungen für AXIS Camera Station Pro finden Sie im *Benutzerhandbuch von AXIS Camera Station Pro*.
3. Das aufgezeichnete Video exportieren.
4. Verwenden Sie das Axis Werkzeug *Signed Media Verifier*, um die Aufzeichnung zu überprüfen.

Einrichten von Regeln für Ereignisse

Es können Regeln erstellt werden, damit das Gerät beim Auftreten bestimmter Ereignisse eine Aktion ausführt. Eine Regel besteht aus Bedingungen und Aktionen. Die Bedingungen können verwendet werden, um die Aktionen auszulösen. Beispielsweise kann das Gerät beim Erfassen einer Bewegung eine Aufzeichnung starten, eine E-Mail senden oder während der Aufzeichnung einen Overlay-Text anzeigen.

Weitere Informationen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Aufzeichnen von Video, wenn die Kamera ein Fahrzeugkennzeichen erkennt

Dieses Beispiel erläutert, wie Sie die Kamera so einrichten, dass die bei Erfassung eines Objekts mit der Aufzeichnung auf SD-Karte startet. Die Aufzeichnung schließt einen Zeitabschnitt von fünf Sekunden vor und einer Minute nach Ende der Objekterkennung ein.

Vorbereitungen:

- Stellen Sie sicher, dass Sie eine SD-Karte eingesetzt haben.

Stellen Sie sicher, dass AXIS Licence Plate Verifier ausgeführt wird:

1. Rufen Sie **Apps > AXIS License Plate Verifier** auf.
2. Wenn die Anwendung noch nicht ausgeführt wird, starten Sie sie.
3. Stellen Sie sicher, dass die Anwendung gemäß Ihren Ansprüchen eingerichtet ist.

Eine Regel erstellen:

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Liste der Bedingungen unter **Application (Anwendung)** die Option **ALPV.PlatesInView** aus.
4. Wählen Sie aus der Liste der Aktionen unter **AufzeichnungenVideo** aufzeichnen, während die Regel aktiv ist.
5. Wählen Sie in der Liste der Speicheroptionen **SD_DISK**.
6. Wählen Sie eine Kamera und ein Videostreamprofil aus.
7. Stellen Sie die Vorpufferzeit auf 5 Sekunden ein.
8. Stellen Sie die Nachpufferzeit auf 1 Minute ein.
9. **Save (Speichern)** anklicken.

Benachrichtigung bei Manipulation an Kameraobjektiv auslösen

In diesem Beispiel wird erklärt, wie Sie eine E-Mail-Benachrichtigung einrichten, die bei Besprühen, Abdecken oder Unschärfwerden des Kameraobjektivs versendet wird.

Manipulationserfassung aktivieren:

1. Gehen Sie auf **System > Melder > Kameramanipulation**.
2. Legen Sie einen Wert für **Trigger delay (Auslöserverzögerung)** fest. Der Wert gibt die Zeit an, die vergehen muss, bevor eine E-Mail gesendet wird.
3. Aktivieren Sie **Bei dunklen Bildern auslösen**, damit erkannt wird, ob das Objektiv besprüht, abgedeckt oder stark defokussiert wurde.

Einen E-Mail-Empfänger hinzufügen:

4. Wechseln Sie zu **Settings > Events > Recipients (Einstellungen > Ereignisse > Empfänger)** und fügen Sie einen Empfänger hinzu.
5. Geben Sie den Namen des Empfängers ein.
6. Wählen Sie **Email (E-Mail)** als Benachrichtigungsart.
7. Geben Sie die E-Mail-Adresse des Empfängers ein.
8. Geben Sie die E-Mail-Adresse ein, an die die Kamera die Benachrichtigungen senden soll.
9. Geben Sie die Anmeldedaten für das sendende E-Mail-Konto sowie den SMTP-Hostnamen und die Portnummer ein.
10. Um Ihren E-Mail-Setup zu testen, klicken Sie auf **Test (Testen)**.
11. **Save (Speichern)** anklicken.

Eine Regel erstellen:

12. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
13. Geben Sie einen Namen für die Regel ein.
14. Wählen Sie in der Liste der Bedingungen unter **Video** die Option **Tampering (Manipulation)**.
15. Wählen Sie in der Liste der Aktionen unter **Benachrichtigungen** die Option **Benachrichtigung an E-Mail-Adresse senden** und wählen Sie dann den Empfänger aus der Liste.
16. Geben Sie einen Betreff und eine Nachricht für die E-Mail ein.
17. **Save (Speichern)** anklicken.

Audio

Videoaufzeichnungen mit Audio ergänzen

Audio aktivieren:

1. Gehen Sie auf **Video > Videostream > Audio** und beziehen Sie Audio ein.
2. Wenn das Gerät über mehrere Eingangsquellen verfügt, wählen Sie unter **Quelle** die richtige aus.
3. Gehen Sie auf **Audio > Geräteeinstellungen** und aktivieren Sie die richtige Eingangsquelle.

Das zum Aufzeichnen verwendete Videostreamprofil bearbeiten:

4. Gehen Sie auf **System > Videostreamprofile** und wählen Sie das Videostreamprofil.
5. Wählen Sie **Audio einbeziehen** und aktivieren Sie es.
6. **Save (Speichern)** anklicken.

Ihrem Produkt mithilfe von Portcast Audiofunktion hinzufügen

Mithilfe der Portcast-Technologie können Sie Ihrem Produkt eine Audiofunktion hinzufügen. Sie ermöglicht Audio- und E/A-Kommunikation digital über das Netzkabel zwischen Kamera und Schnittstelle.

Um dem Axis Netzwerk-Videogerät eine Audiofunktion hinzuzufügen, verbinden Sie das Portcast-fähige Axis Audiogerät und die E/A-Schnittstelle mit Ihrem Gerät und dem PoE-Switch für die Stromversorgung.

1. Verbinden Sie das Axis Netzwerk-Videogerät (1) und Axis Portcast-Gerät (2) mit einem PoE-Kabel.
2. Schließen Sie das Axis Portcast-Gerät (2) und den PoE-Switch (3) über ein PoE-Kabel an.



- 1 *Axis Netzwerk-Videogerät*
- 2 *Axis Portcast-Gerät*
- 3 *Switch*

Sobald die Geräte angeschlossen sind, wird in den Einstellungen Ihres Axis Netzwerk-Videogeräts eine Audio-Registerkarte angezeigt. Aktivieren Sie auf der Registerkarte „Audio“ die Option **Audio zulassen**.

Weitere Informationen finden Sie im Benutzerhandbuch zu Ihrem Axis Portcast-Gerät.

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 **Home (Startseite)**.
2. Gehen Sie zu **Live**.
3. Klicken Sie auf das Pfeilsymbol auf dem registrierten Kennzeichen in der Liste.
4. Klicken Sie auf **Append plate to list (Kennzeichen zur Liste hinzufügen)**.
5. Wählen Sie im Dialog die Liste, der das Fahrzeugkennzeichen hinzugefügt werden soll.
6. Klicken Sie auf **Append (Anhängen)**.

Hinweis

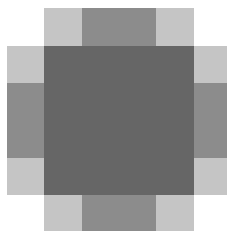
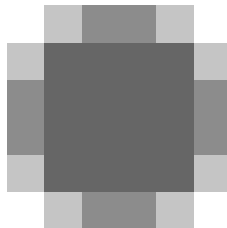
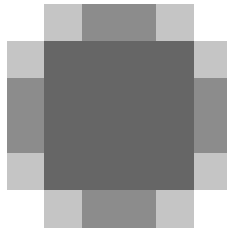
Achten Sie darauf, dass die Symbole <, > und & weder im Fahrzeugkennzeichen noch in der Beschreibung verwendet werden.

Beschreibungen zu Fahrzeugkennzeichen hinzufügen

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

- Gehen Sie zu **Listenverwaltung**.

- Wählen Sie das Fahrzeugkennzeichen aus und klicken Sie auf



. Wählen Sie dann im Drop-Down-Menü **Edit (Bearbeiten)**.

- Geben Sie die relevanten Informationen in das Feld **Description (Beschreibung)** ein.
- **Save (Speichern)** anklicken.

Hinweis

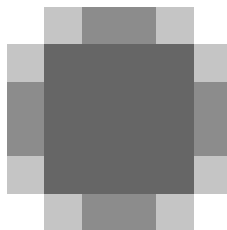
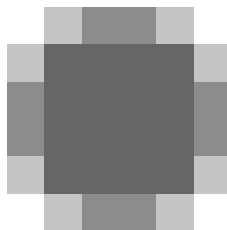
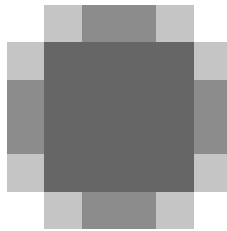
Achten Sie darauf, dass die Symbole **<**, **>** und **&** weder in den Fahrzeugkennzeichen noch in den Beschreibungen verwendet werden.

