

## **AXIS A1610 Network Door Controller**

**Podręcznik użytkownika**

# AXIS A1610 Network Door Controller

## Spis treści

---

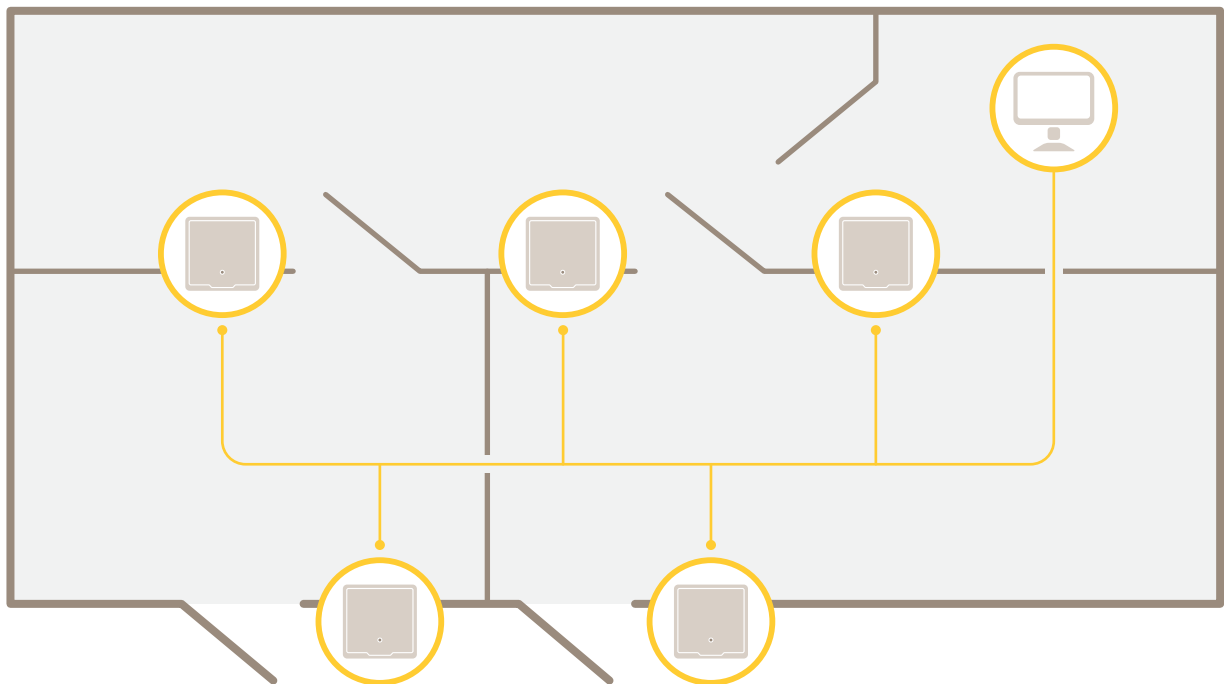
<b>Informacje o rozwiązaniu</b> .....	3
<b>Rozpoczynanie pracy</b> .....	5
Wyszukiwanie urządzenia w sieci .....	5
Otwórz interfejs WWW urządzenia .....	5
Utwórz konto administratora .....	5
Bezpieczne hasła .....	5
Sprawdzanie braku zmian w oprogramowaniu urządzenia .....	6
Omówienie interfejsu WWW .....	6
<b>Konfiguracja urządzenia</b> .....	7
<b>Interfejs WWW</b> .....	8
Stan .....	8
Kontrola dostępu .....	9
System .....	9
Konservacja .....	20
<b>Dowiedz się więcej</b> .....	22
Cyberbezpieczeństwo .....	22
<b>Specyfikacje</b> .....	23
Informacje ogólne o produkcie .....	23
Wskaźniki LED .....	23
Przyciski .....	24
Złącza .....	24
<b>Rozwiązywanie problemów</b> .....	31
Przywróć domyślne ustawienia fabryczne .....	31
Opcje systemu AXIS OS .....	31
Sprawdzanie bieżącej wersji systemu AXIS OS .....	31
Aktualizacja systemu AXIS OS: .....	31
Problemy techniczne, wskazówki i rozwiązania .....	32
Kwestie wydajności .....	33
Kontakt z pomocą techniczną .....	33

# AXIS A1610 Network Door Controller

## Informacje o rozwiązaniu

---

### Informacje o rozwiązaniu

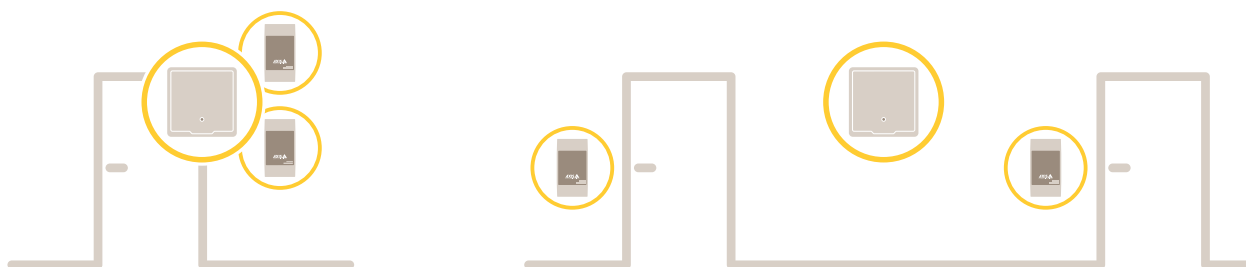


Sieciowy kontroler drzwi można łatwo podłączyć do istniejącej sieci IP i zasilać go z niej z bez konieczności prowadzenia dodatkowego okablowania.

# AXIS A1610 Network Door Controller

## Informacje o rozwiązaniu

---



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

# AXIS A1610 Network Door Controller

## Rozpoczynanie pracy

---

### Rozpoczynanie pracy

#### 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](http://axis.com/support).

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

#### Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

	Chrome™	Firefox®	Edge™	Safari®
Windows®	zalecane	zalecane	✓	
macOS®	zalecane	zalecane	✓	✓
Linux®	zalecane	zalecane	✓	
Inne systemy operacyjne	✓	✓	✓	✓*

\*Aby korzystać z interfejsu sieci Web AXIS OS w systemie iOS 15 lub iPadOS 15, przejdź do menu **Ustawienia > Safari > Zaawansowane > Funkcje eksperymentalne** i wyłącz **NSURLSession Websocket**.

Więcej informacji na temat zalecanych przeglądarek można znaleźć na stronie *AXIS OS Portal*.

#### 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 na stronie 5*.

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: *Interfejs WWW na stronie 8*.

#### Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła na stronie 5*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij **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 na stronie 31*.

# AXIS A1610 Network Door Controller

## Rozpocząwanie pracy

---

### Bezpieczne hasła

#### Ważne

Urządzenia Axis wysyłają wstępnie ustawione hasło przez sieć jako zwykły tekst. Aby chronić urządzenie po pierwszym zalogowaniu, skonfiguruj bezpieczne i szyfrowane połączenie HTTPS, a następnie zmień hasło.

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 utworzonych automatycznym generatorem haseł.
- Nieujawnianie haseł.
- Regularną zmianę haseł co najmniej raz na rok.

### Sprawdzanie 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 na stronie 31*.  
Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

### Omówienie interfejsu WWW

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



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

[help.axis.com/?&pid=81253&section=web-interface-overview](http://help.axis.com/?&pid=81253&section=web-interface-overview)

*Interfejs WWW urządzenia Axis*

# AXIS A1610 Network Door Controller

## Konfiguracja urządzenia

---

### Konfiguracja urządzenia

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


# AXIS A1610 Network Door Controller












## Interfejs WWW

### Interfejs WWW

Aby przejść do interfejsu WWW urządzenia, wpisz adres IP urządzenia w przeglądarce internetowej.

#### Uwaga

Obsługa funkcji i ustawień opisanych w tym rozdziale różni się w zależności od urządzenia. Ta ikona  wskazuje, że funkcja lub ustawienie jest dostępne tylko w niektórych urządzeniach.

-  Wyświetl/ukryj menu główne.
-  Wyświetl informacje o wersji.
-  Uzyskaj dostęp do pomocy dotyczącej produktu.
-  Zmień język.
-  Ustaw jasny lub ciemny motyw.
-    Menu użytkownika zawiera opcje:
  - Informacje o zalogowanym użytkowniku.
  -  **Change account (Zmień konto)**: Wyloguj się z bieżącego konta i zaloguj się na nowe konto.
  -  **Log out (Wyloguj)** : Wyloguj się z bieżącego konta.
-  Menu kontekstowe zawiera opcje:
  - **Analytics data (Dane analityczne)**: Zaakceptuj, aby udostępniać nie osobiste dane przeglądarki.
  - **Feedback (Opinia)**: Ta opcja pozwala wystawiać opinie, by pomagać nam w poprawianiu funkcjonalności produktów i usług.
  - **Legal (Informacje prawne)**: Wyświetl informacje o plikach cookie i licencjach.
  - **About (Informacje)**: Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.
  - **Interfejs starszego urządzenia**: Zmień interfejs WWW urządzenia na starszą wersję.

