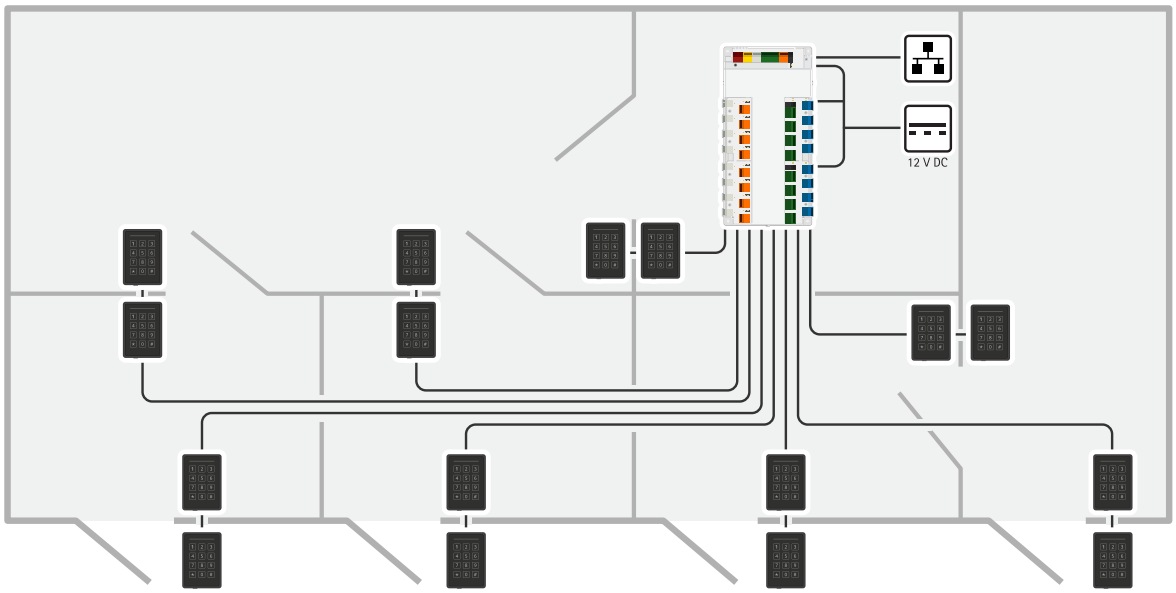
AXIS A1810-B Network Door Controller

Podręcznik użytkownika

Spis treści

Informacje o rozwiązaniu....3
Instalacja....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
Omówienie interfejsu WWW....6
Konfiguracja urządzenia....7
Dodawanie modułu AXIS A9910....7
Kontrola windy....7
Door override (Nadpisanie drzwi)....8
Profil LED OSDP....8
Format karty....10
Interfejs WWW....11
Dowiedz się więcej....12
Cyberbezpieczeństwo....12
Usługa powiadomień o zabezpieczeniach Axis....12
Zarządzanie podatnościami....12
Bezpieczne działanie urządzeń Axis....12
Specyfikacje....13
Przegląd produktów....13
Wskaźniki LED....14
Przyciski....15
Przycisk kontrolny....15
Złącza....15
Złącze sieciowe....15
Opcje zasilania....15
Priorytet mocy....15
Złącze zasilania....15
Złącze wejściowe....16
Złącze wyjściowe....17
Złącze przekaźnikowe....17
Złącze pomocnicze....18
Złącze sabotażu/alarmu....19
Złącze czytnika....20
Złącze drzwi....21
Złącze przekaźnika drzwi....21
Złącze przekaźnika AUX....22
Nadzorowane wejścia....23
....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
Kontakt z pomocą techniczną....27

Informacje o rozwiązaniu



Sieciowy kontroler drzwi można łatwo podłączyć do istniejącej sieci IP. Każdy sieciowy kontroler drzwi może zasilać do 16 czytników i 8 zamków oraz nimi sterować.

Instalacja


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

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.

Omówienie interfejsu WWW

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



Interfejs WWW urządzenia Axis

Konfiguracja urządzenia

Więcej informacji na temat konfiguracji urządzenia można znaleźć w *instrukcji obsługi AXIS Camera Station* lub rozwiązań innych firm.

