

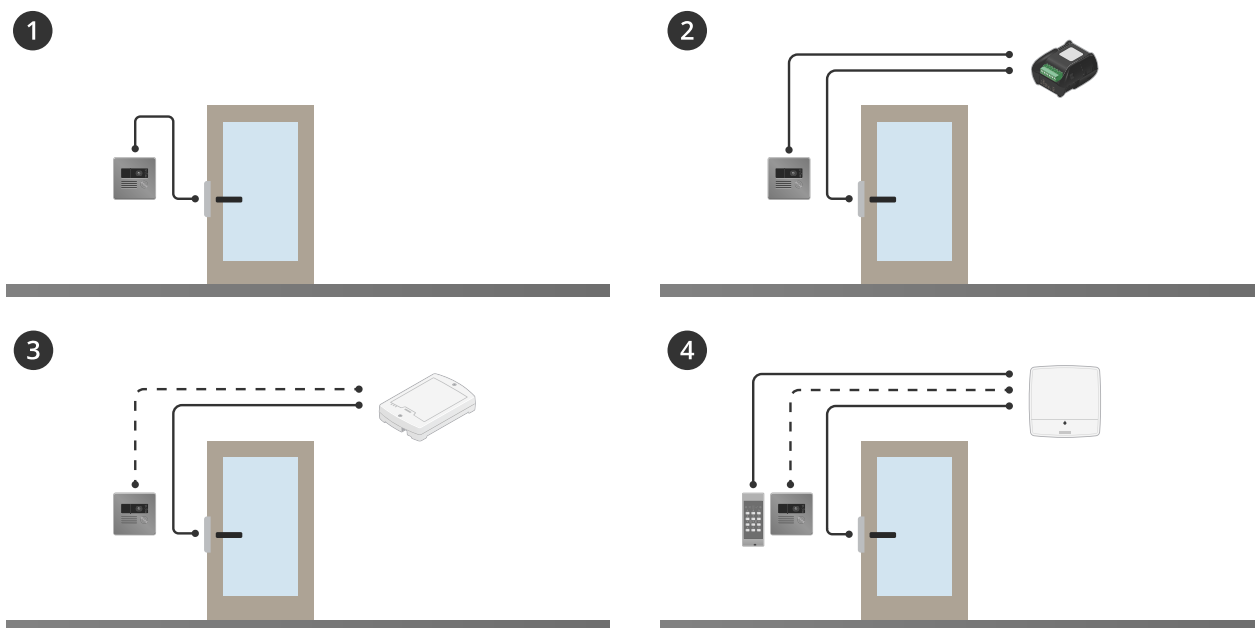
AXIS I8016-LVE Network Video Intercom

Spis treści

Przegląd konfiguracji.....	4
Przegląd produktów	5
.....	5
Od czego zacząć.....	6
Wyszukiwanie urządzenia w sieci.....	6
Obsługiwane przeglądarki.....	6
Otwórz interfejs WWW urządzenia.....	6
Upewnianie się co do braku zmian w oprogramowaniu urządzenia.....	6
Utwórz konto administratora	6
Bezpieczne hasła	7
Konfiguracja urządzenia	8
Kalibracja i przeprowadzanie zdalnego testu głośnika	8
Konfiguracja bezpośredniego połączenia SIP (P2P).....	8
Konfiguracja SIP przez serwer (PBX).....	9
Tworzenie kontaktu	10
Konfiguracja przycisku połączenia.....	10
Korzystanie z DTMF do otwierania drzwi.....	10
Korzystanie z oświetlenia IR w warunkach słabego oświetlenia (tryb nocny).....	11
Interfejs WWW.....	12
Więcej informacji.....	13
Voice over IP (VoIP)	13
Protokół inicjacji sieci (Session Initiation Protocol, SIP).....	13
Peer-to-peer SIP (P2PSIP).....	13
Private Branch Exchange (PBX) – centrala abonencka.....	14
Konfiguracja reguł dotyczących zdarzeń	15
NAT Transversal.....	15
Analizy i aplikacje	15
AXIS Client for Unified Communication Systems.....	15
