

Zestaw weryfikacji tablic rejestracyjnych AXIS Q1800- LE-3 License Plate Verifier Kit

Podręcznik użytkownika

Spis treści

Instalacja.....	5
Tryb podglądu.....	5
Od czego zacząć.....	6
Wyszukiwanie urządzenia w sieci.....	6
Obsługiwane przeglądarki.....	6
Otwórz interfejs WWW urządzenia.....	6
Utwórz konto administratora.....	6
Bezpieczne hasła.....	7
Upewnianie się co do braku zmian w oprogramowaniu urządzenia.....	7
Konfiguracja podstawowa.....	8
Zalecenia dotyczące montażu kamery.....	8
Konfigurowanie aplikacji AXIS License Plate Verifier.....	10
Swobodny przepływ.....	10
Uzyskiwanie dostępu do ustawień aplikacji.....	11
Dostosowywanie obszarów zainteresowania.....	11
Wybór regionu.....	12
Dostosowywanie ustawień przechwytywania obrazu.....	12
Konfiguracja przechowywania zdarzeń.....	12
Konfiguracja urządzenia.....	14
Ustawienia podstawowe.....	14
Regulowanie obrazu.....	14
Poziomowanie kamery.....	14
Korzystanie z oświetlenia IR w warunkach słabego oświetlenia (tryb nocny).....	14
Optymalizacja oświetlenia w podczerwieni.....	15
Stabilizacja obrazu za pomocą funkcji stabilizacji obrazu.....	15
Kompensacja dystorsji beczkowatej.....	15
Sprawdzanie rozdzielczości pikseli.....	15
Ukrywanie części obrazu za pomocą masek prywatności.....	16
Wyświetlanie nakładek na obrazie.....	16
Wyświetlanie nakładki tekstu.....	17
Wyświetlanie nałożenia tablic rejestracyjnych.....	17
Dodawanie nazw ulic i kierunku kompasu do obrazu.....	17
Przeglądanie i rejestracja obrazów wideo.....	17
Zmniejszanie zapotrzebowania na przepustowość i zasób.....	17
Konfiguracja zasobów sieciowej pamięci masowej.....	18
Rejestracja i odtwarzanie obrazu.....	18
Sprawdzanie braku sabotażu wideo.....	19
Parowanie kamery z radarem.....	19
Łączenie z sygnalizatorem akustyczno-optycznym.....	19
Konfiguracja reguł dotyczących zdarzeń.....	20
Wyzwalanie akcji.....	20
Oszczędzanie energii, kiedy nie jest wykrywany żaden ruch.....	20
Rejestrowanie obrazu wideo w momencie wykrycia obiektu.....	21
Wyświetlanie nałożenia tekstu w strumieniu wideo, gdy urządzenie wykryje obiekt.....	21
Zapewnianie wizualnej sygnalizacji trwającego zdarzenia.....	22
Rejestrowanie obrazu wideo w momencie wykrycia głośnych dźwięków przez kamerę.....	23
Rejestrowanie obrazu wideo w momencie wykrycia uderzenia przez kamerę.....	23
Wykrywanie ingerencji w sygnał wejściowy.....	24
Automatyczne przysyłanie wiadomości e-mail w przypadku zamalowania obiektywu farbą w sprayu.....	24
Dźwięk.....	25
Dodawanie dźwięku do zapisu.....	25
Łączenie się z głośnikiem sieciowym.....	25

Łączenie się z mikrofonem sieciowym	25
Zarządzanie listami	27
Dodawanie wykrytej tablicy rejestracyjnej do listy	27
Dodawanie opisów do tablic rejestracyjnych	27
Dostosowywanie nazw list	28
Importowanie numerów rejestracyjnych z listy dozwolonych.....	29
Udostępnianie listy tablic rejestracyjnych innym kamerom	30
Tworzenie harmonogramów dla list.....	31
Ustawienia dodatkowe	32
Konfiguracja nakładki tekstowej	32
Detekcja tablic rejestracyjnych przy słabym oświetleniu	32
Dopuszczanie mniejszej liczby znaków na tablicach rejestracyjnych.....	32
Dopasowywanie wyłącznie identycznych tablic rejestracyjnych	32
Zezwalanie na różnicę więcej niż jednego znaku podczas dopasowywania tablic rejestracyjnych	32
Przyznawanie ograniczonego dostępu operatorom	33
Konfiguracja bezpiecznych połączeń	33
Tworzenie kopii zapasowych i przywracanie ustawień aplikacji	33
Kasowanie wszystkich zdarzeń.....	33
Scenariusz wjazdu i wyjazdu pojazdów	34
Powiadomienia dotyczące nieautoryzowanych pojazdów.....	34
Scenariusz swobodnego przepływu z pomiarem prędkości	35
Konfigurowanie scenariusza	35
Wyszukiwanie określonych zdarzeń.....	36
Eksportowanie i udostępnianie wyników wyszukiwania	36
Integracja	37
Używanie profili w celu wysyłania zdarzeń do różnych serwerów.....	37
Komunikat typu push o zdarzeniu przesyłany do oprogramowania innych firm.....	37
Wysłanie obrazu z tablic rejestracyjnych do serwera	38
Bezpośrednia integracja z 2N	39
Integracja z systemem Genetec Security Center.....	39
Interfejs WWW.....	42
Więcej informacji.....	43
Tryby rejestracji.....	43
Funkcja zdalnego ustawiania ostrości i zbliżenia.....	43
Maski prywatności	43
Nakładki.....	43
Strumieniowanie i pamięć masowa	43
Formaty kompresji obrazów wideo.....	43
W jaki sposób ustawienia obrazu, strumienia i profilu strumienia mogą na siebie wpływać?	44
Sterowanie przepływnością bitową.....	44
Technologia edge-to-edge.....	46
Parowanie głośnika	46
Parowanie mikrofonu	46
Parowanie radaru	46
Parowanie sieciowe	47
Analizy i aplikacje	47
AXIS Image Health Analytics.....	47
Wizualizacja metadanych.....	47
Specyfikacje	48
Przegląd produktów.....	48
.....	48
Wskaźniki LED.....	49
Diody LED i brzęczyk asystenta poziomowania	49
Gniazdo karty SD.....	49
Przyciski	49
Przycisk kontrolny.....	49

Przycisk funkcyjny	50
Złącza	50
Złącze sieciowe	50
Złącze audio.....	50
Złącze I/O	50
Złącze zasilania	51
Czyszczenie urządzenia	52
Rozwiązywanie problemów –	53
Przywróć domyślne ustawienia fabryczne	53
Opcje systemu AXIS OS	53
Sprawdzanie bieżącej wersji systemu AXIS OS	53
Aktualizacja systemu AXIS OS:.....	54
Problemy techniczne i możliwe rozwiązania.....	54
.....	57
Kwestie wydajności	57
Kontakt z pomocą techniczną.....	58
Cyberbezpieczeństwo	59
Postępowanie z lukami w zabezpieczeniach	59
Powiadomienia dotyczące zabezpieczeń	59
Bezpieczny cykl eksploatacji produktu	59

Instalacja

Tryb podglądu

Tryb podglądu bardzo przyda się instalatorom podczas dostrajania widoku kamery w trakcie prac montażowych. W tym trybie można uzyskać dostęp do widoku kamery bez konieczności logowania. Tryb jest dostępny wyłącznie w urządzeniu mającym jeszcze ustawienia fabryczne i tylko przez krótki czas w trakcie włączania urządzenia.



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

W tym filmie pokazano, korzystać z trybu podglądu.

Od czego zacząć

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

✓: zalecane

*: obsługiwane z ograniczeniami

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis. Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora*, on page 6.

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

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła*, on page 7.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne*, on page 53.

Bezpieczne hasła

Ważne

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

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

Aby chronić dane, zalecamy:

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

Upewnianie się co do braku zmian w oprogramowaniu urządzenia

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

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne, on page 53*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

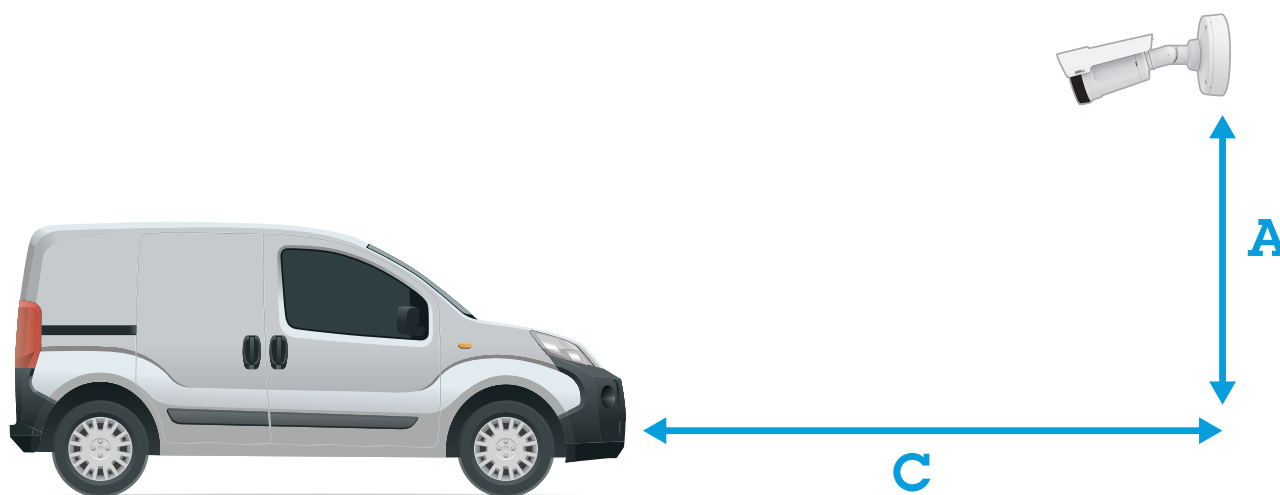
Konfiguracja podstawowa

Poniższe instrukcje dotyczące konfiguracji dotyczą wszystkich scenariuszy:

1. *Zalecenia dotyczące montażu kamery, on page 8*
2. *Konfigurowanie aplikacji AXIS License Plate Verifier, on page 10*
3. *Dostosowywanie obszarów zainteresowania, on page 11*
4. *Wybór regionu, on page 12*
5. *Konfiguracja przechowywania zdarzeń, on page 12*

Zalecenia dotyczące montażu kamery

- Po wybraniu miejsca montażu pamiętaj, że bezpośrednie światło słoneczne (na przykład podczas wschodu i zachodu słońca) może zniekształcić obraz.
- Wysokość mocowania kamery w scenariuszu **Free flow (Swobodnego przepływu)** (rozpoznawanie tablic rejestracyjnych pojazdów poruszających się z niewielką prędkością) powinna być mniejsza niż połowa odległości pomiędzy pojazdem a kamerą.



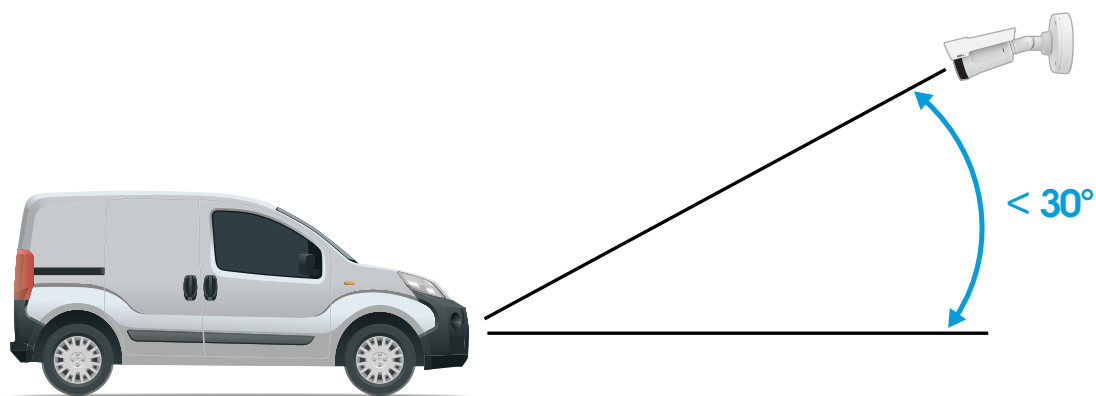
Swobodny przepływ z wbudowanym źródłem IR

Odległość monitorowania (C)	Wysokość mocowania (A)	Maksymalna prędkość pojazdu
20–50 m (65–164 ft)	4 m (13 ft)	90 km/h (56 mil/h)
30–50 m (98–164 ft)	6 m (19,5 stopy)	90 km/h (56 mil/h)
35–50 m (115–164 ft)	8 m (26,2 ft)	90 km/h (56 mil/h)
25–50 m (82–164 ft)	4 m (13 ft)	130 km/h (80 mil/h)
40–50 m (131–164 ft)	6 m (19,5 stopy)	130 km/h (80 mil/h)
n/d	8 m (26,2 ft)	130 km/h (80 mil/h)
40–50 m (131–164 ft)	4 m (13 ft)	200 km/h (124 mil/h) (*)
n/d	6 m (19,5 stopy)	200 km/h (124 mil/h)
n/d	8 m (26,2 ft)	200 km/h (124 mil/h)

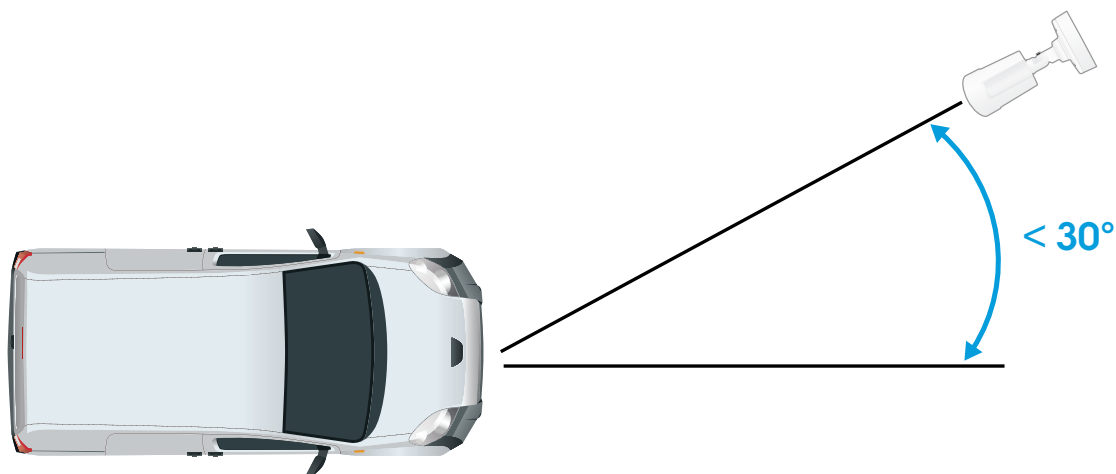
(*) W celu zapewnienia optymalnej detekcji zalecamy użycie zewnętrznego źródła promieniowania IR
Swobodny przepływ z zewnętrznym źródłem IR

Odległość monitorowania (C)	Wysokość mocowania (A)	Maksymalna prędkość pojazdu
20–100 m (65–328 ft)	4 m (13 ft)	90 km/h (56 mil/h)
30–100 m (98–328 ft)	6 m (19,5 stopy)	90 km/h (56 mil/h)
35–100 m (115–328 ft)	8 m (26,2 ft)	90 km/h (56 mil/h)
25–100 m (82–328 ft)	4 m (13 ft)	130 km/h (80 mil/h)
40–100 m (131–328 ft)	6 m (19,5 stopy)	130 km/h (80 mil/h)
50–100 m (164–328 ft)	8 m (26,2 ft)	130 km/h (80 mil/h)
40–100 m (131–328 ft)	4 m (13 ft)	200 km/h (124 mil/h)
60–100 m (197–328 ft)	6 m (19,5 stopy)	200 km/h (124 mil/h)
80–100 m (262–328 ft)	8 m (26,2 ft)	200 km/h (124 mil/h)

- Kamerę należy zamontować pod kątem nie większym niż 30° w dowolnym kierunku.

