



Radargeräte der Serie AXIS D21-VE

AXIS D2122-VE Radar

AXIS D2123-VE Radar

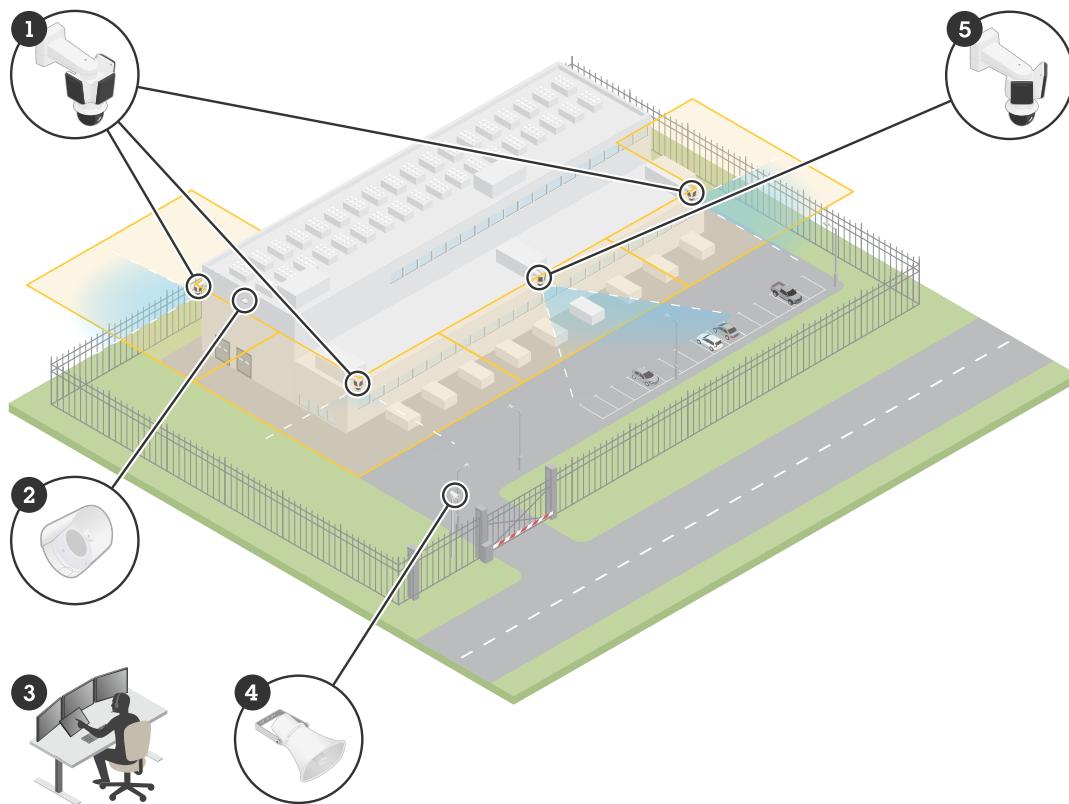
Benutzerhandbuch

Inhalt

Lösungsübersicht	4
Installation	5
Kriterien.....	5
Überwachen der Szene.....	5
Mehrere Radargeräte installieren	6
Erkennungs- und Erfassungsdistanz.....	10
Anwendungsbeispiele.....	12
Funktionsweise.....	15
Das Gerät im Netzwerk ermitteln	15
Unterstützte Browser	15
Weboberfläche des Geräts öffnen	15
Administratorkonto erstellen	15
Sichere Kennwörter	16
Ihr Gerät konfigurieren	17
Montagehöhe festlegen	17
Angabe der Anzahl benachbarter Radargeräte	17
Hinzufügen eines Lageplans als Referenz.....	17
Erstellung eines Szenarios zur Erfassung von Objekten	18
Fehlalarme minimieren	19
Ihre Installation validieren.....	20
Installation des Radars validieren	20
Validierung abschließen	21
Das Radarbild anpassen	22
Ein Bild-Overlay anzeigen.....	22
Video ansehen und aufnehmen	22
Video aufzeichnen und ansehen	22
Einrichten von Regeln für Ereignisse.....	22
Lösen Sie eine Aktion aus	22
Abwechselnd aufblinkendes rotes Licht am Radar	23
E-Mail senden, wenn jemand den Radar mit einem metallischen Gegenstand abdeckt	23
Weboberfläche	25
Status.....	25
Radar.....	26
Einstellungen	26
Videostream.....	28
Kartenkalibrierung	29
Ausschlussbereiche.....	30
Szenarien.....	31
Overlays	32
Dynamische LED-Leiste	34
Analyse	34
Metadatenkonfiguration	34
Aufzeichnungen	35
Apps	36
System.....	37
Uhrzeit und Ort	37
Netzwerk.....	39
Sicherheit.....	43
Konten	49
Ereignisse	52
MQTT	58
Speicherung.....	61
Videostromprofile	65

Über ONVIF.....	66
Melder	69
Energieeinstellungen.....	69
Strommesser.....	70
Edge-to-Edge.....	70
Protokolle	72
Direktkonfiguration.....	73
Wartung.....	74
Wartung	74
Fehler beheben.....	75
Mehr erfahren	76
Radar.....	76
Erkennungs- und Erfassungsbereich.....	76
Szenarien, Einschlussbereiche und Ausschlussbereiche	76
Koexistenzbereich.....	76
Radar-Video-Fusionstechnologie.....	77
Automatische Nachführung.....	77
Overlays	77
Streaming und Speicher.....	77
Video-Komprimierungsformate	77
Bitrate-Steuerung.....	78
Edge-to-Edge-Technologie.....	80
Lautsprecherkopplung	80
Mikrofonkopplung	80
Cybersicherheit.....	80
Axis Sicherheitsbenachrichtigungsdienst.....	80
Schwachstellen-Management.....	80
Sicherer Betrieb von Axis Geräten.....	80
Technische Daten.....	81
Produktübersicht.....	81
LED-Anzeigen	81
.....	81
Einschub für SD-Speicherkarte.....	82
Tasten.....	82
Steuertaste	82
Anschlüsse	82
Netzwerk-Anschluss (PoE in)	82
Netzwerk-Anschluss (PoE out)	82
Gerät reinigen	83
Fehlerbehebung	84
Zurücksetzen auf die Werkseinstellungen.....	84
Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.....	84
Optionen für AXIS OS	84
Aktuelle AXIS OS-Version überprüfen	84
AXIS OS aktualisieren	85
Technische Probleme und mögliche Lösungen.....	85
Leistungsaspekte.....	87
Support.....	88

Lösungsübersicht



Beispiel einer Videosicherheitslösung in einem Rechenzentrum.

- 1 *AXIS D2123-VE Radar in Kombination mit AXIS Q6358-LE PTZ Camera*
- 2 *AXIS D4200-VE Network Strobe Speaker*
- 3 *Überwachungszentrum*
- 4 *AXIS C1310-E Network Horn Speaker*
- 5 *AXIS D2122-VE Radar in Kombination mit AXIS Q6358-LE PTZ Camera*

Installation

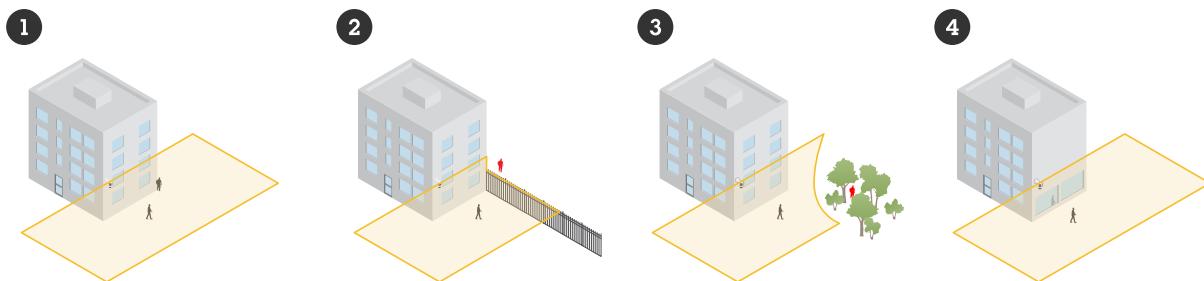


Rufen Sie zur Wiedergabe dieses Videos die Webversion dieses Dokuments auf.

Dieses Video zeigt die Installation am Beispiel eines Radargeräts der Serie AXIS D21-VE. Anweisungen zu allen Installationsszenarien und Sicherheitsinformationen finden Sie in der Installationsanleitung.

Kriterien

- Das Radargerät ist für die Überwachung offener Bereiche bestimmt (1). Jedes feste Objekt wie eine Wand, ein Zaun, ein Baum oder ein großer Busch in der Szene verursacht einen toten Winkel, einen sogenannten Radarschatten, hinter sich (2, 3). Die Montagehöhe wirkt sich auf die Größe des Radarschattens aus.
- Bei komplexeren Szenen, zum Beispiel mit reflektierenden Oberflächen, wird die Nutzung der Radar-Video-Fusionstechnologie ausgewählter PTZ-Kameras empfohlen.
- Das Radargerät funktioniert am zuverlässigsten bei befestigtem Untergrund wie Asphalt. Ist der Boden mit Kies oder Gras bedeckt, kann die Erfassung beeinträchtigt werden.
- Stellen Sie bei der Installation des Radargeräts an einer Wand sicher, dass sich innerhalb eines Meters (drei Fuß) links und rechts vom Radargerät keine anderen Objekte oder Anlagen befinden. Solche Objekte können Funkwellen reflektieren und so die Leistung des Radargeräts beeinträchtigen.
- Bei Installation des Radargeräts an einem Mast achten Sie darauf, dass der Mast stabil ist. Das Radargerät verfügt zwar über eine Stabilisierungsfunktion, die Sie aktivieren können, übermäßige Mastbewegungen können jedoch die Empfindlichkeit des Radargeräts oder die Dauer bis zur Detektion eines sich bewegenden Objekts beeinträchtigen.
- Ein Metallobjekt oder eine reflektierende Oberfläche in einer Szene kann Personen oder Fahrzeuge in der Nähe reflektieren und zu einer Reflexradarerfassung oder Doppelerfassung führen (4). Das kann das Klassifizierungsergebnis des Radargeräts verfälschen und Fehlalarme auslösen. Mithilfe von Ausschlussbereichen können Sie störende Reflexionen herausfiltern. Außerdem können Sie die Auswirkungen von Reflexionen minimieren, indem Sie das Radargerät mit einer Kamera koppeln.
- Die empfohlene Montagehöhe ist dem Datenblatt des Geräts auf axis.com zu entnehmen.

