

AXIS A9210 Network I/O Relay Module

Funktionsweise

Das Gerät im Netzwerk ermitteln

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

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

- 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.
- Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Administratorkonto erstellen, on page 2*.

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter *Weboberfläche, on page 6*.

Administratorkonto erstellen

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

- Einen Benutzernamen eingeben.
- Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter, on page 3*.
- Geben Sie das Kennwort erneut ein.
- Stimmen Sie der Lizenzvereinbarung zu.
- Klicken Sie auf **Konto hinzufügen**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 45*.

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 45*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Übersicht über die Weboberfläche

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



Weboberfläche des Axis Geräts

Ihr Gerät konfigurieren

Einen I/O-Port konfigurieren

1. Wechseln Sie zu **Device > I/Os and relays > AXIS A9210 > I/Os** (Gerät > I/Os und Relais > AXIS A9210 > I/Os).
2. Klicken Sie auf  , um die Einstellungen des I/O-Ports zu erweitern.
3. Benennen Sie den Port um.
4. Konfigurieren Sie den Normalzustand. Klicken Sie auf  für einen geöffneten Schaltkreis oder auf  für einen geschlossenen Schaltkreis.
5. So konfigurieren Sie den I/O-Port als Eingang:
 - 5.1. Klicken Sie unter **Direction (Richtung)** auf .
 - 5.2. Um den Eingangsstatus zu überwachen, schalten Sie **Supervised (Überwacht)** ein. Siehe *Überwachte Eingänge, on page 43*.

Hinweis

Bei APIs funktionieren die überwachten I/O-Ports anders als die überwachten Eingangsanschlüsse. Weitere Informationen finden Sie in der *VAPIX®-Bibliothek*.

6. So konfigurieren Sie den I/O-Port als Ausgang:
 - 6.1. Klicken Sie unter **Direction (Richtung)** auf .
 - 6.2. Um die URLs zum Aktivieren und Deaktivieren von verbundenen Geräten anzuzeigen, rufen Sie **Toggle port URL (Port-URL umschalten)** auf.

Relais konfigurieren

1. Wechseln Sie zu **Device > I/Os and relays > AXIS A9210 > Relays** (Gerät > I/Os und Relais > AXIS A9210 > Relais).
2. Klicken Sie auf  , um die Relaiseinstellungen zu erweitern.
3. Schalten Sie **Relay (Relais)** ein.
4. Benennen Sie das Relais um.
5. Um die URLs zum Aktivieren und Deaktivieren des Relais anzuzeigen, rufen Sie **Toggle port URL (Port-URL umschalten)** auf.

Einrichten von Regeln für Ereignisse

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

Lösen Sie eine Aktion aus

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

Hinweis

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

Weboberfläche

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

Hinweis

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

 Hauptmenü anzeigen oder ausblenden.

 Zugriff auf die Versionshinweise.

 Auf die Hilfe zum Produkt zugreifen.

 Ändern Sie die Sprache.

 Helles oder dunkles Design einstellen.

  Das Benutzermenü enthält:

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

⋮

Das Kontextmenü enthält:

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

Status

Geräteinformationen

Zeigt Informationen zum Gerät an, einschließlich AXIS OS-Version und Seriennummer.

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

Zeitsynchronisierungsstatus

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

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

Sicherheit

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

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

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.

Gerät

E/As und Relais

AXIS A9210

E/A

Eingang

- **Name:** Bearbeiten Sie den Text, um den Port umzubenennen.
- **Richtung:** Zeigt an, dass es sich um einen Eingangsanschluss handelt.
- **Normal state (Normalzustand):** Klicken Sie auf  für einen offenen Schaltkreis und auf  für einen geschlossenen Schaltkreis.
- **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.
 - Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 KΩ)** und **seriellem Widerstand (4,7 KΩ)**.
 - Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.

Ausgang: Schalten Sie diese Funktion ein, um verbundene Geräte zu aktivieren.

- **Name:** Bearbeiten Sie den Text, um den Port umzubenennen.
- **Richtung:** Zeigt an, dass es sich um einen Ausgangsanschluss handelt.
- **Normal state (Normalzustand):** Klicken Sie auf  für einen offenen Schaltkreis und auf  für einen geschlossenen Schaltkreis.
- **Toggle port URL (Port-URL umschalten):** Zeigt die URLs zum Aktivieren und Deaktivieren von verbundenen Geräten über die VAPIX® Application Programming Interface an.

I/O (E/A): Schalten Sie diese Funktion ein, um verbundene Geräte zu aktivieren, wenn der Port als Ausgang konfiguriert ist.

- **Name:** Bearbeiten Sie den Text, um den Port umzubenennen.
- **Richtung:** Klicken Sie auf  oder , um sie als Eingang oder Ausgang zu konfigurieren.
- **Normal state (Normalzustand):** Klicken Sie auf  für einen offenen Schaltkreis und auf  für einen geschlossenen Schaltkreis.
- **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. Sie wird nur angezeigt, wenn der Port als Eingang konfiguriert ist.
 - Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 KΩ)** und **seriellem Widerstand (4,7 KΩ)**.
 - Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.
- **Toggle port URL (Port-URL umschalten):** Zeigt die URLs zum Aktivieren und Deaktivieren von verbundenen Geräten über die VAPIX® Application Programming Interface an. Sie wird nur angezeigt, wenn der Port als Ausgang konfiguriert ist.

