Seria kamer sieciowych AXIS M31

AXIS M3115-LVE Network Camera
AXIS M3116-LVE Network Camera

Podręcznik użytkownika

Spis treści

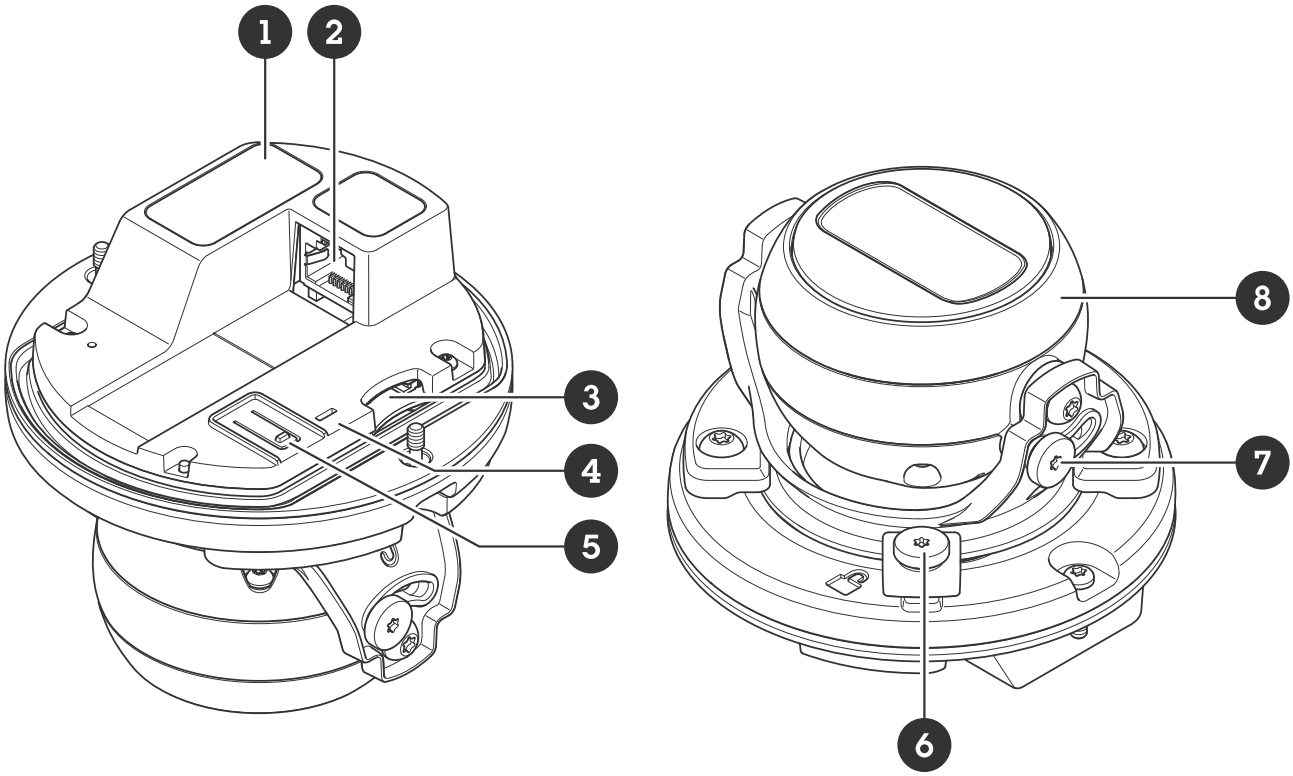
Informacje dotyczące tej instrukcji 4
Przegląd produktów 5
....5
Wyszukiwanie urządzenia w sieci 6
Obsługiwane przeglądarki 6
Otwórz stronę WWW urządzenia. 7
Ustawianie nowego hasła do konta root 7
Bezpieczne hasła 7
Konfiguracja urządzenia 8
Wygląd strony internetowej 8
Potrzebujesz więcej pomocy? 8
Jakość obrazu 8
Wybór trybu ekspozycji 8
Korzystanie z oświetlenia IR w warunkach słabego oświetlenia (tryb nocny) 8
Redukcja szumu w warunkach słabego oświetlenia 9
Zmniejszanie rozmycia obiektów w ruchu w warunkach słabego oświetlenia 9
Maksymalizacja szczegółów obrazu 9
Rejestracja w scenach z jasnym podświetleniem 10
Monitorowanie długich i wąskich obszarów 10
Sprawdzanie rozdzielczości pikseli 11
Obszar obserwacji 11
Maski prywatności 11
Ukrywanie części obrazu za pomocą masek prywatności 12
Nakładki 12
Wyświetlanie nałożenia tekstu w strumieniu wideo, gdy urządzenie wykryje obiekt 12
Strumieniowanie i pamięć masowa 13
Sterowanie przepływnością bitową 13
Formaty kompresji obrazów wideo 14
Zmniejszanie zapotrzebowania na przepustowość i zasób 15
Konfiguracja zasobów sieciowej pamięci masowej 15
W jaki sposób ustawienia obrazu, strumienia i profilu strumienia mogą na siebie wpływać? 16
Rejestracja i odtwarzanie obrazu 16
Konfiguracja reguł dotyczących zdarzeń 16
Wyzwalanie akcji 16
Rejestrowanie obrazu wideo w momencie wykrycia obiektu 16
Automatyczne przesyłanie wiadomości e-mail w przypadku zamalowania obiektywu farbą w sprayu 17
Aplikacje 17
Aplikacje 17
AXIS People Counter 18
Rozwiązywanie problemów – 20
Przywróć domyślne ustawienia fabryczne 20
Opcje oprogramowania sprzętowego 20
Sprawdzanie bieżącej wersji oprogramowania sprzętowego 20
Aktualizacja oprogramowania sprzętowego 21
Problemy techniczne, wskazówki i rozwiązania 21
Kwestie wydajności 23
Interfejs urządzenia 25
....25
....25
Status 25
Nagranie wideo 26
Instalacja 27

Zdjęcie 27
Strumień 34
Nakładki 37
Obszary obserwacji 38
Maski prywatności 38
Nagrania 38
Aplikacje 39
..... 39
System 40
Data i godzina 40
Sieć 40
Bezpieczeństwo 43
Użytkownicy 46
Zdarzenia 46
MQTT 51
Przechowywanie 53
SIP 55
Profile strumienia 59
ONVIF 59
Metadane analityczne 60
Detektory 61
Dzienniki 61
Zwykła konfiguracja 62
Konserwacja 63
Specyfikacje 64
Wskaźniki LED 64
Gniazdo karty SD 64
Przyciski 64
Przycisk kontrolny 64
Złącza 64
Złącze sieciowe 64

Informacje dotyczące tej instrukcji

W niniejszej instrukcji opisano różne produkty. Oznacza to, że może ona zawierać instrukcje, które nie dotyczą danego produktu.

Przegląd produktów



1 *Numer części (P/N) i numer seryjny (S/N)*
2 *Złącze sieciowe (PoE)*
3 *Gniazdo karty SD*
4 *Wskaźnik LED stanu*
5 *Przycisk kontrolny*
6 *Śruba blokująca panoramowanie*
7 *Śruba blokująca pochylenie*

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 stronę 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. Jeżeli uzyskujesz dostęp do urządzenia po raz pierwszy, musisz ustawić hasło root. Patrz .

Ustawianie nowego hasła do konta root

Domyślną nazwą użytkownika - administratora jest `root`. Konto root nie ma domyślnego hasła. Trzeba je ustawić przy pierwszym logowaniu do urządzenia.

1. Wprowadź hasło. Postępuj zgodnie z instrukcjami dotyczącymi bezpieczeństwa haseł. Patrz .
2. Wprowadź ponownie hasło, aby sprawdzić, czy jest ono poprawnie zapisane.
3. Kliknij **Add user (Dodaj użytkownika)**.

