AXIS I7020 Network Intercom

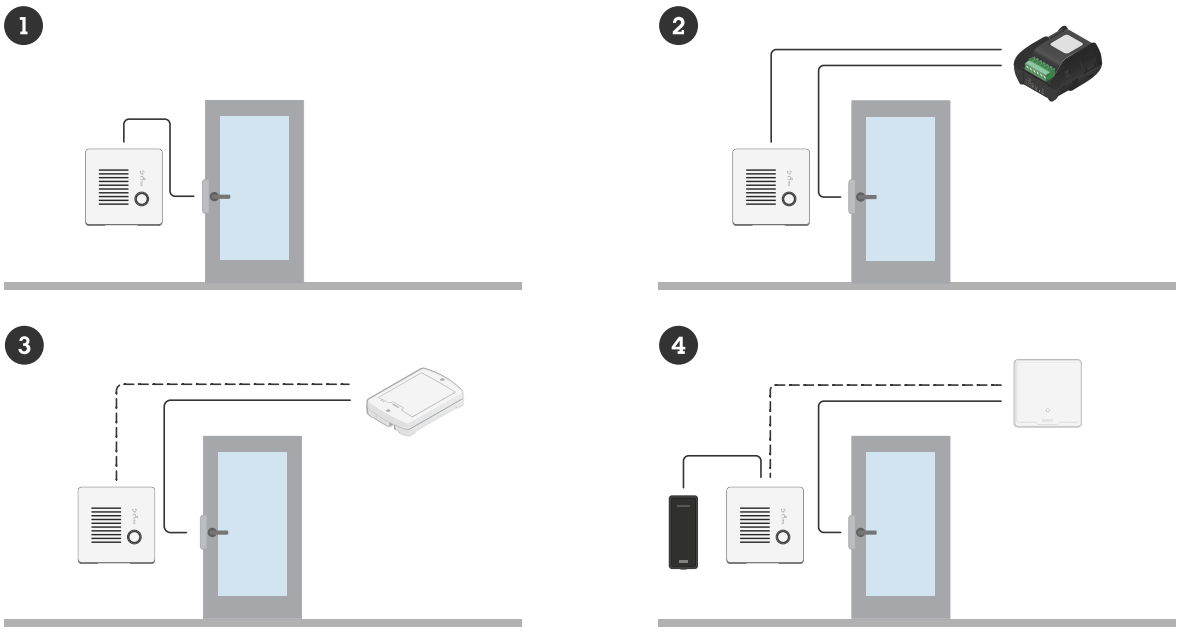
Podręcznik użytkownika

AXIS I7020 Network Intercom

Spis treści

Przegląd konfiguracji

Przegląd konfiguracji



1 *Interkom*
2 *Interkom połączony z AXIS A9801*
3 *Interkom połączony z AXIS A9161*
4 *Interkom połączony z czytnikiem i systemem kontroli dostępu*

Rozpocznij

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

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

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

Otwórz interfejs WWW urządzenia

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

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

2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora na stronie 4*.

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: *Interfejs WWW na stronie 11*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

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

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 61*.

Rozpocznij

Bezpieczne hasła

Ważne

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

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

Aby chronić dane, zalecamy:

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

Sprawdzanie braku zmian w oprogramowaniu urządzenia

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

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 61*.

   Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.

2. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

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

Konfiguracja bezpośredniego połączenia SIP (P2P)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP) na stronie 48*.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP) na stronie 48*

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest łączność bezpośrednia czyli peer-to-peer (P2P). Konfiguracji P2P należy używać wtedy, gdy komunikacja odbywa się pomiędzy niewielką liczbą agentów użytkownika w tej samej sieci IP i nie ma potrzeby zapewniania dodatkowych funkcji serwera PBX. Informacje na temat konfiguracji: *Peer-to-peer SIP (P2PSIP) na stronie 49*.

1. Przejdź do menu **Communication > SIP > Settings (Komunikacja > SIP > Ustawienia)** i wybierz opcję **Enable SIP (Włącz SIP)**.
2. Aby zezwolić urządzeniu na odbieranie połączeń, wybierz opcję **Zezwalaj na połączenia przychodzące**.

POWIADOMIENIE

Po zezwoleniu na połączenia przychodzące urządzenie akceptuje połączenia z dowolnego urządzenia podłączonego do sieci. Zalecamy blokowanie połączeń przychodzących w przypadku produktów dostępnych z sieci publicznych lub Internetu.

3. Kliknij opcję **Call handling (Obsługa połączeń)**.
4. Ustaw maksymalny czas połączenia w przypadku braku odpowiedzi w opcji **Limit czasu nawiązywania połączenia**.
5. Jeżeli zezwalasz na połączenia przychodzące, w polu **Incoming call timeout (Limit czasu połączenia przychodzącego)** ustaw liczbę sekund limitu czasu dla takich połączeń.
6. Kliknij opcję **Ports (Porty)**.
7. Wprowadź numer portu **Port SIP** i numer portu **Port TLS**.

Uwaga

- **Port SIP** – dla sesji SIP. Ruch sygnalizacyjny przez ten port nie jest szyfrowany. Domyślny numer portu to 5060.
- **Port TLS** – dla sesji SIPS oraz sesji SIP zabezpieczonych protokołem TLS. Ruch sygnalizacyjny za pośrednictwem tego portu jest szyfrowany przy użyciu Transport Layer Security (TLS). Domyślny numer portu to 5061.
- **Port początkowy RTP** – port używany do pierwszego strumienia mediów RTP w wywołaniu SIP. Domyślny numer portu to 4000. Niektóre zapory mogą blokować ruch RTP na niektórych numerach portów. Numer portu musi być w przedziale od 1024 do 65535.

8. Kliknij opcję **NAT traversal**.
9. Wybierz protokoły, które chcesz włączyć dla funkcji NAT traversal.

Uwaga

Użyj opcji NAT traversal, gdy urządzenie jest podłączone do sieci za routerem NAT lub znajduje się za zaporą. Więcej informacji znajduje się w rozdziale *NAT Transversal na stronie 50*.

10. Kliknij przycisk **Zapisz**.

Konfiguracja SIP przez serwer (PBX)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP) na stronie 48*.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP) na stronie 48*

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest serwer PBX. Konfiguracji PBX należy używać wtedy, gdy komunikacja odbywa się pomiędzy nieograniczoną liczbą agentów użytkownika w tej samej sieci IP i poza nią. W zależności od dostawcy usługi PBX można dodać dodatkowe funkcje. Więcej informacji znajduje się w rozdziale *Private Branch Exchange (PBX) – centrala abonencka na stronie 49*.

1. Od dostawcy PBX należy uzyskać następujące informacje:
   - ID użytkownika
   - Domena
   - Hasło
   - ID uwierzytelniania
   - ID rozmówcy
   - Rejestrator
   - Port początkowy RTP
2. Wybierz kolejno opcje **Communication > SIP > Accounts (Komunikacja > SIP > Konta)** i kliknij przycisk **+ Add account (+ Dodaj konto)**.
3. Wprowadź **Nazwę** konta.
4. Kliknij opcję **Registered (Zarejestrowane)**.
5. Wybierz tryb transmisji.
6. Podaj dane konta uzyskane od dostawcy serwera PBX.
7. Kliknij przycisk **Zapisz**.
8. Skonfiguruj ustawienia SIP w taki samo sposób, jak peer-to-peer — zobacz *Konfiguracja bezpośredniego połączenia SIP (P2P) na stronie 6*. Użyj portu początkowego RTP od dostawcy PBX.

Dołączanie strumienia wideo z pobliskiej kamery do połączenia SIP

Jeśli w pobliżu interkomu jest zamontowana kamera Axis, można dołączać pochodzący z niej strumień wideo do połączeń SIP i VMS z interkomu.

Wymagania

Kamera Axis z obsługą formatu H.264 i rozdzielczością 1280x720, 800x800 lub 640x480.

Aby podłączyć interkom do kamery:

1. Przejdź do menu **System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie)**.
2. W obszarze **Camera pairing (Parowanie kamery)** wprowadź adres, nazwę użytkownika i hasło kamery Axis.
3. Kliknij przycisk **Połącz**.

Tworzenie kontaktu

W tym przykładzie wyjaśniono sposób tworzenia nowego kontaktu w liście kontaktów. Zanim rozpoczniesz, włącz obsługę protokołu SIP w ustawieniu **Communication > SIP (Komunikacja > SIP)**.

Aby utworzyć nowy kontakt:

1. Przejdź do **Communication > Contact list (Komunikacja > Lista kontaktów)**.
2. Kliknij przycisk **+ Add contact (+ Dodaj kontakt)**.
3. Wprowadź imię i nazwisko kontaktu.
4. Wprowadź adres SIP kontaktu.

Uwaga

Więcej informacji dotyczących adresów SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP) na stronie 48*.

5. Wybierz konto SIP do wykonania połączenia.

Uwaga

Opcje dostępności konfiguruje się w oknie **System** > **Events (Zdarzenia)** > **Schedules (Harmonogramy)**.

6. W polu **Availability (Dostępność)** określ dostępność kontaktu. Jeżeli w czasie niedostępności kontaktu nastąpi próba nawiązania połączenia, połączenie zostanie anulowane, chyba że ustawiono kontakt rezerwowy.

Uwaga

Jest to kontakt, do którego przekierowywane jest połączenie w razie nieodebrania lub niedostępności odbiorcy.

7. W obszarze **Przekierowanie** wybierz opcję **Brak**.
8. Kliknij przycisk **Zapisz**.

Konfiguracja przycisku połączenia

Przycisk połączenia jest domyślnie skonfigurowany tak, aby nawiązywać połączenia przez VMS (oprogramowanie do zarządzania materiałem wideo). Aby zachować taką konfigurację, wystarczy dodać do systemu VMS interkom Axis.

W tym przykładzie wyjaśniono sposób konfigurowania systemu tak, by po na ciśnięciu przycisku połączenia przez gościa wykonywane było połączenie na numer kontaktu z listy kontaktów.

1. Wybierz kolejno **Communication > Calls > Call button (Komunikacja > Połączenia > Przycisk Połącz)**.
2. W obszarze **Recipients (Odbiorcy)** usuń **VMS**.
3. W obszarze **Recipients (Odbiorcy)** wybierz istniejący kontakt lub utwórz nowy.

Aby wyłączyć przycisk nawiązywania połączenia, wyłącz opcję **Enable call button (Włącz przycisk połączenia)**.

Korzystanie z DTMF do otwierania drzwi

Kiedy gość dzwoni interkomem, osoba, która odbierze połączenie, może wykorzystać sygnał (DTMF) urządzenia SIP do odblokowania drzwi. Kontroler drzwi odblokowuje i blokuje drzwi.

W tym przykładzie wyjaśniono, jak:

- zdefiniować sygnał DTMF w interkomie;
- skonfigurować interkom, aby:

- żądać odblokowania drzwi, **lub**
- otwierać drzwi przy użyciu przekaźnika wewnętrznego.

Wszystkie ustawienia należy wprowadzić na stronie internetowej interkomu.

Zanim rozpoczniesz

- Zezwól na połączenia SIP wychodzące z urządzenia i załóż konto SIP. Patrz *Konfiguracja bezpośredniego połączenia SIP (P2P) na stronie 6* i *Konfiguracja SIP przez serwer (PBX) na stronie 6*.

Definiowanie sygnału DTMF w interkomie

1. Przejdź do menu **Communication > SIP > DTMF (Komunikacja > SIP> DTMF)**.
2. Kliknij **+ Add sequence (Dodaj sekwencję)**.
3. W polu **Sequence (Sekwencja)** wprowadź **1**.
4. W polu **Opis** wprowadź **Odblokowanie drzwi**.
5. W polu **Accounts (Konta)** wybierz konto SIP.
6. Kliknij przycisk **Zapisz**.

Skonfiguruj interkom do otwierania drzwi za pomocą przekaźnika wewnętrznego

7. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
8. W polu **Name (Nazwa)** wprowadź **Odblokowanie drzwi przez DTMF**.
9. Z listy warunków w obszarze **Call (Połączenie)** wybierz kolejno opcje **DTMF** i **Unlock door (Odblokuj drzwi)**.
10. Z listy akcji w obszarze **I/O (We/Wy)** wybierz opcję **Toggle I/O once (Przełącz raz WE/WY)**.
11. Z listy portów wybierz **Relay 1 (Przekaźnik 1)**.
12. W polu **Duration (Czas trwania)** zmień wartość na **00:00:07**, co oznacza, że drzwi będą pozostawać otwarte przez 7 sekund.
13. Kliknij przycisk **Zapisz**.

