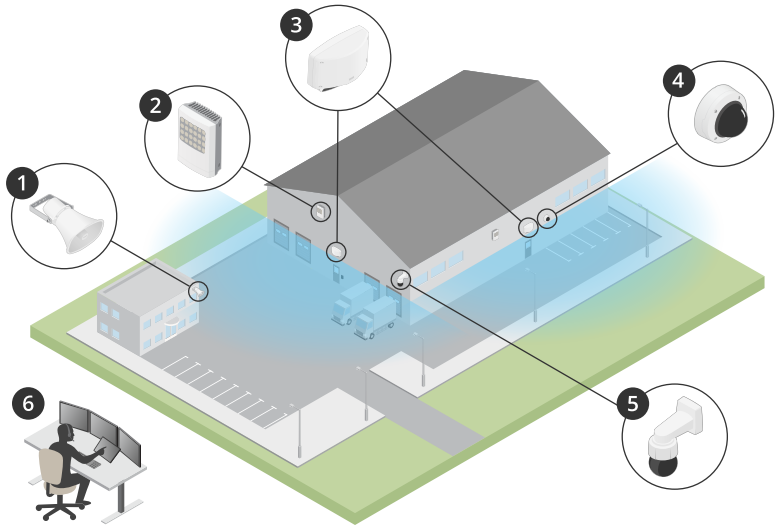
AXIS D2110-VE Security Radar

Benutzerhandbuch

Inhalt

Lösungsübersicht



1 *C1310-E Horn Speaker*
2 *Tür-Controller*
3 *D2110–VE Security Radar*
4 *Eine Fixed-Dome Kamera*
5 *PTZ-Kamera*
6 *Überwachungszentrum*

Radarprofile

Hinweis

Um Radarprofile verwenden zu können, muss auf Ihrem Gerät die Firmwareversion 10.11 oder höher ausgeführt werden. Gehen Sie zu , um Ihre Firmware zu aktualisieren.

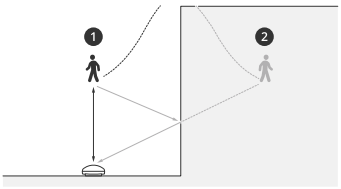
Das Benutzerhandbuch hilft Ihnen dabei, den Radar so nutzen, wie es Ihren Anforderungen entspricht. AXIS D2110-VE Security Radar verfügt über zwei Profile:

- **Profil zur Bereichsüberwachung** zur Verfolgung großer und kleiner Objekte mit Geschwindigkeiten von weniger als 55 km/h (34 mph)
- **Profil zur Straßenüberwachung** zur Verfolgung von Fahrzeugen mit Geschwindigkeiten bis zu 105 km/h (65 mph)

Alle Informationen in diesem Benutzerhandbuch, die sich nicht explizit auf das **Profil zur Bereichsüberwachung** oder **Profil zur Straßenüberwachung** beziehen, gelten für beide Profile und können unabhängig davon, welches Sie verwenden, herangezogen werden.

Der Installationsort des Produkts

- Das Radar ist für die Überwachung offener Bereiche bestimmt. Feststehende Objekte (z. B. Mauern, Zäune, Bäume oder hohe Sträucher) im Erfassungsbereich erzeugen einen blinden Fleck (Radarschatten) hinter dem Objekt.
- Installieren Sie den Radar auf einem stabilen Mast oder an einer Stelle an einer Wand, an der keine weitere Objekte oder Installationen befinden. Objekte innerhalb eines Radius von 1 m links und 3 m rechts des Radars reflektieren Radiowellen und beeinflussen die Leistung des Radars.
- Metallobjekte im Sichtfeld verursachen Reflektionen, die die Klassifizierungsfähigkeit des Radars beeinträchtigen.



1 Tatsächliche Bilderfassung
2 Reflektierte Erfassung (Phantomverfolgung)

Informationen zum Umgang mit reflektierenden Objekten finden Sie unter .

- Weitere Informationen zur Installation von mehr als zwei Radargeräten in derselben Zone finden Sie unter .

Abdeckungsbereich

Der AXIS D2110–VE verfügt über einen horizontalen Abdeckungsbereich von 180°. Der Erfassungsbereich entspricht 5.600 m^2 (61000 ft^2) für Personen und 11.300 m^2 (122000 ft^2) für Fahrzeuge.

Hinweis

Wenn der Radar in einer Höhe von 3,5 bis 4 m (11–13 ft) installiert ist, ist eine optimale Bereichsabdeckung gegeben. Die Montagehöhe beeinflusst die Größe des toten Winkels unter dem Radar.

Profil für Bereichsüberwachung

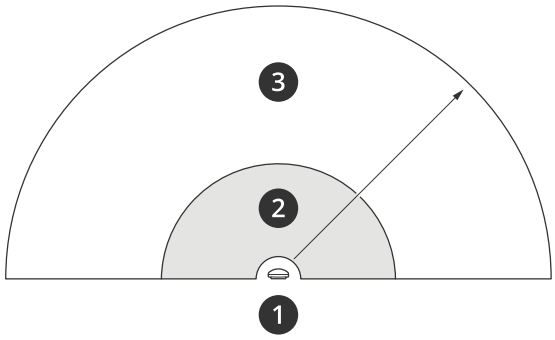
Das **Profil zur Bereichsüberwachung** wurde für Objekte optimiert, die sich mit einer Geschwindigkeit von bis zu 55 km/h bewegen. Mit diesem Profil können Sie erkennen, ob es sich bei einem Objekt um einen Menschen, ein Fahrzeug oder ein unbekanntes Objekt handelt. Eine Regel kann so eingerichtet werden, dass bei Erkennung eines dieser Objekte eine Aktion ausgelöst wird. Verwenden Sie zum Verfolgen von Fahrzeugen mit höheren Geschwindigkeiten das .

Mehrere Radargeräte installieren

Sie können mehrere Radarsysteme installieren, um Bereiche wie die Umgebung eines Gebäudes oder die Pufferzone außerhalb eines Zauns zu abdecken.

Koexistenz

Wenn Sie mehr als zwei Radare in derselben Zone platzieren, können die Radiowellen des Radars innerhalb der Zone Störungen verursachen und die Leistung beeinträchtigen. Der Radius des Koexistenzbereichs beträgt 350 m (380 yd).



1 Radar
2 Erfassungsbereich
3 Koexistenzbereich

Hinweis

Die Leistung des Radars im Koexistenzbereich kann auch durch die Umwelt und/oder die Richtung des Radars in Richtung von Zäunen, Gebäuden oder Radaranlagen beeinflusst werden.

Installieren von 2 bis 3 Radaren in derselben Zone

Wenn Sie zwei oder drei Radare in der gleichen Zone platzieren, müssen Sie die Anzahl der benachbarten Radare in der Geräteschnittstelle festlegen. Dies trägt zur Verbesserung der Leistung des Radars und zur Vermeidung von Störungen bei.

1. Gehen Sie zu **Radar > Einstellungen > Koexistenz**.
2. Wählen Sie die Anzahl der benachbarten Radargeräte aus.

Beispiele für Installationen mit mehreren Radargeräten finden Sie unter .

Installieren von 4 bis 6 Radaren in derselben Zone

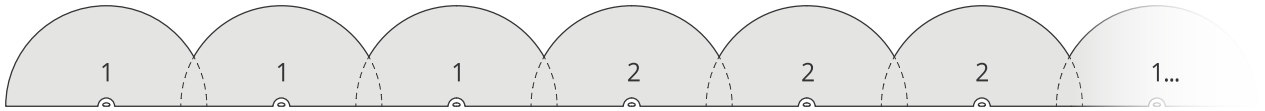
Hinweis

Ab Firmware-Version 11.3 ist die Installation von bis zu sechs Radargeräten in derselben Zone möglich.

Wenn Sie vier bis sechs Radare in derselben Zone montieren, legen Sie zuerst die Anzahl der benachbarten Radare fest und fügen dann jedes Radar zu einer Gruppe hinzu. Beginnen Sie mit dem Radar, das am weitesten entfernt installiert ist, z. B. dem am weitesten links von Ihnen entfernten Radar. Fügen Sie die Radare in Dreiergruppen hinzu und fügen Sie die Radare hinzu, die sich derselben Gruppe am nächsten befinden.

Die Radare der Gruppe synchronisieren sich miteinander, um die Leistung zu optimieren und Störungen untereinander zu vermeiden.

1. Gehen Sie zu **Radar > Einstellungen > Koexistenz**.
2. Stellen Sie die Anzahl der benachbarten Radare auf **3 bis 5** ein.
3. Wählen Sie eine Gruppe für Ihr Radar aus.



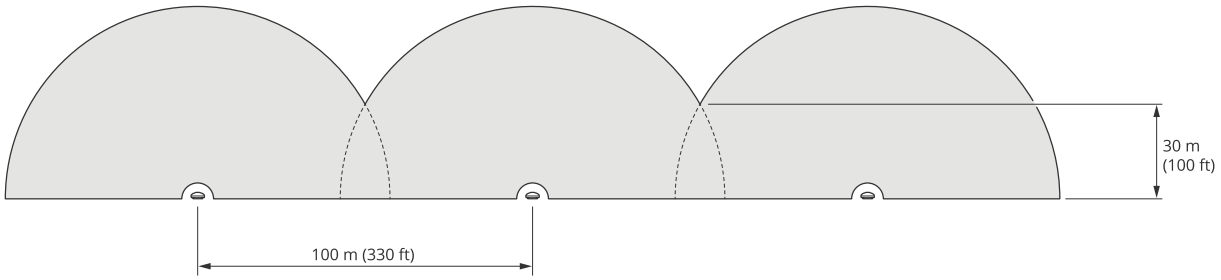
Dies ist ein Beispiel für die Gruppen von mehreren radarbasierten Geräten, die nebeneinander in derselben Zone installiert sind.

Weitere Beispiele für Installationen mit mehreren Radargeräten finden Sie unter .

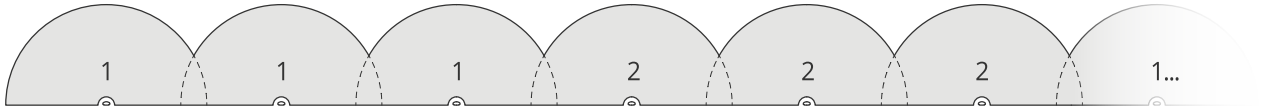
Beispiele für Bereichsinstallationen

Erstellen eines virtuellen Zauns mit mehreren Radargeräten

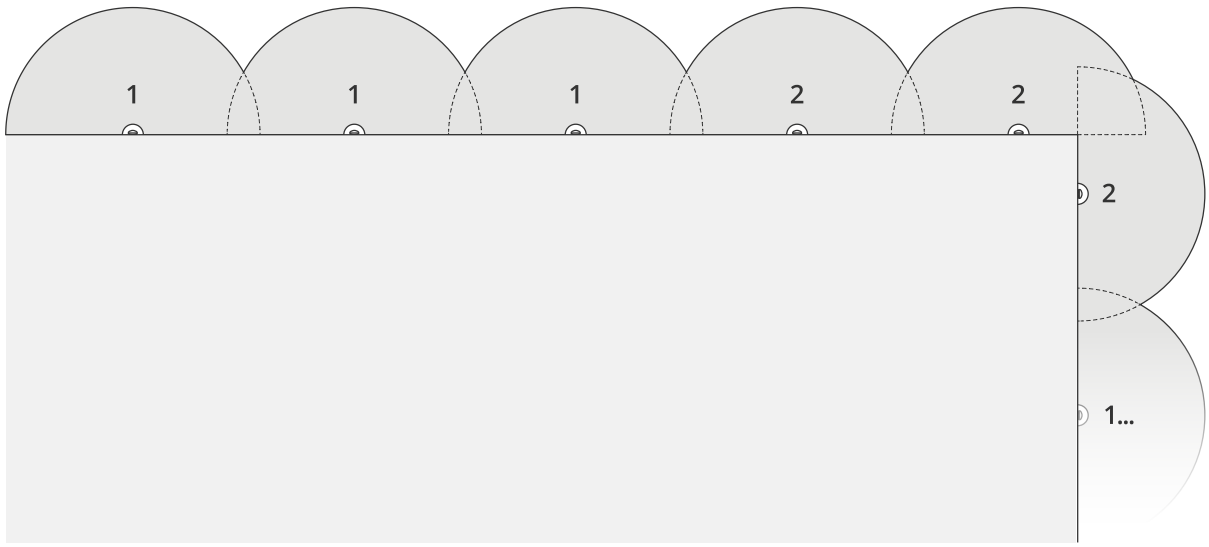
Um einen virtuellen Zaun zu erstellen, z. B. entlang eines Gebäudes oder um ein Gebäude herum, können Sie mehrere Radarsysteme nebeneinander platzieren. Wir empfehlen Ihnen, zwischen den einzelnen Geräte einen Abstand von 100 m (330 ft) einzuhalten.



Legen Sie die Anzahl der Radare in der Geräteschnittstelle fest, um Störungen bei der Montage von mehr als zwei Radaren in derselben Zone zu vermeiden. Fügen Sie bei der Montage von mehr als drei Radargeräten jedes Radar zu einer Gruppe hinzu.



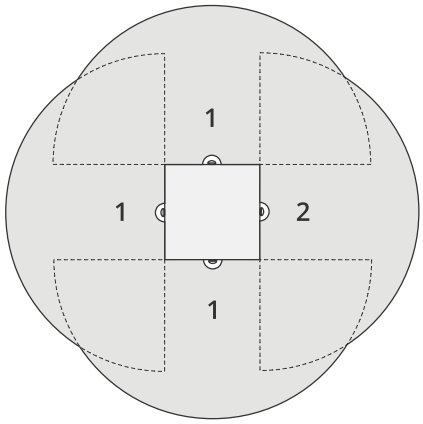
Der virtuelle Zaun kann, wie in diesem Beispiel gezeigt, auch an Ecken angepasst werden.



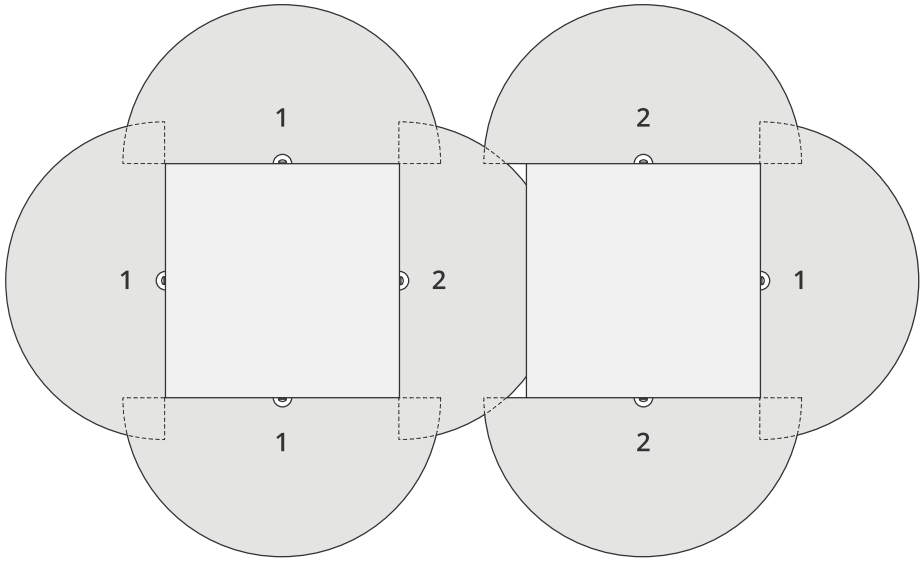
Weitere Informationen zum Erstellen von Radargeräten und Gruppen finden Sie unter .