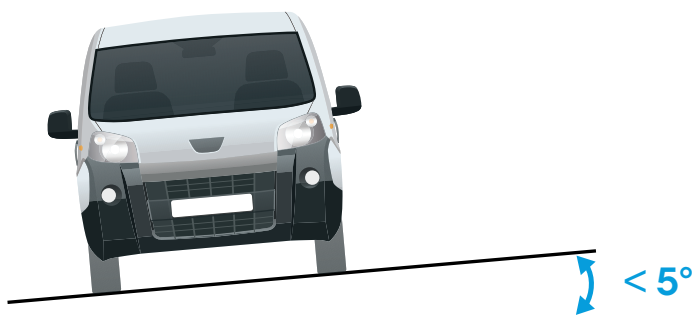


Kąt montażowy z boku.



Kąt montażowy z góry.

- Obraz tablicy rejestracyjnej nie powinien być nachylony o więcej niż 5° w poziomie. Jeśli obraz będzie nachylony o więcej niż 5°, zalecane jest ustawienie kamery w taki sposób, aby w strumieniu na żywo tablica rejestracyjna była wyświetlana poziomo.



Kąt obrotu.

Konfigurowanie aplikacji AXIS License Plate Verifier

1. W interfejsie WWW urządzenia przejdź do sekcji **Apps (Aplikacje)**.
2. Przełącz przełącznik obok aplikacji AXIS License Plate Verifier, aby ją uruchomić.
3. Kliknij **Open (Otwórz)**, aby otworzyć interfejs WWW aplikacji.
4. Postępuj zgodnie z instrukcjami, aby skonfigurować aplikację AXIS License Plate Verifier.
 - Skonfiguruj ustawienia **Free flow (Swobodny przepływ)**. Patrz *Swobodny przepływ, on page 10*.

Podczas pierwszego uruchamiania aplikacji należy przy użyciu asystenta konfiguracji skonfigurować **Free flow (Swobodny przepływ)**. Później można wprowadzić zmiany na karcie **Settings (Ustawienia)** w obszarze **Setup assistant (Asystent konfiguracji)**.

Swobodny przepływ

W swobodnym przepływie aplikacja może wykrywać i odczytywać tablice rejestracyjne pojazdów poruszających się z niewielką prędkością na dużych drogach dojazdowych, w centrach miejskich i terenach zamkniętych, takich jak kampusy, porty lub lotniska. Umożliwia to prace wyjaśniające i wyzwalanie zdarzeń w systemie VMS.

1. Wybierz **Free flow (Swobodny przepływ)** i kliknij przycisk **Next (Dalej)**.
2. Wybierz obracanie obrazu odpowiadające sposobowi zamontowania kamery.
3. Wybierz ilość obszarów zainteresowania. Jeden obszar może wykrywać tablice w obu kierunkach.
4. Wybierz region, w którym znajduje się kamera.
5. Wybierz typ rejestracji.
 - **License plate crop (Przycinanie tablic rejestracyjnych)** umożliwia zapisywanie wyłącznie tablic rejestracyjnych.
 - **Vehicle crop (Przycinanie pojazdu)** powoduje zapisanie całego przechwyconego pojazdu.
 - **Frame downsized 480x270 (Klatka zredukowana do 480x270)** powoduje zapisanie całego obrazu w rozdzielczości 480x270.
 - **Full frame (Pełna klatka)** powoduje zapisanie całego obrazu w pełnej rozdzielczości.
6. Przeciągnij punkty kotwiczące, aby dostosować obszar zainteresowania. Patrz *Dostosowywanie obszarów zainteresowania, on page 11*.

7. Dostosuj kierunek obszaru zainteresowania. Kliknij strzałkę i obróć, aby ustawić kierunek. Kierunek określa w jaki sposób aplikacja rejestruje pojazdy wjeżdżające do lub wyjeżdżające z obszaru.
8. Kliknij przycisk **Next (Dalej)**
9. Z listy rozwijanej **Protocol (Protokół)** wybierz jeden z następujących protokołów:
 - TCP
 - HTTP POST
10. W polu **Server URL (Adres URL serwera)** wpisz adres serwera i port w następującym formacie:
127.0.0.1:8080
11. W polu **Device ID (ID urządzenia)** wpisz nazwę urządzenia lub pozostaw pole bez zmian.
12. W polu **Event types (Typy zdarzeń)** wybierz jedną lub więcej następujących opcji:
 - **New (Nowe)** oznacza pierwsze wykrycie tablicy rejestracyjnej.
 - **Update (Aktualizacja)** jest poprawieniem znaków na wcześniej wykrytej tablicy rejestracyjnej lub po wykryciu kierunku przemieszczania się tablicy rejestracyjnej i śledzeniu jej na obrazie.
 - **Lost (Utrata)** to ostatnie monitorowane zdarzenie dotyczące tablicy rejestracyjnej, zanim opuści ona obszar obrazu. Zawiera również kierunek poruszania się tablic rejestracyjnych.
13. Aby włączyć tę funkcję, wybierz opcję **Send event data to server (Wysyłaj dane zdarzeń na serwer)**.
14. Aby zmniejszyć przepustowość podczas korzystania z protokołu HTTP POST, można wybrać opcję **Do not send images through HTTP POST (Nie wysyłaj obrazów za pośrednictwem protokołu HTTP POST)**.
15. Kliknij **Next (Dalej)**.
16. Jeżeli masz już listę zapisanych tablic, wybierz opcję importowania jako **blocklist (listę blokowanych)** lub **allowlist (listę dozwolonych)**.
17. Kliknij przycisk **Finish (Zakończ)**.

Uzyskiwanie dostępu do ustawień aplikacji

1. W interfejsie WWW kamery przejdź do menu **Apps (Aplikacje)**, uruchom aplikację i kliknij przycisk **Open (Otwórz)**.

Dostosowywanie obszarów zainteresowania

Obszar zainteresowania jest częścią podglądu na żywo, w której aplikacja szuka tablic rejestracyjnych. W celu zapewnienia maksymalnej wydajności warto ustawić jak najmniejszy obszar zainteresowania. Dostosowywanie obszaru zainteresowania:

1. Przejdź do opcji **Settings (Ustawienia)**.
2. Kliknij **Image (Obraz)**.
3. Kliknij przycisk 1:1, aby powiększyć obszar, w którym chcesz monitorować ruch lub zarządzać kontrolą dostępu.
4. Aby polepszyć weryfikację i jakość przechwytywanych obrazów, kliknij **AF (Automatyczne ogniskowanie)**.
5. Aby kamera automatycznie ustawiała ogniskowanie na pojazdach, kliknij **AF (Automatyczne ogniskowanie)**. Aby ręcznie ustawić ogniskowanie, dostosuj je za pomocą suwaka.
6. Kliknij **Area of interest (Obszar zainteresowania)**, aby wyświetlić obszar w obszarze obserwacji.
7. Aby przenieść obszar zainteresowania, kliknij wewnątrz tego obszaru celem jego wybrania, a następnie przesun go w miejsce, w którym tablice rejestracyjne są najlepiej widoczne. Upewnij się, że po zapisaniu tych ustawień obszar zainteresowania pozostaje w tym samym miejscu.
8. Aby dostosować obszar zainteresowania, kliknij w dowolnym miejscu w obszarze celem jego wybrania, a następnie przeciągnij punkty kotwiczące oznaczone na niebiesko.
 - Aby zresetować obszar zainteresowania, kliknij przycisk resetowania w lewym dolnym rogu obok ikony liczby.

- Aby dodać punkty kotwiczenia, kliknij jeden z ciemnych punktów kotwiczenia. Kolor punktu kotwiczenia zmieni się na żółty, co będzie oznaczało, że można nim manipulować. Obok żółtego punktu kotwiczenia zostaną automatycznie dodane nowe ciemne punkty. Można wybrać maksymalnie 8 żółtych punktów kotwiczenia.
9. Kliknij w dowolnym miejscu poza obszarem zainteresowania, aby zapisać zmiany.
 10. Aby uzyskać prawidłowe informacje zwrotne dotyczące kierunku w Event log (Dzienniku zdarzeń), ustaw strzałkę w kierunku jazdy.
 - 10.1. Kliknij ikonę strzałki.
 - 10.2. Wybierz punkt kotwiczenia i obróć strzałkę, tak aby była ustawiona zgodnie z kierunkiem jazdy.
 - 10.3. Kliknij poza obszarem zainteresowania, aby zapisać zmiany.

Jeden obszar może wykrywać tablice w obu kierunkach. Informacja zwrotna zostanie wyświetlona w kolumnie **Direction (Kierunek)**.

11. Aby sprawdzić, czy obszar zainteresowania jest wystarczająco duży do uzyskania najlepszych wyników, wykorzystaj licznik pikseli.
 - Aby wyświetlić licznik pikseli, kliknij ikonę kalkulatora.
 - Aby dostosować pełnowymiarowy obszar licznika pikseli, przeciągnij prawy dolny róg obszaru zaznaczonego na żółto.
 - Aby przenieść obszar licznika pikseli, kliknij w dowolnym miejscu tego obszaru i przeciągnij w wybrane miejsce.
- Aby dodać drugi obszar zainteresowania, kliknij+ obok 1.
- W przypadku używania kamery autonomicznej można wybrać w aplikacji zalecane ustawienia rozpoznawania tablic rejestracyjnych.
 1. Kliknij ikonę różdżki, a ustawienia zostaną zoptymalizowane pod kątem rozpoznawania numerów tablic rejestracyjnych.
 2. Kliknij przycisk menu obok różdżki, aby wyświetlić ustawione wartości.

Wybór regionu

1. Przejdź do Settings > Recognition (Ustawienia > Rozpoznawanie).
2. Z listy rozwijanej Region wybierz region.

Dostosowywanie ustawień przechwytywania obrazu

1. Przejdź do menu Settings (Ustawienia) > Image (Obraz).
2. Aby zmienić rozdzielczość przechwytywanych obrazów, przejdź do Image Resolution (Rozdzielczość obrazu)
3. Aby zmienić orientację przechwytywanych obrazów, przejdź do Rotation (Orientacja)

Konfiguracja przechowywania zdarzeń

Zdarzenie składa się z przechwyconego obrazu, tablicy rejestracyjnej, numeru obszaru zainteresowania, kierunku ruchu pojazdu, dostępu oraz daty i czasu.

W tym przykładzie opisano sposób przechowywania zdarzeń numerów rejestracyjnych z listy dozwolonych przez 30 dni.

Wymagania:

- Kamera jest zamontowana i podłączona do sieci.
 - Aplikacja AXIS License Plate Verifier działa w kamerze.
 - Pamięć wewnętrzna lub karta SD zainstalowane w kamerze.
1. Przejdź do Settings > Storage (Ustawienia > Pamięć masowa).

2. W sekcji **Retain events** (Zachowaj zdarzenia) wybierz polecenie **Allowlisted** (Lista dozwolonych).
3. W sekcji **Retention period** (Okres przechowywania) wybierz **30 days** (30 dni).
4. Aby zmienić sposób zapisywania przechwytywanych obrazów, przejdź do opcji **Save full frame** (Zapisz pełną klatkę):
 - **License plate crop** (Przycinanie tablic rejestracyjnych) umożliwia zapisywanie wyłącznie tablic rejestracyjnych.
 - **Vehicle crop** (Przycinanie pojazdu) powoduje zapisanie całego przechwyconego pojazdu.
 - **Frame downsized 480x270** (Klatka zredukowana do 480x270) powoduje zapisanie całego obrazu w rozdzielczości 480x270.
 - **Full frame** (Pełna klatka) powoduje zapisanie całego obrazu w pełnej rozdzielczości.

Uwaga

Aby wykryć włożoną kartę SD, gdy aplikacja jest uruchomiona, trzeba ją zrestartować. Jeśli w kamerze jest zainstalowana karta SD, aplikacja automatycznie wybierze ją jako domyślne urządzenie pamięci masowej.

AXIS License Plate Verifier może zapisać do 1000 zdarzeń w pamięci wewnętrznej kamery, używając tablic rejestracyjnych jako ramki. Skonfigurowanie większych ramek spowoduje zmianę liczby wydarzeń, które można zapisać.

Na karcie SD można zapisać do 100 000 zdarzeń z użyciem dowolnego typu ramki.

Konfiguracja urządzenia

W tej części zostały opisane wszystkie ważne konfiguracje, które musi przeprowadzić instalator, aby uruchomić produkt po zakończeniu montażu sprzętu.

Ustawienia podstawowe

Ustawianie trybu rejestracji

1. Przejdź do menu **Video > Installation > Capture mode** (Wideo > Instalacja > Tryb rejestracji).
2. Kliknij **Change** (Zmień).
3. Wybierz tryb rejestracji i kliknij **Save and restart** (Zapisz i uruchom ponownie).
Zob. też. *Tryby rejestracji, on page 43.*

Ustawianie częstotliwości zasilania

1. Przejdź do menu **Video > Installation > Power line frequency** (Wideo > Instalacja > Częstotliwość zasilania).
2. Wybierz częstotliwość zasilania, a następnie kliknij przycisk **Save and restart** (Zapisz i uruchom ponownie).

Ustawianie orientacji

1. Przejdź do menu **Video > Installation > Rotate** (Wideo > Instalacja > Obrót).
2. Wybierz 0, 90, 180 lub 270 stopni.
Zob. też..

Regulowanie obrazu

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej na temat działania niektórych funkcji, przejdź do *Więcej informacji, on page 43.*

Poziomowanie kamery

Aby dostosować obszar obserwacji w zależności od obszaru odniesienia lub obiektu, należy użyć siatki poziomej oraz mechanicznie ustawić kamerę.

1. Przejdź do menu **Video (Wideo) > Image (Obraz) >** i kliknij .
2. Kliknij , aby wyświetlać siatkę poziomą.
3. Wyreguluj kamerę tak, aby położenie obszaru odniesienia lub obiektu wyrównało się z siatką poziomą.

Korzystanie z oświetlenia IR w warunkach słabego oświetlenia (tryb nocny)

Kamera w ciągu dnia rejestruje kolorowe obrazy, korzystając ze światła dziennego. Niemniej, wraz ze zmniejszaniem się ilości światła widzialnego obrazy kolorowe stają się mniej jasne i wyraźne. Jeżeli w takiej sytuacji zostanie aktywowany tryb nocny, kamera będzie wykorzystywać zarówno światło widzialne, jak i podczerwień, aby uzyskać jasne i szczegółowe obrazy w czerni i bieli. Istnieje możliwość ustawienia automatycznego przełączania na tryb nocny.

1. Przejdź do **Video > Image > Day-night mode** (Wideo > Obraz > Tryb dzień/noc) i upewnij się, że w opcji **IR cut filter** (Filtr odcinający promieniowanie podczerwone) ustawiono wartość **Auto** (Automatycznie).
2. Aby ustawić, przy jakim poziomie oświetlenia kamera ma się przełączać na tryb nocny, przesun suwak **Threshold** (próg) w kierunku opcji **Bright** (Jasno) lub **Dark** (Ciemno).
3. Aby kamera używała wbudowanego oświetlenia promieniowania IR po włączeniu trybu nocnego, włącz opcje **Allow illumination** (Zezwalaj na oświetlenie) i **Synchronize illumination** (Synchronizuj oświetlenie).

