AXIS Perimeter Defender

AXIS Perimeter Defender

AXIS Perimeter Defender PTZ Autotracking

Podręcznik użytkownika

AXIS Perimeter Defender

Spis treści

AXIS Perimeter Defender

AXIS Perimeter Defender

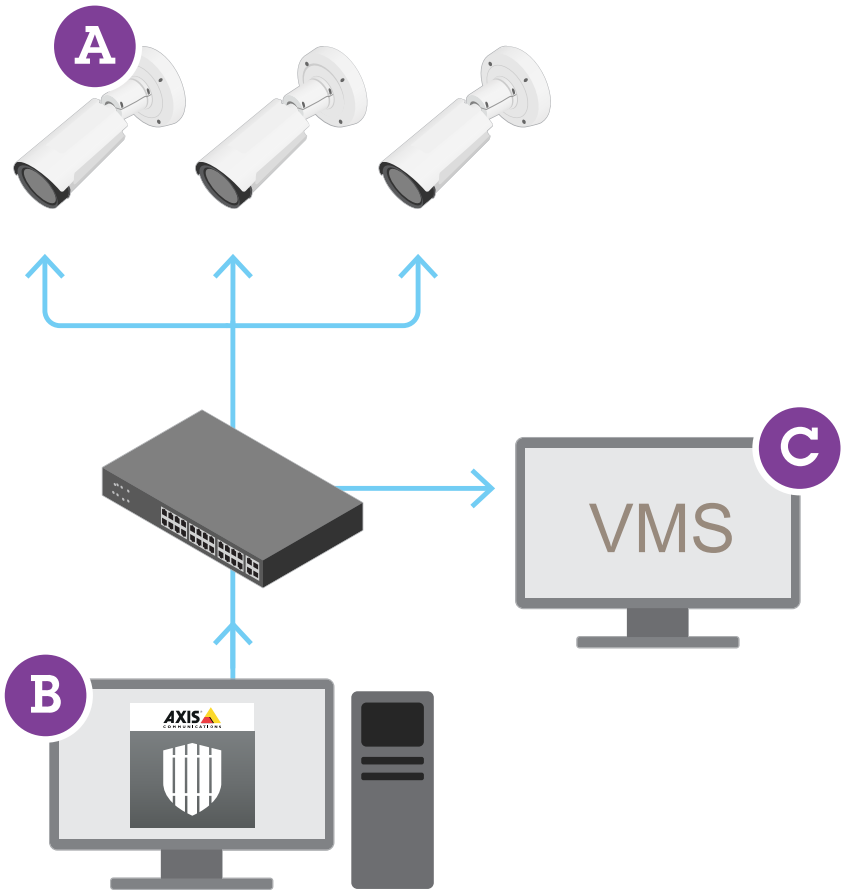
AXIS Perimeter Defender

AXIS Perimeter Defender to aplikacja do dozoru obwodowego i ochrony obwodowej. Nadaje się on idealnie do ochrony obwodowej tam, gdzie konieczne jest wzmocnienie systemu fizycznej kontroli dostępu poprzez dodanie niezawodnej detekcji wtargnięcia na teren.

AXIS Perimeter Defender jest przeznaczona przed wszystkim do ochrony tak zwanej strefy sterylnej, na przykład strefy wzdłuż płotu stanowiącego granicę obszaru. Termin „strefa sterylna" odnosi się do obszaru, w którym nie powinni znaleźć się ludzie.

Aplikacji AXIS Perimeter Defender można używać na zewnątrz pomieszczeń i budynków, aby:

- wykrywać poruszające się osoby,
- wykrywać poruszające się pojazdy bez rozróżniania ich typów.



Kamery termowizyjne AXIS Q1951-E i AXIS Q1952-E mogą uruchamiać aplikację w trybie kalibracji, w trybie AI lub w obu tych trybach jednocześnie. W przypadku uruchomienia aplikacji tylko w trybie AI montaż kamer jest bardziej elastyczny i nie trzeba ich kalibrować.

Aplikacja AXIS Perimeter Defender składa się z interfejsu (B) służącego do instalacji i konfiguracji aplikacji w kamerach (A). System można tak skonfigurować, aby wysyłał alarmy do oprogramowania do zarządzania materiałem wizyjnym (C).

AXIS Perimeter Defender

AXIS Perimeter Defender PTZ Autotracking to wtyczka do aplikacji AXIS Perimeter Defender, która korzysta z tego samego interfejsu. Wtyczka ta umożliwia sparowanie stałopozycyjnej kamery optycznej lub termowizyjnej z kamerą PTZ z serii Axis Q. Można wówczas zachować ciągłą detekcję w scenie za pomocą kamery stałopozycyjnej, podczas gdy kamera PTZ zapewnia automatyczne śledzenie i zbliżenia wykrytych obiektów.

Ważne

Wtyczka AXIS Perimeter Defender PTZ Autotracking wymaga kalibracji zarówno kamer stałopozycyjnych, jak i PTZ.

AXIS Perimeter Defender zawiera następujące typy scenariuszy detekcji:

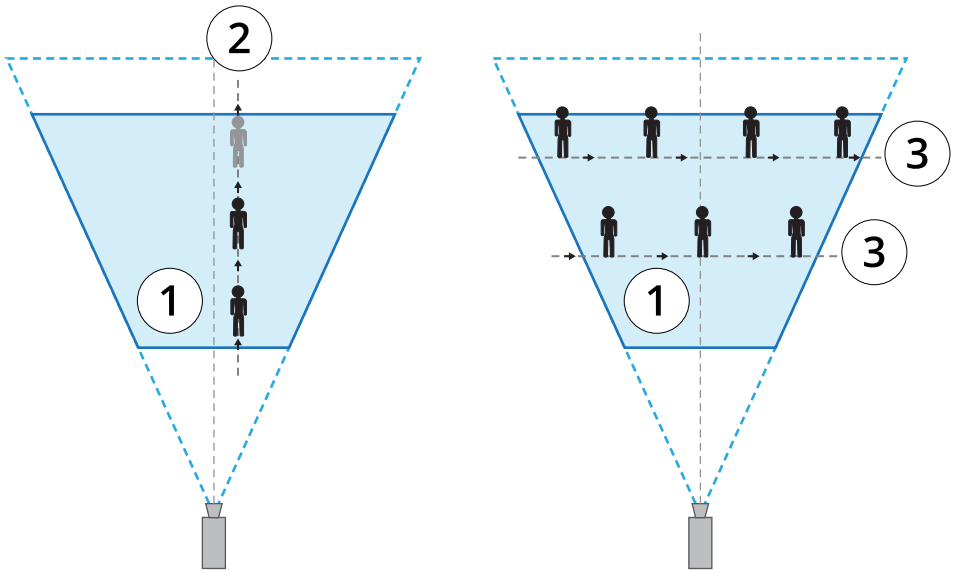
- **Wtargnięcie**: wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu (dowolny kierunek i trajektoria).
- **Podejrzane zachowania**: wyzwala alarm, kiedy osoba lub pojazd pozostaje w strefie zdefiniowanej na podłożu przez czas dłuższy niż podana liczba sekund.
- **Przekroczenie strefy**: wyzwala alarm, kiedy osoba lub pojazd przekracza w określonej sekwencji dwie lub większą liczbę stref zdefiniowanych na podłożu.
- **Warunkowy**: wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu, nie przekraczając wcześniej innych stref.

Jak to działa?

Wykrywanie obiektów

Aplikacja AXIS Perimeter Defender może wykrywać poruszające się osoby lub pojazdy. Aby detekcja była możliwa:

- osoba lub pojazd muszą być w całości widoczne w strefie detekcji przez co najmniej trzy sekundy;
- długość pojazdu nie może przekraczać 12 metrów (39,4 stopy) (w przypadku trybu AI nie obowiązuje ograniczenie długości);
- osoby lub pojazdy muszą poruszać się w polu widzenia kamery — oznacza to, że poziom detekcji osób, które zbliżają się do kamery lub oddalają się od niej w linii prostej, jest niższy niż w przypadku osób przechodzących prostopadle do pola widzenia kamery.

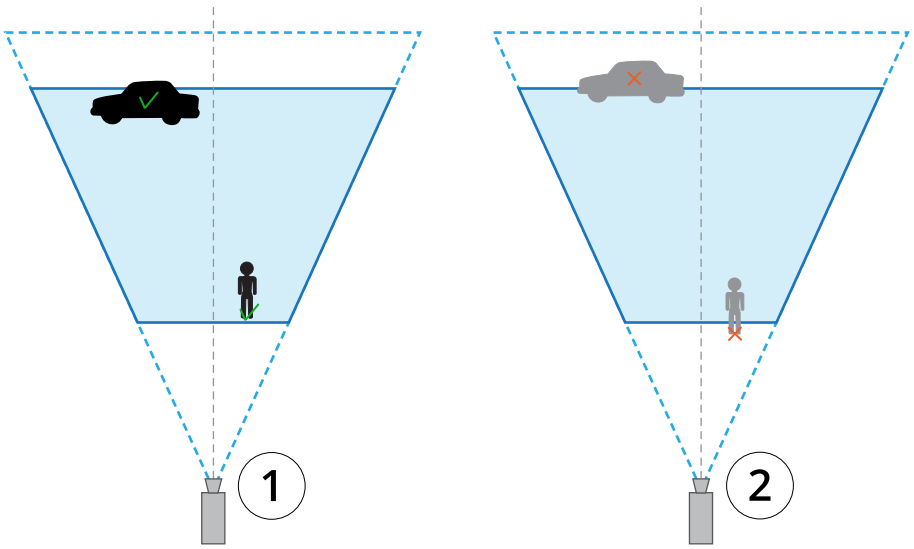


1 Strefa detekcji
2 Osoba oddala się od kamery

AXIS Perimeter Defender

3 *Osoby przechodzi prostopadle do pola widzenia kamery*

- punkt detekcji musi znajdować się w obrębie strefy detekcji. Punkt detekcji osoby to jej stopy, a punkt detekcji pojazdu znajduje się na jego środku.



1 *Punkt detekcji w obrębie strefy detekcji*
2 *Punkt detekcji poza strefą detekcji*

Po wykryciu osoby lub pojazdu aplikacja AXIS Perimeter Defender śledzi tę osobę lub pojazd, nawet jeśli są częściowo zakryte, na przykład w sytuacji, gdy dana osoba jest schowana za samochodem i widać tylko jej głowę.

Jeżeli wykryta osoba lub pojazd przestaną poruszać się przez kilka sekund, to aplikacja AXIS Perimeter Defender przestanie je śledzić. Jeśli osoba lub pojazd zaczną poruszać się ponownie zanim upłynie 15 sekund, aplikacja wznowi śledzenie. Jeżeli dana osoba znajdowała się w obszarze przekraczania strefy, scenariusz mógł nie zostać wyzwolony prawidłowo.

Jak działa funkcja automatycznego śledzenia PTZ?

AXIS Perimeter Defender PTZ Autotracking to aplikacja umożliwiająca wspólne działanie kamery stałopozycyjnej i kamery PTZ. Kiedy kamera stałopozycyjna wykryje poruszające się osoby lub pojazdy, wysyła dane o lokalizacji obiektów do sparowanej kamery PTZ. Dzięki temu kamera PTZ może automatycznie:

- śledzić obiekty i
- dostosować poziom zoomu, by objąć wszystkie obiekty śledzeniem

pod warunkiem, że obiekty znajdują się w polu widzenia kamery stałopozycyjnej.

Warunki powodujące opóźnienie lub brak detekcji

- Mgła
- Światło skierowane na kamerę
- Niewystarczające oświetlenie
- Nadmierny szum na obrazie

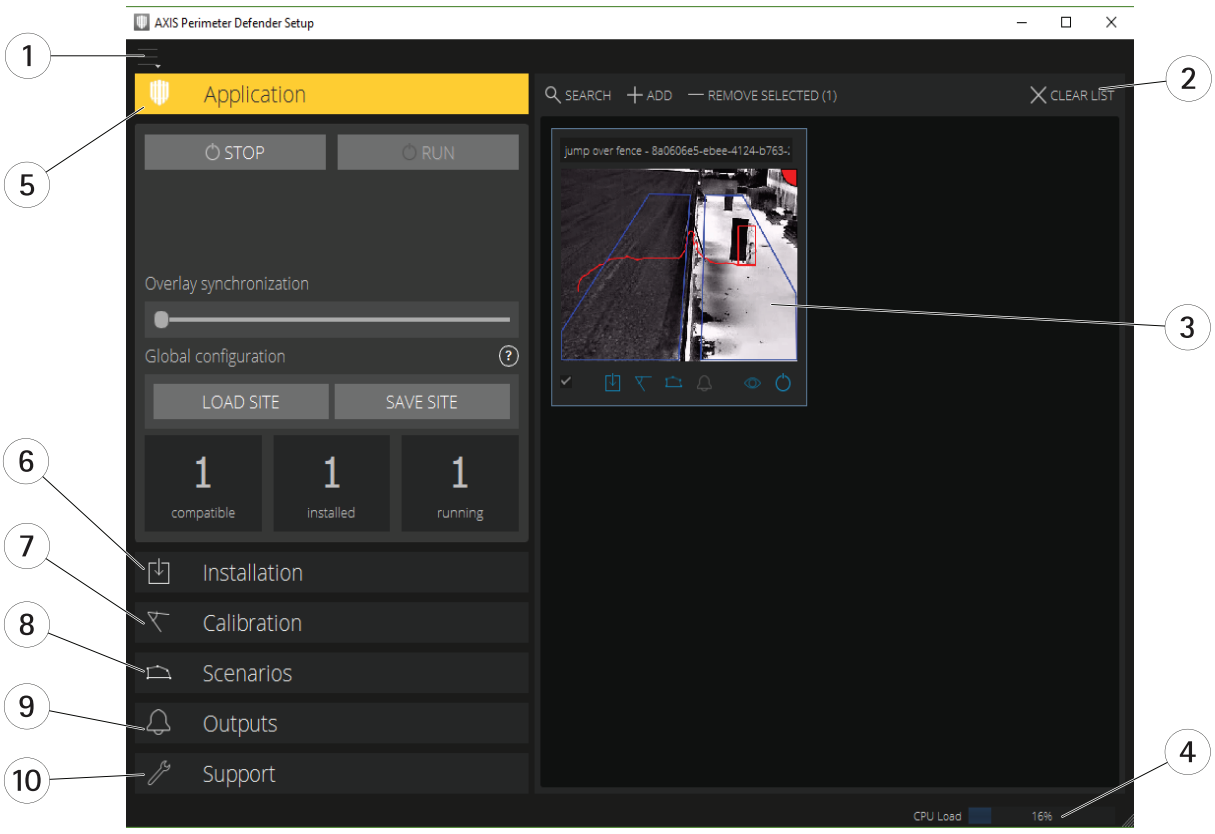
AXIS Perimeter Defender

Sytuacje, które mogą wyzwalać fałszywe alarmy

- Częściowo zakryte osoby lub pojazdy. Na przykład mała furgonetka wyjeżdżająca zza budynku może wyglądać jak osoba, ponieważ widoczna część jest wysoka i wąska.
- Owady na obiektywie kamery. Kamery rejestrujące obraz w dzień i w nocy oraz kamery z oświetleniem w podczerwieni przyciągają owady i pająki.
- Reflektory przejeżdżających pojazdów i ulewny deszcz.
- Zwierzęta o rozmiarach człowieka, zwłaszcza po wybraniu dodatkowych typów zbliżania się (np. czołganie się) na karcie **Scenariusze**.
- Silne oświetlenie powodujące powstawanie cieni.

Interfejs użytkownika

Interfejs aplikacji AXIS Perimeter Defender umożliwia na przykład kalibrację urządzeń, konfigurację scenariuszy i wykonywanie działań dotyczących wielu urządzeń. Konfiguracja zdalna umożliwia konfigurację z dowolnego miejsca z dostępem do sieci.



1 *Ustawienia interfejsu na stronie 7*
2 *Obsługa urządzeń. Patrz Dodawanie urządzeń na stronie 17.*
3 *Podgląd na żywo na stronie 7*
4 *Wskaźnik obciążenia procesora. Patrz Obciążenie procesora na stronie 11.*
5 *Karta Aplikacja na stronie 9*
6 *Karta Instalacja na stronie 9*
7 *Karta Kalibracja na stronie 10*
8 *Karta Scenariusze na stronie 10*
9 *Karta Wyjście na stronie 11*

AXIS Perimeter Defender

10 Karta Pomoc techniczna na stronie 11

Ustawienia interfejsu

Menu ustawień interfejsu zawiera następujące elementy:

Ustawienia folderu –
Ścieżka konfiguracji urządzenia: wybierz lokalizację, w której mają być przechowywane pliki tymczasowe i obraz wideo do kalibracji.
Ścieżka konfiguracji lokalizacji: wybierz lokalizację przechowywania załadowanych plików konfiguracji.

Hasła do kamer – przeglądanie wykorzystywanych haseł i dodawanie nowego hasła. Po zamknięciu aplikacji hasła nie zostaną zapisane.

Zarządzaj pakietami klipów pokazowych – Opcja ta umożliwia importowanie lub usuwanie klipów pokazowych.

Włącz tryb pełnej poklatkowości – Opcja ta służy do zmiany poklatkowości na podglądzie na żywo. Patrz *Obciążenie procesora na stronie 11*.