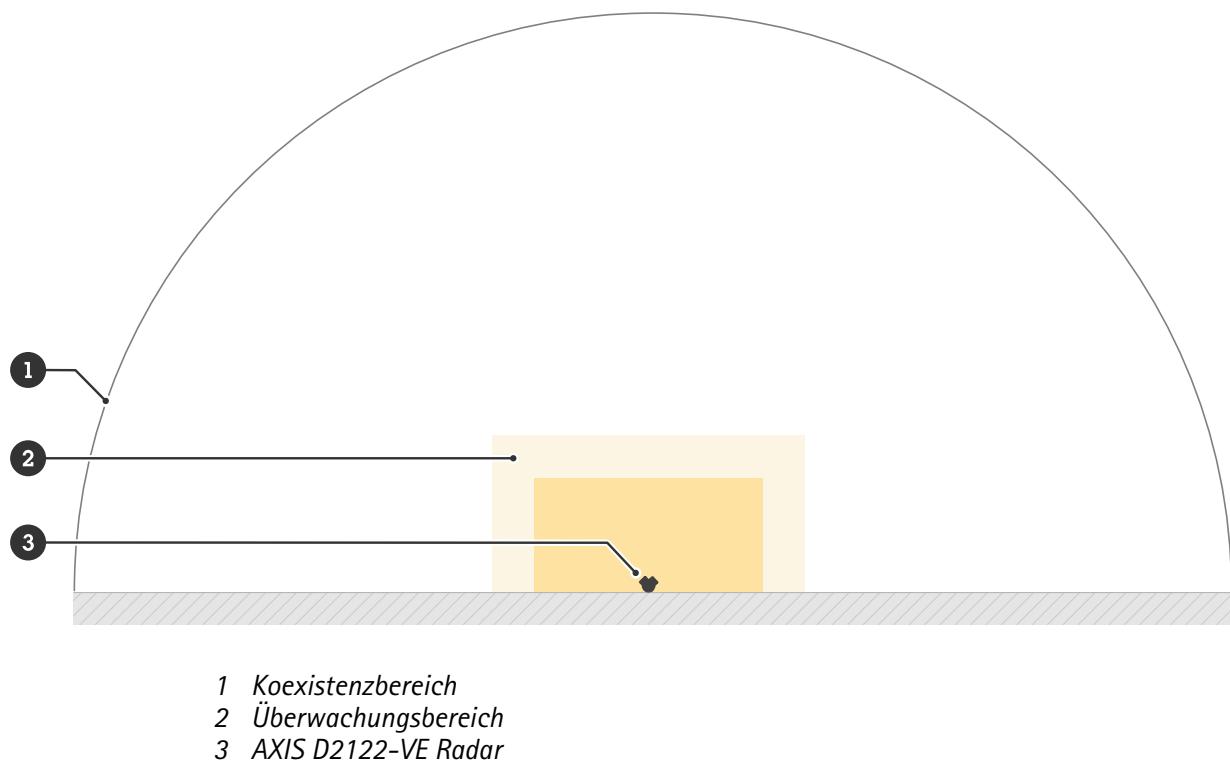


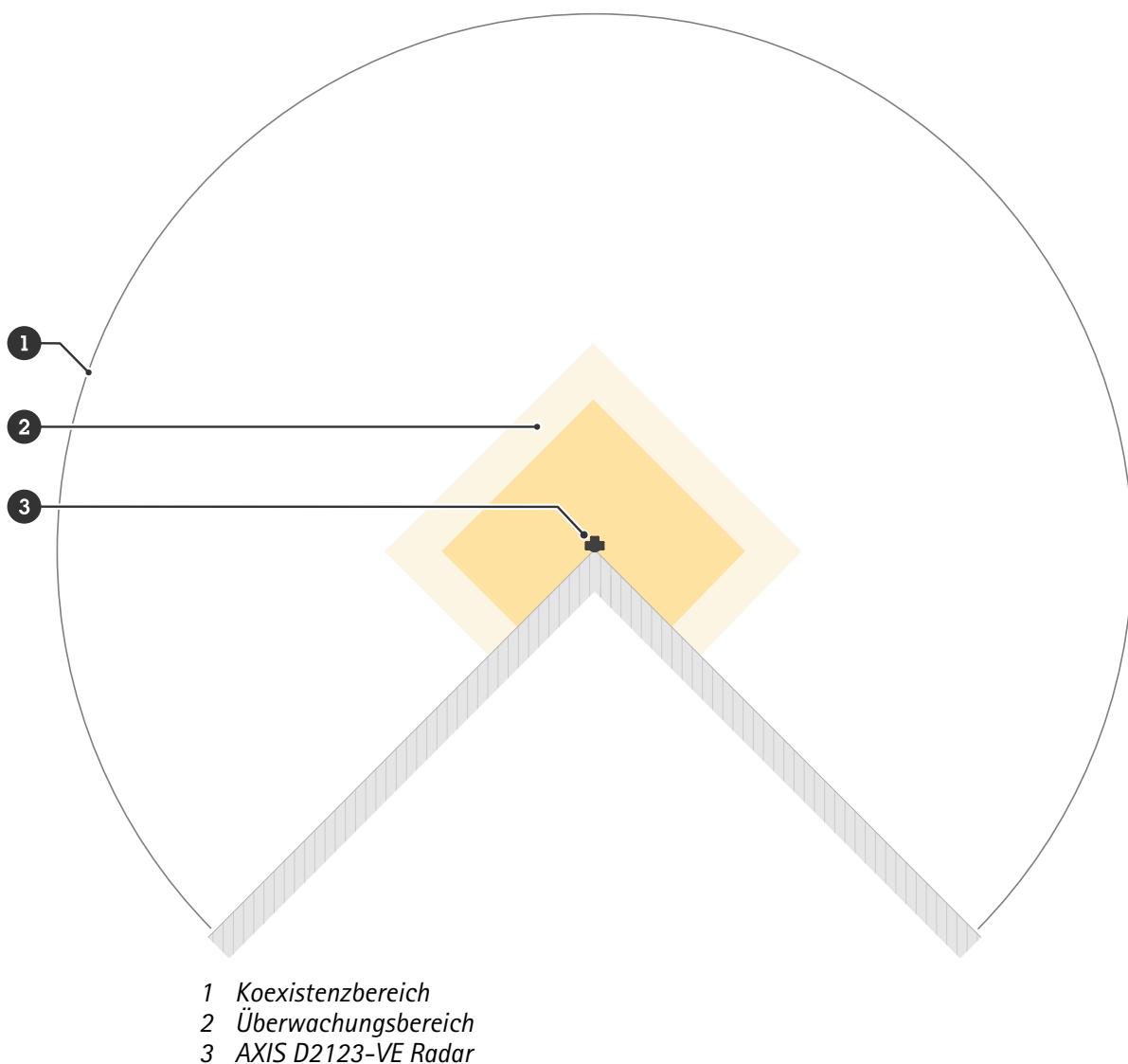
Überwachen der Szene

Das Radargerät kann sich bewegende Objekte detektieren und diese als Personen, Fahrzeuge oder unbekannte Objekte klassifizieren. Verwenden Sie zur Überwachung eines Bereichs das Profil **Area monitoring** (Bereichsüberwachung).

Mehrere Radargeräte installieren

Zur Überwachung von Bereichen wie der Umgebung eines Gebäudes oder der Pufferzone außerhalb eines Zauns können mehrere Radargeräte nahe beieinander installiert werden. Jedes Radargerät kann mit bis zu elf weiteren Radargeräten des Typs AXIS D2122-VE oder AXIS D2123-VE in einem Umkreis von 500 Metern (1640 Fuß), dem so genannten Koexistenzbereich, kombiniert werden. Dieses Radarmodell unterstützt außerdem die Installation im Koexistenzbereich früherer Radarmodelle von Axis, da sich die Modelle nicht gegenseitig stören. Weitere Informationen zum Koexistenzbereich finden Sie unter *Koexistenzbereich, on page 76*.





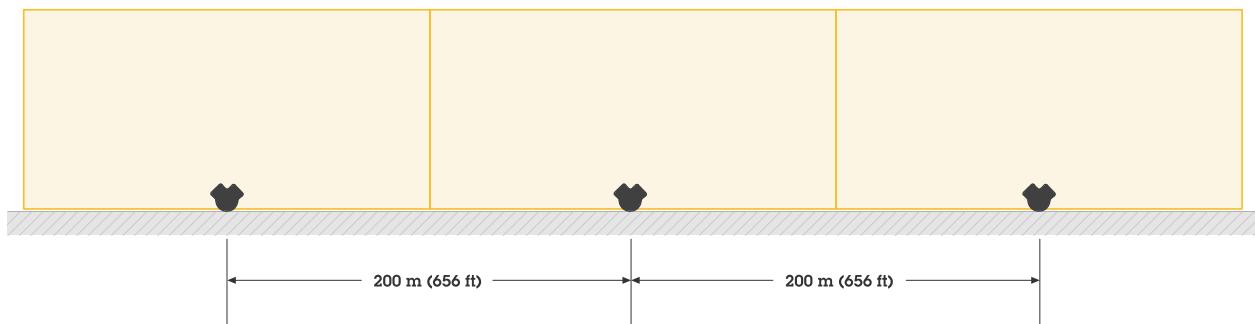
Hinweis

Die Leistung des Radargeräts im Koexistenzbereich kann durch die Umwelt und die Ausrichtung des Radargeräts auf Zäune, Gebäude oder benachbarte Radaranlagen beeinflusst werden.

Installationsbeispiele

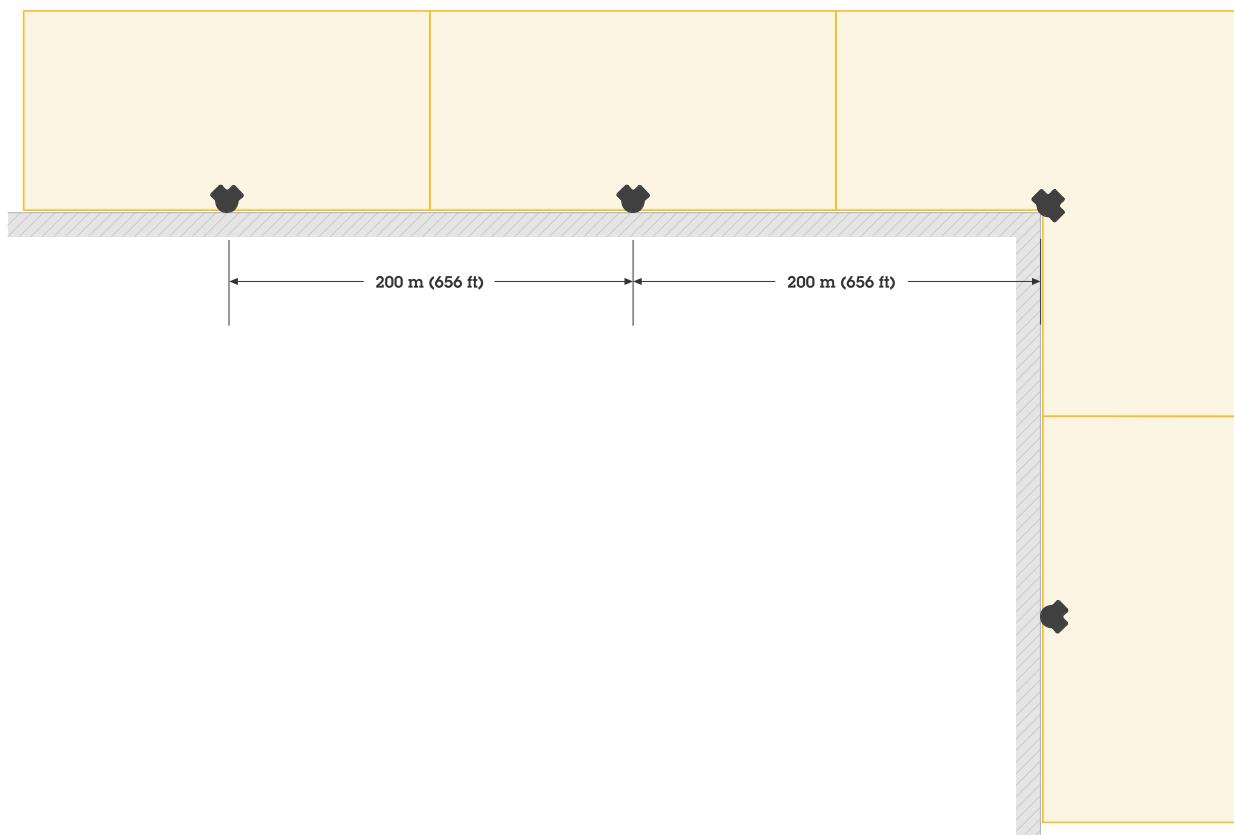
Erstellen eines virtuellen Zauns mit mehreren Radargeräten

Um einen virtuellen Zaun zu erstellen, z. B. entlang eines Gebäudes, können Sie mehrere Radargeräte nebeneinander platzieren. Wir empfehlen Ihnen, zwischen den einzelnen Geräten einen Abstand von 200 m (656 ft) einzuhalten.



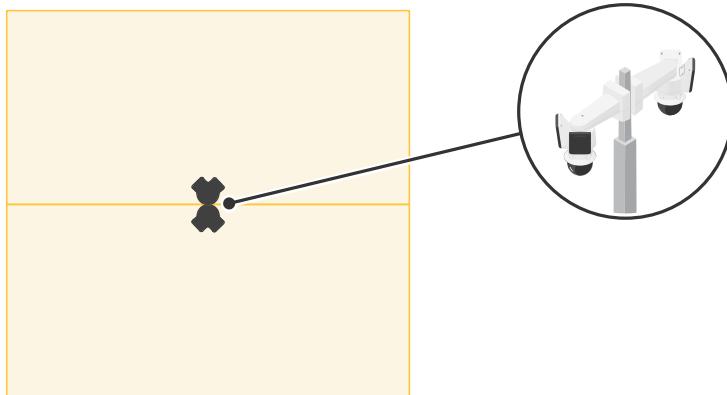
Einen Bereich um ein Gebäude abdecken

Um den Bereich um ein Gebäude herum zu überwachen, bringen Sie Radargeräte nach außen gerichtet an den Mauern des Gebäudes an.



Einen offenen Bereich abdecken

Zur Überwachung eines großen offenen Bereichs müssen zwei Radargeräte des Typs AXIS D2122-VE Radar an zwei Masthalterungen Rücken an Rücken positioniert werden.

