AXIS A9210 Network I/O Relay Module

Podręcznik użytkownika

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 2*.

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

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła, on page 3*.
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.

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.

Omówienie interfejsu WWW

Ten film przybliża najważniejsze elementy i schemat działania interfejsu WWW urządzenia.

Interfejs WWW urządzenia Axis

Konfiguracja urządzenia

Konfiguracja portu WE/WY

1. Wybierz kolejno opcje **Device > I/Os and relays > AXIS A9210 > I/Os (Urządzenia > We/wy i przekaźniki > AXIS A9210 > We/wy)**.
2. Kliknij , aby rozwinąć ustawienia portu WE/WY.
3. Zmień nazwę portu.
4. Skonfiguruj stan normalny. Kliknij w przypadku obwodu otwartego lub w przypadku obwodu zamkniętego.
5. Aby skonfigurować port WE/WY jako wejście:
   5.1. W obszarze **Direction (Kierunek)** kliknij .
   5.2. Aby monitorować stan wejścia, włącz **Supervised (Nadzorowane)**. Patrz *Nadzorowane wejścia, on page 14*.

Uwaga

W interfejsach API nadzorowane porty WE/WY działają inaczej niż nadzorowane porty wejścia. Więcej informacji można uzyskać, przechodząc do *biblioteki VAPIX®*.

6. Aby skonfigurować port WE/WY jako wyjście:
   6.1. W obszarze **Direction (Kierunek)** kliknij .
   6.2. Aby wyświetlić adresy URL służące do aktywacji i dezaktywacji podłączonych urządzeń, przejdź do menu **Toggle port URL (Przełącz adres URL portu)**.

Konfiguracja przekaźnika

1. Wybierz kolejno opcje **Device > I/Os and relays > AXIS A9210 > Relays (Urządzenia > We/wy i przekaźniki > AXIS A9210 > Przekaźniki)**.
2. Kliknij , aby rozwinąć ustawienia przekaźnika.
3. Włącz opcję **Relay (Przekaźnik)**.
4. Zmień nazwę przekaźnika.
5. Aby wyświetlić adresy URL służące do aktywacji i dezaktywacji przekaźnika, przejdź do menu **Toggle port URL (Przełącz adres URL portu)**.

Konfiguracja reguł dotyczących zdarzeń

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

Wyzwalanie akcji

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

Uwaga

- Po dokonaniu zmian w aktywnej regule należy ją uruchomić ponownie, aby uwzględnić zmiany.

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

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 Door Monitoring

Aplikacja ta monitoruje stan drzwi, wskazując, czy są otwarte czy zamknięte, a także czy pozostają otwarte zbyt długo. Aplikacja sprawdzi się choćby w przypadku niewymagających zamka drzwi przeciwpożarowych, o których warto wiedzieć, czy są otwarte.

Zwykłe drzwi zawierają czujnik położenia i przycisk REX, ale także zamki i czytniki powodujące konieczność stosowania kontrolera drzwiowego.

Drzwi monitorowane wymagają jedynie czujnika położenia drzwi i przycisku REX, a monitorować je można za pomocą sieciowego modułu przekaźnikowego we / wy. Każdy sieciowy moduł przekaźnikowy we / wy można dołączyć do maks. pięciu monitorowanych drzwi.

Ograniczenia

Aplikacja dostępna jest jedynie w module AXIS A9210. Przycisk REX można dołączyć wyłącznie do we / wy 1 i we / wy 2; nie jest możliwe skonfigurowanie przycisku REX na we 3, we 4 ani we 5.

Konfiguracja AXIS Monitoring Door

Nazwa	Opis
Drzwi	Numer drzwi.
Wejście DPS	Wejście DPS dot. drzwi.
Wejście REX	Wejście REX dot. drzwi.
Door open too long time (sec) (Drzwi otwarte zbyt długo (s))	Czas (w sekundach), przez jaki drzwi mogą pozostawać otwarte.
Czas dostępu (s)	Czas (w sekundach) odryglowania drzwi po uzyskaniu dostępu.
Status	Status drzwi.

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisie produktu na stronie Axis.com.

Aby uzyskać szczegółowe informacje na temat cyberbezpieczeństwa w systemie AXIS OS, zapoznaj się z *przewodnikiem po zabezpieczeniach systemu operacyjnego AXIS OS*.

