AXIS D3110 Mk II Connectivity Hub

Podręcznik użytkownika

Informacje o rozwiązaniu

To urządzenie umożliwia integrację czujników i dźwięku z sieciowymi systemami wideo, które nie mają takich możliwości lub wymagają dodatkowych akcesoriów. Idealnie się sprawdza w kompleksowym rozwiązaniu firmy Axis, pomagając zwiększyć świadomość sceny bez narażania bezpieczeństwa sieci.

Jeżeli korzystasz z oprogramowania do zarządzania materiałem dźwiękowym i wizyjnym, to właśnie w nim można wygodnie skonfigurować urządzenie. Do sterowania systemem audio można używać następującego oprogramowania zarządzającego:

- **AXIS Audio Manager Edge** — oprogramowanie do zarządzania dźwiękiem dla małych systemów. Jest wstępnie instalowane na wszystkich urządzeniach audio z oprogramowaniem sprzętowym w wersji 10.0 i nowszych.
  - *Podręcznik użytkownika oprogramowania AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro** — zaawansowane oprogramowanie do zarządzania dźwiękiem w dużych systemach.
  - *Podręcznik użytkownika oprogramowania AXIS Audio Manager Pro*
- **AXIS Audio Manager Center** – usługa chmurowa umożliwiająca zdalny dostęp i zarządzanie systemami obejmującymi wiele lokalizacji.
  - *Podręcznik użytkownika oprogramowania AXIS Audio Manager Center*

Więcej informacji można znaleźć w temacie *Oprogramowanie do zarządzania materiałem dźwiękowym*.

Instalacja


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

Od czego zacząć

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

*Nie w pełni obsługiwane. W przypadku problemów ze strumieniowaniem wideo należy użyć innej przeglądarki.

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 .

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: .

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

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

Ważne

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

Bezpieczne hasła

Ważne

Używaj protokołu HTTPS (który jest domyślnie włączony), aby ustawić hasło lub skonfigurować inne poufne dane przez sieć. Protokół HTTPS umożliwia nawiązywanie bezpiecznych, szyfrowanych połączeń sieciowych, chroniąc w ten sposób poufne dane, takie jak hasła.

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

Aby chronić dane, zalecamy:

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

Upewnianie się co do braku zmian w oprogramowaniu urządzenia

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

1. Przywróć domyślne ustawienia fabryczne. Patrz .
   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 reguł dotyczących zdarzeń

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.

Wykrywanie ingerencji w sygnał wejściowy

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

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

Dodaj odbiorcę wiadomości e-mail:

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

Create a rule (Utwórz regułę):

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

Włączanie światła po otworzeniu okna

Ten przykład wyjaśnia, jak podłączyć kontakt okienny do koncentratora łączności i jak skonfigurować zdarzenie pod kątem włączania lampy po otwarciu okna z kontaktem.

Wymagania wstępne

- Podłącz dwuprzewodowy kabel (masa, WE/WY) do styku okna i do złącza WE/WY na koncentratorze połączeń.
- Podłącz lampę elektryczną do złącza przekaźnikowego w koncentratorze połączeń.

Konfiguracja portów WE/WY w koncentratorze łączności

1. Przejdź do menu **System > Accessories (System > Akcesoria)**.
2. Wprowadź następujące informacje w polu **Port 1**:
   - **Nazwa**: Window sensor (Czujnik okna)
   - **Direction (Kierunek)**: **Wejście**
   - **Normal state (Stan normalny)**: **Obwód zamknięty**
3. Wprowadź następujące informacje w polu **Port 2**:
   - **Nazwa**: Lamp (Lampa)
   - **Direction (Kierunek)**: **Wyjście**
   - **Normal state (Stan normalny)**: **Obwód otwarty**

Tworzenie dwóch reguł w centrum łączności

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Window sensor (Czujnik okna)
   - **Condition (Warunek)**: **Wejście cyfrowe**
     Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**
   - **Port**: **Window sensor (Czujnik okna)**
   - **Action (Akcja)**: **Przełącz I/O, gdy reguła jest aktywna**
   - **Port**: **Lamp (Lampa)**
   - **State (Stan)**: **Aktywne**
3. Kliknij przycisk **Zapisz**.

