AXIS D4100-VE Mk II Network Strobe Siren

Podręcznik użytkownika

Spis treści

Instalacja 4
..... 4
Od czego zacząć 5
..... 5
Wyszukiwanie urządzenia w sieci 5
Obsługiwane przeglądarki 5
Otwieranie interfejsu WWW urządzenia 5
Utwórz konto administratora 5
Bezpieczne hasła 5
Konfiguracja urządzenia 7
Wyłączanie trybu konserwacji po zainstalowaniu syreny 7
Włączanie trybu konserwacji 7
Konfiguracja profilu 7
Importowanie/eksportowanie profilu 7
Konfiguracja bezpośredniego połączenia SIP (P2P) 7
Konfiguracja SIP przez serwer (PBX) 8
Konfiguracja reguł dotyczących zdarzeń 9
Wyzwalanie akcji 9
Uruchamianie profilu po wyzwoleniu alarmu 9
Uruchamianie profilu przy użyciu protokołu SIP 9
Sterowanie kilkoma profilami za pomocą rozszerzeń SIP 10
Uruchamianie dwóch profili o różnych priorytetach 11
Aktywowanie syreny stroboskopowej przez wejście wirtualne po wykryciu ruchu przez kamerę 11
Aktywowanie syreny stroboskopowej przez HTTP post po wykryciu ruchu przez kamerę 13
Aktywowanie syreny stroboskopowej przez MQTT po wykryciu ruchu przez kamerę 14
Interfejs WWW 16
Dowiedz się więcej 17
Protokół inicjacji sieci (Session Initiation Protocol, SIP) 17
Peer-to-peer SIP (P2PSIP) 17
Private Branch Exchange (PBX) – centrala abonencka 17
NAT Transversal 17
Specyfikacje 18
Przegląd produktów 18
..... 18
Wskaźniki LED 18
Przyciski 18
Przycisk kontrolny 18
Złącza 19
Złącze sieciowe 19
Złącze I/O 19
Nazwy wzorów świateł 20
Nazwy wzorów dźwiękowych 20
Czyszczenie urządzenia 22
Rozwiązywanie problemów 23
Przywracanie domyślnych ustawień fabrycznych 23
Opcje systemu AXIS OS 23
Sprawdzanie bieżącej wersji systemu AXIS OS 23
Aktualizacja systemu AXIS OS: 24
Problemy techniczne i możliwe rozwiązania 24
..... 26
Kwestie wydajności 26
Kontakt z pomocą techniczną 26
Cyberbezpieczeństwo 27

Zarządzanie podatnościami 27
Powiadomienia dotyczące zabezpieczeń 27
Bezpieczny cykl eksploatacji produktu 27

Instalacja


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

Od czego zacząć

⚠ OSTRZEŻENIE

Błyskające lub migoczące światła mogą wywołać napady u osób z padaczką światłoczułą.

Wyszukiwanie urządzenia w sieci

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

✓: Zalecenie

*: Obsługiwane z ograniczeniami

Otwieranie interfejsu WWW urządzenia

1. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Zob. *Utwórz konto administratora, on page 5*.

Opisy wszystkich funkcji i ustawień znajdujących się w interfejsie internetowym urządzeń z systemem AXIS OS znajdują się w sekcji *Pomoc dotycząca interfejsu internetowego systemu AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

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

Bezpieczne hasła

Ważne

Aby ustawić hasło lub inne poufne konfiguracje przez sieć IP, należy korzystać z protokołu HTTPS (który jest domyślnie włączony). Protokół HTTPS umożliwia bezpieczne i szyfrowane połączenia sieciowe, chroniąc w ten sposób poufne dane takie jak hasła.

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

Aby chronić dane, zalecamy:

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

Konfiguracja urządzenia

Wyłączanie trybu konserwacji po zainstalowaniu syreny

⚠ UWAGA

Aby zapobiec uszkodzeniu słuchu i oślepieniu instalatora jasnym światłem, zalecamy wyłączenie trybu konserwacji na czas instalowania urządzenia.

Jeśli instalujesz urządzenie po raz pierwszy, tryb konserwacji jest domyślnie włączony. Gdy urządzenie jest w trybie konserwacji, syrena nie wydaje żadnych dźwięków, a lampka świeci białym pulsującym światłem.

Przejdź do menu **Overview** (Widok ogólny) > **Maintenance** (Konserwacja) w celu wyłączenia **Maintenance mode** (Trybu konserwacji).

Włączanie trybu konserwacji

Aby wykonać konserwację urządzenia, przejdź do menu **Overview** (Widok ogólny) > **Maintenance** (Konserwacja) i włącz **Maintenance mode** (Tryb konserwacji). Zostanie wstrzymane zwykłe działanie świateł i syren.

Konfiguracja profilu

Profil to zbiór określonych ustawień konfiguracyjnych. Można mieć maksymalnie 30 profili z różnymi priorytetami i wzorami.

Aby ustawić nowy profil:

1. Przejdź do obszaru **Profiles (Profile)** i kliknij opcję + **Create (Utwórz)**.
2. Wypełnij pola **Name (Nazwa)** i **Description (Opis)**.
3. Wybierz ustawienia dla opcji **Light** (Oświetlenie) i **Siren (Syrena)**, które będą używane w profilu.
4. Ustaw **Priority** (Priorytet) dla oświetlenia i syreny, a następnie kliknij przycisk **Save** (Zapisz).

Aby edytować profil, kliknij ⋮ i wybierz opcję **Edit (Edytuj)**.

Importowanie/eksportowanie profilu

Aby użyć wstępnie skonfigurowanego profilu, możesz go zaimportować:

1. Przejdź do obszaru **Profiles (Profile)** i kliknij opcję + **Import (Importuj)**.
2. Przejdź do lokalizacji pliku lub przeciągnij i upuść plik, który chcesz zaimportować.
3. Kliknij przycisk **Save (Zapisz)**.

