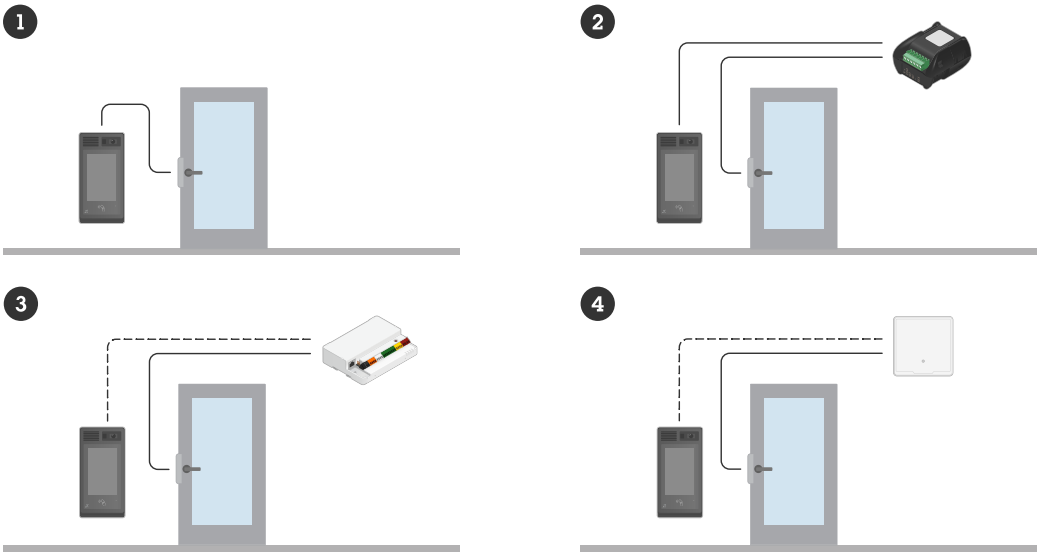
AXIS I8307-VE Network Intercom

Benutzerhandbuch

Inhalt

Lösungsübersicht



1 *Intercoms*
2 *Sprechanlage in Kombination mit AXIS A9801*
3 *Sprechanlage in Kombination mit AXIS A9210*
4 *IP-Türsprechanlage kombiniert mit einem Zutrittssystem*

Installation

Vorschaumodus

Der Vorschaumodus eignet sich optimal für Monteure für die Feinjustierung der Kameraansicht während der Installation. Für den Zugriff auf die Kameraansicht im Vorschaumodus ist keine Anmeldung erforderlich. Sie ist ab dem Einschalten des Geräts nur für eine begrenzte Zeit in der Werkseinstellung verfügbar.

Dieses Video zeigt, wie der Vorschaumodus verwendet wird.

Funktionsweise

Das Gerät im Netzwerk ermitteln

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

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
   Bei unbekannter IP-Adresse AXIS IP Utility oder AXIS Device Manager verwenden, um das Gerät im Netzwerk zu ermitteln.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe .

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter .

Administratorkonto erstellen

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

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

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe .

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

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

Ihr Gerät konfigurieren

In diesem Abschnitt werden alle wichtigen Konfigurationen behandelt, die ein Installationstechniker ausführen muss, um das Produkt nach Abschluss der Hardwareinstallation in Betrieb zu nehmen.

Direktes SIP (P2P) einrichten

Bei VoIP (Voice over IP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimediakommunikation über IP-Netzwerke ermöglicht. Weitere Informationen finden Sie unter .

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter

Es gibt zwei Typen von Setups für SIP: Direkt oder Peer-to-Peer (P2P) ist einer von ihnen. 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 zum Einrichten finden Sie unter .

1. Rufen Sie **Communication > SIP > Settings (Kommunikation > SIP > Einstellungen)** auf und wählen Sie **Enable SIP (SIP aktivieren)** aus.
2. Um auf dem Axis Gerät eingehende Anrufe zu erlauben, **Allow incoming calls (Eingehende Anrufe erlauben)** anklicken.

HINWEIS

Wenn Sie eingehende Anrufe zulassen, nimmt das Gerät Anrufe von allen Geräten an, die mit dem Netzwerk verbunden sind. Wenn auf das Gerät über ein öffentliches Netzwerk oder das Internet zugegriffen werden kann, wird empfohlen, eingehende Anrufe zu deaktivieren.

3. Klicken Sie auf **Call handling (Anrufbehandlung)**.
4. Unter **Calling timeout (Zeitüberschreitung bei Anruf)** die Sekundenanzahl eingeben, nach denen der Anruf ohne Antwort beendet wird.
5. Wenn Sie eingehende Anrufe zugelassen haben, legen Sie in **Incoming call Timeout (Zeitüberschreitung bei eingehenden Anrufen)** die Anzahl der Sekunden fest.
6. Klicken Sie auf **Ports**.
7. Geben Sie die Nummer für den **SIP port (SIP-Port)** und **TLS port (TLS-Port)** ein.

Hinweis

- **SIP-Port** – für SIP-Sitzungen. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Der Standardport ist 5060.
- **TLS port (TLS-Port)** – für SIPs und TLS-gesicherte SIP-Sitzungen. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Der Standardport ist 5061.
- **RTP start port** – der Port für den ersten RTP-Mediastream eines SIP-Anrufs. Der Standardstartport ist 4000. Möglicherweise blockieren einige Firewalls RTP-Datenverkehr an bestimmten Portnummern. Die Portnummer muss zwischen 1024 und 65535 liegen.

8. Klicken Sie auf **NAT Traversal**.
9. Wählen Sie 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 .

10. **Save (Speichern)** anklicken.

SIP über einen Server (PBX) einrichten

Bei VoIP (Voice over IP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimediakommunikation über IP-Netzwerke ermöglicht. Weitere Informationen finden Sie unter .

Auf diesem Gerät wird VoIP über das SIP-Protokoll aktiviert. Weitere Informationen zu SIP finden Sie unter

Es gibt zwei Typen von Setups für SIP: Einer davon ist ein PBX-Server. 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 finden Sie unter .

1. Fordern Sie folgende Informationen von Ihrem PBX-Anbieter an:
   - Benutzer-ID
   - Domäne
   - Kennwort
   - Authentifizierungs-ID
   - Anrufer-ID
   - Registrator
   - RTP-Startport
2. Rufen Sie **Communication > SIP > Accounts (Kommunikation > SIP > Konten)** auf, und klicken Sie auf **+ Add account (+ Konto hinzufügen)**.
3. Einen **Namen** für das Konto eingeben.
4. Wählen Sie **Registered (Registriert)** aus.
5. Transportmodus auswählen.
6. Die Kontoinformationen des PBX-Anbieters hinzufügen.
7. **Save (Speichern)** anklicken.
8. Um die SIP-Einstellungen auf die gleiche Weise wie für Peer-to-Peer einzurichten, siehe Verwenden Sie den RTP-Startport des PBX-Anbieters.

Erstellen eines Kontakts

In diesem Beispiel wird das Erstellen eines neuen Kontakts in der Kontaktliste erläutert. Aktivieren Sie vor dem Start SIP unter **Communication > SIP (System > SIP)**.

So erstellen Sie einen neuen Kontakt:

1. Rufen Sie **Communication > Contact list (Kommunikation > Kontaktliste)** auf.
2. Klicken Sie auf **+ Add contact (+ Kontakt hinzufügen)**.
3. Geben Sie den Vor- und Nachnamen des Kontakts ein.
4. Geben Sie die SIP-Adresse des Kontakts ein.

Hinweis

Weitere Informationen zu SIP-Adressen finden Sie unter .

5. Wählen Sie das SIP-Konto aus, aus dem der Aufruf erfolgen soll.

Hinweis

Verfügbarkeitsoptionen werden unter **System** > **Events (Ereignisse)** > **Schedules (Zeitpläne)** definiert.

6. Wählen Sie die **Availability (Verfügbarkeit)** des Kontakts. Wenn ein Anruf erfolgt, obwohl der Kontakt nicht verfügbar ist, wird der Anruf abgebrochen, es sei denn, es gibt einen Fallback-Kontakt.

Hinweis

Bei einem Fallback-Kontakt handelt es sich um einen Kontakt, an den der Anruf weitergeleitet wird, wenn der ursprüngliche Kontakt nicht antwortet oder nicht verfügbar ist.

7. Wählen Sie unter **Fallback**Keine**.**
8. **Save (Speichern)** anklicken.

Hinzufügen einer Ruftaste auf dem Bildschirm

In diesem Beispiel wird erläutert, wie Sie die Anzeige so konfigurieren, dass eine Schaltfläche angezeigt wird, über die Besucher die Rezeption anrufen können.

Bevor Sie beginnen:

- Erstellen Sie den Rezeptionskontakt. Anweisungen finden Sie unter .

1. Gehen Sie zu **Display (Bildschirm) > Pages (Seiten)**.
2. Klicken Sie in **Default Homepage (Standard-Homepage)** auf die Option ⋮ und wählen Sie **Edit (Bearbeiten)**.
3. **+ hinzufügen** anklicken.
4. Wählen Sie in der Liste **Type (Typ)** die Option **Button (Schaltfläche)** aus.
5. Wählen Sie in der Liste der Kontakte die Rezeption aus.
6. Wählen Sie eine Schaltflächengröße.
7. Um die Schaltfläche zu speichern, klicken Sie auf **Save (Speichern)**.
8. Um die Standard-Homepage zu speichern, klicken Sie auf **Save (Speichern)**.

Einrichten als Kartenleser – Netzwerk-Verbindung

Um die IP-Türsprechanlage als Kartenleser zu verwenden, muss sie an eine Türsteuerung angeschlossen werden. Die Türsteuerung speichert alle Zugangsdaten und überwacht, wer durch die Tür gehen darf. In diesem Beispiel werden die Geräte über das Netzwerk angeschlossen. Wir ändern auch die zulässigen Kartentypen.

Wichtig

Die Netzwerk-Verbindung funktioniert nur mit Axis Türsteuerungen. Um eine Verbindung zu einer Nicht-Axis-Türsteuerung herzustellen, müssen die Geräte physisch mit Kabeln verbunden werden. Siehe .

Einrichten der IP-Türsprechanlage als Kartenleser

1. Rufen Sie **Reader > Connection (Kartenleser > Verbindung)** auf.
2. Wählen Sie den **Protokolltyp des VAPIX-Lesers**.
3. Wählen Sie das Protokoll für die Kommunikation mit der Türsteuerung.

Hinweis

Bei Verwendung von **HTTPS** empfehlen wir Ihnen, **Zertifikat überprüfen** zu aktivieren.

4. Geben Sie die IP-Adresse für die Türsteuerung ein.
5. Geben Sie die Zugangsdaten für die Türsteuerung ein.
6. **Connect (Verbinden)** anklicken.
7. Wählen Sie den Eingangsleser für die entsprechende Tür.
8. **Save (Speichern)** anklicken.

Einrichten als Kartenleser – kabelgebundene Verbindung

Um die IP-Türsprechanlage als Kartenleser zu verwenden, muss sie an eine Türsteuerung angeschlossen werden. Die Türsteuerung speichert alle Zugangsdaten und überwacht, wer durch die Tür gehen darf. In diesem Beispiel verbinden wir die Geräte mit Kabeln, verwenden das Wiegand-Protokoll, aktivieren den Summer und verwenden einen E/A-Port für die LED. Wir ändern auch die zulässigen Kartentypen.

Wichtig

Verwenden Sie E/A-Ports, die noch nicht verwendet werden. Wenn E/A-Ports bereits verwendet werden, funktionieren für diese Ports erstellte Ereignisse nicht mehr.

Bevor Sie beginnen:

- Schließen Sie die IP-Türsprechanlage an die Türsteuerung an.
  Siehe die Zeichnungen für die elektrische Verdrahtung, die Sie unter finden können.
- Konfigurieren Sie die Hardware der Türsteuerung mit dem Wiegand-Protokoll für den Leser. Weitere Anweisungen finden Sie im Benutzerhandbuch der Türsteuerung.

Einrichten der IP-Türsprechanlage als Kartenleser

1. Rufen Sie **Reader > Connection (Kartenleser > Verbindung)** auf.
2. Wählen Sie als Protokolltyp **Wiegand** aus.
3. Aktivieren Sie den **Summer**.
4. Wählen Sie unter **Eingang für Summer** die Option **I3**.
5. Wählen Sie unter **Input used for LED control (Eingang für die LED-Steuerung)** die Option **1** aus.
6. Wählen Sie unter **Eingang für LED1**die Option **I1**.
7. Wählen Sie die für die einzelnen Zustände zu verwendenden Farben aus.
8. Wählen Sie unter **Tastendruckformat** die Option **FourBit**.
9. **Save (Speichern)** anklicken.
10. Wechseln Sie zu **Reader > Chip types (Leser > Chiparten)** und aktivieren Sie die Chiparten, die Sie verwenden möchten.

Hinweis

Sie können die standardmäßig vorgegebenen Chiparten beibehalten. Wir empfehlen jedoch, die Liste ihren besonderen Anforderungen entsprechend zu ändern.

11. Klicken Sie auf **Datensatz hinzufügen**, um die Datensätze für die verschiedenen Chiparten anzugeben.
12. Klicken Sie auf **Save**.

Verwenden Sie geschützte Daten auf Karten, um die Sicherheit zu erhöhen

Für mehr Sicherheit in Ihrem Zutrittssystem können Sie sichere Kartendaten verwenden, die auf bestimmten Kartentypen gespeichert sind. Die Daten werden mit einem sicheren Schlüssel geschützt. Zum Auslesen der Kartendaten müssen der verborgene Schlüssel und weitere Informationen zur Karte auf dem Gerät gespeichert werden.

1. Wechseln Sie zu **Reader > Chip types (Leser > Chiparten)**.
2. Wählen Sie unter **Data sets (Datensätze)** die zu bearbeitenden Chipart und klicken Sie auf **Add data set (Datensatz hinzufügen)** .
3. Geben Sie Informationen zu den Kartendaten ein. Welche Informationen sie eingeben müssen, hängt vom Kartentyp und von der Art der Anmeldung ab.
4. Wenn Sie die Protokolle OSDP oder Wiegand verwenden, wählen Sie **Use as UID (Als UID verwenden)** aus, um die sicheren Daten als UID/CSN anstelle der normalen UID/CSN der Karte zu senden.
5. Damit nur Karten, die den angegebenen Kartendaten entsprechen, an den Zugangscontroller gesendet werden können, wählen Sie die Option **Erforderliche Daten**. Karten, die nicht den Anforderungen entsprechen, werden vom Leser ignoriert.
6. **Save (Speichern)** anklicken.

Verwenden Sie DTMF, um einen Lageplan auf dem Bildschirm anzuzeigen.

Wenn ein Besucher über die IP-Türsprechanlage anruft und Hilfe benötigt, kann die Person, die den Anruf entgegennimmt, per DTMF-Signalisierung (Dual-Tone Multi-Frequency) einen Lageplan auf dem Bildschirm der IP-Türsprechanlage anzeigen.

Dieses Beispiel erläutert, wie:

- Laden Sie ein Lageplanbild auf die IP-Türsprechanlage hoch.
- Erstellen Sie eine Seite, die das Lageplanbild in der IP-Türsprechanlage enthält.

- Definieren der DTMF-Sequenz in der IP-Türsprechanlage.
- Richten Sie die IP-Türsprechanlage so ein, dass die Lageplanseite 30 Sekunden lang als Antwort auf die DTMF-Sequenz angezeigt wird.

Bevor Sie beginnen:

- SIP-Anrufe vom Gerät zulassen und ein SIP-Konto erstellen. Anweisungen finden Sie unter und .

Lageplanbild hochladen

1. Gehen Sie auf **Media (Medien)**.
2. **+ hinzufügen** anklicken.
3. Ziehen Sie per Drag and Drop ein Bild, das einen Lageplan des Gebäudes zeigt. Die empfohlene Bildauflösung ist 480x800 Pixel, die maximale Auflösung beträgt 2048x2048 Pixel.
4. **Save (Speichern)** anklicken.

Erstellen Sie eine Lageplanseite für den Bildschirm.

5. Gehen Sie zu **Display (Bildschirm) > Pages (Seiten)**.
6. **+ hinzufügen** anklicken.
7. Geben Sie einen Namen für die Seite ein, zum Beispiel Lageplanseite.
8. **+ hinzufügen** anklicken.
9. Wählen Sie in der Liste der Typen **Image (Bild)**.
10. Geben Sie einen Namen für das Bild ein, zum Beispiel Lageplanbild.
11. Wählen Sie in der Liste der Lagepläne das Lageplanbild aus.
12. **Save (Speichern)** anklicken.
13. Klicken Sie erneut auf **Save (Speichern)**.

Definieren der DTMF-Sequenz

14. Gehen Sie zu **Communication (Kommunikation) > SIP > DTMF**.
15. Klicken Sie auf **+ Add sequence (+ Sequenz hinzufügen)**.
16. Geben Sie in **Sequence (Sequenz)** 9 ein.
17. Geben Sie in **Description (Beschreibung)** Lageplan anzeigen ein.
18. Wählen Sie ein Konto.
19. **Save (Speichern)** anklicken.

Eine Regel erstellen

20. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
21. Geben Sie einen Namen für die Regel ein, z. B. DTMF verwenden, um Lagepläne anzuzeigen.
22. Wählen Sie aus der Liste der Bedingungen **Call (Anruf) > DTMF**.
23. Wählen Sie in der Liste der DTMF-Ereignis-IDs **Show map (Lagepläne anzeigen)**.
24. Wählen Sie in der Liste der Aktionen **Display (Bildschirm) > Show page (Seite anzeigen)**.
25. Wählen Sie in der Liste der Lagepläne **Map page (Lageplanseite)**.
26. Geben Sie in **Duration (Dauer)**, 00:00:30 ein, um den Lageplan 30 Sekunden lang anzuzeigen.
27. **Save (Speichern)** anklicken.

Zulassen, dass der Eigentümer der Zugangsdaten die Tür öffnet

Mit der Zugangsberechtigungsliste können Eigentümer von Zugangsdaten Aktionen wie das Öffnen einer Tür über ihre Karte oder PIN auslösen. In diesem Beispiel wird erläutert, wie Sie einen Eigentümer von Zugangsdaten hinzufügen, der mit seiner Karte zehnmal die Tür öffnen kann.

Voraussetzungen

- Stellen Sie sicher, dass unter **Reader > Chip types (Leser > Chiptypen)** der richtige Chiptyp aktiviert ist.

Aktivieren Sie die Zugangsberechtigungsliste, und fügen Sie einen Eigentümer von Zugangsdaten hinzu:

1. Gehen Sie zu **Reader > Entry list (Leser > Zugangsberechtigungsliste)**.
2. Aktivieren Sie **Use Entry list (Zugangsberechtigungsliste verwenden)**.
3. Klicken Sie auf **+ Add credential holder (+ Eigentümer von Zugangsdaten hinzufügen)**.
4. Geben Sie den Vor- und Nachnamen des Eigentümers der Anmeldedaten ein. Der Vorname muss eindeutig sein.
5. Wählen Sie **Card (Karte)** aus.
6. Ziehen Sie die Karte des Eigentümers von Zugangsdaten auf dem Gerät durch, und klicken Sie auf **Get latest (Neueste abrufen)**.
7. Behalten Sie **Access granted (Zugang gewährt)** als Ereignisbedingung bei.
8. Wählen Sie unter **Valid to (Gültig bis)** die Option **Number of times (Anzahl)** aus.
9. Geben Sie unter **Number of times (Anzahl)** 10 ein:
10. **Save (Speichern)** anklicken.

Eine Regel erstellen:

1. Gehen Sie auf **System > Ereignisse**.
2. Klicken Sie unter **Rules (Regeln)** auf **+ Add a rule (+ Regel hinzufügen)**.
3. Geben Sie in **Name** Unlock door (Tür entriegeln) ein.
4. Wählen Sie in der Liste der Bedingungen **Entry list > Access granted (Zugangsberechtigungsliste > Zugang gewährt)** aus.
5. Wählen Sie in der Liste der Aktionen **I/O > Toggle I/O once (E/A > E/A einmalig umschalten)** aus.
6. Wählen Sie in der Liste der Ports **Door (Tür)** aus.
7. Wählen Sie unter **State (Status)** die Option **Active (Aktiv)** aus.
8. Legen Sie die Dauer auf 00:00:07 fest:
9. **Save (Speichern)** anklicken.

Weboberfläche

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

Hinweis

Die in diesem Abschnitt beschriebenen Funktionen und Einstellungen werden von Gerät zu Gerät unterschiedlich unterstützt. Dieses Symbol zeigt an, dass die Funktion oder Einstellung nur für einige Geräte verfügbar ist.

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Ändern Sie die Sprache.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

- Informationen zum angemeldeten Benutzer.
- **Konto wechseln**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
- **Abmelden**: Melden Sie sich vom aktuellen Konto ab.

Das Kontextmenü enthält:

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

Status

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich AXIS OS-Version und Seriennummer.

Upgrade AXIS OS (AXIS OS aktualisieren): Aktualisieren Sie die Software auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie die Aktualisierung durchführen können.

Zeitsynchronisierungsstatus

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

NTP-Einstellungen: Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Time and location (Uhrzeit und Standort)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Sicherheit

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

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

Energieverbrauch

Zeigt Informationen zum Energieverbrauch wie aktuelle Leistungsaufnahme, durchschnittliche und maximale Leistungsaufnahme an.

Power settings (Energieeinstellungen): Die Stromeinstellungen des Geräts anzeigen und aktualisieren. Seite „Power settings" (Energieeinstellungen) aufrufen, um die Energieeinstellungen zu ändern.

Laufende Aufzeichnungen

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter

Anzeige des Speicherorts der Aufzeichnung.

Verbundene Clients

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

Details anzeigen: Anzeigen und Aktualisieren der Liste der verbundenen Clients. Die Liste zeigt IP-Adresse, Protokoll, Port, Zustand und PID/Process für jede Verbindung an.

Video

Installation

Capture mode (Aufnahmemodus) : Ein Aufnahmemodus ist eine voreinstellte Konfiguration, in der festzulegt wird, wie die Kamera Bilder aufnehmen soll. Eine Änderung des Aufnahmemodus kann sich auf viele anderen Einstellungen, wie Sichtbereiche und Privatzonenmasken, auswirken.

Mounting position (Montageposition) : Die Bildausrichtung kann sich je nach Installation der Kamera ändern.

Netzfrequenz: Wählen Sie die in Ihrer Region verwendete Frequenz aus, um Bildflimmern zu minimieren. In Amerika wird in der Regel eine Frequenz von 60 Hz verwendet. Auf allen anderen Kontinenten wird in der Regel eine Frequenz von 50 Hz verwendet. Wenden Sie sich bitte bei Fragen zur Netzwerkfrequenz an Ihr Stromversorgungsunternehmen.

Drehen: Verwenden Sie den Schieberegler, um den Winkel so einzustellen, dass das Bild horizontal ist.

Bild

Darstellung

Scene profile (Szene-Profil) : Wählen Sie ein Szeneprofil für Ihr Überwachungsszenario aus. Ein Szene-Profil optimiert die Bildeinstellungen einschließlich Farbstufe, Helligkeit, Schärfe, Kontrast und lokaler Kontrast für eine bestimmte Umgebung oder zu einem bestimmten Zweck.

