AXIS D4100-VE Mk II Network Strobe Siren

Benutzerhandbuch

Inhalt

Installation 4
....4
Funktionsweise....5
....5
Das Gerät im Netzwerk ermitteln....5
Unterstützte Browser....5
Weboberfläche des Geräts öffnen....5
Erstellen Sie ein Administratorenkonto....5
Sichere Kennwörter....5
Ihr Gerät konfigurieren....7
Wartungsmodus nach Installation der Sirene deaktivieren....7
Wartungsmodus einschalten....7
Ein Profil konfigurieren....7
Ein Profil importieren oder exportieren....7
Direktes SIP (P2P) einrichten....7
SIP über einen Server (PBX) einrichten....8
Einrichten von Regeln für Ereignisse....9
Lösen Sie eine Aktion aus....9
Profil starten, wenn ein Alarm ausgelöst wird....9
Profil über SIP starten....9
Mehrere Profile über SIP-Erweiterungen steuern....10
Zwei Profile mit unterschiedlichen Prioritäten ausführen....11
Aktivieren einer Blitzsirene über einen virtuellen Eingang bei Bewegungserkennung durch die Kamera....11
Aktivieren einer Blitzsirene über HTTP POST bei Bewegungserkennung durch die Kamera....13
Blitzsirene über MQTT aktivieren, wenn die Kamera Bewegung erkennt....14
Weboberfläche....16
Mehr erfahren....17
Session Initiation Protocol (SIP)....17
Peer-to-Peer SIP (P2PSIP)....17
Private Branch Exchange (PBX)....17
NAT-Traversal....17
Technische Daten....18
Produktübersicht....18
....18
LED-Anzeigen....18
Tasten....18
Steuertaste....18
Anschlüsse....19
Netzwerk-Steckverbinder....19
E/A-Anschluss....19
Namen von Lichtmustern....20
Namen von Klangmustern....20
Gerät reinigen....22
Fehlerbehebung....23
Zurücksetzen auf die Werkseinstellungen....23
Optionen für AXIS OS....23
Aktuelle AXIS OS-Version überprüfen....23
AXIS OS aktualisieren....24
Technische Probleme und mögliche Lösungen....24
....26
Leistungsaspekte....26
Support....26

Cybersicherheit....27
Schwachstellen-Management....27
Sicherheitsbenachrichtigungen....27
Sicherer Produktlebenszyklus....27

Installation



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

Funktionsweise

⚠ WARNUNG

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

Das Gerät im Netzwerk ermitteln

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Wird mit Einschränkungen unterstützt

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, on page 5*.

Eine Beschreibung aller Funktionen und Einstellungen in der Weboberfläche von Geräten mit AXIS OS finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

Erstellen Sie ein Administratorenkonto

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

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

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

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, erklingt die Sirene nicht und das Licht zeigt weiß pulsierende Lichtmuster.

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

Wartungsmodus einschalten

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

So legen Sie ein neues Standardszenario fest:

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

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

Ein Profil importieren oder exportieren

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

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

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

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

Direktes SIP (P2P) einrichten

Verwenden Sie Peer-to-Peer, wenn die Kommunikation zwischen wenigen Benutzeragenten innerhalb desselben IP-Netzwerks erfolgt und keine zusätzlichen Funktionen erforderlich sind, die von einem PBX-Server bereitgestellt werden können.

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

1. Wechseln Sie zu **System** > **SIP** > **SIP settings** (System > SIP > SIP-Einstellungen), und wählen Sie **Enable SIP (SIP aktivieren)**.
2. Um auf dem Axis Gerät eingehende Anrufe zu erlauben, wählen Sie **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. Der Standardport ist 5060. Geben Sie eine andere Portnummer ein, falls erforderlich.
   - **TLS port (TLS-Port)** – Der für verschlüsselte SIP-Kommunikation genutzte Netzwerk-Port. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Der Standardport ist 5061. Geben Sie eine andere Portnummer ein, falls erforderlich.
   - **RTP start port** – Den Port für den ersten RTP-Mediastream eines SIP-Anrufs eingeben. Der Standard-Startport für die Medienübertragung ist 4000. Einige Firewalls blockieren ggf. den RTP-Datenaustausch über bestimmte Portnummern. Eine Portnummer muss zwischen 1024 und 65535 liegen.
5. Wählen Sie unter **NAT Traversal** die Protokolle, die für NAT Traversal aktiviert werden sollen.