Można także wyeksportować profile w celu ich skopiowania i zapisania na innych urządzeniach:

1. Wybierz Profile.
2. Kliknij **Export (Eksportuj)**.
3. Przeglądaj, aby zlokalizować pliki. JSON.

Konfiguracja bezpośredniego połączenia SIP (P2P)

Konfiguracji P2P należy używać wtedy, gdy komunikacja odbywa się pomiędzy niewielką liczbą agentów użytkownika w tej samej sieci IP i nie ma potrzeby zapewniania dodatkowych funkcji serwera PBX.

Więcej informacji o ustawieniach, p. sekcja *SIP*.

1. Przejdź do menu **System** > **SIP** > **SIP settings (Ustawienia SIP)** i wybierz opcję **Enable SIP (Włącz SIP)**.

2. Aby zezwolić urządzeniu na odbieranie połączeń, wybierz **Allow incoming calls** (Zezwalaj na połączenia przychodzące).
3. W polu **Call handling (Obsługa połączeń)** ustaw limit czasu i czas trwania połączenia.
4. W ustawieniu **Ports (Porty)** wprowadź numery portów.
   - **SIP port (Port SIP)** – Port sieciowy wykorzystywany zazwyczaj do komunikacji SIP. Ruch sygnalizacyjny przez ten port nie jest szyfrowany. Domyślny numer portu to 5060. W razie potrzeby wprowadź inny numer portu.
   - **TLS port (Port TLS)** – Port sieciowy wykorzystywany do szyfrowanej komunikacji SIP. Ruch sygnalizacyjny za pośrednictwem tego portu jest szyfrowany przy użyciu Transport Layer Security (TLS). Domyślny numer portu to 5061. W razie potrzeby wprowadź inny numer portu.
   - **Port początkowy RTP** – wprowadź port używany do pierwszego strumienia mediów RTP w wywołaniu SIP. Domyślnym portem początkowym na potrzeby transportu multimediów jest port 4000. Niektóre zapory mogą blokować ruch RTP na określonych numerach portów. Numer portu musi należeć do przedziału od 1024 do 65535.
5. Wybierz protokoły, które chcesz włączyć dla funkcji **NAT traversal**.

Uwaga

Użyj opcji NAT traversal, gdy urządzenie jest podłączone do sieci za routerem NAT lub znajduje się za zaporą. Więcej informacji, p. sekcja *NAT traversal*.

6. W ustawieniu **Audio (Dźwięk)** wybierz co najmniej jeden kodek audio z żądaną jakością dźwięku na potrzeby połączeń SIP. W celu zmiany kolejności priorytetów przeciągnij i upuść w inne miejsca.
7. W obszarze **Additional (Dodatkowe)** wybierz dodatkowe opcje.
   - **UDP-to-TCP switching** (Przełączanie UDP–TCP) – Wybierz, aby umożliwić tymczasowe przełączenie protokołu transmisji z UDP (User Datagram Protocol) na TCP (Transmission Control Protocol). Przełączanie przydaje się w celu uniknięcia fragmentacji; przełączenie jest możliwe w zakresie 200 bajtów MTU lub więcej niż 1300 bajtów MTU.
   - **Allow via rewrite (Umożliwiaj przepisanie)** – Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
   - **Allow contact rewrite (Umożliwiaj przepisanie przy kontakcie)** – Wybierz, aby wysyłać lokalny adres IP zamiast publicznego adresu IP routera.
   - **Register with server every (Rejestruj na serwerze co)** – Ustaw częstotliwość rejestrowania się urządzenia na serwerze SIP dla istniejących kont SIP.
   - **DTMF payload type (Typ próbki DTMF)** – Zmienia domyślny typ próbki na DTMF.
8. Kliknij przycisk **Save (Zapisz)**.

Konfiguracja SIP przez serwer (PBX)

Użyj serwera PBX, gdy agenci użytkowników będą komunikować się w sieci IP i poza nią. W zależności od dostawcy usługi PBX można dodać dodatkowe funkcje.

Więcej informacji o ustawieniach, p. sekcja *SIP*.

1. Od dostawcy PBX należy uzyskać następujące informacje:

- ID użytkownika
- Domena
- Password (Hasło):
- ID uwierzytelniania
- ID rozmówcy
- Rejestrator
- Port początkowy RTP

2. Aby dodać nowe konto, przejdź do okna **System** > **SIP** > **SIP accounts (Konta SIP)** i kliknij przycisk **+ Account (+ Konto)**.
3. Wprowadź informacje otrzymane od dostawcy usług centrali telefonicznej (PBX).
4. Kliknij opcję **Registered (Zarejestrowane)**.
5. Wybierz tryb transmisji.
6. Kliknij przycisk **Save (Zapisz)**.
7. Skonfiguruj ustawienia SIP w taki samo sposób, jak peer-to-peer. Więcej informacji, p. sekcja *SIP*.

Konfiguracja reguł dotyczących zdarzeń

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

Wyzwalanie akcji

1. Przejdź do **System** > **Events** (System > Zdarzenia) i kliknij **+ Add a rule** (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 **Action (Akcję)**, która ma zostać wykonana po spełnieniu warunków.

Uruchamianie profilu po wyzwoleniu alarmu

W tym przykładzie wyjaśniono, w jaki sposób wyzwolić alarm po zmianie cyfrowego sygnału wejściowego.

Ustaw kierunek wejścia dla portu:

1. Przejdź do menu **System** > **Accessories** > **I/O ports** (System > Akcesoria > Porty we/wy).
2. Przejdź do obszaru **Port 1** > **Normal state** (Normalny stan) i kliknij **Circuit closed** (Obwód zamknięty).

Utwórz regułę:

1. Przejdź do menu **System** > **Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **I/O (We/Wy)** > **Digital input is active (Wejście cyfrowe jest aktywne)**.
4. Wybierz **Port 1**.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active** (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna).
6. Wybierz profil, który chcesz uruchomić.
7. Kliknij przycisk **Save (Zapisz)**.

Uruchamianie profilu przy użyciu protokołu SIP

Ten przykład objaśnia wyzwalanie alarmu za pomocą protokołu SIP.

