

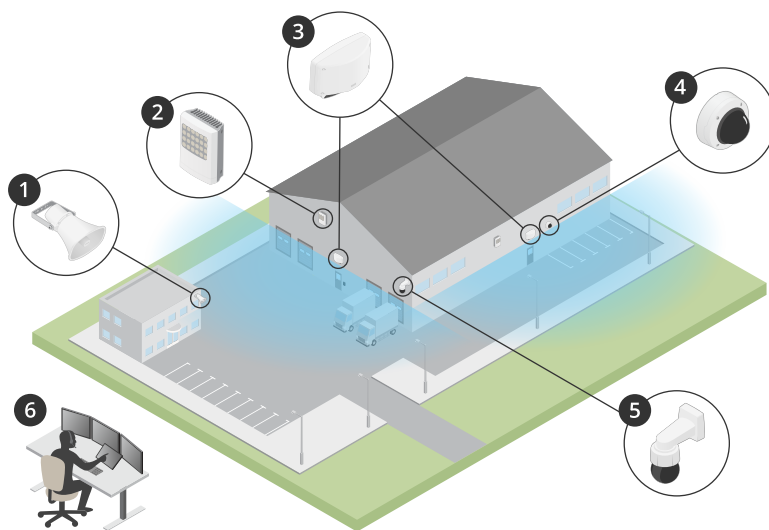
AXIS D2110-VE Security Radar

Spis treści

Informacje o rozwiązaniu.....	4
Profile radaru.....	4
Gdzie montować produkt	4
Pokrywany obszar.....	5
Profil dozoru strefy.....	6
Instalacja wielu radarów	6
Instalacja od 2 do 3 radarów w jednej strefie.....	6
Instalacja od 4 do 6 radarów w jednej strefie.....	6
Przykłady instalacji w strefie	7
Zasięg detekcji w strefie.....	9
Przypadki zastosowań do dozoru stref.....	11
Profil dozoru drogi.....	12
Przykłady instalacji przy drodze	12
Zasięg detekcji na drodze	12
Przypadki zastosowania w dozowaniu drogi	12
Od czego zacząć	15
Wyszukiwanie urządzenia w sieci.....	15
Obsługiwane przeglądarki.....	15
Otwórz interfejs WWW urządzenia.....	15
Utwórz konto administratora.....	15
Bezpieczne hasła.....	16
Omówienie interfejsu WWW	16
Konfiguracja urządzenia	17
Ustawianie poziomu montażu.....	17
Kalibruj mapę referencyjną.....	17
Ustawianie stref detekcji.....	18
Dodawanie scenariuszy	18
Dodawanie stref wykluczenia.....	19
Minimalizowanie fałszywych alarmów.....	20
Przeglądanie i rejestracja obrazów wideo.....	20
Zmniejszanie zapotrzebowania na przepustowość i zasób	21
Konfiguracja zasobów sieciowej pamięci masowej.....	21
Rejestracja i odtwarzanie obrazu.....	21
Sterowanie kamerą PTZ za pomocą radaru	21
Sterowanie kamerą PTZ za pomocą wbudowanej usługi automatycznego śledzenia w radarze	22
Sterowanie kamerą PTZ za pomocą aplikacji AXIS Radar Autotracking for PTZ.....	23
Konfiguracja reguł dotyczących zdarzeń	23
Wyzwalanie akcji.....	23
Wyzwalanie powiadomienia po otwarciu obudowy.....	23
Rejestrowanie obrazu wideo z kamery po wykryciu ruchu	24
Włączanie światła po wykryciu ruchu	25
Wysyłanie wiadomości e-mail, gdy radar zostanie przykryty metalowym przedmiotem.....	25
Interfejs WWW.....	26
Sprawdzanie poprawności instalacji.....	27
Sprawdzanie poprawności instalacji radaru	27
Sprawdzanie poprawności działania radaru	27
Zakończenie sprawdzania poprawności.....	28
Więcej informacji.....	30
Strumieniowanie i pamięć masowa	30
Formaty kompresji obrazów wideo.....	30
Sterowanie przepływnością bitową.....	30
Specyfikacje	33
Przegląd produktów.....	33

.....	33
Wskaźniki LED.....	33
.....	34
Gniazdo karty SD.....	34
Przyciski.....	34
Przycisk kontrolny.....	34
Złącza.....	34
Złącze sieciowe	34
Złącze sieciowe (PoE OUT)	34
Złącze I/O	35
Złącze zasilania	36
Złącze przekaźnikowe.....	36
Czyszczenie urządzenia	37
Rozwiązywanie problemów –	38
Przywróć domyślne ustawienia fabryczne	38
Sprawdzanie bieżącej wersji systemu AXIS OS	38
Aktualizacja systemu AXIS OS:.....	38
Problemy techniczne i możliwe rozwiązania.....	39
Kwestie wydajności	40
Cyberbezpieczeństwo	41
Postępowanie z lukami w zabezpieczeniach	41
Powiadomienia dotyczące zabezpieczeń	41
Bezpieczny cykl eksploatacji produktu	41

Informacje o rozwiązaniu



- 1 Głośnik tubowy C1310-E
- 2 Kontroler drzwi
- 3 D2110-VE Security Radar
- 4 Stałopozycyjna kamera kopułkowa
- 5 Kamera PTZ
- 6 Centrum monitoringu

Profile radaru

Uwaga

Do korzystania z profili radaru konieczne jest oprogramowanie sprzętowe w wersji 10.11 lub nowszej. Najnowszą wersję oprogramowania sprzętowego można pobrać na [www.axis.com](#).

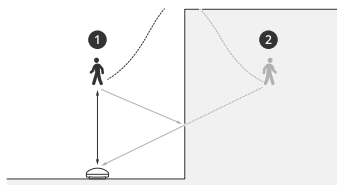
W instrukcji obsługi znajdują się porady dotyczące dostosowywania konfiguracji do indywidualnych potrzeb. AXIS D2110-VE Security Radar ma dwa profile:

- **Profil dozoru strefy**, który służy do śledzenia małych i dużych obiektów poruszających się z prędkością poniżej 55 km/h
- **Profil dozoru drogi**, który służy do śledzenia pojazdów poruszających się z prędkością do 105 km/h

Jeśli przy informacjach podanych w tej instrukcji obsługi nie ma adnotacji, że dotyczą one **Profilu dozoru strefy** lub **Profilu dozoru drogi** oznacza to, że mają one zastosowanie do obu profili.

Gdzie montować produkt

- Radar jest przeznaczony do dozoru otwartych obszarów. Każdy obiekt (taki jak ściana, ogrodzenie, drzewo lub duży krzew) w obszarze objętym zasięgiem powoduje utworzenie dodatkowego martwego punktu (cienia).
- Radar należy zamontować na stabilnym słupie lub w takim miejscu na ścianie, w którego pobliżu nie ma innych obiektów ani instalacji. Na wydajność radaru mogą wpływać obiekty, które odbijają fale radiowe, znajdujące się w odległości 1 m po jego lewej i prawej stronie.
- Obiekty metalowe w polu widzenia powodują odbicia wpływające na skuteczność funkcji klasyfikacji obiektów radaru.



- 1 Rzeczywista detekcja
- 2 Detekcja z odbicia (fałszywe ślady)

Aby uzyskać więcej informacji na temat sposobów postępowania w przypadku obiektów o dużym współczynniku odbicia, zob. *Dodawanie stref wykluczenia, on page 19*.

- Aby zainstalować więcej niż dwa radary w tej samej strefie, zobacz *Instalacja wielu radarów, on page 6*.

Pokrywany obszar

Model AXIS D2110-VE zapewnia pokrycie poziome 180°. Zakres detekcji odpowiada powierzchni 5600 m² (61 000 ft²) w przypadku ludzi i 11 300 m² (122 000 ft²) w przypadku pojazdów.

Uwaga

Aby uzyskać optymalny obszar detekcji, należy zamontować radar na wysokości 3,5–4 m. Wysokość montażowa ma wpływ na martwe pole pod radarem.

Profil dozoru strefy

Area monitoring profile (Profil dozoru strefy) najlepiej sprawdza się w przypadku śledzenia obiektów poruszających się z prędkością do 55 km/h (34 mph). Profil ten umożliwia kategoryzowanie wykrywanych obiektów jako ludzi, pojazdy lub obiekty nieznane. Można ustawić regułę wyzwalającą akcję po wykryciu któregoś z tych obiektów. Aby śledzić pojazdy poruszające się z większą prędkością użyj: *Profil dozoru drogi*, on page 12.

Instalacja wielu radarów

Poprzez instalację kilku radarów można zapewnić dozór takich obszarów, jak otoczenie budynku lub strefa buforowa za ogrodzeniem.

Jednoczesna obecność

Jeżeli w tej samej strefie zostaną zainstalowane więcej niż dwa radary, ich fale radiowe mogą powodować zakłócenia i wpływać na wydajność. Promień strefy współwystępowania wynosi 350 m (380 jardów).



Uwaga

Na wydajność radarów w strefie współwystępowania mogą także wpływać czynniki środowiskowe oraz skierowanie radaru w stronę ogrodzeń, budynków lub pobliskich radarów.

Instalacja od 2 do 3 radarów w jednej strefie

Umieszczając 2–3 radary w tej samej strefie, określ liczbę sąsiadujących radarów w interfejsie urządzenia. Pomoże to zwiększyć wydajność radarów i zapobiec występowaniu zakłóceń.

1. Otwórz menu Radar > Settings > Coexistence (Radar > Ustawienia > Jednoczesna obecność).
2. Wybierz liczbę sąsiadujących radarów.

Przykłady instalacji z zastosowaniem kilku radarów można zobaczyć tutaj: *Przykłady instalacji w strefie*, on page 7.

Instalacja od 4 do 6 radarów w jednej strefie

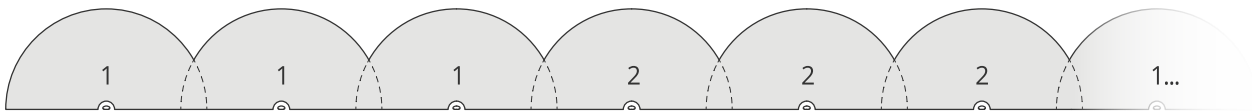
Uwaga

Zainstalowanie maksymalnie sześciu radarów w jednej strefie wymaga oprogramowania sprzętowego w wersji 11.3 lub nowszej.

