AXIS TP3604-E Cellular Back Box

Podręcznik użytkownika

Spis treści

Instalacja 3
Od czego zacząć 4
Wyszukiwanie urządzenia w sieci 4
Obsługiwane przeglądarki 4
Otwieranie interfejsu WWW urządzenia 4
Utwórz konto administratora 4
Bezpieczne hasła 4
Upewnianie się co do braku zmian w oprogramowaniu urządzenia 5
Konfiguracja urządzenia 6
Zarządzanie kartą SIM 6
Ustawianie nazwy APN 6
Sprawdzanie siły sygnału i adresu IP 6
Testowanie połączenia 6
Sprawdzanie portów zarządzania 6
Włączanie przekierowywania do kamery 7
Konfigurowanie przypisania adresu IP do kamery 7
Tryb lokalny 8
Tryb passthrough 8
Konfiguracja reguł dotyczących zdarzeń 9
Wyzwalanie akcji 9
Wyzwalanie powiadomienia po otwarciu obudowy 9
Interfejs WWW 11
Specyfikacje 12
Przegląd produktów 12
Wskaźniki LED 12
Przyciski 13
Przycisk kontrolny 13
Złącza 13
Złącze wejściowe PoE (PoE in) 13
Złącze sieciowe (wyjście PoE) 13
Złącze zasilania 13
Czyszczenie urządzenia 14
Rozwiązywanie problemów 15
Przywracanie domyślnych ustawień fabrycznych 15
Opcje systemu AXIS OS 15
Sprawdzanie bieżącej wersji systemu AXIS OS 15
Aktualizacja systemu AXIS OS: 16
Problemy techniczne i możliwe rozwiązania 16
Kontakt z pomocą techniczną 18
Cyberbezpieczeństwo 19
Zarządzanie podatnościami 19
Powiadomienia dotyczące zabezpieczeń 19
Bezpieczny cykl eksploatacji produktu 19

Instalacja



Wideo pokazuje, jak zainstalować puszkę montażową AXIS TP3604-E Cellular Back Box wraz z kamerami kopułkowymi z serii AXIS P32 Dome Camera Series oraz kamerami z serii AXIS P14 Bullet Camera Series.

Instrukcje dotyczące wszystkich scenariuszy instalacji oraz informacje dotyczące bezpieczeństwa znajdują się w instrukcji instalacji.

Od czego zacząć

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 4*.

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

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę konta.
2. Wprowadź hasło. Zob. *Bezpieczne hasła, on page 4*.
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.

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. Skonfiguruj i zainstaluj urządzenie.

Konfiguracja urządzenia

Aby skonfigurować urządzenie, należy wykonać następujące czynności:

1. *Zarządzanie kartą SIM, on page 6*
2. Jeśli sieć wymaga podania konkretnej nazwy punktu dostępowego (APN), *Ustawianie nazwy APN, on page 6*
3. *Sprawdzanie siły sygnału i adresu IP, on page 6*
4. *Testowanie połączenia, on page 6*
5. *Sprawdzanie portów zarządzania, on page 6*
6. *Włączanie przekierowywania do kamery, on page 7*

Zarządzanie kartą SIM

Zarządzanie kartą SIM jest obowiązkowe, jeśli jest włączony kod PIN karty SIM. Jeśli kod PIN karty SIM jest wyłączony, możesz pominąć ten krok.

1. Włóż kartę SIM. Przejdź do **Modem > SIM management > SIM status (Modem > Zarządzanie kartą SIM > Stan karty SIM)**, aby sprawdzić wynik detekcji modemu / karty SIM.
2. Jeśli kod PIN karty SIM jest zablokowany, przejdź do **Modem > SIM management > SIM PIN > Unlock (Modem > Zarządzanie kartą SIM > Kod PIN karty SIM > Odblokuj)**, aby odblokować go za pomocą prawidłowego kodu PIN.

Ustawianie nazwy APN

Uwaga

Ten krok należy wykonać tylko wtedy, gdy sieć wymaga podania konkretnej nazwy punktu dostępowego (APN).

Aby ustawić konkretną nazwę APN, przejdź do **Modem > Cellular network > APN (Modem > Sieć komórkowa > APN)**.

Sprawdzanie siły sygnału i adresu IP

Uwaga

Ten krok wymaga dostępu do sieci komórkowej.