Relais

- **Relay (Relais):** Schalten Sie das Relais ein oder aus.
- **Name:** Bearbeiten Sie den Text, um das Relais umzubenennen.
- **Richtung:** Zeigt an, dass es sich um ein Ausgangsrelais handelt.
- **Toggle port URL (Port-URL umschalten):** Zeigt die URLs zum Aktivieren und Deaktivieren des Relais über die VAPIX® Application Programming Interface an.

AXIS A9910

Sie können bis zu 16 AXIS A9910 an einen AXIS A9210 anschließen, um 128 E/A, 64 Relais und 64 Modbus-Sensoren zu unterstützen. Die maximale zulässige Entfernung zwischen dem AXIS A9210 und dem letzten AXIS A9910 beträgt 1000 m.

 **Verschlüsselungsschlüssel hinzufügen:** Klicken Sie hier, um einen Verschlüsselungsschlüssel für die verschlüsselte Kommunikation zu einrichten.

 **AXIS A9910 hinzufügen:** Klicken Sie hier, um ein Erweiterungsmodul hinzuzufügen.

- **Name:** Bearbeiten Sie den Text, um das Erweiterungsmodul umzubenennen.
- **Adresse:** Zeigt die Verbindungsadresse des Erweiterungsmoduls an.
- **Device software version (Geräte-Softwareversion):** Zeigt die aktuelle Softwareversion des Erweiterungsmoduls an.
- **Upgrade device software (Gerätesoftware aktualisieren):** Klicken Sie hier, um die Software des Erweiterungsmoduls zu aktualisieren. Sie können wählen, ob Sie eine Aktualisierung auf die mit der Tür-Steuerung mitgelieferte Version durchführen oder eine Version Ihrer Wahl hochladen möchten.

E/A

I/O (E/A): Schalten Sie diese Funktion ein, um verbundene Geräte zu aktivieren, wenn der Port als Ausgang konfiguriert ist.

- **Name:** Bearbeiten Sie den Text, um den Port umzubenennen.
- **Richtung:** Klicken Sie auf  oder , um sie als Eingang oder Ausgang zu konfigurieren.
- **Normal state (Normalzustand):** Klicken Sie auf  für einen offenen Schaltkreis und auf  für einen geschlossenen Schaltkreis.
- **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. Sie wird nur angezeigt, wenn der Port als Eingang konfiguriert ist.
 - Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 KΩ)** und **seriellem Widerstand (4,7 KΩ)**.
 - Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.
- **Toggle port URL (Port-URL umschalten):** Zeigt die URLs zum Aktivieren und Deaktivieren von verbundenen Geräten über die VAPIX® Application Programming Interface an. Sie wird nur angezeigt, wenn der Port als Ausgang konfiguriert ist.

Relais

- **Relay (Relais):** Schalten Sie das Relais ein oder aus.
- **Name:** Bearbeiten Sie den Text, um das Relais umzubenennen.
- **Richtung:** Zeigt an, dass es sich um ein Ausgangsrelais handelt.
- **Toggle port URL (Port-URL umschalten):** Zeigt die URLs zum Aktivieren und Deaktivieren des Relais über die VAPIX® Application Programming Interface an.

Alarme

Gerätebewegung: Schalten Sie diese Option ein, um einen Alarm in Ihrem System auszulösen, wenn eine Bewegung des Geräts erkannt wird.

Gehäuse geöffnet  : Aktivieren Sie diese Option, um einen Alarm in Ihrem System auszulösen, wenn ein geöffnetes Gehäuse der Tür-Steuerung erkannt wird. Deaktivieren Sie diese Einstellung für Barebone-Türsteuerungen.

Externe Manipulation  : Aktivieren Sie diese Option, um bei erkannter externer Manipulation einen Alarm in Ihrem System auszulösen. Zum Beispiel, wenn jemand den externen Schrank öffnet oder schließt.

- **Überwacher Eingang**  : Aktivieren Sie den Eingangsstatus des Monitors und konfigurieren Sie die Abschlusswiderstände.
 - Um die parallele erste Verbindung zu verwenden, wählen Sie **Parallele erste Verbindung mit parallelem Widerstand (22 KΩ)** und **seriellem Widerstand (4,7 KΩ)**.
 - Wählen Sie für eine Serienschaltung Sie **Serienschaltung** und in der Auswahlliste **Widerstandswerte** einen Widerstandswert.

Peripheriegeräte

Sensoren

Zeigt eine Übersicht Ihrer an AXIS A9210 angeschlossenen Sensoren an. Sie können bis zu 8 Modbus-Sensoren direkt an den RS485-Port anschließen oder auf 16 AXIS A9910 erweitern, um 64 Modbus-Sensoren an einem einzigen AXIS A9210 zu betreiben.



Hinzufügen: Klicken Sie auf diese Option, um einen Sensor hinzuzufügen.

Name: Geben Sie den Name des Sensors ein.

