AXIS D4100-E Network Strobe Siren

Benutzerhandbuch

Inhalt

Installation 3
Erste Schritte 4
Das Gerät im Netzwerk ermitteln 4
Weboberfläche des Geräts öffnen 4
Übersicht über die Weboberfläche 5
Ihr Gerät konfigurieren 6
Wartungsmodus nach Installation der Sirene deaktivieren 6
Wartungsmodus aktivieren 6
Ein Profil konfigurieren 6
Ein Profil importieren oder exportieren 6
Direktes SIP (P2P) einrichten 6
SIP über einen Server (PBX) einrichten 7
Einrichten von Regeln für Ereignisse 8
Weitere Informationen 17
Session Initiation Protocol (SIP) 17
Peer-to-Peer SIP (P2PSIP) 17
Private Branch Exchange (PBX) 17
NAT-Traversal 17
Die Weboberfläche 19
Status 19
Übersicht 20
Profile 20
Apps 21
System 22
Wartung 40
Technische Daten 42
Produktübersicht 42
LED-Anzeigen 42
Tasten 42
Anschlüsse 43
Namen von Lichtmustern 44
Maximaler Schalldruckpegel 45
Empfehlungen zur Reinigung 46
Fehlerbehebung 47
Zurücksetzen auf die Werkseinstellungen 47
Firmware-Optionen 47
Aktuelle Firmware überprüfen 47
Firmware aktualisieren 47
Technische Fragen, Hinweise und Lösungen 48
Leistungsaspekte 50
Support 50

Installation

Installation

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

help.axis.com/?&piaId=62021&section=install

Erste Schritte

⚠WARNUNG

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

Das Gerät im Netzwerk ermitteln

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

TUm die Weboberfläche von AXIS OS mit iOS 15 oder iPadOS 15 zu verwenden, deaktivieren Sie unter **Settings (Einstellungen) > Safari > Advanced (Erweitert) > Experimental Features (Experimentelle Funktionen) die Option NSURLSession Websocket.*

Weboberfläche des Geräts öffnen

1. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Erstellen Sie ein Administratorenkonto auf Seite 4*.

Erstellen Sie ein Administratorenkonto

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Kennwort ein. Siehe *Sichere Kennwörter auf Seite 4*.
3. Geben Sie das Kennwort erneut ein.
4. Klicken Sie auf **Add user (Benutzer hinzufügen)**.

Sichere Kennwörter

Wichtig

Das voreingestellte Kennwort wird vom Axis Gerät unverschlüsselt über das Netz gesendet. Um das Gerät zu schützen, nach dem ersten Anmelden eine sichere und verschlüsselte HTTPS-Verbindung einrichten und dann das Kennwort ändern.

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.
- Das Kennwort regelmäßig und mindestens jährlich zu ändern.

Übersicht über die Weboberfläche

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

Weboberfläche des Axis Geräts

Ihr Gerät konfigurieren

Wartungsmodus nach Installation der Sirene deaktivieren

⚠VORSICHT

Zum Schutz des Installateurs vor Hörschäden und Blendschäden durch helles Licht wird eine Installation des Geräts bei aktiviertem Wartungsmodus empfohlen.

Wenn Sie das Gerät zum ersten Mal installieren, ist der Wartungsmodus standardmäßig aktiviert. Wenn sich das Gerät im Wartungsmodus befindet, ertönt keine Sirene, und das Licht zeigt weiß pulsierende Lichtmuster.

Wechseln Sie zu **Overview (Übersicht)** > **Maintenance (Wartung)**, um den Wartungsmodus (**Maintenance mode**) wieder auszuschalten.

Wartungsmodus aktivieren

Wechseln Sie zur Wartung Ihres Geräts zu **Overview (Übersicht)** > **Maintenance (Wartung)**, und aktivieren Sie Option **Maintenance mode (Wartungsmodus)**. Die normalen Licht- und Sirenenaktivitäten werden anschließend angehalten.

Ein Profil konfigurieren

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

Erstellen eines neuen Profils:

1. Wechseln Sie zu **Profiles (Profile)**, und klicken Sie auf + **Create (Anlegen)**.
2. Geben Sie unter **Name** und **Description** einen Namen bzw. eine Beschreibung ein.
3. Wählen Sie unter **Light (Licht)** und **Siren (Sirene)** die Einstellungen aus, die Sie in Ihr Profil übernehmen möchten.
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 importieren oder exportieren

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

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

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

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

Direktes SIP (P2P) einrichten

Verwenden Sie Peer-to-Peer, wenn die Kommunikation zwischen wenigen Benutzern innerhalb desselben IP-Netzwerks erfolgt und keine zusätzlichen Funktionen erforderlich sind, die von einem PBX-Server bereitgestellt werden können. Weitere Informationen zur Funktionsweise von P2P finden Sie unter *Peer-to-Peer SIP (P2PSIP) auf Seite 17*.

Weitere Informationen zu den Einstellungsoptionen finden Sie unter *SIP auf Seite 35*.

1. Wechseln Sie zu **System** > **SIP** > **SIP settings** (System > SIP > SIP-Einstellungen), und wählen Sie **Enable SIP (SIP aktivieren)**.
2. Um die Annahme eingehender Anrufe durch das Gerät zu erlauben, wählen Sie die Option **Allow incoming calls (Eingehende Anrufe erlauben)** aus.
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. Die Standardportnummer ist 5060. Bei Bedarf eine andere Portnummer eingeben.
   - **TLS port (TLS-Port)** – Der für verschlüsselte SIP-Kommunikation genutzte Netzwerk-Port. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Die Standardportnummer ist 5061. Bei Bedarf eine andere Portnummer eingeben.
   - **RTP start port (RTP-Startport)** – Den Port für den ersten RTP-Mediastream eines SIP-Anrufs eingeben. Der Standardstartport für Medienübertragungen ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten 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 auf Seite 17*.

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. Klicken Sie auf **Save (Speichern)**.

SIP über einen Server (PBX) einrichten

Verwenden Sie einen PBX-Server, wenn die Kommunikation zwischen einer unbegrenzten Anzahl von Benutzern innerhalb und außerhalb des IP-Netzwerks erfolgen soll. Je nach PBX-Anbieter können dem Setup zusätzliche Funktionen hinzugefügt werden. Weitere Informationen zur Funktionsweise von P2P finden Sie unter *Private Branch Exchange (PBX) auf Seite 17*.

