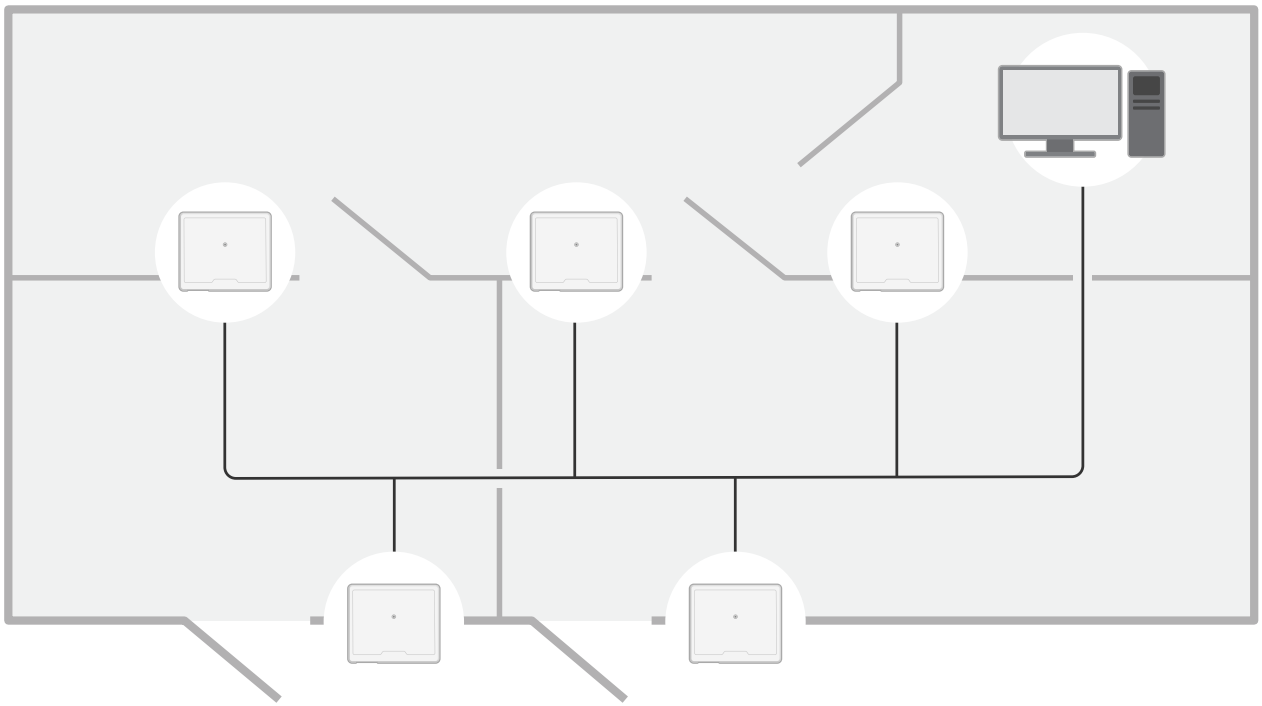
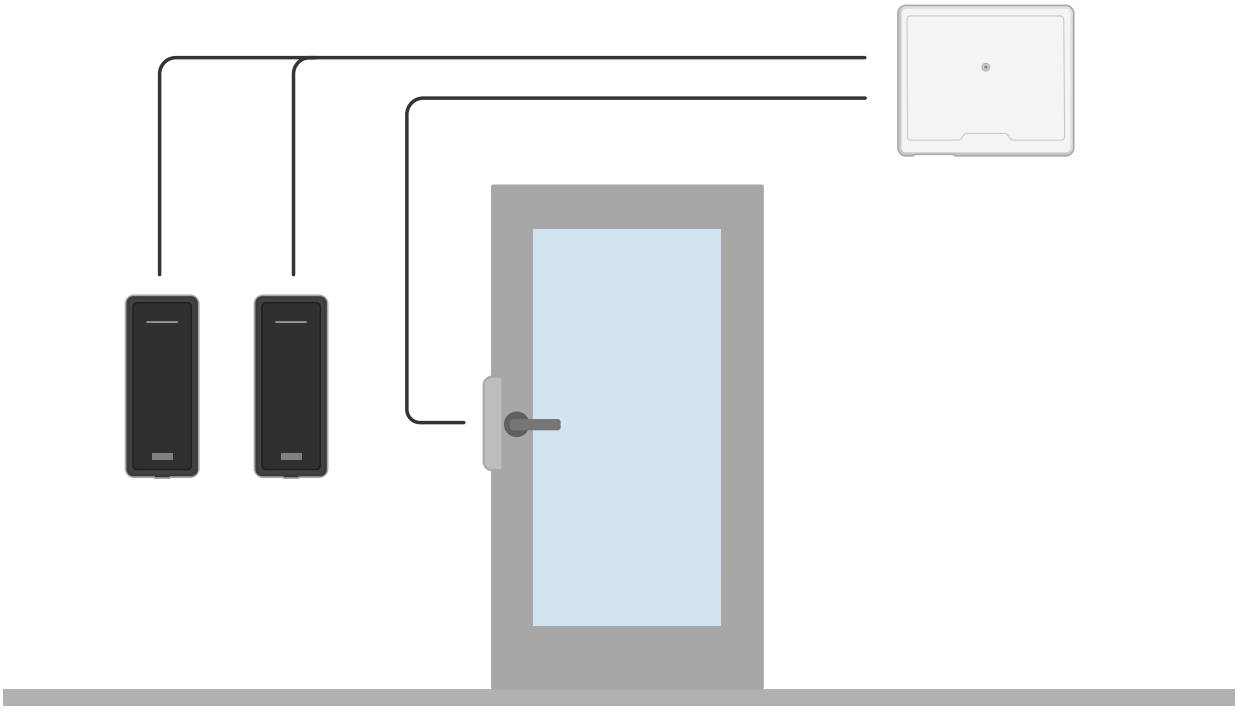
Spis treści

