

Czujnik jakości powietrza AXIS D6310 Air Quality Sensor

Podręcznik użytkownika

Spis treści

Instalacja.....	4
Od czego zacząć.....	5
.....	5
Wyszukiwanie urządzenia w sieci.....	5
Obsługiwane przeglądarki.....	5
Otwórz interfejs WWW urządzenia.....	5
Utwórz konto administratora.....	5
Bezpieczne hasła.....	6
Upewnianie się co do braku zmian w oprogramowaniu urządzenia	6
Konfiguracja urządzenia	7
Konfigurowanie monitora jakości powietrza.....	7
Konfiguracja pulpitu nawigacyjnego czujnika jakości powietrza	7
Ustawienia czujnika jakości powietrza	8
Pobieranie statystyki danych z czujnika.....	9
Kalibracja przy pierwszym uruchomieniu urządzenia	9
Konfiguracja profilu.....	9
Konfiguracja profilu z niestandardowym plikiem audio syreny	10
Importowanie/eksportowanie profilu	10
Konfiguracja bezpośredniego połączenia SIP (P2P)	10
Konfiguracja SIP przez serwer (PBX).....	11
Konfiguracja reguł dotyczących zdarzeń	11
Wyzwalanie akcji.....	12
Zapisywanie obrazu po wykryciu palenia	12
Odtwórz klip audio w przypadku zbyt wysokiego poziomu CO2	12
Włącz profil optyczny i akustyczny za pomocą czujki PIR	13
Uruchamianie profilu po wyzwoleniu alarmu	13
Uruchamianie profilu przy użyciu protokołu SIP	14
Sterowanie kilkoma profilami za pomocą rozszerzeń SIP	14
Uruchamianie dwóch profili o różnych priorytetach.....	15
Uaktywnij profil optyczny i akustyczny przez żądanie HTTP post, gdy kamera wykryje ruch	15
Uaktywnij profil optyczny i akustyczny poprzez wejście wirtualne, gdy kamera wykryje ruch	17
Uaktywnij profil optyczny i akustyczny przez protokół MQTT, gdy kamera wykryje ruch	18
Wysyłanie wiadomości e-mail w razie niepowodzenia testu głośnika.....	19
Odtwarzanie niestandardowego klipu po wyzwoleniu alarmu	20
Zatrzymywanie nadawania audio za pomocą DTMF	21
Konfigurowanie dźwięku dla przychodzących połączeń SIP.....	22
Interfejs WWW.....	23
Status.....	23
Nagranie wideo.....	24
Strumień	24
Czujnik jakości powietrza	25
Pulpit nawigacyjny	25
Ustawienia.....	29
Statystyki	31
Narzędzia analityczne.....	31
AXIS Audio Analytics.....	31
Dźwięk.....	32
Ustawienia urządzenia	32
Strumień	33
Klipy audio.....	33
Wzmocnienie dźwięku.....	33
Informacje ogólne	33
Profile.....	34

Nagrania	36
Media	37
Aplikacje	37
System	38
Czas i lokalizacja	38
Sieć	40
Bezpieczeństwo	44
Konta	49
Zdarzenia	52
MQTT	57
SIP	60
Przechowywanie	65
Profile strumienia	66
ONVIF	67
Detektory	70
Ustawienia zasilania	70
Akcesoria	70
Dzienniki	71
Zwykła konfiguracja	72
Konserwacja	73
Konserwacja	73
Rozwiązywanie problemów	74
Specyfikacje	75
Przegląd produktów	75
.....	75
Dioda stanu	76
Przyciski	76
Przycisk kontrolny	76
Przełącznik mikrofonu	76
Złącza	76
Złącze sieciowe	76
Złącze I/O	76
Złącze RS485/RS422	77
Nazwy wzorów świateł	78
Nazwy sposobów sygnalizacji w sygnalizatorze akustyczno-optycznym	78
Czyszczenie urządzenia	80
Rozwiązywanie problemów –	81
Przywróć domyślne ustawienia fabryczne	81
Problemy techniczne, wskazówki i rozwiązania	81
Kwestie wydajności	82
Kontakt z pomocą techniczną	83

Instalacja

Ważne

- Zachowaj odległość co najmniej 1,5 m (4,9 stopy) od miejsc, w których znajdują się większe otwory wentylacyjne lub źródła zanieczyszczeń. Chodzi o otwory, drzwi, okna, strefy gotowania posiłków itp.
- Zainstaluj urządzenie w miejscu umożliwiającym swobodny przepływ powietrza.
- W celu zapewnienia skutecznego wykrywania dymu tytoniowego lub z papierosów elektronicznych urządzenie należy zainstalować na suficie na wysokości 2,4 - 2,7 m (7,9 - 8,9 stóp) od podłogi.
- W celu zapewnienia skutecznego monitorowania jakości powietrza i otoczenia urządzenie należy zainstalować na wysokości 0,9 - 1,8 m (3,0 - 5,9 stóp) od podłogi.

Proces instalacji opisany jest szczegółowo w instrukcji instalacji.

Od czego zacząć

▲ OSTRZEŻENIE

Błyskające lub migoczące światła mogą wywołać napady u osób z padaczką światłoczułą.

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

✓: zalecane

*: obsługiwane z ograniczeniami

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.

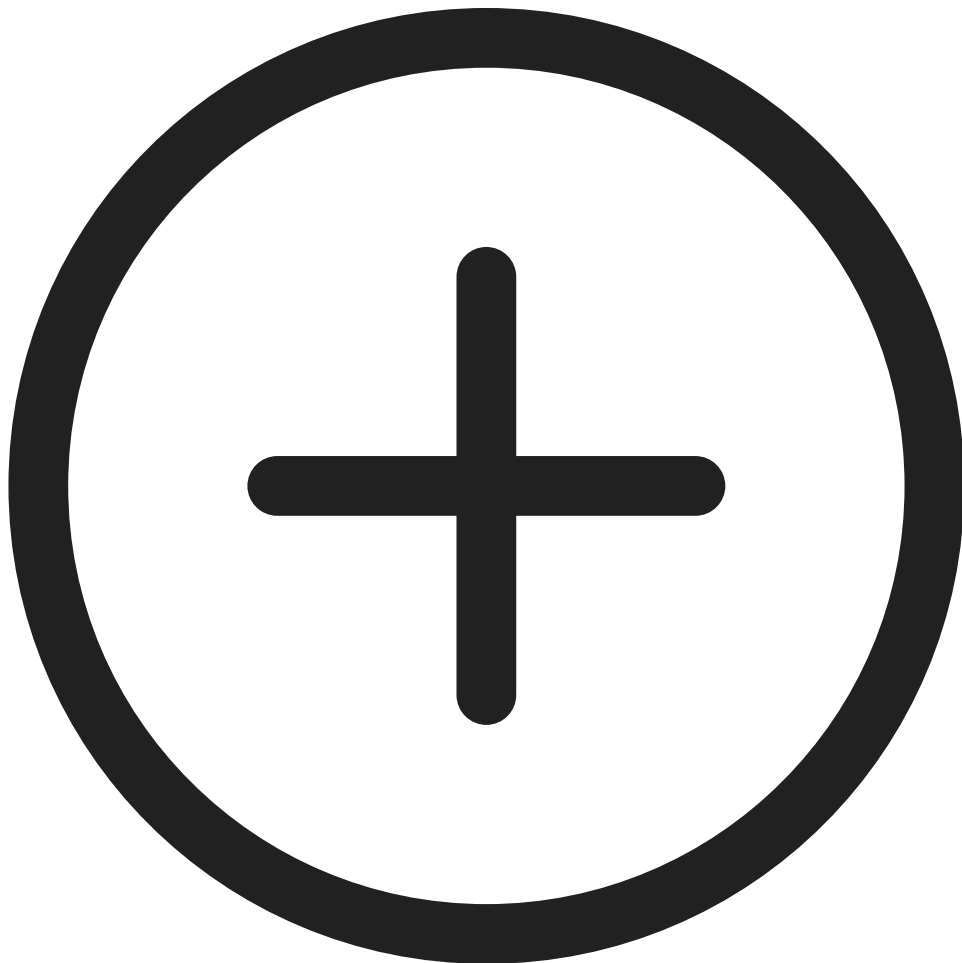
Konfiguracja urządzenia

Konfigurowanie monitora jakości powietrza

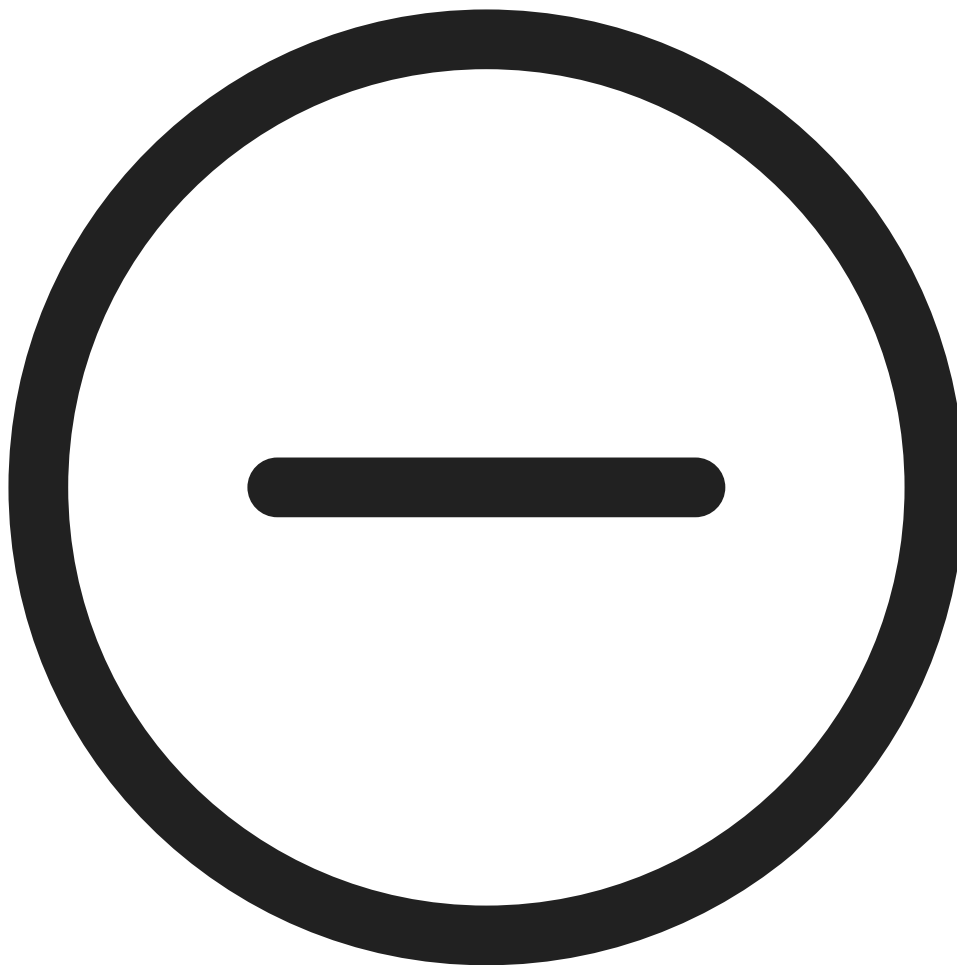
Konfiguracja pulpitu nawigacyjnego czujnika jakości powietrza

Na stronie sieciowej urządzenia przejdź do Air quality monitor > Dashboard (Monitor jakości powietrza > Pulpit nawigacyjny).

