AXIS M1075-L Box Camera

Benutzerhandbuch

Inhalt

Funktionsweise 5
Die Kamera an ein drahtloses Netzwerk anschließen 5
Konfigurieren der Kamera über WLAN-Verbindung 5
Konfigurieren der Kamera über drahtgebundene Verbindung 5
Das Gerät im Netzwerk ermitteln 6
Unterstützte Browser 6
Weboberfläche des Geräts öffnen 6
Administratorkonto erstellen 6
Sichere Kennwörter 7
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat. 7
Übersicht über die Weboberfläche 7
Installation 8
Vorschaumodus 8
Ihr Gerät konfigurieren 9
Grundlegende Einstellungen 9
Bild einstellen 9
Szenen mit starkem Gegenlicht bearbeiten 9
Überwachen Sie lange und schmale Bereiche 10
Überprüfen der Pixelauflösung 10
Teile des Bildes mit Privatzonenmasken verbergen 10
Ein Bild-Overlay anzeigen 11
Einen Text-Overlay anzeigen 11
Video ansehen und aufnehmen 11
Bandbreite und Speicher reduzieren 11
Anzeige eines Live-Videostreams auf einem Monitor 12
Einrichtung eines Netzwerk-Speichers 12
Video aufzeichnen und ansehen 12
Stellen Sie sicher, dass keiner das Video manipuliert hat. 13
Einrichten von Regeln für Ereignisse 13
Lösen Sie eine Aktion aus 13
Video aufzeichnen, wenn die Kamera ein Objekt erfasst 13
PIR und Audio zum Abschrecken von Eindringlingen verwenden 14
Audio 14
..... 14
Videoaufzeichnungen mit Audio ergänzen 14
Weboberfläche 15
Status 15
Video 17
Installation 19
Bild 19
Videostream 27
Overlays 30
Anzeigebereiche 32
Privatzonenmasken 32
Analyse 33
AXIS Object Analytics 33
Metadaten-Visualisierung 33
Metadatenkonfiguration 33
Audio 33
Geräteinstellungen 33
Videostream 34
Audio-Clips 35
Audioverbesserung 35

Aufzeichnungen 35
Apps 37
System 37
Uhrzeit und Ort 37
WLAN 39
Netzwerk 39
Sicherheit 43
Konten 48
Ereignisse 50
MQTT 55
SIP 58
Speicherung 61
Videostromprofile 63
Über ONVIF 64
Melder 67
Video-Ausgang 67
Anzeigen 69
Zubehör 69
Protokolle 70
Direktkonfiguration 71
Wartung 72
Wartung 72
Fehler beheben 73
Mehr erfahren 74
Privatzonenmasken 74
Streaming und Speicher 74
Video-Komprimierungsformate 74
Bitrate-Steuerung 75
Anwendungen 76
AXIS Object Analytics 76
Metadaten-Visualisierung 76
Erweiterte WLAN-Einstellungen 77
WPA™ Personal 77
WPA™ Enterprise 77
EAP-TLS 77
EAP-PEAP/MSCHAPv2 77
Zertifikate für Drahtlosnetzwerke 78
Cybersicherheit 78
Signiertes Betriebssystem 78
Sicheres Hochfahren 78
Axis Edge Vault 78
TPM (Trusted Platform Module) 79
Axis Geräte-ID 79
Signiertes Video 79
Technische Daten 80
Produktübersicht 80
..... 80
LED-Anzeigen 80
Einschub für SD-Speicherkarte 80
Tasten 81
Steuertaste 81
WLAN-Setup-Taste 81
Anschlüsse 81
HDMI-Anschluss 81
Netzwerk-Anschluss 81
USB-Anschluss 81

E/A-Anschluss 81
Gerät reinigen 83
Fehlerbehebung 84
Zurücksetzen auf die Werkseinstellungen 84
Optionen für AXIS OS 84
Aktuelle AXIS OS-Version überprüfen 84
AXIS OS aktualisieren 85
Technische Fragen, Hinweise und Lösungen 85
Leistungsaspekte 87
Support 88

Funktionsweise

Die Kamera an ein drahtloses Netzwerk anschließen

Vorbereitungen:

- Erfahren Sie mehr über die Tasten und Anschlüsse der Kamera. Siehe .
- Schließen Sie den Drahtlosadapter an den USB-Anschluss der Kamera an.

Konfigurieren der Kamera über WLAN-Verbindung

1. Schließen Sie die Stromquelle an die Kamera an.
2. Wenn die Kamera gelb/rot blinkt, drücken Sie die WLAN-Setup-Taste, bis die Status-LED blau leuchtet. Die Kamera befindet sich jetzt im Access Point-Modus.
3. Verbinden Sie sich mit Ihrem Computer oder Mobilgerät mit dem Access Point der Kamera. Verwenden Sie die SSID und das Kennwort, die auf dem Etikett auf der Rückseite der Kamera aufgedruckt sind.
4. Um zur Seite mit den WLAN-Einstellungen zu kommen, öffnen Sie einen Browser und geben Sie die IP-Adresse 192.168.0.1 ein.

Hinweis

Um direkt zur Seite mit den WLAN-Einstellungen zu kommen, können Sie auch den Barcode neben der SSID und dem Kennwort auf dem Etikett scannen.

5. Rufen Sie das drahtlose Netzwerk auf, das Sie verwenden werden, klicken Sie auf ⋮ und konfigurieren Sie es gemäß Ihren Anforderungen.
6. **Save (Speichern)** anklicken. Der Zugriffspunkt der Kamera wird heruntergefahren und die Kamera wird mit dem konfigurierten Zugriffspunkt verbunden.

Wichtig

Aus Sicherheitsgründen müssen Sie auf Werkseinstellungen zurücksetzen, wenn Sie das Verfahren nach dem Verbinden mit dem WLAN wiederholen möchten.

Konfigurieren der Kamera über drahtgebundene Verbindung

1. Das Gerät mit dem Netzwerk-Kabel an das Netzwerk anschließen.
2. Auf der Webseite des Geräts anmelden. Siehe .
3. Wechseln Sie zu **System > WLAN**.

Wenn ein drahtloses Netzwerk in Betrieb ist:

1. Rufen Sie das drahtlose Netzwerk auf, das Sie verwenden werden, klicken Sie auf ⋮ und konfigurieren Sie es gemäß Ihren Anforderungen.
2. **Save (Speichern)** anklicken.
3. Das Netzwerk-Kabel von der Kamera trennen. Schließen Sie die Stromquelle an.

Wenn kein Drahtlosnetzwerk verfügbar ist:

1. Klicken Sie auf + **Add network (Netzwerk hinzufügen)**.
2. Wählen Sie in der Liste der Authentifizierungsmethoden **WPA™Personal aus**.

Hinweis

Informationen zur Konfiguration des Netzwerks mit einer anderen Sicherheitsmethode als WPA™Personal finden Sie unter .

3. Das SSID und das Kennwort für den Access Point eingeben.

4. **Save (Speichern)** anklicken.
5. Das Netzwerk-Kabel von der Kamera trennen. Schließen Sie die Stromquelle an.

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

*Nicht vollständig unterstützt. Verwenden Sie bei Problemen mit dem Videostreaming einen anderen Browser.

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.
   Bei unbekannter IP-Adresse AXIS IP Utility oder AXIS Device Manager verwenden, um das Gerät im Netzwerk zu ermitteln.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe .

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter .

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe .
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 .

Sichere Kennwörter

Wichtig

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

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

Grundlegende Einstellungen

Netzfrequenz einstellen

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

Orientierung einstellen

1. Gehen Sie auf **Video > Installation > Drehen**.
2. Wählen Sie **0**, **90**, **180** oder **270** Grad aus.
   Siehe auch .

Bild einstellen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts. Weitere Informationen zur Arbeitsweise bestimmter Funktionen finden Sie unter .

Szenen mit starkem Gegenlicht bearbeiten

Der Lichtstärkebereich eines Bildes wird als Dynamikbereich bezeichnet. Der Unterschied in der Lichtstärke des dunkelsten und des hellsten Bereichs kann stark ausgeprägt sein. Im Ergebnis sind dann lediglich die dunklen oder die hellen Bereiche sichtbar. Wide Dynamic Range (WDR) macht sowohl dunkle als auch helle Bereiche des Bildes sichtbar.

Bild ohne WDR

Bild mit WDR

Hinweis

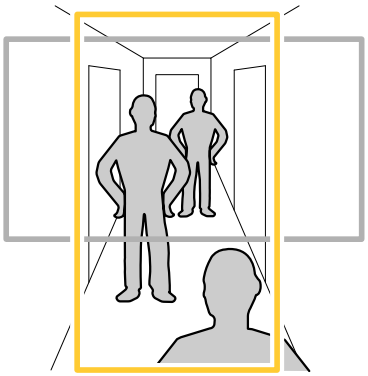
- WDR kann Artefakte im Bild verursachen.
- WDR steht möglicherweise nicht für jeden Aufnahmemodus zur Verfügung.

1. Gehen Sie auf **Video > Bild > Wide Dynamic Range**.
2. Aktivieren Sie WDR.
3. Wenn weiterhin Probleme auftreten, navigieren Sie zu **Exposure (Belichtung)** und passen Sie **Exposure zone (Belichtungsbereich)** an, um den ausgewählten Bereich abzudecken.

Mehr über WDR und seine Einsatzmöglichkeiten erfahren Sie auf *axis.com/web-articles/wdr*.

Überwachen Sie lange und schmale Bereiche

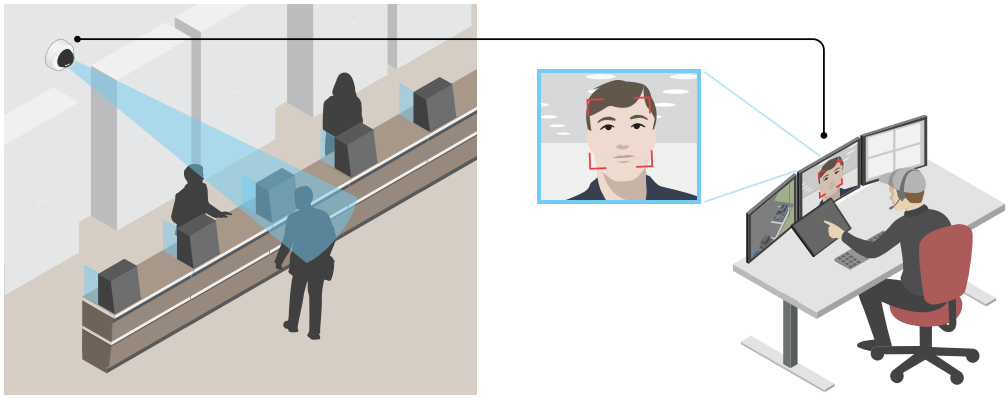
Verwenden Sie das Corridor Format und erfassen Sie somit das Sichtfeld von langen und schmalen Räumen wie Treppenhäusern, Korridoren, Straßen und Tunneln besser.



1. Drehen Sie je nach Gerät die Kamera oder das 3-Achsen-Objektiv in der Kamera um 90° oder 270°.
2. Wenn das Gerät nicht über eine automatische Drehung der Ansicht verfügt, gehen Sie zu **Video > Installation**.
3. Drehen Sie die Ansicht um 90° oder 270°.

Überprüfen der Pixelauflösung

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



1. Wechseln Sie zu **Video > Image (Video > Bild)** und klicken Sie auf .
2. Klicken Sie für **Pixel counter (Pixelzähler)** auf .
3. Passen Sie in der Live-Ansicht der Kamera Größe und Position des Rechtecks um den ausgewählten Bereich herum an, z. B. dort, wo die Gesichter von Passanten voraussichtlich erscheinen werden. Sie können die Pixelanzahl für jede Seite des Rechtecks sehen und entscheiden, ob die Werte für Ihre Anforderungen ausreichen.

Teile des Bildes mit Privatzonenmasken verbergen

Sie können eine oder mehrere Privatzonenmasken erstellen, um Teile des Bilds auszublenden.

1. Gehen Sie auf **Video > Privacy masks (Video > Privatzonenmasken)**.
2. Klicken Sie auf .

3. Klicken Sie auf die neue Maske und geben Sie einen Namen ein.
4. Passen Sie die Größe und Position Privatzonenmaske Ihren Wünschen entsprechend an.
5. Um die Farbe aller Privatzonenmasken zu ändern, klicken Sie auf **Privacy masks (Privatzonenmasken)** und wählen die gewünschte Farbe aus.

Siehe auch

Ein Bild-Overlay anzeigen

Sie können ein Bild als Overlay im Videostream hinzufügen.

1. Gehen Sie auf **Video > Overlays**.
2. Wählen Sie **Image (Bild)** und klicken Sie auf + .
3. **Images (Bilder)** anklicken.
4. Legen Sie ein Bild per Drag & Drop ab.
5. Klicken Sie auf **Upload (Hochladen)**.
6. Klicken Sie auf **Overlay verwalten**.
7. Wählen Sie das Bild und eine Position. Sie können das Overlay-Bild auch per Drag & Drop in der Live-Ansicht ziehen, um die Position zu ändern.

Einen Text-Overlay anzeigen

Sie können ein Textfeld als Overlay im Videostream hinzufügen. Dies ist nützlich, wenn Sie das Datum, die Uhrzeit oder den Firmennamen im Videostream anzeigen möchten.

1. Gehen Sie auf **Video > Overlays**.
2. Wählen Sie **Text** aus und klicken Sie auf + .
3. Geben Sie den Text ein, der im Videostream angezeigt werden soll.
4. Position auswählen. Sie können das Overlay-Textfeld auch per Drag & Drop in der Live-Ansicht ziehen, um die Position zu ändern.