Aktywowanie centrum łączności przez MQTT po wykryciu ruchu przez kamerę

Wymagania wstępne

- Skonfiguruj urządzenie pod kątem portu WE/WY 1 w centrum łączności.
- Skonfiguruj brokera MQTT i uzyskaj adres IP oraz nazwę użytkownika i hasło brokera.
- Skonfiguruj w kamerze funkcję AXIS Motion Guard.

Konfigurowanie klienta MQTT w kamerze

1. W interfejsie urządzenia kamery przejdź do **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wprowadź następujące informacje:
   - **Host**: Adres IP brokera
   - **Client ID (Identyfikator klienta)**: Na przykład Kamera 1
   - **Protocol (Protokół)**: Protokół, na który jest ustawiony broker
   - **Port**: Numer portu używany przez brokera
   - **Username (nazwa użytkownika)** i **Password (hasło)** brokera
2. Kliknij **Save (Zapisz)** i **Connect (Połącz)**.

Tworzenie dwóch reguł w kamerze w celu publikacji MQTT

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Wykryto ruch
   - **Condition (Warunek)**: **Applications > Motion alarm (Aplikacje > Alarm ruchu)**
   - **Action (Akcja)**: **MQTT > Send MQTT publish message (Wyślij wiadomość o publikacji MQTT)**
   - **Topic (Temat)**: Ruch
   - **Payload (Próbka)**: Wł.
   - **QoS**: 0, 1 lub 2
3. Kliknij przycisk **Zapisz.**
4. Dodaj kolejną regułę z następującymi informacjami:
   - **Nazwa**: Brak ruchu
   - **Condition (Warunek)**: **Applications > Motion alarm (Aplikacje > Alarm ruchu)**
     - Wybierz opcję **Invert this condition (Odwróć ten warunek).**
   - **Action (Akcja)**: **MQTT > Send MQTT publish message (Wyślij wiadomość o publikacji MQTT)**
   - **Topic (Temat)**: Ruch
   - **Payload (Próbka)**: Wył.
   - **QoS**: 0, 1 lub 2
5. Kliknij przycisk **Zapisz.**

Konfigurowanie klienta MQTT w centrum łączności

1. W interfejsie urządzenia centrum łączności przejdź do **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wprowadź następujące informacje:
   - **Host**: Adres IP brokera
   - **Client ID (Identyfikator klienta)**: Port 1
   - **Protocol (Protokół)**: Protokół, na który jest ustawiony broker
   - **Port**: Numer portu używany przez brokera
   - **Username (Nazwa użytkownika)** i **Password (Hasło)**
2. Kliknij **Save (Zapisz)** i **Connect (Połącz).**
3. Przejdź do **MQTT subscriptions (Subskrypcje MQTT)** i dodaj subskrypcję.
   Wprowadź następujące informacje:
   - **Subscription filter (Filtr subskrypcyjny)**: Ruch
   - **Subscription type (Typ subskrypcji)**: Ze stanem
   - **QoS**: 0, 1 lub 2
4. Kliknij przycisk **Zapisz.**

Tworzenie reguły w centrum łączności w odniesieniu do subskrypcji MQTT

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Wykryto ruch
   - **Condition (Warunek)**: **MQTT > Stateful (Ze stanem)**
   - **Subscription filter (Filtr subskrypcyjny)**: **Ruch**
   - **Payload (Próbka)**: Wł.
   - **Action (Akcja)**: **I/O (WE/WY) > Toggle I/O while the rule is active (Przełącz WE/WY, gdy reguła jest aktywna)**
   - **Port**: I/O 1 (WE/WY 1).

3. Kliknij przycisk **Zapisz**.

Otwieranie zamka po naciśnięciu przycisku

Ten przykład wyjaśnia, jak podłączyć przekaźnik do koncentratora łączności i jak skonfigurować zdarzenie, aby zamek był otwierany, gdy ktoś naciśnie przycisk podłączony do koncentratora łączności.

Wymagania wstępne

- Podłącz dwuprzewodowy kabel (COM, NO) do zamka i do złącza przekaźnika na koncentratorze połączeń.
- Podłącz dwuprzewodowy kabel (masa, WE/WY) do przycisku i do złącza WE/WY na koncentratorze połączeń.