Listennamen anpassen

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

1. Gehen Sie zu **Listenverwaltung**.

2. Klicken Sie auf



neben der Liste, die Sie ändern möchten.

3. Wählen Sie **Edit (Bearbeiten)**.
4. Geben Sie den Namen der Liste ein.
5. **Submit (Absenden)** anklicken.

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: `license plate, date, description`

Beispiel:

Nur Fahrzeugkennzeichen: `AXIS123`

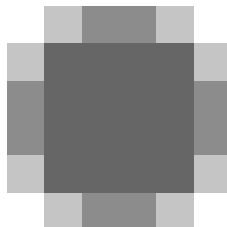
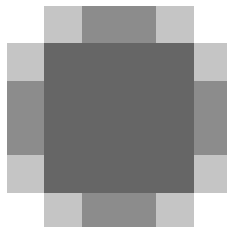
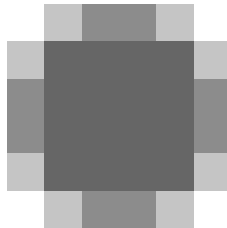
Fahrzeugkennzeichen + Beschreibung: `AXIS123, , John Smith`

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

Hinweis

Achten Sie darauf, dass die Symbole <, > und & weder in den Fahrzeugkennzeichen noch in den Beschreibungen verwendet werden.

1. Gehen Sie zu **Listenverwaltung**.
2. Klicken Sie auf



neben **Allowlist (Zulassungsliste)** und wählen Sie **Import (Importieren)** aus dem Drop-Down-Menü.

3. Auf dem Computer eine CSV-Datei auswählen.
4. Klicken Sie auf **OK**.
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 Kennzeichen-Listen der anderen Kameras außer Kraft gesetzt.

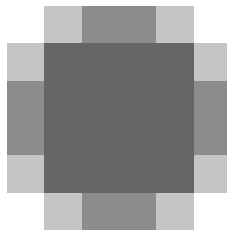
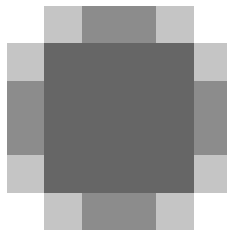
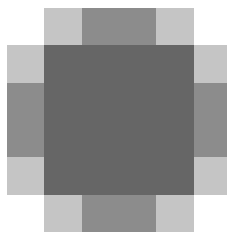
1. Gehen Sie zu **Listenverwaltung (List management) > List synchronization (Listensynchronisierung)**.
2. Geben Sie unter **Remote connected devices (Entfernt verbundene Geräte)** die IP-Adresse, den Benutzernamen und das Kennwort ein.
3. Klicken Sie auf **Hinzufügen**.

4. Klicken Sie auf **Synchronize list (Liste synchronisieren)**.
5. Überprüfen, ob Datum und Uhrzeit unter **Last sync (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:

- Gehen Sie zu **Listenverwaltung**.
- Klicken Sie auf



neben der Liste, die Sie ändern möchten.

- Wählen Sie im Drop-Down-Menü die Option **Schedule (Planen)**.
- Wählen Sie Start- und Endzeit sowie den Tag aus, an dem die Liste aktiv sein soll.
- Klicken Sie auf die Schaltfläche neben **Enabled (Aktiviert)**.
- **Save (Speichern)** anklicken.

Weitere Einstellungen

Text-Overlay konfigurieren

Ein Text-Overlay zeigt die folgenden Ereignisinformationen in der Live-Ansicht an: `weekday`, `month`, `time`, `year`, `license plate number`.

1. Wechseln Sie zu **Settings (Einstellungen) > Image (Bild)**.
2. Aktivieren Sie **Text-Overlay**.
3. Wählen Sie entweder **Timestamp and license plate (Zeitstempel und Kennzeichen)** oder **License plate only (Nur Kennzeichen)**.
4. Die Option **Overlay duration (Overlay-Dauer)** auf einen Wert zwischen 1 und 9 Sekunden festlegen.
5. Sicherstellen, dass das Overlay in der Live-Ansicht angezeigt wird.

Kennzeichen bei schlechten Lichtverhältnissen erkennen

Jede Erfassung erhält durch den Algorithmus eine Punktzahl, die als Vertrauensschwelle bezeichnet wird. Erfassungen mit einer niedrigeren Punktzahl als der ausgewählte Wert werden in der Ereignisliste nicht angezeigt.

Für Szenen mit dunklen Lichtbedingungen können Sie eine niedrigere Vertrauensschwelle festlegen, wodurch mehr Kennzeichen erkannt werden können.

1. Wechseln Sie zu **Settings (Einstellungen) > Recognition (Erkennung)**.
2. Passen Sie den Schieber unter **Confidence threshold (Vertrauensschwelle)** an.
3. Stellen Sie sicher, dass der Algorithmus die Kennzeichen wie erwartet erfasst.

Weniger Zeichen bei Fahrzeugkennzeichen erlauben

Die Anwendung verfügt standardmäßig über eine Mindestanzahl von Zeichen, damit ein Kennzeichen erkannt werden kann. 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) > Recognition (Erkennung)**.
2. Passen Sie unter **Number of characters (Anzahl der Zeichen)** den Schieber an, um die Mindestanzahl der zulässigen Zeichen festzulegen.
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. Einige Szenarien benötigen allerdings eine exakte Übereinstimmung aller Zeichen des Kennzeichens.

1. Gehen Sie zu **Listenverwaltung**.
2. Klicken Sie hier, um **Strikter Abgleich** zu aktivieren.
3. Stellen Sie sicher, dass die Anwendung die Kennzeichen wie erwartet abgleicht.

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) > Recognition (Erkennung)**.

2. Wählen Sie unter **Zulässige Zeichenabweichung** die Anzahl an Zeichen auf, die sich unterscheiden dürfen.
3. Stellen Sie sicher, dass die Anwendung die Kennzeichen wie erwartet abgleicht.

Bedienern begrenzten Zugriff geben

Bedienern kann über eine URL begrenzter Zugriff auf die App gewährt werden. So haben sie nur Zugriff auf das Ereignisprotokoll und die 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. Wählen Sie unter HTTPS entweder **Self-signed (Selbstsigniert)** oder **CA-signed (CA-signiert)**.

Hinweis

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

Sichern und Wiederherstellen von App-Einstellungen

Sie können die in der App vorgenommenen Einstellungen zu Bildaufnahme, Sicherheit, Erkennung und Integration sichern und wiederherstellen. Falls ein Fehler auftritt, können Sie die gesicherten Einstellungen wiederherstellen.

So sichern Sie App-Einstellungen:

- Wechseln Sie zu **Settings > Maintenance (Einstellungen > Wartung)**.
- Klicken Sie auf **Download backup configuration (Sicherungskonfiguration herunterladen)**.

Eine JSON-Datei wird im Downloadordner gespeichert.

App-Einstellungen wiederherstellen:

- Wechseln Sie zu **Settings > Maintenance (Einstellungen > Wartung)**.
- Klicken Sie auf **Restore configuration (Konfiguration wiederherstellen)**.

Wählen Sie die JSON-Datei mit der Sicherungskopie aus.

Die Einstellung wird automatisch wiederhergestellt.

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)**.
- **Yes (Ja)** anklicken

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.

Anforderungen:

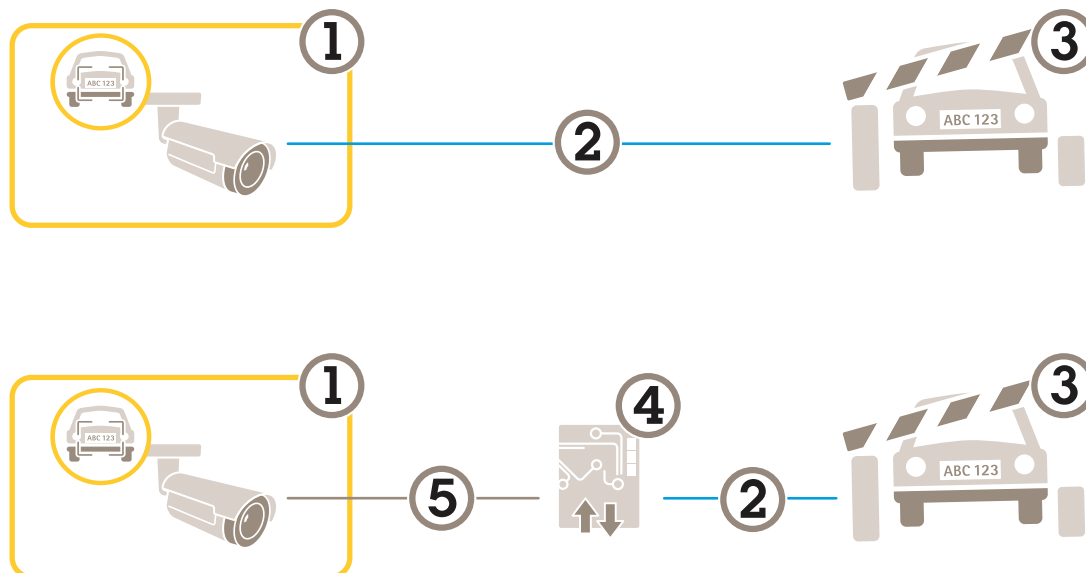
- Physisch installierte und an das Netzwerk angeschlossene Kamera

- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
 - Kabel zwischen Schranke und E/A-Port der Kamera angeschlossen.
 - Die Grundeinstellungen wurden vorgenommen Siehe .
1. Die Webseite der Anwendung aufrufen und dort die Registerkarte **Einstellungen** wählen.
 2. Gehen Sie zu **Zutrittskontrolle**.
 3. Wählen Sie unter **Access control (Zutrittskontrolle)** die Option **Internal I/O (Interne E/A)**.
 4. Wählen Sie die **E/A-Ausgangsnr.**
 5. Wählen Sie in der Auswahlliste **Virtueller Port** einen Port aus.
 6. Wählen Sie unter **Barrier mode (Barriere-Modus)** die Option **Open to all (Für alle öffnen)**.
 7. Wählen Sie unter **Vehicle direction (Fahrzeugrichtung)** die Option **Any (Beliebig)**.
 8. Wählen Sie den gewünschten **Area of interest (Ausgewählter Bereich)** aus.
 9. Wechseln Sie zu die Webseite der Kamera zu **System > Ereignisse**.
 10. Klicken Sie auf **Add rule (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. **Save (Speichern)** anklicken.
 17. Gehen Sie auf **Video > Overlays**.
 18. Rufen Sie **Overlays** auf.
 19. Wählen Sie im Auswahlménü 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.

Anforderungen:

- Physisch installierte und an das Netzwerk angeschlossene Kamera
 - AXIS License Plate Verifier wird auf der Kamera ausgeführt.
 - Kabel zwischen Schranke und Relaismodul angeschlossen
 - Die Grundeinstellungen wurden vorgenommen Siehe *Grundeinstellungen, on page 6*.
1. Die Webseite der Kamera aufrufen, **Einstellungen** auswählen und **AXIS License Plate Verifier** öffnen.
 2. Die Webseite des Relaismoduls aufrufen und sicherstellen, dass der Relaisport an den E/A-Port der Kamera angeschlossen ist.
 3. Die IP-Adresse des Relaismoduls kopieren.
 4. Rufen Sie erneut **AXIS License Plate Verifier** auf.
 5. Rufen Sie **Settings (Einstellungen) > Access control (Zutrittskontrolle)** auf.
 6. Rufen Sie **Type (Typ)** auf und wählen Sie im Drop-Down-Menü die Option **Relais** aus.
 7. Wählen Sie in der Auswahlliste **E/A-Ausgang** den an die Schranke angeschlossenen E/A-Port aus.
 8. Wählen Sie in der Auswahlliste **Schrankenmodus Über Listen öffnen** und überprüfen Sie dann die Freigabeliste.

9. Im Aufklappenmenü **Vehicle direction (Fahrzeugrichtung)** in **(Einfahrt)** wählen.
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. Die Funktionsfähigkeit der Verbindung überprüfen. Dazu **Connect (Verbinden)** anklicken.
13. Um die Verbindung zu aktivieren, klicken Sie auf **Integration einschalten**.
14. Gehen Sie auf die Registerkarte **Listenverwaltung**.
15. Geben Sie das Fahrzeugkennzeichen in das Feld **Freigabeliste** ein.

Hinweis

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

16. Überprüfen Sie, ob der Antrag das Kennzeichen in der Zulassungsliste 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:

- 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 .
1. Gehen Sie auf die Webseite der Anwendung, gehen Sie zu **Home (Startseite)** und fügen Sie die entsprechenden Fahrzeugkennzeichen einer Liste hinzu. Siehe *Erfasstes Fahrzeugkennzeichen der Liste hinzufügen, on page 20*
 2. Um die Listen direkt zu bearbeiten, wechseln Sie zu **List management (Listenverwaltung)**.
 3. Geben Sie die autorisierten Kfz-Kennzeichen in das Feld **Allowlist (Zulässigkeitsliste)** ein.
 4. **Settings (Einstellungen)** aufrufen.
 5. Wählen Sie unter **Access control (Zutrittskontrolle)** die Option **Internal I/O (Interne E/A)**.
 6. Wählen Sie die **E/A-Ausgangsnr.**
 7. Wählen Sie unter **Barrier mode (Barriere-Modus)** die Option **Open from lists (Aus Listen öffnen)** und prüfen Sie dann **Allowlist (Zulassungsliste)**.
 8. Im Aufklappenmenü **Vehicle direction (Fahrzeugrichtung)** in **(Einfahrt)** wählen.
 9. Wählen Sie in **Area of interest (Ausgewählter Bereich)** den in Frage kommenden ausgewählten Bereich oder wählen Sie alle Bereiche.
 10. Überprüfen Sie, ob der Antrag das Kennzeichen in der Zulassungsliste 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

Dieses Beispiel erläutert, wie die Anwendung/Kamera eingestellt wird, damit eine durch ein Ereignis ausgelöste Benachrichtigung versendet wird.

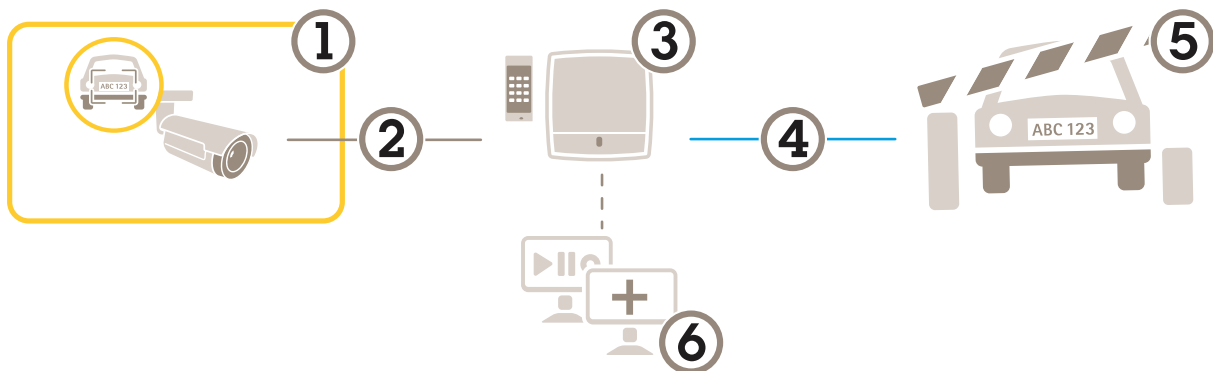
Anforderungen:

- Die Grundeinstellungen wurden vorgenommen Siehe *Grundeinstellungen, on page 6*.
- 1. Gehen Sie zu **Listenverwaltung**.
- 2. Geben Sie das Fahrzeugkennzeichen in das Feld **Sperrliste** ein.
- 3. Die Webseite der Kamera aufrufen.
- 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.

Anforderungen:

- Die Kamera und die Türsteuerung sind physisch installiert und an das Netzwerk angeschlossen
- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
- Die Grundeinstellungen wurden vorgenommen Siehe *Grundeinstellungen, on page 6*.



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. Klicken Sie auf **Next (Weiter)**.