Aktywowanie uwierzytelniania SIP:

1. Przejdź do menu **System** > **SIP** > **SIP settings (Ustawienia SIP)**.
2. Wybierz opcję **Enable SIP** (Włącz protokół SIP) i **Allow incoming calls** (Zezwalaj na połączenia przychodzące).
3. Kliknij przycisk **Save (Zapisz)**.

Utwórz regułę:

1. Przejdź do menu **System** > **Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call** (Połączenie) > **State** (Stan).
4. Na liście stanu wybierz pozycję **Active** (Aktywne).
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active** (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna).
6. Wybierz profil, który chcesz uruchomić.
7. Kliknij przycisk **Save (Zapisz)**.

Sterowanie kilkoma profilami za pomocą rozszerzeń SIP

Aktywowanie uwierzytelniania SIP:

1. Przejdź do menu **System** > **SIP** > **SIP settings (Ustawienia SIP)**.
2. Wybierz opcję **Enable SIP** (Włącz protokół SIP) i **Allow incoming calls** (Zezwalaj na połączenia przychodzące).
3. Kliknij przycisk **Save (Zapisz)**.

Utwórz regułę, aby uruchomić profil:

1. Przejdź do menu **System** > **Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call** (Połączenie) > **State change (Zmiana stanu)**.
4. Na liście przyczyn zaznacz opcję **Accepted by device (Zaakceptowane przez urządzenie)**.
5. W polu **Call direction (Kierunek połączenia)** zaznacz opcję **Incoming (Przychodzące)**.
6. W polu **Local SIP URI** (Lokalny URI SIP) wpisz wyrażenie **<sip:[numer wewnętrzny]@[adres IP]>**, gdzie [numer wewnętrzny] to numer wewnętrzny używany dla profilu, a [adres IP] to adres urządzenia. Na przykład **sip:1001@192.168.0.90**.
7. Na liście działań wybierz **Light and Siren** > **Run light and siren profile** (Sygnalizacja optyczna i akustyczna > Uruchom profil sygnalizacji optycznej i akustycznej).
8. Wybierz profil, który chcesz uruchomić.
9. Wybierz akcję **Start (Uruchamianie)**.
10. Kliknij przycisk **Save (Zapisz)**.

Utwórz regułę, aby zatrzymać profil:

1. Przejdź do menu **System** > **Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **Call** (Połączenie) > **State change (Zmiana stanu)**.
4. Na liście przyczyn zaznacz opcję **Terminated (Przerwane)**.
5. W polu **Call direction (Kierunek połączenia)** zaznacz opcję **Incoming (Przychodzące)**.
6. W polu **Local SIP URI (Lokalny URI SIP)** wpisz wyrażenie **sip:[numer wewnętrzny]@[adres IP]**, gdzie [numer wewnętrzny] to numer wewnętrzny używany dla profilu, a [adres IP] to adres urządzenia. Na przykład **sip:1001@192.168.0.90**.
7. Na liście działań wybierz **Light and Siren** > **Run light and siren profile** (Sygnalizacja optyczna i akustyczna > Uruchom profil sygnalizacji optycznej i akustycznej).
8. Wybierz profil, który chcesz zatrzymać.
9. Wybierz akcję **Stop (Zatrzymanie)**.
10. Kliknij przycisk **Save (Zapisz)**.

Powtórz te kroki, aby utworzyć reguły uruchamiania i zatrzymywania dla każdego profilu, który chcesz kontrolować za pomocą protokołu SIP.

Uruchamianie dwóch profili o różnych priorytetach

Jeśli uruchomione zostaną dwa profile o różnych priorytetach, wówczas profil o wyższym numerze priorytetu przerwie działanie profilu o niższym numerze priorytetu.

Uwaga

W przypadku uruchomienia profili z takim samym priorytetem, nowszy profil anuluje wcześniejszy profil.

W tym przykładzie pokazano, jak ustawić urządzenie, aby po wyzwoleniu przez cyfrowy port We/Wy był wyświetlany jeden profil o priorytecie 4 zamiast innego profilu o priorytecie 3.

Create profiles (Utwórz profile):

1. Utwórz profil o priorytecie 3.
2. Utwórz inny profil o priorytecie 4.

Utwórz regułę:

1. Przejdź do menu **System** > **Events** (System > Zdarzenia) i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków wybierz **I/O (We/Wy)** > **Digital input is active (Wejście cyfrowe jest aktywne)**.
4. Wybierz port.
5. Na liście akcji wybierz opcję **Run light and siren profile while the rule is active** (Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna).
6. Wybierz profil z najwyższym numerem priorytetu.
7. Kliknij przycisk **Save (Zapisz)**.
8. Przejdź do menu **Profiles** (Profile) i uruchom profil z najniższym numerem priorytetu.

Aktywowanie syreny stroboskopowej przez wejście wirtualne po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do syreny stroboskopowej oraz spowodować uaktywnianie się profilu w syrenie stroboskopowej po każdym wykryciu ruchu przez aplikację AXIS Motion Guard zainstalowaną w kamerze.

Zanim rozpoczniesz:

- Utwórz w syrenie stroboskopowej nowe konto z uprawnieniami Operatora lub Administratora.
- Utwórz profil w syrenie stroboskopowej.
- Skonfiguruj aplikację AXIS Motion Guard w kamerze i utwórz profil o nazwie „Profil kamery".

Utworzenie dwóch odbiorców w kamerze:

1. W interfejsie urządzenia kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Aktywacja portu wirtualnego
   - **Type (Typ)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/activate.cgi
     Zastąp element <adresIP> adresem syreny stroboskopowej.
   - Nazwa i hasło nowo utworzonego konta syreny stroboskopowej.
3. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk **Save (Zapisz)**.