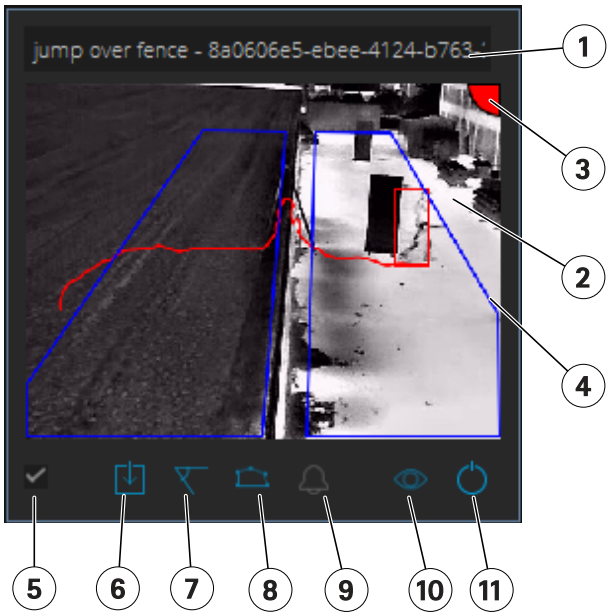
Wyświetl stopy i cale – Opcja ta służy do wyboru pomiędzy jednostkami metrycznymi a imperialnymi.

Zmień język – Opcja ta służy do zmiany języka aplikacji.

O programie – Opcja ta umożliwia sprawdzenie numer wersji aplikacji AXIS Perimeter Defender Setup.

Podgląd na żywo

Każde podłączone urządzenie ma widok podglądu na żywo na głównym interfejsie. W widoku na żywo wyświetlany jest stan urządzenia oraz opcje szybkiego dostępu do najważniejszych funkcji.



1. Nazwa urządzenia – Kliknij, aby edytować nazwę urządzenia. Zawiera ona zawsze adres IP i numer MAC urządzenia. Przesuń kursor nad nazwę urządzenia, aby wyświetlić współczynnik proporcji wykorzystywany do analizy, który zapewnia maksymalne pole widzenia i sprawdzić, czy urządzenie to jest podłączone zdalnie.

2. Obraz na żywo – W trybie widoku ogólnego liczba klatek na sekundę wynosi 1. Kliknij dwukrotnie, aby zmaksymalizować obraz i zwiększyć liczbę klatek na sekundę do 8.

AXIS Perimeter Defender

3. Status alarmów – Status alarmów jest widoczny tylko wtedy, gdy nakładka jest aktywna, a aplikacja AXIS Perimeter Defender jest zainstalowana, skonfigurowana i uruchomiona. Szary kolor oznacza, że funkcje alarmu nie są aktywne lub że ustawienia konfiguracji są dopiero wczytywane. Kolor zielony oznacza, że funkcje alarmu są aktywne. Czerwony kolor oznacza wyzwolenie alarmu.

4. Strefy detekcji – Strefy detekcji są widoczne tylko wtedy, gdy nakładka jest aktywna, a aplikacja AXIS Perimeter Defender jest zainstalowana, skonfigurowana i uruchomiona.

5. Pole wyboru – Użyć tego pola wyboru, aby wybrać wiele urządzeń.

6. Stan instalacji i przycisk szybkiego dostępu – Przesuń kursor na ikonę, aby wyświetlić wersję aplikacji AXIS Perimeter Defender zainstalowanej w urządzeniu. Jeśli ikona zmieni się w , będzie to oznaczać, że dostępna jest nowsza wersja. Kliknij, aby otworzyć kartę Instalacja urządzenia. Kolor szary oznacza, że urządzenie nie jest zainstalowane. Kolor pomarańczowy oznacza, że urządzenie jest zainstalowane, ale nie ma ważnej licencji. Kolor niebieski oznacza, że urządzenie jest zainstalowane, a licencja jest ważna.

7. Stan kalibracji i przycisk szybkiego dostępu – Kliknij, aby otworzyć kartę Kalibracja urządzenia. Kolor szary oznacza, że urządzenie nie jest skalibrowane. Kolor niebieski oznacza, że urządzenie jest skalibrowane.

8. Stan scenariuszy i przycisk szybkiego dostępu – Kliknij, aby otworzyć kartę Scenariusze urządzenia. Kolor szary oznacza brak zdefiniowanych scenariuszy. Kolor niebieski oznacza, że zdefiniowano co najmniej jeden scenariusz.

9. Stan wyjść i przycisk szybkiego dostępu – Kliknij, aby otworzyć kartę Wyjścia urządzenia. Kolor szary oznacza, że nie skonfigurowano wyjść. Kolor niebieski oznacza, że skonfigurowano co najmniej jedno wyjście.

10. Stan nałożenia i przycisk przełącznika – Kliknij, aby włączyć lub wyłączyć nałożenie. Kolor szary oznacza, że nałożenie jest nieaktywne. Kolor niebieski oznacza, że nałożenie jest aktywne. Nałożenie jest wyświetlane jako ramka wokół wykrytych obiektów, a także jako ślad wskazujący trajektorię obiektów.

11. Stan pracy i przycisk przełącznika – Kliknij, aby włączyć/wyłączyć aplikację. Kolor szary oznacza, że aplikacja jest wyłączona. Kolor niebieski oznacza, że aplikacja jest uruchomiona.

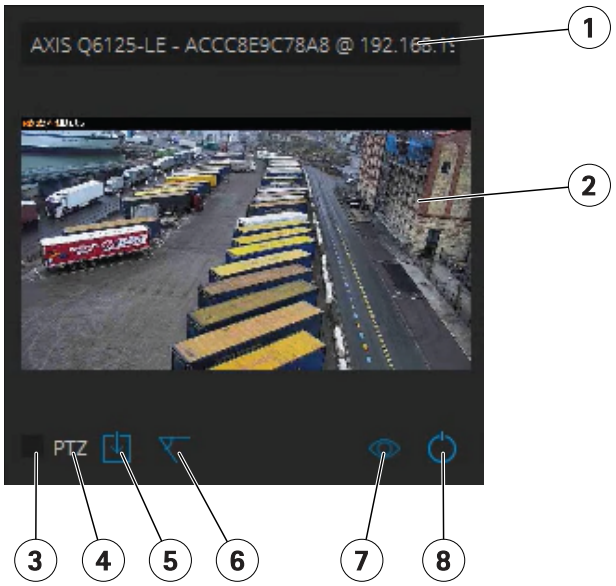
Uwaga

Nałożenie jest dostępne tylko wtedy, gdy dostępne jest bezpośrednie połączenie pomiędzy urządzeniem a komputerem użytkownika, czyli gdy nie zainstalowano zapór ogniowych ani innych zabezpieczeń uniemożliwiających podłączenie do portu nałożenia w urządzeniu.

Podgląd na żywo – PTZ Autotracking

Widok podglądu na żywo z urządzeń z aplikacją AXIS Perimeter Defender PTZ Autotracking różni się nieco od zwykłego podglądu na żywo.

AXIS Perimeter Defender



1 *Nazwa urządzenia*
2 *Obraz na żywo*
3 *Pole wyboru*
4 *Wskazuje, że urządzenie korzysta z aplikacji AXIS Perimeter Defender PTZ Autotracking*
5 *Stan instalacji i przycisk szybkiego dostępu*
6 *Stan kalibracji i przycisk szybkiego dostępu*
7 *Stan nałożenia i przycisk przełącznika*
8 *Stan pracy i przycisk przełącznika*

Karta Aplikacja

- **Uruchom** – służy do uruchamiania funkcji analizy w wybranych urządzeniach.
- **Zatrzymaj** – służy do zatrzymywania funkcji analizy w wybranych urządzeniach.
- **Wczytaj lokalizację** – wczytaj wcześniej zapisaną lokalizację, czyli urządzenia i stosowne pliki konfiguracji
- **Zapisz lokalizację** – zapisz bieżącą lokalizację, czyli wszystkie informacje o urządzeniach i stosowne pliki konfiguracji.
- **Synchronizacja nałożenia** – sterowanie synchronizacją nałożenia metadanych AXIS Perimeter Defender. Ten suwak służy do ustawiania opóźnienia pomiędzy nałożeniem metadanych a odebranymi obrazami w celu zrekompensowania wolniejszego strumieniowania obrazu w porównaniu z przesyłaniem metadanych. Wartość suwaka wskazuje opóźnienie ustawione dla bieżącej wybranej kamery. Jeżeli podłączono więcej niż jedną kamerę, podana wartość jest wartością dla pierwszej wybranej kamery. Zmiana wartości powoduje zmianę opóźnienia we wszystkich zaznaczonych kamerach.

Można również sprawdzić liczbę dodanych zgodnych urządzeń, liczbę urządzeń z zainstalowaną aplikacją AXIS Perimeter Defender oraz liczbę urządzeń, w których uruchomiono funkcje analizy.

Karta Instalacja

- **Aplikacja: instaluj** – służy do instalowania aplikacji na wybranych urządzeniach.
- **Aplikacja: odinstaluj** – służy do usuwania aplikacji z wybranych urządzeń.
- **Licencja: instaluj** – służy do instalowania licencji na wybranych urządzeniach.

AXIS Perimeter Defender

Karta Kalibracja

- **Automatyczna** — umożliwia automatyczną kalibrację wybranych urządzeń.
- **Ręczna** — umożliwia ręczną kalibrację wybranych urządzeń.

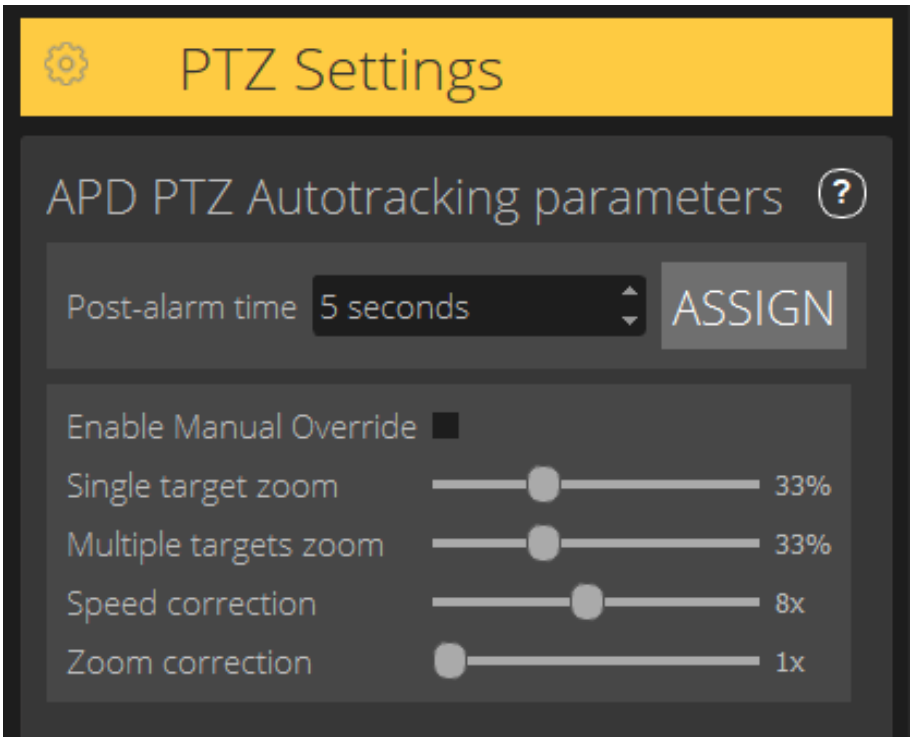
Karta Scenariusze

- **Parametry globalne** – parametry mające zastosowanie do wszystkich scenariuszy.
- **Scenariusze zaawansowane** – służą do tworzenia scenariuszy wtargnięcia, podejrzanych zachowań, przekroczenia strefy i scenariuszy warunkowych.

Karta Ustawienia PTZ

Uwaga

Ta karta jest dostępna tylko po zainstalowaniu wtyczki AXIS Perimeter Defender PTZ Autotracking.



- **Czas po alarmie** – służy do definiowania czasu, który upływa przed powrotem kamery PTZ do pozycji domowej po zniknięciu śledzonego obiektu z widoku.
- **Włącz nadpisanie ręcznie** – po zaznaczeniu tej opcji operator może sterować kamerą PTZ za pomocą joysticka, przez system VMS lub stronę internetową kamery.
- **Powiększenie pojedynczego celu** – służy do regulacji poziomu zoomu w celu śledzenia jednego obiektu. Wyższa wartość zapewnia lepsze możliwości identyfikacji, ale zarazem zwiększa ryzyko przerwania śledzenia szybko poruszających się obiektów.
- **Powiększenie wielu celów** – służy do regulacji poziomu zoomu w celu śledzenia wielu celów.
- **Korekcja prędkości** – służy do regulacji prędkości śledzenia tak, by szybko poruszające się obiekty znajdowały się na środku obrazu z kamery PTZ. Należy pamiętać, że wysoka wartość może prowadzić niestabilnego śledzenia obiektów.

- **Korekcja zoomu** – wyższa wartość zwiększa przybliżanie obiektów znajdujących się w pobliżu krawędzi pola widzenia kamery PTZ.

Karta Wyjście

- **Konfiguruj** – służy do otwarcia strony internetowej urządzenia w celu utworzenia i skonfigurowania alarmów.
- **Testuj alarm** – służy do testowania alarmu skonfigurowanego w urządzeniu.
- **Czas po alarmie: przypisz** – służy do ustawiania czasu po alarmie.

Karta Pomoc techniczna

- **Wczytaj** — wczytywanie konfiguracji dla wybranych urządzeń. Opcja ta jest szczególnie przydatna do przywracania ustawień po awarii lub przypadkowym odinstalowaniu urządzenia. Konfiguracja obejmuje następujące elementy:
  - Licencja
  - Parametry
  - Kalibracja i scenariusze
  - Obraz wideo kalibracji
- **Zapisz** — umożliwia tworzenie kopii zapasowej konfiguracji wybranych urządzeń.
- **Wyczyść** – opcja ta służy do usuwania kalibracji i scenariuszy z wybranych urządzeń. Opcja ta jest przydatna w przypadku zmiany miejsca montażu kamer, ponieważ w takim przypadku kalibracja i strefy detekcji nie są już prawidłowe.
- **Wyświetl dziennik aplikacji** – opcja ta służy do wyświetlania dziennika aplikacji AXIS Perimeter Defender.
- **Eksportuj dziennik** – opcja ta służy do generowania pliku zawierającego szczegółowe informacje dla pomocy technicznej. Plik ten należy zawsze dodawać do zgłoszeń do pomocy technicznej.

Obciążenie procesora

Wskaźnik obciążenia procesora wskazuje bieżące obciążenie procesora komputera w czasie rzeczywistym. Zbyt duże obciążenie procesora CPU może spowodować brak reakcji komputera lub aplikacji. Aby zmaksymalizować przydzielanie zasobów procesora, przed użyciem aplikacji AXIS Perimeter Defender Setup zamknij inne aplikacje. Jeżeli spróbujesz dodać urządzenie przy nadmiernie obciążonym procesorze, system wygeneruje ostrzeżenie.

Dodawane urządzenia wykorzystują procesor komputera hosta, aby zdekodować i wyświetlić strumienie wideo z kamery. W celu ograniczenia wpływu na komputer hosta strumienie wideo z dodanych urządzeń są domyślnie wyświetlane ze zmniejszoną poklatkowością (około 1 kl./s). Po zmaksymalizowaniu strumienia lub podczas procesu kalibracji przywracana jest standardowa poklatkowość (około 8 kl./s).

Ważne

Użycie opcji **Włącz pełną poklatkowość** może spowodować brak odpowiedzi interfejsu w przypadku podłączenia wielu kamer lub korzystania z mało wydajnego komputera.

Wersja demonstracyjna aplikacji AXIS Perimeter Defender

Demonstracyjna wersja aplikacji AXIS Perimeter Defender i AXIS Perimeter Defender PTZ Autotracking ma zainstalowanych kilka klipów, które można wykorzystać do prezentacji funkcji analizy bez konieczności użycia aktywnej kamery. Klipy pokazowe zawierają takie informacje, jak rodzaj detekcji i wyniki automatycznego śledzenia w różnych typach otoczenia.

1. Przejdź do menu **Aplikacja > Dodaj > Klipy demo** i wykonaj co najmniej jedną z następujących czynności:
   - Odfiltruj klipy pokazowe według typu.
   - Wybierz co najmniej jeden klip pokazowy.

AXIS Perimeter Defender

2. Aby dodać klipy pokazowe, kliknij przycisk **Dodaj wybrane klipy demo**.

Po dodaniu klipy pokazowe wyświetlane są w interfejsie jako standardowe strumienie wideo. Dostępna jest kalibracja, a funkcje analizy są aktywne, tak by użytkownik mógł natychmiast zobaczyć wyniki analizy i automatycznego śledzenia w strumieniu wideo. Funkcje analizy i automatycznego śledzenia można zatrzymać lub uruchomić, klikając status uruchomienia w widoku podglądu na żywo lub przycisk **Uruchom** albo **Zatrzymaj** w lewym oknie.

Można modyfikować i ponownie przeprowadzać kalibrację i parowanie. Można również dodawać, usuwać i modyfikować scenariusze detekcji.