Konfiguracja portów WE/WY w koncentratorze łączności

1. Przejdź do menu **System > Accessories (System > Akcesoria)**.
2. Wprowadź następujące informacje w polu **Port 1**:
   - **Nazwa**: Przycisk
   - **Direction (Kierunek)**: **Wejście**
   - **Normal state (Stan normalny)**: **Obwód otwarty**
3. Wprowadź następujące informacje w polu **Port 9**:
   - **Nazwa**: Blokada
   - **Normal state (Stan normalny)**: **Obwód otwarty**

Tworzenie reguły w centrum łączności

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Nazwa**: Open lock (Zamek otwarty)
   - **Condition (Warunek)**: **I/O (WE/WY) > Digital input is active (Wejście cyfrowe jest aktywne)** Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**
   - **Port**: **Przycisk**
   - **Action (Akcja)**: **I/O (WE/WY) > Toggle I/O once (Przełącz raz WE/WY)**
   - **Port**: **Blokada**
   - **State (Stan)**: **Aktywne**
   - **Duration (Czas trwania):** 10 s
3. Kliknij przycisk **Zapisz**.

Dźwięk

Rejestracja dźwięku na karcie SD

W tym przykładzie pokazujemy, jak ustawić zapisywanie dźwięku z dwóch mikrofonów na karcie SD.

Zanim rozpoczniesz

- Podłącz dwa mikrofony i włóż jedną kartę microSD do urządzenia Connectivity Hub.

1. Przejdź do obszaru **Audio > Device settings (Ustawienia urządzenia)** i włącz opcje **Input 0: IN 1 (Wejście 0: WE 1)** oraz **Input 1: IN 2 (Wejście 1: WE 2)**.
2. Wybierz **Input type (Typ wejścia)** i **Power type (Typ zasilania)**.
3. Jeśli spodziewasz się, że poziom dźwięku będzie się różnił w zależności od pomieszczenia, włącz **Automatic gain control (Automatyczna regulacja wzmocnienia)**.
4. Przejdź do menu **System > Storage > Onboard storage (System > Zasób > Pamięć pokładowa)** i ustaw **Retention time (Czas przechowywania)**.

5. Przejdź do menu **Audio > Stream (Dźwięk > Przesyłanie strumieniowe)** i wybierz **Encoding (Kodowanie)**.

Uwaga

Aby utrzymać niski poziom obciążenia procesora podczas uruchamiania wielu strumieni (np. zapisywanie strumienia na żywo z tego samego źródła), ustaw takie samo kodowanie dla obydwu strumieni.

6. Przejdź do obszaru **Audio > Listen and record Słuchanie i nagrywanie)** i kliknij  .

7. Kliknij  .

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

Znajdź urządzenie

Pokazuje informacje o lokalizacji urządzenia, w tym numer seryjny i adres IP.

Locate device (Znajdź urządzenie): Pozwala odtwarzać dźwięk pomagający zidentyfikować głośnik. Na niektórych urządzeniach będą migać diody LED.

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:

Pokazuje lokalizację zapisu nagrania w zasobie.

Narzędzia analityczne

AXIS Audio Analytics

Adaptive audio detection (Adaptacyjna detekcja dźwięku): Włączenie tej opcji pozwala monitorować nagły wzrost głośności dźwięku w bezpośredniej bliskości urządzenia.

Ustawienia zaawansowane

- **Threshold (Próg)**: Ten suwak pozwala ustawić wartość progową detekcji. Przy minimalnej wartości progu nawet niewielkie zmiany głośności dźwięku będą rejestrowane jako zdarzenia detekcji, natomiast przy maksymalnej wartości progu jako detekcja zostanie sklasyfikowany tylko znaczący wzrost głośności dźwięku.
- **Test alarms (Testuj alarm)**: Kliknij przycisk **Test (Testuj)**, aby wyzwolić zdarzenie detekcji na potrzeby testowania.

Audio classification (Klasyfikacja dźwięku): Pozwala monitorować określone typy dźwięków wykrywanych w pobliżu urządzenia.

