AXIS D2210-VE Radar

User manual

Spis treści

Instalacja 4
Uwagi 4
Gdzie montować produkt 4
Instalacja wielu radarów 5
Profile radaru 7
Profil dozorowania strefy 7
Pokrywany obszar 7
Zasięg detekcji w strefie 7
Przykłady instalacji w strefie 8
Przypadki zastosowań do dozorowania stref 9
Profil dozorowania drogi 10
Zasięg detekcji na drodze 10
Przykłady instalacji przy drodze 10
Przypadki zastosowania w dozorowaniu drogi 12
Od czego zacząć 14
Wyszukiwanie urządzenia w sieci 14
Obsługiwane przeglądarki 14
Otwórz interfejs WWW urządzenia 14
Utwórz konto administratora 14
Bezpieczne hasła 14
Sprawdzanie braku zmian w oprogramowaniu urządzenia 15
Omówienie interfejsu WWW 15
Konfiguracja urządzenia 16
Wybór profilu radaru 16
Ustawianie poziomu montażu 16
Kalibruj mapę referencyjną 17
Ustawianie stref detekcji 17
Dodawanie scenariuszy 18
Dodawanie stref wykluczenia 19
Minimalizowanie fałszywych alarmów 19
Regulowanie obrazu radaru 20
Wyświetlanie nakładek na obrazie 20
Wyświetlanie nakładki tekstu 20
Przeglądanie i rejestracja obrazów wideo 21
Zmniejszanie zapotrzebowania na przepustowość i zasób 21
Konfiguracja zasobów sieciowej pamięci masowej 21
Rejestracja i odtwarzanie obrazu 22
Konfiguracja reguł dotyczących zdarzeń 22
Wyzwalanie akcji 22
Rejestrowanie obrazu wideo z kamery po wykryciu ruchu 22
Nagrywanie obrazu z kamery, gdy pojazd jedzie w niewłaściwym kierunku 23
Włączanie czerwonego światła ostrzegawczego na radarze 24
Wysyłanie wiadomości e-mail, gdy radar zostanie przykryty metalowym przedmiotem 25
Włączanie światła po wykryciu ruchu 26
Sterowanie kamerą PTZ za pomocą radaru 26
Wysyłanie danych radaru za pomocą MQTT 28
Interfejs WWW 29
Status 29
Radar 30
Ustawienia 30
Strumień 32
Kalibracja mapy 33
Strefy wykluczenia 34

Scenariusze....35
Nakładki....36
Dynamiczna taśma LED....38
Automatyczne śledzenie radaru PTZ....38
Nagrania....39
Aplikacje....41
System....41
Czas i lokalizacja....41
Sieć....43
Bezpieczeństwo....47
Konta....51
Zdarzenia....53
MQTT....58
Przechowywanie....61
Profile strumienia....63
ONVIF....64
Detektory....67
Akcesoria....67
Edge-to-edge....67
Dzienniki....69
Zwykła konfiguracja....70
Konserwacja....70
Konserwacja....70
Rozwiązywanie problemów....71
Sprawdzanie poprawności instalacji....72
Sprawdzanie poprawności instalacji radaru....72
Zakończenie sprawdzania poprawności....73
Więcej informacji....74
Strumieniowanie i pamięć masowa....74
Formaty kompresji obrazów wideo....74
Sterowanie przepływnością bitową....74
Nakładki....76
Specyfikacje....77
Przegląd produktów....77
Wskaźniki LED....77
....77
Gniazdo karty SD....78
Przyciski....78
Przycisk kontrolny....78
Złącza....78
Złącze sieciowe (PoE IN)....78
Złącze sieciowe (PoE OUT)....78
Złącze I/O....79
Złącze zasilania....80
Czyszczenie urządzenia....81
Rozwiązywanie problemów –....82
Przywróć domyślne ustawienia fabryczne....82
Sprawdzanie bieżącej wersji systemu AXIS OS....82
Aktualizacja systemu AXIS OS:....82
Problemy techniczne, wskazówki i rozwiązania....83
Kwestie wydajności....84
Kontakt z pomocą techniczną....84

Instalacja

To wideo przedstawia przykładową instalację radaru.

Dokładne instrukcje dotyczące wszystkich scenariuszy instalacji, a także ważne informacje dotyczące bezpieczeństwa, można znaleźć na stronie *axis.com/products/axis-d2210-ve-radar/support*.

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

Uwagi

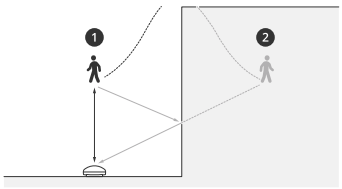
Gdzie montować produkt

Monitorowanie obszaru lub drogi

Radar jest przeznaczony do monitorowania otwartych przestrzeni i można go używać do obserwacji obszaru lub drogi. Radar oferuje dwa profile optymalizujące wydajność w każdym z tych scenariuszy. Więcej informacji na temat zasięgu detekcji, przykłady instalacji oraz przypadki użycia: .

Ignorowanie obiektów i powierzchni odbicia

Większość obiektów (takich jak ściana, ogrodzenie, drzewo lub duży krzew) w obszarze objętym zasięgiem powoduje utworzenie dodatkowego martwego punktu (cienia). Obiekty metalowe w polu widzenia powodują odbicia wpływające na skuteczność funkcji klasyfikacji obiektów radaru. Może to powodować fałszywe ślady i fałszywe alarmy w strumieniu radarowym.



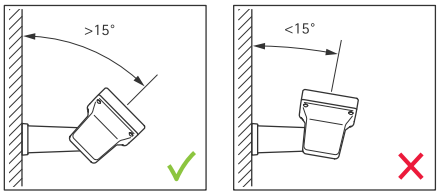
1 *Rzeczywista detekcja*
2 *Detekcja z odbicia (fałszywe ślady)*

Więcej informacji na temat sposobów postępowania w przypadku obiektów odbijających światło: .

Pozycjonowanie

Produkt należy zamontować na stabilnym słupie lub w takim miejscu na ścianie, w którego pobliżu nie ma innych obiektów ani instalacji. Na wydajność produktu mogą wpływać obiekty, które odbijają fale radiowe, znajdujące się w odległości 1 m po jego lewej i prawej stronie.

Jeżeli produkt jest instalowany na ścianie, należy ustawić go dalej od ściany pod kątem co najmniej 15°.

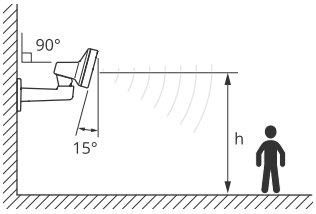


Kąt obrotu

Kąt walca produktu musi być niemal równy zeru, co oznacza, że radar powinien być na równi z horyzontem.

Kąt pochylenia

Radar może być pochylany w zakresie 0–30°, ale zalecane pochylenie montażowe urządzenia wynosi 15°. Aby ułatwić uzyskanie 15-stopniowego kąta pochylenia, należy się upewnić się, że tylna część obudowy jest wypoziomowana, tak jak to pokazano na ilustracji.



W podglądzie na żywo radaru można dodać nakładkę pokazującą kąt pochylenia radaru. Instrukcje:

Jednoczesna obecność

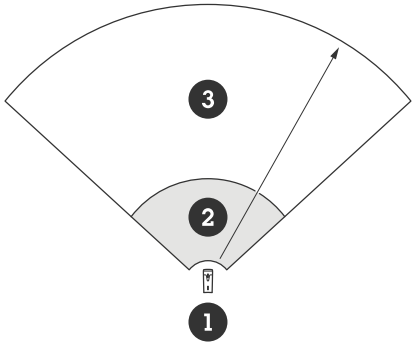
Jeśli zamontowano blisko siebie więcej niż osiem radarów Axis pracujących w paśmie częstotliwości 60 GHz, mogą one wzajemnie zakłócać swoją pracę. Więcej o unikaniu zakłóceń: .

Instalacja wielu radarów

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

Jednoczesna obecność

Fale radiowe radaru wykraczają poza obszar detekcji i mogą zakłócać działanie innych radarów w odległości do 350 m (380 jardów). Nazywa się to strefą współwystępowania.

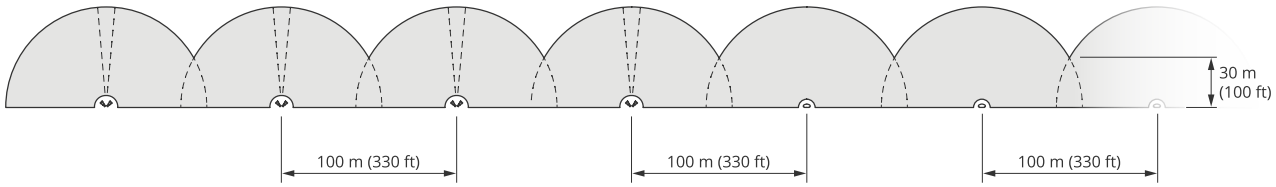


1 Radar
2 Obszar detekcji
3 Obszar współistnienia

Radar ten działa w paśmie częstotliwości 60 GHz. Można zainstalować maksymalnie osiem radarów o częstotliwości 60 GHz blisko siebie lub naprzeciwko siebie bez powodowania zakłóceń. Wbudowany algorytm współistnienia znajdzie odpowiednie przedziały czasu i częstotliwości, aby radary działały bez odczuwalnych zakłóceń.

Jeśli instalacja zawiera więcej niż osiem radarów pracujących w tym samym paśmie częstotliwości, a wiele urządzeń jest od siebie oddalonych, ryzyko zakłóceń jest mniejsze. Ogólnie rzecz biorąc radar wystawiony na zakłócenia nie przestaje działać. W urządzeniu działa algorytm łagodzenia zakłóceń, który w przypadku wystąpienia zakłóceń stara się poprawić jakość sygnału radaru. Ostrzeżenia o zakłóceniach będą wyświetlane w instalacjach, gdzie wiele radarów funkcjonuje w tej samej strefie współwystępowania w tym samym paśmie częstotliwości. Najważniejszą konsekwencją zakłóceń jest pogorszenie skuteczności detekcji, a czasami też zgłaszanie fałszywych śladów.

Radary Axis pracujące w różnych pasmach częstotliwości nie będą się nawzajem zakłócać. Można na przykład połączyć kamerę AXIS D2210-VE z wieloma radarami AXIS D2110-VE Security Radar działającymi w paśmie częstotliwości 24 GHz bez wywoływania zakłóceń.



Cztery pary radarów AXIS D2210-VE i wiele radarów AXIS D2110-VE Security Radars zamontowanych obok siebie.

Uwaga

Radar AXIS D2110-VE Security Radar wymaga dodatkowej konfiguracji, jeśli w tej samej strefie współwystępowania zamontowanych jest więcej niż dwa radary AXIS D2110-VE. Więcej informacji można znaleźć w *instrukcji obsługi radaru AXIS D2110-VE Security Radar*.

Środowisko

Umieszczając wiele radarów w lokalizacji, należy uwzględnić również inne kryteria projektowe, takie jak cechy otoczenia, kołyszące się obiekty, maszty i kołysząca się roślinność. Czasami w celu uniknięcia fałszywych alarmów trzeba odfiltrowywać kołyszące się obiekty ze strumienia danych wysyłanych z radaru.

Profile radaru

Radar może służyć do monitorowania obszaru lub drogi. Dla tych scenariuszy dostępne są dwa zoptymalizowane profile:

- **Area monitoring profile (Profil monitorowania obszaru)**: służy do śledzenia ludzi, pojazdów i niewielkich obiektów poruszających się z prędkością poniżej 55 km/h
- **Road monitoring profile (Profil monitorowania drogi)**: służy głównie do śledzenia pojazdów poruszających się z prędkością do 200 km/h

Wybierz obszar lub profil monitorowania w interfejsie WWW radaru. Instrukcje: .

Profil dozorowania strefy

Area monitoring profile (Profil dozorowania 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: .

Pokrywany obszar

AXIS D2210-VE ma pole detekcji w poziomie wynoszące 95°. Obszar pokrycia odpowiada powierzchni 2700 m^2 (29000 ft^2) w przypadku ludzi i 6100 m^2 (65600 ft^2) w przypadku pojazdów.

Uwaga

Aby uzyskać optymalny obszar detekcji, należy zamontować radar na wysokości 3,5–7 m (11–23 ft). Wysokość montażowa ma wpływ na martwe pole pod radarem.

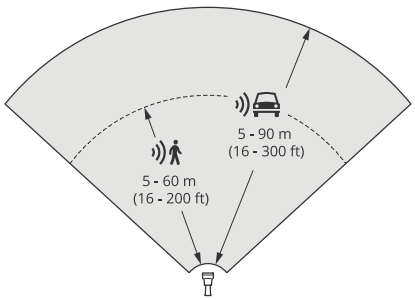
Zasięg detekcji w strefie

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).

Area monitoring profile (Profil dozorowania strefy) jest zoptymalizowany pod kątem wykrywania ludzi. Istnieje jednakże możliwość wykrywania pojazdów oraz innych obiektów poruszających się z prędkością do 55 km/h (34 mph) (z dokładnością prędkości +/- 2 km/h [1,24 mph]).

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

- 5–60 m (16–200 ft) podczas detekcji ludzi
- 5–90 m (16–300 ft) podczas detekcji pojazdów



Uwaga

- Podczas kalibracji radaru w interfejsie WWW należy wprowadzić wysokość montażu.
- Zakres detekcji wpływa na scenę i kąt pochylenia produktu.
- Zakres detekcji zależy od typu poruszającego się obiektu i jego rozmiaru.

Zakres detekcji radaru był mierzony w tych warunkach:

- Zasięg jest mierzony wzdłuż podłoża.
- Obiekt był osobą o wzroście 170 cm (5 ft 7 in).
- Osoba ta przechodziła bezpośrednio przed radarem.
- Wartości zostały zmierzone w momencie, kiedy osoba weszła do strefy detekcji.
- Czułość radaru została ustawiona jako **Medium (Średnia)**.

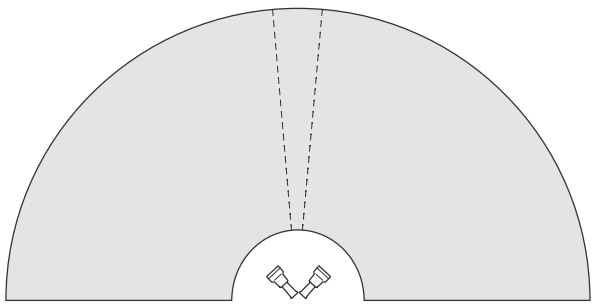
Wysokość montażowa	Pochylenie 0°	Pochylenie 5°	Pochylenie 10°	Pochylenie 15°	Pochylenie 20°	Pochylenie 25°	Pochylenie 30°
3,5 m (11 ft)	6,0–60+ m (19–196+ ft)	5,0–60+ m (16–196+ ft)	4,0–60+ m (13–196+ ft)	4,0–60 m (13–196 ft)	4,0–55 m (13–180 ft)	4,0–40 m (13–131 ft)	4,0–30 m (13–98 ft)
4,5 m (14 ft)	6,0–60+ m (19–196+ ft)	6,0–60+ m (19–196+ ft)	5,0–60+ m (16–196+ ft)	4,0–60+ m (13–96+ ft)	4,0–60 m (13–196 ft)	4,0–45 m (13–147 ft)	4,0–40 m (13–131 ft)
6 m (19 ft)	10–60+ m (32–196+ ft)	9,0–60+ m (29–196+ ft)	7,0–60+ m (22–196+ ft)	6,0–60+ m (19–196+ ft)	6,0–60 m (19–196 ft)	5,0–55 m (16–180 ft)	5,0–55 m (16–180 ft)
8 m (26 ft)	16–60 m (52–196 ft)	14–60 m (45–196 ft)	10–60 m (32–196 ft)	8,0–60+ m (26–196+ ft)	8,0–60+ m (26–196+ ft)	7,0–60 m (22–196 ft)	7,0–60 m (22–196 ft)
10 m (32 ft)	21–60 m (68–196 ft)	19–60 m (62–196 ft)	14–60 m (45–196 ft)	12–60+ m (39–196+ ft)	10–60+ m (32–196+ ft)	9,0–60 m (29–196 ft)	9,0–60 m (29–196 ft)
12 m (39 ft)	25–60 m (82–196 ft)	23–60 m (75–196 ft)	19–60 m (62–196 ft)	16–60+ m (52–196+ ft)	13–60+ m (42–196+ ft)	11–60+ m (36–196+ ft)	11–55 m (36–180 ft)

Uwaga

- Ustawienie czułości radaru **Low (Niska)** zmniejszy zasięg detekcji o 20%, a ustawienie **High (Wysoka)** zwiększy zasięg detekcji o 20%.

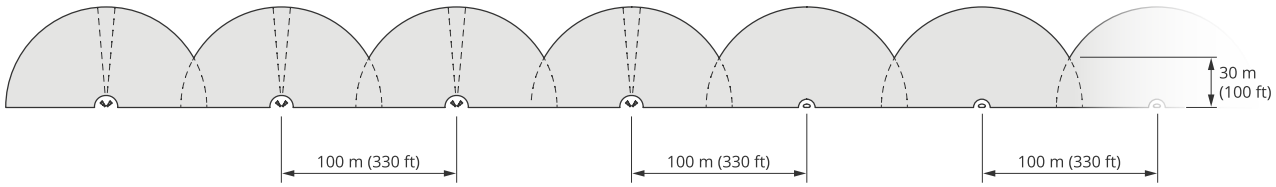
Przykłady instalacji w strefie

Aby utworzyć wirtualne ogrodzenie, na przykład wzdłuż budynku lub wokół niego, można umieścić do ośmiu radarów AXIS D2210-VE obok siebie. Umieszczenie dwóch radarów AXIS D2210-VE obok siebie zapewnia 180-stopniowe pokrycie.



Dwa radary AXIS D2210-VE zamontowane obok siebie zapewniają pokrycie 180°.

Jeśli w układzie obok siebie montujesz więcej niż dwa radary AXIS D2210-VE, każdą następną parę umieść w odstępie 100 m (330 ft) od siebie.



Cztery pary radarów AXIS D2210-VE i wiele radarów AXIS D2110-VE Security Radar zamontowanych w odstępach co 100 m (330 ft).

Radary Axis pracujące w różnych pasmach częstotliwości nie będą się nawzajem zakłócać. Oznacza to, że można połączyć radar AXIS D2210-VE pracujący w paśmie częstotliwości 60 GHz z radarem AXIS D2110-VE Security Radar pracującym w paśmie częstotliwości 24 GHz w strefie współwystępowania.

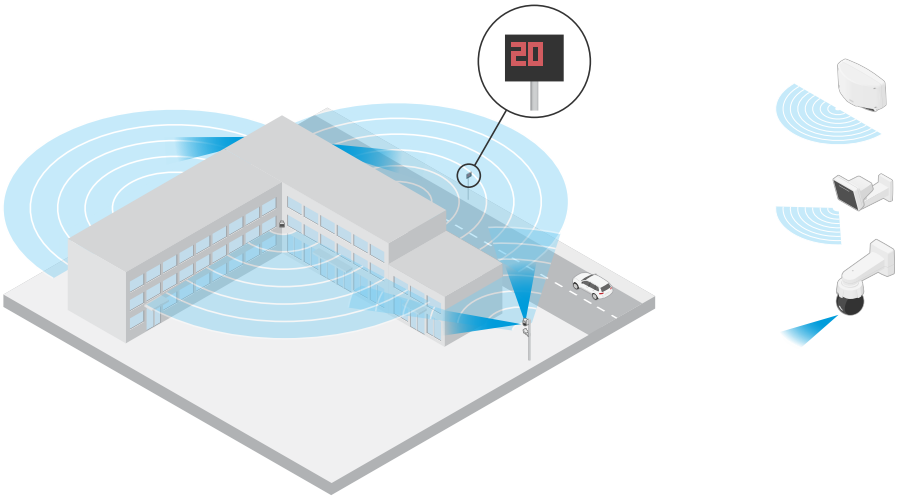
Więcej informacji na temat interfejsu i strefy współwystępowania: .

Przypadki zastosowań do dozorowania stref

Pokrycie obszaru wokół budynku

Firma w biurowcu chce zabezpieczyć swój obiekt przed włamaniami i akrami wandalizmu, szczególnie po godzinach pracy. Aby zapewnić pokrycie obszar wokół budynku, zainstalowano radary i kamery PTZ. Z myślą o zabezpieczeniu dłuższych ścian budynku zamontowano radary AXIS D2110-VE Security Radar z pokryciem 180°, a w celu zabezpieczenia krótszych ścian i narożników — radary AXIS D2210-VE Radar z pokryciem 95°. Radary zostały skonfigurowane tak, aby wyzwalały alarm, gdy osoby zbliżają się do budynku po godzinach pracy. Aby zapewnić wizualnie potwierdzenie obecności potencjalnych intruzów, zamontowano dwie kamery PTZ. Radary mogą sterować kamerami PTZ za pomocą *AXIS Radar Autotracking for PTZ*.