### Stan

#### Time sync status (Stan synchronizacji czasu)

Pokazuje informacje o synchronizacji z usługą NTP, w tym czy urządzenie jest zsynchronizowane z serwerem NTP oraz czas pozostały czas do następnej synchronizacji.

**NTP settings (Ustawienia NTP)**: umożliwia wyświetlenie i zaktualizowanie ustawień NTP. Ta opcja pozwala przejść do strony **Date and time (Data i godzina)**, gdzie można zmienić ustawienia usługi NTP.

#### Device info (Informacje o urządzeniu)

Tutaj znajdziesz informacje o urządzeniu, w tym wersję systemu AXIS OS i numer seryjny.



# AXIS A1610 Network Door Controller


## Interfejs WWW


**Upgrade AXIS OS (Aktualizacja AXIS OS):** umożliwia zaktualizowanie oprogramowania urządzenia. Ta opcja pozwala przejść do strony Maintenance (Konserwacja), gdzie można wykonać aktualizację.


## Kontrola dostępu

### Alarmy

**Device motion (Ruch urządzenia):** Włączenie tej opcji powoduje wyzwalanie alarmu w systemie po wykryciu ruchu urządzenia.

**Otwarcie obudowy**  : Włączenie tej opcji powoduje wyzwalanie alarmu w systemie, gdy zostanie wykryte otwarcie obudowy kontrolera drzwi. Wyłącza to ustawienie dla kontrolerów drzwi typu barebone.

**Sabotaż od zewnątrz**  : Jej włączenie spowoduje emitowanie alarmu w systemie w reakcji na wykrycie zewnętrznej próby ingerencji. Na przykład po otwarciu lub zamknięciu zewnętrznej szafki.

- **Nadzorowane wejście**  : Włączenie tej opcji spowoduje monitorowanie stanu wejścia i umożliwi skonfigurowanie rezystorów końca linii.
  - Aby używać pierwszego połączenia równoległego, wybierz opcję **Pierwsze połączenie równoległe z 22 kΩ opornikiem równoległym i 4,7 kΩ opornikiem szeregowym**.
  - Aby używać pierwszego połączenia szeregowego, select zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z listy rozwijanej **Resistor values (Wartości oporników)** wybierz wartość rezystora.

### Urządzenia peryferyjne

**Upgrade readers (Uaktualnij czytniki):** Kliknij, aby uaktualnić czytniki do nowej wersji systemu AXIS OS. Ta funkcja może aktualizować obsługiwane czytniki tylko wtedy, gdy są one w trybie online.

## System

### Czas i lokalizacja

#### Data i godzina

Format czasu zależy od ustawień językowych przeglądarki internetowej.

#### Uwaga

Zalecamy zsynchronizowanie daty i godziny urządzenia z serwerem NTP.

**Synchronization (Synchronizacja):** pozwala wybrać opcję synchronizacji daty i godziny urządzenia.

- **Automatic date and time (Automatyczna data i godzina, ręczne serwery NTS KE):** Synchronizacja z serwerami bezpiecznych kluczy NTP podłączonym do serwera DHCP.
  - **Ręczne serwery NTS KE:** Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
  - **Max NTP poll time (Maks. czas zapytania NTP):** Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP):** Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
- **Automatyczna data i godzina (serwery NTP z protokołem DHCP):** Synchronizacja z serwerami NTP podłączonymi do serwera DHCP.
  - **Zapasowe serwery NTP:** Wprowadź adres IP jednego lub dwóch serwerów zapasowych.

# AXIS A1610 Network Door Controller

## Interfejs WWW

- **Max NTP poll time (Maks. czas zapytania NTP):** Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Min NTP poll time (Min czas zapytania NTP):** Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Automatyczna data i godzina (ręczne serwery NTP):** Opcja ta umożliwia synchronizowanie z wybranymi serwerami NTP.
    - **Ręczne serwery NTP:** Opcja ta umożliwia wprowadzenie adresu IP jednego lub dwóch serwerów NTP. W przypadku używania dwóch serwerów NTP urządzenie jest zsynchronizowane i dostosowuje czas według danych wejściowych z obu serwerów.
    - **Max NTP poll time (Maks. czas zapytania NTP):** Wybierz maksymalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
    - **Min NTP poll time (Min czas zapytania NTP):** Wybierz minimalny czas oczekiwania urządzenia przed wysłaniem zapytania do serwera NTP w celu uzyskania zaktualizowanego czasu.
  - **Custom date and time (Niestandardowa data i godzina):** Ustaw datę i godzinę ręcznie. Kliknij polecenie **Get from system (Pobierz z systemu)** w celu pobrania ustawień daty i godziny z komputera lub urządzenia przenośnego.
- Time zone (Strefa czasowa):** Wybierz strefę czasową. Godzina zostanie automatycznie dostosowana względem czasu letniego i standardowego.
- **DHCP:** Stosuje strefę czasową serwera DHCP. Aby można było wybrać tę opcję, urządzenie musi być połączone z serwerem DHCP.
  - **Manual (Manualnie):** Wybierz strefę czasową z listy rozwijanej.
- Uwaga**
- System używa ustawień daty i godziny we wszystkich nagraniach, dziennikach i ustawieniach systemowych.

## Sieć

### IPv4

**Przypisz automatycznie IPv4:** wybierz, aby router sieciowy automatycznie przypisywał adres IP do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresu IP (DHCP) dla większości sieci.

**IP address (Adres IP):** wprowadź unikatowy adres IP dla urządzenia. Statyczne adresy IP można przydzielać losowo w sieciach izolowanych, pod warunkiem że adresy są unikatowe. Aby uniknąć występowania konfliktów, zalecamy kontakt z administratorem sieci przed przypisaniem statycznego adresu IP.

**Maska podsieci:** Otwórz maskę podsieci, aby określić adresy w sieci lokalnej. Wszystkie adresy poza siecią lokalną przechodzą przez router.

**Router:** wprowadź adres IP domyślnego routera (bramki) używanego do łączenia z urządzeniami należącymi do innych sieci i segmentów sieci.

**Fallback to static IP address if DHCP isn't available (Jeśli DHCP jest niedostępny, zostanie ono skierowane do statycznego adresu IP):** Wybierz, czy chcesz dodać statyczny adres IP, który ma być używany jako rezerwa, jeśli usługa DHCP jest niedostępna i nie można automatycznie przypisać adresu IP.

#### Uwaga

Jeśli protokół DHCP jest niedostępny, a urządzenie korzysta z adresu rezerwowego dla adresu statycznego, adres statyczny jest skonfigurowany w zakresie ograniczonym.

### IPv6

**Przypisz IPv6 automatycznie:** Włącz IPv6, aby router sieciowy automatycznie przypisywał adres IP do urządzenia.

### Nazwa hosta

**Przypisz automatycznie nazwę hosta:** Wybierz, aby router sieciowy automatycznie przypisywał nazwę hosta do urządzenia.

**Hostname (Nazwa hosta):** Wprowadź ręcznie nazwę hosta, aby zapewnić alternatywny dostęp do urządzenia. W raporcie serwera i dzienniku systemowym jest używana nazwa hosta. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

# AXIS A1610 Network Door Controller

## Interfejs WWW

---

### Serwery DNS

**Assign DNS automatically (Przypisz automatycznie DNS):** Wybierz ustawienie, aby serwer DHCP automatycznie przypisywał domeny wyszukiwania i adresy serwerów DNS do urządzenia. Zalecamy korzystanie z funkcji automatycznego przydzielania adresów DNS (DHCP) dla większości sieci.

**Przeszukaj domeny:** jeżeli używasz nazwy hosta, która nie jest w pełni kwalifikowana, kliknij **Add search domain (Dodaj domenę wyszukiwania)** i wprowadź domenę, w której ma być wyszukiwana nazwa hosta używana przez urządzenie.

**DNS servers (Serwery DNS):** kliknij polecenie **Add DNS server (Dodaj serwer DNS)** i wprowadź adres IP podstawowego serwera DNS. Powoduje to przełożenie nazw hostów na adresy IP w sieci.

### HTTP i HTTPS

HTTPS to protokół umożliwiający szyfrowanie żądań stron wysyłanych przez użytkowników oraz stron zwracanych przez serwer sieci Web. Zasyfrowana wymiana informacji opiera się na użyciu certyfikatu HTTPS, który gwarantuje autentyczność serwera.

Warunkiem używania protokołu HTTPS w urządzeniu jest zainstalowanie certyfikatu HTTPS. Przejdź do menu **System > Security (System > Zabezpieczenia)**, aby utworzyć i zainstalować certyfikaty.

**Allow access through (Zezwalaj na dostęp przez):** wybierz, czy użytkownik może połączyć się z urządzeniem za pośrednictwem protokołów HTTP, HTTPS lub obu.

#### Uwaga

W przypadku przeglądania zasyfrowanych stron internetowych za pośrednictwem protokołu HTTPS może wystąpić spadek wydajności, zwłaszcza przy pierwszym żądaniu strony.

