

AXIS P3265-LVE-3 License Plate Verifier Kit

Spis treści

Od czego zacząć	4
Wyszukiwanie urządzenia w sieci	4
Obsługiwane przeglądarki	4
Otwórz interfejs WWW urządzenia	4
Utwórz konto administratora	4
Bezpieczne hasła	5
Upewnianie się co do braku zmian w oprogramowaniu urządzenia	5
Omówienie interfejsu WWW	5
Konfiguracja podstawowa	6
Zalecenia dotyczące montażu kamery	6
Asystent konfiguracji	8
Swobodny przepływ	8
Kontrola dostępu	9
Uzyskiwanie dostępu do ustawień aplikacji	10
Dostosowywanie obszarów zainteresowania	10
Wybór regionu	11
Dostosowywanie ustawień przechwytywania obrazu	11
Konfiguracja przechowywania zdarzeń	11
Instalacja	13
Tryb podglądu	13
Konfiguracja urządzenia	14
Dla użytkowników oprogramowania AXIS Camera Station	14
Konfigurowanie aplikacji AXIS License Plate Verifier	14
Ustawienia podstawowe	14
Regulowanie obrazu	14
Zmniejszanie czasu przetwarzania obrazu w trybie niskiego opóźnienia	14
Wybór trybu ekspozycji	15
Kompensacja dystorsji beczkowatej	15
Sprawdzanie rozdzielczości pikseli	15
Przeglądanie i rejestracja obrazów wideo	16
Zmniejszanie zapotrzebowania na przepustowość i zasób	16
Konfiguracja zasobów sieciowej pamięci masowej	17
Rejestracja i odtwarzanie obrazu	17
Sprawdzanie braku sabotażu wideo	17
Konfiguracja reguł dotyczących zdarzeń	18
Nagrywanie wideo, gdy kamera wykryje tablicę rejestracyjną	18
Wyzwalanie powiadomienia w przypadku ingerencji w obiektyw kamery	18
Dźwięk	19
Dodawanie dźwięku do zapisu	19
Dodawanie funkcji dźwięku do produktu przy użyciu technologii portcast	19
Zarządzanie listami	21
Dodawanie wykrytej tablicy rejestracyjnej do listy	21
Dodawanie opisów do tablic rejestracyjnych	21
Dostosowywanie nazw list	22
Importowanie numerów rejestracyjnych z listy dozwolonych	23
Udostępnianie listy tablic rejestracyjnych innym kamerom	24
Tworzenie harmonogramów dla list	25
Ustawienia dodatkowe	26
Konfiguracja nakładki tekstowej	26
Detekcja tablic rejestracyjnych przy słabym oświetleniu	26
Dopuszczanie mniejszej liczby znaków na tablicach rejestracyjnych	26
Dopasowywanie wyłącznie identycznych tablic rejestracyjnych	26
Zezwalanie na różnicę więcej niż jednego znaku podczas dopasowywania tablic rejestracyjnych	26

Przyznawanie ograniczonego dostępu operatorom	27
Konfiguracja bezpiecznych połączeń	27
Tworzenie kopii zapasowych i przywracanie ustawień aplikacji	27
Kasowanie wszystkich zdarzeń.....	27
Używanie portów wirtualnych do wyzwalania akcji.....	27
Scenariusz wjazdu i wyjazdu pojazdów	29
Otwieranie szlabanów dla znanych pojazdów przy użyciu modułu przekaźnikowego.....	29
Otwieranie szlabanów dla znanych pojazdów przy użyciu interfejsu I/O kamery	30
Powiadomienia dotyczące nieautoryzowanych pojazdów.....	31
Scenariusz kontroli dostępu pojazdów.....	32
Podłącz do kontrolera drzwi	32
Łączenie z aplikacją AXIS Secure Entry	34
Scenariusz swobodnego przepływu z pomiarem prędkości	36
Konfigurowanie scenariusza	36
Wyszukiwanie określonych zdarzeń.....	38
Eksportowanie i udostępnianie wyników wyszukiwania	38
Integracja	39
Używanie profili w celu wysyłania zdarzeń do różnych serwerów.....	39
Komunikat typu push o zdarzeniu przesyłany do oprogramowania innych firm.....	39
Wysłanie obrazu z tablic rejestracyjnych do serwera	40
Bezpośrednia integracja z 2N	41
Integracja z systemem Genetec Security Center.....	41
Interfejs WWW.....	44
Więcej informacji.....	45
Technologia edge-to-edge.....	45
Parowanie radaru	45
Parowanie głośnika.....	45
Obszar obserwacji	45
AXIS Image Health Analytics.....	45
Specyfikacje	47
Przegląd produktów.....	47
Wskaźniki LED.....	47
Gniazdo karty SD.....	48
Przyciski.....	48
Przycisk kontrolny.....	48
Złącza	48
Złącze sieciowe	48
Złącze audio.....	48
Złącze I/O	48
Rozwiązywanie problemów –	50
Przywróć domyślne ustawienia fabryczne	50
Opcje systemu AXIS OS.....	50
Sprawdzanie bieżącej wersji systemu AXIS OS	50
Aktualizacja systemu AXIS OS:.....	51
Problemy techniczne i możliwe rozwiązania.....	51
.....	54
Kwestie wydajności	55
Kontakt z pomocą techniczną.....	55
Cyberbezpieczeństwo	56
Postępowanie z lukami w zabezpieczeniach	56
Powiadomienia dotyczące zabezpieczeń	56
Bezpieczny cykl eksploatacji produktu	56

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 4.

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 5.
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 50.

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

Omówienie interfejsu WWW

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



Interfejs WWW urządzenia Axis

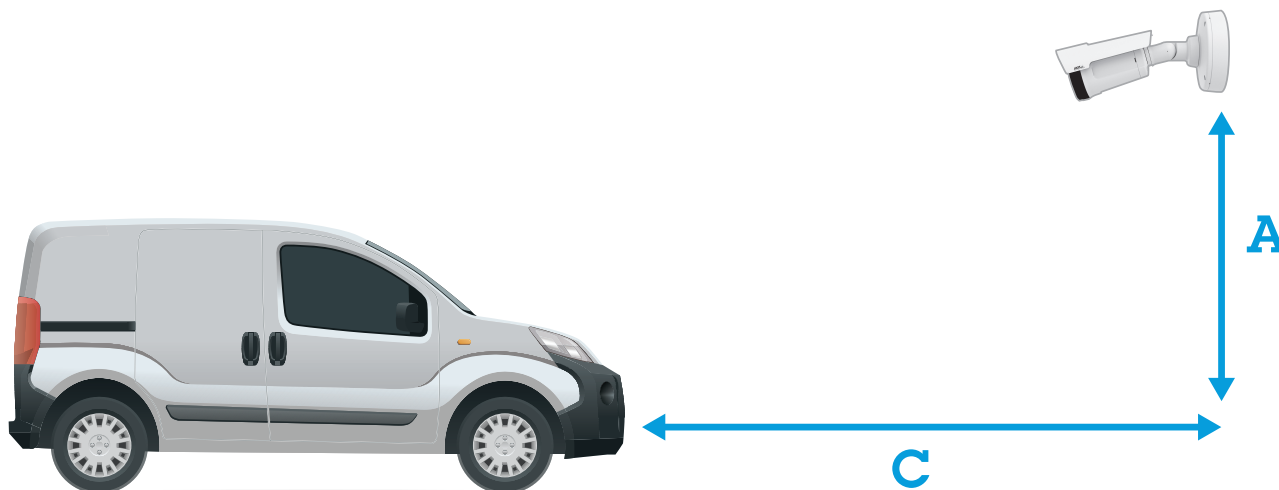
Konfiguracja podstawowa

Poniższe instrukcje dotyczące konfiguracji dotyczą wszystkich scenariuszy:

- 1.
- 2.
3. *Dostosowywanie obszarów zainteresowania, on page 10*
4. *Wybór regionu, on page 11*
5. *Konfiguracja przechowywania zdarzeń, on page 11*

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 **Access control (Kontroli dostępu)** powinna być równa połowie odległości pomiędzy pojazdem a kamerą.
- 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.



Odległość przechwytywania przy kontroli dostępu: 2–7 m (6,6–23 ft). Przykład na podstawie zestawu AXIS P3265–LVE-3 License Plate Verifier do weryfikacji tablic rejestracyjnych.

