

AXIS M1075-L Box Camera

Spis treści

Od czego zacząć	4
Podłączanie kamery do sieci bezprzewodowej.....	4
Konfigurowanie kamery za pomocą połączenia WLAN	4
Konfigurowanie kamery za pomocą połączenia przewodowego.....	4
Wyszukiwanie urządzenia w sieci.....	5
Obsługiwane przeglądarki.....	5
Otwórz interfejs WWW urządzenia.....	5
Utwórz konto administratora.....	5
Bezpieczne hasła.....	6
Upewnianie się co do braku zmian w oprogramowaniu urządzenia	6
Omówienie interfejsu WWW	6
Instalacja.....	7
Tryb podglądu.....	7
Konfiguracja urządzenia	8
Ustawienia podstawowe	8
Regulowanie obrazu.....	8
Rejestracja w scenach z jasnym podświetleniem	8
Monitorowanie długich i wąskich obszarów.....	9
Sprawdzanie rozdzielczości pikseli.....	9
Ukrywanie części obrazu za pomocą masek prywatności	9
Wyświetlanie nakładek na obrazie.....	10
Wyświetlanie nakładki tekstu.....	10
Przeglądanie i rejestracja obrazów wideo.....	10
Zmniejszanie zapotrzebowania na przepustowość i zasób	10
Wyświetlanie strumienia wideo na żywo na monitorze	11
Konfiguracja zasobów sieciowej pamięci masowej.....	11
Rejestracja i odtwarzanie obrazu.....	11
Sprawdzanie braku sabotażu wideo	12
Konfiguracja reguł dotyczących zdarzeń	12
Wyzwalanie akcji.....	12
Rejestrowanie obrazu wideo w momencie wykrycia obiektu	12
Używaj PIR i dźwięków, by odstraszać intruzów	13
Dźwięk.....	13
.....	13
Dodawanie dźwięku do zapisu.....	13
Interfejs WWW.....	14
Więcej informacji.....	15
Maski prywatności	15
Strumieniowanie i pamięć masowa	15
Formaty kompresji obrazów wideo.....	15
Sterowanie przepływnością bitową.....	16
Analizy i aplikacje	17
AXIS Object Analytics.....	17
Wizualizacja metadanych.....	17
Zaawansowane ustawienia sieci bezprzewodowej.....	18
WPA™ Personal	18
WPA™ Enterprise	18
EAP-TLS.....	18
EAP-PEAP/MSCHAPv2	18
Certyfikaty sieci bezprzewodowej.....	19
Specyfikacje	20
Przegląd produktów.....	20
.....	20

Wskaźniki LED.....	20
Gniazdo karty SD.....	20
Przyciski.....	21
Przycisk kontrolny.....	21
Przycisk konfiguracji WLAN	21
Złącza.....	21
Złącze HDMI	21
Złącze sieciowe	21
Złącze USB.....	21
Złącze I/O	21
Czyszczenie urządzenia	23
Rozwiązywanie problemów –	24
Przywróć domyślne ustawienia fabryczne	24
Opcje systemu AXIS OS.....	24
Sprawdzanie bieżącej wersji systemu AXIS OS.....	24
Aktualizacja systemu AXIS OS:.....	25
Problemy techniczne i możliwe rozwiązania.....	25
Kwestie wydajności	28
Kontakt z pomocą techniczną.....	28
Cyberbezpieczeństwo	29
Postępowanie z lukami w zabezpieczeniach	29
Powiadomienia dotyczące zabezpieczeń	29
Bezpieczny cykl eksploatacji produktu	29

Od czego zacząć

Podłączanie kamery do sieci bezprzewodowej

Zanim zaczniesz:

- Więcej informacji na temat przycisków i złącza kamery. Zobacz *Przegląd produktów, on page 20*.
- Podłącz adapter bezprzewodowy do złącza USB kamery.

Konfigurowanie kamery za pomocą połączenia WLAN

1. Podłącz zasilacz do kamery.
2. Kiedy kontrolka LED na kamerze zacznie migać w kolorach żółtym i czerwonym, naciśnij przycisk konfiguracji WLAN i przytrzymaj do czasu, aż kontrolka zacznie świecić stałym światłem ciągłym. Kamera jest teraz w trybie punktu dostępowego.
3. Można podłączyć się do punktu dostępowego kamery za pomocą komputera lub urządzenia mobilnego. Użyj SSID i hasła wydrukowanych na etykiecie z tyłu kamery.
4. Aby przejść na stronę ustawień WLAN, otwórz przeglądarkę internetową i wpisz adres IP 192.168.0.1.

Uwaga

Aby przejść bezpośrednio na stronę ustawień WLAN, można też zeskanować kod kreskowy umieszczony obok SSID i hasła na etykiecie.

5. Przejdź do sieci bezprzewodowej, której chcesz używać, kliknij , a następnie skonfiguruj ją według potrzeb.
6. Kliknij przycisk **Zapisz**. Punkt dostępowy kamery wyłącza się, a kamera łączy się ze skonfigurowanym punktem dostępowym.

Ważne

Aby zapewnić bezpieczeństwo, należy przywrócić ustawienia fabryczne, jeśli chcesz ponowić procedurę po połączeniu się z siecią WLAN.

Konfigurowanie kamery za pomocą połączenia przewodowego

1. Podłącz urządzenie do sieci przy użyciu przewodu sieciowego.
2. Zaloguj się na stronie internetowej urządzenia. Patrz *Wyszukiwanie urządzenia w sieci, on page 5*.
3. Przejdź do menu **System > WLAN**.

Jeżeli masz dostęp do sprawnej sieci bezprzewodowej:

1. Przejdź do sieci bezprzewodowej, której chcesz używać, kliknij , a następnie skonfiguruj ją według potrzeb.
2. Kliknij przycisk **Zapisz**.
3. Odłącz przewód sieciowy od kamery. Podłącz zasilacz.

Jeśli nie masz dostępu do sieci bezprzewodowej:

1. Kliknij  **Add network (Dodaj sieć)**.
2. Z listy metod uwierzytelniania wybierz **WPA™Personal (Osobista)**.

Uwaga

Aby skonfigurować metodę zabezpieczeń inną niż WPA™Personal, zobacz *Zaawansowane ustawienia sieci bezprzewodowej, on page 18*.