**HTTP port (Port HTTP):** wprowadź wykorzystywany port HTTP. urządzenie pozwala na korzystanie z portu 80 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

**HTTPS port (Port HTTPS):** wprowadź wykorzystywany port HTTPS. urządzenie pozwala na korzystanie z portu 443 lub innego portu z zakresu 1024–65535. Jeżeli zalogujesz się jako administrator, możesz również wprowadzić dowolny port z zakresu 1–1023. Jeśli użyjesz portu z tego zakresu, otrzymasz ostrzeżenie.

**Certificate (Certyfikat):** wybierz certyfikat, aby włączyć obsługę protokołu HTTPS w tym urządzeniu.

### Protokoły wykrywania sieci

**Bonjour®:** włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

**Bonjour name (Nazwa Bonjour):** wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.

**UPnP®:** włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

**UPnP name (Nazwa UPnP):** wprowadź przyjazną nazwę, która będzie widoczna w sieci. Nazwa domyślna składa się z nazwy urządzenia i jego adresu MAC.

**WS-Discovery:** włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci.

### One-click cloud connection (Łączenie w chmurze jednym kliknięciem)

Usługa One-Click Cloud Connect (O3C) w połączeniu z systemem AVHS zapewnia łatwe i bezpieczne połączenie z internetem w celu uzyskania dostępu do obrazów wideo w czasie rzeczywistym oraz zarejestrowanych obrazów z dowolnej lokalizacji. Więcej informacji: [axis.com/end-to-end-solutions/hosted-services](http://axis.com/end-to-end-solutions/hosted-services).

# AXIS A1610 Network Door Controller

## Interfejs WWW

### Allow O3C (Zezwalaj na O3C):

- **One-click (Jednym kliknięciem):** Jest to domyślne ustawienie. Naciśnij i przytrzymaj przycisk Control na urządzeniu, aby połączyć się z usługą O3C przez Internet. Urządzenie należy zarejestrować w serwisie O3C w ciągu 24 godzin od naciśnięcia przycisku kontrolnego. W przeciwnym razie urządzenie zakończy połączenie z usługą O3C. Po zarejestrowaniu urządzenia opcja **Always (Zawsze)** jest włączona, a urządzenie zostaje połączone z usługą O3C.
- **Always (Zawsze):** Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenie zostaje połączone z usługą O3C. Opcji tej należy używać wtedy, gdy przycisk Control na urządzeniu jest niedostępny.
- **No (Nie):** wyłącza usługę O3C.

Proxy settings (Ustawienia proxy): W razie potrzeby należy wprowadzić ustawienia proxy, aby połączyć się z serwerem proxy.

Host: Wprowadź adres serwera proxy.

Port: wprowadź numer portu służącego do uzyskania dostępu.

Login i Hasło: W razie potrzeby wprowadź nazwę użytkownika i hasło do serwera proxy.

### Metoda uwierzytelniania:

- **Zwykła:** Ta metoda jest najbardziej zgodnym schematem uwierzytelniania HTTP. Jest ona mniej bezpieczna niż metoda **Digest (Szyfrowanie)**, ponieważ nazwa użytkownika i hasło są wysyłane do serwera w postaci niezaszyfrowanej.
- **Digest (Szyfrowanie):** ta metoda jest bezpieczniejsza, ponieważ zawsze przesyła hasło w sieci w formie zaszyfrowanej.
- **Auto (Automatycznie):** ta opcja umożliwia urządzeniu wybór metody uwierzytelniania w zależności od obsługiwanych metod. Priorytet ma metoda **Digest (Szyfrowanie)**; w dalszej kolejności stosowana jest metoda **Basic (Zwykła)**.

**Owner authentication key (OAK) (Klucz uwierzytelniania właściciela (OAK)):** kliknij polecenie **Get key (Pobierz klucz)**, aby pobrać klucz uwierzytelniania właściciela. Warunkiem jest podłączone urządzenia do Internetu bez użycia zapory lub serwera proxy.

## SNMP

Protokół zarządzania urządzeniami sieciowymi Simple Network Management Protocol (SNMP) umożliwia zdalne zarządzanie urządzeniami sieciowymi.

### SNMP: wybierz wersję SNMP.

- **v1 and v2c (v1 i v2c):**
  - **Read community (Społeczność odczytu):** wprowadź nazwę społeczności, która ma dostęp tylko do odczytu do wszystkich obsługiwanych obiektów SNMP. Wartość domyślna to **public (publiczna)**.
  - **Write community (Społeczność zapisu):** wprowadź nazwę społeczności, która ma dostęp do odczytu/zapisu do wszystkich obsługiwanych obiektów SNMP (poza obiektami tylko do odczytu). Wartość domyślna to **write (zapis)**.
  - **Activate traps (Uaktywnij pułapki):** włącz, aby uaktywnić raportowanie pułapek. Urządzenie wykorzystuje pułapki do wysyłania do systemu zarządzania komunikatów o ważnych zdarzeniach lub zmianach stanu. W interfejsie WWW urządzenia można skonfigurować pułapki dla SNMP v1 i v2c. Pułapki są automatycznie wyłączane w przypadku przejścia na SNMP v3 lub wyłączenia SNMP. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Trap address (Adres pułapki):** Wprowadzić adres IP lub nazwę hosta serwera zarządzania.
  - **Trap community (Społeczność pułapki):** Wprowadź nazwę społeczności używanej, gdy urządzenie wysyła komunikat pułapki do systemu zarządzającego.
  - **Traps (Pułapki):**
    - **Cold start (Zimny rozruch):** wysyła komunikat pułapkę po uruchomieniu urządzenia.
    - **Warm start (Ciepły rozruch):** wysyła komunikat pułapkę w przypadku zmiany ustawienia SNMP.
    - **Link up (Łącze w górę):** wysyła komunikat pułapkę po zmianie łącza w górę.
    - **Authentication failed (Niepowodzenie uwierzytelniania):** wysyła komunikat pułapkę po niepowodzeniu próby uwierzytelnienia.

### Uwaga

Wszystkie pułapki Axis Video MIB są włączone po włączeniu pułapek SNMP v1 i v2c. Więcej informacji: [AXIS OS Portal > SNMP](#).

- **v3:** SNMP v3 to bezpieczniejsza wersja, zapewniająca szyfrowanie i bezpieczne hasła. Aby używać SNMP v3, zalecane jest włączenie protokołu HTTPS, który posłuży do przesłania hasła. Zapobiega to również dostępowi osób

# AXIS A1610 Network Door Controller

## Interfejs WWW

nieupoważnionych do niezasyfrowanych pułapek SNMP v1 i v2c. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.

- Password for the account "initial" (Hasło do konta „wstępnego”): wprowadź hasło SNMP dla konta o nazwie „initial” (wstępne). Chociaż hasło może być wysłane bez aktywacji HTTPS, nie zalecamy tego. Hasło SNMP v3 można ustawić tylko raz i najlepiej tylko po aktywacji HTTPS. Po ustawieniu hasła pole hasła nie jest już wyświetlane. Aby zresetować hasło, należy zresetować urządzenie do ustawień fabrycznych.

### Connected clients (Podłączone klienty)

Pokazuje liczbę połączeń i połączonych klientów.

**View details (Wyświetl szczegóły):** Wyświetla i aktualizuje listę połączonych klientów. Na liście widać adres IP, protokół, port, stan i PID/proces każdego połączenia.

## Zabezpieczenia

### Certyfikaty

Certyfikaty służą do uwierzytelniania urządzeń w sieci. Urządzenie obsługuje dwa typy certyfikatów:

- **Certyfikaty serwera/klienta**  
Certyfikat serwera/klienta potwierdza numer urządzenia i może mieć własny podpis lub podpis jednostki certyfikującej (CA). Certyfikaty z własnym podpisem oferują ograniczoną ochronę i można je wykorzystywać do momentu uzyskania certyfikatu CA.
- **Certyfikaty CA**  
Certyfikaty CA mogą służyć do uwierzytelniania innych certyfikatów, na przykład tożsamości serwera uwierzytelniającego w przypadku połączenia urządzenia z siecią zabezpieczoną za pomocą IEEE 802.1X. Urządzenie ma kilka zainstalowanych wstępnie certyfikatów CA.

Obsługiwane są następujące formaty:


- Formaty certyfikatów: .PEM, .CER i .PFX
- Formaty kluczy prywatnych: PKCS#1 i PKCS#12

#### Ważne

W przypadku przywrócenia na urządzeniu ustawień fabrycznych wszystkie certyfikaty są usuwane. Wstępnie zainstalowane certyfikaty CA są instalowane ponownie.