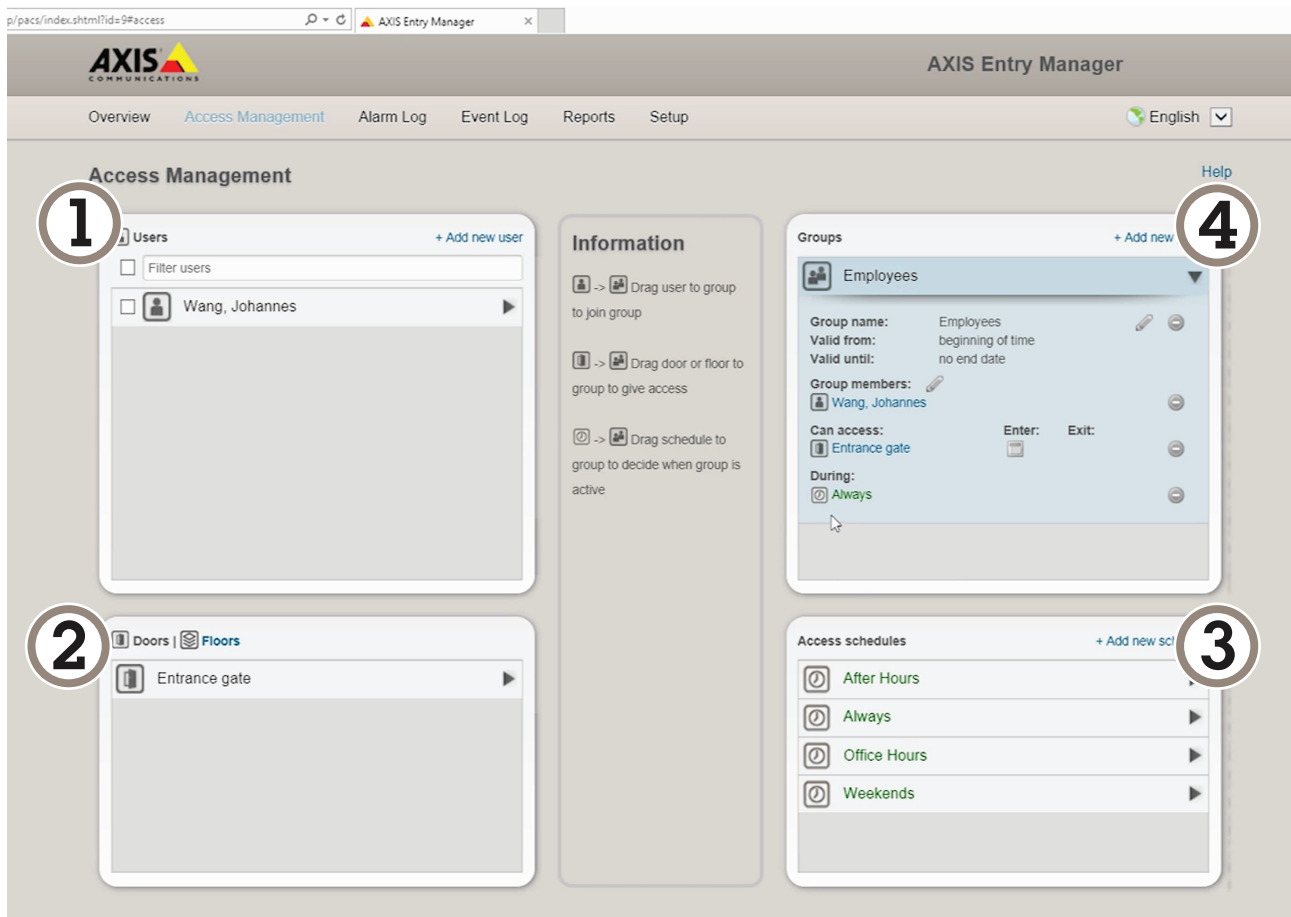
4. In **Configure locks connected to this controller** (An diese Steuerung angeschlossene Schlösser konfigurieren) die Option **Door monitor** (Türmonitor) deaktivieren.
5. Klicken Sie auf **Next** (Weiter).
6. In **Configure readers connected to this controller** (An diese Steuerung angeschlossene Lesegeräte konfigurieren) die Option **Exit reader** (Ausgangslesegerät) deaktivieren.
7. Klicken Sie auf **Finish** (Fertig).

Konfiguration in AXIS License Plate Verifier

1. Die Webseite von **AXIS License Plate Verifier** aufrufen.
2. Wechseln Sie zu **Settings (Einstellungen) > Access control (Zutrittskontrolle)**.
3. Gehen Sie zu **Typ** und wählen Sie in der Auswahlliste **Controller**.
4. Geben Sie folgende Informationen ein:
 - die IP-Adresse der Steuerung im Format 192.168.0.0
 - den Benutzernamen für die Steuerung
 - das Kennwort für die Steuerung
5. **Connect (Verbinden)** anklicken.
6. Bei erfolgreichem Verbindungsaufbau wird im Aufklappmenü **Bezeichnung der Netzwerktürsteuerung** „Eingangssteuerung“ angezeigt. „Eingangssteuerung“ wählen.
7. Wählen Sie im Auswahlmenü **Reader Name (Name des Lesers)** den Kartenleser aus, der mit dem Zugang „Gatecontroller“ (Eingangssteuerung) verbunden ist, z. B. „Reader entrance“ (Leser Zugang)). Diese Namen können im **AXIS Entry Manager** geändert werden.
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. **AXIS Entry Manager** aufrufen.
2. **Zugangsverwaltung** aufrufen.
3. **Doors > Add identification type (Türen > Identifizierungstyp hinzufügen)** aufrufen.
4. Aus dem Aufklappmenu **Erforderliche Berechtigungsnachweise** die Option **Nur Fahrzeugkennzeichen** wählen.
5. Um Nutzungszeiten für den Identifikationstyp vorzugeben, einen **Zeitplan** auf die Tür ziehen und ablegen.
6. Benutzer hinzufügen und für jeden Benutzer den Berechtigungsnachweis **Fahrzeugkennzeichen** hinzufügen.
7. Erneut **Berechtigungsnachweis hinzufügen** anklicken und das Fahrzeugkennzeichen eingeben.
8. **Gruppe hinzufügen** anklicken und die entsprechenden Informationen eingeben.
9. Um einer Gruppe Benutzer hinzuzufügen, ziehen Sie per **Drag and Drop Benutzer** in die Benutzergruppe.
10. Um Benutzern Zugang zu gewähren, **Tür** auf die Benutzergruppe ziehen und ablegen.
11. Um Zugangszeiten vorzugeben, einen **Schedule (Zeitplan)** auf die Benutzergruppe ziehen und ablegen.



Übersicht über die Benutzeroberfläche von AXIS Entry Manager.

- 1 Benutzer
- 2 Türen
- 3 Zeitschemata
- 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.

Anforderungen:

- Die Kamera und die Türsteuerung sind physisch installiert und an das Netzwerk angeschlossen
- AXIS License Plate Verifier wird auf der Kamera ausgeführt.
- AXIS Camera Station Client Version 5.49.449 oder höher.
- Die Grundeinstellungen wurden vorgenommen Siehe *Grundeinstellungen, on page 6*.

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 hinzuzufügen.
6. Wechseln 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. **Connect (Verbinden)** anklicken.
10. Wählen Sie im Auswahlménü unter **Türsteuerung** die gewünschte Türsteuerung.
11. Wählen Sie im Auswahlménü 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 *Den ausgewählten Bereich anpassen, on page 10*.
15. Doppelklicken Sie auf **Next (Weiter)** und dann auf **Finish (Fertigstellen)**.

Freie Fahrt-Szenario mit Geschwindigkeitsmessung

Bei einem Free-Flow-Szenario mit Geschwindigkeitsmessung wird die Kamera durch die Edge-to-Edge-Technologie mit einem Axis Radar gekoppelt. Die Kamera deckt zwei Spuren ab und liest die Fahrzeugkennzeichen der vorbeifahrenden Fahrzeuge. Das gekoppelte Radar erfasst zur Messung der Geschwindigkeit von Fahrzeugen die gleichen zwei Spuren. Zusätzlich kann die Anwendung *AXIS Speed Monitor* über Overlays in der Live-Ansicht der Kamera die maximale Geschwindigkeit in jeder Spur visualisieren.

Weitere Informationen zu Edge-to-Edge finden Sie unter *Edge-to-Edge-Technologie, on page 44*.

Erforderlich:

- Ein AXIS License Plate Verifier Kameraset und *AXIS D2210-VE Radar* sind installiert und an das Netzwerk angeschlossen

Einrichten des Szenarios

Richten Sie das Szenario in vier Schritten ein: Konfigurieren Sie zunächst die Kamera, koppeln und konfigurieren Sie dann das Radar und fügen Sie schließlich per *AXIS Speed Monitor* Overlays hinzu.

Vorbereitungen:

- Stellen Sie sicher, dass Kamera und Radar auf denselben ausgewählten Bereich ausgerichtet sind.
- Stellen Sie sicher, dass Kamera und Radar zeitsynchronisiert sind. Um den Status zu überprüfen, wechseln Sie zu **Installation > Time sync status (Installation > Zeitsynchronisierungsstatus)** in den einzelnen Geräten.
- Stellen Sie sicher, dass der zweite Sichtbereich (**View area 2 (Sichtbereich 2)**) der Kamera nicht verwendet wird, da das Radar ihn nach der Kopplung verwendet.

Die Kamera konfigurieren:

1. Richten Sie die Kamera gemäß den Anweisungen in *Grundeinstellungen, on page 6* ein.
2. Stellen Sie bei der Installation des Setup-Assistenten sicher, dass der freie Datenstrom ausgewählt ist. Weitere Informationen finden Sie unter *Freie Fahrt, on page 8*.

Die Kamera mit einem Radar koppeln:

1. Gehen Sie auf der Weboberfläche der Kamera auf **System > Edge-to-edge > Radar pairing (System > Edge-to-Edge-> Radar-Kopplung)**.
2. Geben Sie den Hostnamen, den Benutzernamen und das Kennwort des Radars ein.
3. Klicken Sie auf **Connect (Verbinden)**, um die Geräte zu koppeln. Sobald eine Verbindung hergestellt ist, werden die Radareinstellungen über die Weboberfläche der Kamera angezeigt.

Hinweis

Die Standard-Auflösung des gekoppelten Radars beträgt 1280 x 720. Behalten Sie die Standard-Auflösung des Radars in der Weboberfläche der Kamera bei, wenn Sie sie zu einem VMS hinzufügen.