Axis Edge Vault

Axis Edge Vault to sprzętowa platforma cyberbezpieczeństwa chroniąca urządzenie Axis. Zawiera funkcje gwarantujące tożsamość i integralność urządzenia oraz ochronę poufnych informacji przed nieuprawnionym dostępem. Rozwiązanie to bazuje na mocnych podstawach zapewnianych przez kryptograficzne moduły obliczeniowe (bezpieczny element i TPM) oraz zabezpieczenia procesora SoC (TEE i bezpieczny start), a także na specjalistycznej wiedzy z zakresu bezpieczeństwa urządzeń brzegowych.

Podpisany system operacyjny

Podpisany system operacyjny jest wdrażany przez dostawcę oprogramowania podpisującego obraz systemu AXIS OS za pomocą klucza prywatnego. Po dołączeniu podpisu do systemu operacyjnego urządzenie sprawdzi poprawność oprogramowania przed jego zainstalowaniem. Jeżeli urządzenie wykryje naruszenie integralności oprogramowania, aktualizacja systemu AXIS OS zostanie odrzucona.

Bezpieczny start

Bezpieczny start to proces składający się z nieprzerwanego łańcucha oprogramowania zweryfikowanego kryptograficznie, rozpoczynający się w pamięci niezmiennej (rozruchowej pamięci ROM). Dzięki wykorzystaniu podpisanego systemu operacyjnego bezpieczny rozruch gwarantuje uruchomienie urządzenia wyłącznie z autoryzowanym oprogramowaniem.

Bezpieczny magazyn kluczy

Jest to zabezpieczone przed sabotażem środowisko do ochrony kluczy prywatnych i bezpiecznego wykonywania operacji kryptograficznych. Zapobiega nieautoryzowanemu dostępowi i złośliwemu wykradaniu w przypadku włamania do systemu. W zależności od wymogów bezpieczeństwa urządzenie Axis może mieć jeden lub kilka sprzętowych modułów kryptograficznych, które udostępniają chroniony sprzętowo bezpieczny magazyn kluczy. W zależności od wymogów dotyczących zabezpieczeń urządzenie Axis może mieć jeden lub wiele sprzętowych kryptograficznych modułów obliczeniowych, takich jak TPM 2.0 (Trusted Platform Module) lub zabezpieczony element i/lub TEE (Trusted Execution Environment), które zapewniają ochronę sprzętową magazynu kluczy. Ponadto wybrane produkty Axis są wyposażone w bezpieczny magazyn kluczy z certyfikatem FIPS 140-2 poziomu 2.

Identyfikator urządzenia axis

możliwość zweryfikowania pochodzenia urządzenia jest kluczowa z perspektywy wiarygodności tożsamości urządzenia. Podczas produkcji urządzenia z rozwiązaniem Axis Edge Vault mają przypisywany unikatowy fabryczny i zgodny ze standardem IEEE 802.1AR certyfikat znany jako identyfikator urządzenia Axis. Jest on swego rodzaju paszportem, który potwierdza pochodzenie urządzenia. Identyfikator urządzenia jest bezpiecznie i trwale przechowywany w bezpiecznym magazynie kluczy w postaci certyfikatu podpisanego za pomocą certyfikatu głównego Axis. ID urządzenia może być wykorzystywany przez infrastrukturę IT klienta do zautomatyzowanego bezpiecznego wdrażania urządzeń i bezpiecznej identyfikacji urządzeń.