Po zainstalowaniu 4–6 radarów w tej samej strefie najpierw skonfiguruj liczbę sąsiadujących radarów, a następnie dodaj je wszystkie do grupy. Zaczynij od radaru znajdującego się najdalej, np. najdalej po lewej stronie. Grupuj radary po trzy i przypisz do grupy radary znajdujące się najbliżej siebie.

Radary w grupie będą się synchronizować w celu zapewnienia najwyższej możliwej wydajności i zapobiegania występowaniu zakłóceń między nimi.

1. Otwórz menu Radar > Settings > Coexistence (Radar > Ustawienia > Jednoczesna obecność).
2. Ustaw liczbę sąsiadujących radarów jako 3–5.
3. Wybierz grupę dla radaru.



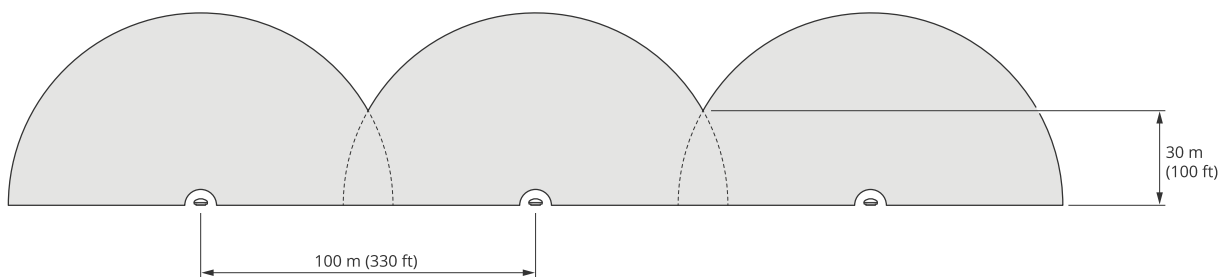
Oto przykład grupowania sąsiadujących radarów w tej samej strefie.

Więcej przykładów instalacji z wykorzystaniem kilku radarów można znaleźć tutaj: *Przykłady instalacji w strefie*, on page 7.

Przykłady instalacji w strefie

Tworzenie wirtualnego ogrodzenia z kilkoma radarami

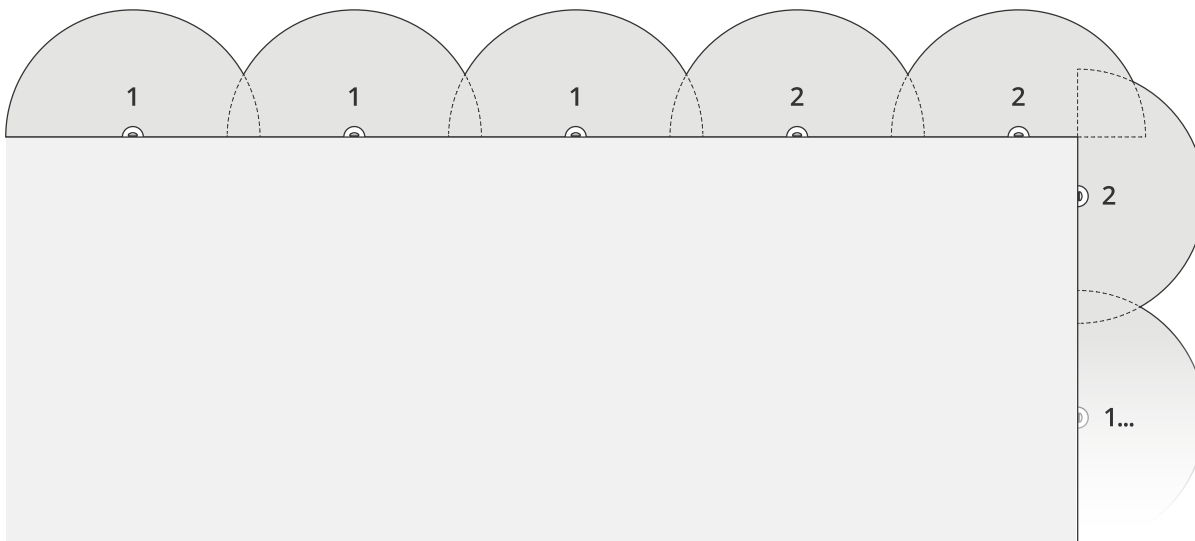
Aby utworzyć wirtualne ogrodzenie, np. wokół budynku, można umieścić wiele radarów obok siebie. Zalecamy umieszczenie ich w odstępach co 100 m (330 ft).



Aby zapobiec występowaniu zakłóceń w przypadku montowania więcej niż dwóch radarów w tej samej strefie, skonfiguruj w interfejsie urządzenia liczbę sąsiadujących radarów. Natomiast w przypadku zastosowania więcej niż trzech radarów dodaj je do grupy.



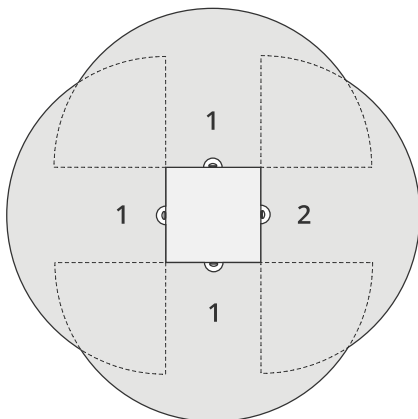
Jak pokazano w tym przykładzie, wirtualne ogrodzenie można też skonfigurować tak, aby obejmowało narożniki.



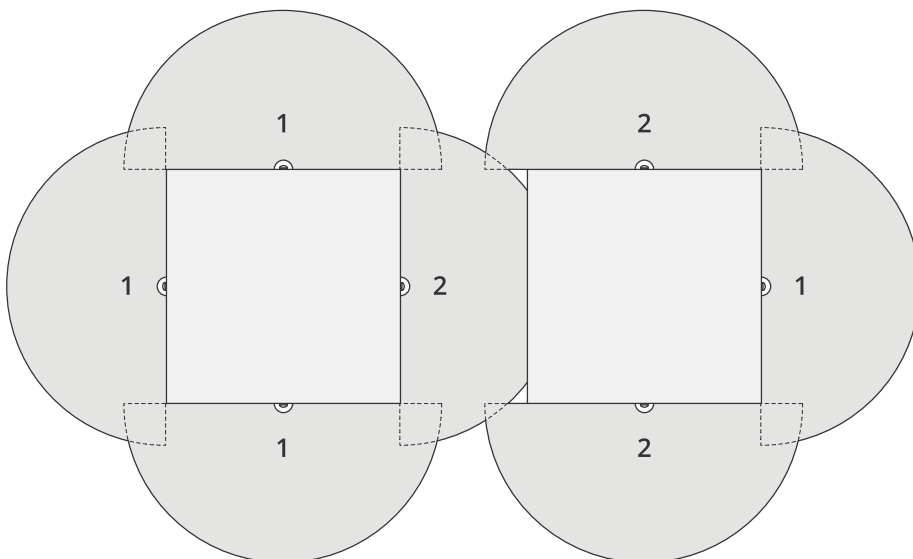
Zobacz *Instalacja wielu radarów*, on page 6, aby uzyskać więcej informacji na temat sąsiadujących radarów i ich grup.

Pokrycie obszaru wokół budynku

Aby pokryć obszar wokół budynku, umieść radary na ścianach budynku, tak aby były skierowane na zewnątrz. W przypadku umieszczenia w jednej strefie więcej niż trzech radarów skonfiguruj w interfejsie urządzenia liczbę sąsiadujących radarów i dodaj je do grupy, jak pokazano w tym przykładzie.



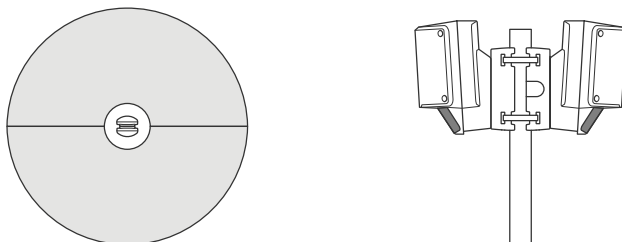
Istnieje także możliwość pokrycia obszaru wokół kilku budynków.



Zobacz *Instalacja wielu radarów*, on page 6, aby uzyskać więcej informacji na temat sąsiadujących radarów i ich grup.

Pokrycie otwartego obszaru

Aby pokryć duży otwarty obszar, użyj dwóch uchwytych do montażu na słupie, aby zamontować dwa radary tyłem do siebie.

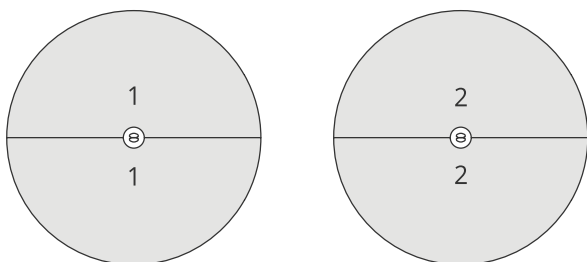


Można użyć wyjścia PoE z jednego radaru do zasilania drugiego radaru, ale trzeciego radaru już nie można podłączyć w ten sposób.

Uwaga

Wyjście PoE radaru jest włączone, gdy radar jest zasilany zasilaczem midspan o mocy 60 W.

W razie konieczności zastosowania w jednej strefie kilku instalacji tyłem do siebie skonfiguruj liczbę sąsiadujących ze sobą radarów w interfejsie urządzenia i dodaj radary do grupy, aby zapobiec występowaniu zakłóceń. To jeden z przykładów grupowania radarów ustawionych tyłem do siebie.



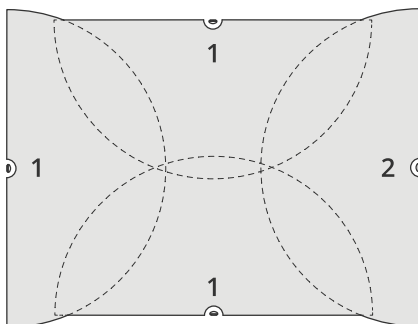
Zobacz *Instalacja wielu radarów*, on page 6, aby uzyskać więcej informacji na temat sąsiadujących radarów i ich grup.

Instalacja radarów ustawionych naprzeciwko siebie

Co do zasady nie jest zalecane instalowanie więcej niż trzech radarów naprzeciwko siebie, ponieważ zwiększa to ryzyko występowania zakłóceń w ich pracy. Niemniej, w przypadku niektórych obszarów może być konieczne zastosowanie takiego ustawienia. Na przykład w przypadku konieczności pokrycia boiska piłkarskiego nie można zainstalować radarów na środku murawy.