Dodawanie modułu AXIS A9910

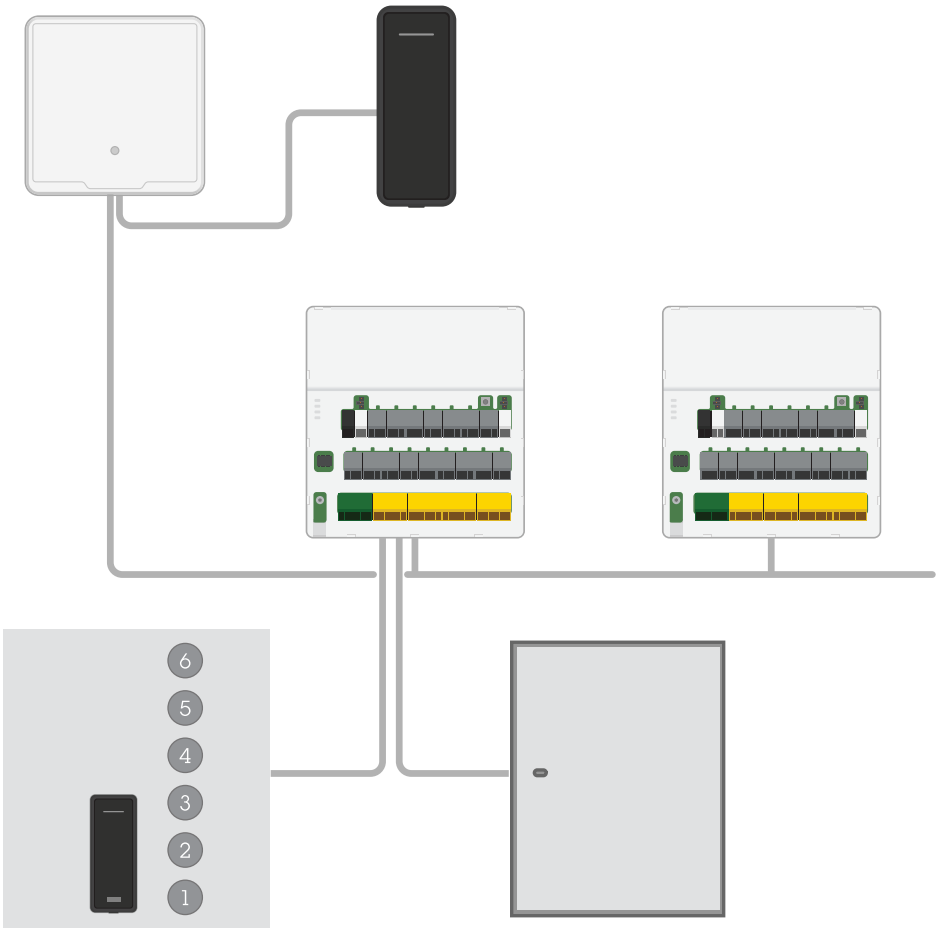
- W interfejsie WWW kontrolera drzwi przejdź do **Device (Urządzenie) > I/Os and relays (WE/WY i przekaźniki)**.
- Kliknij **Add encryption key (Dodaj klucz szyfrowania)**.
- Jeśli klucz szyfrowania został wygenerowany już wcześniej, wprowadź go i kliknij **OK**.
- Aby wygenerować klucz szyfrowania:
  - Kliknij **Generate key (Generuj klucz)**.
  - Kliknij **Export key (Eksportuj klucz)**, aby zapisać klucz. W przypadku zagubienia klucza szyfrowania utracisz dostęp do urządzenia.
  - Kliknij **OK**.
- Kliknij **Add AXIS A9910 (Dodaj AXIS A9910)**.
- Wprowadź nazwę i wybierz port RS485 oraz adres, które mają być używane.
- Kliknij **OK**.

Kontrola windy

Dzięki czytnikowi umieszczonemu w kabinie windy można kontrolować dostęp do poszczególnych pięter za pomocą kontrolera drzwiowego i modułu rozszerzeń Axis.

