

AXIS D4200-VE Network Strobe Speaker

Inhalt

Lösungsübersicht	4
.....	4
Installation	5
Funktionsweise.....	6
.....	6
Das Gerät im Netzwerk ermitteln	6
Unterstützte Browser.....	6
Weboberfläche des Geräts öffnen	6
Administratorkonto erstellen	6
Sichere Kennwörter	7
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.	7
Ihr Gerät konfigurieren	8
Ein Profil konfigurieren	8
Ein Profil mit benutzerdefinierter Audiodatei für die Sirene konfigurieren.....	8
Ein Profil importieren oder exportieren	8
Direktes SIP (P2P) einrichten	9
SIP über einen Server (PBX) einrichten	9
Remote-Lautsprechertests kalibrieren und ausführen	10
Einrichten von Regeln für Ereignisse.....	10
Lösen Sie eine Aktion aus	11
Profil starten, wenn ein Alarm ausgelöst wird	11
Profil über SIP starten	11
Mehrere Profile über SIP-Erweiterungen steuern.....	12
Zwei Profile mit unterschiedlichen Prioritäten ausführen	12
Einen Stroboskop-Lautsprecher über HTTP POST bei Bewegungserkennung durch die Kamera aktivieren	13
Einen Stroboskop-Lautsprecher über virtuellen Eingang bei Bewegungserkennung durch die Kamera aktivieren	14
Stroboskop-Lautsprecher über MQTT aktivieren, wenn die Kamera Bewegung erkennt	15
Senden einer E-Mail, wenn ein Lautsprechertest fehlschlägt	17
Bei Auslösen eines Alarms benutzerdefinierten Clip wiedergeben.....	18
Audio mit DTMF anhalten.....	19
Audio für eingehende SIP-Anrufe einrichten.....	19
Weboberfläche	21
Mehr erfahren	22
Session Initiation Protocol (SIP)	22
Peer-to-Peer SIP (P2PSIP).....	22
Private Branch Exchange (PBX)	22
NAT-Traversal	23
Analysefunktionen und Anwendungen.....	23
AXIS Audio Analytics.....	23
InformaCast®.....	24
Technische Daten.....	25
Produktübersicht.....	25
LED-Anzeigen	26
Einschub für SD-Speicherkarte.....	27
Tasten.....	27
Steuertaste	27
Mikrofonschalter	27
Anschlüsse	27
Netzwerk-Anschluss	27
Audioanschluss	27
E/A-Anschluss.....	28

Namen von Lichtmustern	29
Namen von Klangmustern	30
Gerät reinigen	31
Fehlerbehebung	32
Zurücksetzen auf die Werkseinstellungen.....	32
Optionen für AXIS OS	32
Aktuelle AXIS OS-Version überprüfen	32
AXIS OS aktualisieren	32
Technische Probleme und mögliche Lösungen.....	33
Leistungsaspekte.....	36
Support.....	36
Cybersicherheit.....	37
Schwachstellen-Management	37
Sicherheitsbenachrichtigungen.....	37
Sicherer Produktlebenszyklus.....	37

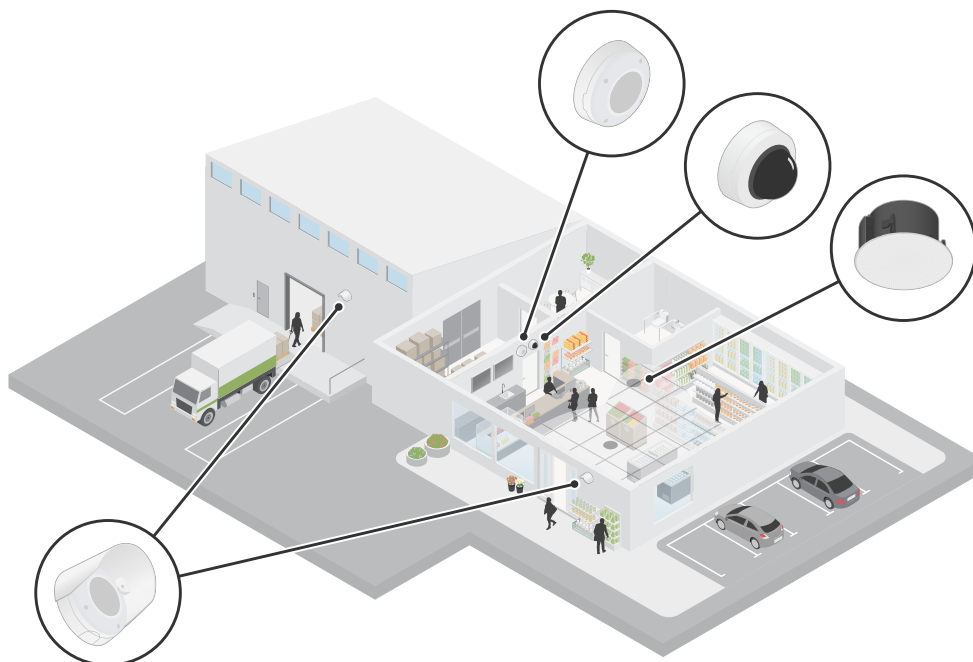
Lösungsübersicht

In diesem Handbuch wird beschrieben, wie Sie das Gerät für Ihr Audiosystem zugänglich machen und wie Sie das Gerät direkt über seine Schnittstelle konfigurieren können.

