# AXIS Camera Station 5

## Podręcznik użytkownika

# Informacje AXIS Camera Station 5

AXIS Camera Station 5 jest kompletnym systemem do dozoru i nagrywania przeznaczonym do małych i średnich instalacji.

Jest kompatybilny ze wszystkimi utrzymywanymi wersjami oprogramowania układowego AXIS OS w ramach ścieżek aktywnych, wsparcia długoterminowego (LTS) oraz wsparcia dla określonych produktów (PSS)*. Więcej informacji znajduje się w informacjach o wersji programu AXIS Camera Station 5 lub na portalu *AXIS OS Portal*. Aby sprawdzić, które produkty współpracują z oprogramowaniem AXIS Camera Station 5, zobacz *Kompatybilne produkty*.

*Zapewniamy zgodność ze starszymi wersjami oprogramowania układowego AXIS OS, o ile jest to komercyjnie opłacalne.

## Opcja dostępu

**AXIS Camera Station 5 serwer –** obsługuje komunikację z kamerami, wideoenkoderami i urządzeniami dodatkowymi w systemie. Dostępna łączna przepustowość nakłada limit liczby kamer i enkoderów, z którymi poszczególne serwery mogą się komunikować.

**AXIS Camera Station 5 klient –** zapewnia dostęp do zapisów, obrazu wideo na żywo, dzienników i konfiguracji. Oprogramowanie klienckie można zainstalować na dowolnym komputerze. W ten sposób uzyskuje się dostęp do podglądu zdalnego i możliwość sterowania z dowolnego miejsca w sieci korporacyjnej lub przez Internet.

**Mobilna aplikacja Axis do oglądania obrazu: –** zapewnia dostęp do zapisów i obrazu wideo na żywo w wielu systemach. Aplikację można zainstalować na urządzeniach z systemem Android i iOS, zapewniając zdalne przeglądanie materiałów z innych lokalizacji. Korzysta ona z protokołu HTTPS do komunikowania się z serwerem AXIS Camera Station 5. Skonfiguruj porty komunikacji mobilnej i strumieniowania mobilnego w sposób opisany w temacie *Zapisy ogólne* w rozdziale Ustawienia serwera. Aby dowiedzieć się więcej na temat korzystania z aplikacji, patrz *Instrukcja obsługi aplikacji mobilnej AXIS Camera Station*.

## Samouczki wideo

Więcej szczegółowych przykładów korzystania z systemu można znaleźć na stronie *Samouczki filmowe o aplikacji AXIS Camera Station*.

## Funkcje systemowe

Więcej informacji o funkcjach systemu można znaleźć w *Przewodniku po funkcjach AXIS Camera Station*.

## Co nowego?

Opisy nowych funkcji dodanych w kolejnych wersjach oprogramowania AXIS Camera Station znajdują się w temacie *Nowości w programie AXIS Camera Station*.

## Przydatne łącza dla administratora

Oto kilka tematów, które mogą Cię zainteresować:

- *Łączenie z serwerem, on page 8*
- *Konfiguruj urządzenia, on page 40*
- *Konfigurowanie pamięci masowej, on page 69*
- *Konfigurowanie nagrywania i zdarzeń, on page 74*
- *Konfigurowanie połączonych usług, on page 112*
- *Konfigurowanie serwera, on page 116*
- *Konfigurowanie licencji, on page 124*
- *Konfigurowanie zabezpieczeń, on page 127*

## Więcej instrukcji

- *Przewodnik integracji AXIS Camera Station*
- *Nowości w programie AXIS Camera Station*
- *Przewodnik po instalacji i migracji AXIS Camera Station*
- *Aplikacja mobilna AXIS Camera Station*
- *Przewodnik po funkcjach AXIS Camera Station*
- *Samouczki filmowe o aplikacji AXIS Camera Station*
- *Poradnik rozwiązywania problemów dotyczących aplikacji AXIS Camera Station*
- *Instrukcje wzmacniania zabezpieczeń systemu AXIS Camera Station*

## Przydatne łącza dla operatora

Oto kilka tematów, które mogą Cię zainteresować:

- *Przewodnik wprowadzający dla operatorów programu AXIS Camera Station*
- *Łączenie z serwerem, on page 8*
- *Konfigurowanie klienta, on page 108*
- *Podgląd na żywo, on page 12*
- *Odtwarzanie nagrań, on page 22*
- *Eksportuj nagrania, on page 24*
- *Ściągawka dla użytkowników aplikacji AXIS Camera Station — sprawdzanie i eksportowanie*

## Szybki Start

Ten samouczek przeprowadzi Cię przez podstawowe kroki, które pozwolą Ci uruchomić system.

Zanim zaczniesz:

- Skonfiguruj sieć w zależności od instalacji. Patrz *Network configuration (Konfiguracja sieci)*.
- W razie potrzeby skonfiguruj porty serwera. Patrz *Konfiguracja portu serwera*.
- Weź pod uwagę kwestie bezpieczeństwa. Patrz *Kwestie dotyczące bezpieczeństwa*.

Administrator:

1. *Uruchom system VMS*
2. *Dodawanie urządzeń*
3. *Konfiguracja metody zapisu, on page 5*

Operator:

1. *Oglądaj materiał wideo na żywo, on page 6*
2. *Wyświetl nagrania, on page 6*
3. *Eksportuj nagrania, on page 6*
4. *Odtwarzanie i weryfikacja zapisów w AXIS File Player, on page 6*

### Uruchom system VMS

Kliknij dwukrotnie ikonę klienta AXIS Camera Station 5, aby uruchomić klienta. Przy pierwszym uruchomieniu klient próbuje zalogować się do serwera AXIS Camera Station 5 zainstalowanego na tym samym komputerze co klient.

Można nawiązać połączenie z wieloma serwerami AXIS Camera Station 5 na kilka sposobów. Patrz *Łączenie z serwerem*.

### Dodawanie urządzeń

Strona **Add devices (Dodaj urządzenia)** zostanie otwarta przy pierwszym uruchomieniu AXIS Camera Station 5. AXIS Camera Station 5 przeszuka sieć pod kątem połączonych urządzeń i wyświetli listę znalezionych urządzeń. Patrz *Dodawanie urządzeń*.

1. Wybierz z listy kamery, które chcesz dodać. Jeśli nie możesz znaleźć kamery, kliknij **Manual search (Wyszukiwanie ręczne)**.
2. Kliknij **Dodaj**.
3. Wybierz **Quick configuration (Szybka konfiguracja)** lub **Site Designer configuration (Konfiguracja AXIS Site Designer)**. Kliknij **Next (Dalej)**. Patrz *Importowanie projektów z aplikacji Site Designer, on page 43*.
4. Użyj ustawień domyślnych i upewnij się, że metoda zapisu jest ustawiona na **None (Brak)**. Kliknij przycisk **Install (Instaluj)**.

### Konfiguracja metody zapisu

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę.
3. Włącz **Motion detection (Po detekcji ruchu)**, or **Continuous (Ciągłe)** lub obie te opcje.
4. Kliknij przycisk **Apply (Zastosuj)**.

## Oglądaj materiał wideo na żywo

1. Otwórz kartę **Live view (Podgląd na żywo)**.
2. Wybierz kamerę, aby oglądać jej obraz na żywo.

Więcej informacji: *Podgląd na żywo, on page 12*.

## Wyświetl nagrania

1. Otwórz kartę **Recordings (Nagrania)**.
2. Wybierz kamerę, z której chcesz wyświetlić nagrania.

Więcej informacji: *Nagrania, on page 22*.

## Eksportuj nagrania

1. Otwórz kartę **Recordings (Nagrania)**.
2. Wybierz kamerę, z której chcesz eksportować nagrania.
3. Kliknij , aby wyświetlić znaczniki wyboru.
4. Przeciągnij odpowiednie znaczniki, aby uwzględnić zapis, który chcesz wyeksportować.
5. Kliknij , aby otworzyć kartę **Export (Eksportuj)**.
6. Kliknij przycisk **Export... (Eksportuj)**.

Więcej informacji: *Eksportuj nagrania, on page 24*.

## Odtwarzanie i weryfikacja zapisów w AXIS File Player

1. Przejdź do folderu z wyeksportowanymi nagraniami.
2. Kliknij dwukrotnie AXIS File Player.
3. Kliknij w celu wyświetlenia notatek dotyczących nagrania.
4. Aby zweryfikować podpis cyfrowy:
   4.1. Przejdź do menu **Tools > Verify digital signature (Narzędzia > Weryfikuj podpis cyfrowy)**.
   4.2. Wybierz **Validate with password (Uwierzytelnij hasłem)** i wprowadź hasło.
   4.3. Kliknij przycisk **Verify (Weryfikuj)**. Zostanie wyświetlona strona wyników weryfikacji.

Uwaga

- Podpis cyfrowy różni się od podpisywanego pliku wideo. Podpisane wideo umożliwia prześledzenie wideo z powrotem do kamery, z której pochodzi, umożliwiając sprawdzenie, czy nagranie nie zostało zmodyfikowane. Więcej informacji można znaleźć w sekcji *Signed video (Podpisane wideo)* i instrukcji użytkownika kamery.
- Jeżeli przechowywane pliki nie mają połączenia z bazą danych programu AXIS Camera Station (pliki nieindeksowane), należy poddać je konwersji, by możliwe było odtwarzanie ich w programie AXIS File Player. Aby uzyskać wsparcie w tym zakresie, prosimy o kontakt z pomocą techniczną Axis.

## Network configuration (Konfiguracja sieci)

Zanim skorzystasz z AXIS Camera Station 5, skonfiguruj ustawienia proxy lub zapory, jeśli klient AXIS Camera Station 5, serwer AXIS Camera Station 5 i połączone urządzenia sieciowe znajdują się w różnych sieciach.

### Ustawienia proxy klienta

Jeśli klient i serwer są oddzielone serwerem proxy, skonfiguruj ustawienia proxy klienta.

1. Otwórz klienta AXIS Camera Station 5.

2. Kliknij **Change client proxy settings (Zmień ustawienia proxy klienta)**.
3. Zmień ustawienia proxy klienta. Patrz *Ustawienia proxy klienta*.
4. Kliknij **OK**.

**Ustawienia proxy na serwerze**

Jeśli urządzenia sieciowe i serwerowe są oddzielone serwerem proxy, skonfiguruj ustawienia proxy serwera.

1. Otwórz aplikację AXIS Camera Station 5 Service Control.
2. Wybierz **Modify settings (Zmień ustawienia)**.
3. W sekcji ustawień proxy użyj domyślnego ustawienia **System account internet option** lub wybierz opcję **Use manual proxy settings (Użyj ręcznych ustawień proxy)**. Patrz *Zapisy ogólne*.
4. Kliknij przycisk **Zapisz**.

**NAT i Zapora sieciowa**

Jeśli klient i serwer są oddzielone przez NAT, zaporę sieciową lub podobny element, należy skonfigurować NAT lub zaporę tak, aby ruch portu HTTP, portu TCP i portu przesyłania strumieniowego, które określono w usłudze AXIS Camera Station 5 Service Control, może przechodzić przez zaporę lub NAT. Skontaktuj się z administratorem sieci w celu uzyskania instrukcji dotyczących konfigurowania NAT lub zapory.

Więcej informacji znajduje się w sekcji *Lista portów dotycząca AXIS Camera Station 5, on page 187*.

## Konfiguracja portu serwera

Serwer AXIS Camera Station używa portów 55752 (HTTP), 55754 (TCP), 55756 (komunikacja mobilna) oraz 55757 (strumieniowanie w sieci komórkowej) do komunikacji między serwerem a klientem. W razie potrzeby porty można zmieniać w usłudze AXIS Camera Station Service Control.

Więcej informacji, patrz *Zapisy ogólne* lub *Często zadawane pytania*.

## Kwestie dotyczące bezpieczeństwa

Aby zapobiec nieuprawnionemu dostępowi do kamer i zapisów, należy pamiętać o następujących kwestiach:

- Używaj silnych haseł dla wszystkich urządzeń sieciowych (kamer, koderów wideo i urządzeń pomocniczych).
- Zainstaluj serwer AXIS Camera Station 5, kamery, kodery wideo i urządzenia pomocnicze w zabezpieczonej sieci oddzielonej od sieci biurowej. Klienta AXIS Camera Station 5 możesz zainstalować na komputerze w innej sieci, na przykład sieci z dostępem do Internetu.
- Upewnij się, że wszyscy użytkownicy mają silne hasła. Usługa Windows® Active Directory zapewnia wysoki poziom zabezpieczeń.

## Łączenie z serwerem

Za pomocą klienta AXIS Camera Station 5 można nawiązywać połączenia z serwerami zainstalowanymi na komputerze lokalnym lub w innym miejscu w sieci. Połączenie z serwerem AXIS Camera Station 5 można nawiązać na kilka sposobów:

**Ostatni używany serwer –** Nawiąż połączenie z serwerami użytymi w poprzedniej sesji.

**Ten komputer –** Nawiąż połączenie z serwerem zainstalowanym na tym samym komputerze, co aplikacja kliencka.

**Serwer zdalny –** Patrz *Łączenie z serwerem zdalnym, on page 8*.

**Axis Secure Remote Access –** Patrz *Zaloguj się do AXIS Secure Remote Access, on page 9*.

Uwaga

Gdy klient próbuje nawiązać połączenie z serwerem po raz pierwszy, sprawdza identyfikator certyfikatu serwera. Aby mieć pewność, że nawiązujesz połączenie z odpowiednim serwerem, ręcznie porównaj identyfikator certyfikatu z identyfikatorem widocznym w aplikacji AXIS Camera Station 5 Service Control. Patrz *Zapisy ogólne, on page 186*.

| | |
|---|---|
| **Server list (Lista serwerów)** | Aby połączyć się z serwerami z listy serwerów, wybierz serwer z menu rozwijanego **Server list (Lista serwerów)**. Kliknij , aby utworzyć lub edytować listy serwerów. Patrz *Listy serwerów*. |
| **Import server list (Importuj listę serwerów)** | Aby zaimportować plik listy serwerów wyeksportowany z AXIS Camera Station 5, kliknij **Import server list (Importuj listę serwerów)** w prawym dolnym rogu i przejdź do pliku .msl. Patrz *Listy serwerów*. |
| **Delete saved passwords (Usuń zapisane hasła)** | Aby usunąć zapisane nazwy użytkowników i hasła ze wszystkich połączonych serwerów, kliknij **Delete saved passwords (Usuń zapisane hasła)**. |
| **Change client proxy settings (Zmień ustawienia klienta proxy)** | Aby połączyć się z serwerem, konieczna może być zmiana ustawień serwera proxy klienta. W tym celu kliknij **Change client proxy settings (Zmień ustawienia serwera proxy klienta)**. Patrz *Ustawienia proxy klienta*. |

## Łączenie z serwerem zdalnym

1. Wybierz opcję **Remote server (Serwer zdalny)**.
2. Wybierz serwer z listy rozwijanej **Remote server (Serwer zdalny)** albo wpisz adres IP lub DNS. Jeżeli serwera nie ma na liście, kliknij , aby ponownie wczytać wszystkie dostępne serwery zdalne. Jeżeli na serwerze skonfigurowano akceptowanie połączenia od klientów na portach innych niż domyślny 55754, wprowadź adres IP, a nim numer portu, na przykład 192.168.0.5:46001.
3. Możesz:
   - Wybierz **Log in as current user (Zaloguj się jako bieżący użytkownik)**, aby zalogować się jako obecny użytkownik systemu Windows®.
   - Wyczyść pole wyboru **Zaloguj się jako bieżący użytkownik** i kliknij przycisk **Zaloguj**. Zaznacz opcję **Other user (Inny użytkownik)** i podaj inną nazwę użytkownika oraz hasło, aby się zalogować za pomocą tych poświadczeń.

## Zaloguj się do AXIS Secure Remote Access

Ważne

Aby zwiększyć bezpieczeństwo i funkcjonalność, uaktualniamy funkcję **Axis Secure Remote Access** (v1) do **Axis Secure Remote Access v2**. Obecna wersja zostanie wycofana 1 grudnia 2025 r. Zalecamy przejście na funkcję Axis Secure Remote Access v2. przed tym terminem.

Co to oznacza dla systemu AXIS Camera Station 5?

- Po 1 grudnia 2025 r. zdalny dostęp do systemu za pośrednictwem funkcji **Axis Secure Remote Access** (v1) nie będzie możliwy.
- Aby korzystać z funkcji **Axis Secure Remote Access v2**, należy wykonać uaktualnienie do AXIS Camera Station Pro w wersji 6.8. Do 1 marca 2026 r. aktualizacja jest bezpłatna dla wszystkich użytkowników systemu AXIS Camera Station 5.

Uwaga

- Klient łączący się z serwerem za pomocą usługi Axis Secure Remote Access. Serwer nie może uaktualnić klienta automatycznie.
- Jeśli serwer proxy znajduje się między urządzeniem sieciowym a serwerem AXIS Camera Station 5, należy skonfigurować ustawienia serwera proxy w systemie Windows na serwerze AXIS Camera Station 5, aby umożliwić dostęp do serwera za pomocą usługi AXIS Secure Remote Access.

1. Kliknij łącze **Sign in to AXIS Secure Remote Access (Zaloguj się do AXIS Secure Remote Access)**.
2. Wprowadź dane swojego konta MyAxis. Patrz *Axis Secure Remote Access*.
3. Kliknij przycisk **Sign in (Zaloguj)**.
4. Kliknij **Grant (Przyznaj)**.

## Ustawienia proxy klienta

Te ustawienia mają zastosowanie do serwera proxy, który znajduje się między klientem AXIS Camera Station 5 a serwerem AXIS Camera Station 5.

Uwaga

Za pomocą aplikacji AXIS Camera Station 5 Service Control można konfigurować ustawienia serwera proxy umieszczonego między serwerem AXIS Camera Station 5 i kamerami sieciowymi. Patrz *AXIS Camera Station 5 Aplikacja Service Control*.

Wybierz opcję odpowiednią do swojej konfiguracji.

- **Direct connection (Połączenie bezpośrednie)**: Wybierz tę opcję, jeśli między klientem AXIS Camera Station 5 a serwerem AXIS Camera Station 5 nie ma serwera proxy.
- **Use Internet Options settings (Użyj ustawień opcji internetowych)** (domyślne): Wybierz tę opcję, aby używać ustawień systemu Windows.
- **Use manual proxy settings (Użyj ręcznych ustawień proxy)**: Wybierz tę opcję, aby ręcznie skonfigurować ustawienia serwera proxy. W sekcji Ustawienia ręczne wprowadź wymagane informacje.
  - **Adres**: Wprowadź adres lub nazwę hosta serwera proxy.
  - **Port**: Wprowadź numer portu serwera proxy.
  - **Do not use proxy server for addresses beginning with (Nie używaj serwera proxy dla adresów zaczynających się od)**: Wpisz serwery, które chcesz wykluczyć z dostępu za pośrednictwem serwera proxy. Poszczególne wpisy rozdzielaj średnikami. W adresach i nazwach hostów można używać symboli wieloznacznych, na przykład: „192.168.*" lub „*.mydomain.com".
  - **Always bypass proxy server for local addresses (Zawsze pomijaj serwer proxy dla adresów lokalnych)**: Zaznacz tę opcję, aby omijać serwer proxy podczas łączenia się z serwerem zainstalowanym na lokalnym komputerze. Adresy lokalne nie mają rozszerzenia nazwy domeny, na przykład http://webserver/, http://localhost, http://loopback, lub http://127.0.0.1.

## AXIS Camera Station 5 klient

Jeśli używasz aplikacji AXIS Camera Station 5 po raz pierwszy, zostanie otwarta strona Add devices (Dodaj urządzenia) na karcie Configuration (Konfiguracja). Patrz *Dodawanie urządzeń*.

**Karty**

| | |
|---|---|
| **Podgląd na żywo** | Wyświetlanie filmowego obrazu na żywo z podłączonych kamer. Patrz *Podgląd na żywo*. |
| **Nagrania** | Wyszukiwanie, odtwarzanie i eksportowanie nagrań. Patrz *Nagrania*. |
| **Inteligentne wyszukiwanie 1** | Znajdź ważne zdarzenia w nagranym obrazie filmowym za pomocą funkcji wyszukiwania ruchu. Patrz *Inteligentne wyszukiwanie 1*. |
| **Wyszukiwanie danych** | Wyszukiwanie danych z zewnętrznego źródła lub systemu i śledzenie tego, co wydarzyło się w czasie każdego zdarzenia. Patrz *Wyszukiwanie danych, on page 37*. |
| **Konfiguracja** | Administrowanie i zarządzanie podłączonymi urządzeniami oraz ustawieniami klienta i serwerów. Patrz *Konfiguracja*. |
| **Klawisze skrótu** | Lista klawiszy szybkiego dostępu do działań. Patrz *Klawisze skrótu*. |
| **Dzienniki** | Rejestry alarmów, zdarzeń i kontroli. Patrz *Dzienniki*. |
| **Zarządzanie dostępem** | Konfigurowanie i zarządzanie posiadaczami kart, grupami, drzwiami, strefami i regułami dostępu w systemie. Patrz *Zarządzanie dostępem, on page 160*. |
| **Inteligentne wyszukiwanie 2** | Zaawansowane filtry do znajdowania pojazdów i osób na podstawie charakterystyki. Patrz *Inteligentne wyszukiwanie 2, on page 33*. |
| **Monitorowanie stanu systemu** | Monitorowanie danych dotyczących kondycji z jednego lub wielu systemów AXIS Camera Station 5. Patrz *Monitorowanie stanu systemu BETA, on page 169*. |
| **Powiadomienia z podglądu na żywo** | Zainicjowanie akcji podglądu na żywo powoduje automatyczne przechodzenie do karty Powiadomienia z podglądu na żywo w ustawieniach widoku lub kamery. Patrz *Tworzenie działań podglądu na żywo*. |
| **Powiadomienia dotyczące nagrań** | Na karcie Alarms (Alarmy) lub Logs (Dzienniki) zaznacz jakiś alarm i kliknij **Go to recordings (Przejdź do nagrań)**, aby otworzyć kartę Recording alerts (Powiadomienia dotyczące nagrań). Patrz *Alarmy* i *Dzienniki*. |

**Menu główne**

| | |
|---|---|
| ☰ | Otwórz menu główne. |
| **Serwery** | Ustanów połączenie z nowym serwerem AXIS Camera Station 5 i wyświetl listy serwerów oraz stan połączenia dla każdego z tych serwerów. Patrz *Konfigurowanie serwera*. |
| **Działania** | Ręczne uruchomienie lub zatrzymanie nagrywania oraz zmiana statusu portów we/wy. Patrz *Ręczne nagrywanie* i *Monitorowanie portów we/wy*. |
| **Pomoc** | Otwarcie opcji pomocy. Kliknij kolejno **Help (Pomoc)** > **About (Informacje)**, aby sprawdzić używaną wersję klienta AXIS Camera Station 5. |
| **Wyloguj się** | Rozłączenie się z serwerem i wylogowanie z klienta AXIS Camera Station 5. |
| **Wyjdź** | Wyjście i zamknięcie klienta AXIS Camera Station 5. |

**Pasek tytułu**

| | |
|---|---|
| ? lub F1 | Otwórz pomoc. |
| ⛶ | Przejdź do trybu pełnoekranowego. |
| ⛶ lub ESC | Zamknij tryb pełnoekranowy. |

**Pasek stanu**

Pasek stanu może zawierać poniższe informacje:

- Niezgodności czasu między klientem i serwerem powoduje wyświetlenie ikony ostrzeżenia. Aby uniknąć problemów z osią czasu, zawsze upewnij się, że czas na kliencie jest zsynchronizowany z czasem na serwerze.
- W sekcji stanu połączenia serwera widać liczbę podłączonych serwerów. Patrz *Status połączenia*.
- W sekcji Status licencji widać liczbę urządzeń bez licencji. Patrz .
- W sekcji Użycie bezpiecznego zdalnego dostępu widać ilość pozostałych danych lub wykorzystanie nadwyżki w obecnym miesiącu z puli dostępnej na danym poziomie usługi. Patrz *Axis Secure Remote Access*.
- **AXIS Camera Station 5 update available (Jest dostępna aktualizacja)** — pojawia się, gdy jest dostępna nowa wersja do pobrania, jeśli zalogowano się jako administrator. Patrz *Aktualizuj AXIS Camera Station 5, on page 119*.

**Alarms and Tasks (Alarmy i zadania)**

Na kartach Alarmy i zadania widoczne są wyzwolone zdarzenia oraz alarmy systemowe. Patrz *Alarmy* i *Zadania*.

# Podgląd na żywo

Podgląd na żywo obejmuje obszary obserwacji, kamery oraz bieżący obraz z połączonych kamer. Widoczne są również wszystkie obszary obserwacji i kamery połączonych serwerów pogrupowane według nazw serwerów, jeśli jest połączonych wiele serwerów AXIS Camera Station 5.

Widoki umożliwiają dostęp do wszystkich kamer i urządzeń dodanych do AXIS Camera Station 5. Widok może zawierać obraz z jednej lub wielu kamer, sekwencję elementów, mapę lub stronę internetową. Podgląd na żywo automatycznie aktualizuje widoki podczas dodawania lub usuwania urządzeń z systemu.

Dostęp do widoków mają wszyscy użytkownicy. Więcej o prawach dostępu użytkowników: *Uprawnienia użytkownika, on page 127*.

Pomoc dotycząca konfigurowania podglądu na żywo: *Ustawienia klienta*.

## Wiele monitorów

Aby otworzyć widok na innym ekranie:

1. Otwórz kartę Live view (Podgląd na żywo).
2. Wybierz jedną lub więcej kamer, widoków lub sekwencji.
3. Przeciągnij je i upuść na drugi ekran.

Aby otworzyć widok na monitorze podłączonym do dekodera wideo Axis:

1. Otwórz kartę Live view (Podgląd na żywo).
2. Wybierz jedną lub więcej kamer, widoków lub sekwencji.
3. Kliknij prawym przyciskiem myszy kamery, widoki lub sekwencje, a następnie wybierz **Show on AXIS T8705 (Pokaż na AXIS T8705)** lub **Show on AXIS D1110 (Pokaż na AXIS D1110)**, w zależności od tego, jaki dekoder wideo jest używany.

Uwaga

- AXIS T8705 obsługuje tylko kamery Axis.
- AXIS D1110 obsługuje do 9 strumieni w jednym podzielonym widoku.

## Zarządzanie widokami w podglądzie na żywo

| | |
|---|---|
| + | Dodaj nowy widok podzielony, sekwencję, widok z kamery, mapę, stronę internetową lub folder. |
| ✎ | Edytuj widok lub nazwę kamery. Aby uzyskać informacje na temat edytowania ustawień kamery, patrz *Edycja ustawień kamery* |
| 🗑 | Usuń widok. Chcąc usunąć widok, trzeba mieć uprawnienia do modyfikowania widoku oraz jego wszystkich widoków podrzędnych. Aby uzyskać informacje na temat usuwania kamer z AXIS Camera Station 5, zob. *Kamery, on page 46*. |
| 🔒 | Administrator może zablokować widok i uniemożliwić operatorom lub widokom przenoszenie i edytowanie widoku. |

## Zarządzanie obrazami w podglądzie na żywo

| | |
|---|---|
| **Navigate (Nawigacja)** | Aby przejść do widoku kamery, kliknij prawym przyciskiem myszy obraz w widoku podzielonym i kliknij przycisk **Navigate (Nawigacja)** |
| **Take snapshot (Wykonaj ujęcie)** | Kliknij obraz prawym przyciskiem myszy i wybierz **Take snapshot (Wykonaj ujęcie)**, aby zarejestrować ujęcie. System zapisze ujęcie w folderze ujęć określonym w obszarze **Configuration > Client > Settings** (Konfiguracja > Klient > Ustawienia). |
| **Dodawanie ujęcia do eksportu** | Aby dodać ujęcie do listy eksportu na karcie Export (Eksport), kliknij obraz prawym przyciskiem myszy i wybierz **Add snapshot to Export** (Dodaj ujęcie do eksportu). |
| **Pokaż na** | Aby otworzyć widok na innym ekranie, kliknij obraz prawym przyciskiem myszy i wybierz polecenie **Show on (Pokaż na)**. |
| **Use Mechanical PTZ (Korzystaj z mechanicznej funkcji PTZ)** | Dostępny w kamerach PTZ oraz kamerach, dla których w interfejsie internetowym włączono cyfrową funkcję PTZ. Aby używać fizycznego mechanizmu PTZ, kliknij obraz prawym przyciskiem myszy i wybierz polecenie **Use Mechanical PTZ (Korzystaj z mechanicznej funkcji PTZ)**. Za pomocą myszy możesz przybliżać/oddalać, pochylać i obracać kamerę. |
| **Zoom** | Za pomocą kółka myszy można przybliżać i oddalać widok. Ewentualnie naciśnij klawisze CTRL + (+), aby zbliżyć obraz, lub klawisze CTRL + (-), aby go oddalić. |
| **Przybliżanie widoku obszaru** | Aby powiększyć obszar na obrazie, narysuj prostokąt wewnątrz obszaru, który chcesz powiększyć. Aby oddalić widok, użyj kółka myszy. Aby przybliżyć obszar w pobliżu środka obrazu, za pomocą prawego przycisku myszy narysuj prostokąt wyznaczający ten obszar. |
| **Obracanie i pochylanie** | Kliknij obraz, w którym chcesz skierować kamerę. Aby obracanie i pochylanie działało ustawicznie dla obrazu w podglądzie na żywo, przesuń kursor do środka obrazu, tak aby pojawiła się strzałka nawigacyjna. Następnie kliknij i przytrzymaj przycisk, a widok zostanie obrócony w kierunku strzałki nawigacyjnej. Aby obracać i pochylać obraz go w szybszym tempie, kliknij i przytrzymaj przycisk myszy, tak aby strzałka nawigacyjna się wydłużyła. |
| **Ustaw ostrość** | Kliknij obraz prawym przyciskiem myszy i wybierz polecenie **Set focus (Ustaw ostrość)**, aby wyregulować ostrość kamery. Kliknij opcję **AF**, aby kamera ustawiała ostrość automatycznie. Aby wyregulować ostrość ręcznie, zaznacz odpowiednie miejsce na słupkach **Near (Blisko)** i **Far (Daleko)**. Słupek **Near (Blisko)** służy do ustawiania ostrości na obiektach znajdujących się blisko kamery. Słupek **Far (Daleko)** służy do ogniskowania na obiekty znajdujące się daleko. |

| | |
|---|---|
| **Focus recall zone (Strefa przywracania ostrości)** | Kliknij obraz prawym przyciskiem myszy, wybierz polecenie **Focus recall zone (Strefa przywracania ostrości)**, a następnie wybierz opcję dodania lub usunięcia strefy przywracania ostrości. |
| **Automatyczne śledzenie wł./wył.** | Kliknij obraz prawym przyciskiem myszy, wybierz opcję **Autotracking on/off (Automatyczne śledzenie wł./wył.)**, a następnie wybierz opcję włączenia lub wyłączenia automatycznego śledzenia dla kamery PTZ Axis ze skonfigurowaną funkcją automatycznego śledzenia ruchu AXIS PTZ Autotracking. |
| **Presety** | Aby przejść do prepozycji, kliknij obraz prawym przyciskiem myszy, wybierz polecenie **Presets (Prepozycje)**, i wybierz prepozycje. Aby utworzyć predefiniowane ustawienie, patrz *Prepozycje PTZ*. |
| **Dodaj prepozycję** | Aby dodać prepozycję, przeciągnij widok obrazu w żądane miejsce, kliknij prawym przyciskiem myszy i wybierz kolejno polecenia **Presets > Add preset (Prepozycje > Dodaj prepozycję)**. |
| **Bezwzględny ruch PTZ** | Dostępny dla urządzeń zgodnych ze standardem ONVIF obsługujących bezwzględne pozycjonowanie PTZ. Użyj tej funkcji, aby przesunąć kamerę do precyzyjnych współrzędnych celem uzyskania powtarzalnego pozycjonowania.<br>Aby użyć funkcji bezwzględnego pozycjonowania PTZ, kliknij prawym przyciskiem myszy kamerę w podglądzie na żywo i wybierz **Absolute PTZ Move** (Bezwzględny ruch PTZ). Wybierz układ współrzędnych: **Generic** (Ogólny) przy współrzędnych standardowych lub **Spherical** (Sferyczny) przy współrzędnych opartych na stopniach kąta. Wpisz wartości pozycji obrotu, pochylenia i zoomu, ustaw szybkość ruchu i kliknij **OK** lub **Send** (Wyślij). |
| **Profil strumienia** | Kliknij obraz prawym przyciskiem myszy i wybierz polecenie **Stream profile (Profil strumienia)**, aby ustawić profil strumieniowania. Patrz *Profile strumienia*. |

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

*Dodawanie cyfrowych ustawień predefiniowanych*

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

*Sterowanie PTZ*

Uwaga

Jako administrator możesz wyłączyć mechaniczny PTZ dla użytkowników. Patrz *Uprawnienia użytkownika*.

## Nagrywanie i natychmiastowe odtwarzanie w podglądzie na żywo

| | |
|---|---|
|  | Zaznacz kamerę lub widok dzielony, a następnie kliknij  , aby przejść do karty Recordings (Nagrania). |
|  | Wskazuje trwające nagranie w podglądzie na żywo. |
|  | Wskazuje, że wykryto ruch. |
|  | Aby odtworzyć bieżące nagranie, zatrzymaj kursor na obrazie i kliknij  **Instant replay (Natychmiastowe odtwarzanie)**. Zostanie otwarta karta Zapisy, na której obejrzysz ostatnie 5 sekund nagrania. |
| **REC** | Aby nagrywać ręcznie z poziomu podglądu na żywo, umieść wskaźnik myszy na obrazie i kliknij przycisk **REC**. Przycisk zmieni się na żółty, wskazując, że nagrywanie jest w toku. Aby zatrzymać rejestrację, kliknij ponownie **REC**. |

Aby skonfigurować ustawienia ręcznego nagrywania takie jak rozdzielczość, kompresja i poklatkowość, patrz *Metoda nagrywania*. Więcej informacji o nagrywaniu i odtwarzaniu: *Odtwarzanie nagrań*.

Uwaga

Administratorzy mogą wyłączyć funkcję ręcznego nagrywania dla użytkowników. Patrz *Uprawnienia użytkownika*.

## Audio w podglądzie na żywo

Dźwięk jest dostępny, jeśli kamera ma funkcje audio oraz włączono obsługę dźwięku w profilu używanym dla podglądu na żywo.

Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumienia)** i skonfiguruj obsługę dźwięku w kamerze. Patrz *Profile strumienia, on page 47*.

| | |
|---|---|
|  **Głośność** | Aby zmienić głośność w widoku, umieść wskaźnik myszy na obrazie, umieść wskaźnik myszy na przycisku głośnika, a następnie użyj suwaka, aby ustawić głośność. Aby wyciszyć dźwięk lub wyłączyć jego wyciszenie, kliknij  . |
|  **Słuchaj tylko tego widoku** | Kliknięcie przycisku  umożliwi wyciszenie pozostałych widoków i słuchanie dźwięku tylko z danego widoku. |

| | |
|---|---|
| **Mówienie przez głośnik** | Aby mówić przez skonfigurowany głośnik w trybie full-duplex, umieść wskaźnik myszy na obrazie i kliknij . |
| **Push-to-talk** | Aby mówić przez skonfigurowany głośnik w trybach simplex i half-duplex, umieść wskaźnik myszy na obrazie, a następnie kliknij i przytrzymaj . Aby wyświetlić przycisk **Push-to-talk** dla wszystkich trybów duplex, włącz **Use push-to-talk for all duplex modes (Użyj push-to-talk dla wszystkich trybów duplex)** w **Configuration > Client > Streaming > Audio (Konfiguracja > Klient > Strumieniowanie > Audio)**. Patrz *Przesyłanie strumieniowe, on page 111*. |

Uwaga

Jako administrator możesz wyłączyć obsługę dźwięku dla użytkowników. Patrz *Uprawnienia użytkownika*.

## Ekranowe elementy sterowania w podglądzie na żywo

Uwaga

Ekranowe elementy sterowania są dostępne w oprogramowaniu sprzętowym począwszy od wersji 7.40.

| | |
|---|---|
| | W podglądzie na żywo kliknij , aby przejść do dostępnych funkcji kamery. |

## Widok dzielony

W widoku dzielonym jedno okno pokazuje wiele widoków. Do widoku podzielonego można dodać widoki kamery, sekwencje, strony internetowe, mapy i inne widoki dzielone.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station 5, do widoku dzielonego można dodać dowolny widok, kamerę, urządzenie lub strefę nagłośnieniową z innych serwerów.

Aby dodać widok dzielony:

1. Na karcie Live view (Podgląd na żywo) kliknij .
2. Kliknij przycisk **New Split View (Nowy widok dzielony)**.
3. Wprowadź nazwę widoku dzielonego.
4. Z rozwijalnego menu **Template (Szablon)** wybierz szablon, którego chcesz używać.
5. Przeciągnij i upuść do siatki widoki, strefy nagłośnieniowe lub kamery (pojedyncze lub kilka).
6. Kliknij **Save view (Zapisz widok)**, aby zapisać widok dzielony na bieżącym serwerze.

| | |
|---|---|
| **Ustaw aktywny punkt** | Aby określić ramkę punktu aktywnego, kliknij prawym przyciskiem myszy i wybierz **Set hotspot (Ustaw punkt aktywny)**. Gdy klikniesz następną ramkę, zostanie ona otwarta w punkcie aktywnym. Punkty aktywne są przydatne w asymetrycznych widokach dzielonych z jedną dużą i kilkoma mniejszymi ramkami. Punktem aktywnym jest zwykle największa ramka. |
| **Profil strumienia** | Aby ustawić profil strumienia kamery, kliknij prawym przyciskiem myszy kamerę w widoku siatki, a następnie wybierz **Stream profile (Profil strumienia)**. Zob. *Profile strumienia*. |


*Dodawanie widoku dzielonego*

## Pulpit nawigacyjny drzwi w widoku podzielonym

Jeśli masz skonfigurowane drzwi, możesz pomagać posiadaczom kart i monitorować stan drzwi oraz ostatnie transakcje w widoku dzielonym.

1. Dodaj drzwi. Patrz *Dodawanie drzwi, on page 138*.
2. Dodaj pulpit nawigacyjny drzwi do widoku dzielonego, zobacz *Widok dzielony, on page 16*.

| | |
|---|---|
| **Pulpit nawigacyjny** | Aby wyświetlić szczegóły drzwi, stan drzwi i stan zamka, otwórz kartę **Dashboard (Pulpit nawigacyjny)**.<br><br>Na pulpicie nawigacyjnym są wyświetlane następujące informacje:<br>• Gdy posiadacz karty przeciągnie kartę w czytniku, zostaną wyświetlone zdarzenia kontroli dostępu z danymi posiadacza karty, w tym jego zdjęciem.<br>• Alarmy z informacjami o ich wyzwalaczach, na przykład zbyt długim otwarciu drzwi.<br>• Najnowsza transakcja. |
| | Aby dodać zdarzenie do zakładek i udostępnić je na karcie Transactions (Transakcje), kliknij . |
| **Wejdź na stronę** | Aby ręcznie udzielić dostępu, kliknij pozycję **Access (Dostęp)**. Spowoduje to odblokowanie drzwi w taki sam sposób, jak w przypadku, gdyby ktoś przedstawia poświadczenia, co zwykle oznacza automatyczne blokowanie po określonym czasie. |
| **Blokada** | Aby ręcznie zablokować drzwi, kliknij pozycję **Lock (Zablokuj)**. |

| | |
|---|---|
| **Odblokuj** | Aby ręcznie odblokować drzwi, kliknij pozycję **Unlock (Odblokuj)**. Drzwi są odblokowane, dopóki nie zostaną ponownie zablokowane ręcznie. |
| **Odcinanie obszaru** | Aby uniemożliwić dostęp do drzwi, kliknij pozycję **Lockdown (Blokada)**. |
| **Transakcje** | Aby wyświetlić ostatnie transakcje i zapisane transakcje, otwórz kartę **Transactions (Transakcje)**. |


*Monitorowanie i wspieranie za pomocą pulpitu nawigacyjnego drzwi*

## Sekwencja

Sekwencja służy do przełączania między widokami.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station 5, do sekwencji można dodać dowolny widok, kamerę lub urządzenie z dowolnego serwera.

Aby utworzyć sekwencję:

1. Na karcie Live view (Podgląd na żywo) kliknij +.
2. Zaznacz opcję **New sequence (Nowa sekwencja)**.
3. Wprowadź nazwę sekwencji.
4. Przeciągnij i upuść do widoku sekwencji widoki lub kamery (pojedyncze lub wiele).
5. Rozmieść widoki w żądanej sekwencji.
6. W każdym widoku można również opcjonalnie ustawić indywidualne czasy wyświetlania.
7. W przypadku kamer z funkcjami PTZ wybierz prepozycję PTZ z listy rozwijanej **PTZ preset (Prepozycja PTZ)**. Patrz *Prepozycje PTZ*.
8. Kliknij przycisk **Save view (Zapisz widok)** , aby zapisać sekwencję na bieżącym serwerze.

| | |
|---|---|
| **Czas wyświetlania** | Czas wyświetlania to liczba sekund wyświetlenia widoku, zanim nastąpi przełączenie na widok następny. Dla każdego widoku można to ustawić indywidualnie. |


*Dodawanie sekwencji*

## Widok kamery

Widok kamery pokazuje obraz na żywo z jednej kamery. Widoki kamery mogą być używane w widokach podzielonych, sekwencjach i mapach.

Uwaga

W przypadku połączenia z wieloma serwerami AXIS Camera Station 5 na liście wyświetlane są wszystkie kamery ze wszystkich połączonych serwerów.

Aby dodać widok kamery:

1. W podglądzie na żywo lub na karcie Recordings (Nagrania) kliknij +.
2. Wybierz opcję **New Camera View (Nowy obraz z kamery_)**.
3. Wybierz kamerę z menu rozwijanego i kliknij przycisk **OK**.

## Mapa

Mapa to importowany obraz, na którym można umieścić widoki kamery, widoki podzielone, sekwencje, strony internetowe, inne mapy i drzwi. Mapa prezentuje całościowy obraz oraz pozwala odszukać poszczególne urządzenia i do nich przejść. W przypadku dużych instalacji można utworzyć kilka map i umieścić je na mapie ogólnej.

Wszystkie przyciski akcji są również dostępne w widoku mapy. Patrz *Tworzenie wyzwalaczy opartych na przyciskach akcji*.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station 5, do widoku mapy można dodać dowolny widok, kamerę lub urządzenie z dowolnego serwera.

Aby dodać mapę:

1. Na karcie Live view (Podgląd na żywo) kliknij +.
2. Kliknij opcję **New map (Nowa mapa)**.
3. Nadaj mapie nazwę.
4. Kliknij przycisk **Choose image (Wybierz obraz)** i znajdź plik mapy. Maksymalny rozmiar pliku to 20 MB. Obsługiwane są formaty BMP, JPG, PNG i GIF.
5. Przeciągnij na mapę widoki, kamery, inne urządzenia oraz drzwi.
6. Kliknij ikonę na mapie, aby zmienić ustawienia.
7. Kliknij przycisk **Add label (Dodaj etykietę)**, nadaj etykiecie nazwę oraz ustaw rozmiar, kąt obrotu, styl i kolor etykiety.

Uwaga

Niektóre ustawienia można edytować dla wielu ikon i etykiet równocześnie.

8. Kliknij przycisk **Save view (Zapisz widok)** , aby zapisać mapę na bieżącym serwerze.

| | |
|---|---|
| | Fizyczny status drzwi, gdy drzwi skonfigurowano z monitorem drzwi. |
| | Fizyczny status drzwi, gdy drzwi skonfigurowano bez monitora drzwi. |
| **Ikona** | Zaznacz ikonę, której chcesz używać. Ta opcja jest dostępna tylko dla kamer i innych urządzeń. |
| **Rozmiar** | Za pomocą suwaka można wyregulować wielkość ikony. |

| | |
|---|---|
| **Kolor** | Kliknij i zmień kolor ikony. |
| **Nazwa** | Włącz tę opcję, aby wyświetlić nazwę ikony. Wybierz **Bottom (U dołu)** lub **Top (U góry)**, aby zmienić położenie nazwy ikony. |
| **Strzałka kierunkowa** | Wyświetla strzałki wskazujące kierunek pola widzenia każdej kamery. Można wyświetlać strzałki z obszarami pokrycia lub bez nich. |
| **Pokryty obszar** | Ta opcja jest dostępna tylko dla kamer i innych urządzeń. Włącz tę opcję, aby obszar objęty zasięgiem urządzenia był wyświetlany na mapie. Można edytować **Range (Zasięg)**, **Width (Szerokość)**, **Direction (Kierunek)** i kolor obszaru objętego zasięgiem. Włącz opcję **Flash (Miganie)**, jeśli obszar objęty zasięgiem ma migać, kiedy nagrywanie zostało wyzwolone detekcją ruchu lub innymi regułami akcji. Na stronie ustawień klienta można wyłączyć miganie obszaru objętego zasięgiem globalnie dla wszystkich urządzeń, patrz: *Ustawienia klienta, on page 108*. |
| **Usuń** | Kliknij , aby usunąć ikonę z mapy. |


*Dodawanie mapy*


*Wyzwalanie audio z poziomu mapy*

## Strona internetowa

Widok strony internetowej pokazuje stronę z Internetu. Stronę internetową można dodać na przykład do widoku podzielonego lub sekwencji.

Aby dodać stronę internetową:

1. Na karcie Live view (Podgląd na żywo) kliknij .
2. Wybierz opcję **New webpage (Nowa strona internetowa)**.
3. Wprowadź nazwę strony internetowej.
4. Wprowadź pełny adres URL strony internetowej.
5. Kliknij **OK**.


## Foldery

Foldery służą do grupowania elementów w kategorie w widoku drzewa. Foldery mogą zawierać widoki podzielone, sekwencje, widoki kamer, mapy, strony internetowe i inne foldery.

Aby dodać folder:

1. W podglądzie na żywo lub na karcie Recordings (Nagrania) kliknij +.
2. Kliknij przycisk **New Folder (Nowy folder)**.
3. Nadaj folderowi nazwę i kliknij przycisk **OK**.

# Nagrania

Na karcie Recordings (Nagrania) znajdują się funkcje wyszukiwania, odtwarzania i eksportowania nagrań. Na karcie znajduje się widok nagrania i dwa panele, w których można znaleźć widoki, obrazy, narzędzia do odtwarzania i kamery podłączonych serwerów pogrupowane według nazwy serwera, zobacz *Podgląd na żywo*.

W widoku głównym nagrania można zarządzać obrazem w taki sam sposób, jak w podglądzie na żywo. Więcej informacji można znaleźć na stronie *Zarządzanie obrazami w podglądzie na żywo, on page 13*.

Aby zmienić metodę nagrywania i ustawienia nagrywania, takie jak rozdzielczość, kompresja i poklatkowość, zob. *Metoda nagrywania*.

Uwaga

Nie można manualnie usunąć nagrań z AXIS Camera Station 5. Trzeba zmienić czas przechowywania w oknie **Configuration (Konfiguracja) > Storage (Pamięć masowa) > Selection (Wybór)**, tak aby były usuwane stare nagrania.

## Odtwarzanie nagrań

Nagrania z wielu kamer mogą być odtwarzane jednocześnie po umieszczeniu znacznika odtwarzania nad wieloma nagraniami na osi czasu.

W przypadku korzystania z wielu monitorów można jednocześnie wyświetlać obraz na żywo i nagrany obraz wideo.

**Oś czasu odtwarzania**

Za pomocą osi czasu można poruszać się po funkcji odtwarzania i sprawdzać, kiedy nastąpiło nagranie. Czerwona linia na osi czasu oznacza nagranie w związku z detekcją ruchu. Niebieska linia na osi czasu oznacza nagranie wywołane przez regułę akcji. Najedź wskaźnikiem myszy na nagranie na osi czasu, aby wyświetlić jego typ i czas. Aby uzyskać lepszy widok i znaleźć nagrania, można przybliżać, oddalać i przeciągać oś czasu. Gdy przeciągasz oś czasu, odtwarzanie jest chwilowo wstrzymywane, a po jej zwolnieniu jest wznawiane. W nagraniu można przesuwać oś czasu (szybki podgląd), aby uzyskać przegląd zawartości i znaleźć określone wystąpienia.

**Find recordings (Znajdowanie nagrań)**

| | |
|---|---|
| | Kliknij, aby wybrać datę i godzinę na osi czasu. |
| | Użyj filtru, aby skonfigurować typ nagrań, które mają być wyświetlane na osi czasu. |
| | Służy do znajdowania zapisanych zakładek, zobacz *Zakładki*. |
| **Inteligentne wyszukiwanie 1** | Inteligentne wyszukiwanie pozwala znajdować nagrania, zob. *Inteligentne wyszukiwanie 1*. |

**Odtwarzanie nagrań**

| | |
|---|---|
| | Odtwórz nagranie. |
| | Wstrzymaj nagranie. |
| | Pozwala przejść do początku trwającego lub poprzedniego nagrania/zdarzenia. Kliknij prawym przyciskiem myszy, aby przejść do nagrań, zdarzeń lub obu kategorii elementów. |

| | |
|---|---|
|  | Pozwala przejść do początku następnego nagrania lub zdarzenia. Kliknij prawym przyciskiem myszy, aby przejść do nagrań, zdarzeń lub obu kategorii elementów. |
|  | Przechodzenie do poprzedniej ramki w nagraniu. Wstrzymaj nagranie, aby użyć tej funkcji. Kliknij prawym przyciskiem myszy, aby ustawić liczbę ramek do pominięcia (do 20 ramek). |
|  | Przechodzenie do następnej ramki w nagraniu. Wstrzymaj nagranie, aby użyć tej funkcji. Kliknij prawym przyciskiem myszy, aby ustawić liczbę ramek do pominięcia (do 20 ramek). |
|  | Zmień prędkość odtwarzania za pomocą mnożników w rozwijalnym menu. |
|  | Wycisz dźwięk. Ta funkcja jest dostępna tylko w przypadku nagrań z dźwiękiem. |
| **Suwak audio** | Za pomocą przesuwania można zmieniać głośność dźwięku. Ta funkcja jest dostępna tylko w przypadku nagrań z dźwiękiem. |
| **Pokaż wszystkie metadane z kamer nasobnych** | Wyświetlanie metadanych systemu nasobnego oraz wyświetlanie notatek i kategorii z aplikacji AXIS Body Worn Assistant. |
| **Obrót, pochylenie i zbliżenie** | Kliknij obraz i przewiń w górę lub w dół, aby powiększyć lub pomniejszyć obraz i przesunąć widok, aby zobaczyć inne części obrazu. Aby powiększyć obszar, umieść w nim kursor myszy i przewijaj. |

## Zakładki

Uwaga

- Nie można usunąć zablokowanego nagrania, chyba że zostanie ręcznie odblokowane.
- System usuwa zablokowane nagrania po usunięciu kamery z aplikacji AXIS Camera Station 5.

| | |
|---|---|
|  | Kliknij, aby wyświetlić wszystkie zakładki. Aby filtrować zakładki, kliknij ikonę. |
|  | Służy do dodawania nowej zakładki. |
|  | Oznacza, że nagranie jest zablokowane. Nagranie zawiera co najmniej 2,5 minuty materiału wideo przed zakładką i po niej. |
|  | Służy do edytowania nazwy i opisu zakładki oraz blokowania lub odblokowania nagrania. |
|  | Usuń zakładkę. Aby usunąć wiele zakładek, zaznacz wiele zakładek i przytrzymaj naciśnięty klawisz CTRL lub SHIFT. |
| **Prevent recording deletion (Chroń zapis przed usunięciem)** | Zaznacz lub odznacz to pole, aby zablokować lub odblokować nagranie. |

### Dodawanie zakładki

1. Przejdź do nagrania.
2. Ustaw znacznik w odpowiednim położeniu poprzez przybliżanie, pomniejszanie i przesuwanie na osi czasu.
3. Kliknij .
4. Wprowadź nazwę i opis zakładki. Użyj słów kluczowych w opisie, aby ułatwić znajdowanie i rozpoznawanie zawartości zakładki.
5. Wybierz **Prevent recording deletion (Chroń zapis przed usunięciem)**, aby zablokować zapis.

Uwaga

Zablokowanego nagrania nie można usunąć. Aby odblokować nagranie, wyczyść opcję lub usuń zakładkę.

6. Kliknij przycisk **OK**, aby zapisać zakładkę.

## Eksportuj nagrania

Na karcie **Export (Eksportu)** można eksportować nagrania do lokalnej pamięci masowej lub lokalizacji w sieci. Tutaj dostępne będą również informacje oraz podgląd nagrania. Można wyeksportować wiele plików jednocześnie i do różnych formatów: .asf, .mp4 i .mkv. Do odtwarzania nagrań najlepiej jest używać programu Windows Media Player (.asf) lub AXIS File Player (.asf, .mp4, .mkv). AXIS File Player to bezpłatne oprogramowanie do odtwarzania wideo i dźwięku, które nie wymaga instalacji.

Uwaga

W aplikacji AXIS File Player można zmieniać szybkość odtwarzania nagrań w formatach .mp4 i .mkv, ale nie w formacie .asf.

Przed rozpoczęciem upewnij się, że masz uprawnienia do eksportowania. Patrz *Uprawnienie użytkownika do eksportowania, on page 27*.

### Eksportuj nagrania

1. Na karcie **Recordings (Zapisy)** wybierz kamerę lub widok.
2. Dodaj nagrania do listy eksportu. Nagrania na osi czasu, które nie zostały objęte eksportem, mają kolor w paski.
   2.1. Kliknij , aby wyświetlić znaczniki wyboru.
   2.2. Przenieś odpowiednie znaczniki, aby uwzględnić zapis, który chcesz wyeksportować.
   2.3. Kliknij , aby otworzyć kartę **Export (Eksportuj)**.
3. Kliknij przycisk **Export (Eksportuj)**.
4. Wybierz folder, do którego chcesz wyeksportować nagrania.
5. Kliknij **OK**. Zadanie eksportu nagrań pojawi się na karcie **Tasks (Zadania)**.

Folder eksportu zawiera następujące elementy:

- Nagrania w wybranym formacie.
- Plik .txt z notatkami, jeśli wybrano opcję **Include notes (Uwzględnij notatki)**.
- Aplikację AXIS File Player, jeśli wybrano opcję **Include AXIS File Player (Dołącz AXIS File Player)**.
- Plik .asx z listą odtwarzania, jeśli wybrano opcję **Create playlist (.asx) (Utwórz listę odtwarzania (.asx))**.


*Eksportuj nagrania*

| Karta **Recordings (Nagrania)** | |
|---|---|
| | Aby zaznaczyć wiele nagrań, kliknij i przesuń znaczniki wyboru do pożądanego początku i końca. |
| | Aby wyeksportować nagrania w obrębie znaczników wyboru, kliknij . |
| **Dodaj zapisy** | Aby wyeksportować pojedyncze nagranie, kliknij je prawym przyciskiem myszy i wybierz polecenie **Export > Add recordings (Eksportuj > Dodaj nagrania)**. |
| **Dodaj zapisy zdarzeń** | Aby dodać wszystkie nagrania, które wystąpiły w czasie zdarzenia, kliknij nagranie prawym przyciskiem myszy i wybierz polecenie **Export > Add event recordings (Eksportuj > Dodaj nagrania zdarzeń)**. |
| **Usuń nagrania** | Aby usunąć nagranie z listy eksportu, kliknij je prawym przyciskiem myszy i wybierz polecenie **Export > Remove recordings (Eksportuj > Usuń nagrania)**. |
| **Usuń nagrania** | Aby usunąć z listy eksportu wiele nagrań w obrębie znaczników wyboru, kliknij prawym przyciskiem myszy poza nagraniem i wybierz polecenie **Export > Remove recordings (Eksportuj > Usuń nagrania)**. |

| Karta **Export (Eksport)** | |
|---|---|
| **Dźwięk** | Aby usunąć dźwięk z eksportu nagrania, odznacz pole wyboru w kolumnie **Audio (Dźwięk)**. Aby zawsze dołączać dźwięk do eksportowanych nagrań, wybierz kolejno opcje **Configuration (Konfiguracja)** > **Server (Serwer)** > **Settings (Ustawienia)** > **Export (Eksport)**, a następnie wybierz **Include audio when adding recordings to export (Uwzględniaj dźwięk podczas dodawania nagrań do eksportu)**. |
| | Aby edytować nagranie, zaznacz je i kliknij . Patrz *Edytowanie nagrania (redagowanie) przed wyeksportowaniem, on page 27*. |
| | Aby edytować notatki do nagrania, zaznacz nagranie i kliknij . |

| Karta **Export (Eksport)** | |
|---|---|
| | Aby usunąć nagranie z listy eksportu, zaznacz je i kliknij . |
| **Przełącz na eksport** | Aby przełączyć na kartę **Export (Eksport)**, jeśli karta **Incident report (Raport zdarzenia)** jest otwarta, kliknij polecenie **Switch to export (Przełącz na eksport)**. |
| **Preferowany profil strumienia** | Wybierz profil strumienia w polu **Preferred stream profile (Preferowany profil strumienia)**. |
| **Podgląd** | Kliknięcie nagrania na liście eksportu spowoduje wyświetlenie jego podglądu. Podgląd może objąć wiele nagrań tylko wtedy, gdy wszystkie pochodzą z jednej kamery. |
| **Zapisz** | Jeżeli chcesz zapisać listę eksportu do pliku, kliknij przycisk **Save (Zapisz)**. |
| **Wczytaj** | Jeżeli chcesz uwzględnić zapisaną wcześniej listę eksportu, kliknij przycisk **Load (Wczytaj)**. |
| **Dołącz uwagi** | Aby dołączyć notatki do nagrań, wybierz opcję **Include notes (Dołącz uwagi)**. Notatki są dostępne zarówno w postaci pliku .txt w wyeksportowanym folderze, jak i w formie zakładki do nagrania w aplikacji AXIS File Player. |
| | |
| | |
| **Ustawienie czasu rozpoczęcia i zakończenia** | Aby ustawić czas rozpoczęcia i zakończenia nagrania, przejdź do osi czasu w podglądzie i ustaw czas rozpoczęcia i zakończenia. Oś czasu pokazuje nagrania w zakresie 30 minut przed wybranym nagraniem i po nim. |
| **Dodaj ujęcie** | Aby dodać ujęcia, przeciągnij oś czasu z podglądu w określone miejsce. Kliknij podgląd prawym przyciskiem myszy i wybierz polecenie **Add snapshot (Dodaj ujęcie)**. |

| **Ustawienia zaawansowane** | |
|---|---|
| | |
| **Include AXIS File Player (Dołącz AXIS File Player)** | Aby do eksportowanych nagrań dołączać aplikację AXIS File Player, zaznacz opcję **Include AXIS File Player (Dołącz AXIS File Player)**. |
| **Create playlist(.asx) (Utwórz listę odtwarzania)** | Aby utworzyć listę odtwarzania w formacie .asx używanym przez program Windows Media Player, zaznacz opcję **Create playlist(.asx) (Utwórz listę odtwarzania)**. Nagrania będą odtwarzane w kolejności, w jakiej dostały dokonane. |
| **Add digital signature (Dodaj podpis cyfrowy)** | Aby zapobiec manipulowaniu obrazem, wybierz opcję **Add digital signature (Dodaj podpis cyfrowy)**. Ta opcja jest dostępna tylko dla nagrań w formacie . |

| Ustawienia zaawansowane | |
|---|---|
| | asf. Patrz *Odtwarzanie i weryfikowanie wyeksportowanych nagrań, on page 29*. |
| **Eksportuj do pliku zip** | Aby wyeksportować listę odtwarzania do pliku zip, zaznacz opcję **Export to Zip file (Eksportuj do pliku zip)** i zaznacz, aby ustawić hasło dostępu do tego pliku. |
| **Export format (Format eksportu)** | Z menu rozwijanego **Export format (Format eksportu)** wybierz format do, którego chcesz wyeksportować nagrania. Jeśli wybrano MP4, eksportowane nagrania nie zawierają dźwięku w formacie G.711 ani G.726. |
| **Edited video encoding (Kodowanie edytowanego obrazu wideo)** | Jeżeli którykolwiek obraz został zmodyfikowany, w sekcji **Edited video encoding** (Kodowanie edytowanego obrazu) ustaw format kodowania obrazu `Automatic` (Automatycznie), `H.264` lub `M-JPEG`. Wybierz ustawienie `Automatic` (Automatycznie), aby stosować kodowanie M-JPEG dla standardu M-JPEG oraz kodowanie H.264 dla pozostałych standardów. |

### Uprawnienie użytkownika do eksportowania

Aby eksportować nagrania lub generować raporty o zdarzeniach, musisz mieć uprawnienia. Możesz mieć uprawnienia do jednej z tych czynności lub obu. Po kliknięciu na karcie **Recordings (Nagrania)** zostanie otwarta połączona z nimi karta eksportu.

Aby skonfigurować uprawnienia, przejdź do *Uprawnienia użytkownika, on page 127*.

### Edytowanie nagrania (redagowanie) przed wyeksportowaniem

#### Rozmywanie ruchomego obiektu

1. Na karcie **Export (Eksportuj)** lub **Incident report (Raport o zdarzeniu)** zaznacz nagranie i kliknij .
2. Przesuń oś czasu do pierwszego wystąpienia ruchomego obiektu, który chcesz zakryć.
3. Kliknij **Bounding boxes > Add (Obwódki > Dodaj)**, aby dodać nową obwódkę.
4. Wybierz kolejno opcje **Bounding box options > Size (Opcje obwódki > Rozmiar)** i wyreguluj rozmiar obwódki.
5. Przesuń obwódkę i umieść ją nad obiektem.
6. Wybierz kolejno opcje **Bounding box options > Fill (Opcje obwódki > Wypełnienie)** i zaznacz wartość **Pixelated (Pikselacja)** lub **Black (Czarny)**.
7. Podczas odtwarzania nagrania kliknij obiekt prawym przyciskiem myszy i wybierz polecenie **Add key frame (Dodaj kluczową klatkę)**.
8. Aby dodać serię kluczowych klatek, podczas odtwarzania nagrania przesuwaj obwódkę nad obiektem.
9. Przesuń oś czasu i upewnij się, że obwódka obejmuje obiekt podczas całego nagrania.
10. Aby ustawić koniec, kliknij prawym przyciskiem myszy kształt rombu w ostatniej kluczowej klatce i wybierz opcję **Set end (Ustaw koniec)**. Spowoduje to usunięcie kluczowych klatek za punktem końcowym.

Uwaga

W nagraniu wideo można dodać wiele obwódek. Jeżeli ramki ograniczające się nakładają, wspólna część będzie wypełniana kolorami w kolejności Czarny, Pikselacja i Przezroczysty.

| | |
|---|---|
| **Usuń wszystko** | Aby usunąć wszystkie obwódki, kliknij przycisk **Bounding boxes > Remove all (Obwódki > Usuń wszystkie)**. |
| **Usuń kluczową klatkę** | Aby usunąć kluczową klatkę, kliknij ją prawym przyciskiem i wybierz polecenie **Remove key frame (Usuń kluczową klatkę)**. |

**Wyświetlanie poruszającego się obiektu z rozmytym tłem**

1. Tworzenie obwódki, zobacz *Rozmywanie ruchomego obiektu, on page 27*.
2. Wybierz kolejno opcje **Bounding box options > Fill (Opcje obwódki > Wypełnienie)** i ustaw wartość **Clear (Przezroczysty)**.
3. Wybierz kolejno opcje **Video background (Tło obrazu wideo)** i ustaw wartość **Pixelated (Pikselacja)** lub **Black (Czarny)**.

| | |
|---|---|
| **Pikselizacja wszystkiego poza zaznaczonym** | Zaznacz wiele obwódek na liście, a następnie kliknij prawym przyciskiem myszy i wybierz polecenie **Pixelate all but this (Pikselizacja wszystkiego poza zaznaczonym)**. Zaznaczone obwódki zmieniają kolor na **Clear (Przezroczyste)** a niezaznaczone są oznaczone jako **Pixelated (Pikselacja)**. |

**Generuj obwódki**

Aby wygenerować obwódki na podstawie danych analitycznych, włącz dane analityczne kamery. Patrz *Profile strumienia, on page 47*.

1. Na karcie **Export (Eksportuj)** lub **Incident report (Raport o zdarzeniu)** kliknij .
2. Kliknij przycisk **Generate bounding boxes (Generuj obwódki)**.
3. Upewnij się, że obwódki obejmują poruszający się obiekt, a w razie potrzeby popraw.
4. Wybierz wypełnienie tła obwódek lub obrazu filmowego.

**Usprawnianie edycji wideo za pomocą aplikacji AXIS Video Content Stream**

Aby usprawnić edycję wideo, zainstaluj aplikację AXIS Video Content Stream 1.0 na kamerach z oprogramowaniem sprzętowym w wersji od 5.50 do 9.60. AXIS Camera Station 5 uruchamia instalację automatycznie po dodaniu kamery do systemu. Patrz *Instalowanie aplikacji do kamery*.


*Edytowanie nagrań przed wyeksportowaniem*

### Odtwarzanie i weryfikowanie wyeksportowanych nagrań

Aby zapobiec manipulowaniu obrazem, do eksportowanych nagrań można dodać podpis cyfrowy z hasłem lub bez. Do zweryfikowania podpisu cyfrowego i sprawdzenia, czy w nagraniu nie wprowadzono zmian użyj aplikacji AXIS File Player.

1. Przejdź do folderu z wyeksportowanymi nagraniami. Jeśli wyeksportowany plik Zip jest chroniony hasłem, wprowadź hasło, aby otworzyć folder.
2. Otwórz aplikację AXIS File Player, a wyeksportowane nagrania zostaną automatycznie odtworzone.
3. W aplikacji AXIS File Player kliknij , a zostaną wyświetlone notatki z nagrań.
4. Jeżeli zaznaczono opcję **Add digital signature (Dodaj podpis cyfrowy)**, w aplikacji AXIS File Player sprawdź podpis cyfrowy nagrań.
   4.1. Przejdź do menu **Tools > Verify digital signature (Narzędzia > Weryfikuj podpis cyfrowy)**.
   4.2. Jeśli ustawiono ochronę hasłem, kliknij opcję **Validate with password (Uwierzytelnij hasłem)** i wprowadź swoje hasło.
   4.3. Aby zobaczyć wyniki weryfikacji, kliknij **Verify (Zweryfikuj)**.

## Eksportowanie raportów o zdarzeniach

Na karcie Raport o zdarzeniu można eksportować raporty o zdarzeniach do lokalnego zasobu pamięci lub lokalizacji sieciowej. Można tu dołączać do raportów nagrania, ujęcia i notatki.

Przed rozpoczęciem upewnij się, że masz uprawnienia do eksportowania. Patrz *Uprawnienie użytkownika do eksportowania, on page 27*.


*Zgłaszanie incydentów*

#### Generowanie raportów o zdarzeniach

1. Na karcie **Recordings (Zapisy)** wybierz kamerę lub widok.
2. Dodaj nagrania do listy eksportu. Patrz *Eksportuj nagrania, on page 24*.
3. Kliknij polecenie **Switch to incident report (Przełącz na raport o zdarzeniu)**, aby przejść do karty z raportami o zdarzeniach.
4. Kliknij przycisk **Create report (Utwórz raport)**.
5. Wybierz folder, w którym chcesz zapisać raport o zdarzeniu.
6. Kliknij **OK**. Zadanie eksportowania raportu o zdarzeniu pojawi się na karcie **Tasks (Zadania)**.

Folder eksportu zawiera następujące elementy:

- AXIS File Player.
- Nagrania w wybranym formacie.
- Plik .txt po wybraniu opcji **Include notes (Dołącz notatki)**.
- Raport o zdarzeniu.
- Lista odtwarzania, jeżeli eksportujesz wiele nagrań.

| | |
|---|---|
| **Dźwięk** | Aby usunąć dźwięk z eksportu nagrania, odznacz pole wyboru w kolumnie **Audio (Dźwięk)**. Aby zawsze dołączać dźwięk do eksportowanych nagrań, wybierz kolejno opcje **Configuration (Konfiguracja)** > **Server (Serwer)** > **Settings (Ustawienia)** > **Export (Eksport)**, a następnie wybierz **Include audio when adding recordings to export (Uwzględniaj dźwięk podczas dodawania nagrań do eksportu)**. |
|  | Aby edytować nagranie, zaznacz je i kliknij  . Patrz *Edytowanie nagrania (redagowanie) przed wyeksportowaniem, on page 27*. |
|  | Aby edytować notatki do nagrania, zaznacz nagranie i kliknij  . |
|  | Aby usunąć nagranie z listy eksportu, zaznacz je i kliknij  . |
| **Przełącz na raport o zdarzeniu** | Aby przejść na kartę **Incident report (Raport o zdarzeniu)** z karty **Export (Eksport)**, kliknij polecenie **Switch to incident report (Przełącz na raport o zdarzeniu)**. |
| **Preferowany profil strumienia** | Z menu rozwijanego wybierz profil strumienia **Preferred stream profile (Preferowany profil strumienia)**. |
| **Podgląd** | Kliknięcie nagrania na liście eksportu spowoduje wyświetlenie jego podglądu i rozpoczęcie jego odtwarzania. Podgląd może objąć wiele nagrań tylko wtedy, gdy wszystkie pochodzą z jednej kamery. |
| **Zapisz** | Jeżeli chcesz zapisać raport o zdarzeniu do pliku, kliknij **Save (Zapisz)**. |
| **Wczytaj** | Jeśli chcesz dołączyć zapisany wcześniej raport o zdarzeniu, kliknij **Load (Wczytaj)**. |
| **Opis** | Pole **Description (Opis)** jest automatycznie wypełniane wstępnie zdefiniowanymi danymi z szablonu opisu. Można też dodać inne informacje, które powinny się znaleźć w raporcie o zdarzeniu. |
| **Kategoria** | Wybierz kategorię, do której należy raport. |
| **Reference ID (Identyfikator referencyjny)** | **Reference ID (Identyfikator referencyjny)** jest generowany automatycznie, w razie potrzeby można go zmienić ręcznie. Identyfikator referencyjny w sposób niepowtarzalny oznacza raport o zdarzeniu. |
| **Dołącz uwagi** | Aby dołączyć notatki do nagrań i ujęć, zaznacz opcję **Include notes (Dołącz notatki)**. Notatki są dostępne zarówno w postaci pliku .txt w wyeksportowanym folderze, jak i w formie zakładki do nagrania w aplikacji AXIS File Player. |
| **Edited video encoding (Kodowanie edytowanego obrazu wideo)** | Jeżeli którykolwiek obraz został zmodyfikowany, w sekcji **Edited video encoding** (Kodowanie edytowanego obrazu) ustaw format kodowania |

| | |
|---|---|
| | obrazu `Automatic` (Automatycznie), `H.264` lub `M-JPEG`. Wybierz ustawienie `Automatic` (Automatycznie), aby stosować kodowanie M-JPEG dla standardu M-JPEG oraz kodowanie H.264 dla pozostałych standardów. |
| **Ustawienie czasu rozpoczęcia i zakończenia** | Aby ustawić czas rozpoczęcia i zakończenia nagrania, przejdź do osi czasu w podglądzie i ustaw czas rozpoczęcia i zakończenia. Oś czasu pokazuje nagrania w zakresie 30 minut przed wybranym nagraniem i po nim. |
| **Dodaj ujęcie** | Aby dodać ujęcie, przejdź na osi czasu dostępnej na podglądzie w określone miejsce. Kliknij podgląd prawym przyciskiem myszy i wybierz polecenie **Add snapshot (Dodaj ujęcie)**. |

## Ręczne nagrywanie

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można manualnie rozpoczynać i kończyć nagrywanie na dowolnym połączonym serwerze. W tym celu wybierz serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.

