

AXIS D3110 Connectivity Hub

AXIS D3110 Connectivity Hub

Inhalt

Installation	3
Erste Schritte	4
Das Gerät im Netzwerk ermitteln	4
Weboberfläche des Geräts öffnen	4
Ihr Gerät konfigurieren	6
Einrichten von Regeln für Ereignisse	6
Audio	10
Weboberfläche	11
Status	11
Audio	12
Aufzeichnungen	13
Apps	13
System	14
Wartung	33
Technische Daten	35
Produktübersicht	35
LED-Anzeigen	35
Einschub für SD-Speicherkarte	36
Tasten	36
Anschlüsse	36
Fehlerbehebung	40
Zurücksetzen auf die Werkseinstellungen	40
Optionen für AXIS OS	40
Aktuelle AXIS OS-Version überprüfen	40
AXIS OS aktualisieren	40
Technische Fragen, Hinweise und Lösungen	41
Leistungsaspekte	42
Support	42

AXIS D3110 Connectivity Hub

Installation

Installation



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

help.axis.com/?&pid=72056§ion=install

AXIS D3110 Connectivity Hub

Erste Schritte

Erste Schritte

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

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

Weitere Informationen zu empfohlenen Browsern finden Sie im [AXIS OS Portal](#).

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 [Administratorkonto erstellen auf Seite 4](#).

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter [Weboberfläche auf Seite 11](#).

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

1. Zurücksetzen auf die Werkseinstellungen. Siehe [Zurücksetzen auf die Werkseinstellungen auf Seite 40](#).
Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe [Sichere Kennwörter auf Seite 5](#).
3. Geben Sie das Kennwort erneut ein.

AXIS D3110 Connectivity Hub

Erste Schritte

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 *Zurücksetzen auf die Werkseinstellungen auf Seite 40*.

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

AXIS D3110 Connectivity Hub

Ihr Gerät konfigurieren

Ihr Gerät konfigurieren

Einrichten von Regeln für Ereignisse

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

Lösen Sie eine Aktion aus

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

Hinweis

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

Erfassen einer Manipulation des Eingangssignals

In diesem Beispiel wird erklärt, wie man eine E-Mail sendet, wenn das Eingangssignal unterbrochen oder kurzgeschlossen wurde. Weitere Informationen zum E/A-Anschluss finden Sie unter *Seite 37*.

1. Gehen Sie auf **System > Accessories (System > Zubehör)** und aktivieren Sie **Supervised (Überwacht)** für den jeweiligen Port.

Einen E-Mail-Empfänger hinzufügen:

1. Wechseln Sie zu **Settings > Events > Recipients (Einstellungen > Ereignisse > Empfänger)** und fügen Sie einen Empfänger hinzu.
2. Geben Sie den Namen des Empfängers ein.
3. Wählen Sie **E-Mail**.
4. Geben Sie eine E-Mail-Adresse ein, an die die E-Mail gesendet werden soll.
5. Die Kamera besitzt keinen eigenen E-Mail-Server. Um Mails senden zu können, muss sie sich bei einem anderen E-Mail-Server anmelden. Geben Sie die anderen Informationen gemäß Ihrem E-Mail-Anbieter ein.
6. Klicken Sie auf **Test**, um eine Test-E-Mail zu senden.
7. **Save (Speichern)** anklicken.

Eine Regel erstellen:

1. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie aus der Liste der Bedingungen unter **I/O** die Option **Überwachte Eingangsmanipulation** aktiv aus.
4. Wählen Sie den entsprechenden Port aus.
5. Wählen Sie in der Liste der Aktionen unter **Benachrichtigungen** die Option **Benachrichtigung an E-Mail-Adresse senden** und wählen Sie dann den Empfänger aus der Liste.
6. Geben Sie einen Betreff und eine Nachricht für die E-Mail ein.

AXIS D3110 Connectivity Hub

Ihr Gerät konfigurieren

7. Save (Speichern) anklicken.

Aktivieren einer Leuchte beim Öffnen des Fensters

In diesem Beispiel wird erläutert, wie Sie einen Fensterkontakt mit einem Connectivity Hub verbinden und ein Ereignis so einrichten, dass eine Leuchte eingeschaltet wird, sobald ein Fenster mit Kontakt geöffnet wird.