Ważne

Jeżeli zapomnisz hasła do konta root, przejdź do sekcji i postępuj zgodnie z instrukcjami.

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.

Konfiguracja urządzenia

Wygląd strony internetowej

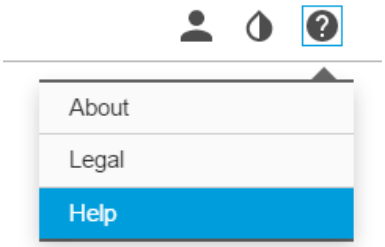
To wideo przybliża najważniejsze elementy i schemat działania interfejsu urządzenia.



Interfejs WWW urządzenia Axis

Potrzebujesz więcej pomocy?

Dostęp do wbudowanej pomocy można uzyskać z poziomu strony WWW urządzenia. Pomoc zawiera bardziej szczegółowe informacje na temat funkcji urządzenia i ich ustawień.



Jakość obrazu

Wybór trybu ekspozycji

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

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

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

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

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

Redukcja szumu w warunkach słabego oświetlenia

Aby zmniejszyć szum w warunkach słabego oświetlenia, można dostosować jedno lub więcej następujących ustawień:

- Regulacja stosunku rozmycia ruchu do szumu. Przejdź do menu **Video > Image > Exposure (Wideo > Obraz > Ekspozycja)** i przesuń suwak **Blur-noise trade-off** (Stosunek rozmycia do szumu) na **Low noise (niski poziom szumu)**.
- Automatyczny tryb ekspozycji.

Uwaga

Wysoka maksymalna wartość migawki może skutkować rozmyciem obiektów w ruchu.

- Aby zmniejszyć prędkość migawki, ustaw wartość maksymalną na najwyższą.
- Jeżeli to możliwe, otwórz aperturę.
- Zmniejsz ostrość obrazu, przechodząc do menu **Video > Image > Appearance (Wideo > Obraz > Wygląd)**.

Zmniejszanie rozmycia obiektów w ruchu w warunkach słabego oświetlenia

Aby zmniejszyć rozmycie obiektów w ruchu w warunkach słabego oświetlenia, można dostosować jedno lub więcej następujących ustawień w menu **Video > Image > Exposure (Wideo > Obraz > Ekspozycja)**:

- Przesuń suwak **Blur-noise trade-off (Stosunek rozmycia do szumu)** w stronę opcji **Low motion blur (Małe rozmycie obiektów w ruchu)**.

Uwaga

Szum zwiększy się w przypadku zwiększenia wzmocnienia.

- Ustaw **Max shutter (Maks. czas migawki)** na niższą wartość, a **Max gain (Maks. wzmocnienie)** na wyższą wartość.

Jeżeli problemy z rozmyciem ruchu są nadal widoczne:

- Zwiększ poziom oświetlenia w scenie.
- Zamontuj kamerę tak, aby obiekty poruszały się w jej kierunku lub przeciwnie, ale nie w poprzek.

Maksymalizacja szczegółów obrazu

Ważne

Po zmaksymalizowaniu szczegółów na obrazie prawdopodobnie wzrośnie przepływność bitowa, a poklatkowość obniży się.

- Wybierz tryb rejestracji o najwyższej rozdzielczości.
- Przejdź do okna **Video > Stream > General (Wideo > Strumień > Ogólne)** i ustaw jak najmniejszą kompresję.
- Poniżej obrazu z podglądu na żywo kliknij , a następnie w ustawieniu **Video format (Format wideo)** zaznacz wartość **MJPEG**.
- Przejdź do okna **Video > Stream > H.264 and H.265 encoding > Zipstream (Wideo > Strumień > Kodowanie w formacie H.264 i H.265 > Zipstream)** i wybierz opcję **Off (Wył)**.

Rejestracja w scenach z jasnym podświetleniem

Zakres dynamiki to różnica w poziomie oświetlenia na obrazie. W niektórych przypadkach różnica pomiędzy najciemniejszymi a najjaśniejszymi obszarami może być bardzo duża. W wyniku tego otrzymujemy obraz, na którym nie widać ani jasnych, ani ciemnych obszarów. Szeroki zakres dynamiki (WDR) służy do wyświetlenia jasnych i ciemnych obszarów na obrazie.



Obraz bez WDR.



Obraz z WDR.

Uwaga

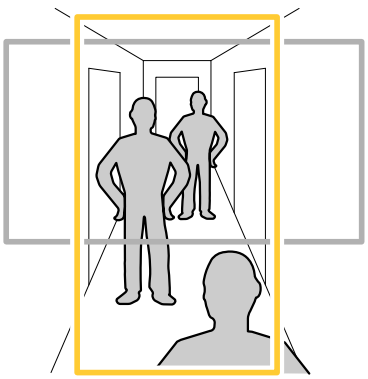
- WDR może powodować występowanie artefaktów na obrazie.
- Funkcja WDR może nie być dostępna dla wszystkich trybów rejestracji.

1. Przejdź do menu **Video > Image > Wide dynamic range (Wideo > Obraz > Szeroki zakres dynamiki)**.
2. Włącz WDR.
3. Użyj suwaka **Local contrast (Kontrast lokalny)**, aby dostosować poziom WDR.
4. Jeżeli nadal występują problemy, przejdź do menu **Exposure (Ekspozycja)** i ustaw **Exposure zone (Strefę ekspozycji)**tak, by pokrywała się z obszarem zainteresowania.

Więcej informacji o funkcji WDR i sposobie jej wykorzystania znajduje się na stronie *axis.com/web-articles/wdr*.

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.

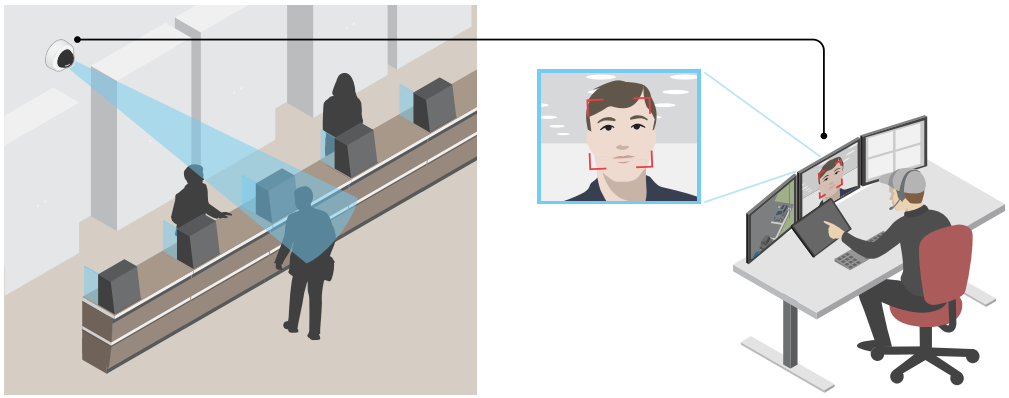


1. W zależności od urządzenia, obróć kamerę lub obiektyw trójosiowy Axis o 90° lub 270°.

2. Jeżeli urządzenie nie ma funkcji automatycznego obrotu widoku, przejdź do okna **Video > Installation (Wideo > Instalacja)**.
3. Obróć widok o 90° lub 270°.

Sprawdzanie rozdzielczości pikseli

Aby sprawdzić, czy zdefiniowana część obrazu zawiera wystarczającą liczbę pikseli, aby na przykład rozpoznać twarz osoby, można użyć licznika pikseli.



1. Przejdź do menu **Video (Wideo) > Image (Obraz)** i kliknij .
2. Kliknij , aby wyświetlić **Pixel counter (Licznik pikseli)**.
3. Dostosuj rozmiar i pozycję prostokąta w podglądzie na żywo kamery, na przykład tak, by obejmował miejsce, w którym mogą pojawić się twarze.
   Możesz zobaczyć liczbę pikseli każdej ze stron prostokąta i zdecydować, czy wartości są wystarczające dla Twoich potrzeb.

