AXIS I7020 Network Intercom

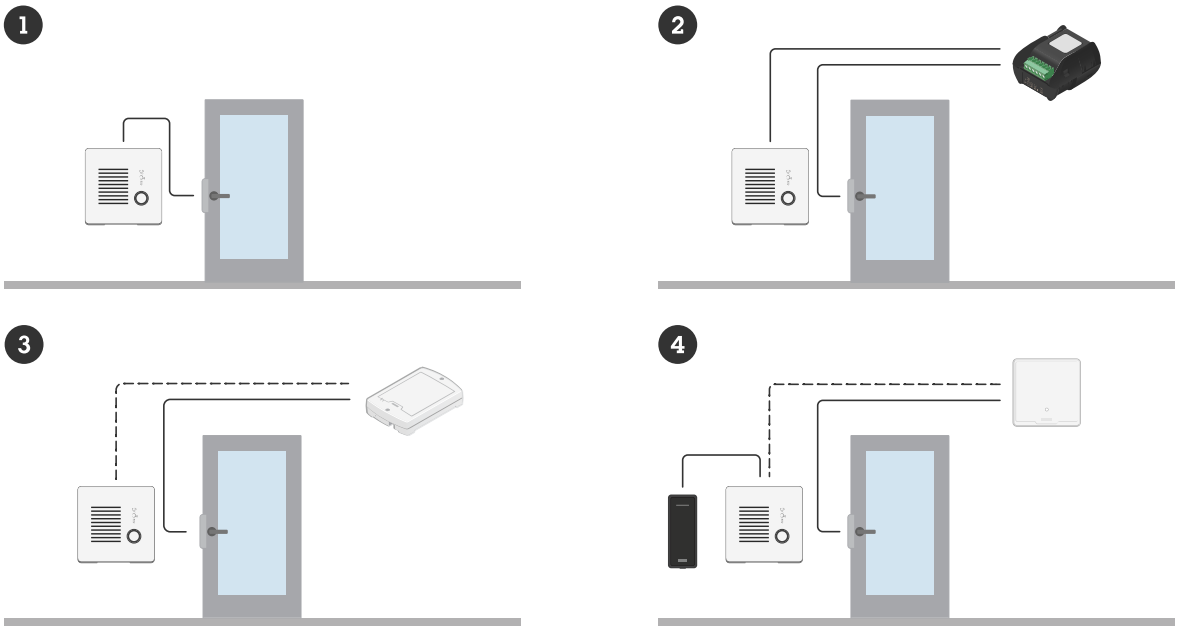
Podręcznik użytkownika

Spis treści

Przegląd konfiguracji....4
Od czego zacząć....5
Wyszukiwanie urządzenia w sieci....5
Obsługiwane przeglądarki....5
Otwieranie interfejsu WWW urządzenia....5
Utwórz konto administratora....5
Bezpieczne hasła....6
Upewnianie się co do braku zmian w oprogramowaniu urządzenia....6
Konfiguracja urządzenia....7
Kalibracja i przeprowadzanie zdalnego testu głośnika....7
Konfiguracja bezpośredniego połączenia SIP (P2P)....7
Konfiguracja SIP przez serwer (PBX)....8
Dołączanie strumienia wideo z pobliskiej kamery do połączenia SIP....9
Tworzenie kontaktu....9
Konfiguracja przycisku połączenia....9
Korzystanie z DTMF do otwierania drzwi....10
Użyj listy wejść, aby zezwolić osobom mającym poświadczenia na otwarcie drzwi....10
Konfiguracja reguł dotyczących zdarzeń....11
Wyzwalanie akcji....11
Interfejs WWW....12
Dowiedz się więcej....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
NAT Transversal....15
Analizy i aplikacje....15
AXIS Client for Unified Communication Systems....15
Specyfikacje....16
Przegląd produktów....16
Wskaźniki i elementy sterowania na panelu przednim....16
Ikony wskaźników....16
Wskaźniki LED....16
Gniazdo karty SD....17
Przyciski....17
Przycisk kontrolny....17
Złącza....17
Złącze sieciowe....17
Złącze audio....17
Złącze WE/WY, czytnika i przekaźnika....17
Sprzęt podłączeniowy....20
Czytnik Axis....20
Przekaźnik zasilany przez zasilacz PoE (12 V)....20
Przekaźnik zasilany przez osobny zasilacz....20
Przekaźnik bezpotencjałowy....21
Bezpieczna blokada 12 V zasilana przez zasilacz PoE z interkomu....21
Bezpieczna blokada 12 V zasilana przez zasilacz zewnętrzny....22
Zalecenia dotyczące czyszczenia....23
Rozwiązywanie problemów....24
Przywracanie domyślnych ustawień fabrycznych....24
Opcje systemu AXIS OS....24
Sprawdzanie bieżącej wersji systemu AXIS OS....24
Aktualizacja systemu AXIS OS:....25

