

AXIS Q21 Thermal Camera Series

AXIS Q2111-E Thermal Camera

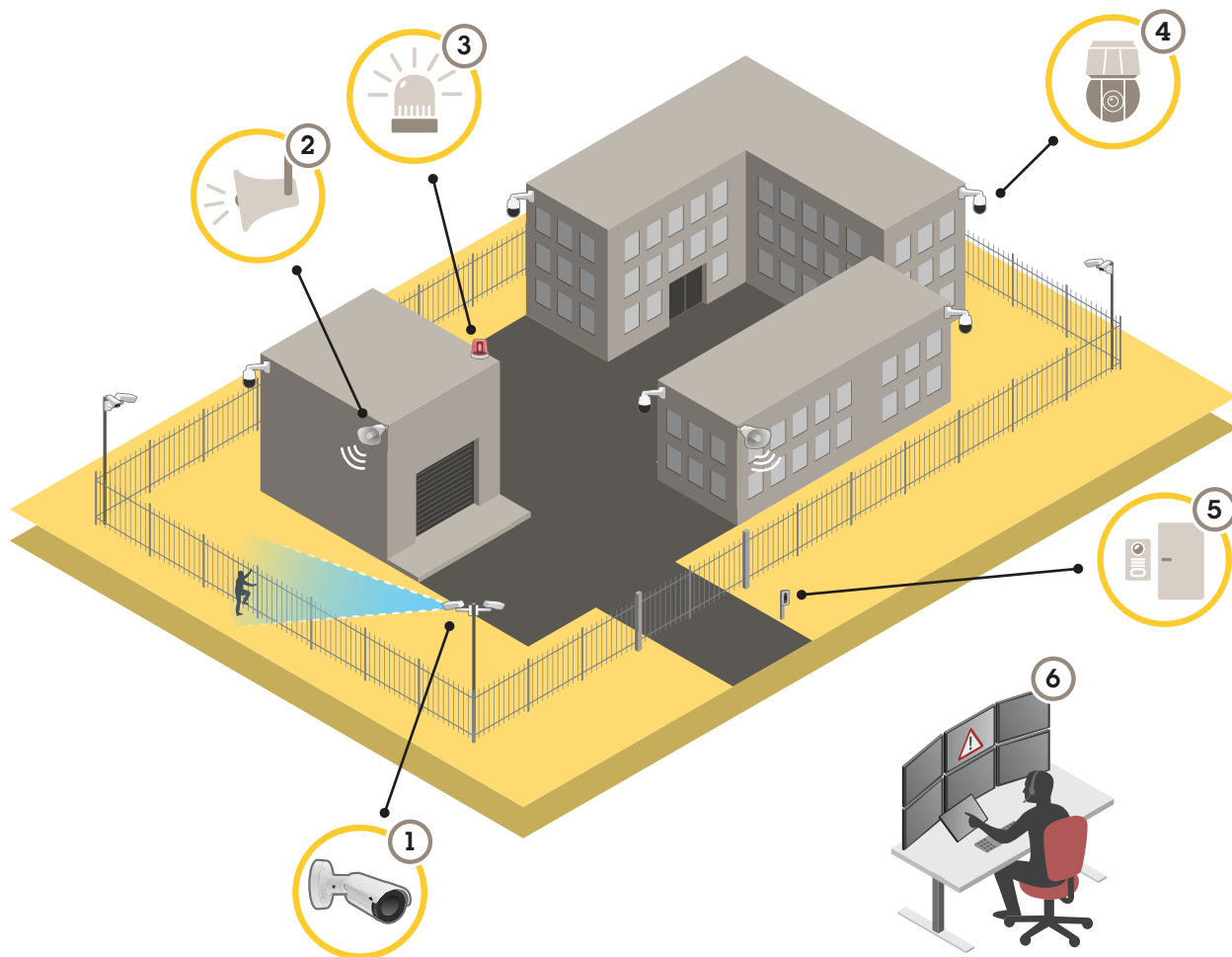
AXIS Q2112-E Thermal Camera

Spis treści

Informacje o rozwiązaniu.....	4
.....	4
Ochrona obwodowa.....	4
Instalacja.....	5
Tryb podglądu.....	5
Od czego zacząć.....	6
Wyszukiwanie urządzenia w sieci.....	6
Obsługiwane przeglądarki.....	6
Otwórz interfejs WWW urządzenia.....	6
Utwórz konto administratora.....	6
Bezpieczne hasła.....	7
Upewnianie się co do braku zmian w oprogramowaniu urządzenia.....	7
Konfiguracja urządzenia.....	8
Ustawienia podstawowe.....	8
Regulowanie obrazu.....	8
Stabilizacja obrazu za pomocą funkcji stabilizacji obrazu.....	8
Monitorowanie długich i wąskich obszarów.....	8
Wyświetlanie nakładek na obrazie.....	9
Wyświetlanie nakładki tekstu.....	9
Przeglądanie i rejestracja obrazów wideo.....	9
Zmniejszanie zapotrzebowania na przepustowość i zasób.....	9
Konfiguracja zasobów sieciowej pamięci masowej.....	10
Rejestracja i odtwarzanie obrazu.....	10
Sprawdzanie braku sabotażu wideo.....	10
Konfiguracja reguł dotyczących zdarzeń.....	11
Odstraszanie intruzów za pomocą sygnalizatora świetlnego.....	11
Odstraszanie intruzów za pomocą dźwięku.....	12
Aktywowanie syreny stroboskopowej przez wejście wirtualne po wykryciu ruchu przez kamerę.....	13
Wykrywanie ingerencji w sygnał wejściowy.....	14
Wyzwalanie powiadomienia po otwarciu obudowy.....	15
Automatyczne przysyłanie wiadomości e-mail w przypadku zamalowania obiektywu farbą w sprayu.....	15
Dźwięk.....	16
Dodawanie dźwięku do zapisu.....	16
Interfejs WWW.....	17
Więcej informacji.....	18
Palety kolorów.....	18
Nakładki.....	18
Strumieniowanie i pamięć masowa.....	18
Formaty kompresji obrazów wideo.....	18
W jaki sposób ustawienia obrazu, strumienia i profilu strumienia mogą na siebie wpływać?.....	19
Sterowanie przepływnością bitową.....	19
Analizy i aplikacje.....	20
AXIS Perimeter Defender.....	21
Cyberbezpieczeństwo.....	22
Axis Edge Vault.....	22
Podpisany system operacyjny.....	22
Bezpieczny start.....	22
Bezpieczny magazyn kluczy.....	22
Identyfikator urządzenia axis.....	23
Podpisany materiał wizyjny.....	23
Zaszyfrowany system plików.....	23
Usługa powiadomień w systemach zabezpieczeń Axis.....	23