- **Forensic (Forensisch):** Zu Überwachungszwecken geeignet.
- **Indoor (Innenbereich)** : Für den Innenbereich geeignet.
- **Outdoor (Außenbereich)** : Für den Außenbereich geeignet.
- **Vivid (Anschaulich)** : Zu Demonstrationszwecken nützlich.
- **Traffic overview (Verkehrsübersicht)** : Für die Überwachung des Fahrzeugverkehrs geeignet.
- **License plate (Fahrzeugkennzeichen):** Geeignet zum Aufzeichnen von Fahrzeugkennzeichen.

Sättigung: Stellen Sie mithilfe des Schiebereglers die Farbintensität ein. Sie können z. B. ein Bild in Graustufen erstellen.

Kontrast: Passen Sie mithilfe des Schiebreglers den Unterschied zwischen hell und dunkel an.

Helligkeit: Stellen Sie mithilfe des Schiebereglers die Lichtstärke ein. Dadurch lassen sich Objekte leichter erkennen. Helligkeit wird nach der Bildaufnahme angewendet und hat keine Auswirkungen auf die Bilddaten. Um mehr Details aus dunklen Bereichen zu erhalten, ist es normalerweise besser, die Verstärkung oder die Belichtungszeit zu erhöhen.

Schärfe: Stellen mithilfe des Schiebereglers den Randkontrast ein, um Objekte in einem Bild schärfer darzustellen. Wenn Sie die Schärfe erhöhen, kann dies zu einer höherem Bitrate und einem höheren Bedarf an Speicherplatz führen.

Wide Dynamic Range

WDR : Aktivieren Sie diese Option, um sowohl helle als auch dunkle Bereiche im Bild darzustellen.

Local contrast (Lokaler Kontrast) : Stellen Sie mithilfe des Schiebereglers den Kontrast des Bildes ein. Bei einem höheren Wert wird der Kontrast zwischen dunklen und hellen Bereichen größer.

Tone mapping (Tone-Mapping) : Passen Sie mithilfe des Schiebereglers das auf das Bild angewendete Tone-Mapping an. Bei einem Korrekturwert von „0" erfolgt lediglich eine normale Gammakorrektur, ein größerer Wert erhöht dagegen die Sichtbarkeit der dunkelsten und hellsten Bildbereiche.

Weißabgleich

Wenn die Kamera die Farbtemperatur der Lichtquelle erfasst, kann sie das Bild anpassen, um natürlichere Farben zu erreichen. Sollte dies nicht ausreichen, können Sie eine geeignete Lichtquelle aus der Liste wählen.

Die Einstellung Automatischer Weißabgleich verringert durch allmähliches Anpassen das Risiko von Farbflimmern. Wenn die Beleuchtung geändert oder die Kamera das erste Mal hochgefahren wird, kann die Anpassung an die veränderten Lichtverhältnisse bis zu 30 Sekunden dauern. Befindet sich in einer Szene mehr als eine Art von Lichtquelle, also wenn sie sich in ihrer Farbtemperatur unterscheiden, dann wird die stärkere Lichtquelle als Bezugswert für den Algorithmus zum Ermitteln des Weißabgleichs verwendet. Dieses Verhalten kann übersteuert werden. Dazu wird ein fester Weißabgleichswert gewählt, welcher der als Bezugswert bevorzugten Lichtquelle entspricht.

Lichtverhältnisse:

- **Automatisch**: Automatisches Identifizieren und Ausgleichen der Lichtfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen verwendet werden kann.
- **Automatic – outdoors (Automatisch – Außenbereich)** : Automatisches Identifizieren und Ausgleichen der Lichtfarbe. Dies ist die empfohlene Einstellung, die für die meisten Situationen im Außenbereich verwendet werden kann.
- **Custom – indoors (Benutzerdefiniert – Innenbereich)** : Fester Farbausgleich für Innenräume mit einem gewissen Anteil an nicht fluoreszierendem Kunstlicht und ausgerichtet auf eine normale Farbtemperatur von etwa 2800 K.
- **Custom – outdoors (Benutzerdefiniert – Außenbereich)** : Fester Farbausgleich für sonniges Wetter und eine Farbtemperatur von etwa 5500 K.
- **Fest – Fluoreszierend 1**: Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 4000 K.
- **Fest – Fluoreszierend 2**: Fester Farbausgleichswert für fluoreszierendes Licht und eine Farbtemperatur von etwa 3000 K.
- **Fest – Innenbereich**: Fester Farbausgleich für Innenräume mit einem gewissen Anteil an nicht fluoreszierendem Kunstlicht und ausgerichtet auf eine normale Farbtemperatur von etwa 2800 K.
- **Fest – Außenbereich 1**: Fester Farbausgleich für sonniges Wetter und eine Farbtemperatur von etwa 5500 K.
- **Fest – Außenbereich 2**: Fester Farbausgleichswert für bewölktes Wetter und eine Farbtemperatur von etwa 6500 K.
- **Street light – mercury (Straßenbeleuchtung – Quecksilber)** : Fester Farbausgleichswert zur Kompensation des ultravioletten Anteil von häufig als Straßenbeleuchtung eingesetzten Quecksilberdampfleuchten.
- **Street light – sodium (Straßenbeleuchtung – Natriumdampf)** : Fester Farbausgleichswert, der das gelbe bis orangefarbene Licht von häufig als Straßenbeleuchtung eingesetzten Natriumdampfleuchten korrigiert.
- **Aktuelle Einstellung beibehalten**: Die aktuelle Einstellung beibehalten und keinen Lichtausgleich vornehmen.
- **Manual (Manuell)** : Legen Sie den Weißabgleich mit Hilfe eines weißen Objekts fest. Dazu ein Objekt, das von der Kamera als weiß interpretiert werden soll (zum Beispiel ein weißes Blatt Papier) in die Mitte des Live-Bildes legen. Stellen Sie mit den Schiebereglern für **Rotabgleich** und **Blauabgleich** den Weißabgleich manuell ein.

Belichtung

Wählen Sie einen Belichtungsmodus, sich rasch verändernde unregelmäßige Bildeffekte zu verringern, zum Beispiel durch unterschiedliche Lichtquellen verursachtes Flimmern. Wir empfehlen dem automatischen Belichtungsmodus oder dieselbe Frequenz wie Ihr Stromnetz.

Belichtungsmodus:

- **Automatisch**: Die Kamera stellt Blende, Verstärkung und Verschlusszeit selbsttätig ein.
- **Automatic aperture (Automatische Blendeneinstellung)** : Die Kamera stellt Blende und Verstärkung selbsttätig ein. Die Verschlusszeit ist vorgegeben.
- **Automatic shutter (Automatische Verschlusseinstellung)** : Die Kamera stellt die Verschlusszeit und die Verstärkung automatisch ein. Die Blende ist vorgegeben.
- **Hold current (Aktuelle Einstellung beibehalten)**: Behält die aktuellen Belichtungseinstellungen bei.
- **Flicker-free (Flimmerfrei)** : Die Kamera stellt unter Verwendung folgender Verschlusszeiten Blende und Verstärkung automatisch ein: 1/50 s (50 Hz) und 1/60 s (60 Hz).
- **Flicker-free 50 Hz (Flimmerfrei 50 Hz)** : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/50 s der Blende und Verstärkung selbsttätig ein.
- **Flicker-free 60 Hz (Flimmerfrei 60 Hz)** : Die Kamera stellt unter Verwendung einer Verschlusszeit ist mit 1/60 s der Blende und Verstärkung selbsttätig ein.
- **Flicker-reduced (Flimmerreduziert)** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden (50 Hz) und 1/120 Sekunden (60 Hz) einsetzen.
- **Flicker-reduced 50 Hz (Flimmerreduziert 50 Hz)** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/100 Sekunden einsetzen.
- **Flicker-reduced 60 Hz (Flimmerreduziert 60 Hz)** : Wie flimmerfrei, allerdings kann die Kamera bei stärker ausgeleuchteten Szenen beliebige Verschlusszeiten von kürzer als 1/120 Sekunden einsetzen.
- **Manual (Manuell)** : Die Blendenöffnung, Verstärkung und Verschlusszeit sind vorgegeben.

Exposure zone (Belichtungszone) : Verwenden Sie Belichtungsbereiche, um die Belichtung in einem ausgewählten Teil der Szene zu optimieren, z. B. dem Bereich vor einer Eingangstür.

Hinweis

Die Belichtungsbereiche beziehen sich auf das Originalbild (nicht gedreht); die Bereichsnamen gelten für das Originalbild. Wenn zum Beispiel der Videostream um 90° gedreht wird, dann wird der **Obere** Bereich zum **Unteren** Bereich des Streams und der **linke** Bereich zum **rechten** Bereich.

- **Automatisch**: Für die meisten Situationen geeignet.
- **Mitte**: Damit wird anhand eines einen fest definierten Bereichs in der Bildmitte die Belichtung berechnet. Dieser Bereich hat in der Live-Ansicht eine feste Größe und Position.
- **Full (Voll)** : Damit wird anhand der kompletten Live-Ansicht die Belichtung berechnet.
- **Upper (Oben)** : Damit wird anhand eines festgelegten Bereichs im oberen Teil des Bildes die Belichtung berechnet.
- **Lower (Unten)** : Damit wird anhand eines festgelegten Bereichs im unteren Teil des Bildes die Belichtung berechnet.

- **Left (Links)** : Damit wird anhand eines festgelegten Bereichs im linken Teil des Bildes die Belichtung berechnet.
- **Right (Rechts)** : Damit wird anhand eines festgelegten Bereichs im rechten Teil des Bildes die Belichtung berechnet.
- **Genau**: Damit wird anhand eines Bereichs mit festgelegter Größe und Position die Belichtung berechnet.
- **Benutzerdefiniert**: Damit wird anhand eines Ausschnitts der Live-Ansicht die Belichtung berechnet. Sie können Größe und Position des Bereichs anpassen.

Maximale Verschlusszeit: Wählen Sie die Verschlusszeit für beste Bildqualität. Zu lange Verschlusszeiten (längere Belichtung) können Bewegungsunschärfe erzeugen, wobei zu kurze Verschlusszeiten die Bildqualität beeinträchtigen können. „Max. Verschluss" verbessert das Bild mithilfe der maximalen Verstärkung.

Maximierte Verstärkung: Wählen Sie die passende maximale Verstärkung aus. Wenn Sie die maximale Verstärkung erhöhen, wird die Detailschärfe dunkler Bilder verbessert, jedoch auch den Rauschpegel erhöht. Mehr Rauschen kann auch mehr Bedarf an Bandbreite und Speicherplatz bewirken. Wenn Sie die maximale Verstärkung auf einen hohen Wert festgelegen, kann die Bildqualität bei verschiedenen Lichtverhältnissen (Tag/Nacht) sehr unterschiedlich ausfallen. Max. Verstärkung verbessert das Bild mithilfe der maximalen Verschlusszeit.

Motion-adaptive exposure (Bewegungsadaptierte Belichtung) : Wählen Sie diese Option, um die Bewegungsunschärfe bei schlechten Lichtverhältnissen zu verringern.

Balance zwischen Bewegungsunschärfe und Rauschen: Passen Sie mithilfe des Schiebereglers an, ob Bewegungsschärfe oder geringes Rauschen Vorrang hat. Um geringere Bandbreite und geringes Rauschen auf Kosten den Bewegungsschärfe zu bevorzugen, schieben Sie den Schieberegler in Richtung **Geringes Rauschen**. Um Bewegungsschärfe auf Kosten geringer Bandbreite und geringen Rauschens zu bevorzugen, schieben den Schieberegler in Richtung **Geringe Bewegungsunschärfe**.

Hinweis

Sie können die Belichtung entweder durch Einstellen der Belichtungszeit oder der Verstärkung verändern. Die Erhöhung der Belichtungszeit führt dies zu mehr Bewegungsunschärfe und die Erhöhung der Verstärkung zu mehr Rauschen. Wenn Sie den **Kompromiss zwischen Unschärfe und Rauschen** in Richtung **Geringes Rauschen** einstellen, wird die automatische Belichtung bei erhöhter Belichtung eher längeren Belichtungszeiten Vorrang geben und umgekehrt, wenn Sie den Kompromiss in Richtung **Geringe Bewegungsunschärfe** anpassen. Bei schwachem Licht erreichen sowohl die Verstärkung und die Belichtungszeit letztendlich ihren jeweiligen Maximalwert und es wird keiner der beiden mehr bevorzugt.

Lock aperture (Blendenöffnung arretieren) : Aktivieren Sie diese Option, um die mithilfe des Schiebereglers der **Blendenöffnung** eingestellte Blendenöffnung zu halten. Aktivieren Sie diese Option, um der Kamera zu erlauben, den Bildfokus automatisch an die Blendenöffnung anzupassen. Sie können z. B. die Öffnung für Szenen mit konstanten Lichtverhältnissen feststellen.

Aperture (Blendenöffnung) : Passen Sie mithilfe des Schiebereglers die Blendenöffnung an, d. h. wie viel Licht durch das Objektiv gelassen wird. Bewegen Sie den Schieberegler in Richtung **Öffnen**, damit mehr Licht in den Sensor gelangen kann, um bei schwachen Lichtverhältnissen ein helleres Bild zu erzeugen. Eine große Blendenöffnung reduziert auch die Schärfentiefe, d.h. dass sich nahe der Kamera oder weit von ihr entfernt befindliche Objekte nur unscharf erfasst werden. Bewegen Sie den Schieberegler in Richtung **Geschlossen**, damit ein das Bild stärker fokussiert werden kann.

Belichtungsgrad: Stellen Sie mithilfe des Schiebereglers die Bildbelichtung ein.

Defog (Entnebelung) : Aktivieren Sie diese Option, damit Nebelwetter erkannt wird und zur Erzeugung eines deutlicheres Bilds Nebeleffekte erfasst und entfernt wird.

Hinweis

Wir raten Ihnen davon ab, bei Szenen mit geringem Kontrast, großen Unterschieden in den Lichtverhältnissen oder bei leicht unscharfem Autofokus **Entnebelung** zu aktivieren. Dies kann die Bildqualität beispielsweise durch erhöhten Kontrast beeinflussen. Bei aktivierter Entnebelung kann sich außerdem zu große Helligkeit negativ auf die Bildqualität auswirken.

Videostream

Allgemeines

Auflösung: Eine für die zu überwachende Szene geeignete Bildauflösung wählen. Eine höhere Auflösung erfordert mehr Bandbreite und Speicherplatz.

Bildrate: Um Bandbreitenprobleme im Netzwerk zu vermeiden oder den Speicherbedarf zu reduzieren, kann die Bildrate auf eine feste Größe begrenzt werden. Wird die Bildrate bei Null belassen, wird die unter den aktuellen Bedingungen höchstmögliche Bildrate zugelassen. Höhere Bildraten erfordern mehr Bandbreite und Speicherkapazität.

P-Frames: Ein P-Frame ist ein vorhersagbares Einzelbild, das nur die Bildänderungen gegenüber dem vorangehenden Einzelbild anzeigt. Geben Sie die gewünschte Anzahl von P-Frames ein. Je höher die Anzahl, desto weniger Bandbreite ist erforderlich. Tritt aber im Netzwerk ein Datenstau auf, könnte es zu einer merklichen Verschlechterung der Videoqualität kommen.

Komprimierung: Stellen Sie mithilfe des Schiebereglers die Bildkomprimierung ein. Höhere Komprimierung hat eine niedrigere Bitrate und eine geringere Bildqualität zur Folge. Eine niedrigere Komprimierung verbessert die Bildqualität, benötigt jedoch beim Aufzeichnen eine höhere Bandbreite und mehr Speicher.

Signiertes Video : Aktivieren Sie diese Option, um Videos die Funktion Signiertes Video hinzuzufügen. Signiertes Video schützt durch das Hinzufügen von kryptografischen Signaturen das Video vor Manipulation.

Zipstream

Zipstream ist eine Technologie zur Bitratenreduzierung, die für die Videosicherheit optimiert wurde. Sie reduziert in Echtzeit die durchschnittliche Bitrate eines H.264- oder H.265-Streams. Bei Szenen mit mehreren Interessensbereichen wendet Axis Zipstream eine hohe Bitrate an, z.B. bei Szenen mit sich bewegenden Objekten. Ist die überwachte Szene eher statisch, wendet Zipstream eine niedrigere Bitrate an und reduziert so den Bedarf an Speicherplatz. Weitere Informationen dazu finden Sie unter *Reduzierung der Bitrate mit Axis Zipstream*

Strength (Stärke) der Bitrate-Verringerung wählen:

- **Aus**: Keine Reduzierung der Bitrate.
- **Niedrig**: In den meisten Szenen keine sichtbaren Qualitätseinbußen Dies ist die Standardoption, die bei allen Szenentypen zur Reduzierung der Bitrate verwendet werden kann.
- **Mittel**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und leicht verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **Hoch**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen). Diese Stufe wird für mit der Cloud verbundene Geräte und Geräte empfohlen, die auf lokalen Speicher zurückgreifen.
- **Höher**: Sichtbare Auswirkungen in einigen Szenen, mit weniger Rauschen und verringerte Detailschärfe in Bereichen von untergeordnetem Interesse (zum Beispiel Bereichen ohne Bewegungsaufkommen).
- **Extreme (Extrem)**: Sichtbarer Effekt in den meisten Szenen: Die Bitrate wird für den kleinsten Speicher optimiert.

Für Speicherung optimieren: Aktivieren Sie dies, um die Bitrate zu minimieren und dabei die Qualität zu erhalten. Die Optimierung wird nicht auf den im Webclient angezeigten Videostream angewendet. Dies kann nur verwendet werden, wenn Ihr VMS B-Rahmen unterstützt. Durch Aktivieren von **Optimize for storage** (Speicheroptimierung) wird auch **Dynamic GOP** aktiviert.

Dynamische FPS (Bilder pro Sekunde): Aktivieren Sie diese Option, damit sich die Bandbreite je nach Aktivitätsniveau der Szene ändern kann. Mehr Aktivität erfordert mehr Bandbreite.

Lower limit (Unterer Grenzwert): Geben Sie einen Wert ein, um je nach Bewegung in der Szene die Bildrate zwischen der Mindestanzahl an Bildern pro Sekunde und den Standardanzahl an Bilder pro Sekunde anzupassen. Wir empfehlen, bei Szenen mit sehr geringer Bewegung, bei denen die Anzahl an Bilder pro Sekunde auf 1 oder niedriger fallen können, einen unteren Grenzwert anzugeben.

Dynamic GOP (Group of Pictures): Aktivieren Sie diese Option, um das Intervall zwischen I-Frames anhand des Aktivitätsniveaus der Szene dynamisch anzupassen.

Upper limit (Oberer Grenzwert): Geben Sie eine maximale GOP-Länge ein, das heißt die maximale Anzahl von P-Frames zwischen zwei I-Frames. Ein I-Frame ist ein Einzelbild, das unabhängig von anderen Einzelbildern dekodierbar ist.

Bitrate-Steuerung

- **Durchschnitt**: Wählen Sie diese Option, um die Bitrate automatisch über einen längeren Zeitraum anzupassen und je nach verfügbaren Speicher die bestmögliche Bildqualität zu liefern.
  -  Klicken Sie darauf, um die Zielbitrate anhand des verfügbaren Speichers, der Aufbewahrungszeit und des Bitratenlimits zu berechnen.
  - **Zielbitrate**: Geben Sie die gewünschte Zielbitrate ein.
  - **Aufbewahrungszeit**: Geben Sie die Aufbewahrungszeit für Aufzeichnungen in Tagen ein.
  - **Speicher:** Zeigt den für den Videostream nutzbaren geschätzten Speicherplatz an.
  - **Maximale Bitrate**: Aktivieren Sie diese Option, um eine Bitratengrenze festzulegen.
  - **Bitratenlimit**: Geben Sie eine Bitratengrenze ein, die über der Zielbitrate liegt.
- **Maximum**: Wählen Sie diese Option, um die maximale Sofort-Bitrate des Videostreams auf Grundlage der Netzwerkbandbreite festzulegen.
  - **Maximum**: Geben Sie die maximale Bitrate ein.
- **Variable**: Wählen Sie diese Option, damit sich die Bitrate je nach Aktivitätsniveau der Szene anpasst. Mehr Aktivität erfordert mehr Bandbreite. Diese Option wird für die meisten Situationen empfohlen.

Ausrichtung

Mirror (Spiegelung): Aktivieren Sie diese Option, um das Bild zu spiegeln.

Audio

Include (Integrieren): Aktivieren Sie diese Option, um Audio im Videostream zu verwenden.

Source (Quelle) : Wählen die zu verwendende Audioquelle.

Stereo : Aktivieren Sie diese Option, um sowohl integriertes Audio als auch Audio von einem externen Mikrofon zu verwenden.

Overlays

: Klicken Sie darauf, um ein Overlay hinzuzufügen. Wählen Sie in der Auswahlliste den Typ des Overlays aus:

- **Text**: Wählen Sie diese Option, um einen Text anzeigen zu lassen, der in das Live-Ansichtsbild integriert und in allen Ansichten, Aufzeichnungen und Schnappschüssen sichtbar ist. Sie können einen eigenen Text eingeben und Sie können auch vorkonfigurierte Modifikatoren verwenden, um z. B. Uhrzeit, Datum und Bildrate automatisch anzeigen zu lassen.
  - : Klicken Sie darauf, um den Datumsmodifikator `%F` hinzufügen und das Format JJJJ-MM-TT anzuzeigen.
  - : Klicken Sie darauf, um den Uhrzeitmodifikator `%X` hinzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
  - **Modifikatoren**: Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel `%a` den Wochentag an.
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  - **Appearance (Darstellung)**: Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
- **Bild**: Wählen Sie diese Option, um ein statisches Bild über dem Videostream zu zeigen. Sie können .bmp-, .png-, .jpeg- oder .s jpeg-Dateien verwenden.
  Um ein Bild hochzuladen, klicken Sie auf **Manage images (Bilder verwalten)**. Bevor Sie ein Bild hochladen, können Sie folgende Optionen festlegen:
  - **An Auflösung anpassen**: Wählen Sie diese Option, um das Overlay-Bild automatisch an die Videoauflösung anzupassen.
  - **Transparenz verwenden**: Wählen Sie den Hexadezimal-RGB-Wert für diese Farbe und geben Sie diesen ein. Verwenden Sie das Format RRGGBB. Beispiele für Hexadezimalwerte: FFFFFF für Weiß, 000000 für Schwarz, FF0000 für Rot, 6633FF für Blau und 669900 für Grün. Nur bei .bmp-Bildern.
- **Scene annotation (Szenen-Kennzeichnung)** : Wählen Sie diese Option aus, um im Videostream ein Text-Overlay anzuzeigen, das an derselben Position bleibt, auch wenn die Kamera in eine andere Richtung schwenkt oder neigt. Sie können festlegen, dass das Overlay nur innerhalb bestimmter Zoomstufen angezeigt wird.
  - : Klicken Sie darauf, um den Datumsmodifikator `%F` hinzufügen und das Format JJJJ-MM-TT anzuzeigen.
  - : Klicken Sie darauf, um den Uhrzeitmodifikator `%X` hinzufügen und das Format hh:mm:ss (24-Stunden) anzeigen zu lassen.
  - **Modifikatoren**: Klicken Sie darauf, um beliebige der in der Liste angezeigten Modifikatoren auszuwählen und sie dem Textfeld hinzuzufügen. So zeigt zum Beispiel `%a` den Wochentag an.
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  - **Appearance (Darstellung)**: Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).