Ustawienia zaawansowane

- **Scream (Wrzask)**: Włączenie tej opcji powoduje aktywację detekcji wrzasku.
- **Shout (Krzyk)**: Włączenie tej opcji powoduje aktywację detekcji krzyku.
- **Glass break (Tłuczenie szkła)**: Włączenie tej opcji powoduje aktywację detekcji tłuczenia szkła.
- **Test alarms (Testuj alarm)**: Kliknij przycisk **Test (Testuj)**, aby wyzwolić detekcję typu dźwięku na potrzeby testowania.

Dźwięk

AXIS Audio Manager Edge

AXIS Audio Manager Edge: Pozwala uruchomić aplikację.

Zabezpieczenie lokalizacji audio

CA certificate (Certyfikat CA): Wybierz certyfikat, który będzie używany podczas dodawania urządzeń do lokalizacji audio. Konieczne jest włączenie uwierzytelniania TLS w aplikacji AXIS Audio Manager Edge.

Save (Zapisz): Pozwala aktywować i zapisać wybrane ustawienia.

Ustawienia urządzenia

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

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

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

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

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

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

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

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

Wyjście: Pokazuje typ urządzenia wyjściowego.

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

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

Strumień

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

Klipy audio

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

Rozpoczynanie odtwarzania klipu audio.

Zatrzymywanie odtwarzania klipu audio.

Menu kontekstowe zawiera opcje:

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

Nasłuchuj i nagrywaj

Kliknij, aby słuchać.

Włącz nagrywanie ciągłe strumienia audio na żywo. Kliknij przycisk ponownie, aby zatrzymać rejestrację. Jeżeli rejestrowanie jest w toku, po ponownym uruchomieniu kamery zostanie wznowione automatycznie.

Uwaga

Słuchanie i nagrywanie jest możliwe tylko wtedy, gdy w urządzeniu włączono wejście. Wybierz kolejno opcje **Audio > Device settings (Dźwięk > Ustawienia urządzenia)** i upewnij się, że wejście jest włączone.

Wyświetla zasób skonfigurowany dla urządzenia. Aby skonfigurować pamięć masową, należy zalogować się jako administrator.

Wzmocnienie dźwięku

Wejście

Dziesięciopasmowy graficzny korektor audio: Włącz tę opcję, aby regulować poziomy różnych zakresów częstotliwości sygnału audio. Ta funkcja jest przeznaczona dla zaawansowanych użytkowników mających doświadczenie w konfigurowaniu ustawień dźwięku.

Talkback range (Zasięg funkcji Talkback) : Wybierz zakres operacyjny zbierania materiału dźwiękowego. Zwiększenie zakresu operacyjnego ogranicza możliwości w zakresie jednoczesnej komunikacji dwukierunkowej.

Voice enhancement (Wzmocnienie głosu) : Włącz tę opcję, aby wzmocnić głośność komunikatów głosowych w odniesieniu do innych dźwięków.

Nagrania

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

● Wybierz, aby rozpocząć nagrywanie w urządzeniu.

Wybierz docelowy zasób, w którym chcesz zapisać nagrania.

● Zatrzymaj nagrywanie w urządzeniu.

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

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

Odtwórz nagranie.

Zatrzymaj odtwarzanie nagrania.

Wyświetl lub ukryj informacje i opcje nagrania.

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

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

Kliknij, aby usunąć nagranie.

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

Kliknij, aby filtrować nagrania.

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

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

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

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

Pamięć masowa: Pokazuje nagrania z podziałem na typy zasobów.

Aplikacje

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

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

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

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.

- **Format (Formatuj)**: Wybierz format, który ma być używany przy wprowadzaniu szerokości i długości geograficznej urządzenia.
- **Latitude (Szerokość geograficzna)**: Wartości dodatnie to szerokość geograficzna na północ od równika.
- **Longitude (Długość geograficzna)**: Wartości dodatnie to długość geograficzna na wschód od południka zerowego.
- **Kierunek**: Wprowadź kierunek (stronę świata), w który skierowane jest urządzenie. 0 to północ.
- **Etykieta**: Wprowadź opisową nazwę urządzenia.
- **Save (Zapisz)**: Kliknij, aby zapisać lokalizację urządzenia.