Postępowanie z lukami w zabezpieczeniach.....	23
Bezpieczne działanie urządzeń Axis	23
Specyfikacje	25
Przegląd produktów.....	25
Wskaźniki LED.....	26
Brzęczyk.....	26
Brzęczyk asystenta poziomowania.....	26
Gniazdo karty SD.....	27
Przyciski.....	27
Przycisk kontrolny.....	27
Złącza	27
Złącze sieciowe	27
Złącze audio.....	27
Złącze I/O	28
Złącze zasilania	29
Złącze RS485/RS422	29
Sterowniki PTZ.....	30
ATP	30
Pelco.....	30
Visca	32
Czyszczenie urządzenia	34
Rozwiązywanie problemów –	35
Przywróć domyślne ustawienia fabryczne	35
Opcje systemu AXIS OS.....	35
Sprawdzanie bieżącej wersji systemu AXIS OS.....	35
Aktualizacja systemu AXIS OS:.....	36
Problemy techniczne i możliwe rozwiązania.....	36
Kwestie wydajności	39
Kontakt z pomocą techniczną.....	39

Informacje o rozwiązaniu



- 1 Kamera termowizyjna z aplikacją AXIS Perimeter Defender
- 2 Głośnik tubowy
- 3 Sygnalizator świetlny
- 4 Kamera sieciowa PTZ
- 5 Kontroler drzwi
- 6 Centrum monitoringu

Ochrona obwodowa

W przypadku obszarów wymagających detekcji wtargnięć można skonfigurować ochronę obwodową za pomocą kamer termowizyjnych z funkcjami analizy. Głównym celem ochrony obwodowej jest detekcja zagrożeń lub faktyczna ingerencja w jak najkrótszym czasie.

Aby skonfigurować ochronę obwodową, należy zainstalować aplikację do analizy (ochrona obwodowa) oraz zabezpieczyć kamerę termowizyjną. Firma Axis zapewnia w tym celu aplikację AXIS Perimeter Defender. Więcej informacji na temat aplikacji AXIS Perimeter Defender znajduje się na stronie axis.com/products/axis-perimeter-defender

- Aby poinformować intruzów o ochronie, można użyć sygnalizatora świetlnego (3). Patrz *Odstraszanie intruzów za pomocą sygnalizatora świetlnego, on page 11.*
- Aby ostrzec i odstraszyć intruzów, należy zamontować głośnik (2), przez który można odtwarzać nagrany komunikat. Patrz *Odstraszanie intruzów za pomocą dźwięku, on page 12.*

Instalacja



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

Film przedstawiający instalację urządzenia.

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.

Od czego zacząć

Wyszukiwanie urządzenia w sieci

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

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

Obsługiwane przeglądarki

Urządzenie obsługuje następujące przeglądarki:

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

✓: zalecane

*: obsługiwane z ograniczeniami

Otwórz interfejs WWW urządzenia

1. Otwórz przeglądarkę i wpisz adres IP lub nazwę hosta urządzenia Axis. Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.
2. Wprowadź nazwę użytkownika i hasło. Jeśli korzystasz z urządzenia po raz pierwszy, musisz utworzyć konto administratora. Patrz *Utwórz konto administratora*, on page 6.

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 7.
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 35.

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

Konfiguracja urządzenia

W tej części zostały opisane wszystkie ważne konfiguracje, które musi przeprowadzić instalator, aby uruchomić produkt po zakończeniu montażu sprzętu.

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 8.

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 18.

Stabilizacja obrazu za pomocą funkcji stabilizacji obrazu

Funkcja stabilizacji jest przeznaczona do użycia w przypadku środowisk, w których produkt jest zamontowany na zewnątrz budynku i narażony na drgania, np. z powodu wiatru lub ruchu pojazdów.

Funkcja ta sprawia, że obraz jest płynniejszy, stabilniejszy i mniej rozmyty. Zmniejsza ona również rozmiar pliku skompresowanego obrazu i obniża przepływność bitową strumienia wideo.

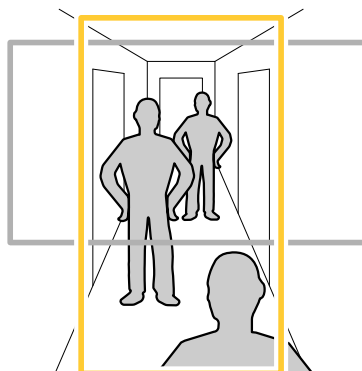
Uwaga

Gdy stabilizacja obrazu jest włączona, obraz będzie lekko przycięty, a jego maksymalna rozdzielczość zostanie obniżona.

1. Przejdź do menu **Video > Installation > Image correction** (Wideo > Instalacja > Korekta obrazu).
2. Włącz **Image stabilization** (Stabilizacja obrazu).

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°.

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 18*.

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**).
5. 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.

Konfiguracja zasobów sieciowej pamięci masowej

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

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

Rejestracja i odtwarzanie obrazu

Nagrywanie obrazu wideo bezpośrednio z kamery

1. Wybierz kolejno opcje **Video > Stream (Wideo > Strumień)**.

2. 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 10*

3. 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. Użyj opcji aplikacji **AXIS Camera Station** (w wersji 5.46 lub nowszej) lub innego zgodnego oprogramowania do zarządzania wideo i zapisu wideo. Aby uzyskać szczegółowe informacje, zobacz *instrukcję obsługi AXIS Camera Station*.

3. Wyeksportuj zarejestrowany materiał wideo.
4. Użyj aplikacji AXIS File Player do odtworzenia wideo. *Pobierz AXIS File Player.*



wskazuje, że nie doszło do sabotażu wideo.

Uwaga

Aby uzyskać więcej informacji o wideo, kliknij wideo prawym przyciskiem myszy i wybierz opcję **Show digital signature** (Pokaż cyfrowy podpis).

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).

Odstraszanie intruzów za pomocą sygnalizatora świetlnego

Można użyć sygnalizatora świetlnego, aby poinformować potencjalnych intruzów, że teren jest chroniony.

W tym przykładzie wyjaśniono sposób podłączania sygnalizatora świetlnego i konfigurowania go w taki sposób, by migał, gdy kamera termowizyjna wykryje wtargnięcie. W podanym przykładzie sygnalizator świetlny można włączyć tylko w przypadku alarmów poza godzinami pracy, od 18:00 do 8:00 od poniedziałku do piątku; będzie on migał przez 30 sekund po każdej aktywacji.

Wymagany sprzęt

- Przewody połączeniowe (jeden niebieski i jeden czerwony, minimalna powierzchnia przekroju: 0,25 mm², maksymalna powierzchnia przekroju: 0,5 mm²)
- Sygnalizator świetlny (12 V DC, maks. 25 mA)

Uwaga

Maksymalna długość przewodów łączących zależy od powierzchni przekroju przewodu i poboru energii przez sygnalizator świetlny.

Fizyczne podłączanie urządzeń

1. Podłącz czerwony przewód do styku 2 (wyjście DC, 12 V DC) złącza we/wy kamery.
2. Podłącz drugi koniec czerwonego przewodu do złącza oznaczonego znakiem + na sygnalizatorze świetlnym.
3. Podłącz niebieski przewód do styku 4 (wejście cyfrowe) złącza we/wy kamery.
4. Podłącz drugi koniec niebieskiego przewodu do złącza oznaczonego znakiem – na sygnalizatorze świetlnym.