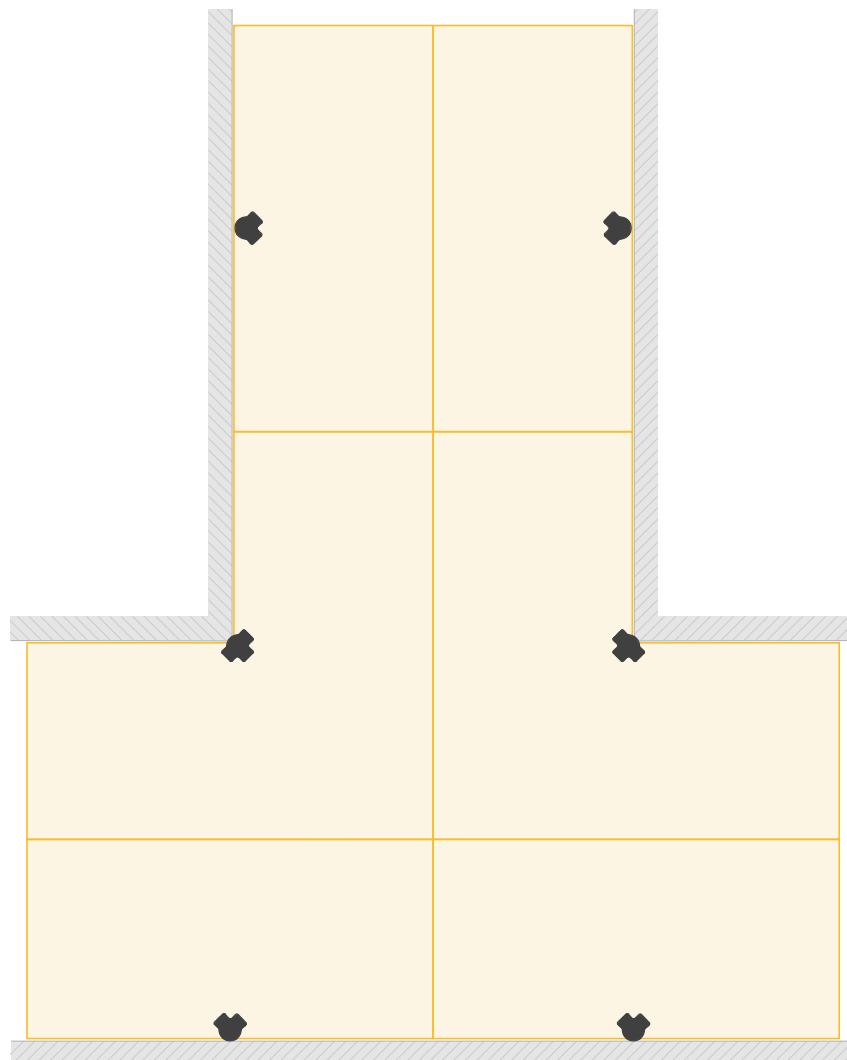


Hinweis

Jedes Radargerät kann einen PoE-Ausgang von bis zu 60 W liefern, wenn es über einen 90-W-Midspan mit Strom versorgt wird. Ein PoE-Ausgang erfordert Power over Ethernet IEEE 802.3bt, Typ 4, Klasse 8.

Installieren mehrerer gegenüberliegender Radargeräte

Um zum Beispiel einen Bereich zwischen Gebäuden zu überwachen, empfiehlt sich die Installation gegenüberliegender Radargeräte. In einem Koexistenzbereich ist es möglich, bis zu 12 sich gegenüberliegende Radargeräte zu installieren.

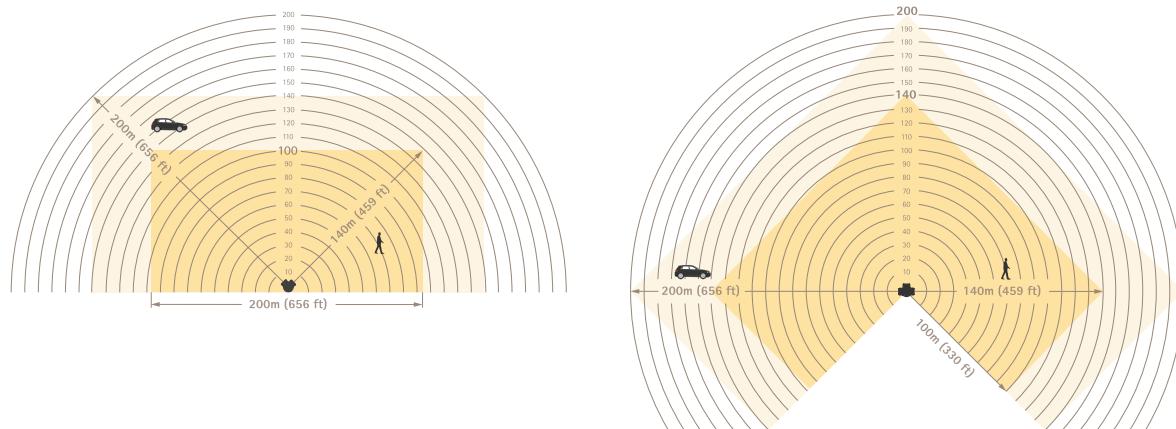


Erkennungs- und Erfassungsdistanz

Bei Installation des Radargeräts in optimaler Montagehöhe:

- Im Erkennungsbereich können Personen bis zu einer Distanz von maximal 100 bis 140 Metern (330–459 Fuß) vom Radargerät detektiert und klassifiziert werden, wobei die tatsächliche Reichweite von der Position der Person zum Radargerät abhängig ist.
- Im Erfassungsbereich können Fahrzeuge bis zu einer Entfernung von maximal 140 bis 200 Metern (459–656 Fuß) vom Radargerät detektiert werden, wobei die tatsächliche Distanz von folgenden Faktoren abhängig ist:
 - Geschwindigkeit des Fahrzeugs
 - Richtung des Fahrzeugs zum Radargerät
 - Ebenheit des Untergrunds
 - Material des Untergrunds

Weitere Informationen zu den Bereichen finden Sie unter *Erkennungs- und Erfassungsbereich, on page 76*.



Erkennungs- und Erfassungsdistanz

Hinweis

- Geben Sie die tatsächliche Montagehöhe bei der Radarkalibrierung des Radars in der Weboberfläche des Radargeräts ein.
- Die Erkennungs- und die Erfassungsdistanz sind von der Szene abhängig.
- Außerdem variieren Erkennungs- und Erfassungsdistanz je nach Typ des Objekts.

Die Erkennungs- und die Erfassungsdistanz wurden unter den folgenden Bedingungen gemessen:

- Die Distanz wurde auf ebenem, horizontalem Untergrund gemessen.
- Das Radargerät war ohne Neigung montiert.
- Das Objekt war eine Person mit einer Größe von 170 cm (5 ft 7 in).
- Es bestand eine ungehinderte Sichtverbindung zwischen Radargerät und Person.
- Die Radarempfindlichkeit wurde auf **Mittel** eingestellt.

Das Radargerät kann Objekte unterhalb der minimalen Erfassungsdistanz nicht detektieren. Die minimale Erfassungsdistanz ist von der Montagehöhe des Radargeräts abhängig:

Montagehöhe	Minimale Erfassungsdistanz
4 m (9,8 ft)	4 m (9,8 ft)
5 m (16,4 ft)	6 m (19,7 ft)
6 m (19,7 ft)	8 m (26 ft)
7 m (23 ft)	11 m (36 ft)
8 m (26 ft)	13 m (42,7 ft)
9 m (29,5 ft)	15 m (49,2 ft)
10 m (32,85 ft)	18 m (59 ft)

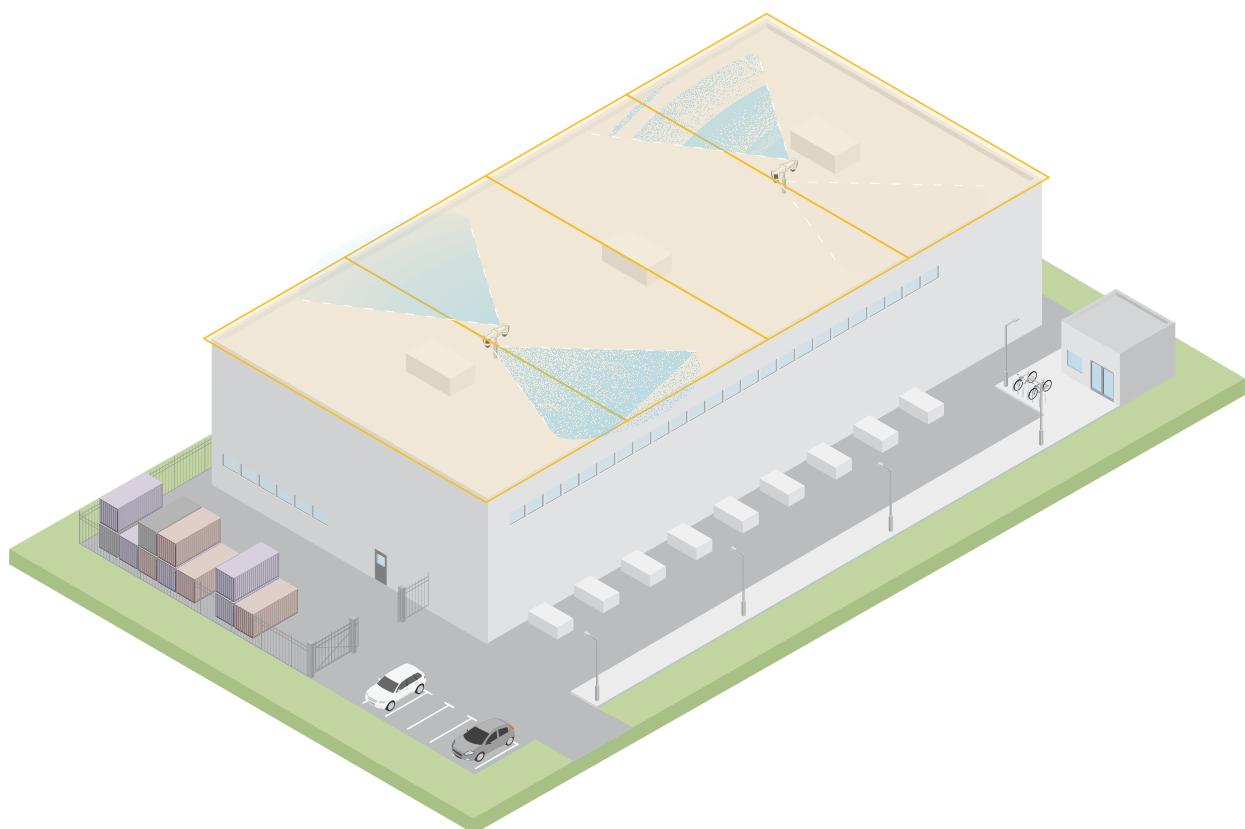
Hinweis

Wenn Sie das Radargerät mit einer PTZ-Kamera kombinieren, kann die Kamera ein Objekt auch unterhalb der minimalen Erfassungsdistanz des Radargeräts weiter verfolgen.

Anwendungsbeispiele

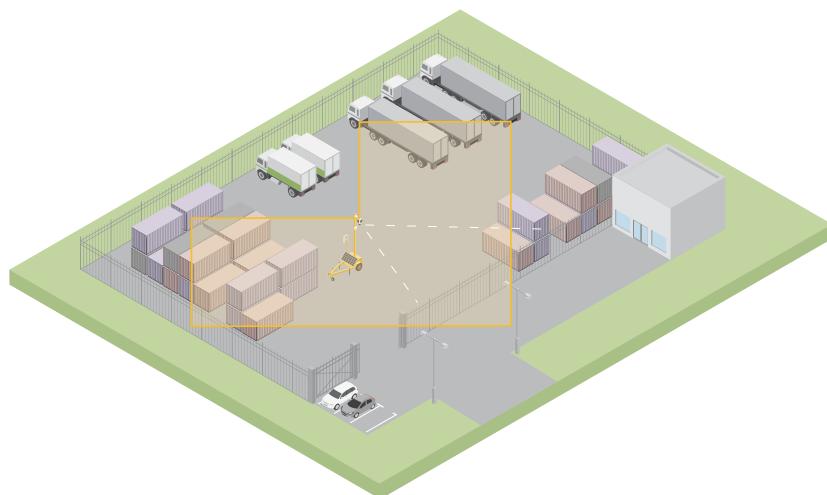
Überwachung einer Dachfläche

Ein großes Verteilerzentrum möchte Radargeräte zur Überwachung des Dachbereichs einsetzen. Die Radargeräte sind mit ARTPEC-9-PTZ-Kameras gekoppelt und Rücken an Rücken montiert, sodass der Überwachungsbereich das gesamte Dach abdeckt. Das Radargerät erkennt und klassifiziert sich bewegende Objekte auf dem Dach, richtet die Kamera auf diese aus und lässt die Klassifizierung von der Kamera bestätigen. Die Kamera verfolgt die Objekte dann per Objektverfolgung weiter.