5. Dodaj drugiego odbiorcę z następującymi informacjami:
   - **Name (Nazwa)**: Dezaktywacja portu wirtualnego
   - **Type (Typ)**: **HTTP**
   - **URL**: http://<IPaddress>/axis-cgi/virtualinput/deactivate.cgi
     Zastąp element <adresIP> adresem syreny stroboskopowej.
   - Nazwa i hasło nowo utworzonego konta syreny stroboskopowej.
6. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
7. Kliknij przycisk **Save (Zapisz)**.

Utworzenie dwóch reguł w kamerze:

1. Przejdź do obszaru **Rules (Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Aktywowanie wirtualnego WE/WY1
   - **Condition** (Warunek): **Applications > Motion Guard: Camera profile** (Aplikacje > Motion Guard: Profil kamery)
   - **Action** (Działanie): **Notifications > Send notification through HTTP** (Powiadomienia > Wyślij powiadomienie przez HTTP)
   - **Recipient** (Odbiorca): **Activate virtual port** (Uaktywnienie portu wirtualnego)
   - **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1
3. Kliknij przycisk **Save (Zapisz)**.
4. Dodaj kolejną regułę z następującymi informacjami:
   - **Name (Nazwa)**: Dezaktywacja wirtualnego WE/WY1
   - **Condition** (Warunek): **Applications > Motion Guard: Camera profile** (Aplikacje > Motion Guard: Profil kamery)
   - Wybierz opcję **Invert this condition (Odwróć ten warunek)**.
   - **Action** (Działanie): **Notifications > Send notification through HTTP** (Powiadomienia > Wyślij powiadomienie przez HTTP)
   - **Recipient** (Odbiorca): **Deactivate virtual port** (Dezaktywacja portu wirtualnego)
   - **Query string suffix (Sufiks ciągu zapytania)**: schemaversion=1&port=1
5. Kliknij przycisk **Save (Zapisz)**.

Utworzenie reguły w syrenie stroboskopowej:

1. W interfejsie WWW syreny stroboskopowej wybierz kolejno opcje **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Wyzwalacz w wirtualnym wejściu 1
   - **Condition (Warunek)**: **I/O (We/Wy) > Virtual input (Wejście wirtualne)**
   - **Port**: **1**
   - **Action** (Działanie): **Light and siren > Run light and siren profile while the rule is active** (Sygnalizacja optyczna i akustyczna > Uruchom profil sygnalizacji optycznej i akustycznej, gdy reguła jest aktywna)
   - **Profile (Profil)**: wybór nowo utworzonego profilu
3. Kliknij przycisk **Save (Zapisz)**.

Aktywowanie syreny stroboskopowej przez HTTP post po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do syreny stroboskopowej oraz spowodować uaktywnianie się profilu w syrenie stroboskopowej po każdym wykryciu ruchu przez aplikację AXIS Motion Guard zainstalowaną w kamerze.

Zanim rozpoczniesz:

- Utwórz w syrenie stroboskopowej nowego użytkownika z rolą Operator lub Administrator.
- Utwórz profil w syrenie stroboskopowej o nazwie: „Strobe siren profile" (Profil syreny stroboskopowej).
- Skonfiguruj aplikację AXIS Motion Guard w kamerze i utwórz profil o nazwie: „Camera profile" (Profil kamery).
- Upewnij się, że masz zainstalowaną aplikację AXIS Device Assistant i oprogramowanie sprzętowe w wersji 10.8.0 lub nowszej.

Tworzenie odbiorcy w kamerze:

1. W interfejsie urządzenia kamery przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Syrena stroboskopowa
   - **Type (Typ)**: **HTTP**
   - **URL**: http://<adresIP>/axis-cgi/siren_and_light.cgi
     Zastąp element <adresIP> adresem syreny stroboskopowej.
   - Nazwa i hasło nowo utworzonego użytkownika syreny stroboskopowej.
3. Kliknij przycisk **Test (Testuj)**, sprawdzić, czy wszystkie dane są prawidłowe.
4. Kliknij przycisk **Save (Zapisz)**.

Utworzenie dwóch reguł w kamerze:

1. Przejdź do obszaru **Rules (Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Aktywowanie syreny po wykryciu ruchu
   - **Condition** (Warunek): **Applications > Motion Guard: Camera profile** (Aplikacje > Motion Guard: Profil kamery)
   - **Action** (Działanie): **Notifications > Send notification through HTTP** (Powiadomienia > Wyślij powiadomienie przez HTTP)
   - **Recipient** (Odbiorca): **Syrena stroboskopowa**.
     Informacje te muszą być takie same, jak podane wcześniej w obszarze **Events > Recipients > Name (Zdarzenia > Odbiorcy > Nazwa)**.
   - **Method** (Metoda): **Post**
   - **Body (Treść)**:

```
{  "apiVersion": "1.0",  "method": "start",  "params": {
"profile" : "Strobe siren profile"  } }
```

Dla parametru '**"profile" : <>**' podaj dane wprowadzone na etapie tworzenia profilu dla syreny stroboskopowej, w tym przypadku: „Strobe siren profile" (Profil syreny stroboskopowej).

3. Kliknij przycisk **Save (Zapisz)**.
4. Dodaj kolejną regułę z następującymi informacjami:
   - **Name (Nazwa)**: Dezaktywowanie syreny po wykryciu ruchu
   - **Condition** (Warunek): **Applications > Motion Guard: Camera profile** (Aplikacje > Motion Guard: Profil kamery)
   - Wybierz opcję **Invert this condition (Odwróć ten warunek)**.

- **Action** (Działanie): **Notifications > Send notification through HTTP** (Powiadomienia > Wyślij powiadomienie przez HTTP)
- **Recipient** (Odbiorca): **Syrena stroboskopowa**
  Informacje te muszą być takie same, jak podane wcześniej w obszarze **Events > Recipients > Name (Zdarzenia > Odbiorcy > Nazwa)**.
- **Method** (Metoda): **Post**
- **Body (Treść)**:

```
{  "apiVersion": "1.0",  "method": "stop",  "params": {    "profile" : "Strobe siren profile"  } }
```

Dla parametru '**"profile" : <>**' podaj dane wprowadzone na etapie tworzenia profilu dla syreny stroboskopowej, w tym przypadku: „Strobe siren profile" (Profil syreny stroboskopowej).