Jeśli zdecydujesz się na zainstalowanie więcej niż trzech radarów naprzeciwko siebie, zachowaj między nimi odległość 40 m (130 ft). Bardzo ważne jest dodanie wszystkich sąsiadujących radarów do grupy i zapisanie ich liczby w interfejsie urządzenia. Dzięki temu można poprawić wydajność ich pracy.

Oto przykład grupowania czterech radarów obejmujących określony teren.



Zobacz *Instalacja wielu radarów*, on page 6, aby uzyskać więcej informacji na temat sąsiadujących radarów i ich grup.

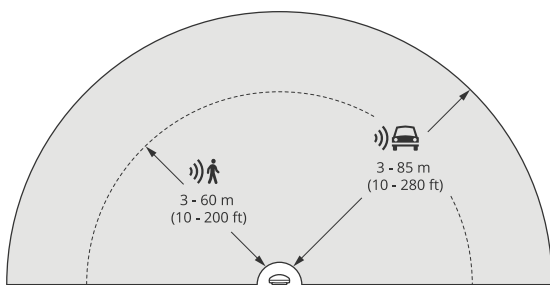
Zasięg detekcji w strefie

Zasięg detekcji jest maksymalną odległością, z jakiej jest możliwe śledzenie obiektu i wyzwalanie alarmu. Mierzy się ją od limitu bliskiej detekcji (na ile blisko urządzenia jest możliwa detekcja) do limitu dalekiej detekcji (na ile daleko od urządzenia jest możliwa detekcja).

Profil monitorowania strefy jest zoptymalizowany pod kątem wykrywania ludzi. Istnieje jednak możliwość wykrywania pojazdów oraz innych obiektów poruszających się z prędkością do 55 km/h (z dokładnością prędkości +/- 2 km/h).

W warunkach montażu na optymalnej wysokości instalacyjnej zasięgi detekcji są następujące:

- 3–60 m podczas detekcji ludzi
- 3–85 m podczas detekcji pojazdów



Uwaga

- Jeżeli chcesz zamontować radar na innej wysokości, podczas jego kalibracji wprowadź rzeczywistą wysokość montażu na stronach internetowych produktu.
- Scena ma wpływ na zakres detekcji.
- Zasięg detekcji zależy od sąsiednich radarów.
- Zakres detekcji zależy od typu obiektu.

Zakres detekcji był mierzony w tych warunkach:

- Zasięg jest mierzony wzdłuż podłoża.
- Obiektem była osoba o wzroście 170 cm.
- Osoba ta przechodziła bezpośrednio przed radarem.
- Wartości zostały zmierzone w momencie, kiedy osoba weszła do strefy detekcji.
- Czułość radaru została ustawiona jako **Medium (Średnia)**.

Wysokość montażowa	Pochylenie 0°	Pochylenie 10°	Pochylenie 20°
2,5 m (8,2 ft)	3,0–60 m (9,8–197 ft)	Niezalecane	Niezalecane
3,5 m (11 ft)	3,0–60 m (9,8–197 ft)	Niezalecane	Niezalecane
4,5 m (15 ft)	4,0–60 m (13–197 ft)	Niezalecane	Niezalecane
5,5 m (18 ft)	7,5–60 m (25–197 ft)	Niezalecane	Niezalecane
6,5 m (21 ft)	7,5–60 m (25–197 ft)	5,5–60 m (18–197 ft)	Niezalecane
8 m (26 ft)	Niezalecane	9–60 m (30–197 ft)	7,5–30 m (25–98 ft)
10 m (33 ft)	Niezalecane	15–60 m (49–197 ft)	9–35 m (30–115 ft)
12 m (39 ft)	Niezalecane	23–60 m (75–197 ft)	13–38 m (43–125 ft)
14 m (36 ft)	Niezalecane	27–60 m (89–197 ft)	17–35 m (56–115 ft)
16 m (52 ft)	Niezalecane	Niezalecane	25–50 m (82–164 ft)

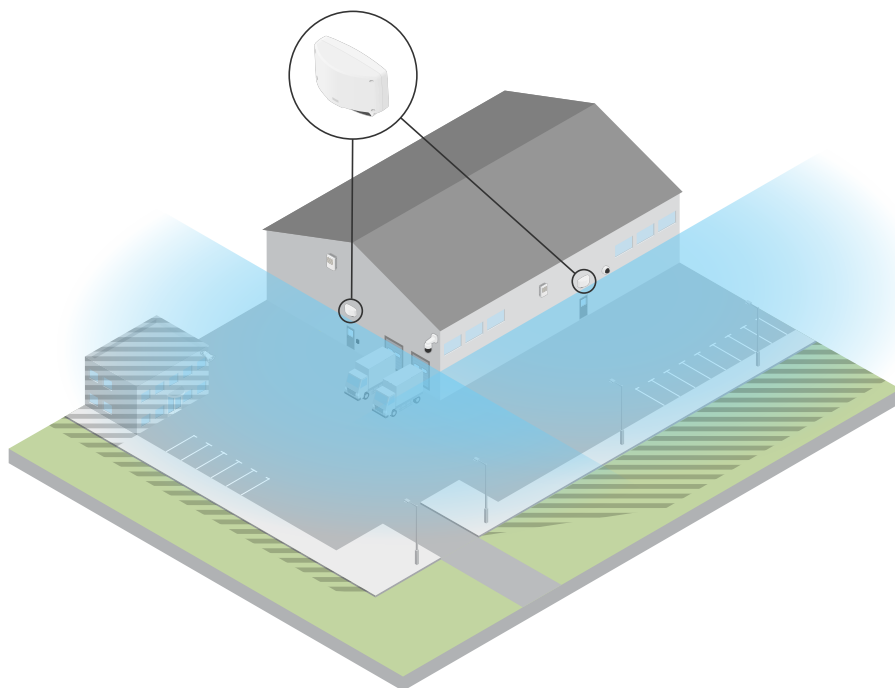
Przypadki zastosowań do dozoru stref

Pokrycie obszaru basenu

Dochodziło do licznych włamań na basen poza godzinami otwarcia. Ze względu na wymagania związane z zachowaniem prywatności właściciel nie mógł zamontować systemu dozoru wideo. Dlatego zdecydował się na zamocowanie radaru i ustawienie **Area monitoring profile (Profilu dozoru strefy)**. Radar jest zamontowany na budynku; pokrywa cały basen i większość obszaru wokół niego. W przypadku wykrycia obecności człowieka poza godzinami otwarcia (między 20:00 a 06:00) radar wyzwala ostrzeżenie nadawane przez głośnik.

Pokrycie obszaru wokół budynku

Zakład produkujący środki chemiczne dodał do swojego systemu kolejną warstwę zabezpieczeń poprzez zastosowanie radarów do pokrycia stref wokół szczególnie wrażliwych budynków. W systemie dozoru są już kamery standardowe, termowizyjne i kontrolery drzwi. Radary mogą wyzwalać zdarzenia, które uruchamiają funkcje śledzenia intruza przez kamery, przybliżanie i nagrywanie jego działań. Następuje uruchomienie sygnałów świetlnych połączonych z sieciowymi kamerami termowizyjnymi, co informuje intruza o tym, że znalazł się w strefie chronionej. A kontrolery drzwi mogą zablokować dostęp. Radary umożliwiają systemowi ochrony reagowanie na długo, zanim intruz dotrze do wrażliwego budynku.



Pokrycie dużej otwartej strefy

Na parkingu przed małym centrum handlowym odnotowano wzrost liczby włamań do samochodów po godzinach pracy. Centrum jest monitorowane przez pracownika ochrony, ale zarząd uznał, że konieczne jest zwiększenie bezpieczeństwa w nocy bez dodatkowych kosztów związanych z zatrudnianiem kolejnych pracowników. Zdecydowano się na zainstalowanie dwóch radarów w **Area monitoring profile (Profilu dozoru strefy)** zamontowanych tyłem do siebie, tak aby pokrywały cały obszar parkingu. Zostały skonfigurowane w taki sposób, aby ostrzegały dyżurnego pracownika ochrony o podejrzanym zachowaniu, dzięki czemu może on zbadać miejsce zdarzenia. Do tego systemu można było dodać megafony, aby odtwarzały nagranie alarmowe odstrasżające złodziei, gdy radary wykryją obecność ludzi w strefie.

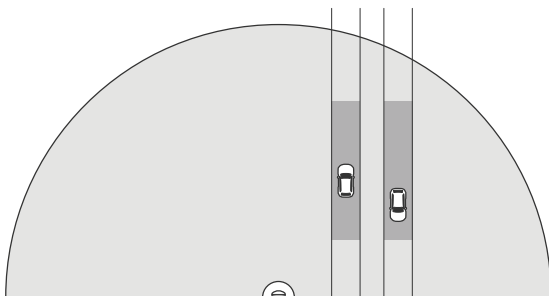
Profil dozoru drogi

Road monitoring profile (Profil dozoru drogi) najlepiej sprawdza się w przypadku monitorowania pojazdów, które poruszają się z prędkością do 105 km/h w mieście, na obszarach zamkniętych i drogach podmiejskich. Tryb ten nie służy do wykrywania ludzi ani innych typów obiektów. W celu monitorowania obiektów innych niż pojazdy, należy używać radaru w *Profil dozoru strefy*, on page 6.

Przykłady instalacji przy drodze

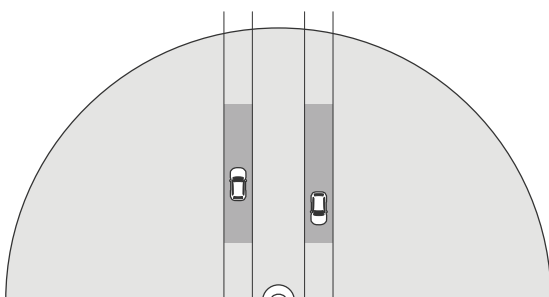
Montaż na poboczu

Aby monitorować pojazdy poruszające się po drodze, można zamontować radar na poboczu. Radar pokryje odległość 10 m po przekątnej.



Montaż na środku

Ta opcja montażu wymaga stabilnego położenia. Radar można zamontować na słupie na środku drogi lub na bramownicy nad drogą. Radar będzie wtedy pokrywał obszar 10 m po bokach z obu stron. Radar obejmie większy obszar z boku, jeśli zostanie zainstalowany w centralnym położeniu.