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.

Anzeige eines Live-Videostreams auf einem Monitor

Ihre Kamera kann einen Live-Videostream sogar ohne Netzwerk-Verbindung an einen HDMI-Monitor übertragen. Der Monitor kann für Überwachungszwecke oder für die öffentliche Wiedergabe, z. B. in einem Ladengeschäft, eingesetzt werden.

1. Schließen Sie einen externen Monitor an den HDMI-Anschluss an.
2. Wechseln Sie **zu System > Video-Ausgang** und aktivieren Sie **HDMI**.
3. Eine **Quelle** wählen. Drehen Sie das Bild bei Bedarf.

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 > Bild**.
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
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. Verwenden Sie AXIS Camera Station (5.46 oder höher) oder eine andere kompatible Video Management Software, um ein Video aufzeichnen. Anweisungen dazu finden Sie im *Benutzerhandbuch von AXIS Camera Station*.
3. Das aufgezeichnete Video exportieren.
4. Geben Sie das Video mit dem AXIS File Player wieder. *AXIS File Player herunterladen.*

   zeigt an, dass keiner das Video manipuliert hat.

Hinweis

Um weitere Informationen über das Video zu erhalten, klicken Sie mit der rechten Maustaste auf das Video und wählen Sie **Digitale Signatur anzeigen** aus.

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 in unserer Anleitung *Erste Schritte mit Regeln für Ereignisse*.

Lösen Sie eine Aktion aus

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu. Die Regel legt fest, wann das Gerät bestimmte Aktionen durchführt. Regeln können als geplant, wiederkehrend oder manuell ausgelöst eingerichtet werden.
2. Unter **Name** einen Dateinamen eingeben.
3. Wählen Sie die **Bedingung**, die erfüllt sein muss, damit die Aktion ausgelöst wird. Wenn für die Regel mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.
4. Wählen Sie, welche **Aktion** das Gerät bei erfüllten Bedingungen durchführen soll.

Hinweis

Damit Änderungen an einer aktiven Aktionsregel wirksam werden, muss die Regel wieder eingeschaltet werden.

Video aufzeichnen, wenn die Kamera ein Objekt erfasst

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 Object Analytics ausgeführt wird:

1. Gehen Sie auf **Apps > AXIS Object Analytics**.
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 unter **Anwendung** aus der Liste der Bedingungen **Object Analytics**.
4. Wählen Sie aus der Liste der Aktionen unter **Aufzeichnungen**Video 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.

PIR und Audio zum Abschrecken von Eindringlingen verwenden

In diesem Beispiel wird erläutert, wie die Kamera so eingerichtet wird, dass ein Audioclip mit Hundegebell wiedergegeben wird, wenn der PIR-Sensor Bewegungen außerhalb der Geschäftszeiten erkennt.

Vorbereitungen:

- Fügen Sie dem Gerät einen Audio-Clip mit einem bellenden Hund hinzu. Weitere Informationen finden Sie unter .

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 den **Gerätestatus > PIR-Sensor** aus.
4. Klicken Sie auf **+**, um eine zweite Bedingung hinzuzufügen.
5. Wählen Sie aus der Liste der Bedingungen **Geplant und wiederkehrend > Zeitplan**.
6. Wählen Sie aus der Liste der Zeitpläne **After hours (Nach Geschäftsschluss)** aus.
7. Wählen Sie in der Liste der Aktionen **Audioclips > Wiedergabe von Audioclips** aus.
8. Wählen Sie in der Liste der Audioclips **Dog barking (Hundegebell)** aus.
9. Klicken Sie auf **Save**.

Audio

Dieses Gerät verfügt über eine automatische Sprachverbesserung.

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.
4. Wenn Sie Änderungen an der Eingangsquelle vornehmen, klicken Sie auf **Änderungen übernehmen**.

Das zum Aufzeichnen verwendete Videostreamprofil bearbeiten:

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

Weboberfläche

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

Hinweis

Die in diesem Abschnitt beschriebenen Funktionen und Einstellungen werden von Gerät zu Gerät unterschiedlich unterstützt. Dieses Symbol zeigt an, dass die Funktion oder Einstellung nur für einige Geräte verfügbar ist.

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Ändern Sie die Sprache.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

- Informationen zum angemeldeten Benutzer.
- **Konto wechseln**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
- **Abmelden**: Melden Sie sich vom aktuellen Konto ab.

Das Kontextmenü enthält:

- **Analysedaten**: Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.
- **Feedback**: Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.
- **Legal (Rechtliches)**: Informationen zu Cookies und Lizenzen anzeigen.
- **About (Info)**: Lassen Sie sich Geräteinformationen, einschließlich AXIS OS-Version und Seriennummer anzeigen.

Status

Sicherheit

Zeigt an, welche Art von Zugriff auf das Gerät aktiv ist, welche Verschlüsselungsprotokolle verwendet werden und unsignierte Apps zulässig sind. Empfehlungen zu den Einstellungen finden Sie im AXIS OS Härtungsleitfaden.

Härtungsleitfaden: Hier gelangen Sie zum *AXIS OS Härtungsleitfaden*, in dem Sie mehr über Best Practices für die Cybersicherheit auf Axis Geräten erfahren.

Zeitsynchronisierungsstatus

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

NTP-Einstellungen: Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Time and location (Uhrzeit und Standort)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Laufende Aufzeichnungen

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter

Anzeige des Speicherorts der Aufzeichnung.

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich AXIS OS-Version und Seriennummer.

Upgrade AXIS OS (AXIS OS aktualisieren): Aktualisieren Sie die Software auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie die Aktualisierung durchführen können.

Verbundene Clients

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

Details anzeigen: Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port, Zustand und PID/Process für jede Verbindung an.

Video

Klicken Sie darauf, um den Live-Videostream wiederzugeben.

Klicken Sie darauf, um den Live-Videostream einzufrieren.

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

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

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

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

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

- **Voreingestellte Steuerelemente**: Aktivieren Sie diese Option, um die auf dem Bildschirm verfügbaren Steuerelemente zu verwenden.
- **Benutzerdefinierte Steuerelemente**: Klicken Sie auf **Add custom control (Benutzerdefinierte Steuerelemente hinzufügen)**, um dem Bildschirm Steuerelemente hinzuzufügen.

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

Startet den Wischer.

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

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

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

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

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

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

Klicken Sie darauf, um auf weitere Einstellungen zuzugreifen:

- **Videoformat**: Wählen Sie das Codierungsformat aus, das in der Live-Ansicht verwendet werden soll.
- **Autoplay**: Aktivieren Sie diese Option, um einen stummgeschalteten Videostream automatisch wieder wiederzugeben, wenn Sie das Gerät in einer neuen Sitzung öffnen.
- **Informationen zum Clientstream**: Aktivieren Sie diese Option, um dynamische Informationen zum Videostream zu sehen, der vom Browser, der den Live-Videostream zeigt, verwendet wird. Die Bitrate-Informationen unterscheiden sich aufgrund unterschiedlicher Informationsquellen von den in einem Text-Overlay angezeigten Informationen. Die Bitrate in den Informationen zum Clientstream ist die Bitrate der letzten Sekunde und stammt vom Codierungstreiber des Geräts. Die Bitrate im Overlay ist die durchschnittliche Bitrate der letzten 5 Sekunden und stammt vom Browser. Beide Werte decken nur den Rohvideostream ab und nicht die zusätzliche Bandbreite, die bei der Übertragung über das Netzwerk via UDP/TCP/HTTP erzeugt wird.
- **Adaptiver Videostream**: Aktivieren Sie diese Option, um die Bildauflösung zur Erhöhung der Benutzerfreundlichkeit an die tatsächliche Bildschirmauflösung des Clients anzupassen und eine mögliche Überlastung der Client-Hardware zu vermeiden. Der adaptive Videostream wird nur eingesetzt, wenn die Wiedergabe des Live-Videostreams über die Weboberfläche in einem Browser erfolgt. Wenn adaptiver Videostream aktiviert ist, beträgt die maximale Bildrate 30 Bilder pro Sekunde. Wenn Sie bei aktiviertem adaptivem Stream eine Momentaufnahme erstellen, wird die vom adaptiven Videostream ausgewählte Bildauflösung verwendet.
- **Nivellierraster**: Klicken Sie auf , um das Nivellierraster anzuzeigen. Mithilfe des Rasters können Sie entscheiden, ob das Bild horizontal ausgerichtet ist. Klicken Sie auf , um es auszublenden.
- **Pixel counter (Pixelzähler)**: Klicken Sie auf , um den Pixelzähler anzuzeigen. Ziehen und ändern Sie die Größe des Felds, um den ausgewählten Bereich einzuschließen. Die Größe des Felds in Pixeln lässt sich auch über die Felder **Width (Breite)** und **Height (Höhe)** definieren.
- **Aktualisieren**: Klicken Sie auf , um das Standbild der Live-Ansicht zu aktualisieren.
- **PTZ-Steuerelemente** : Aktivieren Sie diese Ansicht, um die PTZ-Steuerelemente in der Live-Ansicht anzuzeigen.

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

Klicken Sie darauf, um sich den Live-Videostream im Vollbildmodus anzeigen zu lassen. Zum Beenden des Vollbildmodus ESC drücken.

Installation

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

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

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

Rotate (Drehen): Wählen Sie die bevorzugte Bildausrichtung aus.

Bild

Darstellung

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

- **Forensic (Forensisch):** Zu Überwachungszwecken geeignet.
- **Indoor (Innenbereich)** : Für den Innenbereich geeignet.
- **Outdoor (Außenbereich)** : Für den Außenbereich geeignet.
- **Vivid (Anschaulich)** : Zu Demonstrationszwecken nützlich.
- **Traffic overview (Verkehrsübersicht)** : Für die Überwachung des Fahrzeugverkehrs geeignet.
- **License plate (Fahrzeugkennzeichen):** Geeignet zum Aufzeichnen von Fahrzeugkennzeichen.

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

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

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

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

Wide Dynamic Range

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

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

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

Weißabgleich

Wenn die Kamera die Farbtemperatur der Lichtquelle erfasst, kann sie das Bild anpassen, um natürlichere Farben zu erreichen. Sollte dies nicht ausreichen, können Sie eine geeignete Lichtquelle aus der Liste wählen.

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

Lichtverhältnisse:

- **Automatisch**: Automatisches Identifizieren und Ausgleichen der Lichtfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen verwendet werden kann.
- **Automatic – outdoors (Automatisch – Außenbereich)** : Automatisches Identifizieren und Ausgleichen der Lichtfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen im Außenbereich verwendet werden kann.
- **Custom – indoors (Benutzerdefiniert – Innenbereich)** : Fester Farbausgleich für Innenräume mit einem gewissen Anteil an nicht fluoreszierendem Kunstlicht und ausgerichtet auf eine normale Farbtemperatur von etwa 2800 K.
- **Custom – outdoors (Benutzerdefiniert – Außenbereich)** : Fester Farbausgleich für sonniges Wetter und eine Farbtemperatur von etwa 5500 K.
- **Fest – Fluoreszierend 1**: Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 4000 K.
- **Fest – Fluoreszierend 2**: Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 3000 K.
- **Fest – Innenbereich**: Fester Farbausgleich für Innenräume mit einem gewissen Anteil an nicht fluoreszierendem Kunstlicht und ausgerichtet auf eine normale Farbtemperatur von etwa 2800 K.
- **Fest – Außenbereich 1**: Fester Farbausgleich für sonniges Wetter und eine Farbtemperatur von etwa 5500 K.
- **Fest – Außenbereich 2**: Fester Farbausgleichswert für bewölktes Wetter und eine Farbtemperatur von etwa 6500 K.
- **Street light – mercury (Straßenbeleuchtung – Quecksilber)** : Fester Farbausgleichswert zur Kompensation des ultravioletten Anteil von häufig als Straßenbeleuchtung eingesetzten Quecksilberdampfleuchten.
- **Street light – sodium (Straßenbeleuchtung – Natriumdampf)** : Fester Farbausgleichswert, der das gelbe bis orangefarbene Licht von häufig als Straßenbeleuchtung eingesetzten Natriumdampfleuchten korrigiert.
- **Aktuelle Einstellung beibehalten**: Die aktuelle Einstellung beibehalten und keinen Lichtausgleich vornehmen.
- **Manual (Manuell)** : Legen Sie den Weißabgleich mit Hilfe eines weißen Objekts fest. Dazu ein Objekt, das von der Kamera als weiß interpretiert werden soll (zum Beispiel ein weißes Blatt Papier) in die Mitte des Live-Bildes legen. Stellen Sie mit den Schiebereglern für **Rotabgleich** und **Blauabgleich** den Weißabgleich manuell ein.

Tag-/Nachtmodus

IR-Sperrfilter:

- **Auto**: Wählen Sie diese Option aus, damit sich der Infrarot-Filter automatisch ein- und ausschaltet. Wenn sich die Kamera im Tag-Modus befindet, wird der Infrarot-Sperrfilter eingeschaltet, der die eingehende IR-Beleuchtung blockiert. Im Nachtmodus wird der Infrarot-Sperrfilter ausgeschaltet und die Lichtempfindlichkeit der Kamera wird erhöht.

Hinweis

- Einige Geräte verfügen im Nacht-Modus über IR-Durchlassfilter. Der IR-Durchlassfilter erhöht die Empfindlichkeit gegenüber Infrarotlicht, wohingegen sichtbares Licht blockiert wird.
- **On (Ein)**: Wählen Sie diese Option, um den Infrarot-Sperrfilter zu aktivieren. Das Bild ist in Farbe, aber mit verringerter Lichtempfindlichkeit.
- **Aus**: Wählen Sie diese Option, um den Infrarot-Sperrfilter zu deaktivieren. Das Bild wird schwarzweiß dargestellt und die Lichtempfindlichkeit erhöht.