5. Kliknij przycisk **Save (Zapisz)**.

Aktywowanie syreny stroboskopowej przez MQTT po wykryciu ruchu przez kamerę

W tym przykładzie wyjaśniono, jak podłączyć kamerę do syreny stroboskopowej przez MQTT oraz spowodować uaktywnianie się profilu w syrenie stroboskopowej po każdym wykryciu ruchu przez aplikację AXIS Motion Guard zainstalowaną w kamerze.

Zanim rozpoczniesz:

- Utwórz profil w syrenie stroboskopowej.
- Skonfiguruj brokera MQTT i uzyskaj adres IP oraz nazwę użytkownika i hasło brokera.
- Skonfiguruj w kamerze funkcję AXIS Motion Guard.

Konfigurowanie klienta MQTT w kamerze:

1. W interfejsie urządzenia kamery przejdź do **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wprowadź następujące informacje:
   - **Host**: Adres IP brokera
   - **Client ID (Identyfikator klienta)**: Na przykład Kamera 1
   - **Protocol (Protokół)**: Protokół, na który jest ustawiony broker
   - **Port**: Numer portu używany przez brokera
   - **Username (nazwa użytkownika)** i **Password (hasło)** brokera
2. Kliknij **Save (Zapisz)** i **Connect (Połącz)**.

Tworzenie dwóch reguł w kamerze w celu publikacji MQTT:

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Wykryto ruch
   - **Condition** (Warunek): **Applications > Motion alarm** (Aplikacje > Alarm ruchu)
   - **Action (Akcja)**: **MQTT > Send MQTT publish message (Wyślij wiadomość o publikacji MQTT)**
   - **Topic (Temat)**: Ruch
   - **Payload (Próbka)**: Wł.
   - **QoS**: 0, 1 lub 2
3. Kliknij przycisk **Save (Zapisz)**.
4. Dodaj kolejną regułę z następującymi informacjami:
   - **Name (Nazwa)**: Brak ruchu
   - **Condition** (Warunek): **Applications > Motion alarm** (Aplikacje > Alarm ruchu)
     - Wybierz opcję **Invert this condition (Odwróć ten warunek)**.

- **Action (Akcja)**: **MQTT > Send MQTT publish message (Wyślij wiadomość o publikacji MQTT)**
- **Topic (Temat)**: Ruch
- **Payload (Próbka)**: Wył.
- **QoS**: 0, 1 lub 2

5. Kliknij przycisk **Save (Zapisz)**.

Konfigurowanie klienta MQTT w syrenie stroboskopowej:

1. W interfejsie urządzenia syreny stroboskopowej przejdź do **System > MQTT > MQTT client > Broker (System > MQTT > Klient MQTT > Broker)** i wprowadź następujące informacje:
   - **Host**: Adres IP brokera
   - **Client ID (Identyfikator klienta)**: Syrena 1
   - **Protocol (Protokół)**: Protokół, na który jest ustawiony broker
   - **Port**: Numer portu używany przez brokera
   - **Username (Nazwa użytkownika)** i **Password (Hasło)**
2. Kliknij **Save (Zapisz)** i **Connect (Połącz)**.
3. Przejdź do **MQTT subscriptions (Subskrypcje MQTT)** i dodaj subskrypcję.
   Wprowadź następujące informacje:
   - **Subscription filter (Filtr subskrypcyjny)**: Ruch
   - **Subscription type (Typ subskrypcji)**: Ze stanem
   - **QoS**: 0, 1 lub 2
4. Kliknij przycisk **Save (Zapisz)**.

Tworzenie reguły w syrenie i przeglądarce w odniesieniu do subskrypcji MQTT:

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
   - **Name (Nazwa)**: Wykryto ruch
   - **Condition (Warunek)**: **MQTT > Stateful (Ze stanem)**
   - **Subscription filter** (Filtr subskrypcyjny): **Motion** (Ruch)
   - **Payload (Próbka)**: Wł.
   - **Action** (Działanie): **Light and siren > Run light and siren profile while the rule is active** (Sygnalizacja optyczna i akustyczna > Uruchom profil sygnalizacji optycznej i akustycznej, gdy reguła jest aktywna)
   - **Profile (Profil)**: Wybierz profil, który ma być aktywny.
3. Kliknij przycisk **Save (Zapisz)**.

Interfejs WWW

Aby zapoznać się ze wszystkimi funkcjami i ustawieniami znajdującymi się w interfejsie internetowym urządzeń z systemem AXIS OS, przejdź do sekcji *Pomoc dotycząca interfejsu internetowego systemu AXIS OS*.

Dowiedz się więcej

Protokół inicjacji sieci (Session Initiation Protocol, SIP)

Protokół inicjacji sieci (SIP) jest stosowany do konfiguracji, utrzymywania i kończenia połączeń VoIP. Połączenia można wykonywać pomiędzy dwoma rozmówcami lub większą ich liczbą (tzw. agentami użytkowników SIP). Aby wykonać połączenie SIP, można skorzystać na przykład z telefonów SIP, softphone'ów lub urządzeń Axis obsługujących SIP.

Sygnał audio i wideo jest wymieniany pomiędzy agentami użytkowników SIP z użyciem protokołu transmisji, takiego jak RTP (Real-Time Transport Protocol).

W sieci lokalnej można nawiązywać połączenia w konfiguracji peer-to-peer, a pomiędzy sieciami – za pomocą PBX.

Peer-to-peer SIP (P2PSIP)

Podstawowa komunikacja SIP odbywa się bezpośrednio pomiędzy dwoma lub większą liczba agentów użytkowników SIP. Połączenie takie nazywane jest peer-to-peer SIP (P2PSIP). Jest ono wykonywane w sieci lokalnej i wymaga jedynie adresów SIP agentów użytkowników. Adres SIP to zazwyczaj `sip:<local-ip>`.