Einen Bereich um ein Gebäude abdecken

Um den Bereich um ein Gebäude herum abzudecken, richten Sie die Radargeräte nach außen gerichtet an den Mauern des Gebäudes ein. Wenn Sie mehr als drei Radare in derselben Zone platzieren, legen Sie die Anzahl der benachbarten Radare auf der Geräteschnittstelle fest und fügen Sie, wie in diesem Beispiel gezeigt, jedes Radar zu einer Gruppe hinzu.



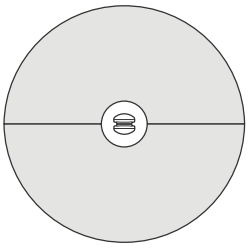
Der Bereich um mehrere Gebäude herum lässt sich ebenfalls abdecken.

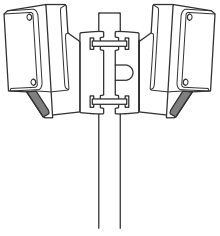


Weitere Informationen zum Erstellen von Radargeräten und Gruppen finden Sie unter .

Einen offenen Bereich abdecken

Zur Abdeckung eines großen offenen Bereichs müssen zwei Radargeräte an zwei Masthalterungen Rücken an Rücken positioniert werden.



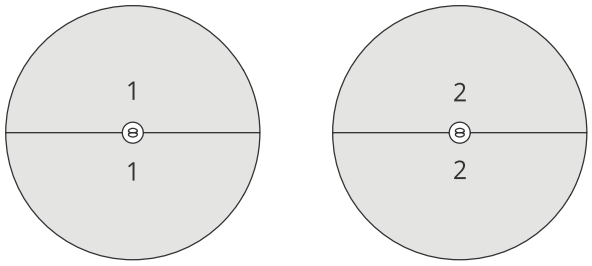


Sie können den PoE-Ausgang eines Radars für die Stromversorgung des zweiten Radars verwenden. Ein dritter Radar kann jedoch auf diese Weise nicht angeschlossen werden.

Hinweis

Der PoE-Ausgang des Radars wird aktiviert, wenn das Radar über einen 60 W-Midspan versorgt wird.

Wenn Sie mehrere benachbarte Radargeräte in derselben Koexistenzzone installieren möchten, stellen Sie deren Anzahl in der Geräteschnittstelle ein und fügen Sie jedes Radargerät zu einer Gruppe hinzu, um Störungen zu vermeiden. Dies ist ein Beispiel, wie Sie Ihre Radargeräte benachbart installieren können.



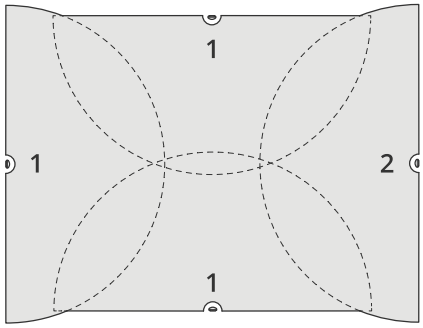
Weitere Informationen zum Erstellen von Radargeräten und Gruppen finden Sie unter .

Installieren mehrerer gegenüberliegender Radargeräte

Allgemein wird empfohlen, nur drei aufeinander gerichtete Radargeräte zu installieren, da die Gefahr von Störungen zwischen den Radaren erhöht wird. In einigen bestimmten Bereichen kann dies jedoch notwendig sein. Wenn Sie z. B. ein Fußballfeld abdecken möchten, können Sie die Radargeräte nicht in der Mitte des Feldes platzieren.

Wenn mehr als drei Radare installiert werden, die aufeinander gerichtet sind, muss die Mindeststrecke zwischen ihnen 40 Meter (130 ft) betragen. Besonders wichtig ist es auch, die Anzahl der benachbarten Radargeräte in der Geräteschnittstelle einzustellen und jedes Radargerät zu einer Gruppe hinzuzufügen. Dies hilft, die Leistung des Radars zu verbessern.

Dies ist ein Beispiel für die Gruppen von vier Radaren, die ein Feld abdecken.



Weitere Informationen zum Erstellen von Radargeräten und Gruppen finden Sie unter .

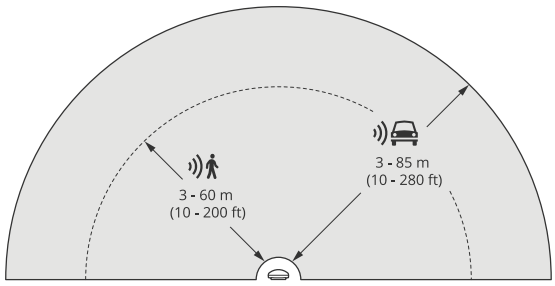
Erfassungsbereich

Der Erfassungsbereich ist die Entfernung, in der ein Objekt verfolgt werden und einen Alarm auslösen kann. Sie wird von der **Naherfassungsgrenze** aus (wie nahe am Gerät kann eine Erfassung stattfinden) bis zu einem **Fernerfassungswert** (bis zu welcher Entfernung kann das Gerät etwas erfassen) gemessen werden.

Das **Profil zur Bereichsüberwachung** ist für die Erfassung von Menschen optimiert. Es damit jedoch auch Fahrzeuge und andere Objekte, die sich bei einer Abweichung von +/- 2 km/h mit bis zu 55 km/h bewegen.

Bei Montage in optimaler Installationshöhe sehen die Erfassungsbereiche wir folgt aus:

- **3–60 m (10–200 ft)** bei der Erfassung eines Menschen
- **3–85 m (10–280 ft)** bei der Erfassung eines Fahrzeugs



Hinweis

- Wenn das Produkt in anderer Höhe montiert wird, geben Sie beim Kalibrieren des Radars über die Weboberfläche des Produktes die tatsächliche Höhe ein.
- Der Erfassungsbereich wird von der Szene beeinflusst.
- Der Erfassungsbereich wird von benachbarten Radargeräten beeinflusst.
- Der Erfassungsbereich wird vom Objekttyp beeinflusst.

Der Erfassungsbereich wurde unter folgenden Bedingungen gemessen:

- Der Bereich wurde entlang des Bodens gemessen.
- Das Objekt war eine 170 cm (5 ft 7 in) große Person.
- Die Person ging geradeaus vor dem Radar.
- Die Werte werden gemessen, wenn die Person in den Erfassungsbereich eindringt.
- Die Radarempfindlichkeit wurde auf **Mittel** eingestellt.

Montagehöhe	0° Neigung	10° Neigung	20° Neigung
2,5 m (8,2 ft)	3,0–60 m (9,8–197 ft)	Nicht empfohlen	Nicht empfohlen
3,5 m (11 ft)	3,0–60 m (9,8–197 ft)	Nicht empfohlen	Nicht empfohlen
4,5 m (15 ft)	4,0–60 m (13–197 ft)	Nicht empfohlen	Nicht empfohlen
5,5 m (18 ft)	7,5–60 m (25–197 ft)	Nicht empfohlen	Nicht empfohlen
6,5 m (21 ft)	7,5–60 m (25–197 ft)	5,5–60 m (18–197 ft)	Nicht empfohlen
8 m (26 ft)	Nicht empfohlen	9–60 m (30–197 ft)	7,5–30 m (25–98 ft)
10 m (33 ft)	Nicht empfohlen	15–60 m (49–197 ft)	9–35 m (30–115 ft)
12 m (39 ft)	Nicht empfohlen	23–60 m (75–197 ft)	13–38 m (43–125 ft)
14 m (36 ft)	Nicht empfohlen	27–60 m (89–197 ft)	17–35 m (56–115 ft)
16 m (52 ft)	Nicht empfohlen	Nicht empfohlen	25–50 m (82–164 ft)

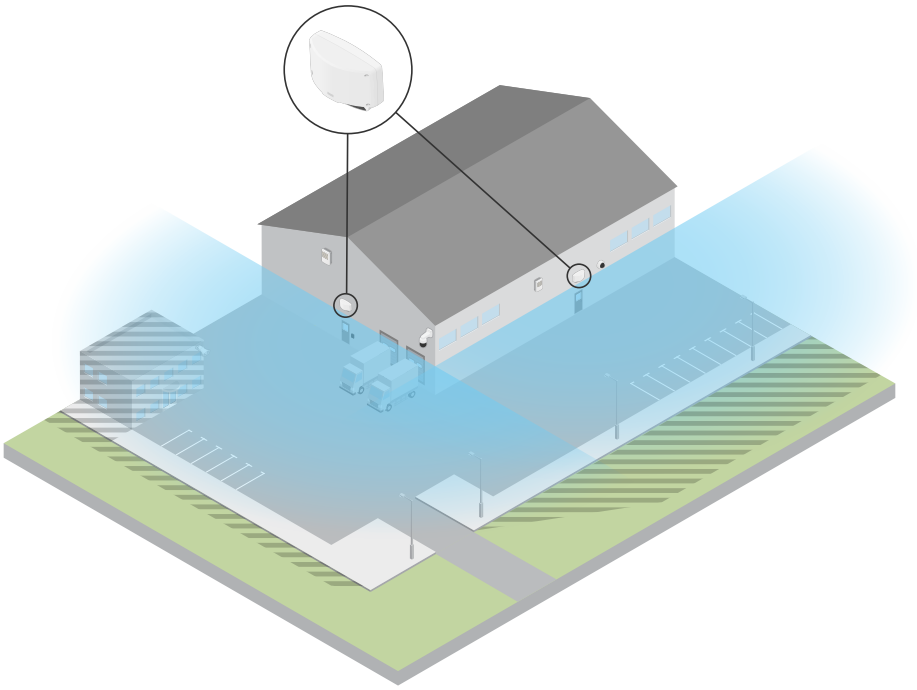
Einsatzgebiete für die Bereichsüberwachung

Abdeckung des Poolbereichs

In einem öffentlichen Pool finden nach der Schließung eine Reihe von Einbrüchen statt. Da das Geschäft privater Natur ist, können die Eigentümer keine Videosicherheit installieren. Sie haben sich für die Installation eines Radars entschieden und das **Profil zur Bereichsüberwachen** eingerichtet. Das Radar ist auf dem Gebäude montiert und deckt den gesamten Pool und den größten Teil des gesamten Geländes ab. Über einen Lautsprecher wird eine Warnung ausgelöst, sobald zwischen der Schließung um 20 Uhr und der Öffnung um 6 Uhr eine Person erkannt wird.

Den Bereich um ein Gebäude abdecken

Eine Chemiefabrik führt ihrem System mithilfe eines Radars zur Abdeckung des Bereichs rund um ein unternehmenskritischen Gebäude eine zusätzliche Sicherheitsebene hinzu. Das Sicherheitssystem umfasst bereits Kameras, Wärmebildkameras und Zugangscontroller. Radarsysteme können Ereignisse auslösen, aufgrund derer Kameras Eindringlinge verfolgen, heranzoomen und Aktivitäten aufzeichnen. Blinkende, an Wärmebildkameras gekoppelte Blitzlichtsignale werden ausgelöst, damit der Eindringling weiß, dass der Bereich geschützt ist. Zusätzlich können Zugangscontroller einschränken. Mithilfe der Radarsysteme kann das System Aktionen auslösen, lange bevor der Eindringling das unternehmenskritische Gebäude erreicht hat.



Einen großen freien Bereich abdecken

Auf einem Parkplatz vor einem kleinen Einkaufszentrum fanden nach Geschäftsabschluss vermehrt Einbrüche in Fahrzeuge statt. Es hat immer ein Wachmann Dienst, aber sie wollen nachts ihre Sicherheitsvorkehrungen erhöhen, ohne zusätzliche Kosten für mehr Personal zu haben. Sie haben sich entschieden, zwei Rücken an Rücken montierte Sicherheitsradargeräte mit dem **Profil zur Bereichsüberwachung** zu installieren, die den gesamten Parkplatz abdecken. Die Radargeräte sind so konfiguriert, dass bei verdächtigem Verhalten das eingesetzte Sicherheitspersonal alarmiert wird, sodass sie sofort die Szene untersuchen könne. Sie können auch einen Hornlautsprecher installieren, der zur Abschreckung von Dieben durch die Radargeräte ausgelöst wird.

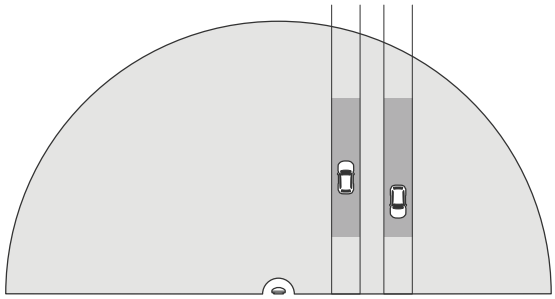
Profil für Straßenüberwachung

Das **Road monitoring profile (Profil zur Straßenüberwachung)** eignet sich am besten zur Verfolgung von Fahrzeugen mit einer Geschwindigkeit von bis zu 105 km/h in Stadtgebieten, Sperrzonen und auf Vorortstraßen bewegen. Dieser Modus sollte nicht zur Erfassung von Menschen oder anderen Objekttypen verwendet werden. Zur Verfolgung von anderen Objekten als Fahrzeugen verwenden Sie Ihr Radargerät mit .

Beispiele für Straßeninstallationen

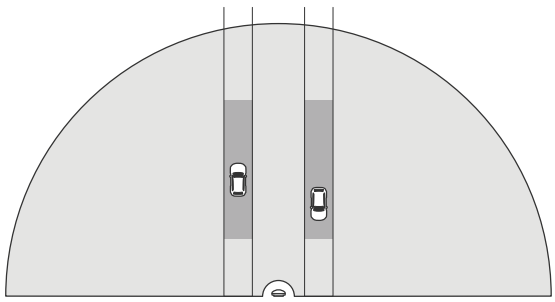
Seitlich montiert

Zur Überwachung von Straßenfahrzeugen kann der Radar am Straßenrand montiert werden. Das Radargerät hat einen seitlichen Erfassungsbereich von 10 m (32 ft).



Mittige Montage

Diese Montagemöglichkeit erfordert eine stabile Position. Der Radar kann an einem Mast in der Straßenmitte oder an einer Brücke oberhalb der Fahrbahn montiert werden. Das Radargerät bietet in diesem Fall einen seitlichen Erfassungsbereich von 10 m (32 ft) zu beiden Seiten des Radars. Das Radargerät hat bei Montage in der Mitte einen größeren Erfassungsbereich.



Hinweis

Für das Profil zur Straßenüberwachung empfehlen wir Ihnen, das Radargerät auf einer Höhe zwischen 3 m (10 ft) und **8 m (26 ft)** zu installieren.

Erfassungsbereich der Straßenüberwachung

Der Erfassungsbereich ist die Entfernung, in der ein Objekt verfolgt werden und einen Alarm auslösen kann. Sie wird von der **Naherfassungsgrenze** aus (wie nahe am Gerät kann eine Erfassung stattfinden) bis zu einem **Fernerfassungswert** (bis zu welcher Entfernung kann das Gerät etwas erfassen) gemessen werden.

