

AXIS D2210-VE Radar

Benutzerhandbuch

AXIS D2210-VE Radar

Inhalt

Installation	3
Installationsanleitung	3
Zu beachtende Aspekte	3
Radarprofile	6
Profil für Bereichsüberwachung	6
Profil für Straßenüberwachung	9
Erste Schritte	14
Das Gerät im Netzwerk ermitteln	14
Weboberfläche des Geräts öffnen	14
Erstellen Sie ein Administratorkonto	14
Sichere Kennwörter	14
Stellen Sie sicher, dass keiner die Firmware manipuliert hat.	15
Übersicht über die Weboberfläche	15
Ihr Gerät konfigurieren	16
Ein Radarprofil auswählen	16
Radar kalibrieren	16
Erfassungsbereiche festlegen	17
Fehlalarme minimieren	20
Das Radarbild anpassen	21
Video ansehen und aufnehmen	22
Einrichten von Regeln für Ereignisse	23
Die Weboberfläche	30
Status	30
Radar	31
Aufzeichnungen	38
Apps	39
System	39
Wartung	60
Ihre Installation validieren	62
Installation des Radars validieren	62
Validierung abschließen	63
Mehr erfahren	64
Streaming und Speicher	64
Overlays	66
Technische Daten	67
Produktübersicht	67
LED-Anzeigen	67
Einschub für SD-Speicherkarte	68
Tasten	68
Anschlüsse	68
Empfehlungen zur Reinigung	71
Fehlerbehebung	72
Zurücksetzen auf die Werkseinstellungen	72
Aktuelle Firmware überprüfen	72
Firmware aktualisieren	72
Technische Fragen, Hinweise und Lösungen	73
Leistungsaspekte	74
Support kontaktieren	74

AXIS D2210-VE Radar

Installation

Installation



Installationsvideo für das Produkt.

Installationsanleitung

Die Installationsanleitung und andere Unterlagen zu diesem Produkt finden Sie auf axis.com/products/axis-d2210-ve-radar/support.

Zu beachtende Aspekte

Der richtige Installationsort

Bereichs- oder Straßenüberwachung

Der Radar wurde für die Überwachung offener Bereiche entwickelt und kann sowohl für die Bereichs- als auch für die Straßenüberwachung eingesetzt werden. Der Radar verfügt über zwei Profile, damit für jedes der Szenarien die optimale Leistung herausgeholt werden kann. Weitere Informationen zu Erfassungsbereich, Installationsbeispielen und Einsatzgebieten finden Sie unter *Radarprofile auf Seite 6*.

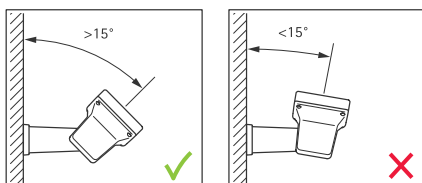
Feststehende und reflektierende Objekte vermeiden

Die meisten feststehende Objekte (z. B. Mauern, Zäune, Bäume oder hohe Sträucher) im Erfassungsbereich erzeugen einen blinden Fleck (Radarschatten) hinter dem Objekt. Metallobjekte im Sichtfeld verursachen Reflexionen, die die Klassifizierungsfähigkeit des Radars beeinträchtigen. Dadurch kann es im Radarstream zu Phantomverfolgungen und Fehlalarmen kommen. Informationen zum Umgang mit feststehenden Objekten und reflektierenden Oberflächen finden Sie unter *Ausschlussbereiche hinzufügen auf Seite 19*.

Positionierung

Installieren Sie das Produkt an einem stabilen Mast oder an einer Wand, an der sich keine anderen Objekte oder Installationen befinden. Objekte im Umkreis von 1 m links und rechts vom Gerät, die Funkwellen reflektieren, beeinträchtigen die Leistungsfähigkeit des Radars.

Wenn Sie das Produkt an einer Wand installieren, muss es in einem Winkel von mindestens 15° von der Wand weg zeigen.



AXIS D2210-VE Radar

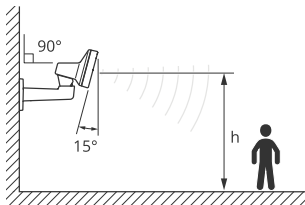
Installation

Drehwinkel

Der Drehwinkel des Produkts muss nahezu gleich Null sein. Das bedeutet, dass der Radar auf Höhe des Horizonts liegen muss.

Neigungswinkel

Der Radar kann um 0 bis 30° geneigt werden. Das Gerät sollte bei der Montage jedoch um 15° geneigt werden. Stellen Sie sicher, dass der hintere Teil des Gehäuses wie in der Abbildung gezeigt um 15° geneigt ist.



In die Live-Ansicht des Radars kann ein Overlay mit Angabe des Neigungswinkels des Radars hinzugefügt werden. Anweisungen dazu finden Sie unter *Text-Overlay mit Angabe des Neigungswinkels des Radars anzeigen auf Seite 21*

Koexistenz

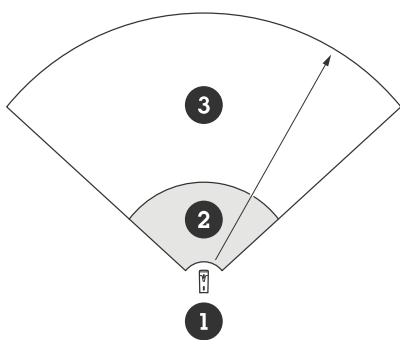
Wenn Sie mehr als acht Axis Radargeräte, die alle auf einer Frequenz von 60 GHz senden, zu dicht aneinander montieren, kann es zu Interferenzen kommen. Informationen dazu, wie sich Interferenzen vermeiden lassen, finden Sie unter *Mehrere Radargeräte installieren auf Seite 4*.

Mehrere Radargeräte installieren

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

Koexistenz

Die Funkwellen des Radars reichen über den Erfassungsbereich hinaus und können andere Radarmelder in einer Entfernung von bis zu 350 m beeinträchtigen. Dies wird als Koexistenzbereich bezeichnet.



- 1 Radar
- 2 Erfassungsbereich
- 3 Koexistenzbereich

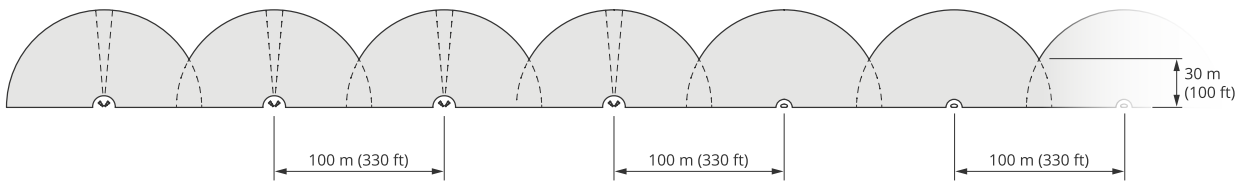
Dieses Radargerät arbeitet auf einer Frequenz von 60 GHz. Es können bis zu acht Radargeräte installiert werden, die auf einer Frequenz von 60 GHz problemlos nahe beieinander oder gegenüberliegend betrieben werden können. Der integrierte Koexistenz-Algorithmus ist in der Lage, ein geeignetes Zeitfenster und einen geeigneten Frequenzkanal zu ermitteln und so mögliche Interferenzen auf ein Minimum zu begrenzen.

AXIS D2210-VE Radar

Installation

Wenn in einer Installation mehr als acht Radare auf derselben Frequenz senden, wobei viele Geräte voneinander weg zeigen, ist die Gefahr von Interferenzen geringer. Radarstörungen führen im Allgemeinen nicht zu einem Ausfall des Radarmelders. Es gibt einen integrierten Algorithmus zur Abschwächung von Interferenzen, der versucht, das Radarsignal auch bei Interferenzen zu reparieren. Bei Betriebsumgebungen mit vielen Radarmeldern, die in ein und demselben Koexistenzbereich auf der gleichen Frequenz senden, ist mit Störungsmeldungen zu rechnen. Störungen wirken sich hauptsächlich in Form einer Verschlechterung der Erkennungsleistung und sporadischer Phantomverfolgungen aus.

Radare von Axis, die auf unterschiedlichen Frequenzen arbeiten, beeinträchtigen sich nicht gegenseitig. Sie können beispielsweise vollkommen störungsfrei AXIS D2210-VE mit mehreren AXIS D2110-VE Security Radars kombinieren, die auf einer Frequenz von 24 GHz senden.



Vier nebeneinander montierte AXIS D2210-VE und mehrere AXIS D2110-VE Security Radars.

Hinweis

AXIS D2110-VE Security Radars erfordert eine zusätzliche Konfiguration, wenn mehr als zwei AXIS D2110-VE in demselben Bereich montiert werden. Weitere Informationen finden Sie im *Benutzerhandbuch zum AXIS D2110-VE Security Radar*.

Umgebung

Bei der Anordnung mehrerer Radarmelder an einem Standort sind weitere Faktoren wie die Umgebung, schaukelnde Objekte, Fahnenmasten und Bepflanzung zu berücksichtigen. In einigen Fällen müssen Sie zur Vermeidung von Fehlalarmen schaukelnde Objekte aus dem Radarstream herausfiltern.

AXIS D2210-VE Radar

Radarprofile

Radarprofile

Mit dem Radar lassen sich Flächen oder Straßen überwachen. Es gibt zwei jeweils für ein Szenario optimierte Profile:

- **Profil für Bereichsüberwachung:** Zur Nachverfolgung von Personen, Fahrzeugen und unbekanntem Objekten, die sich mit einer Geschwindigkeit unter 55 km/h bewegen
- **Profil für Straßenüberwachung:** Hauptsächlich zur Nachverfolgung von Fahrzeugen mit einer Geschwindigkeit von bis zu 200 km/h

Wählen Sie den Bereich bzw. das Überwachungsprofil über die Weboberfläche des Radars aus. Anweisungen dazu finden Sie unter *Ein Radarprofil auswählen auf Seite 16*.

Profil für Bereichsüberwachung

Das Profil zur Bereichsüberwachung wurde für Objekte optimiert, die sich mit einer Geschwindigkeit von bis zu 55 km/h bewegen. Mit diesem Profil können Sie erkennen, ob es sich bei einem Objekt um einen Menschen, ein Fahrzeug oder ein unbekanntes Objekt handelt. Eine Regel kann so eingerichtet werden, dass bei Erkennung eines dieser Objekte eine Aktion ausgelöst wird. Verwenden Sie zum Verfolgen von Fahrzeugen mit höheren Geschwindigkeiten das *Profil für Straßenüberwachung auf Seite 9*.

Abdeckungsbereich

AXIS D2210-VE hat ein horizontales Erfassungsfeld von 95°. Der Abdeckungsbereich entspricht 2.700 m² für Personen und 6.100 m² für Fahrzeuge.

Hinweis

Wenn der Radar in einer Höhe von 3,5 bis 7 m installiert ist, ist eine optimale Bereichsabdeckung gegeben. Die Montagehöhe beeinflusst die Größe des toten Winkels unter dem Radar.

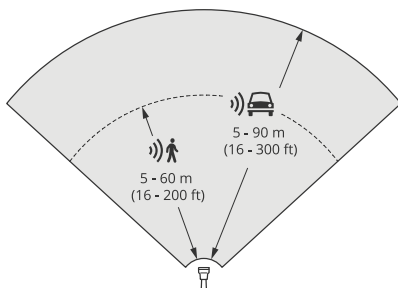
Erfassungsbereich

Der Erfassungsbereich ist die Entfernung, in der ein Objekt verfolgt werden und einen Alarm auslösen kann. Er wird von einer Naherfassungsgrenze (wie nahe am Gerät ist eine Erfassung möglich) bis zu einer Fernerfassungsgrenze (bis zu welcher Entfernung vom Gerät ist eine Erfassung möglich) gemessen.

Das **area monitoring profile (Profil zur Bereichsüberwachung)** ist zwar für die Erfassung von Personen optimiert, aber es lassen damit auch Fahrzeuge und andere Objekte erfassen, die sich bei einer Abweichung von +/- 2 km/h mit bis zu 55 km/h bewegen.

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

- 5 - 60 m bei der Erfassung eines Menschen
- 5 - 90 m bei der Erfassung eines Fahrzeugs



AXIS D2210-VE Radar

Radarprofile

Hinweis

- Geben Sie die Montagehöhe bei der Kalibrierung des Radars auf der Weboberfläche ein.
- Der Erfassungsbereich wird von der Szene und dem Neigungswinkel des Produkts beeinflusst.
- Der Erfassungsbereich wird von Art und Größe des sich bewegenden Objekts beeinflusst.

Der Erfassungsbereich des Radars wurde unter folgenden Bedingungen gemessen:

- Der Bereich wurde entlang des Bodens gemessen.
- Bei dem Objekt handelt es sich um eine 170 cm große Person.
- Die Person ging geradeaus vor dem Radar.
- Die Werte wurden gemessen, als die Person in den Erfassungsbereich eindrang.
- Die Radarempfindlichkeit war auf **Mittel** eingestellt.

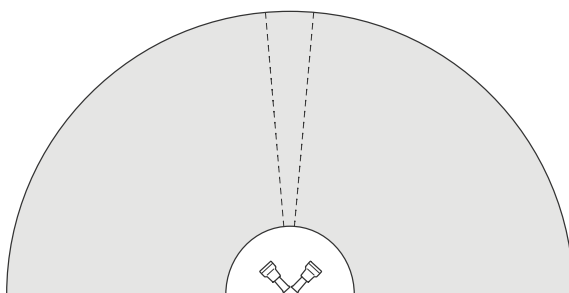
Montagehöhe	0° Neigung	5° Neigung	10° Neigung	15° Neigung	20° Neigung	25° Neigung	30° Neigung
3,5 m	6,0 - 60+ m	5,0 - 60+ m	4,0 - 60+ m	4,0 - 60 m	4,0 - 55 m	4,0 - 40 m	4,0 - 30 m
4,5 m	6,0 - 60+ m	6,0 - 60+ m	5,0 - 60+ m	4,0 - 60+ m	4,0 - 60 m	4,0 - 45 m	4,0 - 40 m
6 m	10 - 60+ m	9,0 - 60+ m	7,0 - 60+ m	6,0 - 60+ m	6,0 - 60 m	5,0 - 55 m	5,0 - 55 m
8 m	16 - 60 m	14 - 60 m	10 - 60 m	8,0 - 60+ m	8,0 - 60+ m	7,0 - 60 m	7,0 - 60 m
10 m	21 - 60 m	19 - 60 m	14 - 60 m	12 - 60+ m	10 - 60+ m	9,0 - 60 m	9,0 - 60 m
12 m	25 - 60 m	23 - 60 m	19 - 60 m	16 - 60+ m	13 - 60+ m	11 - 60+ m	11 - 55 m

Hinweis

- Wenn die Radarempfindlichkeit auf **Niedrig** eingestellt wird, verringert sich der Erfassungsbereich um 20 %, wohingegen eine Einstellung auf **Hoch** den Erfassungsbereich um 20 % erweitert.

Beispiele für Bereichsinstallationen

Um einen virtuellen Zaun zu erstellen, z. B. entlang eines Gebäudes oder um ein Gebäude herum, können Sie bis zu acht AXIS D2210-VE Radare nebeneinander platzieren. Wenn Sie zwei AXIS D2210-VE nebeneinander aufstellen, haben Sie eine Abdeckung von 180°.