Informacje o rozwiązaniu 2
Instalacja 3
..... 3
Od czego zacząć 4
Wyszukiwanie urządzenia w sieci 4
Obsługiwane przeglądarki 4
Otwieranie interfejsu WWW urządzenia 4
Utwórz konto administratora 4
Bezpieczne hasła 5
Upewnianie się co do braku zmian w oprogramowaniu urządzenia 5
Omówienie interfejsu WWW 5
Konfiguracja urządzenia 6
Door override (Nadpisanie drzwi) 6
Profil LED OSDP 6
Format karty 7
Interfejs WWW 9
Dowiedz się więcej 10
Cyberbezpieczeństwo 10
Podpisany system operacyjny 10
Bezpieczne uruchamianie 10
Axis Edge Vault 10
Identyfikator urządzenia Axis 10
Specyfikacje 11
Przegląd produktów 11
..... 11
Wskaźniki LED 11
Przyciski 12
Przycisk kontrolny 12
Złącza 12
Złącze sieciowe 12
Priorytet mocy 12
Złącze czytnika 12
Złącze drzwi 14
Złącze przekaźnikowe 14
Złącze pomocnicze 15
Złącze zewnętrzne 16
Złącze zasilania 17
Nadzorowane wejścia 17
Rozwiązywanie problemów 19
Przywracanie domyślnych ustawień fabrycznych 19
Opcje systemu AXIS OS 19
Sprawdzanie bieżącej wersji systemu AXIS OS 19
Aktualizacja systemu AXIS OS: 20
Problemy techniczne i możliwe rozwiązania 20
Kontakt z pomocą techniczną 22
Cyberbezpieczeństwo 23
Zarządzanie podatnościami 23
Powiadomienia dotyczące zabezpieczeń 23
Bezpieczny cykl eksploatacji produktu 23

Informacje o rozwiązaniu



Sieciowy kontroler drzwi można łatwo podłączyć do istniejącej sieci IP i zasilać go z niej z bez konieczności prowadzenia dodatkowego okablowania.



Każdy sieciowy kontroler drzwi to inteligentne urządzenie, które można łatwo zamontować w pobliżu drzwi. Może ono zasilać i kontrolować maksymalnie dwa czytniki.

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 4*.

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 5*.
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 19*.

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 19*.
   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.

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*.

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.

Bezpieczne uruchamianie

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.