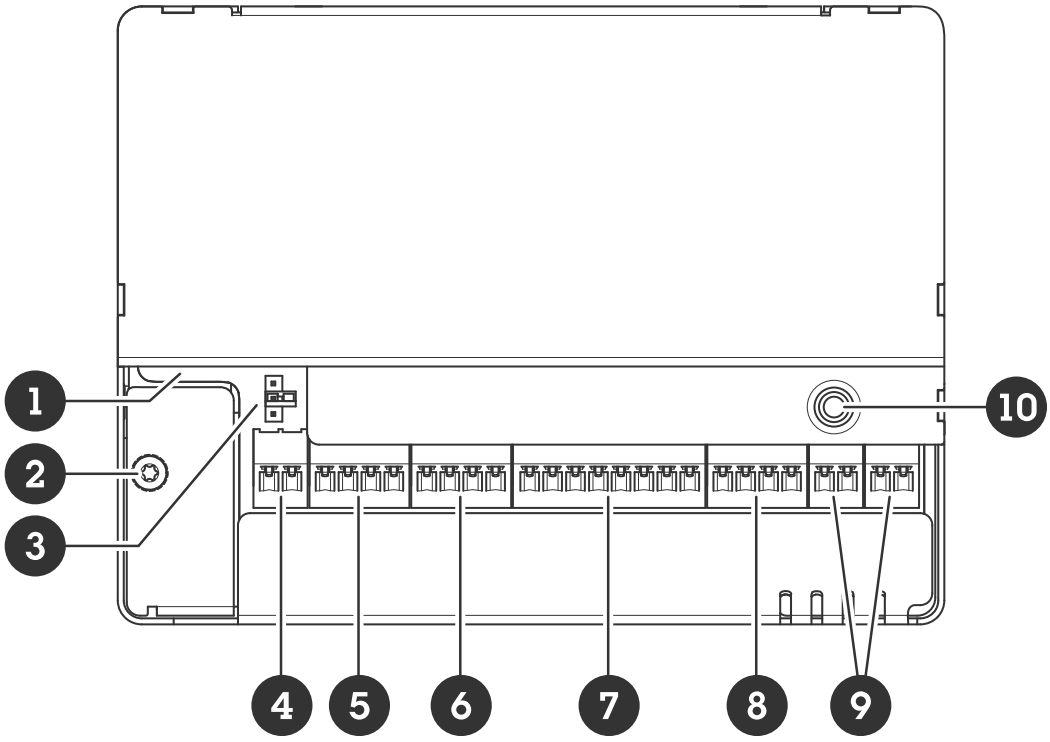
Zaszyfrowany system plików

Bezpieczny magazyn kluczy zapobiega złośliwemu wyprowadzaniu danych i manipulowaniu konfiguracją przez wymuszanie silnego szyfrowania systemu plików. Zapewnia to, że żadne dane przechowywane w systemie plików nie mogą zostać pobrane ani naruszone, gdy urządzenie Axis nie jest używane, uzyskano do niego nieautoryzowany dostęp i/lub zostało skradzione. Podczas bezpiecznego rozruchu system plików z uprawnieniami odczytu/zapisu jest odszyfrowywany, po czym można go zamontować i używać na urządzeniu Axis.

Aby dowiedzieć się więcej o funkcjach cyberbezpieczeństwa stosowanych w urządzeniach Axis, przejdź do strony *axis.com/learning/white-papers* i poszukaj według hasła „cybersecurity".

Specyfikacje

Przegląd produktów



1 *Złącze sieciowe*
2 *Położenie uziemienia*
3 *Zworka przekaźnika*
4 *Złącze zasilania*
5 *Złącze przekaźnikowe*
6 *Złącze wejścia 1*
7 *RS485 i złącze WE/WY*
8 *Złącze I/O*
9 *Złącze wejścia 2*
10 *Przycisk kontrolny*

Wskaźniki LED

dioda LED	Kolor	Wskazanie
Status	Zielony	Stałe zielone światło przy normalnym działaniu.
	Bursztynowy	Stałe światło podczas uruchamiania i odtwarzania ustawień.
	Czerwony	Powolne miganie w przypadku niepowodzenia aktualizacji.
Sieć	Zielony	Stałe światło przy podłączeniu do sieci 100 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Bursztynowy	Stałe światło przy podłączeniu do sieci 10 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Zgaszony	Brak połączenia z siecią.

Zasilanie	Zielony	Normalne działanie.
	Bursztynowy	Miga na zielono/bursztynowo podczas aktualizacji oprogramowania sprzętowego.
Przekaźnik	Zielony	Przekaźnik aktywny.[1]
	Zgaszony	Przekaźnik nieaktywny.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 16*.
- 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 Plus (PoE+).

UL: zasilanie Power over Ethernet (PoE) dostarczane przez zasilacz typu Power Injector Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3 lub Power over Ethernet Plus (PoE+) IEEE 802.3at typ 2 klasa 4 z ograniczeniem mocy, dostarczający zasilanie 44–57 V DC, 15,4 W / 30 W. Zasilanie Power over Ethernet (PoE) zostało ocenione przez UL z zasilaczem AXIS T8133 Midspan 30 W 1-port.

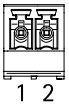
Priorytet mocy

Urządzenie to może być zasilane przez wejście PoE lub DC. Patrz *Złącze sieciowe, on page 9* i *Złącze zasilania, on page 9*.

- Gdy PoE i DC są podłączone przed włączeniem urządzenia, będzie ono zasilane z PoE.
- Zarówno PoE, jak i DC są podłączone, a urządzenie jest zasilane przez wejście PoE Gdy połączenie z PoE zostanie utracone, urządzenie przejdzie na tryb zasilania prądem stałym bez ponownego uruchomienia.
- Zarówno PoE, jak i DC są podłączone, a urządzenie jest zasilane prądem stałym. Gdy połączenie z DC zostanie utracone, nastąpi ponowne uruchomienie urządzenia i przełączenie na zasilanie z PoE.
- Jeżeli podczas rozruchu urządzenie jest zasilane prądem stałym, a po jego uruchomieniu nastąpi podłączenie PoE, urządzenie będzie zasilane prądem stałym.
- Jeżeli podczas rozruchu urządzenie jest zasilane z PoE, a po jego uruchomieniu nastąpi podłączenie DC, urządzenie będzie zasilane z PoE.

