AXIS Perimeter Defender

AXIS Perimeter Defender
AXIS Perimeter Defender PTZ Autotracking

Benutzerhandbuch

Inhalt

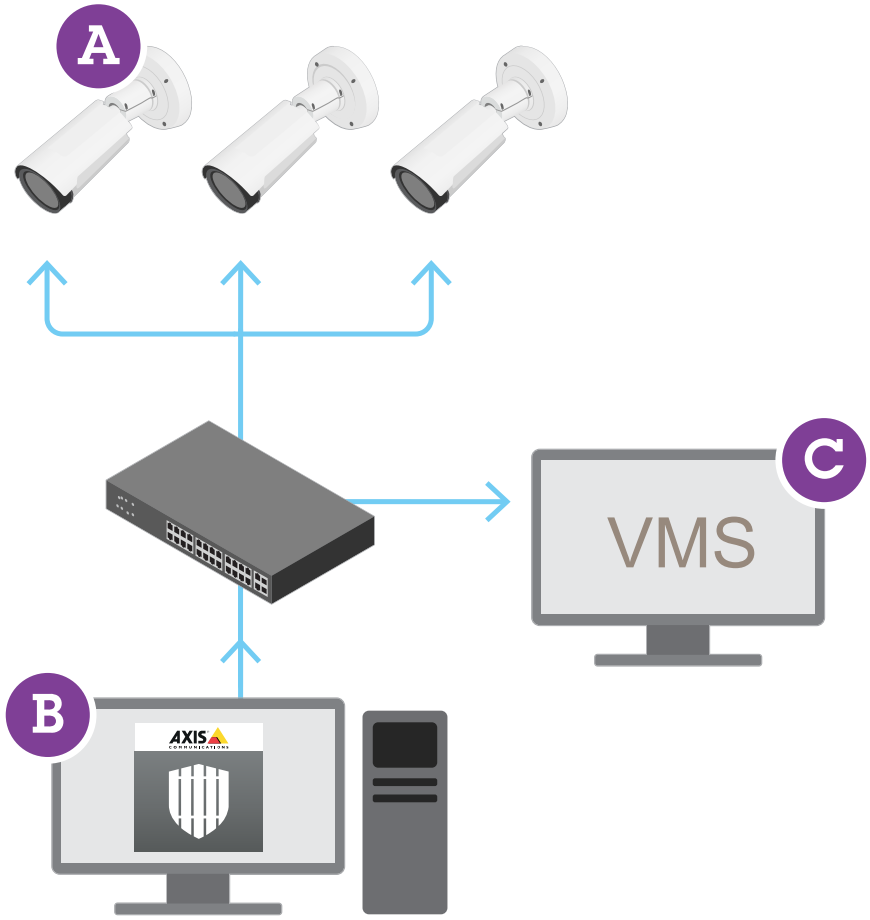
AXIS Perimeter Defender

AXIS Perimeter Defender ist eine Anwendung für die Überwachung und den Schutz von Grundstücken. Sie eignet sich ideal für den Schutz vor Grundstücken, bei denen die physische Zutrittskontrolle durch eine zuverlässige Eindringerkennung unterstützt werden muss.

AXIS Perimeter Defender ist in erster Linie für einen sogenannten sterilen Zonenschutz ausgelegt, beispielsweise an einem Zaun, der eine Grenze markiert. Der Begriff „sterile Zone" bezieht sich auf einen Bereich, in dem Menschen in der Regel nicht zu finden sind.

Verwenden Sie AXIS Perimeter Defender in Außenbereichen, um:

- sich bewegende Personen zu erkennen
- sich bewegende Fahrzeuge, ohne die Fahrzeugtypen zu unterscheiden.



Diese Kamera kann die Anwendung im Kalibrierungsmodus, im KI-Modus oder kombiniert miteinander in beiden Modi ausführen. Wenn Sie die Kameras nur im KI-Modus ausführen möchten, ist eine flexiblerer Installation der Kamera möglich und die Kameras müssen nicht kalibriert werden.

AXIS Perimeter Defender besteht aus einer Desktop-Schnittstelle (B), mit der Sie die Anwendung auf den Kameras (A) installieren und einrichten können. Anschließend können Sie das System so konfigurieren, dass Alarme an die Video Management Software (C) gesendet werden.

AXIS Perimeter Defender PTZ Autotracking ist ein Plug-In für die AXIS Perimeter Defender Anwendung, das dieselbe Desktop-Schnittstelle verwendet. Mit dem Plug-In wird eine feste visuelle oder Wärmebildkamera mit

einer Axis Q-Line PTZ-Kamera gekoppelt. Sie können dann die kontinuierliche Erfassung einer Szene mit der festen Kamera beibehalten, während die PTZ-Kamera die erfassten Objekte automatisch erfasst.

Wichtig

Für AXIS Perimeter Defender PTZ Autotracking sind sowohl die unbewegliche als auch die PTZ-Kamera zu kalibrieren.

AXIS Perimeter Defender bietet die folgenden Typen von Erfassungsszenarien:

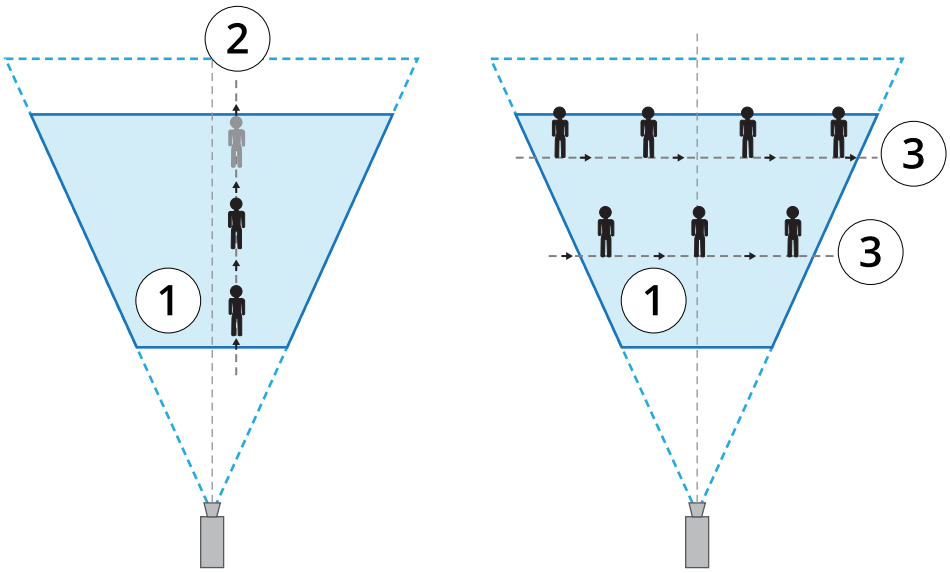
- **Einbruch**: Löst einen Alarm aus, wenn eine Person oder ein Fahrzeug in eine Zone eindringt, die auf dem Boden definiert wurde (aus jeder Richtung und mit jedem Bewegungspfad).
- **Herumlungern**: Löst einen Alarm aus, wenn eine Person oder ein Fahrzeug eine bestimmte Anzahl von Sekunden lang in einer auf dem Boden definierten Zone verbleibt.
- **Zonenübergreifend**: Löst einen Alarm aus, wenn eine Person oder ein Fahrzeug zwei oder mehr Zonen durchläuft, die in einer bestimmten Reihenfolge auf dem Boden definiert sind.
- **Bedingt**: Löst einen Alarm aus, wenn eine Person oder ein Fahrzeug in eine auf dem Boden definierte Zone eindringt, ohne zuvor eine andere Zone oder Zonen durchlaufen zu haben, die auf dem Boden definiert sind.

So funktioniert es:

Erfassung von Objekten

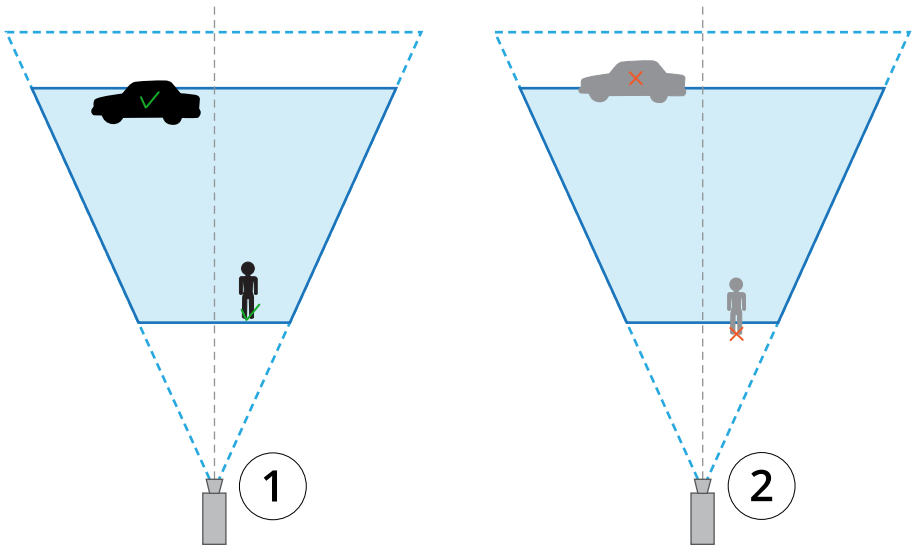
AXIS Perimeter Defender kann sich bewegende Personen oder Fahrzeuge erfassen. Erfasst werden können:

- Eine Person oder ein Fahrzeug muss mindestens drei Sekunden lang vollständig im Erfassungszone sichtbar sein.
- Fahrzeuge dürfen bis zu 12 Meter lang sein (im KI-Modus gibt es keine maximale Länge).
- Personen oder Fahrzeuge müssen sich im Sichtfeld der Kamera aus sichtbar bewegen. Dadurch ist die Erfassungsrate bei Personen, die sich in einer geraden Linie der Kamera nähern oder von der Kamera wegbewegen, niedriger ist als bei Personen, die sich quer zum Sichtfeld der Kamera bewegen.



1 Überwachungsbereich
2 Person geht von der Kamera weg
3 Personen bewegt sich senkrecht zum Sichtfeld der Kamera

- Der Erfassungspunkt muss sich innerhalb der Erfassungszone befinden. Der Erfassungspunkt befindet sich an den Füßen einer Person bzw. in der Mitte eines Fahrzeugs.



1 Erfassungspunkt innerhalb der Erfassungszone
2 Erfassungspunkt außerhalb der Erfassungszone

Nach der Erfassung verfolgt AXIS Perimeter Defender die Person oder das Fahrzeug weiter, auch wenn sie/es teilweise verborgen ist, z. B. wenn der Körper einer Person durch ein verdeckt und nur der Kopf der Person sichtbar ist.

Wenn eine erfasste Person oder ein Fahrzeug sich einige Sekunden lang nicht mehr bewegt, beendet AXIS Perimeter Defender die Verfolgung. Wenn sie/es sich nach weniger als 15 Sekundenerneut bewegt, setzt die Anwendung die Verfolgung fort. Wenn sich die Person in einer Zonenübergangszone befand, gibt es keine Gewährleistung, dass das Szenario ordnungsgemäß ausgelöst wird.

Wie funktioniert PTZ-Autotracking?

In AXIS Perimeter Defender PTZ-Autotracking arbeiten eine feste Kamera und eine PTZ-Kamera zusammen. Wenn die feste Kamera sich bewegende Personen oder Fahrzeuge erfasst, werden die Objektstandortdaten an die gekoppelte PTZ-Kamera gesendet. Solange sich die Objekte im Sichtfeld der unbeweglichen Kamera befinden, kann die PTZ-Kamera den Objekten automatisch folgen und den Zoom anpassen, um sie im Blickfeld zu behalten.

Bedingungen, unter denen Erfassungen verzögert oder übersehen werden können

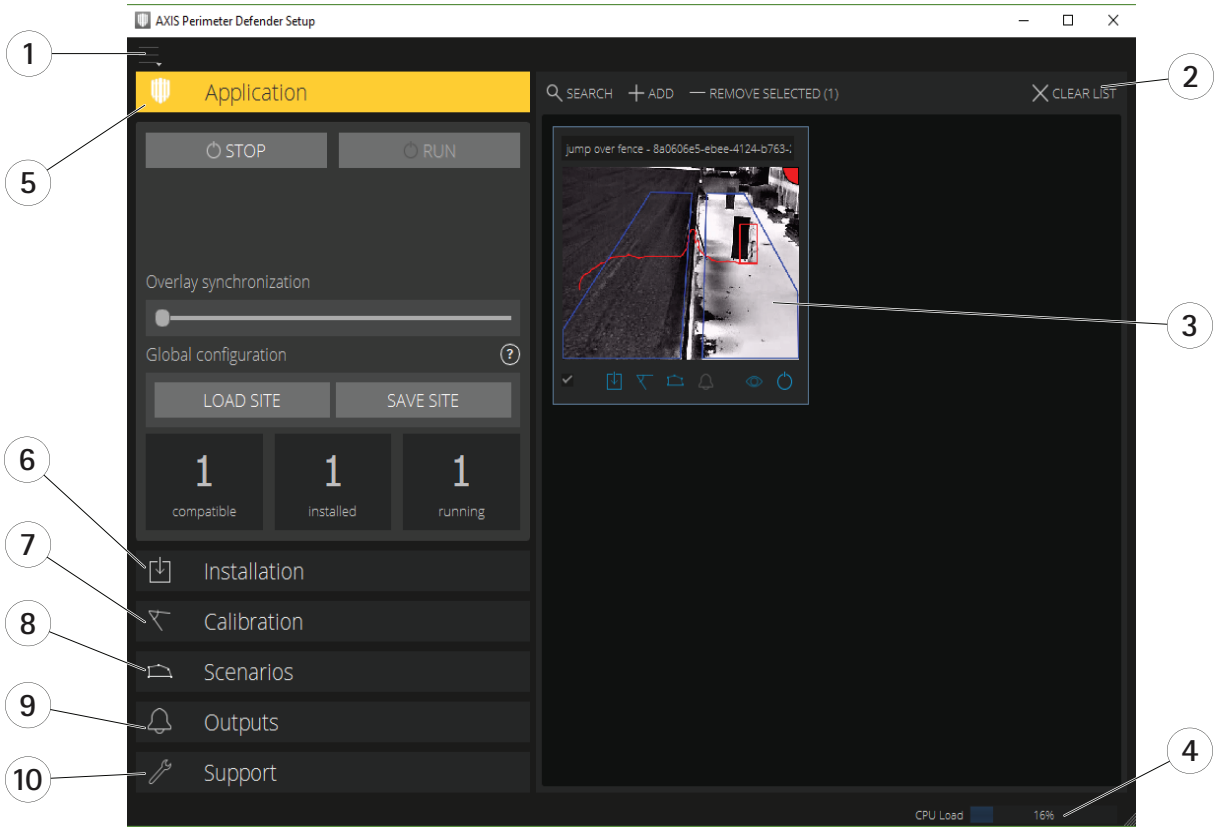
- Nebel
- Licht, das direkt in die Kamera scheint
- Unzureichendes Licht
- Bild mit übermäßigem Rauschen

Situationen, die Fehlalarme auslösen können

- Teilweise versteckte Personen oder Fahrzeuge. Beispielsweise kann ein kleiner Van, der hinter einer Wand auftaucht, wie eine Person aussehen, da der sichtbare Teil hoch und schmal ist.
- Insekten auf dem Kameraobjektiv. Beachten Sie, dass Tag- und Nacht-Kameras mit Infrarotlicht Insekten und Spinnen anziehen.
- Eine Kombination aus Autoscheinwerfern und starkem Regen.
- Tiere in der Größe eines Menschen, insbesondere bei Auswahl der zusätzlichen Annäherungsformen Kriechen oder Rollen in der Registerkarte **Scenarios** (Szenarien).
- Starkes Licht, das Schatten erzeugt.

Die Benutzeroberfläche

Mit der AXIS Perimeter Defender Schnittstelle können Sie beispielsweise Geräte kalibrieren, Szenarien einrichten und Aktionen für mehrere Geräte ausführen. Die Remote-Einrichtung ermöglicht die Konfiguration von jedem Ort mit Netzwerk-Verbindung aus.



1 *Schnittstelleneinstellungen, on page 7*
2 *Handhabung von Geräten Siehe Geräte hinzufügen, on page 17.*
3 *Live-Ansicht, on page 8*
4 *CPU-Lastanzeige Siehe CPU-Last, on page 11.*
5 *Registerkarte „Anwendung", on page 9*
6 *Registerkarte „Installation", on page 10*
7 *Registerkarte „Kalibrierung", on page 10*
8 *Registerkarte „Szenarien", on page 10*
9 *Registerkarte „Ausgabe", on page 11*
10 *Registerkarte „Support", on page 11*

Schnittstelleneinstellungen

Das Menü „Schnittstelleneinstellungen" enthält:

Ordnereinstellungen –

Gerätekonfigurationspfad: Wählen Sie aus, wo temporäre Dateien und Kalibrierungsvideos gespeichert werden sollen.

Standortkonfigurationspfad: Wählen Sie aus, wo Konfigurationsdateien aus Ladepfaden gespeichert werden sollen.

Kamerakennwörter – Anzeige der verwendeten Kennwörter und Hinzufügen neuer Kennwörter. Kennwörter werden nicht gespeichert, sobald der Benutzer die Anwendung beendet hat.

Democlippakete verwalten – Importieren oder entfernen Sie Democlips.

Aktivieren des Vollbildmodus – Ändern Sie die Bildrate in der Live-Ansicht. Siehe *CPU-Last, on page 11*.

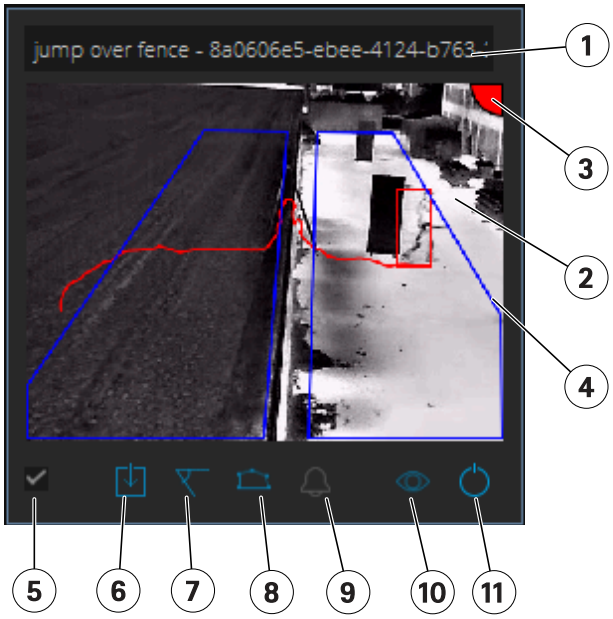
Anzeige von Fuß und Zoll – Wechseln zwischen metrischen und imperialen Einheiten

Sprache ändern – Ändern Sie die Sprache in der Anwendung.

Info – Anzeige der Version des AXIS Perimeter Defender Setups.

Live-Ansicht

Jedes angeschlossene Gerät erhält eine Live-Ansicht in der Hauptschnittstelle. Die Live-Ansicht bietet den Gerätestatus und schnellen Zugriff auf die Hauptfunktionen.