**Add certificate (Dodaj certyfikat):** Kliknij, aby dodać certyfikat.

- **More... (Więcej...)**  : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy):** Wybierz tę opcję, aby używać funkcji **Secure element (Zabezpieczony element)** lub **Trusted Platform Module 2.0 (Moduł TPM 2.0)** do bezpiecznego przechowywania klucza prywatnego. Aby uzyskać więcej informacji na temat bezpiecznego magazynu kluczy, odwiedź stronę [help.axis.com/en-us/axis-os#cryptographic-support](http://help.axis.com/en-us/axis-os#cryptographic-support).
- **Key type (Typ klucza):** Aby zabezpieczyć certyfikat, wybierz domyślny algorytm szyfrowania lub inny z listy rozwijanej.



Menu kontekstowe zawiera opcje:

- **Certificate information (Dane certyfikatu):** Wyświetl właściwości zainstalowanego certyfikatu.
- **Delete certificate (Usuń certyfikat):** Umożliwia usunięcie certyfikatu.
- **Create certificate signing request (Utwórz żądanie podpisania certyfikatu):** Umożliwia utworzenie żądanie podpisania certyfikatu w celu przekazania go do urzędu rejestrycyjnego i złożenia wniosku o wydanie certyfikatu tożsamości cyfrowej.

**Bezpieczny magazyn kluczy**  :

- **Bezpieczny element (CC EAL6+):** Wybierz, aby używać bezpiecznego elementu do bezpiecznego magazynu kluczy.
- **Moduł TPM 2.0 (CC EAL4+, FIPS 140-2 poziom 2):** Wybierz, aby używać modułu TPM 2.0 do bezpiecznego magazynu kluczy.

# AXIS A1610 Network Door Controller

## Interfejs WWW

---

### IEEE 802.1x oraz IEEE 802.1AE MACsec

IEEE 802.1x to standard IEEE dla kontroli dostępu sieciowego opartej na portach, zapewniający bezpieczne uwierzytelnianie przewodowych i bezprzewodowych urządzeń sieciowych. IEEE 802.1x jest oparty na protokole EAP (Extensible Authentication Protocol).

Aby uzyskać dostęp do sieci zabezpieczonej IEEE 802.1x, urządzenia sieciowe muszą dokonać uwierzytelnienia. Do uwierzytelnienia służy serwer, zazwyczaj RADIUS, taki jak FreeRADIUS i Microsoft Internet Authentication Server.

#### Certyfikaty

W przypadku konfiguracji bez certyfikatu CA, sprawdzanie poprawności certyfikatów serwera jest wyłączone, a urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.

Podczas korzystania z certyfikatu w instalacjach firmy Axis urządzenie i serwer uwierzytelniający używają do uwierzytelniania certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security).

Aby zezwolić urządzeniu na dostęp do sieci chronionej za pomocą certyfikatów, w urządzeniu musi być zainstalowany podpisany certyfikat klienta.

**Authentication method (Metoda uwierzytelniania):** Wybierz typ protokołu EAP na potrzeby uwierzytelniania. Domyślnie jest to EAP-TLS. Bezpieczniejszą opcją jest EAP-PEAP/MSCHAPv2.

**Client certificate (Certyfikat klienta):** wybierz certyfikat klienta, aby użyć IEEE 802.1x. Serwer uwierzytelniania używa certyfikatu do weryfikacji tożsamości klienta.

**CA certificate (Certyfikat CA):** wybierz certyfikaty CA w celu potwierdzenia tożsamości serwera uwierzytelniającego. Jeśli nie wybrano żadnego certyfikatu, urządzenie próbuje uwierzytelnić się niezależnie od tego, do jakiej sieci jest podłączone.

**EAP identity (Tożsamość EAP):** wprowadź tożsamość użytkownika powiązaną z certyfikatem klienta.

**EAPOL version (Wersja protokołu EAPOL):** wybierz wersję EAPOL używaną w switchu sieciowym.

**Use IEEE 802.1x (Użyj IEEE 802.1x):** wybierz, aby użyć protokołu IEEE 802.1 x.

#### IEEE 802.1AE MACsec

IEEE 802.1AE MACsec jest standardem IEEE dotyczącym adresu MAC, który definiuje bezpołączeniową poufność i integralność danych dla protokołów niezależnych od dostępu do nośników.

Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą EAP-TLS:

#### Tryb

- **Dynamic CAK / EAP-TLS (Dynamiczne CAK/EAP-TLS):** Opcja domyślna. Po nawiązaniu zabezpieczonego połączenia urządzenie będzie sprawdzać dostępność adresów MAC w sieci.
- **Static CAK / pre-shared key (PSK) (Statyczny CAK/PSK):** Ta opcja pozwala ustawić nazwę i wartość klucza niezbędną do połączenia z siecią.

Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą EAP-PEAP/MSCHAPv2:

- **Password (Hasło):** Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap):** wybierz wersję Peap używaną w switchu sieciowym.
- **Label (Etykieta):** 1 pozwala używać szyfrowania EAP klienta; 2 pozwala używać szyfrowania PEAP klienta. Wybierz etykietę używaną przez przełącznik sieciowy podczas korzystania z wersji 1 protokołu Peap.

Prevent brute-force attacks (Zapobiegaj atakom typu brute force)

# AXIS A1610 Network Door Controller

## Interfejs WWW

**Blocking (Blokowanie):** włącz, aby blokować ataki typu brute force. Ataki typu brute-force wykorzystują metodę prób i błędów do odgadnięcia danych logowania lub kluczy szyfrowania.

**Blocking period (Okres blokowania):** Wprowadź liczbę sekund, w ciągu których ataki typu brute-force mają być blokowane.

**Blocking conditions (Warunki blokowania):** wprowadź dopuszczalną liczbę nieudanych prób uwierzytelnienia na sekundę przed rozpoczęciem blokowania. Liczbę dopuszczalnych niepowodzeń można ustawić zarówno na stronie, jak i w urządzeniu.

### Firewall (Zapora)

**Activate (Aktywuj):** Włącz zaporę sieciową.

**Domyślne ustawienia zasad:** Wybierz stan domyślny zapory.

- **Allow: (Zezwalaj)** Zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **Deny: (Odrzuć)** Odrzuca wszystkie połączenia z urządzeniem.

Aby wprowadzić wyjątki od domyślnych zasad, można utworzyć reguły, które zezwalają lub nie zezwalają na łączenie się z urządzeniem z określonych adresów, protokołów i portów.

- **Address (Adres):** Wprowadź adres w formacie IPv4/IPv6 lub CIDR, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Protocol (Protokół):** Wybierz protokół, w przypadku którego dostęp ma być dozwolony lub niedozwolony.
- **Port:** Wprowadź numer portu, w przypadku którego dostęp ma być dozwolony lub niedozwolony. Podaj numer portu od 1 do 65535.
- **Policy (Zasada):** Wybierz zasadę dla reguły.



: Kliknij, aby utworzyć nową regułę.

**Add rules: (Dodaj reguły)** Kliknij tę opcję, aby dodać zdefiniowane reguły.

- **Time in seconds: (Czas w sekundach)** Pozwala ustawić limit czasu testowania reguł. Domyślny limit czasu to 300 s. Jeśli chcesz od razu aktywować reguły, ustaw czas jako 0 s.
- **Confirm rules: (Potwierdzenie reguł)** Potwierdź reguły i ich limit czasowy. W przypadku ustawienia limitu czasu dłuższego niż 1 sekunda reguły będą aktywne przez ten czas. Jeśli czas zostanie ustawiony jako 0, reguły będą od razu aktywne.

**Pending rules (Oczekujące reguły):** Omówienie ostatnio testowanych reguł, które jeszcze nie zostały potwierdzone.

#### Uwaga

Reguły mające ograniczenie czasowe są widoczne zarówno w menu **Pending rules (Oczekujące reguły)**, jak i **Active rules (Aktywne reguły)**, aż upłynie czas, który został dla nich ustawiony lub zostaną potwierdzone. Jeśli reguły nie zostaną potwierdzone, będą widoczne tylko w menu **Pending rules (Oczekujące reguły)** i zostaną przywrócone wcześniejsze ustawienia zapory. Jeśli reguły zostaną potwierdzone, zastąpią one bieżące aktywne reguły.

**Confirm rules (Potwierdzenie reguł):** Kliknięcie tej opcji aktywuje oczekujące reguły.

**Active rules (Aktywne reguły):** Omówienie reguł obecnie stosowanych w urządzeniu.



: Kliknięcie tej opcji pozwala usunąć aktywną regułę.



: Kliknięcie tej opcji pozwala usunąć wszystkie oczekujące i aktywne reguły.

Niestandardowy podpisany certyfikat systemu AXIS OS



# AXIS A1610 Network Door Controller

## Interfejs WWW

Do zainstalowania w urządzeniu oprogramowania testowego lub innego niestandardowego oprogramowania Axis konieczny jest niestandardowy podpisany certyfikat systemu AXIS OS. Certyfikat służy do sprawdzenia, czy oprogramowanie jest zatwierdzone zarówno przez właściciela urządzenia, jak i przez firmę Axis. Oprogramowanie działa tylko na określonym urządzeniu z niepowtarzalnym numerem seryjnym i identyfikatorem procesora. Niestandardowe podpisane certyfikaty systemu AXIS OS mogą być tworzone tylko przez firmę Axis, ponieważ Axis posiada klucze do ich podpisywania.