Konfigurowanie portów we/wy

Podłącz sygnalizator świetlny do kamery przez interfejs WWW kamery:

1. Przejdź do menu **System > Accessories > I/O ports** (**System > Akcesoria > Porty we/wy**).
2. W polu **Port 2** określ nazwę **Sygnalizator świetlny**.
3. W obszarze **Normal state (Stan normalny)** kliknij NO , aby ustawić normalny stan portu na otwarty (NO). To sprawi, że sygnalizator zacznie migać po wystąpieniu zdarzenia.

Tworzenie reguły

Aby kamera wysłała do sygnalizatora polecenie rozpoczęcia migania w momencie wykrycia zdarzenia, należy utworzyć w niej regułę.

1. Przejdź do menu **System > Events > Rules** (**System > Zdarzenia > Reguły**) i dodaj regułę.
2. W polu **Name (Nazwa)** wpisz **Sygnalizator świetlny**.

3. W polu **Wait between actions (Poczekaj między działaniami)** (o formacie gg:mm:ss) ustaw wartość 30 sekund.
4. Z listy warunków w obszarze **Application (Aplikacja)** wybierz aplikację do ochrony obwodowej.
5. Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**.
6. Kliknij opcję  , aby dodać inny warunek.
7. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
8. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.
9. Z listy akcji w obszarze **I/O (We/Wy)** wybierz opcję **Toggle I/O while the rule is active (Przełącz We/Wy, gdy reguła jest aktywna)**.
10. Z listy portów wybierz port **Flashing beacon (Sygnalizator świetlny)**.
11. W polu **State (stan)** ustaw **Active (aktywny)**.
12. Kliknij przycisk **Zapisz**.

Odstraszanie intruzów za pomocą dźwięku

By ostrzec i odstrzyszyć potencjalnych intruzów, dołącz do instalacji głośnik sieciowy.

W tym przykładzie wyjaśniono sposób podłączania do kamery sieciowego głośnika tubowego Axis i jego konfiguracji w celu odtworzenia klipu audio po wykryciu wtargnięcia przez kamerę termowizyjną. W tym przykładzie głośnik tubowy jest aktywowany tylko w przypadku alarmów poza godzinami pracy: od 18:00 do 08:00, od poniedziałku do piątku.

Podłącz urządzenia

1. Przejdź do menu **System > Edge-to-edge > Pairing (System > Edge-to-edge > Parowanie)**.
2. Wpisz adres IP, nazwę użytkownika oraz hasło dla głośnika. Należy użyć konta administratora lub operatora.
3. Kliknij przycisk **Połącz**.

Przesyłanie klipu audio do kamery

1. Przejdź do obszaru **Audio > Audio clips (Klipy audio)** i kliknij opcję .
2. Kliknij **+ Add clip (Dodaj klip)**.
3. Znajdź i prześlij klip audio.
4. Kliknij przycisk **Zamknij**.

Tworzenie reguły

Aby głośnik odtwarzał klip audio w momencie wykrycia zdarzenia przez kamerę, należy utworzyć w niej regułę.

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. W polu **Name (Nazwa)** wpisz **Odstrasz dźwiękiem**.
3. Z listy warunków w obszarze **Application (Aplikacja)** wybierz aplikację do ochrony obwodowej.
4. Wybierz opcję **Use this condition as a trigger (Użyj tego warunku jako wyzwalacza)**.
5. Kliknij opcję  , aby dodać inny warunek.
6. Z listy warunków w obszarze **Scheduled and recurring (Zaplanowane i cykliczne)** wybierz opcję **Schedule (Harmonogram)**.
7. Z listy harmonogramów wybierz **After hours (Po godzinach pracy)**.
8. Z listy akcji w obszarze **Audio clips (Klip audio)** wybierz opcję **Play audio clip (Odtwórz klip audio)**.
9. W sekcji **Clip (Klip)** zaznacz przesłany klip audio.

10. W obszarze **Audio output (Wyjście audio)** wybierz pozycję 1 dla sparowanego głośnika sieciowego.
11. Kliknij przycisk **Zapisz**.

Aktywowanie syreny stroboskopowej przez wejście wirtualne po wykryciu ruchu przez kamerę

Aby poinformować intruzów o ochronie, można użyć syreny stroboskopowej Axis.

W tym przykładzie wyjaśniono, jak spowodować uaktywnienie się profilu w syrenie stroboskopowej po każdym wykryciu ruchu przez aplikację AXIS Motion Guard.

Zanim zaczniesz:

- Utwórz w syrenie stroboskopowej nowe konto z uprawnieniami Operatora lub Administratora.
- Utwórz profil w syrenie stroboskopowej.
- Skonfiguruj aplikację AXIS Motion Guard w kamerze oraz utworzenie profilu 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:
 - **Nazwa:** Aktywacja portu wirtualnego
 - **Typ:** HTTP
 - **URL:** http://<adresIP>/axis-cgi/virtualinput/activate.cgi
Element <adresIP> zastąp 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 **Zapisz**.
5. Dodaj drugiego odbiorcę z następującymi informacjami:
 - **Nazwa:** Dezaktywacja portu wirtualnego
 - **Typ:** HTTP
 - **URL:** http://<adresIP>/axis-cgi/virtualinput/deactivate.cgi
Element <adresIP> zastąp 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 **Zapisz**.

Utworzenie dwóch reguł w kamerze:

1. Przejdź do obszaru **Rules (Reguły)** i dodaj regułę.
2. Wprowadź następujące informacje:
 - **Nazwa:** Aktywowanie wirtualnego WE/WY1
 - **Condition (Warunek):** Applications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)
 - **Action (Akcja):** Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)
 - **Recipient (Odbiorca):** Aktywacja portu wirtualnego
 - **Query string suffix (Sufiks ciągu zapytania):** schemaversion=1&port=1
3. Kliknij przycisk **Zapisz**.
4. Dodaj kolejną regułę z następującymi informacjami:

- Nazwa: Dezaktywacja wirtualnego WE/WY1
- Condition (Warunek): Applications (Aplikacje) > Motion Guard: Camera profile (Motion Guard: Profil kamery)
- Wybierz opcję Invert this condition (Odwróć ten warunek).
- Action (Akcja): Notifications > Send notification through HTTP (Powiadomienia > Wyślij powiadomienie przez HTTP)
- Recipient (Odbiorca): Dezaktywacja portu wirtualnego
- Query string suffix (Sufiks ciągu zapytania): schemaversion=1&port=1

5. Kliknij przycisk **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:
 - Nazwa: Wyzwalacz w wirtualnym wejściu 1
 - Condition (Warunek): I/O (We/Wy) > Virtual input (Wejście wirtualne)
 - Port: 1
 - Action (Akcja): Light and siren > Run light and siren profile while the rule is active (Światło i syrena > Uruchom profil oświetlenia i syreny, gdy reguła jest aktywna)
 - Profile (Profil): wybierz nowo utworzony profil
3. Kliknij przycisk **Zapisz**.

Wykrywanie ingerencji w sygnał wejściowy

W tym przykładzie wyjaśniono, w jaki sposób wysyłać wiadomość e-mail po odcięciu lub zwarcu obwodu sygnału wejściowego. Więcej informacji na temat złącza I/O: *page 28*.