1. Gerätename – Klicken Sie hier, um den Gerätenamen zu bearbeiten. Er enthält immer die IP-Adresse und MAC-Nummer des Geräts. Zeigen Sie mit dem Mauszeiger auf den Namen, um das für die Analyse verwendete Seitenverhältnis anzuzeigen, das eine maximale Flächenabdeckung bietet, und um zu sehen, ob auf dem Gerät eine Remoteverbindung aktiv ist.

2. Live-Bild – Im Übersichtsmodus lautet die Bildrate 1 fps. Doppelklicken Sie, um das Bild zu maximierenund die Bildrate auf 8 fps zu erhöhen.

3. Alarmstatus – Der Alarmstatus ist nur sichtbar, wenn die Überlagerung aktiv ist und AXIS Perimeter Defender installiert und konfiguriert ist und ausgeführt wird. Grau bedeutet, dass die Alarmfunktion nicht aktiv ist oder dass die Konfigurationseinstellungen geladen werden. Grün bedeutet, dass die Alarmfunktion aktiv ist. Rot bedeutet, dass ein Alarm ausgelöst wurde.

4. Erfassungszonen – Die Erfassungszonen sind nur sichtbar, wenn die Überlagerung aktiv ist, AXIS Perimeter Defender installiert und konfiguriert ist und ausgeführt wird.

5. Auswahl-Kontrollkästchen – Um mehrere Geräte auswählen zu können, verwenden Sie dieses Kontrollkästchen.

6. Installationsstatus und Schnellzugriffstaste – Bewegen Sie den Mauszeiger, um die auf dem Gerät installierte Version von AXIS Perimeter Defender anzuzeigen. Wenn das Symbol durch ersetzt wird, bedeutet dies, dass eine neuere Version verfügbar ist. Klicken Sie hier, um die Registerkarte Installation für das Gerät zu öffnen. Grau bedeutet, dass das Gerät nicht installiert ist. Orange bedeutet, dass das Gerät installiert ist, aber nicht über eine gültige Lizenz verfügt. Blau bedeutet, dass das Gerät mit einer gültigen Lizenz installiert ist.

7. Kalibrierungsstatus und Schnellzugriffstaste – Klicken Sie hier, um die Registerkarte Kalibrierung für das Gerät zu öffnen. Grau bedeutet, dass das Gerät nicht kalibriert ist. Blau bedeutet, dass das Gerät kalibriert ist.

8. Szenariostatus und Schnellzugriffstaste – Klicken Sie hier, um die Registerkarte Szenarios für das Gerät zu öffnen. Grau bedeutet, dass kein Szenario definiert ist. Blau bedeutet, dass mindestens ein Szenario definiert ist.

9. Ausgabestatus und Schnellzugriffstaste – Klicken Sie hier, um die Registerkarte Ausgabe für das Gerät zu öffnen. Grau bedeutet, dass keine Ausgänge konfiguriert sind. Blau bedeutet, dass mindestens eine Ausgabe konfiguriert ist.

10. Überlagerungsstatus und Umschalttaste – Klicken Sie hier, um die Überlagerung ein- und auszuschalten. Grau bedeutet, dass die Überlagerung inaktiv ist. Blau bedeutet, dass die Überlagerung aktiv ist. Die Überlagerung wird als Begrenzungsrahmen um erkannte Objekte sowie als „Schneckenpfad" dargestellt, der den Bewegungspfad von Objekten anzeigt.

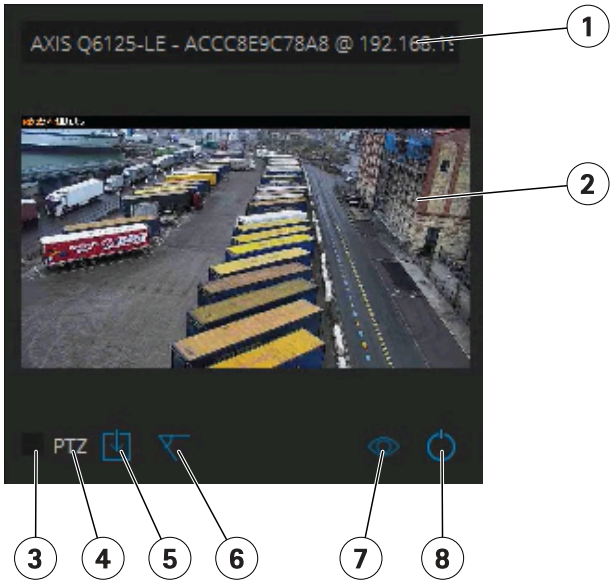
11. Ausführungsstatus und Umschalttaste – Klicken Sie hier, um die Anwendung auf dem Gerät auszuführen/zu stoppen. Grau bedeutet, dass die Anwendung angehalten wird. Blau bedeutet, dass sie ausgeführt wird.

Hinweis

Überlagerung ist nur verfügbar, wenn eine direkte Verbindung zwischen Gerät und Computer des Benutzers verfügbar ist, d. h., wenn keine Firewalls oder Ähnliches die Verbindung mit dem Überlagerungsanschluss auf dem Gerät verhindern.

Live-Ansicht – PTZ-Autotracking

Die Live-Ansicht von Geräten, auf denen AXIS Perimeter Defender PTZ-Autotracking installiert ist, unterscheidet sich leicht von der normalen Live-Ansicht.



1 *Gerätename*
2 *Live-Bild*
3 *Auswahl-Kontrollkästchen*
4 *Gibt an, dass das Gerät AXIS Perimeter Defender PTZ-Autotracking verwendet.*
5 *Installationsstatus und Schnellzugriffstaste*
6 *Kalibrierungsstatus und Schnellzugriffstaste*
7 *Überlagerungsstatus und Umschalttaste*
8 *Ausführungsstatus und Umschalttaste*

Registerkarte „Anwendung"

- **Ausführen** – Startet die Analyse auf dem/den ausgewählten Gerät(en).
- **Anhalten** – Hält die Analyse auf dem/den ausgewählten Gerät(en) an.
- **Standort laden** – Lädt einen zuvor gespeicherten Standort, d. h. Geräte und die dazugehörigen Konfigurationsdateien
- **Standort speichern** – Speichert den aktuellen Standort, d. h. speichert alle Geräteinformationen und die dazugehörigen Konfigurationsdateien

- **Overlay-Synchronisierung** – Steuerung AXIS Perimeter Defender Metadaten-Overlay-Synchronisierung. Mit diesem Schieberegler wird die Verzögerung zwischen den Metadaten-Overlays und den empfangenen Bildern gesteuert, um das Streaming im Vergleich zu Metadaten auszugleichen. Der Schiebereglerwert gibt die Verzögerung an, die für die aktuelle ausgewählte Kamera eingestellt wurde. Wenn mehrere Kameras angeschlossen sind, entspricht der angezeigte Wert der ersten ausgewählten Kamera. Das Ändern des Schiebereglerwerts ändert die Verzögerung aller ausgewählten Kameras.

Sie können auch die Anzahl der hinzugefügten kompatiblen Geräte, die Gesamtanzahl der Geräte mit AXIS Perimeter Defender und die Anzahl der Geräte anzeigen, auf denen die Analyse ausgeführt wird.

Registerkarte „Installation"

- **Application: Install (Anwendung: Installieren)** – Anwendung auf den ausgewählten Geräten installieren.
- **Application: Uninstall (Anwendung: deinstallieren)** – Anwendung auf den ausgewählten Geräten deinstallieren.
- **Licence: Install (Lizenz: Installieren)** – Lizenz auf den ausgewählten Geräten installieren.

Registerkarte „Kalibrierung"

- **Automatisch** – führt eine automatische Kalibrierung der ausgewählten Geräte durch.
- **Manual** (manuell) – manuelle Kalibrierung der ausgewählten Geräte durchführen.

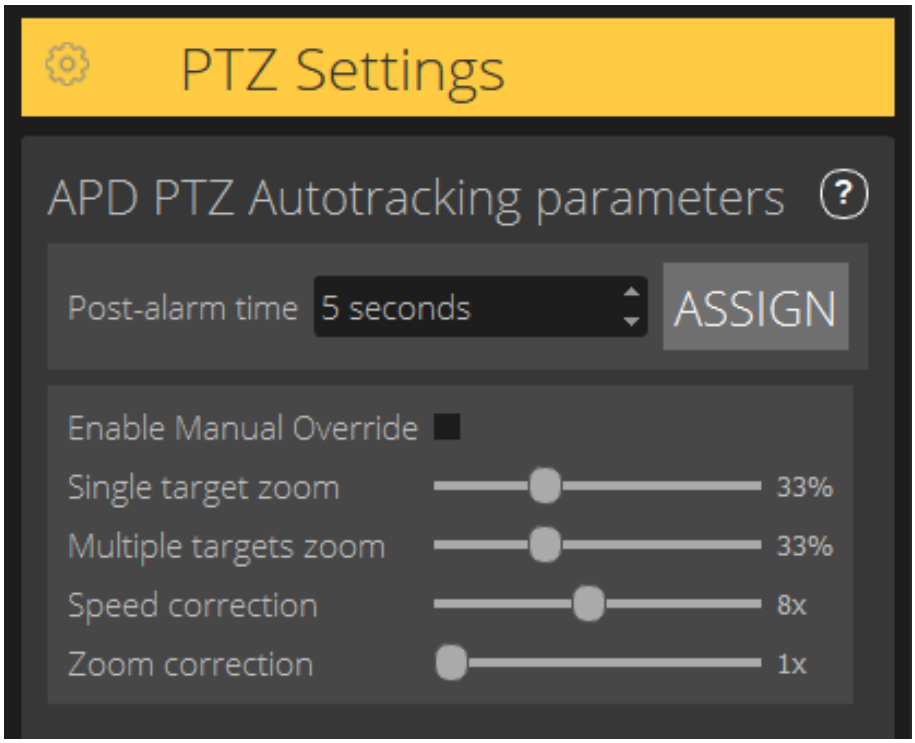
Registerkarte „Szenarien"

- **Globale Parameter** – gelten für alle Szenarien.
- **Erweiterte Szenarien** – erstellt Szenarios für das Eindringen, längere Verweilen, den Zonenübergang und Bedingungen.

Registerkarte „PTZ-Einstellungen"

Hinweis

Diese Registerkarte wird nur angezeigt, wenn Sie über das Plugin AXIS Perimeter Defender PTZ-Autotracking verfügen.



- **Zeit nach dem Alarm** – legen Sie die Zeit fest, nach der die PTZ-Kamera in die Ausgangsposition zurückkehrt, nachdem das nachverfolgte Objekt aus der Ansicht ausgeblendet wird.
- **Manuelle Übersteuerung aktivieren** – Wenn diese Option aktiviert ist, kann der Bediener die PTZ-Kamera mit einem Joystick, im VMS oder auf der Webseite der Kamera steuern.
- **Einzelziel-Zoom** – Passen Sie die Zoomstufe zur Verfolgung eines einzelnen Ziels an. Ein höherer Wert gibt bessere Identifizierungsmöglichkeiten, erhöht jedoch auch die Gefahr, sich schnell bewegende Objekte zu verlieren.
- **Zoom für mehrere Ziele** – Passt die Zoomstufe für mehrere Nachverfolgungsziele an.
- **Geschwindigkeitskorrektur** – Passt die Nachverfolgungsgeschwindigkeit an, damit sich schnell bewegende Objekte im PTZ-Kamerabild zentriert bleiben. Beachten Sie, dass ein hoher Wert zur Unbeständigkeit der Nachverfolgung führen kann.
- **Zoom-Korrektur** – Bei einem höheren Wert wird das Herauszoomen für Objekte erhöht, die sich in der Nähe des Rands des Sichtfelds der PTZ-Kamera befinden.

Registerkarte „Ausgabe"

- **Konfigurieren** – öffnet die Webseite des Geräts, um Alarme zu erstellen und zu konfigurieren.
- **Alarm testen** – testet den für das Gerät konfigurierten Alarm.
- **Post-alarm time: Assign (Nachalarmzeit: zuweisen)** – Einstellen der Nachalarmzeit.

Registerkarte „Support"

- **Laden** – lädt die gesicherte Konfiguration für die ausgewählten Geräte. Dies ist besonders nützlich, um nach einem Geräteausfall oder einer versehentlichen Deinstallation ein Gerät wiederherzustellen. Die Konfiguration umfasst:

– Lizenz
– Parameter
– Kalibrierung und Szenarien
– Kalibrierungsvideo

- **Speichern** – erstellt eine Sicherungskopie der Konfiguration der ausgewählten Geräte.
- **Löschen** – löscht die Kalibrierung und die Szenarios der ausgewählten Geräte. Dies ist nützlich, wenn sich die Kameras bewegt haben, da Kalibrierungs- und Erfassungszonen dann nicht mehr gültig sind.
- **Anwendungsprotokoll anzeigen** – Zeigen Sie das interne Protokoll von AXIS Perimeter Defender an.
- **Supportprotokoll exportieren** – generiert eine Support-Datei mit detaillierten Informationen. Beziehen Sie diese Datei immer in eine Supportanfrage ein.

CPU-Last

Die CPU-Auslastungsanzeige gibt die aktuelle CPU-Auslastung des Computers in Echtzeit an. Eine zu hohe CPU-Auslastung kann das Einfrieren eines Computers oder einer Anwendung zur Folge haben. Schließen Sie andere Anwendungen, während Sie AXIS Perimeter Defender Setup verwenden, um Ihre CPU-Zuweisung zu maximieren. Wenn die CPU-Auslastung zu hoch ist und Sie versuchen, ein Gerät hinzuzufügen, wird eine Warnung ausgegeben.

Jedes hinzugefügte Gerät beansprucht CPU-Ressourcen des Host-Computers, wenn es den Videostream dekodiert und anzeigt. Um die Auswirkungen auf den Host-Computer zu begrenzen, werden die Videostreams von hinzugefügten Geräten standardmäßig mit einer reduzierten Bildrate angezeigt (ca. 1 fps. Die normale Bildrate (ca 8 fps wird beim Maximieren von Streams oder während des Kalibrierungsvorgangs wiederhergestellt.

Wichtig

Die Option **Enable full frame rate mode** (Vollbildmodus aktivieren) kann zu einer nicht reagierenden Schnittstelle führen, wenn Sie eine Verbindung zu einer großen Anzahl von Kameras herstellen oder einen Computer mit niedrigem Stromverbrauch verwenden.

Demo von AXIS Perimeter Defender anzeigen

Für Demo Zwecke sind bei AXIS Perimeter Defender und AXIS Perimeter Defender PTZ Autotracking bereits einige Demo-Clips vorinstalliert, die zur Veranschaulichung der Analyse verwendet werden können, ohne dass eine aktive, installierte Kamera vorhanden sein muss. Die Demo-Clips zeigen die Art der Erfassungs- und Autotracking-Ergebnisse an, die in unterschiedlichen Umgebungen zu erwarten sind.

1. Navigieren Sie zu **Anwendung > Hinzufügen > Demo-Clips** und nehmen Sie einen der folgenden Schritte vor:
   - Filtern Sie die Demo-Clips nach ihrem Typ.
   - Wählen Sie mindestens einen Demo-Clip aus.
2. Um die Demo-Clips hinzuzufügen, klicken Sie auf **Ausgewählte Demo-Clips hinzufügen**.

Nach dem Hinzufügen werden die Demo-Clips als Standard-Videostreams auf der Benutzeroberfläche angezeigt. Die Kalibrierung ist verfügbar und die Analyse bereits aktiviert, sodass der Benutzer die Analyse- und Autotracking-Ergebnisse direkt in dem Videostream sehen kann. Die Analyse und das Autotracking können beendet oder gestartet werden, indem Sie auf den Ausführungsstatus in der Live-Ansicht oder auf die **Ausführen**- oder **Beenden**-Schaltfläche im linken Bereich klicken.

Die Kalibrierung und Kopplung können geändert und erneut durchgeführt werden. Ebenso können Erfassungsszenarien hinzugefügt, entfernt und geändert werden.

Auf der **Support**-Registerkarte auf der linken Seite befindet sich eine **Löschen**-Schaltfläche, mit der Sie die Kalibrierung und die Szenarios auf die ursprünglichen Werte zurücksetzen können. Die Kalibrierung kann nicht vollständig entfernt werden.

Funktionsweise

Der Installationsvorgang für AXIS Perimeter Defender und AXIS Perimeter Defender PTZ-Autotracking unterscheidet sich leicht.

Erste Schritte mit AXIS Perimeter Defender

Sie müssen die folgenden Schritte durchführen, um Ihren Standort mit AXIS Perimeter Defender einzurichten:

1. Montieren Sie die Kamera. Siehe *Montieren der Kamera, on page 13*.
2. Laden Sie die Software herunter und installieren Sie sie auf Ihrem Computer. Siehe *Installation der Software auf Computer, on page 16*.
3. Schließen Sie Ihre Geräte an. Siehe *Geräte hinzufügen, on page 17*.
4. Installieren Sie AXIS Perimeter Defender auf jedem Gerät. Siehe *Installieren von Software auf Geräten, on page 18*.

Hinweis

Geräte, die nur im KI-Modus ausgeführt werden, müssen nicht kalibriert werden. Wenn Geräte gleichzeitig im Kalibrierungsmodus und im KI-Modus ausgeführt werden sollen, müssen Sie sie kalibrieren.

5. Kalibrieren Sie die Geräte. Siehe *Kalibrieren – AXIS Perimeter Defender, on page 19*.
6. Definieren Sie die Regeln für das Auslösen von Alarmen, indem Sie Szenarios hinzufügen. Siehe *Szenarien definieren, on page 26*.
7. Richten Sie die zu sendenden Alarme ein. Siehe *Ausgänge definieren, on page 31*.

Erste Schritte mit AXIS Perimeter Defender PTZ-Autotracking

Sie müssen die folgenden Schritte durchführen, um Ihren Standort mit AXIS Perimeter Defender PTZ Autotracking einzurichten:

1. Montieren Sie die Kameras. Siehe *Montieren der Kamera, on page 13* und *Montieren der PTZ-Kamera, on page 16*.
2. Laden Sie die Software herunter und installieren Sie sie auf Ihrem Computer. Siehe *Installation der Software auf Computer, on page 16*.
3. Schließen Sie Ihre Geräte an. Siehe *Geräte hinzufügen, on page 17*.
4. Installieren Sie AXIS Perimeter Defender Version 2.5.0 oder höher auf der festen Kamera, und AXIS Perimeter Defender PTZ Autotracking auf der PTZ-Kamera. Siehe *Installieren von Software auf Geräten, on page 18*.
5. Kalibrieren Sie die Geräte und Szenarien. Siehe *Kalibrierung – PTZ-Autotracking, on page 26*.
6. Koppeln Sie die Geräte. Siehe *Koppeln der Kameras – PTZ-Autotracking, on page 29*.
7. Richten Sie die zu sendenden Alarme ein. Siehe *Ausgänge definieren, on page 31*.