1. Sprawdź siłę sygnału, wybierając opcje **System > Modem > Cellular network > Radio parameters > Signal strength index (System > Modem > Sieć komórkowa > Parametry radiowe > Wskaźnik siły sygnału)**. Trzy lub cztery kreski oznaczają dobrą jakość sygnału.
2. Wybierając **System > Modem > Cellular network > User equipment IP address (System > Modem > Sieć komórkowa > Adres IP urządzenia użytkownika)**, sprawdź, czy został odebrany adres IP sieci komórkowej.

Testowanie połączenia

Uwaga

Ten krok wymaga dostępu do sieci komórkowej.

1. Przejdź do **System > Modem > Cellular network > Test cellular connection (System > Modem > Sieć komórkowa > Test połączenia komórkowego)**. Wprowadź nazwę hosta lub adres IP.
2. Sprawdź, czy test połączenia zakończył się pomyślnie.

Sprawdzanie portów zarządzania

Przed włączeniem trybu routingu końcowego należy sprawdzić porty zarządzania na puszce montażowej.

1. Przejdź do **Cellular routing > Back box management ports (Routing komórkowy > Porty zarządzania puszką montażową)**.
2. Zmień numery portów, jeśli domyślne wartości nie są obsługiwane przez sieć.

Włączanie przekierowywania do kamery

Ostatnim krokiem jest włączenie przekierowywania do kamery.

1. Przejdź do **Cellular routing > Main mode (Routing komórkowy > Tryb główny** i kliknij opcję **Enable forwarding to connected device (Włącz przekierowywanie do podłączonego urządzenia)**.

Po włączeniu przekierowywania standardowe porty usług są przekierowywane do kamery, a zarządzanie puszką montażową pozostaje dostępne poprzez zarezerwowane porty zarządzania.

2. Przetestuj dostęp do kamery: W przeglądarce internetowej wpisz adres IP sieci komórkowej, a następnie numer portu 80, np. `http://<cellular-ip-address>:80`.
3. Przetestuj dostęp do puszki montażowej: W przeglądarce internetowej wpisz adres IP sieci komórkowej, a następnie numer portu 11080 (domyślny port zarządzania puszką montażową dla protokołu HTTP), `http://<cellular-ip-address>:11080`.

Konfigurowanie przypisania adresu IP do kamery

Uwaga

Ten krok jest opcjonalny i wymagany tylko wtedy, gdy chcesz zmienić domyślne zachowanie podsieci lub dostosować jej działanie.

Sieć komórkowa przydziela tylko jeden adres IP, który jest powiązany z identyfikatorem karty SIM. Standardowa instalacja obejmuje puszkę montażową i podłączoną kamerę. Tryb DHCP decyduje o tym, jaki adres IP zostanie przypisany do kamery. To właśnie ta kluczowa decyzja decyduje o wyborze trybu serwera DHCP.

Domyślnie (tryb lokalny) adres IP sieci komórkowej pozostaje przypisany do puszki montażowej, a kamerze przydzielany jest prywatny adres IP z sieci lokalnej puszki montażowej. Kamera jest nadal w pełni osiągalna z sieci komórkowej. W przypadku większości wdrożeń to wystarczy, a dzięki temu kamera pozostaje bezpiecznie odizolowana w sieci prywatnej.

Różnica staje się widoczna, gdy narzędzie analizuje adres IP z perspektywy samej kamery. Jeśli system VMS odczytuje adres IP zgłaszany przez kamerę lub jeśli kamera jest skonfigurowana tak, by umieszczać swój adres IP w nakładce wideo, adres ten będzie prywatnym adresem IP kamery w sieci LAN, a nie publicznym adresem IP sieci komórkowej, z którego korzystają użytkownicy z zewnątrz, aby się z nią połączyć. Te dwa adresy nie są zgodne, ponieważ adres IP sieci komórkowej należy do identyfikatora karty SIM przechowywanego w puszce montażowej, a nie w kamerze.

Tryb passthrough rozwiązuje ten problem, pobierając pojedynczy adres IP, który sieć komórkowa przydziela do puszki montażowej, i przekierowując go do kamery. Gdy tryb passthrough jest włączony, kamera posiada dokładnie ten sam adres IP, co sieć komórkowa, więc adres zgłaszany przez kamerę (i wyświetlany w nakładce wideo) jest tym samym adresem, którego należy użyć, aby połączyć się z nią zdalnie. Ponieważ kamera posiada teraz identyfikator sieci komórkowej, wybór ten wpływa również na sposób, w jaki może ona nawiązywać połączenia z innymi urządzeniami użytkownika (UE) w sieci komórkowej.