3. Wprowadź SSID i hasło do punktu dostępu.

4. Kliknij przycisk **Zapisz**.
5. Odłącz przewód sieciowy od kamery. Podłącz zasilacz.

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 5.

Opisy wszystkich funkcji i ustawień interfejsu WWW urządzeń z systemem operacyjnym AXIS OS można znaleźć na stronie *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Utwórz konto administratora

Przy pierwszym logowaniu do urządzenia należy utworzyć konto administratora.

1. Wprowadź nazwę użytkownika.
2. Wprowadź hasło. Patrz *Bezpieczne hasła*, on page 6.
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 24.

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 24*. Po zresetowaniu opcja bezpiecznego uruchamiania gwarantuje bezpieczeństwo urządzenia.
2. Skonfiguruj i zainstaluj urządzenie.

Omówienie interfejsu WWW

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



Interfejs WWW urządzenia Axis

Instalacja

Tryb podglądu

Tryb podglądu bardzo przyda się instalatorom podczas dostrajania widoku kamery w trakcie prac montażowych. W tym trybie można uzyskać dostęp do widoku kamery bez konieczności logowania. Tryb jest dostępny wyłącznie w urządzeniu mającym jeszcze ustawienia fabryczne i tylko przez krótki czas w trakcie włączania urządzenia.



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

W tym filmie pokazano, korzystać z trybu podglądu.

Konfiguracja urządzenia

Ustawienia podstawowe

Ustawianie częstotliwości zasilania

1. Przejdź do menu **Video > Installation > Power line frequency** (Wideo > Instalacja > Częstotliwość zasilania).
2. Wybierz częstotliwość zasilania, a następnie kliknij przycisk **Save and restart** (Zapisz i uruchom ponownie).

Ustawianie orientacji

1. Przejdź do menu **Video > Installation > Rotate** (Wideo > Instalacja > Obrót).
2. Wybierz 0, 90, 180 lub 270 stopni.
Zob. też. *Monitorowanie długich i wąskich obszarów, on page 9.*

Regulowanie obrazu

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej na temat działania niektórych funkcji, przejdź do *Więcej informacji, on page 15.*

Rejestracja w scenach z jasnym podświetleniem

Zakres dynamiki to różnica w poziomie oświetlenia na obrazie. W niektórych przypadkach różnica pomiędzy najciemniejszymi a najjaśniejszymi obszarami może być bardzo duża. W wyniku tego otrzymujemy obraz, na którym nie widać ani jasnych, ani ciemnych obszarów. Szeroki zakres dynamiki (WDR) służy do wyświetlenia jasnych i ciemnych obszarów na obrazie.



Obraz bez WDR.



Obraz z WDR.

Uwaga

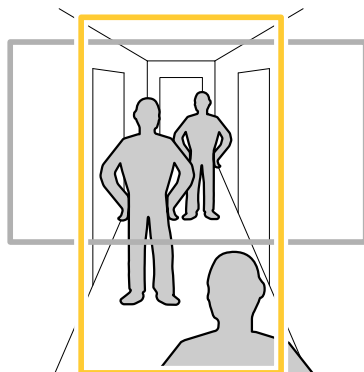
- WDR może powodować występowanie artefaktów na obrazie.
 - Funkcja WDR może nie być dostępna dla wszystkich trybów rejestracji.
1. Przejdź do menu **Video > Image > Wide dynamic range** (Wideo > Obraz > Szeroki zakres dynamiki).
 2. Włącz WDR.

3. Jeżeli nadal występują problemy, przejdź do menu **Exposure (Ekspozycja)** i ustaw **Exposure zone (Strefę ekspozycji)** tak, by pokrywała się z obszarem zainteresowania.

Więcej informacji o funkcji WDR i sposobie jej wykorzystania znajduje się na stronie axis.com/web-articles/wdr.

Monitorowanie długich i wąskich obszarów

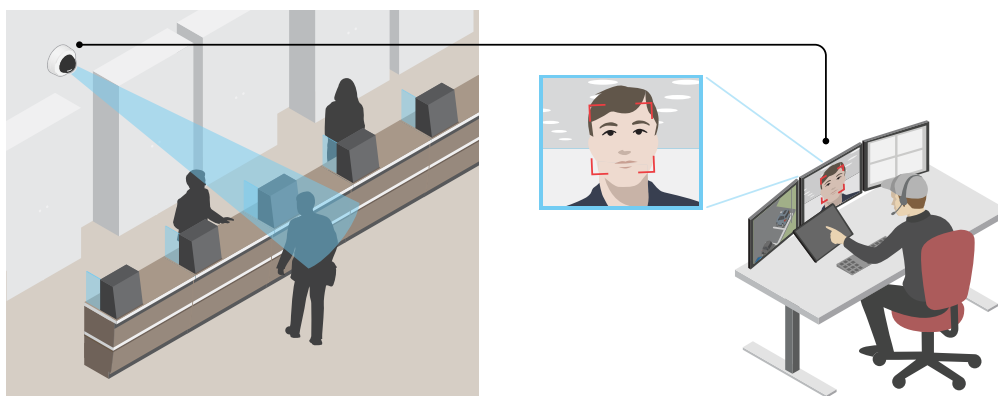
Użyj formatu korytarzowego, aby lepiej używać pełnego pola widzenia w długich i wąskich obszarach, takich jak klatki schodowe, korytarze, drogi czy tunele.



1. W zależności od urządzenia, obróć kamerę lub obiektyw trójosiowy Axis o 90° lub 270°.
2. Jeżeli urządzenie nie ma funkcji automatycznego obrotu widoku, przejdź do okna **Video > Installation (Wideo > Instalacja)**.
3. Obróć widok o 90° lub 270°.

Sprawdzanie rozdzielczości pikseli

Aby sprawdzić, czy zdefiniowana część obrazu zawiera wystarczającą liczbę pikseli, aby na przykład rozpoznać twarz osoby, można użyć licznika pikseli.



1. Przejdź do menu **Video (Wideo) > Image (Obraz)** i kliknij .
2. Kliknij , aby wyświetlić **Pixel counter (Licznik pikseli)**.
3. Dostosuj rozmiar i pozycję prostokąta w podglądzie na żywo kamery, na przykład tak, by obejmował miejsce, w którym mogą pojawić się twarze.
Możesz zobaczyć liczbę pikseli każdej ze stron prostokąta i zdecydować, czy wartości są wystarczające dla Twoich potrzeb.