Dieses Profil ist für die Erfassung von Fahrzeugen optimiert. Damit kann die Geschwindigkeit von Fahrzeugen auf +/- 2 km/h (1.24 mph) genau gemessen werden und Fahrzeuge mit einer Geschwindigkeit von bis zu 105 km/h (65 mph) können überwacht werden.

Erfassungsbereich bei Montage des Radargeräts in optimaler Installationshöhe:

- **25 bis 70 m (82–229 ft)** für Fahrzeuge mit einer Geschwindigkeit von 60 km/h (37 mph).
- **30 bis 60 m (98–196 ft)** für Fahrzeuge mit einer Geschwindigkeit von 105 km/h (65 mph).

Anwendungsfälle für die Straßenüberwachung

Regulierung von Fahrzeugen in verkehrsberuhigten Zonen

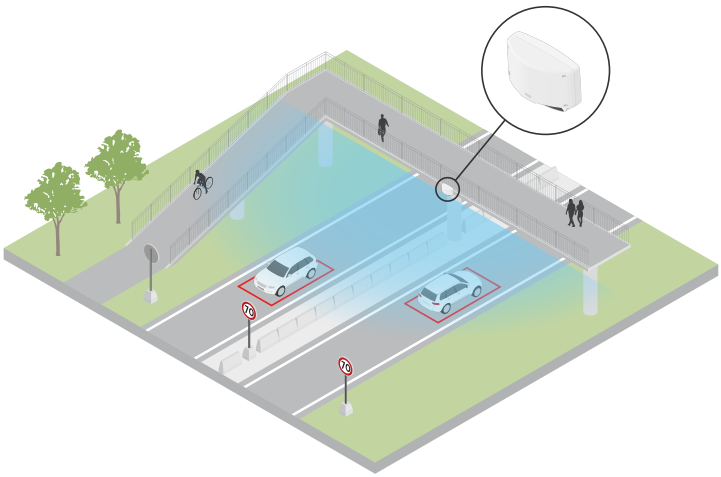
Ein Industriekomplex mit langen Straßen zwischen zwei Lagerhäusern hat ein Radargerät installiert, um eine Geschwindigkeitsbegrenzung von 60 km/h (37 mph) durchzusetzen. Im **Profil zur Straßenüberwachung** erkennt der Radar, wenn ein Fahrzeug in seiner Erfassungszone diese Geschwindigkeit überschreitet. Daraufhin wird ein Ereignis ausgelöst, das eine E-Mail-Benachrichtigung an Fahrer und Manager sendet. Die Erinnerung trägt dazu bei, dass die Geschwindigkeitsbeschränkungen besser eingehalten werden.

Unerwünschte Fahrzeuge auf gesperrter Fahrbahn

Ein kleiner Weg zu einem alten Steinbruch wurde gesperrt. Da jedoch Fahrzeuge weiterhin die Straße benutzten, installierten die Behörden einen Sicherheitsradar mit dem **Profil zur Straßenüberwachung**. Das Radargerät wurde neben der Straße montiert und deckt die gesamte Breite der Straße ab. Jedes Mal, wenn ein Fahrzeug das Szenario betritt, wird ein blinkendes Signal ausgelöst, das Fahrer zum Verlassen der Straße auffordert. Zudem wird eine Nachricht an das Sicherheitsteam gesendet, damit es bei Bedarf eine Einheit hinbeordern kann.

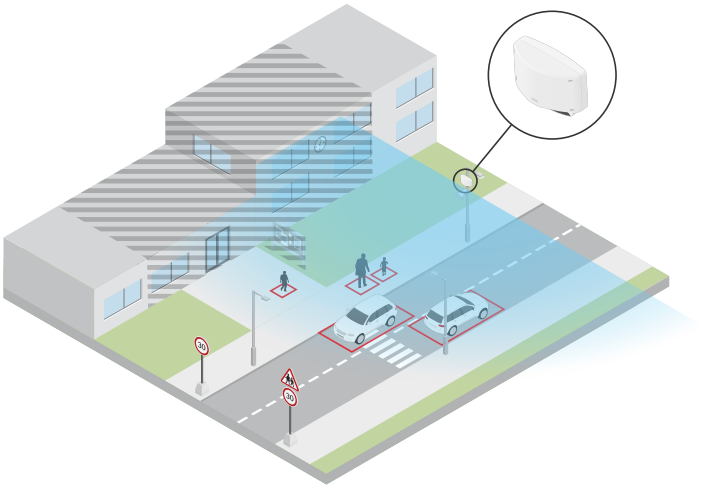
Schneller Übersicht über die Straße

Auf einer durch eine kleine Stadt führende Straße fanden einige Unfälle aufgrund von Geschwindigkeitsüberschreitungen statt. Um die Geschwindigkeitsbegrenzung von 70 km/h (43 mph) durchzusetzen, hat die Verkehrsüberwachung ein Sicherheitsradar mit dem **Profil zur Straßenüberwachung** auf einer Brücke über der Straße installiert. Auf diese Weise können sie die Geschwindigkeit der Fahrzeuge erfassen und überwachen, wann sie Einheiten zur Verkehrskontrolle auf der Straße stationieren sollten.



Sicherheit für Mensch und Fahrzeug

Die Mitarbeitende einer Schule haben zwei Sicherheitsprobleme identifiziert, denen sie auf den Grund gehen möchten. Sie mussten feststellen, dass unerwünschte Besucher während des Schultags das Schulgelände betraten und Fahrzeuge außerhalb der Schule die Geschwindigkeitsbegrenzung von 20 km/h (12 mph) überschritten. Das Radargerät ist an einem Mast neben dem Fußgängerweg angebracht. Als Profil wurde da das Radargerät damit in der Lage ist, sowohl Personen als auch Fahrzeuge zu erfassen, die sich mit einer Geschwindigkeit von unter 55 km/h (34 mph) fortbewegen. Dadurch kann das Personal besser Personen verfolgen, die während der Schulzeit kommen und gehen. Zudem können über einen Lautsprecher die Passanten gewarnt werden, wenn ein vorbeifahrendes Fahrzeug zu schnell ist.



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

*Nicht vollständig unterstützt. Verwenden Sie bei Problemen mit dem Videostreaming einen anderen Browser.

Weboberfläche des Geräts öffnen

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

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

Administratorkonto erstellen

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

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

Wichtig

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

Sichere Kennwörter

Wichtig

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

Übersicht über die Weboberfläche

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

Weboberfläche des Axis Geräts

Ihr Gerät konfigurieren

Montagehöhe festlegen

Stellen Sie in der Weboberfläche des Radars dessen Montagehöhe ein. So kann der Radar die Geschwindigkeit vorbeifahrender Objekte richtig erfassen und messen.

Messen Sie die Höhe vom Boden bis zum Radar so genau wie möglich. Stellen Sie bei Szenen mit unebenen Oberflächen den Wert für die durchschnittliche Höhe der Szene ein.

1. Gehen Sie zu **Radar > Einstellungen > Allgemein**.
2. Legen Sie unter **Montagehöhe** die Höhe fest.

Kalibrieren einer Referenzkarte

Um die Bewegungsrichtung von Objekten leichter zu erkennen, können Sie eine Referenzkarte hochladen. Dies kann z. B. eine Planzeichnung oder ein Luftbild sein, das die vom Radar abgedeckte Fläche darstellt. Kalibrieren Sie die Karte so, dass die vom Radar abgedeckte Fläche mit Position, Ausrichtung und Maßstab der Karte übereinstimmt, und zoomen Sie sie heran, wenn Sie sich bestimmte Teile der Radarabdeckung genauer ansehen möchten.

Sie können sich entweder Schritt für Schritt von einem Einrichtungsassistenten durch die Kartenkalibrierung führen lassen oder jede Einstellung einzeln bearbeiten.

Einrichtungsassistent verwenden:

1. Gehen Sie zu **Radar > Kartenkalibrierung**.
2. Klicken Sie auf **Setup assistent (Einrichtungsassistent)** und befolgen Sie die Anweisungen.

Klicken Sie auf **Reset calibration (Kalibrierung zurücksetzen)**, um die hochgeladene Karte und die von Ihnen hinzugefügten Einstellungen zu entfernen.

Jede Einstellung einzeln bearbeiten:
Die Karte wird mit jeder Anpassung der einzelnen Einstellungen nach und nach kalibriert.

1. Gehen Sie zu **Radar (Radar)> Map calibration (Kartenkalibrierung)> Map (Karte)**.
2. Wählen Sie das hochzuladende Bild aus oder ziehen Sie es per Drag & Drop in den dafür vorgesehenen Bereich.
   Klicken Sie zum erneuten Verwenden eines Kartenbilds mit den aktuellen Einstellungen zum Schwenken und Zoomen auf **Download map (Karte herunterladen)**.
3. Unter **Rotate map (Karte drehen)** können Sie die Karte mit dem Schieberegler in die korrekte Position bringen.
4. Gehen Sie auf **Scale and distance on a map (Maßstab und Entfernung auf einer Karte)** und klicken Sie auf zwei vorher festgelegte Punkte auf der Karte.
5. Geben Sie unter **Distance (Entfernung)** die tatsächliche Entfernung zwischen den beiden Punkten ein, die Sie der Karte hinzugefügt haben.
6. Gehen Sie auf **Pan and zoom map (Karte schwenken und zoomen)** und verwenden Sie die jeweiligen Schaltflächen zum Schwenken, Vergrößern und Verkleinern des Kartenbilds.

Hinweis

Die Zoom-Funktion wirkt sich nicht auf den Erfassungsbereich des Radars aus. Auch wenn nach dem Zoomen Teile des Erfassungsbereichs nicht mehr sichtbar sind, erfasst der Radar weiterhin Objektbewegungen im gesamten Erfassungsbereich. Die einzige Möglichkeit, erfasste Bewegungen auszuschließen, besteht im Hinzufügen von Ausschlussbereichen. Weitere Informationen finden Sie unter .

7. Gehen Sie auf **Radar position (Radarposition)** und verschieben oder drehen Sie die Position des Radars auf der Karte mit den jeweiligen Schaltflächen.

Klicken Sie auf **Reset calibration (Kalibrierung zurücksetzen)**, um die hochgeladene Karte und die von Ihnen hinzugefügten Einstellungen zu entfernen.

Das Video zeigt an einem Beispiel, wie eine Referenzkarte in einem Axis Radar oder einer Radar-Video-Fusionskamera kalibriert wird.

Erfassungsbereiche festlegen

Um festzulegen, wo Bewegungen erfasst werden sollen, können Sie eine oder mehrere Erfassungszonen hinzufügen. Mit verschiedenen Zonen lassen sich unterschiedliche Aktionen auslösen.

Es gibt zwei Arten von Bereichen:

- Ein **Szenario** (früher als Einschlussbereich bezeichnet) ist ein Bereich, in dem sich bewegende Objekte Regeln auslösen. Das Standardszenario entspricht dem gesamten vom Radar abgedeckten Bereich.
- Ein **exclude zone (Ausschlussbereich)** ist ein Bereich, in dem sich bewegende Objekte ignoriert werden. Verwenden Sie Ausschlussbereiche, wenn innerhalb eines Szenarios Bereiche vorhanden sind, die häufig Fehlalarme auslösen.

Szenarien hinzufügen

Ein Szenario besteht aus einer Kombination aus Auslösebedingungen und Erfassungseinstellungen, mit denen Regeln im Ereignissystem erstellt werden können. Fügen Sie Szenarien hinzu, wenn Sie für unterschiedliche Teile der Szene verschiedene Regeln erstellen möchten.

Ein Szenario hinzufügen:

1. Gehen Sie zu **Radar > Szenarien**.
2. Klicken Sie auf **Szenario hinzufügen**.
3. Geben Sie den Namen des Szenarios ein.
4. Wählen Sie aus, ob der Auslöser Objekte sein sollen, die sich in einem bestimmten Bereich bewegen, oder Objekte, die eine oder zwei bestimmte Linien überqueren.

Auslösen bei Objekten, die sich in einem Bereich bewegen:

1. Wählen Sie **Movement in area (Bewegung im Bereich)** aus.
2. Klicken Sie auf **Next (Weiter)**.
3. Wählen Sie den in das Szenario einzubeziehenden Bereichstyp.
   Verschieben und formen Sie den Bereich mit der Maus, sodass er den gewünschten Teil des Radarbilds oder der Referenzkarte abdeckt.
4. Klicken Sie auf **Next (Weiter)**.
5. Fügen Sie Erfassungseinstellungen hinzu.

1. Fügen Sie Sekunden bis zum Auslösung unter **Ignore short-lived objects (Kurzlebige Objekte ignorieren)** hinzu.
2. Wählen Sie unter **Trigger on object type (Auslöser für Objekttyp)** den auslösenden Objekttyp aus.
3. Fügen Sie unter **Speed limit (Geschwindigkeitsbegrenzung)** einen Bereich für die Geschwindigkeitsbegrenzung hinzu.

6. Klicken Sie auf **Next (Weiter)**.
7. Legen Sie die Mindestdauer des Alarms unter **Minimum trigger duration (Minimale Triggerdauer)** fest.
8. **Save (Speichern)** anklicken.

Auslösen für Objekte, die eine Linie überqueren:

1. Wählen Sie **Line crossing (Linienüberschreitung)**.

2. Klicken Sie auf **Next (Weiter)**.
3. Positionieren Sie die Linie in der Szene.
   Verwenden Sie die Maus, um die Linie zu verschieben und zu verformen.
4. Um die Erfassungsrichtung zu ändern, aktivieren Sie die Option **Richtung ändern**.
5. Klicken Sie auf **Next (Weiter)**.
6. Fügen Sie Erfassungseinstellungen hinzu.
   6.1. Fügen Sie Sekunden bis zum Auslösung unter **Ignore short-lived objects (Kurzlebige Objekte ignorieren)** hinzu.
   6.2. Wählen Sie unter **Trigger on object type (Auslöser für Objekttyp)** den auslösenden Objekttyp aus.
   6.3. Fügen Sie unter **Speed limit (Geschwindigkeitsbegrenzung)** einen Bereich für die Geschwindigkeitsbegrenzung hinzu.
7. Klicken Sie auf **Next (Weiter)**.
8. Legen Sie die Mindestdauer des Alarms unter **Minimum trigger duration (Minimale Triggerdauer)** fest. Die Standardvorgabe lautet 2 Sekunden. Wenn das Szenario bei jedem Überqueren der Linie durch ein Objekt ausgelöst werden soll, die Dauer auf 0 Sekunden senken.
9. **Save (Speichern)** anklicken.

Auslösen für Objekte, die zwei Linien überqueren:

1. Wählen Sie **Line crossing (Linienüberschreitung)**.
2. Klicken Sie auf **Next (Weiter)**.
3. Wenn das Objekt zwei Linien überqueren soll, damit der Alarm ausgelöst wird aktivieren Sie **Require crossing of two lines (Überschreiten von zwei Linien erforderlich)**.
4. Linien in der Szene positionieren.
   Verwenden Sie die Maus, um die Linie zu verschieben und zu verformen.
5. Um die Erfassungsrichtung zu ändern, aktivieren Sie die Option **Richtung ändern**.
6. Klicken Sie auf **Next (Weiter)**.
7. Fügen Sie Erfassungseinstellungen hinzu.
   7.1. Legen Sie unter **Max time between crossings (maximale Zeit zwischen den Überquerungen)** die Zeitgrenze zwischen der ersten und der zweiten Linie fest.
   7.2. Wählen Sie unter **Trigger on object type (Auslöser für Objekttyp)** den auslösenden Objekttyp aus.
   7.3. Fügen Sie unter **Speed limit (Geschwindigkeitsbegrenzung)** einen Bereich für die Geschwindigkeitsbegrenzung hinzu.
8. Klicken Sie auf **Next (Weiter)**.
9. Legen Sie die Mindestdauer des Alarms unter **Minimum trigger duration (Minimale Triggerdauer)** fest. Die Standardvorgabe lautet 2 Sekunden. Wenn das Szenario bei jedem Überqueren von zwei Linien durch ein Objekt ausgelöst werden soll, die Dauer auf 0 Sekunden senken.
10. **Save (Speichern)** anklicken.