Wenn Sie eine Audio- oder Videoverwaltungssoftware verwenden, können Sie das Gerät mit dieser Software konfigurieren. Für die Steuerung Ihres Audiosystems steht die folgende Management-Software zur Verfügung:

- **AXIS Audio Manager Edge** – Audioverwaltungs-Software für kleine Systeme. Ist auf allen Audiogeräten mit der Firmware 10.0 oder höher vorinstalliert.
 - *AXIS Audio Manager Edge – Benutzerhandbuch*
- **AXIS Audio Manager Pro** – Fortgeschrittene Audioverwaltungs-Software für große Systeme.
 - *AXIS Audio Manager Pro – Benutzerhandbuch*
- **AXIS Camera Station Pro** – Erweiterte Videoverwaltungs-Software für große Systeme.
 - *Benutzerhandbuch zu AXIS Camera Station Pro*

Weitere Informationen hierzu finden Sie unter *Audioverwaltungssoftware*.



Installation

Wichtig

Installieren Sie den Stroboskop-Lautsprecher und die angeschlossenen Geräte nicht in einem Umkreis von weniger als 3 m von der Mitte von Gleisanlagen.

Dieses Video zeigt die Installation des AXIS D4200-VE Network Strobe Speaker an einem Beispiel.



Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

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 6.

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 7.
- 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 Gerätekenntwort 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.

Ihr Gerät konfigurieren

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 8*.
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 9*.

Remote-Lautsprechertests kalibrieren und ausführen

Mit dem Lautsprechertest kann von einem entfernten Standort aus überprüft werden, ob ein Lautsprecher wie vorgesehen funktioniert. Der Lautsprecher führt den Test durch, indem er eine Reihe von Testsignalen abspielt, die vom eingebauten Mikrofon registriert werden. Bei jeder Durchführung des Tests werden die registrierten Werte mit den Werten verglichen, die während der Kalibrierung registriert wurden.

Hinweis

Der Test muss in der montierten Position am Aufstellungsort kalibriert werden. Wenn der Lautsprecher bewegt wird oder sich die lokale Umgebung verändert (eine Wand wird gebaut/entfernt), muss der Lautsprecher erneut kalibriert werden.

Es wird empfohlen, dass sich während der Kalibrierung eine Person am Standort befindet, um zu überprüfen, dass die Testtöne nicht gedämpft klingen und sich keine Hindernisse im Klangradius des Lautsprechers befinden.

1. Wechseln Sie zu Geräteschnittstelle > **Audio > Speaker test (Audio > Lautsprechertest)**.
2. Klicken Sie zum Kalibrieren des Audio-Geräts auf **Calibrate (Kalibrieren)**.

Hinweis

Sobald das Axis Produkt kalibriert ist, kann der Lautsprechertest jederzeit durchgeführt werden.

3. Zum Starten des Lautsprechertests klicken Sie auf **Run the test (Test ausführen)**.

Hinweis

Die Kalibrierung kann auch durch Drücken der Steuertaste auf dem physikalischen Gerät ausgeführt werden. Unter *Produktübersicht, on page 25* können Sie die Steuertaste identifizieren.

Einrichten von Regeln für Ereignisse

Sie können Regeln erstellen, damit das Gerät beim Auftreten bestimmter Ereignisse Aktionen ausführt. Eine Regel besteht aus Bedingungen und Aktionen. Die Bedingungen können verwendet werden, um die Aktionen auszulösen. So kann das Gerät beispielsweise einen Audioclip nach einem Zeitplan oder bei Eingang eines Anrufs abspielen oder eine E-Mail senden, wenn das Gerät die IP-Adresse ändert.

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.

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.

Einen Stroboskop-Lautsprecher über HTTP POST bei Bewegungserkennung durch die Kamera aktivieren

In diesem Beispiel wird erläutert, wie Sie eine Kamera mit dem Stroboskop-Lautsprecher verbinden und in diesen ein Profil für die Erkennung einer Bewegung durch die in der Kamera installierte Anwendung AXIS Motion Guard aktivieren.