Złącze zasilania

2-pinowy blok złączy na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤100 W lub nominalnym prądem ograniczonym do ≤5 A.



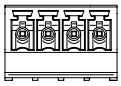
1. *Przekaźnik jest aktywny po podłączeniu COM do NO.*

Funkcje	Styk	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
Wejście DC	2	Do zasilania urządzenia, gdy nie jest używane zasilanie Power over Ethernet. Uwaga: ten styk może być używany tylko jako wejście zasilania.	12 V DC, maks. 36 W

UL: zasilanie prądem stałym dostarczane przy użyciu zasilacza w standardzie UL 603, w zależności od rodzaju zastosowań, o odpowiednich parametrach znamionowych.

Złącze przekaźnikowe

Jeden 4-stykowy blok złączy dla przekaźników typu C, który może być używany na przykład do sterowania zamkiem lub interfejsem do bramy. W przypadku stosowania z obciążeniem indukcyjnym, np. zamkiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
NO	2	Normalnie otwarte. Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NO i DC. Dwa styki przekaźnika są galwanicznie oddzielone od reszty obwodu, jeśli zworki nie są używane.	Maks. prąd = 2 A Maks. napięcie = 30 V DC
COM	3	Wspólny	
NC	4	NC (normalnie zamknięty). Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NC i DC. Dwa styki przekaźnika są galwanicznie oddzielone od reszty obwodu, jeśli zworki nie są używane.	

Zworka zasilania przekaźnika

Po podłączeniu zworki zasilania przekaźnika łączy ona 12 V DC lub 24 V DC z stykiem COM przekaźnika.

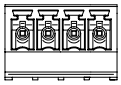
Można jej użyć do połączenia zamka między stykami GND i NO lub GND i NC.

Źródło prądu	Maksymalna moc przy 12 V DC	Maksymalna moc przy 24 V DC
DC IN	2 000 mA	1 000 mA
PoE	350 mA	150 mA
PoE+	1100 mA	500 mA

Złącze wejścia 1

Jeden 4-stykowy blok złączy na wejście.

Obsługuje nadzorowanie przy użyciu rezystorów końca linii. Alarm wyzwalany jest po przerwaniu połączenia. Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii. Dla wejść nadzorowanych użyj schematu połączeń. Patrz *Nadzorowane wejścia, on page 14*.



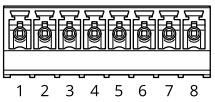
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Wejście	2, 4	Wejście cyfrowe lub wejście nadzorowane — podłącz odpowiednio do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Ważne

Dopuszczalna długość kabla wynosi do 200 m (656 stóp), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 24.

RS485 i złącze WE/WY

Jeden 8-stykowy blok złączy, w tym 4-stykowy RS485 i 4-stykowy WE/WY.



RS485

Funkcje	Styk	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Zasila urządzenia pomocnicze, takie jak czujniki Modbus.	12 V DC, maks. 200 mA
A	3		
B	4		

We/wy

Funkcje	Styk	Uwaga	Specyfikacje
Wyjście cyfrowe	5	W przypadku stosowania z obciążeniem	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

		indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	
Wyjście cyfrowe	6	W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA
Wejście	7	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
Wyjście cyfrowe	8	W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Ważne

- Dopuszczalna długość kabla w przypadku RS485 wynosi do 1000 m (3281 stóp), jeśli spełnione są następujące wymagania dotyczące kabla: 1 skrętka ekranowana, AWG 24, impedancja 120 omów.
- Dopuszczalna długość kabla w przypadku WE/WY wynosi do 200 m (656 stóp).

Złącze I/O

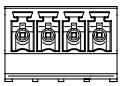
Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

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

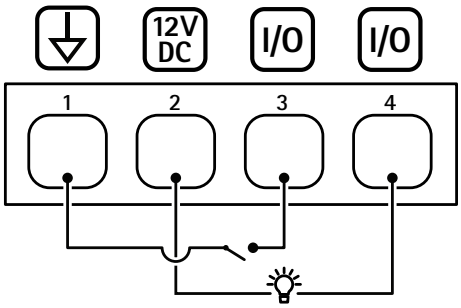
Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

Wyjście cyfrowe – Do podłączania urządzeń zewnętrznych, takich jak przekaźniki i diody LED. Podłączone urządzenia można aktywować za pomocą interfejsu programowania aplikacji (API) VAPIX® lub z poziomu strony internetowej produktu.