Den Radar konfigurieren:

1. Gehen Sie auf die Weboberfläche der Kamera zu **Radar > Scenarios (Radar > Szenarien)**.
2. Fügen Sie ein Radarszenario hinzu, das eine Spur abdeckt und ein zweites Radarszenario, das die andere Spur abdeckt.
3. Wählen Sie für beide Szenarien **Movement in area (Bewegung im Bereich)**, mit Auslöser für **Vehicles (Fahrzeuge)** und legen Sie ein **Speed limit (Geschwindigkeitslimit)**. Weitere Informationen hierzu finden Sie unter *Szenarien hinzufügen* im Benutzerhandbuch des *AXIS D2210-VE Radars*.

Hinweis

Wenn Sie über den *AXIS License Plate Verifier* Overlays mit Fahrzeugkennzeicheninformationen hinzufügen möchten, müssen Sie diese hinzufügen, bevor Sie Overlays in *AXIS Speed Monitor* hinzufügen.

Verwenden Sie *AXIS Speed Monitor*, um Geschwindigkeits-Overlays hinzuzufügen:

1. Laden Sie AXIS Speed Monitor herunter und installieren Sie diesen auf Ihrer Kamera.
2. Fügen Sie für jede Spur ein Overlay hinzu, das die maximale Geschwindigkeit in der Live-Ansicht der Kamera angibt.
Anweisungen zur Installation und Konfiguration finden Sie im *Benutzerhandbuch von AXIS Speed Monitor*.

Suche nach bestimmten Ereignissen

Verwenden Sie die Suchfunktion, um anhand einer Reihe von Kriterien nach Ereignissen zu suchen.

1. Gehen Sie auf die Webseite der Anwendung und wählen Sie die Seite **Search (Suche)**.
2. Wählen Sie das Datum in den Kalendermenüs **From (Von)** und **To (Bis)** aus.
3. Klicken Sie auf das Drop-Down-Menü **AOI**, um auszuwählen, welcher ausgewählte Bereich in die Suche einbezogen werden soll.
4. Wählen Sie **Direction (Richtung)**, um nach Eingang oder Ausgang zu filtern.
5. Geben Sie im Feld **Kennzeichen** das Fahrzeugkennzeichen ein, wenn Sie nach einem Kennzeichen suchen möchten.
6. Um Fahrzeugkennzeichen zu finden, die zu einem bestimmten Land gehören, wählen Sie ein Land aus der Drop-Down-Liste **Country (Land)** aus.
7. Um Bilder basierend auf der Ansicht des Fahrzeugs zu filtern, wählen Sie **Front (Vorn)** oder **Rear (Hinten)** in der Dropdown-Liste **Vehicle view (Fahrzeugansicht)**.
8. Um die Suchergebnisse nach Marke, Modell, Typ oder Farbe des Fahrzeugs zu filtern, wählen Sie in den Drop-Down-Menüs **Vehicle details (Fahrzeugdetails)** die gewünschten Kriterien aus.
9. Klicken Sie auf **Apply filters (Filter anwenden)**, um die Suchergebnisse anzuzeigen.

Suchergebnisse exportieren und freigeben

Um ein beliebiges Suchergebnis als CSV-Datei mit den damaligen Statistiken zu exportieren, klicken Sie auf **Export (Exportieren)**, um die Ergebnisse als CSV-Datei zu speichern

Um die API als Link zu kopieren, der zum Export von Daten in Drittsysteme verwendet werden kann, klicken Sie auf **Copy search link (Suchlink kopieren)**.

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. Gehen Sie zu **Integration** und zur Seite **Push events (Push-Ereignisse)**.
2. Wählen Sie **Profile 1 (Profil 1)**.
3. Regel konfigurieren Siehe *Ereignisinformationen an die Software anderer Hersteller per Push senden, on page 38*.
4. Regel testen.
5. Wählen Sie eine neue Profilregisterkarte aus, um eine neue Regel zu konfigurieren.

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 können lässt sich Software anderer Hersteller integrieren. Dabei werden der Ereignisdaten per Push mittels TCP oder HTTP POST übertragen.

Vorbereitungen:

- Die Kamera muss physisch installiert und an das Netzwerk angeschlossen sein.
 - AXIS License Plate Verifier wird auf der Kamera ausgeführt.
1. Gehen Sie zu **Integration > Ereignisse per Push senden**.
 2. Ein leeres Profil auswählen
 3. Wählen Sie in der Auswahlliste **Protocol (Protokoll)** die Option **HTTP POST**.
 4. Geben Sie in das Feld **Server URL (Server-URL)** die Server-Adresse und den Port im folgenden Format ein: `127.0.0.1:8080`
 5. Geben Sie den Benutzernamen und das Kennwort ein.
 6. Falls Sie einen Proxy verwenden, schalten Sie diesen ein und geben Sie den Host-Name, den Benutzernamen und das Kennwort ein.
 7. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein oder lassen Sie den vorgegebenen Namen stehen.
 8. Wählen Sie unter **Push conditions (Push-Bedingungen)** aus, in welcher Richtung Push-Ereignisse ausgelöst werden sollen.
 9. Wählen Sie unter **LPR Event types (LPR-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.
 - **Conditional (Bedingt)** sendet ein Ereignis für ein Objekt, wenn die Bedingungen erfüllt sind.
 10. Um die Bandbreite bei der Verwendung von HTTP POST zu reduzieren, können Sie **Do not to send images (Keine Bilder senden)** auswählen.
 11. Aktivieren Sie **Event buffer (Ereignispuffer)**, um Ereignisse zu puffern, wenn der Server ausfällt, und senden Sie sie, sobald der Server wieder verfügbar ist.

12. Um zusätzlich zum Bild auch den Ausschnitt mit dem Kennzeichen einzufügen, wählen Sie unter **Retention settings (Aufbewahrungseinstellungen)** die Option **Send two images (Zwei Bilder senden)**.
13. Um die Ereignisse im Multipart-Format anstelle von Base64 zu senden, wählen Sie **Multipart**.
14. Klicken Sie auf **Test**, um die Integration mit einem virtuellen Fahrzeugkennzeichen zu testen.
15. Um die Funktion zu aktivieren, wählen Sie **Activate (Aktivieren)**.

Hinweis

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

Bilder von Nummernschildern an einen Server senden

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

Vorbereitungen:

- Die Kamera muss physisch installiert und an das Netzwerk angeschlossen sein.
 - AXIS License Plate Verifier wird auf der Kamera ausgeführt.
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 `ftp://10.21.65.77/LPR` ein.
 4. Geben Sie den Benutzernamen und das Kennwort für den FTP-Server ein.
 5. Wählen Sie die Pfad- und Namensmodifikatoren für die Dateinamen aus.
 6. Geben Sie in das Feld **Geräte-ID** den Namen des Geräts ein. Für die Bilder wird ein Ordner mit diesem Namen erstellt. Für die Bilder wird das folgende Namensformat verwendet: `Zeitstempel_ausgewählter Bereich_Richtung_FahrzeugID_Kennzeichentext_Land.jpg`.
 7. Wählen Sie unter **Push conditions (Push-Bedingungen)** aus, in welcher Richtung Push-Ereignisse ausgelöst werden sollen.
 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.
 - **Lost (Verloren)** ist das letzte verfolgte Ereignis des Kennzeichens, bevor es das Bild verlässt. Es enthält auch die Richtung des Kennzeichens.
 - **Conditional (Bedingt)** sendet ein Ereignis für ein Objekt, wenn die Bedingungen erfüllt sind.

Hinweis

Die Richtung ist nur im Dateinamen enthalten, wenn **Verloren** oder **Aktualisieren** ausgewählt wurde.

9. Klicken Sie auf **Test**, um die Integration mit einem virtuellen Fahrzeugkennzeichen zu testen.
10. Um die Funktion zu aktivieren, klicken Sie auf **Activate (Aktivieren)**.

Hinweis

Beachten Sie, dass das Bild je nach ausgewähltem Aufnahmemodus anders aussehen kann, siehe *Bilderfassungseinstellungen anpassen, on page 11*.

Hinweis

Wenn das Senden der Ereignisse per Push fehlschlägt, sendet die App maximal die ersten 100 Ereignisse erneut an den Server.

Wenn Sie für das Senden von Ereignissen per Push an einen Windows-Server FTP nutzen, verwenden Sie im Namen von Bildern mit Datums- und Uhrzeitangabe nicht „%c“. Windows unterstützt die Funktion %c für

Datum und Uhrzeit im Dateinamen nicht. Bei Verwendung eines Linux-Servers hingegen besteht hier kein Problem.

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 **Nummernschilderkennung**.
6. Kopieren Sie die IP-Adresse.

In der App AXIS License Plate Verifier:

1. Gehen Sie zu **Integration > Direkte Integration**.
2. Wählen Sie **2N IP Device (2N IP-Gerät)**.
3. Fügen Sie dem 2N-Gerät die IP-Adresse oder URL hinzu.
4. Geben Sie Ihren Benutzernamen und das Kennwort ein.
5. Wählen Sie **Verbindungstyp**.
6. Wählen Sie, wofür die **Schranke verwendet wird**.
7. **Integration aktivieren** anklicken.
8. Wählen Sie die Fahrtrichtung der Fahrzeuge aus.
9. Um die Funktion zu aktivieren, wählen Sie **Activate (Aktivieren)**.

