

AXIS D4200-VE Network Strobe Speaker

Spis treści

Informacje o rozwiązaniu.....	4
.....	4
Instalacja.....	5
Od czego zacząć.....	6
.....	6
Wyszukiwanie urządzenia w sieci.....	6
Obsługiwane przeglądarki.....	6
Otwórz interfejs WWW urządzenia.....	6
Utwórz konto administratora.....	6
Bezpieczne hasła.....	7
Upewnianie się co do braku zmian w oprogramowaniu urządzenia	7
Konfiguracja urządzenia	8
Konfiguracja profilu.....	8
Konfiguracja profilu z niestandardowym plikiem audio syreny.....	8
Importowanie/eksportowanie profilu	8
Konfiguracja bezpośredniego połączenia SIP (P2P).....	8
Konfiguracja SIP przez serwer (PBX)	9
Kalibracja i przeprowadzanie zdalnego testu głośnika	10
Konfiguracja reguł dotyczących zdarzeń	10
Wyzwalanie akcji.....	10
Uruchamianie profilu po wyzwoleniu alarmu	11
Uruchamianie profilu przy użyciu protokołu SIP	11
Sterowanie kilkoma profilami za pomocą rozszerzeń SIP	11
Uruchamianie dwóch profili o różnych priorytetach.....	12
Aktywowanie głośnika ze stroboskopem przez HTTP post po wykryciu ruchu przez kamerę.....	13
Aktywowanie głośnika ze stroboskopem przez wirtualne wejście po wykryciu ruchu przez kamerę	14
Aktywowanie głośnika ze stroboskopem przez MQTT po wykryciu ruchu przez kamerę	15
Wysyłanie wiadomości e-mail w razie niepowodzenia testu głośnika.....	17
Odtwarzanie niestandardowego klipu po wyzwoleniu alarmu	18
Zatrzymywanie nadawania audio za pomocą DTMF	18
Konfigurowanie dźwięku dla przychodzących połączeń SIP.....	19
Interfejs WWW.....	21
Więcej informacji.....	22
Protokół inicjacji sieci (Session Initiation Protocol, SIP)	22
Peer-to-peer SIP (P2PSIP).....	22
Private Branch Exchange (PBX) – centrala abonencka	22
NAT Transversal.....	23
Analizy i aplikacje	23
AXIS Audio Analytics.....	23
InformaCast®	24
Specyfikacje	25
Przegląd produktów.....	25
Wskaźniki LED.....	26
Gniazdo karty SD.....	27
Przyciski.....	27
Przycisk kontrolny.....	27
Przełącznik mikrofonu	27
Złącza	27
Złącze sieciowe	27
Złącze audio.....	27
Złącze I/O	28
Nazwy wzorów świateł	29

Nazwy wzorów dźwiękowych	30
Czyszczenie urządzenia	31
Rozwiązywanie problemów –	32
Przywróć domyślne ustawienia fabryczne	32
Opcje systemu AXIS OS	32
Sprawdzanie bieżącej wersji systemu AXIS OS	32
Aktualizacja systemu AXIS OS:.....	33
Problemy techniczne i możliwe rozwiązania.....	33
Kwestie wydajności	36
Kontakt z pomocą techniczną.....	36
Cyberbezpieczeństwo	37
Postępowanie z lukami w zabezpieczeniach	37
Powiadomienia dotyczące zabezpieczeń	37
Bezpieczny cykl eksploatacji produktu	37