Do jednego kontrolera drzwiowego i modułów rozszerzeń Axis można dołączyć maks. 64 piętra:

- Moduły rozszerzające wykorzystują jeden port czytnika w kontrolerze.
- Drugi port czytnika jest używany przez czytnik umieszczony w kabinie windy.



Door override (Nadpisanie drzwi)

Ważne

Ta funkcja przejmuje bezpośrednią kontrolę nad przekaźnikami drzwiowymi i zastępuje konfigurację przekaźników w programie AXIS Camera Station. Można z niej korzystać wyłącznie w przypadku, gdy dział pomocy technicznej firmy Axis wyraźnie to zalecił.

1. Zatrzymaj usługę Secure Entry w programie AXIS Camera Station.
2. W interfejsie WWW kontrolera drzwi wybierz **Advanced > Door override (Zaawansowane > Nadpisanie drzwi)**.
3. Uważnie zapoznaj się z informacjami podanymi na stronie, a następnie kliknij **I Understand (Rozumiem)**.
4. Włącz opcję **Door override (Nadpisanie drzwi)** i kliknij **Enable (Włącz)**.
5. Przejdź do przekaźnika drzwiowego i kliknij **Lock (Zablokuj)**, **Unlock (Odblokuj)** lub **Access (Dostęp)**, aby zablokować drzwi, odblokować je lub przyznać dostęp.
6. Przejdź do przekaźnika, który chcesz skonfigurować, i kliknij **Activate (Włącz)** lub **Deactivate (Wyłącz)**, aby włączyć lub wyłączyć przekaźnik.

Profil LED OSDP

Można dostosować profile LED czytnika OSDP, aby zdefiniować sygnały świetlne i dźwiękowe wykorzystywane dla różnych zdarzeń. Pełną listę profili można znaleźć w sekcji *LED profiles (Profile LED)*.

Ustawianie poziomów światła i dźwięku

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Rozwiń menu **Light and audio levels (Poziomy światła i dźwięku)**.
3. Wyreguluj jasność paska LED, podświetlenia LED oraz głośność za pomocą suwaka.
4. Kliknij przycisk **Save (Zapisz)**.

Uwaga

Po zmianie poziomów światła i dźwięku ustawienia te są aktualizowane dla wszystkich czytników podłączonych do kontrolera.

Testowanie ustawień LED czytnika OSDP:

Za pomocą menu **OSDP LED test (Test LED czytnika OSDP)** można sprawdzić ustawienia dźwięku i światła dla dowolnego profilu czytnika.

Aby przetestować ustawienia profili LED OSDP:

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Rozwiń menu **OSDP LED test (Test LED OSDP)**.
3. Wybierz sygnalizację LED.
4. Wybierz czytnik, który chcesz przetestować.
5. Kliknij przycisk **Start (Rozpocznij)**.
6. Kliknij **Edit feedback (Edytuj sygnalizację)**, aby zmienić ustawienia światła i dźwięku dla swojego profilu.
   - Wybierz nowy kolor z menu rozwijanego **Color (Kolor)**.
   - W razie potrzeby wybierz częstotliwość dźwięku z menu rozwijanego **Audio**.
   - Można również zresetować ustawienia profilu, klikając opcję **Reset to default values (Przywróć wartości domyślne)**.
   - Kliknij przycisk **Save (Zapisz)**.

Zmiana ustawień profilu LED OSDP:

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Przejdź do menu **OSDP LED profile (Profil LED OSDP)**.
3. Kliknij obok profilu, który chcesz zmienić.
4. Zmodyfikuj odpowiednie ustawienia:
   - Wybierz sposób działania diod LED z menu rozwijanego **Behavior (Zachowanie)**.
   - Wybierz kolor diod LED z menu rozwijanego **Color (Kolor)**.
   - Ustaw parametry **Duration on (Czas włączenia)** i **Duration off (Czas wyłączenia)** dla diod LED.
   - Ustaw parametr **Recurrence (Powtarzanie)** dla diod LED.
   - Z menu rozwijanego **Audio** wybierz parametry **Beep duration, on (Czas trwania sygnału dźwiękowego – włączony)** i **Beep duration, off (Czas trwania sygnału dźwiękowego – wyłączony)**, a następnie ustaw parametr **Recurrence (Powtarzanie)** dla sygnału dźwiękowego. Upewnij się, że parametry **Beep duration, on (Czas trwania sygnału dźwiękowego – włączony)** i **Beep duration, off (Czas trwania sygnału dźwiękowego – wyłączony)** mają taką samą wartość.
5. Kliknij przycisk **Save (Zapisz)**.

Importowanie istniejących ustawień z innego kontrolera

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Kliknij **Import (Importuj)**.
3. Wybierz plik, który chcesz przesłać.
4. Kliknij **Import (Importuj)**.

Eksportowanie bieżących ustawień

1. Przejdź do menu **Peripherals (Urządzenia peryferyjne)** > **Readers (Czytniki)** > **OSDP LED profile (Profil LED OSDP)**.
2. Kliknij **Export (Eksportuj)**.
3. Wybierz lokalizację, w której chcesz zapisać plik json, i kliknij **Save (Zapisz)**.

Format karty

Ta funkcja jest przeznaczona wyłącznie dla zaawansowanych użytkowników. Natychmiast po włączeniu funkcji **Card format (Format karty)**:

- Jeśli używasz poświadczenia 37-bitowego, zostaje usunięte ostatnie 5 bitów.
- Jeśli używasz poświadczenia 64-bitowego (kod QR), zostaje usunięta pierwsza sekwencja 24-bitowa.

Do wyświetlenia poświadczeń można użyć danych przykładowych albo czytnika kart.

1. Wybierz kolejno opcje **Advanced (Zaawansowane)** > **Card format (Format karty)**.
2. Zapoznaj się z ostrzeżeniem i kliknij **I understand (Rozumiem)**, aby włączyć funkcję **Card format (Format karty)**.
3. Wybierz swój czytnik z menu rozwijanego **Reader data visualization (Wizualizacja danych czytnika)**.
4. Kliknij opcję **Get reader data (Pobierz dane czytnika)** lub **Use sample data (Użyj danych przykładowych)**, aby wygenerować dane wyjściowe karty. Zostaną one zastosowane do wszystkich posiadaczy kart w urządzeniu.
5. Włącz opcję **Trim reader data (Przytnij dane czytnika)**, aby usunąć końcowe bity z poświadczeń kart.
6. Kliknij przycisk **Włącz**.

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

Cyberbezpieczeństwo

Informacje na temat cyberbezpieczeństwa dotyczące poszczególnych produktów można znaleźć w opisach produktów 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*.

Usługa powiadomień o zabezpieczeniach Axis

Axis świadczy usługę powiadamiania z informacjami o lukach w zabezpieczeniach i innych sprawach dotyczących bezpieczeństwa urządzeń Axis. Aby otrzymywać powiadomienia, możesz aktywować subskrypcję na stronie *axis.com/security-notification-service*.

