AXIS D6310 Air Quality Sensor

Benutzerhandbuch

Inhalt

Installation 4
Funktionsweise 5
....5
Das Gerät im Netzwerk ermitteln 5
Unterstützte Browser 5
Weboberfläche des Geräts öffnen 5
Administratorkonto erstellen 5
Sichere Kennwörter 6
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat. 6
Ihr Gerät konfigurieren 7
Luftqualitätsmonitor konfigurieren 7
Konfigurieren Sie das Dashboard des Luftqualitätssensors. 7
Luftqualitätssensor einstellen 8
Sensordatenstatistik herunterladen 8
Kalibrierung für den Erstbetrieb des Geräts 9
Ein Profil konfigurieren 9
Ein Profil mit benutzerdefinierter Audiodatei für die Sirene konfigurieren 10
Ein Profil importieren oder exportieren 10
Direktes SIP (P2P) einrichten 10
SIP über einen Server (PBX) einrichten 11
Einrichten von Regeln für Ereignisse 12
Lösen Sie eine Aktion aus 12
Video aufzeichnen, wenn Vaping detektiert wird 12
Audio-Clip abspielen, wenn CO2-Wert zu hoch ist 12
Aktivieren Sie ein Licht- und Sirenenprofil über den externen Bewegungsmelder (PIR-Sensor). 13
Profil starten, wenn ein Alarm ausgelöst wird 13
Profil über SIP starten 14
Mehrere Profile über SIP-Erweiterungen steuern 14
Zwei Profile mit unterschiedlichen Prioritäten ausführen 15
Aktivieren Sie ein Licht- und Sirenenprofil über HTTP Post, wenn eine Kamera ein Bewegungsmuster erkennt 15
Aktivieren Sie ein Licht- und Sirenenprofil über einen virtuellen Eingang, wenn eine Kamera ein Bewegungsmuster erkennt 17
Aktivieren Sie ein Licht- und Sirenenprofil über MQTT, wenn eine Kamera ein Bewegungsmuster erkennt 18
Senden einer E-Mail, wenn ein Lautsprechertest fehlschlägt 19
Bei Auslösen eines Alarms benutzerdefinierten Clip wiedergeben 20
Audio mit DTMF anhalten 21
Audio für eingehende SIP-Anrufe einrichten 22
Weboberfläche 24
Status 24
Video 25
Videostream 25
Luftqualitätssensor 26
Dashboard 26
Einstellungen 30
Statistik 32
Analyse 32
AXIS Audio Analytics 32
Audio 33
Geräteinstellungen 33
Videostream 34
Audio-Clips 34

Audioverbesserung 34
Übersicht 34
Profile 35
Aufzeichnungen 37
Medien 38
Apps 39
System 39
Uhrzeit und Ort 39
Netzwerk 41
Sicherheit 45
Konten 50
Ereignisse 53
MQTT 58
SIP 61
Speicherung 66
Videostromprofile 67
Über ONVIF 68
Melder 71
Energieeinstellungen 71
Zubehör 71
Protokolle 72
Direktkonfiguration 73
Wartung 74
Wartung 74
Fehler beheben 75
Technische Daten 76
Produktübersicht 76
..... 76
Status-LED 77
Tasten 77
Steuertaste 77
Mikrofonschalter 77
Anschlüsse 77
Netzwerk-Anschluss 77
E/A-Anschluss 77
Anschlusstyp RS-485/RS-422 78
Namen von Lichtmustern 79
Sirenenmuster-Namen 79
Gerät reinigen 81
Fehlerbehebung 82
Zurücksetzen auf die Werkseinstellungen 82
Technische Fragen, Hinweise und Lösungen 82
Leistungsaspekte 84
Support 84

Installation

Wichtig

- Halten Sie einen Mindestabstand von 1,5 Metern (4,9 Fuß) zu Bereichen mit großen Lüftungsöffnungen oder Verschmutzungsquellen ein. Dazu gehören Lüftungsöffnungen, Türen, Fenster, Kochstellen usw.
- Installieren Sie das Gerät an einem Einsatzort, der einen ungehinderten Luftstrom ermöglicht.
- Installieren Sie das Gerät an der Decke in einer Höhe von 2,4–2,7 Metern (7,9–8,9 Fuß) über dem Boden, um eine effektive Erfassung von Vapen oder Rauchen zu gewährleisten.
- Um die Luftqualität und die Umwelt effektiv zu überwachen, installieren Sie das Gerät in einer Höhe von 0,9 bis 1,8 Metern (3,0–5,9 Fuß) über dem Boden.

Ausführliche Anweisungen zur Installation finden Sie in der Installationsanleitung.

Funktionsweise

⚠ WARNUNG

Blinkende oder flackernde Lichter können Krampfanfälle bei Personen mit lichtempfindlicher Epilepsie auslösen.

Das Gerät im Netzwerk ermitteln

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

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
   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 *Administratorkonto erstellen, on page 5*.

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter *Weboberfläche, on page 24*.

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter, on page 6*.
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Konto hinzufügen**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 82*.

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 82*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

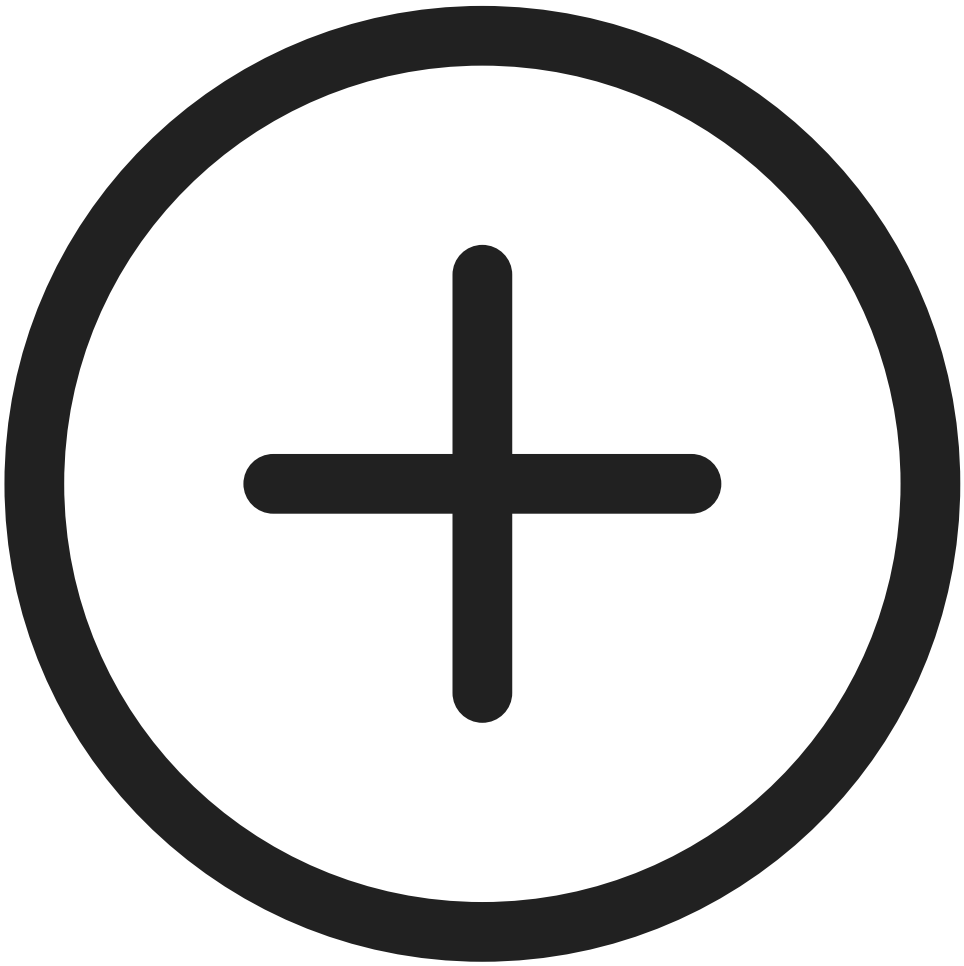
Ihr Gerät konfigurieren

Luftqualitätsmonitor konfigurieren

Konfigurieren Sie das Dashboard des Luftqualitätssensors.

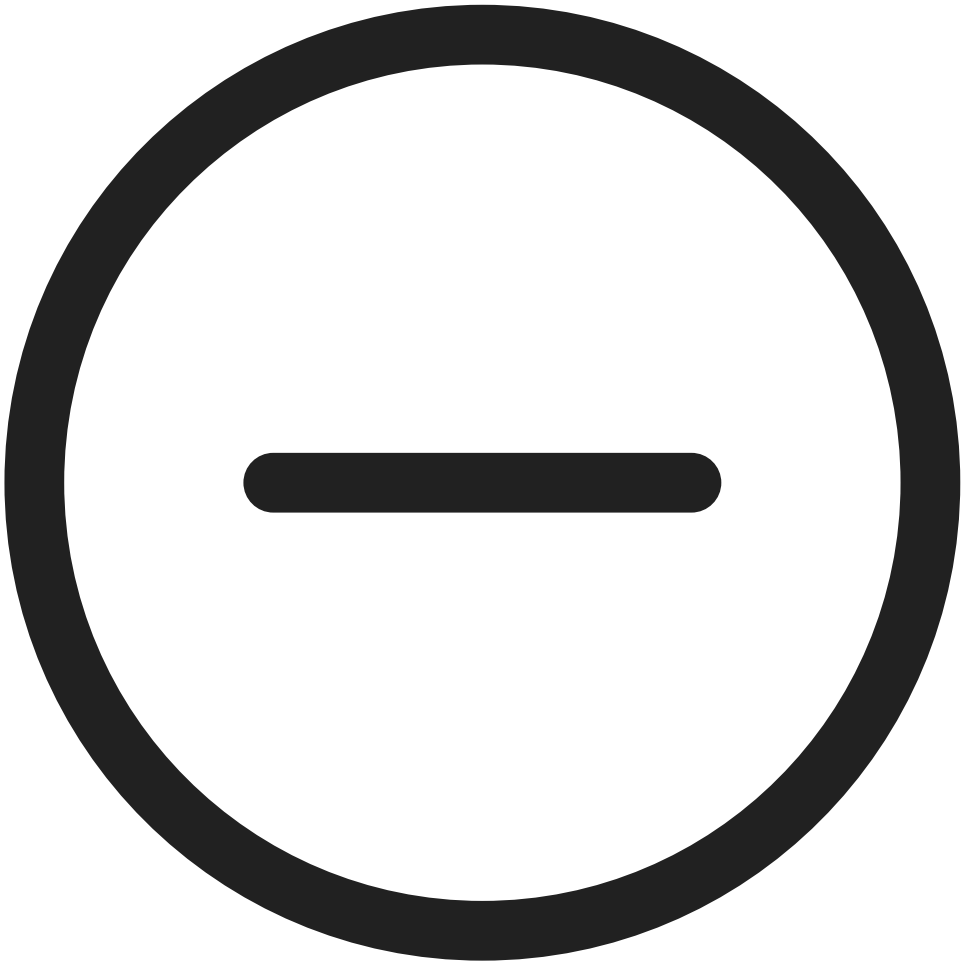
Gehen Sie auf der Gerät-Webseite zu **Air quality monitor (Luftqualitätsmonitor)** > **Dashboard**:

- Um den Namen des Dashboards zu bearbeiten, klicken Sie auf auf der linken Seite.
- Um Daten auf dem Dashboard anzuzeigen, klicken Sie auf **Edit (Bearbeiten)** >



.

- Um Daten auf dem Dashboard auszublenden, klicken Sie auf **Edit (Bearbeiten)** >



.

Luftqualitätssensor einstellen

Gehen Sie auf der Gerät-Webseite zu **Air quality sensor (Luftqualitätssensor)** > **Settings (Einstellungen)**.

- Legen Sie Grenzwerte für Temperatur, Luftfeuchtigkeit, CO2, NOx, PM1.0, PM2.5, PM4.0, PM10.0, VOC und AQI fest, siehe *Einstellungen, on page 30*.
- Stellen Sie die Temperatureinheiten ein, siehe *Einstellungen, on page 30*.
- Stellen Sie die Empfindlichkeit der Vaping-Detektion auf, siehe *Einstellungen, on page 30*.
- Legen Sie die Aufbewahrungszeit fest, siehe *Speicher-Einstellung, on page 31*.
- Stellen Sie die Häufigkeit von Cloud-Metadaten ein, siehe *Häufigkeit von Cloud-Metadaten, on page 31*.
- Stellen Sie den Validierungszeitraum ein, siehe *Validierungszeitraum, on page 31*.

Sensordatenstatistik herunterladen

Sie können Sensorstatistiken für bis zu 365 Tage in eine CSV-Datei exportieren, um sie in Anwendungen wie Microsoft® Excel zu verwenden.

1. Rufen Sie auf der Webseite des Geräts **Air quality monitor (Luftqualitätsmonitor)** > **Statistics (Statistik)** > **Sensor Data Statistics (Sensordatenstatistik)** auf.
2. Wählen Sie einen Datumsbereich:
   - **Custom range (Benutzerdefinierter Bereich)**: Wählen Sie in den Listen **From (Von)** und **To (Bis)** das Start- und Enddatum (bis zu 365 Tage) aus.
   - **Predefined range (Vordefinierter Bereich)**: Wählen Sie in der Liste **Predefined date range (Vordefinierter Datumsbereich)** einen verfügbaren Zeitraum aus.

