Głośnik sieciowy z wyświetlaczem AXIS C1720 Network Display Speaker

Podręcznik użytkownika

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
Kalibracja i przeprowadzanie zdalnego testu głośnika....8
Tworzenie profilu oświetlenia....8
Konfiguracja bezpośredniego połączenia SIP (P2P)....8
Konfiguracja SIP przez serwer (PBX)....9
Konfiguracja reguł dotyczących zdarzeń....10
Wysyłanie wiadomości e-mail w razie niepowodzenia testu głośnika....10
Odtwarzanie audio po wykryciu ruchu przez kamerę....11
Zatrzymywanie nadawania audio za pomocą DTMF....11
Konfigurowanie dźwięku dla przychodzących połączeń SIP....12
Wyświetlenie komunikatu na wyświetlaczu....13
Wyzwalanie diody sygnalizacyjnej LED za pomocą czujnika PIR....13
Interfejs WWW....15
Więcej informacji....16
Voice over IP (VoIP)....16
Protokół inicjacji sieci (Session Initiation Protocol, SIP)....16
Peer-to-peer SIP (P2PSIP)....16
Private Branch Exchange (PBX) – centrala abonencka....16
NAT Transversal....17
Analizy i aplikacje....17
AXIS Audio Analytics....17
Specyfikacje....19
Przegląd produktów....19
Wskaźniki LED....19
Gniazdo karty SD....20
Przyciski....20
Przycisk kontrolny....20
Przycisk wyłączania mikrofonu....20
Złącza....20
Złącze sieciowe....20
Złącze audio....20
Złącze I/O....21
Rozwiązywanie problemów –....23
Przywróć domyślne ustawienia fabryczne....23
Opcje systemu AXIS OS....23
Sprawdzanie bieżącej wersji systemu AXIS OS....23
Aktualizacja systemu AXIS OS:....24
Problemy techniczne i możliwe rozwiązania....24
Kwestie wydajności....27
Uwagi dotyczące zasilania....27
Kontakt z pomocą techniczną....27
Cyberbezpieczeństwo....28

Postępowanie z lukami w zabezpieczeniach 28
Powiadomienia dotyczące zabezpieczeń 28
Bezpieczny cykl eksploatacji produktu 28

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*.



Ogólne informacje o działaniu sieciowych systemów audio.

Instalacja

Poniższe wideo przedstawia przykładowy sposób instalacji urządzenia AXIS C1720 na ścianie. Instrukcje dotyczące instalacji na suficie, a także informacje dotyczące bezpieczeństwa, można znaleźć na stronie *axis.com/products/axis-c1720/support*



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*.

Uwaga

Gdy produkt ma aktywne ustawienia fabryczne, jego adres IP jest widoczny na wyświetlaczu. Po otwarciu interfejsu WWW i utworzeniu użytkownika na wyświetlaczu pojawi się zegar i data.

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

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 23*.

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 23*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

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 jakiekolwiek niezamierzone przeszkody na ścieżce akustycznej głośnika. Aby uniknąć uszkodzenia słuchu, podczas testu instalator powinien zachować bezpieczną odległość od 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 19*.

Tworzenie profilu oświetlenia

Profil to zbiór określonych ustawień konfiguracyjnych. Można mieć maksymalnie 30 profili na źródło oświetlenia z różnymi priorytetami i wzorami. Profil może mieć tylko jedno źródło oświetlenia, więc jeśli chcesz mieć profile dla obu źródeł oświetlenia, musisz utworzyć co najmniej dwa profile.

Tworzenie nowego profilu:

1. Przejdź do obszaru **Light > Profiles (Oświetlenie i profile)** i kliknij opcję + **Create (Utwórz)**.
2. Wypełnij pola **Name (Nazwa)** i **Description (Opis)**.
3. Wybierz ustawienia dla opcji **Light (Oświetlenie)**, które będą używane w profilu.
4. Ustaw **Priority (Priorytet)** dla oświetlenia, a następnie kliknij przycisk **Save (Zapisz)**.
5. Aby edytować profil, kliknij ⋮ i wybierz opcję **Edit (Edytuj)**.

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 żądaną 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*.

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)*.