Weitere Informationen zu den SIP-Einstellungsoptionen finden Sie unter *SIP auf Seite 35*.

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:
   - Benutzer-ID
   - Domain
   - Kennwort
   - Authentifizierungs-ID
   - Caller-ID (Anrufer-ID)
   - Registrator
   - RTP-Startport
2. Um ein neues Konto hinzuzufügen, gehen 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. Klicken Sie auf **Save (Speichern)**.
7. Die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einrichten. Für weitere Informationen dazu siehe *Direktes SIP (P2P) einrichten auf Seite 6* .

Einrichten von Regeln für Ereignisse

Weitere Informationen finden Sie in unserer Anleitung *Erste Schritte mit Regeln für Ereignisse*.

Lösen Sie eine Aktion aus

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

Hinweis

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

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** > **Normalposition** und klicken Sie auf **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 in der Liste der Bedingungen **E/A** > **Digitaler Eingang**.
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 Videostreamprofil aus, das Sie starten möchten.
7. Klicken Sie auf **Save (Speichern)**.

Profil über SIP starten

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

SIP aktivieren:

1. Rufen Sie **System** > **SIP** > **SIP settings (SIP-Einstellungen)** auf.
2. Wählen Sie **Enable SIP (SIP aktivieren)** und **Allow incoming calls (Eingehende Anrufe zulassen)**.
3. Klicken Sie auf **Save (Speichern)**.

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 **Bei aktiver Regel Licht- und Sirenenprofil ausführen**.
6. Wählen Sie das Videostreamprofil aus, das Sie starten möchten.
7. Klicken Sie auf **Save (Speichern)**.

Mehrere Profile über SIP-Erweiterungen steuern

Aktivieren Sie SIP:

1. Wechseln Sie zu **System** > **SIP** > **SIP settings** (System > SIP > SIP-Einstellungen).
2. Wählen Sie **Enable SIP (SIP aktivieren)** und **Allow incoming calls (Eingehende Anrufe zulassen)**.
3. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie eine Regel zum Starten eines Profils:

1. Wechseln Sie zu **System** > **Events** (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** die Anweisung **sip:[Ext]@[IP address]** ein, wobei [Ext] die für das Profil verwendete Erweiterung und [IP adress] die IP-Adresse des Geräts ist. Beispiel: **sip:1001@192.168.0.90**.
7. Wählen Sie in der Aktionsliste **Light and Siren** > **Run light and siren profile** (Licht und Sirene > Licht- und Sirenenprofil ausführen) aus.
8. Wählen Sie das Profil aus, das Sie starten möchten.
9. Wählen Sie die Aktion **Start (Starten)** aus.
10. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie eine Regel zum Stoppen eines Profils:

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

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

Zwei Profile mit unterschiedlichen Prioritäten ausführen

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

Hinweis

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

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

Profile erstellen:

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

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.

3. Wählen Sie in der Liste der Bedingungen **E/A** > **Digitaler Eingang**.
4. Wählen Sie einen Port.
5. Wählen Sie in der Liste mit den Aktionen **Bei aktiver Regel Licht- und Sirenenprofil ausführen**.
6. Wählen Sie das Profil mit der höchsten Prioritätszahl aus.
7. Klicken Sie auf **Save (Speichern)**.
8. Gehen Sie zu **Profile** und starten Sie das Profil mit der niedrigsten Prioritätszahl.

Aktivieren einer Blitzsirene über einen virtuellen Eingang bei Bewegungserkennung durch die Kamera

In diesem Beispiel wird erläutert, wie Sie eine Kamera mit der Blitzsirene verbinden und in der Blitzsirene ein Profil aktivieren, wenn die in der Kamera installierte Anwendung AXIS Motion Guard eine Bewegung erkennt.

Bevor Sie beginnen:

- Erstellen Sie in der Blitzsirene einen neuen Benutzer mit der Rolle Bediener oder Administrator.
- Erstellen Sie ein Profil in der Blitzsirene.
- 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://<IPaddress>/axis-cgi/virtualinput/activate.cgi

     Ersetzen Sie <IPaddress> durch die Adresse der Blitzsirene.
   - Benutzername und Kennwort des neu erstellten Benutzers der Blitzsirene.
3. Klicken Sie auf **Test**, um sicherzustellen, dass alle Daten gültig sind.
4. Klicken Sie auf **Save (Speichern)**.
5. Fügen Sie einen zweiten Empfänger mit den folgenden Informationen hinzu:
   - **Name**: Virtuellen Port deaktivieren
   - **Typ**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi

     Ersetzen Sie <IPaddress> durch die Adresse der Blitzsirene.
   - Benutzername und Kennwort des neu erstellten Benutzers der Blitzsirene.
6. Klicken Sie auf **Test (Testen)**, um sicherzustellen, dass alle Daten gültig sind.
7. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie in der Kamera zwei Regeln:

1. Rufen Sie **Rules (Regeln)** auf und fügen Sie eine Regel hinzu.

2. Geben Sie folgende Informationen ein:
    - **Name**: Virtuellen E/A1 aktivieren
    - **Condition (Bedingung)**: **Applications > Motion Guard: Camera profile (Anwendungen > Motion Guard: Kameraprofil)**
    - **Action (Aktion)**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
    - **Recipient (Empfänger)**: **Virtuellen Port aktivieren**
    - **Query-String-Suffix**: schemaversion=1&port=1
3. Klicken Sie auf **Save (Speichern)**.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
    - **Name**: Virtuellen E/A1 deaktivieren
    - **Condition (Bedingung)**: **Applications > Motion Guard: Camera profile (Anwendungen > Motion Guard: Kameraprofil)**
    - Wählen Sie **Invert this condition (Bedingungen umkehren)** aus.
    - **Action (Aktion)**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
    - **Recipient (Empfänger)**: **Virtuellen Port deaktivieren**
    - **Query-String-Suffix**: schemaversion=1&port=1
5. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie in der Blitzsirene eine Regel:

1. Rufen Sie in der Geräteschnittstelle der Blitzsirene **System > Events (System > Ereignisse)** auf und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
    - **Name**: Auslöser am virtuellen Eingang 1
    - **Condition (Bedingung)**: **E/A > Virtueller Eingang**:
    - **Port**: **1**
    - **Action (Aktion)**: **Licht und Sirene > Bei aktiver Regel Licht- und Sirenenprofil ausführen**
    - **Profil**: Wählen Sie das neu erstellte Profil
3. Klicken Sie auf **Save (Speichern)**.