Zarządzanie podatnościami

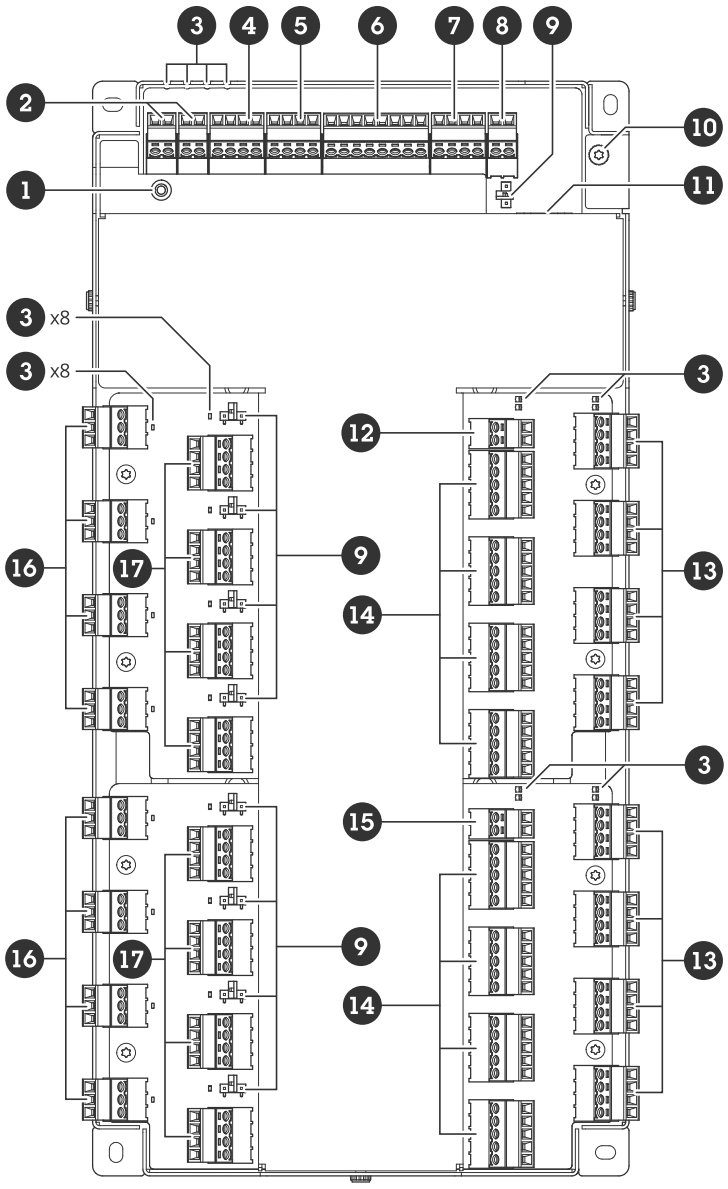
Aby maksymalnie ograniczać narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania w takich przypadkach. Aby uzyskać więcej informacji na temat zasad zarządzania lukami w zabezpieczeniach rozwiązań Axis, sposobu zgłaszania luk w zabezpieczeniach, wykrytych luk w zabezpieczeniach i odpowiednich porad dotyczących bezpieczeństwa, zob. *axis.com/vulnerability-management*.

Bezpieczne działanie urządzeń Axis

Urządzenia Axis z domyślnymi ustawieniami fabrycznymi są wstępnie skonfigurowane z zabezpieczonymi domyślnymi mechanizmami ochrony. Zalecamy korzystanie z lepiej zabezpieczonej konfiguracji podczas instalowania urządzenia. Aby dowiedzieć się więcej o podejściu Axis do cyberbezpieczeństwa, w tym o najlepszych praktykach, zasobach i wytycznych dotyczących zabezpieczania urządzeń, odwiedź stronę *axis.com/about-axis/cybersecurity*.

Specyfikacje

Przegląd produktów



1 *Przycisk kontrolny*
2 *Sabotaż/alarm*
3 *Wskaźniki LED*
4 *Złącze pomocnicze*
5 *Złącze wyjściowe*
6 *Złącze wejściowe*
7 *Złącze przekaźnikowe*
8 *Złącze zasilania (DC WEJŚCIE)*
9 *Zworka przekaźnika*
10 *Położenie uziemienia*
11 *Złącze sieciowe*
12 *Złącze zasilania (WEJŚCIE DC DRZWI 1–4)*
13 *Złącze czytnika*
14 *Złącze drzwi*
15 *Złącze zasilania (WEJŚCIE DC DRZWI 5–8)*
16 *Złącze przekaźnika AUX*
17 *Złącze przekaźnika drzwi*

Wskaźniki LED

LED	Kolor	Wskazanie
Status (STAT)	Zielony	Stałe zielone światło przy normalnym działaniu.
	Bursztynowy	Stałe światło podczas uruchamiania i odtwarzania ustawień.
	Czerwony	Powolne miganie w przypadku niepowodzenia aktualizacji.
Sieć (NET)	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.
	Wyłączona	Brak połączenia z siecią.
Zasilanie (PWR)	Zielony	Normalne działanie.
	Bursztynowy	Miga na zielono/bursztynowo podczas aktualizacji oprogramowania sprzętowego.
Przekaźnik (RELAY)	Zielony	Przekaźnik aktywny. (*)
	Wyłączona	Przekaźnik nieaktywny.