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

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

Infrarot-Licht

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

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

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

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

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

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

Weißlicht

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

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

Belichtung

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

Belichtungsmodus:

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

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

Hinweis

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

- **Automatisch**: Für die meisten Situationen geeignet.
- **Mitte**: Damit wird anhand eines einen fest definierten Bereichs in der Bildmitte die Belichtung berechnet. Dieser Bereich hat in der Live-Ansicht eine feste Größe und Position.
- **Full (Voll)** : Damit wird anhand der kompletten Live-Ansicht die Belichtung berechnet.
- **Upper (Oben)** : Damit wird anhand eines festgelegten Bereichs im oberen Teil des Bildes die Belichtung berechnet.
- **Lower (Unten)** : Damit wird anhand eines festgelegten Bereichs im unteren Teil des Bildes die Belichtung berechnet.

- **Left (Links)** : Damit wird anhand eines festgelegten Bereichs im linken Teil des Bildes die Belichtung berechnet.
- **Right (Rechts)** : Damit wird anhand eines festgelegten Bereichs im rechten Teil des Bildes die Belichtung berechnet.
- **Genau**: Damit wird anhand eines Bereichs mit festgelegter Größe und Position die Belichtung berechnet.
- **Benutzerdefiniert**: Damit wird anhand eines Ausschnitts der Live-Ansicht die Belichtung berechnet. Sie können Größe und Position des Bereichs anpassen.

Maximale Verschlusszeit: Wählen Sie die Verschlusszeit für beste Bildqualität. Zu lange Verschlusszeiten (längere Belichtung) können Bewegungsunschärfe erzeugen, wobei zu kurze Verschlusszeiten die Bildqualität beeinträchtigen können. „Max. Verschluss" verbessert das Bild mithilfe der maximalen Verstärkung.

Maximierte Verstärkung: Wählen Sie die passende maximale Verstärkung aus. Wenn Sie die maximale Verstärkung erhöhen, wird die Detailschärfe dunkler Bilder verbessert, jedoch auch den Rauschpegel erhöht. Mehr Rauschen kann auch mehr Bedarf an Bandbreite und Speicherplatz bewirken. Wenn Sie die maximale Verstärkung auf einen hohen Wert festgelegen, kann die Bildqualität bei verschiedenen Lichtverhältnissen (Tag/Nacht) sehr unterschiedlich ausfallen. Max. Verstärkung verbessert das Bild mithilfe der maximalen Verschlusszeit.

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

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

Hinweis

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

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

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

Belichtungsgrad: Stellen Sie mithilfe des Schiebereglers die Bildbelichtung ein.

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

Hinweis

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

Filter

Der Privatsphärefilter erzeugt eine schwarzweiße Ansicht, die gezeichnet aussieht und auf den Schutz der Privatsphäre von Personen und Ereignisse zielt.

Pencil (Bleistift): Erstellt eine Ansicht mit dem Bleistift-Privatsphärefilter.

Threshold (Grenzwert) : Mit dem Schieberegler oder Textfeld den Grenzwert für die Helligkeit pro Pixel festlegen. Einige Details unterhalb des Grenzwerts werden entfernt und hängen von den Lichtverhältnissen der Szene ab.

Kernel size (Größe des Kernels) : Verwenden Sie den Schieberegler oder das Textfeld, um die Größe des Kernels für die Ansicht zu ändern. Größere Kernels betonen größere Kanten und kleinere Kernels kleinere Kanten.

Videostream

Allgemeines

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

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

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

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

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

Zipstream

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

Strength (Stärke) der Bitrate-Verringerung wählen:

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

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

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

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

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

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

Bitrate-Steuerung

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

Ausrichtung

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

Audio

Include (Integrieren): Aktivieren Sie diese Option, um Audio im Videostream zu verwenden.

Source (Quelle) : Wählen die zu verwendende Audioquelle.

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

Overlays

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

- **Text**: Wählen Sie diese Option, um einen Text anzeigen zu lassen, der in das Live-Ansichtsbild integriert und in allen Ansichten, Aufzeichnungen und Schnappschüssen sichtbar ist. Sie können einen eigenen Text eingeben und Sie können auch vorkonfigurierte Modifikatoren verwenden, um z. B. Uhrzeit, Datum und Bildrate automatisch anzeigen zu lassen.
  - : Anklicken, um den Datumsmodifikator `%F` hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
  - : Anklicken, um den Uhrzeitmodifikator `%X` hinzuzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
  - **Modifikatoren**: Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel `%a` den Wochentag an.
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  - **Appearance (Darstellung)**: Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
- **Bild**: Wählen Sie diese Option, um ein statisches Bild über dem Videostream zu zeigen. Sie können .bmp-, .png-, .jpeg- oder .s jpeg-Dateien verwenden.
  Um ein Bild hochzuladen, klicken Sie auf **Bilder**. Bevor Sie ein Bild hochladen, können Sie folgende Optionen festlegen:
  - **An Auflösung anpassen**: Wählen Sie diese Option, um das Overlay-Bild automatisch an die Videoauflösung anzupassen.
  - **Transparenz verwenden**: Wählen Sie den Hexadezimal-RGB-Wert für diese Farbe und geben Sie diesen ein. Verwenden Sie das Format RRGGBB. Beispiele für Hexadezimalwerte: FFFFFF für Weiß, 000000 für Schwarz, FF0000 für Rot, 6633FF für Blau und 669900 für Grün. Nur bei .bmp-Bildern.
- **Scene annotation (Szenen-Kennzeichnung)** : Wählen Sie diese Option aus, um im Videostream ein Text-Overlay anzuzeigen, das an derselben Position bleibt, auch wenn die Kamera in eine andere Richtung schwenkt oder neigt. Sie können festlegen, dass das Overlay nur innerhalb bestimmter Zoomstufen angezeigt wird.
  - : Anklicken, um den Datumsmodifikator `%F` hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
  - : Anklicken, um den Uhrzeitmodifikator `%X` hinzuzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
  - **Modifikatoren**: Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel `%a` den Wochentag an.
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  - **Appearance (Darstellung)**: Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).

- : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben. Das Overlay wird gespeichert und verbleibt in den Schwenk- und Neigekoordinaten dieser Position.
- **Annotation between zoom levels (%) (Kennzeichnung zwischen diesen Zoomstufen (%))**: Legen Sie die Zoomstufen fest, innerhalb derer das Overlay angezeigt wird.
- **Annotation symbol (Kennzeichnungssymbol)**: Wählen Sie ein Symbol aus, das anstelle des Overlays angezeigt wird, wenn sich die Kamera nicht innerhalb der eingestellten Zoomstufen befindet.

- **Streaming indicator (Streaming-Anzeige)** : Wählen Sie diese Option, um eine Animation über dem Videostream zu einzublenden. Die Animation zeigt an, dass der Videostream live ist, selbst wenn die Szene aktuell bewegungsfrei ist.
  - **Appearance (Darstellung)**: Wählen Sie die Farbe der Animation und des Hintergrunds, zum Beispiel rote Animation auf durchsichtigem Hintergrund (Standardeinstellung).
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
- **Widget: Linegraph (Liniendiagramm)** : Zeigt ein Diagramm an, das verdeutlicht, wie sich ein Messwert im Laufe der Zeit ändert.
  - **Title (Titel)**: Einen Titel für das Widget eingeben.
  - **Overlay modifier (Overlay-Modifikator)**: Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
  - **Size (Größe)**: Die Größe des Overlays auswählen.
  - **Auf allen Kanälen sichtbar**: Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
  - **Aktualisierungsintervall**: Wählen Sie die Zeit zwischen Datenaktualisierungen.
  - **Transparency (Transparenz)**: Legen Sie die Transparenz des gesamten Overlays fest.
  - **Hintergrundtransparenz**: Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
  - **Punkte**: Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
  - **X-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die x-Achse ein.
    - **Zeitfenster**: Geben Sie ein, wie lange die Daten visualisiert werden sollen.
    - **Zeiteinheit**: Geben Sie eine Zeiteinheit für die x-Achse ein.
  - **Y-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die y-Achse ein.
    - **Dynamische Skala**: Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
    - **Min. Alarmschwelle** und **Max. Alarmschwelle**: Diese Werte fügen dem Diagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.

- **Widget: Meter (Zähler)** : Zeigen Sie ein Balkendiagramm an, das den zuletzt gemessenen Datenwert anzeigt.
  - **Title (Titel)**: Einen Titel für das Widget eingeben.
  - **Overlay modifier (Overlay-Modifikator)**: Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
  - **Size (Größe)**: Die Größe des Overlays auswählen.
  - **Auf allen Kanälen sichtbar**: Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
  - **Aktualisierungsintervall**: Wählen Sie die Zeit zwischen Datenaktualisierungen.
  - **Transparency (Transparenz)**: Legen Sie die Transparenz des gesamten Overlays fest.
  - **Hintergrundtransparenz**: Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
  - **Punkte**: Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
  - **Y-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die y-Achse ein.
    - **Dynamische Skala**: Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
    - **Min. Alarmschwelle** und **Max. Alarmschwelle**: Diese Werte fügen dem Balkendiagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.

Anzeigebereiche

: Klicken Sie darauf, um einen Sichtbereich zu erstellen.

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

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

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

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

Privatzonenmasken

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

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

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

Analyse

AXIS Object Analytics

Start: Klicken Sie hier, um AXIS Object Analytics zu starten. Die Anwendung wird im Hintergrund ausgeführt und Sie können anhand der aktuellen Einstellungen der Anwendung Regeln für Ereignisse erstellen.

Offen: Klicken Sie hier, um AXIS Object Analytics zu öffnen. Die Anwendung wird in einer neuen Registerkarte geöffnet, in der Sie die Einstellungen konfigurieren können.

- **Not installed (Nicht installiert)**: AXIS Object Analytics ist auf diesem Gerät nicht installiert. Aktualisieren Sie AXIS OS auf die neueste Version, um die aktuelle Version der Anwendung zu erhalten.

Metadaten-Visualisierung

Die Kamera erkennt sich bewegende Objekte und klassifiziert sie nach Objekttyp. In der Ansicht verfügt ein klassifiziertes Objekt über ein farbiges Umgrenzungsfeld sowie eine zugewiesene ID.

Id: Eine eindeutige Identifizierungsnummer für das identifizierte Objekt und seinen Typ. Diese Zahl wird sowohl in der Liste als auch in der Ansicht angezeigt.

Typ: Ein sich bewegendes Objekt wird als Person, Gesicht, Pkw, Bus, Lkw, Fahrrad oder Fahrzeugkennzeichen klassifiziert. Die Farbe des Umgrenzungsfeldes hängt von der Typklassifizierung ab.

Confidence (Zuverlässigkeit): Der Balken gibt die Zuverlässigkeitsstufe der Klassifizierung des Objekttyps an.

Metadatenkonfiguration

Hersteller von RTSP-Metadaten

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

Hinweis

Diese Einstellungen gelten für den RTSP-Metadaten-Stream, der ONVIF XML verwendet. Die hier vorgenommenen Änderungen wirken sich nicht auf die Visualisierungsseite der Metadaten aus.

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

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

Audio

Geräteinstellungen

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

Stream-Extraktion erlauben : Aktivieren Sie diese Option, um eine Videostream-Extraktion zuzulassen.

Eingangstyp : Wählen Sie die Art des Eingangs aus, z. B. interner Mikrofon- oder Line-Eingang.

Spannung : Wählen Sie die Art der Stromversorgung für den Eingang aus.

Änderungen übernehmen : Wenden Sie Ihre Auswahl an.

Echounterdrückung : Aktivieren Sie diese Option, um Echos während der Zwei-Wege-Kommunikation zu entfernen.

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

Automatische Verstärkungsregelung : Aktivieren Sie dieses Option, damit die Verstärkung dynamisch an Klangänderungen angepasst wird.

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

Ausgang: Zeigt die Ausgangsart an.

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

Automatische Lautstärkeregelung : Aktivieren Sie diese Option, damit das Gerät die Verstärkung automatisch und dynamisch an den Umgebungsgeräuschpegel anpasst. Die automatische Lautstärkeregelung betrifft alle Audio-Ausgänge, einschließlich Line und Telefonspule.

Videostream

Codierung: Wählen Sie die Codierung für das Streaming der Eingangsquelle aus. Sie können die Codierung nur wählen, wenn der Audioeingang aktiviert ist. Klicken Sie auf **Enable audio input (Audioeingang aktivieren)**, falls der Audioeingang deaktiviert ist.

Audio-Clips

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

Audio-Clip abspielen.

Audio-Clip anhalten.

Das Kontextmenü enthält:

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

Audioverbesserung

Eingang

Ten Band Graphic Audio Equalizer (Grafischer Zehnband-Audio-Equalizer): Aktivieren Sie diese Einstellung, um innerhalb eines Audiosignals den Pegel der verschiedenen Frequenzbänder einzustellen. Diese Funktion ist für fortgeschrittene Benutzer mit Erfahrung in der Audiokonfiguration.

Talkback range (Talkbackbereich) : Wählen Sie den Betriebsbereich zum Erfassen von Audioinhalten. Eine Erhöhung des Betriebsbereichs reduziert die simultane 2-Wege-Kommunikationsfähigkeit.

Voice enhancement (Sprachverbesserung) : Aktivieren Sie diese Einstellung, um die Sprachinhalte im Verhältnis zu anderen Sounds zu verbessern.

Aufzeichnungen

Klicken Sie darauf, um die Aufzeichnungen zu filtern.