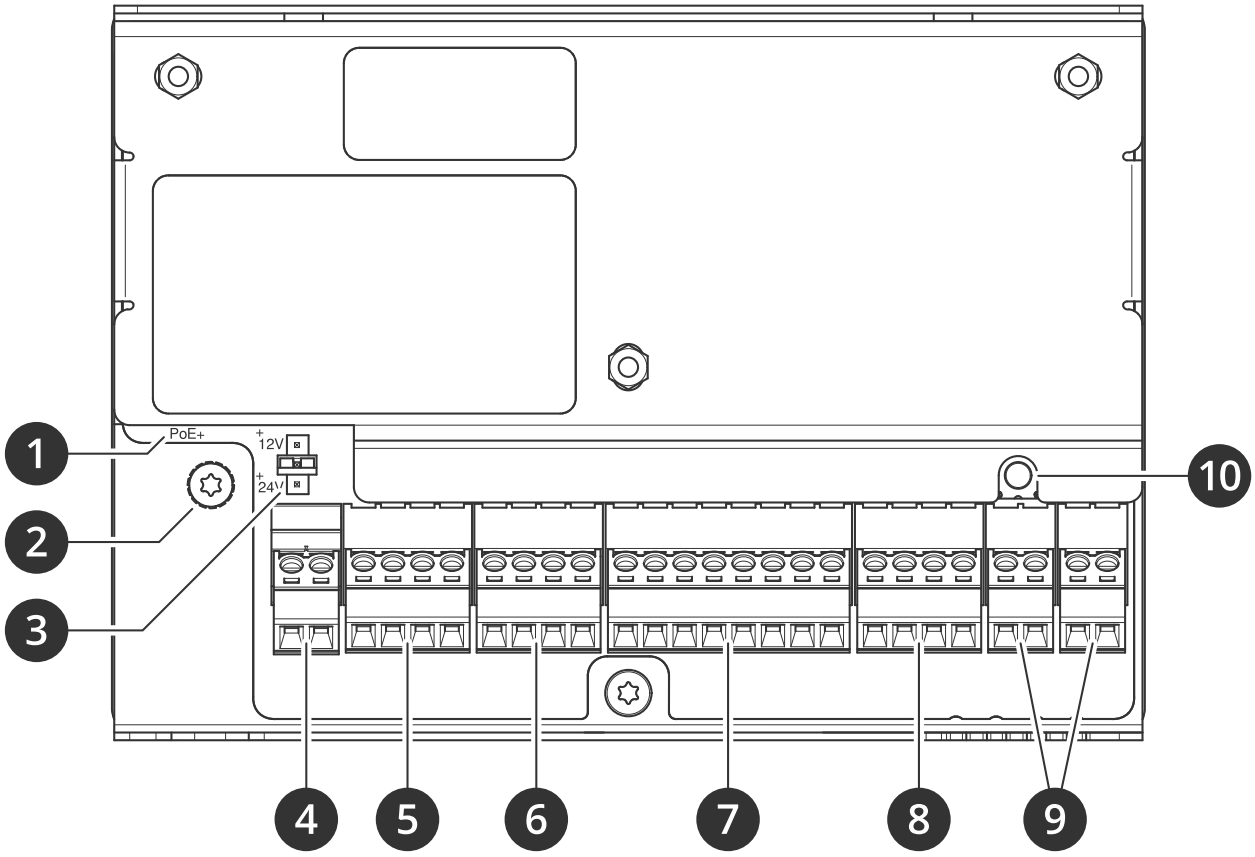
Axis Edge Vault

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.

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.

Przegląd produktów



1 *Złącze sieciowe*
2 *Położenie uziemienia*
3 *Zworka przekaźnika*
4 *Złącze zasilania*
5 *Złącze przekaźnikowe*
6 *Złącze drzwi*
7 *Złącze czytnika*
8 *Złącze pomocnicze*
9 *Złącza zewnętrzne*
10 *Przycisk kontrolny*

Wskaźniki LED

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.
	Wyłączona	Brak połączenia z siecią.

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

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 19*.

Złącza

Złącze sieciowe

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

UL: Zasilanie Power over Ethernet (PoE) powinno odbywać się przez 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 zasilania, które zapewnia 44–57 V DC, 15,4 W / 30 W. Zasilanie Power over Ethernet (PoE) zostało ocenione przez UL dla AXIS T8133 Midspan 30 W 1-port.

