AXIS A9210 Network I/O Relay Module

Podręcznik użytkownika

Od czego zacząć

Wyszukiwanie urządzenia w sieci

Aby znaleźć urządzenia Axis w sieci i przydzielić im adresy IP w systemie Windows®, użyj narzędzia AXIS IP Utility lub AXIS Device Manager. Obie aplikacje są darmowe i można je pobrać ze strony *axis.com/support*.

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

✓: zalecane

*: obsługiwane z ograniczeniami

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis.
   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora, on page 2*.

Opisy wszystkich elementów sterowania i opcji w interfejsie WWW urządzenia można znaleźć tutaj: *Interfejs WWW, on page 5*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła, on page 3*.
3. Wprowadź ponownie hasło.
4. Zaakceptuj umowę licencyjną.
5. Kliknij kolejno opcje **Add account (Dodaj konto)**.

Ważne

W urządzeniu nie ma konta domyślnego. Jeśli nastąpi utrata hasła do konta administratora, należy zresetować urządzenie. Patrz *Przywróć domyślne ustawienia fabryczne, on page 44*.

Bezpieczne hasła

Ważne

Używaj protokołu HTTPS (który jest domyślnie włączony), aby ustawić hasło lub skonfigurować inne poufne dane przez sieć. Protokół HTTPS umożliwia nawiązywanie bezpiecznych, szyfrowanych połączeń sieciowych, chroniąc w ten sposób poufne dane, takie jak hasła.

Hasło urządzenia stanowi podstawową ochronę danych i usług. Urządzenia Axis nie narzucają zasad haseł, ponieważ mogą być one używane w różnych typach instalacji.

Aby chronić dane, zalecamy:

- Używanie haseł o długości co najmniej ośmiu znaków, najlepiej utworzonego automatycznym generatorem haseł.
- Nieujawnianie haseł.
- Regularną zmianę haseł co najmniej raz na rok.

Upewnianie się co do braku zmian w oprogramowaniu urządzenia

Aby upewnić się, że w urządzeniu zainstalowano oryginalny system AXIS OS lub aby odzyskać kontrolę nad urządzeniem w razie ataku:

1. Przywróć domyślne ustawienia fabryczne. Patrz *Przywróć domyślne ustawienia fabryczne, on page 44*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Omówienie interfejsu WWW

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

Interfejs WWW urządzenia Axis

Konfiguracja urządzenia

Konfiguracja portu WE/WY

1. Wybierz kolejno opcje **Device > I/Os and relays > AXIS A9210 > I/Os (Urządzenia > We/wy i przekaźniki > AXIS A9210 > We/wy)**.
2. Kliknij , aby rozwinąć ustawienia portu WE/WY.
3. Zmień nazwę portu.
4. Skonfiguruj stan normalny. Kliknij w przypadku obwodu otwartego lub w przypadku obwodu zamkniętego.
5. Aby skonfigurować port WE/WY jako wejście:
   5.1. W obszarze **Direction (Kierunek)** kliknij .
   5.2. Aby monitorować stan wejścia, włącz **Supervised (Nadzorowane)**. Patrz *Nadzorowane wejścia, on page 42*.

Uwaga

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

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

Konfiguracja przekaźnika

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

Konfiguracja reguł dotyczących zdarzeń

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

Wyzwalanie akcji

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

Uwaga

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

Interfejs WWW

Aby 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. Ikona wskazuje, że funkcja lub ustawienie są 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 się)**: 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.

Status

Informacje o urządzeniu

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

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

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 **Time and location (Czas i lokalizacja)**, gdzie można zmienić ustawienia usługi NTP.

Bezpieczeństwo

Pokazuje, jakiego rodzaju dostęp do urządzenia jest aktywny, które protokoły szyfrowania są używane oraz, czy dozwolone jest korzystanie z niepodpisanych aplikacji. Zalecane ustawienia bazują na przewodniku po zabezpieczeniach systemu operacyjnego AXIS OS.

Hardening guide (Przewodnik po zabezpieczeniach): Kliknięcie spowoduje przejście do *przewodnika po zabezpieczeniach systemu operacyjnego AXIS OS*, gdzie można się dowiedzieć więcej o stosowaniu najlepszych praktyk cyberbezpieczeństwa.

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.

Urządzenie

WE/WY i przekaźniki

AXIS A9210

We/wy

Wejście

- **Nazwa**: edytuj tekst, aby zmienić nazwę portu.
- **Direction (Kierunek)**: Wskazuje, że jest to port wejścia.
- **Normal state (Stan normalny)**: Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.
- **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.
  - 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.

Wyjście: włącz w celu aktywowania połączonych urządzeń.

- **Nazwa**: edytuj tekst, aby zmienić nazwę portu.
- **Direction (Kierunek)**: oznacza, że jest to port wyjścia.
- **Normal state (Stan normalny)**: Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.
- **Toggle port URL (Przełącz adres URL portu)**: wskazuje adresy URL umożliwiające aktywację i dezaktywację połączonych urządzeń przy użyciu interfejsu programowania aplikacji VAPIX®.

I/O (WE/WY): włączenie tej opcji pozwala aktywować podłączone urządzenia, gdy port jest skonfigurowany jako wyjściowy.

- **Nazwa**: edytuj tekst, aby zmienić nazwę portu.
- **Direction (Kierunek)**: kliknij  lub  , aby skonfigurować jako wejście lub wyjście.
- **Normal state (Stan normalny)**: Kliknij  w przypadku obwodu otwartego i  w przypadku obwodu zamkniętego.
- **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. Pojawia się tylko wtedy, gdy port jest skonfigurowany jako port wejścia.
  - 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.
- **Toggle port URL (Przełącz adres URL portu)**: wskazuje adresy URL umożliwiające aktywację i dezaktywację połączonych urządzeń przy użyciu interfejsu programowania aplikacji VAPIX®. Pojawia się tylko wtedy, gdy port jest skonfigurowany jako port wyjścia.

Przekaźniki

- **Relay (Przekaźnik)**: pozwala włączyć lub wyłączyć przekaźnik.
- **Nazwa**: edytuj tekst, aby zmienić nazwę przekaźnika.
- **Direction (Kierunek)**: oznacza, że jest to przekaźnik wyjścia.
- **Toggle port URL (Przełącz adres URL portu)**: wskazuje adresy URL umożliwiające aktywację i dezaktywację przekaźnika przy użyciu interfejsu programowania aplikacji VAPIX®.

AXIS A9910

Do jednego modułu AXIS A9210 można dołączyć maks. 16 modułów AXIS A9910, aby obsługiwać 128 wejść / wyjść, 64 przekaźniki i 64 czujniki Modbus. Maks. odległość od modułu AXIS A9210 do ostatniego modułu AXIS A9910 wynosi 1000 m.

Add encryption key (Dodaj klucz szyfrowania): kliknięcie tej opcji pozwala skonfigurować klucz szyfrowania w celu zapewnienia szyfrowanej komunikacji.