   Hinweis

   Wenn sowohl ein benutzerdefinierter als auch ein vordefinierter Bereich ausgewählt sind, hat der benutzerdefinierte Bereich Vorrang.

   Hinweis

   Der maximale Download-Bereich wird durch die in *Speicher-Einstellung, on page 31* konfigurierte Speicherdauer begrenzt.
3. Wählen Sie in der Liste **Source (Quelle)** die gewünschte Quelle aus; um Daten für alle Quellen zu exportieren, klicken Sie auf **Download all data (Alle Daten herunterladen)**.
4. Klicken Sie auf **Download data (Daten herunterladen)**, um die ausgewählten Statistiken zu exportieren.

Hinweis

Klicken Sie auf **Download all data (Alle Daten herunterladen)**, um Daten für alle Quellen innerhalb des gewählten Zeitraums zu exportieren.

Kalibrierung für den Erstbetrieb des Geräts

Hinweis

- Die volle CO2-Genauigkeit wird bei Erstbetrieb des Geräts erst nach 2 Tagen erreicht.
- Der AQI (Air Quality Index) benötigt bei der ersten Inbetriebnahme des Geräts 12 Stunden, um funktionsfähig zu werden. Der AQI-Wert zeigt **Calculating (wird berechnet)** an, bis genügend Daten vorliegen. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.
- Die volle Genauigkeit des VOC-Wertes erreicht das Gerät nach einer Betriebsstunde. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.
- Die volle Genauigkeit des NOx-Wertes erreicht das Gerät nach sechs Betriebsstunden. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.

Ein Profil konfigurieren

Ein Profil ist eine Sammlung von festgelegten Konfigurationen. Es können bis zu 30 Profile mit unterschiedlichen Prioritäten und Mustern erstellt werden.

So legen Sie ein neues Standardszenario fest:

1. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf + **Create (Anlegen)**.
2. Geben Sie einen **Namen** und eine **Beschreibung** ein.
3. Wählen Sie die Einstellungen für **Licht** und **Sirene** für Ihr Profil.
4. Stellen Sie mit **Priority (Priorität)** den Signalisierungsvorrang (Licht oder Sirene) fest, und klicken Sie auf **Save (Speichern)**.

Um ein Profil zu bearbeiten, klicken Sie auf ⋮ und wählen **Edit (Bearbeiten)**.

Ein Profil mit benutzerdefinierter Audiodatei für die Sirene konfigurieren

Sie können ein Profil mit einer benutzerdefinierten Audiodatei konfigurieren. Sie können Audiodateien mit einer Größe von bis zu 100 MB auf dem Gerät speichern. Verwenden Sie für größere Audio-Dateien eine SD-Karte, wenn das Gerät über einen SD-Karteneinschub verfügt.

Eine Audiodatei hochladen:

1. Wechseln Sie zu **Media (Medien)** und klicken Sie dann auf + **Add (Hinzufügen)**.
2. Nutzen Sie die Funktion zum Durchsuchen, um die Datei auf Ihrem Computer auszuwählen.
3. Gehen Sie auf **Storage location (Speicherort)**.
4. **Save (Speichern)** anklicken.

So verwenden Sie die Audiodatei in einem Profil:

1. Gehen Sie zu **Profiles (Profile)** und erstellen Sie ein Profil. Weitere Informationen finden Sie unter *Ein Profil konfigurieren, on page 9*.
2. Bei einer Konfiguration mit **Siren (Sirene)** wählen Sie die hochgeladene Audiodatei als **Pattern (Muster)** aus.

Ein Profil importieren oder exportieren

Wenn Sie ein Profil mit vordefinierten Konfigurationen verwenden möchten, können Sie es importieren:

1. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf + **Import (Importieren)**.
2. Suchen Sie nach der Datei oder legen Sie die zu importierende Datei per Drag and Drop ab.
3. **Save (Speichern)** anklicken.

Um ein oder mehrere Profile zu kopieren und auf andere Geräte zu speichern, können Sie diese exportieren:

1. Wählen Sie die Profile aus.
2. Klicken Sie auf **Exportieren**.
3. Suchen Sie nach den json-Dateien.

Direktes SIP (P2P) einrichten

Verwenden Sie Peer-to-Peer, wenn die Kommunikation zwischen wenigen Benutzern innerhalb desselben IP-Netzwerks erfolgt und keine zusätzlichen Funktionen erforderlich sind, die von einem PBX-Server bereitgestellt werden können. Weitere Informationen zur Funktionsweise von P2P finden Sie unter .

Weitere Informationen zu den SIP-Einstellungsoptionen finden Sie unter *SIP, on page 61*.

1. Wechseln Sie zu **System** > **SIP** > **SIP settings** (System > SIP > SIP-Einstellungen), und wählen Sie **Enable SIP (SIP aktivieren)**.
2. Um auf dem Axis Gerät eingehende Anrufe zu erlauben, **Allow incoming calls (Eingehende Anrufe erlauben)** anklicken.
3. Legen Sie unter **Call handling (Anrufbehandlung)** die Zeitüberschreitung und Dauer des Anrufs fest.
4. Geben Sie unter **Ports** die Portnummern ein.
   - **SIP port (SIP-Port)** – Der für die SIP-Kommunikation genutzte Netzwerk-Port. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Der Standardport ist 5060. Geben Sie eine andere Portnummer ein, falls erforderlich.
   - **TLS port (TLS-Port)** – Der für verschlüsselte SIP-Kommunikation genutzte Netzwerk-Port. 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 start port** – Den Port für den ersten RTP-Mediastream eines SIP-Anrufs eingeben. Der Standard-Startport für die Medienübertragung ist 4000. Einige Firewalls blockieren ggf. den RTP-Datenaustausch über bestimmte Portnummern. Eine Portnummer muss zwischen 1024 und 65535 liegen.

5. Wählen Sie unter **NAT Traversal** die Protokolle, die für NAT Traversal aktiviert werden sollen.

Hinweis

NAT Traversal verwenden, wenn das Axis Gerät über einen NAT-Router oder eine Firewall mit dem Netzwerk verbunden ist. Weitere Informationen finden Sie unter .

6. Wählen Sie unter **Audio** mindestens einen Audiocodec mit der für SIP-Anrufe gewünschten Audioqualität. Ändern Sie die Prioritätsreihenfolge per Drag & Drop.
7. Wählen Sie unter **Additional (Erweitert)** weitere Optionen aus.
   - **UDP-to-TCP switching (Zwischen UDP und TCP wechseln)** – 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.
   - **Allow via rewrite (Umschreiben erlauben)** – Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
   - **Allow via rewrite (Umschreiben des Kontakts erlauben)** – Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
   - **Register with server every (Häufigkeit der Registrierung am Server)** – Legen Sie fest, wie oft sich das Gerät beim SIP-Server für die vorhandenen SIP-Konten registrieren soll.
   - **DTMF payload type (DTMF-Nutzlasttyp)** – Ändert den Standard-Nutzlasttyp für DTMF.
8. **Save (Speichern)** anklicken.

SIP über einen Server (PBX) einrichten

Verwenden Sie einen PBX-Server, wenn Benutzeragenten innerhalb und außerhalb des IP-Netzwerks kommunizieren sollen. Je nach PBX-Anbieter können dem Setup zusätzliche Funktionen hinzugefügt werden. Weitere Informationen zur Funktionsweise von P2P finden Sie unter .

Weitere Informationen zu den SIP-Einstellungsoptionen finden Sie unter *SIP, on page 61*.

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:

- Benutzer-ID
- Domäne
- Kennwort
- Authentifizierungs-ID
- Anrufer-ID
- Registrator
- RTP-Startport

2. Um ein neues Konto hinzuzufügen, wechseln Sie zu **System** > **SIP** > **SIP accounts (SIP-Konten)** und klicken Sie auf **+ Account (+ Konto)**.
3. Geben Sie die von Ihrem PBX-Anbieter erhaltenen Informationen ein.
4. Wählen Sie **Registered (Registriert)** aus.
5. Transportmodus auswählen.
6. **Save (Speichern)** anklicken.
7. Die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einrichten. Weitere Informationen siehe *Direktes SIP (P2P) einrichten, on page 10*.

Einrichten von Regeln für Ereignisse

Weitere Informationen finden Sie unter *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** bei erfüllten Bedingungen durchgeführt werden soll.

Hinweis

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

Video aufzeichnen, wenn Vaping detektiert wird

Das folgende Beispiel erklärt, wie Sie einen Luftqualitätssensor so einstellen, dass er Videos im Netzwerk-Speicher aufzeichnet, wenn der Luftqualitätssensor Vaping detektiert.

1. Gehen Sie auf der Webseite des Luftqualitätssensors zu **Settings (Einstellungen) > System > Storage (Speicher)**, um zu überprüfen, ob der Netzwerk-Speicher eingerichtet ist.
2. Gehen Sie auf **Settings > System > Events (Einstellungen > System > Ereignisse)** und fügen Sie eine Regel hinzu. Geben Sie folgende Informationen ein:
   - **Name**: Geben Sie einen Namen für die Regel ein.
   - **Condition (Bedingung)**: **Air quality monitor (Luftqualitätsmonitor) > Vaping or smoking detected (Rauchen oder Vapen erkannt)**.
   - **Action (Aktion)** : **Recordings (Aufzeichnungen) > Record video (Video aufzeichnen)**.
   - **Speicher: Network storage (Netzwerk-Speicher)**. Stellen Sie sicher, dass der Netzwerk-Speicher eingereichtet ist.
   - **Kamera**: Wählen Sie einen Ansichtsbereich für die Kamera aus.
   - **Stream profile (Streamprofil)**: Wählen Sie ein Videostreamprofil aus oder **Create a stream profile (Erstellen Sie ein Videostreamprofil)**.
   - **Vorpuffer** und **Nachpuffer**: Stellen Sie die gewünschten Werte ein.
3. **Save (Speichern)** anklicken.

Audio-Clip abspielen, wenn CO2-Wert zu hoch ist

Dieses Beispiel erklärt, wie Audio abgespielt wird, wenn der CO2-Gehalt zu hoch ist.

Eine Regel erstellen

1. Rufen Sie auf der Webseite **Events (Ereignisse)** > **Rules (Regeln)** > **Add a rule (Eine Regel hinzufügen)** auf, um eine Regel zu erstellen.
2. Geben Sie folgende Informationen ein:
   - **Name**: Geben Sie einen Namen für die Regel ein.
   - **Bedingungen**: **Air quality monitor (Luftqualitätsmonitor)** > **Air quality outside acceptable range (Luftqualität außerhalb des zulässigen Bereichs)**
   - **Sensor**: **CO2**
   - **Aktion**: **Wiedergabe von Audioclips**

- **Clip**: Wählen Sie einen Audioclip aus.

3. **Save (Speichern)** anklicken.

Einrichten des Alarmbereichs für CO2

- Rufen Sie auf der Webseite **Air quality monitor (Luftqualitätsmonitor)** > **Settings (Einstellungen)** > **CO2** auf.
- Geben Sie die **MIN** und **MAX** Daten ein, um den CO2-Bereich einzustellen.

Aktivieren Sie ein Licht- und Sirenenprofil über den externen Bewegungsmelder (PIR-Sensor).

Dieses Beispiel erklärt, wie Sie ein Licht- und Sirenenprofil über einen externen Bewegungsmelder (PIR-Sensor) aktivieren können. Die Positionen der Leuchten (Signal-LEDs) und der Sirene finden Sie unter *Produktübersicht, on page 76*.

Erstellen Sie ein Licht- und Sirenenprofil:

1. Gehen Sie auf der Webseite des Geräts zu **Profiles (Profile) > Create (Erstellen)**.
2. Geben Sie folgende Informationen ein:
   - **Name**: Profil 1
   - **Beschreibung**: Fügen Sie die Profilbeschreibung hinzu.
   - **Light (Licht)**: Wählen Sie **Pattern (Muster)**, **Speed (Geschwindigkeit)**, **Intensity (Intensität)**, **Color (Farbe)** und **Duration (Dauer)**.
   - **Siren (Sirene)**: Wählen Sie **Pattern (Muster)**, **Intensity (Intensität)** und **Duration (Dauer)**.

   Hinweis

   Profile mit höheren Zahlen haben eine höhere Priorität.
   - **Priority (Priorität)**: Wählen Sie **Light priority (Lichtpriorität)** und **Siren priority (Sirenenpriorität)**.

Erstellen Sie ein Ereignis:

1. Gehen Sie auf **System** > **Events (Ereignisse)** > **Rules (Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Signal-LEDs und Sirene aktivieren
   - **Condition (Bedingung)**: Externer Bewegungsmelder (PIR-Sensor)
   - **Aktion**: Licht- und Sirenenprofil ausführen
   - **Profile (Profil)**: Profil 1
   - **Aktion**: Starten
3. **Save (Speichern)** anklicken.