Sensor: Wählen Sie das Gerät aus, an dem der Sensor angeschlossen ist.

RS485 port (RS485-Port): Wählen Sie den Port aus, an dem der Sensor angeschlossen ist.

Adresse: Geben Sie die Adresse des Sensors ein. Bei Verwendung von Multidrop geben Sie bitte die eindeutige Adresse zwischen 1 und 247 ein.

Typ:

- Wählen Sie **Custom (Benutzerdefiniert)** aus.
 - **Export template (Vorlage exportieren):** Klicken Sie auf diese Option, um eine JSON-Datei herunterzuladen. Sie können die Datei bearbeiten und später auf das Gerät hochladen.
 - **Select configuration file (Konfigurationsdatei wählen):** Klicken Sie hier, um eine Konfigurationsdatei auszuwählen oder durch Ziehen und Ablegen einzufügen. Sie können die Konfigurationsdatei bearbeiten, kopieren, herunterladen oder ausdrucken.
- Wählen Sie **Hugo** oder **Tibbo** aus.
 - **Read data (Daten auslesen):** Legen Sie fest, wie häufig Daten aus dem Sensor ausgelesen werden sollen.
 - **Thresholds (Grenzwerte):** Legen Sie Grenzwerte für verfügbare Sensordaten wie Temperatur, Luftfeuchtigkeit, Taupunkt, Luftdruck oder Helligkeit fest.

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

In der Liste der Sensoren:

- **Vor- und Nachname:** Bearbeiten Sie den Text, um den Sensor umzubenennen.
- **Device/Port (Gerät/Port):** Die Modbus-ID und die Nummer des Ports, an dem der Sensor angeschlossen ist.
- **Type (Typ):** Der Typ der Messung oder Funktion, die der Sensor ausführt, wie Messung der Temperatur, Luftfeuchtigkeit oder Helligkeit.
- **Modell:** Der Modellname des Sensors.
- **Last value (Letzter Wert):** Der Messwert, der zuletzt aus dem Sensor ausgelesen wurde.
- **Last event (Letztes Ereignis):** Der Grund für das zuletzt ausgelöste Ereignis, wie zum Beispiel die Über- oder Unterschreitung des festgelegten Grenzwerts für den ausgewählten Parameter.
- **Status:** Hier wird angezeigt, ob der Sensor derzeit online oder offline ist.

Apps



App hinzufügen: Installieren einer neuen App.

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



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



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

Hinweis

Die Leistung des Geräts kann beeinträchtigt werden, wenn mehrere Apps gleichzeitig ausgeführt werden. Verwenden Sie den Schalter neben dem App-Namen, um diese zu starten oder anzuhalten.

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



Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

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

System

Uhrzeit und Ort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

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

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

- **DHCP:** Übernimmt die Zeitzone des DHCP-Servers. Bevor Sie diese Option auswählen können, muss das Gerät mit einem DHCP-Server (v4 oder v6) verbunden werden. Wenn beide Versionen verfügbar sind, zieht das Gerät IANA gegenüber POSIX und DHCPv4 gegenüber DHCPv6 vor.
 - DHCPv4 verwendet Option 100 für POSIX-Zeitzone und Option 101 für IANA-Zeitzone.
 - DHCPv6 verwendet Option 41 für POSIX und Option 42 für IANA.
- **Manual (Manuell):** Wählen Sie in der Drop-Down-Liste eine Zeitzone aus.

Hinweis

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

Gerätestandort

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

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

Netzwerk

IPv4

Assign IPv4 automatically (IPv4 automatisch zuweisen): Wählen Sie die automatische IP-Zuweisung per IPv4 (DHCP) aus, damit das Netzwerk IP-Adresse, Subnetzmaske und Router automatisch zuweist und keine manuelle Konfiguration erforderlich ist. Wir empfehlen eine automatische Zuweisung der IP-Adresse (DHCP) für die meisten Netzwerke.

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

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

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

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

Hinweis

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

IPv6

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

Hostname

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

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

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

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

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

DNS-Server

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

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

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

Hinweis

Wenn DHCP deaktiviert ist, sind Funktionen, die auf einer automatischen Netzwerkkonfiguration basieren, wie z. B. Host-Name, DNS-Server, NTP usw., unter Umständen nicht mehr ausführbar.

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.

One-Click Cloud Connect

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

O3C zulassen:

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

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

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

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

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

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

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

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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



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

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



Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) ⓘ:

- **Trusted Execution Environment (SoC TEE):** Auswählen, um SoC TEE für einen sicheren Schlüsselspeicher zu verwenden.
- **Secure element (CC EAL6+, FIPS 140-3 Level 3) (Sicheres Element (CC EAL6+, FIPS 140-3 Stufe 3)) ⓘ:** Wählen Sie diese Option aus, um ein sicheres Element als sicheren Schlüsselspeicher zu verwenden.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 Level 2) ⓘ:** Wählen Sie diese Option aus, um TPM 2.0 für sicheren Schlüsselspeicher zu verwenden.

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Zertifikate

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

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

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

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

Clientzertifikat: Wählen Sie ein Clientzertifikat aus, um IEEE 802.1x zu verwenden. Der Authentifizierungsserver verwendet das Zertifikat zur Validierung der Identität des Clients.