1. Przejdź do obszaru **System > Accessories (Akcesoria) > I/O ports (Porty WE/WY)** i włącz **Supervised (Nadzorowane)** dla odpowiedniego portu.

Dodaj odbiorcę wiadomości e-mail:

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

Create a rule (Utwórz regułę):

1. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
2. Wprowadź nazwę reguły.
3. Z listy warunków w obszarze **I/O (WE/WY)** wybierz **Supervised input tampering is active (Sabotaż wejścia nadzorowanego jest aktywny)**.
4. Wybierz odpowiedni port.
5. Z listy akcji w menu **Notifications (Powiadomienia)** wybierz pozycję **Send notification to email (Wyślij powiadomienie emailem)**, a następnie wybierz odbiorcę z listy.

6. Wpisz temat i treść wiadomości e-mail.
7. Kliknij przycisk **Zapisz**.

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. Jako typ powiadomienia wybierz **Email (E-mail)**.
4. Wpisz adres e-mail odbiorcy.
5. Wpisz adres e-mail, z którego kamera ma wysyłać powiadomienia.
6. Podaj dane logowania do konta e-mail wysyłającego powiadomienia wraz z nazwą hosta SMTP i numerem portu.
7. Aby przetestować ustawienia poczty e-mail, kliknij **Test**.
8. Kliknij przycisk **Zapisz**.

Create a rule (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 **Zapisz**.

Automatyczne przesyłanie wiadomości e-mail w przypadku zamalowania obiektywu farbą w sprayu

Activate the tampering detection (Aktywacja wykrywania sabotażu):

1. Przejdź do menu **System > Detectors > Camera tampering (System > Detektory > Sabotaż kamery)**.
2. Ustaw wartość dla funkcji **Trigger delay (Opóźnienie wyzwalacza)**. Wartość ta wskazuje czas, jaki musi upłynąć przed wysłaniem wiadomości e-mail.

Dodaj odbiorcę wiadomości e-mail:

3. Przejdź do menu **System > Events > Recipients (System > Zdarzenia > Odbiorcy)** i dodaj odbiorcę.
4. Wprowadź nazwę odbiorcy.
5. Wybierz adres **E-mail**.
6. Wprowadź adres e-mail odbiorcy.
7. Kamera nie ma dedykowanego serwera poczty e-mail, więc należy się zalogować na inny serwer, aby wysyłać wiadomości e-mail. Podaj pozostałe informacje wymagane przez dostawcę poczty e-mail.
8. Kliknij przycisk **Test**, aby wysłać testową wiadomość e-mail.
9. Kliknij przycisk **Zapisz**.

Create a rule (Utwórz regułę):

10. Przejdź do menu **System > Events > Rules (System > Zdarzenia > Reguły)** i dodaj regułę.
11. Wprowadź nazwę reguły.

12. Z listy warunków w obszarze **Video (Wideo)** wybierz **Tampering (Sabotaż)**.
13. Z listy akcji w menu **Notifications (Powiadomienia)** wybierz pozycję **Send notification to email (Wyślij powiadomienie emailem)**, a następnie wybierz odbiorcę z listy.
14. Wpisz temat i treść wiadomości e-mail.
15. Kliknij przycisk **Zapisz**.

Dźwięk

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.
4. Jeżeli wprowadzisz jakiekolwiek zmiany w źródle sygnału wejściowego, kliknij przycisk **Apply changes (Zastosuj zmiany)**.

Edytuj profil strumienia używany do rejestracji:

5. Przejdź do okna **System > Stream profiles (System > Profile strumienia)** i wybierz profil strumienia.
6. Kliknij opcję **Include audio (Dołącz audio)** i włącz ją.
7. 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

Palety kolorów

Zastosowanie palety kolorów ułatwi wzrokowe rozróżnianie szczegółów na obrazie termowizyjnym. Barwy te są sztucznie generowane, aby odzwierciedlać różnice temperatur.

Można wybrać jedną z palet zainstalowanych w produkcie. Jeżeli operator ogląda strumień wideo, może wybrać dowolną z palet. Jeżeli strumień wideo jest używany wyłącznie przez aplikacje, należy wybrać paletę „white-hot”.

Nakładki

Nakładki są nakładane na strumień wideo. Służą one do dostarczania dodatkowych informacji podczas instalacji i konfiguracji produktu lub podczas rejestracji obrazu (np. znacznik czasowy). Można dodać tekst lub obraz.

Wskaźnik strumieniowania obrazu wideo jest innym typem nałożenia. Informuje on o tym, że strumień wideo transmitowany jest na żywo.

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

Uwaga

Aby zapewnić obsługę kodeka audio Opus, strumień MJPEG jest zawsze przesyłany przez RTP.

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.

W jaki sposób ustawienia obrazu, strumienia i profilu strumienia mogą na siebie wpływać?

Karta **Obraz** zawiera ustawienia kamery, które wpływają na wszystkie strumienie wideo przesyłane z produktu. Jeśli zmienisz parametry na tej karcie, natychmiast wpłynie to na wszystkie strumienie wideo i zapisy.

Karta **Strumień** zawiera ustawienia strumienia wideo. Te ustawienia są stosowane, gdy zażadasz strumienia wideo z produktu, ale nie podasz na przykład rozdzielczości lub poklatkowości. Zmiana ustawień na karcie **Strumień** nie wpływa na bieżące strumienie, ale będzie wprowadzona po rozpoczęciu nowego strumienia.

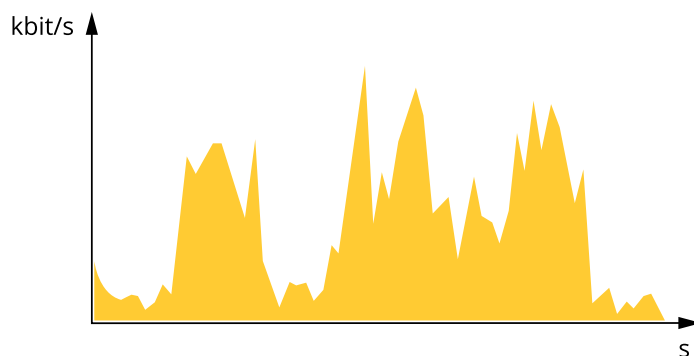
Ustawienia w opcji **Profil strumienia** nadpisują ustawienia z karty **Strumień**. Jeśli zażadasz strumienia z określonym profilem, to strumień będzie mieć ustawienia tego profilu. Jeśli zażadasz strumienia bez określania profilu lub zażadasz profilu strumienia, który nie został zdefiniowany w produkcie, strumień będzie mieć ustawienia z karty **Strumień**.

Sterowanie przepływnością bitową

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

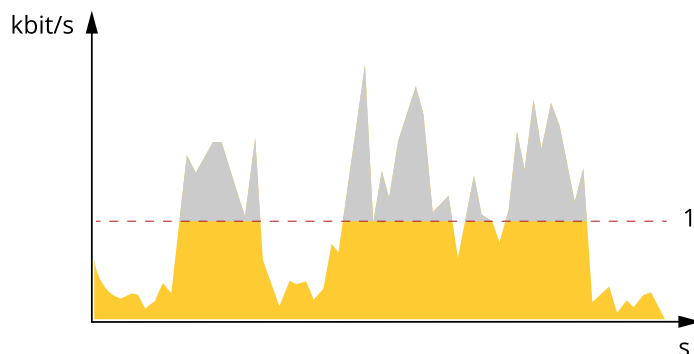
Zmienna przepływność bitowa (VBR)

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.