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 audio po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak skonfigurować urządzenie audio, aby odtwarzało klip audio po wykryciu ruchu przez kamerę sieciową Axis.

Wymagania wstępne

- Urządzenie audio Axis i kamera sieciowa Axis znajdują się w tej samej sieci.
- Aplikacja do detekcji ruchu jest skonfigurowana i uruchomiona w kamerze.

1. Przygotowanie łącza do klipu audio:
   1.1. Przejdź do menu **Audio** > **Audio clips (Klipy audio)**.
   1.2. Wybierz kolejno ⋮ > **Create link (Utwórz łącze)** dla klipu audio.
   1.3. Ustaw głośność i liczbę powtórzeń klipu.
   1.4. Kliknij ikonę kopiowania, aby skopiować łącze.
2. Utwórz regułę akcji:
   2.1. Przejdź do menu **System** > **Events (Zdarzenia)** > **Recipients (Odbiorcy)**.
   2.2. Kliknij przycisk **+ Add recipient (Dodaj odbiorcę)**.
   2.3. Wpisz nazwę odbiorcy, na przykład „Głośnik".
   2.4. Wybierz **HTTP** z listy rozwijanej **Type (Typ)**.
   2.5. Wklej skonfigurowane łącze z urządzenia audio do pola **URL**.
   2.6. Wprowadź nazwę użytkownika i hasło urządzenia audio.
   2.7. Kliknij przycisk **Zapisz**.
   2.8. Przejdź do sekcji **Rules (Reguły)** i kliknij przycisk **+ Add a rule (Dodaj regułę)**.
   2.9. Wprowadź nazwę reguły akcji, na przykład „Odtwórz klip".
   2.10. Z listy **Condition (Warunek)** wybierz w polu **Applications (Aplikacje)** alternatywę dla wizyjnej detekcji ruchu.

   Uwaga

   Jeśli brak opcji wizyjnej detekcji ruchu, przejdź do obszaru **Apps (Aplikacje)**, kliknij **AXIS Video Motion Detection** i włącz detekcję ruchu.

   2.11. Z listy **Action (Akcja)** wybierz opcję **Send notification through HTTP (Wyślij powiadomienie przez HTTP)**.
   2.12. W polu **Recipient (Odbiorca)** wybierz odbiorcę.
   2.13. 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, którzy 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)**.

Wyświetlenie komunikatu na wyświetlaczu

Wyświetlenie komunikatu tekstowego na wyświetlaczu pojedynczego głośnika:

1. Otwórz interfejs WWW, wprowadzając adres IP głośnika w przeglądarce internetowej.
2. Wybierz kolejno opcje **System** > **Events (Zdarzenia)** > **Rules (Reguły)**.
3. Kliknij **+ Add a rule (Dodaj regułę)**.
4. Nadaj nazwę regule.
5. W obszarze **Condition (Warunek)** zaznacz opcję **Manual trigger (Wyzwalacz manualny)**.
6. W obszarze **Action (Akcja)** zaznacz opcję **Speaker display notification (Powiadomienie na wyświetlaczu głośnika)**.
7. W obszarze **Message (Komunikat)** wprowadź tekst, który ma zostać wyświetlony na głośniku.
8. Wypełnij pozostałe pola odpowiednio do potrzeb.
9. Kliknij przycisk **Zapisz**.
10. Upewnij się, że reguła jest włączona.
11. Wybierz opcję **Manual triggers (Wyzwalacze manualne)**.
12. Włącz **Trigger 1 (Wyzwalacz 1)**.
    Powiadomienie jest teraz wysyłane do głośnika.

Wyzwalanie diody sygnalizacyjnej LED za pomocą czujnika PIR

1. Otwórz interfejs WWW, wprowadzając adres IP głośnika w przeglądarce internetowej.
2. Wybierz kolejno opcje **System** > **Events (Zdarzenia)** > **Rules (Reguły)**.
3. Kliknij **+ Add a rule (Dodaj regułę)**.
4. Nadaj nazwę regule.
5. W obszarze **Condition (Warunek)** zaznacz opcję **PIR sensor (Czujnik PIR)**.
6. W obszarze **Action (Akcja)** wybierz opcję **Light and siren (Oświetlenie i syrena) > Run light profile while the rule is active (Uruchom profil oświetlenia, gdy reguła jest aktywna)**.

