

AXIS Camera Station Pro

Informacje

Program AXIS Camera Station Pro to rozwiązanie do zarządzania obrazem służące do dozoru, zapisu i zarządzania strumieniami wizyjnymi z kamer sieciowych Axis. Obsługuje kontrolę dostępu, zarządzanie wieloma lokalizacjami, integrację z AXIS Audio Manager oraz integrację z systemami innych producentów.

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

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

Opcja dostępu

Serwer AXIS Camera Station Pro – obsługuje komunikację z kamerami, wideoenkoderami i urządzeniami dodatkowymi w systemie. Informacje o wymaganiach systemowych i planowaniu możliwości znajdują się w sekcji *Wytyczne dotyczące sprzętu w instrukcji instalacji i migracji programu AXIS Camera Station Pro*.

Klient AXIS Camera Station Pro – zapewnia dostęp do zapisów, obrazu wideo na żywo, dzienników i konfiguracji. Możesz go zainstalować na dowolnym komputerze. W ten sposób uzyskasz dostęp do podglądu zdalnego i możliwość sterowania z dowolnego miejsca w sieci korporacyjnej lub przez internet.

Klient internetowy oprogramowania AXIS Camera Station – umożliwia uzyskanie dostępu do nagrań z oprogramowania AXIS Camera Station Pro oraz obrazu wideo w czasie rzeczywistym za pomocą przeglądarki internetowej. Więcej informacji znajduje się w *instrukcji obsługi klienta internetowego oprogramowania AXIS Camera Station*.

Aplikacja mobilna AXIS Camera Station Pro – 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.

Opcje pobierania

Przejdź na stronę *pobierania programu AXIS Camera Station Pro*, aby pobrać program, zaktualizować go lub wypróbować bezpłatnie przez 90 dni.

- **Free, fully featured 90-day trial** (Bezpłatna, w pełni funkcjonalna 90-dniowa wersja próbna): Wypróbuj program AXIS Camera Station Pro za darmo przez 90 dni. Licencja nie jest potrzebna.
- **Update your client only – Offline** (Zaktualizuj tylko klienta – w trybie offline): Aktualizuje klienta, czyli tę część programu AXIS Camera Station Pro, z którą nawiązujesz bezpośredni kontakt. Skorzystaj z tej opcji, jeżeli konieczna jest aktualizacja wyłącznie klienta, a nie serwera.
- **Update your client and server – Offline:** (Zaktualizuj klienta i serwer – w trybie offline): Skompresowany pakiet aktualizacji przeznaczony zarówno dla klienta, jak i dla serwera. Po pobraniu pliku .zip rozpakuj go, aby uzyskać dostęp do plików .msi i .cab, a następnie uruchom plik .msi, aby rozpocząć aktualizację.
- **Update your client and server – Online:** (Zaktualizuj klienta i serwer – w trybie online): Automatycznie pobiera, rozpakowuje i instaluje aktualizację. Uruchom plik .exe i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Komputer musi być dołączony do internetu aż do zakończenia instalacji.
- **Mobile app for iOS** (Aplikacja mobilna na system iOS): Aplikacja mobilna AXIS Camera Station Pro na urządzenia iPhone i iPad. Dostępna w sklepie App Store.
- **Mobile app for Android** (Aplikacja mobilna na system Android): Aplikacja mobilna AXIS Camera Station Pro na telefony i tablety z systemem Android. Dostępna w sklepie Google Play.

Samouczki wideo

Więcej szczegółowych przykładów korzystania z systemu znajduje się na stronie *AXIS Camera Station Pro tutorial videos*.

Funkcje systemowe

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

Co nowego?

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

Przydatne łącza dla administratora

- *Łączenie z serwerem, on page 9*
- *Konfiguruj urządzenia, on page 47*
- *Konfigurowanie pamięci masowej, on page 76*
- *Konfigurowanie nagrywania i zdarzeń, on page 82*
- *Konfigurowanie połączonych usług, on page 125*
- *Konfigurowanie serwera, on page 127*
- *Konfigurowanie zabezpieczeń, on page 138*

Więcej instrukcji

- *Klient internetowy oprogramowania AXIS Camera Station*
- *Przewodnik integracji AXIS Camera Station Pro*
- *Aplikacja mobilna AXIS Camera Station*
- *Samouczki filmowe o aplikacji AXIS Camera Station Pro*
- *Poradnik rozwiązywania problemów dotyczących aplikacji AXIS Camera Station Pro*
- *Instrukcje wzmacniania zabezpieczeń systemu AXIS Camera Station Pro*

Przydatne łącza dla operatora

- *Łączenie z serwerem, on page 9*
- *Konfigurowanie klienta, on page 120*
- *Podgląd na żywo, on page 13*
- *Odtwarzanie nagrań, on page 26*
- *Eksportowanie nagrań, on page 29*

Szybki Start

W przewodniku opisano uruchomienie systemu.

Zanim rozpocznieś:

- Skonfiguruj sieć IP na potrzeby wykonywanej instalacji. Zob. *Network configuration (Konfiguracja sieci)*.
- W razie potrzeby skonfiguruj porty serwera. Zob. *Konfiguracja portu serwera*.
- Sprawdź, czy Twój system jest bezpieczny. Zob. *Kwestie dotyczące bezpieczeństwa*.

Administrator:

1. *Uruchom system VMS*
2. *Dodawanie urządzeń*
3. *Konfiguracja metody zapisu, on page 7*

Operator:

1. *Oglądaj materiał wideo na żywo, on page 7*
2. *Wyświetl nagrania, on page 7*
3. *Eksportowanie nagrań, on page 7*
4. *Odtwarzanie i weryfikacja zapisów w AXIS File Player, on page 7*

Uruchom system VMS

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

Gdy otworzysz klienta, zobaczysz monit o licencjonowanie systemu. Kliknij **License now** (Licencjonuj teraz), aby przejść na stronę **Manage licenses** (Zarządzaj licencjami), na której możesz zarejestrować serwer w organizacji. Więcej informacji: *Zarządzanie połączonymi usługami, on page 125* i *Zarządzaj licencjami, on page 136*. Aby korzystać z połączonych usług, takich jak klient internetowy VMS, monitorowanie kondycji systemu i licencjonowanie online, należy zarejestrować i połączyć system z organizacją.

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

Dodawanie urządzeń

Przy pierwszym uruchomieniu AXIS Camera Station Pro otwiera się strona **Add devices** (Dodaj urządzenia), która przeszukuje sieć pod kątem urządzeń do dodania. Zob. *Dodawanie urządzeń*.

1. Wybierz z listy urządzenia, które chcesz dodać. Jeśli nie możesz znaleźć urządzenia, kliknij **Manual search** (Ręczne wyszukiwanie) lub wpisać tekst, aby zawęzić wyniki.
2. Kliknij **Dodaj**.
3. Kliknij **Close** (Zamknij), aby pominąć konfigurację i kontynuować później. Aby kontynuować konfigurację teraz:
 - 3.1. Wybierz **Quick configuration (Szybka konfiguracja)** lub **Site Designer configuration (Konfiguracja Site Designer)**. Więcej informacji p. *Importowanie projektów AXIS Site Designer, on page 51*.
 - 3.2. Wybierz **Add image overlay for date, time, and text** (Dodaj nakładkę obrazu z datą, godziną i tekstem), aby dodać nakładki do wszystkich kamer Axis, które jeszcze ich nie mają.
 - 3.3. Kliknij **Next (Dalej)**.
 - 3.4. Wybierz preferowane ustawienie **Recording method (Metoda nagrywania)**.
 - 3.5. Kliknij **Next (Dalej)**.

- 3.6. Wybierz **Retention time** (Czas przechowywania) oraz **Recording storage** (Pamięć masowa nagrań), a następnie kliknij **Finish** (Zakończ), aby zastosować konfigurację.

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 p. *Podgląd na żywo, on page 13*.

Wyświetl nagrania

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

Więcej informacji p. *Nagrania, on page 26*.

Eksportowanie nagrań

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 **Export...** (Eksportuj).

Więcej informacji p. *Eksportowanie nagrań, on page 29*.

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 **Verify** (Weryfikuj), aby zapoznać się z wynikami weryfikacji.

Uwaga

- Podpis cyfrowy różni się od podpisanego obrazu. Podpisany obraz (nagranie) pozwala ustalić kamerę, z

której pochodzi, dzięki czemu można sprawdzić, czy nie doszło w niej do sabotażu. 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 Pro, skonfiguruj ustawienia proxy lub zapory, jeżeli klient, serwer i połączone urządzenia sieciowe znajdują się w różnych sieciach.

Ustawienia proxy klienta

Jeżeli między klientem a serwerem znajduje się serwer proxy, skonfiguruj ustawienia serwera proxy w systemie Windows na komputerze klienckim. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

Ustawienia proxy na serwerze

Jeśli serwer proxy znajduje się między urządzeniem sieciowym a serwerem, należy skonfigurować ustawienia serwera proxy w systemie Windows na serwerze. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

NAT i Zapora sieciowa

Jeżeli klient i serwer są oddzielone przez NAT lub zaporę sieciową, skonfiguruj je tak, aby był przepuszczany ruch przez port HTTP, port TCP i port strumieniowania, które określono w usłudze AXIS Camera Station Pro Service Control. Po pomocy zwróć się do administratora sieci.

Więcej informacji p. *Lista portów dotycząca AXIS Camera Station Pro, on page 216.*

Konfiguracja portu serwera

Serwer AXIS Camera Station Pro używa portów 29202 (TCP) i 29204 (HTTPS) do komunikacji serwer-klient. W razie potrzeby porty można zmieniać w usłudze AXIS Camera Station Pro Service Control.

Uwaga

Numery portów zmień tylko wtedy, gdy zamierzasz używać AXIS Camera Station Pro bez korzystania z usługi „Axis Secure Remote Access v2” ani z żadnych innych usług chmurowych Axis.

Więcej informacji, p. sekcja *Ogólne ustawienia serwera* lub *Często zadawane pytania*.

Kwestie dotyczące bezpieczeństwa

Aby zapobiec nieuprawnionemu dostępowi do kamer i nagrań:

- Używaj silnych haseł dla wszystkich urządzeń sieciowych (kamer, koderów wideo i urządzeń pomocniczych).
- Zainstaluj serwer AXIS Camera Station Pro, kamery, kodery wizyjne i urządzenia pomocnicze w zabezpieczonej sieci odseparowanej od sieci biurowej. Klienta AXIS Camera Station Pro możesz zainstalować na komputerze w innej sieci, na przykład sieci z dostępem do Internetu.
- Upewnij się, że wszyscy użytkownicy mają silne hasła.

Łączenie z serwerem

Klient AXIS Camera Station Pro umożliwia łączenie się z jednym lub kilkoma serwerami na różne sposoby:

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 – Zob. *Łączenie z serwerem zdalnym, on page 9.*

Axis Secure Remote Access v2 – Zob. *Logowanie do funkcji AXIS Secure Remote Access v2, on page 9.*

Uwaga

- Przy pierwszym połączeniu z serwerem klient sprawdza identyfikator certyfikatu serwera. Aby sprawdzić, czy łączysz się z właściwym serwerem, porównaj identyfikator certyfikatu z tym wyświetlanym w AXIS Camera Station Pro Service Control. Więcej informacji p. *Ogólne ustawienia serwera, on page 216.*
- Klient i serwer muszą mieć tę samą wersję. Jeżeli podczas łączenia się z systemem lokalnym lub systemem z mapowaniem portów wystąpi niezgodność wersji, klient może pobrać prawidłową wersję i przełączyć się na nią.
- Aby klient mógł połączyć się z kilkoma serwerami, każdy z nich musi mieć tę samą wersję. Domyślnie skrót klienta korzysta z najnowszej wersji.

Server list (Lista serwerów)	Aby połączyć się z serwerami z listy serwerów, wybierz serwer z menu rozwijalnego Server list (Lista serwerów). Kliknij  , aby utworzyć lub edytować listy serwerów. Zob. <i>Listy serwerów.</i>
Import server list (Importuj listę serwerów)	Aby zaimportować plik listy serwerów wyeksportowany z AXIS Camera Station Pro, kliknij Import server list (Importuj listę serwerów) w prawym dolnym rogu i przejdź do pliku .msl. Zob. <i>Listy serwerów.</i>
Delete saved passwords (Usuń zapisane hasła)	Aby usunąć zapisane nazwy użytkowników i hasła dla wszystkich połączonych serwerów, kliknij Delete saved passwords (Usuń zapisane hasła).

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 na liście nie znajduje się serwer, kliknij , aby odświeżyć listę wszystkich dostępnych serwerów zdalnych. Jeżeli na serwerze skonfigurowano akceptowanie połączenia od klientów na portach innych niż domyślny 29202, wprowadź adres IP, a nim numer portu, na przykład 192.168.0.5:46001.
3. Wypróbuj jedno z poniższych rozwiązań:
 - 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.

Logowanie do funkcji AXIS Secure Remote Access v2

1. Kliknij łącze **Sign in to AXIS Secure Remote Access v2 (Zaloguj się do funkcji AXIS Secure Remote Access v2)**.

2. Wprowadź dane swojego konta MyAxis.
3. Kliknij przycisk **Sign in (Zaloguj)**.
4. Wybierz organizację i kliknij **OK**.
5. Wybierz serwer, do którego chcesz się zalogować.
6. Zaloguj się przy użyciu poświadczeń dostępu do serwera.

Uwaga

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

Pasek stanu u dołu klienta AXIS Camera Station Pro pokazuje stopień wykorzystania funkcji Axis Secure Remote Access v2. W obszarze **Data used this month (Dane wykorzystane w tym miesiącu)** widać łączną ilość danych wykorzystanych przez organizację w ciągu miesiąca. Licznik jest resetowany o północy pierwszego dnia każdego miesiąca.

Axis Secure Remote Access v2 na urządzeniach mobilnych

Aby zalogować się do serwera przy użyciu funkcji Axis Secure Remote Access v2 na urządzeniu mobilnym (iOS i Android):

1. Przejdź do axis.com/products/axis-camera-station/overview i pobierz aplikację mobilną AXIS Camera Station.
2. Zainstaluj tę aplikację mobilną i ją otwórz.
3. Zaloguj się do funkcji Axis Secure Remote Access v2 przy użyciu poświadczeń konta My Axis.
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.
- Zanim się zalogujesz za pomocą konta My Axis, musisz otrzymać zaproszenie umożliwiające dołączenie do organizacji jako użytkownik.

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

Ustawienia proxy klienta

Jeśli między klientem AXIS Camera Station Pro a serwerem AXIS Camera Station Pro znajduje się serwer proxy, należy skonfigurować ustawienia serwera proxy w systemie Windows na komputerze klienckim. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

Klient AXIS Camera Station Pro

Karty

 Podgląd na żywo	Wyświetlanie filmowego obrazu na żywo z podłączonych kamer. Zob. <i>Podgląd na żywo</i> .
 Nagrania	Wyszukiwanie, odtwarzanie i eksportowanie nagrań. Zob. <i>Nagrania</i> .
 Inteligentne wyszukiwanie 1	Znajdź zdarzenia w nagraniu za pomocą funkcji wyszukiwania ruchu. Zob. <i>Inteligentne wyszukiwanie 1</i> .
 Wyszukiwanie danych	Wyszukiwanie danych z zewnętrznego źródła lub systemu i śledzenie tego, co wydarzyło się w czasie każdego zdarzenia. Zob. <i>Wyszukiwanie danych, on page 44</i> .
 Konfiguracja	Zarządzaj dołączonymi urządzeniami i konfiguruj ustawienia klientów i serwerów. Zob. <i>Konfiguracja</i> .
 Klawisze skrótu	Wyświetl i skonfiguruj klawisze skrótu. Zob. <i>Klawisze skrótu</i> .
 Dzienniki	Rejestry alarmów, zdarzeń i kontroli. Zob. <i>Dzienniki</i> .
 Zarządzanie dostępem	Konfigurowanie i zarządzanie posiadaczami kart, grupami, drzwiami, strefami i regułami dostępu w systemie. Zob. <i>Zarządzanie dostępem, on page 185</i> .
 Inteligentne wyszukiwanie 2	Zaawansowane filtry do znajdowania pojazdów i osób na podstawie charakterystyki. Zob. <i>Inteligentne wyszukiwanie 2, on page 38</i> .
 Monitorowanie stanu systemu	Monitorowanie danych dotyczących kondycji z jednego lub wielu systemów AXIS Camera Station Pro. Zob. <i>Monitorowanie stanu systemu BETA, on page 197</i> .
 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. Zob. <i>Tworzenie działań podglądu na żywo</i> .
 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). Zob. <i>Alarmy i Dzienniki</i> .

Menu główne

	Otwórz menu główne.
Serwery	Ustanów połączenie z nowym serwerem AXIS Camera Station Pro i wyświetl listy serwerów oraz stan połączenia dla każdego z tych serwerów. Zob. <i>Konfigurowanie serwera</i> .

Działania	Ręczne uruchomienie lub zatrzymanie nagrywania oraz zmiana statusu portów we/wy. Zob. <i>Ręczne nagrywanie</i> i <i>Monitorowanie portów we/wy</i> .
Pomoc	Dostęp do pomocy i opcji wsparcia. Kliknij kolejno Help (Pomoc) > About (Informacje) , aby sprawdzić używaną wersję klienta AXIS Camera Station Pro.
Wyloguj się	Wyloguj się i rozłącz z serwerem.
Wyjdź	Wyjście i zamknięcie klienta AXIS Camera Station Pro.

Pasek tytułu

 lub F1	Otwórz pomoc.
	Przejdź do trybu pełnoekranowego.
 lub ESC	Zamknij tryb pełnoekranowy.

Pasek stanu

- Ikona ostrzegawcza wskazuje na rozbieżność ustawienia czasu pomiędzy klientem a serwerem. Sprawdź, czy te ustawienia czasu są zsynchronizowane, aby uniknąć problemów z działaniem osi czasu.
- W sekcji stanu połączenia serwera widać liczbę podłączonych serwerów. Zob. *Status połączenia*.
- W sekcji Status licencji widać liczbę urządzeń bez licencji. Zob. *Zarządzaj licencjami*.
- W sekcji „Wykorzystanie funkcji Secure Remote Access v2” można sprawdzić, ile danych zużyto w tym miesiącu.
- Komunikat **AXIS Camera Station Pro update available** (Dostępna aktualizacja) oznacza, że dostępna jest nowa wersja. Widoczny tylko po zalogowaniu jako administrator. Zob. *Aktualizuj AXIS Camera Station Pro*, on page 131.

Alarms and Tasks (Alarmy i zadania)

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

Podgląd na żywo

Podgląd na żywo przedstawia obraz na żywo z dołączonych kamer. Po połączeniu z kilkoma serwerami AXIS Camera Station Pro wyświetlane są wszystkie widoki i kamery pogrupowane według nazw serwerów.

Widoki umożliwiają dostęp do wszystkich kamer i urządzeń dodanych do AXIS Camera Station Pro. 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.

Dzięki integracji z programem AXIS Audio Manager Pro można również konfigurować i dodawać strefy nagłośnieniowe z interfejsami przywołań w widoku na żywo. Więcej informacji znajduje się w sekcji *Korzystanie z interfejsów przywołań w widokach dzielonych*, on page 21

Dostęp do widoków mają wszyscy użytkownicy. Więcej o prawach dostępu użytkowników: *Uprawnienia użytkownika*, on page 138.

Aby skonfigurować podgląd na żywo, p. sekcja *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 wybór, 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 dekodery wizyjny jest w użyciu.

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 dzielony, sekwencję, widok z kamery, mapę, stronę internetową lub folder.
	Edytuj widok lub nazwę kamery. Aby zmodyfikować ustawienia kamery, p. sekcja <i>Edycja ustawień kamery</i>
	Usuń widok. Chcąc usunąć widok, trzeba mieć uprawnienia do modyfikowania widoku oraz jego wszystkich widoków podrzędnych. Aby usunąć kamery z AXIS Camera Station Pro, p. sekcja <i>Kamery</i> , on page 54.
	Jako administrator możesz zablokować widok, aby uniemożliwić operatorom jego przenoszenie lub edycję.

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 określonym w obszarze Configuration > Client > Settings (Konfiguracja > Klient > Ustawienia). Uwaga Program AXIS Camera Station Pro podczas wykonywania ujęć zazwyczaj korzysta ze strumienia wizyjnego, zatem zapisane ujęcie ma tę samą rozdzielczość co strumień wizyjny. Jednak w przypadku kamer panoramicznych i typu „rybie oko”, które wymagają łączenia lub korekcy krzywizn obrazu, ujęcie jest wykonywane po stronie klienta, bezpośrednio z ekranu. Może to dawać obrazy o niższej rozdzielczości, zwłaszcza w widokach obejmujących wiele kamer, gdzie każdy obraz na ekranie jest mniejszy.
Dodawanie ujęcia do eksportu	Aby dodać ujęcie do listy eksportu, 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)	Dostępna w kamerach PTZ oraz kamerach, dla których w interfejsie internetowym skonfigurowano 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.
Przybliżanie	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, 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, na który chcesz skierować kamerę. Aby obracanie i pochylanie działało ustawicznie, przesunij kursor do środka obrazu, tak aby pojawiła się strzałka nawigacyjna. Kliknij i przytrzymaj przycisk, a widok zostanie obrócony w kierunku strzałki. Aby obracać i pochylać w szybszym tempie, kliknij i przytrzymaj przycisk myszy, tak aby strzałka nawigacyjna się wydłużyła.
Ustaw ostrość	Aby wyregulować ostrość w urządzeniu AXIS, kliknij prawym przyciskiem myszy obraz i wybierz opcję Set

	focus (Ustaw ostrość). Użyj pasków Near (Blisko) oraz Far (Daleko), aby ustawić ostrość ręcznie, lub kliknij (AF), aby ustawiać ją automatycznie. Aby wyregulować ostrość w urządzeniu zgodnym ze standardem ONVIF, kliknij prawym przyciskiem myszy obraz i wybierz opcję Set focus (Ustaw ostrość). Wybierz Focus mode (Tryb ustawiania ostrości). Zawartość okna dialogowego zmienia się w zależności od wybranego trybu: • Absolute (Wartość bezwzględna): ustaw ogniskowanie w określonej pozycji, wprowadzając wartość i klikając Apply (Zastosuj). • Relative (Wartość względna): umożliwia stopniową regulację ogniskowania. W przypadku obiektów znajdujących się blisko kamery użyj ustawienia Near (Blisko), a w przypadku znajdujących się dalej – ustawienia Far (Daleko). • Continuous (Tryb ciągły): Przesuwaj punkt ogniskowania za pomocą opcji Nearer (Bliżej) lub Further (Dalej) i po zakończeniu kliknij Stop. • Aby ustawiać ostrość automatycznie, kliknij AF.
Focus recall zone (Strefa przywracania ostrości)	Kliknij obraz prawym przyciskiem myszy, wybierz polecenie Focus recall zone (Strefa przywołania ogniskowania) , a następnie wybierz opcję dodania lub usunięcia strefy przywołania ogniskowania.
Automatyczne śledzenie wł./wył.	Kliknij obraz prawym przyciskiem myszy i 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.
Położenia zaprogramowane	Aby przejść do położenia zaprogramowanego, kliknij obraz prawym przyciskiem myszy, wybierz polecenie Presets (Położenia zaprogramowane) , i wybierz położenie zaprogramowane. Aby utworzyć położenia zaprogramowane, p. <i>Położenia zaprogramowane PTZ</i> .
Dodaj położenie zaprogramowane	Aby dodać położenie zaprogramowane, przeciągnij widok obrazu w żądane miejsce, kliknij prawym przyciskiem myszy i wybierz kolejno polecenia Presets > Add preset (Położenia zaprogramowane > Dodaj położenie zaprogramowane) .

Bezwzględny ruch PTZ	Dostępny dla urządzeń zgodnych ze standardem ONVIF obsługujących bezwzględne pozycjonowanie PTZ. Użyj tej funkcji, aby przesunąć kamerę do precyzyjnych, powtarzalnych współrzędnych. 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. Zob. <i>Profile strumieniowania</i> .



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 mechaniczną funkcję PTZ dla użytkowników. Zob. *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, ustaw kursor na obrazie i kliknij  Instant replay (Natychmiastowe odtwarzanie). Zostanie otwarta karta Zapisy, na której obejrzysz ostatnie 5 sekund nagrania.
REC	Aby zapisywać ręcznie z poziomu podglądu na żywo, ustaw kursor myszy na obrazie i kliknij przycisk REC . Przycisk zmieni się na żółty, wskazując, że trwa zapis. Aby zatrzymać rejestrację, kliknij ponownie REC .

Aby skonfigurować ustawienia ręcznego zapisu takie jak rozdzielczość, kompresja i częstotliwość odświeżania, p. sekcja *Metoda nagrywania*. Więcej informacji o nagrywaniu i odtwarzaniu: *Odtwarzanie nagrań*.

Uwaga

Jako administrator możesz wyłączyć funkcję zapisu ręcznego dla użytkowników. Zob. *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. Zob. *Profile strumieniowania, on page 55*.

 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) . Zob. <i>Przesyłanie strumieniowe, on page 123</i> .

Uwaga

Jako administrator możesz wyłączyć obsługę dźwięku dla użytkowników. Zob. *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 dzielonego możesz dodać widoki kamer, sekwencje, strony internetowe, mapy i inne widoki dzielone.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station Pro, 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 menu rozwijalnego **Template (Szablon)** wybierz układ.
5. Przeciągnij i upuść kamery lub widoki z panelu bocznego na siatkę lub kliknij dwukrotnie, aby dodać je do pierwszego dostępnego okna.
6. Kliknij przycisk **Save view (Zapisz widok)**.

Aby edytować kamerę lub widok w siatce, zaznacz go. W sekcji **Select item to configure** (Wybierz element do konfiguracji) możesz:

- Kliknąć przycisk **Remove** (Usuń), aby usunąć go z siatki.
- Wybrać **PTZ preset** (Położenie zaprogramowane PTZ) z menu rozwijalnego.

Aby dodać aktywny punkt:

- Wybierz ramkę i kliknij **Set hotspot** (Ustaw aktywny punkt) w sekcji **Hotspot** (Aktywny punkt).

Aby automatycznie wyświetlać uruchomione strumienie wizyjne w aktywnym punkcie:

- Wybierz opcję **Dynamic hotspot content** (Treść dynamicznego aktywnego punktu) i skonfiguruj ustawienia. Więcej informacji, p. sekcja *Dynamiczny aktywny punkt, on page 18* (Dynamiczny aktywny punkt).

Aby ustawić profil strumieniowania kamery:

- Kliknij go prawym przyciskiem myszy w widoku siatki i wybierz **Stream profile** (Profil strumieniowania). P. sekcja *Profile strumieniowania, on page 55*.

Dynamiczny aktywny punkt

Wykorzystaj dynamiczne aktywne punkty do jednoczesnego monitorowania wielu zdarzeń. Po uruchomieniu reguł działania strumienie wizyjne pojawiają się automatycznie w aktywnym punkcie. Przykładowo, jeżeli wykryto ruch przy trzech różnych wejściach, obrazy ze wszystkich trzech kamer pojawiają się jednocześnie.

Aktywny punkt dostosowuje swoją siatkę w oparciu o liczbę aktywnych widoków. Każdy widok zawiera licznik czasu i znika po zakończeniu odliczania.

Uwaga

W przypadku kamer, w których wyzwalaczem podglądu na żywo jest określone działanie, odliczanie rozpoczyna się w momencie, gdy działanie to przestaje być aktywne. W przypadku pozostałych kamer i widoków odliczanie rozpoczyna się natychmiast.

Utworzenie dynamicznego aktywnego punktu

Aby dodać nowy widok z dynamicznym aktywnym punktem:

1. Na karcie **Live view** (Podgląd na żywo) kliknij **+**.
2. Kliknij **Add hotspot** (Dodaj aktywny punkt).
3. Wybierz **Dynamic hotspot content** (Zawartość dynamicznego aktywnego punktu).
4. Skonfiguruj ustawienia:
 - **Number of split view cells** (Liczba komórek w widoku dzielonym): Liczba komórek w siatce zachowywana nawet, gdy żadne widoki nie są aktywne. Zakres: 1 – 144.
 - **Countdown in seconds** (Odliczanie w sekundach): Wskazanie jak długo pozostaje widoczny każdy wyzwolony widok. Ustawienie wartości 0 powoduje, że widok pozostaje aktywny do czasu ręcznego usunięcia. Zakres: 0 – 999.
 - **Seconds remaining when countdown appears in view** (Liczba pozostałych sekund, gdy w widoku wyświetlane jest odliczanie): Określa, kiedy licznik odliczający pojawi się na ekranie. Ustaw wartość 0, aby zawsze wyświetlać ten element. Pamiętaj, że wyświetlanie licznika czasu zużywa zasoby systemowe. Zakres: 0 – 999.
 - **Mute audio on incoming views** (Wycisz dźwięk z wyświetlanych widoków): Nowe strumienie wyświetlane są z wyciszonym dźwiękiem. Można anulować ich wyciszenie pojedynczo.
 - **Allow adding views with click on view** (Zezwól na dodawanie widoków poprzez ich kliknięcie): Dodawaj ręcznie widoki do aktywnego punktu, klikając je obok wyzwolonych widoków.
 - **Allow adding views with hotkey** (Zezwól na dodawanie widoków obszarów obserwacji za pomocą klawisza skrótu): Używaj klawiszy skrótu, aby dodawać zdefiniowane widoki do aktywnego punktu obok wyzwolonych widoków.
5. Kliknij przycisk **Save view** (Zapisz widok).

Aby dodać dynamiczny aktywny punkt do istniejącego widoku:

1. Na karcie **Live view** (Podgląd na żywo) kliknij **Edit view** (Edytuj widok).
2. Kliknij **Add hotspot** (Dodaj aktywny punkt).
3. Wybierz **Dynamic hotspot** (Dynamiczny aktywny punkt).
4. Skonfiguruj ustawienia zgodnie z opisem w punkcie 4 powyżej.
5. Kliknij przycisk **Save view** (Zapisz widok).

Uwaga

Możesz przekształcić istniejący aktywny punkt w dynamiczny aktywny punkt, edytując go na karcie **Live view** (Podgląd na żywo).

Kontrola i zarządzanie widokami

Każda komórka w dynamicznym aktywnym punkcie zawiera:

- **Wskaźnik Countdown (Odliczanie)**: Pokazuje czas pozostały do zniknięcia widoku.
- **Przycisk Pause (Pauza)**: Wstrzymanie odliczania, aby dłużej wyświetlać widok.
- **Przycisk Close (Zamknij)**: Natychmiastowe usunięcie widoku z aktywnego punktu.
- **Wskaźnik Flash (Miganie)**: Ramka odliczania miga, gdy widok zostanie ponownie wyzwolony.

Te elementy sterujące są ukrywane po rozwinięciu komórki do pojedynczego widoku lub po przejściu do trybu odtwarzania. Kliknij dwukrotnie dowolną komórkę, aby wyświetlić ją w pełnym widoku. Po rozwinięciu widoku odliczanie zatrzymuje się automatycznie. Dynamiczny aktywny punkt jest na bieżąco aktualizowany w tle, a po powrocie do widoku siatki zobaczysz aktywne widoki.

Uwaga

Po przejściu do trybu odtwarzania strumienie z kamer zostają zatrzymane i nie będą aktualizowane. Przełącz z powrotem do podglądu na żywo, aby wznowić normalne działanie.

Pulpit nawigacyjny drzwi w widoku podzielonym

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

1. Dodaj drzwi. Zob. *Dodaj drzwi*, on page 152.
2. Dodaj pulpit drzwi do widoku dzielonego — zob. *Widok dzielony*, on page 18.

Pulpit nawigacyjny	Aby wyświetlić szczegóły drzwi i stan blokady, otwórz kartę Dashboard (Pulpit nawigacyjny). Na pulpicie nawigacyjnym są wyświetlane następujące informacje: • Zdarzenia kontroli dostępu z danymi posiadacza karty i jego zdjęciem, przykładowo, gdy posiadacz karty okaże kartę w czytniku. • Alarmy z informacjami o ich wyzwalaczach, na przykład zbyt długim otwarciu drzwi. • Najnowsza transakcja.
	Aby dodać zdarzenie do zakładek i udostępnić je na karcie Transactions (Transakcje), kliknij .
Wejdz na stronę	Aby ręcznie udzielić dostępu, kliknij pozycję Access (Dostęp). Powoduje to otwarcie drzwi tak, jakby ktoś okazał swoje uwierzytelnienie. Po upływie ustalonego czasu drzwi ponownie zamykają się automatycznie.
Lock (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).



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

Monitorowanie i wspieranie za pomocą pulpitu nawigacyjnego drzwi

Pulpit AXIS Data Insights w widoku dzielonym

Pulpit AXIS Data Insights Dashboard przedstawia dane analityczne z urządzeń w postaci wykresów i tabel. Aby dodać pulpit nawigacyjny do widoku dzielonego:

1. Skonfiguruj pulpit nawigacyjny. Zob. *AXIS Data Insights Dashboard*, on page 180.

2. Na karcie **Live view** (Podgląd na żywo) kliknij **+**.
3. Kliknij przycisk **New Split View (Nowy widok dzielony)**.
4. Rozwiń folder **Dashboards (Pulpity nawigacyjne)**.
5. Przeciągnij i upuść pulpit nawigacyjny na siatkę.
6. Kliknij przycisk **Save view (Zapisz widok)**.

Pulpity	
Analiza dźwięku	Zawiera dane ze zdarzeń AXIS Audio Analytics.
Liczenie przekroczeń linii	Wyświetla dane zliczania ze scenariusza liczenia naruszeń linii AXIS Object Analytics.
Generyczna	Wyświetla dane ze wszystkich obsługiwanych źródeł danych.
Image health (Stan obrazu)	Zawiera dane ze zdarzeń AXIS Image Health Analytics.
Zajętość obszaru	Zawiera dane o zajętości ze scenariusza zajętości obszaru AXIS Object Analytics.
Zliczanie wchodzących i wychodzących	Wyświetla dane ze scenariusza zliczania naruszeń linii w aplikacjach AXIS Object Analytics, AXIS People Counter oraz AXIS P8815-2 3D Counter.
Monitorowanie jakości powietrza	Wyświetla bieżące dane dotyczące jakości powietrza w pomieszczeniach z czujników AXIS Air Quality Sensor.
Szczegółowe dane monitorowania jakości powietrza	Wyświetla zagregowane dane z czujników AXIS Air Quality Sensor.

Korzystanie z interfejsów przywołań w widokach dzielonych

Możesz używać interfejsów przywołań do ogłaszania komunikatów na żywo, wykonywania wywołań lub odtwarzania plików fonicznych z urządzeń fonicznych. Wymaga to integracji z programem AXIS Audio Manager Pro. Więcej informacji znajduje się w sekcji *Konfiguracja programu AXIS Audio Manager Pro*, on page 175.

Aby korzystać z interfejsów przywołań:

1. Edytuj lub dodaj nowy widok dzielony.
2. Przeciągnij i upuść jedną lub kilka stref nagłośnieniowych na siatkę, aby zmienić ją w interfejs przywołania.

Uwaga

Strefy nagłośnieniowe w programie AXIS Camera Station Pro i strefy skonfigurowane na serwerze AXIS Audio Manager Pro są identyczne.

3. Wybierz **Speak (Mów)**, **Call (Wywołaj)** lub **Play a file (Odtwarzaj plik)**:
 - Wybierz **Speak (Mów)** w przypadku komunikacji jednokierunkowej czyli komunikatów na żywo.
 - Wybierz **Call (Wywołaj)** w przypadku komunikacji dwukierunkowej, na przykład gdy chcesz rozmawiać z kimś przez domofon.
 - Wybierz **Play a file (Odtwarzaj plik)**, aby odtworzyć plik z serwera AXIS Audio Manager Pro przez głośnik.

Sekwencja

Sekwencja służy do automatycznego przełączania między widokami.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station Pro, 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. Ułóż widoki w kolejności, w jakiej mają się pojawiać.
6. Kliknij widok, aby edytować jego ustawienia.
7. Kliknij przycisk **Save view** (Zapisz widok).

Prepozycja PTZ	W przypadku kamer PTZ wybierz, w którym położeniu zaprogramowanym ma się ustawić kamera, gdy ten widok jest aktywny.
Czas wyświetlania	Liczba sekund, przez które wyświetlany jest każdy widok, zanim nastąpi przejście do następnego widoku. Dla każdego widoku można to ustawić indywidualnie.