Uwaga

Zalecana wysokość montażowa dla tego radaru wynosi od 3–8 m w przypadku Profilu dozoru drogi.

Zasięg detekcji na drodze

Zasięg detekcji jest maksymalną odległością, z jakiej jest możliwe śledzenie obiektu i wyzwalanie alarmu. Mierzy się ją od limitu bliskiej detekcji (na ile blisko urządzenia jest możliwa detekcja) do limitu dalekiej detekcji (na ile daleko od urządzenia jest możliwa detekcja).

Ten profil jest zoptymalizowany pod kątem wykrywania pojazdów i zapewnia dokładność pomiaru prędkości rzędu ± 2 km/h podczas monitorowania pojazdów poruszających się z prędkością do 105 km/h.

Zasięg detekcji po zamontowaniu radaru na optymalnej wysokości:

- 25–70 m w przypadku pojazdów poruszających się z prędkością 60 km/h.
- 30–60 m w przypadku pojazdów poruszających się z prędkością 105 km/h.

Przypadki zastosowania w dozoru drogi

Regulowanie ruchu pojazdów w strefach obowiązywania niskiej prędkości

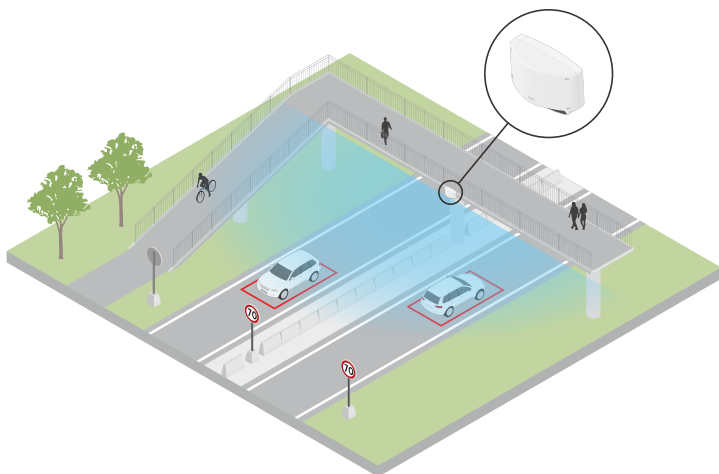
W kompleksie przemysłowym z długą drogą między dwoma magazynami zainstalowano radar, który pomaga egzekwować ograniczenie prędkości do 60 km/h. W **Profilu dozorowania drogi** radar wykrywa przekroczenie prędkości przez pojazd znajdujący się w jego strefie detekcji. Następnie wyzwala zdarzenie wysyłające powiadomienia e-mail do kierowców i kierowników. Przypomnienie pomaga w przestrzeganiu ograniczeń prędkości.

Niepożądane pojazdy na zamkniętej drodze

Niewielka droga prowadząca do starego kamieniołomu została zamknięta, jednak doniesienia o poruszających się po niej pojazdach spowodowały, że władze zainstalowały na niej radar w **Profilu dozorowania drogi**. Radar jest zamontowany wzdłuż drogi i obejmuje całą jej szerokość. Za każdym razem, gdy pojazd wjeżdża do scenariusza, zostaje uruchomiony migający sygnalizator, który informuje kierowców o konieczności opuszczenia drogi. Jest też wysyłana wiadomość do zespołu ochrony, dzięki czemu w razie potrzeby możliwe jest wysłanie patrolu.

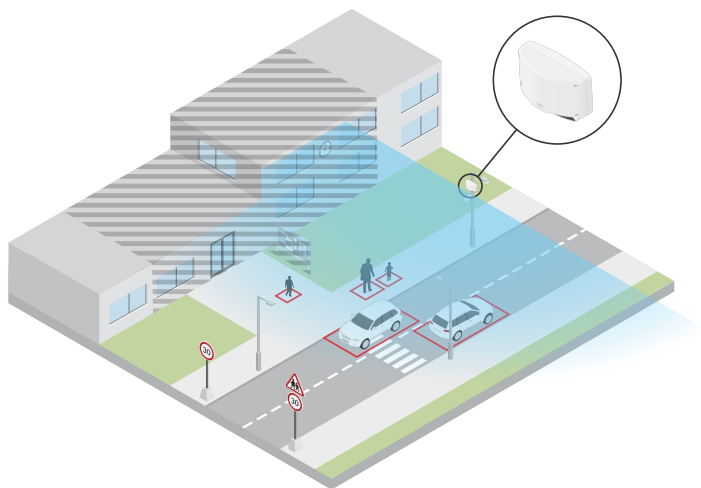
Informacje prędkości pojazdów poruszających się po drodze

Na drodze przebiegającej przez małe miasto odnotowano kilka przypadki przekroczenia prędkości. W celu egzekwowania ograniczenia prędkości do 70 km, kontrolerzy ruchu drogowego zdecydowali się na instalację radaru w **Profilu dozorowania drogi**, na wiadukcie przebiegającym nad drogą. Umożliwia to wykrywanie prędkości, z jaką poruszają się pojazdy, i monitorowanie, kiedy na drodze powinny znajdować się jednostki, które kontrolują ruch.



Bezpieczeństwo ludzi i pojazdów

Pracownicy szkoły zidentyfikowali dwa problemy związane z bezpieczeństwem, które postanowili wyeliminować. Zauważyli, że w ciągu dnia na terenie szkoły pojawiają się niepożądani goście, a kierowcy przejeżdżający obok szkoły nie stosują się do ograniczenia prędkości 20 km/h. Radar jest zamontowany na słupie obok chodnika. Wybrano ustawienie *Profil dozorowania strefy*, on page 6, ponieważ dzięki temu radar może śledzić ludzi i pojazdy poruszające się z prędkością mniejszą niż 55 km/h. Dzięki temu pracownicy szkoły mogą śledzić osoby wchodzące i wychodzące w godzinach pracy szkoły, a także uruchamiać megafon ostrzegający pieszych, gdy przejeżdżający pojazd porusza się ze zbyt dużą prędkością.



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 15.

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 16.
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 38.

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.

Omówienie interfejsu WWW

Ten film przybliży najważniejsze elementy i schemat działania interfejsu WWW urządzenia.



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

Interfejs WWW urządzenia Axis

Konfiguracja urządzenia

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. Jeżeli podłoże jest nierówne, wykonaj pomiar, licząc od średniej wysokości podłoża, a nie od pojedynczego punktu.

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

Kalibruj mapę referencyjną

Aby łatwiej można było zobaczyć, gdzie poruszają się wykryte obiekty, można przesłać mapę w celach informacyjnych. Można użyć planu terenu lub zdjęcia lotniczego przedstawiającego obszar objęty radarem. Skalibruj mapę tak, aby obszar pokrycia radaru pasował do pozycji, kierunku i skali mapy, a następnie zbliż mapę, jeśli 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 będzie kalibrować 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 zoom nie powoduje zmiany pokrywanego obszaru radaru. Nawet jeśli po zoomowaniu część pokrywanego obszaru znajdzie się poza widoczną strefą, radar nadal będzie wykrywał poruszające się obiekty w całym pokrywanym obszarze. Jedynym sposobem na wykluczenie wykrywanego ruchu jest dodanie stref wykluczenia. Więcej informacji znajduje się w rozdziale *Dodawanie stref wykluczenia, on page 19*.

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).



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

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

Ustawianie stref detekcji

Aby określić miejsce detekcji ruchu, można dodać jedną lub więcej stref detekcji. Używaj różnych stref do wyzwalania różnych akcji.

Istnieją dwa rodzaje stref:

- **Scenario (Scenariusz)** (nazywany wcześniej strefą detekcji) to obszar, w którym poruszające się obiekty wyzwalają reguły. Scenariusz domyślny obejmuje cały obszar znajdujący się w zasięgu radaru.
- **Exclude zone (Strefa wykluczenia)** to obszar, w którym poruszające się obiekty są ignorowane. Użyj stref wykluczenia, jeśli w scenariuszu znajdują się miejsca, w których wyzwalane są częste niechciane alarmy.

Dodawanie scenariuszy

Scenariusz to połączenie warunków wyzwalania i ustawień wykrywania, które można wykorzystać do tworzenia reguł w systemie zdarzeń. Aby utworzyć różne reguły dla różnych części sceny, należy dodać scenariusze.

Aby dodać scenariusz:

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 w obszarze lub przekraczające jedną albo dwie linie.

Aby wyzwalać zdarzenia przez ruchome obiekty w obszarze:

1. Wybierz **Movement in area (Ruch w obszarze)**.
2. Kliknij **Next (Dalej)**.
3. Wybierz typ strefy, którą chcesz uwzględnić w scenariuszu.
Użyj myszki, aby zmienić kształt i położenie strefy, tak aby obejmowała tylko pożądaną część obrazu radaru lub mapy referencyjnej.
4. Kliknij **Next (Dalej)**.
5. Dodaj ustawienia detekcji.
1. W obszarze **Ignore short-lived objects (Ignorowanie obiektów krótkotrwałych)** dodaj sekundy, które muszą następnie upłynąć do wyzwolenia.
2. Wybierz typ wyzwalającego obiektu w obszarze **Trigger on object type (Typ wyzwalającego obiektu)**.
3. Dodaj zakres ograniczenia prędkości w obszarze **Speed limit (Ograniczenie prędkości)**.
6. Kliknij **Next (Dalej)**.
7. Ustaw minimalny czas trwania alarmu w obszarze **Minimum trigger duration (Minimalny czas alarmu)**.
8. Kliknij przycisk **Zapisz**.

Wyzwalanie przez obiekty przekraczające linię:

1. Wybierz **Line crossing (Przekroczenie linii)**.
2. Kliknij **Next (Dalej)**.

3. Umieść linię w scenie.
Za pomocą myszy przesun linię i nadaj jej pożądany kształt.
4. Aby zmienić kierunek detekcji, włącz opcję **Change direction (Zmień kierunek)**.
5. Kliknij **Next (Dalej)**.
6. Dodaj ustawienia detekcji.
 - 6.1. W obszarze **Ignore short-lived objects (Ignorowanie obiektów krótkotrwałych)** dodaj sekundy, które muszą następnie upłynąć do wyzwolenia.
 - 6.2. Wybierz typ wyzwalającego obiektu w obszarze **Trigger on object type (Typ wyzwalającego obiektu)**.
 - 6.3. Dodaj zakres ograniczenia prędkości w obszarze **Speed limit (Ograniczenie prędkości)**.
7. Kliknij **Next (Dalej)**.
8. Ustaw minimalny czas trwania alarmu w obszarze **Minimum trigger duration (Minimalny czas alarmu)**. Wartość domyślna jest ustawiona na 2 sekundy. Jeśli scenariusz ma być wyzwalany za każdym razem, gdy obiekt przekroczy linię, zmniejsz czas trwania do 0 sekund.
9. Kliknij przycisk **Zapisz**.

