

AXIS D6310 Air Quality Sensor

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
Positionierung des Geräts.....	6
Erfassungsbereich des Sensors	6
Ihr Gerät konfigurieren	7
Luftqualitätsmonitor konfigurieren	7
Konfigurieren Sie das Dashboard des Luftqualitätssensors.	7
Luftqualitätssensor einstellen	8
Sensordatenstatistik herunterladen	9
Kalibrierung für den ersten Betrieb des Geräts	9
MQTT-Daten veröffentlichen.....	9
Ein Profil konfigurieren	11
Ein Profil mit benutzerdefinierter Audiodatei für die Sirene konfigurieren.....	11
Ein Profil importieren oder exportieren.....	12
Direktes SIP (P2P) einrichten.....	12
SIP über einen Server (PBX) einrichten	13
Einrichten von Regeln für Ereignisse.....	13
Lösen Sie eine Aktion aus	13
Video aufzeichnen, wenn Vaping detektiert wird.....	14
Audio-Clip abspielen, wenn CO2-Wert zu hoch ist	14
Aktivieren Sie ein Licht- und Sirenenprofil über den externen Bewegungsmelder (PIR-Sensor).	14
Profil starten, wenn ein Alarm ausgelöst wird.....	15
Profil über SIP starten	15
Mehrere Profile über SIP-Erweiterungen steuern.....	16
Zwei Profile mit unterschiedlichen Prioritäten ausführen	17
Aktivieren Sie ein Licht- und Sirenenprofil über HTTP Post, wenn eine Kamera ein Bewegungsmuster erkennt.....	17
Aktivieren Sie ein Licht- und Sirenenprofil über einen virtuellen Eingang, wenn eine Kamera ein Bewegungsmuster erkennt.....	18
Aktivieren Sie ein Licht- und Sirenenprofil über MQTT, wenn eine Kamera ein Bewegungsmuster erkennt.....	20
Senden einer E-Mail, wenn ein Lautsprechertest fehlschlägt	21
Bei Auslösen eines Alarms benutzerdefinierten Clip wiedergeben.....	22
Audio mit DTMF anhalten.....	23
Audio für eingehende SIP-Anrufe einrichten.....	23
Weboberfläche	25
Technische Daten.....	26
Produktübersicht.....	26
.....	26
Status-LED	27
Tasten.....	27
Steuertaste	27
Mikrofonschalter	27
Anschlüsse	27
Netzwerk-Anschluss	27
E/A-Anschluss.....	27

Anschlusstyp RS-485/RS-422	28
Namen von Lichtmustern	29
Sirenenmuster-Namen.....	29
Gerät reinigen	31
Fehlerbehebung.....	32
Zurücksetzen auf die Werkseinstellungen.....	32
Technische Fragen, Hinweise und Lösungen.....	32
Leistungsaspekte.....	34
Support.....	34
Cybersicherheit.....	35
Schwachstellen-Management	35
Sicherheitsbenachrichtigungen.....	35
Sicherer Produktlebenszyklus.....	35

Installation

Wichtig

- Halten Sie einen Mindestabstand von 1,5 Metern zu Bereichen mit großen Lüftungsöffnungen oder Verschmutzungsquellen ein. Dazu gehören Lüftungsöffnungen, Türen, Fenster, Kochstellen usw.
- Installieren Sie das Gerät an einem Standort, der einen freien Luftstrom ermöglicht.
- Installieren Sie das Gerät an der Decke in einer Höhe von 2,4-2,7 Metern über dem Boden, um eine effektive Vaping- oder Rauchdetektion zu gewährleisten.
- Installieren Sie das Gerät für eine effektive Überwachung der Luftqualität und der Umwelt in einer Höhe von 0,9 bis 1,8 Metern 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

- Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
Wenn Sie die IP-Adresse nicht kennen, ermitteln Sie das Gerät im Netzwerk mithilfe von AXIS IP Utility oder AXIS Device.
- 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 Funktionen und Einstellungen in der Weboberfläche von Geräten mit AXIS OS finden Sie unter *Hilfe zur Weboberfläche von AXIS OS*.

Administratorkonto erstellen

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

- Einen Benutzernamen eingeben.
- Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter*, on page 6.
- Geben Sie das Kennwort erneut ein.
- Stimmen Sie der Lizenzvereinbarung zu.
- 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 32*.