- Aby edytować nazwę pulpitu nawigacyjnego, kliknij  z lewej strony.
- Aby wyświetlić dane na pulpicie nawigacyjnym, kliknij  Edit (Edytuj) >



- Aby ukryć dane na pulpicie nawigacyjnym, kliknij  Edit (Edytuj) >



Ustawienia czujnika jakości powietrza

Na stronie sieciowej urządzenia przejdź do **Air quality sensor > Settings** (Czujnik jakości powietrza > Ustawienia).

- Ustaw wartości progowe temperatury, wilgotności, CO₂, NO_x, PM_{1.0}, PM_{2.5}, PM_{4.0}, PM_{10.0}, LZ0 i AQI, p. sekcja .
- Ustaw jednostki temperatury, p. sekcja .
- Ustaw czułość detekcji dymu z papierosów elektronicznych, p. sekcja .
- Ustaw czas przechowywania w pamięci masowej, p. sekcja .
- Ustaw częstotliwość metadanych w chmurze, p. sekcja .
- Ustaw okres weryfikacji, p. sekcja .

Pobieranie statystyki danych z czujnika

Można wyeksportować dane statystyczne z czujnika z okresu do 365 dni wstecz do pliku CSV, aby wykorzystać je w aplikacjach w rodzaju Microsoft® Excel.

1. Na stronie sieciowej urządzenia przejdź do **Air quality monitor > Statistics > Sensor Data Statistics** (Monitor jakości powietrza > Statystyki > Statystyki danych z czujnika).
2. Wybierz zakres dat:
 - **Custom range** (Zakres niestandardowy): W sekcji **From** (Od) i **To** (Do) wybierz datę początkową i datę końcową (do 365 dni).
 - **Predefined range** (Zakres zdefiniowany): Na liście **Predefined date range** (Zdefiniowany zakres dat) wybierz dostępny okres.

Uwaga

W razie wyboru obu zakresów, niestandardowego i zdefiniowanego, pierwszeństwo ma zakres niestandardowy.

Uwaga

Maksymalny zakres pobierania jest ograniczony czasem przechowywania danych ustawionym w .

3. Na liście **Source** (Źródło) wybierz źródło; aby wyeksportować dane ze wszystkich źródeł, kliknij **Download all data** (Wyeksportuj wszystkie dane).
4. Kliknij **Download data** (Pobierz dane), aby wyeksportować statystykę.

Uwaga

Kliknij **Download all data** (Pobierz wszystkie dane), aby wyeksportować dane dla wszystkich źródeł w wybranym przedziale czasowym.

Kalibracja przy pierwszym uruchomieniu urządzenia

Uwaga

- Pełną dokładność pomiaru stężenia CO₂ uzyskuje się po 2 dniach od pierwszego uruchomienia urządzenia.
- Przy pierwszym uruchomieniu urządzenia do ustalenia właściwych wskazań AQI (wskaźnika jakości powietrza) potrzeba 12 godzin. Wskaźnik AQI będzie wyświetlany na stronie **Calculating** (Obliczenia) do momentu uzyskania wystarczającej ilości danych. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.
- Pełną dokładność pomiaru LZO uzyskuje się po godzinie od momentu uruchomienia urządzenia. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.
- Pełną dokładność pomiaru NO_x uzyskuje się po 6 godzinach od momentu uruchomienia urządzenia. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.

Konfiguracja profilu

Profil to zbiór określonych ustawień konfiguracyjnych. Można mieć maksymalnie 30 profili z różnymi priorytetami i wzorami.

Aby ustawić nowy profil:

1. Przejdź do obszaru **Profiles (Profile)** i kliknij opcję  **Create (Utwórz)**.
2. Wypełnij pola **Name (Nazwa)** i **Description (Opis)**.
3. Wybierz ustawienia dla opcji **Light** (Oświetlenie) i **Siren** (Syrena), które będą używane w profilu.
4. Ustaw **Priority** (Priorytet) dla oświetlenia i syreny, a następnie kliknij przycisk **Save** (Zapisz).

Aby edytować profil, kliknij  i wybierz opcję **Edit (Edytuj)**.

Konfiguracja profilu z niestandardowym plikiem audio syreny

Istnieje możliwość skonfigurowania profilu z niestandardowym plikiem audio. W urządzeniu można zapisać pliki audio o rozmiarze do 100 Mb. W przypadku większych plików audio należy używać karty SD, o ile urządzenie jest wyposażone w złącze karty SD.

Prześlij plik audio:

1. Przejdź do menu **Media** i kliknij przycisk  **Add (Dodaj)**.
2. Wyszukaj i wybierz plik z komputera.
3. Wybierz **Storage location (Lokalizacja pamięci masowej)**.
4. Kliknij przycisk **Zapisz**.

Aby użyć pliku audio w profilu:

1. Przejdź do strony **Profiles (Profile)** i utwórz profil. Więcej informacji można znaleźć na stronie .
2. Podczas konfiguracji syreny wybierz przesłany plik audio jako **Pattern (Wzór)**.

Importowanie/eksportowanie profilu

Aby użyć wstępnie skonfigurowanego profilu, możesz go zaimportować:

1. Przejdź do obszaru **Profiles (Profile)** i kliknij opcję  **Import (Importuj)**.
2. Przejdź do lokalizacji pliku lub przeciągnij i upuść plik, który chcesz zaimportować.
3. Kliknij przycisk **Zapisz**.

Można także wyeksportować profile w celu ich skopiowania i zapisania na innych urządzeniach:

1. Wybierz **Profile**.
2. Kliknij **Export (Eksportuj)**.
3. Przeglądaj, aby zlokalizować pliki. JSON.

Konfiguracja bezpośredniego połączenia SIP (P2P)

Konfiguracji P2P należy używać wtedy, gdy komunikacja odbywa się pomiędzy niewielką liczbą agentów użytkownika w tej samej sieci IP i nie ma potrzeby zapewniania dodatkowych funkcji serwera PBX. Aby lepiej zrozumieć sposób działania P2P, zobacz .

Więcej informacji na temat wartości ustawień: .

1. Przejdź do menu **System > SIP > SIP settings (Ustawienia SIP)** i wybierz opcję **Enable SIP (Włącz SIP)**.
2. Aby zezwolić urządzeniu na odbieranie połączeń, wybierz opcję **Zezwalaj na połączenia przychodzące**.
3. W polu **Call handling (Obsługa połączeń)** ustaw limit czasu i czas trwania połączenia.
4. W ustawieniu **Ports (Porty)** wprowadź numery portów.
 - **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.
 - **TLS port (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** – wprowadź port używany do pierwszego strumienia mediów RTP w wywołaniu SIP. Domyślnym portem początkowym na potrzeby transportu multimediów jest port

4000. Niektóre zapory mogą blokować ruch RTP na określonych numerach portów. Numer portu musi należeć do przedziału od 1024 do 65535.

- Wybierz protokoły, które chcesz włączyć dla funkcji **NAT traversal**.

Uwaga

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

- W ustawieniu **Audio (Dźwięk)** wybierz co najmniej jeden kodek audio z żadaną jakością dźwięku na potrzeby połączeń SIP. W celu zmiany kolejności priorytetów przeciągnij i upuść w inne miejsca.
- W obszarze **Additional (Dodatkowe)** wybierz dodatkowe opcje.
 - 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 (Umożliwianie przepisywania)** – Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
 - Allow contact rewrite (Umożliwianie przepisywania 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.
- Kliknij przycisk **Zapisz**.

Konfiguracja SIP przez serwer (PBX)

Użyj serwera PBX, gdy agenci użytkowników będą komunikować się w sieci IP i poza nią. W zależności od dostawcy usługi PBX można dodać dodatkowe funkcje. Aby lepiej zrozumieć sposób działania P2P, zobacz .

Więcej informacji na temat wartości ustawień: .

- Od dostawcy PBX należy uzyskać następujące informacje:
 - ID użytkownika
 - Domena
 - Hasło
 - ID uwierzytelniania
 - ID rozmówcy
 - Rejestrator
 - Port początkowy RTP
- Aby dodać nowe konto, przejdź do okna **System > SIP > SIP accounts (Konta SIP)** i kliknij przycisk **+ Account (+ Konto)**.
- Wprowadź informacje otrzymane od dostawcy usług centrali telefonicznej (PBX).
- Kliknij opcję **Registered (Zarejestrowane)**.
- Wybierz tryb transmisji.
- Kliknij przycisk **Zapisz**.
- Skonfiguruj ustawienia SIP w taki samo sposób, jak peer-to-peer. Więcej informacji: .

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.

Zapisywanie obrazu po wykryciu palenia

Poniższy przykład wyjaśnia sposób skonfigurowania czujnika jakości powietrza do zapisu obrazu w sieciowej pamięci masowej po wykryciu przez czujnik jakości powietrza dymu z papierosa elektronicznego.

1. Na stronie sieciowej czujnika jakości powietrza przejdź do **Settings > System > Storage (Ustawienia > System > Pamięć masowa)**, aby sprawdzić, czy jest ustawiona sieciowa pamięć masowa.
2. Przejdź do menu **Settings > System > Events (Ustawienia > System > Zdarzenia)** i dodaj regułę. Wprowadź następujące informacje:
 - **Nazwa:** Wprowadź nazwę reguły.
 - **Condition (Warunek):** **Air quality monitor > Vaping or smoking detected (Monitor jakości powietrza > Wykrywanie palenia papierosów elektronicznych lub tytoniu).**
 - **Action (Działanie) :** **Recordings > Record video (Nagrania > Zapisuj obraz).**
 - **Pamięć masowa:** **Network storage (Sieciowa pamięć masowa).** Sprawdź, czy sieciowa pamięć masowa jest skonfigurowana.
 - **Kamera:** Wybierz obszar obserwacji z kamery.
 - **Stream profile (Profil strumienia):** Wybierz profil strumieniowania lub **Create a stream profile (Utwórz profil strumieniowania).**
 - **Prebuffer (Bufor przed zdarzeniem) i Postbuffer (Bufor po zdarzeniu):** Ustaw potrzebne wartości.
3. Kliknij przycisk **Zapisz**.