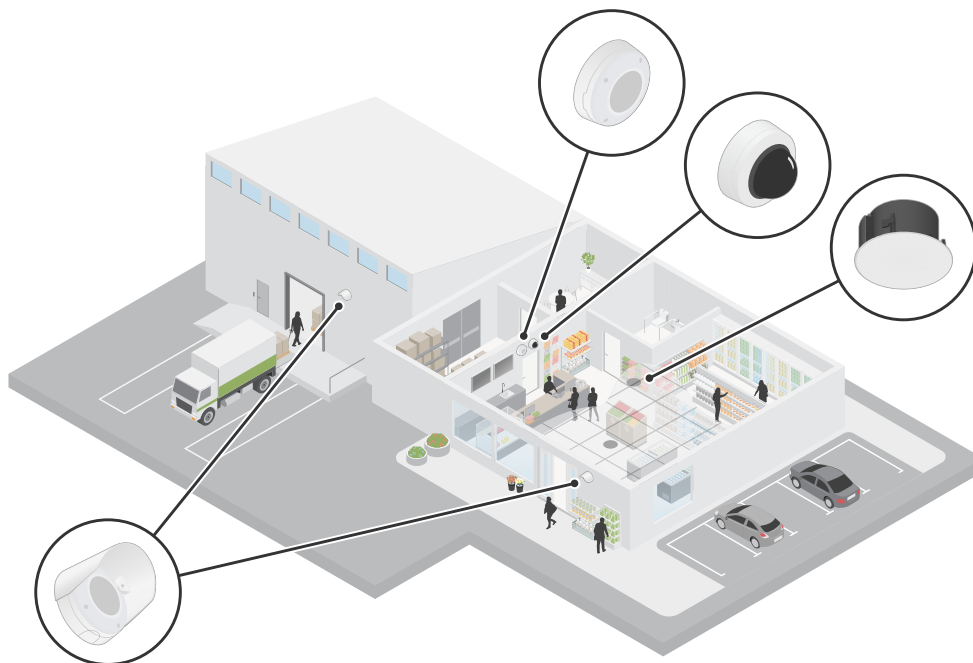
Informacje o rozwiązaniu

W tym podręczniku opisano sposób udostępniania urządzenia w systemie audio oraz konfigurowania urządzenia bezpośrednio w jego interfejsie.

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

- **AXIS Audio Manager Edge** – oprogramowanie do zarządzania dźwiękiem dla małych systemów. Jest wstępnie instalowane na wszystkich urządzeniach audio z oprogramowaniem sprzętowym w wersji 10.0 i nowszych.
 - *Podręcznik użytkownika oprogramowania AXIS Audio Manager Edge*
- **AXIS Audio Manager Pro** – zaawansowane oprogramowanie do zarządzania dźwiękiem w dużych systemach.
 - *Podręcznik użytkownika oprogramowania AXIS Audio Manager Pro*
- **AXIS Camera Station Pro** – zaawansowane oprogramowanie do zarządzania materiałem wizyjnym przeznaczone do dużych systemów.
 - *Instrukcja obsługi użytkownika oprogramowania AXIS Camera Station Pro*

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



Instalacja

Ważne

Nie należy instalować głośnika ze stroboskopem i podłączonych urządzeń w odległości mniejszej niż 3 m od środka torów kolejowych.

Poniższe wideo przedstawia przykładowy sposób instalacji urządzenia AXIS D4200-VE Network Strobe Speaker.



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

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 *Utwórz konto administratora, on page 6*.

Opisy wszystkich funkcji i ustawień interfejsu WWW urządzeń z systemem operacyjnym AXIS OS można znaleźć na stronie *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła, on page 7*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne, on page 32*.

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 *Przywróć domyślne ustawienia fabryczne, on page 32*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

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 *Konfiguracja profilu, on page 8*.
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.

Więcej informacji o ustawieniach, p. sekcja *SIP*.

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.
5. 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, p. sekcja *NAT traversal*.

6. 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.
7. 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 (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.
8. 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.

Więcej informacji o ustawieniach, p. sekcja *SIP*.

1. Od dostawcy PBX należy uzyskać następujące informacje:
 - ID użytkownika
 - Domena
 - Hasło
 - ID uwierzytelniania
 - ID rozmówcy
 - Rejestrator

- Port początkowy RTP
- 2. Aby dodać nowe konto, przejdź do okna **System > SIP > SIP accounts (Konta SIP)** i kliknij przycisk **+ Account (+ Konto)**.
- 3. Wprowadź informacje otrzymane od dostawcy usług centrali telefonicznej (PBX).
- 4. Kliknij opcję **Registered (Zarejestrowane)**.
- 5. Wybierz tryb transmisji.
- 6. Kliknij przycisk **Zapisz**.
- 7. Skonfiguruj ustawienia SIP w taki samo sposób, jak peer-to-peer. Więcej informacji: *Konfiguracja bezpośredniego połączenia SIP (P2P)*, on page 8.

Kalibracja i przeprowadzanie zdalnego testu głośnika

Za pomocą testu głośnika można z odległości sprawdzić, czy głośnik działa w oczekiwany sposób. Test głośnika to seria dźwięków testowych rejestrowanych przez wbudowany mikrofon. Po każdym przeprowadzeniu testu zarejestrowane wartości są porównywane z wartościami zarejestrowanymi podczas kalibracji.

Uwaga

Kalibrację do testu należy wykonać w położeniu montażowym na miejscu instalacji. Jeśli głośnik zostanie przesunięty lub jego lokalne otoczenie ulegnie zmianie, na przykład, jeśli ściana zostanie zbudowana lub usunięta, głośnik należy ponownie skalibrować.

Podczas kalibracji zaleca się, aby ktoś był fizycznie obecny na miejscu instalacji, aby odsłuchać sygnały testowe i upewnić się, że dźwięki testu nie są stłumione ani zablokowane przez jakiegokolwiek niezamierzone przeszkody na ścieżce akustycznej głośnika.

1. Przejdź do interfejsu urządzenia > **Audio > Speaker test (Dźwięk > Test głośnika)**.
2. Aby skalibrować urządzenie audio, kliknij przycisk **Calibrate (Kalibruj)**.

Uwaga

Po kalibracji produktu Axis można w dowolnym momencie przeprowadzić test głośnika.