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 32*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Positionierung des Geräts

Die Positionierung Ihres Geräts hängt von Ihrem Anwendungsfall ab. Installieren Sie Ihr Gerät möglichst nah an Ihrem ausgewählten Bereich und berücksichtigen Sie dabei die folgenden Aspekte:

Ausgewählter Bereich	Montageort	Höhe	Zu vermeiden
Vapen und Zigarettenrauch	Decke	2,4–2,7 m (7,9–8,9 ft)	Ecken
PM, VOC, NO _x , CO ₂	Wand	0,9–1,8 m (3–6 ft)	Ecken, Wärmequellen
Feuchtigkeit	Decke oder Wand	Beliebig	Fenster, Luftzug, Wärmequellen, Ecken
Temperatur	Decke oder Wand	Beliebig	Wärme- und Kältequellen, Ecken

Erfassungsbereich des Sensors

Der Erfassungsbereich erstreckt sich kegelförmig vom Sensor. Der Erfassungsradius beträgt 2 m (6,5 ft), wobei der tatsächliche Gesamterfassungsbereich von Umgebungsfaktoren wie der Luftströmung und der Raumaufteilung abhängig ist.

Der Erfassungsbereich eines Sensors zur Erfassung von Rauchen oder Vapen beträgt 12,6 m² (135 ft²).