Add AXIS A9910 (Dodaj AXIS A9910): kliknij, aby dodać moduł rozszerzający.

- **Nazwa**: w tym miejscu można edytować tekst, aby zmienić nazwę modułu rozszerzającego.
- **Adres**: pozwala wyświetlić adres, do którego podłączony jest moduł rozszerzający.
- **Device software version (Wersja oprogramowania urządzenia)**: Umożliwia zobaczenie bieżącej wersji oprogramowania modułu rozszerzającego.
- **Upgrade device software (Uaktualnienie oprogramowania urządzenia)**: Kliknij, aby uaktualnić oprogramowanie modułu rozszerzającego. Możesz zdecydować się na uaktualnienie do wersji dołączonej do kontrolera drzwi lub wgrać wersję wybraną przez siebie.

We/wy

I/O (WE/WY): włączenie tej opcji pozwala aktywować podłączone urządzenia, gdy port jest skonfigurowany jako wyjściowy.

- **Nazwa**: edytuj tekst, aby zmienić nazwę portu.
- **Direction (Kierunek)**: kliknij lub , aby skonfigurować jako wejście lub wyjście.
- **Normal state (Stan normalny)**: Kliknij w przypadku obwodu otwartego i w przypadku obwodu zamkniętego.
- **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. Pojawia się tylko wtedy, gdy port jest skonfigurowany jako port wejścia.
  - 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.
- **Toggle port URL (Przełącz adres URL portu)**: wskazuje adresy URL umożliwiające aktywację i dezaktywację połączonych urządzeń przy użyciu interfejsu programowania aplikacji VAPIX®. Pojawia się tylko wtedy, gdy port jest skonfigurowany jako port wyjścia.

Przekaźniki

- **Relay (Przekaźnik)**: pozwala włączyć lub wyłączyć przekaźnik.
- **Nazwa**: edytuj tekst, aby zmienić nazwę przekaźnika.
- **Direction (Kierunek)**: oznacza, że jest to przekaźnik wyjścia.
- **Toggle port URL (Przełącz adres URL portu)**: wskazuje adresy URL umożliwiające aktywację i dezaktywację przekaźnika przy użyciu interfejsu programowania aplikacji VAPIX®.

Alarmy

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

Casing open (Otwarcie obudowy) : Włączenie tej opcji powoduje wyzwalanie alarmu w systemie, gdy zostanie wykryte otwarcie obudowy kontrolera drzwi. Wyłącz to ustawienie dla kontrolerów drzwi typu barebone.

External tamper (Sabotaż z zewnątrz) : Jej włączenie spowoduje emitowanie alarmu w systemie w reakcji na wykrycie zewnętrznej próby ingerencji. Na przykład po otwarciu lub zamknięciu zewnętrznej szafki.

- **Supervised input (Wejście nadzorowane)** : 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

Czujniki

Prezentuje przegląd czujników dołączonych do modułu AXIS A9210. Do portu RS-485 można dołączyć bezpośrednio maks. 8 czujników Modbus lub rozbudować do 16 modułów AXIS A9910, celem uzyskania 64 czujników Modbus w jednym module AXIS A9210.

Dodaj: Kliknij, aby dodać czujnik.

Nazwa: Wpisz nazwę czujnika.
Czujnik: Wybierz urządzenie, do którego dołączono czujnik.
Port RS-485: Wybierz port, do którego dołączono czujnik.
Adres: Wpisz adres czujnika. Jeżeli korzystasz z funkcji multidrop, wpisz niepowtarzalny adres z zakresu 1 – 247.
Type (Typ):

- Wybierz **Custom** (Własny).
  - **Export template** (Eksportuj szablon): Kliknij, aby pobrać plik JSON. Możesz edytować plik i przesłać go później do urządzenia.
  - **Select configuration file** (Wybierz plik konfiguracyjny): Kliknij, aby zaznaczyć plik konfiguracyjny lub przeciągnij go. Możesz edytować, kopiować, pobrać lub wydrukować plik konfiguracyjny.
- Wybierz **Hugo** lub **Tibbo**.
  - **Read data** (Odczyt danych): Ustaw częstość odczytu danych z czujnika.
  - **Thresholds** (Progi): Ustaw wartości progowe dotyczące dostępnych funkcji czujników, takich jak temperatura, wilgotność, punkt rosy, ciśnienie atmosferyczne lub natężenie oświetlenia.

Save (Zapisz): Kliknij, aby zapisać konfigurację.

Na liście czujników:

- **Imię:** Edytuj tekst, aby zmienić nazwę czujnika.
- **Device/Port** (Urządzenie / port): Identyfikator Modbus i numer portu, do którego dołączony jest czujnik.
- **Type (Typ):** Rodzaj pomiaru lub funkcji wykonywanej przez czujnik, np. temperatura, wilgotność lub natężenie oświetlenia.
- **Model:** Oznaczenie modelu czujnika.
- **Last value (Ostatnia wartość):** Ostatni odczyt z czujnika.
- **Last event (Ostatnie zdarzenie):** Powód ostatnio wyzwolonego zdarzenia, np. powyżej lub poniżej ustawionego ograniczenia dla wybranego parametru.
- **Stan:** Wskazuje, czy czujnik jest obecnie w trybie online czy offline.

Aplikacje

Add app (Dodaj aplikację): umożliwia zainstalowanie nowej aplikacji.

Find more apps (Znajdź więcej aplikacji): pozwala znaleźć więcej aplikacji do zainstalowania. Nastąpi przekierowanie na stronę z opisem aplikacji Axis.

Allow unsigned apps (Zezwalaj na niepodpisane aplikacje) : włączenie tej opcji umożliwi instalowanie niepodpisanych aplikacji.

Wyświetl aktualizacje zabezpieczeń w aplikacjach AXIS OS i ACAP.

Uwaga

Korzystanie z kilku aplikacji jednocześnie może wpływać na wydajność urządzenia.

Aby włączyć lub wyłączyć aplikację, użyj przełącznika znajdującego się obok jej nazwy.

Open (Otwórz): umożliwia uzyskanie dostępu do ustawień aplikacji. Dostępne ustawienia zależą od aplikacji. W niektórych aplikacjach nie ma żadnych ustawień.