Aktivieren einer Blitzsirene über HTTP POST bei Bewegungserkennung durch die Kamera

In diesem Beispiel wird erläutert, wie Sie eine Kamera mit der Blitzsirene verbinden und in der Blitzsirene ein Profil aktivieren, wenn die in der Kamera installierte Anwendung AXIS Motion Guard eine Bewegung erkennt.

Bevor Sie beginnen:

- Erstellen Sie in der Blitzsirene einen neuen Benutzer mit der Rolle „Bediener" oder „Administrator".
- Erstellen Sie in der Blitzsirene ein Profil mit dem Namen „Profil der Blitzsirene".
- Richten Sie AXIS Motion Guard in der Kamera ein und erstellen Sie ein Profil mit dem Namen „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**: Blitzsirene
   - **Typ**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/siren_and_light.cgi

     Ersetzen Sie <IPaddress> durch die Adresse der Blitzsirene.
   - Benutzername und Kennwort des neu erstellten Benutzers der Blitzsirene.
3. Klicken Sie auf **Test (Testen)**, um sicherzustellen, dass alle Daten gültig sind.
4. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie in der Kamera zwei Regeln:

1. Rufen Sie **Rules (Regeln)** auf und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Aktivieren der Sirene bei Bewegung
   - **Condition (Bedingung)**: **Applications > Motion Guard: Camera profile (Anwendungen > Motion Guard: Kameraprofil)**
   - **Action (Aktion)**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**
   - **Recipient (Empfänger)**: **Strobe siren (Blitzsirene)**.

     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 siren profile"     } }
```

Achten Sie darauf, unter **"profile" : <> („Profil" : <>)** dieselben Informationen wie bei der Erstellung des Profils in der Blitzsirene einzugeben, in diesem Fall also „Profil der Blitzsirene".

3. Klicken Sie auf **Save (Speichern)**.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
   - **Name**: Deaktivieren der Sirene bei Bewegung
   - **Condition (Bedingung)**: **Applications > Motion Guard: Camera profile (Anwendungen > Motion Guard: Kameraprofil)**
   - Wählen Sie **Invert this condition (Bedingungen umkehren)** aus.
   - **Action (Aktion)**: **Notifications > Send notification through HTTP (Benachrichtigungen > Benachrichtigung über HTTP senden)**

- **Recipient (Empfänger)**: **Strobe siren (Blitzsirene)**

  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 siren profile"     } }
```

Achten Sie darauf, unter **"profile" : <> („Profil" : <>)** dieselben Informationen wie bei der Erstellung des Profils in der Blitzsirene einzugeben, in diesem Fall also „Profil der Blitzsirene".

5. Klicken Sie auf **Save (Speichern)**.

Blitzsirene über MQTT aktivieren, wenn die Kamera Bewegung erkennt

In diesem Beispiel wird erläutert, wie Sie eine Kamera über MQTT mit der Blitzsirene verbinden und ein Profil in der Sirene aktivieren, wenn die in der Kamera installierte Anwendung AXIS Motion Guard eine Bewegung erkennt.

Bevor Sie beginnen:

- Erstellen Sie in der Blitzsirene ein Profil.
- Richten Sie einen MQTT-Broker ein, und rufen Sie die IP-Adresse, den Benutzernamen und das Kennwort des Brokers ab.
- Richten Sie AXIS Motion Guard in der Kamera ein.

Richten Sie den MQTT-Client in der Kamera ein:

1. Rufen Sie in der Geräteschnittstelle der Kamera **System > MQTT > MQTT client > Broker (System > MQTT > MQTT-Client > Broker)** auf und geben Sie folgende Informationen ein:
   - **Host**: IP-Adresse des Brokers
   - **Client-ID**: Zum Beispiel Kamera 1
   - **Protokoll**: Das Protokoll, auf das der Broker festgelegt ist
   - **Port**: Die vom Broker verwendete Portnummer
   - **Benutzername** und **Kennwort** des Brokers
2. Klicken Sie auf **Save (Speichern)** und anschließend auf **Connect (Verbinden)**.

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

1. Rufen Sie **System > Events > Rules (System > Ereignisse > Regeln)** auf und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Bewegung erkannt
   - **Bedingung**: **Anwendungen > Motion Alarm**
   - **Aktion**: **MQTT > MQTT-Meldung zu Veröffentlichung senden**:
   - **Thema**: Bewegung
   - **Nutzlast**: Ein
   - **QoS**: 0, 1 oder 2

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

Richten Sie den MQTT-Client in der Blitzsirene ein:

1. Rufen Sie in der Geräteschnittstelle der Blitzsirene **System > MQTT > MQTT client > Broker (System > MQTT > MQTT-Client > Broker)** auf und geben Sie folgende Informationen ein:
   - **Host**: IP-Adresse des Brokers
   - **Client-ID**: Sirene 1
   - **Protokoll**: Das Protokoll, auf das der Broker festgelegt ist
   - **Port**: Die vom Broker verwendete Portnummer
   - **Benutzername** und **Kennwort**
2. Klicken Sie auf **Save (Speichern)** und anschließend auf **Connect (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. Klicken Sie auf **Save (Speichern)**.

Erstellen Sie in der Blitzsirene eine Regel für MQTT-Abonnements:

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

3. Klicken Sie auf **Save (Speichern)**.

Weitere Informationen

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. Eine typische SIP-Adresse in diesem Fall ist `sip:<local-ip>`.

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.

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 Netzwerkumgebung richten.

- **ICE** – Das Protokoll ICE (Interactive Connectivity Establishment) erhöht die Chancen, den effizientesten Kommunikationspfad zwischen gleichrangigen Geräten zu finden. Mit dem Aktivieren von STUN und TURN werden die Chancen des ICE-Protokolls nochmals verbessert.
- **STUN** – STUN (Session Traversal Utilities for NAT) ist ein Client-Server-Netzwerkprotokoll, an dem 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. Die STUN-Server-Adresse eingeben, zum Beispiel eine IP-Adresse.

Weitere Informationen

- **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.

Die Weboberfläche

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

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Die Sprache ändern.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

- Informationen zum angemeldeten Benutzer.
- **Change account (Konto wechseln)**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
- **Log out (Abmelden)**: Melden Sie sich vom aktuellen Konto ab.

Das Kontextmenü enthält:

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

Status

Sicherheit

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

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

Zeitsynchronisierungsstatus

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

NTP settings (NTP-Einstellungen): Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Date and time (Datum und Uhrzeit)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich Firmwareversion und Seriennummer.