Uwaga

W przypadku ustawienia przełączania w tryb nocny wtedy, gdy jest jaśniej, obraz pozostanie ostry, ponieważ będzie zawierał mniej szumu spowodowanego słabym oświetleniem. W przypadku ustawienia przełączania wtedy, gdy jest ciemniej, kolory zostaną zachowane przez dłuższy czas, ale wystąpi szum spowodowany słabym oświetleniem.

Optymalizacja oświetlenia w podczerwieni

W zależności od środowiska montażowego i warunków kamery, na przykład zewnętrznych źródeł światła w scenie, czasami można poprawić jakość obrazu po ręcznym dostosowaniu natężenia oświetlenia LED. Jeżeli występują problemy z odbiciami światła emitowanego przez diody LED, spróbuj zmniejszyć ich intensywność.

1. Przejdź do menu **Video (Wideo) > Image (Obraz) > Day-night mode (Tryb dzienny/nocny)**.
2. Włącz opcję **Allow illumination (Zezwalaj na oświetlenie)**.
3. Kliknij  w podglądzie na żywo i wybierz **Manual (Ręcznie)**.
4. Dostosuj intensywność.

Aby zredukować efekt odbicia, można też zmienić kąt oświetlenia.

1. Przejdź do menu **Video (Wideo) > Image (Obraz) > Day-night mode (Tryb dzienny/nocny)**.
2. Wyłącz funkcję **Automatic illumination angle (Automatyczny kąt oświetlenia)**.
3. Ustaw suwak kąta oświetlenia w odpowiednim położeniu.

Stabilizacja obrazu za pomocą funkcji stabilizacji obrazu

Funkcja stabilizacji jest przeznaczona do użycia w przypadku środowisk, w których produkt jest zamontowany na zewnątrz budynku i narażony na drgania, np. z powodu wiatru lub ruchu pojazdów.

Funkcja ta sprawia, że obraz jest płynniejszy, stabilniejszy i mniej rozmazany. Zmniejsza ona również rozmiar pliku skompresowanego obrazu i obniża przepływność bitową strumienia wideo.

Uwaga

Gdy stabilizacja obrazu jest włączona, obraz będzie lekko przycięty, a jego maksymalna rozdzielczość zostanie obniżona.

1. Przejdź do menu **Video > Installation > Image correction (Wideo > Instalacja > Korekta obrazu)**.
2. Włącz **Image stabilization (Stabilizacja obrazu)**.

Kompensacja dystorsji beczkowatej

Dystorsja beczkowata to zjawisko, w którym linie proste stają się coraz bardziej zagięte bliżej krawędzi klatki. Szerokie pole widzenia często powoduje tworzenie się dystorsji beczkowatej. Korekcja dystorsji beczkowatej to funkcja służąca do kompensacji tego zjawiska.

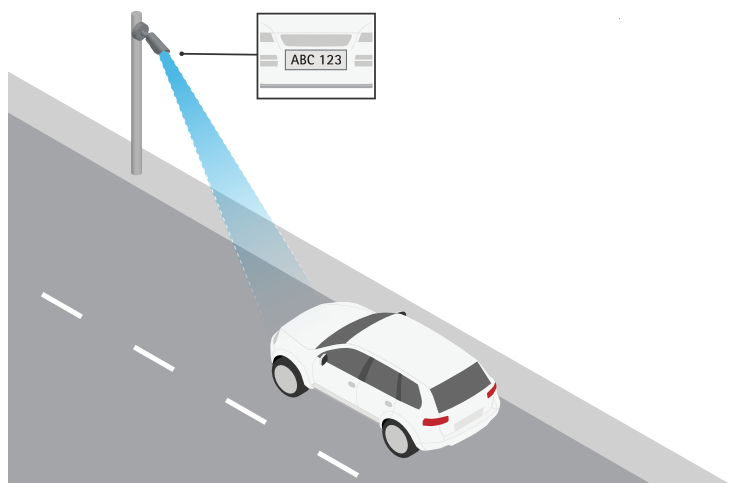
Uwaga

Korekcja dystorsji beczkowatej wpływa na rozdzielczość obrazu i pole widzenia.

1. Przejdź do menu **Video > Installation > Image correction (Wideo > Instalacja > Korekta obrazu)**.
2. Włącz funkcję **Korekcja dystorsji beczkowatej (BDC)**.

Sprawdzanie rozdzielczości pikseli

Aby sprawdzić, czy zdefiniowana część obrazu zawiera wystarczającą liczbę pikseli w celu na przykład rozpoznawania twarzy osób, można użyć licznika pikseli.



1. Wybierz kolejno opcje **Video > Image (Wideo > Obraz)**.
2. Kliknij .
3. Kliknij , aby wyświetlić **Pixel counter (Licznik pikseli)**.
4. Dostosuj rozmiar i pozycję prostokąta w podglądzie na żywo kamery, na przykład tak, aby w obszarze zainteresowania obejmował miejsce, w którym mogą pojawić się tablice rejestracyjne samochodów.
5. Możesz zobaczyć liczbę pikseli każdej ze stron prostokąta i zdecydować, czy wartości są wystarczające dla Twoich potrzeb.

Ukrywanie części obrazu za pomocą masek prywatności

Możesz utworzyć jedną lub kilka masek prywatności, aby ukryć fragmenty obrazu.

1. Przejdź do okna **Video > Privacy masks (Wideo > Maski prywatności)**.
2. Kliknij .
3. Kliknij nową maskę i nadaj jej nazwę.
4. Dostosuj rozmiar i położenie maski prywatności zgodnie z potrzebami.
5. Aby zmienić kolor wszystkich masek prywatności, kliknij **Privacy masks (Maski prywatności)** i wybierz jeden z kolorów.

Zob. też *Maski prywatności*, on page 43

Wyświetlanie nakładek na obrazie

Możesz dodać obraz jako nałożenie do strumienia wideo.

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

Wyświetlanie nakładki tekstu

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

1. Wybierz kolejno opcje **Video > Overlays (Wideo > Nakładki)**.
2. Wybierz opcję **Text (Tekst)** i kliknij .
3. Wpisz tekst, który chcesz wyświetlać, lub wybierz modyfikatory, aby wyświetlać na przykład aktualną datę.
4. Wybierz położenie. Aby zmienić położenie nakładki, można ją również kliknąć i przeciągnąć w podglądzie na żywo.

Wyświetlanie nałożeń tablic rejestracyjnych

Nałożenia tablic rejestracyjnych to funkcja dostępna w aplikacji *AXIS License Plate Verifier*.

1. Wybierz kolejno opcje **Video > Image (Wideo > Obraz)**.
2. Aby uzyskać dostęp do ekranowych elementów sterowania urządzenia, kliknij  w podglądzie na żywo.
3. Rozwiń **Predefined controls (Wstępnie zdefiniowane elementy sterowania)**.
4. Włącz funkcję **License plate overlay (Nałożenia tablic rejestracyjnych)**.
5. Kliknij **Show overlay (Pokaż nałożenie)**.
6. Kliknij **Move overlay (Przesuń nałożenie)**, aby przenieść nałożenie.

Dodawanie nazw ulic i kierunku kompasu do obrazu

Uwaga

Nazwa ulicy i kierunek kompasu będą widoczne na wszystkich strumieniach i zapisach wideo.

1. Przejdź do menu **Apps (Aplikacje)**.
2. Wybierz opcję **axis-orientationaid**.
3. Kliknij przycisk **Otwórz**.
4. Aby dodać nazwę ulicy, kliknij opcję **Add text (Dodaj tekst)** i zmień tekst na nazwę ulicy.
5. Aby dodać kompas, kliknij opcję **Add compass (Dodaj kompas)** i zmień kompas, aby dopasować go do obrazu.

Przeglądanie i rejestracja obrazów wideo

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej o działaniu strumieniowania i pamięci masowej, przejdź do *Strumieniowanie i pamięć masowa, on page 43*.

Zmniejszanie zapotrzebowania na przepustowość i zasób

Ważne

Zmniejszenie przepustowości może skutkować utratą wyrazistości szczegółów na obrazie.

1. Wybierz kolejno opcje **Video > Stream (Wideo > Strumień)**.
2. W podglądzie na żywo kliknij .
3. Wybierz **Video format (Format wideo) AV1**, jeśli urządzenie go obsługuje. W przeciwnym razie wybierz **H.264**.

- Przejdź do okna **Video > Stream > General** (**Wideo > Strumień > Ogólne**) i zwiększ wartość w polu **Compression** (**Kompresja**).
- Przejdź do menu **Video > Stream > Zipstream** (**Wideo > Przesyłanie strumieniowe > Zipstream**) i wykonaj jedną lub więcej z czynności opisanych niżej:

Uwaga

Ustawienia technologii **Zipstream** są stosowane do wszystkich typów kodowania z wyjątkiem **MJPEG**.

- Wybierz opcję **Zipstream Strength** (Siła technologii **Zipstream**), której chcesz użyć.
- Włącz polecenie **Optimize for storage** (Optymalizuj pod kątem zasobu). Tej opcji można użyć tylko wtedy, gdy oprogramowanie do zarządzania materiałem wideo obsługuje ramki B.
- Włącz opcję **Dynamic FPS** (Dynamiczna liczba klatek na sekundę).
- Włącz opcję **Dynamic GOP** (Dynamiczna liczba klatek na sekundę) i dla długości GOP ustaw wysoką wartość parametru **Upper limit** (Górny limit).

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.

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

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z kamery

- Wybierz kolejno opcje **Video > Stream** (**Wideo > Strumień**).
- Aby rozpocząć nagrywanie, kliknij .

Jeżeli jeszcze nie skonfigurowano żadnej pamięci masowej, kliknij  i . Aby uzyskać instrukcje dotyczące konfigurowania sieciowej pamięci masowej, zob. *Konfiguracja zasobów sieciowej pamięci masowej, on page 18*

- Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

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

Sprawdzanie braku sabotażu wideo

Podpis wideo daje pewność, że nikt nie zmienił zapisu wideo w kamerze.

1. Przejdź do menu **Video > Stream > General (Wideo > Strumieniowanie > Ogólne)** i włącz opcję **Signed video (Podpisane wideo)**.
2. Zapisuj obraz bezpośrednio w urządzeniu lub użyj programu **AXIS Camera Station Pro** albo innego kompatybilnego oprogramowania do zarządzania obrazem. Aby uzyskać szczegółowe informacje dotyczące programu **AXIS Camera Station Pro**, p. *instrukcja obsługi AXIS Camera Station Pro*.
3. Wyeksportuj zarejestrowany materiał wideo.
4. Przeprowadź weryfikację nagrań przy użyciu narzędzia *Axis Signed Media Verifier*.

Parowanie kamery z radarem

Parowanie radaru jest konfiguracją jednokierunkową, w ramach której kamera jest parowana z radarem i służy do konfigurowania i obsługi obu urządzeń. Kamera ma przydzielony kanał na potrzeby strumienia radaru, a po sparowaniu strumień radaru zostaje automatycznie przypisany do tego kanału.

Aby dowiedzieć się więcej o technologii edge-to-edge, zobacz *Technologia edge-to-edge, on page 46*.

Zanim zaczniesz:

- Upewnij się, że kamera i radar są skierowane na ten sam obszar zainteresowania.
- Upewnij się, że kamera i radar są zsynchronizowane względem tego samego źródła czasu. Aby sprawdzić status synchronizacji czasu, przejdź do menu **Installation > Time sync status (Instalacja > Status synchronizacji czasu)** w obu urządzeniach.

Parowanie kamery z radarem:

1. Otwórz interfejs WWW kamery i przejdź do obszaru **System > Edge-to-edge > Pairing (Parowanie)**.
2. Kliknij  **Add (Dodaj)**.
3. Z listy rodzajów parowania wybierz **Radar**.
4. Wpisz nazwę hosta, nazwę użytkownika i hasło radaru.
5. Kliknij **Connect (Połącz)**, aby sparować urządzenia.
Gdy nastąpi połączenie urządzeń, ustawienia radaru staną się dostępne w interfejsie internetowym kamery.

Uwaga

Domyślna rozdzielczość sparowanego radaru wynosi 1280x720. Zachowaj domyślną rozdzielczość radaru w interfejsie WWW kamery i w przypadku dodawania urządzenia do systemu VMS.

Konfigurowanie radaru:

1. W interfejsie WWW kamery przejdź do **Radar > Scenarios (Radar > Scenariusze)**.
2. Skonfiguruj radar w zależności od potrzeb.
Więcej informacji na temat konfigurowania radaru można znaleźć w instrukcji obsługi na stronie *help.axis.com*.

Uwaga

W przypadku uaktualniania wersji systemu **AXIS OS** kamery należy również uaktualnić system **AXIS OS** radaru, aby zapewnić aktualność całej instalacji. Zalecamy skorzystanie z narzędzia do zarządzania urządzeniami, takiego jak **AXIS Device Manager**.

Łączenie z sygnalizatorem akustyczno-optycznym

Parowanie sieciowe umożliwia sparowanie kamery z kompatybilnym urządzeniem Axis zawierającym funkcję sygnalizacji akustycznej i optycznej. Po sparowaniu kamera może konfigurować obydwa urządzenia i nimi zarządzać.

Sparuj kamerę z sygnalizatorem akustyczno-optycznym:

1. Przejdź do menu **System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie)**.
2. Kliknij  **Add (Dodaj)** i z rozwijalnej listy wybierz rodzaj parowania **Network pairing (Parowanie sieciowe)**.
3. Wpisz adres IP, nazwę użytkownika i hasło sygnalizatora akustyczno-optycznego.
4. Kliknij przycisk **Połącz**. Zostanie wyświetlony komunikat potwierdzający.

Aby znaleźć urządzenia bezpośrednio w sieci IP, kliknij **Discover devices (Wykryj urządzenia)**.

Uwaga

- Na liście pojawiają się wszystkie znalezione urządzenia Axis, nie tylko urządzenia możliwe do sparowania.
- Urządzenia już sparowane oznaczone są ikoną informacyjną. Najedź kursorem na ikonę, aby pozyskać informacje o aktywnych urządzeniach sparowanych.
- Sprawdź, czy sparowane urządzenia mają tę samą wersję systemu operacyjnego (oprogramowania układowego) AXIS OS.

Ważne

- Możliwe jest wykrywanie wyłącznie urządzeń, w których dostępny jest protokół Bonjour. Aby włączyć protokół Bonjour w urządzeniu, otwórz jego interfejs internetowy i przejdź do **System > Network > Network discovery protocols (System > Sieć IP > Protokoły wykrywania w sieci)**.

Konfiguracja reguł dotyczących zdarzeń

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

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

Wyzwalanie akcji

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

Uwaga

- Jeżeli zostanie zmieniona definicja profilu strumieniowania stosowana w regule, konieczne jest ponowne uruchomienie wszystkich reguł wykorzystujących ten profil strumieniowania.

Oszczędzanie energii, kiedy nie jest wykrywany żaden ruch

Ten przykład pokazuje, jak włączyć tryb oszczędzania energii, gdy w scenie nie jest wykrywany żaden ruch.

Uwaga

Po włączeniu trybu oszczędzania energii zakres oświetlenia w podczerwieni jest zmniejszony.