Hinweis

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

6. Wählen Sie unter **Audio** mindestens einen Audiocodec mit der für SIP-Anrufe gewünschten Audioqualität. Ändern Sie die Prioritätsreihenfolge per Drag & Drop.
7. Wählen Sie unter **Additional (Erweitert)** weitere Optionen aus.
   - **UDP-to-TCP switching (Zwischen UDP und TCP wechseln)** – Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll UDP (User Datagram Protocol) auf 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 Benutzeragenten innerhalb und außerhalb des IP-Netzwerks kommunizieren sollen. Je nach PBX-Anbieter können dem Setup zusätzliche Funktionen hinzugefügt werden.

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

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

- Benutzer-ID
- Domäne
- Kennwort
- Authentifizierungs-ID

- Anrufer-ID
- Registrator
- RTP-Startport

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

Einrichten von Regeln für Ereignisse

Weitere Informationen finden Sie unter *Erste Schritte mit Regeln für Ereignisse*.

Lösen Sie eine Aktion aus

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

Profil starten, wenn ein Alarm ausgelöst wird

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

Die Eingangsrichtung für den Port festlegen:

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

Eine Regel erstellen:

1. Gehen Sie zu **System** > **Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen **I/O** > **Digital input is active (Digitaler Eingang ist aktiv)**.
4. Wählen Sie **Port 1**:
5. Wählen Sie in der Liste mit den Aktionen **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. Gehen Sie zu **System** > **SIP** > **SIP settings (SIP-Einstellungen**.

2. Wählen Sie **SIP aktivieren** und **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

SIP aktivieren:

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

Erstellen Sie eine Regel zum Starten eines Profils:

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

Erstellen Sie eine Regel zum Stoppen eines Profils:

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

10. 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 aus der Liste der Bedingungen **I/O** > **Digital input is active (Digitaler Eingang ist aktiv)**.
4. Wählen Sie einen Port.
5. Wählen Sie in der Liste mit den Aktionen **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.

Vorbereitungen:

- Erstellen Sie in der Blitzsirene ein neues Konto mit Bediener- oder Administratorrechten.
- Erstellen Sie in der Blitzsirene ein Profil.
- Richten Sie AXIS Motion Guard in der Kamera ein und erstellen Sie ein Profil mit dem Namen „Kameraprofil".

Erstellen Sie in der Kamera zwei Empfänger:

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

Zwei Regeln in der Kamera erstellen:

1. **Rules (Regeln)** aufrufen und eine Regel hinzufügen.
2. Geben Sie folgende Informationen ein:
   - **Name**: Virtuellen E/A1 aktivieren
   - **Condition (Bedingung)**: **Applications (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - **Action (Aktion**: **Notifications (Benachrichtigungen) > Send notification through HTTP (Benachrichtigung über HTTP senden)**
   - **Recipient (Empfänger)**: **Activate virtual port (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 (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - Wählen Sie **Diese Bedingung umkehren**.
   - **Action (Aktion**: **Notifications (Benachrichtigungen) > Send notification through HTTP (Benachrichtigung über HTTP senden)**
   - **Recipient (Empfänger)**: **Deactivate virtual port (Virtuellen Port deaktivieren)**
   - **Query-String-Suffix**: schemaversion=1&port=1
5. Klicken Sie auf **Save (Speichern)**.

Eine Regel in der Blitzsirene erstellen:

1. Rufen Sie in der Weboberfläche 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)**: **I/O (E/A) > Virtual input (Virtueller Eingang)**
   - **Port**:**1**
   - **Action (Aktion)**: **Light and siren (Licht und Sirene) > Run light profile while the rule is active (Bei aktiver Regel Licht- und Sirenenprofil ausführen)**
   - **Profile (Profil)**: neu erstelltes Profil auswählen
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.

Vorbereitungen:

- 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**: Stroboskop-Sirene
   - **Typ**: **HTTP**
   - **URL**: http://<IP-Adresse>/axis-cgi/siren_and_light.cgi
     Ersetzen Sie <IP-Adresse> durch die Adresse der Blitzlichtsirene.
   - Benutzername und Kennwort des neu erstellten Benutzers der Blitzsirene.
3. Klicken Sie **Test (Testen)** an, um sicherzustellen, dass alle Daten gültig sind.
4. Klicken Sie auf **Save (Speichern)**.