Uwaga

- Nie możesz dodać widoku sekwencji do innego widoku sekwencji.
- Nie możesz bezpośrednio dodawać widoków komponentów z serwera zdalnego. Rozwiązaniem jest dodanie widoku komponentu do pojedynczego widoku, a następnie dodanie tego widoku z serwera zdalnego.
- Odtwarzanie na osi czasu może działać w sposób nieoczekiwany. W trybie odtwarzania wyświetlane są wszystkie kamery w sekwencji, ale w danym momencie aktywna jest tylko jedna.

Wykorzystanie paska sekwencji

Przy przeglądzie sekwencji pasek znajdujący się na dole obszaru podglądu umożliwia ręczne sterowanie odtwarzaniem:

- Użyj przycisków [**>**] oraz [**<**], aby przejść do następnego lub poprzedniego widoku.
- Użyj przycisku **Hold** (Wstrzymaj) albo **Continue** (Kontynuuj), aby wstrzymać lub wznowić sekwencję.
- Licznik pokazuje, ile sekund pozostało do następnego automatycznego przełączenia.
- Kliknij prawym przyciskiem myszy sekwencję, aby ukryć pasek.
- Gdy sekwencja jest otwarta na karcie **Recording** (Zapis), automatycznie ustawia się na **Hold** (Wstrzymaj) i można się po niej poruszać wyłącznie ręcznie za pomocą przycisków następny i poprzedni.

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 Pro 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 zaimportowany obraz, na którym można umieścić widoki kamery, widoki dzielone, strefy nagłośnieniowe, 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.

Przyciski działań są również dostępne w widoku mapy. Zob. *Tworzenie wyzwalaczy opartych na przyciskach akcji*.

Uwaga

Jeżeli komputer łączy się z kilkoma serwerami AXIS Camera Station Pro, 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. Plik nie może być większy niż 20 MB. Obsługiwane standardy: BMP, JPG, PNG i GIF.
5. Przeciągnij na mapę widoki, kamery, inne urządzenia oraz drzwi.
6. Kliknij ikonę na mapie, aby edytować jej ustawienia.
7. Kliknij przycisk **Add label (Dodaj etykietę)**, nadaj etykietcie nazwę oraz ustaw rozmiar, kąt obrotu, styl i kolor etykiety.
8. Kliknij przycisk **Save view (Zapisz widok)**.

Uwaga

- Niektóre ustawienia można edytować dla wielu ikon i etykiet równocześnie.
- Wszystkie urządzenia, do których Twoje konto użytkownika nie ma dostępu, są usuwane z mapy przy jej edycji.
- Nie możesz bezpośrednio dodawać widoków komponentów z serwera zdalnego. Rozwiązaniem jest dodanie widoku komponentu do pojedynczego widoku, a następnie dodanie tego widoku z serwera zdalnego do mapy.

Ustawienia ikon

Kliknij ikonę na mapie, aby otworzyć ustawienia.

	Fizyczny status drzwi, gdy drzwi skonfigurowano z monitorem drzwi.
	Fizyczny status drzwi, gdy drzwi skonfigurowano bez monitora drzwi.
	Czerwony trójkąt ostrzegawczy sygnalizuje alarm sabotażowy dotyczący drzwi, czytnika lub kontrolera 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.
Pokryty obszar	Dostępne w obsługiwanych urządzeniach. 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 Flash (Miga) , aby obszar pokrycia zaczął migać, gdy zapis uruchamiany jest przez detekcję ruchu lub inne reguły działania. Aby globalnie wyłączyć migające obszary pokrycia dla wszystkich urządzeń, p. sekcja <i>Ustawienia klienta, on page 120</i> .
Strzałka kierunkowa	Wyświetla strzałki wskazujące kierunek pola widzenia każdej kamery. Można wyświetlać strzałki z obszarami pokrycia lub bez nich.
Pokaż wskaźniki nagrywania	Określa, które wskaźniki zapisu są widoczne na ikonie. Włącz Small indicators (Małe wskaźniki) , aby wyświetlić ich pomniejszoną wersję. Za pomocą poszczególnych przełączników możesz wyświetlać lub ukrywać wskaźniki dotyczące zapisu (Recording), detekcji ruchu (Motion detected), wykrytych obiektów (Object detected) oraz aktywnych reguł działania (Action rule active). To ustawienie jest zapisywane na serwerze, zatem wszystkie klienty korzystają z tej samej konfiguracji.
Etykieta	Etykieta ma tekst, wielkość, orientację i kolor. Jest również możliwość podkreślenia lub zapisu zawartości etykiety kursywą.
Usuń	Kliknij  , aby usunąć ikonę z mapy.

Poruszanie się po mapie

Powiększenie i przesuwanie

- Możesz powiększać i przesuwać mapę za pomocą myszy, klawiatury albo joysticka. Nie ma obecnie możliwości obsługi dotykowej.

Mysz

- Za pomocą kółka myszy możesz powiększać i pomniejszać mapę.
- Po powiększeniu przeciągnij, aby poruszać się po mapie.

Klawiatura

- Naciśnij klawisze Ctrl + [+], aby powiększyć, albo Ctrl + [-], aby pomniejszyć mapę.
- Naciśnij klawisze Ctrl + strzałki, aby obracać i pochylać.

Joystick

- Przekręcaj głowicę joysticka, aby powiększać i pomniejszać.
- Przechyl joystick, aby obracać i pochylać.

Wykonaj ujęcie

- Kliknij prawym przyciskiem myszy na mapie, aby otworzyć menu kontekstowe. Możesz zapisać ujęcie mapy na dysku lub dodać je na karcie **Export** (Eksportuj). Ujęcie przedstawia mapę dokładnie taką, jaka jest w danym momencie, łącznie ze wszystkimi aktualnymi statusami kamer i stanami wskaźników.

Web page (Strona internetowa)

Widok strony internetowej pokazuje stronę z internetu. Możesz przykładowo dodać stronę internetową do dzielonego widoku lub sekwencji.

Aby dodać stronę internetową:

1. Na karcie **Live view** (Podgląd na żywo) kliknij **+**.
2. Wybierz **New web page** (Nowa strona internetowa).
3. Wpisz nazwę strony internetowej.
4. Wpisz URL strony internetowej.
5. Kliknij **OK**.



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

Foldery

Foldery służą do grupowania elementów w kategorii 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) możesz wyszukiwać, odtwarzać i eksportować nagrania. Na karcie znajduje się widok główny i dwa panele, w których można znaleźć widoki, obrazy, narzędzia do odtwarzania i kamery z dołączonych serwerów pogrupowane według nazwy serwera. Zob. *Podgląd na żywo*.

W widoku głównym można zarządzać obrazem w taki sam sposób, jak w podglądzie na żywo. Więcej informacji można znaleźć w temacie *Zarządzanie obrazami w podglądzie na żywo, on page 14*.

Aby zmienić metodę zapisu i ustawienia takie jak rozdzielczość, kompresja i częstotliwość odświeżania, p. sekcja *Metoda nagrywania*.

Uwaga

Nie można manualnie usunąć nagrań z AXIS Camera Station Pro. Aby usunąć stare nagrania, zmień czas przechowywania w **Configuration > Storage > Selection** (Konfiguracja > Pamięć masowa > Wybór).

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

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 wznowiane. Przesuń wskaźnik na osi czasu, aby przejrzeć treść i znaleźć konkretne chwile.

- Czerwona linia oznacza nagranie uruchomione detekcją ruchu.
- Niebieska linia oznacza nagranie uruchomione regułą działania.

Find recordings (Znajdowanie nagrań)

	Kliknij, aby wybrać datę i godzinę na osi czasu.
	Filtruj rodzaje nagrań wyświetlane na osi czasu.
	Użyj do znajdowania zapisanych zakładek. Zob. <i>Zakładki</i> .
	Kliknij, aby otworzyć listę nagrań i zakładek utworzonych za pomocą kamery nasobnej Axis. Można tu wyszukiwać datę i godzinę, metodę aktywacji nagrywania oraz wszelkie kategorie i notatki dodane przez użytkownika kamery w aplikacji AXIS Body Worn Assistant.
 Inteligentne wyszukiwanie 1	Wyszukaj nagrania za pomocą funkcji Inteligentne wyszukiwanie 1. Zob. <i>Inteligentne wyszukiwanie 1</i> .

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, aby zbliżyć lub oddalić. Aby zbliżyć dany obszar, przed przewinięciem umieść w nim kursor.

Zakładki

Uwaga

- Nie można usunąć zablokowanego nagrania, chyba że zostanie ręcznie odblokowane.
- Zablokowane nagrania są usuwane po usunięciu z systemu powiązanej kamery.

	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.
	Edytuj nazwę i opis zakładki albo zablokuj i odblokuj nagranie.

	Usuń zakładkę. Aby usunąć kilka zakładek, zaznacz je, przytrzymując klawisz Ctrl lub Shift, a następnie kliknij Remove (Usuń).
Prevent recording deletion (Chroń zapis przed usunięciem)	Zaznacz, aby zablokować nagranie. Usuń zaznaczenie, aby odblokować.

Dodawanie zakładki

1. Przejdź do nagrania.
2. Ustaw znacznik w odpowiednim położeniu poprzez powiększanie, pomniejszanie i przesuwanie na osi czasu.
3. Kliknij .
4. Wprowadź nazwę i opis zakładki. Użyj słów kluczowych, aby z łatwością znaleźć zakładkę.
5. Wybierz **Prevent recording deletion (Chroń zapis przed usunięciem)**, aby zablokować zapis.

Uwaga

Aby odblokować nagranie, usuń zaznaczenie **Prevent recording deletion (Chroń zapis przed usunięciem)** lub usuń zakładkę.

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

Kategorie zdarzeń

Przydzielaj kategorie do nagrań, aby łatwiej znajdować konkretne rodzaje zdarzeń. Zanim zaczniesz, sprawdź, czy posiadasz odpowiednie uprawnienia użytkownika. P. sekcja *Uprawnienia użytkownika/grupy*, on page 140.

Przydzielanie kategorii zdarzeń

1. Na karcie **Recordings** (Nagrania) odszukaj nagranie, któremu chcesz przypisać kategorię.
2. Kliknij prawym przyciskiem myszy nagranie na osi czasu i wybierz **Categorize event (Skategoryzuj zdarzenie)**.
3. Dodaj jedną lub wiele kategorii.
4. Kliknij **OK**.

Po przydzieleniu zdarzenia do kategorii wybrane kategorie pojawiają się na miniaturze nagrania. Jeżeli przydzieliłeś kolor do kategorii, pojawi się on na osi czasu.

Usuwanie kategorii zdarzeń

1. Na karcie **Recordings** (Nagrania) odszukaj nagranie, z którego chcesz usunąć kategorię.
2. Kliknij prawym przyciskiem myszy nagranie na osi czasu i wybierz **Categorize event (Skategoryzuj zdarzenie)**.
3. Na liście przydzielonych kategorii wybierz kategorię, którą chcesz usunąć.
4. Kliknij przycisk **Remove (Usuń)**.
5. Powtórz czynności 3 – 4 dla każdej kategorii, którą chcesz usunąć.
6. Kliknij **OK**.

Uwaga

Z przycisku **Remove (Usuń)** możesz korzystać tylko wtedy, gdy masz uprawnienia do usuwania kategorii lub gdy wybierzesz z listy kategorię, która nie została przydzielona.

Więcej informacji p. *Konfigurowanie kategorii zdarzeń*, on page 91.

Eksportowanie nagrań

Na karcie **Export** (Eksportu) można eksportować nagrania do urządzenia lokalnej pamięci masowej lub lokalizacji w sieci IP. Tutaj dostępne są również informacje oraz podgląd nagrania. Możesz jednocześnie eksportować kilka plików w standardach .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 standardach .mp4 i .mkv, ale nie w standardzie .asf.

Przed rozpoczęciem upewnij się, że masz uprawnienia do eksportowania. Zob. *Uprawnienie użytkownika do eksportowania*, on page 32.

Aby wyeksportować nagranie:

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 **Export...** (Eksportuj).
4. Wybierz folder, do którego chcesz wyeksportować nagrania.
5. Kliknij **OK**. Zadanie eksportowania pojawi się na karcie **Tasks (Zadania)**.

Folder eksportu zawiera następujące elementy:

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



Eksportowanie nagrań

Karta Recordings (Nagrania)	
	Aby zaznaczyć wiele nagrań, kliknij  i przesunź znaczniki wyboru do wybranego punktu początku i końca.
	Aby wyeksportować nagrania w obrębie znaczników wyboru, kliknij  .

Karta Recordings (Nagrania)	
Dodaj zapisy	Aby dodać pojedyncze nagranie, kliknij je prawym przyciskiem myszy i wybierz 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 pojedyncze 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 eksportowanego nagrania, usuń zaznaczenie pola 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  . Zob. <i>Edytowanie nagrań przed wyeksportowaniem, on page 32.</i>
	Aby edytować notatki do nagrania, zaznacz nagranie i kliknij  .
	Aby usunąć nagranie z listy eksportu, zaznacz je i kliknij  .
Przełącz na eksport	Jeżeli otwarta jest karta Incident report (Raport o zdarzeniu), kliknij przycisk Switch to export (Przełącz na eksport), aby powrócić do karty Export (Eksport).
Preferowany profil strumienia	Wybierz profil strumieniowania w polu Preferred stream profile (Preferowany profil strumieniowania).
Podgląd	Kliknięcie nagrania na liście eksportu spowoduje wyświetlenie jego podglądu. Podgląd kilku nagrań jest możliwy tylko, gdy nagrania pochodzą z tej samej kamery.
Zapisz	Aby zapisać listę eksportu do pliku, kliknij przycisk Save (Zapisz).

Karta Export (Eksport)	
Wczytaj	Aby uwzględnić zapisaną wcześniej listę eksportu, kliknij przycisk Load (Wczytaj).
Nazwa eksportu	Wpisz własną nazwę eksportowanego folderu i plików lub pozostaw pole puste, by użyć domyślnej konwencji nazewnictwa w AXIS Camera Station Pro.
Dodawanie nazwy kamery i znacznika czasu	Wybierz tę opcję, aby do nazwy eksportowanego folderu i plików dodać nazwę kamery oraz znacznik czasu.
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, przeciągnij oś czasu na podglądzie do wybranego miejsca, kliknij prawym przyciskiem myszy podgląd i wybierz Add snapshot (Dodaj ujęcie).

Ustawienia zaawansowane	
Dołącz uwagi	Zaznacz Include notes (Dołącz uwagi), aby dołączyć notatki dot. nagrania jako plik .txt w folderze eksportu i jako zakładkę w aplikacji AXIS File Player.
Include AXIS File Player (Dołącz AXIS File Player)	Aby do eksportowanych nagrań dołączyć 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 zostały 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 .asf. P. sekcja <i>Odtwarzanie i weryfikowanie wyeksportowanych nagrań</i> , on page 33.
Eksportuj do pliku zip	Aby wyeksportować do pliku .zip, wybierz opcję Export to Zip file (Eksportuj do pliku zip) i w razie potrzeby wpisz hasło.

Ustawienia zaawansowane	
Export format (Format eksportu)	Z menu rozwijalnego Export format (Standard eksportu) wybierz standard, do którego chcesz wyeksportować nagrania. Jeżeli wybrano MP4, eksportowane nagrania nie zawierają dźwięku w standardzie 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. Zaznacz Automatic (Automatycznie), aby stosować kodowanie M-JPEG dla standardu M-JPEG, a kodowanie H.264 dla wszystkich pozostałych standardów.

Uprawnienie użytkownika do eksportowania

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

Aby skonfigurować uprawnienia, przejdź do tematu *Uprawnienia użytkownika, on page 138*.

Edytowanie nagrań 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. Przejdź do **Bounding box options > Size (Opcje obwódki > Rozmiar)** i dostosuj wielkość obwódki.
5. Przesuń obwódkę i umieść ją nad obiektem.
6. Przejdź do **Bounding box options > Fill (Opcje obwódki > Wypełnienie)** i ustaw je na **Pixelated** (Pikselizacja) 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 punkt końcowy, kliknij prawym przyciskiem myszy kształt rombu w ostatniej kluczowej ramce i wybierz opcję **Set end (Ustaw koniec)**. Spowoduje to usunięcie kluczowych klatek za punktem końcowym.

Uwaga

W nagraniu wideo można dodać wiele obwódek. Jeżeli obwódki nakładają się na siebie, w obszarze nakładania stosuje się wypełnienie w kolejności: Black, Pixelated, Clear (Czarny, Pikselizacja, Przezroczysty).

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

Wyświetlanie poruszającego się obiektu z rozmytym tłem

1. Utwórz obwódkę. Zob. *Rozmywanie ruchomego obiektu, on page 32*.
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 (określane też jako obwiednie i prostokąty ograniczające) na podstawie danych analitycznych, sprawdź, czy narzędzie analityczne w kamerze jest włączone. Zob. *Profile strumieniowania, on page 55*.

1. Na karcie **Export (Eksportuj)** lub **Incident report (Raport o zdarzeniu)** kliknij .
2. Kliknij przycisk **Generate bounding boxes (Generuj obwódki)**.
3. Sprawdź, czy obwódki obejmują poruszający się obiekt. Dostosuj w razie potrzeby.
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 Pro** uruchamia instalację automatycznie po dodaniu kamery do systemu. Zob. *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. Jeżeli wyeksportowany plik Zip jest chroniony hasłem, wpisz hasło, aby otworzyć folder.
2. Otwórz aplikację AXIS File Player. Wyeksportowane nagrania są odtwarzane automatycznie.
3. W aplikacji AXIS File Player kliknij , aby wyświetlić notatki dotyczące nagrania.
4. Aby zweryfikować podpis cyfrowy nagrań wyeksportowanych przy użyciu funkcji **Add digital signature** (Dodaj podpis cyfrowy):
 - 4.1. Przejdź do **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 **Incident report** (Raport o zdarzeniu) można eksportować raporty o zdarzeniach do urządzenia lokalnej pamięci masowej lub lokalizacji sieciowej. Możesz dołączać do raportów nagrania, ujęcia i notatki.

Przed rozpoczęciem upewnij się, że masz uprawnienia do eksportowania. Zob. *Uprawnienie użytkownika do eksportowania*, on page 32.



Zgłaszanie incydentów

Generowanie raportów o zdarzeniach

1. Na karcie **Recordings (Zapisy)** wybierz kamerę lub widok.
2. Dodaj nagrania do listy eksportu. Zob. *Eksportowanie nagrań*, on page 29.
3. Kliknij **Switch to incident report** (Przełącz na raport o zdarzeniu), aby przejść do karty **Incident report** (Raport o zdarzeniu).
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 eksportowanego nagrania, usuń zaznaczenie pola 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  . Zob. <i>Edytowanie nagrań przed wyeksportowaniem, on page 32.</i>
	Aby edytować notatki do nagrania, zaznacz nagranie i kliknij  .
	Aby usunąć nagranie z listy eksportu, zaznacz je i kliknij  .
Przełącz na raport o zdarzeniu	Jeżeli otwarta jest karta Export (Eksport), kliknij Switch to incident report (Przełącz na raport o zdarzeniu) i przejdź do karty Incident report (Raport o zdarzeniu).
Preferowany profil strumienia	Z listy rozwijalnej Preferred stream profile (Preferowany profil strumieniowania) wybierz profil strumieniowania.
Podgląd	Kliknięcie nagrania na liście eksportu spowoduje wyświetlenie jego podglądu. Podgląd kilku nagrań jest możliwy tylko, gdy nagrania pochodzą z tej samej kamery.
Zapisz	Aby zapisać raport o zdarzeniu do pliku, kliknij Save (Zapisz).
Wczytaj	Aby wczytać wcześniej zapisany raport o zdarzeniu, kliknij Load (Wczytaj).
Opis	Pole Description (Opis) jest automatycznie wypełniane wstępnie zdefiniowanymi danymi z szablonu opisu. Możesz też dodać inne informacje, które mają 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 możesz go zmienić ręcznie. Identyfikator w sposób niepowtarzalny oznacza raport o zdarzeniu.
Dołącz uwagi	Zaznacz Include notes (Dołącz uwagi), aby dołączyć notatki dot. nagrania jako plik .txt w folderze eksportu i jako zakładkę 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. Zaznacz <i>Automatic</i> (Automatycznie), aby stosować kodowanie M-JPEG dla standardu M-JPEG, a kodowanie H.264 dla wszystkich 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, przesun oś czasu w podglądzie do określonej lokalizacji, kliknij prawym przyciskiem myszy na podglądzie i wybierz Add snapshot (Dodaj ujęcie).

Ręczne nagrywanie

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station Pro można manualnie rozpoczynać i kończyć nagrywanie na dowolnym połączonym serwerze. W tym celu wybierz serwer z menu rozwijalnego **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. Najedź kursorem na ramkę 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

Użyj funkcji Inteligentne wyszukiwanie 1, aby znaleźć fragmenty nagrania, w których w określonym obszarze wykryto ruch.

Aby przyspieszyć wyszukiwanie, wybierz **Include analytics data** (Uwzględnij dane analityczne) w ustawieniach profilu strumieniowania. Zob. *Profile strumieniowania*.

Aby użyć funkcji Inteligentne wyszukiwanie 1:

1. Kliknij **+** i otwórz kartę **Smart search 1 (Inteligentne wyszukiwanie 1)**.
2. Wybierz kamerę, którą chcesz znaleźć.
3. Dostosowywanie obszarów 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 zakres dat i godzin na potrzeby wyszukiwania. Użyj klawisza Shift, aby wybrać zakres dat.
6. Kliknij **Search (Wyszukaj)**.

Wyniki wyszukiwania zostaną wyświetlone na karcie **Results (Wyniki)**. Kliknij prawym przyciskiem myszy jeden lub więcej wyników, aby wyeksportować nagrania.

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



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

Inteligentne wyszukiwanie 1

Inteligentne wyszukiwanie 2

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

Uwaga

Wymagania funkcji Inteligentne wyszukiwanie 2:

- Strumieniowe przesyłanie metadanych analitycznych za pośrednictwem protokołu RTSP.
- AXIS Video Content Stream na kamerach z systemem operacyjnym AXIS w wersjach starszych niż 9.60. Zob. *Instalowanie aplikacji do kamery, on page 70*.
- Synchronizacja czasu między serwerem AXIS Camera Station Pro a kamerami.

Po włączeniu Inteligentnego wyszukiwania 2 w kamerze Axis program AXIS Camera Station Pro rozpoczyna zapis metadanych z tej kamery i wykorzystuje je do klasyfikowania obiektów w scenie. Dzięki temu możesz korzystać z filtrów do odnajdywania interesujących treści.

Uwaga

- Zaleca się korzystanie z zapisu ciągłego, ponieważ detekcja ruchu może powodować generowanie alarmów bez dostępnego obrazu.
- Korzystaj ze standardu H.264, aby podgląd nagrań był widoczny w wynikach wyszukiwania.
- Sprawdź, czy warunki oświetleniowe są zgodne z danymi technicznymi kamery, aby zapewnić optymalną reprodukcję kolorów. W razie potrzeby użyj dodatkowego źródła światła.

Proces

1. *Konfigurowanie funkcji Inteligentne wyszukiwanie 2, on page 176*
2. Skonfiguruj synchronizację czasu między serwerem AXIS Camera Station Pro a kamerami. Zob. *Synchronizacja czasu, on page 74*.
3. Tworzenie filtra lub wczytanie istniejącego filtra. Zob. *Wyszukiwanie z filtrami, on page 38*.
4. Zarządzanie wynikami wyszukiwania. Zob. *Wyniki inteligentnego wyszukiwania, on page 42*.

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)**.

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

- Włącz klasyfikację 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). Uwaga Funkcja wyszukiwania podobieństw tworzy abstrakcyjne reprezentacje z przyciętych i cechujących się niską rozdzielczością obrazów osób i 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 czyjaś ogólną sylwetkę i kolor ubrania.
Swobodne wyszukiwanie tekstowe	Funkcja swobodnego wyszukiwania tekstowego umożliwia opisanie treści szukanych w nagraniach przy użyciu języka naturalnego (dostępny tylko język angielski). Zob. <i>Swobodne wyszukiwanie tekstowe, on page 40</i> .
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 w razie potrzeby dodaj lub usuń 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 w razie potrzeby dodaj lub usuń punkty.
Rozmiar	Aby filtrować według rozmiaru, kliknij przycisk Size (Rozmiar) , wybierz kamerę i włącz Filter by size on this camera (Filtruj według rozmiaru w tej kamerze) . Dostosuj minimalną wysokość i szerokość jako procent łącznego rozmiaru obrazu.

Czas trwania	Aby filtrować według czasu trwania, kliknij przycisk Duration (Czas trwania) , wybierz kamerę i włącz Filter by duration on this camera (Filtruj według czasu trwania w tej kamerze) . Dostosuj minimalny czas trwania w sekundach.
Szybkość	Aby filtrować według szybkości, kliknij przycisk Speed (Szybkość), wybierz kamerę i włącz Filter by speed on this camera (Filtruj według szybkości w tej kamerze). Określ zakres szybkości, który ma zostać uwzględniony w filtrze. Uwaga Filtr szybkości jest dostępny w urządzeniach radarowych oraz kamerach zintegrowanych z radarem, które umożliwiają wykrywanie szybkości.
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). Wybierz Share with other users (Udostępnij innym użytkownikom), aby udostępnić filtr innym użytkownikom. 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. Aby załadować jeden z zapisanych filtrów, kliknij  > Saved filters (Zapisane filtry) i wybierz filtr. Aby załadować filtr udostępniony przez innego użytkownika, kliknij  > Shared filters (Udostępnione filtry) i wybierz filtr.
	Aby zresetować filtr, kliknij  i Reset (Resetuj) .

Swobodne wyszukiwanie tekstowe

Funkcja swobodnego wyszukiwania tekstowego umożliwia opisanie treści szukanych w nagraniach przy użyciu języka naturalnego.

Uwaga

- Do obsługi swobodnego wyszukiwania tekstowego potrzeba co najmniej 16 GB pamięci RAM.
- Swobodne wyszukiwanie tekstowe wymaga połączenia z Internetem.
 - Funkcja swobodnego wyszukiwania tekstowego używa połączenia z internetem w celu pobrania modelu AI ze strony axis.com przy pierwszym konfigurowaniu oraz przy aktualizacji modelu przez Axis.

- Funkcja swobodnego wyszukiwania tekstowego raz w tygodniu łączy się z usługami Axis w chmurze, aby sprawdzić, czy modele AI wymagają uaktualnienia w celu zapewnienia zgodności z przyszłymi przepisami lub wymogami. Jeśli połączenie się nie powiedzie, nie będzie można korzystać ze swobodnego wyszukiwania tekstowego do czasu ponownego nawiązania połączenia przez system.
- W przypadku swobodnego wyszukiwania tekstowego całe przetwarzanie jest wykonywane lokalnie na serwerze i nie wykorzystuje połączenia internetowego w celu wysyłania jakichkolwiek materiałów wizyjnych, zdjęć czy tekstów zapytań.

Aby włączyć swobodne wyszukiwanie tekstowe:

1. Otwórz kartę **Configuration (Konfiguracja)**.
2. Wybierz kolejno **Smart search 2 (Inteligentne wyszukiwanie 2) > Settings (Ustawienia)**.
3. W sekcji **Free text search (Swobodne wyszukiwanie tekstowe)** wybierz **Use free text search (Użyj swobodnego wyszukiwania tekstowego)**. System pobierze wymagane pliki ze strony axis.com.

Aby wyszukać:

1. Otwórz kartę **Smart search 2 (Inteligentne wyszukiwanie 2)**.
2. Kliknij **Object characteristics (Charakterystyka obiektu)**.
3. Kliknij **Free text (Tekst swobodny)**.
4. Kliknij **Show (Pokaż)**, aby przeczytać informacje o przeznaczeniu, ograniczeniach i odpowiedzialnym użytkowaniu.
5. Określ, co ma zostać uwzględnione w wyszukiwaniu, a co z niego wykluczone.
6. Kliknij **Search (Wyszukaj)**.

Wskazówki dotyczące tworzenia zapytań

Zaleca się stosowanie następującej struktury zapytań:

{person, vehicle or other object} + {specific action or attributes of the person, vehicle, or object}

Opisz obiekt za pomocą kilku istotnych deskryptorów. Na przykład:

Zapytanie	Uwaga
Kobieta w czerwonym swetrze i czarnym kapeluszu	Jest niezłe
Kobieta w czerwieni	Nieco zbyt niejasne
Kobieta o wzroście około 156 cm, ubrana w ciemnoczerwony kardigan z żółtymi akcentami i inspirowany późnymi latami 80. czarny kapelusz przeciwsłoneczny z jasnobrązową obwódką	Zdecydowanie za dużo szczegółów

Opisz sytuację tak jak w rozmowie z osobą, która nie jest ekspertem w sprawach systemów dozorowych. Na przykład:

Zapytanie	Uwaga
Żółta furgonetka zaparkowana przy drzewie	Jest niezłe
Pojazd bez osób wewnątrz, numer rejestracyjny: CHY67F, rodzaj: pickup, kolor: żółty, lokalizacja: obok potężnej topoli.	Za bardzo przypomina raport policyjny

Dobre deskryptory, które mogą być poprawnie interpretowane w ramach swobodnego wyszukiwania tekstowego:

Deskryptor	Przykład
Klasa obiektu	Osoba, Samochód, Rower, Zwierzę
Kolor	Żółty
Pogoda	Słonecznie
Popularne marki (marki samochodów, logo)	Furgonetka UPS

Złe deskryptory:

Deskryptor	Przykład
Tekst	Szyld sklepowy z napisem „Tańczącym niedźwiedziom wstęp wzbroniony”
Określenie emocji	Mężczyzna wyglądający na rozczłuszczanego
Zliczanie	14 osób kręcących się po placu
Regionalizm	Czerwone laczki

Moderacja zapytań wyszukiwania

Wyszukiwania zawierające obraźliwe, krzywdzące lub obsceniczne treści można zablokować w celu zachowania bezpiecznego i godnego otoczenia. Nasz system wykorzystuje model przetwarzania języka naturalnego oraz własną listę niedozwolonych kategorii oraz słów wyszukiwania na potrzeby oceny każdego zapytania.

Jeżeli nie zgadzasz się z blokowaniem danego słowa lub chcesz polecić nowe, możesz przekazać anonimową opinię za pośrednictwem interfejsu użytkownika Inteligentnego wyszukiwania, która trafi do naszego zespołu w celu sprawdzenia.

Uwaga

- Swobodne wyszukiwanie tekstowe jest możliwe tylko w języku angielskim.
- Swobodne wyszukiwanie tekstowe jest obsługiwane w przypadku zdjęć. Uzyskanie dobrych wyników w przypadku czynności, na przykład upadku, biegu czy kradzieży może być trudne, ponieważ wymagają one więcej kontekstu.
- Do swobodnego wyszukiwania tekstowego wykorzystywane są przycięte obrazy i może w nich nie być uwzględniane otoczenie. W przypadku użycia deskryptorów sceny, takich jak miasto, park, ogród, jezioro czy plaża, możliwe są mniej dokładne wyniki.
- Więcej szczegółowych informacji o funkcji swobodnego wyszukiwania tekstowego, w tym o jej ograniczeniach i o najlepszych praktykach, znajduje się w naszej białej księdze *Free text search in AXIS Camera Station Pro*.

Wyniki inteligentnego wyszukiwania

	Aby grupować detekcje, które prawdopodobnie należą do tego samego zdarzenia, kategoryzuj je w przedziałach czasowych. Wybierz interwał z rozwijalnego menu .
Najpierw najpóźniejsze	Inteligentne wyszukiwanie 2 przedstawia 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 pozwala odfiltrować niepewne klasyfikacje.
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 drganiem 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. Nie można włączyć klasyfikacji serwerowej w tle dla radaru.
- W przypadku sieciowych kamer termowizyjnych działanie związane z klasyfikacją obiektów jest nieprzewidywalne.
- Inteligentne wyszukiwanie 2 nie wykrywa poruszających się obiektów w przypadku zmiany położenia zaprogramowanego PTZ oraz przez krótki okres po zmianach położenia.
- Ustawienia przekroczenia linii i filtry obszarów nie naśladują zmian pozycji PTZ.

Wyszukiwanie danych

Wyszukiwanie danych pozwala znajdować dane w źródle zewnętrznym. Źródło to system lub urządzenie, które wytwarza dane dotyczące zdarzeń. Więcej informacji p. *Zewnętrzne źródła danych, on page 74*.

Na przykład:

- 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 długość czasu przechowywania danych zewnętrznych przez AXIS Camera Station Pro, przejdź do **Configuration > Server > Settings > External data** (Konfiguracja > Serwer > Ustawienia > 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 **Search options (Opcje wyszukiwania)**  i zastosuj dodatkowe filtry. Dostępne filtry różnią się w zależności od rodzaju źródła danych.
5. Wpisz słowa kluczowe w polu wyszukiwania. Zob. *Optymalizowanie wyszukiwania, on page 45*.
6. Kliknij **Search (Wyszukaj)**.

Wyszukiwanie danych doda do zakładki 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	Użyj tej opcji, aby uwzględnić wyłącznie dane z tego komponentu. Kontrola dostępu umożliwia filtrowanie według drzwi i stref, posiadaczy kart oraz typów zdarzeń.
Third party (Inne)	Użyj tej opcji, aby dołączyć dane ze źródeł innych niż skonfigurowane komponenty.

W zależności od źródła danych w wynikach wyszukiwania mogą być wyświetlane różne elementy. Na przykład:

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. Przykład: Pojazd.

Aby wyeksportować wyniki wyszukiwania do pliku PDF lub tekstowego, kliknij **Download search result (Pobierz wyniki wyszukiwania)**. Możesz zmienić kolejność kolumn i dostosować ich szerokość, aby poprawić układ tabeli w wyjściowym pliku PDF. Plik PDF może zawierać do 10 kolumn.

Optymalizowanie wyszukiwania

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

Używaj cudzysłów " ", aby znaleźć dokładne dopasowania słów kluczowych	- Szukanie wyrażenia "door 1" spowoduje zwrócenie wyników zawierających tekst „drzwi 1”. - 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”. - 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”. - 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”

	- „drzwi 2” i „Drzwi wyważone” • Szukanie wyrażenia <code>door 1 AND (door (forced open OR open too long))</code> spowoduje zwrócenie wyników zawierających jeden z poniższych tekstów: - „drzwi 1” i „drzwi wyważone” - „drzwi 1” i „przekroczony czas otwarcia drzwi”
Używaj symboli <code>></code> , <code>>=</code> , <code><</code> lub <code><=</code> do filtrowania wartości liczbowych w konkretnych kolumnach.	• Szukanie wyrażenia <code>[Max speed] > 28</code> spowoduje zwrócenie wyników, które w kolumnie Szybkość maksymalna zawierają liczbę większą niż 28. • Szukanie wyrażenia <code>[Average speed] < = 28</code> spowoduje zwrócenie wyników, które w kolumnie Średnia szybkość zawierają liczbę nie większą niż 28.
Użyj operatora <code>CONTAINS</code> , aby wyszukać tekst w określonej kolumnie.	• Szukanie wyrażenia <code>[Cardholder] CONTAINS Oscar</code> spowoduje zwrócenie danych, w których „Oscar” występuje w kolumnie „Cardholder” (Posiadacz karty). • Szukanie wyrażenia <code>[Door] CONTAINS "door 1"</code> spowoduje zwrócenie danych, w których „drzwi 1” występują w kolumnie „Drzwi”.
Użyj operatora <code>=</code> w celu uzyskania dokładnych dopasowań w określonej kolumnie.	Szukanie wyrażenia <code>[CardholderId] = ABC123</code> spowoduje zwrócenie wyników pasujących do wartości „ABC123” w kolumnie „Cardholder” (Posiadacz karty).

Konfiguracja

Na karcie Configuration (Konfiguracja) można zarządzać dołączonymi urządzeniami oraz konfigurować ustawienia klienta i serwerów. Kliknij  i wybierz **Configuration** (Konfiguracja), aby otworzyć kartę Configuration (Konfiguracja).

Konfiguruj urządzenia

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

W środowisku AXIS Camera Station Pro urządzenie może być:

- Kamerą sieciową.
- Koderem wizyjnym z jednym lub kilkoma portami wizyjnymi.
- Urządzeniem dodatkowym niebędącym kamerą, na przykład urządzeniem we / wy audio, głośnikiem sieciowym lub kontrolerem drzwiowym.
- Domofonem.