Problemy techniczne i możliwe rozwiązania....25
Kwestie wydajności....27
Kontakt z pomocą techniczną....28
Cyberbezpieczeństwo....29
Zarządzanie podatnościami....29
Powiadomienia dotyczące zabezpieczeń....29
Bezpieczny cykl eksploatacji produktu....29
Informacje dotyczące bezpieczeństwa....30
Poziomy zagrożenia....30
Inne poziomy komunikatów....30

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*

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	*	*	*	*

✓: Zalecenie

*: Obsługiwane z ograniczeniami

Otwieranie interfejsu WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis.
   Jeżeli nie znasz adresu IP, odnajdź urządzenie w sieci przy pomocy aplikacji AXIS IP Utility lub AXIS Device Manager.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Zob. *Utwórz konto administratora, on page 5*.

Opisy wszystkich funkcji i ustawień znajdujących się w interfejsie internetowym urządzeń z systemem AXIS OS znajdują się w sekcji *Pomoc dotycząca interfejsu internetowego systemu AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę konta.
2. Wprowadź hasło. Zob. *Bezpieczne hasła, on page 6*.
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. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 24*.

Bezpieczne hasła

Ważne

Aby ustawić hasło lub inne poufne konfiguracje przez sieć IP, należy korzystać z protokołu HTTPS (który jest domyślnie włączony). Protokół HTTPS umożliwia bezpieczne i szyfrowane połączenia sieciowe, 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. Przywracanie domyślnych ustawień fabrycznych. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 24*.
   Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

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

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.

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. Zob. *Przegląd produktów, on page 16*, aby zidentyfikować przycisk sterowania.

Konfiguracja bezpośredniego połączenia SIP (P2P)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Aby uzyskać dodatkowe informacje, zob. *Voice over IP (VoIP), on page 13*.

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

Istnieją dwa rodzaje konfiguracji SIP. bezpośrednia lub 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 **Allow incoming calls** (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 port początkowy to 4000. Niektóre zapory mogą blokować ruch RTP na portach o określonych numerach. 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. Aby uzyskać dodatkowe informacje, zob. *NAT Transversal, on page 15*.

10. Kliknij przycisk **Save (Zapisz)**.

Konfiguracja SIP przez serwer (PBX)

VoIP (Voice over IP) to grupa technologii, która umożliwia komunikację głosową i multimedialną w sieciach IP. Aby uzyskać dodatkowe informacje, zob. *Voice over IP (VoIP), on page 13*.

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

Istnieją dwa rodzaje konfiguracji SIP. Jedną z nich jest konfiguracja z serwerem 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. Aby uzyskać dodatkowe informacje, zob. *Private Branch Exchange (PBX) – centrala abonencka, on page 14*.

1. Od dostawcy PBX należy uzyskać następujące informacje:
   - ID użytkownika
   - Domena
   - Password (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 **Save (Zapisz)**.
8. Skonfiguruj ustawienia SIP w taki sam sposób jak dla trybu peer-to-peer — zobacz *Konfiguracja bezpośredniego połączenia SIP (P2P), on page 7*. Użyj portu początkowego RTP od dostawcy PBX.

Dołączanie strumienia wideo z pobliskiej kamery do połączenia SIP

Jeśli w pobliżu interkomu jest zamontowana kamera Axis, można dołączać pochodzący z niej strumień wideo do połączeń SIP i VMS z interkomu.

Wymagania

Kamera Axis z obsługą formatu H.264 i rozdzielczością 1280x720, 800x800 lub 640x480.

Aby podłączyć interkom do kamery:

1. Przejdź do menu **System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie)**.
2. W obszarze **Camera pairing (Parowanie kamery)** wprowadź adres, nazwę użytkownika i hasło kamery Axis.
3. Kliknij przycisk **Połącz**.

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 **Save (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 przekaźnika wewnętrznego.

Wszystkie ustawienia należy wprowadzić na stronie internetowej interkomu.

Zanim rozpoczniesz
- Zezwól na połączenia SIP wychodzące z urządzenia i załóż konto SIP. Zob. *Konfiguracja bezpośredniego połączenia SIP (P2P), on page 7* i *Konfiguracja SIP przez serwer (PBX), on page 8*.

Definiowanie sygnału DTMF w interkomie Axis
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 **Save (Zapisz)**.