-  : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben. Das Overlay wird gespeichert und verbleibt in den Schwenk- und Neigekoordinaten dieser Position.
- **Annotation between zoom levels (%) (Kennzeichnung zwischen diesen Zoomstufen (%))**: Legen Sie die Zoomstufen fest, innerhalb derer das Overlay angezeigt wird.
- **Annotation symbol (Kennzeichnungssymbol)**: Wählen Sie ein Symbol aus, das anstelle des Overlays angezeigt wird, wenn sich die Kamera nicht innerhalb der eingestellten Zoomstufen befindet.

- **Streaming indicator (Streaming-Anzeige)**  : Wählen Sie diese Option, um eine Animation über dem Videostream zu einzublenden. Die Animation zeigt an, dass der Videostream live ist, selbst wenn die Szene aktuell bewegungsfrei ist.
  - **Appearance (Darstellung)**: Wählen Sie die Farbe der Animation und des Hintergrunds, zum Beispiel rote Animation auf durchsichtigem Hintergrund (Standardeinstellung).
  - **Size (Größe)**: Wählen Sie die gewünschte Schriftgröße.
  -  : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
- **Widget: Linegraph (Liniendiagramm)**  : Zeigt ein Diagramm an, das verdeutlicht, wie sich ein Messwert im Laufe der Zeit ändert.
  - **Title (Titel)**: Einen Titel für das Widget eingeben.
  - **Overlay modifier (Overlay-Modifikator)**: Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
  -  : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
  - **Size (Größe)**: Die Größe des Overlays auswählen.
  - **Auf allen Kanälen sichtbar**: Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
  - **Aktualisierungsintervall**: Wählen Sie die Zeit zwischen Datenaktualisierungen.
  - **Transparency (Transparenz)**: Legen Sie die Transparenz des gesamten Overlays fest.
  - **Hintergrundtransparenz**: Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
  - **Punkte**: Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
  - **X-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die x-Achse ein.
    - **Zeitfenster**: Geben Sie ein, wie lange die Daten visualisiert werden sollen.
    - **Zeiteinheit**: Geben Sie eine Zeiteinheit für die x-Achse ein.
  - **Y-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die y-Achse ein.
    - **Dynamische Skala**: Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
    - **Min. Alarmschwelle** und **Max. Alarmschwelle**: Diese Werte fügen dem Diagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.

- **Widget: Meter (Zähler)** : Zeigen Sie ein Balkendiagramm an, das den zuletzt gemessenen Datenwert anzeigt.
  - **Title (Titel)**: Einen Titel für das Widget eingeben.
  - **Overlay modifier (Overlay-Modifikator)**: Wählen Sie einen Overlay-Modifikator als Datenquelle aus. Wenn Sie MQTT-Overlays erstellt haben, werden diese am Ende der Liste angezeigt.
  - : Wählen Sie die Position des Overlay im Bild aus oder klicken und ziehen Sie das Overlay, um es in der Live-Ansicht zu verschieben.
  - **Size (Größe)**: Die Größe des Overlays auswählen.
  - **Auf allen Kanälen sichtbar**: Deaktivieren Sie die Option, um nur auf Ihrem aktuell ausgewählten Kanal anzuzeigen. Schalten Sie diese Option ein, um auf allen aktiven Kanälen anzuzeigen.
  - **Aktualisierungsintervall**: Wählen Sie die Zeit zwischen Datenaktualisierungen.
  - **Transparency (Transparenz)**: Legen Sie die Transparenz des gesamten Overlays fest.
  - **Hintergrundtransparenz**: Stellen Sie die Transparenz nur für den Hintergrund des Overlays ein.
  - **Punkte**: Schalten Sie diese Option ein, um der Diagrammlinie einen Punkt hinzuzufügen, wenn Daten aktualisiert werden.
  - **Y-Achse**
    - **Label (Bezeichnung)**: Geben Sie die Textbeschriftung für die y-Achse ein.
    - **Dynamische Skala**: Schalten Sie diese Option ein, damit sich die Skala automatisch an die Datenwerte anpasst. Schalten Sie diese Option aus, um Werte für eine feste Skala manuell einzugeben.
    - **Min. Alarmschwelle** und **Max. Alarmschwelle**: Diese Werte fügen dem Balkendiagramm horizontale Referenzlinien hinzu, sodass Sie leichter erkennen können, wann der Datenwert zu hoch oder zu niedrig wird.

Privatzonenmasken

: Klicken Sie darauf, um eine neue Privatzonenmaske zu erstellen.

Privatzonenmasken: Klicken Sie darauf, um die Farbe aller Privatzonenmasken zu ändern oder um alle Privatzonenmasken dauerhaft zu löschen.

Mask x (Maske x): Klicken Sie darauf, um die Maske umzubenennen, zu deaktivieren oder dauerhaft zu löschen.

Kommunikation

SIP

Einstellungen

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

SIP-Einrichtungsassistent: Klicken Sie hier, um SIP schrittweise einzurichten und zu konfigurieren.

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

Eingehende Anrufe zulassen: Diese Option wählen, um eingehende Anrufe von anderen SIP-Geräten zuzulassen.

Anrufbearbeitung

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

Ports

Eine Portnummer muss zwischen 1024 und 65535 liegen.

- **SIP-Port**: Der für die SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port ist nicht verschlüsselt. Der Standardport ist 5060. Geben Sie eine andere Portnummer ein, falls erforderlich.
- **TLS_Port**: Der für verschlüsselte SIP-Kommunikation genutzte Netzwerkport. Der Datenverkehr über diesen Port wird mittels Transport Layer Security (TLS) verschlüsselt. Der Standardport ist 5061. Geben Sie eine andere Portnummer ein, falls erforderlich.
- **RTP-Startport**: Der Netzwerkport, der für den ersten RTP-Medienstream in einem SIP-Anruf verwendet wird. Der standardmäßige Startport ist 4000. Einige Firewalls blockieren den RTP-Datenaustausch über bestimmte Portnummern.

NAT-Traversal

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

Hinweis

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

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

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

Audio und Video

- **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.
- **H.264-Paketierungsmodus**: Wählen Sie den zu verwendenden Paketierungsmodus aus.
  - **Auto**: (Empfohlen) Das Gerät entscheidet, welcher Paketierungsmodus verwendet wird.

  - **None (Kein)**: Es wird kein Paketierungsmodus festgelegt. Dieser Modus wird häufig als Modus **0** bezeichnet.
  - **0**: Nicht-verschachtelter Modus.
  - **1**: Modus für eine einzelne NAL-Einheit.
- **Videoausrichtung**: Wählen Sie zulässige Videorichtungen.
- **Zeigt Video in Anruf an** : Zeigt den eingehenden Videostream auf dem Bildschirm des Geräts an.

Zusätzliches

- **Wechsel von UDP zu TCP**: Wählen Sie diese Option, um vorübergehend vom Übertragungsprotokoll (User Datagram Protocol) auf das Protokoll TCP (Transmission Control Protocol) zu wechseln. Mit einem Wechsel wird Fragmentierung vermieden und der Wechsel kann stattfinden sofern eine Anfrage innerhalb von 200 Bytes der maximalen Übertragungseinheit (MTU) liegt oder größer als 1300 Byte ist.
- **Über Umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Kontakt umschreiben zulassen**: Wählen Sie diese Option, um die lokale IP-Adresse anstelle der öffentlichen IP-Adresse des Routers zu senden.
- **Register with server every (Alle ... am Server registrieren)**: Legen Sie fest, wie oft sich das Gerät am SIP-Server für SIP-Konten registrieren soll.
- **DTMF-Nutzlasttyp**: Ändert den Standard-Nutzlasttyp für DTMF.
- **Max retransmissions (Max. erneute Übertragungen)**: Legen Sie fest, wie oft das Gerät maximal versuchen soll, eine Verbindung zum SIP-Server herzustellen.
- **Seconds until failback (Sekunden bis zum Ausfall)**: Legen Sie die Anzahl der Sekunden fest, die das Gerät nach einem Failover auf einen sekundären SIP-Server warten soll, bis es erneut versucht, eine Verbindung zum primären SIP-Server herzustellen.

Konten

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

Das Konto wurde erfolgreich beim SIP-Server registriert.

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

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

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

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

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

DTMF

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

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

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

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

Protokolle

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

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

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

Testanruf

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

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

Zugangsliste

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

Richtlinie:

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

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

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

VMS-Anrufe

VMS-Anrufe

Anrufe in der Video Management Software (VMS) zulassen: Auswählen, um Anrufe vom Gerät zur VMS zuzulassen. Sie können VMS-Anrufe tätigen, auch wenn SIP ausgeschaltet ist.

Call timeout (Zeitüberschreitung bei Anruf): Legen Sie die maximale Dauer eines Anrufversuchs fest, wenn niemand antwortet.

Kontaktliste

Kontakte

Klicken Sie hier, um die Kontaktliste als JSON-Datei herunterzuladen.

Klicken Sie hier, um eine Kontaktliste (json) zu importieren.

Kontakt hinzufügen: Klicken Sie, um der Kontaktliste einen neuen Kontakt hinzuzufügen.

Bild hochladen : Klicken Sie hier, um ein Bild hochzuladen, das den Kontakt darstellt.

First name (Vorname): Geben Sie den Vornamen des Kontakts ein.

Last name (Nachname): Geben Sie den Nachnamen des Kontakts ein.

Schnellwahl : Geben Sie eine verfügbare Schnellwahlnummer für den Kontakt ein. Diese Nummer wird verwendet, um den Kontakt vom Gerät aus anrufen.

SIP-Adresse: Geben Sie die IP-Adresse oder Durchwahl des Kontakts ein, falls Sie SIP verwenden.

: Klicken Sie hier, um einen Testanruf zu tätigen. Der Anruf wird nach der Annahme automatisch beendet.

SIP-Konto: Wählen Sie das SIP-Konto für den Anruf vom Gerät zum Kontakt aus, falls Sie SIP verwenden.

Verfügbarkeit: Wählen Sie den Verfügbarkeitszeitplan des Kontakts aus. Sie können Zeitpläne unter **System > Events (Ereignisse) > Schedules (Zeitpläne)** hinzufügen oder anpassen. Wenn ein Anruf versucht wird, obwohl der Kontakt nicht verfügbar ist, wird der Anruf abgebrochen, es sei denn, es gibt einen Ersatzkontakt.

Fallback (Ausweichoption): Wählen Sie bei Bedarf einen Ersatzkontakt aus der Liste aus.

Hinweise: Fügen Sie optionale Informationen über den Kontakt hinzu.

Das Kontextmenü enthält:

Edit contact (Kontakt bearbeiten): Eigenschaften des Kontakts bearbeiten.

Delete contact (Kontakt löschen): Den Kontakt löschen.

Gruppen

Klicken Sie hier, um die Kontaktliste als JSON-Datei herunterzuladen.

Klicken Sie hier, um eine Kontaktliste (json) zu importieren.

Add group (Gruppe hinzufügen): Klicken Sie hier, um eine neue Gruppe aus bestehenden Kontakten zu erstellen.

Bild hochladen : Klicken Sie hier, um ein Bild hochzuladen, das die Gruppe darstellt.

Name: Geben Sie einen Namen für die Gruppe ein.

Use for group calls only (Nur für Gruppenanrufe verwenden): Einschalten, um die Gruppe nur für Gruppenanrufe zu verwenden. Ausschalten, wenn Sie einzelne Kontakte zu einer Gruppe hinzufügen möchten, diese jedoch nicht für Gruppenanrufe verwenden möchten.

Speed dial (Schnellwahl): Geben Sie eine verfügbare Schnellwahlnummer für die Gruppe ein. Diese Nummer wird verwendet, um die Gruppe vom Gerät aus anrufen. Nur für Gruppenanrufgruppen.

Recipients (Empfänger): Wählen Sie die Kontakte aus, die in die Gruppe aufgenommen werden sollen. Anrufe gehen gleichzeitig an alle Empfänger. Die maximale Anzahl der Empfänger ist sechs.

Fallback (Ausweichoption): Wählen Sie bei Bedarf einen Ersatzkontakt aus der Liste aus. Nur für Gruppenanrufgruppen.

Hinweise: Fügen Sie optionale Informationen über die Gruppe hinzu.

Das Kontextmenü enthält:

Edit group (Gruppe bearbeiten): Bearbeiten der Gruppeneigenschaften.

Delete group (Gruppe löschen): Löscht die Gruppe.

Anrufe

Allgemeines

Audio

Hinweis

- Der ausgewählte Audioclip wird nur bei einem Anruf abgespielt.
- Bei Änderung des Audioclips oder der Lautstärke während eines laufenden Anrufs wird die Änderung erst beim nächsten Anruf wirksam.

Ringtone (Klingelton): Wählen Sie den Audioclip aus, der bei einem eingehenden Anruf auf dem Gerät abgespielt werden soll. Stellen Sie die Lautstärke mithilfe des Schiebereglers ein.

Ringback tone (Freizeichen): Wählen Sie den Audioclip aus, der bei einem ausgehenden Anruf auf dem Gerät abgespielt werden soll. Stellen Sie die Lautstärke mithilfe des Schiebereglers ein.

Anzeige

Seiten

Hinzufügen: Erstellen Sie eine neue Seite für den Bildschirm.

Name: Geben Sie der Seite einen Namen, unter dem Sie sie leicht identifizieren können.

Background image (Hintergrundbild): Wählen Sie ein Bild aus der Mediathek aus, das Sie als Hintergrund verwenden möchten. Die optimale Auflösung beträgt 480x800 Pixel. Die maximal zulässige Auflösung beträgt 2048x2048 Pixel.

Hinzufügen: Fügen Sie der Seite ein Widget hinzu, z. B. eine Schaltfläche, einen Text oder ein Bild. Ein Widget ist ein grafisches Element.

Typ: Wählen Sie einen Widget-Typ aus.

- **Schaltfläche - Schaltflächentyp**: Wählen Sie einen Schaltflächentyp.
  - **Kontakt**
    - **Kontakt**: Weisen Sie der Schaltfläche einen Kontakt zu. Besucher drücken die Schaltfläche, um einen Anruf an den Kontakt zu tätigen.
    - **Size (Größe)**: Wählen Sie die Größe der Schaltfläche „Kontakt".
  - **Benutzerdefiniert**
    - **Text**: Geben Sie einen Text ein, der auf der Schaltfläche angezeigt werden soll.
    - **Name**: Geben Sie der Schaltfläche einen Namen, damit Sie sie beim Erstellen einer Regel im Ereignissystem leichter identifizieren können.
    - **Size (Größe)**: Wählen Sie die Größe der Schaltfläche.
- **Bild**
  - **Name**: Geben Sie dem Bild einen Namen.
  - **Bild-Skalierung**
    - **Auto**: Lassen Sie das System die Skalierung des Bildes optimieren.
    - **Anpassen**: Stellen Sie die Skalierung so ein, dass das Bild auf den Bildschirm passt.
    - **Füllen**: Stellen Sie die Skalierung so ein, dass das Bild den Bildschirm ausfüllt.
  - **Bild**: Wählen Sie ein Bild aus der Mediathek aus. Die maximal zulässige Auflösung beträgt 2048x2048 Pixel.
- **Text**
  - **Text**: Geben Sie einen Text ein, der auf dem Bildschirm angezeigt werden soll.
  - **Stil**: Wählen Sie, wie der Text formatiert werden soll.

Speichern: Speichern Sie die Seite, um sie auf dem Bildschirm anzeigen zu können und um Regeln für die Widgets zu erstellen.

Das Kontextmenü enthält:

Edit (Bearbeiten): Passen Sie die Seite an.

Zurücksetzen: Nicht gespeicherte Änderungen an der Seite rückgängig machen.

Kopieren: Erstellen Sie eine Kopie der Seite.

Als Standard-Homepage definieren: Legen Sie fest, dass diese Seite angezeigt werden soll, wenn keine zeitlich geplante Seite aktiv ist. Sie müssen eine Seite speichern, bevor Sie sie als Homepage festlegen können.

Schedule (Zeitplan): Wählen Sie diese Option, um die Seite gemäß einem der Zeitpläne anzuzeigen, die unter **System > Events (Ereignisse) > Schedules (Zeitpläne)** definiert sind.

Löschen: Löschen Sie die Seite. Sie können die als Standard-Homepage eingestellte Seite nicht löschen.

Allgemeines

Device language (Sprache des Geräts): Wählen Sie die Sprache für die Standardtexte auf dem Bildschirm.

Show keypad on homepage (Tastatur auf Homepage anzeigen): Schalten Sie diese Option ein, um ein Tastaturfeld auf der Standard-Startseite anzuzeigen. Die Besucher können den Knopf drücken, um ein Tastaturfeld zu öffnen und mit ihren Zugangsdaten die Tür zu entriegeln.

Bildschirmschoner

Hinzufügen: Klicken Sie hier, um einen neuen Bildschirmschoner zu erstellen.

Seite: Wählen Sie eine Seite aus, die angezeigt werden soll, wenn der Bildschirmschoner aktiv ist.

Dauer: Wählen Sie die Zeitspanne, währen der der Bildschirmschoner angezeigt werden soll.

Edit (Bearbeiten): Wählen Sie einen Bildschirmschoner aus der Liste aus und klicken Sie hier, um ihn anzupassen.

Entfernen: Wählen Sie einen oder mehrere Bildschirmschoner aus der Liste aus und klicken Sie hier, um sie zu löschen.

Settings (Einstellungen): Klicken Sie hier, um die allgemeinen Einstellungen des Bildschirmschoners anzupassen.

Turn off display when inactive (Bildschirm bei Inaktivität ausschalten): Stellen Sie hier ein, wie lange der Bildschirm inaktiv sein darf, bevor er ausgeschaltet wird.

Start screensaver when inactive (Bildschirmschoner starten, wenn inaktiv): Stellen Sie hier ein, wie lange der Bildschirm inaktiv sein darf, bevor der Bildschirmschoner aktiviert wird. Wenn Sie eine Zeit einstellen, die länger ist als die unter **Turn off display when inactive (Bildschirm bei Inaktivität ausschalten)** eingestellte Zeit, wird der Bildschirmschoner nie aktiviert.

Screensaver sequence (Bildschirmschonersequenz): Wählen Sie hier aus, in welcher Reihenfolge die Bildschirmschoner angezeigt werden sollen, wenn es mehrere gibt. Jeder Bildschirmschoner wird für die unter **Duration (Dauer)** eingestellte Zeit angezeigt.

- **Listed (Aufgeführt)**: Bildschirmschoner in der aufgeführten Reihenfolge anzeigen.
- **Random (Zufällig)**: Bildschirmschoner in einer zufälligen Reihenfolge anzeigen.

Wake-up trigger (Auslöser zum Reaktivieren aus dem Ruhemodus): Wählen Sie aus, wie der Bildschirm aktiviert werden soll, wenn der Bildschirmschoner aktiv ist oder der Bildschirm ausgeschaltet ist.

- **Touch (Berührung)**: Aktivieren Sie den Bildschirm, wenn jemand ihn berührt.
- **Touch or presence detection (Berührungs- oder Anwesenheitserfassung)**: Aktivieren Sie den Bildschirm, wenn jemand ihn berührt oder wenn das Gerät eine Person vor ihm erfasst.

Analyse

AXIS Object Analytics

Start: Klicken Sie hier, um AXIS Object Analytics zu starten. Die Anwendung wird im Hintergrund ausgeführt und Sie können anhand der aktuellen Einstellungen der Anwendung Regeln für Ereignisse erstellen.

Offen: Klicken Sie hier, um AXIS Object Analytics zu öffnen. Die Anwendung wird in einer neuen Registerkarte geöffnet, in der Sie die Einstellungen konfigurieren können.

Not installed (Nicht installiert): AXIS Object Analytics ist auf diesem Gerät nicht installiert. Aktualisieren Sie AXIS OS auf die neueste Version, um die aktuelle Version der Anwendung zu erhalten.

Metadatenkonfiguration

Hersteller von RTSP-Metadaten

Anzeigen und Verwalten der Datenkanäle, die Metadaten streamen, und der von ihnen verwendeten Kanäle.

Hinweis

Diese Einstellungen gelten für den RTSP-Metadaten-Stream, der ONVIF XML verwendet. Die hier vorgenommenen Änderungen wirken sich nicht auf die Visualisierungsseite der Metadaten aus.

Produzent: Ein Datenkanal, der das Real-Time Streaming Protocol (RTSP) zum Senden von Metadaten verwendet.

Kanal: Der Kanal, der zum Senden von Metadaten von einem Producer verwendet wird. Aktivieren Sie diese Option, um den Videostream für Metadaten zu aktivieren. Schalten Sie diese Option aus Gründen der Kompatibilität oder Ressourcenverwaltung aus.

MQTT

Konfigurieren Sie die Producer, die Metadaten über MQTT (Message Queuing Telemetry Transport) generieren und Videostreams übertragen.

- **Create (Erstellen)**: Klicken Sie hier, um einen neuen MQTT-Producer zu erstellen.
  - **Taste**: Wählen Sie einen vordefinierten Bezeichner aus der Dropdown-Liste, um die Quelle des Videostreams anzugeben.
  - **MQTT-Thema**: Geben Sie einen Namen für das MQTT-Topic ein.
  - **QoS (Quality of Service)**: Stellen Sie den Sicherheitsgrad für die Nachrichtenzustellung (0-2) ein.

Retain messages (Nachrichten aufbewahren): Wählen Sie, ob die letzte Nachricht im MQTT-Topic gespeichert werden soll.

Use MQTT client device topic prefix (MQTT-Client-Geräte-Präfix verwenden): Wählen Sie aus, ob dem MQTT-Topic ein Präfix hinzugefügt werden soll, um die Identifizierung des Quellgeräts zu erleichtern.

Das Kontextmenü enthält:

- **Update (Aktualisieren)**: Ändern Sie die Einstellungen des ausgewählten Producer.
- **Löschen**: Löscht den ausgewählten Producer.

Object snapshot (Objekt-Snapshot): Schalten Sie diese Option ein, um von jedem erfassten Objekt einen Bildausschnitt zu erstellen.

Additional crop margin (Zusätzliche Ränder um den Bildausschnitt): Schalten Sie diese Option ein, um zusätzliche Ränder um den Bildausschnitt von erkannten Objekten hinzuzufügen.

PTZ

Positionen voreinstellbar

Bei einer voreingestellten Position handelt es sich um eine bestimmte, im Speicher Ihrer Kamera gespeicherte Schwenk-, Neige- und Zoomposition. Mithilfe von voreingestellten Positionen können Sie schnell zwischen verschiedenen Sichtfeldern wechseln. Wenn Ihr Gerät Guard-Touren unterstützt, können Sie mit voreingestellten Positionen automatische Guard-Touren erstellen.