Montieren der Kamera

Infos über das Design-Tool

Zur Kameraplatzierung vor Ort empfehlen wir das Design-Tool für AXIS Perimeter Defender. Es berücksichtigt sowohl die Anforderungen der Axis Kameras als auch die Anforderungen von AXIS Perimeter Defender. Dieses können Sie auch für doppelte Installationen verwenden, d. h. wenn Sie zwei Kameras kombinieren. Das Tool hilft Ihnen bei der Entscheidung:

- Montagehöhe der Kamera
- Neigungswinkel
- Minimale Erfassungsdistanz

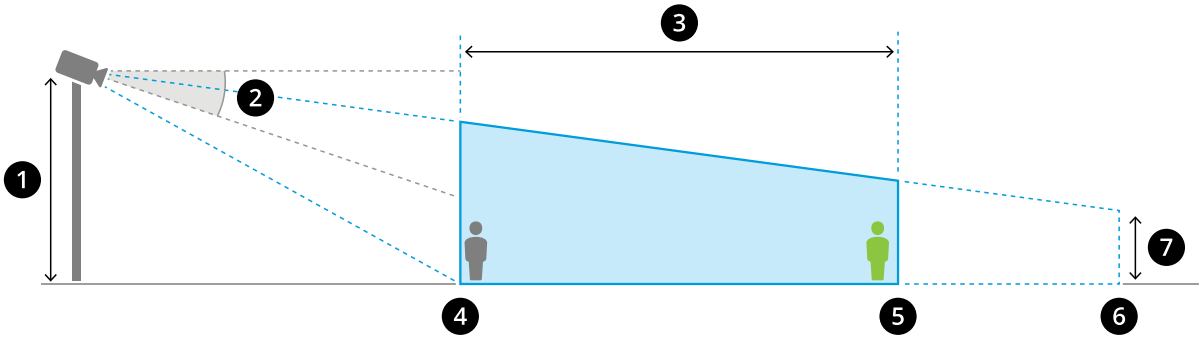
- Maximale Erfassungsdistanz

Um das Tool herunterzuladen, navigieren Sie zu *axis.com/products/axis-perimeter-Defender*

Empfehlungen für die Installation der Kamera

Hinweis

Für Kameras, die nur im KI-Modus betrieben werden, finden Sie Empfehlungen für die Installation der Kamera in der Anwendung.



Eine entsprechend montierte Kamera.

1 *Montagehöhe*
2 *Neigung*
3 *Überwachungsbereich*
4 *Minimale Erfassungsdistanz*
5 *Maximale Erfassungsdistanz*
6 *Sichtfeld-Abstand*
7 *Höhe des Sichtfelds*

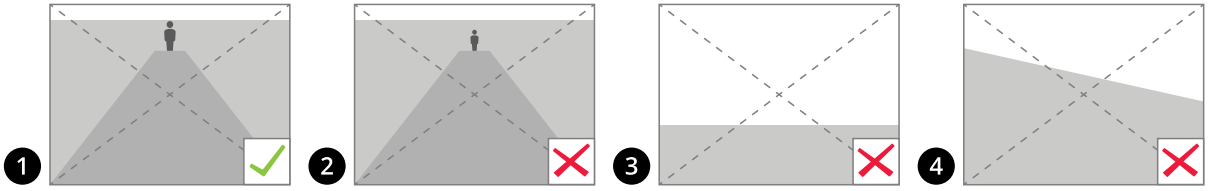
Objekthöhe bei maximalem Erfassungsabstand – Damit eine stehende Person im maximalen Erfassungsabstand erkannt werden kann, muss die Pixelhöhe mindestens 5 % der gesamten Bildhöhe betragen (3,5 % für Wärmebildkameras). Wenn die Höhe des visualisierten Bildes beispielsweise 576 Pixel beträgt, muss die Höhe einer Person, die am Ende der Erfassungszone steht, mindestens 28 Pixel (20 Pixel für Wärmebilder) betragen.

Objekthöhe bei minimalem Erfassungsabstand – Damit eine stehende Person im minimalen Erfassungsabstand erkannt wird, darf die Pixelhöhe nicht mehr als 60 % der gesamten Bildhöhe betragen.

Höhe des Objekts im KI-Modus – Wenn Sie die Anwendung im KI-Modus ausführen, müssen die Objekte mindestens so groß sein wie der zu erfassende Avatar.

Neigungswinkel – Die Kamera muss in Richtung Boden ausgerichtet sein, so dass sich die Bildmitte unter dem Horizont befindet. Montieren Sie die Kamera so, dass der minimale Erfassungsabstand höher ist als die Hälfte der Montagehöhe der Kamera (Mindesterfassungsabstand > Kameramontagehöhe / 2).

Drehwinkel – Der Drehwinkel der Kamera muss nahezu Null sein.



1 *Objekthöhe, Neigungswinkel und Rollwinkel sind geeignet.*
2 *Die Objekthöhe bei maximalem Erfassungsabstand beträgt weniger als 5 % der Bildhöhe (3,5 % bei Wärmebildkameras).*
3 *Die Bildmitte befindet sich über der Horizontlinie.*
4 *Der Rollwinkel der Kamera ist nicht nahezu gleich Null.*

Der maximale Erfassungsabstand hängt von folgenden Faktoren ab:

- Kameratyp und -modell
- Objektiv Eine höhere Brennweite ermöglicht einen höheren Erfassungsabstand.
- Die minimale Pixelgröße, die ein Mensch im zu erfassenden Bild abdecken muss. Die Pixelhöhe einer stehenden Person muss mindestens 5 % der Bildhöhe für visuelle Kameras und 3,5 % für Wärmebildkameras betragen.
- Wetter
- Beleuchtung:
- Kameralast

Beachten Sie beim Befestigen der Kamera Folgendes:

- Die Anwendung toleriert kleine Kameravibrationen, aber Sie erhalten die beste Leistung, wenn die Kamera keinen Vibrationen ausgesetzt ist.
- Das Sichtfeld der Kamera muss fixiert werden.

Montagehöhe

Um einen bestimmten Erfassungsabstand zu erreichen, ist zusätzlich zur erforderlichen Pixelgröße die Kamera außerdem in einer Mindesthöhe angebracht sein. Wenn die anderen Anforderungen, insbesondere der Neigungswinkel, erfüllt sind, gibt es keine maximale Montagehöhe.

Erforderlicher Erfassungsabstand	Mindestmontagehöhe der Kamera
20 m	2,5 m (niedrigste zulässige Höhe)
100 m	3 m
200 m	4 m (13 ft)
300 m	5 m
500 m	6 m

Szene-Anforderungen

Hinweis

Für Kameras, die nur im KI-Modus betrieben werden, finden Sie Szenenvoraussetzungen in der Anwendung.

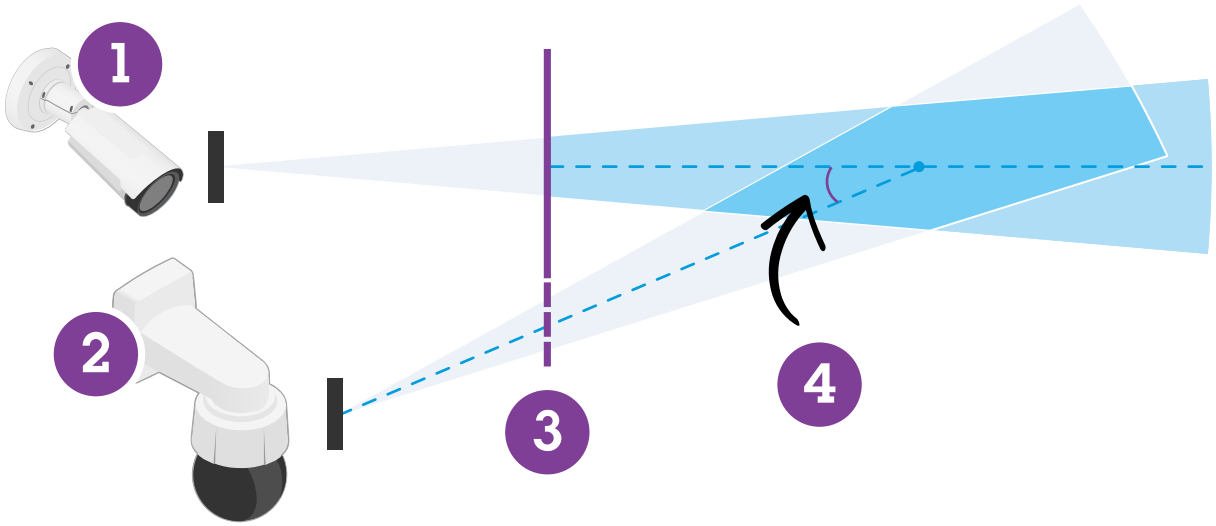
Die Erfassungszone muss folgende Bedingungen erfüllen:

- Freie Sicht
- Der Boden muss eben oder mit nur geringer Neigung sein
- Licht löst nicht durch Bewegung aus
- Freie Sicht
- Bei visuellen Kameras müssen die Beleuchtungsstärke und die Bildeinstellungen ausreichend sein, um einen ausreichenden Kontrast zwischen Menschen und Fahrzeugen und dem Hintergrund zu gewährleisten.
  - Wenn Sie eine Tag- und Nacht-Kamera von Axis mit künstlicher Beleuchtung verwenden, werden in der gesamten Erfassungszone mindestens 50 Lux empfohlen.
  - Wenn Sie externe IR-Spots verwenden, wird ein maximaler Erfassungsabstand von 80 m empfohlen und der Bereich der IR-Spots muss mehr als doppelt so groß sein wie der maximale Erfassungsabstand.
  - Bei Verwendung der integrierten IR-Beleuchtung ist der maximale Erfassungsabstand je nach Kamera und Umgebung auf max. 20 m begrenzt.
- Bei Wärmebildkameras muss ein hoher Kontrast zwischen Hintergrund und Vordergrund vorhanden sein

Um die Erfassungssleistung zu optimieren, ermittelt AXIS Perimeter Defender automatisch den Unterschied zwischen Tag und Nacht und verwendet diese Informationen, um die Erfassungsalgorithmen zu optimieren. Die Feineinstellung dauert etwa 24 Stunden, d. h. die optimale Erfassung bei Tag und Nacht wird nach dem Ausführen der Anwendung für diese Zeit erreicht.

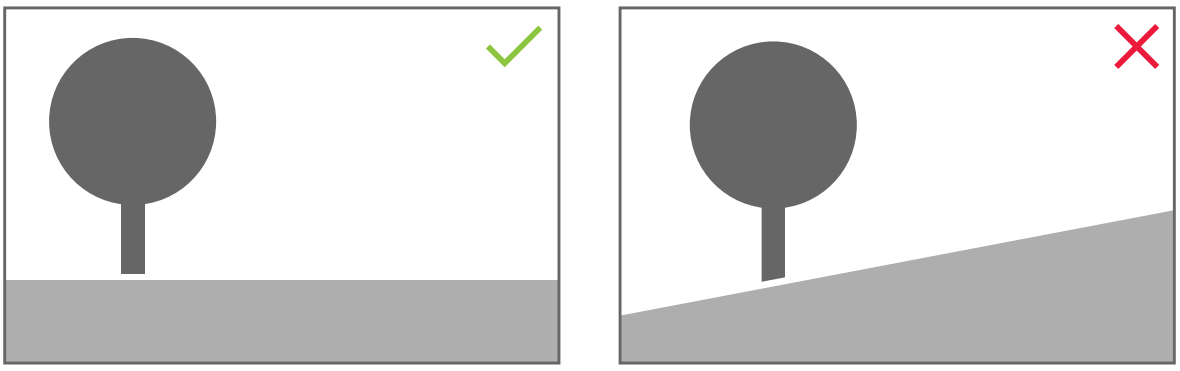
Montieren der PTZ-Kamera

In diesem Kapitel wird beschrieben, wie die PTZ-Kamera in Bezug auf die unbewegliche Kamera montiert werden muss. Anweisungen zur Montage der festen Kamera finden Sie unter *Montieren der Kamera, on page 13*.



1 *Unbewegliche Netzwerk-Kamera*
2 *PTZ-Netzwerk-Kamera*
3 *Minimale Erfassungsdistanz*
4 *Winkel zwischen den Kameras*

- Die voreingestellte Ausgangsposition der PTZ-Kamera muss mehr als 60 % der Erfassungszone der festen Kamera abdecken.
- Um von der PTZ-Kamera nachverfolgt zu werden, muss eine stehende Person mehr als 4 % der Bildhöhe der PTZ-Kamera abdecken.
- Die PTZ-Kamera muss vor dem Mindesterfassungsabstand der festen Kamera (C) platziert werden.
- Der Winkel zwischen der festen Kamera und der PTZ-Kamera muss kleiner als 30° (D) sein.



- Der Boden muss flach sein.

Installation der Software auf Computer

Kameras, auf denen AXIS Perimeter Defender läuft, müssen über HTTP von dem Computer aus erreichbar sein, auf dem die AXIS Perimeter Defender Setup-Schnittstelle läuft.

AXIS Perimeter Defender Setup-Schnittstelle (nur während der Setup-Phase erforderlich) erfordert:

- Intel® CoreTM 2 Duo-Prozessor oder besser
- Unterstützung für Open GL
- Mindestens 16 GB RAM
- Windows® 10, Windows® 11 oder Win Server 2022
- Bildschirmauflösung mindestens 1024 x 768

Bitte beachten Sie, dass ein einzelner Computer nur eine begrenzte Anzahl von Kameras verwalten kann. Für einen Rechner mit einem Intel® CoreTM i5-1135G7 Prozessor der 11. Generation mit 2,40 GHz wird beispielsweise empfohlen, maximal 10 Kameras hinzuzufügen und maximal 5 Kameras gleichzeitig automatisch zu kalibrieren.

Hinweis

Die Ausführung der AXIS Perimeter Defender Setup-Schnittstelle auf einem virtuellen Rechner wird nicht unterstützt.

1. Laden Sie die AXIS Perimeter Defender Software von *axis.com/products/axis-perimeter-Defender herunter*
2. Installieren Sie die Software auf Ihrem Computer.

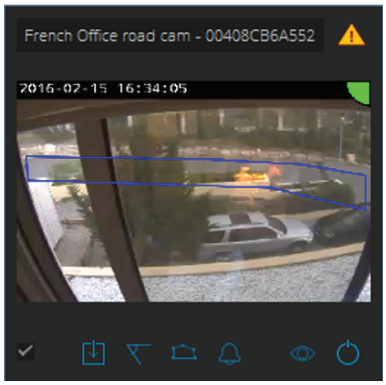
Geräte hinzufügen

Sie können der AXIS Perimeter Defender-Anwendung Geräte auf drei verschiedene Arten hinzufügen:

- Automatisch über einen Netzwerk-Scan Siehe *Automatisches Hinzufügen von Geräten, on page 18*.
- Manuell durch Angabe von Verbindungseinstellungen Siehe *Geräte manuell hinzufügen, on page 18*.
- Automatisch durch Laden eines zuvor gespeicherten Standorts. Siehe *Laden eines vorhandenen Standorts, on page 18*.

Wenn Sie ein Gerät hinzugefügt haben, wird eine Liste aller anderen auf dem Gerät installierten Anwendungen angezeigt. Es wird empfohlen, alle nicht erforderlichen Anwendungen zu beenden, da Sie die CPU-Ressourcen der Kamera verwenden, die sich auf die Leistung von AXIS Perimeter Defender auswirken und die korrekte Installation verhindern können.

Wenn ein Gerät nicht über genügend CPU-Ressourcen verfügt, z. B. weil andere Anwendungen ausgeführt werden, verringert AXIS Perimeter Defender die Bildrate. Wenn die Bildrate unter 5 Bildern pro Sekunde liegt, wird in der Live-Ansicht neben dem Gerätenamen ein gelbes Warndreieck angezeigt. Wenn Sie das Dreieck bewegen, wird die aktuelle Bildrate angezeigt.



Hinweis

Eine Bildrate unter 5 fps kann die Videoanalyseleistung deutlich verringern. Dies kann zu fehlenden und falschen Erfassungen führen.

Weitere Informationen finden Sie unter *CPU-Last, on page 11*.

Automatisches Hinzufügen von Geräten

Wichtig

Die Suchfunktion funktioniert nicht netzwerkübergreifend, d. h. AXIS Perimeter Defender Setup kann nur Geräte finden, die mit demselben Subnetzwerk verbunden sind wie der Client, auf dem die Software ausgeführt wird. Um Geräte hinzuzufügen, die mit einem anderen Unternetzwerk verbunden sind, fügen Sie sie manuell hinzu. Die Suchfunktion kann auch fehlschlagen, wenn die Netzwerkrouter oder Switches so konfiguriert sind, dass Multicast gefiltert wird.

1. Um das umgebende Netzwerk nach Geräten zu durchsuchen, navigieren Sie zu **Anwendung** und klicken Sie auf **Suchen**.
   Wenn Sie zum ersten Mal suchen und keine Kennwörter verfügbar sind, wird ein Kennwort-Dialogfeld geöffnet. Andernfalls wird das verfügbare Kennwort verwendet, um eine Verbindung mit den Geräten herzustellen.
2. Wählen Sie Geräte aus und klicken Sie dann auf **Ausgewählte Geräte hinzufügen**.
   Wenn das Kennwort korrekt ist, wird ein statisches Bild angezeigt, das den Benutzer bei der Auswahl der Geräte unterstützt.

Geräte manuell hinzufügen

1. Navigieren Sie zu **Anwendung** und klicken Sie dann auf **Hinzufügen**.
2. Geben Sie Folgendes ein:

- Die IP-Adresse oder den Hostnamen des Geräts
- Das Root-Kennwort des Geräts, da für AXIS Perimeter Defender ein Root-Zugriff erforderlich ist.
- Der HTTP-Port, der zum Herstellen einer Verbindung verwendet wird. Der Standardport ist 80.
- Ein optionaler Name für das Gerät für eine einfachere Erkennung
- Wenn sich das Gerät in einem Remotenetzwerk befindet, für das die Verbindung langsam sein kann, aktivieren Sie das Kontrollkästchen **Gerät im Remotenetzwerk**. Langsame Verbindungen, die nicht als Remote konfiguriert sind, können zu nicht funktionierenden oder fehlerhaften Kalibrierungen führen.

Hinweis

Für Fernverbindungen muss der Benutzer über HTTP eine Verbindung zum Gerät herstellen können. Achten Sie darauf, den HTTP-Port korrekt einzurichten. Die Remotekonfiguration kann fehlschlagen, wenn die Verbindung nicht über eine ausreichende oder stabile Bandbreite verfügt.

3. Klicken Sie auf **OK**.

Hinweis

Wenn es nicht funktioniert, eine Kamera anhand des Hostnamens hinzuzufügen, überprüfen Sie die Netzwerk- und DNS-Einstellungen oder fügen Sie das Gerät mithilfe der IP-Adresse hinzu.

Laden eines vorhandenen Standorts

So laden Sie eine zuvor gespeicherte Standortkonfiguration:

1. Navigieren Sie zu **Anwendung** und klicken Sie dann auf **Standort laden**.
2. Navigieren Sie zur Auswahl der Standortkonfiguration und klicken Sie auf **Öffnen**. Die Live-Ansicht wird automatisch angezeigt.

Installieren von Software auf Geräten

Sie müssen AXIS Perimeter Defender auf jedem Gerät installieren.

Wenn Sie überprüfen möchten, welche Version von AXIS Perimeter Defender auf einem Gerät installiert ist, können Sie die Maus in der Live-Ansicht über den **Installationsstatus** bewegen.