Vorbereitungen:

- Erstellen Sie im Stroboskop-Lautsprecher einen neuen Benutzer mit Bediener- oder Administratorenrolle.
- Erstellen Sie im Stroboskop-Lautsprecher ein Profil mit der Bezeichnung: „Strobe speaker profile“ (Profil Stroboskop-Lautsprecher).
- 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:** Stroboskop-Lautsprecher
 - **Typ:** HTTP
 - **URL:** `http://<IPaddress>/axis-cgi/siren_and_light.cgi`
Ersetzen Sie <IP-Adresse> durch die Adresse des Stroboskop-Lautsprechers.
 - Benutzername und Kennwort des neu erstellten Benutzers des Stroboskop-Lautsprechers.
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:** Stroboskop-Lautsprecher bei Bewegung aktivieren
 - **Condition (Bedingung):** Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)
 - **Aktion:** Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)
 - **Empfänger:** Stroboskop-Lautsprecher.

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": "Strobe speaker profile"  } }
```

Achten Sie darauf, unter **"profile" : <>**(Profil) dieselben Informationen wie bei der Erstellung des Profils im Stroboskop-Lautsprecher einzugeben, in diesem Fall also „Strobe speaker profile“.

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

4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:

- **Name:** Stroboskop-Lautsprecher bei 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)

- **Empfänger:** Stroboskop-Lautsprecher

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": "Strobe speaker profile"  } }
```

Achten Sie darauf, unter **"profile" : <>**(Profil) dieselben Informationen wie bei der Erstellung des Profils im Stroboskop-Lautsprecher einzugeben, in diesem Fall also „Strobe speaker profile“.

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

Einen Stroboskop-Lautsprecher über virtuellen Eingang bei Bewegungserkennung durch die Kamera aktivieren

In diesem Beispiel wird erläutert, wie Sie eine Kamera mit dem Stroboskop-Lautsprecher verbinden und in diesen ein Profil für die Erkennung einer Bewegung durch die in der Kamera installierte Anwendung AXIS Motion Guard aktivieren.

Vorbereitungen:

- Erstellen Sie im Stroboskop-Lautsprecher ein neues Konto mit Bediener- oder Administratorrechten.
- Erstellen Sie im Stroboskop-Lautsprecher ein Profil.
- 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 Stroboskop-Lautsprechers.
 - Konto und Kennwort des neu erstellten Benutzers des Stroboskop-Lautsprechers.
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 Stroboskop-Lautsprechers.
 - Konto und Kennwort des neu erstellten Benutzers des Stroboskop-Lautsprechers.
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 im Stroboskop-Lautsprecher eine Regel:

1. Rufen Sie in der Weboberfläche des Stroboskop-Lautsprechers **System > Events (Ereignisse)** auf 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 (Virtueller Eingang)
 - **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.

Stroboskop-Lautsprecher über MQTT aktivieren, wenn die Kamera Bewegung erkennt

In diesem Beispiel wird erklärt, wie Sie eine Kamera über MQTT mit dem Stroboskop-Lautsprecher verbinden und ein Profil im Stroboskop-Lautsprecher für die Erkennung von Bewegungen aktivieren.

Vorbereitungen:

- Erstellen Sie im Stroboskop-Lautsprecher ein Profil.
- 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 Stroboskop-Lautsprecher ein:

1. Gehen Sie in der Weboberfläche des Stroboskop-Lautsprechers 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 im Stroboskop-Lautsprecher eine Regel 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 **Ringling (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 **Ringling (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.

Mehr erfahren

Session Initiation Protocol (SIP)

Das SIP (Session Initiation Protocol) wird zum Einrichten, Warten und Beenden von VoIP-Anrufen verwendet. Sie können Anrufe zwischen zwei oder mehreren Teilnehmern, sogenannten SIP-Benutzeragenten, tätigen. Um einen SIP-Anruf zu tätigen, können Sie z. B. SIP-Telefone, Softphones oder SIP-fähige Axis Geräte verwenden.

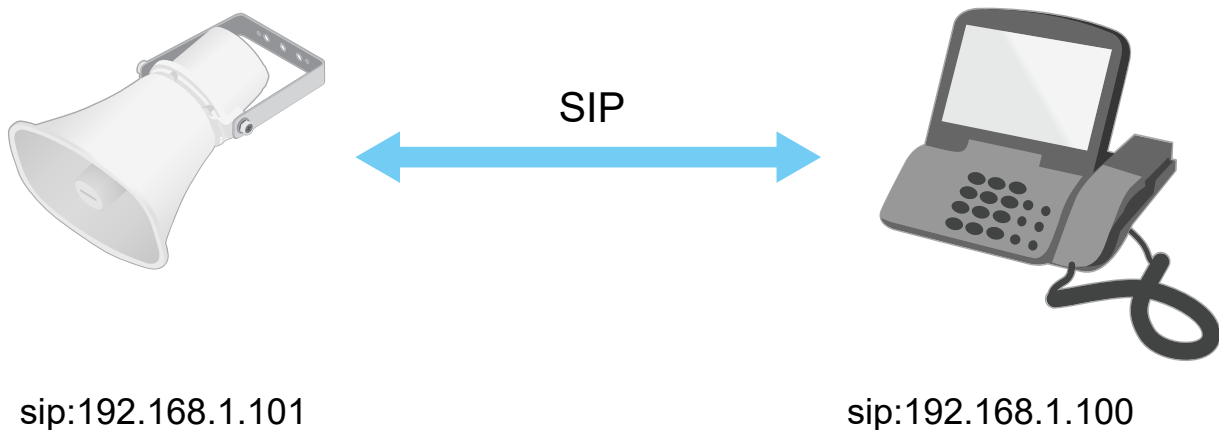
Die eigentlichen Audio- bzw. Videoübertragungen werden zwischen den SIP-Benutzeragenten mit einem Transportprotokoll, wie z. B. RTP (Real-Time Transport Protocol), ausgetauscht.