7. W obszarze **Profile (Profil)** wybierz jeden z profili diod sygnalizacyjnych LED (zobacz podpowiedź wyświetlaną po najechaniu kursorem na alternatywę).
   Aby utworzyć nowy profil, zobacz *Tworzenie profilu oświetlenia, on page 8*.
8. Kliknij przycisk **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

Voice over IP (VoIP)

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

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

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

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

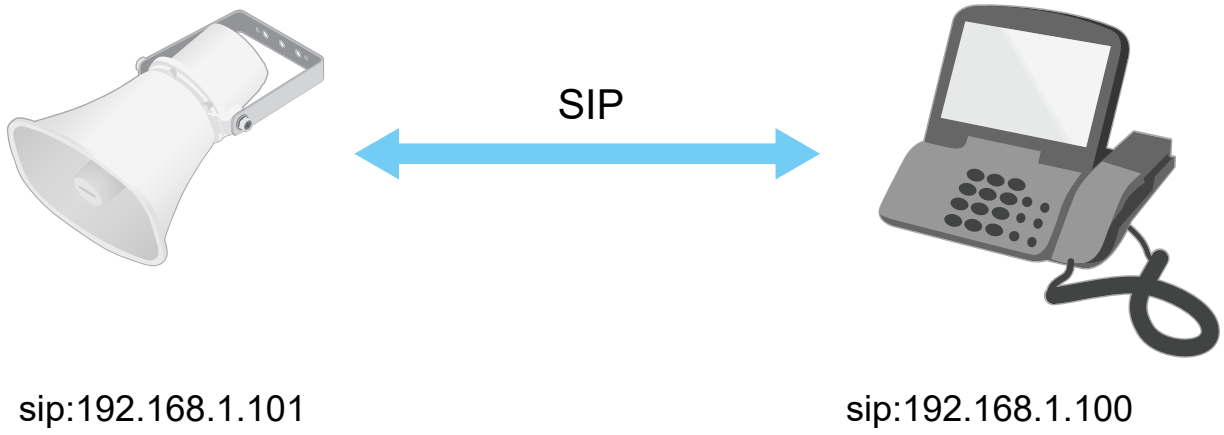
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

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

Peer-to-peer SIP (P2PSIP)

Podstawowa komunikacja SIP odbywa się bezpośrednio pomiędzy dwoma lub większą liczba agentów użytkowników SIP. Połączenie takie nazywane jest peer-to-peer SIP (P2PSIP). Jest ono wykonywane w sieci lokalnej i wymaga jedynie adresów SIP agentów użytkowników. 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.

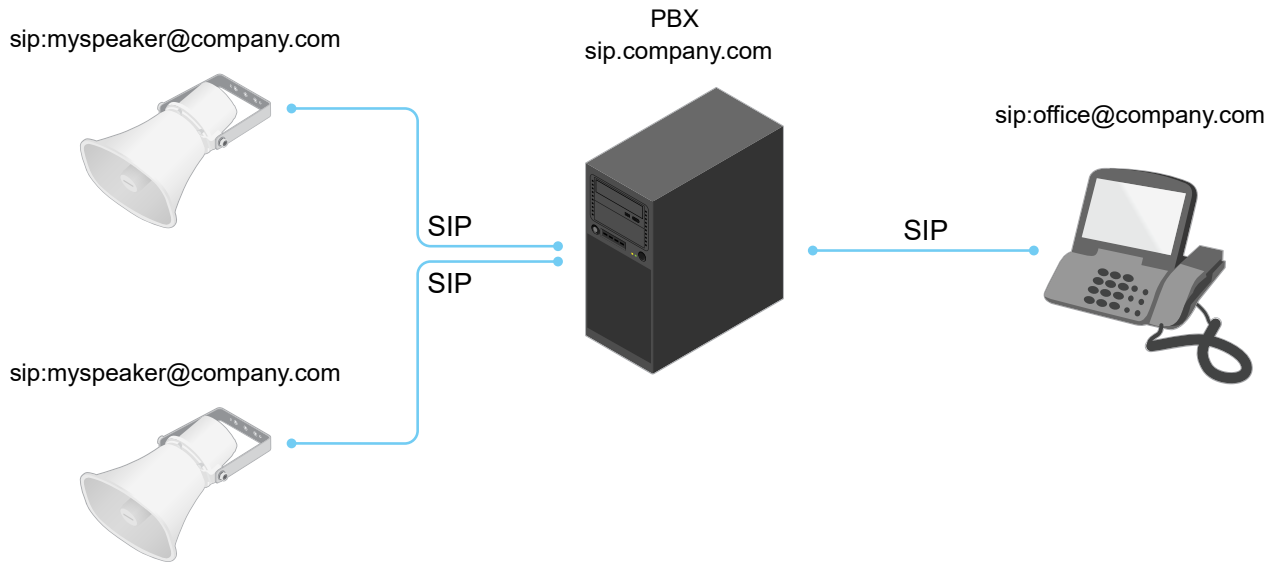
Private Branch Exchange (PBX) – centrala abonencka