Menu kontekstowe może zawierać jedną lub kilka z następujących opcji:

- **Open-source license (Licencja open source)**: pozwala wyświetlić informacje o licencjach open source używanych w aplikacji.
- **App log (Dziennik aplikacji)**: pozwala wyświetlić dziennik zdarzeń aplikacji. Dziennik jest pomocny podczas kontaktowania się z pomocą techniczną.
- **Activate license with a key (Aktywuj licencję kluczem)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie nie ma dostępu do Internetu. Jeśli nie masz klucza licencji, przejdź na stronę *axis.com/products/analytics*. Do wygenerowania klucza potrzebny będzie kod licencyjny oraz numer seryjny produktu Axis.
- **Activate license automatically (Aktywuj licencję automatycznie)**: Jeżeli aplikacja wymaga licencji, konieczne jest jej aktywowanie. Z tej opcji należy korzystać, jeżeli urządzenie ma dostęp do Internetu. Do aktywowania licencji konieczny jest kod.
- **Deactivate the license (Dezaktywuj licencję)**: Aby zastąpić obecną licencję inną licencją, np. w przypadku przejścia z wersji próbnej na pełną, musisz wyłączyć obecną licencję. Jeśli dezaktywujesz licencję, zostanie ona również usunięta z urządzenia.
- **Ustawienia**: Ta opcja umożliwia konfigurowanie parametrów.
- **Usuń**: Ta opcja powoduje trwałe usunięcie aplikacji z urządzenia. Jeśli najpierw nie dezaktywujesz licencji, pozostanie ona aktywna.

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 (PTP) (Automatyczna data i godzina (PTP))**: Synchronizacja przy użyciu protokołu precyzyjnego czasu.
- **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.
  - **Trusted NTS KE CA certificates (Zaufane certyfikaty NTS KE CA)**: Wybierz zaufane certyfikaty CA, które mają być używane do bezpiecznej synchronizacji czasu NTS KE, lub pozostaw bez wyboru certyfikatu.
  - **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.
  - **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.

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 (v4 lub v6). Jeżeli dostępne są obie wersje, urządzenie preferuje strefy czasowe IANA zamiast POSIX oraz DHCPv4 zamiast DHCPv6.
  - DHCPv4 korzysta z opcji 100 w zakresie stref czasowych POSIX oraz opcji 101 w zakresie stref czasowych IANA.
  - DHCPv6 korzysta z opcji 41 w zakresie POSIX i opcji 42 w zakresie IANA.
- **Manual (Ręcznie)**: Wybierz strefę czasową z listy rozwijanej.

Uwaga

System używa ustawień daty i godziny we wszystkich nagraniach, dziennikach i ustawieniach systemowych.

Lokalizacja urządzenia

Wprowadź lokalizację urządzenia. System zarządzania materiałem wizyjnym wykorzysta tę informację do umieszczenia urządzenia na mapie.

- **Latitude (Szerokość geograficzna)**: Wartości dodatnie to szerokość geograficzna na północ od równika.
- **Longitude (Długość geograficzna)**: Wartości dodatnie to długość geograficzna na wschód od południka zerowego.
- **Kierunek**: Wprowadź kierunek (stronę świata), w który skierowane jest urządzenie. 0 to północ.
- **Etykieta**: Wprowadź opisową nazwę urządzenia.
- **Save (Zapisz)**: Kliknij, aby zapisać lokalizację urządzenia.

Sieć

IPv4

Przypisz automatycznie IPv4: Wybierz opcję „Przypisz automatycznie IPv4" (DHCP), aby sieć automatycznie przydzielała adres IP, maskę podsieci i router bez konieczności ręcznej konfiguracji. Zalecamy korzystanie z funkcji automatycznego przydzielania adresu IP (DHCP) dla większości sieci.

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.

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 -.

Włącz aktualizacje dynamiczne DNS: Zezwól urządzeniu na automatyczne aktualizowanie rekordów serwera nazw domen, gdy zmieni się jego adres IP.

Zarejestruj nazwę DNS: Wprowadź unikatową nazwę domeny, która wskazuje adres IP urządzenia. Używaj tylko dozwolonych znaków: A-Z, a-z, 0-9 i -.

TTL: Time to Live (TTL) to ustawienie określające, jak długo rekord DNS zachowuje ważność, zanim trzeba go zaktualizować.

Serwery DNS

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.

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.

Uwaga

Jeśli protokół DHCP jest wyłączony, funkcje oparte na automatycznej konfiguracji sieci, takie jak nazwa hosta, serwery DNS, serwer NTP i inne, mogą przestać działać.

HTTP i HTTPS

HTTPS to protokół umożliwiający szyfrowanie żądań stron wysyłanych przez użytkowników oraz stron zwracanych przez serwer sieci Web. Zaszyfrowana 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 > Zabezpieczenia**, aby utworzyć i zainstalować certyfikaty.

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

Uwaga

W przypadku przeglądania zaszyfrowanych 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.

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.

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.

LLDP and CDP (LLDP i CDP): Włącz, aby umożliwić automatyczne wykrywanie urządzeń w sieci. Wyłączenie funkcji LLDP and CDP może wpływać na negocjowanie zasilania z PoE. Aby rozwiązać ewentualne problemy negocjowania zasilania z PoE, należy skonfigurować przełącznik PoE tylko do sprzętowej negocjacji zasilania PoE.

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

Usługa One-Click Cloud Connection (O3C) w połączeniu z systemem O3C 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*.

Allow O3C (Zezwalaj na O3C):

- **One-click (Jednym kliknięciem)**: Jest to domyślna opcja. Aby połączyć się z usługą O3C, naciśnij przycisk kontrolny na urządzeniu. W zależności od modelu urządzenia, naciśnij i zwolnij lub naciśnij i przytrzymaj, aż dioda stanu zacznie migać. Zarejestruj urządzenie w usłudze O3C w ciągu 24 godzin, aby uaktywnić opcję **Always** i pozostać połączonym. Jeśli nie zarejestrujesz urządzenia, zostanie ono odłączone od usługi O3C.
- **Zawsze**: Urządzenie stale próbuje połączyć się z usługą O3C przez Internet. Po zarejestrowaniu urządzenia pozostaje ono połączone. Opcji tej należy używać wtedy, gdy przycisk kontrolny jest niedostępny.
- **No (Nie)**: rozłącza 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.

Authentication method (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.
- **Szyfrowanie**: ta metoda jest bezpieczniejsza, ponieważ zawsze przesyła hasło w sieci w formie zaszyfrowanej.
- **Automatycznie**: ta opcja umożliwia urządzeniu wybór metody uwierzytelniania w zależności od obsługiwanych metod. Priorytet ma metoda **Szyfrowanie**; w dalszej kolejności stosowana jest metoda **Zwykła**.

Owner authentication key (OAK) (Klucz uwierzytelniania właściciela (OAK)): Kliknij **Get key (Uzyskaj 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 **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 **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.
    - **Link up (Łącze w górę)**: wysyła komunikat pułapkę po zmianie łącza w górę.
    - **Link down (Łącze w dół)**: wysyła komunikat pułapkę po zmianie łącza w dół.
    - **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 nieupoważnionych do niezaszyfrowanych pułapek SNMP v1 i v2c. Jeśli używasz SNMP v3, możesz skonfigurować pułapki za pomocą aplikacji do zarządzania SNMP v3.
  - **Privacy** (Prywatność): Wybierz rodzaj szyfrowania stosowanego do ochrony danych SNMP.
  - **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.