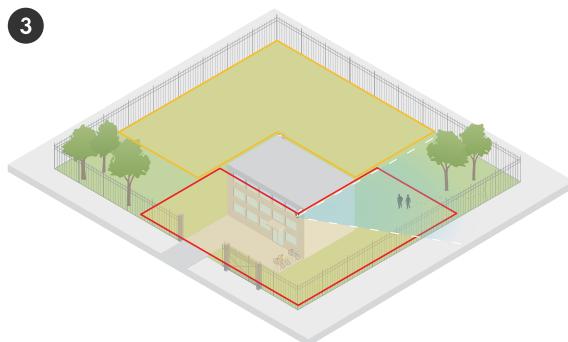
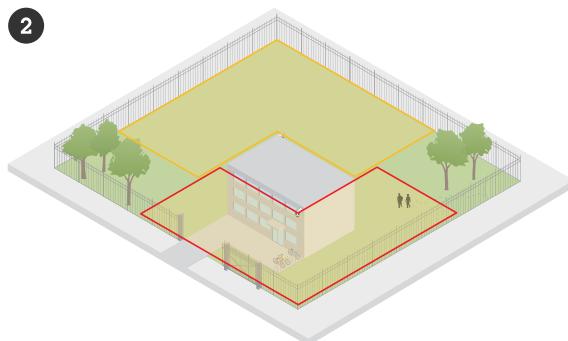
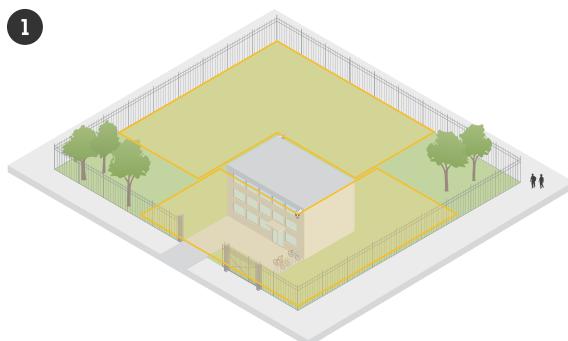
Verwendung eines mobilen Videosicherheitsanhängers zur Überwachung großer offener Bereiche

Im Außenbereich eines Baumarkts kam es nach Geschäftsschluss zu mehreren Einbrüchen. Das Gelände wird immer von einer Person überwacht, aber die Sicherheitsvorkehrungen nachts sollen erhöht werden, ohne dass zusätzliche Kosten für mehr Personal anfallen. Es wurde beschlossen, zwei Rücken an Rücken montierte Radargeräte auf einem mobilen Videosicherheitsanhänger einzusetzen, die das gesamte Außengelände überwachen. Die Radargeräte sind so konfiguriert, dass das eingesetzte Sicherheitspersonal bei verdächtigem Verhalten alarmiert wird und die Szene sofort untersuchen kann. Außerdem wird erwogen, einen Blitzlicht-Lautsprecher zu installieren, der von den Radargeräten zur Abschreckung von Eindringlingen ausgelöst werden soll.



Umzäuntes Gebäude abdecken

Im folgenden Szenario wurde eine PTZ-Kamera mit dem Radargerät kombiniert, um Alarne zu überprüfen und eine genaue Klassifizierung mit Radar-Video-Fusionstechnologie zu ermöglichen.



1. Eindringlinge bewegen sich außerhalb des Zauns, ohne einen Alarm auszulösen.
2. Bei einem Einbruch dringen Eindringlinge durch den Zaun ein und werden vom Radargerät entdeckt, das einen Alarm auslöst.
3. Das Radar richtet die PTZ-Kamera auf die Eindringlinge, die den Alarm per Videoanalyse überprüft.

Weitere Informationen finden Sie unter *Automatische Nachführung, on page 77.*

Funktionsweise

Das Gerät im Netzwerk ermitteln

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

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

✓: Empfohlen

*: Unterstützt mit Einschränkungen

Weboberfläche des Geräts öffnen

1. Öffnen Sie einen Browser, und geben Sie die IP-Adresse oder den Host-Namen des Axis Geräts in die Adresszeile des Browsers ein.
Bei unbekannter IP-Adresse AXIS IP Utility oder AXIS Device Manager verwenden, um das Gerät im Netzwerk zu ermitteln.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Administratorkonto erstellen*, on page 15.

Eine Beschreibung aller Steuerelemente und Optionen auf der Weboberfläche des Geräts finden Sie unter *Weboberfläche*, on page 25.

Administratorkonto erstellen

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

1. Einen Benutzernamen eingeben.
2. Geben Sie ein Passwort ein. Siehe *Sichere Kennwörter*, on page 16.
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 *Zurücksetzen auf die Werkseinstellungen*, on page 84.

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Ihr Gerät konfigurieren

Zur optimalen Nutzung Ihres Geräts wird empfohlen, die folgenden Schritte auszuführen:

1. *Montagehöhe festlegen, on page 17*
2. Bei Installation mehrerer Radargeräte in unmittelbarer Nähe zueinander: *Angabe der Anzahl benachbarter Radargeräte, on page 17*
3. *Hinzufügen eines Lageplans als Referenz, on page 17*
4. *Erstellung eines Szenarios zur Erfassung von Objekten, on page 18*
5. *Fehlalarme minimieren, on page 19*
6. *Ihre Installation validieren, on page 20*

Montagehöhe festlegen

Stellen Sie die Montagehöhe des Radargeräts in der Weboberfläche ein. Die Angabe der Montagehöhe ist wichtig, damit das Radargerät die Geschwindigkeit vorbeifahrender Objekte richtig erfassen und messen kann. Außerdem wird sie für die ordnungsgemäße Objektverfolgung benötigt.

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.

Angabe der Anzahl benachbarter Radargeräte

Bei der Installation weiterer Radargeräte desselben Modells im Koexistenzbereich dieses Radargeräts geben Sie die Anzahl der benachbarten Radargeräte in der Weboberfläche jedes Radargeräts an. Dadurch wird die Funktion der Radargeräte optimiert und das Risiko von Störungen minimiert.

1. Gehen Sie zu **Radar > Einstellungen > Koexistenz**.
2. Wählen Sie die Anzahl benachbarter Radargeräte im Koexistenzbereich dieses Radargeräts aus.

Hinzufügen eines Lageplans als Referenz

Für eine leichtere Erstellung von Szenarien und die schnellere Ortung der Punkte, an denen sich Objekte in der Szene bewegen, können Sie einen Lageplan als Hintergrund für den Radar-Stream wählen. Dies kann z. B. eine Planzeichnung oder ein Luftbild sein, das die vom Radar abgedeckte Fläche darstellt. Justieren und kalibrieren Sie die Karte so, dass die Radaransicht mit Position, Ausrichtung und Maßstab der Karte übereinstimmt, und zoomen Sie sie heran, wenn Sie sich bestimmte Teile der Szene 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 assistant (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 schrittweise 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 verändert die Radaransicht nicht. Auch wenn Teile der Ansicht nach dem Zoomen nicht sichtbar sind, detektiert das Radargerät weiterhin sich bewegende Objekte im gesamten Sichtbereich. Die einzige Möglichkeit, erfasste Bewegungen auszuschließen, besteht im Hinzufügen von Ausschlussbereichen.
 - Sie können die Schwenk- und Zoom-Funktion jederzeit auf den folgenden Seiten **Map calibration** (**Kartenkalibrierung**), **Exclusion zones** (**Ausschlussbereiche**) oder **Scenarios** (**Szenarien**) per Klick auf  anpassen.
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.



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

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

Erstellung eines Szenarios zur Erfassung von Objekten

Mit einem Szenario können Sie sich bewegende Objekte in einer Szene erfassen oder erkennen. Zum Auslösen von Aktionen bei Erfüllung der Bedingungen in Ihrem Szenario erstellen Sie eine Regel unter **Events** (**Ereignisse**). Sie können mehrere Szenarien erstellen, um unterschiedliche Verhaltensweisen zu erfassen oder verschiedene Teile der Szene zu überwachen.

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 bestimmte Linie überqueren.
5. Klicken Sie auf **Next (Weiter)**.
6. Für Szenarien des Typs **Movement in area** (**Bewegung im Bereich**):
 - 6.1. Wählen Sie die Form des Bereichs.
Verschieben Sie den Bereich mit der Maus und passen Sie ihn so an, dass er den gewünschten Teil der Radaransicht oder der Referenzkarte abdeckt.
7. Für Szenarien des Typs **Line crossing** (**Überfahren von Linien / Überschreiten von Linien**):
 - 7.1. Positionieren Sie die Linie in der Szene.
Verwenden Sie die Maus, um die Linie zu verschieben und anzupassen.

- 7.2. Um die Erfassungsrichtung zu ändern, aktivieren Sie die Option **Richtung ändern**.
- 7.3. Um Aktionen nach dem Überfahren / Überschreiten von zwei Linien auslösen zu lassen, aktivieren Sie die Option **Require crossing of two lines** (**Überschreiten von zwei Linien erforderlich**).
Positionieren Sie die zweite Linie in der Szene.
8. Klicken Sie auf **Next (Weiter)**.
9. Fügen Sie Erfassungseinstellungen hinzu.
 - 9.1. Fügen Sie zu Szenarien des Typs **Bewegung im Bereich** und **Überfahren von Linien / Überschreiten von Linien** mit einer Linie unter **Ignore short-lived objects** (**Nur kurz erscheinende Objekte ignorieren**) eine Verzögerungszeit hinzu, um Fehlalarme zu minimieren.
 - 9.2. Legen Sie für Szenarien des Typs **Überfahren von Linien / Überschreiten von Linien** mit zwei Linien unter **Max time between crossings** (**Max. Zeit zwischen Übertritten**) das Zeitlimit zwischen dem Überfahren / Überschreiten der ersten und der zweiten Linie fest.
 - 9.3. Wählen Sie unter **Trigger on object type** (**Auslöser für Objekttyp**) den auslösenden Objekttyp aus.
 - 9.4. Fügen Sie unter **Speed limit** (**Geschwindigkeitsbegrenzung**) einen Geschwindigkeitsbereich hinzu.
10. Klicken Sie auf **Next (Weiter)**.
11. Legen Sie die Mindestdauer des Alarms unter **Minimum trigger duration** (**Minimale Triggerdauer**) fest. Verringern Sie die Zeit bei Szenarien des Typs **Überfahren von Linien / Überschreiten von Linien** auf 0 Sekunden, wenn die Objekte Aktionen sofort bei Übertritt auslösen sollen.
12. **Save (Speichern)** anklicken.

Fehlalarme minimieren

Bei häufigen Fehlalarmen können Sie versuchen, diese durch Anpassung verschiedener Einstellungen zu minimieren. Sie können zum Beispiel bestimmte Typen von Bewegungsabläufen oder Objekten herausfiltern, Bereiche für das Auslösen von Alarmen anpassen oder die Erfassungsempfindlichkeit ändern.

- Erfassungsempfindlichkeit des Radarmelders einstellen:
Gehen Sie zu **Radar > Settings (Einstellungen) > Detection (Erfassung)** und reduzieren Sie die Empfindlichkeit unter **Detection sensitivity** (**Erfassungsempfindlichkeit**).
Die Empfindlichkeitseinstellung wirkt sich auf alle Bereiche aus.
 - Eine geringere Erfassungsempfindlichkeit ist sinnvoll, wenn sich viele Metallobjekte oder große Fahrzeuge in einer Szene befinden. Sie senkt das Risiko von Fehlalarmen, reduziert jedoch auch die Fähigkeit des Radars, kleine Objekte zu klassifizieren.
 - Eine höhere Erfassungsempfindlichkeit eignet sich für offene Szenen, wie zum Beispiel Felder, in denen keine Metallobjekte vorhanden sind.
- Anpassung von Einschluss- und Ausschlussbereichen:
Harte Oberflächen in einer Szene können Reflexionen verursachen, die zu einer Mehrfacherfassung eines einzelnen physischen Objekts führen können. Hier haben Sie entweder die Möglichkeit, die Form des Einschlussbereichs im Szenario anzupassen oder eine allgemeine Ausschlusszone hinzufügen, um einen bestimmten Teil der Szene zu ignorieren.
- Auslösen bei Objekten, die zwei Linien überschreiten anstelle einer:
Wenn sich in einem Szenario mit **Überfahren / Überschreiten von Linien** schaukelnde Objekte oder Tiere in der Szene befinden, besteht die Gefahr, dass diese die Linie übertragen und einen Fehlalarm auslösen. In diesem Fall können Sie das Szenario so anpassen, dass es nur ausgelöst wird, wenn ein Objekt zwei Linien überschritten hat.
- Filter für bestimmte Bewegungen:
 - Um Fehlalarme durch Bäume, Büsche und Flaggen in einer Szene zu minimieren, gehen Sie zu **Radar > Settings (Einstellungen) > Detection (Erfassung)** und aktivieren Sie die Option **Ignore swaying objects** (**Schaukelnde Objekte ignorieren**).