Sie können Anrufe in lokalen Netzwerken über ein Peer-to-Peer-Setup, oder netzwerkübergreifend mit einer PBX-Anlage tätigen.

Peer-to-Peer SIP (P2PSIP)

Die einfachste Art der SIP-Kommunikation findet direkt zwischen zwei oder mehr SIP-Benutzeragenten statt. Dies wird als Peer-to-Peer-SIP (P2PSIP) bezeichnet. Wenn dies in einem lokalen Netzwerk stattfindet, sind nur die SIP-Adressen der Benutzeragenten erforderlich. In diesem Fall ist eine typische SIP-Adresse `sip:<local-ip>`.

Beispiel:



Sie können ein SIP-fähiges Telefon so einrichten, dass ein Audiogerät im selben Netzwerk über ein Peer-to-Peer-SIP-Setup angerufen wird.

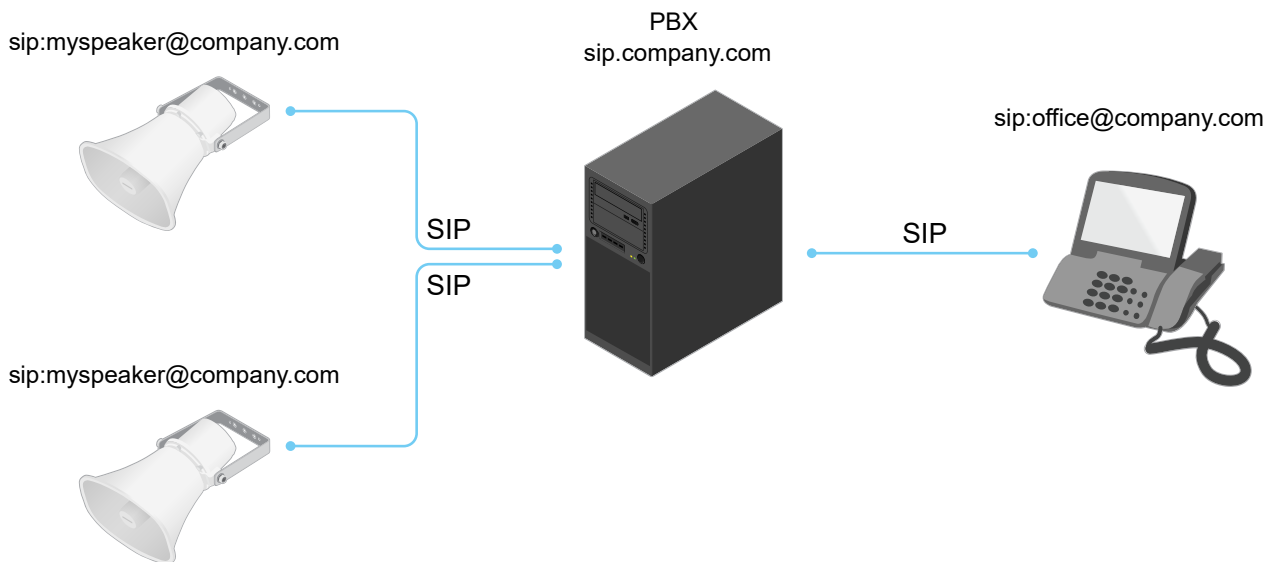
Private Branch Exchange (PBX)

Wenn Sie SIP-Anrufe außerhalb Ihres lokalen IP-Netzwerks tätigen, kann eine PBX (Private Branch Exchange) als zentraler Hub fungieren. Die Hauptkomponente einer PBX ist ein SIP-Server, der auch als SIP-Proxy oder Registrar bezeichnet wird. Eine PBX funktioniert wie eine herkömmliche Telefonzentrale, die den aktuellen Status des Clients anzeigt und beispielsweise Rufweiterleitungen, Voicemail und Weiterleitungen zulässt.

Der PBX-SIP-Server kann lokal oder extern eingerichtet werden. Er kann im Intranet oder durch einen Drittanbieter gehostet werden. Wenn Sie SIP-Anrufe zwischen Netzwerken tätigen, werden Anrufe über einen Satz von PBX-Anlagen weitergeleitet, die den Standort der zu erreichenden SIP-Adresse abfragen.

