AXIS S4000

Benutzerhandbuch

Über das Gerät

Der AXIS S4000 Rack Recorder ist ein Netzwerk-Videorecorder mit für Sicherheitsanwendungen geeigneten Festplatten. Außerdem ist ein USB 3.0-Port zum einfachen Export von Videodateien vorhanden. Der Rekorder ist in drei Modellen erhältlich – 8 TB, 16 TB und 32 TB.

Funktionsweise

Zugriff auf Ihr Gerät

Das Gerät im Netzwerk ermitteln

Ermitteln Sie mit AXIS IP Utility und AXIS Device Manager Extend die Axis Geräte im Netzwerk und weisen Sie ihnen unter Windows® IP-Adressen zu. Beide Anwendungen sind kostenlos und können von *axis.com/support* heruntergeladen werden.

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

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

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

Administratorkonto erstellen

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

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

Wichtig

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

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

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

Übersicht über die Weboberfläche

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

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

Weboberfläche des Axis Geräts

Erste Schritte mit AXIS Camera Station Edge

Hinweis

Für das Einrichten und Verwalten des Systems ist ein Internetzugang erforderlich.

1.
2.
3.
4.
5.

Nach Abschluss der Installation:

- Alle Axis Geräte im System verfügen über die aktuelle AXIS OS.
- Alle Geräte haben ein Kennwort.
- Die Aufzeichnung mit den Standardeinstellungen ist aktiv.
- Sie können den Fernzugriff verwenden.

Ein MyAxis-Konto einrichten

1. Ein **My Axis**-Konto wird unter *axis.com/my-axis/login* eingerichtet.
2. Wählen Sie eine der Multi-Faktor-Authentifizierungsmethoden (MFA) **Authenticator App (TOTP)** oder **Email** und folgen Sie den Anweisungen auf dem Bildschirm. MFA ist ein Sicherheitssystem, das eine weitere Verifizierungsebene hinzufügt, um die Identität des Benutzers sicherzustellen.

Die Hardware installieren

1. Die Kamerahardware installieren.
2. Schließen Sie den Rekorder über den LAN-Anschluss an Ihr Netzwerk an.
3. Verbinden Sie die Kameras mit einem externen PoE-Switch.
4. Den Computer an das Netzwerk des Rekorders anschließen.
5. Schließen Sie die Stromversorgung an den Rekorder an.

Wichtig

Sie müssen zuerst das Netzkabel an den Rekorder und dann das Netzkabel an die Steckdose anschließen.

6. Warten Sie einige Minuten, bis der Rekorder und die Kameras hochgefahren sind, bevor Sie fortfahren.

⚠ VORSICHT

Um Überhitzung zu vermeiden, sicherstellen, dass zwischen dem Rekorder und anderen Objekten genügend Raum für eine ausreichende Belüftung vorhanden ist.

AXIS Camera Station Edge installieren

1. Rufen Sie *axis.com/products/axis-camera-station-edge* auf und klicken Sie auf **Download**.
2. Öffnen Sie die Setup-Datei und folgen Sie dem Setup-Assistenten.
3. Melden Sie sich mit Ihrem *MyAxis-Konto* an.

Standort erstellen

1. Starten Sie AXIS Camera Station Edge.
2. Melden Sie sich mit Ihrem *MyAxis-Konto* an.
3. Auf **Create new site** (Neuen Standort erstellen) klicken und dem Standort einen Namen geben.
4. Klicken Sie auf **Next (Weiter)**.
5. Die dem Standort hinzuzufügenden Geräte auswählen.
6. Klicken Sie auf **Next (Weiter)**.
7. Speicher auswählen.
8. Klicken Sie auf **Next (Weiter)**.
9. Klicken Sie auf **Install (Installieren)**, und warten Sie das Konfigurieren der Geräte durch AXIS Camera Station Edge ab.
   Das Konfigurieren kann einige Minuten in Anspruch nehmen.

Nach Abschluss der Installation:

- Alle Axis Geräte im System verfügen über die aktuelle AXIS OS.
- Alle Geräte haben ein Kennwort.
- Die Aufzeichnung mit den Standardeinstellungen ist aktiv.
- Sie können den Fernzugriff verwenden.