Zezwalanie posiadaczom poświadczeń na otwieranie drzwi

Za pomocą listy wejść można umożliwić posiadaczom poświadczeń korzystanie z karty lub kodu PIN do wyzwalania akcji, takich jak otwieranie drzwi. W tym przykładzie wyjaśniamy, jak dodać posiadacza poświadczeń, który może użyć swojej karty do otwarcia drzwi 10 razy.

Wymagania wstępne

- W menu **Reader > Chip types (Czytnik > Typy chipów)** musi być aktywny odpowiedni typ chipu.

Włącz funkcję listy wejść i dodaj posiadacza poświadczeń:

1. Otwórz menu **Reader > Entry list (Czytnik > Lista wejść)**.
2. Włącz opcję **Use Entry list (Użyj listy wejść)**.
3. Kliknij pozycję **+ Add credential holder (+ Dodaj posiadacza poświadczeń)**.
4. Wprowadź imię i nazwisko posiadacza poświadczeń. Imię musi być unikatowe.
5. Wybierz pozycję **Card (Karta)**.
6. Przesuń kartą posiadacza w urządzeniu i kliknij **Get latest (Pobierz najnowsze)**.

7. Nie zmieniaj warunku **Access granted (Przyznano dostęp)**.
8. W obszarze **Valid to (Ważne do)** wybierz **Number of times (Ile razy)**.
9. W polu **Number of times (Ile razy)** wprowadź **10**.
10. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

1. Przejdź do **System > Events (System > Zdarzenia)**.
2. W menu **Rules (Reguły)** kliknij **+ Add a rule (+ Dodaj regułę)**.
3. W polu **Name (Nazwa)** wprowadź **Otwórz drzwi**.
4. Na liście warunków wybierz **Entry list > Access granted (Lista wejść > Przyznano dostęp)**.
5. Z listy akcji wybierz opcję **I/O > Toggle I/O once Toggle I/O once (We/Wy > Przełącz raz We/Wy)**.
6. Z listy portów wybierz opcję **Door (Drzwi)**.
7. W menu **State (Status)** wybierz **Active (Aktywne)**.
8. Ustaw czas trwania jako **00:00:07**.
9. Kliknij przycisk **Zapisz**.

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.

Interfejs WWW

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

Uwaga

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

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

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

Menu kontekstowe zawiera opcje:

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

Status

Informacje o urządzeniu

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

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

Stan synchronizacji czasu

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

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

Bezpieczeństwo

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

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

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

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

Trwające zapisy

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

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

Pokazuje lokalizację zapisu nagrania w zasobie.

Nagranie wideo

Instalacja

Capture mode (Tryb przechwytywania) : Tryb rejestracji to predefiniowana konfiguracja, która określa sposób zapisywania obrazów przez kamerę. Zmiana trybu rejestracji może wpłynąć na inne ustawienia, takie jak obszary obserwacji i maski prywatności.**Mounting position (Pozycja montażowa)** : Orientacja obrazu może się zmieniać w zależności od sposobu zamontowania kamery.**Power line frequency (Częstotliwość zasilania)**: Wybierz częstotliwość używaną w miejscu użytkowania instalacji, aby zminimalizować migotanie obrazu. W Ameryce z reguły używa się częstotliwości 60 Hz. W pozostałej części świata przeważają sieci o częstotliwości 50 Hz. Jeżeli nie wiesz, z której częstotliwości korzysta sieć w Twoim regionie, zapytaj lokalne władze.

Rotate (Obróć): Wybierz preferowaną orientację obrazu.

Zdjęcie

Wygląd

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

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

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

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

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

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

Szeroki zakres dynamiki

WDR : Włącz tę funkcję, aby wyświetlić zarówno ciemne, jak i jasne obszary na obrazie.**Local contrast (Kontrast lokalny)** : Za pomocą suwaka wyreguluj kontrast obrazu. Wyższa wartość zwiększa kontrast pomiędzy ciemnymi i jasnymi obszarami.**Tone mapping (Mapowanie tonowe)** : Suwak ten służy do zmiany wartości mapowania tonalnego zastosowanego na obrazie. Jeżeli wartość ta wynosi zero, to stosowana jest tylko standardowa korekcja gamma; wyższa wartość zwiększa widoczność najjaśniejszych i najciemniejszych fragmentów obrazu.

Równoważenie bieli

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

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

Light environment (Środowisko oświetlenia):

- **Automatic (Automatyczne)**: 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.

Ekspozycja

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

Exposure mode (Tryb ekspozycji):

- **Automatic (Automatycznie)**: kamera automatycznie dostosowuje wartości apertury, wzmocnienia i migawki.
- **Automatic aperture (Apertura automatyczna)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia. Wartość migawki jest stała.
- **Automatic shutter (Migawka automatyczna)** : Kamera automatycznie dostosowuje wartości migawki i wzmocnienia. Wartość apertury jest stała.
- **Hold current (Zachowaj bieżące)**: Blokuje bieżące ustawienia ekspozycji.
- **Flicker-free (Bez migotania)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia oraz używa tylko poniższych prędkości migawki: 1/50 s (50 Hz) i 1/60 s (60 Hz).
- **Flicker-free 50 Hz (Bez migotania 50 Hz)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia; prędkość migawki wynosi 1/50 s.
- **Flicker-free 60 Hz (Bez migotania 60 Hz)** : Kamera automatycznie dostosowuje wartości apertury i wzmocnienia; prędkość migawki wynosi 1/60 s.

- **Flicker-reduced (Zredukowane migotanie)** : Podobnie jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/100 s (50 Hz) i 1/120 s (60 Hz) dla jaśniejszych scen.
- **Flicker-reduced 50 Hz (Zredukowane migotanie 50 Hz)** : Działa tak samo jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/100 s dla jaśniejszych scen.
- **Flicker-reduced 60 Hz (Zredukowane migotanie 60 Hz)** : Działa tak samo jak „Bez migotania", ale kamera może wykorzystać prędkość migawki wyższą od 1/120 s dla jaśniejszych scen.
- **Manual (Manualnie)** : wartości apertury, wzmocnienia i migawki są stałe.

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

Uwaga

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

- **Automatic (Automatycznie)**: Nadaje się do większości sytuacji.
- **Center (Wyśrodkuj)**: Wykorzystuje ustalony obszar na środku obrazu w celu obliczenia ekspozycji. Obszar ma stały rozmiar i położenie w podglądzie na żywo.
- **Full (Pełny)** : Wykorzystuje cały obszar podglądu na żywo w celu obliczenia ekspozycji.
- **Upper (Górny)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w górnej części obrazu w celu obliczenia ekspozycji.
- **Lower (Dolny)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w dolnej części obrazu w celu obliczenia ekspozycji.
- **Left (Lewy)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w lewej części obrazu w celu obliczenia ekspozycji.
- **Right (Prawy)** : Wykorzystuje obszar o stałym rozmiarze i położeniu w prawej części obrazu w celu obliczenia ekspozycji.
- **Spot (Punktowe)**: Wykorzystuje obszar o stałym rozmiarze i położeniu w podglądzie na żywo w celu obliczenia ekspozycji.
- **Custom (Niestandardowe)**: Wykorzystuje obszar w podglądzie na żywo w celu obliczenia ekspozycji. Można dostosowywać rozmiar i położenie obszaru.

Max shutter (Maksymalny czas otwarcia migawki): Wybierz prędkość migawki zapewniającą najlepszy obraz. Zbyt niska prędkość migawki (dłuższa ekspozycja) może powodować rozmycie wszystkich ruchomych obiektów, a zbyt wysoka — pogarszać ogólną jakość obrazu. Najlepsze efekty działania tego ustawienia uzyskuje się w powiązaniu z maksymalnym wzmocnieniem.**Max gain (Maksymalne wzmocnienie)**: Wybierz odpowiednią maksymalną wartość wzmocnienia. Zwiększenie wartości maksymalnego wzmocnienia zwiększa poziom szczegółów w ciemnych obrazach, ale jednocześnie zwiększa też poziom szumów. Więcej szumu może powodować większe wykorzystanie przepustowości i pamięci. Jeżeli wartość maksymalnego wzmocnienia jest wysoka, to w przypadku znacząco różnych warunków oświetleniowych w dzień i w nocy obrazy mogą bardzo się różnić. Najlepsze efekty działania tego ustawienia uzyskuje się w powiązaniu z maksymalnym czasem migawki.**Motion-adaptive exposure (Ekspozycja przystosowana do ruchu)** : Wybierz, aby zmniejszać rozmycie obiektów w ruchu w warunkach słabego oświetlenia.**Blur-noise trade-off (Stosunek rozmycia do szumu)**: Za pomocą suwaka wyreguluj priorytet między szumem a rozmyciem obiektów w ruchu. Jeśli preferowana jest niska przepustowość i mniej szumu na niekorzyść rejestracji szczegółów poruszających się obiektów, należy przesunąć suwak w kierunku ustawienia **Low noise (Niski poziom szumu)**. Jeśli preferowana jest rejestracja szczegółów poruszających się obiektów (na niekorzyść przepustowości i szumu), należy przesunąć suwak w kierunku ustawienia **Low motion blur (Niski poziom rozmycia obiektów w ruchu)**.

Uwaga

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

Lock aperture (Zablokuj aperturę) : Włącz tę opcję, aby pozostawić rozmiar apertury ustawiony za pomocą suwaka **Aperture (Apertura)**. Wyłączenie opcji umożliwia automatyczne dostosowanie rozmiaru apertury przez kamerę. Można np. zablokować aperturę w przypadku scen ze stałymi warunkami oświetlenia.**Aperture (Apertura)** : Suwak służy do regulacji rozmiaru apertury, to znaczy ilości światła przedostającego się do obiektywu. Aby do przetwornika dostawała się większa ilość światła i w ten sposób w słabych warunkach oświetleniowych udało się uzyskać jaśniejszy obraz, przesuń suwak w kierunku wartości **Open (Otwarta)**. Otwarta apertura zmniejsza również głębię ostrości, co oznacza, że obiekty znajdujące się blisko lub daleko od kamery mogą wydawać się nieostre. Aby większe obszary obrazu były ostre, przesuń suwak w stronę wartości **Closed (Zamknięta)**.**Exposure level (Poziom ekspozycji)**: Użyj suwaka, aby dostosować naświetlenie obrazu.**Defog (Redukcja zamglenia)** : Włącz tę opcję, aby kamera wykrywała wpływ mgły na obraz i automatycznie ją usuwała w celu uzyskania bardziej czytelnego obrazu.

Uwaga

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

Strumień

Zapisy ogólne

Rozdzielczość: Wybierz rozdzielczość obrazu odpowiednią dla monitorowanej sceny. Wyższa rozdzielczość wymaga większej przepustowości i pojemności pamięci.**Frame rate (Liczba klatek na sekundę)**: Aby uniknąć problemów z przepustowością w sieci lub zmniejszyć zapotrzebowanie na zasoby pamięci, można ograniczyć poklatkowość do stałej liczby klatek na sekundę. Jeżeli liczba klatek na sekundę wynosi zero, utrzymywana jest najwyższa poklatkowość możliwa w danych warunkach. Większa poklatkowość wymaga większej przepustowości i pojemności zasobu.**P-frames (Klatki P)**: Ramka P to obraz przewidywany, na którym widać tylko zmiany w obrazie w stosunku do poprzedniej ramki. Wprowadź żądaną liczbę ramek P. Im wyższa wartość, tym mniejsza wymagana przepustowość. Jeżeli jednak w sieci występuje duży ruch, jakość obrazu wideo może widocznie spaść.**Compression (Kompresja)**: Użyj suwaka, aby dostosować kompresję obrazu. Wysoka wartość kompresji powoduje mniejszą przepływność bitową i niższą jakość obrazu. Niska kompresja poprawia jakość obrazu, ale zwiększa zapotrzebowanie na przepustowość i zasoby pamięci podczas nagrywania.**Signed video (Podpisany materiał wizyjny)** : Włącz, aby do sygnału wizyjnego dodawać podpis. Podpisywanie sygnału wizyjnego chroni go przed sabotażem, ponieważ zostaje on opatrzony zaszyfrowanym podpisem.

Zipstream

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

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

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

Optimize for storage (Optymalizacja pod kątem zasobu): Włączenie tej opcji pozwala zminimalizować przepływność bez uszczerbku dla jakości. Optymalizacja nie ma zastosowania do strumienia wyświetlanego w kliencie sieciowym. Tej opcji można użyć tylko wtedy, gdy system VMS obsługuje ramki B. Włączenie **Optymalizacji pod kątem zasobu** powoduje także aktywację funkcji **Dynamic GOP (Dynamicznej grupy obrazów)**.**Dynamic FPS (Dynamiczna liczba klatek na sekundę)**: Włączenie tej funkcji umożliwia różnicowanie przepustowości w zależności od poziomu aktywności w scenie. Większa aktywność wymaga większej przepustowości.**Lower limit (Dolny limit)**: Wprowadź wartość, która ustawi poklatkowość między minimalną liczbą klatek na sekundę a domyślną liczną klatek na sekundę w strumieniu na podstawie ruchu w scenie. Zalecamy stosowanie niższego limitu w scenach z bardzo małą ilością ruchu, gdzie liczba klatek na sekundę może spadać do 1, a nawet niżej.**Dynamic GOP (Dynamiczna grupa obrazów)**: Włącz, aby dynamicznie dostosowywać odstęp czasu między klatkami I w oparciu o stopień aktywności w scenie.**Upper limit (Górny limit)**: Wprowadź maksymalną długość grupy obrazów, tzn. maksymalną liczbę ramek P między dwiema ramkami kluczowymi. Ramka kluczowa to autonomiczna ramka obrazu niezależna od innych ramek.