Odtwórz klip audio w przypadku zbyt wysokiego poziomu CO2

W tym przykładzie wyjaśniono, jak odtworzyć klip audio w przypadku zbyt wysokiego poziomu CO2.

Tworzenie reguły

1. Na stronie sieciowej przejdź do **Events > Rules > Add a rule (Zdarzenia > Reguły > Dodaj regułę)**, aby utworzyć regułę.
2. Wprowadź następujące informacje:
 - **Nazwa:** Wprowadź nazwę reguły.
 - **Warunki:** **Air quality monitor > Air quality outside acceptable range (Monitor jakości powietrza > Jakość powietrza poza dopuszczalnym zakresem)**
 - **Sensor (Czujnik):** **CO2**
 - **Action (Akcja):** **Odtwórz klip audio**
 - **Clip (Klip):** wybierz klip audio.
3. Kliknij przycisk **Zapisz**.

Ustawienie zakresu alarmowego dla CO2

- Na stronie sieciowej przejdź do **Air quality monitor > Settings > CO2 (Monitor jakości powietrza > Ustawienia > CO2).**

- Wpisz wartości **MIN** (MIN.) i **MAX** (MAKS.), aby ustawić zakres CO2.

Włącz profil optyczny i akustyczny za pomocą czujki PIR

W tym przykładzie wyjaśniono, jak włączyć profil optyczny i akustyczny za pomocą czujki PIR. Pozycje optyczne (sygnalizacyjne diody LED) i akustyczne znajdują się na stronie .

Utwórz profil optyczny i akustyczny:

1. Na stronie sieciowej urządzenia przejdź do **Profiles > Create** (Profile > Utwórz).
2. Wprowadź następujące informacje:
 - **Nazwa**: Profil 1
 - **Description (Opis)**: Dodaj opis profilu.
 - **Light (Oświetlenie)**: Wybierz **Pattern (Sposób)**, **Speed (Szybkość)**, **Intensity (Intensywność)**, **Color (Kolor)** i **Duration (Czas trwania)**.
 - **Siren (Syrena)**: Wybierz **Pattern (Sposób)**, **Intensity (Intensywność)** i **Duration (Czas trwania)**.

Uwaga

Profile o wyższych numerach mają wyższy priorytet.

- **Priority (Priorytet)**: Wybierz **Light priority** (Priorytet sygnalizacji optycznej) i **Siren priority** (Priorytet sygnalizacji akustycznej).

Tworzenie zdarzenia:

1. Przejdź do **System > Events > Rules** (System > Zdarzenia > Reguły) i dodaj regułę.
2. Wprowadź następujące informacje:
 - **Nazwa**: Włącz sygnalizację z diodami LED i sygnalizację akustyczną
 - **Condition (Warunek)**: czujka PIR
 - **Action (Akcja)**: Uruchom profil oświetlenia i syreny
 - **Profile (Profil)**: Profil 1
 - **Action (Akcja)**: Start (Uruchom)
3. Kliknij przycisk **Zapisz**.

Uruchamianie profilu po wyzwoleniu alarmu

W tym przykładzie wyjaśniono, w jaki sposób wyzwolić alarm po zmianie cyfrowego sygnału wejściowego.

Ustaw kierunek wejścia dla portu:

1. Przejdź do menu **System > Accessories > I/O ports** (System > Akcesoria > Porty we/wy).
2. Przejdź do obszaru **Port 1 > Normal state** (Normalny stan) i kliknij **Circuit closed** (Obwód zamknięty).

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **I/O (We/Wy) > Digital input is active** (Wejście cyfrowe jest aktywne).
4. Wybierz **Port 1**.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active** (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna).
6. Wybierz profil, który chcesz uruchomić.
7. Kliknij przycisk **Zapisz**.

Uruchamianie profilu przy użyciu protokołu SIP

Ten przykład objaśnia wyzwalanie alarmu za pomocą protokołu SIP.

Aktywowanie uwierzytelniania SIP:

1. Przejdź do menu **System > SIP > SIP settings (Ustawienia SIP)**.
2. Wybierz opcję **Enable SIP (Włącz protokół SIP)** i **Allow incoming calls (Zezwalaj na połączenia przychodzące)**.
3. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call (Połączenie) > State (Stan)**.
4. Na liście stanu wybierz pozycję **Active (Aktywne)**.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna)**.
6. Wybierz profil, który chcesz uruchomić.
7. Kliknij przycisk **Zapisz**.

Sterowanie kilkoma profilami za pomocą rozszerzeń SIP

Aktywowanie uwierzytelniania SIP:

1. Przejdź do menu **System > SIP > SIP settings (Ustawienia SIP)**.
2. Wybierz opcję **Enable SIP (Włącz protokół SIP)** i **Allow incoming calls (Zezwalaj na połączenia przychodzące)**.
3. Kliknij przycisk **Zapisz**.

Utwórz regułę, aby uruchomić profil:

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call (Połączenie) > State change (Zmiana stanu)**.
4. Na liście przyczyn zaznacz opcję **Accepted by device (Zaakceptowane przez urządzenie)**.
5. W polu **Call direction (Kierunek połączenia)** zaznacz opcję **Incoming (Przychodzące)**.
6. W polu **Local SIP URI (Lokalny URI SIP)** wpisz wyrażenie **sip:[numer wewnętrzny]@[adres IP]**, gdzie [numer wewnętrzny] to numer wewnętrzny używany dla profilu, a [adres IP] to adres urządzenia. Na przykład **sip:1001@192.168.0.90**.
7. Na liście akcji wybierz opcję **Light and Siren (Światło i syrena) > Run light and siren profile (Uruchom profil oświetlenia i syreny)**.
8. Wybierz profil, który chcesz uruchomić.
9. Wybierz akcję **Start (Uruchamianie)**.
10. Kliknij przycisk **Zapisz**.

Utwórz regułę, aby zatrzymać profil:

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call (Połączenie) > State change (Zmiana stanu)**.

4. Na liście przyczyn zaznacz opcję **Terminated (Przerwane)**.
5. W polu **Call direction (Kierunek połączenia)** zaznacz opcję **Incoming (Przychodzące)**.
6. W polu **Local SIP URI (Lokalny URI SIP)** wpisz wyrażenie `sip:[numer wewnętrzny]@[adres IP]`, gdzie [numer wewnętrzny] to numer wewnętrzny używany dla profilu, a [adres IP] to adres urządzenia. Na przykład `sip:1001@192.168.0.90`.
7. Na liście akcji wybierz opcję **Light and Siren (Światło i syrena) > Run light and siren profile (Uruchom profil oświetlenia i syreny)**.
8. Wybierz profil, który chcesz zatrzymać.
9. Wybierz akcję **Stop (Zatrzymanie)**.
10. Kliknij przycisk **Zapisz**.

Powtórz te kroki, aby utworzyć reguły uruchamiania i zatrzymywania dla każdego profilu, który chcesz kontrolować za pomocą protokołu SIP.

Uruchamianie dwóch profili o różnych priorytetach

Jeśli uruchomione zostaną dwa profile o różnych priorytetach, wówczas profil o wyższym numerze priorytetu przerwie działanie profilu o niższym numerze priorytetu.

Uwaga

W przypadku uruchomienia profilu z takim samym priorytetem, nowszy profil anuluje wcześniejszy profil.

W tym przykładzie pokazano, jak ustawić urządzenie, aby po wyzwoleniu przez cyfrowy port We/Wy był wyświetlany jeden profil o priorytecie 4 zamiast innego profilu o priorytecie 3.

Create profiles (Utwórz profile):

1. Utwórz profil o priorytecie 3.
2. Utwórz inny profil o priorytecie 4.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **I/O (We/Wy) > Digital input is active (Wejście cyfrowe jest aktywne)**.
4. Wybierz port.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna)**.
6. Wybierz profil z najwyższym numerem priorytetu.
7. Kliknij przycisk **Zapisz**.
8. Przejdź do menu **Profiles (Profile)** i uruchom profil z najniższym numerem priorytetu.

Uaktywnij profil optyczny i akustyczny przez żądanie HTTP post, gdy kamera wykryje ruch

W tym przykładzie wyjaśniono, jak dołączyć kamerę do czujnika jakości powietrza i uaktywnić profil optyczny i akustyczny w czujniku jakości powietrza przy każdym wykryciu ruchu przez aplikację **AXIS Motion Guard** zainstalowaną w kamerze.

Zanim zaczniesz:

- Utwórz w czujniku jakości powietrza nowego użytkownika z rolą **Operator** lub **Administrator**.
- Utwórz profil w czujniku jakości powietrza o nazwie: „Profil optyczny i akustyczny”.
- Skonfiguruj aplikację **AXIS Motion Guard** w kamerze i utwórz profil o nazwie „Profil kamery”.
- Upewnij się, że masz zainstalowaną aplikację **AXIS Device Assistant** i oprogramowanie sprzętowe w wersji 10.8.0 lub nowszej.

Tworzenie odbiorcy w kamerze:

1. W interfejsie urządzenia kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź następujące informacje:
 - **Name (Nazwa):** czujnik jakości powietrza
 - **Typ:** HTTP
 - **URL:** `http://<IPaddress>/axis-cgi/siren_and_light.cgi`
Zastąp <IPaddress> (Adres IP) adresem czujnika jakości powietrza.
 - **Nazwa i hasło** nowo utworzonego użytkownika czujnika jakości powietrza.
3. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk **Zapisz**.

Utworzenie dwóch reguł w kamerze:

1. Przejdź do obszaru **Rules (Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
 - **Nazwa:** Uaktywnij czujnik jakości powietrza poprzez wykryty ruch
 - **Condition (Warunek):** Applications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)
 - **Action (Akcja):** Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)
 - **Recipient (Odbiorca):** czujnik jakości powietrza.
Informacje te muszą być takie same, jak podane wcześniej w obszarze **Events > Recipients > Name (Zdarzenia > Odbiorcy > Nazwa)**.
 - **Method (Metoda):** Post (Post)
 - **Body (Treść):**

```
{  "apiVersion": "1.0",  "method": "start",  "params": {    "profile": "Light and siren profile"  } }
```

Dla parametru **"profile"** : <>' podaj dane wprowadzone na etapie tworzenia profilu dla czujnika jakości powietrza, w tym przypadku: „Profil optyczny i akustyczny”.