Wyzwalanie przez obiekty przekraczające dwie linie:

1. Wybierz **Line crossing (Przekroczenie linii)**.
2. Kliknij **Next (Dalej)**.
3. Aby ustawić wyzwalanie alarmu po przekroczeniu przez obiekt dwóch linii, włącz opcję **Require crossing of two lines (Wymagaj przekroczenia dwóch linii)**.
4. Umieść linie w scenie.
Za pomocą myszy przesun linię i nadaj jej pożądany kształt.
5. Aby zmienić kierunek detekcji, włącz opcję **Change direction (Zmień kierunek)**.
6. Kliknij **Next (Dalej)**.
7. Dodaj ustawienia detekcji.
 - 7.1. W obszarze **Max time between crossings (Maksymalny czas między przejściami)** ustaw limit czasu między przekroczeniem pierwszej i drugiej linii.
 - 7.2. Wybierz typ wyzwalającego obiektu w obszarze **Trigger on object type (Typ wyzwalającego obiektu)**.
 - 7.3. Dodaj zakres ograniczenia prędkości w obszarze **Speed limit (Ograniczenie prędkości)**.
8. Kliknij **Next (Dalej)**.
9. Ustaw minimalny czas trwania alarmu w obszarze **Minimum trigger duration (Minimalny czas alarmu)**. Wartość domyślna jest ustawiona na 2 sekundy. Jeśli scenariusz ma być wyzwalany za każdym razem, gdy obiekt przekroczył dwie linie, zmniejsz czas trwania do 0 sekund.
10. Kliknij przycisk **Zapisz**.

Dodawanie stref wykluczenia

Strefy wykluczenia to obszary, w których poruszające się obiekty są ignorowane. Dodaj strefy wykluczenia, aby ignorować na przykład kołyszące się liście na poboczu drogi. Możesz także dodać strefy wykluczenia, aby ignorować fałszywe ślady powodowane odbłaskowe elementy, takie jak metalowe ogrodzenie.

Dodawanie strefy wykluczenia:

1. Przejdź do menu **Radar > Exclude zones (Radar > Strefy wykluczenia)**.
2. Kliknij **Add exclude zone (Dodaj strefę wykluczenia)**.
Użyj myszki, aby zmienić kształt i położenie strefy, tak aby obejmowała tylko potrzebną część widoku radaru lub mapy referencyjnej.

Minimalizowanie fałszywych alarmów

Jeżeli zauważysz nadmiar fałszywych alarmów, możesz odfiltrować niektóre rodzaje ruchu lub obiekty, zmienić zasięg albo dostosować czułość detekcji. Zobacz, które ustawienia najlepiej sprawdzą się w danych warunkach.

- Wyreguluj czułość detekcji radaru:
Przejdź do **Radar > Settings > Detection (Radar > Ustawienia > Detekcja)** i zmniejsz opcję **Detection sensitivity (Czułość detekcji)**. Zmniejsza to ryzyko fałszywych alarmów, ale może również sprawić, że radar przeoczy jakiś ruch.
Ustawienie czułości dotyczy wszystkich stref.
 - **Niski:** Tej wartości czułości należy użyć w przypadku wielu metalowych obiektów lub dużych pojazdów na obszarze. Śledzenie i klasyfikowanie obiektów przez radar potrwa dłużej. Może to zmniejszyć zakres detekcji, zwłaszcza w przypadku szybko poruszających się obiektów.
 - **Medium (Średni):** Jest to domyślne ustawienie.
 - **Wysoka:** Tej wartości czułości należy użyć w przypadku otwartej przestrzeni bez metalowych obiektów znajdujących się przed radarem. Zwiększy to zakres detekcji dla ludzi.
- Modyfikowanie scenariuszy i wyłączanie stref:
Jeżeli scenariusz obejmuje twarde powierzchnie, takie jak metalowa ściana, mogą w niej pojawiać się odbicia, które powodują wiele detekcji jednego obiektu. Możesz zmienić kształt scenariusza lub dodać strefę wykluczenia, w której będą ignorowane niektóre części scenariusza. Więcej informacji: *Dodawanie scenariuszy, on page 18* i *Dodawanie stref wykluczenia, on page 19*.
- Wyzwalanie w przypadku obiektów przekraczających dwie linie zamiast jednej:
Jeżeli scenariusz przekroczenia linii obejmuje kołyszące się obiekty lub poruszające się zwierzęta, może się tak zdarzyć, że obiekt przekroczy linię i wywoła fałszywy alarm. W takim przypadku scenariusz można dostosować w taki sposób, żeby alarm był wyzwalany tylko wtedy, gdy obiekt przekroczy dwie linie. Więcej informacji znajduje się w rozdziale *Dodawanie scenariuszy, on page 18*.
- Filtrowanie przy ruchu:
 - Przejdź do **Radar > Settings > Detection (Radar > Ustawienia > Detekcja)** i wybierz opcję **Ignore swaying objects (Ignoruj kołyszące się obiekty)**. To ustawienie zmniejsza liczbę fałszywych alarmów wywołanych ruchem drzew, krzewów i masztów w strefie obserwacji.
 - Przejdź do menu **Radar > Settings > Detection (Radar > Ustawienia > Detekcja)** i wybierz opcję **Ignore small objects (Ignoruj małe obiekty)**. To ustawienie jest dostępne w profilu monitorowania obszaru i minimalizuje liczbę fałszywych alarmów powodowanych przez małe obiekty w strefie detekcji, takie jak koty i króliki.
- Filtrowanie według czasu:
 - Wybierz kolejno opcje **Radar > Scenarios (Radar > Scenariusze)**.
 - Zaznacz scenariusz i kliknij  , aby zmodyfikować jego ustawienia.
 - Wybierz wyższą wartość w ustawieniu **Seconds until trigger (Sekundy do wyzwolenia)**. Jest to wartość czasu, przez jaką radar śledzi obiekt przed wyzwoleniem alarmu. Odliczanie rozpoczyna się od pierwszego wykrycia obiektu przez radar, a nie pojawienia się obiektu w określonej strefie w scenariuszu.
- Filtrowanie według typu obiektów:
 - Wybierz kolejno opcje **Radar > Scenarios (Radar > Scenariusze)**.
 - Zaznacz scenariusz i kliknij  , aby zmodyfikować jego ustawienia.
 - Jeśli nie chcesz wyzwalać alarmu po wykryciu konkretnych typów obiektów, wybierz typy obiektów, które nie mają wyzwalać zdarzeń w scenariuszu.

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 30*.

Zmniejszanie zapotrzebowania na przepustowość i zasób

Ważne

Zmniejszenie przepustowości może skutkować utratą wyrazistości szczegółów na obrazie.

1. Wybierz kolejno opcje **Radar > Stream (Radar > Strumień)**.
2. W podglądzie na żywo kliknij  .
3. W ustawieniu **Video format (Format wideo)** wybierz wartość **H.264**.
4. Przejdź do okna **Radar > Stream > General (Radar > Strumień > Ogólne)** i zwiększ wartość w polu **Compression (Kompresja)**.

Uwaga

Większość przeglądarek internetowych nie obsługuje kodowania H.265, dlatego urządzenie nie obsługuje go w swoim interfejsie WWW. Zamiast tego można użyć systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

Konfiguracja zasobów sieciowej pamięci masowej

Aby przechowywać zapisy w sieci, należy skonfigurować zasoby sieciowej pamięci masowej.

1. Przejdź do **System > Storage (Pamięć masowa)**.
2. Kliknij opcję  **Add network storage (Dodaj sieciową pamięć masową)** w obszarze **Network storage (Sieciowa pamięć masowa)**.
3. Wpisz adres IP serwera hosta.
4. W ustawieniu **Network share (Udział sieciowy)** podaj nazwę współdzielonego udziału na serwerze hosta.
5. Wprowadź nazwę użytkownika i hasło.
6. Wybierz wersję protokołu SMB lub pozostaw wartość **Auto (Automatycznie)**.
7. Jeżeli występują tymczasowe problemy z połączeniem lub udział nie został jeszcze skonfigurowany, zaznacz opcję **Add share without testing (Dodaj udział bez testowania)**.
8. Kliknij **Dodaj**.

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. *Konfiguracja zasobów sieciowej pamięci masowej, on page 21*

3. Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

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

Sterowanie kamerą PTZ za pomocą radaru

Można użyć informacji o położeniu obiektów z radaru, aby przesyłać do kamery PTZ polecenie śledzenia obiektu. Można to zrobić na dwa sposoby:

- Sterowanie kamerą PTZ za pomocą wbudowanej usługi automatycznego śledzenia w radarze, on page 22. Wbudowanej opcji można użyć w przypadku jednej kamery PTZ i jednego radaru zamontowanych bardzo blisko siebie.
- Sterowanie kamerą PTZ za pomocą aplikacji *AXIS Radar Autotracking for PTZ*, on page 23. Aplikacja Windows jest odpowiednia w przypadku używania kilku kamer PTZ i radarów do śledzenia obiektów.

Uwaga

Używanie serwera NTP do synchronizowania czasu między kamerami, radarami i komputerem z systemem Windows. W razie braku synchronizacji zegarów może dojść do opóźnień w śledzeniu albo śledzenia fałszywych śladów.

Sterowanie kamerą PTZ za pomocą wbudowanej usługi automatycznego śledzenia w radarze

Wbudowane automatyczne śledzenie radaru to kompleksowe rozwiązanie, w którym radar może bezpośrednio sterować kamerą PTZ. Obsługuje wszystkie kamery PTZ firmy Axis.

Uwaga

Jeden radar można połączyć z jedną kamerą PTZ za pomocą wbudowanej usługi automatycznego śledzenia radarowego. W konfiguracjach z większą liczbą kamer PTZ lub radarów zalecamy używanie narzędzia *AXIS Radar Autotracking for PTZ*. Aby uzyskać dodatkowe informacje, zob. *Sterowanie kamerą PTZ za pomocą aplikacji AXIS Radar Autotracking for PTZ*, on page 23.