Na karcie **Wsparcie** w lewym oknie znajduje się przycisk **Wyczyść**, który umożliwia przywrócenie wyjściowych wartości kalibracji i scenariuszy. Nie można całkowicie usunąć kalibracji.

Rozpoczynanie pracy

Proces instalowania aplikacji AXIS Perimeter Defender i AXIS Perimeter Defender PTZ Autotracking nieco się różni.

Rozpoczynanie pracy z aplikacją AXIS Perimeter Defender

Aby skonfigurować aplikację AXIS Perimeter Defender w lokalizacji, należy wykonać poniższe kroki:

1. Zamontuj kamerę. Patrz *Montaż kamery na stronie 13*.
2. Pobierz i zainstaluj oprogramowanie na komputerze. Patrz *Instalacja oprogramowania na komputerze na stronie 17*.
3. Połącz się z urządzeniami. Patrz *Dodawanie urządzeń na stronie 17*.
4. Zainstaluj na każdym urządzeniu aplikację AXIS Perimeter Defender. Patrz *Instalacja oprogramowania na urządzeniach na stronie 19*.

Uwaga

Nie trzeba kalibrować urządzeń, które działają tylko w trybie AI. Aby uruchomić urządzenia jednocześnie w trybie kalibracji i trybie AI, należy je skalibrować.

5. Skalibruj urządzenia. Patrz *Kalibracja – AXIS Perimeter Defender na stronie 19*.
6. Zdefiniuj reguły wyzwalania alarmów, dodając scenariusze. Patrz *Definiowanie scenariuszy na stronie 27*.
7. Skonfiguruj wysyłanie komunikatów o alarmach. Patrz *Definiowanie wyjść na stronie 31*.

Rozpoczynanie pracy z aplikacją AXIS Perimeter Defender PTZ Autotracking

Aby skonfigurować aplikację AXIS Perimeter Defender PTZ Autotracking w lokalizacji, należy wykonać poniższe kroki:

1. Zamontuj kamery. Patrz *Montaż kamery na stronie 13* i *Zamontuj kamerę PTZ. na stronie 16*.
2. Pobierz i zainstaluj oprogramowanie na komputerze. Patrz *Instalacja oprogramowania na komputerze na stronie 17*.
3. Połącz się z urządzeniami. Patrz *Dodawanie urządzeń na stronie 17*.
4. W kamerze stałopozycyjnej zainstaluj aplikację AXIS Perimeter Defender w wersji 2.5.0 lub nowszej, a w kamerze PTZ zainstaluj aplikację AXIS Perimeter Defender PTZ Autotracking. Patrz *Instalacja oprogramowania na urządzeniach na stronie 19*.
5. Skalibruj urządzenia i skonfiguruj scenariusze. Patrz *Kalibracja – PTZ Autotracking na stronie 26*.
6. Sparuj urządzenia. Patrz *Parowanie kamer – PTZ Autotracking na stronie 30*.
7. Skonfiguruj wysyłanie komunikatów o alarmach. Patrz *Definiowanie wyjść na stronie 31*.

Montaż kamery

Informacje o narzędziu do projektowania (Design Tool)

Aby określić położenie kamery na danym terenie, zalecamy użycie narzędzia do projektowania dla aplikacji AXIS Perimeter Defender. Uwzględnia ono wymogi zarówno kamer Axis, jak i aplikacji AXIS Perimeter Defender. Narzędzie pomaga w podejmowaniu decyzji dotyczących:

- Wysokości montażowej kamery
- Kąta pochylenia

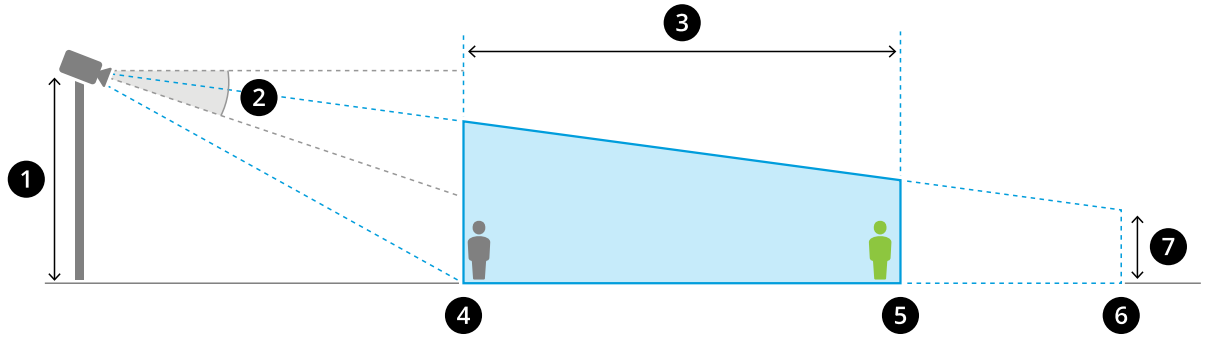
- Minimalnej odległości detekcji
- Maksymalnej odległości detekcji

Aby pobrać narzędzie, przejdź na stronę *axis.com/products/axis-perimeter-defender*.

Zalecenia dotyczące montażu kamery

Uwaga

W przypadku kamer działających tylko w trybie AI zalecenia dotyczące montażu są dostępne w aplikacji.



Prawidłowo zamontowana kamera.

1 *Wysokość montażowa*
2 *Pochylenie*
3 *Strefa detekcji*
4 *Minimalnej odległości detekcji*
5 *Maksymalnej odległości detekcji*
6 *Odległość pola widzenia*
7 *Wysokość pola widzenia*

Wysokość obiektu przy maksymalnej odległości detekcji – Aby stojąca osoba została wykryta przy maksymalnej odległości detekcji, wysokość piksela musi wynosić co najmniej 5% łącznej wysokości obrazu (3,5% w przypadku kamer termowizyjnych). Jeśli na przykład wysokość zwizualizowanego obrazu wynosi 576 pikseli, to wysokość osoby stojącej na końcu strefy detekcji musi wynosić co najmniej 28 pikseli (20 pikseli w przypadku kamer termowizyjnych).

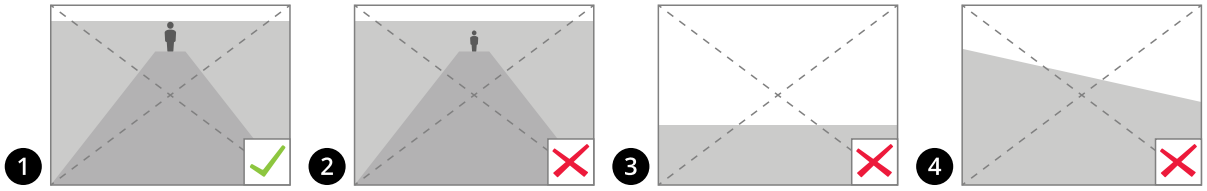
Wysokość obiektu przy minimalnej odległości detekcji – Aby stojąca osoba została wykryta przy minimalnej odległości detekcji, wysokość piksela nie może być większa niż 60% łącznej wysokości obrazu.

Wysokość obiektu podczas pracy w trybie AI – Po uruchomieniu aplikacji w trybie AI obiekty muszą być tego samego rozmiaru co awatar lub większe od niego, aby zostały wykryte.

Kąt pochylenia – Kamera musi być skierowana w stronę podłoża pod odpowiednim kątem, tak aby środek obrazu znalazł się pod linią horyzontu. Kamerę należy zamontować w taki sposób, aby minimalna odległość detekcji przekraczała połowę wysokości montażowej kamery (minimalna odległość detekcji > wysokość montażowa kamery/2).

Kąt obrotu – Kąt obrotu kamery musi być niemal równy zeru.

Rozpoczynanie pracy



1 *Wysokość obiektu, kąt pochylenia i kąt obrotu są odpowiednie.*
2 *Wysokość obiektu przy maksymalnej odległości detekcji jest mniejsza niż 5% wysokości obrazu (3,5% w przypadku kamer termowizyjnych).*
3 *Środek obrazu znajduje się ponad linią horyzontu.*
4 *Kąt obrotu kamery nie jest niemal równy zeru.*

Maksymalna odległość detekcji zależy od następujących czynników:

- Typ i model kamery
- Obiektyw kamery. Większy zasięg obiektywu umożliwia większą odległość detekcji.
- Minimalny rozmiar piksela, jaki musi być pokryty przez człowieka na obrazie, by można go było wykryć. Wysokość piksela stojącej osoby musi wynosić co najmniej 5% wysokości obrazu w przypadku kamer optycznych i 3,5% w przypadku kamer termowizyjnych.
- Warunki pogodowe
- Oświetlenie
- Obciążenie kamery

Po zamontowaniu kamery należy rozważyć następujące kwestie:

- Drgania Aplikacja dopuszcza niewielkie drgania kamery, ale najlepsze efekty uzyskuje się wtedy, gdy kamera nie jest narażona na drgania.
- Pole widzenia Kamera musi mieć stałe pole widzenia.

Wymagania dotyczące scen

Uwaga

W przypadku kamer działających tylko w trybie AI wymagania dotyczące scen są dostępne w aplikacji.

Strefa detekcji musi spełniać następujące warunki:

- Niezakłócony widok
- Płaskie podłoże lub podłoże o niewielkim nachyleniu
- Oświetlenie nie jest wyzwalane ruchem
- Niezakłócony widok
- W przypadku kamer optycznych poziom oświetlenia i ustawienia obrazu muszą być wystarczające, aby zapewnić dostateczny kontrast pomiędzy ludźmi, pojazdami i tłem.
    - W przypadku korzystania z kamery Axis do rejestracji obraz w dzień i w nocy i ze sztucznym oświetleniem zalecamy oświetlenie o natężeniu co najmniej 50 luksów w całej strefie detekcji.
    - W przypadku korzystania z zewnętrznego oświetlenia w podczerwieni zalecamy maksymalną odległość detekcji wynosząca 80 metrów. Zasięg oświetlenia w podczerwieni powinien wynosić ponad dwa razy więcej niż maksymalna odległość detekcji.

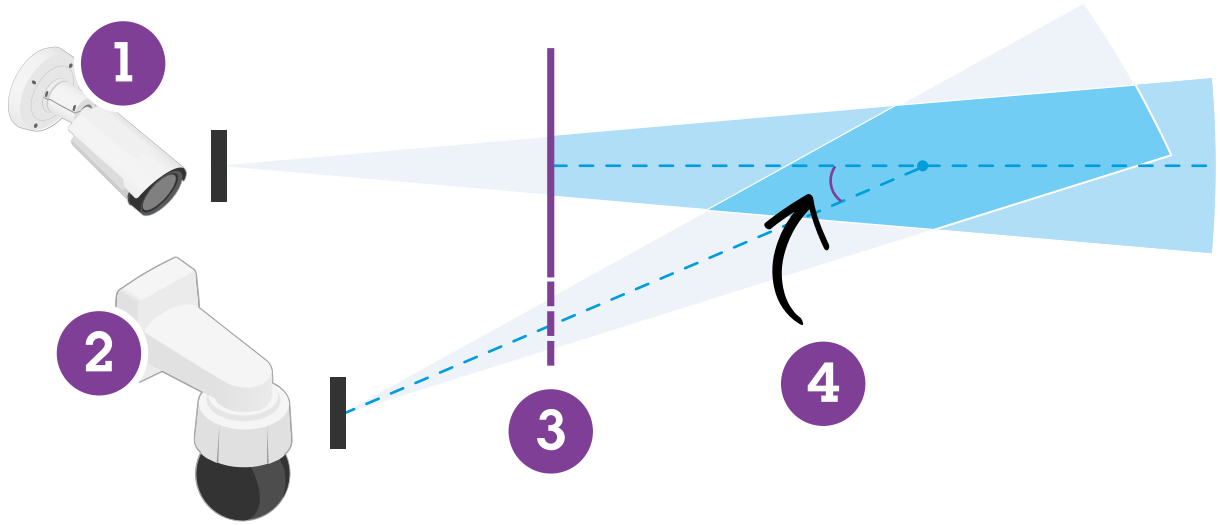
- W przypadku korzystania z wbudowanego oświetlenia w podczerwieni maksymalna odległość detekcji ograniczona jest do 20 metrów, w zależności od kamery i otoczenia.

- W przypadku kamer termowizyjnych konieczny jest wysoki kontrast pomiędzy tłem a pierwszym planem.

Aby zoptymalizować detekcję, aplikacja AXIS Perimeter Defender automatycznie uczy się różnicy pomiędzy dniem i nocą, a następnie wykorzystuje te informacje do dostosowania algorytmów detekcji. Dostosowanie trwa około 24 godzin, co oznacza, że optymalną detekcję w dzień i w nocy osiąga się dopiero po tym, jak aplikacja działa przez ten czas.

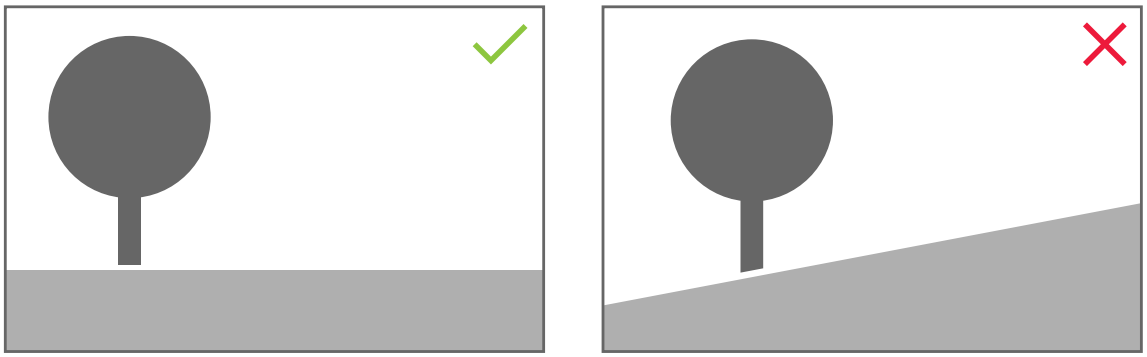
Zamontuj kamerę PTZ.

W niniejszym rozdziale opisano sposób montażu kamery PTZ w odniesieniu do kamery stałopozycyjnej. Instrukcje dotyczące montażu kamery stałopozycyjnej: *Montaż kamery na stronie 13*.



1 Stałopozycyjna kamera sieciowa
2 Kamera sieciowa PTZ
3 Minimalnej odległości detekcji
4 Kąt pomiędzy kamerami

- Pozycja domowa kamery PTZ musi obejmować ponad 60% strefy detekcji kamery stałopozycyjnej.
- Aby dana osoba stojąca była śledzona przez kamerę PTZ, musi pokrywać ponad 4% wysokości obrazu kamery PTZ.
- Kamerę PTZ należy umieścić w obszarze przed minimalną odległością detekcji kamery stałopozycyjnej (C).
- Kąt pomiędzy kamerą stałopozycyjną a kamerą PTZ musi wynosić mniej niż 30° (D).



- Podłoże musi być płaskie.

Instalacja oprogramowania na komputerze

1. Pobierz aplikację AXIS Perimeter Defender ze strony *axis.com/products/axis-perimeter-defender*
2. Zainstaluj oprogramowanie na komputerze.

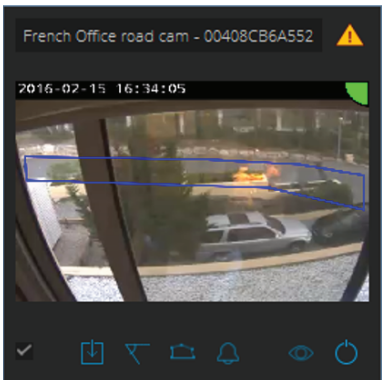
Dodawanie urządzeń

Urządzenia można dodawać do aplikacji do AXIS Perimeter Defender na trzy różne sposoby

- Automatycznie (skanowanie sieciowe). Patrz *Automatyczne dodawanie urządzeń na stronie 18*.
- Ręcznie (wybór ustawień połączenia). Patrz *Ręczne dodawanie urządzeń na stronie 18*.
- Automatycznie (wczytanie zapisanej lokalizacji). Patrz *Wczytywanie istniejącej lokalizacji na stronie 18*.

Po dodaniu urządzenia zostanie wyświetlona lista wszystkich aplikacji zainstalowanych na urządzeniu. Zalecamy zatrzymanie wszelkich aplikacji, które nie są niezbędne, ponieważ wykorzystują one zasoby procesora kamery, co ma wpływ na działanie aplikacji AXIS Perimeter Defender i może uniemożliwić prawidłową instalację.

Jeżeli urządzenie nie ma wystarczających zasobów procesora, na przykład ze względu na inne działające aplikacje, AXIS Perimeter Defender obniży poklatkowość. Jeżeli poklatkowość jest niższa niż 5 klatek na sekundę, obok nazwy urządzenia w podglądzie na żywo wyświetlany jest żółty trójkąt ostrzegawczy. Po umieszczeniu kursora nad trójkątem wyświetlana jest bieżąca liczba klatek na sekundę.



Uwaga

Poklatkowość poniżej 5 kl./s może znacząco zmniejszyć wydajność analizy wideo. Może to skutkować błędami detekcji lub ich pominięciem.