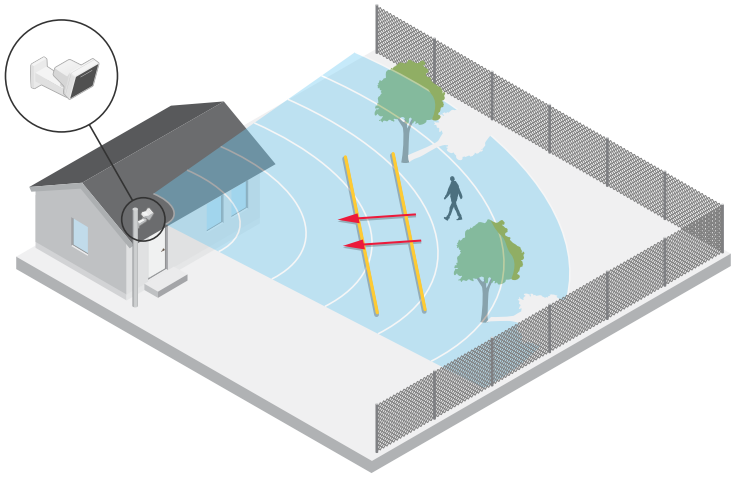
Firma chce również zapewnić bezpieczeństwo na terenie obiektu w godzinach pracy. Aby zapewnić, że pojazdy przejeżdżające drogą obok budynku nie jadą za szybko, jeden z radarów AXIS D2110-VE Security Radar sparowano ze znakiem prędkości Microbus za pomocą *AXIS Radar Integration for Microbus*.



Monitorowanie złożonej sceny

Teren firmy, na którym znajdują się ważne urządzenia, jest otoczony ogrodzeniem, aby zabezpieczyć go przed intruzami. To jednak za mało, by chronić teren przed manipulacją i sabotażem. Firma chce, aby alarm uruchamiał się, gdy osoby zbliżą się do budynku. Jednak w scenie są drzewa z kołyszącymi się gałęziami, metalowe ogrodzenie, które może powodować odbicia, a po terenie niekiedy biegają małe zwierzęta, które mogą wywoływać fałszywe alarmy.

Aby zmniejszyć liczbę fałszywych alarmów, skonfigurowano scenariusz w interfejsie WWW radaru tak, aby alarm były wyzwalany po przekroczeniu przez zbliżający się obiekt dwóch wirtualnych linii. Dzięki temu alarm jest wyzwalany tylko w przypadku obiektów, które celowo zmierzają w kierunku budynku, podczas gdy obiekty, które przekroczą tylko jedną z wirtualnych linii, są ignorowane.



W miejscach, w których nie ma ogrodzeń, dwie linie mogą spełniać rolę wirtualnego ogrodzenia. Więcej o dodawaniu dwóch linii do scenariusza w interfejsie WWW radaru: .

Profil dozorowania drogi

Profil monitorowania drogi jest zoptymalizowany pod kątem śledzenia pojazdów poruszających się z prędkością do 200 km/h na szosach i autostradach. Do obserwacji osób i innych obiektów poruszających się wolniej, należy użyć profilu monitorowania obszaru. Więcej informacji znajduje się w rozdziale .

Zasięg detekcji na drodze

Road monitoring profile (Profil dozorowania drogi) jest zoptymalizowany pod kątem wykrywania pojazdów i zapewnia dokładność pomiaru prędkości rzędu +/- 2 km/h (1,24 mph) podczas dozorowania pojazdów poruszających się z prędkością do 200 km/h (125 mph).

Wysokość montażu radaru i prędkość pojazdu będą miały wpływ na zasięg detekcji. Po zamontowaniu na optymalnej wysokości radar wykrywa zbliżające i oddalające się pojazdy z dokładnością +/- 2 km/h (1,24 mph) w następujących zakresach:

- **25–100 m (82–328 ft)** w przypadku pojazdów poruszających się z prędkością 50 km/h (31 mph).
- **40–80 m (131–262 ft)** w przypadku pojazdów poruszających się z prędkością 100 km/h (62 mph).
- **50–70 m (164–230 ft)** w przypadku pojazdów poruszających się z prędkością 200 km/h (125 mph).

Uwaga

Aby zminimalizować ryzyko niewykrycia pojazdów poruszających się z dużą prędkością, skonfiguruj w radarze scenariusz wyzwalający obiekty o typach **Vehicle (Pojazd)** i **Unknown (Nieznany)**. Więcej informacji o konfigurowaniu scenariusza: .

Przykłady instalacji przy drodze

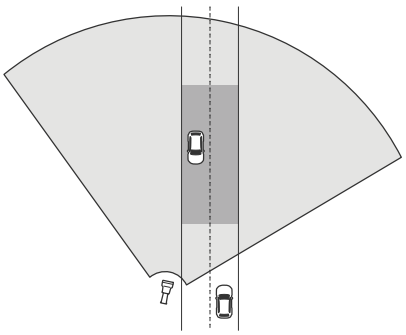
Do celów monitorowania dróg i autostrad radar musi być zamontowany na odpowiedniej wysokości, aby uniknąć martwych punktów (cienia) za pojazdami.

Uwaga

Rozmiar cienia zależy od wysokości montażu radaru oraz wysokości i odległości pojazdów od radaru. Na przykład, gdy pojazd o wysokości 4,5 m (15 ft) znajduje się odległości 50 m (164 ft) od radaru zamontowanego na wysokości 8 m (26 ft), cień za pojazdem będzie wynosił 50 m (164 ft). Jeśli jednak radar jest zamontowany na wysokości 12 m (39 ft), cień za tym samym pojazdem będzie wynosił tylko 23 m (74 ft).

Montaż na poboczu

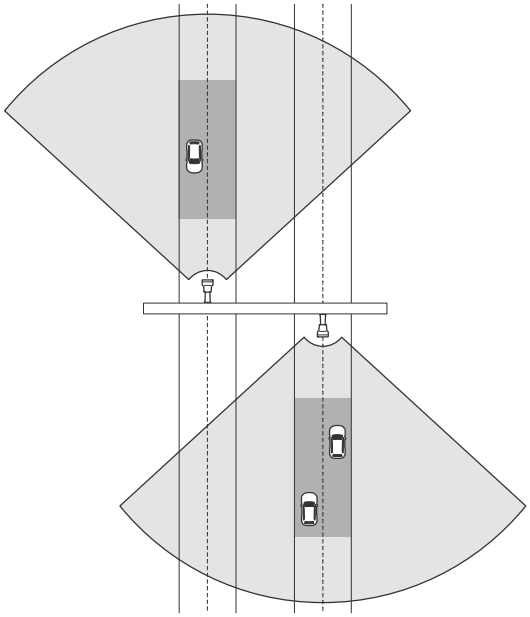
Aby monitorować pojazdy poruszające się po drodze, można zamontować radar na poboczu, na przykład na słupie. W tego typu instalacjach zalecamy obrót pod kątem maksymalnie 25°.



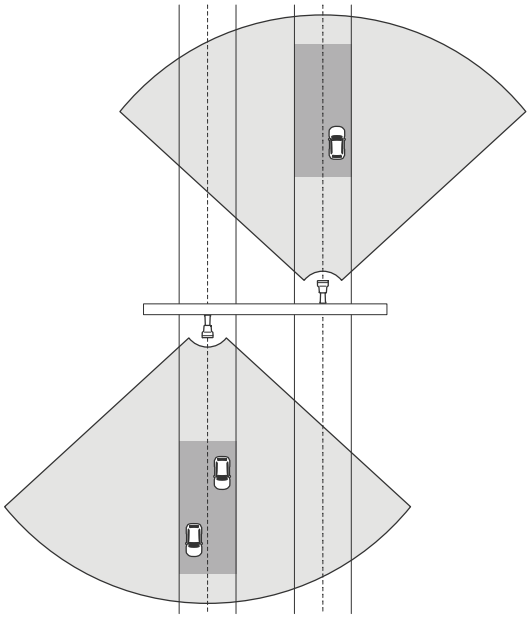
Aby dokładnie mierzyć duże prędkości, radar należy umieścić w odległości 10 m (32 ft) od pojazdów. Więcej o zasięgu detekcji i dokładności wykrywania prędkości: .

Montaż na środku

W celu monitorowania pojazdów na drodze wielopasmowej, można zamontować jeden lub więcej radarów na bramownicy nad drogą.



Tak samo można monitorować pojazdy oddalające się od radaru.



Aby dokładnie mierzyć duże prędkości, radar należy umieścić w odległości 10 m (32 ft) od pojazdów. Więcej o zasięgu detekcji i dokładności wykrywania prędkości: .

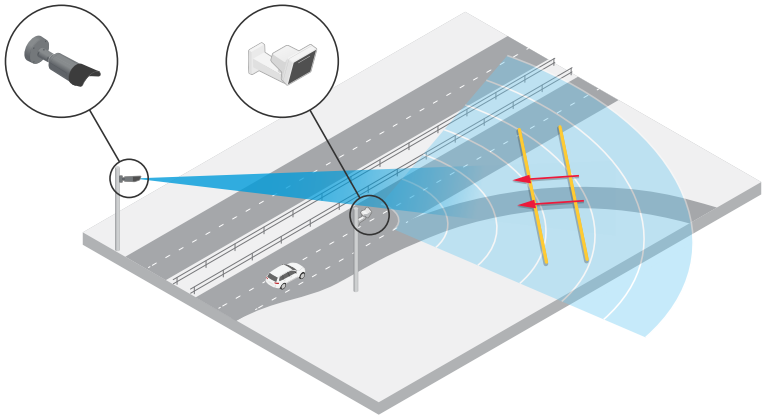
Przypadki zastosowania w dozorowaniu drogi

Typowym zastosowaniem radaru AXIS D2210-VE Radar i profilu monitorowania drogi jest śledzenie i pomiar prędkości pojazdów. Radaru można używać w połączeniu z kamerą wizualną i aplikacją AXIS Speed Monitor do wizualizacji prędkości pojazdów w podglądzie na żywo z kamery lub do rejestrowania śladów radaru do celów statystycznych. Więcej informacji można znaleźć w *podręczniku użytkownika aplikacji AXIS Speed Monitor*.

Więcej przykładów konfiguracji radaru w połączeniu z profilem monitorowania dróg można znaleźć w następujących przypadkach użycia:

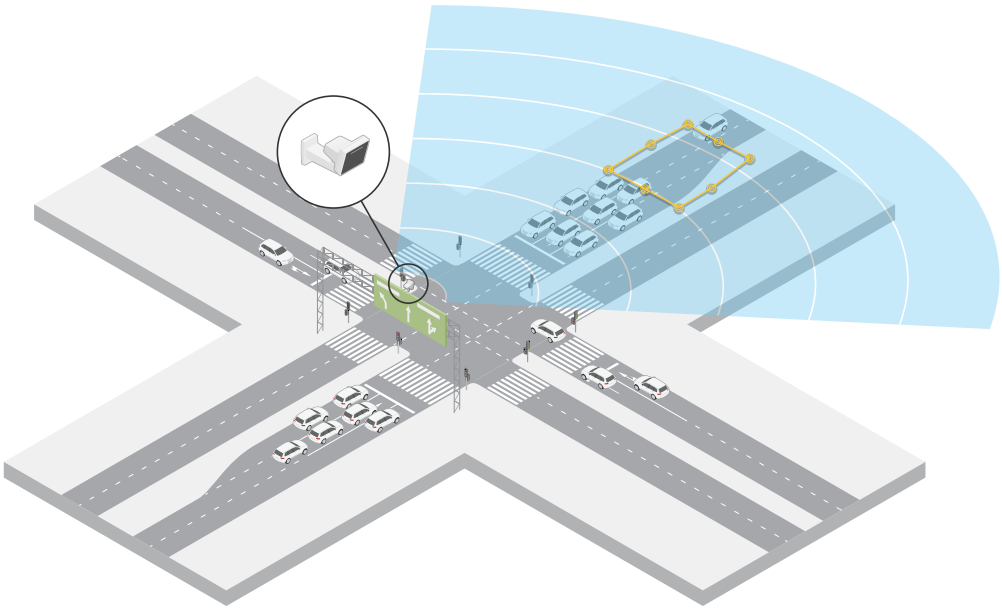
Wykrywanie nieprawidłowej jazdy na rampie autostradowej

W celu wykrywania i identyfikowania pojazdów jadących w nieprawidłowym kierunku na rampie autostradowej, służby kontroli ruchu używają radaru AXIS D2210-VE i kamery Axis typu bullet. Radar jest zamontowany na słupie i skierowany w stronę rampy, aby wykrywać pojazdy jadące w niewłaściwym kierunku. Aby zapewnić niezawodne wykrywanie, stosowany jest scenariusz przekroczenia linii i konfiguracja wyzwalania alarmu przez radar po przekroczeniu przez pojazd dwóch linii. W scenariuszu zostają ustawione dwie linie na rampie, jak pokazano na ilustracji. Określony jest również kierunek jazdy oraz prędkości, przy których ma nastąpić wyzwolenie alarmu. Gdy radar wyzwala alarm, kamera Axis typu bullet może zapewnić wizualną identyfikację pojazdu na rampie.



Monitorowanie natężenia ruchu na skrzyżowaniu — korki

Do monitorowania korków na ruchliwym skrzyżowaniu służby kontroli ruchu instalują radar na bramownicy nad skrzyżowaniem. W interfejsie WWW radaru ustawiają scenariusz i konfigurują go tak, aby był wyzwalany przez pojazdy poruszające się w danym obszarze. Scenariusz obejmuje tylko część drogi prowadzącą do skrzyżowania. Aby alarm był wyzwalany w chwili, gdy tworzy się zator, ustawiana jest prędkość poniżej 5 km/h (3 mph).



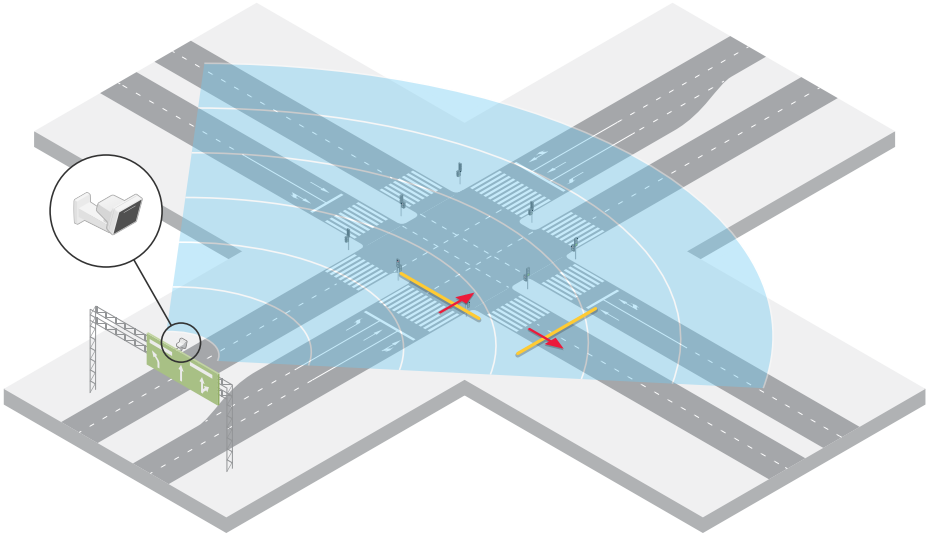
Monitorowanie natężenia ruchu na skrzyżowaniu — kierunek

Aby uzyskać przegląd przepływu ruchu i kierunku jazdy pojazdów na ruchliwym skrzyżowaniu, służby kontroli ruchu instalują radar na bramownicy nad drogą prowadzącą do skrzyżowania. W interfejsie WWW radaru konfigurują scenariusz przekroczenia linii, w którym pojazdy muszą przekroczyć dwie linie, aby uruchomić alarm. Pierwsza z dwóch linii znajduje się nad pasami prowadzącymi do skrzyżowania, za przejściem dla pieszych tak, aby pojazdy nie zatrzymywały się na linii. Druga linia znajduje się nad pasami ruchu prowadzącymi w prawo. Aby wyzwolić alarm, pojazdy muszą przekroczyć obie linie, jadąc w określonym kierunku. Aby uniknąć wyzwalania alarmu dla kilku pojazdów jednocześnie, obniżono minimalny czas wyzwalania w scenariuszu z 2 do 0 sekund.

Aby monitorować przepływ ruchu we wszystkich kierunkach, utworzono jeden scenariusz dla każdego kierunku.

Uwaga

Scenariusz nie zlicza pojazdów przekraczających linie; zamiast tego do zliczania pojazdów można używać systemu zdarzeń w interfejsie WWW radaru. Jednym ze sposobów zliczania pojazdów jest wysyłanie wiadomości MQTT za każdym razem, gdy wyzwalany jest scenariusz, i liczenie tych wyzwoleń po stronie odbiornika MQTT.



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

* Aby korzystać z interfejsu WWW AXIS OS w systemie iOS 15 lub iPadOS 15, przejdź do menu **Settings (Ustawienia) > Safari > Advanced (Zaawansowane) > Experimental Features (Funkcje eksperymentalne)** i wyłącz NSURLSession Websocket.

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 .

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: .

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz .
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 .

Bezpieczne hasła

Ważne

Urządzenia Axis wysyłają wstępnie ustawione hasło przez sieć jako zwykły tekst. Aby chronić urządzenie po pierwszym zalogowaniu, skonfiguruj bezpieczne i szyfrowane połączenie HTTPS, a następnie zmień hasło.

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.

Sprawdzanie 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 .
   Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Omówienie interfejsu WWW

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

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

Interfejs WWW urządzenia Axis

Konfiguracja urządzenia

Wybór profilu radaru

W interfejsie WWW:

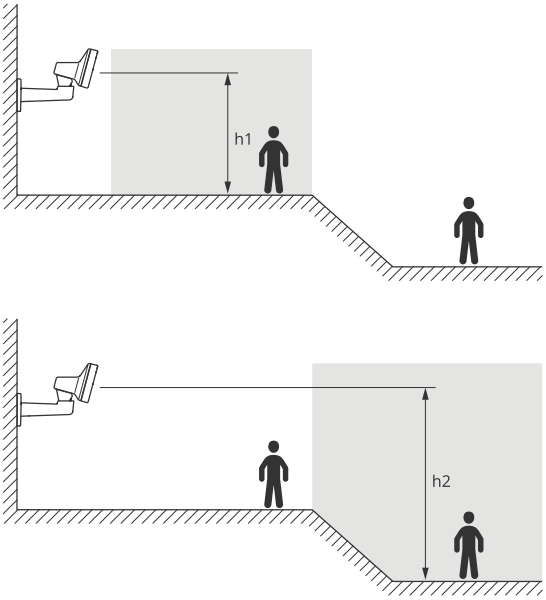
1. Wybierz kolejno opcje **Radar > Settings > Detection (Radar > Ustawienia > Detekcja)**.
2. W menu **Radar profiles (Profile radaru)** wybierz profil.

Ustawianie poziomu montażu

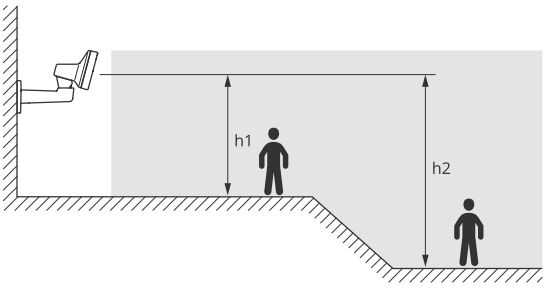
Ustaw wysokość montażu radaru w jego interfejsie WWW. Pomaga to radarowi w prawidłowej detekcji i pomiarze prędkości znajdujących się w jego zasięgu obiektów.

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

Przykład:
W zależności od obszaru zainteresowania wysokość montażu (h1, h2) jest różna.



Jeśli powierzchnia w obszarze zainteresowania jest nierówna, podczas konfigurowania radaru dodaj średnią wysokość (w tym przypadku (h1 + h2) / 2).



Ustawianie wysokości montażu:

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

Kalibruj mapę referencyjną

Prześlij mapę referencyjną, aby łatwiej zobaczyć, gdzie poruszają się wykryte obiekty. Można użyć planu terenu lub zdjęcia lotniczego przedstawiającego obszar objęty radarem. Skalibruj mapę tak, aby zasięg radaru pasował do pozycji, kierunku i skali mapy, a następnie zoomuj mapę, jeśli interesuje Cię konkretna część zasięgu radaru.

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 .

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 przycisk **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 przycisk **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 przycisk **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 przycisk **Dalej**.
3. Umieść linię w scenie.
   Za pomocą myszy przesuń linię i nadaj jej pożądany kształt.
4. Aby zmienić kierunek detekcji, włącz opcję **Change direction (Zmień kierunek)**.
5. Kliknij przycisk **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 przycisk **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 przycisk **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 przesuń linię i nadaj jej pożądany kształt.
5. Aby zmienić kierunek detekcji, włącz opcję **Change direction (Zmień kierunek)**.
6. Kliknij przycisk **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 przycisk **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 odblaskowe 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 pożądaną 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: i .
- 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 .

