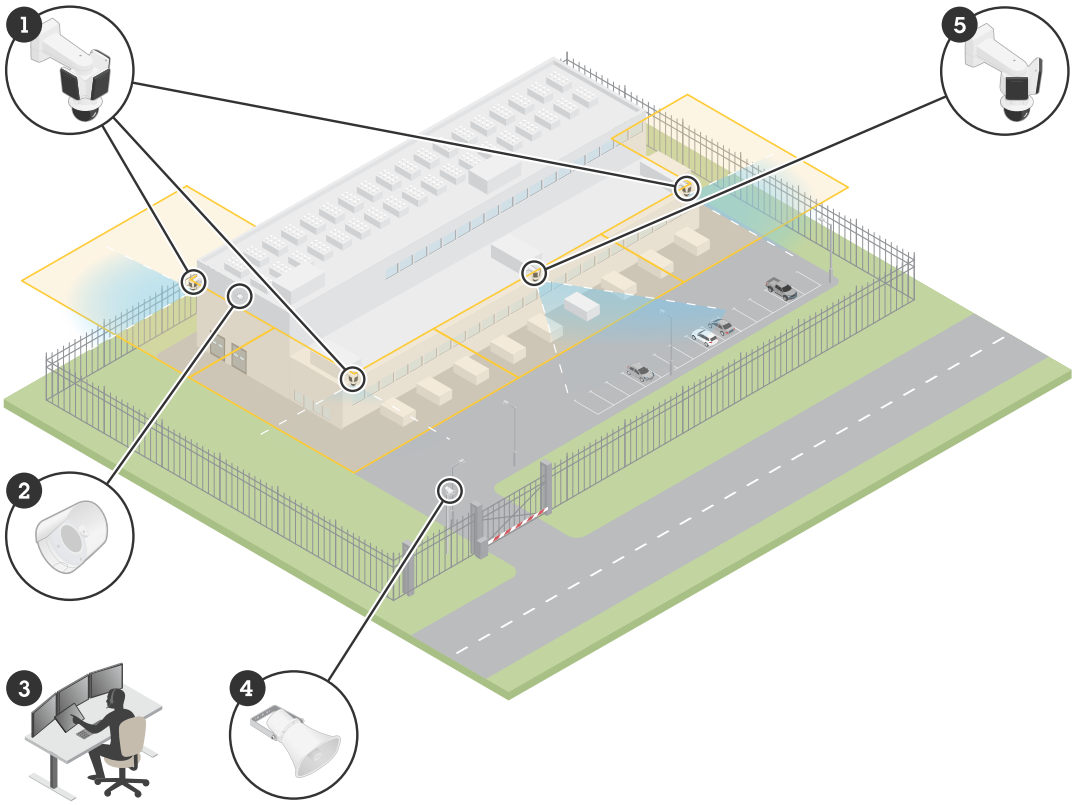
Radary serii AXIS D21-VE Radar

AXIS D2122-VE Radar
AXIS D2123-VE Radar

Podręcznik użytkownika

Spis treści

Informacje o rozwiązaniu



Przykład rozwiązania dozorowego w centrum przetwarzania danych.

1 *Radar AXIS D2123-VE Radar sparowany z kamerą PTZ AXIS Q6358-LE PTZ Camera*
2 *Głośnik z sygnalizatorem optycznym AXIS D4200-VE Strobe Speaker*
3 *Centrum monitoringu*
4 *Głośnik tubowy AXIS C1310-E Horn Speaker*
5 *Radar AXIS D2122-VE Radar sparowany z kamerą PTZ AXIS Q6358-LE PTZ Camera*

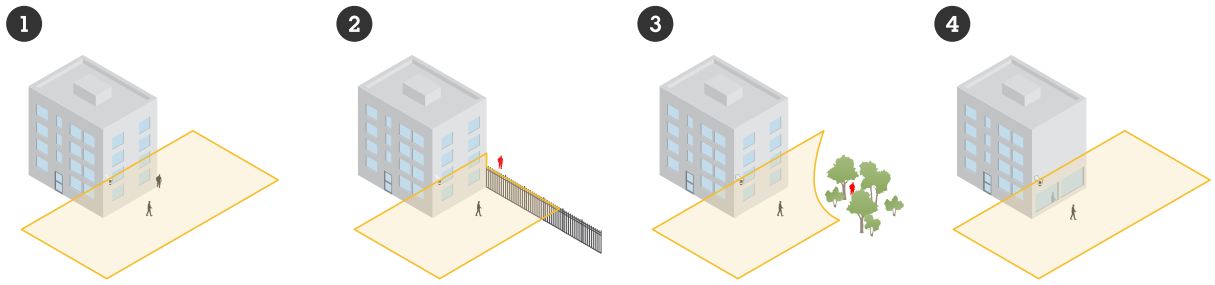
Instalacja

Aby obejrzeć ten film wideo, przejdź do internetowej wersji dokumentu.

W tym filmie przedstawiono przykładową instalację radaru serii AXIS D21-VE Radar. Informacje dotyczące wszystkich scenariuszy instalacji oraz informacje dotyczące bezpieczeństwa znajdują się w instrukcji instalacji.

Uwagi

- Radar jest przeznaczony do dozoru otwartych obszarów (1). Każdy jednorodny obiekt taki jak ściana, ogrodzenie, drzewo czy wysoki krzew w scenie tworzy za sobą martwy punkt, tzw. cień radarowy (2, 3). Wysokość montażu wpływa na wielkość cienia radarowego.
- W przypadku bardziej złożonych scen, zawierających przykładowo powierzchnie odblaskowe, zaleca się stosowanie technologii połączenia funkcji radaru i obrazu obejmującej wybrane kamery PTZ.
- Radar działa najlepiej, gdy powierzchnia gruntu jest pokryta nawierzchnią utwardzoną w rodzaju asfaltu lub kostki brukowej. Gdy powierzchnia gruntu pokryta jest żwirem lub trawą, skuteczność detekcji może być gorsza.
- W przypadku zamocowania radaru na ścianie sprawdź, czy w odległości jednego metra (3 ft) po lewej i po prawej stronie radaru nie ma żadnych innych obiektów ani instalacji. Obiekty takie będą bowiem odbijać fale radiowe, wpływając niekorzystnie na sprawność radaru.
- Jeżeli instalujesz radar na słupie, sprawdź, czy słup jest stabilny. Radar ma mechanizm stabilizacji, który można włączyć, ale który może wpływać na czułość radaru lub czas potrzebny do wykrycia poruszającego się obiektu.
- Metalowy obiekt lub powierzchnia odblaskowa w scenie mogą odbijać obraz ludzi lub pojazdów poruszających się w pobliżu i przez to powodować odbicie wiązki radarowej lub wiązki widma (4). Może to wpływać na możliwości klasyfikacji przez radar i powodować fałszywe alarmy. Do filtrowania takiego rodzaju odbić możesz użyć stref wykluczenia. Możesz też zminimalizować wpływ odbić, parując kamerę z radarem.
- Zalecana wysokość instalacji podana jest w karcie katalogowej na stronie *axis.com*.



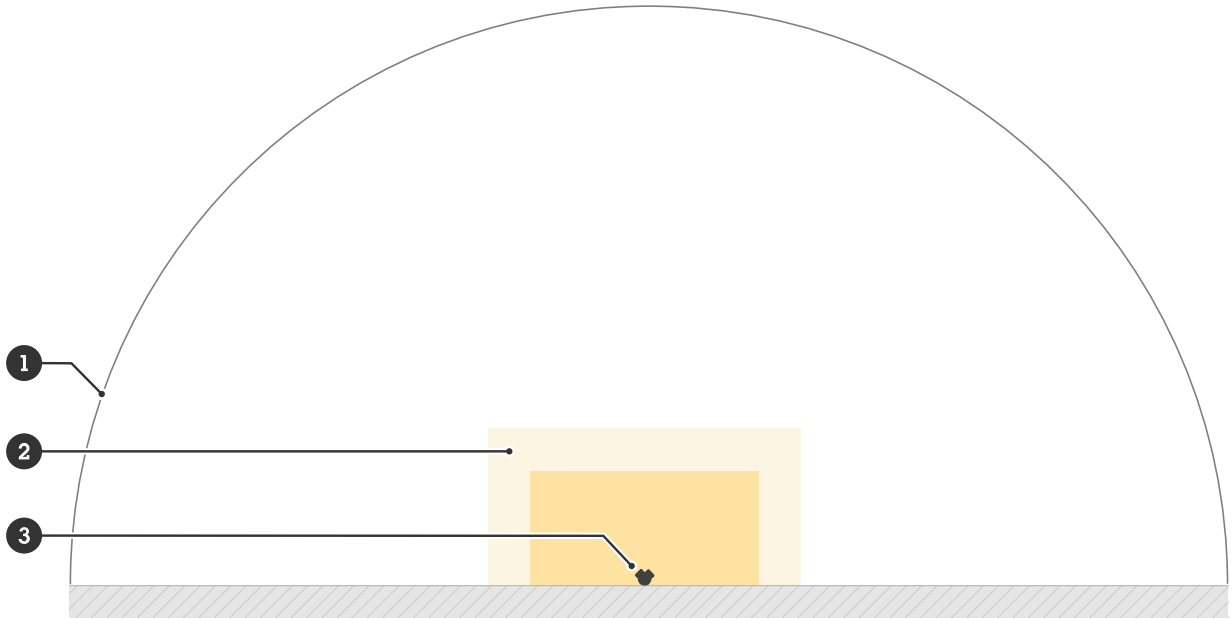
Monitorowanie sceny

Radar wykrywa poruszające się obiekty i klasyfikuje je jako ludzie, pojazdy lub obiekty nieznane. W czasie dozoru obszaru używaj profilu **Area monitoring** (Monitorowanie obszaru).