Aby ręcznie uruchomić i zatrzymać nagrywanie z poziomu menu głównego:

1. Wybierz kolejno ☰ > **Actions (Akcje)** > **Record manually (Nagrywaj manualnie)**.
2. Wybierz jedną lub kilka kamer.
3. Kliknij przycisk **Start**, aby rozpocząć nagrywanie.
4. Kliknij przycisk **Stop**, aby zatrzymać nagrywanie.

Aby rozpocząć lub zatrzymać ręczne nagrywanie z poziomu karty **Live view (Podgląd na żywo)**:

1. Przejdź na kartę **Live view (Podgląd na żywo)**.
2. Przesuń wskaźnik myszy do ramki podglądu na żywo z kamery.
3. Kliknij przycisk **REC**, aby rozpocząć nagrywanie. Podczas nagrywania w ramce widoku będzie widoczny czerwony wskaźnik.
4. Kliknij przycisk **REC**, aby zatrzymać nagrywanie.

## Inteligentne wyszukiwanie 1

Inteligentne wyszukiwanie 1 umożliwia znajdowanie części nagrania, w których występuje ruch w zdefiniowanym obszarze obrazu.

Aby przyspieszyć wyszukiwanie, wybierz **Include analytics data (Uwzględnij dane analityczne)** w profilach strumienia. Patrz *Profile strumienia*.

Używanie funkcji Inteligentne wyszukiwanie 1:

1. Kliknij + i otwórz kartę **Smart search 1 (Inteligentne wyszukiwanie 1)**.
2. Wybierz kamerę, którą chcesz znaleźć.
3. Dostosuj obszar zainteresowania. Do kształtu można dodać maksymalnie 20 punktów. Aby usunąć punkt, kliknij go prawym przyciskiem myszy.
4. Użyj opcji **Short-lived objects filter (Filtr obiektów krótkotrwałych)** i **Small objects filter (Filtr małych obiektów)**, aby odfiltrować niepożądane wyniki.
5. Wybierz godziny rozpoczęcia i zakończenia oraz datę dla wyszukiwania. Użyj klawisza SHIFT, aby wybrać zakres dat.
6. Kliknij **Search (Wyszukaj)**.

Wyniki wyszukiwania zostaną wyświetlone na karcie **Results (Wyniki)**. W tym miejscu można kliknąć prawym przyciskiem myszy jeden lub kilka wyników, aby wyeksportować nagrania.

| | |
|---|---|
| **Short-lived objects filter (Filtr obiektów krótkotrwałych)** | Minimalny czas, przez jaki obiekt musi znajdować się w obszarze zainteresowania, aby został uwzględniony w wynikach wyszukiwania. |
| **Small objects filter (Filtr małych obiektów)** | Minimalna wymagana wielkość obiektu kwalifikująca do uwzględnienia go w wynikach wyszukiwania. |


*Inteligentne wyszukiwanie 1*

## Inteligentne wyszukiwanie 2

Funkcja Inteligentne wyszukiwanie 2 umożliwia znajdowanie w nagraniach poruszających się osób i pojazdów.

Po włączeniu funkcji Smart Search 2 (Inteligentne wyszukiwanie 2) dla kamery Axis AXIS Camera Station 5 rozpocznie rejestrowanie metadanych z tej kamery. Inteligentne wyszukiwanie 2 używa metadanych do klasyfikowania obiektów w scenie i umożliwia znajdowanie interesujących elementów za pomocą filtrów.

Uwaga

Wymagania funkcji Inteligentne wyszukiwanie 2:

- Strumieniowe przesyłanie metadanych analitycznych za pośrednictwem protokołu RTSP.
- Aplikacja AXIS Video Content Stream w kamerach z oprogramowaniem układowym AXIS OS w wersjach starszych niż 9.60. P. sekcja *Instalowanie aplikacji do kamery, on page 63*.
- Synchronizacja czasu między serwerem AXIS Camera Station 5 a kamerami.

Uwaga

Zalecenia ogólne:

- Zalecamy stosowanie nagrywania ciągłego. Korzystanie z detekcji ruchu może skutkować detekcją bez obrazu wideo.
- Zalecamy korzystanie z formatu H.264, aby podgląd nagrań był widoczny w wynikach wyszukiwania.
- Aby zapewnić optymalną klasyfikację kolorów, warunki oświetlenia muszą być zgodne ze specyfikacją kamery. W razie potrzeby użyj dodatkowego źródła światła.

### Proces

1. *Konfigurowanie funkcji Inteligentne wyszukiwanie 2, on page 156*
2. Skonfiguruj synchronizację czasu między serwerem AXIS Camera Station 5 a kamerami. Patrz *Synchronizacja czasu, on page 67*.
3. Tworzenie filtra lub wczytanie istniejącego filtra. Patrz *Wyszukiwanie z filtrami, on page 33*.
4. Zarządzanie wynikami wyszukiwania. Patrz *Wyniki inteligentnego wyszukiwania, on page 35*.

### Wyszukiwanie z filtrami

1. Otwórz menu **Configuration > Smart search 2 > Settings (Konfiguracja > Inteligentne wyszukiwanie 2 > Ustawienia)** i wybierz kamery, których chcesz używać na potrzeby funkcji Inteligentne wyszukiwanie 2.
2. Kliknij + i otwórz kartę **Smart search 2 (Inteligentne wyszukiwanie 2)**.
3. Określ kryteria wyszukiwania.
4. Kliknij **Search (Wyszukaj)**.

Jeśli wyszukiwanie trwa dłużej niż oczekiwano, wypróbuj jedną lub więcej z poniższych metod, aby je przyspieszyć:

- Włącz przetwarzanie w tle na serwerze w przypadku ważnych lub często używanych kamer.
- Zastosuj do kamer filtry przychodzące w celu ograniczenia nieistotnych detekcji.
- Skróć okres objęty wyszukiwaniem.
- Zmniejsz liczbę kamer objętych wyszukiwaniem.
- Zdefiniuj obszar, kierunek ruchu obiektu, wielkość i czas trwania, aby ograniczyć ilość danych.

| | |
|---|---|
| **Kamery** | Aby ograniczyć wyszukiwania według kamery, kliknij pozycję **Cameras (Kamery)** i wybierz kamery, które chcesz uwzględnić w wyszukiwaniu. |
| **Przedział wyszukiwania** | Aby ograniczyć wyszukiwanie według czasu, kliknij opcję **Search interval** (Interwał wyszukiwania), a następnie wybierz zakres czasu, konkretny przedział czasu obejmujący kilka dni, lub utwórz przedział niestandardowy. |
| **Osoba** | W celu detekcji osób, kliknij pozycje **Object characteristics (Cechy obiektu)** > **Pre-classified (Wstępnie sklasyfikowane)**, a następnie wybierz **Person (Osoba)** i kolory odzieży. Można wybrać wiele kolorów. |
| **Pojazd** | W celu detekcji pojazdów kliknij **Object characteristics (Cechy obiektu)** > **Pre-classified (Wstępnie sklasyfikowane)**, a następnie wybierz typy i kolory pojazdów. Można wybrać kilka typów i kolorów. |
| **Podobieństwo wizualne** | Można użyć wyniku wyszukiwania z osobą na obrazie do wyszukania osób o podobnym wyglądzie. Otwórz menu kontekstowe ⋮ w elemencie wyników wyszukiwania i wybierz **Use as visual similarity reference (Użyj jako odniesienie do ustalania podobieństwa wizualnego)**. Następnie kliknij **Search (Wyszukaj)**.<br>Uwaga<br>Funkcja wyszukiwania podobieństw tworzy abstrakcyjne reprezentacje z przyciętych i cechujących się niską rozdzielczością obrazów osób oraz porównuje je z innymi reprezentacjami. Gdy dwie reprezentacje okażą się podobne, wyszukiwanie kończy się trafieniem. Funkcja wyszukiwania podobieństw nie identyfikuje osób na podstawie danych biometrycznych, ale może na przykład rozpoznać czyjąś ogólną sylwetkę i kolor ubrania noszonego w danym czasie. |
| **Obszar** | Aby filtrować według obszaru, kliknij opcję **Area (Obszar)**, wybierz kamerę i włącz polecenie **Filter by area on this camera (Filtruj według obszaru w tej kamerze)**. Dostosuj obszar zainteresowania na obrazie i dodaj lub usuń potrzebne punkty. |
| **Przekroczenie linii** | Aby filtrować według przekroczenia linii, kliknij **Line crossing (Przekroczenie linii)**, wybierz kamerę, a następnie włącz **Filter by line crossing on this camera (Filtruj według przekroczenia linii w tej kamerze)**. Dostosuj linię na obrazie i dodaj lub usuń wybrane punkty. |
| **Rozmiar i czas trwania** | Aby filtrować według rozmiaru i czasu trwania, kliknij opcję **Size and duration (Rozmiar i czas trwania)**, wybierz kamerę i włącz **Filter by size and duration on this camera (Filtruj według rozmiaru i czasu trwania w tej kamerze)**. Dostosuj minimalną szerokość jako |

| | |
|---|---|
| | procent łącznej szerokości obrazu. Dostosuj minimalny czas trwania w sekundach. |
| **Prędkość** | Aby filtrować według prędkości, kliknij przycisk **Speed (Prędkość)**, wybierz kamerę i włącz **Filter by speed on this camera (Filtruj według prędkości w tej kamerze)**. Określ zakres prędkości, które mają zostać uwzględnione w filtrze.<br>Uwaga<br>Filtr prędkości jest dostępny w przypadku takich produktów jak radary i kamery radarowo-optyczne, które umożliwiają detekcję prędkości. |
| **Nieznane detekcje obiektów** | Aby uwzględnić detekcje, które funkcja Inteligentne wyszukiwanie 2 klasyfikuje jako nieznane, wybierz **Object characteristics (Cechy obiektu)**, a następnie **Unknown object detections (Nieznane detekcje obiektów)**. |
| | Aby zapisać filtr, kliknij , nadaj filtrowi nazwę i kliknij **Save (Zapisz)**.<br><br>Aby zastąpić istniejący filtr, kliknij , zaznacz filtr i kliknij **Replace (Zastąp)**. |
| | Aby załadować jedno z ostatnich wyszukiwań, kliknij > **Recent searches (Ostatnie wyszukiwania)** i wybierz wyszukiwanie.<br><br>Aby załadować jeden z zapisanych filtrów, kliknij > **Saved filter settings (Zapisane ustawienia filtrów)** i wybierz filtr. |
| | Aby zresetować filtr, kliknij i **Reset (Resetuj)**. |

## Wyniki inteligentnego wyszukiwania

| | |
|---|---|
| | Aby grupować detekcje, które prawdopodobnie należą do tego samego zdarzenia, można skategoryzować je w przedziałach czasowych. Wybierz interwał z rozwijalnego menu . |
| **Najpierw najpóźniejsze** | Inteligentne wyszukiwanie 2 wyświetla wyniki wyszukiwania w porządku malejącym. Jako pierwsze będą widoczne najnowsze detekcje. Kliknij **Oldest first (Najpierw najstarsze)**, aby najpierw były wyświetlane najdawniejsze detekcje. |
| **Confidence level (Poziom ufności)** | Aby dodatkowo przefiltrować wyniki wyszukiwania, kliknij opcję **Confidence level (Poziom ufności)** i ustaw poziom ufności. Wysoki poziom ufności powoduje ignorowanie niepewnych kategorii. |

| | |
|---|---|
| **Columns (Kolumny)** | Aby dostosować rozmiar miniatur w wynikach wyszukiwania, kliknij pozycję **Columns (Kolumny)** i zmień liczbę kolumn. |
| **Detection view (Widok detekcji)** | Aby wyświetlić przycięty widok wykrytych obiektów jako miniaturę, wybierz **Detection view (Widok detekcji)**. |

## Ograniczenia

- Funkcja Inteligentne wyszukiwanie 2 obsługuje tylko główny (nieprzycięty) obszar obserwacji.
- Funkcja Inteligentne wyszukiwanie 2 obsługuje tylko tryby przechwytywania bez przycięcia.
- W przypadku urządzeń z procesorem ARTPEC-7 lub nowszym i wersją oprogramowania sprzętowego niższą niż 10.6 korzystanie z funkcji Inteligentne wyszukiwanie 2 ze strumieniami z kamer w postaci odbicia lustrzanego i w formie odwróconej może powodować pewne problemy.
- Wysokie lub bardzo zmienne opóźnienia w sieci mogą powodować problem z synchronizowaniem czasu oraz wpływać na klasyfikowanie wykrytych obiektów na podstawie metadanych analitycznych.
- Niska jakość obrazu spowodowana wysokim stopniem kompresji, warunkami pogodowymi takimi jak ulewny deszcz lub intensywne opady śniegu, niską rozdzielczością kamery, znaczącymi zniekształceniami, dużym polem widzenia lub nadmiernym drganiami negatywnie wpływa na klasyfikowanie rodzajów obiektów i dokładność wykrywania.
- Inteligentne wyszukiwanie 2 może nie wykrywać małych i odległych obiektów.
- Rozpoznawanie kolorów nie działa w ciemności ani przy oświetlaniu podczerwienią.
- Kamery nasobne nie są obsługiwane.
- Radar może wykrywać tylko osoby i pojazdy. W przypadku radaru nie można włączyć klasyfikacji serwera w tle.
- Funkcja klasyfikowania obiektów przy wykrywaniu kamerami termowizyjnymi działa w nieprzewidziany sposób.
- Inteligentne wyszukiwanie 2 nie wykrywa poruszających się obiektów w przypadku zmiany prepozycji PTZ oraz przez krótki okres rekalibrowania po zmianie położenia.
- Ustawienia przekroczenia linii i filtry obszarów nie naśladują zmian pozycji PTZ.

## Wyszukiwanie danych

Wyszukiwanie danych pozwala znajdować dane w źródle zewnętrznym. Tym źródłem może być system lub urządzenie generujące dane, z których można uzyskać dodatkowe informacje o zdarzeniach. Więcej informacji: *Zewnętrzne źródła danych, on page 67*. Oto kilka przykładów:

- Zdarzenie wygenerowane przez system kontroli dostępu.
- Numery tablic rejestracyjnych odczytane przez aplikację AXIS License Plate Verifier.
- Prędkość odczytana przez aplikację AXIS Speed Monitor.

Aby zmienić czas przechowywania danych zewnętrznych przez AXIS Camera Station 5, wybierz kolejno **Configuration (Konfiguracja) > Server (Serwer) > Settings (Ustawienia) > External data (Dane zewnętrzne)**.

Aby wyszukać dane:

1. Kliknij + i wybierz **Data search (Wyszukiwanie danych)**.
2. Wybierz interwał wyszukiwania .
3. Wybierz typ źródła danych z listy rozwijanej.
4. Kliknij opcje wyszukiwania i zastosuj dodatkowe filtry. Filtry mogą się różnić w zależności od typu źródła danych.
5. Wpisz słowa kluczowe w polu wyszukiwania. Patrz *Optymalizowanie wyszukiwania, on page 38*.
6. Kliknij **Search (Wyszukaj)**.

Wyszukiwanie danych doda do zakładek dane wygenerowane ze źródła, jeśli skonfigurujesz to w widoku. Kliknięcie danych na liście spowoduje przejście do nagrania skojarzonego ze zdarzeniem.

| Przedział czasowy | |
|---|---|
| **Live (Na żywo)** | Aby przeszukiwać dane w czasie rzeczywistym, jako przedział czasowy wybierz **Live (Na żywo)**. Funkcja wyszukiwania danych pozwala wyświetlić maksymalnie 3000 danych zdarzeń na żywo. W trybie Na żywo operatory wyszukiwania nie działają. |
| **Ostatnia godzina – ostatnie 30 dni** | Aby wyszukać dane z ustawionego zakresu czasu, wybierz jedną z dostępnych opcji: ostatnia godzina, 4 godziny, 12 godzin, 24 godziny, 48 godzin, 7 dni, 30 dni. |
| **Niestandardowa** | Aby wyszukać dane z określonego zakresu czasu, wybierz **Custom** (Niestandardowa) i ustaw datę oraz godzinę początkową i końcową. |

Wyniki wyszukiwania można filtrować według różnych typów źródeł:

| Typ źródła danych | |
|---|---|
| **All data (Wszystkie dane)** | Ta opcja obejmuje dane pochodzące zarówno z komponentów, jak i ze źródeł zewnętrznych. |

| | |
|---|---|
| **Kontrola dostępu** | Kontrola dostępu jest przykładem komponentu generującego dane. Użyj tej opcji, jeśli chcesz dołączyć dane tylko z tego konkretnego komponentu. Kontrola dostępu umożliwia filtrowanie według drzwi i stref, posiadaczy kart oraz typów zdarzeń. |
| **Third party (Zewnętrzny dostawca)** | Użyj tej opcji, jeśli chcesz dołączyć dane ze źródeł innych niż skonfigurowane komponenty. |

W zależności od źródła danych w wynikach wyszukiwania mogą być wyświetlane różne elementy. Oto kilka przykładów:

| Wyniki wyszukiwania | |
|---|---|
| **Serwer** | Serwer, do którego wysłano dane zdarzenia. Widoczna tylko w przypadku połączenia z wieloma serwerami. |
| **Lokalizacja** | Nazwa drzwi oraz nazwa kontrolera drzwi z adresem IP. |
| **Enter speed (Prędkość wejściowa)** | Prędkość (kilometry lub mile na godzinę), z jaką obiekt dociera do strefy radarowej detekcji ruchu (RMD). |
| **Klasyfikacja** | Kategoria obiektu. Na przykład: Pojazdy. |

Aby wyeksportować wyniki wyszukiwania do pliku PDF lub tekstowego, kliknij **Download search result (Pobierz wyniki wyszukiwania)**. Ta funkcja eksportuje tylko informacje o zdarzeniach. Nagrania ani obrazy nie są eksportowane.

## Optymalizowanie wyszukiwania

Aby uzyskać bardziej precyzyjne wyniki, można użyć następujących operatorów wyszukiwania:

| | |
|---|---|
| Używaj cudzysłowów `" "`, aby znaleźć dokładne dopasowania słów kluczowych | • Szukanie wyrażenia `"door 1"` spowoduje zwrócenie wyników zawierających tekst „drzwi 1”.<br>• Szukanie wyrażenia `door 1` spowoduje zwrócenie wyników zawierających zarówno tekst „drzwi”, jak i „1”. |
| Używaj operatora `AND`, aby znaleźć pasujące elementy zawierające wszystkie słowa kluczowe. | • Szukanie wyrażenia `door AND 1` spowoduje zwrócenie wyników zawierających zarówno tekst „drzwi”, jak i „1”.<br>• Szukanie wyrażenia `"door 1" AND "door forced open"` spowoduje zwrócenie wyników zawierających zarówno tekst „drzwi 1”, jak i “drzwi wyważone”. |
| Używaj operatora `OR` albo `\|`, aby znaleźć pasujące elementy zawierające dowolne słowo kluczowe. | • Szukanie wyrażenia `"door 1" OR "door 2"` spowoduje zwrócenie wyników zawierających tekst „drzwi 1” lub „drzwi 2”.<br>• Szukanie wyrażenia `door 1 OR door 2` spowoduje zwrócenie wyników zawierających tekst „drzwi” lub „1” lub „2”. |
| Użyj nawiasów `( )` wraz z operatorem `AND` lub `OR`. | • Szukanie wyrażenia `(door 1 OR door 2) AND "Door forced open"` spowoduje zwrócenie wyników zawierających jeden z poniższych tekstów: |

| | |
|---|---|
| | – „drzwi 1" i „Drzwi wyważone"<br>– „drzwi 2" i „Drzwi wyważone"<br>• Szukanie wyrażenia `door 1 AND (door (forced open OR open too long))` spowoduje zwrócenie wyników zawierających jeden z poniższych tekstów:<br>– „drzwi 1" i „drzwi wyważone"<br>– „drzwi 1" i „przekroczony czas otwarcia drzwi" |
| Używaj symboli >, >=, < lub <= do filtrowania wartości liczbowych w konkretnych kolumnach. | • Szukanie wyrażenia `[Max speed] > 28` spowoduje zwrócenie wyników, które w kolumnie Prędkość maksymalna zawierają liczbę większą niż 28.<br>• Szukanie wyrażenia `[Average speed] <= 28` spowoduje zwrócenie wyników, które w kolumnie Średnia prędkość zawierają liczbę nie większą niż 28. |
| Użyj operatora `CONTAINS`, aby wyszukać tekst w określonej kolumnie. | • Szukanie wyrażenia `[Cardholder] CONTAINS Oscar` spowoduje zwrócenie danych, w których „Oscar" występuje w kolumnie „Cardholder" (Posiadacz karty).<br>• Szukanie wyrażenia `[Door] CONTAINS "door 1"` spowoduje zwrócenie danych, w których „drzwi 1" występują w kolumnie „Drzwi". |

# Konfiguracja

Na karcie Konfiguracja można zarządzać podłączonymi urządzeniami oraz ustawieniami klienta i serwerów.

Kliknij + i wybierz **Configuration (Konfiguracja)**, aby otworzyć kartę Configuration (Konfiguracja).

## Konfiguruj urządzenia

W środowisku AXIS Camera Station 5 urządzenie oznacza produkt sieciowy z adresem IP. Kamera to źródło sygnału wizyjnego. Może nim być kamera sieciowa lub port wideo (z podłączoną kamerą analogową) w wieloportowym wideoenkoderze. Na przykład 4-portowy wideoenkoder to jedno urządzenie z czterema kamerami.

Uwaga

- AXIS Camera Station 5 obsługuje tylko urządzenia z adresami IPv4.
- Niektóre wideoenkodery mają osobne adresy IP dla każdego portu wideo. W takim przypadku AXIS Camera Station 5 traktuje każdy port wideo jak jedno urządzenie z jedną kamerą.

W środowisku AXIS Camera Station 5 urządzenie może być:

- kamerą sieciową
- wideoenkoderem z jednym lub kilkoma portami wideo
- urządzeniem dodatkowym niebędącym kamerą, na przykład urządzeniem we/wy audio, głośnikiem sieciowym lub kontrolerem drzwi
- interkom

Wobec urządzeń można wykonywać następujące czynności:

- Dodawanie kamer i urządzeń bez funkcji wideo. Patrz *Dodawanie urządzeń*.
- Edytowanie preferencji podłączonych kamer. Patrz *Kamery*.
- Edytowanie preferencji urządzeń innych niż kamery. Patrz *Inne urządzenia*.
- Edytowanie profili strumienia obejmujące zmianę rozdzielczości, formatu itd. Patrz *Profile strumienia*.
- Dostosowywanie ustawień obrazu w czasie rzeczywistym. Patrz *Konfiguracja obrazu*.
- Dodawanie i usuwanie prepozycji PTZ. Patrz *Prepozycje PTZ*.
- Zarządzaj i konfiguruj podłączone urządzenia. Patrz *Zarządzanie urządzeniami*.
- Zarządzanie zewnętrznymi źródłami danych. Patrz *Zewnętrzne źródła danych, on page 67*.

### Dodawanie urządzeń

Uwaga

- System traktuje obszary obserwacji jak pojedyncze kamery. Aby móc używać obszarów obserwacji w kamerze, należy je najpierw utworzyć. Patrz *Używanie obszarów obserwacji*.
- Po dodaniu urządzenia synchronizuje ono czas z serwerem AXIS Camera Station 5.
- Najlepiej nie używać w nazwie hosta urządzenia znaków specjalnych, takich jak å, ä czy ö.

1. Znajdowanie urządzeń, strumieni wideo lub wstępnie nagranych filmów.
   - *Znajdowanie urządzeń, on page 42*
   - *Znajdowanie strumieni wideo, on page 42*
   - *Znajdowanie wstępnie nagranych filmów, on page 43*
2. *Dodawanie urządzeń, strumieni wideo lub wstępnie nagranych filmów, on page 43*

Przed dodaniem urządzenia należy rozwiązać wszelkie problemy widoczne w kolumnie statusu urządzenia.

| | |
|---|---|
| **(empty) (puste)** | Jeśli nie ma pokazanego statusu, można dodać urządzenie do AXIS Camera Station 5. |
| **Communicating (Łączenie)** | AXIS Camera Station 5 serwer próbuje uzyskać dostęp do urządzenia. |
| **Device certificate not trusted (Niezaufany certyfikat urządzenia)** | AXIS Camera Station 5 nie można zweryfikować, czy certyfikat HTTPS na urządzeniu został podpisany przez zaufanego wystawcę. Kliknij łącze, aby wystawić nowy certyfikat HTTPS lub poinformować stronę AXIS Camera Station 5, aby zaufała istniejącemu certyfikatowi. |
| **Organ wydający certyfikat wygasł** | Urząd certyfikacji, który wystawił certyfikat urządzenia, nie jest już ważny. Kliknij łącze, aby wystawić nowy certyfikat HTTPS lub poinformować stronę AXIS Camera Station 5, aby zaufała istniejącemu certyfikatowi. |
| **Niezgodność adresu w certyfikacie urządzenia** | Adres urządzenia nie jest zgodny z adresem w certyfikacie. Kliknij łącze, aby wystawić nowy certyfikat HTTPS lub poinformować stronę AXIS Camera Station 5, aby zaufała istniejącemu certyfikatowi. |
| **Communication error (Błąd komunikacji)** | AXIS Camera Station 5 nie można skontaktować się z urządzeniem. |
| **Enter password (Wprowadź hasło)** | AXIS Camera Station 5 nie wie, których poświadczeń użyć w celu uzyskania dostępu do urządzenia. Kliknij łącze, aby wprowadzić nazwę użytkownika i hasło konta administratora na urządzeniu. AXIS Camera Station 5 domyślnie będzie używać tej nazwy użytkownika i hasła na wszystkich urządzeniach, na których użytkownik już istnieje. |
| **Ustaw hasło** | Konto i hasło użytkownika głównego nie zostały skonfigurowane lub urządzenie nadal korzysta z domyślnego hasła. Kliknij łącze, aby ustawić hasło użytkownika głównego.<br>• Wprowadź hasło lub kliknij **Generate (Generuj)** , aby uzyskać hasło. Zalecamy wyświetlenie wygenerowanego hasła i utworzenie jego kopii.<br>• Zaznacz opcję używania tego hasła na wszystkich urządzeniach mających status `Set password` (Ustaw hasło). |
| **Model not supported (Model nie jest obsługiwany)** | AXIS Camera Station 5 nie obsługuje modelu urządzenia. |
| **Obsolete firmware (Przestarzałe oprogramowanie sprzętowe)** | Oprogramowanie sprzętowe urządzenia jest przestarzałe i aby można było dodać urządzenie, należy je zaktualizować. |
| **Urządzenie niesprawne** | Parametry urządzenia pobrane przez AXIS Camera Station 5 są uszkodzone. |
| **Set tilt orientation (Ustaw kierunek pochylenia)** | Kliknij łącze, aby wybrać kierunek przechyłu Sufit, Ściana lub Biurko, zależnie od sposobu montażu |

| | |
|---|---|
| | kamery. W niektórych kamerach orientacja przechyłu jest parametrem obowiązkowym. |
| **Nieobsługiwane urządzenie ONVIF** | AXIS Camera Station 5 nie obsługuje tego urządzenia innego producenta. |
| **Nieobsługiwane urządzenie** | AXIS Camera Station 5 nie obsługuje tego rodzaju urządzeń. |

Uwaga

Nowe certyfikaty HTTPS są wystawiane przez AXIS Camera Station 5 i będą automatycznie odnawiane.

**Znajdowanie urządzeń**

Aby znaleźć urządzenia, których nie ma na liście:

1. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)**.
2. Kliknij przycisk **Cancel (Anuluj)**, aby przerwać trwające przeszukiwanie sieci.
3. Kliknij przycisk **Wyszukiwanie ręczne**.
4. Aby znaleźć wiele urządzeń należących do jednego lub kilku zakresów adresów IP:
   4.1. Zaznacz opcję **Przeszukaj co najmniej jeden zakres adresów IP**.
   4.2. Wpisz zakres adresów IP. Na przykład: 192.168.10.*, 192.168.20-22.*, 192.168.30.0-50
   - Użyj symbolu wieloznacznego, aby znaleźć wszystkie adresy w grupie.
   - Użyj myślnika, aby znaleźć zakres adresów.
   - Do oddzielania zakresów używaj przecinka.

   4.1. Aby zmienić domyślny port 80, wpisz zakres portów. Na przykład: 80, 1080-1090
   - Użyj myślnika, aby określić zakres portów.
   - Do oddzielania zakresów używaj przecinka.

   4.1. Kliknij **Search (Wyszukaj)**.
5. Aby znaleźć jedno lub więcej konkretnych urządzeń:
   5.1. Zaznacz opcję **Wprowadź jedną lub więcej nazw hostów lub adresów IP**.
   5.2. Wprowadź nazwy hostów lub adresy IP, oddzielając je przecinkami.
   5.3. Kliknij **Search (Wyszukaj)**.
6. Kliknij przycisk **OK**.

**Znajdowanie strumieni wideo**

Można dodawać strumienie wideo o następujących parametrach:

- Protokół: RTSP, HTTP, HTTPS
- Kodowanie wideo: M-JPEG dla HTTP i HTTPS, H.264 dla RTSP
- Kodowanie dźwięku: AAC i G.711 dla RTSP

Obsługiwane schematy URL strumieni wideo:

- `rtsp://<address>:<port>/<path>`
  Przykład: `rtsp://<address>:554/axis-media/media.amp`
- `http://<address>:80/<path>`
  Przykład: `http://<address>:80/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

- `https://<address>:443/<path>`
  Przykład: `https://<address>:443/axis-cgi/mjpg/video.cgi?date=1&clock=1&resolution=1920x1080`

1. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)**.
2. Kliknij przycisk **Wprowadź adresy URL strumieni** i wprowadź jeden lub więcej adresów URL strumieni, rozdzielając je przecinkami.
3. Kliknij **Dodaj**.

**Znajdowanie wstępnie nagranych filmów**

Gotowe nagrania wideo w formacie .mkv można dodać do AXIS Camera Station 5.

wymagań dotyczących pliku .mkv:

- Kodowanie wideo: M-JPEG, H.264, H.265
- Kodowanie dźwięku: AAC

1. Utwórz folder **PrerecordedVideos** w lokalizacji `C:\ProgramData\Axis Communications\AXIS Camera Station Server`.
2. Dodaj plik .mkv do tego folderu.
3. Aby korygować zniekształcenia wstępnie nagranego wideo, dodaj do folderu plik .dewarp o takiej samej nazwie, jak plik .mkv. Więcej informacji: *Konfiguracja obrazu, on page 52*.
4. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)** i włącz opcję **Include prerecorded video (Dołącz wstępnie zarejestrowany obraz wideo)**. W oknie zobaczysz swój wstępnie nagrany film oraz kilka wstępnie nagranych filmów umieszczonych fabrycznie w systemie.

**Dodawanie urządzeń, strumieni wideo lub wstępnie nagranych filmów**

1. W systemie wieloserwerowym wybierz serwer z listy rozwijanej **Selected server (Wybrany serwer)**.
2. Wybierz kolejno opcje **Configuration > Devices > Add devices (Konfiguracja > Urządzenia > Dodaj urządzenia)**.
3. Jeżeli chcesz zmienić nazwę urządzenia, kliknij nazwę na liście i wprowadź nową nazwę.
4. Wybierz urządzenia, strumienie wideo lub wstępnie nagrane filmy. Kliknij **Dodaj**.
5. Określ, czy w miarę możliwości zamiast adresów IP mają być używane nazwy hostów.
6. Wybierz opcję **Quick configuration (Szybka konfiguracja)**, jeśli chcesz tylko skonfigurować ustawienia podstawowe.
   Jeśli importujesz projekt narzędzia Site Designer, zob. *Importowanie projektów z aplikacji Site Designer*.
7. Wybierz preferowane ustawienia **Retention time (Czas przechowywania)**, **Recording storage (Pamięć masowa nagrań)** i **Recording method (Metoda nagrywania)**.

Uwaga

W przypadku wybrania opcji **Automatic (Automatycznie)** dla pamięci masowej nagrań, każdej kamerze będzie w miarę możliwości przydzielana pamięć masowa o pojemności co najmniej 32 GB na dysku bez systemu operacyjnego. System automatycznie wybiera pamięci masowe z co najmniej 15 GB dostępnego miejsca, a następnie pamięci masowe z mniejszą liczbą kamer skonfigurowanych do nagrywania oraz wszelkie pamięci masowe zainstalowane już w AXIS Camera Station 5.

8. Kliknij **Install (Zainstaluj)**. AXIS Camera Station 5 automatycznie włącza protokół HTTPS na urządzeniach, które go obsługują.

**Importowanie projektów z aplikacji Site Designer**

AXIS Site Designer to internetowe narzędzie projektowe, które pomaga zbudować instalację w obiekcie opartą na produktach i akcesoriach Axis.

Jeśli utworzono lokalizację w aplikacji AXIS Site Designer, możesz zaimportować ustawienia projektu do AXIS Camera Station 5. Dostęp do projektu można uzyskać za pomocą kodu dostępu lub pobranego pliku konfiguracyjnego programu Site Designer.

Aby zaimportować projekt z programu Site Designer do AXIS Camera Station 5:

1. Wygeneruj kod dostępu do projektu narzędzia Site Designer albo pobierz plik projektu.
   1.1. Zaloguj się na stronie *http://sitedesigner.axis.com* przy użyciu swojego konta MyAxis.
   1.2. Zaznacz projekt i przejdź do strony projektu.
   1.3. Kliknij przycisk **Share (Udostępnij)**.
   1.4. Kliknij **Generate code (Wygeneruj kod)**, jeśli serwer AXIS Camera Station 5 ma połączenie z Internetem. Jeśli serwer nie ma połączenia z Internetem, kliknij **Download settings file (Pobierz plik ustawień)**.
2. W kliencie AXIS Camera Station 5 wybierz kolejno **Configuration (Konfiguracja) > Devices (Urządzenia) > Add devices (Dodaj urządzenia)**.
3. Zaznacz kamery i kliknij przycisk **Add (Dodaj)**.
4. Zaznacz pozycję **Konfiguracja aplikacji Site Designer** i kliknij przycisk **Dalej**.
5. Zaznacz opcję **Access code (Kod dostępu)** i wprowadź kod dostępu. Lub wybierz opcję **Choose file (Wybierz plik)** i znajdź do pobrany plik konfiguracyjny aplikacji Site Designer.
6. Kliknij przycisk **Import (Importuj)**. Podczas importu AXIS Camera Station 5 próbuje dopasować projekt z programu Site Designer do wybranych kamer według adresu IP lub nazwy produktu. W przypadku niepowodzenia dopasowania można wybrać odpowiednią kamerę z rozwijalnego menu.
7. Kliknij przycisk **Install (Instaluj)**.

AXIS Camera Station 5 importuje następujące ustawienia z projektu programu Site Designer:

| | Enkodery, dekodery drzwi, kontrolery drzwi, detektory radarowe i głośniki: | Kamery, interkomy i urządzenia z serii F/FA |
|---|---|---|
| Harmonogramy z nazwami i przedziałami czasowymi | ✓ | ✓ |
| Mapy z nazwami, kolorami ikon, umiejscowieniem ikon i nazwami elementów | ✓ | ✓ |
| Nazwa | ✓ | ✓ |
| Opis | ✓ | ✓ |
| Nagrywanie wyzwalane ruchem: harmonogram i profil nagrywania, w tym poklatkowość, rozdzielczość, kodowanie wideo i kompresja | | ✓ |
| Nagrywanie ciągłe: harmonogram i profil nagrywania, w tym poklatkowość, rozdzielczość, kodowanie wideo i kompresja | | ✓ |
| Siła technologii Zipstream | | ✓ |
| Ustawienia dźwięku w podglądzie na żywo i nagraniach | | ✓ |
| Czas przechowywania nagrań | | ✓ |

Uwaga

- Jeśli zdefiniowano tylko jeden profil nagrywania lub jeśli w projekcie z programu Site Designer istnieją dwa identyczne profile nagrywania, AXIS Camera Station 5 ustawia profil na poziom średni.
- Jeśli w projekcie z programu Site Designer zdefiniowano oba profile nagrywania, AXIS Camera Station 5 ustawi profil nagrywania ciągłego jako średni, a nagrywanie wyzwalane ruchem na poziom wysoki.
- AXIS Camera Station 5 optymalizuje współczynnik proporcji, co oznacza, że rozdzielczość może się różnić między importem a projektem Site Designer.
- AXIS Camera Station 5 może skonfigurować ustawienia dźwięku, jeśli urządzenie ma wbudowany mikrofon lub głośnik. Aby używać zewnętrznego urządzenia audio, włącz je ręcznie po jego zainstalowaniu.
- AXIS Camera Station 5 nie stosuje ustawień dźwięku do interkomów, nawet jeśli ustawienia w aplikacji Site Designer różnią się. W przypadku interkomów dźwięk jest zawsze włączony tylko w podglądzie na żywo.


**Dodawanie urządzeń innych producentów**

Urządzenia innych firm można dodawać do witryny AXIS Camera Station 5 tak samo jak produkty Axis. Patrz *Dodawanie urządzeń*.

Uwaga

Urządzenia innych firm można też dodawać do AXIS Camera Station 5 jako strumienie wideo. Patrz *Znajdowanie strumieni wideo, on page 42*.

Informacje o obsłudze urządzeń innych producentów można znaleźć w *najnowszej dokumentacji technicznej*.

Uwaga

Można pobrać i uruchomić narzędzie AXIS Camera Station Device Compatibility Tool, które zweryfikuje kompatybilność produktów do sieciowego dozoru wizyjnego z aplikacją AXIS Camera Station w wersji 5 lub nowszych. Narzędzie sprawdza, czy system może odbierać strumienie wideo z produktów do sieciowego dozoru wizyjnego. Zobacz *AXIS Camera Station Device Compatibility Tool*.

AXIS Camera Station 5 nie jest zgodny z normą ONVIF, lecz wymaga aby urządzenia innych producentów były zgodne z normą ONVIF Profile S i zweryfikowane za pomocą narzędzia AXIS Camera Station Device Compatibility Tool.

AXIS Camera Station 5 obsługuje następujące funkcje na urządzeniach innych producentów zgodnie z normami IEC62676-2-31 i IEC62676-2-32:

- Wykrywanie kamer
- Kodowanie wideo: M-JPEG, H.264
- Kodowanie dźwięku: G.711 (jednokierunkowe, z urządzenia do AXIS Camera Station 5)
- Jeden profil wideo na kamerę
- Podgląd na żywo
- Nagrywanie ciągłe i ręczne
- Odtwarzanie
- Eksportowanie zapisów
- Wyzwalacze oparte na zdarzeniach w urządzeniach

- Obrót/pochylenie/zbliżenie

**Używanie obszarów obserwacji**

Niektóre modele kamer obsługują obszary obserwacji. AXIS Camera Station 5 wyświetla obszary obserwacji na stronie **Add devices (Dodaj urządzenia)** jako osobne kamery. Patrz *Dodawanie urządzeń*.

Uwaga

- Wszystkie obszary obserwacji w kamerze sieciowej są traktowane jako jedna kamera z perspektywy obliczeń łącznej liczby kamer dozwolonych w ramach licencji AXIS Camera Station 5.
- Liczba kamer, które można dodać, zależy od licencji.
- Każda licencja AXIS Camera Station 5 umożliwia podłączenie określonej liczby kamer.

Aby korzystać z obszarów obserwacji w AXIS Camera Station 5, należy najpierw je włączyć w kamerze:

1. Wybierz kolejno opcje **Configuration > Devices > Cameras (Konfiguracja > > Urządzenia > Kamery)**.
2. Zaznacz kamerę i kliknij łącze w kolumnie Adres.
3. Na stronie konfiguracyjnej kamery wprowadź nazwę użytkownika i hasło, za pomocą których chcesz się logować.
4. Kliknij przycisk **Help (Pomoc)**, aby się dowiedzieć, gdzie znaleźć ustawienia różniące się w zależności od modeli i oprogramowania sprzętowego kamer.

## Kamery

Otwórz menu **Configuration > Devices > Cameras (Konfiguracja > Urządzenia > Kamery)**, aby zobaczyć pełną listę kamer dodanych do systemu.

Na tej stronie można:

- Kliknąć adres kamery, aby otworzyć jej interfejs WWW. Wymaga to braku NAT lub zapory między klientem AXIS Camera Station 5 a urządzeniem.
- Edycja ustawień kamery. Patrz *Edycja ustawień kamery*.
- Usuwanie kamer. W ramach tej operacji AXIS Camera Station 5 usuwa wszystkie nagrania powiązane z usuwanymi kamerami, w tym te zablokowane.

**Edycja ustawień kamery**

Aby zmodyfikować ustawienia kamery:

1. Wybierz kolejno opcje **Configuration > Devices > Cameras (Konfiguracja > > Urządzenia > Kamery)**.
2. Zaznacz kamerę i kliknij przycisk **Edit (Edytuj)**.

| | |
|---|---|
| **Włączone** | Aby zablokować nagrywanie i oglądanie strumienia wideo, odznacz opcję **Enabled (Włączone)**. Nadal można skonfigurować nagrania i podgląd na żywo. |
| **Kanał** | Jeżeli pole **Channel (Kanał)** jest dostępne dla wieloportowych wideoenkoderów, wybierz numer portu.<br><br>Jeżeli pole **Channel (Kanał)** jest dostępne dla obszarów obserwacji, wybierz liczbę odpowiadającą obszarowi obserwacji. |
| **Nazwa użytkownika** | Nazwa użytkownika konta administratora w kamerze. |
| **Hasło** | Hasło dla konta administratora na kamerze. AXIS Camera Station 5 używa tego hasła do komunikacji z kamerą. |

## Inne urządzenia

Otwórz menu **Configuration > Devices > Other devices (Konfiguracja > Urządzenia > Inne urządzenia)**, aby wyświetlić listę urządzeń bez funkcji wideo. Na liście tej widnieją kontrolery drzwi, urządzenia audio i moduły We/Wy.

Więcej informacji o obsługiwanych produktach można uzyskać w witrynie *www.axis.com*. Patrz *Używanie dźwięku z innych urządzeń*.

Na tej stronie można:

- Otworzyć interfejs WWW urządzenia, klikając jego adres. Wymaga to braku NAT lub zapory między klientem AXIS Camera Station 5 a urządzeniem.
- Edytować ustawienia urządzenia, takie jak nazwa urządzenia, adres i hasło.
- Usuwać urządzenia.

### Edytowanie ustawień innych urządzeń

Aby edytować ustawienia urządzenia innego niż kamera:

1. Wybierz kolejno opcje **Configuration > Devices > Other devices (Konfiguracja > Urządzenia > Inne urządzenia)**.
2. Zaznacz urządzenie i kliknij przycisk **Edit (Edytuj)**.

| | |
|---|---|
| **Nazwa użytkownika** | Nazwa użytkownika konta administratora na urządzeniu. |
| **Hasło** | Hasło dla konta administratora na urządzeniu. AXIS Camera Station 5 używa tego hasła do komunikacji z urządzeniem. |

## Profile strumienia

Profil strumienia to grupa ustawień wpływających na strumień wideo, takich jak rozdzielczość, format wideo, liczba klatek na sekundę i kompresja. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumieni)**, a zostanie otwarta strona Profile strumieni. Na stronie zostanie wyświetlona lista wszystkich kamer.

W ustawieniach podglądu na żywo i nagrań można używać następujących profili:

**Wysoki –** Najwyższa jakość i rozdzielczość.

**Średni –** Optymalny kompromis między wysoką jakością a szybkością działania.

**Niski –** Najwyższa szybkość działania.

Uwaga

Profil strumienia jest domyślnie ustawiony na **Automatic (Automatycznie)** w podglądzie na żywo i nagraniach, dlatego w zależności od dostępnego rozmiaru strumienia wideo profil strumienia zmienia się automatycznie na **High (Wysoki)**, **Medium (Średni)** lub **Low (Niski)**.

### Edytowanie profili strumienia

1. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumienia)** i zaznacz kamery, które chcesz skonfigurować.
2. W obszarze **Video profiles (Profile wideo)** skonfiguruj rozdzielczość, format wideo, poklatkowość i kompresję.
3. W obszarze **Audio (Dźwięk)** skonfiguruj mikrofon i głośnik.

4. W obszarze **Advanced (Zaawansowane)** skonfiguruj dane analityczne, przesyłanie strumieniowe FFmpeg, wskaźniki PTZ automatycznego śledzenia obiektów i niestandardowe ustawienia strumienia. W przypadku niektórych produktów te ustawienia nie są dostępne.
5. Kliknij przycisk **Apply (Zastosuj)**.

**Profile wideo**

| | |
|---|---|
| **Enkoder** | • Dostępne opcje zależą od konfiguracji wideoenkodera w urządzeniu. To ustawienie jest dostępne tylko dla urządzeń innych producentów.<br>• Konfiguracji wideoenkodera można używać tylko dla jednego profilu wideo.<br>• Jeżeli urządzenie ma tylko jedną konfigurację kodera, widać tylko profil **Medium (Średni)**. |
| **Rozdzielczość** | Dostępne opcje zależą od modelu kamery. Wyższa rozdzielczość przekłada się na obraz zawierający więcej szczegółów, ale zwiększa zapotrzebowanie na pasmo i pamięć masową. |
| **Formatuj** | Dostępne opcje zależą od modelu kamery. Większość kamer obsługuje standardy **H.264** oraz **M-JPEG**. Standard H.264 wymaga mniejszej przepustowości łącza i mniejszej przestrzeni pamięci masowej niż standard M-JPEG. Niektóre kamery obsługują również standard **H.265** zapewniający nieco lepszą kompresję, wymagający jednak większej mocy obliczeniowej. Nasze kamery najnowszej generacji obsługują standard AV1 zapewniający dobrą kompresję oraz szereg nowych funkcji, takich jak przełączane nakładanie. |
| **Liczba klatek przesyłanych w ciągu zadanej jednostki czasu** | Rzeczywista poklatkowość zależy od modelu kamery, warunków panujących w sieci i konfiguracji komputera. |
| **Kompresja** | Niższa kompresja poprawia jakość obrazu, ale wymaga większej przepustowości i przestrzeni zasobu. |

Uwaga

- Na listach rozwijalnych audio pojawiają się wyłącznie kamery z oprogramowaniem układowym w wersji 5 lub nowszej.
- Jeżeli z tego samego źródła audio korzysta ponad 5 kamer, kamera źródłowa może ulec przeciążeniu i działać z pogorszeniem parametrów.

**Zipstream**

| | | | |
|---|---|---|---|
| **Siła** | Siła Zipstream określa poziom redukcji przepływności w strumieniu H.264 lub H.265 w czasie rzeczywistym. Ta opcja jest dostępna tylko dla urządzeń Axis obsługujących technologię Zipstream. | **Domyślne** | Użyj ustawienia Zipstream skonfigurowanego na stronie interfejsu WWW urządzenia. |
| | | **Wył.** | Brak |
| | | **Niski** | Brak widocznych skutków w większości scen |
| | | **Średni** | Widoczne skutki w niektórych scenach: mniej zakłóceń (szumu) i nieco mniejsza szczegółowość w obszarach mniejszego zainteresowania |
| | | **Wysoki** | Widoczne skutki w wielu scenach: mniej zakłóceń (szumu) i mniejsza szczegółowość w obszarach mniejszego zainteresowania |
| | | **Wyższy** | Widoczne skutki w jeszcze większej liczbie scen: mniej zakłóceń (szumu) i mniejsza szczegółowość w obszarach mniejszego zainteresowania |
| | | **Niezwykle wysoki** | Widoczne skutki w większości scen: mniej zakłóceń (szumu) i mniejsza szczegółowość w obszarach mniejszego zainteresowania |

| | | | |
|---|---|---|---|
| **Optymalizacja pod kątem zasobu** | Zipstream optymalizuje strumień wideo pod kątem zasobu przy użyciu profilu **Optimize for storage (Optymalizuj pod kątem zasobu)**. Optymalizacja pod kątem zasobu wykorzystuje bardziej zaawansowane narzędzia kompresji w celu zaoszczędzenia dodatkowej przestrzeni zasobu w porównaniu z domyślnym ustawieniem Zipstream. Ten profil może dodatkowo zmniejszyć przepływność nawet w przypadku scen z dużą ilością ruchu.<br>• Format asf nie obsługuje ramek B używanych przez tę funkcję.<br>• Ta funkcja nie ma wpływu na wideo nagrane na rejestratorach z serii AXIS S30.<br>• Ta funkcja wymaga systemu AXIS OS 11.7.59 lub nowszego. | | |

**Dźwięk**

| | |
|---|---|
| **Mikrofon:** | W celu powiązania mikrofonu z kamerą zaznacz opcję **Built-in microphone or line in (Wbudowany mikrofon lub wejście liniowe)** albo mikrofon innego urządzenia. Patrz *Używanie dźwięku z innych urządzeń*. |
| **Głośnik:** | W celu powiązania głośnika z kamerą zaznacz opcję **Wbudowany głośnik lub wyjście liniowe** albo głośnik innego urządzenia. Do przekazywania komunikatów głosowych używaj mikrofonu podłączonego do komputera. Patrz *Używanie dźwięku z innych urządzeń*. |
| **Use microphone for: (Użyj mikrofonu przy)** | Włącz transmitowanie dźwięku przez mikrofon dla jednego lub dwóch strumieni. Funkcję można włączyć dla podglądu na żywo i nagrań, tylko podglądu na żywo lub tylko nagrań. |

**Zaawansowane**

| | |
|---|---|
| **Dołącz dane analityczne** | Aby umożliwić zbieranie danych na potrzeby inteligentnego wyszukiwania w trakcie strumieniowego przesyłania wideo, zaznacz opcję **Include analytics data (Uwzględnij dane analityczne)**. Ta opcja jest dostępna tylko dla urządzeń Axis obsługujących dane analityczne. Gromadzenie danych dla funkcji *Inteligentne wyszukiwanie 1* może powodować opóźnienia w strumieniowej transmisji wideo na żywo. |
| **Użyj FFmpeg** | Aby zwiększyć kompatybilność z urządzeniami innych producentów, zaznacz opcję **Use FFmpeg (Użyj FFmpeg)**, co spowoduje włączenie strumieniowego przesyłania w formacie FFmpeg. To ustawienie jest dostępne tylko dla urządzeń innych producentów. |
| **Pokaż wskaźniki PTZ automatycznego śledzenia obiektów** | Aby wskaźniki obiektów wykrywanych przez kamerę PTZ były wyświetlanie w podglądzie na żywo, zaznacz opcję **Show PTZ autotracking object indicators (Pokaż wskaźniki PTZ automatycznego śledzenia obiektów)** oraz ustaw czas buforowania strumienia wideo na maksymalnie 2000 milisekund. Ta opcja jest dostępna tylko dla kamer PTZ Axis używających aplikacji AXIS PTZ Autotracking. Opis całej procedury konfigurowania funkcji AXIS PTZ Autotracking w aplikacji AXIS Camera Station 5 znajduje się w temacie *Konfigurowanie funkcji AXIS PTZ Autotracking*. |
| **Dostosowywanie strumienia** | Aby dostosować ustawienia transmisji strumieniowej dla określonego profilu, wprowadź ustawienia oddzielone znakami `&` dla profilu. Na przykład, wpisz `overlays=off&color=0`, aby ukrywać nałożenia w tej kamerze.<br><br>Ustawienia niestandardowe zastępują wszelkie istniejące ustawienia. W ustawieniach niestandardowych nie podawaj żadnych poufnych informacji. |

Aby **dostosować ustawienia profilu** dotyczące rozdzielczości, poklatkowości, kompresji, formatu wideo i dźwięku, zaznacz kamerę, którą chcesz skonfigurować. W przypadku kamer o takiej samej nazwie modelowej z identycznymi możliwościami konfiguracji można konfigurować wiele kamer naraz. Patrz *Ustawienia konfiguracyjne*.

Aby **dostosować ustawienia profilu dla nagrań**, patrz *Metoda nagrywania*.

Można **zmniejszyć rozdzielczość i poklatkowość podglądu na żywo w celu zmniejszenia wykorzystania pasma**, na przykład w sytuacji wolnego połączenia między klientem AXIS Camera Station 5 a serwerem AXIS Camera Station 5. Patrz punkt Wykorzystanie przepustowości w temacie *Przesyłanie strumieniowe*.

#### Używanie dźwięku z innych urządzeń

Dźwięk z innych urządzeń niebędących kamerami (dodatkowych) można łączyć z materiałem wizyjnym z kamery sieciowej lub wideoenkodera na potrzeby oglądania na żywo lub nagrywania.

1. Dodawanie urządzeń innych niż kamery do AXIS Camera Station 5. Patrz *Dodawanie urządzeń*.
2. Skonfiguruj kamerę, aby używała dźwięku z urządzenia. Patrz *Profile strumienia*.
3. Włącz wykorzystywanie dźwięku w podglądzie na żywo lub nagraniach. Patrz *Profile strumienia*.

W *samouczkach wideo do aplikacji AXIS Camera Station* można znaleźć następujące przykłady:

- Konfiguracja urządzeń audio i ogłaszanie komunikatów na żywo
- Utworzenie przycisku akcji powodującego ręczne odtwarzanie dźwięku po wykryciu ruchu
- Automatycznie odtwarzaj dźwięk po wykryciu ruchu
- Dodawanie klipu audio do głośnika i AXIS Camera Station 5

### Konfiguracja obrazu

Można konfigurować ustawienia obrazu kamer połączonych z AXIS Camera Station 5.

Uwaga

Zmiany dokonane w konfiguracji obrazu są stosowane natychmiast.

Aby skonfigurować ustawienia obrazu:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Devices (Urządzenia) > Image configuration (Konfiguracja obrazu)**. Zostanie wyświetlona lista wszystkich kamer dodanych do AXIS Camera Station 5.
2. Zaznacz kamerę, a pod listą będzie wyświetlany pochodzący z niej sygnał wideo w czasie rzeczywistym. Za pomocą pola **Wpisz, aby wyszukać** odszukaj konkretną kamerę spośród figurujących na liście.
3. Skonfiguruj ustawienia obrazu.

#### Ustawienia obrazu

**Jasność:** Regulacja jasności obrazu. Wyższa wartość powoduje jaśniejszy obraz.

**Poziom koloru:** Regulacja nasycenia koloru. Im niższa wartość, tym mniejsze nasycenie koloru. Poziom koloru 0 skutkuje obrazem czarno-białym. Wartość maksymalna powoduje największe możliwe nasycenie barw.

**Ostrość:** Regulacja ostrości stosowanej do obrazu. Zwiększenie ostrości może zwiększyć szumy w obrazie, zwłaszcza przy słabym oświetleniu. Duża ostrość może również prowadzić do powstawania artefaktów wokół kontrastowych obszarów, na przykład na ostrych krawędziach. Mniejsza ostrość redukuje szumy na obrazie, ale pogarsza wyrazistość obrazu.

**Kontrast:** Regulacja kontrastu obrazu.

**Balans bieli:** Wybierz opcję balansu bieli z listy rozwijanej. Balans bieli pozwala uzyskać spójny wygląd kolorów w obrazie niezależnie od temperatury barwowej źródła światła. Po wybraniu opcji **Automatycznie** lub **Auto** kamera będzie identyfikować źródło światła i automatycznie kompensować barwy względem jego koloru. W

razie niezadowalającego wyniku wybierz opcję odpowiadającą rodzajowi źródła światła. Dostępne opcje zależą od modelu kamery.

**Obróć obraz:** Ustawianie liczby stopni, o jaką obraz zostanie obrócony.

**Automatyczne obracanie obrazu:** Po włączeniu tej opcji obrót obrazu będzie dostosowywany automatycznie.

**Obraz lustrzany:** Włącz, aby zastosować lustrzane odbicie obrazu.

**Backlight compensation (Kompensacja tylnego oświetlenia):** Włącz tę opcję, jeśli plama jasnego światła, na przykład żarówka, sprawia, że inne obszary obrazu wyglądają na zbyt ciemne.

**Dynamic contrast (wide dynamic range) (Kontrast dynamiczny (szeroki zakres dynamiki)):** Włącz to ustawienie, aby używać szerokiego zakresu dynamiki w celu poprawy naświetlenia w przypadku znacznego kontrastu pomiędzy jasnymi i ciemnymi obszarami na obrazie. Za pomocą suwaka dostosuj kontrast dynamiczny. Włączaj kontrast dynamiczny w warunkach intensywnego podświetlenia. Wyłączaj kontrast dynamiczny przy słabym oświetleniu.

**Niestandardowe ustawienia korekcji:** Można zaimportować plik .dewarp zawierający informacje o parametrach obiektywu, środkach optycznych i orientacji przechyłu kamery. Kliknij przycisk **Resetuj**, aby przywrócić pierwotne wartości parametrów.

1. Utwórz plik .dewarp zawierający następujące parametry:
   - Wymagane: `RadialDistortionX`, `RadialDistortionY`, `RadialDistortionZ` oraz `TiltOrientation`. Możliwe wartości dla `TiltOrientation` to `wall`, `desk` oraz `ceiling`.
   - Opcjonalne: `OpticalCenterX` oraz `OpticalCenterY`. Jeżeli chcesz ustawić środki optyczne, należy dodać oba parametry.
2. Kliknij przycisk **Importuj** i przejdź do pliku .dewarp.

Poniżej znajduje się przykład pliku .dewarp:

```
RadialDistortionX=-43.970703 RadialDistortionY=29.148499 RadialDistortionZ=715.732193
TiltOrientation=Desk OpticalCenterX=1296 OpticalCenterY=972
```

## Prepozycje PTZ

Funkcjonalność PTZ (Pan, Tilt, Zoom) to zdolność obrotu (przesuwania w lewo i w prawo), pochylania (przesuwania w górę i w dół) i przybliżania widoku.

Wybierz kolejno opcje **Konfiguracja > Urządzenia > Prepozycje PTZ**. Zostanie wyświetlona lista wszystkich kamer obsługujących funkcje PTZ. Kliknij kamerę, a zostaną wyświetlone wszystkie dostępne dla niej predefiniowane ustawienia. Kliknij przycisk **Odśwież**, aby zaktualizować listę prepozycji.

Funkcji PTZ można używać w:

- Kamerach PTZ, czyli kamerach z wbudowanym fizycznym mechanizmem PTZ
- Kamerach stałopozycyjnych, w których włączono cyfrowy PTZ
- Kamery zgodne ze standardem ONVIF obsługujące położenia zaprogramowane PTZ.

Cyfrowy PTZ włącza się na wbudowanej stronie konfiguracyjnej kamery. Więcej informacji można znaleźć w instrukcji obsługi kamery. Aby otworzyć stronę konfiguracyjną, przejdź do strony zarządzania urządzeniami, zaznacz kamerę i kliknij łącze w kolumnie adresu.

Prepozycje PTZ można konfigurować w aplikacji AXIS Camera Station 5 i na stronie konfiguracyjnej kamery. Zalecamy konfigurowanie prepozycji PTZ w aplikacji AXIS Camera Station 5.

- Jeżeli prepozycje PTZ są definiowane na stronie konfiguracyjnej kamery, można oglądać tylko strumień mieszczący się w granicach tych prepozycji. Ruchy PTZ w podglądzie na żywo można obserwować i są one nagrywane.
- W przypadku skonfigurowania prepozycji PTZ w aplikacji AXIS Camera Station 5 można oglądać cały strumień nadawany z kamery. Ruchy PTZ w podglądzie na żywo nie są widoczne ani nagrywane.

Uwaga

Nie można używać funkcji PTZ, jeśli w kamerze włączono kolejkowanie. Informacje kolejkowania oraz o włączaniu u wyłączaniu tej funkcji znajdują się w podręczniku użytkownika kamery.

Aby dodać prepozycję:

1. Wybierz kolejno opcje **Konfiguracja > Urządzenia > Prepozycje PTZ** i zaznacz kamerę na liście.
2. W kamerach z fizycznym mechanizmem PTZ użyj elementów sterowania PTZ, aby ustawić widok kamery w żądanym położeniu. W kamerach z cyfrowym PTZ używaj kółka myszy do przybliżania widoku oraz przeciągnięcia go w żądane położenie.
3. Kliknij przycisk **Dodaj** i nadaj nazwę nowemu predefiniowanemu ustawieniu.
4. Kliknij przycisk **OK**.

Aby usunąć prepozycję, zaznacz ją i kliknij przycisk **Remove (Usuń)**. Spowoduje to usunięcie prepozycji z aplikacji AXIS Camera Station 5 i z kamery.

## Zarządzanie urządzeniami

Na stronie zarządzania urządzeniami znajdują się narzędzia do administracji urządzeniami połączonymi z AXIS Camera Station 5 i ich konserwacji.

Wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**, a zostanie otwarta strona Manage Devices (Zarządzaj urządzeniami).

Jeżeli w sekcji *Ustawienia aktualizacji oprogramowania sprzętowego, on page 112* skonfigurowano automatyczne sprawdzanie dostępności nowych wersji oprogramowania sprzętowego, pojawienie się aktualizacji będzie powodowało wyświetlenie odpowiedniego łącza. Kliknięcie łącza rozpocznie proces uaktualniania oprogramowania sprzętowego. Patrz *Aktualizuj oprogramowanie sprzętowe*.


*Uaktualnianie wersji oprogramowania sprzętowego*

Jeżeli w sekcji *Aktualizuj AXIS Camera Station 5, on page 119* skonfigurowano automatyczne sprawdzanie dostępności nowych wersji oprogramowania, pojawienie się nowej wersji oprogramowania AXIS Camera Station 5 powoduje wyświetlenie łącza. Kliknij to łącze, aby zainstalować nową wersję oprogramowania AXIS Camera Station 5.


*Instalowanie nowej wersji AXIS Camera Station 5*

Zostanie wyświetlona lista urządzeń dodanych do AXIS Camera Station 5. Za pomocą pola **Type to search (Wpisz, aby wyszukać)** można odnaleźć urządzenia znajdujące się na liście. Aby ukryć lub wyświetlać kolumny, kliknij prawym przyciskiem myszy wiersz nagłówka, a następnie wybierz kolumny, które mają być wyświetlane. Przeciągając i upuszczając nagłówki, można zmienić kolejność wyświetlania kolumn.

Lista urządzeń zawiera następujące informacje:

- **Imię:** Nazwa urządzenia lub lista wszystkich nazw powiązanych kamer, jeśli urządzenie jest wideoenkoderem z wieloma podłączonymi kamerami lub kamerą sieciową z wieloma zdefiniowanymi obszarami obserwacji.
- **Adres MAC:** Adres MAC urządzenia.
- **Stan:** Status urządzenia.
  - **OK:** Standardowy stan ustanowionego połączenia z urządzeniem.
  - **Konserwacja:** Urządzenie jest w trakcie konserwacji i w związku z tym chwilowo niedostępne.
  - **Niedostępne:** Nie można nawiązać połączenia z urządzeniem.
  - **Niedostępne pod wybraną nazwą hosta:** Nie można nawiązać połączenia z urządzeniem przy użyciu jego nazwy hosta.
  - **Serwer jest niedostępny:** Nie można nawiązać połączenia z serwerem, do którego jest podłączone urządzenie.
  - **Wprowadź hasło:** Nie można nawiązać połączenia z urządzeniem, dopóki nie zostaną wprowadzone ważne poświadczenia. Należy kliknąć łącze i wpisać prawidłowe poświadczenia. Jeżeli urządzenie obsługuje połączenia szyfrowane, domyślnie hasło zostanie wysłane w postaci zaszyfrowanej.
  - **Ustaw hasło:** Konto i hasło użytkownika głównego nie zostały skonfigurowane lub urządzenie nadal korzysta z domyślnego hasła. Kliknij łącze, aby ustawić hasło użytkownika głównego.
    - Wpisz hasło lub kliknij przycisk **Wygeneruj**, aby automatycznie wygenerować hasło o maksymalnej długości dozwolonej przez urządzenie. Zalecamy wyświetlenie automatycznego wygenerowanego hasła i utworzenie jego kopii.
    - Zaznacz opcję używania tego hasła na wszystkich urządzeniach mających status `Set password` (Ustaw hasło).
    - Wybierz opcję **Enable HTTPS (Włącz HTTPS)**, aby włączyć protokół HTTPS, jeśli urządzenie je obsługuje.
  - **Typ hasła: niezaszyfrowane:** Nie można nawiązać połączenia z urządzeniem, ponieważ wcześniej łączono się z nim przy użyciu zaszyfrowanego hasła. Ze względów bezpieczeństwa aplikacja AXIS Camera Station 5 nie pozwala na stosowanie niezaszyfrowanych haseł w przypadku urządzeń, dla których wcześniej stosowano zaszyfrowane hasła. W przypadku urządzeń obsługujących szyfrowanie typ połączenia jest konfigurowany na stronie konfiguracji urządzenia.
  - **Błąd certyfikatu:** Wystąpił błąd z certyfikatem na urządzeniu.
  - **Certyfikat wkrótce wygaśnie:** Certyfikat na urządzeniu niedługo straci ważność.
  - **Certyfikat wygasł:** Certyfikat na urządzeniu stracił ważność.
  - **Niezaufany certyfikat HTTPS:** AXIS Camera Station 5 nie ufa certyfikatowi HTTPS dostępnemu na urządzeniu. Kliknij łącze, aby wystawić nowy certyfikat HTTPS.
  - **Niepowodzenie HTTP:** Nie można nawiązać połączenia z urządzeniem przy użyciu protokołu HTTP.
  - **Niepowodzenie HTTPS:** Nie można nawiązać połączenia z urządzeniem przy użyciu protokołu HTTPS.
  - **Połączenia HTTP i HTTPS się nie powiodły (polecenie ping lub połączenie UDP działa):** Nie można nawiązać połączenia z urządzeniem przy użyciu protokołu HTTP ani HTTPS. Urządzenie odpowiada na polecenia ping oraz komunikację przy użyciu protokołu User Datagram Protocol (UDP).
- **Adres:** Adres urządzenia. Kliknięcie łącza spowoduje przejście do strony konfiguracji urządzenia. Widać w nim adres IP lub nazwę hosta, w zależności od tego, której z tych informacji użyto przy dodawaniu urządzenia. Patrz *Karta Konfiguracja urządzenia, on page 66*.
- **Nazwa hosta:** Nazwa hosta urządzenia, jeśli jest dostępna. Kliknięcie łącza spowoduje przejście do strony konfiguracji urządzenia. Wyświetlana nazwa hosta jest w pełni kwalifikowaną nazwą domeny. Patrz *Karta Konfiguracja urządzenia, on page 66*.

- **Producent:** Producent urządzenia.
- **Model:** Model urządzenia.
- **Oprogramowanie sprzętowe:** Wersja oprogramowania sprzętowego aktualnie zainstalowanego na urządzeniu.
- **DHCP:** Jeśli urządzenie łączy się z serwerem za pośrednictwem protokołu DHCP.
- **HTTPS:** Status łączności przez HTTPS w urządzeniu. Informację tę można sprawdzić na stronie *Bezpieczeństwo, on page 64*.
- **IEEE 802.1X:** Status łączności przez IEEE 802.1X w urządzeniu. Informację tę można sprawdzić na stronie *Bezpieczeństwo, on page 64*.
- **Serwer:** Serwer AXIS Camera Station 5, z którym łączy się urządzenie.
- **Tags (Znaczniki):** (Ustawienie domyślnie ukryte) Znaczniki dodane do urządzenia.
- **UPnP Friendly Name (Przyjazna nazwa UPnP):** (Ustawienie domyślnie ukryte) Nazwa UPnP. Jest to nazwa opisowa używana w celu ułatwienia identyfikacji urządzenia.

Wobec urządzeń można wykonywać następujące czynności:

- Przypisywanie adresów IP do urządzeń. Patrz *Przypisywanie adresu IP*.
- Ustawianie haseł dostępu do urządzeń. Patrz *Zarządzanie użytkownikami*.
- Uaktualnianie oprogramowania sprzętowego urządzeń. Patrz *Aktualizuj oprogramowanie sprzętowe*.
- Ustawianie daty i godziny na urządzeniach. Patrz *Ustawianie daty i godziny*.
- Uruchom ponownie urządzenia.
- Przywracanie ustawień w celu zresetowania większości ustawień, w tym haseł, do fabrycznych wartości domyślnych. Nie są resetowane następujące ustawienia: aplikacje przesłane do kamery, protokół uruchamiania (DHCP lub statyczny), statyczny adres IP, domyślny router, maska podsieci, czas systemowy.

Uwaga

- Aby zapobiec nieuprawnionemu dostępowi, stanowczo zalecamy ustawienie hasła po przywróceniu urządzenia.
- Jeśli resetowane urządzenie korzysta z pamięci masowej w chmurze, przejdź do obszaru **Cloud storage (Pamięć masowa w chmurze)** na platformie My Systems i przed zresetowaniem urządzenia wyłącz dla niego pamięć masową w chmurze. Po zresetowaniu urządzenia uruchom ponownie usługę na serwerze AXIS Camera Station 5i włącz dla urządzenia pamięć masową w chmurze na platformie My Systems. Zobacz *Włączanie pamięci masowej w chmurze dla poszczególnych kamer*.
- Instalowanie aplikacji do kamery na urządzeniach. Patrz *Instalowanie aplikacji do kamery*.
- Ponowne wczytywanie urządzeń po zmianie ich ustawień na stronie konfiguracji.
- Konfigurowanie urządzeń. Patrz *Konfiguruj urządzenia*.
- Zarządzanie użytkownikami. Patrz *Zarządzanie użytkownikami*.
- Zarządzanie certyfikatami. Patrz *Bezpieczeństwo, on page 64*.
- Zbieranie danych z urządzeń. Patrz *Zbieranie danych dotyczących urządzeń*.
- Wybór między używaniem adresu IP lub nazwy hosta. Patrz *Połączenie, on page 65*.
- Oznaczanie urządzeń. Patrz *Tagi*.
- Wprowadź dane uwierzytelniające urządzenia. Kliknij prawym przyciskiem myszy, wybierz kolejno polecenia **Zaawansowane > Wprowadź dane uwierzytelniające urządzenia** i wprowadź hasło dostępu do urządzenia.
- Przejdź do karty konfiguracji urządzenia i skonfiguruj urządzenie. Patrz *Karta Konfiguracja urządzenia, on page 66*.