Voraussetzungen

- Schließen Sie ein 2-Drahtkabel (Erde, E/A) an den Fensterkontakt und den E/A-Anschluss des Connectivity Hubs an.
- Schließen Sie die Lampe an die Stromversorgung und den Relaisanschluss des Connectivity Hubs an

Konfiguration der E/A-Anschlüsse im Connectivity Hub

1. Gehen Sie zu **System > Zubehör**.
2. Geben Sie folgende Informationen in **Anschluss 1** ein:
 - **Name:** Fenstersensor
 - **Richtung:** Eingang
 - **Normal state (Normalzustand):** Stromkreis geschlossen
3. Geben Sie folgende Informationen in **Anschluss 2** ein:
 - **Name:** Leuchte
 - **Richtung:** Ausgang
 - **Normal state (Normalzustand):** Stromkreis offen

Erstellen von zwei Regeln im Connectivity Hub

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
 - **Name:** Fenstersensor
 - **Condition (Bedingung):** Digitaleingang
Wählen Sie Die Bedingung als Auslöser verwenden
 - **Port:** Fenstersensor
 - **Aktion:** E/A umschalten während die Regel aktiv ist
 - **Port:** Leuchte
 - **Status:** Aktiv
3. Save (Speichern) anklicken.

Connectivity Hub über MQTT aktivieren, wenn die Kamera Bewegung erkennt

Voraussetzungen

- Konfigurieren Sie ein Gerät für den E/A-Anschluss 1 im Connectivity Hub.
- Richten Sie einen MQTT-Broker ein und rufen Sie die IP-Adresse, den Benutzernamen und das Kennwort des Brokers ab.
- Richten Sie AXIS Motion Guard in der Kamera ein.

AXIS D3110 Connectivity Hub

Ihr Gerät konfigurieren

MQTT-Client in der Kamera einrichten

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

In der Kamera zwei Regeln für die Veröffentlichung über MQTT erstellen

1. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
 - **Name:** Bewegung erkannt
 - **Condition (Bedingung):** Anwendungen > Motion Alarm
 - **Aktion:** MQTT > Send MQTT publish message (MQTT-Meldung zu Veröffentlichung senden)
 - **Topic (Thema):** Bewegung
 - **Nutzlast:** An
 - **QoS:** 0, 1 oder 2
3. **Save (Speichern)** anklicken.
4. Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
 - **Name:** Keine Bewegung
 - **Condition (Bedingung):** Anwendungen > Motion Alarm
 - Wählen Sie **Diese Bedingung umkehren**.
 - **Aktion:** MQTT > Send MQTT publish message (MQTT-Meldung zu Veröffentlichung senden)
 - **Topic (Thema):** Bewegung
 - **Nutzlast:** Aus
 - **QoS:** 0, 1 oder 2
5. **Save (Speichern)** anklicken.

Richten Sie den MQTT-Client im Connectivity Hub ein.

1. Gehen Sie in der Geräteschnittstelle des Connectivity Hub zu **System > MQTT > MQTT-Client > Broker** und geben Sie folgende Informationen ein:
 - **Host:** IP-Adresse des Brokers
 - **Client-ID:** Anschluss 1
 - **Protocol (Protokoll):** Das Protokoll, auf das der Broker festgelegt ist

AXIS D3110 Connectivity Hub

Ihr Gerät konfigurieren

- Port: Die vom Broker verwendete Portnummer
 - Benutzername und Kennwort
2. Klicken Sie auf **Gehe zu** und **Verbinden**.
 3. Gehen Sie zu **MQTT-Abonnements** und fügen Sie ein Abonnement hinzu.

Geben Sie folgende Informationen ein:

- **Abonnementfilter:** Bewegung
 - **Abonnementart:** Statusbehaftet
 - **QoS:** 0, 1 oder 2
4. **Save (Speichern)** anklicken.