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

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

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

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

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

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

Diese Einstellungen stehen nur zur Verfügung, wenn Sie **IEEE 802.1ae MACsec (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 Geräteebe-
festlegen.

Firewall

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

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

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

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

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

Rule type (Regeltyp):

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

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

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

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

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

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

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



Das Kontextmenü enthält:

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

Konten

Konten

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Bediener:** Hat Zugriff auf alle Einstellungen, außer:
 - Alle **System**-Einstellungen
- **Betrachter:** 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.

SSH-Konten

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

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Anmerkung: Geben Sie eine Anmerkung ein (optional).



Das Kontextmenü enthält:

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

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

OpenID-Konfiguration

Wichtig

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

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.



Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

Condition (Bedingung): Wählen Sie eine Bedingung aus der Liste aus. Eine Bedingung muss erfüllt sein, damit das Gerät eine Aktion ausführen kann. Wenn mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein. Informationen zu bestimmten Bedingungen finden Sie 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 Zielserver. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielserver eine Firewall eingerichtet ist.
- **HTTP**
 - **URL:** Die Netzwerkadresse des HTTP-Servers und das Skript, das die Anforderung bearbeiten wird, eingeben. Beispielsweise `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Benutzername):** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Password (Kennwort):** Geben Sie das Kennwort für die Anmeldung ein.
 - **Proxy:** Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTP-Server ein Proxyserver erforderlich ist.
- **HTTPS**
 - **URL:** Die Netzwerkadresse des HTTPS-Servers und das Skript, das die Anforderung bearbeiten wird, eingeben. Beispielsweise `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Server-Zertifikate validieren):** Wählen Sie diese Option, um zu überprüfen, ob das Zertifikat von HTTPS-Server erstellt wurde.
 - **Username (Benutzername):** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Password (Kennwort):** Geben Sie das Kennwort für die Anmeldung ein.
 - **Proxy:** Aktivieren Sie diese Option und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTPS-Server ein Proxyserver erforderlich ist.
- **Netzwerk-Speicher** 

Darüber können Sie einen Netzwerk-Speicher wie NAS (Network Attached Storage) hinzufügen und als Empfänger für zu speichernde Dateien verwenden. Die Dateien werden im Format Matroska (MKV) gespeichert.

 - **Host:** Geben Sie die IP-Adresse oder den Host-Namen der Netzwerk-Speicher ein.
 - **Freigabe:** Den Namen der Freigabe beim Host eingeben.

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

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

Hinweis

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

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

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



Das Kontextmenü enthält:

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

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

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

Zeitschemata

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



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

Manuelle Auslöser

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

MQTT

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

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

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

ALPN

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

MQTT-Client

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

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

Broker

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

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

Port: Geben Sie die Portnummer ein.

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

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

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

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

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

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

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

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

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

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

Device topic prefix (Themenpräfix des Geräts): Wird in den Standardwerten für das Thema in der Verbindungsnachricht und der LWT-Nachricht auf der Registriertkarte **MQTT Client** und in den Veröffentlichungsbedingungen auf der Registriertkarte **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 condition (Bedingung einbeziehen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

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

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



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

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

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

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

MQTT-Abonnements



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

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

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

Abonnementart:

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

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

Protokolle

Protokolle und Berichte

Berichte

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

Protokolle

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

Netzwerk-Trace

Wichtig

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

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

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

Remote System Log

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



Server: Klicken Sie, um einen neuen Server hinzuzufügen.

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

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

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

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

Direktkonfiguration

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

Wartung

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 auf die Werkseinstellungen zurück. Anschließend müssen Sie die IP-Adresse zurücksetzen, um auf das Gerät zugreifen zu können.

Hinweis

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

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

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

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

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

Mehr erfahren

Analysefunktionen und Anwendungen

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

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

AXIS Door Monitoring

Diese Anwendung überwacht den Status eines Zugangs, zeigt an, ob er geöffnet oder geschlossen ist, und meldet, wenn er zu lange geöffnet bleibt. Ein mögliches Einsatzbeispiel ist eine Brandschutztür, die kein Schloss benötigt, aber über die Sie wissen müssen, ob sie geöffnet ist.

Ein regulärer Zugang verfügt über einen Türpositionssensor, ein REX-Gerät sowie Schlösser und Leser, was eine Tür-Steuerung erforderlich macht.

Ein überwachter Zugang benötigt lediglich einen Türpositionssensor und ein REX-Gerät und kann mithilfe eines Netzwerk-I/O-Relaismoduls überwacht werden. Jedes Netzwerk-I/O-Relaismodul kann mit bis zu fünf überwachten Zugängen verbunden werden.

Einschränkungen

Die Anwendung ist ausschließlich auf dem AXIS A9210 verfügbar. Das REX-Gerät kann nur an I/O 1 und I/O 2 angeschlossen werden. Eine Konfiguration des REX an I 3, I 4 oder I 5 ist nicht möglich.