### Przypisywanie adresu IP

AXIS Camera Station 5 może przypisywać adresy IP do wielu urządzeń. Nowe adresy IP mogą być pobierane automatycznie z serwera DHCP lub przypisywane z puli adresów IP.

#### Przydzielanie adresów IP

1. Wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)** i zaznacz urządzenia, które chcesz skonfigurować.
2. Kliknij  lub kliknij prawym przyciskiem myszy i wybierz polecenie **Assign IP address (Przydziel adres IP)**.
3. Jeżeli niektórych urządzeń nie można skonfigurować, na przykład wskutek braku dostępu do nich, zostanie wyświetlone okno dialogowe Nieprawidłowe urządzenia. Kliknij przycisk **Kontynuuj**, aby pominąć urządzenia, których nie można skonfigurować.
4. Jeżeli wybrano jedno urządzenie w celu przypisania adresu IP, kliknij przycisk **Zaawansowane**, co spowoduje otwarcie strony Przypisz adres IP.
5. Zaznacz opcję **Uzyskaj adresy IP automatycznie (DHCP)**, aby adresy IP były pobierane automatycznie z serwera DHCP.
6. Zaznacz opcję **Przypisz następujący zakres adresów IP**, a następnie określ zakres adresów IP, maskę podsieci i domyślny router.
   Aby określić zakres adresów IP:
   - Używaj symboli wieloznacznych. Na przykład: 192.168.0.* lub 10.*.1.*
   - Wpisz pierwszy i ostatni adres IP, rozdzielając je myślnikiem. Na przykład: 192.168.0.10-192.168.0.20 (ten zakres adresów można skrócić do 192.168.0.10-20) czy 10.10-30.1.101
   - Łącz symbole wieloznaczne i zakres. Na przykład: 10.10-30.1.*
   - Do oddzielania zakresów używaj przecinka. Na przykład: 192.168.0.*,192.168.1.10-192.168.1.20

Uwaga

Przydzielanie zakresów adresów IP wymaga połączenia urządzeń z tym samym serwerem AXIS Camera Station 5.

7. Kliknij przycisk **Next (Dalej)**.
8. Obejrzyj obecne i nowe adresy IP. Aby zmienić adres IP urządzenia, zaznacz urządzenie i kliknij przycisk **Edytuj adres IP**.
   - Obecny adres IP, maska podsieci i domyślny router są wyświetlane w sekcji Bieżący adres IP.
   - Zmodyfikuj wartości w sekcji Nowy adres IP i kliknij przycisk **OK**.
9. Po wpisaniu poprawnych nowych adresów IP kliknij przycisk **Zakończ**.

### Konfiguruj urządzenia

Niektóre ustawienia można skonfigurować na wielu urządzeniach jednocześnie, kopiując ustawienia lub stosując plik konfiguracji.

Uwaga

Aby skonfigurować wszystkie ustawienia na jednym urządzeniu, przejdź do jego strony konfiguracyjnej. Patrz *Karta Konfiguracja urządzenia, on page 66*.

- Informacje na temat konfigurowania urządzeń: *Metody konfigurowania*.
- Informacje na temat tworzenia pliku konfiguracyjnego: *Utwórz plik konfiguracyjny*.
- Informacje na temat ustawień, które można kopiować: *Ustawienia konfiguracyjne*.

### Metody konfigurowania

Istnieją różne metody konfigurowania urządzeń. Narzędzie zarządzania urządzeniami AXIS Device Manager próbuje konfigurować wszystkie urządzenia odpowiednio do ustawień objętych każdą metodą. Patrz *Konfiguruj urządzenia*.

#### Używanie konfiguracji wybranego urządzenia

Uwaga

Ta metoda jest dostępna tylko przy konfigurowaniu jednego urządzenia i polega na wykorzystaniu wybranych lub wszystkich istniejących ustawień.

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij jedno urządzenie prawym przyciskiem myszy i wybierz kolejno opcje **Configure Devices > Configure (Konfiguruj urządzenia > Konfiguruj)**.
3. Zaznacz ustawienia, które chcesz zastosować. Patrz *Ustawienia konfiguracyjne, on page 59*.
4. Kliknij przycisk **Dalej**, aby zweryfikować ustawienia przewidziane do zastosowania.
5. Kliknij przycisk **Zakończ**, aby zastosować ustawienia do urządzenia.

#### Kopiowanie konfiguracji z innego urządzenia

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno opcje **Configure Devices > Configure (Konfiguruj urządzenia > Konfiguruj)**. Można wybierać urządzenia o różnych nazwach modelowych i oprogramowaniu sprzętowym.
3. Kliknij przycisk **Urządzenie**, aby wyświetlić urządzenia z konfiguracjami możliwymi do wykorzystania na innych urządzeniach.
4. Zaznacz urządzenie, z którego chcesz skopiować ustawienia, i kliknij przycisk **OK**.
5. Zaznacz ustawienia, które chcesz zastosować. Patrz *Ustawienia konfiguracyjne, on page 59*.
6. Kliknij przycisk **Dalej**, aby zweryfikować ustawienia przewidziane do zastosowania.
7. Kliknij przycisk **Zakończ**, aby zastosować ustawienia do urządzeń.

#### Używanie pliku konfiguracyjnego

Plik konfiguracyjny zawiera ustawienia z jednego urządzenia. Można go użyć do jednoczesnego skonfigurowania wielu urządzeń i ponownego skonfigurowania urządzenia, na przykład w razie przywrócenia ustawień fabrycznych na urządzeniu. Plik konfiguracyjny utworzony na podstawie urządzenia można zastosować do urządzeń o różnych nazwach modelowych i wersjach oprogramowania sprzętowego, nawet jeśli niektóre ustawienia nie występują na wszystkich urządzeniach.

Jeżeli niektóre ustawienia nie istnieją lub nie można ich zastosować, stan zadania będzie wyświetlany jako Error (Błąd) na karcie Tasks (Zadania) u dołu okna klienta AXIS Camera Station 5. Kliknij zadanie prawym przyciskiem myszy i wybierz polecenie Pokaż, a zostaną wyświetlone informacje o ustawieniach, których nie można było zastosować.

Uwaga

Tej metody powinni używać tylko doświadczeni użytkownicy.

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno opcje **Configure Devices > Configure (Konfiguruj urządzenia > Konfiguruj)**.
3. Kliknij przycisk **Plik konfiguracyjny**, aby przejść do pliku konfiguracyjnego. Informacje na temat tworzenia pliku konfiguracyjnego: *Utwórz plik konfiguracyjny, on page 59*.
4. Przejdź do pliku .cfg i kliknij przycisk **Otwórz**.
5. Kliknij przycisk **Dalej**, aby zweryfikować ustawienia przewidziane do zastosowania.
6. Kliknij przycisk **Zakończ**, aby zastosować ustawienia do urządzeń.

### Utwórz plik konfiguracyjny

Plik konfiguracyjny zawiera ustawienia z jednego urządzenia. Ustawienia te można zastosować do innych urządzeń. Aby uzyskać więcej informacji o używaniu pliku konfiguracyjnego, patrz *Metody konfigurowania*.

Wyświetlane ustawienia to ustawienia urządzenia, do których można uzyskać dostęp za pomocą narzędzia zarządzania urządzeniami AXIS Device Manager. Aby odszukać konkretne ustawienie, skorzystaj z pola **Wpisz, aby wyszukać**.

Aby utworzyć plik konfiguracyjny:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Zaznacz urządzenie, na bazie którego chcesz utworzyć plik konfiguracyjny.
3. Kliknij prawym przyciskiem myszy i wybierz kolejno opcje **Konfiguruj urządzenia > Utwórz plik konfiguracyjny**.
4. Zaznacz ustawienia, które chcesz dodać do pliku, i w razie potrzeby zmień ich wartości. Patrz *Ustawienia konfiguracyjne*.
5. Kliknij przycisk **Dalej**, aby sprawdzić ustawienia.
6. Kliknij przycisk **Zakończ**, aby utworzyć plik konfiguracyjny.
7. Kliknij przycisk **Zapisz**, aby zapisać ustawienia w pliku .cfg.

### Ustawienia konfiguracyjne

Podczas konfigurowania urządzeń można ustawiać parametry, reguły akcji i dodatkowe ustawienia urządzeń.

#### Parametry

Parametry to wewnętrzne parametry urządzeń, które służą do kontrolowania zachowania urządzeń. Ogólne informacje o parametrach znajdują się w Podręczniku użytkownika produktu w witrynie *www.axis.com*.

Uwaga

- Parametry powinny modyfikować tylko doświadczeni użytkownicy.
- Nie wszystkie parametry urządzeń są dostępne w narzędziu zarządzania urządzeniami AXIS Device Manager.

W niektórych polach tekstowych można wstawiać zmienne. Zmienne zostaną zastąpione tekstem przed ich zastosowaniem do urządzenia. Aby wstawić zmienną, kliknij pole tekstowe prawym przyciskiem myszy i wybierz polecenie:

- **Wstaw numer seryjny urządzenia:** Ta zmienna zostanie zastąpiona numerem seryjnym urządzenia, do którego zastosowano plik konfiguracyjny.
- **Wprowadź nazwę urządzenia:** Ta zmienna zostanie zastąpiona nazwą urządzenia używaną podczas stosowania pliku konfiguracyjnego. Nazwę urządzenia można znaleźć w kolumnie Nazwa na stronie Zarządzanie urządzeniami. Aby zmienić nazwę urządzenia, przejdź do strony Kamery lub Inne urządzenia.
- **Wprowadź nazwę serwera:** Ta zmienna zostanie zastąpiona nazwą serwera używaną podczas stosowania pliku konfiguracyjnego. Nazwę serwera można znaleźć w kolumnie Serwer na stronie Zarządzanie urządzeniami. Aby zmienić nazwę serwera, przejdź do aplikacji AXIS Camera Station 5 Service Control.
- **Wprowadź strefę czasową serwera:** Ta zmienna zostanie zastąpiona strefą czasową POSIX serwera używaną podczas stosowania pliku konfiguracyjnego. Tej zmiennej można używać w połączeniu z parametrem strefy czasowej POSIX w celu ustawienia prawidłowej strefy czasowej dla wszystkich urządzeń w sieci, które używają serwerów zlokalizowanych w różnych strefach czasowych.

#### Reguły akcji

Reguły akcji można kopiować między urządzeniami. Reguły akcji powinni modyfikować tylko doświadczeni użytkownicy. Ogólne informacje o regułach akcji: *Reguły akcji*.

**Ustawienia dodatkowe**

- **Profile strumieni:** Profil strumienia to wstępnie zaprogramowany profil konfiguracyjny podglądu na żywo zawierający ustawienia kodowania wideo, nieruchomego obrazu i dźwięku. Profile strumieni można kopiować między urządzeniami.
- **Okna detekcji ruchu:** Okna detekcji ruchu służą do definiowania konkretnych obszarów wewnątrz pola widzenia kamery. Zazwyczaj alarmy są generowane po każdym stwierdzeniu ruchu (lub zatrzymaniu się) obiektu wewnątrz wyznaczonych obszarów. Okna detekcji ruchu można kopiować między urządzeniami.

**Zarządzanie użytkownikami**

Wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**. Zostanie wyświetlona strona Manage Devices (Zarządzaj urządzeniami), na której można zarządzać użytkownikami urządzeń.

Po ustawieniu hasła lub usunięciu użytkowników z urządzeń użytkownicy nieobecni na wszystkich urządzeniach będą oznaczeni symbolem . Każdy użytkownik występujący na różnych urządzeniach pod różnymi rolami będzie wyświetlany tylko raz.

Uwaga

Konta są powiązane z konkretnymi urządzeniami, a nie kontami użytkowników AXIS Camera Station 5.

**Ustaw hasło**

Uwaga

- Urządzenia z oprogramowaniem sprzętowym w wersji 5.20 i nowszych obsługują hasła 64-znakowe. Urządzenia ze starszymi wersjami oprogramowania sprzętowego obsługują hasła 8-znakowe. Zalecamy, aby na urządzeniach ze starszymi wersjami oprogramowania sprzętowego hasła ustawiać osobno.
- W przypadku ustawiania hasła na wielu urządzeniach obsługujących hasła o różnych długościach hasło nie może przekroczyć najkrótszej obsługiwanej długości.
- Aby zapobiec nieuprawnionemu dostępowi i zwiększyć bezpieczeństwo, zalecamy zabezpieczenie hasłem wszystkich urządzeń dodanych do aplikacji AXIS Camera Station 5.

W hasłach można używać następujących znaków:

- litery A-Z, a-z
- cyfry 0-9
- spacja, przecinek (,), kropka (.), dwukropek (:), średnik (;)
- !, ", #, $, %, &, ', (, +, *, -, ), /, <, >, =, ?, [, \, ^, -, `, {, |, ~, @, ], }

Aby ustawić hasło dla użytkowników na urządzeniach:

1. Wybierz kolejno opcje **Configuration > Devices > Management > Manage devices (Konfiguracja > Urządzenia > Zarządzanie > Zarządzaj urządzeniami)**.
2. Zaznacz urządzenia i kliknij . Można również kliknąć urządzenia prawym przyciskiem myszy i wybrać kolejno opcje **User Management > Set password (Zarządzanie użytkownikami > Ustaw hasło)**.
3. Wybierz użytkownika.
4. Wpisz hasło lub kliknij przycisk **Generate (Wygeneruj)** i utwórz silne hasło.
5. Kliknij przycisk **OK**.

**Dodaj użytkownika**

Aby dodać użytkowników lokalnych lub Active Directory do AXIS Camera Station 5:

1. Wybierz kolejno opcje **Configuration > Devices > Management > Manage devices (Konfiguracja > Urządzenia > Zarządzanie > Zarządzaj urządzeniami)**.

2. Kliknij prawym przyciskiem myszy urządzenie i wybierz kolejno opcje **User Management > Add user (Zarządzanie użytkownikami > Dodaj użytkownika)**.
3. Wprowadź nazwę użytkownika i hasło, a następnie potwierdź hasło. Lista dozwolonych znaków znajduje się powyżej w sekcji „Ustawianie hasła".
4. W polu **Rola** z listy rozwijanej wybierz uprawnienia dostępu użytkownika:
   - **Administrator:** nieograniczony dostęp do urządzenia.
   - **Operator:** dostęp do strumienia wideo, zdarzeń i wszystkich ustawień oprócz opcji systemowych.
   - **Viewer (Dozorca):** dostęp do strumienia wideo.
5. Zaznacz opcję **Włącz kontrolę PTZ**, aby pozwolić użytkownikowi na obracanie, przechylanie i powiększanie/zmniejszanie w podglądzie na żywo.
6. Kliknij przycisk **OK**.

**Usuń użytkownika**

Aby usunąć użytkowników z urządzeń:

1. Wybierz kolejno opcje **Configuration > Devices > Management > Manage devices (Konfiguracja > Urządzenia > Zarządzanie > Zarządzaj urządzeniami)**.
2. Kliknij prawym przyciskiem myszy urządzenie i wybierz kolejno opcje **User Management > Remove user (Zarządzanie użytkownikami > Usuń użytkownika)**.
3. W polu **Użytkownik** z listy rozwijanej wybierz użytkownika, którego chcesz usunąć.
4. Kliknij przycisk **OK**.

**Wyświetlanie użytkowników**

Aby wyświetlić listę wszystkich użytkowników urządzeń wraz z posiadanymi uprawnieniami dostępu:

1. Wybierz kolejno opcje **Configuration > Devices > Management > Manage devices (Konfiguracja > Urządzenia > Zarządzanie > Zarządzaj urządzeniami)**.
2. Kliknij prawym przyciskiem myszy urządzenie i wybierz kolejno opcje **User Management > List users (Zarządzanie użytkownikami > Wyświetl użytkowników)**.
3. Za pomocą pola **Wpisz, aby wyszukać** odszukaj konkretnych użytkowników spośród figurujących na liście.

**Aktualizuj oprogramowanie sprzętowe**


Oprogramowanie sprzętowe określa funkcje dostępne w produkcie Axis. Instalowanie najnowszego oprogramowania sprzętowego daje pewność, iż urządzenie zawsze będzie miało najnowsze funkcje i ulepszenia.

Nowe oprogramowanie sprzętowe można pobrać za pomocą aplikacji AXIS Camera Station 5 lub zaimportować z pliku umieszczonego na dysku twardym lub karcie pamięci. Wersje oprogramowania sprzętowego dostępne do pobrania są wyświetlane z dopiskiem **(Download) (pobierz)** po numerze wersji. Wersje oprogramowania sprzętowego dostępne na lokalnym kliencie są wyświetlane z dopiskiem **(plik)** po numerze wersji.

Podczas uaktualniania oprogramowania sprzętowego można wybrać sposób przeprowadzenia procesu:

- **Standardowy:** Uaktualnianie do wybranej wersji oprogramowania sprzętowego i zachowanie istniejących wartości ustawień.

- **Ustawienia fabryczne:** Uaktualnianie do wybranej wersji oprogramowania sprzętowego i przywracanie domyślnych wartości fabrycznych we wszystkich ustawieniach.

Aby uaktualnić oprogramowanie sprzętowe:

1. Wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)** i zaznacz urządzenia, które chcesz skonfigurować.
2. Kliknij  lub kliknij prawym przyciskiem myszy i wybierz polecenie **Upgrade firmware (Aktualizuj oprogramowanie sprzętowe)**.
3. Jeżeli niektórych urządzeń nie można skonfigurować, na przykład wskutek braku dostępu do nich, zostanie wyświetlone okno dialogowe Nieprawidłowe urządzenia. Kliknij przycisk **Kontynuuj**, aby pominąć urządzenia, których nie można skonfigurować.
4. W trakcie uaktualniania oprogramowania sprzętowego urządzenie jest niedostępne. Kliknij przycisk **Tak**, aby kontynuować. Jeśli komunikat jest Ci znany i nie chcesz, aby się więcej pojawiał, zaznacz opcję **Nie wyświetlaj ponownie tego okna dialogowego** i kliknij przycisk **Tak**.
5. Okno dialogowe Aktualizuj oprogramowanie sprzętowe zawiera informacje takie jak model urządzenia, liczba urządzeń każdego modelu, istniejąca wersja oprogramowania sprzętowego, dostępne wersje, do których można uaktualnić, oraz rodzaj uaktualnienia. Domyślnie urządzenia wymienione na liście są wstępnie zaznaczane, gdy pojawią się nowe wersje oprogramowania sprzętowego do pobrania. Najnowsze oprogramowanie jest wstępnie wybrane dla każdego urządzenia.
   5.1. Aby zaktualizować listę wersji oprogramowania sprzętowego możliwych do pobrania, kliknij przycisk **Sprawdź dostępność aktualizacji**. Aby wyszukać jeden lub więcej plików oprogramowania sprzętowego zapisanych na lokalnym kliencie, kliknij przycisk **Przeglądaj**.
   5.2. Zaznacz urządzenia, wersje oprogramowania sprzętowego, które chcesz uaktualnić, i typ aktualizacji.
   5.3. Kliknij przycisk **OK**, aby rozpocząć aktualizowanie urządzeń figurujących na liście.

Uwaga

Domyślnie aktualizacje oprogramowania sprzętowego odbywają się na wszystkich zaznaczonych urządzeniach równocześnie. Kolejność uaktualniania można zmienić. Patrz *Ustawienia aktualizacji oprogramowania sprzętowego*.

**Ustawianie daty i godziny**

Ustawienia daty i godziny urządzeń Axis mogą być zsynchronizowane z czasem serwera, serwerem NTP lub ustawiane ręcznie.

Aby ustawić datę i czas na urządzeniach:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Zaznacz urządzenie i kliknij przycisk  lub kliknij prawym przyciskiem myszy i wybierz polecenie **Set date and time (Ustaw datę i godzinę)**.
3. Pole **Czas urządzenia** pokazuje aktualną datę i godzinę skonfigurowane dla używanego urządzenia Axis. W przypadku zaznaczenia kilku urządzeń opcja **Czas urządzenia** jest niedostępna.
4. Wybieranie strefy czasowej.
   – Z listy rozwijanej **Strefa czasowa** wybierz strefę czasową, której chcesz używać dla produktu Axis.
   – Jeżeli urządzenie jest użytkowane w miejscu, w którym stosuje się zmiany czasu na letni i zimowy, zaznacz opcję **Automatycznie dostosuj do zmiany czasu letniego**.

Uwaga

Strefę czasową można ustawić po wybraniu trybu wyświetlania czasu **Synchronizuj z serwerem NTP** lub **Ustaw ręcznie**.

5. W sekcji Tryb wyświetlania czasu:

- Kliknij opcję **Synchronize with server computer time (Synchronizuj z czasem serwera)**, aby zsynchronizować datę i godzinę produktu z zegarem serwera, tzn. z komputerem, na którym jest zainstalowany serwer AXIS Camera Station 5.
- Kliknij opcję **Synchronize with NTP server (Synchronizuj z serwerem NTP)**, aby data i godzina urządzenia były synchronizowane z serwerem NTP. W podanym polu wpisz adres IP, adres DNS lub nazwę hosta serwera NTP.
- Zaznacz opcję **Ustaw ręcznie**, aby ręcznie ustawić datę i godzinę.

6. Kliknij przycisk **OK**.


*Ustawianie daty i godziny*

**Instalowanie aplikacji do kamery**

Aplikacja do kamery to oprogramowanie, które można wczytywać i instalować w produktach Axis do sieciowego dozoru wizyjnego. Aplikacje poszerzają funkcjonalność urządzenia, na przykład o wykrywanie, rozpoznawanie, śledzenie i zliczanie.

Niektóre aplikacje można instalować bezpośrednio z AXIS Camera Station 5. Inne aplikacje należy najpierw pobrać ze strony *www.axis.com/global/en/products/analytics-and-other-applications* albo z witryny aplikacji udostępnionej przez jej producenta.

Aplikacje można instalować na urządzeniach obsługujących rozwiązanie AXIS Camera Application Platform. Niektóre aplikacje wymagają również określonej wersji oprogramowania sprzętowego lub modelu kamery.

Jeżeli aplikacja wymaga licencji, plik klucza licencyjnego można zainstalować równolegle z aplikacją albo później, z poziomu strony konfiguracyjnej urządzenia.

W celu uzyskania klucza licencyjnego należy przejść do strony *www.axis.com/se/sv/products/camera-applications/license-key-registration#/registration* i zarejestrować tam kod licencyjny dołączony do aplikacji.

Jeżeli nie udaje się zainstalować aplikacji, przejdź do witryny *www.axis.com* i sprawdź, czy model urządzenia oraz wersja oprogramowania sprzętowego obsługują rozwiązanie AXIS Camera Application Platform.

Dostępne aplikacje do kamery:

**AXIS Video Motion Detection 4 –** Aplikacja, która wykrywa poruszające się obiekty w obszarze zainteresowania. Nie wymaga żadnej licencji. Można ją instalować w kamerach z oprogramowaniem sprzętowym w wersji 6.50. Warto również sprawdzić w informacjach o wersji oprogramowania sprzętowego produktu, czy obsługuje on oprogramowanie do wizyjnej detekcji ruchu Video Motion Detection w wersji 4.

**AXIS Video Motion Detection 2 –** Aplikacja, która wykrywa poruszające się obiekty w obszarze zainteresowania. Nie wymaga żadnej licencji. Można ją instalować w kamerach z oprogramowaniem sprzętowym w wersji 5.60.

**AXIS Video Content Stream –** Aplikacja, która umożliwia kamerom Axis wysyłanie danych funkcji śledzenia ruchomych obiektów do AXIS Camera Station 5. Można ją instalować w kamerach z oprogramowaniem sprzętowym w wersjach od 5.50 do 9.59. Aplikacja AXIS Video Content Stream może być używana tylko w połączeniu z AXIS Camera Station 5.

**Inne aplikacje –** Wszelkie inne aplikacje, które użytkownik chce zainstalować. Przed rozpoczęciem instalacji należy pobrać aplikację do lokalnego komputera.

Aby instalować aplikacje do kamery:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Zaznacz kamery, na których chcesz zainstalować aplikacje. Kliknij lub kliknij prawym przyciskiem myszy i wybierz polecenie **Install camera application (Zainstaluj aplikację do kamery)**.
3. Zaznacz aplikację do kamery, którą chcesz zainstalować w kamerach. Jeżeli chcesz zainstalować inne aplikacje, kliknij przycisk **Browse (Przeglądaj)** i przejdź do lokalnego pliku aplikacji. Kliknij przycisk **Next (Dalej)**.
4. Jeżeli aplikacja jest już zainstalowana, można wybrać opcję **Zezwalaj na nadpisanie aplikacji** i przeinstalować aplikację lub opcję **Zezwalaj na obniżenie wersji aplikacji** i zainstalować poprzednią wersję aplikacji.

Uwaga

Obniżenie wersji lub nadpisanie aplikacji spowoduje zresetowanie ustawień aplikacji na urządzeniu.

5. Jeżeli aplikacja wymaga licencji, zostanie wyświetlone okno dialogowe Install licenses (Zainstaluj licencje).
   5.1. Kliknij przycisk **Yes (Tak)**, aby rozpocząć instalowanie licencji, a następnie kliknij przycisk **Next (Dalej)**.
   5.2. Kliknij przycisk **Browse (Przeglądaj)**, przejdź do pliku licencji i kliknij przycisk **Next (Dalej)**.

Uwaga

Licencje nie są potrzebne do zainstalowania aplikacji AXIS Video Motion Detection 2, AXIS Video Motion Detection 4 ani AXIS Video Content Stream.

6. Przejrzyj informacje i kliknij przycisk **Finish (Zakończ)**. Status kamery zmieni się z `OK` na `Maintenance` (Konserwacja), a po zakończeniu instalacji z powrotem na `OK`.

### Bezpieczeństwo

Gdy włączysz HTTPS lub IEE 802.1X, urząd certyfikacji (certificate authority, CA) AXIS Camera Station 5 automatycznie podpisuje oraz dystrybuuje certyfikaty klientów i serwerów dla urządzeń. CA ignoruje wstępnie zainstalowane certyfikaty. Informacje na temat konfigurowania certyfikatów: *Certyfikaty, on page 131*.

#### Zarządzanie certyfikatami HTTPS i IEEE 802.1X

Uwaga

Przed włączeniem protokołu IEEE 802.1X upewnij się, że czas na urządzeniach Axis jest zsynchronizowany w AXIS Camera Station 5.

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij urządzenia prawym przyciskiem myszy:
   - Wybierz kolejno opcje **Zabezpieczenia > HTTPS > Włącz/Aktualizuj**, aby włączyć obsługę protokołu HTTPS lub zaktualizować jego ustawienia na urządzeniu.
   - Wybierz kolejno opcje **Zabezpieczenia > IEEE 802.1X > Włącz/Aktualizuj**, aby włączyć obsługę protokołu IEEE 802.1X lub zaktualizować jego ustawienia na urządzeniu.
   - Wybierz kolejno opcje **Security > HTTPS > Disable (Zabezpieczenia > HTTPS > Wyłącz)**, aby wyłączyć obsługę protokołu HTTPS na urządzeniu.
   - Wybierz kolejno opcje **Security > IEEE 802.1X > Disable (Zabezpieczenia > IEEE 802.1X > Wyłącz)**, aby wyłączyć obsługę protokołu IEEE 802.1X na urządzeniach.
   - Wybierz **Certificates... (Certyfikaty...)**, aby uzyskać podgląd, usunąć certyfikaty lub zobaczyć szczegółowe informacje o konkretnym certyfikacie.

Uwaga

Gdy ten sam certyfikat zostanie zainstalowany na kilku urządzeniach, będzie wyświetlany tylko jako jeden element. Usunięcie certyfikatu spowoduje wykasowanie go ze wszystkich urządzeń, na których jest zainstalowany.

#### Status protokołów HTTPS i IEEE 802.1X

Na stronie Zarządzanie urządzeniami jest wyświetlany status protokołów HTTPS i IEEE 802.1X.

| | Status | Opis |
|---|---|---|
| HTTPS | Wł. | AXIS Camera Station 5 używa protokołu HTTPS do łączenia się z urządzeniem. |
| | Wył. | AXIS Camera Station 5 używa protokołu HTTP do łączenia się z urządzeniem. |
| | Nieznany | Urządzenie jest nieosiągalne. |
| | Nieobsługiwane oprogramowanie układowe | Protokół HTTPS nie jest obsługiwany, ponieważ oprogramowanie sprzętowe jest za stare. |
| | Nieobsługiwane urządzenie | Protokół HTTPS nie jest obsługiwany na tym modelu urządzenia. |
| IEEE 802.1X | Włączone | Obsługa protokołu IEEE 802.1X jest aktywna w urządzeniu. |
| | Wyłączone | Obsługa protokołu IEEE 802.1X nie jest aktywna, ale można ją w każdej chwili włączyć na urządzeniu. |
| | Nieobsługiwane oprogramowanie układowe | Protokół IEEE 802.1X nie jest obsługiwany, ponieważ oprogramowanie sprzętowe jest za stare. |
| | Nieobsługiwane urządzenie | Protokół IEEE 802.1X nie jest obsługiwany na tym modelu urządzenia. |

**Zbieranie danych dotyczących urządzeń**

Ta opcja jest zazwyczaj używana do rozwiązywania problemów. Za jej pomocą można wygenerować plik .zip zawierający raport o gromadzeniu danych z określonej lokalizacji na urządzeniach.

Aby zebrać dane z urządzeń:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij urządzenie prawym przyciskiem myszy i wybierz polecenie **Zbierz dane urządzenia**.
3. W sekcji Źródła danych w wybranych urządzeniach:
   – Kliknij opcję **Prepozycja** i wybierz z listy rozwijanej żądane często używane polecenie.

   Uwaga

   Niektóre predefiniowane ustawienia nie działają na wszystkich urządzeniach. Na przykład opcja Stan PTZ nie działa na urządzeniach audio.

   – Kliknij przycisk **Niestandardowe** i podaj ścieżkę URL do źródła na wybranych serwerach, z którego są zbierane dane.
4. W sekcji Zapisz jako podaj nazwę pliku i lokalizację folderu dla pliku .zip mającego zawierać zebrane dane.
5. Zaznacz opcję **Automatycznie otwórz folder po przygotowaniu**, aby po zakończeniu zbierania danych wskazany folder został otwarty.
6. Kliknij przycisk **OK**.

**Połączenie**

Aby komunikować się z urządzeniami przy użyciu adresu IP lub nazwy hosta:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Zaznacz urządzenia, kliknij prawym przyciskiem myszy i wybierz polecenie **Połączenie**.

- Aby się łączyć z urządzeniami przy użyciu adresu IP, wybierz polecenie **Użyj adresu IP**.
- Aby się łączyć się z urządzeniami przy użyciu nazwy hosta, wybierz polecenie **Użyj nazwy hosta**.

**Tagi**

Znaczniki służą do sortowania urządzeń na stronie Zarządzanie urządzeniami. Jedno urządzenie może mieć wiele znaczników.

Urządzenia mogą być na przykład tagowane według kryterium modelu lub lokalizacji. Na przykład znakowanie urządzeń według modelu kamery pozwala szybko odnaleźć wszystkie kamery o tym modelu i zaktualizować na nich oprogramowanie.

Aby oznakować urządzenie:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij urządzenie prawym przyciskiem myszy i wybierz polecenie **Oznacz urządzenia**.
3. Zaznacz opcję **Użyj istniejącego znacznika** i wybierz znacznik lub opcję **Utwórz nowy znacznik** i nadaj nazwę nowemu znacznikowi.
4. Kliknij przycisk **OK**.

Aby usunąć znacznik z urządzenia:

1. Wybierz kolejno **Configuration (Konfiguracja) > Devices (Urządzenia) > Management (Zarządzanie)** i w prawym górnym rogu kliknij  .
2. W folderze Znaczniki wybierz znacznik. Zostaną wyświetlone wszystkie urządzenia skojarzone z tym znacznikiem.
3. Zaznacz urządzenia. Kliknij prawym przyciskiem myszy i wybierz polecenie **Usuń oznaczenie urządzeń**.
4. Kliknij przycisk **OK**.

Aby zarządzać znacznikami:

1. Wybierz kolejno **Configuration (Konfiguracja) > Devices (Urządzenia) > Management (Zarządzanie)** i w prawym górnym rogu kliknij  .
2. Na stronie Znaczniki urządzenia:
   - Kliknij prawym przyciskiem myszy pozycję **Znaczniki** i wybierz polecenie **Nowy znacznik**, aby utworzyć znacznik.
   - Kliknij znacznik prawym przyciskiem myszy, wybierz polecenie **Zmień nazwę znacznika** i wprowadź nową nazwę, która ma być stosowana do znacznika.
   - Kliknij znacznik prawym przyciskiem myszy i wybierz polecenie **Usuń**, aby usunąć znacznik.
   - Kliknij  , aby przypiąć stronę Device tags (Znaczniki urządzenia).
   - Kliknij znacznik, aby wyświetlić wszystkie powiązane z nim urządzenia, lub kliknij przycisk All devices (Wszystkie urządzenia), aby wyświetlić wszystkie urządzenia połączone z aplikacją AXIS Camera Station 5.
   - Kliknij przycisk **Warnings/Errors (Ostrzeżenia/błędy)**, a zostaną wyświetlone urządzenia wymagające uwagi, na przykład takie, do których nie można uzyskać dostępu.

**Karta Konfiguracja urządzenia**

Aby skonfigurować wszystkie ustawienia na jednym urządzeniu:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Kliknij adres lub nazwę hosta urządzenia, aby przejść do karty jego konfiguracji.
3. Zmień ustawienia. Informacje o konfigurowaniu urządzenia znajdują się w jego instrukcji obsługi.

4. Zamknij kartę. Ustawienia urządzenia zostaną wczytane ponownie, co zagwarantuje zaimplementowanie zmian w aplikacji AXIS Camera Station 5.

**Ograniczenia**

- Automatyczne uwierzytelnianie urządzeń innych producentów nie jest obsługiwane.
- Axis nie jest w stanie zagwarantować ogólnego wsparcia technicznego dla urządzeń innych producentów.
- Otwarcie karty Konfiguracja urządzenia przy aktywnych strumieniach wideo powoduje wzrost obciążenia zasobów komputerowych i może spowolnić działanie serwera.

## Zewnętrzne źródła danych

Zewnętrzne źródło danych to system lub źródło danych generujące dane, na podstawie których można wyśledzić okoliczności towarzyszące każdemu zdarzeniu. Patrz *Wyszukiwanie danych, on page 37*.

Wybierz kolejno opcje **Konfiguracja > Urządzenia > Zewnętrzne źródła danych**. Zostanie wyświetlona lista zewnętrznych źródeł danych. Kliknięcie nagłówka kolumny umożliwi posortowanie zawartości.

| Element | Opis |
|---|---|
| Nazwa | Nazwa zewnętrznego źródła danych. |
| Klucz źródłowy | Unikatowy identyfikator zewnętrznego źródła danych. |
| Wyświetl | Widok, z którym jest powiązane zewnętrzne źródło danych. |
| Serwer | Serwer, z którym łączy się zewnętrzne źródło danych. Widoczna tylko w przypadku połączenia z wieloma serwerami. |

Zewnętrzne źródło danych jest dodawane automatycznie, gdy:

- Zostaną utworzone drzwi w obszarze **Konfiguracja > Kontrola dostępu > Drzwi i strefy**. Kompletny proces sposobu konfigurowania sieciowego kontrolera drzwiowego Axis w oprogramowaniu AXIS Camera Station 5 opisano w temacie *Konfigurowanie sieciowego kontrolera drzwiowego Axis*.
- Urządzenie, na którym skonfigurowano aplikację AXIS License Plate Verifier, odbierze pierwsze zdarzenie. Kompletny proces konfigurowania aplikacji AXIS License Plate Verifier w ramach aplikacji AXIS Camera Station 5 opisano w temacie *Konfigurowanie aplikacji AXIS License Plate Verifier*.

Jeżeli dla zewnętrznego źródła danych skonfigurowano widok, dane generowane ze źródła danych będą automatycznie dodawane do zakładek na osi czasu widoku na karcie Wyszukiwanie danych. Aby połączyć źródło danych z widokiem:

1. Wybierz kolejno opcje **Configuration > Devices > External data sources (Konfiguracja > Urządzenia > Zewnętrzne źródła danych)**.
2. Zaznacz zewnętrzne źródło danych i kliknij polecenie **Edit (Edytuj)**.
3. Wybierz widok z listy rozwijanej **Widok**.
4. Kliknij **OK**.

## Synchronizacja czasu

Wybierz kolejno opcje **Configuration > Devices > Time synchronization (Konfiguracja > Urządzenia > Synchronizacja czasu)**, a zostanie otwarta strona Synchronizacja czasu.

Zostanie wyświetlona lista urządzeń dodanych do AXIS Camera Station 5. Kliknij prawym przyciskiem myszy wiersz nagłówka i wskaż, które kolumny mają być wyświetlane. Przeciągając i upuszczając nagłówki, można zmienić kolejność wyświetlania kolumn.

Lista urządzeń zawiera następujące informacje:

- **Imię:** Nazwa urządzenia lub lista wszystkich nazw powiązanych kamer, jeśli urządzenie jest wideoenkoderem z wieloma podłączonymi kamerami lub kamerą sieciową z wieloma zdefiniowanymi obszarami obserwacji.
- **Adres:** Adres urządzenia. Kliknięcie łącza spowoduje przejście do strony konfiguracji urządzenia. Widać w nim adres IP lub nazwę hosta, w zależności od tego, której z tych informacji użyto przy dodawaniu urządzenia. Patrz *Karta Konfiguracja urządzenia, on page 66*.
- **Adres MAC:** Adres MAC urządzenia.
- **Model:** Model urządzenia.
- **Włączony:** Pokazuje, czy funkcja synchronizacji czasu jest włączona.
- **Źródło NTP:** Źródło NTP skonfigurowane dla urządzenia.
  - **Static (Statyczna):** Serwery NTP dla urządzenia konfiguruje się ręcznie w ustawieniach **Podstawowy serwer NTP** i **Dodatkowy serwer NTP**.
  - **DHCP:** Urządzenie otrzymuje funkcjonalność serwera NTP dynamicznie z sieci. Po zaznaczeniu opcji **DHCP** ustawienia **Podstawowy serwer NTP** i **Dodatkowy serwer NTP** są niedostępne.
- **Podstawowy serwer NTP:** Główny serwer NTP skonfigurowany dla urządzenia. Ustawienie jest dostępne tylko po zaznaczeniu opcji **Statyczna**.
- **Dodatkowy serwer NTP:** Pomocniczy serwer NTP skonfigurowany dla urządzenia. Ustawienie jest dostępne tylko dla urządzeń Axis obsługujących dodatkowe serwery NTP i pod warunkiem zaznaczenia opcji **Statyczna**.
- **Przesunięcie czasu serwera:** Różnica czasu pomiędzy urządzeniem a serwerem.
- **Godzina UTC:** Godzina według uniwersalnego czasu koordynowanego w urządzeniu.
- **Zsynchronizowano:** Pokazuje, czy ustawienia synchronizacji czasu zostały faktycznie zastosowane. To ustawienie jest dostępna tylko w urządzeniach z oprogramowaniem sprzętowym w wersji 9.1 lub nowszej.
- **Czas do następnej synchronizacji:** Czas pozostały do następnej sesji synchronizacji.

Usługa Czas systemu Windows (W32Time) wykorzystuje sieciowy protokół synchronizacji czasu (Network Time Protocol, NTP) do synchronizowania daty i godziny z serwerem AXIS Camera Station 5. Są wyświetlane następujące informacje:

- **Serwer:** Serwer AXIS Camera Station 5, na którym działa usługa Czas systemu Windows.
- **Stan:** Status usługi Czas systemu Windows. `Running` (Uruchomiono) albo `Stopped` (Zatrzymano).
- **Serwer NTP:** Serwer NTP skonfigurowany dla usługi Czas systemu Windows.

**Konfigurowanie synchronizacji czasu**

1. Wybierz kolejno opcje **Konfiguracja > Urządzenia > Synchronizacja czasu**.
2. Zaznacz swoje urządzenia i wybierz opcję **Włącz synchronizację czasu**.
3. Wybierz źródło NTP **Statyczna** lub **DHCP**.
4. Jeżeli zaznaczono opcję **Statyczna**, skonfiguruj podstawowy i dodatkowy serwer DNS.
5. Kliknij przycisk **Apply (Zastosuj)**.

| | |
|---|---|
| **Send alarm when the time difference between server and device is larger than 2 seconds (Wyślij alarm, gdy różnica czasu między serwerem a urządzeniem przekroczy 2 sekundy)** | Wybierz tę opcję, aby otrzymać alarm, jeśli różnica czasu między serwerem a urządzeniem przekroczy 2 sekundy. |

## Konfigurowanie pamięci masowej

Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**, aby otworzyć stronę Zarządzaj pamięcią masową. Na stronie Manage storage (Zarządzaj pamięcią masową) znajduje się omówienie lokalnej i sieciowej pamięci masowej, które są dostępne w AXIS Camera Station 5.

| Lista | |
|---|---|
| **Lokalizacja** | Ścieżka i nazwa pamięci masowej. |
| **Przydzielone** | Maksymalna ilość pamięci masowej przydzielona na nagrania. |
| **Wykorzystywana** | Ilość pamięci masowej obecnie wykorzystywana na nagrania. |

| Lista | |
|---|---|
| **Status** | Stan pamięci masowej. Możliwe wartości:<br>• **OK**<br>• **Pamięć masowa zapełniona:** Zasób jest zapełniony. System nadpisuje najstarsze, niezablokowane nagrania.<br>• **Unavailable (Niedostępne):** Informacje o pamięci masowej nie są obecnie dostępne. Dzieje się tak na przykład w razie usunięcia lub odłączenia pamięci masowej.<br>• **Kolidujące dane:** Dane z innych aplikacji wykorzystują przestrzeń dyskową przydzieloną do AXIS Camera Station 5. Lub istnieją nagrania bez połączenia z bazą danych, tak zwane nagrania niezaindeksowane, w przestrzeni dyskowej przydzielonej do AXIS Camera Station 5.<br>• **Brak uprawnień:** Użytkownik nie ma uprawnień do odczytu ani zapisu w pamięci masowej.<br>• **Mało miejsca:** Na dysku jest mniej niż 15 GB wolnego miejsca, czyli zbyt mało z perspektywy AXIS Camera Station 5. Aby zapobiec błędom lub uszkodzeniom, AXIS Camera Station 5 wykonuje wymuszone czyszczenie, niezależnie od położenia suwaka pamięci masowej, w celu ochrony dysku. Podczas wymuszonego czyszczenia AXIS Camera Station 5 blokuje nagrywanie do czasu, gdy będzie dostępne ponad 15 GB wolnego miejsca w pamięci masowej.<br>• **Brak miejsca**: Całkowity rozmiar dysku jest mniejszy niż 32 GB, czyli zbyt mały na AXIS Camera Station 5.<br>W przypadku rejestratorów z systemami AXIS OS obsługujących RAID mogą występować następujące stany:<br>• **Online:** System RAID działa zgodnie z oczekiwaniami. Istnieje nadmiarowość na wypadek awarii jednego z dysków fizycznych w systemie RAID.<br>• **Degraded (Obniżona sprawność):** Jeden z dysków fizycznych w systemie RAID jest uszkodzony. Nadal można nagrywać i odtwarzać nagrania z zasobu, ale już nie ma nadmiarowości. W razie uszkodzenia kolejnego dysku fizycznego stan systemu RAID zmieni się na **Failure (Awaria)**. Zalecamy jak najszybszą wymianę uszkodzonych dysków fizycznych. Po wymianie uszkodzonego dysku stan systemu RAID zostanie zmieniony z **Degraded (Obniżona sprawność)** na **Syncing (Synchronizacja)**.<br>• **Syncing (Synchronizacja):** Dyski RAID są synchronizowane. Możliwe jest nagrywanie i odtwarzanie nagrań z zasobu, ale nie ma nadmiarowości na wypadek awarii dysku fizycznego. Po zsynchronizowaniu dysków fizycznych w systemie RAID powstaje nadmiarowość, a jego stan zmienia się na **Online**.<br>Ważne<br>W trakcie synchronizacji nie wolno usuwać dysków RAID, bo może to spowodować ich uszkodzenie.<br>• **Failure (Awaria):** Wystąpiły błędy kilku dysków fizycznych w systemie RAID. Gdy tak się stanie, wszystkie nagrania zapisane w zasobie zostaną utracone, a nagrywanie będzie możliwe dopiero po wymianie uszkodzonych dysków fizycznych. |
| **Serwer** | Serwer, na którym znajduje się lokalna lub sieciowa pamięć masowa. |

| Informacje ogólne | |
|---|---|
| **Wykorzystywana** | Ilość przestrzeni zasobu obecnie wykorzystywana na potrzeby zindeksowanych nagrań. Jeśli plik przynależy do katalogu nagrań, ale nie został zindeksowany w bazie danych, jest on przypisany do kategorii **Other data (Inne dane)**. Patrz punkt Zbieranie niezaindeksowanych plików w temacie *Zarządzaj pamięcią masową, on page 71*. |
| **Free (Wolne)** | Ilość miejsca pozostała w lokalizacji zasobu. Jest to taka sama wartość, jak w ustawieniu „Wolne miejsce" we właściwościach lokalizacji zasobu w interfejsie systemu Windows. |
| **Other data (Inne dane)** | Ilość miejsca w pamięci masowej zajętego przez pliki niebędące zaindeksowanymi nagraniami, a więc nieznane aplikacji AXIS Camera Station 5.<br><br>Inne dane = Całkowita pojemność - zajęte miejsce - wolne miejsce |
| **Total capacity (Całkowita pojemność)** | Łączna wielkość pamięci masowej. Jest to taka sama wartość, jak w ustawieniu „Całkowity rozmiar" we właściwościach lokalizacji zasobu w interfejsie systemu Windows. |
| **Przydzielone** | Ilość miejsca w pamięci masowej, które AXIS Camera Station 5 może wykorzystać na nagrania. W celu dostosowania przydzielonej ilości miejsca można po prostu wyregulować suwak i kliknąć przycisk **Apply (Zastosuj)**. |

| Sieciowa pamięć masowa | |
|---|---|
| **Ścieżka** | Ścieżka do zasobu sieciowego. |
| **Nazwa użytkownika** | Nazwa użytkownika służąca do łączenia się z zasobem sieciowym. |
| **Hasło** | Hasło dla nazwy użytkownika służącej do łączenia się z sieciową pamięcią masową. |

## Zarządzaj pamięcią masową

Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**, aby otworzyć stronę Zarządzaj pamięcią masową. Na tej stronie można określić folder, w którym mają być przechowywane nagrania. Aby nie doszło do zapełnienia pamięci masowej, ustaw maksymalną wartość procentową łącznej pojemności, którą może zająć aplikacja AXIS Camera Station 5. W celu wzmocnienia bezpieczeństwa i zyskania dodatkowego miejsca można dodać więcej lokalnej pamięci masowej oraz dyski sieciowe.

Uwaga

- W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można zarządzać pamięcią masową, wybierając serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.
- Gdy do usługi logujesz się przy użyciu konta systemowego, nie można dodawać dysków sieciowych połączonych z udostępnionymi folderami znajdującymi się na innych komputerach. Patrz *Pamięć sieciowa jest nieosiągalna*.
- Nie można usunąć lokalnej ani sieciowej pamięci masowej, jeżeli w kamerach ustawiono nagrywanie do tej pamięci albo jeśli pamięć zawiera nagrania.

**Dodawanie lokalnej pamięci masowej lub udostępnionego dysku sieciowego**

1. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
2. Kliknij **Dodaj**.

3. Aby dodać lokalną pamięć masową, zaznacz opcję **Local storage (Zasób lokalny)** i wybierz pamięć masową z menu rozwijanego.
4. Aby dodać współużytkowany dysk sieciowy, zaznacz opcję **Shared network drive (Udostępniony dysk sieciowy)** i wpisz ścieżkę do niego. Na przykład: \\adres_ip\udzial.
5. Kliknij przycisk **OK**, a następnie wprowadź nazwę użytkownika i hasło dostępu do współdzielonego dysku sieciowego.
6. Kliknij **OK**.

**Usuwanie lokalnej pamięci masowej lub udostępnionego dysku sieciowego**

Aby usunąć lokalną pamięć masową lub udostępniony dysk sieciowy, wybierz żądany zasób z listy i kliknij przycisk **Usuń**.

**Przenoszenie nagrań do nowego folderu**

1. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
2. Z listy zasobów pamięci wybierz lokalny zasób lub udostępniony dysk sieciowy.
3. W obszarze **Overview (Przegląd)** w polu **Move recordings to a new folder (Przenieś nagrania do nowego folderu)** wprowadź nazwę folderu, aby zmienić lokalizację zasobu pamięci dla nagrań. Spowoduje to również przeniesienie istniejących nagrań z poprzedniego folderu do nowego.
4. Kliknij przycisk **Apply (Zastosuj)**.

**Dostosowywanie pojemności pamięci masowej**

1. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
2. Z listy zasobów pamięci wybierz lokalny zasób lub udostępniony dysk sieciowy.
3. W obszarze **Overview (Przegląd)** przesuń suwak, aby ustawić maksymalną ilość miejsca, które może zająć aplikacja AXIS Camera Station 5.
4. Kliknij przycisk **Apply (Zastosuj)**.

Uwaga

- Do uzyskania optymalnej wydajności najlepiej jest zostawić nie mniej niż 5% wolnego miejsca na dysku.
- Wymóg minimalnej ilości pamięci masowej dodawany w przypadku aplikacji AXIS Camera Station 5 to 32 GB, przy czym musi być co najmniej 15 GB wolnego miejsca.
- Jeśli jest mniej niż 15 GB wolnego miejsca, AXIS Camera Station 5 automatycznie usuwa stare nagrania, aby zwolnić miejsce.

**Zbierz nieindeksowane pliki**

W zasobie pamięci dużą część kategorii **Other data (Inne dane)** mogą stanowić niezaindeksowane pliki. Niezaindeksowany plik to dowolne dane w folderze nagrań, które nie wchodzą w skład bieżącej bazy danych. Plik może zawierać nagrania z poprzednich instalacji albo dane utracone w momencie użycia punktu przywracania.

System nie usuwa zebranych plików, ale gromadzi je i umieszcza w folderze **Non-indexed files (Nieindeksowane pliki)** w pamięci masowej nagrań. Pamięć masowa może się znajdować na tym samym komputerze, co aplikacja kliencka, lub na zdalnym serwerze. Zależy od konkretnej konfiguracji. Aby uzyskać dostęp do folderu **Non-indexed files (Niezaindeksowane pliki)**, wymagany jest dostęp do serwera. AXIS Camera Station 5 umieszcza dane w folderach w takiej kolejności, w jakiej zostały znalezione, najpierw według serwera, a następnie urządzeń połączonych z tym konkretnym serwerem.

Można wyszukać konkretne utracone nagranie lub dziennik albo po prostu usunąć zawartość w celu zwolnienia miejsca.

Aby zebrać niezaindeksowane pliki w celu przejrzenia lub usunięcia:

1. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.

2. Z listy zasobów pamięci wybierz lokalny zasób lub udostępniony dysk sieciowy.
3. W obszarze **Collect non-indexed files (Zbierz nieindeksowane pliki)** kliknij **Collect (Zbierz)**, aby zainicjować zadanie.
4. Po zakończeniu zadania wybierz kolejno opcje **Alarms and Tasks > Tasks (Alarmy i zadania > Zadania)** i kliknij dwukrotnie zadanie, aby wyświetlić rezultat.

### Wybieranie urządzeń pamięci masowej, z którymi mają zostać nawiązane połączenia

Uwaga

Nagrania mają postać plików .acsm i przed odtworzeniem muszą zostać poddane konwersji. Aby uzyskać wsparcie w tym zakresie, prosimy o kontakt z pomocą techniczną Axis.

Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)**, a zostanie otwarta strona Wybierz pamięć masową. Ta strona zawiera listę wszystkich kamer w AXIS Camera Station 5 i pozwala na określenie liczby dni przechowywania nagrań w przypadku poszczególnych kamer. Po zaznaczeniu kamery informacje o pamięci masowej będą widoczne w sekcji Recording Storage (Pamięć masowa nagrań). Można skonfigurować wiele kamer równocześnie.

| | |
|---|---|
| **Nazwa** | Nazwa urządzenia lub lista wszystkich nazw powiązanych kamer, jeśli urządzenie jest wideoenkoderem z wieloma podłączonymi kamerami lub kamerą sieciową z wieloma zdefiniowanymi obszarami obserwacji. |
| **Adres** | Adres urządzenia. Kliknięcie łącza spowoduje przejście do strony konfiguracji urządzenia. Widać w nim adres IP lub nazwę hosta, w zależności od tego, której z tych informacji użyto przy dodawaniu urządzenia. Patrz *Karta Konfiguracja urządzenia, on page 66*. |
| **Adres MAC** | Adres MAC urządzenia. |
| **Producent** | Producent urządzenia. |
| **Model** | Model urządzenia. |
| **Wykorzystywana pamięć masowa** | Ilość pamięci masowej obecnie wykorzystywana na nagrania. |
| **Lokalizacja** | Ścieżka i nazwa pamięci masowej. |
| **Czas przechowywania** | Czas przechowywania skonfigurowany dla kamery. |
| **Najstarsze nagranie** | Godzina wykonania najstarszego nagrania z kamery, jakie znajduje się w zasobie. |
| **Nagrywanie awaryjne** | Pokazuje, czy kamera używa zapisu awaryjnego. |
| **Zapis zawartości rezerwowej** | Pokazuje, czy kamera używa nagrania zapasowego. |
| **Serwer** | Serwer, na którym znajduje się lokalna lub sieciowa pamięć masowa. |

Pamięć masowa została skonfigurowana dla wszystkich kamer na etapie ich dodawania do aplikacji AXIS Camera Station 5. Aby zmodyfikować ustawienia zasobu dla kamery:

1. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Zasób > Wybór)**.
2. Wybierz kamerę w celu edycji ustawień zasobu.
3. W menu **Recording storage (Pamięć masowa nagrań)** ustaw lokalizację pamięci masowej i czas przechowywania.
4. Kliknij przycisk **Apply (Zastosuj)**.

| Pamięć masowa nagrań | |
|---|---|
| **Store to (Zapisz w)** | W rozwijalnym menu wybierz zasób, w którym mają być zapisywane nagrania. Do wyboru są utworzone zasoby lokalne i sieciowe. |
| **Nagrywanie awaryjne** | Wybierz tę opcję, aby nagrania były zapisywane na karcie SD kamery, gdy AXIS Camera Station 5 i kamera utracą połączenie. Po przywróceniu połączenia zapisy awaryjne są przesyłane do AXIS Camera Station 5.<br><br>Uwaga<br>Tej funkcji można używać tylko w kamerach z kartą pamięci SD oraz oprogramowaniem sprzętowym w wersji 5.20 lub nowszej. |
| **Bez ograniczeń** | Wybierz tę wartość czasu przechowywania, aby nagrania pozostawały w zasobie aż do jego zapełnienia. |
| **Ograniczony** | Ta opcja umożliwia ustawienie maksymalnej liczby dni przechowywania nagrań.<br><br>Uwaga<br>Jeżeli miejsce w pamięci masowej przeznaczone dla AXIS Camera Station 5 zostanie zapełnione, system będzie usuwać nagrania przed upływem ustawionej liczby dni. |
| **Maximum days to keep recordings (Maksymalna liczba dni przechowywania nagrań)** | Określ liczbę dni, przez jaką mają być przechowywane nagrania. |

## Konfigurowanie nagrywania i zdarzeń

Po dodaniu kamer do AXIS Camera Station 5 następuje automatyczna konfiguracja nagrywania wyzwalanego ruchem lub nagrywania ciągłego. Metodę nagrywania można zmienić później, przechodząc do menu *Metoda nagrywania, on page 79*.

### Nagrywanie w trybie detekcji ruchu

Funkcji detekcji ruchu można używać we wszystkich kamerach sieciowych i wideoenkoderach Axis. Nagrywanie tylko po wykryciu ruchu pozwoli oszczędzić mnóstwo pamięci masowej w porównaniu z nagrywaniem ciągłym. W obszarze **Recording method (Metoda nagrywania)** można włączyć i skonfigurować **Motion detection (Detekcję ruchu)**. Można na przykład skonfigurować ustawienia, jeśli kamera wykryje zbyt wiele lub za mało poruszających się obiektów, albo jeśli rozmiar nagranych plików jest zbyt duży w stosunku do dostępnego zasobu pamięci.

Aby skonfigurować nagranie ruchu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę.
3. Zaznacz pole wyboru **Motion detection** (Detekcja ruchu).
4. Kliknij **Motion settings (Ustawienia ruchu)**, aby skonfigurować ustawienia detekcji ruchu, takie jak liczba wykrywanych obiektów. Dostępne ustawienia różnią się w zależności od kamery, zob. *Edytowanie wbudowanej funkcji detekcji ruchu* i *Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4*.
5. W menu rozwijanym wybierz **Profile (Profil)**; domyślnie wybrany jest profil **High (wysoki)**.

6. Wybierz harmonogram lub kliknij **New schedule...** (Nowy harmonogram), aby utworzyć nowy własny harmonogram.
7. Skonfiguruj ustawienia czasowe dotyczące bufora przed i bufora po zdarzeniu, a także okres wyzwalacza.
8. Kliknij przycisk **Apply (Zastosuj)**.

Uwaga

Nagrywanie inicjowane ruchem można skonfigurować przy użyciu reguł akcji. Przed użyciem reguł akcji należy wyłączyć **Motion detection (Detekcja ruchu)** w obszarze **Recording method (Metoda zapisywania)**.

| | |
|---|---|
| **Profil** | Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, patrz *Profile strumienia*. |
| **Schedule** | Harmonogram uruchamiania zapisu. Aby zmniejszyć wpływ na zasób pamięci, nagrywaj tylko w określonych przedziałach czasu. |
| | |
| **Bufor przed zdarzeniem** | Liczba sekund przed wykrytym ruchem do zarejestrowania w nagraniu. |
| **Bufor po zdarzeniu** | Liczba sekund po wykrytym ruchu do zarejestrowania w nagraniu. |
| **Trigger period (Okres wyzwalacza)** | Odstęp czasu między dwoma kolejnymi wyzwalaczami, aby zmniejszyć liczbę nagrań następujących po sobie. Jeśli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, nagrywanie będzie kontynuowane, a okres wyzwalania zostanie uruchomiony ponownie. |
| **Uruchom alarm** | Podnosi alarm po wykryciu ruchu przez kamerę. |


*Konfigurowanie funkcji detekcji ruchu*

### Nagrywanie ciągłe i zaplanowane

Nagrywanie ciągłe polega na ciągłym zapisywaniu obrazów, dlatego wymaga więcej miejsca w pamięci masowej niż inne opcje nagrywania. Aby zmniejszyć rozmiar pliku, rozważ zapis uruchamiany detekcją ruchu.

Aby używać zapisu ciągłego:

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę.
3. Zaznacz pole wyboru **Continuous** (Ciągły), aby korzystać z funkcji zapisu ciągłego.
4. Skonfiguruj ustawienia. W poniższej tabeli znajdują się szczegółowe informacje.
5. Kliknij przycisk **Apply (Zastosuj)**.

| | |
|---|---|
| **Profil** | W menu rozwijalnym wybierz **Profile (Profil)**; domyślnie wybrany jest profil **High** (Wysoki). Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, patrz *Profile strumienia*. |
| **Schedule** | Ustaw harmonogram uruchamiania zapisu. Aby zmniejszyć wpływ na zasób pamięci, nagrywaj tylko w określonych przedziałach czasu. |
| **Średnia przepływność** | Włącz i ustaw maksymalną ilość pamięci masowej. System pokazuje szacowaną średnią przepływność obliczaną na podstawie wskazanej maksymalnej ilości pamięci i czasu przechowywania. Maksymalna średnia przepływność wynosi 50000 kb/s. P. sekcja *Konfigurowanie średniej przepływności, on page 79*. |

### Nagrywanie ręczne

Aby uzyskać więcej informacji na temat nagrywania ręcznego, zob. *Ręczne nagrywanie*.

Aby skonfigurować ustawienia ręcznego nagrywania:

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę.
3. Zaznacz pole wyboru **Manual** (Ręcznie).
4. Skonfiguruj ustawienia. W poniższej tabeli znajdują się szczegółowe informacje.
5. Kliknij przycisk **Apply (Zastosuj)**.

| | |
|---|---|
| **Profil** | W menu rozwijanym wybierz **Profile (Profil)**; domyślnie wybrany jest profil **High (wysoki)**. Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, patrz *Profile strumienia*. |
| | |
| **Bufor przed zdarzeniem** | Ustaw liczbę sekund przed naciśnięciem przycisku zapisu do zarejestrowania w nagraniu. |
| **Bufor po zdarzeniu** | Ustaw liczbę sekund po zatrzymaniu zapisu do zarejestrowania w nagraniu. |
| **Dodawanie zakładek podczas zapisu** | Zaznacz, aby dodawać szczegóły zakładki przy każdym ręcznym uruchomieniu zapisu. Zakładki pomagają później odnaleźć i zidentyfikować konkretne nagrania. To ustawienie dotyczy jedynie operatorów i administratorów i jest domyślnie wyłączone. |
| **Maksymalny czas trwania** | Ustaw maksymalną długość każdego nagrania bez rejestrowania materiału przed lub po zdarzeniu. Ustaw 0, aby uzyskać nieograniczony czas trwania. |

### Nagrywanie wyzwalane regułami

Nagrywanie wyzwalane regułami jest uruchamiane i zatrzymywane zgodnie z regułą utworzoną w oknie Reguły akcji. Reguły mogą na przykład służyć do generowania nagrań inicjowanych sygnałami z portów we/wy, próbami sabotażu czy wykryciem zdarzeń przez aplikację AXIS Cross Line Detection. Reguła może mieć kilka wyzwalaczy.

Aby utworzyć nagranie wyzwalane regułą, zob. *Reguły akcji*.

Uwaga

Jeżeli używasz reguły nagrywania wyzwalanego ruchem, wyłącz funkcję nagrywania wyzwalanego ruchem, tak aby uniknąć dublowania nagrań.

### Nagrywanie awaryjne

Użyj funkcji zapisu awaryjnego, aby upewnić się, że nagrania zostaną zachowane w razie utraty połączenia z AXIS Camera Station 5. Gdy zapis awaryjny jest włączony, kamera zapisuje nagrania na karcie SD, jeżeli połączenie zostanie przerwane na co najmniej 20 sekund. Kamera musi mieć zainstalowaną kartę SD, a funkcja być włączona. Działa ona tylko dla nagrywania w formacie H.264.

Aby włączyć zapis awaryjny:

1. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Zasób > Wybór)**.
2. Wybierz kamerę obsługującą zapis awaryjny.
3. Wybierz opcję **Failover recording (Zapis awaryjny)**.
4. Kliknij przycisk **Apply (Zastosuj)**.

Uwaga

- Ponowne uruchomienie serwera AXIS Camera Station 5 nie powoduje uruchomienia zapisu awaryjnego. Dotyczy to na przykład sytuacji, gdy uruchomisz narzędzie do konserwacji bazy danych, uruchomisz ponownie aplikację AXIS Camera Station 5 lub uruchomisz ponownie komputer, na którym jest zainstalowane oprogramowanie serwera.
- Włączenie zapisu awaryjnego powoduje nadpisanie wszelkich istniejących konfiguracji awaryjnych przypisanych do tej kamery w innych serwerach.
- Zapis awaryjny może być aktywny tylko dla jednego serwera AXIS Camera Station 5 w danym czasie w przypadku każdego widoku z kamery.

Po przywróceniu połączenia serwer AXIS Camera Station 5 automatycznie importuje nagrania awaryjne i oznacza je kolorem ciemnoszarym na osi czasu.

Kamera wykorzystuje 20-sekundowy bufor zapisu przed i po wystąpieniu zdarzenia celem zminimalizowania przerwy w zapisie, jednak mimo tego mogą wystąpić krótkie przerwy trwające około 1 do 4 sekund. W przypadku zapisu awaryjnego zawsze stosowany jest profil strumieniowania High. Zapisywany jest również dźwięk, o ile został ustawiony w kamerze i stanowił część strumieniowania przed włączeniem zapisu awaryjnego.

| Metody nagrywania | |
|---|---|
| **Detekcja ruchu z buforem przez zdarzeniem** | Jeżeli dojdzie do utraty połączenia na ponad 20 sekund, kamera będzie kontynuować zapis na kartę SD do momentu przywrócenia połączenia lub zapełnienia karty SD. |
| **Detekcja ruchu bez bufora przed zdarzeniem** | • Jeżeli dojdzie do utraty połączenia na ponad 20 sekund w przypadku, gdy nie jest ustawiony zapis uruchamiany wykryciem ruchu, zapis awaryjny nie rozpocznie się.<br>• Jeżeli dojdzie do utraty połączenia na ponad 20 sekund w przypadku, gdy ustawiony jest zapis uruchamiany wykryciem ruchu, rozpocznie się zapis awaryjny, który potrwa do chwili przywrócenia połączenia lub zapełnienia karty SD. |
| **Nagrywanie ciągłe** | Jeżeli dojdzie do utraty połączenia na ponad 20 sekund, kamera będzie kontynuować zapis na kartę SD do momentu przywrócenia połączenia lub zapełnienia karty SD. |

Uwaga

Urządzenia z oprogramowaniem układowym AXIS OS w wersji wcześniejszej niż 11.11.42 korzystają ze starszej metody zapisu awaryjnego. Oto najważniejsze różnice:

- Kamera rozpoczyna zapis awaryjny po 10 sekundach od utraty połączenia.
- Kamera wykorzystuje 10-sekundowy bufor pamięci wewnętrznej zamiast 20-sekundowego bufora przed i po zdarzeniu.


*Używanie karty SD do zapisu awaryjnego*

## Zapis zawartości rezerwowej

Na urządzeniu, które roli pamięci masowej nagrań używa rejestratora AXIS S3008 Recorder, można włączyć funkcję zapisu zawartości rezerwowej. Po włączeniu funkcji zapisu awaryjnego urządzenie automatycznie rozpocznie nagrywanie ciągłe w przypadku utraty połączenia między AXIS Camera Station 5 a rejestratorem. Do zapisu zawartości rezerwowej Urządzenie używa profilu średniego.

Uwaga

- Do działania funkcji jest potrzebna aplikacja AXIS Camera Station w wersji 5.36 lub nowszej, oprogramowanie sprzętowe rejestratora AXIS S3008 Recorder w wersji 10.4 lub nowszej oraz oprogramowanie sprzętowe urządzeń Axis w wersji 5.50 lub nowszej.
- Jeśli w momencie rozpoczęcia zapisu zawartości rezerwowego trwa nagrywanie ciągłe, rozpoczyna się nowe nagrywanie ciągłe. System tworzy duplikaty strumienia na rejestratorze.

Aby włączyć funkcję zapisu rezerwowego:

1. Upewnij się, że dodano AXIS S3008 Recorder i urządzenia oraz wybrano rejestrator jako pamięć masową nagrań dla urządzenia. P. sekcja *Konfigurowanie rejestratorów AXIS OS Recorder.*

2. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Zasób > Wybór)**.
3. Zaznacz urządzenie i wybierz opcję **Zapis zawartości rezerwowej**.
4. Kliknij przycisk **Apply (Zastosuj)**.

## Metoda nagrywania

AXIS Camera Station 5 Automatycznie konfiguruje nagrywanie ruchu lub ciągłe podczas dodawania urządzeń.

Symbol zaznaczenia na liście wskazuje metodę nagrywania używaną przez urządzenie. Aby dostosować ustawienia profilu dotyczące obrazu filmowego i dźwięku, zobacz *Profile strumienia*.

Aby zmienić metodę nagrywania:

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz jedno lub kilka urządzeń.
   W przypadku urządzeń o tej samej nazwie modelu można skonfigurować wiele urządzeń naraz.
3. Na ekranie **Recording method (Metoda nagrywania)** włącz lub wyłącz metodę nagrywania.

Uwaga

Obszary obserwacji nie obsługują detekcji ruchu.

### Konfigurowanie średniej przepływności

Średnia przepływność bitowa dostosowuje się automatycznie w dłuższym okresie. Dzięki temu można uzyskać docelową przepływność bitową i zapewnić jak dobrą jakość obrazu wideo przy określonych zasobach pamięci masowej.

Uwaga

- Ta opcja jest dostępna tylko dla nagrywania ciągłego, a kamery muszą obsługiwać funkcję średniej przepływności bitowej oraz mieć zainstalowane oprogramowanie sprzętowe w wersji 9.40 lub nowszej.
- Ustawienia średniej przepływności bitowej wpływają na jakość wybranego profilu strumienia.

1. Wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)** i upewnij się, że ustawiono ograniczony czas przechowywania nagrań w kamerze.
2. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumienia)** i upewnij się, że dla profilu wideo przewidzianego dla ciągłego nagrywania ustawiono format H.264 lub H.265.
3. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
4. Wybierz kamerę i włącz ustawienie **Continuous (Ciągły)**.
5. W obszarze **Video settings (Ustawienia obrazu)** zaznacz skonfigurowany przez siebie profil wideo.
6. Włącz opcję **Average bitrate (Średnia przepływność bitowa)** i ustaw wartość w polu **Max storage (Maks. ilość pamięci)**. System pokazuje szacowaną średnią przepływność obliczaną na podstawie wskazanej maksymalnej ilości pamięci i czasu przechowywania. Maksymalna średnia przepływność bitowa wynosi 50000 Kb/s.

Uwaga

Parametr **Max storage (Maks. ilość pamięci)** określa maksymalną przestrzeń w pamięci przeznaczoną na nagrania w ustawionym okresie przechowywania. Gwarantuje tylko tyle, że nagrania nie przekraczają określonego miejsca, nie gwarantuje natomiast, że jest wystarczająco dużo miejsca na nagrania.

7. Kliknij przycisk **Apply (Zastosuj)**.

### Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4

AXIS Video Motion Detection 2 i 4 to aplikacje do kamery, które można instalować w urządzeniach obsługujących rozwiązanie AXIS Camera Application Platform. Gdy w kamerze zostanie zainstalowana aplikacja AXIS Video Motion Detection 2 lub 4, funkcja detekcji ruchu będzie wykrywać poruszające się obiekty w granicach obszaru zainteresowania. Motion Detection 2 wymaga oprogramowania sprzętowego w wersji 5.60 lub nowszej, a AXIS Video Motion Detection 4 wymaga oprogramowania sprzętowego w wersji 6.50 lub nowszej. Warto również sprawdzić w informacjach o wersji oprogramowania sprzętowego produktu, czy obsługuje on oprogramowanie do wizyjnej detekcji ruchu Video Motion Detection w wersji 4.