Installation der Mobile App

Für Android

Klicken Sie auf *Herunterladen* oder scannen Sie den folgenden QR-Code®.

Für iOS

Klicken Sie auf *Herunterladen* oder scannen Sie den folgenden QR-Code.

Öffnen Sie die mobile App AXIS Camera Station Edge und melden Sie sich mit Ihren Axis Anmeldedaten an.

Wenn Sie kein MyAxis-Konto haben, können Sie *axis.com/my-axis* aufrufen, um ein neues Konto zu registrieren.

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

Erste Schritte mit AXIS Camera Station Pro

Rekorder hinzufügen

Hinweis

AXIS Camera Station entfernt Aufzeichnungen von allen vorherigen Systemen, wenn Sie den Rekorder zu einem neuen System hinzufügen.

1. **Konfiguration > Geräte > Geräte hinzufügen** aufrufen.
2. Wählen Sie Ihren Rekorder aus der Liste und klicken Sie auf **Hinzufügen**. Ist Ihr Rekorder nicht aufgeführt, suchen Sie über die **Manuelle Suche** manuell danach.
3. Wählen Sie die Standardeinstellungen und klicken Sie auf **Weiter**.
4. Legen Sie Ihr Kennwort für die Speicherverschlüsselung fest. Klicken Sie auf **Next (Weiter)**. Dieses Kennwort ist erforderlich, um auf den Rekorder von außerhalb des AXIS Camera Station zugreifen zu können oder wenn der Rekorder über die Weboberfläche des Geräts auf die Werkseinstellungen zurückgesetzt wird.
5. Gehen Sie zu **Konfiguration > Geräte > Weitere Geräte** überprüfen Sie, ob der Rekorder hinzugefügt wurde.

6. Rufen Sie **Configuration > Storage > Management (Konfiguration > Speicher > Verwaltung)** auf und überprüfen Sie, ob der Rekorder zur Speicherliste hinzugefügt wurde.

Hinzufügen von Geräten und Auswahl des Rekorders als Aufzeichnungsspeicher

1. **Konfiguration > Geräte > Geräte hinzufügen** aufrufen.
2. Wählen Sie Ihre Geräte aus der Liste und klicken Sie auf **Hinzufügen**. Falls Ihre Geräte nicht aufgeführt sind, suchen Sie diese manuell mithilfe der **Manuellen Suche**.
3. Wählen Sie die Standardeinstellungen und klicken Sie auf **Weiter**.
4. Wählen Sie den Rekorder manuell aus der Auswahlliste **Recording storage (Aufzeichnungsspeicher)** aus und klicken Sie auf **Install (Installieren)**.

Hinweis

Der Rekorder wird nicht automatisch als Aufzeichnungsspeicher ausgewählt, wenn Sie **Automatic (Automatisch)** wählen.

5. **Konfiguration > Speicher > Auswahl** aufrufen. Klicken Sie auf Ihre Geräte und überprüfen Sie, ob beim Aufzeichnungsspeicher der Rekorder angegeben ist.

Aufzeichnungen konfigurieren

1. Gehen Sie zu **Konfiguration > Speicher >Auswahl** und wählen Sie Ihr Gerät.
2. Konfigurieren Sie die **Retention time (Aufbewahrungszeit)**.
   - Wählen Sie **Unbeschränkte** Aufbewahrungszeit, um die Aufzeichnungen zu speichern, bis der Speicher voll ist.
   - Wählen Sie **Begrenzte** Aufbewahrungszeit und die Anzahl der Tage, für die die Aufzeichnung gespeichert werden soll.
3. Klicken Sie auf **Anwenden**.

Hinweis

Fallback-Aufzeichnung ist als Standard aktiviert, um die Aufzeichnungen auf dem Rekorder zu speichern, wenn die Verbindung von AXIS Camera Station zum Rekorder verloren geht. Siehe *Fallback recording (Fallback-Aufzeichnung)*.