Obszar obserwacji

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

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

Maski prywatności

Maska prywatności to obszar zdefiniowany przez użytkownika, który uniemożliwia podgląd części monitorowanego obszaru. Maski prywatności wyświetlane są jako nieprzezroczyste elementy na strumieniu wideo.

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

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

Ważne

Dodanie wielu masek prywatności może wpłynąć na pracę urządzenia.

Można utworzyć kilka masek prywatności. Maksymalna liczba masek zależy od złożoności wszystkich masek razem wziętych. Czym więcej punktów kotwiczenia ma każda maska, tym mniej masek można będzie utworzyć. Każda maska może mieć od 3 do 10 punktów kotwiczenia.

Ukrywanie części obrazu za pomocą masek prywatności

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

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

Patrz także

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.

Wyświetlanie nałożenia tekstu w strumieniu wideo, gdy urządzenie wykryje obiekt

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

1. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
2. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

Dodaj nałożenie tekstu:

1. Wybierz kolejno opcje **Video > Overlays (Wideo > Nakładki)**.
2. W obszarze **Overlays (Nałożenia)** zaznacz opcję **Text (Tekst)** i kliknij + .
3. W polu tekstowym wpisz `#D`.
4. Wybierz rozmiar i wygląd tekstu.
5. Aby umieścić nałożenie tekstowe, kliknij i wybierz opcję.

Create a rule (Utwórz regułę):

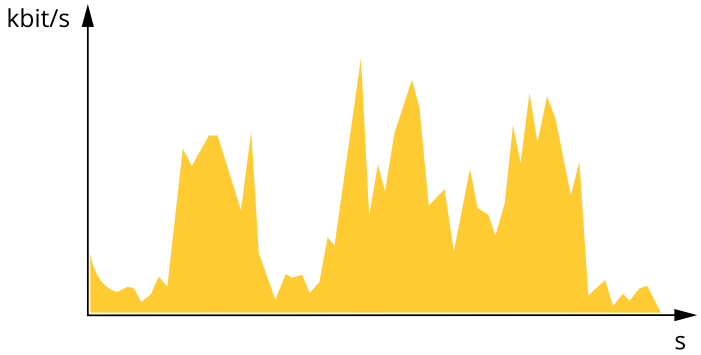
1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Na liście akcji w obszarze **Overlay text (Nałożony tekst)** wybierz opcję **Use overlay text (Użyj nałożonego tekstu)**.
4. Wybierz kanał wideo.
5. W polu **Text (Tekst)** wpisz „Motion detected" (Wykryto ruch).
6. Ustaw czas trwania.
7. Kliknij przycisk **Zapisz**.

Strumieniowanie i pamięć masowa

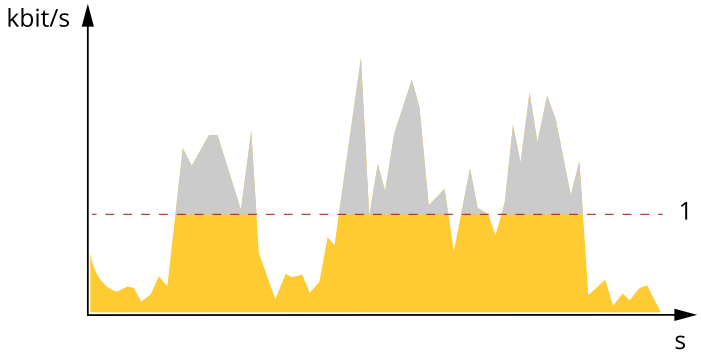
Sterowanie przepływnością bitową

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

Variable bitrate (VBR) (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.



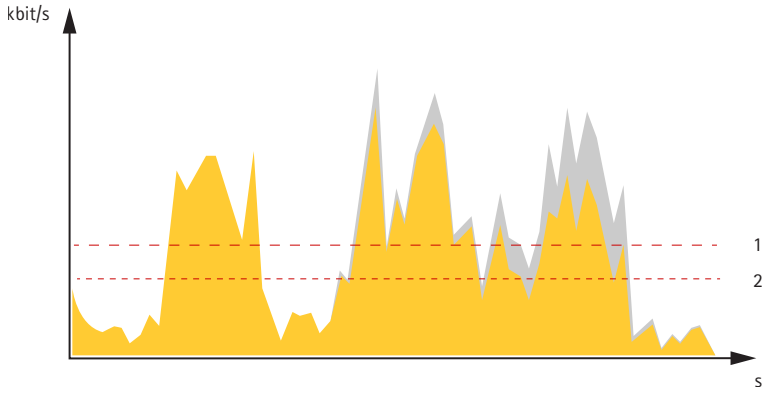
Maximum bitrate (MBR) (Maksymalna przepływność bitowa, MBR) Opcja ta umożliwia ustawienie docelowej przepływności bitowej, aby kontrolować zajętość pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości obrazu lub niższa poklatkowość. Jak priorytet 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

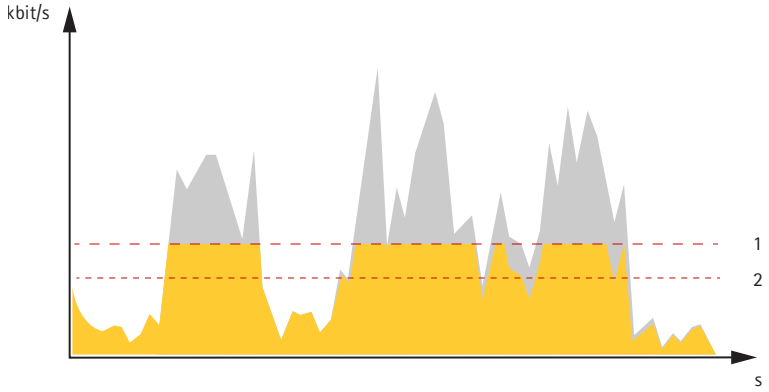
Average bitrate (ABR) (Średnia przepływność bitowa, ABR)Średnia przepływność bitowa jest dostosowywana automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak najlepszą jakość obrazu wideo przy dostępnych zasobach pamięci masowej. Przepływność bitowa jest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

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



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

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



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

Formaty kompresji obrazów wideo

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

MJPEG

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

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

H.264 lub MPEG-4 Part 10/AVC

Uwaga

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

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

H.265 lub MPEG-H Part 2/HEVC

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

Uwaga

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

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. W ustawieniu **Video format (Format wideo)** wybierz wartość **H.264**.
4. Przejdź do okna **Video > Stream > General (Wideo > Strumień > Ogólne)** i zwiększ wartość w polu **Compression (Kompresja)**.
5. Przejdź do okna **Video > Stream > H.264 and H.265 encoding (Wideo > Strumień > Kodowanie w formacie H.264 i H.265)** i wykonaj co najmniej jedną z następujących czynności:
   - W ustawieniu **Zipstream** wybierz poziom, którego chcesz używać.

     Uwaga

     Ustawienia **Zipstream** będą używane zarówno w kompresji H.264, jak i H.265.
   - 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 even if connection fails (Dodaj udział nawet w razie awarii połączenia)**.
8. Kliknij **Dodaj**.

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**.

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 zasobów sieciowej pamięci masowej, zobacz
3. Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

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

Konfiguracja reguł dotyczących zdarzeń

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).

Wyzwalanie akcji

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

Uwaga

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

Rejestrowanie obrazu wideo w momencie wykrycia obiektu

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

Zanim zaczniesz:

- Upewnij się, że karta SD została zainstalowana.

1. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
2. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy akcji w obszarze **Recordings (Zapisy)** wybierz opcję **Record video while the rule is active (Rejestruj wideo, gdy reguła jest aktywna)**.
4. Z listy opcji pamięci masowej wybierz opcję **SD_DISK**.
5. Wybierz kamerę i profil strumienia.
6. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
7. Ustaw czas buforowania po zdarzeniu na 1 minutę.
8. 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 czas **Trigger after (Wyzwalaj po)**. Wartość ta wskazuje czas, jaki musi upłynąć przed wysłaniem wiadomości e-mail.
3. Włącz opcję **Trigger on dark images (Wyzwalaj przy ciemnych obrazach)**, aby wykrywać, czy obiektyw stracił znacząco ostrość lub został zamalowany albo zakryty.

Dodaj odbiorcę wiadomości e-mail:

4. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
5. Wprowadź nazwę odbiorcy.
6. Wybierz adres**E-mail**.
7. Wprowadź adres e-mail odbiorcy.
8. 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.
9. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
10. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

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

Aplikacje

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. Więcej informacji o dostępnych aplikacjach, oprogramowaniu do pobrania, wersjach próbnych i licencjach znajduje się na stronie *axis.com/products/acap/application-gallery*.

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.



Pobieranie i instalowanie aplikacji

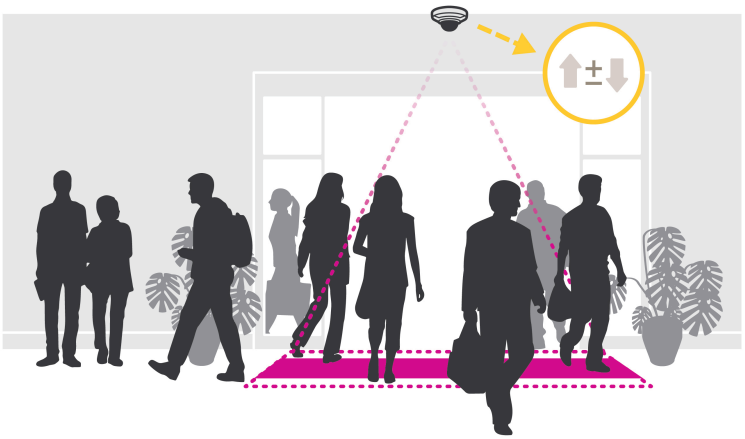


Włączanie aktywacji kodu licencji aplikacji na urządzeniu

AXIS People Counter

AXIS People Counter to aplikacja do analizy, którą można instalować w kamerze sieciowej. Za pomocą aplikacji można policzyć, ile osób przechodzi przez wejście, w jakim kierunku i czy w określonym przedziale czasu przechodzi więcej niż jedna osoba. Możesz również użyć tej aplikacji do oszacowania, ile osób aktualnie przebywa na danym obszarze oraz jaki jest średni czas odwiedzin.

Aplikacja jest wbudowana w kamerę, więc do jej uruchomienia nie jest potrzebny oddzielny komputer. AXIS People Counter nadaje się do każdego rodzaju wnętrz, takich jak sklepy, biblioteki czy siłownie.



Jak działa funkcja szacowania zajętości?

Za pomocą aplikacji można oszacować zajętość w obszarach z jednym lub kilkoma wejściami i wyjściami. Każde wejście i wyjście musi być wyposażone w kamerę sieciową z zainstalowanym licznikiem AXIS People Counter. Jeśli zainstalowano kilka kamer, komunikują się one ze sobą z wykorzystaniem sieci na zasadzie kamery głównej i kamer podrzędnych. Kamera główna przez cały czas pobiera dane od kamer podrzędnych i wyświetla je

w podglądzie na żywo. Co piętnaście minut kamera główna wysyła dane statystyczne do aplikacji AXIS Store Data Manager. W efekcie raporty wygenerowane w aplikacji AXIS Store Data Manager mogą prezentować dane w co najmniej 15-minutowych odstępach.

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

⚠ OSTRZEŻENIE

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

Ważne

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

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz .
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeżeli w sieci nie jest dostępny serwer DHCP, domyślny adres IP to `192.168.0.90`.
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
   Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej *axis.com/support*.

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

Opcje oprogramowania sprzętowego

Axis oferuje zarządzanie oprogramowaniem sprzętowym 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 oprogramowania sprzętowego 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 sprzętowego Axis znajdują się na stronie *axis.com/support/firmware*.

Sprawdzanie bieżącej wersji oprogramowania sprzętowego

Oprogramowanie sprzętowe określa dostępne funkcje urządzeń sieciowych. Podczas rozwiązywania problemów zalecamy rozpoczęcie od sprawdzenia aktualnej wersji oprogramowania sprzętowego. Najnowsza wersja może zawierać poprawki, które rozwiążą problem.

Sprawdzanie bieżącej wersji oprogramowania sprzętowego:

1. Przejdź do interfejsu urządzenia i wybierz opcję **Status**.
2. Przejdź do menu **Device info (Informacje o urządzeniu)** i sprawdź nr wersji oprogramowania sprzętowego.

Aktualizacja oprogramowania sprzętowego

Ważne

- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania sprzętowego (pod warunkiem, że funkcje te są dostępne w nowym oprogramowaniu sprzętowym), 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 oprogramowania sprzętowego umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania sprzętowego zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony *axis.com/support/firmware*, aby znaleźć najnowszą wersję oprogramowania sprzętowego oraz informacje o wersji.

1. Pobierz na komputer plik oprogramowania sprzętowego dostępny bezpłatnie na stronie *axis.com/support/firmware*.
2. Zaloguj się do urządzenia jako administrator.
3. Wybierz kolejno opcje **Maintenance > Firmware upgrade (Konserwacja > Aktualizacja oprogramowania sprzętowego)** > **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 aktualizacją oprogramowania sprzętowego	
Niepowodzenie podczas aktualizacji oprogramowania sprzętowego	Jeśli aktualizacja oprogramowania sprzętowego zakończy się niepowodzeniem, urządzenie załaduje ponownie poprzednią wersję oprogramowania sprzętowego. Najczęstszą przyczyną tego jest wczytanie niewłaściwego oprogramowania sprzętowego. Upewnij się, że nazwa pliku oprogramowania sprzętowego odpowiada danemu urządzeniu i spróbuj ponownie.
Problemy po aktualizacji oprogramowania sprzętowego	Jeśli wystąpią problemy po aktualizacji oprogramowania sprzętowego, 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. Wprowadź polecenie ping (w oknie poleceń Uruchamianie / DOS wpisz `ping` wraz z adresem IP urządzenia): • Jeżeli zostanie zwrócony komunikat: `Reply from <IP address>: bytes=32; time=10...` (Odpowiedź z...), oznacza to, że adres IP może być zajęty przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie. • Jeżeli zostanie zwrócony komunikat: `Request timed out` (Upłynął limit czasu żądania), oznacza to, że adres IP jest dostępny i może zostać przypisany do urządzenia Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Nie można uzyskać dostępu do urządzenia przez przeglądarkę

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

Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

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

- AXIS Companion: bezpłatna aplikacja, idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station: 30-dniowa bezpłatna wersja próbna, idealna do małych i średnich systemów.

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

Problemy z przesyłaniem strumieniowym

Strumień multicast w kodowaniu H.264 jest dostępny wyłącznie dla lokalnych klientów	Sprawdź, czy router obsługuje technologię multicasting lub czy trzeba skonfigurować ustawienia routera w kliencie i urządzeniu. Może być konieczne zwiększenie wartości TTL (Time To Live), czyli czasu do rejestracji na żywo.
W kliencie nie można wyświetlić strumienia	Poproś administratora sieci, aby sprawdził, czy adresy strumienia multicast używane przez urządzenie Axis są prawidłowe dla danej sieci.

multicast w kodowaniu H.264	Poproś administratora sieci, aby sprawdził, czy zapora nie powoduje blokowania strumienia.
Niedostateczne renderowanie obrazów w kompresji H.264	Sprawdź, czy karta graficzna ma zainstalowany najnowszy sterownik. Zazwyczaj najnowsze sterowniki można pobrać z witryny internetowej producenta.
Strumienie H.264 i MJPEG mają różną saturację barw	Zmień ustawienia karty graficznej. Więcej informacji można znaleźć w dokumentacji karty.
Liczba klatek na sekundę jest mniejsza od oczekiwanej	• Patrz . • Zmniejsz liczbę aplikacji uruchomionych na komputerze klienta. • Ogranicz liczbę dozorców mogących oglądać obraz jednocześnie. • Poproś administratora sieci, aby sprawdził, czy dostępna jest wystarczająca przepustowość. • Zmniejsz rozdzielczość obrazu. • Zaloguj się na stronie internetowej urządzenia i ustaw tryb rejestracji, w którym liczba klatek na sekundę ma priorytet. Zmiana trybu rejestracji, aby nadawał priorytet liczbie klatek na sekundę, może obniżyć rozdzielczość w zależności od używanego urządzenia i dostępnych trybów rejestracji. • 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.

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 do dużej liczby klientów MJPEG lub H.264 unicast wpływa na przepustowość.
- Dostęp do dużej liczby klientów MJPEG lub H.265 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 MJPEG i H.264 wpływa na liczbę klatek na sekundę i przepustowość.
- Jednoczesny dostęp do strumieni wideo MJPEG i H.265 wpływa na liczbę klatek na sekundę i przepustowość.
- 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.

Interfejs urządzenia

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

Uwaga

Obsługa funkcji i ustawień opisanych w tym rozdziale różni się w zależności od urządzenia.

Wyświetl/ukryj menu główne.

Uzyskaj dostęp do pomocy dotyczącej produktu.

Zmień język.

Ustaw jasny lub ciemny motyw.

Menu użytkownika zawiera opcje:

- Informacje o zalogowanym użytkowniku.
- **Change user** (Zmień użytkownika): Ta opcja umożliwia wylogowanie bieżącego użytkownika i zalogowanie nowego użytkownika.
- **Log out (Wyloguj się)**: Ta opcja umożliwia wylogowanie bieżącego użytkownika.

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)**: ta opcja pokazuje informacje o urządzeniu, w tym wersję oprogramowania sprzętowego i numer seryjny.
- **Interfejs starszego urządzenia**: Zmień interfejs urządzenia na starszą wersję.

Status

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): Kliknij, aby przejść do strony Date and time (Data i godzina), gdzie można zmienić ustawienia usługi NTP.

Informacje o urządzeniu

Tutaj znajdziesz informacje o urządzeniu, w tym wersję oprogramowania sprzętowego i numer seryjny.

Upgrade firmware (Aktualizuj oprogramowanie sprzętowe): Kliknij, aby przejść do strony Maintenance (Konserwacja), gdzie można wykonać aktualizację oprogramowania sprzętowego.

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 obrazu to [snapshot_RRRR_MM_DD_GG_MM_SS.jpg]. Rozmiar pliku zależy od kompresji zastosowanej w przeglądarce internetowej, do której przysyłane jest ujęcie, więc może 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.

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 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.

- **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.

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.

Zdjęcie

Wygląd

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

- **Do celów dochodzenia**: Nadaje się na potrzeby dozoru.
- **Indoor (Do montażu wewnątrz budynków)** : Nadaje się do wnętrz budynków.
- **Outdoor (Do montażu na zewnątrz)** : Nadaje się do miejsc poza budynkami.
- **Vivid (Żywe kolory)**: Nadaje się do prezentacji.
- **Podgląd ruchu drogowego**: Nadaje się do monitorowania ruchu pojazdów.

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



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



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



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



Szeroki zakres dynamiki

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

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

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

Równoważenie bieli

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

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

Light environment (Środowisko oświetlenia):

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

Tryb dzień/noc

IR-cut filter (Filtr odcinający promieniowanie IR):

- **Automatycznie**: Zaznaczenie tej opcji spowoduje automatyczne włączanie i wyłączanie filtr odcinającego promieniowanie IR. W trybie dziennym filtr odcinający promieniowanie IR jest włączony i blokuje promieniowanie podczerwone; w trybie nocnym jest on wyłączany, co powoduje zwiększenie światłoczułości kamery.
- **On (Wł.)**: Zaznacz tę opcję, aby włączyć filtr odcinający promieniowanie podczerwone. Obraz jest kolorowy, ale przy znacznie ograniczonej światłoczułości.
- **Off (Wyłączona)**: Zaznacz tę opcję, aby wyłączyć filtr odcinający promieniowanie podczerwone. Obraz jest czarno-biały w celu zwiększenia światłoczułości.

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

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

Promieniowanie IR

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

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

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

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

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

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

Światło białe

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

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

Ekspozycja

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

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

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

Uwaga

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

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

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

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

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

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

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

Uwaga

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

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

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

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

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

Uwaga

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

Strumień

Zapisy ogólne

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

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

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.

H.26x encoding (Kodowanie w formacie H.26x)

Zipstream: 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 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*.

Wybierz żądany poziom zmniejszania przepływności:

- **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): istnieje możliwość zoptymalizowania zapisu strumienia poprzez ograniczenie przepływności przy jednoczesnym zachowaniu jakości materiału. Optymalizacja nie ma zastosowania do strumienia wyświetlanego w kliencie sieciowym. 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.

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.

Bitrate control (Kontrola przepływności bitowej):

- **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.

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 czy liczbę klatek na sekundę.
  - : kliknij, aby dodać modyfikator daty `%F` wyświetlający datę w formacie rrrr-mm-dd.
  - : kliknij, aby dodać modyfikator czasu `%X` wyświetlający czas 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 wyświetlenie 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.
- **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.

Obszary obserwacji

: Kliknij, aby utworzyć obszar obserwacji.

Kliknij obszar obserwacji, aby przejść do ustawień.

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

Aspect ratio (Współczynnik proporcji): Wybierz żądany współczynnik proporcji. Rozdzielczość dostosuje się automatycznie.

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

Maski prywatności

: Kliknij, aby utworzyć nową maskę prywatności. Maksymalna liczba masek zależy od złożoności wszystkich masek razem wziętych. Każda maska może mieć maksymalnie 10 punktów kotwiczenia.

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.

Nagrania

Kliknij, aby filtrować nagrania.

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

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

Source (Źródło): Pokazuje nagrania z podziałem na źródła.

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

Pamięć masowa: Pokazuje nagrania z podziałem na typy zasobów.

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

Wybierz, aby rozpocząć zapis na kamerze.

Wybierz docelowy zasób, w którym chcesz zapisać nagrania.

Wybierz, aby zatrzymać zapis na kamerze.

Uruchomione zapisy zostaną zakończone zarówno po zatrzymaniu ręcznym, jak i po zamknięciu kamery.

Zapis ciągły będzie kontynuowane do momentu zatrzymania ręcznego. Jeśli kamera zostanie zamknięta, zapis będzie kontynuowany po ponownym uruchomieniu kamery.

Kliknij, aby odtworzyć nagranie.

Kliknij, aby zatrzymać odtwarzanie zapisu.

Kliknij, aby wyświetlić więcej informacji i opcji dla nagrania.

Set export range (Ustaw zakres eksportu): Jeżeli chcesz wyeksportować tylko część nagrania, określ początek i koniec przedziału czasu.

Kliknij, aby usunąć nagranie.

Export (Eksportuj): Kliknij, aby wyeksportować nagranie lub jego część.

Aplikacje

Add app (Dodaj aplikację): Kliknij tę opcję, aby zainstalować nową aplikację.

Find more apps (Znajdź więcej aplikacji): Kliknij tę opcje, aby przejść na stronę informacji o aplikacjach Axis.

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

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): Kliknij, aby otworzyć ustawienia 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)**: Kliknij tę opcję, aby wyświetlić informacje o licencjach open source używanych w aplikacji.
- **App log (Dziennik aplikacji)**: Kliknij tę opcję, aby 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)**: Dezaktywuj licencję, aby korzystać z niej w innym urządzeniu. Jeśli dezaktywujesz licencję, zostanie ona również usunięta z urządzenia. Do dezaktywowania licencji konieczne jest połączenie internetowe.
- **Ustawienia**: Ta opcja umożliwia konfigurowanie parametrów.
- **Usuń**: Ta opcja powoduje trwałe usunięcie aplikacji z urządzenia. Jeśli najpierw nie dezaktywujesz licencji, pozostanie ona aktywna.

System

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

Synchronization (Synchronizacja): Wybierz opcję synchronizacji daty i godziny na urządzeniu.

- **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.
- **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.
- **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.
- **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.

Uwaga

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

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.

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. Nazwa hosta jest wykorzystywana w raportach serwera oraz w logach systemowych. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

Serwery DNS

Przypisz automatycznie DNS: Wybierz ustawienie, aby router sieciowy 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

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

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.

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. Dozwolony jest port 80 lub dowolny port z zakresu 1024–65535. Jeżeli użytkownik jest zalogowany jako administrator, może również wprowadzić dowolny port z zakresu 1 - 1023. Użycie portu z tego zakresu powoduje wyświetlenie ostrzeżenia.

HTTPS port (Port HTTPS): wprowadź wykorzystywany port HTTPS. Dozwolony jest port 443 lub dowolny port z zakresu 1024–65535. Jeżeli użytkownik jest zalogowany jako administrator, może również wprowadzić dowolny port z zakresu 1 - 1023. Użycie portu z tego zakresu powoduje wyświetlenie ostrzeżenia.

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.

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):

- **One-click** (Jedno kliknięcie): ustawienie domyślne. 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 urządzenia można skonfigurować komunikaty Trap dla protokołu SNMP v1 i v2c. Komunikaty Trap są automatycznie wyłączane w przypadku zmiany na SNMP v3 lub wyłączenia protokołu SNMP. Jeżeli używasz SNMP v3, możesz skonfigurować komunikaty Trap 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 korzystać z protokołu SNMP v3, należy uaktywnić protokół HTTPS, ponieważ hasło zostanie przesłane za pośrednictwem protokołu HTTPS. Zapobiegnie to również dostępowi osób nieupoważnionych do nieszyfrowanych komunikatów Trap 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.

Podłączone klienty

View details (Wyświetl szczegóły): kliknij, aby wyświetlić wszystkie klienty podłączone do urządzenia.

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.

Filtrowanie certyfikatów na liście.

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

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.

IEEE 802.1x

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

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

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.

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

CA certificate (Certyfikat CA): wybierz certyfikat 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.

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.

IP address filter (Filtr adresów IP)

Use filter (Użyj filtra): wybierz, aby filtrować adresy IP, które mogą uzyskiwać dostęp do urządzenia.

Policy (Zasada): wybierz opcję **Allow (Zezwalaj)** lub **Deny (Nie zezwalaj)** na dostęp do określonych adresów IP.

Addresses (Adresy): Wprowadź adresy IP, które mają lub nie mają dostępu do urządzeń. Możesz również użyć formatu CIDR.

Certyfikat oprogramowania sprzętowego z niestandardowym podpisem

Do zainstalowania w urządzeniu testowego oprogramowania sprzętowego lub innego niestandardowego oprogramowania Axis konieczny jest niestandardowy certyfikat producenta. Certyfikat służy do sprawdzenia, czy oprogramowanie sprzętowe jest zatwierdzone zarówno przez właściciela urządzenia, jak i przez firmę Axis. Oprogramowanie układowe może działać tylko w określonym urządzeniu identyfikowanym na podstawie niepowtarzalnego numeru seryjnego i identyfikatora chipu. Certyfikaty oprogramowania układowego podpisane przez użytkownika są tworzone wyłącznie przez firmę Axis, ponieważ firma Axis posiada klucz do ich podpisywania.

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

Użytkownicy

Add user (Dodaj użytkownika): Aby utworzyć nowego użytkownika, kliknij ikonę. Można dodać do 100 użytkowników.

Username (Nazwa użytkownika): Wprowadź unikatową nazwę użytkownika.

Nowe hasło: Wprowadź hasło dla użytkownika. Hasło musi mieć 1–64 znaki. Dozwolone są tylko drukowalne 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 innych użytkowników.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
  - Dodawanie aplikacji.
- **Viewer (Dozorca)**: Może:
  - Oglądać strumienie wideo i robić z nich migawki.
  - Oglądać i eksportować nagrania.
  - Z dostępem dla użytkownika PTZ: wykonywać obrót, pochylenie i zoom.

Menu kontekstowe zawiera opcje:

Update user (Aktualizuj użytkownika): Pozwala edytować właściwości użytkownika.

Delete user (Usuń użytkownika): Umożliwia usunięcie użytkownika. Nie można usunąć użytkownika głównego.

Anonymous users (Anonimowi użytkownicy)

Allow anonymous viewers (Zezwalaj na anonimowych dozorców): Włączenie tej opcji pozwala wszystkim osobom uzyskać dostęp do urządzenia jako dozorca bez logowania się za pomocą konta użytkownika.

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

Zdarzenia

Reguły

Reguła określa warunki, jakie muszą zostać spełnione, aby urządzenie wykonało dane działanie. Na liście znajdują się wszystkie reguły skonfigurowane w produkcie.

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Kliknij, aby utworzyć 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. 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. W ten sposób 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. 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. 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 udziału 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. W ten sposób 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 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.

Wyzwalacz ręczny

Wyzwalacz ręczny służy do ręcznego wyzwalania reguły. Wyzwalacza ręcznego 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 sprzętowym urządzeń Axis może ułatwiać integrację danych i zdarzeń generowanych w urządzeniu z systemami, które nie są systemami 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*.

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.

Status (Stan): pokazuje bieżący status klienta MQTT.

Broker

Host: wprowadź nazwę hosta lub adres IP serwera MQTT.

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

Port: Wprowadź numer portu.

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

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.

Keep alive interval (Przedział czasowy KeepAlive): przedział czasowy KeepAlive umożliwia klientowi wykrywanie, 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.

Przechowywanie

Sieciowa pamięć masowa

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

- **Adres**: Wprowadź adres IP lub nazwę serwera hosta. Zazwyczaj jest nim NAS (sieciowy zasób dyskowy). Zalecamy skonfigurowanie hosta tak, aby używał stałego adresu IP (nie DHCP, ponieważ dynamiczne adresy IP mogą się zmienić) albo używanie DNS. Nazwy Windows SMB/CIFS nie są obsługiwane.
- **Network share (Udział sieciowy)**: Podaj nazwę współdzielonego udziału na serwerze hosta. Z jednego udziału sieciowego może korzystać kilka urządzeń Axis, ponieważ każde z nich ma swój folder.
- **User (Użytkownik)**: Jeżeli serwer wymaga logowania, wprowadź nazwę użytkownika. W celu zalogowania się do konkretnego serwera domeny wpisz `DOMAIN\username`.
- **Hasło**: Jeżeli serwer wymaga logowania, podaj hasło.
- **SMB version (Wersja SMB)**: Wybierz wersję protokołu pamięci masowej SMB, który będzie używany do łączenia z sieciowym zasobem dyskowym. Jeżeli wybierzesz opcję **Auto (Automatycznie)**, urządzenie będzie próbowało użyć jednej z bezpiecznych wersji protokołu SMB: 3.02, 3.0 lub 2.1. Wybierz opcję 1.0 lub 2.0, aby łączyć ze starszymi sieciowymi zasobami dyskowymi, które nie obsługują wyższych wersji. Więcej informacji o obsłudze protokołu SMB w urządzeniach Axis znajdziesz *tutaj*.
- **Add share even if connection test fails (Dodaj udział nawet wtedy, gdy test połączenia zakończy się niepowodzeniem)**: 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 usunięcia połączenia z udziałem sieciowym. Spowoduje to usunięcie wszystkich ustawień 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.