Wenn auf einem Gerät AXIS Perimeter Defender nicht installiert ist, sind alle Symbole in der Live-Ansicht ausgegraut.

Installieren der Software auf einem Gerät

1. Navigieren Sie zur **Installation**.
2. Wählen Sie die Geräte aus, auf denen Sie die Anwendung installieren möchten.
3. Wählen Sie die neueste verfügbare Version von AXIS Perimeter Defender und klicken Sie auf **Installieren**. AXIS Perimeter Defender wird jetzt auf den ausgewählten Geräten installiert und startet automatisch.
4. Suchen Sie nach einer Lizenz und führen Sie eine der folgenden Aktionen aus:

– Bei Installation auf einem einzelnen Gerät: Wählen Sie die Lizenzdatei für das Gerät aus.

– Bei Installation auf mehreren Geräten: Wählen Sie den Ordner, in dem die Lizenzdateien gespeichert sind.

5. **Installieren** anklicken.

Kalibrieren – AXIS Perimeter Defender

Kalibrierung

Hinweis

Geräte, die nur im KI-Modus ausgeführt werden, müssen nicht kalibriert werden. Wenn Geräte gleichzeitig im Kalibrierungsmodus und im KI-Modus ausgeführt werden sollen, müssen Sie sie kalibrieren.

Damit AXIS Perimeter Defender die Szene korrekt interpretiert, müssen alle Geräte kalibriert werden. Bei der Kalibrierung werden Referenzpunkte eingeführt, die für den Prozessor Tiefen- und Höheninformationen bereitstellen. Sie definieren auch die gewünschte Zone.

Die Kalibrierung besteht aus zwei Aufgaben:

1. Kalibrierung durchführen:
   - Automatisch – wird in den meisten Fällen empfohlen. Siehe *Automatische Kalibrierung durchführen, on page 20*.
   - Manuell – wird empfohlen, wenn die automatische Kalibrierung für die Feineinstellung auf einer Kamera fehlschlägt oder es unpraktikabel wäre, die Szene vollständig durchzugehen oder es Objekte mit einer bekannten Höhe in der Szene gibt. Ein Beispiel hierfür ist ein entferntes Grundstück mit einer Umzäunungslinie, die aus einer Reihe von gleichmäßig platzierten Zaunpfosten mit gleich bleibender Höhe besteht. Siehe *Durchführen einer manuellen Kalibrierung, on page 24*.
2. Überprüfen Sie die Kalibrierungsergebnisse. Siehe *Überprüfen der Kalibrierungsqualität , on page 21*.

Um die Konfiguration eines großen Standorts zu beschleunigen, können mehrere Geräte gleichzeitig kalibriert werden. Sie können die Kalibrierung automatisch oder manuell durchführen, genau wie bei einer einzelnen Kamera. Beachten Sie vor der gleichzeitigen Kalibrierung mehrerer Geräte Folgendes:

- Die maximale Anzahl von Geräten, die Sie gleichzeitig installieren und konfigurieren können, hängt von der CPU-Leistung und dem auf dem Computer verfügbaren Speicherplatz ab. Zu viele Geräte im AXIS Perimeter Defender Setup können Abstürze verursachen. Wenn die Warnung zur CPU-Überlastung angezeigt wird, installieren und konfigurieren Sie einen Teil der Geräte mit der Funktion „Standort speichern".
- Die automatische Kalibrierung mehrerer Geräte erfordert mehr CPU-Ressourcen und RAM als ein einzelnes Gerät. Bei Systemen mit wenig Spezifikation kann dies dazu führen, dass der Computer einige Zeit nicht mehr reagiert oder die Anwendung abstürzt. Im Fall eines Absturzes sind die erfassten Videos weiterhin für die Kalibrierung der Einzelkamera verfügbar.

Hinweis

- AXIS Perimeter Defender unterstützt unterschiedliche Bildseitenverhältnisse gemäß der maximalen Auflösung, die von der Kamera bereitgestellt wird. Daher müssen Sie alle bisherigen Kalibrierungen

wiederholen, wenn Sie die Auflösung ändern. Wenn Sie jedoch die Auflösung des Videostreams auf der Webseite der Kamera ändern, müssen Sie die Kalibrierung nicht erneut vornehmen.

- Es wird empfohlen, das gleiche Bildseitenverhältnis in AXIS Perimeter Defender und im VMS zu verwenden, um sicherzustellen, dass die angezeigten Informationen zum Bildinhalt passen. Bewegen Sie den Kameranamen in der Live-Ansicht, um das Seitenverhältnis zu ermitteln.
- Wenn sich eine Kamera nach der Kalibrierung bewegt, müssen Sie sie erneut kalibrieren, damit die Analyseergebnisse korrekt sind.

Automatische Kalibrierung durchführen

Mit der automatischen Kalibrierung können Sie eine oder mehrere Kameras kalibrieren, indem Sie eine Person durch die Überwachungsszene laufen lassen. Die Kamera erfasst automatisch die für die Kalibrierung erforderlichen Informationen.

Für eine erfolgreiche automatische Kalibrierung:

- Kalibrieren Sie diese Option nicht, wenn viele Personen im Sichtfeld sind.
- Kalibrieren Sie diese Option nicht, wenn viele Fahrzeuge im Sichtfeld sind.
- Kalibrieren Sie diese Option nicht, wenn sich andere Objekte im Sichtfeld bewegen. Beispielsweise Bäume oder Fahnen, die sich im Wind bewegen.
- Kalibrieren Sie keine Kamera, die nicht parallel zum Boden installiert wurde.
- Die Person, die durch die Szene geht, muss das gesamte Sichtfeld von vorn nach hinten abdecken können. Ist dies nicht möglich, wechseln Sie besser auf manuelle Kalibrierung.
- Wenn sich die Kamera in einem Remote-Netzwerk befindet, jedoch nicht als Fernbedienung angeschlossen ist, muss die Person, die durch die Szene geht, etwa 5 Minuten lang laufen, um sicherzustellen, dass genügend Bilder erfasst werden. Dies liegt daran, dass die Bildrate bei Geräten in entfernten Netzwerken normalerweise geringer ist.

1. Navigieren Sie zu **Kalibrierung**.
2. Wählen Sie die zu kalibrierenden Geräte aus.
3. Klicken Sie auf **Automatisch**.
4. Legen Sie die Startzeit für die Aufzeichnung fest. Die Erfassung sollte mindestens 10 Sekunden, bevor die Person, die durch die Szene geht, das Sichtfeld betritt, beginnen.
5. Legen Sie die Aufzeichnungsdauer fest. Bedenken Sie, dass:
   - Die Person genügend Zeit haben muss, um durch die ganze Szene hindurch laufen zu können.
   - Die Länge des Videos wirkt sich auf die Kalibrierungsberechnung aus.
6. Geben Sie die Höhe (cm) der Person ein, die durch die Szene geht und klicken Sie dann auf **Aufnahme**. Um ein zuvor aufgenommenes Video wiederzuverwenden, klicken Sie auf **Vorherige Aufnahme verwenden**.
7. Lassen Sie die Person die Szene nach folgenden Anweisungen durchlaufen:
   - Bewegen Sie sich im Zickzackmuster, das eine größtmögliche Fläche der Erfassungszone der Szene von vorn nach hinten abdeckt. Wir empfehlen einen V-förmigen Weg über das Sichtfeld.
   - Bleiben Sie fast immer mit Ihrer ganzen Körpergröße im Sichtfeld.
   - Laufen Sie langsam in geraden Linien.
   - Behalten Sie die ganze Zeit eine aufrechte Position bei.
   - Pausieren Sie für 1-2 Sekunden, bevor Sie die Richtung ändern.

Ein Beispiel für eine Laufsequenz.

8. Stellen Sie sicher, dass die automatische Kalibrierung erfolgreich durchgeführt wurde, indem Sie bestätigen, dass die Person genau erkannt wird. Siehe *Überprüfen der Kalibrierungsqualität , on page 21*.
9. Um die Kalibrierung zu speichern, klicken Sie auf **Azkeptieren**.
   Klicken Sie auf **Neu**, um eine neue Kalibrierung durchzuführen.
   Klicken Sie auf **Manuell**, um eine manuelle Kalibrierung durchzuführen.

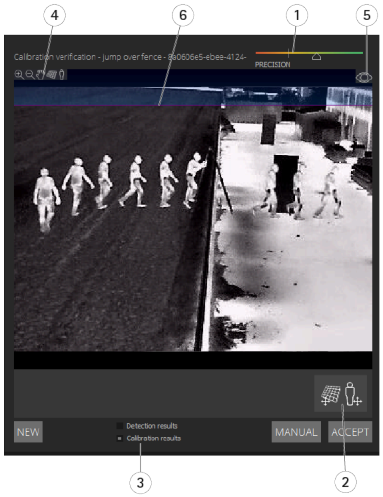
Wenn Sie die Kalibrierung übernommen haben, zeigen blaue Ränder die maximale Erfassungszone an. Die maximale Erfassungszone stellt den größten Bereich dar, der überwacht werden kann. Außerhalb dieses Bereichs können Eindringlinge möglicherweise erkannt werden, jedoch kann dafür keine Gewährleistung übernommen werden.

Überprüfen der Kalibrierungsqualität

Nach einer Kalibrierung sollte die Person angezeigt werden, die an verschiedenen Stellen durch die Szene gelaufen ist. Wenn die Person überhaupt nicht sichtbar ist, ist die automatische Kalibrierung fehlgeschlagen und muss erneut durchgeführt werden.

Es gibt mehrere Möglichkeiten, die Kalibrierungsqualität zu überprüfen:

- Überprüfen Sie die Kalibrierungsgenauigkeitsanzeige. Sie reflektiert eine automatisch berechnete Präzisionsstufe, die die Art und Weise erfasst, in der die Person die Szene erfasst hat. Wenn sich die Genauigkeitsanzeige in der roten Zone befindet, ist die Kalibrierung fehlgeschlagen und Sie können nicht auf **Akzeptieren** klicken. Siehe *Durchführen einer manuellen Kalibrierung, on page 24*.
- Sie können das Rastertool verwenden. Siehe *Überprüfen Sie die Kalibrierung mithilfe des Rasters., on page 22*.
- Sie können das Avatar-Tool verwenden. Siehe *Überprüfen Sie mit dem Avatar die Kalibrierung., on page 23*.
- Sie können die Erfassungsergebnisse überprüfen. Siehe *Überprüfen der Kalibrierung mithilfe der Erfassungsergebnisse, on page 23*.



1 *Kalibrierungsgenauigkeitsanzeige*
2 *Raster- und Avatar-Tools*
3 *Dynamische oder statische Ansicht*
4 *Anzeigemodifikatoren*
5 *Umschalten zwischen Kalibrierungsbild und Live-Ansicht*
6 *Horizontlinie*

Die Horizontlinie stellt das sichtbare Ende des Bodens in der Szene dar. Wenn Sie Szenarien definieren, ist es nicht möglich, Szenariobereiche in den blauen Bereich über der Horizontlinie zu platzieren, da dies über dem Boden liegt und die Szenariozonen per Definition auf dem Boden liegen.

Überprüfen Sie die Kalibrierung mithilfe des Rasters.

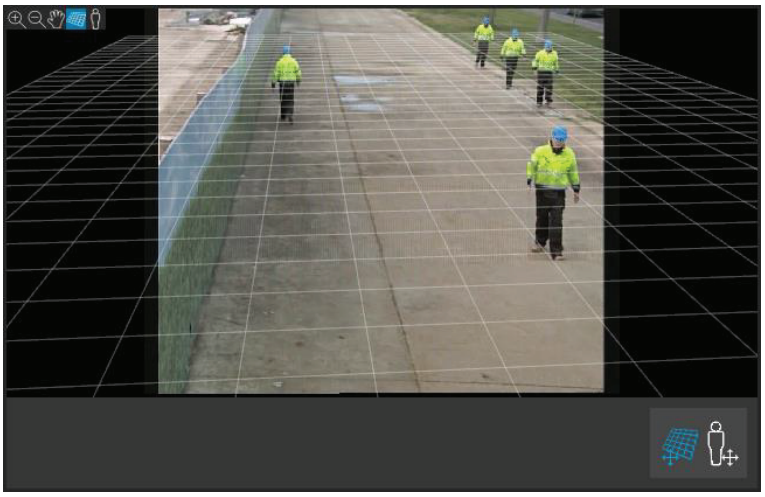
Das Raster sollte einem quadratischen Raster auf dem Boden entsprechen. Sie können die Anzeige des Rasters durch Klicken auf das Anzeigemodifikator-Symbol umstellen.

Wichtig

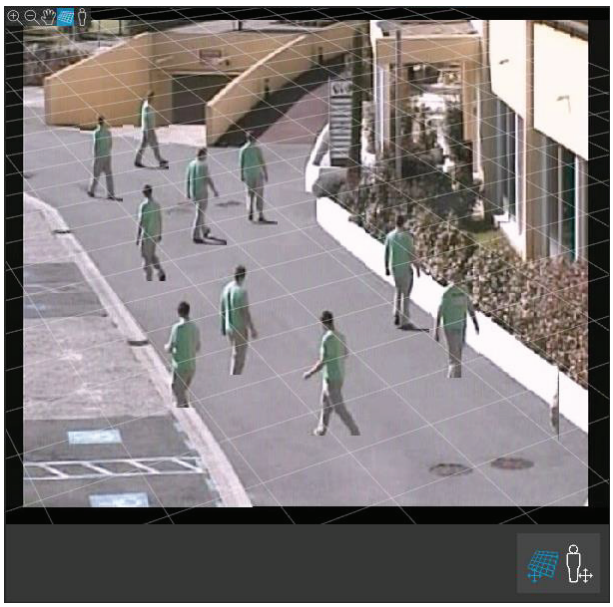
Das Raster wirkt sich nicht auf die Kalibrierung aus, es handelt sich dabei um ein Tool, mit dem sichergestellt wird, dass die Kalibrierung korrekt ist.

Sie können das Raster drehen, indem Sie es in den Vorschaubereich ziehen. Versuchen Sie, die Szene mit einer bestimmten Struktur auszurichten, um zu prüfen, ob das Ergebnis sinnvoll erscheint.

Wenn das Raster parallel zum Boden ausgerichtet ist, keinen schrägen Abhang hat und nachdem die notwendige Drehung auf das Raster angewendet wurde, parallel zu künstlich hergestellten Artefakten, die auch in der realen Welt parallel sind, ist die Kalibrierung gut.



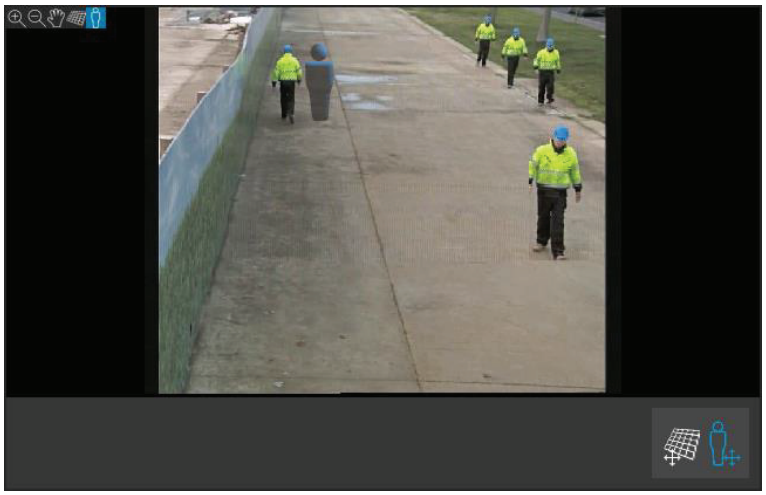
Ein Beispiel für die korrekte Ausrichtung des Rasters an den Straßenrandstreifen.



Ein Beispiel für die nicht korrekte Ausrichtung des Rasters an den Straßenrandstreifen.

Überprüfen Sie mit dem Avatar die Kalibrierung.

Der Avatar ermöglicht es Ihnen, einen 3D-Personen-Avatar von durchschnittlicher Größe in der Szene zu platzieren. Sie können die Darstellung des Avatars durch Klicken auf das Symbol Avatar Anzeigemodifikator umschalten.



Die Größe des Sichtbereichs entspricht der Größe einer durchschnittlichen Person an dieser Position gemäß der aktuellen Kalibrierung. Indem Sie den Avatar bewegen, können Sie sicherstellen, dass seine Größe in Bezug auf andere Objekte oder Personen in der Szene sinnvoll ist. Überprüfen Sie den Avatar an unterschiedlichen Positionen, da der Avatar an einer Position korrekt dimensioniert, aber an anderer Stelle im Bild falsch dimensioniert werden könnte.

Überprüfen der Kalibrierung mithilfe der Erfassungsergebnisse

Mithilfe der Erfassungsergebnisse können Sie überprüfen, wie AXIS Perimeter Defender mit der aktuellen Kalibrierung ausgeführt wird, wenn das Videomaterial das Passieren einer Person als Livestream empfangen wurde.

1. Wechseln Sie von den **Kalibrierungsergebnissen** zu den **Erfassungsergebnissen**.
2. Überprüfen Sie die Erfassungen von Personen oder Fahrzeugen, die die Überwachungsszene betreten:
   - Bei guter Kalibrierung sind die Personen mit roten Rechtecken und Fahrzeuge mit blauen Rechtecken versehen.

– Wenn Personen oder Fahrzeuge häufig nicht markiert sind, ist die automatische Kalibrierung höchstwahrscheinlich fehlgeschlagen.

– Eine rote Zone zeigt die Erfassungsgrenze gemäß der berechneten Kalibrierung, d. h. der Zone, in der die Voraussetzungen für die menschliche Größe im Bild nicht eingehalten werden. In dieser Zone kann die Erfassung aufgrund der Zielgröße fehlschlagen.

Hinweis

- Wenn die berechnete Kalibrierung falsch ist, ist auch die rote Zone falsch.
- Wenn die Person zu weit entfernt ist, ist sie möglicherweise nicht markiert. Eine Mindestgröße ist erforderlich, damit die Erfassung funktioniert. Weitere Informationen finden Sie unter *Montieren der Kamera, on page 13*.
- Die Überprüfung der Erfassungsergebnisse funktioniert möglicherweise nicht bei remote verbundenen Kameras, da die Bildrate zu niedrig ist. Dies bedeutet nicht, dass die Konfiguration fehlgeschlagen ist. Überprüfen Sie stattdessen mit dem Avatar und dem Raster die Kalibrierung.

Durchführen einer manuellen Kalibrierung

Wenn Sie keine automatische Kalibrierung versucht haben, müssen Sie ein kurzes Video aufnehmen und ein zusammengesetztes Bild erstellen, bevor Sie eine manuelle Kalibrierung durchführen können. Führen Sie die gleichen Schritte wie bei einer automatischen Kalibrierung durch (*Automatische Kalibrierung durchführen, on page 20*), wählen Sie jedoch **Manuell** statt **Automatisch** auf der Registerkarte **Kalibrierung**. So erstellen Sie das zusammengesetzte Bild, nachdem Sie ein Video aufgenommen haben:

- Bewegen Sie den Schieberegler, um im Videoclip zu navigieren
- Klicken Sie an Schlüsselpositionen auf das Kamerasymbol, um Bilder zum zusammengesetzten Bild hinzuzufügen

Stellen Sie sicher, dass das zusammengesetzte Bild einen Querschnitt der gesamten Szene wiedergibt: vorne, hinten, links und rechts.