Ukrywanie części obrazu za pomocą masek prywatności

Możesz utworzyć jedną lub kilka masek prywatności, aby ukryć fragmenty obrazu.

1. Przejdź do okna **Video > Privacy masks** (Wideo > Maski prywatności).
2. Kliknij .
3. Kliknij nową maskę i nadaj jej nazwę.
4. Dostosuj rozmiar i położenie maski prywatności zgodnie z potrzebami.
5. Aby zmienić kolor wszystkich masek prywatności, kliknij **Privacy masks (Maski prywatności)** i wybierz jeden z kolorów.

Zob. też *Maski prywatności, on page 15*

Wyświetlanie nakładek na obrazie

Możesz dodać obraz jako nałożenie do strumienia wideo.

1. Wybierz kolejno opcje **Video > Overlays** (Wideo > Nakładki).
2. Kliknij **Manage images** (Zarządzaj obrazami).
3. Prześlij lub przeciągnij i upuść obraz.
4. Kliknij przycisk **Upload** (Prześlij).
5. Wybierz **Image (Obraz)** z listy rozwijanej i kliknij .
6. Wybierz obraz i położenie. Aby zmienić położenie obrazu nakładki, można go również przeciągnąć w podglądzie na żywo.

Wyświetlanie nakładki tekstu

Możesz dodać pole tekstowe jako nakładkę strumienia wideo. Jest to przydatne na przykład do wyświetlania daty, godziny lub nazwy firmy w strumieniu wideo.

1. Wybierz kolejno opcje **Video > Overlays** (Wideo > Nakładki).
2. Wybierz opcję **Text** (Tekst) i kliknij .
3. Wpisz tekst, który chcesz wyświetlać, lub wybierz modyfikatory, aby wyświetlać na przykład aktualną datę.
4. Wybierz położenie. Aby zmienić położenie nakładki, można ją również kliknąć i przeciągnąć w podglądzie na żywo.

Przeglądanie i rejestracja obrazów wideo

W tej części znajdują się instrukcje dotyczące konfigurowania urządzenia. Aby dowiedzieć się więcej o działaniu strumieniowania i pamięci masowej, przejdź do *Strumieniowanie i pamięć masowa, on page 15*.

Zmniejszanie zapotrzebowania na przepustowość i zasób

Ważne

Zmniejszenie przepustowości może skutkować utratą wyrazistości szczegółów na obrazie.

1. Wybierz kolejno opcje **Video > Stream** (Wideo > Strumień).
2. W podglądzie na żywo kliknij .
3. Wybierz **Video format (Format wideo) AV1**, jeśli urządzenie go obsługuje. W przeciwnym razie wybierz **H.264**.
4. Przejdź do okna **Video > Stream > General** (Wideo > Strumień > Ogólne) i zwiększ wartość w polu **Compression** (Kompresja).

- Przejdź do menu **Video > Stream > Zipstream** (**Wideo > Przesyłanie strumieniowe > Zipstream**) i wykonaj jedną lub więcej z czynności opisanych niżej:

Uwaga

Ustawienia technologii Zipstream są stosowane do wszystkich typów kodowania z wyjątkiem MJPEG.

- Wybierz opcję Zipstream **Strength** (Siła technologii Zipstream), której chcesz użyć.
- Włącz polecenie **Optimize for storage** (Optymalizuj pod kątem zasobu). Tej opcji można użyć tylko wtedy, gdy oprogramowanie do zarządzania materiałem wideo obsługuje ramki B.
- Włącz opcję **Dynamic FPS** (Dynamiczna liczba klatek na sekundę).
- Włącz opcję **Dynamic GOP** (Dynamiczna liczba klatek na sekundę) i dla długości GOP ustaw wysoką wartość parametru **Upper limit** (Górny limit).

Uwaga

Większość przeglądarek internetowych nie obsługuje kodowania H.265, dlatego urządzenie nie obsługuje go w swoim interfejsie WWW. Zamiast tego można użyć systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

Wyświetlanie strumienia wideo na żywo na monitorze

Kamera może przysyłać strumień wideo na żywo do monitora HDMI nawet bez połączenia sieciowego. Monitor może być wykorzystywany do celów dozoru lub do publicznego odtwarzania informacji, na przykład w sklepie.

- Podłącz monitor zewnętrzny za pomocą złącza HDMI.
- Przejdź do menu **System > Video out** (**System > Wyjście wideo**) i włącz HDMI.
- Wybierz **Źródło**. W razie potrzeby obróć obraz.

Konfiguracja zasobów sieciowej pamięci masowej

Aby przechowywać zapisy w sieci, należy skonfigurować zasoby sieciowej pamięci masowej.

- Przejdź do **System > Storage** (**Pamięć masowa**).
- Kliknij opcję  **Add network storage** (**Dodaj sieciową pamięć masową**) w obszarze **Network storage** (**Sieciowa pamięć masowa**).
- Wpisz adres IP serwera hosta.
- W ustawieniu **Network share** (**Udział sieciowy**) podaj nazwę współdzielonego udziału na serwerze hosta.
- Wprowadź nazwę użytkownika i hasło.
- Wybierz wersję protokołu SMB lub pozostaw wartość **Auto** (**Automatycznie**).
- Jeżeli występują tymczasowe problemy z połączeniem lub udział nie został jeszcze skonfigurowany, zaznacz opcję **Add share without testing** (**Dodaj udział bez testowania**).
- Kliknij **Dodaj**.

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z kamery

- Wybierz kolejno opcje **Video > Stream** (**Wideo > Strumień**).
- Aby rozpocząć nagrywanie, kliknij .

Jeżeli jeszcze nie skonfigurowano żadnej pamięci masowej, kliknij  i . Aby uzyskać instrukcje dotyczące konfigurowania sieciowej pamięci masowej, zob. *Konfiguracja zasobów sieciowej pamięci masowej, on page 11*

- Aby zatrzymać nagrywanie, ponownie kliknij .

Obejrzyj wideo

1. Przejdź do menu **Recordings (Nagrania)**.
2. Kliknij  obok wybranego nagrania na liście.

Sprawdzanie braku sabotażu wideo

Podpis wideo daje pewność, że nikt nie zmienił zapisu wideo w kamerze.