Bezpieczeństwo

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. Zostanie otwarty przewodnik krok po kroku.

- **More (Więcej)** : Wyświetlanie dodatkowych pól do wypełnienia lub wybrania.
- **Secure keystore (Bezpieczny magazyn kluczy)**: Wybierz tę opcję, aby używać funkcji **Trusted Execution Environment (SoC TEE)**, **Secure element (Bezpieczny 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/axis-os#cryptographic-support*.
- **Key type (Typ klucza)**: Aby zabezpieczyć certyfikat, wybierz domyślny algorytm szyfrowania lub inny z listy rozwijanej.

Menu kontekstowe zawiera opcje:

- **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 rejestracyjnego i złożenia wniosku o wydanie certyfikatu tożsamości cyfrowej.

Secure keystore (Bezpieczny magazyn kluczy) :

- **Trusted Execution Environment (SoC TEE)**: Wybierz, aby używać środowiska SoC TEE na potrzeby bezpiecznego magazynu kluczy.
- **Bezpieczny element (CC EAL6+, FIPS 140-3 poziom 3)** : 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.

Kontrola dostępu do sieci i szyfrowanie

IEEE 802.1x

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.

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.

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.

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

Certyfikaty CA: wybierz certyfikaty CA w celu potwierdzania 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.

Te ustawienia są dostępne wyłącznie w przypadku korzystania z uwierzytelniania za pomocą **IEEE 802.1x PEAP-MSCHAPv2**:

- **Hasło**: Wprowadź hasło do tożsamości użytkownika.
- **Peap version (Wersja Peap)**: wybierz wersję Peap używaną w switchu sieciowym.
- **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.

Te ustawienia są dostępne wyłącznie w przypadku uwierzytelniania za pomocą **IEEE 802.1ae MACsec (klucz CAK/PSK)**:

- **Nazwa klucza skojarzenia łączności umowy klucza**: Wprowadź nazwę skojarzenia łączności (CKN). Musi to być od 2 do 64 (podzielnych przez 2) znaków szesnastkowych. CKN musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.
- **Klucz skojarzenia łączności umowy klucza**: Wprowadź klucz skojarzenia łączności (CAK). Musi mieć 32 lub 64 znaki szesnastkowe. CAK musi być ręcznie skonfigurowany w skojarzeniu łączności i musi być zgodny na obu końcach łącza, aby początkowo włączyć MACsec.

Zapobiegaj atakom typu brute force

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.

Zapora

Firewall (Zapora sieciowa): włącz, aby uaktywnić zaporę sieciową.

Domyślne ustawienia zasad: wybierz sposób, w jaki zapora ma obsługiwać żądania połączeń, które nie są objęte regułami.

- **ACCEPT** (Zezwalaj): zezwala na wszystkie połączenia z urządzeniem. Jest opcja domyślna.
- **DROP** (Odrzucaj): blokuje wszystkie próby połączeń z urządzeniem.

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

+ New rule (Dodaj nową regułę): Kliknij, aby utworzyć regułę.

Rule type (Rodzaj reguły):

- **FILTER** (Filtr): zaznacz, aby zezwolić na lub zablokować połączenia z urządzeń spełniających kryteria określone w regule.
  - **Policy (Zasada)**: wybierz opcję **Accept** (Zezwalaj) lub **Drop** (Odrzucaj) dotyczącą reguły zapory sieciowej.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC** (Adres MAC): wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
    - **UNICAST**: ruch od jednego nadawcy do jednego odbiorcy.
    - **BROADCAST**: ruch od jednego nadawcy do wszystkich urządzeń w sieci.
    - **MULTICAST**: ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.
- **LIMIT** (Ograniczenie): wybierz, aby przyjmować połączenia z urządzeń spełniających kryteria określone w regule, ale stosować ograniczenia w celu zmniejszenia nadmiernego ruchu.
  - **IP range** (Zakres adresów IP): zaznacz, aby określić zakres adresów do zezwolenia lub zablokowania. Użyj IPv4 / IPv6 w pozycji **Start** (Początek) i **End** (Koniec).
  - **Adres IP**: wpisz adres, który ma być przepuszczany lub blokowany. Użyj IPv4 / IPv6 lub formatu CIDR.
  - **Protocol (Protokół)**: wybierz protokół sieciowy (TCP, UDP lub oba), który ma być dozwolony lub blokowany. Po wybraniu protokołu należy również określić port.
  - **MAC** (Adres MAC): wprowadź adres MAC urządzenia, które ma lub nie ma mieć dostępu.
  - **Port range** (Zakres portów): zaznacz, aby określić zakres portów do zezwolenia lub zablokowania. Dodaj je w pozycjach **Start** (Początek) i **End** (Koniec).
  - **Port**: wpisz numer portu, który ma być przepuszczany lub blokowany. Numery portów muszą zawierać się w przedziale od 1 do 65535.
  - **Unit** (Rodzaj połączenia): wybierz rodzaj połączeń, które mają być dozwolone lub blokowane.
  - **Period** (Okres): wybierz okres związany z pozycją **Amount**.
  - **Amount** (Liczba): ustaw maksymalną liczbę połączeń, jaką urządzenie może ustanowić w ustawionym okresie **Period**. Maksymalna wartość to 65535.

- **Burst**: wpisz liczbę połączeń, dla których dozwolone jest jednokrotne przekroczenie ustawionej liczby **Amount** w ustawionym okresie **Period**. Po osiągnięciu tej liczby dozwolona jest tylko ustalona liczba w ustalonym okresie.
- **Traffic type** (Rodzaj ruchu): wybierz rodzaj ruchu, na który chcesz zezwolić lub który chcesz zablokować.
  - **UNICAST**: ruch od jednego nadawcy do jednego odbiorcy.
  - **BROADCAST**: ruch od jednego nadawcy do wszystkich urządzeń w sieci.
  - **MULTICAST**: ruch od jednego lub więcej nadawców do jednego lub więcej odbiorców.

Test rules (Reguły testu): kliknij tę opcję, aby przetestować zdefiniowane reguły.

- **Test time in seconds** (Czas testu w sekundach): Pozwala ustawić limit czasu testowania reguł.
- **Roll back (Przywróć poprzednią wersję)**: kliknij, aby przywrócić zaporę sieciową do stanu sprzed przetestowania reguł.
- **Apply rules** (Zastosuj reguły): kliknij, aby uaktywnić reguły bez testowania. Nie zaleca się wykonywania tej czynności.

Niestandardowy podpisany certyfikat systemu AXIS OS

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

Konta

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

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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 tez dodawać, aktualizować i usuwać inne konta.
- **Operator**: Ma dostęp do wszystkich ustawień poza:
  - Wszystkie ustawienia **System**.
- **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.

Anonimowy dostęp

Allow anonymous viewing (Zezwalaj na anonimowe wyświetlanie): Włączenie tej opcji pozwala wszystkim osobom uzyskać dostęp do urządzenia jako dozorca bez logowania się za pomocą konta.