Ihr Gerät konfigurieren

Die RAID-Ebene ändern

⚠ VORSICHT

Durch Ändern des RAID-Levels wird das Dateisystem neu formatiert und alle Daten werden von Ihren Festplatten gelöscht.

1. Wechseln Sie auf der Weboberfläche des Geräts zu **System > Storage (System > Speicher)**.
2. Unter **Tools (Werkzeuge)**, wählen Sie **Change RAID level (RAID-Level ändern)** und klicken Sie auf **Use tool (Werkzeug verwenden)**.
3. Ein RAID-Level wählen und **Next (Weiter)** anklicken.
4. Wählen Sie **Encrypt the disk (Verschlüsseln der Festplatte)** und geben Sie Ihr Passwort ein. Klicken Sie auf **Next (Weiter)**.
5. **Yes (Ja)** anklicken
6. Die Statusmeldung erscheint in der oberen rechten Ecke. Warten Sie, bis der Vorgang abgeschlossen ist und `RAID configured` vor dem Schließen der Seite angezeigt wird.

Festplattenlaufwerk ersetzen

Hinweis

Zur Vermeidung elektrostatischer Entladungen sollte bei Arbeiten an innenliegenden Systemkomponenten stets eine Antistatikmatte und ein Antistatikband verwendet werden.

1. Lösen Sie die Schrauben links und rechts an der Blende und entfernen Sie die Blende.
2. Suchen Sie die defekte Festplatte, die durch eine rote LED angezeigt wird.
   Bei einem RAID-Fehler leuchten alle LEDs rot. Um die defekte Festplatte zu identifizieren, gehen Sie zur Weboberfläche des Geräts und gehen Sie zu **System > Storage > Hard drive status (System > Speicher > Festplattenstatus)**.
3. Lösen Sie die Schraube für den Festplattenschlitten (T10).
4. Ziehen Sie den Festplattenschlitten aus dem Festplattenschacht.
5. Lösen Sie die vier Schrauben für die Festplatte (T8).
6. Nehmen Sie die Festplatte aus dem Festplattenschlitten.
7. Setzen Sie eine neue Festplatte in den Festplattenschlitten ein.
8. Befestigen Sie die vier Schrauben für die Festplatte.
9. Setzen Sie den Festplattenschlitten vollständig in den Festplattenschacht ein und schieben Sie ihn hinein.
10. Ziehen Sie die Schraube für den Festplattenschlitten fest. Warten Sie, bis die LED grün leuchtet.
11. Bringen Sie die Blende an und ziehen Sie die Schrauben links und rechts an der Blende fest.

Neues RAID erstellen

⚠ VORSICHT

Nur im Falle eines RAID-Ausfalls erstellen Sie ein neues RAID. Beim Erstellen eines neuen RAID werden alle Daten von Ihren Festplatten gelöscht.

1. Ersetzen Sie die defekten Festplatten. Siehe .
2. Konfigurieren Sie das RAID. Siehe .
3. Konfigurieren Sie Aufnahmen in Ihrem Videomanagementsystem. Siehe und .

Einen harten Reset auf einem Rekorder durchführen

Wichtig

Den eingeschalteten Rekorder sehr vorsichtig bewegen. Abrupte Bewegungen oder Stöße können die Festplatte beschädigen.

Hinweis

- Beim Zurücksetzen werden alle Einstellungen einschließlich der IP-Adresse auf die Werkseinstellungen zurückgesetzt.
- Ihre Aufzeichnungen sind vom Zurücksetzen nicht betroffen.

1. Ausschalten des Rekorders:
   Halten Sie die Netztaste an der Rückseite des Rekorders vier bis fünf Sekunden gedrückt, bis ein Signalton ertönt.
2. Warten Sie, bis der Rekorder abgeschaltet hat.
3. Drücken und halten Sie die Steuerungstaste gedrückt. Drücken Sie den Netzschalter und lassen Sie ihn wieder los, um den Rekorder zu starten. Lassen Sie die Steuertaste nach 15–30 Sekunden los wenn die LED-Anzeige gelb blinkt.
4. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, verwendet das Gerät eine IP-Adresse aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16).
5. Wenn Ihre Festplatte verschlüsselt ist, muss sie nach dem Zurücksetzen des Rekorders manuell montiert werden:
   5.1. Rufen Sie die Weboberfläche des Geräts auf.
   5.2. Wechseln Sie zu **System** > **Storage (Speicher)**, und klicken Sie auf **Mount (Laden)**.
   5.3. Geben Sie das Verschlüsselungspasswort ein, das beim Verschlüsseln der Festplatte verwendet wird.