1. Przejdź do menu **Video > Stream > General (Wideo > Strumieniowanie > Ogólne)** i włącz opcję **Signed video (Podpisane wideo)**.
2. Zapisuj obraz bezpośrednio w urządzeniu lub użyj programu AXIS Camera Station Pro albo innego kompatybilnego oprogramowania do zarządzania obrazem. Aby uzyskać szczegółowe informacje dotyczące programu AXIS Camera Station Pro, p. *instrukcja obsługi AXIS Camera Station Pro*.
3. Wyeksportuj zarejestrowany materiał wideo.
4. Przeprowadź weryfikację nagrań przy użyciu narzędzia *Axis Signed Media Verifier*.

Konfiguracja reguł dotyczących zdarzeń

Można utworzyć reguły sprawiające, że urządzenie będzie wykonywać konkretne akcje po wystąpieniu określonych zdarzeń. Reguła składa się z warunków i akcji. Warunki mogą służyć do wyzwalania akcji. Urządzenie może na przykład rozpocząć zapis lub wysłać wiadomość e-mail po wykryciu ruchu albo wyświetlić nałożony tekst podczas rejestracji.

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.

Rejestrowanie obrazu wideo w momencie wykrycia obiektu

W tym przykładzie wyjaśniono, jak skonfigurować kamerę, aby rozpocząć zapis na karcie SD, kiedy kamera wykryje dany obiekt. Zapis obejmuje pięć sekund przed detekcją i minutę po zakończeniu detekcji.

Zanim zaczniesz:

- Upewnij się, że karta SD została zainstalowana.

Upewnij się, że jest uruchomiona aplikacja AXIS Object Analytics:

1. Wybierz kolejno opcje **Apps > AXIS Object Analytics (Aplikacje > AXIS Object Analytics)**.
2. Uruchom aplikację, jeśli jeszcze nie jest uruchomiona.
3. Upewnij się, że aplikacja została skonfigurowana odpowiednio do potrzeb.

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków w obszarze **Application (Zastosowanie)** wybierz **Object Analytics (Analiza obiektów)**.
4. Z listy akcji w obszarze **Recordings (Zapisy)** wybierz opcję **Record video while the rule is active (Rejestruj wideo, gdy reguła jest aktywna)**.

5. Z listy opcji pamięci masowej wybierz opcję **SD_DISK**.
6. Wybierz kamerę i profil strumienia.
7. Ustaw czas buforowania przed zdarzeniem na 5 sekund.
8. Ustaw czas buforowania po zdarzeniu na 1 minutę.
9. Kliknij przycisk **Zapisz**.

Używaj PIR i dźwięków, by odstraszać intruzów

W tym przykładzie wyjaśniono, jak skonfigurować kamerę, by odtwarzała nagranie audio z odgłosem szczekającego psa, gdy czujnik PIR wykryje ruch poza godzinami pracy.

Zanim zaczniesz:

- Dodaj w urządzeniu klip dźwiękowy z nagraniem szczekającego psa. Więcej informacji można znaleźć w sekcji .

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events (System > Zdarzenia)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Na liście warunków wybierz **Device status > PIR sensor (Status urządzenia > Czujnik PIR)**.
4. Kliknij **+**, aby dodać drugi warunek.
5. Z listy warunków w obszarze wybierz opcję **Scheduled and recurring > Schedule (Zaplanowane i cykliczne)**.
6. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.
7. Z listy akcji wybierz opcję **Audio clips > Play audio clip (Klipy audio > Odtwórz klip audio)**.
8. Z listy klipów wybierz opcję **Dog barking (Szczekanie psa)**.
9. Kliknij przycisk **Zapisz**.

Dźwięk

To urządzenie ma funkcję automatycznego wzmacniania głosu.

Dodawanie dźwięku do zapisu

Włącz dźwięk:

1. Przejdź do menu **Video > Stream > Audio (Wideo > Strumień > Dźwięk)** i włącz obsługę audio.
2. Jeżeli urządzenie ma więcej niż jedno źródło sygnału wejściowego, wybierz właściwe w polu **Source (Źródło)**.
3. Wybierz kolejno opcje **Audio > Device settings (Dźwięk > Ustawienia urządzenia)** i włącz odpowiednie źródło sygnału wejściowego.

Edytuj profil strumienia używany do rejestracji:

4. Przejdź do okna **System > Stream profiles (System > Profile strumienia)** i wybierz profil strumienia.
5. Kliknij opcję **Include audio (Dołącz audio)** i włącz ją.
6. Kliknij przycisk **Zapisz**.

Interfejs WWW

Aby zapoznać się ze wszystkimi funkcjami i ustawieniami dostępnymi w interfejsie WWW urządzeń z systemem operacyjnym AXIS OS, przejdź do strony *Pomoc dotycząca interfejsu internetowego AXIS OS*.

Więcej informacji

Maski prywatności

Maska prywatności to obszar zdefiniowany przez użytkownika, który uniemożliwia podgląd części monitorowanego obszaru. Maski prywatności wyświetlane są jako nieprzezroczyste elementy na strumieniu wideo.

Maska prywatności znajduje się na wszystkich zrzutach ekranu, zarejestrowanych obrazach i strumieniach podglądu na żywo.

Aby ukryć maskę prywatności, można użyć interfejsu VAPIX® Application Programming Interface (API).

Ważne

Dodanie wielu masek prywatności może wpłynąć na pracę urządzenia.

Można utworzyć kilka masek prywatności. Każda maska może mieć od 3 do 10 punktów kotwiczenia.

Strumieniowanie i pamięć masowa

Formaty kompresji obrazów wideo

O tym, która metoda kompresji ma być używana, należy zdecydować w zależności od wymagań dotyczących przeglądania i właściwości sieci. Dostępne są następujące opcje:

MJPEG

Motion JPEG (MJPEG), to cyfrowa sekwencja wideo składająca się z szeregu indywidualnych obrazów JPEG. Obrazy te są następnie wyświetlane i aktualizowane z szybkością odpowiednią do utworzenia strumienia pokazującego ciągle zaktualizowany ruch. Aby odbiorca miał wrażenie oglądania obrazu wideo, szybkość musi wynosić co najmniej 16 klatek obrazu na sekundę. Obraz jest odbierany jako ruchomy obraz wideo przy 30 (NTSC) lub 25 (PAL) klatkach na sekundę.