Private Branch Exchange (PBX) – centrala abonencka

Podczas wykonywania połączeń SIP poza lokalną sieć IP PBX może służyć za centralkę. Głównym elementem PBX jest serwer SIP, zwany również serwerem proxy SIP lub rejestratorem. PBX działa jak tradycyjna centralka telefoniczna, wyświetla bieżący status klienta i umożliwia na przykład przekazywanie połączeń, rejestrację wiadomości głosowym i przekierowania.

Serwer SIP PBX można skonfigurować lokalnie lub zdalnie. Można go umieścić w intranecie lub u zewnętrznego dostawcy usług serwerowych. Podczas wykonywania połączeń SIP pomiędzy sieciami połączenia są przekazywane przez zestaw PBX, które wysyłają zapytania o lokalizację docelowego adresu SIP.

Każdy agent użytkownika SIP jest rejestrowany w PBX; mogą łączyć się z innymi poprzez wybranie właściwego numeru wewnętrznego. Typowy adres SIP w tym przypadku to `sip:<user>@<domain>` lub `sip:<user>@<registrar-ip>`. Adres SIP jest niezależny od adresu SIP, a PBX udostępnia urządzenie przez cały czas, kiedy jest ono zarejestrowane.

NAT Transversal

Użyj NAT (Network Address Translation), gdy urządzenie Axis znajduje się w prywatnej sieci (LAN) i chcesz uzyskać do niego dostęp spoza tej sieci.

Uwaga

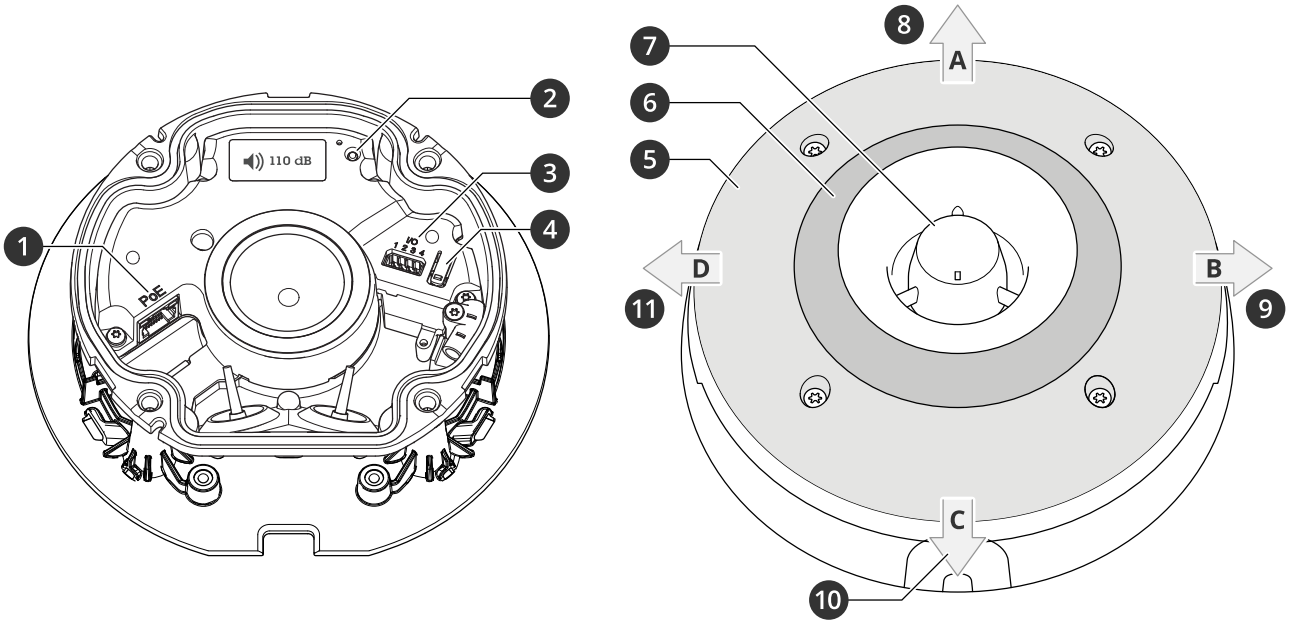
Router musi również obsługiwać NAT Traversal i protokół UPnP®.

Każdy protokół NAT traversal może być używany oddzielnie lub w różnych kombinacjach w zależności od środowiska sieciowego.

- Protokół **ICE** (Interactive Connectivity Establishment) zwiększa szanse na wyszukanie najlepszej ścieżki komunikacji między urządzeniami typu peer. Szanse na wykorzystanie protokołu ICE można zwiększyć po włączeniu STUN i TURN.
- **STUN** (Session Traversal Utilities for NAT) to protokół sieciowy klient-serwer umożliwiający urządzeniom Axis określenie, czy znajduje się on za NAT lub zaporą, a następnie uzyskanie zmapowanego publicznego adresu IP i numeru portu przypisanego do połączeń ze zdalnymi hostami. Wprowadź adres serwera STUN, na przykład adres IP.
- **TURN** (Traversal Using Relays around NAT) to protokół umożliwiający urządzeniem za routerem NAT lub zaporą otrzymywanie danych z innych hostów (poprzez TCP lub UDP). Wprowadź adres serwera TURN i dane logowania.

Specyfikacje

Przegląd produktów



1 *Złącze sieciowe PoE*
2 *Wskaźnik LED stanu*
3 *Złącze I/O*
4 *Przycisk kontrolny*
5 *Białe diody LED*
6 *Diody LED RGBA (czerwone, niebieskie, zielone, bursztynowe)*
7 *Siren (Syrena):*
8 *Kierunek oświetlenia A*
9 *Kierunek oświetlenia B*
10 *Kierunek oświetlenia C*
11 *Kierunek oświetlenia D*

Wskaźniki LED

Dioda stanu	Wskazanie
Zielony	Stałe zielone światło przez 10 sekund przy normalnym działaniu po zakończeniu uruchamiania.
Bursztynowy	Stałe światło podczas uruchamiania, przywracania domyślnych ustawień fabrycznych lub odtwarzania ustawień.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 23*.
- 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

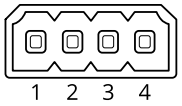
Złącze RJ45 Ethernet z zasilaniem Power over Ethernet (PoE).