Konfiguration von AXIS Door Monitoring

Bezeichnung	Beschreibung
Tür	Die Nummer des Zugangs.
DPS input (DPS-Eingang)	Der DPS-Eingang für den Zugang.
REX input (REX-Eingang)	Der REX-Eingang für den Zugang.
Door open too long time (sec) (Maximale zulässige Öffnungsdauer des Zugangs (s))	Die maximale zulässige Öffnungsdauer des Zugang in Sekunden.
Zugangszeit (s)	Die Dauer in Sekunden, für die der Zugang geöffnet bleiben soll, nachdem Zutritt gewährt wurde.
Status	Der Status des Zugangs.

Cybersicherheit

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

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

Axis Edge Vault

Axis Edge Vault stellt eine Hardware-basierte Cybersicherheitsplattform bereit, die das Axis Gerät schützt. Sie bietet Funktionen, die die Identität und Integrität des Geräts gewährleisten und Ihre vertraulichen Daten vor unbefugtem Zugriff schützen. Es sorgt für eine starke Grundlage kryptografischer Berechnungsmodule (Sicherheitselement und TPM) und SoC-Sicherheit (TEE und Secure Boot), die wir mit Expertise in Edge-Gerätesicherheit kombinieren.

Signiertes Betriebssystem

Signiertes OS wird vom Softwarehersteller implementiert, der das AXIS OS-Image mit einem privaten Schlüssel signiert. Wenn die Signatur an das Betriebssystem angefügt wurde, validiert das Gerät die Software vor der Installation. Wenn das Gerät feststellt, dass die Integrität der Software beeinträchtigt ist, wird die Aktualisierung von AXIS OS abgelehnt.

Sicheres Hochfahren

Sicheres Hochfahren ist ein Boot-Prozess, der aus einer ununterbrochenen Kette von kryptografisch validierter Software besteht, die im unveränderlichen Speicher (Boot-ROM) beginnt. Da sicheres Hochfahren auf der Verwendung von signiertem OS basiert, wird sichergestellt, dass ein Gerät nur mit autorisierter Software booten kann.

Sicherer Schlüsselspeicher

Der sichere Schlüsselspeicher ist eine manipulationssichere Umgebung für den Schutz privater Schlüssel und die sichere Ausführung kryptographischer Operationen. Verhindert unbefugte Zugriffe und böswillige Extraktion im Falle eines Sicherheitsverstoßes. Je nach Sicherheitsbedarf kann ein Axis Gerät einen oder mehrere kryptografische Berechnungsmodule haben, die einen durch die Hardware geschützten sicheren Schlüsselspeicher bereitstellen. Je nach Sicherheitsanforderungen kann ein Axis Gerät entweder über ein oder mehrere hardwarebasierte kryptografische Rechenmodule wie ein TPM 2.0 (Trusted Platform Module) oder ein sicheres Element und/oder eine vertrauenswürdige Ausführungsumgebung (Trusted Execution Environment, TEE) verfügen, die einen hardwaregeschützten sicheren Schlüsselspeicher bereitstellen. Darüber hinaus verfügen ausgewählte Axis Produkte über einen nach FIPS 140-2 Level 2 zertifizierten sicheren Schlüsselspeicher.

Axis Geräte-ID

Den Ursprung eines Gerätes überprüfen zu können, ist der Schlüssel zum Vertrauen in die Geräteidentität. In der Produktion wird Geräten mit Axis Edge Vault ein eindeutiges, von der Fabrik bereitgestelltes und IEEE 802.1AR-kompatibles Zertifikat für die Axis Geräte-ID zugewiesen. Dies funktioniert wie ein Reisepass und weist den Ursprung des Gerätes nach. Die Geräte-ID wird sicher und permanent als vom Axis Root-Zertifikat signiertes Zertifikat im sicheren Schlüsselspeicher aufbewahrt. Die Geräte-ID kann über die IT-Infrastruktur des Kunden für ein automatisiertes, sicheres Geräte-Onboarding und sichere Geräteidentifizierung genutzt werden.