3. Kliknij przycisk **Zapisz**.
4. Dodaj kolejną regułę z następującymi informacjami:
 - **Nazwa:** Wyłącz uaktywnienie czujnika jakości powietrza poprzez wykryty ruch
 - **Condition (Warunek):** Applications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)
 - Wybierz opcję **Invert this condition (Odwróć ten warunek)**.
 - **Action (Akcja):** Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)
 - **Recipient (Odbiorca):** czujnik jakości powietrza
Informacje te muszą być takie same, jak podane wcześniej w obszarze **Events > Recipients > Name (Zdarzenia > Odbiorcy > Nazwa)**.
 - **Method (Metoda):** Post (Post)
 - **Body (Treść):**

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile": "Light and siren profile"  } }
```

Dla parametru **"profile"** : <>' podaj dane wprowadzone na etapie tworzenia profilu dla czujnika jakości powietrza, w tym przypadku: „Profil optyczny i akustyczny”.

5. Kliknij przycisk **Zapisz**.

Uaktywnij profil optyczny i akustyczny poprzez wejście wirtualne, gdy kamera wykryje ruch

W tym przykładzie wyjaśniono, jak dołączyć kamerę do czujnika jakości powietrza i uaktywnić profil optyczny i akustyczny w czujniku jakości powietrza przy każdym wykryciu ruchu przez aplikację AXIS Motion Guard zainstalowaną w kamerze.

Zanim zaczniesz:

- Utwórz w czujniku jakości powietrza nowe konto z uprawnieniami Operatora lub Administratora.
- Utwórz profil w czujniku jakości powietrza. Patrz .
- Skonfiguruj aplikację AXIS Motion Guard w kamerze oraz utworzenie profilu o nazwie „Profil kamery”.

Utworzenie dwóch odbiorców w kamerze:

1. W interfejsie urządzenia kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź następujące informacje:
 - **Nazwa:** Aktywacja portu wirtualnego
 - **Typ:** HTTP
 - **URL:** `http://<adresIP>/axis-cgi/virtualinput/activate.cgi`
Zastąp <IPaddress> (Adres IP) adresem czujnika jakości powietrza.
 - Konto i hasło nowo utworzonego konta czujnika jakości powietrza.
3. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk **Zapisz**.
5. Dodaj drugiego odbiorcę z następującymi informacjami:
 - **Nazwa:** Dezaktywacja portu wirtualnego
 - **Typ:** HTTP
 - **URL:** `http://<adresIP>/axis-cgi/virtualinput/deactivate.cgi`
Zastąp <IPaddress> (Adres IP) adresem czujnika jakości powietrza.
 - Konto i hasło nowo utworzonego konta czujnika jakości powietrza.
6. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
7. Kliknij przycisk **Zapisz**.

Utworzenie dwóch reguł w kamerze:

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

- **Action (Akcja):** Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)
- **Recipient (Odbiorca):** Dezaktywacja portu wirtualnego
- **Query string suffix (Sufiks ciągu zapytania):** schemaversion=1&port=1

5. Kliknij przycisk **Zapisz**.

Utwórz regułę w czujniku jakości powietrza.

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

Uaktywnij profil optyczny i akustyczny przez protokół MQTT, gdy kamera wykryje ruch

W tym przykładzie wyjaśniono, jak dołączyć kamerę do czujnika jakości powietrza i uaktywnić profil optyczny i akustyczny w czujniku jakości powietrza przy każdym wykryciu ruchu przez kamerę.

Zanim zaczniesz:

- Utwórz profil w czujniku jakości powietrza.
- Skonfiguruj brokera MQTT i uzyskaj adres IP oraz nazwę użytkownika i hasło brokera.
- Upewnij się, że aplikacja do detekcji ruchu jest skonfigurowana i uruchomiona w kamerze.

Konfigurowanie klienta MQTT w kamerze:

1. W interfejsie www 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.

Skonfiguruj klienta MQTT w czujniku jakości powietrza:

1. Na stronie sieciowej czujnika jakości powietrza przejdź do **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wprowadź następujące informacje:
 - Host: Adres IP brokera
 - Client ID (Identyfikator klienta): Syrena 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.

Utwórz regułę w czujniku jakości powietrza dla 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): Light and siren > Run light and siren profile while the rule is active (Światło i syrena > Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna)
 - Profile (Profil): Wybierz profil, który ma być aktywny.
3. Kliknij przycisk Zapisz.

Wysyłanie wiadomości e-mail w razie niepowodzenia testu głośnika

W tym przykładzie urządzenie audio jest skonfigurowane do wysyłania wiadomości e-mail do zdefiniowanego odbiorcy w razie niepowodzenia testu głośnika. Test głośnika jest zaplanowany na 18:00 codziennie.

1. Przygotuj harmonogram testu głośnika:
 - 1.1. Przejdź do interfejsu urządzenia > **System > Events (Zdarzenia) > Schedules (Harmonogramy)**.
 - 1.2. Utwórz harmonogram rozpoczynający się codziennie o 18:00 i kończący o 18:01. Nazwij go „Codziennie o 18.00”.
2. Tworzenie odbiorcy wiadomości e-mail:
 - 2.1. Przejdź do interfejsu urządzenia > **System > Events (Zdarzenia) > Recipients (Odbiorcy)**.

- 2.2. Kliknij przycisk **Add recipient (Dodaj odbiorcę)**.
- 2.3. Nazwij odbiorcę „Odbiorcy dla testu głośnika”.
- 2.4. W obszarze **Type (Typ)** wybierz opcję **Email (E-mail)**.
- 2.5. W obszarze **Send email to (Wyślij wiadomość e-mail do)** wprowadź adresy e-mail odbiorców. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
- 2.6. Wprowadź dane konta e-mail nadawcy.
- 2.7. Kliknij przycisk **Testuj**, aby wysłać testową wiadomość e-mail.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużych załączników, odbieranie wiadomości cyklicznych itp. Sprawdź zasady zabezpieczeń dostawcy poczty elektronicznej, aby uniknąć problemów z dostarczaniem e-maili i zablokowania konta.

- 2.8. Kliknij przycisk **Zapisz**.
3. Konfiguracja automatycznego testu głośnika:
 - 3.1. Przejdź do interfejsu urządzenia > **System** > **Events (Zdarzenia)** > **Rules (Reguły)**.
 - 3.2. Kliknij przycisk **Add a rule (Dodaj regułę)**.
 - 3.3. Wprowadź nazwę reguły.
 - 3.4. W obszarze **Condition (Warunek)** kliknij opcję **Schedule (Harmonogram)** i wybierz wyzwalacz z listy.
 - 3.5. W obszarze **Schedule (Harmonogram)** zaznacz swój harmonogram („Codziennie o 18.00”).
 - 3.6. W obszarze **Action (Akcja)** zaznacz opcję **Run automatic speaker test (Uruchom automatyczny test głośnika)**.
 - 3.7. Kliknij przycisk **Zapisz**.
4. Skonfiguruj warunek wysłania wiadomości e-mail w razie niepowodzenia testu głośnika:
 - 4.1. Przejdź do interfejsu urządzenia > **System** > **Events (Zdarzenia)** > **Rules (Reguły)**.
 - 4.2. Kliknij przycisk **Add a rule (Dodaj regułę)**.
 - 4.3. Wprowadź nazwę reguły.
 - 4.4. W obszarze **Condition (Warunek)** zaznacz opcję **Speaker test result (Wynik testu głośnika)**.
 - 4.5. W obszarze **Speaker test status (Stan testu głośnika)** zaznacz opcję **Didn't pass the test (Test zakończony niepowodzeniem)**.
 - 4.6. W obszarze **Action (Akcja)** wybierz opcję **Send notification to email (Wyślij powiadomienie emailem)**.
 - 4.7. W obszarze **Recipient (Odbiorca)** zaznacz swojego odbiorcę („Odbiorcy dla testu głośnika”)
 - 4.8. Wprowadź temat i wiadomość, a następnie kliknij przycisk **Save (Zapisz)**.

Odtworzenie niestandardowego klipu po wyzwoleniu alarmu

W tym przykładzie wyjaśniono, w jaki sposób wyzwolić odtworzenie niestandardowego pliku audio po zmianie sygnału wejścia cyfrowego.

Prześlij plik audio:

1. Przejdź do menu **Media** i kliknij przycisk  **Add (Dodaj)**.
2. Kliknij, aby wyszukać i wybrać plik audio z komputera.
3. Wybierz **Storage location (Lokalizacja pamięci masowej)**.
4. Kliknij przycisk **Zapisz**.

Utwórz profil z plikiem audio:

1. Przejdź do obszaru **Profiles (Profile)** i kliknij opcję  **Create (Utwórz)**.
2. Wprowadź nazwę w polu **Name** i wybierz wzór oświetlenia dla profilu.
3. W sekcji syreny wybierz przesłany plik audio.
4. Wybierz **Intensity (Intensywność)** i **Duration (Czas trwania)**.
5. Kliknij przycisk **Zapisz**.

Ustaw kierunek wejścia dla portu:

1. Przejdź do menu **System > Accessories > I/O ports** (System > Akcesoria > Porty we/wy).
2. Przejdź do obszaru **Port 1 > Normal state** (Normalny stan) i kliknij **Circuit closed** (Obwód zamknięty).

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **I/O (We/Wy) > Digital input is active** (Wejście cyfrowe jest aktywne).
4. Wybierz **Port 1**.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active** (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna).
6. Wybierz profil z przesłanym plikiem audio.
7. Kliknij przycisk **Zapisz**.

Zatrzymywanie nadawania audio za pomocą DTMF

W tym przykładzie wyjaśniono, jak:

- Skonfigurować DTMF w urządzeniu.
 - Skonfigurować zdarzenie, tak, aby po przesłaniu polecenia DTMF nadawanie sygnału audio było wyłączane.
1. Przejdź do menu **System > SIP > SIP settings** (Ustawienia SIP).
 2. Upewnij się, że opcja **Enable SIP** (Włącz SIP) jest włączona. Jeżeli trzeba ją włączyć, pamiętaj, aby na koniec kliknąć przycisk **Save** (Zapisz).
 3. Przejdź do menu **SIP accounts** (Konta SIP).
 4. Obok konta SIP kliknij kolejno  **> Edit** (Edytuj).
 5. W obszarze **DTMF** kliknij przycisk **+ DTMF sequence** (+ Sekwencja DTMF).
 6. W polu **Sequence** (Sekwencja) wpisz wartość „1”.
 7. W polu **Description** (Opis) wpisz „stop audio”.
 8. Kliknij przycisk **Zapisz**.
 9. Przejdź do menu **System > Events** (Zdarzenia) **> Rules** (Reguły) i kliknij przycisk **+ Add a rule** (+ Dodaj regułę).
 10. W polu **Name** (Nazwa) wpisz „DTMF stop audio”.
 11. W ustawieniu **Condition** (Warunek) wybierz opcję **DTMF**.
 12. W ustawieniu **DTMF Event ID** (Identyfikator zdarzenia DTMF) wybierz opcję **stop audio**.