Złącze I/O

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.

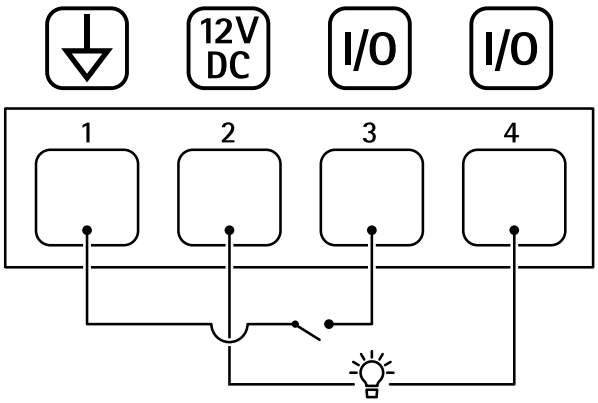
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

4-pinowy blok złączy



Funkcja	Pin	Uwagi	Specyfikacje
Masa DC	1		0 V DC
Wyjście DC	2	⚠ Może być wykorzystywane do zasilania dodatkowego sprzętu. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 50 mA
Konfigurowalne (wejście lub wyjście)	3-4	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe — podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku stosowania z obciążeniem indukcyjnym, np. przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 30 V DC, otwarty dren, 100 mA

Przykład:



1 *Masa DC*
2 *Wyjście DC 12 V, maks. 50 mA*
3 *We/Wy skonfigurowane jako wejście*
4 *We/Wy skonfigurowane jako wyjście*

Nazwy wzorów świateł

Wył.
Stałe światło
Stałe białe + błyskające kolorowe
Alternatywna
Pulse (Impuls):
Nasilanie w 3 stopniach
Miganie
Miganie 3x
Miganie 4x
Miganie 3x i zanikanie
Miganie 4x i zanikanie
Błysk 1x
Błysk 3x
Błysk 1x białe + stałe kolorowe
Błysk 3x białe + stałe kolorowe
Kierunek A + stałe kolorowe
Kierunek B + stałe kolorowe
Kierunek C + stałe kolorowe
Kierunek D + stałe kolorowe
Obrotowe białe + stałe kolorowe
Obrotowe białe z tyłu + stałe kolorowe
Losowe białe + stałe kolorowe
Wirujące białe + stałe kolorowe
Stałe białe + stałe kolorowe

Nazwy wzorów dźwiękowych

Wył.
Alarm: Alarm o wysokich tonach dźwięku
Alarm: Alarm o niskich tonach dźwięku
Alarm: Ptak
Alarm: Syrena na łodzi
Alarm: Alarm samochodowy
Alarm: Szybki alarm samochodowy
Alarm: Zegar klasyczny

Alarm: Pierwszy gość
Alarm: Horror
Alarm: Przemysł
Alarm: Pojedynczy sygnał dźwiękowy
Alarm: Łagodny sygnał dźwiękowy quada
Alarm: Łagodny potrójny sygnał dźwiękowy
Alarm: Potrójny o wysokich tonach dźwięku
Powiadomienie: Odmowa
Powiadomienie: Gotowe
Powiadomienie: Wejście
Powiadomienie: Failed (Niepowodzenie):
Powiadomienie: Pośpiesz się
Powiadomienie: Wiadomość
Powiadomienie: Dalej
Powiadomienie: Otwarte
Siren (Syrena): Alternatywna
Siren (Syrena): Piłka
Siren (Syrena): Ewakuacja
Siren (Syrena): Dźwięk o opadającej wysokości
Siren (Syrena): Łagodny domowy

Czyszczenie urządzenia

Do czyszczenia sprzętu można używać wody z mydłem niezawierającym środków ściernych.

POWIADOMIENIE

- Silne chemikalia mogą uszkodzić urządzenie. Nie należy czyścić urządzenia środkami, takimi jak płyn do mycia okien lub aceton.
- Nie należy czyścić urządzenia w bezpośrednim świetle słonecznym ani w wysokiej temperaturze, ponieważ może to powodować pozostawanie plam na obudowie.

1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
2. W razie potrzeby można wyczyść urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą i łagodnym mydłem niezawierającym środków ściernych.
3. Aby usunąć jakiekolwiek pozostałości środków czyszczących, należy przetrzeć urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą.
4. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

Więcej informacji na temat czyszczenia urządzeń Axis znajduje się w białej księdze *Odporność chemiczna na popularne środki czyszczące*.

Rozwiązywanie problemów

Przywracanie domyślnych ustawień fabrycznych

Ważne

Przywracanie ustawień fabrycznych powinno być dokonywane ze szczególną ostrożnością. Przywrócenie ustawień fabrycznych oznacza zresetowanie wszystkich ustawień, łącznie z adresem IP, do wartości fabrycznych.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk kontrolny i włącz zasilanie. Zob. *Przegląd produktów, on page 18*.
3. Przytrzymuj przycisk Control przez 15–30 sekund, aż wskaźnik LED stanu zacznie migać na bursztynowo.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Jeśli w sieci nie jest dostępny serwer DHCP, zostanie zastosowany domyślny adres IP urządzenia (jeden z poniższych):
   - **Urządzenia z oprogramowaniem AXIS OS w wersji 12.0 i nowszej**: Pobrane z podsieci adresów lokalnych (169.254.0.0/16)
   - **Urządzenia z systemem AXIS OS 11.11 lub starszym:** 192.168.0.90/24
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do urządzenia.
   Narzędzia do instalacji i zarządzania są dostępne na stronach pomocy technicznej *axis.com/support*.