W przypadku wybrania opcji nagrywania ruchu podczas dodawania kamer do aplikacji AXIS Camera Station 5 na kamerach z wymaganym oprogramowaniem sprzętowym jest instalowane narzędzie AXIS Video Motion Detection 2 i 4. Kamery bez wymaganego oprogramowania sprzętowego korzystają z wbudowanej funkcji detekcji ruchu. Aplikację można zainstalować ręcznie z poziomu strony Zarządzanie urządzeniami. Patrz *Instalowanie aplikacji do kamery*.

W aplikacji AXIS Video Motion Detection 2 i 4 można tworzyć następujące encje:

- **Obszar zainteresowania**: Obszar nagrania, w którym kamera wykrywa poruszające się obiekty. Funkcja ignoruje obiekty obszarem zainteresowania. Obszar jest wyświetlany jako wielokąt nałożony na obraz wideo. Obszar może mieć od 3 do 20 punktów (narożników).
- **Obszar do wykluczenia**: Obszar w obrębie obszaru zainteresowania, w którym poruszające się obiekty są ignorowane.
- **Filtry ignorowania**: filtry służące do ignorowania poruszających się obiektów wykrywanych przez aplikację. Należy używać jak najmniejszej liczby filtrów oraz tak konfigurować filtry, aby żadne ważne obiekty nie były ignorowane. Należy włączać o konfigurować po jednym filtrze naraz.
  - **Obiekty krótkotrwałe**: Ten filtr powoduje ignorowanie obiektów pojawiających się w obrazie tylko przez krótki czas. Np.: światła przejeżdżających pojazdów i szybko poruszające się cienie. Ustaw minimalny czas, przez jaki obiekty muszą być widoczne w obrazie, aby został wygenerowany alarm. Czas będzie odliczany od momentu wykrycia obiektu przez aplikację. Filtr wstrzymuje wyzwolenie alarmu i jeśli obiekt zniknie z obrazu w określonym czasie, nie wyzwala go.
  - **Małe obiekty**: Ten filtr powoduje ignorowanie małych obiektów, takich jak niewielkie zwierzęta. Ustaw szerokość i wysokość jako wartość procentową całkowitych wymiarów obrazu. Filtr ignoruje obiekty, które nie osiągają wyznaczonej szerokości i wysokości, i nie wyzwoli alarmu. Aby filtr zignorował obiekt, musi on być mniejszy niż wyznaczona szerokość i wysokość.
  - **Kołyszące się obiekty**: Powoduje ignorowanie obiektów, które poruszają się jedynie na niewielką odległość, takie jak kołyszące się gałęzie, flagi i ich cienie. Ustaw odległość jako wartość procentową całkowitej odległości na obrazie. Filtr ignoruje obiekty przemieszczające się na odległość mniejszą niż odległość od środka elipsy do grotu jednej ze strzałek. Elipsa jest miarą ruchu i jest stosowana do całego ruchu w obrazie.

Aby skonfigurować ustawienia ruchu:

Uwaga

Wprowadzone tutaj ustawienia spowodują zmianę ustawień w kamerze.

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Zaznacz kamerę zawierającą oprogramowanie AXIS Video Motion Detection 2 lub 4 i kliknij przycisk **Motion Settings (Ustawienia ruchu)**.
3. Edytowanie obszaru zainteresowania.
4. Edytowanie obszaru wykluczenia.
5. Tworzenie filtrów ignorowania.
6. Kliknij przycisk **Apply (Zastosuj)**.

| | |
|---|---|
| **Dodanie nowego punktu** | Aby dodać nowy punkt w obszarze zainteresowania, kliknij linię pomiędzy dwoma punktami. |
| **Remove Point (Usuń punkt)** | Aby usunąć punkt z obszaru zainteresowania, kliknij go, a następnie kliknij przycisk **Remove Point (Usuń punkt)**. |
| **Add Exclude Area (Dodaj obszar wykluczenia)** | Aby utworzyć obszar wykluczenia, kliknij przycisk **Add Exclude Area (Dodaj obszar)**, a następnie kliknij linię pomiędzy dwoma punktami. |
| **Remove Exclude Area (Usuń obszar wykluczenia)** | Aby usunąć obszar wykluczenia, kliknij przycisk **Remove Exclude Area (Usuń obszar wykluczenia)**. |
| **Short lived objects filter (Filtr obiektów krótkotrwałych)** | Aby włączyć filtr ignorowania dla obiektów krótkotrwałych, zaznacz opcję **Short lived objects filter (Filtr obiektów krótkotrwałych)**, a następnie na suwaku **Time (Czas)** dostosuj okres, przez jaki obiekty muszą się znajdować w obrazie, aby został zainicjowany alarm. |
| **Small objects filter (Filtr małych obiektów)** | Aby włączyć filtr ignorowania małych obiektów, zaznacz opcję **Small objects filter (Filtr małych obiektów)**, a następnie za pomocą suwaków **Width (Szerokość)** i **Height (Wysokość)** dostosuj rozmiar obiektów, które mają być ignorowane. |
| **Swaying objects filter (Filtr kołyszących się obiektów)** | Aby włączyć filtr ignorowania kołyszących się obiektów, zaznacz opcję **Swaying objects filter (Filtr kołyszących się obiektów)**, a następnie za pomocą suwaka **Distance (Odległość)** dopasuj rozmiar elipsy. |

### Edytowanie wbudowanej funkcji detekcji ruchu

Dzięki wbudowanej detekcji ruchu kamera wykrywa ruch w obrębie jednej lub kilku stref detekcyjnych, a jednocześnie ignoruje pozostały ruch. Strefa detekcyjna to obszar, w którym wykrywany jest ruch. Wewnątrz strefy detekcyjnej można wyznaczyć obszar wykluczenia, w którym ruch będzie ignorowany. Można określić wiele stref detekcyjnych i wykluczenia.

**Aby dodawać i edytować strefy detekcyjne:**

Uwaga

Wprowadzone tutaj ustawienia spowodują zmianę ustawień w kamerze.

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Zaznacz kamerę z wbudowaną funkcją detekcji ruchu i kliknij **Motion Settings (Ustawienia ruchu)**.
3. W obszarze Window (Okno) kliknij **Add (Dodaj)**.
4. Wybierz **Dołącz**.
5. Jeśli chcesz widzieć tylko edytowaną strefę, wybierz **Show selected window (Pokaż wybrane okno)**.
6. Teraz możesz przesuwać kształt i zmieniać jego rozmiar na obrazie wideo. To jest strefa detekcyjna.
7. Ręcznie ustaw parametry, takie jak **Object size (Rozmiar obiektu)**, **History (Historia)** i **Sensitivity manually (Czułość ręcznie)**.
8. Aby używać wstępnie zdefiniowanych ustawień: Wybierz jedną z opcji: **Low (Niska)**, **Moderate (Umiarkowana)**, **High (Wysoka)** lub **Very High (Bardzo wysoka)**. Ustawienie **Low (Niska)** powoduje wykrywanie większych obiektów o krótszej historii. Wartość **Very High (Bardzo wysoka)** powoduje wykrywanie mniejszych obiektów o dłuższej historii.

9. W obszarze **Activity (Działanie)** można zobaczyć ruch wykryty w strefie detekcyjnej. Czerwone szczyty wskazują na ruch. W polu **Activity (Aktywność)** można ustawić parametry, takie jak **Object size (Wielkość obiektu)**, **History (Historia)** i **Sensitivity (Czułość)**.
10. Kliknij **OK**.

| | |
|---|---|
| **Wielkość obiektu** | Rozmiary obiektu względem rozmiarów obszaru. Przy wysokim poziomie kamera wykrywa tylko bardzo duże obiekty. Przy niskim poziomie kamera wykrywa nawet bardzo małe obiekty. |
| **Historia** | Długość przebywania obiektu w pamięci decyduje o tym, ile czasu obiekt musi się znajdować wewnątrz obszaru, zanim zostanie uznany za nieruchomy. Przy wysokiej wartości ruch zostanie wykryty, jeżeli obiekt długo przebywa w granicach obszaru. Przy niskiej wartości ruch zostanie wykryty po krótkim przebywaniu obiektu wewnątrz obszaru. Jeżeli nie chcesz, żeby były wyświetlane obiekty z obszaru, ustaw bardzo wysoką wartość progową historii. Spowoduje to włączenie detekcji ruchu, gdy obiekt znajdzie się w strefie. |
| **Czułość** | Różnica jasności między tłem a obiektem. Przy wysokiej czułości kamera będzie wykrywać zwykłe kolory na zwykłym tle. Przy niskiej czułości kamera wykrywa tylko bardzo jasne obiekty na ciemnym tle. Aby było wykrywane tylko migające światło, ustaw niską czułość. Dla pozostałych sytuacji zalecamy wybieranie wysokiego poziomu czułości. |

**Aby dodawać i edytować obszary wykluczenia:**

1. Na ekranie **Edit Motion Detection (Edytuj detekcję ruchu)** w obszarze Window (Okno) kliknij przycisk **Add (Dodaj)**.
2. Wybierz opcję **Exclude (Wyklucz)**.
3. Teraz możesz przesuwać zacieniony kształt i zmieniać jego rozmiar na obrazie wideo.
4. Kliknij **OK**.

**Aby usunąć strefę detekcyjną lub wykluczenia:**

1. Na ekranie **Edit Motion Detection (Edytuj detekcję ruchu)** wybierz strefę, którą chcesz usunąć.
2. Kliknij przycisk **Remove (Usuń)**.
3. Kliknij przycisk **OK**.

## Porty we/wy

Wiele kamer i wideoenkoderów ma porty we/wy służące do podłączania urządzeń zewnętrznych. Niektóre urządzenia dodatkowe mogą być wyposażone w porty we/wy.

Istnieją dwa rodzaje portów we/wy:

**Port wejścia –** Służy do podłączania urządzeń, które mogą się przełączać między obwodem otwartym i zamkniętym. Na przykład styki drzwi i okien, czujki dymu, czujniki wykrywania zbicia szyby i detektory PIR (pasywne czujki podczerwieni).

**Port wyjścia –** Służy do ustanawiania połączenia z takimi urządzeniami jak przekaźniki, drzwi, zamki i alarmy. AXIS Camera Station 5 może sterować urządzeniami połączonymi za pośrednictwem portów wyjścia.

Uwaga

- W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można wybrać dowolny połączony serwer z rozwijalnego menu **Selected server (Wybrany serwer)**, aby utworzyć reguły akcji i nimi zarządzać.
- Administratorzy mogą wyłączać porty we/wy dla użytkowników. Patrz *Uprawnienia użytkownika*.

Reguły akcji używają portów we/wy jako wyzwalaczy lub akcji. Wyzwalacze wykorzystują sygnały wejściowe, na przykład jeśli AXIS Camera Station 5 odbierze sygnał z urządzenia podłączonego do portu wejścia, wykona określone akcje. Akcje wykorzystują porty wyjścia, na przykład jeśli reguła się aktywuje, AXIS Camera Station 5 może aktywować lub dezaktywować urządzenie podłączone do portu wyjścia. Patrz *Reguły akcji*.

Więcej informacji o podłączaniu urządzeń i konfigurowaniu portów we/wy można znaleźć w instrukcji obsługi lub instalacji produktu Axis. Niektóre urządzenia mają porty, które mogą działać jako wejście lub wyjście.

Portami wyjścia można sterować ręcznie. Patrz *Monitorowanie portów we/wy*.

### Dodawanie portów we/wy

Aby dodać porty we/wy:

1. Wybierz kolejno opcje **Configuration > Recording and events > I/O ports (Konfiguracja > Zapis i zdarzenia > Porty we/wy)**.
2. Kliknij **Add (Dodaj)**, aby wyświetlić listę portów we/wy, które można dodać.
3. Zaznacz port i kliknij przycisk **OK**.
4. Przejrzyj informacje w obszarach **Type (Typ)** i **Device (Urządzenie)**. W razie potrzeby zmień informacje.
5. Wprowadź nazwę w polach **Port**, **Active State (Stan aktywny)**i **Inactive State (Stan nieaktywny)**. Nazwy te będą wyświetlane w oknach Reguły akcji, Dzienniki i Monitorowanie we/wy.
6. Dla portów wyjścia można ustawić stan początkowy na potrzeby sytuacji, gdy AXIS Camera Station 5 łączy się z urządzeniem. Wybierz opcję **On startup set to (Podczas uruchamiania ustaw na)** i wybierz stan początkowy z menu rozwijanego **State (Stan)**.

| | |
|---|---|
| **Edytuj** | Aby zmodyfikować port, zaznacz go i kliknij przycisk **Edit (Edycja)**. W wyskakującym oknie dialogowym zaktualizuj informacje o portach i kliknij przycisk **OK**. |
| **Usuń** | Aby usunąć port, zaznacz go i kliknij przycisk **Remove (Usuń)**. |
| **Reload I/O Ports (Załaduj ponownie porty we/wy)** | Jeśli porty we/wy zostały skonfigurowane na stronie konfiguracji urządzenia, kliknij przycisk **Reload I/O Ports (Załaduj ponownie porty we/wy)**, aby zaktualizować listę. |

### Monitorowanie portów we/wy

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można wybrać dowolny połączony serwer z rozwijalnego menu **Selected server (Wybrany serwer)** , aby monitorować porty WE/WY.

Aby ręcznie sterować portami wyjścia:

1. Wybierz kolejno ☰ **> Actions (Akcje) > I/O Monitoring (Monitorowanie we/wy)**.
2. Wybierz port wyjścia.
3. Kliknij przycisk **Change state (Zmień stan)**.

## Reguły akcji

Użyj reguł działania, aby automatycznie reagować na zdarzenia. Przykładowo wysyłaj wiadomości e-mail, gdy kamera wykryje ruch poza godzinami pracy firmy, komunikuj się z urządzeniami dołączonymi do portów we / wy i powiadamiaj operatorów o ważnych zdarzeniach.

Każda reguła ma wyzwalacze (zdarzenia, które uaktywniają regułę), działania (co się dzieje po wyzwoleniu) oraz opcjonalny harmonogram. Po uaktywnieniu wyzwalaczy reguła wykonuje wszystkie działania.

Uwaga

- W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można wybrać dowolny połączony serwer z rozwijalnego menu **Selected Server** (Wybrany serwer), aby utworzyć reguły działań i nimi zarządzać.
- W przypadku urządzeń innych producentów dostępne akcje mogą się różnić. Zależy to od urządzenia. Wiele tych działań może wymagać skonfigurowania dodatkowych opcji urządzenia.

## Dodawanie wyzwalaczy

Wyzwalacze aktywują reguły, a każda reguła może mieć wiele wyzwalaczy. Dopóki jeden z wyzwalaczy pozostaje aktywny, aktywna pozostaje reguła. Jeśli wszystkie wyzwalacze muszą być aktywne, aby reguła była aktywna, zaznacz opcję **All triggers must be active simultaneously to trigger the actions (Wszystkie wyzwalacze muszą być aktywne jednocześnie, aby wyzwalać akcje)**. Jeśli to ustawienie jest używane do wyzwalaczy impulsowych, wydłuż czas wyzwalania. Wyzwalacze impulsowe są aktywne tylko chwilowo.

Dostępne są następujące wyzwalacze:

**Detekcja ruchu –** Zarejestrowanie ruchu w zdefiniowanym obszarze aktywuje wyzwalacz detekcji ruchu. Patrz *Tworzenie wyzwalaczy opartych na detekcji ruchu, on page 85*.

**Zawsze aktywne –** Wyzwalacz jest zawsze włączony. Można na przykład połączyć go z zawsze włączonym harmonogramem i akcją nagrywania o niskim profilu, aby uzyskać drugie nagranie ciągłe, co sprawdza się w przypadku urządzeń o ograniczonej wydajności.

**Aktywne zabezpieczenie antysabotażowe –** Wyzwalacz oparty na alarmie przeciwsabotażowym aktywuje się, gdy położenie urządzenia zostanie zmienione, zostanie zakryty obiektyw lub obraz stanie się bardzo nieostry. Patrz *Tworzenie wyzwalaczy opartych na aktywnym alarmie antysabotażowym, on page 85*.

**Podgląd na żywo –** Wyzwalacz oparty na podglądzie na żywo uruchamia się, gdy użytkownik otwiera strumień wideo z określonej kamery. Może on służyć na przykład do informowania za pomocą jej diod LED, że osoby znajdujące się w pobliżu kamery są obserwowane. Zob. .

**AXIS Cross Line Detection –** AXIS Cross Line Detection to aplikacja do kamer i wideoenkoderów. Wykrywa ona poruszające się obiekty, które przekraczają wirtualną linię. Może służyć na przykład do monitorowania punktów wejścia i wyjścia. Patrz *Tworzenie wyzwalaczy opartych na aplikacji AXIS Cross Line Detection, on page 86*.

**Zdarzenie systemowe i błąd systemowy –** Wyzwalacz oparty na zdarzeniu i błędzie systemowym jest aktywowany w przypadku błędów nagrywania, zapełnienia pamięci masowej, niemożności nawiązania połączenia z sieciową pamięcią masową albo utraty połączenia z jednym lub kilkoma urządzeniami. Patrz *Tworzenie wyzwalaczy opartych na zdarzeniach i/lub błędach systemowych, on page 86*.

**Wejście/Wyjście –** Wyzwalacz oparty na wejściu/wyjściu (we/wy) aktywuje się, gdy port we/wy urządzenia odbierze sygnał na przykład z połączonych drzwi, czujki dymu lub przełącznika. Patrz *Tworzenie wyzwalaczy opartych na wejściach/wyjściach, on page 87*. Jeśli jest taka możliwość, zalecamy używanie wyzwalaczy opartych na zdarzeniach w urządzeniu zamiast wyzwalaczy wejścia/wyjścia.

**Zdarzenie z urządzenia –** Ten wyzwalacz wykorzystuje zdarzenia bezpośrednio z kamery lub urządzenia dodatkowego. Użyj tej opcji, jeśli w AXIS Camera Station 5 nie ma odpowiedniego wyzwalacza. Patrz *Tworzenie wyzwalaczy opartych na zdarzeniach w urządzeniu, on page 88*.

**Przycisk działania –** Przyciski akcji służą do rozpoczynania i zatrzymywania działań w podglądzie na żywo. Ten sam przycisk może być używany w różnych regułach. Patrz *Tworzenie wyzwalaczy opartych na przyciskach akcji, on page 93*.

**Zdarzenie aplikacji AXIS Entry Manager –** Ten wyzwalacz aktywuje się w sytuacji, gdy AXIS Camera Station 5 odbierze sygnały z drzwi skonfigurowanych w aplikacji AXIS Entry Manager. Na przykład otwarcie drzwi siłą, otwarte zbyt długo lub odmowa dostępu. Patrz *Tworzenie wyzwalaczy zdarzeń aplikacji AXIS Entry Manager, on page 94*.

**Zewnętrzne połączenie HTTPS –** Wyzwalacz oparty na zewnętrznym połączeniu HTTPS umożliwia zewnętrznym aplikacjom wyzwalanie zdarzeń w aplikacji AXIS Camera Station 5 poprzez wysłanie komunikatu połączeniem HTTPS. Patrz *Tworzenie wyzwalaczy opartych na zewnętrznych połączeniach HTTPS, on page 95*.

### Tworzenie wyzwalaczy opartych na detekcji ruchu

Wyzwalacz oparty na detekcji ruchu aktywuje się, gdy kamera wykryje ruch w wyznaczonym obszarze. Ponieważ to kamera przetwarza zdarzenie detekcji, nie zwiększa się obciążenie AXIS Camera Station 5.

Uwaga

Nie używaj wyzwalaczy opartych na detekcji ruchu do rozpoczynania nagrywania razem z funkcją nagrywania inicjowanego ruchem w kamerze. Zanim użyjesz wyzwalaczy opartych na detekcji ruchu wyłącz nagrywanie inicjowane ruchem w kamerze. Aby wyłączyć nagrywanie inicjowane ruchem, przejdź do **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.

Aby utworzyć wyzwalacz oparty na detekcji ruchu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i zaznacz opcję **Motion detection (Detekcja ruchu)**.
4. Kliknij **OK**.
5. Na wyskakującym ekranie:
   5.1. Wybierz kamerę, która ma wykrywać ruch.
   5.2. Ustaw interwał między dwoma kolejnymi nagraniami, aby zmniejszyć liczbę zapisów następujących po sobie. Jeśli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, nagrywanie będzie kontynuowane, a okres wyzwalania zostanie uruchomiony ponownie.
   5.3. Kliknij opcję **Motion settings (Ustawienia ruchu)**, aby skonfigurować ustawienia detekcji ruchu. Dostępne ustawienia różnią się w zależności od kamery. Patrz *Edytowanie wbudowanej funkcji detekcji ruchu* i *Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4*.
6. Kliknij przycisk **OK**.

### Tworzenie wyzwalaczy opartych na aktywnym alarmie antysabotażowym

Wyzwalacz oparty na aktywnym zabezpieczeniu antysabotażowym aktywuje się, gdy położenie kamery zostanie zmienione, zostanie zakryty obiektyw lub obraz stanie się bardzo nieostry. Ponieważ to urządzenie przetwarza detekcję sabotażu, obciążenie serwera AXIS Camera Station 5 nie zwiększa się.

Funkcja aktywnego alarmu antysabotażowego jest dostępna w kamerach obsługujących ochronę antysabotażową oraz mających zainstalowane oprogramowanie sprzętowe w wersji 5.11 lub nowszej.

Aby utworzyć wyzwalacz oparty na aktywnym alarmie antysabotażowym:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Dodaj** i wybierz opcję **Activate tampering alarm (Aktywuj alarm antysabotażowy)**.
4. Kliknij **OK**.
5. W polu **Trigger on (Wyzwalaj przy)** wybierz kamerę, której chcesz używać.
6. Kliknij **OK**.

### Tworzenie wyzwalaczy opartych na aplikacji AXIS Cross Line Detection

AXIS Cross Line Detection to aplikacja do kamer i wideoenkoderów. Wykrywa ona poruszające się obiekty, które przekraczają wirtualną linię, i aktywuje wyzwalacz. Za jej pomocą można też na przykład monitorować punkty wejścia i wyjścia. Ponieważ to kamera przetwarza zdarzenia detekcji, obciążenie serwera AXIS Camera Station 5 nie zwiększa się.

Aplikację można zainstalować tylko na urządzeniach obsługujących platformę AXIS Camera Application Platform. Aby używać aplikacji AXIS Cross Line Detection jako wyzwalacza, należy pobrać aplikację ze strony *axis.com*, a następnie zainstalować ją na urządzeniach. Patrz *Instalowanie aplikacji do kamery*.

Aby utworzyć wyzwalacz w formie aplikacji AXIS Cross Line Detection:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Dodaj** i zaznacz opcję **AXIS Cross Line Detection**.
4. Kliknij **OK**.
5. Kliknij **Refresh (Odśwież)**, aby zaktualizować listę.
6. Z menu rozwijanego **Trigger on (Wyzwalaj przy)** wybierz kamerę, która ma być używana. Można wybrać tylko kamery z zainstalowaną aplikacja AXIS Cross Line Detection.
7. W polu **Trigger period (Czas wyzwalania)** ustaw odstęp czasu pomiędzy kolejnymi wyzwalaczami, aby zmniejszyć liczbę następujących po sobie zapisów.
   Jeśli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, nagrywanie będzie kontynuowane, a okres wyzwalania zostanie uruchomiony ponownie.
8. Kliknij **AXIS Cross Line Detection settings (Ustawienia aplikacji AXIS Cross Line Detection)**, a w przeglądarce internetowej otworzy się strona **Applications (Aplikacje)** dla wybranej kamery. Informacje o dostępnych ustawieniach można znaleźć w dokumentacji dołączonej do aplikacji AXIS Cross Line Detection.

Uwaga

Do konfigurowania aplikacji AXIS Cross Line Detection należy używać przeglądarki Internet Explorer z włączoną obsługą formantów ActiveX. Jeżeli zostanie wyświetlone pytanie o zainstalowanie aplikacji AXIS Media Control, kliknij **Yes (Tak)**.

### Tworzenie wyzwalaczy opartych na zdarzeniach i/lub błędach systemowych

Zaznacz jedno lub więcej zdarzenie i/lub błędy systemowe, które mają być używane jako wyzwalacze. Zdarzenia systemowe to na przykład są błędy nagrywania, pełna pamięć masowa, brak połączenia z sieciową pamięcią masową, a także utrata połączenia z co najmniej jednym urządzeniem.

Aby utworzyć wyzwalacz oparty na zdarzeniach i/lub błędach systemowych:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **System event and error (Zdarzenie i/lub błąd systemowy)**.
4. Kliknij **OK**.
5. Wybierz zdarzenie systemowe lub błąd, aby utworzyć wyzwalacz.
6. Kliknij **OK**.

| | |
|---|---|
| **On recording error (Błąd nagrywania)** | Zaznacz opcję **On recording error (Błąd przy nagrywaniu)**, aby wyzwalacz był aktywowany po wystąpieniu błędów w trakcie nagrywania, na przykład gdy kamera przestanie wysyłać obraz strumieniowo. |
| **Przy zapełnionej pamięci masowej** | Zaznacz opcję **On full storage (Przy zapełnionej pamięci masowej)**, aby wyzwalacz był aktywowany po zapełnieniu pamięci masowej nagrań. |
| **W przypadku braku kontaktu z zasobem sieciowym** | Zaznacz opcję **On no contact with network storage (W przypadku braku kontaktu z zasobem sieciowym)**, aby wyzwalacz był aktywowany w razie problemów z dostępem do sieciowej pamięci masowej. |
| **On lost connection to camera (W przypadku utraconego połączenia z kamerą)** | Zaznacz opcję **On lost connection to camera (W przypadku utraconego połączenia z kamerą)**, aby wyzwalacz był aktywowany w razie problemów z nawiązaniem łączności z jedną lub kilkoma kamerami.<br>• Zaznacz opcję **All (Wszystkie)**, aby były uwzględniane wszystkie kamery dodane do AXIS Camera Station 5.<br>• Wybierz opcję **Selected (Wybrane)** i kliknij **Cameras (Kamery)**, aby wyświetlić listę wszystkich kamer dodanych do AXIS Camera Station 5. Użyj opcji **Select all (Zaznacz wszystko)**, aby zaznaczyć wszystkie kamery lub użyj opcji **Deselect all (Odznacz wszystko)**, aby odznaczyć wszystkie kamery. |

### Tworzenie wyzwalaczy opartych na wejściach/wyjściach

Wyzwalacz oparty na wejściu/wyjściu (we/wy) aktywuje się, gdy port we/wy urządzenia odbierze sygnał na przykład z połączonych drzwi, czujki dymu lub przełącznika.

Uwaga

- Dodaj port WE/WY do AXIS Camera Station 5, zanim użyjesz wyzwalacza WE/WY. Patrz *Porty we/wy*.
- Jeśli jest taka możliwość, używaj wyzwalaczy opartych na zdarzeniach w urządzeniu zamiast wyzwalaczy wejścia/wyjścia. Wyzwalacze oparte na zdarzeniach w urządzeniu zapewniają lepsze ogólne wrażenia użytkownika. Więcej informacji: *Tworzenie wyzwalaczy opartych na zdarzeniach w urządzeniu, on page 88*.

Aby utworzyć wyzwalacz oparty na wejściu/wyjściu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i zaznacz opcję **Input/Output (Wejście/Wyjście)**.
4. Kliknij **OK**.
5. W obszarze **Trigger port and state (Port i stan wyzwalacza)** skonfiguruj ustawienia portu we/wy i wyzwalacza.
6. Kliknij **OK**.

| Port i stan wyzwalacza | |
|---|---|
| **Port we/wy** | W polu **I/O port (Port we/wy)** zaznacz port wejściowy lub wyjściowy. |
| **Trigger state (Stan wyzwalacza)** | W polu **Trigger state (Stan wyzwalacza)** zaznacz stan portu we/wy, który ma powodować aktywowanie wyzwalacza. Dostępne stany zależą od konfiguracji portu. |
| **Trigger period (Okres wyzwalacza)** | W polu **Trigger period (Czas wyzwalania)** ustaw odstęp czasu pomiędzy kolejnymi wyzwalaczami, aby zmniejszyć liczbę następujących po sobie zapisów.<br><br>Jeśli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, nagrywanie będzie kontynuowane, a okres wyzwalania zostanie uruchomiony ponownie. |

**Tworzenie wyzwalaczy opartych na zdarzeniach w urządzeniu**

Ten wyzwalacz wykorzystuje zdarzenia bezpośrednio z kamery lub urządzenia dodatkowego. Użyj tej opcji, jeśli w AXIS Camera Station 5 nie ma odpowiedniego wyzwalacza. Zdarzenia różnią się w zależności od kamery i mają co najmniej jeden filtr, który należy ustawić. Filtry to warunki, które muszą zostać spełnione, aby aktywował się wyzwalacz zdarzeń. Informacje o zdarzeniach i filtrach dla produktów Axis można znaleźć w dokumentacji VAPIX® dostępnej w witrynach *axis.com/partners* i *axis.com/vapix*

Aby utworzyć wyzwalacz zdarzeń w urządzeniu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Device event (Zdarzenie urządzenia)**.
4. Kliknij **OK**.
5. Skonfiguruj wyzwalacz zdarzeń w obszarze **Configure device event trigger (Konfiguracja wyzwalacza zdarzeń w urządzeniu)**.

Uwaga

Dostępne zdarzenia zależą od wybranego urządzenia. W przypadku urządzeń innych firm wiele z tych zdarzeń wymaga skonfigurowania dodatkowych opcji w urządzeniu.

6. W obszarze **Filters (Filtry)** wybierz filtry.
7. W obszarze **Activity (Aktywność)**, sprawdź aktualny stan wyzwalacza zdarzeń w urządzeniu jako funkcję czasu. Zdarzenie może mieć stan lub nie mieć stanu. Aktywność zdarzenia ze stanem jest reprezentowana przez funkcję kroku. Linia prosta z impulsami od momentu wyzwolenia zdarzenia odzwierciedla aktywność zdarzenia bez stanu.
8. Kliknij **OK**.

| Konfiguracja wyzwalacza zdarzeń na urządzeniu | |
|---|---|
| **Urządzenie** | W polu **Device (Urządzenie)** wybierz kamerę lub urządzenie dodatkowe. |
| **Zdarzenie** | W polu **Event (Zdarzenie)** wybierz zdarzenie, które ma być używane jako wyzwalacz. |
| **Trigger period (Okres wyzwalacza)** | W polu **Trigger period (Czas wyzwalania)** ustaw odstęp czasu pomiędzy kolejnymi wyzwalaczami, aby zmniejszyć liczbę następujących po sobie zapisów.<br><br>Jeśli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, nagrywanie będzie kontynuowane, a okres wyzwalania zostanie uruchomiony ponownie. |

**Przykłady zdarzeń na urządzeniach**

| **Kategoria** | **Zdarzenie z urządzenia** |
|---|---|
| Wzmacniacz | Przeciążenie wzmacniacza |
| Sterowanie dźwiękiem | Status sygnału cyfrowego |
| Źródło dźwięku | Detekcja dźwięku |
| Authorization (Autoryzacja) | Żądanie dostępu zaakceptowane |
| | Żądanie dostępu odrzucone |
| Nawiąż połączenie | Status |
| | Zmiana stanu |
| | Jakość sieci |
| | Status konta SIP |
| | Przychodzące wideo |
| Obudowa | Otwarcie obudowy |
| Urządzenie | Zabezpieczenie nadprądowe w obwodzie pierścieniowym |
| Czujniki urządzenia | System gotowy |
| | Czujnik PIR |
| Status urządzeń | System gotowy |
| Drzwi | Drzwi wyważone |
| | Wykryto ingerencję w instalację drzwiową |
| | Drzwi zamknięte |
| | Przekroczony czas otwarcia drzwi |
| | Położenie drzwi |
| | Drzwi odblokowane |
| Bufor zdarzeń | Rozpoczęcie |
| Dziennik zdarzeń | Pominięte alarmy |

| | |
|---|---|
| | Pominięte zdarzenia |
| | Alarm |
| Wentylator | Status |
| Globalna zmiana sceny | Usługa obrazu |
| Awaria sprzętu | Błąd pamięci masowej |
| | Awaria wentylatora |
| Moduł grzewczy | Status |
| Input ports (Porty wejścia) | Wejście wirtualne |
| | Cyfrowy port wejścia |
| | Wyzwalacz ręczny |
| | Nadzorowany port wejścia |
| | Cyfrowy port wyjścia |
| | Wejście sygnału zewnętrznego |
| Oświetlenie | Status |
| Stan oświetlenia uległ zmianie | Status |
| Media | Profil uległ zmianie |
| | Konfiguracja uległa zmianie |
| Monitowanie | Zmiana stanu |
| Detektor ruchu w regionie | Ruch |
| Sieć | Utrata połączenia sieciowego<br><br>Ma zastosowanie tylko do zdarzeń używanych w urządzeniu, a nie zdarzeń używanych w AXIS Camera Station 5. |
| | Dodano adres |
| | Usunięto adres |
| Ruch PTZ | Ruch PTZ na kanale <nazwa kanału> |
| Prepozycje PTZ | Osiągnięta prepozycja PTZ na kanale <nazwa kanału> |
| Kontroler PTZ | Automatyczne śledzenie ruchu |
| | Kolejka sterowania PTZ |
| | Błąd PTZ |
| | PTZ gotowe |
| Konfiguracja nagrywania | Utwórz zapis |
| | Usuń zapis |
| | Konfiguracja śledzenia |
| | Konfiguracja nagrywania |

| | |
|---|---|
| | Konfiguracja zadania nagrywania |
| Zdalna kamera | Status interfejsu Vapix |
| | Pozycja PTZ |
| Schedule | Impuls |
| | Interwał |
| | Zaplanowane wydarzenie |
| Status | Aktywne |
| Przechowywanie | Problem z pamięcią masową |
| | Trwa rejestracja |
| Komunikat systemowy | Nie udało się wykonać działania |
| Sabotaż | Wykryto pochylenie |
| | Wykryto wstrząs |
| Czujniki temperatury | Powyżej temperatury roboczej |
| | Poniżej temperatury roboczej |
| | W granicach temperatury roboczej |
| | Powyżej lub poniżej temperatury roboczej |
| Wyzwalacz | Przekaźniki i wyjścia |
| | Wejście cyfrowe |
| Wizyjna detekcja ruchu | VMD 4: profil <nazwa profilu> |
| | VMD 4: dowolny profil |
| Video Motion Detection 3 | VMD 3 |
| Źródło wideo | Ostrzeżenie o ruchu |
| | Dostęp do strumienia podglądu na żywo |
| | Tryb dzienny/nocny |
| | Sabotaż kamery |
| | Średnia degradacja przepływności bitowej |
| | Podłączenie źródła wideo |

**Zdarzenia w urządzeniu sieciowy kontroler drzwiowy Axis**

| Zdarzenie z urządzenia | Wyzwalanie reguły akcji |
|---|---|
| **Authorization (Autoryzacja)** | |
| Żądanie dostępu zaakceptowane | System przyznał dostęp posiadaczowi karty, gdy zidentyfikował go przy użyciu swoich danych uwierzytelniających. |
| Zagrożenie | Ktoś użył numeru PIN na wypadek zagrożenia. Można go użyć na przykład do wyzwolenia cichego alarmu. |

| | |
|---|---|
| Żądanie dostępu odrzucone | System odmówił dostępu posiadaczowi karty, gdy zidentyfikował go przy użyciu swoich danych uwierzytelniających. |
| Wykrycie Anti-passback | Ktoś użył poświadczeń należących do posiadacza karty, który wszedł do strefy przed nim. |
| **Obudowa** | |
| Otwarcie obudowy | Po usunięciu lub otwarciu obudowy sieciowego kontrolera drzwi. Opcji tej można użyć na przykład do wysłania powiadomienia do administratora o otwarciu obudowy na potrzeby konserwacji lub w przypadku prób sabotażu. |
| **Status urządzeń** | |
| System gotowy | Gdy system znajdzie się w stanie gotowości. Produkt Axis może wykryć na przykład stan sytemu i wysłać powiadomienie do administratora o jego uruchomieniu. Zaznacz przycisk opcji **Tak**, aby wyzwolić regułę akcji po wejściu produktu w stan gotowości. Reguła ta zostanie wyzwolona tylko wtedy, gdy uruchomione zostaną wszystkie wymagane urządzenia, takie jak system wykrywania zdarzeń. |
| **Drzwi** | |
| Drzwi wyważone | Po siłowym otwarciu drzwi. |
| Wykryto ingerencję w instalację drzwiową | Gdy system wykryje następujące:<br>• Otwarcie lub zamknięcie obudowy urządzenia<br>• Ruch urządzenia<br>• Zdjęcie podłączonego czytnika ze ściany<br>• Ingerencja w podłączony monitor drzwi, czytnik lub urządzenie REX. Aby użyć tego wyzwalacza, należy się upewnić, że włączono opcję Nadzorowane wejście, a rezystory końcowe zamontowano na odpowiednich portach wejścia złącza drzwi. |
| Drzwi zamknięte | Zablokowanie zamka drzwi. |
| Przekroczony czas otwarcia drzwi | Drzwi są otwarte zbyt długo. |
| Położenie drzwi | Monitor drzwi wskazuje, że drzwi są otwarte lub zamknięte. |
| Drzwi odblokowane | Zamek drzwi pozostaje odblokowany. Tego stanu można używać na przykład wtedy, gdy istnieją odwiedzający, którzy powinni mieć możliwość otwierania drzwi bez okazywania poświadczeń. |
| **Input ports (Porty wejścia)** | |
| Wejście wirtualne | Zmianie stanu jednego z wejść wirtualnych. Może być używany przez klienta, takiego jak oprogramowanie zarządzające, do inicjowania różnych działań. Wybierz port wejściowy, który ma wyzwalać regułę akcji po jego uaktywnieniu. |
| Cyfrowy port wejścia | Zmiana stanu cyfrowego portu wejścia. Tego wyzwalacza można używać do inicjowania różnych działań, na przykład wysłania powiadomienia czy błyśnięcia diodą LED stanu. Zaznacz port wejściowy, który ma wyzwalać regułę akcji po jej uaktywnieniu, lub opcję **Any (Dowolne)**, aby reguła działania była wyzwala po aktywacji któregokolwiek portu wejścia. |

| | |
|---|---|
| Wyzwalacz ręczny | Aktywuje wyzwalacz ręczny. Tego wyzwalacza można używać do ręcznego uruchamiania lub zatrzymywania reguł akcji za pośrednictwem interfejsu API VAPIX. |
| Wejście sygnału zewnętrznego | Aktywacja lub dezaktywacja wejścia awaryjnego. |
| **Sieć** | |
| Utrata połączenia sieciowego | Sieć traci połączenie sieciowe.<br><br>Ma zastosowanie tylko do zdarzeń używanych w urządzeniu, a nie zdarzeń używanych w AXIS Camera Station 5. |
| Dodano adres | Dodanie nowego adresu IP. |
| Usunięto adres | Usunięcie adresu IP. |
| **Schedule** | |
| Zaplanowane wydarzenie | Zmiana stanu we wstępnie zdefiniowanym harmonogramie. Służy do nagrywania obrazu wideo w określonych przedziałach czasowych, na przykład w godzinach pracy, w weekendy itp. Zaznacz harmonogram w rozwijalnym menu **Schedule (Harmonogram)**. |
| **Komunikat systemowy** | |
| Nie udało się wykonać działania | Nieudane wykonanie reguły akcji oraz wyświetleniu komunikatu systemowego Nie udało się wykonać działania. |
| **Wyzwalacz** | |
| Wejścia cyfrowego | Aktywacja lub dezaktywacja fizycznego cyfrowego portu wejściowego. |

**Tworzenie wyzwalaczy opartych na przyciskach akcji**

Przyciski akcji służą do rozpoczynania i zatrzymywania działań w **Live view (podglądzie na żywo)**. Przyciski akcji są wyświetlane u dołu okna dole podglądu na żywo lub na mapie. Do wielu kamer i map można używać jednego przycisku, a także dla jednej kamery lub mapy można używać wielu przycisków akcji. Przyciski akcji można rozmieścić podczas ich dodawania lub edytowania.

Istnieją dwa rodzaje przycisków akcji:

**Przyciski polecenia –** Służą do ręcznego uruchamiania akcji. Przycisków poleceń należy używać do akcji, które nie wymagają przycisku zatrzymania. Przycisk polecenia ma etykietę i podpowiedź. Etykieta przycisku to tekst wyświetlany na przycisku. Najedź kursorem myszy na przycisk, aby wyświetlić podpowiedź.

**Przykład:** Utwórz przycisk aktywacji wyjścia o wstępnie zdefiniowanej godzinie, uruchomienia alarmu i wysłania wiadomości e-mail.

**Przyciski dwustanowe –** Służą do ręcznego uruchamiania i zatrzymywania akcji. Przycisk ma dwa stany: przełączenie i wyłączenie. Kliknięcie przycisku powoduje przełączenie między tymi dwoma stanami. Przyciski dwustanowe domyślnie uruchamiają akcję w stanie aktywnym, ale mogą również uruchomiać ją w stanie nieaktywnym.

Przycisk przełączania ma etykietę stanu aktywnego, etykietę stanu nieaktywnego i podpowiedź. Teksty wyświetlane na przyciskach w stanach aktywnym i nieaktywnym są etykietami stanów aktywnego i nieaktywnego. Najedź kursorem myszy na przycisk, aby wyświetlić podpowiedź.

**Przykład:** Utwórz przycisk do otwierania i zamykania drzwi, użyj akcji wyjściowej z impulsem ustawionym na „przez czas, kiedy aktywny jest dowolny wyzwalacz".

Aby utworzyć wyzwalacz przycisku akcji:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Action Button (Przycisk akcji)**.
4. Kliknij **OK**.
5. Wybierz opcję **Create new button (Utwórz nowy przycisk)** lub **Use existing button (Użyj istniejącego przycisku)**. Kliknij **Next (Dalej)**.
6. Jeżeli wybierzesz opcję **Create new button (Utwórz nowy przycisk)**:
   6.1. Wybierz opcję **Command button (Przycisk polecenia)** lub **Toggle button (Przycisk dwustanowy)**. Jeżeli przycisk przełączania ma inicjować czynność w stanie nieaktywnym, zaznacz opcję **Trigger on untoggle (Wyzwól przy zmianie stanu na nieaktywny)**.
   6.2. Kliknij **Next (Dalej)**.
   6.3. Dodaj etykiety i podpowiedź dla przycisku.

Uwaga

Litera lub cyfra po pierwszym znaku podkreślenia w etykiecie przycisku akcji staje się klawiszem dostępu do przycisku akcji. Naciśnij klawisz ALT i klawisz dostępu, aby aktywować przycisk akcji. Na przykład jeśli przycisk akcji otrzyma nazwę A_BC, w podglądzie na żywo jego nazwa zmieni się na ABC. Naciśnij klawisze ALT + B, a przycisk akcji zostanie aktywowany.

7. Jeżeli wybrano opcję **Use existing button (Użyj istniejącego przycisku)**:
   7.1. Wyszukaj lub kliknij przycisk, którego chcesz użyć.
   7.2. Jeżeli wybrano używanie istniejącego przycisku przełączania, trzeba zaznaczyć opcję **Trigger on toggle (Wyzwól przy zmianie stanu na aktywny)** lub **Trigger on untoggle (Wyzwól przy zmianie stanu na nieaktywny)**.
   7.3. Kliknij przycisk **Next (Dalej)**.
   7.4. Zmodyfikuj etykietę i podpowiedź przycisku.
8. Wybierz kamerę lub mapę z menu rozwijanego.
9. Aby dodać przycisk do wielu kamer lub map, kliknij opcję **Add to multiple cameras (Dodaj do wielu kamer)** lub **Add to multiple maps (Dodaj do wielu map)**.
10. Jeżeli kamera ma kilka przycisków akcji, kliknij przycisk **Arrange (Rozmieść)** i edytować kolejność przycisków. Kliknij **OK**.
11. Kliknij **Next (Dalej)**.

**Tworzenie wyzwalaczy zdarzeń aplikacji AXIS Entry Manager**

AXIS Camera Station 5 aktywuje wyzwalacz po odebraniu sygnałów z drzwi skonfigurowanych w aplikacji AXIS Entry Manager. Na przykład otwarcie drzwi siłą, otwarte zbyt długo lub odmowa dostępu.

Uwaga

Funkcja wyzwalania zdarzeń aplikacji AXIS Entry Manager jest dostępna tylko po dodaniu do AXIS Camera Station 5 sieciowego kontrolera drzwi AXIS A1001 Network Door Controller.

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i zaznacz pozycję **AXIS Entry Manager event (Zdarzenie aplikacji AXIS Entry Manager)**.
4. Kliknij **OK**.
5. Wybierz zdarzenie oraz drzwi, które mają powodować aktywację wyzwalacza.
6. Kliknij **OK**.

**Tworzenie wyzwalaczy opartych na zewnętrznych połączeniach HTTPS**

Wyzwalacz oparty na zewnętrznym połączeniu HTTPS umożliwia zewnętrznym aplikacjom wyzwalanie zdarzeń w aplikacji AXIS Camera Station 5 poprzez wysłanie komunikatu połączeniem HTTPS. Ten wyzwalacz obsługuje tylko komunikację za pomocą protokołu HTTPS i wymaga, aby w żądaniu HTTPS podać prawidłową nazwę użytkownika aplikacji AXIS Camera Station 5, w tym nazwę domeny i hasło.

Metoda HTTP GET* obsługuje żądania wymienione poniżej. Można również używać metody POST z danymi JSON rozpoczynającymi się w treści żądania.

Uwaga

- Żądania wyzwalaczy zewnętrznych połączeń HTTPS można testować tylko w przeglądarce Google Chrome.
- Wyzwalacz oparty na zewnętrznym połączeniu HTTPS używa tych samych portów, co mobilna aplikacja do przeglądania obrazu. Zobacz omówienie portów komunikacji mobilnej i strumieniowania mobilnego w temacie *Zapisy ogólne*.
- Aktywacja wyzwalacza o identyfikatorze „trigger1": `https://[address]:55756/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Dezaktywacja wyzwalacza o identyfikatorze „trigger1": `https://[address]:55756/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Aktywacja wyzwalacza o identyfikatorze „trigger1", a następnie jego automatyczna dezaktywacja po 30 sekundach: `https://[address]:55756/Acs/Api/TriggerFacade/ActivateDeactivateTrigger?{"triggerName":"trigger1","deactivateAfterSeconds":"30"}`

Uwaga

Czasomierz automatycznej dezaktywacji zostanie wyzerowany w przypadku wysłania jakiegokolwiek innego polecenia do tego samego wyzwalacza.

- Pulsacyjne uruchomienie wyzwalacza o identyfikatorze „trigger1" (aktywacja wyzwalacza, po czym natychmiastowa jego dezaktywacja): `https://[address]:55756/Acs/Api/TriggerFacade/PulseTrigger?{"triggerName":"trigger1"}`

Aby utworzyć wyzwalacz zewnętrznego połączenia HTTPS:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij opcję **New (Nowa)**.
3. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **External HTTPS (Zewnętrzne połączenie HTTPS)**.
4. Kliknij **OK**.
5. W polu **Trigger name (Nazwa wyzwalacza)** nadaj wyzwalaczowi nazwę.
6. Spójrz na przykładowy adres URL, w którym adres serwera jest taki sam, jak adres klienta użyty podczas logowania. Adresy URL będą działać poprawnie dopiero po wykonaniu całej reguły akcji.
7. Kliknij przycisk **OK**.

**Działania obsługiwane przez wyzwalacze zewnętrznych połączeń HTTPS**

- Żądania aktywacji i dezaktywacji wyzwalacza są obsługiwane w akcjach powodujących rozpoczęcie i zatrzymanie nagrywania.
- Żądania pulsacyjnego uruchomienia wyzwalacza są obsługiwane w akcjach takich jak **Raise Alarm (Zgłoś alarm)** i **Send Email (Wyślij wiadomość e-mail)**.

## Dodawanie działań

Do jednej reguły można przypisać wiele akcji. Początkiem akcji jest moment aktywacji reguły.

Dostępne są następujące akcje:

**Rejestrowanie –** To działanie rozpoczyna nagrywanie przez kamerę. Patrz *Tworzenie akcji nagrywania*.

**Uruchom alarm –** Ta akcja powoduje wysłanie alarmu do wszystkich połączonych klientów AXIS Camera Station 5. Patrz *Tworzenie akcji zgłaszania alarmów*.

**Ustaw wyjście –** Ta akcja ustawia stan portu wyjścia. Służy do kontrolowania urządzenia podłączonego do portu wyjścia, na przykład do włączania oświetlenia albo blokowania drzwi. Patrz *Tworzenie akcji wyjściowych*.

**Wyślij wiadomość e-mail –** Ta akcja powoduje wysłanie wiadomości e-mail do jednego lub wielu adresatów. Patrz *Tworzenie akcji wysyłania wiadomości e-mail*.

**Wyślij zapytanie HTTP –** Ta akcja powoduje wysłanie żądania HTTP do kamery, kontrolera drzwi lub zewnętrznego serwera internetowego. Patrz *Tworzenie akcji wysyłania powiadomień HTTP*.

**Syrena i światło –** Działanie to uruchamia sygnalizator akustyczny i sekwencję sygnalizacji optycznej na kompatybilnym urządzeniu zgodnie ze skonfigurowanym profilem. Patrz *Tworzenie akcji syreny i światła, on page 101*.

**AXIS Entry Manager –** Ta czynność umożliwia przyznanie dostępu albo odblokowanie lub zablokowanie drzwi połączonych z kontrolerem drzwi skonfigurowanym przez program AXIS Entry Manager. Patrz *Tworzenie akcji aplikacji AXIS Entry Manager, on page 102*.

**Wyślij powiadomienie do aplikacji mobilnej –** Ta akcja powoduje wysłanie niestandardowego komunikatu do aplikacji mobilnej AXIS Camera Station. Patrz *Tworzenie akcji wysyłania powiadomień do aplikacji mobilnej, on page 102*.

**Włącz lub wyłącz reguły –** Ta akcja służy do włączania lub wyłączania innych reguł akcji. Patrz *Tworzenie akcji, która włącza lub wyłącza inne reguły akcji, on page 103*.

**Wysyłanie do dekodera wideo –** Ta akcja umożliwia wysłanie obszaru obserwacji do dekodera wideo w celu wyświetlenia go na monitorze przez określony czas. Patrz

**Kontrola dostępu –** To działanie obejmuje akcje dotyczące drzwi i stref występujące w aplikacji AXIS Camera Station Secure Entry. Patrz *Tworzenie akcji kontroli dostępu, on page 103*.

### Tworzenie akcji nagrywania

Akcja nagrywania rozpoczyna rejestrowanie obrazu z kamery. Uzyskaj dostęp do nagrania na karcie **Recordings (Nagrania)** i zacznij odtwarzanie.

Aby utworzyć akcję nagrywania:

1. Określ lokalizację zapisu nagrania, przejdź do **Configuration > Storage > Selection (Konfiguracja > Pamięć > Wybór)**.
2. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
3. Kliknij **New** (Nowy).
4. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
5. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Record (Rejestruj)**.
6. Kliknij **OK**.
7. W **Camera (Kamera)** wybierz kamerę, z której obraz ma być nagrywany.
8. W obszarze **Video setting (Ustawienia wideo)** skonfiguruj profil, buforowanie przed zdarzeniem oraz po zdarzeniu.
9. Kliknij przycisk **OK**.

| Video setting | |
|---|---|
| **Profil** | Z menu rozwijanego wybierz **Profile (Profil)**. Aby zmodyfikować ustawienia profilu, patrz *Profile strumienia*. |
| **Bufor przed zdarzeniem** | Ustaw, ile sekund przed wykrytym ruchem ma zostać zarejestrowanych na nagraniu. |
| **Bufor po zdarzeniu** | Ustawi, ile sekund ma zostać zarejestrowanych na nagraniu po zakończeniu zdarzenia. |

**Tworzenie akcji zgłaszania alarmów**

Akcja uruchomienia alarmu powoduje wysłanie alarmu do wszystkich połączonych klientów AXIS Camera Station 5. Alarm zostanie wyświetlony na karcie **Alarms (Alarmy)** oraz jako powiadomienie na pasku zadań. Do alarmu można dołączyć plik z instrukcjami postępowania w razie alarmu. Procedura alarmowa jest dostępna na kartach **Alarms (Alarmy)** i **Logs (Dzienniki)**.

Aby utworzyć akcję zgłaszania alarmu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i zaznacz opcję **Raise alarm (Zgłoś alarm)**.
5. Kliknij **OK**.
6. W menu **Alarm message (Komunikat alarmu)** skonfiguruj tytuł, opis i czas trwania.
7. W menu **Alarm procedure (Procedura alarmowa)**.
   7.1. Zaznacz opcję **On alarm show alarm procedure (W przypadku alarmu pokaż procedurę alarmową)**.
   7.2. Kliknij przycisk **Upload (Prześlij)** i znajdź odpowiedni plik.
   7.3. Kliknij przycisk **Preview (Podgląd)**, a przesłany plik zostanie otwarty w oknie podglądu.
   7.4. Kliknij **OK**.

| Komunikat alarmowy | |
|---|---|
| **Tytuł** | Nadaj alarmowi tytuł. Tytuł jest wyświetlany w menu **Alarms (Alarmy)** na karcie **Alarms (Alarmy)** i w powiadomieniach paska zadań. |
| **Opis** | Wprowadź opis alarmu. Opis zostanie wyświetlony w menu **Alarms > Description (Alarmy > Opis)** na karcie **Alarms (Alarmy)** i w powiadomieniach paska zadań. |
| **Duration (Czas trwania w sekundach)** | Dla alarmu wyświetlanego w postaci wyskakującego okna ustaw czas trwania w zakresie od 1 do 600 sekund. |

**Tworzenie akcji wyjściowych**

Działanie wyjściowe ustawia stan portu wyjścia. Służy do kontrolowania urządzenia podłączonego do portu wyjścia, na przykład do włączania oświetlenia albo blokowania drzwi.

Uwaga

Dodaj port wyjścia do AXIS Camera Station 5, zanim użyjesz akcji wyjścia. Patrz *Porty we/wy*.

Aby utworzyć działanie wyjściowe:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Set output (Ustaw wyjście)**.
5. Kliknij **OK**.
6. W polu **Output port (Port wyjściowy)** wybierz port wyjścia.
7. W polu **State on action (Stan działania)** zaznacz stan, jaki ma zostać ustawiony dla portu. Dostępne opcje zależą od konfiguracji portu.
8. W polu **Pulse (Pulsowanie)** określ, jak długo port wyjścia ma pozostawać w nowym stanie.

Uwaga

Aby port pozostawał w nowym stanie nawet po zakończeniu działania, wyczyść opcję **Pulse (Pulsowanie)**.

9. Kliknij **OK**.

| | |
|---|---|
| **For as long as any trigger is active (Przez czas, kiedy aktywny jest dowolny wyzwalacz)** | Aby port znajdował się w nowym stanie przez cały czas aktywności wszystkich wyzwalaczy zdefiniowanych w regule, zaznacz opcję **For as long as any trigger is active (Przez czas, kiedy aktywny jest dowolny wyzwalacz)**. |
| Utrzymywanie stanu przez ustalony czas | Aby port pozostawał w nowym stanie przez ustalony czas, zaznacz drugą opcję i podaj liczbę sekund. |

**Tworzenie akcji wysyłania wiadomości e-mail**

Działanie e-mail powoduje wysłanie wiadomości e-mail do jednego lub wielu odbiorców. Do wiadomości e-mail można załączać ujęcia z kamer.

Uwaga

Wysyłanie wiadomości e-mail wymaga skonfigurowania serwera SMTP. Patrz *Ustawienia serwera*.

Aby utworzyć akcję wysyłania wiadomości e-mail:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Send email (Wyślij wiadomość e-mail)**.
5. Kliknij **OK**.
6. Dodaj odbiorców w obszarze **Recipients (Odbiorcy)**:
   6.1. Wprowadź adres e-mail w polu **New Recipient (Nowy odbiorca)**, a następnie zaznacz opcję **To (Do)**, **Cc (DW)** lub **Bcc (UDW)**.
   6.2. Kliknij przycisk **Add (Dodaj)**, a adres e-mail zostanie dodany do pola **Recipients (Odbiorcy)**.
7. W obszarze **Contents (Treść)** wpisz temat i treść wiadomości e-mail.
8. W obszarze **Advanced (Zaawansowane)** skonfiguruj załączniki, liczbę wiadomości e-mail i interwały.
9. Kliknij przycisk **OK**.

| Zaawansowane | |
|---|---|
| **Attach snapshots (Dołącz ujęcia)** | Aby w powiadomieniu e-mail dołączyć ujęcia z kamer w postaci załączników w formacie .jpg, zaznacz opcję **Attach snapshots (Dołącz ujęcia)** i kliknij przycisk **Cameras (Kamery)**. Zostanie wyświetlona lista wszystkich kamer dodanych do AXIS Camera Station 5. Możesz użyć opcji **Select all (Zaznacz wszystko)**, aby zaznaczyć wszystkie kamery lub **Deselect all (Odznacz wszystko)**, aby odznaczyć wszystkie kamery. |
| **Send one email for each event (Wyślij jeden e-mail dla każdego zdarzenia)** | Aby zapobiec wysyłaniu wielu wiadomości e-mail o tym samym zdarzeniu, zaznacz opcję **Send one email for each event (Wyślij jeden e-mail dla każdego zdarzenia)**. |
| **Don't send another email for (Nie wysyłaj kolejnego e-maila dla)** | Aby zapobiec wysyłaniu wiadomości e-mail zbyt szybko jedna po drugiej, zaznacz opcję **Don't send another email for (Nie wysyłaj kolejnego e-maila dla)** i z rozwijalnego menu wybierz minimalny czas między wysłaniem kolejnych wiadomości e-mail. |

**Tworzenie działań podglądu na żywo**

Akcja podglądu na żywo powoduje otwarcie karty **Live view (Podgląd na żywo)** z określoną kamerą, widokiem lub prepozycją. Karta **Live view (Podgląd na żywo)** zostanie otwarta we wszystkich połączonych klientach AXIS Camera Station 5. Jeżeli karta **Live view (Podgląd na żywo)** wyświetla widok podzielony z aktywnym punktem, do punktu będzie wczytywany obraz z kamery wybranej w akcji Podgląd na żywo. Więcej informacji na temat aktywnych punktów: *Widok dzielony*.

Można również użyć akcji podglądu na żywo, aby przywrócić otwarte klienty AXIS Camera Station 5 z paska zadań lub przesunąć je na pierwszy plan względem okien innych otwartych aplikacji.

Aby utworzyć akcję podglądu na żywo:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Live view (Podgląd na żywo)**.
5. Kliknij **OK**.
6. W obszarze **Live view actions (Akcje widoku na żywo)** zdecyduj, co ma być wyświetlane po uruchomieniu akcji.
7. W obszarze **Shown in (Pokaż w)** zdecyduj, jak ma być wyświetlany wybrany widok.
8. W sekcji **Bring to front (Przesuń na wierzch)** zaznacz opcję **On trigger bring application to front (Po zadziałaniu wyzwalacza przesuń aplikację na wierzch)**, aby po rozpoczęciu akcji podglądu na żywo okna otwartych klientów AXIS Camera Station 5 były przywracane z paska zadań lub przenoszone na pierwszy plan względem okien innych otwartych aplikacji.
9. Kliknij **OK**.

| Akcje podglądu na żywo | |
|---|---|
| **Wyświetl** | Aby otworzyć widok, kliknij opcję **View (Widok)** i wybierz widok z rozwijalnego menu. |
| **Kamera** | Aby otworzyć kamerę, kliknij opcję **Camera (Kamera)** i wybierz kamerę z rozwijalnego menu. Jeżeli kamera ma zdefiniowaną prepozycję PTZ, kliknij opcję **Go to preset (Przejdź do prepozycji)** i wybierz obszar z rozwijalnego menu, aby otworzyć prepozycję. |
| **No action (Bez akcji)** | Wybierz opcję **No action (Bez akcji)**, aby nie otwierać żadnego widoku. |

| Shown in (Pokaż w) | |
|---|---|
| **Karta podglądu na żywo** | Wybierz opcję **Live alert tab (Karta alertu na żywo)**, aby otworzyć wybrany widok lub widok kamery na karcie **Live alert (Alert na żywo)**. |
| **Hotspot in view (Aktywny punkt w widoku)** | Wybierz opcję **Hotspot in view (Aktywny punkt w widoku)**, a następnie z rozwijalnego menu wybierz widok zawierający aktywny punkt. Jeżeli aktywny punkt jest widoczny w poglądzie na żywo po zainicjowaniu akcji, będzie w nim wyświetlony widok z kamery. |

**Przykład:**
Aby otworzyć kartę **Live view (Podgląd na żywo)**, przejdź do widoku aktywnego punktu i ustaw tam wyświetlanie widoku z kamery. W jednej regule akcji można skonfigurować dwa działania podglądu na żywo:

1. Utwórz akcję widoku na żywo wyświetlającą widok aktywnego punktu na karcie **Live alert (Alert na żywo)**.
   1.1. W obszarze **Live view actions (Akcje podglądu na żywo)** wybierz **View (Widok)**.
   1.2. Wybierz **Hotspot view (Widok aktywnego punktu)**.
   1.3. W obszarze **Show in (Pokaż w)** zaznacz opcję **Live alert tab (Karta alertu na żywo)**.
   1.4. Zaznacz opcję **On trigger bring application to front (Po zadziałaniu wyzwalacza przesuń aplikację na wierzch)**.
2. Utwórz kolejną akcję podglądu na żywo, tym razem powodującą przechodzenie do widoku aktywnego punktu i wyświetlanie w nim widoku z kamery.
   2.1. W obszarze **Live view actions (Akcje podglądu na żywo)** wybierz opcję **Camera (Kamera)** i wybierz widok kamery.
   2.2. W obszarze **Show in (Pokaż w)** wybierz **Hotspot in view (Aktywny punkt w widoku)**.
   2.3. Wybierz **Hotspot view (Widok aktywnego punktu)**.

**Tworzenie akcji wysyłania powiadomień HTTP**

Akcja wysyłania powiadomienia HTTP powoduje wysłanie żądania HTTP do odbiorcy. Odbiorcą może być kamera, kontroler drzwi, zewnętrzny serwer www lub dowolny serwer zdolny odbierać żądania HTTP. Powiadomienia HTTP mogą służyć na przykład do włączania i wyłączania funkcji w kamerze albo otwierania, zamykania, blokowania lub odblokowywania drzwi połączonych z kontrolerem drzwi.

Obsługiwane są metody GET, POST i PUT.

Uwaga

Aby powiadomienia HTTP były wysyłane do odbiorców spoza sieci lokalnej, może być konieczne dostosowanie ustawień serwera proxy AXIS Camera Station 5. Patrz *Zapisy ogólne*.

Aby utworzyć akcję wysyłania powiadomienia HTTP:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Send HTTP Notification (Wyślij zapytanie HTTP)**.
5. Kliknij **OK**.
6. W polu **URL** wprowadź adres odbiorcy oraz skrypt, który będzie odpowiadał za obsługę żądania. Przykład: `https://192.168.254.10/cgi-bin/notify.cgi`.
7. Jeżeli odbiorca wymaga uwierzytelniania, zaznacz opcję **Authentication required (Wymagane uwierzytelnienie)**. Wprowadź nazwę użytkownika oraz hasło.
8. Kliknij przycisk **Advanced (Zaawansowane)**, aby wyświetlić ustawienia zaawansowane.
9. Kliknij **OK**.

| Zaawansowane | |
|---|---|
| **Metoda** | Wybierz metodę HTTP z menu rozwijanego **Method (Metoda)**. |
| **Typ zawartości** | W przypadku metod POST i PUT przejdź do menu rozwijanego **Content type (Typ zawartości)** i wybierz rodzaj zawartości. |
| **Treść** | W przypadku metod POST i PUT w polu **Body (Treść)** wprowadź treść żądania. |
| **Trigger data (Dane wyzwalania)** | Z menu rozwijanego można także wstawić wstępnie zdefiniowane dane wyzwalacza. Zobacz niżej, aby dowiedzieć się więcej. |

| Trigger data (Dane wyzwalania) | |
|---|---|
| **Typ** | Wyzwalacz, który aktywował tę regułę akcji. |
| **Source ID (Identyfikator źródła)** | Identyfikator źródła jest identyfikatorem źródła, które wyzwoliło regułę akcji, i często reprezentuje kamerę lub inny typ urządzenia. Nie wszystkie źródła mają identyfikator źródła. |
| **Source Name (Nazwa źródła)** | Nazwa źródła jest nazwą źródła, które wyzwoliło regułę akcji, i często reprezentuje kamerę lub inny typ urządzenia. Nie wszystkie źródła mają nazwę źródła. |
| **Godzina (UTC)** | Podaje datę i godzinę UTC wyzwolenia reguły alarmu. |
| **Time (local) (Czas lokalny)** | Data i godzina wyzwolenia reguły akcji przez serwer. |

### Tworzenie akcji syreny i światła

Akcja syreny i światła powoduje aktywację schematu sygnałów dźwiękowych i świetlnych w sieciowej syrenie stroboskopowej AXIS D4100-E Network Strobe Siren zgodnie ze skonfigurowanym profilem.

Uwaga

Aby można było używać tej akcji, należy wcześniej utworzyć profil na stronie konfiguracyjnej urządzenia.

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Siren and light (Syrena i światło)**.
5. Kliknij **OK**.
6. Z menu rozwijanego **Device (Urządzenie)** wybierz urządzenie.
7. Z menu rozwijanego wybierz **Profile (Profil)**.
8. Kliknij **OK**.

**Tworzenie akcji aplikacji AXIS Entry Manager**

Akcja aplikacji AXIS Entry Manager może przyznawać dostęp oraz odblokowywać i blokować zamki drzwi połączonych z kontrolerem drzwi skonfigurowanym przez aplikację AXIS Entry Manager.

Uwaga

Akcja aplikacji AXIS Entry Manager jest dostępna tylko wtedy, gdy w AXIS Camera Station 5 jest dostępny sieciowy kontroler drzwi AXIS A1001 Network Door Controller.

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i zaznacz pozycję **AXIS Entry Manager (AXIS Entry Manager)**.
5. Kliknij **OK**.
6. Wybierz akcję oraz drzwi, na których ma ona być wykonywana.
7. Kliknij **OK**.

**Tworzenie akcji wysyłania powiadomień do aplikacji mobilnej**

Akcja Wyślij powiadomienie do aplikacji mobilnej powoduje wysłanie niestandardowego komunikatu do aplikacji mobilnej AXIS Camera Station. Można kliknąć, aby otrzymać powiadomienie i przejść do konkretnego widoku z kamery. Patrz *Instrukcja obsługi aplikacji mobilnej AXIS Camera Station*.

Aby utworzyć akcję wysyłania powiadomień do aplikacji mobilnej:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Send mobile app notification (Wyślij powiadomienie do aplikacji mobilnej)**.
5. Kliknij **OK**.
6. W polu **Message (Wiadomość)** wpisz wiadomość, która ma być wyświetlana w aplikacji mobilnej.
7. W obszarze **Click notification and go to (Kliknij powiadomienie i przejdź do)** określ, co ma być wyświetlane po kliknięciu powiadomienia.
8. Kliknij przycisk **OK**.

| Kliknij powiadomienie i przejdź do | |
|---|---|
| **Kamera** | Z menu rozwijanego **Camera (Kamera)** wybierz widok kamery, który powinien pojawić się po kliknięciu powiadomienia w aplikacji mobilnej. |
| **Domyślne** | Zaznacz opcję **Default (Domyślnie)**, aby kliknięcie powiadomienia w aplikacji komórkowej powodowało przejście do strony startowej aplikacji komórkowej. |

**Tworzenie akcji, która włącza lub wyłącza inne reguły akcji**

Użyj akcji włączania lub wyłączania reguł, na przykład aby wyłączyć wykrywanie ruchu w biurze, gdy pracownik przeciągnie kartę dostępu.

Aby utworzyć akcję włączania lub wyłączania reguł:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz **Turn rules on or off (Włącz lub wyłącz reguły)**.
5. Kliknij **OK**.
6. Wybierz co najmniej jedną regułę akcji.
7. Zdecyduj, czy wybrane reguły akcji mają być włączone, czy wyłączone.
8. Jeśli chcesz ustawić czas między wyzwalaniem a zmianą stanu, wprowadź wartość opóźnienia.
9. Wybierz opcję **Return to the previous state when the trigger is no longer active (Powrót do poprzedniego stanu, gdy wyzwalacz nie jest już aktywny)**, jeśli nie chcesz, aby wybrana reguła akcji pozostała zmieniona, gdy wyzwalacz nie jest aktywny. W powyższym przykładzie oznacza to, że detekcja ruchu włącza się ponownie, gdy pracownik wyjmie kartę dostępu z czytnika.
10. Kliknij przycisk **OK**.

**Tworzenie akcji kontroli dostępu**

Akcja kontroli dostępu może powodować wykonywanie następujących czynności w systemie AXIS Camera Station Secure Entry:

- **Akcje dotyczące drzwi:** przyznawanie dostępu oraz blokowanie, odblokowywanie i blokowanie ogólne wybranych drzwi.
- **Akcje dotyczące stref:** blokowanie, odblokowywanie lub blokowanie ogólne wybranych drzwi w wybranych strefach.

Uwaga

Akcja kontroli dostępu jest dostępna tylko w systemie AXIS Camera Station Secure Entry.

Aby utworzyć akcję kontroli dostępu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Kliknij przycisk **Add (Dodaj)** i utwórz wyzwalacz. Kliknij **Next (Dalej)**. Patrz *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Access control (Kontrola dostępu)**.
5. Kliknij **OK**.
6. Aby wykonać działania na drzwiach:

6.1. W obszarze **Kontrola dostępu** kliknij opcję **Działania drzwi**.

6.2. W obszarze **Skonfiguruj akcję** zaznacz drzwi i działanie.

7. Aby wykonać działania na strefach:
   7.1. W obszarze **Access control (Kontrola dostępu)** kliknij opcję **Zone actions (Działania stref)**.
   7.2. W obszarze **Configure action (Skonfiguruj akcję)** wybierz strefy, typy drzwi i akcję.
8. Kliknij **OK**.

### Harmonogramy

Strona Schedules (Harmonogramy) zawiera wszystkie harmonogramy, które można zastosować do nagrywania, reguł akcji i komponentów takich jak AXIS Secure Entry. AXIS Site Designer tworzy niektóre harmonogramy podczas instalacji.

Funkcja harmonogramów umożliwia tworzenie i edytowanie spersonalizowanych harmonogramów dziennych i tygodniowych, a także harmonogramów nadpisywania. Harmonogramy nadpisywania mają zawsze charakter dzienny, ale można je zastosować zarówno do harmonogramów dziennych, jak i tygodniowych przy wyjątkowych okazjach takich jak dni świąteczne.