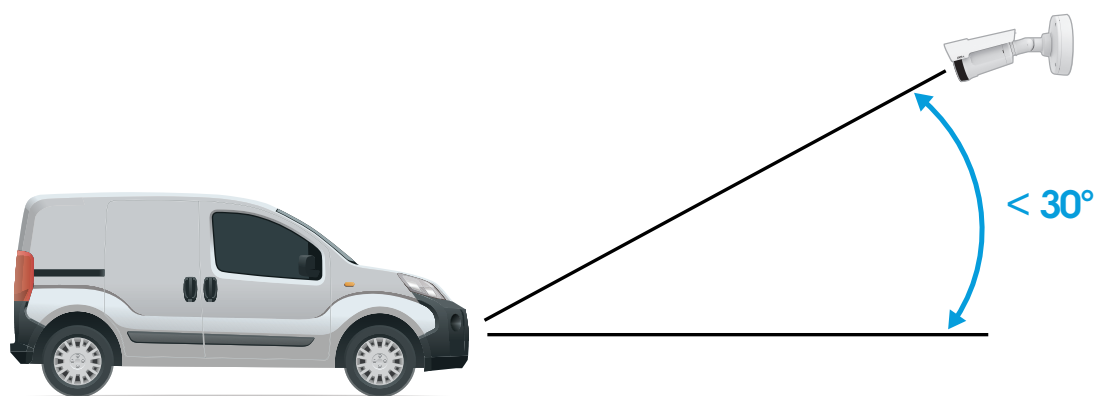
Odległość monitorowania (C)	Wysokość mocowania (A)
2,0 m (6,6 ft)	1,0 m (3,3 ft)
3,0 m (9,8 ft)	1,5 m (4,9 ft)
4,0 m (13 ft)	2,0 m (6,6 ft)
5,0 m (16 ft)	2,5 m (8.2 ft)
7,0 m (23 ft)	3,5 m (11 ft)

Odległość przechwytywania przy swobodnym przepływie: 7–20 m (23–65 ft). Przykład na podstawie zestawu AXIS P1465–LE-3 License Plate Verifier do weryfikacji tablic rejestracyjnych.

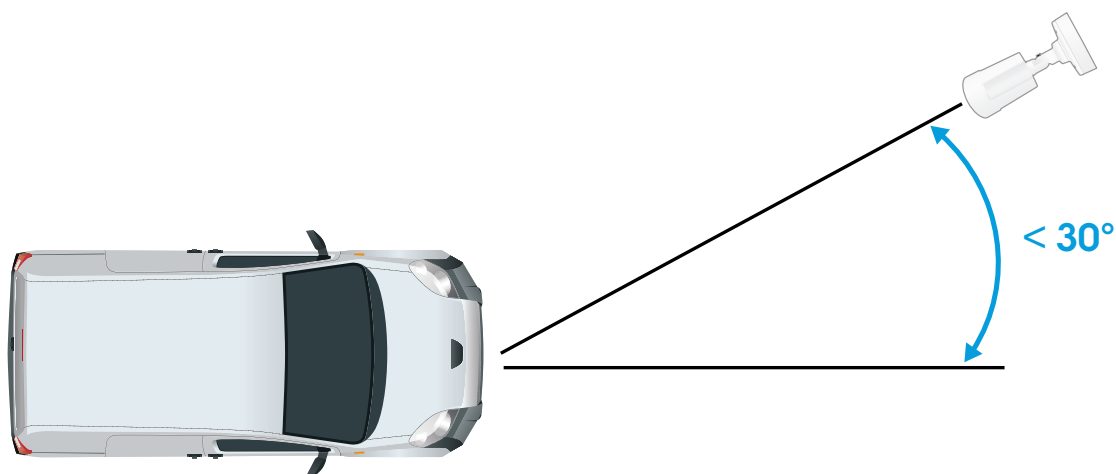
Odległość monitorowania (C)	Wysokość mocowania (A)
7,0 m (23 ft)	3,0 m (9,8 ft)

10,0 m (33 ft)	4,0 m (13 ft)
15,0 m (49 ft)	6,0 m (19,5 ft)
20,0 m (65 ft)	10,0 m (33 ft)

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

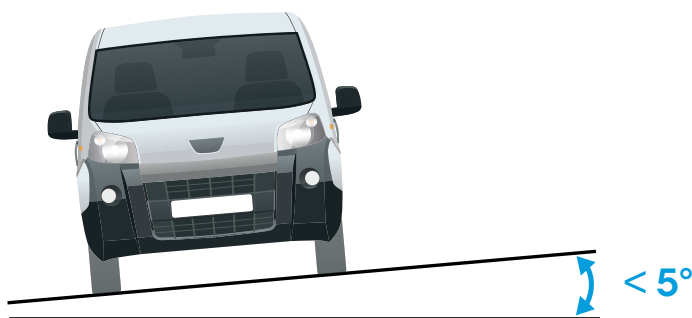


Kąt montażowy z boku.



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.

Asystent konfiguracji

Podczas uruchamiania aplikacji po raz pierwszy należy przy pomocy asystenta konfiguracji skonfigurować **Free flow (Swobodny przepływ)** lub **Access control (Kontrolę dostępu)**. Jeżeli chcesz wprowadzić zmiany w późniejszym czasie, przejdź do **Settings > Maintenance (Ustawienia > Utrzymanie)** i w sekcji **Setup assistant (Asystent ustawień)** naciśnij **Start**.

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 10*.
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 to 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)**.

Kontrola dostępu

Skorzystaj z kreatora konfiguracji do szybkiej i łatwej konfiguracji. Można wybrać opcję **Skip (Pomiń)**, aby opuścić przewodnik w dowolnym momencie.

1. Wybierz opcję **Access control (Kontrola dostępu)** i kliknij przycisk **Next (Dalej)**.
2. Wybierz typ kontroli dostępu:
 - **Internal I/O (Wewnętrzne I/O)**, aby zachować listę w kamerze. Patrz *Otwieranie szlabanów dla znanych pojazdów przy użyciu interfejsu I/O kamery, on page 30*.
 - **Controller (Kontroler)**, aby połączyć kontroler drzwi. Patrz .
 - **Relay (Przełącznik)**, aby połączyć z modułem przełącznikowym. Patrz .
3. Z listy rozwijanej **Barrier mode (Trybu szlabanu)** pod opcją **Open from lists (Otwórz z list)** wybierz **Allowlist (Listę dozwolonych)**.
4. Z listy rozwijanej **Vehicle direction (Kierunek jazdy)** wybierz opcję **out (wyjazd)**.
5. Na liście rozwijanej **ROI (Obszar zainteresowania)** zaznacz obszar zainteresowania, którego chcesz użyć, lub wszystkie.
6. Kliknij **Next (Dalej)**.

Na stronie **Image settings (Ustawienia obrazu)**:

1. Wybierz ilość obszarów zainteresowania.
2. Wybierz region, w którym znajduje się kamera.
3. Wybierz typ rejestracji. Patrz *Dostosowywanie ustawień przechwytywania obrazu, on page 11*.
4. Przeciągnij punkty kotwiczące, aby dostosować obszar zainteresowania. Patrz *Dostosowywanie obszarów zainteresowania, on page 10*.
5. Dostosuj kierunek obszaru zainteresowania. Kierunek określa w jaki sposób aplikacja rejestruje pojazdy wjeżdżające do lub wyjeżdżające z obszaru.
6. Kliknij przycisk **Next (Dalej)**

Na stronie **Dane zdarzenia**:

Uwaga

Szczegółowe ustawienia: *Komunikat typu push o zdarzeniu przesyłany do oprogramowania innych firm, on page 39*.

1. Z listy rozwijanej **Protocol (Protokół)** wybierz jeden z następujących protokołów:
 - TCP

- HTTP POST
- 2. W polu **Server URL (Adres URL serwera)** wpisz adres serwera i port w następującej formie: 127.0.0.1:8080.
- 3. W polu **Device ID (ID urządzenia)** wpisz nazwę urządzenia lub pozostaw pole bez zmian.
- 4. 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.
- 5. Aby włączyć tę funkcję, wybierz opcję **Send event data to server (Wysyłaj dane zdarzeń na serwer)**.
- 6. Aby zmniejszyć przepustowość podczas korzystania z protokołu HTTP POST, można wybrać opcję **Do not to send images through HTTP POST (Nie wysyłaj obrazów za pośrednictwem protokołu HTTP POST)**.
- 7. Kliknij przycisk **Next (Dalej)**

Na stronie **Importuj** listę z pliku .csv.:

1. Jeżeli masz już listę zapisanych tablic, wybierz opcję importowania jako **blocklist (listę blokowanych)** lub **allowlist (listę dozwolonych)**.
2. 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.