Konfigurowanie interkomu do odblokowywania drzwi za pomocą przekaźnika 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 (Przekaźnik 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 **Save (Zapisz)**.

Użyj listy wejść, aby zezwolić osobom mającym poświadczenia na otwarcie drzwi.

Za pomocą listy wejść można umożliwić posiadaczom poświadczeń korzystanie z ich poświadczeń do wyzwalania akcji, takich jak otwieranie drzwi. W tym przykładzie wyjaśniamy, jak dodać posiadacza poświadczeń, który może użyć swojej karty do otwarcia drzwi 10 razy.

Wymagania wstępne
- W menu **Reader > Chip types (Czytnik > Typy chipów)** musi być aktywny odpowiedni typ chipu.

Włącz funkcję listy wejść i dodaj posiadacza poświadczeń:
1. Otwórz menu **Reader > Entry list (Czytnik > Lista wejść)**.
2. Włącz opcję **Use Entry list (Użyj listy wejść)**.
3. Kliknij pozycję **+ Add credential holder (+ Dodaj posiadacza poświadczeń)**.
4. Wprowadź imię i nazwisko posiadacza poświadczeń. Imię musi być unikatowe.
5. Wybierz pozycję **Card (Karta)**.
6. Przesuń kartą posiadacza w urządzeniu i kliknij **Get latest (Pobierz najnowsze)**.
7. Nie zmieniaj warunku **Access granted (Przyznano dostęp)**.

8. W obszarze **Valid to (Ważne do)** wybierz **Number of times (Ile razy)**.
9. W polu **Number of times (Ile razy)** wprowadź 10.
10. Kliknij przycisk **Save (Zapisz)**.

Utwórz regułę:

1. Przejdź do **System > Events (System > Zdarzenia)**.
2. W menu **Rules (Reguły)** kliknij **+ Add a rule (+ Dodaj regułę)**.
3. W polu **Name (Nazwa)** wprowadź Otwórz drzwi.
4. Na liście warunków wybierz **Entry list > Access granted (Lista wejść > Przyznano dostęp)**.
5. Z listy akcji wybierz opcję **I/O > Toggle I/O once Toggle I/O once (We/Wy > Przełącz raz We/Wy)**.
6. Z listy portów wybierz opcję **Door (Drzwi)**.
7. W menu **State (Status)** wybierz **Active (Aktywne)**.
8. Ustaw czas trwania jako 00:00:07.
9. Kliknij przycisk **Save (Zapisz)**.

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)*.

Wyzwalanie akcji

1. Przejdź do **System** > **Events** (System > Zdarzenia) i kliknij **+ Add a rule** (Dodaj regułę). Reguła określa, kiedy urządzenie wykona określone działania. Reguły można ustawić jako zaplanowane, cykliczne lub wyzwalane ręcznie.
2. Wprowadź **Name (Nazwę)**.
3. Wybierz **Condition (Warunek)**, który ma zostać spełniony w celu wyzwolenia akcji. Jeżeli w regule akcji zostanie określony więcej niż jeden warunek, wszystkie muszą zostać spełnione, aby wyzwolić akcję.
4. Wybierz **Action (Akcję)**, która ma zostać wykonana po spełnieniu warunków.

Interfejs WWW

Aby zapoznać się ze wszystkimi funkcjami i ustawieniami znajdującymi się w interfejsie internetowym urządzeń z systemem AXIS OS, przejdź do sekcji *Pomoc dotycząca interfejsu internetowego systemu AXIS OS*.