**Zainstaluj:** Kliknij przycisk Install (Instaluj), aby zainstalować certyfikat. Certyfikat musi zostać zainstalowany przed zainstalowaniem oprogramowania.



Menu kontekstowe zawiera opcje:

- **Delete certificate (Usuń certyfikat):** Umożliwia usunięcie certyfikatu.

## Konta

### Accounts (Konta)



**Add account (Dodaj konto):** Kliknij, aby dodać nowe konto. Można dodać do 100 kont.

**Account (Konto):** Wprowadź niepowtarzalną nazwę konta.

**New password (Nowe hasło):** wprowadzić hasło do konta. Hasło musi mieć 1–64 znaki. Dozwolone są tylko możliwe do wydrukowania znaki ASCII (kod od 32 do 126), na przykład litery, cyfry, znaki interpunkcyjne i niektóre symbole.

**Repeat password (Powtórz hasło):** Wprowadź ponownie to samo hasło.

**Privileges (Przywileje):**

- **Administrator:** Ma nieograniczony dostęp do wszystkich ustawień. Administrator może też dodawać, aktualizować i usuwać inne konta.
- **Operator:** Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
  - Dodawanie aplikacji.
- **Viewer (Dozorca):** Nie może zmieniać ustawień.



Menu kontekstowe zawiera opcje:

**Update account (Zaktualizuj konto):** Pozwala edytować właściwości konta.

**Delete account (Usuń konto):** Pozwala usunąć konto. Nie można usunąć konta root.

## MQTT

MQTT (przesyłanie telemetryczne usługi kolejowania wiadomości) to standardowy protokół do obsługi komunikacji w Internecie rzeczy (IoT). Został on zaprojektowany z myślą o uproszczeniu integracji IoT i jest wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji kodu i przepustowości. Klient MQTT w oprogramowaniu urządzeń Axis może ułatwiać integrację danych i zdarzeń generowanych w urządzeniu z systemami, które nie są oprogramowaniem do zarządzania materiałem wizyjnym (VMS).

Konfiguracja urządzenia jako klienta MQTT. Komunikacja MQTT oparta jest na dwóch jednostkach, klientach i brokerze. Klienci mogą wysyłać i odbierać wiadomości. Broker odpowiedzialny jest za rozsyłanie wiadomości między klientami.

Więcej informacji o protokole MQTT znajdziesz w *portalu poświęconym systemowi AXIS OS*.

## ALPN



# AXIS A1610 Network Door Controller

## Interfejs WWW

ALPN to rozszerzenie TLS/SSL umożliwiające wybranie protokołu aplikacji na etapie uzgadniania połączenia między klientem a serwerem. Służy do włączania ruchu MQTT przez port używany przez inne protokoły, takie jak HTTP. Czasami może nie być dedykowanego portu otwartego dla komunikacji MQTT. W takich przypadkach pomocne może być korzystanie z ALPN do negocjowania użycia MQTT jako protokołu aplikacji na standardowym porcie akceptowanym przez zapory sieciowe.

### MQTT client (Klient MQTT)

**Connect (Połącz):** włącz lub wyłącz klienta MQTT.

**Status (Stan):** pokazuje bieżący status klienta MQTT.

**Broker**

**Host:** wprowadź nazwę hosta lub adres IP serwera MQTT.

**Protocol (Protokół):** wybór protokołu, który ma być używany.

**Port:** wprowadź numer portu.

- 1883 to wartość domyślna dla MQTT przez TCP
- 8883 to wartość domyślna dla MQTT przez SSL
- 80 to wartość domyślna dla MQTT przez WebSocket
- 443 to wartość domyślna dla MQTT przez WebSocket Secure

**ALPN protocol (Protokół ALPN):** Wprowadź nazwę protokołu ALPN dostarczoną przez dostawcę brokera MQTT. Dotyczy to tylko ustawień MQTT przez SSL i MQTT przez WebSocket Secure.

**Username (Nazwa użytkownika):** należy tu wprowadzić nazwę użytkownika, która będzie umożliwiać klientowi dostęp do serwera.

**Password (Hasło):** wprowadzić hasło dla nazwy użytkownika.

**Client ID (Identyfikator klienta):** wprowadź identyfikator klienta. Identyfikator klienta jest wysyłany do serwera w momencie połączenia klienta.

**Clean session (Czysta sesja):** steruje zachowaniem w czasie połączenia i czasie rozłączenia. Po wybraniu tej opcji informacje o stanie są odrzucane podczas podłączania i rozłączania.

**HTTP proxy (Serwer proxy HTTP):** Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTP, możesz zostawić to pole puste.

**HTTPS proxy (Serwer proxy HTTPS):** Adres URL o maksymalnej długości 255 bajtów. Jeśli nie chcesz używać serwera proxy HTTPS, możesz zostawić to pole puste.

**Keep alive interval (Przedział czasowy KeepAlive):** Umożliwia klientowi detekcję, kiedy serwer przestaje być dostępny, bez konieczności oczekiwania na długi limit czasu TCP/IP.

**Timeout (Przekroczenie limitu czasu):** interwał czasowy (w sekundach) pozwalający na zakończenie połączenia. Wartość domyślna: 60

**Prefiks tematu urządzenia:** Używany w domyślnych wartościach tematu w komunikacie łączenia i komunikacie LWT na karcie MQTT client (Klient MQTT) oraz w warunkach publikowania na karcie MQTT publication (Publikacja MQTT).

**Reconnect automatically (Ponowne połączenie automatyczne):** określa, czy klient powinien ponownie połączyć się automatycznie po rozłączeniu.

### Connect message (Komunikat łączenia)

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

**Send message (Wysłanie wiadomości):** włącz, aby wysłać wiadomości.

**Use default (Użyj domyślnych):** wyłącz, aby wprowadzić własną wiadomość domyślną.

**Topic (Temat):** wprowadź temat wiadomości domyślnej.

# AXIS A1610 Network Door Controller

## Interfejs WWW

---

**Payload (Próbka):** wprowadź treść wiadomości domyślnej.

**Retain (Zachowaj):** wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

**QoS:** zmiana warstwy QoS dla przepływu pakietów.

**Last Will and Testament message (Wiadomość Ostatnia Wola i Testament)**

Funkcja Last Will Testament (LWT) zapewnia klientowi dostarczenie informacji wraz z poświadczeniami w momencie łączenia się z brokerem. Jeżeli klient nie rozłączy się w pewnym momencie w późniejszym terminie (może to być spowodowane brakiem źródła zasilania), może umożliwić brokerowi dostarczenie komunikatów do innych klientów. Ten komunikat LWT ma taką samą postać jak zwykła wiadomość i jest kierowany przez tę samą mechanikę.

**Send message (Wysłanie wiadomości):** włącz, aby wysłać wiadomości.

**Use default (Użyj domyślnych):** wyłącz, aby wprowadzić własną wiadomość domyślną.

**Topic (Temat):** wprowadź temat wiadomości domyślnej.

**Payload (Próbka):** wprowadź treść wiadomości domyślnej.

**Retain (Zachowaj):** wybierz, aby zachować stan klienta w tym **Topic (Temacie)**

**QoS:** zmiana warstwy QoS dla przepływu pakietów.

### MQTT publication (Publikacja MQTT)

**Użyj domyślnego prefiksu:** Wybierz ustawienie, aby używać domyślnego prefiksu zdefiniowanego za pomocą prefiksu urządzenia w zakładce MQTT client (Klient MQTT).

**Dołącz nazwę tematu:** Wybierz, aby do tematu MQTT dołączać tematy opisujące warunek.

**Dołącz nazwy przestrzenne tematu:** Wybierz, aby do tematu MQTT dołączać przestrzenie nazw tematów ONVIF.

**Include serial number (Uwzględnij numer seryjny):** Wybierz, aby w danych właściwych usługi MQTT umieszczać numer seryjny urządzenia.

**+ Add condition (Dodaj warunek):** Kliknij, aby dodać warunek.

**Retain (Zachowaj):** Definiuje, które komunikaty MQTT mają być wysyłane jako zachowywane.

- **None (Brak):** Wysyłanie wszystkich komunikatów jako niezachowywanych.
- **Property (Właściwość):** Wysyłanie tylko komunikatów ze stanem jako zachowywanych.
- **All (Wszystkie):** Wysyłanie komunikatów ze stanem i bez stanu jako zachowywanych.

**QoS:** Wybierz żądany poziom publikacji MQTT.

### MQTT subscriptions (Subskrypcje MQTT)

**+ Add subscription (Dodaj subskrypcję):** Kliknij, aby dodać nową subskrypcję usługi MQTT.

**Subscription filter (Filtr subskrypcyjny):** Wprowadź temat MQTT, który chcesz subskrybować.

**Use device topic prefix (Użyj prefiksu tematu urządzenia):** Dodaj filtr subskrypcji jako prefiks do tematu MQTT.

**Subscription type (Typ subskrypcji):**

- **Stateless (Bez stanu):** Wybierz, aby przekształcać komunikaty MQTT na komunikaty bezstanowe.
- **Stateful (Ze stanem):** Wybierz, aby przekształcać komunikaty MQTT na warunek. Dane właściwe będą służyły do określania stanu.