Upgrade firmware (Firmwareaktualisierung): Aktualisieren Sie die Firmware auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie eine Firmwareaktualisierung durchführen können.

Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

View details (Details anzeigen): Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port und PID/Process für jeden Client an.

Übersicht

Light status (Lichtstatus)

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

Sirenenstatus

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

Wartung

Maintenance mode (Wartungsmodus): Schalten Sie diesen Modus ein, um die Beleuchtung und die Sirenenaktivitäten während der Wartung des Geräts anzuhalten. Wenn Sie den Wartungsmodus einschalten, zeigt das Gerät ein weiß pulsierendes Lichtmuster in einem Dreieck und die Sirene ist still. Dies schützt den Installateur vor Hörschäden und blendend hellem Licht.

Wartung hat Priorität 11. Nur systemspezifische Aktivitäten mit höherer Priorität können den Wartungsmodus unterbrechen.

Der Wartungsmodus erfordert einen Neustart. Wenn Sie zum Beispiel die Zeit auf zwei Stunden festlegen, das Gerät deaktivieren und eine Stunde später neu starten, befindet sich das Gerät eine weitere Stunde im Wartungsmodus.

Bei einem standardmäßigen Reset kehrt das Gerät in den Wartungsmodus zurück.

Dauer

- **Kontinuierlich**: Wählen Sie diese Option aus, damit das Gerät so lange im Wartungsmodus bleibt, bis es ausgeschaltet wird.
- **Time (Uhrzeit)**: Wählen Sie mit dieser Option aus, wann der Wartungsmodus ausgeschaltet wird.

Integritätsprüfung

Check (Überprüfen): Überprüfen Sie den Gerätezustands, um sicherzustellen, dass Licht und Sirene funktionieren. Es schaltet jeden Lichtbereich nacheinander ein und gibt einen Testton ab, um zu prüfen, ob das Gerät einwandfrei funktioniert. Falls die Integritätsprüfung nicht bestanden wird, rufen Sie die Systemprotokolle auf, um weitere Informationen zu erhalten.

Profile

Profile

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

Create (Erstellen): Klicken Sie hierauf, um ein Profil zu erstellen.

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

Hinweis

Sie können nicht zwei Profile mit demselben Namen haben.

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

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

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

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

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

Sie können das Profil **Edit (bearbeiten)**, **Copy (kopieren)**, **Export (exportieren)** oder **Delete (löschen)**.

Apps

Add app (App hinzufügen): Installieren einer neuen App.

Find more apps (Weitere Apps finden): Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet.

Allow unsigned apps (Unsignierte Apps erlauben): Aktivieren Sie diese Option, um die Installation unsignierter Apps zu ermöglichen.

Allow root-privileged apps (Apps mit Root-Berechtigungen zulassen): Aktivieren Sie diese Option, um Apps mit Root-Berechtigungen uneingeschränkten Zugriff auf das Gerät zu ermöglichen.

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

Hinweis

Bei gleichzeitiger Ausführung mehrerer Apps kann die Leistung des Geräts beeinträchtigt werden.

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

Open (Öffnen): Auf die Anwendungseinstellungen zugreifen. Die verfügbaren Einstellungen sind anwendungsabhängig. Für einige Anwendungen stehen keine Einstellmöglichkeiten zur Verfügung.

Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

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

System

Uhrzeit und Standort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server))**: Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP))**: Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server)**: Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server))**: Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **Benutzerdefinierte Datum und Uhrzeit**: Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie auf **Get from system (Vom System abrufen)**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

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

Hinweis

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

Gerätestandort

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

- **Latitude (Breite)**: Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Longitude (Länge)**: Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Heading (Ausrichtung)**: Die Ausrichtung des Geräts laut Kompass eingeben. Der Wert 0 steht für: genau nach Norden.
- **Label (Bezeichnung)**: Eine aussagekräftige Bezeichnung für das Gerät eingeben.
- **Save (Speichern)**: Klicken Sie hier, um den Gerätestandort zu speichern.

Netzwerk

IPv4

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

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

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

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

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

Hinweis

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

IPv6

IPv6 automatisch zuweisen: Wählen Sie diese Option, um IPv6 einzuschalten und damit der Netzwerk-Router dem Gerät automatisch eine IP-Adresse zuweisen kann.

Host-Name

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

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

DNS servers (DNS-Server)

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

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

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

HTTP und HTTPS

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

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie für die Erstellung und Installation von Zertifikaten zu **System > Security (System > Sicherheit)**.

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

Hinweis

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

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

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

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

Protokolle zur Netzwerkerkennung

Bonjour®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

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

UPnP®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

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

WS-Erkennung: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

Cloud-Anbindung mit einem Mausklick

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

Allow O3C (O3C zulassen):

- **One-click**: Dies ist die Standardeinstellung. Halten Sie die Steuertaste am Gerät gedrückt, um über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sie müssen das Gerät innerhalb von 24 Stunden nach dem Drücken der Steuertaste beim O3C-Dienst registrieren. Andernfalls wird sich das Gerät vom O3C-Dienst getrennt. Nach der Registrierung des Geräts ist **Always (Immer)** aktiviert und das Gerät bleibt mit dem O3C-Dienst verbunden.
- **Immer**: Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Nach der Registrierung bleibt das Gerät mit dem O3C-Dienst verbunden. Verwenden Sie diese Option, wenn die Steuertaste am Gerät außer Reichweite ist.
- **Nein**: Deaktiviert den O3C-Dienst.

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

Host: Geben Sie die Adresse des Proxy-Servers ein.

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

Anmeldung und **Kennwort**: Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Wählen Sie die zu verwendende SNMP-Version.

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

Hinweis

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

- **v3**: SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden.

Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.

- **Kennwort für das Konto "initial"**: Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

Sicherheit

Zertifikate

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

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

Folgende Formate werden unterstützt:

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

Wichtig

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

Die Zertifikate in der Liste filtern.

Add certificate (Zertifikat hinzufügen): Klicken Sie, um ein Zertifikat hinzuzufügen.

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

Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) :

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

IEEE 802.1x

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

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

Zertifikate

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

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

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

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

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

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

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

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

Brute-Force-Angriffe verhindern

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

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

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

IP address filter (IP-Adressfilter)

Use filter (Filter verwenden): Wählen Sie diese Option, um zu filtern, welche IP-Adressen auf das Gerät zugreifen dürfen.