- Um Fehlalarme durch kleine Objekte oder Tiere wie Katzen oder Hasen in einer Szene zu minimieren, gehen Sie zu **Radar > Settings (Einstellungen) > Detection (Erfassung)** und aktivieren Sie die Option **Ignore small objects (Kleine Objekte ignorieren)**. Die Einstellung ist im Bereichsüberwachungsprofil verfügbar.
- Zeit filtern:
 - Gehen Sie zu **Radar > Szenarien**.
 - Wählen Sie ein Szenario und klicken Sie auf  , um die Einstellungen zu ändern.
 - Erhöhen Sie unter **Seconds until trigger (Sekunden bis zum Auslösen)** die Zeit bis zum Auslösen. Dabei handelt es sich um die Verzögerungszeit zwischen dem Beginn der radargestützten Objektverfolgung und der Auslösung eines Alarms. Der Timer startet, wenn das Radargerät 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 die Objekttypen aus der Auswahl, die in diesem Szenario keinen Alarm auslösen sollen.

Ihre Installation validieren

Installation des Radars validieren

Vor der Benutzung des Radargeräts wird die Validierung der Installation empfohlen. Die Validierung kann Ihnen dabei helfen, Installationsprobleme zu identifizieren oder die Konfiguration an statische Objekte wie Bäume oder reflektierende Oberfläche in der Szene anzupassen.

Hinweis

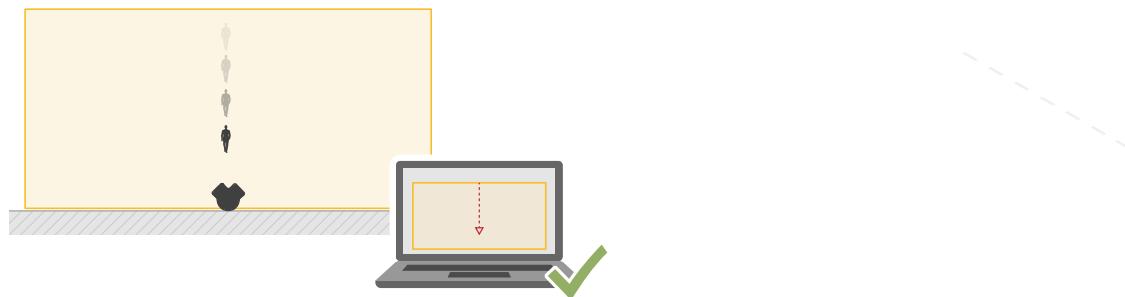
Die Installation wird unter den zum Zeitpunkt der Validierung geltenden Bedingungen überprüft. Eine Veränderung der Bedingungen in der Szene kann die normale Funktion Ihrer Installation beeinträchtigen.

Überprüfen Sie, dass keine falschen Erfassungen vorhanden sind.

1. Stellen Sie sicher, dass im Erkennungsbereich keine menschlichen Aktivitäten stattfinden.
2. Bitte warten Sie einige Minuten, um sicherzustellen, dass das Radargerät keine statischen Objekte im Erkennungsbereich detektiert.
3. Bei einer unerwünschten Detektion können Sie bestimmte Typen von Bewegungsabläufen oder Objekten herausfiltern, Bereiche für das Auslösen von Alarmen anpassen oder die Erfassungsempfindlichkeit ändern. Anweisungen finden Sie unter *Fehlalarme minimieren, on page 19*.

Überprüfung des korrekten Symbols, der Fahrtrichtung und der Position auf dem Lageplan

1. Starten Sie in der Weboberfläche des Radargeräts eine Aufzeichnung. Anweisungen finden Sie unter *Video aufzeichnen und ansehen, on page 22*.
2. Laufen Sie von einem Punkt knapp außerhalb des Erkennungsbereichs direkt auf das Radargerät zu.
3. Überprüfen Sie, ob das Klassifizierungssymbol für eine Person angezeigt wird, wenn die Person den Erkennungsbereich betritt.
4. Stellen Sie sicher, dass auf der Weboberfläche des Radars die korrekte Richtung angezeigt wird.



5. Überprüfen Sie, ob die tatsächliche Position der Person mit der Position auf dem Lageplan übereinstimmt.

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

Test	Bestanden/Fehlgeschlagen	Kommentar
1. Überprüfen Sie, dass bei Inaktivität im Bereich keine unerwünschten Erfassungen gemacht werden.		
2. Überprüfen Sie, ob das Klassifizierungssymbol für eine Person angezeigt wird, wenn die Person den Erkennungsbereich betritt.		
3. Überprüfen Sie, ob die Bewegungsrichtung korrekt ist.		
4. Überprüfen Sie, ob die tatsächliche Position der Person mit der Position auf dem Lageplan übereinstimmt.		

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 Radargerät anweisungsgemäß konfiguriert wurde.
2. Stellen Sie sicher, dass Sie einen Referenzlageplan hinzugefügt und kalibriert haben.
3. Stellen Sie das Radarszenario ein, dass bei Erfassung einer Person ausgelöst werden soll. Standardmäßig ist die Zeit unter **Seconds until trigger** (**Sekunden bis zum Auslösen**) auf zwei Sekunden eingestellt, was Sie jedoch bei Bedarf in der Weboberfläche ändern können.
4. Legen Sie fest, dass das Radargerät eine Videoaufzeichnung auslösen soll, wenn ein geeignetes Objekt erkannt wird.
Anweisungen finden Sie unter *Video aufzeichnen und ansehen, on page 22*.
5. Gehen Sie zu **Radar > Settings (Einstellungen) > Object visualization (Objektvisualisierung)** und legen Sie als **Trail lifetime** (**Spurdauer**) eine Stunde fest, sodass Sie ausreichend Zeit haben, um Ihren Platz zu verlassen, zu Fuß durch den Überwachungsbereich zu gehen und zu Ihrem Platz zurückzukehren. Die Spurdauer setzt die Verfolgung in der Live-Ansicht des Radars für die eingestellte Zeit fort. Nach Abschluss der Validierung können Sie sie deaktivieren.
6. Gehen Sie an der Grenze des Erkennungsbereichs entlang und vergewissern Sie sich, dass die Spur 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.

Das Radarbild anpassen

Dieser Abschnitt enthält Anweisungen zur Konfiguration des Radarbildes. Weitere Informationen zur Arbeitsweise bestimmter Funktionen finden Sie unter *Mehr erfahren, on page 76*.

Ein Bild-Overlay anzeigen

Sie können ein Bild als Overlay im Radarstream hinzufügen.

1. Rufen Sie **Radar > Overlays** auf.
2. Klicken Sie auf **Manage images (Bilder verwalten)**.
3. Laden Sie ein Bild hoch oder ziehen Sie es und legen Sie es ab.
4. Klicken Sie auf **Upload (Hochladen)**.
5. Wählen Sie in der Dropdown-Liste **Image (Bild)** und klicken Sie auf .
6. Wählen Sie das Bild und eine Position. Sie können das Overlay-Bild auch per Drag & Drop in der Live-Ansicht ziehen, um die Position zu ändern.

Video ansehen und aufnehmen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts. Weitere Informationen zum Streamen und Speichern finden Sie unter *Streaming und Speicher, on page 77*.

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.

Einrichten von Regeln für Ereignisse

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

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

Lösen Sie eine Aktion aus

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu. Die Regel legt fest, wann das Gerät bestimmte Aktionen durchführt. Regeln können als geplant, wiederkehrend oder manuell ausgelöst eingerichtet werden.

2. Unter **Name** einen Dateinamen eingeben.
3. Wählen Sie die **Bedingung**, die erfüllt sein muss, damit die Aktion ausgelöst wird. Wenn für die Regel mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.
4. Wählen Sie, welche **Aktion** bei erfüllten Bedingungen durchgeführt werden soll.

Hinweis

- Damit Änderungen an einer aktiven Aktionsregel wirksam werden, muss die Regel wieder eingeschaltet werden.
- Werden Definitionen von in Regeln verwendeten Videostream-Profilen geändert, dann müssen alle Regeln, die diese Videostream-Profile verwenden, neu gestartet werden.

Abwechselnd aufblinkendes rotes Licht am Radar

Mithilfe der dynamischen LED-Leiste an der Vorderseite des Radargeräts können Sie zeigen, dass der Bereich überwacht wird.

Dieses Beispiel erläutert, wie Sie ein wechselndes rotes Licht nach Geschäftsschluss an Werktagen aktivieren.

Einen Zeitplan erstellen:

1. Gehen Sie zu **System > Ereignisse > Zeitpläne** und fügen Sie einen Zeitplan hinzu.
2. Geben Sie einen Namen für den Zeitplan ein, z. B. **Weekday nights**.
3. Wählen Sie unter **Typ** die Option **Zeitplan**.
4. Wählen Sie unter **Recurrence (Wiederholung)** die Option **Daily (Täglich)**.
5. Legen Sie die Startzeit 6 Uhr morgens fest.
6. Legen Sie die Endzeit auf 6 Uhr morgens fest.
7. Wählen Sie unter **Tage** Montag bis Freitag.
8. **Save (Speichern)** anklicken.

Eine Regel erstellen:

1. Gehen Sie auf **System > Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein, z. B. **Red sweeping light**.
3. Wählen Sie in der Bedingungsliste unter **Scheduled and recurring (Geplant und wiederkehrend)** die Option **Schedule (Zeitplan)** aus.
4. Wählen Sie aus der Liste der Zeitpläne **Weekday nights (Nach Geschäftsschluss)** aus.
5. Wählen Sie in der Liste der Aktionen unter **Radar** die Option **Dynamic LED strip (Dynamische LED-Leiste)** aus.
6. Wählen Sie das Muster **Sweeping red (Wechselndes Rot)** aus.
7. Stellen Sie die Dauer auf 12 Stunden ein.
8. **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.

Einen E-Mail-Empfänger hinzufügen:

1. Wechseln Sie zu **Settings > Events > Recipients (Einstellungen > Ereignisse > Empfänger)** und fügen Sie einen Empfänger hinzu.
2. Geben Sie den Namen des Empfängers ein.
3. Wählen Sie unter **Typ** die Option **Email (E-Mail)**.
4. Geben Sie eine E-Mail-Adresse ein, an die die E-Mail gesendet werden soll.

5. Geben Sie die anderen Informationen gemäß Ihrem E-Mail-Anbieter ein.
Das Radargerät besitzt keinen eigenen E-Mail-Server. Um E-Mails senden zu können, muss es sich bei einem anderen E-Mail-Server anmelden.
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, z. B. Tampering mail.
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 Lizzenzen anzeigen.
 - **About (Info):** Lassen Sie sich Geräteinformationen, einschließlich AXIS OS-Version und Seriennummer anzeigen.

Status

Geräteinformationen

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

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

Zeitsynchronisierungsstatus

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

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

Sicherheit

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

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

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.

Laufende Aufzeichnungen

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter **Aufzeichnungen, on page 35**



Anzeige des Speicherorts der Aufzeichnung.

Energieverbrauch

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

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

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.

- **0–3:** Wählen Sie diese Option, wenn Sie ein bis vier Radargeräte in demselben Koexistenzbereich installieren.
- **4–5:** Wählen Sie diese Option, wenn Sie vier bis sechs Radargeräte in demselben Koexistenzbereich installieren.
- **6–11:** Wählen Sie diese Option, wenn Sie sieben bis zwölf Radargeräte in demselben Koexistenzbereich installieren.

Erfassung

Detection sensitivity (Erfassungsempfindlichkeit): Wählen Sie hier die gewünschte Radar-Empfindlichkeit aus. Ein höherer Wert bedeutet einen größeren Erfassungsbereich, aber auch eine 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.
 - **Ignore unknown objects (Unbekannte Objekte ignorieren)**: Aktivieren Sie diese Option, um Fehlalarme durch Objekte zu minimieren, die das Radargerät nicht klassifizieren kann.
- **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.
 - **Ignore unknown objects (Unbekannte Objekte ignorieren)**: Aktivieren Sie diese Option, um Fehlalarme durch Objekte zu minimieren, die das Radargerät nicht klassifizieren kann.