4-pinowy blok złączy



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maksymalne obciążenie = 50 mA łącznie
Konfigurowalne (wejście lub wyjście)	3–4	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Aby mieć możliwość korzystania z nadzorowanego wejścia, zamontuj rezystory końca linii. Patrz diagram połączeń, aby uzyskać informacje na temat podłączania rezystorów.	od 0 do maks. 30 V DC
		Wyjście cyfrowe — podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku użycia z obciążeniem indukcyjnym, np. przekaźnikiem, należy równolegle do obciążenia podłączyć diodę, aby zapewnić ochronę przed stanami nieustalonymi napięcia. Wejścia/wyjścia umożliwiają sterowanie obciążeniem zewnętrznym 12 V DC, 50 mA (maks. wartość łączna), jeśli używane jest wyjście wewnętrzne 12 V DC (styk 2). W przypadku podłączeń z otwartym drenem w połączeniu z zewnętrznym źródłem zasilania WE/WY mogą otrzymywać zasilanie DC 0–30 V DC, 100 mA.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

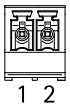


1 *Masa DC*
2 *Wyjście DC 12 V*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*

Złącze wejścia 2

Dwa 2-stykowe bloki złączy umożliwiające podłączenie urządzeń zewnętrznych, na przykład detektorów wybicia szyby lub czujników pożaru.

UL: złącze nie zostało ocenione przez UL pod kątem użytkowania jako alarm antywłamaniowy ani pożarowy.



Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wejście	2	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

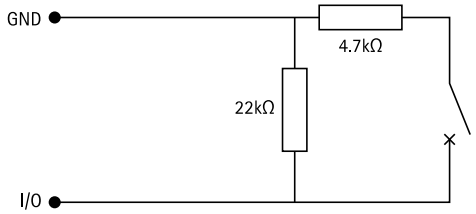
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wejście	2	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Nadzorowane wejścia

Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii zgodnie ze schematem poniżej.

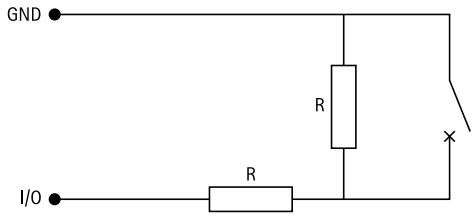
Pierwsze połączenie równoległe

Oporniki muszą mieć wartości 4,7 kΩ i 22 kΩ.



Pierwsze połączenie szeregowe

Wartości oporników muszą być takie same; możliwe wartości: 1 kΩ, 2,2 kΩ, 4,7 kΩ oraz 10 kΩ, 1 %, ¼ W standardowo.



Uwaga

Zaleca się korzystanie ze skrętek ekranowanych. Podłącz ekranowanie do 0 V DC.

Status	Opis
Otwarte	Nadzorowany przełącznik działa w trybie otwartym.
Zamknięte	Nadzorowany przełącznik działa w trybie zamkniętym.

Krótki	Kabel WE/WY lub wejścia 1–5 powoduje zwarcie do GND.
Przerwanie	Kabel WE/WY lub wejścia 1–5 został przecięty i pozostawiony otwarty bez ścieżki prądu do GND.

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 8*.
3. Przytrzymuj przycisk Control przez 25 sekund, aż wskaźnik LED stanu ponownie zmieni kolor na bursztynowy.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
   - **Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej:** Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do produktu.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

- Po aktualizacji oprogramowania urządzenia poczynione ustawienia zostaną zachowane. Axis Communications AB nie gwarantuje, że ustawienia te zostaną zachowane, nawet gdy funkcje są dostępne w nowej wersji systemu operacyjnego AXIS OS.
- Począwszy od systemu operacyjnego AXIS OS w wersji 12.6, pomiędzy aktualną a docelową wersją urządzenia należy zainstalować każdą wersję LTS. Przykładowo, jeżeli aktualnie zainstalowana wersja oprogramowania urządzenia to AXIS OS 11.2, przed aktualizacją urządzenia do wersji AXIS OS 12.6 należy zainstalować wersję LTS AXIS OS 11.11. Więcej informacji znajduje się w *Portalu 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 2*.

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 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.

Problemy z obsługą urządzenia

Przedni grzejnik i wycieraczka nie działają

Jeżeli nie włącza się przedni grzejnik lub wycieraczka, sprawdź, czy górna pokrywa jest prawidłowo zamocowana do dolnej części obudowy.

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

Kontakt z pomocą techniczną

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

T10202445_pl

2026-02 (M7.2)