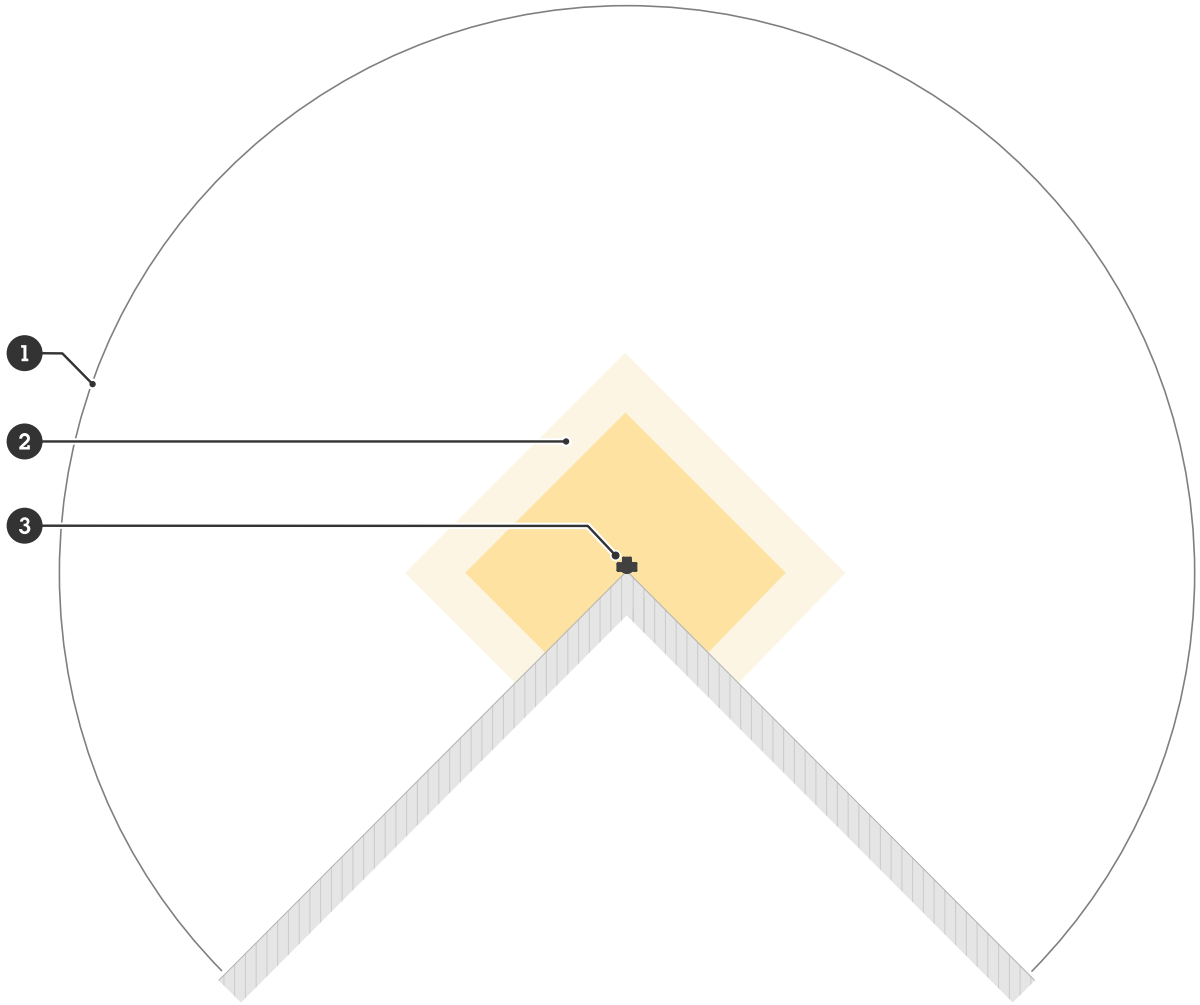
Instalacja wielu radarów

Aby zapewnić dozór takich obszarów jak otoczenie budynku czy strefa buforowa poza ogrodzeniem, można zainstalować kilka radarów obok siebie. Każdy radar może współdziałać z maksymalnie jedenastoma innymi radarami AXIS D2122-VE lub AXIS D2123-VE w promieniu 500 m (1640 ft), co tworzy tzw. strefę stosowania

wielu radarów. Instalację tego modelu można też przeprowadzić w strefie stosowania poprzednich modeli radarów Axis, jako że modele nie zakłócają się wzajemnie. Więcej informacji o strefie stosowania wielu radarów, p. sekcja *Obszar współistnienia, on page 24*.



1 Obszar współistnienia
2 Strefa detekcji
3 AXIS D2122-VE Radar



1 Obszar współistnienia
2 Strefa detekcji
3 AXIS D2123-VE Radar

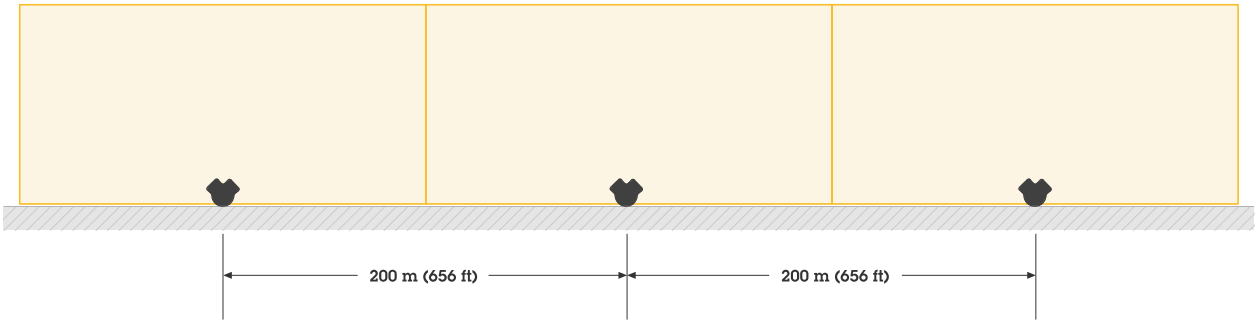
Uwaga

Na działanie radarów w strefie stosowania wielu radarów mogą wpływać czynniki środowiskowe oraz skierowanie radaru w stronę ogrodzeń, budynków lub pobliskich radarów.

Przykłady instalacji

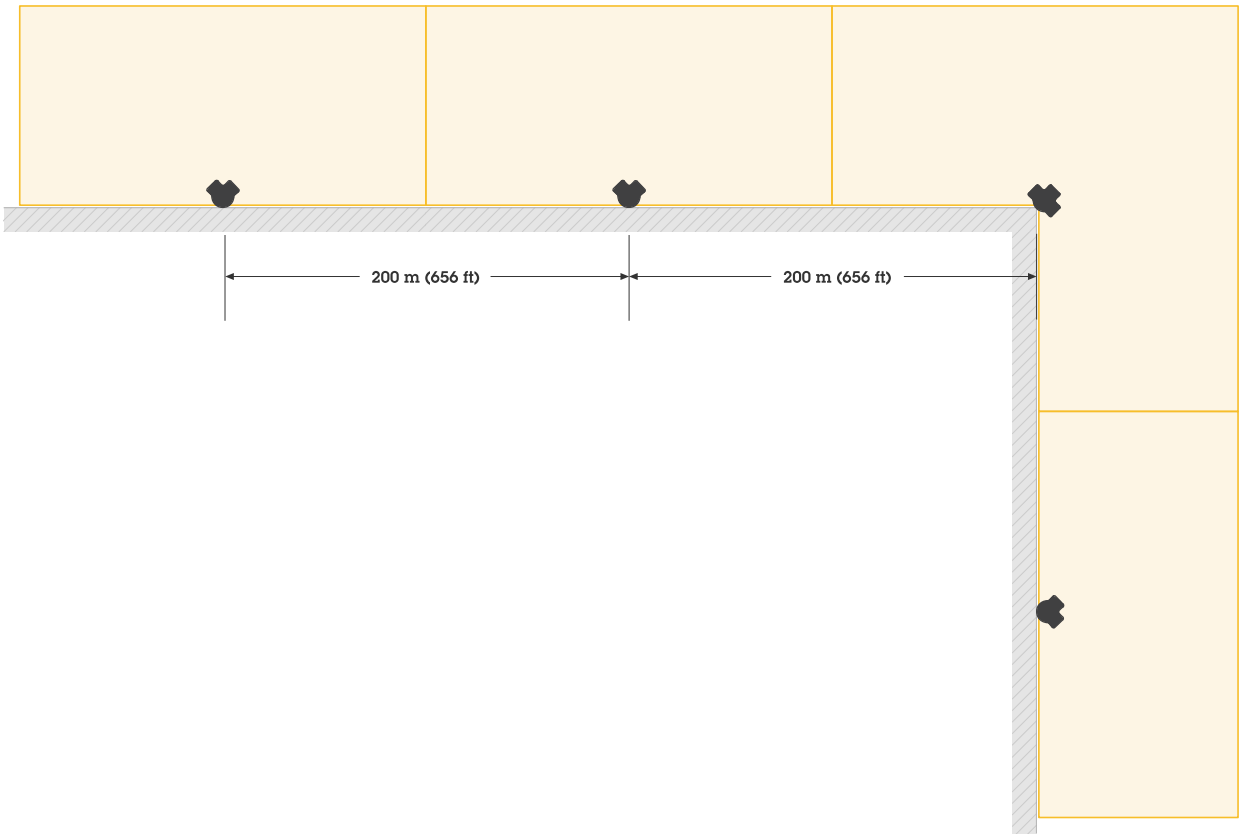
Tworzenie wirtualnego ogrodzenia z kilkoma radarami

Aby utworzyć wirtualne ogrodzenie, np. wokół budynku, umieść kilka radarów obok siebie. Zaleca się rozmieszczenie ich w odstępach co 200 m (656 ft).



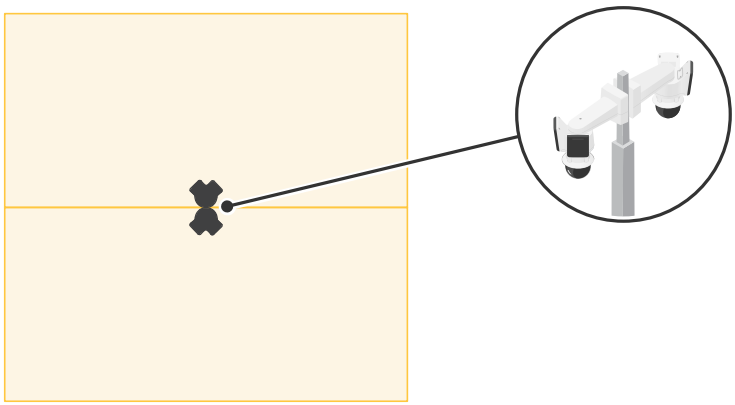
Pokrycie obszaru wokół budynku

Aby monitorować obszar wokół budynku, umieść radary na ścianach budynku, tak aby były skierowane na zewnątrz.



Pokrycie otwartego obszaru

Aby monitorować duży otwarty obszar, użyj dwóch uchwytów do montażu na słupie do zamontowania dwóch radarów AXIS D2122-VE Radar tyłem do siebie.

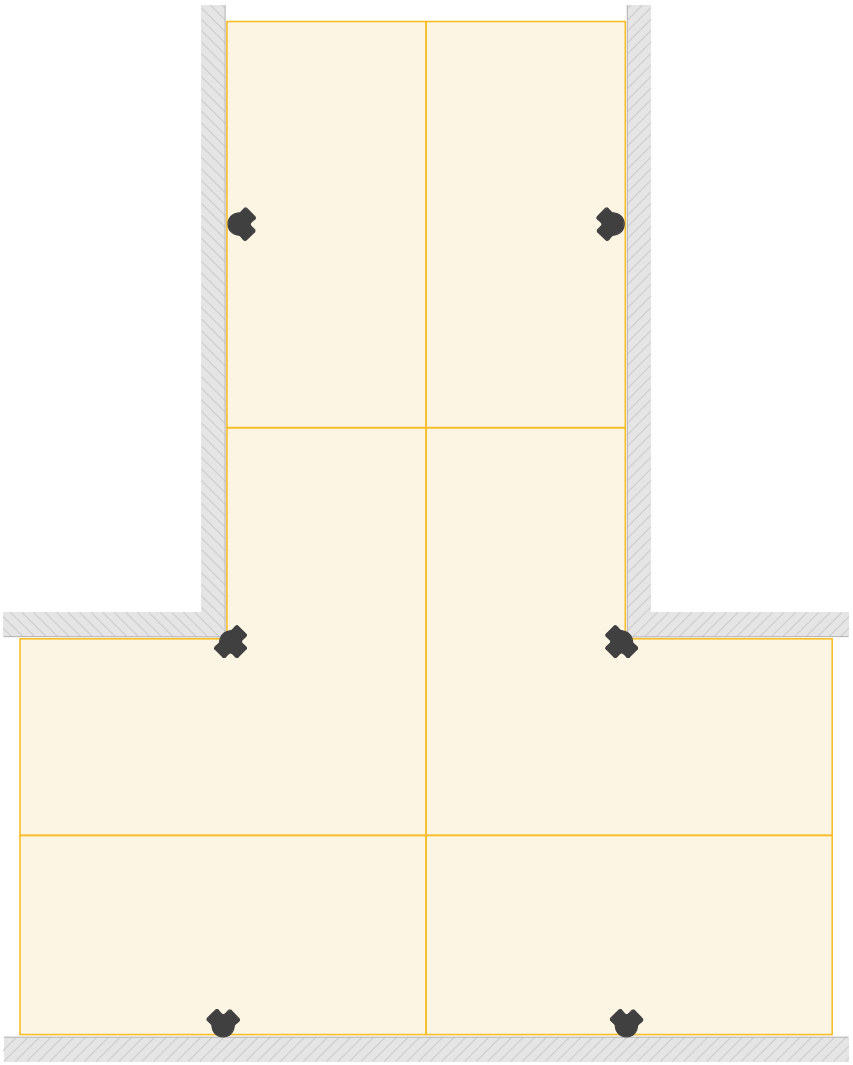


Uwaga

Każdy radar podaje na wyjście PoE zasilanie o mocy maks. 60 W, o ile jest zasilany z modułu zasilania pośredniego o mocy 90 W. Wyjście PoE wymaga standardu zasilania Power over Ethernet IEEE 802.3bt, typ 4 klasa 8.