Im Connectivity Hub eine Regel für MQTT-Abonnements erstellen

1. Gehen Sie auf **System > Events > Rules (System > Ereignisse > Regeln)** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
 - **Name:** Bewegung erkannt
 - **Condition (Bedingung):** MQTT > Stateful (Statusbehaftet)
 - **Abonnementfilter:** Bewegung
 - **Nutzlast:** An
 - **Aktion:** I/O (E/A) > Toggle I/O while the rule is active (Bei aktiver Regel E/A umschalten):
 - **Port:** E/A 1.
3. **Save (Speichern)** anklicken.

Ein Schloss durch Drücken einer Taste öffnen

In diesem Beispiel wird erläutert, wie Sie ein Relais an den Connectivity Hub anschließen und ein Ereignis so einrichten, dass ein Schloss geöffnet wird, wenn eine an den Connectivity Hub angeschlossene Taste gedrückt wird.

Voraussetzungen

- Schließen Sie ein 2-Drahtkabel (COM, NO) an das Schloss und den Relaisanschluss am Connectivity Hub an.
- Schließen Sie ein 2-Drahtkabel (Erde, E/A) an die Taste und den E/A-Anschluss des Connectivity Hub an.

Konfiguration der E/A-Anschlüsse im Connectivity Hub

1. Gehen Sie zu **System > Zubehör**.
2. Geben Sie folgende Informationen in **Anschluss 1** ein:
 - **Name:** Taste
 - **Richtung:** Eingang
 - **Normal state (Normalzustand):** Stromkreis offen
3. Geben Sie folgende Informationen in **Anschluss 9** ein:
 - **Name:** Schloss
 - **Normal state (Normalzustand):** Stromkreis offen

AXIS D3110 Connectivity Hub

Ihr Gerät konfigurieren

Erstellen einer Regel im Connectivity Hub

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie folgende Informationen ein:
 - **Name:** Schloss öffnen
 - **Condition (Bedingung):** I/O > Digital input is active (E/A > Digitaler Eingang ist aktiv)
Wählen Sie Die **Bedingung als Auslöser** verwenden
 - **Port:** Taste
 - **Aktion:** I/O > Toggle I/O once (E/A > Einmalig E/A umschalten):
 - **Port:** Schloss
 - **Status:** Aktiv
 - **Dauer:** 10 s
3. **Save (Speichern)** anklicken.

Audio

Audio auf SD-Karte aufzeichnen



In diesem Beispiel wird erläutert, wie Sie die Aufzeichnung von zwei Mikrofonen auf eine SD-Karte einrichten.

Bevor Sie beginnen:

- Schließen Sie zwei Mikrofone an und setzen Sie eine microSD-Karte in den Connectivity Hub ein.
1. Gehen Sie zu **Audio > Geräteeinstellungen** und aktivieren Sie **Eingang 0: IN 1** und **Eingang 1: IN 2**.
 2. Wählen Sie **Eingangstyp** und **Spannungstyp**.
 3. Wenn die Geräuschpegel innerhalb des Raums schwanken, aktivieren Sie die **Automatische Verstärkungsregelung**.
 4. Gehen Sie zu **System > Speicher > Integrierter Speicher** und legen Sie die **Aufbewahrungszeit** fest.
 5. Gehen Sie zu **Audio > Stream** und wählen Sie **Codierung**.

Hinweis

Um bei mehreren Streams (z. B. Aufzeichnung und Livestream von derselben Quelle) die CPU-Last gering zu halten, verwenden Sie für beide Streams dieselbe Codierung.