Z tego miejsca jest możliwe:

- Dodawanie kamer i urządzeń bez funkcji wideo. Zob. *Dodawanie urządzeń*.
- Edytowanie preferencji podłączonych kamer. Zob. *Kamery*.
- Edytowanie preferencji urządzeń innych niż kamery. Zob. *Inne urządzenia*.
- Edytowanie profili strumieniowania pod kątem rozdzielczości, standardu i innych parametrów. Zob. *Profile strumieniowania*.
- Dostosowywanie ustawień obrazu w czasie rzeczywistym. Zob. *Konfiguracja obrazu*.
- Dodawanie i usuwanie prepozycji PTZ. Zob. *Położenia zaprogramowane PTZ*.
- Zarządzaj i konfiguruj podłączone urządzenia. Zob. *Zarządzanie urządzeniami*.
- Zarządzanie zewnętrznymi źródłami danych. Zob. *Zewnętrzne źródła danych, on page 74*.

Dodawanie urządzeń

Uwaga

- System traktuje obszary obserwacji jak pojedyncze kamery. Aby móc używać obszarów obserwacji w kamerze, należy je najpierw utworzyć. Zob. *Używanie obszarów obserwacji*.
 - Po dodaniu urządzenia synchronizuje ono czas z serwerem AXIS Camera Station Pro.
 - Najlepiej nie używać w nazwie hosta urządzenia znaków specjalnych, takich jak å, ä czy ö.
1. Znajdź urządzenia, strumienie wizyjne lub wstępnie zapisane nagrania.
 - *Znajdowanie urządzeń, on page 49*
 - *Znajdowanie strumieni wideo, on page 49*
 - *Znajdowanie wstępnie nagranych filmów, on page 50*
 2. *Dodawanie urządzeń, strumieni wideo lub wstępnie nagranych filmów, on page 50*

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

(puste)	Jeżeli nie ma pokazanego statusu, można dodać urządzenie do AXIS Camera Station Pro.
Communicating (Łączenie)	Serwer AXIS Camera Station Pro próbuje uzyskać dostęp do urządzenia.
Device certificate not trusted (Niezaufany certyfikat urządzenia)	AXIS Camera Station Pro nie może zweryfikować, czy certyfikat HTTPS w urządzeniu został podpisany przez zaufanego wystawcę. Kliknij łącze, aby wystawić nowy certyfikat HTTPS lub poinformować stronę AXIS Camera Station Pro, aby zaufała istniejącemu certyfikatowi.
Organ wydający certyfikat wygaś	Urząd certyfikacji, który wystawił certyfikat urządzenia, nie jest już ważny. Kliknij łącze, aby wystawić nowy certyfikat HTTPS lub poinformować stronę AXIS Camera Station Pro, 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 Pro, aby zaufała istniejącemu certyfikatowi.
Communication error (Błąd komunikacji)	AXIS Camera Station Pro nie może skontaktować się z urządzeniem.
Wprowadź hasło	AXIS Camera Station Pro nie wie, których uwierzytelnień użyć w celu uzyskania dostępu do urządzenia. Kliknij łącze, aby wprowadzić nazwę użytkownika i hasło konta administratora na urządzeniu. AXIS Camera Station Pro 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. - Wpisz hasło lub kliknij Generate (Generuj), aby uzyskać hasło. Zaleca się zapisanie kopii wygenerowanego hasła. - Zaznacz tę opcję, aby używać tego hasła we wszystkich urządzeniach o statusie Set password (Ustaw hasło). - Jeżeli urządzenie stosuje zasady dotyczące haseł, wskaźnik zgodności z zasadami haseł wskaże, czy hasło spełnia wymagania. Więcej informacji, p. sekcja <i>Zarządzanie użytkownikami, on page 67</i>.
Model not supported (Model nie jest obsługiwany)	AXIS Camera Station Pro nie obsługuje modelu urządzenia.
Obsolete firmware (Przestarzałe oprogramowanie sprzętowe)	Oprogramowanie układowe urządzenia jest nieaktualne. Zaktualizuj je przed dodaniem urządzenia.

Urządzenie niesprawne	Parametry urządzenia pobrane przez AXIS Camera Station Pro 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 modelach kamer konieczne jest ustawienie orientacji pochylenia.
Nieobsługiwane urządzenie ONVIF	AXIS Camera Station Pro nie obsługuje tego urządzenia innego producenta.
Nieobsługiwane urządzenie	AXIS Camera Station Pro nie obsługuje tego rodzaju urządzeń.

Uwaga

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

Znajdowanie urządzeń

Aby znaleźć urządzenia, których nie ma na liście:

- Wybierz kolejno opcje **Configuration > Devices > Add devices** (Konfiguracja > Urządzenia > Dodaj urządzenia).
- Kliknij przycisk **Cancel (Anuluj)**, aby przerwać trwające przeszukiwanie sieci.
- Kliknij przycisk **Wyszukiwanie ręczne**.
- Aby znaleźć wiele urządzeń należących do jednego lub kilku zakresów adresów IP:
 - Zaznacz opcję **Przeszukaj co najmniej jeden zakres adresów IP**.
 - Wpisz zakres adresów IP. 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.
 - Aby zmienić domyślny port 80, wprowadź zakres portów. Na przykład: 80, 1080-1090
 - Użyj myślnika, aby określić zakres portów.
 - Do oddzielania zakresów używaj przecinka.
 - Kliknij **Search (Wyszukaj)**.
- Aby znaleźć jedno lub więcej konkretnych urządzeń:
 - Zaznacz opcję **Wprowadź jedną lub więcej nazw hostów lub adresów IP**.
 - Wprowadź nazwy hostów lub adresy IP, oddzielając je przecinkami.
 - Kliknij **Search (Wyszukaj)**.
- Kliknij **OK**.

Znajdowanie strumieni wideo

Można dodawać strumienie wizyjne 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 wizyjne w standardzie .mkv można dodać do AXIS Camera Station Pro.

Wymagania:

- 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 nagranych wideo, dodaj do folderu plik .dewarp o takiej samej nazwie, jak plik .mkv. Więcej informacji p. *Konfiguracja obrazu, on page 59*.
 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. Wybierz urządzenia, strumienie wideo lub wstępnie nagrane filmy. Kliknij **Dodaj**.
4. Kliknij **Close (Zamknij)**, aby pominąć konfigurację i kontynuować później. Aby kontynuować konfigurację:
 - 4.1. Wybierz opcję **Quick configuration (Szybka konfiguracja)**, aby skonfigurować podstawowe ustawienia. Jeżeli importujesz projekt AXIS Site Designer, wybierz opcję **Site Designer configuration (Konfiguracja Site Designer)**. Więcej informacji p. *Importowanie projektów AXIS Site Designer*.
 - 4.2. Wybierz **Add image overlay for date, time, and text (Dodaj nakładkę obrazu z datą, godziną i tekstem)**, aby dodać nakładki do kamer Axis, które jeszcze ich nie mają.
 - 4.3. Kliknij **Next (Dalej)**.
 - 4.4. Wybierz preferowane ustawienie **Recording method (Metoda nagrywania)**.
 - 4.5. Kliknij **Next (Dalej)**.
 - 4.6. Wybierz **Retention time (Czas przechowywania)** oraz **Recording storage (Pamięć masowa nagrań)**, a następnie kliknij **Finish (Zakończ)**, aby zastosować konfigurację.

Importowanie projektów AXIS 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 Pro. Dostęp do projektu można uzyskać za pomocą kodu dostępu lub pobranego pliku konfiguracyjnego.

Aby zaimportować projekt z aplikacji AXIS Site Designer do AXIS Camera Station Pro:

1. Wygeneruj kod dostępu lub pobierz plik projektu:
 - 1.1. Zaloguj się na stronie <http://sitedesigner.axis.com> przy użyciu swojego konta My Axis.
 - 1.2. Zaznacz projekt i przejdź do strony projektu.
 - 1.3. Kliknij przycisk **Share (Udostępnij)**.
 - 1.4. Kliknij **Generate code** (Wygeneruj kod), jeżeli serwer AXIS Camera Station Pro ma połączenie z internetem, albo kliknij **Download settings file** (Pobierz plik ustawień) przy braku połączenia.
2. W kliencie AXIS Camera Station Pro wybierz kolejno **Configuration (Konfiguracja) > Devices (Urządzenia) > Add devices (Dodaj urządzenia)**.
3. Zaznacz urządzenia i kliknij **Add (Dodaj)**.
4. Zaznacz pozycję **Konfiguracja aplikacji Site Designer** i kliknij przycisk **Dalej**.
5. Zaznacz opcję **Access code (Kod dostępu)** i wprowadź kod dostępu. Aby zamiast tego użyć pobranego pliku instalacyjnego, wybierz **Choose file (Wybierz plik)**.
6. Kliknij **Import (Importuj)**. Program AXIS Camera Station Pro próbuje dopasować projekt do wybranych urządzeń według adresu IP lub nazwy produktu. Jeżeli dopasowanie nie powiedzie się, wybierz prawidłowe urządzenia z menu rozwijalnego.
7. Kliknij **Next (Dalej)**.
8. Wybierz preferowane ustawienie **Recording method (Metoda nagrywania)**. Te ustawienia dotyczą kamer, które nie są zgodne z konfiguracją projektową.
9. Kliknij **Next (Dalej)**.
10. Wybierz **Retention time** (Czas przechowywania) oraz **Recording storage** (Pamięć masowa nagrań), a następnie kliknij **Finish (Zakończ)**, aby zastosować konfigurację.

AXIS Camera Station Pro importuje następujące ustawienia z projektu AXIS 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 ciągłe: harmonogram i profil nagrywania, w tym poklatkowość, rozdzielczość, kodowanie wideo i kompresja		✓
Nagrywanie wyzwalane ruchem: harmonogram i profil nagrywania,		✓

	Enkodery, dekodery drzwi, kontrolery drzwi, detektory radarowe i głośniki:	Kamery, interkomy i urządzenia z serii F/FA
w tym poklatkowość, rozdzielczość, kodowanie wideo i kompresja		
Siła technologii Zipstream		✓
Ustawienia dźwięku w podglądzie na żywo i nagraniach		✓
Czas przechowywania nagrań		✓

Uwaga

- Jeżeli zdefiniowano jeden profil zapisu lub jeżeli w projekcie z aplikacji AXIS Site Designer istnieją dwa identyczne profile zapisu, AXIS Camera Station Pro ustawia profil na poziom średni.
- Jeżeli w projekcie z aplikacji AXIS Site Designer zdefiniowano oba profile zapisu, AXIS Camera Station Pro ustawi profil zapisu ciągłego jako średni, a zapis wyzwalany ruchem na poziom wysoki.
- AXIS Camera Station Pro optymalizuje współczynnik proporcji, zatem rozdzielczość może różnić się od tej z projektu z aplikacji AXIS Site Designer.
- AXIS Camera Station Pro może skonfigurować ustawienia dźwięku, jeżeli urządzenie ma wbudowany mikrofon lub głośnik. Aby skorzystać z zewnętrznego urządzenia fonicznego, włącz je po zakończeniu instalacji.
- AXIS Camera Station Pro nie stosuje ustawień dźwięku do domofonów, nawet jeżeli ustawienia w aplikacji AXIS Site Designer różnią się. W domofonach dźwięk jest zawsze włączony, ale tylko w trybie podglądu na żywo.



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

Dodawanie urządzeń innych producentów

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

Uwaga

Urządzenia innych firm można też dodawać do AXIS Camera Station Pro jako strumień wideo. Zob. *Znajdowanie strumieni wideo, on page 49*.

AXIS Camera Station Pro obsługuje następujące funkcje w urządzeniach innych producentów zgodnie z normami IEC 62676-2-31 i IEC 62676-2-32:

- Wykrywanie kamer
- Kodowanie wideo: M-JPEG, H.264
- Kodowanie dźwięku: G.711 (jednokierunkowe, z urządzenia do AXIS Camera Station Pro)
- Jeden profil wideo na kamerę
- Podgląd na żywo
- Zapis ciągły i uruchamiany ręcznie
- Odtwarzanie

- Eksportowanie nagrań
- Wyzwalacze oparte na zdarzeniach w urządzeniach
- Obrót/pochylenie/zbliżenie

Używanie obszarów obserwacji

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

Uwaga

- Wszystkie widoki w kamerze sieciowej są traktowane jako jedna kamera z perspektywy obliczeń łącznej liczby kamer dozwolonych w ramach licencji AXIS Camera Station Pro.
- Liczba kamer, które można dodać, zależy od posiadanej licencji.

Aby korzystać z widoków w AXIS Camera Station Pro, musisz je najpierw 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 **Help (Pomoc)**, aby uzyskać instrukcje dotyczące odnalezienia tego ustawienia. Lokalizacja różni się w zależności od modelu kamery i wersji oprogramowania układowego.

Wymiana urządzenia

Możesz wymienić urządzenie, zachowując istniejącą konfigurację i nagrania. Liczba skonfigurowanych strumieni wizyjnych w nowej kamerze musi być taka sama jak w starej.

Aby wymienić urządzenie:

1. Jeśli wymieniane urządzenie korzysta z pamięci masowej w chmurze, przejdź do obszaru **Cloud storage (Pamięć masowa w chmurze)** na platformie My Systems i wyłącz dla urządzenia pamięć masową w chmurze.
2. Otwórz kartę **Configuration (Konfiguracja)** i wybierz kolejno opcje **Devices (Urządzenia) > Management (Zarządzanie)**.
3. Wybierz urządzenie, które chcesz wymienić, i kliknij .
4. W oknie dialogowym **Replace device (Zastąp urządzenie)** wybierz urządzenie, którym chcesz zastąpić stary sprzęt.
5. Kliknij przycisk **Finish (Zakończ)**.
6. Zostanie wyświetlone okno dialogowe **Replaced device (Zastąpione urządzenie)** w celu potwierdzenia, że urządzenie zostało pomyślnie wymienione. Kliknij **OK**.
7. Jeżeli wymienione urządzenie korzystało z pamięci masowej w chmurze, uruchom ponownie usługę na serwerze AXIS Camera Station Pro. Następnie na platformie My Systems włącz pamięć masową w chmurze dla tego urządzenia. Zobacz *Włączanie pamięci masowej w chmurze dla poszczególnych kamer*.
8. Sprawdź konfigurację nowego urządzenia, aby upewnić się, że ustawienia są prawidłowe i że działa ono prawidłowo. W razie potrzeby:
 - 8.1. Skonfiguruj ponownie prepozycje PTZ w urządzeniu.
 - 8.2. Dodaj ewentualne usunięte porty WE/WY i zaktualizuj powiązane reguły akcji.
 - 8.3. Skonfiguruj ponownie ustawienia ruchu, jeśli stara kamera używała wbudowanej wizyjnej detekcji ruchu, a nie aplikacji ACAP do detekcji ruchu.

- 8.4. Włóż kartę SD lub wyłącz zapis awaryjny w ustawieniach wyboru pamięci masowej, jeśli stara kamera korzystała z zapisu awaryjnego.

Kamery

Przejdź do **Configuration > Devices > Cameras** (Konfiguracja > Urządzenia > Kamery), aby zobaczyć listę wszystkich kamer dodanych do systemu.

Na tej stronie można:

- Otwórz interfejs internetowy kamery, klikając jej adres. Wymaga to braku NAT lub zapory między klientem AXIS Camera Station Pro a urządzeniem.
- Edycja ustawień kamery. Zob. *Edycja ustawień kamery*.
- Usuwanie kamer. Powoduje również usunięcie wszystkich nagrań powiązanych z usuniętymi kamerami, także z kamerami zablokowanymi.

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)**.

Włączony	Aby zablokować zapis i oglądanie strumienia wizyjnego, usuń zaznaczenie opcji Enabled (Włączone). Nadal można skonfigurować nagrania i podgląd na żywo.
Kanał	Jeżeli pole Channel (Kanał) jest dostępne dla wieloportowych wideoenkoderów, wybierz numer portu. Jeżeli pole Channel (Kanał) jest dostępne dla obszarów obserwacji, wybierz liczbę odpowiadającą obszarowi obserwacji.

Inne urządzenia

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

Więcej informacji o obsługiwanych produktach, p. strona www.axis.com. Zob. *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 Pro a urządzeniem.
- Edytować ustawienia urządzenia, takie jak nazwa urządzenia, adres i hasło.
- Usunąć urządzenie.

Edytowanie ustawień innych urządzeń

Aby zmienić nazwę urządzenia innego niż kamera:

1. Wybierz kolejno opcje **Configuration > Devices > Other devices** (Konfiguracja > Urządzenia > Inne urządzenia).

2. Zaznacz urządzenie i kliknij przycisk **Edit (Edytuj)**.
3. Wprowadź nową nazwę urządzenia.

Profile strumieniowania

Profil strumienia to grupa ustawień wpływających na strumień wideo, takich jak rozdzielczość, format wideo, liczba klatek na sekundę i kompresja. Przejdź do **Configuration > Devices > Stream profiles** (Konfiguracja > Urządzenia > Profile strumieni), a zostanie otwarta strona **Stream profiles** (Profile strumieniowania). Na stronie przedstawiona zostanie 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

W trybie podglądu na żywo i w nagraniach profil strumieniowania jest domyślnie ustawiony na **Automatic** (Automatyczny). Profil strumieniowania zmienia się automatycznie na **High** (Wysoki), **Medium** (Średni) lub **Low** (Niski) w zależności od możliwej przepustowości strumienia wizyjnego.

Profile strumieniowania w kamerze

Program AXIS Camera Station Pro automatycznie dodaje profile strumieniowania do kamery, upraszczając konfigurowanie reguł zapisu bezpośrednio w urządzeniu. Profile są wyświetlane w interfejsie internetowym kamery w części **Stream profiles** (Profile strumieniowania) i mają nazwy składające się z nazwy kamery oraz poziomu profilu, na przykład „Kamera 1_ACS_Pro_High”.

Profile w kamerze są dodawane lub aktualizowane, gdy:

- Do AXIS Camera Station Pro dodano kamerę.
- Profile strumieniowania zmieniono w AXIS Camera Station Pro.
- Trwa nocne odświeżanie.

Po usunięciu kamery z programu AXIS Camera Station Pro profile strumieniowania utworzone przez AXIS Camera Station Pro są usuwane z kamery.

Uwaga

Profile strumieniowania w standardach M-JPEG lub MPEG-4 nie są dodawane do kamery.

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. Dostępne tylko dla urządzeń innych producentów. - Konfiguracji wideoenkodera można używać tylko dla jednego profilu wideo. - 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 i mniej miejsca w pamięci masowej niż standard M-JPEG. Niektóre kamery obsługują również standard H.265 , który zapewnia nieco lepszą kompresję, ale wymaga większej mocy obliczeniowej. Nasze kamery najnowszej generacji obsługują standard AV1 zapewniający dobrą kompresję oraz szereg nowych funkcji, takich jak przełączane nakładanie. Więcej informacji o standardzie AV1 znajduje się na <i>stronie produktów w standardzie AV1</i> . Aby sprawdzić, czy kamera obsługuje standard AV1, p. <i>strona kompatybilnych kamer</i> .
Liczba klatek na sekundę	Rzeczywista częstotliwość odświeżania zależy od modelu kamery, warunków sieciowych 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 dźwięku 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.
		Niezwykłe 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). Ten profil wykorzystuje bardziej zaawansowane narzędzia do kompresji, aby zmniejszyć wykorzystanie pamięci masowej poza domyślnym ustawieniem Zipstream i może dodatkowo zmniejszyć przepływność – nawet w przypadku scen z intensywnym ruchem. • Standard asf nie obsługuje ramek typu B używanych przez tę funkcję. • Ta funkcja nie ma wpływu na nagrania wizyjne w rejestratorach serii AXIS S30. • Ta funkcja wymaga oprogramowania układowego AXIS OS w wersji 11.7.59 lub nowszej.		

Mikrofon:	W celu powiązania mikrofonu z kamerą zaznacz opcję Built-in microphone or line in (Wbudowany mikrofon lub wejście liniowe) albo mikrofon innego urządzenia. Zob. <i>Używanie dźwięku z innych urządzeń</i> .
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. Zob. <i>Używanie dźwięku z innych urządzeń</i> .
Use microphone for: (Użyj mikrofonu przy)	Włącz transmisję dźwięku z mikrofonu dla jednego lub dwóch strumieni. Funkcję można włączyć dla podglądu na żywo i nagrań, tylko dla podglądu na żywo lub tylko dla nagrań.

Po połączeniu z programem AXIS Audio Manager Pro można również wybrać urządzenia foniczne z serwera AXIS Audio Manager Pro jako urządzenia foniczne powiązane z kamerą. Więcej informacji znajduje się w sekcji *Konfiguracja programu AXIS Audio Manager Pro, on page 175*.

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) . Dostępna jest tylko dla urządzeń Axis obsługujących dane analityczne. Gromadzenie danych dla funkcji <i>Inteligentne wyszukiwanie 1</i> może powodować opóźnienia w strumieniowej transmisji podglądu na żywo.
Użyj FFmpeg	Aby zwiększyć kompatybilność z urządzeniami innych producentów, zaznacz opcję Use FFmpeg (Użyj FFmpeg) , co spowoduje włączenie strumieniowania w standardzie FFmpeg. Dostępne tylko dla urządzeń innych producentów.

Pokaż wskaźniki PTZ automatycznego śledzenia obiektów	Aby wskaźniki obiektów wykrywanych przez kamerę PTZ były wyświetlane w podglądzie na żywo, zaznacz opcję Show PTZ autotracking object indicators (Pokaż wskaźniki PTZ automatycznego śledzenia obiektów) oraz ustaw czas buforowania strumienia wizyjnego na maks. 2000 ms. Dostępne tylko dla kamer PTZ Axis z funkcją automatycznego śledzenia PTZ. Opis całej procedury konfigurowania funkcji AXIS PTZ Autotracking w aplikacji AXIS Camera Station Pro znajduje się w temacie <i>Konfigurowanie funkcji AXIS PTZ Autotracking</i>.
Dostosowywanie strumienia	Aby dostosować ustawienia transmisji strumieniowej dla określonego profilu, wprowadź ustawienia oddzielone znakami & dla profilu. Na przykład, wpisz <code>overlays=off&color=0</code>, aby ukrywać nałożenia w tej kamerze. Ustawienia niestandardowe zastępują wszelkie istniejące ustawienia. W ustawieniach niestandardowych nie podawaj żadnych poufnych informacji.

Aby dostosować ustawienia profilu dotyczące rozdzielczości, częstotliwości odświeżania, kompresji, standardu obrazu i dźwięku, wybierz kamerę, którą chcesz skonfigurować. W przypadku kamer o takiej samej nazwie modelowej z identycznymi możliwościami konfiguracji można konfigurować wiele kamer naraz. Zob. *Ustawienia konfiguracyjne*.

Aby dostosować ustawienia profilu dla nagrań, zob. *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 Pro a serwerem AXIS Camera Station Pro. Zob. sekcję Wykorzystanie pasma w temacie *Przesyłanie strumieniowe*.

Używanie dźwięku z innych urządzeń

Dźwięk z urządzeń niebędących kamerami (dodatkowych) można łączyć z obrazem z kamery sieciowej lub kodera wizyjnego na potrzeby podglądu na żywo lub zapisu.

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

W *samouczkach wideo do aplikacji AXIS Camera Station Pro* 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 Pro.

Konfiguracja obrazu

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

Uwaga

Zmiany w konfiguracji obrazu stosowane są natychmiastowo.

Aby skonfigurować ustawienia obrazu:

1. Przejdź do **Configuration > Devices > Image configuration** (Konfiguracja > Urządzenia > Konfiguracja obrazu). AXIS Camera Station Pro wyświetli listę wszystkich kamer.
2. Wybierz kamerę, aby wyświetlić obraz pod listą w czasie rzeczywistym. Za pomocą pola **Wpisz, aby wyszukać** odszukaj konkretną kamerę spośród figurujących na liście.
3. Skonfiguruj ustawienia obrazu:

Brightness – 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.

Równoważenie bieli – Wybierz opcję balansu bieli z listy rozwijanej. Równoważenie bieli służy do zapewnienia spójnego wyglądu kolorów na zdjęciu niezależnie od temperatury barwowej źródła światła w scenie. Po wybraniu opcji **Automatycznie** lub **Auto** kamera będzie identyfikować źródło światła i automatycznie kompensować barwy względem jego koloru. W razie niezadowolającego 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.

Kompensacja tła – Włącz, jeżeli jasne źródło światła, takie jak żarówka, sprawia, że inne obszary obrazu wydają się zbyt ciemne.

Kontrast dynamiczny (szeroki zakres dynamiki) – Włącz, aby poprawić ekspozycję w przypadku znacznego kontrastu pomiędzy jasnymi i ciemnymi obszarami na obrazie. Użyj suwaka, aby dostosować poziom. Wyłącz w warunkach złego oświetlenia.

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.

Aby skonfigurować niestandardowe ustawienia korekcji zniekształceń:

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
```

Położenia zaprogramowane PTZ

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

Przejdź do **Configuration > Devices > PTZ presets** (Konfiguracja > Urządzenia > Położenia zaprogramowane PTZ). AXIS Camera Station Pro wyświetla listę kamer obsługujących funkcję 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
- Kamery stałopozycyjne z funkcją cyfrowego PTZ.
- Kamery zgodne ze standardem ONVIF obsługujące położenia zaprogramowane PTZ.

Funkcję cyfrowego PTZ można włączyć z wbudowanej strony 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 **Address (Adres)**.

Położenia zaprogramowane PTZ można konfigurować w programie AXIS Camera Station Pro i na stronie konfiguracyjnej kamery. Zaleca się konfigurować położenia zaprogramowane PTZ w programie AXIS Camera Station Pro.

- 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 są widoczne i zapisywane.
- W przypadku skonfigurowania prepozycji PTZ w aplikacji AXIS Camera Station Pro można oglądać cały strumień nadawany z kamery. Ruchy kamery PTZ w podglądzie na żywo nie są widoczne ani zapisywane.

Uwaga

Nie można korzystać z funkcji PTZ, gdy włączona jest sekwencja sterowania kamerą. Informacje o sekwencji sterowania oraz sposobie jej włączania i wyłączania znajdują się w instrukcji obsługi 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 **OK**.
- Aby usunąć położenie zaprogramowane, zaznacz je i kliknij przycisk **Remove (Usuń)**. Spowoduje to usunięcie położenia zaprogramowanego z programu AXIS Camera Station Pro i z kamery.

Zarządzanie urządzeniami

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

Przejdź do **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie), a zostanie otwarta strona **Manage Devices** (Zarządzaj urządzeniami).

Jeżeli w sekcji *Ustawienia aktualizacji oprogramowania sprzętowego, on page 126* skonfigurowano automatyczne sprawdzanie dostępności nowych wersji oprogramowania układowego, pojawienie się aktualizacji oprogramowania układowego spowoduje wyświetlenie odpowiedniego łącza. Kliknięcie łącza rozpocznie proces uaktualniania oprogramowania sprzętowego. Zob. *Aktualizuj oprogramowanie sprzętowe*.

Jeżeli w sekcji *Aktualizuj AXIS Camera Station Pro, on page 131* skonfigurowano automatyczne sprawdzanie dostępności nowych wersji oprogramowania, pojawienie się nowej wersji programu AXIS Camera Station Pro spowoduje wyświetlenie łącza. Kliknij to łącze, aby zainstalować nową wersję.

Program AXIS Camera Station Pro wyświetla listę wszystkich dodanych urządzeń. 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:

- **Name (Nazwa):** Nazwa urządzenia lub lista wszystkich nazw powiązanych kamer, jeżeli urządzenie jest koderem wizyjnym z wieloma dołączonymi kamerami lub kamerą sieciową z wieloma zdefiniowanymi widokami.
- **MAC address (Adres MAC):** Adres MAC urządzenia.
- **Status:** Status urządzenia.
 - **OK:** Standardowy stan ustanowionego połączenia z urządzeniem.
 - **Maintenance (Konservacja):** Urządzenie jest obecnie w trakcie procesu konserwacji i tymczasowo niedostępne.
 - **Not accessible (Niedostępne):** Nie można nawiązać połączenia z urządzeniem.
 - **Not accessible over set hostname (Niedostępne pod ustawioną nazwą hosta):** Nie można nawiązać połączenia z urządzeniem za pomocą jego nazwy hosta.
 - **Server not accessible (Serwer niedostępny):** Nie można nawiązać połączenia z serwerem, do którego jest dołączone urządzenie.
 - **Enter password (Wprowadź hasło):** Dostęp do urządzenia będzie niemożliwy do czasu podania prawidłowych uwierzytelnień. Należy kliknąć łącze i wpisać prawidłowe poświadczenia. Jeżeli urządzenie obsługuje połączenia szyfrowane, domyślnie hasło zostanie wysłane w postaci zaszyfrowanej.
 - **Set password (Ustaw hasło):** Konto i hasło użytkownika głównego nie zostały skonfigurowane lub urządzenie nadal korzysta z domyślnego hasła. Kliknij łącze, aby ustawić hasło użytkownika głównego.
 - Wprowadź hasło lub kliknij przycisk **Generate** (Wygeneruj), aby automatycznie wygenerować hasło o maksymalnej długości dozwolonej przez urządzenie. Zaleca się zapisanie wygenerowanego hasła.
 - Zaznacz opcję używania tego hasła na wszystkich urządzeniach mających status **Set password** (Ustaw hasło).
 - Zaznacz **Enable HTTPS** (Włącz HTTPS), aby włączyć protokół HTTPS, jeżeli urządzenie go obsługuje.
 - **Password type: unencrypted (Rodzaj hasła: niezaszyfrowane):** Nie można nawiązać połączenia z urządzeniem, ponieważ wcześniej łączono się z nim przy użyciu zaszyfrowanego hasła. Ze względów bezpieczeństwa AXIS Camera Station Pro 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.
 - **Certificate error (Błąd certyfikatu):** Wystąpił błąd z certyfikatem w urządzeniu.
 - **Certificate about to expire** (Certyfikat wkrótce wygaśnie): Certyfikat zainstalowany w urządzeniu wkrótce straci ważność.
 - **Certificate has expired** (Certyfikat wygaś): Certyfikat w urządzeniu stracił ważność.
 - **HTTPS certificate not trusted** (Niezaufany certyfikat HTTPS): AXIS Camera Station Pro nie uznaje certyfikatu HTTPS zainstalowanego w urządzeniu za zaufany. Kliknij łącze, aby wystawić nowy certyfikat HTTPS.
 - **HTTP failed** (Niepowodzenie HTTP): Nie można nawiązać połączenia z urządzeniem przy użyciu protokołu HTTP.
 - **HTTPS failed** (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).

- **Address (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. Zob. *Karta Konfiguracja urządzenia, on page 73*.
- **Hostname (Nazwa hosta):** Nazwa hosta urządzenia, jeżeli jest dostępna. Kliknięcie łącza spowoduje przejście do strony konfiguracji urządzenia. Wyświetlana nazwa hosta jest w pełni kwalifikowaną nazwą domeny. Zob. *Karta Konfiguracja urządzenia, on page 73*.
- **Manufacturer (Producent):** Producent urządzenia.
- **Model:** Model urządzenia.
- **Firmware (Oprogramowanie układowe):** Wersja oprogramowania układowego aktualnie zainstalowanego w urządzeniu.
- **DHCP:** Wskazuje, czy 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 71*.
- **IEEE 802.1X:** Status łączności przez IEEE 802.1X w urządzeniu. Stan IEEE 802.1X można sprawdzić na stronie *Bezpieczeństwo, on page 71*.
- **Server (Serwer):** Serwer AXIS Camera Station Pro, 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. Zob. *Przypisywanie adresu IP*.
- Ustawianie haseł dostępu do urządzeń. Zob. *Zarządzanie użytkownikami*.
- Uaktualnianie oprogramowania sprzętowego urządzeń. Zob. *Aktualizuj oprogramowanie sprzętowe*.
- Uruchom ponownie urządzenie.
- Przywracanie ustawień fabrycznych urządzeń: resetuje większość ustawień do wartości domyślnych, w tym hasło. Nie są resetowane następujące ustawienia: wczytane aplikacje do kamer, protokół uruchamiania (DHCP lub statyczny), statyczny adres IP, domyślny ruter, maska podsieci i czas systemowy.

Uwaga

- Aby zapobiec nieuprawnionemu dostępowi, po przywróceniu urządzenia zawsze ustawiaj nowe hasło.
- 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 Pro i 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. Zob. *Instalowanie aplikacji do kamery*.
- Po zmianie ustawień na stronie konfiguracyjnej urządzenia odśwież ustawienia urządzeń.
- Konfiguruj urządzenia. Zob. *Konfiguruj urządzenia*.
- Zarządzanie użytkownikami. Zob. *Zarządzanie użytkownikami*.
- Zarządzaj certyfikatami. Zob. *Bezpieczeństwo, on page 71*.
- Zbieranie danych dotyczących urządzeń. Zob. *Zbieranie danych dotyczących urządzeń*.
- Wybór między używaniem adresu IP lub nazwy hosta. Zob. *Połączenie, on page 72*.
- Oznaczanie urządzeń. Zob. *Znaczniki*.
- Wprowadź dane uwierzytelniające urządzenia. Kliknij prawym przyciskiem myszy i przejdź do **Advanced > Enter device credentials** (Zaawansowane > Wprowadź dane uwierzytelniające urządzenia) i wprowadź hasło dostępu do urządzenia.

- Przejdź do karty konfiguracji urządzenia i skonfiguruj urządzenie. Zob. *Karta Konfiguracja urządzenia, on page 73*.

Przypisywanie adresu IP

AXIS Camera Station Pro może przydzielać adresy IP do wielu urządzeń. Możesz automatycznie uzyskać nowe adresy IP z serwera DHCP lub przydzielać je 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 **Advanced (Zaawansowane)**, co spowoduje otwarcie strony **Assign IP address (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 Pro.

7. Kliknij **Next (Dalej)**.
8. Obejrzyj obecne i nowe adresy IP. Aby zmienić adres IP urządzenia, zaznacz urządzenie i kliknij przycisk **Edytuj adres IP**.
 - W sekcji **Current IP address (Aktualny adres IP)** wyświetlane są aktualny adres IP, maska podsieci oraz domyślny ruter.
 - Zmodyfikuj wartości w sekcji **New IP address (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. Zob. *Karta Konfiguracja urządzenia, on page 73*.

- Więcej informacji o konfigurowaniu urządzeń, p. sekcja *Metody konfigurowania*.
- Więcej informacji o tworzeniu pliku konfiguracyjnego, p. sekcja *Utwórz plik konfiguracyjny*.

- Więcej informacji o ustawieniach, które można kopiować, p. sekcja *Ustawienia konfiguracyjne*.

Metody konfigurowania

Istnieją różne metody konfigurowania urządzeń. Aplikacja AXIS Device Manager konfiguruje wszystkie urządzenia odpowiednio do ustawień objętych każdą metodą. Zob. *Konfiguruj urządzenia*.

Używanie konfiguracji wybranego urządzenia

Uwaga

Ta metoda jest dostępna wyłącznie dla jednego urządzenia i polega na ponownym wykorzystaniu niektórych lub wszystkich jego obecnych ustawień.

1. Przejdź do menu **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
2. Kliknij jedno urządzenie prawym przyciskiem myszy i wybierz **Configure Devices > Configure** (Konfiguruj urządzenia > Konfiguruj).
3. Zaznacz ustawienia, które chcesz zastosować. Zob. *Ustawienia konfiguracyjne, on page 66*.
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 **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. Zob. *Ustawienia konfiguracyjne, on page 66*.
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 modelach i wersjach oprogramowania układowego, nawet jeżeli niektóre ustawienia nie występują we wszystkich urządzeniach.

Jeżeli niektóre ustawienia nie istnieją lub nie można ich zastosować, status zadania wyświetla się jako **Error** (Błąd) na karcie **Tasks** (Zadania) u dołu okna klienta AXIS Camera Station Pro. Kliknij zadanie prawym przyciskiem myszy i wybierz polecenie **Show** (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 **Configure Devices > Configure** (Konfiguruj urządzenia > Konfiguruj).
3. Kliknij przycisk **Plik konfiguracyjny**, aby przejść do pliku konfiguracyjnego. Informacje o tworzeniu pliku konfiguracyjnego, p. sekcja *Utwórz plik konfiguracyjny, on page 66*.
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. Następnie możesz zastosować te ustawienia w innych urządzeniach. Aby dowiedzieć się więcej o używaniu pliku konfiguracyjnego, p. sekcja *Metody konfigurowania*.

Przedstawione ustawienia są ustawieniami urządzenia dostępnymi za pośrednictwem aplikacji AXIS Device Management. 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. Zob. *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 ustawienia, które sterują działaniem urządzenia. Ogólne informacje o parametrach znajdują się w instrukcji obsługi urządzenia na stronie www.axis.com.

Uwaga

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

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

- **Insert device serial number variable** (Wstaw numer seryjny urządzenia): Ta zmienna zostanie zastąpiona numerem seryjnym urządzenia, do którego zastosowano plik konfiguracyjny.
- **Insert device name variable** (Wprowadź nazwę urządzenia): Ta zmienna zostanie zastąpiona nazwą urządzenia używaną podczas stosowania pliku konfiguracyjnego. Nazwę urządzenia można znaleźć w kolumnie **Name** (Nazwa) na stronie **Device management** (Zarządzanie urządzeniami). Aby zmienić nazwę urządzenia, przejdź do strony **Cameras** (Kamery) lub **Other devices** (Inne urządzenia).
- **Insert server name variable** (Wprowadź nazwę serwera): Ta zmienna zostanie zastąpiona nazwą serwera używaną podczas stosowania pliku konfiguracyjnego. Nazwę serwera można znaleźć w kolumnie **Server** (Serwer) na stronie **Device management** (Zarządzanie urządzeniami). W celu zmiany nazwy serwera przejdź do aplikacji AXIS Camera Station Pro Service Control.
- **Insert server time zone variable** (Wprowadź strefę czasową serwera): Ta zmienna zostanie zastąpiona strefą czasową POSIX serwera używaną podczas stosowania pliku konfiguracyjnego. Tej zmiennej możesz 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

- **Stream profiles** (Profil strumieniowania): Profil strumieniowania to wstępnie zaprogramowany profil konfiguracyjny podglądu na żywo zawierający ustawienia kodowania obrazu ruchomego, obrazu nieruchomego i dźwięku. Profile strumieni można kopiować między urządzeniami.
- **Motion detection windows** (Okna detekcji ruchu): Okna detekcji ruchu służą do definiowania konkretnych obszarów w polu 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

Aby zarządzać użytkownikami urządzeń, przejdź do **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).

Po ustawieniu hasła lub usunięciu użytkowników z urządzeń użytkownicy nieobecni we wszystkich urządzeniach będą oznaczeni symbolem . Każdy użytkownik pojawia się tylko raz, nawet jeżeli pełni różne role w różnych urządzeniach.

Uwaga

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

Zasady dotyczące haseł

Niektóre urządzenia wymagają, by hasła spełniały określone kryteria. Gdy jedno lub więcej wybranych urządzeń stosuje zasady dotyczące haseł, wskaźnik siły hasła zastępowany jest wskaźnikiem zgodności z zasadami, który wskazuje, czy hasło użytkownika spełnia wymagania obowiązujących zasad.

- Jeżeli nie są wymagane zasady albo urządzenie obsługuje standard ONVIF, wskaźnik siły hasła jest wyświetlany standardowo.
- Jeżeli wybrałeś kilka urządzeń z różnymi zasadami, hasło musi spełniać je wszystkie.
- Jeżeli hasło nie spełnia wymagań, wyświetla się komunikat **Non-compliant** (Nie spełnia wymagań). Najedź kursorem na ikonę informacji, aby wyświetlić szczegółowe wymagania:

Zasady dotyczące długości – Hasło musi się składać z co najmniej 15 znaków.

Zasady dotyczące złożoności – Hasło musi mieć co najmniej 12 znaków oraz zawierać jedną wielką literę, jedną małą literę, jedną cyfrę i jeden znak specjalny.

Obie zasady – Muszą być spełnione zarówno wymagania dotyczące długości, jak i złożoności.

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. Zaleca się, aby w urządzeniach ze starszymi wersjami oprogramowania układowego 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 Pro.

W hasłach można używać następujących znaków:

- Litery A - Z, a - z
- Cyfry 0 - 9
- Spacja, przecinek (,), kropka (.), dwukropek (:), średnik (;)

- !, ", #, \$, %, &, ', (, +, *, -, ., /, <, >, =, ?, [\, ^, _ , ` , {, |, ~, @,], }

Aby ustawić hasło dla użytkowników w 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** (Generuj) i utwórz silne hasło.
5. Kliknij **OK**.

Uwaga

Jeżeli wybierzesz opcję **Use this password for all devices without a factory default password** (Użyj tego hasła dla wszystkich urządzeń bez hasła z ustawień fabrycznych), hasło to zostanie zastosowane do wszystkich urządzeń o statusie **Set password** (Ustaw hasło). Jeżeli długość hasła przekracza maksymalną długość obsługiwaną przez urządzenie, zostaniesz o tym poinformowany przed otwarciem okna dialogowego i będziesz mógł zdecydować się na kontynuowanie bez tych urządzeń.

Dodaj użytkownika

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

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 **Ustaw hasło**.
4. Wybierz uprawnienia użytkownika z listy rozwijalnej **Role** (Rola):
 - **Administrator**: nieograniczony dostęp do urządzenia.
 - **Operator**: dostęp do strumienia wizyjnego, zdarzeń i wszystkich ustawień oprócz opcji systemowych.
 - **Viewer** (Dozorca): dostęp do strumienia wizyjnego.
5. Zaznacz opcję **Enable PTZ control** (Włącz sterowanie PTZ), aby pozwolić użytkownikowi na obracanie, przechylanie i zbliżanie / oddalanie w podglądzie na żywo.
6. Kliknij **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. Z listy rozwijalnej **User** (Użytkownik) wybierz użytkownika, którego dane chcesz usunąć.
4. Kliknij **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 **Type to search** (Wpisz, aby wyszukać) odszukaj użytkowników spośród figurujących na liście.

Aktualizuj oprogramowanie sprzętowe

Oprogramowanie układowe określa funkcje urządzenia Axis. Aktualizowanie oprogramowania układowego zapewnia, że urządzenie będzie miało dostęp do najnowszych funkcji i usprawnień.

Nowe oprogramowanie układowe możesz pobrać z wykorzystaniem programu **AXIS Camera Station Pro** lub zaimportować z pliku znajdującego się na dysku twardym lub karcie pamięci. Wersje oprogramowania układowego dostępne do pobrania są oznaczone napisem **(Download)** (Pobierz) umieszczonym obok numeru 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:

- **Standard** (Standardowy): Aktualizacja do wybranej wersji oprogramowania układowego i zachowanie istniejących wartości ustawień.
- **Factory default** (Ustawienia fabryczne): Aktualizacja do wybranej wersji oprogramowania układowego 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 **Invalid devices** (Nieprawidłowe urządzenia). Kliknij przycisk **Kontynuuj**, aby pominąć urządzenia, których nie można skonfigurować.
4. Podczas aktualizacji oprogramowania układowego urządzenie jest niedostępne. Kliknij przycisk **Yes** (**Tak**), aby kontynuować. Jeżeli nie chcesz, aby ten komunikat pojawiał się ponownie, zaznacz opcję **Do not show this dialog again** (Nie pokazuj ponownie tego okna dialogowego) i kliknij przycisk **Tak**.
5. Okno dialogowe **Upgrade firmware** (Aktualizuj oprogramowanie układowe) zawiera informacje takie jak model urządzenia, liczba urządzeń każdego modelu, istniejąca wersja oprogramowania układowego, dostępne wersje, do których można uaktualnić, oraz rodzaj aktualizacji. Domyślnie urządzenia wymienione na liście są wstępnie zaznaczane, gdy pojawią się nowe wersje oprogramowania układowego 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 układowego, które chcesz uaktualnić, i rodzaj 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. Zob. *Ustawienia aktualizacji oprogramowania sprzętowego*.



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

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 Pro. 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 z kluczem licencyjnym możesz zainstalować razem z aplikacją lub później, korzystając ze 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 licencji. Można ją instalować w kamerach z oprogramowaniem układowym w wersji 6.50 i nowszym. 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 licencji. Można ją instalować w kamerach z oprogramowaniem układowym w wersji 5.60 i nowszym.

AXIS Video Content Stream – Aplikacja, która umożliwia kamerom Axis wysyłanie danych funkcji śledzenia ruchu do AXIS Camera Station Pro. Można ją instalować w kamerach z oprogramowaniem sprzętowym w wersjach od 5.50 do 9.59. Aplikacja AXIS Video Content Stream może być stosowana wyłącznie z AXIS Camera Station Pro.

Inne aplikacje – Wszelkie inne aplikacje, które chcesz 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, w których chcesz zainstalować aplikacje. Kliknij  lub kliknij prawym przyciskiem myszy i wybierz polecenie **Install camera application** (Zainstaluj aplikację do kamery).
3. Wybierz aplikację do kamery, którą chcesz zainstalować. Jeżeli chcesz zainstalować inne aplikacje, kliknij przycisk **Browse** (Przeglądaj) i przejdź do lokalnego pliku aplikacji. Kliknij **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

Powrót do starszej wersji lub nadpisanie aplikacji powoduje zresetowanie jej ustawień w urządzeniach.

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

Nie są potrzebne licencje 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 IEEE 802.1X, urządzenie certyfikacji (certificate authority, CA) AXIS Camera Station Pro automatycznie podpisuje oraz dystrybuje certyfikaty klientów i serwerów dla urządzeń. CA ignoruje wstępnie zainstalowane certyfikaty. Informacje na temat konfigurowania certyfikatów: *Certyfikaty, on page 142*.

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 Pro.

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

Uwaga

Gdy ten sam certyfikat został zainstalowany w kilku urządzeniach, pojawia jako jeden element. Usunięcie certyfikatu spowoduje jego usunięcie ze wszystkich urządzeń, w 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 Pro używa protokołu HTTPS do łączenia się z urządzeniem.
	Wył.	AXIS Camera Station Pro używa protokołu HTTP do łączenia się z urządzeniem.
	Nieznany	Urządzenie jest nieosiągalne.

	Nieobsługiwane oprogramowanie układowe	Protokół HTTPS nie jest obsługiwany, ponieważ oprogramowanie układowe jest za stare.
	Nieobsługiwane urządzenie	Protokół HTTPS nie jest obsługiwany w tym modelu urządzenia.
IEEE 802.1X	Włączony	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 w urządzeniu.
	Nieobsługiwane oprogramowanie układowe	Protokół IEEE 802.1X nie jest obsługiwany, ponieważ oprogramowanie układowe jest za stare.
	Nieobsługiwane urządzenie	Protokół IEEE 802.1X nie jest obsługiwany w 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 w 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 **Data source on selected devices** (Źródła danych w wybranych urządzeniach):
 - Kliknij opcję **Prepozycja** i wybierz z listy rozwijanej żądane często używane polecenie.

Uwaga

Niektóre predefiniowane ustawienia nie działają we wszystkich urządzeniach. Na przykład opcja PTZ status (Status PTZ) nie działa w urządzeniach fonicznych.

- Kliknij przycisk **Niestandardowe** i podaj ścieżkę URL do źródła na wybranych serwerach, z którego są zbierane dane.
4. W sekcji **Save as** (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 **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 **Connection** (Połączenie).
 - Aby się łączyć z urządzeniami przy użyciu adresu IP, wybierz polecenie **Użyj adresu IP**.
 - Aby się łączyć z urządzeniami przy użyciu nazwy hosta, wybierz polecenie **Użyj nazwy hosta**.
 - Aby zmienić poświadczenia lub ustawienia adresu i portu, wybierz **Edit** (Edytuj).

Znaczniki

Znaczniki pomagają w organizowaniu urządzeń na stronie **Device management** (Zarządzanie urządzeniami). Jedno urządzenie może mieć wiele znaczników.

Urządzenia można oznaczać na podstawie modelu, lokalizacji lub innych kryteriów. Na przykład oznaczanie urządzeń na podstawie modelu kamery pozwala szybko odnaleźć wszystkie kamery danego 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. Wybierz **Use existing tag** (Użyj istniejącego znacznika) i wybierz znacznik lub opcję **Create a new tag** (Utwórz nowy znacznik) i nadaj nazwę nowemu znacznikowi.
4. Kliknij **OK**.

Aby usunąć znacznik z urządzenia:

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

Aby zarządzać znacznikami:

1. Wybierz kolejno **Configuration (Konfiguracja) > Devices (Urządzenia) > Management (Zarządzanie)** i w prawym górnym rogu kliknij .
2. Na stronie **Device tags** (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 AXIS Camera Station Pro.
 - 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. Aby uzyskać informacje o konfiguracji urządzenia, zapoznaj się z jego instrukcją obsługi.
4. Zamknij kartę. Urządzenie odświeża się, aby zastosować zmiany w AXIS Camera Station Pro.

Ograniczenia

- Automatyczne uwierzytelnianie urządzeń innych producentów nie jest obsługiwane.
- Nie gwarantuje się ogólnej obsługi urządzeń innych producentów.

- Otwarcie karty konfiguracji urządzenia przy aktywnych strumieniach wizyjnych powoduje wzrost obciążenia i może spowolnić działanie serwera.

Zewnętrzne źródła danych

Zewnętrzne źródło danych to system lub źródło danych generujące dane, na podstawie których można wysledzić okoliczności towarzyszące każdemu zdarzeniu. Zob. *Wyszukiwanie danych, on page 44*.

Przejdź do **Configuration > Devices > External data sources** (Konfiguracja > Urządzenia > Zewnętrzne źródła danych), aby wyświetlić listę 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 Pro 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 Pro 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 zakładki na osi czasu widoku na karcie **Data search** (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

Przejdź do **Configuration > Devices > Time synchronization** (Konfiguracja > Urządzenia > Synchronizacja czasu), a zostanie otwarta strona **Time synchronization** (Synchronizacja czasu).

Program AXIS Camera Station Pro wyświetla listę wszystkich dodanych urządzeń. 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:

- **Name (Nazwa):** Nazwa urządzenia lub lista wszystkich nazw powiązanych kamer, jeżeli urządzenie jest koderem wizyjnym z wieloma dołączonymi kamerami lub kamerą sieciową z wieloma zdefiniowanymi widokami.

- **Address (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. Zob. *Karta Konfiguracja urządzenia, on page 73*.
- **MAC address (Adres MAC):** Adres MAC urządzenia.
- **Model:** Model urządzenia.
- **Enabled (Włączona):** Wskazuje, czy jest włączona synchronizacja czasu.
- **NTP source (Źródło NTP):** Źródło NTP skonfigurowane dla urządzenia.
 - **Static (Statyczne):** Serwery NTP dla urządzenia konfiguruje się ręcznie w ustawieniach **Primary NTP server** (Główny serwer NTP) i **Secondary NTP server** (Rezerwowy 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.
- **Primary NTP server (Główny serwer NTP):** Główny serwer NTP skonfigurowany dla tego urządzenia. Ustawienie jest dostępne tylko po zaznaczeniu opcji **Statyczna**.
- **Secondary NTP server (Rezerwowy serwer NTP):** Rezerwowy serwer NTP skonfigurowany dla tego urządzenia. Ustawienie jest dostępne tylko dla urządzeń Axis obsługujących dodatkowe serwery NTP i pod warunkiem zaznaczenia opcji **Statyczna**.
- **Server time offset (Różnica czasu serwera):** Różnica czasu pomiędzy urządzeniem a serwerem.
- **UTC time (Czas UTC):** Godzina według czasu uniwersalnego w urządzeniu.
- **Synced: (Synchronizacja):** Wskazanie, czy zastosowano ustawienia synchronizacji czasu. Dostępne tylko dla urządzeń z oprogramowaniem układowym w wersji 9.1 lub nowszej.
- **Time to next sync (Czas do następnej synchronizacji):** Czas pozostały do następnej 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 Pro. Są wyświetlane następujące informacje:

- **Server (Serwer):** Serwer AXIS Camera Station Pro, na którym działa usługa Czas systemu Windows.
- **Status (Stan):** Stan usługi Czas systemu Windows. **Running** (Uruchomiono) albo **Stopped** (Zatrzymano).
- **NTP server (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 **Static (Statyczna)**, skonfiguruj podstawowy i dodatkowy serwer NTP.
5. Kliknij przycisk **Apply (Zastosuj)**.

Send alarm when the time difference between server and device is more than 2 seconds (Wyślij alarm, gdy różnica czasu między serwerem a urządzeniem przekroczy 2 sekundy)	Wybierz tę opcję, aby otrzymać alarm, jeżeli różnica czasu między serwerem a urządzeniem przekroczy 2 sekundy.
Set the time zone manually through the device interface (Ustaw manualnie strefę czasową w interfejsie urządzenia)	Wybierz tę opcję, jeśli w lokalizacji urządzenia nie chcesz używać strefy czasowej serwera, tylko innej. W przypadku wybrania tej opcji należy ustawić strefę czasową manualnie za pomocą interfejsu WWW urządzenia.

Konfigurowanie pamięci masowej

Przejdź do **Configuration > Storage > Management** (Konfiguracja > Pamięć masowa > Zarządzanie), aby otworzyć stronę **Manage storage** (Zarządzaj pamięcią masową). Tutaj znajdziesz przegląd lokalnej pamięci masowej i sieciowej pamięci masowej w AXIS Camera Station Pro.

Lista	
Lokalizacja	Ścieżka i nazwa pamięci masowej.
Przydzielone	Maksymalna ilość pamięci masowej przydzielona na nagrania.
Wykorzystane	Ilość pamięci masowej obecnie wykorzystywana na nagrania.

Lista	
Status	Stan pamięci masowej. Możliwe wartości: • OK • Storage full (Pamięć masowa zapelniona): Pamięć masowa jest pełna. System nadpisuje najstarsze, niezablokowane nagrania. • Unavailable (Niedostępne): Informacje o pamięci masowej nie są obecnie dostępne. Dzieje się tak na przykład w razie usunięcia lub odłączenia pamięci masowej. • Intruding data (Kolidujące dane): Dane z innych aplikacji wykorzystują przestrzeń dyskową przydzieloną do AXIS Camera Station Pro. Lub istnieją nagrania bez połączenia z bazą danych, tak zwane nagrania niezaindeksowane, w przestrzeni dyskowej przydzielonej do AXIS Camera Station Pro. • No permissions (Brak upewnień): Użytkownik nie ma uprawnień do odczytu ani zapisu w pamięci masowej. • Low space (Mało miejsca): Na dysku jest mniej niż 15 GB wolnego miejsca, czyli zbyt mało z perspektywy AXIS Camera Station Pro. Aby zapobiec błędom lub uszkodzeniom, AXIS Camera Station Pro wykonuje wymuszone czyszczenie, niezależnie od położenia suwaka pamięci masowej, w celu ochrony dysku. Podczas wymuszonego czyszczenia AXIS Camera Station Pro blokuje nagrywanie do czasu, gdy będzie dostępne ponad 15 GB wolnego miejsca w pamięci masowej. • Insufficient capacity (Brak miejsca): Całkowity rozmiar dysku jest mniejszy niż 32 GB, czyli zbyt mały na AXIS Camera Station Pro. W przypadku rejestratorów z systemami AXIS OS obsługujących RAID mogą występować następujące stany: • Online: System RAID działa zgodnie z oczekiwaniami. Istnieje nadmiarowość na wypadek awarii jednego z dysków fizycznych w macierzy RAID. • Degraded (Obniżona sprawność): Jeden z dysków fizycznych w systemie RAID jest uszkodzony. Nadal można zapisywać i odtwarzać nagrania z pamięci masowej, 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). • Syncing (Synchronizacja): Dyski w macierzy RAID są w trakcie synchronizacji. Możliwy jest zapis i odtwarzanie nagrań z pamięci masowej, 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. Ważne W trakcie synchronizacji nie wolno usuwać dysków RAID, bo może to spowodować ich uszkodzenie. • Failure (Awaria): Wystąpiły błędy kilku dysków fizycznych w macierzy 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	
Wykorzystane	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) . Zob. <i>Zarządzaj pamięcią masową, on page 78</i> .
Free (Wolna)	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 nieznanie aplikacji AXIS Camera Station Pro. 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 Pro 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.
Password (Hasło):	Hasło dla nazwy użytkownika służącej do łączenia się z sieciową pamięcią masową.

Zarządzaj pamięcią masową

Przejdź do **Configuration > Storage > Management** (Konfiguracja > Pamięć masowa > Zarządzanie), aby otworzyć stronę **Manage storage** (Zarządzaj pamięcią masową). W tym miejscu wskaż folder, w którym będą zapisywane nagrania. Aby zapobiec zapełnieniu pamięci masowej, ustaw maksymalny procent całkowitej pojemności, jaki może wykorzystywać program AXIS Camera Station Pro. 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 Pro można zarządzać pamięcią masową, wybierając serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.
- Gdy do usługi logujesz się przy użyciu konta systemowego, nie możesz dodawać dysków sieciowych połączonych z udostępnionymi folderami znajdującymi się na innych komputerach. Zob. *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 **Local storage** (Lokalna pamięć masowa) i wybierz lokalizację pamięci masowej z menu rozwijalnego.

4. Aby dodać współdzielony dysk sieciowy, zaznacz **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 współdzielony dysk sieciowy, wybierz je z listy pamięci masowej i kliknij **Remove** (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)** przesun suwak, aby ustawić maksymalną ilość miejsca, które może zająć aplikacja AXIS Camera Station Pro.
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 programu AXIS Camera Station Pro to 32 GB, przy czym musi być co najmniej 15 GB wolnego miejsca.
- Jeżeli jest mniej niż 15 GB wolnego miejsca, AXIS Camera Station Pro automatycznie usuwa starsze 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** 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**, potrzebujesz dostępu do serwera. Program AXIS Camera Station Pro organizuje dane najpierw według serwerów, a dalej według urządzeń dołączonych do danego serwera.

Możesz wyszukać utracone nagranie lub wpisać, albo usunąć treść, aby zwolnić miejsce.

Aby zebrać niezaindeksowane pliki w celu przejrzania 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.

- Po zakończeniu zadania przejdź do **Alarms and Tasks > Tasks** (Alarmy i zadania > Zadania) i kliknij dwukrotnie zadanie, aby wyświetlić wynik.

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.

Przejdź do **Configuration > Storage > Selection** (Konfiguracja > Pamięć masowa > Wybór), a zostanie otwarta strona **Select storage** (Wybierz pamięć masową). Na tej stronie znajduje się lista wszystkich kamer w programie AXIS Camera Station Pro. Możesz w niej określić, przez ile dni mają być przechowywane nagrania z poszczególnych kamer. Po zaznaczeniu informacje o pamięci masowej będą widoczne w obszarze **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 łączy 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. Zob. <i>Karta Konfiguracja urządzenia, on page 73</i> .
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.
Odtwarzanie z karty SD	Wskazuje, czy kamera jest skonfigurowana do odtwarzania nagrań bezpośrednio z karty SD w programie AXIS Camera Station Pro bez kopiowania ich na serwer.
Zapis awaryjny	Wskazuje, czy kamera korzysta z zapisu awaryjnego.
Kopiuje do ACS Pro	Wskazuje, czy nagrania z karty SD są kopiowane do programu AXIS Camera Station Pro.
Zapis zawartości rezerwowej	Wskazuje, czy kamera korzysta z zapisu zawartości rezerwowej.
Serwer	Serwer, na którym znajduje się lokalna lub sieciowa pamięć masowa.

Ustawienia pamięci masowej dla każdej kamery zostały skonfigurowane w momencie dodania kamer do programu AXIS Camera Station Pro. Aby zmodyfikować ustawienia zasobu dla kamery:

- Wybierz kolejno opcje **Configuration > Storage > Selection** (Konfiguracja > Zasób > Wybór).
- Wybierz kamerę w celu edycji ustawień zasobu.
- W menu **Recording storage (Pamięć masowa nagrań)** ustaw lokalizację pamięci masowej i czas przechowywania.

4. W obszarze **SD card storage** (Przechowywanie na karcie SD) wybierz odpowiednio opcje **Playback of SD card recordings** (Odtwarzanie nagrań z karty SD), **Failover recording** (Zapis awaryjny) oraz **Copy SD card recordings to ACS Pro server** (Kopiowanie nagrań z karty SD na serwer ACS Pro).
5. Kliknij przycisk **Apply** (Zastosuj).

Pamięć masowa nagrań Uwaga - Aby korzystać z pamięci masowej na karcie SD, urządzenie musi obsługiwać technologię VAPIX i być wyposażone w kartę SD Axis. - Funkcje związane z kartą SD nie działają w standardzie M-JPEG. - Nagrania zapisane na karcie SD nie są usuwane w programie AXIS Camera Station Pro. Czas ich przechowywania jest określony na karcie SD w kamerze.	