Allow anonymous PTZ operating (Zezwalaj na anonimową obsługę PTZ) : Jeśli włączysz tę opcję, anonimowi użytkownicy będą mogli obracać, przechylać i powiększać/zmniejszać obraz.

Konta SSH

Add SSH account (Dodaj konto SSH): Kliknij, aby dodać nowe konto SSH.

- **Enable SSH (Włącz SSH)**: Włącz, aby korzystać z usługi SSH.

Account (Konto): Wprowadź niepowtarzalną nazwę konta.

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.

Uwaga: Wprowadź komentarz (opcjonalnie).

Menu kontekstowe zawiera opcje:

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

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

Konfiguracja OpenID

Ważne

Jeśli nie udaje się zalogować za pomocą OpenID, użyj poświadczeń Digest lub Basic, które zostały użyte podczas konfigurowania OpenID.

Client ID (Identyfikator klienta): Wprowadź nazwę użytkownika OpenID.

Outgoing Proxy (Wychodzący serwer proxy): Aby używać serwera proxy, wprowadź adres serwera proxy dla połączenia OpenID.

Admin claim (Przypisanie administratora): Wprowadź wartość roli administratora.

Provider URL (Adress URL dostawcy): Wprowadź łącze internetowe do uwierzytelniania punktu końcowego interfejsu programowania aplikacji (API). Łącze musi mieć format https://[wstaw URL]/.well-known/openid-configuration

Operator claim (Przypisanie operatora): Wprowadź wartość roli operatora.

Require claim (Wymagaj przypisania): Wprowadź dane, które powinny być dostępne w tokenie.

Viewer claim (Przypisanie dozorcy): Wprowadź wartość dla roli dozorcy.

Remote user (Użytkownik zdalny): Wprowadź wartość identyfikującą użytkowników zdalnych. Pomoże to wyświetlić bieżącego użytkownika w interfejsie WWW urządzenia.

Scopes (Zakresy): Opcjonalne zakresy, które mogą być częścią tokenu.

Client secret (Tajny element klienta): Wprowadź hasło OpenID.

Save (Zapisz): Kliknij, aby zapisać wartości OpenID.

Enable OpenID (Włącz OpenID): Włącz tę opcję, aby zamknąć bieżące połączenie i zezwolić na uwierzytelnianie urządzenia z poziomu adresu URL dostawcy.

Zdarzenia

Reguły

Reguła określa warunki wyzwalające w urządzeniu wykonywanie danej akcji. Na liście znajdują się wszystkie reguły skonfigurowane w produkcie.

Uwaga

Można utworzyć maksymalnie 256 reguł akcji.

Add a rule (Dodaj regułę): Utwórz regułę.

Nazwa: Wprowadź nazwę reguły.

Wait between actions (Poczekaj między działaniami): Wprowadź minimalny czas (w formacie gg:mm:ss), jaki musi upłynąć między aktywacjami reguły. Ustawienie to jest przydatne, gdy reguła jest aktywowana na przykład warunkami trybów dziennego i nocnego, ponieważ zapobiega niepożądanemu uruchamianiu reguły przez niewielkie zmiany natężenia światła podczas wschodu i zachodu słońca.

Condition (Warunek): Wybierz warunek z listy. Dopiero po spełnieniu tego warunku urządzenie wykona akcję. Jeśli określono wiele warunków, to do wyzwolenia działania konieczne jest spełnienie wszystkich z nich. Informacje na temat konkretnych warunków można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Use this condition as a trigger (Użyj tego warunku jako wyzwalacza): Zaznacz tę opcję, aby ten pierwszy warunek działał tylko jako wyzwalacz początkowy. Oznacza to, że po aktywacji reguła pozostanie czynna przez cały czas, gdy są spełniane wszystkie pozostałe warunki, bez względu na stan pierwszego warunku. Jeżeli nie zaznaczysz tej opcji, reguła będzie aktywna po spełnieniu wszystkich warunków.

Invert this condition (Odwróć ten warunek): Zaznacz tę opcję, jeśli warunek ma być przeciwieństwem dokonanego przez Ciebie wyboru.

Add a condition (Dodaj warunek): Kliknij, aby dodać kolejny warunek.

Action (Akcja): Wybierz akcję z listy i wprowadź jej wymagane informacje. Informacje na temat konkretnych akcji można znaleźć w części *Get started with rules for events (Reguły dotyczące zdarzeń)*.

Odbiorcy

W urządzeniu można skonfigurować powiadamianie odbiorców o zdarzeniach lub wysyłanie plików.

Uwaga

W przypadku skonfigurowania urządzenia do korzystania z protokołu FTP lub SFTP nie należy zmieniać ani usuwać unikatowego numeru sekwencyjnego dodawanego do nazw plików. Jeśli zostało to zrobione, można wysłać tylko jeden obraz na zdarzenie.

Na liście wyświetlani są wszyscy odbiorcy skonfigurowani dla produktu, a także informacje dotyczące ich konfiguracji.

Uwaga

Można utworzyć maksymalnie 20 odbiorców.

Add a recipient (Dodaj odbiorcę): Kliknij, aby dodać odbiorcę.

Nazwa: Wprowadź nazwę odbiorcy.

Type (Typ): Wybierz z listy:

- FTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer FTP. Domyślny port to 21.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze FTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.
  - **Use passive FTP (Użyj pasywnego FTP)**: W normalnych warunkach produkt po prostu wysyła żądanie otwarcia połączenia do serwera FTP. Urządzenie inicjuje przesyłanie danych na serwer docelowy i kontrolę serwera FTP. Jest to zazwyczaj konieczne w przypadku zapory ogniowej pomiędzy urządzeniem a serwerem FTP.
- HTTP
  - **URL**: Wprowadź adres sieciowy serwera HTTP oraz skrypt obsługujący żądanie. Na przykład: http://192.168.254.10/cgi-bin/notify.cgi.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTP.
- HTTPS
  - **URL**: Wprowadź adres sieciowy serwera HTTPS oraz skrypt obsługujący żądanie. Na przykład: https://192.168.254.10/cgi-bin/notify.cgi.
  - **Validate server certificate (Potwierdź certyfikat serwera)**: Zaznacz tę opcję, aby sprawdzić certyfikat utworzony przez serwer HTTPS.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **Proxy**: Włącz tę opcję i wpisz wymagane informacje, jeżeli konieczne jest dodanie serwera proxy w celu połączenia w serwerem HTTPS.
- Sieciowa pamięć masowa
  Umożliwia dodanie takiego zasobu sieciowego, jak NAS (sieciowy zasób dyskowy), i wykorzystywanie go jako odbiorcy plików. Pliki zapisywane są w formacie Matroska (MKV).

- **Host**: Wprowadź adres IP lub nazwę hosta serwera pamięci sieciowej.
- **Udział**: Podaj nazwę współdzielonego udziału na serwerze hosta.
- **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki.
- **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
- **Hasło**: Wprowadź hasło logowania.