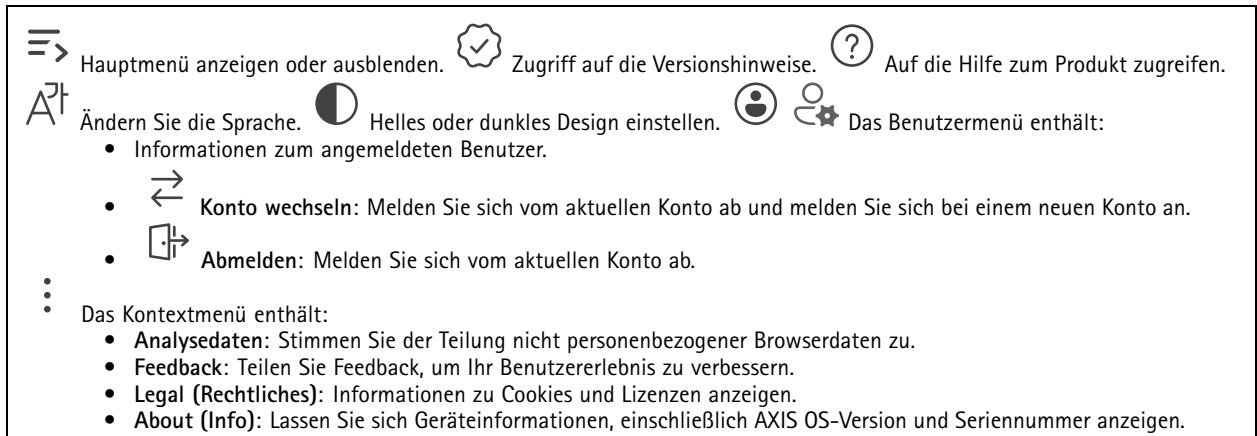
6. Gehen Sie zu **Audio > Listen and record (Hören und aufzeichnen)** und klicken Sie auf .
7. Klicken Sie auf .

AXIS D3110 Connectivity Hub

Weboberfläche

Weboberfläche

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



The screenshot shows the main menu of the AXIS D3110 Connectivity Hub. It includes the following items:

- 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

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 Härtingsleitfaden*.

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

Zeitsynchronisierungsstatus

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

NTP-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.

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.

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 *Aufzeichnungen auf Seite 13* Anzeige des Speicherorts der Aufzeichnung.







AXIS D3110 Connectivity Hub

Weboberfläche

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.  **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.

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.

Mithören und aufzeichnen

 Klicken Sie darauf, um zu hören.  Startet eine ständige Aufzeichnung des Audiostreams. Um den Aufzeichnungsvorgang zu stoppen, erneut anklicken. Wenn eine Aufzeichnung läuft, wird sie nach einem Neustart automatisch fortgesetzt.

Hinweis

Sie können nur zuhören und aufzeichnen, wenn der Eingang für das Gerät aktiviert ist. Wechseln Sie zu **Audio > Device settings (Audio > Geräteinstellungen)**, um sicherzustellen, dass der Eingang aktiviert ist.



 zeigt den konfigurierten Speicher für das Gerät an. Melden Sie sich als Administrator an, um den Speicher zu konfigurieren.

AXIS D3110 Connectivity Hub



Weboberfläche



Audioverbesserung







Eingang

Ten Band Graphic Audio Equalizer (Grafischer Zehnband-Audio-Equalizer): Aktivieren Sie diese Einstellung, um innerhalb eines Audiosignals den Pegel der verschiedenen Frequenzbänder einzustellen. Diese Funktion ist für fortgeschrittene Benutzer mit Erfahrung in der Audiokonfiguration.**Talkback range (Talkbackbereich)**  : Wählen Sie den Betriebsbereich zum Erfassen von Audioinhalten. Eine Erhöhung des Betriebsbereichs reduziert die simultane 2-Wege-Kommunikationsfähigkeit. **Voice enhancement (Sprachverbesserung)**  : Aktivieren Sie diese Einstellung, um die Sprachinhalte im Verhältnis zu anderen Sounds zu verbessern.





Aufzeichnungen

 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.

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.

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.**Anwendungen mit Root-Berechtigung zulassen**  : Aktivieren Sie diese Option, um Apps mit Root-Berechtigungen uneingeschränkter Zugriff auf das Gerät 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.

AXIS D3110 Connectivity Hub

Weboberfläche

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.
 - **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.

AXIS D3110 Connectivity Hub

Weboberfläche

- **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.