Positionen voreinstellbar

- **Create preset position (Voreingestellte Position erstellen)**: Erstellen Sie auf Grundlage der aktuellen Kameraposition eine neue voreingestellte Position.
  - **Thumbnail (Miniaturansicht)**: Schalten Sie diese Option ein, um die Miniaturansicht für die vordefinierte Position hinzuzufügen.
  - **Name**: Geben Sie einen Namen für die Positionsvoreinstellung ein.
  - **Ausgangsposition**: Aktivieren Sie dies, um diese Position als Standardsichtfeld Ihrer Kamera festzulegen. Die Home-Position ist mit gekennzeichnet. Ihre Kamera hat immer eine Home-Position.

Einstellungen

- **Return to home position when inactive (Zur Home-Position zurückkehren wenn inaktiv)**: Aktivieren Sie diese Funktion, damit die Kamera nach einer bestimmten Zeit der Nichtaktivität wieder in ihre Home-Position zurückkehren kann.
- **Use thumbnails (Miniaturansichten verwenden)**: Schalten Sie diese Option ein, um die Miniaturansicht automatisch hinzuzufügen, wenn Sie eine vordefinierte Position hinzufügen.

Das Kontextmenü enthält:

- **Create thumbnails (Miniaturansichten erstellen)** : Erstellen Sie eine Miniaturansicht für alle Ihre voreingestellten Positionen.
- **Refresh thumbnails (Miniaturansichten aktualisieren)**: Ersetzen Sie die Miniaturansichten für Ihre voreingestellten Positionen durch neue und aktualisierte Miniaturansichten.
- **Delete all preset positions (Alle vordefinierten Positionen löschen)**: Entfernen Sie alle voreingestellten Positionen. Dadurch wird automatisch eine neue Home-Position erstellt.

Guard-Tours

Rundgangüberwachung: Guard-Tour erstellen.

- **Preset position (Voreingestellte Position):** Wählen Sie diese Option, um eine Guard-Tour mit vordefinierten Positionen zu erstellen.
- **Recorded (Aufgezeichnet)**: Wählen Sie diese Option, um eine aufgezeichnete Guard-Tour zu erstellen.

Voreingestellte Position

Eine Guard-Tour mit voreingestellten Positionen streamt kontinuierlich Videostreams von einer Auswahl von voreingestellten Positionen in einer zufälligen oder festen Sequenz. Sie können auswählen, wie lange die Kamera an jeder voreingestellten Position bleiben soll, bevor sie zur nächsten wechselt. Die Guard-Tour läuft bis zum Anhalten in endloser Endlosschleife, selbst wenn keine Clients (Web Browser) das Videomaterial streamen.

Einstellungen

- **Allgemeine Einstellungen**
  - **Name**: Geben Sie einen Namen für die Guard-Tour ein.
  - **Play guard tour in random order (Guard-Tour in Zufallsreihenfolge abspielen)**: Aktivieren Sie dies, damit sich die Kamera während der Guard-Tour unberechenbar zwischen den voreingestellten Positionen bewegt.
  - **Pause between runs (Zwischen einzelnen Rundgängen anhalten)**: Geben Sie das gewünschte Zeitintervall zwischen den Guard-Tours ein. Sie können ein beliebiges Intervall von 0 Minuten bis 2 Stunden und 45 Minuten eingeben.
- **Schritteinstellungen**
  - **Dauer**: Wählen Sie aus, wie lange die Kamera an jeder voreingestellten Position bleiben soll. Der Standardwert ist 10 Sekunden und der maximal zulässige Wert ist 60 Minuten.
  - **Move speed (Bewegungsgeschwindigkeit)**: Wählen Sie, wie schnell die Kamera zur nächsten voreingestellten Position wechseln soll. Der Standardwert ist 70. Sie können jedoch einen beliebigen Wert von 1 bis 100 wählen.

Voreingestellte Positionen: Um mehrere voreingestellte Positionen auszuwählen, drücken Sie die UMSCHALTTASTE, während Sie die voreingestellten Positionen auswählen. Klicken Sie auf ⁘ und ziehen Sie die vordefinierten Positionen in den Bereich **View order (Reihenfolge anzeigen)**.

View order (Reihenfolge anzeigen): Zeigt die vordefinierten Positionen an, die in der Guard-Tour enthalten sind.

- **Import all preset positions (Alle voreingestellten Positionen importieren)**: Fügen Sie alle voreingestellten Positionen in der Reihenfolge hinzu, in der sie erstellt wurden, beginnend mit der ältesten.
- ▷: Guard-Tour starten.

Aufgezeichnet

Bei einer aufgezeichneten Tour handelt es sich um die Wiedergabe einer aufgezeichneten Abfolge von PTZ-Bewegungen einschließlich der jeweiligen Verfahrgeschwindigkeiten und -längen.

Allgemeine Einstellungen

- **Name**: Geben Sie einen Namen für die Guard-Tour ein.
- **Pause between runs (Zwischen einzelnen Rundgängen anhalten)**: Geben Sie das gewünschte Zeitintervall zwischen den Guard-Tours ein. Sie können ein beliebiges Intervall von 0 Minuten bis 2 Stunden und 45 Minuten eingeben.

Aufgezeichneter Rundgang

- **Start recording tour (Rundgangaufzeichnung starten)**: Beginnt mit der Aufzeichnung der Schwenk-/Neige-/Zoombewegungen, die von der Guard-Tour repliziert werden soll.
- **Stop recording tour (Rundgangaufzeichnung anhalten)**: Beenden Sie die Aufzeichnung der Schwenk-/Neige-/Zoombewegungen, die von der Guard-Tour repliziert werden soll.
- **Re-record** (Neu aufzeichnen): Startet eine neue Aufzeichnung von Schwenk-/Neige-/Zoombewegungen. Dadurch wird Ihre letzte Aufzeichnung überschrieben.
-  Starten Sie die aufgezeichnete Tour.
-  Halten Sie die aufgezeichnete Tour an.
-  Halten Sie die aufgezeichnete Tour an.

Grenzwerte

Um den zu überwachenden Bereich einzugrenzen, können Sie die PTZ-Bewegungen begrenzen.

Save as Pan 0☐(Als Nullstellung Schwenken speichern): Klicken Sie hier, um die aktuelle Position als Nullpunkt für Schwenkkoordinaten festzulegen.

Pan-tilt limits (Grenzwerte Schwenken/Neigen): Die Kamera verwendet die Koordinaten des Bildmittelpunkts, wenn Sie Grenzwerte Schwenken/Neigen festlegen.

- **Left pan limit (Grenzwert Schwenken links)**: Klicken Sie hier, um die Schwenkbewegungen der Kamera nach links zu begrenzen. Klicken Sie erneut, um den Grenzwert zu entfernen.
- **Grenzwert Schwenken rechts**: Klicken Sie hier, um die Schwenkbewegungen der Kamera nach rechts zu begrenzen. Klicken Sie erneut, um den Grenzwert zu entfernen.
- **Top tilt limit (Oberer Neigegrenzwert)**: Klicken Sie hier, um die Neigungsbewegungen der Kamera auf den oberen Bereich zu beschränken. Klicken Sie erneut, um den Grenzwert zu entfernen.
- **Bottom tilt limit (Unterer Neigegrenzwert)**: Klicken Sie hier, um die Neigungsbewegungen der Kamera auf den unteren Bereich zu beschränken. Klicken Sie erneut, um den Grenzwert zu entfernen.

Auto-flip (Auto-Flip) : Der Kamerakopf kann sofort um 360° umgekehrt und über seinen mechanischen Grenzwert hinaus geschwenkt werden.

E-flip (E-Flip) : Korrigiert die Kameraansicht automatisch, indem das Bild um 180° gedreht wird, wenn die Kamera über -90° hinaus geneigt wird.

Nadir-flip (Nadir-Flip) : Ermöglicht das Schwenken der Kamera um 180°, wenn die Neigung über -90° hinausgeht, und dann weiter nach oben.

Zoomgrenze: Wählen Sie einen Wert, um die maximale Zoomstufe der Kamera zu begrenzen. Es können optische oder digitale Werte (z. B. 480x D) ausgewählt werden. Bei Verwendung eines Joysticks können nur digitale Zoomstufen zur Einstellung der Zoomgrenze verwendet werden.

Nahbereichsfokuslimit: Wählen Sie einen Wert aus, um zu verhindern, dass die Kamera automatisch Objekte unmittelbar vor dem Objektiv fokussiert. Damit ignoriert die Kamera Objekte wie Oberleitungen, Straßenbeleuchtung oder andere Objekte in der Nähe. Um die Kamera auf ausgewählte Bereiche zu fokussieren, den Grenzwert für den Nahbereichsfokus auf einen Wert einstellen, der größer ist als der Abstand zu in der Regel bedeutungslosen Objekten.

Bewegung

Proportional speed (Proportionale Geschwindigkeit) : Schalten Sie diese Option aus, um die proportionale Höchstgeschwindigkeit einzustellen.

- **Max proportional speed (Proportionale Höchstgeschwindigkeit)** : Stellen Sie einen Wert zwischen 1 und 1.000 ein, um die Schwenk- und Neigegeschwindigkeit zu begrenzen. Die proportionale Höchstgeschwindigkeit ist als Prozentwert definiert, wobei 1.000 entspricht 1.000 % entspricht.
  Dies ist nützlich, wenn der Joystick ganz nach außen gedrückt ist. Ein Beispiel: Ein Bild hat eine vollständig herausgezoomt eine Breite von 44 Grad und die maximale proportionale Geschwindigkeit ist auf 100 (100 %) eingestellt. Die maximale Geschwindigkeit beträgt dann 44 Grad pro Sekunde. Wenn das Bild dann von 44 auf 10 Grad Breite vergrößert wird, erreicht die maximale Geschwindigkeit etwa 10 Grad pro Sekunde, was für eine einfache Betrachtung wahrscheinlich zu schnell ist. Um die Geschwindigkeit zu begrenzen, die maximale proportionale Geschwindigkeit auf 50 (50 %) setzen. Dadurch kann die maximale Geschwindigkeit nur 50 % des Maximums für die aktuell eingestellte Zoom-Stufe erreichen. Das heißt, dass bei einer Bildbreite von 44 Grad die mögliche Höchstgeschwindigkeit bei etwa 22 Grad pro Sekunde liegt und beim Einzoomen auf 10 Grad die Geschwindigkeit auf etwa 5 Grad pro Sekunde begrenzt wird.

Einstellbare Zoomgeschwindigkeit: Schalten Sie diese Option ein, um variable Geschwindigkeiten bei der Steuerung des Zooms mit einem Joystick oder einem Mausrad zu verwenden. Die Zoomgeschwindigkeit wird im VAPIX®-Application Programming Interface (API) automatisch mit dem Befehl `continuouszoommove` gesetzt. Deaktivieren Sie die Funktion, um mit der höchsten Zoomgeschwindigkeit, das heißt mit der Geschwindigkeit für das Wechseln zwischen voreingestellten Positionen, zu arbeiten.

Standbild bei PTZ

- **Aus**: Erzeugen Sie niemals ein Standbild.
- **All movements (Alle Bewegungen)**: Erzeugen Sie ein Standbild, während sich die Kamera bewegt. Sobald die Kamera ihren neue Position erreicht hat, wird die Ansicht aus dieser Position gezeigt.
- **Voreingestellte Positionen**: Erzeugen Sie nur ein Standbild, während sich die Kamera zwischen voreingestellten Positionen bewegt.

Geschwindigkeit für Schwenken/Neigen: Wählen Sie die Geschwindigkeit der Schwenk- und Neigebewegungen der Kamera aus.

Steuerungswarteschlange

Steuerungswarteschlange für Benutzer

- **PTZ control queue (PTZ-Steuerungswarteschlange)**: Schalten Sie diese Option ein, um PTZ-Steuerungsanfragen in eine Warteschlange zu stellen. Hier werden der Status und die Position des Benutzers in der Warteschlange angezeigt. Um die PTZ-Steuerung in AXIS Camera Station zu verwenden, deaktivieren Sie diese Einstellung.
  - **Enter queue (Warteschlange betreten)**: Klicken Sie hier, um Ihre Anfrage für die PTZ-Steuerung in die Warteschlange aufzunehmen.
  - **Release control (Steuerung freigeben)**: Klicken Sie hier, um die PTZ-Steuerung freizugeben.
- Die Benutzergruppen sind in einer Rangfolge aufgeführt, wobei die höchste Priorität an erster Stelle steht. Um die Priorität einer Benutzergruppe zu ändern, klicken Sie auf = und ziehen Sie die Benutzergruppe nach oben oder unten.
  Für jede Benutzergruppe:
  - **Timeout duration (Zeitüberschreitungsdauer)**: Legen Sie die Zeitspanne fest, die vor dem Timeout gewartet werden soll. Der Standardwert ist 1 Minute, die zulässigen Werte reichen von 1 Sekunde bis 60 Minuten.
  - **Zeitüberschreitungstyp**
    - **Timespan (Zeitspanne)**: Zeitüberschreitung nach Erreichen der eingestellten Dauer.
    - **Aktivität**: Zeitüberschreitung nach Erreichen der eingestellten Dauer seit der letzten Aktivität.
    - **Infinity (Unendlich)**: Niemals eine Zeitüberschreitung, bis ein Benutzer mit höherer Priorität die Kontrolle übernimmt.

Einstellungen

- **Limit number of users in queue (Anzahl der Benutzer in Warteschlange begrenzen)**: Legen Sie die maximale Anzahl der in einer Warteschlange zulässigen Benutzer fest. Der Standardzahl ist 20, die zulässigen Werte sind 1–100.
- **Control queue poll time (Abfragezeit Steuerungswarteschlange)**: Legen Sie fest, wie oft die Kamera abgefragt werden soll, um die Position der Benutzer oder Benutzergruppen in der Warteschlange zu aktualisieren. Der Standardwert ist 20 Sekunden, die zulässigen Werte reichen von 5 Sekunden bis 60 Minuten.

Einstellungen

Use PTZ (PTZ-Funktion verwenden): Aktivieren Sie diese Option, um die PTZ-Funktion in der ausgewählten Ansicht zu ermöglichen.

Leser

Verbindung

Externer Leser (Eingang)

Use external OSDP reader (Externen OSDP-Leser verwenden): Aktivieren Sie diese Einrichtung, um das Gerät mit einem externen Leser zu verwenden. Schließen Sie den Kartenleser an den Anschluss des Kartenlesers an (IO1, IO2, 12V und GND).

Status:

- **Connected (Verbunden)**: Das Gerät ist mit dem aktiven externen Leser verbunden.
- **Connecting (Verbinden)**: Das Gerät versucht, eine Verbindung mit dem externen Leser herzustellen.
- **Nicht verbunden**: OSDP ist ausgeschaltet.

Kartenleserprotokoll

Protokolltyp des Lesegeräts: Wählen Sie das Protokoll für die Leser-Funktionalität aus.

- **VAPIX-Leser**: Kann nur mit einer Axis Tür-Steuerung verwendet werden.
  - **Protocol (Protokoll)**: Wählen Sie **HTTPS** oder **HTTP** aus.
  - **Adresse der Türsteuerung**: Geben Sie die IP-Adresse für die Türsteuerung ein.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen der Tür-Steuerung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort der Tür-Steuerung ein.
  - **Connect (Verbinden)**: Klicken Sie, um eine Verbindung mit der Tür-Steuerung herzustellen.
  - **Leser auswählen**: Wählen Sie den Eingangsleser für die entsprechende Tür.
- **OSDP**:
  - **OSDP-Adresse**: Geben Sie die OSDP-Adresse des Kartenlesers ein. 0 ist der Standard und die häufigste Adresse für einzelne Kartenleser.
- **Wiegand** :
  - **Signaltongeber**: Anschalten, um den Tonsignaleingang zu aktivieren.
  - **Eingang für Summer**: Wählen Sie den für den Summer verwendeten E/A-Port aus.
  - **Eingang für die LED-Steuerung**: Wählen Sie aus, wie viele E/A-Ports für die Steuerung des LED-Feedbacks auf dem Gerät verwendet werden soll.
  - **Eingang für LED1/LED2**: Auswählen, welche E/A-Ports für den LED-Eingang verwendet werden sollen.
  - **Idle color (Farbe Leerbetrieb)**: Wenn zur Steuerung der LED kein I/O-Port verwendet wird, können Sie eine statische Farbe wählen, die auf dem Kartenleser-Markierungsstreifen angezeigt werden soll.
  - **Farbe für Zustand niedrig/hoch**: Wenn für die LED-Steuerung ein I/O-Port verwendet wird, wählen Sie die Farbe aus, die für den Status niedrig bzw. den Status hoch angezeigt werden soll.
  - **Farbe für Leerbetrieb/LED1-Farbe/LED2-Farbe/LED1 + LED2-Farbe**: Wenn für die LED-Steuerung zwei I/O-Ports verwendet werden, wählen Sie die Farben für Leerbetrieb, LED1, LED2 bzw. LED1 + LED2.
  - **Drucktastenformat**: Wählen Sie aus, wie die PIN formatiert wird, wenn sie an die Zugangskontrolleinheit gesendet wird.
    - **FourBit**: PIN `1234` wird kodiert und als 0x1 0x2 0x3 0x4 gesendet. Dies ist der Standard und das häufigste Verhalten.
    - **EightBitZeroPadded**: PIN `1234` wird codiert und als 0x01 0x02 0x03 0x04 gesendet.
    - **EightBitInvertPadded**: PIN `1234` wird codiert und als 0xE1 0xD2 0xC3 0xB4 gesendet.
    - **Wiegand26**: Die PIN ist im Wiegand26-Format mit einem 8-Bit-Gebäude-Zugangscode und einer 16-Bit-ID codiert.
    - **Wiegand34**: Die PIN ist im Wiegand34-Format mit einem 16-Bit-Gebäude-Zugangscode und einer 16-Bit-ID codiert.
    - **Wiegand37**: Die PIN ist im Wiegand37-Format (H10302) mit einer 35-Bit-ID codiert.
    - **Wiegand37FacilityCode**: Die PIN ist im Wiegand37-Format (H10304) mit einem 16-Bit-Gebäude-Zugangscode und einer 19-Bit-ID codiert.
  - **Facility code (Gebäude-Zugangscode)**: Geben Sie den Gebäude-Zugangscode ein, der gesendet werden soll. Diese Option ist nur für einige Tastendruckformate verfügbar.

Ausgabeformat

Datenformat auswählen: Wählen Sie aus, in welchem Format Kartendaten an die Zugangskontrolleinheit gesendet werden.

- **Raw**: Überträgt die Kartendaten so, wie sie sind.
- **Wiegand26**: Codiert die Kartendaten im Wiegand26-Format mit einem 8-Bit-Gebäude-Zugangscode und einer 16-Bit-ID.
- **Wiegand34**: Codiert die Kartendaten im Wiegand34-Format mit einem 16-Bit-Gebäude-Zugangscode und einer 16-Bit-ID.
- **Wiegand37**: Kodiert die Kartendaten im Wiegand37-Format (H10302) mit einer 35-Bit-ID.
- **Wiegand37FacilityCode**: Codiert die Kartendaten im Wiegand37-Format (H10304) mit einem 16-Bit-Gebäude-Zugangscode und einer 19-Bit-ID.
- **Benutzerdefiniert**: Legen Sie Ihre eigene Formatierung fest.

Überschreibungsmodus für Gebäude-Zugangscode: Wählen Sie eine Option aus, um den Gebäude-Zugangscode zu überschreiben.

- **Auto**: Überschreibt den Gebäude-Zugangscode nicht und erstellt aus der automatischen Erfassung von Eingangsdaten einen Gebäude-Zugangscode. Verwendet entweder den ursprünglichen Gebäude-Zugangscode der Karte oder fälscht ihn aus überschüssigen Bits einer Kartennummer.
- **Optional**: Verwendet den Gebäude-Zugangscode aus den Eingangsdaten oder überschreibt ihn mit einem konfigurierten optionalen Wert.
- **Überschreiben**: Überschreibt stets mit einem bestimmten Gebäude-Zugangscode.

Chiptypen

Chiptypen

Activate chip type (Chiptyp aktivieren): Wählen Sie einen Chiptyp aus der Liste aus, um diesen zu aktivieren.

Activate chip types (Chiptypen aktivieren) zeigt eine Liste aller aktiven Chiptypen an und gibt an, ob diese Standard- oder benutzerdefinierte Daten verwenden.

⋮ Das Kontextmenü enthält:

- **Deaktivieren**: Klicken Sie hier, um den Chiptyp aus der Liste aktiver Chiptypen zu entfernen.

Datensätze

Invert byte order for all chip types using the full card serial number (CSN) (Byte-Reihenfolge für alle Chiptypen unter Verwendung der vollständigen Kartenseriennummer (CSN) invertieren): Aktivieren Sie diese Option, um die Byte-Reihenfolge der Kartenseriennummer umzukehren. Die Seriennummer der Karte ist standardmäßig voreingestellt.

Invert byte order for all chip types using secure card data (Byte-Reihenfolge für alle Chiptypen anhand sicherer Kartendaten invertieren): Aktivieren Sie diese Option, um die Byte-Reihenfolge der sicheren Kartendaten für Chiptypen zu invertieren, die einen benutzerdefinierten Datensatz verwenden.

Add data set (Datensatz hinzufügen): Wählen Sie einen Chiptyp aus, und klicken Sie auf diese Option, um einen Datensatz hinzuzufügen. Für benutzerdefinierte Daten.

- **Name of data set (Datensatzname)**: Benennen Sie den Datensatz zur leichteren Datenzuordnung um. Der Name muss eindeutig sein. Er übernimmt die Funktion einer ID, z. B. in der API.
- **Aktiviert**: Deaktivieren Sie diese Option, um die Verwendung des Datensatzes zu beenden, ohne ihn zu löschen.
- **Required data (Erforderliche Daten)**: Bei Aktivierung dieser Einstellung sendet das Gerät keine Daten an die Türsteuerung, falls aus irgendeinem Grund nicht auf sichere Kartendaten zugegriffen werden kann. Deaktivieren Sie diese Option, um die Karten-Seriennummer (CSN) an die Türsteuerung zu senden, falls keine sicheren Kartendaten zur Verfügung stehen.
- **Use as authenticator (Als Authentifikator verwenden)**: Deaktivieren Sie diese Option, falls Sie keine sicheren Kartendaten für die Authentifizierung verwenden und diese nur als gültige Metadaten für das VAPIX-Protokoll übertragen möchten.
- **Offset (bits) (Offset (Bits))**: Geben Sie die Startposition der Daten ein. 0 bedeutet, dass die Startposition das erste Bit ist.
- **Length (bits) (Länge (Bits))**: Geben Sie die Länge der Daten ein. 0 bedeutet, dass eine beliebige Länge der Daten gelesen wird.
- **Use data on card (Daten auf Karte verwenden)**: Aktivieren Sie diese Option, um sichere Kartendaten zu verwenden. Deaktivieren Sie diese Option, um anstelle sicherer Kartendaten die Karten-Seriennummer (CSN) zu verwenden.

Die übrigen Einstellungen sind chiptyp-spezifisch und legen fest, wie die sicheren Kartendaten ausgelesen werden sollen.

PIN

Die PIN-Einstellungen müssen mit denen übereinstimmen, die in der Zugangskontrolleinheit konfiguriert wurden.

Länge (0–32): Geben Sie die Anzahl der Ziffern der PIN ein. Wenn Benutzer, Anwender nicht verpflichtet sind, bei der Benutzung des Kartenlesers eine PIN zu verwenden, setzen Sie die Länge auf 0.