Ignore (Ignoruj): Włącz tę opcję, aby zaprzestać przechowywania nagrań w udziale sieciowym.

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 sieciowej pamięci masowej spowoduje usunięcie starych nagrań przed upływem wybranego czasu.

Narzędzia

- **Test connection (Test połączenia)**: Opcja ta służy do sprawdzenia połączenia z udziałem sieciowym.
- **Format (Formatuj)**: Polecenie to umożliwia sformatowanie udziału sieciowego, na przykład w razie potrzeby szybkiego usunięcia wszystkich danych. Dostępna opcja dla systemu plików to cifs.

Kliknij polecenie **Use tool (Użyj narzędzia)**, aby aktywować zaznaczone 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 nagrania mają być przechowywane, aby ograniczyć liczbę starych nagrań lub ze względu na zachowanie zgodności z regulacjami w sprawie przechowywania danych. Zapełnienie karty SD spowoduje usunięcie starych nagrań przed upływem wybranego czasu.

Narzędzia

- **Check (Sprawdź)**: Opcja ta umożliwia wykrycie błędów na karcie SD. Jest to możliwe tylko w systemie plików ext4.
- **Napraw**: Opcja ta umożliwia naprawę błędów w systemie plików ext4. Aby naprawić kartę SD z systemem plików VFAT, należy wysunąć kartę SD, umieścić ją w czytniku kart komputera i przeprowadzić naprawę dysku.
- **Format (Formatuj)**: Sformatuj kartę SD na przykład, gdy chcesz zmienić system plików lub szybko usunąć wszystkie dane. Dostępne opcje systemu plików to VFAT i ext4. Zalecanym formatem jest ext4, ze względu na odporność na utratę danych w przypadku wysunięcia karty lub utraty zasilania. Niemniej w celu uzyskania dostępu do danych na karcie z systemu Windows® należy zainstalować sterownik lub aplikację ext4 innego producenta.
- **Encrypt (Szyfruj)**: To narzędzie umożliwia sformatowanie karty SD i włączenie szyfrowania. Polecenie **Encrypt (Szyfruj)** powoduje usunięcie wszystkich danych znajdujących się na karcie SD. Po użyciu polecenia **Encrypt (Szyfruj)** dane przechowywane na karcie SD są chronione poprzez zaszyfrowanie.
- **Decrypt (Odszyfruj)**: To narzędzie pozwala sformatować kartę SD bez szyfrowania. Polecenie **Decrypt (Odszyfruj)** powoduje usunięcie wszystkich danych znajdujących się na karcie SD. Po użyciu polecenia **Decrypt (Szyfruj)** dane przechowywane na karcie SD nie są chronione poprzez zaszyfrowanie.
- **Change password (Zmień hasło)**: Umożliwia zmianę hasła wymaganego do szyfrowania karty SD.

Kliknij polecenie **Use tool (Użyj narzędzia)**, aby aktywować zaznaczone 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.

SIP

SIP settings (Ustawienia SIP)

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

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

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

Obsługa połączeń

- **Call timeout (Limit czasu wywołania)**: Ustaw maksymalny czas połączenia w przypadku braku odpowiedzi (maks. 10 minut).
- **Incoming call duration (Czas trwania rozmowy przychodzącej)**: ustaw maksymalny czas trwania połączenia przychodzącego (maks. 10 min).
- **End calls after (Zakończ połączenie po)**: Ustaw maksymalny czas trwania połączenia (maks. 60 min). Zaznacz opcję **Infinite call duration (Nieskończony czas trwania połączenia)**, jeśli nie chcesz ograniczać długości połączenia.

Porty

Numer portu musi należeć do przedziału od 1024 do 65535.

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

NAT Transversal

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

Uwaga

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

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

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

Dźwięk i obraz wideo

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

Uwaga

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

- **Audio direction (Kierunek dźwięku)**: Wybierz dozwolone kierunki dźwięku.

- **H.264 packetization mode (Tryb pakietyzacji H.264)**: Wybierz tryb pakietyzacji, który ma być używany.
  - **Automatycznie**: (Zalecany) Urządzenie decyduje o wyborze trybu pakietyzacji.
  - **Brak**: Nie jest określony żaden konkretny tryb pakietyzacji. To ustawienie często jest interpretowane jako tryb **0**.
  - **0**: Tryb bez przeplotu.
  - **1**: Tryb pojedynczej jednostki NAL.
- **Kierunek obrazu wideo**: Wybierz dozwolone kierunki obrazu filmowego.

Dodatkowe

- **UDP-to-TCP switching (Przełączanie UDP–TCP)**: Wybierz, aby umożliwić tymczasowe przełączenie protokołu transmisji z UDP (User Datagram Protocol) na TCP (Transmission Control Protocol). Przełączanie przydaje się w celu uniknięcia fragmentacji; przełączenie jest możliwe w zakresie 200 bajtów MTU lub więcej niż 1300 bajtów MTU.
- **Allow via rewrite (Umożliwiaj przepisanie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Allow contact rewrite (Umożliwiaj przepisanie przy kontakcie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Register with server every (Rejestruj na serwerze co)**: Ustaw częstotliwość rejestrowania się urządzenia na serwerze SIP dla istniejących kont SIP.
- **DTMF payload type (Typ próbki DTMF)**: Zmienia domyślny typ próbki na DTMF.

SIP accounts (Konta SIP)

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

• Konto zostało zarejestrowane na serwerze SIP.
● Wystąpił problem z kontem. Możliwe przyczyny: błąd autoryzacji, nieprawidłowe dane uwierzytelniające konta lub brak konta SIP wyszukiwanego przez serwer.

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

+ **Account** (Konto): Kliknij, aby utworzyć nowe konto SIP.

- **Active (Aktywne)**: wybierz tę opcję, aby użyć tego konta.
- **Ustaw jako domyślne**: zaznacz tę opcję, aby ustawić konto jako domyślne. Konto domyślne jest wymagane; można ustawić tylko jedno konto jako domyślne.
- **Nazwa**: Wprowadź nazwę opisową. Może to być na przykład imię i nazwisko, rola lub lokalizacja. Nazwa nie musi być unikalna.
- **User ID (ID użytkownika)**: Wprowadź numer wewnętrzny lub numer telefonu przypisany do urządzenia.
- **Peer-to-peer**: służy do wykonywania bezpośrednich połączeń z innym urządzeniem SIP w sieci lokalnej.
- **Zarejestrowane**: służy do wykonywania połączeń z urządzeniami SIP spoza sieci lokalnej (przez serwer SIP).
- **Domain (Domena)**: jeśli to możliwe, wprowadź nazwę publicznej domeny. Będzie ona wyświetlana jako część adresu SIP podczas wywoływania innych kont.
- **Hasło**: wprowadź hasło powiązane z kontem SIP, aby uwierzytelnić się na serwerze SIP.
- **Authentication ID (ID uwierzytelniania)**: wprowadź identyfikator uwierzytelnienia używany do uwierzytelniania na serwerze SIP. Jeśli jest on taki sam, jak identyfikator użytkownika, nie trzeba go wprowadzać.
- **Caller ID (ID rozmówcy)**: nazwa wyświetlana odbiorcom połączeń przychodzących z urządzenia.
- **Rejestrator**: wprowadź adres IP rejestratora.
- **Tryb transmisji**: Wybierz tryb transportowy SIP dla konta: UPD, TCP lub TLS. Po wybraniu TLS dostępna jest opcja korzystania z szyfrowania multimediów.
- **Media encryption (Szyfrowanie mediów)** (tylko w trybie TLS): wybierz rodzaj szyfrowania mediów (audio i wideo) w połączeniach SIP.
- **Certificate (Certyfikat)** (tylko w trybie TLS): Wybierz certyfikat.
- **Verify server certificate (Potwierdź certyfikat serwera)** (tylko w trybie TLS): zaznacz, aby potwierdzać certyfikat serwera.
- **Secondary SIP server (Dodatkowy serwer SIP)**: Włącz, aby w razie niepowodzenia rejestracji na głównym serwerze SIP urządzenie podjęło próbę rejestracji na serwerze dodatkowym.
- **Answer automatically (Odbierz automatycznie)**: wybierz tę opcję, aby automatycznie odbierać połączenia.
- **SIP secure (Bezpieczny SIP)**: wybierz tę opcję, aby użyć protokołu Secure Session Initiation Protocol (SIPS). Protokół SIPD wykorzystuje tryb transmisji TLS do szyfrowania ruchu.
- **Serwery proxy**
  - + **Proxy**: Kliknij, aby dodać serwer proxy.
  - **Prioritize (Nadaj priorytet)**: Po dodaniu dwóch lub więcej serwerów proxy kliknij, aby określić ich priorytet.