Gerätstandort

Den Gerätstandort 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 das Gerät eingeben.
- **Speichern:** Klicken Sie hier, um den Gerätstandort zu speichern.

Netzwerk

IPv4

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

IP-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

AXIS D3110 Connectivity Hub

Weboberfläche

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 Sie 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**

AXIS D3110 Connectivity Hub

Weboberfläche

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

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.
 - **Warmstart:** Versendet eine Trap-Nachricht, wenn Sie eine SNMP-Einstellung ändern.
 - **Verbindungsaufbau:** Versendet eine Trap-Meldung, wenn der Status eines Links von Down zu Up wechselt.
 - **Authentifizierung fehlgeschlagen:** Versendet eine Trap-Meldung, wenn ein Authentifizierungsversuch fehlschlägt.

Hinweis

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

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

AXIS D3110 Connectivity Hub

Weboberfläche

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.

- **Kenntwort 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.

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.

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 Schlüsseln: 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.

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



Das Kontextmenü enthält:

- **Certificate information (Zertifikatsinformationen):** 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)  :

- **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)

AXIS D3110 Connectivity Hub

Weboberfläche

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 Passwort (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, die der Netzwerk-Switch bei Verwendung von Peap-Version 1 verwendet.

Diese Einstellungen stehen nur zur Verfügung, wenn Sie IEEE 802.1x 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

Activate (Aktivieren): Schalten Sie die Firewall ein.

Default Policy (Standardrichtlinie): Wählen Sie den Standardstatus für die Firewall aus.

- **Allow: (Zulassen:)** Ermöglicht alle Verbindungen mit dem Gerät. Diese Option ist in der Standardeinstellung festgelegt.
- **Deny: (Verweigern:)** Verhindert alle Verbindungen mit dem Gerät.

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

- **Adresse:** Geben Sie eine Adresse im IPv4-/IPv6- oder im CIDR-Format ein, für die Sie den Zugriff zulassen oder verweigern möchten.
- **Protocol (Protokoll):** Wählen Sie ein Protokoll aus, für das Sie den Zugriff zulassen oder verweigern möchten.
- **Port:** Geben Sie eine Portnummer ein, für die Sie den Zugriff zulassen oder verweigern möchten. Sie können eine Portnummer zwischen 1 und 65535 hinzufügen.
- **Richtlinie:** Wählen Sie die Richtlinien der Regel aus.



: Klicken Sie darauf, um eine weitere Regel zu erstellen.

Add rules: (Regeln hinzufügen:) Klicken Sie hier, um die von Ihnen definierten Regeln hinzuzufügen.

AXIS D3110 Connectivity Hub

Weboberfläche


- **Time in seconds: (Zeit in Sekunden):** Legen Sie für das Testen der Regeln ein Zeitlimit fest. Das Standardzeitlimit beträgt 300 Sekunden. Legen Sie als Zeit 0 Sekunden fest, um die Regeln sofort zu aktivieren.
- **Confirm rules: (Regeln bestätigen):** Bestätigen Sie die Regeln und deren Zeitlimit. Wenn Sie eine Zeitbegrenzung von mehr als einer Sekunde festgelegt haben, sind die Regeln in dieser Zeit aktiv. Wenn Sie als Zeit 0 eingestellt haben, sind die Regeln sofort aktiv.

Pending rules (Ausstehende Regeln): Eine Übersicht über die kürzlich getesteten, noch zu bestätigenden Regeln.

Hinweis

Die Regeln mit einer Zeitgrenze werden unter **Active rules (Aktive Regeln)** angezeigt, bis der angezeigte Timer abläuft oder Sie die Regeln bestätigen. Wenn Sie die Regeln nicht bestätigen, werden sie unter **Pending rules (Ausstehende Regeln)** angezeigt, bis der Timer abläuft, und die Firewall wird auf die zuvor festgelegten Einstellungen zurückgesetzt. Wenn Sie diese bestätigen, werden die aktuellen aktiven Regeln ersetzt.