- SFTP
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu wykorzystywanego przez serwer SFTP. Domyślny port to 22.
  - **Folder**: Wprowadź ścieżkę dostępu do katalogu, w którym mają być przechowywane pliki. Jeśli nie ma takiego katalogu na serwerze SFTP, podczas wczytywania plików zostanie wyświetlony komunikat o błędzie.
  - **Username (Nazwa użytkownika)**: Należy tu wprowadzić nazwę użytkownika, która będzie używana przy logowaniu.
  - **Hasło**: Wprowadź hasło logowania.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (MD5)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 32 cyfr w szesnastkowym systemie liczbowym). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **SSH host public key type (Typ klucza publicznego hosta SSH) (SHA256)**: Wprowadź odcisk cyfrowy klucza publicznego zdalnego hosta (ciąg 43 cyfr w systemie kodowania Base64). Klient SFTP obsługuje serwery SFTP stosujące SSH-2 i typy klucza hosta RSA, DSA, ECDSA i ED25519. RSA jest preferowaną metodą podczas negocjacji; następnie wykorzystywane są metody ECDSA, ED25519 i DSA. Upewnij się, że wprowadzono prawidłowy klucz hosta MD5 używany przez serwer SFTP. Urządzenie Axis obsługuje klucze szyfrowania MD5 i SHA-256, ale my zalecamy używanie klucza SHA-256, ponieważ jest bezpieczniejszy niż MD5. Więcej informacji o konfigurowaniu serwera SFTP dla urządzenia Axis można znaleźć w *portalu poświęconym systemowi AXIS OS*.
  - **Use temporary file name (Użyj tymczasowej nazwy pliku)**: Wybierz tę opcję, aby wczytywać pliki z tymczasowymi, automatycznie generowanymi nazwami plików. Po zakończeniu wczytywania nazwy plików zostaną zmienione na docelowe. W przypadku przerwania/wstrzymania wczytywania plików nie zostaną one uszkodzone. Pliki tymczasowe nadal pozostaną na dysku. Dzięki temu będzie wiadomo, że wszystkie pliki o danej nazwie są prawidłowe.

- SIP or VMS (SIP lub VMS) :
  SIP: Wybierz w celu nawiązania połączenia SIP.
  VMS: Wybierz w celu nawiązania połączenia VMS.
  - **From SIP account (Z konta SIP)**: Wybierz z listy.
  - **To SIP address (Na adres SIP)**: Wprowadź adres SIP.
  - **Test (Testuj)**: Kliknij, aby sprawdzić, czy ustawienia połączeń działają prawidłowo.
- E-mail

- **Wyślij wiadomość e-mail do**: Wprowadź adresy odbiorców. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
- **Wyślij e-mail przez**: Wprowadź adres serwera nadawcy.
- **Username (Nazwa użytkownika)**: Wprowadź nazwę użytkownika serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Hasło**: Wprowadź hasło dostępu do serwera poczty. Jeżeli serwer nie wymaga uwierzytelnienia, nie wypełniaj tego pola.
- **Email server (SMTP) (Serwer poczty e-mail (SMTP))**: Wprowadź nazwę serwera SMTP, na przykład smtp.gmail.com, smtp.mail.yahoo.com.
- **Port**: wprowadź numer portu serwera SMTP, używając wartości z zakresu 0–65535. Wartość domyślna to 587.
- **Szyfrowanie**: Aby używać szyfrowania, wybierz opcję SSL lub TLS.
- **Validate server certificate (Potwierdź certyfikat serwera)**: Jeżeli używasz szyfrowania, zaznacz tę opcję, aby weryfikować tożsamość urządzenia. Certyfikat może mieć własny podpis lub podpis jednostki certyfikującej (CA).
- **POP authentication (Uwierzytelnianie POP)**: Włącz tę opcję i wprowadź nazwę serwera POP, na przykład pop.gmail.com.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużej liczby załączników, odbieranie wiadomości cyklicznych itp. Aby zapobiec zablokowaniu konta lub usunięciu wiadomości, należy sprawdzić regulamin zabezpieczeń dostawcy usług.

- **TCP**
  - **Host**: Wprowadź adres IP lub nazwę hosta serwera. W przypadku wprowadzenia nazwy hosta upewnij się, że w ustawieniu **System > Network > IPv4 and IPv6 (System > Sieć > IPv4 i IPv6)** podano serwer DNS.
  - **Port**: Wprowadź numer portu dostępowego serwera.

Test (Testuj): Kliknij, aby przetestować konfigurację.

⋮ Menu kontekstowe zawiera opcje:

View recipient (Pokaż odbiorcę): Kliknij, aby wyświetlić wszystkie dane odbiorcy.

Copy recipient (Kopiuj odbiorcę): Kliknij, aby skopiować odbiorcę. Po skopiowaniu odbiorcy można wprowadzić zmiany w nowym wpisie odbiorcy.

Delete recipient (Usuń odbiorcę): Kliknij, aby trwale usunąć odbiorcę.

Harmonogramy

Harmonogramów i zdarzeń jednorazowych można użyć jako warunków reguł. Na liście wyświetlane są wszystkie harmonogramy i zdarzenia jednorazowe skonfigurowane dla produktu, a także informacje dotyczące ich konfiguracji.

+ **Add schedule (Dodaj harmonogram)**: Kliknij, aby utworzyć harmonogram lub impuls.

Wyzwalacze ręczne

Wyzwalacz manualny służy do ręcznego wyzwalania reguły. Wyzwalacza manualnego można na przykład użyć do walidacji akcji podczas instalacji i konfiguracji produktu.

MQTT

MQTT (przesyłanie telemetryczne usługi kolejkowania wiadomości) to standardowy protokół do obsługi komunikacji w Internecie rzeczy (IoT). Został zaprojektowany z myślą o uproszczeniu integracji IoT i jest wykorzystywany w wielu branżach do podłączania urządzeń zdalnych przy jednoczesnej minimalizacji objętości kodu i obciążenia sieci. 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 *bazie wiedzy na temat systemu AXIS OS*.

ALPN

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.

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 ustawienia **MQTT over TCP (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.

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.

Komunikat łączenia

określa, czy podczas ustanawiania połączenia ma być wysyłany komunikat.

Send message (Wysłanie wiadomości): włącz, aby wysyłać 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.

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 wysyłać 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.

Publikacja MQTT

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

Include condition (Uwzględnij warunek): Wybierz, aby do tematu MQTT dołączać tematy opisujące warunek.

Include namespaces (Uwzględnij przestrzenie nazw): 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.

- **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.

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.