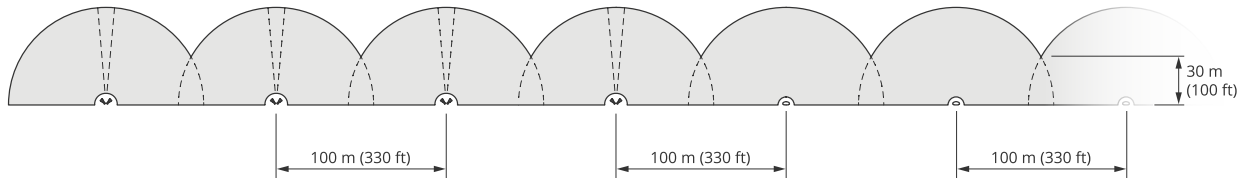


Mit zwei nebeneinander montierten AXIS D2210-VE eine Abdeckung von 180°.

AXIS D2210-VE Radar

Radarprofile

Bei der Installation von mehreren Kameras AXIS D2210-VE nebeneinander sollte jeweils ein Abstand von 100 m eingehalten werden.



Vier Paare der AXIS D2210-VE und mehrere AXIS D2110-VE Security Radars in einem Abstand voneinander von 100 m montiert.

Radare von Axis, die auf unterschiedlichen Frequenzen arbeiten, beeinträchtigen sich nicht gegenseitig. Dies bedeutet, dass Sie AXIS D2210-VE, der auf einer Frequenz von 60 GHz arbeitet, mit dem AXIS D2110-VE Security Radar kombinieren können, der in derselben Zone auf einer Frequenz von 24 GHz arbeitet.

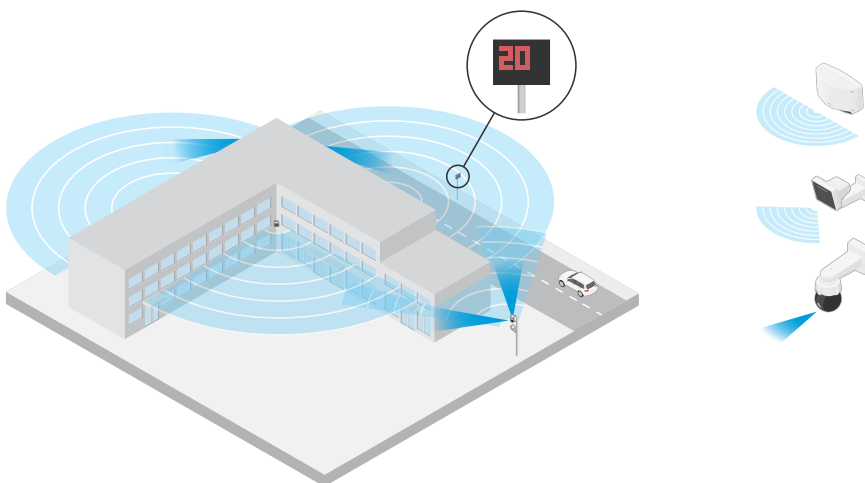
Weitere Informationen zu Koexistenz und Interferenzen finden Sie unter *Mehrere Radargeräte installieren auf Seite 4*.

Einsatzgebiete für die Bereichsüberwachung

Den Bereich um das Gebäude abdecken

Ein in einem Bürogebäude untergebrachtes Unternehmen muss das Gelände vor Eindringlingen und Vandalismus schützen, besonders nach den Geschäftszeiten. Zur Abdeckung des Bereichs um das Gebäude herum installieren sie eine Mischung aus Radaren und PTZ-Kameras. Zur Abdeckung der Längsseiten des Gebäudes setzen sie AXIS D2110-VE Security Radars mit einer Abdeckung von 180° und für die schmalere Seiten und Ecken AXIS D2210-VE Radar mit einer Abdeckung von 95° ein. Sie konfigurieren die Radargeräte so, dass ein Alarm ausgelöst wird, wenn sich Personen außerhalb der Arbeitszeiten dem Gebäude nähern. Zur visuellen Bestätigung potenzieller Eindringlinge fügen sie zwei PTZ-Kameras hinzu. Die Radarsysteme können über *AXIS Radar Autotracking for PTZ* die PTZ-Kameras ansteuern.

Zusätzlich möchte das Unternehmen das Gelände während der Arbeitszeit schützen. Um sicherzustellen, dass sich die Fahrzeuge auf der Straße neben dem Gebäude an die Geschwindigkeitsbegrenzungen halten, wurde mithilfe von *AXIS Radar Integration for Microbus* AXIS D2110-VE Security Radars mit einem Geschwindigkeitszeichen von Microbus kombiniert.



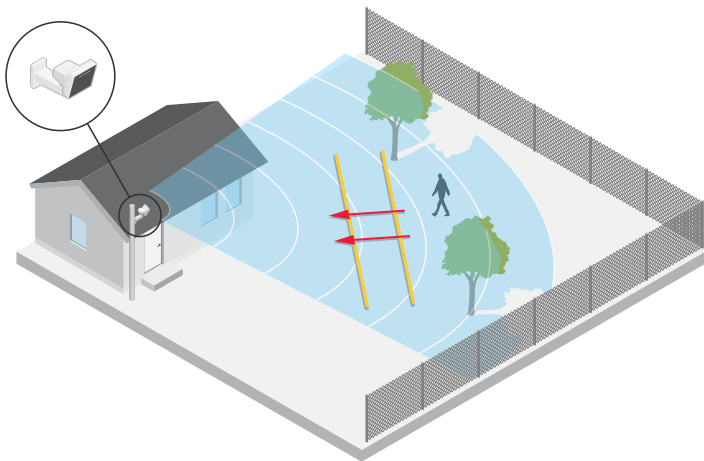
Komplexe Szenen abdecken

Ein Unternehmen mit kritischer Ausrüstung in einem Gebäude auf dem Grundstück hält Eindringlinge mit einem Zaun fern. Zur Vermeidung von Manipulation und Sabotage benötigen sie zusätzlichen Schutz. Es soll ein Alarm ausgelöst werden, sobald sich Personen dem Gebäude nähern. In der Szene befinden sich jedoch Bäume mit sich hin- und her bewegenden Ästen, ein Metallzaun, der Spiegelungen verursachen kann, sowie sich um den Standort herum bewegende kleine Tiere, was zu Fehlalarmen führen kann.

AXIS D2210-VE Radar

Radarprofile

Zur Vermeidung von Fehlalarmen konfigurieren sie über die Weboberfläche des Radars ein Szenario so, dass ein sich näherndes Objekt zwei virtuelle Linien überqueren muss, bevor ein Alarm ausgelöst wird. Auf diese Weise lösen nur die Objekte einen Alarm aus, die sich absichtlich in Richtung des Gebäudes bewegen, während Objekte herausgefiltert werden, die zufällig eine der virtuellen Linien überqueren.



An Standorten ohne Zäune können die beiden Linien als virtueller Zaun fungieren. Weitere Informationen zum Hinzufügen von zwei Linien zu einem Szenario über die Weboberfläche des Radars finden Sie unter *Szenarien hinzufügen auf Seite 17*.

Profil für Straßenüberwachung

Das Profil zur Straßenüberwachung ist für die Verfolgung von Fahrzeugen mit einer Geschwindigkeit von bis zu 200 km/h auf Straßen und Autobahnen optimiert. Verwenden Sie das Profil zur Bereichsüberwachung, um sich mit geringerer Geschwindigkeit bewegend Menschen und andere Objekte zu verfolgen. Weitere Informationen finden Sie unter *Profil für Bereichsüberwachung auf Seite 6*.

Erfassungsbereich der Straßenüberwachung

Das road monitoring profile (Straßenüberwachungsprofil) ist für die Erfassung von Fahrzeugen optimiert. Damit können die Geschwindigkeit von Fahrzeugen auf +/- 2 km/h genau gemessen und Fahrzeuge mit einer Geschwindigkeit von bis zu 200 km/h überwacht werden.

Die Montagehöhe des Radars und die Geschwindigkeit des Fahrzeugs wirken sich auf den Erfassungsbereich aus. Bei Montage in optimaler Installationshöhe erfasst das Radar die Geschwindigkeit heranfahrender und sich bewegend Fahrzeuge mit einer Genauigkeit von +/- 2 km/h in folgenden Bereichen:

- 25 bis 100 m bei Fahrzeugen mit einer Geschwindigkeit von 50 km/h.
- 40 bis 80 m bei Fahrzeugen mit einer Geschwindigkeit von 100 km/h.
- 50 bis 70 m bei Fahrzeugen mit einer Geschwindigkeit von 200 km/h.

Hinweis

Um das Risiko zu minimieren, dass Fahrzeuge mit hohen Geschwindigkeiten nicht erkannt werden, sollten Sie im Radar ein Szenario einrichten, das bei Erfassung der Objekttypen **Fahrzeug** und **Unbekannt** ausgelöst wird. Weitere Informationen zum Einrichten eines Szenarios finden Sie unter *Szenarien hinzufügen auf Seite 17*.

Beispiele für Straßeninstallationen

Achten Sie bei der Überwachung von Straßen und Autobahnen darauf, den Radar in ausreichender Höhe zu montieren, um tote Winkel (Radarschatten) hinter den Fahrzeugen zu vermeiden.

AXIS D2210-VE Radar

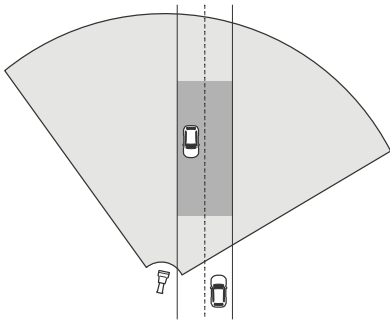
Radarprofile

Hinweis

Die Größe des Radarschattens hängt von der Montagehöhe des Radars sowie von der Höhe und Entfernung der Fahrzeuge vom Radar ab. Wenn beispielsweise ein 4,5 m hohes Fahrzeug 50 m von einem 8 m hoch montierten Radar entfernt ist, beträgt der Radarschatten hinter dem Fahrzeug 50 m. Ist der Radar jedoch in einer Höhe von 12 m montiert, beträgt der Schatten hinter demselben Fahrzeug nur 23 m.

Seitlich montiert

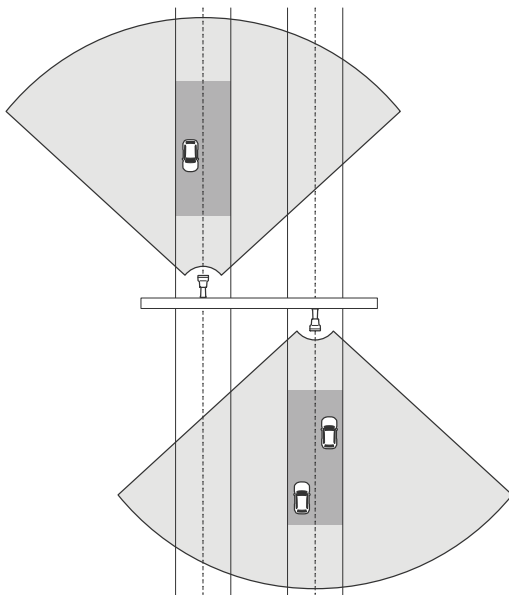
Zur Überwachung von Straßenfahrzeugen kann der Radar am Straßenrand montiert werden, zum Beispiel an einem Mast.



Positionieren Sie für eine genaue Messung von hohen Geschwindigkeiten den Radar in einem Querabstand von 10 m zu den Fahrzeugen. Weitere Informationen zum Erfassungsbereich und zur Genauigkeit von Geschwindigkeiten finden Sie unter *Erfassungsbereich der Straßenüberwachung auf Seite 9*.

Mittige Montage

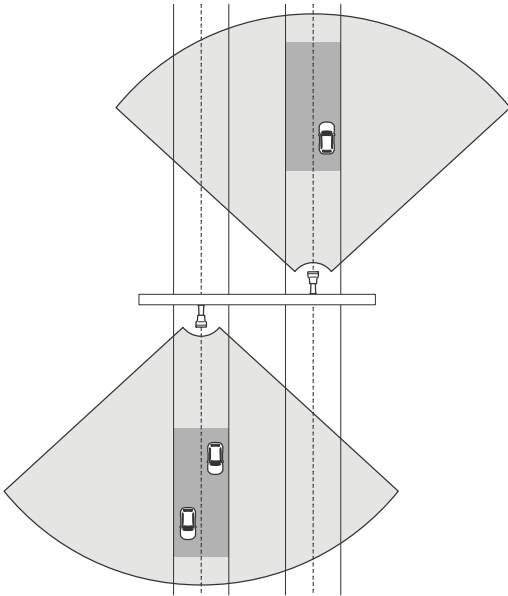
Zur Überwachung von Fahrzeugen auf mehrspurigen Straßen kann ein oder mehrere Radargeräte an einem Gerüst über die Fahrbahn montiert werden.



Dieselbe Installation eignet sich zur Überwachung von Fahrzeugen, die vom Radar wegfahren, anstatt darauf zuzufahren.

AXIS D2210-VE Radar

Radarprofile



Positionieren Sie für eine genaue Messung von hohen Geschwindigkeiten den Radar in einem Querabstand von 10 m zu den Fahrzeugen. Weitere Informationen zum Erfassungsbereich und zur Genauigkeit von Geschwindigkeiten finden Sie unter *Erfassungsbereich der Straßenüberwachung auf Seite 9*.

Einsatzgebiete für die Straßenüberwachung

Oftmals werden der AXIS D2210-VE Radar und das Profil zur Straßenüberwachung zur Verfolgung und Messung der Geschwindigkeit von Fahrzeugen eingesetzt. Zusätzlich können Sie den Radar mit einer visuellen Kamera und der Anwendung AXIS Speed Monitor dazu einsetzen, um die Geschwindigkeit der Fahrzeuge in der Live-Ansicht der Kamera zu visualisieren oder die Radarspuren zur statistischen Verarbeitung zu protokollieren. Weitere Informationen dazu finden Sie im *Benutzerhandbuch zu AXIS Speed Monitor*.

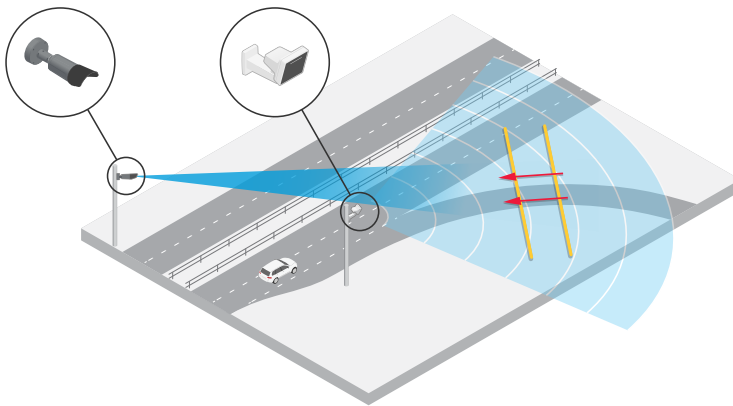
Weitere Beispiele zur Einrichtung des Radars unter Verwendung des Profils zur Straßenüberwachung finden Sie in den folgenden Einsatzfällen:

Erfassung der falschen Richtung auf einer Autobahnauffahrt

Zur Erkennung und Identifizierung von Fahrzeugen, die auf einer Autobahnauffahrt in die falsche Richtung fahren, werden bei Verkehrskontrollen eine AXIS D2210-VE und eine Axis Bullet-Kamera eingesetzt. Dazu wird das Radargerät an einem Mast vor der Auffahrt montiert, sodass Fahrzeuge erkannt, die in die falsche Richtung auffahren. Für zuverlässige Erfassungen richten sie ein Überquerungsszenario ein und konfigurieren das Radargerät so, dass die Fahrzeuge zwei Linien überqueren müssen, um einen Alarm auszulösen. In diesem Szenario werden die beiden Linien auf der Auffahrt wie in der Abbildung gezeigt gezogen. Außerdem werden die Fahrtrichtung und Geschwindigkeit angegeben, die einen Alarm auslösen. Löst der Radar einen Alarm aus, kann die Bullet-Kamera von Axis das Fahrzeug auf der Auffahrt visuell identifizieren.