Sterowanie przepływnością bitową

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

Orientacja

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

Dźwięk

Include (Dołącz): Włącz, aby używać dźwięku w strumieniu wideo.**Source (Źródło)** : Wybierz źródło dźwięku, którego chcesz używać.**Stereo** : Włącz, aby używać dźwięku wewnętrznego oraz dźwięku z zewnętrznego mikrofonu.

Nakładki

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

- **Text (Tekst)**: Wybierz, aby wyświetlać tekst zintegrowany z obrazem podglądu na żywo oraz widoczny we wszystkich widokach, nagraniach i zrzutach ekranu. Można wprowadzić własny tekst oraz dołączyć wstępnie skonfigurowane modyfikatory, które automatycznie pokazują na przykład godzinę, datę i poklatkowość.
  - : Kliknij, aby dodać modyfikator daty `%F` powodujący wyświetlanie daty w formacie rrrr-mm-dd.
  - : Kliknij, aby dodać modyfikator czasu `%X` powodujący wyświetlanie czasu w formacie gg:mm:ss (zegar 24-godzinny).
  - **Modifiers (Modyfikatory)**: Kliknij, aby wybrać dowolny skonfigurowany wstępnie modyfikator widoczny na liście w celu dodania go do pola tekstowego. Na przykład modyfikator `%a` powoduje wyświetlanie dnia tygodnia.
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - **Appearance (Wygląd)**: Umożliwia wybór koloru tekstu i tła, np. białego tekstu na czarnym tle (ustawienie domyślne).
  - : Wybierz lokalizację nałożenia na obrazie.
- **Obraz**: Wybierz, aby wyświetlać statyczny obraz nałożony na strumień wideo. Można użyć plików .bmp, .png, .jpeg lub .svg.
  Aby przesłać obraz, kliknij opcję **Images (Obrazy)**. Przed wysłaniem obrazu można użyć następujących opcji:
  - **Scale with resolution (Skaluj z rozdzielczością)**: Wybierz, aby automatycznie przeskalować obraz nałożenia i dopasować go do rozdzielczości obrazu wideo.
  - **Use transparency (Użyj przezroczystości)**: Wybierz i wprowadź wartość szesnastkową RGB dla danego koloru. Użyj formatu RRGGBB. Przykłady wartości szesnastkowych: FFFFFF (biały), 000000 (czarny), FF0000 (czerwony), 6633FF (niebieski), 669900 (zielony). Tylko dla obrazów .bmp.
- **Scene annotation (Adnotacja sceny)** : Ta opcja pozwala wyświetlać nałożenie tekstowe w strumieniu wideo, które pozostaje w tej samej pozycji, nawet gdy kamera obraca się lub przechyla w innym kierunku. Można wybrać wyświetlanie nałożenia tylko przy określonych zakresach powiększenia.
  - : Kliknij, aby dodać modyfikator daty `%F` powodujący wyświetlanie daty w formacie rrrr-mm-dd.
  - : Kliknij, aby dodać modyfikator czasu `%X` powodujący wyświetlanie czasu w formacie gg:mm:ss (zegar 24-godzinny).
  - **Modifiers (Modyfikatory)**: Kliknij, aby wybrać dowolny skonfigurowany wstępnie modyfikator widoczny na liście w celu dodania go do pola tekstowego. Na przykład modyfikator `%a` powoduje wyświetlanie dnia tygodnia.
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - **Appearance (Wygląd)**: Umożliwia wybór koloru tekstu i tła, np. białego tekstu na czarnym tle (ustawienie domyślne).
  - : Wybierz lokalizację nałożenia na obrazie. Nałożenie zostanie zapamiętane we współrzędnych obrotu i pochylenia tej pozycji.
  - **Annotation between zoom levels (%) (Adnotacja pomiędzy poziomami zoomu (%))**: Pozwala ustawić poziomy zoomu, przy których nałożenie będzie widoczne.
  - **Annotation symbol (Symbol adnotacji)**: Wybierz symbol, który będzie pokazywany zamiast nałożenia, gdy wartość zoomu przekroczy ustawiony zakres.
- **Streaming indicator (Wskaźnik strumieniowania)** : Wybierz, aby wyświetlać animację nałożoną na strumień wideo. Animacja wskazuje, że strumień wideo jest przesyłany na żywo, nawet jeśli w scenie nie ma ruchu.
  - **Appearance (Wygląd)**: Wybierz kolor tekstu i tła animacji, np. czerwoną animację na przezroczystym tle (ustawienie domyślne).
  - **Size (Rozmiar)**: Wybierz rozmiar czcionki.
  - : Wybierz lokalizację nałożenia na obrazie.
- **Widget: Linegraph (Wykres liniowy)** : Wyświetla wykres przedstawiający zmiany mierzonej wartości w czasie.

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

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

Maski prywatności

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

Komunikacja

Odbiorcy

Kontakty

Kliknij, aby pobrać listę kontaktów jako plik json. Kliknij, aby zaimportować listę kontaktów (w formacie json). **Add contact (Dodaj kontakt)**: Kliknij, aby dodać nową osobę do listy kontaktów.**First name (Imię)**: Wpisz imię kontaktu.**Last name (Nazwisko)**: Wpisz nazwisko kontaktu.**Speed dial (Szybkie wybieranie)** : wpisz nr szybkiego wybierania kontaktu. Numer ten będzie używany do dzwonienia do kontaktu z tego urządzenia.**Adres SIP**: Jeśli używasz adresu SIP, wprowadź adres IP kontaktu lub rozszerzenie. : Kliknij w celu nawiązania połączenia testowego. Po odebraniu połączenie zostanie automatycznie zakończone.**SIP account (Konto SIP)**: Jeśli używasz adresu SIP, wybierz konto SIP na potrzeby połączeń z kontaktem za pomocą tego urządzenia.**Dostępność**: Wybierz harmonogram dostępności kontaktu. Jeżeli w czasie niedostępności kontaktu nastąpi próba nawiązania połączenia, połączenie zostanie anulowane, chyba że ustawiono kontakt rezerwowy.**Fallback (Przekierowanie)**: W razie potrzeby wybierz kontakt rezerwowy z listy. Menu kontekstowe zawiera opcje:**Edit contact (Edytuj kontakt)**: edycja właściwości kontaktu.**Delete contact (Usuń kontakt)**: usuwanie kontaktów.

SIP

Ustawienia

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

SIP setup assistant (Asystent konfiguracji SIP): kliknięcie tej opcji pozwala skonfigurować SIP krok po kroku.**Enable SIP (Włącz SIP)**: Zaznacz tę opcję, aby umożliwić inicjowanie i odbieranie połączeń SIP.**Allow incoming calls (Zezwalaj na połączenia przychodzące)**: Zaznacz tę opcję, aby zezwalać na połączenia przychodzące z innych urządzeń SIP.

Obsługa połączeń

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

Porty

Numer portu musi należeć do przedziału od 1024 do 65535.

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

NAT Transversal

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

Uwaga

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

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

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

Dźwięk i obraz wideo

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

Uwaga

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

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

Dodatkowe

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

Konta

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

Konto zostało zarejestrowane na serwerze SIP.

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

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

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

- **Active (Aktywne)**: wybierz tę opcję, aby użyć tego konta.
- **Ustaw jako domyślne**: zaznacz tę opcję, aby ustawić konto jako domyślne. Konto domyślne jest wymagane; można ustawić tylko jedno konto jako domyślne.
- **Answer automatically (Odbierz automatycznie)**: wybierz tę opcję, aby automatycznie odbierać połączenia.

- **Prioritize IPv6 over IPv4 (Pierwszeństwo IPv6 względem IPv4)** : po wybraniu tej opcji adresy IPv6 są traktowane nadrzędnie względem IPv4. Ta funkcja przydaje się podczas łączenia z kontami P2P lub nazwami domen rozpoznawanymi zarówno w adresach IPv4, jak i IPv6. Priorytet IPv6 można nadać tylko tym nazwom domen, które są mapowane na adresy IPv6.
- **Nazwa**: Wprowadź nazwę opisową. Może to być na przykład imię i nazwisko, rola lub lokalizacja. Nazwa nie musi być unikalna.
- **User ID (ID użytkownika)**: Wprowadź numer wewnętrzny lub numer telefonu przypisany do urządzenia.
- **Peer-to-peer**: służy do wykonywania bezpośrednich połączeń z innym urządzeniem SIP w sieci lokalnej.
- **Zarejestrowane**: służy do wykonywania połączeń z urządzeniami SIP spoza sieci lokalnej (przez serwer SIP).
- **Domain (Domena)**: jeśli to możliwe, wprowadź nazwę publicznej domeny. Będzie ona wyświetlana jako część adresu SIP podczas wywoływania innych kont.
- **Hasło**: wprowadź hasło powiązane z kontem SIP, aby uwierzytelnić się na serwerze SIP.
- **Authentication ID (ID uwierzytelniania)**: wprowadź identyfikator uwierzytelnienia używany do uwierzytelniania na serwerze SIP. Jeśli jest on taki sam, jak identyfikator użytkownika, nie trzeba go wprowadzać.
- **Caller ID (ID rozmówcy)**: nazwa wyświetlana odbiorcom połączeń przychodzących z urządzenia.
- **Rejestrator**: wprowadź adres IP rejestratora.
- **Tryb transmisji**: Wybierz tryb transmisji SIP dla konta: UPD, TCP lub TLS.
- **TLS version (Wersja TLS)** (tylko w trybie transportu TLS): wybierz wersję TLS. Wersje **v1.2** and **v1.3** są najbezpieczniejsze. **Automatic (Automatycznie)** wybiera najbezpieczniejszą wersję obsługiwaną przez system.
- **Media encryption (Szyfrowanie mediów)** (tylko w trybie TLS): wybierz rodzaj szyfrowania mediów (audio i wideo) w połączeniach SIP.
- **Certificate (Certyfikat)** (tylko w trybie TLS): Wybierz certyfikat.
- **Verify server certificate (Potwierdź certyfikat serwera)** (tylko w trybie TLS): zaznacz, aby potwierdzać certyfikat serwera.
- **Secondary SIP server (Dodatkowy serwer SIP)**: Włącz, aby w razie niepowodzenia rejestracji na głównym serwerze SIP urządzenie podjęło próbę rejestracji na serwerze dodatkowym.
- **SIP secure (Bezpieczny SIP)**: wybierz tę opcję, aby użyć protokołu Secure Session Initiation Protocol (SIPS). Protokół SIPD wykorzystuje tryb transmisji TLS do szyfrowania ruchu.
- **Serwery proxy**
  - **Proxy**: Kliknij, aby dodać serwer proxy.
  - **Prioritize (Nadaj priorytet)**: Po dodaniu dwóch lub więcej serwerów proxy kliknij, aby określić ich priorytet.
  - **Server address (Adres serwera)**: Tu należy wprowadzić adres IP serwera proxy SIP.
  - **Username (Nazwa użytkownika)**: wprowadź nazwę użytkownika serwera proxy SIP, jeśli to konieczne.
  - **Hasło**: wprowadź hasło do serwera proxy SIP, jeśli to konieczne.
- **Nagranie wideo**
  - **View area (Obszar obserwacji)**: wybierz obszar obserwacji połączeń wideo. Jeśli nie zostanie wybrany obszar obserwacji, zostanie użyty widok natywny.
  - **Rozdzielczość**: wybierz rozdzielczość połączeń wideo. Rozdzielczość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **Frame rate (Liczba klatek na sekundę)**: wybierz liczbę klatek na sekundę w połączeniach wideo. Poklatkowość wpływa na wymagane zapotrzebowanie na przepustowość.
  - **H.264 profile (Profil H.264)**: Wybierz profil połączeń wideo.