W dalszej części tego rozdziału szczegółowo opisano każdy z tych trybów.

Dostęp do kamery podłączonej do puszki montażowej można uzyskać przez adres IP sieci komórkowej na standardowych portach (`80/443/554/22`), a do samej puszki montażowej nadal można uzyskać dostęp przez zarezerwowane porty zarządzania (na przykład `11080/11443/11554/11022`).

Różnica między trybem lokalnym a trybem passthrough:

Tryb lokalny

- Do kamery przydzielana jest prywatna podsieć lokalna.
- Wewnętrzny adres IP kamery różni się od adresu IP, pod którym można się z nią połączyć za pośrednictwem sieci komórkowej.

- W razie wątpliwości należy skorzystać z opcji trybu lokalnego DHCP.

Tryb passthrough

- Do kamery przydzielany jest adres IP sieci komórkowej.

Tryb lokalny

Włączanie trybu lokalnego

1. W menu **Cellular routing > Advanced DHCP configuration > DHCP server mode (Routing komórkowy > Zaawansowana konfiguracja DHCP > Tryb serwera DHCP** wybierz opcję **Local (Lokalny)**.
2. Sprawdź, czy lokalny adres IP kamery nie koliduje z żadnym innym dostępnym adresem IP w sieci: **Cellular routing > Advanced DHCP configuration > Local private network configuration (Routing komórkowy > Zaawansowana konfiguracja DHCP > Konfiguracja lokalnej sieci prywatnej)**
3. W razie potrzeby zmień adres IP w menu **Cellular routing > Advanced DHCP configuration > Local private network configuration (Routing komórkowy > Zaawansowana konfiguracja DHCP > Konfiguracja lokalnej sieci prywatnej**. W polach **Starting IP address (Początkowy adres IP)** i **Ending IP address (Końcowy adres IP)** należy wpisać tę samą wartość.
4. Kliknij przycisk **Save (Zapisz)**.

Tryb passthrough

Jeśli urządzenia użytkownika (UE, tj. kamery) nie komunikują się ze sobą, a ruch zawsze pochodzi z innej sieci LAN systemu VMS i jest kierowany do urządzeń UE, nie ma ścieżki między urządzeniami UE, która umożliwiałaby zacienianie adresu IP (IP shadowing). W takim przypadku tryb passthrough jest uznawany za bezpieczny z punktu widzenia ryzyka IP shadowingu.

W ogólnym ujęciu oznacza to, że sieć komórkowa jest rozszerzona w kierunku kamery. Jest to przydatne, gdy kamera powinna być widoczna bezpośrednio pod adresem IP przypisanym do sieci komórkowej.

Ważne ryzyko: Zacienianie adresu IP w trybie passthrough

Niniejszy opis ryzyka dotyczy konfiguracji z jedną kamerą. Nawet w przypadku jednej kamery tryb passthrough nadal wymaga dwóch adresów IP w podsieci po stronie sieci LAN:

- Jeden adres IP dla kamery.
- Jeden adres IP dla serwera DHCP puszki montażowej po stronie sieci Ethernet.

Scenariusz 1: Minimalna podsieć na urządzenie UE `(/30)`

W tym modelu każde urządzenie UE posiada oddzielną, niewielką podsieć.

- `(/30)` zapewnia dwa adresy IP hosta, z których można korzystać.
- Jeden adres IP jest używany przez kamerę.

Wolny adres IP jest wykorzystywany wewnętrznie przez serwer DHCP puszki montażowej.

Zalecenie dotyczące scenariusza 1:

- Zachowaj odrębność każdej podsieci UE.
- Upewnij się, że każda podsieć UE jest unikalna. Nie dopuszczaj do nakładania się podsieci między urządzeniami UE.

Scenariusz 2: Większa podsieć współdzielona przez wiele urządzeń UE

W niektórych wdrożeniach stosuje się jedną większą podsieć, z której korzysta wiele urządzeń UE. Ryzyko shadowingu pojawia się, gdy kamera próbuje nawiązać połączenie z innym urządzeniem UE, które korzysta z tego samego adresu IP co serwer DHCP puszki montażowej. W takim przypadku ruch sieciowy może zostać skierowany na lokalny adres po stronie puszki montażowej, a nie na docelowe zdalne urządzenie UE.