Ausschlussbereiche hinzufügen

Ausschlussbereiche sind Bereiche, in denen sich bewegende Objekte ignoriert werden. Fügen Sie Ausschlussbereiche hinzu, um etwa schwankende Zweige am Straßenrand zu ignorieren. Sie können auch Ausschlusszonen hinzufügen, um Phantomverfolgungen zu ignorieren, die durch radarreflektierende Materialien wie z. B. einen Metallzaun verursacht werden.

Einen Ausschlussbereich hinzufügen:

1. Gehen Sie zu **Radar > Ausschlussbereiche**.
2. Klicken Sie auf **Ausschlussbereich hinzufügen**.

Verschieben und formen Sie den Bereich mit der Maus, sodass er den gewünschten Teil der Radaransicht oder der Referenzkarte abdeckt.

Fehlalarme minimieren

Wenn Sie feststellen, dass Sie zu viele Fehlalarme erhalten, können Sie bestimmte Bewegungsarten oder Objekte herausfiltern, die Abdeckung ändern oder die Erfassungsempfindlichkeit anpassen. Testen Sie, welche Einstellungen für Ihre Umgebung am besten geeignet sind.

- Erfassungsempfindlichkeit des Radarmelders einstellen:
  Gehen Sie zu **Radar > Einstellungen > Erfassung** und wählen Sie unter **Erfassungsempfindlichkeit** eine niedrigere Empfindlichkeitsstufe aus. Dies verringert die Gefahr von Fehlalarmen, kann aber dazu führen, dass einige Bewegungen nicht vom Radar erfasst werden.
  Die Empfindlichkeitseinstellung wirkt sich auf alle Bereiche aus.
  - **Niedrig**: Verwenden Sie diese Empfindlichkeit, wenn sich viele Metallgegenstände oder große Fahrzeuge in der Umgebung befinden. Die Objektverfolgung und -klassifizierung durch den Radar dauert dann länger. Dadurch kann sich der Erfassungsbereich verkleinern, insbesondere bei sich schnell bewegenden Objekten.
  - **Mittel**: Dies ist die Standardeinstellung.
  - **Hoch**: Stellen Sie diese Empfindlichkeit ein, wenn sich vor dem Radarmelder ein freies Feld ohne Metallobjekte befindet. Dadurch vergrößert sich der Erfassungsbereich für Personen.
- Szenarien ändern und Zonen ausschließen:
  Wenn ein Szenario harte Oberflächen enthält, z. B. eine Wand aus Metall, können Reflektionen zur mehrfachen Erfassung eines einzelnen physikalischen Objekts führen. Sie können entweder die Form des Szenarios ändern oder eine Ausschlusszone hinzufügen, die bestimmte Teile des Szenarios ignoriert. Weitere Informationen finden Sie unter und .
- Auslösen bei Objekten, die zwei Linien überschreiten anstelle einer:
  Wenn in einem Szenario mit Linienüberschreitung schaukelnde Objekte oder sich umher bewegende Tiere eingeschlossen sind, besteht die Gefahr, dass ein Objekt die Linie überquert und einen falschen Alarm auslöst. In diesem Fall können Sie das Szenario so konfigurieren, dass es nur ausgelöst wird, wenn ein Objekt zwei Linien überschritten hat. Weitere Informationen finden Sie unter .
- Nach Bewegung filtern:
  - Gehen Sie zu **Radar > Einstellungen > Erfassung** und wählen Sie **Schaukelnde Objekte ignorieren**. Diese Einstellung minimiert die Anzahl der durch Bäume, Büsche und Fahnenmasten ausgelösten Fehlalarme.
  - Gehen Sie zu **Radar > Settings > Detection (Radar > Einstellungen > Erfassung)** und wählen Sie **Ignore small objects (Kleine Objekte ignorieren)**. Diese Einstellung ist im Profil für die Bereichsüberwachung verfügbar und minimiert die Fehlalarme durch kleine Objekte in der Erfassungszone, z. B. durch Katzen oder Hasen.
- Zeit filtern:
  - Gehen Sie zu **Radar > Szenarien**.
  - Wählen Sie ein Szenario und klicken Sie auf ⋮, um die Einstellungen zu ändern.
  - Stellen Sie unter **Seconds until trigger (Sekunden bis Auslösung)** einen höheren Wert ein. Dies ist die Verzögerungszeit zwischen dem Beginn der radargestützten Objektverfolgung und Auslösung eines Alarms. Der Timer startet, wenn das Radar zuerst ein Objekt erkennt, und nicht, wenn das Objekt den spezifischen Einschlussbereich im Szenario betritt.
- Objekttyp filtern:
  - Gehen Sie zu **Radar > Szenarien**.
  - Wählen Sie ein Szenario und klicken Sie auf ⋮, um die Einstellungen zu ändern.
  - Wenn bei bestimmten Objekttypen kein Ereignis ausgelöst werden soll, entfernen Sie diejenigen Objekttypen aus der Auswahl, die in diesem Szenario keine Ereignisse auslösen sollen.

Video ansehen und aufnehmen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts. Weitere Informationen zum Streamen und Speichern finden Sie unter .

Bandbreite und Speicher reduzieren

Wichtig

Eine Reduzierung der Bandbreite kann zum Verlust von Details im Bild führen.

1. Gehen Sie zu **Radar > Videostream**.
2. Klicken Sie in der Live-Ansicht auf .
3. Wählen Sie **Video format (Videoformat) H.264** aus.
4. Gehen Sie zu **Radar > Videostream > Allgemein** und erhöhen Sie die **Komprimierung**.

Hinweis

Die meisten Webbrowser unterstützen nicht das Dekodieren von H.265. Aus diesem Grund unterstützt das Gerät es auf dessen Weboberfläche nicht. Stattdessen können Sie auf ein Video Management System oder eine Anwendung zurückgreifen, die das Decodieren von H.265 unterstützt.

Einrichtung eines Netzwerk-Speichers

Um Aufzeichnungen im Netzwerk zu speichern, müssen Sie Ihren Netzwerk-Speicher einrichten.

1. Gehen Sie auf **System > Storage (System > Speicher)**.
2. Klicken Sie unter **Network storage (Netzwerk-Speicher)** auf **Add network storage (Netzwerk-Speicher hinzufügen)**.
3. Geben Sie die IP-Adresse des Host-Servers an.
4. Geben Sie unter **Network share (Netzwerk-Freigabe)** den Namen des freigegebenen Speicherorts auf dem Host-Server ein.
5. Geben Sie den Benutzernamen und das Kennwort ein.
6. Wählen Sie die SMB-Version aus oder lassen Sie **Auto** stehen.
7. Wählen Sie **Add share without testing (Freigabe ohne Test hinzufügen)**, wenn vorübergehende Verbindungsprobleme auftreten oder die Freigabe noch nicht konfiguriert ist.
8. Klicken Sie auf **Hinzufügen**.

Video aufzeichnen und ansehen

Video direkt vom Radar aufzeichnen

1. Gehen Sie zu **Radar > Videostream**.
2. Um eine Aufzeichnung zu starten, klicken Sie auf .

   Wenn Sie noch keinen Speicher eingerichtet haben, klicken Sie auf und . Anweisungen zum Einrichten des Netzwerk-Speichers finden Sie unter
3. Um die Aufzeichnung anzuhalten, klicken Sie erneut auf .

Video ansehen

1. Gehen Sie auf **Recordings (Aufzeichnungen)**.
2. Klicken Sie auf für Ihre Aufzeichnung in der Liste.

Eine PTZ-Kamera mittels Radarmelder steuern

Die vom Radar gemeldete Position eines Objekts kann zur Objektverfolgung durch die PTZ-Kamera verwendet werden. Dies kann auf zwei Arten erfolgen:

- . Verwenden Sie diese eingebaute Option, wenn Sie eine PTZ-Kamera und einen Radar dicht nebeneinander montiert haben.
- . Die Windows-Anwendung eignet sich, wenn Sie mehrere PTZ-Kameras und Radare zur Verfolgung von Objekten verwenden möchten.

Hinweis

Verwenden Sie zur Uhrzeitsynchronisation der Kameras, Radargeräten und des Windows-Rechners einen NTP-Server. Bei nicht synchronisierter Uhrzeit kann es zu Verzögerungen bei der Objektverfolgung oder zu Phantomverfolgungen kommen.

Steuern Sie eine PTZ-Kamera mit dem integrierten Radar-Objektverfolgungsdienst

Die integrierte Radar-Objektverfolgung schafft eine Edge-to-Edge-Lösung, bei der das Radar die PTZ-Kamera direkt steuert. Sie unterstützt alle Axis PTZ-Kameras.

Hinweis

Sie können den integrierten Radar-Objektverfolgungsdienst nutzen, um ein Radar mit einer PTZ-Kamera zu verbinden. Für ein Setup, bei dem Sie mehr als eine Radar- oder PTZ-Kamera verwenden möchten, verwenden Sie AXIS Radar Autotracking for PTZ. Weitere Informationen finden Sie unter .

In dieser Anleitung wird erklärt, wie man den Radar mit einer PTZ-Kamera koppelt, wie man die Geräte kalibriert und wie man die Verfolgung von Objekten einrichtet.

Vorbereitungen:

- Wählen Sie den Bereich aus und vermeiden Sie unerwünschte Alarme, indem Sie Ausschlussbereiche für das Radar festlegen. Achten Sie darauf, Bereiche mit radarreflektierenden Materialien oder schaukelnden Objekten, wie z. B. Laub, auszuschließen, damit die PTZ-Kamera keine irrelevanten Objekte verfolgt. Anweisungen finden Sie unter .

Koppeln Sie das Radar mit der PTZ-Kamera:

1. Rufen Sie **System > Edge-to-edge > PTZ pairing (System > Edge-to-Edge > PTZ-Kopplung)** auf.
2. Geben Sie die IP-Adresse, den Benutzernamen und das Passwort für die PTZ-Kamera ein.
3. **Connect (Verbinden)** anklicken.
4. Klicken Sie auf **Configure Radar autotracking (Radar-Objektverfolgung konfigurieren)** oder rufen Sie **Radar > Radar PTZ autotracking (Automatische PTZ-Objektverfolgung per Radar)** auf, um die Radar-Objektverfolgung einzurichten.

Kalibrieren Sie das Radar und die PTZ-Kamera:

5. Rufen Sie **Radar > Radar PTZ autotracking (Automatische PTZ-Objektverfolgung per Radar)** auf.
6. Um die Montagehöhe der Kamera festzulegen, gehen Sie zu **Camera mounting height (Kameramontagehöhe)**.
7. Um die PTZ-Kamera so zu schwenken, dass sie in die gleiche Richtung wie das Radar zeigt, gehen Sie zu **Pan alignment (Schwenkausrichtung)**.
8. Wenn Sie die Neigung anpassen müssen, um einen geneigten Boden auszugleichen, gehen Sie zu **Ground incline offset (Bodenneigungsversatz)** und fügen Sie einen Versatz in Grad hinzu.

Richten Sie die PTZ-Verfolgung ein:

9. Gehen Sie zu **Track (Verfolgen)**, wenn Menschen, Fahrzeuge und/oder unbekannte Objekte verfolgt werden sollen.
10. Um Objekte mit der PTZ-Kamera zu verfolgen, **Tracking (Automatisches Nachführen)** aktivieren. Beim automatischen Nachführen zoomt die Kamera automatisch auf ein Objekt oder eine Gruppe von Objekten, um sie im Sichtfeld zu behalten.

11. Aktivieren Sie **Object switching (Objektwechsel)**, wenn Sie mehrere Objekte erwarten, die nicht in die Kameraansicht passen.
    Bei dieser Einstellung gibt das Radar den zu verfolgenden Objekten Priorität.
12. Um zu bestimmen, wie viele Sekunden jedes Objekt verfolgt werden soll, legen Sie **Object hold time (Objekthaltezeit)** fest.
13. Das Wahlfeld **Zurück zur Ausgangsposition** aktivieren, um die PTZ-Kamera zur Ausgangsposition zurückkehren zu lassen, wenn das Radar keine Objekte mehr verfolgt.
14. Die Funktion **Timeout Zurück zur Startposition** legt fest, wie lange die PTZ-Kamera auf die letzte bekannten Position der verfolgten Objekte ausgerichtet bleibt, bevor sie zur Startposition zurückkehrt.
15. Um den Zoom der PTZ-Kamera fein abzustimmen, passen Sie den Zoom am Schieberegler an.

Steuern einer PTZ-Kamera mit AXIS Radar Autotracking for PTZ

AXIS Radar Autotracking for PTZ ist eine serverbasierte Lösung, die verschiedene Setups bei der Verfolgung von Objekten bewältigen kann:

- Steuerung mehrerer PTZ-Kameras mit einem Radar.
- Steuerung einer PTZ-Kamera mit mehreren Radars.
- Steuerung mehrerer PTZ-Kameras mit mehreren Radars.
- Steuerung einer PTZ-Kamera mit einem Radar bei Montage in unterschiedlichen Positionen und Abdeckung ein und desselben Erfassungsbereichs.

Die Anwendung ist mit einem bestimmten Satz von PTZ-Kameras kompatibel. Weitere Informationen finden Sie unter *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*.

Laden Sie die Anwendung herunter und lesen Sie im Benutzerhandbuch nach, wie Sie die Anwendung einrichten. Weitere Informationen finden Sie unter *axis.com/products/axis-radar-autotracking-for-ptz/support*.

Einrichten von Regeln für Ereignisse

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

Lösen Sie eine Aktion aus

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

Hinweis

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

Benachrichtigung bei Öffnen des Gehäuses auslösen

In diesem Beispiel wird erklärt, wie Sie eine E-Mail-Benachrichtigung einrichten, die bei Öffnen des Gehäuses versendet wird.

Einen E-Mail-Empfänger hinzufügen:

1. Rufen Sie **System (System) > Events (Ereignisse) > Recipients (Empfänger)** auf und klicken Sie auf **Empfänger hinzufügen**.
2. Geben Sie den Namen des Empfängers ein.

3. Wählen Sie **Email (E-Mail)** als Benachrichtigungsart.
4. Geben Sie die E-Mail-Adresse des Empfängers ein.
5. Geben Sie die E-Mail-Adresse ein, an die die Kamera die Benachrichtigungen senden soll.
6. Geben Sie die Anmeldedaten für das sendende E-Mail-Konto sowie den SMTP-Hostnamen und die Portnummer ein.
7. Um Ihren E-Mail-Setup zu testen, klicken Sie auf **Test (Testen)**.
8. **Save (Speichern)** anklicken.