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.

Konfiguracja urządzenia

Dla użytkowników oprogramowania AXIS Camera Station

Konfigurowanie aplikacji AXIS License Plate Verifier

Gdy na urządzeniu jest skonfigurowana aplikacja AXIS License Plate Verifier, system zarządzania sygnałem wizyjnym uznaje ją za zewnętrzne źródło danych. Można podłączyć widok do źródła danych, wyszukać tablice rejestracyjne, które zostały przechwycone przez urządzenie, i wyświetlić powiązany obraz.

Uwaga

- Wymagane jest oprogramowanie AXIS Camera Station w wersji 5.38 lub nowszej.
 - Oprogramowanie AXIS License Plate Verifier wymaga licencji.
1. Pobierz i zainstaluj aplikację na urządzeniu.
 2. Skonfiguruj aplikację. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
 3. W przypadku istniejącej instalacji oprogramowania AXIS Camera Station odnow certyfikat serwera służący do komunikowania się z klientem. Patrz *Odnowienie certyfikatu*.
 4. Aby używać serwera programu AXIS Camera Station jako serwera NTP, włącz synchronizację czasu. Patrz *Ustawienia serwera*.
 5. Dodaj urządzenie do oprogramowania AXIS Camera Station. Patrz *Dodawanie urządzeń*.
 6. Po odebraniu pierwszego zdarzenia źródło danych zostanie dodane automatycznie w folderze **Configuration > Devices > External data sources** (Konfiguracja > Urządzenia > Zewnętrzne źródła danych).
 7. Połącz źródło danych z widokiem. Patrz *Zewnętrzne źródła danych*.
 8. Wyszukaj tablice rejestracyjne zarejestrowane przez urządzenie. Patrz *Wyszukiwanie danych*.
 9. Kliknij przycisk , aby wyeksportować wyniki wyszukiwania do pliku .txt.

Ustawienia podstawowe

Ustaw pozycję montażową

1. Przejdź do menu **Video > Installation > Mounting position** (Wideo > Instalacja > Pozycja montażowa).
2. Kliknij **Change** (Zmień).
3. Wybierz pozycję montażową i kliknij **Save and restart** (Zapisz i uruchom ponownie).

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).

Regulowanie obrazu

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia.

Zmniejszanie czasu przetwarzania obrazu w trybie niskiego opóźnienia

Aby zoptymalizować czas przetwarzania obrazu w strumieniu na żywo, można włączyć tryb niskiego opóźnienia. Opóźnienie strumienia na żywo zmniejsza się do minimum. W trybie niskiego opóźnienia jakość obrazu jest niższa niż zwykle.

1. Przejdź do menu **> System > Plain config** (System > Zwykła konfiguracja).

2. Wybierz **ImageSource (Źródło obrazu)** z listy rozwijanej.
3. Przejdź do opcji **ImageSource/I0/Sensor > Low latency mode (ŹródłoObrazu/I0/Czujnik > Tryb niskiego opóźnienia)** i wybierz opcję **On (Włącz)**.
4. Kliknij przycisk **Zapisz**.

Wybór trybu ekspozycji

Użyj trybów ekspozycji, jeśli chcesz poprawić jakość obrazu w określonych monitorowanych scenach. Tryby ekspozycji umożliwiają sterowanie aperturą, czasem otwarcia migawki i wzmocnieniem. Przejdź do menu **Video > Image > Exposure (Wideo > Obraz > Ekspozycja)** i wybierz tryb ekspozycji:

- W przypadku większości przypadków użycia należy wybrać opcję **Automatic (Automatyczna)**.
- W przypadku środowisk z niektórymi rodzajami sztucznego oświetlenia, na przykład jarzeniowego, wybierz opcję **Flicker-free (Bez migotania)**.
Wybierz taką samą częstotliwość, jaką ma linia zasilania.
- W przypadku środowisk z niektórymi rodzajami sztucznego oświetlenia i jasnym oświetleniem, na przykład na zewnątrz pomieszczeń z oświetleniem jarzeniowym w nocy i światłem słonecznym w dzień, wybierz opcję **Flicker-reduced (Zmniejszone migotanie)**.
Wybierz taką samą częstotliwość, jaką ma linia zasilania.
- Opcja **Hold current (Zachowaj bieżące)** blokuje bieżące ustawienia ekspozycji.

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.

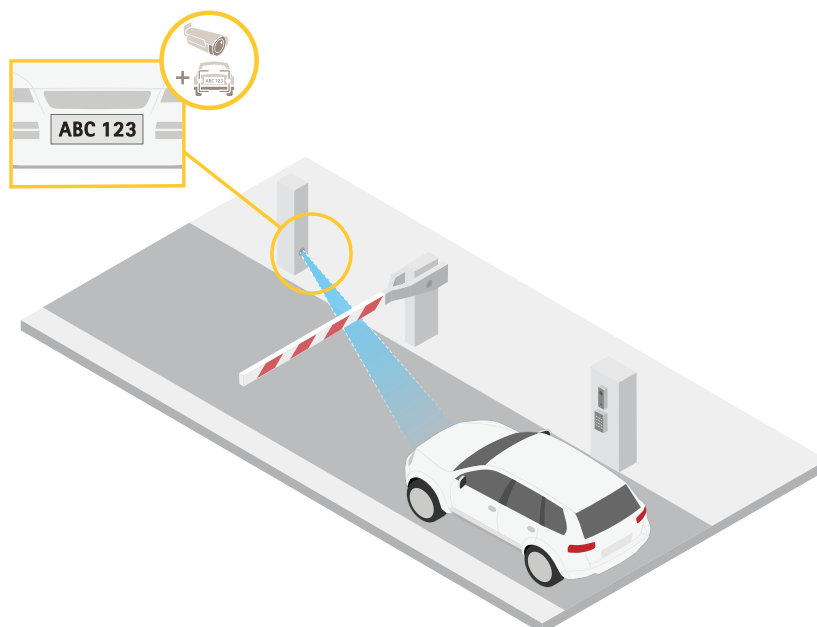
Uwaga

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.

Przeglądanie i rejestracja obrazów wideo

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej o działaniu strumieniowania i pamięci masowej, przejdź do .

Zmniejszanie zapotrzebowania na przepustowość i zasób

Ważne

Zmniejszenie przepustowości może skutkować utratą wyrazistości szczegółów na obrazie.

1. Wybierz kolejno opcje **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**.
4. Przejdź do okna **Video > Stream > General (Wideo > Strumień > Ogólne)** i zwiększ wartość w polu **Compression (Kompresja)**.
5. 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.

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

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z kamery

1. Wybierz kolejno opcje **Video > Stream (Wideo > Strumień)**.

2. Aby rozpocząć nagrywanie, kliknij  .

Jeżeli jeszcze nie skonfigurowano żadnej pamięci masowej, kliknij  i  . Aby uzyskać instrukcje dotyczące konfigurowania sieciowej pamięci masowej, zob. *Konfiguracja zasobów sieciowej pamięci masowej, on page 17*

3. Aby zatrzymać nagrywanie, ponownie kliknij  .

Obejrzyj wideo

1. Przejdź do menu **Recordings (Nagrania)**.
2. 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*.

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)*.

Nagrywanie wideo, gdy kamera wykryje tablicę rejestracyjną

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 działa program **AXIS Licence Plate Verifier**:

1. Przejdź do menu **Apps > AXIS License Plate Verifier (Aplikacje > AXIS License Plate Verifier)**.
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 **ALPV.PlateInView**.
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**.

Wyzwalanie powiadomienia w przypadku ingerencji w obiektyw kamery

W tym przykładzie wyjaśniono, jak ustawić powiadomienie e-mail wyzwalane, gdy obiektyw kamery zostanie zamalowany farbą w sprayu, zakryty lub gdy rejestrowany przez niego obraz zostanie rozmyty.