- 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.

Regulowanie obrazu radaru

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej na temat działania niektórych funkcji, przejdź do .

Wyświetlanie nakładek na obrazie

Możesz dodać obraz jako nałożenie do strumienia radaru.

1. Wybierz kolejno opcje **Radar > Overlays (Radar > Nakładki)**.
2. Wybierz opcję **Image (Obraz)** i kliknij +.
3. Kliknij przycisk **Images (Obrazy)**.
4. Przeciągnij i upuść obraz.
5. Kliknij przycisk **Upload (Prześlij)**.
6. Kliknij przycisk **Manage overlay (Zarządzaj nałożeniem)**.
7. Wybierz obraz i położenie. Aby zmienić położenie obrazu nakładki, można go również przeciągnąć w podglądzie na żywo.

Wyświetlanie nakładki tekstu

Możesz dodać pole tekstowe jako nakładkę strumienia radaru. Jest to przydatne na przykład do wyświetlania daty, godziny lub nazwy firmy w strumieniu wideo.

1. Wybierz kolejno opcje **Radar > Overlays (Radar > Nakładki)**.
2. Wybierz opcję **Text (Tekst)** i kliknij +.

3. Wpisz tekst, który ma być wyświetlany w strumieniu wideo.
4. Wybierz położenie. Aby zmienić położenie pola tekstowego nakładki, można je również przeciągnąć w podglądzie na żywo.

Wyświetlanie nakładki tekstu z kątem pochylenia radaru

W podglądzie na żywo radaru można dodać nakładkę pokazującą kąt pochylenia radaru. Jest to przydatne podczas instalacji lub kiedy trzeba sprawdzić, jaki jest kąt pochylenia urządzenia.

Uwaga

Nałożenie kąta pochylenia wyświetla wartość 90, gdy urządzenie jest ustawione poziomo. Jeżeli na nałożeniu widać wartość 75, oznacza to, że radar jest pochylony pod kątem 15° poniżej linii horyzontu.

1. Wybierz kolejno opcje **Radar > Overlays (Radar > Nakładki)**.
2. Wybierz opcję **Text (Tekst)** i kliknij + .
3. Wybierz **#op**.
   Możesz też kliknąć **Modifier (Modyfikator)** i wybrać **#op** z listy.
4. Wybierz położenie. Aby zmienić położenie pola 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 .

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.
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

Aby uzyskać więcej informacji, zapoznaj się z przewodnikiem *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 **Action (Akcję)**, którą urządzenie ma wykonać po spełnieniu warunków.

Uwaga

Po dokonaniu zmian w aktywnej regule należy ją uruchomić ponownie, aby uwzględnić zmiany.

Uwaga

Jeżeli zmieniasz definicję profilu strumienia używanego w regule, musisz ponownie uruchomić wszystkie reguły korzystające z tego profilu strumienia.

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.

Podłącz urządzenia:

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. Wprowadź nazwę reguły.
5. Z listy warunków wybierz scenariusz w obszarze **Radar motion (Ruch radaru)** .

Aby skonfigurować scenariusz, przejdź do sekcji .

6. Z listy akcji wybierz opcję **Toggle I/O while the rule is active (Przełącz WE/WY 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 wyzwalać 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**.

Nagrywanie obrazu z kamery, gdy pojazd jedzie w niewłaściwym kierunku

W tym przykładzie wyjaśniono, jak skonfigurować radar i kamerę, aby kamera rozpoczynała zapis na karcie SD, gdy radar wykryje pojazd jadący w niewłaściwym kierunku.

Zanim rozpoczniesz

- W interfejsie WWW radaru można utworzyć scenariusz, który uruchamia się po przekroczeniu przez pojazd podwójnej linii.
  Więcej informacji: .
- Umieść dwie linie nad pasem ruchu, w miejscu, w którym chcesz wykrywać pojazdy jadące w niewłaściwym kierunku. Aby łatwiej zobaczyć, gdzie poruszają się obiekty, skorzystaj z mapy referencyjnej, np zdjęć lotniczych.
  Więcej informacji: .

1. Utwórz dwóch odbiorców w radarze.
   1.1. W interfejsie radaru kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj pierwszego odbiorcę.
   1.2. Wprowadź następujące informacje:
   - **Nazwa**: Aktywacja portu wirtualnego
   - **Typ**: **HTTP**
   - **URL**: http://<adresIP>/axis-cgi/virtualinput/activate.cgi
     Element <adresIP> zastąp adresem kamery, dla której chcesz rozpocząć nagrywanie.
   - Nazwa użytkownika i hasło do kamery.

   1.1. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
   1.2. Kliknij przycisk **Zapisz**.
   1.3. Dodaj drugiego odbiorcę z następującymi informacjami:
   - **Nazwa**: Dezaktywacja portu wirtualnego
   - **Typ**: **HTTP**
   - **URL**: http://<adresIP>/axis-cgi/virtualinput/deactivate.cgi
     Element <adresIP> zastąp adresem kamery.

- Nazwa użytkownika i hasło do kamery.

1.1. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.

1.2. Kliknij przycisk **Zapisz**.

2. Utwórz dwóch reguły w radarze.

2.1. W interfejsie radaru kamery przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj pierwszą regułę.

2.2. Wprowadź następujące informacje:

- **Nazwa**: Aktywowanie wirtualnego WE/WY1
- **Condition (Warunek)**: Wybierz scenariusz utworzony w obszarze **Radar motion (Ruch radaru)**.
- **Action (Akcja)**: **Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)**
- **Recipient (Odbiorca)**: **Aktywacja portu wirtualnego**
- **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1

2.1. Kliknij przycisk **Zapisz**.

2.2. Dodaj kolejną regułę z następującymi informacjami:

- **Nazwa**: Dezaktywacja wirtualnego WE/WY1
- **Condition (Warunek)**: Wybierz scenariusz utworzony w obszarze **Radar motion (Ruch radaru)**.
- Wybierz opcję **Invert this condition (Odwróć ten warunek)**.
- **Action (Akcja)**: **Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)**
- **Recipient (Odbiorca)**: **Dezaktywacja portu wirtualnego**
- **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1

2.1. Kliknij przycisk **Zapisz**.

3. Utwórz regułę w kamerze.

3.1. W interfejsie internetowym kamery przejdź do menu **System > Events > Rules (System > Zdarzania > Reguły)** i dodaj regułę.

3.2. Wprowadź następujące informacje:

- **Nazwa**: Wyzwalacz w wirtualnym wejściu 1
- **Condition (Warunek)**: **I/O (WE/WY) > Virtual input is active (Wejście wirtualne jest aktywne)**.
- **Port**: **1**
- **Action (Akcja)**: **Recordings > Record video while the rule is active (Nagrania > Nagrywaj wideo, gdy reguła jest aktywna)**
- **Storage options (Opcje pamięci masowej)**: **SD_DISK**
- Wybierz **Camera (Kamera)** i **Stream profile (Profil strumienia)**.

3.1. Kliknij przycisk **Zapisz**.

Włączanie czerwonego światła ostrzegawczego na radarze

Z przodu radaru możesz włączyć dynamiczną taśmę LED, aby informować, że obszar jest monitorowany.

W tym przykładzie wyjaśniono, jak aktywować to czerwone światło i jak skonfigurować harmonogram, tak aby było widoczne tylko po godzinach pracy w dni powszednie.

Tworzenie harmonogramu:

1. Przejdź do menu **System (System) > Events (Zdarzenia) > Schedules (Harmonogramy)** i dodaj nowy harmonogram.
2. Wprowadź nazwę harmonogramu.
3. W obszarze **Type (Typ)** wybierz opcję **Schedule (Harmonogram)**.
4. W sekcji **Recurrent (Powtarzanie)** wybierz **Daily (Każdego dnia)**.
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. Wprowadź nazwę reguły.
3. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
4. Wybierz harmonogram utworzony w rozwijalnym menu **Schedule (Harmonogram)**.
5. Na liście akcji w obszarze **Radar** wybierz **Dynamic LED strip (Dynamiczna taśma LED)**.
6. Wybierz wzór **Sweeping red (Omiatający czerwony)** z menu rozwijalnego **Pattern (Wzór)**.
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.

Uwaga

Opcja tworzenia reguł dla zdarzeń sabotażu radaru jest dostępna od wersji systemu AXIS OS 11.11.

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. Wybierz adres**E-mail**.
4. Wprowadź adres e-mail odbiorcy.
5. Kamera nie ma dedykowanego serwera poczty e-mail, więc należy się zalogować na inny serwer, aby wysyłać wiadomości e-mail. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
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. Wprowadź nazwę reguły.
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**.

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 .
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**.

Sterowanie kamerą PTZ za pomocą radaru

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

- . Wbudowanej opcji można użyć w przypadku jednej kamery PTZ i jednego radaru zamontowanych bardzo blisko siebie.
- . 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. .

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: .

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, bu 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 zmieszczą 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*.

Wysyłanie danych radaru za pomocą MQTT

Do pobierania danych radaru dotyczących wykrytych obiektów i wysyłania ich prze MQTT służy radar z aplikacją AXIS Speed Monitor.

W tym przykładzie pokazujemy, jak skonfigurować klienta MQTT w urządzeniu, na którym jest zainstalowana aplikacja AXIS Speed Monitor, oraz jak utworzyć warunek publikujący dane pobrane za pomocą aplikacji AXIS Speed jako próbkę do brokera MQTT.

Zanim zaczniesz:

- Zainstaluj AXIS Speed Monitor na radarze lub w kamerze podłączonej do radaru. Więcej informacji można znaleźć w *podręczniku użytkownika aplikacji AXIS Speed Monitor*.
- Skonfiguruj brokera MQTT i uzyskaj adres IP oraz nazwę użytkownika i hasło brokera. Więcej informacji na temat MQTT i brokerów MQTT można znaleźć w bazie wiedzy *AXIS OS Knowledge Base*.

Skonfiguruj klienta MQTT za pomocą interfejsu WWW urządzenia, na którym jest zainstalowana aplikacja AXIS Speed Monitor:

1. Otwórz menu **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wpisz następujące informacje:
   - **Host**: Adres IP brokera
   - **Client ID (Identyfikator klienta)**: Identyfikator urządzenia
   - **Protocol (Protokół)**: Protokół, na który jest ustawiony broker
   - **Port**: Numer portu używany przez brokera
   - **Username (nazwa użytkownika)** i **Password (hasło)** brokera
2. Kliknij **Save (Zapisz)** i **Connect (Połącz)**.

Utwórz warunek publikujący dane radaru jako próbkę do brokera MQTT:

3. Przejdź do menu **System > MQTT > MQTT publication (System > MQTT > Publikacja MQTT)** i kliknij **+ Add condition (dodaj warunek)**.
4. Z listy warunków w obszarze **Application (Aplikacja)** wybierz **Speed Monitor: Track exited zone (Speed Monitor: Śledź opuszczoną strefę)**.

Urządzenie będzie teraz mogło wysyłać informacje o śladach radaru każdego poruszającego się obiektu, który opuszcza strefę scenariusza. Każdy obiekt będzie miał własne parametry śladu radaru, takie jak **rmd_zone_name (nazwa strefy)**, **tracking_id** (id śledzenia) i **trigger_count (liczba wyzwoleń)**. Pełną listę parametrów można znaleźć w *instrukcji obsługi aplikacji AXIS Speed Monitor*.

Interfejs WWW

Aby przejść do interfejsu WWW urządzenia, wpisz adres IP urządzenia w przeglądarce internetowej.

Uwaga

Obsługa funkcji i ustawień opisanych w tym rozdziale różni się w zależności od urządzenia. Ikona wskazuje, że funkcja lub ustawienie są dostępne tylko w niektórych urządzeniach.

Wyświetl/ukryj menu główne.

Wyświetl informacje o wersji.

Uzyskaj dostęp do pomocy dotyczącej produktu.

Zmień język.

Ustaw jasny lub ciemny motyw.

Menu użytkownika zawiera opcje:

- Informacje o zalogowanym użytkowniku.
- **Change account (Zmień konto)**: Wyloguj się z bieżącego konta i zaloguj się na nowe konto.
- **Log out (Wyloguj się)**: Wyloguj się z bieżącego konta.

Menu kontekstowe zawiera opcje:

- **Analytics data (Dane analityczne)**: Zaakceptuj, aby udostępniać nie osobiste dane przeglądarki.
- **Feedback (Opinia)**: Ta opcja pozwala wystawiać opinie, by pomagać nam w poprawianiu funkcjonalności produktów i usług.
- **Legal (Informacje prawne)**: Wyświetl informacje o plikach cookie i licencjach.
- **About (Informacje)**: Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.

Status

Informacje o urządzeniu

Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.

Upgrade AXIS OS (Aktualizacja AXIS OS): umożliwia zaktualizowanie oprogramowania urządzenia. Ta opcja pozwala przejść do strony Maintenance (Konserwacja), gdzie można wykonać aktualizację.

Stan synchronizacji czasu

Pokazuje informacje o synchronizacji z usługą NTP, w tym czy urządzenie jest zsynchronizowane z serwerem NTP oraz czas pozostały czas do następnej synchronizacji.

NTP settings (Ustawienia NTP): umożliwia wyświetlenie i zaktualizowanie ustawień NTP. Ta opcja pozwala przejść do strony **Time and location (Czas i lokalizacja)**, gdzie można zmienić ustawienia usługi NTP.

Bezpieczeństwo

Pokazuje, jakiego rodzaju dostęp do urządzenia jest aktywny, które protokoły szyfrowania są używane oraz, czy dozwolone jest korzystanie z niepodpisanych aplikacji. Zalecane ustawienia bazują na przewodniku po zabezpieczeniach systemu operacyjnego AXIS.

Hardening guide (Przewodnik po zabezpieczeniach): Kliknięcie spowoduje przejście do *przewodnika po zabezpieczeniach systemu operacyjnego AXIS OS*, gdzie można się dowiedzieć więcej o stosowaniu najlepszych praktyk cyberbezpieczeństwa.

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

View details (Wyświetl szczegóły): Wyświetla i aktualizuje listę połączonych klientów. Na liście widać adres IP, protokół, port, stan i PID/proces każdego połączenia.

Trwające zapisy

Ta opcja wyświetla trwające nagrania i zasób pamięci, w którym mają być zapisane.

Nagrania: pozwala wyświetlić trwające i przefiltrowane nagrania oraz ich źródła. Więcej informacji:

Pokazuje lokalizację zapisu nagrania w zasobie.

Radar

Ustawienia

Zapisy ogólne

Radar transmission (Transmisja radaru): Ta opcja pozwala całkowicie wyłączyć moduł radaru.

Channel (Kanał) : Jeżeli obecność wielu urządzeń powoduje wzajemne zakłócanie sygnałów, ustaw ten sam kanał maksymalnie dla czterech urządzeń znajdujących się blisko siebie. W większości instalacji należy wybrać opcję **Auto (Automatycznie)**, aby urządzenia same między sobą uzgadniały, którego kanału mają używać.

Poziom montażu: Wprowadź wysokość zamontowania produktu.

Uwaga

Postaraj się wpisać jak najdokładniejszą wartość. Dzięki temu urządzenie będzie mogło zwizualizować dane detekcji z radaru w odpowiednim miejscu na obrazie.

Detekcja

Detection sensitivity (Czułość detekcji): Wybierz czułość radaru. Wyższa wartość wydłuży zasięg detekcji, ale zwiększy ryzyko fałszywych alarmów. Niższa czułość pozwoli zmniejsza liczbę fałszywych alarmów, ale może skrócić odległość detekcji.

Radar profile (Profil radaru): Wybierz profil pasujący do obszaru zainteresowania.

- **Area monitoring (Dozorowanie obszaru)**: Pozwala dozorować zarówno duże, jak i małe obiekty poruszające się z mniejszą prędkością na otwartych przestrzeniach.
  - **Ignore stationary rotating objects (Ignoruj obracające się, ale nieprzemieszczające się obiekty)** : Włącz, aby maksymalnie ograniczyć liczbę fałszywych alarmów generowanych przez nieruchome, obracające się obiekty, takie jak wentylatory lub turbiny.
  - **Ignore small objects (Ignoruj małe obiekty)**: Włączenie tej opcji pozwala zminimalizować liczbę fałszywych alarmów wywołanych przez małe obiekty, takie jak koty lub króliki.
  - **Ignore swaying objects (Ignoruj kołyszące się obiekty)**: Włączenie tej opcji pozwala ograniczać do minimum liczbę fałszywych alarmów wywoływanych przez kołyszące się obiekty, takie jak drzewa, krzewy czy maszty z flagami.
- **Road monitoring (Dozorowanie drogi)**: Pozwala śledzić pojazdy poruszające się z większą prędkością w mieście i na drogach podmiejskich
  - **Ignore stationary rotating objects (Ignoruj obracające się, ale nieprzemieszczające się obiekty)** : Włącz, aby maksymalnie ograniczyć liczbę fałszywych alarmów generowanych przez nieruchome, obracające się obiekty, takie jak wentylatory lub turbiny.
  - **Ignore swaying objects (Ignoruj kołyszące się obiekty)**: Włączenie tej opcji pozwala ograniczać do minimum liczbę fałszywych alarmów wywoływanych przez kołyszące się obiekty, takie jak drzewa, krzewy czy maszty z flagami.

Wyświetl

Information legend (Legenda informacji): Włączenie tej opcji powoduje wyświetlenie legendy zawierającej typy obiektów, które mogą być wykrywane i śledzone przez radar. Przeciągnij i upuść, aby przesunąć legendę informacji.

Zone opacity (Przezroczystość strefy): Pozwala wybrać oczekiwany stopień nieprzezroczystości lub przezroczystości strefy obserwacji.

Przezroczystość siatki: Wybierz oczekiwaną nieprzezroczystości lub przezroczystości siatki.

Color scheme (Schemat kolorów): Wybór schematu wizualizowania detekcji z radaru.

Rotation (Obrót) : Pozwala wybrać preferowaną orientację obrazu z radaru.

Wizualizacja obiektu

Trail lifetime (Trwanie śladu): Pozwala wybrać, jak długo ma być wyświetlany ślad śledzonego obiektu w widoku radarowym.

Icon style (Styl ikon): Pozwala wybrać styl ikony śledzonego obiektu w widoku radaru. W przypadku zwykłych trójkątów wybierz **Triangle (Trójkąt)**. W przypadku reprezentatywnych symboli wybierz **Symbol**. Bez względu na wybrany styl ikony będą pokazywały kierunek poruszających się śledzonych obiektów.

Show information with icon (Pokaż informacje z ikoną): Pozwala wybrać informacje, które mają być wyświetlane przy ikonie śledzonego obiektu:

- **Object type (Typ obiektu)**: Pozwala wybrać typ obiektu wykrytego przez radar.
- **Classification probability (Prawdopodobieństwo klasyfikacji)**: Pokazuje stopień pewności klasyfikacji obiektu wykrytego przez radar.
- **Velocity (Prędkość)**: Pokazuje, jak szybko porusza się dany obiekt.

Strumień

Zapisy ogólne

Rozdzielczość: Wybierz rozdzielczość obrazu odpowiednią dla monitorowanej sceny. Wyższa rozdzielczość wymaga większej przepustowości i pojemności pamięci.

Frame rate (Liczba klatek na sekundę): Aby uniknąć problemów z przepustowością w sieci lub zmniejszyć zapotrzebowanie na zasoby pamięci, można ograniczyć poklatkowość do stałej liczby klatek na sekundę. Jeżeli liczba klatek na sekundę wynosi zero, utrzymywana jest najwyższa poklatkowość możliwa w danych warunkach. Większa poklatkowość wymaga większej przepustowości i pojemności zasobu.

P-frames (Klatki P): Ramka P to obraz przewidywany, na którym widać tylko zmiany w obrazie w stosunku do poprzedniej ramki. Wprowadź żądaną liczbę ramek P. Im wyższa wartość, tym mniejsza wymagana przepustowość. Jeżeli jednak w sieci występuje duży ruch, jakość obrazu wideo może widocznie spaść.

Compression (Kompresja): Użyj suwaka, aby dostosować kompresję obrazu. Wysoka wartość kompresji powoduje mniejszą przepływność bitową i niższą jakość obrazu. Niska kompresja poprawia jakość obrazu, ale zwiększa zapotrzebowanie na przepustowość i zasoby pamięci podczas nagrywania.

Signed video (Podpisany materiał wizyjny) : Włącz, aby do sygnału wizyjnego dodawać podpis. Podpisywanie sygnału wizyjnego chroni go przed sabotażem, ponieważ zostaje on opatrzony zaszyfrowanym podpisem.