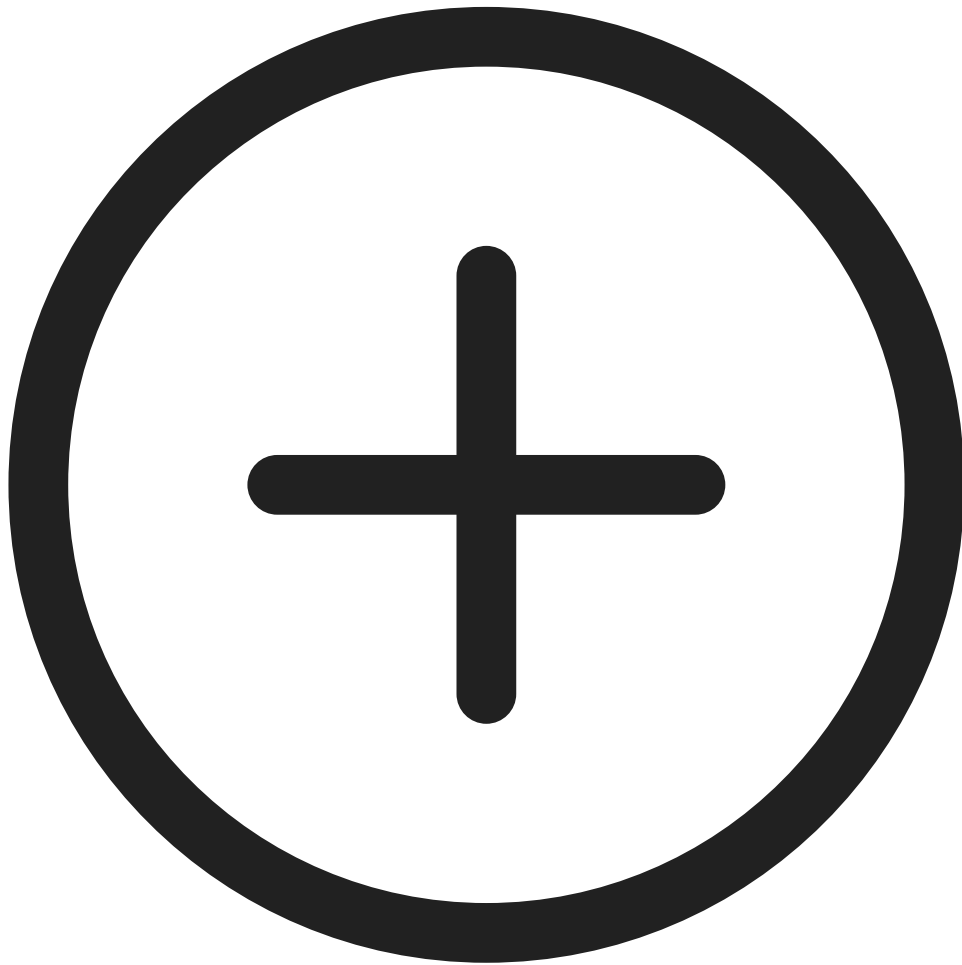
Ihr Gerät konfigurieren

Luftqualitätsmonitor konfigurieren

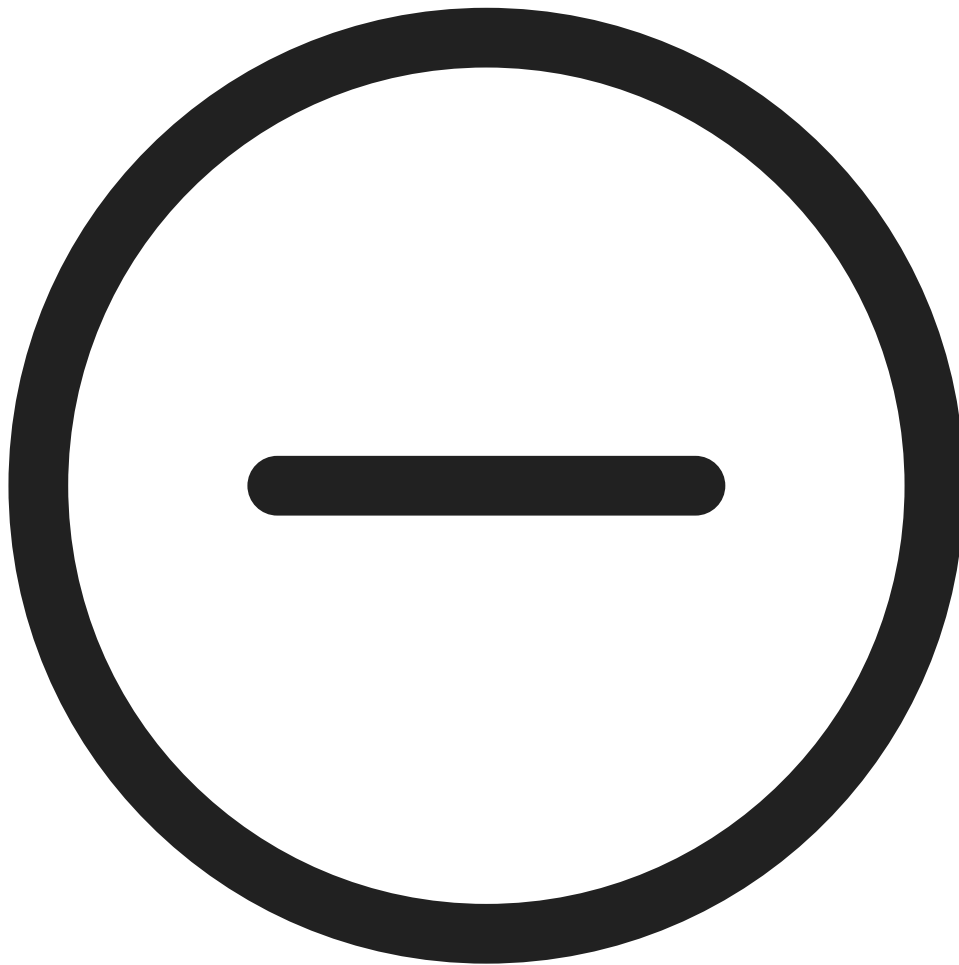
Konfigurieren Sie das Dashboard des Luftqualitätssensors.

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)** >



Hinweis

Auf dem Dashboard werden jeweils maximal 12 Variablen angezeigt. Wenn Ihr Dashboard voll ist, müssen Sie eine aktive Variable ausblenden, bevor Sie eine weitere anzeigen können.

Luftqualitätssensor einstellen

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

- Legen Sie Grenzwerte für Temperatur, Luftfeuchtigkeit, CO₂, NO_x, PM1.0, PM2.5, PM4.0, PM10.0, VOC, AQI, Feuchtigkeitsindex und Hitzeindex fest. Siehe *Einstellungen*.
- Stellen Sie die Empfindlichkeit der Vaping-Detektion auf (siehe *Einstellungen*).
- Legen Sie die Speicherdauer fest (siehe *Speichereinstellungen*).
- Legen Sie die Häufigkeit für die variable Metadatenübertragung fest (siehe *Variable Metadaten*).
- Legen Sie den Validierungszeitraum fest (siehe *Validierungszeitraum*).
- Aktivieren Sie Modbus (siehe *Modbus*).