Priorytet mocy

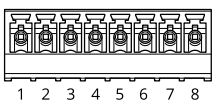
Urządzenie to może być zasilane przez wejście PoE lub DC. Zob. *Złącze sieciowe, on page 12* i *Złącze zasilania, on page 17*.

- 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 czytnika

Jeden 8-pinowy blok złączy obsługujący protokoły OSDP i Wiegand do komunikacji z czytnikiem.

Można do niego podłączyć maksymalnie dwa czytniki OSDP (multi-drop) lub jeden czytnik Wiegand. 500 mA przy 12 V DC jest zarezerwowane dla wszystkich czytników podłączonych do kontrolera drzwi.



Konfiguracja dla jednego czytnika OSDP

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

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 500 mA
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, maks. 500 mA do obu czytników łącznie
A	3	Half duplex	
B	4	Half duplex	

Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 200 m (656 stopy). 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 ekranowana, AWG 24, impedancja 120 omów. Zweryfikowane tylko dla czytników Axis.

Konfiguracja dla jednego czytnika Wiegand

Funkcja	Pin	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 500 mA
D0	3		
D1	4		
LED 1	5	Czerwony	
LED 2	6	Zielony	

SABOTAŻ	7	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
BRZĘCZYK	8	Wyjście cyfrowe – 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

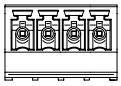
Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 150 m (500 stopy).
- Gdy czytnik nie jest zasilany przez kontroler, dopuszczalna długość kabla dla danych czytnika wynosi do 150 m (500 ft), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 22.

Złącze drzwi

Jeden 4-pinowy blok 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 17*.



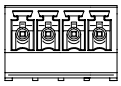
Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Wejście	2, 4	Do komunikacji z monitorem drzwi. Wejście cyfrowe lub wejście nadzorowane — podłącz odpowiednio do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Ważne

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

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. 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	1600 mA	800 mA
PoE	900 mA	450 mA

POWIADOMIENIE

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

Złącze pomocnicze

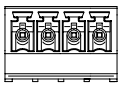
Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

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.

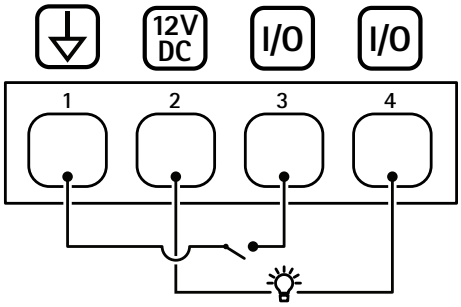
Wejście nadzorowane – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

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 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 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

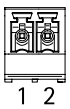


1 *Masa DC*
2 *Wyjście DC 12 V*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*

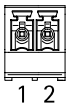
Złącze zewnętrzne

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.



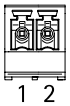
Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
SABOTAŻ	2	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC



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.	od 0 do maks. 30 V DC

Złącze zasilania

2-stykowy zespół zacisków na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤100 W lub nominalnym prądem wyjściowym ograniczonym do ≤5 A.



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

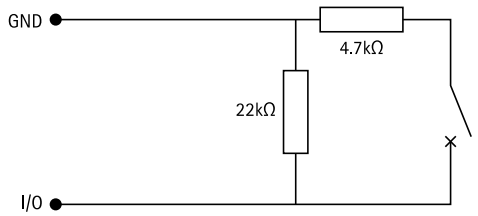
UL: zasilanie prądem stałym dostarczane z zasilaczem w standardzie UL 603, w zależności od oprogramowania, o odpowiednich parametrach.

Nadzorowane wejścia

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

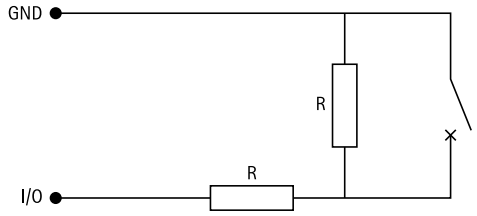
Pierwsze połączenie równoległe

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.

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 11*.
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 19*.

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 4*.

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*.

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.

T10181041_pl

2026-10 (M11.6)

© 2022 – 2026 Axis Communications AB