Confirm rules (Regeln bestätigen): Klicken Sie hier, um die anstehenden Regeln zu aktivieren. **Active rules (Aktive Regeln):** Eine

Übersicht über die Regeln, die momentan auf dem Gerät ausgeführt werden.  : Klicken Sie hier, um eine aktive Regel zu

löschen.  : Klicken Sie hier, um alle Regeln zu löschen, sowohl anstehend als auch aktiv.

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:** Darf keine Änderungen an den Einstellungen vornehmen.



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.

AXIS D3110 Connectivity Hub

Weboberfläche

SSH-Konten

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

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

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.

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.

AXIS D3110 Connectivity Hub

Weboberfläche



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 unter *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 Zielservers. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielservers 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.

AXIS D3110 Connectivity Hub

Weboberfläche


- **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. Weitere Informationen zu AXIS OS Portal finden Sie unter *AXIS OS*.

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. Auf 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.

AXIS D3110 Connectivity Hub

Weboberfläche

MQTT-Client

Connect (Verbinden): Aktivieren oder deaktivieren Sie den MQTT-Client.**Status:** Zeigt den aktuellen Status des MQTT-Clients an.**BrokerHost:** 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-Namespace 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

AXIS D3110 Connectivity Hub

Weboberfläche



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.

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 eingehenden 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.

AXIS D3110 Connectivity Hub

Weboberfläche

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

Hinweis

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

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

Zusätzliches

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

AXIS D3110 Connectivity Hub

Weboberfläche

- **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 Domännennamen hergestellt werden, die sowohl in IPv4- als auch in IPv6-Adressen auflösen. IPv6 kann nur für Domännennamen 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.

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.

Speicherung

Netzwerk-Speicher

AXIS D3110 Connectivity Hub

Weboberfläche

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\Benutzername` 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.

AXIS D3110 Connectivity Hub

Weboberfläche

- **Change password (Kennwort ändern):** Ändern 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 Abnutzungsgrad 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 abgenutzt 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.

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. **Profile name:** 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.

AXIS D3110 Connectivity Hub

Weboberfläche

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

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.

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.


AXIS D3110 Connectivity Hub

Weboberfläche

PortName: Bearbeiten Sie den Text, um den Port umzubenennen. **Direction (Richtung):**  gibt an, dass es sich bei dem Port um einen Eingangsport handelt.  gibt an, dass es sich um einen Ausgangsport handelt. Wenn der Port konfigurierbar ist, können Sie auf die Symbole klicken, um zwischen Eingang und Ausgang zu wechseln. **Normal state (Normalzustand):** Klicken Sie auf  für einen 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.

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.

AXIS D3110 Connectivity Hub

Weboberfläche



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. **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):** Setzen 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: Setzen 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.

AXIS D3110 Connectivity Hub

Weboberfläche

- **Automatisches Zurücksetzen:** 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

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 check (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 **StartNetzwerk-Trace**

Wichtig

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

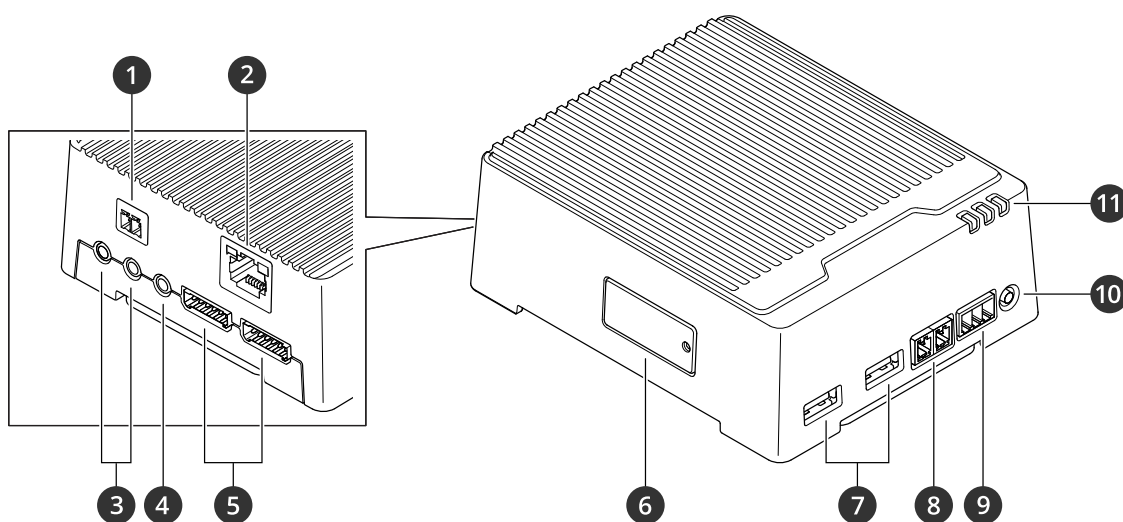
Ein Netzwerk-Trace hilft durch die Aufzeichnung von Aktivitäten im Netzwerk beim Beheben von Problemen. **Trace time (Trace-Dauer):** Die Dauer des Trace in Sekunden oder Minuten angeben und **Herunterladen** anklicken.