 13. W ustawieniu **Action** (Akcja) wybierz opcję **Stop playing audio clip** (Przestań odtwarzać klip audio).
 14. Kliknij przycisk **Zapisz**.

Konfigurowanie dźwięku dla przychodzących połączeń SIP

Można skonfigurować regułę, która będzie powodowała odtwarzanie klipu dźwiękowego po nadejściu połączenia SIP.

Można również skonfigurować dodatkową regułę powodującą automatyczne odbieranie połączenia SIP po zakończeniu odtwarzania klipu audio. Może się to przydać w sytuacjach, gdy operator systemu alarmowego chce przyciągnąć uwagę osoby znajdującej się obok urządzenia audio i nawiązać z nią rozmowę. Odbywa się to poprzez wykonanie połączenia SIP do urządzenia dźwiękowego, które otworzy klip dźwiękowy w celu zwrócenia uwagi osób znajdujących się blisko urządzenia. Po zakończeniu odtwarzania klipu urządzenie automatycznie odbierze połączenie SIP, tak aby umożliwić komunikowanie się operatora systemu alarmowego z osobami przebywającymi obok urządzenia.

Włączanie obsługi protokołu SIP:

1. Przejdź do interfejsu urządzenia głośnika, wprowadzając jego adres IP w przeglądarce internetowej.
2. Wybierz kolejno **System > SIP > SIP settings (Ustawienia SIP)** i wybierz opcję **Enable SIP (Włącz SIP)**.
3. Aby zezwolić urządzeniu na odbieranie połączeń, wybierz opcję **Allow incoming calls (Zezwalaj na połączenia przychodzące)**.
4. Kliknij przycisk **Save (Zapisz)**.
5. Przejdź do menu **SIP accounts (Konta SIP)**.
6. Obok konta SIP kliknij kolejno  > **Edit (Edytuj)**.
7. Wyczyść pole wyboru **Odbierz automatycznie**.

Odtwarzanie dźwięku po odebraniu połączenia SIP:

1. Wybierz kolejno **Settings (Ustawienia) > System > Events (Zdarzenia) > Rules (Reguły)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz opcję **State (Stan)**.
4. Z listy stanów wybierz opcję **Łączenie**.
5. Z listy akcji wybierz opcję **Play audio clip (Odtwórz klip audio)**.
6. Z listy klipów wybierz plik dźwiękowy, który ma być odtwarzany.
7. Wybierz liczbę razy powtarzania klipu. 0 oznacza jednokrotne odtworzenie.
8. Kliknij przycisk **Save (Zapisz)**.

Automatyczne odbieranie połączenia SIP po zakończeniu odtwarzania klipu audio:

1. Wybierz kolejno **Settings (Ustawienia) > System > Events (Zdarzenia) > Rules (Reguły)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz opcję **Audio clip playing (Odtworzenie klipu audio)**.
4. Zaznacz pole wyboru **Użyj tego warunku jako wyzwalacza**.
5. Zaznacz opcję **Odwróć ten warunek**.
6. Kliknij przycisk **+ Dodaj warunek**, aby dodać drugi warunek do zdarzenia.
7. Z listy warunków wybierz opcję **State (Stan)**.
8. Z listy stanów wybierz opcję **Łączenie**.
9. Z listy akcji wybierz opcję **Answer call (Odbierz połączenie)**.
10. Kliknij przycisk **Save (Zapisz)**.

Interfejs WWW

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

Status

Informacje o urządzeniu

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

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

Stan synchronizacji czasu

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

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

Bezpieczeństwo

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

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

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.

Stan zasilania

Wyświetla informacje o stanie zasilania. Informacje różnią się w zależności od produktu.

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.

Podłączone klienty

Pokazuje liczbę połączeń i połączonych klientów.

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

Nagranie wideo

Strumień

Zapisy ogólne

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

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

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

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

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

Sterowanie przepływnością bitową

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

Dźwięk

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

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

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

Czujnik jakości powietrza

Pulpit nawigacyjny

Dane z czujnika w czasie rzeczywistym

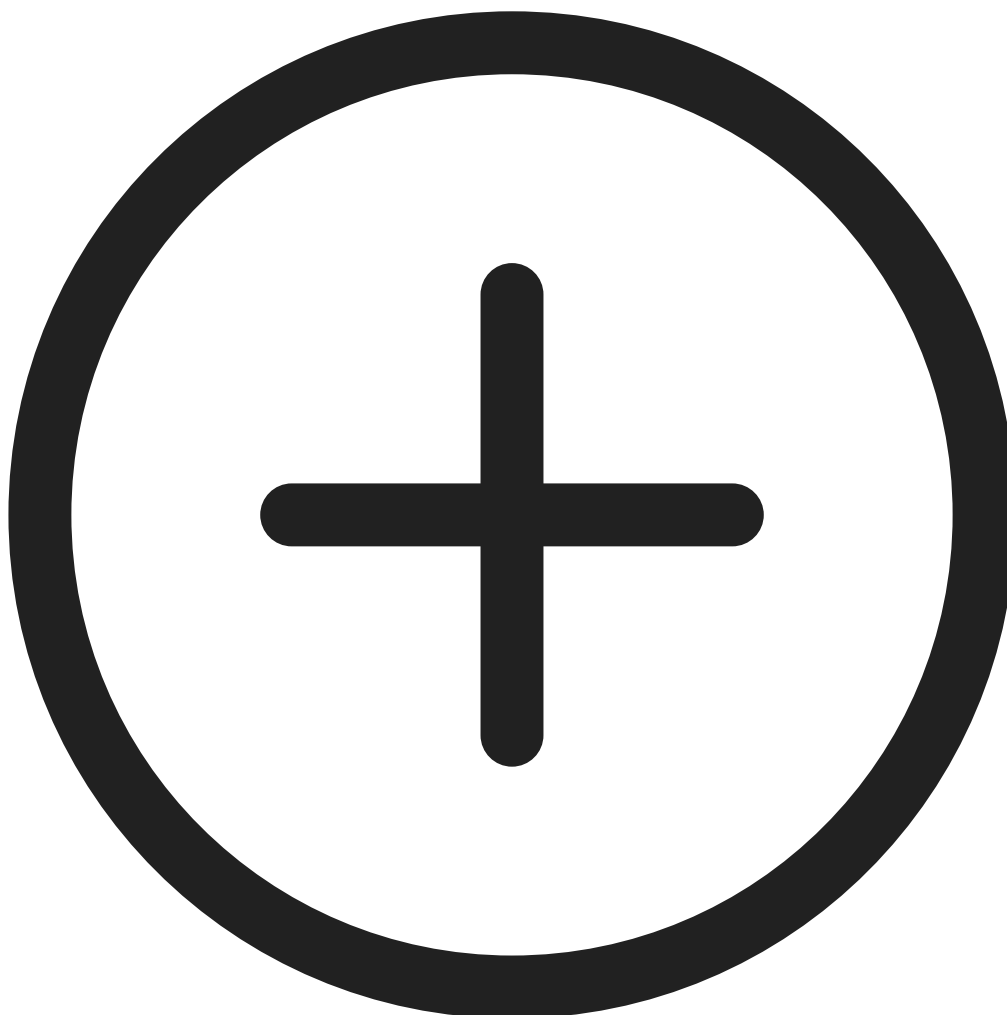
Wyświetlanie danych z czujnika w czasie rzeczywistym.

Uwaga

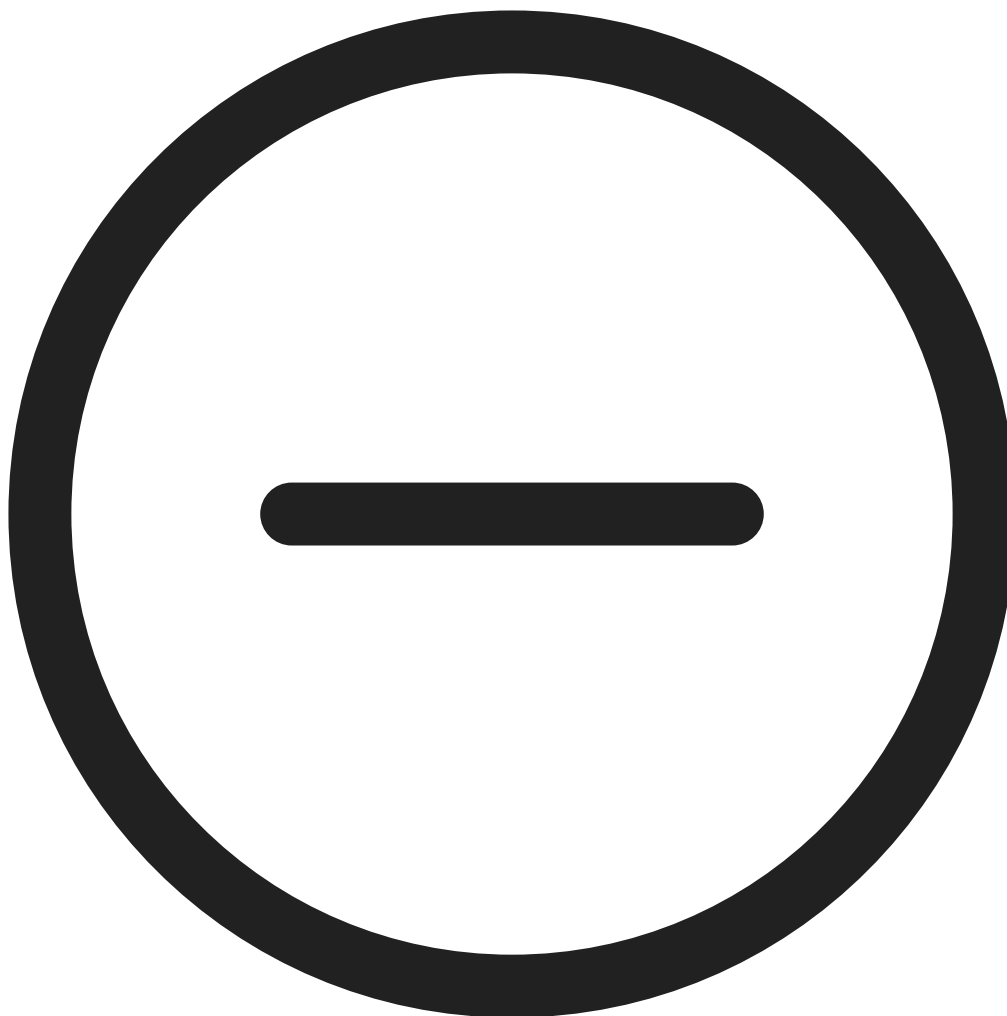
- Pełną dokładność pomiaru stężenia CO₂ uzyskuje się po 2 dniach od pierwszego uruchomienia urządzenia.
- Przy pierwszym uruchomieniu urządzenia do ustalenia właściwych wskazań AQI (wskaźnika jakości powietrza) potrzeba 12 godzin. Wskaźnik AQI będzie wyświetlany na stronie **Calculating** (Obliczenia) do momentu uzyskania wystarczającej ilości danych. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.
- Pełną dokładność pomiaru LZO uzyskuje się po godzinie od momentu uruchomienia urządzenia. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.
- Pełną dokładność pomiaru NO_x uzyskuje się po 6 godzinach od momentu uruchomienia urządzenia. Przy każdym ponownym uruchomieniu urządzenia wymagana jest kalibracja.

 : kliknij, aby ustawić nazwę pulpitu nawigacyjnego.

 Edycja: Kliknij tę opcję, aby wyświetlić lub ukryć dane.



: kliknij, aby dodać dane do pulpitu nawigacyjnego.



: kliknij, aby usunąć dane z pulpitu nawigacyjnego.

Temperatura: Podgląd temperatury w czasie rzeczywistym z czujnika jakości powietrza.

Humidity (Wilgotność): Podgląd wilgotności w czasie rzeczywistym z czujnika jakości powietrza.

CO2: podgląd poziomu dwutlenku węgla w czasie rzeczywistym.

Znaczenie kolorów pasków stanu CO2 jest następujące:

- **Green (0–1000) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Orange (1001–2000) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Osoby wrażliwe mogą odczuwać skutki zdrowotne. Mniej prawdopodobny jest wpływ na ogół społeczeństwa.
- **Red (2001–5000) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Purple (5001–40000) (Fioletowy): Very unhealthy (Bardzo niezdrowe).** Ostrzeżenia zdrowotne o stanach zagrożenia. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.

NOx: wyświetlanie w czasie rzeczywistym stężenia tlenu azotu i dwutlenku azotu.

Znaczenie kolorów pasków stanu NO_x jest następujące:

- **Green (0–30) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Yellow (31–150) (Żółty): Moderate (Umiarkowane).** Dane są akceptowalne. Umiarkowane zagrożenie dla zdrowia może występować w przypadku bardzo niewielkiej liczby wyjątkowo wrażliwych osób.
- **Orange (151–300) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Red (301–500) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.

PM 1.0: podgląd poziomu cząstek stałych 1,0 w czasie rzeczywistym.

PM 2.5: podgląd poziomu cząstek stałych 2,5 w czasie rzeczywistym.

Znaczenie kolorów pasków stanu PM 2,5 jest następujące:

- **Green (0–9) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Yellow (9,1–35,4) (Żółty): Moderate (Umiarkowane).** Dane są akceptowalne. Umiarkowane zagrożenie dla zdrowia może występować w przypadku bardzo niewielkiej liczby wyjątkowo wrażliwych osób.
- **Orange (35,5–55,4) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Red (55,5–125,4) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Purple (125,5–225,4) (Fioletowy): Very unhealthy (Bardzo niezdrowe).** Ostrzeżenia zdrowotne o stanach zagrożenia. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.
- **Maroon (225,5–1000) (Rdzawoczerwony): Hazardous (Niebezpieczne).** Warunki bardzo niebezpieczne. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.

PM 4.0: podgląd poziomu cząstek stałych 4,0 w czasie rzeczywistym.

PM 10.0: podgląd poziomu cząstek stałych 10,0 w czasie rzeczywistym.

Znaczenie kolorów pasków stanu PM 10,0 jest następujące:

- **Green (0–54) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Yellow (55–154) (Żółty): Moderate (Umiarkowane).** Dane są akceptowalne. Umiarkowane zagrożenie dla zdrowia może występować w przypadku bardzo niewielkiej liczby wyjątkowo wrażliwych osób.
- **Orange (155–254) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Red (255–354) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Purple (355–424) (Fioletowy): Very unhealthy (Bardzo niezdrowe).** Ostrzeżenia zdrowotne o stanach zagrożenia. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.
- **Maroon (425–1000) (Rdzawoczerwony): Hazardous (Niebezpieczne).** Warunki bardzo niebezpieczne. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.

Vaping/Smoking (Palenie papierosów elektronicznych / tytoniu): podgląd wykrycia lub braku wykrycia palenia papierosów elektronicznych lub tytoniu.

Znaczenie kolorów pasków stanu palenia papierosów elektronicznych lub tytoniu jest następujące:

- **Zielony: Undetected (Niewykryte).** Nie wykryto palenia papierosów elektronicznych lub tytoniu.
- **Czerwony: Detected (Wykryte).** Wykryto palenie papierosów elektronicznych lub tytoniu.

VOC (LZO): podgląd wskaźnika lotnych związków organicznych.

Znaczenie kolorów pasków stanu LZO jest następujące:

- **Green (0–100) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Yellow (101–300) (Żółty): Moderate (Umiarkowane).** Dane są akceptowalne. Umiarkowane zagrożenie dla zdrowia może występować w przypadku bardzo niewielkiej liczby wyjątkowo wrażliwych osób.
- **Orange (301–400) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Red (401–500) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.

AQI: podgląd wskaźnika jakości powietrza.

Znaczenie kolorów pasków stanu wskaźnika jakości powietrza jest następujące:

- **Green (0–50) (Zielony): Good (Dobry).** Dane uznaje się za zadowalające.
- **Yellow (51–100) (Żółty): Moderate (Umiarkowane).** Dane są akceptowalne. Umiarkowane zagrożenie dla zdrowia może występować w przypadku bardzo niewielkiej liczby wyjątkowo wrażliwych osób.
- **Orange (101–150) (Pomarańczowy): Unhealthy for sensitive group (Niezdrowe dla osób wrażliwych).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Red (151–200) (Czerwony): Unhealthy (Niezdrowe).** Każdy może zacząć odczuwać skutki zdrowotne; osoby wrażliwe mogą odczuwać poważniejsze skutki zdrowotne.
- **Purple (201–300) (Fioletowy): Very unhealthy (Bardzo niezdrowe).** Ostrzeżenia zdrowotne o stanach zagrożenia. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.
- **Maroon (301–500) (Rdzawoczerwony): Hazardous (Niebezpieczne).** Warunki bardzo niebezpieczne. Istnieje większe prawdopodobieństwo, że wpłynie to na całe społeczeństwo.

Ustawienia

Próg

Konfiguracja danych z czujnika jakości powietrza.

Temperatura: ustawienie MIN (MIN.) i MAX (MAKS.) temperatury w zakresie $-10 \div +45$.

Humidity (Wilgotność) : ustawienie MIN (MIN.) i MAX (MAKS.) wilgotności w zakresie 0 – 100.

CO2 : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu dwutlenku węgla w zakresie 0 – 40000.

NOx : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu tlenku azotu i dwutlenku azotu w zakresie 0–500.

PM1.0 : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu cząstek stałych 1,0 w zakresie 0 – 1000.

PM2.5 : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu cząstek stałych 2,5 w zakresie 0 – 1000.

PM4.0 : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu cząstek stałych 4,0 w zakresie 0 – 1000.

PM10.0 : ustawienie MIN (MIN.) i MAX (MAKS.) poziomu cząstek stałych 10,0 w zakresie 0 – 1000.

VOC (LZO) : ustawienie MIN (MIN.) i MAX (MAKS.) wskaźnika lotnych związków organicznych w zakresie 0 – 500.

AQI : ustawienie MIN (MIN.) i MAX (MAKS.) wskaźnika jakości powietrza w zakresie 0 – 500.

Jednostki temperatury

Show temperature in (Pokaż temperaturę w skali): Celsjusza lub Fahrenheita

Czułość wykrywania palenia papierosów elektronicznych

Ustawienie czułości wykrywania palenia papierosów elektronicznych.

Low sensitivity, High sensitivity (Niska czułość, Wysoka czułość): Przy pomocy suwaka ustaw różnicę między niską a wysoką czułością, przy której urządzenie powinno wzbudzić alarm. Wysoka czułość oznacza, że urządzenie wykrywa nawet niewielkie ilości dymu i bardziej prawdopodobne jest, że wyzwoli alarm; niska czułość oznacza, że urządzenie reaguje tylko na większe ilości dymu, co z kolei zmniejsza ryzyko fałszywych alarmów.

Ustawienie pamięci masowej

- **Retention time 1 month, frequency 1s** (Czas przechowywania 1 miesiąc, częstotliwość 1 s): dane gromadzone są co sekundę i przechowywane tylko przez ostatnie 30 dni.
- **Retention time 3 month, frequency 5s** (Czas przechowywania 3 miesiące, częstotliwość 5 s): dane gromadzone są co 5 sekund i przechowywane tylko przez ostatnie 90 dni.
- **Retention time 1 year, frequency 10s** (Czas przechowywania 1 rok, częstotliwość 10 s): dane gromadzone są co 10 sekund i przechowywane tylko przez ostatnie 365 dni.

Uwaga

Zmiana opcji pamięci masowej spowoduje skasowanie istniejących danych.

Częstotliwość metadanych w chmurze

Częstotliwość metadanych w chmurze jest wykorzystywana przez platformy zewnętrznych dostawców, które chcą otrzymywać metadane czujników z regulowaną częstotliwością transmisji. Metadane w chmurze obejmują wszystkie dane z czujników wyświetlane na pulpicie nawigacyjnym.

Cloud metadata (Metadane w chmurze): Włącz, aby korzystać z metadanych w chmurze.

Uwaga

W ustawieniach domyślnych ta funkcja jest wyłączona; nie są wysyłane żadne metadane dotyczące tematu. Po włączeniu metadane dla tematu są przesyłane z poniższymi ustawieniami częstotliwości.

Set frequency range (00:00:01 – 23:59:59) (Ustaw częstotliwość (00:00:01 – 23:59:59): Wprowadź wartość, aby ustawić częstotliwość.

Okres weryfikacji

Możliwe jest ustawienie okresu weryfikacji dla poniższych ustawień jakości powietrza. Okres weryfikacji pełni funkcję progu czasowego; odczyt musi pozostawać powyżej granicy zakresu okresu weryfikacji, aby uruchomić alarm.

Przykład

Jeżeli okres weryfikacji CO₂ wynosi 5 sekund, poziom CO₂ musi pozostawać powyżej granicy przez pełne 5 sekund, aby uruchomić alarm.

Ustaw zakres okresu weryfikacji (0 – 60 sekund) dla poniższych danych:

- Temperatura
- Wilgotność
- CO2
- NOx
- PM1.0
- PM2.5
- PM4.0
- PM10.0
- LZO
- AQI
- Palenie papierosów elektronicznych / tytoniu

Statystyki

Statystyki danych z czujników

Można wyeksportować dane statystyczne z czujnika z okresu do 365 dni wstecz do pliku CSV, aby wykorzystać je w aplikacjach w rodzaju Microsoft® Excel.

- **Predefined date range** (Zdefiniowany zakres dat): aby wybrać zdefiniowany zakres dat, który chcesz pobrać z listy.
- **From (Od) i To (Do)**: aby wybrać niestandardowy zakres, który chcesz pobrać. Dane można pobierać do 365 dni wstecz.

Uwaga

W razie wyboru obu zakresów, niestandardowego i zdefiniowanego, pierwszeństwo ma zakres niestandardowy.

Uwaga

Maksymalny zakres pobierania jest ograniczony czasem przechowywania danych ustawionym w .

- **Select source** (Wybierz źródło): wybierz źródło do pobrania danych.
- **Download data** (Pobierz dane): aby wybrać **Download selected sensor data** (Pobierz wybrane dane z czujnika) z rozwijalnego menu.
- **Download data for all sources** (Pobierz dane ze wszystkich źródeł): aby wyeksportować dane dla wszystkich źródeł w wybranym przedziale czasowym.

Plik zostanie pobrany do folderu pobierania. Pobieranie może nieco potrwać, zależnie od wielkości pliku.

Narzędzia analityczne

AXIS Audio Analytics

Poziom ciśnienia akustycznego (SPL)

Show threshold and events in graph (Wyświetl progi i zdarzenia na wykresie): włącz, aby przedstawić na wykresie, kiedy wykryto skok poziomu dźwięku.

Threshold (Próg): dostosuj wartości progowe na potrzeby detekcji. Aplikacja zarejestruje zdarzenie foniczne dotyczące każdego dźwięku, który wykracza poza wartości progowe.

Adaptacyjna detekcja dźwięku

Show events in graph (Pokaż zdarzenia na wykresie): włącz, aby przedstawić na wykresie, kiedy wykryto skok poziomu dźwięku.

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.

Klasyfikacja dźwięku

Show events in graph (Pokaż zdarzenia na wykresie) ⓘ : włącz, aby przedstawić na wykresie, kiedy wykryto określony rodzaj dźwięku.

Classifications (Klasyfikacje) ⓘ : wybierz rodzaje dźwięków, które ma wykrywać aplikacja.

Test alarms (Testuj alarm) ⓘ : kliknij przycisk Test (Testuj), aby wyzwolić detekcję zdarzenia określonego rodzaju dźwięku na potrzeby testowania.

Dźwięk

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.

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.

Informacje ogólne

Stan diody sygnalizacyjnej LED

Wyświetla różne działania diody sygnalizacyjnej LED wykonywane w urządzeniu. Na liście stanu diody sygnalizacyjnej LED może się znajdować maksymalnie 10 działań. Gdy dwa lub więcej działań jest wykonywanych w tym samym momencie, działanie o najwyższym priorytecie wskazuje stan diody sygnalizacyjnej LED. Odpowiedni wiersz będzie podświetlony na liście stanu.

Audio speaker status (Stan głośnika audio)

Wyświetla różne działania głośnika audio wykonywane w urządzeniu. Na liście stanu głośnika audio może się znajdować maksymalnie 10 działań. Gdy dwa lub więcej działań jest wykonywanych w tym samym momencie, system odtwarza to o najwyższym priorytecie. Ten wiersz będzie podświetlony na zielono na liście stanu.

Profile

Profile

Profil to zbiór określonych ustawień konfiguracyjnych. Można mieć maksymalnie 30 profili z różnymi priorytetami i wzorami. Wyświetlone profile zawierają przegląd ustawień, takich jak nazwa, priorytet, oświetlenie i syrena.



Create (Utwórz): Kliknij w celu utworzenia profilu.

- **Preview/Stop preview (Włącz podgląd/Zatrzymaj podgląd):** Pozwala włączyć lub zatrzymać podgląd profilu przed jego zapisaniem.

Uwaga

Nie można mieć dwóch profili o tej samej nazwie.

- **Nazwa:** Wprowadź nazwę profilu.
- **Description (Opis):** Wprowadź opis profilu.
- **Light (Oświetlenie):** Z rozwijalnego menu wybierz odpowiednie parametry światła: **Pattern (Wzór)**, **Speed (Prędkość)**, **Intensity (Intensywność)** i **Color (Kolor)**.
- **Siren (Syrena):** Z rozwijalnego menu wybierz odpowiednie wartości parametrów **Pattern (Wzór)** i **Intensity (Intensywność)** syreny.
-   Włącz lub wyłącz podgląd tylko oświetlenia lub syreny.
- **Duration (Czas trwania):** Ustaw czas trwania działań.
 - **Continuous (Ciągłe):** Po rozpoczęciu czynności będzie ona trwać aż do zatrzymania.
 - **Time (Godzina):** Ustaw czas, przez jaki ma trwać działanie.
 - **Repetitions (Powtórzenia):** Ustaw, ile razy działanie ma być powtarzane.
- **Priority (Priorytet):** Ustaw priorytet aktywności jako wartość liczbową z zakresu od 1 do 10. Działań o numerze priorytetu wyższym niż 10 nie można usunąć z listy statusów. Istnieją trzy działania o priorytecie wyższym niż 10: **Maintenance (Konserwacja)** (11), **Identify (Identyfikacja)** (12) i **Health check (Kontrola stanu)** (13).



Import (Importuj): Dodaj jeden lub więcej profili ze wstępnie zdefiniowanymi konfiguracjami.

- **Add (Dodaj)**  : Dodaj nowy profil.
- **Delete and add (Usuń i dodaj)**  : Stare profile są usuwane i można wtedy przesłać nowe profile.
- **Overwrite (Nadpisz):** Zaktualizowane profile zastępują istniejące.