3. Aby przetestować głośnik, kliknij przycisk **Run the test (Uruchom test)**.

Uwaga

Inny sposób zainicjowania kalibracji to naciśnięcie przycisku kontrolnego na fizycznym urządzeniu. Znajdowanie pliku *Control: Przegląd produktów*, on page 25.

Konfiguracja reguł dotyczących zdarzeń

Można utworzyć reguły sprawiające, że urządzenie będzie wykonywać konkretne akcje po wystąpieniu określonych zdarzeń. Reguła składa się z warunków i akcji. Warunki mogą służyć do wyzwalania akcji. Urządzenie może na przykład odtworzyć plik dźwiękowy według harmonogramu lub po odebraniu połączenia albo wysłać wiadomość e-mail, jeśli zmieni się adres IP.

Aby dowiedzieć się więcej, zob. *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 działanie (**Action**) do wykonania po spełnieniu warunków.

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 profili 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.

Aktywowanie głośnika ze stroboskopem przez HTTP post po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do głośnika ze stroboskopem oraz spowodować uaktywnianie się w nim profilu po każdym wykryciu ruchu przez aplikację **AXIS Motion Guard** zainstalowaną w kamerze.

Zanim zaczniesz:

- Utwórz w głośniku ze stroboskopem nowego użytkownika z rolą **Operator** lub **Administrator**.
- Utwórz w głośniku ze stroboskopem profil o nazwie „**Profil głośnika ze stroboskopem**”.
- 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:
 - **Nazwa:** Głośnik ze stroboskopem
 - **Typ:** HTTP
 - **URL:** http://<IPAddress>/axis-cgi/siren_and_light.cgi
Element <IPAddress> (adres IP) zastąp adresem głośnika ze stroboskopem.
 - **Nazwa i hasło** nowo utworzonego użytkownika głośnika ze stroboskopem.
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:** Aktywowanie głośnika ze stroboskopem po wykryciu ruchu
 - **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):** Strobe speaker (Głośnik ze stroboskopem).
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": "Strobe speaker profile"  } }
```

Dla parametru **"profile"** : <> podaj dane wprowadzone na etapie tworzenia profilu dla głośnika ze stroboskopem, w tym przypadku: „**Profil głośnika ze stroboskopem**”.

3. Kliknij przycisk **Zapisz**.
4. Dodaj kolejną regułę z następującymi informacjami:

- Nazwa: Dezaktywowanie głośnika ze stroboskopem po wykryciu ruchu
- 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): Głośnik ze stroboskopem
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": "Strobe speaker profile" } }
```

Dla parametru "profile" : <> podaj dane wprowadzone na etapie tworzenia profilu dla głośnika ze stroboskopem, w tym przypadku: „Profil głośnika ze stroboskopem”.

5. Kliknij przycisk Zapisz.

Aktywowanie głośnika ze stroboskopem przez wirtualne wejście po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do głośnika ze stroboskopem oraz spowodować uaktywnianie się w nim profilu po każdym wykryciu ruchu przez aplikację AXIS Motion Guard zainstalowaną w kamerze.

Zanim zaczniesz:

- Utwórz w głośniku ze stroboskopem nowe konto z uprawnieniami Operatora lub Administratora.
- Utwórz profil w głośniku ze stroboskopem.
- 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
Element <IPaddress> (adres IP) zastąp adresem głośnika ze stroboskopem.
 - Konto i hasło nowo utworzonego konta głośnika ze stroboskopem.
3. Kliknij przycisk Test (Testuj), sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk Zapisz.
5. Dodaj drugiego odbiorcę z następującymi informacjami:
 - Nazwa: Dezaktywacja portu wirtualnego
 - Typ: HTTP
 - URL: http://<adresIP>/axis-cgi/virtualinput/deactivate.cgi
Element <IPaddress> (adres IP) zastąp adresem głośnika ze stroboskopem.
 - Konto i hasło nowo utworzonego konta głośnika ze stroboskopem.
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**.

Utworzenie reguły w głośniku ze stroboskopem:

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

Aktywowanie głośnika ze stroboskopem przez MQTT po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do głośnika ze stroboskopem przez MQTT i aktywować w nim profil za każdym razem, gdy kamera wykryje ruch.

Zanim zaczniesz:

- Utwórz profil w głośniku ze stroboskopem.
- 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):** Wyl.
 - **QoS:** 0, 1 lub 2
5. Kliknij przycisk **Zapisz**.

Konfigurowanie klienta MQTT w głośniku ze stroboskopem:

1. W interfejsie www głośnika ze stroboskopem 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**.

Tworzenie reguły w głośniku ze stroboskopem w odniesieniu do subskrypcji MQTT:

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
 - **Nazwa:** Wykryto ruch
 - **Condition (Warunek):** MQTT > Stateful (Ze stanem)
 - **Subscription filter (Filtr subskrypcyjny):** Ruch

- **Payload (Próbka):** Wł.
 - **Action (Akcja):** 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)**.