Zwei Regeln in der Kamera erstellen:

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

Geben Sie unter „**Profile (Profil) : <>**" die gleichen Informationen ein, die Sie beim Erstellen des Profils in der Blitzlichtsirene eingegeben haben, in diesem Fall: „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 (Anwendungen) > Motion Guard: Camera profile (Motion Guard: Kameraprofil)**
   - Wählen Sie **Diese Bedingung umkehren**.

- **Action (Aktion**: **Notifications (Benachrichtigungen) > Send notification through HTTP (Benachrichtigung über HTTP senden)**
- **Recipient (Empfänger)**: **Strobe siren (Blitzlichtsirene)**
  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"  } }
```

Geben Sie unter „**Profile (Profil) : <>**" die gleichen Informationen ein, die Sie beim Erstellen des Profils in der Blitzlichtsirene eingegeben haben, in diesem Fall: „Profil der Blitzsirene".

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

Blitzsirene über MQTT aktivieren, wenn die Kamera Bewegung erkennt

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

Vorbereitungen:

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

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

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

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

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

1. Gehen Sie auf **System > Events (Ereignisse) > Rules (Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
   - **Name**: Bewegung erkannt
   - **Condition (Bedingung)**: **MQTT > Stateful (Statusbehaftet)**:
   - **Subscription filter (Abonnementfilter)**: **Motion (Bewegung)**
   - **Nutzlast**: Ein
   - **Action (Aktion)**: **Light and siren (Licht und Sirene) > Run light profile while the rule is active (Bei aktiver Regel Licht- und Sirenenprofil ausführen)**
   - **Profile (Profil)**: Wählen Sie das Profil aus, das aktiv sein soll.
3. Klicken Sie auf **Save (Speichern)**.

Weboberfläche

Informationen zu allen Funktionen und Einstellungen, die in der Weboberfläche von Geräten mit AXIS OS verfügbar sind, finden Sie in der *Hilfe zur AXIS OS-Weboberfläche*.

Mehr erfahren

Session Initiation Protocol (SIP)

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

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

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

Peer-to-Peer SIP (P2PSIP)

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

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-Benutzeragent wird bei der Nebenstellenanlage registriert und kann dann die anderen über die entsprechende Durchwahl erreichen. Eine typische SIP-Adresse wäre in diesem Fall `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

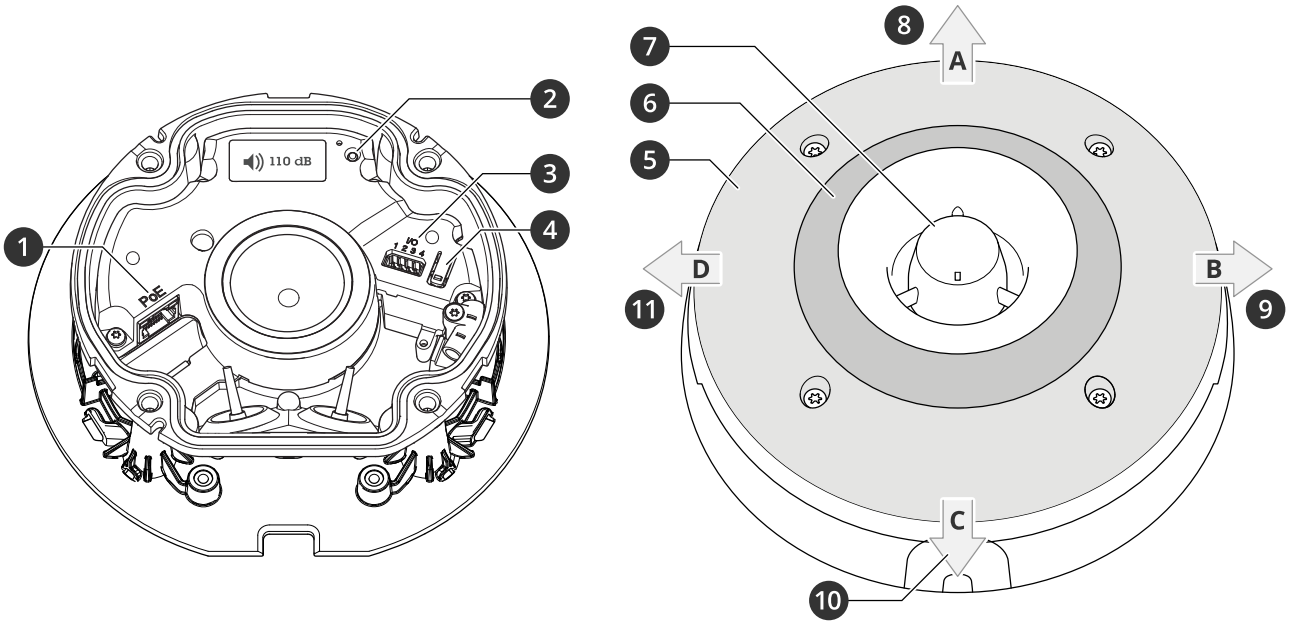
Der Router muss NAT-Traversal und UPnP® unterstützen.

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. Geben Sie die STUN-Server-Adresse ein, z. B. eine IP-Adresse.
- **TURN** – TURN (Traversal Using Relays around NAT) ist ein Protokoll, mit dem Geräte hinter einem NAT-Router oder einer Firewall über TCP oder UDP Daten von anderen Hosts empfangen können. Die TURN-Server-Adresse und die Anmeldedaten eingeben.

Technische Daten

Produktübersicht



1 *Netzwerk-Anschluss (PoE)*
2 *Status-LED*
3 *E/A-Anschluss*
4 *Steuertaste*
5 *Weiße LEDs*
6 *Rote, blaue, grüne und gelbe LEDs (RGBA)*
7 *Siren (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.
Gelb	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, on page 23*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Um eine Verbindung herzustellen, drücken Sie die Taste, lassen Sie sie los und warten Sie, bis die Status LED dreimal grün blinkt.