Sterowanie przepływnością bitową

- **Average (Średnia)**: Wybierz, aby automatycznie dostosowywać przepływność w dłuższym okresie i zapewnić najlepszą możliwą jakość obrazu w oparciu o dostępną pamięć masową.
  -  Kliknij, aby obliczyć docelową przepływność w zależności od dostępnego pamięci masowej, czasu przechowywania i limitu przepływności.
  - **Target bitrate (Docelowa przepływność)**: Wprowadź żądaną szybkość transmisji.
  - **Retention time (Czas przechowywania)**: Wprowadź liczbę dni, przez jaką należy przechowywać nagrania.
  - **Pamięć masowa**: Wyświetla szacowaną ilość pamięci do wykorzystania na potrzeby strumienia.
  - **Maximum bitrate (Maks. przepływność bitowa)**: Włącz, aby ustawić limit przepływności.
  - **Bitrate limit (Ograniczenie przepływności)**: Wprowadź wartość limitu przepływności bitowej powyżej docelowej.
- **Maximum (Maksymalna)**: Wybranie tej opcji powoduje ustawienie maksymalnej natychmiastowej przepływności bitowej strumienia na podstawie przepustowości sieci.
  - **Maximum (Maksymalna)**: Wprowadź maksymalną przepływność.
- **Variable (Zmienna)**: Wybierz, aby umożliwić różnicowanie przepływności w zależności od poziomu aktywności w scenie. Większa aktywność wymaga większej przepustowości. Zalecamy tę opcję do większości sytuacji.

Kalibracja mapy

Funkcja kalibracji mapy pozwala załadować i skalibrować mapę referencyjną. Wynikiem kalibracji jest mapa referencyjna, na której wyświetlany jest zasięg radaru w odpowiedniej skali, co ułatwia dostrzeżenie, gdzie poruszają się obiekty.

Setup assistant (Asystent konfiguracji): Kliknij, aby otworzyć asystenta ustawień, który krok po kroku przeprowadzi Cię przez kalibrację.

Reset calibration (Resetuj kalibrację): Kliknij, aby usunąć bieżący obraz mapy i pozycję radaru na mapie.

Mapa

Upload map (Prześlij mapę): zaznacz lub przeciągnij obraz mapy, który chcesz przesłać.

Download map (Pobierz mapę): kliknij, aby pobrać mapę.

Rotate map (Obróć mapę): Użyj suwaka, aby obrócić obraz mapy.

Skala i odległość na mapie

Distance (Odległość): dodaj odległość między dwoma punktami dodanymi do mapy.

Obracanie i zoomowanie mapy

Panoramowanie: klikaj przyciski, aby obracać obraz mapy.

Zoom: klikaj przyciski, aby powiększać lub pomniejszać obraz mapy.

Reset pan and zoom (Resetuj obrót i zoomowanie): kliknij, aby usunąć ustawienia obrotu i zoomowania.

Umiejscowienie radaru

Położenie: Klikaj przyciski, aby przesuwać radar na mapie.

Obrót: Klikaj przyciski, aby obracać radar na mapie.

Strefy wykluczenia

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.

: Kliknij , aby utworzyć nową strefę wykluczenia.

Aby zmodyfikować strefę wykluczenia, wybierz ją z listy.

Track passing objects (Śledzenie mijanych obiektów): Włącz tę opcję, aby śledzić obiekty przechodzące przez strefę wykluczenia. Mijane obiekty zachowują identyfikatory śladów i są widoczne w całej strefie. Obiekty pojawiają się ze środka strefy wykluczenia nie będą śledzone.

Zone shape presets (Prepozycje kształtu strefy): Wybierz kształt początkowy strefy wykluczenia.

- **Cover everything (Pokryj wszystko)**: Wybierz, aby ustawić strefę wykluczenia obejmującą cały obszar pokrycia radaru.
- **Reset to box (Resetuj do pola)**: Zaznacz, aby umieścić prostokątną strefę wykluczenia na środku obszaru pokrycia.

Aby zmodyfikować kształt strefy, przeciągnij i upuść dowolne punkty na liniach. Aby usunąć punkt, kliknij go prawym przyciskiem myszy.

Scenariusze

Scenariusz to kombinacja warunków wyzwalania oraz ustawień sceny i detekcji.

: Kliknij, aby utworzyć nowy scenariusz. Można utworzyć maksymalnie 20 scenariuszy.

Triggering conditions (Warunki wyzwalania): Wybierz warunek, który będzie wyzwalał alarmy.

- **Movement in area (Ruch w obszarze)**: Pozwala wybrać, czy warunkiem wyzwalania mają być obiekty przemieszczające się w obszarze.
- **Przekroczenie linii**: Pozwala wybrać, czy scenariusz ma być wyzwalany przez obiekty przekraczające jedną lub dwie linie.

Scene (Scena): Pozwala określić obszar lub linie w scenariuszu, w obrębie których poruszające się obiekty będą powodowały wyzwalanie alarmu.

- W przypadku opcji **Movement in area (Ruch w obszarze)** wybierz jeden z wstępnie ustawionych kształtów, by zmienić obszar.
- W przypadku opcji **Line crossing (Przekroczenie linii)** przeciągnij i upuść linię w scenie. Aby utworzyć więcej punktów na linii, kliknij i przeciągnij kursor w dowolne miejsce na linii. Aby usunąć punkt, kliknij go prawym przyciskiem myszy.
  - **Require crossing of two lines (Wymagaj przekraczania dwóch linii)**: Włączenie tej funkcji spowoduje wyzwalanie alarmu dopiero, gdy obiekt przekroczy dwie linie.
  - **Change direction (Zmień kierunek):** Włączenie tej opcji będzie powodowało wyzwalanie alarmu, gdy obiekty przekroczą linię w przeciwnym kierunku.

Detection settings (Ustawienia detekcji): Pozwala zdefiniować kryteria wyzwalania scenariusza.

- W przypadku opcji **Movement in area (Ruch w obszarze)**:
  - **Ignore short-lived objects (Ignorowanie obiektów krótkotrwałych)**: Ustaw wartość opóźnienia w sekundach od wykrycia obiektu przez radar do wyzwolenia alarmu przez scenariusz. W ten sposób możesz ograniczyć liczbę fałszywych alarmów.
  - **Trigger on object type (Wyzwalanie według typu obiektu)**: Wybierz typ obiektów, które będą wyzwalane przez scenariusz (ludzie, pojazdy, nieznane).
  - **Speed limit (Limit prędkości)**: Wyzwalanie w przypadku obiektów poruszających się z szybkością mieszczącą się w konkretnym zakresie.
    - **Invert (Odwróć)**: Pozwala ustawić wyzwalanie alarmu powyżej lub poniżej limitu prędkości.
- W przypadku opcji **Line crossing (Przekroczenie linii)**:
  - **Ignore short-lived objects (Ignorowanie obiektów krótkotrwałych)**: Ustaw wartość opóźnienia w sekundach od wykrycia obiektu przez radar do wyzwolenia akcji przez scenariusz. W ten sposób możesz ograniczyć liczbę fałszywych alarmów. Ta opcja jest niedostępna w przypadku obiektów przekraczających dwie linie.
  - **Max time between crossings (Maksymalny czas między przejściami)**: Ta opcja pozwala ustawić maksymalny czas między przekroczeniem pierwszej a drugiej linii. Ta opcja jest dostępna tylko w przypadku obiektów przekraczających dwie linie.
  - **Trigger on object type (Wyzwalanie według typu obiektu)**: Wybierz typ obiektów, które będą wyzwalane przez scenariusz (ludzie, pojazdy, nieznane).
  - **Speed limit (Limit prędkości)**: Wyzwalanie w przypadku obiektów poruszających się z szybkością mieszczącą się w konkretnym zakresie.
    - **Invert (Odwróć)**: Pozwala ustawić wyzwalanie alarmu powyżej lub poniżej limitu prędkości.

Alarm settings (Ustawienia alarmu): Pozwala zdefiniować kryteria wyzwalania alarmu.

- **Minimum trigger duration (Minimalny czas trwania wyzwalacza)**: Pozwala ustawić minimalny czas trwania wyzwalanego alarmu.

Nakładki

: Kliknij, aby dodać nałożenie. Wybierz typ nałożenia z listy rozwijanej:

- **Text (Tekst)**: Wybierz, aby wyświetlać tekst zintegrowany z obrazem podglądu na żywo oraz widoczny we wszystkich widokach, nagraniach i zrzutach ekranu. Można wprowadzić własny tekst oraz dołączyć wstępnie skonfigurowane modyfikatory, które automatycznie pokazują na przykład godzinę, datę i poklatkowość.
  - : Kliknij, aby dodać modyfikator daty `%F` powodujący wyświetlanie daty w formacie rrrr-mm-dd.
  - : Kliknij, aby dodać modyfikator czasu `%X` powodujący wyświetlanie czasu w formacie gg:mm:ss (zegar 24-godzinny).
  - **Modifiers (Modyfikatory)**: Kliknij, aby wybrać dowolny skonfigurowany wstępnie modyfikator widoczny na liście w celu dodania go do pola tekstowego. Na przykład modyfikator `%a` powoduje wyświetlanie dnia tygodnia.
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - **Appearance (Wygląd)**: Umożliwia wybór koloru tekstu i tła, np. białego tekstu na czarnym tle (ustawienie domyślne).
  - : Wybierz lokalizację nałożenia na obrazie.
- **Obraz**: Wybierz, aby wyświetlać statyczny obraz nałożony na strumień wideo. Można użyć plików .bmp, .png, .jpeg lub .svg.
  Aby przesłać obraz, kliknij opcję **Images (Obrazy)**. Przed wysłaniem obrazu można użyć następujących opcji:
  - **Scale with resolution (Skaluj z rozdzielczością)**: Wybierz, aby automatycznie przeskalować obraz nałożenia i dopasować go do rozdzielczości obrazu wideo.
  - **Use transparency (Użyj przezroczystości)**: Wybierz i wprowadź wartość szesnastkową RGB dla danego koloru. Użyj formatu RRGGBB. Przykłady wartości szesnastkowych: FFFFFF (biały), 000000 (czarny), FF0000 (czerwony), 6633FF (niebieski), 669900 (zielony). Tylko dla obrazów .bmp.
- **Scene annotation (Adnotacja sceny)** : Ta opcja pozwala wyświetlać nałożenie tekstowe w strumieniu wideo, które pozostaje w tej samej pozycji, nawet gdy kamera obraca się lub przechyla w innym kierunku. Można wybrać wyświetlanie nałożenia tylko przy określonych zakresach powiększenia.
  - : Kliknij, aby dodać modyfikator daty `%F` powodujący wyświetlanie daty w formacie rrrr-mm-dd.
  - : Kliknij, aby dodać modyfikator czasu `%X` powodujący wyświetlanie czasu w formacie gg:mm:ss (zegar 24-godzinny).
  - **Modifiers (Modyfikatory)**: Kliknij, aby wybrać dowolny skonfigurowany wstępnie modyfikator widoczny na liście w celu dodania go do pola tekstowego. Na przykład modyfikator `%a` powoduje wyświetlanie dnia tygodnia.
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - **Appearance (Wygląd)**: Umożliwia wybór koloru tekstu i tła, np. białego tekstu na czarnym tle (ustawienie domyślne).
  - : Wybierz lokalizację nałożenia na obrazie. Nałożenie zostanie zapamiętane we współrzędnych obrotu i pochylenia tej pozycji.

- **Annotation between zoom levels (%) (Adnotacja pomiędzy poziomami zoomu (%))**: Pozwala ustawić poziomy zoomu, przy których nałożenie będzie widoczne.
- **Annotation symbol (Symbol adnotacji)**: Wybierz symbol, który będzie pokazywany zamiast nałożenia, gdy wartość zoomu przekroczy ustawiony zakres.

- **Streaming indicator (Wskaźnik strumieniowania)** : Wybierz, aby wyświetlać animację nałożoną na strumień wideo. Animacja wskazuje, że strumień wideo jest przesyłany na żywo, nawet jeśli w scenie nie ma ruchu.
  - **Appearance (Wygląd)**: Wybierz kolor tekstu i tła animacji, np. czerwoną animację na przezroczystym tle (ustawienie domyślne).
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - : Wybierz lokalizację nałożenia na obrazie.
- **Widget: Linegraph (Wykres liniowy)** : Wyświetla wykres przedstawiający zmiany mierzonej wartości w czasie.
  - **Title (Tytuł)**: Umożliwia wpisanie tytułu widgetu.
  - **Overlay modifier (Modyfikator nałożenia)**: Wybierz modyfikator nałożenia jako źródło danych. Utworzone przez Ciebie nałożenia MQTT będą na końcu listy.
  - : Wybierz lokalizację nałożenia na obrazie.
  - **Size (Rozmiar)**: Wybierz rozmiar nałożenia.
  - **Visible on all channels (Widoczne na wszystkich kanałach)**: Wyłącz tę opcję, aby wyświetlać tylko na aktualnie wybranym kanale. Włącz tę opcję, aby wyświetlać na wszystkich aktywnych kanałach.
  - **Update interval (Interwał aktualizacji)**: Pozwala wybrać czas pomiędzy aktualizacjami danych.
  - **Transparency Przezroczystość)**: Ta opcja pozwala ustawić przezroczystość całego nałożenia.
  - **Background transparency (Przezroczystość tła)**: Ta opcja pozwala ustawić tylko przezroczystość tła nałożenia.
  - **Points (Punkty)**: Włączenie tej opcji pozwala dodać punkt do linii wykresu podczas aktualizacji danych.
  - **Oś X**
    - **Label (Etykieta)**: Wprowadź etykietę tekstową osi x.
    - **Time window (Okno czasowe)**: Ta opcja pozwala wprowadzić czas wizualizacji danych.
    - **Time unit (Jednostka czasu)**: Wprowadź jednostkę czasu dla osi x.
  - **Oś Y**
    - **Label (Etykieta)**: Wprowadź etykietę tekstową osi y.
    - **Dynamic scale (Skala dynamiczna)**: Włączenie tej opcji spowoduje automatyczne dostosowywanie skali do wartości danych. Wyłączenie tej opcji pozwoli ręcznie wprowadzać wartości dla stałej skali.
    - **Min alarm threshold** and **Max alarm threshold (Minimalny i maksymalny próg alarmu)**: Wartości te dodadzą do wykresu poziome linie odniesienia, dzięki czemu łatwiej będzie zobaczyć, kiedy wartość danych staje się zbyt wysoka lub zbyt niska.

- **Widget: Meter (Miernik)** : Wyświetl wykres słupkowy pokazujący najnowszą zmierzoną wartość danych.
  - **Title (Tytuł)**: Umożliwia wpisanie tytułu widgetu.

- **Overlay modifier (Modyfikator nałożenia)**: Wybierz modyfikator nałożenia jako źródło danych. Utworzone przez Ciebie nałożenia MQTT będą na końcu listy.
- : Wybierz lokalizację nałożenia na obrazie.
- **Size (Rozmiar)**: Wybierz rozmiar nałożenia.
- **Visible on all channels (Widoczne na wszystkich kanałach)**: Wyłącz tę opcję, aby wyświetlać tylko na aktualnie wybranym kanale. Włącz tę opcję, aby wyświetlać na wszystkich aktywnych kanałach.
- **Update interval (Interwał aktualizacji)**: Pozwala wybrać czas pomiędzy aktualizacjami danych.
- **Transparency Przezroczystość)**: Ta opcja pozwala ustawić przezroczystość całego nałożenia.
- **Background transparency (Przezroczystość tła)**: Ta opcja pozwala ustawić tylko przezroczystość tła nałożenia.
- **Points (Punkty)**: Włączenie tej opcji pozwala dodać punkt do linii wykresu podczas aktualizacji danych.
- **Oś Y**
  - **Label (Etykieta)**: Wprowadź etykietę tekstową osi y.
  - **Dynamic scale (Skala dynamiczna)**: Włączenie tej opcji spowoduje automatyczne dostosowywanie skali do wartości danych. Wyłączenie tej opcji pozwoli ręcznie wprowadzać wartości dla stałej skali.
  - **Min alarm threshold** and **Max alarm threshold (Minimalny i maksymalny próg alarmu)**: Wartości te dodadzą do wykresu poziome linie odniesienia, dzięki czemu łatwiej będzie zobaczyć, kiedy wartość danych staje się zbyt wysoka lub zbyt niska.

Dynamiczna taśma LED

Dynamiczne wzory taśmy LED

Ta strona służy do testowania wzorów dynamicznej taśmy LED.

Pattern (Wzór): Wybierz wzór, który chcesz przetestować.

Duration (Czas trwania): Określ czas trwania testu.

Test (Testuj): Kliknij, aby uruchomić wzór, który chcesz przetestować.

Stop (Zatrzymaj): Kliknij, aby zatrzymać test. Jeśli podczas odtwarzania wzoru zamkniesz stronę, odtwarzanie zatrzyma się automatycznie.

Aby aktywować wzór do celów wskazywania lub odstraszani, przejdź do menu **System > Events (System > Zdarzenia)** i utwórz regułę. Przykład: .

Automatyczne śledzenie radaru PTZ

Sparowanie radaru z kamerą PTZ umożliwia korzystanie z funkcji automatycznego śledzenia w radarze. Aby nawiązać połączenie, przejdź do menu **System > Edge-to-edge**.

Skonfiguruj wstępne ustawienia:

Camera mounting height (Wysokości montażowej kamery): Odległość od podłoża do wysokości, na której zamontowana jest kamera PTZ.

Pan alignment (Wyrównanie obrotu): Obróć kamerę PTZ tak, aby była skierowana w tym samym kierunku co radar. Kliknij adres IP, aby uzyskać dostęp do kamery PTZ.

Save pan offset (Zapisz przesunięcie obrotu): Kliknij tę opcję, aby zapisać wyrównanie obrotu.

Ground incline offset (Przesunięcie nachylenia terenu): Użyj przesunięcia nachylenia terenu, aby precyzyjnie dopasować pochylenie kamery. Jeżeli podłoże jest nachylone lub jeśli kamera nie jest zamontowana poziomo, to podczas śledzenia obiektu kamera może być skierowana za nisko lub za wysoko.

Done (Gotowe): Kliknij tę opcję, aby zapisać ustawienia i kontynuować konfigurację.

Konfigurowanie automatycznego śledzenia kamery PTZ:

Track (Śledź): Można wybrać śledzenie ludzi, pojazdów i/lub nieznanych obiektów.

Śledzenie: Włącz tę opcję, aby rozpocząć śledzenie obiektów za pomocą kamery PTZ. Umożliwia to automatyczne przybliżenie obiektu lub grupy obiektów tak, aby znalazły się w polu widzenia kamery.

Object switching (Przełączanie obiektów): Jeśli radar wykryje wiele obiektów, które nie zmieszczą się w polu widzenia kamery PTZ, będzie ona śledzić obiekt o najwyższym priorytecie nadanym przez radar, a pozostałe obiekty zignoruje.

Object hold time (Czas obserwacji obiektów): Ta opcja pozwala ustawić liczbę sekund przeznaczonych na śledzenie obiektu przez kamerę PTZ.

Return to home (Wróć do pozycji domowej): Włącz opcję Wróć do pozycji domowej, jeżeli kamera PTZ ma powrócić do położenia wyjściowego, gdy radar przestanie śledzić obiekt.

Return to home timeout (Limit czasu powrotu do pozycji domowej): Oznacza czas, przez jaki kamera PTZ pozostaje w ostatniej znanej pozycji śledzonego obiektu przed powrotem do pozycji domowej.

Zoom: Za pomocą suwaka można precyzyjnie wyregulować zoom kamery PTZ.

Reconfigure installation (Skonfiguruj ponownie instalację): Kliknięcie tej opcji pozwala wyczyścić wszystkie ustawienia i powrócić do wstępnej konfiguracji.

Nagrania

Ongoing recordings (Trwające nagrania): Pokaż wszystkie trwające zapisy na urządzeniu.

● Wybierz, aby rozpocząć nagrywanie w urządzeniu.

Wybierz docelowy zasób, w którym chcesz zapisać nagrania.

● Zatrzymaj nagrywanie w urządzeniu.

Uruchomione nagrania zostaną zakończone zarówno po zatrzymaniu ręcznym, jak i po wyłączeniu urządzenia.

Zapis ciągły będzie kontynuowane do momentu zatrzymania ręcznego. Jeśli urządzenie zostanie wyłączone, zapis będzie kontynuowany po jego ponownym włączeniu.

Odtwórz nagranie.

Zatrzymaj odtwarzanie nagrania.

Wyświetl lub ukryj informacje i opcje nagrania.

Set export range (Ustaw zakres eksportu): Jeżeli chcesz wyeksportować tylko część nagrania, określ zakres czasu. Pamiętaj, że jeśli pracujesz w strefie czasowej innej niż lokalizacja urządzenia, przedział czasu jest oparty na strefie czasowej urządzenia.

Encrypt (Szyfruj): ta opcja pozwala skonfigurować hasło do eksportowanych nagrań. Podanie ustawionego hasła będzie konieczne do otworzenia eksportowanego pliku.

Kliknij, aby usunąć nagranie.

Export (Eksportuj): pozwala wyeksportować całe nagranie lub jego fragment.

Kliknij, aby filtrować nagrania.

From (Od): Pokazuje nagrania wykonane po określonym momencie w czasie.

To (Do): Pokazuje nagrania wykonane przed określonym momentem w czasie.

Source (Źródło): Pokazuje nagrania z podziałem na źródła. Źródło odnosi się do czujnika.