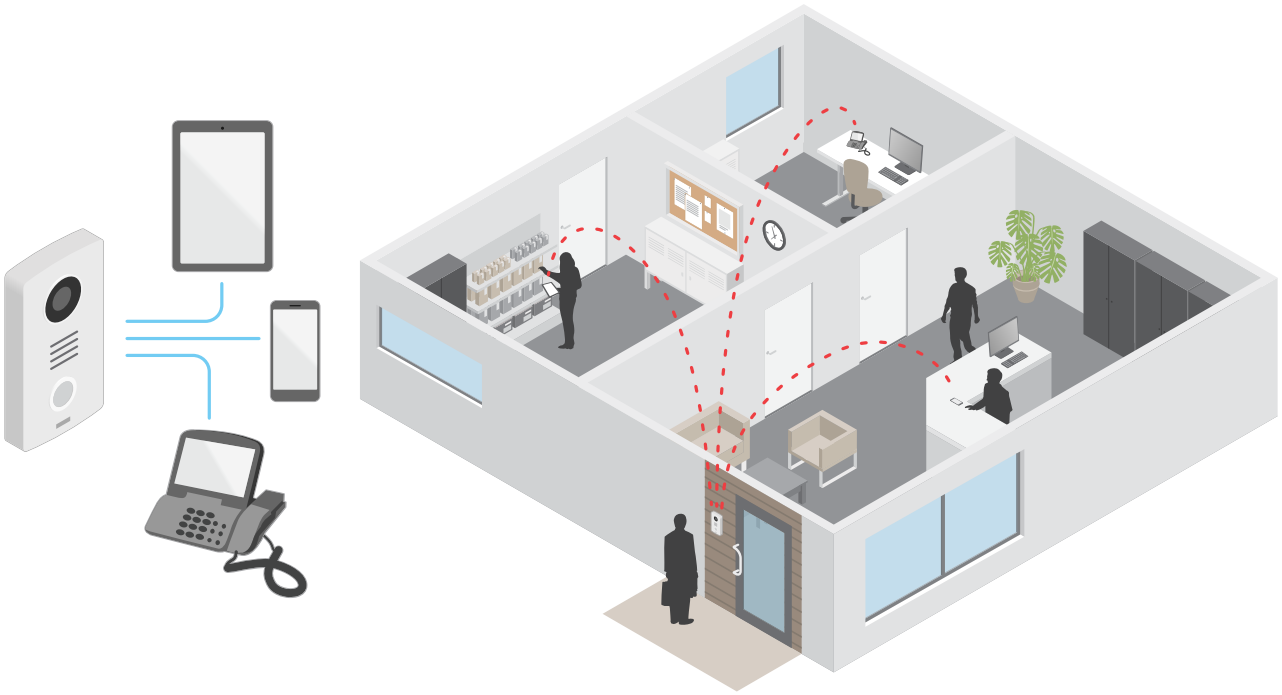
Dowiedz się więcej

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).

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.

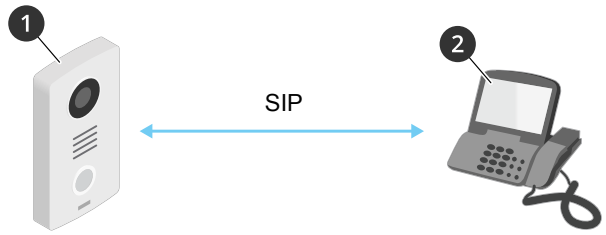
Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

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 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:



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.

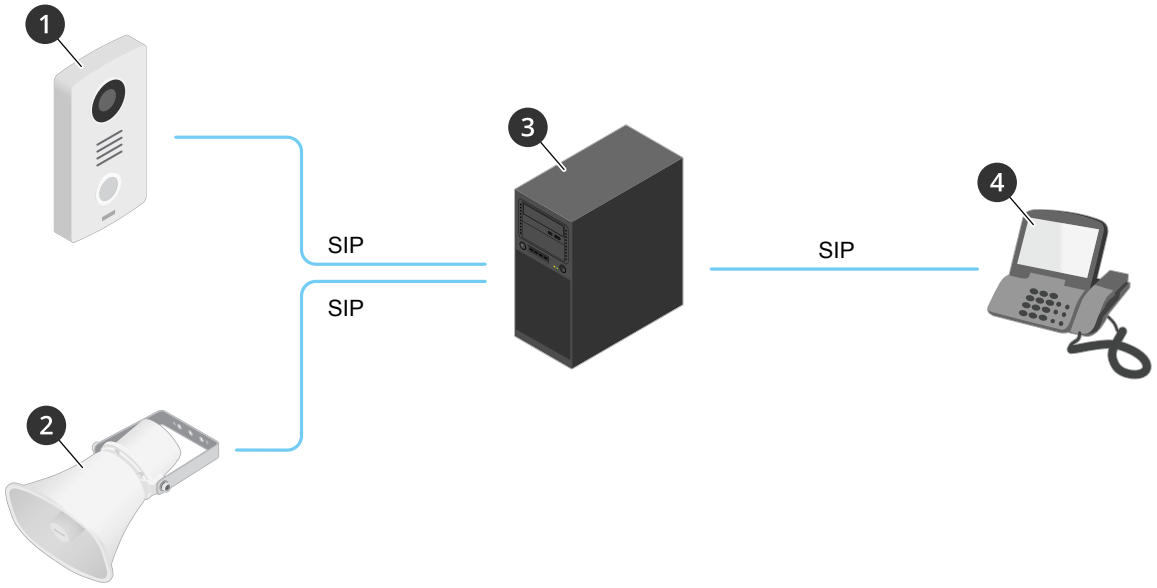
Private Branch Exchange (PBX) – centrala abonencka

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 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. Typowy adres SIP w tym przypadku to `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:



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.