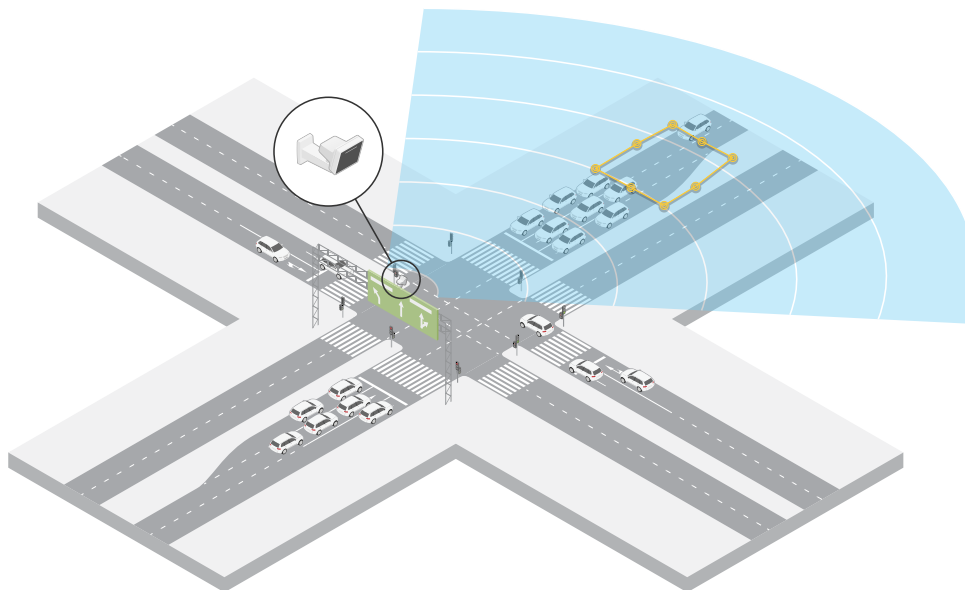
AXIS D2210-VE Radar

Radarprofile



Überwachung des Verkehrsflusses an einer Kreuzung – Bildung von Warteschlangen

Um zu überwachen, wie und wann sich an stark frequentierten Kreuzungen Warteschlangen bilden, installiert die Verkehrsüberwachung auf einem Gerüst oberhalb der Kreuzung ein Radargerät. Über die Weboberfläche des Radars wird ein Szenario erstellt und so konfiguriert, dass bei sich in einem Bereich bewegenden Fahrzeugen ein Alarm ausgelöst wird. Das Szenario wird so gestaltet, dass nur der Teil der Straße, der zur Kreuzung führt, abgedeckt. Damit bereits bei Bildung einer Warteschlange ein Alarm ausgelöst wird, wird das Szenario so konfiguriert, dass Fahrzeuge, die sich mit einer Geschwindigkeit von unter 5 km/h bewegen, als Auslöser dienen.



Überwachung des Verkehrsflusses an Kreuzungen – Richtung

Um sich einen Überblick über den Verkehrsfluss und die Richtung, in der sich die Fahrzeuge an stark frequentierten Kreuzungen bewegen, zu verschaffen, installiert die Verkehrsüberwachung ein Radargerät an einem Gerüst über der Straße, die zur Kreuzung führt. Über die Weboberfläche des Radars wird ein Überquerungsszenario erstellt, bei dem Fahrzeuge zwei Linien überqueren müssen, um einen Alarm auszulösen. Zur Konfiguration dieses Szenarios wird die erste der beiden Linien über die Spuren gezogen, die zur Kreuzung führen, *hinter* des Fußgängerüberwegs, um zu vermeiden, dass Fahrzeuge an der Linie anhalten. Die zweite Linie wird die Spuren gezogen, die nach rechts führen. Die Fahrzeuge müssen beide Linien in die angegebene Richtung überqueren, um einen Alarm auszulösen. Um zu verhindern, dass pro Kreuzung mehr als ein Fahrzeug einen Alarm auslöst, wird die Minstdauer für den Auslöser im Szenario von 2 auf 0 Sekunden reduziert.

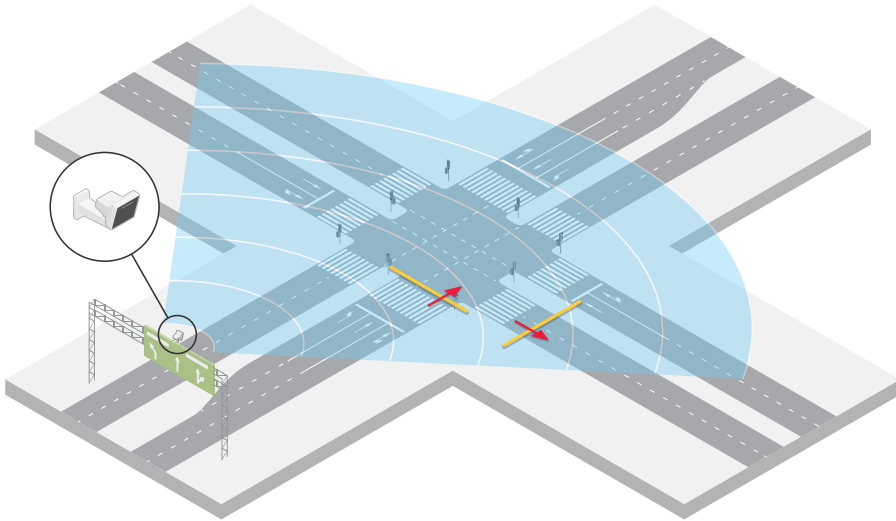
Für die Überwachung des Verkehrsflusses in alle Richtungen wird für jede Richtung ein Szenario erstellt.

AXIS D2210-VE Radar

Radarprofile

Hinweis

Das Szenario zählt nicht die Fahrzeuge, die die Linien überqueren. Zu diesem Zweck können Sie über die Weboberfläche des Radars das Ereignissystem verwenden. Eine Möglichkeit, Fahrzeuge zu zählen, besteht darin, sich – jedes Mal, wenn das Szenario einen Alarm auslöst – eine MQTT-Benachrichtigung senden zu lassen, und die erhaltenen MQTT-Benachrichtigungen zu zählen.



AXIS D2210-VE Radar

Erste Schritte

Erste Schritte

Das Gerät im Netzwerk ermitteln

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

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

Unterstützte Browser

Das Gerät kann mit den folgenden Browsern verwendet werden:

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

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

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.
Wenn Sie die IP-Adresse nicht gehen, ermitteln Sie das Gerät im Netzwerk mithilfe von AXIS IP Utility oder AXIS Device.
2. Geben Sie den Benutzernamen und das Kennwort ein. Wenn Sie zum ersten Mal auf das Gerät zugreifen, müssen Sie ein Administratorkonto erstellen. Siehe *Erstellen Sie ein Administratorkonto auf Seite 14*.

Erstellen Sie ein Administratorkonto

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

1. Einen Benutzernamen eingeben.
2. Ein Kennwort eingeben. Siehe *Sichere Kennwörter auf Seite 14*.
3. Geben Sie das Kennwort erneut ein.
4. Stimmen Sie der Lizenzvereinbarung zu.
5. Klicken Sie auf **Add account (Konto hinzufügen)**.

Wichtig

Das Gerät verfügt über kein Standardkonto. Wenn Sie das Kennwort für Ihr Administratorkonto verloren haben, müssen Sie das Gerät zurücksetzen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 72*.

AXIS D2210-VE Radar

Erste Schritte

Sichere Kennwörter

Wichtig

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

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

Doch zum Schutz Ihrer Daten empfehlen wir dringend:

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

Stellen Sie sicher, dass keiner die Firmware manipuliert hat.

So stellen Sie sicher, dass das Gerät über seine ursprüngliche Firmware von Axis verfügt, bzw. übernehmen nach einem Sicherheitsangriff die volle Kontrolle über das Gerät:

1. Zurücksetzen auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 72*.
Nach dem Zurücksetzen gewährleistet Secure Boot den Status des Geräts.
2. Konfigurieren und installieren Sie das Gerät.

Übersicht über die Weboberfläche

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



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

help.axis.com/?&piald=92321§ion=web-interface-overview

Weboberfläche des Axis Geräts

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

Ihr Gerät konfigurieren

Ein Radarprofil auswählen

In der Weboberfläche:

1. Gehen Sie zu **Radar > Settings > Detection (Radar > Einstellungen > Erfassung)**.
2. Wählen Sie ein Profil unter **Radar profiles (Radarprofile)**.

Radar kalibrieren

In der Standard-Live-Ansicht des Radars werden der vom Radar abgedeckte Bereich und erfasste Bewegungen angezeigt. Erfassungszonen und Regeln können sofort hinzugefügt werden. Um die Bewegungsrichtung von Objekten leichter zu erkennen, können Sie eine Referenzkarte hochladen. Dies kann zum Beispiel eine Planzeichnung oder ein Luftbild sein, das die vom Radar abgedeckte Fläche darstellt.

Bildanforderungen für die Referenzkarte:

- Die unterstützten Dateiformate sind .jpg und .png.
- Die Ausrichtung ist nicht wichtig, da die Form der Radarabdeckung während der Kalibrierung an das Bild angepasst wird.

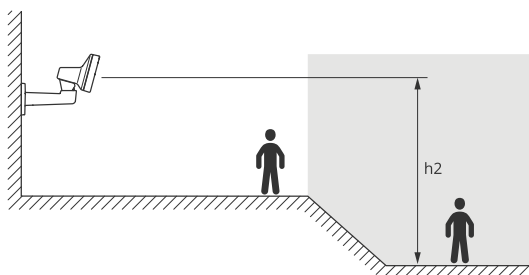
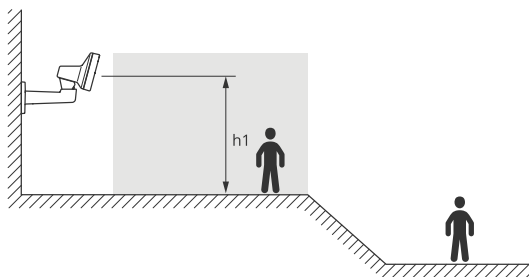
Stellen Sie vor dem Hochladen einer Referenzkarte und der Kalibrierung des Radars die korrekte Montagehöhe auf der Weboberfläche ein.

Montagehöhe festlegen

Messen Sie im ausgewählten Bereich die Montagehöhe vom Boden bis zum Radar.

Beispiel:

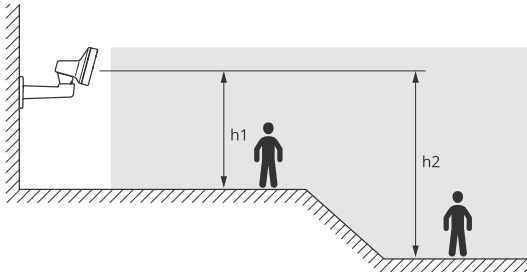
Die Montagehöhe (h_1 , h_2) unterscheidet sich je nach ausgewählten Bereich.



AXIS D2210-VE Radar

Ihr Gerät konfigurieren

Wenn die Oberfläche des ausgewählten Bereichs uneinheitlich ist, fügen Sie bei der Konfiguration des Radars die durchschnittliche Höhe hinzu (in diesem Fall $(h1 + h2) / 2$).



Montagehöhe festlegen:

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

Eine Referenzkarte hochladen

Laden Sie die Referenzkarte hoch und kalibrieren Sie sie, damit die vom Radar abgedeckte Fläche mit der Position, der Ausrichtung und dem Maßstab der Karte übereinstimmt.

1. Gehen Sie zu **Radar > Kartenkalibrierung**.
2. Laden Sie Ihre Referenzkarte hoch und befolgen Sie die Anweisungen des Einrichtungsassistenten.

Erfassungsbereiche festlegen

Um festzulegen, wo Bewegung erkannt werden soll, können Sie mehrere Bereiche hinzufügen. Verschiedene Bereiche können verwendet werden, um verschiedene Aktionen auszulösen.

Es gibt zwei Arten von Bereichen:

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

Szenarien hinzufügen

Ein Szenario (früher als **Einschlussbereich** bezeichnet) ist ein Bereich, in dem sich bewegende Objekte Regeln auslösen. Fügen Sie Szenarien hinzu, wenn Sie für unterschiedliche Teile der Szene verschiedene Regeln erstellen möchten.

Ein Szenario hinzufügen:

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

Auslösen bei Objekten, die sich in einem Bereich bewegen:

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

1. Wählen Sie **Movement in area (Bewegung im Bereich)** aus.
2. Klicken Sie auf **Next (Weiter)**.
3. Wählen Sie den in das Szenario einzubeziehenden Bereichstyp.
Verschieben und formen Sie den Bereich mit der Maus, sodass er den gewünschten Teil des Radarbilds oder der Referenzkarte abdeckt.
4. Klicken Sie auf **Next (Weiter)**.
5. Fügen Sie Erfassungseinstellungen hinzu.
 - 5.1 Fügen Sie Sekunden bis zum Auslösung unter **Ignore short-lived objects (Kurzlebige Objekte ignorieren)** hinzu.
 - 5.2 Wählen Sie unter **Trigger on object type (Auslöser für Objekttyp)** den auslösenden Objekttyp aus.
 - 5.3 Fügen Sie unter **Speed limit (Geschwindigkeitsbegrenzung)** einen Bereich für die Geschwindigkeitsbegrenzung hinzu.
6. Klicken Sie auf **Next (Weiter)**.
7. Legen Sie die Minstdauer des Alarms unter **Minimum trigger duration (Minimale Triggerdauer)** fest.
8. Klicken Sie auf **Save (Speichern)**.

Auslösen für Objekte, die eine Linie überqueren:

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

Auslösen für Objekte, die zwei Linien überqueren:

1. Wählen Sie **Line crossing (Linienüberschreitung)**.
2. Klicken Sie auf **Next (Weiter)**.
3. Wenn das Objekt zwei Linien überqueren soll, damit der Alarm ausgelöst wird aktivieren Sie **Require crossing of two lines (Überschreiten von zwei Linien erforderlich)**.

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

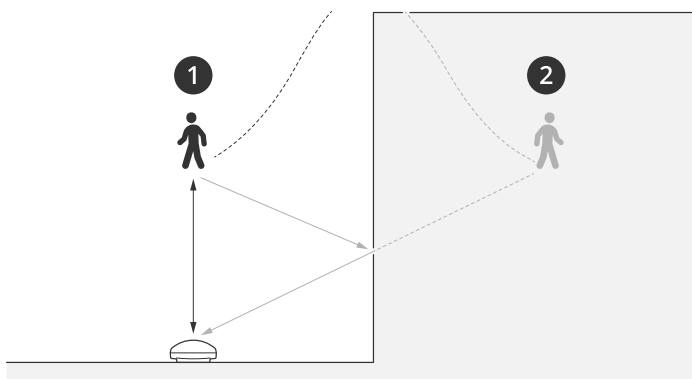
4. Linien in der Szene positionieren.
Verwenden Sie die Maus, um die Linie zu verschieben und zu verformen.
5. Um die Erfassungsrichtung zu ändern, aktivieren Sie die Option **Change direction (Richtung ändern)**.
6. Klicken Sie auf **Next (Weiter)**.
7. Fügen Sie Erfassungseinstellungen hinzu.
 - 7.1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

Ausschlussbereiche hinzufügen

Ausschlussbereiche sind Bereiche, in denen sich bewegende Objekte ignoriert werden. Fügen Sie Ausschlussbereiche hinzu, um Bereiche mit sich bewegenden Objekten zu ignorieren, die Fehlalarme auslösen können.

Beispiel:

Objekte aus radarreflektierenden Materialien wie Metalldächer, Zäune, Fahrzeuge und sogar Ziegelwände können die Leistung des Radars beeinträchtigen. Sie können Reflexionen oder Phantomverfolgungen erzeugen, die scheinbare Erfassungen verursachen, die sich nur schwer von tatsächlichen Erfassungen unterscheiden lassen.