Eine Regel erstellen:

9. Gehen Sie zu **System > Ereignisse > Regeln** und klicken Sie auf **Regel hinzufügen**.
10. Geben Sie einen Namen für die Regel ein.
11. Wählen Sie aus der Liste der Bedingungen **Gehäuse wird geöffnet**.
12. Wählen Sie in der Aktionsliste **Benachrichtigung an E-Mail senden**.
13. Wählen Sie einen Empfänger aus der Liste aus.
14. Geben Sie einen Betreff und eine Nachricht für die E-Mail ein.
15. **Save (Speichern)** anklicken.

Video von einer Kamera aufzeichnen, wenn eine Bewegung erkannt wird.

Dieses Beispiel erläutert, wie der Radarmelder und eine Kamera so eingerichtet werden, dass auf der SD-Karte eine Aufzeichnung gespeichert wird, die 5 Sekunden vor der Bewegungserfassung einsetzt und eine Minute danach endet.

Die Geräte verbinden:

1. Schließen Sie ein Kabel an einem E/A-Ausgang am Radarmelder und an einen E/A-Eingang an der Kamera an.

Den E/A-Port der Radarmelders konfigurieren:

2. Gehen Sie zu **Einstellungen > Zubehör > E/A-Ports** und konfigurieren Sie den E/A-Port als Ausgang und wählen Sie den normalen Status.

Eine Regel im Radarmelder erstellen:

3. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
4. Geben Sie einen Namen für die Regel ein.
5. Wählen Sie aus der Liste der Bedingungen unter **Radarbewegung**ein Szenario.
   Informationen zum Einrichten eines Szenarios finden Sie unter .
6. Wählen Sie aus der Liste der Aktionen die Option **E/A umschalten, während die Regel aktiv ist** und wählen Sie dann den Port aus, an dem Kamera angeschlossen ist.
7. **Save (Speichern)** anklicken.

Den E/A-Port der Kamera konfigurieren:

8. Gehen Sie zu **Einstellungen > Zubehör > E/A-Ports** und konfigurieren Sie den E/A-Port als Eingang und wählen Sie den normalen Status.

Erstellen Sie eine Regel in der Kamera:

9. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
10. Geben Sie einen Namen für die Regel ein.
11. Wählen Sie aus der Liste der Bedingungen die Option **Digitaler Eingang ist aktiv** und wählen Sie dann den Port, der die Regel auslösen soll.
12. Wählen Sie **Video aufnehmen** aus der Liste der Aktionen.
13. Wählen Sie in der Liste der Speicheroptionen **SD-Karte**.
14. Ein vorhandenes Videostream-Profil auswählen oder ein neues anlegen.
15. Stellen Sie den Vorpuffer auf 5 Sekunden ein.

16. Stellen Sie den Nachpuffer auf 1 Minute ein.
17. **Save (Speichern)** anklicken.

Lichtquelle einschalten, wenn eine Bewegung erkannt wird

Das Einschalten einer Lichtquelle, wenn ein Eindringling in den Erfassungsbereich eindringt, kann eine abschreckende Wirkung haben und die Bildqualität einer optischen Kamera, die das Eindringen aufzeichnet, verbessern.

In diesem Beispiel wird das Einrichten des Radarmelders und eines Strahlers erläutert, damit der Strahler sich einschaltet, wenn der Radarmelder Bewegung erfasst, und sich nach einer Minute wieder ausschaltet.

Die Geräte verbinden:

1. Schließen Sie eines der Strahlerkabel über den Relaisanschluss am Radarmelder an die Stromversorgung an. Schließen Sie das andere Kabel direkt an die Stromversorgung und den Strahler an.

Den Relay-Port des Radarmelders konfigurieren:

2. Gehen Sie zu **System > Zubehör > E/A-Ports** und wählen Sie als Normalzustand des Relaisports **Schaltkreis offen**.

Eine Regel im Radarmelder erstellen:

3. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
4. Geben Sie einen Namen für die Regel ein.
5. Wählen Sie aus der Liste der Bedingungen unter **Radarbewegung**ein Szenario.
   Informationen zum Einrichten eines Szenarios finden Sie unter .
6. Wählen Sie in der Liste der Aktionen die Option **Toggle I/O once (E/A einmal umschalten)** aus und wählen Sie dann den Relaisport aus.
7. Wählen Sie **Aktiv**.
8. Legen Sie die **Dauer** fest.
9. **Save (Speichern)** anklicken.

E-Mail senden, wenn jemand den Radar mit einem metallischen Gegenstand abdeckt

In diesem Beispiel wird erläutert, wie Sie eine Regel erstellen, die eine E-Mail-Benachrichtigung sendet, wenn das Radar durch Abdecken mit einem metallischen Gegenstand wie Metallfolie oder -blech manipuliert wird.

Hinweis

Regeln für Radarmanipulationsereignisse können unter AXIS OS 11.11 erstellt werden.

Einen E-Mail-Empfänger hinzufügen:

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

Eine Regel erstellen:

8. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
9. Geben Sie einen Namen für die Regel ein.

10. Wählen Sie in der Liste der Bedingungen unter **Device status (Gerätestatus)** die Option **Radar data failure (Radardatenfehler)** aus.
11. Wählen Sie unter **Reason (Grund)** die Option **Tampering (Manipulation)** aus.
12. Wählen Sie in der Liste der Aktionen unter **Notifications (Benachrichtigungen)** die Option **Send notification to email (Benachrichtigung an E-Mail senden)** aus.
13. Wählen Sie den von Ihnen erstellten Empfänger aus.
14. Geben Sie einen Betreff und eine Nachricht für die E-Mail ein.
15. **Save (Speichern)** anklicken.

Weboberfläche

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

Hinweis

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

Hauptmenü anzeigen oder ausblenden.

Zugriff auf die Versionshinweise.

Auf die Hilfe zum Produkt zugreifen.

Ändern Sie die Sprache.

Helles oder dunkles Design einstellen.

Das Benutzermenü enthält:

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

Das Kontextmenü enthält:

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

Status

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.

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.

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.

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.

Radar

Einstellungen

Allgemeines

Radar transmission (Radarübertragung): Verwenden Sie diese Option, um das Radarmodul vollständig auszuschalten.

Channel (Kanal) : Wählen Sie bei Problemen mit mehreren Geräten, die sich gegenseitig stören, denselben Kanal für maximal vier in unmittelbarer Nähe zueinander angeordnete Geräte aus. Wählen Sie im Normalfall die Option **Auto**, damit die Geräte automatisch den zu verwendenden Kanal aushandeln.

Mounting height (Montagehöhe): Geben Sie hier die Montagehöhe des Geräts ein.

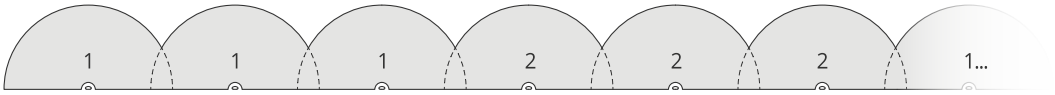
Hinweis

Geben Sie die Montagehöhe so genau wie möglich an, damit das Gerät radargestützte Bewegungserfassungen an der richtigen Stelle im Bild anzeigen kann.

Koexistenz

Anzahl benachbarter Radargeräte: Wählen Sie die Anzahl der Radare, die in demselben Koexistenzbereich installiert sind. Dadurch werden Störungen vermieden. Der Koexistenzradius beträgt 350 m.

- **0–1**: Wählen Sie diese Option, wenn Sie ein bis zwei Radare in demselben Koexistenzbereich installieren.
- **2**: Wählen Sie diese Option, wenn Sie drei Radare in demselben Koexistenzbereich installieren.
- **3–5**: Wählen Sie diese Option, wenn Sie vier bis sechs Radare in demselben Koexistenzbereich installieren.
  - **Gruppen**: Wählen Sie eine Gruppe (**Gruppe 1** oder **Gruppe 2**) für Ihren Radar aus. Dadurch lassen sich Störungen vermeiden. Wir empfehlen Ihnen, jeder Gruppe drei Radare hinzuzufügen und die Radare, die sich am nächsten zueinander befinden, derselben Gruppe hinzuzufügen.



Weitere Informationen finden Sie unter .

Erfassung

Detection sensitivity (Erfassungsempfindlichkeit): Wählen Sie hier die gewünschte Radar-Empfindlichkeit aus. Ein höherer Wert bedeutet einen größeren Erfassungsbereich, aber auch ein höhere Gefahr von Fehlalarmauslösungen. Eine geringere Empfindlichkeit verringert die Anzahl der Fehlalarme, kann aber den Erfassungsbereich verkürzen.

Radarprofil: Wählen Sie ein Profil für Ihren ausgewählten Bereich aus.

- **Area monitoring (Bereichsüberwachung)**: Verfolgen Sie große und kleine Objekte, die sich bei geringerer Geschwindigkeit in offenen Bereichen bewegen.
  - **Ignore stationary rotating objects (Rotierende stationäre Objekte ignorieren)** : Schalten Sie diese Option ein, um Fehlalarme, die von stationären Objekten mit Drehbewegungen, beispielsweise von Lüftern oder Turbinen, verursacht werden, zu minimieren.
  - **Ignore small objects (Kleine Objekte ignorieren)**: Aktivieren Sie diese Option, um die Fehlalarme durch kleine Objekte wie Katzen oder Hasen zu minimieren.
  - **Schaukelnde Objekte ignorieren**: Aktivieren Sie diese Option, um die Fehlalarme aufgrund von schaukelnden Objekten wie Bäumen, Büschen oder Fahnenmasten zu minimieren.
- **Road monitoring (Straßenüberwachung)**: Verfolgung von Fahrzeugen mit einer höheren Geschwindigkeit in Stadtgebieten und auf Vorortstraßen
  - **Ignore stationary rotating objects (Rotierende stationäre Objekte ignorieren)** : Schalten Sie diese Option ein, um Fehlalarme, die von stationären Objekten mit Drehbewegungen, beispielsweise von Lüftern oder Turbinen, verursacht werden, zu minimieren.
  - **Schaukelnde Objekte ignorieren**: Aktivieren Sie diese Option, um die Fehlalarme aufgrund von schaukelnden Objekten wie Bäumen, Büschen oder Fahnenmasten zu minimieren.

Ansehen

Information legend (Zeichenerklärung): Aktivieren Sie diese Option, um eine Erklärung mit den Objekttypen anzeigen zu lassen, die vom Radar erfasst und verfolgt werden können. Verschieben Sie die Zeichenerklärung per Drag & Drop.

Zonentransparenz: Wählen Sie die Abdeckungsstärke bzw. Transparenz des Abdeckungsbereichs aus.

Gittertransparenz: Wählen Sie die Abdeckungsstärke bzw. Transparenz des Rasters aus.

Farbschema: Wählen Sie hier ein Erscheinungsbild für die Radar-Darstellung aus.

Rotation (Drehung) : Wählen Sie die bevorzugte Ausrichtung des Radarbilds.

Objektvisualisierung

Trail lifetime (Spurdauer): Wählen Sie aus, wie lange die Spur eines verfolgten Objekts in der Radaransicht zu sehen ist.

Icon style (Symbolstil): Wählen Sie die Symbolart für die verfolgten Objekte in der Radaransicht. Wählen Sie für einfache Dreiecke die Option **Dreieck**. Wählen Sie für darstellende Symbole die Option **Symbol**. Die Symbole zeigen unabhängig vom Format in die Richtung, in der sich die verfolgten Objekte bewegen.

Informationsanzeige neben Symbol: Wählen Sie aus, welche Informationen neben dem Symbol des verfolgten Objekts angezeigt werden sollen:

- **Object type (Objekttyp)**: Zeigt den vom Radarmelder erkannten Objekttyp an.
- **Classification probability (Klassifizierungswahrscheinlichkeit)**: Zeigt, wie zuverlässig die radargestützte Objektklassifizierung ist.
- **Velocity (Geschwindigkeit)**: Zeigt an, wie schnell sich das Objekt bewegt.

Videostream

Allgemeines

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

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

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

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

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

Bitrate-Steuerung

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

Kartenkalibrierung

Verwenden Sie die Kartenkalibrierung, um eine Referenzkarte hochzuladen und zu kalibrieren. Das Ergebnis der Kalibrierung ist ein Lageplan, der die Radarabdeckung im richtigen Maßstab anzeigt, wodurch der Ort von Objektbewegungen besser zu erkennen ist.

Einrichtungsassistent: Hierüber öffnen Sie den Setup-Assistenten, der Sie Schritt für Schritt durch die Kalibrierung führt.

Kalibrierung zurücksetzen: Hierüber entfernen Sie das aktuelle Kartenbild und die Radarposition auf der Karte.

Lageplan

Karte hochladen: Wählen Sie das hochzuladende Kartenbild aus oder legen Sie es per Drag & Drop ab.

Karte herunterladen: Klicken Sie hier, um die Karte herunterzuladen.

Rotate map (Karte drehen): Mit dem Schieberegler können Sie die Karte drehen.

Maßstab und Entfernung auf der Karte

Entfernung: Geben Sie die Entfernung zwischen den beiden Punkten ein, die Sie der Karte hinzugefügt haben.

Karte schwenken und zoomen

Schwenken: Klicken Sie auf die jeweilige Schaltfläche, um das Kartenbild zu schwenken.

Zoom: Klicken Sie auf die jeweilige Schaltfläche, um das Kartenbild größer oder kleiner darzustellen.

Schwenken und Zoomen zurücksetzen: Klicken Sie hier, um die Einstellungen zum Schwenken und Zoomen zurückzusetzen.

Radarposition

Position: Klicken Sie auf die jeweilige Schaltfläche, um den Radar auf der Karte zu verschieben.

Drehung: Klicken Sie auf die jeweilige Schaltfläche, um den Radar auf der Karte zu drehen.

Ausschlussbereiche

Ein Ausschlussbereich (**exclude zone**) ist ein Bereich, in dem sich bewegende Objekte ignoriert werden. Verwenden Sie Ausschlussbereiche, wenn innerhalb eines Szenarios Bereiche vorhanden sind, die häufig Fehlalarme auslösen.

+ : Klicken Sie auf die Schaltfläche, um einen neuen Ausschlussbereiche zu erstellen.

Um einen Ausschlussbereich zu ändern, wählen Sie diesen aus der Liste aus.

Track passing objects (Passierende Objekte verfolgen): Aktivieren Sie diese Ansicht, um Objekte zu verfolgen, die die Ausschlusszone passieren. Passierende Objekte behalten ihre Track-IDs und sind in der gesamten Zone sichtbar. Objekte, die aus dem Ausschlussbereich kommen, werden nicht verfolgt.

Zone shape presets (Voreinstellungen für Bereichsformen): Die Form des Ausschlussbereichs wählen.

- **Cover everything (Alles abdecken)**: Wählen Sie diese Option aus, um eine Ausschlusszone zu wählen, die den gesamten Bereich des Radarbereichs abdeckt.
- **Reset to box (Auf Feld zurücksetzen)**: Wählen Sie diese Option aus, um eine rechteckige Ausschlusszone in der Mitte des Abdeckungsbereichs zu platzieren.

Um die Form der Zone zu ändern, ziehen Sie einen beliebigen Punkt auf die Linien und legen ihn dort ab. Um einen Punkt zu entfernen, klicken Sie diesen mit der rechten Maustaste an.

Szenarien

Ein Szenario ist eine Kombination aus Auslösebedingungen sowie Szenen- und Erfassungseinstellungen.