Activate the tampering detection (Aktywacja wykrywania sabotażu):

1. Przejdź do menu **System > Detectors > Camera tampering (System > Detektory > Sabotaż kamery)**.
2. Ustaw wartość dla funkcji **Trigger delay (Opóźnienie wyzwalacza)**. Wartość ta wskazuje czas, jaki musi upłynąć przed wysłaniem wiadomości e-mail.
3. Włącz opcję **Trigger on dark images (Wyzwalaj przy ciemnych obrazach)**, aby wykrywać, czy obiektyw stracił znacząco ostrość lub został zamalowany albo zakryty.

Dodaj odbiorcę wiadomości e-mail:

4. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
5. Wprowadź nazwę odbiorcy.
6. Jako typ powiadomienia wybierz **Email (E-mail)**.
7. Wpisz adres e-mail odbiorcy.

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

Create a rule (Utwórz regułę):

12. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
13. Wprowadź nazwę reguły.
14. Z listy warunków w obszarze **Video (Wideo)** wybierz **Tampering (Sabotaż)**.
15. Z listy akcji w menu **Notifications (Powiadomienia)** wybierz pozycję **Send notification to email (Wyślij powiadomienie emailem)**, a następnie wybierz odbiorcę z listy.
16. Wpisz temat i treść wiadomości e-mail.
17. 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:

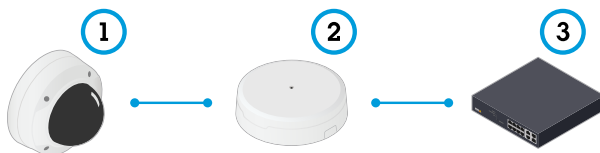
4. Przejdź do okna **System > Stream profiles (System > Profile strumienia)** i wybierz profil strumienia.
5. Kliknij opcję **Include audio (Dołącz audio)** i włącz ją.
6. Kliknij przycisk **Zapisz**.

Dodawanie funkcji dźwięku do produktu przy użyciu technologii portcast

Dzięki technologii portcast można dodać obsługę dźwięku do produktu. Technologia ta umożliwia przesyłanie dźwięku i sygnałów sterujących przez kabel sieciowy poprowadzony między kamerą a interfejsem.

Aby dodać funkcję dźwięku do urządzenia do sieciowego dozoru wizyjnego Axis, podłącz urządzenie audio Axis obsługujące technologię portcast w komplecie z interfejsem we/wy między urządzeniem a zasilającym switchem PoE.

1. Połącz sieciowe urządzenie dozoru wizyjnego Axis (1) i urządzenie Axis obsługujące technologię portcast (2) za pomocą kabla PoE.
2. Połącz urządzenie Axis obsługujące technologię portcast (2) ze switchem PoE (3) za pomocą kabla PoE.



- 1 *Urządzenie sieciowego dozoru wizyjnego Axis*
- 2 *Urządzenie Axis obsługujące technologię portcast*
- 3 *Switch*

Po podłączeniu urządzeń w ustawieniach urządzenia sieciowego dozoru wizyjnego Axis będzie widoczna karta dźwięku. Przejdź do karty **Audio** i włącz opcję **Allow audio (Zezwalaj na dźwięk)**.

Więcej informacji można znaleźć w instrukcji obsługi urządzenia Axis obsługującego technologię portcast.

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

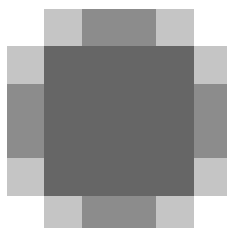
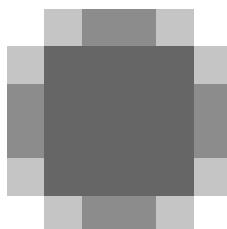
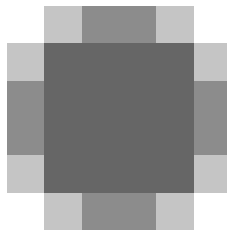
Sprawdź, czy symbole <, > oraz & nie są używane ani w tablicy rejestracyjnej, ani w opisie.

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

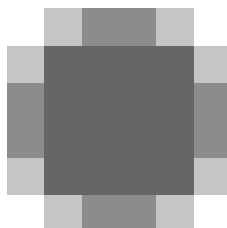
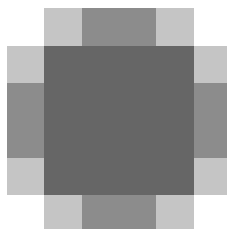
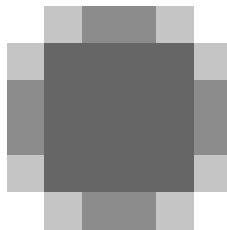
Dopilnuj, aby symbole <, > oraz & nie były używane ani w tablicach rejestracyjnych, ani w opisach.

Dostosowywanie nazw list

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

1. 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`

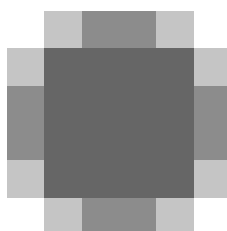
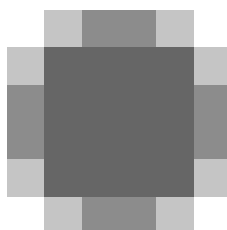
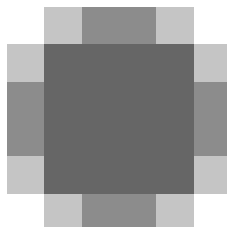
Tablica rejestracyjna + opis: `AXIS123, , John Smith`

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.

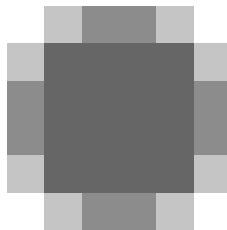
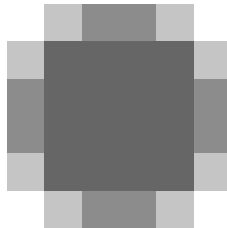
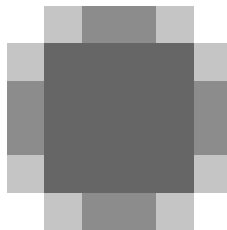
1. Przejdź do List management > List synchronization (Zarządzanie listą > Synchronizacja listy).
2. W sekcji Remote connected devices (Zdalny dostęp do dołączonych urządzeń) wpisz adres IP, nazwę użytkownika oraz hasło.
3. Kliknij Dodaj.

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**.

Używanie portów wirtualnych do wyzwalania akcji

Porty wirtualne w połączeniu z systemem kontroli dostępu mogą służyć do inicjowania dowolnych działań. Ten przykład wyjaśnia, jak ustawić aplikację **AXIS License Plate Verifier** i port I/O kamery, aby wyświetlać nakładkę tekstową za pomocą portu wirtualnego.

Wymagania:

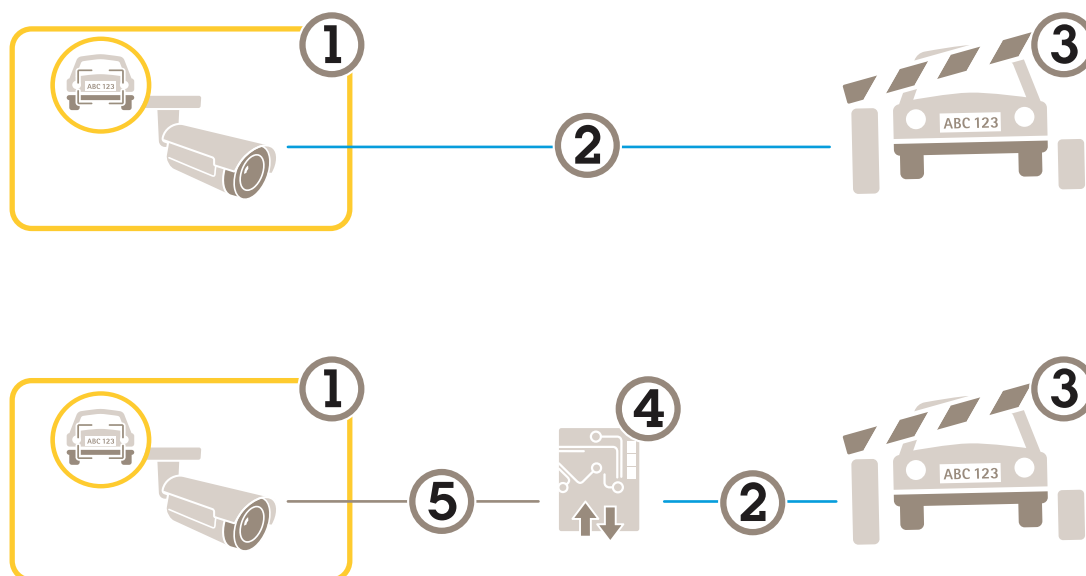
- Kamera jest zamontowana i podłączona do sieci.
- Aplikacja **AXIS License Plate Verifier** działa w kamerze.