Sieć

IPv4

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

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

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

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

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

Uwaga

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

IPv6

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

Nazwa hosta

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

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

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

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

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

Serwery DNS

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

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

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

HTTP i HTTPS

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

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

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

Uwaga

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

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

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

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

Protokoły wykrywania sieci

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

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

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

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

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

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

Globalne serwery proxy

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

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

Dozwolone formaty serwerów proxy HTTP i HTTPS:

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

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

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

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

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

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

Allow O3C (Zezwalaj na O3C):

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

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

Host: Wprowadź adres serwera proxy.

Port: wprowadź numer portu służącego do uzyskania dostępu.

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

Authentication method (Metoda uwierzytelniania):

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

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

SNMP

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

SNMP: Wybierz wersję SNMP.

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

Uwaga

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

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

Bezpieczeństwo

Certyfikaty

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

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

Obsługiwane są następujące formaty:

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

Ważne

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

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

- **More (Więcej)** : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Trusted Execution Environment (SoC TEE)**, **Secure element (Bezpieczny element)** lub **Trusted Platform Module 2.0 (Moduł TPM 2.0)** do bezpiecznego przechowywania klucza prywatnego. Aby uzyskać więcej informacji na temat bezpiecznego magazynu kluczy, odwiedź stronę *help.axis.com/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) :

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

Polityka kryptograficzna

Polityka kryptograficzna definiuje sposób używania szyfrowania do ochrony danych.

Active (Aktywne): Wybierz politykę kryptograficzną, którą chcesz zastosować do urządzenia:

- **Default — OpenSSL (Domyślnie — OpenSSL)**: Równowaga między bezpieczeństwem i wydajnością do użytku ogólnego.
- **FIPS — Policy to comply with FIPS 140–2 (FIPS — Polityka zgodna z FIPS 140–2)**: Szyfrowanie zgodne ze standardem FIPS 140-2 na potrzeby branż regulowanych.

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certyfikaty

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

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

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

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

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

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

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

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

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

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

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

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

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

Zapobiegaj atakom typu brute force

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

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

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

Zapora

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)**: Nie może zmieniać ustawień.

Menu kontekstowe zawiera opcje:

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

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

Anonimowy dostęp

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

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

Konta SSH

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

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Uwaga: Wprowadź komentarz (opcjonalnie).

Menu kontekstowe zawiera opcje:

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

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

Virtual host (Host wirtualny)

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

Włączony: zaznaczenie tej opcji spowoduje używanie tego wirtualnego hosta.

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

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

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

Menu kontekstowe zawiera opcje:

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

Disabled (Wyłączono): Serwer jest wyłączony.

Konfiguracja OpenID

Ważne

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

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

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

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

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

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

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

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

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

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

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

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

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

Zdarzenia

Reguły

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

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.

Nazwa: Wprowadź nazwę reguły.

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

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

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

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

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

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

Odbiorcy

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

Uwaga

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

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

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

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

Nazwa: Wprowadź nazwę odbiorcy.

Type (Typ): Wybierz z listy:

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

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

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

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

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

Uwaga

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

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

Test (Testuj): Kliknij, aby przetestować konfigurację.

⋮ Menu kontekstowe zawiera opcje:

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

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

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

Harmonogramy

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

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

Wyzwalacze ręczne

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

MQTT

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

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

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

ALPN

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

Klient MQTT

Connect (Połącz): włącz lub wyłącz klienta MQTT.

Status (Stan): pokazuje bieżący status klienta MQTT.

Broker

Host: wprowadź nazwę hosta lub adres IP serwera MQTT.

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

Port: Wprowadź numer portu.

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

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

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

Hasło: wprowadzić hasło dla nazwy użytkownika.

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

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

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

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

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

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

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

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

Komunikat łączenia

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

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

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

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

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

QoS: zmiana warstwy QoS dla przepływu pakietów.

Wiadomość Ostatnia Wola i Testament

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

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

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

Topic (Temat): wprowadź temat wiadomości domyślnej.

Payload (Próbka): wprowadź treść wiadomości domyślnej.

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

QoS: zmiana warstwy QoS dla przepływu pakietów.