Jeder SIP-Benutzer wird bei der Nebenstellenanlage registriert und kann dann die anderen über die entsprechende Durchwahl erreichen. In diesem Fall ist eine typische SIP-Adresse `sip:<user>@<domain>` oder `sip:<user>@<registrar-ip>`. Die SIP-Adresse ist unabhängig von der jeweiligen IP-Adresse, und die PBX ermöglicht den Zugriff auf das Gerät, solange es für die PBX registriert ist.

Beispiel:



NAT-Traversal

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

Hinweis

Der Router muss NAT-Traversal und UPnP® unterstützen.

Die Protokolle von NAT Traversal können einzeln oder in verschiedenen Kombinationen verwendet werden, die sich nach der Netzwerkkumgebung 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 Axis Produkte erkennen, ob sie sich hinter einer NAT oder Firewall befinden. Zudem werden mit diesem Protokoll öffentlich zugewiesene 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. Die TURN-Server-Adresse und die Anmeldedaten eingeben.

Analysefunktionen und Anwendungen

Mit den Analysefunktionen und Anwendungen können Sie den Funktionsumfang Ihres Axis Geräts erweitern. Die AXIS Camera Application Platform (ACAP) ist eine offene Plattform, die es anderen Anbietern ermöglicht, Analysefunktionen und andere Anwendungen für Axis Geräte zu entwickeln. Anwendungen können auf dem Gerät vorinstalliert und kostenlos oder für eine Lizenzgebühr heruntergeladen werden.

Benutzerhandbücher zu Axis Analysefunktionen und Anwendungen finden Sie auf help.axis.com.

AXIS Audio Analytics

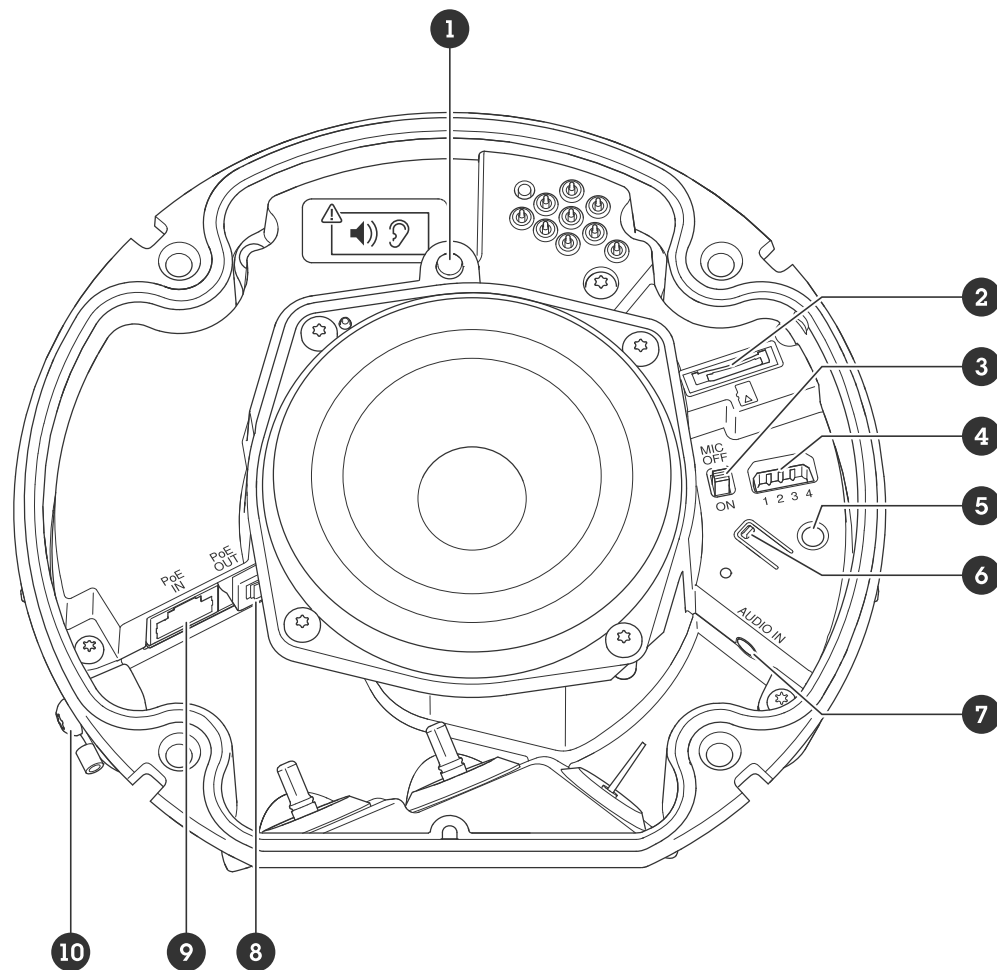
AXIS Audio Analytics erfasst eine plötzliche Zunahme der Lautstärke sowie bestimmte Töne wie Schreie oder Rufe innerhalb der Reichweite des Geräts, auf dem die Anwendung installiert ist. Diese Erfassungen können so konfiguriert werden, dass sie eine Reaktion auslösen, z. B. das Starten einer Videoaufzeichnung, das Abspielen einer Audionachricht oder das Alarmieren des Sicherheitspersonals. Mehr zur Funktionsweise der Anwendung erfahren Sie im *Benutzerhandbuch zu AXIS Audio Analytics*.