- 1 *Tatsächliche Bilderfassung*
- 2 *Reflektierte Bilderfassung*

Einen Ausschlussbereich hinzufügen:

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

Ihr Gerät konfigurieren

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

Hinweis

Ab Firmware-Version 11.4 gibt es keine Einschränkungen mehr bei der Anzahl der Ausschlussbereiche.

Fehlalarme minimieren

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

- Erfassungsempfindlichkeit des Radarmelders einstellen:

Gehen Sie zu **Radar > Einstellungen > Erfassung** und wählen Sie unter **Erfassungsempfindlichkeit** eine niedrigere Empfindlichkeitsstufe aus. Dies verringert die Gefahr von Fehlalarmen, kann aber dazu führen, dass einige Bewegungen nicht vom Radar erfasst werden.

Die Empfindlichkeitseinstellung wirkt sich auf alle Bereiche aus.

- **Low (Niedrig):** Verwenden Sie diese Empfindlichkeit, wenn sich viele Metallgegenstände oder große Fahrzeuge in der Umgebung befinden. Die Objektverfolgung und -klassifizierung durch den Radar dauert dann länger. Dadurch kann sich der Erfassungsbereich verkleinern, insbesondere bei sich schnell bewegenden Objekten.
- **Medium (Mittel):** Dies ist die Standardeinstellung.
- **High (Hoch):** Stellen Sie diese Empfindlichkeit ein, wenn sich vor dem Radarmelder ein freies Feld ohne Metallobjekte befindet. Dadurch vergrößert sich der Erfassungsbereich für Personen.

- Szenarien ändern und Zonen ausschließen:

Wenn ein Szenario harte Oberflächen enthält, z. B. eine Wand aus Metall, können Reflektionen zur mehrfachen Erfassung eines einzelnen physikalischen Objekts führen. Sie können entweder die Form des Szenarios ändern oder eine Ausschlusszone hinzufügen, die bestimmte Teile des Szenarios ignoriert. Weitere Informationen finden Sie unter *Szenarien hinzufügen auf Seite 17* und *Ausschlussbereiche hinzufügen auf Seite 19*.


- Auslösen bei Objekten, die zwei Linien überschreiten anstelle einer:

Wenn in einem Szenario mit Linienüberschreitung schaukelnde Objekte oder sich umher bewegende Tiere eingeschlossen sind, besteht die Gefahr, dass ein Objekt die Linie überquert und einen falschen Alarm auslöst. In diesem Fall können Sie das Szenario so konfigurieren, dass es nur ausgelöst wird, wenn ein Objekt zwei Linien überschritten hat. Weitere Informationen finden Sie unter *Szenarien hinzufügen auf Seite 17*.

- Nach Bewegung filtern:


- Gehen Sie zu **Radar > Einstellungen > Erfassung** und wählen Sie **Schaukelnde Objekte ignorieren**. Diese Einstellung minimiert die Anzahl der durch Bäume, Büsche und Fahnenmasten ausgelösten Fehlalarme.
- Gehen Sie zu **Radar > Einstellungen > Erfassung** und wählen Sie **Kleine Objekte ignorieren**. Diese Einstellung ist im Profil für die Bereichsüberwachung verfügbar und minimiert die Fehlalarme durch kleine Objekte in der Erfassungszone, z. B. durch Katzen oder Hasen.

- Nach Zeit filtern:

- Gehen Sie zu **Radar > Szenarien**.
- Wählen Sie ein Szenario und klicken Sie auf , um die Einstellungen zu ändern.
- Stellen Sie unter **Seconds until trigger (Sekunden bis Auslösung)** einen höheren Wert ein. Dies ist die Verzögerungszeit zwischen dem Beginn der radargestützten Objektverfolgung und Auslösung eines Alarms. Der Timer startet, wenn das Radar zuerst ein Objekt erkennt, und nicht, wenn das Objekt den spezifischen Einschussbereich im Szenario betritt.

AXIS D2210-VE Radar

Ihr Gerät konfigurieren


- Nach Objekttyp filtern:
 - Gehen Sie zu **Radar > Szenarien**.
 - Wählen Sie ein Szenario und klicken Sie auf  , um die Einstellungen zu ändern.
 - Wenn bei bestimmten Objekttypen kein Ereignis ausgelöst werden soll, entfernen Sie diejenigen Objekttypen aus der Auswahl, die in diesem Szenario keine Ereignisse auslösen sollen.

Das Radarbild anpassen

In diesem Abschnitt finden Sie Anweisungen zur Konfiguration Ihres Geräts. Weitere Informationen zur Arbeitsweise bestimmter Funktionen finden Sie unter *Mehr erfahren auf Seite 64*.


Anzeige eines Bild-Overlays

Sie können ein Bild als Overlay im Radarstream hinzufügen.

1. Gehen Sie zu **Radar > Overlays**.
2. Wählen Sie **Image (Bild)** und klicken Sie auf  .
3. Klicken Sie auf **Images (Bilder)**.
4. Legen Sie ein Bild per Drag & Drop ab.
5. Klicken Sie auf **Hochladen**.
6. Klicken Sie auf **Overlay verwalten**.
7. 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.

Einen Text-Overlay anzeigen

Sie können ein Textfeld als Overlay im Radarstream hinzufügen. Dies ist nützlich, wenn Sie das Datum, die Uhrzeit oder den Firmennamen im Videostream anzeigen möchten.

1. Gehen Sie zu **Radar > Overlays**.
2. Wählen Sie **Text** aus und klicken Sie auf  .
3. Geben Sie den Text ein, der im Videostream angezeigt werden soll.
4. Position auswählen. Sie können das Overlay-Textfeld auch per Drag & Drop in der Live-Ansicht ziehen, um die Position zu ändern.

Text-Overlay mit Angabe des Neigungswinkels des Radars anzeigen

In die Live-Ansicht des Radars kann ein Overlay mit Angabe des Neigungswinkels des Radars hinzugefügt werden. Dies ist hilfreich bei der Installation oder wenn Sie wissen müssen, in welchem Winkel das Gerät geneigt ist.


Hinweis

Im Neigungswinkel-Overlay wird der Wert standardmäßig um 90° erhöht. Den Neigungswinkel des Radars erhalten Sie, indem Sie den in der Weboberfläche angezeigten Wert von 90° abziehen. Wird beispielsweise im Overlay der Wert 75 angezeigt, beträgt der Neigungswinkel des Radars 15° unterhalb der Horizontlinie.

1. Gehen Sie zu **Radar > Overlays**.

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

2. Wählen Sie Text aus und klicken Sie auf  .
3. Geben Sie #op ein.
Sie können auch auf **Modifier (Modifikator)** klicken und #op aus der Liste wählen.
4. Position auswählen. Sie können das Overlay-Feld 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* auf Seite 64.

Bandbreite und Speicher reduzieren

Wichtig

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


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

Hinweis

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

Einrichtung eines Netzwerk-Speichers

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


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



Video aufzeichnen und ansehen


Video direkt vom Radar aufzeichnen

1. Gehen Sie zu **Radar > Videostream**.


Ihr Gerät konfigurieren

- 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 *Einrichtung eines Netzwerk-Speichers auf Seite 22*

- Um die Aufzeichnung anzuhalten, klicken Sie erneut auf  .

Video ansehen

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

Einrichten von Regeln für Ereignisse

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

Lösen Sie eine Aktion aus

- 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.
- Unter **Name** einen Dateinamen eingeben.
- Wählen Sie die **Condition (Bedingung)** aus, die erfüllt sein muss, um die Aktion auszulösen. Wenn für die Regel mehrere Bedingungen definiert werden, müssen zum Auslösen der Aktion alle Bedingungen erfüllt sein.
- Wählen Sie, welche **Aktion** das Gerät bei erfüllten Bedingungen durchführen soll.

Hinweis

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

Hinweis

Werden Definitionen von in Regeln verwendeten Videostream-Profilen geändert, dann müssen alle Regeln, die diese Videostream-Profile verwenden, neu gestartet werden.

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

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

Die Geräte verbinden:

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

Den E/A-Port der Radarmelders konfigurieren:

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

Eine Regel im Radarmelder erstellen:

- Gehen Sie zu **System > Ereignisse** und fügen Sie eine Regel hinzu.
- Geben Sie einen Namen für die Regel ein.
- Wählen Sie aus der Liste der Bedingungen unter **Radarbewegungen** ein Szenario.

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

Informationen zum Einrichten eines Szenarios finden Sie unter *Szenarien hinzufügen auf Seite 17*.

6. Wählen Sie in der Liste der Aktionen die Option **Toggle I/O while the rule is active (E/A umschalten, während die Regel aktiv ist)** aus und wählen Sie dann den Port aus, der mit der Kamera verbunden ist.
7. Klicken Sie auf **Save (Speichern)**.

Den E/A-Port der Kamera konfigurieren:

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

Eine Regel in der Kamera erstellen:

9. Gehen Sie zu **System > Ereignisse** und fügen Sie eine Regel hinzu.
10. Geben Sie einen Namen für die Regel ein.
11. Wählen Sie aus der Liste der Bedingungen die Option **Digitaler Eingang ist aktiv** und wählen Sie dann den Port, der die Regel auslösen soll.
12. Wählen Sie **Record video (Video aufzeichnen)** aus der Liste der Aktionen aus.
13. Wählen Sie in der Liste der Speicheroptionen **SD-Karte**.
14. Wählen Sie ein vorhandenes Videostreamprofil oder legen Sie ein neues an.
15. Stellen Sie den Vorpuffer auf 5 Sekunden ein.
16. Stellen Sie den Nachpuffer auf 1 Minute ein.
17. Klicken Sie auf **Save (Speichern)**.

Videoaufzeichnung von einer Kamera, wenn ein Fahrzeug in die falsche Richtung fährt

In diesem Beispiel wird erläutert, wie der Radar und die Kamera so eingerichtet werden, dass die Kamera die Aufzeichnung auf eine SD-Karte startet, sobald der Radar ein Fahrzeug erkennt, das in die falsche Richtung fährt.

Bevor Sie beginnen

- Erstellen Sie über die Weboberfläche des Radars ein Szenario, bei dem das Überschreiten einer Linie und das Überqueren zweier Linien durch Fahrzeuge als Auslöser dient.

Weitere Informationen finden Sie unter *Szenarien hinzufügen auf Seite 17*.

- Achten Sie darauf, dass Sie die beiden Linien auf der Fahrspur ziehen, auf der Sie Fahrzeuge erkennen wollen, die in die falsche Richtung fahren. Arbeiten Sie mit einer Referenzkarte, z. B. ein Foto des Bereichs, um die Erfassung von sich bewegenden Objekten zu erleichtern.

Weitere Informationen finden Sie unter *Eine Referenzkarte hochladen auf Seite 17*.

1. Erstellen Sie im Radar zwei Empfänger.
 - 1.1 Gehen Sie auf der Benutzeroberfläche des Radars zu **System > Ereignisse > Empfänger** und fügen Sie den ersten Empfänger hinzu.
 - 1.2 Fügen Sie folgende Informationen hinzu:
 - **Name:** Virtuellen Port aktivieren
 - **Typ:** HTTP
 - **URL:** `http://<IPaddress>/axis-cgi/virtualinput/activate.cgi`Ersetzen Sie `<IPaddress>` durch die Adresse der Kamera, die Sie mit der Aufzeichnung starten sollen.

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

- Geben Sie den Benutzernamen und das Kennwort der Kamera ein.
- 1.5 Klicken Sie auf **Testen**, um sicherzustellen, dass alle Daten gültig sind.
- 1.6 Klicken Sie auf **Speichern**.
- 1.7 Fügen Sie einen zweiten Empfänger mit den folgenden Informationen hinzu:
 - **Name:** Virtuellen Port deaktivieren
 - **Typ:** HTTP
 - **URL:** http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
Ersetzen Sie <IPaddress> durch die IP-Adresse der Kamera.
 - Geben Sie den Benutzernamen und das Kennwort der Kamera ein.
 - 1.5 Klicken Sie auf **Testen**, um sicherzustellen, dass alle Daten gültig sind.
 - 1.6 Klicken Sie auf **Speichern**.
- 2. Erstellen Sie im Radar zwei Regeln.
 - 2.1 Gehen Sie auf der Benutzeroberfläche des Radars zu **System > Ereignisse > Regeln** und fügen Sie die erste Regel hinzu.
 - 2.2 Fügen Sie folgende Informationen hinzu:
 - **Name:** Virtuellen E/A1 aktivieren
 - **Bedingung:** Wählen Sie das unter **Radarbewegung** erstellte Szenario.
 - **Aktion:** **Benachrichtigungen > Benachrichtigung über HTTP senden**
 - **Empfänger:** **Virtuellen Port aktivieren**
 - **Query-String-Suffix:** schemaversion=1&port=1
 - 2.6 Klicken Sie auf **Save (Speichern)**.
 - 2.7 Fügen Sie eine weitere Regel mit folgenden Informationen hinzu:
 - **Name:** Virtuellen E/A1 deaktivieren
 - **Bedingung:** Wählen Sie das unter **Radarbewegung** erstellte Szenario.
 - Wählen Sie **Bedingungen umkehren**.
 - **Aktion:** **Benachrichtigungen > Benachrichtigung über HTTP senden**
 - **Recipient (Empfänger):** **Virtuellen Port deaktivieren**
 - **Query-String-Suffix:** schemaversion=1&port=1
 - 2.7 Klicken Sie auf **Speichern**.
- 3. Erstellen Sie eine Regel in der Kamera.
 - 3.1 Gehen Sie auf der Benutzeroberfläche der Kamera zu **System > Ereignisse > Regeln** und fügen Sie eine Regel hinzu.
 - 3.2 Fügen Sie folgende Informationen hinzu:
 - **Name:** Auslöser am virtuellen Eingang 1

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

- Bedingung: E/A > Virtueller Eingang ist aktiv.
 - Port: 1
 - Aktion: Aufzeichnungen > Bei aktiver Regel Video aufzeichnen
 - Speicheroptionen: SD_DISK
 - Wählen Sie eine Kamera und ein Videostreamprofil.
- 3.7 Klicken Sie auf **Speichern**.

Abwechselnd aufblinkendes rotes Licht am Radar

Mithilfe der dynamischen LED-Leiste an der Vorderseite des Radars können Sie darauf hinweisen, dass der Bereich überwacht wird.

In diesem Beispiel wird erläutert, wie Sie ein rot aufblinkendes Licht aktivieren und einen Zeitplan so einrichten, dass es nur nach den Arbeitszeiten an Wochentagen aufblinkt.

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.
3. Wählen Sie unter **Typ** die Option **Zeitplan**.
4. Wählen Sie unter **Wiederholen** die Option **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. Klicken Sie auf **Speichern**.

Eine Regel erstellen:

1. Gehen Sie zu **System > Ereignisse** und fügen Sie eine Regel hinzu.
2. Geben Sie einen Namen für die Regel ein.
3. Wählen Sie in der Bedingungsliste unter **Geplant und wiederkehrend** die Option **Zeitplan**.
4. Wählen Sie in der Liste der Aktionen unter **Radar** die Option **Dynamische LED-Leiste**.
5. Wählen Sie ein Muster aus.
6. Stellen Sie die Dauer auf 12 Stunden ein.
7. Klicken Sie auf **Speichern**.

Lichtquelle einschalten, wenn eine Bewegung erkannt wird

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

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

Die Geräte verbinden:

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

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

Den Relay-Port des Radarmelders konfigurieren:

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

Eine Regel im Radarmelder erstellen:

3. Gehen Sie zu **System > Ereignisse** und fügen Sie eine Regel hinzu.
4. Geben Sie einen Namen für die Regel ein.
5. Wählen Sie aus der Liste der Bedingungen unter **Radarbewegungen** ein Szenario.