Odtwarzanie niestandardowego klipu po wyzwoleniu alarmu

W tym przykładzie wyjaśniono, w jaki sposób wyzwoić 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 zapoznać się ze wszystkimi funkcjami i ustawieniami dostępnymi w interfejsie WWW urządzeń z systemem operacyjnym AXIS OS, przejdź do strony *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Więcej informacji

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

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

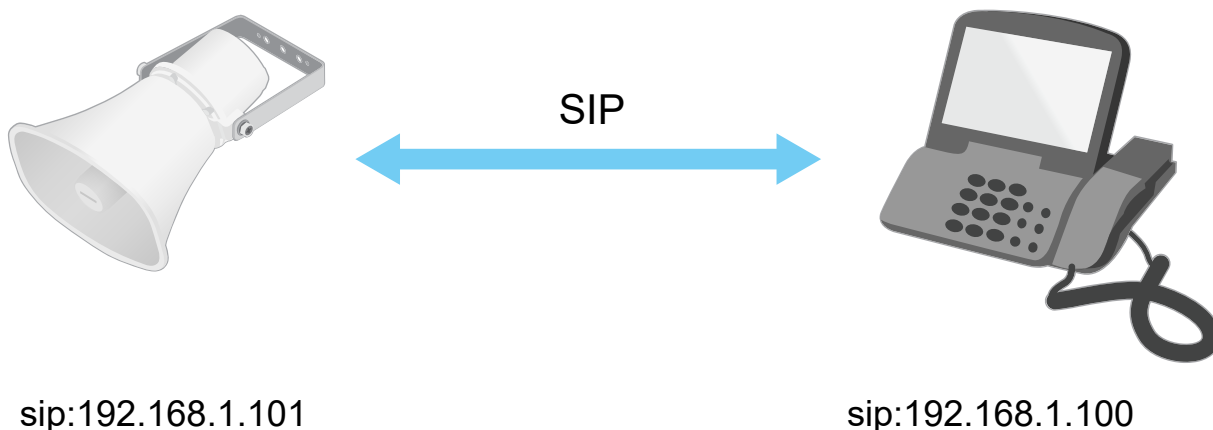
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

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

Peer-to-peer SIP (P2PSIP)

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

Przykład:



Można skonfigurować telefon SIP tak, by łączył się z urządzeniem audio w tej samej sieci za pomocą peer-to-peer SIP.

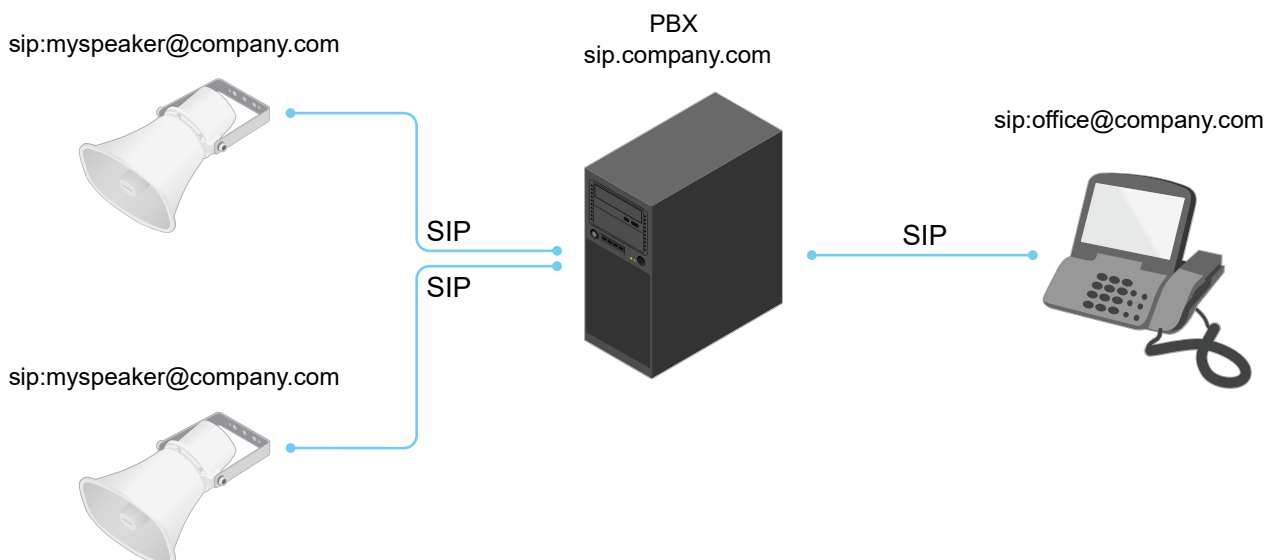
Private Branch Exchange (PBX) – centrala abonencka

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

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

Każdy agent użytkownika SIP jest rejestrowany w PBX; mogą łączyć się z innymi poprzez wybranie właściwego numeru wewnętrznego. Adres SIP to zazwyczaj `sip:<user>@<domain>` lub `sip:<user>@<registrar-ip>`. Adres SIP jest niezależny od adresu IP, a PBX udostępnia urządzenie przez cały czas, kiedy jest ono zarejestrowane.