Upewnij się, że jest uruchomiona aplikacja AXIS Video Motion Detection:

1. Wybierz kolejno opcje **Apps > AXIS Video Motion Detection (Aplikacje > AXIS Video Motion Detection)**.
2. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
3. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

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 **Application (Aplikacja)** wybierz **VMD4**.
4. Wybierz opcję **Invert this condition (Odwróć ten warunek)**.
5. Na liście akcji w obszarze **Power saving mode (Tryb oszczędzania energii)** wybierz opcję **Use power saving mode while the rule is active (Tryb oszczędzania energii, gdy reguła jest aktywna)**.
6. Kliknij przycisk **Zapisz**.

Rejestrowanie obrazu wideo w momencie wykrycia obiektu

W tym przykładzie wyjaśniono, jak skonfigurować kamerę, aby rozpocząć zapis na karcie SD, kiedy kamera wykryje dany obiekt. Zapis obejmuje pięć sekund przed detekcją i minutę po zakończeniu detekcji.

Zanim zaczniesz:

- Upewnij się, że karta SD została zainstalowana.

Upewnij się, że jest uruchomiona aplikacja **AXIS Video Motion Detection**:

1. Wybierz kolejno opcje **Apps > AXIS Video Motion Detection (Aplikacje > AXIS Video Motion Detection)**.
2. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
3. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

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 **Application (Aplikacja)** wybierz **VMD4**.
4. Z listy akcji w obszarze **Recordings (Zapisy)** wybierz opcję **Record video while the rule is active (Rejestruj wideo, gdy reguła jest aktywna)**.
5. Z listy opcji pamięci masowej wybierz opcję **SD_DISK**.
6. Wybierz kamerę i profil strumienia.
7. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
8. Ustaw czas buforowania po zdarzeniu na 1 minutę.
9. Kliknij przycisk **Zapisz**.

Wyświetlanie nałożenia tekstu w strumieniu wideo, gdy urządzenie wykryje obiekt

W poniższym przykładzie wyjaśniono sposób wyświetlania tekstu „Motion detected” (Wykryto ruch), gdy urządzenie wykryje obiekt.

Upewnij się, że jest uruchomiona aplikacja **AXIS Video Motion Detection**:

1. Wybierz kolejno opcje **Apps > AXIS Video Motion Detection (Aplikacje > AXIS Video Motion Detection)**.
2. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
3. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

Dodaj nałożenie tekstu:

1. Wybierz kolejno opcje **Video > Overlays (Wideo > Nakładki)**.
2. W obszarze **Overlays (Nałożenia)** zaznacz opcję **Text (Tekst)** i kliknij **+**.
3. W polu tekstowym wprowadź **#D**.
4. Wybierz rozmiar i wygląd tekstu.

5. Aby umieścić nałożenie tekstowe, kliknij  i wybierz opcję.

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 **Application (Aplikacja)** wybierz **VMD4**.
4. Na liście akcji w obszarze **Overlay text (Nałożony tekst)** wybierz opcję **Use overlay text (Użyj nałożonego tekstu)**.
5. Wybierz kanał wideo.
6. W polu **Text (Tekst)** wpisz „Motion detected” (Wykryto ruch).
7. Ustaw czas trwania.
8. Kliknij przycisk **Zapisz**.

Uwaga

Aktualizacja nałożonego tekstu będzie automatycznie wprowadzana na wszystkich strumieniach wideo.

Zapewnianie wizualnej sygnalizacji trwającego zdarzenia

Dostępna jest możliwość podłączenia AXIS I/O Indication LED do kamery sieciowej. Wskaźnik LED można skonfigurować tak, aby włączał się zawsze po wystąpieniu pewnych zdarzeń w kamerze. Na przykład po to, aby poinformować, że trwa nagrywanie wideo.

Wymagany sprzęt

- AXIS I/O Indication LED
- Sieciowa kamera wideo Axis

Uwaga

Instrukcje podłączenia AXIS I/O Indication LED znaleźć można w instrukcji montażu dołączonej do produktu.

Poniższy przykład ilustruje sposób konfigurowania reguły, która włącza AXIS I/O Indication LED, aby wskazać, że trwa nagrywanie.

1. Przejdź do menu **System > Accessories > I/O ports (System > Akcesoria > Porty we/wy)**.
2. W przypadku portu, do którego podłączony jest AXIS I/O Indication LED, kliknij , aby ustawić kierunek na **Output (Wyjście)**, a następnie kliknij , aby ustawić stan normalny na **Circuit open (Obwód otwarty)**.
3. Przejdź do **System > Events (System > Zdarzenia)**.
4. Utwórz nową regułę.
5. Wybierz **Condition (Warunek)**, który musi zostać spełniony w celu rozpoczęcia nagrywania. Może to na przykład być harmonogram czasowy lub detekcja ruchu.
6. Z listy akcji wybierz opcję **Record video (Zarejestruj wideo)**. Wybierz pamięć masową. Wybierz profil strumienia lub utwórz nowy. Ustaw również **Prebuffer (Bufor przed zdarzeniem)** i **Postbuffer (Bufor po zdarzeniu)**.
7. Zapisz regułę.
8. Utwórz drugą regułę i wybierz ten sam **Condition (Warunek)**, co w pierwszej regule.
9. Z listy akcji wybierz opcję **Toggle I/O while the rule is active (Przełącz I/O, gdy reguła jest aktywna)**, a następnie wybierz port, do którego podłączony jest the AXIS I/O Indication LED. Ustaw stan na **Active (Aktywny)**.
10. Zapisz regułę.

Inne sytuacje, w których można wykorzystać AXIS I/O Indication LED, to na przykład:

- Konfiguracja wskaźnika LED tak, by włączył się, gdy kamera zostaje uruchomiona, tak by wskazywać na jej obecność. Wybierz jako warunek **System ready (System gotowy)**.
- Konfiguracja wskaźnika LED tak, by włączył się, gdy aktywny jest strumień na żywo i by wskazywał, że osoba lub program uzyskali dostęp do strumienia z kamery. Wybierz jako warunek **Live stream accessed (Dostęp do strumienia na żywo)**.

Rejestrowanie obrazu wideo w momencie wykrycia głośnych dźwięków przez kamerę

W tym przykładzie wyjaśniono sposób konfiguracji kamery w celu rozpoczęcia zapisu na karcie SD w ciągu pięciu sekund przed wykryciem głośnego dźwięku i zakończenia rejestracji po dwóch minutach.

Uwaga

Zgodnie z poniższymi instrukcjami wymagane jest podłączenie mikrofonu do wejścia audio.

Włącz dźwięk:

1. Skonfiguruj profil strumienia, tak by włączyć opcję audio; patrz: *Dodawanie dźwięku do zapisu, on page 25*.

Włącz detekcję dźwięku:

1. Przejdź do menu **System > Detectors > Audio detection (System > Detektory > Detekcja dźwięku)**.
2. Dostosuj poziom dźwięku w zależności od potrzeb.

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 **Audio (Dźwięk)** wybierz opcję **Audio Detection (Detekcja dźwięku)**.
4. Z listy akcji w obszarze **Recordings (Zapisy)** wybierz opcję **Record video (Rejestruj wideo)**.
5. Z listy opcji pamięci masowej wybierz opcję **SD_DISK**.
6. Wybierz profil strumienia, w którym włączono dźwięk.
7. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
8. Ustaw czas buforowania po zdarzeniu na 2 minuty.
9. Kliknij przycisk **Zapisz**.

Rejestrowanie obrazu wideo w momencie wykrycia uderzenia przez kamerę

Funkcja wykrywania wstrząsów umożliwia wykrywanie sabotażu spowodowanego przez drgania lub wstrząsy. Drgania spowodowane przez otoczenie lub jakiś obiekt mogą wyzwolić akcję w zależności od ustawionego zakresu – od 0 do 100. W tym scenariuszu ktoś rzuca kamieniami w kamerę po godzinach, a ty chcesz nagrać wideo ze zdarzenia.

Włącz wykrywanie wstrząsów:

1. Przejdź do menu **System > Detectors > Shock detection (System > Detektory > Detekcja wstrząsów)**.
2. Włącz detekcję wstrząsów i ustaw czułość na wstrząsy.

Create a rule (Utwórz regułę):

3. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
4. Wprowadź nazwę reguły.
5. Z listy warunków w obszarze **Device status (Stan urządzenia)** wybierz opcję **Shock detected (Wykryto wstrząs)**.
6. Kliknij **+**, aby dodać drugi warunek.
7. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
8. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.

9. Z listy akcji w obszarze **Recordings (Zapisy)** wybierz opcję **Record video while the rule is active (Rejestruj wideo, gdy reguła jest aktywna)**.
10. Wybierz lokalizację zapisu.
11. Wybierz opcję **Camera (Kamera)**.
12. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
13. Ustaw czas buforowania po zdarzeniu na 50 sekund.
14. Kliknij przycisk **Zapisz**.

Wykrywanie ingerencji w sygnał wejściowy

W tym przykładzie wyjaśniono, w jaki sposób wysyłać wiadomość e-mail po odcięciu lub zwarceniu obwodu sygnału wejściowego. Więcej informacji na temat złącza I/O: *page 50*.

1. Przejdź do obszaru **System > Accessories (Akcesoria) > I/O ports (Porty WE/WY)** i włącz **Supervised (Nadzorowane)** dla odpowiedniego portu.

Dodaj odbiorcę wiadomości e-mail:

1. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź nazwę odbiorcy.
3. Jako typ powiadomienia wybierz **Email (E-mail)**.
4. Wpisz adres e-mail odbiorcy.
5. Wpisz adres e-mail, z którego kamera ma wysyłać powiadomienia.
6. Podaj dane logowania do konta e-mail wysyłającego powiadomienia wraz z nazwą hosta SMTP i numerem portu.
7. Aby przetestować ustawienia poczty e-mail, kliknij **Test**.
8. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków w obszarze **I/O (WE/WY)** wybierz **Supervised input tampering is active (Sabotaż wejścia nadzorowanego jest aktywny)**.
4. Wybierz odpowiedni port.
5. Z listy akcji w menu **Notifications (Powiadomienia)** wybierz pozycję **Send notification to email (Wyślij powiadomienie emailem)**, a następnie wybierz odbiorcę z listy.
6. Wpisz temat i treść wiadomości e-mail.
7. Kliknij przycisk **Zapisz**.

Automatyczne przesyłanie wiadomości e-mail w przypadku zamalowania obiektywu farbą w sprayu

W tym przykładzie wyjaśniono, jak skonfigurować regułę w interfejsie WWW kamery, która wysyła e-mail, gdy obraz jest zasłonięty przez ponad 40 sekund, na przykład z powodu zamalowania obiektywu sprayem.

Zanim zaczniesz:

- Utwórz adresata e-maila w interfejsie WWW kamery.

W aplikacji **AXIS Image Health Analytics**:

1. Włącz **Blocked image (Zablokowany obraz)**.
2. Ustaw **Validation period (Okres weryfikacji)** na 40 sekund.

W interfejsie WWW kamery:

3. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
4. Wprowadź nazwę reguły.

5. Z listy warunków w obszarze Applications (Aplikacje) wybierz Image Health Analytics – Block (Image Health Analytics – zablokowanie).
6. Z listy akcji w obszarze Notifications (Powiadomienia) wybierz opcję Send notification to email (Wyślij powiadomienie w wiadomości e-mail).
7. Wybierz odbiorcę z listy.
8. Wpisz temat i treść e-maila.
9. Kliknij przycisk Zapisz.

Dźwięk

Dodawanie dźwięku do zapisu

Włącz dźwięk:

1. Przejdź do menu Video > Stream > Audio (Wideo > Strumień > Dźwięk) i włącz obsługę audio.
2. Jeżeli urządzenie ma więcej niż jedno źródło sygnału wejściowego, wybierz właściwe w polu Source (Źródło).
3. Wybierz kolejno opcje Audio > Device settings (Dźwięk > Ustawienia urządzenia) i włącz odpowiednie źródło sygnału wejściowego.

Edytuj profil strumienia używany do rejestracji:

4. Przejdź do okna System > Stream profiles (System > Profile strumienia) i wybierz profil strumienia.
5. Kliknij opcję Include audio (Dołącz audio) i włącz ją.
6. Kliknij przycisk Zapisz.

Łączenie się z głośnikiem sieciowym

Parowanie głośników sieciowych umożliwia korzystanie z kompatybilnego głośnika Axis tak, jakby był podłączony bezpośrednio do kamery. Po sparowaniu głośnik działa jako urządzenie audio, które umożliwia odtwarzanie klipów audio i przesyłanie dźwięku za pośrednictwem kamery.

Ważne

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

Sparuj kamerę z głośnikiem sieciowym

1. Przejdź do menu System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie).
2. Kliknij  Add (Dodaj) i wybierz typ parowania Audio z listy rozwijanej.
3. Wybierz opcję Speaker pairing (Parowanie głośnika).
4. Wpisz adres IP głośnika sieciowego, nazwę użytkownika i hasło.
5. Kliknij przycisk Połącz. Zostanie wyświetlony komunikat potwierdzający.

Łączenie się z mikrofonem sieciowym

Sparowanie mikrofonu sieciowego umożliwia korzystanie z kompatybilnego mikrofonu Axis tak, jakby był podłączony bezpośrednio do kamery. Po sparowaniu mikrofon sieciowy zbiera dźwięki z otoczenia i udostępnia je jako urządzenie wejściowe audio, wykorzystywane w strumieniach multimedialnych i zapisach.

Ważne

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

Sparuj kamerę z mikrofonem sieciowym

1. Przejdź do menu System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie).

2. Kliknij  **Add (Dodaj)** i wybierz typ parowania **Audio** z listy rozwijanej.
3. Wybierz polecenie **Microphone pairing (Parowanie mikrofonu)**.
4. Wpisz adres IP mikrofonu sieciowego, nazwę użytkownika i hasło.
5. Kliknij przycisk **Połącz**. Zostanie wyświetlony komunikat potwierdzający.

Zarządzanie listami

Dodawanie wykrytej tablicy rejestracyjnej do listy

Tablicę rejestracyjną można dodać do listy bezpośrednio po wykryciu jej przez aplikację.

1. Kliknij **Home** (Pozycja wyjściowa).
2. Przejdź do **Live** (Na żywo).
3. Kliknij ikonę strzałki na tablicy rejestracyjnej zapisanej na liście.
4. Kliknij **Append plate to list** (Dodaj tablicę rejestracyjną do listy).
5. Z okna dialogowego wybierz listę, do której chcesz dodać tablicę rejestracyjną.
6. Kliknij **Append (Dodaj)**.

Uwaga

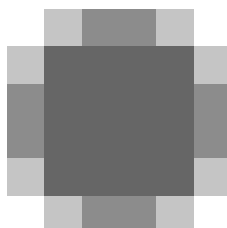
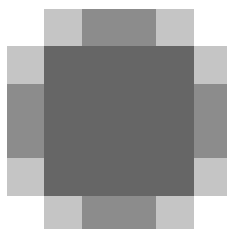
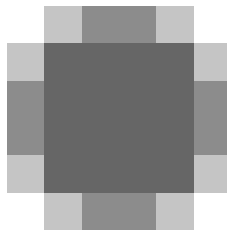
Sprawdź, czy symbole <, > oraz & nie są używane ani w tablicy rejestracyjnej, ani w opisie.

Dodawanie opisów do tablic rejestracyjnych

Aby dodać opis do tablicy rejestracyjnej na liście:

- Przejdź do **List management (Zarządzania listami)**.

- Wybierz tablicę rejestracyjną i kliknij



, a następnie z menu rozwijalnego wybierz **Edit** (Edycja).

- Wpisz odpowiednie informacje w polu **Description** (Opis).
- Kliknij przycisk **Zapisz**.