InformaCast®

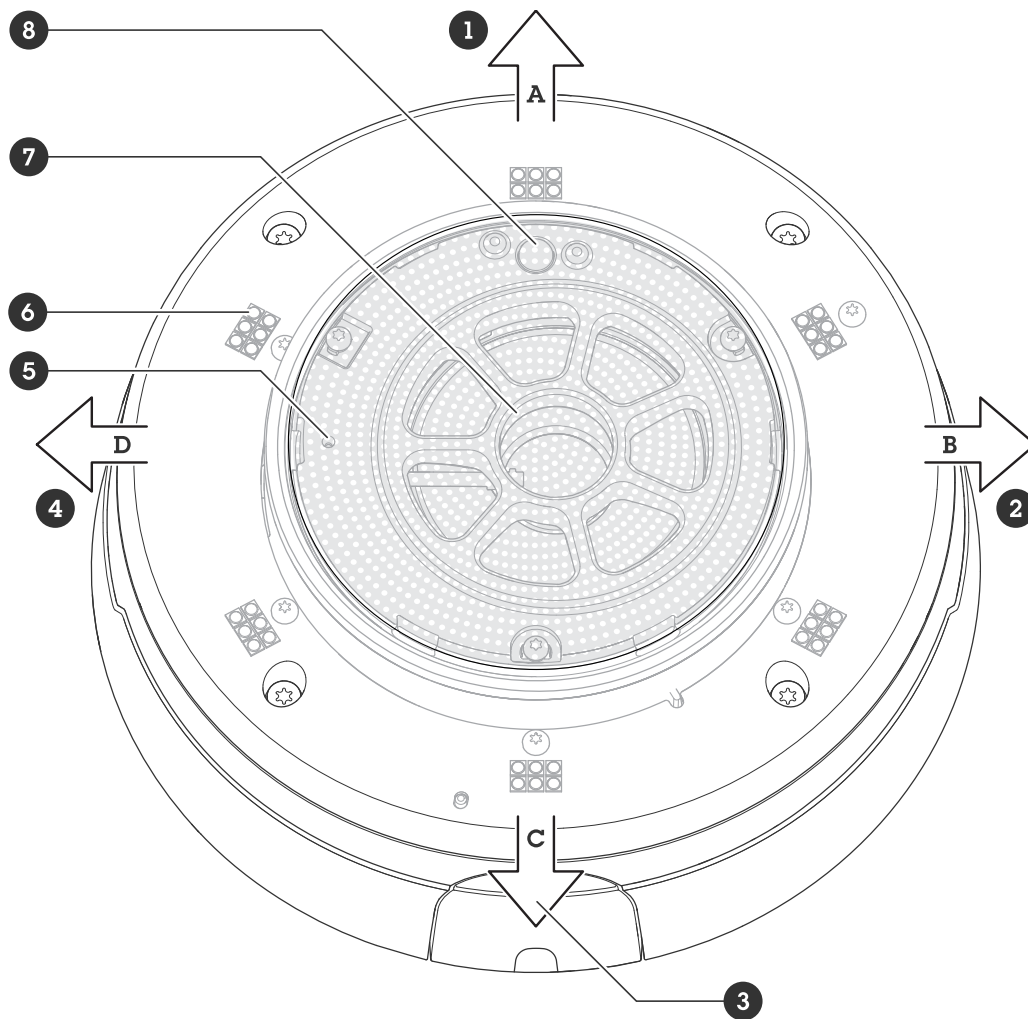
InformaCast ist eine Plattform, die es Ihnen ermöglicht, Notfallbenachrichtigungen zu senden und über die in Ihrer Organisation bereits vorhandenen Kanäle zu auszugeben, einschließlich der Axis Netzwerklautsprecher. Das InformaCast-System für Massenbenachrichtigungen liefert in Ihrer gesamten Einrichtung Alarme mit aufsehenerregenden Audiosignalen. Weitere Informationen über die Anwendung finden Sie unter *AXIS Lautsprecherfunktion für Singlewire InformaCast*.