Zeitüberschreitung (Sekunden, 3–50): Geben Sie die Anzahl der Sekunden ein, die vergehen müssen, bis das Gerät in den Stromsparmodus zurückkehrt, wenn keine PIN empfangen wird.

Zugangsberechtigungsliste

Mit der Zugangsberechtigungsliste können Sie das Gerät so einrichten, dass Eigentümer von Zugangsdaten ihre Karte, PIN oder QR Code® verwenden können, um verschiedene Aktionen wie etwa das Öffnen einer Tür durchzuführen. Die Zugangsdaten werden lokal im Gerät gespeichert. Diese Funktion kann auch mit einer externen Tür-Steuerung kombiniert werden.

QR Code ist eine eingetragene Marke von Denso Wave Incorporated in Japan und anderen Ländern.

Eigentümer der Anmeldedaten

Use Entry list (Zugangsberechtigungsliste verwenden): Aktivieren Sie die Funktion, um die Zugangsberechtigungsliste zu verwenden.

Use connected door controller (Verbundene Tür-Steuerung verwenden): Aktivieren Sie diese Funktion, wenn das Gerät bereits mit einer Tür-Steuerung verbunden ist. Wenn eine Person Zugangsdaten angibt, die nicht in der Zugangsberechtigungsliste aufgeführt sind, senden wir die Anfrage an die verbundene Tür-Steuerung. Wir senden keine Zugangsdaten, die in der Zugangsberechtigungsliste verfügbar sind.

Add credential holder (Eigentümer von Zugangsdaten hinzufügen): Klicken Sie hier, um einen neuen Eigentümer von Zugangsdaten hinzuzufügen.

First name (Vorname): Geben Sie einen Vornamen ein.

Last name (Nachname): Geben Sie einen Nachnamen ein.

Credential type (Art der Zugangsdaten):

- **PIN**:
  - **PIN**: Geben Sie eine eindeutige PIN ein, oder klicken Sie auf **Generate (Generieren)**, um automatisch eine erstellen zu lassen.
- **Card (Karte)**:
  - **UID**: Geben Sie die UID und die Bitlänge der Karte ein, oder klicken Sie auf **Get latest (Neueste abrufen)**, um die Daten des letzten Durchziehens einer Karte abzurufen.
- **QR Code®**

Event condition (Ereignisbedingung): Wählen Sie eine oder mehrere Bedingungen aus, die ausgelöst werden, wenn der Eigentümer der Zugangsdaten seine Zugangsdaten verwendet. Um die daraus resultierende Aktion einzurichten, gehen Sie zu **System > Events (System > Ereignisse)**, und erstellen Sie eine Regel mit der Bedingung, die Sie hier ausgewählt haben.

Valid from (Gültig ab): Wählen Sie **Current device time (Aktuelle Gerätezeit)** aus, um die Zugangsdaten sofort zu aktivieren. Hier können Sie angeben, wann die Zugangsdaten aktiviert werden sollen.

Valid to (Gültig bis):

- **No end date (Kein Enddatum)**: Die Zugangsdaten sind unbegrenzt gültig.
- **End date (Enddatum)**: Geben Sie das Datum und die Uhrzeit des Zeitpunkts an, zu dem die Zugangsdaten ungültig werden.
- **Number of times (Anzahl)**: Geben Sie an, wie oft der Eigentümer der Zugangsdaten die Zugangsdaten verwenden kann. Der Wert im Feld verringert sich, wenn die Zugangsdaten verwendet werden, und zeigt die verbleibende Anzahl von Verwendungen an.

Hinweise: Geben Sie optionale Informationen ein.

Suspend (Aussetzen): Wählen Sie diese Option aus, um die Zugangsdaten vorübergehend ungültig zu machen.

Download QR Code when saving (QR-Code beim Speichern herunterladen): Wenn Sie QR-Code als Berechtigungstyp ausgewählt haben, aktivieren Sie dieses Kontrollkästchen, um den QR-Code herunterzuladen, wenn Sie auf **Save (Speichern)** klicken.

Ereignisprotokoll

Das Ereignisprotokoll zeigt eine Liste der Ereignisse in der Eintragsliste. Die maximale Größe der Protokolldatei beträgt 2 MB, was etwa 6000 Ereignissen entspricht.

Export all (Alle exportieren): Klicken Sie hier, um alle Ereignisse in der Liste zu exportieren. Um nur eine Teilmenge zu exportieren, wählen Sie die Ereignisse aus, an denen Sie interessiert sind. Die Ereignisse werden in eine CSV-Datei exportiert.

Filter: Klicken Sie hier, um Ereignisse anzuzeigen, die in einem bestimmten Zeitraum aufgetreten sind.

: Tippen Sie hier, um nach allen übereinstimmenden Inhalten in der Liste zu suchen.

Audio

Geräteinstellungen

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

Eingangstyp : Wählen Sie die Art des Eingangs aus, z. B. interner Mikrofon- oder Line-Eingang.

Spannung : Wählen Sie die Art der Stromversorgung für den Eingang aus.

Änderungen übernehmen : Wenden Sie Ihre Auswahl an.

Noise cancellation (Geräuschreduktion): Aktivieren Sie dies, um die Audioqualität durch Entfernen von Hintergrundgeräuschen zu verbessern.

Echounterdrückung : Aktivieren Sie diese Option, um Echos während der Zwei-Wege-Kommunikation zu entfernen.

Separate Verstärkungsregler : Aktivieren Sie diese Option, um die Verstärkung für die verschiedenen Eingangsarten separat einzustellen.

Automatische Verstärkungsregelung : Aktivieren Sie dieses Option, damit die Verstärkung dynamisch an Klangänderungen angepasst wird.

Verstärkung: Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Mikrofonsymbol.

Ausgang: Zeigt die Ausgangsart an.

Verstärkung: Ändern Sie mithilfe des Schiebereglers die Verstärkung. Klicken Sie zum Stummschalten oder Aufheben der Stummschaltung auf das Lautsprechersymbol.

Automatische Lautstärkeregelung : Aktivieren Sie diese Option, damit das Gerät die Verstärkung automatisch und dynamisch an den Umgebungsgeräuschpegel anpasst. Die automatische Lautstärkeregelung betrifft alle Audio-Ausgänge, einschließlich Line und Telefonspule.

Videostream

Codierung: Wählen Sie die Codierung für das Streaming der Eingangsquelle aus. Sie können die Codierung nur wählen, wenn der Audioeingang aktiviert ist. Klicken Sie auf **Enable audio input (Audioeingang aktivieren)**, falls der Audioeingang deaktiviert ist.

Audio-Clips

Clip hinzufügen: Fügen Sie einen neuen Audioclip hinzu. Sie können Dateien wie .au, .mp3, .opus, .vorbis, .wav verwenden.

Audio-Clip abspielen.

Audio-Clip anhalten.

Das Kontextmenü enthält:

- **Umbenennen**: Den Namen des Audio-Clip ändern.
- **Link erstellen**: Erstellen Sie eine URL, über die der Audioclip auf dem Gerät abgespielt wird. Legen Sie für den Clip die Lautstärke und die Anzahl der Wiederholungen fest.
- **Herunterladen**: Laden Sie den Audioclip auf Ihren Computer herunter.
- **Löschen**: Entfernen Sie den Audioclip vom Gerät.

Aufzeichnungen

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

Starten einer Aufzeichnung des Geräts.

Wählen Sie das Speichermedium, auf dem die Aufzeichnung gespeichert werden soll.

Beenden einer Aufzeichnung des Geräts.

Ausgelöste Aufzeichnungen können entweder manuell gestoppt oder durch Ausschalten des Geräts beendet werden.

Fortlaufende Aufzeichnungen laufen so lange weiter, bis sie manuell gestoppt werden. Bei Ausschalten des Geräts wird die Aufzeichnung nach dem Wiedereinschalten fortgesetzt.

Die Aufzeichnung wiedergeben.

Abspielen der Aufzeichnung anhalten.

Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

Exportbereich festlegen: Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten. Beachten Sie, dass die Zeitspanne auf der Zeitzone des Geräts basiert, wenn Sie in einer anderen Zeitzone als der am Standort des Geräts arbeiten.

Encrypt (Verschlüsseln): Legen Sie mit dieser Option ein Kennwort für exportierte Aufzeichnungen fest. Die exportierte Datei kann ohne das Kennwort nicht geöffnet werden.

Klicken Sie auf , um eine Aufzeichnung zu löschen.

Exportieren: Exportieren der ganzen Aufzeichnung oder eines Teils davon.

Klicken Sie darauf, um die Aufzeichnungen zu filtern.

Von: Zeigt Aufzeichnungen, die nach einem bestimmten Zeitpunkt gemacht wurden.

Bis: Zeigt Aufzeichnungen, die bis zu einem bestimmten Zeitpunkt gemacht wurden.

Source (Quelle): Zeigt Aufzeichnungen auf Grundlage der Quelle. Die Quelle bezieht sich auf den Sensor.

Ereignis: Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Speicher: Zeigt Aufzeichnungen nach Speichertyp.

Medien

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

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

Das Kontextmenü enthält:

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

Apps

App hinzufügen: Installieren einer neuen App.

Weitere Apps finden: Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet.

Nicht signierte Apps zulassen : Aktivieren Sie diese Option, um die Installation unsignierter Apps zu ermöglichen.

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

Hinweis

Die Leistung des Geräts kann beeinträchtigt werden, wenn mehrere Apps gleichzeitig ausgeführt werden.

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

Offen: Auf die Anwendungseinstellungen zugreifen. Die zur Verfügung stehenden Einstellungen hängen von der Anwendung ab. Für einige Anwendungen gibt es keine Einstellungen.

Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

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

System

Uhrzeit und Ort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server))**: Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
  - **Trusted NTS KE CA certificates (Vertrauenswürdige NTS KE CA-Zertifikate)**: Wählen Sie die vertrauenswürdigen CA-Zertifikate aus, die für die sichere NTS KE-Zeitsynchronisierung verwendet werden sollen, oder wählen Sie keines aus.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (NTP servers using DHCP) (Datum und Uhrzeit automatisch (NTP-Server mit DHCP))**: Synchronisieren Sie das Gerät mit den NTP-Servern, die mit dem DHCP-Server verbunden sind.
  - **Fallback NTP servers (NTP-Reserve-Server)**: Geben Sie die IP-Adresse eines oder zweier Reserve-Server ein.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Automatic date and time (manual NTP servers) (Datum und Uhrzeit automatisch (manuelle NTP-Server))**: Führen Sie eine Synchronisierung mit NTP-Servern Ihrer Wahl durch.
  - **Manual NTP servers (Manuelle NTP-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
  - **Max NTP poll time (Max. NTP-Abfragezeit)**: Wählen Sie die maximale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
  - **Min NTP poll time (Min. NTP-Abfragezeit)**: Wählen Sie die minimale Zeitspanne aus, die das Gerät warten soll, bis es den NTP-Server abfragt, um eine aktualisierte Zeit zu erhalten.
- **Custom date and time (Datum und Uhrzeit benutzerdefiniert)**: Manuelles Einstellen von Datum und Uhrzeit. Klicken Sie auf **Vom System abrufen**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

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

- **DHCP**: Übernimmt die Zeitzone des DHCP-Servers. Bevor Sie diese Option auswählen können, muss das Gerät mit einem DHCP-Server verbunden werden.
- **Manual (Manuell)**: Wählen Sie in der Drop-Down-Liste eine Zeitzone aus.

Hinweis

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

Gerätestandort

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

- **Breite**: Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Länge**: Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Ausrichtung**: Die Kompassrichtung des Geräts eingeben. Der Wert 0 steht für: genau nach Norden.
- **Bezeichnung**: Eine aussagekräftige Bezeichnung für Ihr Gerät eingeben.
- **Speichern**: Klicken Sie hier, um den Gerätestandort zu speichern.

Konfigurationsprüfung

Interactive device image (Interaktives Gerätebild): Klicken Sie auf die Schaltflächen im Bild, um die Tastenbedienung zu simulieren. Auf diese Weise können Sie Konfigurationen ausprobieren oder eine Fehlerbehebung für die Hardware durchführen, ohne physischen Zugriff auf das Gerät zu haben.

Letzte Zugangsdaten : Zeigt Informationen zu den zuletzt registrierten Zugangsdaten an.

Die aktuellen Zugangsdaten anzeigen.

Das Kontextmenü enthält:

- **UID umdrehen**: Die Byte-Reihenfolge der UID umdrehen.
- **UID wiederherstellen**: Die Byte-Reihenfolge der UID zurück in die ursprüngliche Reihenfolge bringen.
- **Copy to clipboard (In die Zwischenablage kopieren)**: Kopieren Sie die UID.

Zugangsdaten überprüfen : Geben Sie eine UID oder eine PIN ein und senden Sie, um die Zugangsdaten zu überprüfen. Das System antwortet auf die gleiche Weise, als hätten Sie Zugangsdaten für das Gerät verwendet. Wenn sowohl UID als auch PIN erforderlich sind, geben Sie zunächst die UID ein.

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

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

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

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

Hinweis

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

IPv6

Assign IPv6 automatically (IPv6 automatisch zuweisen): Wählen Sie diese Option aus, um IPv6 einzuschalten und damit der Netzwerkrouter dem Gerät automatisch eine IP-Adresse zuweisen kann.

Hostname

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

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

Dynamische DNS-Aktualisierung aktivieren: Erlauben Sie Ihrem Gerät, seine Domainnamen-Server-Einträge automatisch zu aktualisieren, wenn sich seine IP-Adresse ändert.

DNS-Namen registrieren: Geben Sie einen eindeutigen Domainnamen ein, der auf die IP-Adresse Ihres Geräts verweist. Zugelassene Zeichen sind A–Z, a–z, 0–9 und -).

TTL: Time to Live (TTL) legt fest, wie lange ein DNS-Eintrag gültig bleibt, bevor er aktualisiert werden muss.

DNS-Server

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

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

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

HTTP und HTTPS

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

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Um Zertifikate zu erstellen und zu installieren, **System > Security (System > Sicherheit)** aufrufen.

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

Hinweis

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

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

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

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

Netzwerk-Erkennungsprotokolle

Bonjour®: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

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

UPnP®: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

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

WS-Erkennung: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung.

LLDP und CDP: Ermöglicht das automatische Erkennen im Netzwerk bei Aktivierung. Das Deaktivieren von LLDP und CDP kann sich auf das PoE-Leistungsmanagement auswirken. Konfigurieren Sie den PoE-Switch nur für das Hardware-PoE-Leistungsmanagement, um Probleme mit dem PoE-Leistungsmanagement zu beheben.

Globale Proxys

HTTP proxy (HTTP-Proxy): Geben Sie einen globalen Proxy-Host oder eine IP-Adresse in einem unterstützten Format an.

HTTPS proxy (HTTPS-Proxy): Geben Sie einen globalen Proxy-Host oder eine IP-Adresse in einem unterstützten Format an.

Unterstützte HTTP- und HTTPS-Proxy-Formate:

- http(s)://host:port
- http(s)://user@host:port
- http(s)://user:pass@host:port

Hinweis

Starten Sie das Gerät neu, um die Einstellungen für den globalen Proxy anzuwenden.

No proxy (Kein Proxy): Verwenden Sie die Option **No proxy (Kein Proxy)**, um globale Proxys zu umgehen. Geben Sie eine Option oder mehrere durch Kommas getrennte Optionen aus der Liste ein:

- Leer lassen
- IP-Adresse angeben
- IP-Adresse im CIDR-Format angeben
- Geben Sie einen Domainnamen an, zum Beispiel: www.<Domainname>.com
- Geben Sie alle Subdomains einer bestimmten Domain an, z. B. .<Domainname>.com

One-Click Cloud Connect

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

O3C zulassen:

- **One-click**: Dies ist die Standardoption. Um eine Verbindung zum O3C herzustellen, drücken Sie die Steuertaste am Gerät. Je nach Gerätetyp entweder drücken und loslassen oder drücken und halten, bis die Status-LED blinkt. Registrieren Sie das Gerät innerhalb von 24 Stunden beim O3C-Service, um **Always (Immer)** zu aktivieren, und bleiben Sie verbunden. Wenn Sie sich nicht registrieren, wird die Verbindung zwischen dem Gerät und O3C unterbrochen.
- **Immer**: Das Gerät versucht ständig, über das Internet eine Verbindung mit einem O3C-Dienst herzustellen. Sobald Sie das Gerät registriert haben, bleibt es verbunden. Verwenden Sie diese Option, wenn die Steuertaste außer Reichweite ist.
- **No (Nein)**: Trennt den O3C-Dienst.

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

Host: Geben Sie die Adresse des SIP-Proxyservers ein.

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

Anmeldung und **Kennwort**: Bei Bedarf einen Benutzernamen und ein Kennwort für den Proxyserver eingeben.

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

- **v3**: SNMP v3 ist eine Version mit höherer Sicherheit, die Verschlüsselung und sichere Kennwörter bereitstellt. Beim Verwenden von SNMP v3 empfehlen wir Ihnen, HTTPS zu aktivieren, da Kennwörter dann über HTTPS gesendet werden. Dadurch wird auch verhindert, dass Unbefugte auf unverschlüsselte Traps des Typs SNMP v1 und v2c zugreifen können. Wenn Sie SNMP v3 verwenden, können Sie Traps über die Verwaltungsanwendung für SNMP v3 einrichten.
  - **Kennwort für das Konto "initial"**: Geben Sie das SNMP-Kennwort für das Konto mit dem Namen "initial" ein. Obwohl das Kennwort ohne Aktivierung von HTTPS gesendet werden kann, empfehlen wir es nicht. Das Kennwort für SNMP v3 kann nur einmal und vorzugsweise dann bei aktiviertem HTTPS festgelegt werden. Nach dem Einrichten des Kennworts wird das Kennwortfeld nicht mehr angezeigt. Wenn ein neues Kennwort eingerichtet werden soll, muss das Gerät auf die Werkseinstellungen zurückgesetzt werden.

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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

Zertifikat hinzufügen: Klicken, um ein Zertifikat hinzuzufügen. Es wird eine Schritt-für-Schritt-Anleitung geöffnet.

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

Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) :

- **Trusted Execution Environment (SoC TEE)**: Auswählen, um SoC TEE für einen sicheren Schlüsselspeicher zu verwenden.
- **Secure element (CC EAL6+)**: 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.

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec ist ein IEEE-Standard für MAC-Sicherheit (Media Access Control), der die Vertraulichkeit und Integrität verbindungsloser Daten für medienzugriffsunabhängige Protokolle definiert.

Zertifikate

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

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

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

Authentication method (Authentifizierungsmethode): Wählen Sie einen EAP-Typ aus, der für die Authentifizierung verwendet wird.

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

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

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

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

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

Diese Einstellungen stehen nur zur Verfügung, wenn Sie **IEEE 802.1x PEAP-MSCHAPv2** als Authentifizierungsmethode verwenden:

- **Password (Kennwort)**: Geben Sie das Password (Kennwort) für die Benutzeridentität ein.
- **Peap version (Peap-Version)**: Wählen Sie die in dem Netzwerk-Switch verwendete Peap-Version aus.
- **Bezeichnung**: Wählen Sie 1 aus, um die EAP-Verschlüsselung des Client zu verwenden. Wählen Sie 2 aus, um die PEAP-Verschlüsselung des Client zu verwenden. Wählen Sie die Bezeichnung aus, das der Netzwerk-Switch bei Verwendung von Peap-Version 1 verwendet.

Diese Einstellungen stehen nur zur Verfügung, wenn Sie **IEEE 802.1ae MAGCsec (Static CAK/Pre-Shared Key)** als Authentifizierungsmethode verwenden:

- **Key agreement connectivity association key name (Schlüsselname der Key Agreement Connectivity Association)**: Geben Sie den Namen der Connectivity Association (CKN) ein. Der Name muss aus 2 bis 64 (durch 2 teilbare) Hexadezimalzeichen bestehen. Der CKN muss manuell in der Connectivity Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.
- **Key agreement connectivity association key (Schlüssel der Key Agreement Connectivity Association)**: Geben Sie den Schlüssel der Connectivity Association (CAK) ein. Der Schlüssellänge sollte entweder 32 oder 64 Hexadezimalzeichen betragen. Der CAK muss manuell in der Connectivity

Association konfiguriert werden und auf beiden Seiten der Verbindung gleich sein, um MACsec zu initialisieren.

Brute-Force-Angriffe verhindern

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

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

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

Firewall

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

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

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

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

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

Rule type (Regeltyp):

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

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

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

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

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

Zum Installieren von Testsoftware oder anderer benutzerdefinierter Software von Axis auf dem Gerät benötigen Sie ein benutzerdefiniertes signiertes AXIS OS-Zertifikat. Das Zertifikat prüft, ob die Software sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Software kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Spezifisch signierte AXIS OS-Zertifikate können nur von Axis erstellt werden, da Axis den Schlüssel zum Signieren besitzt.

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

Das Kontextmenü enthält:

- **Delete certificate (Zertifikat löschen)**: Löschen Sie das Zertifikat.

Konten

Konten

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Bediener**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**-Einstellungen
- **Betrachter**: Hat Zugriff auf:
  - Einen Videostream ansehen und Schnappschüsse machen.
  - Aufzeichnungen ansehen und exportieren.
  - Schwenken, Neigen und Zoomen; Zugang über **PTZ-Konto**.

Das Kontextmenü enthält:

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

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

Anonymer Zugriff

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

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

SSH-Konten

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

- **Enable SSH (SSH aktivieren)**: Den SSH-Dienst aktivieren.

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Anmerkung: Geben Sie eine Anmerkung ein (optional).

Das Kontextmenü enthält:

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

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

Virtual host (Virtueller Host)

Add virtual host (Virtuellen Host hinzufügen): Klicken Sie hier, um einen neuen virtuellen Host hinzuzufügen.

Aktiviert: Wählen Sie diese Option aus, um diesen virtuellen Host zu verwenden.

Server name (Servername): Geben Sie den Namen des Servers ein. Verwenden Sie nur die Zahlen 0 bis 9, die Buchstaben A bis Z und den Bindestrich (-).

Port: Geben Sie den Port ein, mit dem der Server verbunden ist.

Typ: Wählen Sie den Typ der Authentifizierung aus. Sie haben die Wahl zwischen **Basic**, **Digest** und **Open ID**.

Das Kontextmenü enthält:

- **Update (Aktualisieren)**: Aktualisieren Sie den virtuellen Host.
- **Löschen**: Löschen Sie den virtuellen Host.

Disabled (Deaktiviert): Der Server ist deaktiviert.

Konfiguration der Client-Zugangsdaten-Genehmigung

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

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

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

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

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

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

OpenID-Konfiguration

Wichtig

Wenn Sie sich nicht mit OpenID anmelden können, verwenden Sie die Digest- oder Basic-Anmeldeinformationen, die Sie bei der Konfiguration von OpenID für die Anmeldung verwendet haben.

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

Condition (Bedingung): Wählen Sie eine Bedingung aus der Liste aus. Eine Bedingung muss erfüllt sein, damit das Gerät eine Aktion ausführen kann. Wenn mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein. Informationen zu bestimmten Bedingungen finden Sie 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.