W tej instrukcji znajdują się informacje na temat parowania kamery PTZ z radarem, kalibrowania tych urządzeń i konfigurowania funkcji śledzenia obiektów.

Zanim zaczniesz:

- Zdefiniuj obszar zainteresowania, a następnie skonfiguruj w radarze strefy wykluczenia, aby uniknąć niechcianych alarmów. Zadbaj o wykluczenie stref zawierających materiały odbijające promieniowanie radarowe lub kołyszące się obiekty, takie jak liście, aby kamera PTZ nie śledziła nieistotnych obiektów. Instrukcje: *Dodawanie stref wykluczenia*, on page 19.

Parowanie radaru z kamerą PTZ:

1. Przejdź do menu **System > Edge-to-edge > PTZ pairing** (**System > Edge-to-edge > Parowanie PTZ**).
2. Wpisz adres IP, nazwę użytkownika oraz hasło do kamery PTZ.
3. Kliknij przycisk **Połącz**.
4. Kliknij polecenie **Configure Radar autotracking** (Skonfiguruj automatyczne śledzenie radarowe) lub otwórz menu **Radar > Radar PTZ autotracking** (**Radar > Automatyczne śledzenie PTZ**), aby skonfigurować automatyczne śledzenie radarowe.

Kalibracja radaru i kamery PTZ:

5. Przejdź do menu **Radar > Radar PTZ autotracking** (**Radar > Automatyczne śledzenie PTZ**).
6. Aby ustawić wysokość montażu kamery, otwórz menu **Camera mounting height** (**Wysokość montażu kamery**).
7. Aby obrócić kamerę PTZ w taki sposób, by skierować ją w tym samym kierunku, w którym został ustawiony radar, przejdź do menu **Pan alignment** (**Wyrównanie obrotu**).
8. Aby dostosować pochylenie w celu skompensowania nachylenia terenu, otwórz menu **Ground incline offset** (**Przesunięcie nachylenia terenu**) i podaj wartość przesunięcia w stopniach.

Konfiguracja śledzenia kamery PTZ:

9. Przejdź do menu **Track (Śledzenie)**, aby wybrać śledzenie ludzi, pojazdów i/lub nieznanych obiektów.
10. Aby rozpocząć śledzenie obiektów kamerą PTZ, włącz funkcję **Tracking (Śledzenie)**. Umożliwia to automatyczne przybliżenie obiektu lub grupy obiektów tak, aby znalazły się w polu widzenia kamery.
11. Włącz opcję **Object switching** (**Przełączanie obiektów**) jeśli spodziewasz się w scenie wielu obiektów, które nie mieszczą się w widoku kamery. Przy tym ustawieniu radar nadaje priorytet śledzonym obiektom.

12. Aby określić, przez ile sekund każdy obiekt ma być śledzony, ustaw **Object hold time (Czas śledzenia obiektu)**.
13. Aby kamera PTZ wracała do pozycji domowej, gdy radar przestaje śledzić obiekty, włącz opcję **Return to home (Wróć do pozycji domowej)**.
14. Aby określić czas, przez jaki kamera PTZ pozostaje w ostatniej znanej pozycji śledzonego obiektu przed powrotem do pozycji domowej, ustaw **Return to home timeout (Limit czasu powrotu do pozycji domowej)**.
15. Aby precyzyjnie ustawić zoom kamery PTZ, użyj suwaka.

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.

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.

Wyzwalanie powiadomienia po otwarciu obudowy

W tym przykładzie wyjaśniono, jak ustawić powiadomienie e-mail wyzwalane w przypadku otwarcia obudowy urządzenia.

Dodaj odbiorcę wiadomości e-mail:

1. Przejdź do **System (System) > Events (Zdarzenia) > Recipients (Odbiorcy)** i kliknij **Add recipient (Dodaj odbiorcę)**.
2. Wprowadź nazwę odbiorcy.
3. Jako typ powiadomienia wybierz **Email (E-mail)**.
4. Wpisz adres e-mail odbiorcy.

5. Wpisz adres e-mail, z którego kamera ma wysyłać powiadomienia.
6. Podaj dane logowania do konta e-mail wysyłającego powiadomienia wraz z nazwą hosta SMTP i numerem portu.
7. Aby przetestować ustawienia poczty e-mail, kliknij **Test**.
8. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

9. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i kliknij **Add a rule (Dodaj regułę)**.
10. Wprowadź nazwę reguły.
11. Z listy warunków wybierz opcję **Casing open (Otwarcie obudowy)**.
12. Z listy akcji wybierz opcję **Send notification to email (Wyślij powiadomienie przez email)**.
13. Wybierz odbiorcę z listy.
14. Wpisz temat i treść wiadomości e-mail.
15. Kliknij przycisk **Zapisz**.

Rejestrowanie obrazu wideo z kamery po wykryciu ruchu

W tym przykładzie wyjaśniono sposób konfigurowania radaru i kamery, tak aby kamera rozpoczynała rejestrację na karcie SD pięć sekund przed wykryciem ruchu przez radar i kończyła ją minutę po wykryciu ruchu.

Połącz urządzenia ze sobą:

1. Podłącz przewód z wyjścia I/O radaru do wejścia I/O kamery.

Skonfiguruj port I/O radaru:

2. Przejdź do menu **System > Akcesoria > I/O ports (Ustawienia > System > Porty WE/WY)**, skonfiguruj port WE/WY jako wyjście i wybierz stan normalny.

Utwórz regułę w radarze:

3. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
4. Wpisz nazwę reguły, na przykład **Rejestruj wideo po wykryciu ruchu**.
5. Z listy warunków wybierz scenariusz w obszarze **Radar motion (Ruch radaru)**.
6. Z listy akcji wybierz opcję **Toggle I/O while the rule is active (Przełącz I/O, gdy reguła jest aktywna)**, a następnie wybierz port podłączony do kamery.
7. Kliknij przycisk **Zapisz**.

Skonfiguruj port I/O kamery:

8. Przejdź do menu **System > Akcesoria > I/O ports (Ustawienia > System > Porty WE/WY)**, skonfiguruj port WE/WY jako wejście i wybierz stan normalny.

Utwórz regułę w kamerze:

9. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
10. Wprowadź nazwę reguły.
11. Z listy warunków wybierz **Digital input is active (Wejście cyfrowe jest aktywne)**, a następnie wybierz port, który ma wyzwać regułę.
12. Z listy akcji wybierz opcję **Record video (Zarejestruj wideo)**.
13. Z listy opcji pamięci masowej wybierz opcję **SD card (Karta SD)**.
14. Wybierz istniejący profil strumienia lub utwórz nowy.
15. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
16. Ustaw bufor po zdarzeniu na 1 minutę.
17. Kliknij przycisk **Zapisz**.

Włączanie światła po wykryciu ruchu

Włączenie światła po wejściu intruza w obszar detekcji może zapobiegać przestępstwom, a także poprawić jakość obrazu w przypadku kamery optycznej, która rejestruje wtargnięcie.

W tym przykładzie wyjaśniono sposób konfigurowania radaru i oświetlenia, tak aby oświetlacz włączył się po wykryciu ruchu przez radar, a następnie wyłączył po minucie.

Podłącz urządzenia:

1. Podłącz przewód oświetlacza do zasilania za pośrednictwem portu przekaźnika radaru. Podłącz drugi przewód bezpośrednio od zasilacza do oświetlacza.

Skonfiguruj port przekaźnika radaru:

2. Wybierz kolejno opcje **System > Accessories > I/O ports (System > Akcesoria > Porty I/O)** i jako normalny stan portu przekaźnika ustaw wartość **Open circuit (Obwód otwarty)**.

Utwórz regułę w radarze:

3. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
4. Wprowadź nazwę reguły.
5. Z listy warunków wybierz scenariusz w obszarze **Radar motion (Ruch radaru)**. Aby skonfigurować scenariusz, przejdź do sekcji *Dodawanie scenariuszy, on page 18*.
6. Z listy działań wybierz opcję **Toggle I/O once (Przełącz raz I/O)**, a następnie wybierz port przekaźnika.
7. Wybierz opcję **Active (Aktywna)**.
8. Ustaw czas trwania w opcji **Duration (Czas trwania)**.
9. Kliknij przycisk **Zapisz**.

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

W tym przykładzie wyjaśniamy, jak utworzyć regułę, która wysła 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*.

Sprawdzanie poprawności instalacji

Sprawdzanie poprawności instalacji radaru

Uwaga

Wykonując ten test, można sprawdzić poprawność instalacji w obecnych warunkach. Wydajność instalacji może zależeć od zmian w scenie.

Radar jest gotowy do pracy od razu po zainstalowaniu, ale zalecamy, aby przed przystąpieniem do jego użytkowania sprawdzić, czy działa on prawidłowo. Może to zwiększyć dokładność radaru, pomagając w identyfikacji wszelkich problemów z instalacją lub zarządzaniu obiektami (takimi jak drzewa i powierzchnie odbijające światło) w scenie.

Przed przystąpieniem do sprawdzenia poprawności działania konieczne jest .

Sprawdzenie poprawności działania radaru warto wykonywać za każdym razem, gdy:

- W scenie znajdują się obiekty, które należy wykluczyć, aby strefy mogły zawierać określone obiekty, takie jak roślinność lub powierzchnie metalowe.
- Radar zostanie sparowany z kamerą PTZ i chcesz skonfigurować funkcję **Radar autotracking** (Automatyczne śledzenie radaru).
- Nastąpi zmiana wysokości montażowej radaru.

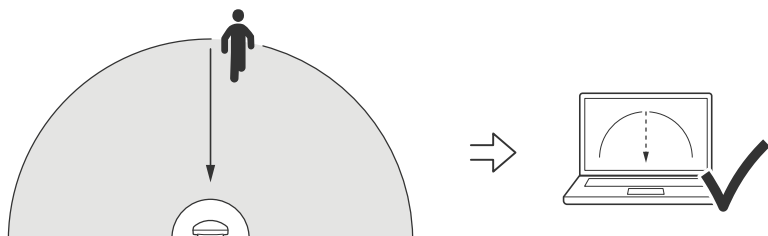
Sprawdzanie poprawności działania radaru

Sprawdź, czy nie ma fałszywych detekcji

1. Sprawdź, czy strefa detekcji jest wolna od działalności ludzi.
2. Odczekaj kilka minut, upewniając się, że radar nie wykrywa żadnych statycznych obiektów w granicach strefy detekcji.
3. Jeśli radar nie wykryje żadnych niepożądanych zjawisk, pomini krok 4.
4. W przypadku niepożądanych detekcji dowiedz się, jak odfiltrować określone typy ruchu lub obiektów, zmienić pokrycie lub ustawić czułość detekcji. W tym celu zapoznaj się z informacjami podanymi w części *Minimalizowanie fałszywych alarmów*, on page 20.