+ : Klicken Sie auf die Schaltfläche, um ein neues Szenarien zu erstellen. Sie können bis zu 20 Szenarien erstellen.

Triggering conditions (Auslösebedingungen): Wählen Sie die Bedingung aus, die Alarme auslöst.

- **Movement in area (Bewegung im Bereich)**: Wählen Sie aus, ob die Auslösung des Szenarios bei Objekten erfolgen soll, die sich in einem bestimmten Bereich bewegen.
- **Linienübergang**: Wählen Sie aus, ob das Szenario für eine oder zwei Linien überschreitende Objekte ausgelöst werden soll.

Scene (Szene): Definieren Sie den Bereich bzw. die Linien des Szenarios, in dem bewegliche Objekte Alarme auslösen.

- Wählen Sie für **Movement in area (Bewegung im Bereich)** eine vorgegebene Form aus, um den Erfassungsbereich zu ändern.
- Ziehen Sie für **Line crossing (Linienüberquerung)** die Linie per Drag and Drop in die Szene. Um weitere Punkte auf der Linie zu erstellen, klicken Sie auf die Linie und ziehen den Punkt an die gewünschte Stelle. Um einen Punkt zu entfernen, klicken Sie diesen mit der rechten Maustaste an.
  - **Require crossing of two lines (Überschreiten von zwei Linien erforderlich)**: Aktivieren Sie dieses Signal, wenn das Objekt zwei Linien überqueren muss, bevor das Szenario einen Alarm auslöst.
  - **Richtung ändern:** Aktivieren Sie dies, wenn für das Szenario ein Alarm ausgelöst werden soll, wenn Objekte die Linie in die andere Richtung überqueren.

Detection settings (Erfassungseinstellungen): Festlegung der Auslösekriterien für das Szenario.

- Für **Movement in area (Bewegung im Bereich)**:
  - **Ignore short-lived objects (Kurzlebige Objekte ignorieren)**: Legen Sie die Verzögerung in Sekunden fest, ab der das Radar das Objekt erkennt, bis das Szenario einen Alarm auslöst. Auf diese Weise lassen sich Fehlalarme reduzieren.
  - **Trigger on object type (Auslösung nach Objekttyp)**: Wählen Sie den Typ der Objekte (Mensch, Fahrzeug, unbekannt), für die das Szenario ausgelöst werden soll.
  - **Speed limit (Grenzgeschwindigkeit)**: Auslöser für Objekte, die sich in einer bestimmten Geschwindigkeit innerhalb eines bestimmten Bereichs bewegen.
    - **Invert (Invertieren)**: Wählen Sie diese Option aus, wenn Geschwindigkeiten oberhalb oder unterhalb der festgelegten Höchstgeschwindigkeit Auslöser sein sollen.
- Für **Line crossing (Linienübergang)**:
  - **Ignore short-lived objects (Kurzlebige Objekte ignorieren)**: Legen Sie die Verzögerung in Sekunden fest, ab der das Radar das Objekt erkennt, bis das Szenario eine Aktion auslöst. Auf diese Weise lassen sich Fehlalarme reduzieren. Diese Option ist nicht verfügbar für Objekte, die zwei Linien überschreiten.
  - **Max time between crossings (Max. Zeit zwischen Übertritten)**: Legen Sie die maximale Zeit zwischen dem Überschreiten der ersten und der zweiten Linie fest. Diese Option ist nur verfügbar für Objekte, die zwei Linien überschreiten.
  - **Trigger on object type (Auslösung nach Objekttyp)**: Wählen Sie den Typ der Objekte (Mensch, Fahrzeug, unbekannt), für die das Szenario ausgelöst werden soll.
  - **Speed limit (Grenzgeschwindigkeit)**: Auslöser für Objekte, die sich in einer bestimmten Geschwindigkeit innerhalb eines bestimmten Bereichs bewegen.
    - **Invert (Invertieren)**: Wählen Sie diese Option aus, wenn Geschwindigkeiten oberhalb oder unterhalb der festgelegten Höchstgeschwindigkeit Auslöser sein sollen.

Alarm settings (Alarmeinstellungen): Definieren Sie die Kriterien für den Alarm.

- **Minimum trigger duration (Mindestdauer des Auslösers)**: Legen Sie die Mindestdauer für den ausgelösten Alarm fest.

Overlays

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

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

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

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

Automatische PTZ-Objektverfolgung per Radar

Koppeln Sie das Radar mit einer PTZ-Kamera, um die Radar-Objektverfolgung zu verwenden. Wechseln Sie zum Herstellen der Verbindung zu **System > Edge-to-edge**.

Anfangseinstellungen konfigurieren:

Camera mounting height (Montagehöhe der Kamera): Entfernung zwischen Boden und Montageposition der PTZ-Kamera.

Schwenkausrichtung: Schwenken Sie die PTZ-Kamera so, dass sie in die gleiche Richtung wie das Radar weist. Um auf die PTZ-Kamera zuzugreifen, die IP-Adresse der Kamera anklicken.

Schwenkausgleich speichern: Klicken Sie hier, um die Schwenkausrichtung zu speichern.

Ausgleich Bodenneigung: Verwenden Sie den Ausgleich der Bodenneigung, um die Neigung der Kamera zu optimieren. Wenn der Boden geneigt ist oder die Kamera nicht horizontal montiert ist, kann es sein, dass die Kamera beim Verfolgen eines Objekts zu hoch oder niedrig abtastet.

Done (Fertig): Klicken Sie hier, um Ihre Einstellungen zu speichern, und fahren Sie mit der Konfiguration fort.

PTZ-Objektverfolgung konfigurieren:

Verfolgen: Wählen Sie diese Option aus, wenn Menschen, Fahrzeuge und/oder unbekannte Objekte verfolgt werden sollen.

Automatisches Nachführen: Um Objekte mit der PTZ-Kamera zu verfolgen, Automatisches Nachführen aktivieren. Beim automatischen Nachführen zoomt die Kamera automatisch auf ein Objekt oder eine Gruppe von Objekten, um sie im Sichtfeld zu behalten.

Objektwechsel: Wenn das Radar mehrere Objekte erfasst, die nicht vom Sichtfeld der PTZ-Kamera erfasst werden, verfolgt die PTZ-Kamera das vom Radar mit der höchsten Priorität eingestufte Objekt und ignoriert die anderen.

Objekthaltezeit: Legt fest, wie viele Sekunden die PTZ-Kamera jedes Objekt verfolgt.

Zurück zur Ausgangsposition: Aktivieren Sie diese Option, um die PTZ-Kamera zur Home-Position zurückkehren zu lassen, wenn das Radar keine Objekte mehr verfolgt.

Return to home timeout (Zeitüberschreitung Zurück zur Ausgangsposition): Legt fest, wie lange die PTZ-Kamera auf die letzte bekannten Position der verfolgten Objekte ausgerichtet bleibt, bevor sie zur Startposition zurückkehrt.

Zoom: Mit dem Schieberegler können Sie den Zoom der PTZ-Kamera fein abstimmen.

Reconfigure installation (Installation neu konfigurieren): Klicken Sie, um alle Einstellungen zu löschen, und wechseln Sie zur anfänglichen Konfiguration.

Aufzeichnungen

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

- Starten einer Aufzeichnung des Geräts.

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

- Beenden einer Aufzeichnung des Geräts.

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

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

Die Aufzeichnung wiedergeben.

Abspielen der Aufzeichnung anhalten.

Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

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

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

Klicken Sie auf , um eine Aufzeichnung zu löschen.

Exportieren: Exportieren der ganzen Aufzeichnung oder eines Teils davon.

Klicken Sie darauf, um die Aufzeichnungen zu filtern.

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

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

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

Ereignis: Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Speicher: Zeigt Aufzeichnungen nach Speichertyp.

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

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

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

Hinweis

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

Gerätestandort

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

- **Formatieren**: Wählen Sie das Format für die Eingabe des Breiten- und Längengrads Ihres Geräts.
- **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.

Regionale Einstellungen

Wählt das Messsystem aus, das in allen Systemeinstellungen verwendet werden soll.

Metric (m, km/h) (Metrisch): Wählen Sie diese Option, damit der Abstand in Metern und Geschwindigkeit in Kilometern pro Stunde gemessen wird.

U.S. customary (ft, mph) (USA (Fuß, mph): Wählen Sie diese Option, damit der Abstand in Fuß und Geschwindigkeit in Meilen pro Stunde gemessen wird.

Netzwerk

IPv4

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

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

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

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

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

Hinweis

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

IPv6

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

Hostname

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

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

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

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

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

DNS-Server

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

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

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

HTTP und HTTPS

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

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

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

Hinweis

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

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

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

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

Netzwerk-Erkennungsprotokolle

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

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

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

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

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

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

Globale Proxys

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

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

Unterstützte HTTP- und HTTPS-Proxy-Formate:

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

Hinweis

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

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

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

One-Click Cloud Connect

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

O3C zulassen:

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

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

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

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

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

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

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

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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

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

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

Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher) :

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

Network access control and encryption (Netzwerkzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Zertifikate

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Brute-Force-Angriffe verhindern

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

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

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

Firewall

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

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

- **ACCEPT (AKZEPTIEREN):** Ermöglicht alle Verbindungen mit dem Gerät. Diese Option ist in der Standardeinstellung festgelegt.
- **DROP (VERWERFEN):** 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 Geräts ein, das Sie zulassen oder blockieren möchten.
  - **Port range (Portbereich)**: Wählen Sie diese Option, um den Bereich der 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 (GRENZE)**: 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 Geräts ein, das Sie zulassen oder blockieren möchten.
  - **Port range (Portbereich)**: Wählen Sie diese Option, um den Bereich der 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 (Menge)**.
- **Amount (Menge)**: Stellen Sie ein, wie oft ein Gerät innerhalb des eingestellten **Zeitraums** maximal eine Verbindung herstellen darf. Der Höchstbetrag liegt bei 65535.
- **Burst (Impulspaket)**: Geben Sie die Anzahl der Verbindungen ein, die die eingestellte **Menge** einmal während des eingestellten **Zeitraums** überschreiten dürfen. Sobald die Anzahl erreicht ist, ist nur noch die festgelegte Menge während des festgelegten Zeitraums zulässig.
- **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 prüfen.

- **Test time in seconds: (Prüfungszeit 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 Überprüfung 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.

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.

Client Credentials Grant Configuration (Konfiguration der Client-Zugangsdaten-Genehmigung)

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

Überprüfungs-URI (Provider-URL): Geben Sie den Weblink für die API-Endpunkt-Authentifizierung ein.

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

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

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

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

OpenID-Konfiguration

Wichtig

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

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

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

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.

Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

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

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

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

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

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

Empfänger

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

Hinweis

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

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

Hinweis

Sie können bis zu 20 Empfänger erstellen.

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

Name: Geben Sie den Name des Empfängers ein.

Typ: Aus der Liste auswählen:

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

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

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

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

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

Hinweis

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

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

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

⋮ Das Kontextmenü enthält:

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

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

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

Zeitschemata

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

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

Manuelle Auslöser

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

MQTT

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

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

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

ALPN

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

MQTT-Client

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

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

Broker

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

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

Port: Geben Sie die Portnummer ein.

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

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

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

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

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

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

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

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

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

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

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

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

Nachricht zum Verbindungsaufbau

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

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

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

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

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

Nachricht zum letzten Willen und Testament

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

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

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

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

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

MQTT-Warteschlange

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

Include topic name (Themanamen einschließen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

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

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

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

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

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

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

MQTT-Abonnements

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

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

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

Abonnementart:

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

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

MQTT-Overlays

Hinweis

Stellen Sie eine Verbindung mit einem MQTT-Broker her, bevor Sie MQTT-Overlay-Modifikatoren hinzufügen.

Overlay-Modifikator hinzufügen: Klicken Sie hier, um einen neuen Overlay-Modifikator hinzuzufügen.

Themenfilter: Fügen Sie das MQTT-Thema hinzu, das die Daten enthält, die im Overlay angezeigt werden sollen.

Datenfeld: Geben Sie den Schlüssel für die Nutzdaten der Nachricht an, die Sie im Overlay anzeigen möchten, vorausgesetzt, die Nachricht ist im JSON-Format.

Modifikator: Verwenden Sie beim Erstellen des Overlays den resultierenden Modifikator.

- Modifikatoren, die mit **#XMP** beginnen, zeigen alle vom Thema empfangenen Daten an.
- Modifikatoren, die mit **#XMD** beginnen, zeigen die im Datenfeld angegebenen Daten an.

Speicherung

Netzwerk-Speicher

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

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

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

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

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

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

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

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

Werkzeuge

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

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

Onboard-Speicher

Wichtig

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

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

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

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

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

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

Werkzeuge

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

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

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

Videostromprofile

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

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

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

Name: Fügen Sie einen Namen für Ihr Profil hinzu.

Beschreibung: Fügen Sie eine Profilbeschreibung hinzu.

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

Auflösung: Siehe für eine Beschreibung dieser Einstellung.

Bildrate: Siehe für eine Beschreibung dieser Einstellung.

Komprimierung: Siehe für eine Beschreibung dieser Einstellung.

Zipstream : Siehe für eine Beschreibung dieser Einstellung.

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

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

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

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

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

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

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

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

Über ONVIF

ONVIF-Konten

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

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

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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Role (Rolle):

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

Das Kontextmenü enthält:

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

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

ONVIF-Medienprofile

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

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

Profilname: Fügen Sie einen Namen für das Medienprofil hinzu.

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

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

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

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

Hinweis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Melder

Stoßerfassung

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

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

Zubehör

E/A-Ports

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

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

Port

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

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

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

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

Hinweis

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

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

Edge-to-Edge

Kopplung

Durch Kopplung können kompatible Geräte von Axis so eingesetzt werden, als seien sie Teil des Hauptgeräts.

Audio-Kopplung ermöglicht die Kopplung mit einem Netzwerk-Lautsprecher oder -Mikrofon. Nach den Kopplung fungiert der Netzwerk-Lautsprecher als Audioausgabegerät, mit dem Audioclips abgespielt und Audio über die Kamera übertragen kann. Das Netzwerkmikrofon nimmt Geräusche aus der Umgebung auf und stellt sie als Audioeingabegerät zur Verfügung, das in Medienstreams und Aufnahmen verwendet werden kann.

Wichtig

Um diese Funktion mit einer Video Management Software (VMS) verwenden zu können, koppeln Sie zuerst die Kamera mit dem Lautsprecher oder Mikrofon und fügen dann Ihrer VMS die Kamera hinzu.

Legen Sie in der Ereignisregel ein Limit für „Zwischen Aktionen warten (hh:mm:ss)" fest, wenn Sie ein mit dem Netzwerk gekoppeltes Audiogerät in einer Ereignisregel mit „Audioerfassung" als Bedingung und „Wiedergabe von Audio-Clips" als Aktion verwenden. Damit wird eine Rückkopplungsschlaufe vermieden, wenn das erfassende Mikrofon Audio vom Lautsprecher mit aufnimmt.

Hinzufügen: Fügen Sie ein Gerät hinzu, mit dem Sie eine Kopplung durchführen möchten.

Discover devices (Geräte erkennen): Klicken Sie hier, um Geräte im Netzwerk zu finden. Wenn das Netzwerk gescannt wurde, wird eine Liste der verfügbaren Geräte angezeigt.

Hinweis

In der Liste werden alle gefundenen Axis Geräte angezeigt, nicht nur Geräte, die gekoppelt werden können.