Store to (Zapisz w)	W menu rozwijalnym wybierz lokalizację pamięci masowej dla nagrań. Do wyboru są utworzone zasoby lokalne i sieciowe.
Czas przechowywania	Unlimited (Bez ograniczeń): Zachowuj nagrania do chwili zapełnienia pamięci masowej. Limited (Z ograniczeniem): Ustaw maksymalną liczbę dni przechowywania nagrań. Uwaga Jeżeli miejsce w pamięci masowej przeznaczone dla AXIS Camera Station Pro 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.

Karta pamięci SD	
Odtwarzanie nagrań z karty SD	Włącz, aby odtwarzać nagrania bezpośrednio z karty SD kamery w programie AXIS Camera Station Pro bez konieczności kopiowania ich na serwer. Nagrania z karty SD widoczne na osi czasu można również eksportować. Ta funkcja wymaga systemu AXIS OS w wersji 5.60 lub nowszej.
Zapis awaryjny	Zaznacz, aby zapisywać nagrania na karcie SD kamery w przypadku utraty połączenia z programem AXIS Camera Station Pro. Dostępne dla kamer z kartą pamięci SD oraz oprogramowaniem układowym w wersji 5.20 lub nowszej.
Kopiowanie nagrań z karty SD na serwer ACS	Wybierz, aby skopiować wszystkie nagrania z karty SD kamery na serwer. W obszarze Schedule (Harmonogram) ustaw, kiedy mają być kopiowane nagrania. Domyślnym ustawieniem harmonogramu jest Always (Zawsze).

Konfigurowanie nagrywania i zdarzeń

Po dodaniu kamer do AXIS Camera Station Pro system automatycznie konfiguruje zapis ruchu lub zapis ciągły. Metodę zapisu można później zmienić. Zob. *Metoda nagrywania, on page 87*.

Nagrywanie w trybie detekcji ruchu

Funkcji detekcji ruchu możesz używać we wszystkich kamerach sieciowych i koderach wizyjnych Axis. Zapis tylko po wykryciu ruchu pozwoli oszczędzić znaczącą ilość pamięci masowej względem zapisu ciągłego. W obszarze **Recording method (Metoda nagrywania)** można włączyć i skonfigurować **Motion detection (Detekcję ruchu)**. Można na przykład skonfigurować ustawienia, jeżeli kamera wykryje zbyt wiele lub zbyt niewiele poruszających się obiektów, albo jeżeli rozmiar zapisanych plików jest zbyt duży w stosunku do dostępnej wielkości pamięci masowej.

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, p. sekcja *Edytowanie wbudowanej funkcji detekcji ruchu i Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4*.
5. W menu rozwijalnym wybierz **Profile (Profil)**; domyślnie wybrany jest profil **High (Wysoki)**.
6. Wybierz harmonogram lub kliknij **New schedule...** (Nowy harmonogram), aby utworzyć nowy własny harmonogram.
7. Ustaw czasy buforowania przed i po zdarzeniu oraz okres wyzwalania.
8. Kliknij przycisk **Apply (Zastosuj)**.

Uwaga

Nagrywanie inicjowane ruchem można skonfigurować przy użyciu reguł akcji. Przed zastosowaniem reguł działania sprawdź, czy w obszarze **Recording method (Metoda zapisu)** wyłączona jest opcja **Motion detection (Detekcja ruchu)**.

Profil	Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, zob. <i>Profile strumieniowania</i> .
Harmonogram	Harmonogram nagrań. Aby zmniejszyć wpływ na zasób pamięci, nagrywaj tylko w określonych przedziałach czasu.
Kategoria zdarzenia	Kategoria zdarzenia, do której ma należeć nagranie, o ile w ogóle chcesz je przyporządkować.
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)	Ustawia minimalny czas pomiędzy dwoma wyzwalaczami, aby zmniejszyć liczbę nagrań następujących bezpośrednio po sobie. Jeżeli w tym odstępie czasu wystąpi kolejny wyzwalacz, zapis będzie kontynuowany, a odstęp czasu będzie odliczany ponownie.
Powiadomienia	Powiadomienie jest wysyłane, gdy kamera wykryje ruch. Aplikacja mobilna wysyła powiadomienie push do aplikacji mobilnej AXIS Camera Station. Alarm serwera podnosi alarm w programie AXIS Camera Station Pro.



Konfigurowanie funkcji detekcji ruchu

Detekcja obiektów

Funkcja zapisu detekcji obiektów wykonuje rejestrację obrazu po wykryciu i sklasyfikowaniu przez aplikację AXIS Object Analytics rodzaju obiektów takich jak ludzie i pojazdy. Aby mieć pewność, że żadne zdarzenie nie zostanie pominięte, zaleca się korzystanie z tej funkcji wraz z detekcją ruchu lub zapisem ciągłym. Aplikacja AXIS Object Analytics obsługuje maks. 10 scenariuszy na każdą kamerę.

Uwaga

Aby korzystać z tej funkcji, kamera musi mieć oprogramowanie układowe w wersji 12.4.26 lub nowszej, pojedynczy przetwornik obrazu oraz zainstalowaną aplikację AXIS Object Analytics ACAP.

Aby użyć funkcji detekcji obiektów:

- Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
- Wybierz kamerę.
- Zaznacz pole wyboru **Object detection (Detekcja obiektów)**.
- Skonfiguruj ustawienia. W poniższej tabeli znajdują się szczegółowe informacje.
- Kliknij przycisk **Apply (Zastosuj)**.
 - Zdarzenia detekcji obiektów wyświetlane są na osi czasu w kolorze różowym.

Ustawienia detekcji obiektów...	Kliknij, aby otworzyć interfejs internetowy aplikacji AXIS Object Analytics i zdecyduj, które rodzaje obiektów (ludzie, pojazdy) będą wyzwalaczami zapisu, ustaw minimalną wielkość obiektu, określ obszary detekcji i dostosuj ustawienia czasu przebywania w obszarze.
Profil	Wybierz Profile (Profil) z menu rozwijalnego. High (Wysoki) to domyślny profil. Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, zob. <i>Profile strumieniowania</i> .

Harmonogram	Ustaw harmonogram nagrań. Aby zmniejszyć wpływ na zasób pamięci, nagrywaj tylko w określonych przedziałach czasu.
Kategoria zdarzenia	Wybierz kategorię zdarzenia, do której ma należeć nagranie, o ile w ogóle chcesz je przyporządkować. Więcej informacji, p. sekcja <i>Kategorie zdarzeń</i> , on page 28.
Bufor przed zdarzeniem	Ustaw, ile sekund przed wykryciem obiektu ma zostać zarejestrowanych w nagraniu.
Bufor po zdarzeniu	Ustaw, ile sekund po wykryciu obiektu ma zostać zarejestrowanych w nagraniu.
Trigger period (Okres wyzwalacza)	Ustaw minimalny odstęp czasu pomiędzy wyzwalaczami, aby ograniczyć liczbę nagrań następujących bezpośrednio po sobie. Jeżeli w tym odstępie czasu wystąpi następny wyzwalacz, zapis będzie kontynuowany, a okres wyzwalania zostanie uruchomiony ponownie.
Powiadomienia	Wysyła powiadomienie, gdy aplikacja AXIS Object Analytics wykryje obiekt. Aplikacja mobilna wysyła powiadomienie push do aplikacji mobilnej AXIS Camera Station. Alarm serwera wzbudza alarm w programie AXIS Camera Station Pro.

Nagrywanie ciągłe i zaplanowane

Zapis ciągły polega na zapisywaniu obrazów bez przerwy, dlatego wymaga więcej miejsca w pamięci masowej niż inne opcje zapisu. Aby zmniejszyć rozmiar pliku, rozważ zamienne użycie zapisu uruchamianego 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)**.
4. Skonfiguruj ustawienia. W poniższej tabeli znajdują się szczegółowe informacje.
5. Kliknij przycisk **Apply (Zastosuj)**.

Profil	Wybierz Profile (Profil) z menu rozwijalnego. High (Wysoki) to profil domyślny. Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, zob. <i>Profile strumieniowania</i> .
Harmonogram	Ustaw harmonogram nagrań. Aby zmniejszyć wpływ na zasób pamięci, nagrywaj tylko w określonych przedziałach czasu.
Średnia przepływność	Włącz, aby ustawić maksymalne ograniczenie 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 <i>Konfigurowanie średniej przepływności, on page 88</i> .

Nagrywanie ręczne

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	Wybierz Profile (Profil) z menu rozwijalnego. High (Wysoki) to profil domyślny. Aby zmniejszyć rozmiar nagrania, użyj niższej rozdzielczości. Aby zmodyfikować ustawienia profilu, zob. <i>Profile strumieniowania</i> .
Kategoria zdarzenia	Wybierz kategorię zdarzenia, do której ma należeć nagranie, o ile w ogóle chcesz je przyporządkować.
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	Dodaje 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.

Aby uzyskać więcej informacji o zapisie ręcznym, p. sekcja *Ręczne nagrywanie*.

Zapis wyzwalany regułami

Nagrywanie wyzwalane regułami jest uruchamiane i zatrzymywane zgodnie z regułą utworzoną w oknie Reguły akcji. Regułę można używać na przykład do generowania nagrań wyzwalanych sygnałami z portów we/wy lub zdarzeniami urządzeń. Reguła może mieć kilka wyzwalaczy.

Aby utworzyć zapis wyzwalany regułą, p. sekcja *Reguły akcji*.

Uwaga

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

Zapis awaryjny

Skorzystaj z funkcji zapisu awaryjnego, aby zapisywać nagrania na karcie SD kamery w razie utraty połączenia z programem AXIS Camera Station Pro.

AXIS Camera Station Pro automatycznie wybiera metodę przełączania awaryjnego w zależności od wersji oprogramowania układowego kamery:

- **Oprogramowanie układowe w wersji 11.11.42 lub nowszej:** Zapis awaryjny rozpoczyna się w momencie utraty połączenia kamery z serwerem.
- **Wcześniejsza wersja oprogramowania układowego:** Zapis awaryjny rozpoczyna się dopiero w przypadku nieoczekiwanej utraty połączenia. Planowane ponowne uruchomienia serwerów nie są powodem uruchomienia zapisu awaryjnego.

Aby skonfigurować zapis awaryjny, p. sekcja *Wybieranie urządzeń pamięci masowej, z którymi mają zostać nawiązane połączenia, on page 80*.

Uwaga

- W przypadku aktualizacji, jeżeli zapis awaryjny był wcześniej włączony, opcja **Copy SD card recordings to ACS Pro server** (Kopiuj nagrania z karty SD na serwer ACS Pro) włącza się automatycznie.
- Program AXIS Camera Station Pro nie usuwa nagrań z karty SD. Okres przechowywania tych danych określa ustawienie czasu przechowywania na karcie SD w kamerze.
- Włączenie zapisu awaryjnego powoduje nadpisanie wszelkich istniejących konfiguracji awaryjnych przypisanych do tej kamery w innych serwerach.
- Zapis awaryjny może być aktywny jednocześnie tylko na jednym serwerze AXIS Camera Station Pro na każdy widok z kamery.

Gdy połączenie zostanie przywrócone, a opcja **Copy SD card recordings to ACS Pro server** (Kopiuj nagrania z karty SD na serwer ACS Pro) jest włączona, nagrania zostaną skopiowane na serwer i zaznaczone na osi czasu kolorem ciemnoszarym. Kamera wykorzystuje 20-sekundowy bufor zapisu przed i po wystąpieniu zdarzenia, ale mogą wystąpić krótkie przerwy trwające 1 do 4 sekund.

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. • 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.



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

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 urządzenie automatycznie rozpoczyna zapis ciągły w momencie utraty połączenia pomiędzy programem AXIS Camera Station Pro a rejestratorem. Do zapisu zawartości rezerwowej urządzenie używa profilu Medium (Średni).

Uwaga

- Do działania funkcji jest potrzebny program AXIS Camera Station w wersji 5.36 lub nowszej, oprogramowanie układowe rejestratora AXIS S3008 Recorder w wersji 10.4 lub nowszej oraz oprogramowanie układowe urządzeń Axis w wersji 5.50 lub nowszej.
- Jeżeli w momencie rozpoczęcia zapisu zawartości rezerwowej trwa zapis ciągły, rozpoczyna się nowy zapis ciągły. System tworzy duplikaty strumienia na rejestratorze.

Aby włączyć funkcję zapisu rezerwowego:

1. Sprawdź, czy dodano rejestrator 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 Pro automatycznie konfiguruje zapis ruchu lub zapis ciągły podczas dodawania urządzeń.

Zaznaczenie wskazuje metodę zapisu stosowaną przez dane urządzenie. Aby dostosować ustawienia profilu dotyczącego obrazu wideo i dźwięku, zobacz *Profile strumieniowania*.

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 zapisu) można włączyć lub wyłączyć daną metodę zapisu.

Uwaga

Obszary obserwacji nie obsługują detekcji ruchu.

Konfigurowanie średniej przepływności

Średnia przepływność bitowa dostosowuje się automatycznie w dłuższym okresie. Dzięki temu uzyskuje się docelową przepływność i zapewnia dobrą jakość obrazu przy określonej specyfikacji pamięci masowej.

Uwaga

- Opcja ta dostępna jest wyłącznie w trybie zapisu ciągłego. Kamery muszą obsługiwać ustawienie średniej przepływności i mieć oprogramowanie układowe w wersji 9.40 lub nowszej.
 - Ustawienia średniej przepływności bitowej wpływają na jakość wybranego profilu strumienia.
1. Przejdź do **Configuration > Storage > Selection** (Konfiguracja > Pamięć masowa > Wybór) i sprawdź, czy 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 wynosi 50000 kb/s.

Uwaga

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

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

Edytowanie ustawień ruchu

Jeśli urządzenie korzysta z AXIS Object Analytics, można tam edytować ustawienia nagrywania wyzwalanego ruchem.

Uwaga

AXIS Object Analytics w oprogramowaniu AXIS Camera Station Pro wymaga systemu AXIS OS 12.4.

1. Otwórz kartę **Configuration** (Konfiguracja).
2. Przejdź do menu **Recording and events** (Zapis i zdarzenia) > **Recording method** (Metoda zapisywania).
3. Wybierz kamerę, którą chcesz skonfigurować.
4. Włącz **Motion detection** (Detekcja ruchu).

5. Kliknij **Motion settings (Ustawienia ruchu)**.

Przeczytaj *instrukcję obsługi AXIS Object Analytics*, aby uzyskać informacje na temat konfigurowania AXIS Object Analytics na urządzeniu.

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

AXIS Video Motion Detection 2 i 4 to aplikacje do kamer przeznaczone do urządzeń obsługujących platformę 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 zapisu ruchu podczas dodawania kamer do programu AXIS Camera Station Pro w kamerach z wymaganym oprogramowaniem układowym jest instalowana aplikacja 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. Zob. *Instalowanie aplikacji do kamery*.

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

- **Area of interest (Obszar zainteresowania):** Obszar w nagraniu, 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).
- **Area to exclude (Obszar wykluczony):** Obszar w obrębie obszaru zainteresowania, w którym poruszające się obiekty są ignorowane.
- **Ignore filters (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.
 - **Short-lived objects filter (Filtr obiektów krótkotrwałych):** Filtr ten powoduje ignorowanie obiektów pojawiających się w obrazie tylko przez krótki czas. Przykładowo 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 jeżeli obiekt zniknie z obrazu w określonym czasie, nie wyzwala go.
 - **Small objects filter (Filtr małych obiektów):** Filtr pomija małe obiekty w rodzaju zwierząt. Ustaw szerokość i wysokość jako wartość procentową całkowitych wymiarów obrazu. Filtr ignoruje obiekty mniejsze od wyznaczonej szerokości i wysokości, i nie wyzwala alarmu. Aby filtr zignorował obiekt, musi on być mniejszy niż wyznaczona szerokość i wysokość.
 - **Swaying objects filter (Filtr kołyszących się obiektów):** 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

Ustawienia te stosowane są bezpośrednio w kamerze.

1. Wybierz kolejno opcje **Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania)**.
2. Wybierz kamerę zawierającą aplikację **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 jednego lub kilku obszarów detekcji, a jednocześnie ignoruje pozostały ruch. Strefa detekcyjna to obszar, w którym wykrywany jest ruch. Możesz korzystać z wielu obszarów detekcji i wykluczenia, a także umieścić obszar wykluczenia w obrębie obszaru detekcji, aby ignorować określony ruch.

Aby dodawać i edytować strefy detekcyjne:

Uwaga

Ustawienia te stosowane są bezpośrednio 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. Aby wyświetlić tylko obszar, który edytujesz, zaznacz **Show selected window (Pokaż zaznaczone okno)**.
6. Teraz możesz przesuwając kształt i zmieniać jego rozmiar na obrazie wideo. To jest strefa detekcyjna.
7. Ustaw parametry **Object size (Rozmiar obiektu)**, **History (Historia)** i **Sensitivity manually (Czułość ręcznie)**.

8. Aby stosować wstępnie zdefiniowane ustawienia, 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 po długim przebywaniu obiektu wewnątrz 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 **OK**.

Konfigurowanie kategorii zdarzeń

Kategorie zdarzeń ułatwiają wyszukiwanie nagrań określonego rodzaju. Aby utworzyć kategorię zdarzeń:

1. Przejdź do obszaru **Configuration** (Konfiguracja) > **Recording and events** (Nagrywanie i zdarzenia) > **Event categories** (Kategorie zdarzeń).
2. Kliknij **New** (Nowy).
3. Wprowadź nazwę kategorii zdarzeń.

4. Opcjonalnie można ustawić kolor kategorii zdarzeń i niestandardowy czas jej przechowywania.
5. Kliknij przycisk **Apply (Zastosuj)**.

Nazwa	Zalecamy użycie nazwy kategorii odpowiadającej typowi zdarzenia, takiej jak napaść lub zatrzymanie na drodze.
Czas przechowywania	Dla każdej kategorii zdarzeń można ustawić niestandardowy czas przechowywania, który zastępuje domyślny czas przechowywania określony dla kamery. Niestandardowy czas przechowywania kategorii zdarzeń ma zastosowanie tylko wtedy, gdy jest dłuższy od domyślnego.

Więcej informacji p. *Kategorie zdarzeń, on page 28.*

Porty we/wy

Wiele kamer i koderów wizyjnych ma porty we / wy służące do dołączania 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 zbitcia szyby i detektory PIR (pasywne czujki podczerwieni).

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

Uwaga

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

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

Informacje na temat dołączania urządzeń i konfiguracji portów we / wy znajdują w instrukcji obsługi lub instalacji urządzenia Axis. Niektóre urządzenia mają porty, które mogą działać jako wejście lub wyjście.

Portami wyjścia można sterować ręcznie. Zob. *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)**. Zaktualizuj w razie potrzeby.
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 Pro łączy się z urządzeniem. Wybierz opcję **On startup set to** (Podczas uruchamiania ustaw na) i wybierz stan początkowy z menu rozwijalnego **State** (Stan).

Edycja	Aby edytować port, zaznacz go i kliknij przycisk Edit (Edytuj). W 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)	Jeżeli 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 Pro można wybrać dowolny połączony serwer z menu rozwijalnego **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 Pro 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. Niektóre z tych działań wymagają dodatkowej konfiguracji urządzeń.

Utwórz nową regułę akcji

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
2. Kliknij **New...** (Nowy).
3. Wpisz nazwę reguły w polu reguły **Name** (Nazwa).
4. W obszarze **Schedule** (Harmonogram) wybierz **Always** (Zawsze) lub **Custom schedule** (Harmonogram niestandardowy), aby wybrać harmonogram z menu rozwijalnego. Możesz również utworzyć nowy harmonogram lub zmodyfikować istniejący.
5. W obszarze **Triggers** (Wyzwalacze) kliknij **Add...** (Dodaj), wybierz rodzaj wyzwalacza, skonfiguruj go i kliknij **OK**. Więcej informacji znajduje się w sekcji *Dodawanie wyzwalaczy*.

6. W obszarze **Actions** (Działania) kliknij **Add...** (Dodaj), wybierz rodzaj działania, skonfiguruj je i kliknij **OK**. Więcej informacji znajduje się w sekcji *Dodawanie działań*.
7. Kliknij przycisk **Apply** (Zastosuj).
 - Reguła zostaje automatycznie włączona po jej zapisaniu.

Edycja	Aby zmodyfikować istniejącą regułę, zaznacz ją i kliknij Edit (Edytuj).
Kopiuuj	Aby skopiować istniejącą regułę, zaznacz ją i kliknij Copy (Kopiuuj).
Usuń	Aby usunąć regułę, zaznacz ją i kliknij Remove (Usuń).

Konfigurowanie kilku reguł działań

Po wybraniu kilku reguł widoczne są jedynie wyzwalacze i działania takie same we wszystkich wybranych regułach. Wprowadzone zmiany będą zastosowane do wszystkich wybranych reguł.

- Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
- Wybierz kilka reguł.
- Wprowadź zmiany:
 - Dodaj wyzwalacze lub działania, które będą zastosowane do wszystkich wybranych reguł.
 - Usuń wspólne wyzwalacze lub działania ze wszystkich wybranych reguł.
 - Zmień harmonogram dotyczący wszystkich wybranych reguł.
- Kliknij przycisk **Apply** (Zastosuj).

Uwaga

Nie można edytować poszczególnych wyzwalaczy ani działań, gdy wybrano kilka reguł. Jeżeli wprowadzone zmiany spowodują niewłaściwe działanie dowolnej reguły, nie można ich zastosować.

Dodawanie wyzwalaczy

Wyzwalacze uaktywniają 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). Jeżeli korzystasz z tego ustawienia w połączeniu z wyzwalaczami impulsowymi, zwiększ okres wyzwalania. Wyzwalacze impulsowe są aktywne tylko chwilowo.

Dostępne są następujące wyzwalacze:

Detekcja ruchu – Zarejestrowanie ruchu w zdefiniowanym obszarze aktywuje wyzwalacz detekcji ruchu. Zob. *Tworzenie wyzwalaczy opartych na detekcji ruchu, on page 95*.

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.

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. *Tworzenie wyzwalaczy podglądu na żywo, on page 95*.

Zdarzenie systemowe i błąd systemowy – Wyzwalacz oparty na zdarzeniu i błędzie systemowym jest uaktywniany w przypadku błędów zapisu, zapelnienia pamięci masowej, niemożności nawiązania połączenia z siecią pamięcią masową albo utraty połączenia z jednym lub kilkoma urządzeniami. P. sekcja *Tworzenie wyzwalaczy opartych na zdarzeniach i/lub błędach systemowych, on page 96*.

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. Zob. *Tworzenie wyzwalaczy opartych na wejściach/wyjściach*, on page 97. Jeżeli jest taka możliwość, zaleca się 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 Pro nie ma odpowiedniego wyzwalacza. P. sekcja *Tworzenie wyzwalaczy opartych na zdarzeniach w urządzeniu*, on page 97.

Przycisk działania – Przyciski akcji służą do rozpoczynania i zatrzymywania działań w podglądzie na żywo. Ten sam przycisk może być używany w różnych regułach. P. sekcja *Tworzenie wyzwalaczy opartych na przyciskach akcji*, on page 102.

Zdarzenie aplikacji AXIS Entry Manager – Ten wyzwalacz aktywuje się w sytuacji, gdy AXIS Camera Station Pro odbierze sygnały z drzwi skonfigurowanych w aplikacji AXIS Entry Manager. Na przykład otwarcie drzwi siłą, otwarte zbyt długo lub odmowa dostępu. P. sekcja *Tworzenie wyzwalaczy zdarzeń aplikacji AXIS Entry Manager*, on page 104.

Zewnętrzne połączenie HTTPS – Zewnętrzny wyzwalacz HTTPS umożliwia aplikacjom zewnętrznym wyzwalanie zdarzeń w programie AXIS Camera Station Pro poprzez komunikację HTTPS. P. sekcja *Tworzenie wyzwalaczy opartych na zewnętrznych połączeniach HTTPS*, on page 104.

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 przetwarzania w AXIS Camera Station Pro.

Uwaga

Nie używaj wyzwalaczy detekcji ruchu do uruchamiania nagrań, jeżeli w kamerze jest już włączona opcja zapisu po wykryciu ruchu. 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. W oknie dialogowym:
 - 5.1. Wybierz kamerę, która ma wykrywać ruch.
 - 5.2. Ustaw minimalny odstęp czasu pomiędzy wyzwalaczami, aby ograniczyć liczbę nagrań następujących bezpośrednio po sobie. Jeżeli w tym odstępie czasu wystąpi następny wyzwalacz, zapis będzie kontynuowany, 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. Zob. *Edytowanie wbudowanej funkcji detekcji ruchu* i *Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4*.
6. Kliknij **OK**.

Tworzenie wyzwalaczy podglądu 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.

Aby utworzyć wyzwalacz 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 wybierz opcję **Live view** (Podgląd na żywo).
4. Kliknij **OK**.
5. Zaznacz kamerę powiązaną z wyzwalaczem.
6. Kliknij **OK**.

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 błędy zapisu, pełna pamięć masowa, brak połączenia z siecią 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 zapelnionej pamięci masowej	Zaznacz opcję On full storage (Przy zapelnionej pamięci masowej), aby wyzwalacz był aktywowany po zapelnieniu pamięci masowej nagrań.
W przypadku braku kontaktu z zasobem sieciowym	Zaznacz opcję On no contact with network storage (W przypadku braku kontaktu z siecią pamięcią masową), aby wyzwalacz był uaktywniany 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 uaktywniany w razie problemów z nawiązaniem łączności z kamerami. • Zaznacz opcję All (Wszystkie), aby były uwzględniane wszystkie kamery dodane do AXIS Camera Station Pro. • Wybierz opcję Selected (Wybrane) i kliknij Cameras (Kamery), aby wyświetlić listę wszystkich kamer dodanych do AXIS Camera Station Pro. W polu Select all (Zaznacz wszystko) albo Deselect all (Usuń zaznaczenie wszystkiego) zaznacz albo usuń zaznaczenie wszystkich kamer.

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 Pro, zanim użyjesz wyzwalacza WE/WY. Zob. *Porty we/wy*.
- Jeżeli jest taka możliwość, zaleca się używanie wyzwalaczy opartych na zdarzeniach w urządzeniu zamiast wyzwalaczy wejścia / wyjścia. Więcej informacji p. *Tworzenie wyzwalaczy opartych na zdarzeniach w urządzeniu, on page 97*.

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)	Ustaw minimalny odstęp czasu pomiędzy dwoma kolejnymi wyzwalaczami, aby ograniczyć liczbę nagrań następujących bezpośrednio po sobie. Jeżeli w tym odstępie czasu wystąpi następny wyzwalacz, zapis będzie kontynuowany, 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, jeżeli w AXIS Camera Station Pro nie ma odpowiedniego wyzwalacza. Zdarzenia różnią się w zależności od kamery i mają co najmniej jeden filtr, który musi być ustawiony. Filtry to warunki, które muszą zostać spełnione, aby uaktywnił 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 na przestrzeni czasu. Zdarzenie może mieć stan lub nie mieć stanu. Funkcja krokowa oznacza zdarzenie zależne od stanu. Prosta linia z impulsami oznacza zdarzenie 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)	Ustaw minimalny odstęp czasu pomiędzy dwoma kolejnymi wyzwalaczami, aby ograniczyć liczbę nagrań następujących bezpośrednio po sobie. Jeżeli w tym odstępie czasu wystąpi następny wyzwalacz, zapis będzie kontynuowany, 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	Stan
	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	Network lost (Utracono sieć)
	Ma zastosowanie tylko do zdarzeń używanych w urządzeniu, a nie zdarzeń używanych w AXIS Camera Station Pro.
	Dodano adres
	Usunięto adres
Ruch PTZ	Ruch PTZ na kanale <nazwa kanału>
Położenia zaprogramowane 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
Harmonogram	Pulse (Impuls):
	Interwał
	Zaplanowane wydarzenie
Stan	Aktywne
Pamięć masowa	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	Przełączniki 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.
Dwukrotne przeciągnięcie	Posiadacz karty dwukrotnie przeciągnął kartę. Dwukrotne przeciągnięcie karty pozwala posiadaczowi karty zmienić bieżący stan drzwi. Mogą go na przykład użyć do odblokowania drzwi poza regularnym harmonogramem.
Wykrycie Anti-passback	Ktoś użył poświadczeń należących do posiadacza karty, który wszedł do strefy przed nim.
Authorization with two-person rule (Autoryzacja za pomocą reguły dwóch osób)	
Oczekujące żądanie dostępu	Pierwszy z dwóch posiadaczy kart zidentyfikował się przy użyciu swoich danych uwierzytelniających.
Żądanie dostępu zaakceptowane	System przyznał dostęp ostatniemu posiadaczowi karty, gdy zidentyfikował go przy użyciu swoich danych uwierzytelniających.
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	System jest w stanie gotowości. Produkt Axis może wykryć na przykład stan sytemu i wysłać powiadomienie do administratora o jego uruchomieniu. Zaznacz Yes (Tak), aby wyzwolić regułę działania po wejściu produktu w stan gotowości. Reguła ta zostanie wyzwolona tylko wtedy, gdy uruchomione zostaną wszystkie wymagane usługi, takie jak system wykrywania zdarzeń.
Drzwi	
Drzwi wyważone	Po siłowym otwarciu drzwi.
Wykryto ingerencję w instalację drzwiową	Gdy system wykryje następujące stany: • Obudowa urządzenia jest otwarta lub zamknięta • Ruch urządzenia • Usunięcie dołączonego czytnika ze ściany • Sabotaż dołączonego monitora drzwi, czytnika lub urządzenia REX. Aby użyć tego wyzwalacza, sprawdź, czy włączono opcję Supervised input (Wejście nadzorowane), a rezystory końca linii założono 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 są odwiedzający, którzy powinni mieć możliwość otwierania drzwi bez potrzeby okazywania uwierzytelnień.
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 wyzwać 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 migania diody LED stanu. Zaznacz port wejściowy, który ma wyzwać regułę działania po jej uaktywnieniu, lub opcję Any (Dowolne) , aby reguła działania była wyzwalana po uaktywnieniu 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 IP traci połączenie. Dotyczy wyłącznie zdarzeń związanych z urządzeniami, a nie zdarzeń wykorzystywanych przez program AXIS Camera Station Pro.
Dodano adres	Dodanie nowego adresu IP.
Usunięto adres	Usunięcie adresu IP.
Harmonogram	
Zaplanowane wydarzenie	Zmiana stanu we wstępnie zdefiniowanym harmonogramie. Służy do zapisu obrazu 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 działania służą do rozpoczynania i zatrzymywania działań w podglądzie na żywo. Przyciski działań są wyświetlane u dołu okna 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 działań można rozmieścić podczas ich dodawania lub edytowania dla danej kamery.

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 odpowiedź. Etykieta przycisku to tekst wyświetlany na przycisku. Najedź kursorem myszy na przycisk, aby wyświetlić odpowiedź.

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

Przyciski dwustanowe – Służą do ręcznego uruchamiania i zatrzymywania działania. Przycisk ma dwa stany: przełączenie i wyłączenie. Kliknięcie przycisku powoduje przełączenie między tymi dwoma stanami. Przyciski dwustanowe domyślnie uruchamiają działanie w stanie aktywnym, ale możesz również uruchomić działanie w stanie nieaktywnym.

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

Przykład: Utwórz przycisk do otwierania i zamykania drzwi, użyj działania wyjściowego 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 odpowiedź 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 uaktywnić przycisk działania. Na przykład jeśli przycisk akcji otrzyma nazwę A_BC, w podglądzie na żywo jego nazwa zmieni się na ABC. Naciśnij klawisze Alt + B, aby uaktywnić przycisk działania.

7. Jeżeli wybrano opcję **Use existing button (Użyj istniejącego przycisku)**:
 - 7.1. Wyszukaj lub kliknij przycisk, którego chcesz użyć.
 - 7.2. Jeżeli wybrano istniejący przycisk przełączania, musisz zaznaczyć opcję **Trigger on toggle (Wyzwól przy zmianie stanu na aktywny)** lub **Trigger on untoggle (Wyzwól przy zmianie stanu na nieaktywny)**.
 - 7.3. Kliknij **Next (Dalej)**.
 - 7.4. Zmodyfikuj etykietę i odpowiedź 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 Pro uaktywnia 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 Pro 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

Zewnętrzny wyzwalacz HTTPS umożliwia aplikacjom zewnętrznym wyzwalanie zdarzeń w programie AXIS Camera Station Pro poprzez komunikację HTTPS. Ten wyzwalacz obsługuje tylko komunikację za pomocą protokołu HTTPS i wymaga w żądaniach HTTPS prawidłowej nazwy użytkownika programu AXIS Camera Station Pro, w tym nazwy domenowej i hasła.

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 oglądania obrazu. Zobacz omówienie portów komunikacji mobilnej i strumieniowania mobilnego w temacie *Ogólne ustawienia serwera*.
- Aktywacja wyzwalacza o identyfikatorze „trigger1”: `https://[address]:29204/Acs/Api/TriggerFacade/ActivateTrigger?{"triggerName":"trigger1"}`
- Dezaktywacja wyzwalacza o identyfikatorze „trigger1”: `https://[address]:29204/Acs/Api/TriggerFacade/DeactivateTrigger?{"triggerName":"trigger1"}`
- Aktywacja wyzwalacza o identyfikatorze „trigger1”, a następnie jego automatyczna dezaktywacja po 30 sekundach: `https://[address]:29204/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]:29204/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. Zobacz przykładowy adres URL, który wykorzystuje ten sam adres serwera, z którego klient loguje się do systemu. Adresy URL będą działać poprawnie dopiero po wykonaniu całej reguły akcji.
7. Kliknij **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)**.

Tworzenie wyzwalaczy funkcji Smart search 2

Aby utworzyć wyzwalacz funkcji Smart search 2:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New (Nowy)**.
3. Kliknij **Add (Dodaj)** i wybierz **Smart search 2**.
4. Kliknij **OK**.
5. Wybierz i skonfiguruj wyzwalacz:
 - Aby utworzyć filtr inteligentnego wyszukiwania, który będzie służył jako wyzwalacz, p. sekcja *Zdarzenia powodujące uruchomienie nagrywania, on page 177*.
 - Wybierz **High processing delay (Wysokie opóźnienie przetwarzania)**, aby uruchomić wyzwalacz zawsze wtedy, gdy przetworzenie wykrytych elementów zajmuje funkcji Inteligentne wyszukiwanie 2 ponad minutę.
6. Kliknij **OK**.

Tworzenie wyzwalaczy aplikacji AXIS Audio Manager

Aby utworzyć wyzwalacz w aplikacji AXIS Audio Manager:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New (Nowy)**.
3. Kliknij **Add (Dodaj)** i wybierz **Audio manager**.
4. Kliknij **OK**.
5. Wybierz i skonfiguruj wyzwalacz.
6. Kliknij **OK**.

Zmieniono stan urządzenia	Wybierz Device status changed (Zmieniono stan urządzenia), aby uruchomić wyzwalacz w przypadku zmiany stanu urządzenia na tryb online lub offline.
Zmieniono stan odtwarzania	Wybierz Playback status changed (Zmieniono stan odtwarzania), aby uruchomić wyzwalacz w przypadku rozpoczęcia lub zatrzymania odtwarzania.

Obiekt docelowy włączony lub wyłączony	Wybierz Target enabled or disabled (Obiekt docelowy włączony lub wyłączony), aby uruchomić wyzwalacz, gdy wyzwalany obiekt docelowy jest włączony lub wyłączony.
Zmieniono głośność w kontrolerze głośności	Wybierz Volume controller volume changed (Zmieniono głośność w kontrolerze głośności), aby uruchomić wyzwalacz po zmianie ustawień kontrolera głośności.

Dodawanie działań

Do jednej reguły można przypisać wiele akcji. Działania rozpoczynają się po uaktywnieniu reguły.

Dostępne są następujące akcje:

Rejestrowanie – Rozpoczyna zapis z kamery. Zob. *Tworzenie akcji nagrywania*.

Uruchom alarm – Wysła alarm do wszystkich połączonych klientów AXIS Camera Station Pro. Zob. *Tworzenie akcji zgłaszania alarmów*.

Ustaw wyjście – Ustawia stan portu wyjścia. Służy do kontrolowania urządzenia dołączonego do portu wyjścia, na przykład do włączania oświetlenia albo blokowania drzwi. Zob. *Tworzenie akcji wyjściowych*.

Wyślij wiadomość e-mail – Wysła wiadomość e-mail do jednego lub kilku odbiorców. Zob. *Tworzenie akcji wysyłania wiadomości e-mail*.

Podgląd na żywo – Otwiera podgląd na żywo z konkretnej kamery, widoku lub położenia zaprogramowanego na wszystkich połączonych klientach AXIS Camera Station Pro. Można również użyć działania podglądu na żywo, aby przywrócić otwarte klienty z paska zadań lub przesunąć je na pierwszy plan względem innych otwartych aplikacji. Zob. *Tworzenie działań podglądu na żywo*.

Wyślij zapytanie HTTP – Wysła żądania HTTP do kamery, kontrolera drzwiowego lub zewnętrznego serwera internetowego. Zob. *Tworzenie akcji wysyłania powiadomień HTTP*.

Syrena i światło – Uruchamia sygnalizator akustyczno-optyczny i sekwencję sygnalizacji optycznej na kompatybilnym urządzeniu zgodnie ze skonfigurowanym profilem. Zob. *Tworzenie akcji syreny i światła, on page 112*.