Policy (Richtlinie): Wählen Sie, ob Sie den Zugriff für bestimmte IP-Adressen **Allow (erlauben)** oder **Deny (verweigern)** möchten.

Addresses (Adressen): Geben Sie die IP-Nummern ein, denen der Zugriff auf das Gerät erlaubt oder verweigert wird. Sie können auch das CIDR-Format verwenden.

Spezifisch signiertes Firmwarezertifikat

Zum Installieren von Test-Firmware oder anderer benutzerdefinierter Firmware von Axis auf dem Gerät benötigen Sie ein individuell signiertes Firmwarezertifikat. Das Zertifikat prüft, ob die Firmware sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Firmware kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Benutzersignierte Firmwarezertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

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

Konten

Accounts (Konten)

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

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener)**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**einstellungen.
  - Apps werden hinzugefügt.

⋮ Das Kontextmenü enthält:

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

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

Anonymous access (Anonymer Zugriff)

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

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

SSH accounts (SSH-Konten)

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

- **Restrict root access (Root-Zugriff beschränken)**: Aktivieren, um die Funktion einzuschränken, die einen Root-Zugriff erfordert.
- **Enable SSH (SSH aktivieren)**: Den SSH-Dienst aktivieren.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

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

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

Comment (Anmerkung): Geben Sie eine Anmerkung ein (optional).

⋮ Das Kontextmenü enthält:

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

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

OpenID Configuration (OpenID-Konfiguration)

Wichtig

Geben Sie die richtigen Werte ein, um sicherzustellen, dass Sie sich erneut am Gerät anmelden können.

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

+ **Add a rule (Regel hinzufügen)**: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

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

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

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

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

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

Empfänger

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis

Sie können bis zu 20 Empfänger erstellen.

+ **Einen Empfänger hinzufügen**: Klicken Sie darauf, um einen Empfänger hinzuzufügen.

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

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

- **Network storage (Netzwerk-Speicher)**
  Darüber können Sie einen Netzwerk-Speicher wie NAS (Network Attached Storage) hinzufügen und als Empfänger für zu speichernde Dateien verwenden. Die Dateien werden im Format Matroska (MKV) gespeichert.
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen der Netzwerk-Speicher ein.
  - **Freigabe**: Geben Sie den Namen der Freigabe auf dem Host ein.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
- **SFTP**
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Geben Sie die vom SFTP-Server verwendete Portnummer ein. Der Standardport ist 22.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem SFTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Benutzername**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Kennwort**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Öffentlicher SSH-Host-Schlüsseltyp (MD5)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine hexadezimale Zeichenfolge mit 32 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Öffentlicher SSH-Host-Schlüsseltyp (SHA256)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine Base64-kodierte Zeichenfolge mit 43 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.
- **SIP or VMS (SIP oder VMS)** :
  SIP: Wählen Sie diese Option, um einen SIP-Anruf zu starten.
  VMS: Wählen Sie diese Option, um einen VMS-Anruf zu starten.
  - **From SIP account (Von SIP-Konto)**: Wählen Sie die entsprechende Option aus der Liste aus.
  - **To SIP address (An SIP-Adresse)**: Geben Sie die entsprechende SIP-Adresse ein.
  - **Test**: Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.
- **E-Mail**
  - **Send email to (E-Mail senden an)**: Geben Sie die gewünschte(n) E-Mail-Versandadresse(n) ein. Trennen Sie mehrere Adressen jeweils mit einem Komma.
  - **E-Mail senden von**: Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.
  - **Benutzername**: Geben Sie den Benutzernamen für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
  - **Kennwort**: Geben Sie das Kennwort für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
  - **Email server (SMTP) (E-Mail-Server (SMTP))**: Geben Sie den Namen des SMTP-Servers ein. Zum Beispiel smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port**: Geben Sie die Portnummer des SMTP-Servers ein. Zulässig sind Werte zwischen 0 und 65535. Der Standardport ist 587.
  - **Verschlüsselung**: Um die Verschlüsselung zu verwenden, wählen Sie SSL bzw. TLS.
  - **Server-Zertifikate validieren**: Wenn Sie eine Verschlüsselung verwenden, wählen Sie diese Option zur Überprüfung der Identität des Geräts. Das Zertifikat kann ein eigensigniertes oder ein von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat sein.
  - **POP authentication (POP-Authentifizierung)**: Aktivieren Sie diese Option, um den Namen des POP-Servers einzugeben, z.B. pop.gmail.com.

Hinweis

Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, geplante E-Mails erhalten usw. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, damit Ihr E-Mail-Konto nicht gesperrt wird oder die erwarteten E-Mails nicht verloren gehen.

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

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

⋮ Das Kontextmenü enthält:

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

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

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

Zeitpläne

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

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

Manuelle Auslöser

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

MQTT

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

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

Weitere Informationen zu MQTT finden Sie im *AXIS OS Portal*.

ALPN

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

MQTT-Client

Verbinden: Aktivieren oder deaktivieren Sie den MQTT-Client.

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

Broker

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

Protokoll: Wählen Sie das zu verwendende Protokoll aus.

Port: Geben Sie die Portnummer ein.

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

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

Username (Benutzername): Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll.

Kennwort: Geben Sie ein Kennwort für den Benutzernamen ein.

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

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

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

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

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

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

Nachricht zum Verbindungsaufbau

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

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

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

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

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

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

Nachricht zum letzten Willen und Testament

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

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

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

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

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

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

MQTT publication (MQTT-Veröffentlichung)

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

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

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

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

+ **Bedingung hinzufügen**: Klicken Sie darauf, um eine Bedingung hinzuzufügen.

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

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

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

MQTT-Abonnements

+ **Abonnement hinzufügen**: Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

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

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

Abonnementart:

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

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

MQTT-Overlays

Hinweis

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

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

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

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

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

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

SIP

Settings (Einstellungen)

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

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

Eingehende Anrufe zulassen: Wählen Sie diese Option, um eingehende Anrufe von anderen SIP-Geräten zuzulassen.

Call handling (Anrufbearbeitung)

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

Ports

Eine Portnummer muss zwischen 1024 und 65535 liegen.

- **SIP-Port**: Der für die SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Die Standardportnummer ist 5060. Bei Bedarf eine andere Portnummer eingeben.
- **TLS_Port**: Der für verschlüsselte SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Die Standardportnummer ist 5061. Bei Bedarf eine andere Portnummer eingeben.
- **RTP-Startport**: Der Netzwerkport, der für den ersten RTP-Medienstream in einem SIP-Anruf verwendet wird. Der Standardstartport ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern.