Rozwiązywanie problemów –	16
Przywróć domyślne ustawienia fabryczne	16
Sprawdzanie bieżącej wersji systemu AXIS OS	16
Aktualizacja systemu AXIS OS:.....	16
Problemy techniczne i możliwe rozwiązania.....	17
Kwestie wydajności	18
Kontakt z pomocą techniczną.....	19
Sprzęt podłączeniowy.....	20
Przełącznik zasilany przez zasilacz PoE (12 V).....	20
Przełącznik zasilany przez osobny zasilacz	20
Przełącznik bezpotencjałowy	21
Bezpieczna blokada 12 V zasilana przez zasilacz PoE z interkomu.....	21
Bezpieczna blokada 12 V zasilana przez zasilacz zewnętrzny.....	22
Specyfikacje	23
Wskaźniki i elementy sterowania na panelu przednim	23
Ikony wskaźników.....	23
Wskaźniki LED.....	23
Gniazdo karty SD.....	23
Przyciski.....	23
Przycisk kontrolny.....	23
Złącza.....	23
Złącze sieciowe	23
Złącze audio.....	24
Złącze I/O	24
Informacje dotyczące bezpieczeństwa.....	25

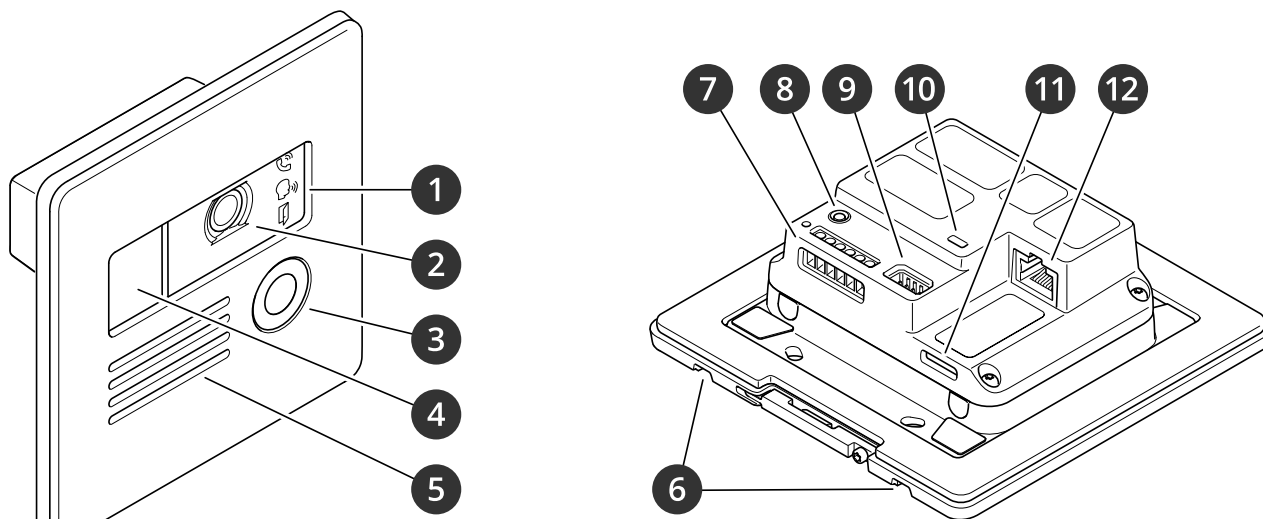
Poziomy zagrożenia	25
Inne poziomy komunikatów	25
Cyberbezpieczeństwo	26
Postępowanie z lukami w zabezpieczeniach	26
Powiadomienia dotyczące zabezpieczeń	26
Bezpieczny cykl eksploatacji produktu	26