DTMF

Add sequence (Dodaj sekwencję): Kliknięcie tej opcji pozwala utworzyć nową sekwencję DTMF. Aby utworzyć regułę wyzwalaną przez sygnał wybierania, otwórz menu **Events > Rules (Zdarzenia > Reguły)**.**Sequence (Sekwencja)**: Wprowadź znaki aktywujące tę regułę. Dozwolone znaki: 0–9, A–D, # oraz *.**Description (Opis)**: Wprowadź opis akcji, która będzie wyzwalana przez sekwencję.**Accounts (Konta)**: Wybierz konta, które mają używać sekwencji DTMF. W przypadku wybrania konfiguracji **peer-to-peer** wszystkie konta peer-to-peer będą współdzieliły jedną sekwencję DTMF.

ProtokołyWybierz protokoły, które mają być używane dla każdego konta. Wszystkie konta peer-to-peer mają takie same ustawienia protokołu.**Use RTP (RFC2833) (Użyj RTP (RFC2833))**: Włącz tę opcję, aby zezwalać na sygnały DTMF, inne sygnały i zdarzenia telefoniczne w pakietach RTP.**Użyj SIP INFO (RFC2976)**: Włącz tę opcję, aby dołączyć metodę INFO do protokołu SIP. Metoda INFO służy do dodania opcjonalnych informacji o warstwie, zazwyczaj powiązanych z sesją.

Połączenie testowe

SIP account (Konto SIP): Wybierz konto, z którego ma zostać wykonane połączenie testowe.**Adres SIP**: Wprowadź adres SIP i kliknij , aby wykonać połączenie testowe i zweryfikować działanie konta.

Lista dostępu

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

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

Add source (Dodaj źródło): Kliknij, aby utworzyć nowy wpis na liście dostępu.**SIP source (Źródło SIP)**: Wpisz identyfikator rozmówcy lub adres serwera SIP źródła.

Kontroler Multicast

Use multicast controller (Użyj kontrolera Multicast): Włącz tę opcję, aby aktywować kontroler multicast.**Audio codec (Kodek audio)**: Wybierz kodek audio. **Source (Źródło)**: Dodaj nowe źródło kontrolera Multicast.

- **Etykieta**: Wprowadź nazwę etykiety, która nie jest jeszcze używana przez źródło.
- **Source (Źródło)**: Wprowadź źródło.
- **Port**: Wprowadź port.
- **Priority (Priorytet)**: Wybierz priorytet.
- **Profile (Profil)**: Wybierz profil.
- **SRTP key (Przycisk SRTP)**: Wprowadź przycisk SRTP.

Menu kontekstowe zawiera opcje:**Edit (Edycja)**: Edytuj źródło kontrolera Multicast.**Usuń**: Usuń źródło kontrolera Multicast.

Połączenia

Przycisk połączenia

Enable call button (Włącz przycisk połączenia): Po włączeniu tej opcji można używać przycisku połączenia.**Standby light (Kontrolka trybu gotowości)**: Umożliwia wybranie opcji dla kontrolki świetlnej otaczającej przycisk połączenia.

- **Auto (Automatycznie)** : urządzenie włącza lub wyłącza wbudowaną kontrolkę zależnie od warunków oświetleniowych w otoczeniu.
- **On (Włączona)**: wbudowana kontrolka jest zawsze włączona w trybie gotowości urządzenia.
- **Off (Wyłączona)**: wbudowana kontrolka jest zawsze wyłączona w trybie gotowości urządzenia.

Recipients (Odbiorcy): ta opcja pozwala wybrać co najmniej jeden lub kilka kontaktów, z którymi będzie nawiązywanie połączenie po naciśnięciu przycisku. W przypadku dodania kilku odbiorców zostanie nawiązane połączenie ze wszystkimi osobami jednocześnie. Maksymalna liczba odbiorców połączeń SIP wynosi sześć, podczas gdy można mieć nieograniczoną liczbę odbiorców połączeń VMS.**Fallback (Przekierowanie)**: ta opcja pozwala dodać kontakt do przekierowania połączenia, gdy żaden z odbiorców z listy nie odpowiada.

Zapisy ogólne

Dźwięk

Uwaga

- Wybrany klip audio jest odtwarzany tylko w przypadku nawiązywania połączenia.
- Jeżeli w trakcie połączenia nastąpi zmiana klipu audio lub wzmocnienia, nie będzie ona obowiązywać, aż do następnego połączenia.

Ringtone (Dźwięk dzwonka): Wybierz klip audio, który ma będzie odtwarzany, gdy ktoś wywoła połączenie z urządzeniem. Użyj suwaka, aby dostosować wzmocnienie.**Ringback tone (Sygnał oddzwaniania)**: Wybierz klip audio, który ma będzie odtwarzany, gdy ktoś wywoła połączenie z urządzenia. Użyj suwaka, aby dostosować wzmocnienie.

połączenia VMS

połączenia VMS

Allow calls in the video management software (VMS) (Zezwalaj na połączenia w oprogramowaniu do zarządzania materiałem wizyjnym (VMS)): wybierz tę opcję, aby zezwolić na połączenia z urządzenia do oprogramowania VMS. Połączenia VMS są możliwe także w przypadku wyłączonego protokołu SIP.**Call timeout (Limit czasu wywołania)**: ta opcja pozwala ustawić maksymalny czas prób nawiązania połączenia, gdy nikt nie odbiera.

Narzędzia analityczne

Konfiguracja metadanych

RTSP metadata producers (Producenci metadanych RTSP)

Wyświetla listę aplikacji transmitujących metadane oraz wykorzystywane przez nie kanały.

Uwaga

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

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

Czytnik

Połączenie

Czytnik zewnętrzny (wejście)

Używanie zewnętrznego czytnika OSDP: włączenie tej opcji pozwala korzystać z urządzenia w połączeniu z zewnętrznym czytnikiem. Podłącz czytnik do złącza czytnika.
Status (Stan):

- **Connected (Podłączony)**: Urządzenie jest podłączone do aktywnego zewnętrznego czytnika.
- **Connecting (Trwa łączenie)**: Urządzenie próbuje połączyć się z zewnętrznym czytnikiem.
- **Not connected (Brak połączenia)**: Usługa OSDP jest wyłączona.

Protokół czytnika

Typ protokołu czytnika: Wybierz protokół, z którego ma korzystać funkcja czytnika.

- **VAPIX reader (Czytnik VAPIX)**: Może być używany tylko z kontrolerem drzwi Axis.
  - **Protocol (Protokół)**: Wybierz **HTTPS** lub **HTTP**.
  - **Door controller address (Adres kontrolera drzwi)**: Wprowadź adres IP kontrolera drzwi.
  - **User name (Nazwa użytkownika)**: Wpisz nazwę użytkownika kontrolera drzwi.
  - **Hasło**: Wpisz hasło kontrolera drzwi.
  - **Connect (Połącz)**: Kliknij, aby połączyć się z kontrolerem drzwi.
  - **Select reader (Wybierz czytnik)**: Wybierz czytnik wejścia dla odpowiednich drzwi.
- **OSDP**:
  - **OSDP address (Adres OSDP)**: Wprowadź adres czytnika OSDP. Domyślny i najczęściej używany adres w przypadku pojedynczych czytników to 0.
- **Wiegand** :
  - **Beeper (Sygnał dźwiękowy)**: włączenie tej opcji aktywuje wejście sygnału dźwiękowego.
  - **Input for beeper (Wejście sygnału dźwiękowego)**: wybierz port WE/WY dla sygnału dźwiękowego.
  - **Input used for LED control (Wejście wykorzystywane do sterowania oświetleniem LED)**: Wybierz liczbę portów WE/WY do sterowania odpowiedzią LED w urządzeniu.
  - **Input for LED1/LED2 (Wejście wskaźnika LED1/LED2)**: wybierz porty WE/WY, które mają być używane na potrzeby wejścia wskaźnika LED.
  - **Idle color (Kolor w trybie bezczynności)**: Jeśli do sterowania wskaźnikiem LED nie są używane porty WE/WY, można wybrać statyczny kolor wyświetlany na pasku wskaźnika czytnika kart.
  - **Color for state low/high (Kolor stanu niskiego/wysokiego)**: jeżeli do sterowania wskaźnikiem LED jest używany jeden port WE/WY, wybierz kolory wyświetlane w przypadku stanów niskiego i wysokiego.
  - **Idle color/LED1 color/LED2 color/LED1 + LED2 color (Kolor w trybie bezczynności/LED1 kolor/LED2 kolor LED1 + kolor LED2)**: Jeżeli do sterowania wskaźnikami LED są używane 2 porty WE/WY, wybierz kolory wyświetlane w przypadku stanów bezczynności, LED1, LED2 i LED1 + LED2.
  - **Keypress format (Format naciśnięcia klawisza)**: Wybierz metodę formatowania kodu PIN wysyłanego do urządzenia kontroli dostępu.
  - **FourBit (Czterobitowy)**: PIN `1234` jest kodowany i wysyłany jako 0x1 0x2 0x3 0x4. Jest to działanie domyślne i najczęściej stosowane.
  - **EightBitZeroPadded (Ośmiobitowy z dodanym zerem)**: PIN `1234` jest kodowany i wysyłany jako 0x01 0x02 0x03 0x04.
  - **EightBitInvertPadded (Ośmiobitowy z inwersją)**: PIN `1234` jest kodowany i wysyłany jako 0XE1 0XD2 0xC3 0xB4.
  - **Wiegand26**: PIN jest kodowany w formacie Wiegand26 za pomocą ośmiobitowego kodu obiektu i szesnastobitowego identyfikatora.
  - **Wiegand34**: PIN jest kodowany w formacie Wiegand34 za pomocą szesnastobitowego kodu obiektu i szesnastobitowego identyfikatora.
  - **Wiegand37**: PIN jest kodowany w formacie Wiegand37 (H10302) za pomocą 35-bitowego identyfikatora.
  - **Wiegand37FacilityCode (Kod obiektu Wiegand 37)**: PIN jest kodowany w formacie Wiegand37 (H10304) za pomocą szesnastobitowego kodu obiektu i dziewiętnastobitowego identyfikatora.
  - **Facility code (Kod obiektu)**: Wpisz kod obiektu, który ma być wysyłany. Ta opcja jest obsługiwana tylko w przypadku niektórych formatów naciśnięcia klawisza.

Format wyjściowy

Select data format (Wybierz format danych): wybranie formatu, w którym dane karty będą wysyłane do urządzenia kontroli dostępu.

- **Raw (Surowe dane)**: dane karty są przekazywane w niezmienionej postaci.
- **Wiegand26**: dane karty są kodowane w formacie Wiegand26 za pomocą ośmiobitowego kodu obiektu i szesnastobitowego identyfikatora.
- **Wiegand34**: dane karty są kodowane w formacie Wiegand34 za pomocą szesnastobitowego kodu obiektu i szesnastobitowego identyfikatora.
- **Wiegand37**: dane karty są kodowane w formacie Wiegand37 (H10302) za pomocą 35-bitowego identyfikatora.
- **Wiegand37FacilityCode (Kod obiektu Wiegand37)**: dane karty są kodowane w formacie Wiegand37 (H10304) za pomocą szesnastobitowego kodu obiektu i dziewiętnastobitowego identyfikatora.
- **Custom (Niestandardowe)**: pozwala określić własną metodę formatowania.

Facility code override mode (Tryb nadpisania kodu obiektu): umożliwia wybranie opcji zastępowania kodu obiektu.

- **Automatycznie**: nie zastępuje kodu obiektu; tworzy go na podstawie automatycznie wykrywanych danych wejściowych. Funkcja ta wykorzystuje oryginalny kod obiektu lub fałszuje go na podstawie nadmiarowych bitów numeru karty.
- **Optional (Opcjonalne)**: używa kodu obiektu z danych wejściowych lub zastępuje go skonfigurowaną wartością opcjonalną.
- **Override (Zastąpienie)**: zawsze zastępuje wartość na określony kod obiektu.

PIN

Ustawienia kodu PIN muszą odpowiadać konfiguracji urządzenia kontroli dostępu.

Length (0–32) (Długość (0–32)): wprowadź liczbę cyfr w kodzie PIN. Jeśli podczas korzystania z czytnika użytkownicy nie muszą wprowadzać kodu PIN, ustaw wartość 0.**Timeout (seconds, 3–50) (Limit czasu (3–50 sekund))** wprowadź liczbę sekund, które muszą upłynąć, zanim w urządzeniu zostanie przywrócony tryb bezczynności w przypadku nieotrzymania kodu PIN.

Lista wejść

Za pomocą listy wejść można skonfigurować urządzenie tak, aby umożliwić osobom mającym poświadczenia używanie karty lub numeru PIN do wykonywania różnych czynności, w tym otwierania drzwi. Poświadczenia są przechowywane lokalnie w urządzeniu. Można również połączyć tę funkcję z zewnętrznym kontrolerem drzwi.