NAT-Traversal

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

Hinweis

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

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

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

Audio

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

Hinweis

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

- **Audioausrichtung**: Wählen Sie zulässige Audiorichtungen.

Zusätzliches

- **Wechsel von UDP zu TCP**: Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll (User Datagram Protocol) auf das Protokoll TCP (Transmission Control Protocol) zu wechseln. Mit einem Wechsel wird Fragmentierung vermieden und der Wechsel kann stattfinden sofern eine Anfrage innerhalb von 200 Bytes der maximalen Übertragungseinheit (MTU) liegt oder größer als 1300 Byte ist.
- **Über Umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Kontakt umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Alle ... am Server registrieren**: Legen Sie fest, wie oft sich das Gerät am SIP-Server für SIP-Konten registrieren soll.
- **DTMF-Nutzlasttyp**: Ändert den Standard-Nutzlasttyp für DTMF.

Accounts (Konten)

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

● Das Konto wurde erfolgreich beim SIP-Server registriert.

● Es liegt bei diesem Konto ein Problem vor. Mögliche Gründe: Autorisierungsfehler, falsche Kontendaten oder der SIP-Server kann das Konto nicht ermitteln.

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

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

- **Active (Aktiv)**: Wählen Sie diese Option, um das Konto nutzen zu können.
- **Als Standard setzen**: Mit dieser Option dieses Konto als Standardkonto verwenden. Es muss ein und nur ein Standardkonto vorhanden sein.
- **Answer automatically (Automatisch annehmen)**: Einen eingehenden Anruf automatisch annehmen.
- **Prioritize IPv6 over IPv4 (IPv6 über IPv4 bevorzugen)** ⓘ : Wählen Sie diese Option aus, um IPv6-Adressen gegenüber IPv4-Adressen zu bevorzugen. Dies ist nützlich, wenn Verbindungen zu Peer-to-Peer-Konten oder

Domänennamen hergestellt werden, die sowohl in IPv4- als auch in IPv6-Adressen auflösen. IPv6 kann nur für Domänennamen priorisiert werden, die IPv6-Adressen zugeordnet sind.

- **Name**: Geben Sie einen beschreibenden Namen ein. Das kann zum Beispiel ein Vor- und Nachname, eine Funktion oder ein Standort sein. Der Name muss nicht eindeutig sein.
- **Benutzer-ID**: Geben Sie die dem Axis Gerät zugeordnete eindeutige Telefonnummer oder Durchwahl an.
- **Peer-to-Peer**: Für Direktanrufe an ein anderes SIP-Gerät im lokalen Netzwerk.
- **Registriert**: Für Anrufe an SIP-Geräte außerhalb des lokalen Netzwerks über einen SIP-Server.
- **Domain**: Sofern verfügbar, geben Sie den Domainnamen ein. Dieser wird bei Anrufen bei anderen Konten als Teil der SIP-Adresse angezeigt.
- **Kennwort**: Geben Sie zum Authentifizieren am SIP-Server das dem SIP-Konto zugeordnete Kennwort ein.
- **Authentifizierungs-ID**: Geben Sie die Authentifizierungs-ID für den SIP-Server ein. Wenn diese mit der Benutzer-ID identisch ist, muss sie nicht gesondert eingegeben werden.
- **Anrufer-ID**: Der dem Empfänger der von diesem Gerät aus getätigten Anrufe angezeigte Name.
- **Registrierungsstelle**: Geben Sie die IP-Adresse der Registrierungsstelle ein.
- **Übertragungsmodus**: Den SIP-Übertragungsmodus für das Konto wählen: UPD, TCP oder TLS.
- **TLS version** (nur mit Übertragungsmodus TLS): Wählen Sie die zu verwendende TLS-Version. Die Versionen **v1.2** und **v1.3** sind die sichersten. **Automatic (Automatisch)** wählt die sicherste Version aus, die das System verarbeiten kann.
- **Media encryption (Medienverschlüsselung)** (nur mit Übertragungsmodus TLS): Die Art der Verschlüsselung für Medien (Audio und Video) für SIP-Anrufe wählen.
- **Zertifikat** (nur mit Übertragungsmodus TLS): Ein Zertifikat wählen.
- **Server-Zertifikat überprüfen** (nur mit Übertragungsmodus TLS): Markieren Sie diese Option, um das Server-Zertifikat zu überprüfen.
- **Sekundärer SIP-Server**: Aktivieren Sie diese Option, damit bei fehlgeschlagener Registrierung am primären SIP-Server das Gerät versucht, sich am sekundären SIP-Server zu registrieren.
- **SIP secure (SIP-Secure)**: Diese Option zum Verwenden von Secure Session Initiation Protocol (SIPS) wählen. SIPS verwendet zum Verschlüsseln den Übertragungsmodus TLS.
- **Proxys**
  - + **Proxy**: Klicken Sie darauf, um einen Proxy hinzuzufügen.
  - **Priorisieren**: Klicken Sie darauf, um Proxys zu priorisieren, wenn Sie zwei oder mehrere davon haben.
  - **Server-Adresse**: Geben Sie die IP-Adresse des primären SIP-Servers ein.
  - **Username (Benutzername)**: Falls verlangt, einen Benutzernamen für den SIP-Proxyserver eingeben.
  - **Kennwort**: Geben Sie das Kennwort für den SIP-Proxyserver ein, falls erforderlich.
- **Video** ⓘ
  - **Sichtbereich**: Wählen Sie den für Videoanrufe zu verwendenden Sichtbereich. Ohne Auswahl wird die Standardansicht verwendet.
  - **Auflösung**: Wählen Sie die für Videoanrufe zu verwendende Auflösung. Die Auflösung wirkt sich auf die erforderliche Bandbreite aus.
  - **Bildrate**: Wählen Sie die Bildrate für Videoanrufe auf. Die Bildrate wirkt sich auf die erforderliche Bandbreite aus.
  - **H.264 profile (Profil H.264)**: Wählen Sie das Profil aus, das für Videoanrufe verwendet werden soll.

DTMF

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

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

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

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

Protocols (Protokolle):

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

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

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

Test call (Testanruf)

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

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

Access list (Zugangsliste)

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

Policy (Richtlinie):

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

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

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

Zubehör

E/A-Ports

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

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

Port

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

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

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

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

Hinweis

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

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

Protokolle

Protokolle und Berichte

Berichte

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

Protokolle

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

Netzwerk-Trace

Wichtig

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

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

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

Remote-Systemprotokoll

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.