Strumień MJPEG wykorzystuje przepustowość w dużym stopniu, ale zapewnia doskonałą jakość obrazu i dostęp do wszystkich obrazów zawartych w strumieniu.

H.264 lub MPEG-4 Part 10/AVC

Uwaga

Kompresja H. 264 to licencjonowana technologia. W produkcie Axis znajduje się jedna licencja klienta do przeglądania obrazów w kompresji H.264. Nie wolno instalować dodatkowych kopii klienta bez licencji. Aby zakupić dodatkowe licencje, skontaktuj się z dystrybutorem Axis.

Dzięki kompresji H.264 można, bez uszczerbku na jakości, zmniejszyć rozmiar cyfrowego pliku wideo o ponad 80% w porównaniu z formatem MJPEG i nawet 50% w porównaniu ze starszymi formatami MPEG. Oznacza to, że w przypadku pliku wideo wymagana jest mniejsza przepustowość i mniej zasobów pamięci masowej. Inaczej mówiąc, dla danej przepływności bitowej można uzyskać obraz o wyższej jakości.

H.265 lub MPEG-H Part 2/HEVC

Dzięki kompresji H.265 można, bez uszczerbku na jakości, zmniejszyć rozmiar cyfrowego pliku wideo o ponad 25% w porównaniu z kompresją H.264.

Uwaga

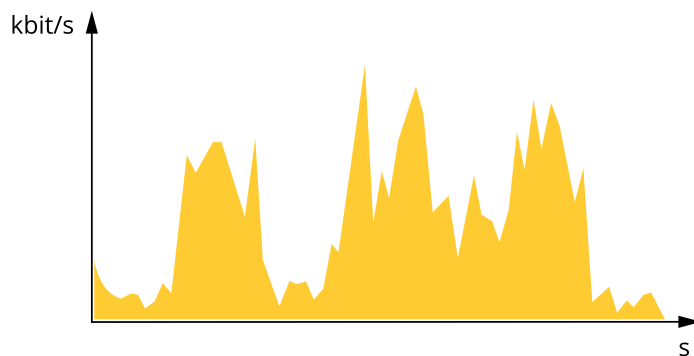
- Kompresja H.265 to licencjonowana technologia. W produkcie Axis znajduje się jedna licencja klienta do przeglądania obrazów w kompresji H.265. Nie wolno instalować dodatkowych kopii klienta bez licencji. Aby zakupić dodatkowe licencje, skontaktuj się z dystrybutorem Axis.
- Większość przeglądarek internetowych nie obsługuje dekodowania H.265 i dlatego kamera nie ma dla niego opcji w swoim interfejsie internetowym. Zamiast tego można użyć systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

Sterowanie przepływnością bitową

Dzięki kontroli przepływności bitowej można zarządzać zajętością pasma przez strumień wideo.

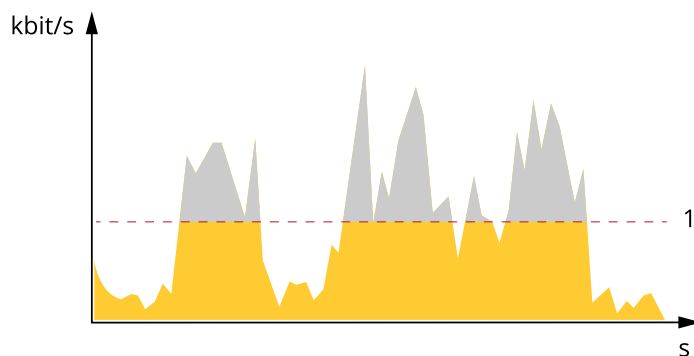
Zmienna przepływność bitowa (VBR)

Przy zmiennej przepływności bitowej zajętość pasma zmienia się w zależności od natężenia aktywności w scenie. Przy większym natężeniu aktywności potrzebna jest większa przepustowość. Zmienna przepływność zapewnia stałą jakość obrazu, ale funkcja ta wymaga odpowiedniej ilości miejsca w zasobach pamięci.



Maksymalna przepływność bitowa (MBR)

Opcja ta umożliwia ustawienie docelowej przepływności bitowej w celu kontrolowania zajętości pasma. Gdy bieżąca przepływność bitowa jest utrzymywana poniżej określonej szybkości, może wystąpić spadek jakości obrazu lub niższa poklatkowość. Jak priorytet można wybrać opcję ustawienia jakości obrazu lub poklatkowości. Zalecamy skonfigurowanie docelowej wartości przepływności bitowej na wartość większą niż oczekiwana. Dzięki temu można zachować margines, jeśli w scenie występuje wysoki poziom aktywności.

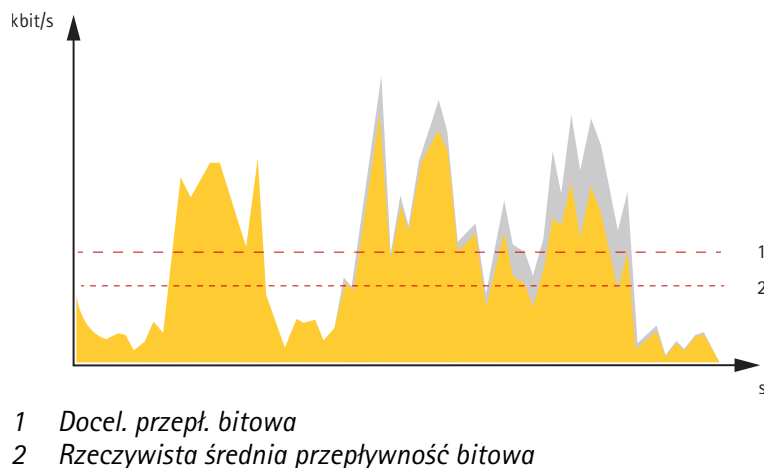


1 Docel. przepł. bitowa

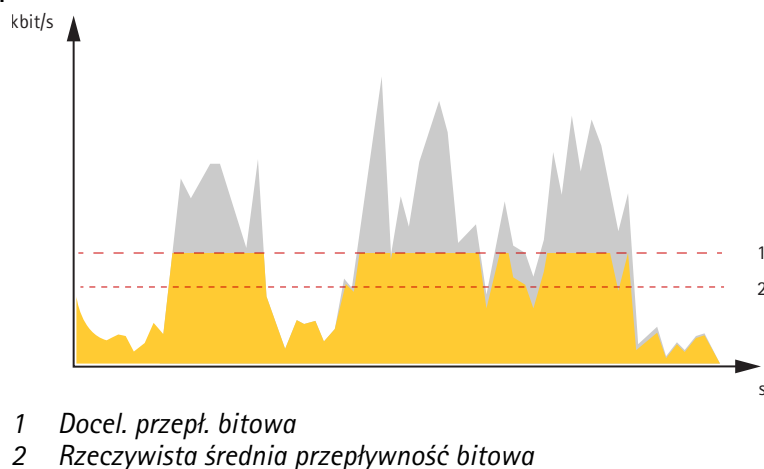
Średnia przepływność bitowa (ABR)