Event (Zdarzenie): Pokazuje nagrania z podziałem na zdarzenia.

Pamięć masowa: Pokazuje nagrania z podziałem na typy zasobów.

Aplikacje

Add app (Dodaj aplikację): umożliwia zainstalowanie nowej aplikacji.

Find more apps (Znajdź więcej aplikacji): pozwala znaleźć więcej aplikacji do zainstalowania. Nastąpi przekierowanie na stronę z opisem aplikacji Axis.

Allow unsigned apps (Zezwalaj na niepodpisane aplikacje) : włączenie tej opcji umożliwi instalowanie niepodpisanych aplikacji.

Allow root-privileged apps (Zezwalaj na aplikacje z uprawnieniami roota) : włączenie tej opcji umożliwi aplikacjom z uprawnieniami roota pełny dostęp do urządzenia.

Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

Aby włączyć lub wyłączyć aplikację, użyj przełącznika znajdującego się obok jej nazwy.

Open (Otwórz): umożliwia uzyskanie dostępu do ustawień aplikacji. Dostępne ustawienia zależą od aplikacji. W niektórych aplikacjach nie ma żadnych ustawień.

Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

- **Open-source license (Licencja open source)**: pozwala wyświetlić informacje o licencjach open source używanych w aplikacji.
- **App log (Dziennik aplikacji)**: pozwala wyświetlić dziennik zdarzeń aplikacji. Dziennik jest pomocny podczas kontaktowania się z pomocą techniczną.
- **Activate license with a key (Aktywuj licencję kluczem)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie nie ma dostępu do Internetu. Jeśli nie masz klucza licencji, przejdź na stronę *axis.com/products/analytics*. Do wygenerowania klucza potrzebny będzie kod licencyjny oraz numer seryjny produktu Axis.
- **Activate license automatically (Aktywuj licencję automatycznie)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie ma dostęp do Internetu. Do aktywowania licencji konieczny jest kod.
- **Deactivate the license (Dezaktywuj licencję)**: Aby zastąpić obecną licencję inną licencją, np. w przypadku przejścia z wersji próbnej na pełną, musisz wyłączyć obecną licencję. Jeśli dezaktywujesz licencję, zostanie ona również usunięta z urządzenia.
- **Ustawienia**: Ta opcja umożliwia konfigurowanie parametrów.
- **Usuń**: Ta opcja powoduje trwałe usunięcie aplikacji z urządzenia. Jeśli najpierw nie dezaktywujesz licencji, pozostanie ona aktywna.

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

Synchronization (Synchronizacja): pozwala wybrać opcję synchronizacji daty i godziny urządzenia.

- **Automatyczna data i godzina (ręczne serwery NTS KE)**: Synchronizacja z serwerami bezpiecznych kluczy NTP podłączonym do serwera DHCP.
  - **Ręczne serwery NTS KE**: Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Automatyczna data i godzina (serwery NTP z protokołem DHCP)**: Synchronizacja z serwerami NTP podłączonymi do serwera DHCP.
  - **Zapasowe serwery NTP**: Wprowadź adres IP jednego lub dwóch serwerów zapasowych.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Automatyczna data i godzina (ręczne serwery NTP)**: Opcja ta umożliwia synchronizowanie z wybranymi serwerami NTP.
  - **Ręczne serwery NTP**: Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
  - **Max NTP poll time (Maks. czas zapytania NTP)**: Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP)**: Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Custom date and time (Niestandardowa data i godzina)**: Ustaw datę i godzinę ręcznie. Kliknij polecenie **Get from system (Pobierz z systemu)** w celu pobrania ustawień daty i godziny z komputera lub urządzenia przenośnego.

Strefa czasowa: Wybierz strefę czasową. Godzina zostanie automatycznie dostosowana względem czasu letniego i standardowego.

- **DHCP**: Stosuje strefę czasową serwera DHCP. Aby można było wybrać tę opcję, urządzenie musi być połączone z serwerem DHCP.
- **Manual (Ręcznie)**: Wybierz strefę czasową z listy rozwijanej.

Uwaga

System używa ustawień daty i godziny we wszystkich nagraniach, dziennikach i ustawieniach systemowych.

Lokalizacja urządzenia

Wprowadź lokalizację urządzenia. System zarządzania materiałem wizyjnym wykorzysta tę informację do umieszczenia urządzenia na mapie.

- **Format (Formatuj)**: Wybierz format, który ma być używany podczas wprowadzania szerokości i długości geograficznej urządzenia.
- **Latitude (Szerokość geograficzna)**: Wartości dodatnie to szerokość geograficzna na północ od równika.
- **Longitude (Długość geograficzna)**: Wartości dodatnie to długość geograficzna na wschód od południka zerowego.
- **Kierunek**: Wprowadź kierunek (stronę świata), w który skierowane jest urządzenie. 0 to północ.
- **Etykieta**: Wprowadź opisową nazwę urządzenia.
- **Save (Zapisz)**: Kliknij, aby zapisać lokalizację urządzenia.

Ustawienia regionalne

Wybierz system jednostek stosowany we wszystkich ustawieniach systemu.

Metric (m, km/h) (Metryczny (m, km/h)): wybierz tę opcję, aby odległość była podawana w metrach, a prędkość w kilometrach na godzinę.

U.S. customary (ft, mph) (Amerykański (ft, mph)): wybierz tę opcję, aby odległość była podawana w stopach, a prędkość w milach na godzinę.

Sieć

IPv4

Przypisz automatycznie IPv4: wybierz, aby router sieciowy automatycznie przypisywał adres IP do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresu IP (DHCP) dla większości sieci.

Adres IP: wprowadź unikatowy adres IP dla urządzenia. Statyczne adresy IP można przydzielać losowo w sieciach izolowanych, pod warunkiem że adresy są unikatowe. Aby uniknąć występowania konfliktów, zalecamy kontakt z administratorem sieci przed przypisaniem statycznego adresu IP.

Maska podsieci: Otwórz maskę podsieci, aby określić adresy w sieci lokalnej. Wszystkie adresy poza siecią lokalną przechodzą przez router.

Router: wprowadź adres IP domyślnego routera (bramki) używanego do łączenia z urządzeniami należącymi do innych sieci i segmentów sieci.

Fallback to static IP address if DHCP isn't available (Jeśli DHCP jest niedostępny, zostanie ono skierowane do statycznego adresu IP): Wybierz, czy chcesz dodać statyczny adres IP, który ma być używany jako rezerwa, jeśli usługa DHCP jest niedostępna i nie można automatycznie przypisać adresu IP.

Uwaga

Jeśli protokół DHCP jest niedostępny, a urządzenie korzysta z adresu rezerwowego dla adresu statycznego, adres statyczny jest skonfigurowany w zakresie ograniczonym.

IPv6

Przypisz IPv6 automatycznie: Włącz IPv6, aby router sieciowy automatycznie przypisywał adres IP do urządzenia.

Nazwa hosta

Przypisz automatycznie nazwę hosta: Wybierz, aby router sieciowy automatycznie przypisywał nazwę hosta do urządzenia.

Nazwa hosta: Wprowadź ręcznie nazwę hosta, aby zapewnić alternatywny dostęp do urządzenia. W raporcie serwera i dzienniku systemowym jest używana nazwa hosta. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

Włącz aktualizacje dynamiczne DNS: Zezwól urządzeniu na automatyczne aktualizowanie rekordów serwera nazw domen, gdy zmieni się jego adres IP.

Zarejestruj nazwę DNS: Wprowadź unikatową nazwę domeny, która wskazuje adres IP urządzenia. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

TTL: Time to Live (TTL) to ustawienie określające, jak długo rekord DNS zachowuje ważność, zanim trzeba go zaktualizować.

Serwery DNS

Przypisz automatycznie DNS: Wybierz ustawienie, aby serwer DHCP automatycznie przypisywał domeny wyszukiwania i adresy serwerów DNS do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresów DNS (DHCP) dla większości sieci.

Przeszukaj domeny: jeżeli używasz nazwy hosta, która nie jest w pełni kwalifikowana, kliknij **Add search domain (Dodaj domenę wyszukiwania)** i wprowadź domenę, w której ma być wyszukiwana nazwa hosta używana przez urządzenie.

Serwery DNS: kliknij polecenie **Add DNS server (Dodaj serwer DNS)** i wprowadź adres IP podstawowego serwera DNS. Powoduje to przełożenie nazw hostów na adresy IP w sieci.

HTTP i HTTPS

HTTPS to protokół umożliwiający szyfrowanie żądań stron wysyłanych przez użytkowników oraz stron zwracanych przez serwer sieci Web. Zaszyfrowana wymiana informacji opiera się na użyciu certyfikatu HTTPS, który gwarantuje autentyczność serwera.

Warunkiem używania protokołu HTTPS w urządzeniu jest zainstalowanie certyfikatu HTTPS. Przejdź do menu **System > Zabezpieczenia**, aby utworzyć i zainstalować certyfikaty.

Zezwalaj na dostęp przez: wybierz, czy użytkownik może połączyć się z urządzeniem za pośrednictwem protokołów **HTTP**, **HTTPS** lub obu.

Uwaga

W przypadku przeglądania zaszyfrowanych stron internetowych za pośrednictwem protokołu HTTPS może wystąpić spadek wydajności, zwłaszcza przy pierwszym żądaniu strony.

HTTP port (Port HTTP): wprowadź wykorzystywany port HTTP. urządzenie pozwala na korzystanie z portu 80 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

HTTPS port (Port HTTPS): wprowadź wykorzystywany port HTTPS. urządzenie pozwala na korzystanie z portu 443 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

Certificate (Certyfikat): wybierz certyfikat, aby włączyć obsługę protokołu HTTPS w tym urządzeniu.

Protokoły wykrywania sieci

Bonjour®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

Nazwa Bonjour: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.

UPnP®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

Nazwa UPnP: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.

WS-Discovery: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

LLDP and CDP (LLDP i CDP): Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci. Wyłączenie funkcji LLDP and CDP może wpływać na negocjowanie zasilania z PoE. Aby rozwiązać ewentualne problemy negocjowania zasilania z PoE, należy skonfigurować przełącznik PoE tylko do sprzętowej negocjacji zasilania PoE.

Globalne serwery proxy

Http proxy (Serwer proxy HTTP): Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.

Https proxy (Serwer proxy HTTPS): Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.

Dozwolone formaty serwerów proxy HTTP i HTTPS:

- http(s)://host:port
- http(s)://użytkownik@host:port
- http(s)://użytkownik:pass@host:port

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

No proxy (Brak serwera proxy): Użyj opcji **No proxy (Brak serwera proxy)**, aby pominąć globalne serwery proxy. Wprowadź jedną z opcji na liście lub kilka opcji rozdzielonych przecinkami:

- Pozostaw puste
- Określ adres IP
- Określ adres IP w formacie CIDR
- Określ nazwę domeny, na przykład: www.<nazwa domeny>.com
- Określ wszystkie poddomeny w określonej domenie, na przykład .<nazwa domeny>.com

One-click cloud connection (Łączenie w chmurze jednym kliknięciem)

Usługa One-Click Cloud Connect (O3C) w połączeniu z systemem AVHS zapewnia łatwe i bezpieczne połączenie z internetem w celu uzyskania dostępu do obrazów wideo w czasie rzeczywistym oraz zarejestrowanych obrazów z dowolnej lokalizacji. Więcej informacji: *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Zezwalaj na O3C):

- **Jednym kliknięciem**: Jest to domyślne ustawienie. Naciśnij i przytrzymaj przycisk Control na urządzeniu, aby połączyć się z usługą O3C przez Internet. Urządzenie należy zarejestrować w serwisie O3C w ciągu 24 godzin od naciśnięcia przycisku kontrolnego. W przeciwnym razie urządzenie zakończy połączenie z usługą O3C. Po zarejestrowaniu urządzenia opcja **Always (Zawsze)** jest włączona, a urządzenie zostaje połączone z usługą O3C.
- **Zawsze**: Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenie zostaje połączone z usługą O3C. Opcji tej należy używać wtedy, gdy przycisk kontrolny na urządzeniu jest niedostępny.
- **Nie**: wyłącza usługę O3C.

Proxy settings (Ustawienia proxy): W razie potrzeby należy wprowadzić ustawienia proxy, aby połączyć się z serwerem proxy.

Host: Wprowadź adres serwera proxy.

Port: wprowadź numer portu służącego do uzyskania dostępu.

Login i **Hasło**: W razie potrzeby wprowadź nazwę użytkownika i hasło do serwera proxy.

Authentication method (Metoda uwierzytelniania):

- **Zwykła**: Ta metoda jest najbardziej zgodnym schematem uwierzytelniania HTTP. Jest ona mniej bezpieczna niż metoda **Digest (Szyfrowanie)**, ponieważ nazwa użytkownika i hasło są wysyłane do serwera w postaci niezaszyfrowanej.
- **Szyfrowanie**: ta metoda jest bezpieczniejsza, ponieważ zawsze przesyła hasło w sieci w formie zaszyfrowanej.
- **Automatycznie**: ta opcja umożliwia urządzeniu wybór metody uwierzytelniania w zależności od obsługiwanych metod. Priorytet ma metoda **Szyfrowanie**; w dalszej kolejności stosowana jest metoda **Zwykła**.

Owner authentication key (OAK) (Klucz uwierzytelniania właściciela (OAK)): Kliknij **Get key (Uzyskaj klucz)**, aby pobrać klucz uwierzytelniania właściciela. Warunkiem jest podłączone urządzenia do Internetu bez użycia zapory lub serwera proxy.

SNMP

Protokół zarządzania urządzeniami sieciowymi Simple Network Management Protocol (SNMP) umożliwia zdalne zarządzanie urządzeniami sieciowymi.

SNMP: Wybierz wersję SNMP.

- **v1 and v2c (v1 i v2c)**:
  - **Read community (Społeczność odczytu)**: wprowadź nazwę społeczności, która ma dostęp tylko do odczytu do wszystkich obsługiwanych obiektów SNMP. Wartość domyślna to **publiczna**.
  - **Write community (Społeczność zapisu)**: wprowadź nazwę społeczności, która ma dostęp do odczytu/zapisu do wszystkich obsługiwanych obiektów SNMP (poza obiektami tylko do odczytu). Wartość domyślna to **zapis**.
  - **Activate traps (Uaktywnij pułapki)**: włącz, aby uaktywnić raportowanie pułapek. Urządzenie wykorzystuje pułapki do wysyłania do systemu zarządzania komunikatów o ważnych zdarzeniach lub zmianach stanu. W interfejsie WWW urządzenia można skonfigurować pułapki dla SNMP v1 i v2c. Pułapki są automatycznie wyłączane w przypadku przejścia na SNMP v3 lub wyłączenia SNMP. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Trap address (Adres pułapki)**: Wprowadzić adres IP lub nazwę hosta serwera zarządzania.
  - **Trap community (Społeczność pułapki)**: Wprowadź nazwę społeczności używanej, gdy urządzenie wysyła komunikat pułapki do systemu zarządzającego.
  - **Traps (Pułapki)**:
    - **Cold start (Zimny rozruch)**: wysyła komunikat pułapkę po uruchomieniu urządzenia.
    - **Ciepły rozruch**: wysyła komunikat pułapkę w przypadku zmiany ustawienia SNMP.
    - **Link up (Łącze w górę)**: wysyła komunikat pułapkę po zmianie łącza w górę.
    - **Niepowodzenie uwierzytelniania**: wysyła komunikat pułapkę po niepowodzeniu próby uwierzytelnienia.

Uwaga

Wszystkie pułapki Axis Video MIB są włączone po włączeniu pułapek SNMP v1 i v2c. Więcej informacji: *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 to bezpieczniejsza wersja, zapewniająca szyfrowanie i bezpieczne hasła. Aby używać SNMP v3, zalecane jest włączenie protokołu HTTPS, który posłuży do przesłania hasła. Zapobiega to również dostępowi osób nieupoważnionych do niezaszyfrowanych pułapek SNMP v1 i v2c. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Password for the account "initial" (Hasło do konta „wstępnego")**: wprowadź hasło SNMP dla konta o nazwie „initial" (wstępne). Chociaż hasło może być wysłane bez aktywacji HTTPS, nie zalecamy tego. Hasło SNMP v3 można ustawić tylko raz i najlepiej tylko po aktywacji HTTPS. Po ustawieniu hasła pole hasła nie jest już wyświetlane. Aby zresetować hasło, należy zresetować urządzenie do ustawień fabrycznych.

Bezpieczeństwo

Certyfikaty

Certyfikaty służą do uwierzytelniania urządzeń w sieci. Urządzenie obsługuje dwa typy certyfikatów:

- **Certyfikaty serwera/klienta**
  Certyfikat serwera/klienta potwierdza numer urządzenia i może mieć własny podpis lub podpis jednostki certyfikującej (CA). Certyfikaty z własnym podpisem oferują ograniczoną ochronę i można je wykorzystywać do momentu uzyskania certyfikatu CA.
- **Certyfikaty CA**
  Certyfikaty CA mogą służyć do uwierzytelniania innych certyfikatów, na przykład tożsamości serwera uwierzytelniającego w przypadku połączenia urządzenia z siecią zabezpieczoną za pomocą IEEE 802.1X. Urządzenie ma kilka zainstalowanych wstępnie certyfikatów CA.

Obsługiwane są następujące formaty:

- Formaty certyfikatów: .PEM, .CER i .PFX
- Formaty kluczy prywatnych: PKCS#1 i PKCS#12

Ważne

W przypadku przywrócenia na urządzeniu ustawień fabrycznych wszystkie certyfikaty są usuwane. Wstępnie zainstalowane certyfikaty CA są instalowane ponownie.

Add certificate (Dodaj certyfikat) : Kliknij, aby dodać certyfikat.

- **More (Więcej)** : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Secure element (Zabezpieczony element)** lub **Trusted Platform Module 2.0 (Moduł TPM 2.0)** do bezpiecznego przechowywania klucza prywatnego. Aby uzyskać więcej informacji na temat bezpiecznego magazynu kluczy, odwiedź stronę *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Typ klucza)**: Aby zabezpieczyć certyfikat, wybierz domyślny algorytm szyfrowania lub inny z listy rozwijanej.

Menu kontekstowe zawiera opcje:

- **Dane certyfikatu**: Wyświetl właściwości zainstalowanego certyfikatu.
- **Delete certificate (Usuń certyfikat)**: Umożliwia usunięcie certyfikatu.
- **Create certificate signing request (Utwórz żądanie podpisania certyfikatu)**: Umożliwia utworzenie żądanie podpisania certyfikatu w celu przekazania go do urzędu rejestracyjnego i złożenia wniosku o wydanie certyfikatu tożsamości cyfrowej.

Secure keystore (Bezpieczny magazyn kluczy) :

- **Bezpieczny element (CC EAL6+)**: Wybierz, aby używać bezpiecznego elementu do bezpiecznego magazynu kluczy.
- **Moduł TPM 2.0 (CC EAL4+, FIPS 140-2 poziom 2)**: Wybierz, aby używać modułu TPM 2.0 do bezpiecznego magazynu kluczy.

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1x

IEEE 802.1x to standard IEEE dla kontroli dostępu sieciowego opartej na portach, zapewniający bezpieczne uwierzytelnianie przewodowych i bezprzewodowych urządzeń sieciowych. IEEE 802.1x jest oparty na protokole EAP (Extensible Authentication Protocol).

Aby uzyskać dostęp do sieci zabezpieczonej IEEE 802.1x, urządzenia sieciowe muszą dokonać uwierzytelnienia. Do uwierzytelnienia służy serwer, zazwyczaj RADIUS, taki jak FreeRADIUS i Microsoft Internet Authentication Server.

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec jest standardem IEEE dotyczącym adresu MAC, który definiuje bezpołączeniową poufność i integralność danych dla protokołów niezależnych od dostępu do nośników.

Certyfikaty

W przypadku konfiguracji bez certyfikatu CA, sprawdzanie poprawności certyfikatów serwera jest wyłączone, a urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.

Podczas korzystania z certyfikatu w instalacjach firmy Axis urządzenie i serwer uwierzytelniający używają do uwierzytelniania certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Aby zezwolić urządzeniu na dostęp do sieci chronionej za pomocą certyfikatów, w urządzeniu musi być zainstalowany podpisany certyfikat klienta.

Authentication method (Metoda uwierzytelniania): Wybierz typ protokołu EAP na potrzeby uwierzytelniania.

Client certificate (Certyfikat klienta): wybierz certyfikat klienta, aby użyć IEEE 802.1x. Serwer uwierzytelniania używa certyfikatu do weryfikacji tożsamości klienta.

Certyfikaty CA: wybierz certyfikaty CA w celu potwierdzania tożsamości serwera uwierzytelniającego. Jeśli nie wybrano żadnego certyfikatu, urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.

EAP identity (Tożsamość EAP): wprowadź tożsamość użytkownika powiązaną z certyfikatem klienta.

EAPOL version (Wersja protokołu EAPOL): wybierz wersję EAPOL używaną w switchu sieciowym.

Use IEEE 802.1x (Użyj IEEE 802.1x): wybierz, aby użyć protokołu IEEE 802.1 x.

Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą **IEEE 802.1x PEAP-MSCHAPv2**:

- **Hasło**: Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap)**: wybierz wersję Peap używaną w switchu sieciowym.
- **Etykieta**: 1 pozwala używać szyfrowania EAP klienta; 2 pozwala używać szyfrowania PEAP klienta. Wybierz etykietę używaną przez przełącznik sieciowy podczas korzystania z wersji 1 protokołu Peap.

Te ustawienia są dostępne wyłącznie w przypadku uwierzytelniania za pomocą **IEEE 802.1ae MACsec (klucz CAK/PSK)**:

- **Nazwa klucza skojarzenia łączności umowy klucza**: Wprowadź nazwę skojarzenia łączności (CKN). Musi to być od 2 do 64 (podzielnych przez 2) znaków szesnastkowych. CKN musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.
- **Klucz skojarzenia łączności umowy klucza**: Wprowadź klucz skojarzenia łączności (CAK). Musi mieć 32 lub 64 znaki szesnastkowe. CAK musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.

Zapobiegaj atakom typu brute force

Blocking (Blokowanie): włącz, aby blokować ataki typu brute force Ataki typu brute-force wykorzystują metodę prób i błędów do odgadnięcia danych logowania lub kluczy szyfrowania.

Blocking period (Okres blokowania): Wprowadź liczbę sekund, w ciągu których ataki typu brute-force mają być blokowane.

Blocking conditions (Warunki blokowania): wprowadź dopuszczalną liczbę nieudanych prób uwierzytelnienia na sekundę przed rozpoczęciem blokowania. Liczbę dopuszczalnych niepowodzeń można ustawić zarówno na stronie, jak i w urządzeniu.

Zapora

Activate (Aktywuj): Włącz zaporę sieciową.

Domyślne ustawienia zasad: Wybierz stan domyślny zapory.

- **Allow (Zezwalaj):** Zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **Deny: (Odrzuć)** Odrzuca wszystkie połączenia z urządzeniem.

Aby wprowadzić wyjątki od domyślnych zasad, można utworzyć reguły, które zezwalają lub nie zezwalają na łączenie się z urządzeniem z określonych adresów, protokołów i portów.

- **Adres**: Wprowadź adres w formacie IPv4/IPv6 lub CIDR, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Protocol (Protokół)**: Wybierz protokół, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Port**: Wprowadź numer portu, w przypadku którego dostęp ma być dozwolony lub niedozwolony. Podaj numer portu od 1 do 65535.
- **Policy (Zasada)**: Wybierz zasadę dla reguły.

+ : Kliknij, aby utworzyć nową regułę.

Add rules: (Dodaj reguły) Kliknij tę opcję, aby dodać zdefiniowane reguły.

- **Time in seconds: (Czas w sekundach)** Pozwala ustawić limit czasu testowania reguł. Domyślny limit czasu to 300 sekund. Jeśli chcesz od razu aktywować reguły, ustaw czas 0 sekund.
- **Confirm rules (Potwierdzenie reguł):** Potwierdź reguły i ich limit czasowy. W przypadku ustawienia limitu czasu dłuższego niż 1 sekunda reguły będą aktywne przez ten czas. Jeśli ustawiono czas 0, reguły będą aktywowane od razu.

Pending rules (Oczekujące reguły): Omówienie ostatnio testowanych reguł, które jeszcze nie zostały potwierdzone.

Uwaga

Reguły z limitem czasu są widoczne w obszarze **Active rules (Aktywne reguły)**, aż upłynie czas ustawiony w czasomierzu lub nastąpi ich potwierdzenie. Jeśli nie zostaną potwierdzone, po upłynięciu czasu ustawionego w czasomierzu, pojawią się w menu **Pending rules (Oczekujące reguły)**, i zostaną przywrócone wcześniejsze ustawienia zapory. Jeśli reguły zostaną potwierdzone, zastąpią one bieżące aktywne reguły.

Confirm rules (Potwierdzenie reguł): Kliknięcie tej opcji aktywuje oczekujące reguły.

Active rules (Aktywne reguły): Omówienie reguł obecnie stosowanych w urządzeniu.

: Kliknięcie tej opcji pozwala usunąć aktywną regułę.

: Kliknięcie tej opcji pozwala usunąć wszystkie oczekujące i aktywne reguły.

Niestandardowy podpisany certyfikat systemu AXIS OS

Do zainstalowania w urządzeniu oprogramowania testowego lub innego niestandardowego oprogramowania Axis konieczny jest niestandardowy podpisany certyfikat systemu AXIS OS. Certyfikat służy do sprawdzenia, czy oprogramowanie jest zatwierdzone zarówno przez właściciela urządzenia, jak i przez firmę Axis. Oprogramowanie działa tylko na określonym urządzeniu z niepowtarzalnym numerem seryjnym i identyfikatorem procesora. Niestandardowe podpisane certyfikaty systemu AXIS OS mogą być tworzone tylko przez firmę Axis, ponieważ Axis posiada klucze do ich podpisywania.

Zainstaluj: Kliknij przycisk Install (Instaluj), aby zainstalować certyfikat. Certyfikat musi zostać zainstalowany przed zainstalowaniem oprogramowania.

Menu kontekstowe zawiera opcje:

- **Delete certificate (Usuń certyfikat)**: Umożliwia usunięcie certyfikatu.

Konta

Konta

Add account (Dodaj konto): Kliknij, aby dodać nowe konto. Można dodać do 100 kont.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

Nowe hasło: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.

Repeat password (Powtórz hasło): Wprowadź ponownie to samo hasło.

Privileges (Przywileje):

- **Administrator**: Ma nieograniczony dostęp do wszystkich ustawień. Administrator może tez dodawać, aktualizować i usuwać inne konta.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
- **Viewer (Dozorca)**: Nie może zmieniać ustawień.

Menu kontekstowe zawiera opcje:

Update account (Zaktualizuj konto): Pozwala edytować właściwości konta.

Delete account (Usuń konto): Pozwala usunąć konto. Nie można usunąć konta root.

Anonimowy dostęp

Allow anonymous viewing (Zezwalaj na anonimowe wyświetlanie): Włączenie tej opcji pozwala wszystkim osobom uzyskać dostęp do urządzenia jako dozorca bez logowania się za pomocą konta.

Allow anonymous PTZ operating (Zezwalaj na anonimową obsługę PTZ) : Jeśli włączysz tę opcję, anonimowi użytkownicy będą mogli obracać, przechylać i powiększać/zmniejszać obraz.

Konta SSH

Add SSH account (Dodaj konto SSH): Kliknij, aby dodać nowe konto SSH.

- **Restrict root access (Ogranicz dostęp do konta root)**: Włącz, aby ograniczyć funkcjonalność wymagającą dostępu root.
- **Enable SSH (Włącz SSH)**: Włącz, aby korzystać z usługi SSH.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

Nowe hasło: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.

Repeat password (Powtórz hasło): Wprowadź ponownie to samo hasło.

Uwaga: Wprowadź komentarz (opcjonalnie).

Menu kontekstowe zawiera opcje:

Update SSH account (Zaktualizuj konto SSH): Pozwala edytować właściwości konta.

Delete SSH account (Usuń konto SSH): Pozwala usunąć konto. Nie można usunąć konta root.

Virtual host (Host wirtualny)

Add virtual host (Dodaj host wirtualny): kliknięcie tej opcji pozwala dodać nowego wirtualnego hosta.

Włączony: zaznaczenie tej opcji spowoduje używanie tego wirtualnego hosta.

Server name (Nazwa serwera): w tym polu można wpisać nazwę serwera. Używaj tylko cyfr 0-9, liter A-Z i łącznika (-).

Port: w tym polu należy podać port, z którym jest połączony serwer.

Type (Typ): pozwala wybrać typ poświadczenia, które ma być używane. Dostępne są opcje **Basic (Podstawowe)**, **Digest (Szyfrowane)** oraz **Open ID (Otwarte ID)**.

Menu kontekstowe zawiera opcje:

- **Update (Aktualizuj)**: Zaktualizuj wirtualnego hosta.
- **Usuń**: Usuń wirtualnego hosta.

Disabled (Wyłączono): Serwer jest wyłączony.

Konfiguracja OpenID

Ważne

Jeśli nie udaje się zalogować za pomocą OpenID, użyj poświadczeń Digest lub Basic, które zostały użyte podczas konfigurowania OpenID.

Client ID (Identyfikator klienta): Wprowadź nazwę użytkownika OpenID.

Outgoing Proxy (Wychodzący serwer proxy): Aby używać serwera proxy, wprowadź adres serwera proxy dla połączenia OpenID.

Admin claim (Przypisanie administratora): Wprowadź wartość roli administratora.

Provider URL (Adress URL dostawcy): Wprowadź łącze internetowe do uwierzytelniania punktu końcowego interfejsu programowania aplikacji (API). Łącze musi mieć format https://[wstaw URL]/.well-known/openid-configuration

Operator claim (Przypisanie operatora): Wprowadź wartość roli operatora.

Require claim (Wymagaj przypisania): Wprowadź dane, które powinny być dostępne w tokenie.

Viewer claim (Przypisanie dozorcy): Wprowadź wartość dla roli dozorcy.

Remote user (Użytkownik zdalny): Wprowadź wartość identyfikującą użytkowników zdalnych. Pomoże to wyświetlić bieżącego użytkownika w interfejsie WWW urządzenia.

Scopes (Zakresy): Opcjonalne zakresy, które mogą być częścią tokenu.

Client secret (Tajny element klienta): Wprowadź hasło OpenID.

Save (Zapisz): Kliknij, aby zapisać wartości OpenID.

Enable OpenID (Włącz OpenID): Włącz tę opcję, aby zamknąć bieżące połączenie i zezwolić na uwierzytelnianie urządzenia z poziomu adresu URL dostawcy.

Zdarzenia

Reguły

Reguła określa warunki wyzwalające w urządzeniu wykonywanie danej akcji. Na liście znajdują się wszystkie reguły skonfigurowane w produkcie.

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.

Nazwa: Wprowadź nazwę reguły.

Wait between actions (Poczekaj między działaniami): Wprowadź minimalny czas (w formacie gg:mm:ss), jaki musi upłynąć między aktywacjami reguły. Ustawienie to jest przydatne, gdy reguła jest aktywowana na przykład warunkami trybów dziennego i nocnego, ponieważ zapobiega niepożądanemu uruchamianiu reguły przez niewielkie zmiany natężenia światła podczas wschodu i zachodu słońca.

Condition (Warunek): Wybierz warunek z listy. Dopiero po spełnieniu tego warunku urządzenie wykona akcję. Jeśli określono wiele warunków, to do wyzwolenia działania konieczne jest spełnienie wszystkich z nich. Informacje na temat konkretnych warunków można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Use this condition as a trigger (Użyj tego warunku jako wyzwalacza): Zaznacz tę opcję, aby ten pierwszy warunek działał tylko jako wyzwalacz początkowy. Oznacza to, że po aktywacji reguła pozostanie czynna przez cały czas, gdy są spełniane wszystkie pozostałe warunki, bez względu na stan pierwszego warunku. Jeżeli nie zaznaczysz tej opcji, reguła będzie aktywna po spełnieniu wszystkich warunków.

Invert this condition (Odwróć ten warunek): Zaznacz tę opcję, jeśli warunek ma być przeciwieństwem dokonanego przez Ciebie wyboru.

Add a condition (Dodaj warunek): Kliknij, aby dodać kolejny warunek.

Action (Akcja): Wybierz akcję z listy i wprowadź jej wymagane informacje. Informacje na temat konkretnych akcji można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Odbiorcy

W urządzeniu można skonfigurować powiadamianie odbiorców o zdarzeniach lub wysyłanie plików.

Uwaga

W przypadku skonfigurowania urządzenia do korzystania z protokołu FTP lub SFTP nie należy zmieniać ani usuwać unikatowego numeru sekwencyjnego dodawanego do nazw plików. Jeśli zostało to zrobione, można wysłać tylko jeden obraz na zdarzenie.

Na liście wyświetlani są wszyscy odbiorcy skonfigurowani dla produktu, a także informacje dotyczące ich konfiguracji.

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

Add a recipient (Dodaj odbiorcę): Kliknij, aby dodać odbiorcę.

Nazwa: Wprowadź nazwę odbiorcy.

Type (Typ): Wybierz z listy:

- **FTP**
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer FTP. Domyślny port to 21.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze FTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.
  - **Use passive FTP (Użyj pasywnego FTP)**: W normalnych warunkach produkt po prostu wysyła żądanie otwarcia połączenia do serwera FTP. Urządzenie inicjuje przesyłanie danych na serwer docelowy i kontrolę serwera FTP. Jest to zazwyczaj konieczne w przypadku zapory ogniowej pomiędzy urządzeniem a serwerem FTP.
- **HTTP**
  - **URL**: Wprowadź adres sieciowy serwera HTTP oraz skrypt obsługujący żądanie. Na przykład: http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTP.
- **HTTPS**
  - **URL**: Wprowadź adres sieciowy serwera HTTPS oraz skrypt obsługujący żądanie. Na przykład: https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Potwierdź certyfikat serwera)**: Zaznacz tę opcję, aby sprawdzić certyfikat utworzony przez serwer HTTPS.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTPS.
- **Sieciowa pamięć masowa**
  Umożliwia dodanie takiego zasobu sieciowego, jak NAS (sieciowy zasób dyskowy), i wykorzystywanie go jako odbiorcy plików. Pliki zapisywane są w formacie Matroska (MKV).

- **Host**: Wprowadź adres IP lub nazwę hosta serwera pamięci sieciowej.
- **Udział**: Podaj nazwę współdzielonego udziału na serwerze hosta.
- **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki.
- **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
- **Hasło**: Wprowadź hasło logowania.

- SFTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer SFTP. Domyślny port to 22.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze SFTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (MD5)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 32 cyfr w szesnastkowym systemie liczbowym). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (SHA256)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 43 cyfr w systemie kodowania Base64). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.

- SIP or VMS (SIP lub VMS) :
  SIP: Wybierz w celu nawiązania połączenia SIP.
  VMS: Wybierz w celu nawiązania połączenia VMS.
  - **From SIP account (Z konta SIP)**: Wybierz z listy.
  - **To SIP address (Na adres SIP)**: Wprowadź adres SIP.
  - **Test (Testuj)**: Kliknij, aby sprawdzić, czy ustawienia połączeń działają prawidłowo.
- E-mail

- **Wyślij wiadomość e-mail do**: Wprowadź adresy odbiorców. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
- **Wyślij e-mail przez**: Wprowadź adres serwera nadawcy.
- **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Hasło**: Wprowadź hasło dostępu do serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Email server (SMTP) (Serwer poczty e-mail (SMTP))**: Wprowadź nazwę serwera SMTP, na przykład smtp.gmail.com, smtp.mail.yahoo.com.
- **Port**: wprowadź numer portu serwera SMTP, używając wartości z zakresu 0–65535. Wartość domyślna to 587.
- **Szyfrowanie**: Aby używać szyfrowania, wybierz opcję SSL lub TLS.
- **Validate server certificate (Potwierdź certyfikat serwera)**: Jeżeli używasz szyfrowania, zaznacz tę opcję, aby weryfikować tożsamość urządzenia. Certyfikat może mieć własny podpis lub podpis jednostki certyfikującej (CA).
- **POP authentication (Uwierzytelnianie POP)**: Włącz tę opcję i wprowadź nazwę serwera POP, na przykład pop.gmail.com.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużej liczby załączników, odbieranie wiadomości cyklicznych itp. Aby zapobiec zablokowaniu konta lub usunięciu wiadomości, należy sprawdzić regulamin zabezpieczeń dostawcy usług.

- **TCP**
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu dostępowego serwera.

Test (Testuj): Kliknij, aby przetestować konfigurację.

⋮ Menu kontekstowe zawiera opcje:

View recipient (Pokaż odbiorcę): Kliknij, aby wyświetlić wszystkie dane odbiorcy.

Copy recipient (Kopiuj odbiorcę): Kliknij, aby skopiować odbiorcę. Po skopiowaniu odbiorcy można wprowadzić zmiany w nowym wpisie odbiorcy.

Delete recipient (Usuń odbiorcę): Kliknij, aby trwale usunąć odbiorcę.

Harmonogramy

Harmonogramów i zdarzeń jednorazowych można użyć jako warunków reguł. Na liście wyświetlane są wszystkie harmonogramy i zdarzenia jednorazowe skonfigurowane dla produktu, a także informacje dotyczące ich konfiguracji.

+ **Add schedule (Dodaj harmonogram)**: Kliknij, aby utworzyć harmonogram lub impuls.

Wyzwalacze ręczne

Wyzwalacz manualny służy do ręcznego wyzwalania reguły. Wyzwalacza manualnego można na przykład użyć do walidacji akcji podczas instalacji i konfiguracji produktu.

MQTT

MQTT (przesyłanie telemetryczne usługi kolejkowania wiadomości) to standardowy protokół do obsługi komunikacji w Internecie rzeczy (IoT). Został zaprojektowany z myślą o uproszczeniu integracji IoT i jest wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji objętości kodu i obciążenia sieci. Klient MQTT w oprogramowaniu urządzeń Axis może ułatwiać integrację danych i zdarzeń generowanych w urządzeniu z systemami, które nie są oprogramowaniem do zarządzania materiałem wizyjnym (VMS).

Konfiguracja urządzenia jako klienta MQTT. Komunikacja MQTT oparta jest na dwóch jednostkach, klientach i brokerze. Klienci mogą wysyłać i odbierać wiadomości. Broker odpowiedzialny jest za rozsyłanie wiadomości między klientami.

Więcej informacji o protokole MQTT znajdziesz w *portalu poświęconym systemowi AXIS OS*.

ALPN

ALPN to rozszerzenie TLS/SSL umożliwiające wybranie protokołu aplikacji na etapie uzgadniania połączenia między klientem a serwerem. Służy do włączania ruchu MQTT przez port używany przez inne protokoły, takie jak HTTP. Czasami może nie być dedykowanego portu otwartego dla komunikacji MQTT. W takich przypadkach pomocne może być korzystanie z ALPN do negocjowania użycia MQTT jako protokołu aplikacji na standardowym porcie akceptowanym przez zapory sieciowe.

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.

Status (Stan): pokazuje bieżący status klienta MQTT.

Broker

Host: wprowadź nazwę hosta lub adres IP serwera MQTT.

Protocol (Protokół): wybór protokołu, który ma być używany.

Port: Wprowadź numer portu.

- 1883 to wartość domyślna ustawienia **MQTT over TCP (MQTT przez TCP)**
- 8883 to wartość domyślna dla **MQTT przez SSL**
- 80 to wartość domyślna dla **MQTT przez WebSocket**
- 443 to wartość domyślna dla **MQTT przez WebSocket Secure**

ALPN protocol (Protokół ALPN): Wprowadź nazwę protokołu ALPN dostarczoną przez dostawcę brokera MQTT. Dotyczy to tylko ustawień MQTT przez SSL i MQTT przez WebSocket Secure.

Username (Nazwa użytkownika): należy tu wprowadzić nazwę użytkownika, która będzie umożliwiać klientowi dostęp do serwera.

Hasło: wprowadzić hasło dla nazwy użytkownika.

Client ID (Identyfikator klienta): wprowadź identyfikator klienta. Identyfikator klienta jest wysyłany do serwera w momencie połączenia klienta.

Clean session (Czysta sesja): steruje zachowaniem w czasie połączenia i czasie rozłączenia. Po wybraniu tej opcji informacje o stanie są odrzucane podczas podłączania i rozłączania.

HTTP proxy (Serwer proxy HTTP): Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTP, możesz zostawić to pole puste.

HTTPS proxy (Serwer proxy HTTPS): Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTPS, możesz zostawić to pole puste.

Keep alive interval (Przedział czasowy KeepAlive) Umożliwia klientowi detekcję, kiedy serwer przestaje być dostępny, bez konieczności oczekiwania na długi limit czasu TCP/IP.

Timeout (Przekroczenie limitu czasu): interwał czasowy (w sekundach) pozwalający na zakończenie połączenia. Wartość domyślna: 60

Prefiks tematu urządzenia: Używany w domyślnych wartościach tematu w komunikacie łączenia i komunikacie LWT na karcie **MQTT client (Klient MQTT)** oraz w warunkach publikowania na karcie **MQTT publication (Publikacja MQTT)**.

Reconnect automatically (Ponowne połączenie automatyczne): określa, czy klient powinien ponownie połączyć się automatycznie po rozłączeniu.

Komunikat łączenia

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

Send message (Wysłanie wiadomości): włącz, aby wysyłać wiadomości.

Use default (Użyj domyślnych): wyłącz, aby wprowadzić własną wiadomość domyślną.

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

Retain (Zachowaj): wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

QoS: zmiana warstwy QoS dla przepływu pakietów.