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 głosowym i przekierowania.

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

Każdy agent użytkownika SIP jest rejestrowany w PBX; mogą łączyć się z innymi poprzez wybranie właściwego numeru wewnętrznego. Adres SIP to zazwyczaj `sip:<user>@<domain>` lub `sip:<user>@<registrar-ip>`. Adres SIP jest niezależny od adresu SIP, 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 urządzeniem 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*.

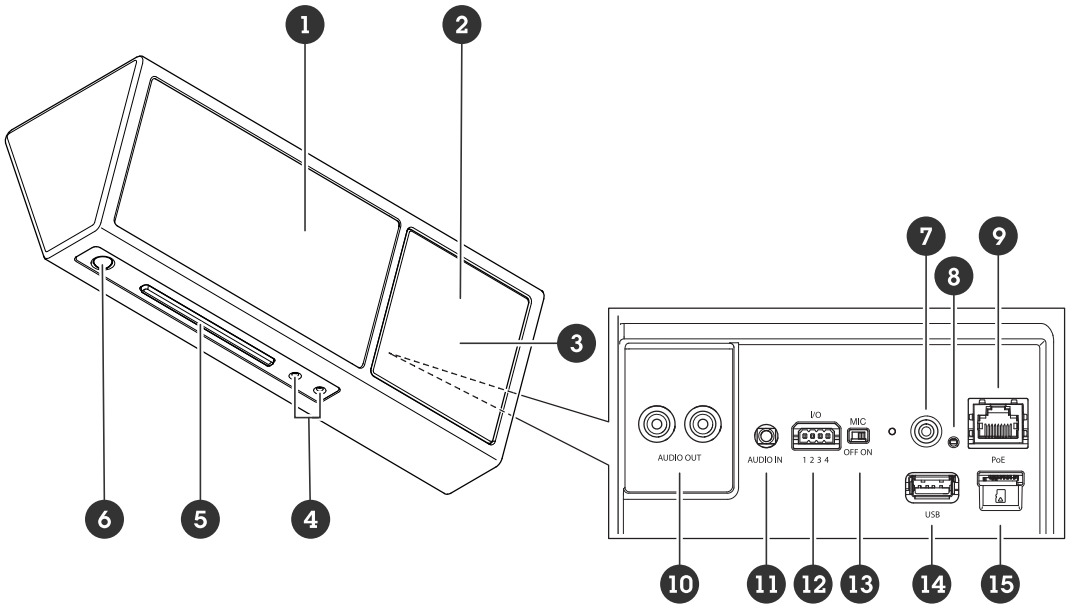
AXIS Audio Analytics

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*.

Specyfikacje

Przegląd produktów



1 *Wyświetlacz*
2 *Wskaźnik LED audio*
3 *Głośnik*
4 *Mikrofony*
5 *Dioda sygnalizacyjna LED*
6 *Czujnik PIR*
7 *Przycisk kontrolny*
8 *Dioda stanu*
9 *Złącze sieciowe*
10 *Wyjście audio (złącze RCA)*
11 *Wejście audio*
12 *Złącze I/O*
13 *Przycisk wyłączania mikrofonu*
14 *Złącze USB (wyłączone, zarezerwowane do wykorzystania w przyszłości)*
15 *Gniazdo karty SD*

Wskaźniki LED

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.