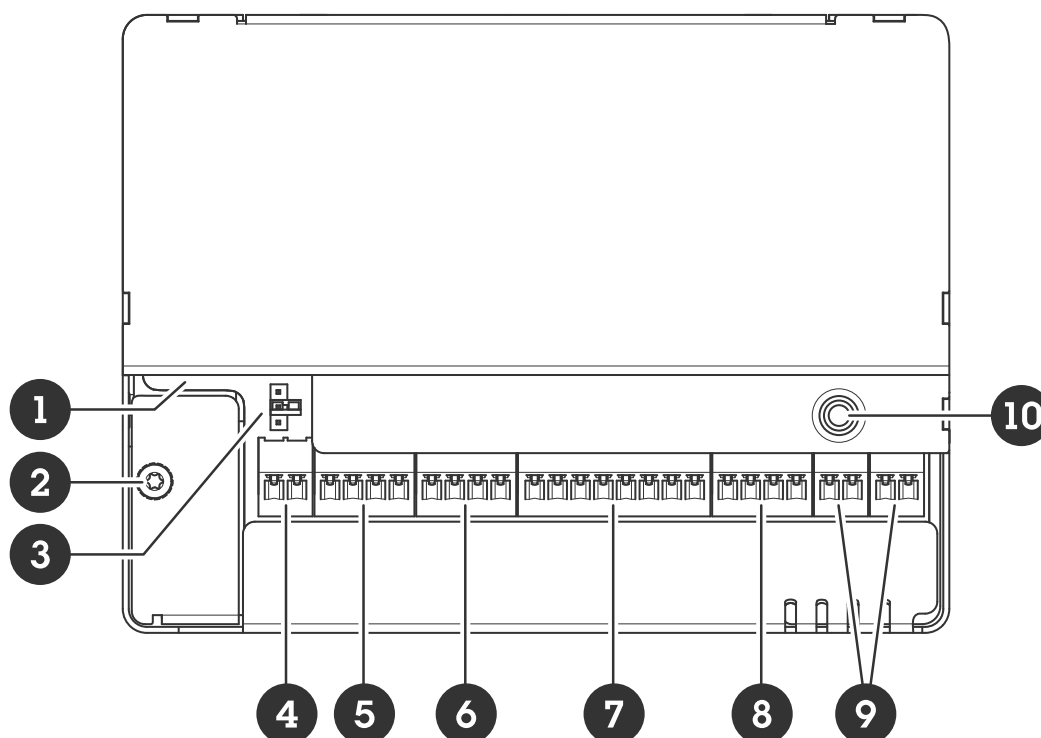
Verschlüsseltes Dateisystem

Der sichere Schlüsselspeicher verhindert das böswillige Herausschleusen von Informationen und Veränderungen der Konfiguration, indem es eine starke Verschlüsselung des Dateisystems erzwingt. So wird sichergestellt, dass keine im Dateisystem gespeicherten Daten extrahiert oder manipuliert werden können, wenn das Gerät nicht in Betrieb ist, unbefugte Zugriffe auf das Gerät erfolgen und/oder das Axis Gerät gestohlen wird. Das Read-Write-Dateisystem wird während des sicheren Systemstarts entschlüsselt und dem Axis Gerät zur Verwendung bereitgestellt.

Um mehr zu den Cybersicherheitsfunktionen von Axis Geräten zu erfahren, gehen Sie auf axis.com/learning/white-papers und suchen Sie nach Cybersicherheit.

Technische Daten

Produktübersicht



- 1 Netzwerk-Anschluss
- 2 Position Erdung
- 3 Relaisbrücke
- 4 Stromanschluss
- 5 Relaisanschluss
- 6 Steckverbinder Eingang 1
- 7 RS485 und E/A-Anschluss
- 8 E/A-Anschluss
- 9 Steckverbinder Eingang 2
- 10 Steuertaste

LED-Anzeigen

LED	Farbe	Anzeige
Status	Grün	Leuchtet bei Normalbetrieb grün.
	Gelb	Dauerhaft beim Hochfahren und beim Wiederherstellen von Einstellungen
	Rot	Blinkt langsam bei einem Aktualisierungsfehler.
Netzwerk	Grün	Dauerhaft bei Verbindung mit einem Netzwerk mit 100 MBit/s Blinkt bei Netzwerkaktivität.
	Gelb	Dauerhaft bei Verbindung mit einem 10 MBit/s-Netzwerk. Blinkt bei Netzwerkaktivität.
	Aus	Keine Netzwerk-Verbindung

Stromversorgung	Grün	Normalbetrieb
	Gelb	Blinkt während einer Firmware-Aktualisierung grün/orange.
Relay	Grün	Relais aktiv. ¹
	Aus	Relais nicht aktiv.

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 45*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Um eine Verbindung herzustellen, drücken Sie die Taste, lassen Sie sie los und warten Sie, bis die Status LED dreimal grün blinkt.

Anschlüsse

Netzwerk-Anschluss

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

UL: Power over Ethernet (PoE) muss ein Power over Ethernet IEEE 802.3 AF/802.3at Typ 1 Klasse 3 oder Power over Ethernet Plus (PoE+) IEEE 802.3at Typ 2 Klasse 4 Power Limited Injector sein, der 44 bis 57 V Gleichstrom, 15,4 W/30 W liefert. Power over Ethernet (PoE) wurde durch UL mit AXIS T8133 Midspan 30 W 1-Port bewertet.

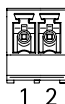
Strompriorität

Dieses Gerät kann entweder über PoE oder Gleichstromeingang mit Strom versorgt werden. Siehe *Netzwerk-Anschluss, on page 38* und *Stromanschluss, on page 38*.

- Wenn PoE und Gleichstrom vor dem Einschalten des Geräts verbunden sind, wird PoE für die Stromversorgung verwendet.
- PoE und Gleichstrom sind beide angeschlossen und die Stromversorgung geschieht derzeit über PoE. Bei Verlust von PoE wird das Gerät für die Stromversorgung ohne Neustart mit Gleichstrom verwendet.
- PoE und Gleichstrom sind beide angeschlossen und die Stromversorgung geschieht derzeit über Gleichstrom. Bei Verlust des Gleichstroms wird das Gerät neu gestartet und verwendet PoE für die Stromversorgung.
- Wenn Gleichstrom beim Start verwendet wird und PoE nach dem Start des Geräts angeschlossen wird, wird Gleichstrom für die Stromversorgung verwendet.
- Wenn PoE beim Start verwendet wird und Gleichstrom nach dem Start des Geräts angeschlossen wird, wird PoE für die Stromversorgung verwendet.