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 ist ein Bereich, in dem sich bewegende Objekte ignoriert werden. Verwenden Sie Ausschlussbereiche, wenn es in einem Szenarios Bereiche gibt, die häufig Fehlalarme auslösen.



: Klicken Sie hier, um einen neuen Ausschlussbereich 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 Ausschlussbereiche 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): Wählen Sie die vorläufige Form des Ausschlussbereichs.

- **Cover everything (Alles abdecken):** Wählen Sie diese Option aus, um eine Ausschlusszone zu wählen, die den gesamten Überwachungsbereich des Radargeräts abdeckt.
- **Reset to box (Auf Feld zurücksetzen):** Wählen Sie diese Option aus, um einen rechteckigen Ausschlussbereich in der Mitte des Überwachungsbereichs 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 Szenario zu erstellen. Sie können bis zu 20 Szenarien erstellen.

Triggering conditions (Auslösebedingungen): Wählen Sie die Bedingung aus, die Alarne 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 Alarne 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.
 - : Klicken Sie darauf, um den Datumsmodifikator %F hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
 - : Klicken Sie darauf, 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.
 - : Klicken Sie darauf, um den Datumsmodifikator %F hinzuzufügen und das Format JJJJ-MM-TT anzuzeigen.
 - : Klicken Sie darauf, 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.

Dynamische LED-Leiste

Muster dynamischer LED-Leisten

Auf dieser Seite können Sie die Muster der dynamischen LED-Leiste testen.

Muster: Wählen Sie das Muster aus, das Sie testen möchten.

Dauer: Geben Sie die Dauer des Tests an.

Test: Klicken Sie hier, um das zu testende Muster zu starten.

Stopp: Klicken Sie hier, um den Test anzuhalten. Wenn Sie die Seite verlassen, während ein Muster abgespielt wird, wird der Test automatisch angehalten.

Um ein Muster zu Anzeige- oder Abschreckungszwecken zu aktivieren, gehen Sie zu **System > Ereignisse** und erstellen Sie eine Regel. Ein Beispiel dazu finden Sie unter *Abwechselnd aufblinkendes rotes Lichts am Radar, on page 23*.

Analyse

Metadatenkonfiguration

Hersteller von RTSP-Metadaten

Zeigen Sie die Datenkanäle an, die Metadaten streamen, und übernehmen Sie die Verwaltung dieser sowie der von ihnen verwendeten Kanäle.

Hinweis

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

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

Kanal: Der Kanal, über den Metadaten von einem Produzenten gesendet werden. Aktivieren Sie diese Option, um den Metadaten-Stream zu aktivieren. Schalten Sie diese Option aus Gründen der Kompatibilität oder Ressourcenverwaltung aus.

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 unsignerter 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 Lizenzcode und die Seriennummer des Axis Produkts, um einen Lizenzschlüssel zu generieren.
- **Lizenz automatisch aktivieren:** Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Gehen Sie über diese Option, wenn Ihr Gerät über einen Internetzugang verfügt. Sie benötigen einen Lizenzschlüssel, um die Lizenz zu aktivieren.
- **Lizenz deaktivieren:** Deaktivieren Sie die Lizenz, um sie durch eine andere Lizenz zu ersetzen, z. B. wenn Sie von einer Testlizenz zu einer vollständigen Lizenz wechseln. Wenn Sie die Lizenz deaktivieren, wird sie damit auch vom Gerät entfernt.
- **Settings (Einstellungen):** Darüber werden die Parameter konfiguriert.
- **Löschen:** Löschen Sie die App dauerhaft vom Gerät. Wenn Sie nicht erst die Lizenz deaktivieren, bleibt sie aktiv.

System

Uhrzeit und Ort

Datum und Uhrzeit

Das Zeitformat hängt von den Spracheinstellungen des Webbrowsers ab.

Hinweis

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

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

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

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

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

Hinweis

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

Gerätestandort

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

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

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

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

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

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

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

Hinweis

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

IPv6

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

Hostname

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

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

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

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

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

DNS-Server

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

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

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

Hinweis

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

HTTP und HTTPS

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

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

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

Hinweis

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

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

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

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

Netzwerk-Erkennungsprotokolle

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

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

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

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

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

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

Netzwerk-Ports

Power and ethernet (Stromversorgung und Ethernet): Wählen Sie diese Option aus, um das Netzwerk für den Switch Port einzuschalten.

Power only (Nur Strom): Wählen Sie diese Option aus, um das Netzwerk für den Switch Port auszuschalten. Der Port stellt weiterhin Power over Ethernet bereit.

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 Domännamen 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.

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

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

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

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

Authentication method (Authentifizierungsmethode):

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

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

SNMP

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

SNMP: Die zu verwendende SNMP-Version wählen.

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

Hinweis

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

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

Sicherheit

Zertifikate

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

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

Diese Formate werden unterstützt:

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

Wichtig

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



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

- **Mehr** : Weitere Felder anzeigen, die Sie ausfüllen oder auswählen müssen.
 - **Secure keystore (Sicherer Schlüsselspeicher)**: Wählen Sie Trusted Execution Environment (SoC TEE), Secure element oder Trusted Platform Module 2.0 zum sicheren Speichern des privaten Schlüssels aus. Weitere Informationen zum zu wählenden sicheren Schlüsselspeicher finden Sie unter help.axis.com/axis-os#cryptographic-support.
 - **Key type (Schlüsseltyp)**: Wählen Sie in der Dropdown-Liste zum Schutz des Zertifikats den Standard- oder einen anderen Verschlüsselungsalgorithmus aus.
- ⋮
- Das Kontextmenü enthält:
 - **Certificate information (Zertifikatsinformationen)**: Die Eigenschaften eines installierten Zertifikats anzeigen.
 - **Delete certificate (Zertifikat löschen)**: Löschen Sie das Zertifikat.
 - **Create certificate signing request (Signierungsanforderung erstellen)**: Erstellen Sie eine Anforderung zur Zertifikatsignierung, um sie an eine Registrierungsstelle zu senden und ein digitales Zertifikat zu erhalten.

Secure keystore (Sicherer Schlüsselspeicher) :

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

Kryptografierichtlinie

Die Kryptografierichtlinie legt fest, wie die Verschlüsselung zum Schutz der Daten eingesetzt wird.

Aktiv: Wählen Sie die Kryptografierichtlinie aus, die auf das Gerät angewendet werden soll:

- Standard – OpenSSL: Ausgewogene Sicherheit und Leistung für den allgemeinen Gebrauch.
- FIPS – Richtlinie zur Einhaltung von FIPS 140-2: Verschlüsselung gemäß FIPS 140-2 für regulierte Industrien.

Network access control and encryption (Netzwerzugangskontrolle und Verschlüsselung)

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Zertifikate

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Brute-Force-Angriffe verhindern

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

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

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

Firewall

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

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

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

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

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

Rule type (Regeltyp):

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

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

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

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

Benutzerdefiniertes signiertes AXIS OS-Zertifikat

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

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

- ⋮
 - Das Kontextmenü enthält:
 - **Delete certificate (Zertifikat löschen):** Löschen Sie das Zertifikat.

Konten

Konten



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

Konto: Geben Sie einen eindeutigen Kontonamen ein.

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

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

Privileges (Rechte):

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
 - **Bediener:** Hat Zugriff auf alle Einstellungen, außer:
 - Alle **System-Einstellungen**
 - **Betrachter:** 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**, **OpenID** und **Client Credential Grant (Client-Zugangsdaten-Genehmigung)**.

HTTPS: Wählen Sie diese Option aus, um HTTPS zu verwenden.



Das Kontextmenü enthält:

- **Update virtual host (Virtuellen Host aktualisieren)**
- **Delete virtual host (Virtuellen Host löschen)**

Konfiguration der Client-Zugangsdaten-Genehmigung

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

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

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

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

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

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

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

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

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

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

Ereignisse

Regeln

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

Hinweis

Es können bis zu 256 Aktionsregeln erstellt werden.



Regel hinzufügen: Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

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

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

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

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



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

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

Ihr Produkt verfügt möglicherweise über einige der folgenden vorkonfigurierten Regeln:

Front-facing LED Activation (Aktivierung der Front-LED): LiveStream: Wenn das Mikrofon eingeschaltet ist und ein Live-Stream empfangen wird, wird die Front-LED des Audiogeräts grün.

Front-facing LED Activation (Aktivierung der Front-LED): Recording (Aufzeichnung): Wenn das Mikrofon eingeschaltet ist und eine Aufzeichnung läuft, wird die Front-LED des Audiogeräts grün.

Front-facing LED Activation (Aktivierung der Front-LED): SIP : Wenn das Mikrofon eingeschaltet ist und ein SIP-Anruf aktiv ist, leuchtet die Front-LED des Audiogeräts grün. SIP muss auf dem Audiogerät aktiviert sein, bevor dieses Ereignis ausgelöst werden kann.

Pre-announcement tone: Play tone on incoming call (Durchsageton: Abspielen eines Tons bei eingehendem Anruf): Wenn ein SIP-Anruf beim Audiogerät erfolgt, wird vom Gerät ein vordefinierter Audioclip abgespielt. SIP muss für das Audiogerät aktiviert sein. Damit der SIP-Anrufer einen Klingelton hört, während der Audioclip abgespielt wird, muss das SIP-Konto des Audiogeräts so konfiguriert werden, dass es den Anruf nicht automatisch beantwortet.

Pre-announcement tone: Answer call after incoming call-tone (Durchsageton: Anruf nach eingehendem Rufton annehmen): Nach dem Ende des Audioclips wird der eingehende SIP-Anruf beantwortet. SIP muss für das Audiogerät aktiviert sein.

Loud ringer (Lauter Klingelton): Wenn ein SIP-Anruf beim Audiogerät erfolgt, wird ein vordefinierter Audioclip abgespielt, solange die Regel aktiv ist. SIP muss für das Audiogerät aktiviert sein.

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. Andernfalls 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 anzugebende E-Mail-Adresse ein.

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

Hinweis

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

- **TCP**

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

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



Das Kontextmenü enthält:

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

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

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

Zeitschemata

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



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

Manuelle Auslöser

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

MQTT

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

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

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

ALPN

Bei ALPN handelt es sich um eine TLS/SSL-Erweiterung, mit der während der Handshake-Phase der Verbindung zwischen Client und Server ein Anwendungsprotokoll ausgewählt werden kann. Auf diese Weise können Sie 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 Verbindungsrichtung 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 einzugeben 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 einzugeben zu können.

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

Nutzlast: Geben Sie den Inhalt für die Standardnachricht ein.

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

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

MQTT-Warteschlange

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

Include condition (Bedingung einbeziehen): Wählen Sie diese Option aus, um das Thema einzufügen, das die Bedingung des MQTT-Themas beschreibt.

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

Include serial number (Seriennummer hinzufügen): Wählen Sie diese Option aus, 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

Network storage (Netzwerk-Speicher): Schalten Sie diese Option ein, um den Netzwerk-Speicher zu benutzen.

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):** Ändern Sie das zum Verschlüsseln der SD-Karte erforderliche Kennwort.

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

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

Onboard-Speicher

Festplatte

- **Free (Frei)**: Freier Platz auf dem Datenträger.
- **Status**: Ob das Laufwerk bereitsteht ist oder nicht.
- **Dateisystem**: Das von der Festplatte verwendete Dateisystem.
- **Verschlüsselt**: Ob das Laufwerk verschlüsselt ist oder nicht.
- **Temperatur**: Die aktuelle Temperatur der Hardware.
- **Overall health test (Allgemeiner Zustandstest)**: Das Ergebnis nach Überprüfung des Datenträgerzustands.

Werkzeuge

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

Unmount (Trennen)  : Klicken Sie, bevor Sie das Gerät vom System trennen. Dies beendet alle laufenden Aufzeichnungen.

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

Autoformat (Automatisch formatieren)  : Das Laufwerk wird automatisch mit dem ext4-Dateisystem formatiert.

Onboard-Speicher

RAID

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

Werkzeuge

Hinweis

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

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

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

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

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 einzubehaltenden Overlays aus. Weitere Informationen zum Hinzufügen von Overlays finden Sie unter *Overlays, on page 32*.

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.

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
 - 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 Medienstremeinstellungen 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.

Profilename: 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

Stoßfassung

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

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

Energieeinstellungen

Energieverbrauch

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

Energieeinstellungen

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

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

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

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

Hinweis

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

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

Power warning overlay (Overlay für Energiewarnung)  : Aktivieren Sie diese Option, um ein Overlay für die Energiewarnung anzuzeigen, wenn das Gerät nicht über ausreichend Energie verfügt.