AXIS D3110 Connectivity Hub

Technische Daten

Technische Daten

Produktübersicht



- 1 Stromanschluss
- 2 Ethernetanschluss RJ-45
- 3 2 Mikrofonanschlüsse
- 4 Audio-Ausgang
- 5 2 E/A-Anschlüsse
- 6 Einschub für MicroSD-Karte
- 7 2 USB-Anschlüsse
- 8 Anschlussstyp RS-485/RS-422
- 9 Relaisanschluss
- 10 Steuertaste
- 11 Status-LED

LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.

AXIS D3110 Connectivity Hub

Technische Daten

Gelb	Leuchtet beim Start. Blinkt bei der Aktualisierung der Gerätesoftware.
Gelb/rot	Blinkt orange/rot, wenn die Netzwerk-Verbindung nicht verfügbar ist oder unterbrochen wurde.
Rot	Blinkt rot bei einem Fehler bei der Aktualisierung der Gerätesoftware.

Einschub für SD-Speicherkarte

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 *Zurücksetzen auf die Werkseinstellungen auf Seite 40*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Drücken Sie zum Herstellen der Verbindung die Taste und halten Sie sie etwa 3 Sekunden lang gedrückt, bis die Status-LED grün blinkt.

Anschlüsse

Netzwerk-Anschluss

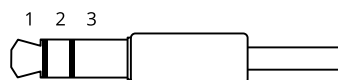
Ethernet-Anschluss RJ-45

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

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

Audioanschluss

- **Audioeingang** – 3,5 mm-Eingang für ein digitales Mikrofon, ein analoges Monomikrofon oder ein Line-In-Monosignal (linker Kanal wird aus einem Stereosignal verwendet).
- **Audioausgang** – 3,5-mm-Audioausgang (Leitungspegel) zum Anschluss an eine Beschallungsanlage (PA) oder einen Aktivlautsprecher mit integriertem Verstärker. Für den Audioausgang muss ein Stereostecker verwendet werden.



Audioeingang

1 Spitze	2 Ring	3 Hülse
Unsymmetrisches Mikrofon (mit oder ohne Elektretspeisung) oder Leitung	Elektretspeisung, sofern ausgewählt	Masse
Symmetrisches Mikrofon (mit oder ohne Phantomspannung) oder Leitung, „Hot“-Signal	Symmetrisches Mikrofon (mit oder ohne Phantomspannung) oder Leitung, „Cold“-Signal	Masse
Digitales Signal	Klingelstrom, sofern ausgewählt	Masse

AXIS D3110 Connectivity Hub

Technische Daten

Audio-Ausgang

1 Spitze	2 Ring	3 Hülse
Kanal 1, unsymmetrische Leitung, Mono	Kanal 1, unsymmetrische Leitung, Mono	Masse

E/A-Anschluss

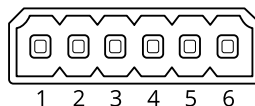
Über den E/A-Anschluss werden externe Geräte in Verbindung mit Manipulationsalarmen, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Zusätzlich zum Gleichstrombezugspunkt 0 V DC und der Stromversorgung (12-VDC-Ausgang) stellt der E/A-Anschluss folgende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