Anschlüsse

Netzwerk-Steckverbinder

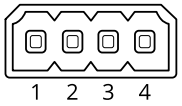
RJ-45-Ethernetanschluss mit Power over Ethernet (PoE).

E/A-Anschluss

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

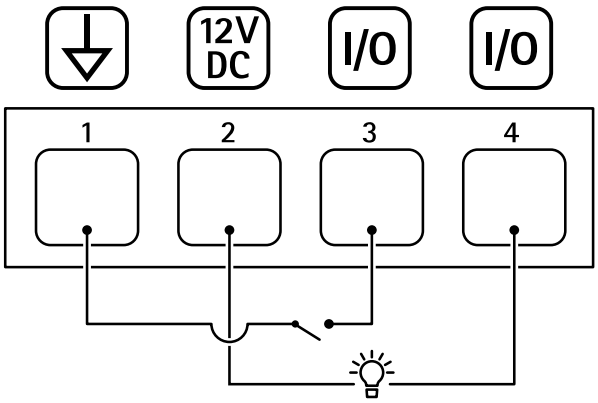
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

4-poliger Anschlussblock



Funktion	Pin	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstrom-ausgang	2	⚠ Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 50 mA
Konfigurierbar (Ein- oder Ausgang)	3-4	Digitaleingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open-Drain, 100 mA

Beispiel:



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

4 E/A als Ausgang konfiguriert

Namen von Lichtmustern

Aus
Konstant
Kontant Weiß + blinkende Farbe
Alternierend
Pulse (Impuls):
Eskaliert in 3 Schritten
Blinken
3 x Blinken
4 x Blinken
3 x schwaches Blinken
4 x schwaches Blinken
1 x Blitzlicht
3 x Blitzlicht
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

Namen von Klangmustern

Aus
Alarm: Alarm mit hoher Tonlage
Alarm: Alarm mit niedriger Tonlage
Alarm: Vogel
Alarm: Schiffshorns
Alarm: Fahrzeugalarm
Alarm: Autoalarm schnell
Alarm: Klassische Uhr

Alarm: Erstbegleiter
Alarm: Horror
Alarm: Industrie
Alarm: Einzelner Signalton
Alarm: Weicher Vierfachton
Alarm: Weicher dreifacher Signalton
Alarm: Dreifach hohe Tonlage
Benachrichtigung über: Abgelehnt
Benachrichtigung über: Fertig
Benachrichtigung über: Eintrag
Benachrichtigung über: Fehlgeschlagen
Benachrichtigung über: Eilt
Benachrichtigung über: Nachricht
Benachrichtigung über: Weiter
Benachrichtigung über: Offen
Siren (Sirene): Alternierend
Siren (Sirene): Springend
Siren (Sirene): Evac.
Siren (Sirene): Fallender Ton
Siren (Sirene): Home weich

Gerät reinigen

Sie können Ihr Gerät mit lauwarmem Wasser und milder, nicht scheuernder Seife reinigen.

HINWEIS

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

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

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

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

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

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht, on page 18*.
3. Halten Sie die Steuertaste etwa 15–30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird die IP-Adresse des Geräts standardmäßig auf eine der folgenden Adressen eingestellt:
   - **Geräte mit AXIS OS 12.0 und höher:** Beziehen sich auf das Subnetz der Adressen lokaler Links (169.254.0.0/16)
   - **Geräte bis AXIS OS 11.11:** 192.168.0.90/24
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.
   Die Softwaretools für die Installation und Verwaltung stehen auf den Supportseiten unter *axis.com/support* zur Verfügung.

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

Optionen für AXIS OS

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

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

Aktuelle AXIS OS-Version überprüfen

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

So überprüfen Sie die aktuelle AXIS OS-Version:

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

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.
- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Lifecycle guide: Upgrade path* (AXIS OS Lebenszyklus-Leitfaden: Aktualisierungspfad).
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

- Beim Aktualisieren mit der aktuellen AXIS OS-Version im aktiven Track werden auf dem Gerät die neuesten verfügbaren Funktionen bereitgestellt. Lesen Sie vor der Aktualisierung stets die entsprechenden Aktualisierungsanweisungen und Versionshinweise. Die aktuelle AXIS OS-Version und die Versionshinweise finden Sie unter *axis.com/support/device-software*.