Use Entry list (Używanie listy wejść): włączenie tej opcji pozwala korzystać z listy wejść.**Use connected door controller (Używanie podłączonego kontrolera drzwi)**: tę opcję należy włączyć, gdy urządzenie jest już połączone z kontrolerem drzwi. Jeśli użytkownik poda dane uwierzytelniające, których nie ma na liście wejść, zostanie wysłane żądanie do podłączonego kontrolera drzwi. Nie są wysyłane poświadczenia wpisane na listę wejść.**Add credential holder (Dodaj posiadacza poświadczeń)**: Kliknij tę opcję, aby dodać nowego posiadacza poświadczeń.**First name (Imię)**: Wprowadź imię.**Last name (Nazwisko)**: Wprowadź nazwisko.**Credential type (Typ poświadczeń)**:

- **PIN**:
  - **PIN**: Wprowadź niepowtarzalny numer PIN lub kliknij przycisk **Generate (Generuj)**, aby automatycznie utworzyć numer.
- **Card (Karta)**:
  - **UID**: Wprowadź identyfikator UID i długość bitową karty lub kliknij przycisk **Get latest (Pobierz najnowsze)**, aby pobrać informacje z ostatniego przeciągnięcia karty w czytniku.

Event condition (Warunek zdarzenia): Wybierz jeden lub więcej warunków, które zostaną aktywowane, gdy posiadacz poświadczeń użyje swoich poświadczeń. Aby skonfigurować akcję w odpowiedzi na zdarzenie, przejdź do menu **System > Events (System > Zdarzenia)**, a następnie utwórz regułę, używając warunku wybranego w tym miejscu.**Valid from (Ważne od)**: Wybierz **Current device time (Bieżący czas urządzenia)**, aby od razu aktywować poświadczenie. Wyczyść zaznaczenie tej opcji, jeśli chcesz określić inny moment aktywacji poświadczeń.**Valid to (Ważne do)**:

- **No end date (Brak daty zakończenia)**: Poświadczenie jest ważne bezterminowo.
- **End date (Data zakończenia)**: Podaj datę i godzinę wygaśnięcia ważności poświadczeń.
- **Number of times (Ile razy)**: Określ, ile razy posiadacz poświadczeń może z nich korzystać. Wartość w polu zmniejsza się po każdym użyciu poświadczeń i pokazuje ile razy pozostało.

Notes (Uwagi): Tu można wprowadzić dodatkowe informacje.**Suspend (Zawieś)**: Zaznaczenie tego pola spowoduje tymczasowe unieważnienie poświadczeń.

Dźwięk

Ustawienia urządzenia

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

Noise cancellation (Redukcja szumów): włączenie tej funkcji pozwala poprawić jakość dźwięku dzięki usunięciu szumów z tła.**Input type (Typ wejścia)** : wybierz typ źródła sygnału wejściowego, na przykład wewnętrzny mikrofon lub wejście liniowe.**Power type (Typ zasilania)** : Wybierz typ zasilania źródła sygnału wejściowego.**Apply changes (Zastosuj zmiany)** : powoduje zastosowanie wybranych ustawień.**Echo cancellation (Usuwanie efektu echa)** : Włącz, aby usuwać echo podczas komunikacji dwukierunkowej.**Separate gain controls (Oddzielna regulacja wzmocnienia)** : Włącz, aby regulować wzmocnienie osobno dla poszczególnych źródeł sygnału wejściowego.**Automatic gain control (Automatyczna regulacja wzmocnienia)** : Włącz, aby dynamicznie dostosować wzmocnienie do zmian dźwięku.**Gain (Wzmocnienie)**: Za pomocą suwaka zmień wartość wzmocnienia. Kliknij ikonę mikrofonu, aby wyciszyć lub wyłączyć wyciszenie.

Wyjście: Pokazuje typ urządzenia wyjściowego.

Gain (Wzmocnienie): Za pomocą suwaka zmień wartość wzmocnienia. Kliknij ikonę głośnika, aby wyciszyć lub wyłączyć wyciszenie.**Automatic volume control (Automatyczna regulacja głośności)**: Automatic volume control (Automatyczna regulacja głośności) : Włącz, aby urządzenie automatycznie i dynamicznie dostosowywało wzmocnienie zgodnie z poziomem szumów otoczenia. Automatyczna regulacja głośności dotyczy wszystkich wyjść audio, w tym liniowego i cewki indukcyjnej.

Strumień

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

Klipy audio

Add clip (Dodaj klip): umożliwia dodanie nowego klipu audio. Obsługiwane formaty plików: .au,. mp3,. Opus,. Vorbis,. wav. Rozpoczynanie odtwarzania klipu audio. Zatrzymywanie odtwarzania klipu audio. Menu kontekstowe zawiera opcje:

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

Nagrania

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

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

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

Aplikacje

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

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

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

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

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

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

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

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

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

Uwaga

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

Lokalizacja urządzenia

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

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

Test konfiguracji

Interactive device image (Interaktywny obraz urządzenia): Klikaj przyciski na obrazie, aby zobaczyć, jaka będzie reakcja na naciskanie przycisków. Pozwala to na przetestowanie konfiguracji lub rozwiązywanie problemów ze sprzętem bez fizycznego dostępu do urządzenia.**Latest credentials (Najnowsze poświadczenia)**  : ta opcja pokazuje ostatnio zapisane poświadczenia.  Wyświetlanie najnowszych danych poświadczeń.  Menu kontekstowe zawiera opcje:

- **Reverse UID (Odwracanie kolejności w UID)**: Odwraca kolejność bajtów identyfikatora UID.
- **Revert UID (Przywracanie kolejności w UID)**: Przywraca pierwotną kolejność bajtów identyfikatora UID.
- **Copy to clipboard (Kopiowanie do schowka)**: Kopiuje identyfikator UID.

Check credentials (Sprawdź poświadczenia)  : Podaj UID lub PIN i prześlij, aby sprawdzić poświadczenia. System zareaguje w taki sam sposób, jak w przypadku użycia poświadczeń w urządzeniu. Jeśli wymagane jest podanie zarówno identyfikatora UID, jak i kodu PIN, najpierw wprowadź UID.

Sieć

IPv4

Przypisz automatycznie IPv4: wybierz, aby router sieciowy automatycznie przypisywał adres IP do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresu IP (DHCP) dla większości sieci.**Adres IP**: wprowadź unikatowy adres IP dla urządzenia. Statyczne adresy IP można przydzielać losowo w sieciach izolowanych, pod warunkiem że adresy są unikatowe. Aby uniknąć występowania konfliktów, zalecamy kontakt z administratorem sieci przed przypisaniem statycznego adresu IP.**Maska podsieci**: Otwórz maskę podsieci, aby określić adresy w sieci lokalnej. Wszystkie adresy poza siecią lokalną przechodzą przez router.**Router**: wprowadź adres IP domyślnego routera (bramki) używanego do łączenia z urządzeniami należącymi do innych sieci i segmentów sieci.**Fallback to static IP address if DHCP isn't available (Jeśli DHCP jest niedostępny, zostanie ono skierowane do statycznego adresu IP)**: Wybierz, czy chcesz dodać statyczny adres IP, który ma być używany jako rezerwa, jeśli usługa DHCP jest niedostępna i nie można automatycznie przypisać adresu IP.

Uwaga

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

IPv6

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

Nazwa hosta

Przypisz automatycznie nazwę hosta: Wybierz, aby router sieciowy automatycznie przypisywał nazwę hosta do urządzenia.**Nazwa hosta**: Wprowadź ręcznie nazwę hosta, aby zapewnić alternatywny dostęp do urządzenia. W raporcie serwera i dzienniku systemowym jest używana nazwa hosta. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.**Włącz aktualizacje dynamiczne DNS**: Zezwól urządzeniu na automatyczne aktualizowanie rekordów serwera nazw domen, gdy zmieni się jego adres IP.**Zarejestruj nazwę DNS**: Wprowadź unikatową nazwę domeny, która wskazuje adres IP urządzenia. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.**TTL**: Time to Live (TTL) to ustawienie określające, jak długo rekord DNS zachowuje ważność, zanim trzeba go zaktualizować.

Serwery DNS

Przypisz automatycznie DNS: Wybierz ustawienie, aby serwer DHCP automatycznie przypisywał domeny wyszukiwania i adresy serwerów DNS do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresów DNS (DHCP) dla większości sieci.**Przeszukaj domeny**: jeżeli używasz nazwy hosta, która nie jest w pełni kwalifikowana, kliknij **Add search domain (Dodaj domenę wyszukiwania)** i wprowadź domenę, w której ma być wyszukiwana nazwa hosta używana przez urządzenie.**Serwery DNS**: kliknij polecenie **Add DNS server (Dodaj serwer DNS)** i wprowadź adres IP podstawowego serwera DNS. Powoduje to przełożenie nazw hostów na adresy IP w sieci.

HTTP i HTTPS

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

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

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

Uwaga

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

HTTP port (Port HTTP): wprowadź wykorzystywany port HTTP. urządzenie pozwala na korzystanie z portu 80 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.**HTTPS port (Port HTTPS)**: wprowadź wykorzystywany port HTTPS. urządzenie pozwala na korzystanie z portu 443 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.**Certificate (Certyfikat)**: wybierz certyfikat, aby włączyć obsługę protokołu HTTPS w tym urządzeniu.

Protokoły wykrywania sieci

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

Globalne serwery proxy

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

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

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

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

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

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

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

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

Proxy settings (Ustawienia proxy): W razie potrzeby należy wprowadzić ustawienia proxy, aby połączyć się z serwerem proxy.**Host**: Wprowadź adres serwera proxy.**Port**: wprowadź numer portu służącego do uzyskania dostępu.**Login** i **Hasło**: W razie potrzeby wprowadź nazwę użytkownika i hasło do serwera proxy.**Authentication method (Metoda uwierzytelniania)**:
- **Zwykła**: Ta metoda jest najbardziej zgodnym schematem uwierzytelniania HTTP. Jest ona mniej bezpieczna niż metoda **Digest (Szyfrowanie)**, ponieważ nazwa użytkownika i hasło są wysyłane do serwera w postaci niezaszyfrowanej.
- **Szyfrowanie**: ta metoda jest bezpieczniejsza, ponieważ zawsze przesyła hasło w sieci w formie zaszyfrowanej.
- **Automatycznie**: ta opcja umożliwia urządzeniu wybór metody uwierzytelniania w zależności od obsługiwanych metod. Priorytet ma metoda **Szyfrowanie**; w dalszej kolejności stosowana jest metoda **Zwykła**.

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

SNMP

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

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

Uwaga

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

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

Bezpieczeństwo

Certyfikaty

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

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

Obsługiwane są następujące formaty:

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

Ważne

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

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

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

Menu kontekstowe zawiera opcje:

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

Secure keystore (Bezpieczny magazyn kluczy) :

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

Kontrola dostępu do sieci i szyfrowanie

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

- **Hasło**: Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap)**: wybierz wersję Peap używaną w switchu sieciowym.

- **Etykieta**: 1 pozwala używać szyfrowania EAP klienta; 2 pozwala używać szyfrowania PEAP klienta. Wybierz etykietę używaną przez przełącznik sieciowy podczas korzystania z wersji 1 protokołu Peap.

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

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

Zapobiegaj atakom typu brute force

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

Zapora

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

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

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

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

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

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

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

Uwaga

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

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

Niestandardowy podpisany certyfikat systemu AXIS OS

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

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

Konta

Konta

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

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

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

Anonimowy dostęp

Allow anonymous viewing (Zezwalaj na anonimowe wyświetlanie): Włączenie tej opcji pozwala wszystkim osobom uzyskać dostęp do urządzenia jako dozorca bez logowania się za pomocą konta.**Allow anonymous PTZ operating (Zezwalaj na anonimową obsługę PTZ)** : Jeśli włączysz tę opcję, anonimowi użytkownicy będą mogli obracać, przechylać i powiększać/zmniejszać obraz.

Konta SSH

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

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

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

Virtual host (Host wirtualny)

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

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

Disabled (Wyłączono): Serwer jest wyłączony.

Konfiguracja OpenID

Ważne

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

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

Zdarzenia

Reguły

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

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

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

Odbiorcy

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

Uwaga

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

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

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

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

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

- **Hasło**: Wprowadź hasło logowania.