Więcej informacji: *Obciążenie procesora na stronie 11*.

Automatyczne dodawanie urządzeń

Ważne

Funkcja wyszukiwania nie działa w obrębie wielu sieci, co oznacza, że aplikacja AXIS Perimeter Defender Setup może wyszukiwać jedynie te urządzenia, które znajdują się w tej samej podsieci, co klient, na którym uruchomiono oprogramowanie. Urządzenia podłączone do innej podsieci trzeba dodać ręcznie. Funkcja wyszukiwania może również przestać działać po skonfigurowaniu routerów lub przełączników sieciowych tak, by filtrować przesyłanie multicast.

1. Aby przeskanować sieć w poszukiwaniu urządzeń, przejdź do menu **Aplikacja** i kliknij opcję **Wyszukaj**.

   Jeśli wyszukujesz urządzenia pierwszy raz i hasła nie są dostępne, zostanie otwarte okno dialogowe haseł. W przeciwnym wypadku do połączenia się z urządzeniami zostaną wykorzystane dostępne hasła.

2. Wybierz urządzenia i kliknij przycisk **Dodaj wybrane urządzenia**.

   Jeżeli hasło jest prawidłowe, po wybraniu urządzeń wyświetlany jest pochodzący z nich obraz statyczny.

Ręczne dodawanie urządzeń

1. Przejdź do menu **Aplikacja** i kliknij przycisk **Dodaj**.
2. Wprowadź następujące informacje:
   - Adres IP lub nazwę hosta urządzenia.
   - Hasło root urządzenia, ponieważ aplikacja AXIS Perimeter Defender wymaga dostępu do katalogu root.
   - Port HTTP używany do połączenia. Domyślny port to 80.
   - Opcjonalną nazwę urządzenia ułatwiającą jego rozpoznanie.
   - Jeżeli urządzenie jest podłączone w zdalnej sieci o słabej jakości połączenia, zaznacz ustawienie **Urządzenie w sieci zdalnej**. Jeśli połączenie słabej jakości nie zostanie zdefiniowane jak zdalne, może to spowodować nieprawidłowości w kalibracji lub brak działania aplikacji.

   Uwaga

   W przypadku połączeń zdalnych użytkownik musi być w stanie podłączyć urządzenie za pośrednictwem protokołu HTTP. Należy upewnić się, że port HTTP jest prawidłowo skonfigurowany. Konfiguracja zdalna może zakończyć się niepowodzeniem wtedy, gdy połączenie nie ma wystarczającej lub stabilnej przepustowości.

3. Kliknij przycisk **OK**.

Uwaga

Jeżeli nie można dodać kamery za pośrednictwem nazwy hosta, sprawdź ustawienia sieciowe i DNS lub dodaj urządzenie, używając jego adresu IP.

Wczytywanie istniejącej lokalizacji

Wczytywanie zapisanej wcześniej konfiguracji danej lokalizacji:

1. Przejdź do opcji **Aplikacja** i kliknij **Wczytaj lokalizację**.
2. Znajdź plik konfiguracji i kliknij polecenie **Otwórz**. Zostanie automatycznie wyświetlony widok podglądu na żywo.

Instalacja oprogramowania na urządzeniach

Aplikację AXIS Perimeter Defender należy zainstalować na każdym urządzeniu.

Aby sprawdzić wersję aplikacji AXIS Perimeter Defender zainstalowaną na urządzeniu, przesuń kursor myszy nad opcję **Status instalacji** w widoku podglądu na żywo.

Jeżeli na urządzeniu nie zainstalowano aplikacji AXIS Perimeter Defender, wszystkie ikony w widoku podglądu na żywo będą szare.

Instalowanie oprogramowania na urządzeniu

1. Przejdź do karty **Instalacja**.
2. Wybierz urządzenia, na których chcesz zainstalować aplikację.
3. Wybierz najnowszą dostępną wersję programu AXIS Perimeter Defender, a następnie kliknij przycisk **Instaluj**.

   Aplikacja AXIS Perimeter Defender zostanie zainstalowana na wybranych urządzeniach i uruchomiona automatycznie.
4. Wyszukaj licencję i wykonaj jedną z następujących czynności:
   - Jeżeli instalujesz aplikację na jednym urządzeniu: wybierz plik licencji dla tego urządzenia.
   - Jeżeli instalujesz aplikację na wielu urządzeniach: wybierz folder, w którym znajdują się pliki licencji.
5. Kliknij przycisk **Instaluj**.

Kalibracja – AXIS Perimeter Defender

Kalibracja

Uwaga

Nie trzeba kalibrować urządzeń, które działają tylko w trybie AI. Aby uruchomić urządzenia jednocześnie w trybie kalibracji i trybie AI, należy je skalibrować.

Aby aplikacja AXIS Perimeter Defender mogła prawidłowo zinterpretować scenę, należy skalibrować wszystkie urządzenia. Podczas kalibracji wprowadza się punkty odniesienia, które dostarczają do procesora informacje o głębi i wysokości. Definiowana jest również strefa zainteresowania.

Kalibracja obejmuje dwa zadania:

1. Przeprowadzenie kalibracji:
   - automatycznie – zalecane w większości przypadków. Patrz *Przeprowadzanie kalibracji automatycznej na stronie 20*.
   - ręcznie – zalecane w przypadku, gdy nie można przeprowadzić automatycznej kalibracji kamery lub gdy przechodzenie przez scenę byłoby niepraktyczne, ale w scenie znajdują się obiekty o znanej wysokości. Przykładem jest zdalny obwód z linią ogrodzenia składającą się z wielu równomiernie rozmieszczonych słupów o jednakowej wysokości. Patrz *Ręczna kalibracja na stronie 24*.
2. Sprawdź wyniki kalibracji. Patrz *Weryfikacja jakości kalibracji na stronie 21*.

Aby przyspieszyć konfigurację dużej lokalizacji, można jednocześnie skalibrować wiele urządzeń. Kalibrację można przeprowadzać automatycznie lub ręcznie, podobnie jak w przypadku pojedynczej kamery. Przed kalibracją wielu urządzeń jednocześnie należy wziąć pod uwagę następujące kwestie:

- Maksymalna liczba urządzeń, które można zainstalować i jednocześnie skonfigurować zależy od mocy procesora i pamięci dostępnej w komputerze. Zbyt wiele urządzeń dodanych do aplikacji AXIS Perimeter Defender Setup może powodować zawieszanie się aplikacji. Po wyświetleniu ostrzeżenia o przeciążeniu procesora należy zainstalować i skonfigurować podzestaw urządzeń za pomocą funkcji zapisywania lokalizacji.

- Automatyczna kalibracja wielu urządzeń wymaga większej części zasobów procesora i ilości pamięci RAM niż w przypadku kalibracji jednego urządzenia. W systemach o niskich parametrach może to powodować brak reakcji komputera lub zawieszanie się aplikacji. W przypadku zawieszenia się aplikacji zarejestrowane obrazy wideo są nadal dostępne w celu kalibracji jednej kamery.

Uwaga

- Aplikacja AXIS Perimeter Defender obsługuje różne współczynniki proporcji obrazu zgodnie z maksymalną rozdzielczością zapewnianą przez kamerę. W związku z tym w razie zmiany rozdzielczości należy ponownie przeprowadzić wszystkie kalibracje. Jeżeli zmienisz rozdzielczość strumienia na stronie internetowej kamery, ponowna kalibracja nie będzie konieczna.
- Zalecamy stosowanie tego samego współczynnika proporcji w aplikacji AXIS Perimeter Defender i systemie VMS, aby upewnić się, że wyświetlane informacje pasują do zawartości obrazu. Aby ustalić współczynnik proporcji, umieść kursor na nazwie kamery w podglądzie na żywo.
- Jeżeli po kalibracji zmieni się położenie kamery, trzeba ją będzie skalibrować ponownie, aby wyniki analizy były prawidłowe.

Przeprowadzanie kalibracji automatycznej

Kalibracja automatyczna umożliwia skalibrowanie jednej lub większej liczby kamer poprzez przejście osoby przez monitorowaną scenę. Kamera automatycznie gromadzi informacje potrzebne do przeprowadzenia kalibracji.

Warunki konieczne do pomyślnego przeprowadzenia kalibracji automatycznej:

- Nie należy przeprowadzać kalibracji, jeśli w polu widzenia znajduje się wiele osób.
- Nie należy przeprowadzać kalibracji, jeśli w polu widzenia znajduje się wiele przejeżdżających pojazdów.
- Nie należy przeprowadzać kalibracji, jeśli w polu widzenia poruszają się inne obiekty. Na przykład drzewa lub flagi poruszające się na wietrze.
- Nie należy kalibrować kamery, która nie została zamontowana równolegle do podłoża.
- Osoba, która przechodzi przez scenę, musi być w stanie zająć całe pole widzenia od przodu do tyłu. Jeżeli nie jest to możliwe, lepiej będzie przeprowadzić kalibrację ręczną.
- Jeżeli kamera znajduje się w sieci zdalnej, ale nie jest podłączona jako zdalna kamera, osoba przechodząca przez scenę musi iść przez około 5 minut, aby zapewnić zarejestrowanie wystarczającej liczby obrazów. Wynika to z zazwyczaj niskiej poklatkowości w przypadku rządzeń w zdalnej sieci.

1. Przejdź do obszaru **Kalibracja**.
2. Wybierz urządzenia, które chcesz skalibrować.
3. Kliknij przycisk **Automatyczna**.
4. Ustaw godzinę rozpoczęcia rejestracji. Rejestracja powinna rozpocząć się co najmniej 10 sekund przed znalezieniem się przechodzącej osoby w polu widzenia.
5. Ustaw czas trwania rejestracji. Należy wziąć pod uwagę następujące kwestie:
   - konieczne jest zapewnienie wystarczająco dużo czasu na przejście osoby przez scenę w obie strony;
   - czas trwania wideo wpływa na obliczanie kalibracji.
6. Wprowadź wzrost (w cm) osoby, która będzie przechodzić przez scenę i kliknij przycisk **Rejestruj**.

   Aby ponownie użyć zarejestrowanego obrazu wideo, kliknij przycisk **Użyj poprzedniego obrazu**.
7. Osoba powinna przejść przez scenę, postępując według następujących instrukcji:
   - Przejść zygzakiem ścieżkę pokrywającą jak największy obszar strefy detekcji od przodu do tyłu sceny. Zalecamy pokonanie ścieżki w kształcie litery V w poprzek sceny.
   - Należy zawsze pozostawać widocznym od stóp do głów w polu widzenia.

- Należy iść powoli i na wprost.
- Cały czas utrzymywać sylwetkę w pionie.
- Przed zmianą kierunku odczekać 1–2 sekundy.

Przykład sekwencji przechodzenia przez scenę.

8. Upewnij się, że automatyczna kalibracja zakończyła się powodzeniem, potwierdzając prawidłowe wykrycie osoby. Patrz *Weryfikacja jakości kalibracji na stronie 21*.
9. Aby zapisać kalibrację, kliknij przycisk **Akceptuj**.

   Aby przeprowadzić nową kalibrację, kliknij przycisk **Nowa**.

   Aby przeprowadzić kalibrację ręczną, kliknij przycisk **Ręczna**.

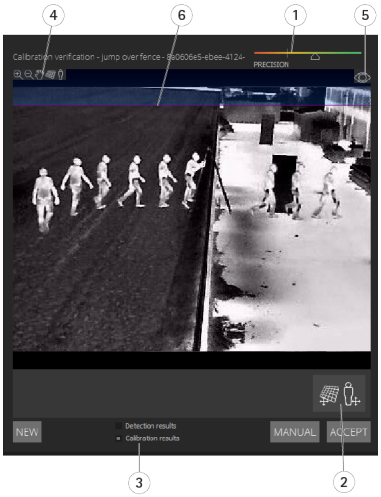
Po zaakceptowaniu kalibracji niebieskie obramowanie będzie wskazywać maksymalną strefę detekcji. Maksymalna strefa detekcji to największe pole, które można monitorować. Poza tym obszarem można wykryć intruzów, ale nie jest to gwarantowane.

Weryfikacja jakości kalibracji

Po kalibracji powinna być widoczna osoba, która przeszła przez scenę w kilku różnych miejscach. Jeżeli osoba ta nie jest widoczna, oznacza to, że kalibracja automatyczna zakończyła się niepowodzeniem i trzeba przeprowadzić ją ponownie.

Jakość kalibracji można zweryfikować na kilka sposobów:

- Sprawdź wskaźnik dokładności kalibracji. Wskazuje on automatycznie obliczony poziom dokładności mierzący pokrycie sceny przez osobę oraz jakość detekcji. Jeżeli wskaźnik dokładności znajduje się w czerwonej strefie, oznacza to, że kalibracja zakończyła się niepowodzeniem i nie można kliknąć przycisku **Akceptuj**. Patrz *Ręczna kalibracja na stronie 24*.
- Użyj siatki. Patrz *Korzystanie z siatki do weryfikacji kalibracji na stronie 22*.
- Użyj awatara. Patrz *Korzystanie z awatara w celu weryfikacji kalibracji na stronie 23*.
- Sprawdź wyniki detekcji. Patrz *Korzystanie z wyników detekcji do weryfikacji kalibracji na stronie 24*.



1 *Wskaźnik dokładności kalibracji*
2 *Siatka i awatar*
3 *Widok dynamiczny lub statyczny*
4 *Wyświetlanie modyfikatorów*
5 *Przełączanie pomiędzy obrazem kalibracji a podglądem na żywo*
6 *Linia horyzontu*

Linia horyzontu to widoczny koniec ziemi w scenie. Podczas definiowania scenariuszy nie można umieszczać stref scenariuszy w niebieskim obszarze powyżej linii horyzontu, ponieważ znajduje się on ponad podłożem, a strefy scenariuszy co do zasady znajdują się na podłożu.

Korzystanie z siatki do weryfikacji kalibracji

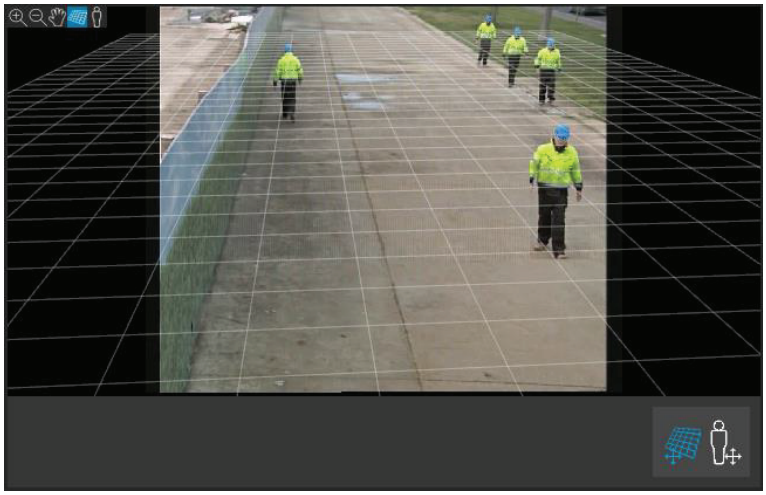
Siatka powinna odpowiadać kwadratowej siatce umieszczonej na podłożu. Można włączać i wyłączać wyświetlanie siatki, klikając ikonę modyfikacji widoku siatki.

Ważne

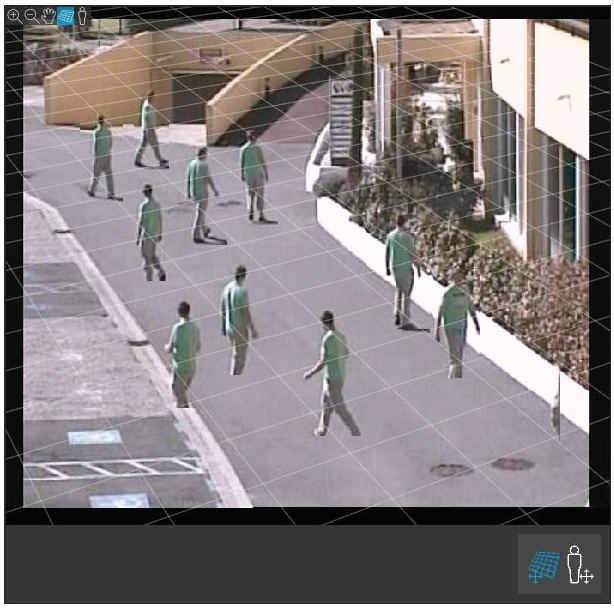
Siatka nie ma wpływu na kalibrację; jest ona jedynie narzędziem, które pozwala upewnić się, że kalibracja jest poprawna.

Siatkę można obrócić, przeciągając ją w oknie podglądu. Spróbuj wyrównać ją do jakiejś struktury w scenie, aby sprawdzić, czy wynik wydaje się być odpowiedni.

Jeżeli siatka jest równoległa do podłoża, nie jest wygięta pod nietypowym kątem, a po obróceniu jest równoległa do obiektów równoległych w świecie rzeczywistym, oznacza to, że kalibracja została przeprowadzona prawidłowo.