Przegląd konfiguracji



- 1 Interkom
- 2 Interkom połączony z AXIS A9801
- 3 Interkom połączony z AXIS A9161
- 4 Interkom połączony z czytnikiem i systemem kontroli dostępu, na przykład AXIS A1001 lub AXIS A1601

Przegląd produktów



- 1 Ikony wskaźników, on page 23
- 2 Kamera
- 3 Przycisk połączenia
- 4 Oświetlenie w podczerwieni
- 5 Głośnik
- 6 Mikrofon
- 7 Złącze I/O, on page 24
- 8 Przycisk kontrolny, on page 23
- 9 Złącze audio, on page 24
- 10 Dioda stanu
- 11 Gniazdo karty SD, on page 23 (microSD/microSDHC/microSDXC)
- 12 Złącze sieciowe, on page 23

Od czego zacząć

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

	Chrome™	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*.

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

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 16*.

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.

Konfiguracja urządzenia

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

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 5.

Konfiguracja bezpośredniego połączenia SIP (P2P)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP)*, on page 13.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 13

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest łączność bezpośrednia czyli peer-to-peer (P2P). Konfiguracji P2P należy używać wtedy, gdy komunikacja odbywa się pomiędzy niewielką liczbą agentów użytkownika w tej samej sieci IP i nie ma potrzeby zapewniania dodatkowych funkcji serwera PBX. Informacje na temat konfiguracji: *Peer-to-peer SIP (P2PSIP)*, on page 13.

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

POWIADOMIENIE

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

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

7. Wprowadź numer portu **Port SIP** i numer portu **Port TLS**.

Uwaga

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

Uwaga

Użyj opcji NAT traversal, gdy urządzenie jest podłączone do sieci za routerem NAT lub znajduje się za zaporą. Więcej informacji znajduje się w rozdziale *NAT Traversal*, on page 15.

10. Kliknij przycisk **Zapisz**.

Konfiguracja SIP przez serwer (PBX)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Więcej informacji znajduje się w rozdziale *Voice over IP (VoIP)*, on page 13.

W tym urządzeniu komunikację VoIP umożliwia protokół SIP. Więcej informacji dotyczących protokołu SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 13

Istnieją dwa rodzaje konfiguracji protokołu SIP. Jednym z nich jest serwer PBX. Konfiguracji PBX należy używać wtedy, gdy komunikacja odbywa się pomiędzy nieograniczoną liczbą agentów użytkownika w tej samej sieci IP i poza nią. W zależności od dostawcy usługi PBX można dodać dodatkowe funkcje. Więcej informacji znajduje się w rozdziale *Private Branch Exchange (PBX) – centrala abonencka*, on page 14.

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

Tworzenie kontaktu

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

Aby utworzyć nowy kontakt:

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

Uwaga

Więcej informacji dotyczących adresów SIP: *Protokół inicjacji sieci (Session Initiation Protocol, SIP)*, on page 13.

5. Wybierz konto SIP do wykonania połączenia.

Uwaga

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

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

Uwaga

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

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

Konfiguracja przycisku połączenia

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

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

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

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

Korzystanie z DTMF do otwierania drzwi

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

W tym przykładzie wyjaśniono, jak:

- zdefiniować sygnał DTMF w interkomie;
- skonfigurować interkom, aby:
 - żądać odblokowania drzwi, lub
 - otwierać drzwi przy użyciu przekaznika wewnętrznego.

Wszystkie ustawienia należy wprowadzić na stronie internetowej interkomu.

Zanim rozpoczniesz

- Zezwól na połączenia SIP wychodzące z urządzenia i załóż konto SIP. Patrz *Konfiguracja bezpośredniego połączenia SIP (P2P), on page 8* i *Konfiguracja SIP przez serwer (PBX), on page 9*.