Zalecenie dotyczące scenariusza 2:

- Sprawdź adres IP serwera DHCP puszki montażowej w ustawieniach trybu passthrough.
- Upewnij się, że ten adres IP nie jest przydzielany do żadnego innego urządzenia UE.
- Upewnij się, że ten adres IP nie jest przydzielany do żadnej karty SIM w portalu usług sieciowych.

Włączanie trybu passthrough

Uwaga

Wymagany jest dostęp do sieci komórkowej.

1. W menu **Cellular routing > Advanced DHCP configuration > DHCP server mode (Routing komórkowy > Zaawansowana konfiguracja DHCP > Tryb serwera DHCP** wybierz opcję **Passthrough**.
2. W menu **Cellular routing > Advanced DHCP configuration > Local private network configuration > Server IP and prefix length (Routing komórkowy > Zaawansowana konfiguracja DHCP > Konfiguracja lokalnej sieci prywatnej > Adres IP serwera i długość prefiksu)** sprawdź, czy automatycznie wybrany adres IP serwera i długość prefiksu podsieci nie kolidują z innymi dostępnymi adresami IP.
3. Kliknij przycisk **Save (Zapisz)**.

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.

Wyzwalanie powiadomienia po otwarciu obudowy

W tym przykładzie wyjaśniono, jak ustawić powiadomienie e-mail wyzwalane w przypadku otwarcia obudowy urządzenia.

Dodaj odbiorcę wiadomości e-mail:

1. Przejdź do **System (System) > Events (Zdarzenia) > Recipients (Odbiorcy)** i kliknij **Add recipient (Dodaj odbiorcę)**.
2. Wprowadź nazwę odbiorcy.
3. Wybierz **Email (E-mail)** jako typ powiadomienia.
4. Wpisz adres e-mail odbiorcy.
5. Wpisz adres e-mail, z którego kamera ma wysyłać powiadomienia.
6. Podaj dane logowania do konta, z którego wysyłane są powiadomienia wraz z nazwą hosta SMTP i numerem portu.
7. Aby przetestować ustawienia poczty e-mail, kliknij **Test** (Testuj).
8. Kliknij przycisk **Save (Zapisz)**.

Utwórz regułę:

9. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i kliknij **Add a rule (Dodaj regułę)**.
10. Wprowadź nazwę reguły.
11. Z listy warunków wybierz opcję **Casing open (Otwarcie obudowy)**.

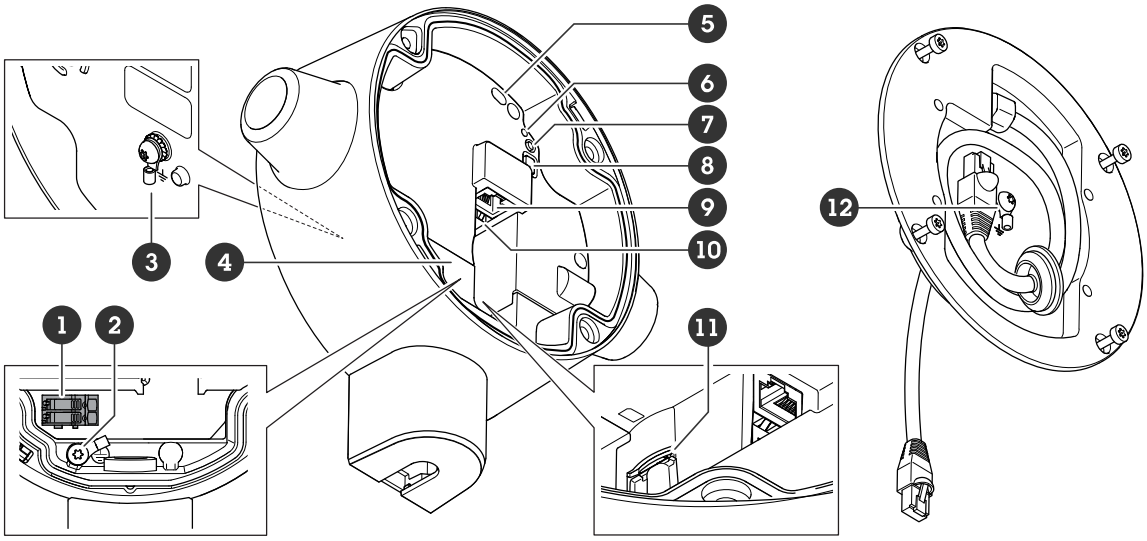
12. Z listy akcji wybierz opcję **Send notification to email (Wyślij powiadomienie przez email)**.
13. Wybierz odbiorcę z listy.
14. Wpisz temat i treść wiadomości e-mail.
15. Kliknij przycisk **Save (Zapisz)**.