Wirtualne porty WE/WY – Wyzwala określony wirtualny port wejścia w urządzeniu. Zob. *Tworzenie akcji dotyczących wirtualnych WE/WY, on page 112*

AXIS Entry Manager – Przyznaje dostęp, odblokowuje lub blokuje drzwi dołączone do kontrolera drzwiowego skonfigurowanego przez aplikację AXIS Entry Manager. Zob. *Tworzenie akcji aplikacji AXIS Entry Manager, on page 113*.

Wyślij powiadomienie do aplikacji mobilnej – Wysła niestandardowy komunikat do aplikacji mobilnej AXIS Camera Station. Zob. *Tworzenie akcji wysyłania powiadomień do aplikacji mobilnej, on page 113*.

Włącz lub wyłącz reguły – Włącza lub wyłącza inne reguły działań. Zob. *Tworzenie akcji, która włącza lub wyłącza inne reguły akcji, on page 113*.

Wysyłanie do dekodera wideo – Wysła widok do dekodera wizyjnego w celu wyświetlenia go na monitorze przez określony czas. Zob. *Tworzenie akcji wysyłającej obszar obserwacji do dekodera wideo, on page 114*

Kontrola dostępu – Obejmuje działania dotyczące drzwi i stref występujące w aplikacji AXIS Camera Station Secure Entry. Zob. *Tworzenie akcji kontroli dostępu, on page 115*.

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, gdzie ma być zapisane nagranie, przejdź do **Configuration > Storage > Selection** (Konfiguracja > Pamięć masowa > 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)**. Zob. *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. W obszarze **Event setting (Ustawienia zdarzeń)** wybierz kategorię zdarzenia dotyczącą nagrania, o ile jest to potrzebne.
10. Kliknij **OK**.

Video setting	
Profil	Z menu rozwijanego wybierz Profile (Profil) . Aby zmodyfikować ustawienia profilu, zob. <i>Profile strumieniowania</i> .
Bufor przed zdarzeniem	Ustaw, ile sekund przed wykrytym ruchem ma zostać zarejestrowanych na nagraniu.
Bufor po zdarzeniu	Określ, 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 Pro. Alarm pojawia się na karcie **Alarms (Alarmy)** oraz jako powiadomienie na pasku zadań. Możesz dołączyć plik zawierający procedury alarmowe. 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 **Add (Dodaj)** i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i zaznacz opcję **Raise alarm (Zgłoś alarm)**.
5. Kliknij **OK**.
6. W menu **Alarm message** (Komunikat alarmowy) skonfiguruj nazwę, opis i czas trwania.
7. Skonfiguruj procedurę alarmową (**Alarm procedure**).
 - 7.1. Zaznacz opcję **On alarm show alarm procedure** (W przypadku alarmu pokaż procedurę alarmową).
 - 7.2. Kliknij przycisk **Upload (Prześlij)** i zlokalizuj plik.
 - 7.3. Kliknij **Preview (Podgląd)**, aby wyświetlić podgląd pliku.
 - 7.4. Kliknij **OK**.

Komunikat alarmowy	
Nazwa	Nadaj alarmowi nazwę. Nazwa jest wyświetlana w menu Alarms (Alarmy) na karcie Alarms (Alarmy) i w powiadomieniach na pasku 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 powiadomienia ustaw czas trwania w zakresie od 1 do 600 s.

Tworzenie akcji wyjściowych

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

Uwaga

Dodaj port wyjścia do AXIS Camera Station Pro, zanim użyjesz akcji wyjścia. Zob. *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 **Add (Dodaj)** i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *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)** ustaw, jak długo port wyjścia pozostanie 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 Keep the state for a fixed time (Utrzymywanie stanu przez ustalony czas) i podaj liczbę sekund.

Tworzenie akcji wysyłania wiadomości e-mail

Działanie e-mail powoduje wysłanie wiadomości e-mail do co najmniej jednego odbiorcy. Do wiadomości e-mail możesz załączyć ujęcia z kamer.

Uwaga

Wysyłanie wiadomości e-mail wymaga skonfigurowania serwera SMTP. Zob. *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 **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add** (Dodaj) i wybierz opcję **Send email** (Wyślij wiadomość e-mail).
5. Kliknij **OK**.
6. W obszarze **Recipients** (Odbiorcy) dodaj adresy e-mail:
 - 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 **Dodaj**.
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 **OK**.

Zaawansowane	
Attach snapshots (Dołącz ujęcia)	Aby dołączyć ujęcia z kamer w postaci załączników w standardzie .jpg, zaznacz opcję Attach snapshots (Dołącz ujęcia) i kliknij przycisk Cameras (Kamery). Zostanie wyświetlona lista wszystkich kamer dodanych do AXIS Camera Station Pro. Kliknij Select all (Zaznacz wszystko), aby zaznaczyć wszystkie kamery lub Deselect all (Usuń zaznaczenie wszystkiego), aby usunąć całe zaznaczenie.
Send one email for each event (Wyślij jeden e-mail dla każdego zdarzenia)	Aby uniemożliwić wysyłanie 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 uniknąć wysyłania wiadomości e-mail w zbyt krótkich odstępach czasu, wybierz opcję Don't send another email for (Nie wysyłaj kolejnej wiadomości przez) i w rozwijalnym menu ustaw minimalny czas pomiędzy wiadomościami.

Tworzenie działań podglądu na żywo

Działanie podglądu na żywo otwiera określoną kamerę, widok lub położenie zaprogramowane na karcie **Live view** (Podgląd na żywo) we wszystkich dołączonych klientach AXIS Camera Station Pro. Jeżeli karta **Live view** (Podgląd na żywo) wyświetla widok dzielony z aktywnym punktem, w punkcie pojawi się obraz z kamery wybranej w działaniu podgląd na żywo. Więcej informacji na temat aktywnych punktów: *Widok dzielony*.

Można również użyć działania podglądu na żywo, aby przywrócić otwarte klienty AXIS Camera Station Pro 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 **Add (Dodaj)** i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add (Dodaj)** i wybierz opcję **Live view (Podgląd na żywo)**.
5. Kliknij **OK**.
6. W obszarze **Live view actions** (Działania widoku na żywo) zdecyduj, co ma być wyświetlane po uruchomieniu działania.
7. W obszarze **Shown in (Pokaż w)** zdecyduj, jak ma być wyświetlany wybrany widok.
8. W obszarze **Bring to front** (Przesuń na wierzch) zaznacz opcję **On trigger bring application to front** (Po zadziałaniu wyzwalacza przesun aplikację na wierzch), aby po rozpoczęciu działania okna otwartych klientów AXIS Camera Station Pro były przywracane z paska zadań lub przenoszone na pierwszy plan względem okien innych otwartych aplikacji.
9. Kliknij **OK**.

Akcje podglądu na żywo	
Wyświetl	Wybierz View (Widok) , a następnie wybierz widok z menu rozwijalnego.
Kamera	Wybierz Camera (Kamera) , a następnie wybierz kamerę z rozwijalnego menu. Jeżeli kamera ma zdefiniowane położenie zaprogramowane PTZ, kliknij opcję Go to preset (Przejdź do położenia zaprogramowanego) i wybierz obszar z menu rozwijalnego, aby otworzyć położenie zaprogramowane.
No action (Bez akcji)	Wybierz No action (Brak działania), jeżeli nie chcesz otwierać 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 działania, pojawi się w nim widok z kamery.

Przykład:

W tym przykładzie wykorzystano dwa działania podglądu na żywo w tej samej regule działania.

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 przesun aplikację na wierzch).
2. Utwórz kolejne działanie podglądu na żywo, tym razem powodujące przechodzenie do widoku aktywnego punktu i wyświetlanie w nim widoku z kamery.

- 2.1. W obszarze **Live view actions** (Działania podglądu na żywo) wybierz opcję **Camera** (Kamera), a następnie widok z 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. Za pomocą powiadomień HTTP możesz przykładowo włączyć lub wyłączyć daną funkcję w kamerze albo otworzyć, zamknąć, zablokować lub odblokować drzwi dołączone do kontrolera drzwiowego.

Obsługiwane są metody GET, POST i PUT.

Uwaga

Aby powiadomienia HTTP były wysyłane do odbiorców spoza sieci lokalnej, może być potrzebne dostosowanie ustawień serwera proxy AXIS Camera Station Pro. W celu uzyskania dalszych informacji skontaktuj się ze wsparciem Axis.

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 **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *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. Wybierz metodę uwierzytelniania.
9. Kliknij przycisk **Advanced** (Zaawansowane), aby wyświetlić ustawienia zaawansowane.
10. Kliknij **OK**.

Metoda uwierzytelniania	
Skrót	Zaleca się skorzystanie z tej opcji, ponieważ zapewnia ona najlepszą ochronę przed podsłuchem.
Skrót z metodą podstawową jako rozwiązanie awaryjne	Użyj tej opcji, jeśli nie wiesz, jakiej metody uwierzytelniania używa urządzenie.

Zaawansowane	
Metoda	Wybierz metodę HTTP z menu rozwijalnego Method (Metoda).
Typ zawartości	W przypadku metod POST i PUT przejdź do menu rozwijanego Content type (Typ zawartości) i wybierz rodzaj zawartości.

Zaawansowane	
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.

Trigger data (Dane wyzwalania)	
Type (Typ):	Wyzwalacz, który aktywował tę regułę akcji.
Source ID (Identyfikator źródła)	Określa źródło, które wyzwoliło regułę działania. Często jest to kamera lub innego rodzaju urządzenie. Nie wszystkie źródła mogą pełnić tę funkcję.
Source Name (Nazwa źródła)	Nazwa źródła, które wyzwoliło regułę działania. Często jest to kamera lub innego rodzaju urządzenie. Nie wszystkie źródła mogą pełnić tę funkcję.
Godzina (UTC)	Podaje datę i godzinę UTC wyzwolenia reguły alarmu.
Time (local) (Czas lokalny)	Data i godzina wyzwolenia reguły akcji przez serwer.

Tworzenie akcji dotyczących wirtualnych WE/WY

Użyj działań dotyczących wirtualnych we / wy, aby uaktywnić określony wirtualny port wejścia w urządzeniu. Każdy port urządzenia może być używany w przypadku jednej akcji.

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules (Konfiguracja > Zapis i zdarzenia > Reguły akcji)**.
2. Kliknij **New (Nowy)**.
3. Kliknij **Add (Dodaj)** i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *Dodawanie wyzwalaczy*.
4. Kliknij **Add (Dodaj)** i wybierz **Virtual I/O (Wirtualne WE/WY)**.
5. Kliknij **OK**.
6. Wybierz urządzenie i port do uaktywnienia.
7. Kliknij **OK**.

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 **Add (Dodaj)** i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *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

Działanie aplikacji AXIS Entry Manager przyznaje dostęp oraz odblokowuje i blokuje zamki drzwi połączonych z kontrolerem drzwiowym skonfigurowanym przez aplikację AXIS Entry Manager.

Uwaga

Akcja aplikacji AXIS Entry Manager jest dostępna tylko wtedy, gdy w AXIS Camera Station Pro 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 **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *Dodawanie wyzwalaczy*.
4. Kliknij przycisk **Add** (Dodaj) i zaznacz pozycję **AXIS Entry Manager** (**AXIS Entry Manager**).
5. Kliknij **OK**.
6. Wybierz działanie i drzwi, do których ma zostać zastosowane.
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. Możesz kliknąć otrzymane powiadomienie, aby 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 **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *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** (Komunikat) wpisz treść komunikatu, jaki ma się wyświetlić w aplikacji mobilnej.
7. W obszarze **Click notification and go to** (Kliknij powiadomienie i przejdź do) określ, co się wyświetli po kliknięciu powiadomienia.
8. Kliknij **OK**.

Kliknij powiadomienie i przejdź do	
Kamera	Wybierz widok z kamery, który ma się wyświetlić po naciśnięciu powiadomienia.
Domyślne	Zaznacz opcję Default (Domyślnie), aby naciśnięcie powiadomienia powodowało przejście do strony startowej aplikacji mobilnej.

Tworzenie akcji, która włącza lub wyłącza inne reguły akcji

Za pomocą tego działania można na przykład wyłączyć detekcję ruchu w biurze, gdy pracownik okaże swoją kartę dostępu.

Aby utworzyć działanie 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 **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *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 działania.
7. Zdecyduj, czy wybrane reguły działania mają być włączone czy wyłączone.
8. Jeżeli chcesz dodać 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), jeżeli nie chcesz, aby reguła działania 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 **OK**.

Tworzenia zakładki działania

Działanie dodania zakładki powoduje dodanie zakładki do nagrania w chwili uruchomienia reguły działania.

Aby utworzyć zakładkę działania:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
2. Kliknij **New** (Nowy).
3. Kliknij **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *Dodawanie wyzwalaczy*.
4. Kliknij **Add (Dodaj)** i wybierz **Add bookmark** (Dodaj zakładkę).
5. Kliknij **OK**.
6. Skonfiguruj zakładkę, wprowadzając nazwę i opcjonalnie opis.
7. Kliknij **OK**.

Tworzenie akcji wysyłającej obszar obserwacji do dekodera wideo

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

Aby utworzyć działanie wysyłania do dekodera wizyjnego:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
2. Kliknij **New** (Nowy).
3. Kliknij **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next (Dalej)**. Zob. *Dodawanie wyzwalaczy*.
4. Kliknij **Add (Dodaj)** i wybierz **Send to video decoder** (Wyślij do dekodera wideo).
5. Kliknij **OK**.
6. W sekcji **Decoder (Dekoder)** wybierz dekodera wideo, do którego chcesz wysłać obszar obserwacji.
7. W sekcji **View (Obszar obserwacji)** wybierz kamerę lub obszar obserwacji do wysłania.
8. W polu **Duration** (Czas trwania) wpisz czas wyświetlania widoku w sekundach.
9. Kliknij **OK**.

Tworzenie akcji kontroli dostępu

Działanie kontroli dostępu może powodować wykonywanie następujących czynności w programie AXIS Camera Station Secure Entry:

- **Działania dotyczące drzwi:** przyznawanie dostępu oraz blokowanie, odblokowywanie, resetowanie i odcinanie obszaru wybranych drzwi.
- **Działania dotyczące stref:** blokowanie, odblokowywanie, resetowanie lub odcinanie obszaru wybranych drzwi w wybranych strefach.
- **Działania dotyczące reguł dostępu:** włączanie i wyłączanie reguł dostępu.

Uwaga

Działanie dotyczące kontroli dostępu jest dostępne tylko w programie AXIS Camera Station Secure Entry.

Aby utworzyć działanie dotyczące kontroli dostępu:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
2. Kliknij **New** (Nowy).
3. Kliknij **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *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. Aby włączyć lub wyłączyć reguły dostępu:
 - 8.1. W sekcji **Access control** (Kontrola dostępu) wybierz **Action rule actions** (Akcje reguł akcji).
 - 8.2. W sekcji **Configure action** (Skonfiguruj akcję) wybierz regułę akcji, którą chcesz włączyć lub wyłączyć.
 - 8.3. W obszarze **Action** (Działanie) wybierz **Enable** (Włącz) lub **Disable** (Wyłącz).
9. Kliknij **OK**.
 - Aby zapisać raport w ramach akcji, wybierz **Save report** (Zapisz raport) i skonfiguruj ustawienia raportu.

Tworzenie działań aplikacji AXIS Audio Manager

Działanie w aplikacji AXIS Audio Manager steruje odtwarzaniem dźwięku i ustawieniami głośności w dołączonych urządzeniach fonicznych.

Aby utworzyć działanie w aplikacji AXIS Audio Manager:

1. Wybierz kolejno opcje **Configuration > Recording and events > Action rules** (Konfiguracja > Zapis i zdarzenia > Reguły akcji).
2. Kliknij **New** (Nowy).
3. Kliknij **Add** (Dodaj) i skonfiguruj wyzwalacz. Kliknij **Next** (Dalej). Zob. *Dodawanie wyzwalaczy*.
4. Kliknij **Add** (Dodaj) i wybierz **Audio manager**.
5. Kliknij **OK**.
6. Wybierz i skonfiguruj działanie, które chcesz uruchomić.
7. Kliknij **OK**.

Działania aplikacji AXIS Audio Manager	
Odtwarzaj plik foniczny	Wybierz Play audio file (Odtwarzaj plik foniczny), aby odtworzyć wybrany plik foniczny. Możesz również skonfigurować parametry odtwarzania takie jak liczba powtórzeń, priorytet i profil wizualny.
Zatrzymaj plik foniczny	Wybierz Stop audio file (Zatrzymaj plik foniczny), aby zatrzymać odtwarzanie dźwięku.
Włącz lub wyłącz urządzenia	Wybierz Enable or disable target (Włącz lub wyłącz urządzenia), aby włączyć lub wyłączyć urządzenia.
Wycisz	Wybierz Mute volume (Wycisz), aby wyciszyć dźwięk w kontrolerze głośności.
Ustaw głośność	Wybierz Set volume (Ustaw głośność), aby ustawić głośność za pomocą regulatora głośności. Wybrana wartość może być dodatnia lub ujemna.
Różnica głośności	Wybierz Offset volume (Różnica głośności), aby wyregulować głośność w stosunku do bieżącego poziomu. Wprowadź wartość dodatnią, aby zwiększyć głośność, lub ujemną, aby ją zmniejszyć.

Harmonogramy

Strona Schedules (Harmonogramy) zawiera wszystkie harmonogramy, które możesz zastosować do zapisu, reguł działań oraz komponentów w rodzaju aplikacji AXIS Secure Entry. Niektóre harmonogramy są tworzone automatycznie w czasie instalacji przez aplikację AXIS Site Designer.

Możesz utworzyć i edytować spersonalizowane harmonogramy dzienne i tygodniowe, a także harmonogramy 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:

- **Name (Nazwa):** Nazwa harmonogramu.
- **Type (Rodzaj):** Wskazuje, czy harmonogram jest harmonogramem dziennym czy tygodniowym.
- **In use (W użyciu):** Wskazuje, czy komponent, reguła zapisu lub reguła działania aktualnie korzysta z harmonogramu.
- **Override schedules (Harmonogramy nadpisywania):** Wyświetla listę harmonogramów nadpisywania, które mają zastosowanie do tego harmonogramu.

Karta **Override schedules (Harmonogramy nadpisywania)** to widok główny umożliwiający zarządzanie harmonogramami nadpisywania, w którym można zobaczyć, których harmonogramów dziennych i tygodniowych dotyczy nadpisywanie.

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station Pro można dodawać harmonogramy i zarządzać nimi na dowolnym połączonym serwerze. Wybierz serwer z menu rozwijalnego **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 usunięciem sprawdź, czy harmonogram nie jest aktualnie w użyciu.

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 ten przedstawia ustawienia w AXIS Camera Station Pro reguły działania, która wyzwala zapis i alarm, gdy ktoś wyważy drzwi wejściowe.

Zanim zaczniesz:

- Zainstaluj sieciowy kontroler drzwiowy Axis. Zob. *Dodawanie urządzeń*, on page 47.
- Skonfiguruj kontroler drzwi. P. sekcja *Dodaj drzwi*, on page 152.

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 zdarzenie drzwi wyważone jako wyzwalacz:
 - 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)** sprawdź, czy 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 rozwijanym 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) .

Ustawienia wizyjne	
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 ten przedstawia utworzenie w AXIS Camera Station Pro reguły działania, która powoduje odtworzenie wiadomości powitalnej i wezwanie windy, gdy wchodzi ktoś ważny.

Zanim zaczniesz:

- Zainstaluj i skonfiguruj sieciowy kontroler drzwiowy Axis i dodaj posiadaczy kart. Zob. *Skonfiguruj kontrolę dostępu, on page 148* i *Zarządzanie dostępem, on page 185*.
- Zainstaluj sieciowe urządzenie foniczne Axis i powiąż je z kamerą. Zob. *Profile strumieniowania, on page 55*.

- 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 Pro. Zob. *Porty we/wy, on page 92*.

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 zdarzenie związane z urządzeniem jako wyzwalacz:
 - 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) sprawdź, czy wyzwalacz pokazuje aktywność na linii sygnałowej.
 - 3.6. Kliknij **OK**.
4. Kliknij **Next** (Dalej).
5. Dodaj działanie wysyłania powiadomienia 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 działanie Ustaw wyjście:
 - 6.1. Kliknij przycisk **Add** (Dodaj) i wybierz opcję **Set output** (Ustaw wyjście).
 - 6.2. Kliknij **OK**.
 - 6.3. W menu rozwijalnym **Output port** (Port wyjściowy) zaznacz port wyjściowy modułu we / wy, który jest dołączony 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. Wybierz **Pulse** (Impuls) i ustaw czas trwania na 60 s.
 - 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	Wybierz Card number (Numer karty) i wpisz numer karty danej osoby.

Konfigurowanie klienta

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

- Edytować ustawienia klienta w rodzaju motywu i języka. Zob. *Ustawienia klienta, on page 120*.
- Edytować ustawienia użytkownika w rodzaju powiadomień i opcji uruchamiania. Zob. *Ustawienia użytkownika, on page 121*.
- Edytować ustawienia wydajności strumieniowania specyficzne dla klienta w rodzaju skalowania obrazu i dekodowania sprzętowego. Zob. *Przesyłanie strumieniowe, on page 123*.

Ustawienia klienta

Ustawienia te mają zastosowanie do wszystkich użytkowników aplikacji AXIS Camera Station Pro na komputerze. Przejdź do **Configuration > Client > Client settings (Konfiguracja > Klient > Ustawienia klienta)**.

Schemat	
System, Light, Dark (Systemowy, Jasny, Ciemny)	Wybierz wizualny motyw przewodni interfejsu klienta. Domyślnym motywem dla nowych instalacji jest System (Systemowy) . Jeżeli wybierzesz System , motyw zostanie dostosowany do motywu systemowego Windows.

Zapisy ogólne	
Uruchom aplikację po uruchomieniu systemu Windows	Włącz, aby program AXIS Camera Station Pro uruchamiać automatycznie wraz z uruchomieniem systemu Windows.

Podgląd na żywo	
Pokaż nazwy kamer w podglądach na żywo	Wyświetla nazwy kamer w podglądzie na żywo.
	Włącz Show recording indicators in live views and maps (Pokaż wskaźniki nagrań w podglądzie na żywo i na mapach) , aby wyświetlać wskaźniki nagrań z detekcji ruchu lub nagrań uruchomionych przez regułę działania.
	Włącz Show event indicators in live views and maps (Pokaż wskaźniki zdarzeń w podglądzie na żywo i na mapach) , aby wyświetlać wskaźniki nagrań z detekcji ruchu lub nagrań uruchomionych przez regułę działania.

Mapy	
Allow flashing coverage areas for all maps (Zezwalaj na migające obszary pokrycia dla wszystkich map)	Włącz lub wyłącz to ustawienie, aby określić, czy obszary pokrycia mają migać na wszystkich mapach. To ustawienie globalne nie wpływa na ustawienia lokalne na poziomie mapy. Zob. <i>Mapa, on page 23</i> .

Język
Zmiana języka klienta AXIS Camera Station Pro. Aby zmiana zaczęła obowiązywać, uruchom ponownie 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 użytkownika klienta, co pomoże nam usprawnić aplikację i korzystanie z niej)	Pozwala udostępniać firmie Axis anonimowe dane w celu ich wykorzystywania do poprawy jakości jej produktów konsumenckich. Aby zmienić to ustawienie serwera, p. sekcja <i>Ustawienia serwera, on page 127</i> .

Ustawienia użytkownika

Te ustawienia dotyczą użytkowników zalogowanych w programie AXIS Camera Station Pro. Przejdź do **Configuration > Client > User settings** (Konfiguracja > Klient > Ustawienia użytkownika).

System nawigacji	
System nawigacji z widokiem drzewka	Domyślnie włączone. Wyświetla widoki, kamery lub jedno i drugie w okienku nawigacyjnym.
Show in navigation (Pokaż w nawigacji)	W menu rozwijalnym wybierz, co chcesz wyświetlić: widoki, kamery lub jedno i drugie.
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 tę 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 po dodaniu lub zakończeniu zadania.
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 dołączonym domofonie.

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 Pro w trybie pełnoekranowym.
Zapamiętaj ostatnio używane karty	Włącz, aby uruchomić program AXIS Camera Station Pro z tymi samymi otwartymi kartami, widokami i kamerami, które były otwarte w chwili ostatniego zamknięcia.
Zapamiętaj ostatnio używane monitory	Włącz, aby uruchomić program AXIS Camera Station Pro na tym samym monitorze, który był używany przy ostatnim zamknięciu programu.

Uwaga

- System zapisuje widoki i widoki kamer są zapisywane dla poszczególnych kart. System zapamiętuje te ustawienia tylko wtedy, gdy komputer kliencki połączy się z tym samym serwerem.
- 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)	Zaznacz tę opcję, aby po wyzwoleniu alarmu nie odtwarzać dźwięku.
Beep (Sygnał dźwiękowy)	Zaznacz tę opcję, aby po wyzwoleniu alarmu odtworzyć sygnał dźwiękowy.
Sound file (Plik dźwiękowy)	Zaznacz tę opcję i kliknij przycisk Browse (Przeglądaj), aby ustawić własny plik dźwiękowy odtwarzany po wyzwoleniu alarmu. Obsługuje wszystkie standardy plików zgodne z programem Windows Media Player.
Odtwarzaj	Kliknij, aby przetestować dźwięk.

Włącz dźwięk połączenia przychodzącego	
No sound (Brak dźwięku)	Zaznacz tę opcję, aby nie odtwarzać sygnału dźwiękowego przy połączeniu przychodzącym.
Beep (Sygnał dźwiękowy)	Zaznacz tę opcję, aby przy połączeniu przychodzącym odtwarzany był sygnał dźwiękowy.

Włącz dźwięk połączenia przychodzącego	
Sound file (Plik dźwiękowy)	Zaznacz opcję i kliknij przycisk Browse (Przeglądaj), aby ustawić własny plik dźwiękowy odtwarzany przy połączeniu przychodzącym. Obsługuje wszystkie standardy plików zgodne z programem Windows Media Player.
Odtwarzaj	Kliknij, aby przetestować dźwięk.

Cechy	
Pokaż inteligentne wyszukiwanie 1	Wyświetlane domyślnie. Wyłącz, aby ukryć Inteligentne wyszukiwanie 1.

Pokazuj okna dialogowe ostrzeżeń	
Ostrzeżenie o nieprawidłowym certyfikacie	Włącz tę opcję, aby wyświetlać ostrzeżenie w przypadku wykrycia nieprawidłowego certyfikatu.

Przesyłanie strumieniowe

Przejdź do **Configuration > Client > Streaming** (Konfiguracja > Klient > Strumieniowanie), aby skonfigurować opcje strumieniowania.

Skalowanie obrazu	
Skaluj, aby dopasować	Pozwala dopasować obraz do dostępnego miejsca bez przycinania lub zamiany współczynnika proporcji.
Wypełnij obszar obrazu (może przyciąć część obrazu)	Zaznacz, aby wypełnić obrazem dostępną przestrzeń. Jeżeli współczynnik proporcji dostępnej przestrzeni różni się od współczynnika proporcji obrazu, system przycina obraz w taki sposób, aby go dopasować.

Dekodowanie sprzętowe									
Tryb	Automatic (Automatyczny): Strumień w rozdzielczościach ponad 3840 x 2160p przy 25 obrazach/s (nazywanej również 4K lub UHD) są dekodowane przy użyciu karty graficznej. On (Wł.): Strumień w rozdzielczościach ponad 1920 x 1080p przy 25 obrazach/s (nazywanej również 1080p lub HD) są dekodowane przy użyciu karty graficznej. Off (Wyłączone): Program AXIS Camera Station Pro wykorzystuje procesor do dekodowania obrazu.								
Karta graficzna	Wybierz kartę graficzną z menu rozwijanego. <table border="1"> <thead> <tr> <th>Obsługiwane karty graficzne</th><th>Technologia dekodera</th></tr> </thead> <tbody> <tr> <td>NVIDIA</td><td>PureVideo</td></tr> <tr> <td>AMD</td><td>Unified Video Decoder (UVD)</td></tr> <tr> <td>Intel</td><td>Intel Quick Sync Video (QSV)</td></tr> </tbody> </table>	Obsługiwane karty graficzne	Technologia dekodera	NVIDIA	PureVideo	AMD	Unified Video Decoder (UVD)	Intel	Intel Quick Sync Video (QSV)
Obsługiwane karty graficzne	Technologia dekodera								
NVIDIA	PureVideo								
AMD	Unified Video Decoder (UVD)								
Intel	Intel Quick Sync Video (QSV)								

Uwaga

- Dekodowanie sprzętowe wykorzystuje kartę graficzną do dekodowania obrazu. Dzięki karcie graficznej o wysokiej wydajności dekodowanie sprzętowe może poprawić działanie i zmniejszyć obciążenie procesora, w szczególności przy strumieniowaniu w wysokiej rozdzielczości. Dekodowanie sprzętowe obsługuje wyłącznie strumień w standardach H.264 i AV1.
- Dekodowania sprzętowego nie mogą stosować kamery o rozdzielczości mniejszej niż 1080p, nawet jeżeli jest włączone.
- Jeżeli karta graficzna nie obsługuje dekodowania 4K, funkcja ta działa tylko w strumieniach o rozdzielczości 1080p, nawet jeżeli jest włączona.
- Do dekodowania sprzętowego wykorzystywana jest tylko jedna karta graficzna nawet w systemach wyposażonych w kilka kart graficznych.

Wykorzystanie przepustowości	
Zawsze używaj profilu strumienia Niski w tym kliencie	Pozwala używać profilu Low (Niski) w podglądzie na żywo. Zob. <i>Profile strumieniowania</i>. To ustawienie wpływa na obraz w standardach H.264 oraz M-JPEG i obniża wykorzystanie przepustowości.
Wstrzymaj strumień wideo w nieaktywnych kartach	Włącz, aby zawiesić strumień wideo na nieaktywnych kartach. Dzięki temu obniża się wykorzystanie przepustowości.

PTZ (obrót, pochylenie, zbliżenie)	
Wybierz widok po pierwszym kliknięciu zamiast uruchamiać PTZ	Włącz, aby pierwsze kliknięcie w widoku powodowało zaznaczenie go. Kolejne kliknięcia sterują funkcjami PTZ.

Dźwięk	
Push-to-talk release delay (ms) (Opóźnienie zwalniania push-to-talk (ms))	Określa, jak długo (w milisekundach) dźwięk przesyłany jest 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	Włącz, aby słuchać i rozmawiać przez domofony nawet przy braku połączeń przychodzących.

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

Zarządzanie połączonymi usługami

Dzięki funkcji Połączone usługi dostępne są:

- Klient internetowy oprogramowania AXIS Camera Station
- Zarządzanie urządzeniami
- Automatycznego zarządzania licencjami
- Monitorowanie stanu systemu

Aby korzystać z tych usług, musisz zarejestrować system i połączyć go z organizacją. Więcej informacji p. *Rejestracja systemu w organizacji, on page 125.*

Status	Karta stanu pokazuje stan połączenia pomiędzy serwerem a połączonymi usługami oraz nazwę organizacji, w której jesteś zarejestrowany.
Rozłącz	Po rozłączeniu serwer będzie nadal zarejestrowany w organizacji.
License management (Zarządzanie licencjami)	Włącz funkcję License management (Zarządzanie licencjami) , aby automatycznie synchronizować licencje. System przesyła zmiany dotyczące licencji do aplikacji AXIS License Manager i pobiera zaktualizowany stan licencji. Wyłącz funkcję License management (Zarządzanie licencjami) , aby ręcznie zarządzać licencjami, np., gdy system nie ma połączenia z internetem. Więcej informacji znajduje się w sekcji Zarządzanie licencjami. Więcej informacji p. <i>Zarządzaj licencjami, on page 136.</i>
Synchronize system (Synchronizacja systemu)	Włącz funkcję Synchronize system (Synchronizuj system) , aby automatycznie synchronizować urządzenia i widoki z klientem sieciowym aplikacji AXIS Camera Station i AXIS Device Manager.

Rejestracja systemu w organizacji

Aby zarejestrować system:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Connected services (Połączone usługi) > Management (Zarządzanie)**.
2. Kliknij **Register (Zarejestruj)** and i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

Aby uzyskać więcej informacji o rejestracji systemu, zapoznaj się z *Instrukcją instalacji i migracji AXIS Camera Station Pro*.

Ustawienia aktualizacji oprogramowania sprzętowego

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station Pro 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)	Wybierz Every start-up (Przy każdym uruchomieniu), aby sprawdzać dostępność nowych wersji oprogramowania układowego przy każdym uruchomieniu serwera. Domyślne ustawienie w AXIS Camera Station Pro 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 wolniej, 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).



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

Włącz automatyczne sprawdzanie dostępności nowych wersji oprogramowania sprzętowego

Axis Secure Remote Access v2

Axis Secure Remote Access v2 umożliwia nawiązanie połączenia z serwerem AXIS Camera Station Pro za pośrednictwem zaszyfrowanego połączenia internetowego.

Uwaga

Funkcja Axis Secure Remote Access v2 jest dostępna w aplikacji AXIS Camera Station Pro w wersji 6.8 i nowszych.

Aby włączyć funkcję Axis Secure Remote Access v2:

1. Zarejestruj serwer w organizacji. Zob. *Rejestracja systemu w organizacji, on page 125*.
2. Zaloguj się z wykorzystaniem funkcji Axis Secure Remote Access v2. Zob. *Logowanie do funkcji AXIS Secure Remote Access v2, on page 9*.

Aby ograniczyć dostęp wyłącznie do serwerów AXIS Camera Station Pro:

1. Przejdź do **Organization > Users** (Organizacja > Użytkownicy) w My Systems.
2. Wybierz użytkownika, którego chcesz skonfigurować.
3. Kliknij **Roles and access** (Role i dostęp).
4. Przydziel rolę **ACS Pro Secure Remote Access**. Rola ta ogranicza dostęp tylko do serwerów AXIS Camera Station Pro bez dostępu do innych funkcji Axis My Systems.

Po zarejestrowaniu można zarządzać uprawnieniami dostępu, przydzielając role użytkownikom organizacji w Axis My Systems. Więcej o uprawnieniach dostępu użytkowników programu AXIS Camera Station Pro, p. sekcja *Uprawnienia użytkownika, on page 138*.

Pamięć masowa w chmurze

AXIS Camera Station Cloud Storage to licencjonowana usługa do przechowywania nagrań w chmurze. Więcej informacji, p. *AXIS Camera Station Cloud Storage – instrukcja obsługi*.

Ważne

Usługa AXIS Camera Station Cloud Storage współpracuje wyłącznie z programem AXIS Camera Station Pro w wersji 6.18 lub starszej. Zaleca się wyeksportowanie nagrań do lokalnej pamięci masowej przed aktualizacją. W przypadku aktualizacji do wersji wyższej niż 6.18 usługa przechowywania danych w chmurze przestanie działać i utracisz wszystkie dane obecnie przechowywane w chmurze. Aktualizacje zabezpieczeń dla wersji 6.18 będą kontynuowane do momentu przywrócenia obsługi pamięci masowej w chmurze w jednej z kolejnych wersji.

Zanim zaczniesz korzystać z usługi przechowywania nagrań w chmurze, musisz zarejestrować Twój system w ramach połączonych usług. Po zarejestrowaniu systemu możesz zarządzać nagraniami z kamer w chmurze na platformie My Systems.

Konfigurowanie serwera

Ustawienia serwera

Przejdź do **Configuration > Server** (Konfiguracja > Serwer).

Uwaga

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

Eksportuj...	
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 dzienników kontroli. Ustaw wartość pomiędzy 7 a 1000 dni.	
Aby w trybie ciągłym zapisywać dzienniki do pliku w czasie rzeczywistym w celu wykorzystania ich przez systemy innych producentów, takie jak Splunk, Elastic lub narzędzie SIEM, wybierz opcję Write audit logs to file (Zapisywanie dzienników kontroli do pliku), opcję Write event logs to file (Zapisywanie dzienników zdarzeń do pliku) lub obie te opcje.	
Serwer zapisuje wpisy dziennika w pliku C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Server\Logs. Pliki te mają postać zwykłego tekstu i nie są uwzględniane w raportach systemowych.	
Plik	Opis
AcsService.exe.audit.log.export	Wpisy dziennika audytu
AcsService.exe.event.log.export	Wpisy dziennika zdarzeń

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 uaktywnianiu reguł działań.

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 polu **Sender (Nadawca)** wpisz adres e-mail oraz nazwę, która ma być wyświetlana jako nadawca.

Serwer	
Adres	Wprowadź adres IP serwera SMTP.
Port	Wprowadź portu Domyślnym portem dla połączeń protokołu SMTP TLS jest port 587.
Use TLS (Użyj TLS)	Zaznacz tę opcję, jeśli serwer SMTP korzysta z protokołu TLS. TLS jest protokołem domyślnym.
Użyj uwierzytelniania	Zaznacz, czy serwer wymaga podania nazwy użytkownika i hasła, a następnie wprowadź dane logowania.

Edycja	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 oknie dialogowym kliknij przycisk Yes (Tak) , aby usunąć serwer.

Test all... (Testuj wszystkie)	Aby przetestować serwer SMTP, zaznacz go i kliknij przycisk Test all... (Testuj wszystkie) . W oknie dialogowym 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 za pomocą strzałek ustaw kolejność. System łączy się z serwerami w podanej kolejności.

Wyniki testów serwera	
OK	Połączenie z serwerem SMTP zostało nawiązane. Sprawdź, czy adresaci otrzymali testową wiadomość e-mail.