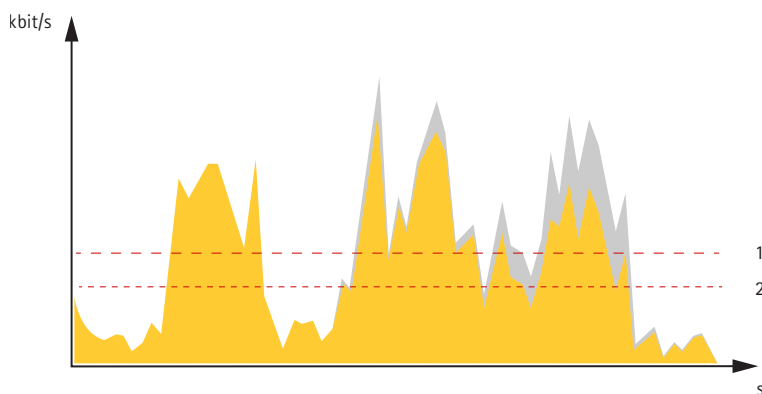


1 Docel. przepł. bitowa

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:

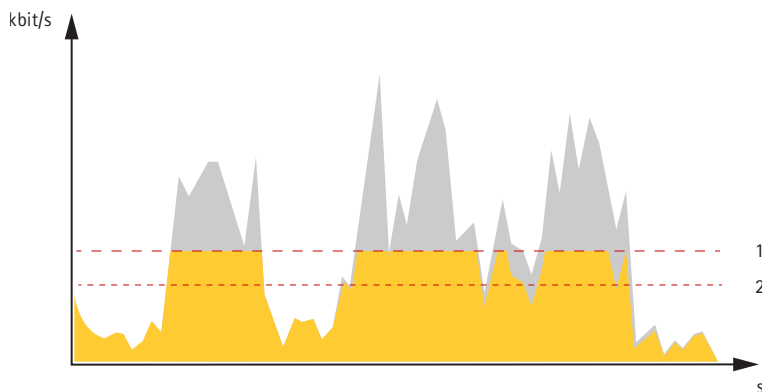
- Aby obliczyć przybliżone zapotrzebowanie na zasoby pamięci masowej, należy ustawić wartość docelową przepływności bitowej i czas retencji.
- Użyj kalkulatora przepływności bitowej, aby obliczyć średnią przepływność bitową w zależności od dostępnego miejsca w zasobach pamięci i czasu retencji.



1 Docel. przepł. bitowa

2 Rzeczywista średnia przepływność bitowa

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



1 Docel. przepł. bitowa

2 Rzeczywista średnia przepływność bitowa

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.

Uwaga

- Kilka aplikacji może być uruchomionych w tym samym czasie, ale niektóre z nich mogą ze sobą nie współpracować. Niektóre zestawy aplikacji mogą wymagać zbyt wiele mocy obliczeniowej lub pamięci przy ich jednoczesnym uruchomieniu. Przed uruchomieniem aplikacji należy sprawdzić, czy mogą one być uruchomione jednocześnie.

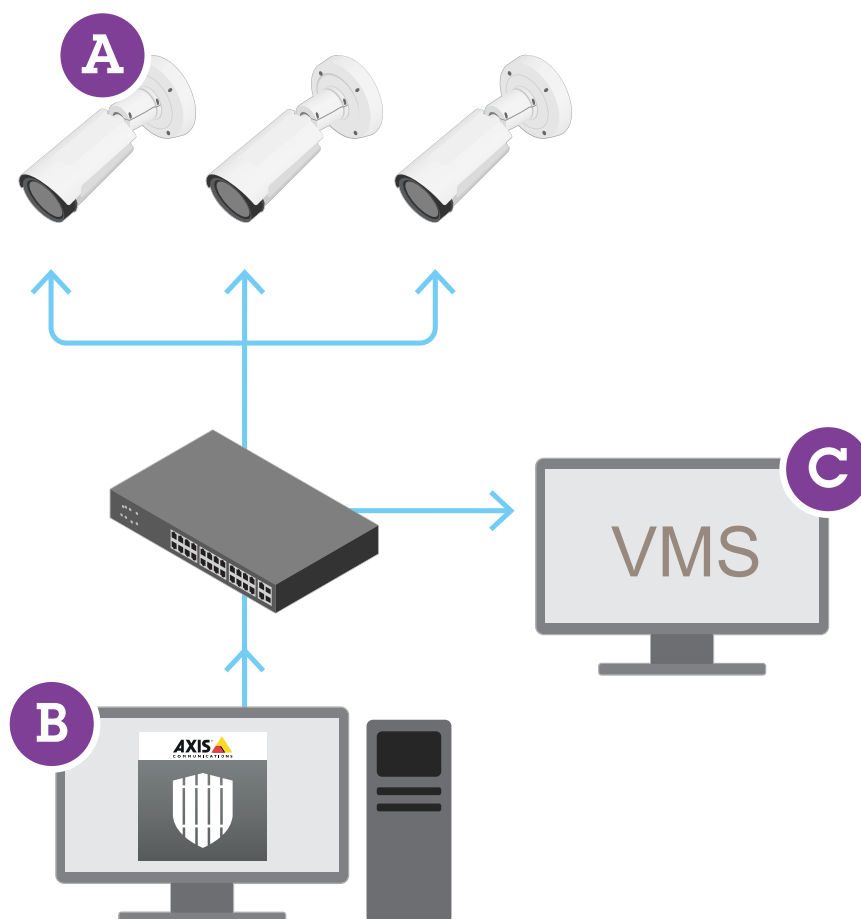
AXIS Perimeter Defender

AXIS Perimeter Defender to aplikacja do dozoru i ochrony obwodowej. Nadaje się ona idealnie do ochrony obwodowej tam, gdzie konieczne jest wzmocnienie systemu fizycznej kontroli dostępu poprzez dodanie niezawodnej detekcji wtargnięcia na teren.

AXIS Perimeter Defender jest przeznaczona przede wszystkim do ochrony tak zwanej strefy sterylnej, na przykład strefy wzdłuż płotu stanowiącego granicę obszaru. Termin „strefa sterylna” odnosi się do obszaru, w którym nie powinni znaleźć się ludzie.

Aplikacji AXIS Perimeter Defender można używać na zewnątrz pomieszczeń i budynków, aby:

- wykrywać poruszające się osoby,
- wykrywać poruszające się pojazdy, bez względu na ich typ.



Kamera może włączać aplikację w trybie kalibracji, AI lub obu tych trybach jednocześnie. W przypadku uruchomienia aplikacji tylko w trybie AI montaż kamer jest bardziej elastyczny i nie trzeba ich kalibrować.

Aplikacja AXIS Perimeter Defender składa się z interfejsu (B) służącego do instalacji i konfiguracji aplikacji w kamerach (A). System można tak skonfigurować, aby wysyłał alarmy do oprogramowania do zarządzania materiałem wizyjnym (C).