Czerwony	Miga powoli w przypadku niepowodzenia uaktualnienia.
Czerwony/zielony	Miga szybko w przypadku wybrania opcji **Locate device (Zlokalizuj urządzenie)**.

Gniazdo karty SD

POWIADOMIENIE

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

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 23*.

Przycisk wyłączania mikrofonu

Lokalizacja przycisku wyłączania mikrofonu: *Przegląd produktów, on page 19*.

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

Złącza

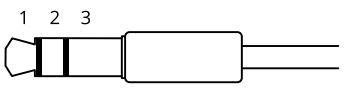
Złącze sieciowe

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

POWIADOMIENIE

Ten produkt musi zostać podłączony przy pomocy kabla ekranowanego (STP). Wszystkie kable łączące produkt 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*.

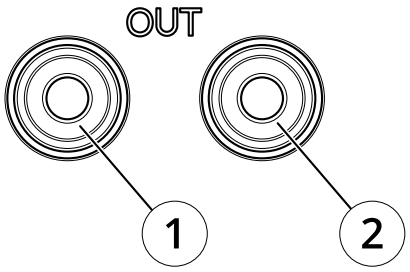
Złącze audio



Wejście audio

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

Wyjście audio (złącze RCA)



	1 białe złącze	2 czerwone złącze
Wyjście audio	Wyjście audio (lewa)	Wyjście audio (prawa)

Złącze I/O

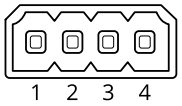
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

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

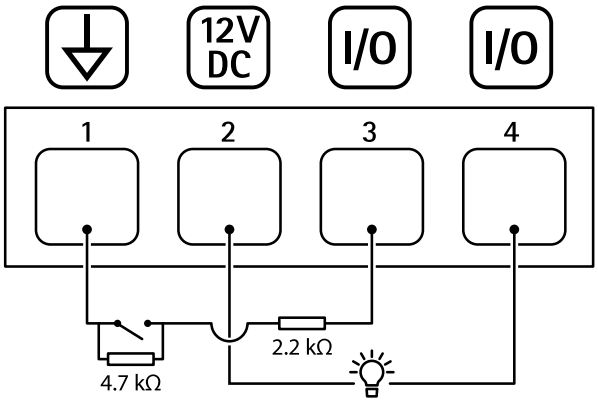
4-pinowy blok złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	⚠ Może być wykorzystywane do zasilania dodatkowego sprzętu.	12 V DC Maks. obciążenie = 50 mA

		Uwaga: ten styk może być używany tylko jako wyjście zasilania.	
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. 50 mA*
3 *I/O skonfigurowane jako wejście nadzorowane*
4 *We/Wy skonfigurowane jako wyjście*

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 19*.
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 wydaniami wersji zawierającymi głównie poprawki i aktualizacje dotyczące bezpieczeństwa.

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

- 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 23*.

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 .

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 częstością próbkowania 8 do 48 kHz.
- format plików mp3, mono lub stereo z przepływnością 64 kb/s do 320 kb/s, z częstością próbkowania 8 do 48 kHz.

Klipy multimedialne są odtwarzane z różna 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 żadne przeszkody.

Problemy ze światłem	
Urządzenie nie jest tak jasne, jak oczekiwano	Sprawdź, czy używany jest zasilacz PoE klasy 6. 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.

Uwagi dotyczące zasilania

Możliwości mogą być ograniczone zależnie od stosowanej klasy PoE.

PoE klasa 6	Brak ograniczeń.
PoE klasa 4	Ograniczony poziom ciśnienia akustycznego, jasność wyświetlacza i jasność wskaźnika sygnalizacyjnego LED.
PoE klasa 3	Możliwe jest skonfigurowanie urządzenia w taki sposób, aby przygotować je do instalacji, niemiej musi ono mieć klasę PoE 4 lub 6, aby mogło być stosowane w instalacji końcowej.

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.

T10224719_pl

2026-07 (M7.2)

© 2025 – 2026 Axis Communications AB