Wiadomość Ostatnia Wola i Testament

Funkcja Last Will Testament (LWT) zapewnia klientowi dostarczenie informacji wraz z poświadczeniami w momencie łączenia się z brokerem. Jeżeli klient nie rozłączy się w pewnym momencie w późniejszym terminie (może to być spowodowane brakiem źródła zasilania), może umożliwić brokerowi dostarczenie komunikatów do innych klientów. Ten komunikat LWT ma taką samą postać jak zwykła wiadomość i jest kierowany przez tę samą mechanikę.

Send message (Wysłanie wiadomości): włącz, aby wysyłać wiadomości.

Use default (Użyj domyślnych): wyłącz, aby wprowadzić własną wiadomość domyślną.

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

Retain (Zachowaj): wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

QoS: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

Użyj domyślnego prefiksu: Wybierz ustawienie, aby używać domyślnego prefiksu zdefiniowanego za pomocą prefiksu urządzenia w zakładce **MQTT client (Klient MQTT)**.

Dołącz nazwę tematu: Wybierz, aby do tematu MQTT dołączać tematy opisujące warunek.

Dołącz nazwy przestrzenne tematu: Wybierz, aby do tematu MQTT dołączać przestrzenie nazw tematów ONVIF.

Include serial number (Uwzględnij numer seryjny): Wybierz, aby w danych właściwych usługi MQTT umieszczać numer seryjny urządzenia.

Add condition (Dodaj warunek): Kliknij, aby dodać warunek.

Retain (Zachowaj): Definiuje, które komunikaty MQTT mają być wysyłane jako zachowywane.

- **Brak**: Wysyłanie wszystkich komunikatów jako niezachowywanych.
- **Property (Właściwość)**: Wysyłanie tylko komunikatów ze stanem jako zachowywanych.
- **All (Wszystkie)**: Wysyłanie komunikatów ze stanem i bez stanu jako zachowywanych.

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

Add subscription (Dodaj subskrypcję): Kliknij, aby dodać nową subskrypcję usługi MQTT.

Subscription filter (Filtr subskrypcyjny): Wprowadź temat MQTT, który chcesz subskrybować.

Use device topic prefix (Użyj prefiksu tematu urządzenia): Dodaj filtr subskrypcji jako prefiks do tematu MQTT.

Subscription type (Typ subskrypcji):

- **Stateless (Bez stanu)**: Wybierz, aby przekształcać komunikaty MQTT na komunikaty bezstanowe.
- **Stateful (Ze stanem)**: Wybierz, aby przekształcać komunikaty MQTT na warunek. Dane właściwe będą służyły do określania stanu.

QoS: Wybierz żądany poziom subskrypcji MQTT.

Nałożenia MQTT

Uwaga

Zanim będzie można dodawać modyfikatory nakładek MQTT, należy ustanowić połączenie z brokerem MQTT.

Add overlay modifier (Dodaj modyfikator nałożenia): Kliknij, aby dodać nowy modyfikator nakładki.

Topic filter (Filtr tematów): Dodaj temat MQTT zawierający dane, które mają być pokazywane w nakładce.

Data field (Pole danych): Wprowadź klucz danych właściwych komunikatu, które mają być wyświetlane w nakładce, zakładając, że komunikat jest w formacie JSON.

Modifier (Modyfikator): Używanie utworzonego modyfikatora podczas tworzenia nakładki.

- Modyfikatory rozpoczynające się ciągiem znaków **#XMP** pokazują wszystkie dane otrzymane z tematu.
- Modyfikatory rozpoczynające się ciągiem znaków **#XMD** pokazują dane wprowadzone w polu danych.

Przechowywanie

Sieciowa pamięć masowa

Ignore (Ignoruj): włączenie tej opcji będzie powodowało ignorowanie zasobów pamięci sieciowej.

Add network storage (Dodaj zasób sieciowy): Kliknij tę opcję w celu dodania udziału sieciowego, w którym będziesz zapisywać nagrania.

- **Adres**: Wprowadź adres IP lub nazwę serwera hosta. Zazwyczaj jest nim NAS (sieciowy zasób dyskowy). Zalecamy skonfigurowanie hosta tak, aby używał stałego adresu IP (nie DHCP, ponieważ dynamiczne adresy IP mogą się zmienić) albo używanie DNS. Nazwy Windows SMB/CIFS nie są obsługiwane.
- **Network share (Udział sieciowy)**: Podaj nazwę współdzielonego udziału na serwerze hosta. Z jednego udziału sieciowego może korzystać kilka urządzeń Axis, ponieważ każde z nich ma swój folder.
- **User (Użytkownik)**: Jeżeli serwer wymaga logowania, wprowadź nazwę użytkownika. W celu zalogowania się do konkretnego serwera domeny wprowadź `domenę azwę użytkownika`.
- **Hasło**: Jeżeli serwer wymaga logowania, podaj hasło.
- **SMB version (Wersja SMB)**: Wybierz wersję protokołu pamięci masowej SMB, który będzie używany do łączenia z sieciowym zasobem dyskowym. Jeżeli wybierzesz opcję **Auto (Automatycznie)**, urządzenie będzie próbowało użyć jednej z bezpiecznych wersji protokołu SMB: 3.02, 3.0 lub 2.1. Wybierz opcję 1.0 lub 2.0, aby łączyć ze starszymi sieciowymi zasobami dyskowymi, które nie obsługują wyższych wersji. Więcej informacji o obsłudze protokołu SMB w urządzeniach Axis znajdziesz *tutaj*.
- **Add share without testing (Dodaj udział bez testowania)**: Wybierz tę opcję, aby dodać udział sieciowy, nawet jeżeli podczas testu połączenia zostanie wykryty błąd. Błąd może wynikać na przykład z niepodania hasła, podczas gdy serwer go wymaga.

Remove network storage (Usuń sieciową pamięć masową): Kliknij tę opcję w celu odinstalowania, odpięcia i usunięcia połączenia z udziałem sieciowym. Spowoduje to usunięcie wszystkich ustawień udziału sieciowego.

Unbind (Odepnij): Kliknięcie tej opcji spowoduje odpięcie i odłączenie udziału sieciowego.
Bind (Powiąż): kliknięcie tej opcji spowoduje powiązanie i połączenie udziału sieciowego.

Odmontuj: Kliknięcie tej opcji spowoduje odmontowanie udziału sieciowego.
Mount (Zamontuj): kliknięcie tej opcji spowoduje zamontowanie udziału sieciowego.

Write protect (Zabezpieczenie przed zapisem): Włącz tę opcję, aby uniemożliwić zapis w udziale sieciowym i zabezpieczyć nagrania przed usunięciem. Nie można formatować udziału sieciowego zabezpieczonego przed zapisem.

Retention time (Czas przechowywania): Wybierz, jak długo nagrania mają być przechowywane, aby ograniczyć liczbę starych nagrań lub ze względu na zachowanie zgodności z regulacjami w sprawie przechowywania danych. Zapełnienie zasobu sieciowego spowoduje usunięcie starych nagrań przed upływem wybranego czasu.

Narzędzia

- **Test connection (Test połączenia)**: Opcja ta służy do sprawdzenia połączenia z udziałem sieciowym.
- **Format (Formatuj)**: Istnieje możliwość sformatowania udziału sieciowego, np., gdy chcesz szybko usunąć wszystkie dane. CIFS jest dostępną opcją systemu plików.

Use tool (Użyj narzędzia): Kliknij, aby aktywować wybrane narzędzie.

Pamięć pokładowa

Ważne

Ryzyko utraty danych i uszkodzenia nagrań. Nie wyjmuj karty SD, gdy urządzenie działa. Odłącz kartę SD przed jej usunięciem.

Odmontuj: Kliknij w celu bezpiecznego usunięcia karty SD.

Write protect (Zabezpieczenie przed zapisem): Włącz, aby uniemożliwić zapis na karcie SD i zabezpieczyć zapisy przed usunięciem. Nie można formatować kart SD zabezpieczonych przed zapisem.

Autoformat (Automatyczne formatowanie): Włącz, aby automatycznie formatować nowo włożoną kartę SD. Powoduje to formatowanie systemu plików do ext4.

Ignore (Ignoruj): Włączenie tej opcji powoduje zaprzestanie przechowywania nagrań na karcie SD. Jeżeli zignorujesz kartę SD, urządzenie nie będzie jej rozpoznawać. Z tego ustawienia mogą korzystać tylko administratorzy.

Retention time (Czas przechowywania): Wybierz, jak długo mają być przechowywane nagrania, aby ograniczyć liczbę starych nagrań lub zachować zgodność z regulacjami z zakresu przechowywania danych. Zapełnienie karty SD powoduje usuwanie starych nagrań przed upływem czasu ich przechowywania.

Narzędzia

- **Check (Sprawdź)**: Opcja ta umożliwia wykrycie błędów na karcie SD.
- **Napraw**: Opcja ta umożliwia naprawę błędów w systemie plików.
- **Format (Formatuj)**: Opcja ta umożliwia sformatowanie karty SD w celu zmiany systemu plików i usunięcia wszystkich danych. Kartę SD można sformatować tylko w systemie plików ext4. W celu uzyskania dostępu do danych na karcie z poziomu systemu Windows® należy zainstalować sterownik lub aplikację ext4 innego producenta.
- **Encrypt (Szyfruj)**: To narzędzie umożliwia sformatowanie karty SD i włączenie szyfrowania. Powoduje to usunięcie wszystkich danych znajdujących się na karcie SD. Wszelkie nowe dane zapisane na karcie SD zostaną zaszyfrowane.
- **Decrypt (Odszyfruj)**: To narzędzie pozwala sformatować kartę SD bez szyfrowania. Powoduje to usunięcie wszystkich danych znajdujących się na karcie SD. Wszelkie nowe dane zapisane na karcie SD nie zostaną zaszyfrowane.
- **Change password (Zmień hasło)**: Umożliwia zmianę hasła wymaganego do szyfrowania karty SD.

Use tool (Użyj narzędzia): Kliknij, aby aktywować wybrane narzędzie.

Wear trigger (Wyzwalacz reakcji na zużycie): Ustaw wartość poziomu zużycia karty SD, przy którym ma być wyzwalana akcja. Poziom zużycia może się mieścić w przedziale od 0 do 200%. Nowa karta SD, która nigdy nie była używana, ma poziom zużycia równy 0%. Poziom zużycia w 100% wskazuje, że kończy się przewidywany okres przydatności użytkowej karty. Gdy poziom zużycia osiągnie 200%, istnieje wysokie ryzyko nieprawidłowego działania karty SD. Zalecamy ustawienie wartości wyzwalacza zużycia w zakresie od 80 do 90%. Zapewni to czas na pobranie wszystkich potrzebnych nagrań i wymianę karty, zanim zużyje się ona w nadmiernym stopniu. Funkcja wyzwalacza zużycia pozwala skonfigurować zdarzenie, a następnie otrzymać powiadomienie, że karta zużyła się w określonym stopniu.

Profile strumienia

Profil strumienia to grupa ustawień wpływających na strumień wideo. Profili strumieni można używać w różnych sytuacjach, na przykład podczas tworzenia zdarzeń oraz rejestrowania za pomocą reguł.

Add stream profile (Dodaj profil strumienia): Kliknij to polecenie w celu utworzenia nowego profilu strumienia.

Preview (Podgląd): Podgląd strumienia wideo z wybranymi ustawieniami profilu strumienia. Zmiana ustawień na stronie powoduje aktualizowanie podglądu. Jeśli urządzenie ma różne obszary obserwacji, aktywny obszar obserwacji można zmienić w menu rozwijanym w lewym dolnym rogu obrazu.

Nazwa: Nadaj profilowi nazwę.

Description (Opis): Dodaj opis profilu.

Video codec (Kodek wideo): Wybierz kodek wideo, który ma być stosowany w profilu.

Rozdzielczość: Opis tego ustawienia znajduje się w temacie .

Frame rate (Liczba klatek na sekundę): Opis tego ustawienia znajduje się w temacie .

Compression (Kompresja): Opis tego ustawienia znajduje się w temacie .

Zipstream : Opis tego ustawienia znajduje się w temacie .

Optimize for storage (Optymalizacja pod kątem pamięci masowej) : Opis tego ustawienia znajduje się w temacie .

Dynamic FPS (Dynamiczna liczba klatek na sekundę) : Opis tego ustawienia znajduje się w temacie .

Dynamic GOP (Dynamiczna grupa obrazów) : Opis tego ustawienia znajduje się w temacie .

Mirror (Odbicie lustrzane) : Opis tego ustawienia znajduje się w temacie .

GOP length (Długość grupy obrazów) : Opis tego ustawienia znajduje się w temacie .

Bitrate control (Kontrola przepływności bitowej): Opis tego ustawienia znajduje się w temacie .

Include overlays (Uwzględnij nałożenia) : Wybierz typ nakładek, jakie mają być dołączane. Informacje o dodawaniu nakładek znajdują się w temacie .

Include audio (Dołącz audio) : Opis tego ustawienia znajduje się w temacie .

ONVIF

Konta ONVIF

ONVIF (Open Network Video Interface Forum) to międzynarodowy standard interfejsu, który ułatwia użytkownikom końcowym, integratorom, konsultantom i producentom wykorzystanie możliwości oferowanych przez technologie sieciowe. ONVIF zapewnia zgodność operacyjną miedzy urządzeniami różnych producentów, zwiększa elastyczność systemu, zmniejsza jego koszty i upraszcza obsługę.

Utworzenie konta ONVIF powoduje automatyczne włączenie komunikacji ONVIF. Nazwy konta i hasła należy używać podczas komunikacji ONVIF z urządzeniem. Więcej informacji znajduje się na stronach dla programistów Axis Developer Community w witrynie *axis.com*.

Add accounts (Dodaj konta): Kliknij, aby dodać nowe konto ONVIF.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

Nowe hasło: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.

Repeat password (Powtórz hasło): Wprowadź ponownie to samo hasło.

Rola:

- **Administrator**: Ma nieograniczony dostęp do wszystkich ustawień. Administrator może tez dodawać, aktualizować i usuwać inne konta.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
  - Dodawanie aplikacji.
- **Media account (Konto multimediów)**: Dostęp wyłącznie do strumienia wideo.

Menu kontekstowe zawiera opcje:

Update account (Zaktualizuj konto): Pozwala edytować właściwości konta.

Delete account (Usuń konto): Pozwala usunąć konto. Nie można usunąć konta root.

Profile mediów ONVIF

Profil mediów ONVIF składa się z zestawu konfiguracji, które można wykorzystać do zmiany ustawień strumienia mediów. Możesz tworzyć nowe profile z własnym zestawem konfiguracji lub używać wstępnie skonfigurowanych profili do szybkiego ustawienia funkcji.

Add media profile (Dodaj profil mediów): Kliknij, aby dodać nowy profil ONVIF.

Profile name (Nazwa profilu): Dodaj nazwę profilu multimediów.

Video source (Źródło wideo): Wybierz źródło wideo dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika. Konfiguracje na liście rozwijanej odpowiadają kanałom wideo urządzenia, w tym widokom wieloobrazowym, obszarom obserwacji i kanałom wirtualnym.

Video encoder (Wideoenkoder): Wybierz format kodowania wideo dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia kodowania. Konfiguracje na liście rozwijanej pełnią rolę identyfikatorów/nazw konfiguracji wideoenkodera. Wybierz użytkownika od 0 do 15, aby zastosować własne ustawienia, lub wybierz jednego z użytkowników domyślnych, aby użyć wstępnie zdefiniowanych ustawień dla określonego formatu kodowania.

Uwaga

Aby uzyskać dostęp do opcji wyboru źródła dźwięku i konfiguracji enkodera audio, włącz dźwięk w urządzeniu.

Audio source (Źródło audio) : Wybierz źródło sygnału wejściowego audio dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia audio. Konfiguracje na liście rozwijanej odpowiadają wejściom audio urządzenia. Jeśli urządzenie ma jedno wejście audio, będzie ono oznaczone jako „user0". Jeżeli w urządzeniu jest kilka wejść audio, na liście pojawi się odpowiadająca im liczba użytkowników.

Audio encoder (Audioenkoder) : Wybierz format kodowania audio dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia kodowania audio. Konfiguracje na liście rozwijanej pełnią rolę identyfikatorów/nazw konfiguracji wideoenkodera audio.

Audio decoder (Audiodekoder) : Wybierz format dekodowania audio dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia. Konfiguracje na liście rozwijanej pełnią rolę identyfikatorów/nazw konfiguracji.

Audio output (Wyjście audio) : Wybierz format wyjścia audio dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia. Konfiguracje na liście rozwijanej pełnią rolę identyfikatorów/nazw konfiguracji.

Metadata (Metadane): Wybierz metadane, które chcesz uwzględnić w konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj metadanych Konfiguracje na liście rozwijanej pełnią rolę identyfikatorów/nazw konfiguracji metadanych.

PTZ : Wybierz ustawienia PTZ dla swojej konfiguracji.

- **Select configuration (Wybierz konfigurację)**: Wybierz z listy konfigurację zdefiniowaną przez użytkownika i skonfiguruj ustawienia PTZ. Konfiguracje na liście rozwijanej odpowiadają kanałom wideo urządzenia z obsługą PTZ.

Create (Utwórz): Kliknij tę opcję, aby zapisać ustawienia i utworzyć profil.

Cancel (Anuluj): Kliknij tę opcję, aby anulować konfigurację i wyzerować wszystkie ustawienia.

profile_x (profil_x): Kliknij nazwę profilu, aby otworzyć i edytować wstępnie skonfigurowany profil.

Detektory

Wykrywanie wstrząsów

Shock detector (Detektor wstrząsów): Włącz, aby generować alarm, jeśli urządzenie zostanie uderzone przez przedmiot lub ktoś będzie przy nim manipulował.

Sensitivity level (Poziom czułości): Przesuń suwak, aby wyregulować poziom czułości, przy którym urządzenie powinno generować alarm. Niska wartość sprawi, że urządzenie będzie generować alarm tylko po mocnym uderzeniu. Przy wysokiej wartości urządzenie będzie generować alarm nawet w reakcji na delikatne manipulowanie.

Akcesoria

Porty we/wy

Użyj wejścia cyfrowego do podłączenia zewnętrznych urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okien lub drzwi oraz czujników wykrywania zbicia szyby.

Użyj wyjścia cyfrowego do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączone urządzenia można aktywować poprzez interfejs programowania aplikacji VAPIX® lub w interfejsie WWW.

Port

Nazwa: edytuj tekst, aby zmienić nazwę portu.

Direction (Kierunek):  oznacza, że port jest portem wejścia.  oznacza, że jest to port wyjścia. Jeśli port jest konfigurowalny, można kliknąć ikony, aby przełączać się między wejściem a wyjściem.

Normal state (Stan normalny): Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.

Current state (Bieżący stan): wyświetla bieżący stan portu. Wejście lub wyjście jest aktywowane w momencie zmiany bieżącego stanu na inny niż stan normalny. Obwód wejścia urządzenia jest otwarty po odłączeniu lub po doprowadzeniu napięcia powyżej 1 V DC.

Uwaga

Podczas ponownego uruchomienia obwód pozostaje otwarty. Po ponownym uruchomieniu obwód powraca do pozycji normalnej. Po zmianie ustawień na tej stronie obwody wyjść powracają do normalnych pozycji, niezależnie od aktywnych wyzwalaczy.

Supervised (Nadzorowane)  : włącz, aby umożliwić wykrywanie i wyzwalanie działań, jeśli ktoś manipuluje przy połączeniu z cyfrowymi urządzeniami We/Wy. Oprócz wykrywania, czy wejście jest otwarte lub zamknięte, można również wykryć, czy ktoś przy nim manipulował (tzn. przeciął lub doprowadził do zwarcia). Nadzorowanie połączenia wymaga dodatkowego sprzętu (rezystorów końcowych) w zewnętrznej pętli We./Wy.

Edge-to-edge

parowanie

Parowanie pozwala korzystać ze zgodnego urządzenia Axis tak, jakby było ono wbudowane w urządzenie główne.

Parowanie audio umożliwia sparowanie z głośnikiem sieciowym lub mikrofonem. Po sparowaniu głośnik sieciowy działa jako urządzenie audio, które umożliwia odtwarzanie klipów audio i przesyłanie dźwięku za pośrednictwem kamery. Mikrofon sieciowy zbiera dźwięki z otoczenia i udostępnia je jako urządzenie wejściowe audio, wykorzystywane w strumieniach multimediów i zapisach.

Ważne

Aby ta funkcja mogła współpracować z oprogramowaniem do zarządzania materiałem wizyjnym (VMS), trzeba najpierw sparować kamerę z głośnikiem lub mikrofonem, a następnie dodać kamerę do systemu VMS.

W przypadku używania sparowanego urządzenia audio w regule zdarzenia z warunkiem „Audio detection" (Detekcja dźwięku) i akcją „Play audio clip" (Odtwórz klip audio), ustaw limit „Wait between actions (hh:mm:ss)" (Oczekiwanie między akcjami (gg:mm:ss) w regule zdarzeń. Pomoże to uniknąć wykrywania zapętlenia, jeśli mikrofon przechwytujący odbiera dźwięk z głośnika.

Dodaj: Dodaj urządzenie do sparowania.

Wybierz typ parowania: Wybierz z listy rozwijanej.