Dzienniki

Raporty i dzienniki

Raporty

- **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.
- **Download the crash report (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.
- **Wyświetl dziennik dostępu**: Kliknij tutaj, by wyświetlić wszystkie nieudane próby uzyskania dostępu do urządzenia, na przykład gdy użyto nieprawidłowego hasła logowania.
- **View the audit log (Wyświetl dziennik kontroli)**: Kliknij, aby wyświetlić informacje o działaniach użytkownika i systemu, na przykład o udanych lub nieudanych uwierzytelnieniach i konfiguracjach.

Ślad sieciowy

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

Syslog to standard rejestrowania komunikatów. Umożliwia on oddzielenie oprogramowania, które generuje komunikaty, systemu przechowującego je i oprogramowania, które je raportuje i analizuje. Każdy komunikat jest oznaczany 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 komunikatów Syslog, 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.

Type (Typ): wybierz rodzaj dzienników do wysłania.

Test server setup (Testuj ustawienia serwera): wyślij wiadomość testową do wszystkich serwerów przed zapisaniem ustawień.

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

Zwykła konfiguracja

Opcja zwykłej konfiguracji przeznaczona jest dla zaawansowanych użytkowników, którzy mają doświadczenie w konfigurowaniu urządzeń Axis. Na stronie tej można skonfigurować i edytować większość parametrów.

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

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*.

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 najnowsza wersję, odwiedź stronę *axis.com/support*.

Po uaktualnieniu masz do wyboru trzy opcje:

- **Standard upgrade (Aktualizacja standardowa)**: Umożliwia uaktualnienie do nowej wersji systemu AXIS OS.
- **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.
- **Automatic rollback** (Automatyczne przywracanie): 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.

Więcej informacji

Analizy i aplikacje

Analizy i aplikacje pozwalają lepiej wykorzystać potencjał urządzeń Axis. AXIS Camera Application Platform (ACAP) to otwarta platforma umożliwiająca podmiotom zewnętrznym opracowywanie funkcji analizy i innych aplikacji dla urządzeń Axis. Aplikacje mogą być fabrycznie zainstalowane na urządzeniu, dostępne do pobrania za darmo lub oferowane za opłatą licencyjną.

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

AXIS Door Monitoring

Aplikacja ta monitoruje stan drzwi, wskazując, czy są one otwarte czy zamknięte, a także czy pozostają otwarte zbyt długo. Aplikacji tej używa się na przykład w przypadku drzwi przeciwpożarowych, które nie wymagają zamka, ale o których warto wiedzieć, czy są otwarte.

Zwykłe drzwi zawierają czujnik położenia, przycisk REX oraz zamki i czytniki, co wymaga stosowania kontrolera drzwiowego.

Monitorowane drzwi wymagają jedynie czujnika położenia drzwi i przycisku REX, dzięki czemu mogą być monitorowane za pomocą sieciowego modułu przekaźnikowego we / wy. Każdy sieciowy moduł przekaźnikowy we / wy można dołączyć do maks. pięciu monitorowanych drzwi.

Ograniczenia

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

Konfiguracja AXIS Monitoring Door

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

Cyberbezpieczeństwo

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

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

Axis Edge Vault

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

Podpisany system operacyjny

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

Bezpieczny start

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

Bezpieczny magazyn kluczy

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

Identyfikator urządzenia axis

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

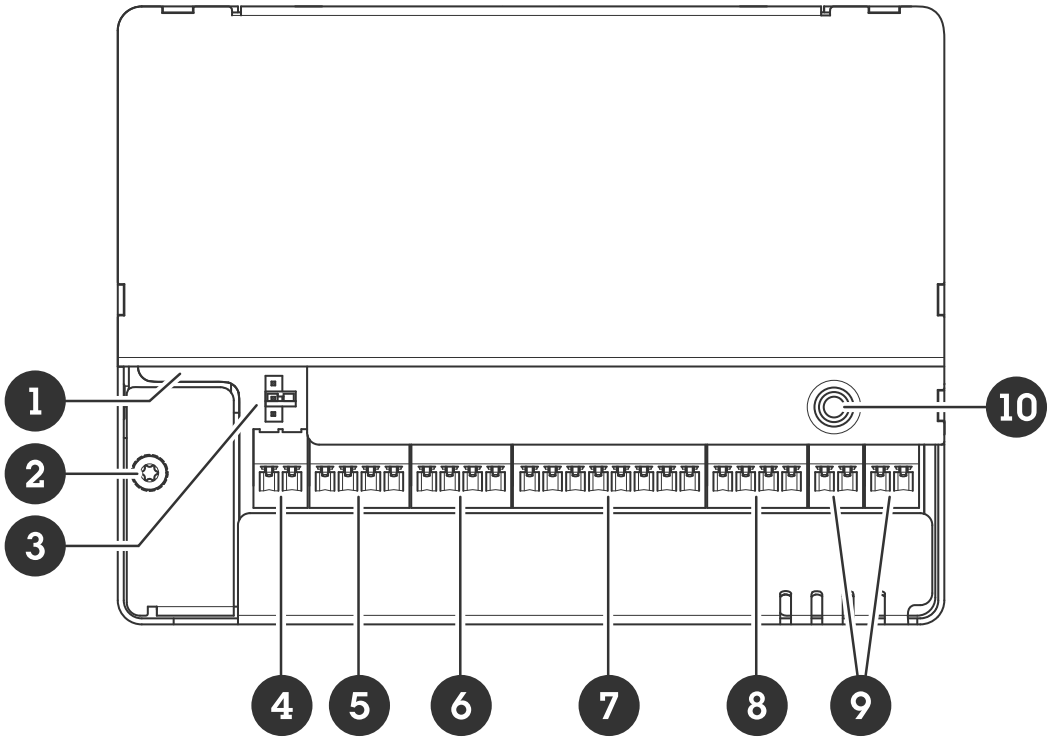
Zaszyfrowany system plików

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

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

Specyfikacje

Przegląd produktów



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

Wskaźniki LED

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

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

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 44*.
- Nawiązywanie połączenia przez Internet z usługą łączenia w chmurze jednym kliknięciem (O3C). Aby nawiązać połączenie, naciśnij i zwolnij przycisk, a następnie poczekaj, aż dioda LED stanu mignie trzy razy na zielono.

Złącza

Złącze sieciowe

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

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

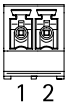
Priorytet mocy

Urządzenie to może być zasilane przez wejście PoE lub DC. Patrz *Złącze sieciowe, on page 37* i *Złącze zasilania, on page 37*.

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

Złącze zasilania

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



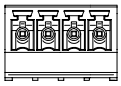
1. *Przekaźnik jest aktywny po podłączeniu COM do NO.*

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

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

Złącze przekaźnikowe

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



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

Zworka zasilania przekaźnika

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

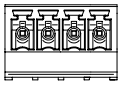
Można jej użyć do połączenia zamka między stykami GND i NO lub GND i NC.

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

Złącze wejścia 1

Jeden 4-stykowy blok złączy na wejście.