Wenn Sie ein zusammengesetztes Bild haben, das manuell oder automatisch erstellt wurde, können Sie die manuelle Kalibrierung fortsetzen.

Das Kalibrierungsmodul kalibriert, indem es Folgendes schätzt:

- den Horizont
- die Art, wie vertikale Linien im Bild verteilt oder ausgefächert werden.
- den Maßstab der Szene

Wenn Sie eine manuelle Kalibrierung durchführen, müssen Sie diese Informationen über Kalibrierungselemente für das Kalibrierungsmodul bereitstellen. Es gibt drei Arten von Kalibrierungselementen:

- **Personenlinien** werden verwendet, um die bekannte Höhe einer durchschnittlichen Person an verschiedenen Stellen in der Szene zu markieren. Wenn Sie bereits eine automatische Kalibrierung durchgeführt haben, ist es sehr wahrscheinlich, dass das im Editorfenster angezeigte Bild mehrere Instanzen derselben Person anzeigt. Positionieren Sie die Personenlinien von Grund auf, um die Höhe und die Ausrichtung der Person an einer oder mehreren Stellen zu markieren. Eine Personenlinie muss auf dem Boden beginnen und sollte in der realen Welt vertikal sein. Die Länge einer Personenlinie in der realen Welt muss der Höhe entsprechen, die neben der Schaltfläche **Person** im Editorfenster angegeben ist. Personenlinien sind mit einem halbdurchsichtigen hellblau gekennzeichnet.
  So platzieren Sie eine Personenlinie am besten

– Es wird empfohlen, die Linie auf eine Person zu setzen, die Ihre Füße nah beieinander hat.

– Wenn Sie eine Linie auf eine Person setzen, die auf dem Boden mit den Füßen auseinander steht, platzieren Sie den unteren Punkt mittig zwischen den Fersen der Person.

– Richten Sie die Linie am Rumpf der Person aus. Wenn er oder sie sich jedoch in eine Richtung lehnt, in die beim Gehen eine Verlagerung stattfindet, versuchen Sie die Neigung durch eine aufrechtere Platzierung auszugleichen. Verwenden Sie in der Szene beliebige Anhaltspunkte, wie z. B. Bäume, Zäune oder Laternenmasten.

– Für den Maßstab der Szene wird mindestens eine Personenlinie mit der entsprechenden Personenhöhe benötigt. Wenn in der Szene keine Person sichtbar ist, können Sie eine Personenlinie auf einem anderen vertikalen Objekt mit bekannter Höhe hinzufügen, z. B. 3 m Zaunpfosten, legen Sie für die Personenhöhe die Höhe des Objekts fest.

- **Parallele horizontale Linien (H-Linien)** werden verwendet, um bekannte horizontale und parallele Linien in der Szene zu markieren. Diese Linien können sich auf dem Boden oder an einer Wand oder an beiden Elementen befinden, sie müssen jedoch alle parallel sein. Beim Hinzufügen von H-Lines müssen mindestens zwei hinzugefügt werden. Sie können sie an den Seiten oder an den Markierungen auf einer geraden Straße, einer Reihe von geraden Bahngleisen, einer sichtbaren Struktur an einer Wand oder auf den Ober- und Unterseiten einer Reihe von Zaunpfosten platzieren. H-Linien sind hellblau markiert.
- **Vertikale Linien (V-Linien)** werden verwendet, um bekannte vertikale Linien in der Szene zu markieren. Eine V-Linie sollte eine vertikale Struktur in der realen Welt markieren. Dies kann z. B. ein Zaunpfosten, die Ecke eines Gebäudes oder ein Schild sein. Eine V-Linie muss nicht auf dem Boden beginnen. V-Linien sind dunkelblau markiert. Beachten Sie, dass die V-Linien sehr empfindlich sind, sodass eine kleine Änderung der Ausrichtung die Kalibrierung drastisch ändern kann. Als Faustregel gilt, dass sich die V-Linien auf der rechten Seite des Bildes nach rechts neigen und die auf der linken Seite nach links.

1 *Personenlinien*
2 *Vertikale Linien (V-Linien)*
3 *Parallele horizontale Linien (H-Linien)*
4 *Raster- und Avatar-Tools*

Anzahl der Kalibrierungselemente

Im Allgemeinen gilt beim Hinzufügen von Personenlinien, H-Linien und V-Linien zur Szene, je mehr desto besser. Das Kalibrierungsmodul kann mit sehr wenigen Linien kalibriert werden. Die Kalibrierungsqualität wird jedoch in der Regel besser, je mehr Linien gezogen werden. Beim Hinzufügen von Personenlinien wird empfohlen, sie in der Nähe und Ferne sowie links und rechts zu platzieren.

Vertikale Strukturen im Bild

Entsprechend *Empfehlungen für die Installation der Kamera, on page 14* müssen alle Kameras leicht nach unten ausgerichtet sein. Infolgedessen scheinen sich alle vertikalen Strukturen in der realen Welt wie ein Pfauenschwanz im Bild aufzufächern. Dies bedeutet, dass sich alle Personlinien und V-Linien in Richtung des Bildrands neigen sollten. Eine Linie auf der rechten Hälfte des Bildes sollte nach rechts geneigt werden, und eine Linie auf der linken Seite sollte nach links geneigt werden. Mindestens eine der platzierten Personenlinien oder V-Linien muss „richtig geneigt" sein, damit die Kalibrierung funktioniert.

Die Präzisionsanzeige stellt visuelles Feedback zur Ebene und Detailgenauigkeit bereit, die der Szene hinzugefügt wurden. Für eine erfolgreiche manuelle Kalibrierung müssen Markierungen die Szene von vorn nach hinten und von links nach rechts abdecken. Dies wird durch eine grüne Präzisionsanzeige angezeigt.

Kalibrierungsqualität

Die Kalibrierungsqualität kann mit den Raster- oder Avatar-Manipulatoren überprüft werden. Siehe *Überprüfen der Kalibrierungsqualität , on page 21*. Klicken Sie alternativ auf **Überprüfen**. Dies zeigt das Ergebnis der Ausführung von AXIS Perimeter Defender auf dem erfassten Video mithilfe der aktuellen manuellen Kalibrierung.

Kalibrierung – PTZ-Autotracking

Wichtig

Die Kalibrierung muss eine hohe Qualität haben, um gute Ergebnisse zu erzielen. Befolgen Sie die Richtlinien und Anweisungen sorgfältig.

Hinweis

Sie können beide Kameras gleichzeitig oder nacheinander kalibrieren.

1. Wählen Sie sowohl die feste Kamera als auch die PTZ-Kamera aus.
2. Navigieren Sie zu **Kalibrierung** und klicken Sie auf **PTZ–Position einrichten**. Ein Popup mit der Ansicht der festen Kamera wird angezeigt.
   Die PTZ-Kamera wird beim Starten der Anwendung kurzzeitig schwenken, neigen und zoomen.
3. Stellen Sie sicher, dass die Ansicht der beiden Kameras zueinander ausgerichtet ist.
   Falls nicht, klicken Sie in die Live-Ansicht und passen Sie die Ansicht der PTZ-Kamera an, bis sie der Ansicht der unbeweglichen Kamera entspricht. Stellen Sie sicher, dass keine Rolle vorhanden ist.
4. Klicken Sie auf **PTZ–Position einrichten**.
   Wenn die Schaltfläche nicht sichtbar ist, bewegen Sie das Popup mit der Ansicht der festen Kamera.
5. Klicken Sie auf **Automatisch**.
6. Führen Sie eine automatische Kalibrierung gemäß den Anweisungen unter *Automatische Kalibrierung durchführen, on page 20* durch.
7. Überprüfen Sie mit dem Avatar die Kalibrierungsqualität der festen Kamera. Siehe *Überprüfen Sie mit dem Avatar die Kalibrierung., on page 23*.
   Wenn die Qualität gut genug ist, klicken Sie auf **Akzeptieren**.
   Wenn die Qualität nicht ausreichend gut ist, verwenden Sie das Video der automatischen Kalibrierung, um eine manuelle Kalibrierung durchzuführen. Klicken Sie auf **Manuell** und befolgen Sie die Anweisungen unter *Durchführen einer manuellen Kalibrierung, on page 24*.
8. Definieren Sie unter **Szenarios** die Regeln für das Auslösen von Alarmen. Siehe *Szenarien definieren, on page 26*.
9. Klicken Sie unter **Kalibrierung** in der Live-Ansicht der PTZ-Kamera auf **Überprüfung**.
10. Überprüfen Sie mit dem Avatar die Kalibrierungsqualität der PTZ-Kamera. Siehe *Überprüfen Sie mit dem Avatar die Kalibrierung., on page 23*.
    Wenn die Qualität gut genug ist, klicken Sie auf **Akzeptieren**.
    Wenn die Qualität nicht ausreichend gut ist, verwenden Sie das Video der automatischen Kalibrierung, um eine manuelle Kalibrierung durchzuführen. Klicken Sie auf **Manuell** und befolgen Sie die Anweisungen unter *Durchführen einer manuellen Kalibrierung, on page 24*.
11. Koppeln Sie die Kameras. Siehe *Koppeln der Kameras – PTZ-Autotracking, on page 29*.

Szenarien definieren

Szenarien

AXIS Perimeter Defender umfasst gemeinsame Szenarien mit steriler Zone, die Sie zur Sicherung und Überwachung sensibler Bereiche konfigurieren können. Im Kalibrierungsschritt wurde der maximale Erfassungsbereich erstellt, um ein Standardszenario des Typs Einbruch/Längeres Verweilen bereitzustellen. In diesem Schritt können Sie drei Typen von anspruchsvolleren Erfassungsszenarien definieren:

Hinweis

Wenn Sie AXIS Perimeter Defender 4.0 nutzen, können Sie Szenarien nun auch ohne die Desktop-Anwendung konfigurieren. Die Änderungen werden in die Desktop-Anwendung übernommen. Mehr lesen Sie unter *Weboberfläche, on page 39*.

- Einbruch/Längeres Verweilen. Siehe *Einrichten des Szenarios für Eindringen/Längeres Verweilen, on page 27*
- Zonenübergang. Siehe *Einrichten des Szenarios für Zonenübergänge, on page 28*
- Bedingung Siehe *Einrichten des bedingten Szenarios, on page 28*

Wenn das **!** Symbol anhand eines Szenarionamens angezeigt wird, bedeutet dies, dass das Setup des Szenarios nicht abgeschlossen ist. Das häufigste Problem besteht darin, dass die Erfassungszone noch nicht definiert wurde.

Allgemeine Parameter

Die auf der Benutzeroberfläche festgelegten globalen Parameter gelten für alle Szenarios.

Kameratyp – Wählen Sie für visuelle Kameras die Option **Farbe – Tag-Nacht**. Bei Wärmebildkameras wird der Kameratyp automatisch auf thermisch festgelegt.

Hinweis

- Zusätzliche Ansatztypen können das Risiko von Fehlalarmen, z. B. durch Tiere, erhöhen.
- Zusätzliche Ansatztypen werden bei Geräten nicht unterstützt, die nur im KI-Modus ausgeführt werden.

Zusätzliche Annäherungsarten – Wählen Sie die Objekte aus, die Sie mit Ihrem Erfassungsszenario abdecken möchten.

Erweiterte Abschwächung – Aktivieren Sie bei Geräten mit dem KI-Modus **KI**, um ihn einzuschalten. Sie können die Option **Scheinwerfer/Fahrzeuge in der Szene** verwenden, wenn die Szene Fahrzeuge, Scheinwerfer oder Scheinwerfer-Effekte wie z. B. Reflexionen enthält. Bei Verwendung dieser Einstellung kann die Leistung unter normalen Bedingungen manchmal reduziert werden. In der Standardeinstellung müssen alle Szenarien Fahrzeuge und dadurch Scheinwerfer enthalten. Sie können die Option **Insects/droplets on lens (Insekten/ Tropfen auf dem Kameraobjektiv)** verwenden, um durch Regentropfen oder Insekten ausgelöste Alarme zu ignorieren und die Fehlalarme zu verringern.

Empfindlichkeit – Bewegen Sie den Schieberegler nach rechts, um die Empfindlichkeit des Systems zu erhöhen. Eine höhere Empfindlichkeit verringert das Risiko von fehlenden Alarmen, erhöht jedoch das Risiko von Fehlalarmen.

Filtern der Zielgröße – Bei Geräten mit dem KI-Modus können Objekte herausgefiltert werden, die kleiner als die Zielgröße sind.

Parameter Verweildauer

Für jedes erstellte Szenario können Sie die Parameter Verweildauer festlegen.

Mindestverweilzeit in Zone – Legen Sie fest, wie lange ein Objekt in einer Zone bleiben muss, damit die Zone aktiviert wird.

Schmaler Bereich – Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, besteht die Möglichkeit, dass die Alarme übersehen werden. Sie können dies durch Auswählen der Option **Narrow zone (schmaler Bereich)** minimieren. Beachten Sie, dass diese Einstellung nicht mit der Option **Min presence in zone (Mindestverweildauer in Zone)** kombiniert werden kann.

Einrichten des Szenarios für Eindringen/Längeres Verweilen

Das Szenario für Eindringen/Längeres Verweilen löst einen Alarm aus, wenn ein Objekt in eine bestimmte Zone eindringt und länger als die vordefinierte Zeit in der Zone verbleibt.

Das im Kalibrierungsschritt erstellte Standardszenario entspricht dem Typ Eindringen/Längeres Verweilen und verwendet die maximale Erfassungszone. Um dieses Szenario zu verwenden, klicken Sie auf der Registerkarte **Szenarien** auf **Akzeptieren**.

So ändern Sie das Standardszenario:

1. Navigieren Sie zu **Szenarios > Erweiterte Szenarios**.

2. So ändern Sie die Standard-Erfassungszone:
   - Um vorhandene Punkte in der Erfassungszone zu bewegen, klicken Sie darauf und bewegen Sie diese mit der Maus.
   - Um zusätzliche Punkte zu erstellen, klicken Sie auf eines der vorhandenen Segmente und ziehen Sie es mit der Maus.
3. Wählen Sie unter **Erfassen** den zu erfassenden Objekttypen aus.
4. Legen Sie unter **Parameter Verweildauer** fest, ob ein Objekt einen Alarm auslösen soll, sobald es in die Zone eindringt, indem Sie die Zeit für das längere Verweilen in **Mindestverweildauer in Zone** einstellen.
5. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Diese Einstellung kann nicht mit der Option **Min presence in zone (Mindestverweildauer in Zone)** kombiniert werden. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
6. Klicken Sie auf **Akzeptieren**, um die Änderungen an der Kamera hochzuladen und zurück zur Hauptansicht zu wechseln.

Einrichten des Szenarios für Zonenübergänge

Das Zonenübergangsszenario ist so konzipiert, dass ein Alarm ausgelöst wird, wenn ein Objekt in einer bestimmten Reihenfolge zwei Erfassungszonen durchläuft.

Wichtig

Für das Zonenübergangsszenario gilt folgende Einschränkung: Wenn sich das Objekt, das das Szenario auslöst, in der Ursprungszone einige Sekunden lang nicht mehr bewegt, bevor es zur Endzone übergeht, wird das Szenario nicht ausgelöst.

Unter **Parameter Verweildauer** können Sie für jede der Zonen im Szenario eine Mindestverweildauer festlegen. Wenn T_A die Mindestzeit in der Ursprungszone und T_B in der Endzone ist, wird ein Alarm nur dann ausgelöst, wenn das Objekt länger als T_A in der Ursprungszone und dann länger als T_B in der Endzone bleibt.

1. Navigieren Sie zu **Szenarios > Erweiterte Szenarios**.
2. Klicken Sie auf **Neu** und wählen Sie **Zonenübergang** aus.
3. Erstellen Sie zwei Erfassungszonen, die durch mindestens einen Meter getrennt sind (3 Fuß 3 3/8 Zoll):
   - Um eine Erfassungszone zu erstellen, klicken Sie mehrmals in das Bild.
   - Klicken Sie mit der rechten Maustaste in das Bild, um die Zone zu beenden.
4. Um die unzulässige Übergangsrichtung anzugeben, klicken Sie auf **Ursprung auswählen** und klicken Sie dann auf eine der Zonen.
5. Wählen Sie unter **Erfassen** den zu erfassenden Objekttypen aus.
6. Legen Sie unter **Parameter Verweildauer**die **Mindestverweildauer in** für eine oder beide Zonen fest, wenn Sie nicht möchten, dass eine Zone beim Eindringen eines Objekts aktiviert wird.
7. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Diese Einstellung kann nicht mit der Option **Min presence in zone (Mindestverweildauer in Zone)** kombiniert werden. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
8. Klicken Sie auf **Akzeptieren**, um die Änderungen an der Kamera hochzuladen und zurück zur Hauptansicht zu wechseln.

Einrichten des bedingten Szenarios

Das bedingte Szenario löst einen Alarm aus, wenn ein Objekt in eine bestimmte Zone eindringt, ohne vorher andere durchzulaufen.

Unter **Parameter Verweildauer** können Sie für jede der Zonen im Szenario eine Mindestverweildauer festlegen. Wenn T_A die Mindestzeit in der erlaubten Zone und T_B in der Eindringzone liegt, wird ein Alarm nur ausgelöst, wenn das Objekt:

- sich länger als T_B in der Eindringzone aufhält, ohne zuvor die erlaubte Zone betreten zu haben.
- kürzer als T_A in der zugelassenen Zone bleibt und dann die Eindringzone betritt und dort länger als T_B bleibt.

Kein Alarm wird ausgelöst, wenn das Objekt:

- nicht in die Eindringzone eintritt oder kürzer als T_B dort bleibt.
- länger als T_A in der autorisierten Zone bleibt, dann in die Eindringzone eindringt (unabhängig davon, wie lange das Objekt dort bleibt).

1. Navigieren Sie zu **Szenarios > Erweiterte Szenarios**.
2. Klicken Sie auf **Neue** und wählen Sie dann **Bedingung** aus.
3. Erstellen Sie zwei oder mehr Erfassungszonen, die durch mindestens einen Meter getrennt sind (3 Fuß 3 3/8 Zoll):
   - Um eine Erfassungszone zu erstellen, klicken Sie mehrmals in das Bild.
   - Klicken Sie mit der rechten Maustaste in das Bild, um die Zone zu beenden.
4. Um die zulässige Querrichtung festzulegen, klicken Sie auf **Eindringzone auswählen** und klicken Sie dann auf eine der Zonen.
5. Wählen Sie unter **Erfassen** den zu erfassenden Objekttypen aus.
6. Legen Sie unter **Parameter Verweildauer**die **Mindestverweildauer in** für eine oder beide Zonen fest, wenn Sie nicht möchten, dass eine Zone beim Eindringen eines Objekts aktiviert wird.
7. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Diese Einstellung kann nicht mit der Option **Min presence in zone (Mindestverweildauer in Zone)** kombiniert werden. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
8. Klicken Sie auf **Akzeptieren**, um die Änderungen an der Kamera hochzuladen und zurück zur Hauptansicht zu wechseln.