+ **Server**: Klicken Sie, um einen neuen Server hinzuzufügen.

Host: Geben Sie den Host-Namen oder die IP-Adresse des Servers ein.

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokoll): Wählen Sie das zu verwendende Protokoll und den zu verwendenden Port aus:

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

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

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

Direktkonfiguration

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

Wartung

Neustart: Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.

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

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

Sämtliche Firmware des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Firmware auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper "Signierte Firmware, sicherer Start und Sicherheit von Privatschlüsseln" auf *axis.com*.

Firmwareaktualisierung: Aktualisieren Sie auf eine neue Firmwareversion. Neue Firmwareversionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu *axis.com/support*.

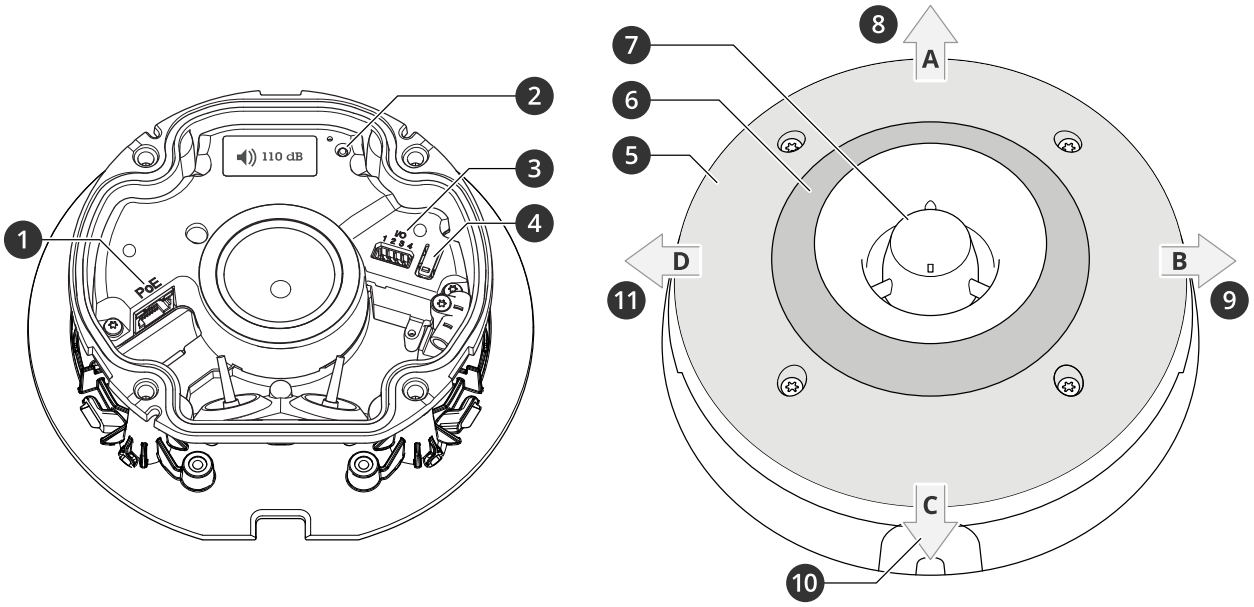
Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

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

Firmware zurücksetzen: Gehen Sie auf die vorherige Firmwareversion zurück.

Technische Daten

Produktübersicht



1 *Netzwerk-Anschluss (PoE)*
2 *LED-Statusanzeige*
3 *E/A-Anschluss*
4 *Steuertaste*
5 *Weiße LEDs*
6 *Rote, blaue, grüne und gelbe LEDs (RGBA)*
7 *Sirene*
8 *Beleuchtungsrichtung A*
9 *Beleuchtungsrichtung B*
10 *Beleuchtungsrichtung C*
11 *Beleuchtungsrichtung D*

LED-Anzeigen

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

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 47*.

- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Drücken Sie zum Herstellen der Verbindung die Taste und halten Sie sie etwa 3 Sekunden lang gedrückt, bis die Status-LED grün blinkt.

Anschlüsse

Netzwerk-Anschluss

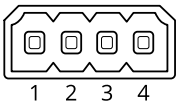
RJ45-Ethernetanschluss mit Power over Ethernet (PoE).

E/A-Anschluss

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

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

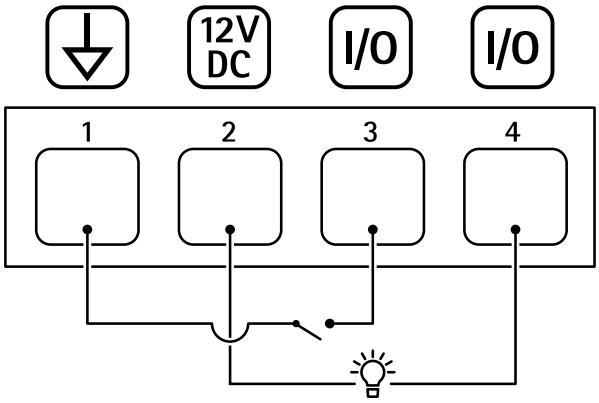
4-poliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Darf für die Stromversorgung von Zusatzgeräten verwendet werden. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	12 V DC Max. Stromstärke = 50 mA
Konfigurierbar (Ein- oder Ausgang)	3–4	Digitaleingang – zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang - Interne Verbindung mit Kontakt 1 (Gleichstrom Erdschluss), 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

Technische Daten



1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V, max. 50mA*
3 *E/A als Eingang konfiguriert*
4 *E/A als Ausgang konfiguriert*

Namen von Lichtmustern

Aus
Konstant
Kontant Weiß + blinkende Farbe
Alternierend
Pulsierend
Eskaliert in 3 Schritten
3 x Blinken
4 x Blinken
3 x schwaches Blinken
4 x schwaches Blinken
1 x Blitzlicht
3 x Blitzlicht
1 x weißes Blinken + konstant leuchtende Farbe
3 x weißes Blinken + konstant leuchtende Farbe
Richtung A + konstant leuchtende Farbe
Richtung B + konstant leuchtende Farbe
Richtung C + konstant leuchtende Farbe
Richtung D + konstant leuchtende Farbe
Weiß rotierend + konstant leuchtende Farbe
Drehendes Heck Weiß + konstant leuchtende Farbe
Zufällig Weiß + konstant leuchtende Farbe
Schnelles Drehen Weiß + konstant leuchtende Farbe
Konstant Weiß + konstant leuchtende Farbe