Informationen zum Einrichten eines Szenarios finden Sie unter *Szenarien hinzufügen auf Seite 17*.

6. Wählen Sie in der Liste der Aktionen die Option **Toggle I/O once (E/A einmal umschalten)** aus und wählen Sie dann den Relaisport aus.
7. Wählen Sie **Active (Aktiv)** aus.
8. Legen Sie die **Duration (Dauer)** fest.
9. Klicken Sie auf **Save (Speichern)**.

Eine PTZ-Kamera mittels Radarmelder steuern

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

- *Steuern Sie eine PTZ-Kamera mit dem integrierten Radar-Objektverfolgungsdienst auf Seite 27*. Verwenden Sie diese eingebaute Option, wenn Sie eine PTZ-Kamera und einen Radar dicht nebeneinander montiert haben.
- *Steuern einer PTZ-Kamera mit AXIS Radar Autotracking for PTZ auf Seite 28*. Die Windows-Anwendung eignet sich, wenn Sie mehrere PTZ-Kameras und Radare zur Verfolgung von Objekten verwenden möchten.

Hinweis

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

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

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

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

Hinweis

Sie können den integrierten Radar-Objektverfolgungsdienst nutzen, um ein Radar mit einer PTZ-Kamera zu verbinden. Für ein Setup, bei dem Sie mehr als eine Radar- oder PTZ-Kamera verwenden möchten, verwenden Sie *AXIS Radar Autotracking for PTZ*. Weitere Informationen finden Sie unter *Steuern einer PTZ-Kamera mit AXIS Radar Autotracking for PTZ auf Seite 28*.

Koppeln Sie das Radar mit der PTZ-Kamera:

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

Kalibrieren Sie das Radar und die PTZ-Kamera:

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

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

Richten Sie die PTZ-Verfolgung ein:

9. Gehen Sie zu Track (Verfolgen), wenn Menschen, Fahrzeuge und/oder unbekannte Objekte verfolgt werden sollen.
10. Um Objekte mit der PTZ-Kamera zu verfolgen, Tracking (Automatisches Nachführen) aktivieren.
Beim automatischen Nachführen zoomt die Kamera automatisch auf ein Objekt oder eine Gruppe von Objekten, um sie im Sichtfeld zu behalten.
11. Aktivieren Sie Object switching (Objektwechsel), wenn Sie mehrere Objekte erwarten, die nicht in die Kameraansicht passen.
Bei dieser Einstellung gibt das Radar den zu verfolgenden Objekten Priorität.
12. Um zu bestimmen, wie viele Sekunden jedes Objekt verfolgt werden soll, legen Sie Object hold time (Objekthaltezeit) fest.
13. Das Wahlfeld Zurück zur Ausgangsposition aktivieren, um die PTZ-Kamera zur Ausgangsposition zurückkehren zu lassen, wenn das Radar keine Objekte mehr verfolgt.
14. Die Funktion Timeout Zurück zur Startposition legt fest, wie lange die PTZ-Kamera auf die letzte bekannten Position der verfolgten Objekte ausgerichtet bleibt, bevor sie zur Startposition zurückkehrt.
15. Um den Zoom der PTZ-Kamera fein abzustimmen, passen Sie den Zoom am Schieberegler an.

Steuern einer PTZ-Kamera mit AXIS Radar Autotracking for PTZ

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

- Steuerung mehrerer PTZ-Kameras über einen Radarmelder.
- Steuerung einer PTZ-Kamera über mehrere Radarmelder.
- Steuerung mehrerer PTZ-Kameras über mehrere Radarmelder.
- Steuerung einer PTZ-Kamera über einen Radarmelder bei unterschiedlichen Installationsorten, die ein und denselben Bereich abdecken.

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.

Senden von Radardaten mithilfe von MQTT

Verwenden Sie den Radar mit der Anwendung AXIS Speed Monitor, um Radardaten für erfasste Objekte zu erfassen und über MQTT zu versenden.

In diesem Beispiel wird erläutert, wie sich auf dem Gerät mit AXIS Speed Monitor ein MQTT-Client einrichten lässt und eine Bedingung erstellt wird, unter der die in AXIS Speed Monitor erfassten Radardaten als Payload zu einem MQTT-Broker veröffentlicht werden.

Bevor Sie beginnen:

AXIS D2210-VE Radar

Ihr Gerät konfigurieren

- Installieren Sie AXIS Speed Monitor auf Ihrem Radar oder auf einer Kamera, die Sie an Ihr Radar anschließen.
Weitere Informationen dazu finden Sie im *Benutzerhandbuch zu AXIS Speed Monitor*.
- Richten Sie einen MQTT-Broker ein und rufen Sie die IP-Adresse, den Benutzernamen und das Kennwort des Brokers ab.
Mehr zu MQTT und MQTT-Broker erfahren Sie im *AXIS OS Portal*.

Richten Sie den MQTT-Client auf der Weboberfläche des Geräts mit AXIS Speed Monitor ein:

1. Gehen Sie zu **System > MQTT > MQTT-Client > Broker** und geben Sie folgende Informationen ein:
 - **Host:** Die IP-Adresse des Brokers
 - **Client-ID:** Die ID des Geräts.
 - **Protokoll:** Das Protokoll, auf das der Broker festgelegt ist
 - **Port:** Die vom Broker verwendete Portnummer
 - **Benutzername und Kennwort** des Brokers
2. Klicken Sie auf **Speichern** und dann auf **Verbinden**.

Erstellen Sie eine Bedingung, unter der die Radardaten als Payload zum MQTT-Broker veröffentlicht werden:

3. Gehen Sie zu **System > MQTT > MQTT-Veröffentlichung** und klicken Sie auf **Bedingung hinzufügen**.
4. Wählen Sie unter **Anwendung** die Option **Speed Monitor** aus der Bedingungsliste aus. **Aus der Zone Verlassene verfolgen**.

Das Gerät kann nun für jedes sich bewegende Objekt, das ein Szenario verlässt, Informationen dazu liefern, die sich aus der Radarverfolgung ergeben haben. Für jedes Objekt sind eigene Parameter wie zum Beispiel `rmd_zone_name`, `tracking_id` und `trigger_count` vorhanden. Die vollständige Parameterliste finden Sie im *Benutzerhandbuch zu AXIS Speed Monitor*.

AXIS D2210-VE Radar


Die Weboberfläche












Die 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.
-  Die Sprache ändern.
-  Helles oder dunkles Design einstellen.
-    Das Benutzermenü enthält:
 - Informationen zum angemeldeten Benutzer.
 -  **Change account (Konto wechseln)**: Melden Sie sich vom aktuellen Konto ab und melden Sie sich bei einem neuen Konto an.
 -  **Log out (Abmelden)**: Melden Sie sich vom aktuellen Konto ab.
-  Das Kontextmenü enthält:
 - **Analytics data (Analysedaten)**: Stimmen Sie der Teilung nicht personenbezogener Browserdaten zu.
 - **Feedback**: Teilen Sie Feedback, um Ihr Benutzererlebnis zu verbessern.
 - **Rechtliches**: Lassen Sie sich Informationen zu Cookies und Lizenzen anzeigen.
 - **Info**: Lassen Sie sich Geräteinformationen anzeigen, einschließlich Firmwareversion und Seriennummer.
 - **Legacy device interface (Frühere Benutzeroberfläche)**: Wechseln Sie zur früheren Weboberfläche des Geräts.

Status

Geräteinformationen

Zeigt die Geräteinformationen an, einschließlich Firmwareversion und Seriennummer.

Upgrade firmware (Firmwareaktualisierung): Aktualisieren Sie die Firmware auf Ihrem Gerät. Klicken Sie darauf, um zur Wartungsseite zu gehen, auf der Sie eine Firmwareaktualisierung 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.

AXIS D2210-VE Radar

Die Weboberfläche

NTP settings (NTP-Einstellungen): Anzeigen und Aktualisieren der NTP-Einstellungen. Klicken Sie darauf, um zur Seite **Date and time (Datum und Uhrzeit)** zu wechseln, auf der Sie die NTP-Einstellungen ändern können.

Sicherheit

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

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

Connected clients (Verbundene Clients)

Zeigt die Anzahl der Verbindungen und der verbundenen Clients an.

View details (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.

Ongoing recordings (Laufende Aufzeichnungen)

Zeigt laufende Aufzeichnungen und den dafür vorgesehenen Speicherplatz an.

Aufzeichnungen: Aktuelle und gefilterte Aufzeichnungen und deren Quelle anzeigen. Weitere Informationen finden Sie unter *Aufzeichnungen auf Seite 38*




Anzeige des Speicherorts der Aufzeichnung.

Radars

Einstellungen

Allgemein

Radars transmission (Radarsübertragung): Verwenden Sie diese Option, um das Radarmodul vollständig auszuschalten.

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.

Erfassung

AXIS D2210-VE Radar

Die Weboberfläche

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

Radar profile (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 swaying objects (Schaukelnde Objekte ignorieren):** Aktivieren Sie diese Option, um die Fehlalarme aufgrund von schaukelnden Objekten wie Bäumen, Büschen oder Fahnenmasten zu minimieren.
 - **Ignore small objects (Kleine Objekte ignorieren):** Aktivieren Sie diese Option, um die Fehlalarme durch kleine Objekte wie Katzen oder Hasen zu minimieren.
- **Road monitoring (Straßenüberwachung):** Verfolgung von Fahrzeugen mit einer höheren Geschwindigkeit in Stadtgebieten und auf Vorortstraßen
 - **Ignore swaying objects (Schaukelnde Objekte ignorieren):** Aktivieren Sie diese Option, um die Fehlalarme aufgrund von schaukelnden Objekten wie Bäumen, Büschen oder Fahnenmasten zu minimieren.


Ansicht

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.

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.

Symbolart: 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

Allgemein


AXIS D2210-VE Radar

Die Weboberfläche

Auflösung: Wählen Sie eine für die zu überwachende Szene geeignete Bildauflösung. 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.


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.

Zipstream

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.

Bitrate control (Bitratensteuerung)

- **Average (Durchschnitt):** Wählen Sie diese Option, um die Bitrate automatisch über einen längeren Zeitraum anzupassen und je nach verfügbarem 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.
 - **Bitratengrenze:** 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. Dadurch lässt sich leichter erkennen, wo sich Objekte im vom Radar abgedeckten Bereich bewegen.

Karte hochladen: Wählen Sie die Referenzkarte aus, die Sie hochladen möchten.

Radarposition auf Karte festlegen: Geben Sie auf der Karte die Position des Radars an, fügen Sie direkt vor dem Radar einen Bezugspunkt hinzu und geben Sie den Abstand zwischen Radar und Bezugspunkt ein. Klicken Sie auf Kalibrieren, um die Kalibrierung zu starten.

Das Ergebnis der Kalibrierung ist eine Referenzkarte mit der Radarabdeckung im passenden Maßstab.

Ausschlussbereiche

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



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

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

Wählen Sie unter **Zone shape presets (Zonenkontur vorgeben)** eine Kontur für den Ausschlussbereich aus. Mit **Cover everything (Alles abdecken)** legen Sie die Zone auf den gesamten Radarerfassungsbereich fest. Mit **Reset to box (Auf Rechteck zurücksetzen)** wird in der Mitte des Erfassungsbereichs ein Rechteck erzeugt.

Um die 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 Alarme auslöst.

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

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

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

AXIS D2210-VE Radar

Die Weboberfläche




- **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 (Grenzggeschwindigkeit):** 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 (Alarminstellungen):** 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.
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 - **Darstellung:** Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
 -  : Wählen Sie die Position des Overlays im Bild.
- **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 **Bilder**. 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: FFFFFFF für Weiß, 000000 für Schwarz, FF0000 für Rot, 6633FF für Blau und 669900 für Grün. Nur bei .bmp-Bildern.
- **Scene annotation (Szenenkennzeichnung)**  : 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.
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 - **Darstellung:** Wählen Sie die Textfarbe und den Hintergrund, zum Beispiel weißer Text auf schwarzem Hintergrund (Standardeinstellung).
 -  : Wählen Sie die Position des Overlays im Bild. 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-Indikator)**  : 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.
 - **Darstellung:** Wählen Sie die Farbe der Animation und des Hintergrunds, zum Beispiel rote Animation auf durchsichtigem Hintergrund (Standardeinstellung).
 - **Größe:** Wählen Sie die gewünschte Schriftgröße.
 -  : Wählen Sie die Position des Overlays im Bild.
- **Widget: 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 Overlays im Bild.
 - **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.
 - **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**
 - **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**
 - **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: Messen**  : 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 Overlays im Bild.
 - **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.
 - **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**
 - **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.

AXIS D2210-VE Radar

Die Weboberfläche

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.

Anhalten: 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 auf Seite 26*.

Automatische PTZ-Objektverfolgung per Radar

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

Anfangseinstellungen konfigurieren:

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

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

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

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

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

PTZ-Objektverfolgung konfigurieren:

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

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

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

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

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


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

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

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

Aufzeichnungen


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



- Starten einer Aufzeichnung des Geräts.
-  Wählen Sie das Speichermedium, auf dem die Aufzeichnung gespeichert werden soll.
- Beenden einer Aufzeichnung des Geräts.

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

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


 Die Aufzeichnung wiedergeben.

 Abspielen der Aufzeichnung anhalten.


  Informationen und Aufzeichnungsoptionen anzeigen oder verbergen.

Set export range (Exportbereich festlegen): Geben Sie den Zeitraum ein, wenn Sie nur einen Teil der Aufzeichnung exportieren möchten.

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


Klicken Sie auf , um eine Aufzeichnung zu löschen.

Export (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.

Event (Ereignis): Zeigt Aufzeichnungen auf Grundlage von Ereignissen.

Storage (Speicher): Zeigt Aufzeichnungen nach Speichertyp.

AXIS D2210-VE Radar

Die Weboberfläche

Apps



Add app (App hinzufügen): Installieren einer neuen App.

Find more apps (Weitere Apps finden): Finden weiterer zu installierender Apps. Sie werden zu einer Übersichtsseite der Axis Apps weitergeleitet.



Allow unsigned apps (Unsignierte Apps erlauben) : Schalten Sie diese Option ein, um die Installation unsignierter Apps zu ermöglichen.



Allow root-privileged apps (Apps mit Root-Berechtigungen zulassen) : Schalten Sie diese Option ein, um Apps mit Root-Berechtigungen uneingeschränkter Zugriff auf das Gerät zu ermöglichen.



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

Hinweis

Bei gleichzeitiger Ausführung mehrerer Apps kann die Leistung des Geräts beeinträchtigt werden.

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

Open (Öffnen): Auf die Anwendungseinstellungen zugreifen. Die verfügbaren Einstellungen sind anwendungsabhängig. Für einige Anwendungen stehen keine Einstellmöglichkeiten zur Verfügung.



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 müssen.
- **Lizenz mit Schlüssel aktivieren:** Wenn für die App eine Lizenz erforderlich ist, muss sie aktiviert werden. Verwenden Sie diese Option, wenn Ihr Gerät keinen Internetzugang besitzt. Falls Sie keinen Lizenzschlüssel besitzen, gehen Sie zu axis.com/products/analytics. Um einen Lizenzschlüssel zu erzeugen, benötigen Sie einen Lizenzcode und die Seriennummer Ihres Axis Produkts.
- **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.
- **Deactivate the license (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.
- **Delete (Löschen):** Darüber löschen Sie die App dauerhaft vom Gerät. Die Lizenz muss zuerst deaktiviert werden, da sie andernfalls weiterhin aktiv ist.

System

Uhrzeit und Standort

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.