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.

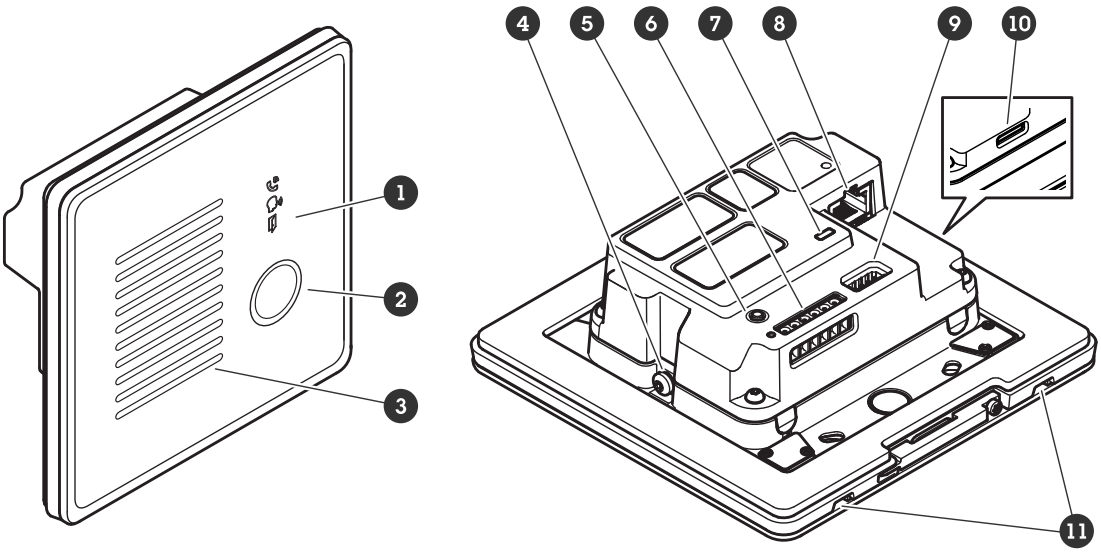
Podręczniki użytkownika do analiz i aplikacji Axis można znaleźć na stronie *help.axis.com*.

AXIS 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*.

Specyfikacje

Przegląd produktów



1 *Ikony wskaźników, on page 16*
2 *Przycisk połączenia*
3 *Głośnik*
4 *Śruba uziemienia*
5 *Przycisk kontrolny, on page 17*
6 *Złącze WE/WY, czytnika i przekaźnika, on page 17*
7 *Dioda stanu*
8 *Złącze sieciowe, on page 17*
9 *Złącze audio, on page 17*
10 *Gniazdo karty SD, on page 17 (microSD/microSDHC/microSDXC)*
11 *Mikrofon (2x)*

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. Podczas wkładania lub wyjmowania karty SD nie używaj ostrych narzędzi, przedmiotów metalowych ani nadmiernej siły. Kartę wkładaj i wyjmuj 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.

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 kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 24*.
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby nawiązać połączenie, naciśnij i zwolnij przycisk, a następnie poczekaj, aż dioda LED stanu mignie trzy razy na zielono.

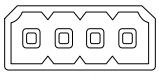
Złącza

Złącze sieciowe

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

Złącze audio

4-pinowy blok złączy wejść i wyjść audio.

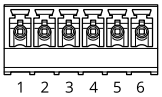


Funkcja	Pin	Uwagi
Wejście liniowe	1	Wejście liniowe (mono)
GND	2	Uziemienie audio
Wyjście liniowe	3	Wyjście liniowe (mono)
GND	4	Uziemienie audio

Złącze WE/WY, czytnika i przekaźnika

Tego złącza można używać do obsługi WE/WY i przekaźnika lub do podłączania czytników.

6-stykowy blok złączy



1 -
2 12 V
3 A/IO1
4 B/IO2
5 COM
6 NO/NZ

Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może służyć do zasilania urządzeń pomocniczych, jeśli dane urządzenie korzysta z zasilania PoE klasy 4. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC **We/Wy**: Maks. obciążenie = 50 mA **Czytnik/przekaźnik**: Maks. obciążenie = 350 mA
We/Wy: Konfigurowalne (wejście lub wyjście) **Czytnik**: A	3	**We/Wy**: Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. 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: **Czytnik**: RS485 – A	**We/Wy**: wejście – od 0 do maks. 30 V DC wyjście – od 0 do maks. 30 V DC, otwarty dren, 100 mA
We/Wy: Konfigurowalne (wejście lub wyjście) **Czytnik**: B	4	**We/Wy**: takie samo jak styk 3 **Czytnik**: RS485 – B	**We/Wy**: takie samo jak styk 3
Relay (Przekaźnik): COM	5	Wspólny	
Relay (Przekaźnik): NO/NZ	6	Normalnie otwarte/normalnie zamknięte. Do podłączania urządzeń przekaźnikowych. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd = 700 mA, maks. napięcie = 30 V DC