Maximaler Schalldruckpegel

Name des Tonmusters	Schalldruckpegel (dB) [1]
Alarm: Alarm mit hoher Tonlage	111
Alarm: Alarm mit niedriger Tonlage	108
Alarm: Vogel	112
Alarm: Schiffshorns	91
Alarm: Autoalarm schnell	107
Alarm: Autoalarm langsam	110
Alarm: Klassische Uhr	96
Alarm: Erstbegleiter	98
Alarm: Horror	109
Alarm: Industriell	103
Alarm: Einzelner Signalton	98
Alarm: Weicher Vierfachton	100
Alarm: Weicher dreifacher Signalton	103
Alarm: Dreifach hohe Tonlage	112
Benachrichtigung: Akzeptiert	83
Benachrichtigung: Wird angerufen	92
Benachrichtigung: Verweigert	89
Benachrichtigung: Erledigt	92
Benachrichtigung: Eintrag	96
Benachrichtigung: Fehlgeschlagen	97
Benachrichtigung: Eilt	88
Benachrichtigung: Nachricht	96
Benachrichtigung: Weiter	85
Benachrichtigung: Offen	100
Sirene: Alternierend	110
Sirene: Springend	112
Sirene: Evac.	102
Sirene: Fallender Ton	112
Sirene: Home weich	111

1. Wandmontage in einem Abstand von 1 Meter von Axis bei Lautstärkeeinstellung 5.

Empfehlungen zur Reinigung

Wenn das Gerät Fettflecken bekommt oder stark verschmutzt wird, kann es mit milder, lösemittelfreier Seife oder ebensolchem Reinigungsmittel gereinigt werden.

HINWEIS

Verwenden Sie niemals ein grobes Reinigungsmittel wie Benzin, Benzol oder Aceton.

1. Verwenden Sie eine Druckluft-Dose zum Entfernen von Staub oder Schmutz von dem Gerät.
2. Reinigen Sie das Gerät mit einem weichen Tuch, das mit mildem Reinigungsmittel und lauwarmem Wasser angefeuchtet ist.
3. Wischen Sie vorsichtig mit einem trockenen Tuch nach.

Hinweis

Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken beim Trocknen der Wassertropfen führen kann.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 42*.
3. Halten Sie die Steuertaste etwa 15 bis 30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse `192.168.0.90`.
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.

   Die Installations- und Verwaltungstools finden auf den Supportseiten unter *axis.com/support*.

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

Firmware-Optionen

Axis bietet eine Produkt-Firmware-Verwaltung 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, die Firmware 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 Produktfirmware finden Sie unter *axis.com/support/Firmware*.

Aktuelle Firmware überprüfen

Firmware ist die Software, mit der die Funktionalität von Netzwerk-Geräten festgelegt wird. Wir empfehlen Ihnen, vor jeder Problembehebung zunächst die aktuelle Firmwareversion zu überprüfen. Die aktuelle Firmwareversion enthält möglicherweise eine Verbesserung, mit der das Problem behoben werden kann.

So überprüfen Sie die aktuelle Firmware:

1. Gehen Sie zur Weboberfläche des Geräts > **Status**.
2. Die Firmwareversion finden Sie unter **Geräteinformationen**.

Fehlerbehebung

Firmware aktualisieren

Wichtig

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Firmware gespeichert (sofern die Funktionen als Teil der neuen Firmware verfügbar sind). Es besteht diesbezüglich jedoch keine Garantie seitens Axis Communications AB.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

Beim Aktualisieren mit der aktuellen Firmware im aktiven Track werden auf das Gerät die neuesten verfügbaren Funktionen versorgt. Lesen Sie vor der Aktualisierung der Firmware stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise dazu. Die aktuelle Version der Firmware und die Versionshinweise finden Sie auf *axis.com/support/firmware*.

1. Die Firmware können Sie auf *axis.com/support/firmware* kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Navigieren Sie zu **Maintenance > Firmware upgrade (Wartung > Firmwareaktualisierung)** und klicken Sie auf **Upgrade (Aktualisieren)**.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Fragen, Hinweise und Lösungen

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

Probleme beim Aktualisieren der Firmware	
Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche Firmwaredatei hochgeladen wurde. Überprüfen, ob der Name der Firmwaredatei dem Gerät entspricht und erneut versuchen.
Probleme nach dem Aktualisieren von Firmware	Bei nach dem Aktualisieren von Firmware auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurückrollen.

Probleme beim Einstellen der IP-Adresse	
Das Gerät befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster `ping` und die IP-Adresse des Geräts ein): • Wenn Folgendes angezeigt wird: `Reply from (Antwort von)<IP address>: bytes=32; time=10...` dies bedeutet, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut. • Wenn Folgendes angezeigt wird: `Request timed out` bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Fehlerbehebung

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell `http` oder `https` in die Adressleiste 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 auf Seite 47*.
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. Ermitteln Sie das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde). 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 Companion: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Video Management Software: Kostenlose 30-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 mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.

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.
Das Gerät gibt kein Laut von sich.	Überprüfen Sie, ob sich das Gerät im **Wartungsmodus** befindet. Wenn es sich im Wartungsmodus befindet, deaktivieren Sie diesen.

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.

Fehlerbehebung

Leistungsaspekte

Es sind folgende Faktoren zu beachten:

- Intensive Netzwerk-Nutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Für eine maximale Lichtleistung ist eine Stromquelle der PoE Klasse 4 erforderlich.
- Bei Verschmutzung des Geräts oder hohen Umgebungstemperaturen kann die Lichtleistung reduziert werden.
- In hellen Umgebungen, z. B. bei direkter Sonneneinstrahlung, sollten Sie zur Verbesserung der Sicht den Einsatz der Sonnenblende in Betracht ziehen.
- Die Tonausgabe kann verringert werden, wenn die Sirene blockiert ist oder das Gerät nicht ordnungsgemäß geschlossen ist.
- Die Installationsumgebung kann sich auf den Audioausgang auswirken. Die Lautstärke kann höher sein, wenn das Gerät an einer Wand oder in einem geschlossenen Raum installiert ist, und niedriger, wenn es auf einem Mast in einem offenen Raum installiert wird.

Support

Supportinformationen erhalten Sie unter *axis.com/support*.

Benutzerhandbuch
AXIS D4100-E Network Strobe Siren

Vers. M8.2
Datum: November 2023
Teil-Nr. T10166226