Definiowanie sygnału DTMF w interkomie

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

Skonfiguruj interkom do otwierania drzwi za pomocą przełącznika wewnętrznego

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

Korzystanie z oświetlenia IR w warunkach słabego oświetlenia (tryb nocny)

Kamera w ciągu dnia rejestruje kolorowe obrazy, korzystając ze światła dziennego. Niemniej, wraz ze zmniejszaniem się ilości światła widzialnego obrazy kolorowe stają się mniej jasne i wyraźne. Jeżeli w takiej sytuacji zostanie aktywowany tryb nocny, kamera będzie wykorzystywać zarówno światło widzialne, jak i podczerwień, aby uzyskać jasne i szczegółowe obrazy w czerni i bieli. Istnieje możliwość ustawienia automatycznego przełączania na tryb nocny.

1. Przejdź do **Video > Image > Day-night mode** (Wideo > Obraz > Tryb dzień/noc) i upewnij się, że w opcji **IR cut filter** (Filtr odcinający promieniowanie podczerwone) ustawiono wartość **Auto** (Automatycznie).

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*.

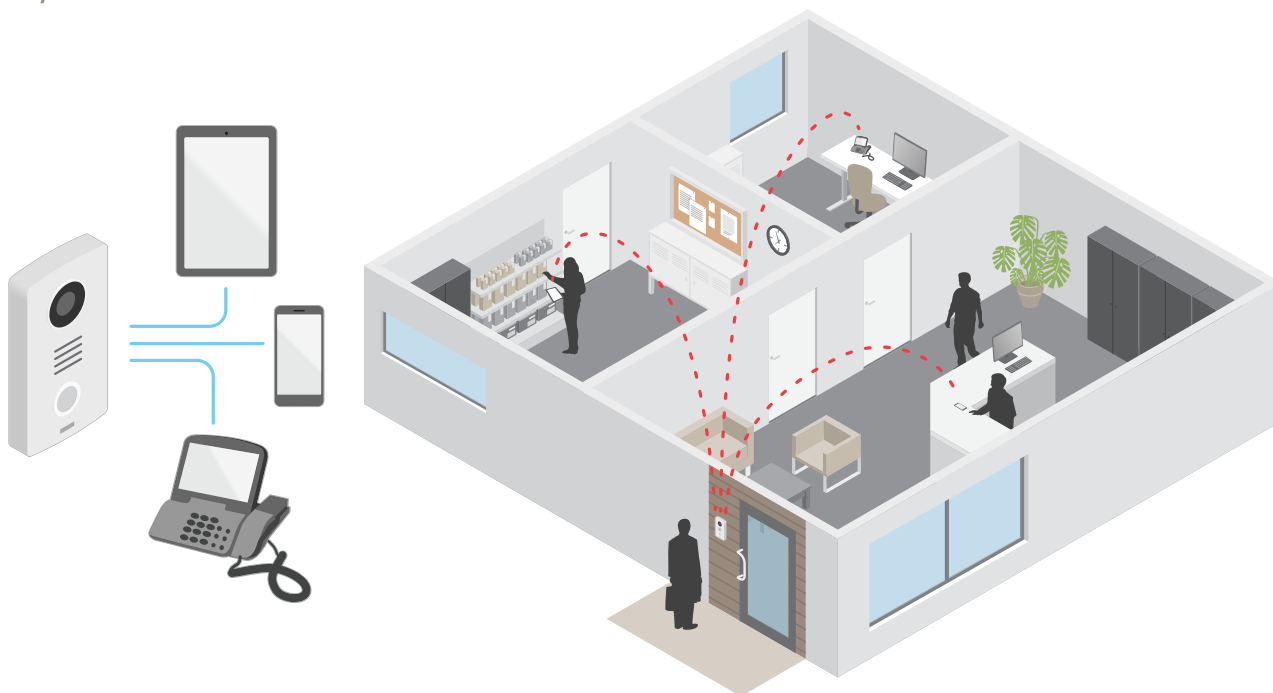
Więcej informacji

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 można je było przesyłać jako pakiety danych przez lokalne sieci IP lub Internet.