Instalacja radarów ustawionych naprzeciwko siebie

Aby dozorować obszar przykładowo między budynkami, umieść radary naprzeciw siebie. W tym samym obszarze stosowania wielu radarów może znajdować się maks. 12 radarów skierowanych na siebie.

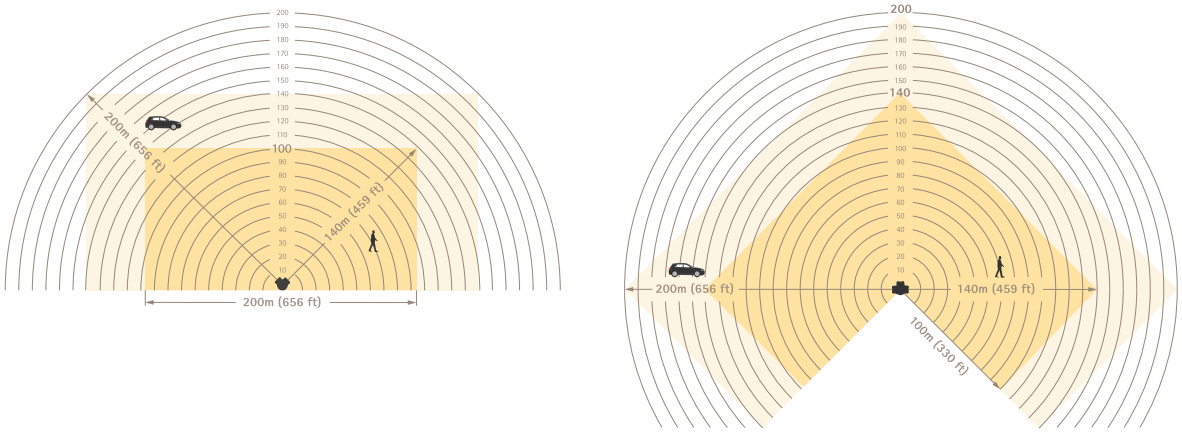


Odległości rozpoznania i detekcji

Po zamontowaniu radaru na optymalnej wysokości:

- W strefie rozpoznania można wykrywać i klasyfikować ludzi w maksymalnej odległości 100 – 140 m (330 – 459 ft) od radaru w zależności od ich położenia względem radaru.
- W strefie detekcji można wykrywać pojazdy w maksymalnej odległości 140 – 200 m (459 – 656 ft) od radaru w zależności od:
  - szybkości pojazdu
  - kierunku ruchu względem radaru
  - płaszczyzny podłoża
  - materiału podłoża

Więcej informacji o strefach, p. sekcja *Strefy rozpoznania i detekcji, on page 24*.



Odległości rozpoznania i detekcji

Uwaga

- Podczas kalibracji radaru w interfejsie internetowym urządzenia wprowadź faktyczną wysokość montażu.
- Na odległość rozpoznania i detekcji ma wpływ zawartość sceny.
- Odległości rozpoznania i detekcji są różne dla różnych rodzajów obiektów.

Odległości rozpoznania i detekcji zmierzono w następujących warunkach:

- Odległość zmierzona na płaskim, poziomym terenie.
- Radar zamontowano bez pochylenia.
- Obiektem była osoba o wzroście 170 cm (5 ft 7 in).
- Osoba była dobrze widoczna z radaru.
- Czułość radaru została ustawiona jako **Medium (Średnia)**.

Radar nie wykrywa obiektów znajdujących się bliżej niż minimalna odległość detekcji. Minimalna odległość detekcji zależy od wysokości montażu radaru:

Wysokość montażowa	Minimalnej odległości detekcji
4 m (9,8 ft)	4 m (9,8 ft)
5 m (16,4 ft)	6 m (19,7 ft)
6 m (19,7 ft)	8 m (26 ft)
7 m (23 ft)	11 m (36 ft)
8 m (26 ft)	13 m (42,7 ft)
9 m (29,5 ft)	15 m (49,2 ft)
10 m (32,8 ft)	18 m (59 ft)

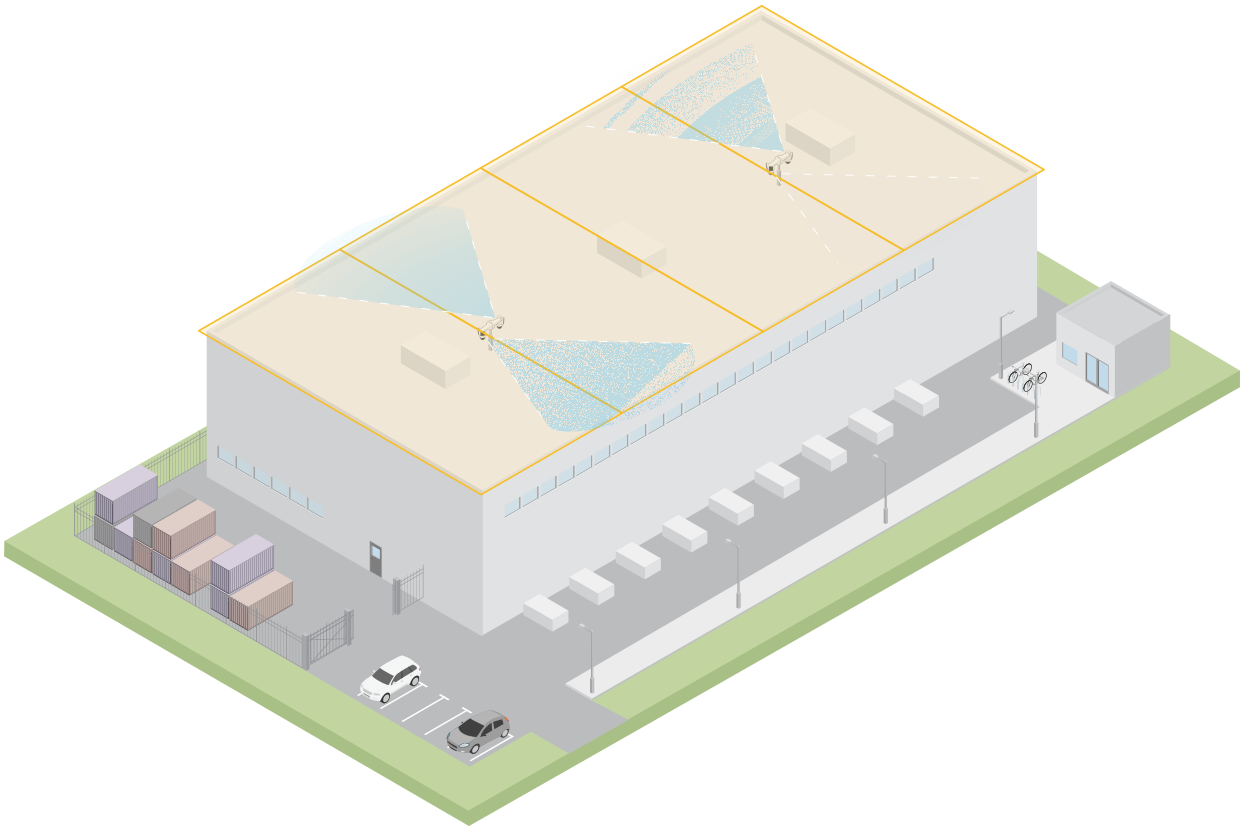
Uwaga

Po sparowaniu radaru z kamerą PTZ kamera może kontynuować śledzenie obiektu nawet przy minimalnej odległości detekcji radaru.

Zastosowania

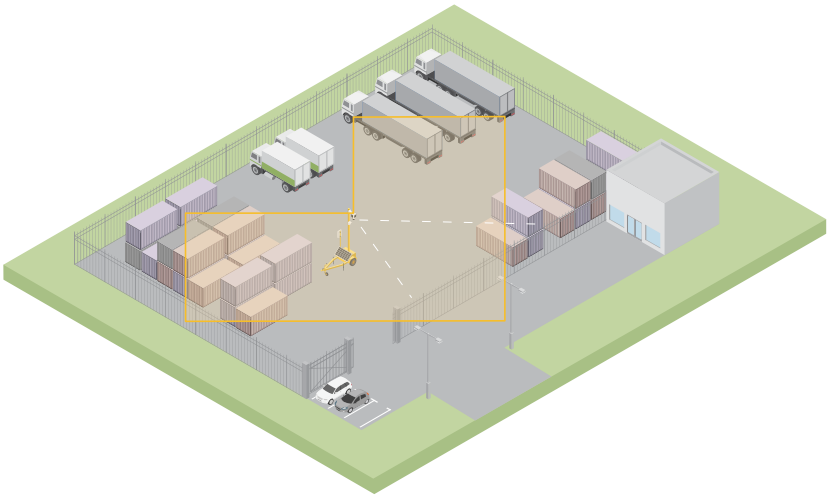
Dozór powierzchni dachu

Duże centrum dystrybucyjne chce wykorzystać radary do dozoru obszaru dachu. Radary są sparowane z kamerami PTZ ARTPEC-9 i zamontowane tyłem do siebie na słupach, obejmując całą powierzchnię dachu. Radar wykrywa i klasyfikuje poruszające się obiekty na dachu, kieruje kamerę na obiekt i umożliwia kamerze weryfikację tejże klasyfikacji. Kamera wykorzystuje funkcję automatycznego śledzenia do kontynuowania śledzenia obiektu.



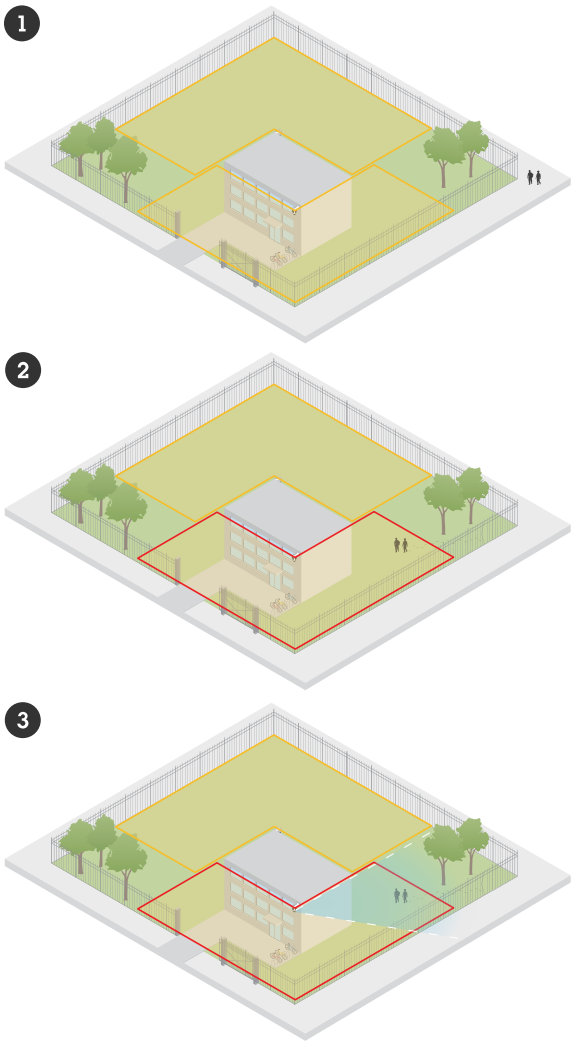
Użyj przyczepy samochodowej z instalacją dozorową, aby dozorem objąć rozległy obszar

Na zewnętrznym dziedzińcu sklepu z artykułami metalowymi doszło do kilku włamań po godzinach pracy. Sklepu pilnuje pracownik ochrony, ale za konieczne uznano zwiększenie bezpieczeństwa w nocy bez ponoszenia kosztów związanych z zatrudnieniem kolejnych pracowników. Postanowiono zainstalować dwa radary zamontowane tyłem do siebie na przyczepie samochodowej z instalacją dozorową, by objęły cały dziedziniec. Radary zostały skonfigurowane tak, by ostrzegały o podejrzanym zachowaniu, dzięki czemu strażnik może skontrolować miejsce zdarzenia. Rozważana jest również możliwość instalacji głośnika z sygnalizatorem optycznym uruchamianego przez radary do odstraszania intruzów.