Hinweis

Wenn Ihr Gerät für die Verwendung von FTP oder SFTP eingerichtet ist, dürfen Sie die eindeutige Sequenznummer, die den Dateinamen hinzugefügt wird, nicht ändern oder entfernen. Anderenfalls kann nur ein Bild pro Ereignis gesendet werden.

Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis

Sie können bis zu 20 Empfänger erstellen.

Empfänger hinzufügen: Klicken Sie darauf, um einen Empfänger hinzuzufügen.

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

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

- **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
- **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
- **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.

- SFTP
  - **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Servers ein. Stellen Sie bei der Eingabe eines Host-Namen sicher, dass unter **System > Network > IPv4 und IPv6** ein DNS-Server angegeben ist.
  - **Port**: Die vom SFTP-Server verwendete Portnummer eingeben. Die Standardeinstellung lautet 22.
  - **Ordner**: Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten. Wenn dieses Verzeichnis noch nicht auf dem SFTP-Server eingerichtet ist, erhalten Sie beim Hochladen eine Fehlermeldung.
  - **Username (Benutzername)**: Geben Sie den Benutzernamen für die Anmeldung ein.
  - **Password (Kennwort)**: Geben Sie das Kennwort für die Anmeldung ein.
  - **Öffentlicher SSH-Host-Schlüsseltyp (MD5)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine hexadezimale Zeichenfolge mit 32 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Öffentlicher SSH-Host-Schlüsseltyp (SHA256)**: Geben Sie der Fingerabdruck des öffentlichen Schlüssels des Zielrechners (eine Base64-kodierte Zeichenfolge mit 43 Stellen) ein. Der SFTP-Client unterstützt SFTP-Server, die SSH-2 mit RSA-, DSA-, ECDSA- und ED25519-Schlüsseltypen verwenden. RSA ist die bevorzugte Methode während der Aushandlung, gefolgt von ECDSA, ED25519 und DSA. Stellen Sie sicher, dass Sie den richtigen MD5-Hostschlüssel eingeben, der von Ihrem SFTP-Server verwendet wird. Das Axis Gerät unterstützt zwar sowohl MD5- als auch SHA-256-Hash-Schlüssel, wir empfehlen jedoch die Verwendung von SHA-256, da es sicherer ist als MD5. Weitere Informationen zur Konfiguration eines SFTP-Servers mit einem Axis Gerät finden Sie im *AXIS OS-Portal*.
  - **Temporären Dateinamen verwenden**: Wählen Sie diese Option zum Hochladen von Dateien mit temporären, automatisch generierten Dateinamen. Die Dateien werden nach abgeschlossenem Hochladen in die gewünschten Namen umbenannt. Wenn das Hochladen abgebrochen oder unterbrochen wird, werden keine beschädigten Dateien eingestellt. Jedoch werden möglicherweise die temporären Dateien eingestellt. So wissen Sie, dass alle Dateien mit dem gewünschten Namen in Ordnung sind.

- SIP oder VMS :
  SIP: Wählen Sie diese Option, um einen SIP-Anruf zu starten.
  VMS: Wählen Sie diese Option, um einen VMS-Anruf zu starten.
  - **Vom SIP-Konto**: Wählen Sie aus der Liste.
  - **An SIP-Adresse**: Geben Sie die SIP-Adresse ein.
  - **Test**: Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.
- E-Mail
  - **E-Mail senden an**: Geben Sie die E-Mail-Adresse ein, an die E-Mails gesendet werden sollen. Trennen Sie mehrere Adressen jeweils mit einem Komma.
  - **E-Mail senden von**: Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.

- **Username (Benutzername)**: Geben Sie den Benutzernamen für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **Password (Kennwort)**: Geben Sie das Kennwort für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **E-Mail-Server (SMTP)**: Geben Sie den Namen des SMTP-Servers ein. Zum Beispiel smtp.gmail.com, smtp.mail.yahoo.com.
- **Port**: Die Portnummer des SMTP-Servers eingeben. Zulässig sind Werte zwischen 0 und 65535. Die Nummer des Standardports ist 587.
- **Verschlüsselung**: Um die Verschlüsselung zu verwenden, wählen Sie SSL bzw. TLS.
- **Validate server certificate (Server-Zertifikate validieren)**: Wenn Sie eine Verschlüsselung verwenden, wählen Sie diese Option zur Überprüfung der Identität des Geräts. Das Zertifikat kann ein eigensigniertes oder ein von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestelltes Zertifikat sein.
- **POP-Authentifizierung**: Schalten Sie diese Option ein, um den Namen des POP-Servers einzugeben, z.B. pop.gmail.com.

Hinweis

Die Sicherheitsfilter einiger E-Mail-Anbieter verhindern das Empfangen oder Anzeigen vieler Anlagen, das Empfangen geplanter E-Mails usw. Prüfen Sie die Sicherheitsrichtlinien des E-Mail-Anbieters, damit Ihr E-Mail-Konto nicht gesperrt wird oder die erwarteten E-Mails nicht verloren gehen.

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

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

⋮ Das Kontextmenü enthält:

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

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

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

Zeitschemata

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

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

Manuelle Auslöser

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

MQTT

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

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

Mehr lesen zu MQTT in der *AXIS OS Knowledge base*.

ALPN

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

MQTT-Client

Connect (Verbinden): Aktivieren oder deaktivieren Sie den MQTT-Client.

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

Broker

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

Protocol (Protokoll): Wählen Sie das zu verwendende Protokoll aus.

Port: Geben Sie die Portnummer ein.

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

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

Username (Benutzername): Den Benutzernamen eingeben, den der Client für den Zugriff auf den Server verwenden soll.

Password (Kennwort): Ein Kennwort für den Benutzernamen eingeben.

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

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

HTTP proxy (HTTP-Proxy): eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTP-Proxy verwenden möchten.

HTTPS proxy (HTTPS-Proxy): eine URL mit einer maximalen Länge von 255 Byte. Sie können das Feld leer lassen, wenn Sie keinen HTTPS-Proxy verwenden möchten.

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

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

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

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

Nachricht zum Verbindungsaufbau

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

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

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

Topic (Thema): Geben Sie das Thema für die Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

Nachricht zum letzten Willen und Testament

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

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

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

Topic (Thema): Geben Sie das Thema für die Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

MQTT-Warteschlange

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

Include 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.

Add condition (Bedingung hinzufügen): Klicken Sie darauf, um eine Bedingung hinzuzufügen.

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

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

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

MQTT-Abonnements

Add subscription (Abonnement hinzufügen): Klicken Sie darauf, um ein neues MQTT-Abonnement hinzuzufügen.

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

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

Abonnementart:

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

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

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.

Speicherung

Netzwerk-Speicher

Ignorieren: Schalten Sie diese Option ein, um den Netzwerk-Speicher zu ignorieren.

Netzwerk-Speicher hinzufügen: Klicken Sie auf diese Option zum Hinzufügen einer Netzwerk-Freigabe, auf der Sie Aufzeichnungen speichern können.

- **Adresse**: Geben Sie die IP-Adresse des Host-Servers, in der Regel ein NAS (Network Attached Storage), ein. Wir empfehlen Ihnen, den Host für eine statische IP-Adresse zu konfigurieren (nicht DHCP, da sich eine dynamische IP-Adresse ändern kann) oder DNS zu verwenden. Namen des Typs Windows SMB/CIFS werden nicht unterstützt.
- **Netzwerk-Freigabe**: Den Namen des freigegebenen Speicherorts auf dem Host-Server eingeben. Mehrere Axis Geräte können dieselbe Netzwerk-Freigabe verwenden, da jedes Gerät einen eigenen Ordner erhält.
- **Benutzer**: Wenn der Server eine Anmeldung erfordert, geben Sie den Benutzernamen ein. Zur Anmeldung an einem bestimmten Domainserver geben Sie `DOMAIN\username` ein.
- **Password (Kennwort)**: Wenn der Server eine Anmeldung erfordert, geben Sie das Kennwort ein.
- **SMB-Version**: Wählen Sie die SMB-Speicherprotokollversion für die Verbindung mit dem NAS. Wenn Sie **Auto** wählen, versucht das Gerät, eine der sicheren Versionen SMB zu installieren: 3.02, 3.0 oder 2.1. Wählen Sie 1.0 oder 2.0 zur Herstellung einer Verbindung zu älteren NAS, die höhere Versionen nicht unterstützen. Weitere Informationen zur SMB-Unterstützung in Axis Geräten finden Sie *hier*.
- **Add share without testing (Freigabe ohne Test hinzufügen)**: Wählen Sie diese Option, um die Netzwerk-Freigabe hinzuzufügen, auch wenn während des Verbindungstests ein Fehler erkannt wurde. Bei dem Fehler kann es beispielsweise sein, dass Sie kein Kennwort eingegeben haben, obwohl für den Server ein Kennwort erforderlich ist.

Netzwerk-Speicher entfernen: Klicken Sie hier, um die Verbindung zur Netzwerk-Freigabe zu trennen, zu lösen oder zu entfernen. Dadurch werden alle Einstellungen für die Netzwerk-Freigabe entfernt.

Unbind (Lösen): Klicken Sie hier, um die Netzwerk-Freigabe zu lösen und zu trennen.
Bind (Zuweisen): Klicken Sie hier, um die Netzwerk-Freigabe zuzuweisen und zu verbinden.

Unmount (Trennen): Klicken Sie hier, um die Netzwerk-Freigabe zu trennen.
Mount (Einbinden): Klicken Sie hier, um die Netzwerk-Freigabe einzubinden.

Write protect (gegen Überschreiben schützen): Aktivieren Sie diese Option, damit nicht mehr auf die Netzwerk-Freigabe geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte Netzwerk-Freigabe kann nicht formatiert werden.

Aufbewahrungszeit: Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Datenmenge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn der Netzwerk-Speicher voll ist, werden alte Aufzeichnungen gelöscht, bevor der ausgewählte Zeitraum verstrichen ist.

Werkzeuge

- **Verbindung testen**: Prüfen Sie die Verbindung zur Netzwerk-Freigabe.
- **Formatieren**: Formatieren Sie die Netzwerk-Freigabe, wenn zum Beispiel schnell alle Daten gelöscht werden müssen. CIFS ist die verfügbare Dateisystemoption.

Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Onboard-Speicher

Wichtig

Gefahr von Datenverlust und beschädigten Aufzeichnungen. Die SD-Karte darf nicht entfernt werden, während das Gerät in Betrieb ist. Trennen Sie die SD-Karte, bevor Sie sie entfernen.

Unmount (Trennen): Klicken Sie hier, um die SD-Karte sicher zu entfernen.

Write protect (gegen Überschreiben schützen): Aktivieren, damit nicht mehr auf die SD-Karte geschrieben werden kann und bestehende Aufzeichnungen nicht entfernt werden können. Eine schreibgeschützte SD-Karte kann nicht formatiert werden.

Automatisch formatieren: Aktivieren Sie diese Option, um eine neu eingesetzte SD-Karte automatisch zu formatieren. Sie wird als Dateisystem ext4 formatiert.

Ignorieren: Aktivieren Sie diese Option, um die Speicherung der Aufzeichnungen auf der SD-Karte zu beenden. Wenn Sie die SD-Karte ignorieren, erkennt das Gerät nicht mehr, dass die Karte vorhanden ist. Diese Einstellung steht nur Administratoren zur Verfügung.

Aufbewahrungszeit: Wählen Sie, wie lange die Aufzeichnungen gespeichert werden, um die Menge alter Aufzeichnungen zu begrenzen oder die Bestimmungen zur Datenspeicherung einzuhalten. Wenn die SD-Speicherkarte voll ist, werden alte Aufzeichnungen vor Ablauf der Aufbewahrungsfrist gelöscht.

Werkzeuge

- **Check (Überprüfen)**: Die SD-Speicherkarte auf Fehler überprüfen.
- **Repair (Reparieren)**: Fehler im Dateisystem beheben.
- **Formatieren**: Die SD-Speicherkarte formatieren, um das Dateisystem zu ändern und alle Daten zu löschen. Sie können die SD-Speicherkarte nur mit dem Dateisystem ext4 formatieren. Sie benötigen einen externen ext4-Treiber oder eine Anwendung, um unter Windows® auf das Dateisystem zuzugreifen.
- **Encrypt (Verschlüsseln)**: Verwenden Sie dieses Tool, um die SD-Karte zu formatieren und die Verschlüsselung zu aktivieren. Alle auf der SD-Karte gespeicherten Daten werden gelöscht. Alle neuen Daten, die Sie auf der SD-Speicherkarte speichern, werden verschlüsselt.
- **Entschlüsseln**: Verwenden Sie dieses Tool, um die SD-Karte ohne Verschlüsselung zu formatieren. Alle auf der SD-Karte gespeicherten Daten werden gelöscht. Alle neuen Daten, die Sie auf der SD-Speicherkarte speichern, werden nicht verschlüsselt.
- **Change password (Kennwort ändern)**: Andern Sie das zum Verschlüsseln der SD-Karte erforderliche Kennwort.

Use tool (Werkzeug verwenden): Klicken Sie hier, um das ausgewählte Werkzeug zu aktivieren.

Auslöser für Abnutzung: Legen Sie einen Wert für die Abnutzung der SD-Speicherkarte fest, bei dem eine Aktion ausgelöst werden soll. Der Abnutzungsgrad reicht von 0 bis 200 %. Eine neue SD-Karte, die noch nie verwendet wurde, hat einen Abnutzungsgrad von 0 %. Ein Abnutzungsgrad von 100 % gibt an, dass die zu erwartende Lebensdauer der SD-Karte bald abläuft. Wenn der Abnutzungsgras 200% erreicht, besteht ein hohes Risiko einer Fehlfunktion der SD-Karte. Wir empfehlen Ihnen, den Auslöser für Abnutzung auf 80 bis 90 % einzustellen. Dadurch haben Sie Zeit, Aufzeichnungen herunterzuladen und die SD-Karte zu ersetzen, bevor sie möglicherweise abgebnutzt ist. Mit dem Auslöser für Abnutzung können Sie ein Ereignis einrichten und sich eine Benachrichtigung senden lassen, wenn der Abnutzungsgrad den von Ihnen festgelegten Wert erreicht.

Videostromprofile

Ein Videostreamprofil besteht aus einer Gruppe von Einstellungen, die sich auf den Videostream auswirken. Videostreamprofile können in verschiedenen Situationen verwendet werden, z. B. bei der Erstellung von Ereignissen und der Verwendung von Aufzeichnungsregeln.

Add stream profile (Videostreamprofil hinzufügen): Klicken Sie, um ein neues Videostreamprofil zu erstellen.

Preview (Vorschau): Eine Vorschau des Videostreams mit den ausgewählten Einstellungen des Videostreamprofils. Die Vorschau wird aktualisiert, wenn Sie die Einstellungen auf der Seite ändern. Wenn Ihr Gerät unterschiedliche Sichtbereiche hat, können Sie den Sichtbereich in der Dropdown-Ansicht in der unteren linken Ecke des Bildes ändern.

Name: Fügen Sie einen Namen für Ihr Profil hinzu.

Beschreibung: Fügen Sie eine Profilbeschreibung hinzu.

Video codec (Video-Codec): Wählen Sie den Video-Codec aus, der für das Profil verwendet werden soll.

Auflösung: Siehe für eine Beschreibung dieser Einstellung.

Bildrate: Siehe für eine Beschreibung dieser Einstellung.

Komprimierung: Siehe für eine Beschreibung dieser Einstellung.

Zipstream : Siehe für eine Beschreibung dieser Einstellung.

Optimize for storage (Für Speicherung optimieren) : Siehe für eine Beschreibung dieser Einstellung.

Dynamic FPS (Dynamische Bilder pro Sekunde) : Siehe zu einer Beschreibung dieser Einstellung.

Dynamic GOP (Dynamische Bildergruppe) : Siehe zu einer Beschreibung dieser Einstellung.

Mirror (Spiegelung) : Siehe für eine Beschreibung dieser Einstellung.

GOP length (GOP-Länge) : Siehe für eine Beschreibung dieser Einstellung.

Bitrate control (Bitratensteuerung): Siehe für eine Beschreibung dieser Einstellung.

Include overlays (Overlays einbeziehen) : Wählen Sie den Typ der einzubeziehenden Overlays aus. Weitere Informationen zum Hinzufügen von Overlays finden Sie unter .

Include audio (Audio einbeziehen) : Siehe für eine Beschreibung dieser Einstellung.

Über ONVIF

ONVIF-Konten

ONVIF (Open Network Video Interface Forum) ist ein globaler Schnittstellenstandard, der Endbenutzern, Integratoren, Beratern und Herstellern die Nutzung der Vorteile von Netzwerk-Videotechnologie erleichtert. ONVIF ermöglicht die Kompatibilität zwischen Produkten unterschiedlicher Hersteller, erhöhte Flexibilität, verringerte Kosten und zukunftssichere Systeme.

Beim Erstellen eines ONVIF-Kontos wird automatisch die ONVIF-Kommunikation aktiviert. Verwenden Sie den Kontonamen und das Kennwort für sämtliche ONVIF-Kommunikation mit dem Gerät. Weitere Informationen finden Sie auf den Seiten für die Axis Developer Community auf *axis.com*.

Add accounts (Konten hinzufügen): Klicken Sie darauf, um ein neues ONVIF-Konto hinzuzufügen.

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Role (Rolle):

- **Administrator**: Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Bediener**: Hat Zugriff auf alle Einstellungen, außer:
  - Alle **System**-Einstellungen
  - Apps werden hinzugefügt.
- **Media account (Medienkonto)**: Erlaubt nur Zugriff auf den Videostream.

Das Kontextmenü enthält:

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

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

ONVIF-Medienprofile

Ein ONVIF-Medienprofil besteht aus einem Satz von Konfigurationen, mit deren Hilfe Sie die Medienstreameinstellungen ändern können. Sie können neue Profile mit Ihren eigenen Konfigurationen erstellen oder vorkonfigurierte Profile für eine schnelle Einrichtung verwenden.

Add media profile (Medienprofil hinzufügen): Klicken Sie darauf, um ein neues ONVIF-Medienprofil hinzuzufügen.

Profilname: Fügen Sie einen Namen für das Medienprofil hinzu.

Video source (Videoquelle): Wählen Sie die Videoquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts, einschließlich Multiviews, Sichtbereichen und virtuellen Kanälen.

Video encoder (Video-Encoder): Wählen Sie das Videokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Video-Encoders. Wählen Sie Benutzer 0 bis 15 aus, um Ihre eigenen Einstellungen anzuwenden, oder wählen Sie einen der Standardbenutzer aus, wenn Sie vordefinierte Einstellungen für ein bestimmtes Codierungsformat verwenden möchten.

Hinweis

Aktivieren Sie Audio im Gerät, um die Option zur Auswahl einer Audioquelle und Audio-Encoder-Konfiguration zu erhalten.

Audio source (Audioquelle) : Wählen Sie die Audioeingangsquelle für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audioeinstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Audioeingängen des Geräts. Wenn das Gerät über einen Audioeingang verfügt, ist es user0. Wenn das Gerät über mehrere Audioeingänge verfügt, werden weitere Benutzer in der Liste angezeigt.

Audio encoder (Audio-Encoder) : Wählen Sie das Audiokodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Audio-Kodierungseinstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration des Audio-Encoders.

Audio decoder (Audio-Decoder) : Wählen Sie das Audiodekodierungsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.

Audio output (Audioausgang) : Wählen Sie das Audioausgangsformat für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration.

Metadata (Metadaten): Wählen Sie die Metadaten aus, die in Ihre Konfiguration einbezogen werden sollen.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die Metadaten-Einstellungen an. Die Konfigurationen in der Dropdown-Liste dienen als Kennungen/Namen der Konfiguration der Metadaten.

PTZ : Wählen Sie die PTZ-Einstellungen für Ihre Konfiguration aus.

- **Select configuration (Konfiguration wählen)**: Wählen Sie eine benutzerdefinierte Konfiguration aus der Liste aus und passen Sie die PTZ-Einstellungen an. Die Konfigurationen in der Dropdown-Liste entsprechen den Videokanälen des Geräts mit PTZ-Unterstützung.

Create (Erstellen): Klicken Sie hier, um Ihre Einstellungen zu speichern und das Profil zu erstellen.

Cancel (Abbrechen): Klicken Sie hier, um die Konfiguration abzubrechen und alle Einstellungen zu löschen.

profile_x: Klicken Sie auf den Profilnamen, um das vorkonfigurierte Profil zu öffnen und zu bearbeiten.

Melder

Kamera-Manipulation

Der Manipulationsmelder der Kamera generiert einen Alarm, wenn sich die Szene ändert, beispielsweise wenn das Objektiv abgedeckt, besprüht oder stark defokussiert ist, und die in **Trigger delay (Verzögerung beim Auslösen)** festgelegte Zeit verstrichen ist. Der Manipulationsmelder wird nur aktiviert, wenn die Kamera mindestens 10 Sekunden lang nicht bewegt wurde. In dieser Zeit richtet der Melder ein Szenemodell ein, um durch einen Vergleich Manipulationen in aktuellen Bildern zu erkennen. Stellen Sie zur ordnungsgemäßen Einrichtung des Szenemodells sicher, dass die Kamera fokussiert ist, die Lichtbedingungen stimmen und die Kamera nicht auf eine konturlose Szene wie etwa eine leere Wand gerichtet ist. Die Funktion Kameramanipulation kann auch als Bedingung für das Auslösen von Aktionsregeln verwendet werden.

Verzögerung beim Auslösen: Geben Sie ein, wie lange die Manipulationsbedingungen gegeben sein müssen, bevor der Alarm ausgelöst wird. So können falsche Alarme bei bekannten Bedingungen, die das Bild beeinträchtigen, verhindert werden.

Auslösen bei dunklem Bild: Es ist schwer möglich einen Alarm zu generieren, wenn das Kameraobjektiv besprüht wird, denn dieses Ereignis ist unmöglich von anderen Situationen zu unterscheiden, in denen der gleiche Effekt auftritt, also wenn sich etwa die Lichtverhältnisse ändern. Aktivieren Sie diese Einstellung, um in allen Fällen, in denen sich das Bild verdunkelt, Alarme zu erzeugen. Wenn das Gerät ausgeschaltet ist, erzeugt es keinen Alarm, wenn sich das Bild verdunkelt.

Hinweis

Zur Erfassung von Manipulationsversuchen in statischen und nicht überfüllten Szenen.

Audioerkennung

Diese Einstellungen sind für jeden Audioeingang verfügbar.

Lautstärke: Die Lautstärke kann auf einen Wert von 0 bis 100 festgelegt werden, wobei 0 die empfindlichste und 100 die unempfindlichste Einstellung ist. Richten Sie die Lautstärke mithilfe der Aktivitätsanzeige als Richtwert ein. Beim Erstellen von Ereignissen kann der Schallpegel als Bedingung verwendet werden. Sie können wählen, ob eine Aktion ausgelöst werden soll, wenn der Schallpegel den eingestellten Wert übersteigt, unter- oder überschreitet.

Stoßerfassung

Stoßmelder: Aktivieren Sie diese Option, damit ein Alarm erzeugt wird wenn das Gerät von einem Objekt getroffen oder manipuliert wird.