AXIS Perimeter Defender PTZ Autotracking to wtyczka do aplikacji AXIS Perimeter Defender, która korzysta z tego samego interfejsu. Wtyczka ta umożliwia sparowanie stałopozycyjnej kamery optycznej lub termowizyjnej z kamerą PTZ z serii Axis Q. Można wówczas zachować ciągłą detekcję w scenie za pomocą kamery stałopozycyjnej, podczas gdy kamera PTZ zapewnia automatyczne śledzenie i zbliżenia wykrytych obiektów.

Ważne

Wtyczka AXIS Perimeter Defender PTZ Autotracking wymaga kalibracji zarówno kamer stałopozycyjnych, jak i PTZ.

AXIS Perimeter Defender zawiera następujące typy scenariuszy detekcji:

- **Intrusion (Wtargnięcie):** wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu (dowolny kierunek i trajektoria).
- **Loitering (Podejrzane zachowanie):** wyzwala alarm, kiedy osoba lub pojazd pozostaje w strefie zdefiniowanej na podłożu przez czas dłuższy niż podana liczba sekund.
- **Zone-crossing (Przekroczenie strefy):** wyzwala alarm, kiedy osoba lub pojazd przekracza w określonej kolejności dwie lub większą liczbę stref zdefiniowanych na podłożu.
- **Conditional (Warunkowy):** wyzwala alarm, kiedy osoba lub pojazd znajdzie się w strefie zdefiniowanej na podłożu, nie przekraczając wcześniej innych zdefiniowanych na nim stref.

Cyberbezpieczeństwo

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

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

Axis Edge Vault

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

Podpisany system operacyjny

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

Bezpieczny start

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

Bezpieczny magazyn kluczy

Jest to zabezpieczone przed sabotażem środowisko do ochrony kluczy prywatnych i bezpiecznego wykonywania operacji kryptograficznych. Zapobiega nieautoryzowanemu dostępowi i złośliwemu wykradaniu w przypadku włamania do systemu. W zależności od wymogów bezpieczeństwa urządzenie Axis może mieć jeden lub kilka

sprzętowych modułów kryptograficznych, które udostępniają chroniony sprzętowo bezpieczny magazyn kluczy. W zależności od wymogów dotyczących zabezpieczeń urządzenie Axis może mieć jeden lub wiele sprzętowych kryptograficznych modułów obliczeniowych, takich jak TPM 2.0 (Trusted Platform Module) lub zabezpieczony element i/lub TEE (Trusted Execution Environment), które zapewniają ochronę sprzętową magazynu kluczy. Ponadto wybrane produkty Axis są wyposażone w bezpieczny magazyn kluczy z certyfikatem FIPS 140-2 poziomu 2.

Identyfikator urządzenia axis

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

Podpisany materiał wizyjny

podpis dodany do materiału wizyjnego umożliwia potwierdzenie autentyczności dowodowej bez konieczności potwierdzenia całego łańcucha pochodzenia pliku wideo. Każda kamera podpisuje materiał wizyjny za pomocą własnego unikatowego klucza, który jest bezpiecznie przechowywany w bezpiecznym magazynie kluczy. W trakcie odtwarzania wideo program odtwarzający informuje o tym, czy materiał jest nienaruszony. Podpisany materiał wizyjny umożliwia ustalenie, z której kamery materiał pochodzi, i wykrycie ewentualnych nieuprawnionych modyfikacji wprowadzonych w materiale po tym, jak opuścił on kamerę.

Zaszyfrowany system plików

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

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

Usługa powiadomień w systemach zabezpieczeń Axis

Axis świadczy usługę powiadamiania z informacjami o lukach w zabezpieczeniach i innych sprawach dotyczących bezpieczeństwa urządzeń Axis. Aby otrzymywać powiadomienia, możesz aktywować subskrypcję na stronie axis.com/security-notification-service.

Postępowanie z lukami w zabezpieczeniach

Aby maksymalnie ograniczyć narażenie rozwiązań klientów na ataki, firma Axis, będąca **organem numeracji w programie CVE (Common Vulnerability and Exposures)**, przestrzega standardów branżowych w zakresie zarządzania wykrytymi lukami w naszych urządzeniach, oprogramowaniu i usługach oraz reagowania w takich przypadkach. Aby uzyskać więcej informacji na temat zasad zarządzania lukami w zabezpieczeniach rozwiązań Axis, sposobu zgłaszania luk w zabezpieczeniach, wykrytych luk w zabezpieczeniach i odpowiednich porad dotyczących bezpieczeństwa, zob. axis.com/vulnerability-management.

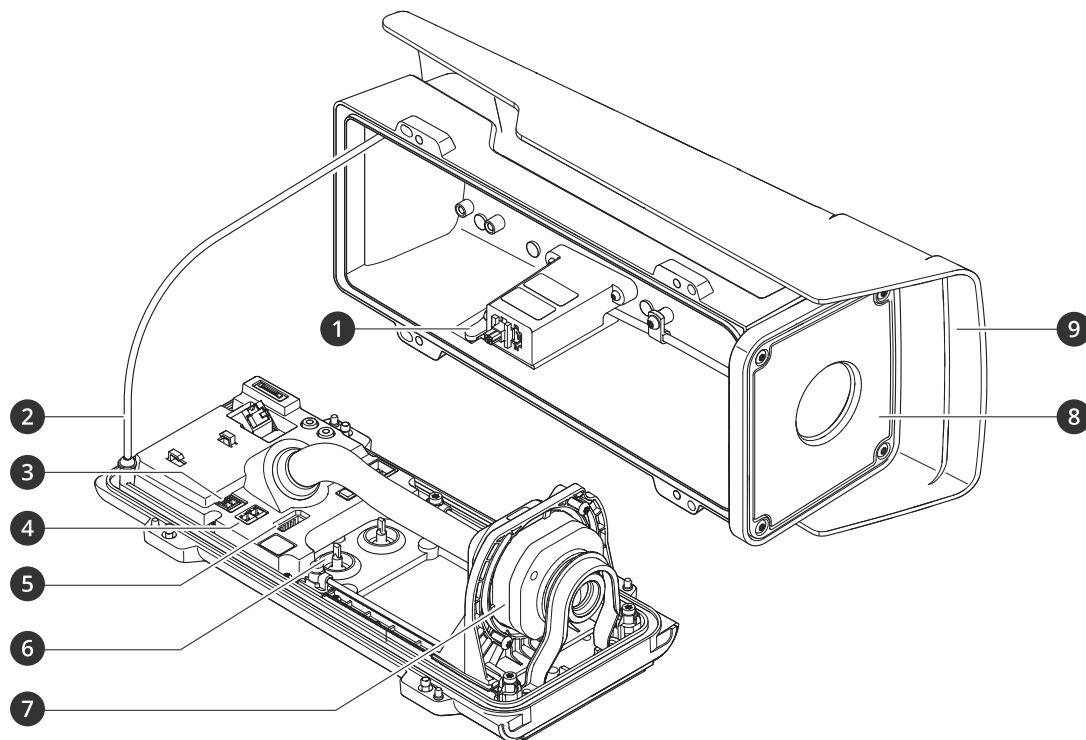
Bezpečne działanie urządzeń Axis

Urządzenia Axis z domyślnymi ustawieniami fabrycznymi są wstępnie skonfigurowane z zabezpieczonymi domyślnymi mechanizmami ochrony. Zalecamy korzystanie z lepiej zabezpieczonej konfiguracji podczas instalowania urządzenia. Aby dowiedzieć się więcej o podejściu Axis do cyberbezpieczeństwa, w tym o

najlepszych praktykach, zasobach i wytycznych dotyczących zabezpieczania urządzeń, odwiedź stronę axis.com/about-axis/cybersecurity.