Pokrycie ogrodzonego budynku

W poniższym scenariuszu kamera PTZ została zamontowana wraz z radarem celem weryfikacji alarmów i zapewnienia dokładnej klasyfikacji dzięki technologii połączenia funkcji radaru i obrazu.



1. Osoby poruszające się poza ogrodzeniem nie wywołują alarmu.
2. Intruzi przechodzący przez ogrodzenie wpadają w zasięg radaru, który ich wykrywa i uruchamia alarm.
3. Radar kieruje kamerę PTZ na intruzów i umożliwia jej potwierdzenie alarmu dzięki analizie obrazu.

Więcej informacji znajduje się w rozdziale *Automatyczne śledzenie ruchu, on page 25*.

Od czego zacząć

Wyszukiwanie urządzenia w sieci

Aby znaleźć urządzenia Axis w sieci i przydzielić im adresy IP w systemie Windows®, użyj narzędzia AXIS IP Utility lub AXIS Device Manager. Obie aplikacje są darmowe i można je pobrać ze strony *axis.com/support*.

Więcej informacji na temat wykrywania i przydzielania adresów IP znajduje się w dokumencie *Jak przydzielić adres IP i uzyskać dostęp do urządzenia*.

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

	Chrome™	Edge™	Firefox®	Safari®
Windows®	✓	✓	*	*
macOS®	✓	✓	*	*
Linux®	✓	✓	*	*
Inne systemy operacyjne	*	*	*	*

✓: zalecane

*: obsługiwane z ograniczeniami

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis.
   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora, on page 14*.

Opisy wszystkich funkcji i ustawień interfejsu WWW urządzeń z systemem operacyjnym AXIS OS można znaleźć na stronie *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła, on page 15*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne, on page 32*.

Bezpieczne hasła

Ważne

Używaj protokołu HTTPS (który jest domyślnie włączony), aby ustawić hasło lub skonfigurować inne poufne dane przez sieć. Protokół HTTPS umożliwia nawiązywanie bezpiecznych, szyfrowanych połączeń sieciowych, chroniąc w ten sposób poufne dane, takie jak hasła.

Hasło urządzenia stanowi podstawową ochronę danych i usług. Urządzenia Axis nie narzucają zasad haseł, ponieważ mogą być one używane w różnych typach instalacji.

Aby chronić dane, zalecamy:

- Używanie haseł o długości co najmniej ośmiu znaków, najlepiej utworzonego automatycznym generatorem haseł.
- Nieujawnianie haseł.
- Regularną zmianę haseł co najmniej raz na rok.

Konfiguracja urządzenia

Aby w pełni wykorzystać możliwości urządzenia, zaleca się wykonanie następujących czynności:

1. *Ustawianie poziomu montażu, on page 16*
2. Jeżeli instalujesz kilka radarów blisko siebie: *Ustawienie liczby pobliskich radarów, on page 16*
3. *Dodawanie mapy jako odniesienia, on page 16*
4. *Tworzenie scenariusza detekcji obiektów, on page 17*
5. *Minimalizowanie fałszywych alarmów, on page 18*
6. *Sprawdzanie poprawności instalacji, on page 19*

Ustawianie poziomu montażu

Ustaw wysokość montażu radaru w interfejsie internetowym. Właściwa wysokość montażu jest niezbędna do prawidłowej detekcji i pomiaru szybkości obiektów znajdujących się w zasięgu radaru. Bardzo ważne jest również prawidłowe działanie funkcji automatycznego śledzenia.

Zmierz wysokość od podłoża do radaru jak najdokładniej. W przypadku scen z nierównymi powierzchniami należy ustawić wartość odpowiadającą średniej wysokości sceny.

1. Przejdź do menu **Radar > General (Radar > Ogólne)**.
2. Ustaw wysokość w menu **Mounting height (Poziom montażu)**.

Ustawienie liczby pobliskich radarów

Jeżeli instalujesz inne radary tego samego modelu w strefie stosowania kilku radarów, podaj liczbę pobliskich radarów w interfejsie internetowym każdego z nich. Poprawi to sprawność działania radarów i zminimalizuje ryzyko wystąpienia zakłóceń.

1. Otwórz menu **Radar > Settings > Coexistence (Radar > Ustawienia > Jednoczesna obecność)**.
2. Wybierz liczbę pobliskich radarów w strefie stosowania kilku radarów.

Dodawanie mapy jako odniesienia

Aby usprawnić ustawianie scenariuszy i dowiedzieć się, gdzie w scenie poruszają się obiekty, możesz użyć mapy jako tła w obszarze działania radaru. Można użyć planu terenu lub zdjęcia lotniczego przedstawiającego obszar objęty radarem. Dostosuj i skalibruj mapę tak, aby obszar pokrycia radaru pasował do pozycji, kierunku i skali mapy, a następnie zbliż mapę, o ile interesuje cię konkretna część sceny.

Możesz skorzystać z asystenta ustawień, który krok po kroku przeprowadzi cię przez kalibrację mapy, lub edytować każde ustawienie z osobna.

Use the setup assistant (Użyj asystenta ustawień):

1. Przejdź do menu **Radar > Map calibration (Radar > Kalibracja mapy)**.
2. Kliknij **Setup assistant (Asystent ustawień)** i postępuj zgodnie z instrukcjami.

Aby usunąć przesłaną mapę i dodane ustawienia, kliknij **Reset calibration (Resetuj kalibrację)**.

Edit each setting individually (Edytuj każde ustawienie z osobna):
Mapa kalibruje się stopniowo po dostosowaniu każdego ustawienia.

1. Przejdź do menu **Radar > Map calibration (Kalibracja mapy) > Map (Mapa)**.
2. Wybierz obraz, który chcesz przesłać, lub przeciągnij go do wyznaczonego obszaru.
   Aby ponownie użyć obrazu mapy z bieżącymi ustawieniami obrotu i zoomowania, kliknij **Download map (Pobierz mapę)**.
3. W obszarze **Rotate map (Obróć mapę)** użyj suwaka, aby obrócić mapę w odpowiednie położenie.
4. Przejdź do sekcji **Scale and distance on a map** (Skala i odległość na mapie) i kliknij dwa wcześniej określone punkty na mapie.

5. W sekcji **Distance (Odległość)** dodaj rzeczywistą odległość między dwoma punktami dodanymi do mapy.
6. Przejdź do sekcji **Pan and zoom map (Obracanie i zoomowanie mapy)** i korzystaj z przycisków w celu obracania lub powiększania i pomniejszania obrazu mapy.

Uwaga

- Funkcja zoomu nie zmienia obszaru widoku radaru. Jeżeli nawet po użyciu zoomu część widoku jest zasłonięta, radar nadal wykrywa poruszające się obiekty w całym widoku. Jedynym sposobem na wykluczenie wykrywanego ruchu jest dodanie stref wykluczenia.
- W każdej chwili można dostosować obrót i zoom w pozycjach **Map calibration** (Kalibracja mapy), **Exclusion zones** (Strefy wykluczenia) lub **Scenarios** (Scenariusze), klikając .

7. Przejdź do sekcji **Radar position (Pozycja radaru)** i korzystaj z przycisków w celu przesuwania lub obracania pozycji radaru na mapie.

Aby usunąć przesłaną mapę i dodane ustawienia, kliknij **Reset calibration (Resetuj kalibrację)**.

Film przedstawia przykład kalibrowania mapy referencyjnej w radarze lub kamerze z syntezą radaru i wideo firmy Axis.

Tworzenie scenariusza detekcji obiektów

Dzięki scenariuszowi możesz wykryć lub rozpoznać obiekty poruszające się w scenie. Aby uruchomić działania po spełnieniu warunków określonych w scenariuszu, utwórz regułę w sekcji **Events** (Zdarzenia). Możesz utworzyć kilka scenariuszy do wykrywania różnych zachowań lub pokrycia różnych części sceny.

1. Wybierz kolejno opcje **Radar > Scenarios (Radar > Scenariusze)**.
2. Kliknij **Add scenario (Dodaj scenariusz)**.
3. Wpisz nazwę scenariusza.
4. Pozwala wybrać, czy warunkiem wyzwalania mają być obiekty przemieszczające się wewnątrz obszaru lub naruszające linię.
5. Kliknij **Next (Dalej)**.
6. W przypadku scenariuszy **Movement in area** (Ruch w obszarze):
   6.1. Wybierz kształt strefy.
   Użyj myszy, aby przesunąć i dostosować strefę, tak aby obejmowała tylko potrzebną część widoku radaru lub mapy referencyjnej.
7. W przypadku scenariuszy **Line crossing** (Naruszenie linii):
   7.1. Umieść linię w scenie.
   Za pomocą myszy przesuń linię.
   7.2. Aby zmienić kierunek detekcji, włącz opcję **Change direction (Zmień kierunek)**.
   7.3. Aby obiekt musiał naruszyć dwie linie, by nastąpiło uruchomienie działań, włącz opcję **Require crossing of two lines** (Wymagaj naruszenia dwóch linii).
   Umieść drugą linię w scenie.
8. Kliknij **Next (Dalej)**.
9. Dodaj ustawienia detekcji.
   9.1. W przypadku scenariuszy **Movement in area** (Ruch w obszarze) i **Line crossing** (Naruszenie linii) przy jednej linii dodaj czas opóźnienia, aby zminimalizować fałszywe alarmy w pozycji **Ignore short-lived objects** (Ignoruj obiekty krótkotrwałe).

9.2. W przypadku scenariuszy **Line crossing** (Naruszenie linii) przy dwóch liniach ustaw limit czasu między przekroczeniem pierwszej i drugiej linii w pozycji **Max time between crossings** (Maksymalny czas pomiędzy naruszeniami).

9.3. Wybierz typ wyzwalającego obiektu w obszarze **Trigger on object type (Typ wyzwalającego obiektu)**.

9.4. Dodaj zakres szybkości w obszarze **Speed limit** (Ograniczenie szybkości).

10. Kliknij **Next (Dalej)**.
11. Ustaw minimalny czas trwania alarmu w obszarze **Minimum trigger duration (Minimalny czas alarmu)**. W przypadku scenariuszy **Line crossing** (Naruszenie linii) skróć czas trwania do 0 s, jeżeli obiekty mają uruchamiać działania natychmiast po naruszeniu linii.
12. Kliknij przycisk **Zapisz**.

Minimalizowanie fałszywych alarmów

Jeżeli fałszywych alarmów jest wiele, spróbuj zminimalizować ich liczbę, zmieniając różne ustawienia. Możesz na przykład odfiltrować określone rodzaje ruchu lub obiektów, dostosować strefy, w których obiekty uruchamiają alarmy, albo dostosować czułość detekcji.