Nieznany błąd	Podczas wysyłania wiadomości e-mail wystąpił nieznany błąd. Sprawdź, czy serwer SMTP działa poprawnie.
Brak kontaktu	AXIS Camera Station Pro nie może połączyć się z serwerem SMTP. Sprawdź, czy serwer SMTP działa i czy routery oraz serwery proxy pomiędzy AXIS Camera Station Pro 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	Przy negocjacji TLS / SSL wystąpił błąd, np. nieprawidłowy certyfikat serwera.
Authentication required (Wymagane uwierzytelnienie)	Serwer wymaga uwierzytelniania do wysyłania poczty e-mail.
Błąd uwierzytelniania	Poświadczenia są niepoprawne.
Połączenie przerwane	Połączenie zostało nawiązane, lecz następnie zostało utracone.

Alarm systemowy

Alarm systemowy występuje, gdy kamera traci połączenie, nie ma dostępu do pamięci masowej nagrań, serwer nieoczekiwanie się wyłącza lub występują błędy zapisu. Możesz wysłać powiadomienia e-mailowe dotyczące alarmów systemowych.

Uwaga

W tym celu należy najpierw dodać serwer SMTP.

Aby wysłać wiadomość e-mail informującą 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 skonfigurować powiadomienia 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)**, aby zapisać adres e-mail w polu **Recipients (Odbiorcy)**.

Połączenie z urządzeniem	
W miarę możliwości używaj nazw hostów zamiast adresu IP dla nowo dodanych urządzeń	W miarę możliwości używa nazw hostów do łączenia się z nowo dodanymi urządzeniami. Jeśli nazwa hosta jest niedostępna, zamiast niej używany jest adres IP.
Zachowuj niedostępne nazwy hostów	Aby nawiązać połączenie, użyj nazwy hosta. Aby zamiennie automatycznie przełączać na adres IP, usuń zaznaczenie z pola wyboru. Można ręcznie ustawić, aby łączność z urządzeniami była nawiązywana przy użyciu nazwy hosta lub adresu IP. Zob. <i>Połączenie, on page 72</i> .

Język	
Zmień język serwera	Zmienia język AXIS Camera Station Pro Service Control i AXIS Camera Station Secure Entry. Na przykład, alarmy systemowe, komunikaty dziennika kontroli i zewnętrzne dane na karcie Data search (Wyszukiwanie danych). Aby zmiana zaczęła obowiązywać, uruchom ponownie serwer.

Urządzenia nasobne	
Dysk Folder	Wybierz dysk i folder do przechowywania odrzuconych treści z systemu nasobnego. Więcej informacji można znaleźć w sekcji <i>Przesyłanie nagrań do lokalizacji przechowywania odrzuconej zawartości w Instrukcji obsługi rozwiązania nasobnego Axis</i> .
Liczba dni przetrzymywania odrzuconej zawartości z systemu nasobnego.	Ustawia liczbę dni przetrzymywania odrzuconej treści z systemu nasobnego.

Informacja zwrotna	
Prześlij anonimowe dane dotyczące użytkowania serwera do Axis Communications	Zaznacz tę opcję, aby przekazywać do Axis anonimowe dane, co pomoże nam usprawniać aplikację i korzystanie z niej. Aby zmienić to ustawienie dla klienta, p. sekcja <i>Ustawienia klienta, on page 120</i> .

Ustawienia zaawansowane

Ustawienia te zmieniaj wyłącznie na podstawie instrukcji z działu pomocy technicznej Axis. Aby zmienić ustawienie zaawansowane:

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

Aby włączyć rejestrowanie debugowania na potrzeby rozwiązywania problemów, zaznacz opcję **Enable server side debug logging** (Włącz rejestrowanie usuwania błędów po stronie serwera). To ustawienie powoduje zajęcie większej ilości miejsca na dysku. Plik `log4net.config` znajdujący się w katalogu **ProgramData** ma tu pierwszeństwo.

Aby uzyskać więcej informacji, patrz *Advanced server setting (Zaawansowane ustawienia serwera)* w przewodniku rozwiązywania problemów dotyczących oprogramowania **AXIS Camera Station Pro**.

Składniki

Elementy to moduły oprogramowania rozszerzające możliwości systemu. Strona **Components (Elementy)** umożliwia zarządzanie elementami (lub komponentami) i wyświetlanie ich stanu.

Aby wyświetlić listę zainstalowanych elementów:

1. Wybierz kolejno opcje **Configuration > Server > Components (Konfiguracja > Serwer > Elementy)**.
2. Włącz opcję **Show components (Pokaż elementy)**.

Uwaga

Elementy są przez nas uznawane za ustawienia zaawansowane. Wyświetlanie i zarządzanie elementami powinno odbywać się wyłącznie w konsultacji z działem pomocy technicznej Axis.

Aktualizuj AXIS Camera Station Pro

Aby zaktualizować AXIS Camera Station Pro:

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

Uwaga

- Po rozpoczęciu aktualizacji – niezależnie czy jest przeprowadzana ręcznie czy w oparciu o harmonogram – nie można jej anulować.
- Zaplanowane aktualizacje rozpoczynają się automatycznie.
- W systemie obejmującym kilka serwerów serwer lokalny jest zawsze aktualizowany jako ostatni.
- Podczas aktualizacji lokalnego serwera klient i sterowanie usługami są tymczasowo zamknięte. Podczas aktualizacji nie będzie widoczny wskaźnik postępu. Komputer serwera powinien być włączony do momentu ponownego uruchomienia klienta i serwera.

Raport o zdarzeniu

Po włączeniu uprawnień do utworzenia raportów o zdarzeniach można generować raporty zawierające nagrania, ujęcia i notatki. Zob. *Eksportowanie raportów o zdarzeniach, on page 34*.

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 rozwijalnego **Export format (Standard eksportu)** wybierz standard, do którego chcesz wyeksportować nagrania.
4. W obszarze **Categories (Kategorie)** dodaj lub usuń kategorie w celu pogrupowania raportów o zdarzeniach. Jeżeli zostaną skonfigurowane jako zmienna w ścieżce katalogu serwera, kategorie staną się nazwami folderów w lokalizacji eksportu.
 - 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. Przykład: „Zgłoszone przez: [imię i nazwisko, adres e-mail, numer telefonu]”.
6. Kliknij przycisk **Apply (Zastosuj)**.

Lokalizacja	
Server directory path (Ścieżka katalogu serwera)	Wprowadź ścieżkę 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 tę 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 Pro. Informacje o dodawaniu pamięci masowej na potrzeby nagrań można znaleźć w temacie <i>Zarządzaj pamięcią masową</i> .

Export format (Format eksportu)	
ASF	Wybierz opcję Add digital signature (Dodaj podpis cyfrowy), aby przyczynić się do zapobiegania sabotażowi obrazu. Zob. sekcję Podpis cyfrowy w temacie <i>Eksportowanie nagrań</i> . 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

Przejdź do **Configuration > Server > Scheduled export** (Konfiguracja > Serwer > Zaplanowany eksport) i zaplanuj harmonogram eksportowania nagrań.

W czasie określonym harmonogramem program AXIS Camera Station Pro eksportuje wszystkie nagrania z okresu od ostatniego eksportu. Jeżeli poprzedni eksport został wykonany ponad tydzień wcześniej lub jeżeli brakuje poprzedniego eksportu, uwzględniane będą wyłącznie nagrania z ostatniego tygodnia. Aby wyeksportować starsze nagrania, wybierz opcję **Recordings (Nagrania)** i wyeksportuj je ręcznie. Zob. *Eksportowanie nagrań*.

Uwaga

W przypadku aktywnego połączenia z kilkoma serwerami AXIS Camera Station Pro można zarządzać zaplanowanym eksportem, wybierając dowolny serwer z rozwijalnego menu **Selected server** (Wybrany serwer).

Eksportowanie zaplanowanych nagrań

1. W obszarze **Scheduled export** (Zaplanowany eksport) zaznacz **Enable scheduled export** (Włącz zaplanowany eksport).
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).

Eksportuj...	
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 tę 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 Pro. Informacje o dodawaniu pamięci masowej na potrzeby nagrań można znaleźć w temacie <i>Zarządzaj pamięcią masową</i> .
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 zostały dokonane.
Export format (Format eksportu)	Wybierz standard, do którego zostaną wyeksportowane nagrania. ASF – zaznacz Add digital signature (Dodaj podpis cyfrowy), aby zapobiec sabotażowi obrazu. Zob. sekcję Podpis cyfrowy w temacie <i>Eksportowanie nagrań</i>. 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.

Microsoft Windows 2012 Server

Aby wyeksportować nagrania z serwera z systemem Microsoft Windows Server 2012, zainstaluj pakiet 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 Roles 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).

Ustawienia WebRTC

Klient internetowy AXIS Camera Station używa WebRTC do komunikacji z serwerem.

Włącz TURN	Włącza lokalny serwer TURN na serwerze AXIS Camera Station Pro, umożliwiając komunikację WebRTC celem korzystania z jednego portu. Może to ułatwić konfigurację zapory sieciowej.
Prioritize TURN (Nadaj priorytet TURN)	Zaznacz tę opcję, aby sygnalizacja WebRTC uwzględniała tylko adres sieciowy i ścieżkę połączenia.

Nowe połączenie

Przejdź do  > Servers > New connection (Serwery > Nowe połączenie) w celu nawiązania połączenia z serwerem AXIS Camera Station Pro. Zob. *Łączenie z serwerem*.

Status połączenia

Przejdź do  > Servers > Connection status (Serwery > Status połączenia), aby sprawdzić status połączenia wszystkich serwerów.

Użyj suwaka obok nazwy serwera, aby połączyć się lub rozłączyć z serwerem.

Kod stanu	Opis	Możliwe rozwiązania
Łączenie	Klient próbuje nawiązać połączenie z serwerem.	
Połączono	Klient jest połączony z tym serwerem za pośrednictwem protokołu TCP.	
Połączono (Axis Secure Remote Access v2)	Klient jest połączony z tym serwerem za pomocą funkcji Axis Secure Remote Access v2.	
Połączono (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 z tym serwerem.	
Rozłączono	Klient nie jest połączony z tym serwerem.	
Ponowne łączenie	Klient utracił połączenie z tym serwerem i próbuje ponownie się połączyć.	
Nie udało się ponownie nawiązać połączenia	Serwer jest odnaleziony, ale uprawnienia lub hasło użytkownika mogły ulec zmianie.	• Dodaj użytkownika w oknie dialogowym User permission (Uprawnienia użytkownika). • 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 User permission (Uprawnienia użytkownika).

Niepowodzenie weryfikacji zabezpieczeń	Sprawdzenie zabezpieczeń powiązanych z usługą WCF nie powiodło się.	Zsynchronizuj czas UTC na komputerze klienckim i komputerze serwera.
Brak kontaktu z serwerem	Komputer serwera nie odpowiedział pod podanym adresem.	• Sprawdź, czy sieć działa prawidłowo. • Sprawdź, czy serwer działa.
Żaden serwer nie pracuje	Komputer z oprogramowaniem serwerowym jest dostępny, ale serwer nie działa.	Uruchom serwer.
Błąd komunikacji	Połączenie z serwerem nie powiodło się.	• Upewnij się, że komputer serwera jest dostępny. • Sprawdź, czy sieć działa prawidłowo. • Sprawdź, czy serwer działa.
Nieprawidłowa nazwa hosta	System DNS nie może zmienić nazwy hosta na adres IP.	• Sprawdź, czy nazwa hosta jest prawidłowo wpisana. • Sprawdź, czy serwer DNS potrafi rozpoznać nazwę hosta.
Już nawiązano połączenie z tym samym serwerem	Klient jest już połączony z tym serwerem.	Usuń zduplikowany wpis serwera.
Nieoczekiwany serwer	Na tym adresie odpowiedział serwer inny, niż oczekiwano.	Dokonaj zmiany na serwerze, podając prawidłowe dane serwera.
Wersja klienta (x) jest niezgodna z wersją serwera (y)	Oprogramowanie klienta jest zbyt stare lub zbyt nowe względem oprogramowania serwera.	Zainstaluj tę samą wersję programu AXIS Camera Station Pro zarówno na komputerze klienckim, jak i na serwerze.
Serwer jest zbyt zajęty	Serwer nie może odpowiedzieć z powodu problemów z wydajnością.	Sprawdź, czy komputer serwera i sieć IP nie są przeciążone.



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

Wiele serwerów

Listy serwerów

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

Przejdź do  > Servers > Server lists (Serwery > Listy serwerów).

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

	Wybierz listę serwerów i kliknij  , aby ją usunąć.
 New server list (Nowa lista serwerów)	Kliknij, aby dodać nową listę serwerów i nadać 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. Możesz zaimportować listy serwerów, aby nawiązać połączenie z serwerami. Zob. <i>Łączenie z serwerem</i> .
Edycja	Aby edytować serwer figurujący na liście serwerów, zaznacz go i kliknij przycisk Edit (Edytuj). Można edytować tylko jeden serwer naraz.
Usuń	Aby usunąć serwer z listy serwerów, zaznacz go i kliknij Remove (Usuń).
Zmień nazwę listy	Kliknij dwukrotnie listę i wprowadź nową nazwę.



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

Grupowanie serwerów w listy serwerów

Konfigurowanie przełącznika

Jeżeli posiadasz rejestrator serii AXIS Camera Station S22 Appliance, możesz go skonfigurować w AXIS Camera Station Pro. Przejdź do **Configuration > Switch > Management** (Konfiguracja > Przełącznik > Zarządzanie) i wpisz swoje uwierzytelnienia, aby otworzyć stronę zarządzania przełącznikami.

Aby skonfigurować przełącznik, p. instrukcja obsługi AXIS Camera Station S22 Appliance series na stronie axis.com.

Uwaga

AXIS Camera Station Pro może się łączyć tylko z adresem <https://192.168.0.1/>, czyli domyślnym adresem IP przełącznika sieciowego.

Zarządzaj licencjami

Na stronie Zarządzanie licencjami jest wyświetlany bieżący stan licencji.

Wersja próbna	Po zainstalowaniu aplikacji AXIS Camera Station Pro uzyskasz 90-dniowy okres próbny. W tym okresie system jest w pełni funkcjonalny. Możesz go konfigurować i wypróbować wszystkie funkcje przed zakupem jakichkolwiek licencji.
Check your licenses (Sprawdzanie licencji)	Jeżeli okres licencji systemu wygaśnie bez automatycznego odnowienia, aplikacja AXIS License Manager zapewnia 30-dniowy okres karencji.

Przydzielono licencję	System jest w pełni licencjonowany do najwcześniejszej daty wygaśnięcia.
Changes made in the system require a license synchronization (Zmiany wprowadzone w systemie wymagają synchronizacji licencji)	Po dodaniu urządzeń do licencjonowanego systemu program AXIS Camera Station Pro próbuje zsynchronizować zmiany z aplikacją AXIS License Manager w celu aktualizacji stanu licencji systemu. Jeśli korzystasz z automatycznego licencjonowania, możesz tego nie zauważyć. Jeżeli korzystasz z ręcznego licencjonowania i nie przeprowadzisz ponownej synchronizacji w ciągu 60 dni, system straci licencję.
Brak licencji	System działa, ale jego funkcjonalność jest ograniczona. Reguły dotyczące nagrań i działań obowiązują nadal, żadne nagrania nie zostaną utracone. Nie będą działać następujące funkcje: • strumieniowanie na żywo • odtwarzanie nagrań • natychmiastowe odtwarzanie • ujęcia • eksportowanie nagrań

Licencję na system można uzyskać na dwa sposoby:

Automatyczne licencjonowanie (systemy online) – System automatycznie przysyła zmiany wpływające na liczbę licencji do aplikacji AXIS License Manager i pobiera nowy stan licencji. Wymaga to aktywnego połączenia z Internetem. Więcej informacji p. *Licencja na system online, on page 137.*

Licencjonowanie ręczne (systemy offline) – Przy tej opcji ręcznie eksportujesz plik systemowy, przesyłasz go do aplikacji AXIS License Manager i importujesz nową licencję. Za każdym razem po wprowadzeniu w systemie zmian, które mają wpływ na liczbę licencji, trzeba powtórzyć ten proces. Wybierz tę opcję, jeśli preferujesz ręczną obsługę licencji lub system nie ma połączenia z Internetem. Więcej informacji p. *Licencja na system w trybie offline, on page 137.*

Licencja na system online

Aby korzystać z automatycznego licencjonowania, zarejestruj system i połącz go z organizacją.

1. Przejdź do menu **Configuration (Konfiguracja) > Licenses (Licencje) > Management (Zarządzanie)**.
2. Upewnij się, że została włączona funkcja **Automatic licensing (Automatyczne licencjonowanie)**.
3. Kliknij polecenie **Register... (Zarejestruj...)**.
4. Zaloguj się za pomocą konta My Axis i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
5. Kliknij **Go to AXIS License Manager** (Przejdź do aplikacji AXIS License Manager), aby zarządzać licencjami. Aby dowiedzieć się więcej, przeczytaj *Podręcznik użytkownika funkcji My Systems na stronie help.axis.com*.

Licencja na system w trybie offline

Aby ręcznie licencjonować system:

1. Przejdź do menu **Configuration (Konfiguracja) > Licenses (Licencje) > Management (Zarządzanie)**.
2. Wyłącz **Automatic licensing (Automatyczne licencjonowanie)**.
3. Kliknij polecenie **Export system file... (Eksportuj plik systemowy...)** i zapisz ten plik na komputerze.

Uwaga

Korzystanie z aplikacji AXIS License Manager wymaga połączenia z Internetem. Jeśli komputer kliencki nie ma połączenia z Internetem, skopiuj plik systemowy na komputer z dostępem do Internetu.

4. Otwórz aplikację *AXIS License Manager*.
5. W aplikacji *AXIS License Manager*:
 - 5.1. Wybierz lub utwórz odpowiednią organizację. Aby dowiedzieć się więcej, przeczytaj *Podręcznik użytkownika funkcji My Systems na stronie help.axis.com*.
 - 5.2. Przejdź do menu **System setup (Konfiguracja systemu)**.
 - 5.3. Kliknij polecenie **Upload system file (Prześlij plik systemowy)**.
 - 5.4. Kliknij polecenie **Upload system file (Prześlij plik systemowy)** i wybierz plik systemowy.
 - 5.5. Kliknij polecenie **Upload system file (Prześlij plik systemowy)**.
 - 5.6. Kliknij **Download license file (Pobierz plik licencji)**.
6. Wróć do klienta *AXIS Camera Station Pro*.
7. Kliknij **Import license file... (Importuj plik licencji)** i wybierz swój plik licencji.
8. Kliknij **Go to AXIS License Manager (Przejdź do aplikacji AXIS License Manager)**, aby zarządzać licencjami.

Konfigurowanie zabezpieczeń

Uprawnienia użytkownika

Przejdź do **Configuration > Security > User permissions (Konfiguracja > Bezpieczeństwo > Uprawnienia użytkowników)**, aby wyświetlić użytkowników i grupy w *AXIS Camera Station Pro*.

Uwaga

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

Zanim dodasz użytkownika lub grupę, sprawdź, czy są zarejestrowani na komputerze lokalnym lub mają konto użytkownika w usłudze Windows® Active Directory. Aby dodać użytkowników lub grupy, zob. *Dodawanie użytkowników lub grup*.

Gdy użytkownik należy do grupy, otrzymuje najwyższą rolę uprawnień przydzielaną mu indywidualnie lub przydzielaną tej grupie. Na przykład użytkownik mający dostęp do kamery X, który jednocześnie należy do grupy mającej dostęp do kamer Y i Z, ma dostęp do wszystkich trzech kamer.

	Wskazuje, że dana pozycja dotyczy indywidualnego użytkownika.
	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 przydzielona do użytkownika lub grupy. Możliwe wartości: Administrator, Operator i Viewer (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 Pro. Aby dodać użytkownika do AXIS Camera Station Pro, 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 > Users** (Lokalni użytkownicy i grupy > Użytkownicy).
- Kliknij prawym przyciskiem myszy **Users** (Użytkownicy) i wybierz opcję **New User** (Nowy użytkownik).
- W wyskakującym oknie dialogowym wpisz 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 pojawią się dostępni użytkownicy 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. Wyniki wyszukiwania mogą się nie wyświetlić, jeżeli liczba użytkowników lub grup jest zbyt duża. Użyj filtru, aby zawęzić wyniki.
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 połączenia z wieloma serwerami AXIS Camera Station Pro wybierz serwer, na którym odbędzie się wyszukiwanie użytkowników lub grup.

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. Zob. *Uprawnienia użytkownika/grupy*.
4. Kliknij przycisk **Save** (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, zob. *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. Rola ta wymagana jest, aby uzyskać dostęp do konfiguracji systemowej.

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 Pro – 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)	Zezwalanie na ręczne uruchamianie i zatrzymywanie nagrań.
Mechanical PTZ (Mechaniczny PTZ)	Zezwalanie na dostęp do mechanicznych funkcji sterowania PTZ. Opcja dostępna tylko dla kamer wyposażonych w mechaniczne sterowanie PTZ.
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 dla kamer z mechanicznym sterowaniem PTZ, które mają zaznaczoną opcję 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 Pro.
Edycja	Umożliwia edycję widoków w AXIS Camera Station Pro.

We/wy

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

Wejść na stronę	Zezwala na pełny dostęp do portu WE/WY.
Zapoznaj się z	Umożliwia wyświetlanie stanu portu we / wy bez wprowadzania zmian.
Write (Zapis)	Umożliwia zmianę stanu portu we / wy.

System

Nie można skonfigurować wyszczególnionych 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 trybie zapisu.
Eksportowanie nagrań	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 środowiska wieloserwerowego.
Zarządzanie dostępem	Umożliwia zarządzanie dostępem i dostęp do ustawień usługi Active Directory .

AXIS Audio Manager Pro

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

Dostęp do ustawień składnika AXIS Audio Manager Pro	Umożliwia konfigurację składnika AXIS Audio Manager Pro w programie AXIS Camera Station Pro oraz dostęp do interfejsu serwera AXIS Audio Manager Pro. Dostępne tylko dla roli Operator.
Dostęp do interfejsu AXIS Audio Manager Pro	Umożliwia dostęp do interfejsu serwera AXIS Audio Manager Pro. Dostępne wyłącznie dla roli Dozorca.

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)	Umożliwia konfigurowanie monitorowania stanu systemu.
Access to system health monitoring (Dostęp do monitorowania stanu systemu)	Umożliwia dostęp do monitorowania stanu systemu.

Certyfikaty

Aby zarządzać ustawieniami certyfikatów na serwerze AXIS Camera Station Pro i dołączonymi urządzeniami, przejdź do **Configuration > Security > Certificates** (Konfiguracja > Bezpieczeństwo > Certyfikaty).

Aby uzyskać informacje o włączaniu, usuwaniu i przeglądaniu certyfikatów HTTPS i IEEE 802.1X, p. sekcja *Bezpieczeństwo, on page 71*.

AXIS Camera Station Pro może być używany jako:

- **Root certificate authority (CA)** (Główny urząd certyfikacji (CA)): Serwis AXIS Camera Station Pro wykorzystuje własny certyfikat root do wydawania certyfikatów serwerowych, bez udziału żadnego innego głównego urzędu certyfikacji.
- **Intermediate certificate authority** (Pośredni organ wydający certyfikat): Importuj certyfikat urzędu certyfikacji wraz z kluczem prywatnym do AXIS Camera Station Pro celem podpisywania i wydawania certyfikatów serwerowych dla urządzeń Axis. Może być on certyfikatem głównym lub pośrednim certyfikatem CA.

Uwaga

W przypadku odinstalowania aplikacji AXIS Camera Station Pro 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 Pro 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 Pro jako główny urząd certyfikacji lub zaimportować certyfikat urzędu certyfikacji i pozwolić, by rozwiązanie AXIS Camera Station Pro 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 Pro przechowuje hasło certyfikatu.
Wygeneruj	Kliknij, aby wygenerować nowy klucz publiczny i prywatny oraz certyfikat CA z podpisem własnym, ważne przez 10 lat. Wygenerowany nowy urząd certyfikacji zastępuje wszystkie certyfikaty komponentów i ponownie uruchamia komponenty.
Wyświetl	Kliknij, aby wyświetlić szczegóły certyfikatu CA.
Eksportuj...	Kliknij, aby wyeksportować certyfikat UC do pliku. Certyfikat eksportować można na dwa sposoby: • Without the private key (Bez klucza prywatnego): Zapisuje certyfikat 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 Pro. • With the private key (Z kluczem prywatnym): Zapisuje urząd certyfikacji w formacie PKCS#12 (.pfx lub .p12). Użyj tej opcji, jeżeli musisz zaimportować certyfikat UC do innego serwera AXIS Camera Station Pro. Nie można ponownie zaimportować certyfikatu .cer lub .crt do programu AXIS Camera Station Pro.
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). Urząd certyfikacji nie podpisuje certyfikatów, których ważność wykracza poza datę wygaśnięcia samego urzędu.

Generowanie głównego organu wydającego certyfikat

Gdy aplikacja AXIS Camera Station Pro zostanie uruchomiona, szuka urzędu certyfikacji. Jeżeli nie zostanie znaleziony żaden urząd certyfikacji, system automatycznie wygeneruje główny urząd certyfikacji. Zawiera on certyfikat główny z podpisem własnym i klucz prywatny chroniony hasłem. AXIS Camera Station Pro przechowuje hasło, ale nie jest ono widoczne. Certyfikat urzędu certyfikacji wygenerowany przez aplikację AXIS Camera Station Pro jest ważny przez 10 lat.

Aby ręcznie wygenerować nowy urząd certyfikacji w celu zastąpienia starego, zob. *Zastępowanie organu wydającego certyfikat, on page 144*.

W przypadku dokonywania uaktualnienia wersji 5.45 lub starszej z certyfikatem ręcznie zainstalowanym w urządzeniu program AXIS Camera Station Pro automatycznie używa istniejącego głównego urzędu certyfikacji w celu zainstalowania nowego certyfikatu, gdy ręcznie 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 programu AXIS Camera Station Pro jako pośredniego urzędu certyfikacji. Zaimportuj istniejący już urząd certyfikacji składający się z certyfikatu i klucza prywatnego, aby umożliwić programowi AXIS Camera Station Pro 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, certyfikat musi być używany w okresie jego ważności. Aby zaimportować urząd certyfikacji w celu zastąpieniu dotychczasowego urzędu certyfikacji, p. sekcja *Zastępowanie organu wydającego certyfikat, on page 144*.

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. Kliknij przycisk **OK**, aby kontynuować.
- Po zaimportowaniu certyfikat CA jest dodawany do zaufanego certyfikatu głównego systemu Windows.
- Podczas importowania certyfikatu pośredniego urzędu certyfikacji certyfikat główny musi już znajdować się w magazynie certyfikatów systemu Windows. W przypadku braku certyfikatu głównego import nie powiedzie się i pojawi się komunikat o błędzie. Program AXIS Camera Station Pro będzie nadal korzystać z poprzedniego CA.
- Po odinstalowaniu aplikacji AXIS Camera Station Pro 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).

Wystawianie certyfikatu niestandardowego

Można utworzyć certyfikat niestandardowy podpisany przez organ wydającego certyfikat AXIS Camera Station Pro. Certyfikatów tych można używać na przykład w zewnętrznych punktach końcowych HTTPS. Po wygaśnięciu tych certyfikatów należy odnowić ręcznie. Aby wystawić certyfikat niestandardowy:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Security (Bezpieczeństwo) > Certificates (Certyfikaty)**.
2. W obszarze **Issue custom certificate (Wystawianie certyfikatu niestandardowego)** kliknij **Issue certificate... (Wystaw certyfikat...)**.
3. Wprowadź szczegóły certyfikatu i kliknij **OK**.

Wystawianie certyfikatu	
Nazwa zwyczajowa (CN)	Identyfikuje posiadacza certyfikatu. CN to zazwyczaj w pełni kwalifikowana nazwa domeny (FQDN) lub adres IP, na którym jest instalowany certyfikat.
Private key password (Hasło klucza prywatnego)	Hasło chroniące klucz prywatny.
Duration (days) (Czas trwania (dni))	Liczba dni ważności certyfikatu.

Wystawianie certyfikatu	
Server authentication (Uwierzytelnianie serwera)	Zaznacz tę opcję, jeżeli używasz certyfikatu na serwerze w celu potwierdzenia tożsamości serwera. Zazwyczaj urządzenia lub inne punkty końcowe, z którymi łączy się AXIS Camera Station Pro przy użyciu protokołu HTTPS, są uznawane za urządzenia serwera, a ich certyfikaty powinny używać uwierzytelniania serwera.
Client authentication (Uwierzytelnianie klienta)	Zaznacz tę opcję, jeżeli korzystasz z certyfikatu na komputerze klienckim w celu potwierdzenia tożsamości klienta przed dołączeniem do serwera. Na przykład urządzenia, które chcą uzyskać dostęp do sieci z kontrolą dostępu przez protokół IEEE 802.1X, muszą użyć tego certyfikatu przed wejściem.
Organizacja (O)	Organizacja posiadacza certyfikatu.
Country code (C) (Kod kraju)	Kod kraju posiadacza certyfikatu.
DNS SAN	Alternatywne nazwy tematów dynamicznego serwera nazw. Alternatywne nazwy FQDN służące do kontaktowania się z posiadaczem certyfikatu. Podczas wystawiania certyfikatu system automatycznie dodaje CN jako DNS SAN. Można wprowadzić kilka adresów oddzielonych przecinkami, np. adres-1.com.pl,adres-2.com.pl.
IP SAN	Alternatywne nazwy podmiotów adresów IP. Alternatywne adresy IP do kontaktowania się z posiadaczem certyfikatu. System automatycznie dodaje CN jako sieć SAN IP, jeśli CN jest adresem IP. Można wprowadzić wiele adresów oddzielonych przecinkami, na przykład: 192.168.1.1,192.168.1.2.

HTTPS

AXIS Camera Station Pro domyślnie weryfikuje aktywny certyfikat serwera HTTPS na każdym połączonym urządzeniu i nie nawiązuje połączenia z urządzeniem bez ważnego certyfikatu. Certyfikat serwera musi być podpisany przez aktywny urząd certyfikacji w AXIS Camera Station Pro lub zweryfikowany przez magazyn certyfikatów systemu Windows. AXIS Camera Station Pro weryfikuje również, czy adres w certyfikacie HTTPS urządzenia jest zgodny z adresem używanym do komunikacji z urządzeniem, gdy 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 uznawane za zaufane. Zamiast tego należy wygenerować lub zaimportować urząd certyfikacji, aby umożliwić aplikacji AXIS Camera Station Pro wystawianie nowych certyfikatów dla urządzeń w przypadku korzystania z protokołu HTTPS.

Potwierdź certyfikat	Włącz, aby łączyć się jedynie z urządzeniami mającymi ważny certyfikat. Bez weryfikacji certyfikatów możliwe jest łączenie się urządzeń z nieważnymi certyfikatami.
Potwierdź adres urządzenia	Wyłącz, aby zapewnić bardziej stabilne działanie w sieciach DHCP, które nie korzystają z nazw hostów. Włącz, aby konieczne było dopasowanie adresów w celu dodatkowego zabezpieczenia. Zaleca się włączenie tego ustawienia jedynie w sieciach, w których urządzenia korzystają głównie z nazw hostów lub mają statyczne adresy IP.

Uwaga

- Jeśli bezpieczne połączenie (HTTPS) jest niedostępne, można wystawić nowy certyfikat HTTPS. Patrz *Dodawanie urządzeń, on page 47*
- 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 kanały podstawowe (Basic). W urządzeniach ustaw opcje **Encrypted & unencrypted** (Zaszyfrowane i niezaszyfrowane) lub **Encrypted only** (Tylko zaszyfrowane), aby zezwolić na komunikację **Digest**.
- W przełącznikach sieciowych serii AXIS T85 PoE+ Network Switch nie można włączyć protokołu HTTPS.

IEEE 802.1X

Z perspektywy uwierzytelniania IEEE 802.1X w AXIS Camera Station Pro suplikantem jest dowolne urządzenie sieciowe Axis, które chce połączyć się 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 wygenerowany bezpośrednio z AXIS Camera Station Pro. Ten certyfikat instalowany jest w każdym urządzeniu Axis celem weryfikacji serwera 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 rozwijalnym **EAPOL Version** (Wersja protokołu EAPoL) wybierz wykorzystywaną wersję protokołu Extensible Authentication Protocol (EAP).
3. W menu rozwijalnym **EAP identity** (Tożsamość EAP) wybierz adres MAC urządzenia, nazwę hosta urządzenia lub niestandardowy tekst.
4. Jeżeli wybrano **Custom** (Niestandardowe), wprowadź tekst, który ma służyć jako tożsamość EAP.

5. Kliknij **Import (Importuj)** i wybierz plik certyfikatu CA uwierzytelniania IEEE 802.1X.
6. Z menu rozwijalnego **Common name** (Nazwa zwyczajowa) wybierz **Device IP address** (Adres IP urządzenia) lub **Device EAP identity** (Tożsamość EAP urządzenia) jako nazwy zwyczajowe w certyfikatach tworzonych dla każdego urządzenia.
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, które nie mają parametru `Network.Interface.I0.dot1x.Enabled`, nie są obsługiwane. Na przykład: urządzenia z serii AXIS P39, AXIS T85 i dekodery wideo T87 Video Decoder.
- Na certyfikatach nie można wykonywać operacji przez nieszyfrowane kanały, czyli kanały podstawowe (Basic). W urządzeniach ustaw opcje **Encrypted & unencrypted** (Zaszyfrowane i niezaszyfrowane) lub **Encrypted only** (Tylko zaszyfrowane), aby zezwolić na komunikację **Digest**.

Ostrzeżenie o wygaśnięciu certyfikatu

Ostrzeżenie jest wyświetlane po wygaśnięciu certyfikatu klienta lub serwera albo krótko przed ich wygaśnięciem. W przypadku niektórych certyfikatów ostrzeżenie wyzwała też alarm systemowy. Dotyczy to wszystkich certyfikatów klienta i serwera, certyfikatów urzędu certyfikacji urządzeń instalowanych przez AXIS Camera Station Pro, certyfikatu urzędu certyfikacji AXIS Camera Station Pro 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 Pro.

Odnowienie certyfikatu

Odnawianie certyfikatu uwierzytelniającego komunikację między serwerem i urządzeniami

Certyfikaty klienta i serwera wygenerowane przez AXIS Camera Station Pro są odnawiane automatycznie 7 dni przed pojawieniem się ostrzeżenia o wygaśnięciu. Wymaga to włączenia protokołu HTTPS lub standardu IEEE 802.1X na tym urządzeniu. Aby ręcznie odnowić lub zaktualizować certyfikat, p. sekcja *Bezpieczeństwo, on page 71*.

Odnawianie certyfikatu uwierzytelniającego komunikację między serwerem i klientem

Nowy certyfikat serwera można wygenerować na karcie **Certificates** (Certyfikaty) w aplikacji AXIS Camera Station Pro Service Control. Instrukcje znajdują się w sekcji *Certyfikaty, on page 230*.

Resetowanie hasła

1. Wybierz kolejno opcje **Configuration > Security > Certificates** (Konfiguracja > Zabezpieczenia > Certyfikaty).
2. Wyłącz opcję **Validate device certificate** (Sprawdzaj certyfikat urządzenia), aby urządzenia korzystające z certyfikatów urzędu certyfikacji pozostały 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).

Skonfiguruj kontrolę 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 Pro opisano w temacie *Konfigurowanie sieciowego kontrolera drzwi Axis*.

Uwaga

Na początek wykonaj następujące czynności:

- Zaktualizuj wersję systemu operacyjnego AXIS OS kontrolera w obszarze **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, p. sekcja *Profile identyfikacji*, on page 167.
2. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, zob. *Formaty kart i kod PIN*, on page 169.
3. Dodaj drzwi i zastosuj do nich profil identyfikacji. Zob. *Dodaj drzwi*, on page 152.
4. Skonfiguruj drzwi:
 - *Dodawanie czujnika pozycji drzwi*, on page 158
 - *Dodawanie czujnika awaryjnego*, on page 160
 - *Dodawanie czytnika*, on page 161
 - *Dodawanie urządzenia REX*, on page 164
5. Dodaj strefę, a następnie drzwi do strefy. Zob. *Dodawanie strefy*, on page 164.

Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

Ważne

Przy aktualizacji oprogramowania układowego AXIS OS w sterowniku drzwiowym pamiętaj o poniższych kwestiach:

- **Obsługiwane wersje oprogramowania układowego AXIS OS:** Wymienione poniżej obsługiwane wersje systemu (oprogramowania układowego) AXIS OS mają zastosowanie tylko w przypadku wykonywania aktualizacji z oryginalnej zalecanej wersji programu AXIS Camera Station Pro i gdy system zawiera skonfigurowane drzwi. Jeżeli system nie spełnia tych warunków, musisz dokonać aktualizacji do wersji systemu AXIS OS zalecanej dla konkretnej wersji AXIS Camera Station Pro.
- **Minimalna obsługiwana wersja oprogramowania układowego AXIS OS:** Najstarsza wersja systemu AXIS OS zainstalowana w systemie określa minimalną obsługiwaną wersję AXIS OS – z ograniczeniem do dwóch wcześniejszych wersji. Załóżmy, że korzystasz z programu AXIS Camera Station Pro w wersji 6.5 i aktualizujesz wszystkie urządzenia do zalecanej wersji oprogramowania układowego AXIS OS 12.0.86.2. W związku z tym wersja oprogramowania AXIS OS 12.0.86.2 będzie od tej pory minimalną obsługiwaną wersją Twojego systemu.