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

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

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

Sechspoliger Anschlussblock

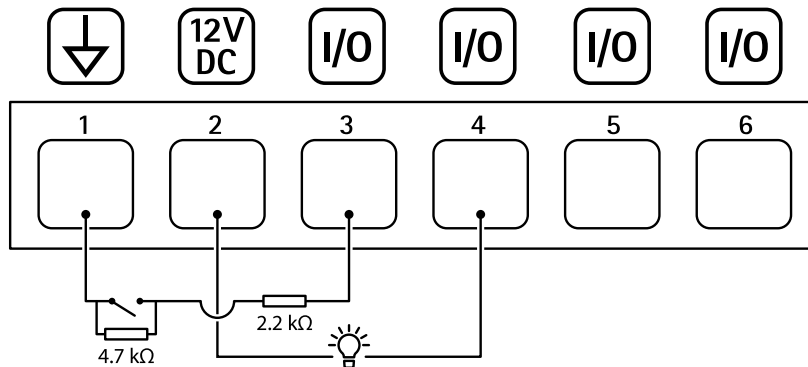


Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 50 mA
Konfigurierbar (Ein- oder Ausgang)	3-6	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen. Um überwachten Eingang zu nutzen, Abschlusswiderstände anschließen. Informationen zum Anschließen der Widerstände bietet der Schaltplan.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last wie etwa einem Relais muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

Beispiel:

AXIS D3110 Connectivity Hub

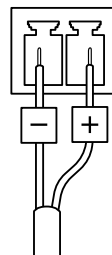
Technische Daten



- 1 Erdung Gleichstrom
- 2 Gleichstromausgang 12 V, max. 50 mA
- 3 Als überwachter Eingang konfigurierter E/A
- 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) kompatible Stromquelle mit begrenzter Leistung (LPS) verwenden. Die Nennausgangsleistung muss dabei auf ≤ 100 W begrenzt sein oder der Nennausgangsstrom auf ≤ 5 A.

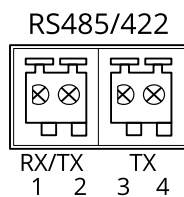


Anschluss typ RS-485/RS-422

Zwei 2-polige Anschlussblöcke für serielle Schnittstellen vom Typ RS485/RS422.

Der serielle Anschluss kann in den folgenden Anschlussmodi konfiguriert werden:

- zweidriger RS485-Halbduplex-Anschluss
- vierdriger RS485-Vollduplex-Anschluss
- zweidriger RS422-Simplex-Anschluss
- vierdriger RS422-Vollduplex-Anschluss (Punkt-zu-Punkt-Verbindung)



AXIS D3110 Connectivity Hub

Technische Daten

Funktion	Kontakt	Hinweise
RS485/RS422 RX/TX A	1	(RX) RS485/RS422 für Vollduplex (RX/TX) Für Halbduplex RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) RS485/RS422 für Vollduplex
RS485/RS422 TX B	4	

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

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

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 35*.
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 D3110 Connectivity Hub

Fehlerbehebung

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 <code>ping</code> und die IP-Adresse des Geräts ein): <ul style="list-style-type: none">• Wenn Folgendes angezeigt wird: <code>Reply from (Antwort von) <IP address (IP-Adresse)>: bytes=32; time=10...</code> 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 Folgendes angezeigt wird: <code>Request timed out</code> 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.

AXIS D3110 Connectivity Hub

Fehlerbehebung

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Stellen Sie bei aktiviertem HTTPS sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell <code>http</code> oder <code>https</code> in das Adressfeld des Browsers eingeben. Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe <i>Zurücksetzen auf die Werkseinstellungen auf Seite 40</i> .
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.	<p>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.</p> <ul style="list-style-type: none">• 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

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.
- Das gleichzeitige Ausführen mehrerer Aktivitäten kann die Audioleistung beeinträchtigen.
- Um die CPU-Auslastung gering zu halten, verwenden Sie für mehrere Streams dieselbe Codierung.

Support

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