Speaker pairing (Parowanie głośnika): Wybranie tej opcji pozwala sparować głośnik sieciowy.

Microphone pairing (Parowanie mikrofonu) : Wybranie tej opcji pozwala sparować mikrofon.

Adres: Wprowadź nazwę hosta lub adres IP głośnika sieciowego.

Username (Nazwa użytkownika): Wprowadź nazwę użytkownika.

Hasło: Wprowadź hasło dla użytkownika.

Zamknij: Kliknij, aby usunąć zawartość wszystkich pól.

Connect (Połącz): Kliknij, aby nawiązać połączenie z urządzeniem do sparowania.

Funkcja **PTZ pairing (Parowania PTZ)** pozwala sparować radar i kamerę PTZ w celu korzystania z automatycznego śledzenia. Funkcja automatycznego śledzenia ruchu radaru uruchamia śledzenie przez kamerę PTZ obiektów według danych o ich pozycjach przekazanych przez radar.

Dodaj: Dodaj urządzenie do sparowania.

Select pairing type (Wybierz typ parowania): Wybierz z listy rozwijanej.

Adres: Wprowadź nazwę hosta lub adres IP kamery PTZ.

Username (Nazwa użytkownika): Wprowadź nazwę użytkownika kamery PTZ.

Hasło: Wprowadź hasło do kamery PTZ.

Zamknij: Kliknij, aby usunąć zawartość wszystkich pól.

Connect (Połącz): Kliknij, aby nawiązać połączenie z kamerą PTZ.

Configure radar autotracking (Skonfiguruj automatyczne śledzenie w radarze): Kliknij, aby otworzyć i skonfigurować automatyczne śledzenie ruchu. Tę opcję można też skonfigurować w menu **Radar > Radar PTZ autotracking (Radar > Automatyczne śledzenie PTZ)**.

Dzienniki

Raporty i dzienniki

Raporty

- **Wyświetl raport serwera o urządzeniu**: Opcja ta pozwala wyświetlić informacje o stanie produktu w wyskakującym oknie. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.
- **Download the device server report (Pobierz raport serwera o urządzeniu)**: Opcja ta powoduje utworzenie pliku ZIP, który zawiera pełny raport serwera w pliku tekstowym w formacie UTF–8 oraz migawkę bieżącego podglądu na żywo. Podczas kontaktowania się z pomocą techniczną zawsze dodawaj plik zip raportu serwera.
- **Download the crash report (Pobierz raport o awarii)**: Pobierz archiwum ze szczegółowymi informacjami o stanie serwera. Raport o awarii zawiera informacje znajdujące się w raporcie o serwerze oraz szczegółowe dane pomocne w usuwaniu błędów. W raporcie tym mogą się znajdować informacje poufne, np. ślady sieciowe. Wygenerowanie raportu może potrwać kilka minut.

Dzienniki

- **View the system log (Wyświetl dziennik systemu)**: Kliknij tutaj, aby wyświetlić informacje o zdarzeniach systemowych, takich jak uruchamianie urządzenia, ostrzeżenia i komunikaty krytyczne.
- **Wyświetl dziennik dostępu**: Kliknij tutaj, by wyświetlić wszystkie nieudane próby uzyskania dostępu do urządzenia, na przykład gdy użyto nieprawidłowego hasła logowania.

Zdalny dziennik systemu

Dziennik systemowy to standard rejestracji komunikatów. Umożliwia on oddzielenie oprogramowania, które generuje komunikaty, systemu przechowującego je i oprogramowania, które je raportuje i analizuje. Każdy komunikat jest oznaczany etykietą z kodem obiektu wskazującym typ oprogramowania, które wygenerowało komunikat, oraz przypisany poziom ważności.

 **Server (Serwer)**: Kliknij, aby dodać nowy serwer.

Host: Wprowadź nazwę hosta lub adres IP serwera.

Format (Formatuj): Wybierz format komunikatu dziennika systemowego, który ma być używany.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protokół): Wybierz protokołu, który ma być używany:

- UDP (port domyślny to 514)
- TCP (port domyślny to 601)
- TLS (port domyślny to 6514)

Port: Wpisywanie innego numeru portu w miejsce obecnego.

Severity (Ciężkość): Zdecyduj, które komunikaty będą wysyłane po wyzwoleniu.

CA certificate set (Certyfikat CA ustawiony): Umożliwia wyświetlenie aktualnych ustawień lub dodanie certyfikatu.

Zwykła konfiguracja

Opcja zwykłej konfiguracji przeznaczona jest dla zaawansowanych użytkowników, którzy mają doświadczenie w konfigurowaniu urządzeń Axis. Na stronie tej można skonfigurować i edytować większość parametrów.

Konserwacja

Konserwacja

Restart (Uruchom ponownie): Uruchom ponownie urządzenie. Nie wpłynie to na żadne bieżące ustawienia. Uruchomione aplikacje zostaną ponownie uruchomione automatycznie.

Restore (Przywróć): Opcja ta umożliwia przywrócenie większości domyślnych ustawień fabrycznych. Następnie konieczne jest ponowne skonfigurowanie urządzeń i aplikacji, zainstalowanie aplikacji, które nie zostały wstępnie zainstalowane, a także ponowne utworzenie wszystkich zdarzeń i wstępnych ustawień.

Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

- protokół uruchamiania (DHCP lub stały adres),
- statyczny adres IP,
- Router domyślny
- Maska podsieci
- ustawienia 802.1X.
- Ustawienia O3C
- Adres IP serwera DNS

Ustawienia fabryczne: Przywróć wszystkie ustawienia do domyślnych wartości fabrycznych. Po zakończeniu tej operacji konieczne będzie zresetowanie adresu IP w celu uzyskania dostępu do urządzenia.

Uwaga

Wszystkie składniki oprogramowania urządzenia firmy Axis posiadają podpisy cyfrowe zapewniające, że na urządzeniu będzie instalowane wyłącznie zweryfikowane oprogramowanie. To dodatkowo zwiększa minimalny ogólny poziom cyberbezpieczeństwa urządzeń Axis. Więcej informacji znajduje się w oficjalnym dokumencie „Axis Edge Vault" dostępnym na *axis.com*.

Uaktualnianie systemu AXIS OS: Umożliwia uaktualnienie do nowej wersji AXIS OS. Nowe wersje mogą zawierać udoskonalenia działania i poprawki błędów oraz zupełnie nowe funkcje. Zalecamy, aby zawsze korzystać z najnowszej wersji systemu AXIS OS. Aby pobrać najnowsza wersję, odwiedź stronę *axis.com/support*.

Po uaktualnieniu masz do wyboru trzy opcje:

- **Standard upgrade (Aktualizacja standardowa)**: Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **Ustawienia fabryczne**: Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej wersji systemu AXIS OS.
- **Autorollback (Automatyczne przywrócenie wersji)**: Uaktualnij i potwierdź uaktualnienie w ustawionym czasie. Jeżeli nie potwierdzisz, w urządzeniu zostanie przywrócona poprzednia wersja systemu AXIS OS.

Przywracanie systemu AXIS OS: Przywróć poprzednio zainstalowaną wersję systemu AXIS OS.

Rozwiązywanie problemów

Reset PTR (Resetuj PTR) : Opcji Reset PTR (Resetuj PTR) należy użyć w sytuacji, gdy z jakiegoś powodu ustawienia **Pan (Obrót)**, **Tilt (Pochylenie)** i **Roll (Przechylenie)** nie działają w oczekiwany sposób. W nowej kamerze silniczki układu PTR są zawsze skalibrowane. Jednak kalibracja może zostać utracona, na przykład w razie odcięcia zasilania kamery lub ręcznego przestawienia kamery w którymś kierunku. Po zresetowaniu ustawień PTR kamera jest ponownie kalibrowana i wraca do położenia fabrycznego.

Calibrate (Kalibruj) : Kliknij **Calibrate (Kalibruj)**, aby zrekalibrować silniki obrotu, pochylenia i przechylenia do pozycji domyślnych.

Ping: Aby sprawdzić, czy określony adres jest dostępny dla urządzenia, wprowadź nazwę lub adres IP hosta, do którego chcesz wysłać polecenie ping, i kliknij **Start (Uruchom)**.

Port check (Kontrola portu): Aby zweryfikować łączność urządzenia z określonym adresem IP i portem TCP/UDP, wprowadź nazwę hosta lub adres IP i numer portu, które chcesz sprawdzić, a następnie kliknij **Start (Uruchom)**.

Ślad sieciowy

Ważne

Plik śladu sieciowego może zawierać dane poufne, takie jak certyfikaty lub hasła.

Plik śladu sieciowego, rejestrujący aktywność w sieci, może pomóc w rozwiązywaniu problemów.

Trace time (Czas śledzenia): Wybierz czas trwania śledzenia w sekundach lub minutach i kliknij przycisk **Download (Pobierz)**.

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.

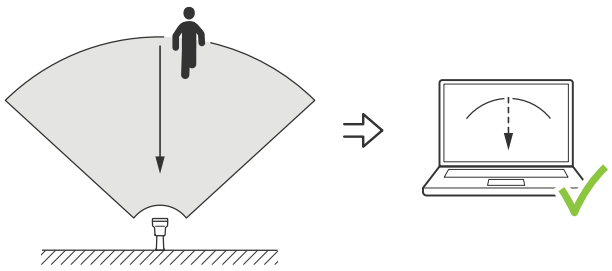
Przed przystąpieniem do sprawdzenia poprawności działania konieczne jest . Następnie wykonaj następujące czynności:

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, pomiń 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 .

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 .
2. Stań w odległości nie większej niż 60 m (196 ft) 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 .
2. Stań w odległości 30 m (98 ft) 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 .
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.

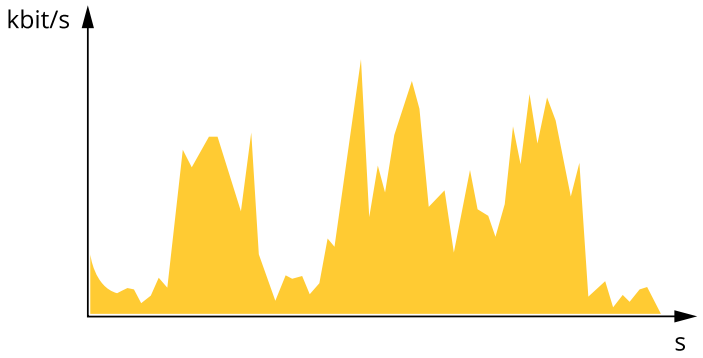
Uwaga

- 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.

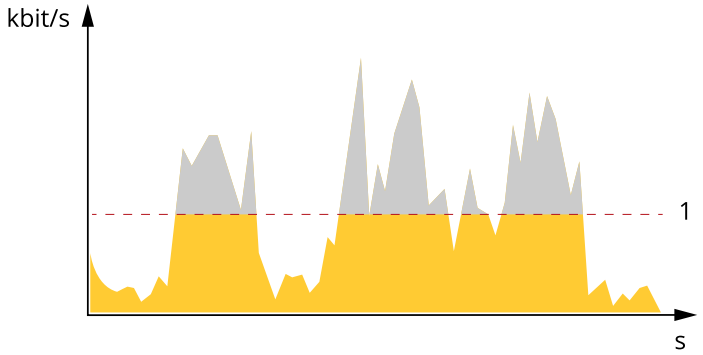
Sterowanie przepływnością bitową

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.



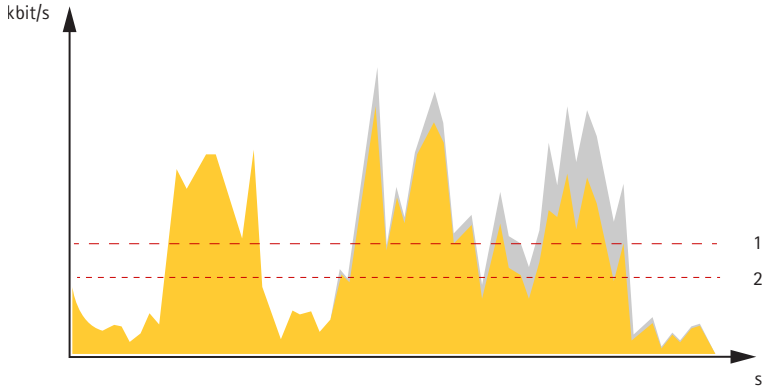
Maksymalna przepływność bitowa (MBR)
Opcja ta umożliwia ustawienie docelowej przepływności bitowej w celu kontrolowania zajętości pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości obrazu lub niższa poklatkowość. Jak priorytet można wybrać 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

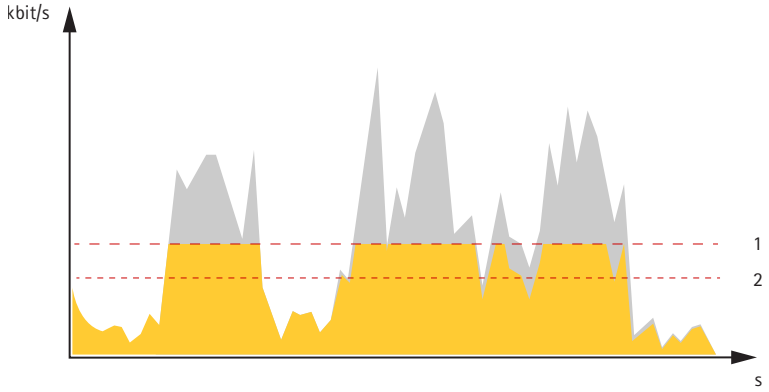
Średnia przepływność bitowa (ABR)
Średnia przepływność bitowa jest dostosowywana automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak najlepszą jakość obrazu wideo przy dostępnych zasobach pamięci masowej. Przepływność bitowa jest wyższa w scenach z 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 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.



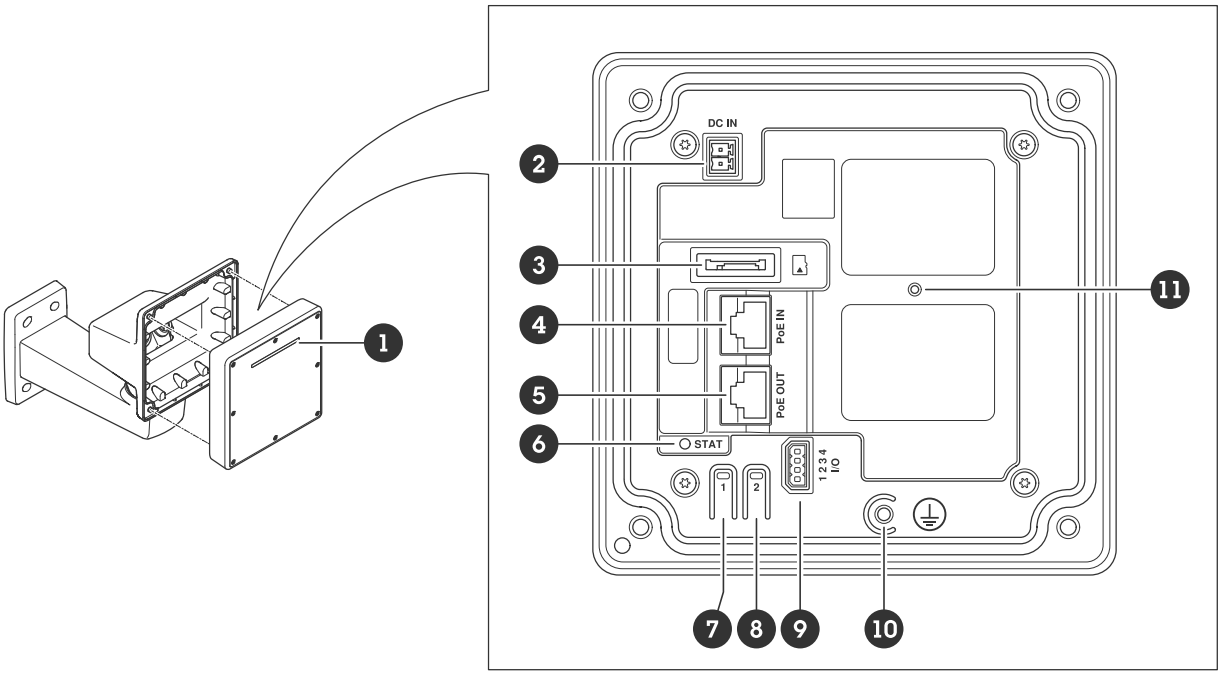
1 *Docel. przepł. bitowa*
2 *Rzeczywista średnia przepływność bitowa*

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.

Specyfikacje

Przegląd produktów



1 *Dynamiczna taśma LED*
2 *Złącze zasilania (DC)*
3 *Gniazdo kart microSD*
4 *Złącze sieciowe (PoE IN)*
5 *Złącze sieciowe (PoE OUT)*
6 *Wskaźnik LED stanu*
7 *Przycisk kontrolny*
8 *Przycisk działania*
9 *Złącze I/O*
10 *Śruba uziemienia*
11 *Przycisk resetowania*

Wskaźniki LED

Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.

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.
Czerwony	Błąd aktualizacji oprogramowania urządzenia.

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 ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz .
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około trzy sekundy, aż dioda LED stanu zacznie migać na zielono.

Złącza

Złącze sieciowe (PoE IN)

Złącze Ethernet RJ45 z zasilaniem Power over Ethernet IEEE 802.3bt, typ 3 klasa 6.

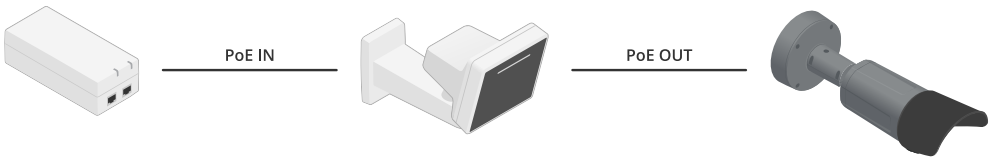
Uwaga

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

Złącze RJ45 Ethernet zapewniające zasilanie Power over Ethernet IEEE 802.3at, typ 2 klasa 4, 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 radaru i urządzeniem. Zasilacz Midspan będzie dostarczał zasilanie do urządzenia, natomiast radar zapewni połączenie z siecią Ethernet.

Złącze I/O

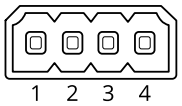
Złącze WE/WY służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze WE/WY zapewnia interfejs do:

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 zbicia szyby.

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

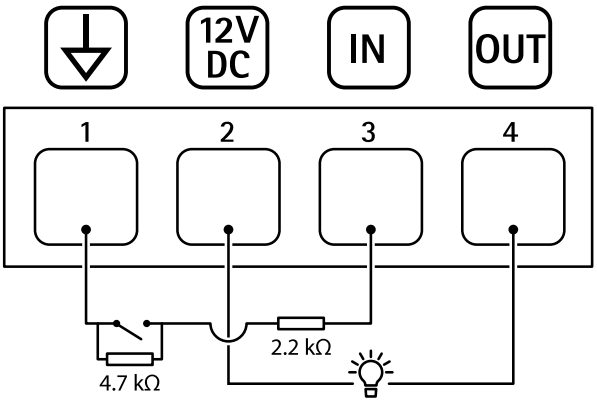
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

4-pinowy blok 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 = 25 mA
Wejścia cyfrowego	3	Podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
Wyjście cyfrowe	4	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

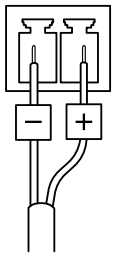
Przykład:



1 *Masa DC*
2 *Wyjście DC 12 V, maks. 25 mA*
3 *Nadzorowane wejście*
4 *Wyjście cyfrowe*

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.



Czyszczenie urządzenia

Urządzenie można czyścić letnią wodą.

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 pozostawanie 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.
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 .
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

- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania urządzenia (pod warunkiem, że funkcje te są dostępne w nowym systemie AXIS OS), choć Axis Communications AB tego nie gwarantuje.
- 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, wskazówki i rozwiązania

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

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	
Urządzenie należy do innej podsieci	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 jest używany przez inne urządzenie	Odłącz urządzenie Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia): • Jeśli otrzymasz odpowiedź: `Reply from <adres IP>: bytes=32; time=10...` oznacza to, że dany adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie. • Jeśli otrzymasz odpowiedź: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
Możliwy konflikt adresów 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.

Nie można uzyskać dostępu do urządzenia przez przeglądarkę	
Nie można zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki. W razie utraty hasła dla konta root należy przywrócić ustawienia fabryczne urządzenia. Patrz .

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 można przydzielić samodzielnie 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)**.

Dostęp do urządzenia można uzyskać lokalnie, ale nie 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 5: 30-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.
- 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*.

Nie można połączyć przez port 8883 z MQTT przez SSL

Zapora blokuje ruch przy użyciu 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.

Kwestie wydajności

Podczas konfiguracji systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na zapotrzebowanie na przepustowość (przepływność bitową).

Najważniejsze czynniki, które należy wziąć pod uwagę:

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

Kontakt z pomocą techniczną

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

T10193646_pl

2025-01 (M13.2)