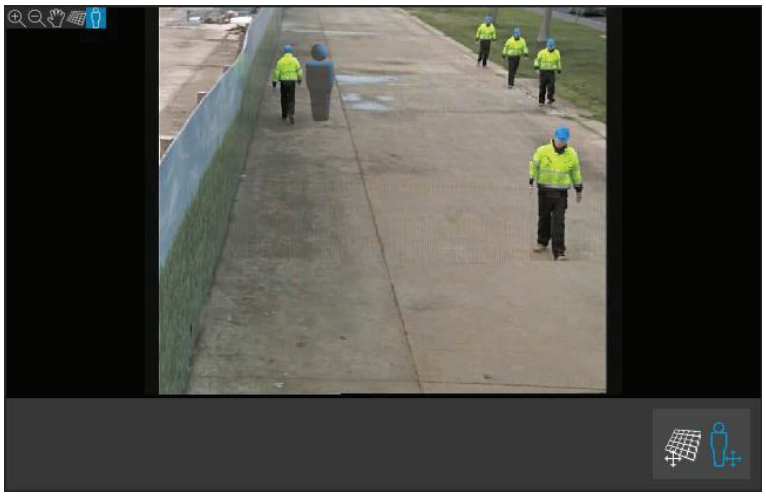
Przykład poprawnego wyrównania siatki do poboczy.



Przykład niepoprawnego wyrównania siatki do poboczy.

Korzystanie z awatara w celu weryfikacji kalibracji

Awatar umieszczany w scenie to trójwymiarowa osoba przeciętnego wzrostu. Można go włączać i wyłączać, klikając ikonę modyfikacji awatara.



Jego rozmiar w oknie podglądu odpowiada rozmiarowi przeciętnej osoby w tym położeniu, zgodnie z bieżącą kalibracją. Przesuwając awatar, można upewnić się, że jego rozmiar jest odpowiedni w stosunku do innych obiektów lub osób w scenie. Należy sprawdzić różne położenia awatara, ponieważ może mieć on nieprawidłowy rozmiar w innym miejscu na obrazie.

Korzystanie z wyników detekcji do weryfikacji kalibracji

Wyniki detekcji umożliwiają sprawdzenie, w jaki sposób aplikacja AXIS Perimeter Defender będzie działać przy bieżącej kalibracji na strumieniu wideo na żywo i zarejestrowanej przechodzącej osobie.

1. Przełącz **Wyniki kalibracji** na **Wyniki detekcji**.
2. Sprawdź, jak wykryte zostały osoby lub pojazdy w monitorowanej scenie:
   - Przy prawidłowej kalibracji osoby oznaczone są czerwonymi prostokątami, a pojazdy – niebieskimi.
   - Jeżeli często zdarza się, że osoby lub pojazdy nie zostają oznaczone, najprawdopodobniej nie powiodła się kalibracja automatyczna.
   - Czerwona strefa wskazuje strefę graniczną detekcji według wyliczonej kalibracji, czyli strefę, gdzie nie są przestrzegane wymogi wstępne dotyczące wzrostu osób na obrazie. W tej strefie detekcja może zakończyć się niepowodzeniem z powodu docelowego rozmiaru.

Uwaga

- Jeżeli wyliczona kalibracja jest nieprawidłowa, to czerwona strefa również będzie nieprawidłowa.
- Jeżeli osoba jest zbyt daleko, może ona nie zostać oznaczona. Aby detekcja zadziałała, konieczny jest minimalny rozmiar. Więcej informacji: *Montaż kamery na stronie 13*.
- Weryfikacja wyników detekcji może nie działać w kamerach podłączonych zdalnie, ponieważ zarejestrowany obraz może mieć zbyt niską poklatkowość. Nie oznacza to, że konfiguracja zakończyła się niepowodzeniem. W takim przypadku do zweryfikowania kalibracji należy użyć siatki i awatara.

Ręczna kalibracja

Jeżeli nie przeprowadzono automatycznej kalibracji, należy zarejestrować krótki film wideo i utworzyć obraz zespolony, a dopiero potem można przeprowadzić kalibrację ręczną. Należy postępować tak samo, jak w przypadku kalibracji automatycznej (*Przeprowadzanie kalibracji automatycznej na stronie 20*), tylko trzeba wybrać opcję **Ręczna** zamiast **Automatyczna** na karcie **Kalibracja**. Tworzenie obrazu zespolonego po zarejestrowaniu wideo:

- Przesuń suwak, aby przejść do
- najważniejszych punktów w klipie wideo i kliknij ikonę aparatu, by dodać obrazy do obrazu zespolonego.

Upewnij się, że obraz zespolony zawiera pełen przekrój sceny: przód, tył oraz lewą i prawą stronę.

Po utworzeniu obrazu zespolonego (ręcznie lub automatycznie) można kontynuować kalibrację ręczną.

Silnik kalibracji dokonuje kalibracji według oszacowania:

- horyzontu,
- rozprzestrzeniania się linii pionowych na obrazie,
- skali sceny.

Podczas przeprowadzania ręcznej kalibracji należy wprowadzić te informacje do silnika kalibracji za pomocą znaczników kalibracji. Dostępne są trzy rodzaje znaczników kalibracji:

- **Figurki** służą do oznaczania znanego wzrostu przeciętnej osoby w różnych miejscach sceny. Jeżeli przeprowadzono już automatyczną kalibrację, to najprawdopodobniej na obrazie w oknie edytora wyświetlana jest kilka razy ta sama osoba. Umieść figurki na podłożu, aby oznaczyć wzrost oraz kierunek poruszania się w jednym lub wielu miejscach. Figurka w świecie rzeczywistym musi być umieszczona stopami na podłożu i być pionowa. Długość figurki w świecie rzeczywistym musi odpowiadać wzrostowi podanemu obok przycisku **Osoba** w oknie edytora. Figurki oznaczone są półprzezroczystym jasnoniebieskim symbolem.

  Optymalne umieszczanie figurek

  - Zalecamy umieszczenie figurki na osobie ze złączonymi stopami.
  - W przypadku umieszczenia jej na osobie z rozstawionymi stopami należy dolną krawędź umieścić na podłożu pomiędzy piętami tej osoby.
  - Wyrównaj figurkę z tułowiem. Jeśli osoba jest przechylona w którąś stronę, czyli zazwyczaj do przodu, jeśli idzie, spróbuj skompensować wychylenie, umieszczając figurkę bardziej prosto. Użyj wskazówek obecnych w scenie, takich jak drzewa, płoty lub lampy.
  - Aby uzyskać skalę sceny, konieczne jest użycie co najmniej jednej figurki i odpowiadającej jej osoby. Jeżeli w scenie nie ma osoby, można umieścić figurkę na innym pionowym obiekcie o znanej wysokości, na przykład na słupie liczącym 3 m i ustawić wysokość obiektu jako wzrost osoby.

- **Równoległe linie poziome (linie H)** służą do oznaczania znanych linii poziomych i równoległych w scenie. Linie te mogą znajdować się na podłożu, ścianie lub w obu miejscach, ale wszystkie muszą być równoległe. Zawsze należy dodać co najmniej dwie linie H. Można je umieszczać po bokach prostej drogi lub na oznaczeniach, na prostych torach kolejowych, widocznym elemencie ściany lub na górze i dole słupków ogrodzenia. Linie H są oznaczone kolorem jasnoniebieskim.

- **Linie pionowe (linie V)** służą do oznaczania znanych linii pionowych w scenie. Linia V powinna być umieszczona na rzeczywistym pionowym obiekcie. Może to być na przykład słupek ogrodzenia, narożnik budynku lub znak. Linia V nie musi zaczynać się od podłoża. Linie V są oznaczone kolorem ciemnoniebieskim. Należy pamiętać, że niewielkie zmiany orientacji linii V mogą znacząco zmienić kalibrację. Generalnie rzecz biorąc, linie V powinny pochylać się bardziej w prawo po prawej stronie obrazu i w lewo – po lewej stronie.

1 *Figurki*
2 *Linie pionowe (linie V)*
3 *Równoległe linie poziome (linie H)*
4 *Siatka i awatar*

Liczba znaczników kalibracji

Czym więcej figurek, linii H i linii V w scenie, tym lepiej. Silnik kalibracji jest w stanie przeprowadzić kalibrację przy niewielu liniach, ale czym więcej linii i figurek, tym lepsza jakość kalibracji. Zalecamy umieszczanie figurek blisko, daleko, po lewej i po prawej.

Pionowe struktury na obrazie

Zgodnie z zaleceniami w *Zalecenia dotyczące montażu kamery na stronie 14* wszystkie kamery muszą być skierowane nieco w dół. Dzięki temu wszystkie rzeczywiste struktury będą na obrazie wyglądać jak wachlarz. Oznacza to, że wszystkie figurki i linie V powinny pochylać się w kierunku krawędzi obrazu. Figurka po prawej stronie obrazu powinna być pochylona w prawo, a figurka po lewej stronie – w lewo. Aby kalibracja została przeprowadzona prawidłowo, co najmniej jedna z figurek lub linii V musi być nachylona we właściwą stronę.

Wskaźnik dokładności dostarcza informacje zwrotne na temat poziomu i jakości szczegółów dodanych do sceny. Aby kalibracja ręczna została przeprowadzona prawidłowo, znaczniki powinny obejmować scenę od przodu do tyłu i od lewej do prawej. Sprawdzenie tego umożliwia zielony wskaźnik dokładności.

Jakość kalibracji

Jakość kalibracji można sprawdzić za pomocą siatki lub awatara. Patrz *Weryfikacja jakości kalibracji na stronie 21*. Można również kliknąć przycisk **Zweryfikuj**. Zostanie wyświetlony efekt działania aplikacji AXIS Perimeter Defender na zarejestrowanym obrazie wideo przy pomocy bieżącej kalibracji.

Kalibracja – PTZ Autotracking

Ważne

Aby uzyskać dobre wyniki, kalibracja musi być najwyższej jakości. Należy dokładnie przestrzegać wytycznych i instrukcji.

Uwaga

Obie kamery można skalibrować w tym samym czasie lub osobno.

1. Wybierz kamerę stałopozycyjną i kamerę PTZ.

2. Przejdź do opcji **Kalibracja** i kliknij opcję **Ustaw pozycję PTZ**. Zostanie wyświetlone wyskakujące okno zawierające widok z kamery stałopozycyjnej.

   Kamera PTZ może poruszać się przez chwilę po uruchomieniu aplikacji.

3. Sprawdź, czy widok z obu kamer jest wyrównany.

   W przeciwnym razie kliknij obraz na żywo i dostosuj widok z kamery PTZ, tak by był wyrównany z widokiem z kamery stałopozycyjnej. Upewnij się, że kamera się nie przesuwa.

4. Kliknij opcję **Konfiguracja pozycji PTZ**.

   Jeżeli przycisk nie jest widoczny, przesuń wyskakujące okno z widokiem z kamery stałopozycyjnej.

5. Kliknij przycisk **Automatyczna**.

6. Wykonaj kalibrację automatyczną zgodnie z instrukcjami w rozdziale *Przeprowadzanie kalibracji automatycznej na stronie 20*.

7. Użyj awatara, aby sprawdzić jakość kalibracji kamery stałopozycyjnej. Patrz *Korzystanie z awatara w celu weryfikacji kalibracji na stronie 23*.

   Jeżeli jakość jest wystarczająca, kliknij przycisk **Akceptuj**.

   Jeżeli jakość nie jest wystarczająca, użyj obrazu wideo z automatycznej kalibracji, aby przeprowadzić kalibrację ręczną. Kliknij opcję **Ręczna** i postępuj zgodnie z instrukcjami w rozdziale *Ręczna kalibracja na stronie 24*.

8. Na karcie **Scenariusze** zdefiniuj reguły wyzwalania alarmów. Patrz *Definiowanie scenariuszy na stronie 27*.

9. Na karcie **Kalibracja** kliknij opcję **Weryfikuj** w widoku podglądu na żywo z kamery PTZ.

10. Użyj awatara, aby sprawdzić jakość kalibracji kamery PTZ. Patrz *Korzystanie z awatara w celu weryfikacji kalibracji na stronie 23*.

    Jeżeli jakość jest wystarczająca, kliknij przycisk **Akceptuj**.

    Jeżeli jakość nie jest wystarczająca, użyj obrazu wideo z automatycznej kalibracji, aby przeprowadzić kalibrację ręczną. Kliknij opcję **Ręczna** i postępuj zgodnie z instrukcjami w rozdziale *Ręczna kalibracja na stronie 24*.

11. Sparuj kamery. Patrz *Parowanie kamer – PTZ Autotracking na stronie 30*.

Definiowanie scenariuszy

Scenariusze

Aplikacja AXIS Perimeter Defender zawiera często stosowane scenariusze stref sterylnych, które można skonfigurować tak, by zabezpieczyć i monitorować ważne obszary. Na etapie kalibracji utworzono maksymalną strefę detekcji w celu przygotowania domyślnego scenariusza wykrywania wtargnięć/podejrzanych zachowań. Na tym etapie można zdefiniować bardziej zaawansowane scenariusze detekcji trzech typów:

- Wtargnięcie/podejrzane zachowania. Patrz *Konfiguracja scenariusza wtargnięcia/podejrzanych zachowań na stronie 28*
- Przekroczenie strefy. Patrz *Konfiguracja scenariusza przekroczenia strefy na stronie 29*
- Warunkowy. Patrz *Konfiguracja scenariusza warunkowego na stronie 29*

Jeżeli w nazwie scenariusza znajduje się symbol **!** , oznacza to, że nie zakończono jego konfiguracji. Zazwyczaj oznacza to, że nie zdefiniowano jeszcze strefy detekcji tego scenariusza.

Parametry globalne

Parametry globalne ustawione w interfejsie użytkownika mają zastosowanie do wszystkich scenariuszy.

Typ kamery – W przypadku kamer optycznych wybierz opcję **Kolor – dzień–noc**. W przypadku kamer termowizyjnych typ kamery jest automatycznie ustawiany na kamerę termowizyjną.

Uwaga

- Dodatkowe typy zbliżania się mogą zwiększyć ryzyko wywołania fałszywych alarmów, na przykład spowodowanych przez zwierzęta.
- Dodatkowe typy zbliżania się nie są obsługiwane w przypadku urządzeń działających tylko w trybie AI.

Dodatkowe typy zbliżania się – Wybierz te typy, które ma obejmować scenariusz detekcji.

Zaawansowane niwelowanie – W przypadku urządzeń z trybem AI zaznacz opcję **AI**, aby go włączyć. Można użyć opcji **Headlights/vehicles in scene (Reflektory/pojazdy w scenie)**, jeśli w scenie znajdują się pojazdy, reflektory lub odbicia światła. W przypadku użycia tego ustawienia wydajność w normalnych warunkach może ulec zmniejszeniu. Domyślnie wszystkie scenariusze powinny zawierać pojazdy, a więc i światła reflektorów. Można użyć opcji **Insects/droplets on lens (Owady/krople na obiektywie)**, by ignorować fałszywe alarmy wywoływane kroplami deszczu lub obecnością owadów na obiektywie.

Czułość – Aby zwiększyć czułość systemu, przesuń suwak w prawo. Wyższa czułość zmniejsza ryzyko pominięcia detekcji, ale za to zwiększa ryzyko wywołania fałszywych alarmów.

Filtrowanie według rozmiaru docelowego – W przypadku urządzeń z trybem AI można odfiltrować obiekty o rozmiarze mniejszym niż docelowy.

Parametry czasu trwania

Dla każdego tworzonego scenariusza można ustawić parametry czasu trwania.

Minimalny czas obecności w strefie – Ustaw czas, przez jaki obiekt ma pozostać w strefie, aby stała się ona aktywna.

Wąska strefa – Jeżeli strefa jest wąska i można ją przekroczyć w 1–2 sekundy, istnieje ryzyko pominięcia alarmów. Można temu zapobiec przy użyciu funkcji **Narrow zone (Wąska strefa)**. Opcji tej nie można łączyć z opcją **Min presence in zone (Minimalny czas obecności w strefie)**.

Konfiguracja scenariusza wtargnięcia/podejrzanych zachowań

Scenariusz wtargnięcia/podejrzanych zachowań jest przeznaczony do wyzwalania alarmów po znalezieniu się obiektu w określonej strefie i pozostawaniu tam przez czas dłuższy niż wstępnie zdefiniowany.

Domyślnym scenariuszem utworzonym na etapie kalibracji jest scenariusz wtargnięcia/podejrzanych zachowań, który wykorzystuje maksymalną strefę detekcji. Aby użyć tego scenariusza, kliknij przycisk **Akceptuj** na karcie **Scenariusze**.

Zmień domyślny scenariusz:

1. Przejdź do menu **Scenariusze > Scenariusze zaawansowane**.
2. Zmień domyślną strefę detekcji:
   - Aby przenieść istniejące punkty w strefie detekcji, kliknij je i przeciągnij myszą.
   - Aby utworzyć dodatkowe punkty, kliknij dowolny z istniejących segmentów i przeciągnij go myszą.
3. W obszarze **Wykryj** wybierz typy obiektów do wykrycia.
4. Jeśli nie chcesz, by obiekt wyzwalał alarm od razu po znalezieniu się w strefie, w obszarze **Parametry czasu trwania** ustaw wartość opcji **Min. czas przebywania w strefie**.
5. Jeżeli strefa jest wąska i można ją przekroczyć w 1–2 sekundy, ale nadal powinny być w niej wyzwalane alarmy, wybierz opcję **Narrow zone (Wąska strefa)**. Ustawienia tego nie można łączyć z opcją **Min presence in zone (Minimalny czas obecności w strefie)**. Więcej informacji: *Parametry czasu trwania na stronie 28*.
6. Aby wczytać zmiany do kamery i przełączyć się z powrotem do widoku głównego, kliknij przycisk **Akceptuj**.