Weboberfläche

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

Hinweis

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

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Ändern Sie die Sprache.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

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

Das Kontextmenü enthält:

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

Status

Geräteinformationen

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

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

Zeitsynchronisierungsstatus

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

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

Sicherheit

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

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

Speicherung

Zeigt den Speicherstatus und Informationen an, einschließlich freiem Speicherplatz und Festplattentemperatur.

Storage settings (Speichereinstellungen): Klicken Sie darauf, um zur Seite Integrierter Speicher zu wechseln, auf der Sie die Einstellungen ändern können.

Laufende Aufzeichnungen

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

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

Anzeige des Speicherorts der Aufzeichnung.

Verbundene Clients

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

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

Aufzeichnungen

Die Aufzeichnung wiedergeben.

Abspielen der Aufzeichnung anhalten.

Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

Exportbereich festlegen: Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten.

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

Klicken Sie auf , um eine Aufzeichnung zu löschen.

Exportieren: Exportieren der ganzen Aufzeichnung oder eines Teils davon.

Klicken Sie darauf, um die Aufzeichnungen zu filtern.

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

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

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

Ereignis: Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Speicher: Zeigt Aufzeichnungen nach Speichertyp.

Apps

App hinzufügen: Installieren einer neuen App.

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

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

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

Hinweis

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

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

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

Das Kontextmenü kann je nachdem die folgenden Optionen enthalten:

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

System

Uhrzeit und Ort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server))**: Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
  - **Manual NTS KE servers (Manuelle NTS-KE-Server)**: Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
  - **Trusted NTS KE CA certificates (Vertrauenswürdige NTS KE CA-Zertifikate)**: Wählen Sie die vertrauenswürdigen CA-Zertifikate aus, die für die sichere NTS KE-Zeitsynchronisierung verwendet werden sollen, oder 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 verbunden werden.
- **Manual (Manuell)**: Wählen Sie in der Drop-Down-Liste eine Zeitzone aus.

Hinweis

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

Netzwerk

IPv4

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

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

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

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

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

Hinweis

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

IPv6

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

Hostname

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

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

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

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

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

DNS-Server

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

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

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

HTTP und HTTPS

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

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

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

Hinweis

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

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

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

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

Netzwerk-Erkennungsprotokolle

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

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

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

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

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

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

Globale Proxys

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

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

Unterstützte HTTP- und HTTPS-Proxy-Formate:

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

Hinweis

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

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

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

One-Click Cloud Connect

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

O3C zulassen:

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

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

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

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

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

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

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

Netzwerk-Ports

Klicken Sie, um das Portbild anzuzeigen oder auszublenden.

- Klicken Sie auf einen Port im Bild, um die Portdetails in der Portliste anzuzeigen.

Portliste

- **Port**: Die Portnummer.
- **PoE**: Aktivieren oder deaktivieren Sie für den jeweiligen Port PoE.
- **Netzwerk**: Aktivieren oder deaktivieren Sie für den Port das Netzwerk.
- **Status**: Zeigt an, ob an diesem Port ein Gerät angeschlossen ist.
- **Friendly name (Anzeigename)**: Der Anzeigename wird unter **Network settings (Netzwerkeinstellungen)** festgelegt. Der Standardname stellt eine Kombination aus dem Modell und der MAC-Adresse (Media Access Control) des verbundenen Geräts dar.

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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

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

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

Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) :

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

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Zertifikate

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Firewall

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

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

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

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

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

Rule type (Regeltyp):

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

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

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

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

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

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

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

Das Kontextmenü enthält:

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

Konten

Konten

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

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

Das Kontextmenü enthält:

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

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

SSH-Konten

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

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Anmerkung: Geben Sie eine Anmerkung ein (optional).