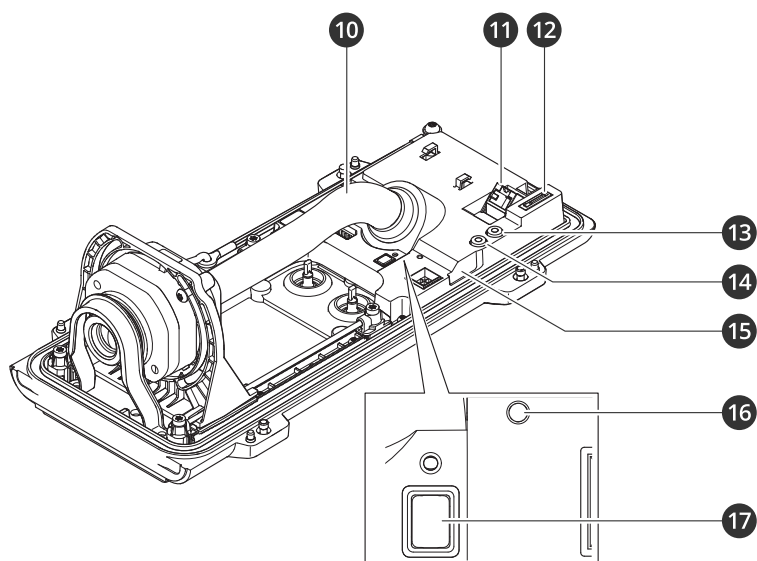
Specyfikacje

Przegląd produktów



- 1 Magnes alarmu wtargnięć
- 2 Przewód bezpieczeństwa
- 3 Złącze zasilania
- 4 Złącze RS485/422
- 5 Złącze I/O
- 6 Uszczelka kabla M20 (2x)
- 7 Jednostka optyczna*
- 8 Przednia szybka
- 9 Osłona chroniąca przed wpływem warunków atmosferycznych

*Wygląd jednostki optycznej może się różnić w zależności od wybranego wariantu obiektywu.



- 1 Osłona kabla
- 2 Złącze sieciowe (PoE)
- 3 Gniazdo kart microSD
- 4 Wyjście audio
- 5 Wejście audio
- 6 Czujnik alarmu wtargnięć
- 7 Dioda stanu
- 8 Przycisk kontrolny

Wskaźniki LED

Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.
- Wskaźniki LED wyłączają się po zamknięciu obudowy.

Dioda stanu	Wskazanie
Zgaszony	Połączenie i normalne działanie.
Zielony	Połączenie i normalne działanie.
Bursztynowy	Stałe światło podczas uruchamiania. Miga podczas aktualizacji oprogramowania urządzenia lub przywracania domyślnych ustawień fabrycznych.
Bursztynowy/czerwony	Miga na bursztynowo/czerwono, gdy połączenie sieciowe jest niedostępne lub przerwane.
Czerwony	Błąd aktualizacji oprogramowania urządzenia.

Brzęczyk

Brzęczyk asystenta poziomowania

Aby uzyskać informacje na temat przycisku kontrolnego służącego do poziomowania obrazu, zobacz [page 27](#).

Brzęczyk	Umieszczenie kamery
Dźwięk stały	Poziom
Szybkie sygnały dźwiękowe	Blisko poziom
Średnie sygnały dźwiękowe	Brak poziomu
Wolne sygnały dźwiękowe	Całkowity brak poziomu

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 wydymuj kartę palcami.
- Ryzyko utraty danych i uszkodzenia nagrań. Odłącz kartę SD od interfejsu WWW urządzenia, zanim ją wyjmiesz. Nie wydymuj 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 kontrolny ma następujące zastosowania:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *Przywróć domyślne ustawienia fabryczne, on page 35*.
- Upewniania się, że kamera jest zamontowana poziomo. Naciśnij przycisk i przytrzymaj go przez nie więcej niż dwie sekundy, aby uruchomić asystenta poziomowania; naciśnij przycisk ponownie, aby wyłączyć asystenta. Sygnał brzęczyka (patrz *page 26*) ułatwiający poziomowanie kamery. Kamera jest zamontowana poziomo, kiedy brzęczyk nie wyłącza się.

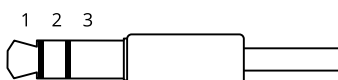
Złącza

Złącze sieciowe

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

Złącze audio

- Wejście audio** – wejście 3,5 mm dla mikrofonu cyfrowego, analogowego mikrofonu mono lub liniowego sygnału mono (w przypadku wejścia audio z sygnału stereofonicznego używany jest kanał lewy).
- Wyjście audio** – wyjście audio 3,5 mm (poziom linii), które można podłączyć do systemu nagłośnienia (PA) lub aktywnego głośnika z wbudowanym wzmacniaczem. Do wyjścia audio musi być użyte złącze stereo.



Wejście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Niezbalansowany mikrofon (z zasilaniem elektretowym lub bez) lub wejście liniowe	Zasilanie elektretowe po wybraniu	Masa
Sygnał cyfrowy	Zasilanie z obwodu pierścieniowego po wybraniu	Masa

Wyjście audio

1 Końcówka	2 Pierścień	3 Kołnierz
Kanał 1, wejście liniowe niezbalansowane, mono	Kanał 1, wejście liniowe niezbalansowane, mono	Masa

Złącze I/O

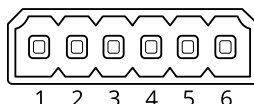
Złącze I/O służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z wykrywaniem ruchu, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe 12 V) złącze WE/WY zapewnia interfejs do:

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 zbitcia szyby.

Nadzorowane wejście – Umożliwia wykrywanie sabotażu wejścia cyfrowego.

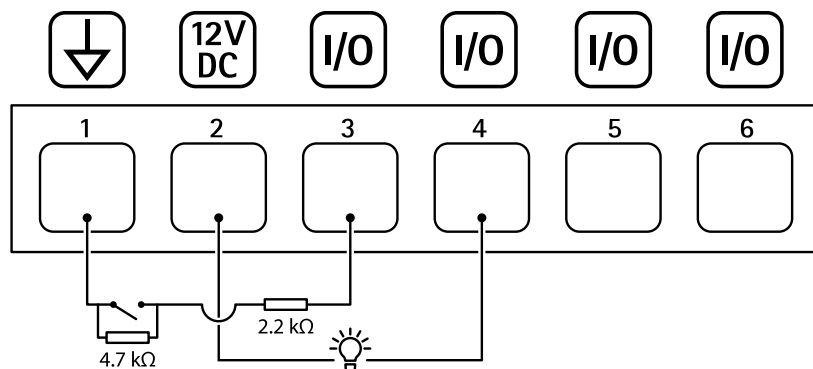
Wyjście cyfrowe – Do podłączenia urządzeń zewnętrznych, takich jak przekaźniki czy diody LED. Podłączonymi urządzeniami można zarządzać poprzez API VAPIX®, zdarzenie lub interfejs WWW urządzenia.