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 auf **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 **Next (Weiter)**.
7. Klicken Sie auf **Next (Weiter)**.
8. Klicken Sie auf **Next (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 in **API path prefix (API-Pfadpräfix)** lpr ein.
13. Wählen Sie in **REST-Port** 443.
14. Geben Sie in **WebSDK host (WebSDK-Host)** localhost ein.
15. Wählen Sie im **WebSDK-Port** 443.
16. Markieren Sie **Selbstsignierte Zertifikate** zulassen.

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

17. Markieren Sie **Aktiviert**.
18. Geben Sie in **Name Security Center Lpr Events (Lpr-Ereignisse Security Center)** ein.
19. Wählen Sie unter im Auswahlmenü unter **Verarbeitungsfrequenz** die Option **5 Sek.**
20. Wechseln Sie zur Registerkarte **Data sinks (Datensenken)**.
21. **+** anklicken.
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 **Name Lese-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. Benutzernamen und Kennwort eingeben. 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 **Anwenden**.

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

1. Gehen Sie zu **Integration > Direct integration (Direkte Integration)**.
2. Wählen Sie **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. Wählen Sie **Verbindungstyp**.
6. Um die Funktion zu aktivieren, wählen Sie **Activate (Aktivieren)**.
7. Klicken Sie auf **Test**, um die Integration mit einem virtuellen Fahrzeugkennzeichen zu testen.
8. Wenn Sie **HTTPS** ausgewählt haben, gehen Sie zur Registerkarte **Settings (Einstellungen)**.
9. Unter **Sicherheit > HTTPS**.
10. 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).*

Weboberfläche

Um sich über alle Funktionen und Einstellungen zu informieren, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, rufen Sie die *Hilfe zur Weboberfläche von AXIS OS* auf.

Mehr erfahren

Edge-to-Edge-Technologie

Edge-to-Edge ist eine Technologie, mit der IP-Geräte direkt miteinander kommunizieren. Sie bietet eine intelligente Koppelungsfunktion z. B. zwischen Axis Kameras und Axis Audio- oder Radarprodukten.

Hinweis

Stellen Sie sicher, dass die gekoppelten Geräte dieselbe AXIS OS-Version verwenden.

Weitere Informationen finden Sie im Whitepaper „Edge-to-Edge-Technologie“ unter whitepapers.axis.com/edge-to-edge-technology.

Radarkopplung

Mit einer Edge-to-Edge-Radarkopplung können Sie Ihre Kamera an ein kompatibles Axis Radarsystem anschließen und von integrierten Radarfunktionen wie der Geschwindigkeitserfassung profitieren.

Radarkopplung ist ein Einweg-Setup, bei dem eine Kamera mit einem Radar gekoppelt und mit dieser beide Geräte konfiguriert und verwaltet werden. Über die Kopplung können Sie auf die Radareinstellungen zugreifen und direkt über die Weboberfläche der Kamera Regeln für radarspezifische Ereignisse erstellen. Die Kamera identifiziert sich dem VMS als Kamera mit integrierter Radarfunktion.

Der Radarstream wird im zweiten Sichtbereich der Kamera, dem sogenannten **Sichtbereich 2**, visualisiert. Die vom Radar erzeugten Metadaten sind über den zweiten Metadatenkanal der Kamera, **Kanal 2**, verfügbar.

Lautsprecherkopplung

Mit der Edge-to-edge-Lautsprecher-Kopplung können kompatible Netzwerk-Lautsprecher von Axis so eingesetzt werden, als seien sie ein Teil der Kamera. Nach der Kopplung werden die Lautsprecherfunktionen in die Weboberfläche der Kamera integriert. Der Netzwerklautsprecher fungiert als Audio-Out-Gerät, mit dem Sie Audio-Clips wiedergeben und Audiosignale über die Kamera übertragen können.

Die Kamera identifiziert sich zur VMS als Kamera mit integriertem Audioausgang und leitet alle abgespielten Audiosignale an den Lautsprecher weiter.

Anzeigebereich

Ein Sichtbereich ist ein ausgeschnittener Teil einer Gesamtansicht. Um den Bedarf an Bandbreite und Speicherplatz zu minimieren, können Sie anstelle der vollständigen Ansicht Sichtbereiche streamen und speichern. Wenn Sie PTZ für einen Sichtbereich aktivieren, können Sie darin schwenken, neigen und zoomen. Mit Sichtbereichen können Sie Teile der Vollansicht entfernen, z. B. den Himmel.

Für das Einrichten eines Sichtbereichs empfehlen wir, die Auflösung des Videostreams höchstens auf die Größe des Sichtbereichs einzustellen. Wenn die Auflösung des Videostreams auf einen höheren Wert als die Größe des Sichtbereichs eingestellt wird, wird das Video nach der Aufnahme mit dem Sensor digital vergrößert. Dies erfordert eine größere Bandbreite, ohne dass weitere Bildinformationen hinzukommen.

Hinweis

Wenn Sie die Kamera mit einem Radar durch Edge-to-Edge koppeln, wird der Radarstream im zweiten Sichtbereich der Kamera visualisiert.

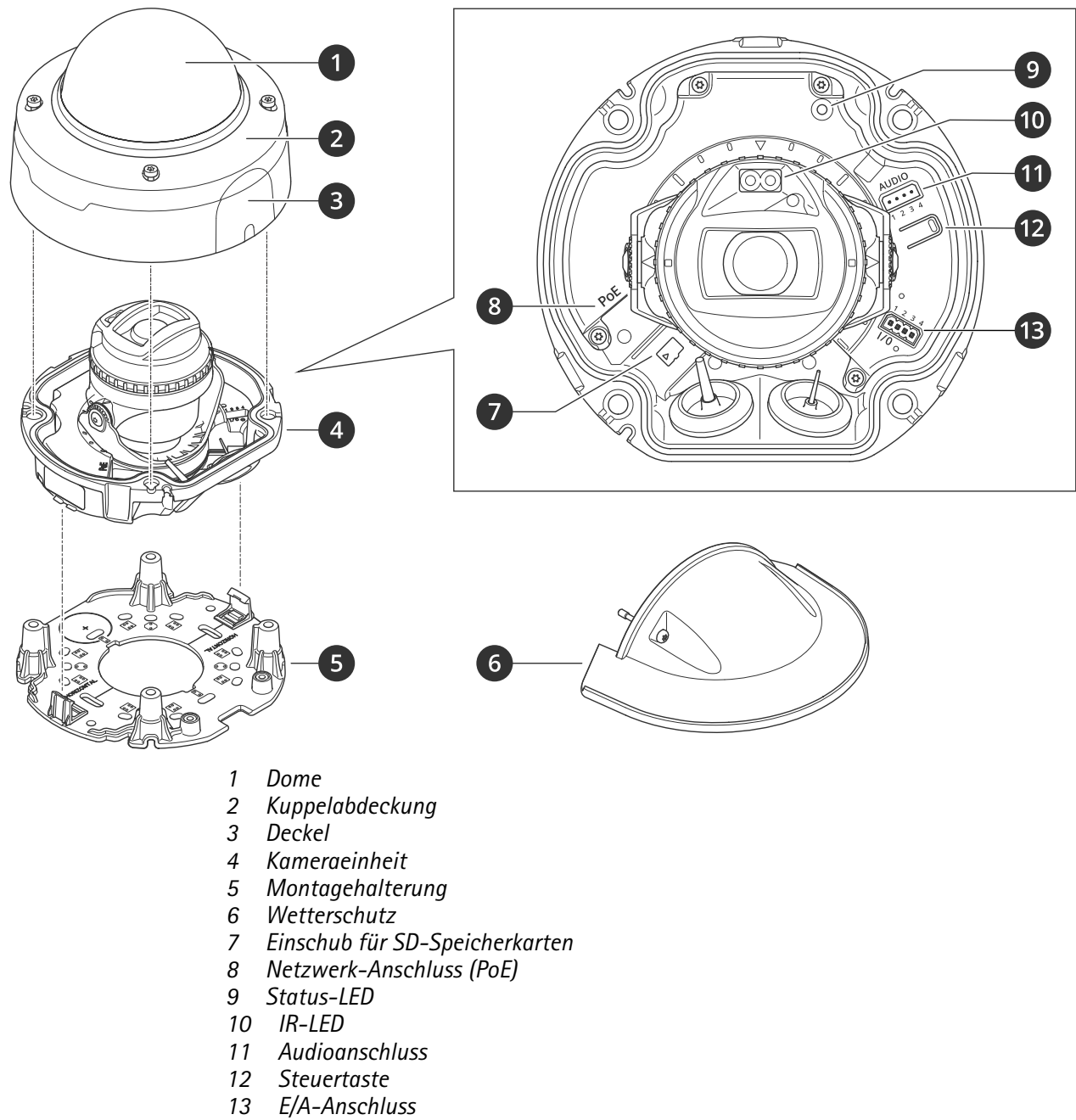
AXIS Image Health Analytics

Mit der KI-basierten Anwendung AXIS Image Health Analytics lassen sich eine nachlassende Bildqualität und Manipulationsversuche erkennen. Die Anwendung analysiert und lernt die Vorgänge in der Szene ein, um Unschärfe, Unterbelichtung sowie eine Abdeckung oder veränderte Ausrichtung des Kamerabilds zu erkennen. Sie können die Anwendung so einstellen, dass sie für jede Erkennung ein Ereignis meldet und über das Ereignissystem der Kamera oder Software von Drittanbietern bestimmte Aktionen auslöst.