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

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

Uwaga

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

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

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

Harmonogramy

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

Wyzwalacze ręczne

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

MQTT

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

ALPN

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

Klient MQTT

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

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

ALPN protocol (Protokół ALPN): Wprowadź nazwę protokołu ALPN dostarczoną przez dostawcę brokera MQTT. Dotyczy to tylko ustawień MQTT przez SSL i MQTT przez WebSocket Secure.**Username (Nazwa użytkownika)**: należy tu wprowadzić nazwę użytkownika, która będzie umożliwiać klientowi dostęp do serwera.**Hasło**: wprowadzić hasło dla nazwy użytkownika.**Client ID (Identyfikator klienta)**: wprowadź identyfikator klienta. Identyfikator klienta jest wysyłany do serwera w momencie połączenia klienta.**Clean session (Czysta sesja)**: steruje zachowaniem w czasie połączenia i czasie rozłączenia. Po wybraniu tej opcji informacje o stanie są odrzucane podczas podłączania i rozłączania.**HTTP proxy (Serwer proxy HTTP)**: Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTP, możesz zostawić to pole puste.**HTTPS proxy (Serwer proxy HTTPS)**: Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTPS, możesz zostawić to pole puste.**Keep alive interval (Przedział czasowy KeepAlive)** Umożliwia klientowi detekcję, kiedy serwer przestaje być dostępny, bez

konieczności oczekiwania na długi limit czasu TCP/IP.**Timeout (Przekroczenie limitu czasu)**: interwał czasowy (w sekundach) pozwalający na zakończenie połączenia. Wartość domyślna: 60**Prefiks tematu urządzenia**: Używany w domyślnych wartościach tematu w komunikacie łączenia i komunikacie LWT na karcie **MQTT client (Klient MQTT)** oraz w warunkach publikowania na karcie **MQTT publication (Publikacja MQTT)**.**Reconnect automatically (Ponowne połączenie automatyczne)**: określa, czy klient powinien ponownie połączyć się automatycznie po rozłączeniu.**Komunikat łączenia**określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.**Send message (Wysłanie wiadomości)**: włącz, aby wysyłać wiadomości.**Use default (Użyj domyślnych)**: wyłącz, aby wprowadzić własną wiadomość domyślną.**Topic (Temat)**: wprowadź temat wiadomości domyślnej.**Payload (Próbka)**: wprowadź treść wiadomości domyślnej.**Retain (Zachowaj)**: wybierz, aby zachować stan klienta w tym **Topic (Temacie)QoS**: zmiana warstwy QoS dla przepływu pakietów.**Wiadomość Ostatnia Wola i Testament**Funkcja Last Will Testament (LWT) zapewnia klientowi dostarczenie informacji wraz z poświadczeniami w momencie łączenia się z brokerem. Jeżeli klient nie rozłączy się w pewnym momencie w późniejszym terminie (może to być spowodowane brakiem źródła zasilania), może umożliwić brokerowi dostarczenie komunikatów do innych klientów. Ten komunikat LWT ma taką samą postać jak zwykła wiadomość i jest kierowany przez tę samą mechanikę.**Send message (Wysłanie wiadomości)**: włącz, aby wysyłać wiadomości.**Use default (Użyj domyślnych)**: wyłącz, aby wprowadzić własną wiadomość domyślną.**Topic (Temat)**: wprowadź temat wiadomości domyślnej.**Payload (Próbka)**: wprowadź treść wiadomości domyślnej.**Retain (Zachowaj)**: wybierz, aby zachować stan klienta w tym **Topic (Temacie)QoS**: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

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

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

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

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

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

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

QoS: Wybierz żądany poziom subskrypcji MQTT.

Nałożenia MQTT

Uwaga

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

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

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

Przechowywanie

Sieciowa pamięć masowa

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

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

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

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

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

Pamięć pokładowa

Ważne

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

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

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

- **Decrypt (Odszyfruj)**: To narzędzie pozwala sformatować kartę SD bez szyfrowania. Powoduje to usunięcie wszystkich danych znajdujących się na karcie SD. Wszelkie nowe dane zapisane na karcie SD nie zostaną zaszyfrowane.
- **Change password (Zmień hasło)**: Umożliwia zmianę hasła wymaganego do szyfrowania karty SD.

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

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

Profile strumienia

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

Add stream profile (Dodaj profil strumienia): Kliknij to polecenie w celu utworzenia nowego profilu strumienia.**Preview (Podgląd)**: Podgląd strumienia wideo z wybranymi ustawieniami profilu strumienia. Zmiana ustawień na stronie powoduje aktualizowanie podglądu. Jeśli urządzenie ma różne obszary obserwacji, aktywny obszar obserwacji można zmienić w menu rozwijanym w lewym dolnym rogu obrazu. **Nazwa**: Nadaj profilowi nazwę.**Description (Opis)**: Dodaj opis profilu.**Video codec (Kodek wideo)**: Wybierz kodek wideo, który ma być stosowany w profilu.**Rozdzielczość**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Frame rate (Liczba klatek na sekundę)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Compression (Kompresja)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Zipstream** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Optimize for storage (Optymalizacja pod kątem pamięci masowej)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Dynamic FPS (Dynamiczna liczba klatek na sekundę)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16* .**Dynamic GOP (Dynamiczna grupa obrazów)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16* .**Mirror (Odbicie lustrzane)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**GOP length (Długość grupy obrazów)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Bitrate control (Kontrola przepływności bitowej)**: Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.**Include overlays (Uwzględnij nałożenia)** : Wybierz typ nakładek, jakie mają być dołączane. Informacje o dodawaniu nakładek znajdują się w temacie *Nakładki na stronie 18*.**Include audio (Dołącz audio)** : Opis tego ustawienia znajduje się w temacie *Strumień na stronie 16*.

ONVIF

Konta ONVIF

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

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

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

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

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

Profile mediów ONVIF

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

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

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

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

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

Uwaga

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

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

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

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

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

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

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

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

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

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

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

PTZ  : Wybierz ustawienia PTZ dla swojej konfiguracji.

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

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

Detektory

Sabotaż kamery

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

Trigger delay (Opóźnienie wyzwalacza): Wprowadź minimalny czas, przez jaki muszą być aktywne warunki sabotażu, zanim nastąpi wyzwolenie alarmu. Pozwoli to zapobiec fałszywym alarmom wywoływanym przez znane warunki wpływające na obraz.**Trigger on dark images (Wyzwól przy ciemnym obrazie)**: Po spryskaniu obiektywu farbą trudno jest wywołać alarm, ponieważ nie można odróżnić tej sytuacji od innych, podczas których występuje ten sam efekt zaciemnienia obrazu, na przykład kiedy warunki oświetlenia ulegają zmianie. Po włączeniu tego parametru alarmy będą generowane we wszystkich przypadkach, w których obraz ulegnie zaciemnieniu. Gdy funkcja jest wyłączona, urządzenie nie będzie generować alarmów w razie zaciemnienia obrazu.

Uwaga

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

Detekcja dźwięku

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

Wykrywanie wstrząsów

Shock detector (Detektor wstrząsów): Włącz, aby generować alarm, jeśli urządzenie zostanie uderzone przez przedmiot lub ktoś będzie przy nim manipulował.**Sensitivity level (Poziom czułości)**: Przesuń suwak, aby wyregulować poziom czułości, przy którym urządzenie powinno generować alarm. Niska wartość sprawi, że urządzenie będzie generować alarm tylko po mocnym uderzeniu. Przy wysokiej wartości urządzenie będzie generować alarm nawet w reakcji na delikatne manipulowanie.

Akcesoria

Porty we/wy

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

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

PortNazwa: edytuj tekst, aby zmienić nazwę portu.**Usage (Użycie)**: Domyślne ustawienie portu przekaźnika to **Door (Drzwi)**. W przypadku urządzeń z ikonami wskaźników  zmienia kolor na zielony, kiedy zmienia się stan i zostają odblokowane drzwi. Jeśli używasz przekaźnika do innych celów niż obsługa drzwi i nie chcesz, aby ikona zapalała się przy zmianie stanu, możesz wybrać inne ustawienie portu.**Direction (Kierunek)**:  oznacza, że port jest portem wejścia.  oznacza, że jest to port wyjścia. Jeśli port jest konfigurowalny, można kliknąć ikony, aby przełączać się między wejściem a wyjściem.**Normal state (Stan normalny)**: Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.**Current state (Bieżący stan)**: wyświetla bieżący stan portu. Wejście lub wyjście jest aktywowane w momencie zmiany bieżącego stanu na inny niż stan normalny. Obwód wejścia urządzenia jest otwarty po odłączeniu lub po doprowadzeniu napięcia powyżej 1 V DC.

Uwaga

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

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

Edge-to-edge

Funkcja parowania kamery umożliwia sparowanie interkomu Axis ze zgodną kamerą Axis w celu dołączania strumienia na żywo pochodzącego z kamery do połączeń SIP i VMS.

Parowanie kameryAdres: Wprowadź nazwę hosta lub adres IP kamery.**Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika odpowiadającą kamerze.**Hasło**: Wprowadź hasło kamery.**Disconnect (Rozłącz)**: Kliknij, aby odłączyć już podłączoną kamerę.**Connect (Połącz)**: Kliknij, aby podłączyć kamerę.

Dzienniki

Raporty i dzienniki

Raporty

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

Dzienniki

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

Zdalny dziennik systemu

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

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

- Axis
- RFC 3164
- RFC 5424

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

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

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

Zwykła konfiguracja

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

Konserwacja

Konserwacja

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

Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

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

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

Uwaga

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

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

- **Standard upgrade (Aktualizacja standardowa)**: Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **Ustawienia fabryczne**: Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej wersji systemu AXIS OS.

- **Autorollback (Automatyczne przywrócenie wersji)**: Uaktualnij i potwierdź uaktualnienie w ustawionym czasie. Jeżeli nie potwierdzisz, w urządzeniu zostanie przywrócona poprzednia wersja systemu AXIS OS.

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

Rozwiązywanie problemów

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

Ważne

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

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

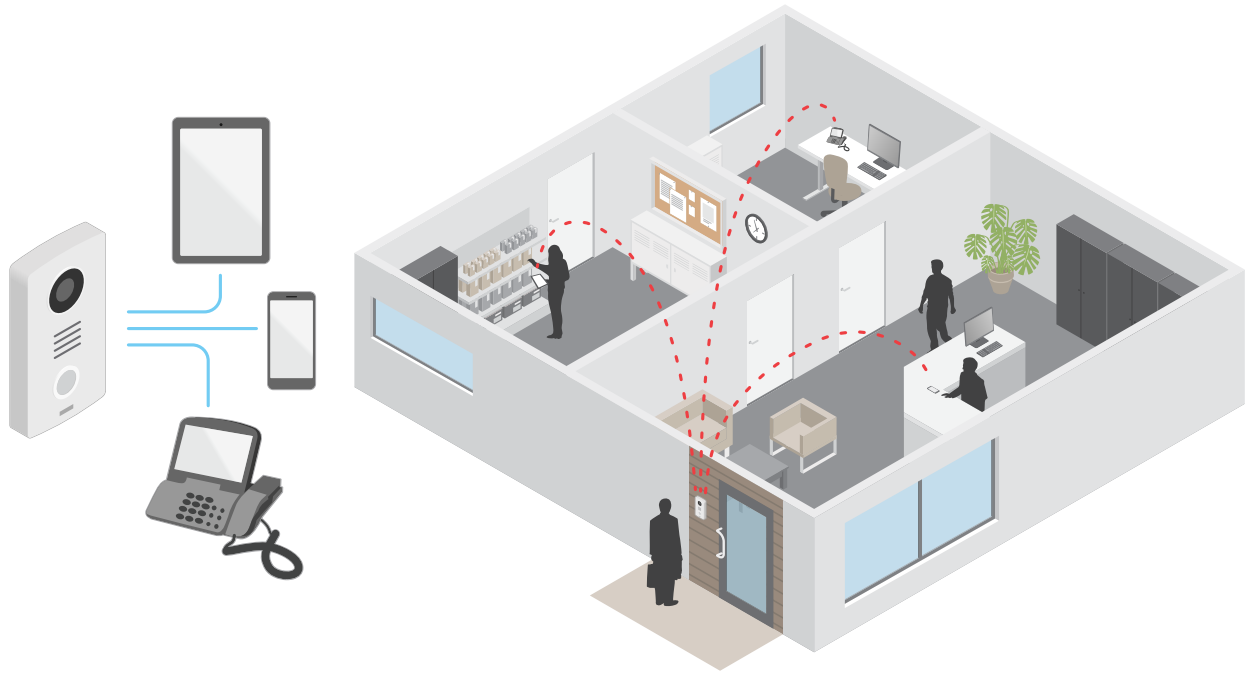
Więcej informacji

Voice over IP (VoIP)

Voice over IP (VoIP) to grupa technologii, która umożliwia komunikację głosową i sesje multimedialne w sieciach IP, na przykład przez internet. Podczas tradycyjnych połączeń telefonicznych sygnały analogowe przesyłane są obwodami przez publiczną komutowaną sieć telefoniczną – Public Switched Telephone Network (PSTN). Podczas połączeń VoIP sygnały analogowe są konwertowane na sygnały cyfrowe, tak aby możne je było przesyłać jako pakiety danych przez lokalne sieci IP lub Internet.

W produkcie Axis protokół VoIP jest włączany za pośrednictwem sygnalizacji Session Initiation Protocol (SIP) i Dual-Tone Multi-Frequency (DTMF).