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

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

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

Ereignis: Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Speicher: Zeigt Aufzeichnungen nach Speichertyp.

Ongoing recordings (Laufende Aufzeichnungen): Anzeige aller laufenden Aufzeichnungen des Geräts.

● Starten einer Aufzeichnung des Geräts.

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

● Beenden einer Aufzeichnung des Geräts.

Ausgelöste Aufzeichnungen können entweder manuell gestoppt oder durch Ausschalten des Geräts beendet werden.

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

Die Aufzeichnung wiedergeben.

Abspielen der Aufzeichnung anhalten.

Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

Exportbereich festlegen: Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten. Beachten Sie, dass die Zeitspanne auf der Zeitzone des Geräts basiert, wenn Sie in einer anderen Zeitzone als der am Standort des Geräts arbeiten.

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

Klicken Sie auf , um eine Aufzeichnung zu löschen.

Exportieren: Exportieren der ganzen Aufzeichnung oder eines Teils davon.

Apps

App hinzufügen: Installieren einer neuen App.

Weitere Apps finden: Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet.

Nicht signierte Apps zulassen : Aktivieren Sie diese Option, um die Installation unsignierter Apps zu ermöglichen.

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

Hinweis

Die Leistung des Geräts kann beeinträchtigt werden, wenn mehrere Apps gleichzeitig ausgeführt werden.

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

Offen: Auf die Anwendungseinstellungen zugreifen. Die zur Verfügung stehenden Einstellungen hängen von der Anwendung ab. Für einige Anwendungen gibt es keine Einstellungen.

Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

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

System

Uhrzeit und Ort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server))**: Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP))**: Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server)**: Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server))**: Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Custom date and time (Datum und Uhrzeit benutzerdefiniert)**: Manuelles Einstellen von Datum und Uhrzeit. Klicken Sie auf **Vom System abrufen**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

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

- **DHCP**: Übernimmt die Zeitzone des DHCP-Servers. Bevor Sie diese Option auswählen können, muss das Gerät mit einem DHCP-Server verbunden werden.
- **Manual (Manuell)**: Wählen Sie in der Drop-Down-Liste eine Zeitzone aus.

Hinweis

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

Gerätestandort

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

- **Formatieren**: Wählen Sie das Format für die Eingabe des Breiten- und Längengrads Ihres Geräts.
- **Breite**: Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Länge**: Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Ausrichtung**: Die Kompassrichtung des Geräts eingeben. Der Wert 0 steht für: genau nach Norden.
- **Bezeichnung**: Eine aussagekräftige Bezeichnung für Ihr Gerät eingeben.
- **Speichern**: Klicken Sie hier, um den Gerätestandort zu speichern.

WLAN

Über einen drahtlosen USB-Adapter kann das Gerät eine Verbindung mit einem Drahtlosnetzwerk herstellen.

Country (Land): Um die Fähigkeiten des Treibers bei der Suche nach Netzwerkzugriffspunkten zu verbessern, das Land wählen, in dem sich das Gerät befindet.

Add network (Netzwerk hinzufügen): Drahtlosnetzwerk hinzufügen, das nicht die SSID (Name) überträgt. Den SSID und alle nötigen Einstellungen für das Netzwerk eingeben. Wenden Sie sich zur an Ihren Netzwerkadministrator, um die nötigen Einstellungen zu erhalten.

Refresh (Aktualisieren): Liste der verfügbaren Drahtlosnetzwerke aktualisieren.

Das Kontextmenü enthält:

- **Info**: Signalstärke, Kanal und Sicherheitstyp des Netzwerks anzeigen.
- **Konfigurieren**: Netzwerkeinstellungen ändern.

Netzwerk

IPv4

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

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

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

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

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

Hinweis

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

IPv6

Assign IPv6 automatically (IPv6 automatisch zuweisen): Wählen Sie diese Option aus, um IPv6 einzuschalten und damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann.

Hostname

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

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

Dynamische DNS-Aktualisierung aktivieren: Erlauben Sie Ihrem Gerät, seine Domainnamen-Server-Einträge automatisch zu aktualisieren, wenn sich seine IP-Adresse ändert.

DNS-Namen registrieren: Geben Sie einen eindeutigen Domainnamen ein, der auf die IP-Adresse Ihres Geräts verweist. Zugelassene Zeichen sind A–Z, a–z, 0–9 und -).

TTL: Time to Live (TTL) legt fest, wie lange ein DNS-Eintrag gültig bleibt, bevor er aktualisiert werden muss.

DNS-Server

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

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

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

HTTP und HTTPS

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

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Um Zertifikate zu erstellen und zu installieren, **System > Security (System > Sicherheit)** aufrufen.

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

Hinweis

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

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

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

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

Netzwerk-Erkennungsprotokolle

Bonjour®: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

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

UPnP®: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

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

WS-Erkennung: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

LLDP und CDP: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung. Das Deaktivieren von LLDP und CDP kann sich auf das PoE-Leistungsmanagement auswirken. Konfigurieren Sie den PoE-Switch nur für das Hardware-PoE-Leistungsmanagement, um Probleme mit dem PoE-Leistungsmanagement zu beheben.

Globale Proxys

HTTP proxy (HTTP-Proxy): Geben Sie einen globalen Proxy-Host oder eine IP-Adresse in einem unterstützten Format an.

HTTPS proxy (HTTPS-Proxy): Geben Sie einen globalen Proxy-Host oder eine IP-Adresse in einem unterstützten Format an.

Unterstützte HTTP- und HTTPS-Proxy-Formate:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

Hinweis

Starten Sie das Gerät neu, um die Einstellungen für den globalen Proxy anzuwenden.

No proxy (Kein Proxy): Verwenden Sie die Option **No proxy (Kein Proxy)**, um globale Proxys zu umgehen. Geben Sie eine Option oder mehrere durch Kommas getrennte Optionen aus der Liste ein:

- Leer lassen
- IP-Adresse angeben
- IP-Adresse im CIDR-Format angeben
- Geben Sie einen Domainnamen an, zum Beispiel: www.<Domainname>.com
- Geben Sie alle Subdomains einer bestimmten Domain an, z. B. .<Domainname>.com

One-Click Cloud Connect

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

O3C zulassen:

- **One-click**: Dies ist die Standardoption. Um eine Verbindung zum O3C herzustellen, drücken Sie die Steuertaste am Gerät. Je nach Gerätetyp entweder drücken und loslassen oder drücken und halten, bis die Status LED blinkt. Registrieren Sie das Gerät innerhalb von 24 Stunden beim O3C-Service, um **Always (Immer)** zu aktivieren, und bleiben Sie verbunden. Wenn Sie sich nicht registrieren, wird die Verbindung zwischen dem Gerät und O3C unterbrochen.
- **Immer**: Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sobald Sie das Gerät registriert haben, bleibt es verbunden. Verwenden Sie diese Option, wenn die Steuertaste außer Reichweite ist.
- **No (Nein)**: Trennt den O3C-Dienst.

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

Host: Geben Sie die Adresse des SIP-Proxyservers ein.

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

Anmeldung und **Kennwort**: Bei Bedarf einen Benutzernamen und ein Kennwort für den Proxyserver eingeben.

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

- **v3**: SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden. Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Kennwort für das Konto "initial"**: Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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

Zertifikat hinzufügen: Klicken, um ein Zertifikat hinzuzufügen. Es wird eine Schritt-für-Schritt-Anleitung geöffnet.

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

Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) :

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

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec ist ein IEEE-Standard für MAC-Sicherheit (Media Access Control), der die Vertraulichkeit und Integrität verbindungsloser Daten für medienzugriffsunabhängige Protokolle definiert.

Zertifikate

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

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

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

Authentication method (Authentifizierungsmethode): Wählen Sie einen EAP-Typ aus, der für die Authentifizierung verwendet wird.

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

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

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

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

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

Diese Einstellungen stehen nur zur Verfügung, wenn Sie **IEEE 802.1x PEAP-MSCHAPv2** als Authentifizierungsmethode verwenden:

- **Password (Kennwort)**: Geben Sie das Password (Kennwort) für die Benutzeridentität ein.
- **Peap version (Peap-Version)**: Wählen Sie die in dem Netzwerk-Switch verwendete Peap-Version aus.
- **Bezeichnung**: Wählen Sie 1 aus, um die EAP-Verschlüsselung des Client zu verwenden. Wählen Sie 2 aus, um die PEAP-Verschlüsselung des Client zu verwenden. Wählen Sie die Bezeichnung aus, das der Netzwerk-Switch bei Verwendung von Peap-Version 1 verwendet.

Diese Einstellungen stehen nur zur Verfügung, wenn Sie **IEEE 802.1ae MACsec (Static CAK/Pre-Shared Key)** als Authentifizierungsmethode verwenden:

- **Key agreement connectivity association key name (Schlüsselname der Key Agreement Connectivity Association)**: Geben Sie den Namen der Connectivity Association (CKN) ein. Der Name muss aus 2 bis 64 (durch 2 teilbare) Hexadezimalzeichen bestehen. Der CKN muss manuell in der Connectivity Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.
- **Key agreement connectivity association key (Schlüssel der Key Agreement Connectivity Association)**: Geben Sie den Schlüssel der Connectivity Association (CAK) ein. Der Schlüssellänge sollte entweder 32 oder 64 Hexadezimalzeichen betragen. Der CAK muss manuell in der Connectivity

Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.

Brute-Force-Angriffe verhindern

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

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

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

Firewall

Activate (Aktivieren): Schalten Sie die Firewall ein.

Default Policy (Standardrichtlinie): Wählen Sie den Standardstatus für die Firewall aus.

- **Allow: (Zulassen:)** Ermöglicht alle Verbindungen mit dem Gerät. Diese Option ist in der Standardeinstellung festgelegt.
- **Deny: (Verweigern:)** Verhindert alle Verbindungen mit dem Gerät.

Für Ausnahmen von der Standardrichtlinie können Sie Regeln erstellen, die über bestimmte Adressen, Protokolle und Ports Verbindungen zum Gerät zulassen oder verweigern.

- **Adresse**: Geben Sie eine Adresse im IPv4-/IPv6- oder im CIDR-Format ein, für die Sie den Zugriff zulassen oder verweigern möchten.
- **Protocol (Protokoll)**: Wählen Sie ein Protokoll aus, für das Sie den Zugriff zulassen oder verweigern möchten.
- **Port**: Geben Sie eine Portnummer ein, für die Sie den Zugriff zulassen oder verweigern möchten. Sie können eine Portnummer zwischen 1 und 65535 hinzufügen.
- **Richtlinie**: Wählen Sie die Richtlinien der Regel aus.

+ : Klicken Sie darauf, um eine weitere Regel zu erstellen.

Add rules: (Regeln hinzufügen:) Klicken Sie hier, um die von Ihnen definierten Regeln hinzuzufügen.

- **Time in seconds: (Zeit in Sekunden:)** Legen Sie für das Testen der Regeln ein Zeitlimit fest. Das Standardzeitlimit beträgt 300 Sekunden. Legen Sie als Zeit 0 Sekunden fest, um die Regeln sofort zu aktivieren.
- **Confirm rules: (Regeln bestätigen:)** Bestätigen Sie die Regeln und deren Zeitlimit. Wenn Sie eine Zeitbegrenzung von mehr als einer Sekunde festgelegt haben, sind die Regeln in dieser Zeit aktiv. Wenn Sie als Zeit 0 eingestellt haben, sind die Regeln sofort aktiv.

Pending rules (Ausstehende Regeln): Eine Übersicht über die kürzlich getesteten, noch zu bestätigenden Regeln.

Hinweis

Die Regeln mit einer Zeitgrenze werden unter **Active rules (Aktive Regeln)** angezeigt, bis der angezeigte Timer abläuft oder Sie die Regeln bestätigen. Wenn Sie die Regeln nicht bestätigen, werden sie unter **Pending rules (Ausstehende Regeln)** angezeigt, bis der Timer abläuft, und die Firewall wird auf die zuvor festgelegten Einstellungen zurückgesetzt. Wenn Sie diese bestätigen, werden die aktuellen aktiven Regeln ersetzt.

Confirm rules (Regeln bestätigen): Klicken Sie hier, um die anstehenden Regeln zu aktivieren.

Active rules (Aktive Regeln): Eine Übersicht über die Regeln, die momentan auf dem Gerät ausgeführt werden.

: Klicken Sie hier, um eine aktive Regel zu löschen.

: Klicken Sie hier, um alle Regeln zu löschen, sowohl anstehend als auch aktiv.

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

Zum Installieren von Testsoftware oder anderer benutzerdefinierter Software von Axis auf dem Gerät benötigen Sie ein benutzerdefiniertes signiertes AXIS OS-Zertifikat. Das Zertifikat prüft, ob die Software sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Software kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Spezifisch signierte AXIS OS-Zertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

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

Das Kontextmenü enthält:

- **Delete certificate (Zertifikat löschen)**: Löschen Sie das Zertifikat.

Konten

Konten

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Bediener**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**-Einstellungen
- **Betrachter**: Hat Zugriff auf:
  - Einen Videostream ansehen und Schnappschüsse machen.
  - Aufzeichnungen ansehen und exportieren.
  - Schwenken, Neigen und Zoomen; Zugang über **PTZ-Konto**.

Das Kontextmenü enthält:

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

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

Anonymer Zugriff

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

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

SSH-Konten

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

- **Enable SSH (SSH aktivieren)**: Den SSH-Dienst aktivieren.

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Anmerkung: Geben Sie eine Anmerkung ein (optional).

Das Kontextmenü enthält:

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

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

Virtual host (Virtueller Host)

Add virtual host (Virtuellen Host hinzufügen): Klicken Sie hier, um einen neuen virtuellen Host hinzuzufügen.

Aktiviert: Wählen Sie diese Option aus, um diesen virtuellen Host zu verwenden.

Server name (Servername): Geben Sie den Namen des Servers ein. Verwenden Sie nur die Zahlen 0 bis 9, die Buchstaben A bis Z und den Bindestrich (-).

Port: Geben Sie den Port ein, mit dem der Server verbunden ist.

Typ: Wählen Sie den Typ der Authentifizierung aus. Sie haben die Wahl zwischen **Basic**, **Digest** und **Open ID**.

Das Kontextmenü enthält:

- **Update (Aktualisieren)**: Aktualisieren Sie den virtuellen Host.
- **Löschen**: Löschen Sie den virtuellen Host.

Disabled (Deaktiviert): Der Server ist deaktiviert.

OpenID-Konfiguration

Wichtig

Wenn Sie sich nicht mit OpenID anmelden können, verwenden Sie die Digest- oder Basic-Anmeldeinformationen, die Sie bei der Konfiguration von OpenID für die Anmeldung verwendet haben.

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

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

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

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

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

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

Empfänger

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden.

Hinweis

Wenn Ihr Gerät für die Verwendung von FTP oder SFTP eingerichtet ist, dürfen Sie die eindeutige Sequenznummer, die den Dateinamen hinzugefügt wird, nicht ändern oder entfernen. Anderenfalls kann nur ein Bild pro Ereignis gesendet werden.

Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis

Sie können bis zu 20 Empfänger erstellen.

Empfänger hinzufügen: Klicken Sie darauf, um einen Empfänger hinzuzufügen.

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

- FTP
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Die vom FTP-Server verwendete Portnummer eingeben. Der Standardport ist Port 21.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem FTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
  - **Passives FTP verwenden**: Normalerweise fordert das Produkt den FTP-Zielserver zum Öffnen der Datenverbindung auf. Normalerweise initiiert das Gerät die FTP-Steuerung und die Datenverbindungen zum Zielserver. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielserver eine Firewall eingerichtet ist.
- HTTP
  - **URL**: Die Netzwerkadresse des HTTP-Servers und das Skript, das die Anforderung bearbeiten wird, eingeben. Beispielsweise http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Proxy**: Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTP-Server ein Proxyserver erforderlich ist.
- HTTPS
  - **URL**: Die Netzwerkadresse des HTTPS-Servers und das Skript, das die Anforderung bearbeiten wird, eingeben. Beispielsweise https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Server-Zertifikate validieren)**: Wählen Sie diese Option, um zu überprüfen, ob das Zertifikat von HTTPS-Server erstellt wurde.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Proxy**: Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTPS-Server ein Proxyserver erforderlich ist.
- Netzwerk-Speicher
  Darüber können Sie einen Netzwerk-Speicher wie NAS (Network Attached Storage) hinzufügen und als Empfänger für zu speichernde Dateien verwenden. Die Dateien werden im Format Matroska (MKV) gespeichert.
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen der Netzwerk-Speicher ein.
  - **Freigabe**: Den Namen der Freigabe beim Host eingeben.

- **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
- **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
- **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.

- SFTP
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Die vom SFTP-Server verwendete Portnummer eingeben. Die Standardeinstellung lautet 22.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem SFTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Öffentlicher SSH-Host-Schlüsseltyp (MD5)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine hexadezimale Zeichenfolge mit 32 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Öffentlicher SSH-Host-Schlüsseltyp (SHA256)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine Base64-kodierte Zeichenfolge mit 43 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.

- SIP oder VMS :
  SIP: Wählen Sie diese Option, um einen SIP-Anruf zu starten.
  VMS: Wählen Sie diese Option, um einen VMS-Anruf zu starten.
  - **Vom SIP-Konto**: Wählen Sie aus der Liste.
  - **An SIP-Adresse**: Geben Sie die SIP-Adresse ein.
  - **Test**: Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.
- E-Mail
  - **E-Mail senden an**: Geben Sie die E-Mail-Adresse ein, an die E-Mails gesendet werden sollen. Trennen Sie mehrere Adressen jeweils mit einem Komma.
  - **E-Mail senden von**: Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.

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

Hinweis

Die Sicherheitsfilter einiger E-Mail-Anbieter verhindern das Empfangen oder Anzeigen vieler Anlagen, das Empfangen geplanter E-Mails usw. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, damit Ihr E-Mail-Konto nicht gesperrt wird oder die erwarteten E-Mails nicht verloren gehen.

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

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

⋮ Das Kontextmenü enthält:

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

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

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

Zeitschemata

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

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

Manuelle Auslöser

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

MQTT

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

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

Mehr lesen zu MQTT in der *AXIS OS Knowledge base*.

ALPN

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

MQTT-Client

Connect (Verbinden): Aktivieren oder deaktivieren Sie den MQTT-Client.

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

Broker

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

Protocol (Protokoll): Wählen Sie das zu verwendende Protokoll aus.

Port: Geben Sie die Portnummer ein.

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

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

Username (Benutzername): Den Benutzernamen eingeben, den der Client für den Zugriff auf den Server verwenden soll.

Password (Kennwort): Ein Kennwort für den Benutzernamen eingeben.

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

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

HTTP proxy (HTTP-Proxy): eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTP-Proxy verwenden möchten.

HTTPS proxy (HTTPS-Proxy): eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTPS-Proxy verwenden möchten.

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

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

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

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

Nachricht zum Verbindungsaufbau

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

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

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

Topic (Thema): Geben Sie das Thema für die Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

Nachricht zum letzten Willen und Testament

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

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

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

Topic (Thema): Geben Sie das Thema für die Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

MQTT-Warteschlange

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

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

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

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

Add condition (Bedingung hinzufügen): Klicken Sie darauf, um eine Bedingung hinzuzufügen.

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

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

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

MQTT-Abonnements

Add subscription (Abonnement hinzufügen): Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

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

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

Abonnementart:

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

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

MQTT-Overlays

Hinweis

Stellen Sie eine Verbindung mit einem MQTT-Broker her, bevor Sie MQTT-Overlay-Modifikatoren hinzufügen.

Overlay-Modifikator hinzufügen: Klicken Sie hier, um einen neuen Overlay-Modifikator hinzuzufügen.

Themenfilter: Fügen Sie das MQTT-Thema hinzu, das die Daten enthält, die im Overlay angezeigt werden sollen.

Datenfeld: Geben Sie den Schlüssel für die Nutzdaten der Nachricht an, die Sie im Overlay anzeigen möchten, vorausgesetzt, die Nachricht ist im JSON-Format.

Modifikator: Verwenden Sie beim Erstellen des Overlays den resultierenden Modifikator.

- Modifikatoren, die mit **#XMP** beginnen, zeigen alle vom Thema empfangenen Daten an.
- Modifikatoren, die mit **#XMD** beginnen, zeigen die im Datenfeld angegebenen Daten an.

SIP

Einstellungen

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

SIP-Einrichtungsassistent: Klicken Sie hier, um SIP schrittweise einzurichten und zu konfigurieren.

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

Eingehende Anrufe zulassen: Diese Option wählen, um eingehende Anrufe von anderen SIP-Geräten zuzulassen.

Anrufbearbeitung

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

Ports

Eine Portnummer muss zwischen 1024 und 65535 liegen.

- **SIP-Port**: Der für die SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Der Standardport ist 5060. Geben Sie eine andere Portnummer ein, falls erforderlich.
- **TLS_Port**: Der für verschlüsselte SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Der Standardport ist 5061. Geben Sie eine andere Portnummer ein, falls erforderlich.
- **RTP-Startport**: Der Netzwerkport, der für den ersten RTP-Medienstream in einem SIP-Anruf verwendet wird. Der standardmäßige Startport ist 4000. Einige Firewalls blockieren den RTP-Datenaustausch über bestimmte Portnummern.

NAT-Traversal

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

Hinweis

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

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

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

Audio und Video

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

Hinweis

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

- **Audioausrichtung**: Wählen Sie zulässige Audiorichtungen.
- **H.264-Paketierungsmodus**: Wählen Sie den zu verwendenden Paketierungsmodus aus.
  - **Auto**: (Empfohlen) Das Gerät entscheidet, welcher Paketierungsmodus verwendet wird.

- **None (Kein)**: Es wird kein Paketierungsmodus festgelegt. Dieser Modus wird häufig als Modus **0** bezeichnet.
- **0**: Nicht-verschachtelter Modus.
- **1**: Modus für eine einzelne NAL-Einheit.

- **Videoausrichtung**: Wählen Sie zulässige Videorichtungen.

Zusätzliches

- **Wechsel von UDP zu TCP**: Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll (User Datagram Protocol) auf das Protokoll TCP (Transmission Control Protocol) zu wechseln. Mit einem Wechsel wird Fragmentierung vermieden und der Wechsel kann stattfinden sofern eine Anfrage innerhalb von 200 Bytes der maximalen Übertragungseinheit (MTU) liegt oder größer als 1300 Byte ist.
- **Über Umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Kontakt umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Register with server every (Alle ... am Server registrieren)**: Legen Sie fest, wie oft sich das Gerät am SIP-Server für SIP-Konten registrieren soll.
- **DTMF-Nutzlasttyp**: Ändert den Standard-Nutzlasttyp für DTMF.
- **Max retransmissions (Max. erneute Übertragungen)**: Legen Sie fest, wie oft das Gerät maximal versuchen soll, eine Verbindung zum SIP-Server herzustellen.
- **Seconds until failback (Sekunden bis zum Ausfall)**: Legen Sie die Anzahl der Sekunden fest, die das Gerät nach einem Failover auf einen sekundären SIP-Server warten soll, bis es erneut versucht, eine Verbindung zum primären SIP-Server herzustellen.

DTMF

Add sequence (Sequenz hinzufügen): Klicken Sie hier, um eine neue DTMF-Sequenz (Dual-Tone Multifrequency) zu erstellen. Um eine Regel zu erstellen, die mit dem Ton aktiviert wird, wechseln Sie zu **Events > Rules (Ereignisse > Regeln)**.

Sequenz: Geben Sie zum Aktivieren der Regel zu verwendenden Zeichen ein. Zulässige Zeichen: 0–9, A–D, #, und *.

Beschreibung: Geben Sie eine Beschreibung der durch die Sequenz auszulösenden Aktion ein.

Accounts (Konten): Wählen Sie die Konten aus, die die DTMF-Sequenz verwenden sollen. Wenn Sie Sich für **peer-to-peer (Peer-to-Peer)** entscheiden, teilen alle Peer-to-Peer-Konten dieselbe DTMF-Sequenz.

Protokolle

Wählen Sie die Protokolle für die einzelnen Konten aus. Alle Peer-to-Peer-Konten teilen die gleichen Protokolleinstellungen.

RTP (RFC2833) verwenden: Wählen Sie diese Option, um die Mehrfrequenzwahl, weitere Tonsignale und Telefonie-Ereignisse in RTP-Paketen zuzulassen.

Use SIP INFO (RFC2976) (SIP INFO (RFC2976) verwenden): Diese Option verwenden, um die Methode INFO in das SIP-Protokoll aufzunehmen. Mit der Methode INFO werden optionale, in der Regel auf die Sitzung bezogene, Anwendungsschichten aufgenommen.

Testanruf

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

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

Zugangsliste

Use access list (Zugangsliste verwenden): Aktivieren Sie dies, um die Zahl der Anrufer auf das Gerät begrenzen.

Richtlinie:

- **Allow (Zulassen)**: Wählen Sie diese Option aus, um eingehende Anrufe nur von den Quellen in der Zugangsliste zu erlauben.
- **Block (Blockieren)**: Wählen Sie diese Option aus, um eingehende Anrufe von den Quellen in der Zugangsliste zu blockieren.

Quelle hinzufügen: Klicken Sie hier, um einen neuen Eintrag in der Zugangsliste zu erstellen.

SIP source (SIP-Quelle): Geben Sie die Anrufer-ID oder die SIP-Server-Adresse der Quelle ein.

Speicherung

Netzwerk-Speicher

Ignorieren: Schalten Sie diese Option ein, um den Netzwerk-Speicher zu ignorieren.

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

- **Adresse**: Geben Sie die IP-Adresse des Host-Servers, in der Regel ein NAS (Network Attached Storage), ein. Wir empfehlen Ihnen, den Host für eine statische IP-Adresse zu konfigurieren (nicht DHCP, da sich eine dynamische IP-Adresse ändern kann) oder DNS zu verwenden. Namen des Typs Windows SMB/CIFS werden nicht unterstützt.
- **Netzwerk-Freigabe**: Den Namen des freigegebenen Speicherorts auf dem Host-Server eingeben. Mehrere Axis Geräte können dieselbe Netzwerk-Freigabe verwenden, da jedes Gerät einen eigenen Ordner erhält.
- **Benutzer**: Wenn der Server eine Anmeldung erfordert, geben Sie den Benutzernamen ein. Zur Anmeldung an einem bestimmten Domainserver geben Sie `DOMAIN\username` ein.
- **Password (Kennwort)**: Wenn der Server eine Anmeldung erfordert, geben Sie das Kennwort ein.
- **SMB-Version**: Wählen Sie die SMB-Speicherprotokollversion für die Verbindung mit dem NAS. Wenn Sie **Auto** wählen, versucht das Gerät, eine der sicheren Versionen SMB zu installieren: 3.02, 3.0 oder 2.1. Wählen Sie 1.0 oder 2.0 zur Herstellung einer Verbindung zu älteren NAS, die höhere Versionen nicht unterstützen. Weitere Informationen zur SMB-Unterstützung in Axis Geräten finden Sie *hier*.
- **Add share without testing (Freigabe ohne Test hinzufügen)**: Wählen Sie diese Option, um die Netzwerk-Freigabe hinzuzufügen, auch wenn während des Verbindungstests ein Fehler erkannt wurde. Bei dem Fehler kann es beispielsweise sein, dass Sie kein Kennwort eingegeben haben, obwohl für den Server ein Kennwort erforderlich ist.

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

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

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

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

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

Werkzeuge

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

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

Onboard-Speicher

Wichtig

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

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

Write protect (gegen Überschreiben schützen): Aktivieren, damit nicht mehr auf die SD-Karte geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte SD-Karte kann nicht formatiert werden.

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

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

Aufbewahrungszeit: Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Menge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn die SD-Speicherkarte voll ist, werden alte Aufzeichnungen vor Ablauf der Aufbewahrungsfrist gelöscht.

Werkzeuge

- **Check (Überprüfen)**: Die SD-Speicherkarte auf Fehler überprüfen.
- **Repair (Reparieren)**: Fehler im Dateisystem beheben.
- **Formatieren**: Die SD-Speicherkarte formatieren, um das Dateisystem zu ändern und alle Daten zu löschen. Sie können die SD-Speicherkarte nur mit dem Dateisystem ext4 formatieren. Sie benötigen einen externen ext4-Treiber oder eine Anwendung, um unter Windows® auf das Dateisystem zuzugreifen.
- **Encrypt (Verschlüsseln)**: Verwenden Sie dieses Tool, um die SD-Karte zu formatieren und die Verschlüsselung zu aktivieren. Alle auf der SD-Karte gespeicherten Daten werden gelöscht. Alle neuen Daten, die Sie auf der SD-Speicherkarte speichern, werden verschlüsselt.
- **Entschlüsseln**: Verwenden Sie dieses Tool, um die SD-Karte ohne Verschlüsselung zu formatieren. Alle auf der SD-Karte gespeicherten Daten werden gelöscht. Alle neuen Daten, die Sie auf der SD-Speicherkarte speichern, werden nicht verschlüsselt.
- **Change password (Kennwort ändern)**: Andern Sie das zum Verschlüsseln der SD-Karte erforderliche Kennwort.

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

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

Videostromprofile

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

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

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

Name: Fügen Sie einen Namen für Ihr Profil hinzu.

Beschreibung: Fügen Sie eine Profilbeschreibung hinzu.

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

Auflösung: Siehe für eine Beschreibung dieser Einstellung.

Bildrate: Siehe für eine Beschreibung dieser Einstellung.

Komprimierung: Siehe für eine Beschreibung dieser Einstellung.

Zipstream : Siehe für eine Beschreibung dieser Einstellung.

Optimize for storage (Für Speicherung optimieren) : Siehe für eine Beschreibung dieser Einstellung.

Dynamic FPS (Dynamische Bilder pro Sekunde) : Siehe zu einer Beschreibung dieser Einstellung.

Dynamic GOP (Dynamische Bildergruppe) : Siehe zu einer Beschreibung dieser Einstellung.

Mirror (Spiegelung) : Siehe für eine Beschreibung dieser Einstellung.

GOP length (GOP-Länge) : Siehe für eine Beschreibung dieser Einstellung.

Bitrate control (Bitratensteuerung): Siehe für eine Beschreibung dieser Einstellung.

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

Include audio (Audio einbeziehen) : Siehe für eine Beschreibung dieser Einstellung.

Über ONVIF

ONVIF-Konten

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

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

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Role (Rolle):

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

Das Kontextmenü enthält:

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

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

ONVIF-Medienprofile

Ein ONVIF-Medienprofil besteht aus einem Satz von Konfigurationen, mit deren Hilfe Sie die Medienstreameinstellungen ändern können. Sie können neue Profile mit Ihren eigenen Konfigurationen erstellen oder vorkonfigurierte Profile für eine schnelle Einrichtung verwenden.

Add media profile (Medienprofil hinzufügen): Klicken Sie darauf, um ein neues ONVIF-Medienprofil hinzuzufügen.

Profilname: Fügen Sie einen Namen für das Medienprofil hinzu.

Video source (Videoquelle): Wählen Sie die Videoquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts, einschließlich Multiviews, Sichtbereichen und virtuellen Kanälen.

Video encoder (Video-Encoder): Wählen Sie das Videokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Video-Encoders. Wählen Sie Benutzer 0 bis 15 aus, um Ihre eigenen Einstellungen anzuwenden, oder wählen Sie einen der Standardbenutzer aus, wenn Sie vordefinierte Einstellungen für ein bestimmtes Codierungsformat verwenden möchten.

Hinweis

Aktivieren Sie Audio im Gerät, um die Option zur Auswahl einer Audioquelle und Audio-Encoder-Konfiguration zu erhalten.

Audio source (Audioquelle) : Wählen Sie die Audioeingangsquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audioeinstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Audioeingängen des Geräts. Wenn das Gerät über einen Audioeingang verfügt, ist es user0. Wenn das Gerät über mehrere Audioeingänge verfügt, werden weitere Benutzer in der Liste angezeigt.

Audio encoder (Audio-Encoder) : Wählen Sie das Audiokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audio-Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Audio-Encoders.

Audio decoder (Audio-Decoder) : Wählen Sie das Audiodekodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.

Audio output (Audioausgang) : Wählen Sie das Audioausgangsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.

Metadata (Metadaten): Wählen Sie die Metadaten aus, die in Ihre Konfiguration einbezogen werden sollen.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Metadaten-Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration der Metadaten.

PTZ : Wählen Sie die PTZ-Einstellungen für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die PTZ-Einstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts mit PTZ-Unterstützung.

Create (Erstellen): Klicken Sie hier, um Ihre Einstellungen zu speichern und das Profil zu erstellen.

Cancel (Abbrechen): Klicken Sie hier, um die Konfiguration abzubrechen und alle Einstellungen zu löschen.

profile_x: Klicken Sie auf den Profilnamen, um das vorkonfigurierte Profil zu öffnen und zu bearbeiten.

Melder

Kamera-Manipulation

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

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

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

Hinweis

Zur Erfassung von Manipulationsversuchen in statischen und nicht überfüllten Szenen.

Audioerkennung

Diese Einstellungen sind für jeden Audioeingang verfügbar.

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

PIR-Sensor

Der PIR-Sensor misst das von Objekten im Sichtfeld ausstrahlende Infrarotlicht.

Empfindlichkeitsstufe: Die Lautstärke kann auf einen Wert von 0 bis 100 festgelegt werden, wobei 0 die unempfindlichste und 100 die empfindlichste Einstellung ist.

Video-Ausgang

HDMI

Über ein HDMI-Kabel kann ein externer Monitor an das Gerät angeschlossen werden.

Einzelquelle

Auf dem externen Monitor wird ein Videostream einer einzelnen Kamera angezeigt.

- **Source (Quelle)**: Wählen Sie nur eine Kamera aus.
- **Rotate image 180° (Bild um 180° drehen)**: Klicken Sie hier zum Drehen des Bildes.
- **Mirror image (Bild spiegeln)**: Klicken Sie hier, um das Bild zu spiegeln.
- **Dynamic overlays (Dynamische Overlays)** : Klicken Sie hier für ein Overlay.

Vierfachansicht

Zeigen Sie Streams von vier separaten Kameras gleichzeitig auf dem externen Monitor an.

- **Sources (Quellen)**: Wählen Sie in jedem der vier Aufklappmenüs eine andere Kamera aus. Das Bild neben der Quelle zeigt, wo das Video von dieser Kamera auf dem Bildschirm angezeigt wird.
- **Rotate image 180° (Bild um 180° drehen)**: Klicken Sie hier zum Drehen aller Bilder.

Wiedergabeliste

Einzelne Streams von mehreren Kameras wechseln sich auf dem externen Monitor ab.

- **Rotate image 180° (Bild um 180° drehen)**: Klicken Sie hier zum des Bildes aus allen Quellen.
- +: Klicken Sie hier, um eine Kamera zur Wiedergabeliste hinzuzufügen.
- **Source (Quelle)**: Wählen Sie die gewünschte Kamera aus.
- **Dauer**: Legen Sie fest, wie lange (in mm:ss) die Wiedergabeliste bei jeder Drehung von dieser Kamera gestreamt wird.
- **Mirror image (Bild spiegeln)**: Klicken Sie hier, um das Bild zu spiegeln.
- **Create (Erstellen)**: Zum Speichern hier klicken.

Bild-in-Bild

Auf dem externen Monitor werden gleichzeitig zwei Streams angezeigt. Ein Stream füllt den Bildschirm vollständig aus, während der andere in einem kleineren Bild angezeigt wird. Die Einstellungen für **Position**, **Picture size (Bildgröße)** und **Borders (Ränder)** können angepasst werden.

- **Bild-in-Bild**
  - **Source (Quelle)**: Wählen Sie die Kamera aus, die als kleineres Bild gestreamt werden soll.
  - **Rotate image 180° (Bild um 180° drehen)**: Klicken Sie hier zum Drehen des Bildes.
  - **Mirror image (Bild spiegeln)**: Klicken Sie hier, um das Bild zu spiegeln.
  - **Position**: Wählen Sie die Stelle aus, an der das Bild am Bildschirm angezeigt werden soll.
  - **Bildgröße**: Legen Sie mit dem Schieberegler die Bildgröße (in % des Bildschirms) fest.
  - **Rahmen**: Klicken Sie auf diese Schaltfläche, um Rahmen für das Bild ein- oder auszuschalten.
  - : Ziehen Sie den Schieberegler, um die Dicke des gesamten Rahmens zu ändern.
  - : Ziehen Sie den Schieberegler, um die Dicke des oberen Rands des Rahmens zu ändern.
  - : Ziehen Sie den Schieberegler, um die Dicke des rechten Rands des Rahmens zu ändern.
  - : Ziehen Sie den Schieberegler, um die Dicke des unteren Rands des Rahmens zu ändern.

- : Ziehen Sie den Schieberegler, um die Dicke des linken Rands des Rahmens zu ändern.
- **Border color (Rahmenfarbe)**: Wählen Sie eine Farbe für den Rahmen aus.

• **Hauptansicht**

- **Source (Quelle)**: Wählen Sie die Kamera aus, die auf dem gesamten Bildschirm gestreamt werden soll.
- **Rotate image 180° (Bild um 180° drehen)**: Klicken Sie hier zum Drehen des Bildes.
- **Mirror image (Bild spiegeln)**: Klicken Sie hier, um das Bild zu spiegeln.

Anzeigen

Anzeigen

Zähler-LED: Lassen Sie sich mithilfe der Signal-LED zeigen, wann sich jemand den Videostream ansieht.

Ein: Die LED ist immer eingeschaltet, auch wenn von diesem Gerät aus keine Videostreams übertragen werden.

Aus: Die LED ist immer ausgeschaltet, auch jemand von diesem Gerät aus keine Videostreams übertragen werden.

Auto: Die LED ist eingeschaltet, wenn jemand einen Videostream vom Gerät aus überträgt.

Zubehör

E/A-Ports

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

Digitale Ausgänge zum Anschließen externer Geräte wie Relais und LEDs verwenden. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

Port

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

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

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

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

Hinweis

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

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

Protokolle

Protokolle und Berichte

Berichte

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

Protokolle

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

Remote System Log

Syslog ist ein Standard für die Nachrichtenprotokollierung. Er ermöglicht die Trennung von der Software, die Nachrichten generiert, dem System, in dem sie gespeichert sind, sowie der Software, die sie meldet und

analysiert. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.

Server: Klicken Sie, um einen neuen Server hinzuzufügen.

Host: Geben Sie den Hostnamen oder die Adresse des Servers ein.

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokoll): Wählen Sie das gewünschte Protokoll aus:

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

Port: Bearbeiten Sie die Port-Nummer, um einen anderen Port zu verwenden.

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

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

Direktkonfiguration

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

Wartung

Wartung

Restart (Neustart): Gerät neu starten. Die aktuellen Einstellungen werden dadurch nicht beeinträchtigt. Aktive Anwendungen werden automatisch neu gestartet.

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

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

Sämtliche Software des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Software auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper „Axis Edge Vault" unter *axis.com*.

AXIS OS upgrade (AXIS OS-Aktualisierung): Aktualisieren Sie auf eine neue AXIS OS-Version. Neue Versionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste AXIS OS-Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu *axis.com/support*.

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

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

AXIS OS rollback (AXIS OS zurücksetzen): Setzen Sie die Version auf die vorherige AXIS OS-Version zurück.

Fehler beheben

PTR zurücksetzen : Setzen Sie PTR zurück, wenn die Einstellungen für **Pan (Schwenken)**, **Tilt (Neigen)** oder **Roll (Drehen)** aus irgendeinem Grund nicht erwartungsgemäß funktionieren. Die PTR-Motoren werden immer mit einer neuen Kamera kalibriert. Die Kalibrierung kann jedoch verloren gehen, beispielsweise wenn die Kamera an Leistung verliert oder die Motoren von Hand bewegt werden. Beim Zurücksetzen von PTR wird die Kamera neu kalibriert und kehrt in die Werkseinstellungen zurück.

Kalibrierung : Klicken Sie auf **Calibrate (Kalibrieren)**, um die Schwenk-, Neige- und Rollmotoren auf ihre Standardpositionen zu kalibrieren.

Ping: Um zu prüfen, ob das Gerät eine bestimmte Adresse erreichen kann, geben Sie den Host-Namen oder die IP-Adresse des Hosts ein, den Sie anpingen möchten, und klicken Sie auf **Start**.

Port prüfen: Um die Konnektivität des Geräts mit einer bestimmten IP-Adresse und einem TCP/UDP-Port zu überprüfen, geben Sie den Host-Namen oder die IP-Adresse und die Port-Nummer ein, die Sie überprüfen möchten, und klicken Sie auf **Start**.

Netzwerk-Trace

Wichtig

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

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

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

Mehr erfahren

Privatzonenmasken

Eine Privatzonenmaske ist ein benutzerdefinierter Bereich, mit dem das Anzeigen von Teilen des überwachten Bereichs durch Benutzer verhindert wird. Privatzonenmasken werden im Videostream als nicht transparente Farbflächen angezeigt.

Die Privatzonenmaske wird auf bzw. in allen Schnappschüssen, aufgezeichneten Videos und Live-Videostreams angezeigt.

Mit dem VAPIX® Application Programming Interface (API) können Sie die Privatzonenmasken verbergen.

Wichtig

Wenn Sie mehrere Privatzonenmasken nutzen, beeinträchtigt dies möglicherweise die Leistung des Produkts.

Sie können mehrere Privatzonenmasken erstellen. Jede Maske kann maximal 3 bis 10 Ankerpunkte haben.

Streaming und Speicher

Video-Komprimierungsformate

Die Wahl des Komprimierungsverfahrens richtet sich nach den Wiedergabeanforderungen und den Netzwerkeigenschaften. Es stehen folgende Optionen zur Verfügung:

Motion JPEG

Motion JPEG oder MJPEG ist eine digitale Videosequenz, die aus einer Reihe von einzelnen JPEG-Bildern erstellt wird. Diese Bilder werden mit einer Bildrate dargestellt und aktualisiert, die ausreicht, um einen ständig aktualisierten Videostream wiederzugeben. Um für das menschliche Auge Videobewegung darzustellen, muss die Bildrate mindestens 16 Bilder pro Sekunde betragen. Video wird bei 30 (NTSC) oder 25 (PAL) Bildern pro Sekunde als vollbewegt wahrgenommen.

Ein Videostream des Typs Motion JPEG erfordert erhebliche Bandbreite, liefert jedoch ausgezeichnete Bildqualität und ermöglicht Zugriff auf jedes einzelne Bild des Videostreams.

H.264 oder MPEG-4 Part 10/AVC

Hinweis

H.264 ist eine lizenzierte Technologie. Das Axis Produkt beinhaltet eine Lizenz zur Wiedergabe von H.264. Die Installation weiterer nicht lizenzierter Kopien des Clients ist untersagt. Für den Erwerb weiterer Lizenzen wenden Sie sich bitte an Ihren Axis Händler.

Mit H.264 kann die Größe einer digitalen Videodatei ohne Beeinträchtigung der Bildqualität im Vergleich zum Format Motion JPEG um mehr als 80 % und im Vergleich zum älteren MPEG-Formaten um mehr als 50 % reduziert werden. Das bedeutet weniger Bandbreite und Speicherplatz für eine Videodatei. Anders ausgedrückt: Bei einer bestimmten Bitrate kann eine höhere Videoqualität erzielt werden.

H.265 oder MPEG-H Part 2/HEVC

Mit H.265 kann die Größe einer digitalen Videodatei ohne Beeinträchtigung der Bildqualität im Vergleich zu H.264 um mehr als 25 % reduziert werden.

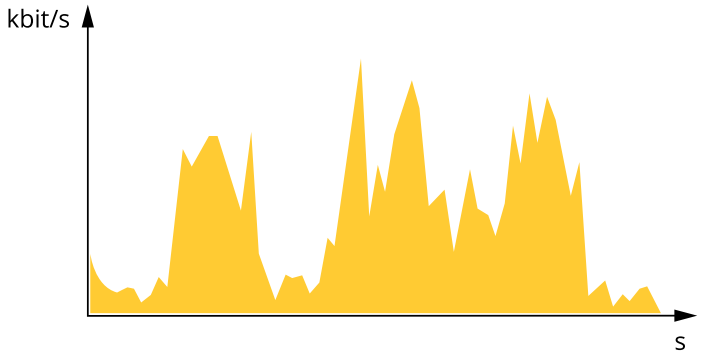
Hinweis

- H.265 ist eine lizenzierte Technologie. Das Axis Produkt beinhaltet eine Lizenz zur Wiedergabe von H.265. Die Installation weiterer nicht lizenzierter Kopien des Clients ist untersagt. Für den Erwerb weiterer Lizenzen wenden Sie sich bitte an Ihren Axis Händler.
- Die meisten Webbrowser unterstützen nicht das Dekodieren von H.265. Aus diesem Grund wird sie auf der Weboberfläche der Kamera nicht unterstützt. Stattdessen können Sie auf ein Videoverwaltungssystem oder eine Anwendung zurückgreifen, die das Decodieren von H.265 unterstützt.

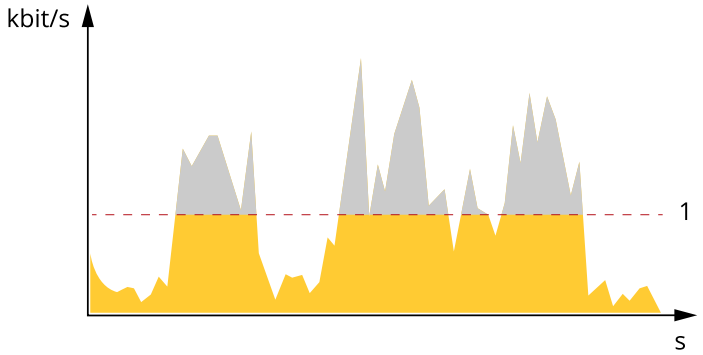
Bitrate-Steuerung

Die Bitratensteuerung hilft Ihnen bei der Verwaltung der Bandbreitennutzung Ihres Videostreams.

Variable Bitrate (VBR)
Mit der variablen Bitrate können Sie den Bandbreitenverbrauch je nach Aktivitätslevel in der Szene ändern. Je mehr Aktivität stattfindet, desto mehr Bandbreite ist erforderlich. Mit der variablen Bitrate ist eine konstante Bildqualität garantiert, wobei jedoch sichergestellt sein muss, dass Speichermargen vorhanden sind.



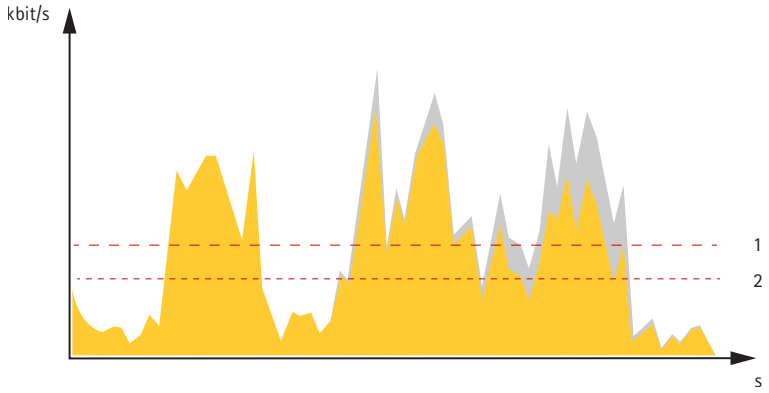
Maximale Bitrate (MBR)
Mit der maximalen Bitrate können Sie eine Zielbitrate einstellen, um die Bitratenbeschränkungen in Ihrem System einzubeziehen. Möglicherweise wird die Bildqualität oder die Bildrate verringert, da die augenblickliche Bitrate unterhalb der angegebenen Zielbitrate gehalten wird. Sie können festlegen, ob die Bildqualität oder die Bildrate priorisiert werden soll. Wir empfehlen Ihnen, die Zielbitrate auf einen höheren Wert als die erwartete Bitrate zu konfigurieren. Dadurch haben Sie einen Spielraum, wenn sich das Aktivitätsniveau in der Szene erhöht.



1 Zielbitrate

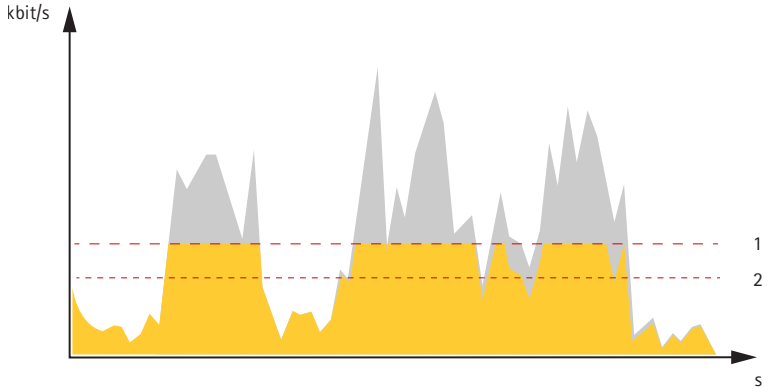
Durchschnittliche Bitrate (Average Bitrate, ABR)
Bei durchschnittlicher Bitrate wird die Bitrate automatisch über einen längeren Zeitraum angepasst. Dadurch können Sie das angegebene Ziel erfüllen und die beste Videoqualität auf Grundlage Ihres verfügbaren Speichers bereitstellen. Im Vergleich zu statischen Szenen ist die Bitrate in Szenen mit viel Aktivität höher. In Szenen mit viel Aktivität erhalten Sie mit der Option „durchschnittliche Bitrate" eher eine bessere Bildqualität. Sie können den erforderlichen Gesamtspeicher für die Speicherung des Videostreams für eine festgelegte Zeitspanne (Aufbewahrungszeit) festlegen, wenn die Bildqualität auf die angegebene Zielbitrate eingestellt wird. Stellen Sie die durchschnittliche Bitrate auf folgende Arten ein:

- Um den geschätzten Speicherbedarf zu berechnen, stellen Sie die Zielbitrate und die Aufbewahrungszeit ein.
- Um die durchschnittliche Bitrate auf Grundlage des verfügbaren Speichers und der erforderlichen Aufbewahrungszeit zu berechnen, verwenden Sie den Zielbitratenrechner.



1 *Zielbitrate*
2 *Tatsächliche durchschnittliche Bitrate*

Sie können auch die maximale Bitrate aktivieren und innerhalb der durchschnittlichen Bitrate eine Zielbitrate festlegen.



1 *Zielbitrate*
2 *Tatsächliche durchschnittliche Bitrate*

Anwendungen

Mit Anwendungen erhalten Sie mehr aus Ihrem Axis Gerät. Die AXIS Camera Application Platform (ACAP) ist eine offene Plattform, die es für andere Anbietern möglich macht, Analysefunktionen und andere Anwendungen für Axis Geräte zu entwickeln. Anwendungen können auf dem Gerät vorinstalliert werden und können kostenlos oder für eine Lizenzgebühr heruntergeladen werden.

Benutzerhandbücher zu Axis Anwendungen finden Sie auf *help.axis.com*.

AXIS Object Analytics

AXIS Object Analytics ist eine Analyseanwendung, die auf der Kamera vorinstalliert ist. Es erkennt Objekte, die sich in der Szene bewegen, und klassifiziert sie z. B. als Menschen oder Fahrzeuge. Sie können die Anwendung so einrichten, dass sie Alarme für verschiedene Arten von Objekten sendet. Mehr zur Funktionsweise der Anwendung erfahren Sie im *Benutzerhandbuch zu AXIS Object Analytics*.

Metadaten-Visualisierung

Metadaten für Analysefunktionen sind für sich bewegende Objekte in der Szene verfügbar. Unterstützte Objektklassen werden im Videostream über ein Umgrenzungsfeld um das Objekt herum dargestellt. Dort finden Sie außerdem Informationen über den Objekttyp und die Zuverlässigkeitsstufe der Klassifizierung. Weitere Informationen zum Konfigurieren und Nutzen von Analyse-Metadaten finden Sie im *AXIS Scene Metadata-Integrationsleitfaden*.

Erweiterte WLAN-Einstellungen

Die gängigste Sicherheitsmethode ist WPA™-Personal. Dieses Gerät unterstützt auch WPA™-Enterprise, eine sicherere Methode. Alle Einstellungen müssen mit den Einstellungen des Zugriffspunkts übereinstimmen.

WPA™ Personal

Die Sicherheitsmethode **WPA-Personal** ist für kleine Netzwerke ausgelegt und erfordert keinen Authentifizierungsserver.

WPA™ Enterprise

Die Sicherheitsmethode **WPA-Enterprise** ist für große Netzwerke ausgelegt und erfordert einen Authentifizierungsserver. Das Netzwerk wird durch EAPOL (Extensible Authentication Protocol Over LAN) geschützt.

Wählen Sie den vom Zugriffspunkt verwendeten WPA-Enterprise-Typ aus:

- EAP-TLS. Siehe .
- EAP-PEAP/MSCHAPv2. Siehe .

EAP-TLS

Mithilfe des Authentifizierungsprotokolls **EAP-TLS** (Extensible Authentication Protocol – Transport Layer Security) können sich Client und Server gegenseitig mit digitalen Zertifikaten authentifizieren, die von einer Zertifikatstelle bereitgestellt werden. Für den Zugriff auf das geschützte Netzwerk präsentiert das Axis Produkt dem Netzwerkzugriffspunkt sein Zertifikat. Bei Genehmigung des Zertifikats wird der Zugriff gewährt.

Wichtig

Für eine erfolgreiche Validierung des Zertifikats sollte auf allen Clients und Servern vor der Konfiguration eine Zeitsynchronisierung durchgeführt werden.

Konfigurieren der WLAN-Verbindung mithilfe von WPA™ Enterprise und EAP-TLS

1. Wechseln Sie zu **System > WLAN**.
2. Klicken Sie auf + **Add network (Netzwerk hinzufügen)**.
3. Wählen Sie in der Liste der Authentifizierungsmethoden **WPA-Enterprise EAP-TLS** aus.
4. Geben Sie die mit dem Zertifikat verknüpfte SSID ein.
5. Wählen Sie unter **EAPoL -Version** die Version (1, 2 oder 3) aus, die für den Zugriffspunkt verwendet wird.
6. Wählen Sie das **CA-Zertifikat** und das **Clientzertifikat** aus, die für die drahtlose Authentifizierung verwendet werden sollen.
7. Klicken Sie auf **Save**.

EAP-PEAP/MSCHAPv2

Mithilfe des Authentifizierungsprotokolls **EAP-PEAP/MSCHAPv2** (Extensible Authentication Protocol – Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) kann der Client das Netzwerk mit einem digitalen Zertifikat authentifizieren, das von einer Zertifikatstelle bereitgestellt wird. Das Netzwerk authentifiziert den Client mit einer Identität und einem Kennwort. Für den Zugriff auf das geschützte Netzwerk präsentiert das Axis Produkt dem Netzwerkzugriffspunkt seine Identität und sein Kennwort. Wenn diese Anmeldeinformationen genehmigt werden, gewährt der Zugriffspunkt den Zugriff über einen vorkonfigurierten Port.

Wichtig

Für eine erfolgreiche Validierung des Zertifikats sollte auf allen Clients und Servern vor der Konfiguration eine Zeitsynchronisierung durchgeführt werden.

Konfigurieren der WLAN-Verbindung mithilfe von WPA™ Enterprise und EAP-PEAP/MSCHAPv2

1. Wechseln Sie zu **System > WLAN**.
2. Klicken Sie auf + **Add network (Netzwerk hinzufügen)**.
3. Wählen Sie in der Liste der Authentifizierungsmethoden **WPA-Enterprise EAP-PEAP/MSCHAPv2** aus.
4. Geben Sie die mit dem Zertifikat verknüpfte SSID ein.
5. Geben Sie das Password (Kennwort) für die Benutzeridentität ein.
6. Wählen Sie unter **EAPoL -Version** die Version (1, 2 oder 3) aus, die für den Zugriffspunkt verwendet wird.
7. Wählen Sie unter **Peap-Version** (0 oder 1) aus, die für den Zugriffspunkt verwendet wird.
8. Wählen Sie das **Label (Etikett)** aus, das der Zugriffspunkt bei Verwendung von Peap Version 1 verwendet. Wählen Sie 1 zur Verwendung von EAP-Verschlüsselung für den Client und 2 zur Verwendung von PEAP-Verschlüsselung für den Client aus.
9. Wählen Sie das **CA-Zertifikat** aus, mit dem das Zertifikat des Netzwerks/Zugriffspunkts überprüft werden soll.
10. Klicken Sie auf **Save**.

Zertifikate für Drahtlosnetzwerke

Zertifikate für Drahtlosnetzwerke werden zum Authentifizieren von Geräten in einem Drahtlosnetzwerk verwendet. Drahtlosnetzwerke mit der Sicherheitsmethode WPA™-/IEEE-Enterprise werden durch EAPoL (Extensible Authentication Protocol over Lan) geschützt. Dieses Protokoll ist Teil des Standards IEEE 802.1X. Der Client authentifiziert den Server mithilfe von digitalen Zertifikaten. Der Server authentifiziert den Client gemäß dem ausgewählten WPA-Enterprise-Typ mithilfe von digitalen Zertifikaten oder über ein Kennwort.

Cybersicherheit

Produktspezifische Informationen zur Cybersicherheit finden Sie im Datenblatt des Produkts auf axis.com.

Ausführliche Informationen zur Cybersicherheit in AXIS OS finden Sie im *AXIS OS Härtungsleitfaden*.

Signiertes Betriebssystem

Signiertes OS wird vom Softwarehersteller implementiert, der das AXIS OS-Image mit einem privaten Schlüssel signiert. Wenn die Signatur an das Betriebssystem angefügt wurde, validiert das Gerät die Software vor der Installation. Wenn das Gerät feststellt, dass die Integrität der Software beeinträchtigt ist, wird die Aktualisierung von AXIS OS abgelehnt.

Sicheres Hochfahren

Sicheres Hochfahren ist ein Boot-Prozess, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Hochfahren auf der Verwendung von signiertem OS basiert, wird sichergestellt, dass ein Gerät nur mit autorisierter Software booten kann.

Axis Edge Vault

Axis Edge Vault stellt eine Hardware-basierte Cybersicherheitsplattform bereit, die das Axis Gerät schützt. Sie bietet Funktionen, die die Identität und Integrität des Geräts gewährleisten und Ihre vertraulichen Daten vor unbefugtem Zugriff schützen. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule

(Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

TPM (Trusted Platform Module)

Das TPM (Trusted Platform Module) ist eine Komponente, die kryptografische Funktionen zum Schutz von Daten vor unbefugtem Zugriff bereitstellt. Sie wird immer aktiviert und es gibt keine Einstellungen, die geändert werden können.

Axis Geräte-ID

Den Ursprung eines Gerätes überprüfen zu können, ist der Schlüssel zum Vertrauen in die Geräteidentität. In der Produktion wird Geräten mit Axis Edge Vault ein eindeutiges, von der Fabrik bereitgestelltes und IEEE 802.1AR-kompatibles Zertifikat für die Axis Geräte-ID zugewiesen. Dies funktioniert wie ein Reisepass und weist den Ursprung des Gerätes nach. Die Geräte-ID wird sicher und permanent als vom Axis Root-Zertifikat signiertes Zertifikat im sicheren Schlüsselspeicher aufbewahrt. Die Geräte-ID kann über die IT-Infrastruktur des Kunden für ein automatisiertes, sicheres Geräte-Onboarding und sichere Geräteidentifizierung genutzt werden.

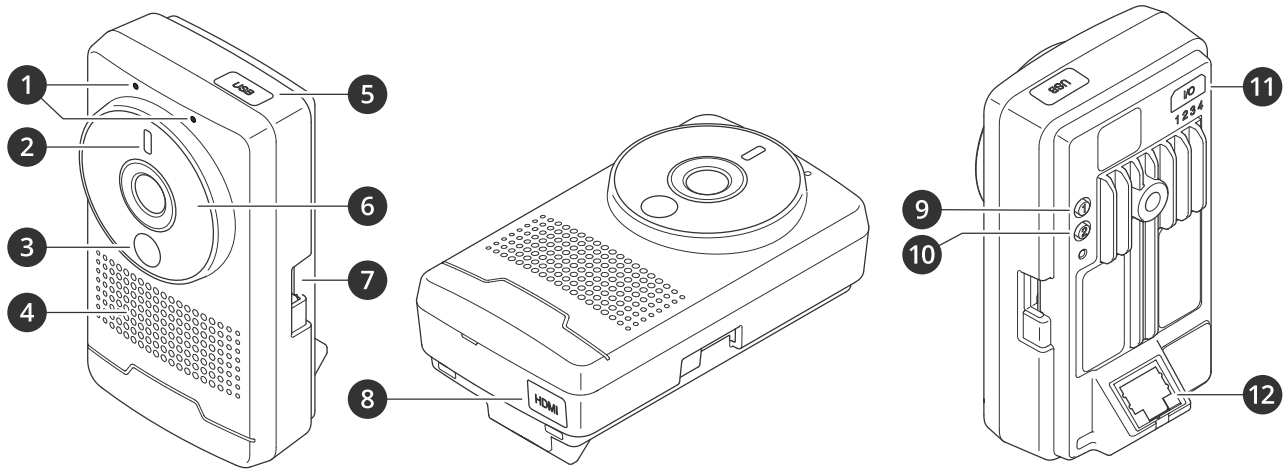
Signiertes Video

Signiertes Video sorgt dafür, dass Videobeweise als nicht manipuliert verifiziert werden können, ohne die Produktkette der Videodatei überprüfen zu müssen. Jede Kamera hat ihren eigenen, eindeutigen Videosignierschlüssel, der zuverlässig im sicheren Schlüsselspeicher aufbewahrt wird und eine Signatur zum Videostream hinzufügt. Beim Abspielen des Videos zeigt der Datei-Player an, ob das Video intakt ist. Signiertes Video ermöglicht die Nachverfolgung des Videos bis zur Kamera und die Überprüfung, ob das Video nach der Aufzeichnung verfälscht wurde.

Um mehr zu den Cybersicherheitsfunktionen von Axis Geräten zu erfahren, gehen Sie auf *axis.com/learning/white-papers* und suchen Sie nach Cybersicherheit.

Technische Daten

Produktübersicht



1 *Mikrofon*
2 *Status-LED*
3 *PIR-Sensor*
4 *Lautsprecher*
5 *USB-Anschluss*
6 *IR-LED*
7 *Einschub für SD-Speicherkarte*
8 *MicroHDMI-Anschluss Typ D*
9 *Steuertaste*
10 *WLAN-Setup-Taste*
11 *E/A-Anschluss*
12 *Netzwerk-Anschluss*

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 der Firmware-Aktualisierung und Wiederherstellung der Werkseinstellungen.
Gelb/rot	Blinkt orange/rot, wenn die Netzwerk-Verbindung nicht verfügbar ist oder unterbrochen wurde.
Rot	Leuchtet rot, wenn Live-Stream oder Aufzeichnung an ist.
Blau	Leuchtet im WLAN-Setup-Modus blau.

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 .
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Um eine Verbindung herzustellen, drücken Sie die Taste, lassen Sie sie los und warten Sie, bis die Status LED dreimal grün blinkt.

WLAN-Setup-Taste

Mit der Schaltfläche WLAN-Setup wird die WLAN-Verbindung eingerichtet.

Anschlüsse

HDMI-Anschluss

Über den microHDMI™-Anschluss werden Displays oder öffentliche Monitore angeschlossen.

Netzwerk-Anschluss

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

USB-Anschluss

Schließen Sie externes Zubehör über den USB-Anschluss an. Unterstütztes Zubehör finden Sie im Datenblatt des Produkts.

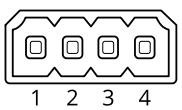
E/A-Anschluss

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.

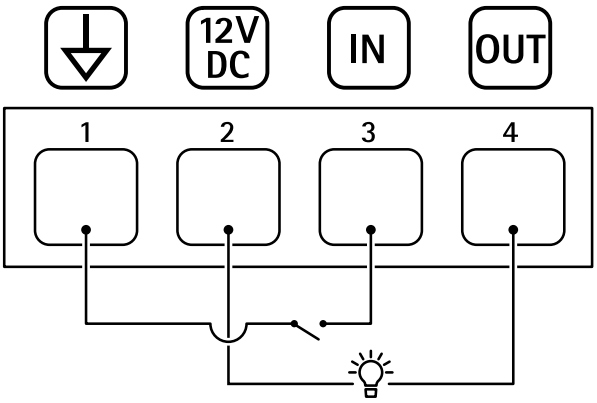
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

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	3	Zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	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:



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

Gerät reinigen

Sie können Ihr Gerät mit lauwarmem Wasser reinigen.

HINWEIS

- Aggressive Chemikalien können das Gerät beschädigen. Verwenden Sie zur Reinigung Ihres Geräts keine chemischen Substanzen wie Fensterreiniger oder Aceton.
- Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken führen kann.

1. Verwenden Sie eine Druckluft-Dose zum Entfernen von Staub und Schmutz von dem Gerät.
2. Reinigen Sie das Gerät ggf. mit einem weichen, mit lauwarmem Wasser angefeuchteten Mikrofasertuch.
3. Trocknen Sie das Gerät mit einem sauberen, nicht scheuernden Tuch ab, um Flecken zu vermeiden.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen muss mit Umsicht geschehen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Drücken und halten Sie die Steuertaste, um das Gerät wieder einzuschalten. Siehe .
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. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
   - **Geräte mit AXIS OS 12.0 oder höher:** Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
   - **Geräte mit AXIS OS 11.11 oder niedriger:** 192.168.0.90/24
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

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Gerätesoftware gespeichert (sofern die Funktionen als Teil der neuen AXIS OS-Version verfügbar sind). Es besteht diesbezüglich jedoch keine Gewährleistung seitens Axis Communications AB.
- 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 Fragen, Hinweise und Lösungen

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

Probleme beim Aktualisieren von AXIS OS	
Fehler bei der AXIS OS-Aktualisierung	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	
Das Gerät befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.

Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein): • `Reply from <IP address>: bytes=32; time=10...` bedeutet, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut. • `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Wenn daher ein anderes Gerät standardmäßig dieselbe statische IP-Adresse verwendet, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Stellen Sie bei aktiviertem HTTPS sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell `http` oder `https` in das Adressfeld des Browsers eingeben. Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe .
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 kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen dazu finden Sie auf *axis.com/support*.
Zertifikatfehler beim Verwenden von IEEE 802.1X	Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **Einstellungen > System > Datum und Uhrzeit**.

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

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

- AXIS Camera Station Edge: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station 5: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.
- 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 bietet die Dokumentation des Adapters.
Niedrigere Bildrate als erwartet	• Siehe . • 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.
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.

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

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

Leistungsaspekte

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

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Hohe Bildauflösung und geringe Komprimierung führen zu Bildern mit mehr Daten, die wiederum mehr Bandbreite erfordern.
- Durch Drehen des Bildes in der GUI kann sich die CPU-Auslastung des Geräts erhöhen.

- Der Zugriff von vielen Clients des Typs Motion JPEG oder Unicast H.264/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*.

T10180154_de

2025-06 (M16.2)

© 2022 – 2025 Axis Communications AB