Stromanschluss

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



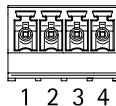
1. Aktives Relais wenn COM an NO angeschlossen.

Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromeingang	2	Stromversorgung des Geräts bei Nichtverwendung von Power over Ethernet. Hinweis: Dieser Kontakt kann nur für den Stromeingang verwendet werden.	12 V DC, max 36 W

UL: Die Gleichstromleistung muss je nach Anwendung über ein UL 603-gelistetes Netzteil mit entsprechenden Nennleistungen bereitgestellt werden.

Relaisanschluss

Ein vierpoliger Anschlussblock für Relais Typ C, der zum Beispiel ein Schloss oder eine Schnittstelle zu einem Tor steuert. Bei Verwendung mit einer induktiven Last wie etwa einem Schloss muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
NEIN	2	Schließer-Kontakt. Zum Anschluss von Relaisgeräten. Schalten Sie ein ausfallsicheres Schloss zwischen NO und DC-Masse an. Bei Nichtverwendung der Steckbrücken sind die zwei Relaiskontakte galvanisch vom restlichen Schaltkreis getrennt.	Max. Strom = 2 A Max. Spannung = 30 V DC
COM	3	Gemeinsam	
NC	4	Öffner-Kontakt. Zum Anschluss von Relaisgeräten. Schalten Sie ein ausfallsicheres Schloss zwischen NC und DC-Masse an. Bei Nichtverwendung der Steckbrücken sind die zwei Relaiskontakte galvanisch vom restlichen Schaltkreis getrennt.	

Relaisstrombrücke

Die Relaisstrombrücke überbrückt 12 V Gleichstrom oder 24 V Gleichstrom und den Relaiskontakt COM.

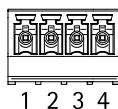
Mit ihr kann ein Schloss an die Kontakte GND und NO oder GND und NC geschaltet werden.

Stromquelle	Maximale Leistung bei 12 V Gleichstrom	Maximale Leistung bei 24 V Gleichstrom
Gleichstrom IN	2000 mA	1000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Steckverbinder Eingang 1

Ein 4-poliger Anschlussblock für den Eingang.

Er unterstützt das Überwachen mit Abschlusswiderständen. Bei Unterbrechen der Verbindung wird ein Alarm ausgelöst. Um überwachte Eingänge zu verwenden, Abschlusswiderstände anbringen. Das Anschlussschaltdiagramm für überwachte Eingänge beachten. Siehe *Überwachte Eingänge*, on page 43.



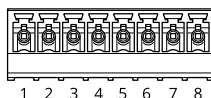
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1, 3		0 V Gleichstrom
Eingang	2, 4	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 oder 3 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom

Wichtig

Das Kabel darf bis zu 200 m (656 ft) lang sein, wenn es folgende Anforderungen erfüllt: AWG 24.

RS485 und E/A-Anschluss

Ein 8-poliger Anschlussblock mit 4-poligem RS485- und 4-poligem I/O-Stecker.



RS485

Funktion	Kontakt	Hinweis	Technische Daten
Erdung Gleichstrom (GND)	1		0 V Gleichstrom
Gleichstromausgang (+12 V)	2	Versorgt Zusatzgeräte, z. B. Modbus-Sensoren, mit Strom.	12 V Gleichstrom, max 200 mA
A	3		
B	4		

I/O

Funktion	Kontakt	Hinweis	Technische Daten
Digitalausgang	5	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
Digitalausgang	6	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
Eingang	7	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
Digitalausgang	8	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

Wichtig

- Die zulässige Kabellänge für RS485 beträgt bis zu 1000 m (3281 ft), wenn die folgenden Kabelanforderungen erfüllt sind: 1 Twisted Pair mit Schirmung, AWG 24 und Impedanz von 120 Ohm.
- Für E/A darf das Kabel bis zu 200 m (656 ft) lang sein.

E/A-Anschluss

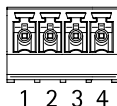
Über den Zusatzanschluss wird Zusatzausrüstung für Funktionen wie Manipulationsalarm, Bewegungserkennung, Ereignisauslösung, Alarmbenachrichtigung und andere angeschlossen. Abgesehen vom Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) verfügt der Zusatzanschluss über eine Schnittstelle zum:

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

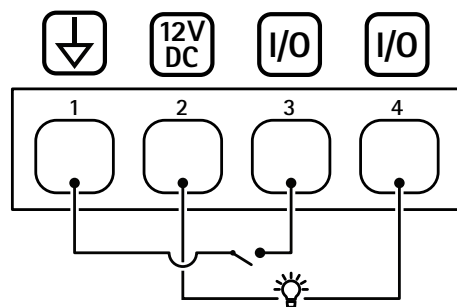
Überwachter Eingang – Ermöglicht das Erfassen von Manipulation an einem digitalen Eingang.