Przykład:



Po naciśnięciu przycisku nawiązywania połączenia na interkomie Axis wykonywane jest połączenie do jednego ze wstępnie zdefiniowanych odbiorców. Po odebraniu połączenia rozpoczyna się rozmowa. Obraz i dźwięk są transmitowane za pomocą technologii VoIP.

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

Protokół inicjacji sieci (SIP) jest stosowany do konfiguracji, utrzymywania i kończenia połączeń VoIP. Połączenia można wykonywać pomiędzy dwoma rozmówcami lub większą ich liczbą (tzw. agentami użytkowników SIP). Aby wykonać połączenie SIP, można skorzystać na przykład z telefonów SIP, softphone'ów lub urządzeń Axis obsługujących SIP.

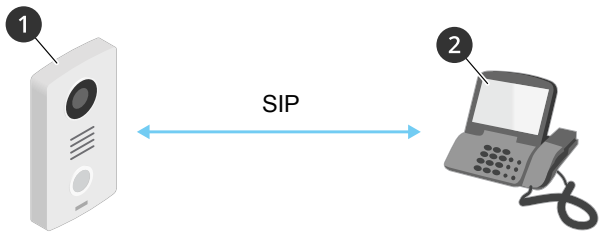
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

W sieci lokalnej można nawiązywać połączenia w konfiguracji peer-to-peer, a pomiędzy sieciami – za pomocą PBX.

Peer-to-peer SIP (P2PSIP)

Podstawowa komunikacja SIP odbywa się bezpośrednio pomiędzy dwoma lub większą liczba agentów użytkowników SIP. Połączenie takie nazywane jest peer-to-peer SIP (P2PSIP). Jest ono wykonywane w sieci lokalnej i wymaga jedynie adresów SIP agentów użytkowników. W takim przypadku adres SIP to zazwyczaj `sip:<ip-lokalny>`.

Przykład:



1 *Agent użytkownika A — interkom. Adres SIP: sip:192.168.1.101*
2 *Agent użytkownika B — telefon z włączonym SIP. Adres SIP: sip:192.168.1.100*

Można skonfigurować interkom Axis tak, by łączył się z telefonem SIP w tej samej sieci za pomocą peer-to-peer SIP.

Private Branch Exchange (PBX) – centrala abonencka

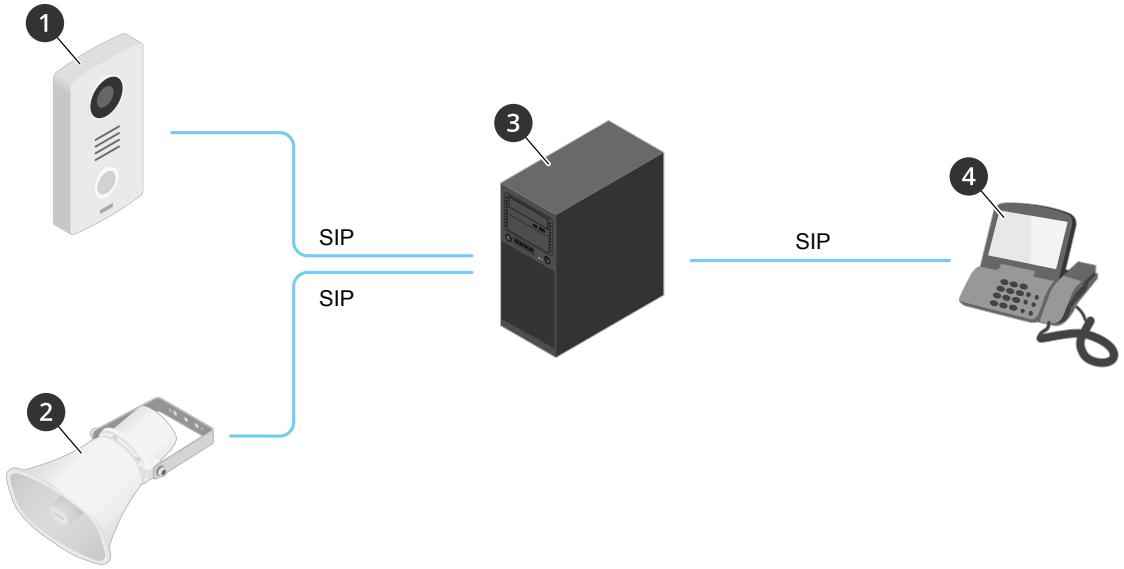
Podczas wykonywania połączeń SIP poza lokalną sieć IP PBX może służyć za centralkę. Głównym elementem PBX jest serwer SIP, zwany również serwerem proxy SIP lub rejestratorem. PBX działa jak tradycyjna centralka telefoniczna, wyświetla bieżący status klienta i umożliwia na przykład przekazywanie połączeń, rejestrację wiadomości głosowym i przekierowania.

Serwer SIP PBX można skonfigurować lokalnie lub zdalnie. Można go umieścić w intranecie lub u zewnętrznego dostawcy usług serwerowych. Podczas wykonywania połączeń SIP pomiędzy sieciami połączenia są przekazywane przez zestaw PBX, które wysyłają zapytania o lokalizację docelowego adresu SIP.

Każdy agent użytkownika SIP jest rejestrowany w PBX; mogą łączyć się z innymi poprzez wybranie właściwego numeru wewnętrznego. Typowy adres SIP w tym przypadku to `sip:<użytkownik>@<domena>` lub `sip:<użytkownik>@<ip-rejestratora>`. Adres SIP jest niezależny od adresu SIP, a PBX udostępnia urządzenie przez cały czas, kiedy jest ono zarejestrowane.

Przykład:

Więcej informacji



1 *sip:mydoor@company.com*
2 *sip:myspeaker@company.com*
3 ***PBX*** *sip.company.com*
4 *sip:office@company.com*

Po naciśnięciu przycisku wykonywania połączenia na interkomie Axis połączenie jest przekazywane przez jedną lub więcej centralek PBX do adresu SIP w lokalnej sieci IP lub przez internet.

NAT Transversal

Użyj NAT (Network Address Translation), gdy urządzenie Axis znajduje się w prywatnej sieci (LAN) i chcesz uzyskać do niego dostęp spoza tej sieci.

Uwaga

Router musi również obsługiwać NAT Traversal i protokół UPnP®.

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

- 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** (Session Traversal Utilities for NAT) to protokół sieciowy klient-serwer umożliwiający urządzeniom Axis 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** (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.

Cyberbezpieczeństwo

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

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

Więcej informacji

Usługa powiadomień w systemach zabezpieczeń Axis

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

Postępowanie z lukami w zabezpieczeniach

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

Bezpieczne działanie urządzeń Axis

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

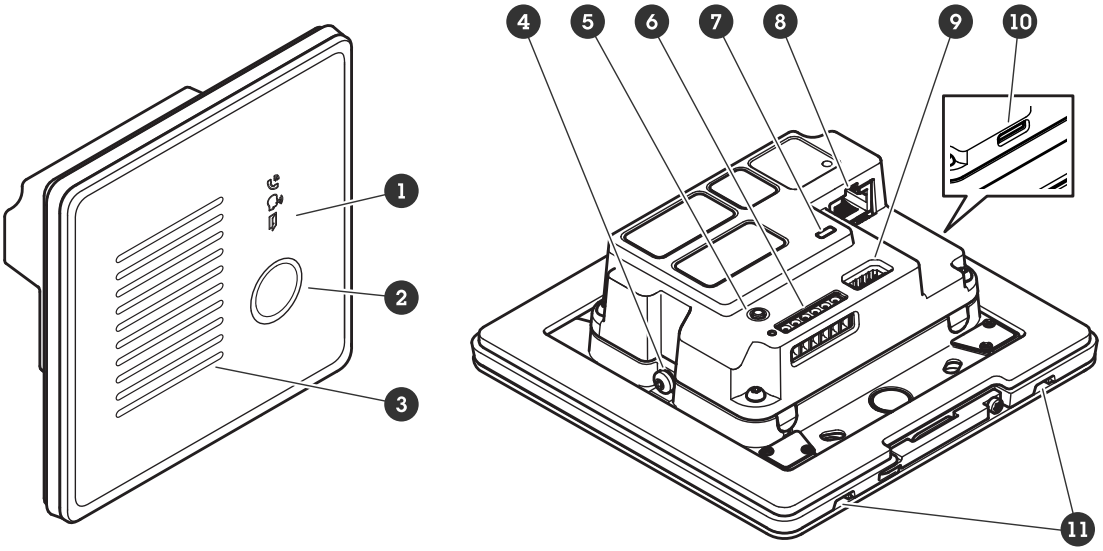
Aplikacje

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

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

Specyfikacje

Przegląd produktów



1 *Ikony wskaźników na stronie 52*
2 *Przycisk połączenia*
3 *Głośnik*
4 *Śruba uziemienia*
5 *Przycisk kontrolny na stronie 53*
6 *Złącze WE/WY, czytnika i przekaźnika na stronie 54*
7 *Dioda stanu*
8 *Złącze sieciowe na stronie 53*
9 *Złącze audio na stronie 53*
10 *Gniazdo karty SD na stronie 53 (microSD/microSDHC/microSDXC)*
11 *Mikrofon (2x)*

Wskaźniki i elementy sterowania na panelu przednim

Po podłączeniu produktu do zasilania wskaźniki na panelu przednim zaświecą się na kilka sekund.

Ikony wskaźników

Ikona	Wskazanie
	Stałe bursztynowe światło po zainicjowaniu połączenia wychodzącego.Miga na bursztynowo po zainicjowaniu połączenia przychodzącego.
	Stałe niebieskie światło podczas trwającego połączenia.
	Stałe zielone światło po otwarciu drzwi.

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przy normalnym działaniu.

Gniazdo karty SD

POWIADOMIENIE

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

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

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

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

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 61*.
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około trzy sekundy, aż dioda LED stanu zacznie migać na zielono.

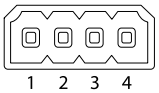
Złącza

Złącze sieciowe

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

Złącze audio

4-pinowy blok złączy wejść i wyjść audio.



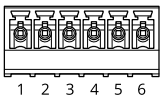
Funkcje	Styk	Uwagi
Wejście liniowe	1	Wejście liniowe (mono)
GND	2	Uziemienie audio

Wyjście liniowe	3	Wyjście liniowe (mono)
GND	4	Uziemienie audio

Złącze WE/WY, czytnika i przekaźnika

Tego złącza można używać do obsługi WE/WY i przekaźnika lub do podłączania czytników.

6-pinowego bloku złączy



1 -
2 *12 V*
3 *A/IO1*
4 *B/IO2*
5 *COM*
6 *NO/NZ*

Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może służyć do zasilania urządzeń pomocniczych, jeśli dane urządzenie korzysta z zasilania PoE klasy 4. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC **We/wy** : Maks. obciążenie = 50 mA **Czytnik/przekaźnik**: maks. obciążenie = 350 mA
We/wy: konfigurowalne (wejście lub wyjście) **Czytnik**: A	3	**We/wy**: wejście cyfrowe — podłącz do styku 1, aby aktywować, lub pozostaw rozłączone, aby dezaktywować. Wyjście cyfrowe — podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia. **Czytnik**: RS485 – A	**We/wy** : wejście – od 0 do maks. 30 V DC wyjście od 0 do maks. 30 V DC, otwarty dren, 100 mA)
We/wy: konfigurowalne (wejście lub wyjście) **Czytnik**: B	4	**We/wy**: tak samo jak styk 3 **Czytnik**: RS485 – B	**We/wy**: tak samo jak styk 3
Przekaźnik: COM	5	Wspólny	
Przekaźnik: NO/NC	6	Normalnie otwarte/normalnie zamknięte. Do podłączania urządzeń przekaźnikowych. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd = 700 mA, maks. napięcie = 30 V DC

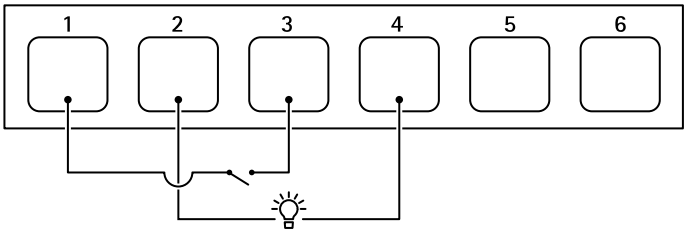
Złącze I/O

Jedna opcja pozwala używać złącza jako WE/WY do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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

Wyjście cyfrowe – Do podłączania urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączone urządzenia mogą być aktywowane za pośrednictwem interfejsu API VAPIX®, zdarzeń lub interfejsu urządzenia.