Profil starten, wenn ein Alarm ausgelöst wird

In diesem Beispiel wird erklärt, wie ein Alarm ausgelöst wird, wenn das digitale Eingangssignal geändert wurde.

Die Eingangsrichtung für den Port festlegen:

1. Gehen Sie zu **System** > **Zubehör** > **E/A-Ports**.
2. Gehen Sie zu **Port 1** > **Normal state (Normalzustand)** und klicken Sie auf **Circuit closed (Schaltkreis geschlossen)**.

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen **I/O** > **Digital input is active (Digitaler Eingang ist aktiv)**.

4. Wählen Sie **Port 1**:
5. Wählen Sie in der Liste mit den Aktionen **Run light and siren profile while the rule is active (Bei aktiver Regel Licht- und Sirenenprofil ausführen)**.
6. Wählen Sie das Videostreamprofil aus, das Sie starten möchten.
7. **Save (Speichern)** anklicken.

Profil über SIP starten

In diesem Beispiel wird erläutert, wie Sie einen Alarm über SIP auslösen.

SIP aktivieren:

1. Gehen Sie zu **System** > **SIP** > **SIP settings (SIP-Einstellungen**.
2. Wählen Sie **SIP aktivieren** und **Eingehende Anrufe zulassen**.
3. **Save (Speichern)** anklicken.

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen **Anruf** > **Status**.
4. Wählen Sie in der Statusliste **Aktiv**.
5. Wählen Sie in der Liste mit den Aktionen **Run light and siren profile while the rule is active (Bei aktiver Regel Licht- und Sirenenprofil ausführen)**.
6. Wählen Sie das Videostreamprofil aus, das Sie starten möchten.
7. **Save (Speichern)** anklicken.

Mehrere Profile über SIP-Erweiterungen steuern

SIP aktivieren:

1. Gehen Sie zu **System** > **SIP** > **SIP settings (SIP-Einstellungen**.
2. Wählen Sie **SIP aktivieren** und **Eingehende Anrufe zulassen**.
3. **Save (Speichern)** anklicken.

Erstellen Sie eine Regel zum Starten eines Profils:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Bedingung **Call** > **State change** (Anruf > Statusänderung) aus.
4. Wählen Sie in der Ursachenliste den Grund **Accepted by device (Per Gerät akzeptiert)**.
5. Wählen Sie unter **Call direction (Anrufrichtung)** die Option **Incoming (Eingehend)**.
6. Geben Sie für **Local SIP URI <sip:[Ext]@[IP address]>** ein, wobei [Ext] die für das Profil verwendete Erweiterung und [IP address] die IP-Adresse des Geräts ist. Beispiel: **sip:1001@192.168.0.90**.
7. Wählen Sie in der Aktionsliste **Light and Siren (Licht und Sirene)** > **Run light and siren profile (Licht- und Sirenenprofil ausführen)** aus.
8. Wählen Sie das Videostreamprofil aus, das Sie starten möchten.
9. Wählen Sie die Aktion **Start (Starten)** aus.
10. **Save (Speichern)** anklicken.

Erstellen Sie eine Regel zum Stoppen eines Profils:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Bedingung **Call** > **State change** (Anruf > Statusänderung) aus.
4. Wählen Sie in der Ursachenliste den Grund **Terminated (Beendet)** aus.
5. Wählen Sie unter **Call direction (Anrufrichtung)** die Option **Incoming (Eingehend)**.
6. Geben Sie für **Local SIP URI** die Anweisung **sip:[Ext]@[IP address]** ein, wobei [Ext] die für das Profil verwendete Erweiterung und [IP adress] die IP-Adresse des Geräts ist. Beispiel: **sip:1001@192.168.0.90**.
7. Wählen Sie in der Aktionsliste **Light and Siren (Licht und Sirene)** > **Run light and siren profile (Licht- und Sirenenprofil ausführen)** aus.
8. Wählen Sie das Profil aus, das Sie stoppen möchten.
9. Wählen Sie die Aktion **Stop (Stoppen)** aus.
10. **Save (Speichern)** anklicken.

Wiederholen Sie für jedes Profil, das Sie über SIP steuern möchten, die Schritte zur Erstellung von Start- und Stoppregeln.

Zwei Profile mit unterschiedlichen Prioritäten ausführen

Wenn Sie zwei Profile mit unterschiedlichen Prioritäten ausführen, unterbricht das Profil mit einer höheren Prioritätszahl das Profil mit einer niedrigeren Prioritätszahl.

Hinweis

Wenn Sie zwei Profile mit der gleichen Priorität ausführen, bricht das letzte Profil das vorherige ab.

In diesem Beispiel wird erläutert, wie das Gerät so eingerichtet wird, dass ein Profil mit Priorität 4 vor einem anderen Profil mit Priorität 3 angezeigt wird, wenn es durch den digitalen E/A-Anschluss ausgelöst wird.

Profile erstellen:

1. Erstellen Sie ein Profil mit Priorität 3.
2. Erstellen Sie ein anderes Profil mit Priorität 4.

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen **I/O** > **Digital input is active (Digitaler Eingang ist aktiv)**.
4. Wählen Sie einen Port.
5. Wählen Sie in der Liste mit den Aktionen **Run light and siren profile while the rule is active (Bei aktiver Regel Licht- und Sirenenprofil ausführen)**.
6. Wählen Sie das Profil mit der höchsten Prioritätszahl aus.
7. **Save (Speichern)** anklicken.
8. Gehen Sie zu **Profile** und starten Sie das Profil mit der niedrigsten Prioritätszahl.

Aktivieren Sie ein Licht- und Sirenenprofil über HTTP Post, wenn eine Kamera ein Bewegungsmuster erkennt.

Dieses Beispiel erklärt, wie Sie eine Kamera an den Luftqualitätssensor anschließen und ein Licht- und Sirenenprofil im Luftqualitätssensor aktivieren können, sobald die Anwendung AXIS Motion Guard, installiert in der Kamera, ein Bewegungsmuster erkennt.

Vorbereitungen:

- Erstellen Sie im Luftqualitätssensor einen neuen Benutzer mit der Rolle „Bediener" oder „Administrator".

- Erstellen Sie im Luftqualitätssensor ein Profil mit dem Namen „Licht- und Sirenenprofil".
- Richten Sie AXIS Motion Guard in der Kamera ein und erstellen Sie ein Profil mit dem Namen „Camera profile" (Kameraprofil).
- Stellen Sie sicher, dass AXIS Device Assistant mit Firmware-Version 10.8.0 oder höher verwendet wird.

Erstellen eines Empfängers in der Kamera:

1. Rufen Sie in der Geräteschnittstelle der Kamera **System > Events > Recipients (System > Ereignisse > Empfänger)** auf und fügen Sie einen Empfänger hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Luftqualitätssensor
   - **Typ**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi
     Ersetzen Sie <IPadresse> durch die Adresse des Luftqualitätssensors.
   - Benutzername und Kennwort des neu erstellten Benutzers des Luftqualitätssensors.
3. Klicken Sie **Test (Testen)** an, um sicherzustellen, dass alle Daten gültig sind.
4. **Save (Speichern)** anklicken.

Erstellen Sie in der Kamera zwei Regeln:

1. **Rules (Regeln)** aufrufen und eine Regel hinzufügen.
2. Geben Sie folgende Informationen ein:
   - **Name**: Luftqualitätssensor mit Bewegung aktivieren
   - **Condition (Bedingung)**: **Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - **Aktion**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
   - **Recipient (Empfänger)**: **Luftqualitätssensor.**
     Die Informationen müssen mit den zuvor unter **Events > Recipients > Name (Ereignisse > Empfänger > Name)** eingegebenen Informationen übereinstimmen.
   - **Method (Methode)**: **Post**
   - **Body (Text)**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Light and siren profile"  } }
```

Vergewissern Sie sich, dass Sie unter „**Profile (Profil) : <>**" die gleichen Informationen eingeben, wie Sie sie beim Erstellen des Profils im Luftqualitätssensor eingegeben haben, in diesem Fall: „Licht- und Sirenenprofil".

3. **Save (Speichern)** anklicken.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
   - **Name**: Luftqualitätssensor mit Bewegung deaktivieren
   - **Condition (Bedingung)**: **Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - Wählen Sie **Diese Bedingung umkehren.**
   - **Aktion**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
   - **Recipient (Empfänger)**: **Luftqualitätssensor**
     Die Informationen müssen mit den zuvor unter **Events > Recipients > Name (Ereignisse > Empfänger > Name)** eingegebenen Informationen übereinstimmen.
   - **Method (Methode)**: **Post**
   - **Body (Text)**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Light and siren
profile"  } }
```

Vergewissern Sie sich, dass Sie unter „**Profile (Profil) : <>**“ die gleichen Informationen eingeben, wie Sie sie beim Erstellen des Profils im Luftqualitätssensor eingegeben haben, in diesem Fall: „Licht- und Sirenenprofil“.

5. **Save (Speichern)** anklicken.

Aktivieren Sie ein Licht- und Sirenenprofil über einen virtuellen Eingang, wenn eine Kamera ein Bewegungsmuster erkennt.

Dieses Beispiel erklärt, wie Sie eine Kamera an den Luftqualitätssensor anschließen und ein Licht- und Sirenenprofil im Luftqualitätssensor aktivieren können, sobald die Anwendung AXIS Motion Guard, installiert in der Kamera, ein Bewegungsmuster erkennt.

Vorbereitungen:

- Erstellen Sie im Luftqualitätssensor ein neues Konto mit Bediener- oder Administratorrechten.
- Erstellen Sie ein Profil im Luftqualitätssensor. Siehe *Profile, on page 35*.
- Richten Sie AXIS Motion Guard in der Kamera ein und erstellen Sie ein Profil mit dem Namen „Kameraprofil“.

Erstellen Sie in der Kamera zwei Empfänger:

1. Rufen Sie in der Geräteschnittstelle der Kamera **System > Events > Recipients (System > Ereignisse > Empfänger)** auf und fügen Sie einen Empfänger hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Virtuellen Port aktivieren
   - **Typ**: **HTTP**
   - **URL**: http://<IP-Adresse>/axis-cgi/virtualinput/activate.cgi
     Ersetzen Sie <IPadresse> durch die Adresse des Luftqualitätssensors.
   - Konto und Kennwort des neu erstellten Kontos des Luftqualitätssensors.
3. Klicken Sie **Test (Testen)** an, um sicherzustellen, dass alle Daten gültig sind.
4. **Save (Speichern)** anklicken.
5. Fügen Sie einen zweiten Empfänger mit den folgenden Informationen hinzu:
   - **Name**: Virtuellen Port deaktivieren
   - **Typ**: **HTTP**
   - **URL**: http://<IP-Adresse>/axis-cgi/virtualinput/deactivate.cgi
     Ersetzen Sie <IPadresse> durch die Adresse des Luftqualitätssensors.
   - Konto und Kennwort des neu erstellten Kontos des Luftqualitätssensors.
6. Klicken Sie **Test (Testen)** an, um sicherzustellen, dass alle Daten gültig sind.
7. **Save (Speichern)** anklicken.

Erstellen Sie in der Kamera zwei Regeln:

1. **Rules (Regeln)** aufrufen und eine Regel hinzufügen.
2. Geben Sie folgende Informationen ein:
   - **Name**: Virtuellen E/A1 aktivieren
   - **Condition (Bedingung)**: **Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - **Aktion**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
   - **Empfänger**: **Virtuellen Port aktivieren**
   - **Suffix der Abfragezeichenfolge**: schemaversion=1&port=1
3. **Save (Speichern)** anklicken.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
   - **Name**: Virtuellen E/A1 deaktivieren

- **Condition (Bedingung)**: **Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
- Wählen Sie **Diese Bedingung umkehren**.
- **Aktion**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
- **Empfänger**: **Virtuellen Port deaktivieren**
- **Suffix der Abfragezeichenfolge**: schemaversion=1&port=1

5. **Save (Speichern)** anklicken.

Erstellen Sie eine Regel im Luftqualitätssensor:

1. Wechseln Sie in der Weboberfläche des Luftqualitätssensors zu **System > Events (Ereignisse)**, und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Auslöser am virtuellen Eingang 1
   - **Condition (Bedingung)**: **I/O (E/A) > Virtual input is active (Virtual input is active)**
   - **Port**: **1**
   - **Aktion**: **Licht und Sirene > Bei aktiver Regel Licht- und Sirenenprofil ausführen**
   - **Profile (Profil)**: Wählen Sie das neu erstellte Profil
3. **Save (Speichern)** anklicken.

Aktivieren Sie ein Licht- und Sirenenprofil über MQTT, wenn eine Kamera ein Bewegungsmuster erkennt.

Dieses Beispiel erklärt, wie Sie eine Kamera an den Luftqualitätssensor anschließen und ein Licht- und Sirenenprofil im Luftqualitätssensor aktivieren können, sobald die Kamera ein Bewegungsmuster erkennt.

Vorbereitungen:

- Erstellen Sie ein Profil im Luftqualitätssensor.
- Richten Sie einen MQTT-Broker ein und rufen Sie die IP-Adresse, den Benutzernamen und das Kennwort des Brokers ab.
- Stellen Sie sicher, dass die Anwendung für die Bewegungserfassung konfiguriert ist und auf der Kamera ausgeführt wird.