Das Kontextmenü enthält:

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

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

Virtual host (Virtueller Host)

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

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

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

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

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

Das Kontextmenü enthält:

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

Disabled (Deaktiviert): Der Server ist deaktiviert.

Konfiguration der Client-Zugangsdaten-Genehmigung

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

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

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

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

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

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

OpenID-Konfiguration

Wichtig

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

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

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

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

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

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

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

Empfänger

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden.

Hinweis

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

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

Hinweis

Sie können bis zu 20 Empfänger erstellen.

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

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

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

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

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

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

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

Hinweis

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

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

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

⋮ Das Kontextmenü enthält:

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

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

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

Zeitschemata

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

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

Manuelle Auslöser

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

Speicherung

Onboard-Speicher

RAID

- **Free (Frei)**: Freier Platz auf dem Datenträger.
- **Status**: Ob das Laufwerk bereitsteht ist oder nicht.
- **Dateisystem**: Das von der Festplatte verwendete Dateisystem.
- **Verschlüsselt**: Ob das Laufwerk verschlüsselt ist oder nicht.
- **Temperatur**: Die aktuelle Temperatur der Hardware.
- **Overall heath test (Allgemeiner Zustandstest)**: Das Ergebnis nach Überprüfung des Datenträgerzustands.
- **RAID level (RAID-Stufe)**: Das für den Speicher verwendete RAID-Level. Unterstützte RAID-Level sind 0, 1, 5, 6, 10.
- **RAID status (RAID-Status)**: Der RAID-Status des Speichers. Mögliche Werte sind **Online**, **Degraded (Heruntergestuft)**, **Syncing (Synchronisierung)** und **Failed (Fehlgeschlagen)**. Der Synchronisierungsvorgang kann mehrere Stunden dauern.

Werkzeuge

Hinweis

Warten Sie beim Ausführen der folgenden Tools unbedingt, bis der Vorgang abgeschlossen ist, bevor Sie die Seite schließen.

- **Check (Überprüfen)**: Überprüfen Sie das Speichergerät auf Fehler und versuchen Sie es automatisch zu reparieren.
- **Repair (Reparieren)**: Reparieren Sie das Speichergerät. Während der Reparatur werden laufende Aufzeichnungen unterbrochen. Das Reparieren eines Speichergeräts kann zu einem Datenverlust führen.
- **Formatieren**: Alle Aufzeichnungen löschen und das Speichergerät formatieren. Wählen Sie ein Dateisystem.
- **Encrypt (Verschlüsseln)**: Gespeicherte Daten werden verschlüsselt. Alle Dateien auf dem Speichergerät werden gelöscht.
- **Entschlüsseln**: Gespeicherte Daten werden entschlüsselt. Alle Dateien auf dem Speichergerät werden gelöscht.
- **Change password (Kennwort ändern)**: Ändern Sie das Kennwort für die Festplattenverschlüsselung. Das Ändern des Kennworts beeinträchtigt laufende Aufzeichnungen nicht.
- **Change RAID level (RAID-Ebene ändern)**: Löschen Sie alle Aufzeichnungen und ändern Sie das RAID-Level für den Speicher.
- **Use tool (Werkzeug verwenden)**: Klicken Sie hier, um das ausgewählte Werkzeug ausführen zu können.

Hard drive status (Festplattenstatus): Klicken Sie hier, um den Festplattenstatus, die Kapazität und die Seriennummer anzuzeigen.

Write protect (gegen Überschreiben schützen): Aktivieren Sie den Schreibschutz, um das Speichergerät gegen Überschreiben zu schützen.

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.