Uwaga

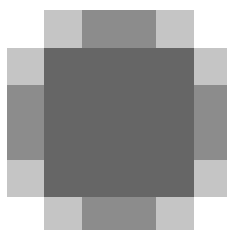
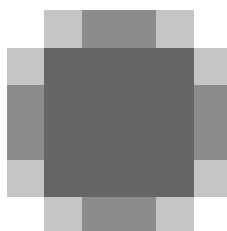
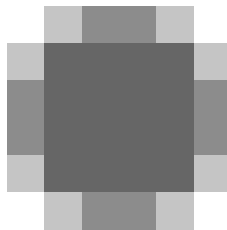
Dopilnuj, aby symbole <, > oraz & nie były używane ani w tablicach rejestracyjnych, ani w opisach.

Dostosowywanie nazw list

Można zmienić nazwy dowolnych list, aby dopasowywać je do konkretnych zastosowań.

- Przejdź do **List management** (Zarządzania listami).

2. Kliknij



obok listy, którą chcesz zmienić.

3. Wybierz **Edit (Edycja)**.
4. Wpisz nazwę listy.
5. Kliknij przycisk **Submit (Prześlij)**.

Nowa nazwa listy zostanie zaktualizowana we wszystkich istniejących konfiguracjach.

Importowanie numerów rejestracyjnych z listy dozwolonych

Można zaimportować numery rejestracyjne z listy dozwolonych z pliku .csv na komputerze. Oprócz numeru tablic rejestracyjnych można również dodać komentarze dla każdego numeru tablicy rejestracyjnej w pliku .csv.

Struktura pliku .csv musi wyglądać następująco: `license plate, date, description`

Przykład:

Tylko tablica rejestracyjna: `AXIS123`

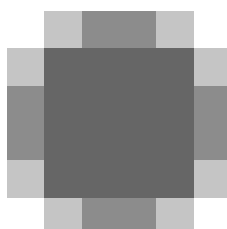
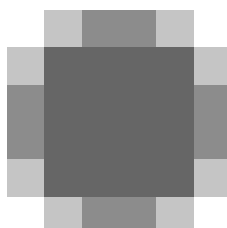
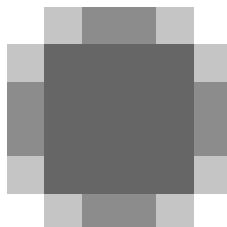
Tablica rejestracyjna + opis: `AXIS123, , John Smith`

Tablica rejestracyjna + data + opis: `AXIS123, 2022-06-08, John Smith`

Uwaga

Dopilnuj, aby symbole <, > oraz & nie były używane ani w tablicach rejestracyjnych, ani w opisach.

1. Przejdź do List management (Zarządzania listami)
2. Kliknij



obok Allowlist (Lista dozwolonych) i z rozwijalnego menu wybierz Import (Importuj).

3. Przejdź do pliku .csv na komputerze, aby go wybrać.
4. Kliknij OK.
5. Sprawdź, czy zaimportowane numery rejestracyjne wyświetlane są w polu Allowlist (Lista dozwolonych).

Udostępnianie listy tablic rejestracyjnych innym kamerom

Listę tablic rejestracyjnych można udostępniać innym kamerom w sieci. Synchronizacja zastąpi wszystkie bieżące listy tablic rejestracyjnych w innych kamerach.

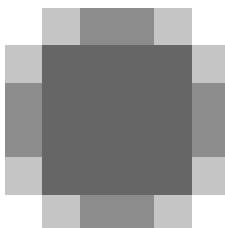
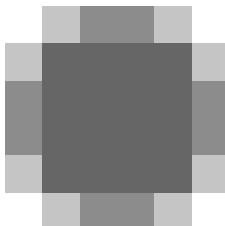
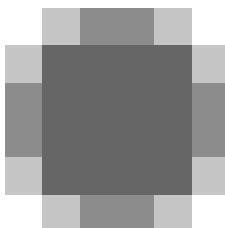
1. Przejdź do List management > List synchronization (Zarządzanie listą > Synchronizacja listy).
2. W sekcji Remote connected devices (Zdalny dostęp do dołączonych urządzeń) wpisz adres IP, nazwę użytkownika oraz hasło.
3. Kliknij Dodaj.

4. Kliknij **Synchronize list** (Synchronizuj listę).
5. Sprawdź, czy data i godzina w polu **Last sync (Ostatnia synchronizacja)** została zaktualizowana.

Tworzenie harmonogramów dla list

Dla list można utworzyć harmonogramy powodujące ich aktywność tylko w określonych porach wybranych dni tygodnia. Aby utworzyć harmonogram aktywności listy:

- Przejdź do **List management (Zarządzania listami)**.
- Kliknij



obok listy, którą chcesz zmienić.

- W menu rozwijalnym wybierz **Schedule** (Harmonogram).
- Wybierz godziny rozpoczęcia i zakończenia oraz dzień, w którym lista ma być aktywna.
- Kliknij przycisk obok pozycji **Enabled (Włączone)**.
- Kliknij przycisk **Zapisz**.

Ustawienia dodatkowe

Konfiguracja nakładki tekstowej

Nakładka tekstowa przedstawia następujące informacje o zdarzeniach w podglądzie na żywo: `weekday`, `month`, `time`, `year`, `license plate number`.

1. Przejdź do menu **Settings (Ustawienia) > Image (Obraz)**.
2. Aktywuj **Text overlay (Nałożenie tekstu)**.
3. Wybierz opcję **Timestamp and license plate (Znacznik czasu i tablica rejestracyjna)** lub **License plate only (Tylko tablica rejestracyjna)**.
4. Ustaw **Overlay duration (Czas nałożenia)** na wartość od 1 do 9 sekund.
5. Sprawdź, czy nakładka jest widoczna w podglądzie na żywo.

Detekcja tablic rejestracyjnych przy słabym oświetleniu

Algorytm przypisuje każdej dokonanej detekcji ocenę zwaną progiem ufności. Detekcje o ocenie poniżej wartości wybranego poziomu nie są wyświetlane na liście zdarzeń.

W scenach źle oświetlonych można ustawić niższy próg ufności, co umożliwi wykrycie większej liczby tablic rejestracyjnych.

1. Przejdź do **Settings > Recognition (Ustawienia > Rozpoznawanie)**.
2. Ustaw odpowiednio suwak w sekcji **Confidence threshold (Próg ufności)**.
3. Sprawdź, czy algorytm właściwie wykrywa tablice rejestracyjne.

Dopuszczanie mniejszej liczby znaków na tablicach rejestracyjnych

Aplikacja ma domyślną minimalną liczbę znaków, jaka może zostać wykryta przez tablicę rejestracyjną. Domyślna minimalna liczba znaków wynosi pięć. Aplikację można skonfigurować tak, aby nie wykrywała tablic rejestracyjnych o mniejszej liczbie znaków.

1. Przejdź do **Settings > Recognition (Ustawienia > Rozpoznawanie)**.
2. W sekcji **Number of characters (Liczba znaków)** przesun suwak, aby ustawić minimalną liczbę znaków, na jaką chcesz zezwolić.
3. Sprawdź, czy aplikacja właściwie rozpoznaje tablice rejestracyjne.

Dopasowywanie wyłącznie identycznych tablic rejestracyjnych

Algorytm dopasowywania automatycznie zezwala na różnice jednego znaku podczas dopasowywania wykrytej tablicy rejestracyjnej do listy dozwolonych lub listy blokowanych. W niektórych scenariuszach jednak konieczne jest dopasowanie wszystkich znaków tablicy rejestracyjnej.

1. Przejdź do **List management (Zarządzania listami)**.
2. Kliknij, aby włączyć opcję **Strict matching (Dokładne dopasowanie)**.
3. Sprawdź, czy aplikacja właściwie dopasowuje tablice rejestracyjne.

Zezwalanie na różnicę więcej niż jednego znaku podczas dopasowywania tablic rejestracyjnych

Algorytm dopasowywania automatycznie zezwala na różnice jednego znaku podczas dopasowywania wykrytej tablicy rejestracyjnej do listy dozwolonych lub listy blokowanych. Możliwe jest zezwalanie na różnicę więcej niż jednego znaku.

1. Przejdź do **Settings > Recognition (Ustawienia > Rozpoznawanie)**.

2. W polu **Allowed character deviation (Dozwolone różne znaki)** wybierz ile znaków, może się różnić.
3. Sprawdź, czy aplikacja właściwie dopasowuje tablice rejestracyjne.

Przyznawanie ograniczonego dostępu operatorom

Operatorom można przyznać ograniczony dostęp do aplikacji za pośrednictwem adresu URL. W ten sposób zyskują dostęp tylko do obszarów **Event log (Dziennik zdarzeń)** i **List management (Zarządzanie listami)**. Adres URL znajduje się w sekcji **Settings > User rights (Ustawienia > Prawa użytkownika)**.

Konfiguracja bezpiecznych połączeń

Aby chronić komunikację i dane przesyłane między urządzeniami, na przykład pomiędzy kamerą a kontrolerem drzwi, skonfiguruj bezpieczne połączenie przez protokół HTTPS za pomocą certyfikatów.

1. Przejdź do menu **Settings (Ustawienia) > Security (Zabezpieczenia)**.
2. W sekcji HTTPS wybierz opcję **Self-signed (Samopodpisany)** albo **CA-signed (Z podpisem UC)**.

Uwaga

Więcej informacji o protokole HTTPS i jego zastosowaniach na stronie: .

Tworzenie kopii zapasowych i przywracanie ustawień aplikacji

Można tworzyć kopie zapasowe i przywracać ustawienia wprowadzone w aplikacji dotyczące rejestrowania obrazów, bezpieczeństwa, wykrywania i integracji. W razie późniejszych problemów można po prostu przywrócić ustawienia z kopii zapasowej.

Aby utworzyć kopię zapasową ustawień aplikacji:

- Przejdź do menu **Settings > Maintenance (Ustawienia > Konserwacja)**.
- Kliknij **Download backup configuration** (Pobierz kopię zapasową konfiguracji).

Do folderu pobierania zostanie pobrany plik JSON.

Aby przywrócić ustawienia aplikacji:

- Przejdź do menu **Settings > Maintenance (Ustawienia > Konserwacja)**.
- Kliknij opcję **Restore configuration (Przywróć konfigurację)**.

Zaznacz plik JSON zawierający kopię zapasową.

Ustawienia zostaną przywrócone automatycznie.

Kasowanie wszystkich zdarzeń

Po skonfigurowaniu aplikacji warto usunąć z procesu konfiguracji ślady wszystkich obrazów i zarejestrowanych tablic.

Aby wykasować wszystkie obrazy i tablice z bazy danych:

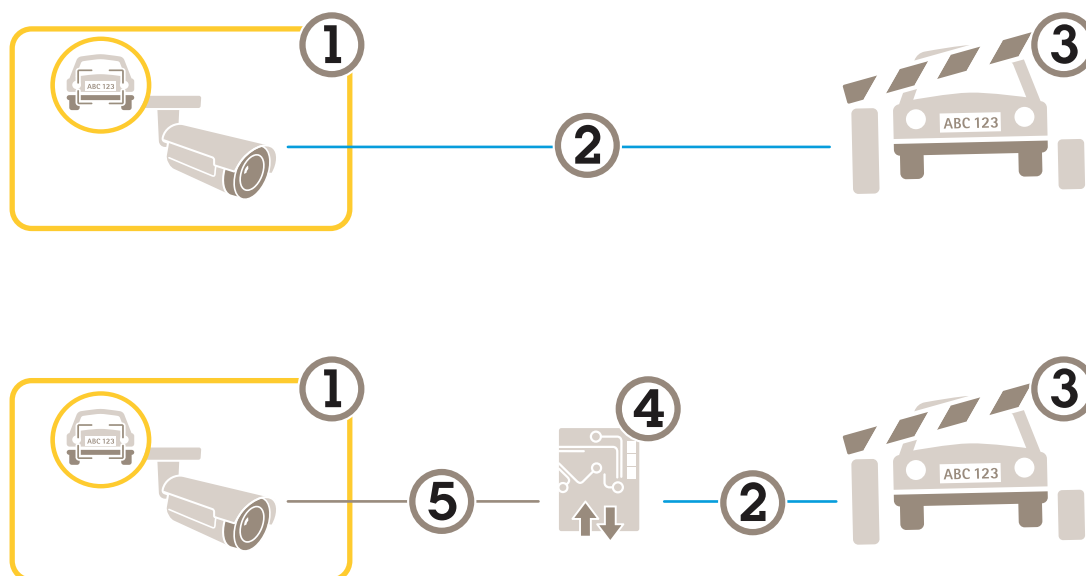
Przejdź do menu **Settings > Maintenance (Ustawienia > Konserwacja)**.

- Kliknij opcję **Clear all recognition results (Usuń wszystkie rezultaty rozpoznawania)**.
- Kliknij **Tak**.

Scenariusz wjazdu i wyjazdu pojazdów

W scenariuszu wjazdu i wyjazdu pojazdów aplikacja odczytuje tablicę rejestracyjną zarejestrowaną przez kamerę i weryfikuje ją na podstawie listy autoryzowanych i nieautoryzowanych tablic rejestracyjnych zapisanej w kamerze.

Ten scenariusz wymaga aplikacji zainstalowanej w kamerze z obsługą I/O lub podłączonego modułu przekaźnika I/O w celu otwierania i zamykania szlabanu.



Dwie przykładowe konfiguracje dla scenariusza wjazdu i wyjazdu.

- 1 Kamera Axis z aplikacją AXIS License Plate Verifier
- 2 Komunikacja I/O
- 3 Szlaban
- 4 Moduł przekaźnikowy I/O Axis
- 5 Komunikacja IP

Powiadomienia dotyczące nieautoryzowanych pojazdów

W tym przykładzie wyjaśniono, jak skonfigurować aplikację, aby utworzyć w kamerze zdarzenie wyzwalające wysłanie powiadomienia.

Wymagania:

- Konfiguracja podstawowa. Patrz *Konfiguracja podstawowa, on page 8*.
1. Przejdź do List management (Zarządzania listami).
 2. Wprowadź numer tablicy rejestracyjnej w polu Blocklist (Lista blokowanych).
 3. Przejdź na stronę internetową kamery.
 4. Przejdź do Settings (Ustawienia) > Events (Zdarzenia) i skonfiguruj regułę akcji, w której warunkiem jest aplikacja, a akcją – powiadomienie.
 5. Sprawdź, czy aplikacja rozpoznaje dodany numer tablicy rejestracyjnej jako tablicę nieautoryzowanego pojazdu, i czy reguła akcji działa zgodnie z oczekiwaniami.

Scenariusz swobodnego przepływu z pomiarem prędkości

W scenariuszu swobodnego przepływu z pomiarem prędkości kamera jest sparowana z radarem Axis dzięki technologii edge-to-edge. Kamera obejmuje dwa pasy ruchu i odczytuje tablice rejestracyjne przejeżdżających pojazdów. Sparowany radar mierzy prędkość tych pojazdów. Ponadto aplikacja *AXIS Speed Monitor* może wizualizować maksymalną prędkość na każdym pasie ruchu poprzez nałożenia w podglądzie na żywo kamery.

Aby dowiedzieć się więcej o technologii edge-to-edge, zobacz *Technologia edge-to-edge, on page 46*.

Wymagania:

- Zestaw z kamerą, AXIS License Plate Verifier oraz radarem *AXIS D2210-VE Radar* został zainstalowany i podłączony do sieci

Konfigurowanie scenariusza

Skonfiguruj scenariusz w czterech krokach: najpierw skonfiguruj kamerę, następnie sparuj i skonfiguruj radar, a na zakończenie użyj aplikacji *AXIS Speed Monitor*, aby dodać nakładki.