AXIS D2210-VE Radar

Die Weboberfläche

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

- **Automatic date and time (manual NTS KE servers) (Datum und Uhrzeit automatisch (manuelle NTS-KE-Server)):** Diese Option führt eine Synchronisierung mit den sicheren NTP-Schlüssel-Servern durch, die mit dem DHCP-Server verbunden sind.
 - **Manual NTS KE servers (Manuelle NTS-KE-Server):** Geben Sie die IP-Adresse eines oder zweier NTP-Server ein. Wenn Sie zwei NTP-Server verwenden, synchronisiert und passt das Gerät die Uhrzeit anhand der Eingangsdaten beider Geräte an.
- **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.
- **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.
- **Benutzerdefinierte Datum und Uhrzeit:** Stellen Sie Datum und Uhrzeit manuell ein. Klicken Sie auf **Get from system (Vom System abrufen)**, um die Datums- und Uhrzeiteinstellungen einmalig von Ihrem Computer oder Mobilgerät zu abrufen.

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

- **DHCP:** Übernimmt die Zeitzone des DHCP-Servers. Bevor Sie diese Option auswählen können, muss das Gerät mit einem DHCP-Server verbunden werden.
- **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.

- **Latitude (Breite):** Positive Werte bezeichnen Standorte nördlich des Äquators.
- **Longitude (Länge):** Positive Werte bezeichnen Standorte östlich des Referenzmeridians.
- **Heading (Ausrichtung):** Die Ausrichtung des Geräts laut Kompass eingeben. Der Wert 0 steht für: genau nach Norden.
- **Label (Bezeichnung):** Eine aussagekräftige Bezeichnung für das Gerät eingeben.
- **Save (Speichern):** Klicken Sie hier, um den Gerätestandort zu speichern.

Regional settings (Regionale Einstellungen)

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

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

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

Netzwerk

IPv4

AXIS D2210-VE Radar

Die Weboberfläche

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

IP address (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.

Subnet mask (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

IPv6 automatisch zuweisen: Wählen Sie diese Option, um IPv6 einzuschalten und damit der Netzwerk-Router dem Gerät automatisch eine IP-Adresse zuweisen kann.

Host-Name

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

Host-Name: 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 -.

DNS servers (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).

Search domains (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 servers (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 Host-Namen in IP-Adressen übersetzt.

HTTP und HTTPS

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

Um HTTPS auf dem Gerät verwenden zu können, muss ein HTTPS-Zertifikat installiert werden. Gehen Sie für die Erstellung und Installation von Zertifikaten zu **System > Security (System > Sicherheit)**.

AXIS D2210-VE Radar

Die Weboberfläche

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

Protokolle zur Netzwerkerkennung

Bonjour®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

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®: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

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: Aktivieren Sie diese Option, um die automatische Erkennung im Netzwerk bei Aktivierung zuzulassen.

Cloud-Anbindung mit einem Mausklick

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 finden Sie unter axis.com/end-to-end-solutions/hosted-services.

Allow O3C (O3C zulassen):

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

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

Host: Geben Sie die Adresse des Proxy-Servers ein.

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

Anmeldung und Kennwort: Geben Sie falls erforderlich einen Benutzernamen und ein Kennwort für den Proxyserver ein.

Authentication method (Authentifizierungsmethode):

- **Basic (Einfach):** 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.

AXIS D2210-VE Radar

Die Weboberfläche

- **Auto:** Bei dieser Option kann das Gerät die Authentifizierungsmethode automatisch je nach unterstützten Methoden auswählen. Die Methode **Digest** wird gegenüber der Methode **Einfach** bevorzugt.
- Besitzerauthentifizierungsschlüssel (OAK): Klicken Sie auf **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: Wählen Sie die zu verwendende SNMP-Version.

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

Hinweis

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

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

Sicherheit

Zertifikate

AXIS D2210-VE Radar

Die Weboberfläche

Zertifikate werden in Netzwerken zum Authentifizieren von Geräten 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 vor Erhalt eines CA-Zertifikats verwendet werden.
- **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.

Folgende 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 Sie auf diese Option, um ein Zertifikat hinzuzufügen.

- **More (Mehr)**  : Anzeige weiterer Ausfüll- oder Auswahlfelder.
- **Secure keystore (Sicherer Schlüsselspeicher)**: Wählen Sie **Secure element (Sicheres Element)** oder **Trusted Platform Module 2.0** zum sicheren Speichern des privaten Schlüssels aus. Weitere Informationen zum zu wählenden sicheren Schlüsselspeicher finden Sie unter help.axis.com/en-us/axis-os#cryptographic-support.
- **Key type (Schlüsseltyp)**: Wählen Sie in der Dropdown-Liste zum Schutz des Zertifikats den Standard- oder einen anderen Verschlüsselungsalgorithmus aus.



Das Kontextmenü enthält:

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

Secure keystore (Sicherer Schlüsselspeicher)  :

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

IEEE 802.1x and IEEE 802.1AE MACsec (IEEE 802.1x und IEEE 802.1AE MACsec)

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).

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).

AXIS D2210-VE Radar

Die Weboberfläche

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. Die Standardoption ist EAP-TLS. EAP-PEAP/MSCHAPv2 ist eine sicherere Option.

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

CA certificate (CA-Zertifikat): 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: Wählen Sie die in dem Netzwerk-Switch verwendete EAPOL-Version.

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

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.

Die Einstellungen sind nur verfügbar, wenn Sie EAP-TLS als Authentifizierungsmethode verwenden:

Mode (Modus)

- **Dynamic CAK / EAP-TLS:** Die Standardoption. Nach einer gesicherten Verbindung prüft das Gerät, ob MACsec im Netzwerk vorhanden ist.
- **Static CAK / pre-shared key (PSK):** Wählen Sie diese Option aus, um den Schlüsselnamen und -wert für die Verbindung mit dem Netzwerk festzulegen.

Die Einstellungen sind nur verfügbar, wenn Sie EAP-PEAP/MSCHAPv2 als Authentifizierungsmethode verwenden:

- **Password (Kennwort):** Geben Sie das Kennwort für die Benutzeridentität ein.
- **Peap version (Peap-Version):** Wählen Sie die in dem Netzwerk-Switch verwendete Peap-Version aus.
- **Label (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.

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

AXIS D2210-VE Radar

Die Weboberfläche

Activate (Aktivieren): Verwenden Sie den Umschalter, um die Firewall einzuschalten.

Default Policy (Standardrichtlinie): Wählen Sie **Allow (Zulassen)** oder **Deny (Verweigern)**, um für die Firewall einen Standardstatus zuzulassen oder nicht.

Address (Adresse): Geben Sie die IP-Nummern ein, denen der Zugriff auf das Gerät erlaubt oder verweigert wird. Als Format können Sie IPv4/IPv6 oder CIDR verwenden.

Protocol (Protokoll): Wählen Sie, welches Protokoll zur Regel hinzugefügt werden soll.

Port: Geben Sie eine Portnummer zwischen 1 und 65535 ein.

Policy (Richtlinie): Wählen Sie **Allow (Zulassen)** oder **Deny (Verweigern)**, um diese Regel zuzulassen oder nicht.

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

Confirm rules (Regeln bestätigen): Anklicken, um eine ausgewählte Regel zu aktivieren.

Active rules (Aktive Regeln): Eine Übersicht über die Regeln, die momentan auf dem Gerät ausgeführt werden.

Spezifisch signiertes Firmwarezertifikat

Zum Installieren von Test-Firmware oder anderer benutzerdefinierter Firmware von Axis auf dem Gerät benötigen Sie ein spezifisch signiertes Firmwarezertifikat. Das Zertifikat prüft, ob die Firmware sowohl vom Geräteeigentümer als auch von Axis genehmigt wurde. Die Firmware kann nur auf einem bestimmten Gerät ausgeführt werden, das anhand seiner eindeutigen Seriennummer und Chip-ID identifiziert wird. Spezifisch signierte Firmwarezertifikate 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 Firmware installieren.



Das Kontextmenü enthält:

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

Konten

Accounts (Konten)



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

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

New password (Neues Kennwort): Geben Sie ein Kennwort für den Kontonamen 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 erneut ein.

Privileges (Rechte):

- **Administrator:** Hat uneingeschränkten Zugriff auf alle Einstellungen. Administratoren können auch Konten hinzufügen, aktualisieren, bearbeiten und entfernen.
- **Operator (Bediener):** Hat Zugriff auf alle Einstellungen, außer:
 - Alle Systemeinstellungen.
 - Apps werden hinzugefügt.
- **Betrachter:** Darf keine Änderungen an den Einstellungen vornehmen.



Das Kontextmenü enthält:

AXIS D2210-VE Radar


Die Weboberfläche

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

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

Anonymous access (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)  : Schalten Sie diese Option ein, damit anonyme Benutzer das Bild schwenken, neigen und zoomen können.

SSH accounts (SSH-Konten)



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

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

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

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 erneut ein.

Comment (Anmerkung): Geben Sie eine Anmerkung ein (optional).



Das Kontextmenü enthält:

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

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

OpenID Configuration (OpenID-Konfiguration)

Wichtig

Geben Sie die richtigen Werte ein, um sicherzustellen, dass Sie sich erneut am Gerät anmelden können.

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

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

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

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

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

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

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

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

AXIS D2210-VE Radar

Die Weboberfläche

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

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

Save (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.



Add a rule (Regel hinzufügen): Eine Regel erstellen.

Name: Geben Sie einen Namen für die Regel ein.

Wait between actions (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.

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

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

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



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

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

Empfänger

Sie können Ihr Gerät so einrichten, dass Empfänger über Ereignisse benachrichtigt oder Dateien gesendet werden. Die nachfolgende Liste führt alle aktuell im Produkt konfigurierten Empfänger sowie Informationen zur Konfigurierung aus.

Hinweis



Sie können bis zu 20 Empfänger erstellen.




Einen 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:** Geben Sie die vom FTP-Server verwendete Portnummer ein. Der Standardport ist 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.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **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.
 - **Use passive FTP (Passives FTP verwenden):** Normalerweise fordert das Produkt den FTP-Zielsever zum Öffnen der Datenverbindung auf. Normalerweise initiiert das Gerät die FTP-Steuerung und die Datenverbindungen zum Zielsever. Dies ist in der Regel erforderlich, wenn zwischen dem Gerät und dem FTP-Zielsever eine Firewall eingerichtet ist.
- HTTP
 - **URL:** Geben Sie die Netzwerkadresse des HTTP-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise `http://192.168.254.10/cgi-bin/notify.cgi`.
 - **Username (Benutzername):** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **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:** Geben Sie die Netzwerkadresse des HTTPS-Servers und das Skript, das die Anforderung bearbeiten wird, ein. Beispielsweise `https://192.168.254.10/cgi-bin/notify.cgi`.
 - **Validate server certificate (Server-Zertifikat validieren):** Wählen Sie diese Option, um zu überprüfen, ob das Zertifikat von HTTPS-Server erstellt wurde.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **Kennwort:** Geben Sie das Kennwort für die Anmeldung ein.
 - **Proxy:** Schalten Sie diese Option ein und geben Sie die erforderlichen Informationen ein, wenn für die Verbindung mit dem HTTPS-Server ein Proxyserver erforderlich ist.
- Network storage (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:** Geben Sie den Namen der Freigabe auf dem Host ein.
 - **Ordner:** Geben Sie den Pfad zum Verzeichnis ein, in dem Sie die Dateien speichern möchten.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **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:** Geben Sie die vom SFTP-Server verwendete Portnummer ein. Der Standardport ist 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.
 - **Benutzername:** Geben Sie den Benutzernamen für die Anmeldung ein.
 - **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 den 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 or VMS (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.

- **From SIP account (Von SIP-Konto):** Wählen Sie die entsprechende Option aus der Liste aus.
- **To SIP address (An SIP-Adresse):** Geben Sie die entsprechende SIP-Adresse ein.
- **Test:** Klicken Sie hier, um die Anrufeinstellungen auf einwandfreie Funktion zu überprüfen.

- **E-Mail**

- **Send email to (E-Mail senden an):** Geben Sie die gewünschte(n) E-Mail-Versandadresse(n) ein. Trennen Sie mehrere Adressen jeweils mit einem Komma.
- **E-Mail senden von:** Geben Sie die als Absender anzuzeigende E-Mail-Adresse ein.
- **Benutzername:** Geben Sie den Benutzernamen für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **Kennwort:** Geben Sie das Kennwort für den Mailserver ein. Lassen dieses Feld frei, wenn der Mailserver keine Authentifizierung erfordert.
- **Email server (SMTP) (E-Mail-Server (SMTP)):** Geben Sie den Namen des SMTP-Servers ein. Zum Beispiel smtp.gmail.com, smtp.mail.yahoo.com.
- **Port:** Geben Sie die Portnummer des SMTP-Servers ein. Zulässig sind Werte zwischen 0 und 65535. Der Standardport ist 587.
- **Verschlüsselung:** Um die Verschlüsselung zu verwenden, wählen Sie SSL bzw. TLS.
- **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 authentication (POP-Authentifizierung):** Schalten Sie diese Option ein, um den Namen des POP-Servers einzugeben, z.B. pop.gmail.com.

Hinweis

Einige E-Mail-Dienste verwenden Sicherheitsfilter, die verhindern, dass Benutzer eine große Anzahl von Anhängen erhalten oder anzeigen, geplante E-Mails erhalten 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:** Geben Sie die Nummer des für den Zugriff auf den Server verwendeten Ports ein.

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.

AXIS D2210-VE Radar

Die Weboberfläche

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.

Zeitpläne

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.



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 Netzwerkbandbreite verwendet. Der MQTT-Client in der Axis Geräte-Firmware kann die Integration der im Gerät erzeugten Daten und Ereignisse in Systeme vereinfachen, bei denen es sich nicht um Video Management Software (VMS) handelt.

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

Weitere Informationen zu MQTT finden Sie im *AXIS OS Portal*.

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

Verbinden: Aktivieren oder deaktivieren Sie den MQTT-Client.

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

Broker

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

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.

AXIS D2210-VE Radar

Die Weboberfläche

Username (Benutzername): Geben Sie den Benutzernamen ein, den der Client für den Zugriff auf den Server verwenden soll.

Kennwort: Geben Sie ein Kennwort für den Benutzernamen ein.

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

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

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

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

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

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

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

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

Nachricht zum Verbindungsaufbau

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

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

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

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

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.

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

Thema: Geben Sie das Thema der Standardnachricht ein.

Nutzlast: Geben Sie den Inhalt der Standardnachricht ein.

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

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

MQTT publication (MQTT-Veröffentlichung)

AXIS D2210-VE Radar

Die Weboberfläche

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

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

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

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

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

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

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

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

MQTT-Abonnements

+ 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.

Speicher

Network storage (Netzwerk-Speicher)

AXIS D2210-VE Radar

Die Weboberfläche

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

Add network storage (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:** Geben Sie den Namen des freigegebenen Speicherorts auf dem Host-Server ein. Mehrere Axis Geräte können dieselbe Netzwerk-Freigabe verwenden, da jedes Gerät einen eigenen Ordner erhält.
- **User (Benutzer):** Wenn der Server eine Anmeldung erfordert, geben Sie den Benutzernamen ein. Zur Anmeldung an einem bestimmten Domainserver geben Sie DOMAIN\Benutzername ein.
- **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.

Remove network storage (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 (Schreibschutz): Schalten Sie diese Option ein, 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.

Retention time (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.

Tools (Werkzeuge)

- **Test connection (Verbindung testen):** Prüfen Sie die Verbindung zur Netzwerk-Freigabe.
- **Format (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.

Integrierter Speicher

Wichtig

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

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

Schreibschutz: Aktivieren Sie diese Option, 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.