Średnia przepływność bitowa jest dostosowywana automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak najlepszą jakość obrazu wideo przy dostępnych zasobach pamięci masowej. Przepływność bitowa jest wyższa w scenach z dużą aktywnością w porównaniu ze scenami statycznymi. Korzystanie z opcji średniej przepływności zwiększa szanse uzyskania lepszej jakości obrazu w scenach o wysokim poziomie aktywności. Można zdefiniować łączną ilość pamięci masowej wymaganej do przechowywania strumienia wideo przez określony czas (czas retencji) po dostosowaniu jakości obrazu tak, by odpowiadała określonej przepływności bitowej. Określ średnią wartość przepływności bitowej w jeden z następujących sposobów:

- Aby obliczyć przybliżone zapotrzebowanie na zasoby pamięci masowej, należy ustawić wartość docelową przepływności bitowej i czas retencji.
- Użyj kalkulatora przepływności bitowej, aby obliczyć średnią przepływność bitową w zależności od dostępnego miejsca w zasobach pamięci i czasu retencji.



Można również włączyć maksymalną przepływność bitową i określić przepływność bitową w ramach średniej przepływności bitowej.



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 Object Analytics

AXIS Object Analytics to aplikacja analityczna zainstalowana fabrycznie w kamerze. Wykrywa obiekty poruszające się w scenie i klasyfikuje je jako ludzi lub pojazdy itd. Aplikację można skonfigurować tak, aby wysyłała alarmy dotyczące różnych typów obiektów. Aby dowiedzieć się więcej o działaniu aplikacji, zapoznaj się z *instrukcją użytkownika AXIS Object Analytics*.

Wizualizacja metadanych

Metadane analityczne są dostępne w przypadku poruszających się obiektów w scenie. Obsługiwane klasy obiektów są wizualizowane w strumieniu wideo za pomocą obwiedni otaczającej obiekt, wraz z informacją o typie obiektu i poziomie ufności klasyfikacji. Aby dowiedzieć się więcej na temat konfigurowania metadanych analitycznych i korzystania z nich, zobacz *podręcznik integracji AXIS Scene Metadata*.

Zaawansowane ustawienia sieci bezprzewodowej

Najczęściej używaną metodą zabezpieczeń jest WPA™ Personal. To urządzenie obsługuje również protokół WPA™ Enterprise, który jest bezpieczniejszą metodą. Wszystkie ustawienia muszą być zgodne z ustawieniami w punkcie dostępu.

WPA™ Personal

Metoda zabezpieczeń WPA Personal jest przeznaczona do małych sieci i nie wymaga serwera uwierzytelniania.

WPA™ Enterprise

Metoda zabezpieczeń WPA Enterprise jest przeznaczona do dużych sieci i wymaga serwera uwierzytelniania. Sieć jest chroniona przez EAPOL Extensible Authentication Protocol Over LAN).

Wybierz typ WPA-Enterprise używany przez punkt dostępu:

- EAP-TLS. Patrz *page 18*.
- EAP-PEAP/MSCHAPv2. Patrz *page 18*.

EAP-TLS

Protokół uwierzytelniania EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) umożliwia klientowi i serwerowi wzajemne uwierzytelnianie za pośrednictwem certyfikatów cyfrowych dostarczanych przez jednostkę certyfikującą. Aby uzyskać dostęp do zabezpieczonej sieci, produkt Axis przedstawia certyfikat punktom dostępu do sieci. Dostęp zostanie udzielony po zatwierdzeniu certyfikatu.

Ważne

Aby zapewnić pomyślne sprawdzenie certyfikatu, należy przeprowadzić synchronizację czasu na wszystkich klientach i serwerach przed rozpoczęciem konfiguracji.

Konfiguracja ustawień sieci bezprzewodowej za pomocą protokołów WPA™ Enterprise i EAP-TLS

1. Przejdź do menu **System > WLAN**.
2. Kliknij  **Add network (Dodaj sieć)**.
3. Z listy metod uwierzytelniania wybierz opcję **WPA-Enterprise EAP-TLS**.
4. Wprowadź identyfikator SSID skojarzony z certyfikatem.
5. Wybierz **EAPoL version (Wersję EAPoL)** (1, 2 lub 3) używaną w punkcie dostępu.
6. Wybierz **CA certificate (certyfikat CA)** i **Client certificate (certyfikat klienta)**, który ma być używany do uwierzytelniania w sieci bezprzewodowej.
7. Kliknij przycisk **Zapisz**.

EAP-PEAP/MSCHAPv2

Protokół uwierzytelniania EAP-PEAP/MSCHAPv2 (Extensible Authentication Protocol – Protected Extensible Authentication Protocol/Microsoft Challenge Handshake Authentication Protocol) umożliwia klientowi uwierzytelnianie sieci przy użyciu cyfrowego certyfikatu dostarczonego przez jednostkę certyfikującą. Sieć uwierzytelnia klienta przy użyciu tożsamości i hasła. Aby uzyskać dostęp do zabezpieczonej sieci, produkt Axis przedstawia swoją tożsamość i hasło do punktu dostępu do sieci. Po zatwierdzeniu tych poświadczeń punkt dostępu umożliwia dostęp na wstępnie skonfigurowanym porcie.

Ważne

Aby zapewnić pomyślne sprawdzenie certyfikatu, należy przeprowadzić synchronizację czasu na wszystkich klientach i serwerach przed rozpoczęciem konfiguracji.