Zanim zaczniesz:

- Upewnij się, że kamera i radar są skierowane na ten sam obszar zainteresowania.
- Upewnij się, że został zsynchronizowany czas między kamerą i radarem. Aby sprawdzić status, przejdź do menu *Installation > Time sync status (Instalacja > Status synchronizacji czasu)* w obu urządzeniach.

Konfiguracja kamery:

1. Skonfiguruj kamerę, postępując zgodnie z instrukcjami przedstawionymi w *Konfiguracja podstawowa, on page 8*.
2. Korzystając z pomocy asystenta ustawień wybierz swobodny przepływ. Więcej informacji znajduje się w rozdziale *Swobodny przepływ, on page 10*.

Parowanie kamery z radarem:

1. Otwórz interfejs WWW kamery i przejdź do menu *System > Edge-to-edge > Radar pairing (System > Łączność edge-to-edge > Parowanie radaru)*.
2. Wprowadź nazwę hosta, nazwę użytkownika i hasło radaru.
3. Kliknij **Connect (Połącz)**, aby sparować urządzenia.
Gdy nastąpi połączenie urządzeń, ustawienia radaru będą dostępne w interfejsie WWW kamery.

Uwaga

Domyślna rozdzielczość sparowanego radaru wynosi 1280x720. Zachowaj domyślną rozdzielczość radaru w interfejsie WWW kamery i w przypadku dodawania urządzenia do systemu VMS.

Konfigurowanie radaru:

1. W interfejsie WWW kamery przejdź do *Radar > Scenarios (Radar > Scenariusze)*.
2. Dodaj jeden scenariusz radaru obejmujący jeden pas ruchu i kolejny scenariusz radaru obejmujący drugi pas ruchu.
3. W obu scenariuszach wybierz opcję **Movement in area (Ruch w obszarze)**, wyzwalanie przez **Vehicles (Pojazdy)**, a następnie ustaw **Speed limit (Ograniczenie prędkości)**.
Aby uzyskać dodatkowe informacje, przejdź do menu *Add scenarios (Dodaj scenariusze)* w instrukcji obsługi urządzenia AXIS D2210-VE Radar.

Uwaga

Aby dodać nałożenia z numerami tablic rejestracyjnych w aplikacji *AXIS License Plate Verifier*, musisz je ustawić, zanim dodasz nałożenia w aplikacji *AXIS Speed Monitor*.

Dodawanie nałożeń z informacją o prędkości w aplikacji *AXIS Speed Monitor*:

1. Pobierz i zainstaluj w kamerze aplikację *AXIS Speed Monitor*.
2. Dodaj po jednym nałożeniu dla każdego pasa. Będą one wyświetlały prędkość maksymalną w podglądzie na żywo z kamery.
Informacje o instalacji i konfiguracji znajdziesz w *instrukcji obsługi aplikacji AXIS Speed Monitor*.

Wyszukiwanie określonych zdarzeń

Funkcja wyszukiwania umożliwia znajdowanie zdarzeń na podstawie szeregu kryteriów.

1. Przejdź na stronę internetową aplikacji i wybierz stronę **Search** (Wyszukiwanie).
2. Z menu kalendarza wybierz daty **From (Od)** i **To (Do)**.
3. Kliknij menu rozwijalne **AOI** (Obszar zainteresowania), aby wybrać obszar, który ma być uwzględniony w wyszukiwaniu.
4. Wybierz **Direction (Kierunek)**, aby filtrować według wejścia lub wyjścia.
5. Wprowadź numer tablicy rejestracyjnej w polu **Plate (Tablica)**, aby wyszukać tablicę rejestracyjną.
6. Aby odnaleźć tablice rejestracyjne należące do określonego kraju, wybierz kraj z listy rozwijalnej **Country** (Kraj).
7. Aby odfiltrować obrazy na podstawie widoku pojazdu, z listy rozwijalnej wybierz **Front** (Przód) lub **Rear** (Tył) w sekcji **Vehicle view** (Widok pojazdu).
8. Aby odfiltrować wyniki wyszukiwania na podstawie marki, modelu, rodzaju lub koloru pojazdu, wybierz odpowiednią opcję wyglądu z menu rozwijalnych **Vehicle details** (Informacje o pojeździe).
9. Kliknij **Apply filters** (Zastosuj filtry), aby wyświetlić wyniki wyszukiwania.

Eksportowanie i udostępnianie wyników wyszukiwania

Aby wyeksportować wyniki wyszukiwania jako plik CSV ze statystykami z danej godziny, kliknij przycisk **Export** (Eksportuj) w celu zapisania wyników w pliku CSV.

Aby skopiować interfejs API jako łącze, które można wykorzystać do eksportowania danych do systemów innych firm, kliknij **Copy search link** (Kopiuje łącze wyszukiwania).

Integracja

Używanie profili w celu wysyłania zdarzeń do różnych serwerów

Za pomocą profili można wysyłać zdarzenia do różnych serwerów równocześnie przy użyciu różnych protokołów. Aby używać profili:

1. Przejdź do **Integration (Integracja)** i strony **Push events (Zdarzenia typu push)**.
2. Wybierz **Profile 1 (Profil 1)**.
3. Skonfiguruj regułę. Patrz *Komunikat typu push o zdarzeniu przesyłany do oprogramowania innych firm, on page 37*.
4. Testowanie reguły.
5. Wybierz nową kartę profilu, aby skonfigurować nową regułę.

Komunikat typu push o zdarzeniu przesyłany do oprogramowania innych firm

Uwaga

Aplikacja wysyła informacje o zdarzeniach w formacie JSON. Aby uzyskać więcej informacji, *zaloguj się przy użyciu konta MyAxis*, przejdź do *biblioteki AXIS VAPIX* i wybierz **AXIS License Plate Verifier**

Dzięki tej funkcji można zintegrować oprogramowanie innych firm, przysyłając dane zdarzeń za pośrednictwem protokołu TCP lub HTTP POST jako komunikat typu push.

Zanim zaczniesz:

- Kamera musi być zamontowana i podłączona do sieci.
 - Aplikacja **AXIS License Plate Verifier** musi być uruchomiona w kamerze.
1. Przejdź do opcji **Integration (Integracja) > Push events (Zdarzenia typu push)**.
 2. Wybierz pusty profil
 3. Na liście rozwijalnej **Protocol (Protokół)** wybierz **HTTP POST**.
 4. W polu **Server URL (Adres URL serwera)** wpisz adres serwera i port w następującym formacie:
127.0.0.1:8080
 5. Wprowadź nazwę użytkownika i hasło.
 6. Jeżeli korzystasz z serwera proxy, włącz go i wpisz nazwę hosta, nazwę użytkownika i hasło.
 7. W polu **Device ID (ID urządzenia)** wpisz nazwę urządzenia lub pozostaw pole bez zmian.
 8. W sekcji **Push conditions (Warunki zdarzeń typu push)** wybierz kierunek wyzwalania zdarzeń typu push.
 9. W sekcji **LPR Event types (Rodzaje zdarzeń rozpoznawania numerów tablic rejestracyjnych)** wybierz jedną lub więcej następujących opcji:
 - **New (Nowe)** oznacza pierwsze wykrycie tablicy rejestracyjnej.
 - **Update (Aktualizacja)** jest poprawieniem znaków na wcześniej wykrytej tablicy rejestracyjnej lub po wykryciu kierunku przemieszczania się tablicy rejestracyjnej i śledzeniu jej na obrazie.
 - **Lost (Utrata)** to ostatnie monitorowane zdarzenie dotyczące tablicy rejestracyjnej, zanim opuści ona obszar obrazu. Zawiera również kierunek poruszania się tablic rejestracyjnych.
 - **Conditional (Warunkowy)** wysyła jedno zdarzenie dotyczące jednego obiektu po spełnieniu warunków.
 10. Aby zmniejszyć przepustowość podczas korzystania z protokołu HTTP POST, można wybrać opcję **Do not to send images (Nie wysyłaj obrazów)**.
 11. Włącz **Event buffer (Bufor zdarzeń)**, aby buforować zdarzenia w razie niedostępności serwera i wysłać je, gdy serwer będzie ponownie dostępny.
 12. Aby oprócz zdjęcia dołączyć wycinek tablicy rejestracyjnej, jeżeli wybrałeś **Retention settings (Ustawienia przechowywania)**, wybierz **Send two images (Wyślij dwa obrazy)**.

13. Aby wysłać zdarzenia w formacie wieloczęściowym zamiast base64, wybierz **Multipart** (Wieloczęściowe).
14. Kliknij **Test** (Testuj), aby przetestować integrację z wirtualną tablicą rejestracyjną.
15. Aby włączyć tę funkcję, wybierz **Activate** (Uaktywnij).

Uwaga

Aby wysłać informacje o zdarzeniach za pomocą metody HTTP POST, możesz użyć nagłówka autoryzacji zamiast nazwy użytkownika i hasła. Przejdź do **Auth-Header** (Nagłówek autoryzacji) i dodaj ścieżkę do interfejsu API uwierzytelniania.

Wysyłanie obrazu z tablic rejestracyjnych do serwera

Funkcja ta pozwala przysyłać obrazy tablic rejestracyjnych do serwera przy użyciu protokołu FTP.

Zanim zaczniesz:

- Kamera musi być zamontowana i podłączona do sieci.
 - Aplikacja AXIS License Plate Verifier musi być uruchomiona w kamerze.
1. Przejdź do opcji **Integration (Integracja) > Push events (Zdarzenia typu push)**.
 2. Na liście rozwijanej **Protocol (Protokół)** wybierz **FTP**.
 3. W polu **Server URL (Adres URL serwera)** wpisz adres serwera w następującym formacie: `ftp://10.21.65.77/LPR`.
 4. Wpisz nazwę użytkownika i hasło serwera FTP.
 5. Wybierz ścieżkę i modyfikatory nazw plików.
 6. W polu **Device ID (ID urządzenia)** wpisz nazwę urządzenia. Zostanie utworzony folder o tej nazwie przeznaczony do przechowywania obrazów. Obrazy są tworzone w następującym formacie: `znacznik_czasowy_obszar_zainteresowania_kierunek_ID_samochodu_treść_tablicy_rejestracyjnej_kraj.jpg`.
 7. W sekcji **Push conditions** (Warunki zdarzeń typu push) wybierz kierunek wyzwalania zdarzeń typu push.
 8. W polu **Event types (Typy zdarzeń)** wybierz jedną lub więcej następujących opcji:
 - **New (Nowe)** oznacza pierwsze wykrycie tablicy rejestracyjnej.
 - **Update (Aktualizacja)** jest poprawieniem znaków na wcześniej wykrytej tablicy rejestracyjnej lub po wykryciu kierunku przemieszczania się tablicy rejestracyjnej i śledzeniu jej na obrazie.
 - **Lost (Utrata)** to ostatnie monitorowane zdarzenie dotyczące tablicy rejestracyjnej, zanim opuści ona obszar obrazu. Zawiera również kierunek poruszania się tablic rejestracyjnych.
 - **Conditional** (Warunkowy) wysyła jedno zdarzenie dotyczące jednego obiektu po spełnieniu warunków.

Uwaga

Kierunek jest uwzględniany w nazwie pliku tylko w przypadku wybrania opcji **Lost (Utrata)** lub **Update (Aktualizacja)**.

9. Kliknij **Test** (Testuj), aby przetestować integrację z wirtualną tablicą rejestracyjną.
10. Aby włączyć tę funkcję, kliknij **Activate** (Uaktywnij).

Uwaga

Uwaga: obraz może się różnić w zależności od wybranego trybu rejestracji. Patrz *Dostosowywanie ustawień przechwytywania obrazu, on page 12*.

Uwaga

Jeśli wystąpią błędy dotyczące zdarzeń typu push, aplikacja ponownie wyśle na serwer do 100 pierwszych nieudanych zdarzeń.

W przypadku korzystania z protokołu FTP w zdarzeniach typu push kierowanych na serwer Windows, do tworzenia nazw obrazów nie należy używać funkcji `%c` podającej datę i godzinę. Wynika to z faktu, że system Windows nie akceptuje nazw ustawionych przez funkcję `%c` przeznaczoną do daty i godziny. Ten problem nie występuje w przypadku korzystania z serwera Linux.

Bezpośrednia integracja z 2N

W tym przykładzie opisano bezpośrednią integrację z urządzeniem 2N IP.

Skonfiguruj konto w urządzeniu 2N:

1. Przejdź do 2N IP Verso.
2. Przejdź do menu **Services (Usługi) > HTTP API > Account 1 (Konto 1)**.
3. Wybierz opcję **Enable account (Aktywuj konto)**.
4. Wybierz opcję **Camera access (Dostęp do kamery)**.
5. Wybierz pozycję **License plate recognition (Rozpoznawanie tablic rejestracyjnych)**.
6. Skopiuj adres IP.

W aplikacji AXIS License Plate Verifier:

1. Przejdź do menu **Integration (Integracja) > Direct integration (Bezpośrednia integracja)**.
2. Zaznacz **2N IP Device (Urządzenie IP 2N)**.
3. Dodaj adres IP lub URL w urządzeniu 2N.
4. Wpisz swoją nazwę użytkownika i hasło.
5. Wybierz **Connection type (Typ połączenia)**.
6. Wybierz, do czego będzie używana ten szlaban.
7. Kliknij przycisk **Enable integration (Włącz integrację)**.
8. Wybierz kierunek ruchu pojazdów.
9. Aby włączyć tę funkcję, wybierz **Activate (Uaktywnij)**.

Aby sprawdzić, czy integracja działa:

1. Przejdź do 2N IP Verso.
2. Przejdź do menu **Status > Events (Zdarzenia)**.

Integracja z systemem Genetec Security Center

W tym przykładzie opisano konfigurowanie bezpośredniej integracji z oprogramowaniem Genetec Security Center.

W programie Genetec Security Center:

1. Przejdź do obszaru **Overview (Informacje ogólne)**.
2. Upewnij się, że usługi **Database (Baza danych)**, **Directory (Katalog)** i **License (Licencja)** są aktywne. Jeśli tak nie jest, uruchom wszystkie usługi Genetec i SOLEXPRESS w systemie Windows.
3. Przejdź do okna **Genetec Config Tool (Narzędzie konfiguracyjne Genetec) > Plugins (Wtyczki)**.
4. Kliknij przycisk **Add an entity (Dodaj jednostkę)**.
5. Przejdź do obszaru **Plugin (Wtyczka)** i wybierz opcję **LPR plugin (Wtyczka LPR)**.
6. Kliknij **Next (Dalej)**.
7. Kliknij **Next (Dalej)**.
8. Kliknij **Next (Dalej)**.
9. Zaznacz dodaną wtyczkę LPR i przejdź do okna **Data sources (Źródła danych)**.

W ustawieniu **ALPR reads API (ALPR odczytuje API)**:

10. Zaznacz opcję **Enabled (Włączone)**.
11. W polu **Name (Nazwa)** wpisz: **Plugin REST API (Wtyczka REST API)**.
12. W polu **API path prefix (Prefiks ścieżki interfejsu API)** wpisz: **lpr**.

13. W polu **REST port (Port REST)** wybierz wartość 443.
14. W polu **WebSDK host (Host WebSDK)** wpisz: localhost.
15. W polu **WebSDK port (Port WebSDK)** wybierz wartość 443.
16. Zaznacz opcję **Allow self-signed certificates (Zezwalaj na certyfikaty z własnym podpisem)**.

