AXIS P3245-LVE-3 License Plate Verifier Kit

Podręcznik użytkownika

Informacje o produkcie

Zestaw AXIS P3245–LVE-3 License Plate Verifier Kit do weryfikacji tablic rejestracyjnych składa się z kamery sieciowej AXIS P3245–LVE Network Camera oraz zainstalowanej aplikacji AXIS License Plate Verifier i służy do rozpoznawania tablic rejestracyjnych i automatyzacji zarządzania wjazdem i wyjazdem pojazdów.
AXIS P1455-LE-3 weryfikuje dostęp obszarów kontrolowanych, takich jak parkingi, na podstawie listy elementów zablokowanych i dozwolonych.

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.



W tym filmie pokazano, korzystać z trybu podglądu.

Od czego zacząć

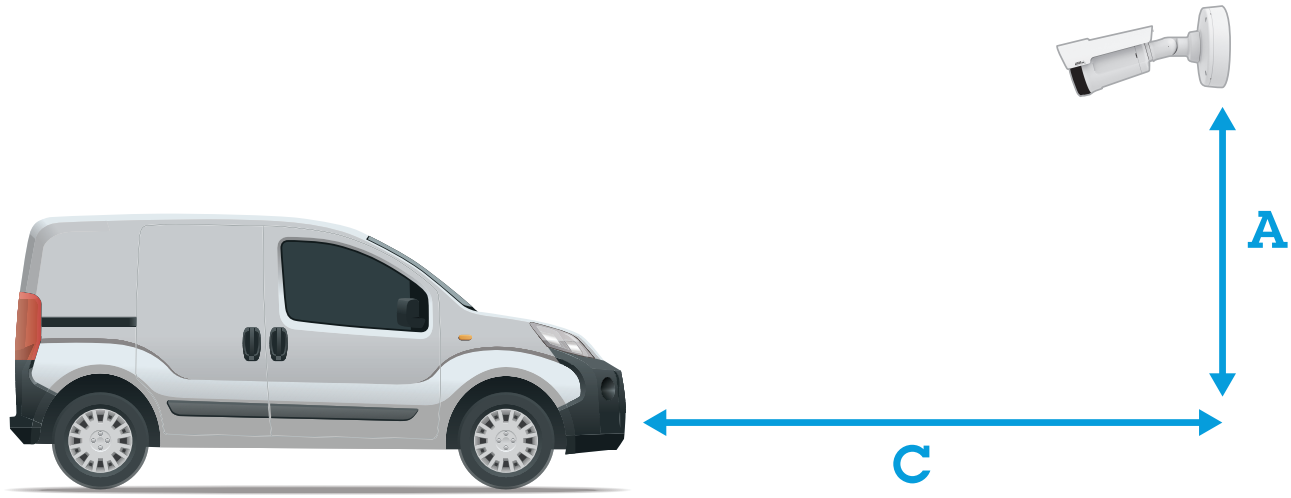
Konfiguracja podstawowa

Poniższe instrukcje dotyczące konfiguracji dotyczą wszystkich scenariuszy:

1.
2.
3.
4.
5.

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.



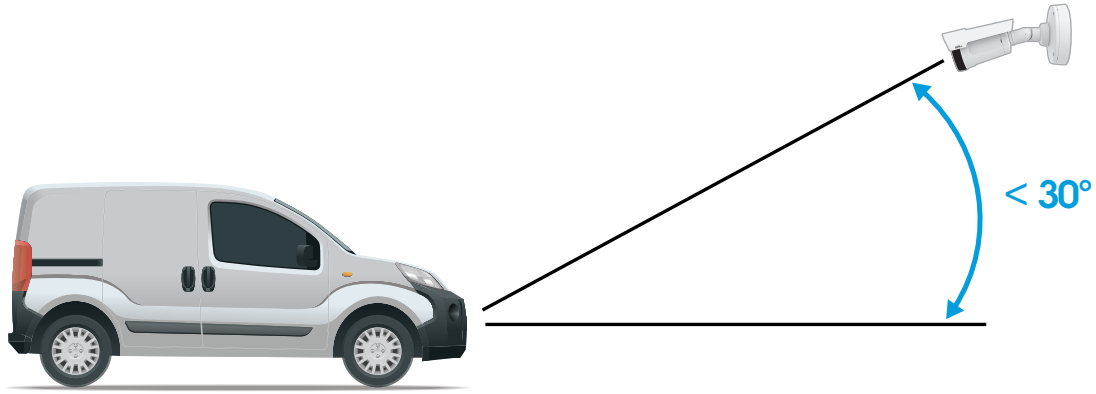
Odległość przechwytywania przy **kontroli dostępu**: 2–7 m (6,6–23 ft). Przykład na podstawie zestawu AXIS P3265–LVE-3 License Plate Verifier do weryfikacji tablic rejestracyjnych.

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)

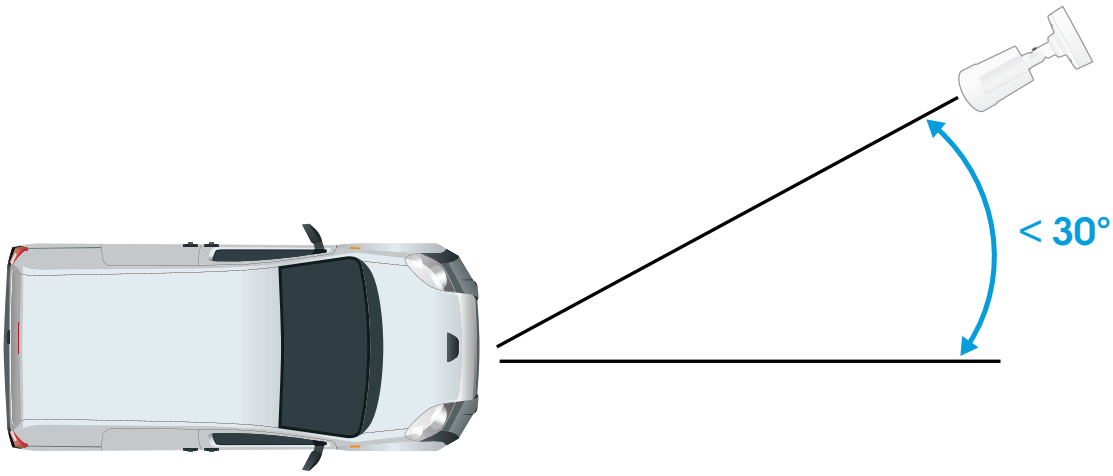
Odległość przechwytywania przy **swobodnym przepływie**: 7–20 m (23–65 ft). Przykład na podstawie zestawu AXIS P1465–LE-3 License Plate Verifier do weryfikacji tablic rejestracyjnych.

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.

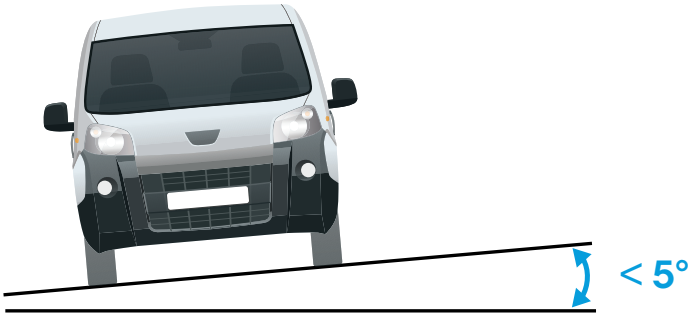


Kąt montażowy z boku.



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.

Uzyskiwanie dostępu do strony internetowej produktu

Jeśli nie znasz adresu IP swojego produktu, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować produkt w sieci. Obie aplikacje są darmowe i można je pobrać ze strony *axis.com/support*.

Zalecamy następujące przeglądarki:

- Chrome™
- Firefox®

1. Uruchom przeglądarkę internetową.
2. Wprowadź adres IP lub nazwę hosta produktu Axis w polu adresu przeglądarki.
3. Wprowadź nazwę użytkownika oraz hasło. Jeśli uzyskujesz dostęp do produktu po raz pierwszy, najpierw skonfiguruj hasło użytkownika root.
4. Jeśli uzyskujesz dostęp do produktu po raz pierwszy, otrzymasz komunikat o konieczności wstępnej konfiguracji niektórych ustawień. Kiedy skończysz, w przeglądarce zostanie otwarta strona podglądu na żywo produktu.

Więcej informacji dotyczących wykrywania i przypisywania adresów IP znajduje się w dokumencie Jak przypisać adres IP i uzyskać dostęp do urządzenia na stronie produktu w witrynie *axis.com*

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

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

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz .

Bezpieczne hasła

Ważne

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.

Asystent konfiguracji

Podczas uruchamiania aplikacji po raz pierwszy należy przy pomocy asystenta konfiguracji skonfigurować **Free flow (Swobodny przepływ)** lub **Access control (Kontrolę dostępu)**. Później można wprowadzić zmiany na karcie **Settings (Ustawienia)** w obszarze **Setup assistant (Asystent konfiguracji)**.

Swobodny przepływ

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

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

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 następującym formacie: `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)**.

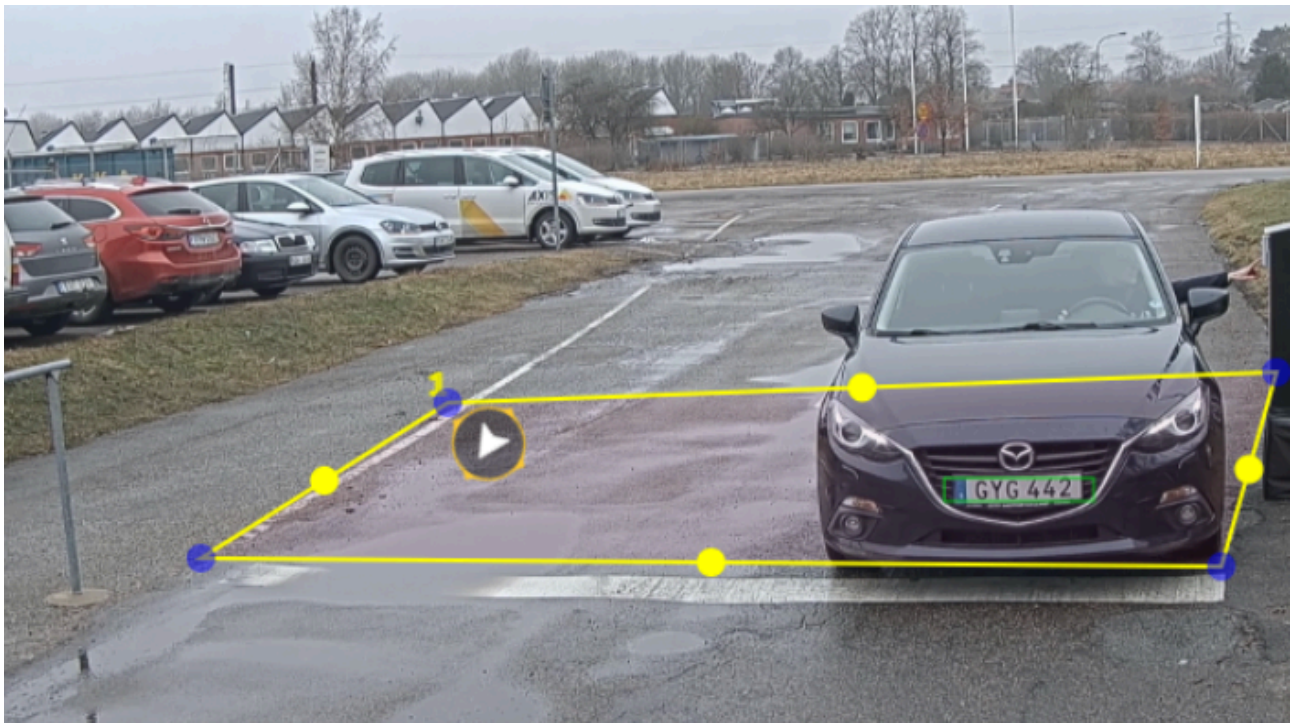
Dostosowywanie obszarów zainteresowania

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 **Edit area of interest (Edytuj obszar zainteresowania)**.
3. Aby poprawić weryfikację i jakość przechwytywanych obrazów, przejdź do ustawienia **Zoom** i dostosuj suwak do swoich potrzeb.
4. Aby kamera automatycznie ustawiała ostrość na pojazdach, kliknij przycisk **Autofocus (Autofokus)**. Aby ustawić ostrość ręcznie, przejdź do ustawienia **Focus (Ostrość)** i dostosuj ją za pomocą suwaka.
5. Aby przenieść obszar zainteresowania, kliknij wewnątrz tego obszaru, a następnie przesuń go w miejsce, w którym tablice rejestracyjne są najlepiej widoczne. Jeśli umieścisz obszar zainteresowania poza podglądem na żywo, automatycznie powróci on do domyślnego położenia. Upewnij się, że po zapisaniu tych ustawień obszar zainteresowania pozostaje w tym samym miejscu.
6. Aby dostosować obszar zainteresowania, kliknij w dowolnym miejscu w obszarze, a następnie przeciągnij punkty kotwiczące oznaczone na niebiesko.
   - Aby zresetować obszar zainteresowania, kliknij go prawym przyciskiem myszy i wybierz **Reset (Resetuj)**.
   - Aby dodać punkty kotwiczenia, kliknij jeden z żółtych punktów kotwiczenia. Kolor punktu kotwiczenia zmieni się na niebieski, co będzie oznaczało, że można nim manipulować. Obok niebieskiego punktu kotwiczenia zostaną automatycznie dodane nowe żółte punkty. Można wybrać maksymalnie 8 punktów kotwiczenia.
7. Kliknij w dowolnym miejscu poza obszarem zainteresowania, aby zapisać zmiany.
8. Aby uzyskać prawidłowe informacje zwrotne dotyczące kierunku w **Event log (Dzienniku zdarzeń)**, ustaw strzałkę w kierunku jazdy.
   8.1. Kliknij ikonę strzałki.
   8.2. Wybierz punkt kotwiczenia i obróć strzałkę, tak aby była ustawiona zgodnie z kierunkiem jazdy.
   8.3. Kliknij poza obszarem zainteresowania, aby zapisać zmiany.

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

- Aby dodać drugi obszar zainteresowania, wybierz **2** z menu rozwijanego **Area of interest** (Obszar zainteresowania).



Przykład z jednym obszarem zainteresowania.

Uwaga

- W przypadku używania kamery autonomicznej można wybrać w aplikacji zalecane ustawienia rozpoznawania tablic rejestracyjnych.
  1. Kliknij **Recommended LPR settings (Zalecane ustawienia rozpoznawania tablic rejestracyjnych)**. Zostanie wyświetlona tabela, w której będzie widać różnice między bieżącymi i zalecanymi ustawieniami.
  2. Kliknij **Update settings (Aktualizuj ustawienia)**, aby zmienić wartości ustawione w aplikacji na zalecane.

Wybór regionu

1. Przejdź do menu **Settings (Ustawienia)** > **Image (Obraz)**.
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 opcji **Resolution (Rozdzielczość)**
3. Aby zmienić obrót przechwytywanych obrazów, przejdź do opcji **Image rotation (Obracanie obrazu)**
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.

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 opcji **Settings (Ustawienia)** > **Events (Zdarzenia)**.
2. W menu **Save events (Zapisz zdarzenia)** wybierz polecenie **Allowlisted (Lista dozwolonych)**.
3. W menu **Delete events after (Usuń zdarzenia po)** wybierz opcję **30 days (30 dni)**.

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.

Aby zmienić ustawienia przechwytywania obrazu, przejdź do **Settings > Image (Ustawienia > Obraz)**. Na karcie SD można zapisać do 100 000 zdarzeń z użyciem dowolnego typu ramki.

Zarządzanie listami

Dodawanie wykrytej tablicy rejestracyjnej do listy

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

1. Kliknij kartę **Event log (Dziennik zdarzeń)**.
2. Przejdź do **Latest Event (Ostatniego zdarzenia)**.
3. Kliknij przycisk **Add to list (Dodaj do listy)** znajdujący się obok tablicy rejestracyjnej, którą chcesz dodać.
4. Z menu rozwijanego wybierz listę, do której chcesz dodać tablicę rejestracyjną.
5. Kliknij **Append (Dodaj)**.

Uwaga

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

Dodawanie opisów do tablic rejestracyjnych

Aby dodać opis do tablicy rejestracyjnej na liście:

- Przejdź do **List management (Zarządzania listami)**.
- Zaznacz tablicę rejestracyjną, którą chcesz edytować, i kliknij ikonę pióra.
- Wpisz odpowiednie informacje w polu **Description (Opis)** na górze listy.
- Kliknij ikonę dysku, aby zapisać nowe ustawienia.

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. Przejdź do menu listy, którą chcesz zmienić.
3. Wybierz opcję **Rename (Zmień nazwę)**.
4. Wpisz nazwę listy.

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. Przejdź do menu kontekstowego znajdującego się obok **Allowlist (Listy dozwolonych)** i wybierz opcję **Import from file (Importuj z pliku)**.

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 (Zarządzania listami)**.
2. W polu **Camera synchronization (Synchronizacja kamery)** wpisz adres IP, nazwę użytkownika i hasło.
3. Kliknij **+**.
4. Kliknij **Camera synchronization (Synchronizacja kamery)**.
5. Sprawdź, czy data i godzina w polu **Last sync (Ostatnia synchronizacja)** została zaktualizowana.

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. Ustaw **Overlay duration (Czas nałożenia)** na wartość od 1 do 9 sekund.
4. Wybierz opcję data, godzina i tablica rejestracyjna (**DateTime + LP**) lub samą tablicę rejestracyjną (**LP**).
5. Sprawdź, czy nakładka jest widoczna w podglądzie na żywo.

Detekcja tablic rejestracyjnych przy słabym oświetleniu

Algorytm przypisuje każdej dokonanej detekcji ocenę, zwaną poziomem czułości (parametr ufności). Detekcje o ocenie poniżej wartości wybranego poziomu nie są wyświetlane na liście zdarzeń.

W scenach o słabym oświetleniu można obniżyć poziom czułości.

1. Przejdź do opcji **Settings (Ustawienia)** > **Detection Parameters (Parametry detekcji)**.
2. Dostosuj suwak pod **Sensitivity level (Poziomem czułości)**. Aby uniknąć fałszywych detekcji, zalecamy obniżanie wartości progowej co 0,05.
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 opcji **Settings (Ustawienia)** > **Detection Parameters (Parametry detekcji)**.
2. W polu **Minimum number of characters (Minimalna liczba znaków)** wpisz minimalną dozwoloną liczbę znaków.
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 opcji **Settings (Ustawienia)** > **Detection Parameters (Parametry detekcji)**.
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 obszarze HTTPS, **Enable HTTPS (Włącz HTTPS)**.
3. Wybierz opcję **Self-signed (Z własnym podpisem)** lub **CA-signed (Z podpisem CA)**.

Uwaga

Więcej informacji na temat protokołu HTTPS i jego zastosowań: .

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 obszarze **Access control (Kontrola dostępu)** z listy rozwijanej wybierz **Type (Typ)**, a następnie **Internal I/O (Wewnętrzne I/O)**.
4. Wybierz **I/O output # (Numer wyjścia I/O)**.
5. Na liście rozwijanej **Virtual port (Port wirtualny)** zaznacz port.
6. Z listy rozwijanej **Barrier mode (Tryb szlabanu)** wybierz opcję **Open to all (Otwarty dla wszystkich)**.
7. Z listy rozwijanej **Vehicle direction (Kierunek jazdy)** wybierz opcję **any (dowolny)**.
8. Na liście rozwijanej **ROI (Obszar zainteresowania)** zaznacz obszar zainteresowania, którego chcesz użyć, lub wszystkie.
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.

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.
4. Jeżeli wprowadzisz jakiekolwiek zmiany w źródle sygnału wejściowego, kliknij przycisk **Apply changes (Zastosuj zmiany)**.

Edytuj profil strumienia używany do rejestracji:

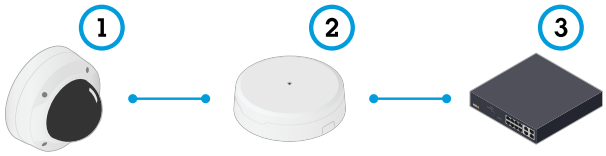
5. Przejdź do okna **System > Stream profiles (System > Profile strumienia)** i wybierz profil strumienia.
6. Kliknij opcję **Include audio (Dołącz audio)** i włącz ją.
7. Kliknij przycisk **Zapisz**.

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*

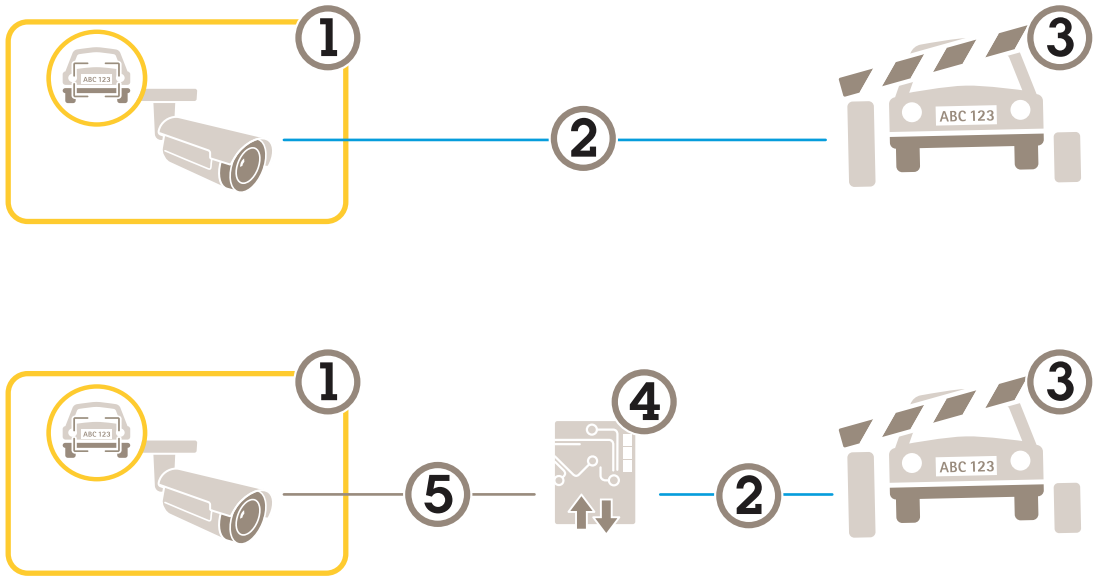
Po podłączeniu urządzeń w ustawieniach urządzenia sieciowego dozoru wizyjnego Axis będzie widoczna karta dźwięku. Przejdź do karty Audio i włącz opcję **Allow audio (Zezwalaj na dźwięk)**.

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

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 przekaźnikowe 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 .

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 .



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

1. Przejdź do strony internetowej aplikacji i wybierz kartę **Event log (Dziennik zdarzeń)** i dodaj wykryte tablice rejestracyjne do listy. Patrz
2. Aby bezpośrednio edytować listę, przejdź do karty **List management (Zarządzanie listami)**.
3. Wprowadź autoryzowany numer tablicy rejestracyjnej w polu **Allowlist (Lista dozwolonych)**.
4. Przejdź do karty **Settings (Ustawienia)**.
5. W obszarze **Access control (Kontrola dostępu)** z listy rozwijanej wybierz **Type (Typ)**, a następnie **Internal I/O (Wewnętrzne I/O)**.
6. Wybierz **I/O output # (Numer wyjścia I/O)**.
7. Z listy rozwijanej **Barrier mode (Trybu szlabanu)** wybierz opcję **Open from lists (Otwórz z list)**, a następnie zaznacz **Allowlist (Listę dozwolonych)**.

8. Z listy rozwijanej **Vehicle direction (Kierunek jazdy)** wybierz opcję **in (wjazd)**.
9. Na liście rozwijanej **ROI (Obszar zainteresowania)** zaznacz obszar zainteresowania, którego chcesz użyć, lub wszystkie.
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:

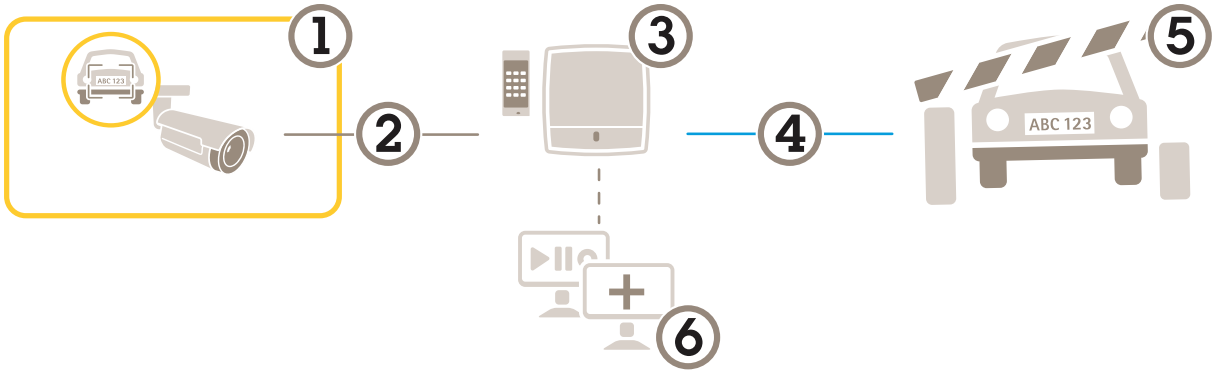
- Konfiguracja podstawowa. Patrz .

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 wyzwala zdarzenia.

Uwaga

Niniejsza instrukcja dotyczy wyłącznie kontrolera drzwiowego AXIS A1001 Door controller.

Nie zapomnij odświeżyć stron internetowych, aby uzyskać dostęp do wszystkich parametrów podczas przełączania się pomiędzy aplikacjami AXIS License Plate Verifier a AXIS Entry Manager.

Wymagania:

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

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

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)**.

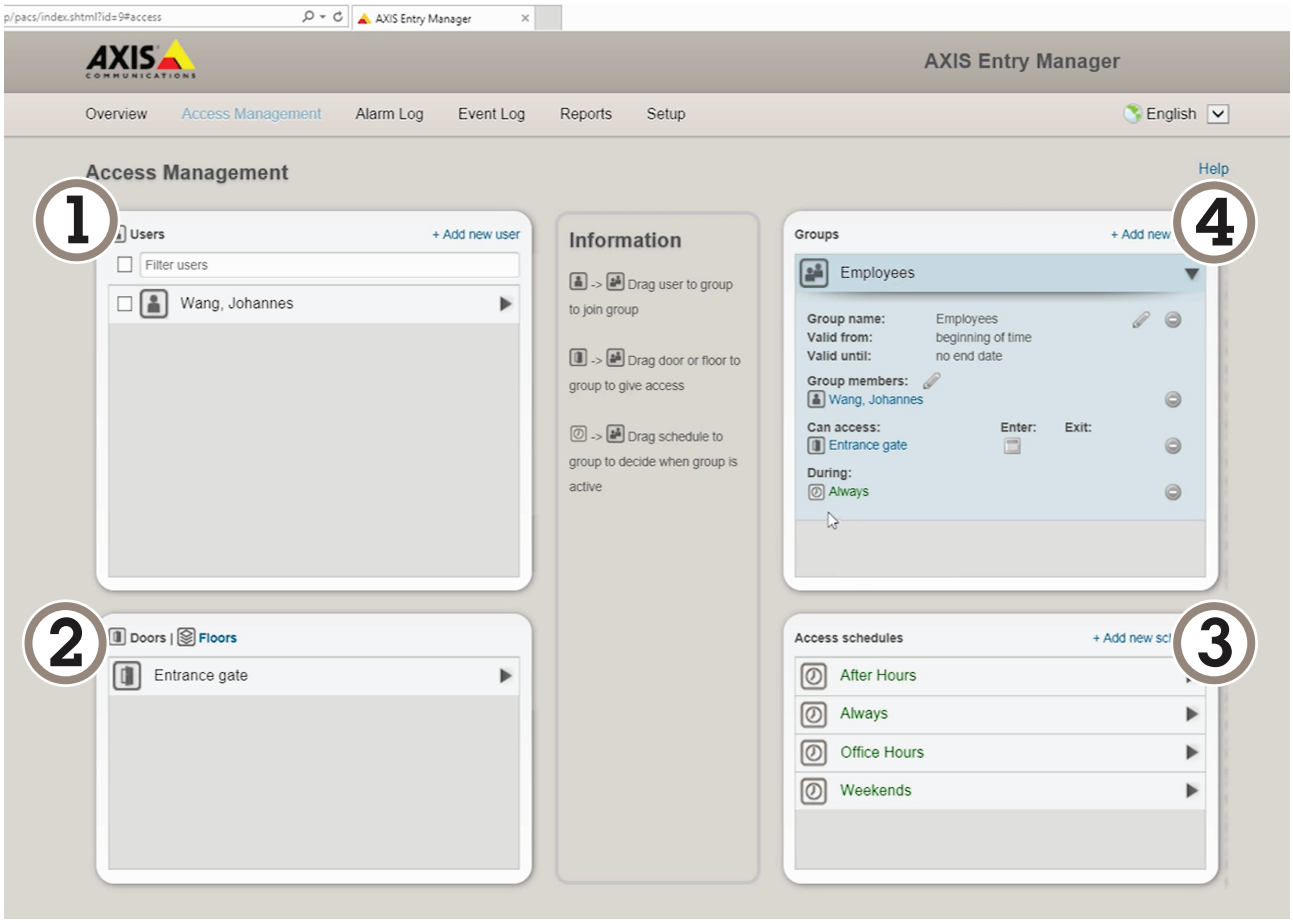
4. W opcji **Configure locks connected to this controller (Skonfiguruj zamki podłączone do tego kontrolera)** usuń opcję **Door monitor (Monitor drzwi)**.
5. Kliknij **Next (Dalej)**.
6. W opcji **Configure readers connected to this controller (Skonfiguruj czytniki podłączone do tego kontrolera)** usuń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

Uwaga

Poniższe instrukcje dotyczą wyłącznie następujących urządzeń: A1210, A1201-B, A1214, A1610, A1610-B, A1710-B i A1810-B.

Wymagania:

- Kamera i kontroler drzwiowy zainstalowane i dołączone do sieci IP.
- Aplikacja AXIS License Plate Verifier działa w kamerze.
- Zainstalowany klient aplikacji AXIS Camera Station w wersji 5.49.449 lub nowszej.
- Konfiguracja podstawowa. Patrz .

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 dres 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 .
15. Kliknij dwa razy przycisk **Next (Dalej)** i kliknij **Finish (Zakończ)**.

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. W menu rozwijanym **Profiles (Profile)** zaznacz profil.
2. Skonfiguruj regułę. Patrz .
3. Kliknij przycisk Zapisz.
4. W menu rozwijanym **Profiles (Profile)** zaznacz nowy profil.

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, przesyłając 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. Z listy rozwijanej **Protocol (Protokół)** wybierz jeden z następujących protokołów:
   - TCP
   - HTTP POST
     - Wprowadź nazwę użytkownika i hasło.
3. W polu **Server URL (Adres URL serwera)** wpisz adres serwera i port w następującym formacie: `127.0.0.1:8080`
4. W polu **Device ID (ID urządzenia)** wpisz nazwę urządzenia lub pozostaw pole bez zmian.
5. 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.
6. Aby włączyć tę funkcję, wybierz opcję **Send event data to server (Wysyłaj dane zdarzeń na serwer)**.
7. 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)**.
8. Kliknij przycisk **Zapisz**.

Uwaga

Aby wysyłać informacje o zdarzeniach za pomocą metody HTTP POST, można używać nagłówka autoryzacji zamiast nazwy użytkownika i hasła. Przejdź do pola **Auth-Header** i dodaj ścieżkę do interfejsu API uwierzytelniania.

Wysłanie obrazu z tablic rejestracyjnych do serwera

Funkcja ta pozwala przesyłać 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. 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.
5. Wpisz nazwę użytkownika i hasło serwera FTP.
6. Wybierz ścieżkę i modyfikatory nazw plików.
7. Kliknij **Gotowe**.
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.

   Uwaga

   Kierunek jest uwzględniany w nazwie pliku tylko w przypadku wybrania opcji **Lost (Utrata)** lub **Update (Aktualizacja)**.
9. Aby włączyć tę funkcję, wybierz opcję **Send event data to server (Wysyłaj dane zdarzeń na serwer)**.
10. Kliknij przycisk **Zapisz**.

Uwaga

Uwaga: obraz może się różnić w zależności od wybranego trybu rejestracji. Patrz .

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 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. Dodaj adres IP lub URL w urządzeniu 2N.

3. Wybierz **Connection type (Typ połączenia)**.
4. Wybierz, **do czego będzie używana ten szlaban**.
5. Wpisz swoją nazwę użytkownika i hasło.
6. Kliknij przycisk **Enable integration (Włącz integrację)**.
7. Kliknij przycisk **Zapisz**.

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 SQLEXPRESS 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 karty **Integration (Integracja)**.
2. Z listy rozwijanej wybierz opcję **Genetec Security Center**.
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. Kliknij przycisk **Enable integration (Włącz integrację)**.
6. Przejdź do karty **Settings (Ustawienia)**.
7. W ustawieniu **Security > HTTPS (Zabezpieczenia > HTTPS)**.
8. 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 przejść do interfejsu WWW urządzenia, wpisz adres IP urządzenia w przeglądarce internetowej.

Uwaga

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

Wyświetl/ukryj menu główne.

Wyświetl informacje o wersji.

Uzyskaj dostęp do pomocy dotyczącej produktu.

Zmień język.

Ustaw jasny lub ciemny motyw.

Menu użytkownika zawiera opcje:

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

Menu kontekstowe zawiera opcje:

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

Status

Bezpieczeństwo

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

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

Stan synchronizacji czasu

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

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

Trwające zapisy

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

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

 Pokazuje lokalizację zapisu nagrania w zasobie.

Informacje o urządzeniu

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

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

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

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

Nagranie wideo

Kliknij, aby odtworzyć strumień wideo na żywo.

Kliknij, aby zatrzymać odtwarzanie strumienia wideo na żywo.

Kliknij, aby zapisać zrzut ekranu ze strumienia wideo na żywo. Plik jest zapisywany w folderze „Pobrane" na komputerze. Nazwa pliku to [snapshot_YYYY_MM_DD_HH_MM_SS.jpg]. Rozmiar pliku zależy od kompresji zastosowanej w przeglądarce internetowej, do której przysyłane jest ujęcie, więc może on różnić się od wartości ustawienia kompresji w urządzeniu.

Kliknij, aby wyświetlić porty wyjścia we/wy. Użyj przełącznika, aby otworzyć lub zamknąć obwód portu, na przykład w celu przetestowania urządzeń zewnętrznych.

Kliknij, aby ręcznie włączyć lub wyłączyć oświetlenie w podczerwieni.

Kliknij, aby ręcznie włączyć lub wyłączyć oświetlanie białym światłem.

Kliknij, aby uzyskać dostęp do ekranowych elementów sterowania. Włącz grupy ekranowych elementów sterowania, aby użytkownicy mogli uzyskiwać dostęp do ustawień w każdej grupie klikając prawym przyciskiem myszy strumień wideo w oprogramowaniu do zarządzania materiałem wizyjnym.

- **Predefined controls (Wstępnie zdefiniowane elementy sterowania)**: Wyświetla domyślne ekranowe elementy sterowania.
- **Custom controls (Niestandardowe elementy sterowania)**: Kliknij **Add custom control (Dodaj niestandardowy element sterowania)**, aby utworzyć niestandardowe ekranowe elementy sterowania.

Służy do uruchomienia myjki. Po rozpoczęciu sekwencji mycia kamera przemieszcza się do skonfigurowanej pozycji, gdzie jest spryskiwana. Po całej zakończeniu sekwencji mycia kamera powraca do poprzedniej pozycji. Ikona jest widoczna tylko po podłączeniu i skonfigurowaniu myjki.

Służy do uruchomienia wycieraczki.

Kliknij i wybierz prepozycję, aby do niej przejść w widoku na żywo. Można też kliknąć przycisk **Setup (Ustawienia)** i przejść do strony prepozycji.

Dodawanie lub usuwanie obszaru przywracania ostrości. Po dodaniu obszaru przywracania ostrości kamera zapisuje ustawienia ostrości w danym zakresie obrotu/pochylenia. Po ustawieniu obszaru przywracania ostrości kamera będzie odtwarzać uprzednio zapisaną ostrość wtedy, gdy znajdzie się w tym obszarze w podglądzie na żywo. Wystarczy pokrycie połowy obszaru, aby kamera przywróciła ostrość.

Kliknij, aby wybrać trasę strażnika, a następnie kliknij **Start (Rozpocznij)**, aby odtworzyć trasę strażnika. Alternatywnie kliknij przycisk **Setup (Ustawienia)** i przejdź do strony tras strażników.

Kliknij, aby ręcznie włączyć grzejnik na określony czas.

Kliknij, aby rozpocząć ciągłą rejestrację strumienia wideo na żywo. Kliknij przycisk ponownie, aby zatrzymać rejestrację. Jeżeli rejestrowanie jest w toku, po ponownym uruchomieniu kamery zostanie wznowione automatycznie.

Kliknij, aby wyświetlić pamięć masową skonfigurowaną dla urządzenia. Aby skonfigurować pamięć masową, należy zalogować się jako administrator.

Kliknij, aby przejść do ustawień automatycznego śledzenia. Więcej ustawień jest dostępnych po kliknięciu ikony w sekcji **Analytics > Autotracking** (Narzędzia analityczne > Automatyczne śledzenie).

Kliknij, aby wyświetlić więcej ustawień:

- **Format wideo**: Wybierz format kodowania, który ma być zastosowany w podglądzie na żywo.
- **Autoplay (Odtwarzanie automatyczne)**: Włącz, aby automatycznie odtwarzać wyciszony strumień wideo przy każdym otwarciu urządzenia w nowej sesji.
- **Client stream information (Dane strumienia klienta)**: Włącz, aby wyświetlać dynamiczne informacje o strumieniu wideo na żywo odtwarzanym w przeglądarce. Informacje o przepływności różnią się od informacji podanych w nakładce tekstowej, ponieważ pochodzą one z różnych źródeł. Przepływność w informacjach o strumieniu na urządzeniu klienckim dotyczy ostatniej sekundy i pochodzi ze sterownika kodowania w urządzeniu. Przepływność w nakładce tekstowej to średnia z ostatnich 5 sekund i pochodzi z przeglądarki. Obie wartości obejmują tylko nieprzetworzony strumień wideo, a nie dodatkową przepustowość generowaną w trakcie przesyłania przez sieć przy użyciu protokołu UDP/TCP/HTTP.
- **Adaptive stream (Strumień adaptacyjny)**: Włącz, aby dostosować rozdzielczość obrazu do rzeczywistej rozdzielczości wyświetlania w kliencie, co poprawi jakość odbioru i zapobiegnie przeciążeniu sprzętu klienta. Strumień adaptacyjny jest stosowany tylko podczas oglądania strumienia wideo na żywo w interfejsie WWW za pomocą przeglądarki internetowej. Po włączeniu funkcji strumienia adaptacyjnego maksymalna poklatkowość wynosi 30 kl./s. Wykonanie zrzutu ekranu przy włączonej funkcji strumienia adaptacyjnego spowoduje, że zrzut użyje rozdzielczości obrazu wybranej w strumieniu adaptacyjnym.
- **Level grid (Siatka poziomu)**: Kliknij , aby wyświetlać siatkę poziomu. Siatka pomaga stwierdzić, czy obraz jest wyrównany w poziomie. Kliknij , aby ukryć siatkę.
- **Licznik pikseli**: Kliknij , aby wyświetlić licznik pikseli. Przeciągnij ten obszar i zmień jego rozmiar, aby objąć nim obszar zainteresowanie. W polach **Width (Szerokość)** i **Height (Wysokość)** można również zdefiniować liczbę pikseli określającą rozmiar obszaru.
- **Refresh (Odśwież)**: Kliknij , aby odświeżyć nieruchomy obraz w podglądzie na żywo.
- **PTZ controls (Sterowanie PTZ)** : Włączenie opcji spowoduje wyświetlenie elementów sterowania parametrami PTZ w widoku na żywo.

Kliknij, aby wyświetlać podgląd na żywo w pełnej rozdzielczości. Jeśli pełna rozdzielczość jest większa niż rozmiar ekranu, do nawigowania po obrazie użyj mniejszej rozdzielczości.

Kliknij, aby wyświetlać strumień wideo na żywo na pełnym ekranie. Naciśnij ESC, aby opuścić tryb pełnoekranowy.

Instalacja

Capture mode (Tryb przechwytywania) : Tryb rejestracji to predefiniowana konfiguracja, która określa sposób zapisywania obrazów przez kamerę. Zmiana trybu rejestracji może wpłynąć na inne ustawienia, takie jak obszary obserwacji i maski prywatności.

Mounting position (Pozycja montażowa) : Orientacja obrazu może się zmieniać w zależności od sposobu zamontowania kamery.

Power line frequency (Częstotliwość zasilania): Wybierz częstotliwość używaną w miejscu użytkowania instalacji, aby zminimalizować migotanie obrazu. W Ameryce z reguły używa się częstotliwości 60 Hz. W pozostałej części świata przeważają sieci o częstotliwości 50 Hz. Jeżeli nie wiesz, z której częstotliwości korzysta sieć w Twoim regionie, zapytaj lokalne władze.

Rotate (Obróć): Wybierz preferowaną orientację obrazu.

Zoom : Użyj suwaka, aby dostosować stopień powiększenia.

Autofocus after zooming (Autofokus po zoomowaniu) : włącz tę opcję, aby włączyć autofokus po zoomowaniu.

Focus (Ostrość): Użyj suwaka, aby manualnie ustawić ostrość.

Autofocus (Autofokus): Kliknij, aby włączyć samoczynne ustawianie ostrości na wybranym obszarze. Jeżeli nie wybrano obszaru autofokusu, kamera ustawia ostrość dla całej sceny.

Autofocus area (Obszar autofokusu): Kliknij , a zostanie wyświetlony obszar automatycznego ustawiania ostrości. Ten obszar powinien obejmować obszar zainteresowania.

Reset focus (Resetuj ostrość): Kliknij, aby przywrócić poprzednie umiejscowienie obszaru ostrości.

Uwaga

W niskich temperaturach może upłynąć kilka minut, zanim zoom i ostrość staną się dostępne.

Korekcja obrazu

Ważne

Zalecamy, aby nie używać wielu funkcji korekcji obrazu jednocześnie, ponieważ może to powodować problemy z wydajnością.

Barrel distortion correction (BDC) (Korekcja dystorsji beczkowatej) : Włącz tę opcję, aby uzyskać bardziej wyprostowany obraz, jeżeli ulega temu zniekształceniu. Dystorsja beczkowata to zniekształcenie obrazu polegające na jego zakrzywieniu i wygięciu na zewnątrz. Jest ona bardziej widoczna w przypadku obrazów z małym zoomem.

Crop (Przytnij) : Użyj suwaka, aby dostosować poziom korekcji. Niższy poziom oznacza zachowanie szerokości obrazu kosztem wysokości i rozdzielczości. Wyższy poziom oznacza zachowanie wysokości i rozdzielczości obrazu kosztem szerokości.

Remove distortion (Usuń dystorsję) : Użyj suwaka, aby dostosować poziom korekcji. Opcja Pucker (Ściągnij) spowoduje zachowanie szerokości obrazu kosztem wysokości i rozdzielczości. Opcja Bloat (Rozciągnij) pozwala na zachowanie wysokości i rozdzielczości obrazu kosztem szerokości.

Image stabilization (Stabilizacja obrazu) : Włącz tę opcję, aby uzyskać płynniejszy i stabilniejszy obraz z mniejszym rozmyciem. Zalecamy używanie funkcji stabilizacji obrazu w środowiskach, w których produkt jest zamontowany na zewnątrz budynku i narażony na drgania, np. z powodu wiatru lub ruchu pojazdów.

Focal length (Długość ogniskowej) : Użyj suwaka, aby dostosować długość ogniskowej. Wyższa wartość powoduje większe powiększenie i węższy kąt widzenia; krótsza długość ogniskowej oznacza z kolei mniejsze powiększenie i szerszy kąt widzenia.

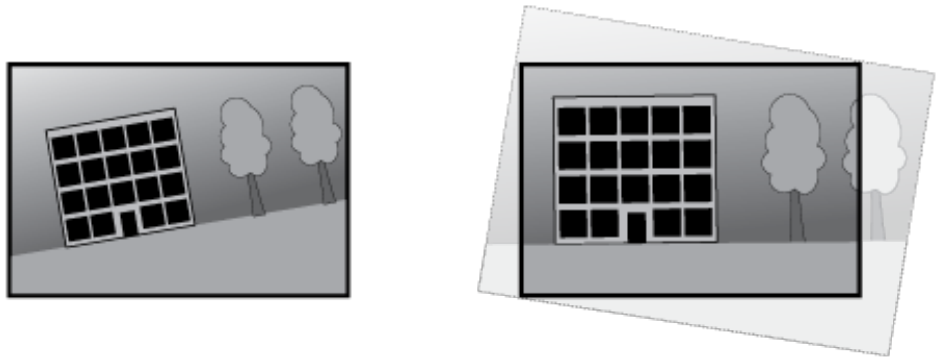
Stabilizer margin (Margines stabilizatora) : Użyj suwaka, aby dostosować wielkość marginesu stabilizacji, co spowoduje ustalenie poziomu drgań do ustabilizowania. Jeżeli produkt zamontowano w miejscu, w którym występują znaczne drgania, przesuń suwak w kierunku pozycji **Max (Maks.)**. W rezultacie zostanie uchwycona scena o mniejszych wymiarach. Jeżeli produkt zamontowano w miejscu, w którym występuje mniej drgań, przesuń suwak w stronę pozycji **Min**.

Korekcja oddychania obiektywu : Włącz tę opcję, aby zachować stały kąt widzenia podczas zmiany ustawienia ostrości. Gdy ta funkcja jest włączona, dostępny zakres zbliżenia może być ograniczony.

Straighten image (Wyprostuj obraz) : Włącz tę opcję, a następnie za pomocą suwaka wyprostuj obraz w poziomie dzięki cyfrowemu obrotowi i kadrowaniu. Funkcja jest przydatna wtedy, gdy nie można idealnie wypoziomować kamery. Najlepiej prostować obraz podczas montażu kamery.

: Kliknij, aby wyświetlać siatkę pomocniczą na obrazie.

: Kliknij, aby ukryć siatkę.



Obraz sprzed wyprostowania i po wyprostowaniu.

Zdjęcie

Wygląd

Scene profile (Profil sceny) : Wybierz profil sceny pasujący do scenariusza dozoru. Profil sceny optymalizuje ustawienia obrazu, w tym poziom koloru, jasność, ostrość, kontrast i kontrast lokalny, dla określonego środowisku lub przeznaczenia.

- **Forensic (Do celów dochodzenia)** : Nadaje się na potrzeby dozoru.
- **Indoor (Do montażu wewnątrz budynków)** : Nadaje się do wnętrz budynków.
- **Outdoor (Do montażu na zewnątrz)** : Nadaje się do miejsc poza budynkami.
- **Vivid (Żywe kolory)** : Nadaje się do prezentacji.
- **Traffic overview (Podgląd ruchu drogowego)** : Nadaje się do monitorowania ruchu pojazdów.
- **License plate (Tablica rejestracyjna)** : Nadaje się do monitorowania tablic rejestracyjnych.

Nasycenie: Użyj suwaka, aby dostosować intensywność kolorów. Można na przykład uzyskać obraz w odcieniach szarości.



Kontrast: Suwak służy do regulacji różnicy między jasnymi a ciemnymi fragmentami obrazu.



Jasność: Użyj suwaka, aby dostosować intensywność światła. Może to poprawić widoczność obiektów. Ustawienie jasności jest stosowane po rejestracji obrazu i nie wpływa na zawarte w nim informacje. Aby uzyskać lepszą widoczność szczegółów na ciemnym obszarze, zazwyczaj lepiej jest zwiększyć wzmocnienie lub czas ekspozycji.



Sharpness (Ostrość): Aby zwiększyć wyrazistość obiektów na obrazie, należy za pomocą suwaka wyregulować kontrast krawędzi. Zwiększenie ostrości może spowodować wzrost przepływności bitowej i efekcie zapotrzebowania na zasób.



Szeroki zakres dynamiki

WDR : Włącz tę funkcję, aby wyświetlić zarówno ciemne, jak i jasne obszary na obrazie.

Local contrast (Kontrast lokalny) : Za pomocą suwaka wyreguluj kontrast obrazu. Wyższa wartość zwiększa kontrast pomiędzy ciemnymi i jasnymi obszarami.

Tone mapping (Mapowanie tonowe) : Suwak ten służy do zmiany wartości mapowania tonalnego zastosowanego na obrazie. Jeżeli wartość ta wynosi zero, to stosowana jest tylko standardowa korekcja gamma; wyższa wartość zwiększa widoczność najjaśniejszych i najciemniejszych fragmentów obrazu.

Równoważenie bieli

Kiedy kamera wykryje temperaturę barwową docierającego do niej światła, może ona dostosować obraz w celu zwiększenia naturalności kolorów. Jeśli to nie wystarczy, można wybrać odpowiednie źródło światła z listy.

Automatyczne ustawienie balansu bieli zmniejsza ryzyko migotania dzięki stopniowemu dostosowywaniu się do zmian. W przypadku zmiany oświetlenia lub podczas pierwszego uruchomienia kamery dostosowanie się do nowego źródła światła może zająć maksymalnie 30 sekund. Jeżeli w scenie znajduje się więcej niż jeden typ źródła światła, tj. różnią się one temperaturą barwową, to algorytm automatycznego balansu bieli bierze pod uwagę dominujące źródło światła. Można to obejść poprzez wybranie stałego balansu bieli, który dostosowuje się do referencyjnego źródła światła.

Light environment (Środowisko oświetlenia):

- **Automatic (Automatycznie)**: Automatyczna identyfikacja i kompensacja względem koloru źródła światła. Jest to zalecane ustawienie, które można wykorzystać w większości sytuacji.
- **Automatic – outdoors (Automatyczne – na zewnątrz)** : Automatyczna identyfikacja i kompensacja względem koloru źródła światła. Jest to zalecane ustawienie, które można wykorzystać w większości sytuacji dla dozoru na zewnątrz pomieszczeń.
- **Custom – indoors (Niestandardowe – we wnętrzu)** : Stałe dostosowanie koloru dla pomieszczenia z oświetleniem innym niż jarzeniowe, odpowiednie dla zwykłej temperatury barwowej około 2800 K.
- **Custom – indoors (Niestandardowe – na zewnątrz)** : Stałe dostosowanie koloru dla słonecznej pogody z temperaturą barwową około 5500 K.
- **Fixed – fluorescent 1 (Stały — fluorescencyjny 1)**: Stałe dostosowanie koloru dla oświetlenia jarzeniowego z temperaturą barwową około 4000 K.
- **Fixed – fluorescent 2 (Stały — fluorescencyjny 2)**: Stałe dostosowanie koloru dla oświetlenia jarzeniowego z temperaturą barwową około 3000 K.
- **Fixed – indoors (Stały — wewnętrzny)**: Stałe dostosowanie koloru dla pomieszczenia z oświetleniem innym niż jarzeniowe, odpowiednie dla zwykłej temperatury barwowej około 2800 K.
- **Fixed – outdoors 1 (Stały — zewnętrzny 1)**: Stałe dostosowanie koloru dla słonecznej pogody z temperaturą barwową około 5500 K.
- **Fixed – outdoors 2 (Stały — zewnętrzny 2)**: Stałe dostosowanie koloru dla pochmurnej pogody z temperaturą barwową około 6500 K.
- **Street light – mercury (Światło uliczne – rtęciowe)** : Stałe dostosowanie koloru dla typowej emisji rtęciowego oświetlenia ulicznego.
- **Street light – sodium (Światło uliczne – sodowe)** : Stałe dostosowanie koloru, z kompensacją względem typowego pomarańczowego oświetlenia ulicznego.
- **Hold current (Zachowaj bieżący)**: Zachowuje bieżące ustawienia bez kompensacji względem zmian oświetlenia.
- **Manual (Manualnie)** : Umożliwia ustalenie balansu bieli na podstawie białego obiektu. Przeciągnij okrąg na obiekt, który ma być interpretowany jako biały w podglądzie na żywo. Użyj suwaków **Red balance (Balans czerwieni)** i **Blue balance (Balans niebieskiego)**, aby ręcznie dostosować balans bieli.

Tryb dzień/noc

IR-cut filter (Filtr odcinający promieniowanie IR):

- **Automatycznie**: Zaznaczenie tej opcji spowoduje automatyczne włączanie i wyłączanie filtr odcinającego promieniowanie IR. W trybie dziennym filtr odcinający promieniowanie IR jest włączony i blokuje promieniowanie podczerwone; w trybie nocnym jest on wyłączany, co powoduje zwiększenie światłoczułości kamery.

Uwaga

- Niektóre urządzenia mają filtry przepuszczające promieniowanie podczerwone w trybie nocnym. Filtr przepuszczający promieniowanie podczerwone zwiększa czułość na światło podczerwone, ale blokuje światło widzialne.
- **On (Wł.)**: Zaznacz tę opcję, aby włączyć filtr odcinający promieniowanie podczerwone. Obraz jest kolorowy, ale przy znacznie ograniczonej światłoczułości.
- **Off (Wyłączona)**: Zaznacz tę opcję, aby wyłączyć filtr odcinający promieniowanie podczerwone. Obraz jest czarno-biały w celu zwiększenia światłoczułości.

Threshold (Próg): Użyj suwaka, aby ustawić próg oświetlenia, przy którym tryb kamery zmienia się z dziennego na nocny.

- Aby obniżyć próg dla filtra odcinającego promieniowanie podczerwone, przesuń suwak w kierunku wartości **Bright (Jasno)**. Kamera przełączy się na tryb nocny wcześniej.
- Aby zwiększyć próg dla filtra odcinającego promieniowanie podczerwone, przesuń suwak w kierunku wartości **Dark (Ciemno)**. Kamera przełączy się na tryb nocny później.

Promieniowanie IR

Jeżeli urządzenie nie ma wbudowanego oświetlenia, te elementy sterowania będą dostępne wyłącznie po podłączeniu obsługiwanego oświetlacza Axis.

Allow illumination (Zezwalaj na oświetlenie): Włącz tę opcję, aby umożliwić kamerze używanie wbudowanego oświetlenia w trybie nocnym.

Synchronize illumination (Synchronizuj oświetlenie): Włączenie tej opcji spowoduje automatyczne synchronizowanie oświetlenia z natężeniem światła w otoczeniu. Synchronizacja pomiędzy dniem i nocą działa tylko wtedy, gdy filtr odcinający promieniowanie IR ustawiono na **Automatyczne** lub **Wył.**.

Automatic illumination angle (Automatyczny kąt oświetlenia) : Włącz tę opcję, aby używać automatycznego kąta oświetlenia. Wyłącz tę opcję, aby ręcznie ustawić kąt oświetlenia.

Illumination angle (Kąt oświetlenia) : Za pomocą suwaka ręcznie ustaw kąt oświetlenia, na przykład wtedy, gdy musi on być inny niż kąt widzenia kamery. Jeżeli kamera ma szeroki kąt widzenia, kąt oświetlenia można ustawić na węższy, jak dla teleobiektywu. Spowoduje to jednak powstanie ciemnych narożników na obrazie.

IR wavelength (Długość fali IR) : Wybierz żądaną długość fali światła podczerwonego.

Światło białe

Allow illumination (Zezwalaj na oświetlenie) : Włącz tę opcję, aby w trybie nocnym kamera używała światła białego.

Synchronize illumination (Synchronizuj oświetlenie) : Włączenie tej opcji spowoduje automatyczne synchronizowanie białego światła z natężeniem światła w otoczeniu.

Ekspozycja

Wybierz tryb naświetlania, aby ograniczyć na obrazie szybkozmienne, nieregularne efekty, np. migotania wywoływanego przez różne źródła światła. Zalecamy używanie trybu ekspozycji Automatycznie lub częstotliwości identycznej ze stosowaną w lokalnej sieci elektrycznej.

Exposure mode (Tryb ekspozycji):

- **Automatic (Automatycznie)**: kamera automatycznie dostosowuje wartości apertury, wzmocnienia i migawki.
- **Automatic aperture (Apertura automatyczna)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia. Wartość migawki jest stała.
- **Automatic shutter (Migawka automatyczna)** : Kamera automatycznie dostosowuje wartości migawki i wzmocnienia. Wartość apertury jest stała.
- **Hold current (Zachowaj bieżące)**: Blokuje bieżące ustawienia ekspozycji.
- **Flicker-free (Bez migotania)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia oraz używa tylko poniższych prędkości migawki: 1/50 s (50 Hz) i 1/60 s (60 Hz).
- **Flicker-free 50 Hz (Bez migotania 50 Hz)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia; prędkość migawki wynosi 1/50 s.
- **Flicker-free 60 Hz (Bez migotania 60 Hz)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia; prędkość migawki wynosi 1/60 s.
- **Flicker-reduced (Zredukowane migotanie)** : Podobnie jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/100 s (50 Hz) i 1/120 s (60 Hz) dla jaśniejszych scen.
- **Flicker-reduced 50 Hz (Zredukowane migotanie 50 Hz)** : Działa tak samo jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/100 s dla jaśniejszych scen.
- **Flicker-reduced 60 Hz (Zredukowane migotanie 60 Hz)** : Działa tak samo jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/120 s dla jaśniejszych scen.
- **Manual (Manualnie)** : wartości apertury, wzmocnienia i migawki są stałe.

Exposure zone (Strefa ekspozycji) : Strefy ekspozycji umożliwiają optymalizowanie ekspozycji w wybranej części sceny, na przykład w obszarze przed drzwiami wejściowymi.

Uwaga

Strefy ekspozycji są związane z oryginalnym obrazem (nieobróconym), a nazwy stref mają zastosowanie do oryginalnego obrazu. Oznacza to, że jeśli na przykład strumień wideo jest obrócony o 90°, to strefa **Upper (Górne)** będzie w strumieniu strefą **Right (Prawe)**, a strefa **Left (Lewe)** strefą **Lower (Dolne)**.

- **Automatic (Automatycznie)**: Nadaje się do większości sytuacji.
- **Center (Wyśrodkuj)**: Wykorzystuje ustalony obszar na środku obrazu w celu obliczenia ekspozycji. Obszar ma stały rozmiar i położenie w podglądzie na żywo.
- **Full (Pełny)** : Wykorzystuje cały obszar podglądu na żywo w celu obliczenia ekspozycji.
- **Upper (Górny)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w górnej części obrazu w celu obliczenia ekspozycji.
- **Lower (Dolny)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w dolnej części obrazu w celu obliczenia ekspozycji.

- **Left (Lewy)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w lewej części obrazu w celu obliczenia ekspozycji.
- **Right (Prawy)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w prawej części obrazu w celu obliczenia ekspozycji.
- **Spot (Punktowe)**: Wykorzystuje obszar o stałym rozmiarze i położeniu w podglądzie na żywo w celu obliczenia ekspozycji.
- **Custom (Niestandardowe)**: Wykorzystuje obszar w podglądzie na żywo w celu obliczenia ekspozycji. Można dostosowywać rozmiar i położenie obszaru.

Max shutter (Maksymalny czas otwarcia migawki): Wybierz prędkość migawki zapewniającą najlepszy obraz. Zbyt niska prędkość migawki (dłuższa ekspozycja) może powodować rozmycie wszystkich ruchomych obiektów, a zbyt wysoka — pogarszać ogólną jakość obrazu. Najlepsze efekty działania tego ustawienia uzyskuje się w powiązaniu z maksymalnym wzmocnieniem.

Max gain (Maksymalne wzmocnienie): Wybierz odpowiednią maksymalną wartość wzmocnienia. Zwiększenie wartości maksymalnego wzmocnienia zwiększa poziom szczegółów w ciemnych obrazach, ale jednocześnie zwiększa też poziom szumów. Więcej szumu może powodować większe wykorzystanie przepustowości i pamięci. Jeżeli wartość maksymalnego wzmocnienia jest wysoka, to w przypadku znacząco różnych warunków oświetleniowych w dzień i w nocy obrazy mogą bardzo się różnić. Najlepsze efekty działania tego ustawienia uzyskuje się w powiązaniu z maksymalnym czasem migawki.

Motion-adaptive exposure (Ekspozycja przystosowana do ruchu) : Wybierz, aby zmniejszać rozmycie obiektów w ruchu w warunkach słabego oświetlenia.

Blur-noise trade-off (Stosunek rozmycia do szumu): Za pomocą suwaka wyreguluj priorytet między szumem a rozmyciem obiektów w ruchu. Jeśli preferowana jest niska przepustowość i mniej szumu na niekorzyść rejestracji szczegółów poruszających się obiektów, należy przesunąć suwak w kierunku ustawienia **Low noise (Niski poziom szumu)**. Jeśli preferowana jest rejestracja szczegółów poruszających się obiektów (na niekorzyść przepustowości i szumu), należy przesunąć suwak w kierunku ustawienia **Low motion blur (Niski poziom rozmycia obiektów w ruchu)**.

Uwaga

Poziom ekspozycji można zmienić za pomocą zmiany wartości czasu ekspozycji lub regulacji wzmocnienia. Wydłużenie czasu ekspozycji spowoduje większe rozmycie obiektów w ruchu, a większe wzmocnienie spowoduje większy szum. Przesunięcie suwaka **Blur-noise trade-off (Stosunek rozmycia do szumu)** w kierunku ustawienia **Low noise (Niski poziom szumu)** spowoduje, że funkcja automatycznej ekspozycji będzie nadawać priorytet dłuższym czasom ekspozycji, a nie wzmocnieniu, natomiast przesunięcie w kierunku ustawienia **Low motion blur (Niski poziom rozmycia obiektów w ruchu)** przyniesie odwrotny efekt. Przy słabym oświetleniu wartości wzmocnienia i czasu ekspozycji osiągną wartość minimalną niezależnie od nadanego priorytetu.

Lock aperture (Zablokuj aperturę) : Włącz tę opcję, aby pozostawić rozmiar apertury ustawiony za pomocą suwaka **Aperture (Apertura)**. Wyłączenie opcji umożliwia automatyczne dostosowanie rozmiaru apertury przez kamerę. Można np. zablokować aperturę w przypadku scen ze stałymi warunkami oświetlenia.

Aperture (Apertura) : Suwak służy do regulacji rozmiaru apertury, to znaczy ilości światła przedostającego się do obiektywu. Aby do przetwornika dostawała się większa ilość światła i w ten sposób w słabych warunkach oświetleniowych udało się uzyskać jaśniejszy obraz, przesuń suwak w kierunku wartości **Open (Otwarta)**. Otwarta apertura zmniejsza również głębię ostrości, co oznacza, że obiekty znajdujące się blisko lub daleko od kamery mogą wydawać się nieostre. Aby większe obszary obrazu były ostre, przesuń suwak w stronę wartości **Closed (Zamknięta)**.

Exposure level (Poziom ekspozycji): Użyj suwaka, aby dostosować naświetlenie obrazu.

Defog (Redukcja zamglenia) : Włącz tę opcję, aby kamera wykrywała wpływ mgły na obraz i automatycznie ją usuwała w celu uzyskania bardziej czytelnego obrazu.

Uwaga

Zalecamy, aby nie włączać opcji **Defog (Redukcji zamglenia)** w scenach o słabym kontraście, dużej zmienności poziomu oświetlenia lub złym ustawieniu ostrości. Może to wpłynąć na jakość obrazu, na przykład poprzez zwiększenie kontrastu. Zbyt duża jasność może też negatywnie wpłynąć na jakość obrazu przy włączonej redukcji zamglenia.

Optyka

Temperature compensation (Kompensacja temperatury) : Włącz, jeśli pozycja ostrości ma być korygowana na podstawie temperatury w układzie optycznym.

IR compensation (Kompensacja podczerwieni) : Włącz, jeśli pozycja ostrości ma być korygowana przy wyłączonym filtrze odcinającym promieniowanie IR, gdy występuje promieniowanie IR.

Kalibruj powiększenie i ostrość: Kliknij, przywrócić domyślne ustawienia fabryczne układu optycznego, powiększenia i ostrości. Trzeba to zrobić, jeśli podczas transportu układ optyczny się rozkalibrował albo urządzenie było narażone na bardzo silne drgania.

Strumień

Zapisy ogólne

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

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

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

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

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

Zipstream

Zipstream to technologia zmniejszania przepływności bitowej zoptymalizowana pod kątem dozoru wizyjnego; umożliwia ona zmniejszenie średniej przepływności bitowej w strumieniu H.264 lub H.265 w czasie rzeczywistym. Axis Zipstream stosuje wysoką przepływność bitową w scenach z wieloma obszarami zainteresowanie, na przykład scenach zawierających poruszające się obiekty. Kiedy scena jest bardziej statyczna, funkcja Zipstream używa niższej przepływności bitowej, zmniejszając zapotrzebowanie na zasoby pamięci. Więcej informacji znajduje się w części *Zmniejszanie zajętości pasma transmisji przy użyciu technologii Axis Zipstream*.

W ustawieniu **Strength (Stopień redukcji)** wybierz zakres redukcji przepływności bitowej:

- **Off (Wyłączona)**: Brak redukcji przepływności bitowej.
- **Niski**: Brak widocznego spadku jakości w większości scen. Jest to opcja domyślna i można jej używać we wszystkich typach scen w celu zmniejszenia przepływności.
- **Medium (Średni)**: Efekty widoczne w niektórych scenach poprzez zmniejszenie ilości zakłóceń (szumu) oraz nieco mniejszą szczegółowość w obszarach mniejszego zainteresowania, np. tam, gdzie brak ruchu.
- **Wysoka**: Efekty widoczne w niektórych scenach poprzez zmniejszenie ilości zakłóceń (szumu) oraz mniejszą szczegółowość w obszarach mniejszego zainteresowania, np. tam, gdzie brak ruchu. Zalecamy ten poziom dla urządzeń połączonych z chmurą oraz wykorzystujących lokalną pamięć masową.
- **Higher (Wyższe)**: Efekty widoczne w niektórych scenach poprzez zmniejszenie ilości zakłóceń (szumu) oraz mniejszą szczegółowość w obszarach mniejszego zainteresowania, np. tam, gdzie brak ruchu.
- **Extreme (Niezwykle wysoki)**: Efekty widoczne w większości scen. Przepływność jest zoptymalizowana pod kątem jak najmniejszego obciążania pamięci masowej.

Optimize for storage (Optymalizacja pod kątem zasobu): Włączenie tej opcji pozwala zminimalizować przepływność bez uszczerbku dla jakości. Optymalizacja nie ma zastosowania do strumienia wyświetlanego w kliencie sieciowym. Tej opcji można użyć tylko wtedy, gdy system VMS obsługuje ramki B. Włączenie **Optymalizacji pod kątem zasobu** powoduje także aktywację funkcji **Dynamic GOP (Dynamicznej grupy obrazów)**.

Dynamic FPS (Dynamiczna liczba klatek na sekundę): Włączenie tej funkcji umożliwia różnicowanie przepustowości w zależności od poziomu aktywności w scenie. Większa aktywność wymaga większej przepustowości.

Lower limit (Dolny limit): Wprowadź wartość, która ustawi poklatkowość między minimalną liczbą klatek na sekundę a domyślną liczną klatek na sekundę w strumieniu na podstawie ruchu w scenie. Zalecamy stosowanie niższego limitu w scenach z bardzo małą ilością ruchu, gdzie liczba klatek na sekundę może spadać do 1, a nawet niżej.

Dynamic GOP (Dynamiczna grupa obrazów): Włącz, aby dynamicznie dostosowywać odstęp czasu między klatkami I w oparciu o stopień aktywności w scenie.

Upper limit (Górny limit): Wprowadź maksymalną długość grupy obrazów, tzn. maksymalną liczbę ramek P między dwiema ramkami kluczowymi. Ramka kluczowa to autonomiczna ramka obrazu niezależna od innych ramek.

Sterowanie przepływnością bitową

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

Orientacja

Mirror (Odbicie lustrzane): Włącz, aby zastosować lustrzane odbicie obrazu.

Dźwięk

Include (Dołącz): Włącz, aby używać dźwięku w strumieniu wideo.

Source (Źródło)  : Wybierz źródło dźwięku, którego chcesz używać.

Stereo  : Włącz, aby używać dźwięku wewnętrznego oraz dźwięku z zewnętrznego mikrofonu.

Nakładki

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

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

- – : Wybierz pozycję nakładki w obrazie lub kliknij i przeciągnij nakładkę, aby przesunąć ją w podglądzie na żywo. Nałożenie zostanie zapamiętane we współrzędnych obrotu i pochylenia tej pozycji.
- – **Annotation between zoom levels (%) (Adnotacja pomiędzy poziomami zoomu (%))**: Pozwala ustawić poziomy zoomu, przy których nałożenie będzie widoczne.
- – **Annotation symbol (Symbol adnotacji)**: Wybierz symbol, który będzie pokazywany zamiast nałożenia, gdy wartość zoomu przekroczy ustawiony zakres.

- **Streaming indicator (Wskaźnik strumieniowania)** : Wybierz, aby wyświetlać animację nałożoną na strumień wideo. Animacja wskazuje, że strumień wideo jest przesyłany na żywo, nawet jeśli w scenie nie ma ruchu.
  - – **Appearance (Wygląd)**: Wybierz kolor tekstu i tła animacji, np. czerwoną animację na przezroczystym tle (ustawienie domyślne).
  - – **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - – : Wybierz pozycję nakładki w obrazie lub kliknij i przeciągnij nakładkę, aby przesunąć ją w podglądzie na żywo.

- **Widget: Linegraph (Wykres liniowy)** : Wyświetla wykres przedstawiający zmiany mierzonej wartości w czasie.
  - – **Title (Tytuł)**: Umożliwia wpisanie tytułu widgetu.
  - – **Overlay modifier (Modyfikator nałożenia)**: Wybierz modyfikator nałożenia jako źródło danych. Utworzone przez Ciebie nałożenia MQTT będą na końcu listy.
  - – : Wybierz pozycję nakładki w obrazie lub kliknij i przeciągnij nakładkę, aby przesunąć ją w podglądzie na żywo.
  - – **Size (Rozmiar)**: Wybierz rozmiar nałożenia.
  - – **Visible on all channels (Widoczne na wszystkich kanałach)**: Wyłącz tę opcję, aby wyświetlać tylko na aktualnie wybranym kanale. Włącz tę opcję, aby wyświetlać na wszystkich aktywnych kanałach.
  - – **Update interval (Interwał aktualizacji)**: Pozwala wybrać czas pomiędzy aktualizacjami danych.
  - – **Transparency Przezroczystość)**: Ta opcja pozwala ustawić przezroczystość całego nałożenia.
  - – **Background transparency (Przezroczystość tła)**: Ta opcja pozwala ustawić tylko przezroczystość tła nałożenia.
  - – **Points (Punkty)**: Włączenie tej opcji pozwala dodać punkt do linii wykresu podczas aktualizacji danych.
  - – **Oś X**
    - – **Label (Etykieta)**: Wprowadź etykietę tekstową osi x.
    - – **Time window (Okno czasowe)**: Ta opcja pozwala wprowadzić czas wizualizacji danych.
    - – **Time unit (Jednostka czasu)**: Wprowadź jednostkę czasu dla osi x.
  - – **Oś Y**
    - – **Label (Etykieta)**: Wprowadź etykietę tekstową osi y.
    - – **Dynamic scale (Skala dynamiczna)**: Włączenie tej opcji spowoduje automatyczne dostosowywanie skali do wartości danych. Wyłączenie tej opcji pozwoli ręcznie wprowadzać wartości dla stałej skali.

- **Min alarm threshold** and **Max alarm threshold (Minimalny i maksymalny próg alarmu)**: Wartości te dodadzą do wykresu poziome linie odniesienia, dzięki czemu łatwiej będzie zobaczyć, kiedy wartość danych staje się zbyt wysoka lub zbyt niska.

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

Obszary obserwacji

: Kliknij, aby utworzyć obszar obserwacji.

Kliknij obszar obserwacji, aby przejść do ustawień.

Nazwa: Wprowadź nazwę obszaru obserwacji. Maksymalna długość wynosi 64 znaki.

PTZ: Włącz, aby używać funkcji obrotu, pochylenia i zbliżenia w obszarze obserwacji.

Maski prywatności

: Kliknij, aby utworzyć nową maskę prywatności.

Privacy masks x/32 (Maski prywatności x/32): kliknij ten pasek nazwy, aby zmienić kolor **wszystkich** masek prywatności lub trwale usunąć **wszystkie** maski prywatności.

Cell size (Rozmiar komórki): Po wybraniu opcji kolorowej mozaiki maski prywatności będą wyświetlane w postaci pikselowanego wzoru. Za pomocą suwaka można zmienić wielkość pikseli.

Mask x (Maska x): Kliknij nazwę / numer konkretnej maski, aby zmienić jej nazwę, wyłączyć ją lub trwale usunąć.

Use zoom level (Użyj poziomu zoomu): Włącz, aby ta maska prywatności pojawiała się tylko wtedy, gdy osiągnie poziom zoomu, dla którego została utworzona. Oddalanie obrazu powoduje ponowne ukrycie maski.

Narzędzia analityczne

AXIS Object Analytics

Start (Rozpocznij): Kliknij, aby rozpocząć AXIS Object Analytics. Aplikacja będzie działać w tle i można tworzyć reguły dla zdarzeń na podstawie bieżących ustawień aplikacji.

Open (Otwórz): Kliknij, aby otworzyć AXIS Object Analytics. Aplikacja zostanie otwarta w nowej karcie przeglądarki, w której można skonfigurować jej ustawienia.

Not installed (Nie zainstalowano): AXIS Object Analytics nie jest zainstalowana na tym urządzeniu. Aby pobrać najnowszą wersję aplikacji, uaktualnij system AXIS OS do najnowszej wersji.

Dźwięk

Ustawienia urządzenia

Wejście: Włączanie lub wyłączanie wejścia audio. Pokazuje typ urządzenia wejściowego.

Allow stream extraction (Zezwalaj na wyodrębnianie strumienia) : Włącz, aby zezwolić na wyodrębnianie strumienia.

Input type (Typ wejścia) : wybierz typ źródła sygnału wejściowego, na przykład wewnętrzny mikrofon lub wejście liniowe.

Power type (Typ zasilania) : Wybierz typ zasilania źródła sygnału wejściowego.

Apply changes (Zastosuj zmiany) : powoduje zastosowanie wybranych ustawień.

Echo cancellation (Usuwanie efektu echa) : Włącz, aby usuwać echo podczas komunikacji dwukierunkowej.

Separate gain controls (Oddzielna regulacja wzmocnienia) : Włącz, aby regulować wzmocnienie osobno dla poszczególnych źródeł sygnału wejściowego.

Automatic gain control (Automatyczna regulacja wzmocnienia) : Włącz, aby dynamicznie dostosować wzmocnienie do zmian dźwięku.

Gain (Wzmocnienie): Za pomocą suwaka zmień wartość wzmocnienia. Kliknij ikonę mikrofonu, aby wyciszyć lub wyłączyć wyciszenie.

Wyjście: Pokazuje typ urządzenia wyjściowego.

Gain (Wzmocnienie): Za pomocą suwaka zmień wartość wzmocnienia. Kliknij ikonę głośnika, aby wyciszyć lub wyłączyć wyciszenie.

Automatic volume control (Automatyczna regulacja głośności) : Włącz, aby urządzenie automatycznie i dynamicznie dostosowywało wzmocnienie zgodnie z poziomem szumów otoczenia. Automatyczna regulacja głośności dotyczy wszystkich wyjść audio, w tym liniowego i cewki indukcyjnej.

Strumień

Encoding (Kodowanie): Wybierz kodowanie, które ma być stosowane do strumieniowego przesyłania ze źródła wejściowego. Kodowanie można wybrać tylko wtedy, gdy wejście audio jest włączone. Jeżeli wejście audio jest wyłączone, kliknij opcję **Enable audio input (Włącz wejście audio)**, aby je włączyć.

Klipy audio

Add clip (Dodaj klip): umożliwia dodanie nowego klipu audio. Obsługiwane formaty plików: .au,. mp3,. Opus,. Vorbis,. wav.

Rozpoczynanie odtwarzania klipu audio.

Zatrzymywanie odtwarzania klipu audio.

Menu kontekstowe zawiera opcje:

- **Rename (Zmień nazwę)**: Zmień nazwę klipu audio.
- **Create link (Utwórz łącze)**: pozwala utworzyć adres URL, którego użycie będzie powodowało odtwarzanie klipu audio w urządzeniu. Ustaw głośność i liczbę powtórzeń klipu.
- **Download (Pobierz)**: Pobieranie klipu audio do komputera.
- **Usuń**: Usuwanie klipu audio z urządzenia.

Nagrania

Kliknij, aby filtrować nagrania.

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

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

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

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

Pamięć masowa: Pokazuje nagrania z podziałem na typy zasobów.

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

Wybierz, aby rozpocząć nagrywanie w urządzeniu.

Wybierz docelowy zasób, w którym chcesz zapisać nagrania.

Zatrzymaj nagrywanie w urządzeniu.

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

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

 Odtwórz nagranie.

 Zatrzymaj odtwarzanie nagrania.

 Wyświetl lub ukryj informacje i opcje nagrania.

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

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

 Kliknij, aby usunąć nagranie.

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

Aplikacje

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

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

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

Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

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

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

Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

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

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

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

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

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

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

Uwaga

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

Lokalizacja urządzenia

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

- **Latitude (Szerokość geograficzna)**: Wartości dodatnie to szerokość geograficzna na północ od równika.
- **Longitude (Długość geograficzna)**: Wartości dodatnie to długość geograficzna na wschód od południka zerowego.
- **Kierunek**: Wprowadź kierunek (stronę świata), w który skierowane jest urządzenie. 0 to północ.
- **Etykieta**: Wprowadź opisową nazwę urządzenia.
- **Save (Zapisz)**: Kliknij, aby zapisać lokalizację urządzenia.

Sieć

IPv4

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

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

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

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

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

Uwaga

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

IPv6

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

Nazwa hosta

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

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

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

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

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

Serwery DNS

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

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

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

HTTP i HTTPS

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

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

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

Uwaga

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

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

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

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

Globalne serwery proxy

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

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

Dozwolone formaty serwerów proxy HTTP i HTTPS:

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

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

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

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

Protokoły wykrywania sieci

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

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

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

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

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

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

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

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

Allow O3C (Zezwalaj na O3C):

- **One-click (Jednym kliknięciem)**: Jest to domyślna opcja. Aby połączyć się z usługą O3C, naciśnij przycisk kontrolny na urządzeniu. W zależności od modelu urządzenia, naciśnij i zwolnij lub naciśnij i przytrzymaj, aż dioda stanu zacznie migać. Zarejestruj urządzenie w usłudze O3C w ciągu 24 godzin, aby uaktywnić opcję **Always** i pozostać połączonym. Jeśli nie zarejestrujesz urządzenia, zostanie ono odłączone od usługi O3C.
- **Zawsze**: Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenia pozostaje ono połączone. Opcji tej należy używać wtedy, gdy przycisk kontrolny jest niedostępny.
- **No (Nie)**: rozłącza usługę O3C.

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

Host: Wprowadź adres serwera proxy.

Port: wprowadź numer portu służącego do uzyskania dostępu.

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

Authentication method (Metoda uwierzytelniania):

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

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

SNMP

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

SNMP: Wybierz wersję SNMP.

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

Uwaga

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

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

Bezpieczeństwo

Certyfikaty

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

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

Obsługiwane są następujące formaty:

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

Ważne

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

Add certificate (Dodaj certyfikat) : Kliknij, aby dodać certyfikat. Zostanie otwarty przewodnik krok po kroku.

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

Menu kontekstowe zawiera opcje:

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

Secure keystore (Bezpieczny magazyn kluczy) :

- **Trusted Execution Environment (SoC TEE)**: Wybierz, aby używać środowiska SoC TEE na potrzeby bezpiecznego magazynu kluczy.
- **Bezpieczny element (CC EAL6+)**: Wybierz, aby używać bezpiecznego elementu do bezpiecznego magazynu kluczy.
- **Moduł TPM 2.0 (CC EAL4+, FIPS 140-2 poziom 2)**: Wybierz, aby używać modułu TPM 2.0 do bezpiecznego magazynu kluczy.

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certyfikaty

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

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

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

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

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

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

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

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

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

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

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

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

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

Zapobiegaj atakom typu brute force

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

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

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

Zapora

Firewall (Zapora sieciowa): włącz, aby uaktywnić zaporę sieciową.

Domyślne ustawienia zasad: wybierz sposób, w jaki zapora ma obsługiwać żądania połączeń, które nie są objęte regułami.

- **ACCEPT** (Zezwalaj): zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **DROP** (Odrzucaj): blokuje wszystkie próby połączeń z urządzeniem.

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

+ New rule (Dodaj nową regułę): Kliknij, aby utworzyć regułę.

Rule type (Rodzaj reguły):

- **FILTER** (Filtr): zaznacz, aby zezwolić na lub zablokować połączenia z urządzeń spełniających kryteria określone w regule.
  - **Policy (Zasada)**: wybierz opcję **Accept** (Zezwalaj) lub **Drop** (Odrzucaj) dotyczącą reguły zapory sieciowej.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC** (Adres MAC): wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
    - **UNICAST**: ruch od jednego nadawcy do jednego odbiorcy.
    - **BROADCAST**: ruch od jednego nadawcy do wszystkich urządzeń w sieci.
    - **MULTICAST**: ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.
- **LIMIT** (Ograniczenie): wybierz, aby przyjmować połączenia z urządzeń spełniających kryteria określone w regule, ale stosować ograniczenia w celu zmniejszenia nadmiernego ruchu.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC** (Adres MAC): wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Unit** (Rodzaj połączenia): wybierz rodzaj połączeń, które mają być dozwolone lub blokowane.
  - **Period** (Okres): wybierz okres związany z pozycją **Amount**.
  - **Amount** (Liczba): ustaw maksymalną liczbę połączeń, jaką urządzenie może ustanowić w ustawionym okresie **Period**. Maksymalna wartość to 65535.

- **Burst**: wpisz liczbę połączeń, dla których dozwolone jest jednokrotne przekroczenie ustawionej liczby **Amount** w ustawionym okresie **Period**. Po osiągnięciu tej liczby dozwolona jest tylko ustalona liczba w ustalonym okresie.
- **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
  - **UNICAST**: ruch od jednego nadawcy do jednego odbiorcy.
  - **BROADCAST**: ruch od jednego nadawcy do wszystkich urządzeń w sieci.
  - **MULTICAST**: ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.

Test rules (Reguły testu): kliknij tę opcję, aby przetestować zdefiniowane reguły.

- **Test time in seconds** (Czas testu w sekundach): Pozwala ustawić limit czasu testowania reguł.
- **Roll back (Przywróć poprzednią wersję)**: kliknij, aby przywrócić zaporę sieciową do stanu sprzed przetestowania reguł.
- **Apply rules** (Zastosuj reguły): kliknij, aby uaktywnić reguły bez testowania. Nie zaleca się wykonywania tej czynności.

Niestandardowy podpisany certyfikat systemu AXIS OS

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

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

⋮ Menu kontekstowe zawiera opcje:

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

Konta

Konta

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Privileges (Przywileje):

- **Administrator**: Ma nieograniczony dostęp do wszystkich ustawień. Administrator może tez dodawać, aktualizować i usuwać inne konta.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
- **Viewer (Dozorca)**: Może:
  - Oglądać strumienie wideo i robić z nich migawki.
  - Oglądać i eksportować nagrania.
  - Korzystać z funkcji obracania, pochylania i zoomowania, jeśli ma dostęp do **konta PTZ**.

Menu kontekstowe zawiera opcje:

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

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

Anonimowy dostęp

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

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

Konta SSH

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

- **Enable SSH (Włącz SSH)**: Włącz, aby korzystać z usługi SSH.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Uwaga: Wprowadź komentarz (opcjonalnie).

Menu kontekstowe zawiera opcje:

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

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

Virtual host (Host wirtualny)

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

Włączony: zaznaczenie tej opcji spowoduje używanie tego wirtualnego hosta.

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

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

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

Menu kontekstowe zawiera opcje:

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

Disabled (Wyłączono): Serwer jest wyłączony.

Konfiguracja OpenID

Ważne

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

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

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

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

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

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

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

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

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

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

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

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

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

Zdarzenia

Reguły

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

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.

Nazwa: Wprowadź nazwę reguły.

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

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

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

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

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

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

Odbiorcy

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

Uwaga

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

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

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

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

Nazwa: Wprowadź nazwę odbiorcy.

Type (Typ): Wybierz z listy:

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

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

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

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

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

Uwaga

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

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

Test (Testuj): Kliknij, aby przetestować konfigurację.

⋮ Menu kontekstowe zawiera opcje:

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

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

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

Harmonogramy

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

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

Wyzwalacze ręczne

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

MQTT

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

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

Więcej informacji o protokole MQTT znajdziesz w *bazie wiedzy na temat systemu AXIS OS*.

ALPN

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

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.

Status (Stan): pokazuje bieżący status klienta MQTT.

Broker

Host: wprowadź nazwę hosta lub adres IP serwera MQTT.

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

Port: Wprowadź numer portu.

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

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

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

Hasło: wprowadzić hasło dla nazwy użytkownika.

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

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

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

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

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

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

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

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

Komunikat łączenia

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

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

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

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

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

QoS: zmiana warstwy QoS dla przepływu pakietów.

Wiadomość Ostatnia Wola i Testament

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

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

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

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

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

QoS: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

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

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

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

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

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

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

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

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

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

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

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

Subscription type (Typ subskrypcji):

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

QoS: Wybierz żądany poziom subskrypcji MQTT.

Nałożenia MQTT

Uwaga

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

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

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

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

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

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

Przechowywanie

Sieciowa pamięć masowa

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

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

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

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

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

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

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

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

Narzędzia

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

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

Pamięć pokładowa

Ważne

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

Odmontuj: Kliknij w celu bezpiecznego usunięcia karty SD.

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

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

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

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

Narzędzia

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

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

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

Pamięć pokładowa

Dysk twardy

- **Free (Wolne)**: Ilość wolnego miejsca na dysku.
- **Status (Stan)**: Czy dysk jest zainstalowany.
- **System plików**: System plików używany przez dysk.
- **Zaszyfrowane**: Czy dysk jest zaszyfrowany.
- **Temperatura**: Bieżąca temperatura sprzętu.
- **Overall heath test (Ogólny test stanu)**: Wynik kontroli kondycji dysku.

Narzędzia

- **Check (Sprawdź)**: Sprawdza, czy urządzenie pamięci masowej jest wolne od błędów, i spróbuje je naprawić automatycznie.
- **Napraw**: Naprawia urządzenie pamięci masowej. Podczas naprawy zostaną wstrzymane aktywne nagrania. Naprawa urządzenia pamięci masowej może spowodować utratę danych.
- **Format (Formatuj)**: Usuń wszystkie zapisy i sformatuj urządzenie pamięci masowej. Wybierz system plików.
- **Encrypt (Szyfruj)**: Aktywuje szyfrowanie przechowywanych danych.
- **Decrypt (Odszyfruj)**: Aktywuje deszyfrowanie przechowywanych danych. System wykasuje wszystkie pliki w urządzeniu zasobu.
- **Change password (Zmień hasło)**: Zmień hasło szyfrowania dysków. Zmiana hasła nie zakłóca nagrywania.
- **Use tool (Użyj narzędzia)**: Kliknij, aby uruchomić wybrane narzędzie

Unmount (Odmontuj) : Kliknij przed odłączeniem urządzenia od systemu. Spowoduje to zatrzymanie wszystkich nagrań w toku.

Write protect (Zabezpieczenie przed zapisem): Pozwala włączyć zabezpieczenie urządzenia zasobu przed nadpisaniem.

Autoformat (Formatowanie automatyczne) : Dysk zostanie automatycznie sformatowany przy użyciu systemu plików ext4.

SIP

Ustawienia

Protokół SIP (Session Initiation Protocol) służy do prowadzenia sesji komunikacji interaktywnej pomiędzy użytkownikami. Sesje mogą zawierać audio i wideo.

SIP setup assistant (Asystent konfiguracji SIP): kliknięcie tej opcji pozwala skonfigurować SIP krok po kroku.

Enable SIP (Włącz SIP): Zaznacz tę opcję, aby umożliwić inicjowanie i odbieranie połączeń SIP.

Allow incoming calls (Zezwalaj na połączenia przychodzące): Zaznacz tę opcję, aby zezwalać na połączenia przychodzące z innych urządzeń SIP.

Obsługa połączeń

- **Calling timeout (Limit czasu wywołania)**: ta opcja pozwala ustawić maksymalny czas prób nawiązania połączenia, gdy nikt nie odbiera.
- **Incoming call duration (Czas trwania rozmowy przychodzącej)**: ustaw maksymalny czas trwania połączenia przychodzącego (maks. 10 min).
- **End calls after (Zakończ połączenie po)**: ustaw maksymalny czas trwania połączenia (maks. 60 min). Zaznacz opcję **Infinite call duration (Nieskończony czas trwania połączenia)**, jeśli nie chcesz ograniczać długości połączenia.

Porty

Numer portu musi należeć do przedziału od 1024 do 65535.

- **SIP port (Port SIP)**: Port sieciowy wykorzystywany zazwyczaj do komunikacji SIP. Ruch sygnalizacyjny przez ten port nie jest szyfrowany. Domyślny numer portu to 5060. W razie potrzeby wprowadź inny numer portu.
- **Port TLS**: Port sieciowy wykorzystywany do szyfrowanej komunikacji SIP. Ruch sygnalizacyjny za pośrednictwem tego portu jest szyfrowany przy użyciu Transport Layer Security (TLS). Domyślny numer portu to 5061. W razie potrzeby wprowadź inny numer portu.
- **Port początkowy RTP**: Port sieciowy wykorzystywany do pierwszego przesłania strumienia mediów RTP w połączeniu SIP. Domyślny początkowy numer portu to 4000. Niektóre zapory mogą blokować ruch RTP na portach o określonych numerach.

NAT Transversal

Użyj NAT (Network Address Translation), gdy urządzenie znajduje się w prywatnej sieci (LAN) i chcesz je udostępnić spoza tej sieci.

Uwaga

Router musi obsługiwać NAT Traversal, aby można było włączyć te opcję. Router musi również obsługiwać protokół UPnP®.

Każdy protokół NAT traversal może być używany oddzielnie lub w różnych kombinacjach w zależności od środowiska sieciowego.

- **ICE**: Protokół ICE (Interactive Connectivity Establishment) zwiększa szanse na wyszukanie najlepszej ścieżki komunikacji między urządzeniami typu peer. Szanse na wykorzystanie protokołu ICE można zwiększyć po włączeniu STUN i TURN.
- **STUN** : STUN (Session Traversal Utilities for NAT) to protokół sieciowy klient-serwer umożliwiający urządzeniom określenie, czy znajduje się on za NAT lub zaporą, a następnie uzyskanie zmapowanego publicznego adresu IP i numeru portu przypisanego do połączeń ze zdalnymi hostami. Wprowadź adres serwera STUN, na przykład adres IP.
- **TURN**: TURN (Traversal Using Relays around NAT) to protokół umożliwiający urządzeniem za routerem NAT lub zaporą otrzymywanie danych z innych hostów (poprzez TCP lub UDP). Wprowadź adres serwera TURN i dane logowania.

Dźwięk i obraz wideo

- **Audio codec priority (Priorytet kodeka audio)**: Wybierz co najmniej jeden kodek audio z żądaną jakością dźwięku na potrzeby połączeń SIP. W celu zmiany kolejności priorytetów przeciągnij i upuść w inne miejsca.

Uwaga

Wybrane kodeki muszą być takie same, jak kodeki odbiorcy, ponieważ to one decydują o jakości połączenia.

- **Audio direction (Kierunek dźwięku)**: Wybierz dozwolone kierunki dźwięku.
- **H.264 packetization mode (Tryb pakietyzacji H.264)**: Wybierz tryb pakietyzacji, który ma być używany.

  - **Automatycznie**: (Zalecany) Urządzenie decyduje o wyborze trybu pakietyzacji.
  - **Brak**: Nie jest określony żaden konkretny tryb pakietyzacji. To ustawienie często jest interpretowane jako tryb **0**.
  - **0**: Tryb bez przeplotu.
  - **1**: Tryb pojedynczej jednostki NAL.
- **Kierunek obrazu wideo**: Wybierz dozwolone kierunki obrazu filmowego.

Dodatkowe

- **UDP-to-TCP switching (Przełączanie UDP–TCP)**: Wybierz, aby umożliwić tymczasowe przełączenie protokołu transmisji z UDP (User Datagram Protocol) na TCP (Transmission Control Protocol). Przełączanie przydaje się w celu uniknięcia fragmentacji; przełączenie jest możliwe w zakresie 200 bajtów MTU lub więcej niż 1300 bajtów MTU.
- **Allow via rewrite (Umożliwiaj przepisanie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Allow contact rewrite (Umożliwiaj przepisanie przy kontakcie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Register with server every (Rejestruj na serwerze co)**: Ustaw częstotliwość rejestrowania się urządzenia na serwerze SIP dla istniejących kont SIP.
- **DTMF payload type (Typ próbki DTMF)**: Zmienia domyślny typ próbki na DTMF.
- **Maksymalna liczba retransmisji**: Ustaw maksymalną liczbę prób nawiązywania przez urządzenie połączenia z serwerem SIP, zanim urządzenie zrezygnuje.
- **Sekundy do odblokowania awaryjnego**: Ustaw liczbę sekund, po której urządzenie spróbuje ponownie się połączyć z głównym serwerem SIP po awaryjnym przełączeniu na dodatkowy serwer SIP.

Konta

Wszystkie bieżące konta SIP znajdują się na karcie **SIP accounts (Konta SIP)**. Zarejestrowane konta oznaczone są kolorowymi okręgami statusu.

● Konto zostało zarejestrowane na serwerze SIP.

● Wystąpił problem z kontem. Możliwe przyczyny: błąd autoryzacji, nieprawidłowe dane uwierzytelniające konta lub brak konta SIP wyszukiwanego przez serwer.

Konto **peer to peer (domyślne)** jest kontem tworzonym automatycznie. Można je usunąć po utworzeniu co najmniej jednego innego konta i ustawieniu go jako domyślne. Konto domyślne zawsze będzie wykorzystywane do nawiązania połączenia VAPIX ® Application Programming Interface (API) w przypadku, gdy nie zostanie określone, z którego konta SIP ma być wykonane połączenie.

+ **Add account (Dodaj konto)**: Kliknij, aby utworzyć nowe konto SIP.

- **Active (Aktywne)**: wybierz tę opcję, aby użyć tego konta.
- **Ustaw jako domyślne**: zaznacz tę opcję, aby ustawić konto jako domyślne. Konto domyślne jest wymagane; można ustawić tylko jedno konto jako domyślne.
- **Answer automatically (Odbierz automatycznie)**: wybierz tę opcję, aby automatycznie odbierać połączenia.
- **Prioritize IPv6 over IPv4 (Pierwszeństwo IPv6 względem IPv4)** : po wybraniu tej opcji adresy IPv6 są traktowane nadrzędnie względem IPv4. Ta funkcja przydaje się podczas łączenia z kontami P2P lub nazwami domen rozpoznawanymi zarówno w adresach IPv4, jak i IPv6. Priorytet IPv6 można nadać tylko tym nazwom domen, które są mapowane na adresy IPv6.
- **Nazwa**: Wprowadź nazwę opisową. Może to być na przykład imię i nazwisko, rola lub lokalizacja. Nazwa nie musi być unikalna.
- **User ID (ID użytkownika)**: Wprowadź numer wewnętrzny lub numer telefonu przypisany do urządzenia.
- **Peer-to-peer**: służy do wykonywania bezpośrednich połączeń z innym urządzeniem SIP w sieci lokalnej.
- **Zarejestrowane**: służy do wykonywania połączeń z urządzeniami SIP spoza sieci lokalnej (przez serwer SIP).
- **Domain (Domena)**: jeśli to możliwe, wprowadź nazwę publicznej domeny. Będzie ona wyświetlana jako część adresu SIP podczas wywoływania innych kont.
- **Hasło**: wprowadź hasło powiązane z kontem SIP, aby uwierzytelnić się na serwerze SIP.
- **Authentication ID (ID uwierzytelniania)**: wprowadź identyfikator uwierzytelnienia używany do uwierzytelniania na serwerze SIP. Jeśli jest on taki sam, jak identyfikator użytkownika, nie trzeba go wprowadzać.
- **Caller ID (ID rozmówcy)**: nazwa wyświetlana odbiorcom połączeń przychodzących z urządzenia.
- **Rejestrator**: wprowadź adres IP rejestratora.
- **Tryb transmisji**: Wybierz tryb transmisji SIP dla konta: UPD, TCP lub TLS.
- **TLS version (Wersja TLS)** (tylko w trybie transportu TLS): wybierz wersję TLS. Wersje **v1.2** and **v1.3** są najbezpieczniejsze. **Automatic (Automatycznie)** wybiera najbezpieczniejszą wersję obsługiwaną przez system.
- **Media encryption (Szyfrowanie mediów)** (tylko w trybie TLS): wybierz rodzaj szyfrowania mediów (audio i wideo) w połączeniach SIP.
- **Certificate (Certyfikat)** (tylko w trybie TLS): Wybierz certyfikat.
- **Verify server certificate (Potwierdź certyfikat serwera)** (tylko w trybie TLS): zaznacz, aby potwierdzać certyfikat serwera.

- **Secondary SIP server (Dodatkowy serwer SIP)**: Włącz, aby w razie niepowodzenia rejestracji na głównym serwerze SIP urządzenie podjęło próbę rejestracji na serwerze dodatkowym.
- **SIP secure (Bezpieczny SIP)**: wybierz tę opcję, aby użyć protokołu Secure Session Initiation Protocol (SIPS). Protokół SIPD wykorzystuje tryb transmisji TLS do szyfrowania ruchu.
- **Serwery proxy**
  - **Proxy**: Kliknij, aby dodać serwer proxy.
  - **Prioritize (Nadaj priorytet)**: Po dodaniu dwóch lub więcej serwerów proxy kliknij, aby określić ich priorytet.
  - **Server address (Adres serwera)**: Tu należy wprowadzić adres IP serwera proxy SIP.
  - **Username (Nazwa użytkownika)**: wprowadź nazwę użytkownika serwera proxy SIP, jeśli to konieczne.
  - **Hasło**: wprowadź hasło do serwera proxy SIP, jeśli to konieczne.
- **Nagranie wideo**
  - **View area (Obszar obserwacji)**: wybierz obszar obserwacji połączeń wideo. Jeśli nie zostanie wybrany obszar obserwacji, zostanie użyty widok natywny.
  - **Rozdzielczość**: wybierz rozdzielczość połączeń wideo. Rozdzielczość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **Frame rate (Liczba klatek na sekundę)**: wybierz liczbę klatek na sekundę w połączeniach wideo. Poklatkowość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **H.264 profile (Profil H.264)**: Wybierz profil połączeń wideo.

DTMF

Add sequence (Dodaj sekwencję): Kliknięcie tej opcji pozwala utworzyć nową sekwencję DTMF. Aby utworzyć regułę wyzwalaną przez sygnał wybierania, otwórz menu **Events > Rules (Zdarzenia > Reguły)**.

Sequence (Sekwencja): Wprowadź znaki aktywujące tę regułę. Dozwolone znaki: 0–9, A–D, # oraz *.

Description (Opis): Wprowadź opis akcji, która będzie wyzwalana przez sekwencję.

Accounts (Konta): Wybierz konta, które mają używać sekwencji DTMF. W przypadku wybrania konfiguracji **peer-to-peer** wszystkie konta peer-to-peer będą współdzieliły jedną sekwencję DTMF.

Protokoły

Wybierz protokoły, które mają być używane dla każdego konta. Wszystkie konta peer-to-peer mają takie same ustawienia protokołu.

Use RTP (RFC2833) (Użyj RTP (RFC2833)): Włącz tę opcję, aby zezwalać na sygnały DTMF, inne sygnały i zdarzenia telefoniczne w pakietach RTP.

Użyj SIP INFO (RFC2976): Włącz tę opcję, aby dołączyć metodę INFO do protokołu SIP. Metoda INFO służy do dodania opcjonalnych informacji o warstwie, zazwyczaj powiązanych z sesją.

Połączenie testowe

SIP account (Konto SIP): Wybierz konto, z którego ma zostać wykonane połączenie testowe.

Adres SIP: Wprowadź adres SIP i kliknij , aby wykonać połączenie testowe i zweryfikować działanie konta.

Lista dostępu

Use access list (Użyj listy dostępu): Włącz tę opcję, aby ograniczyć listę użytkowników mogących nawiązywać połączenia z urządzeniem.

Policy (Zasada):

- **Allow (Zezwalaj)**: Zaznaczenie tej opcji zezwoli na połączenia przychodzące tylko ze źródeł z listy dostępu.
- **Block (Blokuj)**: Zaznaczenie tej opcji zablokuje połączenia przychodzące ze źródeł z listy dostępu.

Add source (Dodaj źródło): Kliknij, aby utworzyć nowy wpis na liście dostępu.

SIP source (Źródło SIP): Wpisz identyfikator rozmówcy lub adres serwera SIP źródła.

Profile strumienia

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

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

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

Nazwa: Nadaj profilowi nazwę.

Description (Opis): Dodaj opis profilu.

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

Rozdzielczość: Opis tego ustawienia znajduje się w temacie .

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

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

Zipstream : Opis tego ustawienia znajduje się w temacie .

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

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

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

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

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

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

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

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

ONVIF

Konta ONVIF

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

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

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Rola:

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

Menu kontekstowe zawiera opcje:

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

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

Profile mediów ONVIF

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

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

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

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

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

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

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

Uwaga

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

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

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

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

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

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

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

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

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

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

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

PTZ : Wybierz ustawienia PTZ dla swojej konfiguracji.

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

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

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

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

Metadane analityczne

RTSP metadata producers (Producenci metadanych RTSP)

Wyświetlaj i zarządzaj kanałami danych, które przesyłają strumień metadanych, oraz kanałami, z których korzystają.

Uwaga

Te ustawienia dotyczą strumieni metadanych RTSP korzystających z formatu ONVIF XML. Wprowadzone tutaj zmiany nie mają wpływu na stronę wizualizacji metadanych.

Producer (Producent): Kanał danych wykorzystujący protokół RTSP (Real-Time Streaming Protocol) do przesyłania metadanych.

Kanał: Kanał używany do wysyłania metadanych od producenta. Aktywuj tę opcję, aby włączyć strumień metadanych. Wyłącz tę opcję, aby zapewnić zgodność lub zarządzać zasobami.

Detektory

Sabotaż kamery

Gdy scena ulegnie zmianie, na przykład z powodu zasłonięcia obiektywu, spryskania go farbą lub znaczącego rozregulowania ostrości, to po upływie czasu określonego w ustawieniu **Trigger delay (Opóźnienie wyzwalacza)** detektor sabotażu kamery wygeneruje alarm. Detektor sabotażu aktywuje się tylko w razie braku ruchu kamery przez 10 sekund. W tym czasie detektor ustawia model sceny, którego używa do porównania w celu wykrycia sabotażu w rejestrowanych obrazach. Aby model sceny został prawidłowo skonfigurowany, obraz musi być ostry, warunki oświetlenia prawidłowe, a kamera nie może być skierowana w miejsce bez konturów, takie jak gładka ściana. Funkcji wykrywania sabotażu kamery można użyć jako warunku wyzwalania akcji.

Trigger delay (Opóźnienie wyzwalacza): Wprowadź minimalny czas, przez jaki muszą być aktywne warunki sabotażu, zanim nastąpi wyzwolenie alarmu. Pozwoli to zapobiec fałszywym alarmom wywoływanym przez znane warunki wpływające na obraz.

Trigger on dark images (Wyzwól przy ciemnym obrazie): Po spryskaniu obiektywu farbą trudno jest wywołać alarm, ponieważ nie można odróżnić tej sytuacji od innych, podczas których występuje ten sam efekt zaciemnienia obrazu, na przykład kiedy warunki oświetlenia ulegają zmianie. Po włączeniu tego parametru alarmy będą generowane we wszystkich przypadkach, w których obraz ulegnie zaciemnieniu. Gdy funkcja jest wyłączona, urządzenie nie będzie generować alarmów w razie zaciemnienia obrazu.

Uwaga

Do wykrywania prób sabotażu w scenach statycznych i zawierających niewiele obiektów.

Detekcja dźwięku

Ustawienia te są dostępne dla każdego wejścia audio.

Sound level (Poziom dźwięku): Wyreguluj poziom dźwięku w zakresie od 0 do 100, gdzie 0 oznacza największą czułość, a 100 — najmniejszą. Podczas ustawiania poziomu dźwięku można skorzystać ze wskaźnika aktywności. Podczas tworzenia zdarzeń można używać poziomu dźwięku jako warunku. Użytkownik określa, czy działanie będzie inicjowane wtedy, gdy poziom dźwięku wzrośnie powyżej, spadnie poniżej lub przekroczy ustawioną wartość.

Wykrywanie wstrząsów

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

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

Wyjście wideo

Ustawienia zasilania

Ustawienia zasilania

Delayed shutdown (Opóźnione wyłączenie) : Włącz tę opcję, jeśli chcesz ustawić czas opóźnienia wyłączenia zasilania.

Delay time (Czas opóźnienia) : Ustaw czas opóźnienia od 1 do 60 minut.

Power saving mode (Tryb oszczędzania energii) : Włącz tę opcję, aby aktywować tryb oszczędzania energii w urządzeniu. Po włączeniu trybu oszczędzania energii zakres oświetlenia w podczerwieni jest zmniejszony.

Set power configuration (Ustaw konfigurację zasilania) : Aby zmienić konfigurację zasilania, wybierz inną opcję klasy PoE. Aby zapisać zmiany, kliknij przycisk **Save and restart (Zapisz i uruchom ponownie)**.

Uwaga

W przypadku skonfigurowania zasilania jako PoE klasy 3 zalecamy wybranie opcji **Low power profile (Profil niskiego poboru mocy)**, jeżeli jest ona dostępna w urządzeniu.

Dynamic power mode (Tryb zasilania dynamicznego) : Włącz, aby zmniejszyć zużycie energii, gdy urządzenie jest nieaktywne.

Power warning overlay (Wyświetlanie ostrzeżenia dotyczącego zasilania): Włącz, aby wyświetlić nałożone na obraz ostrzeżenie dotyczące zasilania w przypadku, gdy urządzenie nie otrzymuje wystarczającej mocy.

I/O port power (zasilanie z portu we/wy) : Włącz, aby dostarczać zasilanie 12 V do urządzeń zewnętrznych podłączonych do portów we/wy. Wyłącz, aby nadać priorytet funkcjom wewnętrznym, takim jak podczerwień, ogrzewanie i chłodzenie. W wyniku tego urządzenia i czujniki wymagające zasilania 12 V przestaną działać prawidłowo.

Akcesoria

Porty we/wy

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

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

Port

Nazwa: edytuj tekst, aby zmienić nazwę portu.

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

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

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

Uwaga

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

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

Dzienniki

Raporty i dzienniki

Raporty

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

Dzienniki

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

Ślad sieciowy

Ważne

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

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

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

Zdalny dziennik systemu

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

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

Host: Wprowadź nazwę hosta lub adres IP serwera.

Format (Formatuj): Wybierz format komunikatów Syslog, który ma być używany.

- Axis
- RFC 3164
- RFC 5424

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

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

Port: Wpisywanie innego numeru portu w miejsce obecnego.

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

Type (Typ): wybierz rodzaj dzienników do wysłania.

Test server setup (Testuj ustawienia serwera): wyślij wiadomość testową do wszystkich serwerów przed zapisaniem ustawień.