Przykład:



NAT Transversal

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

Uwaga

Router musi również obsługiwać NAT Traversal i protokół UPnP®.

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

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

Analizy i aplikacje

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

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

AXIS Audio Analytics

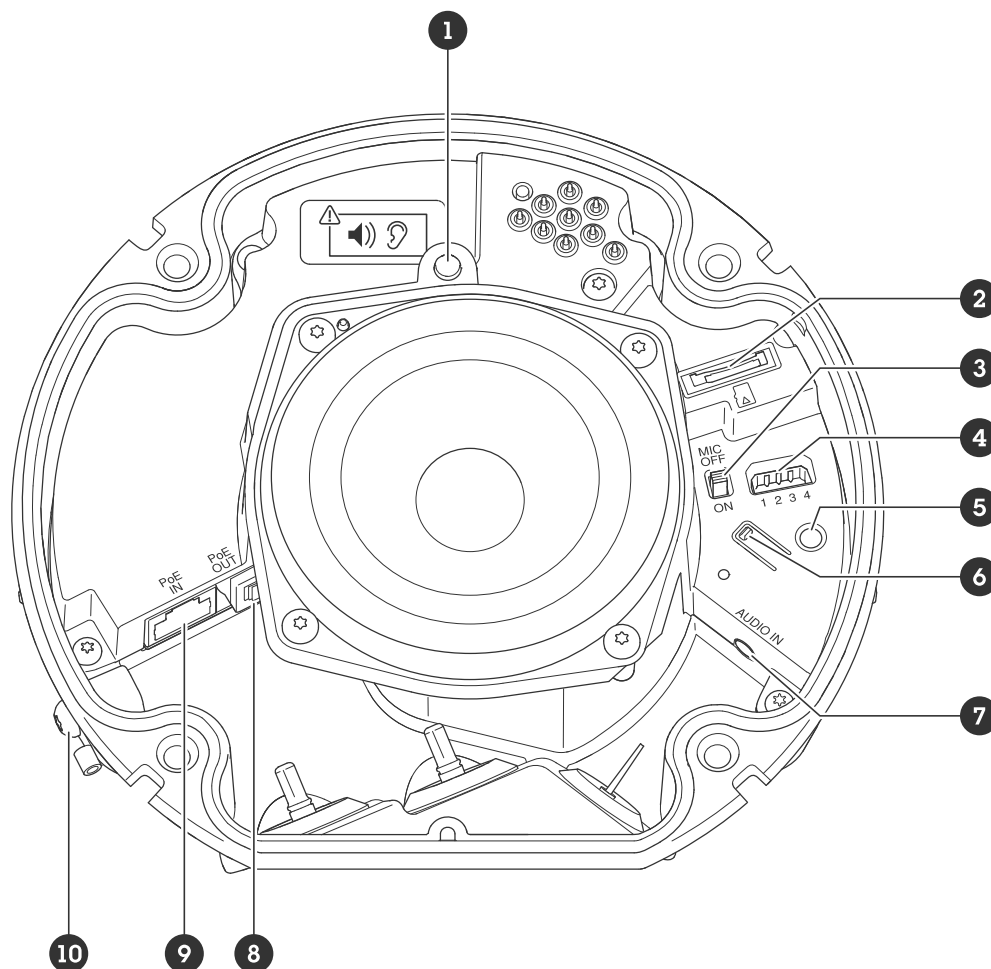
Aplikacja AXIS Audio Analytics wykrywa nagły wzrost głośności dźwięku oraz rozpoznaje typy dźwięków, takie jak wrzaski lub strzały, w zasięgu urządzenia, na którym jest zainstalowana. Funkcje detekcji można skonfigurować tak, aby powodowały wyzwolenie określonej reakcji, np. uruchomienie nagrywania wideo,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