Es können nur Geräte gefunden werden, bei denen **Bonjour** aktiviert ist. Um **Bonjour** für ein Gerät zu aktivieren, öffnen Sie die Weboberfläche des Geräts und gehen Sie zu **System > Network (Netzwerk) > Network discovery protocols (Netzwerkerkennungsprotokolle)**.

Hinweis

Bei Geräten, die bereits gekoppelt wurden, wird ein Infosymbol angezeigt. Bewegen Sie den Mauszeiger über das Symbol, um Informationen über bereits aktive Kopplungen zu erhalten.

Um ein Gerät aus der Liste zu koppeln, klicken Sie auf .

Kopplungstyp auswählen: Aus dem Aufklappmenü wählen.

Speaker pairing (Lautsprecher-Kopplung): Wählen Sie diese Option, um einen Netzwerk-Lautsprecher zu koppeln.

Microphone pairing (Mikrofonkopplung) : Wählen Sie diese Option, um ein Mikrofon zu koppeln.

Adresse: Geben Sie den Host-Namen oder die IP-Adresse des Netzwerk-Lautsprechers ein.

Username (Benutzername): Geben Sie den Benutzernamen ein.

Password (Kennwort): Geben Sie ein Benutzerkennwort ein.

Close (Schließen): Klicken Sie hier, um alle Felder zu löschen.

Connect (Verbinden): Klicken Sie hier, um eine Verbindung mit dem Gerät herzustellen, mit dem Sie die Kopplung herstellen möchten.

Mit **PTZ pairing (PTZ-Kopplung)** können Sie ein Radar mit einer PTZ-Kamera koppeln, um die Objektverfolgung zu verwenden. Mit der automatischen PTZ-Objektverfolgung per Radar können Objekte anhand von Radarinformationen über die Position der Objekte von der PTZ-Kamera verfolgt werden.

Hinzufügen: Fügen Sie ein Gerät hinzu, mit dem Sie eine Kopplung durchführen möchten.

Discover devices (Geräte erkennen): Klicken Sie hier, um Geräte im Netzwerk zu finden. Wenn das Netzwerk gescannt wurde, wird eine Liste der verfügbaren Geräte angezeigt.

Hinweis

In der Liste werden alle gefundenen Axis Geräte angezeigt, nicht nur Geräte, die gekoppelt werden können.

Es können nur Geräte gefunden werden, bei denen **Bonjour** aktiviert ist. Um **Bonjour** für ein Gerät zu aktivieren, öffnen Sie die Weboberfläche des Geräts und gehen Sie zu **System > Network (Netzwerk) > Network discovery protocols (Netzwerkerkennungsprotokolle)**.

Hinweis

Bei Geräten, die bereits gekoppelt wurden, wird ein Infosymbol angezeigt. Bewegen Sie den Mauszeiger über das Symbol, um Informationen über bereits aktive Kopplungen zu erhalten.

Um ein Gerät aus der Liste zu koppeln, klicken Sie auf .

Kopplungstyp auswählen: Aus dem Aufklappmenü wählen.

Adresse: Geben Sie die IP-Adresse oder den Hostnamen der PTZ-Kamera ein.

Username (Benutzername): Geben Sie den Benutzernamen der PTZ-Kamera ein.

Password (Kennwort): Geben Sie das Kennwort für die PTZ-Kamera ein.

Close (Schließen): Klicken Sie hier, um alle Felder zu löschen.

Connect (Verbinden): Klicken Sie hier, um eine Verbindung mit der PTZ-Kamera herzustellen.

Configure radar autotracking (Radar-Objektverfolgung konfigurieren): Klicken Sie hier, um die Objektverfolgung zu öffnen und zu konfigurieren. Sie können die Konfiguration auch unter **Radar > Autotracking (Radar > Objektverfolgung)** vornehmen.

Protokolle

Protokolle und Berichte

Berichte

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

Protokolle

- **View the system log (Systemprotokoll anzeigen)**: Klicken Sie, um Informationen zu Systemereignissen, wie z. B. Gerätestart, Warnungen und wichtige Meldungen, zu sehen.
- **View the access log (Zugangsprotokoll anzeigen)**: Klicken Sie darauf, um alle fehlgeschlagenen Zugriffsversuche auf das Gerät zu sehen, bei denen z. B. ein falsches Anmeldekennwort verwendet wurde.

Remote System Log

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

+ **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.
- **Automatisches Zurücksetzen**: Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige AXIS OS-Version zurückgesetzt.

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

Fehler beheben

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)**.

Ihre Installation validieren

Installation des Radars validieren

Hinweis

Mit diesem Test können Sie Ihre Installation unter aktuellen Bedingungen validieren. Änderungen in der Szene können die Leistungsfähigkeit Ihrer Installation beeinträchtigen.

Der Radar ist nach der Installation einsatzbereit. Wir empfehlen Ihnen jedoch, vor der Verwendung eine Validierung durchzuführen. Damit lässt sich die Genauigkeit des Radars erhöhen, da auf diese Weise Probleme mit der Installation erkannt oder Objekte (z. B. Bäume und reflektierende Flächen) in der Szene werden können.

, bevor Sie mit der Validierung anfangen.

Eine Validierung sollte dann durchgeführt werden, wenn:

- Sich Objekte in der Szene vorhanden sind, die Sie ausschließen möchten, sodass die Zonen bestimmte Objekte wie Vegetation oder Metalloberflächen enthalten können.
- Sie den Radar mit einer PTZ-Kamera koppeln und **Radarverfolgung** konfigurieren möchten.
- Die Höhe der Radarhalterung geändert wurde.

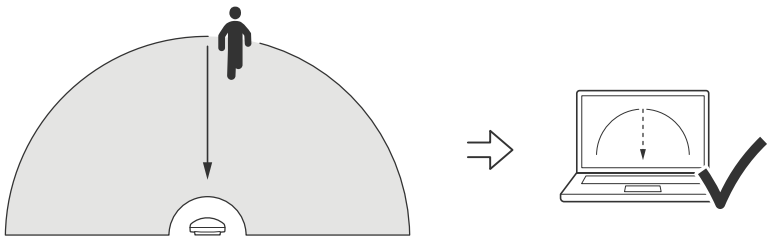
Radar validieren

Überprüfen Sie, dass keine falschen Erfassungen vorhanden sind.

1. Stellen Sie sicher, dass im Erfassungsbereich keine menschlichen Aktivitäten stattfinden.
2. Warten Sie einige Minuten, bis sichergestellt ist, dass der Radar keine statischen Objekte im Erfassungsbereich erkennt.
3. Wenn keine unerwünschten Erfassungen vorhanden sind, können Sie Schritt 4 überspringen.
4. Erfahren Sie unter Fehlalarme minimieren, wie Sie bei unerwünschten Erfassungen bestimmte Arten von Bewegungen oder Objekten herausfiltern, die Abdeckung ändern oder die Erfassungsempfindlichkeit anpassen.

Überprüfen Sie, ob das richtige Symbol und die richtige Fahrtrichtung angezeigt werden, wenn sich der Radar von vorne annähert.

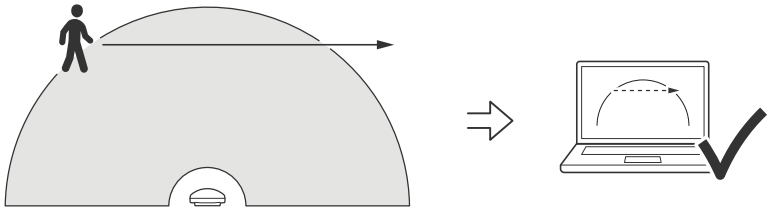
1. Gehen Sie auf die Weboberfläche des Radars und zeichnen Sie die Sitzung auf. Hilfe dazu finden Sie unter .
2. Starten Sie 60 m (197 ft) vor dem Radar und laufen Sie direkt auf den Radar zu.
3. Überprüfen Sie die Sitzung auf der Weboberfläche des Radars. Das Symbol für eine menschliche Klassifizierung sollte angezeigt werden, sofern Sie erkannt wurden.
4. Stellen Sie sicher, dass auf der Weboberfläche des Radars die korrekte Richtung angezeigt wird.



Überprüfen Sie, ob das richtige Symbol und die richtige Fahrtrichtung angezeigt werden, wenn sich der Radar von der Seite annähert.

1. Gehen Sie auf die Weboberfläche des Radars und zeichnen Sie die Sitzung auf. Hilfe dazu finden Sie unter .
2. Starten Sie 60 m (197 ft) vom Radar und durchkreuzen Sie den Abdeckungsbereich.

3. Stellen Sie sicher, dass auf der Weboberfläche des Radars das Symbol für eine menschliche Klassifizierung angezeigt wird.
4. Stellen Sie sicher, dass auf der Weboberfläche des Radars die korrekte Richtung angezeigt wird.



Erstellen Sie eine ähnliche Tabelle wie unten, um die Daten Ihrer Prüfung aufzeichnen zu können.

Test	Bestanden/Fehlgeschlagen	Kommentar
1. Überprüfen Sie, dass bei klarer Umgebung keine unerwünschten Erfassungen gemacht werden.		
2a. Überprüfen Sie, dass das Objekt mit dem richtigen Symbol für "Mensch" erkannt wird, wenn der Radar von vorne angenähert wird.		
2b. Überprüfen Sie, ob die Richtung korrekt ist, wenn der Radar von vorne angenähert wird.		
3a. Überprüfen Sie, ob das Objekt mit dem richtigen Symbol für "Mensch" erkannt wird, wenn sich der Radar von der Seite annähert.		
3b. Überprüfen Sie, ob die Richtung korrekt ist, wenn sich der Radar von der Seite annähert.		

Validierung abschließen

Nach erfolgreichem Abschluss des ersten Teils der Validierung sollten Sie zum Abschließen des Validierungsprozesses folgende Tests durchführen.

1. Stellen Sie sicher, dass Ihr Radar konfiguriert ist und befolgen Sie die Anweisungen.
2. Für eine weitere Validierung fügen Sie eine Referenzkarte hinzu und kalibrieren Sie sie.
3. Stellen Sie das Radarszenario ein, dass Daten aufgezeichnet werden, wenn ein geeignetes Objekt erkannt wird. Standardmäßig ist **Sekunden bis zum Auslösen** auf zwei Sekunden eingestellt, aber Sie können die Zahl bei Bedarf über die Weboberfläche ändern.
4. Legen Sie fest, dass der Radar Daten aufzeichnen soll, wenn ein geeignetes Objekt erkannt wird. Anweisungen finden Sie unter .
5. Legen Sie die **Dauer der Spur** auf eine Stunde fest, sodass Sie auf jeden Fall ausreichend Zeit haben, um Ihren Platz zu verlassen, zu Fuß durch den Überwachungsbereich zu gehen und zu Ihrem Platz zurückzukehren. Die **Dauer der Spur** hält in der Live-Ansicht des Radars die Verfolgung für die eingestellte Zeit aufrecht. Nach Abschluss der Validierung kann sie deaktiviert werden.
6. Gehen Sie entlang der Grenze des vom Radar abgedeckten Bereichs und vergewissern Sie sich, dass die Verfolgung auf dem System mit der Route übereinstimmt, die Sie zurückgelegt haben.

7. Wenn Sie mit den Ergebnissen Ihrer Validierung nicht zufrieden sind, kalibrieren Sie die Referenzkarte neu und wiederholen Sie die Validierung.

Mehr erfahren

Streaming und Speicher

Video-Komprimierungsformate

Die Wahl des Komprimierungsverfahrens richtet sich nach den Wiedergabeanforderungen und den Netzwerkeigenschaften. Es stehen folgende Optionen zur Verfügung:

Motion JPEG

Motion JPEG oder MJPEG ist eine digitale Videosequenz, die aus einer Reihe von einzelnen JPEG-Bildern erstellt wird. Diese Bilder werden mit einer Bildrate dargestellt und aktualisiert, die ausreicht, um einen ständig aktualisierten Videostream wiederzugeben. Um für das menschliche Auge Videobewegung darzustellen, muss die Bildrate mindestens 16 Bilder pro Sekunde betragen. Video wird bei 30 (NTSC) oder 25 (PAL) Bildern pro Sekunde als vollbewegt wahrgenommen.

Ein Videostream des Typs Motion JPEG erfordert erhebliche Bandbreite, liefert jedoch ausgezeichnete Bildqualität und ermöglicht Zugriff auf jedes einzelne Bild des Videostreams.

H.264 oder MPEG-4 Part 10/AVC

Hinweis

H.264 ist eine lizenzierte Technologie. Das Axis Produkt beinhaltet eine Lizenz zur Wiedergabe von H.264. Die Installation weiterer nicht lizenzierter Kopien des Clients ist untersagt. Für den Erwerb weiterer Lizenzen wenden Sie sich bitte an Ihren Axis Händler.

Mit H.264 kann die Größe einer digitalen Videodatei ohne Beeinträchtigung der Bildqualität im Vergleich zum Format Motion JPEG um mehr als 80 % und im Vergleich zum älteren MPEG-Formaten um mehr als 50 % reduziert werden. Das bedeutet weniger Bandbreite und Speicherplatz für eine Videodatei. Anders ausgedrückt: Bei einer bestimmten Bitrate kann eine höhere Videoqualität erzielt werden.

H.265 oder MPEG-H Part 2/HEVC

Mit H.265 kann die Größe einer digitalen Videodatei ohne Beeinträchtigung der Bildqualität im Vergleich zu H.264 um mehr als 25 % reduziert werden.

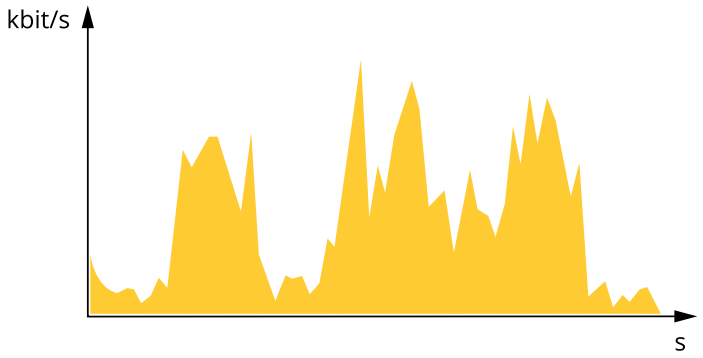
Hinweis

- H.265 ist eine lizenzierte Technologie. Das Axis Produkt beinhaltet eine Lizenz zur Wiedergabe von H.265. Die Installation weiterer nicht lizenzierter Kopien des Clients ist untersagt. Für den Erwerb weiterer Lizenzen wenden Sie sich bitte an Ihren Axis Händler.
- Die meisten Webbrowser unterstützen nicht das Dekodieren von H.265. Aus diesem Grund wird sie auf der Weboberfläche der Kamera nicht unterstützt. Stattdessen können Sie auf ein Videoverwaltungssystem oder eine Anwendung zurückgreifen, die das Decodieren von H.265 unterstützt.