W ustawieniu **Security Center events data source (Źródła danych zdarzeń programu Security Center)**:

17. Zaznacz opcję **Enabled (Włączone)**.
18. W polu **Name (Nazwa)** wpisz **Security Center Lpr Events (Zdarzenia Lpr w programie Security Center)**.
19. W ustawieniu **Processing frequency (Częstotliwość przetwarzania)** w menu rozwijanym zaznacz wartość 5 sec (5 s).
20. Przejdź do karty **Data sinks (Ujęcia danych)**.
21. Kliknij **+**.
22. W ustawieniu **Type (Typ)** zaznacz opcję **Database (Baza danych)**.
23. Wybierz i skonfiguruj bazę danych:
 - Zaznacz opcję **Enabled (Włączone)**.
 - W polu **Source (Źródło)** zaznacz pozycje **Plugin REST API (Wtyczka REST API)** i **Native ALPR Events (Macierzyste zdarzenia ALPR)**.
 - W polu **Name (Nazwa)** wpisz **Reads DB (Odczyty bazy danych)**.
 - W polu **Include (Dołącz)** zaznacz pozycje **Reads (Odczyty)**, **Hits (Trafienia)** i **Images (Obrazy)**.
 - Przejdź do karty **Resources (Zasoby)**.
 - Kliknij kolejno opcje **Delete the database (Usuń bazę danych)** i **Create a database (Utwórz bazę danych)**.

Tworzenie użytkownika interfejsu API:

24. Przejdź do okna **Config Tool > User Management (Narzędzie konfiguracyjne > Zarządzanie użytkownikami)**.
25. Kliknij przycisk **Add an entity (Dodaj jednostkę)**.
26. Zaznacz opcję **User (Użytkownik)**.
27. Wpisz nazwę użytkownika i hasło. Pozostaw pozostałe pola bez zmian.
28. Zaznacz dodanego użytkownika i przejdź do karty **Privileges (Uprawnienia)**.
29. W obszarze **Application privileges (Uprawnienia do aplikacji)** przyznaj wszystkie uprawnienia, zaznaczając odpowiednie opcje.
30. Zaznacz opcję zezwolenia na uprawnienie **Third-party ALPR reads API (Zewnętrzny ALPR czyta API)**.
31. Kliknij przycisk **Apply (Zastosuj)**.

W aplikacji **AXIS License Plate Verifier**:

1. Przejdź do **Integration > Direct integration (Integracja > Bezpośrednia integracja)**.
2. Wybierz **Genetec Security Center (Centrum bezpieczeństwa Genetec)**.
3. W polu **URL/IP** wpisz adres zgodnie z tym szablonem: `https://server-address/api/V1/lpr/lpringestion/reads`.
4. Wpisz nazwę użytkownika i hasło dostępu do systemu Genetec.
5. Wybierz **Connection type (Typ połączenia)**.
6. Aby włączyć tę funkcję, wybierz **Activate (Uaktywnij)**.
7. Kliknij **Test (Testuj)**, aby przetestować integrację z wirtualną tablicą rejestracyjną.
8. Jeżeli wybrałeś protokół HTTPS, przejdź do karty **Settings (Ustawienia)**.
9. W ustawieniu **Security > HTTPS (Zabezpieczenia > HTTPS)**.

10. Zaznacz opcję **Self-signed** (Z własnym podpisem) lub **CA-signed** (Z podpisem urzędu certyfikacji), zależnie od ustawień w programie Genetec Security Center.

W programie Genetec Security Center:

1. Przejdź do okna **Genetec Security Desk**.
2. W ustawieniu **Investigation (Dochodzenie)** kliknij opcję **Reads (Odczyty)**.
3. Przejdź do karty **Reads (Odczyty)**.
4. Wyfiltruj wyniki zgodnie ze swoimi potrzebami.
5. Kliknij **Generate report (Generuj raport)**.

Uwaga

W dokumentacji Genetec znajdziesz również informacje o integrowaniu zewnętrznych wtyczek ALPR. *Można to zrobić tutaj (wymaga rejestracji).*

Interfejs WWW

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

Więcej informacji

Tryby rejestracji

Wybór trybu rejestracji zależy od wymagań dotyczących poklatkowości i rozdzielczości w określonej konfiguracji dozoru. Specyfikacje dostępnych trybów rejestracji znajdują się w opisach produktów na stronie axis.com.

Funkcja zdalnego ustawiania ostrości i zbliżenia

Funkcja zdalnego ustawiania ostrości i zoomu umożliwia regulację ostrości i zoomu kamery przy użyciu komputera. W ten sposób można wygodnie sprawdzić, czy ostrość sceny, kąt widzenia i rozdzielczość są optymalne bez konieczności udawania się do miejsca, gdzie zainstalowano kamerę.

Maski prywatności

Maska prywatności to zdefiniowany przez użytkownika obszar, który zasłania część monitorowanego obszaru. Maski prywatności wyświetlane są jako bloki koloru lub mozaika zastosowane na strumieniu wideo.

Maska prywatności jest zgodna ze współrzędnymi obrotu, pochyleń i zbliżenia – niezależnie od miejsca, w którym znajduje się kamera, maska prywatności pokrywa to samo miejsce lub obiekt.

Maska prywatności znajduje się na wszystkich zrzutach ekranu, zarejestrowanych obrazach i strumieniach podglądu na żywo.

Aby ukryć maskę prywatności, można użyć interfejsu VAPIX® Application Programming Interface (API).

Ważne

Dodanie wielu masek prywatności może wpłynąć na pracę urządzenia.

Można utworzyć kilka masek prywatności. Każda maska może mieć od 3 do 10 punktów kotwiczenia.

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.

Uwaga

Nakładki są umieszczane we wszystkich strumieniach wizyjnych z wyjątkiem połączeń SIP, gdy połączenie odbywa się przy zasilaniu PoE klasy 3.

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.

W jaki sposób ustawienia obrazu, strumienia i profilu strumienia mogą na siebie wpływać?

Karta **Obraz** zawiera ustawienia kamery, które wpływają na wszystkie strumienie wideo przesyłane z produktu. Jeśli zmienisz parametry na tej karcie, natychmiast wpłynie to na wszystkie strumienie wideo i zapisy.

Karta **Strumień** zawiera ustawienia strumienia wideo. Te ustawienia są stosowane, gdy żądasz strumienia wideo z produktu, ale nie podasz na przykład rozdzielczości lub poklatkowości. Zmiana ustawień na karcie **Strumień** nie wpływa na bieżące strumienie, ale będzie wprowadzona po rozpoczęciu nowego strumienia.

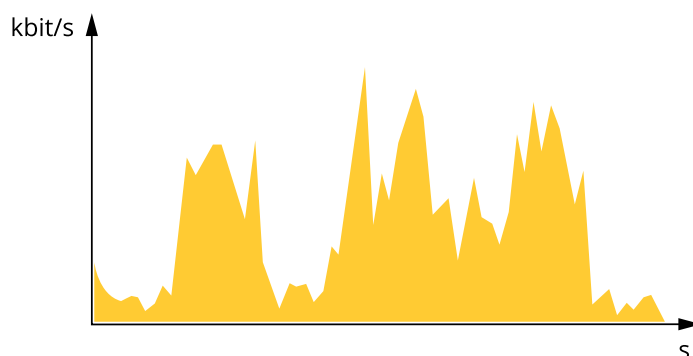
Ustawienia w opcji **Profile strumienia** nadpisują ustawienia z karty **Strumień**. Jeśli zażądasz strumienia z określonym profilem, to strumień będzie mieć ustawienia tego profilu. Jeśli zażądasz strumienia bez określania profilu lub zażądasz profilu strumienia, który nie został zdefiniowany w produkcie, strumień będzie mieć ustawienia z karty **Strumień**.

Sterowanie przepływnością bitową

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

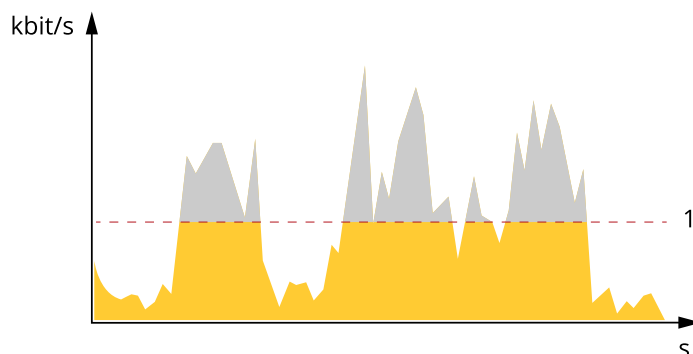
Zmienna przepływność bitowa (VBR)

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

**Maksymalna przepływność bitowa (MBR)**

Opcja ta umożliwia ustawienie docelowej przepływności bitowej w celu kontrolowania zajętości pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości

obrazu lub niższa poklatkowość. Jak priorytet można wybrać opcję ustawienia jakości obrazu lub poklatkowości. Zalecamy skonfigurowanie docelowej wartości przepływności bitowej na wartość większą niż oczekiwana. Dzięki temu można zachować margines, jeśli w scenie występuje wysoki poziom aktywności.

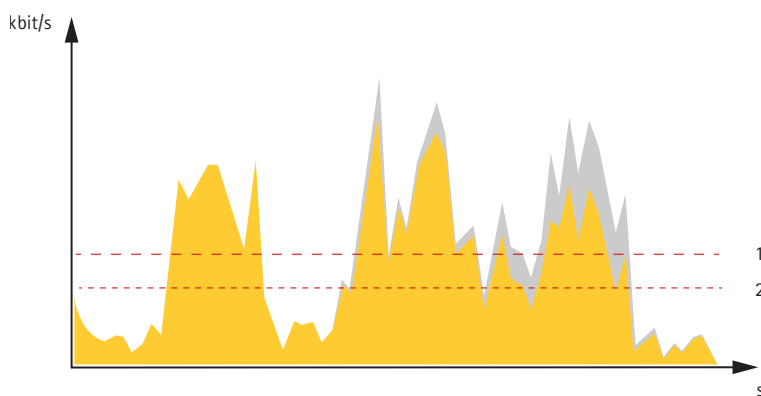


1 Docel. przepł. bitowa

Średnia przepływność bitowa (ABR)

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

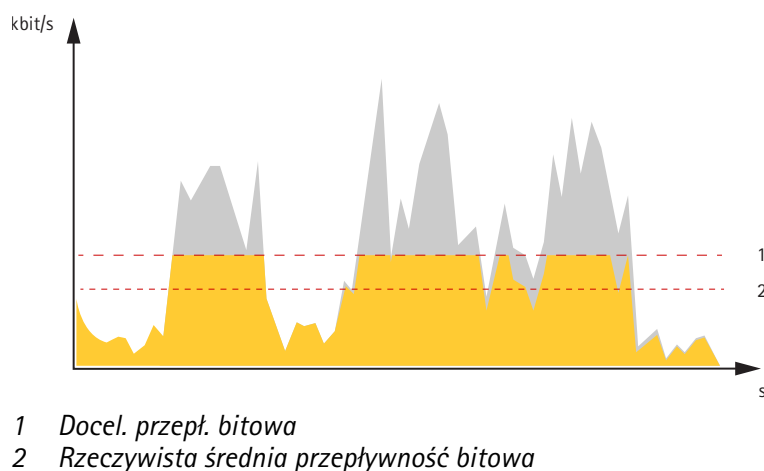
- Aby obliczyć przybliżone zapotrzebowanie na zasoby pamięci masowej, należy ustawić wartość docelową przepływności bitowej i czas retencji.
- Użyj kalkulatora przepływności bitowej, aby obliczyć średnią przepływność bitową w zależności od dostępnego miejsca w zasobach pamięci i czasu retencji.



1 Docel. przepł. bitowa

2 Rzeczywista średnia przepływność bitowa

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



Technologia edge-to-edge

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

Uwaga

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

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

Parowanie głośnika

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

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

Parowanie mikrofonu

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

Parowanie radaru

Dzięki parowaniu radarów w technologii edge-to-edge można podłączyć kamerę do kompatybilnego radaru Axis i korzystać z jego wbudowanych funkcji, takich jak wykrywanie prędkości.

Parowanie radarów jest konfiguracją jednokierunkową, gdzie jedna kamera jest parowana z jednym radarem i służy do konfiguracji i obsługi obu urządzeń. Po sparowaniu można uzyskać dostęp do ustawień radaru i tworzyć reguły dla zdarzeń specyficznych dla radaru bezpośrednio w interfejsie WWW kamery. Kamera identyfikuje się w systemie VMS jako kamera z radarem.

Kamera ma przydzielony kanał na potrzeby strumienia radaru, a po sparowaniu strumień radaru zostaje automatycznie przypisany do tego kanału.

Ponadto po sparowaniu metadane radaru są dostępne za pośrednictwem oferowanych przez kamerę kanałów producenta metadanych. Jeśli sama kamera ma jeden kanał, metadane radaru są dostępne za pośrednictwem drugiego kanału.

Parowanie sieciowe

Dzięki funkcji parowania sieciowego „edge-to-edge” możesz połączyć kamerę z kompatybilnym urządzeniem Axis zawierającym funkcję sygnalizacji akustycznej oraz optycznej lub oświetlacza i korzystać z jego wbudowanych funkcji.

Analizy i aplikacje

Analizy i aplikacje pozwalają lepiej wykorzystać potencjał urządzeń Axis. AXIS Camera Application Platform (ACAP) to otwarta platforma umożliwiająca podmiotom zewnętrznym opracowywanie funkcji analizy i innych aplikacji dla urządzeń Axis. Aplikacje mogą być fabrycznie zainstalowane na urządzeniu, dostępne do pobrania za darmo lub oferowane za opłatą licencyjną.

Podręczniki użytkownika do analiz i aplikacji Axis można znaleźć na stronie help.axis.com.

Uwaga

- Kilka aplikacji może być uruchomionych w tym samym czasie, ale niektóre z nich mogą ze sobą nie współpracować. Niektóre zestawy aplikacji mogą wymagać zbyt wiele mocy obliczeniowej lub pamięci przy ich jednoczesnym uruchomieniu. Przed uruchomieniem aplikacji należy sprawdzić, czy mogą one być uruchomione jednocześnie.

AXIS Image Health Analytics

AXIS Image Health Analytics to aplikacja oparta na sztucznej inteligencji, która może służyć do detekcji degradacji obrazu lub prób sabotażu. Aplikacja analizuje zachowania w scenie i uczy się ich w celu wykrywania rozmycia lub niedoświetlenia obrazu, a także detekcji zasłoniętego lub przekierowanego widoku. Aplikację można skonfigurować tak, aby wysyłała zdarzenia w przypadku każdej z tych detekcji i wyzwała akcje za pośrednictwem systemu zdarzeń kamery lub oprogramowania firm trzecich.