InformaCast®

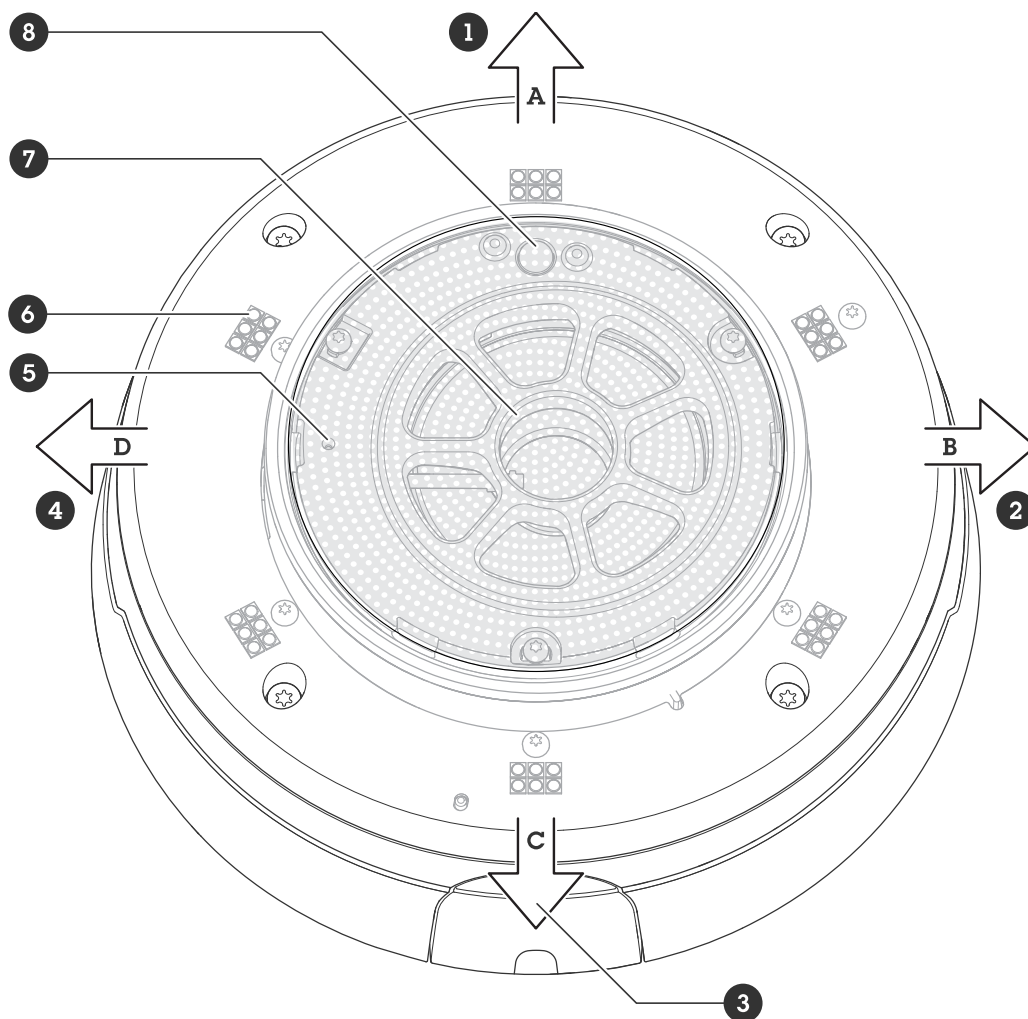
InformaCast to platforma umożliwiająca wysyłanie komunikatów alarmowych i komunikację za pośrednictwem kanałów komunikacyjnych już istniejących w organizacji, w tym głośników sieciowych Axis. System masowego powiadamiania InformaCast rozpowszechnia w całym obiekcie alerty dźwiękowe skutecznie przyciągające uwagę. Więcej informacji na temat aplikacji można znaleźć na stronie *AXIS Speaker Functionality for Singlewire InformaCast*.

Specyfikacje

Przegląd produktów



- 1 Wskaźnik LED audio
- 2 Gniazdo kart microSD
- 3 Przełącznik mikrofonu
- 4 Złącze I/O
- 5 Wskaźnik LED stanu
- 6 Przycisk kontrolny
- 7 Złącze audio
- 8 Złącze sieciowe (PoE OUT)
- 9 Złącze sieciowe (PoE IN)
- 10 Śruba uziemienia



- 1 Kierunek oświetlenia A
- 2 Kierunek oświetlenia B
- 3 Kierunek oświetlenia C
- 4 Kierunek oświetlenia D
- 5 Wewnętrzny mikrofon
- 6 Diody sygnalizacyjne LED
- 7 Głośnik
- 8 Wskaźnik LED audio

Wskaźniki LED

Dioda stanu	Wskazanie
Zgaszony	Połączenie i normalne działanie.
Zielony	Stałe zielone światło przez 10 sekund przy normalnym działaniu po zakończeniu uruchamiania.
Bursztynowy	Stałe światło podczas uruchamiania, przywracania domyślnych ustawień fabrycznych lub odtwarzania ustawień.

Gniazdo karty SD

POWIADOMIENIE

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

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



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

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Kalibracji testu głośnika. Naciśnij i zwolnij przycisk Control; zostanie odtworzony sygnał testowy.
- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne*, on page 32.
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby nawiązać połączenie, naciśnij i zwolnij przycisk, a następnie poczekaj, aż dioda LED stanu mignie trzy razy na zielono.

Przełącznik mikrofonu

Lokalizacja przycisku mikrofonu: *Przegląd produktów*, on page 25.

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

Złącza

Złącze sieciowe

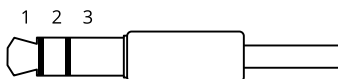
Złącze RJ45 Ethernet z zasilaniem Power over Ethernet (PoE).