Karta **Schedules (Harmonogramy)** to widok główny służący do zarządzania wszystkimi harmonogramami dziennymi i tygodniowymi:

- **Nazwa**: Nazwa harmonogramu.
- **Type (Typ)**: Wskazuje, czy harmonogram jest harmonogramem dziennym czy tygodniowym.
- **In use (W użyciu)**: Wskazuje, czy komponent, reguła nagrywania lub reguła akcji aktualnie korzysta z harmonogramu.
- **Override schedules (Harmonogramy zastępcze)**: Wyświetla listę harmonogramów zastępczych, które mają zastosowanie do tego harmonogramu.

Karta **Override schedules (Harmonogramy zastępcze)** to widok główny umożliwiający zarządzanie harmonogramami zastępczymi, w którym można zobaczyć, do których harmonogramów dziennych i tygodniowych zostały one zastosowane.

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można dodawać harmonogramy i zarządzać nimi na dowolnym połączonym serwerze. Wybierz serwer z rozwijalnego menu **Selected server (Wybrany serwer)**, aby zarządzać harmonogramami.

**Zarządzanie harmonogramami dziennymi i tygodniowymi**

Aby zarządzać harmonogramami dziennymi i tygodniowymi, przejdź na kartę **Schedules (Harmonogramy)**.

Aby utworzyć nowy harmonogram dzienny lub tygodniowy, kliknij **New schedule (Nowy harmonogram)**.

Aby usunąć harmonogram, wybierz go z listy i naciśnij **Delete (Usuń)**. Przed próbą usunięcia harmonogramu upewnij się, że nie jest on używany.

Utwórz lub wybierz harmonogram dzienny lub tygodniowy, aby wyświetlić jego szczegóły.

- Jeśli jest to harmonogram dzienny, kliknij **Add dates (Dodaj daty)**, aby dodać do niego nowy zakres dat. Do tego samego harmonogramu dziennego można dodać wiele zakresów dat.
- Aby dodać przedział czasu, kliknij **+** lub dwukrotnie kliknij wiersz.
- Aby edytować zakres dat lub przedział czasu, kliknij go lewym przyciskiem myszy.
- Aby dodać harmonogram zastępczy, wybierz go z rozwijalnego menu i kliknij **Add (Dodaj)**. Aby usunąć harmonogram zastępczy, wybierz go z listy i kliknij przycisk **Remove (Usuń)**.
- Kliknij **Apply (Zastosuj)**, aby zapisać zmiany.

**Zarządzanie harmonogramami zastępczymi**

- Aby zarządzać harmonogramami zastępczymi, przejdź na kartę **Override schedules (Harmonogramy zastępcze)**.
- Kliknij **Add dates (Dodaj daty)**, aby dodać nowy zakres dat do harmonogramu. Do tego samego harmonogramu zastępczego można dodać wiele zakresów dat.
- Aby dodać przedział czasu, kliknij **+** lub dwukrotnie kliknij wiersz.
- Aby edytować zakres dat lub przedział czasu, kliknij go lewym przyciskiem myszy.
- Kliknij **Apply (Zastosuj)**, aby zapisać zmiany.

## Przykłady reguł akcji

### Przykład: Drzwi wyważone

**Drzwi wyważone**

Przykład ustawienia w AXIS Camera Station 5 reguły akcji, która wyzwala nagrywanie i alarm, gdy ktoś sforsuje drzwi wejściowe.

Zanim zaczniesz:

- Zainstaluj sieciowy kontroler drzwiowy Axis. Patrz *Dodawanie urządzeń, on page 40*.
- Skonfiguruj kontroler drzwi. P. sekcja *Dodawanie drzwi, on page 138*.

Tworzenie reguły akcji:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Dodaj wyzwalacz zdarzenia Drzwi wyważone.
   3.1. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Device event (Zdarzenie urządzenia)**.
   3.2. Kliknij **OK**.
   3.3. Skonfiguruj ustawienia wyzwalacza w obszarze **Configure device event trigger (Konfiguracja wyzwalacza zdarzeń w urządzeniu)**.
   3.4. W obszarze **Filters (Filtry)** skonfiguruj ustawienia filtru.
   3.5. W obszarze **Activity (Aktywność)** upewnij się, że wyzwalacz pokazuje aktywność na linii sygnałowej.
   3.6. Kliknij **OK**.
4. Kliknij **Next (Dalej)**.
5. Dodaj akcję nagrywania.
   5.1. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Record (Rejestruj)**.
   5.2. Kliknij **OK**.
   5.3. W menu rozwijanym **Camera (Kamera)** wybierz kamerę.
   5.4. W obszarze **Video setting (Ustawienia wideo)** skonfiguruj profil, buforowanie przed zdarzeniem oraz po zdarzeniu.
   5.5. Kliknij **OK**.
6. Dodaj akcję zgłaszania alarmu.
   6.1. Kliknij przycisk **Add (Dodaj)** i zaznacz opcję **Raise alarm (Zgłoś alarm)**.
   6.2. Kliknij **OK**.
   6.3. W sekcji **Komunikat alarmowy** wprowadź tytuł i opis alarmu. Na przykład Główne wejście zostało otwarte siłą.
   6.4. Kliknij **OK**.
7. Kliknij przycisk **Next (Dalej)**, a w ustawieniu harmonogramu zaznacz opcję **Always (Zawsze)**.

8. Kliknij przycisk **Finish (Zakończ)**.

| Konfiguracja wyzwalacza zdarzeń na urządzeniu | |
|---|---|
| **Urządzenie** | W menu rozwijalnym **Device** (Urządzenie) wybierz sieciowy kontroler drzwiowy Axis. |
| **Zdarzenie** | W menu rozwijanym **Event (Zdarzenie)** wybierz kolejno opcje **Door > Door forced (Drzwi > Drzwi wyważone)**. |
| **Trigger period (Okres wyzwalacza)** | W polu **Trigger period (Okres wyzwalacza)** ustaw wartość 10 sekund. |

| Filtry | |
|---|---|
| **Nazwa drzwi** | Z menu rozwijanego **Door name (Nazwa drzwi)** wybierz drzwi. |
| **Status drzwi** | W menu rozwijanym **Door status (Status drzwi)** wybierz opcję **Forced (Otwarto siłą)**. |

| Video setting | |
|---|---|
| **Profil** | W menu rozwijanym **Profile (Profil)** wybierz opcję **High (Wysoki)**. |
| **Bufor przed zdarzeniem** | W polu **Prebuffer (Bufor przed zdarzeniem)** ustaw wartość 3 sekundy. |
| **Bufor po zdarzeniu** | W polu **Postbuffer (Bufor po zdarzeniu)** ustaw wartość 5 sekund. |

### Przykład: Gdy wchodzi ktoś ważny

**Gdy wchodzi ktoś ważny**

Przykład tworzenia w AXIS Camera Station 5 reguły akcji, która powoduje odtworzenie wiadomości powitalnej i wezwanie windy, gdy wejdzie ważna osoba.

Zanim zaczniesz:

- Zainstaluj i skonfiguruj sieciowy kontroler drzwiowy Axis i dodaj posiadaczy kart. Patrz *Konfigurowanie kontroli dostępu, on page 135* i *Zarządzanie dostępem, on page 160*.
- Zainstaluj sieciowe urządzenie dźwiękowe Axis oraz powiąż je z kamerą. Patrz *Profile strumienia, on page 47*.
- Zainstaluj moduł przekaźnikowy AXIS A9188 Network I/O Relay Module, podłącz wejścia i wyjścia do windy, a następnie dodaj porty WE/WY sieciowego modułu przekaźnikowego WE/WY do AXIS Camera Station 5. Patrz *Porty we/wy, on page 82*.

Tworzenie reguły akcji:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New** (Nowy).
3. Dodaj wyzwalacz zdarzenia w urządzeniu.
   3.1. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Device event (Zdarzenie urządzenia)**.
   3.2. Kliknij **OK**.

3.3. Skonfiguruj ustawienia zdarzeń w obszarze **Configure device event trigger (Konfiguracja wyzwalacza zdarzeń w urządzeniu)**.

3.4. W obszarze **Filters (Filtry)** skonfiguruj ustawienia filtru.

3.5. W obszarze **Activity (Aktywność)** upewnij się, że wyzwalacz pokazuje aktywność na linii sygnałowej.

3.6. Kliknij **OK**.

4. Kliknij **Next (Dalej)**.

5. Dodaj akcję Wyślij zapytanie HTTP, aby odtwarzać wiadomość powitalną.

5.1. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Send HTTP notification (Wyślij zapytanie HTTP)**.

5.2. Kliknij **OK**.

5.3. W polu **URL** wprowadź adres URL klipu dźwiękowego z wiadomością powitalną.

5.4. Zaznacz opcję **Authentication required (Wymagane uwierzytelnienie)**, a następnie wpisz nazwę użytkownika i hasło dostępu do urządzenia audio.

5.5. Kliknij **OK**.

6. Dodaj akcję Ustaw wyjście.

6.1. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Set output (Ustaw wyjście)**.

6.2. Kliknij **OK**.

6.3. W menu rozwijanym **Output port (Port wyjściowy)** zaznacz port wyjściowy modułu we/wy, który jest podłączony do windy.

6.4. W menu rozwijanym **State on action (Stan działania)** zaznacz stan modułu we/wy mający powodować wykonanie połączenia do windy.

6.5. Zaznacz opcję **Pulse (Pulsowanie)** i ustaw 60 sekund jako okres utrzymania portu w tym stanie.

6.6. Kliknij **OK**.

7. Kliknij przycisk **Next (Dalej)**, a w ustawieniu harmonogramu zaznacz opcję **Always (Zawsze)**.

8. Kliknij przycisk **Finish (Zakończ)**.

| Konfiguracja wyzwalacza zdarzeń na urządzeniu | |
|---|---|
| **Urządzenie** | W menu rozwijalnym **Device** (Urządzenie) wybierz sieciowy kontroler drzwiowy Axis. |
| **Zdarzenie** | W menu rozwijanym **Event (Zdarzenie)** wybierz kolejno opcje **Authorization > Access request granted (Autoryzacja > Żądanie dostępu zaakceptowane)**. |
| **Trigger period (Okres wyzwalacza)** | W polu **Trigger period (Okres wyzwalacza)** ustaw wartość 10 sekund. |

| Filtry | |
|---|---|
| **Nazwa drzwi** | Z menu rozwijanego **Door name (Nazwa drzwi)** wybierz drzwi. |
| **Door side (Strona drzwi)** | W menu rozwijanym **Door side (Strona drzwi)** wybierz stronę drzwi. |
| **Numer karty** | Zaznacz opcję **Card number (Numer karty)** i wpisz numer karty ważnej osoby. |

## Konfigurowanie klienta

Po wybraniu kolejno opcji **Configuration > Client (Konfiguracja > Klient)** można:

- Edytować ustawienia klienta, takie jak motyw i język. Patrz *Ustawienia klienta, on page 108*.
- Edytować ustawienia użytkownika, np. powiadomienia i opcje uruchamiania. Patrz *Ustawienia użytkownika, on page 109*.
- Edytować ustawienia wydajności strumieniowania specyficzne dla klienta, takie jak skalowanie wideo i dekodowanie sprzętowe. Patrz *Przesyłanie strumieniowe, on page 111*.

### Ustawienia klienta

Ustawienia te mają zastosowanie do wszystkich użytkowników aplikacji AXIS Camera Station 5 na komputerze. Wybierz kolejno **Configuration (Konfiguracja) > Client (Klient) > Client settings (Ustawienia klienta)**, aby skonfigurować ustawienia klienta AXIS Camera Station 5.

| Schemat | |
|---|---|
| **System, Light, Dark (Systemowy, Jasny, Ciemny)** | Wybierz wizualny motyw przewodni interfejsu klienta. Domyślnym motywem dla nowych instalacji jest **System (Systemowy)**.<br><br>W przypadku wybrania opcji **System (Systemowy)** system używa jasnego lub ciemnego motywu w zależności od motywu systemu Windows. |

| Zapisy ogólne | |
|---|---|
| **Uruchom aplikację po uruchomieniu systemu Windows** | Włącz, jeśli chcesz, by strona AXIS Camera Station 5 była automatycznie uruchamiana po każdym uruchomieniu systemu Windows. |

| Podgląd na żywo | |
|---|---|
| **Pokaż nazwy kamer w podglądach na żywo** | Wyświetlanie nazwy kamery w podglądzie na żywo. |
|  | Aby wskazać typ nagrywania, włącz opcję **Show recording indicators in live views and maps (Pokaż wskaźniki rejestracji w widokach na żywo i w mapach)**. |
|  | Aby wskazać nagranie z detekcji ruchu lub nagrania rozpoczęte przez regułę akcji, włącz opcję **Show event indicators in live views and maps (Pokaż wskaźniki zdarzeń w podglądach na żywo i mapach)**. |

| Mapy | |
|---|---|
| **Allow flashing coverage areas for all maps (Zezwalaj na migające obszary pokrycia dla wszystkich map)** | Globalnego blokowanie migania lub zezwalania na miganie wszystkich obszarów objętych zasięgiem za pomocą opcji **Flash (Miganie)**. To ustawienie globalne nie wpływa na ustawienia lokalne na poziomie mapy. Patrz *Mapa, on page 19*. |

| Język |
|---|
| Zmiana języka klienta AXIS Camera Station 5. Zmiana zaczyna obowiązywać po zrestartowaniu klienta. |

| Informacja zwrotna | |
|---|---|
| **Share anonymous client usage data with Axis Communications to help improve the application and user experience (Przesyłaj do Axis Communications anonimowe dane dotyczące użytkowania klienta, co pomoże nam usprawniać aplikację i korzystanie z niej)** | Pozwala udostępniać firmie Axis anonimowe dane w celu ich wykorzystywania do poprawy jakości jej produktów konsumenckich. Jak zmienić opcję serwera: *Ustawienia serwera, on page 116*. |

### Ustawienia użytkownika

Te ustawienia dotyczą użytkowników zalogowanych w aplikacji AXIS Camera Station 5. Wybierz kolejno **Configuration (Konfiguracja) > Client (Klient) > User settings (Ustawienia użytkownika)**, aby skonfigurować ustawienia użytkownika klienta AXIS Camera Station 5.

| System nawigacji | |
|---|---|
| **System nawigacji z widokiem drzewka** | Włącza się domyślnie, aby uruchomić panel nawigacji widoku drzewa z widokami i kamerami. |
| **Show in navigation (Pokaż w nawigacji)** | Wybierz, czy w rozwijalnym menu mają być wyświetlane widoki lub kamery. |
| **Pokaż ścieżkę nawigacyjną podczas nawigacji w widoku** | Włącz tę opcję, aby wyświetlać ścieżkę nawigacji na górze widoku podczas nawigacji w widoku podzielonym. |

| Powiadomienia | |
|---|---|
| **Show taskbar notification on alarms (Pokaż powiadomienie na pasku zadań dla alarmów)** | Włącz te opcję, aby wyświetlać powiadomienie na pasku zadań systemu Windows po uruchomieniu alarmu. |
| **Show taskbar notification for tasks (Pokaż powiadomienie na pasku zadań dla zadań)** | Włącz tę opcję, aby wyświetlać powiadomienie na pasku zadań systemu Windows, gdy ktoś doda zadanie lub je zakończy. |
| **Pokaż powiadomienia w obszarze zarządzania urządzeniami** | Włącz tę opcję, aby wyświetlać powiadomienia o nowym oprogramowaniu sprzętowym do pobrania. |
| **Pokaż okno powiadomienia interkomu** | Włącz tę opcję, aby wyświetlać okno powiadomienia, gdy ktoś naciśnie przycisk połączenia na podłączonym interkomie. |

| Ujęcie | |
|---|---|
| **Po wykonaniu ujęcia wyświetl komunikat** | Włącz tę opcję, aby wyświetlać komunikat, gdy ktoś zrobi ujęcie. |
| **Po wykonaniu ujęcia otwórz folder ujęć** | Włącz tę opcję, aby otwierać folder ujęć, gdy zostanie zrobione ujęcie. |
| **Przeglądaj** | Kliknij przycisk **Browse (Przeglądaj)**, aby wybrać folder, w którym mają być zapisywane ujęcia. |

| Uruchom | |
|---|---|
| **Uruchom w widoku pełnoekranowym** | Włącz, aby uruchomić aplikację AXIS Camera Station 5 w trybie pełnoekranowym. |
| **Zapamiętaj ostatnio używane karty** | Włącz, aby uruchomić aplikację AXIS Camera Station 5 z tymi samymi otwartymi kartami, widokami i obszarami obserwacji kamery, które były otwarte w chwili ostatniego zamknięcia aplikacji AXIS Camera Station 5. |
| **Zapamiętaj ostatnio używane monitory** | Włącz, aby uruchomić aplikację AXIS Camera Station 5 na tym samym monitorze, który był używany przy ostatnim zamknięciu aplikacji AXIS Camera Station 5. |

Uwaga

- System zapisuje widoki i widoki kamer są zapisywane dla poszczególnych kart. System zapamiętuje ustawienia tylko wtedy, gdy komputer kliencki połączy się z tym samym serwerem.
- Zapamiętaj karty, aby zapamiętać monitory, widoki i widoki kamery.
- System nigdy nie zapamiętuje widoków dynamicznych przeciąganych i upuszczanych w podglądzie na żywo.
- W przypadku połączenia z wieloma serwerami z różnymi użytkownikami, system nie obsługuje funkcji **Remember last used tabs (Zapamiętaj ostatnio używane karty)**.

| Dźwięk podczas alarmu | |
|---|---|
| **No sound (Brak dźwięku)** | Wybierz tę opcję, jeśli nie chcesz, aby w razie alarmu rozlegał się dźwięk. |
| **Beep (Sygnał dźwiękowy)** | Wybierz tę opcję, jeżeli alarmowi ma towarzyszyć typowy dźwięk ostrzegawczy. |
| **Sound file (Plik dźwiękowy)** | Jeżeli do alarmu chcesz używać niestandardowego dźwięku, zaznacz i kliknij opcję **Browse (Przeglądaj)**, aby znaleźć odpowiedni plik dźwiękowy. Możesz wybrać dowolny format pliku obsługiwany w Windows Media Player. |
| **Odtwarzaj** | Kliknij, aby przetestować dźwięk. |

| Włącz dźwięk połączenia przychodzącego | |
|---|---|
| **No sound (Brak dźwięku)** | Wybierz tę opcję, jeśli nie chcesz, aby połączenie przychodzące było sygnalizowane dźwiękiem. |
| **Beep (Sygnał dźwiękowy)** | Wybierz tę opcję, jeżeli połączeniu przychodzącemu ma towarzyszyć typowy dźwięk ostrzegawczy. |
| **Sound file (Plik dźwiękowy)** | Jeżeli do połączenia przychodzącego chcesz używać niestandardowego dźwięku, zaznacz i kliknij opcję **Browse (Przeglądaj)**, aby znaleźć odpowiedni plik dźwiękowy. Możesz wybrać dowolny format pliku obsługiwany w Windows Media Player. |
| **Odtwarzaj** | Kliknij, aby przetestować dźwięk. |

| Cechy | |
|---|---|
| **Pokaż inteligentne wyszukiwanie 1** | Domyślnie jest wyświetlana funkcja Inteligentne wyszukiwanie 1. Wyłącz, aby ukryć tę funkcję. |

| Pokazuj okna dialogowe ostrzeżeń | |
|---|---|
| **Ostrzeżenie o nieprawidłowym certyfikacie** | Włącz, aby wyświetlać to ostrzeżenie w stosownych przypadkach. |

### Przesyłanie strumieniowe

W oknie **Configuration (Konfiguracja) > Client (Klient) > Streaming (Strumieniowanie)** można skonfigurować opcje strumieniowania w kliencie AXIS Camera Station 5.

| Skalowanie obrazu | |
|---|---|
| **Skaluj, aby dopasować** | Pozwala wyświetlać obraz na całej dostępnej przestrzeni i bez utraty proporcji ani przycięć. |
| **Wypełnij obszar obrazu (może przyciąć część obrazu)** | Pozwala dopasować wideo do dostępnego miejsca z zachowaniem współczynnika proporcji. Jeżeli dostępne miejsce ma inne proporcje niż obraz filmowy, system przytnie obraz. |

| Dekodowanie sprzętowe | |
|---|---|
| **Tryb** | • **Automatic (Automatyczny)** Strumienie w rozdzielczościach ponad 3840 x 2160p przy 25 kl./s (nazywanej również 4K lub UHD) są dekodowane przy użyciu karty graficznej (o ile jest obsługiwana).<br>• **On (Wł.)** Strumienie w rozdzielczościach ponad 1920 x 1080p przy 25 kl./s (nazywanej również 1080p lub HD) są dekodowane przy użyciu karty graficznej (o ile jest obsługiwana).<br>• **Off (Wyłączone)** Dekodowanie sprzętowe jest wyłączone i AXIS Camera Station 5 używa procesora do dekodowania obrazu wideo. |
| **Karta graficzna** | Wybierz kartę graficzną z menu rozwijanego. |

Uwaga

- Dekodowanie sprzętowe wykorzystuje kartę graficzną do dekodowania obrazu wideo i wyświetlania go na ekranie. Jeżeli masz wydajną kartę graficzną, dekodowanie sprzętowe to dobry sposób na zwiększenie wydajności i ograniczenie użycia procesora, szczególnie w przypadku strumieniowania wideo w wysokiej rozdzielczości. Dekodowanie sprzętowe obsługuje formaty M-JPEG i H.264.
- Dekodowania sprzętowego nie mogą używać kamery o rozdzielczości mniejszej niż 1080p, nawet jeśli dekodowanie sprzętowe jest **On (Wł.)**.
- Jeśli karta graficzna nie obsługuje dekodowania 4K, funkcja ta działa tylko w strumieniach o rozdzielczości 1080p, nawet jeśli dekodowanie sprzętowe jest **On (Wł.)**.

| Wykorzystanie przepustowości | |
|---|---|
| **Zawsze używaj profilu strumienia Niski w tym kliencie** | Pozwala używać niskiego profilu strumienia dla podglądu na żywo. Patrz *Profile strumienia*.<br><br>To ustawienie wpływa na wideo H.264 i M-JPEG i obniża wykorzystanie przepustowości. |
| **Wstrzymaj strumień wideo w nieaktywnych kartach** | Włącz, aby zawiesić strumień wideo na nieaktywnych kartach. Zmniejsza to wykorzystanie przepustowości. |

| PTZ (obrót, pochylenie, zbliżenie) | |
|---|---|
| **Wybierz widok po pierwszym kliknięciu zamiast uruchamiać PTZ** | Włącz, aby aktywować wybieranie widoku po pierwszym kliknięciu widoku. Wszystkie następne kliknięcia w widoku będą sterowały obrotem, pochylaniem i przybliżaniem. |

| Dźwięk | |
|---|---|
| **Push-to-talk release delay (ms) (Opóźnienie zwalniania push-to-talk (ms))** | Pozwala ustawić liczbę sekund, przez jaką ma być transmitowany dźwięk z mikrofonu po zwolnieniu przycisku **Push-to-talk**. |
| **Użyj push-to-talk dla wszystkich trybów duplex** | Pozwala używać funkcji push-to-talk w trybach simplex, half-duplex i full-duplex. |
| **Zawsze zezwalaj na dźwięk interkomów** | Pozwala prowadzić nasłuch interkomów i rozmawiać z nimi, nawet jeśli z ich strony nie ma żadnych trwających połączeń. |

| Natychmiastowa powtórka | |
|---|---|
| **Playback duration (s) (Czas trwania odtwarzania (s))** | Ustaw czas trwania odtwarzania w przedziale od 1 do 600 sekund, co pozwoli przeskakiwać z powrotem na osi czasu i ponawiać odtwarzanie nagrania. |

## Konfigurowanie połączonych usług

### Ustawienia aktualizacji oprogramowania sprzętowego

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można skonfigurować ustawienia uaktualnień oprogramowania sprzętowego, wybierając dowolny serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.

1. Wybierz kolejno opcje **Configuration > Connected services > Firmware upgrade settings (Konfiguracja > Połączone usługi > Ustawienia aktualizacji oprogramowania sprzętowego)**.
2. W menu **Automatic check for updates (Sprawdzaj automatycznie, czy są dostępne aktualizacje)** ustaw częstotliwość i sposób sprawdzania dostępności oprogramowania sprzętowego.
3. W menu **Upgrade order (Kolejność aktualizowania)** ustaw kolejność aktualizowania urządzeń.

| Automatycznie sprawdzaj dostępność aktualizacji | |
|---|---|
| **Check for updates (Sprawdź dostępność aktualizacji)** | Z rozwijalnego menu wybierz opcję **Every start-up (Każde uruchomienie)**. Dostępność nowych wersji oprogramowania sprzętowego na serwerze będzie sprawdzana przy każdym uruchomieniu. Domyślne ustawienie w aplikacji AXIS Camera Station 5 to **Never (Nigdy)**. |
| **Check now (Sprawdź teraz)** | Kliknięcie tej opcji spowoduje sprawdzenie serwera pod kątem dostępności nowych wersji oprogramowania sprzętowego. |

| Upgrade order (Kolejność aktualizowania) | |
|---|---|
| **Parallel (Równolegle)** | Zaznaczenie tej opcji spowoduje, że wszystkie urządzenia będą uaktualniane w tym samym czasie. Ta opcja działa szybciej niż **Sequential (Sekwencyjnie)**, ale powoduje jednocześnie, że wszystkie urządzenia są offline w tym samym czasie. |
| **Sekwencyjnie** | Zaznaczenie tej opcji powoduje, że urządzenia są uaktualniane po kolei. Ta opcja działa wolnej, ale urządzenia nie są przełączane w tryb offline w tym samym czasie. Aby wyłączyć aktualizację sekwencyjną, wybierz **Cancel remaining upgrades if one device fails (Anulowanie pozostałych aktualizacji w przypadku awarii jednego urządzenia)**. |


*Włącz automatyczne sprawdzanie dostępności nowych wersji oprogramowania sprzętowego*

## Axis Secure Remote Access

Ważne

Aby zwiększyć bezpieczeństwo i funkcjonalność, uaktualniamy funkcję **Axis Secure Remote Access** (v1) do **Axis Secure Remote Access v2**. Obecna wersja zostanie wycofana 1 grudnia 2025 r. Zalecamy przejście na funkcję Axis Secure Remote Access v2. przed tym terminem.

Co to oznacza dla systemu AXIS Camera Station 5?

- Po 1 grudnia 2025 r. zdalny dostęp do systemu za pośrednictwem funkcji **Axis Secure Remote Access** (v1) nie będzie możliwy.
- Aby korzystać z funkcji **Axis Secure Remote Access v2**, należy wykonać uaktualnienie do AXIS Camera Station Pro w wersji 6.8. Do 1 marca 2026 r. aktualizacja jest bezpłatna dla wszystkich użytkowników systemu AXIS Camera Station 5.

Axis Secure Remote Access umożliwia nawiązanie połączenia z serwerem AXIS Camera Station 5 za pośrednictwem bezpiecznego i szyfrowanego połączenia internetowego. Funkcja Axis Secure Remote Access nie używa przekierowywania portów na routerze, aby uzyskać dostęp do kamery.

Uwaga

- Funkcja Axis Secure Remote Access jest dostępna tylko w aplikacji w wersji AXIS Camera Station w wersji 5.12 i nowszych.
- W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można skonfigurować funkcję Axis Secure Remote Access, wybierając dowolny serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.

**Włączanie usługi Axis Secure Remote Access**

Funkcja Axis Secure Remote Access jest dostępna po zalogowaniu się na koncie MyAxis. Usługę Axis Secure Remote Access należy włączyć ręcznie. Ta funkcja umożliwia zdalne zalogowanie się do serwera, zobacz *Łączenie z serwerem*.

1. Wybierz kolejno opcje **Configuration > Connected services > Axis Secure Remote Access (Konfiguracja > Połączone usługi > Axis Secure Remote Access)**.
2. Na koncie My Axis wprowadź poświadczenia swojego konta My Axis.
3. Kliknij przycisk **Apply (Zastosuj)**.
4. W sekcji Axis Secure Remote Access kliknij przycisk **Enable (Włącz)**, aby włączyć funkcję zdalnego dostępu.

**Axis Secure Remote Access na urządzeniach mobilnych**

Aby zalogować się do serwera przy użyciu bezpiecznego zdalnego dostępu na urządzeniu mobilnym (iOS i Android):

1. Korzystając z urządzenia mobilnego, otwórz stronę *axis.com/products/axis-camera-station/overview* i pobierz aplikację AXIS Camera Station Mobile.
2. Zainstaluj tę aplikację mobilną i ją otwórz.
3. Zaloguj się do aplikacji Axis Secure Remote Access przy użyciu tego samego konta My Axis, którego użyto do aktywacji zdalnego dostępu.
4. Wybierz serwer, do którego chcesz się zalogować.
5. Zaloguj się przy użyciu poświadczeń dostępu do serwera.

Uwaga

Poświadczenia dostępu do serwera różnią się od poświadczeń konta My Axis.

W aplikacji mobilnej widać łączną ilość danych wykorzystanych przez konto My Axis w ciągu miesiąca. Aby uzyskać więcej informacji, zapoznaj się z *instrukcją obsługi aplikacji mobilnej AXIS Camera Station*.

**Korzystanie z usługi Axis Secure Remote Access**

Informacja o korzystaniu z Axis Secure Remote Access pojawia się na pasku stanu u dołu okna klienta AXIS Camera Station 5. Kliknij łącze, a zobaczysz podsumowanie informacji o używaniu bezpiecznego połączenia zdalnego.

| | |
|---|---|
| **Poziom usługi** | Pokazuje poziom wykupionej subskrypcji usługi Axis Secure Remote Access. |
| **Dane wykorzystane w tym miesiącu** | Pokazuje, ile danych użyto w tym miesiącu. Licznik jest resetowany o północy pierwszego dnia każdego miesiąca. |
| **Nadwyżka** | Pokazuje ilość danych użytych w danym miesiącu ponad kwotę przewidzianą na danym poziomie usługi. To ustawienie jest wyświetlane tylko w przypadku włączenia funkcji nadwyżki w ustawieniach subskrypcji. |
| **Połączenia** | Pokazuje serwery połączone za pośrednictwem usługi Secure Remote Access. |

## Konfigurowanie usługi AXIS System Health Monitoring Cloud Service

Usługa AXIS System Health Monitoring Cloud Service umożliwia monitorowanie danych o stanie pochodzących z systemów rozmieszczonych w różnych sieciach. Więcej informacji: *Organizacje, on page 115*.

Przed skonfigurowaniem usługi AXIS System Health Monitoring Cloud Service należy utworzyć konto My Axis. Patrz *my.axis.com*.

1. Przejdź do obszaru **Configuration (Konfiguracja) System Health Monitoring (Monitorowanie stanu systemu) > Settings (Ustawienia)**.
2. Kliknij **Manage (Zarządzaj)**.
3. Zaloguj się za pomocą konta My Axis i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

### Organizacje

Organizacja znajduje się w samym centrum usług chmurowych.

- Łączy ona system AXIS Camera Station 5 z użytkownikami różnych usług w chmurze.
- Umożliwia monitorowanie stanu systemu w chmurze. Więcej informacji znajduje się w rozdziale *Konfigurowanie usługi AXIS System Health Monitoring Cloud Service, on page 115*.
- Definiuje różne role użytkowników, na przykład administratora usługi i operatora.
- Organizację można podzielić na foldery, które na przykład odpowiadają systemom umieszczonym w różnych lokalizacjach. Aby utworzyć organizację, musisz mieć konto My Axis. Patrz *my.axis.com*.

#### Odłączanie systemu od organizacji

W niektórych przypadkach może być konieczne odłączenie systemu od obecnej organizacji. Powodem może być na przykład przenoszenie systemu z jednej organizacji do drugiej.

1. Przejdź do obszaru **Configuration (Konfiguracja) > Connected services (Połączone usługi) > AXIS System Health Monitoring Cloud Service**.
2. Kliknij **Disconnect (Odłącz)**.

#### Zapraszanie użytkownika do organizacji

1. Przejdź do obszaru **Configuration (Konfiguracja) > System Health Monitoring (Monitorowanie stanu systemu) > Settings (Ustawienia)**.
2. Kliknij **Open AXIS System Health Monitoring Cloud Service (Otwórz usługę AXIS System Health Monitoring Cloud Service)**.
3. Wybierz organizację, do której chcesz zaprosić użytkownika.
4. Otwórz ustawienia użytkownika i kliknij **Manage organizations (Zarządzaj organizacjami)**.
5. Otwórz kartę **Users (Użytkownicy)**.
6. Kliknij przycisk **Generate (Generuj)**.
7. Skopiuj kod zaproszenia i wyślij go do użytkownika, którego chcesz zaprosić.

Uwaga

Udostępniając użytkownikowi kod zaproszenia, podaj w zaproszeniu nazwę organizacji.

#### Dołączanie do organizacji

Gdy ktoś chce Cię zaprosić do dołączenia do organizacji, otrzymujesz kod zaproszenia. Aby dołączyć do organizacji:

1. Skopiuj kod zaproszenia.

2. Przejdź do obszaru **Configuration (Konfiguracja) > System Health Monitoring (Monitorowanie stanu systemu) > Settings (Ustawienia)**.
3. Kliknij **Open AXIS System Health Monitoring Cloud Service (Otwórz usługę AXIS System Health Monitoring Cloud Service)**.
4. Wybierz organizację, do której chcesz zaprosić użytkownika.
5. Otwórz ustawienia użytkownika i kliknij **Manage organizations (Zarządzaj organizacjami)**.
6. Otwórz kartę **Users (Użytkownicy)**.
7. Wklej kod zaproszenia.
8. Kliknij **Join (Dołącz)**.

## Konfigurowanie serwera

### Ustawienia serwera

Wybierz kolejno opcje **Configuration (Konfiguracja) > Server (Serwer) > Settings (Ustawienia)**, aby skonfigurować ustawienia serwera AXIS Camera Station 5.

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 można skonfigurować ustawienia dowolnego serwera, wybierając go z rozwijalnego menu **Selected server (Wybrany serwer)**.

| Eksport | |
|---|---|
| **Uwzględniaj dźwięk podczas dodawania zapisów do eksportu** | Wybierz, aby dołączyć dźwięk podczas dodawania nagrania do listy eksportu. |

| Dzienniki |
|---|
| Określ liczbę dni przechowywania alarmów, zdarzeń i audytów. Ustaw wartość pomiędzy 7 a 1000 dni. |

| Dane zewnętrzne |
|---|
| Określ liczbę dni, przez jaką mają być przechowywane dane zewnętrzne. Ustaw wartość pomiędzy 1 a 1000 dni. |

#### Serwery SMTP

Dodaj serwery SMTP, aby wysyłać wiadomości e-mail po wyzwoleniu alarmów systemowych lub aktywowaniu reguły konfiguracji zdarzeń.

Aby dodać serwer SMTP:

1. W obszarze **SMTP servers (Serwery SMTP)** kliknij **Add (Dodaj)**.
2. W obszarze **Server (Serwery)** skonfiguruj adres serwera, port, uwierzytelnianie oraz protokół TLS.
3. W obszarze **Sender (Nadawca)** wprowadź adres e-mail i nazwę, które mają być widoczne w wiadomości e-mail nadawcy.

| Serwer | |
|---|---|
| **Adres** | Wprowadź adres IP serwera SMTP. |
| **Port** | Wprowadź portu Domyślnym portem dla połączeń protokołu SMTP TLS jest port 587. |

| Serwer | |
|---|---|
| **Use TLS (Użyj TLS)** | Zaznacz tę opcję, jeśli serwer SMTP korzysta z protokołu TLS. TLS jest protokołem domyślnym. |
| **Użyj uwierzytelniania** | Zaznacz tę opcję, jeśli ten serwer wymaga podawania nazwy użytkownika i hasła. Wprowadź nazwę użytkownika i hasło umożliwiające dostęp do serwera. |

| | |
|---|---|
| **Edytuj** | Aby zmodyfikować dane serwera SMTP, zaznacz go i kliknij przycisk **Edit (Edytuj)**. |
| **Usuń** | Aby usunąć serwer SMTP, zaznacz go i kliknij przycisk **Remove (Usuń)**. W wyskakującym oknie dialogowym kliknij przycisk **Yes (Tak)**, aby potwierdzić chęć usunięcia serwera. |
| **Test all... (Testuj wszystkie)** | Aby przetestować serwer SMTP, zaznacz go i kliknij przycisk **Test all... (Testuj wszystkie)**. W wyskakującym oknie dialogowym w polu **Recipient (Odbiorca)** wprowadź adres e-mail, a następnie kliknij **OK**, aby wysłać testową wiadomość e-mail. Po przetestowaniu serwera SMTP zostanie wyświetlona lista wyników oraz dostępnych działań naprawczych. |
| Strzałki | Wybierz serwer i użyj strzałek, aby zmienić kolejność serwerów na liście. System używa serwerów w kolejności, w jakiej są na liście. |

| Wyniki testów serwera | |
|---|---|
| **OK** | Połączenie z serwerem SMTP zostało pomyślnie nawiązane. Zapytaj adresatów, czy otrzymali testową wiadomość e-mail. |
| **Nieznany błąd** | W trakcie próby wysłania wiadomości e-mail wystąpił nieoczekiwany błąd. Sprawdź, czy serwer SMTP działa poprawnie. |
| **Brak kontaktu** | AXIS Camera Station 5 nie może połączyć się z serwerem SMTP. Upewnij się, że serwer SMTP działa poprawnie i że wszystkie routery oraz serwery proxy między AXIS Camera Station 5 a serwerem SMTP zezwalają na ruch. |
| **Błąd konfiguracji** | Otrzymano żądanie TLS, ale serwer nie obsługuje StartTLS, nie obsługuje uwierzytelniania lub nie ma żadnego zgodnego mechanizmu uwierzytelniania. |
| **Błąd uzgadniania TLS/SSL** | Błąd podczas uzgadniania TLS/SSL, np. nieprawidłowy certyfikat serwera. |
| **Authentication required (Wymagane uwierzytelnienie)** | Serwer wymaga uwierzytelniania do wysyłania poczty e-mail. |
| **Błąd uwierzytelniania** | Poświadczenia są nieprawidłowe. |
| **Połączenie przerwane** | Połączenie zostało nawiązane, lecz następnie zostało utracone. |

### Alarm systemowy

Alarm systemowy występuje w przypadku utraty połączenia przez kamerę, odmowy dostępu do pamięci nagrań, nieoczekiwanego wyłączenia serwera lub wystąpienia błędów nagrywania. Mogą być wysyłane powiadomienia e-mail o alarmach systemowych.

Uwaga

W tym celu należy najpierw dodać serwer SMTP.

Aby wysłać wiadomość e-mail informujące o alarmach systemowych:

1. Zaznacz opcję **Send email on system alarm to the following recipients (W przypadku alarmu systemowego wyślij wiadomość e-mail do następujących odbiorców)**, aby aktywować funkcjonalność powiadamiania e-mailem o alarmach systemowych.
2. W obszarze **Recipients (Odbiorcy)**:
   2.1. Określ, czy adres ma trafić do pola **To (Do)**, **Cc (DW)**, czy **Bcc (UDW)**, a następnie wprowadź adres.
   2.2. Wprowadź adres e-mail.
   2.3. Kliknij przycisk **Add (Dodaj)**, a adres e-mail zostanie dodany do pola **Recipients (Odbiorcy)**.

| Połączenie z urządzeniem | |
|---|---|
| **Zachowuj niedostępne nazwy hostów** | Aby nawiązać połączenie, użyj nazwy hosta. Aby system automatycznie przełączał na łączenie za pomocą adresu IP, wyczyść pole wyboru. Można ręcznie ustawić, aby łączność z urządzeniami była nawiązywana przy użyciu nazwy hosta lub adresu IP. Patrz *Połączenie, on page 65*. |

| Język | |
|---|---|
| **Zmień język serwera** | Zmienia nazwę AXIS Camera Station 5 Service Control i AXIS Camera Station Secure Entry. Na przykład: alarmy systemowe, komunikaty dziennika audytu i zewnętrzne dane na karcie **Data search (Wyszukiwanie danych)**. Zmiana zaczyna obowiązywać po zrestartowaniu. |

| Urządzenia nasobne | |
|---|---|
| **Dysk**<br>**Folder** | Wybierz dysk i folder, w którym chcesz odbierać odrzuconą zawartość z systemu nasobnego. Więcej informacji można znaleźć w sekcji *Przesyłanie nagrań do lokalizacji przechowywania odrzuconej zawartości w Instrukcji obsługi rozwiązania nasobnego Axis*. |
| **Liczba dni przetrzymywania odrzuconej zawartości z systemu nasobnego.** | Jest to czas, przez który jest przechowywana odrzucona zawartość. |

| Informacja zwrotna | |
|---|---|
| **Prześlij anonimowe dane dotyczące użytkowania serwera do Axis Communications** | Zaznacz tę opcję, aby pomóc nam ulepszać aplikację i zwiększać satysfakcję użytkowników. Aby zmienić opcje dla klienta, zobacz *Ustawienia klienta, on page 108*. |

### Ustawienia zaawansowane

Ustawienia należy zmieniać tylko według zaleceń wsparcia technicznego Axis. Aby zmienić ustawienie zaawansowane:

1. Wprowadź ustawienie i jego wartość.
2. Kliknij **Dodaj**.

Aby aktywować rejestrowanie debugowania na potrzeby rozwiązywania problemów, zaznacz opcję **Enable server side debug logging (Włącz rejestrowanie usuwania błędów po stronie serwera)**. To ustawienie zajmuje więcej miejsca na dysku, a plik `log4net.config` w katalogu **ProgramData** zastępuje je.

### Aktualizuj AXIS Camera Station 5

W celu pobrania najnowszej wersji AXIS Camera Station 5:

1. Wybierz kolejno opcje **Configuration > Server > Update (Konfiguracja > Serwer > Aktualizacja)**.
2. Kliknij przycisk **Download and install... (Pobierz i zainstaluj)**.

Uwaga

- Nie można anulować aktualizacji bez względu na to, czy została uruchomiona manualnie, czy automatycznie.
- Zaplanowane aktualizacje rozpoczynają się automatycznie.
- System nie aktualizuje klientów połączonych za pośrednictwem bezpiecznego dostępu zdalnego.
- W systemie obejmującym kilka serwerów serwer lokalny jest zawsze aktualizowany jako ostatni.
- Podczas aktualizacji lokalnego serwera klient i sterowanie usługami zostaną tymczasowo zamknięte. Podczas aktualizacji nie będzie widoczny interfejs użytkownika ani wskaźnik postępu. Komputer serwera powinien być włączony do momentu ponownego uruchomienia klienta i serwera.
- Ta funkcja korzysta z narzędzia Windows installer (msi) niezależnie od aktualnie używanego typu.

### Raport o zdarzeniu

Jeżeli masz włączone uprawnienie do tworzenia raportów o zdarzeniach, możesz tworzyć takie raporty włącznie z nagraniami, ujęciami i notatkami. Patrz *Eksportowanie raportów o zdarzeniach, on page 29*.

Aby skonfigurować ustawienia raportów o zdarzeniach:

1. Wybierz kolejno opcje **Konfiguracja > Serwer > Raport o zdarzeniu**.
2. W polu **Location (Lokalizacja)** wskaż miejsce, gdzie mają być przechowywane raporty o zdarzeniach.
3. Z menu rozwijanego **Export format (Format eksportu)** wybierz format, do którego chcesz wyeksportować nagrania.
4. W obszarze **Categories (Kategorie)** dodaj lub usuń kategorie w celu pogrupowania raportów o zdarzeniach. Kategoriami mogą być nazwy folderów w lokalizacji eksportu, jeżeli w ustawieniu Ścieżka katalogu serwera kategorię skonfigurowano jako zmienną.
   4.1. W polu nadaj kategorii nazwę, na przykład Wypadek lub Kradzież.
   4.2. Kliknij **Dodaj**.
   4.3. Aby usunąć kategorię, zaznacz ją i kliknij przycisk **Remove (Usuń)**.
5. W obszarze **Description template (Szablon opisu)** wprowadź informacje, które mają być wyświetlane w polu **Description (Opis)** podczas generowania raportów o zdarzeniach. Na przykład: Zgłoszone przez: <Wpisz swoje imię i nazwisko, adres e-mail i numer telefonu>.
6. Kliknij przycisk **Apply (Zastosuj)**.

| Lokalizacja | |
|---|---|
| **Server directory path (Ścieżka katalogu serwera)** | Wybierz i wprowadź ścieżką katalogu, gdzie mają być zapisywane raporty w folderze na komputerze. Zmiennymi mogą być nazwa serwera, kategoria i nazwa użytkownika. Przykład: `C:\Reports\$(Server Name)\$(Category)\$(User Name)\`. |
| **Network directory path (Ścieżka katalogu sieciowego)** | Wybierz te opcję, aby zapisywać raporty o zdarzeniach w folderze w zasobie sieciowym. Wprowadź ścieżkę katalogu lub użyj danych uwierzytelniających zasobu sieciowego. Udział musi być dostępny z poziomu serwera AXIS Camera Station 5. Informacje o dodawaniu zasobów na potrzeby zapisywania nagrań można znaleźć w temacie *Zarządzaj pamięcią masową*. |

| Export format (Format eksportu) | |
|---|---|
| **ASF** | Jeśli ta opcja jest zaznaczona, można wybrać polecenie **Add digital signature (Dodaj podpis cyfrowy)**, aby w ten sposób uniemożliwić modyfikowanie obrazu. Patrz rozdział Podpis cyfrowy w temacie *Eksportuj nagrania*. Można również zaznaczyć opcję **Use password (Użyj hasła)** i stosować hasło do podpisu cyfrowego. |
| **MP4** | Eksportowane nagrania nie obejmują dźwięku w formatach G.711 i G.726. |

### Zaplanowany eksport

Otwórz menu **Configuration > Server > Scheduled export (Konfiguracja > Serwer > Zaplanowany eksport)** i zaplanuj terminarz eksportowania nagrań.

O wybranej godzinie rozpocznie się eksportowanie wszystkich nagrań dodanych od ostatniej operacji eksportu. Jeśli poprzednia operacja eksportowania została wykonana wcześniej niż przed tygodniem lub nie była jeszcze w ogóle wykonywana, wyeksportowane zostaną tylko nagrania mające mniej niż tydzień. Aby wyeksportować starsze nagrania, wybierz opcję **Recordings (Nagrania)** i wyeksportuj je ręcznie. Patrz *Eksportuj nagrania*.

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 wybierz dowolny serwer z rozwijalnego menu **Selected server (Wybrany serwer)**, aby włączyć zaplanowane operacje eksportu i nimi zarządzać.

**Eksportowanie zaplanowanych nagrań**

1. W sekcji **Scheduled export (Zaplanowany eksport)** zaznacz opcję **Enable scheduled export (Włącz zaplanowany eksport)**. Spowoduje to włączenie funkcji zaplanowanego eksportu.
2. W sekcji **Cameras (Kamery)** wybierz kamery, z których chcesz eksportować nagrania. System domyślnie wybierze wszystkie kamery na liście. Wyczyść pole wyboru **Use all cameras (Użyj wszystkich kamer)** i wybierz odpowiednie kamery z listy.
3. W menu **Export (Eksport)** określ miejsce docelowe zapisu nagrań, format i utworzenie listy odtwarzania.
4. W obszarze **Weekly schedule (Harmonogram tygodniowy)** zaznacz godziny i dni, w których nagrania mają być eksportowane.
5. Kliknij przycisk **Apply (Zastosuj)**.

| Eksport | |
|---|---|
| **Server directory path (Ścieżka katalogu serwera)** | Aby zapisywać nagrania w folderze na komputerze, zaznacz opcję ścieżki katalogu serwera i wprowadź ścieżkę prowadzącą do katalogu. |
| **Network directory path (Ścieżka katalogu sieciowego)** | Wybierz te opcję, aby zapisywać nagrania w folderze w zasobie sieciowym. Wprowadź ścieżkę katalogu lub użyj danych uwierzytelniających zasobu sieciowego. Udział musi być dostępny z poziomu serwera AXIS Camera Station 5. Informacje o dodawaniu zasobów na potrzeby zapisywania nagrań można znaleźć w temacie *Zarządzaj pamięcią masową*. |
| **Create playlist (.asx) (Utwórz listę odtwarzania)** | Wybierz tę opcję, aby utworzyć listę odtwarzania w formacie .asx używanym przez program Windows Media Player. Nagrania będą odtwarzane w kolejności, w jakiej dostały dokonane. |
| **Export format (Format eksportu)** | Wybierz format, do którego mają być eksportowane nagrania.<br><br>**ASF** – wybierz opcję **Add digital signature (Dodaj sygnaturę cyfrową)**, aby używać sygnatury cyfrowej jako zabezpieczenia obrazu przed niepożądaną ingerencją. Patrz rozdział Podpis cyfrowy w temacie *Eksportuj nagrania*. Można również zaznaczyć opcję **Use password (Użyj hasła)** i stosować hasło do podpisu cyfrowego.<br><br>**MP4** – eksportowane nagrania nie obejmują dźwięku w formatach G.711 i G.726. |

**Microsoft Windows 2008 Server**

Aby można było eksportować nagrania z serwera wyposażonego w system operacyjny Microsoft Windows 2008 Server, należy zainstalować aplikację Desktop Experience:

1. Kliknij kolejno opcje **Start > Administrative Tools > Server Manager (Start > Narzędzia administracyjne > Menedżer serwera)**, aby otworzyć aplet Menedżer serwera.
2. W menu **Features Summary (Podsumowanie funkcji)** kliknij **Add features (Dodaj funkcje)**.
3. Wybierz **Desktop Experience** i kliknij **Next (Dalej)**.
4. Kliknij przycisk **Install (Instaluj)**.

**Microsoft Windows 2012 Server**

Aby można było eksportować nagrania z serwera wyposażonego w system operacyjny Microsoft Windows 2012 Server, należy zainstalować aplikację Desktop Experience:

1. Kliknij kolejno opcje **Start > Administrative Tools > Server Manager (Start > Narzędzia administracyjne > Menedżer serwera)**, aby otworzyć aplet Menedżer serwera.
2. Wybierz kolejno opcje **Manage > Add Rules and Features (Zarządzaj > Dodaj role i funkcje)**, aby uruchomić Kreatora dodawania ról i funkcji.
3. W menu **Features Summary (Podsumowanie funkcji)** wybierz **User Interfaces and Infrastructure (Interfejsy użytkownika i infrastruktura)**.
4. Wybierz **Desktop Experience** i kliknij **Next (Dalej)**.
5. Kliknij przycisk **Install (Instaluj)**.

### Nowe połączenie

Wybierz kolejno ☰ > **Servers (Serwery) > New connection (Nowe połączenie)** w celu nawiązania połączenia z serwerem AXIS Camera Station 5. Patrz *Łączenie z serwerem*.

### Status połączenia

Wybierz kolejno ☰ > **Servers (Serwery) > Connection status (Status połączenia)**, aby wyświetlić listę statusów połączeń serwerów.

Aby połączyć lub rozłączyć się z serwerem, użyj suwaka przed nazwą serwera.

| Kody stanu | Opis | Możliwe rozwiązania |
|---|---|---|
| Łączenie | Klient próbuje nawiązać połączenie z serwerem. | |
| Połączono | Klient jest połączony z tym serwerem za pośrednictwem protokołu TCP. | |
| Połączono (bezpieczny zdalny dostęp) | Klient jest połączony z tym serwerem za pomocą funkcji bezpiecznego zdalnego dostępu. | |
| Połączono (za pomocą HTTP) | Klient jest połączony z tym serwerem za pośrednictwem protokołu HTTP. Takie połączenie ma gorszą jakość niż połączenie przez TCP i jest wolniejsze w przypadku komunikacji z wieloma serwerami. | |
| Rozłączanie | Klient rozłącza się od tego serwera. | |
| Rozłączono | Brak połączenia między klientem a tym serwerem. | |
| Ponowne łączenie | Klient utracił połączenie z tym serwerem i próbuje ponownie się połączyć. | |
| Nie udało się ponownie nawiązać połączenia | Klientowi nie udało się ponownie nawiązać połączenia z tym serwerem. Serwer jest odnajdowany, ale uprawnienia lub hasło użytkownika mogły ulec zmianie. | • Dodaj użytkownika w oknie dialogowym Uprawnienia użytkownika.<br>• Sprawdź nazwę użytkownika oraz hasło. |
| Logowanie anulowane | Operacja logowania została anulowana przez użytkownika. | |
| Niepoprawna nazwa użytkownika lub hasło | Kliknij łącze w kolumnie **Action (Akcja)** i wprowadź prawidłowe poświadczenia. | |
| Użytkownik nie jest autoryzowany na serwerze | Serwer nie zezwala użytkownikowi na zalogowanie się. | Dodaj użytkownika w oknie dialogowym Uprawnienia użytkownika. |

| | | |
|---|---|---|
| Niepowodzenie weryfikacji zabezpieczeń | Sprawdzenie zabezpieczeń powiązanych z usługą WCF nie powiodło się. Upewnij się, że godziny UTC w programie klienckim i na serwerze są zsynchronizowane. | |
| Brak kontaktu z serwerem | Komputer serwera nie przysłał odpowiedzi dla użytego adresu. | • Sprawdź, czy sieć działa prawidłowo.<br>• Sprawdź, czy serwer pracuje. |
| Żaden serwer nie pracuje | Komputer z oprogramowaniem serwerowym jest dostępny, ale nie serwer nie pracuje. | Uruchom serwer. |
| Błąd komunikacji | Połączenie z serwerem nie powiodło się. Upewnij się, że komputer serwera jest dostępny. | • Sprawdź, czy sieć działa prawidłowo.<br>• Sprawdź, czy serwer pracuje. |
| Nieprawidłowa nazwa hosta | System DNS nie może zmienić nazwy hosta na adres IP. | • Sprawdź, czy pisownia nazwy hosta jest prawidłowa.<br>• Sprawdź, czy system DNS ma potrzebne informacje. |
| Już nawiązano połączenie z tym samym serwerem | Klient jest już połączony z tym serwerem. | Usuń zduplikowany wpis serwera. |
| Nieoczekiwany serwer | Z tego adresu odpowiedział serwer inny niż oczekiwano. | Aby się połączyć z tym serwerem, zaktualizuj listę serwerów. |
| Wersja klienta (x) jest niezgodna z wersją serwera (y) | Oprogramowanie klienta jest zbyt stare lub zbyt nowe względem oprogramowania serwera. | Upewnij się, że na komputerze klienckim i serwerze jest zainstalowana ta sama wersja aplikacji AXIS Camera Station 5. |
| Serwer jest zbyt zajęty | Serwer nie może odpowiedzieć z powodu problemów z wydajnością. | Upewnij się, że komputer serwera i sieć nie są przeciążone. |


*Wiele serwerów*

## Listy serwerów

Serwery AXIS Camera Station 5 można organizować za pomocą list. Jeden serwer może figurować na wielu listach serwerów. Można importować i eksportować listy serwerów oraz używać ich w innych klientach AXIS Camera Station 5.

Wybierz kolejno ☰ > **Servers (Serwery) > Server lists (Listy serwerów)**, aby otworzyć okno dialogowe Server lists (Listy serwerów).

Zostanie wyświetlona domyślna lista **Recent connections (Ostatnie połączenia)**, na której są wyszczególnione serwery uczestniczące w poprzedniej sesji. Listy **Recent connections (Ostatnie połączenia)** nie można usunąć.

| | |
|---|---|
| | Wybierz listę serwerów i kliknij . |
| **+ New server list (+ Nowa lista serwerów)** | Klikniecie tego polecenia pozwala dodać nową listę serwerów i jej nazwę. |
| **Dodaj** | Aby dodać serwer do listy serwerów, wybierz listę i kliknij przycisk Add (Dodaj). Wprowadź wymagane informacje. |
| **Export lists (Eksportowanie list)** | Kliknij tę opcję, aby wyeksportować wszystkie listy w pliku .msl. Można zaimportować listę serwerów i następnie logować się do serwerów, które na niej figurują. Patrz *Łączenie z serwerem*. |
| **Edytuj** | Aby edytować serwer figurujący na liście serwerów, zaznacz go i kliknij przycisk **Edit (Edytuj)**. Można edytować tylko jeden serwer naraz. |
| **Usuń** | Aby usunąć serwery z listy serwerów, wybierz je i kliknij przycisk **Remove (Usuń)**. |
| Zmiana nazwy serwera | Kliknij dwukrotnie listę i wprowadź jej nową nazwę. |

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

*Grupowanie serwerów w listy serwerów*

## Konfigurowanie przełącznika

Jeśli masz urządzenie z serii AXIS Camera Station S22 Appliance, masz możliwość skonfigurowania urządzenia z poziomu AXIS Camera Station 5. Wybierz kolejno **Configuration (Konfiguracja) > Switch (Przełącznik) > Management (Zarządzanie)** i wpisz swoje poświadczenia, aby otworzyć stronę zarządzania przełącznikami w kliencie AXIS Camera Station 5. Aby dowiedzieć się, jak skonfigurować przełącznik, patrz instrukcja obsługi AXIS Camera Station S22 Appliance series na stronie *axis.com*.

Uwaga

AXIS Camera Station 5 może się łączyć tylko z adresem https://192.168.0.1/, czyli domyślnym adresem IP switcha.

## Konfigurowanie licencji

Na stronie License (Licencja) można przeglądać klucze licencyjne i stany licencji oraz zarządzać licencjami podłączonych urządzeń.

Uwaga

- W przypadku połączenia z wieloma serwerami AXIS Camera Station wybierz dowolny serwer z menu rozwijanego **Selected server (Wybrany serwer)**, aby zarządzać licencjami.
- Zalecamy spisanie kluczy licencyjnych na papierze albo zapisanie ich w formacie cyfrowym na dysku

flash USB ponieważ mogą się przydać w przyszłości. Utraconych kluczy licencyjnych nie można odzyskać.

- Po zarejestrowaniu sieciowego rejestratora wideo Axis w portalu AXIS License Portal otrzymasz licencję Core na urządzenie NVR. Licencje Core dla urządzeń NVR są trwale powiązane z warstwą sprzętową urządzenia i nie można ich przenosić. Licencję Core na urządzenie NVR można rozszerzyć do poziomu Universal analogicznie jak licencje Core dla innych urządzeń. Licencje rozszerzające można przenosić i wykorzystywać w dowolnym systemie.

## License management (Zarządzanie licencjami)

Wybierz kolejno opcje **Configuration > Licenses > Management (Konfiguracja > Licencje > Zarządzanie)**, a zobaczysz całościowy obraz urządzeń bez licencji łączących się z serwerem. Licencjami można zarządzać online i offline. Należy pamiętać, aby dodać licencje dla wszystkich urządzeń przed zakończeniem 30-dniowego okresu próbnego. Patrz *Jak zakupić licencje*. Można również kliknąć łącze stanu licencji na pasku stanu, aby wyświetlić przegląd licencji urządzeń.

Jako administrator licencji możesz dodać wiele kont My Axis do systemu AXIS Camera Station.

**Dodawanie konta MyAxis do systemu w trybie online**

1. Przejdź do menu **Configuration > Licenses > Management (Konfiguracja > Licencje > Zarządzanie)**.
2. Sprawdź, czy opcja **Manage licenses online** (Zarządzaj licencjami online) jest włączona.
3. Kliknij **Go to AXIS License Portal (Przejdź do portalu licencyjnego AXIS)**.
4. W portalu AXIS License Portal zaloguj się przy użyciu nowego konta My Axis, które chcesz dodać.
5. Przejdź do obszaru **Edit license admins (Edytuj administratorów licencji)** i sprawdź, czy konto zostało dodane jako administrator licencji.

**Dodawanie konta MyAxis do systemu w trybie offline**

1. Przejdź do menu **Configuration > Licenses > Management (Konfiguracja > Licencje > Zarządzanie)**.
2. Wyłącz opcję **Manage licenses online (Zarządzaj licencjami online)**.
3. Kliknij **Export system file (Eksportuj plik systemowy)**.
4. Zapisz plik systemowy na dysku flash USB.
5. Przejdź do portalu AXIS License Portal pod adresem *license-portal.lp.axis.com*.
6. Zaloguj się przy użyciu nowego konta MyAxis, które chcesz dodać.
7. Prześlij plik systemowy.
8. Przejdź do obszaru **Edit license admins (Edytuj administratorów licencji)** i sprawdź, czy konto zostało dodane jako administrator licencji.

Istnieją różne sposoby licencjonowania systemu w zależności od posiadanego połączenia z Internetem.

- *Licencja na system online*
- *Licencja na system w trybie offline*
- *Przenoszenie licencji między systemami, on page 126*

### Status urządzeń

Przejdź do obszaru **Configuration (Konfiguracja) > Licenses (Licencje) > Device status (Stan urządzeń)**, aby wyświetlić listę wszystkich podłączonych urządzeń i stan ich licencji.

### Klucze

Wybierz kolejno opcje **Configuration > Licenses > Keys (Konfiguracja > Licencja > Klucze)**, a zostanie wyświetlona lista kluczy niezbędnych dla wszystkich licencji na wszystkich połączonych urządzeniach.

### Licencja na system online

Zarówno klient AXIS Camera Station, jak i serwer muszą mieć połączenie z Internetem.

1. Przejdź do menu **Configuration > Licenses > Management (Konfiguracja > Licencje > Zarządzanie)**.
2. Upewnij się, że opcja **Manage licenses online (Zarządzaj licencjami online)** zostanie włączona.
3. Zaloguj się przy użyciu konta My Axis.
4. W sekcji **Add license key (Dodaj klucz licencyjny)** wprowadź klucz licencyjny.
5. Kliknij **Dodaj**.
6. W kliencie AXIS Camera Station upewnij się, że klucze licencyjne są wyświetlane w sekcji **Configuration (Konfiguracja) > Licenses (Licencje) > Keys (Klucze)**.

### Licencja na system w trybie offline

1. Przejdź do menu **Configuration > Licenses > Management (Konfiguracja > Licencje > Zarządzanie)**.
2. Wyłącz opcję **Manage licenses online (Zarządzaj licencjami online)**.
3. Kliknij **Export system file (Eksportuj plik systemowy)**.
4. Zapisz plik systemowy na dysku flash USB.
5. Przejdź do portalu AXIS License Portal pod adresem *license-portal.lp.axis.com*.
6. Zaloguj się przy użyciu konta My Axis.
7. Kliknij **Upload system file (Wczytaj plik systemowy)**, aby wczytać plik z dysku flash USB.
8. W sekcji **Add license key (Dodaj klucz licencyjny)** wprowadź klucz licencyjny.
9. Kliknij **Dodaj**.
10. W obszarze **License keys (Klucze licencji)** kliknij **Download license file (Pobierz plik licencji)** i zapisz plik na dysku flash USB.
11. W kliencie AXIS Camera Station przejdź do obszaru **Configuration (Konfiguracja) > Licenses (Licencje) > Management (Zarządzanie)**.
12. Kliknij **Import license file (Importuj plik licencji** i wybierz plik licencji znajdujący się na dysku flash USB.
13. Upewnij się, że klucze licencyjne są wyświetlane w sekcji **Configuration (Konfiguracja) > Licenses (Licencje) > Keys (Klucze)**.

### Przenoszenie licencji między systemami

Uwaga

Nie można przenosić licencji NVR Core, ponieważ są one powiązane na stałe z elementami sprzętowymi urządzenia.

Aby przenieść licencje z jednego systemu do drugiego w ramach tego samego konta My Axis:

1. Przejdź do portalu AXIS License Portal pod adresem *license-portal.lp.axis.com*.
2. W obszarze **My systems** kliknij nazwę systemu, z którego chcesz przenieść licencję.
3. W obszarze **Klucze licencyjne** odszukaj klucz licencyjny, który chcesz przenieść.
4. Kliknij kolejno przyciski ⋮ i **Przenieś**.
5. W menu rozwijanym **To system (System docelowy)** zaznacz system, do którego ma zostać przeniesiona licencja.
6. Kliknij kolejno przyciski **Move license key (Przenieś klucz licencyjny(** i **Zamknij**. Szczegóły operacji są wyświetlane obszarze **Historia**.
7. Przejdź do obszaru **My Systems** i upewnij się, że licencje są wyświetlane pod właściwym systemem.


*Przenoszenie licencji do innego systemu*

Aby zwolnić licencje w systemie, a następnie dodać je do innego systemu pod innym kontem MyAxis:

1. Przejdź do portalu AXIS License Portal pod adresem *license-portal.lp.axis.com*.
2. W obszarze **My systems** kliknij nazwę systemu, z którego chcesz przenieść licencję.
3. W obszarze **Klucze licencyjne** odszukaj klucz licencyjny, który chcesz przenieść.
4. Najpierw wykonaj kopię klucza licencyjnego.
5. Kliknij ⋮ i **Release (Zwolnij)**.
6. Wyloguj się, a następnie zaloguj przy użyciu innego konta MyAxis.
7. W obszarze **My Systems** kliknij system, na który chcesz uzyskać licencję.
8. W obszarze **Add license key (Dodaj klucz licencyjny)** wprowadź zwolniony klucz licencyjny.
9. Kliknij **Dodaj**. Szczegóły operacji są wyświetlane obszarze **Historia**.
10. Przejdź do obszaru **My Systems** i upewnij się, że licencje są wyświetlane pod właściwym systemem.

## Konfigurowanie zabezpieczeń

### Uprawnienia użytkownika

Przejdź do sekcji **Configuration (Konfiguracja) > Security (Zabezpieczenia) > User permissions (Uprawnienia użytkowników)**, aby wyświetlić użytkowników i grupy, którzy występują w AXIS Camera Station 5.

Uwaga

Administratorzy komputera, na którym jest uruchomiony serwer AXIS Camera Station 5, automatycznie otrzymują uprawnienia administratora serwera AXIS Camera Station 5. Nie można zmienić ani usunąć uprawnień grupy administratorów.

Aby można było dodać użytkownika lub grupę, użytkownik lub grupa muszą być zarejestrowani na komputerze lokalnym lub mieć konto użytkownika usługi Active Directory systemu Windows®. Aby dodać użytkowników lub grupy, patrz *Dodawanie użytkowników lub grup*.

Użytkownik będący częścią grupy otrzymuje najwyższy zakres uprawnień przypisany do osoby i grupy. Użytkownik będący częścią grupy otrzymuje dostęp jako osoba indywidualna, a także uprawnienia wynikające z przynależności do grupy. Na przykład użytkownik otrzymuje dostęp do kamery X jako osoba indywidualna. Użytkownik należy też do grupy, która ma dostęp do kamer Y i Z. Użytkownik ma zatem dostęp do kamer X, Y i Z.

| | |
|---|---|
| person | Wskazuje, że dana pozycja dotyczy indywidualnego użytkownika. |
| group | Wskazuje, że pozycja dotyczy grupy. |
| **Nazwa** | Nazwa użytkownika wyświetlana na komputerze lokalnym lub w usłudze Active Directory. |
| **Domena** | Domena, do której należy użytkownik lub grupa. |
| **Rola** | Rola dostępu przypisana do użytkownika lub grupy.<br><br>Możliwe wartości: administrator, operator i dozorca. |

| | |
|---|---|
| **Szczegóły** | Szczegółowe informacje o użytkownikach pojawiające się na komputerze lokalnym lub w usłudze Active Directory. |
| **Serwer** | Serwer, do którego należy użytkownik lub grupa. |

**Dodawanie użytkowników lub grup**

Użytkownicy i grupy systemu Microsoft Windows® oraz usługi Active Directory mają dostęp do AXIS Camera Station 5. Aby dodać użytkownika do AXIS Camera Station 5, należy dodać użytkowników lub grupę do systemu Windows®.

Aby dodać użytkownika w systemie Windows® 10 i 11:

- Naciśnij klawisz Windows + X i wybierz opcję **Computer Management (Zarządzanie komputerem)**.
- W oknie **Computer Management (Zarządzanie komputerem)** przejdź do sekcji **Local Users and Groups (Lokalni użytkownicy i grupy)** > **(Users) Użytkownicy**.
- Kliknij prawym przyciskiem myszy **Users (Użytkownicy)** i wybierz opcję **New User (Nowy użytkownik)**.
- W wyskakującym oknie dialogowym wprowadź dane nowego użytkownika i usuń zaznaczenie pola **User must change password at next login (Użytkownik musi zmienić hasło przy następnym logowaniu)**.
- Kliknij polecenie **Create (Utwórz)**.

Jeżeli korzystasz z domeny Active Directory, skonsultuj się z administratorem sieci.

**Dodawanie użytkowników lub grup**

1. Przejdź do obszaru **Configuration (Konfiguracja) > Security (Zabezpieczenia) > User permissions (Uprawnienia użytkownika)**.
2. Kliknij **Dodaj**.
   Na liście zobaczysz dostępnych użytkowników i grupy.
3. W obszarze **Scope (Zakres)** wybierz lokalizację, w której chcesz szukać użytkowników i grupy.
4. W menu **Show (Pokaż)** wybierz wyświetlanie użytkowników lub grup.
   W przypadku zbyt dużej liczby użytkowników lub grup wynik wyszukiwania nie jest wyświetlany. Użyj funkcji filtrowania.
5. Wybierz użytkowników lub grupy i kliknij **Add (Dodaj)**.

| Scope (Zakres) | |
|---|---|
| **Serwer** | Wybierz tę opcję, aby wyszukać użytkowników lub grupy na komputerze lokalnym. |
| **Domena** | Ta funkcja umożliwia wyszukiwanie użytkowników lub grupy usługi Active Directory. |
| **Selected server (Wybrany serwer)** | W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station 5 należy wybrać serwer z rozwijalnego menu **Selected server (Wybrany serwer)**. |

**Konfigurowanie użytkownika lub grupy**

1. Wybierz użytkownika lub grupę z listy.
2. W obszarze **Role (Rola)** wybierz opcję **Administrator**, **Operator** lub **Viewer (Dozorca)**.
3. W przypadku wybrania opcji **Operator** lub **Viewer (Dozorca)** można skonfigurować uprawnienia użytkownika lub grupy. Patrz *Uprawnienia użytkownika/grupy*.
4. Kliknij przycisk **Zapisz**.

### Usuwanie użytkownika lub grupy

1. Wybierz użytkownika lub grupę.
2. Kliknij przycisk **Remove (Usuń)**.
3. W wyskakującym oknie dialogowym kliknij przycisk **OK**, aby usunąć użytkownika lub grupę.

### Uprawnienia użytkownika/grupy

Do użytkownika lub grupy można przypisać trzy role. Aby uzyskać informacje na temat definiowania roli dla użytkownika lub grupy, zobacz *Dodawanie użytkowników lub grup*.

**Administrator –** Pełny dostęp do całego systemu, w tym dostęp do obrazów na żywo i zarejestrowanego materiału wideo z wszystkich kamer. Użytkownik z tymi uprawnieniami ma dostęp do wszystkich portów i widoków WE/WY. Ta rola jest wymagana do skonfigurowania dowolnego systemu.

**Operator –** Wybierz kamery, widoki i porty We/Wy, aby uzyskać dostęp do podglądu na żywo i nagrań. Operator ma pełny dostęp do wszystkich funkcji AXIS Camera Station 5 — oprócz opcji konfiguracji systemu.