LED DRZWI 1–4 DRZWI 5–8	Kolor	Wskazanie
Status (STAT)	Zielony	Miga (włączany i wyłączany na zmianę na sekundę) w trybie offline.
	Zielony	Miga (włączony przez 200 milisekund, wyłączony przez 2 sekundy) w trybie online.
	Czerwony	Miga na zielono/czerwono podczas aktualizacji oprogramowania urządzenia.
Zasilanie (PWR)	Zielony	Normalne działanie.
RS485 nadprądowy (OC READER)	Czerwony	Usterka nadmiernego lub niedostatecznego napięcia dowolnego portu RS485.
Przekaźnik nadprądowy (OC RELAY)	Czerwony	Usterka nadmiernego lub niedostatecznego napięcia dowolnego portu przekaźnika.
Przekaźnik (RELAY)	Zielony	Przekaźnik aktywny. (*)
	Wyłączona	Przekaźnik nieaktywny.
Przekaźnik AUX (RELAY)	Zielony	Przekaźnik aktywny. (*)
	Wyłączona	Przekaźnik nieaktywny.

(*) Przekaźnik jest aktywny po podłączeniu COM do NO.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 24*.

Złącza

Złącze sieciowe

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

UL: Zasilanie Power over Ethernet (PoE) pochodzi ze źródła zasilania zgodnego z 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 prądowym zapewniającego napięcie 44 – 57 V DC i moc 15,4 W / 30 W. Zasilanie Power over Ethernet (PoE) zostało przetestowane na zgodność z przepisami UL przy pomocy modułu zasilania pośredniego AXIS 30 W Midspan.

Opcje zasilania

Aby zasilać urządzenie, należy podłączyć następujące złącza:

1. PoE lub WEJŚCIE DC. Zob. *Priorytet mocy, on page 15*.
2. WEJŚCIE DC DRZWI 1–4 (wymagane).
3. WEJŚCIE DC DRZWI 5–8 (wymagane).

Priorytet mocy

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

Złącze zasilania

Trzy 2-stykowe bloki złączy na wejście zasilania DC. Zob. *Opcje zasilania, on page 15*.



DC IN

Opcjonalnie do zasilania urządzenia. Zamiast niego można użyć PoE. Zob. *Priorytet mocy, on page 15*.

Funkcja	Pin	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

WEJŚCIE DC DRZWI 1–4

Wymagane do zasilania urządzenia.

Funkcja	Pin	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
Wejście DC	2	Wymagane do zasilania urządzenia. Uwaga: ten styk może być używany tylko jako wejście zasilania.	12 V DC, maks. 96 W

WEJŚCIE DC DRZWI 5–8

Wymagane do zasilania urządzenia.

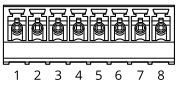
Funkcja	Pin	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
Wejście DC	2	Wymagane do zasilania urządzenia. Uwaga: ten styk może być używany tylko jako wejście zasilania.	12 V DC, maks. 96 W

UL: Zasilanie DC podawane z zasilacza zgodnego z UL 294, UL 603 lub UL 2610 w zależności od rodzaju zastosowań, o odpowiednich parametrach znamionowych.

Złącze wejściowe

Jeden 8-stykowy blok zacisków

Wejścia cyfrowe obsługują 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. Zob. *page 23*.