Sprawdź, czy symbol i kierunek przemieszczania są prawidłowe przy zbliżaniu się do radaru od przodu

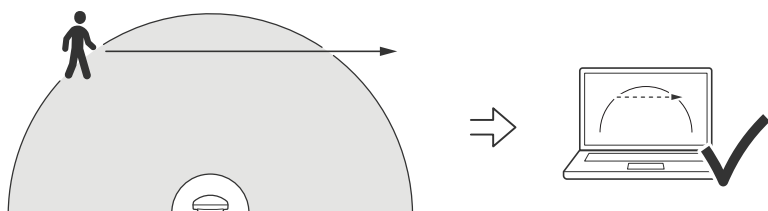
1. Przejdź do interfejsu WWW radaru i nagraj sesję. Pomoc na ten temat można znaleźć w temacie *Rejestracja i odtwarzanie obrazu*, on page 21.
2. Stań w odległości 60 m naprzeciwko radaru i idź bezpośrednio w jego kierunku.
3. Obejrzyj sesję w interfejsie WWW radaru. Jeśli radar Cię wykryje, powinien być widoczny symbol klasyfikacji ludzi.
4. Sprawdź, czy w interfejsie WWW radaru jest widoczny prawidłowy kierunek ruchu.



Sprawdź, czy symbol i kierunek przemieszczania są prawidłowe przy zbliżaniu się do radaru z boku

1. Przejdź do interfejsu WWW radaru i nagraj sesję. Pomoc na ten temat można znaleźć w temacie *Rejestracja i odtwarzanie obrazu*, on page 21.
2. Stań w odległości 60 m od radaru, a następnie idź bezpośrednio przez obszar pokrycia radaru.
3. Sprawdź, czy w interfejsie WWW radaru zostanie wyświetlony symbol klasyfikacji ludzi.

4. Sprawdź, czy w interfejsie WWW radaru jest widoczny prawidłowy kierunek ruchu.



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		
2a. Sprawdź, czy do wykrytego obiektu jest przypisany odpowiedni symbol człowieka, gdy idziesz w kierunku radaru z naprzeciwka		
2b. Sprawdź, czy kierunek ruchu jest prawidłowy, gdy idąc z naprzeciwka zbliżasz się do radaru		
3a. Sprawdź, czy do wykrytego obiektu jest przypisany odpowiedni symbol człowieka, gdy idziesz w kierunku radaru z boku		
3b. Sprawdź, czy kierunek ruchu jest prawidłowy, gdy idąc z boku zbliżasz się do radaru		

Zakończenie sprawdzania poprawności

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

1. Upewnij się, że radar został skonfigurowany według przedstawionych instrukcji.
2. Aby przeprowadzić bardziej szczegółowe sprawdzanie poprawności, dodaj i skalibruj mapę referencyjną.
3. Ustaw w radarze scenariusz inicjowany po wykryciu odpowiedniego obiektu. Domyślnie **liczba sekund do wyzwolenia** jest określony jako 2 s, ale w razie potrzeby można go zmienić to ustawienie w interfejsie WWW.
4. Ustaw w radarze rejestrowanie danych po wykryciu odpowiedniego obiektu. Instrukcje znajdują się w temacie *Rejestracja i odtwarzanie obrazu, on page 21*.
5. Ustaw **trwanie śladu** na 1 godz., tak aby w bezpieczny sposób przekraczał on czas potrzebny na opuszczenie miejsca, obejście obszaru dozoru i powrót na swoje miejsce. Wybrany czas **trwania śladu** spowoduje kontynuowanie śledzenia w podglądzie na żywo radaru przez ustawiony czas, a po zakończeniu sprawdzania poprawności można go wyłączyć.
6. Przejdź wzdłuż granicy strefy zasięgu radaru i upewnij się, że trasa w systemie pokrywa się z trasą przebytą przez Ciebie.

7. Jeżeli wyniki sprawdzania poprawności nie spełnią Twoich oczekiwań, skalibruj od nowa mapę referencyjną i powtórz procedurę sprawdzania poprawności.

Więcej informacji

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.

H.265 lub MPEG-H Part 2/HEVC

Dzięki kompresji H.265 można, bez uszczerbku na jakości, zmniejszyć rozmiar cyfrowego pliku wideo o ponad 25% w porównaniu z kompresją H.264.

Uwaga

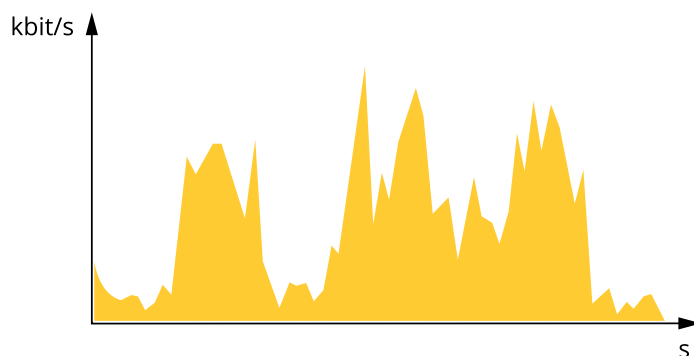
- Kompresja H.265 to licencjonowana technologia. W produkcie Axis znajduje się jedna licencja klienta do przeglądania obrazów w kompresji H.265. Nie wolno instalować dodatkowych kopii klienta bez licencji. Aby zakupić dodatkowe licencje, skontaktuj się z dystrybutorem Axis.
- Większość przeglądarek internetowych nie obsługuje dekodowania H.265 i dlatego kamera nie ma dla niego opcji w swoim interfejsie internetowym. Zamiast tego można użyć systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

Sterowanie przepływnością bitową

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

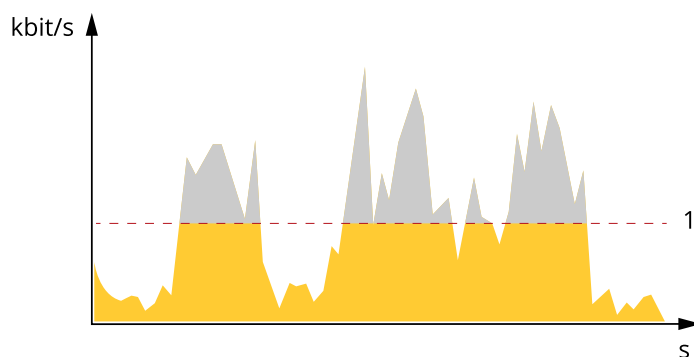
Zmienna przepływność bitowa (VBR)

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.

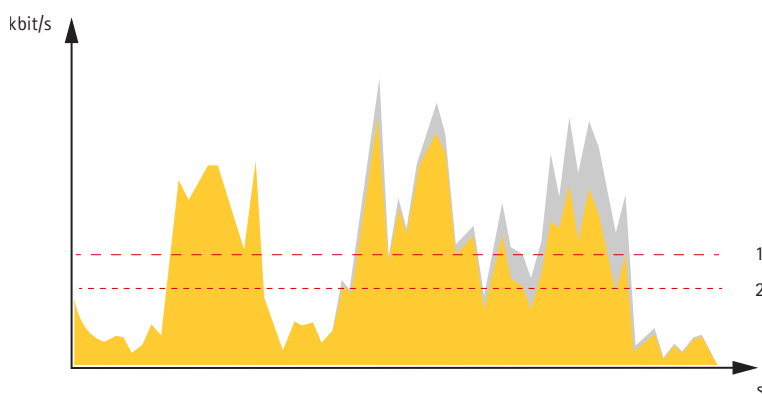


1 Docel. przepł. bitowa

Średnia przepływność bitowa (ABR)

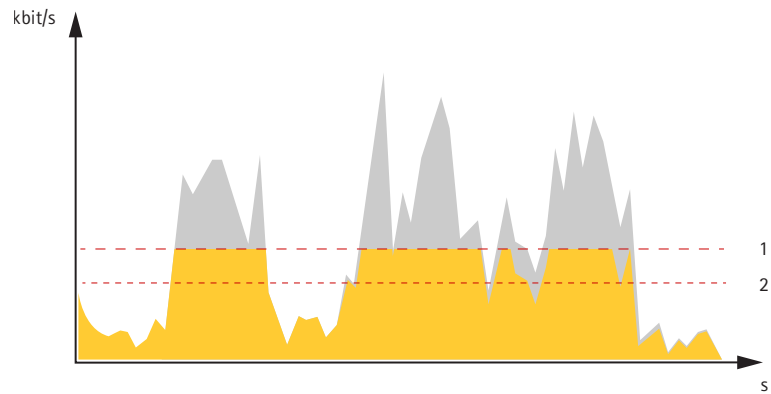
Średnia przepływność bitowa jest dostosowywana automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak najlepszą jakość obrazu wideo przy dostępnych zasobach pamięci masowej. Przepływność bitowa jest wyższa w scenach z dużą aktywnością w porównaniu ze scenami statycznymi. Korzystanie z opcji średniej przepływności zwiększa szanse uzyskania lepszej jakości obrazu w scenach o wysokim poziomie aktywności. Można zdefiniować łączną ilość pamięci masowej wymaganej 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