- Wyreguluj czułość detekcji radaru:
  Przejdź do **Radar > Settings > Detection** (Radar > Ustawienia > Detekcja) i zmniejsz czułość detekcji w pozycji **Detection sensitivity**.
  Ustawienie czułości dotyczy wszystkich stref.
  - Niższa czułość detekcji sprawdza się, gdy w scenie jest wiele metalowych obiektów lub dużych pojazdów. Zmniejsza ryzyko fałszywych alarmów, jednak ogranicza też zdolność radaru do klasyfikowania małych obiektów.
  - Wyższa czułość detekcji jest natomiast odpowiednia dla otwartych przestrzeni, takich jak pola, pozbawionych metalowych obiektów.
- Zmiana stref włączenia i wykluczenia:
  Twarde powierzchnie w scenie mogą powodować odbicia skutkujące wielokrotnymi detekcjami jednego obiektu fizycznego. W takiej sytuacji możesz dostosować kształt strefy włączenia w scenariuszu lub dodać ogólną strefę wykluczenia, by pominąć określoną część sceny.
- Wyzwalanie w przypadku obiektów przekraczających dwie linie zamiast jednej:
  Jeżeli w scenariuszu naruszenia linii scena zawiera kołyszące się obiekty lub zwierzęta, istnieje ryzyko, że obiekt naruszy linię i wywoła fałszywy alarm. W takim przypadku scenariusz możesz dostosować tak, by alarm był wyzwalany tylko, gdy obiekt naruszy dwie linie.
- Filtrowanie przy określonym ruchu:
  - Aby zminimalizować liczbę fałszywych alarmów powodowanych przez drzewa, krzewy bądź flagi w scenie, przejdź do **Radar > Settings > Detection** (Radar > Ustawienia > Detekcja) i włącz opcję **Ignore swaying objects** (Ignoruj kołyszące się obiekty).
  - Aby zminimalizować liczbę fałszywych alarmów powodowanych przez małe obiekty, takie jak koty czy lisy w scenie, przejdź do **Radar > Settings > Detection** (Radar > Ustawienia > Detekcja) i włącz opcję **Ignore small objects** (Ignoruj małe obiekty). Ustawienie to dostępne jest w profilu dozoru obszaru.
- Filtrowanie według czasu:
  - Wybierz kolejno opcje **Radar > Scenarios (Radar > Scenariusze)**.
  - Zaznacz scenariusz i kliknij ⋮, aby zmodyfikować jego ustawienia.
  - Zwiększ wartość w polu **Seconds until trigger** (Sekundy do wyzwolenia). Jest to wartość czasu, przez jaką radar śledzi obiekt przed wyzwoleniem alarmu. Odliczanie rozpoczyna się od wykrycia obiektu przez radar, a nie pojawienia się obiektu w strefie włączenia w scenariuszu.
- Filtrowanie według typu obiektów:
  - Wybierz kolejno opcje **Radar > Scenarios (Radar > Scenariusze)**.

- Zaznacz scenariusz i kliknij ⋮, aby zmodyfikować jego ustawienia.
- Jeżeli nie chcesz wyzwalać alarmu po wykryciu konkretnych rodzajów obiektów, usuń rodzaje obiektów, które nie mają wyzwalać alarmów w scenariuszu.

Sprawdzanie poprawności instalacji

Sprawdzanie poprawności instalacji radaru

Przed rozpoczęciem korzystania z radaru zaleca się sprawdzenie poprawności jego instalacji. Sprawdzenie to będzie pomocne w razie potrzeby identyfikacji problemów związanych z instalacją lub zarządzaniem obiektami statycznymi w scenie takimi jak drzewa lub powierzchnie odblaskowe.

Uwaga

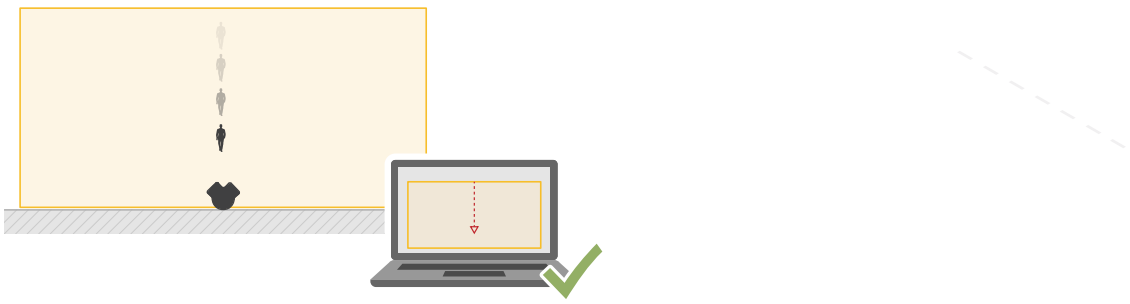
Instalację uznaje się za sprawdzoną na warunkach obowiązujących w czasie sprawdzania. Zmiany warunków w scenie mogą wpływać na codzienne działanie instalacji.

Sprawdź, czy nie ma fałszywych detekcji

1. Sprawdź, czy strefa rozpoznania jest wolna od aktywności ludzi.
2. Poczekaj kilka minut, aby upewnić się, że w strefie rozpoznania radar nie wykrywa żadnych obiektów statycznych.
3. W razie zbędnych detekcji możesz odfiltrować określone rodzaje ruchu lub obiektów, dostosować strefy, w których obiekty uruchamiają alarmy, albo dostosować czułość detekcji. Instrukcje: *Minimalizowanie fałszywych alarmów, on page 18*.

Sprawdź, czy symbol, kierunek przemieszczania i pozycja na mapie są prawidłowe

1. W interfejsie internetowym radaru uruchom zapis. Instrukcje: *Rejestracja i odtwarzanie obrazu, on page 21*.
2. Idź tuż poza strefą rozpoznania i kieruj się bezpośrednio w stronę radaru.
3. Sprawdź, czy po wejściu człowieka do strefy rozpoznania wyświetla się symbol klasyfikacji osoby.
4. Sprawdź, czy w interfejsie WWW radaru jest widoczny prawidłowy kierunek ruchu.



5. Sprawdź, czy rzeczywista pozycja człowieka jest zgodna z pozycją na mapie.

Utwórz tabelę podobną do poniższej, aby ułatwić sobie zapisywanie danych z procesu sprawdzania poprawności działania radaru.

Testuj	Pass/Fail (Powodzenie/ Niepowodzenie)	Uwagi
1. Sprawdź, czy w pustym obszarze nie występują żadne niepożądane detekcje.		

2. Sprawdź, czy po wejściu człowieka do strefy rozpoznania wyświetla się symbol klasyfikacji osoby.		
3. Sprawdź, czy kierunek przemieszczania się jest prawidłowy.		
4. Sprawdź, czy rzeczywista pozycja człowieka jest zgodna z pozycją na mapie.		

Zakończenie sprawdzania poprawności

Po pomyślnym wykonaniu pierwszej części procedury należy wykonać następujące testy w celu dokończenia procesu sprawdzania poprawności.

1. Sprawdź, czy radar został skonfigurowany zgodnie z podanymi instrukcjami.
2. Sprawdź, czy dodałeś i skalibrowałeś mapę odniesienia.
3. Ustaw w radarze scenariusz inicjowany po wykryciu człowieka. Domyślnie liczba sekund do wyzwolenia **(Seconds until trigger)** ustawiona jest na 2 s, ale w razie potrzeby możesz ją zmienić.
4. Ustaw w radarze zapisywanie obrazu po wykryciu odpowiedniego obiektu.
   Instrukcje: *Rejestracja i odtwarzanie obrazu, on page 21*.
5. Przejdź do **Radar > Settings > Object visualization** (Radar > Ustawienia > Wizualizacja obiektów) i ustaw **Trail lifetime** (Czas trwania śladu) na 1 godz., tak aby w bezpieczny sposób przekraczał czas potrzebny na opuszczenie miejsca, obejście obszaru dozoru i powrót na miejsce. Wybrany czas trwania śladu spowoduje kontynuowanie śledzenia w podglądzie na żywo radaru przez ustawiony czas, a po zakończeniu sprawdzania poprawności możesz go wyłączyć.
6. Przejdź wzdłuż granicy strefy rozpoznania radaru i sprawdź, czy trasa w systemie pokrywa się z przebytą trasą.
7. Jeżeli wyniki sprawdzenia poprawności nie spełnią oczekiwań, skalibruj od nowa mapę referencyjną i powtórz procedurę sprawdzania poprawności.

Regulowanie obrazu radaru

W sekcji tej zawarto informacje o konfigurowaniu obrazu radarowego. Aby dowiedzieć się więcej na temat działania niektórych funkcji, przejdź do *Więcej informacji, on page 24*.

Wyświetlanie nakładek na obrazie

Możesz dodać obraz jako nałożenie do strumienia radaru.

1. Wybierz kolejno opcje **Radar > Overlays (Radar > Nakładki)**.
2. Kliknij **Manage images (Zarządzaj obrazami)**.
3. Prześlij lub przeciągnij i upuść obraz.
4. Kliknij przycisk **Upload (Prześlij)**.
5. Wybierz **Image (Obraz)** z listy rozwijanej i kliknij **+**.
6. Wybierz obraz i położenie. Aby zmienić położenie obrazu nakładki, można go również przeciągnąć w podglądzie na żywo.

Przeglądanie i rejestracja obrazów wideo

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej o działaniu strumieniowania i pamięci masowej, przejdź do *Strumieniowanie i pamięć masowa, on page 25*.

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z radaru

1. Wybierz kolejno opcje **Radar > Stream (Radar > Strumień)**.
2. Aby rozpocząć nagrywanie, kliknij .

   Jeżeli jeszcze nie skonfigurowano żadnej pamięci masowej, kliknij i . Aby uzyskać instrukcje dotyczące konfigurowania sieciowej pamięci masowej, zob.
3. Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

1. Przejdź do menu **Recordings (Nagrania)**.
2. Kliknij obok wybranego nagrania na liście.

Konfiguracja reguł dotyczących zdarzeń

Można utworzyć reguły sprawiające, że urządzenie będzie wykonywać konkretne akcje po wystąpieniu określonych zdarzeń. Reguła składa się z warunków i akcji. Warunki mogą służyć do wyzwalania akcji. Urządzenie może na przykład rozpocząć zapis lub wysłać wiadomość e-mail po wykryciu ruchu albo wyświetlić nałożony tekst podczas rejestracji.

Aby dowiedzieć się więcej, zob. *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Wyzwalanie akcji

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę. Reguła określa, kiedy urządzenie wykona określone działania. Reguły można ustawić jako zaplanowane, cykliczne lub wyzwalane ręcznie.
2. Wprowadź **Name (Nazwę)**.
3. Wybierz **Condition (Warunek)**, który ma zostać spełniony w celu wyzwolenia akcji. Jeżeli w regule akcji zostanie określony więcej niż jeden warunek, wszystkie muszą zostać spełnione, aby wyzwolić akcję.
4. Wybierz działanie (**Action**) do wykonania po spełnieniu warunków.

Uwaga

- Po dokonaniu zmian w aktywnej regule należy ją uruchomić ponownie, aby uwzględnić zmiany.
- Jeżeli zostanie zmieniona definicja profilu strumieniowania stosowana w regule, konieczne jest ponowne uruchomienie wszystkich reguł wykorzystujących ten profil strumieniowania.

Włączanie czerwonego światła ostrzegawczego na radarze

Z przodu radaru możesz włączyć dynamiczny pasek LED, który będzie wskazywał, że obszar jest dozorowany.

Przykład ten pokazuje, jak uaktywnić czerwone światło ostrzegawcze po godzinach pracy w dni powszednie.

Tworzenie harmonogramu:

1. Przejdź do menu **System (System) > Events (Zdarzenia) > Schedules (Harmonogramy)** i dodaj nowy harmonogram.
2. Wpisz nazwę harmonogramu, na przykład `Weekday nights`.
3. W obszarze **Type (Typ)** wybierz opcję **Schedule (Harmonogram)**.
4. W sekcji **Recurrence** (Powtarzanie) wybierz **Daily** (Codziennie).