Konfiguracja ustawień sieci bezprzewodowej za pomocą protokołów WPA™ Enterprise i EAP-PEAP/MSCHAPv2

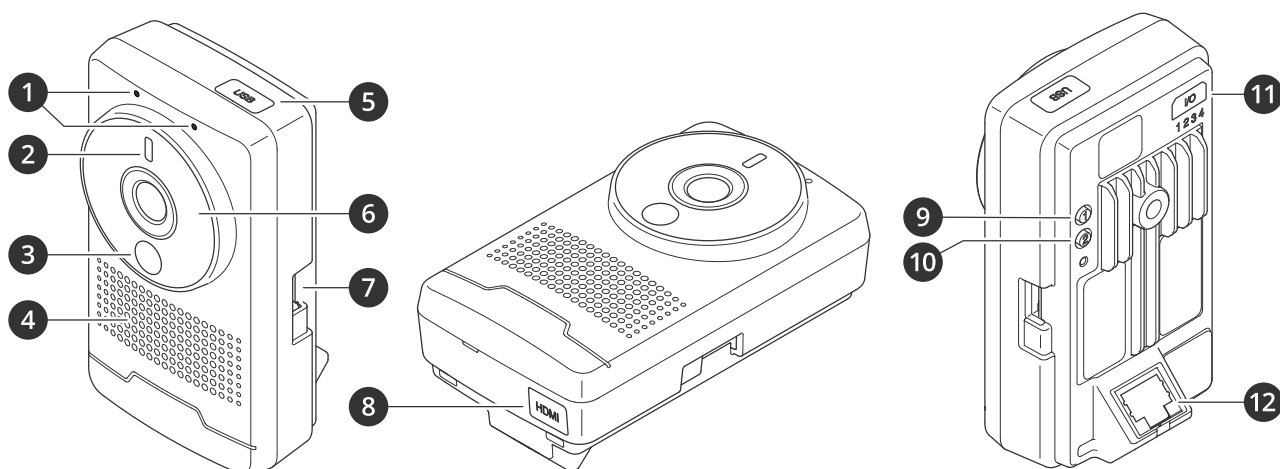
1. Przejdź do menu **System > WLAN**.
2. Kliknij  **Add network (Dodaj sieć)**.
3. Z listy metod uwierzytelniania wybierz opcję **WPA-Enterprise EAP-PEAP/MSCHAPv2**.
4. Wprowadź identyfikator SSID skojarzony z certyfikatem.
5. Wprowadź hasło do tożsamości użytkownika.
6. Wybierz **EAPoL version (Wersję EAPoL)** (1, 2 lub 3) używaną w punkcie dostępu.
7. Wybierz **Peap version (Wersję Peap)** (0 lub 1) używaną w punkcie dostępu.
8. Wybierz **Label (Etykietę)** używaną przez punkt dostępu podczas korzystania z wersji 1 Peap. Wybierz 1, by używać szyfrowania EAP po stronie klienta; wybierz 2, by używać szyfrowania PEAP po stronie klienta.
9. Wybierz **CA certificate (Certyfikat CA)**, którego chcesz użyć do sprawdzenia certyfikatu sieciowego / AP.
10. Kliknij przycisk **Zapisz**.

Certyfikaty sieci bezprzewodowej

Certyfikaty sieci bezprzewodowej służą do uwierzytelniania urządzeń w sieci bezprzewodowej. Sieci bezprzewodowe korzystające z metody zabezpieczeń WPA™ Enterprise są chronione przez EAPoL (Extensible Authentication Protocol over LAN), który jest częścią standardu IEEE 802.1X. Klient uwierzytelnia serwer za pomocą certyfikatów cyfrowych. Serwer uwierzytelnia klienta za pomocą certyfikatów cyfrowych lub hasła, w zależności od wybranego typu WPA Enterprise.

Specyfikacje

Przegląd produktów



- 1 Mikrofon
- 2 Dioda stanu
- 3 Czujnik PIR
- 4 Głośnik
- 5 Złącze USB
- 6 IR LED
- 7 Gniazdo karty SD
- 8 Złącze MicroHDMI typu D
- 9 Przycisk kontrolny
- 10 Przycisk konfiguracji WLAN
- 11 Złącze I/O
- 12 Złącze sieciowe

Wskaźniki LED

Dioda stanu	Wskazanie
Zgaszony	Połączenie i normalne działanie.
Zielony	Stałe zielone światło przez 10 sekund przy normalnym działaniu po zakończeniu uruchamiania.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania sprzętowego lub przywracania domyślnych ustawień fabrycznych.
Bursztyno-wy/czerwony	Miga na bursztynowo/czerwono, gdy połączenie sieciowe jest niedostępne lub przerwane.
Czerwony	Świeci ciągle na czerwono podczas strumieniowania na żywo lub zapisu.
Niebieski	Świeci ciągle na niebiesko w trybie konfiguracji WLAN.

Gniazdo karty SD

POWIADOMIENIE

- Ryzyko uszkodzenia karty SD. Nie używaj ostrych narzędzi, metalowych przedmiotów ani nadmiernej siły podczas wkładania i wyjmowania karty SD. Wkładaj i wyjmuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wyjmuj karty SD w trakcie działania produktu.

Urządzenie obsługuje karty microSD/microSDHC/microSDXC.

Zalecenia dotyczące kart SD można znaleźć w witrynie *axis.com*.



Logo microSD, microSDHC i microSDXC są znakami towarowymi firmy SD-3C LLC. microSD, microSDHC, microSDXC są znakami towarowymi lub znakami towarowymi firmy SD-3C, LLC w Stanach Zjednoczonych, innych krajach lub w Stanach Zjednoczonych i innych krajach.

Przyciski

Przycisk kontrolny

Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 24*.
- 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.

Przycisk konfiguracji WLAN

Przycisk konfiguracji sieci WLAN służy do konfigurowania połączenia WLAN.

Złącza

Złącze HDMI

Użyj złącza microHDMI™, aby podłączyć wyświetlacz lub monitor dostępne publicznie.

Złącze sieciowe

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

Złącze USB

Za pomocą złącza USB można podłączyć akcesoria zewnętrzne. Informacje na temat obsługiwanych akcesoriów można znaleźć w karcie charakterystyki produktu.

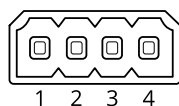
Złącze I/O

Złącze I/O 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 12 V) złącze WE/WY 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.