AXIS D2210-VE Radar

Die Weboberfläche

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

Werkzeuge

- **Überprüfen:** Überprüfen Sie die SD-Speicherkarte auf Fehler. Diese Funktion steht nur für das Dateisystem ext4 zur Verfügung.
- **Reparieren:** Beheben Sie Fehler im Dateisystem ext4. Um eine SD-Karte mit dem Dateisystem VFAT zu reparieren, werfen Sie die SD-Karte aus und setzen Sie sie einem Computer ein, bevor Sie die Festplattenreparatur durchführen.
- **Format (Formatieren):** Formatieren Sie die SD-Karte zum Beispiel, wenn das Dateisystem geändert oder alle Daten schnell gelöscht werden sollen. Die beiden verfügbaren Dateisysteme sind VFAT und ext4. Das Format ext4 wird wegen des Schutzes vor Datenverlust beim Auswerfen der Karte oder bei plötzlichem Stromausfall empfohlen. Sie benötigen jedoch 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. **Encrypt (Verschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Verschlüsselung mit **Encrypt** sind alle auf der SD-Karte gespeicherten Daten mittels Verschlüsselung geschützt.
- **Decrypt (Entschlüsseln):** Verwenden Sie dieses Tool, um die SD-Karte ohne Verschlüsselung zu formatieren. **Decrypt (Entschlüsseln)** löscht alle auf der SD-Karte gespeicherten Daten. Nach der Entschlüsselung mit **Decrypt** sind die auf der SD-Karte gespeicherten Daten nicht mehr mittels Verschlüsselung geschützt.
- **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.

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

Videostreamprofile

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): 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.


Description (Beschreibung): Fügen Sie eine Profilbeschreibung hinzu.

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

Resolution (Auflösung): Siehe für eine Beschreibung dieser Einstellung.

Frame rate (Bildrate): Siehe für eine Beschreibung dieser Einstellung.

Compression (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.


AXIS D2210-VE Radar

Die Weboberfläche

Dynamic FPS (Dynamische Bilder pro Sekunde)  : Siehe für eine Beschreibung dieser Einstellung.


Dynamic GOP (Dynamic Group of Pictures)  : Siehe für eine Beschreibung dieser Einstellung.

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

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

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

Include overlays (Overlays einbeziehen): Wählen Sie den Typ der einzubeziehenden Overlays aus. Weitere Informationen zum Hinzufügen von Overlays finden Sie unter *Overlays auf Seite 35*.

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

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 sorgt für 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.

Account (Konto): Geben Sie einen eindeutigen Kontonamen ein.

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 erneut ein.

Rolle:

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

AXIS D2210-VE Radar

Die Weboberfläche

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

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

Profile name (Profilname): Fügen Sie einen Namen für das Medienprofil hinzu.

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


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

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


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

Hinweis

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

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


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

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

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

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 abubrechen und alle Einstellungen zu löschen.

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

Melder

Stoßerkennung

AXIS D2210-VE Radar

Die Weboberfläche

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

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

Zubehör



E/A-Ports



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

Schließen Sie externe Geräte wie Relais und LEDs über digitale Ausgänge an. Sie können verbundene Geräte über die VAPIX® Application Programming Interface oder über die Weboberfläche aktivieren.

Port

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


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

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

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

Hinweis

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

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

Edge-to-Edge

Mit **Audio pairing (Audio-Kopplung)** können kompatible Netzwerk-Lautsprecher oder Mikrofone von Axis so eingesetzt werden, als seien sie Teil des Hauptgeräts. Nach den Kopplung fungiert der Netzwerklautsprecher als Audioausgabegerät, mit dem Audioclips abgespielt und Audio übertragen werden kann.

Wichtig

Um diese Funktion mit einer Video Management Software (VMS) verwenden zu können, koppeln Sie zuerst das Gerät mit dem Lautsprecher und fügen dann Ihrer VMS das Gerät 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 Rückkopplungsschleife vermieden, wenn das erfassende Mikrofon Audio vom Lautsprecher mit aufnimmt.

AXIS D2210-VE Radar

Die Weboberfläche

Audiokopplung

Address (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.

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

Clear fields (Felder löschen): Klicken Sie hier, um alle Felder zu löschen.

Connect (Verbinden): Klicken Sie hier, um eine Verbindung mit dem Lautsprecher herzustellen.

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.

PTZ-Koppelung

Address (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.

Clear fields (Felder löschen): Klicken Sie hier, um alle Felder zu löschen.

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

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

Protokolle

Protokolle und Berichte

Berichte

- **View the device server report (Geräteserver-Bericht anzeigen):** Zeigt Informationen zum Produktstatus in einem Popup-Fenster bereit. Das Zugangsprotokoll wird automatisch dem Server-Bericht angefügt.
- **Download the device server report (Bericht zum Geräteserver herunterladen):** Dabei wird eine .zip-Datei mit dem vollständigen Server-Bericht als Textdatei im Format UTF-8 sowie einer Momentaufnahme 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

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

Netzwerk-Trace

AXIS D2210-VE Radar

Die Weboberfläche

Wichtig

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

Netzwerkablaufsverfolgungsdateien zeichnen Netzwerkaktivitäten auf und helfen so bei der Fehlersuche und -behebung.

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

Remote-Systemprotokoll

Syslog ist ein Standard für die Nachrichtenprotokollierung. Dadurch können die Software, die Nachrichten generiert, das System, in dem sie gespeichert sind, und die Software, die sie meldet und analysiert voneinander getrennt werden. 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 Host-Namen oder die IP-Adresse des Servers ein.

Format: 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.

Severity (Schweregrad): Wählen Sie aus, welche Meldungen bei Auslösung gesendet werden sollen.

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

Neustart: Starten Sie das Gerät neu. Dies hat keine Auswirkungen auf aktuelle Einstellungen. Aktive Anwendungen werden automatisch neu gestartet.

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

AXIS D2210-VE Radar

Die Weboberfläche

Wichtig

Die einzigen nach der Wiederherstellung weiterhin gespeicherten Einstellungen sind:

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

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

Hinweis

Sämtliche Firmware des Axis Geräts ist digital signiert, um sicherzustellen, dass Sie nur die verifizierte Firmware auf Ihrem Gerät installieren. Diese Maßnahme erhöht das allgemeine Mindestniveau der Cybersicherheit für die Geräte von Axis. Weitere Informationen finden Sie im Whitepaper "Signierte Firmware, sicherer Start und Sicherheit von Privatschlüsseln" auf axis.com.

Firmwareaktualisierung: Aktualisieren Sie auf eine neue Firmwareversion. Neue Firmwareversionen können verbesserte Funktionen, Fehlerkorrekturen und vollständig neue Merkmale beinhalten. Wir empfehlen Ihnen, stets die aktuellste 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 Firmwareversion.
- **Werkseinstellungen:** Aktualisieren und alle Einstellungen werden auf die Werkseinstellungen zurückgesetzt. Wenn Sie diese Option wählen, können Sie nach der Aktualisierung nicht mehr zur vorherigen Firmwareversion zurückkehren.
- **Automatisches Zurücksetzen:** Aktualisieren Sie und bestätigen Sie die Aktualisierung innerhalb der festgelegten Zeit. Wenn Sie diese nicht bestätigen, wird das Gerät auf die vorherige Firmwareversion zurückgesetzt.

Firmware zurücksetzen: Gehen Sie auf die vorherige Firmwareversion zurück.

AXIS D2210-VE Radar

Ihre Installation validieren

Ihre Installation validieren

Installation des Radars validieren

Hinweis

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

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

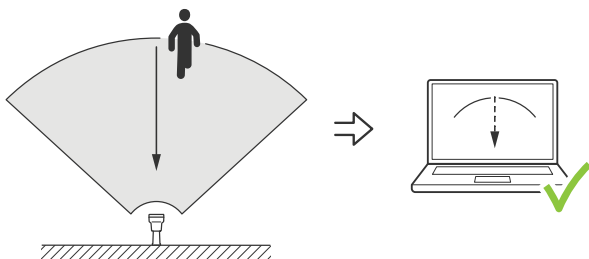
Zuerst *Radar kalibrieren auf Seite 16*, bevor die Validierung versucht wird. Führen Sie dann folgende Schritte aus:

Stellen Sie sicher, dass keine falschen Erfassungen vorhanden sind.

1. Stellen Sie sicher, dass im Erfassungsbereich keine menschlichen Aktivitäten stattfinden.
2. Warten Sie einige Minuten, bis sichergestellt ist, dass der Radar keine statischen Objekte im Erfassungsbereich erkennt.
3. Wenn keine unerwünschten Erfassungen vorhanden sind, können Sie Schritt 4 überspringen.
4. Erfahren Sie unter *Fehlalarme minimieren auf Seite 20* Fehlalarme minimieren, wie Sie bei unerwünschten Erfassungen bestimmte Arten von Bewegungen oder Objekten herausfiltern, die Abdeckung ändern oder die Erfassungsempfindlichkeit anpassen.

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

1. Gehen Sie auf die Weboberfläche des Radars und zeichnen Sie die Sitzung auf. Hilfe dazu finden Sie unter *Video aufzeichnen und ansehen auf Seite 22*.
2. Starten Sie bis zu 60 m vor dem Radar und laufen Sie direkt auf den Radar zu.
3. Überprüfen Sie die Sitzung auf der Weboberfläche des Radars. Das Symbol für eine menschliche Klassifizierung sollte angezeigt werden, sofern Sie erkannt wurden.
4. Stellen Sie sicher, dass auf der Weboberfläche des Radars die korrekte Richtung angezeigt wird.



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

1. Gehen Sie auf die Weboberfläche des Radars und zeichnen Sie die Sitzung auf. Hilfe dazu finden Sie unter *Video aufzeichnen und ansehen auf Seite 22*.
2. Starten Sie 30 m vom Radar entfernt und durchkreuzen Sie den Abdeckungsbereich des Radars.
3. Stellen Sie sicher, dass auf der Weboberfläche des Radars das Symbol für eine menschliche Klassifizierung angezeigt wird.
4. Stellen Sie sicher, dass auf der Weboberfläche des Radars die korrekte Richtung angezeigt wird.

AXIS D2210-VE Radar

Ihre Installation validieren

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

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

Validierung abschließen

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

1. Stellen Sie sicher, dass Ihr Radar konfiguriert ist und befolgen Sie die Anweisungen.
2. Für eine weitere Validierung fügen Sie eine Referenzkarte hinzu und kalibrieren Sie sie.
3. Stellen Sie das Radarszenario ein, dass Daten aufgezeichnet werden, wenn ein geeignetes Objekt erkannt wird. Standardmäßig ist **Sekunden bis zum Auslösen** auf zwei Sekunden eingestellt, aber Sie können die Zahl bei Bedarf über die Weboberfläche ändern.

4. Legen Sie fest, dass der Radar Daten aufzeichnen soll, wenn ein geeignetes Objekt erkannt wird.

Anweisungen finden Sie unter *Video aufzeichnen und ansehen auf Seite 22*.

5. Legen Sie die **Dauer der Spur** auf eine Stunde fest, sodass Sie auf jeden Fall ausreichend Zeit haben, um Ihren Platz zu verlassen, zu Fuß durch den Überwachungsbereich zu gehen und zu Ihrem Platz zurückzukehren. Die **Dauer der Spur** hält in der Live-Ansicht des Radars die Verfolgung für die eingestellte Zeit aufrecht. Nach Abschluss der Validierung kann sie deaktiviert werden.
6. Gehen Sie entlang der Grenze des vom Radar abgedeckten Bereichs und vergewissern Sie sich, dass die Verfolgung auf dem System mit der Route übereinstimmt, die Sie zurückgelegt haben.
7. Wenn Sie mit den Ergebnissen Ihrer Validierung nicht zufrieden sind, kalibrieren Sie die Referenzkarte neu und wiederholen Sie die Validierung.

Mehr erfahren

Streaming und Speicher

Videokomprimierungsformate

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

Motion JPEG

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

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

H.264 oder MPEG-4 Part 10/AVC

Hinweis

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

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

H.265 oder MPEG-H Part 2/HEVC

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

Hinweis

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

Bitratensteuerung

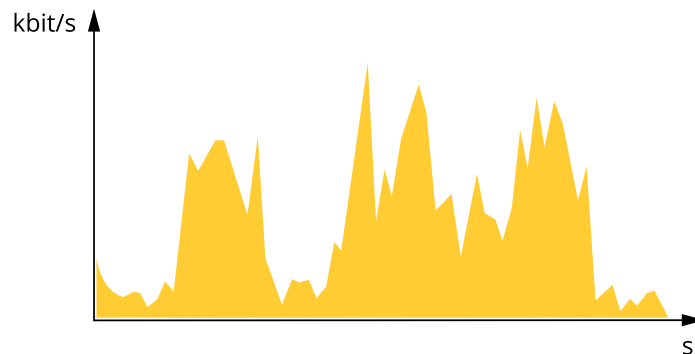
Die Bitratensteuerung hilft Ihnen bei der Verwaltung der Bandbreitennutzung Ihres Videostreams.

Variable Bitrate (VBR)

Mit variabler 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.

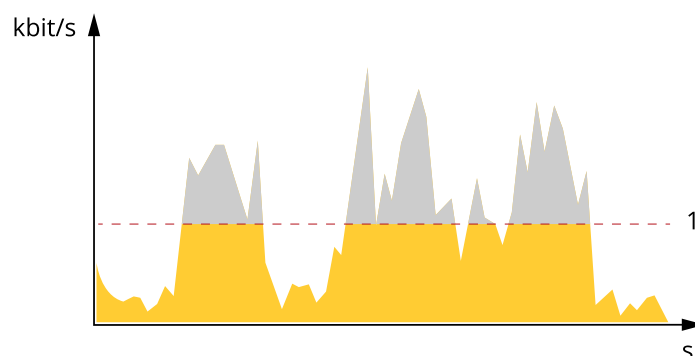
AXIS D2210-VE Radar

Mehr erfahren



Maximale Bitrate (MBR)

Mit maximaler 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

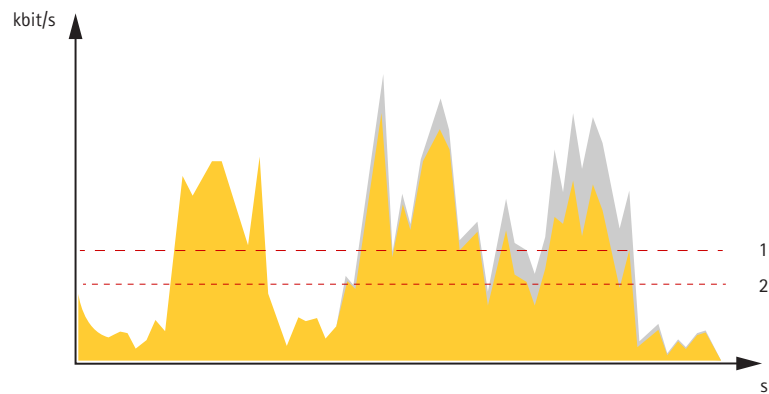
Durchschnittliche Bitrate (ABR)

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 (Vorhaltezeit) 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.