5. Ustaw godzinę rozpoczęcia na 18:00.
6. Ustaw godzinę zakończenia na 06:00.
7. W obszarze **Days (Dni)** wybierz Od poniedziałku do piątku.
8. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wpisz nazwę reguły, na przykład `Red sweeping light`.
3. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
4. Z listy harmonogramów wybierz **Weekday nights** (Noce w dni powszednie).
5. Na liście akcji w obszarze **Radar** wybierz **Dynamic LED strip (Dynamiczna taśma LED)**.
6. Wybierz sposób świecenia czerwonego światła ostrzegawczego – **Sweeping red**.
7. Ustaw czas trwania na 12 godzin.
8. Kliknij przycisk **Zapisz**.

Wysyłanie wiadomości e-mail, gdy radar zostanie przykryty metalowym przedmiotem

W tym przykładzie wyjaśniamy, jak utworzyć regułę, która wysyła powiadomienie e-mail, gdy ktoś manipuluje radarem, zakrywając go metalowym przedmiotem, np. arkuszem blachy.

Dodaj odbiorcę wiadomości e-mail:

1. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź nazwę odbiorcy.
3. W obszarze **Type** (Typ) wybierz opcję **Email (E-mail)**.
4. Wprowadź adres e-mail odbiorcy.
5. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
   Radar nie ma własnego serwera poczty e-mail, więc żeby wysłać e-maile, musi zalogować się na serwer poczty.
6. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
7. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

8. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
9. Wpisz nazwę reguły, na przykład `Tampering mail`.
10. Przejdź do listy warunków w menu **Device status (Status urządzenia)**, wybierz **Radar data failure (Błąd danych radaru)**.
11. W menu **Reason (Przyczyna)** wybierz pozycję **Tampering (Sabotaż)**.
12. Z listy akcji w obszarze **Notifications (Powiadomienia)** wybierz opcję **Send notification to email (Wyślij powiadomienie w wiadomości e-mail)**.
13. Wybierz utworzonego odbiorcę.
14. Wpisz temat i treść wiadomości e-mail.
15. Kliknij przycisk **Zapisz**.

Interfejs WWW

Aby zapoznać się ze wszystkimi funkcjami i ustawieniami dostępnymi w interfejsie WWW urządzeń z systemem operacyjnym AXIS OS, przejdź do strony *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Więcej informacji

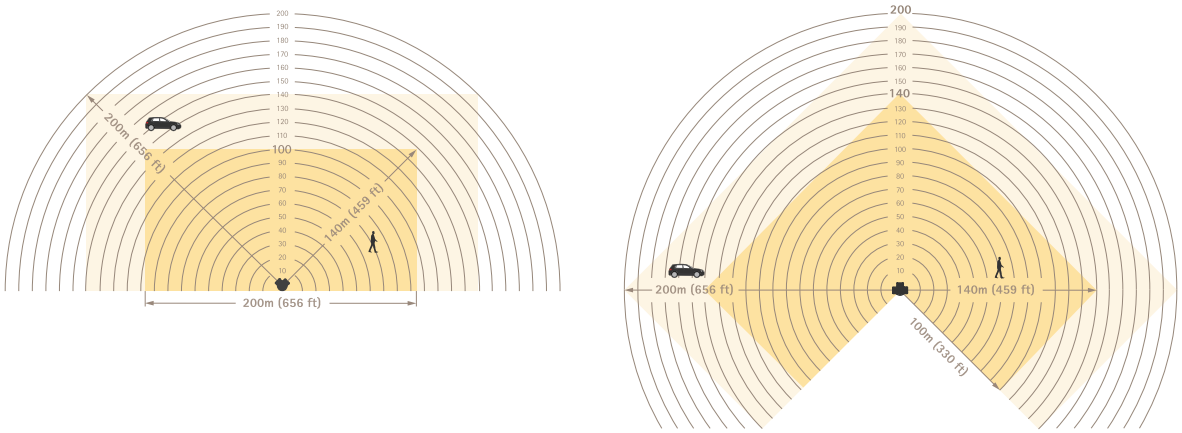
Radar

Strefy rozpoznania i detekcji

Strefa rozpoznania jest obszarem, w którym radar może z całą pewnością sklasyfikować obiekty jako ludzi lub pojazdy.

Strefa detekcji to obszar, w którym radar jest w stanie wykryć szybko poruszające się pojazdy.

Wielkość każdej strefy zależy od wysokości instalacji urządzenia i innych czynników.



Strefa rozpoznania jest ciemnożółta, a strefa detekcji jasnożółta.

Scenariusze, strefy włączenia i strefy wykluczenia

Scenariusz składa się z zestawu warunków, które muszą spełnić poruszające się obiekty, aby uruchomić reguły w systemie zdarzeń. Niektóre z warunków to:

- Rodzaj obiektu (człowiek, pojazd, nieznany)
- Zachowanie obiektu (ruch w obszarze lub naruszenie linii)
- Część sceny (strefa włączenia lub linia wirtualna)
- Prędkość poruszania się obiektu

Strefa włączenia to część sceny, w której następuje wykrywanie i klasyfikacja obiektów w scenariuszu ruchu w obszarze.

Jeżeli w scenie znajdują się obszary, w których poruszające się obiekty nie mają wyzwalać alarmów, możesz utworzyć **strefy wykluczenia**. Możesz również użyć stref wykluczenia, jeżeli w strefie włączenia znajdują się obszary, które powodują wiele niechcianych alarmów. Poruszające się obiekty w strefie wykluczenia są ignorowane. Użyj tych stref do odfiltrowywania np. kołyszących się liści na poboczu drogi lub wiązek widm powodowanych przez obiekty wykonane z materiałów odbijających fale radarowe, takie jak metalowe ogrodzenia.

Obszar współistnienia

Możesz zainstalować wiele radarów w celu pokrycia większego obszaru niż określona strefa detekcji jednego radaru. Radary wykorzystujące tę samą częstotliwość fali radiowej mogą powodować zakłócenia elektromagnetyczne pogarszające działanie innych urządzeń. Każdy model radaru Axis ma określony obszar stosowania kilku radarów. W ramach tego obszaru możesz zainstalować określoną liczę radarów, które nie będą się wzajemnie zakłócać. Aby poznać promień i zalecaną maksymalną liczbę radarów w obszarze stosowania kilku radarów, zapoznaj się z kartą katalogową urządzenia dostępną na stronie *axis.com*.

Technologia integracji funkcji radaru i obrazu

Połączenie funkcji radaru i obrazu łączy zalety radarów Axis z zaletami kamer Axis. Połączenie to zapewnia doskonałą orientację w sytuacji i ogranicza liczbę fałszywych alarmów. Po sparowaniu kamery PTZ ARTPEC-9 z radarem ARTPEC-9 poprzez interfejs internetowy kamery radar może wykrywać i klasyfikować poruszające się obiekty, kierować kamerę na obiekt i umożliwiać kamerze weryfikację przeprowadzonej klasyfikacji. Kamera może następnie kontynuować śledzenie obiektu za pomocą funkcji automatycznego śledzenia, której opis znajduje się w instrukcji obsługi kamery PTZ.

Automatyczne śledzenie ruchu

Możesz wykorzystać dane radarowe dotyczące pozycji różnych obiektów do śledzenia obiektów przez kamerę PTZ. Dostępne są trzy opcje:

- Jeżeli chcesz połączyć kilka kamer PTZ i radarów, użyj aplikacji AXIS Radar Autotracking for PTZ. Więcej informacji, p. sekcja *Sterowanie kamerą PTZ za pomocą aplikacji AXIS Radar Autotracking for PTZ, on page 25*.
- Jeżeli chcesz połączyć jeden radar i jedną kamerę ARTPEC-7 PTZ, które są zamontowane blisko siebie, użyj funkcji parowania kamer celem wykorzystania funkcji automatycznego śledzenia radaru.
- Jeżeli chcesz połączyć jeden radar i jedną kamerę ARTPEC-9 PTZ, które są zamontowane razem, użyj funkcji parowania radarów celem wykorzystania wbudowanej funkcji automatycznego śledzenia opartej na połączeniu funkcji obrazu i radaru. Opcja łączy radar i analizę obrazu wsparte sztuczną inteligencją na potrzeby minimalizacji liczby fałszywych alarmów. Informacje dotyczące konfiguracji automatycznego śledzenia z wykorzystaniem technologii połączenia funkcji radaru i obrazu znajdują się w instrukcji obsługi kamery PTZ dostępnej pod adresem *help.axis.com/axis-q6325-le*.

Sterowanie kamerą PTZ za pomocą aplikacji AXIS Radar Autotracking for PTZ

AXIS Radar Autotracking for PTZ to rozwiązanie serwerowe, które może obsługiwać różne konfiguracje podczas śledzenia obiektów:

- Sterowanie kilkoma kamerami PTZ za pomocą jednego radaru.
- Sterowanie jedną kamerą PTZ za pomocą kilku radarów.
- Sterowanie kilkoma kamerami PTZ za pomocą kilku radarów.
- Sterowanie jedną kamerą PTZ za pomocą jednego radaru po zamontowaniu ich w różnych położeniach na tym samym obserwowanym obszarze.

Aplikacja współpracuje z określonym zestawem kamer PTZ. Aby dowiedzieć się więcej, przejdź na stronę *axis.com/products/axis-radar-autotracking-for-ptz#compatible-products*.

Aby dowiedzieć się, jak skonfigurować aplikację, pobierz ją i przeczytaj jej instrukcję obsługi. Aby dowiedzieć się więcej, przejdź na stronę *axis.com/products/axis-radar-autotracking-for-ptz/support*.

Nakładki

Nakładki są nakładane na strumień wideo. Służą one do dostarczania dodatkowych informacji podczas instalacji i konfiguracji produktu lub podczas rejestracji obrazu (np. znacznik czasowy). Można dodać tekst lub obraz.

Strumieniowanie i pamięć masowa

Formaty kompresji obrazów wideo

O tym, która metoda kompresji ma być używana, należy zdecydować w zależności od wymagań dotyczących przeglądania i właściwości sieci. Dostępne są następujące opcje:

MJPEG

Motion JPEG (MJPEG), to cyfrowa sekwencja wideo składająca się z szeregu indywidualnych obrazów JPEG. Obrazy te są następnie wyświetlane i aktualizowane z szybkością odpowiednią do utworzenia strumienia

pokazującego ciągle zaktualizowany ruch. Aby odbiorca miał wrażenie oglądania obrazu wideo, szybkość musi wynosić co najmniej 16 klatek obrazu na sekundę. Obraz jest odbierany jako ruchomy obraz wideo przy 30 (NTSC) lub 25 (PAL) klatkach na sekundę.

Strumień MJPEG wykorzystuje przepustowość w dużym stopniu, ale zapewnia doskonałą jakość obrazu i dostęp do wszystkich obrazów zawartych w strumieniu.

H.264 lub MPEG-4 Part 10/AVC

Uwaga

Kompresja H. 264 to licencjonowana technologia. W produkcie Axis znajduje się jedna licencja klienta do przeglądania obrazów w kompresji H.264. Nie wolno instalować dodatkowych kopii klienta bez licencji. Aby zakupić dodatkowe licencje, skontaktuj się z dystrybutorem Axis.

Dzięki kompresji H.264 można, bez uszczerbku na jakości, zmniejszyć rozmiar cyfrowego pliku wideo o ponad 80% w porównaniu z formatem MJPEG i nawet 50% w porównaniu ze starszymi formatami MPEG. Oznacza to, że w przypadku pliku wideo wymagana jest mniejsza przepustowość i mniej zasobów pamięci masowej. Inaczej mówiąc, dla danej przepływności bitowej można uzyskać obraz o wyższej jakości.