1. Die AXIS OS-Datei können Sie von *axis.com/support/device-software* kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.
3. Rufen Sie **Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung)** auf und klicken Sie **Upgrade (Aktualisieren)** an.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

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

Probleme nach der AXIS OS-Aktualisierung

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

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

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

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

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

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 23*.

Die IP-Adresse wurde von DHCP geändert

Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Gerät mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln.

Bei Bedarf können Sie manuell eine statische IP-Adresse zuweisen. Anweisungen dazu finden Sie auf *axis.com/support*.

Zertifikatfehler beim Verwenden von IEEE 802.1X

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

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 5*.

Externer Zugriff auf das Gerät ist nicht möglich

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

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

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

Probleme mit MQTT

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

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

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

- Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll.
- Wenn der Server/Broker ALPN unterstützt, kann die Verwendung von MQTT über einen offenen Port, z. B. 443, ausgehandelt werden. Erkundigen Sie sich bei Ihrem Server-/Brokeranbieter, ob ALPN unterstützt wird und welches ALPN-Protokoll und welchen Port Sie verwenden müssen.

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

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

Leistungsaspekte

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

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

Support

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

Cybersicherheit

Cybersicherheit trägt zu einem erfolgreichen Produktlebenszyklus bei, bei dem Risiken auf ein Minimum reduziert werden. Ausführliche Informationen und Dokumente zu unserer Cybersicherheitsstrategie finden Sie auf *axis.com/about-axis/cybersecurity*. Befolgen Sie die nachstehenden Richtlinien zur Cybersicherheit, um Sicherheitsbenachrichtigungen von Axis zu erhalten und Ihr Produkt für eine sichere Benutzung und Außerbetriebnahme zu konfigurieren.

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

Schwachstellen-Management

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

Sicherheitsbenachrichtigungen

Sicherheitsbenachrichtigungs-E-Mails von Axis können Sie auf *axis.com/security-notification-service* abonnieren. Wir informieren Sie über Schwachstellen, geben entsprechende Sicherheitshinweise und benachrichtigen Sie zu anderen sicherheitsrelevanten Themen für Ihr Axis Produkt.

Sicherer Produktlebenszyklus

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

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

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

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

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

T10223803_de

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB