AXIS Q21 Thermal Camera Series

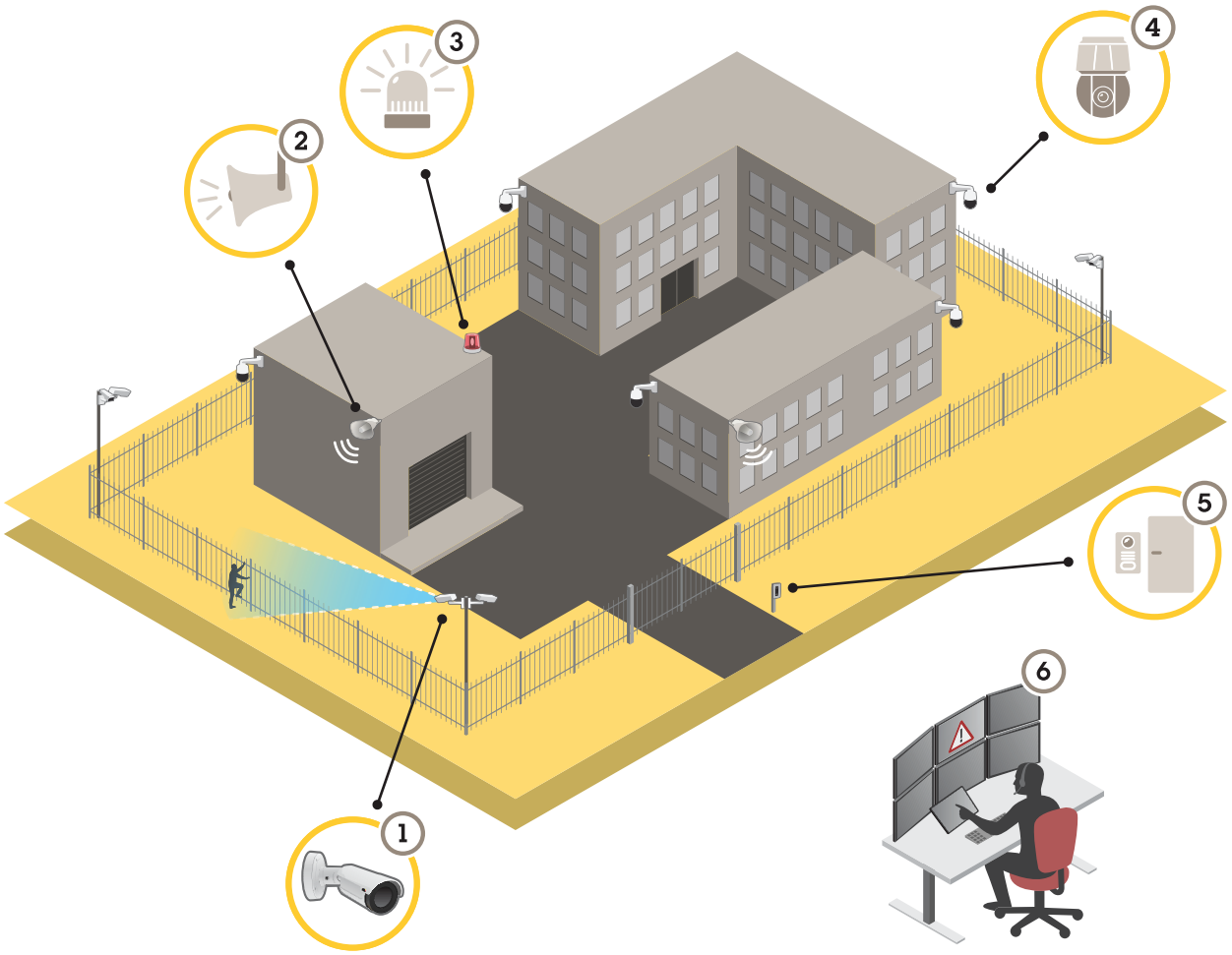
AXIS Q2111-E Thermal Camera

AXIS Q2112-E Thermal Camera

Podręcznik użytkownika

Spis treści

Informacje o rozwiązaniu



1 *Kamera termowizyjna z aplikacją AXIS Perimeter Defender*
2 *Głośnik tubowy*
3 *Sygnalizator świetlny*
4 *Kamera sieciowa PTZ*
5 *Kontroler drzwi*
6 *Centrum monitoringu*

Ochrona obwodowa

W przypadku obszarów wymagających detekcji wtargnięć można skonfigurować ochronę obwodową za pomocą kamer termowizyjnych z funkcjami analizy. Głównym celem ochrony obwodowej jest detekcja zagrożeń lub faktyczna ingerencja w jak najkrótszym czasie.

Aby skonfigurować ochronę obwodową, należy zainstalować aplikację do analizy (ochrona obwodowa) oraz zabezpieczyć kamerę termowizyjną. Firma Axis zapewnia w tym celu aplikację AXIS Perimeter Defender. Więcej informacji na temat aplikacji AXIS Perimeter Defender znajduje się na stronie *axis.com/products/axis-perimeter-defender*

Informacje o rozwiązaniu

- Aby poinformować intruzów o ochronie, można użyć sygnalizatora świetlnego (3). Patrz *Odstraszanie intruzów za pomocą sygnalizatora świetlnego na stronie 11*.
- Aby ostrzec i odstraszyć intruzów, należy zamontować głośnik (2), przez który można odtwarzać nagrany komunikat. Patrz *Odstraszanie intruzów za pomocą dźwięku na stronie 12*.

Instalacja

Film przedstawiający instalację urządzenia.

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

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

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

Więcej informacji na temat zalecanych przeglądarek można znaleźć na stronie *AXIS OS Portal*.

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis.

   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.

2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora na stronie 6*.

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: *Interfejs WWW na stronie 18*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła na stronie 6*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 65*.

Od czego zacząć

Bezpieczne hasła

Ważne

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

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

Aby chronić dane, zalecamy:

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

Sprawdzanie braku zmian w oprogramowaniu urządzenia

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

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 65*.

   Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.

2. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

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

Ustawienia podstawowe

Ustawianie częstotliwości zasilania

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

Ustawianie orientacji

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

   Zob. też.*Monitorowanie długich i wąskich obszarów na stronie 8* .

Regulowanie obrazu

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej na temat działania niektórych funkcji, przejdź do *Więcej informacji na stronie 48*.

Stabilizacja obrazu za pomocą funkcji stabilizacji obrazu

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

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

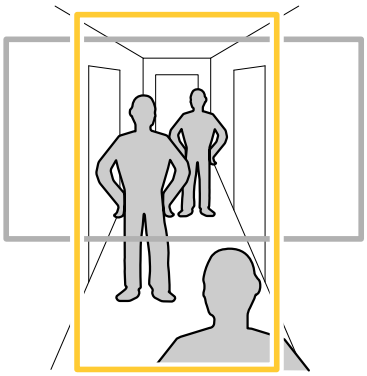
Uwaga

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

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

Monitorowanie długich i wąskich obszarów

Użyj formatu korytarzowego, aby lepiej używać pełnego pola widzenia w długich i wąskich obszarach, takich jak klatki schodowe, korytarze, drogi czy tunele.



1. W zależności od urządzenia, obróć kamerę lub obiektyw trójosiowy Axis o 90° lub 270°.
2. Jeżeli urządzenie nie ma funkcji automatycznego obrotu widoku, przejdź do okna **Video > Installation (Wideo > Instalacja)**.
3. Obróć widok o 90° lub 270°.

Wyświetlanie nakładek na obrazie

Możesz dodać obraz jako nałożenie do strumienia wideo.

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

Wyświetlanie nakładki tekstu

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

1. Wybierz kolejno opcje **Video > Overlays (Wideo > Nakładki)**.
2. Wybierz opcję **Text (Tekst)** i kliknij + .
3. Wpisz tekst, który ma być wyświetlany w strumieniu wideo.
4. Wybierz położenie. Aby zmienić położenie pola tekstowego nakładki, można je również przeciągnąć w podglądzie na żywo.

Przeglądanie i rejestracja obrazów wideo

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej o działaniu strumieniowania i pamięci masowej, przejdź do *Strumieniowanie i pamięć masowa na stronie 48*.

Zmniejszanie zapotrzebowania na przepustowość i zasób

Ważne

Zmniejszenie przepustowości może skutkować utratą wyrazistości szczegółów na obrazie.

1. Wybierz kolejno opcje **Video > Stream (Wideo > Strumień)**.
2. W podglądzie na żywo kliknij .
3. Wybierz **Video format (Format wideo) AV1**, jeśli urządzenie go obsługuje. W przeciwnym razie wybierz **H.264**.
4. Przejdź do okna **Video > Stream > General (Wideo > Strumień > Ogólne)** i zwiększ wartość w polu **Compression (Kompresja)**.
5. Przejdź do menu **Video > Stream > Zipstream (Wideo > Przesyłanie strumieniowe > Zipstream)** i wykonaj jedną lub więcej z czynności opisanych niżej:

   Uwaga

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

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

Uwaga

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

Konfiguracja zasobów sieciowej pamięci masowej

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

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

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z kamery

1. Wybierz kolejno opcje **Video > Image (Wideo > Obraz)**.
2. Aby rozpocząć nagrywanie, kliknij .

   Jeżeli jeszcze nie skonfigurowano żadnej pamięci masowej, kliknij i . Aby uzyskać instrukcje dotyczące konfigurowania sieciowej pamięci masowej, zob. *Konfiguracja zasobów sieciowej pamięci masowej na stronie 10*
3. Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

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

Sprawdzanie braku sabotażu wideo

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

1. Przejdź do menu **Video > Stream > General (Wideo > Strumieniowanie > Ogólne)** i włącz opcję **Signed video (Podpisane wideo)**.
2. Użyj opcji aplikacji AXIS Camera Station (w wersji 5.46 lub nowszej) lub innego zgodnego oprogramowania do zarządzania wideo i zapisu wideo. Aby uzyskać szczegółowe informacje, zobacz *instrukcję obsługi AXIS Camera Station*.
3. Wyeksportuj zarejestrowany materiał wideo.
4. Użyj aplikacji AXIS File Player do odtworzenia wideo. *Pobierz AXIS File Player.*

   wskazuje, że nie doszło do sabotażu wideo.

Uwaga

Aby uzyskać więcej informacji o wideo, kliknij wideo prawym przyciskiem myszy i wybierz opcję **Show digital signature (Pokaż cyfrowy podpis)**.

Konfiguracja reguł dotyczących zdarzeń

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

Aby uzyskać więcej informacji, zapoznaj się z przewodnikiem *Get started with rules for events* (Reguły dotyczące zdarzeń).

Odstraszanie intruzów za pomocą sygnalizatora świetlnego

Można użyć sygnalizatora świetlnego, aby poinformować potencjalnych intruzów, że teren jest chroniony.

W tym przykładzie wyjaśniono sposób podłączania sygnalizatora świetlnego i konfigurowania go w taki sposób, by migał, gdy kamera termowizyjna wykryje wtargnięcie. W podanym przykładzie sygnalizator świetlny można włączyć tylko w przypadku alarmów poza godzinami pracy, od 18:00 do 8:00 od poniedziałku do piątku; będzie on migał przez 30 sekund po każdej aktywacji.

Wymagany sprzęt

- Przewody połączeniowe (jeden niebieski i jeden czerwony, minimalna powierzchnia przekroju: 0,25 mm^2, maksymalna powierzchnia przekroju: 0,5 mm^2)
- Sygnalizator świetlny (12 V DC, maks. 25 mA)

Uwaga

Maksymalna długość przewodów łączących zależy od powierzchni przekroju przewodu i poboru energii przez sygnalizator świetlny.

Fizyczne podłączanie urządzeń

1. Podłącz czerwony przewód do styku 2 (wyjście DC, 12 V DC) złącza we/wy kamery.
2. Podłącz drugi koniec czerwonego przewodu do złącza oznaczonego znakiem **+** na sygnalizatorze świetlnym.
3. Podłącz niebieski przewód do styku 4 (wejście cyfrowe) złącza we/wy kamery.
4. Podłącz drugi koniec niebieskiego przewodu do złącza oznaczonego znakiem **–** na sygnalizatorze świetlnym.