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

Opcje systemu AXIS OS

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

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

Sprawdzanie bieżącej wersji systemu AXIS OS

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

Aby sprawdzić bieżącą wersję systemu AXIS OS:

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

Aktualizacja systemu AXIS OS:

Ważne

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

Uwaga

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

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. Jeżeli zostanie zwrócony komunikat: `Reply from <IP address>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci IP. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie urządzenie.
  4. Jeżeli zostanie zwrócony komunikat: `Request timed out` (Upłynął limit czasu żądania), oznacza to, że adres IP jest dostępny i może zostać przypisany do urządzenia Axis. Sprawdź całe okablowanie i zainstaluj urządzenie ponownie.
- Może występować potencjalny konflikt adresu IP z innym urządzeniem w tej samej podsieci. Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP urządzenia Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do urządzenia.

Problemy z dostępem do urządzenia

Nie można się zalogować podczas dostępu do urządzenia z poziomu przeglądarki

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

Jeśli hasło do konta root zostało utracone, należy zresetować urządzenie do domyślnych ustawień fabrycznych. Instrukcje p. *Przywracanie domyślnych ustawień fabrycznych, on page 23*.

Serwer DHCP zmienił adres IP

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

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

Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X

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

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, p. *Obsługiwane przeglądarki, on page 5*.

Nie można uzyskać dostępu do urządzenia z zewnątrz

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

- AXIS Camera Station Edge: darmowa aplikacja idealna do małych systemów o niewielkich wymaganiach w zakresie dozoru.
- AXIS Camera Station Pro: 90-dniowa darmowa wersja próbna, idealna do małych i średnich systemów.

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

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

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

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

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

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

Wystąpiły problemy z dźwiękiem	
Urządzenie nie jest tak głośne, jak oczekiwano	Sprawdź, czy urządzenie jest prawidłowo zamknięte i czy w tubie lub na elemencie głośnikowym nie ma występują żadne przeszkody.
Urządzenie nie emituje żadnych dźwięków	Sprawdź, czy urządzenie jest w trybie **Maintenance (Konserwacja)**. Jeśli jest w trybie konserwacji, wyłącz go.

Problemy ze światłem	
Urządzenie nie jest tak jasne, jak oczekiwano	Sprawdź, czy używany jest zasilacz PoE klasy 4. Sprawdź, jaka jest temperatura otoczenia urządzenia. Jeśli urządzenie działa w środowisku, w którym panuje wysoka temperatura, światła zostaną automatycznie przyciemnione.

Kwestie wydajności

Najważniejsze czynniki, które należy uwzględnić:

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

Kontakt z pomocą techniczną

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

Cyberbezpieczeństwo

Bezpieczeństwo cybernetyczne jest składnikiem udanego cyklu eksploatacji produktu dzięki minimalizacji narażeń. Szczegółowe informacje i dokumentacja na temat naszego podejścia do bezpieczeństwa cybernetycznego znajdują się na stronie *axis.com/about-axis/cybersecurity*. Przestrzegaj poniższych wytycznych dotyczących bezpieczeństwa cybernetycznego, aby otrzymywać powiadomienia od Axis dotyczące bezpieczeństwa produktów oraz skonfigurować produkt w sposób zapewniający bezpieczny cykl eksploatacji oraz wycofanie z użytku.

Na stronie *Axis Trust Center* znajdują się informacje o sposobach, w jakie Axis zapewnia zgodność z wymogami bezpieczeństwa, transparentność, ochronę danych oraz ochronę prywatności.

Zarządzanie podatnościami

Axis ma status *Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA)*. Aby zminimalizować ryzyko narażenia na zagrożenia, postępujemy zgodnie z branżowymi normami w zakresie wykrywania i usuwania luk w zabezpieczeniach naszych urządzeń, oprogramowania i usług. Informacje na temat naszej polityki zarządzania lukami w zabezpieczeniach oraz instrukcje dotyczące zgłaszania luk znajdują się na stronie *axis.com/vulnerability-management*.

Powiadomienia dotyczące zabezpieczeń

Subskrybuj powiadomienia o zagrożeniach bezpieczeństwa w produktach Axis na stronie *axis.com/security-notification-service*. Będziemy informować Cię o lukach w zabezpieczeniach, udzielać odnośnych wskazówek oraz powiadamiać o innych kwestiach związanych z bezpieczeństwem użytkowanego produktu Axis.

Bezpieczny cykl eksploatacji produktu

Axis minimalizuje ryzyko w całym cyklu eksploatacji swoich produktów dzięki bezpiecznemu zarządzaniu cyklem eksploatacji. Skorzystaj z naszych przewodników dotyczących zwiększenia bezpieczeństwa dostępnych na stronie *help.axis.com*, aby bezpieczniej konfigurować i obsługiwać produkty Axis oraz uzyskać informacje na poniższe tematy:

Bezpieczne pierwsze użycie – Produkty Axis są skonfigurowane fabrycznie z wysokim poziomem domyślnej ochrony, co oznacza bezpieczną pierwszą konfigurację oraz szyfrowaną komunikację od samego początku użytkowania.

Przeznaczenie i typowe błędy w konfiguracji – Nasze przewodniki zawierają informacje o przeznaczeniu produktów Axis, w tym o typowych błędach użytkowania związanych z bezpieczeństwem oraz błędach przy konfiguracji, których należy unikać.

Zarządzanie lukami w zabezpieczeniach i transparentność łańcucha dostaw – Wraz z każdą wersją oprogramowania na stronie *axis.com* publikowany jest wykaz komponentów oprogramowania (SBOM – Software Bill of Material) w celu poinformowania o lukach w zabezpieczeniach (podatnościach na zagrożenie) oraz zwiększenia transparentności łańcucha dostaw.

Wycofanie z eksploatacji i bezpieczne usuwanie danych – Aby bezpiecznie wycofać produkt po zakończeniu cyklu eksploatacji, przywróć jego ustawienia fabryczne. Spowoduje to usunięcie konfiguracji, zapisanych danych oraz informacji poufnych.

T10223803_pl

2026-10 (M7.2)

© 2025 – 2026 Axis Communications AB