POWIADOMIENIE

Urządzenie musi zostać podłączone przy pomocy kabla ekranowanego (STP). Wszystkie kable łączące urządzenie z siecią powinny być używane zgodnie z przeznaczeniem. Upewnij się, że urządzenia sieciowe zainstalowane są zgodnie z zaleceniami producenta. Informacje dotyczące wymogów regulacyjnych znajdują się w instrukcji instalacji kamery dostępnej w witrynie www.axis.com.

Złącze audio

- **Wejście audio** – wejście 3,5 mm dla mikrofonu cyfrowego, analogowego mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).



Wejście audio

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

Uwaga

Maksymalna długość podłączonego przewodu wynosi 30 m.

Złącze I/O

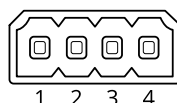
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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 zbitcia szyby.

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

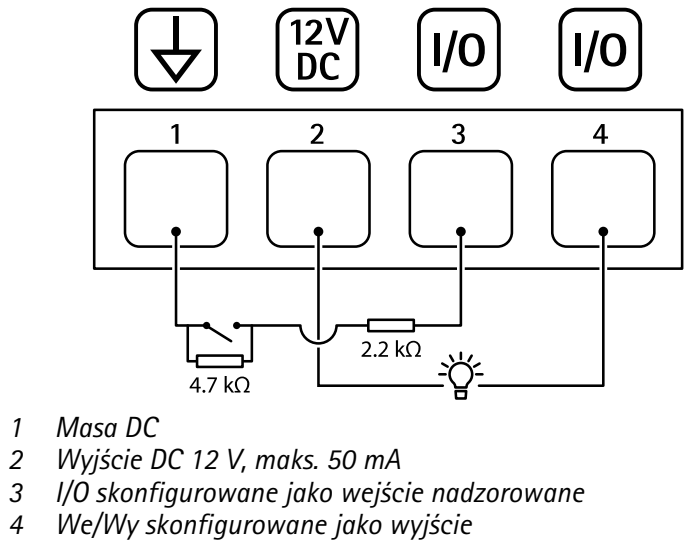
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

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 = 50 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:



Uwaga

Maksymalna długość podłączonego przewodu wynosi 30 m.

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
Kierunek A
Kierunek B
Kierunek C
Kierunek D
Obróć
Losowo
Wirujące

Nazwy wzorów dźwiękowych

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

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

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
 - Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawianie plam na obudowie.
1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
 2. W razie potrzeby można wyczyścić urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą i łagodnym mydłem niezawierającym środków ściernych.
 3. Aby usunąć jakiegokolwiek pozostałości środków czyszczących, należy przetrzeć urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą.
 4. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Więcej informacji na temat czyszczenia urządzeń Axis znajduje się w białej księdze *Odporność chemiczna na popularne środki czyszczące*.

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

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

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów*, on page 25.
3. Przytrzymuj przycisk Control przez 10 sekund, aż wskaźnik LED stanu ponownie zmieni kolor na bursztynowy.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
 - Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej: Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
 - Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej: 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do produktu.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

- Po aktualizacji oprogramowania urządzenia poczynione ustawienia zostaną zachowane. Axis Communications AB nie gwarantuje, że ustawienia te zostaną zachowane, nawet gdy funkcje są dostępne w nowej wersji systemu operacyjnego AXIS OS.
- Począwszy od systemu operacyjnego AXIS OS w wersji 12.6, pomiędzy aktualną a docelową wersją urządzenia należy zainstalować każdą wersję LTS. Przykładowo, jeżeli aktualnie zainstalowana wersja oprogramowania urządzenia to AXIS OS 11.2, przed aktualizacją urządzenia do wersji AXIS OS 12.6 należy zainstalować wersję LTS AXIS OS 11.11. Więcej informacji znajduje się w dokumencie *Cykl eksploatacji oprogramowania AXIS OS: ścieżka aktualizacji*.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony axis.com/support/device-software, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.
1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie axis.com/support/device-software.
 2. Zaloguj się do urządzenia jako administrator.
 3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS) > Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

Problemy techniczne i możliwe rozwiązania

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

Nie można ustawić adresu IP

- 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 może być używany przez inne urządzenie. Aby to sprawdzić:
 1. Odłącz urządzenie Axis od sieci.
 2. W oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia.
 3. Jeśli otrzymasz: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie.
 4. Jeśli otrzymasz: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
- Może występować potencjalny konflikt adresu 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.

Problemy z dostępem do urządzenia

Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki

Gdy protokół HTTPS jest włączony, upewnij się, że podczas próby zalogowania się używasz prawidłowego protokołu (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki.

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje: *Przywróć domyślne ustawienia fabryczne, on page 32.*

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 możesz ręcznie przydzielić 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)**.