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

Przykład:



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

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

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

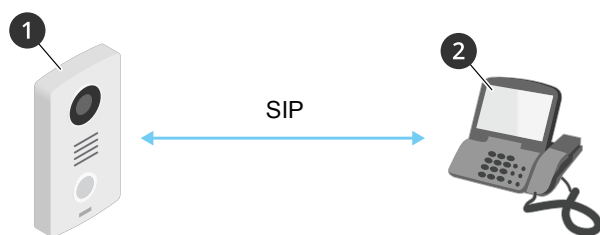
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

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

Peer-to-peer SIP (P2PSIP)

Podstawowa komunikacja SIP odbywa się bezpośrednio pomiędzy dwoma lub większą 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:



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

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

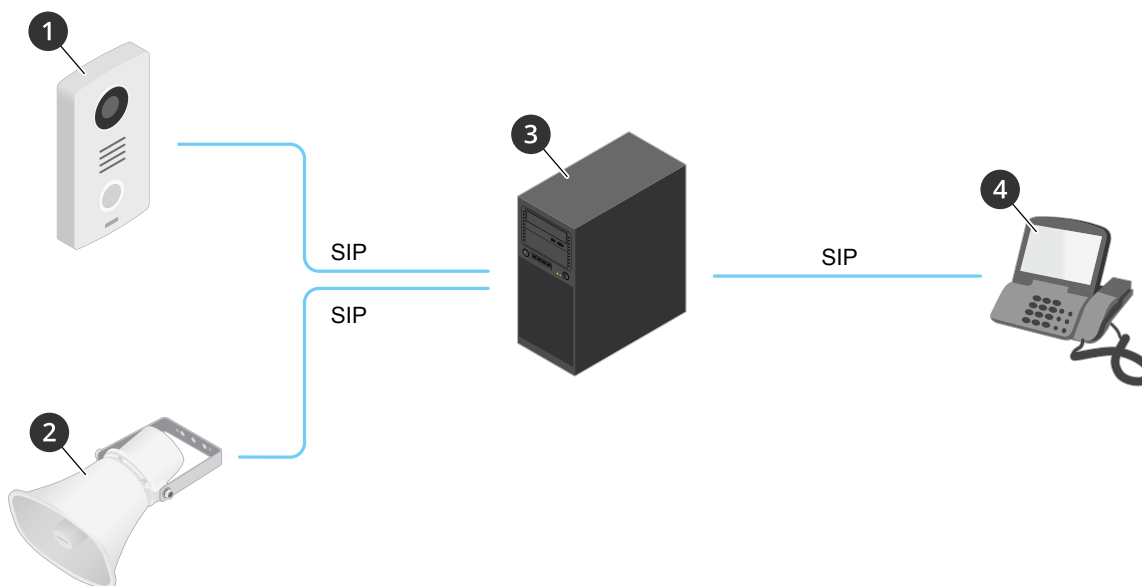
Private Branch Exchange (PBX) – centrala abonencka

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



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

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

Konfiguracja reguł dotyczących zdarzeń

Można utworzyć reguły sprawiające, że urządzenie będzie wykonywać konkretne akcje po wystąpieniu określonych zdarzeń. Reguła składa się z warunków i akcji. Warunki mogą służyć do wyzwalania akcji. Urządzenie może na przykład rozpocząć zapis lub wysłać wiadomość e-mail po wykryciu ruchu albo wyświetlić nałożony tekst podczas rejestracji.

Aby dowiedzieć się więcej, zob. *Get started with rules for events (Reguły dotyczące zdarzeń)*.

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 Client for Unified Communication Systems

Dzięki tej platformie możesz wykonywać połączenia pomiędzy urządzeniami Axis z protokołem SIP a powiązanymi kontami Microsoft® Teams. Więcej informacji znajduje się w *instrukcji obsługi platformy AXIS Client for Unified Communication Systems*.

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 5*.
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
 - Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej: Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
 - Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej: 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej axis.com/support.