- Kable połączone ze szlabanem i portem I/O kamery.
 - Konfiguracja podstawowa. Patrz .
1. Przejdź na stronę aplikacji i wybierz kartę **Settings (Ustawienia)**.
 2. Przejdź okna **Access control (Kontrola dostępu)**.
 3. W sekcji **Access control (Kontrola dostępu)** wybierz **Internal I/O (Wewnętrzne we / wy)**.
 4. Wybierz **I/O output # (Numer wyjścia I/O)**.
 5. Na liście rozwijanej **Virtual port (Port wirtualny)** zaznacz port.
 6. W sekcji **Barrier mode (Tryb zapory)** wybierz **Open to all (Otwarta dla wszystkich)**.
 7. W sekcji **Vehicle direction (Kierunek ruchu pojazdu)** wybierz **Any (Dowolny)**.
 8. Wybierz obszar zainteresowania **Area of interest**, którego chcesz użyć.
 9. Na stronie internetowej kamery przejdź do **System > Events (Zdarzenia)**.
 10. Kliknij przycisk **Add rule (Dodaj regułę)**.
 11. W ustawieniu **Condition (Warunek)** zaznacz wartość **Virtual input is active (Wejście wirtualne jest aktywne)** oraz wybrany przez siebie numer portu.
 12. W ustawieniu **Action (Akcja)** zaznacz opcję **Use overlay text (Użyj nałożonego tekstu)**.
 13. Zaznacz opcję **Video channels (Kanały wideo)**.
 14. Wpisz tekst, który ma być wyświetlany.
 15. Dodaj czas trwania wyświetlania tekstu.
 16. Kliknij przycisk **Zapisz**.
 17. Wybierz kolejno opcje **Video > Overlays (Wideo > Nakładki)**.
 18. Wybierz opcję **Overlays (Nakładki)**.
 19. Z listy rozwijanej wybierz opcję **Text (Tekst)** i kliknij przycisk **+**.
 20. Wpisz #D lub wybierz modyfikator z listy rozwijanej **Modifiers (Modyfikatory)**.
 21. Sprawdź, czy nakładka tekstowa jest wyświetlana, gdy pojazd wjedzie do obszaru zainteresowania w podglądzie na żywo.

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

Otwieranie szlabanów dla znanych pojazdów przy użyciu modułu przekaźnikowego

Poniższy przykład ilustruje sposób konfiguracji weryfikatora tablic rejestracyjnych AXIS License Plate Verifier z modułem przekaźnikowym w celu otwierania szlabanu dla znanych pojazdów w określonym obszarze zainteresowania, na przykład na parkingu.

Wymagania:

- Kamera jest zamontowana i podłączona do sieci.
 - Aplikacja AXIS License Plate Verifier działa w kamerze.
 - Kable połączone ze szlabanem i modułem przekaźnikowym.
 - Konfiguracja podstawowa. Patrz *Konfiguracja podstawowa, on page 6*.
1. Przejdź na stronę internetową kamery, wybierz opcję **Settings (Ustawienia)** i otwórz aplikację AXIS License Plate Verifier.
 2. Przejdź na stronę internetową modułu przekaźnikowego i upewnij się, że port przekaźnika jest podłączony do portu I/O kamery.
 3. Skopiuj adres IP modułu przekaźnikowego.
 4. Wróć do AXIS License Plate Verifier.
 5. Przejdź do obszaru **Settings (Ustawienia) > Access Control (Kontrola dostępu)**.
 6. Przejdź do **Type (Typ)** i z listy rozwijanej wybierz opcję **Relay (Przekaźnik)**.
 7. Z listy rozwijanej **I/O output (Wyjście I/O)** wybierz port I/O podłączony do szlabanu.

8. Z listy rozwijanej **Barrier mode (Trybu szlabanu)** wybierz opcję **Open from lists (Otwórz z list)**, a następnie zaznacz **Allowlist (Listę dozwolonych)**.
9. Z listy rozwijanej **Vehicle direction (Kierunek jazdy)** wybierz opcję **in (wjazd)**.
10. Z listy rozwijanej **ROI (Obszar zainteresowania)** wybierz obszar zainteresowania obejmujący pas ruchu.
11. Wprowadź następujące informacje:
 - adres IP modułu przekaźnikowego w formacie 192.168.0.0;
 - nazwa użytkownika dla modułu przekaźnikowego;
 - hasło dla modułu przekaźnikowego.
12. Aby upewnić się, że połączenie działa poprawnie, kliknij przycisk **Connect (Połącz)**.
13. Aby aktywować połączenie, kliknij opcję **Turn on integration (Włącz integrację)**.
14. Przejdź do karty **List management (Zarządzanie listami)**
15. Wprowadź numer tablicy rejestracyjnej w polu **Allowlist (Lista dozwolonych)**.

Uwaga

Porty wejść fizycznych 1–8 na module przekaźnikowym odpowiadają portom 1–8 na liście rozwijanej. Jednak porty wejść przekaźnika 1–8 na module przekaźnikowym odpowiadają portom 9–16 na liście rozwijanej. Ma to zastosowanie również w przypadku, gdy moduł przekaźnikowy ma tylko 8 portów.

16. Sprawdź, czy aplikacja rozpoznaje numer tablicy rejestracyjnej z listy dozwolonych jako tablicę znanego pojazdu, i czy szlaban otwiera się zgodnie z oczekiwaniami.

Otwieranie szlabanów dla znanych pojazdów przy użyciu interfejsu I/O kamery

Ten przykład wyjaśnia, jak ustawić aplikację AXIS License Plate Verifier i port I/O kamery, aby otworzyć szlaban dla znanego pojazdu, na przykład wjeżdżającego na parking.

Wymagania:

- Kamera jest zamontowana i podłączona do sieci.
 - Aplikacja AXIS License Plate Verifier działa w kamerze.
 - Kable połączone ze szlabanem i portem I/O kamery.
 - Konfiguracja podstawowa. Patrz .
1. Przejdź do strony internetowej aplikacji, dalej do **Home (Strona główna)** i dodaj wykryte tablice rejestracyjne do listy. Patrz *Dodawanie wykrytej tablicy rejestracyjnej do listy, on page 21*
 2. Aby bezpośrednio edytować listę, przejdź do **List management (Zarządzanie listami)**.
 3. Wprowadź autoryzowany numer tablicy rejestracyjnej w polu **Allowlist (Lista dozwolonych)**.
 4. Przejdź do opcji **Settings (Ustawienia)**.
 5. W sekcji **Access control (Kontrola dostępu)** wybierz **Internal I/O (Wewnętrzne we / wy)**.
 6. Wybierz **I/O output # (Numer wyjścia I/O)**.
 7. W sekcji **Barrier mode (Tryb bariery)** wybierz **Open from lists (Otwórz z list)**, a następnie zaznacz **Allowlist (Lista dozwolonych)**.
 8. Z listy rozwijanej **Vehicle direction (Kierunek jazdy)** wybierz opcję **in (wjazd)**.
 9. W sekcji **Area of interest (Obszar zainteresowania)** zaznacz obszar zainteresowania, którego chcesz użyć albo zaznacz, że chcesz wykorzystać wszystkie obszary.
 10. Sprawdź, czy aplikacja rozpoznaje numer tablicy rejestracyjnej z listy dozwolonych jako tablicę znanego pojazdu, i czy szlaban otwiera się zgodnie z oczekiwaniami.

Uwaga

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

Powiadomienia dotyczące nieautoryzowanych pojazdów

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

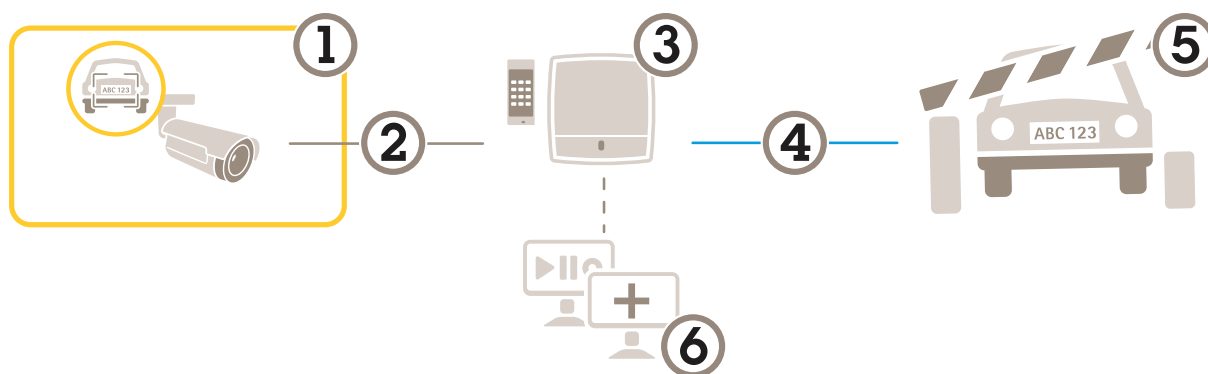
Wymagania:

- Konfiguracja podstawowa. Patrz *Konfiguracja podstawowa, on page 6*.
- 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 kontroli dostępu pojazdów

W scenariuszu kontroli dostępu pojazdów aplikacja może być połączona z sieciowym kontrolerem drzwi Axis w celu konfiguracji reguł dostępu, utworzenia rozkładów godzin dostępu i zarządzania dostępem pojazdów nie tylko pracowników, ale też na przykład gości i dostawców.

W celu dodatkowego zabezpieczenia użyj systemu dostępu obejmującego kontrolery drzwi i czytniki kart. Aby skonfigurować kontrolery drzwi i czytniki kart, zapoznaj się z dokumentacją użytkownika na stronie axis.com



- 1 Kamera Axis z aplikacją *AXIS License Plate Verifier*
- 2 Komunikacja IP
- 3 Sieciowy kontroler drzwi Axis z czytnikiem kart
- 4 Komunikacja I/O
- 5 Szlaban
- 6 Opcjonalne oprogramowanie innych firm

Podłącz do kontrolera drzwi

W tym przykładzie podłączymy kamerę do sieciowego kontrolera drzwi, co oznacza, że kamera będzie pełnić funkcję czujnika. Kamera przekazuje dane do kontrolera, który z kolei je analizuje i wyzwała zdarzenia.

Uwaga

Przełączając pomiędzy aplikacjami *AXIS License Plate Verifier* i *AXIS Entry Manager* należy dopilnować odświeżenia stron, aby uzyskać dostęp do wszystkich parametrów.

Wymagania:

- Kamera i kontroler drzwi zamontowane i podłączone do sieci.
- Aplikacja *AXIS License Plate Verifier* działa w kamerze.
- Konfiguracja podstawowa. Patrz *Konfiguracja podstawowa, on page 6*.



*Konfigurowanie aplikacji pod kątem współpracy z kontrolerem *AXIS A1001 Door Controller*.*

Konfiguracja sprzętowa w aplikacji *AXIS Entry Manager*

1. Przejdź do aplikacji *AXIS Entry Manager* i rozpocznij nową konfigurację sprzętową w menu **Konfiguracja**.
2. W konfiguracji sprzętowej zmień nazwę sieciowego kontrolera drzwi na „Gate controller (Kontroler bramy)”.
3. Kliknij **Next (Dalej)**.

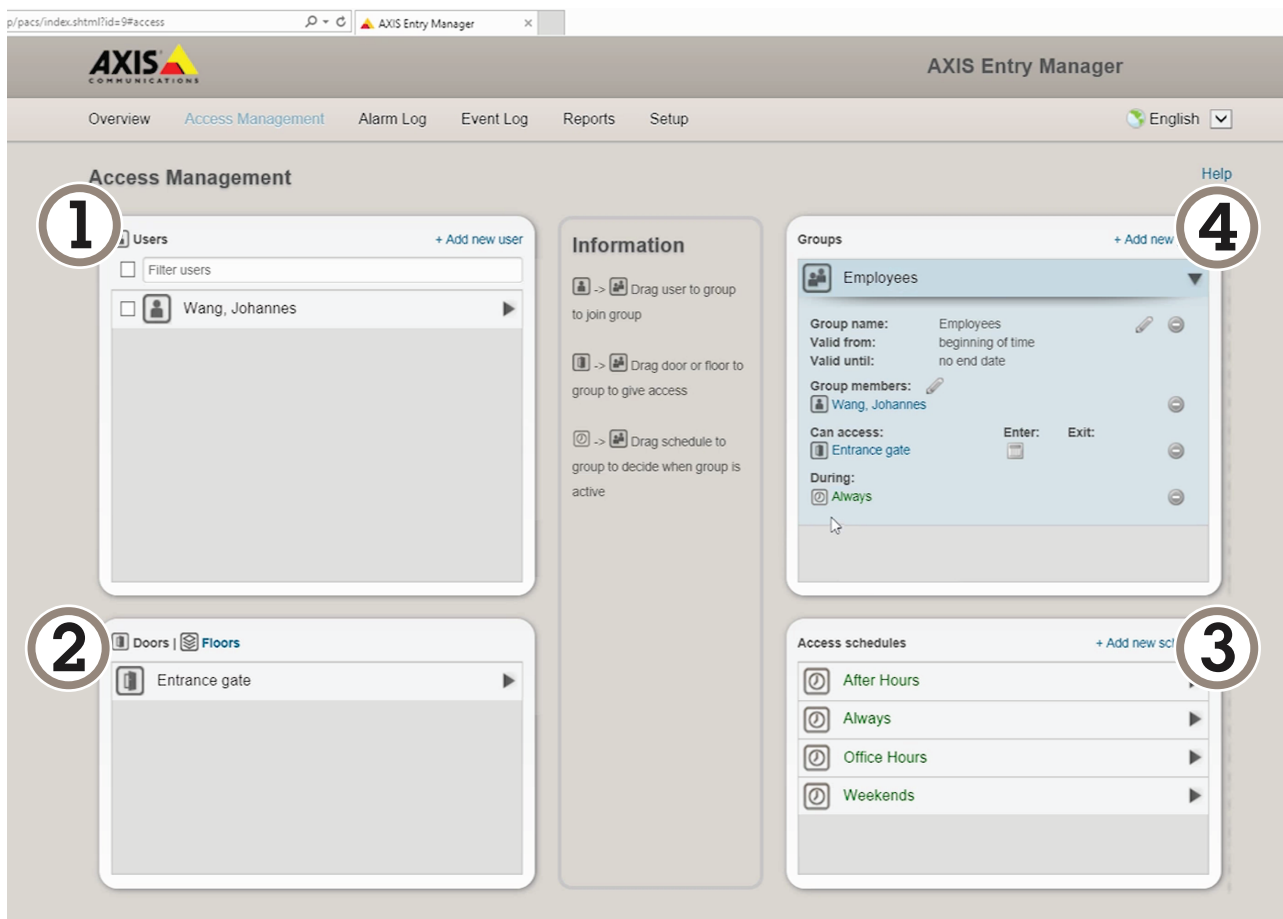
4. W opcji **Configure locks connected to this controller** (Skonfiguruj zamki podłączone do tego kontrolera) usuń opcję **Door monitor** (Monitor drzwi).
5. Kliknij **Next** (Dalej).
6. W opcji **Configure readers connected to this controller** (Skonfiguruj czytniki podłączone do tego kontrolera) usuń opcję **Exit reader** (Czytnik wyjścia).
7. Kliknij przycisk **Finish** (Zakończ).