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, patrz *Obsługiwane przeglądarki, on page 6.*

Nie można uzyskać dostępu do urządzenia 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 Pro: 90-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

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

Problemy z plikami audio

Nie można przesłać klipu multimedialnego

Obsługiwane są następujące formaty klipów:

- format pliku au, zakodowany przy użyciu μ -law z próbkowaniem 8 lub 16 kHz.
- format pliku wav, zakodowany w formacie audio PCM. Obsługa kodowania w formacie 8 lub 16-bitowym mono lub stereo z częstotnością próbkowania 8 do 48 kHz.
- format plików mp3, mono lub stereo z przepływnością 64 kb/s do 320 kb/s, z częstotnością próbkowania 8 do 48 kHz.

Klipy multimedialne są odtwarzane z różną głośnością

Plik dźwiękowy jest rejestrowany ze pewnym wzmocnieniem. Jeżeli utworzono klipy audio z różnym wzmocnieniem, będą one odtwarzane z różną głośnością. Upewnij się, że korzystasz z klipów, które mają takie samo wzmocnienie.

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

Zapora sieciowa blokuje ruch korzystający z 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.

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

Wystąpiły problemy z dźwiękiem

Urządzenie nie jest tak głośne, jak oczekiwano	Sprawdź, czy urządzenie jest prawidłowo zamknięte i czy w tubie lub na elemencie głośnikowym nie ma występują żadnych przeszkody.
--	---

Problemy ze światłem	
Urządzenie nie jest tak jasne, jak oczekiwano	Sprawdź, czy używany jest zasilacz PoE klasy 4. Sprawdź, jaka jest temperatura otoczenia urządzenia. Jeśli urządzenie działa w środowisku, w którym panuje wysoka temperatura, światła zostaną automatycznie przyciemnione.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wymaganą przepustowość (przepływność).

Najważniejsze czynniki, które należy uwzględnić:

- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

Kontakt z pomocą techniczną

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

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do cyberbezpieczeństwa znajdują się na stronie: axis.com/about-axis/cybersecurity. Przestrzegaj poniższych wytycznych dotyczących cyberbezpieczeństwa, aby otrzymywać powiadomienia od Axis dotyczące bezpieczeństwa produktów oraz skonfigurować produkt w sposób zapewniający bezpieczny cykl eksploatacji oraz wycofanie z użytku.

Na stronie *Axis Trust Center* znajdują się informacje o sposobach, w jakie Axis zapewnia zgodność z wymogami bezpieczeństwa, transparentność, ochronę danych oraz ochronę prywatności.

Postępowanie z lukami w zabezpieczeniach

Axis ma status *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA)*. Aby zminimalizować ryzyko narażenia na zagrożenia, postępujemy zgodnie z branżowymi normami w zakresie wykrywania i usuwania luk w zabezpieczeniach naszych urządzeń, oprogramowania i usług. Informacje na temat naszej polityki zarządzania lukami w zabezpieczeniach oraz instrukcje dotyczące zgłaszania luk znajdują się na stronie axis.com/vulnerability-management.

Powiadomienia dotyczące zabezpieczeń

Subskrybuj powiadomienia o zagrożeniach bezpieczeństwa w produktach Axis na stronie axis.com/security-notification-service. Będziemy informować Cię o lukach w zabezpieczeniach, udzielać odnośnych wskazówek oraz powiadamiać o innych kwestiach związanych z bezpieczeństwem użytkowanego produktu Axis.

Bezpieczny cykl eksploatacji produktu

Axis minimalizuje ryzyko w całym cyklu eksploatacji swoich produktów dzięki bezpiecznemu zarządzaniu cyklem eksploatacji. Skorzystaj z naszych przewodników dotyczących zwiększenia bezpieczeństwa dostępnych na stronie help.axis.com, aby bezpieczniej konfigurować i obsługiwać produkty Axis oraz uzyskać informacje na poniższe tematy:

Bezpieczne pierwsze użycie – Produkty Axis są skonfigurowane fabrycznie z wysokim poziomem domyślnej ochrony, co oznacza bezpieczną pierwszą konfigurację oraz szyfrowaną komunikację od samego początku użytkowania.

Przeznaczenie i typowe błędy w konfiguracji – Nasze przewodniki zawierają informacje o przeznaczeniu produktów Axis, w tym o typowych błędach użytkowania związanych z bezpieczeństwem oraz błędach przy konfiguracji, których należy unikać.

Zarządzanie lukami w zabezpieczeniach i transparentność łańcucha dostaw – Wraz z każdą wersją oprogramowania na stronie axis.com publikowany jest wykaz komponentów oprogramowania (SBOM – Software Bill of Material) w celu poinformowania o lukach w zabezpieczeniach (podatnościach na zagrożenie) oraz zwiększenia transparentności łańcucha dostaw.

Wycofanie z eksploatacji i bezpieczne usuwanie danych – Aby bezpiecznie wycofać produkt po zakończeniu cyklu eksploatacji, przywróć jego ustawienia fabryczne. Spowoduje to usunięcie konfiguracji, zapisanych danych oraz informacji poufnych.

T10217687_pl

2026-07 (M6.2)

© 2025 – 2026 Axis Communications AB