**Dozorca –** Dostęp do obrazów na żywo z wybranych kamer i dostęp do zaznaczonych portów oraz widoków WE/WY. Dozorca nie ma dostępu do zarejestrowanego materiału wideo ani konfiguracji systemu.

#### Kamery

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**.

| | |
|---|---|
| **Wejdź na stronę** | Umożliwia dostęp do kamery i wszystkich funkcji kamery. |
| **Nagranie wideo** | Umożliwia dostęp do wideo w trybie na żywo z kamery. |
| **Nasłuch audio** | Umożliwia dostęp w celu słuchania przez kamerę. |
| **Odtwarzanie komunikatu audio** | Dostęp do mówienia do kamery. |
| **Manual Recording (Nagrywanie manualne)** | Zezwolenie na ręczne rozpoczynanie i zatrzymywanie zapisów. |
| **Mechanical PTZ (Mechaniczny PTZ)** | Zezwalanie na dostęp do mechanicznych funkcji sterowania PTZ. Dostępne tylko w przypadku kamer z PTZ ze sterowaniem mechanicznym. |
| **Priorytet PTZ** | Umożliwia ustawienie priorytetu PTZ. Mniejsza wartość oznacza wyższy priorytet. Żaden przypisany priorytet nie jest ustawiony jako `0`. Najwyższy priorytet ma administrator. Gdy kamera PTZ jest obsługiwana przez osobę o wyższym priorytecie, inne osoby nie mogą obsługiwać tej samej kamery przez 10 sekund. Opcja dostępna tylko w przypadku kamer z PTZ mechanicznymi funkcjami sterowania i zaznaczoną opcją **Mechanical PTZ (Mechaniczne PTZ)**. |

#### Widoki

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**. Można wybrać wiele widoków i ustawić uprawnienia dostępu.

| | |
|---|---|
| **Wejdź na stronę** | Umożliwia dostęp do widoków w AXIS Camera Station 5. |
| **Edytuj** | Umożliwia edycję widoków w AXIS Camera Station 5. |

**We/wy**

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator (Operator)** lub **Viewer (Dozorca)**.

| | |
|---|---|
| **Wejdź na stronę** | Zezwala na pełny dostęp do portu WE/WY. |
| **Zapoznaj się z** | Zezwala na wyświetlenie stanu portu WE/WY. Użytkownik nie może zmienić stanu portu. |
| **Write (Zapis)** | Zezwala na zmianę stanu portu WE/WY. |

**System**

Nie można skonfigurować wyszarzonych uprawnień dostępu na liście. Znacznik oznacza, że uprawnienie jest domyślnie przypisane do użytkownika albo grupy.

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. W przypadku roli **Viewer (Dozorca)** dostępna jest też funkcja **Take snapshots (Wykonywanie ujęć)**.

| | |
|---|---|
| **Wykonaj ujęcia** | Umożliwia tworzenie ujęć w trybie podglądu na żywo i zapisu. |
| **Eksportuj nagrania** | Umożliwia eksportowanie zapisów. |
| **Generuj raport o zdarzeniu** | Zezwala na generowanie raportów o zdarzeniach. |
| **Prevent access to recordings older than (Blokowanie dostępu do nagrań starszych niż)** | Zapobiega dostępowi do nagrań wcześniejszych niż podana liczba minut. Użytkownicy nie znajdą tych nagrań przy wyszukiwaniu. |
| **Dostęp do alarmów, zadań i dzienników** | Umożliwia odbierania powiadomień o alarmach i zezwala na dostęp do paska **Alarms and tasks (Alarmy i zadania)** oraz karty **Logs (Dzienniki)**. |
| **Access data search (Dostęp do wyszukiwania danych)** | Umożliwiają wyszukiwanie danych w celu śledzenia tego, co wydarzyło się w czasie zdarzenia. |
| **Add categories to events (Dodaj kategorie do zdarzeń)** | Umożliwia dodawanie kategorii do zdarzeń na karcie **Recordings** (Nagrania). |
| **Remove categories from event (Usuń kategorie ze zdarzenia)** | Umożliwia usuwanie kategorii ze zdarzeń na karcie **Recordings** (Nagrania). |

**Kontrola dostępu**

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. **Access Management (Zarządzanie dostępem)** jest też dostępne dla roli **Viewer (Dozorca)**.

| | |
|---|---|
| **Konfiguracja kontroli dostępu** | Umożliwia konfigurację drzwi i stref, profili identyfikacyjnych, formatów kart i kodów PIN, szyfrowanej komunikacji i wielu serwerów. |
| **Zarządzanie dostępem** | Zezwalanie na zarządzanie dostępem i dostęp do ustawień usługi Active Directory. |

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Viewer** (Dozorca).

**Monitorowanie stanu systemu**

Następujące uprawnienia dostępu są dostępne dla użytkowników lub grup z rolą **Operator**. **Access to system health monitoring (Dostęp do monitorowania stanu systemu)** jest też możliwy w przypadku roli **Viewer (Dozorca)**.

| | |
|---|---|
| **Configuration of system health monitoring (Konfiguracja monitorowania stanu systemu)** | Zezwalanie na konfigurację systemu do monitorowania stanu systemu. |
| **Access to system health monitoring (Dostęp do monitorowania stanu systemu)** | Zezwalanie na dostęp do systemu monitorowania stanu systemu. |

## Certyfikaty

Aby zarządzać ustawieniami certyfikatów między serwerem AXIS Camera Station 5 a urządzeniami, wybierz kolejno **Configuration (Konfiguracja) > Security (Zabezpieczenia) > Certificates (Certyfikaty)**.

Aby uzyskać informacje na temat włączania, usuwania i przeglądania certyfikatów HTTPS i IEEE 802.1X, zob. *Bezpieczeństwo, on page 64*.

AXIS Camera Station 5 może być używany jako:

- **Główny urząd certyfikacji (CA):** Jeśli używasz AXIS Camera Station 5 jako głównego urzędu certyfikacji, oznacza to, że AXIS Camera Station 5 używa własnego certyfikatu głównego do wydawania certyfikatów serwera i nie ma innego głównego urzędu certyfikacji zaangażowanego w ten proces.
- **Pośredni organ wydający certyfikat:** W tym scenariuszu należy zaimportować certyfikat CA i jego klucz prywatny do aplikacji AXIS Camera Station 5, tak aby mogła ona podpisywać i wystawiać certyfikaty serwera dla urządzeń Axis. Ten CA może być certyfikatem głównym lub pośrednim certyfikatem CA.

Uwaga

W przypadku odinstalowania aplikacji AXIS Camera Station 5 usuwa ona swoje certyfikaty CA z zaufanych głównych urzędów certyfikacji systemu Windows. Zaimportowane certyfikaty CA nie są usuwane. Należy je usunąć ręcznie.

### Organ wydający certyfikat (CA)

Funkcja organu wydającego certyfikat umożliwia korzystanie z protokołów HTTPS i IEEE 802.1X na urządzeniach, które nie zawierają żadnych certyfikatów klientów/serwerów. Urząd certyfikacji AXIS Camera Station 5 może automatycznie tworzyć, podpisywać i instalować na urządzeniach certyfikaty klientów/serwerów, jeśli używane są protokoły HTTPS lub IEEE 802.1X. Można wykorzystać AXIS Camera Station 5 jako główny urząd certyfikacji lub zaimportować certyfikat urzędu certyfikacji i pozwolić, by rozwiązanie AXIS Camera Station 5 działało jako pośredni urząd certyfikacji. System generuje główny urząd certyfikacji podczas instalacji serwera.

| | |
|---|---|
| **Importuj** | Kliknij, aby zaimportować istniejący certyfikat urzędu certyfikacji i jego klucz prywatny. AXIS Camera Station 5 przechowuje jego hasło. |
| **Wygeneruj** | Kliknij, aby wygenerować nowy klucz publiczny i prywatny oraz certyfikat CA z podpisem własnym, ważne przez 10 lat. Podczas generowania nowego CA zastępuje on wszystkie certyfikaty komponentów i ponownie uruchamia wszystkie komponenty. |
| **Wyświetl** | Kliknij, aby wyświetlić szczegóły certyfikatu CA. |

| | |
|---|---|
| **Eksport** | Kliknij, aby wyeksportować certyfikat UC do pliku. Certyfikat eksportować można na dwa sposoby:<br>• **Bez klucza prywatnego:** Certyfikat zapisywany jest w formacie .cer lub .crt. Użyj tej opcji, jeżeli chcesz tylko zainstalować certyfikat publiczny w innych systemach, w których powinny być użyte zaufane certyfikaty podpisane przez AXIS Camera Station 5.<br>• **Z kluczem prywatnym:** Certyfikat UC zapisywany jest w formacie PKCS#12 (.pfx lub .p12). Użyj tej opcji, jeżeli musisz zaimportować certyfikat UC do innego serwera AXIS Camera Station 5. |
| **Number of dates the signed client/server certificates will be valid for (Liczba dni ważności podpisanych certyfikatów klientów/serwerów)** | Ustaw liczbę dni ważności certyfikatów klientów/serwerów tworzonych automatycznie. Maksymalna liczba dni to 1095 (trzy lata). Uwaga: CA nie podpisuje certyfikatów, które są ważne po jego dacie ważności. |

**Generowanie głównego organu wydającego certyfikat**

Gdy aplikacja AXIS Camera Station 5 zostanie uruchomiona, szuka urzędu certyfikacji. W przypadku jego braku automatycznie generuje główny urząd certyfikacji. Zawiera on certyfikat główny z podpisem własnym i klucz prywatny chroniony hasłem. AXIS Camera Station 5 przechowuje hasło, ale nie jest ono widoczne. Certyfikat urzędu certyfikacji wygenerowany przez aplikację AXIS Camera Station 5 jest ważny przez 10 lat.

Aby ręcznie wygenerować nowy organ wydający certyfikat w celu zastąpienia starego organu, patrz *Zastępowanie organu wydającego certyfikat, on page 133*.

W przypadku dokonywania uaktualnienia wersji 5.45 lub starszej, która używa certyfikatu manualnie zainstalowanego na urządzeniu, aplikacja AXIS Camera Station 5 automatycznie używa istniejącego głównego urzędu certyfikacji w celu zainstalowania nowego certyfikatu, gdy manualnie zainstalowany certyfikat wygaśnie.

Uwaga

Po wygenerowaniu certyfikat CA jest dodawany do zaufanego certyfikatu głównego systemu Windows.

**Importowanie organu wydającego certyfikat**

Instalując certyfikat urzędu certyfikacji z innego urzędu certyfikacji, można użyć aplikacji AXIS Camera Station 5 jako pośredniego urzędu certyfikacji. Zaimportuj istniejący już urząd certyfikacji składający się z certyfikatu i klucza prywatnego, aby umożliwić aplikacji AXIS Camera Station 5 podpisywanie certyfikatów w imieniu tego urzędu certyfikacji. Plik musi być plikiem PKCS#12, certyfikat musi mieć podstawowe ograniczenie (2.5.29.19) wskazujące, że jest to certyfikat urzędu certyfikacji, i musi być używany w okresie jego ważności. Aby zaimportować organ wydający certyfikat w celu zastąpieniu istniejącego CA, patrz *Zastępowanie organu wydającego certyfikat, on page 133*.

Uwaga

- Jeśli zaimportowany CA nie wymaga hasła, będzie wyświetlane okno dialogowe, gdy tylko jakiś element będzie wymagał hasła. Będzie tak na przykład w przypadku używania protokołu HTTPS lub IEEE w urządzeniu albo dodawaniu urządzenia. Wtedy aby kontynuować, musisz kliknąć przycisk **OK**.
- Po zaimportowaniu certyfikat CA jest dodawany do zaufanego certyfikatu głównego systemu Windows.
- Po odinstalowaniu aplikacji AXIS Camera Station 5 konieczne jest ręczne usunięcie zaimportowanych certyfikatów urzędów certyfikacji z zaufanych głównych urzędów certyfikacji systemu Windows.

### Zastępowanie organu wydającego certyfikat

Aby zastąpić CA, który wydaje podpisane certyfikaty używane na urządzeniach z połączeniem HTTPS:

1. Wybierz kolejno opcje **Configuration > Security > Certificates > HTTPS (Konfiguracja > Zabezpieczenia > Certyfikaty > HTTPS)**.
2. Wyłącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).
3. W obszarze **Certificate authority (Organ wydający certyfikat (CA))** kliknij polecenie **Generate (Generuj)** lub **Import (Importuj)**.
4. Wpisz hasło i kliknij przycisk **OK**.
5. Wybierz liczbę dni, przez jaką podpisane certyfikaty klientów/serwerów pozostają ważne.
6. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
7. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno polecenia **Zabezpieczenia > HTTPS > Włącz/Aktualizuj**.
8. Przejdź do **Configuration > Security > Certificates > HTTPS** (Konfiguracja > Bezpieczeństwo > Certyfikaty > HTTPS) i włącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).

### HTTPS

AXIS Camera Station 5 domyślnie weryfikuje podpis aktywnego certyfikatu serwera HTTPS na każdym połączonym urządzeniu i nie nawiązuje połączenia z urządzeniem bez zweryfikowanego certyfikatu. Certyfikat serwera musi być podpisany przez aktywny urząd certyfikacji w AXIS Camera Station 5 lub zweryfikowany przez magazyn certyfikatów systemu Windows. AXIS Camera Station 5 weryfikuje również, czy adres w certyfikacie HTTPS urządzenia jest zgodny z adresem używanym do komunikacji z urządzeniem, jeśli jest włączona opcja **Validate device address (Zweryfikuj adres urządzenia)**.

Kamery z oprogramowaniem układowym w wersji 7.20 i w wersjach nowszych mają skonfigurowany certyfikat samopodpisany. Te certyfikaty nie są zaufane. Zamiast tego należy wygenerować lub zaimportować urząd certyfikacji, aby umożliwić aplikacji AXIS Camera Station 5 wystawianie nowych certyfikatów dla urządzeń w przypadku korzystania z protokołu HTTPS.

| | |
|---|---|
| **Tymczasowo ignoruj potwierdzenie certyfikatu** | Włącz, aby aplikacja AXIS Camera Station 5 mogła zaakceptować dowolny certyfikat HTTPS i aby zezwolić na konfigurowanie niezabezpieczonych urządzeń.<br><br>Wyłącz, aby aplikacja AXIS Camera Station 5 mogła zweryfikować certyfikaty urządzeń. Jeśli urządzenie nie jest zaufane, w obszarze **Status** na karcie **Device management (Zarządzanie urządzeniami)** zostanie wyświetlony komunikat ostrzegawczy i urządzenie będzie niedostępne. |
| **Potwierdź adres urządzenia** | Wyłącz, aby zapewnić stabilne działanie w sieciach DHCP bez używania nazw hostów.<br><br>Włącz, aby konieczne było dopasowanie adresów w celu dodatkowego zabezpieczenia. Zalecamy włączanie tego ustawienia tylko w sieciach, w których urządzenia używają głównie nazwy hosta do komunikacji lub urządzenia mają statyczny adres IP. |

Uwaga

- Jeśli bezpieczne połączenie (HTTPS) jest niedostępne, można wystawić nowy certyfikat HTTPS. Patrz *Dodawanie urządzeń, on page 40*
- Aby można było używać protokołu HTTPS, urządzenia wideo muszą mieć zainstalowane oprogramowanie sprzętowe w wersji 5.70 lub nowszej, a urządzenia kontroli dostępu i audio potrzebują oprogramowania sprzętowego w wersji 1.25 lub nowszej.

**Ograniczenia**

- Porty inne niż domyślne (czyli 443) nie są obsługiwane.
- Wszystkie certyfikaty instalowane w operacji wsadowej muszą mieć takie samo hasło.
- Na certyfikatach nie można wykonywać operacji przez nieszyfrowane kanały, czyli zwykłe/podstawowe. Na urządzeniach należy zaznaczyć opcje „Zaszyfrowane i niezaszyfrowane" lub „Tylko zaszyfrowane".
- Na AXIS T85 PoE+ Network Switch Series nie można włączyć protokołu HTTPS.

### IEEE 802.1X

Z perspektywy uwierzytelniania IEEE 802.1X w AXIS Camera Station 5 suplikantem jest dowolne urządzenie sieciowe Axis, które chce nawiązać połączenie z siecią LAN. Elementem uwierzytelniającym jest urządzenie sieciowe, takie jak przełącznik Ethernet lub bezprzewodowy punkt dostępowy. Serwer uwierzytelniający jest zwykle hostem z uruchomionym oprogramowaniem obsługującym protokoły RADIUS i EAP.

Aby włączyć IEEE 802.1X, należy zaimportować certyfikat urzędu certyfikacji uwierzytelniania IEEE 802.1X. Certyfikat CA uwierzytelniania IEEE 802.1X i certyfikat klienta IEEE 802.1X są instalowane po włączeniu lub aktualizacji protokołu IEEE 802.1X. Certyfikat służący do uwierzytelniania może być pozyskiwany z zewnątrz, na przykład z serwera uwierzytelniania w standardzie IEEE 802.1X, lub bezpośrednio z AXIS Camera Station 5. Ten certyfikat instaluje się na każdym urządzeniu Axis i sprawdza serwer uwierzytelniania.

Uwaga

Aby można było używać certyfikatów IEEE 802.1X, urządzenia wideo muszą mieć zainstalowane oprogramowanie sprzętowe w wersji 5.50 lub nowszej, a urządzenia kontroli dostępu i audio potrzebują oprogramowania sprzętowego w wersji 1.25 lub nowszej.

Aby skonfigurować protokół IEEE 802.1X:

1. Wybierz kolejno opcje **Configuration > Security > Certificates (Konfiguracja > Zabezpieczenia > Certyfikaty)**.
2. W menu rozwijanym **EAPOL Version (Wersja protokołu EAPO)** zaznacz wersję protokołu Extensible Authentication Protocol (EAP), której chcesz używać.
3. W menu rozwijanym **EAP identity (Tożsamość EAP)** wybierz używanie adresu MAC urządzenia, nazwy hosta urządzenia lub niestandardowego tekstu.
4. Jeżeli zaznaczono opcję **Custom (Niestandardowa)**, w polu **Custom (Niestandardowa)** wprowadź dowolny tekst, który ma pełnić rolę tożsamości EAP.
5. Kliknij **Import (Importuj)** i wybierz plik certyfikatu CA uwierzytelniania IEEE 802.1X.
6. Z rozwijalnego menu **Common name (Nazwa pospolita)** wybierz **Device IP address (Adres IP urządzenia)** lub **Device EAP identity (Tożsamość EAP urządzenia)** jako nazwy używane w poszczególnych certyfikatach tworzonych dla każdego urządzenia, gdy AXIS Camera Station 5 pełni funkcję urzędu certyfikacji.
7. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
8. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno opcje **Security > IEEE 802.1X > Enable/Update (Bezpieczeństwo > IEEE 802.1X > Włącz/aktualizuj)**.

**Ograniczenia**

- W urządzeniach z kilkoma kartami sieciowymi (np. w kamerach bezprzewodowych) obsługę protokołu IEEE 802.1X można włączyć tylko dla pierwszej karty, zazwyczaj przewodowej.

- Urządzenia, w których brakuje parametru `Network.Interface.I0.dot1x.Enabled`, nie są obsługiwane. Na przykład: urządzenia z serii AXIS P39, AXIS T85 i dekoder wideo T87 Video Decoder.
- Na certyfikatach nie można wykonywać operacji przez nieszyfrowane kanały, czyli zwykłe/podstawowe. Na urządzeniach należy zaznaczyć opcje „Zaszyfrowane i niezaszyfrowane" lub „Tylko zaszyfrowane".

**Ostrzeżenie o wygaśnięciu certyfikatu**

Ostrzeżenie jest wyświetlane po wygaśnięciu certyfikatu klienta lub serwera albo krótko przed ich wygaśnięciem. W przypadku niektórych certyfikatów ostrzeżenie wyzwala też alarm systemowy. Dotyczy to wszystkich certyfikatów klienta i serwera, certyfikatów urzędu certyfikacji urządzeń instalowanych przez AXIS Camera Station 5, certyfikatu urzędu certyfikacji CA AXIS Camera Station 5 i certyfikatu IEEE 802.1X. Ostrzeżenie wyświetlane jest jako komunikat w sekcji **Status (Stan)** na stronie **Device management (Zarządzanie urządzeniem)** oraz w formie ikony na liście **Installed certificates (Zainstalowane certyfikaty)**.

W obszarze **Certificate expiration warning (Ostrzeżenie o wygaśnięciu certyfikatu)** określ, na ile dni przed wygaśnięciem certyfikatu chcesz otrzymać powiadomienie z AXIS Camera Station 5.

**Odnowienie certyfikatu**

**Odnawianie certyfikatu uwierzytelniającego komunikację między serwerem i urządzeniami**

Certyfikaty klienta urządzenia lub serwera wygenerowane przez AXIS Camera Station 5 są odnawiane automatycznie 7 dni przed pojawieniem się ostrzeżenia o wygaśnięciu. Aby było to możliwe, na urządzeniu musi być włączony protokół HTTPS lub IEEE 802.1X. Jeśli chcesz manualnie odnowić lub zaktualizować certyfikat, zobacz *Bezpieczeństwo, on page 64*.

**Odnawianie certyfikatu uwierzytelniającego komunikację między serwerem i klientem**

1. Wybierz kolejno opcje **Configuration (Konfiguracja)** > **Security (Bezpieczeństwo)** > **Certificates (Certyfikaty)**.
2. W obszarze **Odnowienie certyfikatu** kliknij przycisk **Odnów**.
3. Aby odnowiony certyfikat został zastosowany, zrestartuj serwer.

**Resetowanie hasła**

1. Wybierz kolejno opcje **Configuration > Security > Certificates (Konfiguracja > Zabezpieczenia > Certyfikaty)**.
2. Włącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia), aby upewnić się, że urządzenia korzystające z certyfikatów UC są dostępne.
3. W obszarze **Certificate authority (Organ wydający certyfikat)** kliknij **Generate (Generuj)** i wprowadź hasło.
4. W obszarze **Certificate authority (Organ wydający certyfikat)** kliknij **Export (Eksportuj)**, aby lokalnie zapisać certyfikat CA.
5. Wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)** i włącz obsługę protokołu HTTPS na wybranych urządzeniach.
6. Włącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).

## Konfigurowanie kontroli dostępu

Jeżeli do systemu dodano sieciowy kontroler drzwiowy Axis, można skonfigurować sprzęt kontroli dostępu w programie AXIS Camera Station w wersji 6.x lub nowszej.

Kompletny proces konfigurowania sieciowego kontrolera drzwi Axis w oprogramowaniu AXIS Camera Station 5 opisano w temacie *Konfigurowanie sieciowego kontrolera drzwi Axis*.

Uwaga

Na początek wykonaj następujące czynności:

- Zaktualizuj wersję systemu operacyjnego AXIS OS kontrolera w sekcji **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
- Ustaw datę i godzinę kontrolera w oknie **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
- Włącz obsługę protokołu HTTPS na kontrolerze w oknie **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.

**Proces konfigurowania kontroli dostępu**

1. Aby zmodyfikować predefiniowane profile identyfikacji lub utworzyć nowy profil identyfikacji, patrz *Profile identyfikacji, on page 149*.
2. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, patrz *Formaty kart i kod PIN, on page 150*.
3. Dodaj drzwi i zastosuj do nich profil identyfikacji. Patrz *Dodawanie drzwi, on page 138*.
4. Skonfiguruj drzwi.
   - *Dodawanie monitora drzwi, on page 142*
   - *Dodaj wejście awaryjne, on page 143*
   - *Dodawanie czytnika, on page 143*
   - *Dodawanie urządzenia REX, on page 146*
5. Dodaj strefę, a następnie drzwi do strefy. Patrz *Dodawanie strefy, on page 146*.

## Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

W poniższej tabeli przedstawiono minimalną i zalecaną wersję systemu AXIS OS dla poszczególnych wersji programu AXIS Camera Station 5:

| Wersja AXIS Camera Station | Zalecana wersja systemu AXIS OS |
|---|---|
| 5.59 | 12.4.68.1 |
| 5.58 | 12.4.68.1 |
| 5.57 | 11.8.20.2 |

## Drzwi i strefy

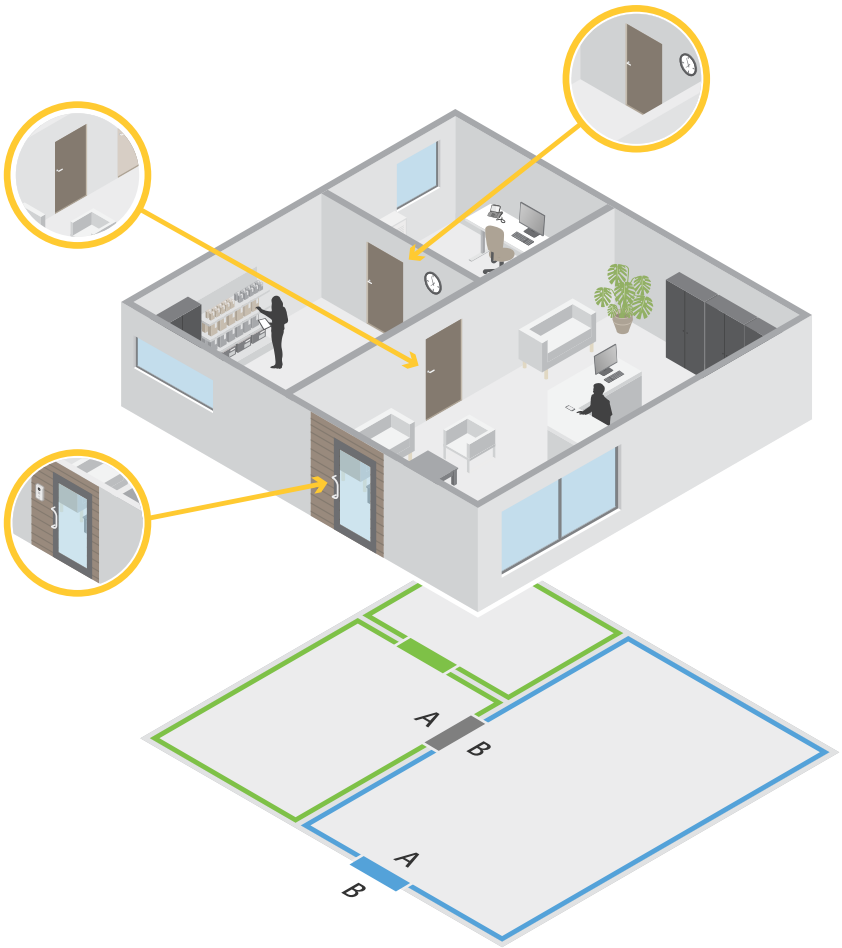
Wybierz kolejno opcje **Configuration > Access control > Doors and zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**, aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

| | |
|---|---|
| **Przypnij wykres** | Wyświetlić schemat styków kontrolera drzwi. Jeżeli chcesz wydrukować schemat styków, kliknij przycisk **Print (Drukuj)**. |
| **Profil identyfikacji** | Zmień profil identyfikacji w drzwiach. |
| **Bezpieczny kanał** | Włącz lub wyłącz bezpieczny kanał OSDP dla konkretnego czytnika. |

| **Drzwi** | |
|---|---|
| Nazwa | Nazwa drzwi. |
| Kontroler drzwi | Kontroler drzwi, z którym są połączone drzwi. |
| Strona A | Strefa, w której znajduje się strona A drzwi. |

| | |
|---|---|
| Strona B | Strefa, w której znajduje się strona B drzwi. |
| Profil identyfikacji | Profil identyfikacji przypisany do drzwi. |
| Formaty kart i kod PIN | Pokazuje typ formatów kart lub długość kodu PIN. |
| Status | Status drzwi.<br>• **Online:** Drzwi są w trybie online i działają prawidłowo.<br>• **Czytnik offline:** Czytnik podany w konfiguracji drzwi jest w trybie offline.<br>• **Błąd czytnika:** Czytnik podany w konfiguracji drzwi nie obsługuje bezpiecznego kanału albo dla czytnika nie włączono bezpiecznego kanału. |
| **Strefy** | |
| Nazwa | Nazwa strefy. |
| Liczba drzwi | Liczba drzwi należących do strefy. |

**Przykład drzwi i stref**




- Istnieją dwie strefy: zielona i niebieska.
- Istnieje troje drzwi: zielone, niebieskie i brązowe.
- Zielone drzwi są wewnętrznymi drzwiami w zielonej strefie.
- Niebieskie drzwi są drzwiami obwodowymi wyłącznie niebieskiej strefy.

- Brązowe drzwi są drzwiami obwodowymi stref zielonej i niebieskiej.

**Dodawanie drzwi**

Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku.

Aby dodać drzwi poprzez utworzenie nowej konfiguracji drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **Add door** (Dodaj drzwi) i z rozwijalnej listy wybierz rodzaj drzwi.

| **Typy drzwi** | |
|---|---|
| **Drzwi** | Zwykłe drzwi z monitorem drzwi obsługującym rygle i czytniki. Wymaga kontrolera drzwiowego. |
| **Drzwi bezprzewodowe** | Drzwi, które można skonfigurować za pomocą bezprzewodowych rygli i koncentratorów komunikacyjnych ASSA ABLOY Aperio®. Więcej informacji znajduje się w sekcji *Dodaj zamek bezprzewodowy, on page 141*. |
| **Drzwi dozorujące** | Drzwi, które mogą zgłaszać, czy są otwarte, czy zamknięte. Więcej informacji znajduje się w sekcji . |
| **Drzwi zastępcze** | Drzwi, które można dodać do systemu jako symbol zastępczy bez konieczności dobierania do nich osprzętu. |
| **Piętro** | Rodzaj drzwi do sterowania windą uwierzytelniający dostęp do pięter z windy za pomocą czytników kart. Więcej informacji znajduje się w sekcji . |

3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami. Kontroler jest wyszarzony, gdy nie można dodać kolejnych drzwi, gdy jest offline lub serwer HTTPS nie jest aktywny.
4. Kliknij przycisk **Next (Dalej)**, aby przejść do strony konfiguracyjnej drzwi.
5. W rozwijalnym menu **Primary lock (Zamek główny)** wybierz port przekaźnika.
6. Aby skonfigurować dwa zamki w drzwiach, wybierz port przekaźnika z rozwijalnego menu **Secondary lock (Drugi zamek)**.
7. Wybierz profil identyfikacji. Patrz *Profile identyfikacji, on page 149*.
8. Skonfiguruj ustawienia drzwi. Zobacz *Ustawienia drzwi, on page 139*.
9. *Dodawanie monitora drzwi, on page 142*
10. *Dodaj wejście awaryjne, on page 143*
11. *Dodawanie czytnika, on page 143*
12. *Dodawanie urządzenia REX, on page 146*
13. Kliknij przycisk **Zapisz**.

Aby dodać drzwi poprzez skopiowanie istniejącej konfiguracji drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).

2. Kliknij **Add door (Dodaj drzwi)**.
3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami.
4. Kliknij **Next (Dalej)**.
5. Z rozwijalnego menu **Copy configuration (Kopiuj konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarzony, jeśli został skonfigurowany z dwoma drzwiami lub jednymi drzwiami z dwoma zamkami.
6. W razie potrzeby zmień ustawienia.
7. Kliknij przycisk **Zapisz**.

Aby zmodyfikować drzwi:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Doors (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Drzwi)**.
2. Wybierz drzwi z listy.
3. Kliknij **Edit (Edytuj)**.
4. Zmień ustawienia i kliknij przycisk **Save (Zapisz)**.

Aby usunąć drzwi:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Doors (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Drzwi)**.
2. Wybierz drzwi z listy.
3. Kliknij **Remove (Usuń)**.
4. Kliknij **Tak**.


*Dodawanie i konfigurowanie drzwi i stref*

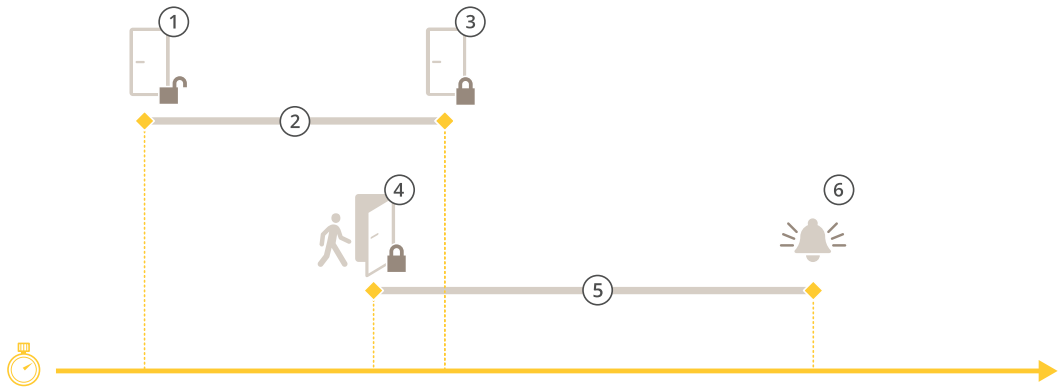
**Ustawienia drzwi**

1. Wybierz kolejno opcje **Configuration > Access control > Door and Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**.
2. Wybierz drzwi, które chcesz edytować.
3. Kliknij **Edit (Edytuj)**.

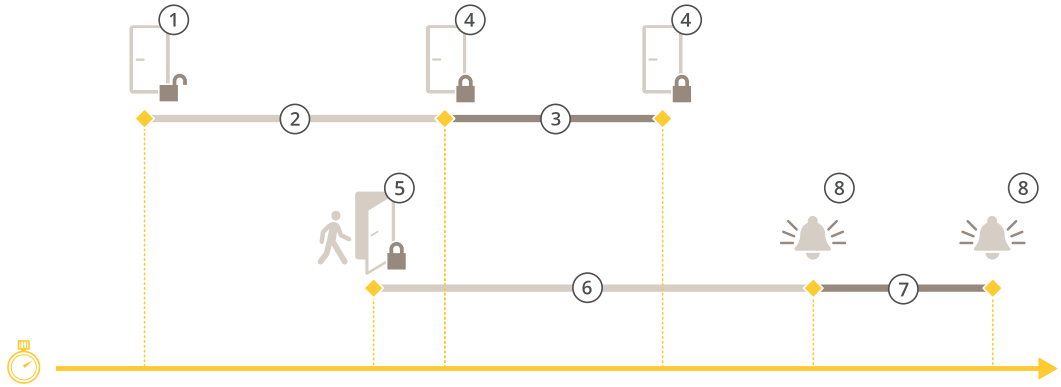
| | |
|---|---|
| **Czas dostępu (s)** | Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Drzwi pozostają odblokowane do momentu ich otwarcia lub przez określony czas. Drzwi blokują się po zamknięciu, nawet jeśli nie upłynął limit czasu dostępu. |
| **Open-too-long time (sec) (Przekroczony czas otwarcia drzwi (s))** | Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączony alarm zbyt |

| | |
|---|---|
| | długiego otwarcia drzwi. Ustaw regułę akcji, aby skonfigurować akcję, którą powinno wyzwolić zdarzenie zbyt długiego otwarcia drzwi. |
| **Długi czas dostępu (s)** | Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Po włączeniu tego ustawienia zastępuje ono czas dostępu obecnie ustawiony dla posiadaczy kart. |
| **Long open-too-long time (sec) (Długi czas przekroczenia otwarcia drzwi (s))** | Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączone zdarzenie zbyt długiego otwarcia drzwi. Długi czas przekroczenia otwarcia drzwi zastępuje już ustawiony czas otwarcia dla posiadaczy kart, jeśli włączona jest opcja **Long access time (Długi czas dostępu)**. |
| **Czas opóźnienia do ponownego zablokowania (ms)** | Ustaw czas w milisekundach, przez jaki drzwi pozostają odblokowane po ich otwarciu lub zamknięciu. |
| **Ponowne zablokowanie** | • **After opening: (Po otwarciu)** Dotyczy tylko scenariuszy z dodanym monitorem drzwi.<br>• **After closing: (Po zamknięciu)** Dotyczy tylko scenariuszy z dodanym monitorem drzwi. |
| **Drzwi wyważone** | Wybierz, czy system ma wyzwalać alarm w przypadku wyważenia drzwi. |
| **Przekroczony czas otwarcia drzwi** | Wybierz, czy system ma wyzwalać alarm w przypadku, gdy drzwi pozostają zbyt długo otwarte. |

**Opcje czasu**




1 *Dostęp przyznany – zamek odblokowany*
2 *Czas dostępu*
3 *Nie podjęto żadnych działań – zamek zablokowany*
4 *Podjęto działanie (otwarto drzwi) – zamek zablokowany lub pozostaje odblokowany do momentu zamknięcia drzwi*
5 *Przekroczony czas otwarcia drzwi*
6 *Otwarte zbyt długo – uruchamiany jest alarm*




1 *Dostęp przyznany – zamek odblokowany*
2 *Czas dostępu*
3 *2+3: Długi czas dostępu*
4 *Nie podjęto żadnych działań – zamek zablokowany*
5 *Podjęto działanie (otwarto drzwi) – zamek zablokowany lub pozostaje odblokowany do momentu zamknięcia drzwi*
6 *Przekroczony czas otwarcia drzwi*
7 *6+7: Długi czas przekroczenia otwarcia drzwi*
8 *Otwarte zbyt długo – uruchamiany jest alarm*

### Dodaj zamek bezprzewodowy

AXIS Camera Station 5 obsługuje zamki bezprzewodowe ASSA ABLOY Aperio® i koncentratory komunikacyjne. Zamek bezprzewodowy łączy się z systemem za pośrednictwem koncentratora komunikacyjnego Aperio podłączonego do złącza RS485 kontrolera drzwi. Do jednego kontrolera drzwi można podłączyć 16 zamków bezprzewodowych.

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

Uwaga

- Konfiguracja wymaga, aby kontroler drzwi Axis miał system AXIS OS w wersji 11.6.16.1 lub nowszej.
- Konfiguracja wymaga ważnej licencji AXIS Door Controller Extension.
- Czas na kontrolerze drzwi Axis i serwerze AXIS Camera Station 5 musi być zsynchronizowany.
- Przed rozpoczęciem skorzystaj z aplikacji Aperio obsługiwanej przez ASSA ABLOY, aby sparować zamki Aperio z koncentratorem Aperio.
- Zamki bezprzewodowe nie działają zgodnie z harmonogramami odblokowywania, gdy są w trybie offline.

1. Otwórz kontroler drzwi.
   1.1. Wybierz kolejno opcje **Configuration > Devices > Other devices (Konfiguracja > Urządzenia > Inne urządzenia)**.
   1.2. Otwórz interfejs WWW kontrolera drzwi podłączonego do koncentratora komunikacyjnego Aperio.
2. Włącz AXIS Door Controller Extension.
   2.1. W interfejsie WWW kontrolera drzwi przejdź do opcji **Apps (Aplikacje)**.
   2.2. Otwórz menu kontekstowe AXIS Door Controller Extension .

2.3. Kliknij polecenie **Activate license with a key (Aktywuj licencję kluczem)** i wybierz licencję.

2.4. Włącz **AXIS Door Controller Extension**.

3. Podłącz zamek bezprzewodowy do kontrolera drzwi za pośrednictwem koncentratora komunikacyjnego.

3.1. W interfejsie WWW kontrolera drzwi przejdź do menu **Access control > Wireless locks (Kontrola dostępu > Zamki bezprzewodowe)**.

3.2. Kliknij polecenie **Connect communication hub (Połącz koncentrator komunikacyjny)**.

3.3. Wprowadź nazwę koncentratora i kliknij przycisk **Connect (Połącz)**.

3.4. Kliknij przycisk **Connect wireless lock (Podłącz zamek bezprzewodowy)**.

3.5. Wybierz adres i funkcje zamka, który chcesz dodać, a następnie kliknij przycisk **Save (Zapisz)**.

4. Dodaj i skonfiguruj drzwi z zamkiem bezprzewodowym.

4.1. W sekcji AXIS Camera Station 5 wybierz kolejno **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.

4.2. Kliknij + **Add door (Dodaj drzwi)**.

4.3. Wybierz kontroler drzwi podłączony do koncentratora komunikacyjnego Aperio, wybierz **Wireless door (Drzwi bezprzewodowe)** jako **Door type (Typ drzwi)**.

4.4. Kliknij **Next (Dalej)**.

4.5. Wybierz **Wireless lock (Zamek bezprzewodowy)**.

4.6. Określ strony A i B drzwi i dodaj czujniki. Więcej informacji znajduje się w rozdziale *Drzwi i strefy, on page 136*.

4.7. Kliknij przycisk **Zapisz**.

Po podłączeniu zamka bezprzewodowego można sprawdzić poziom naładowania baterii i stan zamka w przeglądzie drzwi.

| Poziom baterii | Akcja |
|---|---|
| Dobrze | Brak |
| Niski | Zamek działa zgodnie z przeznaczeniem, ale należy wymienić baterię, zanim jej poziom stanie się krytyczny. |
| Krytyczny | Wymień baterię. Zamek może nie działać prawidłowo. |

| Status zamka | Akcja |
|---|---|
| Online | Brak |
| Zacięcie zamka | Rozwiąż wszelkie problemy mechaniczne. |

**Dodawanie monitora drzwi**

Monitor drzwi to przełącznik położenia drzwi, który monitoruje fizyczny stan drzwi. Po dodaniu monitora do drzwi można określić sposób podłączenia jego obwodów.

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 138*.
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.
3. Wybierz opcję **Door monitor sensor (Czujnik monitora drzwi)**.
4. Zaznacz port we/wy, do którego chcesz podłączyć monitor drzwi.
5. W obszarze **Door open if (Otwórz drzwi, jeśli)**, wybierz sposób podłączenia obwodów monitora drzwi.

6. Aby zmiany stanu cyfrowego wejścia były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Debounce time (Czas odbicia)**.
7. Aby przerwanie połączenia między kontrolerem drzwi i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Patrz *Nadzorowane wejścia, on page 148*.

| **Drzwi otwarte, jeśli** | |
|---|---|
| **Obwód jest otwarty** | Obwód monitora drzwi jest rozwierny (NC). Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty. |
| **Obwód jest zamknięty** | Obwód monitora drzwi jest zwierny (NO). Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty. |

### Dodaj wejście awaryjne

Można dodać i skonfigurować wejście awaryjne, aby zainicjować akcję blokującą lub odblokowującą drzwi. Można również skonfigurować sposób łączenia obwodu.

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 138*.
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.
3. Wybierz opcję **Emergency input (Wejście awaryjne)**.
4. W obszarze **Emergency state (Stan awaryjny)** wybierz połączenie obwodu.
5. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
6. Wybierz **Emergency action (Akcję awaryjną)**, która ma być wyzwalana po odebraniu przez drzwi sygnału stanu awaryjnego.

| **Stan awaryjny** | |
|---|---|
| **Obwód jest otwarty** | Obwód wejścia awaryjnego jest rozwierny (NC). Wejście awaryjne będzie wysyłać sygnał stanu awaryjnego, gdy obwód zostanie otwarty. |
| **Obwód jest zamknięty** | Obwód wejścia awaryjnego jest zwierny (NO). Wejście awaryjne będzie wysyłać sygnał stanu awaryjnego, gdy obwód zostanie zamknięty. |

| **Działanie awaryjne** | |
|---|---|
| **Odblokuj drzwi** | Drzwi odblokowują się po otrzymaniu sygnału stanu awaryjnego. |
| **Zablokuj drzwi** | Drzwi blokują się po otrzymaniu sygnału stanu awaryjnego. |

### Dodawanie czytnika

Kontroler drzwiowy można skonfigurować tak, aby obsługiwał kilka czytników przewodowych. Czytniki można dodać po jednej lub obu stronach drzwi.

Jeżeli do czytnika zastosujesz niestandardową konfigurację formatów kart lub długości numerów PIN, będzie to wyraźnie zaznaczone w kolumnie **Card formats (Formaty kart)** w oknie **Configuration > Access control > Doors and zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**. Patrz *Drzwi i strefy, on page 136*.

Uwaga

- Do kontrolera drzwiowego można również dołączyć maks. 16 czytników Bluetooth. Więcej informacji znajduje się w sekcji *Dodawanie czytnika Bluetooth, on page 145*.
- Jeśli jako czytnik IP używany jest interkom sieciowy Axis, system używa konfiguracji kodu PIN ustawionej na stronie internetowej urządzenia.

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 138*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **Card reader (Czytnik kart)**.
4. Wybierz **Reader type (Typ czytnika)**.
5. Aby użyć niestandardowej konfiguracji długości kodu PIN tego czytnika.
   5.1. Kliknij przycisk **Advanced (Zaawansowane)**.
   5.2. Włącz opcję **Custom PIN length (Niestandardowa długość kodu PIN)**.
   5.3. Wypełnij pola **Min PIN length (Min. długość kodu PIN)**, **Max PIN length (Maks. długość kodu PIN)** i **End of PIN character (Koniec znaku kodu PIN)**.
6. Aby użyć niestandardowego formatu karty tego czytnika.
   6.1. Kliknij przycisk **Advanced (Zaawansowane)**.
   6.2. Włącz opcję **Custom card formats (Niestandardowe formaty kart)**.
   6.3. Wybierz formaty karty na takie, których chcesz używać w czytniku. Jeżeli format karty o tej samej liczbie bitów jest już używany, należy go najpierw zdezaktywować. Gdy konfiguracja formatu karty różni się od skonfigurowanej konfiguracji systemu, w aplikacji klienckiej wyświetlana jest Ikona ostrzeżenia.
7. Kliknij **Dodaj**.
8. Aby dodać czytnik po drugiej stronie drzwi, wykonaj tę procedurę ponownie.

Aby uzyskać informacje o instalacji czytnika kodów kreskowych AXIS Barcode Reader, p. sekcja .

| **Typ czytnika** | |
|---|---|
| **OSDP RS485 half duplex** | Dla czytników RS485 należy wybrać **OSDP RS485 half duplex** i port czytnika. |
| **Wiegand** | W przypadku czytników używających protokołów Wiegand zaznacz opcję **Wiegand** oraz w sekcji Ogólne wybierz port dla czytnika. |
| **Czytnik IP** | W przypadku czytników sieciowych zaznacz opcję **IP reader (Czytnik IP)** i wybierz urządzenie z menu rozwijanego. Wymagania i obsługiwane urządzenia są opisane w temacie *Czytnik IP, on page 145*. |

| **Wiegand** | |
|---|---|
| **Sterowanie LED** | Wybierz opcję **Single wire (Pojedynczy przewód)** lub **Dual wire (R/G) (Podwójny przewód (R/G))**. Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED. |
| **Powiadomienie o sabotażu** | Określ, kiedy wejście wykrywania sabotażu w czytniku ma być aktywne. |

| | |
|---|---|
| | • **Open circuit (Obwód otwarty)**: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie otwarty.<br>• **Closed circuit (Obwód zamknięty)**: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie zamknięty. |
| **Tamper debounce time (Czas odbicia zabezpieczenia sabotażowego)** | Aby zmiany stanu wejścia wykrywania sabotażu w czytniku były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Tamper debounce time (Czas odbicia zabezp. przeciwsab.)**. |
| **Nadzorowane wejście** | Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. Patrz *Nadzorowane wejścia, on page 148*. |

### Dodawanie czytnika Bluetooth

Czytnik AXIS A4612 Network Bluetooth Reader można zastosować do rozszerzenia limitów okablowanych drzwi w kontrolerach drzwiowych Axis, które umożliwiają przydzielenie maks. 16 takich czytników do odnośnych drzwi. Każdy czytnik może zarządzać ryglem drzwiowym, przyciskiem wyjścia (REX) i przełącznikiem pozycji drzwi (DPS).

Dodanie i stosowanie tych czytników nie wymaga dodatkowych licencji.

Aby dodać czytnik AXIS A4612 Network Bluetooth Reader do drzwi:

1. Sprawdź, czy czytnik AXIS A4612 został sparowany z kontrolerem drzwiowym. P. sekcja .
2. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodawanie drzwi, on page 138*.
3. Pod jedną stroną drzwi kliknij przycisk **Add** (Dodaj), a następnie **Card reader** (Czytnik kart).
4. Zaznacz **IP reader** (Czytnik IP) i wybierz sparowany czytnik AXIS A4612 z rozwijalnego menu. Jeżeli czytnik ten będzie stosowany do parowania poświadczeń, zaznacz go na potrzeby parowania. Kliknij **Dodaj**.
5. Na karcie **Overview** (Przegląd) zmień profil identyfikacji. Można użyć profili **Tap in app** (Dotknij w aplikacji) lub **Touch reader** (Czytnik dotykowy), jeżeli czytnik AXIS A4612 jest dołączony po jednej stronie drzwi, a po drugiej stosowany jest przycisk wyjścia REX.

### Czytnik IP

Interkomy sieciowe Axis mogą pełnić rolę czytników IP w aplikacji AXIS Camera Station Secure Entry.

Uwaga

- Potrzebna jest do tego aplikacja AXIS Camera Station w wersji 5.38 lub nowszej oraz kontroler drzwi Axis z oprogramowaniem sprzętowym w wersji 10.6.0.2 lub nowszej.
- Interkom nie wymaga żadnej specjalnej konfiguracji, aby mógł pełnić rolę czytnika IP.

Obsługiwane urządzenia:

- Wideodomofon sieciowy AXIS A8207-VE Network Video Door Station z oprogramowaniem sprzętowym w wersji 10.5.1 lub nowszej
- Wideodomofon sieciowy AXIS A8207-VE Mk II Network Video Door Station z oprogramowaniem sprzętowym w wersji 10.5.1 lub nowszej
- AXIS I8116-E Network Video Intercom

### Dodawanie urządzenia REX

Urządzenie REX (żądanie wyjścia) można dodać z jednej lub obu stron drzwi. Rolę urządzenia REX może pełnić czujnik PIR, przycisk REX lub zamknięcie drążkowe.

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 138*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **REX device (Urządzenie REX)**.
4. Zaznacz port we/wy, na którym chcesz połączyć urządzenie REX. Jeżeli jest dostępny tylko jeden port, zostanie on wybrany automatycznie.
5. Wybierz **Action (Akcja)**, która ma być wyzwalana po odebraniu sygnału REX przez drzwi.
6. W obszarze **REX active (Aktywne REX)** wybierz połączenie obwodu monitora drzwi.
7. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
8. Aby przerwanie połączenia między kontrolerem drzwi i urządzeniem REX powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Patrz *Nadzorowane wejścia, on page 148*.

| **Akcja** | |
|---|---|
| **Odblokuj drzwi** | Wybierz tę opcję, aby odblokować drzwi po odebraniu sygnału REX. |
| **Brak** | Wybierz, jeśli po odebraniu przez drzwi sygnału REX nie ma być wykonywane żadne działanie. |

| **Urządzenie REX aktywne** | |
|---|---|
| **Obwód jest otwarty** | Wybierz, jeżeli obwód REX jest rozwierny. Urządzenie REX wysyła sygnał po otwarciu obwodu. |
| **Obwód jest zamknięty** | Wybierz, jeżeli obwód REX jest zwierny. Urządzenie REX wysyła sygnał po zamknięciu obwodu. |

### Dodawanie strefy

Strefa to konkretny fizyczny obszar zawierający grupę drzwi. Można tworzyć strefy oraz dodawać do nich drzwi. Istnieją dwa rodzaje drzwi:

- **Perimeter door: (Drzwi na obwodzie)** Posiadacze kart wchodzą do strefy i wychodzą ze strefy przez te drzwi.
- **Drzwi wewnętrzne:** Wewnętrzne drzwi w strefie.

Uwaga

Drzwi obwodowe mogą należeć do dwóch stref. Drzwi wewnętrzne mogą należeć tylko do jednej strefy.

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Kliknij + **Add zone (Dodaj strefę)**.
3. Wprowadź nazwę strefy.
4. Kliknij **Add door (Dodaj drzwi)**.
5. Zaznacz drzwi, które chcesz dodać do strefy, i kliknij przycisk **Add (Dodaj)**.
6. Domyślnie drzwi zostaną ustawione jako obwodowe. Aby to zmienić, z menu rozwijanego wybierz pozycję **Internal door (Drzwi wewnętrzne)**.

7. Drzwi obwodowe domyślnie jako wejścia do strefy używają drzwi A. Aby to zmienić, z menu rozwijanego wybierz opcję **Leave (Opuść)**.
8. Aby usunąć drzwi ze strefy, zaznacz ją i kliknij przycisk **Remove (Usuń)**.
9. Kliknij przycisk **Zapisz**.

Aby zmodyfikować strefę:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Wybierz strefę z listy.
3. Kliknij **Edit (Edytuj)**.
4. Zmień ustawienia i kliknij przycisk **Save (Zapisz)**.

Aby usunąć strefę:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Wybierz strefę z listy.
3. Kliknij **Remove (Usuń)**.
4. Kliknij **Tak**.

**Poziom zabezpieczeń strefy**

Do strefy można dodać następujące funkcje zabezpieczeń:

**Anti-passback –** Uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Wymusza on, że dana osoba musi najpierw opuścić obszar, zanim będzie mogła ponownie użyć swoich poświadczeń.

Uwaga

- W przypadku korzystania z funkcji anti-passback wszystkie drzwi w strefie muszą być wyposażone w czujniki położenia drzwi, aby system był w stanie zarejestrować, że użytkownik otworzył drzwi po przeciągnięciu karty.
- Jeśli kontroler drzwi przejdzie w tryb offline, funkcja anti-passback będzie nadal działać, pod warunkiem, że wszystkie drzwi w strefie należą do tego samego kontrolera drzwi. Jeśli jednak drzwi w strefie należą do różnych kontrolerów drzwi, które przejdą w tryb offline, funkcja anti-passback przestanie działać.

Poziom zabezpieczeń można skonfigurować podczas dodawania nowej strefy lub w istniejącej strefie. Aby dodać poziom zabezpieczeń do istniejącej strefy:

1. Wybierz kolejno opcje **Configuration (Konfiguracja)** > **Access control (Kontrola dostępu)** > **Doors and zones (Drzwi i strefy)**.
2. Wybierz strefę, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz zabezpieczenia, które chcesz dodać do drzwi.
6. Kliknij przycisk **Apply (Zastosuj)**.

| **Anti-passback** | |
|---|---|
| **Log violation only (Soft) (Tylko rejestrowanie naruszeń (wersja miękka))** | Użyj tej opcji, jeśli chcesz, aby druga osoba mogła wejść przez drzwi przy użyciu tych samych poświadczeń, co pierwsza osoba. Ta opcja powoduje tylko wywołanie alarmu systemowego. |

| | |
|---|---|
| **Deny access (Hard) (Odmowa dostępu (wersja twarda))** | Użyj tej opcji, jeśli chcesz uniemożliwić drugiej osobie wejście przez drzwi, jeśli używa on tych samych poświadczeń, co pierwsza osoba. Ta opcja powoduje także wywołanie alarmu systemowego. |
| **Limit czasu (w sekundach)** | Czas, po którym system zezwoli użytkownikowi na ponowne wejście. Wprowadź 0, jeśli nie chcesz ustawiać limitu czasu. Oznacza to, że w strefie obowiązuje zasada anti-passback do momentu opuszczenia jej przez użytkownika. Użyj limitu czasu **0** z opcją **Deny access (Hard) (Odmowa dostępu (w wersji twardej)** tylko wtedy, gdy wszystkie drzwi w strefie mają czytniki po obu stronach. |

**Nadzorowane wejścia**

Nadzorowane wejścia mogą wyzwalać zdarzenie w przypadku przerwy w połączeniu z kontrolerem drzwi.

- Podłączenie miedzy kontrolerem drzwi a monitorem drzwi. Patrz *Dodawanie monitora drzwi, on page 142*.
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Patrz *Dodawanie czytnika, on page 143*.
- Podłączenie miedzy kontrolerem drzwi a urządzeniem REX. Patrz *Dodawanie urządzenia REX, on page 146*.

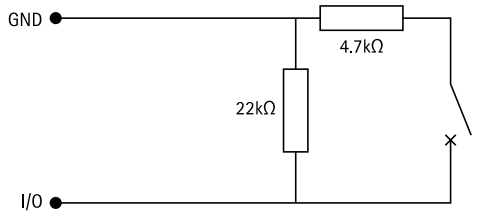
Aby użyć nadzorowanych wejść:

1. Zamontuj rezystory końca linii zgodnie ze schematem połączeń jak najbliżej urządzeń peryferyjnych.
2. Przejdź do strony konfiguracyjnej czytnika, monitora drzwi lub urządzenia REX i włącz opcję **Supervised input (Nadzorowane wejście)**.
3. Jeżeli zastosowano schemat pierwszego połączenia równoległego, wybierz opcję **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Pierwsze połączenie równoległe z 22 kΩ opornikiem równoległym i 4,7 kΩ opornikiem szeregowym)**.
4. Jeżeli zastosowano schemat pierwszego połączenia szeregowego, zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z rozwijalnego menu **Resistor values (Wartości oporników)** wybierz wartość rezystora.

**Schematy połączeń**

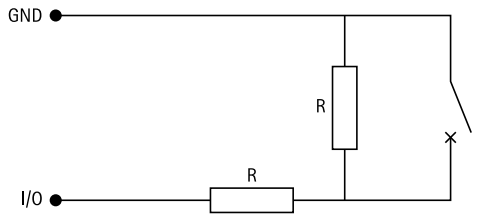
**Pierwsze połączenie równoległe**

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




**Pierwsze połączenie szeregowe**

Oporniki muszą mieć takie same wartości w przedziale 1-10 kΩ.




## Profile identyfikacji

Profil identyfikacji to połączenie typów i harmonogramów identyfikacji. Do jednych lub większej liczby drzwi można zastosować profil identyfikacji, aby określić, jak i kiedy posiadacz karty może uzyskać dostęp do drzwi.

Typy identyfikacji to nośniki informacji o poświadczeniach niezbędnych do uzyskania dostępu do drzwi. Typowe typy identyfikacji to tokeny, osobiste numery identyfikacyjne (PIN), linie papilarne, skany twarzy oraz urządzenia REX. Typ identyfikacji może zawierać jeden lub więcej typów informacji.

Obsługiwane typy identyfikacji: karta, numer PIN, urządzenie REX, statyczne kody QR i dynamiczne kody QR.

Uwaga

Dynamicznych kodów QR i PIN należy używać razem.

Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**, a zostanie wyświetlone okno, w którym można tworzyć, edytować i usuwać profile identyfikacji.

Istnieje pięć domyślnych profili identyfikacji, których można używać w niezmienionej lub zmodyfikowanej postaci.

**Karta –** Aby uzyskać dostęp do drzwi, posiadacz karty musi przeciągnąć kartę przez czytnik.

**Karta i PIN –** Aby uzyskać dostęp do drzwi, posiadacz karty musi przeciągnąć kartę i wpisać numer PIN.

**PIN –** Aby uzyskać dostęp do drzwi, posiadacz karty musi wpisać kod PIN.

**Karta lub kod PIN –** Aby uzyskać dostęp do drzwi, posiadacz karty musi przeciągnąć kartę lub wpisać numer PIN.

**Kod QR –** Aby uzyskać dostęp do drzwi, posiadacz kart musi okazać kod QR Code® do kamery. Profil identyfikacji Kod QR jest używany do statycznych i dynamicznych kodów QR.

**Tablica rejestracyjna –** Posiadacz karty musi jechać w kierunku kamery pojazdem z zatwierdzoną tablicą rejestracyjną.

QRCode to zastrzeżony znak towarowy należący do Denso Wave Incorporated w Japonii i w innych krajach.

Aby utworzyć profil identyfikacji:

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.
2. Kliknij **Create identification profile (Utwórz profil identyfikacji)**.
3. Nadaj nazwę profilowi identyfikacji.
4. Zaznacz opcję **Include facility code for card validation (Uwzględnij kod obiektu w celu weryfikacji karty)**, aby używać kodu obiektu jako jednego z pól służących do weryfikacji poświadczeń. To pole jest dostępne tylko po włączeniu ustawienia **Facility code (Kod obiektu)** w obszarze **Access management > Settings (Zarządzanie dostępem > Ustawienia)**.
5. Skonfiguruj profil identyfikacji po jednej stronie drzwi.
6. Po drugiej stronie drzwi powtórz poprzednie kroki.
7. Kliknij **OK**.

Aby zmodyfikować profil identyfikacji:

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.
2. Zaznacz profil identyfikacji i kliknij .
3. Aby zmienić nazwę profilu identyfikacji, wpisz nową nazwę.
4. Wprowadź zmiany z boku drzwi.
5. Aby zmodyfikować profil identyfikacji po drugiej stronie drzwi, powtórz poprzednie kroki.
6. Kliknij **OK**.

Aby usunąć profil identyfikacji:

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.
2. Zaznacz profil identyfikacji i kliknij .
3. Jeżeli profil identyfikacji został zastosowany do drzwi, wybierz dla nich inny profil identyfikacji.
4. Kliknij **OK**.

| **Edytuj profil identyfikacji** | |
|---|---|
| × | Aby usunąć typ identyfikacji i powiązany z nim harmonogram. |
| **Typ identyfikacji** | Aby zmienić typy identyfikacji, zaznacz je na liście rozwijanej **Identification type (Typ identyfikacji)**. |
| **Schedule** | Aby zmienić harmonogramy, zaznacz je z menu rozwijanego **Schedule (Harmonogram)**. |
| + **Dodaj** | Dodaj typ identyfikacji i powiązany z nim harmonogram, kliknij przycisk **Add (Dodaj)**, a następnie skonfiguruj żądane typy identyfikacji i harmonogramy. |

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

*Konfigurowanie profilu identyfikacji*

## Formaty kart i kod PIN

Format karty decyduje o sposobie przechowywania danych na karcie. Jest to tabela translacji między danymi przychodzącymi a zweryfikowanymi danymi w systemie. Każdy format karty ma inny zestaw reguł i sposób uporządkowania informacji przechowywanych na karcie. Dzięki zdefiniowaniu formatu karty system będzie wiedział, jak interpretować informacje, które kontroler pobiera z czytnika kart.

Istnieje kilka predefiniowanych powszechnie używanych schematów kart, których można używać w istniejącej postaci lub zmodyfikować. Można również tworzyć niestandardowe formaty kart.

Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > kontroli dostępu > Formaty kart i kod PIN)**, aby utworzyć, edytować lub aktywować formaty kart. Można również skonfigurować numer PIN.

Niestandardowe formaty kart mogą zawierać następujące pola danych służące do weryfikowania poświadczeń:

**Numer karty –** Podzbiór binarnych danych poświadczenia, które są zakodowane jako liczby dziesiętne lub szesnastkowe. Numer karty służy do identyfikowania konkretnej karty lub jej posiadacza.

**Kod obiektu –** Podzbiór binarnych danych poświadczenia, które są zakodowane jako liczby dziesiętne lub szesnastkowe. Kod obiektu służy do identyfikowania określonego klienta końcowego lub lokalizacji.

Aby utworzyć format karty:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Kliknij polecenie **Add card format (Dodaj format karty)**.
3. Wprowadź nazwę formatu karty.
4. W polu **Bit length (Liczba bitów)** wpisz liczbę bitów między 1 i 256.
5. Zaznacz opcję **Invert bit order (Odwróć kolejność bitów)**, jeżeli chcesz odwracać kolejność bitów w danych odbieranych z czytnika kart.
6. Zaznacz opcję **Invert byte order (Odwróć kolejność bajtów)**, jeżeli chcesz odwracać kolejność bajtów w danych odbieranych z czytnika kart. Ta opcja jest dostępna tylko w przypadku określenia liczby bitów, którą można podzielić przez osiem.
7. Wybierz i skonfiguruj pola danych, które mają być aktywne w formacie karty. W formacie karty koniecznie musi być aktywne pole **Card number (Numer karty)** lub **Facility code (Kod obiektu)**.
8. Kliknij **OK**.
9. Aby aktywować format karty, zaznacz pole wyboru przed jego nazwą.

Uwaga

- Dwa formaty kart o tej samej długości bitów nie mogą być aktywne w tym samym czasie. Na przykład, jeśli zdefiniowano dwa formaty kart 32-bitowych, tylko jeden z nich może być aktywny. Dezaktywuj jeden format karty, aby aktywować drugi.
- Możesz aktywować i dezaktywować formaty kart tylko wtedy, gdy kontroler drzwi w systemie został skonfigurowany z przynajmniej jednym czytnikiem.

| | |
|---|---|
| ⓘ | Kliknij ⓘ, aby zobaczyć przykład rezultatu odwrócenia kolejności bitów. |
| **Zasięg** | Ustaw zakres bitów danych dla pola danych. Musi się on mieścić w przedziale określonym w polu **Bit length (Liczba bitów)**. |
| **Format wyjściowy** | Wybierz format wyjściowy danych dla pola danych.<br><br>**Decimal (Dziesiętny)**: Nazywany jest również „pozycyjnym systemem liczbowym o podstawie 10", są używane cyfry 0–9.<br><br>**Hexadecimal (Szesnastkowy)**: nazywany również pozycyjnym systemem liczbowym o podstawie 16 – składa się z 16 unikatowych symboli: cyfr 0–9 i liter a–f. |
| **Kolejność bitów podzakresu** | Wybierz kolejność bitów.<br><br>**Little endian**: Pierwszy bit jest najmniejszy (najmniej znaczący).<br><br>**Big endian**: Pierwszy bit jest największy (najbardziej znaczący). |

Aby edytować format karty:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Wybierz format karty i kliknij .
3. W przypadku edytowania wstępnie zdefiniowanego formatu karty można edytować tylko opcje **Invert bit order (Odwracanie kolejności bitów)** i **Invert byte order (Odwróć kolejność)**.
4. Kliknij **OK**.

Usuwać można tylko niestandardowe formaty kart. Aby usunąć niestandardowy format karty:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Zaznacz niestandardowy format karty, a następnie kliknij i **Yes (Tak)**.

Aby zresetować wstępnie zdefiniowany format karty:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Kliknij , aby w formacie karty przywrócić domyślną mapę pól.

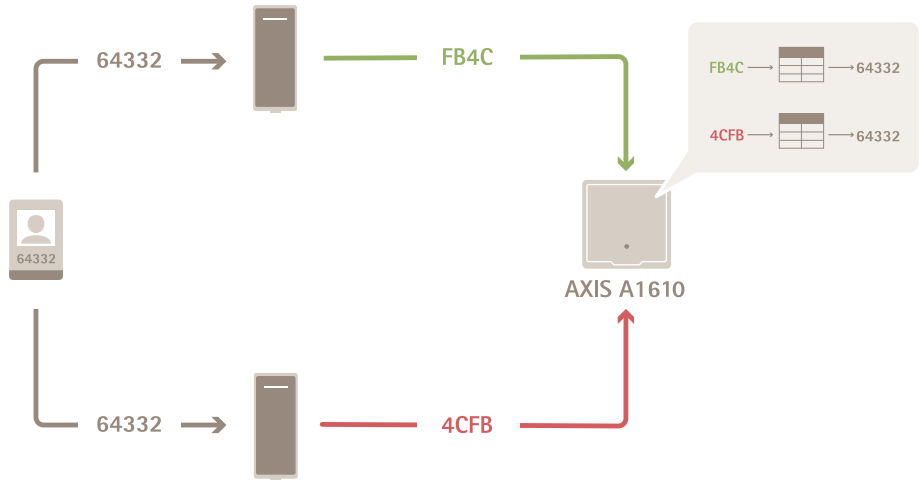
Aby skonfigurować długość numeru PIN:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. W obszarze **PIN configuration (Konfiguracja kodu PIN)** kliknij .
3. Wypełnij pola **Min. długość kodu PIN**, **Maks. długość kodu PIN** i **Koniec znaku kodu PIN**.
4. Kliknij **OK**.


*Konfigurowanie formatów kart*

**Ustawienia formatu karty**

**Informacje ogólne**




- Numer karty w zapisie dziesiętnym ma wartość `64332`.
- Jeden czytnik przekształca numer karty na liczbę szesnastkową `FB4C`. Drugi czytnik przekształca go na liczbę szesnastkową `4CFB`.
- Kontroler AXIS A1610 Network Door Controller odbiera wartość `FB4C` i przekształca ją na wartość dziesiętną `64332` zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.
- Kontroler AXIS A1610 Network Door Controller odbiera wartość `4CFB`, zmienia ją na `FB4C`, odwracając porządek bajtów, i przekształca na wartość dziesiętną `64332` zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.

### Odwróć kolejność bitów

Po odwrócenia kolejności bitów dane karty odebrane od czytnika są odczytywane bit po bicie od prawej do lewej.


### Odwróć kolejność bajtów

Grupa ośmiu bitów tworzy bajt. Po odwrócenia kolejności bajtów dane karty odebrane od czytnika są odczytywane bajt po bajcie od prawej do lewej.


### 26-bitowy standardowy format karty Wiegand


*1 Parzystość wiodąca*
*2 Kod obiektu*

3 *Numer karty*
4 *Parzystość końcowa*

## Szyfrowana komunikacja

### Bezpieczny kanał OSDP

AXIS Camera Station Secure Entry obsługuje bezpieczny kanał OSDP (Open Supervised Device Protocol), który umożliwia szyfrowanie komunikacji pomiędzy kontrolerem i czytnikami Axis.

Włączanie bezpiecznego kanału OSDP dla całego systemu:

1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.
2. Podaj główny klucz szyfrowania i kliknij **OK**.
3. Włącz **OSDP Secure Channel (Bezpieczny kanał OSDP)**. Opcja ta jest dostępna tylko po wprowadzeniu głównego klucza szyfrowania.
4. Domyślnie główny klucz szyfrowania generuje klucz bezpiecznego kanału OSDP. Aby ręcznie ustawić klucz bezpiecznego kanału OSDP:
   4.1. W obszarze **OSDP Secure Channel (Bezpieczny kanał OSDP)** kliknij .
   4.2. Wyczyść opcję **Use main encryption key to generate OSDP Secure Channel key (Użyj głównego klucza szyfrowania, aby wygenerować klucz bezpiecznego kanału OSDP)**.
   4.3. Wpisz klucz bezpiecznego kanału OSDP, a następnie kliknij **OK**.

Aby włączyć lub wyłączyć bezpieczny kanał OSDP dla konkretnego czytnika, zobacz *Drzwi i strefy*.

### AXIS Barcode Reader

AXIS Barcode Reader to aplikacja, którą można instalować w kamerach Axis. Kontroler drzwiowy Axis wykorzystuje klucz uwierzytelniający urządzenia peryferyjnego do przyznawania dostępu oraz uwierzytelniania czytnika AXIS Barcode Reader i aplikacji AXIS License Plate Verifier.

## Multiserwer BETA

W konfiguracji wieloserwerowej globalni posiadacze kart i grupy posiadaczy kart zdefiniowane na serwerze głównym mogą być wykorzystywane na połączonych serwerach podrzędnych.