- **Server address (Adres serwera)**: Tu należy wprowadzić adres IP serwera proxy SIP.
- **Username (Nazwa użytkownika)**: wprowadź nazwę użytkownika serwera proxy SIP, jeśli to konieczne.
- **Hasło**: wprowadź hasło do serwera proxy SIP, jeśli to konieczne.

- **Nagranie wideo**
  - **View area (Obszar obserwacji)**: wybierz obszar obserwacji połączeń wideo. Jeśli nie zostanie wybrany obszar obserwacji, zostanie użyty widok natywny.
  - **Rozdzielczość**: wybierz rozdzielczość połączeń wideo. Rozdzielczość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **Frame rate (Liczba klatek na sekundę)**: wybierz liczbę klatek na sekundę w połączeniach wideo. Poklatkowość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **H.264 profile (Profil H.264)**: Wybierz profil połączeń wideo.
- **DTMF**
  - **Use RTP (RFC2833)** (Używaj RTP (RFC2833)): zaznacz, aby zezwolić na sygnalizację DTMF oraz inną sygnalizację telefoniczną w pakietach RTP.
  - **Use SIP INFO (RFC2976)** (Używaj SIP INFO (RFC2976)): zaznacz, aby uwzględnić metodę INFO w protokole SIP. Metoda INFO służy do dodania opcjonalnych informacji o warstwie, zazwyczaj powiązanych z sesją.
  - **DTMF sequence** (Sekwencja DTMF): Kliknij, aby dodać regułę akcji wyzwalaną przez sygnał wybierania. Regułę akcji należy aktywować na karcie **Events (Zdarzenia)**.
  - **Sequence (Sekwencja)**: Wprowadź znaki wyzwalające regułę akcji. Dozwolone znaki: 0–9, A–D, # oraz *.
  - **Description (Opis)**: Wprowadź opis akcji, która zostanie wyzwolona.

SIP test call (Połączenie testowe SIP)

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

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

Profile strumienia

Kliknij przycisk , aby utworzyć i zapisać grupy ustawień strumienia wizyjnego. Ustawień można używać w różnych sytuacjach, na przykład podczas ciągłego zapisu albo nagrywania przy użyciu reguł.

ONVIF

Użytkownicy 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 użytkownika ONVIF powoduje automatyczne włączenie komunikacji ONVIF. Nazwy użytkownika 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 user (Dodaj użytkownika): Kliknij, aby dodać nowego użytkownika ONVIF.

Username (Nazwa użytkownika): Wprowadź unikatową nazwę użytkownika.

Nowe hasło: Wprowadź hasło dla użytkownika. Hasło musi mieć 1–64 znaki. Dozwolone są tylko drukowalne 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 innych użytkowników.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
  - Dodawanie aplikacji.
- **Media user (Użytkownik mediów)**: Dostęp wyłącznie do strumienia wideo.

Menu kontekstowe zawiera opcje:

Update user (Aktualizuj użytkownika): Pozwala edytować właściwości użytkownika.

Delete user (Usuń użytkownika): Umożliwia usunięcie użytkownika. Nie można usunąć użytkownika głównego.

Profile mediów ONVIF

Profil mediów ONVIF składa się z zestawu konfiguracji, które można wykorzystać do zmiany ustawień strumienia mediów.

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

profile_x (Profil_x): kliknij profil do wyedytowania.

Metadane analityczne

Producenci metadanych

Na liście **Metadata producers (Producentów metadanych)** jest widoczna lista kanałów używanych przez aplikacje oraz metadane przesyłane strumieniowo z urządzenia.

Producer (Producent): Aplikacja generująca metadane.

Kanał: Kanał używany przez aplikację. Należy zaznaczyć to pole, aby włączyć strumień metadanych. Należy usunąć to zaznaczenie, aby wyłączyć strumień w celu zarządzania zgodnością lub zasobami.

Detektory

Sabotaż kamery

Gdy scena ulegnie zmianie, na przykład z powodu zasłonięcia obiektywu, spryskania go farbą lub znaczącego rozregulowania ostrości, to po upływie czasu określonego w ustawieniu **Trigger after (Wyzwól po)** 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 after (Wyzwól po): 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.

Dzienniki

Raporty i dzienniki

Raporty

- **Wyświetl raport serwera o urządzeniu**: Kliknij, aby wyświetlić status produktu w oknie wyskakującym. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.
- **Download the device server report (Pobierz raport serwera o urządzeniu)**: Kliknij i pobierz raport serwera. 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)**: Kliknij w celu pobrania 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.

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

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.

- RFC 3164
- RFC 5424

Protocol (Protokół): Wybierz protokół i port, które mają być używane:

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

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

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 PTZ.

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

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 sprzętowego firmy Axis posiadają podpisy cyfrowe zapewniające, że na urządzeniu będzie instalowane wyłącznie zweryfikowane oprogramowanie sprzętowe. To dodatkowo zwiększa minimalny ogólny poziom cyberbezpieczeństwa urządzeń Axis. Aby dowiedzieć się więcej, zapoznaj się z oficjalnym dokumentem „Signed firmware, secure boot, and security of private keys" („Podpisane oprogramowanie sprzętowe, bezpieczne uruchamianie i bezpieczeństwo kluczy prywatnych") na stronie *axis.com*.

Firmware upgrade (Uaktualnienie oprogramowania sprzętowego): Umożliwia uaktualnienie do nowej wersji oprogramowania sprzętowego. Nowe wersje oprogramowania sprzętowego mogą zawierać udoskonalenia działania i poprawki błędów oraz zupełnie nowe funkcje. Zalecamy, aby zawsze korzystać z najnowszej wersji. 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 oprogramowania sprzętowego.
- **Ustawienia fabryczne**: Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej wersji oprogramowania sprzętowego.
- **Autorollback (Automatyczne przywrócenie wersji)**: Uaktualnij i potwierdź uaktualnienie w ustawionym czasie. Jeżeli nie potwierdzisz, w urządzeniu zostanie przywrócona poprzednia wersja oprogramowania sprzętowego.

Firmware rollback (Przywracanie poprzedniej wersji oprogramowania sprzętowego): Przywróć poprzednio zainstalowaną wersję oprogramowania sprzętowego.

Specyfikacje

Wskaźniki LED

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

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 na stronie produktu przed jej wyjęciem. Nie wyjmuj karty SD w trakcie działania produktu.

Produkt obsługuje karty microSD/microSDHC/microSDXC.

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

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

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz .

Złącza

Złącze sieciowe

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

T10139115_pl

2023-04 (M7.5)

© 2019 – 2023 Axis Communications AB