Publikacja MQTT

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

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

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

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

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

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

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

QoS: Wybierz żądany poziom publikacji MQTT.

Subskrypcje MQTT

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

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

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

Subscription type (Typ subskrypcji):

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

QoS: Wybierz żądany poziom subskrypcji MQTT.

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.
- **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.

Dodatkowe

- **UDP-to-TCP switching (Przełączanie UDP–TCP)**: Wybierz, aby umożliwić tymczasowe przełączenie protokołu transmisji z UDP (User Datagram Protocol) na TCP (Transmission Control Protocol).

Przełączanie przydaje się w celu uniknięcia fragmentacji; przełączenie jest możliwe w zakresie 200 bajtów MTU lub więcej niż 1300 bajtów MTU.

- **Allow via rewrite (Umożliwiaj przepisanie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Allow contact rewrite (Umożliwiaj przepisanie przy kontakcie)**: Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
- **Register with server every (Rejestruj na serwerze co)**: Ustaw częstotliwość rejestrowania się urządzenia na serwerze SIP dla istniejących kont SIP.
- **DTMF payload type (Typ próbki DTMF)**: Zmienia domyślny typ próbki na DTMF.
- **Maksymalna liczba retransmisji**: Ustaw maksymalną liczbę prób nawiązywania przez urządzenie połączenia z serwerem SIP, zanim urządzenie zrezygnuje.
- **Sekundy do odblokowania awaryjnego**: Ustaw liczbę sekund, po której urządzenie spróbuje ponownie się połączyć z głównym serwerem SIP po awaryjnym przełączeniu na dodatkowy serwer SIP.

Konta

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

Konto zostało zarejestrowane na serwerze SIP.

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

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

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

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

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

DTMF

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

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

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

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

Protokoły

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

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

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

Połączenie testowe

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

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

Lista dostępu

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

Policy (Zasada):

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

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

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

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.

Przechowywanie

Sieciowa pamięć masowa

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

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

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

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

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

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

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

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

Narzędzia

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

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

Pamięć pokładowa

Ważne

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

Odmontuj: Kliknij w celu bezpiecznego usunięcia karty SD.

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

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

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

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

Narzędzia

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

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

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

ONVIF

To urządzenie nie obsługuje profili ONVIF.

Detektory

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.

Akcesoria

Porty we/wy

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

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

Port

Nazwa: edytuj tekst, aby zmienić nazwę portu.

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

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

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

Uwaga

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

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

Konfiguracja USB

Enable on reboot (Włącz przy ponownym uruchomieniu): Włącz, aby aktywować funkcję USB. Uruchom ponownie urządzenie, aby zastosować zmiany.

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

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

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

Host: Wprowadź nazwę hosta lub adres IP serwera.

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

- Axis
- RFC 3164
- RFC 5424

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

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

Port: Wpisywanie innego numeru portu w miejsce obecnego.

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

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

Reset PTR (Resetuj PTR) : Opcji Reset PTR (Resetuj PTR) należy użyć w sytuacji, gdy z jakiegoś powodu ustawienia **Pan (Obrót)**, **Tilt (Pochylenie)** i **Roll (Przechylenie)** nie działają w oczekiwany sposób. W nowej kamerze silniczki układu PTR są zawsze skalibrowane. Jednak kalibracja może zostać utracona, na przykład w razie odcięcia zasilania kamery lub ręcznego przestawienia kamery w którymś kierunku. Po zresetowaniu ustawień PTR kamera jest ponownie kalibrowana i wraca do położenia fabrycznego.

Calibration (Kalibracja) : Kliknij **Calibrate (Kalibruj)**, aby zrekalibrować silniki obrotu, pochylenia i przechylenia do pozycji domyślnych.

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

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*.

AXIS Audio Analytics

Aplikacja AXIS Audio Analytics wykrywa nagły wzrost głośności dźwięku oraz rozpoznaje typy dźwięków, takie jak wrzaski lub strzały, w zasięgu urządzenia, na którym jest zainstalowana. Funkcje detekcji można skonfigurować tak, aby powodowały wyzwolenie określonej reakcji, np. uruchomienie nagrywania wideo, odtworzenie komunikatu głosowego lub powiadomienie pracowników ochrony. Aby dowiedzieć się więcej o działaniu aplikacji, zapoznaj się z *instrukcją użytkownika AXIS Audio Analytics*.