Richten Sie den MQTT-Client in der Kamera ein:

1. Gehen Sie in der Weboberfläche der Kamera zu **System > MQTT > MQTT Client > Broker** und geben Sie folgende Informationen ein:
   - **Host**: IP-Adresse des Brokers
   - **Client-ID**: Zum Beispiel Kamera 1
   - **Protocol (Protokoll)**: Das Protokoll, auf das der Broker festgelegt ist
   - **Port**: Die vom Broker verwendete Portnummer
   - **Benutzername** und **Kennwort** des Brokers
2. Klicken Sie auf **Gehe zu** und **Verbinden**.

Erstellen Sie in der Kamera zwei Regeln für die Veröffentlichung über MQTT:

1. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Bewegung erkannt
   - **Condition (Bedingung)**: **Anwendungen > Motion Alarm**
   - **Aktion**: **MQTT > Send MQTT publish message (MQTT-Meldung zu Veröffentlichung senden)**
   - **Topic (Thema)**: Bewegung

- **Nutzlast**: Ein
- **QoS**: 0, 1 oder 2

3. **Save (Speichern)** anklicken.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
   - **Name**: Keine Bewegung
   - **Condition (Bedingung)**: **Anwendungen > Motion Alarm**
     - Wählen Sie **Diese Bedingung umkehren.**
   - **Aktion**: **MQTT > Send MQTT publish message (MQTT-Meldung zu Veröffentlichung senden)**
   - **Topic (Thema)**: Bewegung
   - **Nutzlast**: Aus
   - **QoS**: 0, 1 oder 2
5. **Save (Speichern)** anklicken.

Richten Sie den MQTT-Client im Luftqualitätssensor ein:

1. Gehen Sie in der Weboberfläche des Luftqualitätssensors zu **System > MQTT > MQTT Client > Broker** und geben Sie folgende Informationen ein:
   - **Host**: IP-Adresse des Brokers
   - **Client-ID**: Sirene 1
   - **Protocol (Protokoll)**: Das Protokoll, auf das der Broker festgelegt ist
   - **Port**: Die vom Broker verwendete Portnummer
   - **Benutzername** und **Kennwort**
2. Klicken Sie auf **Gehe zu** und **Verbinden.**
3. Gehen Sie zu **MQTT-Abonnements** und fügen Sie ein Abonnement hinzu.
   Geben Sie folgende Informationen ein:
   - **Abonnementfilter**: Bewegung
   - **Abonnementart**: Statusbehaftet
   - **QoS**: 0, 1 oder 2
4. **Save (Speichern)** anklicken.

Erstellen Sie eine Regel im Luftqualitätssensor für MQTT-Abonnements:

1. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Bewegung erkannt
   - **Condition (Bedingung)**: **MQTT > Stateful (Statusbehaftet)**
   - **Abonnementfilter**: **Bewegung**
   - **Nutzlast**: Ein
   - **Aktion**: **Licht und Sirene > Bei aktiver Regel Licht- und Sirenenprofil ausführen**
   - **Profile (Profil)**: Wählen Sie das Profil aus, das aktiv sein soll.
3. **Save (Speichern)** anklicken.

Senden einer E-Mail, wenn ein Lautsprechertest fehlschlägt

In diesem Beispiel wird das Audiogerät so konfiguriert, dass eine E-Mail an einen definierten Empfänger gesendet wird, wenn ein Lautsprechertest fehlschlägt. Der Lautsprechertest ist so konfiguriert, dass er täglich um 18 Uhr ausgeführt wird.

1. Einen Zeitplan für den Lautsprechertest erstellen:
   1.1. Gehen Sie zu Geräteschnittstelle > **System** > **Events (Ereignisse)** > **Schedules (Zeitpläne)**.

1.2. Erstellen Sie einen Zeitplan, der täglich um 18 Uhr beginnt und um 18:01 Uhr endet. Nennen Sie ihn „Täglich um 18 Uhr"

2. Einen E-Mail-Empfänger erstellen:
   2.1. Wechseln Sie zu Geräteschnittstelle > **System** > **Events (Ereignisse)** > **Recipients (Empfänger)**.
   2.2. Klicken Sie auf **Add recipient (Empfänger hinzufügen)**.
   2.3. Nennen Sie den Empfänger „Lautsprechertest-Empfänger
   2.4. Wählen Sie unter **Typ** die Option **Email (E-Mail)**.
   2.5. Geben Sie unter **Send email to (E-Mail senden)** die E-Mail-Adressen der Empfänger ein. Trennen Sie mehrere Adressen mit Kommas.
   2.6. Geben Sie die Details für das E-Mail-Konto des Absenders ein.
   2.7. Klicken Sie auf **Test**, um eine Test-E-Mail zu senden.

   Hinweis

   Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, zeitgeplante E-Mails erhalten und anderes. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, um Sendeprobleme und gesperrte E-Mail-Konten zu vermeiden.

   2.8. **Save (Speichern)** anklicken.

3. Einen automatischen Lautsprechertest einrichten:
   3.1. Wechseln Sie zu Geräteschnittstelle > **System** > **Events (Ereignisse)** > **Rules (Regeln)**.
   3.2. Klicken Sie auf **Add a rule (Regel hinzufügen)**:
   3.3. Geben Sie einen Namen für die Regel ein.
   3.4. Wählen Sie unter **Condition (Bedingung)** die Option **Schedule (Zeitplan)** und einen Eintrag in der Auslöseliste.
   3.5. Wählen Sie unter **Schedule (Zeitplan)** Ihren Zeitplan aus („Täglich um 18 Uhr").
   3.6. Wählen Sie unter **Action (Aktion)** die Option **Run automatic speaker test (Automatischen Lautsprechertest ausführen)**.
   3.7. **Save (Speichern)** anklicken.

4. Legen Sie die Bedingung für das Senden einer E-Mail fest, wenn der Lautsprechertest fehlschlägt:
   4.1. Wechseln Sie zu Geräteschnittstelle > **System** > **Events (Ereignisse)** > **Rules (Regeln)**.
   4.2. Klicken Sie auf **Add a rule (Regel hinzufügen)**:
   4.3. Geben Sie einen Namen für die Regel ein.
   4.4. Wählen Sie unter **Condition (Bedingung)** die Option **Speaker test result (Lautsprechertestergebnis)**.
   4.5. Wählen Sie unter **Speaker test status (Lautsprechertestst atus)**die Option **Didn't pass the test (Test nicht bestanden)**.
   4.6. Wählen Sie unter **Aktion** die Option **Send notification to email (Benachrichtigung per E-Mail senden**.
   4.7. Wählen Sie unter **Recipient (Empfänger)** Ihren Empfänger aus („Empfänger des Lautsprechertests")
   4.8. Einen Betreff und eine Nachricht eingeben und auf **Speichern** klicken.

Bei Auslösen eines Alarms benutzerdefinierten Clip wiedergeben

In diesem Beispiel wird erläutert, wie Sie die Wiedergabe einer benutzerdefinierten Audiodatei auslösen lassen können, wenn sich das digitale Eingangssignal ändert.

Eine Audiodatei hochladen:

1. Wechseln Sie zu **Media (Medien)** und klicken Sie dann auf **Add (Hinzufügen)**.
2. Klicken Sie auf „Browse" (Durchsuchen), um die Audiodatei auf Ihrem Computer zu suchen und auszuwählen.
3. Gehen Sie auf **Storage location (Speicherort)**.
4. **Save (Speichern)** anklicken.

Erstellen Sie ein Profil mit der Audiodatei:

1. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf **Create (Anlegen)**.
2. Geben Sie unter **Name** einen Namen ein und wählen Sie ein Lichtmuster für das Profil.
3. Wählen Sie im Abschnitt „Sirene" (Sirene) die hochgeladene Audiodatei aus.
4. Legen Sie Werte für **Intensity (Intensität)** und **Duration (Dauer)** fest.
5. **Save (Speichern)** anklicken.

Die Eingangsrichtung für den Port festlegen:

1. Gehen Sie zu **System** > **Zubehör** > **E/A-Ports**.
2. Gehen Sie zu **Port 1** > **Normal state (Normalzustand)** und klicken Sie auf **Circuit closed (Schaltkreis geschlossen)**.

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen **I/O > Digital input is active (Digitaler Eingang ist aktiv)**.
4. Wählen Sie **Port 1**:
5. Wählen Sie in der Liste mit den Aktionen **Bei aktiver Regel Licht- und Sirenenprofil ausführen**.
6. Wählen Sie das Profil mit der hochgeladenen Audiodatei aus.
7. **Save (Speichern)** anklicken.

Audio mit DTMF anhalten

Dieses Beispiel erläutert, wie:

- DTMF auf einem Gerät konfiguriert werden kann.
- Ein Ereignis eingerichtet werden kann, um die Audiofunktion anzuhalten, wenn ein DTMF-Befehl an das Gerät gesendet wird.

1. Gehen Sie zu **System** > **SIP** > **SIP settings (SIP-Einstellungen**.
2. Stellen Sie sicher, dass **Enable SIP (SIP aktivieren)** eingeschaltet ist.
   Wenn Sie dies aktivieren müssen, klicken Sie anschließend auf **Speichern**.
3. Wechseln Sie zu **SIP accounts (SIP-Konten)**.
4. Klicken Sie neben dem SIP-Konto auf > **Edit (Bearbeiten)**.
5. Klicken Sie unter **DTMF** auf **+ DTMF sequence (+ DTMF-Sequenz)**.
6. Geben Sie unter **Sequence (Sequenz)** „1" ein.
7. Geben Sie unter **Description (Beschreibung)** „Audio anhalten" ein.
8. **Save (Speichern)** anklicken.
9. Wechseln Sie zu **System** > **Events (Ereignisse)** > **Rules (Regeln)** und klicken Sie auf **+ Add a rule (+ Regel hinzufügen)**.
10. Geben Sie unter **Name** „DTMF – Audio anhalten" ein.

11. Wählen Sie unter **Condition (Bedingung)** die Option **DTMF**.
12. Wählen Sie unter **DTMF Event ID (DTMF-Ereignis-ID)** die Option **stop audio (Audio anhalten)**.
13. Wählen Sie unter **Action (Aktion)** die Option **Stop playing audio clip (Audioclip anhalten)**.
14. **Save (Speichern)** anklicken.

Audio für eingehende SIP-Anrufe einrichten

Für eingehende SIP-Anrufe können Sie eine Regel erstellen, die einen bestimmten Audioclip abspielt.

Daneben können Sie zudem eine zusätzliche Regel zur automatischen Annahme des SIP-Anrufs nach Abspielen des Audioclips erstellen. Dies kann nützlich sein, um bei Bedarf andere Personen im Bereich eines Audiogeräts zu alarmieren und eine Kommunikationsverbindung zur Alarmzentrale herzustellen. Hierzu erfolgt ein SIP-Anruf an das jeweilige Audiogerät, das einen Audioclip abspielt, um die Personen seinem Einzugsbereich zu warnen. Nach Abspielen des Audioclips nimmt das Audiogerät den SIP-Anruf automatisch an und stellt eine Kommunikationsverbindung zwischen der Alarmzentrale und den Personen im Einzugsbereich des Audiogeräts her.

SIP-Einstellungen aktivieren:

1. Rufen Sie die Geräteschnittstelle des Lautsprechers auf, indem Sie seine IP-Adresse in einen Webbrowser eingeben.
2. Gehen Sie zu **System (System)** > **SIP (SIP)** > **SIP settings (SIP-Einstellungen)** und wählen Sie **Enable SIP (SIP aktivieren)** aus.
3. Um auf dem Axis Gerät eingehende Anrufe zu erlauben, **Allow incoming calls (Eingehende Anrufe erlauben)** anklicken.
4. Klicken Sie auf **Save (Speichern)**.
5. Wechseln Sie zu **SIP accounts (SIP-Konten)**.
6. Klicken Sie neben dem SIP-Konto auf ⋮ > **Edit (Bearbeiten)**.
7. Deaktivieren Sie die Option **Answer automatically (Automatische Annahme)**.

Audiowiedergabe bei eingehendem SIP-Anruf:

1. Gehen Sie auf **Settings > System > Events > Rules (Einstellungen > System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Option **State (Zustand)** aus.
4. Wählen Sie in der Zustandsliste die Option **Ringing (Klingelton)** aus.
5. Wählen Sie in der Liste der Aktionen **Play audio clip (Wiedergabe von Audioclips)** aus.
6. Wählen Sie aus der Liste der Audioclips den Clip aus, den Sie abspielen möchten.
7. Wählen Sie aus, wie oft der Audioclip abgespielt werden soll. „0" bedeutet „nur einmal".
8. Klicken Sie auf **Save (Speichern)**.

SIP-Anruf nach Abspielen des Audioclips automatisch annehmen:

1. Gehen Sie auf **Settings > System > Events > Rules (Einstellungen > System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Option **Audio clip playing (Audioclip abspielen)** aus.
4. Aktivieren Sie die Option **Use this condition as a trigger (Diese Bedingung als Auslöser verwenden).**
5. Aktivieren Sie die Option **Invert this condition (Diese Bedingung umkehren)**
6. Klicken Sie auf **+ Add a condition (+ Bedingung hinzufügen)**, um dem Ereignis eine zweite Bedingung hinzuzufügen.
7. Wählen Sie in der Bedingungsliste die Option **State (Zustand)** aus.

8. Wählen Sie in der Zustandsliste die Option **Ringing (Klingelton)** aus.
9. Wählen Sie in der Aktionsliste die Option **Answer call (Anruf annehmen)** aus.
10. Klicken Sie auf **Save (Speichern)**.

Weboberfläche

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

Status

Geräteinformationen

Zeigt Informationen zum Gerät 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.

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.

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.

Gerät lokalisieren

Zeigt die Gerätelokalisierungsinformationen an, einschließlich Seriennummer und IP-Adresse.

Locate device (Gerät lokalisieren): Spielt einen Ton ab, der Ihnen bei der Erkennung des Lautsprechers hilft. Bei einigen Produkten blinkt eine LED auf dem Gerät.

Energieverbrauch

Zeigt Informationen zum Strom an. Die Angaben variieren je nach Produkt.

Laufende Aufzeichnungen

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter *Aufzeichnungen, on page 37*

Anzeige des Speicherorts der Aufzeichnung.

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

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.

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.

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.

Luftqualitätssensor

Dashboard

Echtzeit-Sensordaten

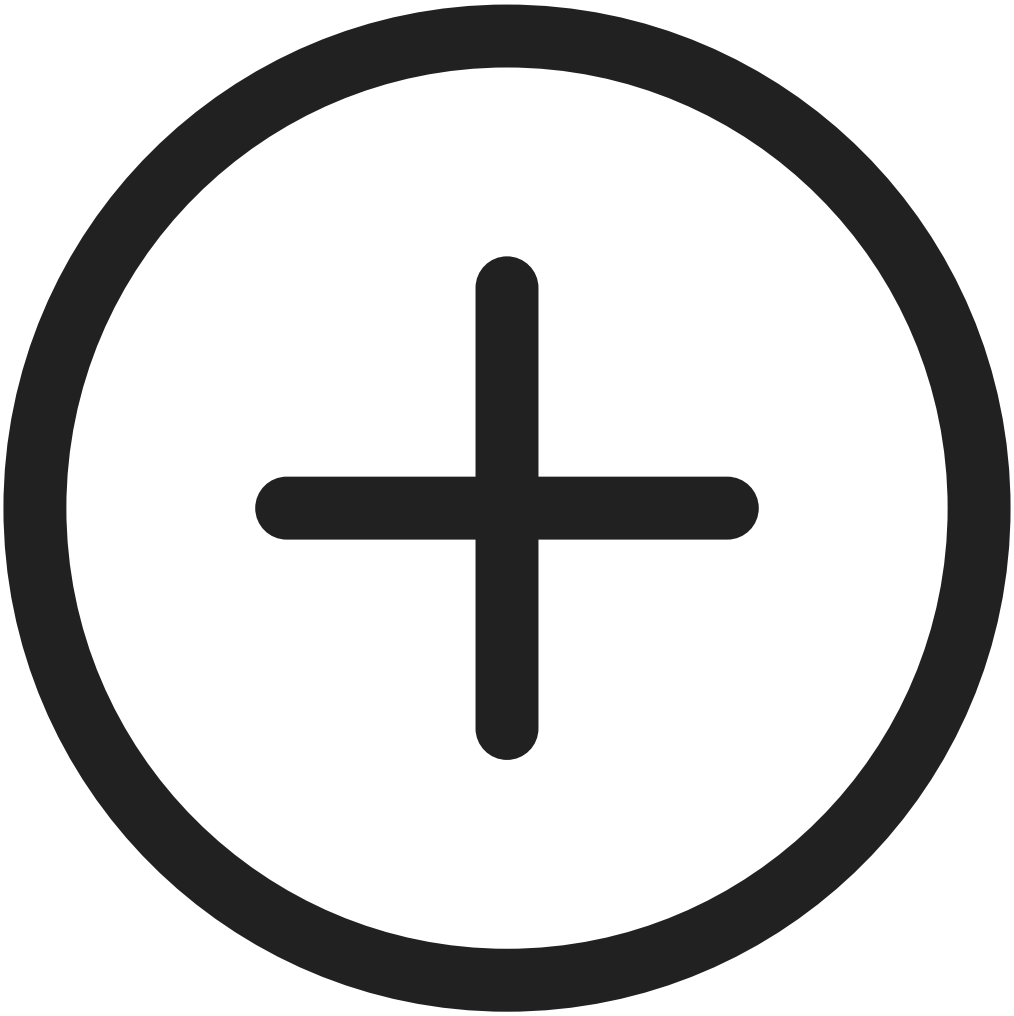
Zeigt die Sensordaten in Echtzeit an.

Hinweis

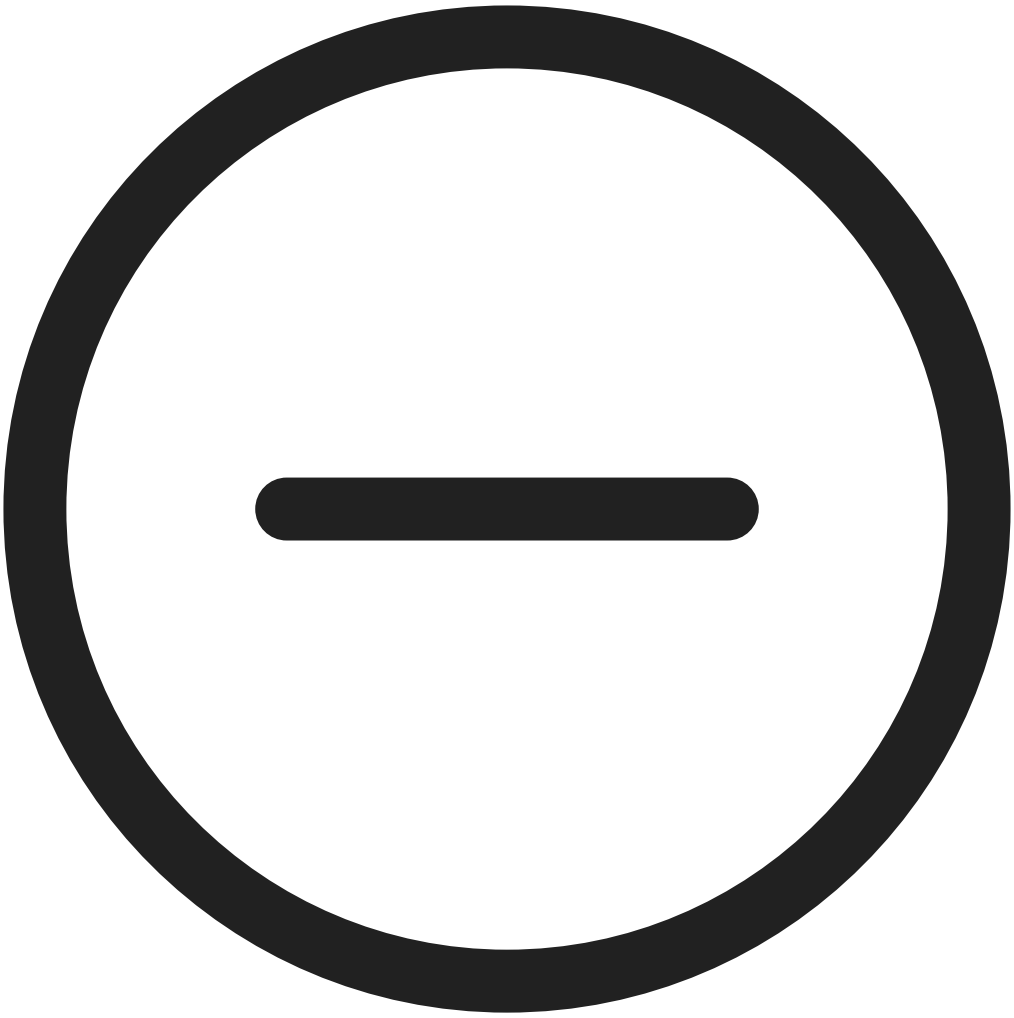
- Die volle CO2-Genauigkeit wird bei Erstbetrieb des Geräts erst nach 2 Tagen erreicht.
- Der AQI (Air Quality Index) benötigt bei der ersten Inbetriebnahme des Geräts 12 Stunden, um funktionsfähig zu werden. Der AQI-Wert zeigt **Calculating (wird berechnet)** an, bis genügend Daten vorliegen. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.
- Die volle Genauigkeit des VOC-Wertes erreicht das Gerät nach einer Betriebsstunde. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.
- Die volle Genauigkeit des NOx-Wertes erreicht das Gerät nach sechs Betriebsstunden. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.

: Anklicken, um den Namen des Dashboards festzulegen.

Edit (Bearbeiten): Klicken Sie hier, um die Daten anzuzeigen oder auszublenden.



: Klicken Sie hier, um Daten zum Dashboard hinzuzufügen.



: Klicken Sie hier, um Daten aus dem Dashboard zu entfernen.

Temperatur: Ansicht der Echtzeit-Temperatur des Luftqualitätssensors.

Luftfeuchtigkeit: Ansicht der Echtzeit-Feuchtigkeit vom Luftqualitätssensor.

CO2: Ansicht des Echtzeit-Kohlendioxids.

Die Farbbedeutungen der CO2-Statusbalken sind folgende:

- **Grün (0–1000)**: **gut**. Die Daten werden als zufriedenstellend angesehen.
- **Orange (1001–2000)**: **ungesund für empfindliche Personengruppe**. Bei Mitgliedern empfindlicher Personengruppen können gesundheitliche Auswirkungen auftreten. Die breite Öffentlichkeit ist weniger wahrscheinlich betroffen.
- **Rot (2001–5000)**: **ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Violett (5001–40000)**: **sehr ungesund**. Gesundheitswarnungen vor Notfällen. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.

NOx: Ansicht der Stickstoffoxide und Stickstoffdioxide in Echtzeit.

Die Farbbedeutungen der NOx-Statusbalken sind folgende:

- **Grün (0–30): gut**. Die Daten werden als zufriedenstellend angesehen.
- **Gelb (31–150): Mäßig**. Die Daten sind akzeptabel. Bei einer sehr kleinen Anzahl von Menschen, die ungewöhnlich empfindlich sind, kann ein mäßiges Gesundheitsrisiko bestehen.
- **Orange (151–300): ungesund für empfindliche Personengruppe**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Rot (301–500): ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.

PM 1.0: Echtzeitansicht Feinstaub 1.0.

PM 2.5: Echtzeitansicht Feinstaub 2.5.

Die Farbbedeutungen der PM 2.5-Statusbalken sind folgende:

- **Grün (0–9): gut**. Die Daten werden als zufriedenstellend angesehen.
- **Gelb (9,1–35,4): Mäßig**. Die Daten sind akzeptabel. Bei einer sehr kleinen Anzahl von Menschen, die ungewöhnlich empfindlich sind, kann ein mäßiges Gesundheitsrisiko bestehen.
- **Orange (35,5–55,4): ungesund für empfindliche Personengruppe**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Rot (55,5–125,4): ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Violett (125,5–225,4): sehr ungesund**. Gesundheitswarnungen vor Notfällen. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.
- **Kastanienbraun (225.5–1000): gefährlich**. Notfälle. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.

PM 4.0: Echtzeitansicht Feinstaub 4.0.

PM 10.0: Echtzeitansicht Feinstaub 10.0.

Die Farbbedeutungen der PM 10.0-Statusbalken sind folgende:

- **Grün (0–54): gut**. Die Daten werden als zufriedenstellend angesehen.
- **Gelb (55–154): mäßig**. Die Daten sind akzeptabel. Bei einer sehr kleinen Anzahl von Menschen, die ungewöhnlich empfindlich sind, kann ein mäßiges Gesundheitsrisiko bestehen.
- **Orange (155–254): ungesund für empfindliche Personengruppe**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Rot (255–354): ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Violett (355–424): sehr ungesund**. Gesundheitswarnungen vor Notfällen. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.
- **Kastanienbraun (425–1000): gefährlich**. Notfälle. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.

Vapen/Rauchen: Ansicht des detektierten oder nicht detektierten Vapens oder Rauchens.

Die Farbbedeutungen der Statusbalken für Vapen/Rauchen sind folgende:

- **Grün: Nicht detektiert**. Die vermutete Vaping- oder Raucheraktivität wird nicht detektiert.
- **Rot: Detektiert**. Die vermutete Vaping- oder Raucheraktivität wird detektiert.

VOC: Ansicht des Index flüchtiger organischer Verbindungen.

Die Farbbedeutungen der VOC-Statusbalken sind folgende:

- **Grün (0–200): gut**. Die Daten werden als zufriedenstellend angesehen.
- **Gelb (201–300): mäßig**. Die Daten sind akzeptabel. Bei einer sehr kleinen Anzahl von Menschen, die ungewöhnlich empfindlich sind, kann ein mäßiges Gesundheitsrisiko bestehen.
- **Orange (301–400): ungesund für empfindliche Personengruppe**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Rot (401–500): ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.

AQI: Ansicht des Luftqualitätsindex.

Die Farbbedeutungen der Statusbalken des Luftqualitätsindex sind folgende:

- **Grün (0–50): gut**. Die Daten werden als zufriedenstellend angesehen.
- **Gelb (51–100): mäßig**. Die Daten sind akzeptabel. Bei einer sehr kleinen Anzahl von Menschen, die ungewöhnlich empfindlich sind, kann ein mäßiges Gesundheitsrisiko bestehen.
- **Orange (101–150): ungesund für empfindliche Personengruppe**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Rot (151–200): ungesund**. Bei allen Menschen können erste gesundheitliche Auswirkungen auftreten; bei Mitgliedern empfindlicher Gruppen können schwerwiegendere gesundheitliche Auswirkungen auftreten.
- **Violett (201–300): sehr ungesund**. Gesundheitswarnungen vor Notfällen. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.
- **Kastanienbraun (301–500): gefährlich**. Notfälle. Die Wahrscheinlichkeit, dass die gesamte Bevölkerung betroffen ist, ist größer.

Einstellungen

Grenzwert

Richtet die Daten des Luftqualitätssensors ein.

Temperatur: Stellen Sie die Temperatur **MIN** und **MAX** innerhalb des Bereichs **–10 bis 45** ein.

Luftfeuchtigkeit : Stellen Sie die Luftfeuchtigkeit **MIN** und **MAX** innerhalb des Bereichs **0 bis 100** ein.

CO2 : Kohlendioxid **MIN** und **MAX** innerhalb des Bereichs **0 bis 40000** einstellen.

NOx : Stickstoffoxid und Stickstoffdioxid **MIN** und **MAX** innerhalb des Bereichs **0 bis 500** einstellen.

PM1.0 : Feinstaub 1.0 **MIN** und **MAX** innerhalb des Bereichs **0 bis 1000** einstellen.

PM2.5 : Feinstaub 2.5 **MIN** und **MAX** innerhalb des Bereichs **0 bis 1000** einstellen.

PM4.0 : Feinstaub 4.0 **MIN** und **MAX** innerhalb des Bereichs **0 bis 1000** einstellen.

PM10.0 : Feinstaub **MIN** und **MAX** innerhalb des Bereichs **0 bis 1000** einstellen.

VOC : Index flüchtiger organischer Verbindungen **MIN** und **MAX** innerhalb des Bereichs **0 bis 500** einstellen.

AQI : Luftqualitätsindex **MIN** und **MAX** innerhalb des Bereichs **0 bis 500** einstellen.

Temperatureinheiten

Temperatur anzeigen in: **Celsius** oder **Fahrenheit**

Vaping-Erfassungsempfindlichkeit

Richtet die Erfassungsempfindlichkeit für das Vapen ein.

Geringe Empfindlichkeit ,Hohe Empfindlichkeit: Verwenden Sie den Schieberegler, um den Unterschied zwischen niedriger und hoher Empfindlichkeit einzustellen, bei der das Gerät einen Alarm auslösen soll. Eine hohe Empfindlichkeit bedeutet, dass das Gerät selbst geringe Mengen an Rauch oder Dampf detektiert und eher als Auslöser für einen Alarm dient. Eine geringe Empfindlichkeit bedeutet, dass es nur auf größere Mengen an Rauch oder Dampf reagiert, wodurch die Wahrscheinlichkeit von Fehlalarmen verringert wird.

Speicher-Einstellung

- **Retention time 1 month, frequency 1s (Speicherdauer 1 Monat, Häufigkeit 1 Sekunde)**: Ihre Daten werden jede Sekunde erfasst und nur für die letzten 30 Tage gespeichert.
- **Retention time 3 month, frequency 5s (Speicherdauer 3 Monate, Häufigkeit 5 Sekunden)**: Ihre Daten werden alle 5 Sekunden erfasst und nur für die letzten 90 Tage gespeichert.
- **Retention time 1 year, frequency 10s (Speicherdauer 1 Jahr, Häufigkeit 10 Sekunden)**: Ihre Daten werden alle 10 Sekunden erfasst und nur für die letzten 365 Tage gespeichert.

Hinweis

Durch Ändern der Speicheroption werden vorhandene Daten gelöscht.

Häufigkeit von Cloud-Metadaten

Die Häufigkeit der Cloud-Metadaten wird von Drittanbieterplattformen verwendet, die Sensor-Metadaten mit einer einstellbaren Übertragungsfrequenz abonnieren möchten. Die Cloud-Metadaten umfassen alle auf dem Dashboard angezeigten Sensordaten.

Cloud metadata (Cloud-Metadaten): Aktivieren Sie diese Option, um Cloud-Metadaten zu verwenden.

Hinweis

Der Standard ist, dass diese Funktion deaktiviert ist; es werden keine Metadaten für das Thema gesendet. Nach der Aktivierung werden die Metadaten für das Thema in dem unten eingestellten Frequenzbereich übertragen.

Set frequency range (00:00:01 – 23:59:59) (Frequenzbereich einstellen (00:00:01 – 23:59:59)): Geben Sie einen Wert ein, um den Frequenzbereich einzustellen.

Validierungszeitraum

Sie können einen Validierungszeitraum für die folgenden Luftqualität-Einstellungen festlegen. Der Validierungszeitraum fungiert als zeitlicher Schwellenwert, und der Messwert muss über dem Grenzwert des Validierungszeitraums liegen, um einen Alarm auszulösen.

Beispiel

Wenn die CO_2-Validierungsdauer 5 Sekunden beträgt, muss der CO_2-Wert während der gesamten 5 Sekunden über dem Grenzwert liegen, damit der Alarm ausgelöst wird.

Legen Sie den Validierungszeitraum (0–60 Sekunden) für die folgenden Daten fest:

- **Temperatur**
- **Feuchtigkeit**
- **CO2**
- **NOx**
- **PM1.0**
- **PM2.5**
- **PM4.0**
- **PM10.0**
- **VOC**
- **AQI**
- **Vaping/Rauchen**

Statistik

Statistik der Sensordaten

Sie können Sensorstatistiken für bis zu 365 Tage in eine CSV-Datei exportieren, um sie in Anwendungen wie Microsoft® Excel zu verwenden.

- **Predefined date range (Vordefinierter Datumsbereich)**: Wählen Sie aus der Liste den vordefinierten Datumsbereich aus, den Sie herunterladen möchten.
- **From (Von)** und **To (Bis)**: Wählen Sie den gewünschten Bereich aus, den Sie herunterladen möchten. Sie können die Daten bis zu 365 Tage lang herunterladen.

Hinweis

Wenn sowohl ein benutzerdefinierter als auch ein vordefinierter Bereich ausgewählt sind, hat der benutzerdefinierte Bereich Vorrang.

Hinweis

Der maximale Download-Bereich wird durch die in *Speicher-Einstellung, on page 31* konfigurierte Speicherdauer begrenzt.

- **Select a source (Eine Quelle auswählen)**: Wählen Sie die gewünschte Quelle aus, die Sie herunterladen möchten.
- **Download data (Daten herunterladen)**: zum Auswählen von **Download selected sensor data (Ausgewählte Sensordaten herunterladen)** aus dem Drop-Down-Menü.
- **Download data for all sources (Daten für alle Quellen herunterladen)**, um Daten für alle Quellen innerhalb des gewählten Zeitraums zu exportieren.

Die Datei wird in Ihren Download-Ordner heruntergeladen. Je nach Dateigröße kann der Download einige Zeit in Anspruch nehmen.

Analyse

AXIS Audio Analytics

Schalldruckpegel

Show threshold and events in graph (Grenzwerte und Ereignisse in Diagramm anzeigen): Schalten Sie diese Option ein, um eine erfasste Geräuschspitze im Diagramm anzuzeigen.

Grenzwert: Stellen Sie die Grenzwerte für die Erfassung ein. Die Anwendung registriert Audio-Ereignisse für sämtliche Geräusche, die außerhalb der Grenzwerte liegen.

Adaptive Audioerfassung

Show events in graph (Ereignisse in Diagramm anzeigen): Schalten Sie diese Option ein, um eine erfasste Geräuschspitze im Diagramm anzuzeigen.

Grenzwert: Den Schieber bewegen, um den Erfassungsgrenzwert einzustellen. Beim Erreichen des Mindestgrenzwerts werden selbst schwache Lautstärkespitzen registriert, während dies beim maximalen Grenzwert nur für hohe Lautstärkespitzen der Fall ist.

Test alarms (Probealarme): Klicken Sie **Test (Testen)** an, um zu Testzwecken eine Erfassung auszulösen.

Audioklassifizierung

Show events in graph (Ereignisse in Diagramm anzeigen) : Schalten Sie diese Option ein, um im Diagramm anzuzeigen, wann eine bestimmte Art von Geräusch erfasst wurde.

Classifications (Klassifizierungen) : Wählen Sie aus, welche Arten von Geräuschen die Anwendung erfassen soll.

Test alarms (Probealarme) : Klicken Sie auf **Test (Testen)**, um zu Testzwecken die Erfassung eines bestimmten Geräuschs auszulösen.

Audio

Geräteinstellungen

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

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.

Übersicht

Status Signal-LED

Zeigt die verschiedenen Signal-LED-Aktivitäten an, die auf dem Gerät ausgeführt werden. Sie können bis zu 10 Aktivitäten gleichzeitig in der Statusliste der Signal-LED anzeigen lassen. Wenn zwei oder mehr Aktivitäten

gleichzeitig ausgeführt werden, zeigt die Aktivität mit der höchsten Priorität den Status der Signal-LED an. Diese Zeile wird in der Statusliste markiert.

Audio speaker status (Status des Audiolautsprechers)

Zeigt die verschiedenen Aktivitäten des Audiolautsprechers an, die auf dem Gerät ausgeführt werden. In der Statusliste des Audiolautsprechers können bis zu zehn Aktivitäten gleichzeitig ausgeführt werden. Wenn mindestens zwei Aktivitäten gleichzeitig ausgeführt werden, wird die Aktivität mit der höchsten Priorität ausgeführt. Diese Zeile wird in der Statusliste grün markiert.

Profile

Profile

Ein Profil ist eine Sammlung von festgelegten Konfigurationen. Es können bis zu 30 Profile mit unterschiedlichen Prioritäten und Mustern erstellt werden. Die Profile werden aufgelistet, um eine Übersicht über Namen, Priorität sowie Licht- und Sireneneinstellungen zu erhalten.

Create (Erstellen): Klicken Sie auf diese Option, um ein Profil zu erstellen.

- **Preview/Stop preview (Vorschau/Stopp der Vorschau)**: Starten oder stoppen Sie vor dem Speichern eine Vorschau des Profils.

Hinweis

Sie können nicht zwei Profile mit demselben Namen haben.

- **Name**: Geben Sie einen Namen für das Profil ein.
- **Beschreibung**: Geben Sie eine Beschreibung für das Profil ein.
- **Light (Licht)**: Wählen Sie aus dem Auswahlmenü aus, welche **Pattern (Muster)**, **Speed (Geschwindigkeit)**, **Intensity (Stärke)** und **Color (Farbe)** des Lichts Sie wünschen.
- **Siren (Sirene)**: Wählen Sie aus dem Auswahlmenü aus, welche Art von **Pattern (Muster)** und welche **Intensity (Lautstärke)** der Sirene Sie wünschen.
- Starten oder stoppen Sie eine Vorschau nur des Lichts oder der Sirene.
- **Dauer**: Legen Sie die Dauer der Aktivitäten fest.
  - **Continuous (Durchgehend)**: Nach dem Start werden sie solange ausgeführt, bis sie beendet werden.
  - **Zeit**: Legen Sie eine bestimmte Zeit für die Dauer der Aktivität fest.
  - **Repetitions (Wiederholungen)**: Legen Sie fest, wie oft sich die Aktivität wiederholen soll.
- **Priority (Priorität)**: Stellen Sie die Priorität einer Aktivität auf eine Zahl von 1 bis 10. Aktivitäten, deren Priorität höher als 10 ist, können nicht aus der Statusliste entfernt werden. Es gibt drei Aktivitäten mit einer höheren Priorität als 10; **Maintenance (Wartung)** (11), **Identify (Identifizieren)** (12) und **Health check (Integritätsprüfung)** (13).

Import (Importieren): Fügen Sie ein oder mehrere Profile mit einer vordefinierten Konfiguration hinzu.

- **Add (Hinzufügen)** : Neue Profile hinzufügen.
- **Delete and add (Löschen und hinzufügen)** : Die alten Profile sind gelöscht, Sie können neue Profile hochladen.
- **Überschreiben**: Aktualisierte Profile überschreiben vorhandene Profile.

Um ein Profil zu kopieren und auf anderen Geräten zu speichern, wählen Sie das Profil/die Profile aus und klicken Sie auf **Export (Exportieren)**. Eine json-Datei wird exportiert.

Profil starten. Das Profil und seine Aktivitäten werden in der Statusliste angezeigt.

Für das Profil stehen die Funktionen **Edit (Bearbeiten)**, **Copy (Kopieren)**, **Export (Exportieren)** und **Delete (Löschen)** zur Verfügung.

Aufzeichnungen

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

Aufzeichnung starten.

Wählen Sie einen Speicher, der als Netzwerk-Speicher eingerichtet wurde.

Aufzeichnung stoppen.

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.

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.

Medien

+ Hinzufügen: Klicken Sie, um eine neue Datei hinzuzufügen.

Storage location (Speicherort): Wählen Sie aus, ob die Datei im internen Speicher oder im integrierten Speicher (SD-Speicherkarte, falls verfügbar) gespeichert werden soll.

Das Kontextmenü enthält:

- **Information (Informationen)**: Zeigen Sie Informationen über die Datei an.
- **Copy link (Link kopieren)**: Kopieren Sie den Link zum Standort der Datei auf dem Gerät.
- **Löschen**: Löschen Sie die Datei am Speicherort.

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 (PTP) (Datum und Uhrzeit automatisch (PTP))**: Diese Option erlaubt das automatische Synchronisieren der Zeit mithilfe des Precision Time Protocol (PTP).
- **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.
  - **Trusted NTS KE CA certificates (Vertrauenswürdige NTS KE CA-Zertifikate)**: Wählen Sie die vertrauenswürdigen CA-Zertifikate aus, die für die sichere NTS KE-Zeitsynchronisierung verwendet werden sollen, oder lassen Sie das Feld leer.
  - **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 (v4 oder v6) verbunden werden. Wenn beide Versionen verfügbar sind, zieht das Gerät IANA gegenüber POSIX und DHCPv4 gegenüber DHCPv6 vor.
  - DHCPv4 verwendet Option 100 für POSIX-Zeitzonen und Option 101 für IANA-Zeitzonen.
  - DHCPv6 verwendet Option 41 für POSIX und Option 42 für IANA.
- **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.

- **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.

Netzwerk

IPv4

Assign IPv4 automatically (IPv4 automatisch zuweisen): Wählen Sie die automatische IP-Zuweisung per IPv4 (DHCP) aus, damit das Netzwerk IP-Adresse, Subnetzmaske und Router automatisch zuweist und keine manuelle Konfiguration erforderlich ist. Wir empfehlen eine automatische Zuweisung der IP-Adresse (DHCP) für die meisten Netzwerke.

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.

Hinweis

Wenn DHCP deaktiviert ist, sind Funktionen, die auf einer automatischen Netzwerkkonfiguration basieren, wie z. B. Host-Name, DNS-Server, NTP usw., unter Umständen nicht mehr ausführbar.

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.
  - **Privacy (Datenschutz)**: Wählen Sie die gewünschte Verschlüsselung zum Schutz Ihrer SNMP-Daten aus.
  - **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/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+, FIPS 140-3 Level 3) (Sicheres Element (CC EAL6+, FIPS 140-3 Stufe 3))** : Wählen Sie diese Option aus, um ein sicheres Element als 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 MAGCsec (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

Firewall: Schalten Sie diese Option ein, um die Firewall zu aktivieren.

Default Policy (Standardrichtlinie): Wählen Sie aus, wie die Firewall Verbindungsanfragen behandeln soll, die nicht durch Regeln abgedeckt sind.

- **ACCEPT (ZULASSEN):** Ermöglicht alle Verbindungen mit dem Gerät. Diese Option ist in der Standardeinstellung festgelegt.
- **DROP (BLOCKIEREN):** Blockiert alle Verbindungen zu dem Gerät.

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

+ New rule (+ Neue Regel): Klicken Sie darauf, um eine Regel zu erstellen.

Rule type (Regeltyp):

- **FILTER**: Wählen Sie aus, ob Verbindungen von Geräten, die den in der Regel definierten Kriterien entsprechen, zugelassen oder blockiert werden sollen.
  - **Richtlinie**: Wählen Sie **Accept (Akzeptieren)** oder **Drop (Verwerfen)** für die Firewall-Regel.
  - **IP range (IP-Adressbereich)**: Wählen Sie diese Option, um einen Bereich von Adressen zuzulassen oder zu blockieren. Verwenden Sie IPv4/IPv6 in **Start** und **Ende**.
  - **IP-Adresse**: Geben Sie eine Adresse ein, die Sie zulassen oder blockieren möchten. Verwenden Sie das Format IPv4/IPv6 oder CIDR.
  - **Protocol (Protokoll)**: Wählen Sie ein Netzwerkprotokoll (TCP, UDP oder beide), das zugelassen oder blockiert werden soll. Wenn Sie ein Protokoll auswählen, müssen Sie auch einen Port angeben.
  - **MAC**: Geben Sie die MAC-Adresse eines Gerätes ein, das Sie zulassen oder blockieren möchten.
  - **Port range (Portbereich)**: Wählen Sie diese Option, um den Bereich von Ports zuzulassen oder zu blockieren. Fügen Sie sie in **Start** und **Ende** ein.
  - **Port**: Geben Sie eine Portnummer ein, die Sie zulassen oder blockieren möchten. Portnummern müssen zwischen 1 und 65535 liegen.
  - **Traffic type (Art des Datenaustauschs)**: Wählen Sie die Art des Datenaustauschs, die Sie zulassen oder blockieren möchten.
    - **UNICAST**: Datenaustausch von einem einzigen Absender zu einem einzigen Empfänger.
    - **BROADCAST**: Datenaustausch von einem einzigen Absender zu allen Geräten im Netzwerk.
    - **MULTICAST**: Datenaustausch von einem oder mehreren Absendern zu einem oder mehreren Empfängern.
- **LIMIT**: Wählen Sie diese Option, um Verbindungen von Geräten zu akzeptieren, die den in der Regel definierten Kriterien entsprechen, aber Grenzen anzuwenden, um übermäßigen Datenaustausch zu reduzieren.
  - **IP range (IP-Adressbereich)**: Wählen Sie diese Option, um einen Bereich von Adressen zuzulassen oder zu blockieren. Verwenden Sie IPv4/IPv6 in **Start** und **Ende**.
  - **IP-Adresse**: Geben Sie eine Adresse ein, die Sie zulassen oder blockieren möchten. Verwenden Sie das Format IPv4/IPv6 oder CIDR.
  - **Protocol (Protokoll)**: Wählen Sie ein Netzwerkprotokoll (TCP, UDP oder beide), das zugelassen oder blockiert werden soll. Wenn Sie ein Protokoll auswählen, müssen Sie auch einen Port angeben.
  - **MAC**: Geben Sie die MAC-Adresse eines Gerätes ein, das Sie zulassen oder blockieren möchten.
  - **Port range (Portbereich)**: Wählen Sie diese Option, um den Bereich von Ports zuzulassen oder zu blockieren. Fügen Sie sie in **Start** und **Ende** ein.

- **Port**: Geben Sie eine Portnummer ein, die Sie zulassen oder blockieren möchten. Portnummern müssen zwischen 1 und 65535 liegen.
- **Unit (Einheit)**: Wählen Sie die Art der Verbindungen, die zugelassen oder blockiert werden sollen.
- **Period (Zeitraum)**: Wählen Sie den Zeitraum für **Amount (Betrag)**.
- **Amount (Betrag)**: Stellen Sie ein, wie oft ein Gerät innerhalb des eingestellten **Period (Zeitraum)** maximal eine Verbindung herstellen darf. Der Höchstbetrag liegt bei 65535.
- **Burst (Impulspaket)**: Geben Sie die Anzahl der Verbindungen ein, die den eingestellten **Amount (Betrag)** einmal während des eingestellten **Period (Zeitraums)** überschreiten dürfen. Sobald die Zahl erreicht ist, ist nur noch der festgelegte Betrag während des festgelegten Zeitraums erlaubt.
- **Traffic type (Art des Datenaustauschs)**: Wählen Sie die Art des Datenaustauschs, die Sie zulassen oder blockieren möchten.
  - **UNICAST**: Datenaustausch von einem einzigen Absender zu einem einzigen Empfänger.
  - **BROADCAST**: Datenaustausch von einem einzigen Absender zu allen Geräten im Netzwerk.
  - **MULTICAST**: Datenaustausch von einem oder mehreren Absendern zu einem oder mehreren Empfängern.

Test rules (Test-Regeln): Klicken Sie hier, um die von Ihnen definierten Regeln zu testen.

- **Test time in seconds: (Testdauer in Sekunden)**: Legen Sie für das Testen der Regeln ein Zeitlimit fest.
- **Zurückrollen**: Klicken Sie hier, um die Firewall auf den vorherigen Zustand zurückzusetzen, bevor Sie die Regeln getestet haben.
- **Apply rules (Regeln anwenden)**: Klicken Sie hier, um die Regeln ohne Test zu aktivieren. Wir empfehlen Ihnen, dies nicht zu tun.

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**: Darf keine Änderungen an den Einstellungen vornehmen.

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**, **OpenID** und **Client Credential Grant (Client-Zugangsdaten-Genehmigung)**.

HTTPS: Wählen Sie diese Option aus, um HTTPS zu verwenden.

Das Kontextmenü enthält:

- **Update virtual host (Virtuellen Host aktualisieren)**
- **Delete virtual host (Virtuellen Host löschen)**

Konfiguration der Client-Zugangsdaten-Genehmigung

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

Verification URI (Verifizierungs-URI): Geben Sie den Weblink für die API-Endpunkt-Authentifizierung ein.

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.

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

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 unter *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 condition (Bedingung einbeziehen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

Include namespaces (Namespaces einbeziehen): 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.

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-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.

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.

Konten

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

Das Konto wurde erfolgreich beim SIP-Server registriert.

Es besteht ein Problem mit dem Konto. Mögliche Gründe: Autorisierungsfehler, falsche Kontendaten oder der SIP-Server kann das Konto nicht ermitteln.

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

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

- **Aktiv**: Mit dieser Option das Konto nutzbar machen.
- **Make default (Als Standard setzen)**: Mit dieser Option dieses Konto als Standardkonto verwenden. Es muss ein und nur ein Standardkonto vorhanden sein.
- **Answer automatically (Automatisch annehmen)**: Einen eingehenden Anruf automatisch annehmen.
- **Prioritize IPv6 over IPv4 (IPv6 gegenüber IPv4 bevorzugen)** : Wählen Sie diese Option aus, um IPv6-Adressen gegenüber IPv4-Adressen zu bevorzugen. Dies ist nützlich, wenn Verbindungen zu Peer-to-Peer-Konten oder Domänennamen hergestellt werden, die sowohl in IPv4- als auch in IPv6-Adressen auflösen. IPv6 kann nur für Domänennamen priorisiert werden, die IPv6-Adressen zugeordnet sind.
- **Name**: Einen aussagekräftigen Namen eingeben. Dies kann zum Beispiel ein Vor- und Nachname, eine Funktion oder ein Standort sein. Der Name muss nicht eindeutig sein.
- **Benutzer-ID**: Geben Sie die dem Axis Gerät zugeordnete eindeutige Telefonnummer oder Durchwahl an.
- **Peer-to-peer (Gleichrangig)**: Für Direktanrufe an ein anderes SIP-Gerät im lokalen Netzwerk.
- **Registriert**: Für Anrufe an SIP-Geräte außerhalb des lokalen Netzwerks über einen SIP-Server.
- **Domain**: Falls verfügbar, den Namen der öffentlichen Domain eingeben. Er wird bei Anrufen bei anderen Konten als Teil der SIP-Adresse angezeigt.
- **Password (Kennwort)**: Geben Sie das dem SIP-Konto zugehörige Kennwort ein, um sich beim SIP-Server zu authentifizieren.
- **Authentifizierungs-ID**: Die Authentifizierungs-ID für den SIP-Server eingeben. Wenn diese mit der Benutzer-ID identisch ist, muss sie nicht gesondert eingegeben werden.
- **Anrufer-ID**: Der dem Empfänger der von diesem Gerät aus getätigten Anrufe angezeigte Name.
- **Registrar (Registrierung)**: Geben Sie die IP-Adresse der Registrierungsstelle ein.
- **Übertragungsmodus**: Den SIP-Übertragungsmodus für das Konto wählen: UPD, TCP oder TLS.
- **TLS version** (nur mit Übertragungsmodus TLS): Wählen Sie die zu verwendende TLS-Version. Die Versionen **v1.2** und **v1.3** sind die sichersten. **Automatic (Automatisch)** wählt die sicherste Version aus, die das System verarbeiten kann.
- **Medienverschlüsselung** (nur mit Übertragungsmodus TLS): Die Art der Verschlüsselung für Medien (Audio und Video) für SIP-Anrufe wählen.
- **Zertifikat** (nur mit Übertragungsmodus TLS): Ein Zertifikat wählen.
- **Server-Zertifikat überprüfen** (nur mit Übertragungsmodus TLS): Markieren Sie diese Option, um das Server-Zertifikat zu überprüfen.
- **Sekundärer SIP-Server**: Aktivieren Sie diese Option, damit bei fehlgeschlagener Registrierung am primären SIP-Server das Gerät versucht, sich am sekundären SIP-Server zu registrieren.

- **SIP secure (SIP-Secure)**: Diese Option zum Verwenden von Secure Session Initiation Protocol (SIPS) wählen. SIPS verwendet zum Verschlüsseln den Übertragungsmodus TLS.
- **Proxies**
  - **Proxy**: Klicken Sie darauf, um einen Proxy hinzuzufügen.
  - **Priorisieren**: Bei zwei oder mehreren Proxies, diese zum Priorisieren anklicken.
  - **Server-Adresse**: Geben Sie die IP-Adresse des primären SIP-Servers ein.
  - **Username (Benutzername)**: Falls verlangt, einen Benutzernamen für den SIP-Proxyserver eingeben.
  - **Password (Kennwort)**: Falls verlangt, das Kennwort für den SIP-Proxyserver eingeben.
- **Video**
  - **Sichtbereich**: Den für Videoanrufe zu verwendenden Sichtbereich wählen. Ohne Auswahl wird die Standardansicht verwendet.
  - **Auflösung**: Wählen Sie die für Videoanrufe zu verwendende Auflösung. Die Auflösung wirkt sich auf die erforderliche Bandbreite aus.
  - **Bildrate**: Wählen Sie die Bildrate für Videoanrufe. Die Bildrate wirkt sich auf die erforderliche Bandbreite aus.
  - **H.264-Profil**: Wählen Sie das Profil aus, das für Videoanrufe verwendet werden soll.

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.

Multicast-Controller

User multicast controller (Benutzer Multicast-Controller): Aktivieren Sie den Multicast-Controller.

Audio codec (Audio-Codec): Wählen Sie einen Audio-Codec aus.

Source (Quelle): Neue Quelle für Multicast-Controller hinzufügen.

- **Bezeichnung**: Geben Sie den Namen einer Bezeichnung ein, die noch nicht von einer Quelle verwendet wird.
- **Source (Quelle)**: Geben Sie eine Quelle ein.
- **Port**: Geben Sie einen Port ein.
- **Priority (Priorität)**: Wählen Sie eine Priorität aus.
- **Profile (Profil)**: Ein Profil auswählen.
- **SRTP key (SRTP-Schlüssel)**: Geben Sie einen SRTP-Schlüssel ein.

Das Kontextmenü enthält:

Edit (Bearbeiten): Quelle für den Multicast-Controller bearbeiten.

Löschen: Löschen Sie die Quelle des Multicast-Controllers.

Speicherung

Netzwerk-Speicher

Network storage (Netzwerk-Speicher): Schalten Sie diese Option ein, um den Netzwerk-Speicher zu benutzen.

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.

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 *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Bildrate: Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Komprimierung: Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Zipstream : Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Optimize for storage (Für Speicherung optimieren) : Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Dynamic FPS (Dynamische Bilder pro Sekunde) : Siehe *Videostream, on page 25* zu einer Beschreibung dieser Einstellung.

Dynamic GOP (Dynamische Bildergruppe) : Siehe *Videostream, on page 25* zu einer Beschreibung dieser Einstellung.

Mirror (Spiegelung) : Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

GOP length (GOP-Länge) : Siehe *Videostream, on page 25* für eine Beschreibung dieser Einstellung.

Bitrate control (Bitratensteuerung): Siehe *Videostream, on page 25* 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 *Videostream, on page 25* 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.

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
  - 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

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.

Energieeinstellungen

Energieverbrauch

Zeigt Informationen zum Strom an. Die Angaben variieren je nach Produkt.

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.
- **View the audit log (Audit-Protokoll anzeigen)**: Klicken Sie hier, um Informationen zu Benutzer- und Systemaktivitäten anzuzeigen, z. B. erfolgreiche oder fehlgeschlagene Authentifizierungen und Konfigurationen.

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.

Typ: Wählen Sie die Art der Protokolle, die Sie senden möchten.

Test server setup (Servereinrichtung testen): Senden Sie eine Testnachricht an alle Server, bevor Sie die Einstellungen speichern.

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.
- **Automatic rollback (Automatisches Rollback)**: 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

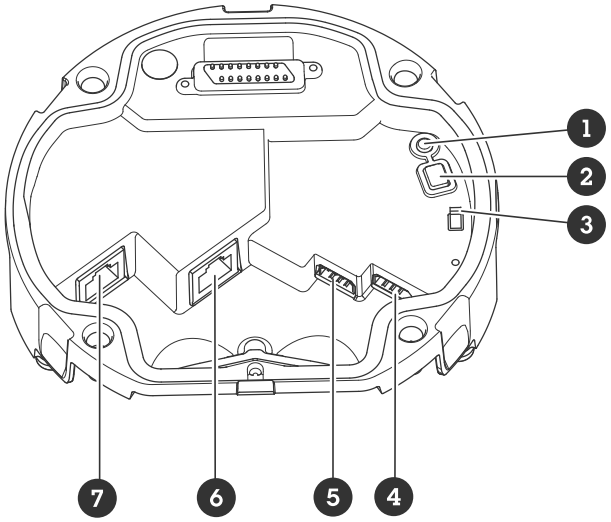
Eine Datei zum Netzwerk-Trace enthält möglicherweise vertrauliche Informationen wie Zertifikate oder Kennwörter.

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

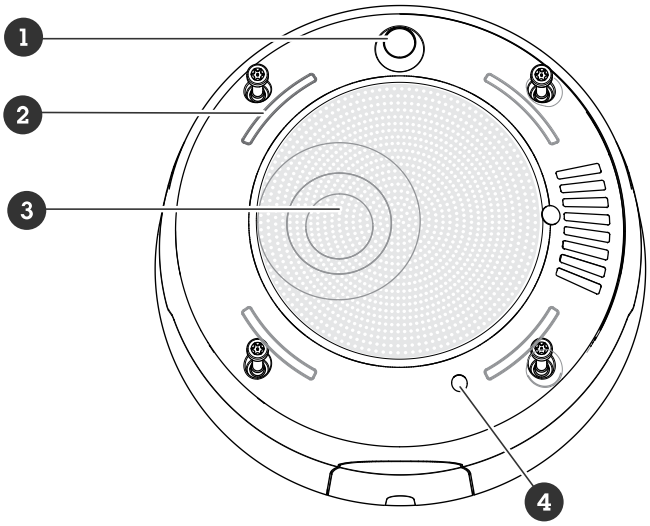
Trace time (Trace-Dauer): Geben Sie die Verfolgungsdauer in Sekunden oder Minuten an, und klicken Sie auf **Download (Herunterladen)**.

Technische Daten

Produktübersicht



1 *Status-LED*
2 *Steuertaste*
3 *Mikrofonschalter*
4 *E/A-Anschluss*
5 *RS-485-Anschluss*
6 *Netzwerk-Anschluss (PoE-Ausgang)*
7 *Netzwerk-Anschluss (PoE IN)*



1 *PIR-Sensor*
2 *Signal-LEDs*
3 *Lautsprecher*
4 *Internes Mikrofon*

Status-LED

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

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 82*.

Mikrofonschalter

Zur Einbaulage des Mikrofonschalters, siehe *Produktübersicht, on page 76*.

Mit dem Mikrofonschalter wird das Mikrofon in die Position **ON (EIN)** oder **OFF (AUS)** geschaltet. Die Werkseinstellung ist **OFF (AUS)**.

Anschlüsse

Netzwerk-Anschluss

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

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

E/A-Anschluss

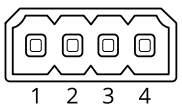
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

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

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

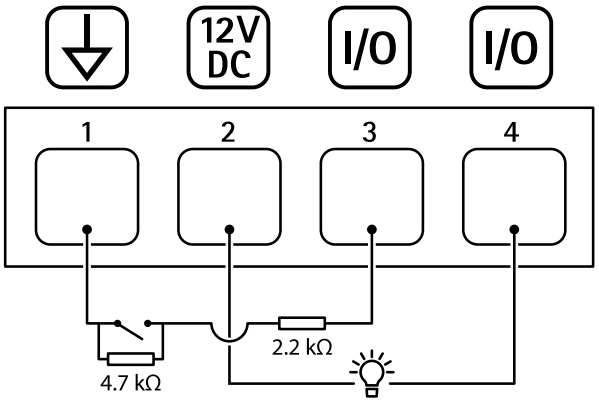
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

4-poliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	⚠ Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 25 mA
Konfigurierbar (Ein- oder Ausgang)	3–4	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen. Um überwachten Eingang zu nutzen, Abschlusswiderstände anschließen. Informationen zum Anschließen der Widerstände bietet der Schaltplan.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – 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:

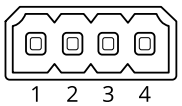


1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V, max. 25 mA*
3 *Als überwachter Eingang konfigurierter E/A*
4 *E/A als Ausgang konfiguriert*

Anschlusstyp RS-485/RS-422

Zwei 2-polige Anschlussblöcke für serielle Schnittstellen vom Typ RS485/RS422. Der serielle Anschluss kann in den folgenden Anschlussmodi konfiguriert werden:

- zweiadriger RS485-Halbduplex-Anschluss
- vieradriger RS485-Vollduplex-Anschluss
- zweiadriger RS422-Simplex-Anschluss
- vieradriger RS422-Vollduplex-Anschluss (Punkt-zu-Punkt-Verbindung)



Funktion	Kontakt	Hinweise
RS485/RS422 RX/TX A	1	(RX) RS485/RS422 für Vollduplex (RX/TX) Für Halbduplex RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) RS485/RS422 für Vollduplex
RS485/RS422 TX B	4	

Namen von Lichtmustern

Aus
Konstant
Alternierend
Impuls
Eskaliert in 3 Schritten
Blinken
3 x Blinken
4 x Blinken
3 x schwaches Blinken
4 x schwaches Blinken
1 x Blitzlicht
3 x Blitzlicht

Sirenenmuster-Namen

Aus
Alarm: Alarm mit hoher Tonlage
Alarm: Alarm mit niedriger Tonlage
Alarm: Vogel
Alarm: Schiffshorns
Alarm: Fahrzeugalarm
Alarm: Autoalarm schnell
Alarm: Klassische Uhr
Alarm: Erstbegleiter
Alarm: Horror
Alarm: Industrie
Alarm: Einzelner Signalton
Alarm: Weicher Vierfachton
Alarm: Weicher dreifacher Signalton
Alarm: Dreifach hohe Tonlage

Benachrichtigung über: Akzeptiert
Benachrichtigung über: Wird angerufen
Benachrichtigung über: Abgelehnt
Benachrichtigung über: Fertig
Benachrichtigung über: Eintrag
Benachrichtigung über: Fehlgeschlagen
Benachrichtigung über: Eilt
Benachrichtigung über: Nachricht
Benachrichtigung über: Weiter
Benachrichtigung über: Offen
Siren (Sirene): Alternierend
Siren (Sirene): Springend
Siren (Sirene): Evac.
Siren (Sirene): Fallender Ton
Siren (Sirene): Home weich

Gerät reinigen

Sie können Ihr Gerät mit lauwarmem Wasser reinigen.

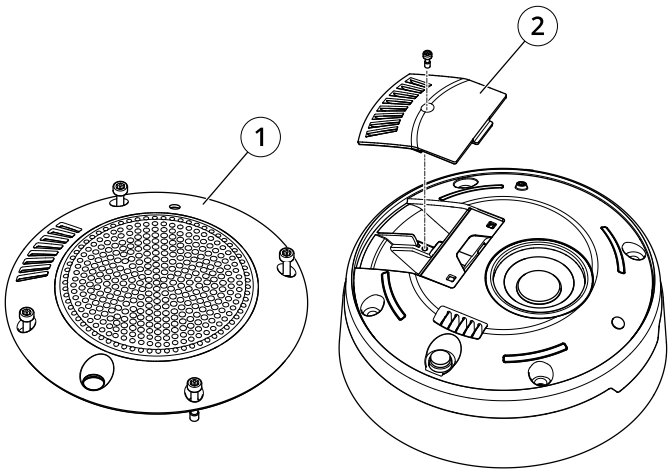
HINWEIS

- Aggressive Chemikalien können das Gerät beschädigen. Verwenden Sie zur Reinigung Ihres Geräts keine chemischen Substanzen wie Fensterreiniger oder Aceton.

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.

Hinweis

- Entfernen Sie die Abdeckung (1) und den Zugang (2).
- Verwenden Sie eine Bürste, um den Staub zu entfernen.



1 Abdeckung
2 Tür

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:

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

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): • Wenn Sie `Reply from <IP address>: bytes=32; time=10...` empfangen, bedeutet dies, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut. • Wenn Sie `Request timed out` empfangen, bedeutet dies, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
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 *Zurücksetzen auf die Werkseinstellungen, on page 82*.
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.

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.

Das Gerät wird nach dem Anschließen an ein anderes Produkt nicht mehr gestartet.

Falsche PoE-Klasse	Stellen Sie sicher, dass eine PoE-Stromversorgung der Klasse 4 verwendet wird, wenn das Gerät an ein anderes Produkt angeschlossen ist.

Die Sensordaten sind nicht genau.

Die Sensordaten sind ungenau.	Der AQI (Luftqualitätsindex), CO2, VOC und NOx benötigen Zeit, um wirksam zu sein. Siehe *Kalibrierung für den Erstbetrieb des Geräts, on page 9*.

Leistungsaspekte

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

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

Support

Weitere Hilfe erhalten Sie hier: *axis.com/support*.

T10222990_de

2026-01 (M3.2)