Konfigurowanie portów we/wy

Podłącz sygnalizator świetlny do kamery przez interfejs WWW kamery:

1. Przejdź do menu **System > Accessories > I/O ports (System > Akcesoria > Porty we/wy)**.
2. W polu **Port 2** określ nazwę **Sygnalizator świetlny**.
3. W obszarze **Normal state (Stan normalny)** kliknij , aby ustawić normalny stan portu na otwarty (NO). To sprawi, że sygnalizator zacznie migać po wystąpieniu zdarzenia.

Tworzenie reguły

Aby kamera wysłała do sygnalizatora polecenie rozpoczęcia migania w momencie wykrycia zdarzenia, należy utworzyć w niej regułę.

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. W polu **Name (Nazwa)** wpisz **Sygnalizator świetlny**.
3. W polu **Wait between actions (Poczekaj między działaniami)** (o formacie gg:mm:ss) ustaw wartość 30 sekund.
4. Z listy warunków w obszarze **Application (Aplikacja)** wybierz aplikację do ochrony obwodowej.
5. Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**.
6. Kliknij opcję , aby dodać inny warunek.
7. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
8. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.
9. Z listy akcji w obszarze **I/O (We/Wy)** wybierz opcję **Toggle I/O while the rule is active (Przełącz We/Wy, gdy reguła jest aktywna)**.
10. Z listy portów wybierz port **Flashing beacon (Sygnalizator świetlny)**.
11. W polu **State (stan)** ustaw **Active (aktywny)**.
12. Kliknij przycisk **Zapisz**.

Odstraszanie intruzów za pomocą dźwięku

By ostrzec i odstraszyć potencjalnych intruzów, dołącz do instalacji głośnik sieciowy.

W tym przykładzie wyjaśniono sposób podłączania do kamery sieciowego głośnika tubowego Axis i jego konfiguracji w celu odtworzenia klipu audio po wykryciu wtargnięcia przez kamerę termowizyjną. W tym przykładzie głośnik tubowy jest aktywowany tylko w przypadku alarmów poza godzinami pracy: od 18:00 do 08:00, od poniedziałku do piątku.

Podłącz urządzenia

1. Przejdź do menu **System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie)**.
2. Wpisz adres IP, nazwę użytkownika oraz hasło dla głośnika. Należy użyć konta administratora lub operatora.
3. Kliknij przycisk **Połącz**.

Przesyłanie klipu audio do kamery

1. Przejdź do obszaru **Audio > Audio clips (Klipy audio)** i kliknij opcję  .
2. Kliknij **+ Add clip (Dodaj klip)**.
3. Znajdź i prześlij klip audio.
4. Kliknij przycisk **Zamknij**.

Tworzenie reguły

Aby głośnik odtwarzał klip audio w momencie wykrycia zdarzenia przez kamerę, należy utworzyć w niej regułę.

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. W polu **Name (Nazwa)** wpisz **Odstrasz dźwiękiem**.
3. Z listy warunków w obszarze **Application (Aplikacja)** wybierz aplikację do ochrony obwodowej.
4. Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**.
5. Kliknij opcję  , aby dodać inny warunek.
6. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
7. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.
8. Z listy akcji w obszarze **Audio clips (Klip audio)** wybierz opcję **Play audio clip (Odtwórz klip audio)**.
9. W sekcji **Clip (Klip)** zaznacz przesłany klip audio.
10. W obszarze **Audio output (Wyjście audio)** wybierz pozycję **1** dla sparowanego głośnika sieciowego.
11. Kliknij przycisk **Zapisz**.

Aktywowanie syreny stroboskopowej przez wejście wirtualne po wykryciu ruchu przez kamerę

Aby poinformować intruzów o ochronie, można użyć syreny stroboskopowej Axis.

W tym przykładzie wyjaśniono, jak spowodować uaktywnianie się profilu w syrenie stroboskopowej po każdym wykryciu ruchu przez aplikację AXIS Motion Guard.

Zanim zaczniesz:

- Utwórz w syrenie stroboskopowej nowe konto z uprawnieniami Operatora lub Administratora.
- Utwórz profil w syrenie stroboskopowej.
- Skonfigurowanie aplikacji AXIS Motion Guard w kamerze oraz utworzenie profilu o nazwie „Profil kamery".

Utworzenie dwóch odbiorców w kamerze:

1. W interfejsie urządzenia kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.

2. Wprowadź następujące informacje:
   - **Nazwa**: Aktywacja portu wirtualnego
   - **Typ**: **HTTP**
   - **URL**: http://<adresIP>/axis-cgi/virtualinput/activate.cgi

     Element <adresIP> zastąp adresem syreny stroboskopowej.
   - Nazwa i hasło nowo utworzonego konta syreny stroboskopowej.
3. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk **Zapisz**.
5. Dodaj drugiego odbiorcę z następującymi informacjami:
   - **Nazwa**: Dezaktywacja portu wirtualnego
   - **Typ**: **HTTP**
   - **URL**: http://<adresIP>/axis-cgi/virtualinput/deactivate.cgi

     Element <adresIP> zastąp adresem syreny stroboskopowej.
   - Nazwa i hasło nowo utworzonego konta syreny stroboskopowej.
6. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
7. Kliknij przycisk **Zapisz**.

Utworzenie dwóch reguł w kamerze:

1. Przejdź do obszaru **Rules (Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Aktywowanie wirtualnego WE/WY1
   - **Condition (Warunek)**: **Aplications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)**
   - **Action (Akcja)**: **Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)**
   - **Recipient (Odbiorca)**: **Aktywacja portu wirtualnego**
   - **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1
3. Kliknij przycisk **Zapisz**.
4. Dodaj kolejną regułę z następującymi informacjami:
   - **Nazwa**: Dezaktywacja wirtualnego WE/WY1
   - **Condition (Warunek)**: **Aplications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)**
   - Wybierz opcję **Invert this condition (Odwróć ten warunek)**.
   - **Action (Akcja)**: **Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)**
   - **Recipient (Odbiorca)**: **Dezaktywacja portu wirtualnego**
   - **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1

5. Kliknij przycisk **Zapisz**.

Utworzenie reguły w syrenie stroboskopowej:

1. W interfejsie WWW syreny stroboskopowej wybierz kolejno opcje **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Wyzwalacz w wirtualnym wejściu 1
   - **Condition (Warunek)**: **I/O (We/Wy) > Virtual input (Wejście wirtualne)**
   - **Port**: **1**
   - **Action (Akcja)**: **Light and siren > Run light and siren profile while the rule is active (Światło i syrena > Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna)**
   - **Profile (Profil)**: wybierz nowo utworzony profil
3. Kliknij przycisk **Zapisz**.

Wykrywanie ingerencji w sygnał wejściowy

W tym przykładzie wyjaśniono, w jaki sposób wysyłać wiadomość e-mail po odcięciu lub zwarciu obwodu sygnału wejściowego. Więcej informacji na temat złącza I/O: *strona 58*.

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

Dodaj odbiorcę wiadomości e-mail:

1. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź nazwę odbiorcy.
3. Wybierz adres**E-mail**.
4. Wprowadź adres e-mail odbiorcy.
5. Kamera nie ma dedykowanego serwera poczty e-mail, więc należy się zalogować na inny serwer, aby wysyłać wiadomości e-mail. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
6. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
7. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

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

Wyzwalanie alarmu, gdy ktoś otwiera obudowę

W tym przykładzie wyjaśniono, jak wyzwolić alarm, gdy ktoś otworzy obudowę urządzenia.

Add a recipient (Dodaj odbiorcę):

1. Przejdź do **System (System) > Events (Zdarzenia) > Recipients (Odbiorcy)** i kliknij **Add recipient (Dodaj odbiorcę)**.
2. Wprowadź nazwę odbiorcy.
3. Wybierz adres**E-mail**.
4. Wprowadź adres e-mail odbiorcy.
5. Kamera nie ma dedykowanego serwera poczty e-mail, więc należy się zalogować na inny serwer, aby wysyłać wiadomości e-mail. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
6. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
7. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

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

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

Activate the tampering detection (Aktywacja wykrywania sabotażu):

1. Przejdź do menu **System > Detectors > Camera tampering (System > Detektory > Sabotaż kamery)**.
2. Ustaw wartość dla funkcji **Trigger delay (Opóźnienie wyzwalacza)**. Wartość ta wskazuje czas, jaki musi upłynąć przed wysłaniem wiadomości e-mail.

Dodaj odbiorcę wiadomości e-mail:

3. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
4. Wprowadź nazwę odbiorcy.
5. Wybierz adres**E-mail**.
6. Wprowadź adres e-mail odbiorcy.
7. Kamera nie ma dedykowanego serwera poczty e-mail, więc należy się zalogować na inny serwer, aby wysyłać wiadomości e-mail. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
8. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
9. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

10. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.

11. Wprowadź nazwę reguły.
12. Z listy warunków w obszarze **Video (Wideo)** wybierz **Tampering (Sabotaż)**.
13. Z listy akcji w menu **Notifications (Powiadomienia)** wybierz pozycję **Send notification to email (Wyślij powiadomienie emailem)**, a następnie wybierz odbiorcę z listy.
14. Wpisz temat i treść wiadomości e-mail.
15. Kliknij przycisk **Zapisz**.

Dźwięk

Dodawanie dźwięku do zapisu

Włącz dźwięk:

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

Interfejs WWW

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

Uwaga

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

Wyświetl/ukryj menu główne. Wyświetl informacje o wersji. Uzyskaj dostęp do pomocy dotyczącej produktu. Zmień język. Ustaw jasny lub ciemny motyw. Menu użytkownika zawiera opcje:

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

Menu kontekstowe zawiera opcje:

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

Status

Informacje o urządzeniu

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

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

Stan synchronizacji czasu

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

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

Bezpieczeństwo

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

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

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

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

Trwające zapisy

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

Nagrania: pozwala wyświetlić trwające i przefiltrowane nagrania oraz ich źródła. Więcej informacji: *Nagrania na stronie 27*

 Pokazuje lokalizację zapisu nagrania w zasobie.

Nagranie wideo

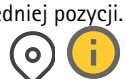
 Kliknij, aby odtworzyć strumień wideo na żywo.  Kliknij, aby zatrzymać odtwarzanie strumienia wideo na żywo.

 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:

- **Predefined controls (Wstępnie zdefiniowane elementy sterowania)**: Włącz, aby używać dostępnych ekranowych elementów sterowania.
- **Custom controls (Niestandardowe elementy sterowania)**: Kliknij  **Add custom control (Dodaj niestandardowy element sterujący)**, aby dodać ekranowy element sterujący.

 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 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.

1:1 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.

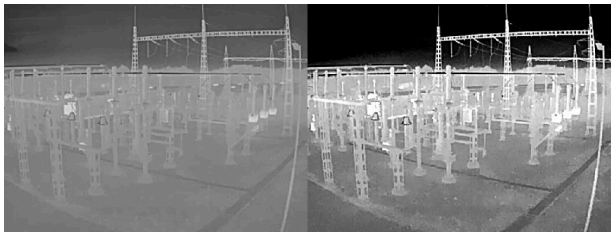
Korekcja obrazu

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.**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**.

Zdjęcie

Wygląd

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

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

Ekspozycja

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 gain (Maksymalne wzmocnienie): Wybierz odpowiednią maksymalną wartość wzmocnienia. Zwiększenie wartości maksymalnego wzmocnienia zwiększa poziom szczegółów w obrazach o niskim kontraście, ale jednocześnie zwiększa też poziom szumów. Więcej szumu może powodować większe wykorzystanie przepustowości i pamięci.

Strumień

Zapisy ogólne

Rozdzielczość: Wybierz rozdzielczość obrazu odpowiednią dla monitorowanej sceny. Wyższa rozdzielczość wymaga większej przepustowości i pojemności pamięci.**Palette (Paleta)** : Wybierz paletę, aby kolorować przy użyciu różnych kolorów w zależności od temperatury. Paleta może poprawić widoczność drobnych szczegółów.**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 lokalizację nałożenia na obrazie.
- **Obraz**: Wybierz, aby wyświetlać statyczny obraz nałożony na strumień wideo. Można użyć plików .bmp, .png, .jpeg lub .svg.
  Aby przesłać obraz, kliknij opcję **Images (Obrazy)**. Przed wysłaniem obrazu można użyć następujących opcji:
  - **Scale with resolution (Skaluj z rozdzielczością)**: Wybierz, aby automatycznie przeskalować obraz nałożenia i dopasować go do rozdzielczości obrazu wideo.
  - **Use transparency (Użyj przezroczystości)**: Wybierz i wprowadź wartość szesnastkową RGB dla danego koloru. Użyj formatu RRGGBB. Przykłady wartości szesnastkowych: FFFFFF (biały), 000000 (czarny), FF0000 (czerwony), 6633FF (niebieski), 669900 (zielony). Tylko dla obrazów .bmp.
- **Scene annotation (Adnotacja sceny)** : Ta opcja pozwala wyświetlać nałożenie tekstowe w strumieniu wideo, które pozostaje w tej samej pozycji, nawet gdy kamera obraca się lub przechyla w innym kierunku. Można wybrać wyświetlanie nałożenia tylko przy określonych zakresach powiększenia.
  - : Kliknij, aby dodać modyfikator daty `%F` powodujący wyświetlanie daty w formacie rrrr-mm-dd.
  - : Kliknij, aby dodać modyfikator czasu `%X` powodujący wyświetlanie czasu w formacie gg:mm:ss (zegar 24-godzinny).
  - **Modifiers (Modyfikatory)**: Kliknij, aby wybrać dowolny skonfigurowany wstępnie modyfikator widoczny na liście w celu dodania go do pola tekstowego. Na przykład modyfikator `%a` powoduje wyświetlanie dnia tygodnia.
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - **Appearance (Wygląd)**: Umożliwia wybór koloru tekstu i tła, np. białego tekstu na czarnym tle (ustawienie domyślne).
  - : Wybierz lokalizację nałożenia na obrazie. Nałożenie zostanie zapamiętane we współrzędnych obrotu i pochylenia tej pozycji.
  - **Annotation between zoom levels (%) (Adnotacja pomiędzy poziomami zoomu (%))**: Pozwala ustawić poziomy zoomu, przy których nałożenie będzie widoczne.
  - **Annotation symbol (Symbol adnotacji)**: Wybierz symbol, który będzie pokazywany zamiast nałożenia, gdy wartość zoomu przekroczy ustawiony zakres.

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

Maski prywatności

: Kliknij, aby utworzyć nową maskę prywatności.**Privacy masks (Maski prywatności)**: Kliknij, aby zmienić kolor wszystkich masek prywatności albo trwale usunąć wszystkie maski prywatności. **Mask x (Maska x)**: Kliknij, aby zmienić nazwę maski, wyłączyć ją lub trwale usunąć.

Narzędzia analityczne

Konfiguracja metadanych

RTSP metadata producers (Producenci metadanych RTSP)

Wyświetla listę aplikacji transmitujących metadane oraz wykorzystywane przez nie kanały.

Uwaga

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

Producer (Producent): Aplikacja generująca metadane. Poniżej aplikacji znajduje się lista typów metadanych przesyłanych przez nią strumieniowo z urządzenia.**Kanał**: Kanał używany przez aplikację. Należy zaznaczyć to pole, aby włączyć strumień metadanych. Usuń zaznaczenie, aby zapewnić zgodność lub zarządzać zasobami.

Dźwięk

Ustawienia urządzenia

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

Input type (Typ danych wejściowych): Wybierz typ źródła sygnału wejściowego, na przykład mikrofon lub wejście liniowe.**Power type (Rodzaj 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.

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.

Wzmocnienie dźwięku

Wejście

Dziesięciopasmowy graficzny korektor audio: Włącz tę opcję, aby regulować poziomy różnych zakresów częstotliwości sygnału audio. Ta funkcja jest przeznaczona dla zaawansowanych użytkowników mających doświadczenie w konfigurowaniu ustawień dźwięku.**Talkback range (Zasięg funkcji Talkback)** : Wybierz zakres operacyjny zbierania materiału dźwiękowego. Zwiększenie zakresu operacyjnego ogranicza możliwości w zakresie jednoczesnej komunikacji dwukierunkowej. **Voice enhancement (Wzmocnienie głosu)** : Włącz tę opcję, aby wzmocnić głośność komunikatów głosowych w odniesieniu do innych dźwięków.

Nagrania

Ongoing recordings (Trwające nagrania): Pokaż wszystkie trwające zapisy na urządzeniu. Wybierz, aby rozpocząć nagrywanie w urządzeniu. Wybierz docelowy zasób, w którym chcesz zapisać nagrania. Zatrzymaj nagrywanie w urządzeniu.**Uruchomione nagrania** zostaną zakończone zarówno po zatrzymaniu ręcznym, jak i po wyłączeniu urządzenia.**Zapis ciągły** będzie kontynuowane do momentu zatrzymania ręcznego. Jeśli urządzenie zostanie wyłączone, zapis będzie kontynuowany po jego ponownym włączeniu.

Odtwórz nagranie. Zatrzymaj odtwarzanie nagrania. Wyświetl lub ukryj informacje i opcje nagrania.**Set export range (Ustaw zakres eksportu)**: Jeżeli chcesz wyeksportować tylko część nagrania, określ zakres czasu. Pamiętaj, że jeśli pracujesz w strefie czasowej innej niż lokalizacja urządzenia, przedział czasu jest oparty na strefie czasowej urządzenia.**Encrypt (Szyfruj)**: ta opcja pozwala skonfigurować hasło do eksportowanych nagrań. Podanie ustawionego hasła będzie konieczne do otworzenia eksportowanego pliku. Kliknij, aby usunąć nagranie.**Export (Eksportuj)**: pozwala wyeksportować całe nagranie lub jego fragment.

Kliknij, aby filtrować nagrania.**From (Od)**: Pokazuje nagrania wykonane po określonym momencie w czasie.**To (Do)**: Pokazuje nagrania wykonane przed określonym momentem w czasie.**Source (Źródło)** : Pokazuje nagrania z podziałem na źródła. Źródło odnosi się do czujnika.**Event (Zdarzenie)**: Pokazuje nagrania z podziałem na zdarzenia.**Pamięć masowa**: Pokazuje nagrania z podziałem na typy zasobów.

Aplikacje

Add app (Dodaj aplikację): umożliwia zainstalowanie nowej aplikacji.**Find more apps (Znajdź więcej aplikacji)**: pozwala znaleźć więcej aplikacji do zainstalowania. Nastąpi przekierowanie na stronę z opisem aplikacji Axis.**Allow unsigned apps (Zezwalaj na niepodpisane aplikacje)** : włączenie tej opcji umożliwi instalowanie niepodpisanych aplikacji.**Allow root-privileged apps (Zezwalaj na aplikacje z uprawnieniami roota)** : włączenie tej opcji umożliwi aplikacjom z uprawnieniami roota pełny dostęp do urządzenia. Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

Aby włączyć lub wyłączyć aplikację, użyj przełącznika znajdującego się obok jej nazwy.**Open (Otwórz)**: umożliwia uzyskanie dostępu do ustawień aplikacji. Dostępne ustawienia zależą od aplikacji. W niektórych aplikacjach nie ma żadnych ustawień. Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

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

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

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

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

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

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

Uwaga

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

Lokalizacja urządzenia

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

- **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.

Protokoły wykrywania sieci

Bonjour®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**Nazwa Bonjour**: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.**UPnP**®: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**Nazwa UPnP**: wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.**WS-Discovery**: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.**LLDP and CDP (LLDP i CDP)**: Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci. Wyłączenie funkcji LLDP and CDP może wpływać na negocjowanie zasilania z PoE. Aby rozwiązać ewentualne problemy negocjowania zasilania z PoE, należy skonfigurować przełącznik PoE tylko do sprzętowej negocjacji zasilania PoE.

Globalne serwery proxy

Http proxy (Serwer proxy HTTP): Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.**Https proxy (Serwer proxy HTTPS)**: Określ hosta lub adres IP globalnego serwera proxy, używając dozwolonego formatu.
Dozwolone formaty serwerów proxy HTTP i HTTPS:

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

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

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

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

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

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

Allow O3C (Zezwalaj na O3C):

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

Proxy settings (Ustawienia proxy): W razie potrzeby należy wprowadzić ustawienia proxy, aby połączyć się z serwerem proxy.**Host**: Wprowadź adres serwera proxy.**Port**: wprowadź numer portu służącego do uzyskania dostępu.**Login** i **Hasło**: W razie potrzeby wprowadź nazwę użytkownika i hasło do serwera proxy.**Authentication method (Metoda uwierzytelniania)**:

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

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

SNMP

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

SNMP: Wybierz wersję SNMP.

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

Uwaga

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

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

Bezpieczeństwo

Certyfikaty

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

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

Obsługiwane są następujące formaty:

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

Ważne

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

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

- **More (Więcej)** : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Secure element (Zabezpieczony element)** lub **Trusted Platform Module 2.0 (Moduł TPM 2.0)** do bezpiecznego przechowywania

klucza prywatnego. Aby uzyskać więcej informacji na temat bezpiecznego magazynu kluczy, odwiedź stronę *help.axis.com/en-us/axis-os#cryptographic-support*.
- **Key type (Typ klucza)**: Aby zabezpieczyć certyfikat, wybierz domyślny algorytm szyfrowania lub inny z listy rozwijanej.

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

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

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1xIEEE 802.1x to standard IEEE dla kontroli dostępu sieciowego opartej na portach, zapewniający bezpieczne uwierzytelnianie przewodowych i bezprzewodowych urządzeń sieciowych. IEEE 802.1x jest oparty na protokole EAP (Extensible Authentication Protocol).Aby uzyskać dostęp do sieci zabezpieczonej IEEE 802.1x, urządzenia sieciowe muszą dokonać uwierzytelnienia. Do uwierzytelnienia służy serwer, zazwyczaj RADIUS, taki jak FreeRADIUS i Microsoft Internet Authentication Server.**IEEE 802.1AE MACsec**IEEE 802.1AE MACsec jest standardem IEEE dotyczącym adresu MAC, który definiuje bezpołączeniową poufność i integralność danych dla protokołów niezależnych od dostępu do nośników.**Certyfikaty**W przypadku konfiguracji bez certyfikatu CA, sprawdzanie poprawności certyfikatów serwera jest wyłączone, a urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.Podczas korzystania z certyfikatu w instalacjach firmy Axis urządzenie i serwer uwierzytelniający używają do uwierzytelniania certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).Aby zezwolić urządzeniu na dostęp do sieci chronionej za pomocą certyfikatów, w urządzeniu musi być zainstalowany podpisany certyfikat klienta.**Authentication method (Metoda uwierzytelniania)**: Wybierz typ protokołu EAP na potrzeby uwierzytelniania.**Client certificate (Certyfikat klienta)**: wybierz certyfikat klienta, aby użyć IEEE 802.1x. Serwer uwierzytelniania używa certyfikatu do weryfikacji tożsamości klienta.**Certyfikaty CA**: wybierz certyfikaty CA w celu potwierdzania tożsamości serwera uwierzytelniającego. Jeśli nie wybrano żadnego certyfikatu, urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.**EAP identity (Tożsamość EAP)**: wprowadź tożsamość użytkownika powiązaną z certyfikatem klienta.**EAPOL version (Wersja protokołu EAPOL)**: wybierz wersję EAPOL używaną w switchu sieciowym.**Use IEEE 802.1x (Użyj IEEE 802.1x)**: wybierz, aby użyć protokołu IEEE 802.1 x.Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą **IEEE 802.1x PEAP-MSCHAPv2**:
- **Hasło**: Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap)**: wybierz wersję Peap używaną w switchu sieciowym.
- **Etykieta**: 1 pozwala używać szyfrowania EAP klienta; 2 pozwala używać szyfrowania PEAP klienta. Wybierz etykietę używaną przez przełącznik sieciowy podczas korzystania z wersji 1 protokołu Peap.

Te ustawienia są dostępne wyłącznie w przypadku uwierzytelniania za pomocą **IEEE 802.1ae MACsec (klucz CAK/PSK)**:
- **Nazwa klucza skojarzenia łączności umowy klucza**: Wprowadź nazwę skojarzenia łączności (CKN). Musi to być od 2 do 64 (podzielnych przez 2) znaków szesnastkowych. CKN musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.
- **Klucz skojarzenia łączności umowy klucza**: Wprowadź klucz skojarzenia łączności (CAK). Musi mieć 32 lub 64 znaki szesnastkowe. CAK musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.

Zapobiegaj atakom typu brute force

Blocking (Blokowanie): włącz, aby blokować ataki typu brute force Ataki typu brute-force wykorzystują metodę prób i błędów do odgadnięcia danych logowania lub kluczy szyfrowania.**Blocking period (Okres blokowania)**: Wprowadź liczbę sekund, w ciągu których ataki typu brute-force mają być blokowane.**Blocking conditions (Warunki blokowania)**: wprowadź dopuszczalną liczbę nieudanych prób uwierzytelnienia na sekundę przed rozpoczęciem blokowania. Liczbę dopuszczalnych niepowodzeń można ustawić zarówno na stronie, jak i w urządzeniu.

Zapora

Activate (Aktywuj): Włącz zaporę sieciową.
Domyślne ustawienia zasad: Wybierz stan domyślny zapory.

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

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

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

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

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

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

Uwaga

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

Confirm rules (Potwierdzenie reguł): Kliknięcie tej opcji aktywuje oczekujące reguły.**Active rules (Aktywne reguły)**: Omówienie reguł obecnie stosowanych w urządzeniu. : Kliknięcie tej opcji pozwala usunąć aktywną regułę. : Kliknięcie tej opcji pozwala usunąć wszystkie oczekujące i aktywne reguły.

Niestandardowy podpisany certyfikat systemu AXIS OS

Do zainstalowania w urządzeniu oprogramowania testowego lub innego niestandardowego oprogramowania Axis konieczny jest niestandardowy podpisany certyfikat systemu AXIS OS. Certyfikat służy do sprawdzenia, czy oprogramowanie jest zatwierdzone zarówno przez właściciela urządzenia, jak i przez firmę Axis. Oprogramowanie działa tylko na określonym urządzeniu z niepowtarzalnym numerem seryjnym i identyfikatorem procesora. Niestandardowe podpisane certyfikaty systemu AXIS OS mogą być tworzone tylko przez firmę Axis, ponieważ Axis posiada klucze do ich podpisywania.**Zainstaluj**: Kliknij przycisk Install (Instaluj), aby zainstalować certyfikat. Certyfikat musi zostać zainstalowany przed zainstalowaniem oprogramowania.
Menu kontekstowe zawiera opcje:

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

Konta

Konta

Add account (Dodaj konto): Kliknij, aby dodać nowe konto. Można dodać do 100 kont.**Account (Konto)**: Wprowadź niepowtarzalną nazwę konta.**Nowe hasło**: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.**Repeat password (Powtórz hasło)**: Wprowadź ponownie to samo hasło.**Privileges (Przywileje)**:

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

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.**Nowe hasło**: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.**Repeat password (Powtórz hasło)**: Wprowadź ponownie to samo hasło.**Uwaga**: Wprowadź komentarz (opcjonalnie). Menu kontekstowe zawiera opcje:**Update SSH account (Zaktualizuj konto SSH)**: Pozwala edytować właściwości konta.**Delete SSH account (Usuń konto SSH)**: Pozwala usunąć konto. Nie można usunąć konta root.

Virtual host (Host wirtualny)

Add virtual host (Dodaj host wirtualny): kliknięcie tej opcji pozwala dodać nowego wirtualnego hosta.**Włączony**: zaznaczenie tej opcji spowoduje używanie tego wirtualnego hosta.**Server name (Nazwa serwera)**: w tym polu można wpisać nazwę serwera. Używaj tylko cyfr 0-9, liter A-Z i łącznika (-).**Port**: w tym polu należy podać port, z którym jest połączony serwer.**Type (Typ)**: pozwala wybrać typ poświadczenia, które ma być używane. Dostępne są opcje **Basic (Podstawowe)**, **Digest (Szyfrowane)** oraz **Open ID (Otwarte ID)**. Menu kontekstowe zawiera opcje:

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

Disabled (Wyłączono): Serwer jest wyłączony.

Konfiguracja OpenID

Ważne

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

Client ID (Identyfikator klienta): Wprowadź nazwę użytkownika OpenID.**Outgoing Proxy (Wychodzący serwer proxy)**: Aby używać serwera proxy, wprowadź adres serwera proxy dla połączenia OpenID.**Admin claim (Przypisanie administratora)**: Wprowadź wartość roli administratora.**Provider URL (Adress URL dostawcy)**: Wprowadź łącze internetowe do uwierzytelniania punktu końcowego interfejsu programowania aplikacji (API). Łącze musi mieć format https://[wstaw URL]/.well-known/openid-configuration**Operator claim (Przypisanie operatora)**: Wprowadź wartość roli operatora.**Require claim (Wymagaj przypisania)**: Wprowadź dane, które powinny być dostępne w tokenie.**Viewer claim (Przypisanie dozorcy)**: Wprowadź wartość dla roli dozorcy.**Remote user (Użytkownik zdalny)**: Wprowadź wartość identyfikującą użytkowników zdalnych. Pomoże to wyświetlić bieżącego użytkownika w interfejsie WWW urządzenia.**Scopes (Zakresy)**: Opcjonalne zakresy, które mogą być częścią tokenu.**Client secret (Tajny element klienta)**: Wprowadź hasło OpenID. **Save (Zapisz)**: Kliknij, aby zapisać wartości OpenID.**Enable OpenID (Włącz OpenID)**: Włącz tę opcję, aby zamknąć bieżące połączenie i zezwolić na uwierzytelnianie urządzenia z poziomu adresu URL dostawcy.

Zdarzenia

Reguły

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

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.**Nazwa**: Wprowadź nazwę reguły.**Wait between actions (Poczekaj między działaniami)**: Wprowadź minimalny czas (w formacie gg:mm:ss), jaki musi upłynąć między aktywacjami reguły. Ustawienie to jest przydatne, gdy reguła jest aktywowana na przykład warunkami trybów dziennego i nocnego, ponieważ zapobiega niepożądanemu uruchamianiu reguły przez niewielkie zmiany natężenia światła podczas wschodu i zachodu słońca.**Condition (Warunek)**: Wybierz warunek z listy. Dopiero po spełnieniu tego warunku urządzenie wykona akcję. Jeśli określono wiele warunków, to do wyzwolenia działania konieczne jest spełnienie wszystkich z nich. Informacje na temat konkretnych warunków można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.**Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**: Zaznacz tę opcję, aby ten pierwszy warunek działał tylko jako wyzwalacz początkowy. Oznacza to, że po aktywacji reguła pozostanie czynna przez cały czas, gdy są spełniane wszystkie pozostałe warunki, bez względu na stan pierwszego warunku. Jeżeli nie zaznaczysz tej opcji, reguła będzie aktywna po spełnieniu wszystkich warunków.**Invert this condition (Odwróć ten warunek)**: Zaznacz tę opcję, jeśli warunek ma być przeciwieństwem dokonanego przez Ciebie wyboru. **Add a condition (Dodaj warunek)**: Kliknij, aby dodać kolejny warunek. **Action (Akcja)**: Wybierz akcję z listy i wprowadź jej wymagane informacje. Informacje na temat konkretnych akcji można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Odbiorcy

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

Uwaga

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

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

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

Add a recipient (Dodaj odbiorcę): Kliknij, aby dodać odbiorcę. **Nazwa**: Wprowadź nazwę odbiorcy.**Type (Typ)**: Wybierz z listy:

- FTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer FTP. Domyślny port to 21.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze FTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.
  - **Use passive FTP (Użyj pasywnego FTP)**: W normalnych warunkach produkt po prostu wysyła żądanie otwarcia połączenia do serwera FTP. Urządzenie inicjuje przesyłanie danych na serwer docelowy i kontrolę serwera FTP. Jest to zazwyczaj konieczne w przypadku zapory ogniowej pomiędzy urządzeniem a serwerem FTP.
- HTTP
  - **URL**: Wprowadź adres sieciowy serwera HTTP oraz skrypt obsługujący żądanie. Na przykład: http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTP.
- HTTPS
  - **URL**: Wprowadź adres sieciowy serwera HTTPS oraz skrypt obsługujący żądanie. Na przykład: https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Potwierdź certyfikat serwera)**: Zaznacz tę opcję, aby sprawdzić certyfikat utworzony przez serwer HTTPS.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTPS.
- **Sieciowa pamięć masowa**
  Umożliwia dodanie takiego zasobu sieciowego, jak NAS (sieciowy zasób dyskowy), i wykorzystywanie go jako odbiorcy plików. Pliki zapisywane są w formacie Matroska (MKV).
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera pamięci sieciowej.
  - **Udział**: Podaj nazwę współdzielonego udziału na serwerze hosta.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
- SFTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer SFTP. Domyślny port to 22.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze SFTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.

- **SSH host public key type (Typ klucza publicznego hosta SSH) (MD5)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 32 cyfr w szesnastkowym systemie liczbowym). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
- **SSH host public key type (Typ klucza publicznego hosta SSH) (SHA256)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 43 cyfr w systemie kodowania Base64). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
- **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.

- **SIP or VMS (SIP lub VMS)** :
  SIP: Wybierz w celu nawiązania połączenia SIP.
  VMS: Wybierz w celu nawiązania połączenia VMS.
  - **From SIP account (Z konta SIP)**: Wybierz z listy.
  - **To SIP address (Na adres SIP)**: Wprowadź adres SIP.
  - **Test (Testuj)**: Kliknij, aby sprawdzić, czy ustawienia połączeń działają prawidłowo.
- **E-mail**
  - **Wyślij wiadomość e-mail do**: Wprowadź adresy odbiorców. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
  - **Wyślij e-mail przez**: Wprowadź adres serwera nadawcy.
  - **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
  - **Hasło**: Wprowadź hasło dostępu do serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
  - **Email server (SMTP) (Serwer poczty e-mail (SMTP))**: Wprowadź nazwę serwera SMTP, na przykład smtp.gmail.com, smtp.mail.yahoo.com.
  - **Port**: wprowadź numer portu serwera SMTP, używając wartości z zakresu 0–65535. Wartość domyślna to 587.
  - **Szyfrowanie**: Aby używać szyfrowania, wybierz opcję SSL lub TLS.
  - **Validate server certificate (Potwierdź certyfikat serwera)**: Jeżeli używasz szyfrowania, zaznacz tę opcję, aby weryfikować tożsamość urządzenia. Certyfikat może mieć własny podpis lub podpis jednostki certyfikującej (CA).
  - **POP authentication (Uwierzytelnianie POP)**: Włącz tę opcję i wprowadź nazwę serwera POP, na przykład pop.gmail.com.

  Uwaga

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

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

Test (Testuj): Kliknij, aby przetestować konfigurację. Menu kontekstowe zawiera opcje:**View recipient (Pokaż odbiorcę)**: Kliknij, aby wyświetlić wszystkie dane odbiorcy.**Copy recipient (Kopiuj odbiorcę)**: Kliknij, aby skopiować odbiorcę. Po skopiowaniu odbiorcy można wprowadzić zmiany w nowym wpisie odbiorcy.**Delete recipient (Usuń odbiorcę)**: Kliknij, aby trwale usunąć odbiorcę.

Harmonogramy

Harmonogramów i zdarzeń jednorazowych można użyć jako warunków reguł. Na liście wyświetlane są wszystkie harmonogramy i zdarzenia jednorazowe skonfigurowane dla produktu, a także informacje dotyczące ich konfiguracji. + **Add schedule (Dodaj harmonogram)**: Kliknij, aby utworzyć harmonogram lub impuls.

Wyzwalacze ręczne

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

MQTT

MQTT (przesyłanie telemetryczne usługi kolejkowania wiadomości) to standardowy protokół do obsługi komunikacji w Internecie rzeczy (IoT). Został zaprojektowany z myślą o uproszczeniu integracji IoT i jest wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji objętości kodu i obciążenia sieci. Klient MQTT w oprogramowaniu urządzeń Axis może ułatwiać integrację danych i zdarzeń generowanych w urządzeniu z systemami, które nie są oprogramowaniem do zarządzania materiałem wizyjnym (VMS).Konfiguracja urządzenia jako klienta MQTT. Komunikacja MQTT oparta jest na dwóch jednostkach, klientach i brokerze. Klienci mogą wysyłać i odbierać wiadomości. Broker odpowiedzialny jest za rozsyłanie wiadomości między klientami.Więcej informacji o protokole MQTT znajdziesz w *portalu poświęconym systemowi AXIS OS*.

ALPN

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

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.**Status (Stan)**: pokazuje bieżący status klienta MQTT.**BrokerHost**: wprowadź nazwę hosta lub adres IP serwera MQTT.**Protocol (Protokół)**: wybór protokołu, który ma być używany.**Port**: Wprowadź numer portu.

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

ALPN protocol (Protokół ALPN): Wprowadź nazwę protokołu ALPN dostarczoną przez dostawcę brokera MQTT. Dotyczy to tylko ustawień MQTT przez SSL i MQTT przez WebSocket Secure.**Username (Nazwa użytkownika)**: należy tu wprowadzić nazwę użytkownika, która będzie umożliwiać klientowi dostęp do serwera.**Hasło**: wprowadzić hasło dla nazwy użytkownika.**Client ID (Identyfikator klienta)**: wprowadź identyfikator klienta. Identyfikator klienta jest wysyłany do serwera w momencie połączenia klienta.**Clean session (Czysta sesja)**: steruje zachowaniem w czasie połączenia i czasie rozłączenia. Po wybraniu tej opcji informacje o stanie są odrzucane podczas podłączania i rozłączania.**HTTP proxy (Serwer proxy HTTP)**: Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTP, możesz zostawić to pole puste.**HTTPS proxy (Serwer proxy HTTPS)**: Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTPS, możesz zostawić to pole puste.**Keep alive interval (Przedział czasowy KeepAlive)** Umożliwia klientowi detekcję, kiedy serwer przestaje być dostępny, bez konieczności oczekiwania na długi limit czasu TCP/IP.**Timeout (Przekroczenie limitu czasu)**: interwał czasowy (w sekundach) pozwalający na zakończenie połączenia. Wartość domyślna: 60**Prefiks tematu urządzenia**: Używany w domyślnych wartościach tematu w komunikacie łączenia i komunikacie LWT na karcie **MQTT client (Klient MQTT)** oraz w warunkach publikowania na karcie **MQTT publication (Publikacja MQTT)**.**Reconnect automatically (Ponowne połączenie automatyczne)**: określa, czy klient powinien ponownie połączyć się automatycznie po rozłączeniu.**Komunikat łączenia**określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.**Send message (Wysłanie wiadomości)**: włącz, aby wysyłać wiadomości.**Use default (Użyj domyślnych)**: wyłącz, aby wprowadzić własną wiadomość domyślną.**Topic (Temat)**: wprowadź temat wiadomości domyślnej.**Payload (Próbka)**: wprowadź treść wiadomości domyślnej.**Retain (Zachowaj)**: wybierz, aby zachować stan klienta w tym **Topic (Temacie)QoS**: zmiana warstwy QoS dla przepływu pakietów.**Wiadomość Ostatnia Wola i Testament**Funkcja Last Will Testament (LWT) zapewnia klientowi dostarczenie informacji wraz z poświadczeniami w momencie łączenia się z brokerem. Jeżeli klient nie rozłączy się w pewnym momencie w późniejszym terminie (może to być spowodowane brakiem źródła zasilania), może umożliwić brokerowi dostarczenie komunikatów do innych klientów. Ten komunikat LWT ma taką samą postać jak zwykła

wiadomość i jest kierowany przez tę samą mechanikę.**Send message (Wysłanie wiadomości)**: włącz, aby wysyłać wiadomości.**Use default (Użyj domyślnych)**: wyłącz, aby wprowadzić własną wiadomość domyślną.**Topic (Temat)**: wprowadź temat wiadomości domyślnej.**Payload (Próbka)**: wprowadź treść wiadomości domyślnej.**Retain (Zachowaj)**: wybierz, aby zachować stan klienta w tym **Topic (Temacie)QoS**: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

Użyj domyślnego prefiksu: Wybierz ustawienie, aby używać domyślnego prefiksu zdefiniowanego za pomocą prefiksu urządzenia w zakładce **MQTT client (Klient MQTT)**.**Dołącz nazwę tematu**: Wybierz, aby do tematu MQTT dołączać tematy opisujące warunek.**Dołącz nazwy przestrzenne tematu**: Wybierz, aby do tematu MQTT dołączać przestrzenie nazw tematów ONVIF.**Include serial number (Uwzględnij numer seryjny)**: Wybierz, aby w danych właściwych usługi MQTT umieszczać numer seryjny urządzenia.

Add condition (Dodaj warunek): Kliknij, aby dodać warunek.**Retain (Zachowaj)**: Definiuje, które komunikaty MQTT mają być wysyłane jako zachowywane.

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

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

Add subscription (Dodaj subskrypcję): Kliknij, aby dodać nową subskrypcję usługi MQTT.**Subscription filter (Filtr subskrypcyjny)**: Wprowadź temat MQTT, który chcesz subskrybować.**Use device topic prefix (Użyj prefiksu tematu urządzenia)**: Dodaj filtr subskrypcji jako prefiks do tematu MQTT.**Subscription type (Typ subskrypcji)**:

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

QoS: Wybierz żądany poziom subskrypcji MQTT.

Nałożenia MQTT

Uwaga

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

Add overlay modifier (Dodaj modyfikator nałożenia): Kliknij, aby dodać nowy modyfikator nakładki.**Topic filter (Filtr tematów)**: Dodaj temat MQTT zawierający dane, które mają być pokazywane w nakładce.**Data field (Pole danych)**: Wprowadź klucz danych właściwych komunikatu, które mają być wyświetlane w nakładce, zakładając, że komunikat jest w formacie JSON.
Modifier (Modyfikator): Używanie utworzonego modyfikatora podczas tworzenia nakładki.

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

Przechowywanie

Sieciowa pamięć masowa

Ignore (Ignoruj): włączenie tej opcji będzie powodowało ignorowanie zasobów pamięci sieciowej.**Add network storage (Dodaj zasób sieciowy)**: Kliknij tę opcję w celu dodania udziału sieciowego, w którym będziesz zapisywać nagrania.

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

Remove network storage (Usuń sieciową pamięć masową): Kliknij tę opcję w celu odinstalowania, odpięcia i usunięcia połączenia z udziałem sieciowym. Spowoduje to usunięcie wszystkich ustawień udziału sieciowego.**Unbind (Odepnij)**: Kliknięcie tej opcji spowoduje odpięcie i odłączenie udziału sieciowego.
Bind (Powiąż): kliknięcie tej opcji spowoduje powiązanie i połączenie udziału sieciowego.**Odmontuj**: Kliknięcie tej opcji spowoduje odmontowanie udziału sieciowego.
Mount (Zamontuj): kliknięcie tej opcji spowoduje zamontowanie udziału sieciowego.**Write protect (Zabezpieczenie przed zapisem)**: Włącz tę opcję, aby uniemożliwić zapis w udziale sieciowym i zabezpieczyć nagrania przed usunięciem. Nie można formatować udziału sieciowego zabezpieczonego przed zapisem.**Retention time (Czas przechowywania)**: Wybierz, jak długo nagrania mają być przechowywane, aby ograniczyć liczbę starych nagrań lub ze względu na zachowanie zgodności z regulacjami w sprawie przechowywania danych. Zapełnienie zasobu sieciowego spowoduje usunięcie starych nagrań przed upływem wybranego czasu. **Narzędzia**

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

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

Pamięć pokładowa

Ważne

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

Odmontuj: Kliknij w celu bezpiecznego usunięcia karty SD.**Write protect (Zabezpieczenie przed zapisem)**: Włącz, aby uniemożliwić zapis na karcie SD i zabezpieczyć zapisy przed usunięciem. Nie można formatować kart SD zabezpieczonych przed zapisem.**Autoformat (Automatyczne formatowanie)**: Włącz, aby automatycznie formatować nowo włożoną kartę SD. Powoduje to formatowanie systemu plików do ext4.**Ignore (Ignoruj)**: Włączenie tej opcji powoduje zaprzestanie przechowywania nagrań na karcie SD. Jeżeli zignorujesz kartę SD, urządzenie nie będzie jej rozpoznawać. Z tego ustawienia mogą korzystać tylko administratorzy.**Retention time (Czas przechowywania)**: Wybierz, jak długo mają być przechowywane nagrania, aby ograniczyć liczbę starych nagrań lub zachować zgodność z regulacjami z zakresu przechowywania danych. Zapełnienie karty SD powoduje usuwanie starych nagrań przed upływem czasu ich przechowywania.**Narzędzia**

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

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

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

Profile strumienia

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

Add stream profile (Dodaj profil strumienia): Kliknij to polecenie w celu utworzenia nowego profilu strumienia.**Preview (Podgląd)**: Podgląd strumienia wideo z wybranymi ustawieniami profilu strumienia. Zmiana ustawień na stronie powoduje aktualizowanie podglądu. Jeśli urządzenie ma różne obszary obserwacji, aktywny obszar obserwacji można zmienić w menu rozwijanym w lewym dolnym rogu obrazu. **Nazwa**: Nadaj profilowi nazwę.**Description (Opis)**: Dodaj opis profilu.**Video codec (Kodek wideo)**: Wybierz kodek wideo, który ma być stosowany w profilu.**Rozdzielczość**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Frame rate (Liczba klatek na sekundę)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Compression (Kompresja)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Zipstream** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Optimize for storage (Optymalizacja pod kątem pamięci masowej)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Dynamic FPS (Dynamiczna liczba klatek na sekundę)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Dynamic GOP (Dynamiczna grupa obrazów)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Mirror (Odbicie lustrzane)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**GOP length (Długość grupy obrazów)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Bitrate control (Kontrola przepływności bitowej)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.**Include overlays (Uwzględnij nałożenia)** : Wybierz typ nakładek, jakie mają być dołączane. Informacje o dodawaniu nakładek znajdują się w temacie *Nakładki na stronie 24*.**Include audio (Dołącz audio)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 22*.

ONVIF

Konta ONVIF

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

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

Add accounts (Dodaj konta): Kliknij, aby dodać nowe konto ONVIF.**Account (Konto)**: Wprowadź niepowtarzalną nazwę konta.**Nowe hasło**: wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.**Repeat password (Powtórz hasło)**: Wprowadź ponownie to samo hasło.**Rola**:

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

Menu kontekstowe zawiera opcje:**Update account (Zaktualizuj konto)**: Pozwala edytować właściwości konta.**Delete account (Usuń konto)**: Pozwala usunąć konto. Nie można usunąć konta root.

Profile mediów ONVIF

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

Add media profile (Dodaj profil mediów): Kliknij, aby dodać nowy profil ONVIF.**Profile name (Nazwa profilu)**: Dodaj nazwę profilu multimediów.**Video source (Źródło wideo)**: Wybierz źródło wideo dla swojej konfiguracji.

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

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

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

Uwaga

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

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

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

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

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

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

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

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

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

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

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

PTZ  : Wybierz ustawienia PTZ dla swojej konfiguracji.

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

Create (Utwórz): Kliknij tę opcję, aby zapisać ustawienia i utworzyć profil.**Cancel (Anuluj)**: Kliknij tę opcję, aby anulować konfigurację i wyzerować wszystkie ustawienia.**profile_x (profil_x)**: Kliknij nazwę profilu, aby otworzyć i edytować wstępnie skonfigurowany profil.

Detektory

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.

Akcesoria

Obrót/pochylenie/zbliżenie

Do połączeń z zewnętrznymi urządzeniami PTZ należy używać sterowników PTZ.

- **Driver (Sterownik)**: Wybierz sterownik urządzenia PTZ. Aby podłączone urządzenie działało poprawnie, wymagany jest sterownik.
- **Device type (Typ urządzenia)**: Wybierz typ podłączanego urządzenia z listy rozwijanej. Typ urządzenia to zależny od sterownika.
- **Device id (ID urządzenia)**: Wpisz ID lub adres podłączonego urządzenia PTZ. Adres można znaleźć w dokumentacji urządzenia.

Więcej informacji dotyczących sterowników PTZ: *Sterowniki PTZ na stronie 60*.

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.

PortNazwa: edytuj tekst, aby zmienić nazwę portu.**Direction (Kierunek)**:  oznacza, że port jest portem wejścia.  oznacza, że jest to port wyjścia. Jeśli port jest konfigurowalny, można kliknąć ikony, aby przełączać się między wejściem a wyjściem.**Normal state (Stan normalny)**: Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.**Current state (Bieżący stan)**: wyświetla bieżący stan portu. Wejście lub wyjście jest aktywowane w momencie zmiany bieżącego stanu na inny niż stan normalny. Obwód wejścia urządzenia jest otwarty po odłączeniu lub po doprowadzeniu napięcia powyżej 1 V DC.

Uwaga

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

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

Edge-to-edge

parowanie

Parowanie pozwala korzystać z kompatybilnego głośnika lub mikrofonu Axis w sieci tak, jakby były one wbudowanymi elementami kamery. Po sparowaniu głośnik sieciowy działa jako urządzenie audio, które umożliwia odtwarzanie klipów audio i przesyłanie dźwięku za pośrednictwem kamery. Mikrofon sieciowy zbiera dźwięki z otoczenia i udostępnia je jako urządzenie wejściowe audio, wykorzystywane w strumieniach multimediów i zapisach.

Ważne

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

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

Adres: Wprowadź nazwę hosta lub adres IP głośnika sieciowego.**Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika.**Hasło**: Wprowadź hasło dla użytkownika.**Speaker pairing (Parowanie głośnika)**: Wybranie tej opcji pozwala sparować głośnik sieciowy.**Microphone pairing (Parowanie mikrofonu)**  : Wybranie tej opcji pozwala sparować mikrofon. **Clear fields (Wyczyść pola)**: Kliknij, aby usunąć zawartość wszystkich pól.**Connect (Połącz)**: Kliknij tę opcję w celu nawiązania połączenia z głośnikiem lub mikrofonem.

Dzienniki

Raporty i dzienniki

Raporty

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

Dzienniki

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

Zdalny dziennik systemu

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

+ **Server (Serwer)**: Kliknij, aby dodać nowy serwer.**Host**: Wprowadź nazwę hosta lub adres IP serwera.**Format (Formatuj)**: Wybierz format komunikatu dziennika systemowego, który ma być używany.

- Axis
- RFC 3164
- RFC 5424

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

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

Port: Wpisywanie innego numeru portu w miejsce obecnego.**Severity (Ciężkość)**: Zdecyduj, które komunikaty będą wysyłane po wyzwoleniu.**CA certificate set (Certyfikat CA ustawiony)**: Umożliwia wyświetlenie aktualnych ustawień lub dodanie certyfikatu.

Zwykła konfiguracja

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

Konserwacja

Konserwacja

Restart (Uruchom ponownie): Uruchom ponownie urządzenie. Nie wpłynie to na żadne bieżące ustawienia. Uruchomione aplikacje zostaną ponownie uruchomione automatycznie.**Restore (Przywróć)**: Opcja ta umożliwia przywrócenie *większości* domyślnych ustawień fabrycznych. Następnie konieczne jest ponowne skonfigurowanie urządzeń i aplikacji, zainstalowanie aplikacji, które nie zostały wstępnie zainstalowane, a także ponowne utworzenie wszystkich zdarzeń i wstępnych ustawień.

Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

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

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

Uwaga

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

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

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

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

Rozwiązywanie problemów

Ping: Aby sprawdzić, czy określony adres jest dostępny dla urządzenia, wprowadź nazwę lub adres IP hosta, do którego chcesz wysłać polecenie ping, i kliknij **Start (Uruchom)**.**Port check (Kontrola portu)**: Aby zweryfikować łączność urządzenia z określonym adresem IP i portem TCP/UDP, wprowadź nazwę hosta lub adres IP i numer portu, które chcesz sprawdzić, a następnie kliknij **Start (Uruchom)**.**Ślad sieciowy**

Ważne

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

Plik śladu sieciowego, rejestrujący aktywność w sieci, może pomóc w rozwiązywaniu problemów. **Trace time (Czas śledzenia)**: Wybierz czas trwania śledzenia w sekundach lub minutach i kliknij przycisk **Download (Pobierz)**.

Więcej informacji

Palety kolorów

Zastosowanie palety kolorów ułatwi wzrokowe rozróżnianie szczegółów na obrazie termowizyjnym. Barwy te są sztucznie generowane, aby odzwierciedlać różnice temperatur.

Można wybrać jedną z palet zainstalowanych w produkcie. Jeżeli operator ogląda strumień wideo, może wybrać dowolną z palet. Jeżeli strumień wideo jest używany wyłącznie przez aplikacje, należy wybrać paletę „white-hot".

Nakładki

Nakładki są nakładane na strumień wideo. Służą one do dostarczania dodatkowych informacji podczas instalacji i konfiguracji produktu lub podczas rejestracji obrazu (np. znacznik czasowy). Można dodać tekst lub obraz.

Wskaźnik strumieniowania obrazu wideo jest innym typem nałożenia. Informuje on o tym, że strumień wideo transmitowany jest na żywo.

Strumieniowanie i pamięć masowa

Formaty kompresji obrazów wideo

O tym, która metoda kompresji ma być używana, należy zdecydować w zależności od wymagań dotyczących przeglądania i właściwości sieci. Dostępne są następujące opcje:

MJPEG

Uwaga

Aby zapewnić obsługę kodeka audio Opus, strumień MJPEG jest zawsze przesyłany przez RTP.

Motion JPEG (MJPEG), to cyfrowa sekwencja wideo składająca się z szeregu indywidualnych obrazów JPEG. Obrazy te są następnie wyświetlane i aktualizowane z szybkością odpowiednią do utworzenia strumienia pokazującego ciągle zaktualizowany ruch. Aby odbiorca miał wrażenie oglądania obrazu wideo, szybkość musi wynosić co najmniej 16 klatek obrazu na sekundę. Obraz jest odbierany jako ruchomy obraz wideo przy 30 (NTSC) lub 25 (PAL) klatkach na sekundę.

Strumień MJPEG wykorzystuje przepustowość w dużym stopniu, ale zapewnia doskonałą jakość obrazu i dostęp do wszystkich obrazów zawartych w strumieniu.

H.264 lub MPEG-4 Part 10/AVC

Uwaga

Kompresja H. 264 to licencjonowana technologia. W produkcie Axis znajduje się jedna licencja klienta do przeglądania obrazów w kompresji H.264. Nie wolno instalować dodatkowych kopii klienta bez licencji. Aby zakupić dodatkowe licencje, skontaktuj się z dystrybutorem Axis.

Dzięki kompresji H.264 można, bez uszczerbku na jakości, zmniejszyć rozmiar cyfrowego pliku wideo o ponad 80% w porównaniu z formatem MJPEG i nawet 50% w porównaniu ze starszymi formatami MPEG. Oznacza to, że w przypadku pliku wideo wymagana jest mniejsza przepustowość i mniej zasobów pamięci masowej. Inaczej mówiąc, dla danej przepływności bitowej można uzyskać obraz o wyższej jakości.

H.265 lub MPEG-H Part 2/HEVC

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

Więcej informacji

Uwaga

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

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

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

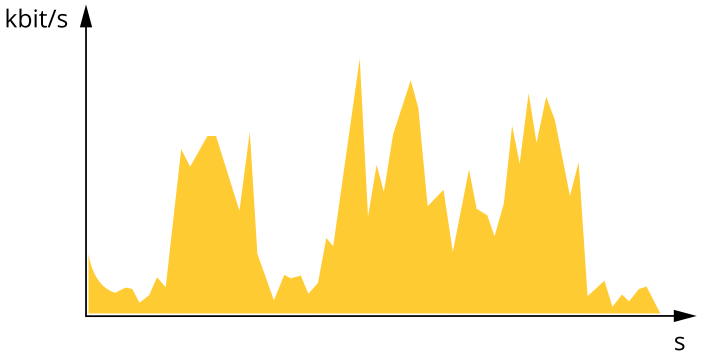
Karta **Strumień** zawiera ustawienia strumieni wideo. Te ustawienia są stosowane, gdy żądasz strumienia wideo z produktu, ale nie podasz na przykład rozdzielczości lub poklatkowości. Zmiana ustawień na karcie **Strumień** nie wpływa na bieżące strumienie, ale będzie wprowadzona po rozpoczęciu nowego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

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

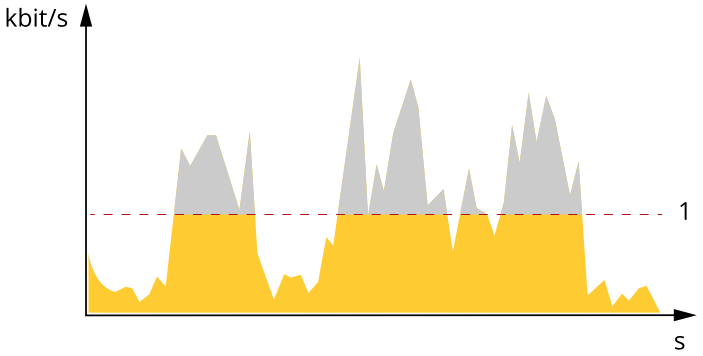
Sterowanie przepływnością bitową

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

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



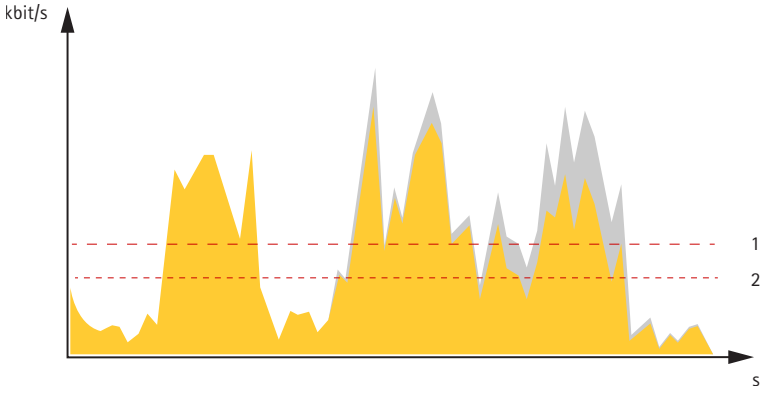
Maksymalna przepływność bitowa (MBR)
Opcja ta umożliwia ustawienie docelowej przepływności bitowej w celu kontrolowania zajętości pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości obrazu lub niższa poklatkowość. Jak priorytet można wybrać opcję ustawienia jakości obrazu lub poklatkowości. Zalecamy skonfigurowanie docelowej wartości przepływności bitowej na wartość większą niż oczekiwana. Dzięki temu można zachować margines, jeśli w scenie występuje wysoki poziom aktywności.



1 Docel. przepł. bitowa

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

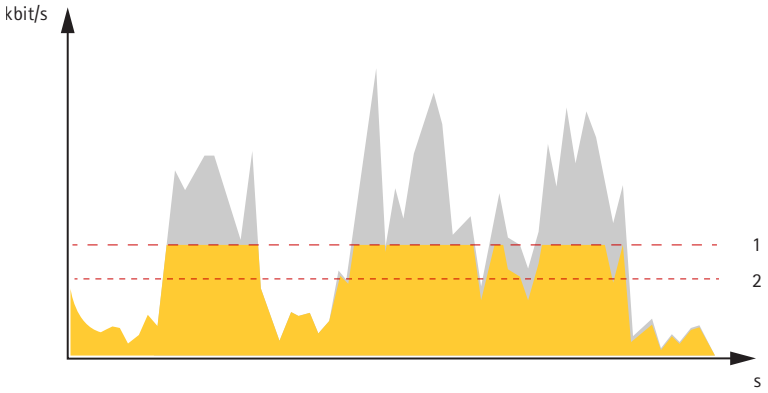
- Aby obliczyć przybliżone zapotrzebowanie na zasoby pamięci masowej, należy ustawić wartość docelową przepływności bitowej i czas retencji.
- Użyj kalkulatora przepływności bitowej, aby obliczyć średnią przepływność bitową w zależności od dostępnego miejsca w zasobach pamięci i czasu retencji.



1 Docel. przepł. bitowa
2 Rzeczywista średnia przepływność bitowa

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

Więcej informacji



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

Aplikacje

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

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

Uwaga

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

AXIS Perimeter Defender

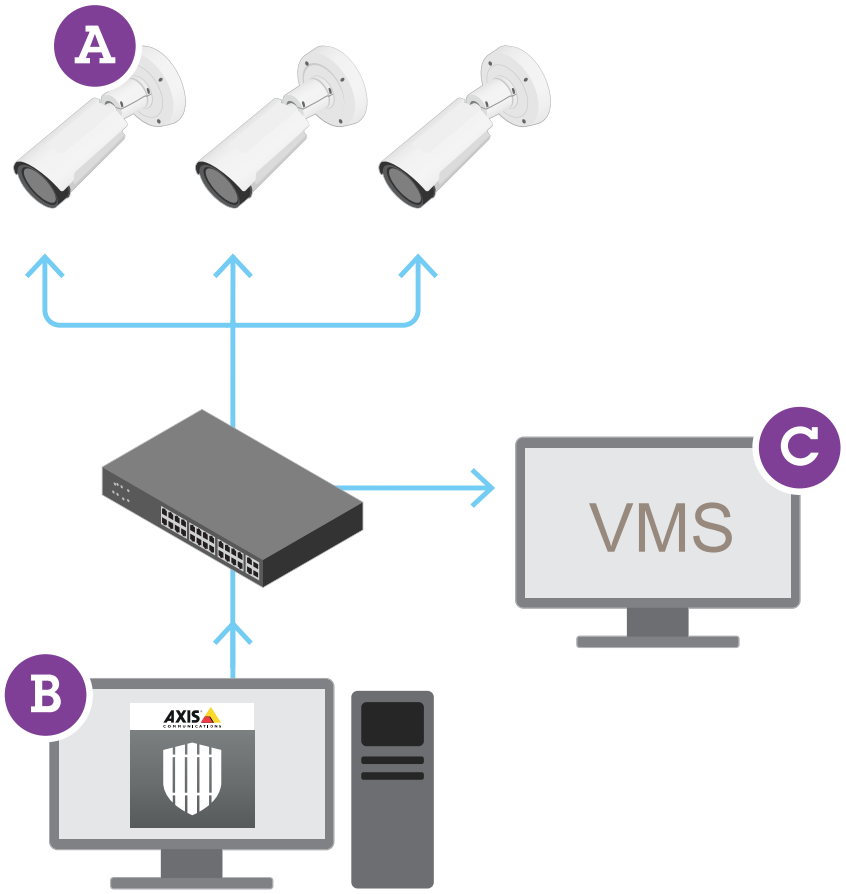
AXIS Perimeter Defender to aplikacja do dozoru i ochrony obwodowej. Nadaje się ona idealnie do ochrony obwodowej tam, gdzie konieczne jest wzmocnienie systemu fizycznej kontroli dostępu poprzez dodanie niezawodnej detekcji wtargnięcia na teren.

AXIS Perimeter Defender jest przeznaczona przed wszystkim do ochrony tak zwanej strefy sterylnej, na przykład strefy wzdłuż płotu stanowiącego granicę obszaru. Termin „strefa sterylna" odnosi się do obszaru, w którym nie powinni znaleźć się ludzie.

Aplikacji AXIS Perimeter Defender można używać na zewnątrz pomieszczeń i budynków, aby:

- wykrywać poruszające się osoby,
- wykrywać poruszające się pojazdy, bez względu na ich typ.

Więcej informacji



Kamera może włączać aplikację w trybie kalibracji, AI lub obu tych trybach jednocześnie. W przypadku uruchomienia aplikacji tylko w trybie AI montaż kamer jest bardziej elastyczny i nie trzeba ich kalibrować.

Aplikacja AXIS Perimeter Defender składa się z interfejsu (B) służącego do instalacji i konfiguracji aplikacji w kamerach (A). System można tak skonfigurować, aby wysyłał alarmy do oprogramowania do zarządzania materiałem wizyjnym (C).

AXIS Perimeter Defender PTZ Autotracking to wtyczka do aplikacji AXIS Perimeter Defender, która korzysta z tego samego interfejsu. Wtyczka ta umożliwia sparowanie stałopozycyjnej kamery optycznej lub termowizyjnej z kamerą PTZ z serii Axis Q. Można wówczas zachować ciągłą detekcję w scenie za pomocą kamery stałopozycyjnej, podczas gdy kamera PTZ zapewnia automatyczne śledzenie i zbliżenia wykrytych obiektów.

Ważne

Wtyczka AXIS Perimeter Defender PTZ Autotracking wymaga kalibracji zarówno kamer stałopozycyjnych, jak i PTZ.

AXIS Perimeter Defender zawiera następujące typy scenariuszy detekcji:

- **Intrusion (Wtargnięcie)**: wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu (dowolny kierunek i trajektoria).

- **Loitering (Podejrzanie zachowanie)**: wyzwala alarm, kiedy osoba lub pojazd pozostaje w strefie zdefiniowanej na podłożu przez czas dłuższy niż podana liczba sekund.
- **Zone-crossing (Przekroczenie strefy)**: wyzwala alarm, kiedy osoba lub pojazd przekracza w określonej kolejności dwie lub większą liczbę stref zdefiniowanych na podłożu.
- **Conditional (Warunkowy)**: wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu, nie przekraczając wcześniej innych zdefiniowanych na nim stref.

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisie produktu na stronie Axis.com.

Aby uzyskać szczegółowe informacje na temat cyberbezpieczeństwa w systemie AXIS OS, zapoznaj się z *przewodnikiem po zabezpieczeniach systemu operacyjnego AXIS OS*.

Axis Edge Vault

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Zawiera funkcje gwarantujące tożsamość i integralność urządzenia oraz ochronę poufnych informacji przed nieuprawnionym dostępem. Rozwiązanie to bazuje na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych.

Podpisany system operacyjny

Podpisany system operacyjny jest wdrażany przez dostawcę oprogramowania podpisującego obraz systemu AXIS OS za pomocą klucza prywatnego. Po dołączeniu podpisu do systemu operacyjnego urządzenie sprawdzi poprawność oprogramowania przed jego zainstalowaniem. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania, aktualizacja systemu AXIS OS zostanie odrzucona.

Bezpieczny start

Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego systemu operacyjnego bezpieczny rozruch gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem.

Bezpieczny magazyn kluczy

Jest to zabezpieczone przed sabotażem środowisko do ochrony kluczy prywatnych i bezpiecznego wykonywania operacji kryptograficznych. Zapobiega nieautoryzowanemu dostępowi i złośliwemu wykradaniu w przypadku włamania do systemu. W zależności od wymogów bezpieczeństwa urządzenie Axis może mieć jeden lub kilka sprzętowych modułów kryptograficznych, które udostępniają chroniony sprzętowo bezpieczny magazyn kluczy. W zależności od wymogów dotyczących zabezpieczeń urządzenie Axis może mieć jeden lub wiele sprzętowych kryptograficznych modułów obliczeniowych, takich jak TPM 2.0 (Trusted Platform Module) lub zabezpieczony element i/lub TEE (Trusted Execution Environment), które zapewniają ochronę sprzętową magazynu kluczy. Ponadto wybrane produkty Axis są wyposażone w bezpieczny magazyn kluczy z certyfikatem FIPS 140-2 poziomu 2.

Identyfikator urządzenia axis

możliwość zweryfikowania pochodzenia urządzenia jest kluczowa z perspektywy wiarygodności tożsamości urządzenia. Podczas produkcji urządzenia z rozwiązaniem Axis Edge Vault mają przypisywany unikatowy fabryczny i zgodny ze standardem IEEE 802.1AR certyfikat znany jako identyfikator urządzenia Axis. Jest on swego rodzaju paszportem, który potwierdza pochodzenie urządzenia. Identyfikator urządzenia jest bezpiecznie i trwale przechowywany w bezpiecznym magazynie kluczy w postaci certyfikatu podpisanego za pomocą certyfikatu głównego Axis. ID urządzenia może być wykorzystywany przez infrastrukturę IT klienta do zautomatyzowanego bezpiecznego wdrażania urządzeń i bezpiecznej identyfikacji urządzeń.

Podpisany materiał wizyjny

podpis dodany do materiału wizyjnego umożliwia potwierdzenie autentyczności dowodowej bez konieczności potwierdzenia całego łańcucha pochodzenia pliku wideo. Każda kamera podpisuje materiał wizyjny za pomocą własnego unikatowego klucza, który jest

bezpiecznie przechowywany w bezpiecznym magazynie kluczy. W trakcie odtwarzania wideo program odtwarzający informuje o tym, czy materiał jest nienaruszony. Podpisany materiał wizyjny umożliwia ustalenie, z której kamery materiał pochodzi, i wykrycie ewentualnych nieuprawnionych modyfikacji wprowadzonych w materiale po tym, jak opuścił on kamerę.

Zaszyfrowany system plików

Bezpieczny magazyn kluczy zapobiega złośliwemu wyprowadzaniu danych i manipulowaniu konfiguracją przez wymuszanie silnego szyfrowania systemu plików. Zapewnia to, że żadne dane przechowywane w systemie plików nie mogą zostać pobrane ani naruszone, gdy urządzenie Axis nie jest używane, uzyskano do niego nieautoryzowany dostęp i/lub zostało skradzione. Podczas bezpiecznego rozruchu system plików z uprawnieniami odczytu/zapisu jest odszyfrowywany, po czym można go zamontować i używać na urządzeniu Axis.

Aby dowiedzieć się więcej o funkcjach cyberbezpieczeństwa stosowanych w urządzeniach Axis, przejdź do strony *axis.com/learning/white-papers* i poszukaj według hasła „cybersecurity".

Usługa powiadomień w systemach zabezpieczeń Axis

Axis świadczy usługę powiadamiania z informacjami o lukach w zabezpieczeniach i innych sprawach dotyczących bezpieczeństwa urządzeń Axis. Aby otrzymywać powiadomienia, możesz aktywować subskrypcję na stronie *axis.com/security-notification-service*.

Postępowanie z lukami w zabezpieczeniach

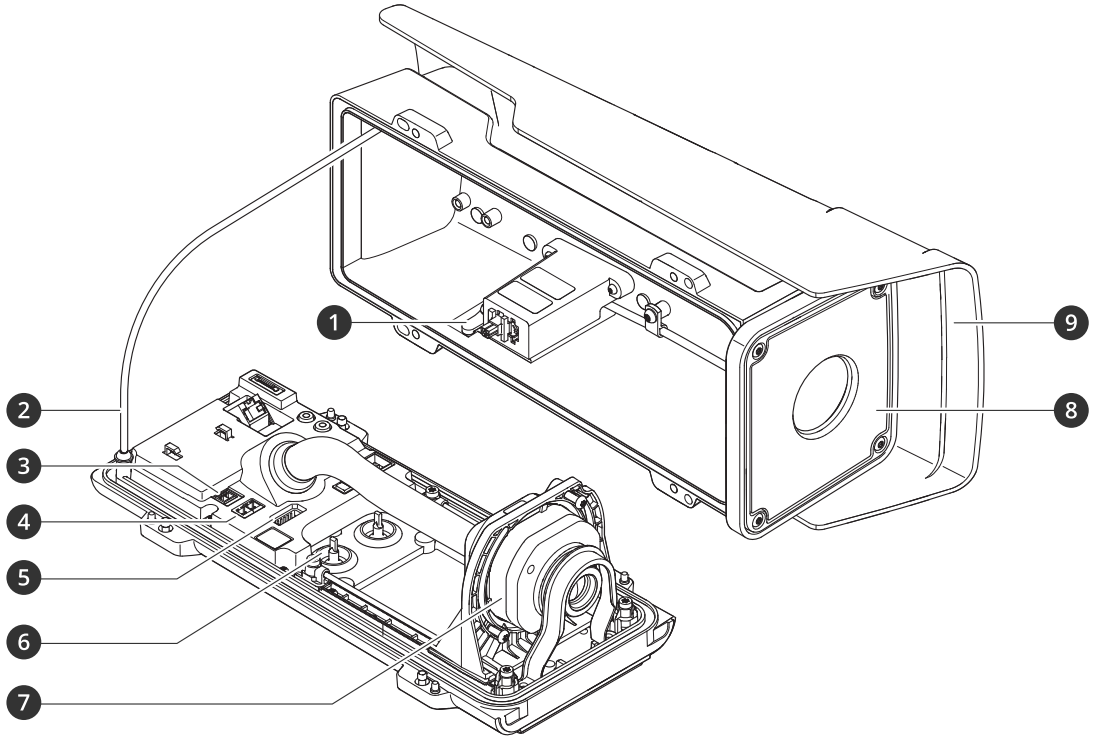
Aby maksymalnie ograniczyć narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania w takich przypadkach. Aby uzyskać więcej informacji na temat zasad zarządzania lukami w zabezpieczeniach rozwiązań Axis, sposobu zgłaszania luk w zabezpieczeniach, wykrytych luk w zabezpieczeniach i odpowiednich porad dotyczących bezpieczeństwa, zob. *axis.com/vulnerability-management*.