Obsługuje nadzorowanie przy użyciu rezystorów końca linii. Alarm wyzwalany jest po przerwaniu połączenia. Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii. Dla wejść nadzorowanych użyj schematu połączeń. Patrz *Nadzorowane wejścia, on page 42*.



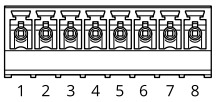
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1, 3		0 V DC
Wejście	2, 4	Wejście cyfrowe lub wejście nadzorowane — podłącz odpowiednio do styku 1 lub 3, aby aktywować, lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Ważne

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

RS485 i złącze WE/WY

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



RS485

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

We/wy

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

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

Ważne

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

Złącze I/O

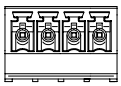
Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

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

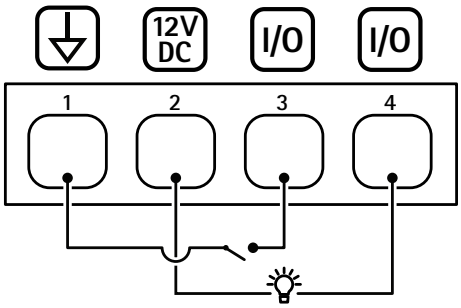
Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

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

4-pinowy blok złączy



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

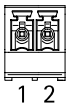


1 *Masa DC*
2 *Wyjście DC 12 V*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*

Złącze wejścia 2

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

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



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

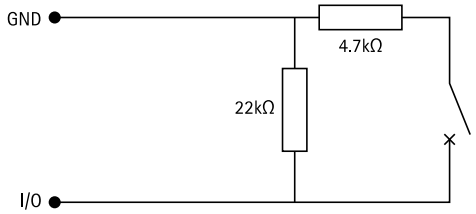
Funkcje	Styk	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wejście	2	Wejście cyfrowe lub wejście nadzorowane — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	od 0 do maks. 30 V DC

Nadzorowane wejścia

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

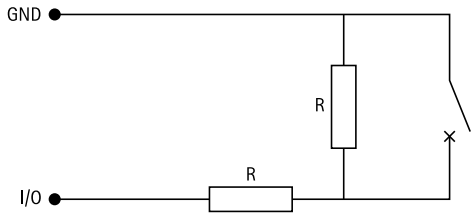
Pierwsze połączenie równoległe

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



Pierwsze połączenie szeregowe

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



Uwaga

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

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

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

Rozwiązywanie problemów –

Przywróć domyślne ustawienia fabryczne

Ważne

Przywracanie domyślnych ustawień fabrycznych należy stosować rozważnie. Opcja resetowania do domyślnych ustawień fabrycznych powoduje przywrócenie wszystkich domyślnych ustawień fabrycznych produktu, włącznie z adresem IP.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Patrz *Przegląd produktów, on page 36*.
3. Przytrzymuj przycisk Control przez 25 sekund, aż wskaźnik LED stanu ponownie zmieni kolor na bursztynowy.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie ma żadnego serwera DHCP, urządzenie będzie mieć domyślnie jeden z następujących adresów IP:
   - **Urządzenia z systemem AXIS OS w wersji 12.0 lub nowszej:** Uzyskany z podsieci adres łącza lokalnego (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS w wersji 11.11 lub starszej:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do produktu.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

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

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony *axis.com/support/device-software*, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.

1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie *axis.com/support/device-software*.
2. Zaloguj się do urządzenia jako administrator.
3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS)** > **Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

Problemy techniczne i możliwe rozwiązania

Problemy z uaktualnianiem systemu AXIS OS

Niepowodzenie uaktualniania systemu AXIS OS

Jeśli aktualizacja zakończy się niepowodzeniem, urządzenie załaduje ponownie poprzednią wersję. Najczęstszą przyczyną tego jest wczytanie niewłaściwego systemu AXIS OS. Upewnij się, że nazwa pliku systemu AXIS OS odpowiada danemu urządzeniu i spróbuj ponownie.

Problemy po aktualizacji systemu AXIS OS

Jeśli wystąpią problemy po aktualizacji, przejdź do strony **Konserwacja** i przywróć poprzednio zainstalowaną wersję.

Problemy z ustawieniem adresu IP

Nie można ustawić adresu IP

- Jeśli adres IP przeznaczony dla danego urządzenia oraz adres IP komputera używanego do uzyskania dostępu do urządzenia należą do różnych podsieci, ustawienie adresu IP jest niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.
- Adres IP może być używany przez inne urządzenie. Aby to sprawdzić:
  1. Odłącz urządzenie Axis od sieci.
  2. W oknie polecenia/DOS wpisz `ping` oraz adres IP urządzenia.
  3. Jeśli otrzymasz: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie.
  4. Jeśli otrzymasz: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez urządzenie Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
- Może występować potencjalny konflikt adresu IP z innym urządzeniem w tej samej podsieci. Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Problemy z dostępem do urządzenia

Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki

Gdy protokół HTTPS jest włączony, upewnij się, że podczas próby zalogowania się używasz prawidłowego protokołu (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki.

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje: *Przywróć domyślne ustawienia fabryczne, on page 44*.

Serwer DHCP zmienił adres IP

Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci. Znajdź urządzenie przy użyciu nazwy modelu lub numeru seryjnego bądź nazwy DNS (jeśli skonfigurowano tę nazwę).

W razie potrzeby możesz ręcznie przydzielić statyczny adres IP. Instrukcje można znaleźć na stronie *axis.com/support*.

Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X

Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w urządzeniu Axis muszą być zsynchronizowane z serwerem NTP. Wybierz kolejno opcje **System > Date and time (System > Data i godzina)**.

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, patrz *Obsługiwane przeglądarki, on page 2*.

Nie można uzyskać dostępu do urządzenia z zewnątrz

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

- AXIS Camera Station Pro: 90-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

Instrukcje i plik do pobrania znajdują się na stronie *axis.com/vms*.

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

Zapora sieciowa blokuje ruch korzystający z portu 8883, ponieważ jest on uważany za niebezpieczny.

Czasami serwer/broker może nie zapewniać konkretnego portu dla komunikacji MQTT. W takiej sytuacji może być dostępne korzystanie z MQTT przez port zwykle używany do obsługi ruchu HTTP/HTTPS.

- Jeśli serwer/broker obsługuje protokół WebSocket/WebSocket Secure (WS/WSS), typowo w porcie 443, użyj tego protokołu. Skontaktuj się z dostawcą serwera/brokera, aby dowiedzieć się, czy protokół WS/WSS jest obsługiwany oraz którego portu i ścieżki podstawowej należy używać.
- Jeśli serwer/broker obsługuje ALPN, korzystanie z MQTT może być negocjowane na otwartym porcie, na przykład porcie 443. Skontaktuj się z dostawcą serwera/brokera, aby sprawdzić, czy jest obsługiwany ALPN oraz jakiego protokołu ALPN i portu należy użyć.

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

Kontakt z pomocą techniczną

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

T10202445_pl

2026-01 (M5.5)