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

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 *Cykł 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 16.*

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 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.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wydajność. Niektóre czynniki wpływają na przepustowość (przepływność), inne na poklatkowość, a jeszcze inne na oba te parametry.

Najważniejsze czynniki, które należy uwzględnić:

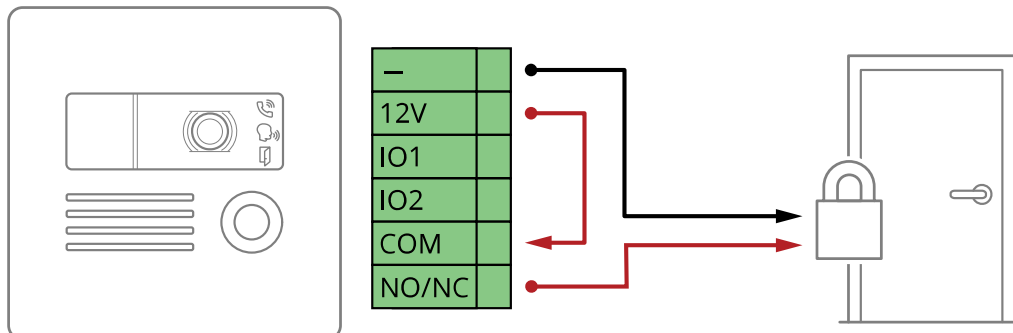
- Wysoka rozdzielczość obrazu lub niższe poziomy kompresji zapewniają obrazy zawierające więcej danych, co z kolei wpływa na przepustowość.
- Dostęp ze strony dużej liczby klientów MJPEG lub H.264/H.265/AV1 unicast wpływa na przepustowość.
- Jednoczesne oglądanie różnych strumieni (rozdzielczość, kompresja) za pomocą różnych klientów wpływa zarówno na liczbę klatek na sekundę, jak i na przepustowość. W miarę możliwości używaj identycznych strumieni, aby utrzymać wysoką liczbę klatek na sekundę. Aby upewnić się, że strumienie są identyczne, możesz użyć profili strumieni.
- Jednoczesny dostęp do strumieni wideo z różnymi kodekami wpływa zarówno na poklatkowość, jak i na przepustowość. Aby uzyskać optymalną wydajność, należy używać strumieni z tym samym kodekiem.
- Intensywne korzystanie z ustawień zdarzeń wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.
- Korzystanie z protokołu HTTPS może zmniejszać liczbę klatek na sekundę, szczególnie w przypadku przesyłania strumieniowego obrazów wideo w formacie MJPEG.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Wyświetlanie obrazu z użyciem komputerów klienckich o niewystarczających parametrach obniża subiektywnie obserwowaną wydajność i wpływa na liczbę klatek na sekundę.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

Kontakt z pomocą techniczną

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

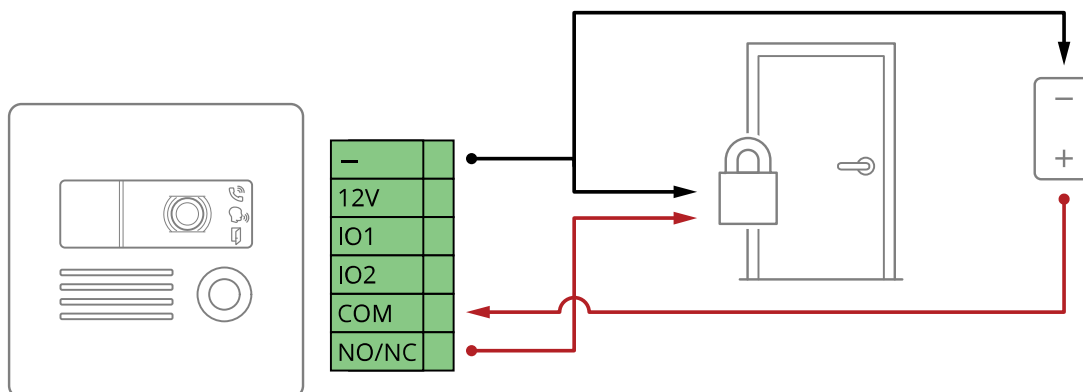
Sprzęt podłączeniowy

Przełącznik zasilany przez zasilacz PoE (12 V)