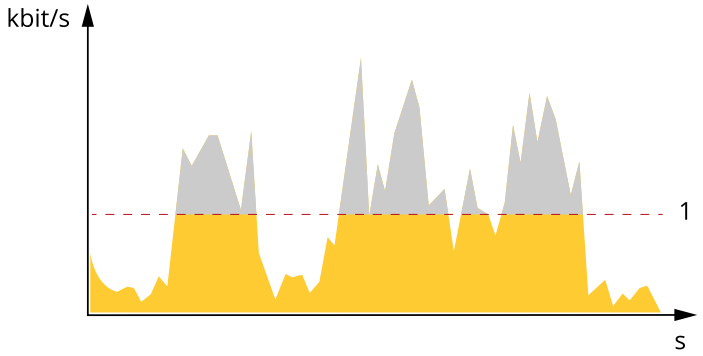
Bitrate-Steuerung

Die Bitratensteuerung hilft Ihnen bei der Verwaltung der Bandbreitennutzung Ihres Videostreams.

Variable Bitrate (VBR)
Mit der variablen Bitrate können Sie den Bandbreitenverbrauch je nach Aktivitätslevel in der Szene ändern. Je mehr Aktivität stattfindet, desto mehr Bandbreite ist erforderlich. Mit der variablen Bitrate ist eine konstante Bildqualität garantiert, wobei jedoch sichergestellt sein muss, dass Speichermargen vorhanden sind.



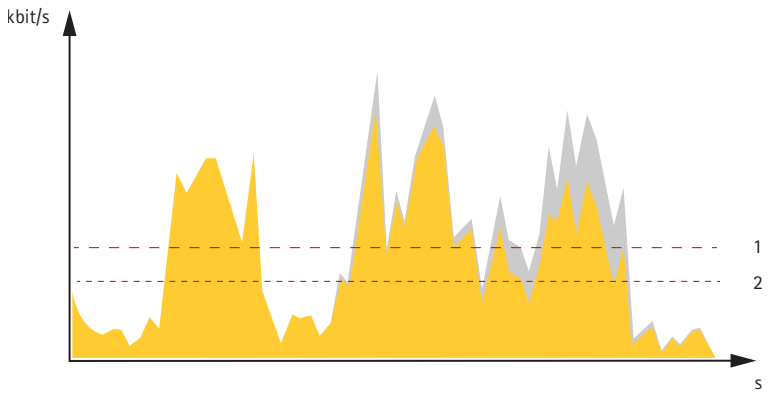
Maximale Bitrate (MBR)
Mit der maximalen Bitrate können Sie eine Zielbitrate einstellen, um die Bitratenbeschränkungen in Ihrem System einzubeziehen. Möglicherweise wird die Bildqualität oder die Bildrate verringert, da die augenblickliche Bitrate unterhalb der angegebenen Zielbitrate gehalten wird. Sie können festlegen, ob die Bildqualität oder die Bildrate priorisiert werden soll. Wir empfehlen Ihnen, die Zielbitrate auf einen höheren Wert als die erwartete Bitrate zu konfigurieren. Dadurch haben Sie einen Spielraum, wenn sich das Aktivitätsniveau in der Szene erhöht.



1 Zielbitrate

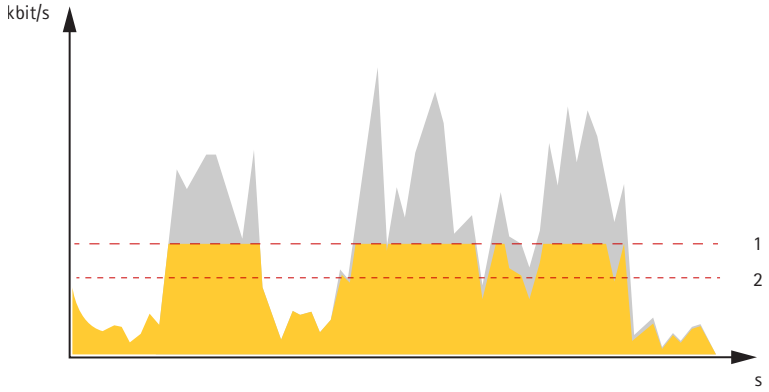
Durchschnittliche Bitrate (Average Bitrate, ABR)
Bei durchschnittlicher Bitrate wird die Bitrate automatisch über einen längeren Zeitraum angepasst. Dadurch können Sie das angegebene Ziel erfüllen und die beste Videoqualität auf Grundlage Ihres verfügbaren Speichers bereitstellen. Im Vergleich zu statischen Szenen ist die Bitrate in Szenen mit viel Aktivität höher. In Szenen mit viel Aktivität erhalten Sie mit der Option „durchschnittliche Bitrate" eher eine bessere Bildqualität. Sie können den erforderlichen Gesamtspeicher für die Speicherung des Videostreams für eine festgelegte Zeitspanne (Aufbewahrungszeit) festlegen, wenn die Bildqualität auf die angegebene Zielbitrate eingestellt wird. Stellen Sie die durchschnittliche Bitrate auf folgende Arten ein:

- Um den geschätzten Speicherbedarf zu berechnen, stellen Sie die Zielbitrate und die Aufbewahrungszeit ein.
- Um die durchschnittliche Bitrate auf Grundlage des verfügbaren Speichers und der erforderlichen Aufbewahrungszeit zu berechnen, verwenden Sie den Zielbitratenrechner.



1 *Zielbitrate*
2 *Tatsächliche durchschnittliche Bitrate*

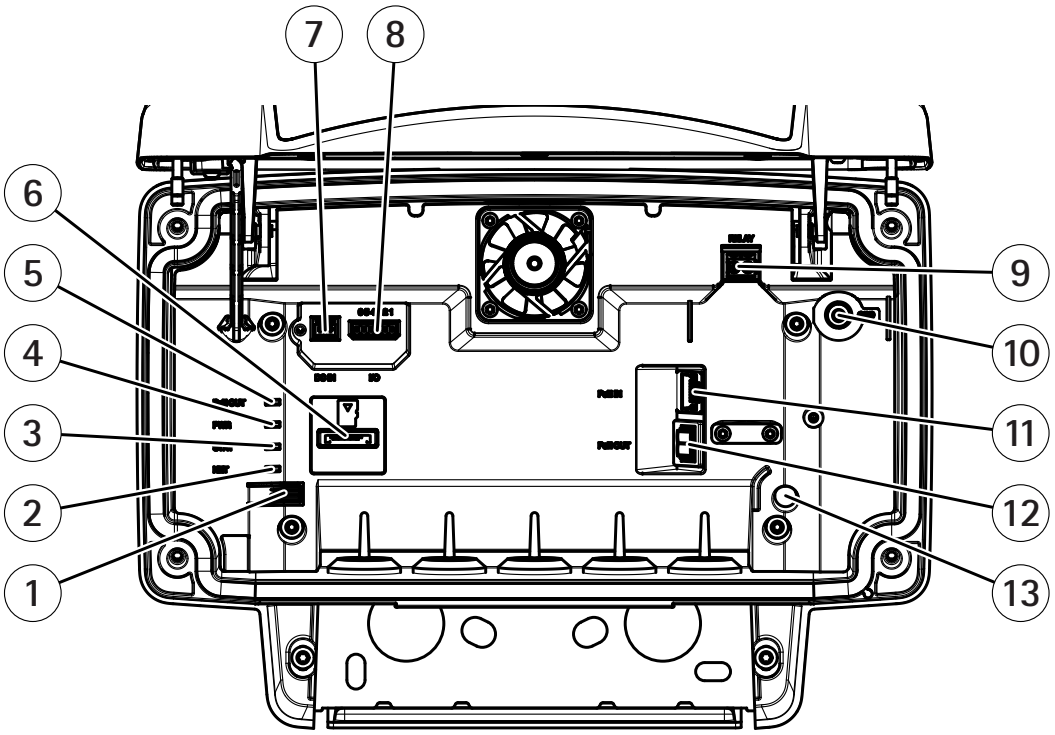
Sie können auch die maximale Bitrate aktivieren und innerhalb der durchschnittlichen Bitrate eine Zielbitrate festlegen.



1 *Zielbitrate*
2 *Tatsächliche durchschnittliche Bitrate*

Technische Daten

Produktübersicht



1 *Steuertaste*
2 *Netzwerk-LED*
3 *Status-LED*
4 *Power-LED*
5 *PoE-Ausgang-LED*
6 *Einschub für microSD-Speicherkarte*
7 *Netzanschluss (Gleichstrom)*
8 *E/A-Anschluss*
9 *Relaisanschluss*
10 *Erdungsschraube*
11 *Netzwerk-Anschluss (PoE in)*
12 *Netzwerk-Anschluss (PoE out)*
13 *Einbruchalarmsensor*

Technische Daten, siehe .

LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.

Netzwerk-LED	Anzeige
Grün	Leuchtet bei Verbindung mit einem 100-MBit/s-Netzwerk konstant. Blinkt bei Netzwerkaktivität.
Gelb	Leuchtet bei Verbindung mit einem 10-MBit/s-Netzwerk konstant. Blinkt bei Netzwerkaktivität.
Aus	Keine Netzwerk-Verbindung

Power-LED	Anzeige
Grün	Normalbetrieb

PoE-Ausgang-LED	Anzeige
Aus	PoE-Ausgang ausgeschaltet
Grün	PoE-Ausgang eingeschaltet

Einschub für SD-Speicherkarte

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

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

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

Tasten

Steuertaste

Die Position der Steuertaste finden Sie unter: .
Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe .
- Verbinden mit einem AXIS Video Hosting System-Dienst Siehe . Halten Sie zum Verbinden die Taste für ca. 3 Sekunden gedrückt, bis die Status-LED-Leuchte grün blinkt.

Anschlüsse

Netzwerk-Anschluss

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

⚠ VORSICHT

Risiko, dass das Gerät beschädigt wird. Versorgen Sie das Gerät nicht sowohl mit PoE als auch mit Gleichstrom.

Netzwerk-Anschluss (PoE out)

Power over Ethernet IEEE 802.3at Typ 2, max. 30 W

Über diesem Anschluss können Sie ein anderes PoE-Gerät mit Strom versorgen, z. B. eine Kamera, einen Hornlautsprecher oder zweiten Axis Radar.

Hinweis

Der PoE-Ausgang wird aktiviert, wenn das Radar über einen 60-W-Midspan (Power over Ethernet IEEE 802.3bt, Typ 3) versorgt wird.

Hinweis

Wenn das Radar mit einer 30-W-Midspan- oder Gleichstromleistung betrieben wird, wird der PoE-Ausgang deaktiviert.

Hinweis

Die maximale Ethernet-Kabellänge beträgt 100 m insgesamt für PoE-Ausgang und PoE-Eingang kombiniert. Sie können sie mit einem PoE-Extender verlängern.

Hinweis

Wenn für das angeschlossene PoE-Gerät mehr als 30 W erforderlich sind, können Sie zwischen dem PoE-Ausgang auf dem Radargerät und dem Gerät einen 60 W Midspan hinzufügen. Der Midspan stellt die Stromversorgung des Geräts her, während das Sicherheitsradar die Ethernet-Verbindung bietet.

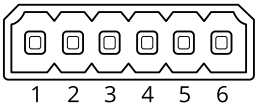
E/A-Anschluss

Über den E/A-Anschluss werden externe Geräte in Verbindung mit Ereignisauslösung, Alarmbenachrichtigungen und anderen Funktionen angeschlossen. Außer dem Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) besitzt der E/A-Anschluss 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.

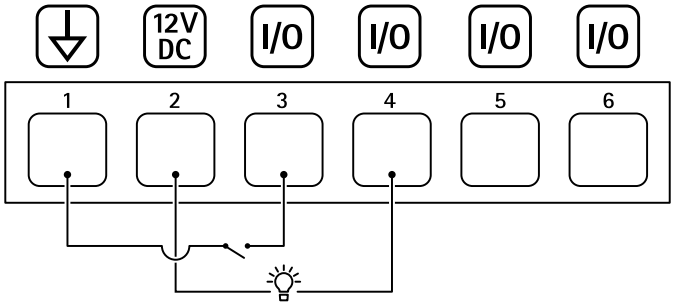
Digitalausgang – Zum Anschluss externer Geräte wie Relais und LEDs. Die angeschlossenen Geräte können über das VAPIX® Application Programming Interface, über ein Ereignis oder über die Weboberfläche des Geräts aktiviert werden.

Sechspoliger Anschlussblock



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

Beispiel:

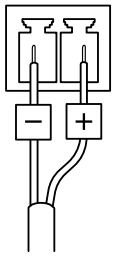


1 *Erdung Gleichstrom*
2 *Gleichstromausgang 12 V, max. 50 mA*
3 *E/A als Eingang konfiguriert*

4 *E/A als Ausgang konfiguriert*
5 *Konfigurierbarer E/A*
6 *Konfigurierbarer E/A*

Stromanschluss

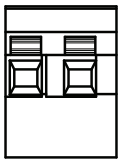
2-poliger Anschlussblock für die Gleichstromversorgung. Eine den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS) verwenden. Die Nennausgangsleistung muss dabei auf ≤100 W begrenzt sein oder der Nennausgangsstrom auf ≤5 A.



⚠ VORSICHT

Risiko, dass das Gerät beschädigt wird. Versorgen Sie das Gerät nicht sowohl mit PoE als auch mit Gleichstrom.

Relaisanschluss



⚠ VORSICHT

Für den Relaisanschluss einadrige Kabel verwenden.

Funktion	Technische Daten
Typ	Schliesser-Kontakt
Nennspannung	24 V DC/5 A
Isolation von anderen Stromkreisen	2,5 kV

Gerät reinigen

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

HINWEIS

- Aggressive Chemikalien können das Gerät beschädigen. Verwenden Sie zur Reinigung Ihres Geräts keine chemischen Substanzen wie Fensterreiniger oder Aceton.
- Sprühen Sie Reinigungsmittel nicht direkt auf das Gerät. Sprühen Sie das Reinigungsmittel stattdessen auf ein nicht scheuerndes Tuch, und verwenden Sie dieses zur Reinigung des Geräts.
- Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken führen kann.

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

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

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

Um das Produkt auf die Werkseinstellungen zurückzusetzen:

1. Trennen Sie das Gerät von der Stromversorgung.
2. Drücken und halten Sie die Steuertaste, um das Gerät wieder einzuschalten. Siehe .
3. Halten Sie die Steuertaste etwa 15–30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die LED-Statusanzeige grün wird. Wenn im Netzwerk kein DHCP-Server verfügbar ist, wird dem Gerät standardmäßig eine der folgenden IP-Adressen zugewiesen:
   - **Geräte mit AXIS OS 12.0 oder höher:** Zuweisung aus dem Subnetz der verbindungslokalen Adressen (169.254.0.0/16)
   - **Geräte mit AXIS OS 11.11 oder niedriger:** 192.168.0.90/24
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.
   Die Softwaretools für die Installation und Verwaltung stehen auf den Supportseiten unter *axis.com/support* zur Verfügung.

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

Aktuelle AXIS OS-Version überprüfen

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

So überprüfen Sie die aktuelle AXIS OS-Version:

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

AXIS OS aktualisieren

Wichtig

- Vorkonfigurierte und angepasste Einstellungen werden beim Aktualisieren der Gerätesoftware gespeichert (sofern die Funktionen als Teil der neuen AXIS OS-Version verfügbar sind). Es besteht diesbezüglich jedoch keine Gewährleistung seitens Axis Communications AB.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.

Hinweis

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

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

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Fragen, Hinweise und Lösungen

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

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

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

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

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

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

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

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

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

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

Leistungsaspekte

Achten Sie beim Einrichten Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die erforderliche Menge der benötigten Bandbreite (die Bitrate) auswirken.

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

T10145149_de

2025-06 (M31.2)