Konfiguracja w aplikacji AXIS License Plate Verifier

1. Przejdź do strony internetowej aplikacji **AXIS License Plate Verifier**.
2. Przejdź do obszaru **Settings** (Ustawienia) > **Access Control** (Kontrola dostępu).
3. Przejdź do **Type** (Typ) i z listy rozwijanej wybierz opcję **Controller** (Kontroler).
4. Wprowadź następujące informacje:
 - adres IP kontrolera w formacie 192.168.0.0;
 - nazwa użytkownika dla kontrolera;
 - hasło dla kontrolera.
5. Kliknij przycisk **Połącz**.
6. Jeśli połączenie zostanie nawiązane, na liście rozwijanej **Network Door Controller name** (Nazwa sieciowego kontrolera drzwi) pojawi się „Gatecontroller (Kontroler bramy)”. Wybierz „Gatecontroller (Kontroler bramy)”.
7. Z listy rozwijanej **Reader name** (Nazwa czytnika) wybierz czytnik podłączony do drzwi „Gatecontroller (Kontroler bramy), na przykład „Reader entrance” (Czytnik przy wejściu). Nazwy te można zmienić w aplikacji **AXIS Entry Manager**.
8. Aby aktywować połączenie, wybierz opcję **Turn on integration** (Włącz integrację).
9. W polu testowym wprowadź jeden z numerów tablic rejestracyjnych użytkownika lub numer domyślny, a następnie kliknij przycisk **Test integration** (Testowanie integracji). Sprawdź, czy test się powiódł.

Konfiguracja użytkowników, grup, drzwi i harmonogramów w aplikacji AXIS Entry Manager

1. Przejdź do aplikacji **AXIS Entry Manager**.
2. Przejdź do opcji **Access Management** (Zarządzanie dostępem).
3. Przejdź do menu **Doors** (Drzwi) > **Add identification type** (Dodaj typ identyfikacji).
4. Z listy rozwijanej **Credentials needed** (Wymagane poświadczenia) wybierz **License plate only** (Tylko tablica rejestracyjna).
5. Aby nałożyć ograniczenia czasowe na możliwość korzystania z danego typu identyfikacji, przeciągnij i upuść **Schedule** (Harmonogram) na drzwi.
6. Dodaj użytkowników i dla każdego użytkownika dodaj poświadczenie **License plate** (Tablica rejestracyjna).
7. Kliknij opcję **Add credential** (Dodaj poświadczenie) ponownie i wprowadź dane tablicy rejestracyjnej.
8. Kliknij opcję **Add new group** (Dodaj nową grupę) i wprowadź dane.
9. Aby przydzielić użytkowników do grupy, przeciągnij i upuść **Users** (Użytkowników) do grupy użytkowników.
10. Aby przydzielić użytkownikom dostęp, przeciągnij i upuść **Door** (Drzwi) do grupy użytkowników.
11. Aby ograniczyć czas dostępu, przeciągnij i upuść **Schedule** (Harmonogram) do grupy użytkowników.



Ogólne informacje o interfejsie użytkownika aplikacji AXIS Entry Manager.

- 1 Użytkownicy
- 2 Drzwi
- 3 Harmonogramy
- 4 Grupy użytkowników

Łączenie z aplikacją AXIS Secure Entry

W tym przykładzie opisano łączenie kontrolera drzwi Axis w oprogramowaniu AXIS Camera Station i AXIS Secure Entry za pomocą aplikacji AXIS Licence Plate Verifier.

Wymagania:

- Kamera i kontroler drzwi zamontowane i podłączone do sieci.
- Aplikacja AXIS License Plate Verifier działa w kamerze.
- Zainstalowany klient aplikacji AXIS Camera Station w wersji 5.49.449 lub nowszej.
- Konfiguracja podstawowa. Patrz *Konfiguracja podstawowa, on page 6*.

W aplikacji AXIS Camera Station zob. *Add a reader (Dodawanie czytnika)*.

W aplikacji AXIS License Plate Verifier:

1. W zakładce Settings (Ustawienia) przejdź do pozycji Configuration wizard (Kreator konfiguracji) i kliknij Start (Rozpocznij).
2. Wybierz opcję Access Control (Kontrola dostępu).
3. Wybierz Secure Entry (Bezpieczne wchodzenie) i kliknij przycisk Next (Dalej).

W oprogramowaniu AXIS Camera Station:

4. Wpisz adres IP kontrolera drzwi, dostępnego na liście urządzeń w menu AXIS Camera Station > Configuration > Other Devices (AXIS Camera Station > Konfiguracja > Inne urządzenia).

5. Aby dodać klucz uwierzytelniania, przejdź do menu **AXIS Camera Station > Configuration > Encrypted communication** (AXIS Camera Station > Konfiguracja > Szyfrowana komunikacja).
6. Otwórz **External Peripheral Authentication Key** (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego) i kliknij **Show authentication key** (Pokaż klucz uwierzytelniania).
7. Kliknij przycisk **Copy key** (Kopiuj klucz).

W aplikacji **AXIS License Plate Verifier**:

8. Przejdź do pozycji **Authentication key** (Klucz uwierzytelniania) w kreatorze konfiguracji i wklej klucz.
9. Kliknij przycisk **Połącz**.
10. Z rozwijalnego menu wybierz **Door controller name** (Nazwa kontrolera drzwi).
11. Z rozwijalnego menu wybierz **Reader name** (Nazwa czytnika).
12. Zaznacz opcję **Turn on integration** (Włącz integrację).
13. Kliknij **Next** (Dalej).
14. Dostosuj obszar zainteresowania. Zobacz temat *Dostosowywanie obszarów zainteresowania, on page 10*.
15. Kliknij dwa razy przycisk **Next** (Dalej) i kliknij **Finish** (Zakończ).

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 45*.

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.
- Upewnij się, że drugi obszar obserwacji kamery (obszar obserwacji 2) nie jest używany, ponieważ radar użyje go po sparowaniu.

Konfiguracja kamery:

1. Skonfiguruj kamerę, postępując zgodnie z instrukcjami przedstawionymi w *Konfiguracja podstawowa, on page 6*.
2. Korzystając z pomocy asystenta ustawień wybierz swobodny przepływ. Więcej informacji znajduje się w rozdziale *Swobodny przepływ, on page 8*.

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 39*.
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 11.

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 (Ujścia 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

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 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.

Oprócz tego strumień radaru jest wizualizowany w drugim obszarze obserwacji kamery, nazywanym **obszarem obserwacji 2**. Metadane generowane przez radar są dostępne za pośrednictwem drugiego kanału generatora metadanych kamery, tzw. **kanału 2**.

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.

Obszar obserwacji

Obszar obserwacji to przycięty fragment pełnego widoku. Obszary obserwacji można przysyłać strumieniowo i zapisywać zamiast pełnego widoku, aby zminimalizować zapotrzebowanie na przepustowość i zasoby pamięci masowej. W przypadku włączenia PTZ w obszarze obserwacji można w obszarze używać funkcji PTZ. Za pomocą obszarów obserwacji można usuwać fragmenty pełnego widoku, na przykład niebo.

Podczas konfigurowania obszaru obserwacji zaleca się ustawienie rozdzielczości strumienia wideo o rozmiarze mniejszym lub większym niż rozmiar obszaru obserwacji. Jeżeli rozdzielczość strumienia wideo będzie większa niż rozmiar obszaru obserwacji, obraz wideo zostanie uznany za skalowany cyfrowo po przechwyceniu przez przetwornik, co wymaga większej przepustowości bez dodawania informacji o obrazie.

Uwaga

Po sparowaniu kamery z radarem za pomocą technologii edge-to-edge strumień radaru będzie wizualizowany w drugim obszarze obserwacji kamery.