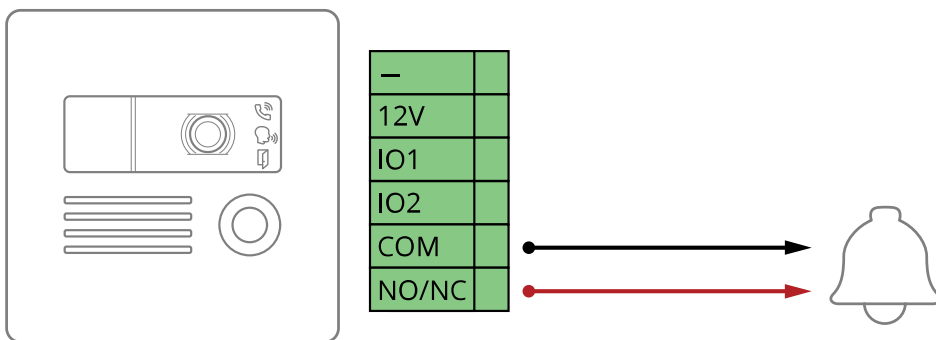
1. Aby sprawdzić stan przełącznika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przełącznika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
 -  do zamka zabezpieczonego podczas awarii zasilania
 -  do zamka zabezpieczonego

Przełącznik zasilany przez osobny zasilacz



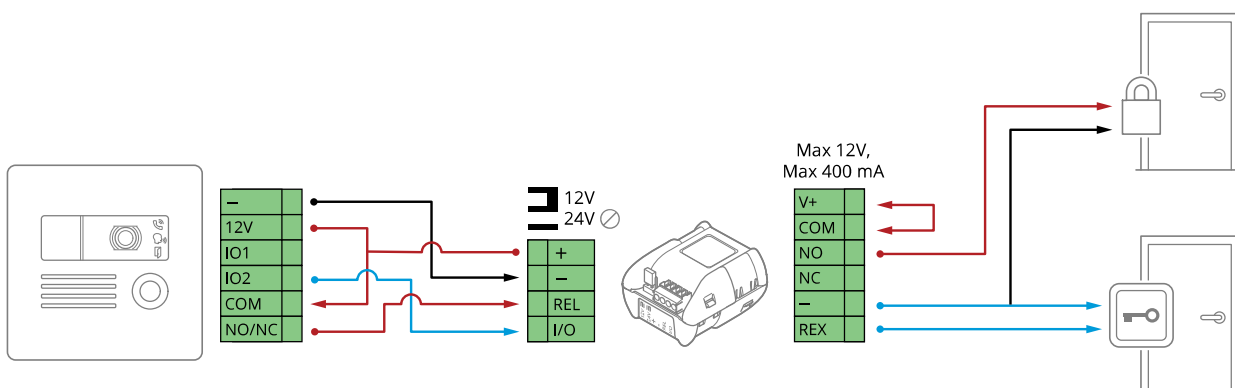
1. Aby sprawdzić stan przełącznika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przełącznika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
 -  do zamka zabezpieczonego podczas awarii zasilania
 -  do zamka zabezpieczonego