Konfiguracja scenariusza przekroczenia strefy

Scenariusz przekroczenia strefy zaprojektowano tak, aby wyzwalał alarm, gdy obiekt przechodzi przez dwie strefy detekcji w konkretnej kolejności.

Ważne

Istnieją następujące ograniczenia scenariusza przekroczenia strefy: jeżeli obiekt wyzwalający scenariusz przestaje się poruszać przez kilka sekund w wyjściowej strefie przed przejściem do strefy końcowej, ten scenariusz nie zostanie wyzwolony.

W obszarze **Parametry czasu trwania** można określić minimalny czas obecności dla każdej ze stref w danym scenariuszu. Jeżeli T_A to minimalny czas w strefie wyjściowej, a T_B to czas w strefie końcowej, alarm zostanie wyzwolony tylko wtedy, gdy obiekt pozostanie w strefie wyjściowej dłużej niż T_A a następnie dłużej niż T_B w strefie końcowej.

1. Przejdź do menu **Scenariusze > Scenariusze zaawansowane**.
2. Kliknij przycisk **Nowy** i wybierz opcję **Przekroczenie strefy**.
3. Utwórz dwie strefy detekcji oddalone od siebie o co najmniej metr (3 stopy 3 3/8 cala):
   - Aby utworzyć strefę detekcji, kliknij kilka razy na obrazie.
   - Aby zakończyć tworzenie strefy, kliknij prawym przyciskiem myszy na obrazie.
4. Aby określić kierunek, w którym przekraczanie strefy jest niedozwolone, kliknij przycisk **Wybierz strefę wyjściową**, a następnie kliknij jedną ze stref.
5. W obszarze **Wykryj** wybierz typy obiektów do wykrycia.
6. W obszarze **Parametry czasu trwania**, jeśli strefa ma nie być aktywowana po pojawieniu się w niej obiektu, ustaw opcję **Minimalna obecność w** dla jednej lub obu stref.
7. Jeżeli strefa jest wąska i można ją przekroczyć w 1–2 sekundy, ale nadal powinny być w niej wyzwalane alarmy, wybierz opcję **Narrow zone (Wąska strefa)**. Ustawienia tego nie można łączyć z opcją **Min presence in zone (Minimalny czas obecności w strefie)**. Więcej informacji: *Parametry czasu trwania na stronie 28*.
8. Aby wczytać zmiany do kamery i przełączyć się z powrotem do widoku głównego, kliknij przycisk **Akceptuj**.

Konfiguracja scenariusza warunkowego

Scenariusz warunkowy jest przeznaczony do wyzwalania alarmów, gdy dany obiekt pojawia się w strefie bez przemieszczenia się przez inne.

W obszarze **Parametry czasu trwania** można określić minimalny czas obecności dla każdej ze stref w danym scenariuszu. Jeżeli T_A to minimalny czas w autoryzowanej strefie, a T_B w strefie wtargnięcia, to alarm wyzwalany jest tylko wtedy, gdy obiekt:

- pozostaje w strefie wtargnięcia dłużej niż T_B bez uprzedniego pojawienia się w strefie autoryzowanej.
- pozostaje w strefie autoryzowanej krócej niż T_A a następnie pojawia się w strefie i pozostaje w niej dłużej niż T_B .

Alarm nie jest wyzwalany, jeśli obiekt:

- nie pojawia się w strefie wtargnięcia lub pozostaje w niej krócej niż T_B .
- pozostaje w strefie autoryzowanej dłużej niż T_A a następnie pojawia się w strefie wtargnięcia (niezależnie od tego, jak długo w niej pozostaje).

1. Przejdź do menu **Scenariusze > Scenariusze zaawansowane**.
2. Kliknij przycisk **Nowy** i wybierz opcję **Warunkowy**.
3. Utwórz dwie lub więcej stref detekcji oddalonych od siebie o co najmniej metr (3 stopy 3 3/8 cala):
   - Aby utworzyć strefę detekcji, kliknij kilka razy na obrazie.

- Aby zakończyć tworzenie strefy, kliknij prawym przyciskiem myszy na obrazie.

4. Aby określić dozwolony kierunek przekraczania, kliknij przycisk **Wybierz strefę wtargnięcia**, a następnie kliknij jedną ze stref.
5. W obszarze **Wykryj** wybierz typy obiektów do wykrycia.
6. W obszarze **Parametry czasu trwania**, jeśli strefa ma nie być aktywowana po pojawieniu się w niej obiektu, ustaw opcję **Minimalna obecność w** dla jednej lub obu stref.
7. Jeżeli strefa jest wąska i można ją przekroczyć w 1–2 sekundy, ale nadal powinny być w niej wyzwalane alarmy, wybierz opcję **Narrow zone (Wąska strefa)**. Ustawienia tego nie można łączyć z opcją **Min presence in zone (Minimalny czas obecności w strefie)**. Więcej informacji: *Parametry czasu trwania na stronie 28*.
8. Aby wczytać zmiany do kamery i przełączyć się z powrotem do widoku głównego, kliknij przycisk **Akceptuj**.

Parowanie kamer – PTZ Autotracking

Podczas konfiguracji aplikacji AXIS Perimeter Defender PTZ Autotracking należy sparować kamerę stałopozycyjną i kamerę PTZ, aby upewnić się, że poruszający się obiekt będzie odpowiednio śledzony przez kamerę PTZ.

Jeżeli przeprowadzono kalibrację automatyczną, można przeprowadzić kalibrację automatyczną obu kamer (*Przeprowadzanie automatycznego parowania na stronie 30*). W przeciwnym razie trzeba przeprowadzić kalibrację ręczną (*Przeprowadzenie ręcznego parowania na stronie 30*).

Przeprowadzanie automatycznego parowania

Na sparowanym obrazie wideo czerwone linie przedstawiają osobę, a pomarańczowa ramka – przybliżony obraz z kamery PTZ.

1. W menu **Kalibracja > Sparowany widok PTZ** zweryfikuj sparowanie obrazów wideo z obu kamer:
   - sprawdź, czy czerwone linie na dwóch obrazach są wyrównane na obrazie wideo;
   - sprawdź, czy czerwone linie zawsze przechodzą od stóp do głowy osoby;
   - sprawdź, czy dana osoba jest zawsze wyśrodkowywana w pomarańczowej ramce na obrazie wideo z kamery PTZ.
2. Po spełnieniu warunków z etapu 1 wybierz opcję **Interaktywna weryfikacja parowania**.

   Jeżeli warunki nie zostały spełnione, kliknij opcję **Ręczne** i postępuj zgodnie z instrukcjami w rozdziale *Przeprowadzenie ręcznego parowania na stronie 30*.
3. Przesuń suwak, aby przejść do klipu wideo. Sprawdź, czy:
   - niebieskie linie na obu obrazach są wyrównane na całym obrazie wideo;
   - dana osoba jest zawsze wyśrodkowywana w pomarańczowej ramce na obrazie wideo z kamery PTZ.
4. W przypadku scen, w których brak pomarańczowej ramki:

   4.1 Aktywuj awatar na obrazie z kamery stałopozycyjnej.

   4.2 Użyj suwaka, aby przewijać obraz wideo do przodu i do tyłu. Umieść awatar na osobie w widoku kamery stałopozycyjnej i sprawdź, czy czerwona kropka znajduje się u stóp osoby na obrazie z kamery PTZ.
5. Jeżeli są dostępne sceny, w których podczas automatycznego parowania nie dodano niebieskich linii, kliknij opcję **Ręczne**, aby ręcznie dodać czerwone linie do osoby. Szczegółowe instrukcje: *Przeprowadzenie ręcznego parowania na stronie 30*.
6. Kliknij przycisk **Akceptuj** i **Zamknij**.

Przeprowadzenie ręcznego parowania

Podczas ręcznego parowania dodaje się pionowe czerwone linie od stóp do głowy osoby, która podczas kalibracji przeszła przez scenę dozoru. Aby objąć całą scenę, należy dodać czerwone linie na całym obrazie wideo.

Jeżeli przeprowadzono już parowanie automatyczne, to na obrazie wideo znajdują się niebieskie linie.

Usuń te niebieskie i czerwone linie, które:

- nie zaczynają się przy stopach osoby,
- nie docierają do głowy osoby,
- nie mają odpowiednika na obrazie z kamery PTZ.

Aby usunąć linię, kliknij ją i naciśnij klawisz DELETE.

1. Przesuń suwak, aby w klipie wideo przejść do obrazu, w którym dana osoba jest widoczna.
2. Dodaj czerwoną linię do osoby na obrazie z kamery stałopozycyjnej. Linia musi zaczynać się u stóp osoby. Każda linia otrzymuje numer identyfikacyjny.
3. Dodaj do tego samego obiektu odpowiadającą czerwoną linię na obrazie z kamery PTZ. Sprawdź, czy numer identyfikacyjny jest zgodny z numerem na obrazie z kamery stałopozycyjnej.
4. Powtarzaj kroki 1–3 do momentu objęcia całej sceny.

   Jeżeli na klipie wideo znajduje się wystarczająca liczba linii, by przeprowadzić parowanie:

   - przycisk **Akceptuj** staje się aktywny;
   - na obrazie z kamery PTZ wyświetlana jest pomarańczowa ramka.
5. Sprawdź, czy dana osoba zawsze znajduje się na środku pomarańczowej ramki. Jeśli w niektórych scenach tak nie jest, dodaj więcej czerwonych linii.
6. Aktywuj awatar na obrazie z kamery stałopozycyjnej.
7. Przesuń suwak, aby przejść do klipu wideo. Użyj awatara, aby upewnić się, że:
   - rozmiar awatara na obrazie z kamery stałopozycyjnej odpowiada rozmiarom osoby w różnych położeniach;
   - na obrazie z kamery PTZ czerwona kropka znajduje się u stóp osoby;
   - dana osoba jest zawsze wyśrodkowywana w pomarańczowej ramce na obrazie z kamery PTZ.
8. Kliknij przycisk **Akceptuj**. Jeżeli przycisk jest nieaktywny, trzeba najpierw dodać więcej czerwonych linii.
9. Kliknij przycisk **Zakończ**.

Definiowanie wyjść

Aby aplikacja AXIS Perimeter Defender przesyłała do wyjść informacje o alarmie po wykryciu wtargnięcia, należy najpierw zdefiniować odpowiednie reguły. System może wysyłać alarmy na przykład do systemu VMS.

Aplikacja AXIS Perimeter Defender może wysyłać alarmy za pośrednictwem różnych interfejsów.

Z samej aplikacji:

- Powiadomienia o alarmach w formacie XML lub zwykłym tekstem przez TCP/IP
- Strumienie metadanych w formacie XML przez HTTP multipart

Z urządzenia:

- Podstawowe powiadomienia w formacie tekstowym przez TCP/IP
- Wyjścia elektryczne (styki pod napięciem lub nie pod napięciem)
- Powiadomienia e-mail

- Wysyłanie obrazów dotyczących alarmu za pośrednictwem protokołu FTP

Można aktywować wiele interfejsów naraz.

Więcej szczegółowych informacji: *Wyjścia na stronie 33*.

Aby zdefiniować reguły wysyłania alarmów z urządzenia:

1. Przejdź do opcji **Outputs (Wyjścia)** i kliknij przycisk **Configure (Konfiguruj)**. W przeglądarce zostanie otwarta strona internetowa urządzenia.
2. Utwórz nową regułę akcji.
3. Z listy wyzwalaczy wybierz opcję **Aplikacje**, a następnie **AXISPerimeterDefender** i scenariusz, który ma wyzwalać akcję.

Uwaga

Aby wyzwalać tę samą akcję dla wszystkich zdefiniowanych scenariuszy, wybierz opcję **WSZYSTKIE_SCENARIUSZE**.

4. Z listy akcji wybierz akcję, która ma zostać wykonana po spełnieniu warunku.
5. Kliknij przycisk **OK**.

Aby uzyskać bardziej szczegółowe informacje na temat tworzenia reguł akcji, zapoznaj się z instrukcją obsługi urządzenia.

Konfiguracja zaawansowana

Wyjścia

Powiadomieni o alarmie w formacie XML/tekstowym

Ten interfejs umożliwia odbiorcy TCP/IP otrzymywanie komunikatów XML (pełniejszych i opisowych) lub tekstowych dla każdego alarmu. W przeciwieństwie do interfejsu tekstowego, interfejs XML/tekstowy ma następujące korzyści:

- Powiadomienie jest wysyłane po rozpoczęciu alarmu, po jego zakończeniu oraz co 10 sekund podczas jego trwania.
- Znacznik czasowy: powiadomienia o rozpoczęciu i zakończeniu alarmu mają znacznik czasowy zsynchronizowany z zegarem kamery i podający dokładną datę i godzinę zdarzenia.
- Typ alarmu: AXIS Perimeter Defender obsługuje kilka typów alarmów: *Definiowanie scenariuszy na stronie 27*. Powiadomienia w formacie XML/tekstowym zawierają informacje o typie wyzwolonego alarmu. Uwaga: scenariusz „przekroczenia strefy" to typ „przejście", a scenariusz podejrzanych zachowań to typ „obecność".
- Strefy objęte alarmem; jeżeli każdy scenariusz AXIS Perimeter Defender jest powiązany z jedną lub wieloma strefami, powiadomienia XML/tekstowe zawierają informację o strefie objętej alarmem (tj. w przypadku alarmu wtargnięcia jest to strefa wtargnięcia, w której wykryto osobę).

W przeciwieństwie do interfejsu tekstowego, interfejs XML/tekstowy ma następujące ograniczenia:

- Tekst komunikatu jest stały i nie zawiera pól na dowolny tekst.
- Jedna kamera może obsługiwać tylko jednego odbiorcę.

Odbiorcy powiadomień XML/tekstowych otrzymują cztery rodzaje komunikatów:

- Aplikacja AXIS Perimeter Defender wysyła komunikat CONNECTION_TEST po skonfigurowaniu powiadomienia XML, aby potwierdzić prawidłową komunikację z odbiorcą.
- Kiedy aplikacja AXIS Perimeter Defender wyzwoli alarm, wysyłany jest komunikat ALARM_START.
- Podczas trwania alarmu aplikacja AXIS Perimeter Defender przesyła kilka komunikatów „alarm w toku" co 10 sekund. Wszystkie te komunikaty mają taki sam znacznik GUID, identyczny jak znacznik w komunikatach ALARM_START i ALARM_STOP dotyczących tego samego alarmu.
- Po zakończeniu alarmu aplikacja AXIS Perimeter Defender wysyła komunikat ALARM_STOP.

Objaśnienie formatu tych komunikatów w formacie XML i tekstowym: *Przykłady formatów XML i tekstowych na stronie 33*.

Przykłady formatów XML i tekstowych

Format XML jest formatem domyślnym dla powiadomień TCP/IP. Jeżeli jednak istotny jest rozmiar powiadomienia, można użyć formatu tekstowego, który powoduje generowanie krótszych komunikatów. Aby wybrać format tekstowy, należy zaznaczyć opcję **Nie używaj XML dla parametrów alarmów** na stronie konfiguracji aplikacji AXIS Perimeter Defender.