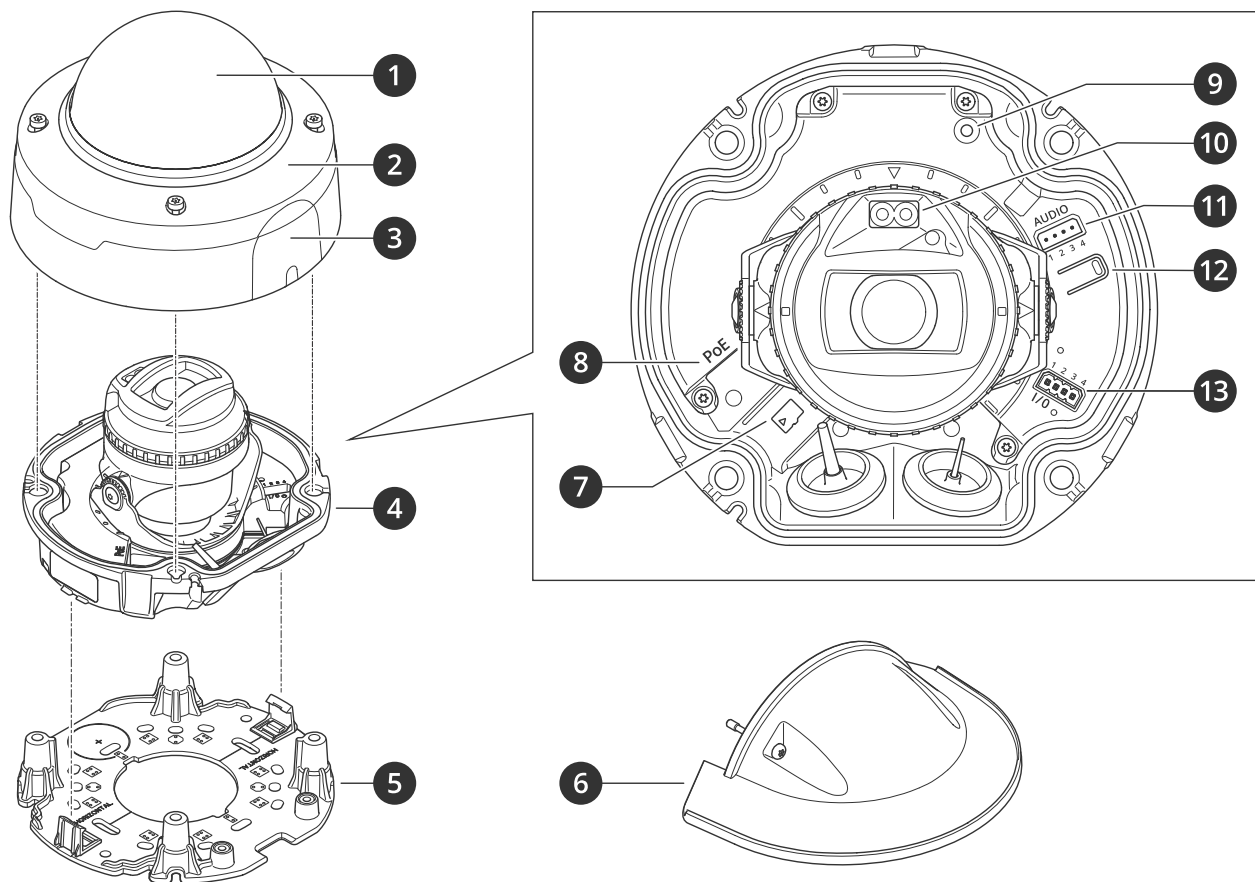
AXIS Image Health Analytics

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*.

Specyfikacje

Przegląd produktów



- 1 Kopułka
- 2 Osłona kopułki
- 3 Pokrywa
- 4 Kamera
- 5 Uchwyt montażowy
- 6 Osłona chroniąca przed wpływem warunków atmosferycznych
- 7 Gniazdo karty pamięci SD
- 8 Złącze sieciowe (PoE)
- 9 Wskaźnik LED stanu
- 10 IR LED
- 11 Złącze audio
- 12 Przycisk kontrolny
- 13 Złącze I/O

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.

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 wydymuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wydymuj 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 50*.

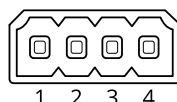
Złącza

Złącze sieciowe

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

Złącze audio

4-pinowy blok złączy wejść i wyjść audio.



Funkcje	Styk	Uwagi
GND	1	Masa
Zasilanie obwodem pierścieniowym	2	12 V dla źródła zewnętrznego
Wejście liniowe mikrofonu	3	Wejście mikrofonu (analogowego lub cyfrowego) lub wejście liniowe (mono). Dostępne jest zasilanie bias mikrofonu 5 V.
Wyjście liniowe	4	Wyjście audio na poziomie linii (mono). Można je podłączyć do systemu nagłośnienia (PA) lub aktywnego głośnika z wbudowanym wzmacniaczem.

Złącze I/O

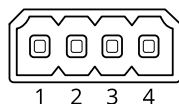
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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.

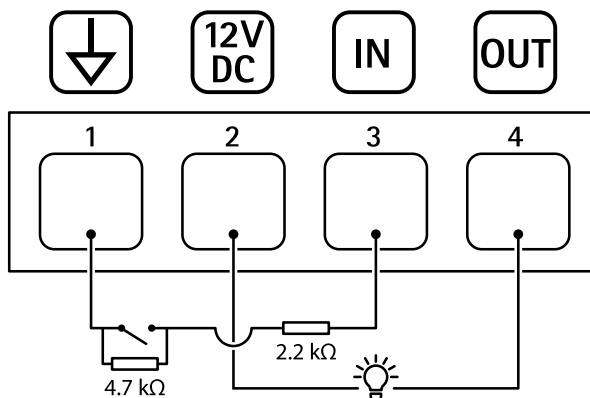
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

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 = 25 mA
Wejście cyfrowe lub wejście nadzorowane	3	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	4	Podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Przykład:



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

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 47*.
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.
1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie axis.com/support/device-software.
 2. Zaloguj się do urządzenia jako administrator.
 3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS) > Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

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 50.*

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 4.*

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 55.
- 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.
- Zaloguj się w interfejsie WWW urządzenia i ustaw tryb rejestracji, w którym liczba klatek na sekundę ma priorytet. Zmiana trybu rejestracji, aby nadawał priorytet liczbie klatek na sekundę, może obniżyć rozdzielczość w zależności od używanego urządzenia i dostępnych trybów rejestracji.

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 26* 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

Nie można sparować kamery z radarem	Upewnij się, że drugi obszar obserwacji kamery (obszar obserwacji 2) nie jest wykorzystywany, ponieważ radar zostanie do niego przydzielony automatycznie. Jeżeli drugi obszar obserwacji jest w użyciu, przejdź do menu Video > View areas (Wideo > Obszary obserwacji), usuń go i spruj ponownie urządzenia.
Poruszające się pojazdy w widoku kamery nie są zsynchronizowane z nałożeniami prędkości ani ze śladami w widoku radaru	Upewnij się, że został zsynchronizowany czas między kamerą i radarem. Aby sprawdzić stan, przejdź do menu Status > Time sync status (Stan > Stan synchronizacji czasu) w interfejsach WWW urządzeń. Jeśli wyświetlany jest stan Synchronized: No (Zsynchronizowano: Nie), kliknij NTP settings (Ustawienia NTP) i wybierz źródło czasu do synchronizacji urządzenia. Upewnij się, że używasz tego samego źródła czasu dla obu urządzeń.
Drugi obszar obserwacji kamery nie wyświetla prawidłowo strumienia radaru	Domyślna rozdzielczość radaru po sparowaniu w technologii edge-to-edge wynosi 1280x720, zarówno w interfejsie WWW kamery, jak i w systemie VMS. W przypadku wybrania innej rozdzielczości strumień danych radaru będzie miał nieprawidłowy wygląd. Aby dostosować rozdzielczość do radaru, przejdź do menu Video > Stream > General (Wideo > Strumień > Ogólne) w interfejsie WWW kamery i wybierz View area 2 (Obszar obserwacji 2).

Problemy z nałożeniami	
Nałożenia dodane przeze mnie w interfejsie WWW kamery znikają po sparowaniu radaru	Jeśli w kamerze dodano więcej niż jeden obszar obserwacji, wszystkie nałożenia dodane wcześniej znikną z jej interfejsu WWW. Po sparowaniu radaru zajmie on drugi obszar obserwacji, dlatego z interfejsu WWW kamery znikną wszystkie istniejące nałożenia. Nałożenia zostaną usunięte tylko z interfejsu WWW. Nadal będzie możliwe korzystanie ze strumienia z nałożeniami, np. w VMS.
Nie widać nałożeń tabli rejestracyjnych dodanych w aplikacji AXIS License Plate Verifier	Jeśli zostały dodane nałożenia wyświetlające prędkość pojazdu w aplikacji AXIS Speed Monitor, a następnie włączono nałożenia tablic rejestracyjnych w aplikacji AXIS License Plate Verifier, nałożenia z tablicami rejestracyjnymi nie będą pokazywane. Najpierw włącz nałożenia w aplikacji AXIS License Plate Verifier, a następnie dodaj ewentualne nałożenia z informacjami o prędkości w aplikacji AXIS Speed Monitor.

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.

T10191705_pl

2026-07 (M16.2)

© 2023 – 2026 Axis Communications AB