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*.

Specyfikacje

Przegląd produktów



1 *Złącze prądu przemiennego*
2 *Uziemienie ochronne*
3 *Śruba uziemienia*
4 *Osłona ochronna (AC)*
5 *Czujnik otwarcia obudowy*
6 *Przycisk resetowania*
7 *Dioda stanu*
8 *Przycisk kontrolny*
9 *Wyjście PoE (dane)*
10 *Wejście PoE*
11 *Slot karty SIM*
12 *Śruba uziemienia (kamera)*

Wskaźniki LED

Dioda stanu w trybie konfiguracji

Dioda stanu	Wskazanie
Wyłączona	Czujnik IR detekcji obudowy jest zasłonięty.
Zielony	Normalne działanie, interfejs Ethernet jest gotowy.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.
Bursztynowy/ czerwony	Brak połączenia Ethernet, trwa konfiguracja modemu podczas uruchamiania.
Czerwony	Błąd aktualizacji oprogramowania urządzenia.

Dioda stanu w trybie połączonym

Dioda stanu	Wskazanie
Wyłączona	Czujnik IR detekcji obudowy jest zasłonięty.
Zielony	Modem jest podłączony do sieci.

Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.
Bursztynowy/ czerwony	Trwa konfiguracja modemu podczas uruchamiania.
Czerwony	Błąd aktualizacji oprogramowania urządzenia.

Przyciski

Przycisk kontrolny

Przycisk kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Zob. *Przywracanie domyślnych ustawień fabrycznych, on page 15*.
- 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 wejściowe PoE (PoE in)

Złącze Ethernet RJ45 z zasilaniem Power over Ethernet (PoE) IEEE 802.3af/802.3at/802.3bt typ 3 klasa 5.

Uwaga

To złącze służy wyłącznie do wejścia zasilania; nie ma możliwości utworzenia połączenia sieciowego.

Uwaga

- Dla wyjścia PoE IEEE 802.3at typ 2 klasa 4 wymagane jest wejście zasilania prądem przemiennym.
- Dla wyjścia PoE IEEE 802.3af typ 1 klasa 3 wymagane jest wejście IEEE 802.3at typ 2 klasa 4 lub wyższa.
- W przypadku wejścia PoE IEEE 802.3af typ 1 klasa 3 urządzenie działa, ale nie dostarcza zasilania.

Uwaga

Maksymalna długość kabla Ethernet wynosi 20 m.

Złącze sieciowe (wyjście PoE)

Złącze RJ45 Ethernet.

Uwaga

- Dla wyjścia PoE IEEE 802.3at typ 2 klasa 4 wymagane jest wejście zasilania prądem przemiennym.
- Dla wyjścia PoE IEEE 802.3af typ 1 klasa 3 wymagane jest wejście IEEE 802.3at typ 2 klasa 4 lub wyższa.
- W przypadku wejścia PoE IEEE 802.3af typ 1 klasa 3 urządzenie działa, ale nie dostarcza zasilania.

Uwaga

Maksymalna długość kabla Ethernet wynosi 20 m.

Złącze zasilania

Blok zacisków do podłączania zasilania prądem przemiennym.

Uwaga

Dla wyjścia PoE IEEE 802.3at typ 2 klasa 4 wymagane jest wejście zasilania prądem przemiennym.

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 12*.
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 15*.

Serwer DHCP zmienił adres IP

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

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

Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X

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

Przeglądarka nie jest obsługiwana

Lista zalecanych przeglądarek, p. *Obsługiwane przeglądarki, on page 4*.

Nie można uzyskać dostępu do urządzenia z zewnątrz

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

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

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

Problemy z MQTT

Nie można połączyć przez port 8883 z MQTT przez SSL

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

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

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

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

Kontakt z pomocą techniczną

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

Cyberbezpieczeństwo

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

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

Zarządzanie podatnościami

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

Powiadomienia dotyczące zabezpieczeń

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

Bezpieczny cykl eksploatacji produktu

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

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

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

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

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

T10233346_pl

2026-10 (M2.2)

© 2026 Axis Communications AB