Mehr zur Funktionsweise der Anwendung erfahren Sie im *Benutzerhandbuch zu AXIS Image Health Analytics*.

Technische Daten

Produktübersicht



LED-Anzeigen

Status-LED	Anzeige
Aus	Anschluss und Normalbetrieb.
Grün	Leuchtet bei Normalbetrieb nach Abschluss des Startvorgangs 10 Sekunden lang grün.
Gelb	Leuchtet beim Start. Blinkt während Gerätesoftwareaktualisierung und Wiederherstellung der Werkseinstellungen.
Gelb/rot	Blinkt orange/rot, wenn die Netzwerk-Verbindung nicht verfügbar ist oder unterbrochen wurde.

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 per Hand ein. Das Gleiche gilt für das Entfernen.
- 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.

Für Empfehlungen zu SD-Karten siehe 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, on page 48*.

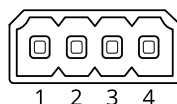
Anschlüsse

Netzwerk-Anschluss

RJ-45-Ethernetanschluss mit Power over Ethernet (PoE).

Audioanschluss

Vierpolige Klemmleiste für Audioeingang und -ausgang.



Funktion	Kontakt	Hinweise
GND	1	Masse
Klingelstrom	2	12 V für externe Quelle
Eingang Mikrofon/ Audio	3	Mikrofon (analog oder Digital) oder Audioeingang (Mono). Eine Mikrofon-Vorspannung von 5 V steht zur Verfügung.
Line-Out	4	Audioausgang (Leistungsstufe, Mono). Zum Anschließen einer Rundrufanlage (PA) oder eines Aktivlautsprechers mit integriertem Verstärker.

E/A-Anschluss

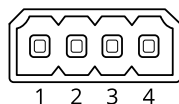
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

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

Überwachter Eingang – Ermöglicht das Erfassen von Manipulation an einem digitalen Eingang.

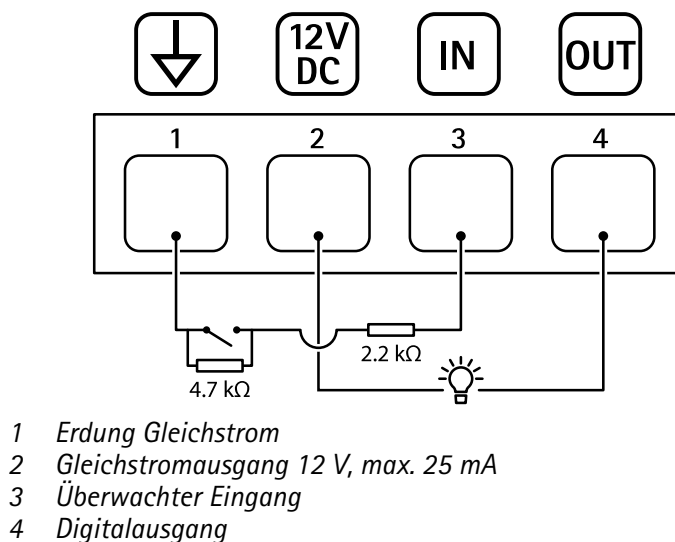
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

4-poliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	 Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Last = 25 mA
Digitaler Eingang oder überwachter Eingang	3	Zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen. Um überwachten Eingang zu nutzen, Abschlusswiderstände anschließen. Informationen zum Anschließen der Widerstände bietet der Schaltplan.	0 bis max. 30 V Gleichstrom
Digitaler Ausgang	4	Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

Beispiel:



Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

⚠️ WARNUNG

⚠️ Von diesem Produkt geht potenziell gefährliche optische Strahlung aus. Diese kann zu Augenschäden führen. Schauen Sie nicht in die aktive Leuchte.

Wichtig

Das Zurücksetzen auf die Werkseinstellungen muss mit Umsicht geschehen. 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 behalten Sie den Lizenzschlüssel. Sie müssen die Anwendung nach dem Zurücksetzen auf die Werkseinstellungen nicht erneut installieren.

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht, on page 45*.
3. Halten Sie die Steuertaste etwa 15–30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. 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 Softwaretools für die Installation und Verwaltung stehen auf den Supportseiten unter axis.com/support zur Verfügung.

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

Optionen für AXIS OS

Axis bietet eine Softwareverwaltung für Geräte entweder gemäß des aktiven Tracks oder gemäß Tracks für Langzeitunterstützung (LTS). Beim aktiven Track erhalten Sie einen kontinuierlichen Zugriff auf alle aktuellen Funktionen des Produkts. Die LTS-Tracks bieten eine feste Plattform, die regelmäßig Veröffentlichungen mit Schwerpunkt auf Bugfixes und Sicherheitsaktualisierungen bereitstellt.

Es wird empfohlen, AXIS OS vom aktiven Track zu verwenden, wenn Sie auf die neuesten Funktionen zugreifen möchten oder Axis End-to-End-Systemangebote nutzen. Die LTS-Tracks werden empfohlen, wenn Sie Integrationen von Drittanbietern verwenden, die nicht kontinuierlich auf den neuesten aktiven Track überprüft werden. Mit LTS kann die Cybersicherheit der Produkte gewährleistet werden, ohne dass signifikante Funktionsänderungen neu eingeführt oder vorhandene Integrationen beeinträchtigt werden. Ausführliche Informationen zur Vorgehensweise von Axis in Bezug auf Gerätesoftware finden Sie unter axis.com/support/device-software.

Aktuelle AXIS OS-Version überprüfen

AXIS OS bestimmt die Funktionalität unserer Geräte. Wir empfehlen Ihnen, vor jeder Problembehebung zunächst die aktuelle AXIS OS-Version zu überprüfen. Die aktuelle Version enthält möglicherweise eine Verbesserung, die das Problem behebt.

So überprüfen Sie die aktuelle AXIS OS-Version:

1. Rufen Sie die Weboberfläche des Geräts > **Status** auf.
2. Die AXIS OS-Version ist unter **Device info (Geräteinformationen)** angegeben.

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.
- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Leitfaden zum Lebenszyklus: Upgrade-Pfad*.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

- Beim Aktualisieren mit der aktuellen AXIS OS-Version im aktiven Track werden auf dem Gerät die neuesten verfügbaren Funktionen bereitgestellt. Lesen Sie vor der Aktualisierung stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise. Die aktuelle AXIS OS-Version und die Versionshinweise finden Sie unter axis.com/support/device-software.
1. Die AXIS OS-Datei können Sie von axis.com/support/device-software kostenlos auf Ihren Computer herunterladen.
 2. Melden Sie sich auf dem Gerät als Administrator an.
 3. Rufen Sie **Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung)** auf und klicken Sie **Upgrade (Aktualisieren)** an.

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.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

Nach fehlgeschlagener Aktualisierung lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche AXIS OS-Datei hochgeladen wurde. Überprüfen, ob der Name der AXIS OS-Datei dem Gerät entspricht und erneut versuchen.

Probleme nach der AXIS OS-Aktualisierung

Bei nach dem Aktualisieren auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurücksetzen.

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

- 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 unter Umständen von einem anderen Gerät verwendet. Zur Überprüfung:
 1. Trennen Sie das Axis Gerät vom Netzwerk.
 2. Geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein.
 3. Erscheint daraufhin `Reply from <IP address>: bytes=32; time=10...`, heißt das, 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.
 4. Wenn Sie `Request timed out` empfangen, bedeutet dies, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
- Es besteht unter Umständen ein Konflikt mit der IP-Adresse eines anderen Geräts 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.

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

Stellen Sie bei aktiviertem HTTPS sicher, dass Sie das richtige Protokoll (HTTP oder HTTPS) bei der Anmeldung verwenden. Gegebenenfalls müssen Sie manuell `http` oder `https` in das Adressfeld des Browsers eingeben.

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 48*.

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. Das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln.

Bei Bedarf können Sie manuell eine statische IP-Adresse zuweisen. 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**.

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 4*.

Externer Zugriff auf das Gerät ist nicht möglich

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

- AXIS Camera Station Edge: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Pro: Kostenlose 90-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

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

Probleme beim Streaming

Auf Multicast H.264 kann nur von lokalen Clients aus 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 sind der Dokumentation zum Adapter zu entnehmen.