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 *Storage settings (Speichereinstellungen)* 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 ersten Betrieb des Geräts

Hinweis

- Die vollständige CO₂-Genauigkeit wird bei der ersten Inbetriebnahme des Geräts nach 2 Tagen erreicht.
- Der AQI (Luftqualitätsindex) benötigt 12 Stunden, um bei der ersten Inbetriebnahme des Geräts funktionsfähig zu sein. Der AQI-Wert zeigt **Calculating (Berechnung)** 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 NO_x-Wertes erreicht das Gerät nach sechs Betriebsstunden. Die Kalibrierungszeit ist bei jedem Neustart des Geräts erforderlich.

MQTT-Daten veröffentlichen

Aktivieren Sie variable Metadaten:

1. Gehen Sie zu **Air quality monitor (Luftqualitätsmessgerät) > Settings (Einstellungen) > Variable metadata (Variabel übertragene Metadaten)**.
2. Aktivieren Sie die Option **Variable metadata (Variabel übertragene Metadaten)**.
3. Legen Sie die Häufigkeit der Datenübertragung fest.

Richten Sie den MQTT-Broker ein:

1. Wechseln Sie zu **System (System) > MQTT**.
2. Geben Sie Informationen zum Broker ein:
 - **Host:** IP-Adresse
 - **Benutzername und Kennwort**

- **Device topic prefix (Themenpräfix des Geräts):** Hier werden die MQTT-Daten veröffentlicht. Standardmäßig ist das Thema `axis/MAC-address`.
- 3. Schalten Sie den MQTT-Client ein. Der Text sollte sich wie folgt ändern: **Status: Connected (Status: Verbunden)**.
- 4. **Save (Speichern)** anklicken.

Veröffentlichen Sie die MQTT-Daten:

1. Klicken Sie auf der Registerkarte **MQTT publication (MQTT-Veröffentlichung)** auf **Add condition (Bedingung hinzufügen)**.
2. Geben Sie im Dialogfeld **Add condition (Bedingung hinzufügen)** Folgendes ein:
 - **Condition (Bedingung):** Air quality cloud monitoring active (Cloudbasierte Luftqualitätsüberwachung aktiv)
 - **MQTT topic (MQTT-Thema):** `axis/{serial}/event/tns:axis/AirQualityMonitor/VariableMetadata`
 - **Payload topic (Nutzlast-Thema):** `axis:AirQualityMonitor/VariableMetadata`
3. Klicken Sie auf **Hinzufügen**.

Hinweis

Falls Ihnen nicht **Air quality cloud monitoring active (Cloudbasierte Luftqualitätsüberwachung aktiv)** angezeigt wird, müssen Sie die variabel übertragenen Metadaten unter **Air quality monitor (Luftqualitätsmonitor) > Settings (Einstellungen)** aktivieren.

Die Bedingung führt zur Veröffentlichung aller Sensorparameter in dem von Ihnen gewählten Intervall für die variabel übertragenen Metadaten in einem Format wie dem folgenden:

```
{ "topic": "axis:AirQualityMonitor/Metadata", "timestamp": 1772553621219,
  "message": { "source": { "sensor_name": "D6310" }, "key": {}, "data": { "NOx":
    "4.000000", "Humidity": "21.290001", "Temperature": "26.430000", "PM10.0":
    "5.200000", "AQI": "28", "PM4.0": "5.000000", "PM1.0": "3.800000", "CO2":
    "580", "VOC": "180.000000", "PM2.5": "4.500000", "Humidex": "25", "Heat
    index": "26",
```

Die generierten Metadatenfelder umfassen:

Feld	Beschreibung
<code>topic</code>	Das Nutzlast-Thema, das die Bedingung ausgelöst hat.
<code>timestamp</code>	Zeitstempel, zu dem die Daten erstellt wurden.
<code>serial</code>	MAC-Adresse des Geräts. Die Seriennummer wird nur angezeigt, wenn Sie die Option Include serial number (Seriennummer hinzufügen) auf der Registerkarte MQTT publication (MQTT-Veröffentlichung) aktivieren.
<code>message</code>	Ein JSON-Objekt, das Informationen über die Bedingung enthält.
<code>message.source</code>	n. v.
<code>message.source.sensor_name</code>	Name des Geräts, das die Bedingung ausgelöst hat.
<code>message.key</code>	n. v.
<code>message.data</code>	Ein JSON-Objekt, das die Dateninformationen enthält.
<code>message.data.NOx</code>	Stickstoffmonoxid- und Stickstoffdioxidkonzentration in Echtzeit.

message.data.Humidity	Echtzeit-Luftfeuchtigkeit vom Luftqualitätssensor.
message.data.Temperature	Echtzeit-Temperatur vom Luftqualitätssensor in °C oder °F.
message.data.PM1.0	Echtzeit-Feinstaubkonzentration PM1,0.
message.data.PM2.5	Echtzeit-Feinstaubkonzentration PM2,5.
message.data.PM4.0	Echtzeit-Feinstaubkonzentration PM4,0.
message.data.PM10.0	Echtzeit-Feinstaubkonzentration PM10,0.
message.data.AQI	Echtzeit-Luftqualitätsindex auf der Grundlage der Daten vom Luftqualitätssensor.
message.data.CO2	Echtzeit-Kohlendioxidkonzentration.
message.data.VOC	Echtzeit-Index für flüchtige organische Verbindungen.
message.data.Humindex	Echtzeit-Feuchtigkeitsindex auf der Grundlage der Feuchtigkeits- und Temperaturdaten.
message.data.Heat_index	Echtzeit-Hitzeindex auf der Grundlage der Feuchtigkeits- und Temperaturdaten.

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 11*.
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 zu den SIP-Einstellungsoptionen finden Sie unter *SIP*.

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 *NAT-Traversal*.

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 zu den SIP-Einstellungsoptionen finden Sie unter *SIP*.

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 12*.

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.

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 eingerichtet ist.
 - **Kamera:** Wählen Sie einen Sichtbereich der Kamera aus.
 - **Stream profile (Streamprofil):** Wählen Sie ein Videostreamprofil aus oder 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.

Einstellen 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 26*.

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 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 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 Stopregeln.

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*.
- 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 <IP-Adresse> 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 <IP-Adresse> 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 aus.
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 (Lautsprecherteststatus)** 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:

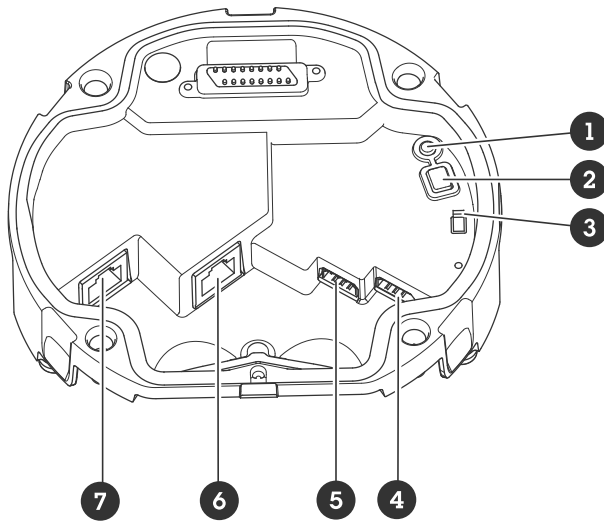
1. Gehen Sie auf **Settings > System > Events > Rules (Einstellungen > System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste die Option **Audio clip playing (Audioclip abspielen)** aus.
4. Aktivieren Sie die Option **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

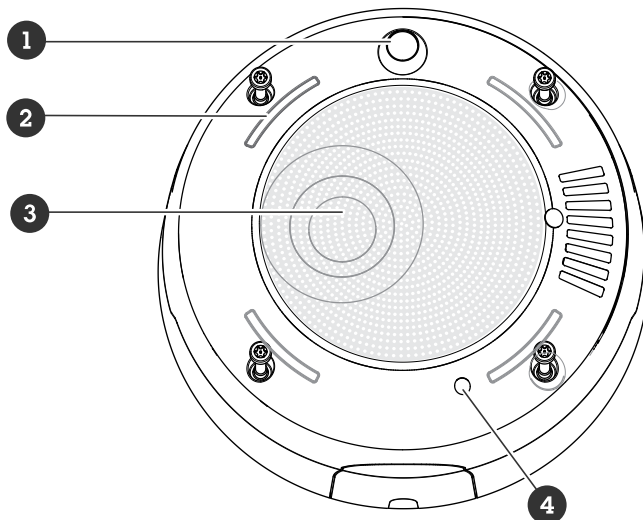
Um sich über alle Funktionen und Einstellungen zu informieren, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, rufen Sie die *Hilfe zur Weboberfläche von AXIS OS* auf.