AV1

AV1 (AOMedia Video 1) to niewymagający licencji format kodowania wideo zoptymalizowany pod kątem multimediów strumieniowych. AV1 umożliwia strumieniowe przesyłanie wysokiej jakości materiału wizyjnego nawet w środowiskach o ograniczonej przepustowości. Zmniejszając stopień zajętości pasma przez materiał wizyjny, format AV1 zachowuje jakość wideo, a jednocześnie minimalizuje zużycie danych.

AV1 obsługuje wszystkie popularne przeglądarki, komputerowe systemy operacyjne i platformy mobilne.

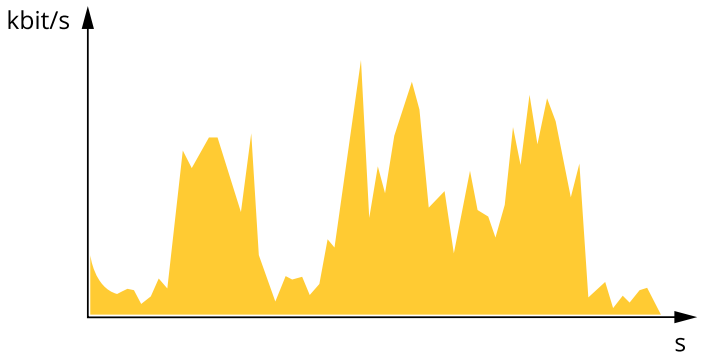
Uwaga

W porównaniu do niektórych innych kodeków AV1 wymaga większej mocy obliczeniowej na potrzeby kodowania i dekodowania.

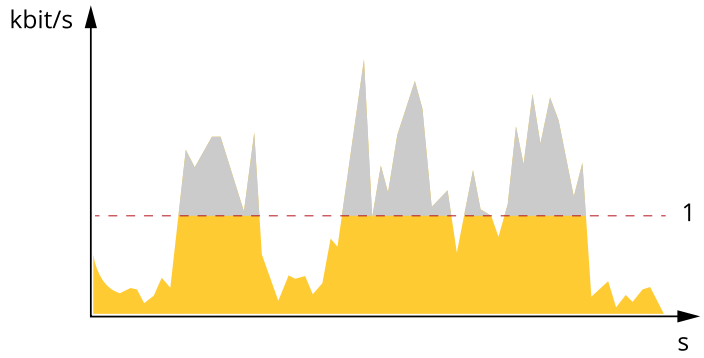
Sterowanie przepływnością bitową

Dzięki kontroli przepływności bitowej można zarządzać zajętością pasma przez strumień wideo.

Zmienna przepływność bitowa (VBR)
Przy zmiennej przepływności bitowej zajętość pasma zmienia się w zależności od natężenia aktywności w scenie. Przy większym natężeniu aktywności potrzebna jest większa przepustowość. Zmienna przepływność zapewnia stałą jakość obrazu, ale funkcja ta wymaga odpowiedniej ilości miejsca w zasobach pamięci.



Maksymalna przepływność bitowa (MBR)
Opcja ta umożliwia ustawienie docelowej przepływności bitowej w celu kontrolowania zajętości pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości obrazu lub niższa poklatkowość. Jak priorytet można wybrać opcję ustawienia jakości obrazu lub poklatkowości. Zalecamy skonfigurowanie docelowej wartości przepływności bitowej na wartość większą niż oczekiwana. Dzięki temu można zachować margines, jeśli w scenie występuje wysoki poziom aktywności.

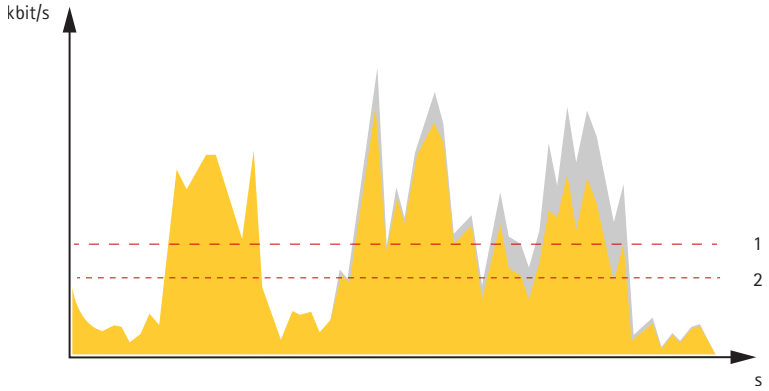


1 Docel. przepł. bitowa

Średnia przepływność bitowa (ABR)

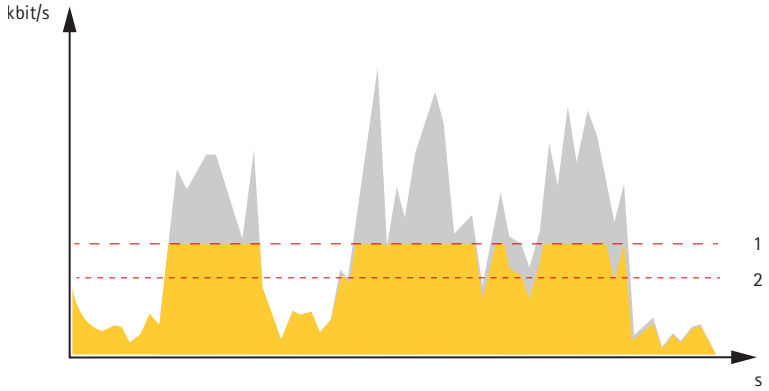
Średnia przepływność bitowa jest dostosowywana automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak najlepszą jakość obrazu wideo przy dostępnych zasobach pamięci masowej. Przepływność bitowa jest wyższa w scenach z dużą aktywnością w porównaniu ze scenami statycznymi. Korzystanie z opcji średniej przepływności zwiększa szanse uzyskania lepszej jakości obrazu w scenach o wysokim poziomie aktywności. Można zdefiniować łączną ilość pamięci masowej wymaganą do przechowywania strumienia wideo przez określony czas (czas retencji) po dostosowaniu jakości obrazu tak, by odpowiadała określonej przepływności bitowej. Określ średnią wartość przepływności bitowej w jeden z następujących sposobów:

- Aby obliczyć przybliżone zapotrzebowanie na zasoby pamięci masowej, należy ustawić wartość docelową przepływności bitowej i czas retencji.
- Użyj kalkulatora przepływności bitowej, aby obliczyć średnią przepływność bitową w zależności od dostępnego miejsca w zasobach pamięci i czasu retencji.



1 Docel. przepł. bitowa
2 Rzeczywista średnia przepływność bitowa

Można również włączyć maksymalną przepływność bitową i określić przepływność bitową w ramach średniej przepływności bitowej.



1 Docel. przepł. bitowa

2 Rzeczywista średnia przepływność bitowa

Technologia edge-to-edge

Edge-to-edge to technologia umożliwiająca bezpośrednią komunikację między urządzeniami sieciowymi. Zapewnia ona inteligentną funkcję parowania na przykład kamer Axis z produktami audio lub radarowymi Axis.

Uwaga

Sprawdź, czy sparowane urządzenia mają tę samą wersję systemu operacyjnego (oprogramowania układowego) AXIS OS.

Więcej informacji można znaleźć w białej księdze „Technologia edge-to-edge" pod adresem *whitepapers.axis.com/edge-to-edge-technology*.

Parowanie głośnika

Parowanie głośników sieciowych w technologii edge-to-edge umożliwia korzystanie z kompatybilnego głośnika sieciowego Axis tak, jakby był częścią kamery. Po sparowaniu funkcje głośnika są zintegrowane z interfejsem WWW kamery i pełni on funkcję urządzenia wyjściowego audio, w którym można odtwarzać klipy audio i przesyłać dźwięk przez kamerę.

Kamera identyfikuje się w VMS jako kamera z wyjściem audio i przekieruje odtwarzany dźwięk do głośnika.

Parowanie mikrofonu

Sparowanie mikrofonu w technologii edge-to-edge umożliwia korzystanie z kompatybilnego mikrofonu Axis tak, jakby był częścią kamery. Po sparowaniu mikrofon sieciowy zbiera dźwięki z otoczenia i udostępnia je jako urządzenie wejściowe audio, wykorzystywane w strumieniach multimediów i zapisach.

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisie produktu na stronie Axis.com.

Aby uzyskać szczegółowe informacje na temat cyberbezpieczeństwa w systemie AXIS OS, zapoznaj się z *przewodnikiem po zabezpieczeniach systemu operacyjnego AXIS OS*.

Usługa powiadomień w systemach zabezpieczeń Axis

Axis świadczy usługę powiadamiania z informacjami o lukach w zabezpieczeniach i innych sprawach dotyczących bezpieczeństwa urządzeń Axis. Aby otrzymywać powiadomienia, możesz aktywować subskrypcję na stronie *axis.com/security-notification-service*.

Postępowanie z lukami w zabezpieczeniach

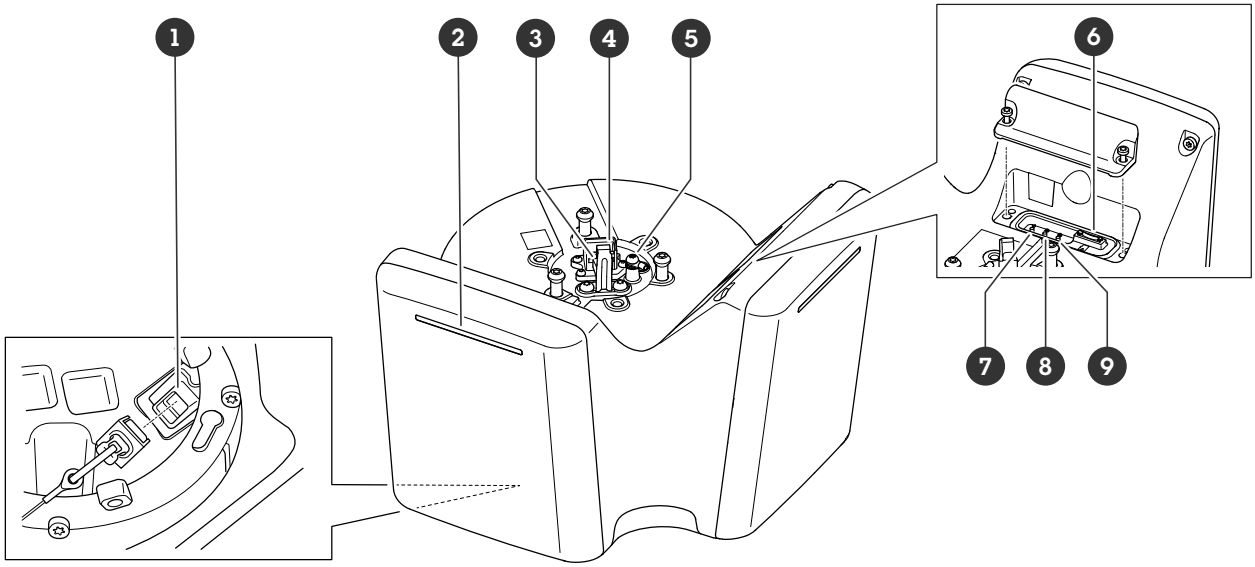
Aby maksymalnie ograniczyć narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania w takich przypadkach. Aby uzyskać więcej informacji na temat zasad zarządzania lukami w zabezpieczeniach rozwiązań Axis, sposobu zgłaszania luk w zabezpieczeniach, wykrytych luk w zabezpieczeniach i odpowiednich porad dotyczących bezpieczeństwa, zob. *axis.com/vulnerability-management*.

Bezpieczne działanie urządzeń Axis

Urządzenia Axis z domyślnymi ustawieniami fabrycznymi są wstępnie skonfigurowane z zabezpieczonymi domyślnymi mechanizmami ochrony. Zalecamy korzystanie z lepiej zabezpieczonej konfiguracji podczas instalowania urządzenia. Aby dowiedzieć się więcej o podejściu Axis do cyberbezpieczeństwa, w tym o najlepszych praktykach, zasobach i wytycznych dotyczących zabezpieczania urządzeń, odwiedź stronę *axis.com/about-axis/cybersecurity*.