Uwaga

- Jeden system może obsługiwać do 64 serwerów podrzędnych.
- Wymagane jest oprogramowanie AXIS Camera Station w wersji 5.47 lub nowszej.
- Serwer główny i podrzędne muszą się znajdować w tej samej sieci.
- Na serwerze głównym i podrzędnych koniecznie w Zaporze systemu Windows włącz zezwalanie na przychodzące połączenia TCP na porcie bezpiecznego wchodzenia. Domyślnie jest to port 55767. Niestandardowe konfiguracje portów są omówione w temacie *Zapisy ogólne, on page 186*.
- Dołączenie serwera podrzędnego do serwera głównego powoduje zastąpienie klucza czytnika, a w konsekwencji utratę ważności wszelkich danych uwierzytelniających Bluetooth. Aby do tego nie doszło, utwórz dane uwierzytelniające Bluetooth na serwerze głównym zamiast na serwerze podrzędnym.

### Proces

1. Skonfiguruj serwer jako podrzędny i wygeneruj plik konfiguracyjny. Patrz *Generowanie pliku konfiguracyjnego z serwera podrzędnego, on page 155*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. Patrz *Importowanie pliku konfiguracyjnego do serwera głównego, on page 155*.

3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz *Dodawanie posiadacza karty, on page 160* i *Dodawanie grupy, on page 164*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz *Zarządzanie dostępem, on page 160*.

**Generowanie pliku konfiguracyjnego z serwera podrzędnego**

1. Na serwerze podrzędnym wybierz kolejno opcje **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
2. Kliknij opcję **Sub server (Serwer podrzędny)**.
3. Kliknij przycisk **Generate (Generuj)**. Generuje plik konfiguracyjny w formacie .json.
4. Kliknij przycisk **Download (Pobierz)** i wybierz lokalizację, w której ma zostać zapisany plik.

**Importowanie pliku konfiguracyjnego do serwera głównego**

1. Na serwerze głównym wybierz kolejno opcje **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
2. Kliknij opcję **Main server (Główny serwer)**.
3. Kliknij przycisk + **Add (Dodaj)** i przejdź do pliku konfiguracyjnego wygenerowanego na serwerze podrzędnym.
4. Wprowadź nazwę, adres IP i numer portu serwera podrzędnego.
5. Kliknij przycisk **Import (Importuj)**, aby dodać serwer podrzędny.
6. Stan serwera podrzędnego będzie widoczny jako `Connected` (Połączony).

**Unieważnianie serwera podrzędnego**

Serwer podrzędny można unieważnić tylko zanim jego plik konfiguracyjny zostanie zaimportowany do serwera głównego.

1. Na serwerze głównym wybierz kolejno opcje **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
2. Zaznacz opcję **Serwer podrzędny** i kliknij przycisk **Unieważnij serwer**.
   Teraz można skonfigurować ten serwer jako główny lub podrzędny.

**Usuwanie serwera podrzędnego**

Po zaimportowaniu pliku konfiguracyjnego serwera podrzędnego ów serwer zostanie połączony z serwerem głównym.

Aby usunąć serwer podrzędny:

1. Na serwerze głównym:
   1.1. Wybierz kolejno opcje **Access management > Dashboard (Zarządzanie dostępem > Pulpit nawigacyjny)**.
   1.2. Zmień globalnych posiadaczy kart i grupy na lokalnych posiadaczy kart i grupy.
   1.3. Przejdź do menu **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
   1.4. Kliknij **Main server (Główny serwer)** w celu wyświetlenia listy serwerów podrzędnych.
   1.5. Zaznacz serwer podrzędny i kliknij przycisk **Delete (Usuń)**.
2. Na serwerze podrzędnym:
   – Przejdź do menu **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.

– Kliknij polecenie **Sub server (Serwer podrzędny)** i kliknij przycisk **Revoke server (Unieważnij serwer)**.

### Ustawienia usługi Active directory[BETA]

Uwaga

Konta użytkowników w systemie Microsoft Windows oraz użytkownicy i grupy Active Directory mogą uzyskać dostęp do AXIS Camera Station 5. Sposób dodawania użytkowników w systemie Windows różni się w zależności od wersji. Więcej informacji można uzyskać na stronie *support.microsoft.com*. Jeżeli korzystasz z sieci domeny Active Directory, skonsultuj się z administratorem sieci.

Gdy po raz pierwszy otworzysz ustawienia usługi Active Directory, będziesz mieć możliwość zaimportowania użytkowników Microsoft Active Directory do obszaru posiadaczy kart w AXIS Camera Station 5. Patrz *Importowanie użytkowników usługi Active Directory, on page 156*.

Po wstępnej konfiguracji na stronie ustawień usługi Active Directory pojawią się następujące opcje.

- Tworzenie i zarządzanie grupami posiadaczy kart w oparciu o grupy w Active Directory.
- Skonfiguruj zaplanowaną synchronizację między Active Directory a systemem zarządzania dostępem.
- Zsynchronizuj manualnie, aby zaktualizować dane wszystkich posiadaczy kart zaimportowanych z usługi Active Directory.
- Zarządzaj mapowaniem danych między danymi użytkownika z Active Directory a właściwościami posiadacza karty.

#### Importowanie użytkowników usługi Active Directory

Aby zaimportować użytkowników usługi Active Directory do obszaru posiadaczy kart w AXIS Camera Station 5:

1. W obszarze **Configuration (Konfiguracja)** > **Access control (Kontrola dostępu)** > **Active directory settings (Ustawienia usługi Active Directory)**[BETA].
2. Kliknij **Set up import (Konfiguruj importowanie)**.
3. Postępuj zgodnie z instrukcjami na ekranie, aby wykonać następujące trzy główne kroki:
   3.1. Wybierz użytkownika z usługi Active Directory, który posłuży za szablon mapowania danych.
   3.2. Mapuj dane użytkowników z bazy danych usługi Active Directory do właściwości posiadaczy kart.
   3.3. Utwórz nową grupę posiadaczy kart w systemie zarządzania dostępem i wybierz grupy Active Directory do zaimportowania.

Nie można zmienić żadnych zaimportowanych danych użytkownika, ale można dodać poświadczenia do zaimportowanego posiadacza karty – zob. *Dodaj poświadczenia, on page 161*.

## Konfigurowanie funkcji Inteligentne wyszukiwanie 2

W funkcji Inteligentne wyszukiwanie 2 można ustawić kilka filtrów ułatwiających znajdowanie osób i pojazdów w nagraniach wygenerowanych za pomocą kamer Axis.


Wymagania, ograniczenia i zasady posługiwania się funkcją Inteligentne wyszukiwanie 2 omówiono w temacie *Inteligentne wyszukiwanie 2, on page 33*.

1. Wybierz kolejno **Configuration (Konfiguracja) > Smart search 2 (Inteligentne wyszukiwanie 2) > Settings (Ustawienia)**.
2. W obszarze **Cameras (Kamery)**:
   2.1. Zaznacz kamery, aby wysłać metadane do inteligentnego wyszukiwania 2.
   2.2. Aby zezwolić na klasyfikację serwera w tle dla kamery, wybierz opcję **Allow (Zezwalaj)** w obszarze **Background server classification (Klasyfikacja serwera w tle)**.
   Zwiększy to obciążenie serwera, ale poprawi szybkość działania aplikacji.
   2.3. Aby ograniczyć liczbę detekcji zapisywanych na serwerze, w sekcji **Filter (Filtr)** kliknij ⚙ i utwórz filtry dla funkcji **Area (Obszar)**, **Size and duration (Rozmiar i czas trwania)** oraz **Swaying objects (Kołyszące się obiekty)**.
   Możesz użyć tych filtrów, aby wykluczyć obszary, niewielkie obiekty, obiekty które pojawiają się tylko przez chwilę, albo obiekty kołyszące się takie jak listowie.
3. W obszarze **Storage (Zasób pamięci)**:
   – Zaznacz dysk i folder, gdzie mają być przechowywane nagrania wykrytych obiektów, i kliknij przycisk **Apply (Zastosuj)**.
   – Ustaw limit wielkości pamięci masowej i kliknij przycisk **Apply (Zastosuj)**. Gdy zasób osiągnie swój limit, usuwa najstarsze przypadki detekcji.
4. Wybierz opcję **Include periods with missing metadata (Uwzględnij okresy z brakującymi metadanymi)**, aby wyświetlić wyniki wskazujące, że w danym okresie nie zarejestrowano żadnych metadanych.
5. Zaznacz **Let the server classify detections when you start a search** (Pozwól serwerowi klasyfikować detekcje przy uruchamianiu wyszukiwania), aby uzyskać bardziej szczegółowe wyniki wyszukiwania, w tym detekcje, których kamera nie sklasyfikowała. Aby uzyskać szybsze wyniki wyszukiwania, pozostaw tę opcję bez zaznaczenia.

| **Klasyfikowanie przez serwer w tle** | |
|---|---|
| | Stan klasyfikacji serwera z ostatniej godziny, gdy mechanizm klasyfikowania na serwerze działa wolno. Występuje, gdy program sklasyfikował poniżej 95% wykrytych obiektów. |
| | Stan klasyfikacji serwera z ostatniej godziny, gdy mechanizm klasyfikowania na serwerze działa wolno. Pojawia się w przypadku, gdy program sklasyfikował poniżej 50% wykrytych obiektów. |

## Konfigurowanie funkcji Monitorowanie stanu systemu BETA

Uwaga

- W przypadku aktywnego połączenia z wieloma serwerami AXIS Camera Station 5 można dokonać konfiguracji funkcji Monitorowanie stanu systemu na dowolnym połączonym serwerze. W tym celu wybierz serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.
- W przypadku zarządzania systemami w różnych sieciach usługa chmurowa AXIS System Health Monitoring zapewnia te same funkcje, ale za pośrednictwem chmury. Więcej informacji: *Konfigurowanie usługi AXIS System Health Monitoring Cloud Service, on page 115*.

### Powiadomienia

Aby wysyłać powiadomienia pocztą elektroniczną:

1. Skonfiguruj serwer SMTP oraz serwer poczty e-mail, za pośrednictwem których będą wysyłane powiadomienia. Patrz *Ustawienia serwera, on page 116*
2. Skonfiguruj adresy e-mail, na które będą odbierane powiadomienia. Patrz *Konfigurowanie odbiorców poczty e-mail, on page 158*.

3. Skonfiguruj reguły powiadamiania. Patrz *Konfigurowanie reguł powiadamiania, on page 158*.

**Konfigurowanie odbiorców poczty e-mail**

1. Wybierz kolejno opcje **Configuration > System Health Monitoring > Notifications (Konfiguracja > Monitorowanie stanu systemu > Powiadomienia)**.
2. W polu **Email recipients (Odbiorcy wiadomości e-mail)** wprowadź adres e-mail i kliknij przycisk **Save (Zapisz)**. Powtórz te czynności, aby dodać więcej adresatów wiadomości e-mail.
3. Aby przetestować serwer SMTP, kliknij przycisk **Send test email (Wyślij testową wiadomość e-mail)**. Zostanie wyświetlony komunikat informujący o wysłaniu testowej wiadomości e-mail.

**Konfigurowanie reguł powiadamiania**

Domyślnie są aktywowane dwie reguły powiadamiania.

**System nie działa –** Wysyłanie powiadomienia, gdy system w konfiguracji jednokomputerowej lub dowolny system w konfiguracji wielokomputerowej przestanie działać na co najmniej 5 minut.

**Urządzenie nie działa –** Wysyłanie powiadomienia, gdy urządzenie wyszczególnione w oknie funkcji Monitorowanie stanu systemu przestanie działać na co najmniej 5 minut.

1. Wybierz kolejno opcje **Configuration > System Health Monitoring > Notifications (Konfiguracja > Monitorowanie stanu systemu > Powiadomienia)**.
2. W obszarze **Notification rules (Reguły powiadomienia)** włącz lub wyłącz reguły powiadamiania.
3. W obszarze **Applied rules (Zastosowane reguły)** zostanie wyświetlona lista systemów i urządzeń.

## Multisystem


W funkcji Monitorowania stanu systemu z jednego systemu głównego można śledzić kondycję różnych systemów podrzędnych.

1. W systemie dodatkowym wygeneruj konfigurację systemu. Patrz *Generuj konfigurację systemu, on page 158*.
2. Na komputerze głównym wczytaj konfigurację systemu. Patrz *Pobierz dane z innych systemów, on page 159*.
3. Powtórz poprzednie czynności w pozostałych systemach podrzędnych.
4. Odtąd w systemie głównym można śledzić informacje o kondycji różnych komputerów podrzędnych. Patrz *Monitorowanie stanu systemu [BETA], on page 169*.

**Generuj konfigurację systemu**

1. Wybierz kolejno opcje **Configuration > System Health Monitoring > Multisystem (Konfiguracja > Monitorowanie stanu systemu > Multisystem)**.
2. Kliknij przycisk **Generate (Generuj)**.
3. Kliknij przycisk **Copy (Kopiuj)**, aby przygotować konfigurację do wysłania do głównego komputera.
4. Aby wyświetlić szczegóły konfiguracji systemu, kliknij przycisk **Pokaż szczegóły**.
5. Aby ponownie wygenerować konfigurację systemu, najpierw kliknij przycisk **Delete (Usuń)** i wykasuj istniejącą konfigurację.

Po przekazaniu konfiguracji systemu do głównego systemu informacje o głównym systemie będą wyświetlane w oknie **Systems with access (Systemy z dostępem)**.

**Pobierz dane z innych systemów**

Po wygenerowaniu i skopiowaniu konfiguracji podrzędnego komputera można ją przesłać do głównego komputera.

1. Na głównym komputerze wybierz kolejno opcje **Configuration > System Health Monitoring > Multisystem (Konfiguracja > Monitorowanie stanu systemu > Multisystem)**.
2. Kliknij przycisk **Paste (Wklej)**, aby wprowadzić informacje skopiowane z podrzędnego systemu.
3. Sprawdź adres IP hosta i kliknij przycisk **Add (Dodaj)**.
   Podrzędny system będzie wyświetlany w oknie**Available systems (Dostępne systemy)**.

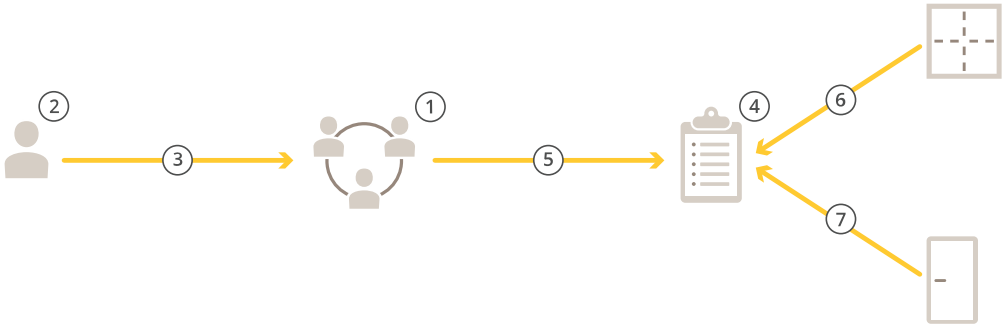
# Zarządzanie dostępem

Karta Access management (Zarządzanie dostępem) umożliwia konfigurowanie posiadaczy kart, grup i reguł dostępu w systemie oraz zarządzanie nimi.

Kompletny proces konfigurowania sieciowego kontrolera drzwi Axis w oprogramowaniu AXIS Camera Station 5 opisano w temacie *Konfigurowanie sieciowego kontrolera drzwi Axis*.

## Proces zarządzania dostępem

Struktura zarządzania dostępem jest elastyczna i pozwala utworzyć przepływ pracy, który najlepiej odpowiada potrzebom użytkownika. Oto przykład przepływu pracy:




1. Dodaj grupy. Patrz *Dodawanie grupy, on page 164*.
2. Dodaj posiadaczy kart. Patrz *Dodawanie posiadacza karty, on page 160*.
3. Dodaj posiadaczy kart do grup.
4. Dodaj reguły dostępu. Patrz *Dodawanie reguły dostępu, on page 164*.
5. Przypisz grupy do reguł dostępu.
6. Przypisz strefy do reguł dostępu.
7. Przypisz drzwi do reguł dostępu.

## Dodawanie posiadacza karty

Posiadacz karty to osoba posiadająca unikatowy identyfikator zarejestrowany w systemie. Skonfiguruj posiadacza karty z poświadczeniami osoby oraz czas i sposób udzielania temu posiadaczowi karty dostępu do drzwi.

Można również wybrać opcję zamapowania użytkowników w bazie danych usługi Active Directory jako posiadaczy kart, patrz *Ustawienia usługi Active directory*$^{BETA}$*, on page 156*.

1. Otwórz kartę zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)** > **Cardholders (Posiadacze kart)** i kliknij **+ Add (+ Dodaj)**.
3. Wprowadź imię i nazwisko posiadacza karty i kliknij **Next (Dalej)**.
4. Opcjonalnie kliknij **Advanced (Zaawansowane)** i wybierz dowolne opcje.
5. Dodaj poświadczenie do posiadacza karty. Patrz *Dodaj poświadczenia, on page 161*
6. Kliknij przycisk **Zapisz**.
7. Dodaj posiadacza karty do grupy.
   7.1. W obszarze **Groups (Grupy)** wybierz grupę, do której chcesz dodać posiadacza karty, i kliknij **Edit (Edytuj)**.

7.2. Kliknij **+ Add (+ Dodaj)** i wybierz posiadacza karty, którego chcesz dodać do grupy. Można wybrać wielu posiadaczy kart.

7.3. Kliknij **Dodaj**.

7.4. Kliknij przycisk **Zapisz**.

| **Zaawansowane** | |
|---|---|
| **Długi czas dostępu** | Wybierz tę opcję, aby w sytuacji, gdy jest zainstalowany monitor drzwi, posiadacz karty miał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi. |
| **Zawieś posiadacza karty** | Wybierz, aby zawiesić posiadacza karty. |
| **Zezwól na podwójne przeciągnięcie** | Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Mogą go na przykład użyć do odblokowania drzwi poza regularnym harmonogramem. |
| **Zwolnienie z blokady ogólnej** | Zaznacz, aby zezwolić posiadaczowi karty na dostęp podczas blokady. |
| **Exempt from anti-passback (Zwolnienie z reguły anti-passback)** | Wybierz tę opcję, aby przyznać zwolnić posiadacza karty z reguły anti-passback. Reguła Anti-passback uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Zanim takie poświadczenia będą mogły zostać użyte ponownie, posiadacz kart z tymi danymi musi najpierw opuścić obszar. |
| **Globalny posiadacz karty** | Zaznacz tę opcję, aby możliwe było wyświetlanie i monitorowanie posiadacza karty na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Patrz *Multiserwer BETA, on page 154*. |

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

*Dodawanie posiadaczy kart i grup*

## Dodaj poświadczenia

Do posiadacza karty można dodać następujące typy poświadczeń:

- Kod QR
- PIN
- Karta
- Tablica rejestracyjna

**Aby dodać do posiadacza karty poświadczenie w postaci kodu QR:**

Uwaga

Korzystanie z kodów QR jako poświadczeń wymaga zsynchronizowania czasu na kontrolerze systemu i kamerze z aplikacją AXIS Barcode Reader. Abu uzyskać idealną synchronizację czasu, zaleca się korzystanie z tego samego źródła czasu dla obu urządzeń.

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **QR-code (Kod QR)**.
2. Wprowadź nazwę poświadczenia.
3. Domyślnie jest włączona opcja **Dynamic QR (Dynamiczny kod QR)**. Używanie dynamicznego kodu QR wymaga podania kodu PIN.
4. Ustaw datę początkową i końcową poświadczenia.
5. Aby kod QR był wysyłany automatycznie po zapisaniu posiadacza karty, zaznacz opcję **Send QR code to cardholder when credential is saved (Po zapisaniu poświadczenia wyślij kod QR do posiadacza karty)**.
6. Kliknij **Dodaj**.

**Aby dodać do posiadacza karty poświadczenie w postaci numeru PIN:**

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **PIN**.
2. Wprowadź numer PIN.
3. Aby używać kodu PIN na wypadek zagrożenia w celu inicjowania cichego alarmu, włącz opcję **Duress PIN (PIN na wypadek zagrożenia)** i wprowadź odpowiedni numer PIN.
4. Ustaw daty ważności poświadczenia: **Valid from** (Ważne od) i **Valid to** (Ważne do).
5. Kliknij **Dodaj**.

Można również skonfigurować PIN na wypadek zagrożenia, który otwiera drzwi oraz dodatkowo wyzwala cichy alarm w systemie.

Uwaga

Posiadacz karty musi mieć adres e-mail, aby otrzymać poświadczenie mobilne.

**Aby dodać do posiadacza karty poświadczenie w postaci karty:**

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **Card (Karta)**.
2. Aby ręcznie wprowadzić dane karty, wprowadź nazwę karty, jej numer i liczbę bitów.

Uwaga

Liczbę bitów można określić tylko w przypadku tworzenia formatu karty o liczbie bitów, która jeszcze nie istnieje w systemie.

3. Aby następowało automatyczne pobieranie danych ostatnio przeciągniętej karty:
   3.1. W menu rozwijanym **Select reader (Wybierz czytnik)** zaznacz czytnik.
   3.2. Przeciągnij kartę w czytniku podłączonym do tych drzwi.
   3.3. Kliknij **Get last swiped card data from the door's reader(s) (Odczytaj dane ostatniej przeciągniętej karty z czytnika)**.

Uwaga

Do sczytania danych karty można użyć biurkowego czytnika kart USB marki 2N. Więcej informacji znajdziesz w temacie *Konfigurowanie biurkowego czytnika kart USB firmy 2N*.

4. Wprowadź kod obiektu. To pole jest dostępne tylko po włączeniu ustawienia **Facility code (Kod obiektu)** w obszarze **Access management > Settings (Zarządzanie dostępem > Ustawienia)**.
5. Ustaw datę początkową i końcową poświadczenia.
6. Kliknij **Dodaj**.

**Aby dodać do posiadacza karty poświadczenie w postaci tablicy rejestracyjnej:**

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **License plate (Tablica rejestracyjna)**.

2. Wprowadź nazwę poświadczenia opisującą dany pojazd.
3. Wprowadź numer tablic rejestracyjnych dla pojazdu.
4. Ustaw datę początkową i końcową poświadczenia.
5. Kliknij **Dodaj**.

Zobacz przykład w temacie *Używanie numeru rejestracyjnego jako poświadczenia, on page 163*.

| **Data wygaśnięcia** | |
|---|---|
| **Ważne od** | Ustaw datę i godzinę ważności poświadczeń. |
| **Ważne do** | Wybierz opcję z menu rozwijanego. |

| **Ważne do** | |
|---|---|
| **Brak daty zakończenia** | Poświadczenie nigdy nie wygasa. |
| **Data** | Ustaw datę i godzinę wygaśnięcia poświadczenia. |
| **Od pierwszego użycia** | Określ, jak długo poświadczenie będzie ważne po pierwszym użyciu. Może to być liczba dni, miesięcy lub lat albo liczba razy po pierwszym użyciu. |
| **Od ostatniego użycia** | Określ, jak długo poświadczenie będzie ważne po ostatnim użyciu. Wybierz dni, miesiące lub lata po ostatnim użyciu. |

### Używanie numeru rejestracyjnego jako poświadczenia

W tym przykładzie pokazano, jak użyć kontrolera drzwi, kamery z AXIS License Plate Verifier i numeru rejestracyjnego pojazdu jako danych uwierzytelniających do przyznania dostępu.

1. Dodaj kontroler drzwi i kamerę do AXIS Camera Station 5. Patrz *Dodawanie urządzeń, on page 5*
2. Ustaw datę i godzinę dla nowych urządzeń, wybierając polecenie **Synchronize with server computer time (Synchronizuj z czasem serwera)**. Patrz *Ustawianie daty i godziny, on page 62*.
3. Uaktualnij oprogramowanie sprzętowe na nowych urządzeniach do najnowszej dostępnej wersji. Patrz *Aktualizuj oprogramowanie sprzętowe, on page 61*.
4. Dodaj nowe drzwi połączone z kontrolerem drzwi. Patrz *Dodawanie drzwi, on page 138*.
   4.1. Dodaj czytnik w obszarze **Side A (Strona A)**. Zob. *Dodawanie czytnika, on page 143*.
   4.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
   4.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
   4.4. Kliknij **OK**.
5. Zainstaluj i włącz w kamerze aplikację AXIS License Plate Verifier. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
6. Włącz aplikację AXIS License Plate Verifier.
7. Skonfiguruj aplikację AXIS License Plate Verifier.
   7.1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.
   7.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuj klucz)**.
   7.3. Otwórz aplikację AXIS License Plate Verifier z poziomu interfejsu WWW kamery.

7.4. Nie przeprowadzaj konfiguracji.

7.5. Przejdź do opcji **Settings (Ustawienia)**.

7.6. W obszarze **Access control (Kontrola dostępu)** wybierz **Secure Entry (Bezpieczne wejście)** jako **Type (Typ)**.

7.7. W obszarze **IP address (Adres IP)** wpisz adres IP kontrolera drzwi.

7.8. W obszarze **Authentication key (Klucz uwierzytelniania)** wklej skopiowany wcześniej klucz uwierzytelniania.

7.9. Kliknij przycisk **Połącz**.

7.10. W obszarze **Door controller name (Nazwa kontrolera drzwi)** wybierz kontroler drzwi.

7.11. W obszarze **Reader name (Nazwa czytnika)** wybierz czytnik dodany wcześniej.

7.12. Włącz integrację.

8. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Patrz *Dodawanie posiadacza karty, on page 160*
9. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Patrz *Dodaj poświadczenia, on page 161*
10. Dodaj regułę dostępu. Patrz *Dodawanie reguły dostępu, on page 164*.
    10.1. Dodaj harmonogram.
    10.2. Dodaj posiadacza karty, któremu chcesz przyznać dostęp do tablicy rejestracyjnej.
    10.3. Dodaj drzwi z czytnikiem AXIS License Plate Verifier.

## Dodawanie grupy

Grupy pozwalają zarządzać posiadaczami kart oraz regułami ich dostępu zbiorowo i skutecznie.

1. Otwórz kartę zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)** > **Groups (Grupy)** i kliknij **+ Add (+ Dodaj)**.
3. Wprowadź nazwę i opcjonalnie inicjały grupy.
4. Zaznacz opcję **Global group (Grupa globalna)**, aby posiadaczy kart można było wyświetlać i monitorować na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Patrz *Multiserwer BETA, on page 154*.
5. Dodawanie posiadaczy kart do grupy:
   5.1. Kliknij **+ Dodaj**.
   5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add (Dodaj)**.
6. Kliknij przycisk **Zapisz**.

## Dodawanie reguły dostępu

Reguła dostępu określa warunki, które muszą zostać spełnione w celu udzielenia dostępu.

Reguła dostępu zawiera następujące elementy:

**Posiadacze kart i ich grupy –** komu ma zostać przyznany dostęp.

**Drzwi i strefy –** gdzie ma zostać przyznany dostęp.

**Harmonogramy –** kiedy ma zostać przyznany dostęp.

Aby dodać regułę dostępu:

1. Otwórz kartę zarządzania dostępem.

2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)**.
3. W obszarze **Access rules (Reguły dostępu)** kliknij **+ Add (+ Dodaj)**.
4. Wprowadź nazwę reguły dostępu i kliknij **Next (Dalej)**.
5. Skonfiguruj posiadaczy kart i grupy:
   5.1. W obszarze **Cardholders (Posiadacze kart)** lub **Groups (Grupy)** kliknij **+ Add (+ Dodaj)**.
   5.2. Wybierz posiadaczy kart lub grupy i kliknij **Add (Dodaj)**.
6. Konfiguracja drzwi i stref:
   6.1. W obszarze **Doors (Drzwi)** lub **Zones (Strefy)** kliknij **+ Add (+ Dodaj)**.
   6.2. Wybierz drzwi lub strefy i kliknij **Add (Dodaj)**.
7. Konfiguracja harmonogramów:
   7.1. W obszarze **Schedules (Harmonogramy)** kliknij **+ Add (+ Dodaj)**.
   7.2. Wybierz jeden lub więcej harmonogramów i kliknij **Add (Dodaj)**.
8. Kliknij przycisk **Zapisz**.

Reguła dostępu, w której brakuje co najmniej jednego z opisanych powyżej składników, jest niekompletna. Wszystkie niekompletne reguły dostępu można obejrzeć na karcie **Incomplete (Niekompletne)**.


### Drzwi

Aby uzyskać informacje na temat czynności wykonywanych ręcznie, takich jak ręczne odblokowywanie drzwi, patrz .

### Strefy

Aby uzyskać informacje na temat czynności wykonywanych ręcznie, takich jak ręczne odblokowywanie strefy, patrz .

## Eksportowanie raportów konfiguracji systemu

Można eksportować raporty zawierające różne rodzaje informacji o systemie. AXIS Camera Station 5 eksportuje raport jako plik CSV (zawierający wartości rozdzielone przecinkami) i zapisuje go w domyślnym folderze pobierania. Aby wyeksportować raport:

1. Otwórz kartę zarządzania dostępem.
2. Przejdź do obszaru **Reports (Raporty)** > **System configuration (Konfiguracja systemu)**.
3. Wybierz raporty, które chcesz wyeksportować, i kliknij **Download (Pobierz)**.

| | |
|---|---|
| **Raport szczegółów posiadaczy kart** | Zawiera informacje o posiadaczach kart, poświadczeniach, weryfikacjach kart i ostatnich transakcjach. |
| **Dziennik dostępu posiadaczy kart** | Zawiera informacje o posiadaczu karty, grupach posiadaczy kart, regułach dostępu, drzwiach i strefach powiązanych z posiadaczami kart. |

| | |
|---|---|
| **Raport dostępu grupy posiadaczy kart** | Zawiera nazwę grupy posiadaczy kart oraz informacje o posiadaczach kart, regułach dostępu, drzwiach i strefach, z którymi jest powiązana grupa posiadaczy kart. |
| **Raport reguły dostępu** | Zawiera nazwę reguły dostępu oraz informacje o posiadaczach kart, grupach posiadaczy kart, drzwiach i strefach, z którymi jest powiązana reguła dostępu. |
| **Raport dostępu do drzwi** | Zawiera nazwę drzwi oraz informacje o posiadaczach kart, grupach posiadaczy kart, regułach dostępu i strefach, z którymi są powiązane drzwi. |
| **Raport dostępu do strefy** | Zawiera nazwę strefy oraz informacje o posiadaczach kart, grupach posiadaczy kart, regułach dostępu i drzwiach, z którymi jest powiązana strefa. |

## Ustawienia zarządzania dostępem

Aby dostosować pola posiadacza karty używane na pulpicie nawigacyjnym dostępu:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia)** > **Custom cardholder fields (Niestandardowe pola posiadacza karty)**.
2. Kliknij **+ Add (+ Dodaj)** i wprowadź nazwę. Można dodać maksymalnie 6 pól niestandardowych.
3. Kliknij **Dodaj**.

Aby używać kodu obiektu do weryfikowania systemu kontroli dostępu:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia)** > **Facility code (Kod obiektu)**.
2. Wybierz **Facility code on (Kod obiektu włączony)**.

Uwaga

Podczas konfigurowania profili identyfikacji należy również zaznaczyć opcję **Include facility code for card validation (Dołącz kod obiektu do sprawdzania poprawności karty)**. Patrz *Profile identyfikacji, on page 149*.

Aby zmodyfikować szablon wiadomości e-mail służący do wysłania poświadczeń QR lub mobilnych:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia)** > **Email templates (Szablony e-mail)**.
2. Zmodyfikuj szablon i kliknij **Update (Aktualizuj)**.

## Import i eksport

### Importuj posiadaczy kart

Ta opcja służy do importowania danych posiadaczy kart i grup posiadaczy karty, poświadczeń oraz zdjęć posiadaczy kart z pliku CSV. Aby można było zaimportować zdjęcia posiadaczy kart, serwer musi mieć dostęp do tych zdjęć.

Po zaimportowaniu posiadaczy kart system zarządzania dostępem automatycznie zapisuje konfigurację systemu, w tym całą konfigurację sprzętową, i usuwa wszystkie wcześniejsze ustawienia.

Można również wybrać opcję zamapowania użytkowników w bazie danych usługi Active Directory jako posiadaczy kart, patrz *Ustawienia usługi Active directory[BETA], on page 156*.

| Opcje importu | |
|---|---|
| **Nowość** | Ta opcja powoduje usunięcie istniejących posiadaczy kart i dodanie nowych. |
| **Aktualizuj** | Opcja ta pozwala zaktualizować dane istniejących posiadaczy kart i dodanie nowych posiadaczy kart. |
| **Dodaj** | Ta opcja powoduje zachowanie istniejących posiadaczy kart i dodanie nowych. Numery kart i identyfikatory posiadaczy kart są unikatowe i można ich użyć tylko raz. |

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Import cardholders (Importuj posiadaczy kart)**.
3. Kliknij przycisk **New (Nowy)**, **Update (Aktualizuj)** lub **Add (Dodaj)**.
4. Kliknij **Next (Dalej)**.
5. Kliknij **Choose a file (Wybierz plik)** i przejdź do pliku CSV. Kliknij przycisk **Otwórz**.
6. Wprowadź separator kolumn i wybierz unikatowy identyfikator, a następnie kliknij **Next (Dalej)**.
7. Przypisz nagłówek do każdej kolumny.
8. Kliknij przycisk **Import (Importuj)**.

| Ustawienia importu | |
|---|---|
| **Pierwszy wiersz to nagłówek** | Wybierz, czy plik CSV zawiera nagłówek kolumny. |
| **Ogranicznik kolumny** | Wprowadź format ogranicznika kolumn w pliku CSV. |
| **Unikalny identyfikator** | Do identyfikowania posiadacza karty system domyślnie używa **Cardholder ID (Identyfikatora posiadacza karty)**. Możesz również użyć imienia i nazwiska lub adresu e-mail. Unikatowy identyfikator zapobiega importowaniu duplikatów rekordów personelu. |
| **Format numeru karty** | Domyślnie jest zaznaczona opcja **Allow both hexadecimal and number (Zezwalaj na liczbę szesnastkową i liczbową)**. |

### Eksportowanie danych posiadaczy kart

Ta opcja powoduje wyeksportowanie zapisanych w systemie danych posiadacza karty do pliku CSV.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Export cardholders (Eksportuj posiadaczy kart)**.
3. Wybierz lokalizację pobierania i kliknij **Save (Zapisz)**.

AXIS Camera Station 5 aktualizuje zdjęcia posiadaczy kart w katalogu `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` przy każdej zmianie konfiguracji.

### Cofanie importu

System automatycznie zapisuje własną konfigurację w momencie importowania posiadaczy kart. Opcja **Undo import (Cofnij import)** powoduje przywrócenie danych posiadaczy kart i całej konfiguracji sprzętowej do stanu sprzed ostatniego importu posiadaczy kart.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Undo import (Cofnij import)**.
3. Kliknij **Tak**.

## Monitorowanie stanu systemu BETA

Karta Monitorowanie stanu systemu umożliwia monitorowanie danych stanu z jednego lub wielu systemów AXIS Camera Station 5 w ramach tej samej sieci.

W przypadku zarządzania systemami w różnych sieciach usługa chmurowa AXIS System Health Monitoring zapewnia te same funkcje, ale za pośrednictwem chmury. Więcej informacji: *Konfigurowanie usługi AXIS System Health Monitoring Cloud Service, on page 115*.

| | |
|---|---|
| | Pokazuje podsumowanie urządzeń i systemów, do których masz dostęp. Patrz *Magazyn, on page 169*. |
| | Pokazuje podsumowanie informacji o pamięci masowej i szczegółów nagrywania dla wszystkich kamer z monitorowanych komputerów. Patrz *Przechowywanie, on page 170*. |
| | Pokazuje dzienniki funkcji Monitorowanie stanu systemu z monitorowanych systemów. Patrz *Powiadomienia, on page 171*. |

### Ograniczenia

- Nie można monitorować przestrzeni dyskowej dla nagrań w AXIS S3008 Recorder.
- Ustawienia powiadomień dotyczą tylko lokalnego serwera funkcji Monitorowanie stanu systemu.
- System flaguje nagrania z wyjątkiem nagrań ciągłych i wyzwalanych ruchem z wartością **None (Brak)** jako typem nagrania.

### Proces

1. *Konfigurowanie funkcji Monitorowanie stanu systemu BETA, on page 157*
   1.1. Skonfiguruj powiadomienia. Patrz *Powiadomienia, on page 157*.
   1.2. Skonfiguruj system wielokomputerowy. Patrz *Multisystem, on page 158*.
2. Monitoruj dane o kondycji z systemów AXIS Camera Station 5.
   2.1. *Magazyn, on page 169*
   2.2. *Przechowywanie, on page 170*
   2.3. *Powiadomienia, on page 171*

### Magazyn

Na stronie Magazyn jest wyświetlane podsumowanie informacji o urządzeniach i systemach, do których masz dostęp.

1. Na karcie **System Health Monitoring (Monitorowanie stanu systemu)** BETA kliknij .
2. Aby zobaczyć podsumowanie systemu, kliknij pozycję **AXIS Camera Station**.
   W prawym panelu zostaną wyświetlone informacje, w tym szczegóły systemu i serwera.
3. Aby wyświetlić podsumowanie informacji o urządzeniu w systemie, kliknij urządzenie na liście.
   W prawym panelu zostaną wyświetlone informacje, w tym szczegóły urządzenia i pamięci masowej oraz informacja, czy urządzenie zawiera źródło wideo.
4. Aby pobrać raport systemowy, wybierz **AXIS Camera Station system report (Raport systemowy AXIS Camera Station)** z rozwijalnego menu **Create report (Utwórz raport)**. Patrz *Raport systemowy, on page 181*.
5. Aby pobrać raport funkcji Monitorowanie stanu systemu:

5.1. Z rozwijalnego menu **Create report (Utwórz raport)** wybierz pozycję **System Health Monitoring report (raport funkcji Monitorowanie stanu systemu)**.

5.2. Aby do raportu dołączyć bazę danych, zaznacz opcję **Include all databases (Dołącz wszystkie bazy danych)** i kliknij przycisk **Download (Pobierz)**.

5.3. Gdy raport będzie gotowy, kliknij, aby go zapisać.

## Przechowywanie

Strona Pamięć masowa zawiera podsumowanie informacji o pamięci masowej oraz szczegóły nagrywania na każdej kamerze należącej do monitorowanego systemu. Kliknięcie nagłówka kolumny umożliwi posortowanie zawartości.

1. Na karcie **System Health Monitoring (Monitorowanie stanu systemu)** BETA kliknij .
2. Jeżeli monitorujesz dane o kondycji systemu wielokomputerowego, wybierz system z rozwijalnego menu.

| **Streszczenie** | |
|---|---|
| Status | Stan pamięci masowej. Patrz *Konfigurowanie pamięci masowej, on page 69*. |
| Lokalizacja | Ścieżka i nazwa pamięci masowej. |
| Łącznie | Łączna wielkość pamięci masowej. Jest to taka sama wartość, jak w ustawieniu „Całkowity rozmiar" we właściwościach lokalizacji zasobu w interfejsie systemu Windows. |
| Przydzielone | Maksymalna ilość zasobu przeznaczona na nagrania. |
| Wykorzystywana | Ilość zasobu obecnie wykorzystywana na nagrania. |
| Data ostatniej aktualizacji | Data i godzina ostatniego zaktualizowania informacji. |

| **Kamera** | |
|---|---|
| Status | (puste): Stan normalny.<br><br>Ikona ostrzeżenia: Kryterium czasu przechowywania nie zostało spełnione.<br><br>Ikona informacyjna: Kryterium czasu przechowywania nie zostało spełnione, ponieważ nagrania z kamery są zbyt krótkie |
| Nazwa | Nazwa kamery. |
| Typ nagrania | Rodzaje nagrywania stosowane w kamerze. |
| Ustaw przechowywanie | Czas przechowywania skonfigurowany dla kamery w oknie **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)**. |
| Bieżące przechowywanie | Liczba dni, przez jaką nagrania z kamery są dotychczas przechowywane w zasobie. |
| Najstarsze nagranie | Godzina wykonania najstarszego nagrania z kamery, jakie znajduje się w zasobie. |
| Najnowsze nagranie | Godzina wykonania najnowszego nagrania z kamery, jakie znajduje się w pamięci masowej. |
| Lokalizacja | Lokalizacja pamięci masowej wykorzystywana przez kamerę. |

| Kamera | |
|---|---|
| Wykorzystywana pamięć masowa | Ilość pamięci masowej zajmowana przez tę kamerę na nagrania. |
| Data ostatniej aktualizacji | Data i godzina ostatniego zaktualizowania informacji. |

## Powiadomienia

Na stronie Powiadomienia są pokazywane dzienniki funkcji Monitorowanie stanu systemu z monitorowanych komputerów. Kliknięcie nagłówka kolumny umożliwi posortowanie zawartości.

Na karcie **System Health Monitoring (Monitorowanie stanu systemu)** BETA kliknij .

| Historia | |
|---|---|
| Wysłano powiadomienie | Data i godzina wysłania powiadomienia. |
| Element | Wyświetla nazwę urządzenia w przypadku powiadomień wyzwalanych regułą `device down` (Urządzenie niedziałające) lub `system` w przypadku powiadomień wyzwalanych regułą `system down` (System niedziałający). |
| System | Nazwa systemu, na którym występuje zdarzenie. |
| Reguła | Reguła, która wyzwoliła powiadomienie. `System down` (System niedziałający) lub `Device down` (Urządzenie niedziałające). |
| Wykryte | Data i godzina wykrycia problemu. |
| Rozwiązane | Data i godzina rozwiązania problemu. |

## Klawisze skrótu

Na karcie „Klawisze skrótu" widoczne są wszystkie dostępne skróty klawiaturowe. Typ klawisza skrótu zależy od metody używanej do sterowania AXIS Camera Station 5.

- Kombinacja klawiszy z klawiatury
- Kombinacja klawiszy z klawiatury numerycznej
- Przycisk joysticka
- Przycisk pokrętła

Usunięcie kamery lub widoku z połączonego serwera powoduje usunięcie również powiązanych skrótów klawiaturowych.

System grupuje klawisze skrótu w następujące kategorie:

- Kamera
- Zarządzanie urządzeniami
- Przejdź do kamery
- Przejdź do widoku
- Nawigacja
- Prepozycje PTZ
- Nagrania
- Sekwencje
- Widok dzielony
- Karta
- Inne

W kategoriach Przejdź do kamer i Przejdź do widoków trzeba przypisać je ręcznie.

Uwaga

- Jeżeli podczas dodawania lub edytowania klawisza skrótu, dany klawisz skrótu jest używany do innej akcji, pojawi się ikona ostrzegawcza. Umieszczenie wskaźnika myszy na ikonie ostrzegawczej spowoduje wyświetlenie akcji powodującej konflikt. Naciśnij klawisz ESC, aby anulować. Naciśnij klawisz ENTER, aby użyć klawisza skrótu i automatycznie usunąć jego powiązanie z inną akcją.
- W przypadku nawiązywania połączenia z wieloma serwerami w kategoriach Przejdź do kamer i Przejdź do widoków również wyświetlane są listy kamer i widoków na podłączonych serwerach.

| | |
|---|---|
| **Przypisanie klawisza skrótu** | Jeżeli wartość klawisza dla akcji jest pusta, możesz ją kliknąć i dodać żądany klawisz szybkiego dostępu do tego działania.<br>• Aby dodać klawisz skrótu za pomocą klawiatury, należy nacisnąć klawisz Ctrl i co najmniej jeden inny klawisz lub klawisz funkcyjny F2–F12.<br>• Aby dodać klawisz skrótu używający elementu klawiatury numerycznej, naciśnij żądaną kombinację klawiszy numerycznych lub jeden z klawiszy funkcyjnych F1-F5.<br>• Aby dodać klawisz szybkiego dostępu używający joysticka lub pokrętła, naciśnij przycisk joysticka lub pokrętła, który ma zostać przypisany do akcji. |
| **Edycja klawisza skrótu** | Kliknij wartość na klawiaturze przypisaną do akcji i zmień tę wartość. |
| **Usuwanie klawisza skrótu** | Kliknij wartość na klawiaturze przypisaną do akcji i usuń tę wartość. |
|  | Kliknij, aby wydrukować tabelę klawiszy skrótów klawiaturowych. |
|  | Kliknij, aby przywrócić domyślne wartości wszystkich klawiszy skrótu. |

## Klawisze panelu sterowania dozoruj wizyjnego

| Mapowanie klawiszy skrótu - joystick | Domyślna akcja | AXIS TU9002 | AXIS T8311 |
|---|---|---|---|
| Przycisk 1 | Przejdź do prepozycji 1 | J1 | J1 |
| Przycisk 2 | Przejdź do prepozycji 2 | J2 | J2 |
| Przycisk 3 | Przejdź do prepozycji 3 | J3 | J3 |
| Przycisk 4 | Przejdź do prepozycji 4 | J4 | J4 |
| Przycisk 5 | Symuluj lewy prawy przycisk | J5 | L |
| Przycisk 6 | Symuluj lewy i prawy przycisk | J6 | R |
| Przycisk 7 | Wybierz poprzednią komórkę w widoku dzielonym | Lewy górny róg | - |
| Przycisk 8 | Wybierz następną komórkę w widoku dzielonym | Prawy górny róg | - |
| Przycisk 9 | Przejdź do poprzedniego nagrania |  | - |
| Przycisk 10 | Odtwórz/wstrzymaj |  | - |

| Mapowanie klawiszy skrótu - joystick | Domyślna akcja | AXIS TU9002 | AXIS T8311 |
|---|---|---|---|
| Przycisk 11 | Przejdź do następnego nagrania |  | - |
| Przycisk 12 | Dodaj zakładkę |  | - |
| Przycisk 13 | Przełączanie funkcji pierścienia zoomu między zoomem cyfrowym a prędkością odtwarzania | M1 | - |
| Przycisk 14 | Przełącz między widokiem na żywo/zarejestrowanym obrazem | M2 | - |
| Przycisk 15 | Klatka: krok wstecz | Lewy górny przełączony | - |
| Przycisk 16 | Klatka: krok do przodu | Prawy górny przełączony | - |

| Mapowanie klawiszy skrótu - klawiatura | Domyślna akcja | AXIS TU9003 | AXIS T8312 |
|---|---|---|---|
| A | Otwórz widoki |  |  |
| B | Przejdź do następnej kamery lub widoku |  |  |
| ALT+B | Przejdź do poprzedniej kamery lub widoku | Alt+  | - |
| KARTA | Przejdź do następnej karty |  | - |
| ALT+TAB | Przejdź do poprzedniej karty | Alt+  | - |
| C | - | - |  |
| D | - | - |  |
| E | - | - |  |
| PLUS | Nastaw ostrość na dalszą odległość | + | - |
| MINUS | Ustaw ostrość na bliższą odległość | - | - |
| F2 | Otwórz klawisze skrótu | F2 | F2 |
| F4 | Otwórz dzienniki | F4 | F4 |

| Mapowanie klawiszy skrótu - klawiatura | Domyślna akcja | AXIS TU9003 | AXIS T8312 |
|---|---|---|---|
| F5 | Otwórz ustawienia | F5 | F5 |
| F10 | Autofokus | F10 | - |

| Mapowanie klawiszy skrótu - pokrętło | Domyślna akcja | AXIS T8313 |
|---|---|---|
| Przycisk 1 pokrętła | Pokazywanie lub ukrywanie znaczników eksportu | L |
| Przycisk 2 pokrętła | Dodaj zakładkę |  |
| Przycisk 3 pokrętła | Przejdź do poprzedniego nagrania |  |
| Przycisk 4 pokrętła | Odtwórz/wstrzymaj |  |
| Przycisk 5 pokrętła | Przejdź do następnego nagrania |  |
| Przycisk 6 pokrętła | Przełącz między widokiem na żywo/ zarejestrowanym obrazem | R |

Uwaga

AXIS T8311 Video Surveillance Joystick nie obsługuje przycisków joysticka 7–10.

## Dzienniki

Domyślnie na karcie Dzienniki są wyświetlane dzienniki na żywo, w tym alarmów na żywo, zdarzeń i audytu. Można również wyszukiwać poprzednie dzienniki. W oknie **Configuration > Server > settings (Konfiguracja > Serwer > Ustawienia)** można określić liczbę dni przechowywania dzienników.

| | |
|---|---|
| **Time (Godzina)** | Data i godzina działania. |
| **Typ** | Typ akcji: Alarm, Zdarzenie lub Audyt. |
| **Kategoria** | Kategoria akcji. |
| **Wiadomość** | Krótki opis akcji. |
| **Użytkownik** | AXIS Camera Station 5 użytkownik wykonujący akcję. |
| **Komputer** | Komputer (nazwa domeny systemu Windows), na którym zainstalowano AXIS Camera Station 5. |
| **Window user (Użytkownik systemu Windows)** | Użytkownik systemu Windows z rolą administratora AXIS Camera Station 5. |
| **Serwer** | Widoczna tylko w przypadku połączenia z wieloma serwerami.<br><br>Serwer, na którym wystąpiło działanie. |
| **Element** | Element, na podstawie którego został wygenerowany dziennik. |

### Wyszukiwanie dzienników

1. Na karcie Logs (Dzienniki) w obszarze **Log search (Przeszukiwanie dziennika)** kliknij przycisk **Search (Szukaj)**.
2. W polu filtrowania wpisz słowa kluczowe. AXIS Camera Station 5 przeszukuje listę dzienników z wyjątkiem **Time (Czas)** i pokazuje wyniki wyszukiwania zawierające wszystkie słowa kluczowe. Obsługiwane operatory wyszukiwania są opisane w temacie *Optymalizowanie wyszukiwania, on page 38*.
3. Wybierz pozycję **Alarms (Alarmy)**, **Audits (Audyty)** lub **Events (Zdarzenia)** w menu **Filter (Filtruj)**.
4. W kalendarzu zaznacz datę lub zakres dat.
5. Z rozwijalnych menu wybierz **Start time (Czas rozpoczęcia)** i **End time (Czas zakończenia)**.
6. Kliknij **Search (Wyszukaj)**.

### Dziennik alarmów

W dzienniku alarmów są wyświetlane listy zawierające alarmy systemowe oraz wygenerowane przez reguły i funkcję detekcji ruchu. Na liście są też takie informacje, jak data i godzina wystąpienia alarmu, kategoria alarmu i komunikat alarmu. Patrz *Alarmy*.

| | |
|---|---|
|  | Kliknij alarm i  , aby otworzyć kartę Recordings (Nagrania) i rozpocząć odtwarzanie, jeśli alarm zawiera nagranie. |
|  | Kliknij alarm i  , aby otworzyć procedurę alarmową, jeśli alarm zawiera procedurę alarmową. |

| | |
|---|---|
|  | Kliknij alarm i  , aby wysłać do innych klientów powiadomienie o podjęciu interwencji po alarmach. |
|  | Kliknij alarm i  , aby wyeksportować dziennik do pliku tekstowego. |

**Dziennik zdarzeń**

W dzienniku zdarzeń na liście są wyświetlane zdarzenia dotyczące kamer i serwera, na przykład zapisów, wyzwalaczy, alarmów, błędów i komunikatów systemowych. Widoczne informacje obejmują datę i godzinę zdarzenia, kategorię zdarzenia oraz komunikat o zdarzeniu. Zaznacz zdarzenia i na pasku narzędzi kliknij  , aby wyeksportować zdarzenia w postaci pliku tekstowego.

**Dziennik audytu**

W dzienniku audytu są widoczne wszystkie działania podjęte przez użytkownika, na przykład ręczne nagrywanie, rozpoczęcie lub zatrzymano przesyłanie strumieniowego przesyłania wideo, aktywowanie reguł akcji, utworzenie drzwi i utworzenie posiadacza karty. Zaznacz audyty i na pasku narzędzi kliknij  , aby wyeksportować audyty w postaci pliku tekstowego.

## Alarmy

Na karcie Alarms (Alarmy), dostępnej w dolnej części okna klienta AXIS Camera Station 5, wyświetlane są wyzwalane zdarzenia oraz alarmy systemowe. Informacje na temat tworzenia alarmów: *Reguły akcji*. Więcej informacji o alarmie „Wymagana jest konserwacja bazy danych" można znaleźć w temacie *Konserwacja bazy danych, on page 199*.

| | |
|---|---|
| **Time (Godzina)** | Godzina wystąpienia alarmu. |
| **Kategoria** | Kategoria zainicjowanego alarmu. |
| **Opis** | Krótki opis alarmu. |
| **Serwer** | Dostępne w przypadku połączenia z kilkoma serwerami. Serwer AXIS Camera Station 5 wysyłający alarm. |
| **Element** | Element, który wyzwala alarm. |
|  | Wyświetlenie procedury alarmowej jest możliwe tylko wtedy, gdy alarm zawiera procedurę alarmową. |
|  | Funkcja przejścia do nagrań jest dostępna tylko wtedy, gdy alarm zawiera nagranie. |
|  | Potwierdź wybrany alarm |
|  | Usuń alarm. Alarm jest usuwany tylko tymczasowo, jeśli nie zostanie potwierdzony przed usunięciem. |

Aby zareagować na konkretny alarm:

1. Kliknij **Alarms and Tasks (Alarmy i zadania)** w dolnej części okna klienta AXIS Camera Station 5 i otwórz kartę **Alarms (Alarmy)**.
2. W przypadku alarmów zawierających nagrania wybierz alarm i kliknij , aby przejść do nagrania na karcie **Recording alerts (Powiadomienia dotyczące nagrań)**.
3. W przypadku alarmów bez nagrań otwórz kartę z podglądem na żywo i kliknij dwukrotnie alarm, aby wyświetlić nagranie z czasu alarmu na karcie **Recording alerts (Powiadomienia dotyczące nagrań)**.
4. W przypadku alarmów zawierających procedurę alarmową wybierz alarm i kliknij , aby otworzyć procedurę alarmową.
5. Aby przekazać innym klientom powiadomienie o obsłużeniu alarmów, wybierz alarmy i kliknij .
6. Aby usunąć alarmy z listy, wybierz je i kliknij .

## Zadania

Karta Tasks (Zadania) znajduje się w dolnej części okna klienta AXIS Camera Station 5.

Zadania wymienione poniżej są osobiste, a w związku z tym widoczne tylko dla administratorów i użytkowników, którzy je rozpoczęli.

- Raport systemowy
- Utwórz raport o zdarzeniu
- Eksportuj nagrania

Administrator może przeglądać i obsługiwać wszystkie zadania uruchomione przez dowolnego użytkownika, w tym zadania osobiste.

Operator lub dozorca może:

- Wyświetlać wszystkie zadania uruchomione przez Ciebie i innych użytkowników, które nie są osobiste.
- Anulować zadania uruchomione przez Ciebie oraz próbować ponownie je uruchomić. Ty możesz tylko próbować ponownie wykonać zadania utworzenia raportu o zdarzeniu i wyeksportowania nagrań.
- Wyświetlać wyniki wszystkich zadań figurujących na liście.
- Usuwać wszystkie zakończone zadania z listy. Dotyczy to tylko lokalnego klienta.

| | |
|---|---|
| **Nazwa** | Nazwa zadania. |
| **Start (Uruchom)** | Godzina rozpoczęcia zadania. |
| **Wiadomość** | Wyświetla stan lub informacje o zadaniu.<br><br>Możliwe statusy:<br>• **Canceling (Anulowanie)**: Czyszczenie przed anulowaniem zadania.<br>• **Canceled (Anulowane)**: Czyszczenie zostało ukończone, a zadanie anulowane.<br>• **Error (Błąd)**: Zadanie zostało ukończone z błędami, tzn. nie zostało pomyślnie wykonane na co najmniej jednym urządzeniu.<br>• **Finished (Zakończono)**: Zadanie zostało ukończone.<br>• **Finished during lost connection (Zakończono podczas utraty połączenia)**: Wyświetlany, jeśli zadanie zostało ukończone w czasie braku połączenia z serwerem. Nie można ustalić stanu zadania.<br>• **Lost connection (Utracono połączenie)**: Wyświetlany, jeśli podczas wykonywania zadania komputer kliencki utracił połączenie z serwerem. Nie można ustalić stanu zadania.<br>• **Running (Uruchomione)**: Zadanie jest w trakcie wykonywania.<br>• **Pending (Oczekiwanie)**: Oczekiwanie na ukończenie innego zadania. |
| **Właściciel** | Użytkownik, który zainicjował zadanie. |
| **Postęp** | Pokazuje postęp zadania. |
| **Serwer** | Opcja dostępna w przypadku połączenia z wieloma serwerami. Powoduje wyświetlenia serwera AXIS Camera Station 5, który wykonuje zadanie. |

Aby wykonać jedno lub więcej zadań:

1. Kliknij **Alarms and Tasks (Alarmy i zadania)** w dolnej części okna klienta AXIS Camera Station 5 i kliknij kartę **Tasks (Zadania)**.

2. Wybierz zadania i kliknij jedną z akcji

| | |
|---|---|
|  | Kliknij, aby wyświetlić okno dialogowe Task result (Wynik zadania). |
|  | Kliknij, aby anulować zadanie. |
|  | Kliknij, aby usunąć zadania z listy. |
|  | Jeżeli zadanie się nie powiedzie w trakcie eksportowania nagrań lub tworzenia raportów o zdarzeniu, kliknij, aby podjąć ponowną próbę wykonania nieudanego zadania. |

**Task result (Wynik zadania)**

Jeżeli zadanie zostało wykonane na wielu urządzeniach, okno dialogowe pokazuje wyniki z każdego urządzenia. Wszystkie nieudane operacje należy dokładniej zbadać, a odnośnych konfiguracji dokonać ręcznie.

W przypadku większości zadań są wyświetlanie informacje wymienione poniżej. W przypadku zadań takich jak eksportowanie nagrań czy raport systemowy dwukrotne kliknięcie zadanie spowoduje otwarcie folderu, w którym pliki zostały zapisane.

| | |
|---|---|
| **Adres MAC** | Adres MAC zaktualizowanego urządzenia. |
| **Adres** | Adres IP zaktualizowanego urządzenia. |
| **Wiadomość** | Informacje o sposobie wykonania zadania:<br>• **Finished (Zakończono)**: Zadanie zostało pomyślnie ukończone.<br>• **Error (Błąd)**: Nie można było ukończyć zadania na urządzeniu.<br>• **Canceled (Anulowane)**: Zadanie zostało anulowane przed ukończeniem. |
| **Opis** | Informacje o zadaniu. |

Zależnie od rodzaju wykonywanego zadania są wyświetlane następujące informacje:

| | |
|---|---|
| **New address (Nowy adres)** | Nowo przypisany adres IP urządzenia. |
| **Reguły akcji** | Wersja oprogramowania sprzętowego i nazwa produktu urządzenia. |
| **Szczegóły** | Numery seryjne i adresy IP zastępowanego i nowego urządzenia. |
| **Reference ID (Identyfikator referencyjny)** | Identyfikator referencyjny raportu o zdarzeniu. |

# Generowanie raportów

## Arkusz konfiguracji klienta

Arkusz konfiguracji klienta przydaje się podczas rozwiązywania problemów i kontaktowania się z działem wsparcia.

Aby wyświetlić raport w formacie HTML z przeglądem konfiguracji systemu klienckiego:

1. Przejdź do obszaru **Configuration (Konfiguracja)** > **Server (Serwer)** > **Diagnostics (Diagnostyka)**.
2. Kliknij **View client configuration sheet (Wyświetl arkusz konfiguracji klienta)**.

## Arkusz konfiguracji serwera

Arkusz konfiguracji serwera zawiera informacje o ogólnej konfiguracji, ustawieniach kamer, regułach akcji, harmonogramach, pamięci masowej nagrań, urządzeniach dodatkowych i licencjach. Przydaje się przy rozwiązaniu problemów oraz kontaktowaniu z działem wsparcia technicznego.

Aby wyświetlić raport w formacie HTML z przeglądem konfiguracji systemu serwera:

1. Przejdź do obszaru **Configuration (Konfiguracja)** > **Server (Serwer)** > **Diagnostics (Diagnostyka)**.
2. Kliknij **View server configuration sheet (Wyświetl arkusz konfiguracji serwera)**.

## Raport systemowy

Raport systemowy jest plikiem .zip, który zawiera parametry i pliki dziennika, pomagające działowi pomocy technicznej Axis zbadać zgłoszony problem.

Przy kontaktowaniu się z działem wsparcia technicznego zawsze dołączaj raport systemowy.

Aby utworzyć raport systemowy:

1. Przejdź do menu w prawym górnym rogu.
2. Kliknij pozycję **Help** > **System report** (Pomoc > Raport systemowy).
3. Jeśli chcesz zmienić automatycznie wygenerowaną nazwę pliku, zmień ją.
4. Kliknij przycisk **Browse (Przeglądaj)** i wskaż miejsce, gdzie chcesz zapisać raport systemowy.
5. Wybierz preferowane ustawienia:
   - **Automatically open folder when report is ready** (Automatyczne otwieranie folderu, gdy raport jest gotowy), aby wyświetlić raport od razu.
   - **Include all databases** (Uwzględnij wszystkie bazy danych), aby dodać szczegółowe informacje o nagraniach i danych systemowych.
   - **Include screenshots of all monitors** (Dołącz zrzuty ekranu wszystkich monitorów), aby uprościć analizę raportów systemowych.
6. Kliknij przycisk **OK**.


*Generowanie raportu systemowego*

## AXIS Installation Verifier

AXIS Installation Verifier umożliwia przeprowadzenie testu działania po zakończeniu instalacji w celu potwierdzenia, że wszystkie urządzenia w systemie są w pełni funkcjonalne. Test trwa ok. 20 minut.

| Testowane są | |
|---|---|
| **Normal conditions (Warunki normalne)** | Test strumieniowania i zapisywania danych przy użyciu bieżących ustawień systemu w aplikacji AXIS Camera Station 5. Wyjście: Powodzenie lub niepowodzenie. |
| **Złe oświetlenie** | Test strumieniowania i zapisywania danych przy użyciu ustawień zoptymalizowanych dla typowych warunków oświetleniowych, na przykład wzmocnienia. Wyjście: Powodzenie lub niepowodzenie. |
| **Test obciążenia** | Test polegający na stopniowym zwiększaniu ilości strumieniowanych i zapisywanych danych do czasu, aż system osiągnie maksimum swoich możliwości. Wyjście: Informacje o maksymalnej wydajności systemu. |

Uwaga

- Można testować tylko wyłącznie urządzenia obsługujące środowisko AXIS Camera Application Platform w wersji 2 (ACAP 2) lub nowszej.
- W czasie testu aplikacja AXIS Camera Station 5 przechodzi w tryb konserwacji, a wszystkie działania systemu dozoru są chwilowo niedostępne.

Aby uruchomić test:

1. Przejdź do obszaru **Configuration (Konfiguracja)** > **Server (Serwer)** > **Diagnostics (Diagnostyka)**.
2. Kliknij **Open AXIS installation verifier (Otwórz narzędzie AXIS installation verifier)**.
3. Kliknij przycisk **Start (Rozpocznij)**.
4. Po zakończeniu testu kliknij przycisk **View report (Wyświetl raport)**, aby obejrzeć raport, lub przycisk **Save report (Zapisz raport)**, aby go zapisać.

## Informacja zwrotna

Można wybrać opcję automatycznego udostępniania anonimowych danych o korzystaniu z aplikacji klienckiej podczas jej konfigurowania oraz ręcznego wysyłania opinii, aby pomagać nam w ulepszaniu aplikacji AXIS Camera Station 5 i poprawianiu wrażeń z jej użytkowania. Patrz *Konfigurowanie klienta, on page 108*.

Uwaga

Nie używaj formularza opinii do przesyłania zgłoszeń o pomoc techniczną.

1. Wybierz kolejno ☰ > **Help (Pomoc)** > **Feedback (Opinia)**.
2. Wybierz reakcję i wypełnij pole opinii.
3. Kliknij przycisk **Send (Wyślij)**.

## Lista zasobów

Można wyeksportować listę zasobów systemu VMS. Lista zawiera nazwy, typy, modele, statusy i numery seryjne następujących składników:

- Wszystkie połączone serwery

- Wszystkie połączone urządzenia
- Terminal klienci, z którego wyeksportowano listę zasobów, jeżeli do systemu podłączono wiele terminali

Aby wyeksportować listę zasobów:

1. Wybierz kolejno > **Other (Inne)** > **Asset list (Lista zasobów)**.
2. Kliknij **Export (Eksportuj)**.
3. Zaznacz lokalizację pliku i kliknij przycisk **Save (Zapisz)**.
4. W menu **Latest export (Ostatni eksport)** zostanie wyświetlone lub uaktualnione łącze do pliku.
5. Kliknięcie łącza spowoduje przejście do lokalizacji pliku.

## Ustawienia urządzenia noszalnego

Aby można było nawiązać połączenie z urządzeniem nasobnym, należy utworzyć plik połączenia. Patrz *Konfigurowanie systemu nasobnego Axis*.

Uwaga

Jeżeli adres IP serwera się zmienił albo oprogramowanie AXIS Camera Station zostało uaktualnione z wersji starszej niż 5.33, to przed wyeksportowaniem pliku połączenia trzeba odnowić certyfikat serwera. Procedurę odnawiania certyfikatu opisano w temacie *Certyfikaty, on page 131*.

Aby utworzyć plik połączenia:

1. Wybierz kolejno > **Other (Inne)** > **Body worn settings (Ustawienia urządzenia nasobnego)**.
2. Aby zmienić domyślną nazwę lokalizacji wyświetlaną w urządzeniu ubieralnym, wpisz nową nazwę.
3. Kliknij **Export (Eksportuj)**.
4. W menu **Latest export (Ostatni eksport)** zostanie wyświetlone lub uaktualnione łącze do pliku.
5. Kliknięcie łącza spowoduje przejście do lokalizacji pliku.


*Konfigurowanie systemu nasobnego Axis*


*Odtwarzane i eksportowane nagrań z kamery nasobnej Axis*

## Status usług Axis

Aby wyświetlić status usług online Axis:

1. Przejdź do obszaru **Configuration (Konfiguracja)** > **Server (Serwer)** > **Diagnostics (Diagnostyka)**.
2. Kliknij **View status of Axis services (Przeglądaj status usług Axis)**.

## AXIS Camera Station 5 Aplikacja Service Control

Serwer używa aplikacji AXIS Camera Station 5 Service Control do uruchamiania się i wyłączania oraz zmieniania swoich ustawień. Aplikacja uruchamia się automatycznie po zakończeniu instalacji. Jeżeli komputer serwera zostanie zrestartowany, sterowanie usługami w ciągu ok. 2 minut również automatycznie się ponownie uruchomi. Ikona w obszarze powiadomień systemu Windows pokazuje, czy status usługi.

Kliknij ikonę prawym przyciskiem myszy. Zobaczysz wtedy następujące polecenia do wyboru: **Open AXIS Camera Station Service Control (Otwórz program AXIS Camera Station Service Control)**, **Start Service (Uruchom usługę)**, **Stop Service (Zatrzymaj usługę)**, **Restart Service (Uruchom ponownie usługę)** oraz **Exit (Zakończ)**.

Aby otworzyć aplikacją Service Control z menu Start:

Przejdź do menu **Start** i wybierz kolejno **All Programs > Tools > Service Control (Wszystkie programy > Narzędzia > Kontrola usług)**.

| | |
|---|---|
|  | Uruchomiono |
|  | Rozpoczynanie |
|  | Zatrzymane |

| | |
|---|---|
| **Modify Settings (Zmień ustawienia)** | Wybierz tę opcję, aby zmienić ustawienia serwera. |
| **Restore Default Settings (Przywróć ustawienia domyślne)** | Kliknij tę opcję, aby przywrócić wszystkie ustawienia domyślne. |
| **Start (Uruchom)** | Kliknij tę opcję, aby zmienić stan serwera. |
| **Zatrzymaj** | |
| **Rozpocznij ponownie** | Kliknij tę opcję, aby zrestartować serwer. |

## Zapisy ogólne

W aplikacji AXIS Camera Station 5 Service Control kliknij **Modify settings (Modyfikuj ustawienia)**, a następnie **General (Ogólne)**, aby zmienić ogólne ustawienia serwera.

| **Ustawienia serwera** | |
|---|---|
| **Nazwa serwera** | Nazwa serwera. Nazwa serwera jest wyświetlana w programie klienckim. Domyślnie nazwą serwera jest nazwa komputera. Nazwa ta nie ulegnie zmianie w przypadku zmiany nazwy komputera. |
| **Ports range (Zakres portów)** | Określ zakres portów. Pozostałe porty zmienią się automatycznie. |
| **Server HTTP port (Port HTTP serwera)** | Numer portu HTTP używany przez serwer do komunikacji z klientem. Domyślny port to 55752. |
| **Server TCP port (Port TCP serwera)** | Numer portu TCP używany przez serwer do komunikacji z klientem. Domyślny port to 55754. Numer portu jest obliczany przez dodanie 2 do numeru portu serwera. |
| **Mobile communication port (Port komunikacji mobilnej)** | Numer portu łączności komórkowej używany przez serwer do komunikacji z klientem. Domyślny port to 55756. Numer portu jest obliczany przez dodanie 4 do numeru portu serwera. |
| **Mobile streaming port (Mobilny port strumieniowania)** | Numer portu łączności komórkowej używany przez serwer do strumieniowego przesyłania wideo. Domyślny port to 55757. Numer portu jest obliczany przez dodanie 5 do numeru portu serwera. |
| **Component communication port (Port komunikacji elementu)** | Numer portu używany przez komponent do komunikowania się z urządzeniami sieciowymi za pośrednictwem serwera. Domyślny port to 55759. Numer portu jest obliczany przez dodanie 7 do numeru portu serwera. |
| **Porty używane przez komponenty aplikacji AXIS Camera Station 5** | Po ustaleniu zakresu portów na liście będą widoczne te porty, z których mogą korzystać komponenty. Domyślny zakres portów dla komponentów aplikacji AXIS Camera Station 5 to 55760–55764. |
| **Allow AXIS Camera Station 5 to add exceptions to the Windows Firewall (Zezwalaj aplikacji na dodawanie wyjątków do Zapory systemu Windows)** | Wybierz tę opcję, jeśli chcesz zezwolić aplikacji AXIS Camera Station 5 na automatyczne dodawanie wyjątków do Zapory systemu Windows, jeśli użytkownik zmieni zakres portów. |

Uwaga

- Jeżeli między serwerem a klientem istnieje brama NAT, zapora sieciowa lub podobne rozwiązanie, skonfiguruj przepuszczanie ruchu wykorzystującego te porty.
- Numery portów muszą być w zakresie 1024–65534.

| **Ustawienia proxy** | |
|---|---|
| **Direct connection (Połączenie bezpośrednie)** | Wybierz tę opcję, jeśli między serwerem AXIS Camera Station 5 a kamerami w systemie nie ma serwera proxy. |
| **System account Internet options / automatic (Opcje internetowe konta systemu / automatycznie)** | Domyślne ustawienia serwera proxy. Ta opcja powoduje używanie aktualnych ustawień serwera proxy określonych w aplecie Opcje internetowe dla konta systemowego. |
| **Use manual proxy settings (Użyj ręcznych ustawień proxy)** | Wybierz tę opcję, jeśli serwer proxy oddziela serwer AXIS Camera Station 5 i jakiekolwiek kamery w systemie. Wprowadź adres i numer portu serwera proxy. Zazwyczaj są to te same adres i numer portu, jak w oknie Opcje internetowe w Panelu sterowania systemu Windows.<br>• Można określić, aby nie były używane serwery proxy o adresach rozpoczynających się określonymi znakami.<br>• Zaznacz opcję **Always bypass proxy server for local addresses (Zawsze pomijaj serwer proxy dla adresów lokalnych)**, a następnie wprowadź lokalne adresy lub nazwy hostów lokalnych kamer, z którymi komunikacja nie musi przechodzić przez serwer proxy. W adresach i nazwach hostów można używać symboli wieloznacznych, na przykład: „192.*" lub „*.mydomain.com". |

## Lista portów dotycząca AXIS Camera Station 5

W poniższych tabelach opisano, z jakich portów i protokołów korzysta aplikacja AXIS Camera Station 5. Może być konieczne zezwolenie na nie w zaporze w celu uzyskania optymalnej wydajności i użyteczności. Numery portów są obliczane na podstawie domyślnego głównego portu HTTP 55752.