Niedrigere Bildrate als erwartet

- Siehe *Leistungsaspekte, on page 53*.
- Verringern Sie die Anzahl der auf dem Clientcomputer ausgeführten Anwendungen.
- Begrenzen Sie die Anzahl der gleichzeitigen Anzeigen.
- Gemeinsam mit dem Netzwerkadministrator prüfen, ob ausreichend Bandbreite zur Verfügung steht.
- Die Bildauflösung verringern.
- Melden Sie auf der Weboberfläche des Geräts an und wählen Sie einen Aufnahmemodus, der die Bildrate bevorzugt behandelt. Die Änderung zu einem Aufnahmemodus, der die Bildrate bevorzugt behandelt, kann je nach verwendeten Gerät und den verfügbaren Aufnahmemodi zu einer geringeren maximalen Auflösung führen.

Die Codierung H.265 steht in der Live-Ansicht nicht zur Verfügung.

Webbrowser unterstützen nicht die Decodierung von H.265. Verwenden Sie ein Videoverwaltungssystem oder eine Anwendung, die das Decodieren von H.265 unterstützt.

Probleme mit MQTT

Verbindung über Port 8883 mit MQTT über SSL kann nicht hergestellt werden

Die Firewall blockiert den Datenaustausch über Port 8883, da dieser als unsicher gilt.

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 in Rücksprache mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.

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

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.

Enthält die Genehmigungsliste z. B. **AXI S1234**, lässt die Anwendung **AXI SI234** passieren.

Gleichmaßen darf **AXI 1234** passieren, wenn sich **AXIS 1234** in der Freigabeliste befindet.

Gehen Sie zu *Weitere Einstellungen*, on page 25, um die zulässigen Zeichen festlegen.

Die Verbindung zwischen Anwendung und Steuergerät oder Relaismodul arbeitet nicht

Vergewissern Sie sich, dass das Steuergerät oder das Relaismodul den Datenaustausch über HTTP zulässt. Wie Sie diese Einstellung ändern können, ist dem Benutzerhandbuch des entsprechenden Geräts zu entnehmen.

Probleme mit der Radarkopplung

Die Kamera kann nicht mit dem Radar gekoppelt werden.

Stellen Sie sicher, dass der zweite Sichtbereich (**View area 2 (Sichtbereich 2)**) der Kamera nicht verwendet wird, da diesem automatisch das Radar zugewiesen wird.

Wenn der zweite Sichtbereich verwendet wird, wechseln Sie zu **Video > View areas (Video > Sichtbereiche)**, um diesen zu entfernen, und versuchen Sie dann erneut, die Geräte zu koppeln.

Die sich bewegenden Fahrzeuge in der Kameraansicht sind nicht mit den Geschwindigkeits-Overlays oder den Spuren in der Radaransicht synchronisiert.	Stellen Sie sicher, dass Kamera und Radar zeitsynchronisiert sind. Um den Status zu überprüfen, wechseln Sie auf der Weboberfläche jedes Geräts auf Status > Time sync status (Status > Status der Zeitsynchronisierung). Wenn als Status Synchronized: No (Synchronisiert: Nein) angezeigt wird, klicken Sie auf NTP settings (NTP-Einstellungen) und wählen Sie eine Zeitquelle für die Synchronisierung des Geräts aus. Stellen Sie sicher, dass für beide Geräte dieselbe Zeitquelle verwendet wird.
Im zweiten Sichtbereich der Kamera wird der Radarstream nicht korrekt angezeigt.	Bei Edge-to-Edge-Kopplung beträgt die Standard-Auflösung des Radars sowohl in der Weboberfläche der Kamera als auch in einem VMS 1280 x 720. Wenn Sie eine andere Auflösung auswählen, wird der Videostream nicht korrekt angezeigt. Um die Auflösung des Radars einzustellen, wechseln Sie zu Video > Stream > General (Video > Stream > Allgemein) auf der Weboberfläche der Kamera und wählen Sie View area 2 (Sichtbereich 2) aus.

Probleme mit Overlays	
Die Overlays, die ich über die Weboberfläche der Kamera hinzugefügt habe, werden nach der Radarkopplung nicht mehr angezeigt.	Wenn Sie der Kamera mehr als einen Sichtbereich hinzugefügt haben, werden zuvor hinzugefügte Overlays nicht mehr auf der Weboberfläche der Kamera angezeigt. Da das Radar nach der Radarkopplung den zweiten Sichtbereich einnehmen wird, werden alle vorhandenen Overlays auf der Weboberfläche der Kamera nicht mehr angezeigt. Die Overlays werden nur von der Weboberfläche entfernt. Sie können weiterhin einen Videostream anfordern, der Overlays enthält, z. B. in einem VMS.
Die im AXIS License Plate Verifier hinzugefügten Fahrzeugkennzeichen-Overlays werden nicht angezeigt.	Wenn Sie Overlays hinzugefügt haben, die die Fahrzeuggeschwindigkeit in AXIS Speed Monitor anzeigen und dann im AXIS License Plate Verifier Fahrzeugkennzeichen-Overlays aktivieren, werden die Fahrzeugkennzeichen-Overlays nicht angezeigt. Zuerst die Overlays im AXIS License Plate Verifier aktivieren, bevor Sie Geschwindigkeits-Overlays über den AXIS Speed Monitor hinzufügen.

Leistungsaspekte

Achten Sie bei der Einrichtung Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die Leistung auswirken. Einige Faktoren beeinflussen die Bandbreite (Bitrate), andere die Bildrate und wieder andere beides.

Die wichtigsten Umstände, die Sie berücksichtigen müssen, sind die folgenden:

- 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/H.265/AV1 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 Video-Streams mit unterschiedlichen Codecs wirkt sich sowohl auf die Bildrate als auch auf die Bandbreite aus. Für eine optimale Leistung sollten Sie Video-Streams mit demselben Codec verwenden.

- 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.
- 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.

Support

Weitere Hilfe erhalten Sie hier: [*axis.com/support*](https://axis.com/support).

Cybersicherheit

Cybersicherheit trägt zu einem erfolgreichen Produktlebenszyklus bei, bei dem Risiken auf ein Minimum reduziert werden. Ausführliche Informationen und Dokumentationen zu unserem Ansatz im Bereich Cybersicherheit finden Sie unter axis.com/about-axis/cybersecurity. Befolgen Sie die nachstehenden Cybersicherheitsrichtlinien, um Produktsicherheitsbenachrichtigungen von Axis zu erhalten und Ihre Konfiguration für einen sicheren Lebenszyklus und eine sichere Außerbetriebnahme durchzuführen.

Unter *Axis Trust Center* finden Sie Informationen darüber, wie Axis die Einhaltung von Sicherheitsvorschriften, Transparenz, Datenschutz und den Schutz der Privatsphäre implementiert.

Schwachstellen-Management

Axis ist eine *Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)*. Um das Risiko einer Gefährdung für Sie so gering wie möglich zu halten, halten wir uns bei der Erkennung und Behebung von Sicherheitslücken in unseren Geräten, unserer Software und unseren Diensten an die Branchenstandards. Weitere Informationen zu unseren Richtlinien zur Verwaltung von Sicherheitslücken oder zur Meldung einer Schwachstelle finden Sie unter axis.com/vulnerability-management.

Sicherheitsbenachrichtigungen

Abonnieren Sie die Sicherheits-E-Mails von Axis unter axis.com/security-notification-service. Wir senden Ihnen Informationen zu Sicherheitslücken, entsprechenden Sicherheitshinweisen und anderen sicherheitsrelevanten Themen für Ihr Axis Produkt.

Sicherer Produktlebenszyklus

Axis minimiert Risiken über die gesamte Lebensdauer unserer Produkte hinweg durch eine sichere Verwaltung des Lebenszyklus. Nutzen Sie unsere Sicherheitsrichtlinien unter help.axis.com, um Ihre Axis Produkte sicherer zu konfigurieren und zum Betrieb zu nutzen und um Informationen zu folgenden Themen zu erhalten:

Sichere Erstnutzung – Axis Produkte sind standardmäßig mit einem hohen Sicherheitsniveau in der Konfiguration vorkonfiguriert, um von Anfang an eine sichere Inbetriebnahme und verschlüsselte Kommunikation zu gewährleisten.

Bestimmungsgemäßer Gebrauch und häufige Fehler bei der Konfiguration – Unsere Anleitungen enthalten Informationen zur bestimmungsgemäßen Verwendung von Axis Produkten, einschließlich häufiger sicherheitsrelevanter Fehlbedienungen und Fehler bei der Konfiguration, die vermieden werden sollten.

Sicherheitslücken und Transparenz in der Lieferkette verwalten – Mit jeder Softwareversion wird auf axis.com eine Software-Bestellliste (SBOM) veröffentlicht, um Sicherheitslücken offenzulegen und die Transparenz in der Lieferkette zu verbessern.

Stilllegung und die sichere Löschung von Daten – Um ein Produkt am Ende seines Lebenszyklus sicher außer Betrieb zu nehmen, setzen Sie es auf die Werkseinstellungen zurück. Dadurch werden Ihre Konfigurationen, gespeicherten Daten und vertraulichen Informationen gelöscht.

T10191705_de

2026-07 (M16.2)

© 2023 – 2026 Axis Communications AB