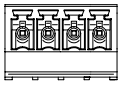


Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1, 3, 5, 7		0 V DC

Wejście	2, 4, 6	Wejście cyfrowe — podłącz do styku 1, aby aktywować, lub pozostaw rozłączone, aby dezaktywować. Możliwość nadzorowania. Zob. *Nadzorowane wejścia, on page 23*.	0–30 V DC
+12 V DC	8		Maks. 190 mA

Złącze wyjściowe

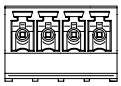
Jeden 4-stykowy blok zacisków



Funkcja	Pin	Specyfikacje
Masa DC (GND)	1	0 V DC
Wyjście	2,3,4	Otwarty dren, 0–30 V DC, maks. 100 mA

Złącze przekaźnikowe

Jeden 4-stykowy blok złączy dla przekaźników typu C, który może być używany na przykład do sterowania zamkiem lub interfejsem do bramy.



Funkcja	Pin	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.	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.	

Uwaga

Przekaźnik jest galwanicznie oddzielony 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	1900 mA	1000 mA
PoE	150 mA	50 mA
PoE+	920 mA	420 mA

POWIADOMIENIE

Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

Złącze pomocnicze

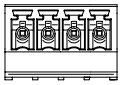
Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

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.

Wejście nadzorowane – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

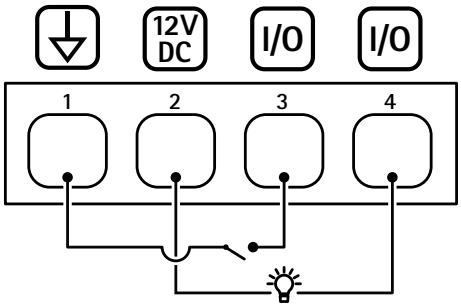
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX® lub stronę internetową produktu.

4-pinowy blok złączy



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = łącznie 250 mA
Konfigurowalne (wejście lub wyjście)	3-4	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Aby mieć możliwość korzystania z nadzorowanego wejścia, zamontuj rezystory końca linii. Patrz diagram połączeń, aby uzyskać informacje na temat podłączania rezystorów.	od 0 do maks. 30 V DC

		Wyjście cyfrowe — podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia. Każde WE/WY może przyjąć zewnętrzne obciążenie 12 V DC, 50 mA (łączna wartość maks.) jeśli użyto wewnętrznego wyjścia 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

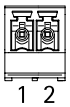


1 *Masa DC*
2 *Wyjście DC 12 V*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*

Złącze sabotażu/alarmu

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 lub pożarowy.



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
SABOTAŻ	2	Wejście cyfrowe — podłącz do styku 1, aby aktywować, lub pozostaw rozłączone, aby dezaktywować. Możliwość nadzorowania. Zob. *Nadzorowane wejścia, on page 23*.	od 0 do maks. 30 V DC



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
ALARM	2	Wejście cyfrowe — podłącz do styku 1, aby aktywować, lub pozostaw rozłączone, aby dezaktywować. Możliwość nadzorowania. Zob. *Nadzorowane wejścia, on page 23*.	od 0 do maks. 30 V DC

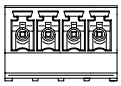
Złącze czytnika

Osiem 4-stykowych bloków zacisków obsługujących protokół OSDP do celów komunikacji z czytnikiem.

Umożliwia podłączenie do szesnastu czytników OSDP lub czytników Wiegand. 2 A przy 12 V DC jest zarezerwowane dla czytników podłączonych osobno do DRZWI 1–4 oraz DRZWI 5–8.

Uwaga

Czytniki Wiegand wymagają, aby między czytnikiem i kontrolerem było podłączone urządzenie AXIS TA1101-B Wiegand to OSDP Converter.



Konfiguracja dla jednego czytnika OSDP

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, łącznie 2 A dla wszystkich złączy czytnika.
A	3	Half duplex	
B	4	Half duplex	

Konfiguracja dla dwóch czytników OSDP („multi-drop")

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do obu czytników.	12 V DC, łącznie 2 A dla wszystkich złączy czytnika.
A	3	Half duplex	
B	4	Half duplex	

Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 200 m (656 ft) w

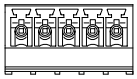
przypadku spełnienia następującego wymogu dotyczącego kabla: AWG 22–14. Zweryfikowane tylko dla czytników Axis.