Empfindlichkeitsstufe: Bewegen Sie den Schieberegler, um die Empfindlichkeitsstufe einzustellen, bei der das Gerät einen Alarm erzeugen soll. Bei einem niedrigen Wert erzeugt das Gerät nur bei starkem Schlag einen Alarm. Bei einem hohen Wert erzeugt das Gerät schon bei leichter Manipulation einen Alarm.

Energieeinstellungen

Energieverbrauch

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

Energieeinstellungen

Delayed shutdown (Verzögerte Abschaltung) : Aktivieren Sie dies, wenn Sie eine Verzögerung vor dem Ausschalten der Stromversorgung festlegen möchten.

Delay time (Verzögerungszeit) : Legen Sie eine Verzögerung von 1 bis 60 Minuten fest.

Power saving mode (Energiesparmodus) : Aktivieren Sie diese Option, um das Gerät in den Energiesparmodus zu schalten. Wenn Sie den Energiesparmodus aktivieren, ist die Reichweite der IR-Beleuchtung herabgesetzt.

Energieversorgungskonfiguration einstellen : Ändern Sie die Energieversorgungskonfiguration, indem Sie eine andere PoE-Klasse aus den Optionen auswählen. Klicken Sie auf **Speichern und Neustart**, um die Änderung zu speichern.

Hinweis

Wenn Sie die Stromversorgung auf PoE Klasse 3 festlegen, wird das Profil **Low power profile (Niedrigspannung)** empfohlen, wenn Ihr Gerät über diese Option verfügt.

Dynamic power mode (Dynamischer Energiesparmodus) : Schalten Sie diese Option ein, um den Stromverbrauch zu reduzieren, wenn das Gerät nicht aktiv ist.

I/O port power (Versorgung I/O-Ports) : Schalten Sie diese Option ein, um externe Geräte, die an die I/O-Ports angeschlossen sind, mit 12 V zu versorgen. Schalten Sie diese Option aus, um internen Funktionen wie IR, Heizung und Kühlung Priorität einzuräumen. Dies hat zur Folge, dass Geräte und Sensoren, die eine 12-V-Stromversorgung benötigen, nicht mehr richtig funktionieren.

Strommesser

Energieverbrauch

Zeigt den aktuellen Stromverbrauch, den durchschnittlichen Stromverbrauch, den maximalen Stromverbrauch und den Stromverbrauch im Zeitverlauf an.

Das Kontextmenü enthält:

- **Exportieren**: Klicken Sie hier, um die Diagrammdaten zu exportieren.

Zubehör

E/A-Ports

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

Digitale Ausgänge zum Anschließen externer Geräte wie Relais und LEDs verwenden. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

Port

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

Usage (Nutzung): Die Standardoption für den Relais-Port ist **Door (Zugang)**. Bei Geräten mit Indikatorsymbolen wird  grün, wenn sich der Status ändert und der Zugang entsperrt ist. Wenn Sie das Relais nicht für einen Zugang verwenden und verhindern möchten, dass das Symbol bei einer Statusänderung aufleuchtet, können Sie eine der anderen Optionen für den Port auswählen.

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

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

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

Hinweis

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

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

Protokolle

Protokolle und Berichte

Berichte

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

Protokolle

- **View the system log (Systemprotokoll anzeigen)**: Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **View the access log (Zugangsprotokoll anzeigen)**: Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekennwort verwendet wurde.
- **View the audit log (Audit-Protokoll anzeigen)**: Klicken Sie hier, um Informationen über Benutzer- und Systemaktivitäten anzuzeigen, z. B. erfolgreiche oder fehlgeschlagene Authentifizierungen und Konfigurationen.

Remote System Log

Syslog ist ein Standard für die Nachrichtenprotokollierung. Er ermöglicht die Trennung von der Software, die Nachrichten generiert, dem System, in dem sie gespeichert sind, sowie der Software, die sie meldet und analysiert. Jede Nachricht ist mit einem Einrichtungscode versehen, der den Softwaretyp, der die Nachricht generiert, angibt, und einem Schweregrad zugewiesen.

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

Host: Geben Sie den Hostnamen oder die Adresse des Servers ein.

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

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokoll): Wählen Sie das gewünschte Protokoll aus:

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

Port: Bearbeiten Sie die Port-Nummer, um einen anderen Port zu verwenden.

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

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

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

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

Direktkonfiguration

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

Wartung

Wartung

Restart (Neustart): Gerät neu starten. Die aktuellen Einstellungen werden dadurch nicht beeinträchtigt. Aktive Anwendungen werden automatisch neu gestartet.

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

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

Sämtliche Software des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Software auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper „Axis Edge Vault" unter *axis.com*.

AXIS OS upgrade (AXIS OS-Aktualisierung): Aktualisieren Sie auf eine neue AXIS OS-Version. Neue Versionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste AXIS OS-Version zu verwenden. Um die neueste Version herunterzuladen, gehen Sie zu *axis.com/support*.

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

- **Standardaktualisierung**: Aktualisieren Sie auf die neue AXIS OS-Version.
- **Werkseinstellung**: Aktualisieren und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen AXIS OS-Version zurückkehren.
- **Automatic rollback (Automatisches Rollback)**: Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige AXIS OS-Version zurückgesetzt.

AXIS OS rollback (AXIS OS zurücksetzen): Setzen Sie die Version auf die vorherige AXIS OS-Version zurück.

Fehler beheben

PTR zurücksetzen : Setzen Sie PTR zurück, wenn die Einstellungen für **Pan (Schwenken)**, **Tilt (Neigen)** oder **Roll (Drehen)** aus irgendeinem Grund nicht erwartungsgemäß funktionieren. Die PTR-Motoren werden immer mit einer neuen Kamera kalibriert. Die Kalibrierung kann jedoch verloren gehen, beispielsweise wenn die Kamera an Leistung verliert oder die Motoren von Hand bewegt werden. Beim Zurücksetzen von PTR wird die Kamera neu kalibriert und kehrt in die Werkseinstellungen zurück.

Kalibrierung : Klicken Sie auf **Calibrate (Kalibrieren)**, um die Schwenk-, Neige- und Rollmotoren auf ihre Standardpositionen zu kalibrieren.

Ping: Um zu prüfen, ob das Gerät eine bestimmte Adresse erreichen kann, geben Sie den Host-Namen oder die IP-Adresse des Hosts ein, den Sie anpingen möchten, und klicken Sie auf **Start**.

Port prüfen: Um die Konnektivität des Geräts mit einer bestimmten IP-Adresse und einem TCP/UDP-Port zu überprüfen, geben Sie den Host-Namen oder die IP-Adresse und die Port-Nummer ein, die Sie überprüfen möchten, und klicken Sie auf **Start**.

Netzwerk-Trace

Wichtig

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

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

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

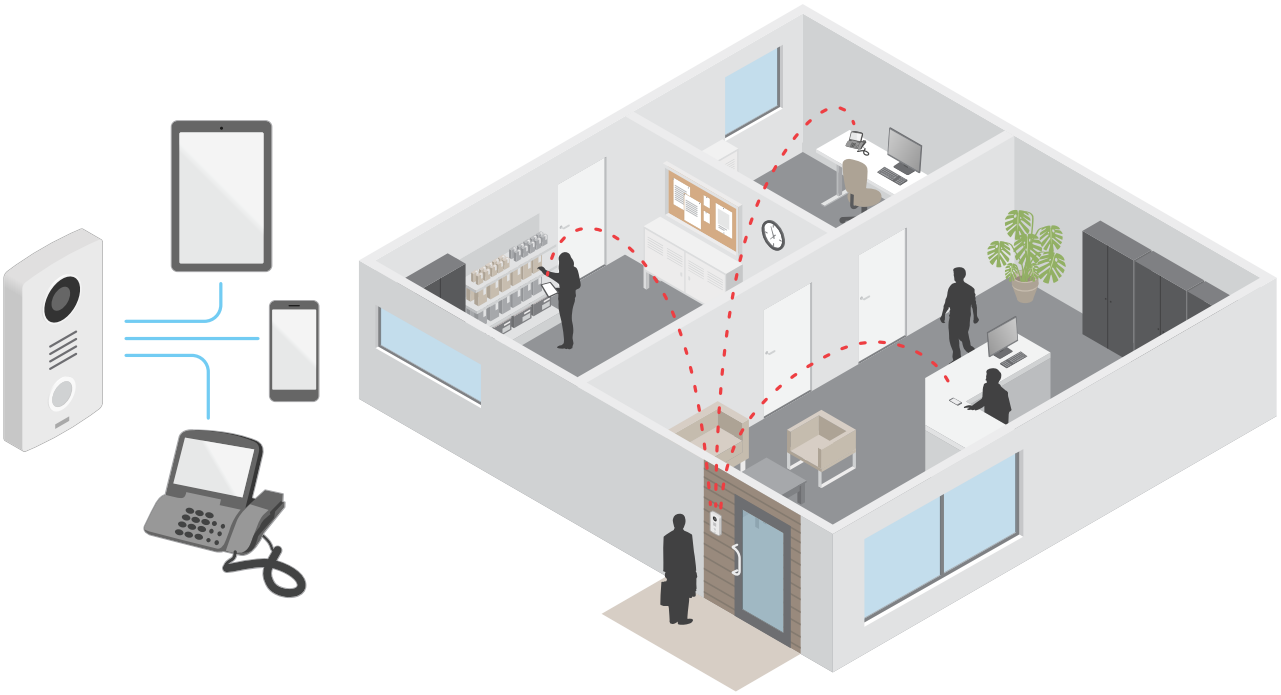
Mehr erfahren

Voice over IP (VoIP)

Bei Voice over IP (VoIP) handelt es sich um eine Technologiegruppe, die Sprachkommunikation und Multimedia-Sitzungen über IP-Netzwerke ermöglicht, z. B. das Internet. Bei herkömmlichen Telefongesprächen werden analoge Signale über einen Übertragungsschaltkreis über das öffentliche Telefonnetz (Public Switched Telephone Network - PSTN) gesendet. Bei einem VoIP-Anruf werden analoge Signale in digitale Signale umgewandelt, um sie über lokale IP-Netzwerke oder das Internet in Datenpaketen zu senden.

Im Axis Produkt wird VoIP durch das Session Initiation Protocol (SIP) und die Signalgebung Dual-Tone Multi-Frequency (DTMF) ermöglicht.

Beispiel:



Wenn Sie die Anruftaste einer Axis IP-Türsprechanlage drücken, wird ein Anruf für einen oder mehrere vordefinierte Empfänger initiiert. Wenn ein Empfänger antwortet, wird ein Anruf eingerichtet. Die Sprach- und Videoübertragung erfolgt über VoIP-Technologien.

Session Initiation Protocol (SIP)

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

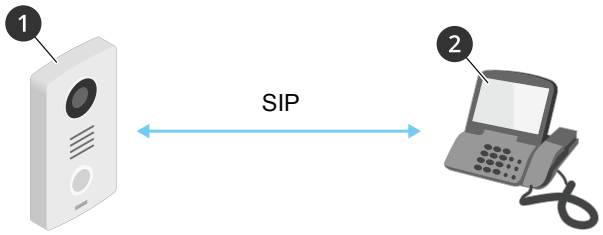
Die eigentlichen Audio- bzw. Videoübertragungen werden zwischen den SIP-Benutzeragenten mit einem Transportprotokoll, wie z. B. RTP (Real-Time Transport Protocol), ausgetauscht.

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

Peer-to-Peer SIP (P2PSIP)

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

Beispiel:



1 *Benutzeragent A – IP-Türsprechanlage. SIP-Adresse: sip:192.168.1.101*
2 *Benutzeragent B – SIP-fähiges Telefon. SIP-Adresse: sip:192.168.1.100*

Sie können die Axis IP-Türsprechanlage so einrichten, dass sie beispielsweise ein SIP-fähiges Telefon im selben Netzwerk mit einem Peer-to-Peer-SIP-Setup anruft.

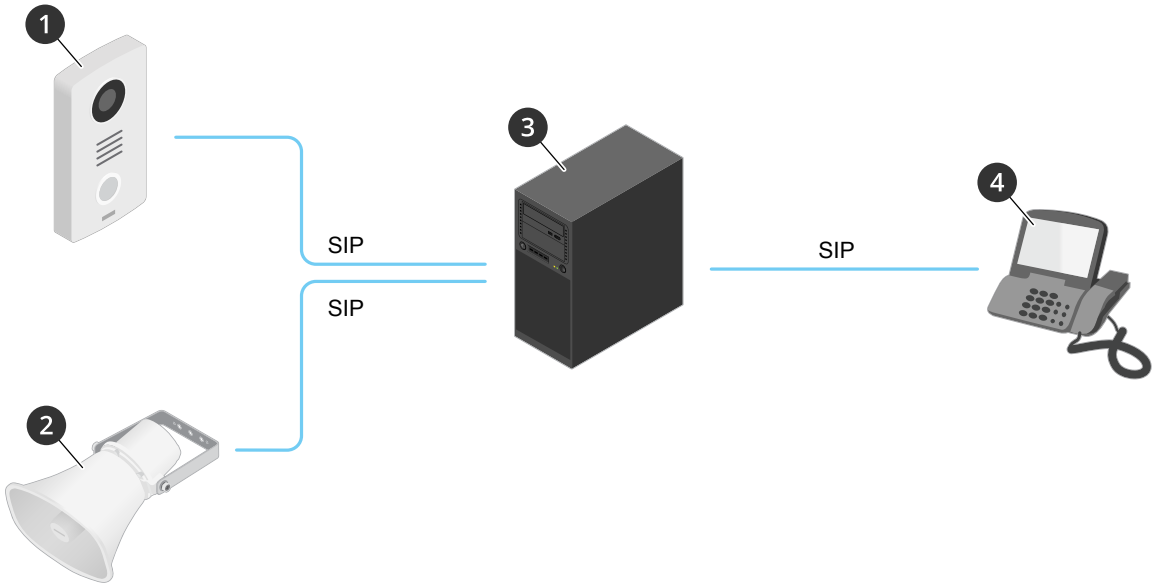
Private Branch Exchange (PBX)

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

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

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

Beispiel:



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX** sip.company.com*
4 *sip:office@company.com*

Wenn Sie die Anruftaste einer Axis IP-Türsprechanlage drücken, wird der Anruf über eine oder mehrere PBX-Anlagen an eine SIP-Adresse entweder im lokalen IP-Netzwerk oder über das Internet weitergeleitet.

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.

Einrichten von Regeln für Ereignisse

Es können Regeln erstellt werden, damit das Gerät beim Auftreten bestimmter Ereignisse eine Aktion ausführt. Eine Regel besteht aus Bedingungen und Aktionen. Die Bedingungen können verwendet werden, um die Aktionen auszulösen. Beispielsweise kann das Gerät beim Erfassen einer Bewegung eine Aufzeichnung starten, eine E-Mail senden oder während der Aufzeichnung einen Overlay-Text anzeigen.

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

Anwendungen

Mit Anwendungen erhalten Sie mehr aus Ihrem Axis Gerät. Die AXIS Camera Application Platform (ACAP) ist eine offene Plattform, die es für andere Anbietern möglich macht, Analysefunktionen und andere Anwendungen für Axis Geräte zu entwickeln. Anwendungen können auf dem Gerät vorinstalliert werden und können kostenlos oder für eine Lizenzgebühr heruntergeladen werden.

Benutzerhandbücher zu Axis Anwendungen finden Sie auf *help.axis.com*.

Cybersicherheit

Produktspezifische Informationen zur Cybersicherheit finden Sie im Datenblatt des Produkts auf axis.com.

Ausführliche Informationen zur Cybersicherheit in AXIS OS finden Sie im *AXIS OS Härtungsleitfaden*.

Axis Sicherheitsbenachrichtigungsdienst

Axis bietet einen Benachrichtigungsdienst mit Informationen zu Sicherheitslücken und anderen sicherheitsrelevanten Angelegenheiten für Axis Geräte. Um Benachrichtigungen zu erhalten, können Sie sich unter *axis.com/security-notification-service* registrieren.

Schwachstellen-Management

Um das Risiko für die Kunden zu minimieren, hält sich Axis als **Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)** an Branchenstandards, um entdeckte Schwachstellen in unseren Geräten, unserer Software und unseren Dienstleistungen zu verwalten und darauf zu reagieren. Weitere Informationen zu den Richtlinien von Axis für das Management von Schwachstellen, zur Meldung von Schwachstellen, zu bereits

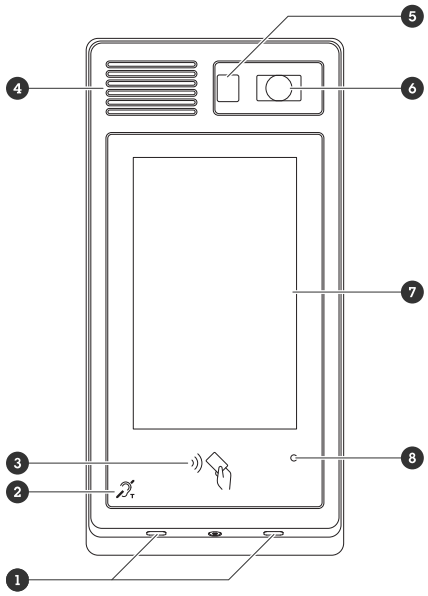
bekannt gewordenen Schwachstellen und zu entsprechenden Sicherheitshinweisen finden Sie unter *axis.com/vulnerability-management*.

Sicherer Betrieb von Axis Geräten

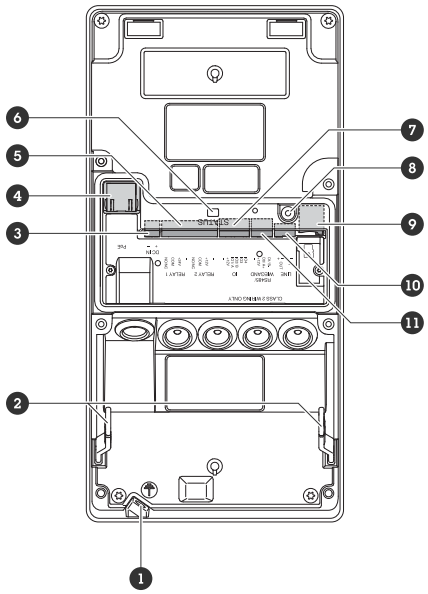
Axis Geräte mit werksseitig festgelegten Standardeinstellungen sind mit sicheren Standardschutzeinrichtungen vorkonfiguriert. Es wird empfohlen, das Gerät mit mehr Sicherheit zu konfigurieren. Mehr erfahren über den Ansatz von Axis zur Cybersicherheit, einschließlich bewährter Praktiken, Ressourcen und Richtlinien zur Sicherung Ihrer Geräte, können Sie unter *https://www.axis.com/about-axis/cybersecurity* aufrufen.

Technische Daten

Produktübersicht



1 *Mikrophone (x2)*
2 *T-Spule*
3 *RFID-Lesegerät*
4 *Lautsprecher*
5 *PIR-Sensor*
6 *Kamera*
7 *Anzeige*
8 *Lichtsensor*



1 *Erdungsschraube*
2 *Scharniere für die Installation*
3 *Stromanschluss*
4 *Netzwerk-Anschluss*
5 *Relaisanschluss (x2)*
6 *Status-LED*

7 E/A-Anschluss
8 Steuertaste
9 Einschub für SD-Karte (MicroSD)
10 Audioanschluss
11 Lesegerätanschluss

LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.

Einschub für SD-Speicherkarte

HINWEIS

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

Dieses Gerät unterstützt Karten des Typs microSD/microSDHC/microSDXC.

Für Empfehlungen zu SD-Karten siehe *axis.com*.

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

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe .

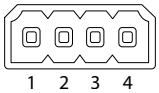
Anschlüsse

Netzwerk-Anschluss

RJ45-Ethernetanschluss mit Power over Ethernet Plus (PoE+).

Audioanschluss

Vierpolige Klemmleiste für Audioeingang und -ausgang.

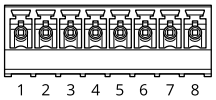


Funktion	Kontakt	Hinweise
Leitungseingang	1	Eingang (Mono)
GND	2	Audio-Masse
Line-Out	3	Line-Out
GND	4	Audio-Masse

Relaisanschluss

8-polige Klemmleiste für Solid State-Relais, der auf folgende Arten eingesetzt werden kann:

- Als Standardrelais, das zum Öffnen und Schließen von Zusatzstromkreisen verwendet wird.
- Zur direkten Steuerung einer Verriegelung.
- Zur Steuerung einer Verriegelung durch ein Sicherheitsrelais. Die Verwendung eines Sicherheitsrelais an der sicheren Seite der Tür verhindert ein Erwärmen der Drähte.



Funktion	Kontakt	Hinweise	Technische Daten
NO/NC	1	Normalerweise geöffnet/normalerweise geschlossen Zum Anschluss von Relaisgeräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Maximalstrom 1 A Max. Spannung 30 V DC
COM	2	Gemeinsam	
24 V Gleichstrom	3	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	Ausgangsspannung 24 V Gleichstrom Maximalstrom 50 mA[1] Maximalstrom 300 mA[2]
Erdung Gleichstrom	4		0 V Gleichstrom
NO/NC	5	Normalerweise geöffnet/normalerweise geschlossen Zum Anschluss von Relaisgeräten. Die beiden Relaisanschlüsse sind galvanisch von den anderen Schaltkreisen getrennt.	Maximalstrom 1 A Max. Spannung 30 V DC
COM	6	Gemeinsam	
12 V Gleichstrom	7	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	Ausgangsspannung 12 V Gleichstrom Maximalstrom 100 mA[1] Maximalstrom 600 mA[2]
Erdung Gleichstrom	8		0 V Gleichstrom

Lesegerätanschluss

4-polige Klemmleiste für den Anschluss externer Leser.

Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
12 V Gleichstrom	2	Zur Stromversorgung von Zusatzgeräten. Hinweis: Dieser Kontakt kann nur als	Ausgangsspannung 12 V Gleichstrom

1. *Bei Stromversorgung über Power over Ethernet IEEE 802.3af/802.3at Typ 1 Klasse 3.*
2. *Bei Stromversorgung über Power over Ethernet Plus (PoE+) IEEE 802.3at Typ 2 Klasse 4 oder DC-Stromeingang.*

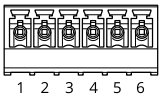
		Stromausgang verwendet werden.	
D0/A+	3	Wiegand: Ausgang DATA0 RS485: A+	
D1/B-	4	Wiegand: Ausgang DATA1 RS485: B-	

E/A-Anschluss

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

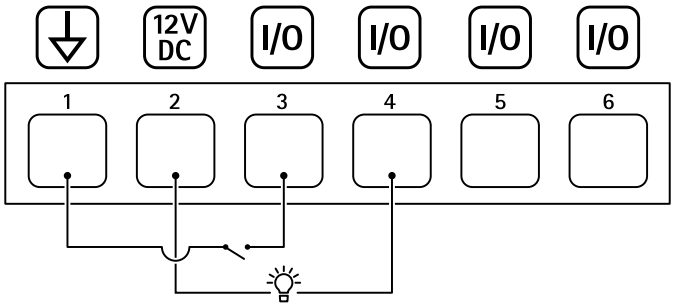
Digitaleingang – Zum Anschließen von Geräten, die zwischen geöffnetem und geschlossenem Schaltkreis wechseln können wie etwa PIR-Sensoren, Tür- und Fensterkontakte sowie Glasbruchmelder.