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*.

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

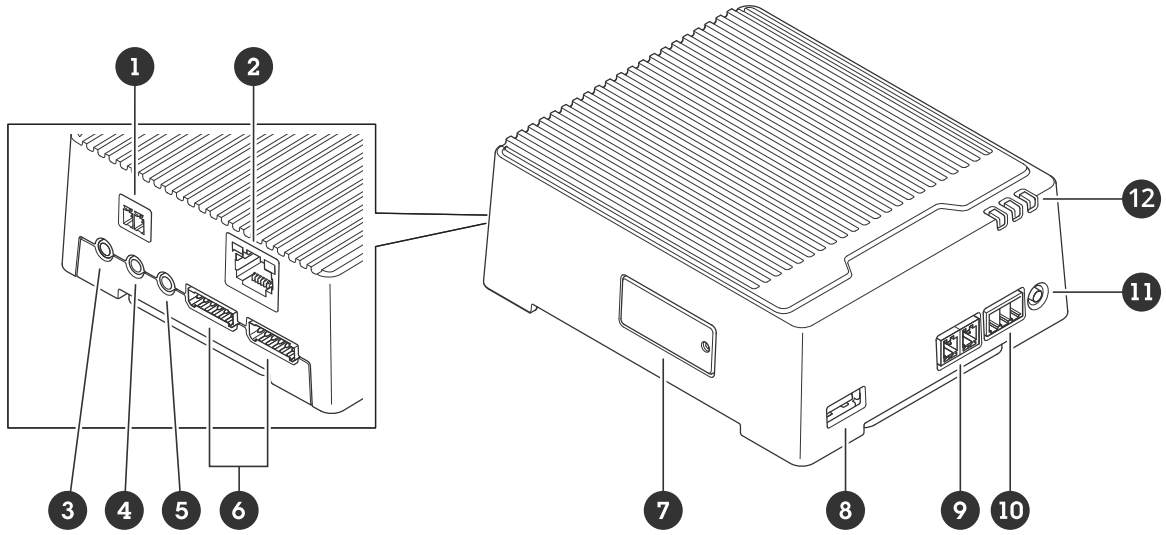
Aby maksymalnie ograniczyć narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania 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. Aby dowiedzieć się więcej o podejściu Axis do cyberbezpieczeństwa, w tym o najlepszych praktykach, zasobach i wytycznych dotyczących zabezpieczania urządzeń, odwiedź stronę *https://www.axis.com/about-axis/cybersecurity*.

Specyfikacje

Przegląd produktów



1 *Złącze zasilania*
2 *Złącze RJ45 ethernet*
3 *Port 2 mikrofonu (analogowy)*
4 *Port 1 mikrofonu (cyfrowy i analogowy)*
5 *Wyjście audio*
6 *2 złącza WE/WY (6-pinowe)*
7 *Gniazdo kart microSD*
8 *Port USB*
9 *Złącze RS485/RS422*
10 *Złącze przekaźnikowe*
11 *Przycisk kontrolny*
12 *Dioda stanu*

Gniazdo karty SD

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

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

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz .
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby nawiązać połączenie, naciśnij i zwolnij przycisk, a następnie poczekaj, aż dioda LED stanu mignie trzy razy na zielono.

Złącza

Złącze sieciowe

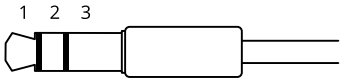
Złącze RJ45 Ethernet.

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

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

Złącze audio

- **Wejście audio** (port 1 mikrofonu) – wejście 3,5 mm dla mikrofonu cyfrowego, analogowego mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).
- **Wejście audio** (port 2 mikrofonu) – wejście 3,5 mm dla analogowego mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).
- **Wyjście audio** – wyjście audio 3,5 mm (poziom linii), które można podłączyć do systemu nagłośnienia (PA) lub aktywnego głośnika z wbudowanym wzmacniaczem. Można do niego również podłączyć słuchawki. Do wyjścia audio musi być użyte złącze stereo.