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

Zwykła konfiguracja

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

Konserwacja

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

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

Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

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

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

Uwaga

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

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

Po uaktualnieniu masz do wyboru trzy opcje:

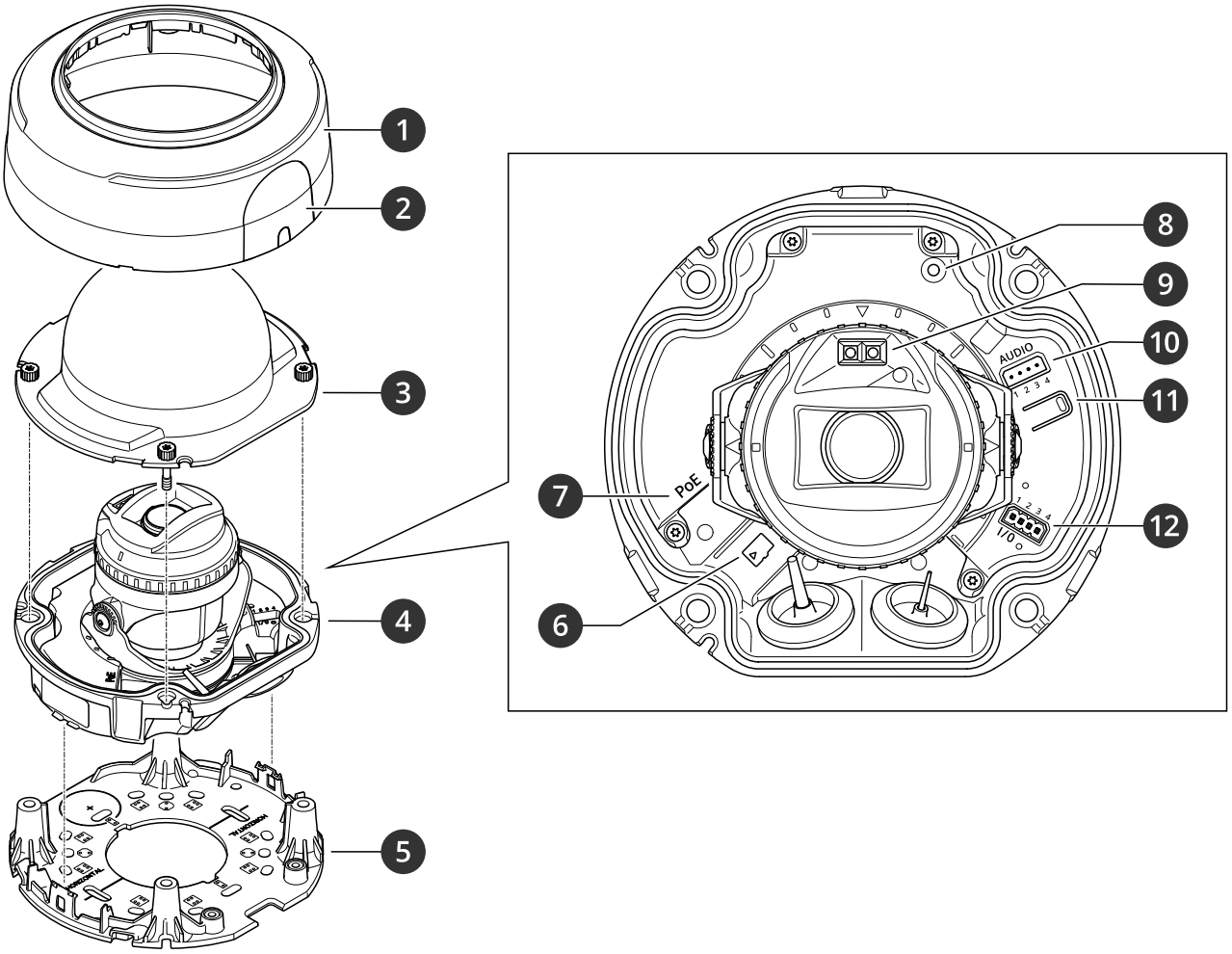
- **Standard upgrade (Aktualizacja standardowa)**: Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **Ustawienia fabryczne**: Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej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

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

Specyfikacje

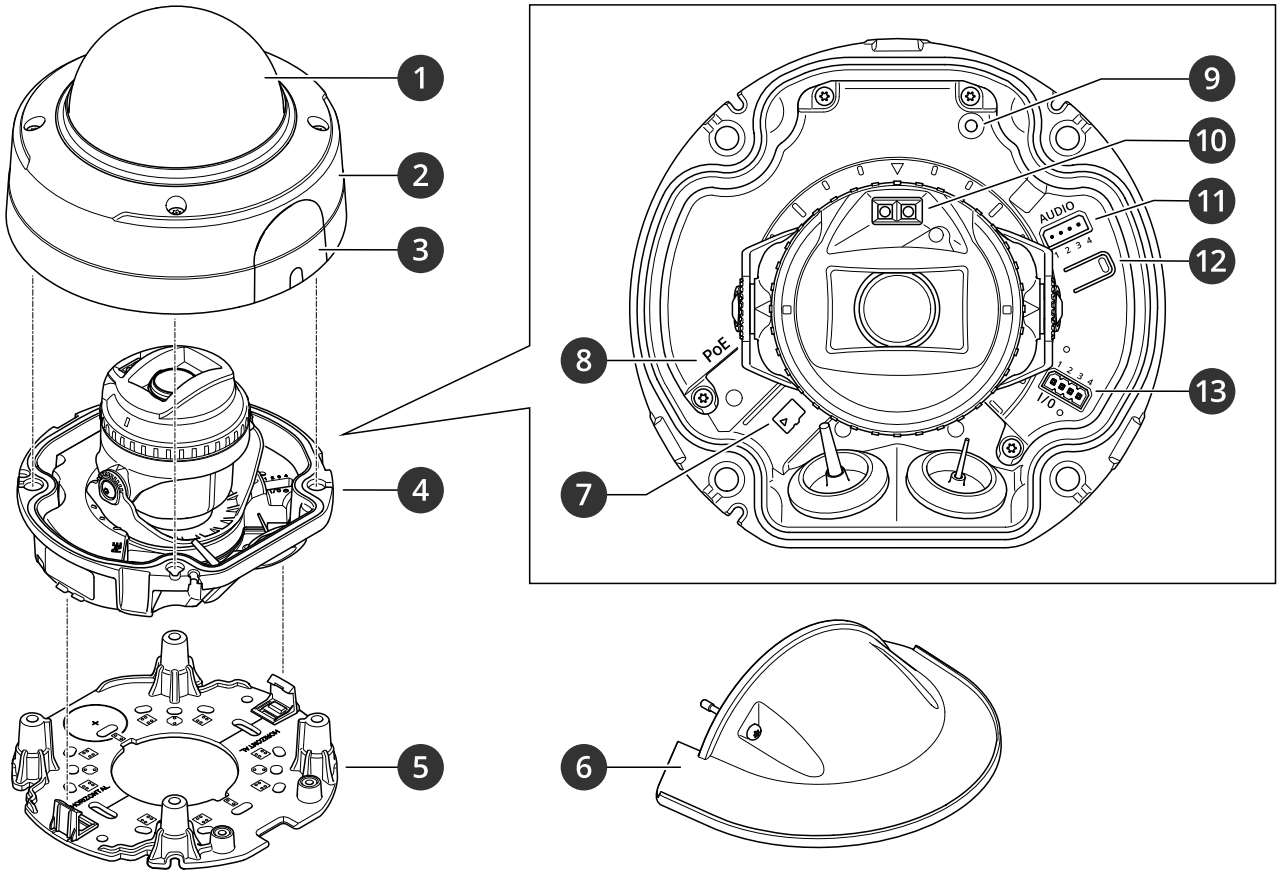
Przegląd produktów

AXIS P3245-LV



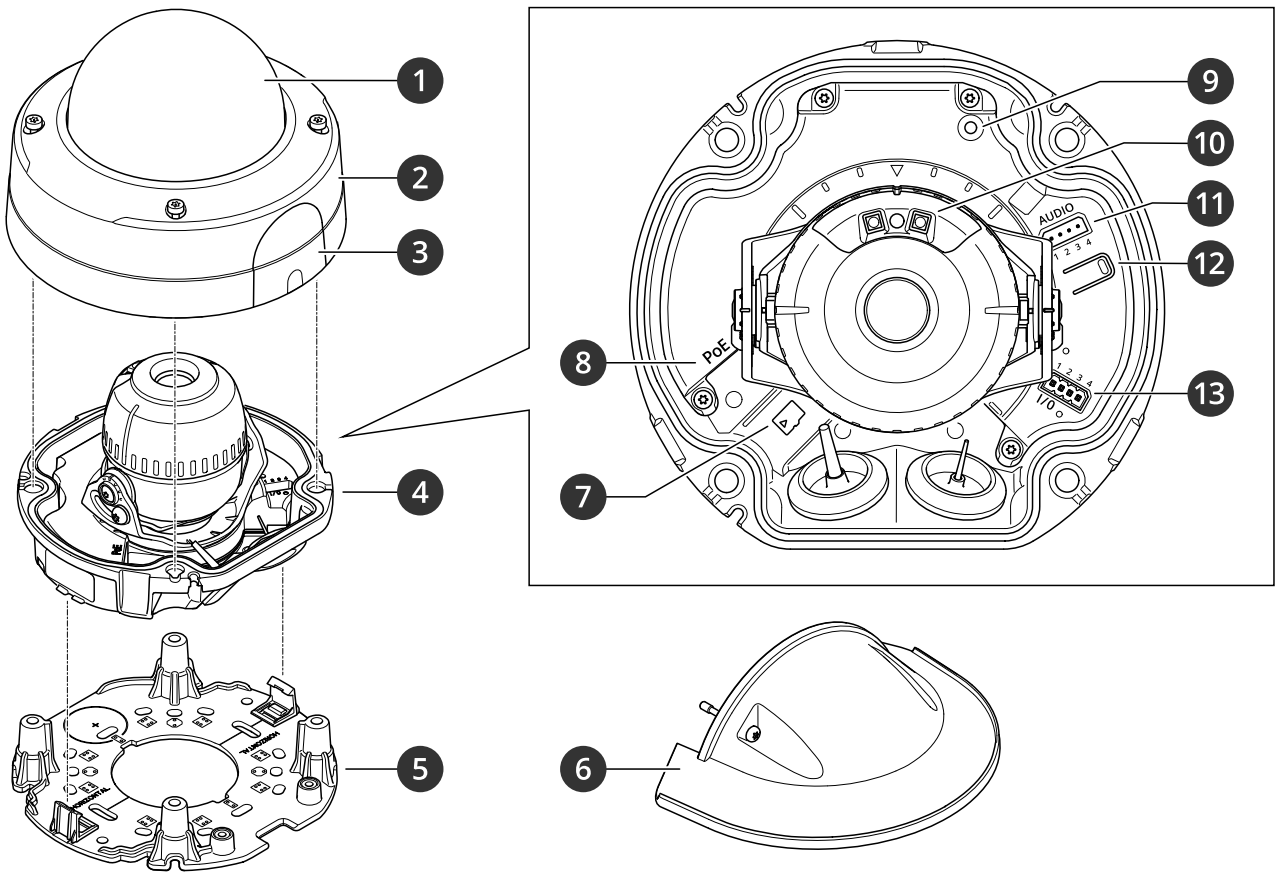
1 *Osłona kopułki*
2 *Pokrywa*
3 *Kopułka*
4 *Kamera*
5 *Uchwyt montażowy*
6 *Gniazdo karty pamięci SD*
7 *Złącze sieciowe (PoE)*
8 *Wskaźnik LED stanu*
9 *IR LED*
10 *Złącze audio*
11 *Przycisk kontrolny*
12 *Złącze I/O*

AXIS P3245-LVE 9 mm



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

AXIS P3245-LVE 22 mm



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 wyjmuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wyjmuj karty SD w trakcie działania produktu.

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

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

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

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz .

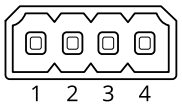
Złącza

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

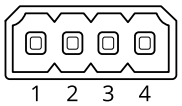
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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 zbicia szyby.

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

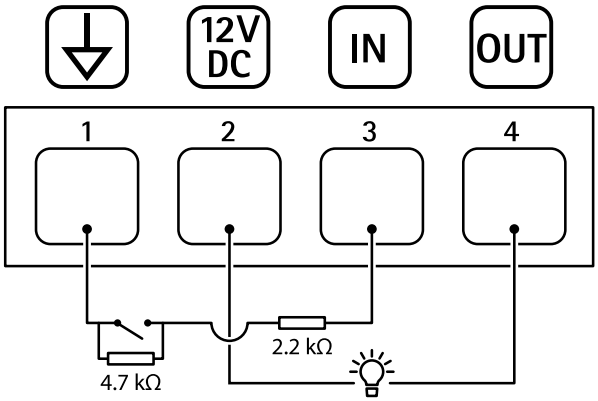
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

4-pinowy blok złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	⚠ Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 25 mA
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 –

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 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.

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.

Problemy techniczne, wskazówki i rozwiązania

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

Problemy z uaktualnianiem systemu AXIS OS

Niepowodzenie uaktualniania systemu AXIS OS	Jeśli aktualizacja zakończy się niepowodzeniem, urządzenie załaduje ponownie poprzednią wersję. Najczęstszą przyczyną tego jest wczytanie niewłaściwego systemu AXIS OS. Upewnij się, że nazwa pliku systemu AXIS OS odpowiada danemu urządzeniu i spróbuj ponownie.
Problemy po aktualizacji systemu AXIS OS	Jeśli wystąpią problemy po aktualizacji, przejdź do strony **Konserwacja** i przywróć poprzednio zainstalowaną wersję.

Problemy z ustawieniem adresu IP

Urządzenie należy do innej podsieci	Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsieci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.

Adres IP jest używany przez inne urządzenie	Odłącz urządzenie Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia): • Jeśli otrzymasz: `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. • 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.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Nie można uzyskać dostępu do urządzenia przez przeglądarkę

Nie można zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki. W razie utraty hasła dla konta root należy przywrócić ustawienia fabryczne urządzenia. Patrz .
Serwer DHCP zmienił adres IP	Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę). W razie potrzeby można przydzielić samodzielnie statyczny adres IP. Instrukcje można znaleźć na stronie *axis.com/support*.
Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X	Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w urządzeniu Axis muszą być zsynchronizowane z serwerem NTP. Wybierz kolejno opcje **System > Date and time (System > Data i godzina)**.

Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

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

- AXIS Camera Station Edge: darmowa aplikacja idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station 5: 30-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.
- AXIS Camera Station Pro: 90-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

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

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

multicast w kodowaniu H.264	Poproś administratora sieci, aby sprawdził, czy zapora 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 . • 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.

Nie można połączyć przez port 8883 z MQTT przez SSL

Zapora blokuje ruch przy użyciu portu 8883, ponieważ jest on uważany za niebezpieczny.	Czasami serwer/broker może nie zapewniać konkretnego portu dla komunikacji MQTT. W takiej sytuacji może być dostępne korzystanie z MQTT przez port zwykle używany do obsługi ruchu HTTP/HTTPS. • Jeśli serwer/broker obsługuje protokół WebSocket/WebSocket Secure (WS/WSS), typowo w porcie 443, użyj tego protokołu. Skontaktuj się z dostawcą serwera/brokera, aby dowiedzieć się, czy protokół WS/WSS jest obsługiwany oraz którego portu i ścieżki podstawowej należy używać. • Jeśli serwer/broker obsługuje ALPN, korzystanie z MQTT może być negocjowane na otwartym porcie, na przykład porcie 443. Skontaktuj się z dostawcą serwera/brokera, aby sprawdzić, czy jest obsługiwany ALPN oraz jakiego protokołu ALPN i portu należy użyć.

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.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.

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

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

Aktualizacja systemu AXIS OS:

Ważne

- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania urządzenia (pod warunkiem, że funkcje te są dostępne w nowym systemie AXIS OS), choć Axis Communications AB tego nie gwarantuje.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

Uwaga

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

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

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

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

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wydajność. Niektóre czynniki wpływają na wymaganą przepustowość, a inne mogą wpływać na liczbę klatek na sekundę; niektóre z nich wpływają na oba te parametry. Jeśli obciążenie procesora osiągnie maksimum, wpłynie to również na liczbę klatek na sekundę.

Najważniejsze czynniki, które należy wziąć pod uwagę:

- 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.

T10168181_pl

2024-06 (M19.2)

© 2021 – 2024 Axis Communications AB