**QoS:** Wybierz żądany poziom subskrypcji MQTT.

# AXIS A1610 Network Door Controller

## Interfejs WWW

### Akcesoria



#### I/O ports (Porty I/O)



Użyj wejścia cyfrowego do podłączenia zewnętrznych urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okien lub drzwi oraz czujników wykrywania zbitcia szyby.

Użyj wyjścia cyfrowego do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączone urządzenia można aktywować poprzez interfejs programowania aplikacji VAPIX® lub w interfejsie WWW.

#### Port

**Name (Nazwa):** edytuj tekst, aby zmienić nazwę portu.


**Direction (Kierunek):**  wskazuje, że port jest portem wejścia.  wskazuje, że jest to port wyjścia. Jeśli port jest konfigurowalny, można kliknąć ikony, aby przełączać się między wejściem a wyjściem.

**Normal state (Stan normalny):** Kliknij opcję  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.

**Current state (Bieżący stan):** wyświetla bieżący stan portu. Wejście lub wyjście jest aktywowane w momencie zmiany bieżącego stanu na inny niż stan normalny. Obwód wejścia urządzenia jest otwarty po odłączeniu lub doprowadzeniu napięcia powyżej 1 V DC.

#### Uwaga

Podczas ponownego uruchomienia obwód pozostaje otwarty. Po ponownym uruchomieniu obwód powraca do pozycji normalnej. Po zmianie ustawień na tej stronie obwody wyjść powracają do normalnych pozycji, niezależnie od aktywnych wyzwalaczy.

**Supervised (Nadzorowane)**  : włącz, aby umożliwić wykrywanie i wyzwalanie działań, jeśli ktoś manipuluje przy połączeniu z cyfrowymi urządzeniami We/Wy. Oprócz wykrywania, czy wejście jest otwarte lub zamknięte, można również wykryć, czy ktoś przy nim manipulował (tzn. przeciął lub doprowadził do zwarcia). Nadzorowanie połączenia wymaga dodatkowego sprzętu (rezystorów końcowych) w zewnętrznej pętli We./Wy.

### Dzienniki

#### Raporty i dzienniki

#### Reports (Raporty)

- **View the device server report (Wyświetl raport serwera o urządzeniu):** Opcja ta pozwala wyświetlić informacje o stanie produktu w wyskakującym oknie. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.
- **Download the device server report (Pobierz raport serwera o urządzeniu):** Opcja ta powoduje utworzenie pliku ZIP, który zawiera pełny raport serwera w pliku tekstowym w formacie UTF-8 oraz migawkę bieżącego podglądu na żywo. Podczas kontaktowania się z pomocą techniczną zawsze dodawaj plik zip raportu serwera.
- **Pobierz raport o awarii:** Pobierz archiwum ze szczegółowymi informacjami o stanie serwera. Raport o awarii zawiera informacje znajdujące się w raporcie o serwerze oraz szczegółowe dane pomocne w usuwaniu błędów. W raporcie tym mogą się znajdować informacje poufne, np. ślady sieciowe. Wygenerowanie raportu może potrwać kilka minut.

#### Dzienniki

- **View the system log (Wyświetl dziennik systemu):** Kliknij tutaj, aby wyświetlić informacje o zdarzeniach systemowych, takich jak uruchamianie urządzenia, ostrzeżenia i komunikaty krytyczne.
- **View the access log (Wyświetl dziennik dostępu):** Kliknij tutaj, by wyświetlić wszystkie nieudane próby uzyskania dostępu do urządzenia, na przykład gdy użyto nieprawidłowego hasła logowania.

#### Ślad sieciowy

# AXIS A1610 Network Door Controller

## Interfejs WWW

---

### Ważne

Plik śladu sieciowego może zawierać dane poufne, takie jak certyfikaty lub hasła.

Plik śladu sieciowego, rejestrujący aktywność w sieci, może pomóc w rozwiązywaniu problemów.

**Trace time (Czas śledzenia):** Wybierz czas trwania śledzenia w sekundach lub minutach i kliknij przycisk **Download (Pobierz)**.

### Zdalny dziennik systemu

Dziennik systemowy to standard rejestracji komunikatów. Umożliwia on oddzielenie oprogramowania, które generuje komunikaty, systemu przechowującego je i oprogramowania, które je raportuje i analizuje. Każdy komunikat jest oznaczony etykietą z kodem obiektu wskazującym typ oprogramowania, które wygenerowało komunikat, oraz przypisany poziom ważności.



**Server (Serwer):** Kliknij, aby dodać nowy serwer.

**Host:** Wprowadź nazwę hosta lub adres IP serwera.

**Format (Formatuj):** Wybierz format komunikatu dziennika systemowego, który ma być używany.

- Axis
- RFC 3164
- RFC 5424

**Protocol (Protokół):** Wybierz protokołu, który ma być używany:

- UDP (port domyślny to 514)
- TCP (port domyślny to 601)
- TLS (port domyślny to 6514)

**Port:** Wpisywanie innego numeru portu w miejsce obecnego.

**Severity (Ciężkość):** Zdecyduj, które komunikaty będą wysyłane po wyzwoleniu.

**CA certificate set (Certyfikat CA ustawiony):** Umożliwia wyświetlenie aktualnych ustawień lub dodanie certyfikatu.

## Konserwacja

**Restart (Uruchom ponownie):** Uruchom ponownie urządzenie. Nie wpłynie to na żadne bieżące ustawienia. Uruchomione aplikacje zostaną ponownie uruchomione automatycznie.

**Restore (Przywróć):** Opcja ta umożliwia przywrócenie *większości* domyślnych ustawień fabrycznych. Następnie konieczne jest ponowne skonfigurowanie urządzeń i aplikacji, zainstalowanie aplikacji, które nie zostały wstępnie zainstalowane, a także ponowne utworzenie wszystkich zdarzeń i wstępnych ustawień.

### Ważne

Operacja przywrócenia spowoduje, że będą zapisane tylko następujące ustawienia:

- protokół uruchamiania (DHCP lub stały adres),
- Statyczny adres IP
- Router domyślny
- Maska podsieci
- Ustawienia 802.1X
- Ustawienia O3C
- Adres IP serwera DNS

# AXIS A1610 Network Door Controller

## Interfejs WWW

---

**Factory default (Ustawienia fabryczne):** Przywróć *wszystkie* ustawienia do domyślnych wartości fabrycznych. Po zakończeniu tej operacji konieczne będzie zresetowanie adresu IP w celu uzyskania dostępu do urządzenia.

### Uwaga

Wszystkie składniki oprogramowania urządzenia firmy Axis posiadają podpisy cyfrowe zapewniające, że na urządzeniu będzie instalowane wyłącznie zweryfikowane oprogramowanie. To dodatkowo zwiększa minimalny ogólny poziom cyberbezpieczeństwa urządzeń Axis. Więcej informacji znajduje się w oficjalnym dokumencie „Axis Edge Vault” dostępnym na [axis.com](http://axis.com).

**Uaktualnianie systemu AXIS OS:** Umożliwia uaktualnienie do nowej wersji AXIS OS. Nowe wersje mogą zawierać udoskonalenia działania i poprawki błędów oraz zupełnie nowe funkcje. Zalecamy, aby zawsze korzystać z najnowszej wersji systemu AXIS OS. Aby pobrać najnowszą wersję, odwiedź stronę [axis.com/support](http://axis.com/support).

Po uaktualnieniu masz do wyboru trzy opcje:

- **Standard upgrade (Aktualizacja standardowa):** Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **Factory default (Ustawienia fabryczne):** Umożliwia uaktualnienie i przywrócenie ustawień do domyślnych wartości fabrycznych. Jeżeli wybierzesz tę opcję, po uaktualnieniu nie będzie możliwości przywrócenia poprzedniej wersji systemu AXIS OS.
- **Autorollback (Automatyczne przywrócenie wersji):** Uaktualnij i potwierdź uaktualnienie w ustawionym czasie. Jeżeli nie potwierdzisz, w urządzeniu zostanie przywrócona poprzednia wersja systemu AXIS OS.

**Przywracanie systemu AXIS OS:** Przywróć poprzednio zainstalowaną wersję systemu AXIS OS.

# AXIS A1610 Network Door Controller

## Dowiedz się więcej

---

### Dowiedz się więcej

## Cyberbezpieczeństwo

### 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

Bezpieczne uruchamianie 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.

### Moduł Axis Edge

Urządzenie może być chronione przez sprzętową platformę cyberbezpieczeństwa Axis Edge Vault. Zawiera funkcje gwarantujące tożsamość i integralność urządzenia oraz ochronę poufnych informacji przed nieuprawnionym dostępem. Jest ona oparta na silnej podstawie kryptograficznych modułów obliczeniowych (bezpiecznych elementów i modułów TPM) i zabezpieczeniu SoC (TEE i Secure Boot) w połączeniu z fachową wiedzą o bezpieczeństwie urządzeń brzegowych.