Koppeln der Kameras – PTZ-Autotracking

Im Setup für AXIS Perimeter Defender PTZ-Autotracking müssen Sie die feste Kamera und die PTZ-Kamera miteinander verbinden, um sicherzustellen, dass ein sich bewegendes Objekt von der PTZ-Kamera auf effiziente Weise nachverfolgt wird.

Wenn Sie eine automatische Kalibrierung durchgeführt haben, können Sie *Durchführen einer automatischen Kopplung, on page 29* der beiden Kameras durchführen. Andernfalls müssen Sie *Durchführen einer manuellen Kopplung, on page 30* durchführen.

Durchführen einer automatischen Kopplung

Im Kopplungsvideo stellen die roten Linien die Person dar, und der orangefarbene Begrenzungsrahmen stellt das vergrößerte Bild der PTZ-Kamera dar.

1. Überprüfen Sie unter **Kalibrierung > PTZ-Kopplungsüberprüfung** die Kopplungsvideos der beiden Kameras:
   - stellen Sie sicher, dass die roten Linien in den beiden Bildern im gesamten Video ausgerichtet sind
   - stellen Sie sicher, dass die roten Linien stets von den Füßen bis zum Kopf der Person reichen
   - stellen Sie sicher, dass die Person stets innerhalb des orangefarbenen Begrenzungsrahmens im Video der PTZ-Kamera zentriert ist
2. Wenn die Bedingungen in Schritt 1 erfüllt sind, wählen Sie **Interaktive Kopplungsüberprüfung** aus. Wenn die Bedingungen nicht erfüllt sind, klicken Sie auf **Manuell** und befolgen Sie die Schritte unter *Durchführen einer manuellen Kopplung, on page 30*.
3. Bewegen Sie den Schieberegler, um im Videoclip zu navigieren. Überprüfen Sie Folgendes:
   - Die blauen Linien in den beiden Bildern sind im gesamten Video ausgerichtet.

- stellen Sie sicher, dass die Person stets innerhalb des orangefarbenen Begrenzungsrahmens im Video der PTZ-Kamera zentriert ist

4. Bei Szenen mit fehlenden orangefarbenen Begrenzungsrahmen:
   4.1. Aktivieren Sie den Avatar im festen Kamerabild.
   4.2. Verwenden Sie den Schieberegler, um sich im Video vor- und zurückzubewegen. Platzieren Sie den Avatar auf der Person in der festen Kameraansicht, und überprüfen Sie, ob sich der rote Punkt der PTZ-Kamera an den Füßen der Person im Bild befindet.
5. Wenn in Szenen mit automatischer Kopplung keine blauen Linien hinzugefügt wurden, klicken Sie auf **Manuell** und fügen Sie manuell rote Linien hinzu. Siehe dazu *Durchführen einer manuellen Kopplung, on page 30* für detaillierte Anweisungen.
6. Klicken Sie auf **Akzeptieren** und **Beenden**.

Durchführen einer manuellen Kopplung

Wenn Sie eine manuelle Kopplung durchführen, fügen Sie im Kalibrierungsschritt vertikale rote Linien von Fuß bis Kopf der Person hinzu, die die Überwachungsszene durchlaufen hat. Sie müssen im gesamten Video Linien hinzufügen, um die gesamte Szene abzudecken.

Wenn Sie bereits eine automatische Kopplung durchgeführt haben, enthält das Video bereits blaue Linien.

Entfernen Sie blaue und rote Linien, die:
- nicht an den Füßen der Person beginnen
- nicht den ganzen Weg zum Kopf der Person reichen
- keine entsprechende Zeile im PTZ-Kamerabild aufweisen

Um eine Linie zu entfernen, klicken Sie darauf und drücken Sie auf Del (Löschen).

1. Bewegen Sie den Schieberegler, um zu einem Bild im Videoclip zu navigieren, in dem die Person sichtbar ist.
2. Fügen Sie der Person im festen Kamerabild eine rote Linie hinzu. Beginnen Sie die Linie an den Füßen der Person. Die Zeile erhält eine ID-Nummer.
3. Fügen Sie im PTZ-Kamerabild eine entsprechende rote Linie an demselben Objekt hinzu. Stellen Sie sicher, dass die ID-Nummer der im festen Kamerabild entspricht.
4. Wiederholen Sie die Schritte 1 bis 3, bis Sie die gesamte Szene abgedeckt haben.
   Wenn der Videoclip eine ausreichende Anzahl von Zeilen für eine gültige Kopplung enthält:
   - Die **Akzeptieren**-Schaltfläche wird aktiviert
   - Im PTZ-Kamerabild wird ein orangefarbenes Begrenzungsrechteck angezeigt
5. Stellen Sie sicher, dass die Person stets innerhalb des orangefarbenen Begrenzungsrahmens zentriert ist. Wenn es keine Szenen gibt, fügen Sie weitere rote Linien hinzu.
6. Aktivieren Sie den Avatar im festen Kamerabild.
7. Bewegen Sie den Schieberegler, um im Videoclip zu navigieren. Überprüfen Sie mit dem Avatar Folgendes:
   - Im festen Kamerabild entspricht die Größe des Avatars der Größe der Person in unterschiedlichen Positionen
   - Im PTZ-Kamerabild befindet sich der rote Punkt an den Füßen der Person.
   - In dem PTZ-Kamerabild ist die Person stets innerhalb des orangefarbenen Begrenzungsrahmens zentriert
8. Klicken Sie auf **Akzeptieren**. Wenn die Schaltfläche deaktiviert ist, müssen Sie zunächst mehr rote Linien hinzufügen.
9. Klicken Sie auf **Beenden**.

Ausgänge definieren

Damit AXIS Perimeter Defender beim Erfassen eines Eindringens Alarme ausgibt, müssen Sie dafür Regeln definieren. Das System kann Alarme an z. B. ein VMS senden.

AXIS Perimeter Defender kann Alarme über verschiedene Schnittstellen senden.

Aus der Anwendung selbst:

- XML- oder Nur-Text-Alarmbenachrichtigungen über TCP/IP
- XML-Metadaten-Streams über mehrteiliges HTTP

Vom Gerät:

- Grundlegende kostenlose Text-Benachrichtigungen für Alarme über TCP/IP
- Elektrische Ausgänge (trockene oder feuchte Kontakte)
- E-Mail-Benachrichtigungen
- FTP-Upload von Alarmbildern

Sie können mehrere Schnittstellen gleichzeitig aktivieren.

Weitere ausführliche Informationen finden Sie unter *Ausgänge, on page 32*.

So definieren Sie Regeln für das Senden von Alarmen vom Gerät:

1. Navigieren Sie zu den **Ausgängen** und klicken Sie auf **Konfigurieren**. Die Webseite des Geräts wird in einem Webbrowser geöffnet.
2. Erstellen Sie eine neue Aktionsregel.
3. Wählen Sie aus der Liste der Auslöser **Anwendungen**, **AXIS PerimeterDefender** und das Szenario zum Auslösen der Aktion.

Hinweis

Wählen Sie **ALL_SCENARIOS**aus, um die gleiche Aktion für alle definierten Szenarien auszulösen.

4. Wählen Sie aus der Liste der Aktionen die Aktion aus, die durchgeführt werden soll, wenn die Bedingung erfüllt ist.
5. Klicken Sie auf **OK**.

Detaillierte Informationen zum Erstellen von Aktionsregeln finden Sie im Benutzerhandbuch des Geräts.

Erweiterte Konfiguration

Ausgänge

XML/Textalarm-Benachrichtigungen

Mit dieser Schnittstelle kann ein TCP/IP-Empfänger für jeden Alarm eine vollständigere und beschreibende XML- oder Textnachricht empfangen. In Bezug auf die Freitextschnittstelle bietet die XML/Text-Schnittstelle folgende Vorteile:

- Eine Benachrichtigung wird am Anfang des Alarms, am Ende des Alarms und alle 10 Sekunden während des Alarms gesendet.
- Timestamp (Zeitstempel): Die Benachrichtigungen zum Beginn und Ende des Alarms enthalten einen Zeitstempel, der mit der Kamera-Uhr synchronisiert wird und das Datum und die Uhrzeit der Ereignisse genau angibt.
- Alarmtyp: AXIS Perimeter Defender unterstützt mehrere Alarmtypen (siehe *Szenarien definieren, on page 26*. Die XML/Text-Benachrichtigungen enthalten die Informationen über den Typ des ausgelösten Alarms. Achtung: Das Szenario „Zonenübergang" hat den Typ „Passage" und das Szenario „Längeres Verweilen" hat den Typ „Presence"
- An der Alarmgenerierung beteiligte Zonen; wenn jedes AXIS Perimeter Defender-Szenario einer oder mehreren Zonen zugeordnet ist, sind in den XML-Text-Benachrichtigungen die mit dem Alarm verknüpfte Zone (d. h. für einen Eindringalarm, die Eindringzone, in der eine Person erkannt wurde)

In Bezug auf die Freitextschnittstelle bietet die XML/Text-Schnittstelle folgende Beschränkungen:

- Der Meldungstext wurde korrigiert und es sind keine freien Textfelder vorhanden.
- Pro Kamera wird jeweils nur ein Empfänger unterstützt.

Der Empfänger der XML/Text-Benachrichtigungen erhält vier Nachrichtentypen:

- AXIS Perimeter Defender sendet beim Konfigurieren der XML-Benachrichtigung eine CONNECTION_TEST-Meldung, um sicherzustellen, dass die Kommunikation mit dem Empfänger erwartungsgemäß funktioniert.
- Wenn AXIS Perimeter Defender einen Alarm auslöst, wird eine ALARM_START-Meldung gesendet.
- Während der Alarmdauer sendet AXIS Perimeter Defender mehrere „Alarm wird verarbeitet"-Meldungen, eine alle zehn Sekunden. All diese Nachrichten haben dasselbe GUID-Tag, das identisch mit der ALARM_START-Meldung und ALARM_STOP-Meldungen im Zusammenhang mit demselben Alarm ist.
- Am Ende des Alarms sendet AXIS Perimeter Defender einen ALARM_STOP-Alarm.

Erläuterungen zum Format dieser Meldungen, sowohl im XML-Format als auch im Textformat, finden Sie unter *Beispiele für XML- und Textformat, on page 32*.

Beispiele für XML- und Textformat

Das XML-Format ist das Standardformat für TCP/IP-Benachrichtigungen. Wenn die Benachrichtigungsgröße jedoch von Bedeutung ist, kann ein Textformat mit kürzeren Meldungen verwendet werden. Um das Textformat auszuwählen, muss auf der Konfigurationsseite von **AXIS Perimeter** Defender die Option
Für Alarmparameter nicht XML verwenden ausgewählt werden.

Beispiel:
Eine CONNECTION_TEST-Nachricht im XML-Format ähnelt diesem Beispiel:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"          ID="1"          TYPE="CONNECTION_TEST"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">  <REFERENTIAL>45</REFERENTIAL></KEENEO_MESSAGE>
```

- VERSION ist die interne Version der XML-Syntax und des Protokolls.
- ID ist eine numerische Kennung für die Nachricht. IDs sind weder garantiert eindeutig noch progressiv.

- TYPE ist der Typ der Meldung, hier „CONNECTION_TEST“. Der Meldungstyp bestimmt die Sub-Tags der Meldung (keine bei Meldungen des Typs „CONNECTION_TEST“).
- SENDER_IP ist die IP-Adresse der Axis Kamera, die die XML-Benachrichtigung sendet.
- SENDER_PORT ist stets Null; die Kamera kann keine eingehenden Nachrichten empfangen.
- REFERENTIAL entspricht der der Kamera zugeordneten numerischen ID

Wenn das Textformat gewählt wird, enthalten die Benachrichtigungen jeweils 7 Felder, die durch das „Pipe“-Zeichen | getrennt sind. Wenn ein Feld nicht angegeben werden kann (z. B. weil es für diesen Nachrichtentyp nicht sinnvoll ist), wird es durch „-“ ersetzt.

Die sieben Felder vom ersten bis zum letzten (in der Klammer, das entsprechende XML-Feld, wenn das Format XML lautet):

1. Die numerische ID der Meldung („ID“-Attribut des XML-Headers „KEENEO_MESSAGE“).
2. Die IPv4-Adresse der Kamera („SENDER_IP“-Attribut des XML-Headers „KEENEO_MESSAGE“).
3. Die referenzielle Zahl, die der AXIS Perimeter Defender-Instanz („REFERENTIAL“-Tag) zugeordnet ist.
4. Der Nachrichtentyp („TYPE“-Attribut des XML-Headers „KEENEO_MESSAGE“).
5. Der Alarmtyp („TYPE“-Tag).
6. Der Name des Szenarios, das den Alarm ausgelöst hat („SCENARIO_NAME“-Tag).
7. Der Zeitstempel („TIMESTAMP“-Tag). Das Timestamp-Format entspricht dem des XML-Formats.

Die vorherige CONNECTION_TEST-Nachricht im Textformat lautet:

```
1|192.168.1.40|45|CONNECTION_TEST|-|-|-
```

Beispiel:
Eine ALARM_START-Nachricht im XML-Format sieht wie in diesem Beispiel aus:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"         xmlns:xsd="http://www.w3.org/2001/XMLSchema"         VERSION=
"5.0.0"         ID="9999"         TYPE="ALARM_START"         SENDER_IP=
"192.168.1.40"         SENDER_PORT="0">  <REFERENTIAL>0</REFERENTIAL>  <TYPE>INTRUSION</
TYPE>  <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>  <EXTRA_DATA>zone=testzone</EXTRA_
DATA>  <TIMESTAMP>2014-03-01T21:24:12.114</TIMESTAMP>  <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- Der Nachrichtenheader entspricht der Meldung „CONNECTION_TEST“.
- Der Nachrichtentyp entspricht „ALARM_START“ und verfügt über eine Reihe von untergeordneten Tags.

– REFERENTIAL entspricht der der Kamera zugeordneten numerischen ID.

– TYPE gibt den Typ des Alarms an, der von AXIS Perimeter Defender, „INTRUSION“ in diesem Beispiel, ausgelöst wurde. Andere mögliche Typen sind „PRESENCE“, „PASSAGE“ und „CONDITIONAL“.

– SCENARIO_NAME ist der Name des Szenarios, das den Alarm ausgelöst hat, wie in der Konfigurationsschnittstelle definiert. Siehe *Einrichten des Szenarios für Eindringen/Längeres Verweilen, on page 27*

– EXTRA_DATA trägt den Zonennamen (bzw. die Liste der Zonennamen), die mit dem Alarm verbunden ist, wie z. B. die Eindringzone.

– TIMESTAMP ist das Datum und die Uhrzeit des Alarmstarts im Format JJJJ-MM-TTTHH: mm:ss.zzz, wobei:
  – JJJJ entspricht dem Jahr auf vier Stellen, z. B 2014.
  – MM ist der Monat auf 2 Stellen, z. B. 01 für Januar.
  – TT ist die Tag auf 2 Stellen, z. B. 03 für den Dritten.
  – T ist ein fester Buchstabe
  – SS ist die Stunde im 24-Stunden-Format, von 00 bis 23
  – mm sind die Minuten auf 2 Stellen, von 00 bis 59
  – ss sind die Sekunden auf 2 Stellen, von 00 bis 59
  – zzz sind die Millisekunden auf 3 Stellen, von 000 bis 999.

AXIS Perimeter Defender verwendet das interne Datum und die Uhrzeit der Kamera für die Generierung des Alarmzeitstempels, daher ist es wichtig, die Kamera mit einer externen Uhr zu synchronisieren.

– GUID ist ein eindeutiger Bezeichner, der für alle mit demselben Alarm verknüpften Meldungen konstant ist (also ALARM_START, ALARM_IN_PROGRESS und ALARM_STOP).

Dies entspricht im Textformat der ALARM_START-Meldung:

```
9999|192.168.1.40|0|ALARM_START|INTRUSION|Intrusion-0|2014-03-01T21:24:12.114
```

Beispiel:
Eine ALARM_IN_PROGRESS-Meldung im XML-Format sieht wie folgendes Beispiel aus:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"          ID="9999"          TYPE="ALARM_IN_PROGRESS"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- Der Nachrichtenheader entspricht der Meldung „CONNECTION_TEST“ und „ALARM_START“.
- Der Nachrichtentyp entspricht „ALARM_IN_PROGRESS“ und verfügt über eine Reihe von untergeordneten Tags.

– REFERENTIAL entspricht der der Kamera zugeordneten numerischen ID.

– TYPE ist der Typ des Alarms, der von AXIS Perimeter Defender mit dem entsprechenden ALARM_START ausgelöst wurde.

– SCENARIO_NAME ist der Name des Szenarios, das den Alarm ausgelöst hat, dem dazugehörigen ALARM_START entspricht.

– Die GUID entspricht dem dazugehörigen ALARM_START.

Die entsprechende ALARM_IN_PROGRESS-Meldung im Textformat:

```
9999|192.168.1.40|0|ALARM_IN_PROGRESS|INTRUSION|Intrusion-0|-
```

Beispiel:
Eine ALARM_STOP-Meldung im XML-Format sieht wie in diesem Beispiel aus:

```
<?xml version="1.0"?><KEENEO_MESSAGE xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"          xmlns:xsd="http://www.w3.org/2001/XMLSchema"          VERSION=
"5.0.0"          ID="9999"          TYPE="ALARM_STOP"          SENDER_IP=
"192.168.1.40"          SENDER_PORT="0">   <REFERENTIAL>0</REFERENTIAL>   <TYPE>INTRUSION</
TYPE>   <SCENARIO_NAME>Intrusion-0</SCENARIO_NAME>   <EXTRA_DATA>zone=testzone</EXTRA_
DATA>   <TIMESTAMP>2014-03-01T21:24:26.304</TIMESTAMP>   <GUID>77acddf9-e0d4-402e-a497-
231aeee22788</GUID></KEENEO_MESSAGE>
```

- Die Kopfzeile der Meldung entspricht den vorherigen Meldungen.
- Der Nachrichtentyp entspricht „ALARM_STOP“ und hat die gleiche Gruppe von Subtypen der ALARM_START-Meldung.

Die entsprechende ALARM_IN_PROGRESS-Meldung im Textformat:

```
9999|192.168.1.40|0|ALARM_STOP|INTRUSION|Intrusion-0|2014-03-01T21:24:26.304
```

Die TCP/IP-Verbindung wird nach jeder Nachricht immer geschlossen. Daher muss der Empfänger den Abhörsocket stets geöffnet lassen, um weitere Benachrichtigungen empfangen zu können.

Kommunikationsfehler

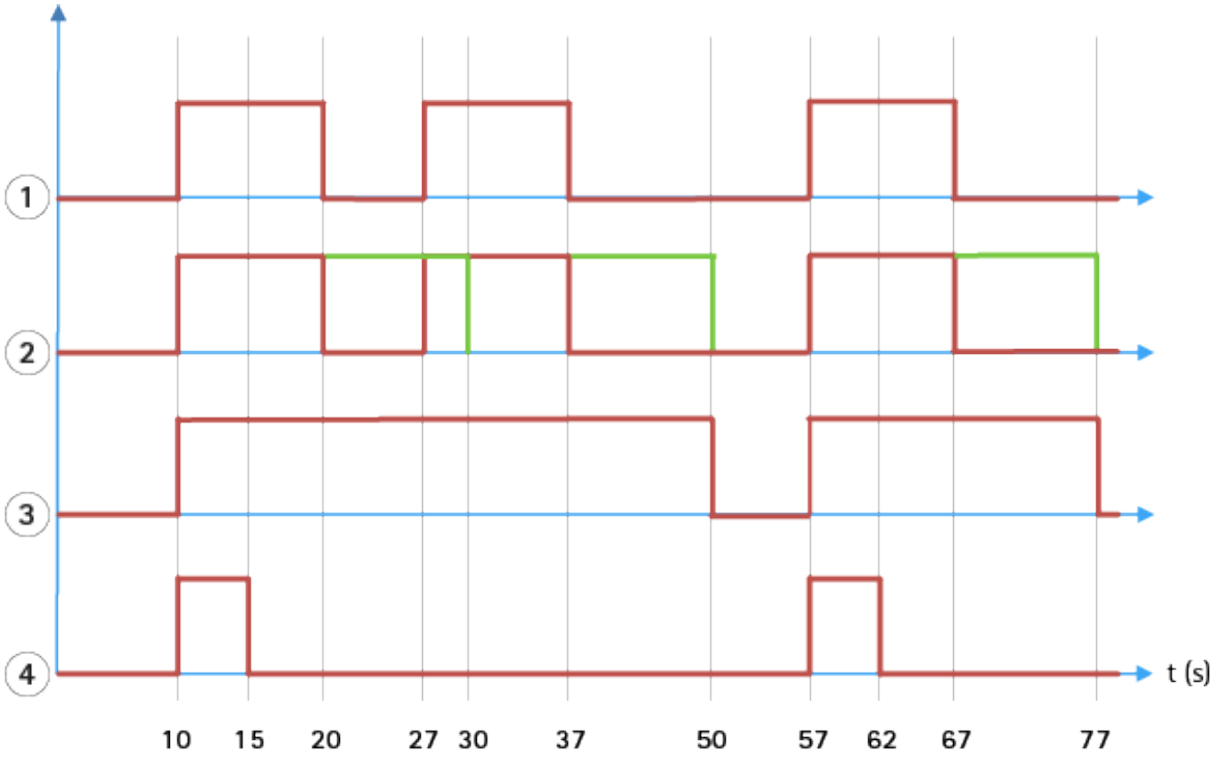
Wenn der Fernempfänger von XML-Benachrichtigungen nicht erreichbar ist, z. B. aufgrund einer Netzwerk-Trennung, beginnt AXIS Perimeter Defender mit dem Puffern der intern nicht zugestellten Alarme und versucht regelmäßig (mindestens alle 10 Sekunden), diese erneut zuzustellen. Nach einer aufeinander folgenden Anzahl von Fehlern bei der Bereitstellung neuer Nachrichten (Fehler beim erneuten Übermitteln einer Nachricht aus dem Puffer wird nicht berücksichtigt), erklärt AXIS Perimeter Defender den Empfänger als „dauerhaft offline“ und beendet das Senden von XML-Benachrichtigungen an den Empfänger. Die Anzahl der aufeinander folgenden Fehler wird auf 20 festgelegt, das entspricht in etwa 4 oder 5 Eindringalarmen mit einer durchschnittlichen

Dauer von 40 Sekunden. AXIS Perimeter Defender sendet die Benachrichtigungen erneut an denselben Empfänger, wenn eines der folgenden Ereignisse auftritt:

- AXIS Perimeter Defender wird neu gestartet.
- Derselbe Wert des Parameters „Alarm-Streaming-URL" wird erneut gespeichert.

Nachalarmzeit

AXIS Perimeter Defender implementiert die Idee der „Zeit nach dem Alarm". Dies wird als das Zeitintervall nach einem Alarm festgelegt, bei dem ein anderer Alarm ausgelöst wird. Beide Alarme werden zu einer eindeutigen Einheit zusammengeführt.



1 Drei Alarme, die von AXIS Perimeter Defender zu der Zeit 10, 27 und 57 ausgelöst werden. Jeder Alarm hat eine Dauer von 10 Sekunden, d. h. ein Eindringling hat 10 Sekunden gebraucht, um die Eindringzone zu durchqueren.
2 Es wird eine Zeit nach dem Alarm von 10 Sekunden hinzugefügt.
3 Alarme mit XML-Benachrichtigungen und XML-Metadaten.
4 Alarme mithilfe von E-Mail-Benachrichtigungen, Hochladen von Bildern per FTP, elektrische Kontakte und grundlegende TCP/IP-Benachrichtigungen.

(2) Beachten Sie, dass die Dauer der Zeit nach einem Alarm von 10 Sekunden (in grün) die Dauer der einzelnen Alarme erhöht, sodass dies zur Fusion (Zusammenführung) zweier Alarme führt, die 10 Sekunden oder weniger voneinander getrennt sind.

(3) Sie können die resultierende Alarmnummer und Dauer anzeigen, die von AXIS Perimeter Defender durch XML-Benachrichtigungen und XML-Metadaten ausgelöst wurden. Die Zeit nach dem Alarm kann verwendet werden, um weniger lange Alarme anstelle von mehreren, kürzeren und aufeinander folgenden zu erhalten.

(4) Für E-Mail-Benachrichtigungen, das Hochladen von Bildern per FTP, elektrische Kontakte und grundlegende TCP/IP-Benachrichtigungen ist das Ergebnis der Verwendung einer 10-Sekunden-Nach-Alarm-Zeit unterschiedlich. Diese Benachrichtigungen berücksichtigen nur den Alarmstart und vernachlässigen den Alarmstopp. Daher gibt es bei Verwendung dieser Benachrichtigungen keine „Alarmdauer". Die Dauer der Benachrichtigung wird daher durch die Nach-Alarm-Zeit nicht geändert. Sie wird stets auf den vom Benutzer beim Konfigurieren der Benachrichtigung gewählten Wert festgelegt. Daher wird beim Zusammenführen von aufeinander folgenden Alarmen aufgrund der Nach-Alarm-Zeit nur eine Benachrichtigung gesendet. Sie können

sehen, dass AXIS Perimeter Defender die ersten beiden Alarme zusammenführt, sodass nur eine Benachrichtigung gesendet wird. Daher werden E-Mail-Benachrichtigungen, das Hochladen von ftp-Bildern, elektrische Kontakte und einfache TCP/IP-Benachrichtigungen nur für zwei von ihnen versendet. Für diese Benachrichtigungen wird eine feste Dauer von 5 Sekunden in der Grafik dargestellt.

So konfigurieren Sie die Zeit nach dem Alarm

1. Öffnen Sie das AXIS Perimeter Defender Setup.
2. Navigieren Sie zu **Ausgänge**.
3. Ändern Sie die Einstellung für die **Zeit nach dem Alarm**. Die Standardvorgabe lautet 7 Sekunden.
4. Klicken Sie auf **Zuweisen**.

Metadaten

Burnt-in Metadata Overlay

Mit der Funktion „Auftragen auf das Metadaten-Overlay" können Sie Analyse-Erfassungen direkt in die Kamera ziehen. Die Erfassungsen sind grafische Overlays in Form von Begrenzungsfeldern und Bewegungslinien. Die Videostreams werden anhand ihrer Auflösung und, falls das Gerät Sichtbereiche unterstützt, in einem Sichtbereich ausgewählt. Die aufgetragenen Metadaten werden in der Live-Ansicht und während der Wiedergabe von aufgezeichnetem Material angezeigt.

Aufgetragene Metadaten-Overlays in ausgewählten Streams

Sie können die Anwendung z. B. so einstellen, dass sie Overlays für alle Videostreams mit der Auflösung 640x480 hinzufügt. Dann werden nur die Videostreams mit dieser Auflösung mit einem Overlay versehen, die übrigen bleiben unverändert.

Aufgetragene Metadaten-Overlays in ausgewählten Sichtbereichen

Wenn sie unterstützt werden, können Sie auch einen Sichtbereich zusammen mit der Auflösung anzeigen. Sie können zum Beispiel Overlays nur auf Streams aus Sichtbereich 3 mit Auflösung 1280x720 legen lassen. In diesem Fall werden nur die Videostreams, die dieser Konfiguration entsprechen, mit Overlays versehen, während die übrigen Videostreams unverändert bleiben, einschließlich derjenigen, die aus dem Sichtbereich 3, aber mit einer anderen Auflösung abgerufen werden, und derjenigen, die mit 1280x720, aber nicht aus dem Sichtbereich 3 abgerufen werden.

Hinzufügen von aufgetragenen Metadaten zum Videostream

Hinweis

Diese Funktion ist nur auf Geräten mit Software 7.30 oder höher verfügbar.

In diesem Beispiel wird erklärt, wie man aufgetragene Metadaten-Overlays für alle Video-Streams mit der Auflösung 640x480 aktiviert. Videostreams mit anderen Auflösungen bleiben davon unbeeinflusst.

1. Wählen Sie im Bereich mit Live-Ansichten die Option Kamera aus.
2. Navigieren Sie zu **Ausgänge > Aufgetragenes Metadaten-Overlay**.
3. Wählen Sie **Aktiviert**.
4. Wählen Sie in der Dropdownliste die Auflösung 640 x 480.
5. Klicken Sie auf **Anwenden**.
6. Stellen Sie sicher, dass die Metadaten in der Live-Ansicht für diese Auflösung angezeigt werden.

VMS-Integration

AXIS Perimeter Defender integriert sich nahtlos in folgende Videoverwaltungssysteme (VMS):

- Sicherheitscenter von Genetec™
- XProtect® von Milestone

Weitere Informationen zu unterstützten VMS-Versionen finden Sie unter *axis.com/products/axis-perimeter-defender/support-and-documentation*

Von AXIS Perimeter Defender ausgelöste Alarme werden automatisch in Ereignisse im VMS umgewandelt, die wiederum eine breite Palette von Aktionen auslösen und die gesamten Möglichkeiten des VMS nutzen können. Gleichzeitig werden die von AXIS Perimeter Defender generierten Live-Metadaten zur Live-Anzeige und -Aufzeichnung an das VMS gesendet. Daher stehen die Metadaten auch zur Verfügung, wenn die aufgezeichneten Videosequenzen im Wiedergabemodus wiedergegeben werden.

Ein automatisches Eindringerkennungssystem dient zum Auslösen von Alarmen und zur Bereitstellung von Informationen, die über die Sicherheitsmaßnahmen informieren. Dazu gehören möglicherweise eine Eingabeaufforderung an ein mobiles Gerät oder das Anzeigen des Alarmereignisses innerhalb eines VMS, möglicherweise mit dem Betreff, der das Alarmereignis erzeugt hat, das auf dem Bildschirm hervorgehoben wird.

Standard-Ereignisintegration

AXIS Perimeter Defender nutzt und erweitert die nativen ACAP-Schnittstellen und -Funktionen zum Senden von Alarmen und zusätzlichen Informationen an externe Geräte oder VMS. Von AXIS Perimeter Defender gemeldete Ereignisse können in Nachrichten an das VMS übersetzt werden, indem man Aktionsregeln mit ihnen verknüpft.

Folgende Alarmkanäle von der Kamera zu den VMS stehen zur Verfügung:

- Grundlegende Freitext-Benachrichtigungen für Alarme (TCP/IP)
- Elektrische Ausgänge (trockene oder feuchte Kontakte)
- E-Mail-Benachrichtigungen
- FTP-Upload von Alarmbildern

Diese Integrationen können auf der Kamera konfiguriert werden. Siehe *Nachalarmzeit, on page 35*.

VMS-Brücken

Für die folgenden Videoverwaltungssysteme stellen wir vorentwickelte Integrationsmodule bereit, die als „Brücken" bezeichnet werden:

- Milestone XProtect® 2014 und 2016 Corporate/Expert/Enterprise/Professional/Express: Die Editionen Enterprise/Professional/Express unterstützen keine Metadaten (keine Live- oder Wiedergabe-Anzeige von Metadaten)
- Genetec™ Service Center 5.3 und 5.4 Pro/Enterprise/SV32/SV16

Die Brücken bieten zwei Integrationen:

- Erstellen Sie benutzerdefinierte Alarmereignisse im VMS, die der Ereignisausgabe von AXIS Perimeter Defender entspricht.
- Anzeigen von Alarm-Overlays oder Begrenzungsfeldern, Live- und aufgezeichnetes Videomaterial (mit Ausnahme von Milestone XProtect® Enterprise/Professional/Express-Editionen).

Sie müssen die VMS-Brücken als separate Anwendungen herunterladen und installieren. Weitere Informationen zum Installieren und Konfigurieren dieser Brücken finden Sie im Benutzerhandbuch für die jeweilige Bridge.

Eine Regel in AXIS Camera Station erstellen

In diesem Bereich wird erläutert, wie der AXIS Perimeter Defender mit dem AXIS Camera Station Ereignissystem integriert wird. Es wird beschrieben, wie Sie:

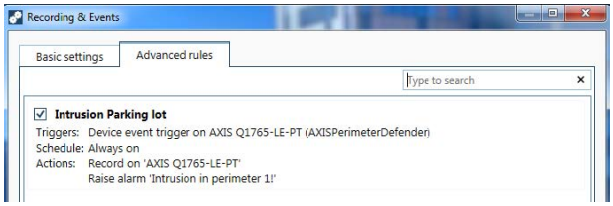
- Eine Regel für die AXIS Camera Station konfigurieren, um einen Alarm bei einem Einbruch auszulösen.
- Überprüfen, ob die Konfiguration korrekt durchgeführt wurde.

1. Den AXIS Perimeter Defender in der AXIS Perimeter Defender Setup-Software konfigurieren und kalibrieren. In dem AXIS Perimeter Defender Benutzerhandbuch oder unter *oder der Produktseite* erhalten Sie Hilfe bei der Installation und Kalibrierung des AXIS Perimeter Defender.

2. Um die Kamera zu AXIS Camera Station hinzuzufügen, dem Assistenten für **Add Camera (Kamera hinzufügen)** folgen.
3. Einen Geräte-Ereignisauslöser konfigurieren:
   3.1. Gehen Sie zu **Konfiguration** > **Aufzeichnung und Ereignisse** und rufen Sie den Tab **Erweiterte Regeln** auf.
   3.2. Erstellen Sie eine neue Regel und wählen Sie den **Geräte-Ereignis**auslöser.
   3.3. Wählen Sie die Kamera, auf der AXIS Perimeter Defender installiert ist.
   3.4. Wählen Sie **AXISPerimeterDefender** aus der **Ereignis**-Liste aus.
   3.5. In der **Funktions**-Liste wählen Sie den Namen der konfigurierten Einbruchsregel (in diesem Fall Einbruch-1). Wenn Sie diese Regel für alle konfigurierten Szenarios auslösen möchten, wählen Sie **ALL_SCENARIOS** aus.
   3.6. Wählen Sie **Ja** aus, um die Aktionsregel auszulösen, wenn ein Einbruch stattfindet. Wenn ein Einbruch erkannt wird, zeigt das Aktivitätsfenster eine Statusänderung an, mit der bestätigt wird, dass das Setup korrekt ist.
   3.7. Klicken Sie auf **OK** und **Nächste**, um die Aktionen zu konfigurieren.
   3.8. Im Dialogfenster **Aktion hinzufügen** können Sie eine oder mehrere Aktionen für die Regel hinzufügen.

In diesem Beispiel wird eine Aufnahmeaktion und eine Alarmaktion hinzugefügt.

   3.9. Klicken Sie auf **Finish** (Fertig).



Das Beispiel zeigt eine Regel, die zwei Aktionen auslöst, wenn ein Einbruch stattfindet.

4. Simulieren Sie einen Einbruch, z.°B. durch Betreten des überwachten Bereichs, um zu testen, ob die Konfiguration wie gewünscht funktioniert.

Weboberfläche

Ab AXIS Perimeter Defender 4.0 haben Sie Zugriff auf eine Weboberfläche, über die Sie Szenarien konfigurieren können, ohne dass die Desktop-Anwendung installiert sein muss.

So gelangen Sie zur Weboberfläche:

- Öffnen Sie einen Webbrowser.
- Geben Sie die IP-Adresse des Geräts ein
- Wechseln Sie zu Apps
- Gehen Sie in der Liste zu **AXIS Perimeter Defender** und klicken Sie auf **Open (Öffnen)**.

Hinweis

Die Kalibrierung ist in der Weboberfläche noch nicht verfügbar. Verwenden Sie zur Kalibrierung der Kamera die Desktop-Anwendung. Weitere Informationen finden Sie unter *Kalibrieren – AXIS Perimeter Defender, on page 19*

Szenarien

Ein Einbruchszenario erstellen

Das Einbruchszenario löst einen Alarm aus, wenn ein Objekt in eine bestimmte Zone eindringt und länger als die vordefinierte Zeit in der Zone verbleibt.

Ein Einbruchszenario erstellen:

1. Rufen Sie in der Weboberfläche den Menüpunkt **Scenarios (Szenarien)** auf.
2. Klicken Sie auf **+ Create (+ erstellen)**.
3. Wählen Sie **Intrusion (Einbruch)**.
4. Klicken Sie auf **Select this template (Diese Vorlage auswählen)**.
5. Legen Sie einen benutzerdefinierten und aussagekräftigen Namen für das Szenario fest
6. Auswählen Sie den Typ der Objekte, die als Auslöser für einen Alarm dienen sollen.
7. Um die Standarderfassungszone anzupassen, ziehen Sie die Ankerpunkte in eine beliebige Richtung. Sobald ein Ankerpunkt verschoben wurde, werden neue Ankerpunkte erstellt, um die Form weiter anzupassen.
8. Wenn Sie unter **Intrusion zone (Einbruchszone)** nicht möchten, dass ein Objekt einen Alarm auslöst, sobald es die Zone betritt, stellen Sie die **Minimum presence in zone (Mindestverweildauer in der Zone)** ein.
9. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
10. **Save (Speichern)** anklicken.

Szenario für Zonenübergänge erstellen

Szenario für Zonenübergänge ist so designt, dass ein Alarm ausgelöst wird, wenn sich ein Objekt aus einer vordefinierten Zone in eine Sperrzone bewegt.

So erstellen Sie ein Szenario für Zonenübergänge:

1. Rufen Sie in der Weboberfläche den Menüpunkt **Scenarios (Szenarien)** auf.
2. Klicken Sie auf **+ Create (+ erstellen)**.
3. Wählen Sie **Zone crossing (Zonenübergang)**.
4. Klicken Sie auf **Select this template (Diese Vorlage auswählen)**.

5. Legen Sie einen benutzerdefinierten und aussagekräftigen Namen für das Szenario fest
6. Auswählen Sie den Typ der Objekte, die als Auslöser für einen Alarm dienen sollen.
7. Um die Standardzonen anzupassen, ziehen Sie die Ankerpunkte in eine beliebige Richtung. Sobald ein Ankerpunkt verschoben wurde, werden neue Ankerpunkte erstellt, um die Form weiter anzupassen.
8. Wenn Sie unter **Zone 1** nicht möchten, dass ein Objekt einen Alarm auslöst, sobald es die Zone betritt, stellen Sie die **Minimum presence in zone (Mindestverweildauer in der Zone)** ein.
9. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
10. Um festzulegen, welcher Bereich gesperrt werden soll, klicken Sie auf den Pfeil neben **Restricted zone entry (Zugang zum gesperrten Bereich)**. Standardmäßig ist **Zone 2** die gesperrte Zone.
11. Legen Sie die Parameter für **Zone 2** fest.
12. **Save (Speichern)** anklicken.

Ein bedingtes Szenario erstellen

Das bedingte Szenario bietet Ihnen die Möglichkeit, die Bedingungen für die Auslösung von Alarmen als Auslöser in einer Szene festzulegen.

So erstellen Sie ein bedingtes Szenario:

1. Rufen Sie in der Weboberfläche den Menüpunkt **Scenarios (Szenarien)** auf.
2. Klicken Sie auf **+ Create (+ erstellen)**.
3. Wählen Sie **Conditional (Bedingt)**.
4. Klicken Sie auf **Select this template (Diese Vorlage auswählen)**.
5. Legen Sie einen benutzerdefinierten und aussagekräftigen Namen für das Szenario fest
6. Auswählen Sie den Typ der Objekte, die als Auslöser für einen Alarm dienen sollen.
7. Wenn Sie mehr Zonen als die Standardanzahl benötigen, klicken Sie auf **+ Add zone (+ Zone hinzufügen)**