- Gdy czytnik nie jest zasilany przez kontroler, dopuszczalna długość kabla dla danych czytnika wynosi do 1000 m (3280,8 ft), jeśli spełnione są następujące wymagania dotyczące kabla: 1 skrętka, AWG 26–14. Zweryfikowane tylko dla czytników Axis.

Złącze drzwi

Osiem 5-stykowych bloków złączy do urządzeń monitorujących drzwi (wejście cyfrowe).

Monitor drzwi 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. Zob. *page 23*.



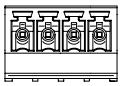
Funkcja	Pin	Uwagi	Specyfikacje
Masa DC (GND)	1, 3		0 V DC
Wejście	2, 4	Do komunikacji z monitorem drzwi. Wejście cyfrowe lub wejście nadzorowane — podłącz odpowiednio do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC
+12 V DC	5	Dostarczanie zasilania do takich urządzeń jak czujniki drzwiowe.	Łączny prąd 400 mA obejmujący wszystkie złącza drzwi

Ważne

Dopuszczalna długość kabla wynosi do 200 m (656 ft), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 24–14.

Złącze przekaźnika drzwi

Osiem 4-stykowych bloków złączy dla przekaźników typu C, które mogą być używane na przykład do sterowania zamkiem lub interfejsem do bramy.



Funkcja	Pin	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.	Maks. prąd = 4 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.	

Uwaga

Przekaźnik jest galwanicznie oddzielony 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
COM Łączna moc 46 W obejmująca wszystkie złącza przekaźników drzwiowych	Łączny prąd 3,8 A obejmujący wszystkie złącza przekaźników drzwiowych	Łączny prąd 1,5 A obejmujący wszystkie złącza przekaźników drzwiowych

POWIADOMIENIE

Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

Złącze przekaźnika AUX

Osiem 3-stykowych bloków złączy dla przekaźników typu C, które mogą być używane na przykład do sterowania zamkiem lub interfejsem do bramy.



Funkcja	Pin	Uwagi	Specyfikacje
NO	1	Normalnie otwarte. Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NO i DC.	Maks. prąd = 2 A Maks. napięcie = 30 V DC
COM	2	Wspólny	
NC	3	NC (normalnie zamknięty). Do podłączania urządzeń przekaźnikowych. Podłącz bezpieczną blokadę między masą NC i DC.	

Uwaga

Przekaźnik jest galwanicznie oddzielony od reszty obwodu, jeśli zworki nie są używane.

POWIADOMIENIE

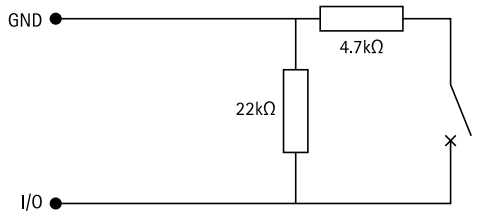
Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

Nadzorowane wejścia

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

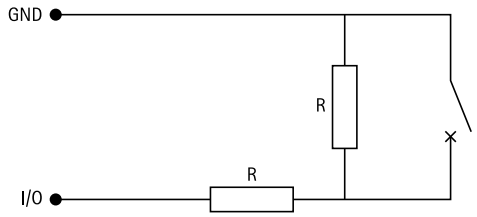
Pierwsze połączenie równoległe

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.



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 powoduje zwarcie do GND.
Przerwanie	Kabel WE/WY został przecięty i pozostawiony w stanie otwartym bez ścieżki prądu do GND.

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 13*.
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 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 produktu.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

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

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony *axis.com/support/device-software*, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.
- Pierwsze uruchomienie może potrwać kilka minut, ponieważ po aktualizacji systemu AXIS OS następuje uaktualnienie bazy danych zawierającej użytkowników, grupy, poświadczenia i inne dane. Wymagany czas zależy od ilości danych.

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.

4. Gdy produkt zostanie uruchomiony ponownie, należy wyczyścić pamięć podręczną przeglądarki internetowej.

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, przejdź na stronę poświęconą rozwiązywaniu problemów: *axis.com/support*.

Kontakt z pomocą techniczną

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

T10217726_pl

2026-09 (M7.3)

© 2024 – 2026 Axis Communications AB