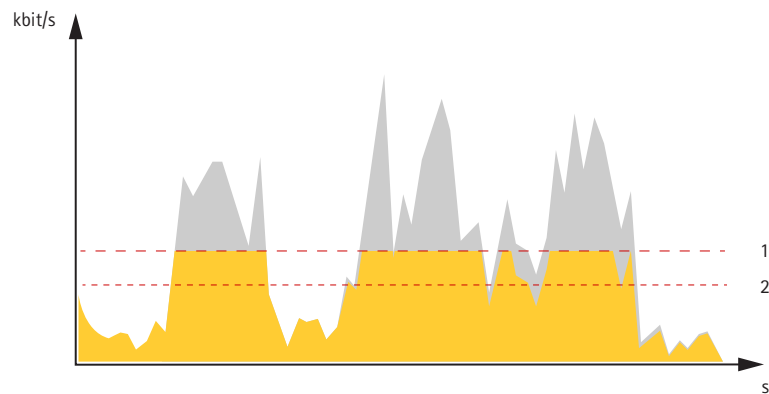
AXIS D2210-VE Radar

Mehr erfahren



- 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

Overlays

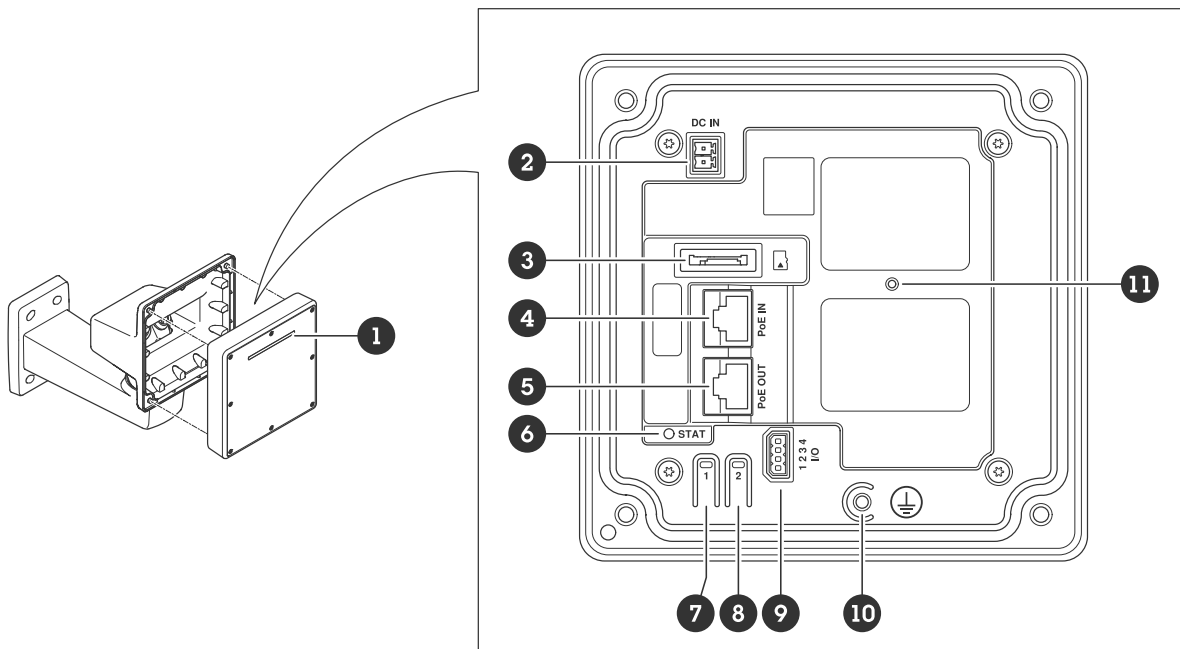
Overlays werden über den Videostream gelegt. Sie werden verwendet, um weitere Informationen wie etwa Zeitstempel anzuzeigen, oder auch beim Installieren und Konfigurieren des Produkts. Sie können entweder Text oder ein Bild hinzufügen.

AXIS D2210-VE Radar

Technische Daten

Technische Daten

Produktübersicht



- 1 Dynamische LED-Leiste
- 2 Stromanschluss (Gleichstrom)
- 3 microSD-Karteneinschub
- 4 Netzwerk-Anschluss (PoE in)
- 5 Netzwerk-Anschluss (PoE out)
- 6 Status-LED
- 7 Steuertaste
- 8 Aktionstaste
- 9 E/A-Anschluss
- 10 Erdungsschraube
- 11 Reset-Taste

LED-Anzeigen

Hinweis

Die Status-LED kann so eingestellt werden, dass sie bei einem aktiven Ereignis blinkt.

Status-LED	Anzeige
Grün	Leuchtet bei Normalbetrieb grün.
Gelb	Leuchtet beim Start. Blinkt während Firmware-Aktualisierung und Wiederherstellung der Werkseinstellungen.
Rot	Firmwareaktualisierung fehlgeschlagen.

AXIS D2210-VE Radar

Technische Daten

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.

Empfehlungen zu SD-Karten finden Sie auf axis.com.



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

Tasten

Steuertaste

Die Steuertaste hat folgende Funktionen:

- Zurücksetzen des Produkts auf die Werkseinstellungen. Siehe *Zurücksetzen auf die Werkseinstellungen auf Seite 72*.
- Herstellen einer Verbindung mithilfe eines O3C-Diensts mit nur einem Klick über das Internet. Drücken Sie zum Herstellen der Verbindung die Taste und halten Sie sie etwa 3 Sekunden lang gedrückt, bis die Status-LED grün blinkt.

Anschlüsse

Netzwerk-Anschluss (PoE in)

RJ45-Ethernetanschluss mit Power over Ethernet IEEE 802.3bt, Typ 3 Klasse 6.

Hinweis

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

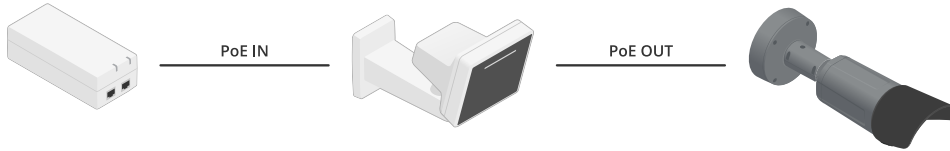
Netzwerk-Anschluss (PoE out)

RJ45-Ethernetanschluss für Power over Ethernet IEEE 802.3at, Typ 2 Klasse 4, max. 30 W.

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

AXIS D2210-VE Radar

Technische Daten



Hinweis

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

Hinweis

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

Hinweis

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

Hinweis

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

E/A-Anschluss

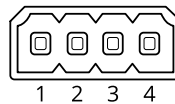
Über den E/A-Anschluss wird Zusatzausrüstung in Verbindung mit Ereignisauslösungen, Alarmbenachrichtigungen und anderen Funktionen angeschaltet. Außer dem Bezugspunkt 0 V Gleichstrom und Strom (Gleichstromausgang) besitzt der E/A-Anschluss eine Schnittstelle zum:

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

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

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

4-poliger Anschlussblock



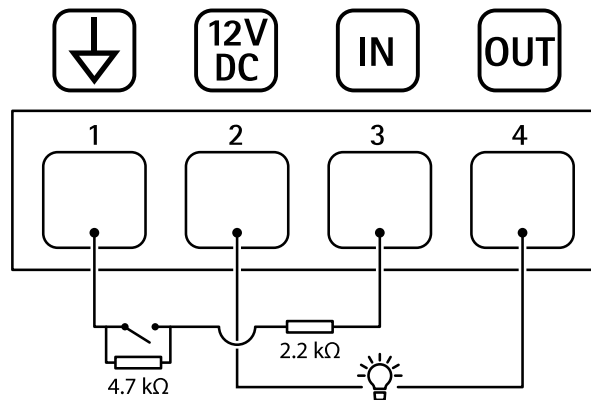
Funktion	Kontakt	Hinweise	Technische Daten
Erdung Gleichstrom	1		0 V Gleichstrom
Gleichstromausgang	2	Darf für die Stromversorgung von Zusatzgeräten verwendet werden. Hinweis: Dieser Kontakt darf nur für den Stromausgang verwendet werden.	12 V Gleichstrom Max. Stromstärke = 25 mA

AXIS D2210-VE Radar

Technische Daten

Digitaleingang	3	Zum Aktivieren an Kontakt 1 anschließen; zum Deaktivieren nicht anschließen.	0 bis max. 30 V Gleichstrom
Digitalausgang	4	Interne Verbindung mit Kontakt 1 (Gleichstrom Erdschluss), wenn aktiviert; unverbunden, wenn deaktiviert. Bei Verwendung mit einer induktiven Last, wie etwa einem Relais, muss zum Schutz vor Spannungssprüngen eine Diode parallel zur Last geschaltet werden.	0 bis max. 30 V Gleichstrom, Open Drain, 100 mA

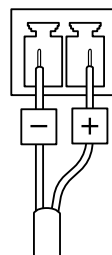
Beispiel:



- 1 Erdung Gleichstrom
- 2 Gleichstromausgang 12 V, max. 25 mA
- 3 Überwacher Eingang
- 4 Digitaler Ausgang

Stromanschluss

2-poliger Anschlussblock für die Gleichstromversorgung. Verwenden Sie eine mit den Anforderungen für Schutzkleinspannung (SELV) kompatible Stromquelle mit begrenzter Leistung (LPS) mit einer Nennausgangsleistung von ≤ 100 W oder einem dauerhaft auf ≤ 5 A begrenzten Nennausgangsstrom.



AXIS D2210-VE Radar

Empfehlungen zur Reinigung

Empfehlungen zur Reinigung

HINWEIS

Verwenden Sie niemals ein grobes Reinigungsmittel wie Benzin, Benzol oder Aceton.

1. Verwenden Sie eine Druckluft-Dose zum Entfernen von Staub oder Schmutz von dem Gerät.
2. Ggf. die Linse mit einem weichen, mit lauwarmem Wasser angefeuchteten Tuch reinigen.

Hinweis

Vermeiden Sie die Reinigung bei direktem Sonnenlicht oder bei erhöhten Temperaturen, da dies zu Flecken beim Trocknen der Wassertropfen führen kann.

Fehlerbehebung

Zurücksetzen auf die Werkseinstellungen

Wichtig

Das Zurücksetzen auf die Werkseinstellungen sollte mit Vorsicht erfolgen. Beim Zurücksetzen auf die Werkseinstellungen werden alle Einstellungen einschließlich der IP-Adresse zurückgesetzt.

So wird das Produkt auf die werksseitigen Standardeinstellungen zurückgesetzt:

1. Trennen Sie das Produkt von der Stromversorgung.
2. Halten Sie die Steuertaste gedrückt und stellen Sie die Stromversorgung wieder her. Siehe *Produktübersicht auf Seite 67*.
3. Halten Sie die Steuertaste etwa 15 bis 30 Sekunden gedrückt, bis die Status-LED gelb blinkt.
4. Lassen Sie die Steuertaste los. Der Vorgang ist abgeschlossen, wenn die Status-LED grün leuchtet. Das Produkt wurde auf die Werkseinstellungen zurückgesetzt. Wenn im Netzwerk kein DHCP-Server verfügbar ist, lautet die Standard-IP-Adresse 192.168.0.90.
5. Verwenden Sie Installations- und Verwaltungstools, um IP-Adressen zuzuweisen, das Kennwort festzulegen und auf das Gerät zuzugreifen.

Die Installations- und Verwaltungstools finden auf den Supportseiten unter axis.com/support.

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

Aktuelle Firmware überprüfen

Firmware ist die Software, mit der die Funktionalität von Netzwerk-Geräten festgelegt wird. Wir empfehlen Ihnen, vor jeder Problembehebung zunächst die aktuelle Firmwareversion zu überprüfen. Die aktuelle Firmwareversion enthält möglicherweise eine Verbesserung, mit der das Problem behoben werden kann.

So überprüfen Sie die aktuelle Firmware:

1. Wechseln Sie zur Weboberfläche des Geräts > **Status**.
2. Die Firmwareversion finden Sie unter **Geräteinformationen**.

Firmware aktualisieren

Wichtig

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

Hinweis

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

1. Die Firmware können Sie auf axis.com/support/device-software kostenlos auf Ihren Computer herunterladen.
2. Melden Sie sich auf dem Gerät als Administrator an.

AXIS D2210-VE Radar

Fehlerbehebung

3. Rufen Sie Maintenance > Firmware upgrade (Wartung > Firmwareaktualisierung) auf und klicken Sie auf Upgrade (Aktualisierung).

Nach der Aktualisierung wird das Produkt automatisch neu gestartet.

Technische Fragen, Hinweise und Lösungen

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

Probleme beim Aktualisieren der Firmware

Aktualisierung der Firmware fehlgeschlagen	Nach fehlgeschlagener Aktualisierung der Firmware lädt das Gerät erneut die Vorversion. Die häufigste Fehlerursache ist, wenn eine falsche Firmwaredatei hochgeladen wurde. Überprüfen, ob der Name der Firmwaredatei dem Gerät entspricht und erneut versuchen.
Probleme nach dem Aktualisieren von Firmware	Bei nach dem Aktualisieren von Firmware auftretenden Problemen die Installation über die Wartungsseite auf die Vorversion zurückrollen.

Probleme beim Einstellen der IP-Adresse

Das Gerät befindet sich in einem anderen Subnetz	Wenn sich die IP-Adresse des Geräts und die IP-Adresse des zum Zugriff auf das Gerät verwendeten Computers in unterschiedlichen Subnetzen befinden, kann die IP-Adresse nicht eingestellt werden. Wenden Sie sich an Ihren Netzwerkadministrator, um eine IP-Adresse zu erhalten.
Die IP-Adresse wird von einem anderen Gerät verwendet	Trennen Sie das Axis Gerät vom Netzwerk. Führen Sie einen Ping-Befehl aus (geben Sie in einem Befehls-/DOS-Fenster <code>ping</code> und die IP-Adresse des Geräts ein): <ul style="list-style-type: none">• Wenn Folgendes angezeigt wird: <code>Reply from (Antwort von)<IP address>: bytes=32; time=10...</code> dies bedeutet, dass die IP-Adresse möglicherweise bereits von einem anderen Gerät im Netzwerk verwendet wird. Bitten Sie den Netzwerkadministrator um eine neue IP-Adresse, und installieren Sie das Gerät erneut.• Wenn Folgendes angezeigt wird: <code>Request timed out</code> bedeutet, dass die IP-Adresse mit dem Axis Gerät verwendet werden kann. Prüfen Sie alle Kabel und installieren Sie das Gerät erneut.
Möglicher IP-Adressenkonflikt mit einem anderen Gerät im selben Subnetz.	Die statische IP-Adresse des Axis Geräts wird verwendet, bevor der DHCP-Server eine dynamische Adresse festlegt. Verwendet also ein anderes Gerät standardmäßig dieselbe statische IP-Adresse, treten beim Zugreifen auf das Gerät möglicherweise Probleme auf.

Vom Browser aus ist kein Zugriff auf das Gerät möglich

Anmeldung nicht möglich	Wenn HTTPS aktiviert ist, stellen Sie sicher, dass beim Anmelden das korrekte Protokoll (HTTP oder HTTPS) verwendet wird. Möglicherweise müssen Sie manuell <code>http</code> oder <code>https</code> in die Adressleiste des Browsers eingeben. Wenn das Kennwort für das Haupt-Konto vergessen wurde, muss das Gerät auf die werksseitigen Standardeinstellungen zurückgesetzt werden. Siehe <i>Zurücksetzen auf die Werkseinstellungen auf Seite 72</i> .
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. Ermitteln Sie das Gerät anhand seiner Modellnummer, Seriennummer oder anhand des DNS-Namens (sofern der Name konfiguriert wurde). Bei Bedarf kann eine statische IP-Adresse manuell zugewiesen werden. Anweisungen dazu finden Sie auf axis.com/support .
Zertifikatfehler beim Verwenden von IEEE 802.1X	Damit die Authentifizierung ordnungsgemäß funktioniert, müssen die Datums- und Uhrzeiteinstellungen des Axis Geräts mit einem NTP-Server synchronisiert werden. Gehen Sie auf Einstellungen > System > Datum und Uhrzeit .

AXIS D2210-VE Radar

Fehlerbehebung

Auf das Gerät kann lokal, nicht jedoch extern zugegriffen werden

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

- AXIS Companion: Kostenlos, ideal für kleine Systeme mit grundlegenden Überwachungsanforderungen.
- AXIS Camera Station Video Management Software: Kostenlose 30-Tage-Testversion, ideal für kleine bis mittelgroße Systeme.

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

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

Die Firewall blockiert den Datenverkehr über Port 8883, da er als ungesichert eingestuft wird.

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

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

Leistungsaspekte

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

Die folgenden wichtigen Faktoren müssen beachtet werden:

- Intensive Netzwerknutzung aufgrund mangelhafter Infrastruktur beeinflusst die Bandbreite.

Support kontaktieren

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