Remote System Log

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

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

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

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

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

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

Direktkonfiguration

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

Wartung

Wartung

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

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

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

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

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

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

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

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

Fehler beheben

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

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

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

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

Netzwerk-Trace

Wichtig

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

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

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

Mehr erfahren

Cybersicherheit

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

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

Axis Sicherheitsbenachrichtigungsdienst

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

Schwachstellen-Management

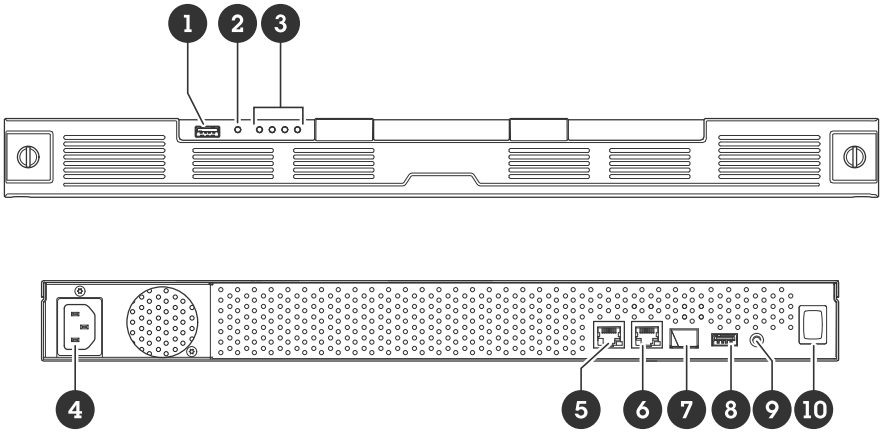
Um das Risiko für die Kunden zu minimieren, hält sich Axis als **Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)** an Branchenstandards, um entdeckte Schwachstellen in unseren Geräten, unserer Software und unseren Dienstleistungen zu verwalten und darauf zu reagieren. Weitere Informationen zu den Richtlinien von Axis für das Management von Schwachstellen, zur Meldung von Schwachstellen, zu bereits bekannt gewordenen Schwachstellen und zu entsprechenden Sicherheitshinweisen finden Sie unter *axis.com/vulnerability-management*.

Sicherer Betrieb von Axis Geräten

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

Technische Daten

Produktübersicht



1 *USB-3.0-Port*
2 *Status-LED Gerät*
3 *Status-LEDs Festplatten*
4 *Stromanschluss*
5 *AUX-RJ45-Port*
6 *LAN-RJ45-Port*
7 *LAN-SFP-Port*
8 *USB 2.0 Port*
9 *Steuertaste*
10 *Ein/-Ausschalter*

LED-Anzeigen

Front-LEDs

LED	Farbe	Anzeige
Produktstatus	Grün	Der Rekorder ist eingeschaltet und der Status in Ordnung.
	Gelb	Der Rekorder startet gerade, oder die Gerätesoftware wird aktualisiert. Warten Sie, bis die LED grün leuchtet.
Festplattenstatus	Grün	Das Laufwerk ist online.
	Blinkt abwechselnd grün	RAID wird synchronisiert. Die Aufzeichnung ist möglich, aber es ist noch keine Redundanz erreicht.
	Gelb	Dieses Laufwerk ist online, aber ein anderes Laufwerk ist defekt. Dem RAID fehlt Redundanz.
	Rot	Das Laufwerk ist defekt.

	Alle sind rot	Das RAID ist fehlgeschlagen. System zeichnet nicht auf. Um die defekte Festplatte im Falle eines RAID-Fehlers zu identifizieren, gehen Sie zur Weboberfläche des Geräts und gehen Sie zu **System > Storage > Hard drive status (System > Speicher > Festplattenstatus)**.
	Aus	Keine Festplatte.

LEDs hinten

LED	Farbe	Anzeige
Netzwerk-Port	Blinkt grün	1 Gbit/s
	Blinkt gelb	100 Mbit/s
	Aus	Kein Netzwerk

Ein/-Ausschalter

- Um den Rekorder abzuschalten, drücken Sie die Power-Taste so lange, bis der Summer einen kurzen Ton abgibt.
- Um den Summer auszuschalten, drücken Sie kurz auf die Power-Taste.