Przełącznik bezpotencjałowy



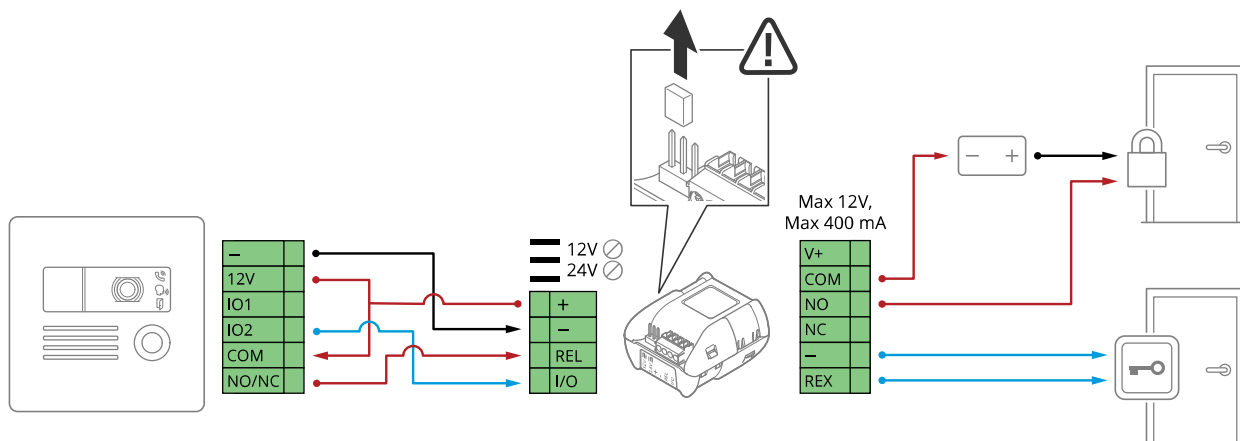
1. Aby sprawdzić stan przełącznika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przełącznika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
 -  do zamka zabezpieczonego podczas awarii zasilania
 -  do zamka zabezpieczonego

Bezpieczna blokada 12 V zasilana przez zasilacz PoE z interkomu



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

Bezpieczna blokada 12 V zasilana przez zasilacz zewnętrzny



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

Specyfikacje

Wskaźniki i elementy sterowania na panelu przednim

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

Ikony wskaźników

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

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przy normalnym działaniu.

Gniazdo karty SD

POWIADOMIENIE

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

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

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



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

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 16*.

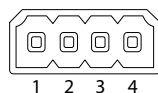
Złącza

Złącze sieciowe

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

Złącze audio

4-pinowy blok złączy wejść i wyjść audio.



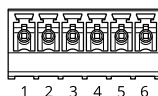
Funkcje	Styk	Uwagi
Wejście liniowe	1	Wejście liniowe (mono)
GND	2	Uziemienie audio
Wyjście liniowe	3	Wyjście liniowe (mono)
GND	4	Uziemienie audio

Złącze I/O

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

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

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



Funkcje	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
12 V DC	2		Maks. prąd = 400 mA
Konfigurowalne (wejście lub wyjście)	3–4	Wejście cyfrowe – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC
		Wyjście cyfrowe – podłączone do styku 1 po aktywacji, rozłączone po dezaktywacji. 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
Wspólny	5		Maks. prąd/napięcie = 700mA przy 30 V ze źródła zewnętrznego
Normalnie otwarte/ normalnie zamknięte	6	Do podłączania urządzeń przekaźnikowych. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd/napięcie = 700mA przy 30 V ze źródła zewnętrznego

Informacje dotyczące bezpieczeństwa

Poziomy zagrożenia

▲ NIEBEZPIECZEŃSTWO

Wskazuje zagrożenie, które spowoduje zgon lub ciężkie obrażenia.

▲ OSTRZEŻENIE

Wskazuje zagrożenie, które może spowodować zgon lub ciężkie obrażenia.

▲ UWAGA

Wskazuje zagrożenie, które może spowodować niewielkie lub umiarkowane obrażenia.

POWIADOMIENIE

Wskazuje zagrożenie, które może spowodować uszkodzenie mienia.

Inne poziomy komunikatów

Ważne

Wskazuje istotne informacje niezbędne do poprawnego działania produktu.

Uwaga

Wskazuje przydatne informacje, które ułatwiają wykorzystanie możliwości produktu.

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.

T10154915_pl

2026-07 (M24.2)

© 2020 – 2026 Axis Communications AB