**AXIS Camera Station 5 (serwer programu) wysyła dane do urządzeń na następujących portach:**

| Port | Liczba | Protokół | Wejście/wyjście | Opis |
|---|---|---|---|---|
| Główne porty HTTP i HTTPS | 80 i 443 | TCP | Wychodzący | Używany do strumieni wideo i danych urządzeń. |
| Domyślny port protokołu Bonjour | 5353 | UDP | Multiemisja (ruch przychodzący + wychodzący) | Używany do wykrywania urządzeń przy użyciu mechanizmu mDNS (Bonjour). Multiemisja na adresie 224.0.0.251. |

| | | | | |
|---|---|---|---|---|
| | | | | Brak możliwości utworzenia powiązania z domyślnym portem może wynikać z faktu, że port jest używany przez inną aplikację, która odmawia jego współużytkowania. W takiej sytuacji będzie używany losowy port. Gdy używany jest losowy port protokół Bonjour nie wykrywa urządzeń z adresami lokalnego powiązania. |
| Domyślny port SSDP | 1900 | UDP | Multiemisja (ruch przychodzący + wychodzący) | Używany do wykrywania urządzeń przy użyciu protokołu SSDP (UPNP).<br><br>Multiemisja na adresie 239.255.255.250. |
| Domyślny port protokołu WS-Discovery | 3702 | UDP | Multiemisja (ruch przychodzący + wychodzący) | Wykrywanie usług internetowych przy użyciu protokołu WS-Discovery służące do wykrywania urządzeń Onvif.<br><br>Multiemisja na adresie 239.255.255.250. |

**AXIS Camera Station 5 (serwer programu) odbiera dane od klientów na następujących portach:**

| Port | Liczba | Protokół | Wejście/wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|
| Domyślny port SSDP | 1900 | UDP | Multiemisja (ruch przychodzący + wychodzący) | Serwera i klienta | Używany do wykrywania serwerów AXIS Camera Station 5 przy użyciu protokołu SSDP (UPNP).<br><br>Multiemisja na adresie |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | 239.255.255.2-50. |
| Główny port HTTP i port strumieniowania HTTP | 55752 | TCP | Przychodzący | Serwera i klienta | Używany do strumieniowego przesyłania wideo, dźwięku i metadanych (szyfrowanie AES). |
| Główny port TCP | 55754 | TCP | Przychodzący | Serwera i klienta | Przesunięcie +2 względem głównego portu HTTP.<br><br>Używany do danych aplikacji (szyfrowanie TLS 1.2).<br>W wersjach 5.15.007 i starszych jest używane szyfrowanie TLS 1.1. |
| Port serwera www SSDP | 55755 | TCP | Przychodzący | Serwera i klienta | Przesunięcie +3 względem głównego portu HTTP.<br><br>Służy do wykrywania serwerów AXIS Camera Station 5 przy użyciu protokołu SSDP/UPNP. |
| Port serwera www API | 55756 | TCP | Przychodzący | Serwer i aplikacja mobilna | Przesunięcie +4 względem głównego portu HTTP.<br><br>Używany do przesyłania danych aplikacji i strumienia wideo MP4 za pośrednictwem protokołu HTTPS. |
| Port multimediów API | 55757 | TCP | Przychodzący | Serwer i aplikacja mobilna | Przesunięcie +5 względem głównego portu HTTP.<br><br>Używany do przesyłania |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | strumienia wideo RTSP za pośrednictwem protokołu HTTP. |
| Lokalny port HTTP serwera proxy | 55758 | TCP | Przychodzący | Wewnętrzna komunikacja na serwerze | Przesunięcie +6 względem głównego portu HTTP.<br><br>Przesunięcie +2 względem portu serwera internetowego API.<br><br>Dostęp tylko wewnętrznie na komputerze serwera AXIS Camera Station 5.<br><br>Port obejściowy dla nieznanych problemów. Aplikacje mobilne wykonują wywołania do modułu SRA, który odbiera komunikację HTTPS, przekształca ją na HTTP, po czym wysyła z powrotem do lokalnego portu HTTP serwera proxy i portu multimediów API. |
| Port punktu końcowego internetowego serwera proxy | 55759 | TCP | Przychodzący | Serwer i składnik | Przesunięcie +7 względem głównego portu HTTP.<br><br>Używany do bezpiecznej komunikacji między składnikiem a urządzeniami. |

**Porty zarezerwowane dla składników**

| Element | Nasłuchuje na interfejsie | Port | Liczba | Protokół | Wejście/ wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|---|---|
| Bezpieczne wchodzenie | Localhost (127.0.0.1) | Port serwera www | 55766 | HTTPS | Przychodzący | Klient (karta Zarządzanie dostępem) i składnik | Przesunięcie +14 względem głównego portu HTTP.<br>Starsze instalacje korzystały z portu 8081. |
| Bezpieczne wchodzenie | Wszystkie (0.0.0.0/ INADDR_ ANY) | Port serwera www | 55767 | HTTPS | Przychodzący | Serwer główny i serwery podrzędne | Przesunięcie +15 względem głównego portu HTTP.<br>Używany do komunikacji między głównym serwerem a serwerami podrzędnymi w konfiguracji wieloserwerowej. |
| Monitorowanie stanu systemu | Wszystkie (0.0.0.0/ INADDR_ ANY) | Port serwera www | 55768 | HTTPS | Przychodzący | Klient (karta Monitorowanie stanu systemu) i składnik | Przesunięcie +16 względem głównego portu HTTP.<br>Używany do hostowania stron internetowych funkcji Monitorowanie stanu systemu oraz do udostępniania danych w konfiguracji wielosystemowej. |

| Element | Nasłuchuje na interfejsie | Port | Liczba | Protokół | Wejście/ wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|---|---|
| Usługa chmurowa Monitorowanie stanu systemu AXIS | host lokalny | Port serwera www | 55769 | HTTPS | Przychodzący | AXIS Camera Station 5 (strona internetowa) i backend CloudService (wtyczka) | Przesunięcie +17 względem głównego portu HTTP.<br>Opcja używana przez usługę chmurową Monitorowanie stanu systemu do uruchamiania monitorowania stanu systemu. |
| Inteligentne wyszukiwanie 2 | host lokalny | Port serwera www | 55770 | HTTPS | Przychodzący | Klient (karta Inteligentne wyszukiwanie) i składnik | Przesunięcie +18 względem głównego portu HTTP.<br>Używamy do hostowania interfejsu API funkcji Inteligentne wyszukiwanie oraz do obsługi strony internetowej klienta. |
| | | | 55771 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55772 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55773 | | | | Zarezerwowane do przyszłego |

| Element | Nasłuchuje na interfejsie | Port | Liczba | Protokół | Wejście/ wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|---|---|
| | | | | | | | wykorzystania. |
| | | | 55774 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55775 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55776 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55777 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55778 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55779 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55780 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55781 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55782 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55783 | | | | Zarezerwowane do |

| Element | Nasłuchuje na interfejsie | Port | Liczba | Protokół | Wejście/ wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|---|---|
| | | | | | | | przyszłego wykorzystania. |
| Local-IAM (IDP) | 0.0.0.0 | IDP_OIDC (Public) | 55784 | HTTPS | Przychodzący | Odwrotny proxy i Local-IAM | Przesunięcie +32 względem głównego portu HTTP.<br>Port publiczny. |
| Local-IAM (IDP) | 0.0.0.0 | MTLS (Administrator) | 55785 | HTTPS | Przychodzący | Usługi innych firm | Przesunięcie +33 względem głównego portu HTTP.<br>Port administratora. |
| Local-IAM (IDP) | 127.0.0.1 | TOKENIZER | 55786 | HTTPS | Przychodzący | Usługi innych firm | Przesunięcie +34 względem głównego portu HTTP.<br>Port tokenizera. |
| | | | 55787 | | | | Zarezerwowane do przyszłego wykorzystania. |
| Opentelemetry | 127.0.0.1 | Port gRPC | 55788 | gRPC | Przychodzący | Usługi innych firm | Przesunięcie +36 względem głównego portu HTTP. |
| Opentelemetry | 127.0.0.1 | Port HTTP | 55789 | HTTPS | Przychodzący | Usługi innych firm | Przesunięcie +37 względem głównego portu HTTP. |
| | | Port serwera www | 55790 | HTTPS | Przychodzący | Usługi integracji i komponenty innych firm | |
| | | | 55791 | | | | Zarezerwowane do przyszłego |

| Element | Nasłuchuje na interfejsie | Port | Liczba | Protokół | Wejście/ wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|---|---|
| | | | | | | | wykorzystania. |
| | | | 55792 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55793 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55794 | | | | Zarezerwowane do przyszłego wykorzystania. |
| | | | 55795 | | | | Zarezerwowane do przyszłego wykorzystania. |
| Broker NATS | 127.0.0.1 | NATS | 55796 | NATS | Przychodzący | Między aplikacją AXIS Camera Station 5 i składnikami oraz między samymi składnikami | Przesunięcie +44 względem głównego portu HTTP. |
| Opentelemetry | 127.0.0.1 | Port HTTP | 55797 | HTTP | Przychodzący | Monitorowanie punktu końcowego w celu pobrania metryk z otwartego modułu zbierającego dane telemetryczne | Przesunięcie +45 względem głównego portu HTTP. |

**Inne porty**

| Port | Liczba | Protokół | Wejście/wyjście | Komunikacja między | Opis |
|---|---|---|---|---|---|
| HTTPS dla Internetu | 80 i 443 | TCP | Wychodzący | Klient i serwer z Internetem | Używany do aktywowania licencji, pobierania oprogramowania sprzętowego, połączonych usług itd. |
| Port TCP strumieniowania z serwera | 55750 | TCP | Przychodzący | Serwer i urządzenie | Przesunięcie -2 względem głównego portu HTTP. |
| Port UDP stanu aktualizacji | 15156 | UDP | Przychodzący + wychodzący | Serwer i sterowanie usługami | AXIS Camera Station 5 Aplikacja Service Control nasłuchuje na porcie, a serwer rozgłasza status trwającego uaktualniania. |

## Baza danych

### Pliki baz danych

#### Podstawowe pliki baz danych

AXIS Camera Station 5 przechowuje podstawowe pliki bazy danych w folderze `C:\ProgramData\AXIS Communications\AXIS Camera Station Server`.

Wersje AXIS Camera Station starsze niż 5.13 mają tylko jeden plik bazy danych: **ACS.FDB**.

Wersja AXIS Camera Station 5.13 i nowsze mają trzy pliki baz danych:

- **ACS.FDB**: Ten główny plik bazy danych zawiera konfigurację systemu obejmującą urządzenia, widoki, uprawnienia, zdarzenia i profile strumieniowania.
- **ACS_LOGS.FDB**: Ten bazodanowy plik dzienników zawiera odwołania do dzienników.
- **ACS_RECORDINGS.FDB**: Ten plik bazy danych nagrań zawiera metadane i odwołania do nagrań przechowywanych w lokalizacji określonej w sekcji **Configuration (Konfiguracja) > Storage (Pamięć masowa)**. AXIS Camera Station 5 wymaga tego pliku do wyświetlania nagrań na osi czasu podczas odtwarzania.

#### Pliki baz danych składników

**SecureEntry.db –** Plik bazy danych programu AXIS Secure Entry zawiera wszystkie dane związane z kontrolą dostępu, z wyjątkiem zdjęć posiadaczy kart. Jest on zapisany w folderze `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry`.

**smartSearch.sqlite3 –** To plik bazy danych inteligentnego wyszukiwania zawierający konfigurację kamery i zapisane filtry wyszukiwania. Jest on zapisany w folderze `C:\ProgramData\Axis Communications\AXIS Smart Search\data`.

### Ustawienia bazy danych

Kopia bazy danych jest tworzona codziennie w porze nocnej oraz przed każdym uaktualnieniem systemu. W aplikacji AXIS Camera Station 5 Service Control kliknij **Modify settings (Modyfikuj ustawienia)**, a następnie **Database (Baza danych)**, aby zmienić ustawienia kopii zapasowej.

| | |
|---|---|
| **Backup folder (Folder kopii zapasowych)** | Kliknij przycisk **Browse (Przeglądaj)** i wybierz miejsce, w którym mają być zapisywane kopie zapasowe baz danych. Uruchom ponownie serwer AXIS Camera Station 5 w celu zastosowania wprowadzonej zmiany.<br><br>Jeżeli ścieżka folderu kopii zapasowej jest nieprawidłowa lub AXIS Camera Station 5 nie ma dostępu do zasobu sieciowego, kopia zapasowa zostanie zapisana w folderze `C:\ProgramData\Axis Communications\AXIS Camera Station Server\backup`. |
| **Days to keep backups (Liczba dni przechowywania kopii zapasowych)** | Określ liczbę dni, przez jaką mają być zachowywane kopie zapasowe. Może to być dowolna liczba z przedziału od 1 do 30. Domyślna wartość to 14 dni. |
| **Postęp uaktualnienia** | Kliknij przycisk **View details (Wyświetl szczegóły)**, aby zobaczyć szczegółowe informacje o ostatnim uaktualnianiu bazy danych. Możesz zobaczyć zdarzenia, które wystąpiły od ostatniego ponownego uruchomienia aplikacji AXIS Camera Station 5 Service Control. |

### Przygotuj kopię zapasową bazy danych

Baza danych zawiera informacje o nagraniach oraz inne metadane niezbędne do prawidłowego działania systemu.

Ważne

- Baza danych nie przechowuje nagrań. Przejdź do menu **Configuration > Storage (Konfiguracja > Zasób)** i określ lokalizację, w której nagrania mają być przechowywane. Kopie zapasowe nagrań muszą zostać wykonane osobno.
- Ustawienia serwera, ustawienia proxy i ustawienia bazy danych w aplikacji AXIS Camera Station 5 Service Control nie zostały zapisane.

#### Kopia zapasowa systemu

System automatycznie zapisuje kopię zapasową systemu w folderze określonym na karcie **Database (Baza danych)**, patrz *Ustawienia bazy danych, on page 197*. Kopia zapasowa systemu zawiera podstawowe pliki bazy danych oraz pliki baz danych składników. Zobacz *Pliki baz danych, on page 196*.

| Pliki kopii zapasowej | |
|---|---|
| `System_YYYY-MM-DD-HH-mm-SSSS.zip` | Kopia zapasowa uruchamiana co noc. |
| `PreUpgrade_YYYY-MM-DD-HH-mm-SSSS.zip` | Kopia zapasowa tworzona przed aktualizacją bazy danych. |
| `User_YYYY-MM-DD-HH-mm-SSSS.zip` | Kopia zapasowa generowana przed usunięciem zasobu. |

W pliku .zip znajdują się następujące pliki:

| | |
|---|---|
| **ACS** | Folder ten zawiera podstawowe pliki bazy danych `ACS.FDB`, `ACS_LOGS.FDB` oraz `ACS_RECORDINGS.FDB`. |
| **Składniki** | Ten folder jest dostępny tylko w przypadku używania składnika. Na przykład AXIS Camera Station Secure Entry lub Inteligentne wyszukiwanie.<br>• **ACMSM**: Folder ten zawiera plik bazy danych programu AXIS Camera Station Secure Entry `SecureEntry.db` oraz zdjęcia posiadaczy kart.<br>• **smartsearch**: Folder ten zawiera plik bazy danych inteligentnego wyszukiwania `smartSearch-backup-yyyyMMddHHmmssfff.sqlite3`. |
| `backup_summary.json` | Te pliki zawierają dokładniejsze informacje o kopii zapasowej. |
| | |

**Konserwacyjne kopie zapasowe**

Określ folder kopii zapasowych do przechowywania konserwacyjnych kopii zapasowych na karcie **Database (Baza danych)**, zob. *Ustawienia bazy danych, on page 197*. Konserwacyjna kopia zapasowa zawiera podstawowe pliki bazy danych, z których każdy znajduje się w osobnym folderze `PreMaintenance_YYYY-MM-DD-HH-mm-SSSS`.

Ta funkcja może być wywoływana na różne sposoby:

- Automatycznie po aktualizacji AXIS Camera Station 5.
- Po ręcznym uruchomieniu narzędzia do konserwacji bazy danych w aplikacji AXIS Camera Station 5 Service Control. Patrz *Konserwacja bazy danych, on page 199*.
- Automatycznie przez zaplanowane zadanie konserwacji bazy danych skonfigurowane w harmonogramie zadań systemu Windows. Patrz *Narzędzia, on page 200*.

**Ręczne tworzenie kopii zapasowej**

Uwaga

Ręcznie tworzona kopia zapasowa może zawierać kopie tylko podstawowych plików bazy danych. Nie obejmuje ona plików baz danych składników, na przykład pliku bazy danych funkcji Inteligentne wyszukiwanie.

Kopię zapasową można utworzyć manualnie, korzystając z dwóch sposobów:

- Przejdź do folderu `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` i wykonaj kopię plików bazy danych.
- Wygeneruj raport systemowy zawierający wszystkie bazy danych i skopiuj pliki kopii zapasowej bazy danych. Pamiętaj o zaznaczeniu opcji **Include all databases (Uwzględnij wszystkie bazy danych)**. Patrz *Raport systemowy, on page 181*.

## Przywracanie bazy danych

Jeżeli baza danych zostanie utracona wskutek awarii sprzętu lub innych problemów, można ją przywrócić z jednej z zapisanych kopii zapasowych. Domyślnie system przechowuje pliki kopii zapasowej przez 14 dni. Aby uzyskać więcej informacji o tworzeniu kopii zapasowych baz danych, patrz *Przygotuj kopię zapasową bazy danych, on page 197*.

Uwaga

Baza danych nie przechowuje nagrań. Przejdź do menu **Configuration > Storage (Konfiguracja > Zasób)** i określ lokalizację, w której nagrania mają być przechowywane. Kopie zapasowe nagrań muszą zostać wykonane osobno.

Aby przywrócić bazę danych:

1. Przejdź do aplikacji AXIS Camera Station 5 Service Control i kliknij przycisk **Stop (Zatrzymaj)**, aby zatrzymać usługę.
2. Przejdź do plików kopii zapasowych bazy danych. Patrz *Przygotuj kopię zapasową bazy danych, on page 197*.
3. Wyodrębnij pliki.
4. W wyodrębnionym folderze skopiuj następujące pliki bazy danych z **ACS** do `C:\ProgramData\AXIS Communications\AXIS Camera Station Server\`.
   - **ACS.FDB** - ten plik trzeba skopiować, aby w ogóle można było przywrócić bazę danych.
   - **ACS_LOGS.FDB** - skopiuj ten plik, jeżeli chcesz przywrócić dzienniki.
   - **ACS_RECORDINGS.FDB** - skopiuj ten plik, jeśli chcesz przywrócić nagrania.
5. Jeżeli używasz programu AXIS Camera Station Secure Entry, skopiuj plik **SecureEntry.db** z `Components > ACMSM` do `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db`.
6. Jeżeli używasz inteligentnego wyszukiwania, skopiuj plik **smartSearch-backup-yyyMMddHHmmssfff.sqlite3** z `smartsearch` do `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Smart Search\data` i zmień jego nazwę na **smartSearch.sqlite3**.
7. Wróć do aplikacji AXIS Camera Station 5 Service Control i kliknij przycisk **Start (Rozpocznij)**, aby uruchomić usługę.

### Konserwacja bazy danych

Przeprowadź konserwację bazy danych po wystąpieniu alarmu `Database maintenance is required` (Wymagana jest konserwacja bazy danych) lub po nieoczekiwanym wyłączeniu systemu, na przykład na skutek awarii zasilania.

Aby rozpocząć konserwację bazy danych, zobacz *Narzędzia, on page 200*.

Uwaga

AXIS Camera Station Secure Entry wykorzystuje narzędzie DB Janitor do monitorowania plików bazy danych i ich zmniejszania w razie potrzeby. W rzadkich przypadkach wymuszonego zmniejszania rozmiaru system kontroli dostępu staje się tymczasowo niedostępny.

### Najważniejsze praktyki dotyczące baz danych

Aby uniknąć problemów, pamiętaj o następujących kwestiach:

**Sprawdzaj dysk pod kątem błędów –** Błędy dysku mogą powodować uszkodzenie bazy danych. Używaj narzędzi takich jak chkdsk (Sprawdź dysk, znane również pod nazwą Sprawdzanie błędów) do wyszukania uszkodzonych sektorów na dysku twardym zawierającym bazę danych. Uruchamiaj narzędzie chkdsk regularnie.

**Oprogramowanie antywirusowe a zewnętrzne kopie zapasowe –** Nie włączaj skanowania anytywirusowego bazy danych, ponieważ niektóre programy antywirusowe uszkadzają bazy danych. Jeżeli używasz zewnętrznego systemu przechowywania kopii zapasowych, nie twórz kopii zapasowych bieżącej ani aktywnej bazy danych. Zamiast tego utwórz kopię zapasową z plików w folderze zawierającym kopie zapasowe.

**Awaria zasilania –** Nieoczekiwane wyłączenie komputera, na przykład spowodowane awarią zasilania, może uszkodzić bazę danych. W krytycznych instalacjach stosuj zasilacze awaryjne (UPS).

**Brak miejsca na dysku –** Baza danych może się uszkodzić wskutek braku miejsca na dysku twardym. Aby tego uniknąć, zainstaluj serwer AXIS Camera Station 5 na komputerze z wystarczającą ilością pamięci. Wymagania sprzętowe, p. strona *axis.com/products/axis-camera-station/hardware-guidelines*.

**Uszkodzona pamięć RAM –** Regularnie uruchamiaj narzędzie Diagnostyka pamięci systemu Windows, które szuka ewentualnych błędów w pamięci operacyjnej.

## Narzędzia

W aplikacji AXIS Camera Station 5 Service Control wybierz **Modify settings (Modyfikuj ustawienia)** i kliknij kartę **Tools (Narzędzia)**, aby rozpocząć konserwację bazy danych i utworzyć częściowe raporty systemowe.

**Narzędzie konserwacji bazy danych**

- Otwórz aplikację AXIS Camera Station 5 Service Control.
- Kliknij **Tools (Narzędzia)**.
- W obszarze **Database maintainer (Narzędzie konserwacji bazy danych)** kliknij **Run (Uruchom)**.
- Zostanie wyświetlony szacowany czas przestoju. Kliknij przycisk **Yes (Tak)**, aby kontynuować. Uruchomionego procesu nie można anulować. Serwer

Uwaga

- AXIS Camera Station 5 i wszystkie bieżące nagrania są zatrzymywane na czas konserwacji. Po zakończeniu konserwacji serwer uruchamia się automatycznie.
- Podczas konserwacji nie należy wyłączać komputera.
- Do przeprowadzenia konserwacji bazy danych trzeba mieć uprawnienia administratora na komputerze z systemem Windows.
- Jeżeli konserwacja nie jest w stanie przywrócić bazy danych, skontaktuj się z działem pomocy technicznej Axis.

Koniecznie przeprowadź konserwację bazy danych w reakcji na alarm „Wymagana jest konserwacja bazy danych" albo jeśli system nieoczekiwanie wyłączy się, na przykład po awarii zasilania.

Można również zaplanować automatyczne uruchamianie konserwacji bazy danych. W tym celu w systemie Windows w narzędziu Harmonogram zadań należy włączyć zadanie „ AXIS Camera Station 5 Database Maintenance" (Konserwacja bazy danych). Można edytować ustawienia wyzwalacza, aby ustawić kiedy i jak często ma być uruchamiana konserwacja bazy danych.

**Raport systemowy**

Częściowy raport systemowy jest plikiem .zip, który zawiera parametry i pliki dziennika, pomagające działowi pomocy technicznej Axis zbadać zgłoszony problem. Przy kontaktowaniu się z działem wsparcia technicznego zawsze dołączaj raport systemowy. Aby wygenerować pełny raport systemowy, wybierz kolejno  **> Help (Pomoc) > System report (Raport systemowy)** w kliencie AXIS Camera Station 5.

Aby utworzyć częściowy raport systemowy:

1. Kliknij przycisk **Run (Uruchom)**.
2. Wybierz i wprowadź wymagane informacje w oknie dialogowym.
3. Kliknij **Generate report (Generuj raport)**.

| Narzędzie raportu systemowego | |
|---|---|
| **Nazwa pliku** | Wprowadź nazwę pliku raportu systemowego. |
| **Folder** | Wybierz lokalizację zapisu raportu systemowego. |

| Narzędzie raportu systemowego | |
|---|---|
| **Automatically open folder when report is ready (Automatycznie otwórz folder, kiedy raport będzie gotowy)** | Ta opcja automatycznie otwiera folder, kiedy raport systemowy będzie gotowy. |
| **Include database file in report (Dołącz plik bazy danych do raportu)** | Wybierz w celu uwzględnienia bazy danych w raporcie systemowym. Baza danych AXIS Camera Station 5 zawiera informacje o nagraniach i dane niezbędne do prawidłowego działania systemu. |

**Rejestracja ruchu sieciowego**

- Kliknij łącze, aby pobrać aplikację analizatora protokołów sieciowych.
- Po jej zainstalowaniu kliknij **Start**, aby uruchomić aplikację.

**Reset certificate authority (Zresetuj urząd certyfikacji)**

- Kliknij **Reset** (Resetuj), aby utworzyć nowy urząd certyfikacji i ponownie uruchomić usługę.
- Po ponownym uruchomieniu usługi będziesz mógł zalogować się i w razie potrzeby zaimportować własny urząd certyfikacji.

# Rozwiązywanie problemów –

## Informacje dotyczące tego przewodnika

Niniejszy przewodnik to zbiór problemów związanych z AXIS Camera Station 5 i sposobów ich rozwiązywania. Umieściliśmy informacje o problemach w powiązanych z nimi tematach, aby ułatwić znalezienie tego, czego szukasz; tematem może być na przykład dźwięk lub podgląd na żywo. Obok każdego problemu znajdziesz opis jego rozwiązania.

### Więcej informacji

Odwiedź *axis.com/support*, aby uzyskać odpowiedzi na

- Często zadawane pytania
- Wymagania sprzętowe
- Aktualizacje oprogramowania
- Samouczki, materiały szkoleniowe i inne użyteczne informacje

## Usługa AXIS Camera Station 5

### Usługa często uruchamia się ponownie

Serwer może być przeciążony, co wydłuża kolejkę zadań i zagraża integralności bazy danych.

- W sekcji zarządzania zasobami systemu należy sprawdzić, czy AXIS Camera Station 5 lub jakakolwiek inna aplikacja korzysta z dużej liczby zasobów.
- Uruchom narzędzie do konserwacji bazy danych — zob. *Konserwacja bazy danych* w instrukcji obsługi aplikacji AXIS Camera Station 5.

Jeśli żadne z powyższych, skontaktuj się z pomocą techniczną Axis. Przejdź do *Proces eskalacji, on page 217*.

## Urządzenia w systemie VMS

### Typowe problemy

| Nie można nawiązać kontaktu z kamerą | |
|---|---|
| System VMS nie może nawiązać połączenia z kamerą. Kamery widoczne na liście nie zostały dodane. | 1. Upewnij się, że kamera ma połączenie sieciowe, jest zasilanie i że działa.<br>2. Wybierz kolejno opcje **Configuration > Add devices (Konfiguracja > Dodaj urządzenia)** i spróbuj ponownie dodać kamerę. |

| Instalacja została anulowana | |
|---|---|
| Operacja instalacji została anulowana przez użytkownika. Kamery widoczne na liście nie zostały dodane. | Aby dodać kamery, wybierz kolejno opcje **Configuration > Add devices (Konfiguracja > Dodaj urządzenia)**. |

| Niepowodzenie ustawiania hasła na kamerze | |
|---|---|
| Nie można ustawić hasła dostępu do kamer widocznych na liście. | 1. Aby ręcznie ustawić hasło, przejdź do **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.<br>2. Kliknij kamerę prawym przyciskiem myszy i wybierz **User Management > Set password (Zarządzanie użytkownikami > Ustaw hasło)**. |

### Nie można dodać urządzenia

**Jeśli urządzenie było używane w innym systemie, zanim zostało dodane do AXIS Camera Station 5:**

- Zastosuj ustawienia fabryczne urządzenia.

Jeśli urządzenia nadal nie można dodać do systemu VMS, spróbuj dodać je do aplikacji AXIS Device Manager.

**Możliwe jest dodanie innego modelu urządzenia niż wybrany:**

- Jeśli urządzenie jest nowym produktem lub ma nowo wydane oprogramowanie sprzętowe, może występować problem ze zgodnością. Upewnij się, że korzystasz z najnowszej wersji oprogramowania AXIS Camera Station 5.

**Jeśli nie można dodać innego modelu urządzenia:**

- Rozwiąż problemy z kamerą, zobacz na stronie *axis.com/support/troubleshooting*.

### Nie można zaktualizować oprogramowania sprzętowego urządzenia za pomocą AXIS Camera Station 5

**Aktualizacja kamery z poziomu interfejsu WWW nie jest możliwa:**

- Rozwiąż problemy z kamerą, zobacz na stronie *axis.com/support/troubleshooting*.

**Nie można zaktualizować oprogramowania sprzętowego dla wszystkich urządzeń:**

- Upewnij się, że połączenie sieciowe jest aktywne.
- Jeśli nie chodzi o problem z siecią, skontaktuj się z pomocą techniczną Axis. Przejdź do *Proces eskalacji, on page 217*.

**Nie można zaktualizować oprogramowania sprzętowego konkretnych modeli:**

- Być może występuje problem ze zgodnością, skontaktuj się z działem pomocy technicznej Axis. Przejdź do *Proces eskalacji, on page 217*.

### Nie znaleziono urządzeń

System zarządzania materiałem wideo automatycznie wyszukuje w sieci podłączone kamery i enkodery wideo, ale nie może znaleźć żadnych kamer.

- Upewnij się, że kamera jest połączona z siecią i ma zasilanie.
- Jeżeli klient, serwer lub kamery znajdują się w różnych sieciach, skonfiguruj ustawienia serwera proxy i zapory.
  - Jeśli klient i serwer są oddzielone serwerem proxy, zmień ustawienia proxy klienta. Zob. sekcję *Ustawienia proxy klienta* w instrukcji obsługi aplikacji AXIS Camera Station 5.
  - Zmień NAT lub system zabezpieczeń, jeśli NAT lub system zabezpieczeń oddziela klienta od serwera. Upewnij się, że port HTTP, port TCP (Transmission Control Protocol) i port strumieniowania określone w funkcjach sterowania programu AXIS Camera Station mogą przechodzić przez system zabezpieczeń lub przez NAT. Pełna lista portów, p. sekcja *Lista portów z przeznaczeniem dla programu AXIS Camera Station 5*.

- Jeśli serwer i urządzenia są oddzielone serwerem proxy, zmień ustawienia proxy serwera. Zapoznaj się sekcją Ustawienia proxy w rozdziale *Informacje ogólne na temat sterowania usługami* w instrukcji obsługi aplikacji AXIS Camera Station 5.

- Dodaj kamery manualnie — zob. sekcję *Dodawanie urządzeń* w instrukcji obsługi aplikacji AXIS Camera Station 5.

### Powtarzający się komunikat „Ponowne połączenie z kamerą za 15 s"

**Możliwe problemy:**

- Przeciążenie sieci.
- Kamera jest niedostępna. Upewnij się, że kamera jest połączona z siecią i ma zasilanie.
- Występują problemy z kartą graficzną.

**Możliwe rozwiązania problemów z kartą graficzną:**

- Zainstaluj najnowszy sterownik karty graficznej.
- Zmień kartę graficzną na lepszą, która ma więcej pamięci wideo i wyższą wydajność.
- Użyj głównego procesora komputera do renderowania wideo.
- Zmień ustawienia wideo i dźwięku, na przykład optymalizując ustawienia profilu dla niskiej przepustowości.

## Nagrania

Więcej informacji o możliwych problemach z wydajnością podczas nagrywania i odtwarzania obrazu, zob. *Podgląd na żywo, on page 206*.

### Typowe problemy

| Nagrywanie ciągłe nie zostało włączone | |
|---|---|
| W kamerach widniejących na liście nie zostało włączone nagrywanie ciągłe. | 1. Aby wyłączyć nagrywanie ciągłe, przejdź do menu **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.<br>2. Wybierz kamerę i włącz ustawienie **Continuous (Ciągły)**. |

| Nie można nagrywać na określonym napędzie | |
|---|---|
| System nie może skonfigurować pamięci masowej nagrań. | 1. Aby użyć innej pamięci masowej, wybierz kolejno opcje **Configuration > Storage > management (Konfiguracja > Pamięć masowa > Zarządzanie)**.<br>2. Dodaj zasób pamięci i skonfiguruj jego ustawienia dla kamer. |

| Niepowodzenie instalacji aplikacji AXIS Video Content Stream | |
|---|---|
| Ten komunikat o błędzie jest wyświetlany w razie niemożności zainstalowania aplikacji AXIS Video Content Stream w kamerze, która ją obsługuje. | 1. Aby zainstalować aplikację ręcznie, wybierz kolejno opcje **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.<br>2. Zaznacz kamerę i kliknij  . |

### Nagrywanie nie rozpoczyna się

Jeśli nagrywanie nie zacznie się lub nie zatrzyma po kilku sekundach, oznacza to, że dysk jest zapełniony lub że jest na nim zbyt dużo danych.

- Na arkuszu konfiguracji serwera w obszarze **Recording Storage (Pamięć masowa nagrań)** sprawdź, czy jest wolne miejsce i czy nie ma na nim kolidujących danych.
- Zwiększ limit zasobu dla VMS.
- Przypisz więcej miejsca do puli zasobu. Zob. sekcję *Konfiguracja pamięci masowej* w instrukcji obsługi aplikacji AXIS Camera Station 5.

### Przerwy w nagrywaniu podczas ciągłego nagrywania

Wraz z przerwami alarmy z etykietą **Recording errors (Błędy nagrywania)**. Przerwy w nagrywaniu mogą wynikać z różnych przyczyn, takich jak:

- Przeciążenie serwera
- Problem z siecią
- Przeciążenie kamery
- Przeciążenie dysku

Sprawdź, czy przerwy w nagrywaniu występują we wszystkich kamerach. Jeśli nie występuje we wszystkich kamerach, może to oznaczać przeciążenie konkretnej kamery. Aby znaleźć przyczynę, odpowiedz na następujące pytania:

- Jak często występują przerwy? (co godzinę czy codziennie?)
- Jak długa jest przerwa? (Trwa sekundy, czy godziny?)
- O której godzinie pojawia się przerwa?

**Możliwe rozwiązania:**

- W menedżerze zadań serwera sprawdź, czy system wykorzystuje jeden z zasobów sprzętowych w sposób bardziej intensywny niż zwykle. Jeśli dysk wykazuje oznaki nadmiernego przeciążenia, dodaj więcej dysków i ustaw w kilku kamerach zapisywanie nagrań na nowych dyskach.
- Ogranicz ilość danych zapisywanych na dysku (ustawienia wideo, strumień ZIP, FPS, rozdzielczość). Weź pod uwagę przepustowość szacowaną przez AXIS Site Designer, zob. *axis.com/support/tools/axis-site-designer*.

Więcej informacji znajduje się w rozdziale *Jakość widoku na żywo i odtwarzania, on page 206*.

### Nie można odtwarzać eksportowanych zapisów

Jeżeli program Windows Media Player nie odtwarza eksportowanych zapisów, sprawdź format pliku. Do odtwarzania nagrań wyeksportowanych najlepiej jest używać programu Windows Media Player (.asf) lub AXIS File Player (.asf, .mp4, .mkv).

Aby uzyskać więcej informacji, zobacz *Odtwarzanie i weryfikowanie wyeksportowanych nagrań* w instrukcji obsługi aplikacji AXIS Camera Station 5.

Uwaga

AXIS File Player automatycznie otwiera wszystkie nagrania znajdujące się w tym samym folderze co odtwarzacz.

### Znikające nagrania

Nagrania są zachowywane tylko przez określoną liczbę dni. Aby zmienić tę liczbę dni, wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)**.

Jeżeli pamięć zostanie zapełniona, nagrania będą usuwane przed upływem ustawionej liczby dni.

Aby uniknąć zapełnienia zasobu pamięci, spróbuj następujące rozwiązania:

- Dodaj więcej pamięci masowej. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
- Zmień ilości miejsca w pamięci masowej przydzielonej dla AXIS Camera Station 5. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
- Zmniejsz rozmiar nagrywanych plików, zmieniając na przykład rozdzielczość lub poklatkowość. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumieni)**.
  - Użyj formatu wideo w formacie H. 264, aby nagranie, format M-JPEG wymaga znacznie więcej miejsca na pamięć.
  - Aby dodatkowo zmniejszyć rozmiary nagrań, należy użyć Zipstream firmy.

### Problemy z zapisem awaryjnym

Zapis awaryjny nie jest nagrywany na serwerze po przywróceniu połączenia.

| Przyczyna | Rozwiązanie |
|---|---|
| Przepustowość sieci łączącej kamerę z serwerem jest niewystarczająca do przesłania nagrania. | Zwiększ przepustowość sieci |
| W okresie braku połączenia kamera nie zapisywała nagrań na karcie SD. | • Zobacz raport serwera kamery. Zobacz na stronie *axis.com/support/troubleshooting*.<br>• Upewnij się, że karta SD działa prawidłowo i są na niej nagrania. |
| Czas kamery zmienił się lub przesunął od momentu zerwania połączenia. | • Pamiętaj o konieczności zsynchronizowania NTP na potrzeby przyszłych nagrań.<br>• Zsynchronizuj czas kamery z serwerem lub skonfiguruj ten sam serwer NTP w kamerze, co na serwerze. |

Zapis awaryjny w AXIS Camera Station 5 nie działa w następujących scenariuszach:

- Kontrolowane wyłączenia serwerów.
- Krótkie przerwy w połączeniu trwające mniej niż 10 sekund.

## Podgląd na żywo

### Jakość widoku na żywo i odtwarzania

W tej sekcji opisano możliwe rozwiązania w przypadku utraty klatek lub problemów graficznych w kliencie AXIS Camera Station 5.

| Urządzenie klienckie | |
|---|---|
| Sprawdź, czy sterowniki karty graficznej lub karty sieciowej są aktualne. | 1. Otwórz narzędzie diagnostyczne DirectX (wyszukaj dxdiag na komputerze).<br>2. Sprawdź w witrynie producenta urządzenia, czy masz najnowszy sterownik dla używanego systemu operacyjnego.<br>3. Sprawdź, czy aplikacje kliencka i serwera działają na tym samym komputerze.<br>4. Spróbuj uruchomić klienta na dedykowanym komputerze. |
| Sprawdź liczbę monitorów | W przypadku korzystania z wewnętrznej karty graficznej nie zalecamy używania więcej niż dwóch monitorów na kartę graficzną.<br>1. Otwórz narzędzie diagnostyczne DirectX (wyszukaj dxdiag na komputerze)<br>2. Sprawdź, czy AXIS Camera Station 5 obsługuje dedykowaną kartę graficzną – p. strona *axis.com/products/axis-camera-station/hardware-guidelines*.<br>Uwaga<br>Nie można uruchomić klienta na maszynie wirtualnej. |

| Podłączone urządzenia | |
|---|---|
| Wiele klientów połączonych w tym samym czasie | Zależnie od typowego zastosowania sprawdź, czy system spełnia jego wymagania i postępuj zgodnie ze wskazówkami dotyczącymi sprzętu. P. strona *axis.com/products/axis-camera-station/hardware-guidelines*. |
| Kamera jest podłączona do innego systemu zarządzania materiałem wizyjnym niż AXIS Camera Station 5 | Odłącz kamerę od innego klienta i ustaw ją jako domyślną, zanim ją połączysz z AXIS Camera Station 5. |
| Jedna kamera wykorzystuje wiele różnych strumieni, zwłaszcza wysokiej rozdzielczości: | Może to być problem, zwłaszcza w przypadku niektórych kamer z linii M.<br>• Zmień strumień na ten sam profil strumieniowania lub ustaw niższą rozdzielczość. Zob. *Profile strumieni* w instrukcji obsługi aplikacji AXIS Camera Station 5. |

| Przeciążenie serwera | |
|---|---|
| Nietypowe użycie procesora/ pamięci RAM równolegle z występowaniem problemu | Upewnij się, że w tym samym czasie nie jest uruchomiona żadna inna aplikacja korzystająca z procesora/pamięci RAM. |

| Problem z siecią | |
|---|---|
| Nietypowe wykorzystanie przepustowości równolegle z występowaniem problemu | Upewnij się, że w tym samym czasie nie jest uruchomiona żadna inna aplikacja korzystająca z przepustowości |
| Wystarczająca przepustowość/ zdalna lub lokalna sieć | • Zapoznaj się z topologią sieci.<br>• Sprawdź stan dowolnego urządzenia sieciowego, np. przełącznika, routera, karty sieciowej i kabla, używanych między kamerami, serwerem i klientem. |

### Brak wideo w podglądzie na żywo

W podglądzie na żywo nie ma obrazu ze znanej kamery.

- Należy wyłączyć dekodowanie sprzętowe. Dekodowanie sprzętowe włącza się domyślnie — zob. sekcję Dekodowanie sprzętowe w rozdziale *Strumieniowanie* w instrukcji obsługi aplikacji AXIS Camera Station 5.

**Inne możliwe rozwiązania:**

- Jeśli nie widzisz podglądu na żywo w interfejsie WWW lub jeśli interfejs WWW nie działa, spróbuj procedury rozwiązywania problemów z kamerą. Przejdź do *axis.com/support/troubleshooting*.
- Utwórz raport o serwerze kamer, przejdź do *axis.com/support/troubleshooting* .
- Jeśli masz zainstalowany program antywirusowy, może on blokować transmisje na żywo.
- Zezwól na foldery i procesy AXIS Camera Station 5 — zob. *Często zadawane pytania*.
- Upewnij się, że zapora nie blokuje połączeń na niektórych portach — zob. *Informacje ogólne na temat sterowania usługami* w instrukcji obsługi aplikacji AXIS Camera Station 5.
- Upewnij się, że zostało zainstalowane środowisko pulpitu dla obsługiwanych wersji systemu Windows Server. Zob. *Zaplanowany eksport* w instrukcji obsługi aplikacji AXIS Camera Station 5.
- Upewnij się, że strumień o niższej rozdzielczości działa.

Jeśli żadne z opisanych powyższej rozwiązań nie pomoże, zgłoś się do działu pomocy technicznej Axis, przejdź do *Proces eskalacji, on page 217*.

## Przechowywanie

### Pamięć sieciowa jest nieosiągalna

W przypadku używania lokalnego konta systemowego do logowania się w aplikacji AXIS Camera Station 5 Service Control nie można dodać sieciowej pamięci masowej, która ma powiązania z folderami udostępnionymi na innych komputerach.

Aby zmienić konto logowania do usługi:

1. Otwórz **Windows Control Panel (Panel sterowania w systemie Windows)**.
2. Wyszukaj „Services".
3. Kliknij **View local services (Wyświetl usługi lokalne)**.
4. Kliknij prawym przyciskiem myszy AXIS Camera Station 5 i wybierz opcję **Properties (Właściwości)**.
5. Przejdź do karty **Log on (Logowanie)**.
6. Zamiast opcji **Local System account (Lokalne konto systemowe)** zaznacz opcję **This account (To konto)**.
7. Zaznacz użytkownika z dostępem do usługi Windows Active Directory.

### Sieciowy zasób pamięci jest niedostępny

Upewnij się, że komputer i serwer, na których działa oprogramowanie do zarządzania materiałem wizyjnym, należą do tej samej domeny, co sieciowy zasób pamięci.

### Nie można nawiązać połączenia z sieciową pamięcią masową przy użyciu nowej nazwy użytkownika i hasła

Jeżeli sieciowa pamięć masowa wymaga uwierzytelniania, to przed zmianą nazwy użytkownika i hasła trzeba koniecznie rozłączyć jej wszystkie istniejące połączenia.

Aby zmienić nazwę użytkownika i hasło dostępu do pamięci masowej, a następnie ponownie nawiązać z nią połączenie:

1. Rozłącz wszystkie istniejące połączenia sieciowej pamięci masowej.
2. Zmień nazwę użytkownika i hasło.
3. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)** i ustanów połączenie z sieciową pamięcią masową za pomocą nowej nazwy użytkownika i hasła.

## Detekcja ruchu

### Typowe problemy

| Instalacja aplikacji AXIS Video Motion Detection nie powiodła się | |
|---|---|
| Nie można zainstalować aplikacji AXIS Video Motion Detection 2 lub 4. Do nagrywania wyzwalanego ruchem będzie używana wbudowana funkcja detekcji ruchu. | Więcej informacji o manualnym instalowaniu aplikacji, zob. *Instalowanie aplikacji kamery* w instrukcji obsługi aplikacji AXIS Camera Station 5. |

| Pobierania bieżącej wersji aplikacji Motion Detection nie powiodło się | |
|---|---|
| System zarządzania materiałem wizyjnym nie może pobrać parametrów detekcji ruchu z kamery. Do nagrywania wyzwalanego ruchem będzie używana wbudowana funkcja detekcji ruchu. | Więcej informacji o manualnym instalowaniu aplikacji, zob. *Instalowanie aplikacji kamery* w instrukcji obsługi aplikacji AXIS Camera Station 5. |

| Detekcja ruchu nie jest skonfigurowana | |
|---|---|
| Nie można skonfigurować detekcji ruchu w kamerach wymienionych na liście. | 1. Aby ręcznie skonfigurować funkcjonalność wykrywania ruchu, wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.<br>2. Zaznacz kamerę i kliknij **Motion settings (Ustawienia ruchu)**, aby skonfigurować detekcję ruchu. |

| Detekcja ruchu nie jest włączona | |
|---|---|
| W kamerach wymienionych na liście nie włączono nagrywania ruchu. | 1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.<br>2. Zaznacz kamerę i włącz opcję **Motion detection (Detekcja ruchu)**, aby włączyć nagrywanie wykrytego ruchu. |

### Funkcja detekcji ruchu wykrywa za dużo lub za mało poruszających się obiektów

W tej części opisano możliwe rozwiązania w przypadku większej lub mniejszej liczby detekcji w nagraniach związanych z funkcją Video Motion Detection.

#### Wyreguluj ustawienia wykrywania ruchu

Można wybrać ustawienia ruchu, aby ustawić obszar detekcji poruszających się obiektów.

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Zaznacz kamerę i wybierz polecenie **Motion Settings (Ustawienia ruchu)**.
3. Wybierz ustawienia zgodnie z oprogramowaniem sprzętowym kamery.

| | |
|---|---|
| **Aplikacje AXIS Video Motion Detection 2 i 4** | Można skonfigurować obszar zainteresowania. Zob. *Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4* w instrukcji obsługi aplikacji AXIS Camera Station 5. |
| **Wbudowana funkcja detekcji ruchu** | Można skonfigurować okna uwzględniane i pomijane. Zob. *Edytowanie wbudowanej funkcji detekcji ruchu* w instrukcji obsługi aplikacji AXIS Camera Station 5. |

#### Wyreguluj okres wyzwalacza

Czas wyzwalania jest przerwą pomiędzy kolejnymi wyzwalaczami. Użyj tego ustawienia, aby zmniejszyć liczbę następujących po sobie zapisów. Nagrywanie jest kontynuowane, jeżeli w tym interwale wystąpi jakikolwiek dodatkowy wyzwalacz. Okres wyzwalacza będzie wtedy liczony od tego momentu.

Aby zmienić okres wyzwalacza:

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Zaznacz kamerę.
3. W obszarze **Advanced (Zaawansowane)** ustaw **Trigger period (Czas wyzwalania)** w sekundach.

## Dźwięk

### Brak dźwięku w podglądzie na żywo

Jeżeli w podglądzie na żywo nie ma dźwięku, wykonaj następujące czynności:

- Upewnij się, że kamera ma funkcje obsługi dźwięku.
- Upewnij się, że w komputerze jest zainstalowana karta dźwiękowa i czy jest ona używana.
- Upewnij się, że używany profil został skonfigurowany do obsługi dźwięku.
- Upewnij się, że użytkownik ma prawa dostępu do dźwięku.

#### Konfigurowanie obsługi dźwięku w profilach

1. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumieni)**.
2. Zaznacz kamerę.
3. W ustawieniach profilu wideo w polu **Format** zaznacz wartość **MPEG-4** lub **H.264**.
4. W obszarze **Audio (Dźwięk)** wybierz mikrofon z rozwijalnego menu **Microphone (Mikrofon)**.
5. Z rozwijalnego menu **Use microphone for (Użyj mikrofonu przy)** wybierz, kiedy ma być używany dźwięk.
6. W razie potrzeby wybierz głośnik menu rozwijanego **Speaker (Głośnik)**.
7. Kliknij **OK**.

#### Sprawdzanie i zmienianie uprawnień dostępu użytkownika

Uwaga

Aby wykonać te kroki, musisz mieć uprawnienia administratora do aplikacji AXIS Camera Station 5.

1. Przejdź do obszaru **Configuration (Konfiguracja) > Security (Zabezpieczenia) > User permissions (Uprawnienia użytkownika)**.
2. Wybierz użytkownika lub grupę.
3. Wybierz **Audio listen (słuchanie audio)** lub **Audio speak (mówienie audio)**dla konkretnego urządzenia.
4. Kliknij przycisk **Apply (Zastosuj)**.

### Brak dźwięku w sekwencjach

W profilach strumienia można włączać i wyłączać dźwięk. Aby uzyskać więcej informacji, zob. *Profile strumieni* w instrukcji obsługi aplikacji AXIS Camera Station 5.

### Brak dźwięku podczas odtwarzania

Dźwięk jest dostępny podczas odtwarzania, jeżeli obsługa dźwięku była włączona w profilu używanym podczas nagrywania.

Uwaga

Dźwięk nie działa w materiałach wideo o kodowaniu M-JPEG. Wybierz inny format wideo.

Aby użyć dźwięku w nagraniach:

1. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumieni)**, aby ustawić format wideo dla używanego profilu wideo.
2. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
3. Zaznacz kamerę.
4. Wybierz skonfigurowany profil z menu rozwijanego **Profile (Profil)**.
5. Kliknij przycisk **Apply (Zastosuj)**.

#### Nagrania wyzwalane regułami

Aby włączyć dźwięk w istniejącej regule:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Zaznacz regułę i kliknij przycisk **Edit (Edytuj)**.
3. Kliknij **Next (Dalej)**, aby przejść do **Actions (Akcje)**.
4. Wybierz akcję **Record (Nagrywanie)** i kliknij **Edit (Edycja)**.
5. Wybierz profil, w którym jest używana ścieżka dźwiękowa.
6. Kliknij przycisk **Finish (Zakończ)**, aby zapisać.

## Logowanie

### Nie można zalogować do serwera albo nawiązać z nim połączenia

W tej części omówiono problemy z logowaniem i nawiązywaniem łączności, które występują w trakcie ustanawiania połączenia z jednym serwerem. Podczas logowania do wielu serwerów klient zostanie uruchomiony, a stan połączenia będzie wyświetlany na pasku stanu. Aby uzyskać więcej informacji o statusie połączenia, zob. *Status połączenia* w instrukcji obsługi aplikacji AXIS Camera Station 5.

| | | |
|---|---|---|
| Nazwa użytkownika lub hasło są niepoprawne | Kombinacja nazwy użytkownika i hasła jest nieprawidłowa do logowania na wskazanym serwerze. | • Sprawdź pisownię lub użyj innego konta.<br>• Upewnij się, że użytkownik ma prawa dostępu do serwera AXIS Camera Station 5.<br>• Zegary serwera i klienta AXIS Camera Station 5 muszą być zsynchronizowane. W przypadku użytkowników domenowych zegar serwera domeny musi być zsynchronizowany z serwerem i klientem.<br>• Użytkownik, który nie został dodany do serwera, a należy do lokalnej grupy administratorów na serwerze, musi uruchomić klienta jako administrator.<br>• Aby uzyskać informacje o prawach dostępu użytkowników, zob. *Konfigurowanie uprawnień użytkowników* w instrukcji obsługi aplikacji AXIS Camera Station 5. |
| Użytkownik nie ma uprawnień do zalogowania się na serwerze | Użytkownik nie może korzystać z aplikacji AXIS Camera Station 5 na danym serwerze. | Dodaj użytkownika w oknie dialogowym Uprawnienia użytkownika. |
| Nie można zweryfikować zabezpieczeń wiadomości | Podczas konfigurowania bezpiecznego połączenia z serwerem wystąpił błąd, najprawdopodobniej spowodowany brakiem synchronizacji czasu komputera klienckiego lub serwera. | Czasy UTC serwera i klienta muszą być odpowiednio zsynchronizowane. Wyreguluj czas na kliencie i serwerze w taki sposób, aby różnica między nimi nie przekraczała 3 godzin. |
| Brak kontaktu z serwerem | Klient nie jest w stanie ustanowić połączenia z serwerem. | • Upewnij się, czy serwer może połączyć się z siecią.<br>• Upewnij się, że komputer serwera jest uruchomiony.<br>• Upewnij się, że zapora była poprawnie skonfigurowana.<br>• Sprawdź pisownię adresu serwera.<br>• Sprawdź ustawienia proxy klienta. |
| Brak odpowiedzi z serwera | Klient może się połączyć z serwerem, ale żaden serwer AXIS Camera Station 5 nie jest uruchomiony. | Upewnij się, że łączysz się z właściwym komputerem i że serwer AXIS Camera Station 5 jest uruchomiony. |
| Klient nie może połączyć się z serwerem | Klient nie może połączyć się z serwerem i zostanie wyświetlony komunikat o błędzie. | Upewnij się, że sieć jest poprawnie skonfigurowana:<br>• Sprawdź, czy system operacyjny jest obsługiwany. Aby uzyskać pełną listę obsługiwanych systemów operacyjnych, przejdź do *informacji o wersji*<br>• Z poziomu aplikacji Service Control sprawdź, czy serwer AXIS Camera Station 5 jest uruchomiony lub go uruchom w razie potrzeby. |

| | | |
|---|---|---|
| | | • Sprawdź, czy klient i serwer są połączone z tą samą siecią.<br>– Jeżeli nie, klient powinien używać zewnętrznego adresu IP serwera.<br>• Sprawdź, czy między serwerem a klientem jest serwer proxy.<br>– Skonfiguruj serwer proxy w ustawieniach sterowania usługami.<br>– Skonfiguruj ustawienie serwera proxy klienta na stronie logowania, wybierz opcję **Change proxy settings (Zmień ustawienia serwera proxy)**.<br>– Skonfiguruj ustawienia serwera proxy klienta w oknie Opcje internetowe systemu Windows i wybierz opcję domyślną w oknie **Change Proxy settings (Zmień ustawienia serwera proxy)**. |
| Nie można połączyć się z serwerem | Wystąpił nieznany błąd w trakcie nawiązywania połączenia z serwerem. | • Upewnij się, że adres i port serwera AXIS Camera Station 5 są prawidłowe.<br>• Upewnij się, że żadna brama NAT, zapora sieciowa ani oprogramowanie antywirusowe nie blokują połączenia z serwerem. Więcej informacji: *Konfigurowanie zapory sieciowej w celu umożliwienia dostępu do aplikacji AXIS Secure Remote Access*.<br>• Skorzystaj z aplikacji AXIS Camera Station 5 Service Control, aby sprawdzić, czy serwer jest uruchomiony.<br>– Otwórz aplikację AXIS Camera Station 5 Service Control — zob. *AXIS Camera Station Service Control* w instrukcji obsługi aplikacji AXIS Camera Station 5.<br>– Wyświetl stan serwera na karcie **General (Ogólne)**. Jeśli serwer ma stan **Stopped (Zatrzymany)**, kliknij **Start** , aby uruchomić serwer. |
| Nie można znaleźć serwera | Klient nie może zinterpretować wprowadzonego adresu jako adresu IP. | • Upewnij się, czy serwer może połączyć się z siecią.<br>• Upewnij się, że adres i port serwera AXIS Camera Station 5 są prawidłowe.<br>• Upewnij się, że żadna brama NAT, zapora sieciowa ani oprogramowanie antywirusowe nie blokują połączenia z serwerem. Więcej informacji: *Konfigurowanie zapory sieciowej w celu umożliwienia dostępu do aplikacji AXIS Secure Remote Access*. |

| | | |
|---|---|---|
| Wersje serwera i klienta są różne | Klient ma nowszą wersję AXIS Camera Station 5 niż serwer. | Uaktualnij serwer, aby używał tej samej wersji, co klient. |
| | Serwer ma nowszą wersję AXIS Camera Station 5 niż klient. | Uaktualnij klienta, aby używał tej samej wersji, co serwer. |
| Nie można połączyć się z serwerem. Serwer jest zbyt zajęty. | Serwer nie może odpowiedzieć z powodu problemów z wydajnością. | Upewnij się, że komputer serwera i sieć nie są przeciążone. |
| Lokalny serwer AXIS Camera Station 5 nie jest uruchomiony | Używasz opcji **This computer (Ten komputer)** w celu ustanowienia połączenia, ale zainstalowany serwer AXIS Camera Station 5 nie jest uruchomiony. | Użyj aplikacji service control, aby uruchomić AXIS Camera Station 5, lub wybierz serwer zdalny, do którego chcesz się zalogować. |
| Na tym komputerze nie zainstalowano serwera AXIS Camera Station 5. | Do połączenia używasz apletu **This computer (Ten komputer)**, ale na tym komputerze nie zainstalowano serwera. | Zainstaluj serwer AXIS Camera Station 5 lub wybierz inny serwer. |
| Wybrana lista serwerów jest pusta | Lista serwerów wybrana na potrzeby logowania była pusta. | Aby dodać serwery do listy, kliknij **Edit (Edytuj)** obok opcji wyboru listy serwerów. |

## Licencje

### Problemy z rejestracją licencji

Jeżeli automatyczna rejestracja nie się powiedzie, wypróbuj następujące rozwiązania:

- Sprawdź, czy klucz licencyjny został wprowadzony poprawnie.
- Zmień ustawienia serwera proxy klienta, aby zezwolić aplikacji AXIS Camera Station 5 na dostęp do Internetu.
- Zarejestruj licencje offline — zob. *Licencja na system w trybie offline* w instrukcji obsługi aplikacji AXIS Camera Station 5.
- Zanotuj identyfikator serwera i aktywuj licencję AXIS Camera Station 5 z poziomu strony *license-portal.lp.axis.com*.
- Upewnij się, że czas serwera jest aktualny.

## Użytkownicy

### Nie można odnaleźć użytkowników domeny

Jeżeli wyszukiwanie użytkownika w domenie nie powiedzie się, zmień konto logowania do usługi:

1. Otwórz **Windows Control Panel (Panel sterowania w systemie Windows)**.
2. Wyszukaj „Services".
3. Kliknij **View local services (Wyświetl usługi lokalne)**.
4. Kliknij prawym przyciskiem myszy AXIS Camera Station 5 i wybierz opcję **Properties (Właściwości)**.
5. Kliknij kartę **Log on (Logowanie)**.

6. Zamiast opcji **Local System account (Lokalne konto systemowe)** zaznacz opcję **This account (To konto)**.
7. Zaznacz użytkownika z dostępem do usługi Windows Active Directory.

## Błędy certyfikatów

AXIS Camera Station 5 nierozwiązany błąd certyfikatu uniemożliwia komunikację z urządzeniem.

| Możliwe błędy | | |
|---|---|---|
| **Certificate Not Found (Nie znaleziono certyfikatu)** | Jeżeli został usunięty certyfikat urządzenia. | Jeśli znasz przyczynę, kliknij **Repair (Napraw)**. Jeżeli podejrzewasz nieautoryzowany dostęp, przed przywróceniem certyfikatu dokładnie zbadaj problem Kliknij przycisk **Advanced (Zaawansowane)**, aby wyświetlić szczegóły certyfikatu. Możliwe przyczyny usunięcia certyfikatu:<br>• Urządzenie zresetowano do ustawień fabrycznych.<br>• Wyłączono funkcję bezpiecznej komunikacji przy użyciu protokołu HTTPS.<br>• Nieuprawniona osoba uzyskała dostęp do urządzenia i zmieniła jego ustawienia. |
| **Niezaufany certyfikat** | Certyfikat urządzenia został zmieniony poza AXIS Camera Station 5. Może to wskazywać, iż nieuprawniona osoba uzyskała dostęp do urządzenia i zmieniła jego ustawienia. | Jeśli wiesz, jaka jest przyczyna, kliknij polecenie **Trust This Device (Ufaj temu urządzeniu)**. Jeśli nie znasz źródła problemu, dowiedz się, na czym polega problem, zanim uznasz certyfikat za zaufany. Kliknij przycisk **Advanced (Zaawansowane)**, aby wyświetlić szczegóły certyfikatu. |

### Brak hasła dla organu wydającego certyfikat

Jeśli w aplikacji AXIS Camera Station 5 znajduje się urząd certyfikacji bez zapisanego hasła, pojawi się poniższy alarm.

| **You need to provide a passphrase for the Certificate Authority certificate. (Należy podać hasło dla certyfikatu CA). Więcej informacji znajduje się w Podręczniku użytkownika.** |
|---|

Istnieją trzy rozwiązania tego problemu:

- Włączenie protokołu HTTPS na urządzeniu
- Zaimportowanie istniejącego CA
- Wygenerowanie nowego CA

Włączenie protokołu HTTPS na urządzeniu:

1. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
2. Na liście prawym przyciskiem myszy kliknij urządzenie i wybierz **Security > HTTPS > Enable/Update** (Bezpieczeństwo > HTTPS > Włącz / aktualizuj).
3. Kliknij przycisk **Yes (Tak)**, aby potwierdzić.
4. Wprowadź hasło CA.
5. Kliknij **OK**.

Importowanie istniejącego CA:

1. Przejdź do **Configuration > Security > Certificates > Devices** (Konfiguracja > Bezpieczeństwo > Certyfikaty > Urządzenia).
2. W pozycji HTTPS wyłącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).
3. W obszarze **Certificate authority (Organ wydający certyfikat (CA))** kliknij przycisk **Import (Importuj)**.
4. Wpisz hasło i kliknij przycisk **OK**.
5. Wybierz liczbę dni, przez jaką podpisane certyfikaty klientów/serwerów pozostają ważne.
6. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
7. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno polecenia **Zabezpieczenia > HTTPS > Włącz/Aktualizuj**.
8. Przejdź do **Configuration > Security > Certificates > Devices** (Konfiguracja > Bezpieczeństwo > Certyfikaty > Urządzenia) i włącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).

Uwaga

AXIS Camera Station 5 traci połączenie z urządzeniami, a niektóre składniki systemu uruchamiają się ponownie.

Aby umożliwić aplikacji AXIS Camera Station 5 wygenerowanie nowego urzędu certyfikacji:

1. Przejdź do **Configuration > Security > Certificates > Devices** (Konfiguracja > Bezpieczeństwo > Certyfikaty > Urządzenia).
2. W pozycji HTTPS wyłącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).
3. W obszarze **Certificate authority (Organ wydający certyfikat (CA))** kliknij przycisk **Generate (Generuj)**.
4. Wpisz hasło i kliknij przycisk **OK**.
5. Wybierz liczbę dni, przez jaką podpisane certyfikaty klientów/serwerów pozostają ważne.
6. Przejdź do menu **Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie)**.
7. Kliknij urządzenia prawym przyciskiem myszy i wybierz kolejno polecenia **Zabezpieczenia > HTTPS > Włącz/Aktualizuj**.
8. Przejdź do **Configuration > Security > Certificates > Devices** (Konfiguracja > Bezpieczeństwo > Certyfikaty > Urządzenia) i włącz opcję **Validate device certificate** (Potwierdź certyfikat urządzenia).

Uwaga

AXIS Camera Station 5 traci połączenie z urządzeniami, a niektóre składniki systemu uruchamiają się ponownie.

## Synchronizacja czasu

### Usługa Czas systemu Windows nie działa

Czas systemu Windows i serwer NTP nie są zsynchronizowane. Przyczyną może być brak możliwości połączenia się usługi Czas systemu Windows z serwerem NTP.

- Upewnij się, że serwer NTP jest online.
- Upewnij się, że ustawienia zapory sieciowej są prawidłowe.

- Upewnij się, że urządzenie znajduje się w sieci, która ma dostęp do serwera NTP.

W celu uzyskania pomocy skontaktuj się z administratorem systemu.

### Wykryto różnicę czasu w urządzeniu

Urządzenie nie jest zsynchronizowane z czasem na serwerze. Nagranie ma sygnaturę czasową momentu odebrania przez serwer, a nie nagrania przez urządzenie.

1. Wybierz kolejno opcje **Configuration > Devices > Time synchronization (Konfiguracja > Urządzenia > Synchronizacja czasu)** i sprawdź przesunięcie względem czasu na serwerze.
2. Jeżeli przesunięcie wynosi ponad 2 sekundy:
   2.1. Wybierz **Enable time synchronization (Włącz synchronizację czasu)**.
   2.2. Upewnij się, że urządzenie ma dostęp do wyznaczonego serwera NTP.
   2.3. Wczytaj ponownie urządzenie w oknie **Konfiguracja > Urządzenia > Zarządzanie**.
3. Jeżeli przesunięcie względem czasu serwera nie przekracza 2 sekund, być może urządzenie nie wysyła odpowiedniej ilości danych niezbędnych do synchronizowania czasu.
   3.1. Aby wyłączyć generowanie alarmów, wyczyść opcję **Send alarm when the time difference between server and device is larger than 2 seconds (Wyślij alarm, gdy różnica czasu między serwerem a urządzeniem przekroczy 2 sekundy)**.

W celu uzyskania wsparcia skontaktuj się z działem pomocy technicznej Axis.

## Wsparcie techniczne

Wsparcie techniczne jest dostępne dla klientów mających licencjonowaną wersję aplikacji AXIS Camera Station 5. Aby się skontaktować z działem pomocy technicznej, wybierz kolejno  **> Help (Pomoc) > Online Support (Wsparcie online)** lub przejdź do strony *axis.com/support*.

Zalecamy, aby do zgłoszenia o pomoc techniczną dołączyć raport systemowy i zrzut ekranu.

W celu utworzenia raportu systemowego wybierz kolejno  **> Help (Pomoc) > System report (Raport systemowy)**.

### Proces eskalacji

W przypadku wystąpienia problemów, których nie można rozwiązać za pomocą tego przewodnika, zgłoś problem do internetowego punktu pomocy technicznej Axis, patrz *Internetowy punkt pomocy technicznej Axis*. Aby nasz zespół pomocy technicznej mógł zrozumieć i rozwiązać Twój problem, musisz podać następujące informacje:

- Jasny opis, jak odtworzyć problem lub okoliczności, w jakich występuje.
- Godzina i nazwa kamery lub adres IP, gdzie występuje problem.
- AXIS Camera Station 5 : raport systemowy generowany bezpośrednio po wystąpieniu problemu. Raport systemowy musi zostać wygenerowany przez klienta lub serwer, na którym odtworzono problem.
- Opcjonalne zrzuty ekranu lub nagrania ze wszystkich monitorów, pokazujące problem. Podczas wykonywania zrzutów ekranu/nagrań włącz funkcję nakładki debugowania.
- W razie potrzeby dołącz pliki bazy danych. Aby przyspieszyć przesyłanie, możesz je pominąć.

Niektóre problemy wymagają podania dodatkowych informacji, których zespół pomocy technicznej zażąda w razie potrzeby.

Uwaga

Jeśli rozmiar pliku (na przykład ślad sieciowy lub plik bazy danych) przekracza 100 MB użyj zaufanej usługi bezpiecznego udostępniania plików.

| Informacje dodatkowe | |
|---|---|
| **Dzienniki poziomu debugowania** | Czasami używamy dzienników poziomu debugowania do zebrania większej ilości informacji. Odbywa się to wyłącznie na żądanie inżyniera pomocy technicznej firmy Axis. Instrukcje można znaleźć w *internetowym centrum pomocy technicznej Axis*. |
| **Nakładka debugowania podglądu na żywo** | Czasami pomocne jest przekazanie zrzutów ekranu z danymi nakładki lub filmu pokazującego zmiany wartości w interesującym nas czasie. Aby dodać dane nakładki, wykonaj następujące czynności:<br>• Naciśnij klawisze Ctrl + i raz, aby wyświetlić dane nałożenia w podglądzie na żywo.<br>• Naciśnij klawisze Ctrl + i dwa razy, aby dodać informacje dotyczące usuwania błędów.<br>• Naciśnij klawisze Ctrl + i trzy razy, aby ukryć nałożenie. |
| **Ślad sieciowy** | Jeśli poprosi o to inżynier pomocy technicznej, wygeneruj ślady sieciowe podczas tworzenia raportu systemowego. Wykonaj ślady sieciowe w czasie, gdy występuje problem, jeśli jest to proces, który da się odtworzyć. Obejmuje to:<br>• 60-sekundowy ślad sieciowy zarejestrowany kamerą (dotyczy tylko oprogramowania sprzętowego w wersji 5.20 i nowszych)<br>W razie potrzeby użyj następującego polecenia VAPIX, aby zmienić login, adres IP i czas trwania (w sekundach):<br>`http://root:pass@192.168.0.90/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=60`<br>• 10–30-sekundowy ślad sieciowy na serwerze, ukazujący komunikację między serwerem a kamerą. |
| **Pliki baz danych** | W przypadkach, gdy musimy sprawdzić lub ręcznie naprawić bazę danych. Przed wygenerowaniem raportu systemowego zaznacz opcję **Include database in the report (Dołącz bazę danych do raportu)**. |
| **Zrzuty ekranu** | Użyj zrzutów ekranu, jeśli problem podglądu na żywo jest związany z interfejsem użytkownika. Na przykład, gdy chcesz pokazać oś czasu nagrań lub gdy trudno opisać problem. |
| **Nagrania ekranu** | Użyj nagrań ekranu, jeśli trudno jest opisać problem słowami, na przykład gdy odtworzenie problemu wymaga wiele interakcji z interfejsem użytkownika. |

T10122292_pl

2026-02 (M72.2)