Technische Daten

Produktübersicht



- 1 Audio-LED
- 2 Einschub für microSD-Speicherkarte
- 3 Mikrofonswitch
- 4 E/A-Anschluss
- 5 Status-LED
- 6 Steuertaste
- 7 Audioanschluss
- 8 Netzwerk-Anschluss (PoE-Ausgang)
- 9 Netzwerk-Anschluss (PoE IN)
- 10 Erdungsschraube



- 1 Beleuchtungsrichtung A
- 2 Beleuchtungsrichtung B
- 3 Beleuchtungsrichtung C
- 4 Beleuchtungsrichtung D
- 5 Internes Mikrofon
- 6 Signal-LEDs
- 7 Lautsprecher
- 8 Audio-LED

LED-Anzeigen

Status-LED	Anzeige
Aus	Anschluss und Normalbetrieb.
Grün	Leuchtet bei Normalbetrieb nach Abschluss des Startvorgangs 10 Sekunden lang grün.
Gelb	Leuchtet beim Einschalten, beim Wiederherstellen der werksseitigen Standardeinstellungen bzw. beim Zurücksetzen von Einstellungen konstant.

Einschub für SD-Speicherkarte

HINWEIS

- Gefahr von Schäden an der SD-Karte Benutzen Sie beim Einsetzen oder Entfernen der SD-Karte keine scharfen Werkzeuge oder Gegenstände aus Metall und wenden Sie keine übermäßige Kraft an. Setzen Sie die Karte per Hand ein. Das Gleiche gilt für das Entfernen.
- Gefahr von Datenverlust und beschädigten Aufzeichnungen. Entfernen Sie vor dem Herausnehmen die SD-Karte von der Weboberfläche des Geräts. Die SD-Karte darf nicht entfernt werden, während das Produkt in Betrieb ist.

Für Empfehlungen zu SD-Karten siehe axis.com.



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

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Den Lautsprechertest kalibrieren. Die Steuertaste drücken und wieder loslassen. Ein Testton wird abgespielt.
- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 32*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Um eine Verbindung herzustellen, drücken Sie die Taste, lassen Sie sie los und warten Sie, bis die Status LED dreimal grün blinkt.

Mikrofonschalter

Zur Einbaulage des Mikrofonschalters, siehe *Produktübersicht, on page 25*.

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

Anschlüsse

Netzwerk-Anschluss

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

HINWEIS

Das Gerät muss mit einem abgeschirmten Netzkabel (STP) angeschlossen werden. Alle Kabel, die das Gerät mit dem Netzwerk-Switch verbinden, müssen dafür ausgelegt sein. Sicherstellen, dass die Netzwerk-Geräte gemäß den Anweisungen des Herstellers installiert werden. Informationen zu gesetzlichen Bestimmungen finden Sie in der Installationsanleitung auf www.axis.com.

Audioanschluss

- **Audioeingang** – 3,5 mm-Eingang für ein digitales Mikrofon, ein analoges Monomikrofon oder ein Line-In-Monosignal (linker Kanal wird aus einem Stereosignal verwendet).



Audioeingang

1 Spitze	2 Ring	3 Hülse
Unsymmetrisches Mikrofon (mit oder ohne Elektretspeisung) oder Leitung	Elektretspeisung, sofern ausgewählt	Masse
Digitales Signal	Klingelstrom, sofern ausgewählt	Masse

Hinweis

Die maximale Länge des angeschlossenen Kabels beträgt 30 m (98,4 ft).

E/A-Anschluss

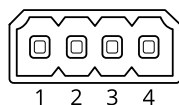
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

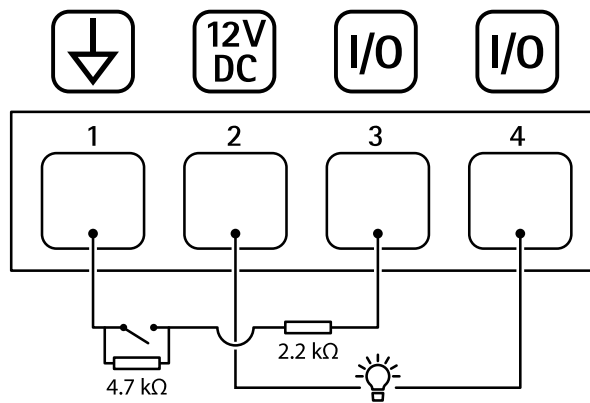
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

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 = 50 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. 50 mA
- 3 Als überwachter Eingang konfigurierter E/A
- 4 E/A als Ausgang konfiguriert

Hinweis

Die maximale Länge des angeschlossenen Kabels beträgt 30 m (98,4 ft).

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
Richtung A
Richtung B
Richtung C
Richtung D
Drehen
Zufällig
Rotierend

Namen von Klangmustern

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 und milder, nicht scheuernder Seife reinigen.