Aby skopiować profil i zapisać go na innych urządzeniach, wybierz co najmniej jeden profil i kliknij przycisk **Export (Eksportuj)**. Zostanie wyeksportowany plik .json.



Uruchom profil. Profil i jego działania zostaną wyświetlone na liście stanu.



Wybierz, co chcesz zrobić z profilem: **Edit (Edytuj)**, **Copy (Kopiuj)**, **Export (Eksportuj)** lub **Delete (Usuń)**.

Nagrania

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

- Rozpoczęcie rejestrowania.



Wybierz skonfigurowaną siećową pamięć masową.



Zatrzymywanie nagrywania.

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.

Media

+ Dodaj: Kliknij, aby dodać nowy plik.

Storage location (Lokalizacja pamięci masowej): Wybierz zapisywanie pliku w pamięci wewnętrznej lub w zainstalowanej pamięci masowej (karta SD, o ile jest dostępna).



Menu kontekstowe zawiera opcje:

- **Information (Informacje):** Wyświetlanie informacji o pliku.
- **Copy link (Kopiuje łącze):** Kopiowanie łącza do lokalizacji pliku w urządzeniu.
- **Usuń:** Usunięcie pliku z lokalizacji pamięci masowej.

Aplikacje



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

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

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



Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

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

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



Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

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

System

Czas i lokalizacja

Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

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

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

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

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

Uwaga

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

Lokalizacja urządzenia

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

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

Sieć

IPv4

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

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

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

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

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

Uwaga

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

IPv6

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

Nazwa hosta

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

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

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

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

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

Serwery DNS

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

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

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

HTTP i HTTPS

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

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

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

Uwaga

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

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

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

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

Protokoły wykrywania sieci

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

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

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

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

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

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

Globalne serwery proxy

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

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

Dozwolone formaty serwerów proxy HTTP i HTTPS:

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

Uwaga

Uruchom urządzenie ponownie, aby zastosować ustawienia globalnych serwerów proxy.

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

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

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

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

Allow O3C (Zezwalaj na O3C):

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

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

Host: Wprowadź adres serwera proxy.

Port: wprowadź numer portu służącego do uzyskania dostępu.

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

Authentication method (Metoda uwierzytelniania):

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

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

SNMP

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

SNMP: Wybierz wersję SNMP.

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

Uwaga

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

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

Bezpieczeństwo

Certyfikaty

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

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

Obsługiwane są następujące formaty:

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

Ważne

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



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

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



Menu kontekstowe zawiera opcje:

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

Secure keystore (Bezpieczny magazyn kluczy)  :

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

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1x

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

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

IEEE 802.1AE MACsec

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

Certyfikaty

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

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

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

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

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

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

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

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

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

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

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

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

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

Zapobiegaj atakom typu brute force

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

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

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

Zapora

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

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

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

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

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

Rule type (Rodzaj reguły):

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

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

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

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

Niestandardowy podpisany certyfikat systemu AXIS OS

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

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



Menu kontekstowe zawiera opcje:

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

Konta

Konta

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Privileges (Przywileje):

- **Administrator:** Ma nieograniczony dostęp do wszystkich ustawień. Administrator może też 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 przyznania poświadczeń klienta

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

Verification URI (Weryfikacja URI): wprowadź łącze internetowe do uwierzytelniania punktu końcowego interfejsu programowania aplikacji (API).

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

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

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

Save (Zapisz): kliknij, aby zapisać wartości.

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 (Adres 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 dozorczy): Wprowadź wartość dla roli dozorczy.

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 wyzwajające 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 kolejowania 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 tę 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 urządzeniom 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 żadaną 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 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: UDP, 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 SIPS 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 zmieniać) 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.

Profile strumienia

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



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

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

Nazwa: Nadaj profilowi nazwę.

Description (Opis): Dodaj opis profilu.

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

Rozdzielczość: Opis tego ustawienia znajduje się w temacie .

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

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

Zipstream  : Opis tego ustawienia znajduje się w temacie .

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

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