### ID urządzenia Axis

Możliwość zidentyfikowania urządzenia ma kluczowe znaczenie dla ustalenia relacji zaufania w tożsamości urządzenia. Podczas produkcji urządzenia z Axis Edge Vault otrzymują unikalny, fabrycznie przydzielony i zgodny ze standardem IEEE 802.1AR certyfikat ID urządzenia Axis. Ten certyfikat to swego rodzaju paszport poświadczający pochodzenie urządzenia. ID urządzenia jest trwale zapisany w bezpiecznym magazynie kluczy jako certyfikat z podpisem certyfikatu głównego Axis. ID urządzenia może być wykorzystywany przez infrastrukturę IT klienta do zautomatyzowanego bezpiecznego wdrażania urządzeń i bezpiecznej identyfikacji urządzeń.

Aby dowiedzieć się więcej o funkcjach cyberbezpieczeństwa stosowanych w urządzeniach Axis, przejdź do strony [axis.com/learning/white-papers](https://axis.com/learning/white-papers) i poszukaj według hasła „cybersecurity”.

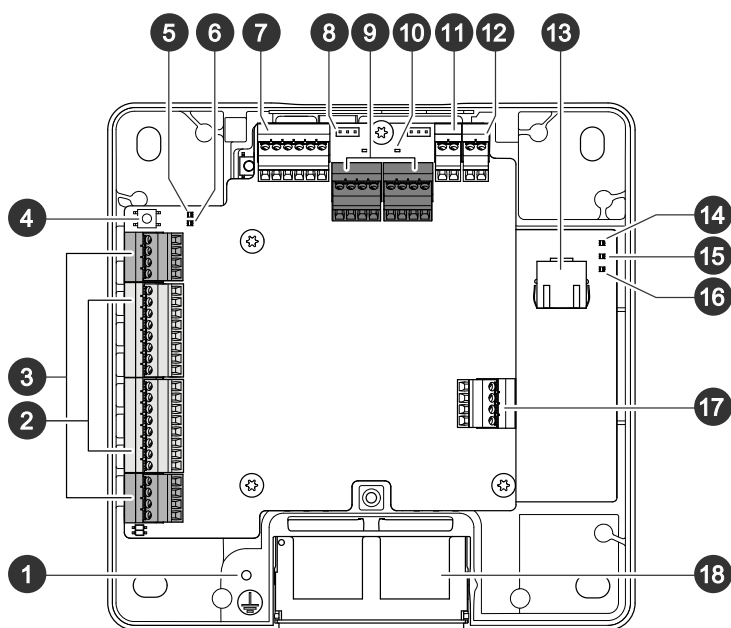
# AXIS A1610 Network Door Controller

## Specyfikacje

### Specyfikacje

Tekst oznaczony jako UL dotyczy tylko instalacji UL 294.

### Informacje ogólne o produkcie



- 1 Położenie uziemienia
- 2 Złącze czytnika, 2x
- 3 Złącze drzwi, 2x
- 4 Przycisk kontrolny
- 5 Wskaźnik LED nadprądu przekaźnika
- 6 Wskaźnik LED nadprądu czytnika
- 7 Złącze pomocnicze
- 8 Zworka przekaźnika, 2x
- 9 Złącze przekaźnikowe, 2x
- 10 Wskaźnik LED przekaźnika, 2x
- 11 Pomocnicze wejście zasilania 12 V
- 12 Złącze zasilania
- 13 Złącze sieciowe
- 14 Wskaźnik LED zasilania
- 15 Wskaźnik LED stanu
- 16 Wskaźnik LED sieci
- 17 Złącze zewnętrzne
- 18 Odwracalna osłona kabla

# AXIS A1610 Network Door Controller

## Specyfikacje

### Wskaźniki LED

LED	Kolor	Wskazanie
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.
Stan	Zielony	Stałe zielone światło przy normalnym działaniu.
	Bursztynowy	Stałe światło podczas uruchamiania i odtwarzania ustawień.
	Czerwony	Powolne miganie w przypadku niepowodzenia aktualizacji.
Zasilanie	Zielony	Normalne działanie.
	Bursztynowy	Miga na zielono/bursztynowo podczas aktualizacji oprogramowania sprzętowego.
Nadprąd przełącznika	Czerwony	Stałe światło po zwarceniu lub wykryciu nadprądu.
	Zgaszony	Normalne działanie.
Nadprąd czytnika	Czerwony	Stałe światło po zwarceniu lub wykryciu nadprądu.
	Zgaszony	Normalne działanie.
Przełącznik	Zielony	Przełącznik aktywny. <sup>1</sup>
	Zgaszony	Przełącznik nieaktywny.

1. Przełącznik jest aktywny po podłączeniu COM do NO.

#### Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.
- Wskaźnik LED stanu można skonfigurować tak, by migał po rozpoznaniu jednostki. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.

### Przyciski

#### Przycisk Control

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 31*.

### Złącza

#### Złącze sieciowe

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

UL: Zasilanie Power over Ethernet (PoE) dostarczane przez Power Injector Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3 (UL 294) 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. Power over Ethernet (PoE) ocenione przez UL z zasilaczem midspan AXIS T8133 Midspan 30 W 1-port.

#### Priorytet mocy

Urządzenie to może być zasilane przez wejście PoE lub DC. Patrz *Złącze sieciowe na stronie 24* i *Złącze zasilania na stronie 29*.

- Gdy PoE i DC są podłączone przed włączeniem urządzenia, będzie ono zasilane z PoE.



# AXIS A1610 Network Door Controller

## Specyfikacje

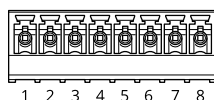
- Zarówno PoE, jak i DC są podłączone, a urządzenie jest zasilane przez wejście PoE. Gdy połączenie z PoE zostanie utracone, urządzenie przejdzie na tryb zasilania prądem stałym bez ponownego uruchomienia.
- Zarówno PoE, jak i DC są podłączone, a urządzenie jest zasilane prądem stałym. Gdy połączenie 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

Dwa 8-pinowe bloki złączy obsługujące protokoły RS485 i Wiegand do komunikacji z czytnikiem.

Podane wartości mocy wyjściowej są współdzielone między dwoma portami czytnika. Oznacza to, że 500 mA przy 12 V DC jest zarezerwowane dla wszystkich czytników podłączonych do kontrolera drzwi.

Na stronie internetowej produktu wybierz odpowiedni protokół, którego chcesz używać.



### Konfiguracja na potrzeby RS485

Funkcja	Styk	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 500 mA do wszystkich czytników
RX/TX	3-4	Full-duplex: RX. Half-duplex: RX/TX.	
TX	5-6	Full duplex: TX.	
Konfigurowalne (wejście lub wyjście)	7-8	Wejście cyfrowe – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		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 maks. 100 mA

### Ważne

- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 200 m (656 stopy).
- 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 20-16.

### Konfiguracja na potrzeby Wiegand

# AXIS A1610 Network Door Controller

## Specyfikacje

Funkcja	Styk	Uwaga	Specyfikacje
Masa DC (GND)	1		0 V DC
Wyjście DC (+12 V)	2	Dostarcza zasilanie do czytnika.	12 V DC, maks. 500 mA do wszystkich czytników
D0	3		
D1	4		
0	5-6	Wyjście cyfrowe, otwarty dren	
Konfigurowalne (wejście lub wyjście)	7-8	Wejście cyfrowe – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		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 maks. 100 mA

### Ważne

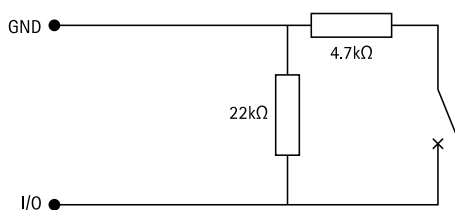
- Gdy czytnik jest zasilany przez kontroler, dopuszczalna długość kabla wynosi do 150 m (500 stopy).
- Gdy czytnik nie jest zasilany przez kontroler, dopuszczalna długość kabla dla danych czytnika wynosi do 150 m (500 ft), jeśli spełnione jest następujące wymaganie dotyczące kabla: AWG 20-16.

### Nadzorowane wejścia

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

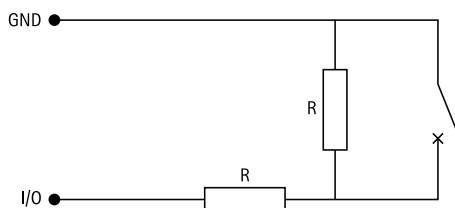
#### Pierwsze połączenie równoległe

Oporniki muszą mieć wartości 4,7 k $\Omega$  i 22 k $\Omega$ .



#### Pierwsze połączenie szeregowe

Wartości oporników muszą być takie same; możliwe wartości: 1 k $\Omega$ , 2,2 k $\Omega$ , 4,7 k $\Omega$  oraz 10 k $\Omega$ .