HINWEIS

- Aggressive Chemikalien können das Gerät beschädigen. Verwenden Sie zur Reinigung Ihres Geräts keine chemischen Substanzen wie Fensterreiniger oder Aceton.
 - Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken führen kann.
1. Verwenden Sie eine Druckluft-Dose zum Entfernen von Staub und Schmutz von dem Gerät.
 2. Reinigen Sie das Gerät ggf. mit einem weichen, mit lauwarmem Wasser und lauwarmer, nicht scheuernder Seife angefeuchteten Mikrofasertuch.
 3. Um eventuelle Reinigungsmittelrückstände zu entfernen, wischen Sie das Gerät mit einem weichen, mit lauwarmem Wasser angefeuchteten Mikrofasertuch ab.
 4. Trocknen Sie das Gerät mit einem sauberen, nicht scheuernden Tuch ab, um Flecken zu vermeiden.

Weitere Informationen zur Reinigung von Axis Geräten finden Sie im Whitepaper *Chemische Beständigkeit gegenüber gängigen Reinigungsmitteln*.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

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

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht, on page 25*.
3. Halten Sie die Steuertaste 10 Sekunden gedrückt, bis die Status-LED zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
 - Geräte mit AXIS OS 12.0 oder höher: Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
 - Geräte mit AXIS OS 11.11 oder niedriger: 192.168.0.90/24
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

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

Optionen für AXIS OS

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

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

Aktuelle AXIS OS-Version überprüfen

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

So überprüfen Sie die aktuelle AXIS OS-Version:

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

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten

Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.

- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Leitfaden zum Lebenszyklus: Upgrade-Pfad*.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

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

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

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

Probleme nach der AXIS OS-Aktualisierung

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

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

- Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
- Die IP-Adresse wird unter Umständen von einem anderen Gerät verwendet. Zur Überprüfung:
 1. Trennen Sie das Axis Gerät vom Netzwerk.
 2. Geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein.
 3. Erscheint daraufhin `Reply from <IP address>: bytes=32; time=10...`, heißt das, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut.
 4. Wenn Sie `Request timed out` empfangen, bedeutet dies, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
- Es besteht unter Umständen ein Konflikt mit der IP-Adresse eines anderen Geräts im selben Subnetz. Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

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

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 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 können Sie manuell eine statische IP-Adresse zuweisen. Anweisungen dazu finden Sie auf *axis.com/support*.

Zertifikatfehler beim Verwenden von IEEE 802.1X

Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **Einstellungen > System > Datum und Uhrzeit**.

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 6*.

Externer Zugriff auf das Gerät ist nicht möglich

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

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

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

Probleme mit Audiodateien

Medienclip kann nicht hochgeladen werden

Folgende Audioclipformate werden unterstützt:

- au-Dateiformat, in μ -law codiert und mit 8 oder 16 kHz abtastiert.
- wav-Dateiformat, in PCM-Audio codiert. Codierung als 8- oder 16-Bit-Mono oder Stereo und eine Abtastrate von 8 bis 48 kHz werden unterstützt.
- mp3-Dateiformat, mono oder stereo, mit einer Bitrate von 64 bis 320 kHz und einer Abtastrate von 8 bis 48 kHz.

Medienclips werden in unterschiedlicher Lautstärke abgespielt.

Eine Sounddatei wird mit einer bestimmten Verstärkung aufgezeichnet. Wenn bei der Erstellungen Ihrer Audioclips verschiedenen Verstärkungsarten eingestellt waren, werden sie in unterschiedlicher Lautstärke abgespielt. Stellen Sie sicher, dass Sie Clips mit derselben Verstärkung verwenden.

Probleme mit MQTT

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

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

In einigen Fällen stellt der Server/Broker möglicherweise keinen bestimmten Port für die MQTT-Kommunikation bereit. Möglicherweise kann MQTT über einen Port verwendet werden, der normalerweise für HTTP/HTTPS-Datenverkehr verwendet wird.

- Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll.
- Wenn der Server/Broker ALPN unterstützt, kann darüber verhandelt werden, ob MQTT über einen offenen Port (wie z. B. 443) verwendet werden soll. Prüfen Sie in Rücksprache mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.

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

Probleme mit dem Ton

Das Gerät ist nicht so laut wie erwartet	Stellen Sie sicher, dass das Gerät richtig geschlossen ist und nichts das Horn oder Lautsprecherelement behindert.
--	--

Probleme mit dem Licht

Das Gerät leuchtet nicht so hell wie erwartet

Stellen Sie sicher, dass ein Netzteil der PoE-Klasse 4 verwendet wird.

Überprüfen Sie die Umgebungstemperatur des Geräts. Wenn das Gerät in einer Umgebung mit hohen Temperaturen installiert ist, wird das Licht automatisch gedämmt.

Leistungsaspekte

Achten Sie bei der Einrichtung Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die erforderliche Bandbreite (Bitrate) auswirken.

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

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Mehrere gleichzeitig ausgeführte ACAP-Anwendungen (AXIS Camera Application Platform) können die allgemeine Leistung beeinflussen.

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.

T10217687_de

2026-07 (M6.2)

© 2025 – 2026 Axis Communications AB