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

Stommesser

Energieverbrauch

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

- ⋮
 - Das Kontextmenü enthält:
 - Exportieren: Klicken Sie hier, um die Diagrammdaten zu exportieren.

Edge-to-Edge

Kopplung

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



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

Discover devices (Geräte erkennen): Klicken Sie, um Geräte im Netzwerk zu suchen. Nach der Suche wird eine Liste der im Netzwerk verfügbaren Geräte angezeigt.

Hinweis

Die Liste enthält alle gefundenen Axis Geräte und nicht nur die, die gekoppelt werden können.

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

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.

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.

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.

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.

Mit **Generic pairing (Generische Kopplung)** können Sie ein Gerät mit Licht- und Sirenenfunktion koppeln.

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

Kopplungstyp auswählen: Aus dem Aufklappmenü wählen.

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

Username (Benutzername): Geben Sie den Benutzernamen ein.

Password (Kennwort): Geben Sie das Kennwort ein.

Certificate name (Name des Zertifikats): Geben Sie den Namen des Zertifikats 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.

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

Remote System Log

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



Server: Klicken Sie, um einen neuen Server hinzuzufügen.

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

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

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

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

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

Direktkonfiguration

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

Wartung

Wartung

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

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

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

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

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

Bei der Aktualisierung können Sie zwischen drei Optionen wählen:

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

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

Fehler beheben

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

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

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

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

Netzwerk-Trace

Wichtig

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

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

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

Mehr erfahren

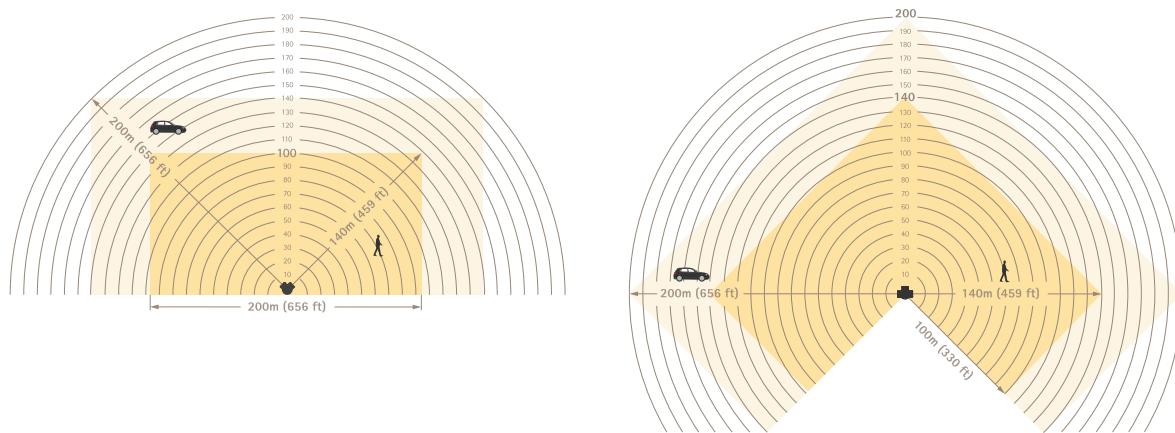
Radar

Erkennungs- und Erfassungsbereich

Der Erkennungsbereich ist der Bereich, in dem das Radargerät Objekte mit Sicherheit als Personen oder Fahrzeuge klassifizieren kann.

Der Erfassungsbereich ist der Bereich, in dem das Radargerät schnell fahrende Fahrzeuge detektieren kann.

Die Größe der Bereiche hängt von der Montagehöhe des Radargeräts sowie anderen Faktoren ab.



Der Koexistenzbereich ist dunkelgelb und der Erfassungsbereich ist hellgelb.

Szenarien, Einschlussbereiche und Ausschlussbereiche

Ein Szenario besteht aus einer Reihe von Bedingungen, die sich bewegende Objekte erfüllen müssen, um Regeln im Ereignissystem auszulösen. Zu den Bedingungen gehören die folgenden:

- Objekttyp (Person, Fahrzeug, unbekannt)
- Objektverhalten (Bewegung im Bereich oder Überfahren von Linien / Überschreiten von Linien)
- Teil der Szene (Einschlussbereich oder virtuelle Linie)
- Objektgeschwindigkeit

Der **Einschlussbereich** ist der Teil der Szene, in dem Objekte in einem Szenario des Typs „Bewegung im Bereich“ detektiert und klassifiziert werden.

Gibt es in einer Szene Bereiche, in denen sich bewegende Objekte keinen Alarm auslösen sollen, können Sie **Ausschlussbereiche** für diese festlegen. Außerdem können Sie Ausschlussbereiche für Zonen in einem Einschlussbereich verwenden, in denen häufig Fehlalarme ausgelöst werden. In einem Ausschlussbereich werden sich bewegende Objekte ignoriert. Sie erlauben zum Beispiel das Herausfiltern von schaukelndem Laub am Straßenrand oder Doppelerfassungen, die durch Objekte aus radarreflektierenden Materialien wie Metallzäunen verursacht werden.

Koexistenzbereich

Sie können mehrere Radargeräte installieren, um Bereiche abzudecken, die größer sind als der angegebene Erfassungsbereich eines einzelnen Radargeräts. Radargeräte mit derselben Funkfrequenz können sich gegenseitig elektromagnetisch stören, was ihre Leistung beeinträchtigen kann. Jedes Radarmodell von Axis besitzt einen festgelegten Koexistenzbereich. Innerhalb dieses Bereichs können Sie eine bestimmte Anzahl von Radargeräten installieren, ohne dass sich diese gegenseitig stören. Informationen zum Radius und zur empfohlenen maximalen Anzahl von Radargeräten in einem Koexistenzbereich finden Sie im Datenblatt des Geräts auf axis.com.

Radar-Video-Fusionstechnologie

Die Radar-Video-Fusion vereint die Vorteile eines Axis Radargeräts mit denen einer Axis Kamera. Diese Kombination ermöglicht ein hervorragendes Situationsbewusstsein und reduziert Fehlalarme. Bei Kopplung einer ARTPEC-9-PTZ-Kamera mit einem ARTPEC-9-Radargerät in der Weboberfläche der Kamera kann das Radargerät ein sich bewegendes Objekt erkennen und klassifizieren, die Kamera auf das Objekt ausrichten und die Klassifizierung von der Kamera überprüfen lassen. Die Kamera kann das Objekt dann mit der Objektverfolgung weiter verfolgen. Weitere Informationen hierzu finden Sie im Benutzerhandbuch der PTZ-Kamera.

Automatische Nachführung

Sie können Radardaten zu den Positionen verschiedener Objekte verwenden, um eine PTZ-Kamera Objekte verfolgen zu lassen. Es gibt drei verschiedene Optionen:

- Die Kopplung mehrerer PTZ-Kameras und Radargeräte ist mit der Anwendung AXIS Radar Autotracking for PTZ möglich. Weitere Informationen finden Sie unter *Steuern einer PTZ-Kamera mit AXIS Radar Autotracking for PTZ, on page 77*.
- Zur Kopplung eines Radargeräts und einer ARTPEC-7-PTZ-Kamera bei benachbarter Montage können Sie die integrierte Radar-Objektverfolgung über die Kamerakopplung verwenden.
- Wenn Sie ein Radargerät und eine ARTPEC-9-PTZ-Kamera bei kombinierter Montage koppeln möchten, können Sie die integrierte Objektverfolgung mit Radar-Video-Fusion über die Kamerakopplung verwenden. Diese Option kombiniert Kl-gestützte Radar- und Videoanalysefunktionen zur Minimierung von Fehlalarmen. Anweisungen zur Einrichtung der Objektverfolgung mit Radar-Video-Fusion finden Sie im Benutzerhandbuch der PTZ-Kamera auf help.axis.com/axis-q6325-le.

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.

Overlays

Overlays werden über den Videostream gelegt. Sie werden verwendet, um weitere Informationen anzuzeigen, wie etwa Zeitstempel oder auch während des Installierens und Konfigurierens des Produkts. Sie können entweder Text oder ein Bild hinzufügen.

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 lizenziierter 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.

AV1

AV1 (AOMedia Video 1) ist ein lizenzenfreies Videocodierungsformat, das für Videostreaming optimiert ist. AV1 aktiviert Videostreams in hoher Qualität auch in Umgebungen mit begrenzter Bandbreite. Durch die Reduzierung der Bitrate eines Videos bewahrt AV1 die Videoqualität und minimiert gleichzeitig den Datenverbrauch.

AV1 unterstützt alle wichtigen Browser, Computer-Betriebssysteme und mobilen Plattformen.

Hinweis

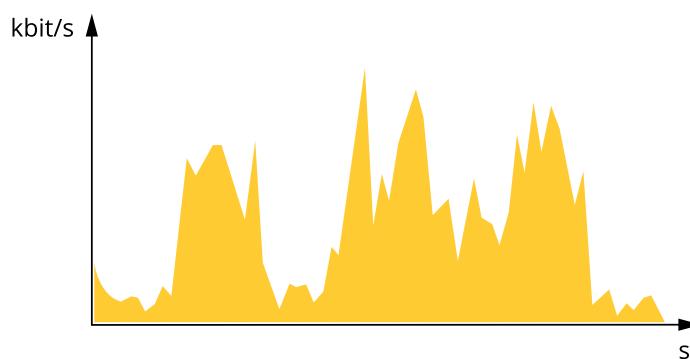
AV1 erfordert im Vergleich zu einigen anderen Codecs mehr Rechenleistung für die Encoder und Decoder.

Bitrate-Steuerung

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

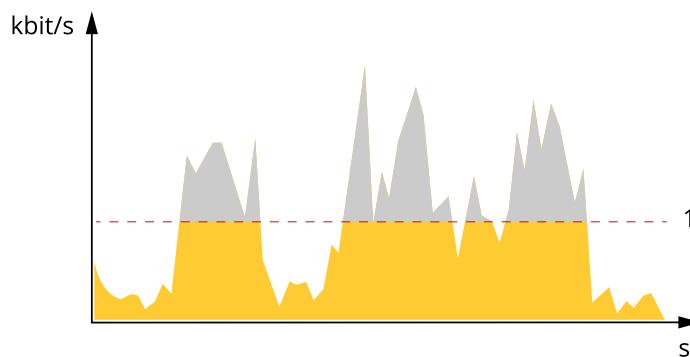
Variable Bitrate (VBR)

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.

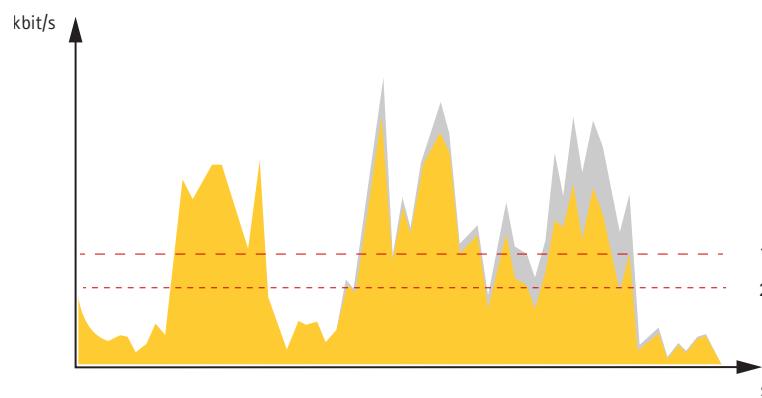


1 Zielbitrate

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:

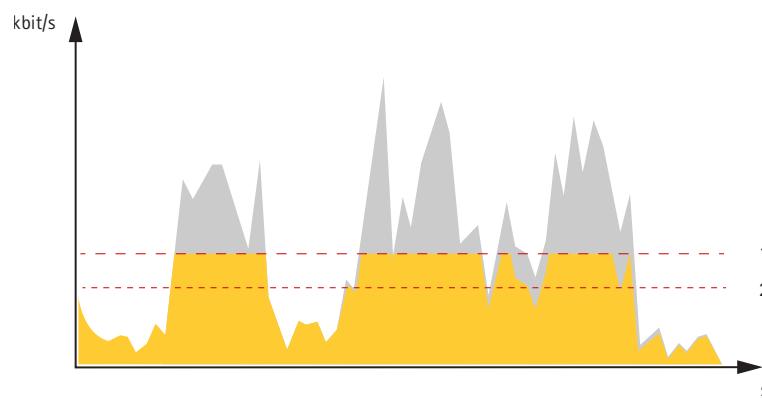
- Um den geschätzten Speicherbedarf zu berechnen, stellen Sie die Zielbitrate und die Aufbewahrungszeit ein.
- Um die durchschnittliche Bitrate auf Grundlage des verfügbaren Speichers und der erforderlichen Aufbewahrungszeit zu berechnen, verwenden Sie den Zielbitratenrechner.