Bezpieczne działanie urządzeń Axis

Urządzenia Axis z domyślnymi ustawieniami fabrycznymi są wstępnie skonfigurowane z zabezpieczonymi domyślnymi mechanizmami ochrony. Zalecamy korzystanie z lepiej zabezpieczonej konfiguracji podczas instalowania urządzenia. Więcej o przewodnikach Axis dotyczących zabezpieczeń i innej dokumentacji związanej z cyberbezpieczeństwem można znaleźć na stronie *axis.com/support/cybersecurity/resources*.

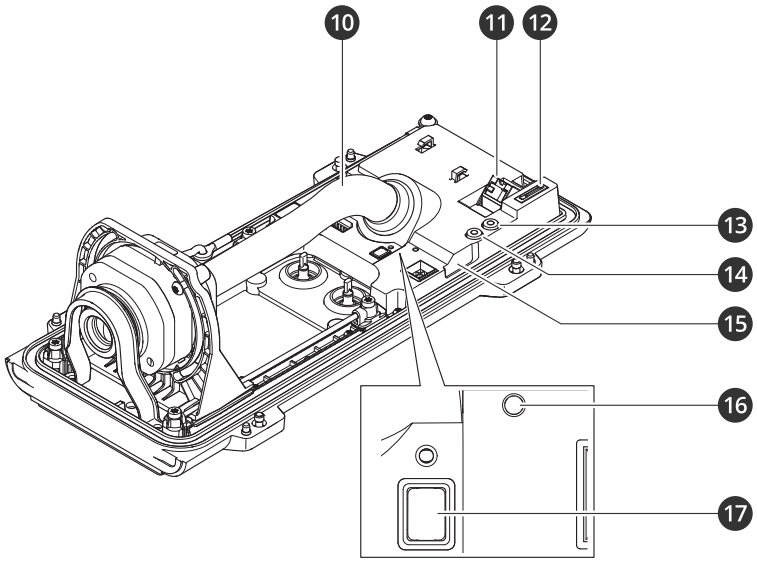
Specyfikacje

Przegląd produktów



1 *Magnes alarmu wtargnięć*
2 *Przewód bezpieczeństwa*
3 *Złącze zasilania*
4 *Złącze RS485/422*
5 *Złącze I/O*
6 *Uszczelka kabla M20 (2x)*
7 *Jednostka optyczna**
8 *Przednia szybka*
9 *Osłona chroniąca przed wpływem warunków atmosferycznych*

*Wygląd jednostki optycznej może się różnić w zależności od wybranego wariantu obiektywu.



10 Osłona kabla
11 Złącze sieciowe (PoE)
12 Gniazdo kart microSD
13 Wyjście audio
14 Wejście audio
15 Czujnik alarmu wtargnięć
16 Dioda stanu
17 Przycisk kontrolny

Wskaźniki LED

Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.
- Wskaźniki LED wyłączają się po zamknięciu obudowy.

Dioda stanu	Wskazanie
Zgaszony	Połączenie i normalne działanie.
Zielony	Połączenie i normalne działanie.
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.
Czerwony	Błąd aktualizacji oprogramowania urządzenia.

Brzęczyk

Brzęczyk asystenta poziomowania

Aby uzyskać informacje na temat przycisku kontrolnego służącego do poziomowania obrazu, zobacz *strona 57*.

Brzęczyk	Umiejscowienie kamery
Dźwięk stały	Poziom
Szybkie sygnały dźwiękowe	Blisko poziomu
Średnie sygnały dźwiękowe	Brak poziomu
Wolne sygnały dźwiękowe	Całkowity brak poziomu

Gniazdo karty SD

POWIADOMIENIE

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

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

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

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

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 65*.
- Upewniania się, że kamera jest zamontowana poziomo. Naciśnij przycisk i przytrzymaj go przez nie więcej niż dwie sekundy, aby uruchomić asystenta poziomowania; naciśnij przycisk ponownie, aby wyłączyć asystenta. Sygnał brzęczyka (patrz *strona 57*) ułatwiający poziomowanie kamery. Kamera jest zamontowana poziomo, kiedy brzęczyk nie wyłącza się.

Złącza

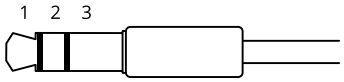
Złącze sieciowe

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

Złącze audio

- **Wejście audio** – wejście 3,5 mm dla mikrofonu cyfrowego, analogowego mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).
- **Wyjście audio** – wyjście audio 3,5 mm (poziom linii), które można podłączyć do systemu nagłośnienia (PA) lub aktywnego głośnika z wbudowanym wzmacniaczem. Do wyjścia audio musi być użyte złącze stereo.

Specyfikacje



Wejście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Niezbalansowany mikrofon (z zasilaniem elektretowym lub bez) lub wejście liniowe	Zasilanie elektretowe po wybraniu	Masa
Sygnał cyfrowy	Zasilanie z obwodu pierścieniowego po wybraniu	Masa

Wyjście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Kanał 1, wejście liniowe niezbalansowane, mono	Kanał 1, wejście liniowe niezbalansowane, mono	Masa

Złącze I/O

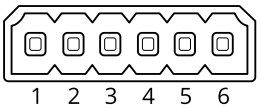
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

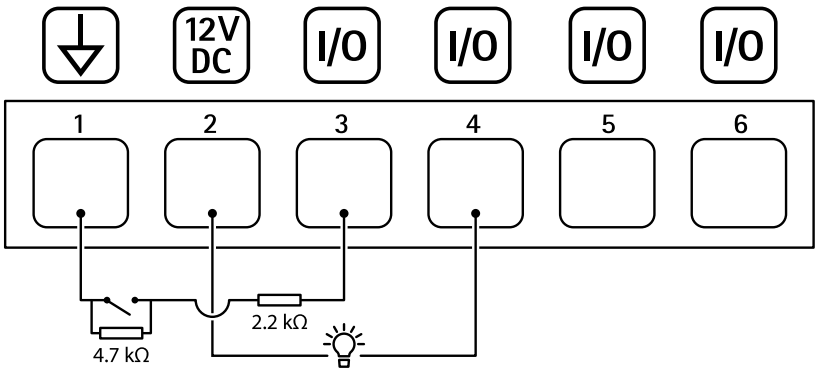
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

6-pinowego bloku złączy



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

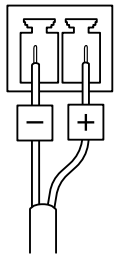
Przykład:



1 *Masa DC*
2 *Wyjście DC 12 V, maks. 50 mA*
3 *I/O skonfigurowane jako wejście nadzorowane*
4 *We/Wy skonfigurowane jako wyjście*
5 *Konfigurowalne We/Wy*
6 *Konfigurowalne We/Wy*

Złącze zasilania

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

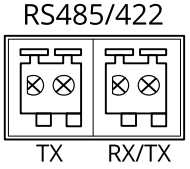


Złącze RS485/RS422

Dwa 2-stykowe bloki złączy interfejsu szeregowego RS485/RS422

Port szeregowy można skonfigurować do obsługi następujących funkcji:

- RS485 half duplex (dwużyłowy)
- RS485 full duplex (czterożyłowy)
- Dwuprzewodowy RS422 simplex
- Czteroprzewodowy RS422 full duplex do komunikacji P2P



Funkcje	Uwagi
RS485/RS422 TX(A)	Para TX do RS422 i 4-przewodowego RS485
RS485/RS422 TX(B)	
RS485A alt RS485/422 RX(A)	Para RX dla wszystkich trybów (połączone RX/TX dla 2-przewodowego RS485)
RS485B alt RS485/422 RX(B)	

Uwaga

Aby używać kamery wraz z AXIS T99 Positioning Unit, podłącz ją so RS485A i RS485B (RX/TX).

Sterowniki PTZ

APTP

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele z interfejsem RS485 2-wire:

- Moduły pozycjonujące z serii AXIS T99A.

  Informacje o zgodnych produktach Axis można znaleźć na stronie *axis.com*.

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	APTP
Wersja	1.1.0

Domyślna konfiguracja seryjna:

Portmode	RS485
BaudRate	115200
DataBits	8
StopBits	1
Parity	Brak

DOMYŚLNIE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	tak	tak	tak
Pochylenie	tak	tak	tak

Pelco

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	Pelco
Wersja	4.17

Domyślna konfiguracja seryjna:

Portmode	RS485
BaudRate	2400
DataBits	8
StopBits	1
Parity	Brak

DOMYŚLNIE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	nie	tak	tak
Pochylenie	nie	tak	tak

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Zoom	nie	tak	tak
Ostrość	nie	tak	tak
Przysłona	nie	tak	tak

AutoIris	tak
AutoFocus	tak
IrCutFilter	nie
BackLight	tak
OSDMenu	tak

Visca

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele z interfejsem RS422 4-wire:

- Sony EVI-D70/D70P
- WISKA DCP-27 (PT-head)

Obsługiwane modele z interfejsem RS232 (może być konieczny zewnętrzny przetwornik RS422-4-wire/RS232):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	Visca/EVI
Wersja	4.11

Domyślna konfiguracja seryjna:

Portmode	RS422
BaudRate	9600
DataBits	8
StopBits	1
Parity	Brak

Specyfikacje

DOMYŚLNIE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	tak	tak	tak
Pochylenie	tak	tak	tak
Zoom	tak	tak	tak
Ostrość	tak	tak	tak
Przysłona	tak	tak	nie

AutoIris	tak
AutoFocus	tak
IrCutFilter	tak
BackLight	tak
OSDMenu	nie

Czyszczenie urządzenia

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

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
- Nie należy rozpylać detergentu bezpośrednio na urządzenie. Detergent należy najpierw nanieść na miękką ściereczkę, a następnie przetrzeć nią urządzenie.
- Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawanie plam na obudowie.

1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
2. W razie potrzeby można wyczyść urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą i łagodnym mydłem niezawierającym środków ściernych.
3. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

Przywracanie domyślnych ustawień fabrycznych należy stosować rozważnie. Opcja resetowania do domyślnych ustawień fabrycznych powoduje przywrócenie wszystkich domyślnych ustawień fabrycznych produktu, włącznie z adresem IP.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów na stronie 55*.
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)**.

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

- 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*.

Problemy techniczne, wskazówki i rozwiązania

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

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

Problemy z ustawieniem adresu IP	
Urządzenie należy do innej podsieci	Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsieci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
Adres IP jest używany przez inne urządzenie	Odłącz urządzenie Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia): • Jeśli otrzymasz odpowiedź: `Reply from <adres IP>: bytes=32; time=10...` oznacza to, że dany adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie. • Jeśli otrzymasz odpowiedź: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Rozwiązywanie problemów –

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 *Przywróć domyślne ustawienia fabryczne na stronie 65*.
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 multicast w kodowaniu H.264	Poproś administratora sieci, aby sprawdził, czy adresy strumienia multicast używane przez urządzenie Axis są prawidłowe dla danej sieci.Poproś administratora sieci, aby sprawdził, czy 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.
Liczba klatek na sekundę jest mniejsza od oczekiwanej	• Patrz *Kwestie wydajności na stronie 68*. • 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. • Maksymalna liczba klatek na sekundę zależy od częstotliwości roboczej (60/50 Hz) urządzenia Axis.
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.

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.
- Używanie palet kolorów wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.

Kontakt z pomocą techniczną

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

Podręcznik użytkownika
AXIS Q21 Thermal Camera Series

Wer. M2.4
Data: Luty 2025
Nr katalogowy T10208523