Wejście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Niezbalansowany mikrofon (z zasilaniem elektretowym lub bez) lub wejście liniowe	Zasilanie elektretowe po wybraniu	Masa
Zbalansowany mikrofon (z zasilaniem fantomowym lub bez) lub wejście linowe, sygnał „gorący"	Zbalansowany mikrofon (z zasilaniem fantomowym lub bez) lub wejście linowe, sygnał „zimny"	Masa
Sygnał cyfrowy	Zasilanie z obwodu pierścieniowego po wybraniu	Masa

Wyjście audio

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

Złącze I/O

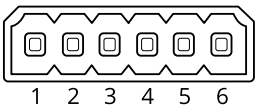
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

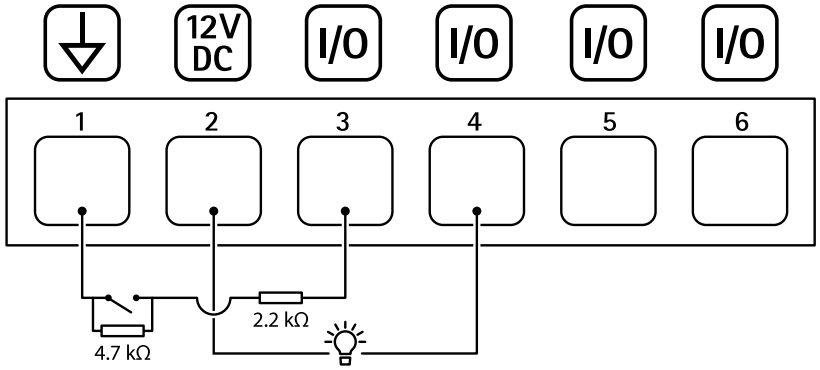
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

6-pinowego bloku złączy



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

Przykład:



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

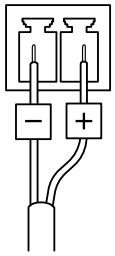
Specyfikacja projektu elektrycznego dla cyfrowego We/Wy

Parametr	Wartość
Minimalne dopuszczalne napięcie wejściowe	-30 V DC
Maksymalne dopuszczalne napięcie wejściowe	+30 V DC
Maksymalne niskie napięcie wejścia cyfrowego	+0,50 V przy 25°C +0,40 V przy 85°C
Minimalne wysokie napięcie wejścia cyfrowego	+1,5 V

Maksymalne niskie napięcie wyjścia przy 100 mA	+0,6 V
Maksymalne niskie napięcie wyjścia przy 10 mA	+0,06 V
Maksymalny czas narastania (uwzględniający opóźnienie z GPIO) przy 10 kHz	5 µs
Maksymalny czas opadania (uwzględniający opóźnienie z GPIO) przy 10 kHz	5 µs
Maksymalny prąd upływu wyjścia	100 mA
Maksymalny prąd upływu We/Wy	100 µA przy 12 V DC

Złącze zasilania

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

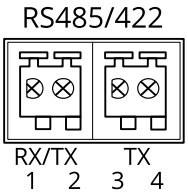


Złącze RS485/RS422

Dwa 2-stykowe bloki złączy interfejsu szeregowego RS485/RS422

Port szeregowy można skonfigurować do obsługi następujących funkcji:

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



Funkcje	Styk	Uwagi
RS485/RS422 RX/TX A	1	(RX) Full duplex RS485/RS422 (RX/TX) Half duplex RS485
RS485/RS422 RX/TX B	2	
RS485/RS422 TX A	3	(TX) Full duplex RS485/RS422
RS485/RS422 TX B	4	

Czyszczenie urządzenia

Urządzenie można czyścić letnią wodą.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
- 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 wyczyścić urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą.
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 .
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: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie. • Jeśli otrzymasz: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Nie można uzyskać dostępu do urządzenia przez przeglądarkę

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

Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

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

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

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

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

Najważniejsze czynniki, które należy wziąć pod uwagę:

- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Jednoczesne uruchamianie wielu działań może wpłynąć na wydajność dźwięku.

Kontakt z pomocą techniczną

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

T10208737_pl

2025-05 (M4.10)