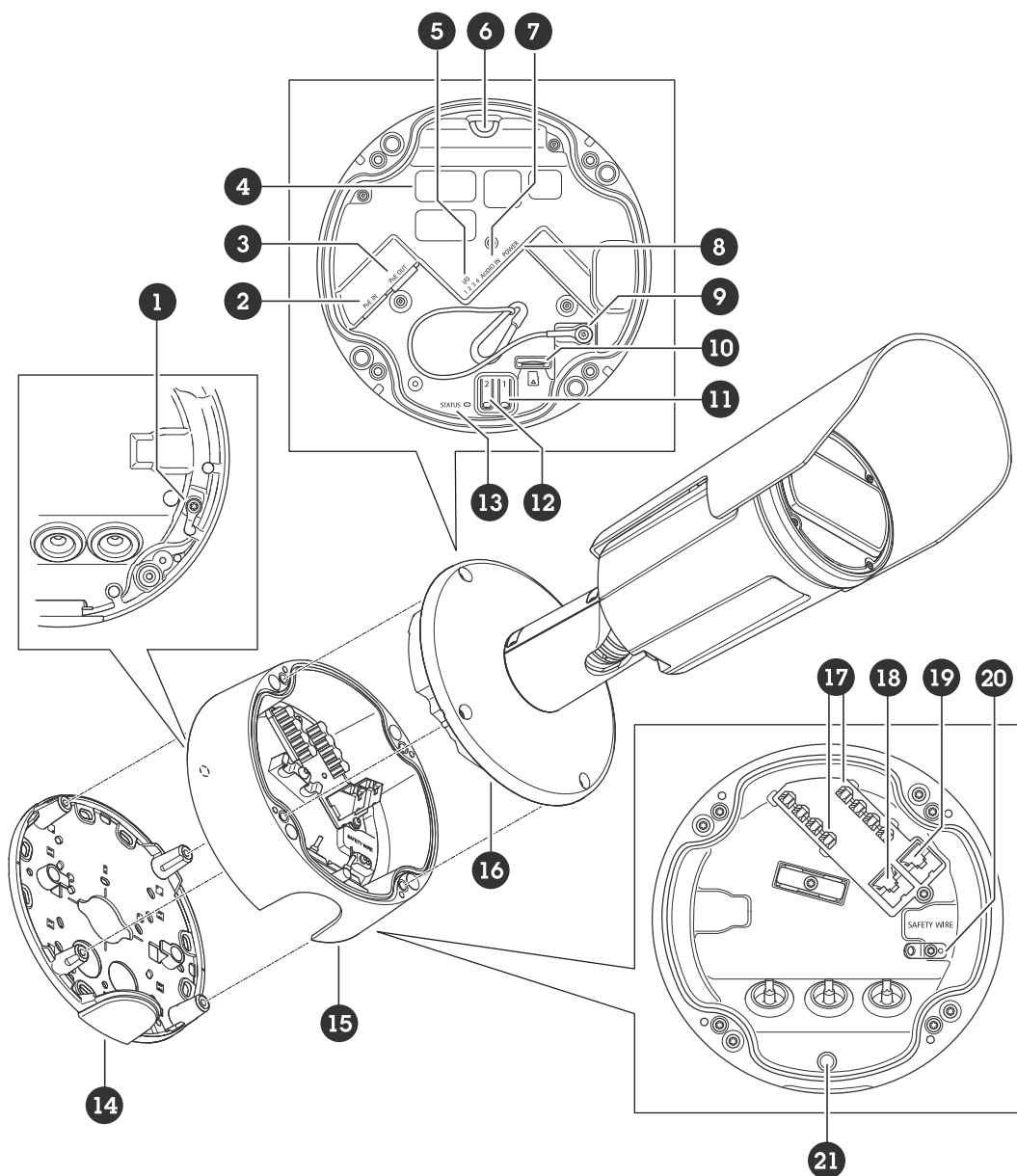
Aby dowiedzieć się więcej o działaniu tej aplikacji, zapoznaj się z *instrukcją obsługi aplikacji AXIS Image Health Analytics*.

Wizualizacja metadanych

Metadane analityczne są dostępne w przypadku poruszających się obiektów w scenie. Obsługiwane klasy obiektów są wizualizowane w strumieniu wideo za pomocą obwiedni otaczającej obiekt, wraz z informacją o typie obiektu i poziomie ufności klasyfikacji. Aby dowiedzieć się więcej na temat konfigurowania metadanych analitycznych i korzystania z nich, zobacz *podręcznik integracji AXIS Scene Metadata*.

Specyfikacje

Przegląd produktów



- 1 Śruba uziemienia
- 2 Złącze sieciowe RJ45 (Wejście PoE)
- 3 Złącze sieciowe RJ45 (Wyjście PoE)
- 4 Numer części (P/N) i numer seryjny (S/N)
- 5 Złącze I/O
- 6 Znak umożliwiający wyrównanie podczas instalacji
- 7 Złącze audio
- 8 Złącze zasilania
- 9 Przewód bezpieczeństwa
- 10 Gniazdo kart microSD
- 11 Przycisk kontrolny
- 12 Przycisk funkcyjny
- 13 Wskaźnik LED stanu
- 14 Uchwyt montażowy
- 15 Pokrywa przyłączeniowa
- 16 Kamera
- 17 2 złącza sieciowe IDC (IDC IN, IDC OUT)

- 18 Złącze sieciowe RJ45 (Wejście PoE)
- 19 Złącze sieciowe RJ45 (Wyjście PoE)
- 20 Przewód bezpieczeństwa
- 21 Znak umożliwiający wyrównanie podczas instalacji

Wskaźniki LED

Dioda stanu	Wskazanie
Zgaszony	Połączenie i normalne działanie.
Zielony	Stałe zielone światło przez 10 sekund przy normalnym działaniu po zakończeniu uruchamiania.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.
Bursztynowy/czerwony	Miga na bursztynowo/czerwono, gdy połączenie sieciowe jest niedostępne lub przerwane.

Diody LED i brzęczyk asystenta poziomowania

Informacje dotyczące przycisku funkcyjnego do poziomowania obrazu: *page 49*.

Kolor	Brzęczyk	Umieszczenie kamery
Zielona, stała	Dźwięk stały	Poziom
Zielona, miga	Szybkie sygnały dźwiękowe	Blisko poziomu
Pomarańczowa, miga	Średnie sygnały dźwiękowe	Brak poziomu
Czerwona, miga	Wolne sygnały dźwiękowe	Całkowity brak poziomu

Gniazdo karty SD

POWIADOMIENIE

- Ryzyko uszkodzenia karty SD. Nie używaj ostrych narzędzi, metalowych przedmiotów ani nadmiernej siły podczas wkładania i wyjmowania karty SD. Wkładaj i wyjmuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wyjmuj karty SD w trakcie działania produktu.

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 *Przywróć domyślne ustawienia fabryczne, on page 53*.

- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby nawiązać połączenie, naciśnij i zwolnij przycisk, a następnie poczekaj, aż dioda LED stanu mignie trzy razy na zielono.

Przycisk funkcyjny

Przycisk funkcyjny:

- Asystent poziomowania** – funkcja ta pomaga upewnić się, że obraz jest wypoziomowany. Naciśnij przycisk i przytrzymaj go przez około dwie sekundy, aby uruchomić asystenta poziomowania; naciśnij przycisk ponownie, aby wyłączyć asystenta.

Złącza

Złącze sieciowe

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

Złącze audio

- Wejście audio** – wejście 3,5 mm dla mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).



Wejście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Niezbalansowany mikrofon (z zasilaniem elektretowym lub bez) lub wejście liniowe	Zasilanie elektretowe po wybraniu	Masa
Zbalansowany mikrofon (z zasilaniem fantomowym lub bez) lub wejście linowe, sygnał „gorący”	Zbalansowany mikrofon (z zasilaniem fantomowym lub bez) lub wejście linowe, sygnał „zimny”	Masa

Złącze I/O

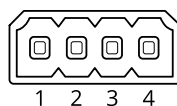
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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

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.

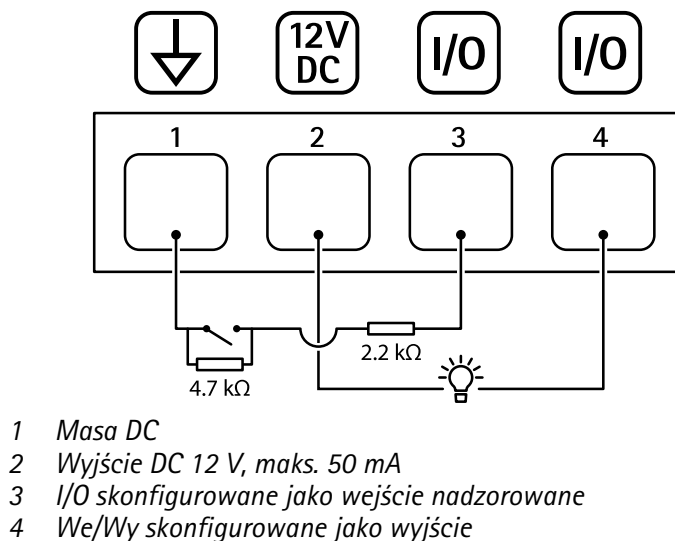
4-pinowy blok złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC

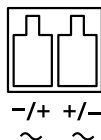
Wyjście DC	2	 Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 50 mA
Konfigurowalne (wejście lub wyjście)	3–4	Wejście cyfrowe lub wejście nadzorowane – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Aby mieć możliwość korzystania z nadzorowanego wejścia, zamontuj rezystory końca linii. Patrz diagram połączeń, aby uzyskać informacje na temat podłączania rezystorów.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Przykład:



Złącze zasilania

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



Czyszczenie urządzenia

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

POWIADOMIENIE

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

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

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

⚠ OSTRZEŻENIE

 Ten produkt emituje potencjalnie niebezpieczne promieniowanie optyczne. Może ono być szkodliwe dla oczu. Nie patrz na pracującą lampę.

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.

Uwaga

Aplikacja AXIS License Plate Verifier jest wstępnie skonfigurowana w kamerze. Po przywróceniu domyślnych ustawień fabrycznych klucz licencyjny zostanie zachowany. Po zresetowaniu do ustawień fabrycznych nie trzeba ponownie instalować aplikacji.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów, on page 48*.
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. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeżeli w sieci nie jest dostępny serwer DHCP, domyślny adres IP to 192.168.0.90.
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 strony internetowej urządzenia. Wybierz kolejno opcje **Maintenance (Konserwacja) > Factory default (Ustawienia fabryczne) > Default (Domyślne)**.

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

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

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony axis.com/support/device-software, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.
- Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie axis.com/support/device-software.
 - Zaloguj się do urządzenia jako administrator.
 - Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS) > Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

W programie AXIS Device Manager można uaktualnić wiele urządzeń jednocześnie. Dowiedz się więcej na stronie axis.com/products/axis-device-manager.

Problemy techniczne i możliwe rozwiązania

Problemy z uaktualnianiem systemu AXIS OS

Niepowodzenie uaktualniania systemu AXIS OS

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

Problemy po aktualizacji systemu AXIS OS

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

Problemy z ustawieniem adresu IP

Nie można ustawić adresu IP

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

Problemy z dostępem do urządzenia**Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki**

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

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje: *Przywróć domyślne ustawienia fabryczne, on page 53.*

Serwer DHCP zmienił adres IP

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

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

Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X

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

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, patrz *Obsługiwane przeglądarki, on page 6.*

Nie można uzyskać dostępu do urządzenia z zewnątrz

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

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

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

Problemy z przesyłaniem strumieniowym

Strumień multicast w kodowaniu H.264 jest dostępny wyłącznie dla lokalnych klientów

Sprawdź, czy router obsługuje technologię multicasting lub czy trzeba skonfigurować ustawienia routera w kliencie i urządzeniu. Może być konieczne zwiększenie wartości TTL (Time To Live), czyli czasu do rejestracji na żywo.

W kliencie nie można wyświetlić strumienia multicast w kodowaniu H.264

Poproś administratora sieci, aby sprawdził, czy adresy strumienia multicast używane przez urządzenie Axis są prawidłowe dla danej sieci.

Poproś administratora sieci, aby sprawdził, czy zaporę nie powoduje blokowania strumienia.

Niedostateczne renderowanie obrazów w kompresji H.264

Sprawdź, czy karta graficzna ma zainstalowany najnowszy sterownik. Zazwyczaj najnowsze sterowniki można pobrać z witryny internetowej producenta.

Strumienie H.264 i MJPEG mają różną saturację barw

Zmień ustawienia karty graficznej. Więcej informacji można znaleźć w dokumentacji karty.

Liczba klatek na sekundę jest mniejsza od oczekiwanej

- Patrz *Kwestie wydajności*, on page 57.
- Zmniejsz liczbę aplikacji uruchomionych na komputerze klienta.
- Ogranicz liczbę dozorców mogących oglądać obraz jednocześnie.
- Poproś administratora sieci, aby sprawdził, czy dostępna jest wystarczająca przepustowość.
- Zmniejsz rozdzielczość obrazu.

Nie można wybrać kodowania H.265 w podglądzie na żywo

Przeglądarki internetowe nie obsługują dekodowania H.265. Użyj systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

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

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

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

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

Nieznane pojazdy są oznaczone jako zaakceptowane

Jeśli aplikacja akceptuje pojazdy z tablicami rejestracyjnymi, które nie znajdują się na liście dozwolonych, to najprawdopodobniej oznacza to, że algorytm porównania zezwala na różnicę jednego znaku.

Przykład: jeśli tablica **AXI S1234** znajduje się na liście dozwolonych, aplikacja akceptuje tablicę **AXI SI234**.

Podobnie, jeśli tablica **AXIS 1234** znajduje się na liście dozwolonych, aplikacja akceptuje tablicę **AXI 1234**.

Wybierz kolejno opcje *Ustawienia dodatkowe*, *on page 32* i ustaw dozwoloną liczbę znaków.

Połączenie między aplikacją a kontrolerem lub modułem przekaźnikowym nie działa

Upewnij się, że kontroler lub moduł przekaźnikowy zezwala na przesyłanie danych za pośrednictwem protokołu HTTP. Aby się dowiedzieć, jak zmienić to ustawienie, zapoznaj się z instrukcją obsługi odpowiedniego urządzenia.

Problemy z parowaniem radaru

Po sparowaniu radaru jego strumień jest pokazywany nad strumieniem wideo. Upewnij się, że obraz z kamery nie jest obrócony o 180°. Przejdź do sekcji **Vide (Wideo) > Installation (Instalacja) > Rotation (Obrót)** i ustaw orientację na 0°.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wydajność. Niektóre czynniki wpływają na przepustowość (przepływność), inne na poklatkowość, a jeszcze inne na oba te parametry.

Najważniejsze czynniki, które należy uwzględnić:

- Wysoka rozdzielczość obrazu lub niższe poziomy kompresji zapewniają obrazy zawierające więcej danych, co z kolei wpływa na przepustowość.
- Obracanie obrazu w graficznym interfejsie użytkownika zwiększy obciążenie procesora produktu.
- Dostęp ze strony dużej liczby klientów MJPEG lub H.264/H.265/AV1 unicast wpływa na przepustowość.
- Jednoczesne oglądanie różnych strumieni (rozdzielczość, kompresja) za pomocą różnych klientów wpływa zarówno na liczbę klatek na sekundę, jak i na przepustowość.

W miarę możliwości używaj identycznych strumieni, aby utrzymać wysoką liczbę klatek na sekundę. Aby upewnić się, że strumienie są identyczne, możesz użyć profili strumieni.

- Jednoczesny dostęp do strumieni wideo z różnymi kodekami wpływa zarówno na poklatkowość, jak i na przepustowość. Aby uzyskać optymalną wydajność, należy używać strumieni z tym samym kodekiem.
- Intensywne korzystanie z ustawień zdarzeń wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.
- Korzystanie z protokołu HTTPS może zmniejszać liczbę klatek na sekundę, szczególnie w przypadku przesyłania strumieniowego obrazów wideo w formacie MJPEG.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Wyświetlanie obrazu z użyciem komputerów klienckich o niewystarczających parametrach obniża subiektywnie obserwowaną wydajność i wpływa na liczbę klatek na sekundę.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

Kontakt z pomocą techniczną

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

Cyberbezpieczeństwo

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

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

Postępowanie z lukami w zabezpieczeniach

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

Powiadomienia dotyczące zabezpieczeń

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

Bezpieczny cykl eksploatacji produktu

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

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

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

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

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

T10213367_pl

2026-07 (M14.2)

© 2024 – 2026 Axis Communications AB