Specyfikacje

Przegląd produktów



1 *Złącze sieciowe (PoE OUT)*
2 *Dynamiczna taśma LED*
3 *Haczyk na przewód bezpieczeństwa*
4 *Złącze sieciowe (PoE IN)*
5 *Śruba uziemienia*
6 *Gniazdo kart microSD*
7 *Przycisk kontrolny*
8 *Przycisk działania*
9 *Przycisk funkcyjny (nieużywany)*

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przy normalnym działaniu.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.

Dynamiczne wzory taśmy LED
Czerwony
Niebieski
Zielony
Żółty
Biały
Omiatający czerwony
Omiatający niebieski
Omiatający zielony
Miga na czerwono, niebiesko, biało

Gniazdo karty SD

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

Zalecenia dotyczące kart SD można znaleźć w witrynie *axis.com*.

Logo microSD, microSDHC i microSDXC są znakami towarowymi firmy SD-3C LLC. microSD, microSDHC, microSDXC są znakami towarowymi lub znakami towarowymi firmy SD-3C, LLC w Stanach Zjednoczonych, innych krajach lub w Stanach Zjednoczonych i innych krajach.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 32*.

Złącza

Złącze sieciowe (PoE IN)

Złącze Ethernet RJ45 z zasilaniem Power over Ethernet IEEE 802.3bt, typ 4 klasa 8.

Uwaga

Power over Ethernet IEEE 802.3bt, typ 4 klasa 8 jest wymagane dla wyjścia PoE. Jeśli drugie urządzenie nie jest zasilane, wystarczy zasilanie Power over Ethernet IEEE 802.3at typ 2 klasa 4.

Złącze sieciowe (PoE OUT)

Power over Ethernet IEEE 802.3bt, typ 3 klasa 6.

Złącze to służy do zasilania innego urządzenia PoE, np. kamery, głośnika lub drugiego radaru Axis.

Uwaga

- Zasilanie radaru za pomocą technologii Power over Ethernet IEEE 802.3bt, typ 4 klasa 8 umożliwia dołączenie drugiego urządzenia korzystającego z Power over Ethernet IEEE 802.3bt, typ 3 klasa 6.
- Zasilanie radaru za pomocą technologii Power over Ethernet IEEE 802.3bt, typ 3 klasa 6 umożliwia dołączenie drugiego urządzenia korzystającego z Power over Ethernet IEEE 802.3bt, typ 2 klasa 4.
- W przypadku zasilania radaru Power over Ethernet IEEE 802.3bt, typ 2 klasa 4 wyjście PoE jest niedostępne.

Uwaga

Maksymalna długość kabla Ethernet to łącznie 100 m w przypadku połączenia PoE OUT i PoE IN. Można ją zwiększyć za pomocą przedłużacza PoE.

Czyszczenie urządzenia

Do czyszczenia sprzętu można używać wody z mydłem niezawierającym środków ściernych.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
- Nie należy rozpylać detergentu bezpośrednio na urządzenie. Detergent należy najpierw nanieść na miękką ściereczkę, a następnie przetrzeć nią urządzenie.
- Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawanie plam na obudowie.

1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
2. W razie potrzeby można wyczyść urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą i łagodnym mydłem niezawierającym środków ściernych.
3. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

Przywracanie domyślnych ustawień fabrycznych należy stosować rozważnie. Opcja resetowania do domyślnych ustawień fabrycznych powoduje przywrócenie wszystkich domyślnych ustawień fabrycznych produktu, włącznie z adresem IP.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów, on page 29*.
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
   - **Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej:** Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
   Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej *axis.com/support*.

Fabryczne wartości parametrów można również przywrócić za pośrednictwem interfejsu WWW urządzenia. Wybierz kolejno opcje **Maintenance (Konserwacja)** > **Factory default (Ustawienia fabryczne)** > **Default (Domyślne)**.

Upewnianie się co do braku zmian w oprogramowaniu urządzenia

Aby upewnić się, że w urządzeniu zainstalowano oryginalny system AXIS OS lub aby odzyskać kontrolę nad urządzeniem w razie ataku:

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne, on page 32*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Opcje systemu AXIS OS

Axis oferuje zarządzanie oprogramowaniem urządzenia w formie zarządzania aktywnego lub długoterminowego wsparcia (LTS). Zarządzanie aktywne oznacza stały dostęp do najnowszych funkcji produktu, a opcja LTS to stała platforma z okresowymi wydaniami wersji zawierającymi głównie poprawki i aktualizacje dotyczące bezpieczeństwa.

Aby uzyskać dostęp do najnowszych funkcji lub w razie korzystania z kompleksowych systemów Axis, należy użyć systemu AXIS OS w opcji aktywnego zarządzania. Opcja LTS zalecana jest w przypadku integracji z urządzeniami innych producentów, które nie są na bieżąco weryfikowane z najnowszymi aktywnymi wersjami. Urządzenie dzięki LTS może utrzymywać odpowiedni stopień cyberbezpieczeństwa bez konieczności wprowadzania zmian w funkcjonowaniu ani ingerowania w istniejący system. Szczegółowe informacje dotyczące strategii oprogramowania urządzenia Axis znajdują się na stronie *axis.com/support/device-software*.

Sprawdzanie bieżącej wersji systemu AXIS OS

System AXIS OS określa funkcjonalność naszych urządzeń. W przypadku pojawienia się problemów zalecamy rozpoczęcie ich rozwiązywania od sprawdzenia bieżącej wersji systemu AXIS OS. Najnowsza wersja może zawierać poprawki, które rozwiążą problem.

Aby sprawdzić bieżącą wersję systemu AXIS OS:

1. Przejdź do interfejsu WWW urządzenia i wybierz opcję **Status**.
2. W menu **Device info (Informacje o urządzeniu)** sprawdź wersję systemu AXIS OS.

Aktualizacja systemu AXIS OS:

Ważne

- Po aktualizacji oprogramowania urządzenia poczynione ustawienia zostaną zachowane. Axis Communications AB nie gwarantuje, że ustawienia te zostaną zachowane, nawet gdy funkcje są dostępne w nowej wersji systemu operacyjnego AXIS OS.
- Począwszy od systemu operacyjnego AXIS OS w wersji 12.6, pomiędzy aktualną a docelową wersją urządzenia należy zainstalować każdą wersję LTS. Przykładowo, jeżeli aktualnie zainstalowana wersja oprogramowania urządzenia to AXIS OS 11.2, przed aktualizacją urządzenia do wersji AXIS OS 12.6 należy zainstalować wersję LTS AXIS OS 11.11. Więcej informacji znajduje się w *Portalu AXIS OS: ścieżka aktualizacji*.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.
- Aby instalacja się powiodła, upewnij się, że podczas aktualizacji osłona jest zamocowana.

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony *axis.com/support/device-software*, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.

1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie *axis.com/support/device-software*.
2. Zaloguj się do urządzenia jako administrator.
3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS)** > **Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

Problemy techniczne i możliwe rozwiązania

Problemy z uaktualnianiem systemu AXIS OS

Niepowodzenie uaktualniania systemu AXIS OS

Jeśli aktualizacja zakończy się niepowodzeniem, urządzenie załaduje ponownie poprzednią wersję. Najczęstszą przyczyną tego jest wczytanie niewłaściwego systemu AXIS OS. Upewnij się, że nazwa pliku systemu AXIS OS odpowiada danemu urządzeniu i spróbuj ponownie.

Problemy po aktualizacji systemu AXIS OS

Jeśli wystąpią problemy po aktualizacji, przejdź do strony **Konserwacja** i przywróć poprzednio zainstalowaną wersję.

Problemy z ustawieniem adresu IP

Nie można ustawić adresu IP

- Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsieci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
- Adres IP może być używany przez inne urządzenie. Aby to sprawdzić:
  1. Odłącz urządzenie Axis od sieci.
  2. W oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia.
  3. Jeśli otrzymasz: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie.
  4. Jeśli otrzymasz: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
- Może występować potencjalny konflikt adresu IP z innym urządzeniem w tej samej podsieci. Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Problemy z dostępem do urządzenia

Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki

Gdy protokół HTTPS jest włączony, upewnij się, że podczas próby zalogowania się używasz prawidłowego protokołu (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki.

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje: *Przywróć domyślne ustawienia fabryczne, on page 32*.

Serwer DHCP zmienił adres IP

Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę).

W razie potrzeby możesz ręcznie przydzielić statyczny adres IP. Instrukcje można znaleźć na stronie *axis.com/support*.

Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X

Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w urządzeniu Axis muszą być zsynchronizowane z serwerem NTP. Wybierz kolejno opcje **System > Date and time (System > Data i godzina)**.

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, patrz *Obsługiwane przeglądarki, on page 14*.

Nie można uzyskać dostępu do urządzenia z zewnątrz

Aby uzyskać dostęp do urządzenia z zewnątrz, zalecamy skorzystanie z jednej z następujących aplikacji dla systemu Windows®:

- AXIS Camera Station Edge: darmowa aplikacja idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station Pro: 90-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

Instrukcje i plik do pobrania znajdują się na stronie *axis.com/vms*.

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

Zapora sieciowa blokuje ruch korzystający z portu 8883, ponieważ jest on uważany za niebezpieczny.

Czasami serwer/broker może nie zapewniać konkretnego portu dla komunikacji MQTT. W takiej sytuacji może być dostępne korzystanie z MQTT przez port zwykle używany do obsługi ruchu HTTP/HTTPS.

- Jeśli serwer/broker obsługuje protokół WebSocket/WebSocket Secure (WS/WSS), typowo w porcie 443, użyj tego protokołu. Skontaktuj się z dostawcą serwera/brokera, aby dowiedzieć się, czy protokół WS/WSS jest obsługiwany oraz którego portu i ścieżki podstawowej należy używać.
- Jeśli serwer/broker obsługuje ALPN, korzystanie z MQTT może być negocjowane na otwartym porcie, na przykład porcie 443. Skontaktuj się z dostawcą serwera/brokera, aby sprawdzić, czy jest obsługiwany ALPN oraz jakiego protokołu ALPN i portu należy użyć.

Problemy z obsługą urządzenia

Przedni grzejnik i wycieraczka nie działają

Jeżeli nie włącza się przedni grzejnik lub wycieraczka, sprawdź, czy górna pokrywa jest prawidłowo zamocowana do dolnej części obudowy.

Jeśli nie możesz znaleźć tego, czego szukasz, przejdź na stronę poświęconą rozwiązywaniu problemów: *axis.com/support*.

Wystąpiły problemy z obrazem

Pogorszenie jakości lub utrata obrazu

- Sprawdź w raporcie z serwera urządzeń, ile razy utracono połączenie z modułem przetwornika.
- Sprawdź, czy kabel połączeniowy między modułem czujnika i jednostką główną jest solidnie zamocowany.
- Wymień kabel modułu czujnika na nowy.

Problemy z samoczynnym wyłączaniem się urządzenia

Urządzenie wyłącza się

- Odłącz zasilanie od urządzenia, a następnie podłącz je ponownie.
- Sprawdź, czy jest włączona opcja **Opóźnione wyłączenie**. Jeżeli tak, to jednostka główna będzie się wyłączać według ustawionego czasu opóźnienia. Masz 300 sekund na wyłączenie funkcji **Opóźnione wyłączenie**, zanim urządzenie ponownie samoczynnie się wyłączy.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wymaganą przepustowość (przepływność).

Najważniejsze czynniki, które należy uwzględnić:

- Zdjęcie lub założenie osłony spowoduje ponowne uruchomienie kamery.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.

Kontakt z pomocą techniczną

Aby uzyskać pomoc, przejdź na stronę *axis.com/support*.

T10223326_pl

2026-02 (M2.2)