Przykład

Komunikat CONNECTION_TEST w formacie XML wygląda jak w poniższym przykładzie:

```
<?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 to wewnętrzna wersja składni i protokołu XML.
- ID to numeryczna tożsamość komunikatu. Identyfikatory nie są unikatowe ani progresywne.
- TYPE to typ komunikatu, na przykład „CONNECTION_TEST". Typ komunikatu wyznacza podrzędne znaczniki komunikatu (brak dla komunikatów typu „CONNECTION_TEST").
- SENDER_IP to adres IP kamery Axis, która wysyła powiadomienie XML.
- SENDER_PORT ma zawsze wartość zero; kamera nie może odbierać komunikatów przychodzących.
- REFERENTIAL to identyfikator numeryczny kamery.

Jeżeli wybrano format tekstowy, komunikaty powiadomienia zawierają po 7 pól oddzielonych pałką „|". Jeżeli nie można określić pola (na przykład nie jest ono potrzebne dla tego typu komunikatu), pałka jest zastępowana przez znak „-".

Siedem pól, od pierwszego do ostatniego (w nawiasie odpowiadające pola XML w formacie XML), przedstawia się następująco:

1. Identyfikator numeryczny komunikatu (atrybut „ID" nagłówka „KEENEO_MESSAGE" w XML).
2. Adres IPv4 kamery (atrybut „SENDER_IP" nagłówka XML „KEENEO_MESSAGE").
3. Numer referencyjny przypisany do instancji aplikacji AXIS Perimeter Defender (znacznik „REFERENTIAL").
4. Typ komunikatu (atrybut „TYPE" nagłówka XML „KEENEO_MESSAGE").
5. Typ alarmu (znacznik „TYPE").
6. Nazwa scenariusza, który wyzwolił alarm (znacznik „SCENARIO_NAME").
7. Znacznik czasowy (znacznik „TIMESTAMP"). Format znacznika czasowego jest taki sam, jak w formacie XML.

Poprzedni komunikat CONNECTION_TEST w formacie tekstowym wygląda następująco:

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

Przykład

Komunikat ALARM_START w formacie XML wygląda jak w poniższym przykładzie:

```
<?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>
```

- Nagłówek komunikatu jest taki sam, jak w komunikacie „CONNECTION_TEST".
- Typ komunikatu to „ALARM_START" i zawiera on zestaw znaczników podrzędnych.
  - REFERENTIAL to identyfikator numeryczny kamery.

- TYPE to typ alarmu wyzwolonego przez aplikację AXIS Perimeter Defender; w tym przykładzie jest to „INTRUSION" (wtargnięcie). Pozostałe możliwe typy to „PRESENCE" (obecność), „PASSAGE" (przejście) i „CONDITIONAL" (warunkowy).
- SCENARIO_NAME to nazwa scenariusza, który wyzwolił alarm, zdefiniowanego w interfejsie konfiguracji. Patrz *Konfiguracja scenariusza wtargnięcia/podejrzanych zachowań na stronie 28*
- EXTRA_DATA to nazwa strefy (lub lista nazw stref), w której został wyzwolony alarm, na przykład strefa wtargnięcia.
- TIMESTAMP to data i godzina rozpoczęcia alarmu, podana w formacie YYYY-MM-DDTHH:mm:ss.zzz, gdzie:
  - YYYY to cztery cyfry roku, na przykład 2014;
  - MM to dwie cyfry miesiąca, np. 01 dla stycznia;
  - DD to dwie cyfry dnia, na przykład 03 dla trzeciego dnia miesiąca;
  - T jest stałą literą;
  - HH to godzina w formacie 24-godzinnym, od 00 do 23;
  - mm dwie cyfry minut, od 00 do 59;
  - ss to dwie cyfry sekund, od 00 do 59;
  - zzz to trzy cyfry milisekund, od 000 do 999.

  Aplikacja AXIS Perimeter Defender generuje znacznik czasowy alarmu na podstawie daty i godziny ustawionej w kamerze, więc należy koniecznie zsynchronizować kamerę z zewnętrznym zegarem.
- GUID to unikatowy identyfikator, niezmienny dla wszystkich komunikatów dotyczących tego samego alarmu (czyli ALARM_START, ALARM_IN_PROGRESS i ALARM_STOP).

Jest to odpowiednik tekstowego komunikatu ALARM_START:

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

Przykład

Komunikat ALARM_IN_PROGRESS w formacie XML wygląda jak w poniższym przykładzie:

```
<?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>
```

- Nagłówek komunikatu jest taki sam, jak komunikatu „CONNECTION_TEST" i „ALARM_START".
- Typ komunikatu to „ALARM_IN_PROGRESS" i zawiera on zestaw znaczników podrzędnych.
  - REFERENTIAL to identyfikator numeryczny kamery.
  - TYPE to typ alarmu wyzwolonego przez aplikację AXIS Perimeter Defender, taki sam jak w odpowiadającym mu komunikacie ALARM_START.

- SCENARIO_NAME to nazwa scenariusza, który wyzwolił alarm, taka sama, jak w odpowiadającym mu komunikacie ALARM_START.
- Identyfikator GUID jest taki sam, jak w odpowiadającym mu komunikacie ALARM_START.

Odpowiadający mu komunikat ALARM_IN_PROGRESS w formacie tekstowym:

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

Przykład

Komunikat ALARM_STOP w formacie XML wygląda jak w poniższym przykładzie:

```
<?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>
```

- Nagłówek komunikatu jest taki sam, jak w poprzednich komunikatach.
- Typ komunikatu to „ALARM_STOP"; ma on taki sam zestaw podtypów, jak komunikat ALARM_START.

Odpowiadający mu komunikat ALARM_IN_PROGRESS w formacie tekstowym:

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

Połączenie TCP/IP jest zawsze zamykane po każdym komunikacie. W związku z tym gniazdo odbioru musi być zawsze otwarte, aby można było odbierać kolejne powiadomienia.

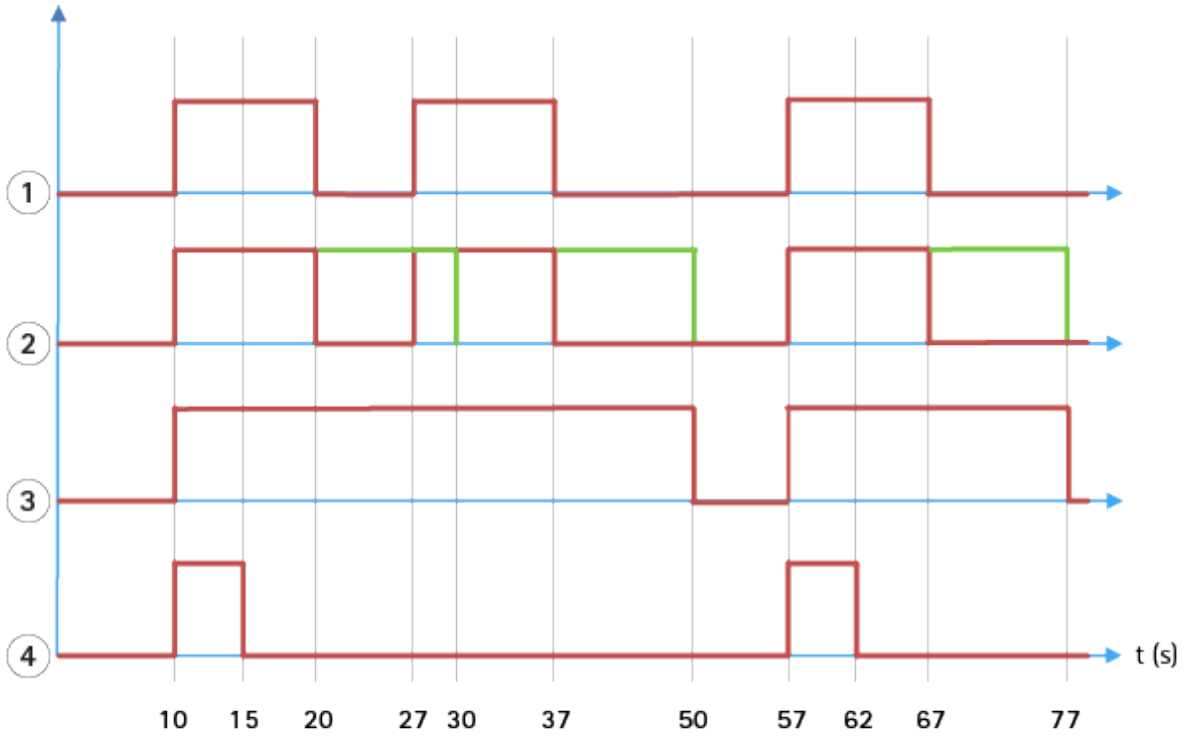
Błędy komunikacji

Jeżeli zdalny odbiorca komunikatów XML jest niedostępny, na przykład z powodu braku połączenia sieciowego, aplikacja AXIS Perimeter Defender rozpoczyna wewnętrzne buforowanie niedostarczonych komunikatów o alarmie i ponawia próbę ich dostarczenia co jakiś czas (co najmniej co 10 sekund). Po kolejnych nieudanych próbach dostarczenia nowych komunikatów (nie są w to wliczane ponowne próby dostarczania zbuforowanych komunikatów) aplikacja AXIS Perimeter Defender oznacza odbiorcę jako „offline na stałe" i przestaje do niego wysyłać komunikaty XML. Liczba kolejnych nieudanych prób to 20, co w przybliżeniu odpowiada 4 lub 5 alarmom o wtargnięciu o średnim czasie trwania 40 sekund każdy. Aplikacja AXIS Perimeter Defender ponawia wysyłanie komunikatów do tego samego odbiorcy w następujących przypadkach:

- Po ponownym uruchomieniu AXIS Perimeter Defender.
- Po ponownym zapisaniu tej samej wartości parametru „Adres URL strumieniowania alarmu".

Czas po alarmie

Aplikacja AXIS Perimeter Defender stosuje tak zwany „czas po alarmie". Jest to przedział czasowy po zakończeniu alarmu, podczas którego w razie wyzwolenia kolejnego alarmu oba alarmy są scalane w oddzielny alarm.



1 *Trzy alarmy wyzwolone przez aplikację AXIS Perimeter Defender o czasie 10, 27 i 57. Każdy alarm trwa 10 sekund, tj. 10 sekund zajęło intruzowi przejście przez strefę wtargnięcia.*
2 *Dodawany jest czas po alarmie, wynoszący 10 sekund.*
3 *Alarmy wykorzystujące powiadomienia XML i metadane XML.*
4 *Alarmy wykorzystujące powiadomienia pocztą elektroniczną, wczytywanie obrazów przez FTP, styki elektryczne i podstawowe powiadomienia TCP/IP.*

(2) Należy zwrócić uwagę na to, że czas po alarmie, wynoszący 10 sekund (w kolorze zielonym), wydłuża czas trwania każdego alarmu, powodując połączenie (scalenie) dwóch alarmów oddzielonych od siebie o 10 sekund lub mniej.

(3) Nazwę i czas trwania wynikowego alarmu wywołanego przez AXIS Perimeter Defender można znaleźć w powiadomieniach XML i metadanych XML. Czas po alarmie można wykorzystać do otrzymywania mniejszej liczby dłuższych alarmów zamiast kilku krótkich, jeden po drugim.

(4) Wynik użycia 10-sekundowego czasu po alarmie jest różny dla powiadomień pocztą elektroniczną, wczytywania obrazów przez FTP, styków elektrycznych i podstawowych powiadomień TCP/IP. Te powiadomienia uwzględniają tylko czas rozpoczęcia alarmu i pomijają koniec alarmu. Oznacza to, że w przypadku tych powiadomień nie jest podawany „czas trwania alarmu", a w konsekwencji czas po alarmie nie zmienia czasu trwania powiadomienia. Czas ten ma zawsze stałą wartość wybraną przez użytkownika podczas konfiguracji powiadomienia. Tak więc po scaleniu kolejnych alarmów wysyłane jest tylko jedno powiadomienie. Widać, że aplikacja AXIS Perimeter Defender scaliła dwa pierwsze alarmy i zostało wysłane tylko jedno powiadomienie. Oznacza to, że w przypadku powiadomień pocztą elektroniczną, wczytania obrazów przez FTP, styków elektrycznych i podstawowych powiadomień TCP/IP wysyłana jest informacja tylko dla tych dwóch alarmów. Na wykresie widać stały czas trwania powiadomień, wynoszący 5 sekund.

Konfigurowanie czasu po alarmie

1. Otwórz aplikację AXIS Perimeter Defender Setup.
2. Przejdź do opcji **Wyjścia**.
3. Zmień wartość ustawienia **Czas po alarmie**. Wartość domyślna to 7 sekund.
4. Kliknij przycisk **Przypisz**.

Metadane

Stałe nałożenie metadanych

Stałe nałożenie metadanych to funkcja, dzięki której można nałożyć dane analityczne detekcji bezpośrednio na strumień na żywo przesyłany z kamery. Informacje o detekcji są nakładane jako ramki i linie trajektorii. Strumienie wybierane są w zależności od ich rozdzielczości, a jeżeli urządzenie obsługuje obszary obserwacji – na podstawie obszaru obserwacji. Nałożone na stałe metadane wyświetlane są zarówno w widoku na żywo, jak i podczas odtwarzania zarejestrowanego materiału.

Metadane nałożone na stałe na wybrane strumienie

Można na przykład skonfigurować aplikację w taki sposób, aby dodawać nałożenie do wszystkich strumieni o rozdzielczości 640x480. W takim przypadku dane zostaną nałożone tylko na strumienie o tej rozdzielczości, a pozostałe strumienie nie zostaną zmodyfikowane.

Metadane nałożone na stałe na wybrane obszary obserwacji

Jeśli obszary obserwacji są obsługiwane oprócz rozdzielczości można dodać obszar obserwacji. Można na przykład wybrać opcję nakładania danych na strumieniach z obszaru obserwacji numer 3 w rozdzielczości 1280x720. W tym przypadku dane zostaną nałożone wyłącznie na strumienie pasujące do tych kryteriów, a inne strumienie pozostaną niezmienione, w tym strumienie z obszaru obserwacji numer 3, ale w innej rozdzielczości, oraz strumienie w rozdzielczości 1280x720, ale nie z obszaru obserwacji numer 3.

Dodawanie nałożonych na stałe metadanych do strumienia wideo

Uwaga

Funkcja ta jest dostępna tylko w urządzeniach z oprogramowaniem sprzętowym w wersji 7.30 lub nowszej.

W poniższym przykładzie wyjaśniono sposób nakładania na stałe metadanych na wszystkie strumienie wideo o rozdzielczości 640x480. Ustawienia te nie wpływają na strumienie wideo w innej rozdzielczości.

1. Wybierz kamerę w panelu z podglądem na żywo.
2. Przejdź do menu **Wyjścia > Stałe nałożenie metadanych**.
3. Wybierz opcję **Włączone**.
4. Z listy rozwijanej wybierz rozdzielczość 640x480.
5. Kliknij przycisk **Zastosuj**.
6. Upewnij się, że w podglądzie na żywo w tej rozdzielczości wyświetlane są metadane.

Integracja z VMS

Aplikacja AXIS Perimeter Defender integruje się z następującymi systemami zarządzania materiałem wizyjnym (VMS):

- Security Center firmy Genetec™
- XProtect® firmy Milestone

Więcej informacji o obsługiwanych wersjach systemów VMS znajduje się na stronie *axis.com/products/axis-perimeter-defender/support-and-documentation*.

Alarmy wyzwalane przez aplikację AXIS Perimeter Defender są automatycznie konwertowane na zdarzenia w systemie VMS. Zdarzenia te mogą wyzwalać wiele akcji i korzystać z pełnego potencjału systemu VMS. Metadane wygenerowane przez aplikację AXIS Perimeter Defender (w czasie rzeczywistym) wysyłane są do systemu VMS, gdzie można je wyświetlić lub zarejestrować wraz z obrazem. W związku z tym metadane są również dostępne podczas odtwarzania zarejestrowanych sekwencji wideo.

Zautomatyzowany system detekcji wtargnięć służy do wyzwalania alarmów i zapewnia informacje pomagające poinformować personel ochrony. Może to obejmować monit przesłany na urządzenie mobilne lub wyświetlenie alarmu w systemie VMS, na przykład z wyróżnieniem przyczyny wywołania zdarzenia alarmowego na ekranie.

Standardowa integracja zdarzeń

Aplikacja AXIS Perimeter Defender wykorzystuje właściwości natywnych interfejsów ACAP i poszerza je w zakresie wysyłania komunikatów o alarmach oraz dodatkowych informacji do urządzeń zewnętrznych lub systemów VMS. Zdarzenia wysyłane przez aplikację AXIS Perimeter Defender można przełożyć na komunikaty wysyłane do systemu VMS, dołączając do nich reguły akcji.

Dostępne są następujące kanały wysyłania komunikatów o alarmach z kamery do systemu VMS:

- Podstawowe powiadomienia w formacie tekstowym (TCP/IP)
- Wyjścia elektryczne (styki pod napięciem lub nie pod napięciem)
- Powiadomienia e-mail
- Wysyłanie obrazów dotyczących alarmu za pośrednictwem protokołu FTP

Integrację taką można skonfigurować w kamerze. Patrz *Czas po alarmie na stronie 36*.

Mostki VMS

Do następujących systemów zarządzania materiałem wizyjnym oferujemy wstępnie opracowane moduły integracji zwane „mostkami":

- Milestone XProtect® 2014 i 2016 Corporate/Expert/Enterprise/Professional/Express. Wersje Enterprise/Professional/Express nie obsługują metadanych (nie są odtwarzane w czasie rzeczywistym ani na zapisach).
- Genetec™ Service Center 5.3 i 5.4 Pro/Enterprise/SV32/SV16

Mostki oferują dwa rodzaje integracji:

- Tworzenie niestandardowych zdarzeń alarmowych w systemie VMS, pasujących do zdarzeń generowanych przez aplikację AXIS Perimeter Defender.
- Wyświetlanie nałożenia alarmu (ramek) na obrazach wideo w czasie rzeczywistym i w zapisach (poza wersjami Milestone XProtect® Enterprise/Professional/Express).

Mostki VMS należy pobrać i zainstalować jako oddzielne aplikacje. Więcej informacji na temat instalacji i konfiguracji tych mostków znajduje się w instrukcji użytkownika danego mostka.

Tworzenie reguły w systemie AXIS Camera Station

W tej części opisano sposób integrowania aplikacji AXIS Perimeter Defender z systemem zdarzeń Axis Camera Station. Dowiesz się, jak:

- skonfigurować regułę systemu AXIS Camera Station, która będzie wyzwalana w przypadku wtargnięcia;
- sprawdzić, czy konfiguracja została przeprowadzona prawidłowo.

1. Skonfiguruj i skalibruj aplikację AXIS Perimeter Defender w oprogramowaniu AXIS Perimeter Defender Setup. Aby uzyskać pomoc w zakresie instalacji i kalibracji aplikacji AXIS Perimeter Defender, zapoznaj się z jej instrukcją obsługi *lub stroną produktu*.
2. Dodaj kamerę do systemu AXIS Camera Station, postępując zgodnie z kreatorem **Add Camera (Dodaj kamerę)**.
3. Skonfiguruj wyzwalacz zdarzenia urządzenia:
    3.1 Przejdź do menu **Configuration (Konfiguracja)** > **Recording & Events (Zapis i zdarzenia)** i otwórz kartę **Advanced rules (Reguły zaawansowane)**.
    3.2 Utwórz nową regułę i wybierz wyzwalacz **Device Event (Zdarzenie urządzenia)**.
    3.3 Wybierz kamerę, w której zainstalowano aplikację AXIS Perimeter Defender.
    3.4 Z listy **Event (Zdarzenie)** wybierz opcję **AXISPerimeterDefender**.

3.5 Z listy **Feature (Funkcja)** wybierz nazwę skonfigurowanego wtargnięcia (w tym przypadku „Intrusion-1"). Jeśli chcesz, aby reguła była wyzwalana dla wszystkich skonfigurowanych scenariuszy, wybierz opcję **ALL_SCENARIOS (WSZYSTKIE SCENARIUSZE)**.

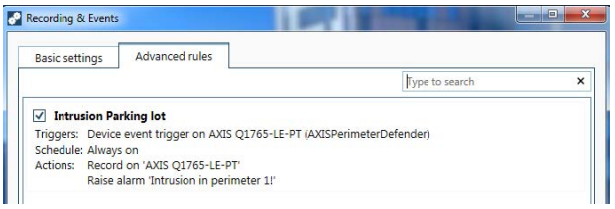
3.6 Wybierz opcję **Yes (Tak)**, jeśli wyzwalacz ma zostać aktywowany w przypadku wtargnięcia. Po wykryciu wtargnięcia w oknie Activity (Aktywność) zostanie wyświetlona zmiana stanu, co pomoże sprawdzić, czy konfiguracja została przeprowadzona prawidłowo.

3.7 Kliknij opcję **OK**, a następnie opcję **Next (Dalej)**, aby skonfigurować akcje.

3.8 W oknie dialogowym **Add Action (Dodaj akcję)** można dodać jedną lub kilka akcji dla danej reguły.

W tym przykładzie dodajemy akcję nagrywania i akcję alarmu.

3.9 Kliknij opcję **Finish (Zakończ)**.



W przykładzie przedstawiono regułę systemu AXIS Camera Station, która wyzwala dwie akcje w przypadku wtargnięcia.

4. Sprawdź, czy konfiguracja działa zgodnie z oczekiwaniami, symulując wtargnięcie — na przykład poprzez fizyczne wejście na monitorowany obszar.

Rozwiązywanie problemów

Aby wszystkie funkcje działały zgodnie z oczekiwaniami, należy skonfigurować następujące parametry Axis:

- Sieć / TCP-IP / Podstawowe / Domyślny router
- Sieć / TCP-IP / Zaawansowane / Nazwa domeny
- Sieć / TCP-IP / Główny serwer DNS
- Sieć / TCP-IP / Dodatkowy serwer DNS
- Sieć / TCP-IP / Adres serwera NTP
- Sieć / TCP-IP / SMTP (e-mail)
- Opcje systemowe / Data i godzina / Strefa czasowa
- Opcje systemowe /Data i godzina / Synchronizuj z serwerem NTP

Aktualizacja do najnowszej wersji

Aby skorzystać z najnowszych ulepszeń bez konieczności ponownej kalibracji i ponownego definiowania scenariuszy, zalecamy uaktualnienie do najnowszej wersji aplikacji AXIS Perimeter Defender.

1. Pobierz i zainstaluj najnowszą wersję aplikacji AXIS Perimeter Defender.
2. Kliknij przycisk **Instaluj**. Aplikacja AXIS Perimeter Defender Setup automatycznie wykonuje zadania konieczne do ukończenia instalacji:
   - Wykonanie kopii zapasowej istniejącej kalibracji, scenariuszy, parametrów i licencji.
   - Instalacja nowej wersji.
   - Przywrócenie licencji.
   - Przywrócenie kalibracji i scenariuszy.
   - Przywrócenie parametrów.
   - Jeżeli aplikacja była uruchomiona podczas instalacji, to zostanie uruchomiona ponownie.

Aktualizacja oprogramowania sprzętowego kamery

Uwaga

Przed uaktualnieniem oprogramowania sprzętowego kamery zapisz wszystkie ustawienia aplikacji AXIS Perimeter Defender. Aktualizacja oprogramowania sprzętowego spowoduje usunięcie aplikacji i jej ustawień z kamery. Zapisane ustawienia można przywrócić dzięki aplikacji AXIS Perimeter Defender Setup.

1. Aby zapisać konfigurację lokalizacji, użyj aplikacji AXIS Perimeter Defender Setup.
2. Zaktualizuj oprogramowanie sprzętowe kamery. Aby uzyskać szczegółowe informacje, zapoznaj się z instrukcją obsługi kamery.
3. Uruchom aplikację AXIS Perimeter Defender Setup.
4. Użyj opcji wczytywania lokalizacji, aby automatycznie wczytać zapisaną konfigurację lokalizacji do każdej uaktualnionej kamery.

Rozwiązywanie problemów z instalacją

Problem	Możliwa przyczyna	Rozwiązanie
Wyświetlany jest komunikat systemu Windows® z informacją, że instalacja oprogramowania jest niemożliwa.	System operacyjny komputera typu laptop lub PC nie jest zgodny z systemem operacyjnym.	Sprawdź, czy system operacyjny Windows® jest zgodny z wymogami.
Wyświetlany jest komunikat systemu Windows® z informacją, że instalacja przebiegła nieprawidłowo.	Asystent zgodności Windows® wykrył potencjalny problem z instalacją.	Upewnij się, że instalacja przebiegła prawidłowo, i przejdź dalej.
Instalacja zakończyła się niepowodzeniem podczas instalacji XVID.	Instalacja XVID nie powiodła się z powodu wykrycia starszej wersji XVID na komputerze.	Usuń folder XVID ze ścieżki C:\Program Files (x86) i spróbuj zainstalować XVID ponownie.
Po wyświetleniu umowy EULA pakiet instalatora nagle przestaje działać. Wyświetlany jest komunikat o błędzie systemu Windows® informujący o nietypowym wyłączeniu aplikacji. Nie można zamknąć instalatora.	Znany problem instalatora prowadzi do zamknięcia aplikacji w pewnych warunkach.	Otwórz menedżera zadań i zamknij wszystkie procesy „msiexec. exe". Następnie zamknij proces instalatora i uruchom go ponownie.

Rozwiązywanie problemów z konfiguracją

Problem	Możliwa przyczyna	Rozwiązanie
Problemy z uruchamianiem aplikacji AXIS Perimeter Defender.	Brak wystarczających uprawnień użytkownika systemu Windows®.	Upewnij się, że masz uprawnienia administratora.
Podczas wyszukiwania nie są wykrywane kamery.	Zapora	Zapora i program antywirusowy mogą czasem blokować wykrywanie kamer. W razie potrzeby skonfiguruj zaporę, aby zezwalać programowi AXIS Perimeter Defender na obustronny dostęp przez zaporę. Jeśli to nie rozwiąże problemu, skonfiguruj zaporę, otwierając następujące porty: port 5353 UDP oraz port 80 TCP.
	Problemy z adresem IP	Każde urządzenie działające w sieci musi posiadać swój unikatowy adres IP, aby móc komunikować się z innymi urządzeniami. Podczas korzystania z aplikacji AXIS Perimeter Defender zalecane jest przypisanie do kamer stałych adresów IP. Upewnij się, że każde urządzenie IP w sieci ma własny adres IP i nie używa adresu IP, który został już wykorzystany.
	Kamera nie jest dostępna z poziomu komputera użytkownika.	W przeglądarce przejdź do adresu IP kamery, aby sprawdzić, czy jest dostępny. Jeżeli nie można nawiązać połączenia z kamerą, to nie została ona prawidłowo zainstalowana w sieci lub komputer nie ma dostępu do kamery.

Rozwiązywanie problemów

Problem	Możliwa przyczyna	Rozwiązanie
Nie można dodać kamery.	Parametry połączenia z kamerą, np. adres IP, hasło lub port HTTP, są nieprawidłowe.	Upewnij się, że wprowadzone parametry są prawidłowe i spróbuj ponownie.
	Brak podglądu z kamery na komputerze użytkownika.	W przeglądarce przejdź do adresu IP kamery, aby sprawdzić, czy jest dostępny. Jeżeli kamera nie jest dostępna, to nie została poprawnie zainstalowana w sieci lub komputer nie ma dostępu do sieci, w której się ona znajduje.
Utrata strumieni wideo w aplikacji AXIS Perimeter Defender Setup.	Źródło obrazu wideo nie jest już dostępne.	Przerwano strumieniowanie ze źródła obrazu wideo i obraz nie został odświeżony.
	Użyj przeglądarki, aby sprawdzić, czy kamera jest dostępna.	Kliknij kafelek, na którym powinien być wyświetlany strumień i zmień rozmiar interfejsu. Strumień powinien zostać wyświetlony ponownie.
Automatyczna kalibracja nie działa lub jej wynik jest nieprawidłowy.	Nie spełniono wymogów wstępnych.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Kamera przesuwa się.	Nie można skalibrować kamery, która się przesuwa.
	Wolne połączenie z kamerą nie zostało skonfigurowane jako połączenie zdalne.	Podłącz kamerę jako urządzenie zdalne, by obniżyć wymogi dotyczące przepustowości.
	W scenie wykorzystywanej do automatycznej kalibracji znajdują się inne ruchome obiekty, na przykład samochody, drzewa lub inne osoby.	Ponownie przeprowadź kalibrację automatyczną lub skalibruj urządzenie ręcznie.
	Pole widzenia jest nieczytelne, a osoba przechodząca przed kamerą jest przez większość czasu częściowo ukryta.	Skalibruj urządzenie ręcznie.
	Pole widzenia jest niewielkie (np. wejścia).	Skalibruj urządzenie ręcznie.
	Przechwycony obraz wideo nie został prawidłowo zarejestrowany z powodu braku miejsca na dysku.	Sprawdź, czy jest dostępna wystarczająca ilość miejsca na dysku i czy aplikacja ma uprawnienia do zapisu obrazu wideo na komputerze z aplikacją AXIS Perimeter Defender.

Rozwiązywanie problemów z działaniem aplikacji

Problem	Możliwa przyczyna	Rozwiązanie
Aplikacja nie działa nawet po właściwym skonfigurowaniu.	Oprogramowanie sprzętowe kamery jest nieaktualne.	Upewnij się, że zainstalowano najnowsze oprogramowanie sprzętowe kamery.

Mimo uruchomienia analizy w AXIS Perimeter Defender Setup nie jest wyświetlane nałożenie.	Aplikacja jest blokowana po uruchomieniu lub zatrzymaniu, lub aktualizacji pakietu AXIS Perimeter Defender.	Uruchom ponownie kamerę.
	Zapora ogniowa blokuje połączenie z portem odbioru metadanych w kamerze.	Skonfiguruj zaporę tak, aby umożliwić interfejsowi konfiguracji połączenie z portem odbioru metadanych w kamerze.
	Program antywirusowy blokuje odbieranie nałożenia.	Skonfiguruj oprogramowanie antywirusowe, aby odbierać dane nałożenia.
W aplikacji AXIS Perimeter Defender Setup na komputerze konfiguracji nie są wyzwalane alarmy mimo uruchomionej analizy i widocznego nałożenia.	Obiekt docelowy znajduje się w scenie, ale nie pasuje do scenariusza warunkowego, czyli na przykład nie przemieszcza się z jednej strefy do drugiej w scenariuszu przekroczenia strefy.	Upewnij się, że scenariusz (i jego warunki) jest poprawnie zdefiniowany.
	Mało dokładna detekcja.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*. Upewnij się również, że kalibracja jest wystarczająco dokładna, a czułość wystarczająco wysoka.

Rozwiązywanie problemów z wydajnością

Problem	Możliwa przyczyna	Rozwiązanie
Interfejs ekranowy i analizy włączają się i wyłączają samoczynnie.	Obciążenie procesora kamery jest zbyt duże.	Możliwe rozwiązania: • Upewnij się, że strumień danych z kamery nie jest wizualizowany w zbędnej lokalizacji, ponieważ każda wizualizacja strumienia zwiększa obciążenie procesora kamery. • Jeżeli włączono wbudowaną funkcję rejestracji detekcji ruchu, spróbuj zmniejszyć jakość zapisu, aby zwolnić zasoby procesora. • Dezaktywuj wbudowaną rejestrację detekcji ruchu i upewnij się, że detekcja ruchu jest wyłączona.
Obiekt pojawia się w sterylnej strefie, wyzwalając wiele alarmów.	Czas rejestracji po alarmie jest za krótki.	Ustaw odpowiedni czas rejestracji po alarmie. Przejdź do menu AXIS Perimeter Defender Setup > **Wyjścia**.

Rozwiązywanie problemów

Problem	Możliwa przyczyna	Rozwiązanie
Potencjalny cel pojawia się w sterylnej strefie, ale nie jest wykrywany i nie jest wyzwalany alarm.	Kontrast obiektu względem tła w scenie jest zbyt niski.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Brak dostatecznego oświetlenia w scenie lub kamera nie rejestruje obrazów prawidłowo przy słabym oświetleniu.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Czułość aplikacji AXIS Perimeter Defender jest zbyt niska.	Zwiększ czułość globalnych parametrów scenariuszy.
	Kamera znajduje się w innym położeniu, powodując nieprawidłową kalibrację.	Ponownie przeprowadź kalibrację.
	Kalibracja nie jest wystarczająco dokładna.	Zweryfikuj kalibrację kamery. Przejdź do aplikacji AXIS Perimeter Defender Setup.
	Obiekt docelowy znajduje się w scenie, ale nie pasuje do scenariusza warunkowego, czyli na przykład nie przemieszcza się z jednej strefy do drugiej w scenariuszu przekroczenia strefy.	Upewnij się, że scenariusz (i jego warunki) jest poprawnie zdefiniowany.
Obiekt docelowy został wykryty, ale nie został prawidłowo sklasyfikowany (osoba jako pojazd lub pojazd jako osoba).	Nieprawidłowa wysokość, położenie lub orientacja kamery.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Kamera jest zbyt oddalona od strefy.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Kalibracja nie jest wystarczająco dokładna.	Zweryfikuj kalibrację kamery. Przejdź do aplikacji AXIS Perimeter Defender Setup.
AXIS Perimeter Defender generuje alarm mimo braku wtargnięcia do strefy sterylnej.	Czułość analizy jest zbyt wysoka.	Zmniejsz czułość. Przejdź do aplikacji AXIS Perimeter Defender Setup.
	Kalibracja nie jest wystarczająco dokładna.	Zweryfikuj kalibrację kamery. Przejdź do aplikacji AXIS Perimeter Defender Setup.
	Kamera znajduje się w innym położeniu, powodując nieprawidłową kalibrację.	Ponownie przeprowadź kalibrację.
	Nieprawidłowa wysokość, położenie lub orientacja kamery.	Upewnij się, że spełniono wymogi dotyczące montażu. Patrz *Montaż kamery na stronie 13*.
	Kamera porusza się, na przykład kołysze lub poddawana jest drganiom.	Zamontuj kamerę w bardziej stabilnym otoczeniu.
	Roślinność lub inne ruchome obiekty, na przykład flagi, znajdują się blisko kamery.	Usuń elementy powodujące problemy z pola widzenia kamery. Obiekty znajdujące się na stałe w scenie, ale nie w pobliżu kamery, są ignorowane przez aplikację AXIS Perimeter Defender.
	Po obiektywie lub w jego pobliżu przemieszczają się owady.	W miarę możliwości zapobiegaj przedostawaniu się owadów na obiektyw lub w jego pobliże.

Niniejsza instrukcja jest przeznaczona dla administratorów i użytkowników aplikacji AXIS Perimeter Defender. Zawiera ona instrukcje dotyczące używania produktu i zarządzania nim w sieci. Podczas korzystania z tego produktu wymagane jest doświadczenie z zarządzania siecią.

Informacje o znakach towarowych

AXIS COMMUNICATIONS, AXIS, ARTPEC i VAPIX są zarejestrowanymi znakami towarowymi firmy Axis AB w różnych jurysdykcjach. Wszystkie inne znaki towarowe są własnością odpowiednich podmiotów.

Apple, Apache, Bonjour, Ethernet, Internet Explorer, Linux, Microsoft, Mozilla, Real, SMPTE, QuickTime, UNIX, Windows i WWW są zarejestrowanymi znakami towarowymi odpowiednich właścicieli. Java i wszystkie znaki towarowe oraz logo oparte na słowie/symbolu Java są znakami towarowymi lub zarejestrowanymi znakami towarowymi firmy Oracle lub jej podmiotów stowarzyszonych. Znak słowny UPnP i logo UPnP są znakami towarowymi Open Connectivity Foundation, Inc. w USA lub innych krajach.

Genetec jest znakiem towarowym, a Milestone XProtect® jest zarejestrowanym znakiem towarowym odpowiednich właścicieli.

Podręcznik użytkownika
AXIS Perimeter Defender
© Axis Communications AB, 2016 - 2021
Wer. M15.5
Data: Sierpień 2021
Nr części T10068952