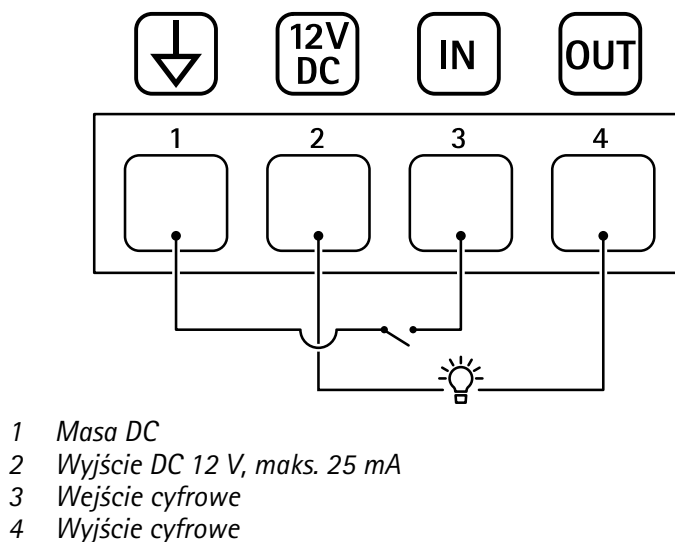
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

4-pinowy blok złączy



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 Maks. obciążenie = 25 mA
Wejścia cyfrowe	3	Podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 30 V DC
Wyjście cyfrowe	4	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:



Czyszczenie urządzenia

Urządzenie można czyścić letnią wodą.

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 pozostawianie plam na obudowie.
1. Można użyć sprężonego powietrza, aby usunąć z urządzenia pył i nieprzylegający brud.
 2. W razie potrzeby można wyczyścić urządzenie miękką ściereczką z mikrofibry zwilżoną letnią wodą.
 3. 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 –

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 20*.
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 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 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 wydaniem wersji zawierającymi głównie poprawki i aktualizacje dotyczące bezpieczeństwa.

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

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.

W programie AXIS Device Manager można uaktualnić wiele urządzeń jednocześnie. Dowiedz się więcej na stronie axis.com/products/axis-device-manager.

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 24.*

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 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 przesyłaniem strumieniowym

Strumień multicast w kodowaniu H.264 jest dostępny wyłącznie dla lokalnych klientów

Sprawdź, czy router obsługuje technologię multicasting lub czy trzeba skonfigurować ustawienia routera w kliencie i urządzeniu. Może być konieczne zwiększenie wartości TTL (Time To Live), czyli czasu do rejestracji na żywo.

W kliencie nie można wyświetlić strumienia multicast w kodowaniu H.264

Poproś administratora sieci, aby sprawdził, czy adresy strumienia multicast używane przez urządzenie Axis są prawidłowe dla danej sieci.

Poproś administratora sieci, aby sprawdził, czy zaporę nie powoduje blokowania strumienia.

Niedostateczne renderowanie obrazów w kompresji H.264

Sprawdź, czy karta graficzna ma zainstalowany najnowszy sterownik. Zazwyczaj najnowsze sterowniki można pobrać z witryny internetowej producenta.

Strumienie H.264 i MJPEG mają różną saturację barw

Zmień ustawienia karty graficznej. Więcej informacji można znaleźć w dokumentacji karty.

Liczba klatek na sekundę jest mniejsza od oczekiwanej

- Patrz *Kwestie wydajności*, on page 28.
- Zmniejsz liczbę aplikacji uruchomionych na komputerze klienta.
- Ogranicz liczbę dozorców mogących oglądać obraz jednocześnie.
- Poproś administratora sieci, aby sprawdził, czy dostępna jest wystarczająca przepustowość.
- Zmniejsz rozdzielczość obrazu.

Nie można wybrać kodowania H.265 w podglądzie na żywo

Przeglądarki internetowe nie obsługują dekodowania H.265. Użyj systemu zarządzania materiałem wizyjnym lub aplikacji obsługującej dekodowanie H.265.

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.

Kwestie wydajności

Podczas konfigurowania systemu należy wziąć pod uwagę wpływ różnych ustawień i sytuacji na wydajność. Niektóre czynniki wpływają na przepustowość (przepływność), inne na poklatkowość, a jeszcze inne na oba te parametry.

Najważniejsze czynniki, które należy uwzględnić:

- Wysoka rozdzielczość obrazu lub niższe poziomy kompresji zapewniają obrazy zawierające więcej danych, co z kolei wpływa na przepustowość.
- Obracanie obrazu w graficznym interfejsie użytkownika zwiększy obciążenie procesora produktu.
- Dostęp ze strony dużej liczby klientów MJPEG lub H.264/H.265/AV1 unicast wpływa na przepustowość.
- Jednoczesne oglądanie różnych strumieni (rozdzielczość, kompresja) za pomocą różnych klientów wpływa zarówno na liczbę klatek na sekundę, jak i na przepustowość. W miarę możliwości używaj identycznych strumieni, aby utrzymać wysoką liczbę klatek na sekundę. Aby upewnić się, że strumienie są identyczne, możesz użyć profili strumieni.
- Jednoczesny dostęp do strumieni wideo z różnymi kodekami wpływa zarówno na poklatkowość, jak i na przepustowość. Aby uzyskać optymalną wydajność, należy używać strumieni z tym samym kodekiem.
- Intensywne korzystanie z ustawień zdarzeń wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.
- Korzystanie z protokołu HTTPS może zmniejszać liczbę klatek na sekundę, szczególnie w przypadku przesyłania strumieniowego obrazów wideo w formacie MJPEG.
- Znaczące obciążenie sieci ze względu na słabą infrastrukturę wpływa na przepustowość.
- Wyświetlanie obrazu z użyciem komputerów klienckich o niewystarczających parametrach obniża subiektywnie obserwowaną wydajność i wpływa na liczbę klatek na sekundę.
- Jednoczesne uruchamianie wielu aplikacji AXIS Camera Application Platform (ACAP) może mieć wpływ na liczbę klatek na sekundę i ogólną wydajność.

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 cyberbezpieczeństwa znajdują się na stronie: axis.com/about-axis/cybersecurity. Przestrzegaj poniższych wytycznych dotyczących cyberbezpieczeństwa, 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.

Postępowanie z lukami w zabezpieczeniach

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.

T10180154_pl

2026-07 (M20.2)

© 2022 – 2026 Axis Communications AB