Przykład:



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

Złącze przekaźnikowe

W połączeniu z WE/WY to złącze może służyć do podłączenia przekaźnika półprzewodnikowego i używania go:

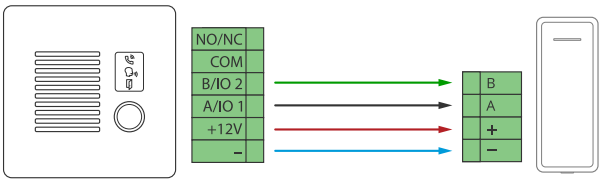
- jako standardowego przekaźnika otwierającego i zamykającego obwody pomocnicze;
- do bezpośredniego sterowania zamkiem;
- do sterowania zamkiem przez przekaźnik bezpieczeństwa. Korzystanie z przekaźnika bezpieczeństwa po bezpiecznej stronie drzwi zapobiega podłączeniu zewnętrznych przewodów.

Złącze czytnika

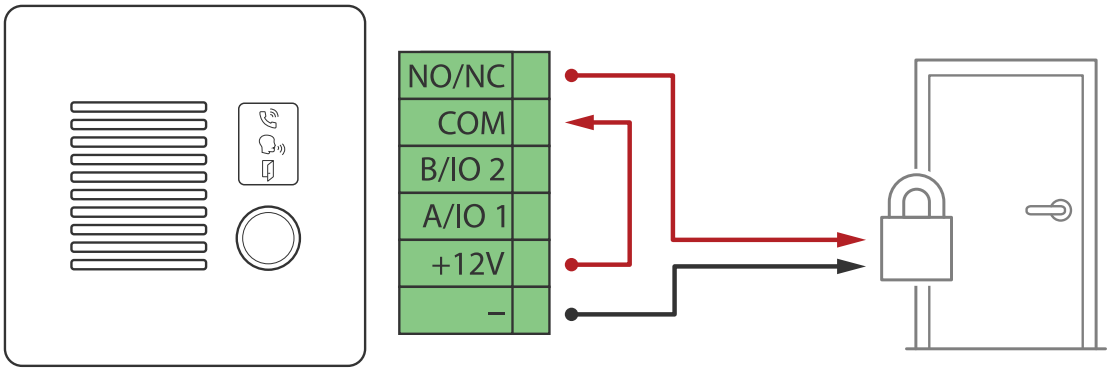
Trzecią opcją jest użycie tego złącza do podłączenia zewnętrznego czytnika.

Sprzęt podłączeniowy

Czytnik Axis

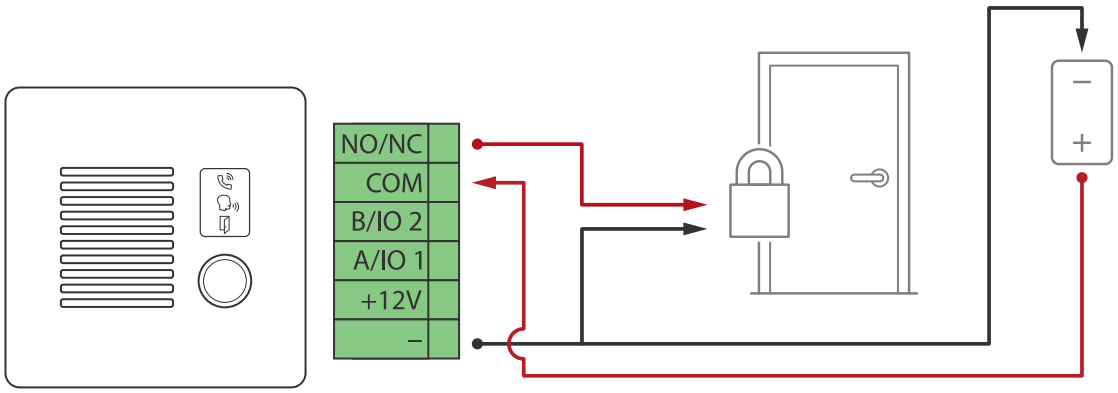


Przekaźnik zasilany przez zasilacz PoE (12 V)



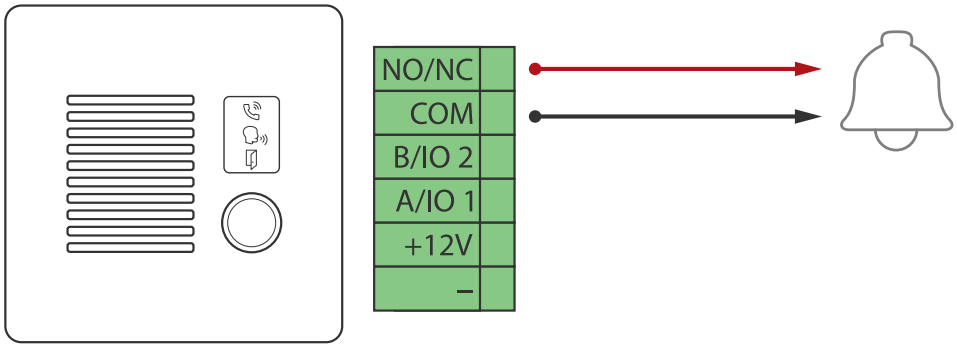
1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   - do zamka zabezpieczonego podczas awarii zasilania
   - do zamka zabezpieczonego

Przekaźnik zasilany przez osobny zasilacz



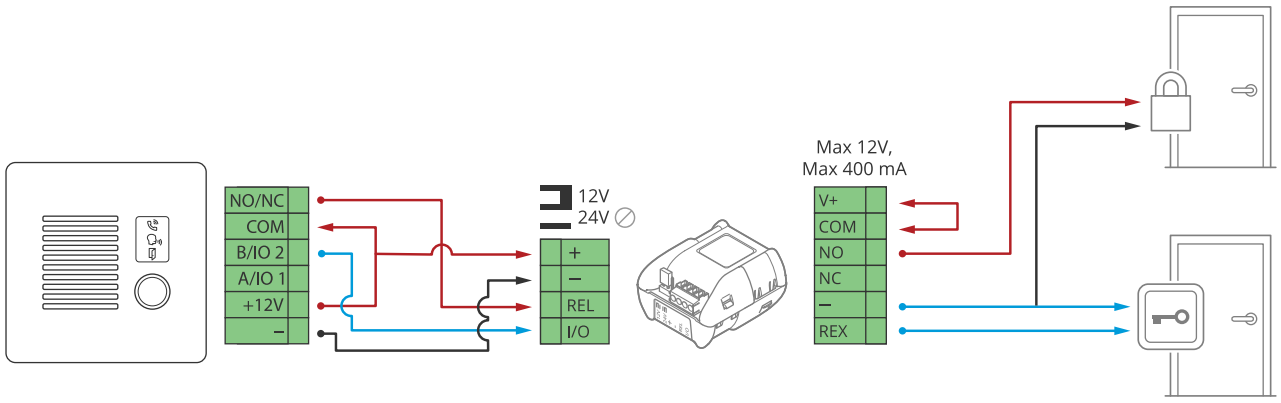
1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   - do zamka zabezpieczonego podczas awarii zasilania
   - do zamka zabezpieczonego

Przekaźnik bezpotencjałowy



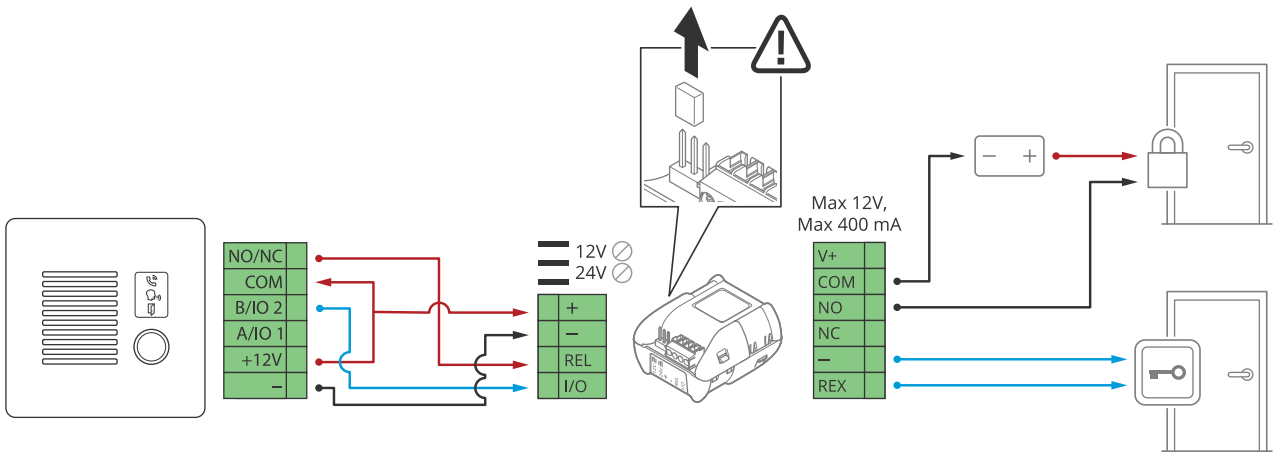
1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   - do zamka zabezpieczonego podczas awarii zasilania
   - do zamka zabezpieczonego

Bezpieczna blokada 12 V zasilana przez zasilacz PoE z interkomu



1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   - do zamka zabezpieczonego podczas awarii zasilania
   - do zamka zabezpieczonego

Bezpieczna blokada 12 V zasilana przez zasilacz zewnętrzny



1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   - do zamka zabezpieczonego podczas awarii zasilania

-  do zamka zabezpieczonego

Czyszczenie urządzenia

Urządzenie można czyścić letnią wodą z dodatkiem detergentów zawierających substancje wymienione niżej:

- Izopropanol 70% (IPA)
- Nadtlenek wodoru 3% (H_2O_2)
- Podchloryn sodu <5% (NaClO)

⚠UWAGA

Przed użyciem detergentu należy przeczytać jego etykietę i stosować się do podanych na niej zaleceń.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia acetonem ani benzyną.
- Nie należy rozpylać detergentu bezpośrednio na urządzenie. Detergent należy najpierw nanieść na miękką ściereczkę, a następnie przetrzeć nią urządzenie.
- Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawanie plam na obudowie.

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

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

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

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów na stronie 52*.
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
   - **Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej:** Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.

   Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej *axis.com/support*.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

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

Uwaga

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

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

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

Problemy techniczne, wskazówki i rozwiązania

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

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

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

Nie można uzyskać dostępu do urządzenia przez przeglądarkę

Nie można zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki.W razie utraty hasła dla konta root należy przywrócić ustawienia fabryczne urządzenia. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 61*.
Serwer DHCP zmienił adres IP	Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę).W razie potrzeby można przydzielić samodzielnie statyczny adres IP. Instrukcje można znaleźć na stronie *axis.com/support*.
Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X	Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w urządzeniu Axis muszą być zsynchronizowane z serwerem NTP. Wybierz kolejno opcje **System > Date and time (System > Data i godzina)**.

Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

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

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

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

Nie można połączyć przez port 8883 z MQTT przez SSL

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

Kwestie wydajności

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

Najważniejsze czynniki, które należy wziąć pod uwagę:

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

  W miarę możliwości używaj identycznych strumieni, aby utrzymać wysoką liczbę klatek na sekundę. Aby upewnić się, że strumienie są identyczne, możesz użyć profili strumieni.
- Jednoczesny dostęp do strumieni wideo z różnymi kodekami wpływa zarówno na poklatkowość, jak i na przepustowość. Aby uzyskać optymalną wydajność, należy używać strumieni z tym samym kodekiem.

- Intensywne korzystanie z ustawień zdarzeń wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.
- Korzystanie z protokołu HTTPS może zmniejszać liczbę klatek na sekundę, szczególnie w przypadku przesyłania strumieniowego obrazów wideo w formacie MJPEG.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Wyświetlanie obrazu z użyciem komputerów klienckich o niewystarczających parametrach obniża subiektywnie obserwowaną wydajność i wpływa na liczbę klatek na sekundę.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

Kontakt z pomocą techniczną

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

Informacje dotyczące bezpieczeństwa

Poziomy zagrożenia

⚠NIEBEZPIECZEŃSTWO

Wskazuje zagrożenie, które spowoduje zgon lub ciężkie obrażenia.

⚠OSTRZEŻENIE

Wskazuje zagrożenie, które może spowodować zgon lub ciężkie obrażenia.

⚠UWAGA

Wskazuje zagrożenie, które może spowodować niewielkie lub umiarkowane obrażenia.

POWIADOMIENIE

Wskazuje zagrożenie, które może spowodować uszkodzenie mienia.

Inne poziomy komunikatów

Ważne

Wskazuje istotne informacje niezbędne do poprawnego działania produktu.

Uwaga

Wskazuje przydatne informacje, które ułatwiają wykorzystanie możliwości produktu.

Podręcznik użytkownika
AXIS I7020 Network Intercom

Wer. M3.4
Data: Styczeń 2025
Nr katalogowy T10213215