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.



Funktion	Kontakt	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)	3–6	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

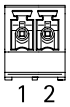
Beispiel:



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

Stromanschluss

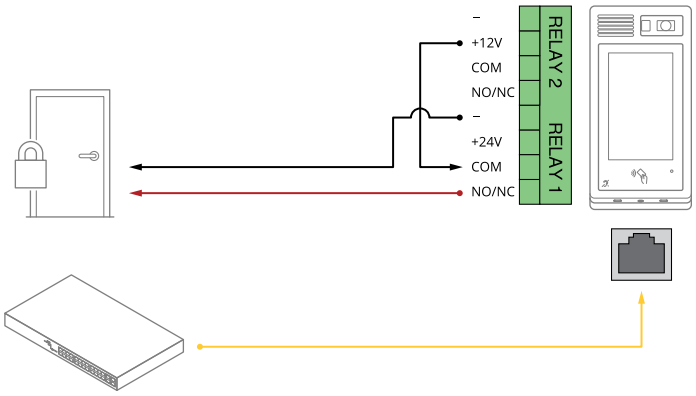
2-poliger Anschlussblock für die Gleichstromversorgung. Eine den Anforderungen für Schutzkleinspannung (SELV) entsprechende Stromquelle mit begrenzter Leistung (LPS) verwenden. Die Nennausgangsleistung muss dabei auf ≤100 W begrenzt sein oder der Nennausgangsstrom auf ≤5 A.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromeingang	2	Stromversorgung der Steuerung bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	18 bis 28 V DC, max. 22 W Max. Last an Ausgängen 9 W

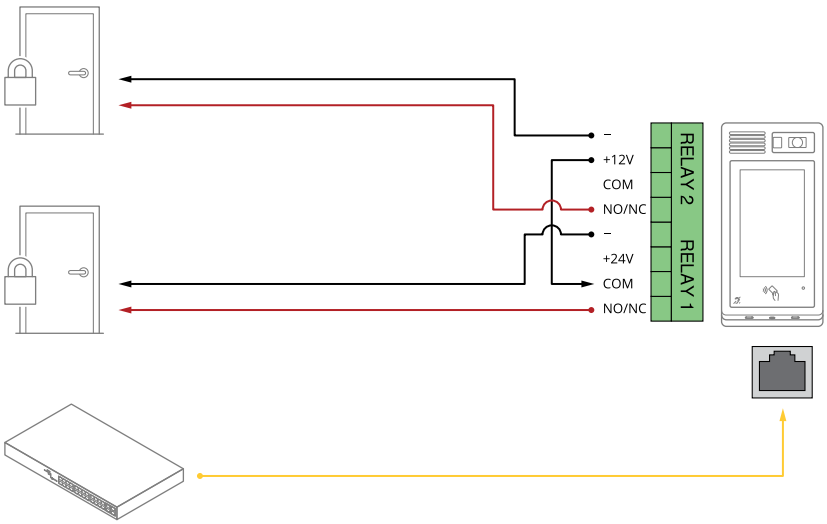
Geräte anschließen

Ein über PoE (12 V) gespeistes Relais



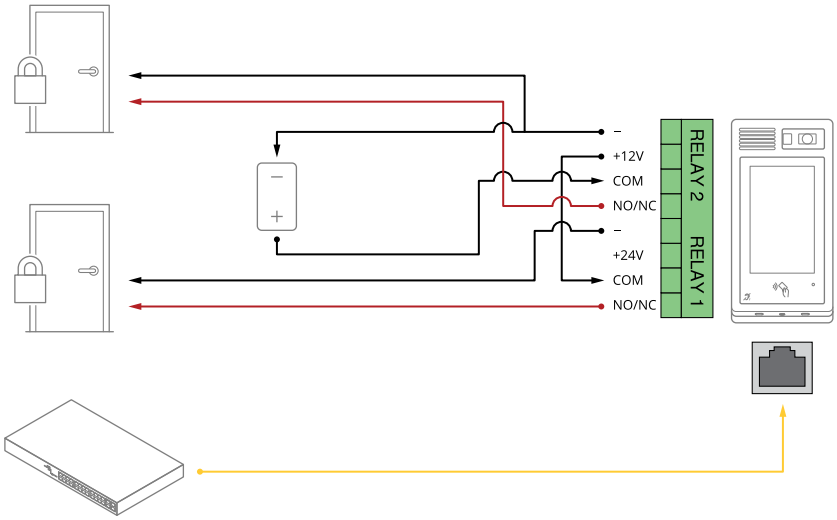
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

Zwei über PoE (12 V) gespeiste Relais



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

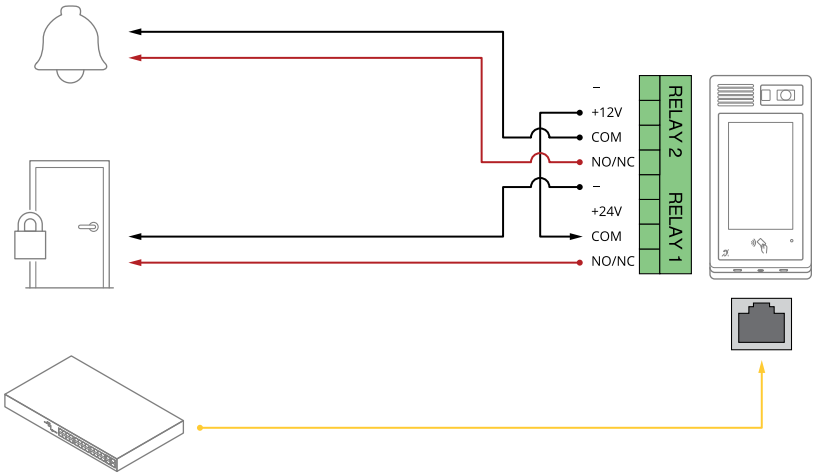
Ein über PoE (12 V) gespeistes Relais + ein über eine externe Stromversorgung gespeistes Relais



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   -  für eine ausfallsichere Verriegelung.
   -  für eine ausfallsichere Verriegelung.

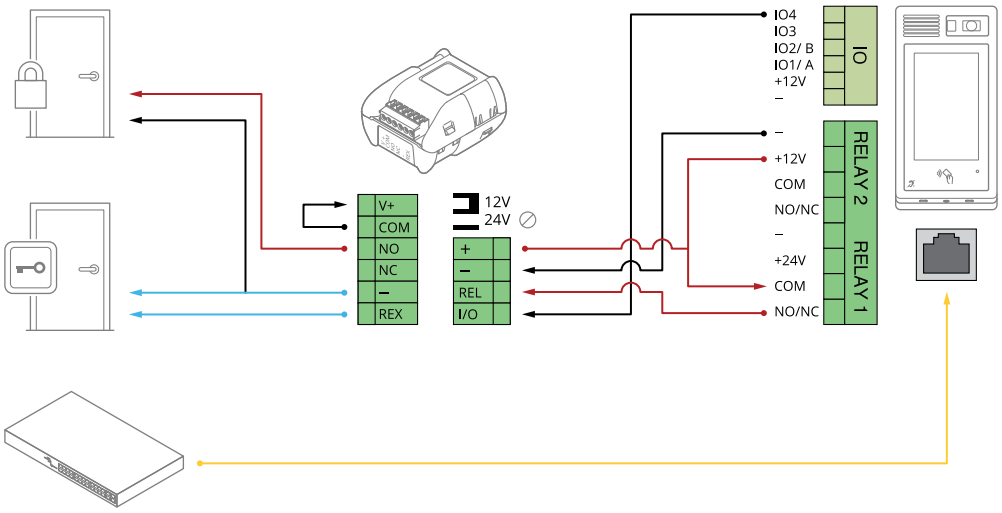
Ein über PoE (12 V) gespeistes Relais + ein potentialfreier Relaiskontakt

Der potenzialfreie Kontakt kann z. B. eine Türglocke sein.



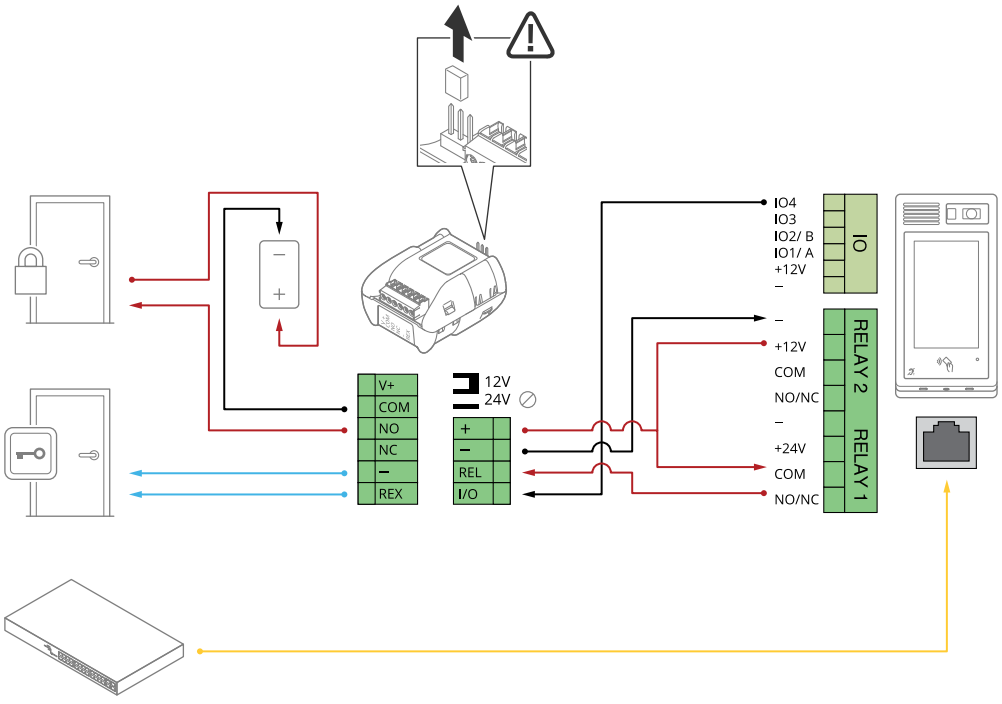
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   -  für eine ausfallsichere Verriegelung.
   -  für eine ausfallsichere Verriegelung.

Ausfallsicheres Schloss (12 V) mit PoE+ Stromversorgung über IP-Türsprechanlage



1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.
   - für eine ausfallsichere Verriegelung.

Ausfallsicheres Schloss mit Stromversorgung über ein externes Netzteil

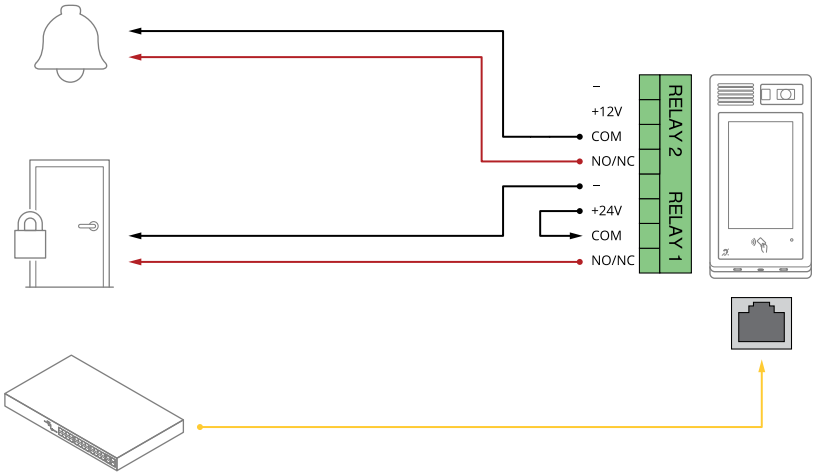


1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   - für eine ausfallsichere Verriegelung.

–  für eine ausfallsichere Verriegelung.

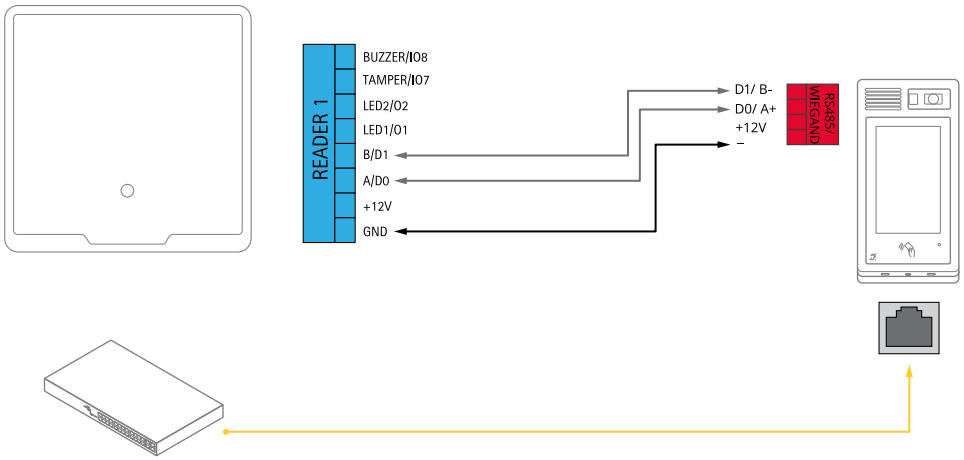
Ein über PoE (24 V) gespeistes Relais + ein potentialfreier Relaiskontakt

Der potenzialfreie Kontakt kann z. B. eine Türglocke sein.



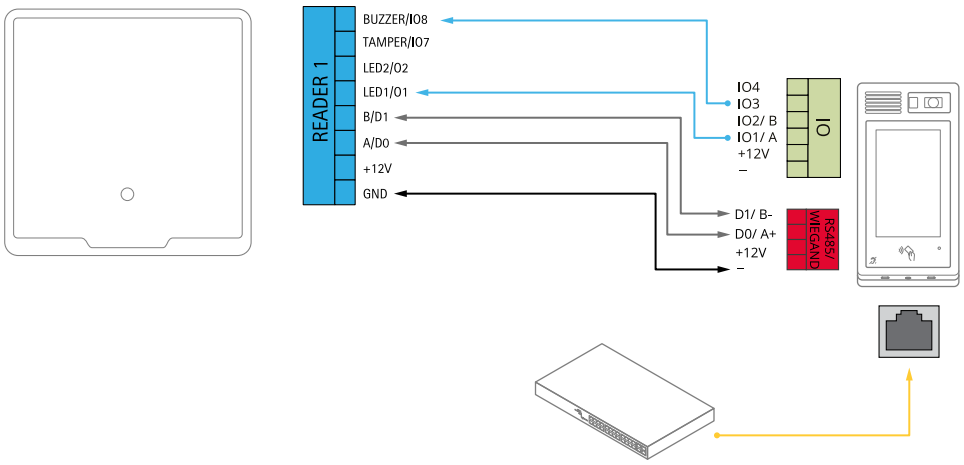
1. Um den Relaisstatus zu überprüfen, wechseln Sie zu **System > Accessories (System > Zubehör)** suchen Sie den Relaisport.
2. Stellen Sie den **Normal state (den Normalzustand)** auf:
   –  für eine ausfallsichere Verriegelung.
   –  für eine ausfallsichere Verriegelung.

Kartenleser verbunden mit Tür-Controller über OSDP



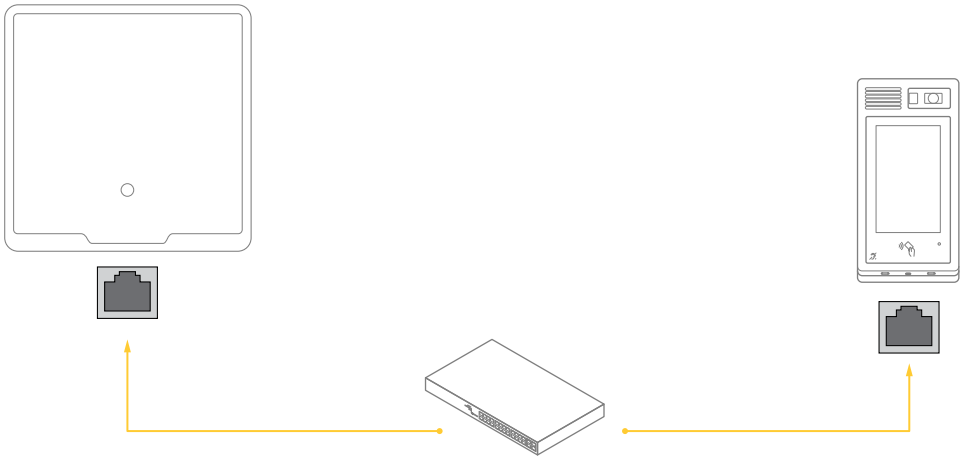
1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **OSDP** und klicken Sie auf **Save (Speichern)**.

Kartenleser verbunden mit Tür-Controller über Wiegand



1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **Wiegand** ein.
3. Aktivieren Sie den **Summer**.
4. Wählen Sie unter **Input for beeper (Eingang für Summer)** die Option **I3**.
5. Wählen Sie unter **Input used for LED control (Eingang für die LED-Steuerung)** die Option **1** aus.
6. Wählen Sie unter **Input for LED1 (Eingang für LED1)** die Option **I1**.
7. Nehmen Sie weitere Einstellungen vor und klicken Sie auf **Save (Speichern)**.

Kartenleser an Axis Tür-Controller mit VAPIX Kartenleser angeschlossen



1. Gehen Sie zu **Reader (Kartenleser) > Connection (Verbindung) > Reader protocol (Kartenleserprotokoll)**.
2. Stellen Sie den **Reader protocol type (Protokolltyp des Kartenlesers)** auf **VAPIX reader (VAPIX Kartenleser)** ein.
3. Verbinden Sie sich mit einem Axis Tür-Controller.

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. Drücken und halten Sie die Steuertaste, um das Gerät wieder einzuschalten. Siehe .
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 dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
   - **Geräte mit AXIS OS 12.0 oder höher:** Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
   - **Geräte mit AXIS OS 11.11 oder niedriger:** 192.168.0.90/24
5. 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

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Gerätesoftware gespeichert (sofern die Funktionen als Teil der neuen AXIS OS-Version verfügbar sind). Es besteht diesbezüglich jedoch keine Gewährleistung seitens Axis Communications AB.
- 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 Fragen, Hinweise und Lösungen

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

Probleme beim Aktualisieren von AXIS OS

Fehler bei der AXIS OS-Aktualisierung	Nach fehlgeschlagener Aktualisierung lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche AXIS OS-Datei hochgeladen wurde. Überprüfen, ob der Name der AXIS OS-Datei dem Gerät entspricht und erneut versuchen.
Probleme nach der AXIS OS-Aktualisierung	Bei nach dem Aktualisieren auftretenden Problemen die Installation über die **Wartungsseite** auf die Vorversion zurücksetzen.

Probleme beim Einrichten der IP-Adresse

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

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Stellen Sie bei aktiviertem HTTPS sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell `http` oder `https` in das Adressfeld des Browsers eingeben. Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe .
Die IP-Adresse wurde von DHCP geändert	Von einem DHCP-Server zugeteilte IP-Adressen sind dynamisch und können sich ändern. Wenn die IP-Adresse geändert wurde, das Gerät mit AXIS IP Utility oder AXIS Camera Management im Netzwerk zu ermitteln. Das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde) ermitteln. Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen dazu finden Sie auf *axis.com/support*.
Zertifikatfehler beim Verwenden von IEEE 802.1X	Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf **Einstellungen > System > Datum und Uhrzeit**.

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

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

- AXIS Camera Station Edge: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station 5: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.
- AXIS Camera Station Pro: Kostenlose 90-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

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

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

Die Firewall blockiert den Datenverkehr über Port 8883, da er als ungesichert eingestuft wird.	In einigen Fällen stellt der Server/Broker möglicherweise keinen bestimmten Port für die MQTT-Kommunikation bereit. Möglicherweise kann MQTT über einen Port verwendet werden, der normalerweise für HTTP/HTTPS-Datenverkehr verwendet wird. • Wenn der Server/Broker WebSocket/WebSocket Secure (WS/WSS) unterstützt (in der Regel auf Port 443, verwenden Sie stattdessen dieses Protokoll. Prüfen Sie mit dem Betreiber des Servers/Brokers, ob WS/WSS unterstützt wird und welcher Port und welcher Basispfad verwendet werden soll. • Wenn der Server/Broker ALPN unterstützt, kann darüber verhandelt werden, ob MQTT über einen offenen Port (wie z. B. 443) verwendet werden soll. Prüfen Sie in Rücksprache mit dem Betreiber Ihres Servers/Brokers, ob ALPN unterstützt wird und welches Protokoll und welcher Port verwendet werden soll.

Leistungsaspekte

Achten Sie beim Einrichten Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die Leistung auswirken. Einige Faktoren wirken sich auf die erforderliche Bandbreite (die Bitrate) aus, andere auf die Bildrate und einige sowohl auf die Bandbreite als auch die Bildrate. Wenn die CPU-Auslastung ihre Grenze erreicht, wirkt sich dies ebenfalls auf die Bildrate aus.

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Hohe Bildauflösung und geringe Komprimierung führen zu Bildern mit mehr Daten, die wiederum mehr Bandbreite erfordern.
- Der Zugriff von vielen Clients des Typs Motion JPEG oder Unicast H.264/H.265/AV1 beeinflusst die Bandbreite.
- Die gleichzeitige Wiedergabe verschiedener Videostreams (Auflösung, Komprimierung) durch mehrere Clients beeinflusst sowohl die Bildrate als auch die Bandbreite.
  Wo immer möglich, identisch konfigurierte Videostreams verwenden, um eine hohe Bildrate zu erhalten. Videostreamprofile werden verwendet, um identische Videostreams sicherzustellen.
- Der gleichzeitige Zugriff auf Video-Streams mit unterschiedlichen Codecs wirkt sich sowohl auf die Bildrate als auch auf die Bandbreite aus. Für eine optimale Leistung sollten Sie Video-Streams mit demselben Codec verwenden.
- Die intensive Verwendung von Ereignissen beeinflusst die CPU-Auslastung, die sich wiederum auf die Bildrate auswirkt.
- Die Verwendung von HTTPS kann, besonders beim Streaming im Format Motion JPEG, die Bildrate reduzieren.
- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Die Wiedergabe auf schlecht arbeitenden Clientcomputern verringert die wahrgenommene Leistung und beeinflusst die Bildrate.
- Mehrere gleichzeitig ausgeführte ACAP-Anwendungen (AXIS Camera Application Platform) können die Bildrate und die allgemeine Leistung beeinflussen.

Support

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

Sicherheitsinformationen

Gefährdungsstufen

⚠ GEFAHR

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠ WARNUNG

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Tod oder schweren Verletzungen führen kann.

⚠ VORSICHT

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu geringfügiger oder mäßiger Verletzung führen kann.

HINWEIS

Weist auf eine gefährliche Situation hin, welche, falls nicht verhindert, zu Sachschäden führen kann.

Andere Meldeebenen

Wichtig

Weist auf wichtige Informationen hin, die den richtigen Betrieb des Produkts gewährleisten.

Hinweis

Weist auf nützliche Informationen hin, die die optimale Verwendung des Produkts unterstützen.

T10213214_de

2025-09 (M4.2)