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 32*.

Mikrofonschalter

Zur Einbaulage des Mikrofonschalters, siehe *Produktübersicht, on page 26*.

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

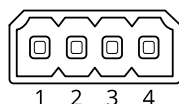
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

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

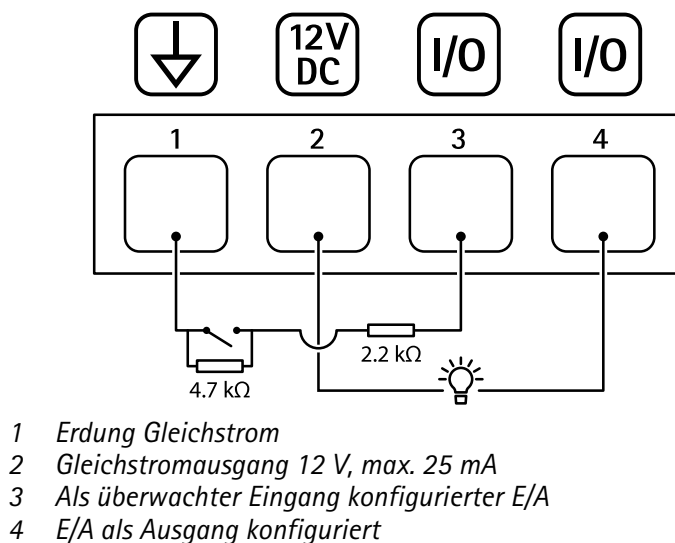
Überwachter Eingang – Ermöglicht das Erfassen von Manipulation an einem digitalen Eingang.

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

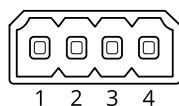


Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	 Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 25 mA
Konfigurierbar (Ein- 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:

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:

- zweiadrigter RS485-Halbduplex-Anschluss
- vieradriger RS485-Vollduplex-Anschluss
- zweiadrigter 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

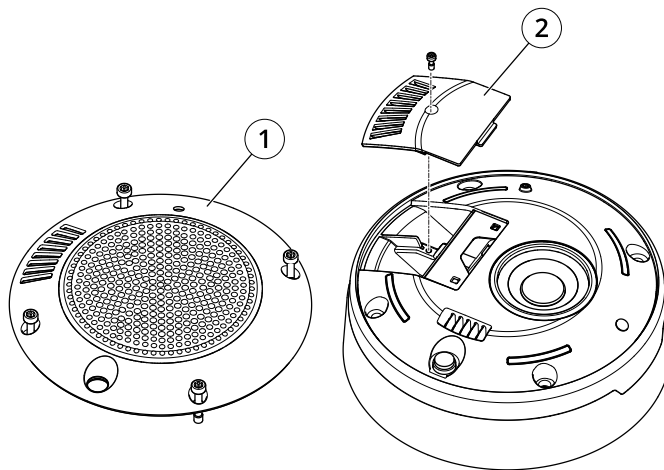
Sie können Ihr Gerät mit lauwarmem Wasser reinigen.

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 <code>ping</code> und die IP-Adresse des Geräts ein): - Wenn Sie <code>Reply from <IP address>: bytes=32; time=10...</code> 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 <code>Request timed out</code> 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 <code>http</code> oder <code>https</code> 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 32.

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 NO_x benötigen Zeit, um wirksam zu sein. Siehe *Kalibrierung für den ersten Betrieb 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.

Cybersicherheit

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

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

Schwachstellen-Management

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

Sicherheitsbenachrichtigungen

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

Sicherer Produktlebenszyklus

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

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

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

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

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

T10222990_de

2026-07 (M6.2)

© 2025 – 2026 Axis Communications AB