# AXIS A1610 Network Door Controller

## Specyfikacje

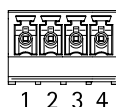
### Uwaga

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

### Złącze drzwi

Dwa 4-pinowe bloki 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. Patrz *Nadzorowane wejścia na stronie 26*.



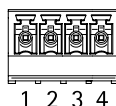
Funkcja	Styk	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Wejście	2, 4	Do komunikacji z monitorem drzwi. Wejście cyfrowe lub nadzorowane wejście – podłącz do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

### Ważne

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

### Złącze przekaźnikowe

Dwa 4-pinowe bloki zacisków dla przekaźników typu C, które mogą być używane na przykład do sterowania zamkiem lub interfejsem do bramy.



Funkcja	Styk	Uwagi	Specyfikacje
Masa DC (GND)	1		0 V DC
NO	2	Normalnie otwarty. 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 na przekaźnik Maks. napięcie = 30 V DC
COM	3	Typowy	
NC	4	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.

# AXIS A1610 Network Door Controller

## Specyfikacje

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

Źródło prądu	Maksymalna moc przy 12 V DC <sup>1</sup>	Maksymalna moc przy 24 V DC
DC IN	1 800 mA	750 mA
PoE	900 mA	410 mA

1. Moc jest dzielona między dwa przekaźniki i AUX I/O 12 V DC.

### **POWIADOMIENIE**

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

### Złącze pomocnicze

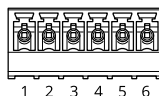
Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

**Wejścia cyfrowego** – Do podłączenia urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR, czujników okien lub drzwi oraz czujników wykrywania zbitcia szyby.

**Nadzorowanego wejścia** – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

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

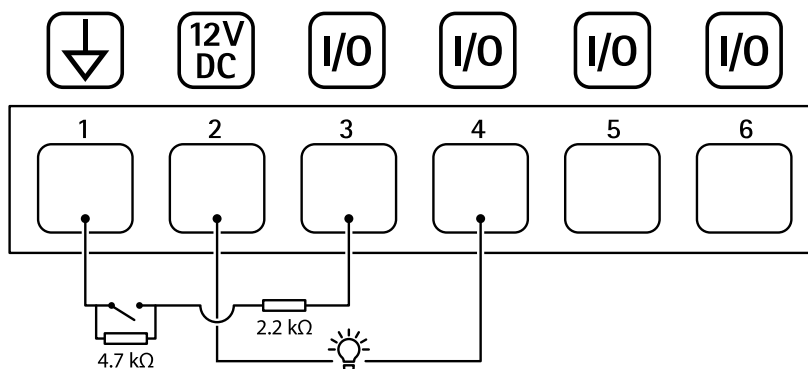
6-pinowego bloku złączy



Funkcja	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: To złącze może być użyte tylko jako wyjście zasilania po bezpiecznej stronie, ponieważ współdzieli zasilanie z przekaźnikami.	12 V DC Maks. obciążenie = 50 mA na każde WE/WY
Konfigurowalne (wejście lub wyjście)	3-6	Wejście cyfrowe lub wejście nadzorowane – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Aby móc korzystać z nadzorowanych wejść, 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 I/O może przyjąć zewnętrzne obciążenie 12 V DC, 50 mA (maks.)m jeśli użyto wewnętrznego wyjścia 12 V DC (styk 2). W przypadku podłączeń z otwartym drenem w połączeniu z zewnętrznym źródłem zasilania I/O mogą otrzymywać zasilanie DC 0-30 V DC, 100 mA.	Od 0 do maks. 30 V DC, otwarty dren maks. 100 mA

# AXIS A1610 Network Door Controller

## Specyfikacje

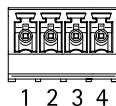


- 1 Masa DC
- 2 Wyjście DC 12 V, maks. 50 mA
- 3 WE/WY skonfigurowane jako wejście nadzorowane
- 4 I/O skonfigurowane jako wyjście
- 5 Konfigurowalne I/O
- 6 Konfigurowalne I/O

### Złącze zewnętrzne

4-pinowy blok złączy umożliwiający podłączenie urządzeń zewnętrznych, na przykład detektorów wybicia szyby lub czujników pożaru.

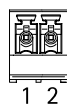
UL: Złącze nie zostało ocenione przez UL pod kątem użytkowania jako alarm antywłamaniowy/pożarowy.



Funkcja	Styk	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Konfigurowalne (wejście lub wyjście)	2, 4	Wejście cyfrowe – podłącz do styku 1 lub 3, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – podłącz do styku 1 lub 3, aby aktywować lub pozostaw rozłączone, aby dezaktywować. 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 maks. 100 mA

### Złącze zasilania

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



# AXIS A1610 Network Door Controller

## Specyfikacje

Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wejście DC	2	Do zasilania kontrolera, gdy nie jest używane zasilanie Power over Ethernet. Uwaga: ten styk może być używany tylko jako wejście zasilania.	10,5–28 V (prąd stały), maks. 36 W

UL: zasilanie prądem stałym dostarczane z zasilaczem w standardzie UL 294, UL 293 lub UL 603, w zależności od oprogramowania, o odpowiednich parametrach.

### Pomocnicze wejście zasilania 12 V

Do podłączenia zapasowego akumulatora z wbudowaną ładowarką. Wejście 12 V DC.

UL: Złącze nie zostało ocenione przez UL.

#### Ważne

Podczas korzystania z wejścia akumulatora należy włączyć szeregowo w obwód zewnętrzny bezpiecznik 3 A.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wejście akumulatora	2	Do zasilania kontrolera drzwi, gdy nie są dostępne inne źródła zasilania. Uwaga: ten styk może być używany tylko jako wejście zasilania z akumulatora. Używać tylko z UPS.	11–13,7 V DC, maks. 36 W

# AXIS A1610 Network Door Controller

## Rozwiązywanie problemów

---

### 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 Control i włącz zasilanie. Patrz *Informacje ogólne o produkcie na stronie 23*.
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. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeśli w sieci brak serwera DHCP, domyślny adres IP to 192.168.0.90.
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 wydaniem 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](https://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

- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania urządzenia (pod warunkiem, że funkcje te są dostępne w nowym systemie AXIS OS), choć Axis Communications AB tego nie gwarantuje.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

# AXIS A1610 Network Door Controller

## Rozwiązywanie problemów

---

### 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](http://axis.com/support/device-software), aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.

### Uwaga

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](http://axis.com/support/device-software).
2. Zaloguj się do urządzenia jako administrator.
3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konservacja > 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, wskazówki i rozwiązania

Jeśli nie możesz znaleźć tego, czego szukasz, przejdź na stronę poświęconą rozwiązywaniu problemów: [axis.com/support](http://axis.com/support).

### 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 <b>Konservacja</b> i przywróć poprzednio zainstalowaną wersję.

### Problemy z ustawieniem adresu IP

---

Urządzenie należy do innej podsięci	Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsięci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
Adres IP jest używany przez inne urządzenie	Odłącz urządzenie Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz <code>ping</code> oraz adres IP urządzenia): <ul style="list-style-type: none"><li>• Jeśli otrzymasz odpowiedź: <code>Reply from &lt;adres IP&gt;: bytes=32; time=10...</code>, 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.</li><li>• Jeśli otrzymasz odpowiedź: <code>Request timed out</code>, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.</li></ul>
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsięci	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.



# AXIS A1610 Network Door Controller

## Rozwiązywanie problemów

---

### Nie można uzyskać dostępu do urządzenia przez przeglądarkę

---

Nie można zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania <code>http</code> lub <code>https</code> w polu adresu przeglądarki.  W razie utraty hasła dla konta root należy przywrócić ustawienia fabryczne urządzenia. Patrz <i>Przywróć domyślne ustawienia fabryczne na stronie 31</i> .
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 można przydzielić samodzielnie statyczny adres IP. Instrukcje można znaleźć na stronie <a href="http://axis.com/support">axis.com/support</a> .
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 <b>System &gt; Date and time (System &gt; Data i godzina)</b> .

### Dostęp do urządzenia można uzyskać lokalnie, ale nie z zewnątrz

---

Aby uzyskać dostęp do urządzenia z zewnątrz, zalecamy skorzystanie z jednej z następujących aplikacji dla systemu Windows®:

- AXIS Companion: darmowa aplikacja idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station 5: 30-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.
- 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](http://axis.com/vms).

### Nie można połączyć przez port 8883 z MQTT przez SSL

---

Zapora blokuje ruch przy użyciu 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. <ul style="list-style-type: none"><li>• 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.</li><li>• Jeżeli serwer/broker obsługuje ALPN, korzystanie z MQTT może być negocjowane w otwartym porcie, np. 443. Skontaktuj się z dostawcą serwera/brokera, aby dowiedzieć się, czy negocjacja ALPN jest obsługiwana oraz jakiego protokołu i portu ALPN należy użyć.</li></ul>
--	--

## Kwestie wydajności

Najważniejsze czynniki, które należy wziąć pod uwagę:

- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.

## Kontakt z pomocą techniczną

Aby uzyskać pomoc, przejdź na stronę [axis.com/support](http://axis.com/support).