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

4-poliger Anschlussblock



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Kann für die Stromversorgung von Zusatzausrüstung verwendet werden. Hinweis: Dieser Kontakt kann nur als Stromausgang verwendet werden.	12 V Gleichstrom Maximale Last = 50 mA insgesamt
Konfigurierbar (Ein- oder Ausgang)	3–4	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen. Um überwachten Eingang zu nutzen, Abschlusswiderstände anschließen. Informationen zum Anschließen der Widerstände bietet der Schaltplan.	0 bis max. 30 V Gleichstrom
		Digitaler Ausgang – Interne Verbindung mit Kontakt 1 (Erdschluss Gleichstrom), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last, z. B. einem Relais, eine Diode parallel zur Last anschließen, um vor Spannungstransienten zu schützen. Die E/As können eine externe Last von 12 V DC, 50 mA (kombiniert maximal) treiben, wenn der interne 12 V-Gleichspannungsausgang (Pin 2) verwendet wird. Bei der Verwendung von Open-Drain-Anschlüssen in Kombination mit einer externen Stromversorgung können die E/As eine Gleichstromversorgung von jeweils 0 bis 30 V DC, 100 mA bereitstellen.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

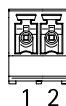


- 1 Erdung Gleichstrom
- 2 Gleichstromausgang 12 V
- 3 E/A als Eingang konfiguriert
- 4 E/A als Ausgang konfiguriert

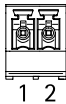
Steckverbinder Eingang 2

Zwei zweipolige Anschlussblöcke für externe Geräte wie Glasbruchmelder oder Feuermelder.

UL: Der Steckverbinder wurde nicht für die Verwendung als Einbruch- oder Feueralarm von UL bewertet.



Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Eingang	2	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom



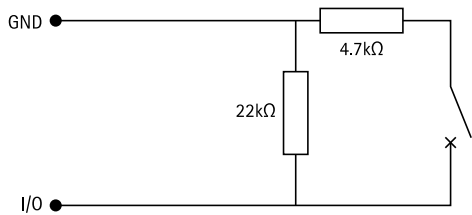
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Eingang	2	Digitaler Eingang oder überwachter Eingang – Zum Aktivieren an Kontakt 1 anschließen, zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom

Überwachte Eingänge

Um überwachte Eingänge zu verwenden, die Abschlusswiderstände wie im Schaltbild unten dargestellt anschließen.

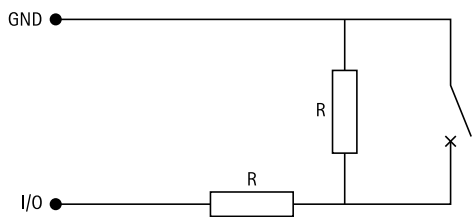
Paralleler Anschluss hat Vorrang

Die Widerstandswerte müssen 4,7 kΩ und 22 kΩ betragen.



Serielle erste Verbindung

Die Widerstandswerte müssen identisch sein und die möglichen Werte sind 1 kΩ, 2.2 kΩ, 4.7 kΩ und 10 kΩ, 1 %, ¼ Watt (Standard).



Hinweis

Es wird empfohlen, verdrehte und geschirmte Kabel zu verwenden. Die Abschirmung an 0 V Gleichstrom anschließen.

Status	Beschreibung
Offen	Der überwachte Schalter befindet sich im offenen Modus.
Geschlossen	Der überwachte Schalter befindet sich im geschlossenen Modus.

Kurzschluss	Das I/O-Kabel oder das Kabel für die Eingänge 1–5 ist an GND kurzgeschlossen.
Schneiden	Das I/O-Kabel oder das Kabel für die Eingänge 1–5 ist unterbrochen und es ist kein Strompfad zu GND vorhanden.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

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

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Drücken und halten Sie die Steuertaste, um das Gerät wieder einzuschalten. Siehe *Produktübersicht*, on page 37.
3. Halten Sie die Steuertaste 25 Sekunden gedrückt, bis die LED-Statusanzeige zum zweiten Mal gelb leuchtet.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
 - Geräte mit AXIS OS 12.0 oder höher: Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
 - Geräte mit AXIS OS 11.11 oder niedriger: 192.168.0.90/24
5. Mithilfe der Softwaretools für das Installieren und Verwalten, IP-Adressen zuweisen, das Kennwort festlegen und auf das Produkt zugreifen.

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

Optionen für AXIS OS

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

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

Aktuelle AXIS OS-Version überprüfen

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

So überprüfen Sie die aktuelle AXIS OS-Version:

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

AXIS OS aktualisieren

Wichtig

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

Hinweis

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

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

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

Probleme nach der AXIS OS-Aktualisierung

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

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

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

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

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

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 45*.

Die IP-Adresse wurde von DHCP geändert

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

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

Zertifikatfehler beim Verwenden von IEEE 802.1X

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

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 2*.

Externer Zugriff auf das Gerät ist nicht möglich

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

- AXIS Camera Station Pro: Kostenlose 90-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

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

Probleme mit MQTT

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

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

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

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

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

Support

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

T10202445_de

2026-01 (M5.5)

© 2023 Axis Communications AB