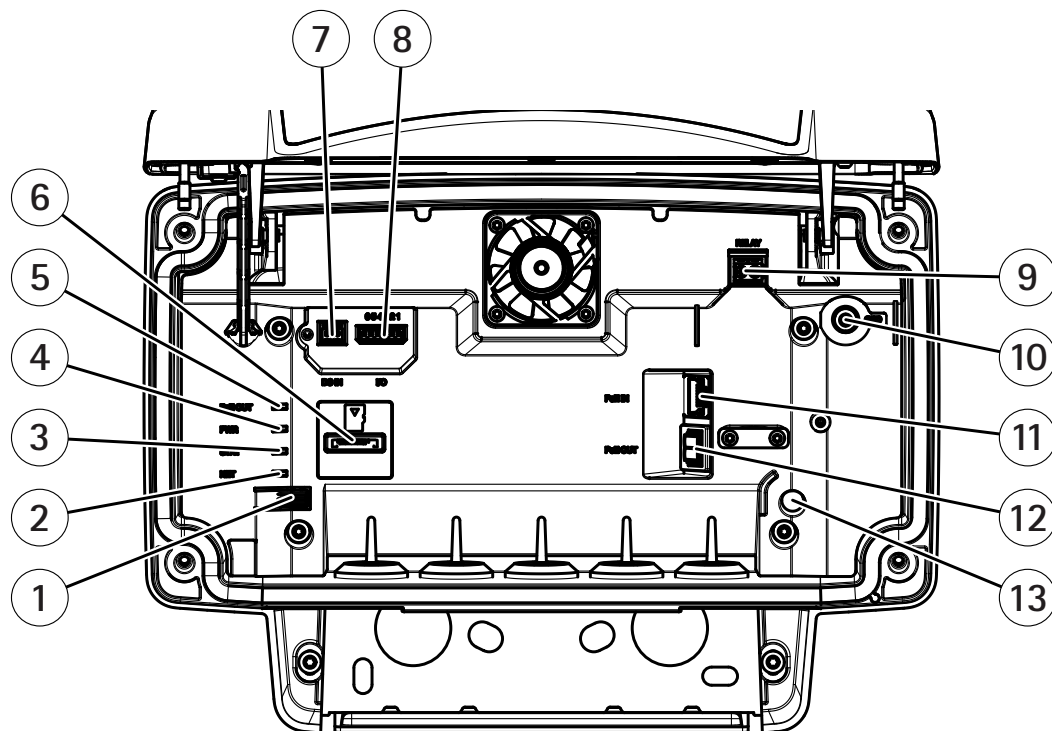
Można również włączyć maksymalną przepływność bitową i określić przepływność bitową w ramach średniej przepływności bitowej.



- 1 Docel. przepł. bitowa
- 2 Rzeczywista średnia przepływność bitowa

Specyfikacje

Przegląd produktów



- 1 Przycisk kontrolny
- 2 Wskaźnik LED sieci
- 3 Dioda stanu
- 4 Wskaźnik LED zasilania
- 5 Wskaźnik LED wyjścia PoE
- 6 Gniazdo kart microSD
- 7 Złącze zasilania (DC)
- 8 Złącze I/O
- 9 Złącze przekaźnikowe
- 10 Śruba uziemienia
- 11 Złącze sieciowe (PoE IN)
- 12 Złącze sieciowe (PoE OUT)
- 13 Czujnik alarmu wtargnięć

Specyfikacja techniczna: *Specyfikacje*, on page 33.

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przy normalnym działaniu.

Wskaźnik LED sieci	Wskazanie
Zielony	Stałe światło przy podłączeniu do sieci 100 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
Bursztynowy	Stałe światło przy podłączeniu do sieci 10 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
Zgaszony	Brak połączenia z siecią.

Wskaźnik LED zasilania	Wskazanie
Zielony	Normalne działanie.

Wskaźnik LED wyjścia PoE	Wskazanie
Zgaszony	PoE wyłączone
Zielony	PoE włączone

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

Lokalizacja przycisku Control: *Przegląd produktów, on page 33.*

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *page 38.*
- Łączenia się z usługą AXIS Video Hosting System. Patrz . Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około trzy sekundy, aż dioda LED stanu zacznie migać na zielono.

Złącza

Złącze sieciowe

Złącze RJ45 Ethernet z zasilaniem Power over Ethernet Plus (PoE+).

▲ UWAGA

Ryzyko zniszczenia urządzenia. Urządzenie nie może być zasilane jednocześnie ze źródeł PoE i DC.

Złącze sieciowe (PoE OUT)

Power over Ethernet IEEE 802.3 typu 2, maks. 30 W

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

Uwaga

Wyjście PoE jest włączone, gdy radar jest zasilany zasilaczem midspan o mocy 60 W (Power over Ethernet IEEE 802.3bt, typu 3).

Uwaga

Jeżeli radar jest zasilany przez 30-woltowy zasilacz midspan lub prąd stały, wyjście PoE OUT jest wyłączone.

Uwaga

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

Uwaga

Jeżeli do podłączonego urządzenia PoE potrzeba więcej niż 30 W, można rozszerzyć instalację o zasilacz midspan 60 W zasilacz między portem PoE wyjściowym w radarze i urządzeniem. Zasilacz Midspan będzie dostarczał zasilanie do urządzenia, natomiast radar dozorowy zapewni połączenie z siecią Ethernet.

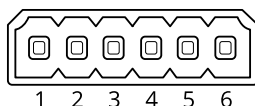
Złącze I/O

Złącze WE/WY służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wyzwaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze WE/WY zapewnia interfejs do:

Wejście cyfrowe – Do podłączenia urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okiennych lub drzwiowych oraz czujników wykrywania zbiecia szyby.

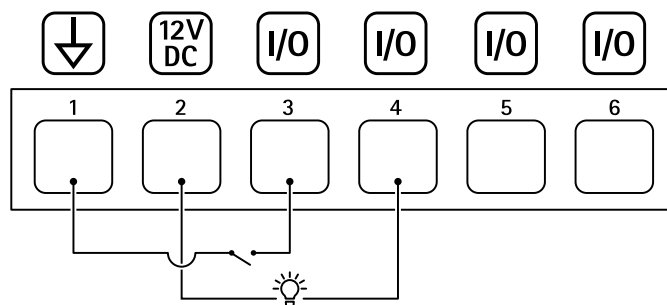
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

6-pinowego bloku złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	 Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 50 mA
Konfigurowalne (wejście lub wyjście)	3–6	Wejście cyfrowe – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Przykład:

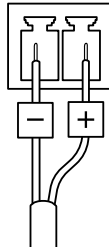


- 1 Masa DC
- 2 Wyjście DC 12 V, maks. 50 mA
- 3 We/Wy skonfigurowane jako wejście
- 4 We/Wy skonfigurowane jako wyjście

- 5 Konfigurowalne We/Wy
6 Konfigurowalne We/Wy

Złącze zasilania

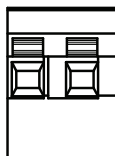
2-pinowy blok złączy na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤ 100 W lub nominalnym prądem ograniczonym do ≤ 5 A.



▲ UWAGA

Ryzyko zniszczenia urządzenia. Urządzenie nie może być zasilane jednocześnie ze źródeł PoE i DC.

Złącze przekaźnikowe



▲ UWAGA

W złączu przekaźnikowym należy używać przewodów jednodrutowych.

Funkcje	Specyfikacje
Typ	Normalnie otwarte
Zasilanie	24 V DC/5 A
Izolacja od innych obwodów	2,5 kV

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 czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawianie plam na obudowie.
1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
 2. W razie potrzeby można wyczyścić urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą i łagodnym mydłem niezawierającym środków ściernych.
 3. Aby usunąć jakiegokolwiek pozostałości środków czyszczących, należy przetrzeć urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą.
 4. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Więcej informacji na temat czyszczenia urządzeń Axis znajduje się w białej księdze *Odporność chemiczna na popularne środki czyszczące*.

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 33*.
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).

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 dokumencie *Cykł eksploatacji oprogramowania AXIS OS: ścieżka aktualizacji*.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

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 38.*

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 15*.

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.

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

Kwestie wydajności

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

Najważniejsze czynniki, które należy uwzględnić:

- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do cyberbezpieczeństwa znajdują się na stronie: axis.com/about-axis/cybersecurity. Przestrzegaj poniższych wytycznych dotyczących cyberbezpieczeństwa, aby otrzymywać powiadomienia od Axis dotyczące bezpieczeństwa produktów oraz skonfigurować produkt w sposób zapewniający bezpieczny cykl eksploatacji oraz wycofanie z użytku.

Na stronie *Axis Trust Center* znajdują się informacje o sposobach, w jakie Axis zapewnia zgodność z wymogami bezpieczeństwa, transparentność, ochronę danych oraz ochronę prywatności.

Postępowanie z lukami w zabezpieczeniach

Axis ma status *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA)*. Aby zminimalizować ryzyko narażenia na zagrożenia, postępujemy zgodnie z branżowymi normami w zakresie wykrywania i usuwania luk w zabezpieczeniach naszych urządzeń, oprogramowania i usług. Informacje na temat naszej polityki zarządzania lukami w zabezpieczeniach oraz instrukcje dotyczące zgłaszania luk znajdują się na stronie axis.com/vulnerability-management.

Powiadomienia dotyczące zabezpieczeń

Subskrybuj powiadomienia o zagrożeniach bezpieczeństwa w produktach Axis na stronie axis.com/security-notification-service. Będziemy informować Cię o lukach w zabezpieczeniach, udzielać odnośnych wskazówek oraz powiadamiać o innych kwestiach związanych z bezpieczeństwem użytkowanego produktu Axis.

Bezpieczny cykl eksploatacji produktu

Axis minimalizuje ryzyko w całym cyklu eksploatacji swoich produktów dzięki bezpiecznemu zarządzaniu cyklem eksploatacji. Skorzystaj z naszych przewodników dotyczących zwiększenia bezpieczeństwa dostępnych na stronie help.axis.com, aby bezpieczniejszymi konfigurować i obsługiwać produkty Axis oraz uzyskać informacje na poniższe tematy:

Bezpieczne pierwsze użycie – Produkty Axis są skonfigurowane fabrycznie z wysokim poziomem domyślnej ochrony, co oznacza bezpieczną pierwszą konfigurację oraz szyfrowaną komunikację od samego początku użytkowania.

Przeznaczenie i typowe błędy w konfiguracji – Nasze przewodniki zawierają informacje o przeznaczeniu produktów Axis, w tym o typowych błędach użytkowania związanych z bezpieczeństwem oraz błędach przy konfiguracji, których należy unikać.

Zarządzanie lukami w zabezpieczeniach i transparentność łańcucha dostaw – Wraz z każdą wersją oprogramowania na stronie axis.com publikowany jest wykaz komponentów oprogramowania (SBOM – Software Bill of Material) w celu poinformowania o lukach w zabezpieczeniach (podatnościach na zagrożenie) oraz zwiększenia transparentności łańcucha dostaw.

Wycofanie z eksploatacji i bezpieczne usuwanie danych – Aby bezpiecznie wycofać produkt po zakończeniu cyklu eksploatacji, przywróć jego ustawienia fabryczne. Spowoduje to usunięcie konfiguracji, zapisanych danych oraz informacji poufnych.

T10145149_pl

2026-07 (M33.2)

© 2020 – 2026 Axis Communications AB