6-pinowego bloku 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 = 50 mA
Konfigurowalne (wejście lub wyjście)	3–6	Wejście cyfrowe lub wejście nadzorowane – podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Aby mieć możliwość korzystania z nadzorowanego wejścia, zamontuj rezystory końca linii. Patrz diagram połączeń, aby uzyskać informacje na temat podłączania rezystorów.	Od 0 do maks. 30 V DC
		Wyjście cyfrowe – podłączone wewnętrznie do styku 1 (masa DC), gdy aktywne i niepodłączone, gdy nieaktywne. W przypadku 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

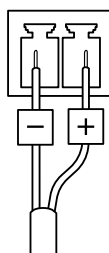
Przykład:



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

Złącze zasilania

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

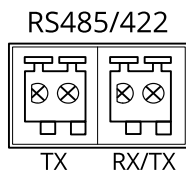


Złącze RS485/RS422

Dwa 2-stykowe bloki złączy interfejsu szeregowego RS485/RS422

Port szeregowy można skonfigurować do obsługi następujących funkcji:

- RS485 half duplex (dwużyłowy)
- RS485 full duplex (czterużyłowy)
- Dwuprzewodowy RS422 simplex
- Czteroprzewodowy RS422 full duplex do komunikacji P2P



Funkcje	Uwagi
RS485/RS422 TX(A)	Para TX do RS422 i 4-przewodowego RS485
RS485/RS422 TX(B)	
RS485A alt RS485/422 RX (A)	Para RX dla wszystkich trybów (połączone RX/TX dla 2-przewodowego RS485)

RS485B alt RS485/422 RX (B)	
-----------------------------	--

Uwaga

Aby używać kamery wraz z AXIS T99 Positioning Unit, podłącz ją do RS485A i RS485B (RX/TX).

Sterowniki PTZ

APTP

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele z interfejsem RS485 2-wire:

- Moduły pozycjonujące z serii AXIS T99A.
Informacje o zgodnych produktach Axis można znaleźć na stronie axis.com.

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	APTP
Wersja	1.1.0

Domyślna konfiguracja seryjna:

Portmode	RS485
BaudRate	115,200
DataBits	8
StopBits	1
Parity	Brak

DOMYŚLNE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	tak	tak	tak
Pochylenie	tak	tak	tak

Pelco

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele:

- Pelco DD5-C
- Pelco Esprit ES30C/ES31C
- Pelco LRD41C21
- Pelco LRD41C22
- Pelco Spectra III
- Pelco Spectra IV
- Pelco Spectra Mini
- Videotec DTRX3/PTH310P
- Videotec ULISSE
- PTK AMB
- YP3040

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	Pelco
Wersja	4.17

Domyślna konfiguracja seryjna:

Portmode	RS485
BaudRate	2,400
DataBits	8
StopBits	1
Parity	Brak

DOMYŚLNE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	nie	tak	tak
Pochylenie	nie	tak	tak
Zoom	nie	tak	tak
Ostrość	nie	tak	tak
Przysłona	nie	tak	tak

Autoliris	tak
AutoFocus	tak
IrCutFilter	nie

BackLight	tak
OSDMenu	tak

Visca

Oto lista modeli obsługiwanych przez ten sterownik. Fizyczna instalacja zależy od produktu Axis i jednostki PTZ.

Ważne

Sprawdź, czy w jakiej komunikacji szeregowej są obsługiwane Twój produkt Axis i jednostka PTZ.

Obsługiwane modele z interfejsem RS422 4-wire:

- Sony EVI-D70/D70P
- WISKA DCP-27 (PT-head)

Obsługiwane modele z interfejsem RS232 (może być konieczny zewnętrzny przetwornik RS422-4-wire/RS232):

- Axis EVI-D30/D31
- Sony EVI-G20/G21
- Sony EVI-D30/D31
- Sony EVI-D100/D100P
- Sony EVI-D70/D70P

Inne modele mogą być obsługiwane, ale nie zostało to zweryfikowane przez Axis.

Informacje techniczne

DOMYŚLNE funkcje dla sterownika PTZ:

Sterownik	Visca/EVI
Wersja	4.11

Domyślna konfiguracja seryjna:

Portmode	RS422
BaudRate	9,600
DataBits	8
StopBits	1
Parity	Brak

DOMYŚLNE obsługiwane funkcje w tym sterowniku PTZ:

Uwaga

Możliwości mogą się różnić zależnie od jednostki PTZ (mogą być zarówno mniejsze, jak i większe).

Ruch	Bezwzględny	Względny	Nagrywanie ciągłe
Obrót	tak	tak	tak
Pochylenie	tak	tak	tak
Zoom	tak	tak	tak
Ostrość	tak	tak	tak
Przysłona	tak	tak	nie

Autolris	tak
AutoFocus	tak
IrCutFilter	tak
BackLight	tak
OSDMenu	nie

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 rozpylać detergentu bezpośrednio na urządzenie. Detergent należy najpierw nanieść na miękką ściereczkę, a następnie przetrzeć nią urządzenie.
 - 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 i łagodnym mydłem niezawierającym środków ściernych.
 3. Aby nie dopuścić do powstania plam, należy wytrzeć urządzenie do sucha miękką, delikatną ściereczką.

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 25.
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 *Portalu AXIS OS: ścieżka aktualizacji*.
- Upewnij się, że podczas całego procesu aktualizacji urządzenie jest podłączone do źródła zasilania.

Uwaga

- Aktualizacja urządzenia Axis do najnowszej dostępnej wersji systemu AXIS OS umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją. Przejdź do strony axis.com/support/device-software, aby znaleźć najnowszą wersję systemu AXIS OS oraz informacje o wersji.
1. Pobierz na komputer plik systemu AXIS OS dostępny bezpłatnie na stronie axis.com/support/device-software.
 2. Zaloguj się do urządzenia jako administrator.
 3. Wybierz kolejno opcje **Maintenance > AXIS OS upgrade (Konserwacja > Aktualizacja systemu AXIS OS) > Upgrade (Aktualizuj)**.

Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie.

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 35.*

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 6.*

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.

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.

Problemy z obsługą urządzenia

Przedni grzejnik i wycieraczka nie działają

Jeżeli nie włącza się przedni grzejnik lub wycieraczka, sprawdź, czy górna pokrywa jest prawidłowo zamocowana do dolnej części obudowy.

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.
- Używanie palet kolorów wpływa na obciążenie procesora, co z kolei wpływa na liczbę klatek na sekundę.

Kontakt z pomocą techniczną

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

T10208523_pl

2026-02 (M7.2)

© 2024 – 2026 Axis Communications AB