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

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

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

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

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

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

ONVIF

Konta ONVIF

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

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



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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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

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

Rola:

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



Menu kontekstowe zawiera opcje:

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

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

Profile mediów ONVIF

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



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

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

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

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

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

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

Uwaga

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

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

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

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

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

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

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

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

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

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

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

PTZ  : Wybierz ustawienia PTZ dla swojej konfiguracji.

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

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

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

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

Detektory

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.

Czujnik PIR

Czujnik PIR mierzy natężenie promieniowania IR emitowanego przez obiekty znajdujące się w jego polu widzenia.

Sensitivity level (Poziom czułości): Wyreguluj poziom w zakresie od 0 do 100, gdzie 0 oznacza najmniejszą czułość, a 100 – największą.

Ustawienia zasilania

Stan zasilania

Wyświetla informacje o stanie zasilania. Informacje różnią się w zależności od produktu.

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 zbiecia szyby.

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

Port

Nazwa: edytuj tekst, aby zmienić nazwę portu.

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

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

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

Uwaga

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

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

Dzienniki**Raporty i dzienniki****Raporty**

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

Dzienniki

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

Zdalny dziennik systemu

Syslog to standard rejestrowania komunikatów. Umożliwia on oddzielenie oprogramowania, które generuje komunikaty, systemu przechowującego je i oprogramowania, które je raportuje i analizuje. Każdy komunikat jest

oznaczany etykietą z kodem obiektu wskazującym typ oprogramowania, które wygenerowało komunikat, oraz przypisany poziom ważności.



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

Host: Wprowadź nazwę hosta lub adres IP serwera.

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

- Axis
- RFC 3164
- RFC 5424

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

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

Port: Wpisywanie innego numeru portu w miejsce obecnego.

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

Type (Typ): wybierz rodzaj dzienników do wysłania.

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

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

Zwykła konfiguracja

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

Konserwacja

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
- Maskę 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 najnowszą wersję, odwiedź stronę axis.com/support.

Po uaktualnieniu masz do wyboru trzy opcje:

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

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

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

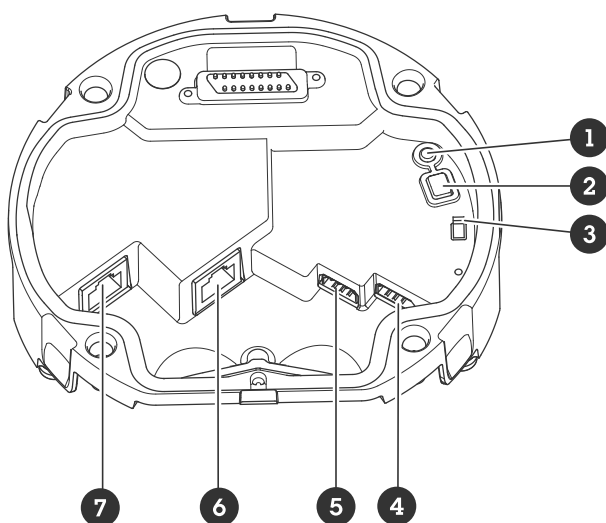
Plik śladu sieciowego może zawierać dane poufne, takie jak certyfikaty lub hasła.

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

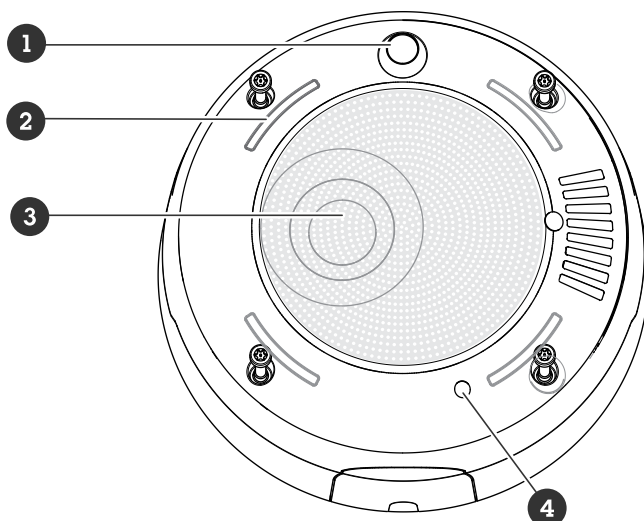
Trace time (Czas śledzenia): Wybierz czas trwania śledzenia w sekundach lub minutach i kliknij przycisk **Download (Pobierz)**.

Specyfikacje

Przegląd produktów



- 1 Wskaźnik LED stanu
- 2 Przycisk kontrolny
- 3 Przełącznik mikrofonu
- 4 Złącze I/O
- 5 Złącze RS-485
- 6 Złącze sieciowe (PoE OUT)
- 7 Złącze sieciowe (PoE IN)



- 1 Czujnik PIR
- 2 Diody sygnalizacyjne LED
- 3 Głośnik
- 4 Wewnętrzny mikrofon

Dioda stanu

Dioda stanu	Wskazanie
Zgaszony	Zgaszony przy normalnym działaniu.
Zielony	Stałe światło przez 10 sekund przy normalnym działaniu po zakończeniu uruchamiania.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.
Bursztynowy/czerwony	Miga, gdy połączenie sieciowe jest niedostępne lub przerwane.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz .

Przełącznik mikrofonu

Lokalizacja przycisku mikrofonu: .

Przycisk mikrofonu to mechaniczny przycisk służący do **włączania** lub **wyłączania** mikrofonu. Domyślnie mikrofon ma ustawienie **OFF** (Wyłączony).

Złącza

Złącze sieciowe

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

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

Złącze I/O

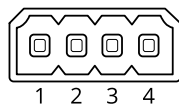
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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 zbiecia szyby.

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

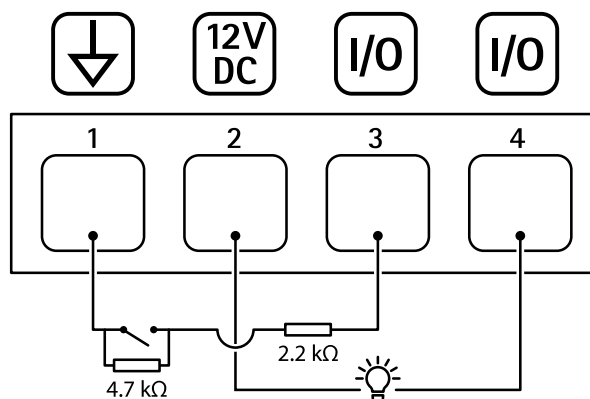
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

4-pinowy blok złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	 Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 25 mA
Konfigurowalne (wejście lub wyjście)	3–4	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:

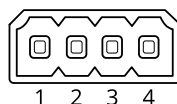


- 1 Masa DC
- 2 Wyjście DC 12 V, maks. 25 mA
- 3 I/O skonfigurowane jako wejście nadzorowane
- 4 We/Wy skonfigurowane jako wyjście

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 (czterużyłowy)
- 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	

Nazwy wzorów świateł

Wył.
Stałe światło
Alternatywna
Impuls
Nasilanie w 3 stopniach
Miganie
Miganie 3x
Miganie 4x
Miganie 3x i zanikanie
Miganie 4x i zanikanie
Błysk 1x
Błysk 3x

Nazwy sposobów sygnalizacji w sygnalizatorze akustyczno-optycznym

Wył.
Alarm: Alarm o wysokich tonach dźwięku
Alarm: Alarm o niskich tonach dźwięku
Alarm: Ptak
Alarm: Syrena na łodzi
Alarm: Alarm samochodowy
Alarm: Szybki alarm samochodowy
Alarm: Zegar klasyczny
Alarm: Pierwszy gość
Alarm: Horror
Alarm: Przemysł
Alarm: Pojedynczy sygnał dźwiękowy
Alarm: Łagodny sygnał dźwiękowy quada

Alarm: Łagodny potrójny sygnał dźwiękowy
Alarm: Potrójny o wysokich tonach dźwięku
Powiadomienie: Zaakceptowano
Powiadomienie: Nawiązywanie połączenia
Powiadomienie: Odmowa
Powiadomienie: Gotowe
Powiadomienie: Wejście
Powiadomienie: Niepowodzenie
Powiadomienie: Pośpiesz się
Powiadomienie: Wiadomość
Powiadomienie: Dalej
Powiadomienie: Otwarte
Siren (Syrena): Alternatywna
Siren (Syrena): Piłka
Siren (Syrena): Ewakuacja
Siren (Syrena): Dźwięk o opadającej wysokości
Siren (Syrena): Łagodny domowy

Czyszczenie urządzenia

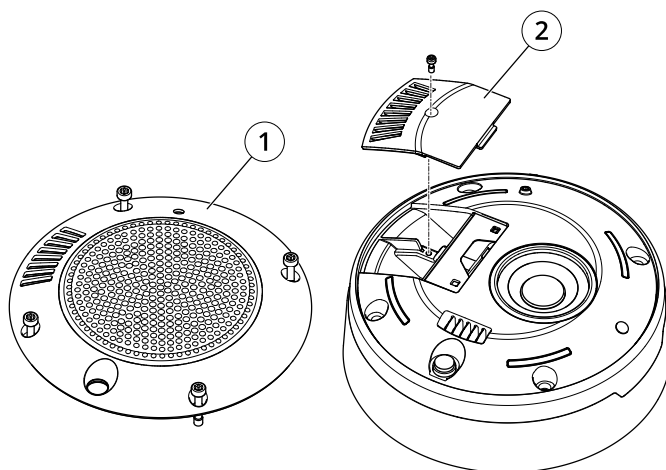
Urządzenie można czyścić letnią wodą.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
- 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.

Uwaga

- Zdejmij pokrywę (1) i drzwi (2).
- Usuń kurz przy użyciu szczotki.



- 1 Osłona
2 Drzwi

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:

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

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 <code>ping</code> oraz adres IP urządzenia): - Jeśli otrzymasz: <code>Reply from <IP address>: bytes=32; time=10...</code>, 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: <code>Request timed out</code>, 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 <code>http</code> lub <code>https</code> 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.
--	---

Urządzenie nie uruchamia się po dołączeniu go do innego produktu

Nieodpowiednia klasa PoE	Gdy urządzenie jest dołączone do innego produktu, sprawdź, czy stosowane jest zasilanie PoE klasy 4.
--------------------------	--

Dane z czujnika są niedokładne

Niedokładne dane z czujnika	Wskaźniki AQI (Wskaźnik jakości powietrza), CO ₂ , LZO i NO _x potrzebują czasu, aby prezentować prawidłowe wartości. Patrz .
-----------------------------	--

Kwestie wydajności

Najważniejsze czynniki, które należy wziąć pod uwagę:

- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.

Kontakt z pomocą techniczną

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

T10222990_pl

2025-09 (M2.4)

© 2025 Axis Communications AB