8. Wählen Sie im Drop-Down Menü unter **Intrusion Zone (Einbruchzone)** die Zone aus, die als Einbruchzone dienen soll. Die Pfeile zeigen die Lage der verschiedenen Zonen im Verhältnis zur gewählten Einbruchszone an.
9. Um die Standardzonen anzupassen, ziehen Sie die Ankerpunkte in eine beliebige Richtung. Sobald ein Ankerpunkt verschoben wurde, werden neue Ankerpunkte erstellt, um die Form weiter anzupassen.
10. Wenn Sie nicht möchten, dass ein Objekt einen Alarm auslöst, sobald es den Bereich betritt, stellen Sie die Option **Minimum presence in zone (Mindestverweildauer im Bereich)** ein.
11. Wenn der Bereich schmal ist und in 1-2 Sekunden durchquert werden kann, aber die Alarme trotzdem ausgelöst werden sollen, wählen Sie die Option **Narrow Zone (schmaler Bereich)** aus. Weitere Informationen finden Sie unter *Parameter Verweildauer, on page 27*.
12. **Save (Speichern)** anklicken.

Szenarien bearbeiten

So bearbeiten Sie ein Szenario, das Sie in der Weboberfläche oder in der Desktop-App erstellt haben:

1. Rufen Sie in der Weboberfläche den Menüpunkt **Scenarios (Szenarien)** auf.
2. Klicken Sie bei dem Szenario, das Sie bearbeiten möchten, auf **Edit (Bearbeiten)**.
3. Klicken Sie auf **Save (Speichern)**, sobald Sie fertig sind.

Szenarien umbenennen

So ändern Sie die Namen mehrerer Szenarien gleichzeitig:

1. Wählen Sie die Szenarien aus, die Sie umbenennen möchten
2. Klicken Sie auf **Rename (Umbenennen)**, das nun im Menü verfügbar ist.
3. Ändern Sie die Namen nach Belieben.
4. **Save (Speichern)** anklicken.

Szenarien löschen

So löschen Sie mehrere Szenarien auf einmal:

1. Wählen Sie die Szenarien aus, die Sie löschen möchten
2. Klicken Sie auf **Delete (Löschen)**, das nun im Menü verfügbar ist.
3. Klicken Sie zur Bestätigung auf **Delete (Löschen)**.

Einstellungen

Die Weboberfläche verfügt über eine integrierte Hilfe mit Informationen zu den verschiedenen Einstellungen auf jeder Seite. Klicken Sie auf das Hilfe-Symbol (?), um auf das Fenster zuzugreifen.

Fehlerbehebung

Damit alle Funktionen wie erwartet funktionieren, müssen folgende Axis Parameter konfiguriert werden:

- Netzwerk/TCP-IP/Grundlegende/Standardrouter
- Netzwerk/TCP-IP/Erweitert/Domänenname
- Netzwerk/TCP-IP/Primärer DNS-Server
- Netzwerk/TCP-IP/Sekundärer DNS-Server
- Netzwerk-/TCP-IP/NTP-Server-Adresse
- Netzwerk/TCP-IP/SMTP (E-Mail)
- Systemoptionen/Datum und Uhrzeit/Zeitzone
- Systemoptionen/Datum und Uhrzeit/mit NTP-Server synchronisieren

Aktualisieren auf die neueste Version

Um die neuesten Verbesserungen nutzen zu können, ohne Szenarien neu kalibrieren und definieren zu müssen, empfehlen wir Ihnen, ein Upgrade auf die neueste Version von AXIS Perimeter Defender durchzuführen.

1. Laden Sie die neueste Version von AXIS Perimeter Defender herunter und installieren Sie sie.
2. **Installieren** anklicken. AXIS Perimeter Defender Setup führt automatisch die erforderlichen Schritte zum Abschluss der Installation aus:

– Sichern Sie die vorhandene Kalibrierung, Szenarien, Parameter und Lizenz.

– Installieren Sie die neue Version.

– Stellen Sie die Lizenz wieder her.

– Stellen Sie die Kalibrierung und Szenarien wieder her.

– Stellen Sie die Parameter wieder her.

– Wenn eine Anwendung ausgeführt wurde, wird sie neu gestartet.

Aktualisierung der Kamerasoftware

Hinweis

Speichern Sie vor dem Aktualisieren der Kamera-Software alle Einstellungen von AXIS Perimeter Defender. Durch die Aktualisierung der Software werden die Anwendung und Ihre Einstellungen aus der Kamera gelöscht. Wenn die Einstellungen gespeichert werden, können Sie mit dem AXIS Perimeter Defender Setup wiederhergestellt werden.

1. Verwenden Sie das AXIS Perimeter Defender Setup, um die Standortkonfiguration zu speichern.
2. Aktualisieren Sie die Kamerasoftware. Anweisungen dazu finden Sie im Benutzerhandbuch der Kamera.
3. Starten Sie das AXIS Perimeter Defender Setup.
4. Verwenden Sie die Option „Standort laden“, um die gespeicherte Standortkonfiguration für jede aktualisierte Kamera automatisch zu laden.

Fehlerbehebung bei der Installation

Problem	Möglicher Grund	Lösung
Es wird eine Windows® Meldung angezeigt, die besagt, dass die Software nicht installiert werden kann.	Das Betriebssystem auf dem Laptop oder PC ist nicht kompatibel.	Überprüfen Sie, ob das Windows® Betriebssystem der Version in den Anforderungen entspricht.
Es gibt eine Windows® Meldung, dass die Installation nicht korrekt durchgeführt wurde.	DerWindows® Kompatibilitätsassistent hat ein mögliches Problem mit der Installation festgestellt.	Stellen Sie sicher, dass die Installation trotzdem korrekt ist und fahren Sie fort.
Während der Installation von Xvid wird die Installation abgebrochen.	Die Installation von Xvid wird abgebrochen aufgrund einer alten Teilinstallation von Xvid auf dem Computer.	Löschen Sie den Ordner Xvid unter C:\Program Files (x86) und versuchen Sie es erneut.
Das Installationspaket stürzt nach dem Anzeigen der EULA plötzlich ab. Es gibt eine Windows® Fehlermeldung, die besagt, dass die Anwendung auf ungewöhnliche Weise beendet wurde. Es ist nicht möglich, das Installationsprogramm zu schließen.	Ein bekanntes Problem im Installationsprogramm führt unter bestimmten Umständen zu einem Anwendungsabsturz.	Öffnen Sie den Task-Manager und beenden Sie alle „msiexec. exe"-Prozesse. Beenden Sie dann den Installations-Vorgang und starten Sie ihn neu.

Fehlerbehebung bei der Konfiguration

Problem	Möglicher Grund	Lösung
Probleme beim Öffnen von AXIS Perimeter Defender	Sie verfügen nicht über genügend Windows® Benutzerrechte.	Stellen Sie sicher, dass Sie über Administratorrechte verfügen.
Die Suchfunktion findet meine Kameras nicht.	Firewall	Es kann manchmal vorkommen, dass durch Firewalls und Antivirensoftware Kameras nicht erkannt werden. Konfigurieren Sie bei Bedarf die Firewall so, dass der Netzwerk-Verkehr zu und von AXIS Perimeter Defender zugelassen wird. Sollte das Problem weiterhin bestehen, konfigurieren Sie die Firewall so, dass folgende Ports zugelassen werden: UDP Port 5353 und TCP Port 80.
	Probleme mit der IP-Adresse	Jedes Gerät im Netzwerk muss über eine eindeutige IP-Adresse verfügen, um mit anderen Geräten kommunizieren zu können. Bei der Verwendung von AXIS Perimeter Defender wird empfohlen, für die Kameras feste IP-Adressen zu verwenden. Stellen Sie sicher, dass jedes IP-Gerät im Netzwerk über eine eigene IP-Adresse verfügt und

Problem	Möglicher Grund	Lösung
		die bereits verwendete IP-Adresse nicht erneut genutzt werden kann.
	Die Kamera ist nicht auf dem Benutzer-Computer verfügbar.	Rufen Sie in einem Browser die IP-Adresse der Kamera auf, um zu bestätigen, ob sie verfügbar ist. Wenn Sie die Kamera nicht erreichen können, wurde sie nicht ordnungsgemäß im Netzwerk installiert oder der Computer hat keinen Zugriff auf die Kamera.
Es kann keine Kamera hinzugefügt werden.	Kamera-Verbindungsparameter wie z. B. IP-Adresse, Kennwort oder HTTP-Port sind falsch.	Überprüfen Sie, ob die eingegebenen Parameter korrekt sind und wiederholen Sie den Vorgang.
	Die Kamera kann auf dem Benutzer-Computer nicht angezeigt werden.	Rufen Sie in einem Browser die IP-Adresse der Kamera auf, um zu bestätigen, ob sie verfügbar ist. Wenn Sie die Kamera nicht erreichen können, wurde sie nicht ordnungsgemäß im Netzwerk installiert oder der Computer hat keinen Zugriff auf das Netzwerk, in dem sich die Kamera befindet.
Verlust von Videostreams im AXIS Perimeter Defender Setup.	Die Videoquelle ist nicht mehr verfügbar.	Die Videoquelle wurde unterbrochen und wird nicht auf dem Bildschirm aktualisiert.
	Überprüfen Sie mit einem Browser, ob die Kamera verfügbar ist.	Klicken Sie auf die Kachel, in der sich der Stream befinden soll, und ändern Sie die Größe der Schnittstelle und der Stream sollte zurückkommen.
Die automatische Kalibrierung funktioniert nicht oder liefert schlechte Ergebnisse.	Die Voraussetzungen werden nicht erfüllt.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Kamera verfügt über eine Rolle.	Es ist nicht möglich, die Kamera mit einer Rolle zu kalibrieren.
	Die Verbindung zu einer Kamera, die nicht als ferngesteuert konfiguriert ist, ist langsam.	Schließen Sie die Kamera als ferngesteuert an, um den Bedarf an Bandbreite zu verringern.
	Für die automatische Kalibrierung werden andere sich bewegende Objekte in der Szene verwendet, wie z. B. Autos, Bäume oder andere Personen.	Wiederholen Sie die automatische Kalibrierung oder kalibrieren Sie das Gerät manuell.
	Das Sichtfeld ist unübersichtlich, sodass die Person, die vor der Kamera geht, für einen längeren Zeitraum teilweise verborgen ist.	Kalibrieren Sie das Gerät manuell.

Problem	Möglicher Grund	Lösung
	Das Sichtfeld ist so klein wie Eingänge.	Kalibrieren Sie das Gerät manuell.
	Das Aufnahmevideo wurde aufgrund von unzureichendem Speicherplatz nicht ordnungsgemäß aufgezeichnet.	Stellen Sie sicher, dass genügend Speicherplatz vorhanden ist und dass die Anwendung berechtigt ist, die Videoaufzeichnung auf dem Computer zu speichern, auf dem die AXIS Perimeter Defender Schnittstelle ausgeführt wird.

Fehlerbehebung im Betrieb

Problem	**Möglicher Grund**	**Lösung**
Die Anwendung wird nicht ausgeführt, obwohl die Konfiguration in Ordnung ist.	Die Software der Kamera ist nicht aktuell.	Stellen Sie sicher, dass die aktuelle Kamerasoftware geladen ist.
Das Overlay wird nicht im AXIS Perimeter Defender Setup angezeigt, obwohl die Analyse ausgeführt wird.	Die Anwendung wird nach einem Start- oder Stopp-Vorgang oder einer Aktualisierung des AXIS Perimeter Defender Pakets blockiert.	Starten Sie die Kamera neu.
	Eine Firewall blockiert die Verbindung zum Empfangsport der Kamera-Metadaten.	Konfigurieren Sie die Firewall, sodass die Konfigurationsschnittstelle eine Verbindung zum Empfangsport für Metadaten der Kamera herstellen kann.
	Ein Antivirusprogramm blockiert den Empfang des Overlays.	Konfigurieren Sie den Antivirenschutz, damit das Overlay empfangen werden kann.
Im AXIS Perimeter Defender Setup auf dem Konfigurationscomputer werden keine Alarme ausgelöst, obwohl die Analyse ausgeführt wird und das Overlay sichtbar ist.	Obwohl sich das Ziel in der Szene befindet, entspricht es nicht einem Bedingungsszenario, z. B. nicht beim Übergang von einer Zone in eine andere.	Stellen Sie sicher, dass das Szenario korrekt angegeben ist, einschließlich der Bedingungen.
	Schlechte Erfassung.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*. Stellen Sie außerdem sicher, dass die Kalibrierung präzise genug und die Empfindlichkeit hoch genug ist.

Fehlerbehebung bei der Leistung

Problem	Möglicher Grund	Lösung
Das OSD und die Analyse werden immer ein- und ausgeschaltet.	Die CPU-Belastung der Kamera ist zu hoch.	Mögliche Lösungen: • Stellen Sie sicher, dass Videostreams nicht unnötig visualisiert werden, da jede Instanz die CPU-Belastung erhöht. • Wenn die Aufzeichnung bei eingebauter Bewegungserkennung aktiviert ist, versuchen Sie, die Aufzeichnungsqualität zu verringern, um CPU-Kapazität freizugeben. • Deaktivieren Sie die Aufzeichnung nach Bewegungserkennung und stellen Sie sicher, dass die Bewegungserkennung deaktiviert ist.
Die Bildrate des angezeigten Videos ist sehr niedrig.	Zu viele Videostream-Visualisierungen können dazu führen, dass die Bildrate unter den Standardwert von 8 Bildern pro Sekunde fällt.	Stellen Sie sicher, dass Videostreams nicht unnötig visualisiert werden, da jede Instanz die CPU-Belastung erhöht.
Eine Zielperson dringt in die sterile Zone ein und löst mehrere Alarme aus.	Die Nachalarmdauer ist zu kurz.	Passen Sie die Nachalarmdauer an. Navigieren Sie zu AXIS Perimeter Defender Setup > **Ausgänge**.
Eine potenzielle Zielperson dringt in die sterile Zone ein, löst jedoch keinen Alarm aus und wird deshalb nicht erfasst.	Der Kontrast des Objekts vor dem Hintergrund ist zu gering.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Beleuchtung der Szene ist unzureichend oder die Leistung der Kamera bei schwachem Licht ist unzureichend.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Empfindlichkeit von AXIS Perimeter Defender ist zu niedrig eingestellt.	Erhöhen Sie die Empfindlichkeit der globalen Szenario-Parameter.
	Die Kamera wurde bewegt, sodass die Kalibrierung nun falsch ist.	Wiederholen Sie die Kalibrierung.
	Die Kalibrierung ist nicht präzise genug.	Überprüfen Sie die Kalibrierung der Kamera. Navigieren Sie zum AXIS Perimeter Defender Setup.
	Obwohl sich das Ziel in der Szene befindet, entspricht es keinem bedingten Szenario. Im Szenario der Zonenüberquerung beispielsweise bewegt sich das	Stellen Sie sicher, dass das Szenario korrekt angegeben ist, einschließlich seiner Bedingungen.

Problem	Möglicher Grund	Lösung
	Objekt nicht von einer Zone zur anderen.	
Das Ziel wird erfasst, jedoch falsch klassifiziert (Person als Fahrzeug oder Fahrzeug als Person).	Die Höhe, Positionierung oder Ausrichtung der Kamera ist falsch.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Kamera ist zu weit von der Zone entfernt.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Kalibrierung ist nicht präzise genug.	Überprüfen Sie die Kalibrierung der Kamera. Navigieren Sie zum AXIS Perimeter Defender Setup.
AXIS Perimeter Defender generiert einen Alarm, wenn kein Eindringen in die sterile Zone erfolgt.	Die Empfindlichkeit der Analyse ist zu hoch.	Verringern Sie die Empfindlichkeit. Navigieren Sie zum AXIS Perimeter Defender Setup.
	Die Kalibrierung ist nicht präzise genug.	Überprüfen Sie die Kalibrierung der Kamera. Navigieren Sie zum AXIS Perimeter Defender Setup.
	Die Kamera wurde bewegt, sodass die Kalibrierung nun falsch ist.	Wiederholen Sie die Kalibrierung.
	Falsche Höhe, Positionierung oder Ausrichtung der Kamera.	Stellen Sie sicher, dass die Montageanforderungen erfüllt sind. Siehe *Montieren der Kamera, on page 13*.
	Die Kamera bewegt sich, schwankt oder vibriert.	Befestigen Sie die Kamera stabiler.
	Vegetation, Flaggen oder andere bewegliche Objekte in der Nähe der Kamera.	Entfernen Sie die problematischen Objekte aus dem Sichtfeld der Kamera. Objekte, die sich ständig in der Szene befinden, jedoch nicht nah an der Kamera sind, werden von AXIS Perimeter Defender ignoriert.
	Insekten auf oder in der Nähe des Kameraobjektivs.	Verhindern Sie, dass Insekten auf oder in die Nähe des Kameraobjektivs gelangen.

Über dieses Handbuch

Dieses Handbuch ist für Administratoren und Benutzer von AXIS Perimeter Defender vorgesehen. Es enthält Anweisungen zum Verwenden und Verwalten des Produkts im Netzwerk. Für die Verwendung dieses Produkts sind Erfahrungen mit Netzwerktechnologie von Vorteil.

Hinweise zu Markenzeichen

AXIS COMMUNICATIONS, AXIS, ARTPEC und VAPIX sind in verschiedenen Jurisdiktionen eingetragene Marken von Axis AB. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Apple, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows und WWW sind eingetragene Markenzeichen der jeweiligen Inhaber. Java und alle auf Java basierenden Markenzeichen und Logos sind Markenzeichen oder eingetragene Markenzeichen von Oracle und/oder seiner Tochterunternehmen. Das Warenzeichen und das Logo UPnP sind in den USA und anderen Ländern Markenzeichen der Open Connectivity Foundation Inc.

Genetec ist ein Markenzeichen und Milestone XProtect® ist ein eingetragenes Markenzeichen der jeweiligen Inhaber.

T10068952_de

2026-03 (M17.3)