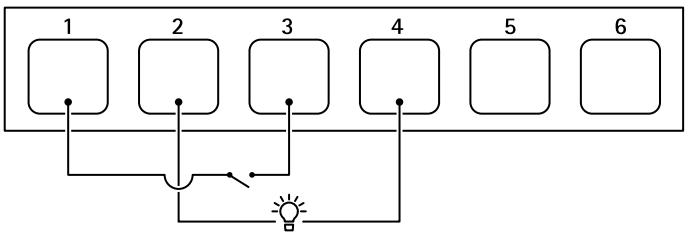
Złącze I/O

Jedna opcja pozwala używać złącza jako WE/WY 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.

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

Przykład:



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

Złącze przekaźnikowe

W połączeniu z WE/WY to złącze może służyć do podłączenia przekaźnika półprzewodnikowego i używania go:

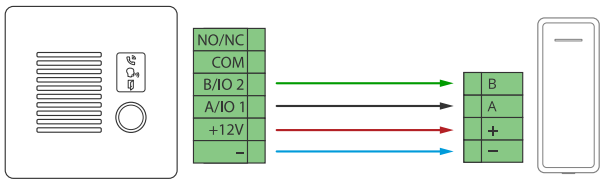
- jako standardowego przekaźnika otwierającego i zamykającego obwody pomocnicze;
- do bezpośredniego sterowania zamkiem;
- do sterowania zamkiem przez przekaźnik bezpieczeństwa. Korzystanie z przekaźnika bezpieczeństwa po bezpiecznej stronie drzwi zapobiega podłączeniu zewnętrznych przewodów.

Złącze czytnika

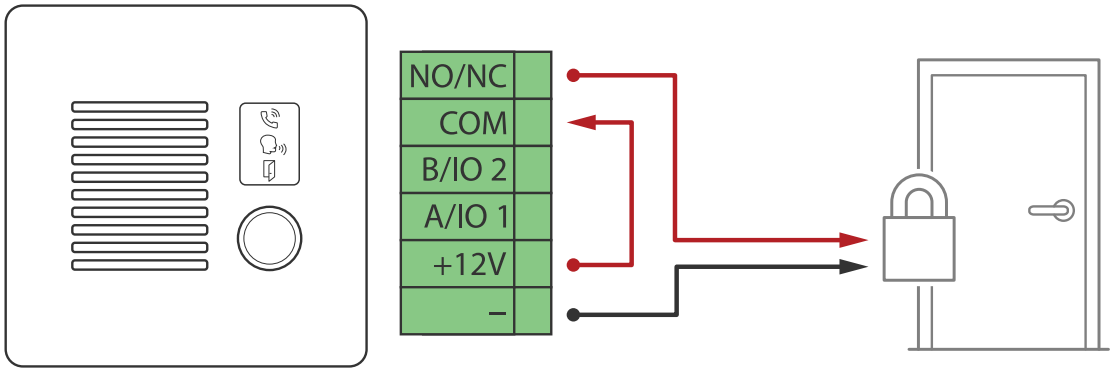
Trzecią opcją jest użycie tego złącza do podłączenia zewnętrznego czytnika.

Sprzęt podłączeniowy

Czytnik Axis

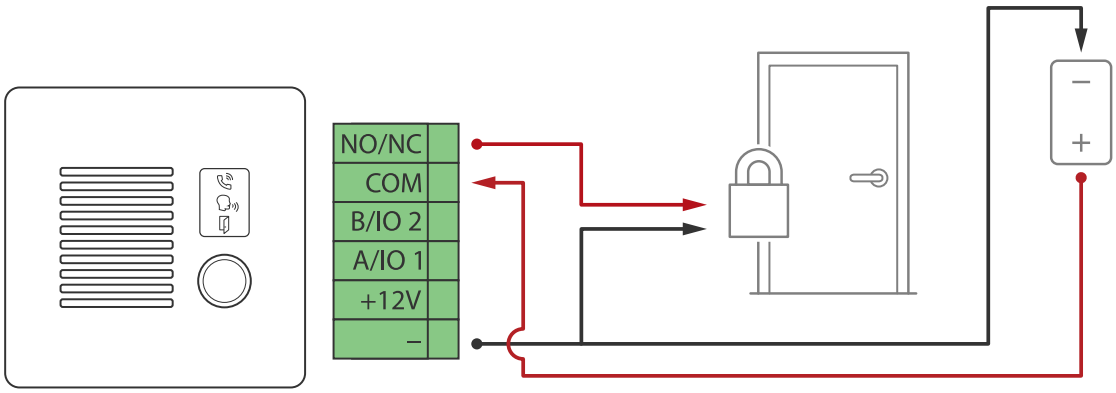


Przekaźnik zasilany przez zasilacz PoE (12 V)