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

Edge-to-Edge-Technologie

Edge-to-Edge ist eine Technologie, mit der IP-Geräte direkt miteinander kommunizieren. Sie bietet eine intelligente Koppelungsfunktion z. B. zwischen Axis Kameras und Axis Audio- oder Radarprodukten.

Weitere Informationen finden Sie im Whitepaper „Edge-to-Edge-Technologie“ unter whitepapers.axis.com/edge-to-edge-technology.

Lautsprecherkopplung

Mit der Edge-to-edge-Lautsprecher-Kopplung können kompatible Netzwerk-Lautsprecher von Axis so eingesetzt werden, als seien sie ein Teil der Kamera. Nach der Kopplung werden die Lautsprecherfunktionen in die Weboberfläche der Kamera integriert. Der Netzwerklautsprecher fungiert als Audio-Out-Gerät, mit dem Sie Audio-Clips wiedergeben und Audiosignale über die Kamera übertragen können.

Die Kamera identifiziert sich zur VMS als Kamera mit integriertem Audioausgang und leitet alle abgespielten Audiosignale an den Lautsprecher weiter.

Mikrofonkopplung

Mit der Edge-to-edge-Mikrofon-Kopplung können kompatible Mikrofon von Axis so eingesetzt werden, als seien sie ein Teil der Kamera. Nach der Kopplung nimmt das Netzwerk-Mikrofon Geräusche aus der Umgebung auf und steht als Audioeingabegerät zur Verfügung, das in Medienstreams und Aufzeichnungen verwendet werden kann.

Cybersicherheit

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

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

Axis Sicherheitsbenachrichtigungsdienst

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

Schwachstellen-Management

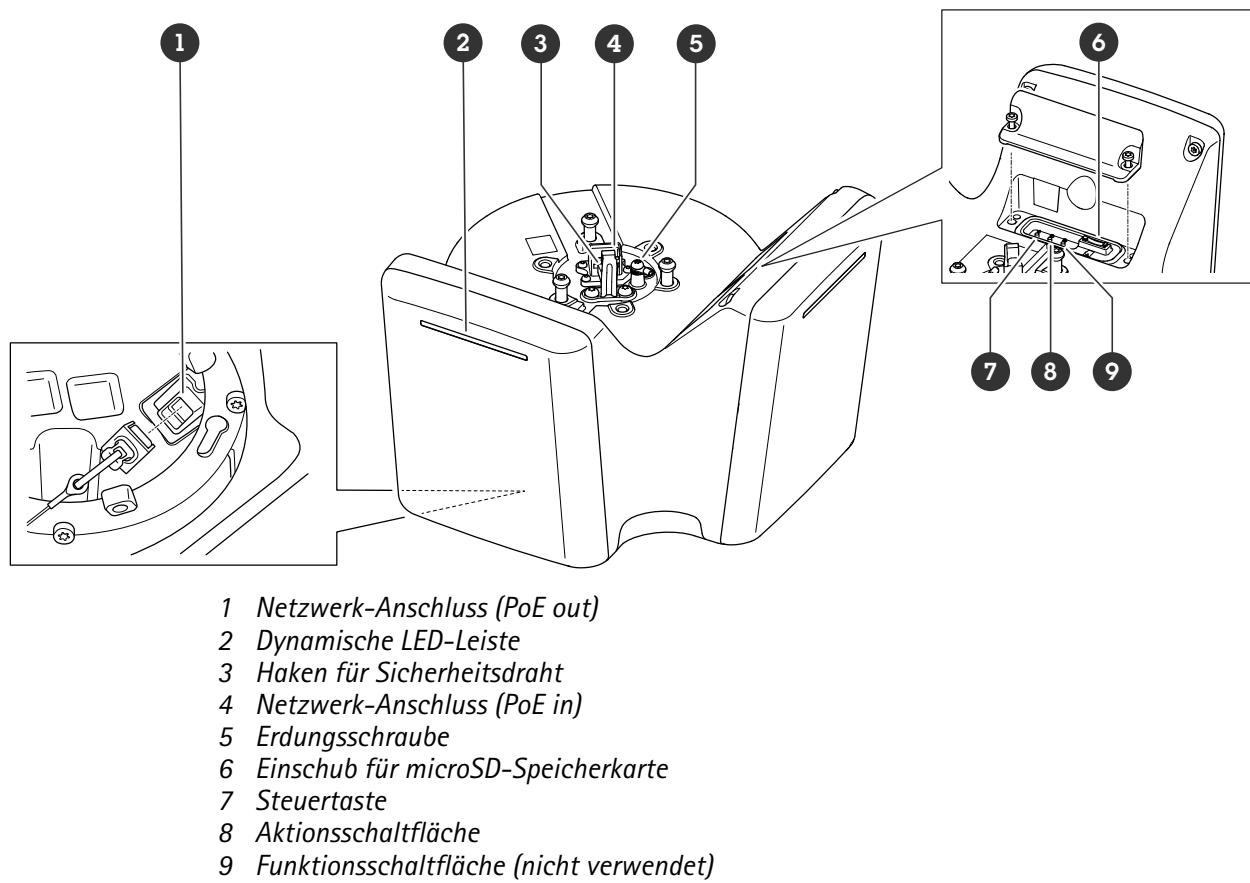
Um das Risiko für die Kunden zu minimieren, hält sich Axis als **Common Vulnerability and Exposures (CVE) Numbering Authority (CNA)** an Branchenstandards, um entdeckte Schwachstellen in unseren Geräten, unserer Software und unseren Dienstleistungen zu verwalten und darauf zu reagieren. Weitere Informationen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

Sicherer Betrieb von Axis Geräten

Axis Geräte mit werksseitig festgelegten Standardeinstellungen sind mit sicheren Standardschutzeinrichtungen vorkonfiguriert. Es wird empfohlen, das Gerät mit mehr Sicherheit zu konfigurieren. Mehr über den Ansatz von Axis für die Cybersicherheit, einschließlich bewährter Verfahren, Ressourcen und Richtlinien zur Sicherung Ihrer Geräte, lesen Sie auf axis.com/about-axis/cybersecurity.

Technische Daten

Produktübersicht



LED-Anzeigen

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.
Gelb	Leuchtet beim Start. Blinkt während Gerätesoftwareaktualisierung und Wiederherstellung der Werkseinstellungen.

Muster dynamischer LED-Leisten
Rot
Blau
Grün
Gelb
Weiß
Wechselndes Rot
Wechselndes Blau
Wechselndes Grün
Blinkend rot, blau, weiß

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 Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 84*.

Anschlüsse

Netzwerk-Anschluss (PoE in)

RJ45-Ethernetanschluss mit Power over Ethernet IEEE 802.3bt, Typ 4 Klasse 8.

Hinweis

Power over Ethernet IEEE 802.3bt, Typ 4 Klasse 8 ist für PoE-Ausgang erforderlich. Wenn kein zweites Gerät mit Strom zu versorgen ist, reicht Power over Ethernet IEEE 802.3at, Typ 2 Klasse 4, aus.

Netzwerk-Anschluss (PoE out)

Power over Ethernet IEEE 802.3bt, Typ 3 Klasse 6.

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

Hinweis

- Die Stromversorgung des Radargeräts über Power over Ethernet IEEE 802.3bt, Typ 4, Klasse 8 ermöglicht den Anschluss eines zweiten Geräts, das Power over Ethernet IEEE 802.3bt, Typ 3, Klasse 6 verwendet.
- Die Stromversorgung des Radargeräts über Power over Ethernet IEEE 802.3bt, Typ 3, Klasse 6 ermöglicht den Anschluss eines zweiten Geräts, das Power over Ethernet IEEE 802.3bt, Typ 2, Klasse 4 verwendet.
- Bei der Stromversorgung des Radargeräts über Power over Ethernet IEEE 802.3bt, Typ 2, Klasse 4 ist 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.

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 *Produktübersicht, on page 81*.
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**.

Stellen Sie sicher, dass keiner die Gerätesoftware manipuliert hat.

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

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen, on page 84*. Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Optionen für AXIS OS

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

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

Aktuelle AXIS OS-Version überprüfen

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

So überprüfen Sie die aktuelle AXIS OS-Version:

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

AXIS OS aktualisieren

Wichtig

- Bei der Aktualisierung der Gerätesoftware werden Ihre vorkonfigurierten und benutzerdefinierten Einstellungen gespeichert. Axis Communications AB kann nicht garantieren, dass die Einstellungen gespeichert werden, selbst wenn die Funktionen in der neuen AXIS OS-Version verfügbar sind.
- Ab AXIS OS 12.6 müssen Sie jede einzelne LTS-Version zwischen der aktuellen Version Ihres Geräts und der Zielversion installieren. Wenn beispielsweise die derzeit installierte Gerätesoftwareversion AXIS OS 11.2 ist, müssen Sie die LTS-Version AXIS OS 11.11 installieren, bevor Sie das Gerät auf AXIS OS 12.6 aktualisieren können. Weitere Informationen finden Sie unter *AXIS OS Portal: Upgrade-Pfad*.
- Stellen Sie sicher, dass das Gerät während der Aktualisierung an die Stromversorgung angeschlossen ist.
- Stellen Sie zur Vermeidung von Fehlschlägen bei der Installation sicher, dass während des Aktualisierens die Abdeckung angebracht 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 Aktualisieranweisungen und Versionshinweise. Die aktuelle AXIS OS-Version und die Versionshinweise finden Sie unter axis.com/support/device-software.
1. Die AXIS OS-Datei können Sie von axis.com/support/device-software kostenlos auf Ihren Computer herunterladen.
 2. Melden Sie sich auf dem Gerät als Administrator an.
 3. Rufen Sie Maintenance (Wartung) > AXIS OS upgrade (AXIS OS-Aktualisierung) auf und klicken Sie Upgrade (Aktualisieren) an.

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Probleme und mögliche Lösungen

Probleme beim Aktualisieren von AXIS OS

Aktualisierung von AXIS OS fehlgeschlagen

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

Probleme nach der AXIS OS-Aktualisierung

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

Probleme beim Einrichten der IP-Adresse

IP-Adresse kann nicht eingestellt werden

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

Probleme beim Zugriff auf das Gerät

Anmeldung bei Gerätezugriff über einen Browser nicht möglich

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

Bei Verlust des Kennworts für das Haupt-Konto müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen. Anweisungen finden Sie unter *Zurücksetzen auf die Werkseinstellungen, on page 84*.

Die IP-Adresse wurde von DHCP geändert

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

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

Zertifikatfehler beim Verwenden von IEEE 802.1X

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

Der Browser wird nicht unterstützt.

Eine Liste der empfohlenen Browser finden Sie unter *Unterstützte Browser, on page 15*.

Externer Zugriff auf das Gerät ist nicht möglich

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

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

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

Probleme mit MQTT

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

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

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

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

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

Probleme mit dem Bild

Bildverschlechterung oder Bildverlust

- Überprüfen Sie den Server-Bericht des Geräts auf die Anzahl der zur Sensoreinheit verloren gegangenen Verbindungen.
- Stellen Sie sicher, dass das Verbindungskabel zwischen Sensoreinheit und Haupteinheit fest sitzt.
- Wechseln Sie das Kabel der Sensoreinheit.

Probleme aufgrund von Selbstabschaltung des Geräts

Das Gerät schaltet sich ab

- Trennen Sie das Gerät und schließen Sie es erneut an.
- Überprüfen Sie, ob das **Verzögerte Herunterfahren** aktiviert ist. Ist diese Option aktiviert, wird die Haupteinheit gemäß der festgelegten Verzögerungszeit ausgeschaltet. Sie können die Option **Delayed shutdown (Verzögertes Herunterfahren)** innerhalb von 300 Sekunden deaktivieren, bevor sich das Gerät erneut ausschaltet.

Leistungsaspekte

Achten Sie bei der Einrichtung Ihres Systems unbedingt darauf, wie sich die verschiedenen Einstellungen und Situationen auf die erforderliche Bandbreite (Bitrate) auswirken.

Die wichtigsten Umstände, die Sie berücksichtigen müssen, sind die folgenden:

- Durch Entfernen oder Anbringen der Abdeckung wird die Kamera neu gestartet.
- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

Support

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

T10223326_de

2026-01 (M1.36)

© 2025 – 2026 Axis Communications AB