Steuertaste

Die Steuertaste hat folgende Funktionen:

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

Fehlerbehebung

Technische Probleme, Hinweise und Lösungen

Ausgabe	Lösung
Keine Aufzeichnungen verfügbar.	Wechseln Sie zu .
Keine Verbindung zu Kameras	Wechseln Sie zu .
Ich erhalte eine Fehlermeldung: „No contact" (Kein Kontakt).	Wechseln Sie zu .
Die Standorte werden nicht in der Mobile App angezeigt.	Achten Sie darauf, dass Sie die neueste Version der AXIS Camera Station Edge Mobile App verwenden.

Einfache Probleme lösen

Bevor Sie neu starten, konfigurieren oder setzen Sie Ihre Geräte zurück.

1. Sicherstellen, dass die Kameras an die Stromversorgung angeschlossen sind.
2. Überprüfen, ob eine Internetverbindung besteht.
3. Sicherstellen, dass das Netzwerk richtig funktioniert.
4. Sicherstellen, dass sich die Kameras in demselben Netzwerk wie der Rechner befinden. Hinweise: Dies gilt nicht für den Fernzugriff.

Falls die vorherigen Maßnahmen erfolglos waren:

5. Stellen Sie sicher, dass Ihre Kameras, Ihr Recorder und AXIS Camera Station Edge die neueste Gerätesoftware nutzen.
   Siehe .
6. Starten Sie AXIS Camera Station Edge neu.
7. Die Kameras und Rekorder neu starten.

Falls die vorherigen Maßnahmen erfolglos waren:

8. Einen harten Reset der Kameras und des Rekorders durchführen, um die Werkseinstellungen vollständig wiederherzustellen.
   Siehe .
9. Die zurückgesetzten Kameras erneut zum Standort hinzufügen.

Falls die vorherigen Maßnahmen erfolglos waren:

10. Ihre Grafikkarte mit den neuesten Treibern aktualisieren.

Falls die vorherigen Maßnahmen erfolglos waren:

11. Einen Systembericht speichern und den technischen Support von Axis kontaktieren.
    Siehe .

AXIS OS aktualisieren

Die Software-Updates für ein Gerät sorgen für die fortlaufende Aktualisierung mit den aktuellen und verbesserten Funktions- und Sicherheitsmerkmalen.

1. Gehen Sie zur Weboberfläche des Leitgeräts.
2. Rufen Sie **Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung)** auf und klicken Sie **Upgrade (Aktualisieren)** an.

3. Die Anweisungen auf den Bildschirmseiten befolgen.

Ich kann mich nicht auf der Weboberfläche des Produkts anmelden.

Wenn Sie beim Konfigurieren ein Kennwort eingerichtet haben und das Produkt später einem Standort zuordnen, können Sie sich mit dem von Ihnen eingerichteten Kennwort nicht mehr auf der Weboberfläche des Produkts anmelden. Der Grund dafür ist, dass AXIS Camera Station Edge die Kennwörter aller Geräte eines Standorts ändert.

Um sich bei einem Gerät auf Ihrer Website anzumelden, geben Sie den Benutzernamen ein **root (Wurzel)** und Ihr Website-Passwort.

Das Löschen aller Aufzeichnungen

1. Wechseln Sie auf der Weboberfläche des Geräts zu **System** > **Storage (Speicher)**.
2. Wählen Sie **Format** und klicken Sie **Use tool (Tool verwenden)**.

Hinweis

Dieses Verfahren löscht alle Aufzeichnungen von der Festplatte, aber die Konfiguration des Rekorders und des Standorts ändert sich nicht.

Einen Systembericht speichern

1. Gehen Sie in AXIS Camera Station Edge zu  > **Save system report (Systembericht speichern)**.
2. Gehen Sie in AXIS Camera Station Pro zu  **> Help (Hilfe) > System report (Systembericht)**.
3. Wenn Sie beim Axis Helpdesk ein Problem einreichen, bitte den Systembericht beifügen.

Benötigen Sie Hilfe?

Nützliche Links

- *Benutzerhandbuch zu AXIS Camera Station Edge*
- *Benutzerhandbuch zu AXIS Camera Station Pro*

Support

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

T10230523_de

2025-10 (M1.7)