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

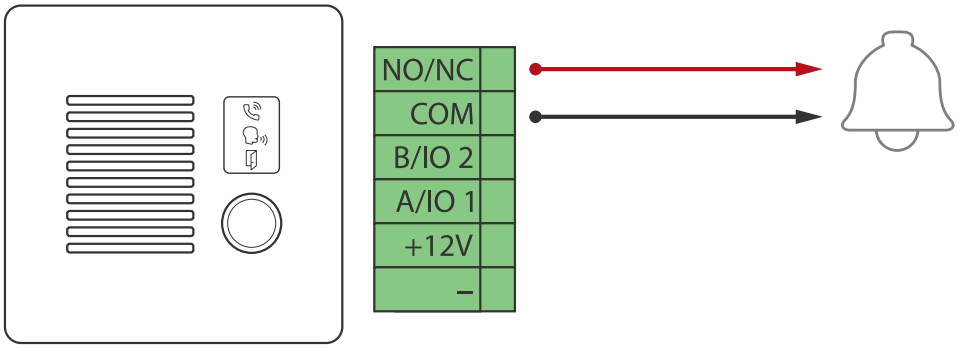
Przekaźnik zasilany przez osobny zasilacz



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

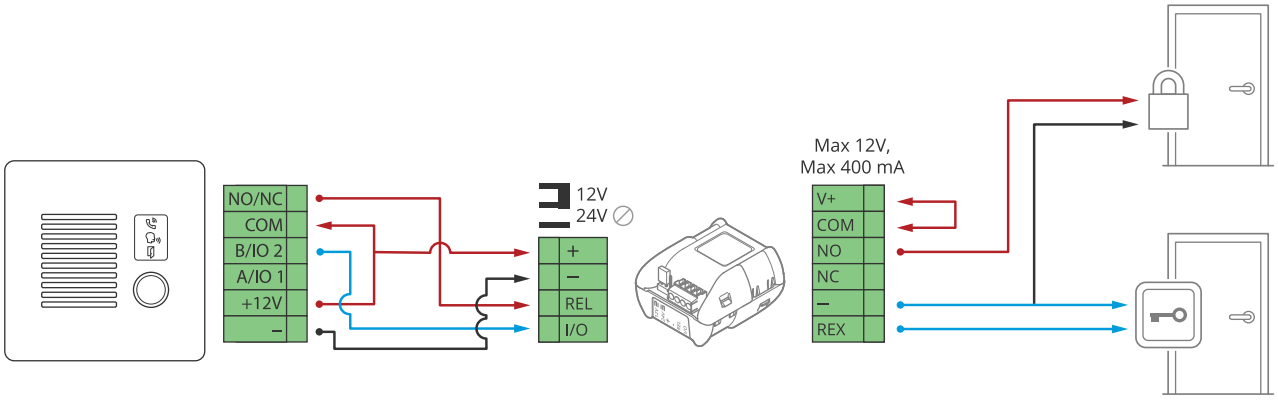
– do zamka zabezpieczonego

Przekaźnik bezpotencjałowy



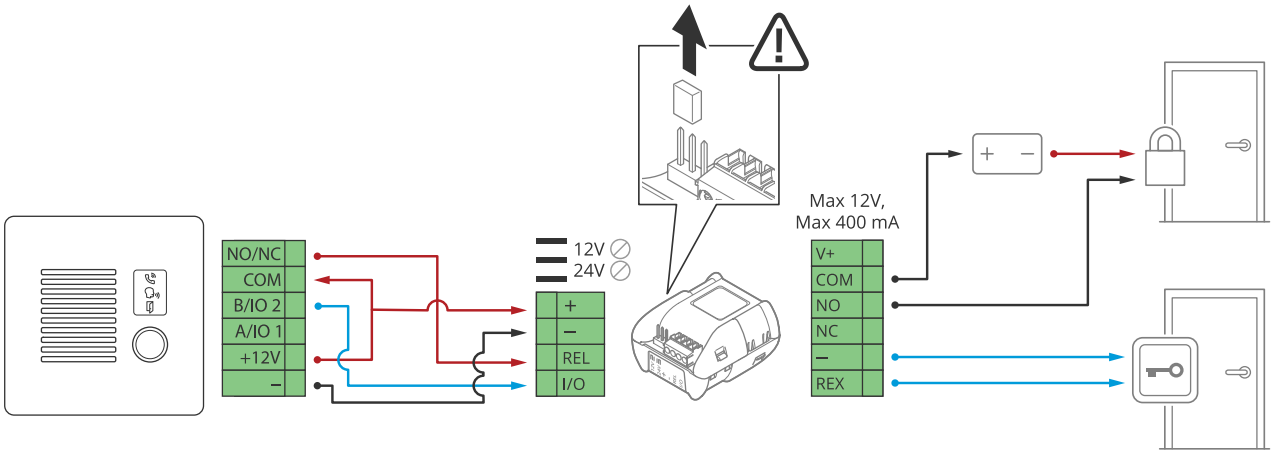
1. Aby sprawdzić stan przekaźnika, wybierz kolejno opcje **System > Accessories (System > Akcesoria)** i odszukaj port przekaźnika.
2. W ustawieniu **Normal state (Stan normalny)** zaznacz wartość:
   – do zamka zabezpieczonego podczas awarii zasilania
   – do zamka zabezpieczonego

Bezpieczna blokada 12 V zasilana przez zasilacz PoE z interkomu



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

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

Zalecenia dotyczące czyszczenia

Domofon sieciowy AXIS I7020 Network Intercom jest odporny na codzienne wielokrotne czyszczenie przy użyciu wyżej wymienionych środków chemicznych przez okres co najmniej pięciu lat.

Płyta czołowa domofonu jest odporna na powtarzalne i częste czyszczenie miękką szmatką z użyciem środka chemicznego. Nie występuje reakcja chemiczna między materiałem płyty czołowej a środkami czyszczącymi. Fizyczna integralność domofonu zostaje zachowana nawet w przypadku codziennego przecierania przy użyciu substancji chemicznych. Urządzenie można czyścić letnią wodą z dodatkiem następujących substancji:

- Alkohol izopropylowy 70% (IPA)
- Nadtlenek wodoru 3% (H_2O_2)
- Roztwór podchlorynu sodu <5% (NaClO) (wybielacz na bazie chlorku)
- Kwas octowy (10%)
- Kwas nadoctowy (0,12%)

⚠ UWAGA

Przed użyciem detergentu należy przeczytać jego etykietę i stosować się do podanych na niej zaleceń.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia acetonem ani benzyną.
- Nie należy rozpylać detergentu bezpośrednio na urządzenie. Detergent należy najpierw nanieść na miękką ściereczkę, a następnie przetrzeć nią urządzenie.
- Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawanie plam na obudowie.

1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
2. W razie potrzeby można przetrzeć urządzenie ściereczką zwilżoną letnią wodą i detergentem.
3. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Rozwiązywanie problemów

Przywracanie domyślnych ustawień fabrycznych

Ważne

Przywracanie ustawień fabrycznych powinno być dokonywane ze szczególną ostrożnością. Przywrócenie ustawień fabrycznych oznacza zresetowanie wszystkich ustawień, łącznie z adresem IP, do wartości fabrycznych.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Zob. *Przegląd produktów, on page 16*.
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 jest dostępny serwer DHCP, zostanie zastosowany domyślny adres IP urządzenia (jeden z poniższych):
   - **Urządzenia z oprogramowaniem AXIS OS w wersji 12.0 i nowszej**: Pobrane z podsieci adresów lokalnych (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS 11.11 lub starszym:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
   Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej *axis.com/support*.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

- 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. Jeżeli zostanie zwrócony komunikat: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci IP. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie.
  4. Jeżeli zostanie zwrócony komunikat: `Request timed out` (Upłynął limit czasu żądania), oznacza to, że adres IP jest dostępny i może zostać przypisany do urządzenia 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 p. *Przywracanie domyślnych ustawień fabrycznych, on page 24*.

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, p. *Obsługiwane przeglądarki, on page 5*.

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, odwiedź 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*.

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do bezpieczeństwa cybernetycznego znajdują się na stronie *axis.com/about-axis/cybersecurity*. Przestrzegaj poniższych wytycznych dotyczących bezpieczeństwa cybernetycznego, 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.

Zarządzanie podatnościami

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.

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.

T10213215_pl

2026-10 (M15.2)

© 2024 – 2026 Axis Communications AB