- **Aktualizacja do wersji oprogramowania AXIS OS wyższej niż zalecana:** Załóżmy, że aktualizujesz oprogramowanie do wersji AXIS OS wyższej niż zalecana dla konkretnej wersji programu AXIS Camera Station Pro. Będziesz mógł zawsze bez problemów obniżyć wersję z powrotem do zalecanej wersji

oprogramowania AXIS OS, o ile będzie się ona mieścić w limitach obsługi określonych dla danej wersji programu AXIS Camera Station Pro.

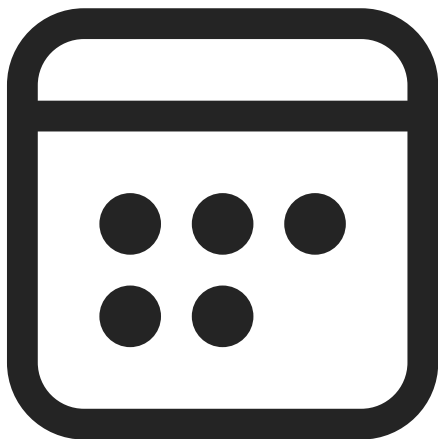
- **Przyszłe zalecenia dotyczące oprogramowania AXIS OS:** Aby zapewnić stabilność systemu i pełną zgodność, należy zawsze przestrzegać wersji oprogramowania AXIS OS zalecanej dla danej wersji programu AXIS Camera Station Pro.
- **Zmiana ścieżki:** Zmiana ścieżki oprogramowania układowego z 10.12.xx na 11.0.xx lub wyższą wymaga przywrócenia ustawień fabrycznych.

W poniższej tabeli przedstawiono minimalną i zalecaną wersję systemu AXIS OS dla poszczególnych wersji oprogramowania AXIS Camera Station Pro:

Wersja AXIS Camera Station	Minimalna wersja systemu AXIS OS	Zalecana wersja systemu AXIS OS
Pro 6.17	12.6.102.1	12.9.65.3
Pro 6.16	12.6.102.1	12.9.65.3
Pro 6.15	12.5.68.1	12.8.55.1

Drzwi i strefy

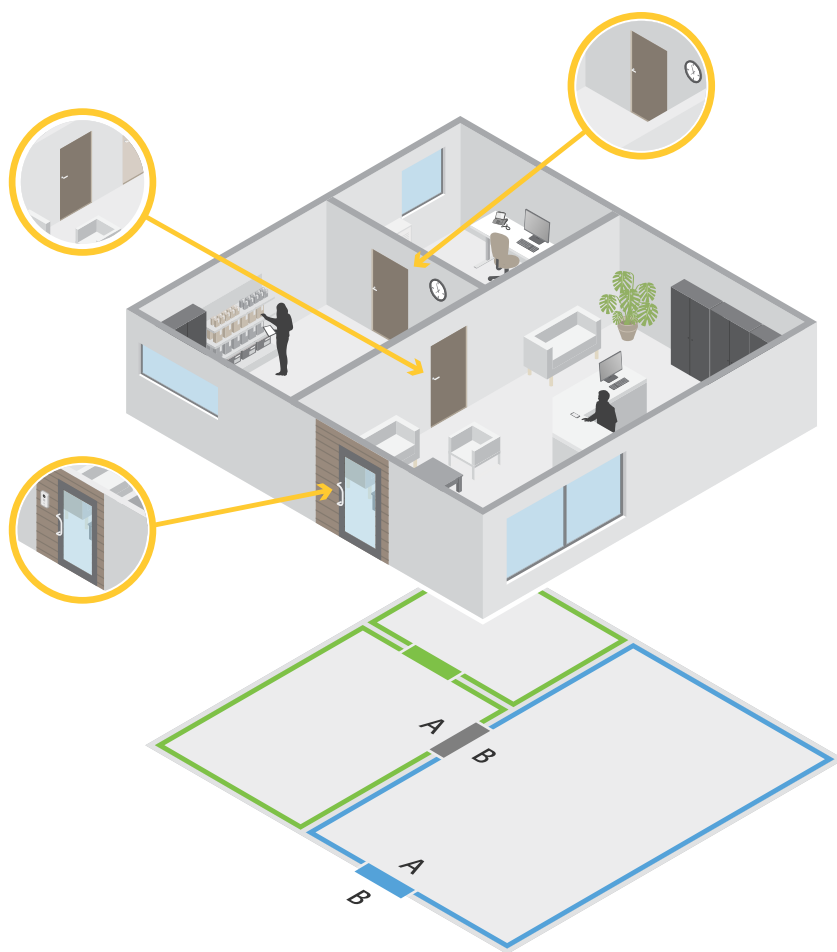
Wybierz kolejno opcje **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy), aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

 Akcje wykonywane ręcznie	Ręcznie ustaw stan drzwi. Wybierz jedną z poniższych opcji: Reset (Resetowanie) (zgodnie z regułami systemu), Grant access (Przyznawanie dostępu) (odblokuj drzwi na 7 sekund), Unlock (Odblokowane) (pozostaw drzwi odblokowane), Lock (Zablokowane) (pozostaw drzwi zablokowane) lub Lockdown (Odcinanie obszaru) (nikt nie może wejść ani wyjść).
 Harmonogramy odblokowania	Ustaw harmonogram, aby automatycznie odblokowywać drzwi o określonych godzinach. W pozostałych godzinach drzwi pozostają zamknięte. Aby harmonogram aktywował się dopiero po ręcznym odblokowaniu drzwi przez pierwszą osobę, włącz opcję First person in (Wejście pierwszej osoby).
 Profil identyfikacji	Zmień profil identyfikacji w drzwiach.
 Przypnij wykres	Wyświetlić schemat styków kontrolera drzwi. Aby wydrukować tabelę rozkładu styków, kliknij Print (Drukuj).
 Bezpieczny kanał	Włącz lub wyłącz bezpieczny kanał OSDIP dla konkretnego czytnika.

Drzwi	
Nazwa	Nazwa drzwi.
Type (Typ):	Typ konfiguracji drzwi.
Urządzenie	Urządzenie podłączone do drzwi.

IP address (Adres IP)	Adres IP sterownika drzwiowego dołączonego do 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.
Akumulator	Stan akumulatora kontrolera drzwi.
Status	Stan drzwi. • Online: Drzwi są w trybie online i działają prawidłowo. • Reader offline (Czytnik offline): Czytnik w konfiguracji drzwi jest w trybie offline. • Reader error (Błąd czytnika): Czytnik nie obsługuje bezpiecznego kanału lub funkcja ta została dla niego wyłączona. • Old firmware (Stare oprogramowanie układowe): Urządzenie korzysta z przestarzałej wersji oprogramowania układowego. Zaktualizuj oprogramowanie układowe, aby zapewnić najlepsze działanie i bezpieczeństwo.
Strefy	
Nazwa	Nazwa strefy.
Liczba drzwi	Liczba drzwi należących do strefy.
Poziom zabezpieczeń	Poziom zabezpieczeń zastosowany w tej strefie.

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.

Dodaj drzwi

Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku. Kontrolery wielofunkcyjne obsługują dodatkowe konfiguracje zamków.
- Jeżeli kontroler drzwiowy nie ma drzwi i używasz nowej wersji AXIS Camera Station Pro ze starszym oprogramowaniem układowym w kontrolerze drzwiowym, system uniemożliwia dodanie drzwi. System zezwala jednak na tworzenie nowych drzwi na kontrolerach systemowych ze starszym oprogramowaniem układowym, jeżeli drzwi już istnieją.

Aby dodać drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **+** Add (Dodaj) i z listy rozwijalnej wybierz rodzaj drzwi.

Typy drzwi	
Drzwi	Zwykłe drzwi z monitorem drzwi obsługującym rygle i czytniki. Wymaga kontrolera drzwiowego.
Piętro	Rodzaj drzwi do sterowania windą uwierzytelniający dostęp do pięter z windy za pomocą czytników kart. Więcej informacji znajduje się w sekcji <i>Dodawanie piętra^{BETA}</i> , on page 160.
Drzwi dozoruujące	Drzwi, które mogą zgłaszać, czy są otwarte, czy zamknięte. Więcej informacji znajduje się w sekcji <i>Dodawanie drzwi dozoruujących</i> , on page 159.
Drzwi bezprzewodowe	Drzwi, które można skonfigurować za pomocą bezprzewodowych rygli i koncentratorów komunikacyjnych ASSA ABLOY Aperio®. Więcej informacji znajduje się w sekcji <i>Dodaj zamek bezprzewodowy</i> , on page 157.
Drzwi zastępcze	Drzwi zastępcze, które możesz dodać do systemu bez wybierania sprzętu.

3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami. Sterownik jest wyszarzony, gdy nie można dodać kolejnych drzwi, gdy jest w trybie offline lub gdy nie jest włączony protokół HTTPS.
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. Zob. *Profile identyfikacji*, on page 167.
8. Konfiguruj drzwi, dodając czujniki lub czytniki w obszarze **Sensors** (Czujniki), **Side A** (Strona A) i **Side B** (Strona B).
9. Skonfiguruj ustawienia właściwe dla drzwi. Zobacz *Ustawienia drzwi*, on page 154.
10. Skonfiguruj poziom zabezpieczeń. Zob. *Poziom zabezpieczeń drzwi*, on page 155.
11. Kliknij przycisk **Save (Zapisz)**.

Kopiowanie konfiguracji drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **+ Add (Dodaj)**.
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 (Kopiuje konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarzony, jeśli został skonfigurowany z dwoma drzwiami lub jednym z dwoma zamkami.
6. W razie potrzeby zmień ustawienia.
7. Kliknij przycisk **Save (Zapisz)**.



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

Dodawanie i konfigurowanie drzwi i stref

Ustawienia drzwi

Aby zmodyfikować 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)**.
4. W obszarze **Door settings (Ustawienia drzwi)** zmień dowolne ustawienia i kliknij **Save (Zapisz)**.

Czas dostępu (s)	Ustaw, przez ile sekund drzwi pozostaną odblokowane po przyznaniu dostępu. Drzwi ponownie zaryglują się po zamknięciu, nawet gdy pozostał jeszcze czas.
Open-too-long time (sec) (Przekroczony czas otwarcia drzwi (s))	Dotyczy tylko, gdy monitor drzwi jest skonfigurowany. Ustaw, przez ile sekund drzwi mogą pozostać otwarte. Jeżeli drzwi będą nadal otwarte po upływie określonego czasu, uruchomi się alarm sygnalizujący zbyt długie otwarcie drzwi. Skonfiguruj regułę działania, aby określić, co ma się stać po wystąpieniu tego zdarzenia będącego wyzwalaczem.
Długi czas dostępu (s)	Ustaw, przez ile sekund drzwi pozostają odblokowane po przyznaniu dostępu posiadaczom kart, u których ustawienie to jest dostępne. Ma to priorytet przed standardowym czasem dostępu.
Long open-too-long time (sec) (Długi czas przekroczenia otwarcia drzwi (s))	Dotyczy tylko, gdy monitor drzwi jest skonfigurowany. Ustaw, przez ile sekund drzwi mogą pozostać otwarte dla posiadaczy kart z dostępną opcją Long access time (Długi czas dostępu) . Ma to priorytet przed standardowym czasem zbyt długiego otwarcia.
Czas opóźnienia do ponownego zablokowania (ms)	Ustaw, ile milisekund drzwi pozostają odblokowane po ich otwarciu lub zamknięciu.
Ponowne zablokowanie	• After opening (Po otwarciu): Dotyczy tylko scenariuszy z dodanym monitorem drzwi. • After closing (Po zamknięciu): Dotyczy tylko scenariuszy z dodanym monitorem drzwi.
Drzwi wyważone	Określ, czy system ma wyzwać alarm systemowy w przypadku wyważenia drzwi. Wymagany jest czujnik położenia drzwi (DPS).
Przekroczony czas otwarcia drzwi	Określ, czy system ma wyzwać alarm systemowy w przypadku pozostawienia na zbyt długo otwartych drzwi.

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)** i potwierdź.

Akcje wykonywane ręcznie

W stosunku do drzwi i stref można wykonywać następujące czynności ręczne:

Resetuj – Powoduje powrót do skonfigurowanych reguł systemowych.

Przyznawanie dostępu – Odblokowuje drzwi lub strefę na 7 sekund, a następnie ponownie je blokuje.

Odblokuj – Utrzymuje drzwi w stanie odblokowania do momentu zresetowania.

Lock (Blokada) – Utrzymuje drzwi w stanie zablokowania do czasu, aż system przyzna dostęp posiadaczowi karty.

Odcinanie obszaru – Nikt nie może wejść ani wyjść do czasu zresetowania lub odblokowania.

Aby wykonać akcję ręcznie:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
2. Wybierz drzwi albo strefę.
3. Kliknij dowolną akcję wykonywaną ręcznie.

Poziom zabezpieczeń drzwi

Do drzwi można dodać następujące zabezpieczenia:

Reguła dwóch osób – Reguła dwóch osób wymaga, aby dwie osoby użyły prawidłowych poświadczeń w celu uzyskania dostępu.

Dwukrotne przeciągnięcie – Dwukrotne przeciągnięcie karty umożliwia posiadaczowi karty zmianę bieżącego stanu drzwi. Może to służyć na przykład do blokowania lub odblokowywania drzwi poza regularnym harmonogramem, co jest wygodniejsze niż odblokowanie drzwi przez wchodzenie do systemu. Przeciągnięcie dwóch kart nie ma wpływu na istniejący harmonogram. Jeżeli na przykład drzwi mają zostać zablokowane o godzinie zamknięcia, a pracownik wyjdzie na przerwę obiadową, drzwi zostaną zablokowane zgodnie z harmonogramem.

Poziom zabezpieczeń można skonfigurować podczas dodawania nowych drzwi albo dla już istniejących drzwi.

Aby dodać regułę dwóch osób do istniejących drzwi:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
2. Wybierz drzwi, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz **Two-person rule (Reguła dwóch osób)**.
6. Kliknij przycisk **Apply (Zastosuj)**.

Reguła dwóch osób	
Side A (Strona A) i Side B (Strona B)	Wybierz, po których stronach drzwi ma być używana reguła.

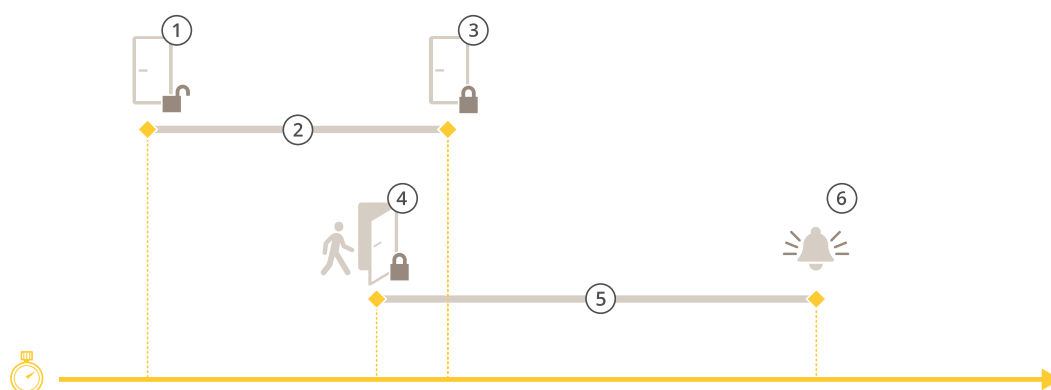
Harmonogramy	Wybierz, kiedy reguła jest aktywna.
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi uwierzytelnieniami dostępu.

Aby dodać przeciągnięcie dwóch kart do istniejących drzwi:

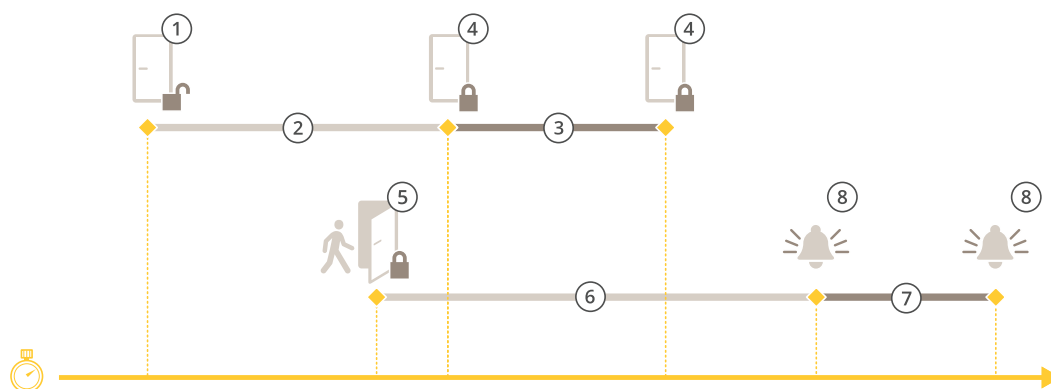
1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
2. Wybierz drzwi, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz **Double-swipe (Przeciągnięcie dwóch kart)**.
6. Kliknij przycisk **Apply (Zastosuj)**.
7. Zastosuj opcję **Double-swipe (Przeciągnięcie dwóch kart)** do posiadacza karty.
 - 7.1. Otwórz kartę **Access Management (Zarządzanie dostępem)**.
 - 7.2. Kliknij  przy posiadaczu karty, którego chcesz edytować, a następnie kliknij **Edit (Edytuj)**.
 - 7.3. Kliknij **More (Więcej)**.
 - 7.4. Wybierz **Allow double-swipe (Zezwól na przeciągnięcie dwóch kart)**.
 - 7.5. Kliknij przycisk **Apply (Zastosuj)**.

Dwukrotne przeciągnięcie	
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi uwierzytelnieniami dostępu.

Opcje czasu



- 1 Dostęp przyznany – zamek odblokowany
- 2 Czas dostępu
- 3 Nie podjęto żadnych działań – zamek pozostaje 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 pozostaje 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 Pro 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.



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 drzwiowym Axis i serwerze AXIS Camera Station Pro musi być zsynchronizowany.
 - Przed rozpoczęciem skorzystaj z aplikacji Aperio obsługiwanej przez ASSA ABLOY, aby sparować zamki Aperio z koncentratorem Aperio.
 - Do każdego złącza RS485 można podłączyć tylko jeden koncentrator komunikacyjny Aperio. Technologia multi-drop nie jest obsługiwana.
 - 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 Pro wybierz kolejno **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
 - 4.2. W obszarze **Doors (Drzwi)** kliknij  **Add (Dodaj)**.
 - 4.3. Jako **Door type (Rodzaj drzwi)** wybierz **Wireless door (Drzwi bezprzewodowe)** i kontroler drzwiowy dołączony do koncentratora komunikacyjnego Aperio.
 - 4.4. Kliknij **Next (Dalej)**.
 - 4.5. Wybierz **Wireless lock (Zamek bezprzewodowy)**.
 - 4.6. Określ strony A i B drzwi i dodaj czujniki. Aby uzyskać dodatkowe informacje, zob. *Drzwi i strefy, on page 149*.
 - 4.7. Kliknij przycisk **Save (Zapisz)**.

Po dołączeniu zamka bezprzewodowego można sprawdzić poziom naładowania baterii i stan zamka w przeglądzie drzwi.

Poziom baterii	Działanie
Dobrze	Brak
Niski	Zamek działa zgodnie z przeznaczeniem, ale należy wymienić baterię, zanim jej poziom stanie się krytyczny.
Krytyczny	Wymiana akumulatora. Zamek może nie działać prawidłowo.

Status zamka	Działanie
Online	Brak
Zacięcie zamka	Rozwiąż wszelkie problemy mechaniczne.

Dodawanie czujnika pozycji drzwi

Czujnik pozycji drzwi to przełącznik, który monitoruje fizyczny stan drzwi. Możesz dodać czujnik pozycji drzwi do drzwi i skonfigurować sposób jego dołączenia.

1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 152*.
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.

3. Wybierz **Door position sensor** (Czujnik pozycji 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 drzwiowym i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Zob. *Nadzorowane wejścia*, on page 166.

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.

Dodawanie drzwi dozorujących

Drzwi dozorujące to typ drzwi, które mogą sygnalizować, czy są otwarte, czy zamknięte. Technologii tej można używać na przykład w przypadku drzwi przeciwpożarowych, które nie wymagają zamka, ale w których przypadku warto wiedzieć, czy są otwarte.

Drzwi dozorujące różnią się od zwykłych drzwi z monitorem drzwi. Zwykłe drzwi z monitorem drzwi obsługują zamki i czytniki, ale wymagają kontrolera drzwi. Drzwi dozorujące obsługują jeden czujnik położenia drzwi, ale wymagają tylko sieciowego modułu przekaźnikowego WE/WY podłączonego do kontrolera drzwi. Do jednego sieciowego modułu przekaźnikowego WE/WY można podłączyć do pięciu czujników położenia drzwi.

Uwaga

Drzwi dozorujące wymagają modułu przekaźnikowego AXIS A9210 Network I/O Relay Module z najnowszym oprogramowaniem sprzętowym, w tym z aplikacją AXIS Monitoring Door ACAP.

Aby skonfigurować drzwi dozorujące:

1. Zainstaluj moduł AXIS A9210 i uaktualnij jego system AXIS OS do najnowszej wersji.
2. Zainstaluj czujniki położenia drzwi.
3. W aplikacji AXIS Camera Station Pro przejdź do sekcji **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
4. Kliknij **Add door (Dodaj drzwi)**.
5. Wprowadź nazwę.
6. W sekcji **Type (Typ)** wybierz **Monitoring door (Drzwi dozorujące)**.
7. W sekcji **Device (Urządzenie)** wybierz sieciowy moduł przekaźnikowy WE/WY.
8. Kliknij **Next (Dalej)**.
9. W obszarze **Sensors (Czujniki)** kliknij  **Add (Dodaj)** i wybierz **Door position sensor (Czujnik położenia drzwi)**.
10. Wybierz WE/WY podłączone do czujnika położenia drzwi.
11. Kliknij **Dodaj**.

Dodawanie piętra^{BETA}

Piętro to rodzaj drzwi, które służą do kontroli dostępu do pięter z windy. Dodając piętro, tworzysz zasób windy, który grupuje wszystkie piętra dla tej windy. W kabinie windy znajduje się czytnik kart, dzięki któremu uprawniony użytkownik uzyska dostęp do konkretnego piętra.

Zanim zaczniesz, potrzebujesz:

- Obsługiwanego sieciowego kontrolera drzwiowego dodanego do systemu np. *A1610*, *A1710-B* lub *A1810-B*.
- *Modułu przekaźnikowego rozszerzeń we / wy A9910* na potrzeby współpracy z dodatkowymi przekaźnikami. Aby dodać moduł do kontrolera, p. sekcja .

Uwaga

Ta funkcja jest w fazie Beta i obecnie obsługuje jedynie maks. 16 pięter oraz czytniki kart.

Aby skonfigurować piętro:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **+** **Add (Dodaj)** i wybierz **Floor^{BETA}** (Piętro).
3. Wpisz nazwę piętra.
4. Wybierz kontroler.
5. W sekcji **Elevator** (Winda) wybierz istniejącą windę lub kliknij **Create new elevator** (Utwórz nową windę), aby dodać nową, następnie wpisz nazwę.
6. W pozycji **Side A** (Strona A) wybierz **Card reader** (Czytnik kart) i skonfiguruj czytnik. Pozycji **Side B** (Strona B) nie konfiguruje się ze względów bezpieczeństwa.
7. Kliknij **Save and add new** (Zapisz i dodaj nowe), aby dodać więcej pięter do tej samej windy. Konfiguracja windy i czytnika pozostaje wypełniona dla następnego piętra. Opcja ta jest dostępna wyłącznie, gdy kontroler ma przekaźniki.
8. Kliknij **Save** (Zapisz) po dodaniu piętra. Nazwy pięter wyświetlane są w następujący sposób: „Nazwa windy – nazwa piętra”, na przykład: „Zachodnie skrzydło – piętro 1”.

Uwaga

- Czytniki stosowane na wielu piętrach można edytować tylko na pierwszym piętrze, na którym zostały dodane.
- Windy są automatycznie usuwane po usunięciu wszystkich odnośnych pięter.

Dodawanie czujnika awaryjnego

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. Zob. *Dodaj drzwi, on page 152*.
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 IP

Jako czytnik można wykorzystać domofon sieciowy Axis lub inne urządzenie działające w oparciu o protokół IP. Przed przydzieleniem go do drzwi musisz dodać urządzenie do programu AXIS Camera Station Pro.

Uwaga

Zanim rozpoczniesz, sprawdź, czy czytnik IP jest zasilany i dołączony do tej samej sieci IP co program AXIS Camera Station Pro.

1. Przejdź do **Configuration > Devices > Add devices** (Konfiguracja > Urządzenia > Dodaj urządzenia).
2. Wybierz czytnik IP z listy wykrytych urządzeń i kliknij **Add** (Dodaj).
3. Po wyświetleniu monitu wpisz dane uwierzytelniające urządzenia.

Po dodaniu urządzenie możesz przydzielić do drzwi. Zobacz *Dodawanie czytnika, on page 161*.

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 kodów PIN, pojawi się to w kolumnie **Card formats** (Formaty kart) w obszarze **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy). Zob. *Drzwi i strefy, on page 149*.

Uwaga

- Do kontrolera drzwiowego można również dołączyć maks. 16 czytników Bluetooth. Więcej informacji znajduje się w sekcji *Dodawanie czytnika Bluetooth, on page 163*.
 - Jeżeli jako czytnik IP używany jest domofon sieciowy Axis, system używa konfiguracji kodu PIN ustawionej na stronie internetowej urządzenia.
1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 152*.
 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 długości kodu PIN dla 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 poczynionej w konfiguracji systemu, w aplikacji klienckiej pojawia się ikona ostrzeżenia.
7. Kliknij **Dodaj**.
8. Aby dodać czytnik po drugiej stronie drzwi, powtórz tę procedurę.

Aby uzyskać informacje o instalacji czytnika kodów kreskowych AXIS Barcode Reader, p. sekcja *Instalowanie aplikacji AXIS Barcode Reader, on page 172*.

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. Domofony sieciowe Axis możesz wykorzystać jako czytniki IP.

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	Wybierz stan obwodu, który uaktywnia wejście sabotażu w czytniku. • Open circuit (Obwód rozarty): Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie otwarty. • Closed circuit (Obwód zwarty): 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.) .
Wejście nadzorowane	Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. Zob. <i>Nadzorowane wejścia, on page 166</i> .

Dodawanie czytnika Bluetooth

Czytnik AXIS A4612 Network Bluetooth® Reader pozwala rozszerzyć możliwości przewodowych kontrolerów drzwiowych Axis. Do jednego kontrolera drzwiowego można przydzielić maks. 16 takich czytników. Każdy czytnik może zarządzać rygłem drzwiowym, przyciskiem wyjścia (REX) i przełącznikiem pozycji drzwi (DPS).

Instalacja 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 *Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth, on page 163*.
2. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodaj drzwi, on page 152*.
3. Pod jedną stroną drzwi kliknij **+** 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 jest stosowany do parowania uwierzytelnień, 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.

Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth

W tym przykładzie pokazano, jak dodać do systemu czytnik AXIS A4612 Bluetooth Reader, aby umożliwić posiadaczom kart odblokowywanie drzwi za pomocą aplikacji AXIS Mobile Credential.

1. Zainstaluj czytnik Bluetooth i podłącz go do kontrolera drzwi.
2. Dodaj czytnik Bluetooth w interfejsie WWW kontrolera drzwi.
 - 2.1. Uzyskaj dostęp do kontrolera drzwi i przejdź do sekcji **Peripherals (Urządzenia peryferyjne) > Readers (Czytniki)**.
 - 2.2. Kliknij **Add reader (Dodaj czytnik)**.
 - 2.3. Wprowadź wymagane informacje w oknie dialogowym **Add Bluetooth reader (Dodaj czytnik Bluetooth)**.
 - 2.4. Kliknij **Dodaj**.
3. Dodaj czytnik Bluetooth do drzwi w programie AXIS Camera Station Pro.
 - 3.1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
 - 3.2. Wybierz drzwi, do których chcesz dodać czytnik Bluetooth, i kliknij **Edit (Edytuj)**.
 - 3.3. Kliknij **+** Add (Dodaj) po stronie drzwi, gdzie znajduje się czytnik Bluetooth.
 - 3.4. Wybierz **Card reader (Czytnik kart)**.
 - 3.5. W sekcji **Add IP reader (Dodaj czytnik IP)** wybierz **IP reader (Czytnik IP)**.
 - 3.6. W sekcji **Select IP reader (Wybierz czytnik IP)** wybierz czytnik Bluetooth.
 - 3.7. Kliknij **Dodaj**.
4. Wybierz czytnik Bluetooth do sparowania. Należy je przeprowadzić w przypadku co najmniej jednego czytnika Bluetooth w systemie.
 - 4.1. Wybierz nowo dodany czytnik Bluetooth.
 - 4.2. Kliknij **Edit (Edycja)**.
 - 4.3. W sekcji **Edit bluetooth reader (Edytuj czytnik Bluetooth)** wybierz **Use this reader for pairing (Użyj tego czytnika do parowania)**.
 - 4.4. Kliknij przycisk **Apply (Zastosuj)**.

5. Wybierz profil identyfikacji **Tap in app (Dotknij w aplikacji)** lub **Touch reader (Dotknij czytnika)**. Więcej informacji p. *Profile identyfikacji, on page 167*.
6. Dodaj mobilne poświadczenia do posiadacza karty. Zob. *Dodaj poświadczenia, on page 187*.
7. Sparuj mobilne poświadczenia z czytnikiem z włączonym trybem parowania:
 - 7.1. Zbliż telefon komórkowy posiadacza karty do czytnika Bluetooth z włączonym trybem parowania.
 - 7.2. Postępuj zgodnie z instrukcjami podanymi w e-mailu wysłanym do posiadacza karty.

Dodawanie urządzenia REX

Urządzenie REX (żądanie wyjścia) możesz 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. Zob. *Dodaj drzwi, on page 152*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **REX device (Urządzenie REX)**.
4. Zaznacz port we / wy, do którego chcesz dołączyć urządzenie REX. Jeżeli dostępny jest 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 drzwiowym i urządzeniem REX powodowało wyzwolenie zdarzenia, włącz **Supervised input (Nadzorowane wejście)**. Zob. *Nadzorowane wejścia, on page 166*.

Działanie	
Odblokuj drzwi	Wybierz tę opcję, aby odblokować drzwi po odebraniu sygnału REX.
Brak	Wybierz, aby nie podejmować żadnych działań w przypadku odebrania przez drzwi sygnału REX.

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.
- **Internal door (Drzwi wewnętrzne)**: Wewnętrzne drzwi w strefie.

Uwaga

Drzwi obwodowe mogą należeć do dwóch stref. Drzwi wewnętrzne mogą należeć tylko do jednej strefy. Patrz punkt *Przykład drzwi i stref, on page 152*, gdzie znajduje się ogólny przegląd.

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 na obwodzie domyślnie jako wejścia do strefy używają strony 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 **Save (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. Aby ponownie skorzystać z uwierzytelnień, osoba musi najpierw opuścić obszar.

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 albo 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 strefy.
6. Kliknij przycisk **Apply (Zastosuj)**.

Anti-passback	
Log violation only (Soft) (Tylko rejestrowanie naruszeń (wersja miękka))	Zaznacz tę opcję, aby umożliwić drugiej osobie wejście przy użyciu uwierzytelnień, których użyła pierwsza osoba. Ta opcja powoduje tylko wywołanie alarmu systemowego.
Deny access (Hard) (Odmowa dostępu (wersja twarda))	Zaznacz tę opcję, aby uniemożliwić wejście drugiej osobie, jeżeli korzysta z uwierzytelnień, których użyła pierwsza osoba. Ta opcja powoduje także wywołanie alarmu systemowego.
Limit czasu (w sekundach)	Czas, po którym system zezwoli użytkownikowi na ponowne wejście. Wpisz 0 , aby wyłączyć limit czasu, co oznacza, że funkcja anti-passback będzie obowiązywać do momentu opuszczenia strefy 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

Wejścia nadzorowane mogą wyzwać zdarzenie w przypadku przerwy w połączeniu z kontrolerem drzwiowym.

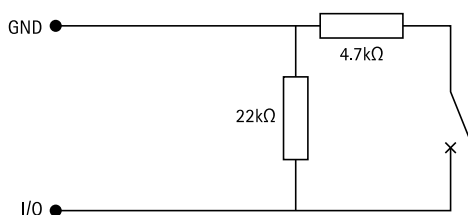
- Podłączenie między kontrolerem drzwi a monitorem drzwi. Zob. *Dodawanie czujnika pozycji drzwi, on page 158.*
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Zob. *Dodawanie czytnika, on page 161.*
- Podłączenie między kontrolerem drzwi a urządzeniem REX. Zob. *Dodawanie urządzenia REX, on page 164.*

Aby użyć nadzorowanych wejść:

1. Zamontuj rezystory końca linii zgodnie ze schematem połączeń jak najbliższej 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 K Ω parallel resistor and a 4.7 K Ω serial resistor (Pierwsze połączenie równoległe z 22 k Ω opornikiem równoległym i 4,7 k Ω 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.

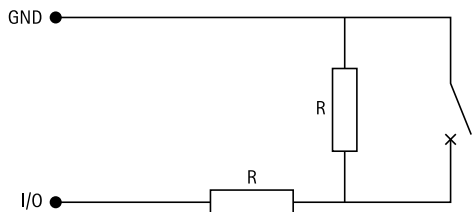
Pierwsze połączenie równoległe

Oporniki muszą mieć wartości 4,7 k Ω i 22 k Ω .



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.

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.

Dostępne profile identyfikacji:

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.

Kod 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.

Dotknij w aplikacji – Posiadacz karty musi dotknąć poświadczenia w aplikacji mobilnej AXIS Camera Station, stojąc w zasięgu czytnika Bluetooth.

Czytnik dotykowy – Posiadacz karty musi dotknąć czytnika Bluetooth, mając przy sobie telefon komórkowy z poświadczeniem mobilnym.

*QRCode to zastrzeżony znak towarowy należący do Denso Wave Incorporated w Japonii i w innych krajach.

Tworzenie profilu identyfikacji

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.
2. Kliknij **+** **Create identification profile (Utwórz profil identyfikacyjny)**.
3. Wpisz nazwę profilu 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. W przypadku strony A (Side A) kliknij **+** **Add (Dodaj)**, a następnie wybierz rodzaj identyfikacji i harmonogram.

- Aby wymagać od posiadaczy kart użycia więcej niż jednego rodzaju identyfikacji, zaznacz kilka rodzajów w tym samym wierszu.
 - Aby umożliwić posiadaczom kart korzystanie z obu rodzajów, kliknij ponownie **+** Add (Dodaj) i dodaj kolejny wiersz.
6. W przypadku strony B (Side B) kliknij **+** Add (Dodaj), a następnie wybierz rodzaj identyfikacji i harmonogram.
 7. Kliknij OK.



Konfigurowanie profilu identyfikacji

Edycja profilu 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.

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) .
Harmonogram	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.

Usuwanie profilu 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.

Resetowanie wstępnie zdefiniowanego formatu 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.

Formaty kart i kod PIN

Format kart określa, w jaki sposób czytnik kart interpretuje dane z karty. Dostępne są gotowe formaty kart, z których można korzystać lub które można edytować; można również utworzyć własne 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.

Konfiguracja kodu 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**.

Tworzenie formatu 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.
- Wstępnie zdefiniowane formaty kart można edytować, ale nie można ich usuwać. Aby cofnąć wszelkie zmiany wprowadzone w predefiniowanym formacie, kliknij ikonę resetowania celem przywrócenia jego ustawień domyślnych. Utworzone formaty kart można usuwać.

	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. Decimal (Dziesiętny): Nazywany również „pozycyjnym systemem liczbowym o podstawie 10”, w którym używane są cyfry 0 – 9. 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. Little endian: Pierwszy bit jest najmniejszy (najmniej znaczący). Big endian: Pierwszy bit jest największy (najbardziej znaczący).



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

Konfigurowanie formatów kart

Edycja formatu karty

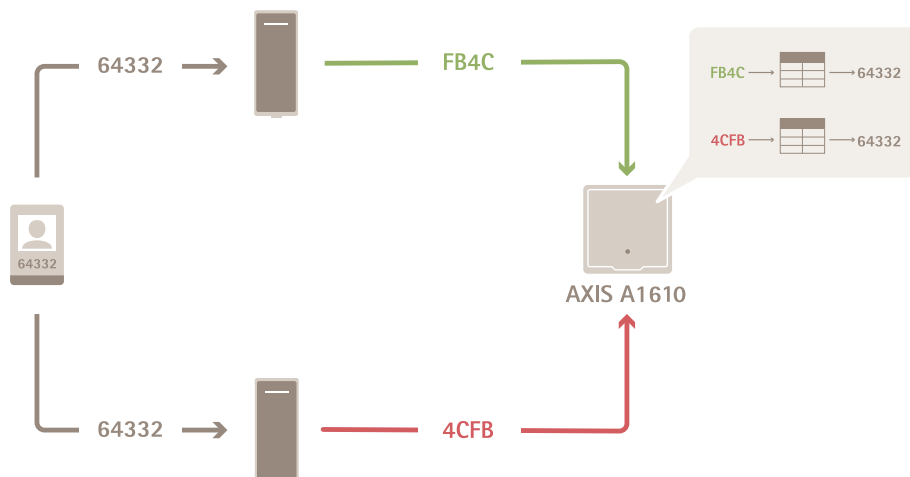
1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Wybierz format karty i kliknij .
3. W przypadku edytowania wstępnie zdefiniowanego formatu karty można edytować tylko opcje **Invert bit order (Odwracanie 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)**.

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.

64332 = 1111 1011 0100 1100 $\longrightarrow$ 0011 0010 1101 1111 = 13023
 $\longrightarrow$ Read from left Read from right $\longleftarrow$

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.

64 332 = 1111 1011 0100 1100 $\longrightarrow$ 0100 1100 1111 1011 = 19707
 F B 4 C 4 C F B

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. Kompletny proces konfigurowania aplikacji AXIS License Plate Verifier w ramach programu AXIS Camera Station Pro opisano w sekcji .

Instalowanie aplikacji AXIS Barcode Reader

1. Pobierz plik instalacyjny aplikacji ze strony *axis.com*.
2. Przejdź do strony internetowej swojego interkomu lub kamery Axis.
3. Zainstaluj aplikację.
4. Aktywuj licencję.
5. Uruchamianie aplikacji.
6. W celu uzyskania lepszej dokładności kodu QR zalecamy zmianę następującego ustawienia kamery.
 - 6.1. Przejdź do strony ustawień kamery.
 - 6.2. W obszarze **Obraz > Ekspozycja** przesun suwak **Stosunek rozmycia do szumu** na środek.

Konfigurowanie aplikacji AXIS Barcode Reader

1. Aby zmienić profil identyfikacji za pomocą kodów QR, wybierz kolejno opcje **Configuration > Access control > Identification profiles** (Konfiguracja > Kontrola dostępu > Profile identyfikacji) i kliknij przycisk . Zobacz *Profile identyfikacji*.
2. Dodaj drzwi. P. sekcja *Dodawanie drzwi*.
3. Jako profil identyfikacji tych drzwi wybierz opcję **QR**. P. sekcja *Ustawienia drzwi*.
4. Dodaj czytnik kodów kreskowych. Zobacz *Dodawanie czytnika*.
 - 4.1. Pod jedną stroną drzwi kliknij przycisk **Add reader (Dodaj czytnik)**.
 - 4.2. Z listy rozwijanej **Reader type (Typ czytnika)** wybierz opcję **AXIS Barcode Reader**. Wprowadź nazwę i kliknij przycisk **OK**.

Tworzenie połączenia z kontrolerem drzwi

1. W programie AXIS Camera Station Pro:
 - 1.1. Przejdź do **Configuration > Access control > Encrypted communication** (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana).
 - 1.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuje klucz)**.
2. W interfejsie WWW urządzenia, na którym działa aplikacja AXIS Barcode Reader:
 - 2.1. otwórz aplikację **AXIS Barcode Reader**.
 - 2.2. Jeśli certyfikat serwera nie został skonfigurowany w aplikacji AXIS Camera Station Pro, włącz **Ignore server certificate validation (Ignoruj sprawdzanie poprawności certyfikatu serwera)**. Więcej informacji znajduje się na stronie *Certificates (Certyfikaty)*.
 - 2.3. Jeśli certyfikat serwera nie został skonfigurowany w aplikacji AXIS Camera Station Pro, włącz **Ignore server certificate validation (Ignoruj sprawdzanie poprawności certyfikatu serwera)**. Więcej informacji znajduje się na stronie *Certificates (Certyfikaty)*.
 - 2.4. Włącz opcję **AXIS Camera Station Secure Entry**.
 - 2.5. Kliknij przycisk **Add (Dodaj)**, a następnie wprowadź adres IP kontrolera drzwi i wklej klucz uwierzytelniania.
 - 2.6. Z rozwijalnego menu wybierz czytnik, który ma służyć do skanowania kodów kreskowych.

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. Domyślny port to 55767. Aby uzyskać niestandardową konfigurację portów, zob. *Ogólne ustawienia serwera, on page 216*.
- 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. Zob. *Generowanie pliku konfiguracyjnego z serwera podrzędnego, on page 174*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. Zob. *Importowanie pliku konfiguracyjnego do serwera głównego, on page 174*.
3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. Zob. *Dodawanie posiadacza karty, on page 185* i *Dodawanie grupy, on page 190*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Zob. *Zarządzanie dostępem, on page 185*.

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 Pro. Sposób dodawania użytkowników w systemie Windows różni się w zależności od wersji. Więcej informacji, p. strona 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 Pro. Zob. *Importowanie użytkowników usługi Active Directory, on page 175*.

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 Pro:

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 187*.

Ważne

W przypadku wyłączenia użytkownika w usłudze Active Directory program AXIS Camera Station Pro trwale usuwa posiadacza karty oraz wszystkie powiązane dane, w tym jego historię. Tego działania nie można cofnąć. Aby zablokować dostęp posiadaczowi karty bez utraty jego danych, należy zawiesić go w programie AXIS Camera Station Pro zamiast wyłączać w usłudze Active Directory.

Konfiguracja programu AXIS Audio Manager Pro

Możesz połączyć się z serwerem AXIS Audio Manager Pro i korzystać z dołączonych do niego urządzeń audio w programie AXIS Camera Station Pro.

Ta konfiguracja wymaga programu AXIS Camera Station Pro w wersji 6.12 lub nowszej oraz programu AXIS Audio Manager Pro w wersji 5.0 lub nowszej. Oba serwery muszą być skonfigurowane – na tym samym serwerze bądź na różnych komputerach w tej samej sieci IP.

Ważne

Jeżeli na tym samym serwerze działa tak program AXIS Camera Station Pro, jak i AXIS Audio Manager Pro, oba korzystają domyślnie z portu 443. Aby zapobiec problemom z połączeniem, skonfiguruj jeden z programów tak, aby korzystał z innego portu.

Konfigurację portów w programie AXIS Camera Station Pro możesz zmienić z użyciem aplikacji *Ogólne ustawienia serwera*, on page 216. Informacje na temat zmiany ustawień portów w programie AXIS Audio Manager Pro znajdują się w instrukcji obsługi programu *AXIS Audio Manager Pro*.

Aby rozpocząć pracę z programem AXIS Audio Manager Pro w AXIS Camera Station Pro:

1. W aplikacji AXIS Audio Manager Pro:
 - 1.1. Przejdź do **System settings > API access** (Ustawienia systemu > Dostęp przez interfejs API).
 - 1.2. Włącz interfejs API i wprowadź nazwę użytkownika oraz hasło.
2. W oprogramowaniu AXIS Camera Station Pro:
 - 2.1. Przejdź do **Configuration > AXIS Audio Manager Pro** (Konfiguracja > AXIS Audio Manager Pro) i kliknij **Connect** (Połącz), aby skonfigurować połączenie z serwerem AXIS Audio Manager Pro.
 - 2.2. W wyskakującym oknie dialogowym wpisz **Server URL** (Adres URL serwera), **API username** (Nazwa użytkownika API) i **API password** (Hasło API) serwera AXIS Audio Manager Pro, a następnie kliknij przycisk **Connect** (Połącz).

Po nawiązaniu połączenia możesz:

- Wyświetlić **Server status** (Stan serwera) w serwerze AXIS Audio Manager Pro i **Device status** (Stan urządzeń) dołączonych do tegoż serwera.
- Otworzyć nową kartę AXIS Audio Manager Pro, aby uzyskać dostęp do interfejsu internetowego serwera.
- Korzystanie z nowych funkcji związanych z dźwiękiem w programie AXIS Camera Station Pro.

Więcej informacji znajduje się w sekcji *AXIS Audio Manager Pro*, on page 207.

Uwaga

Aby uniknąć problemów związanych z certyfikatami, zaleca się utworzenie lub uzyskanie certyfikatu z zaufanego urzędu certyfikacji (CA – UC), przesłanie go do programu AXIS Audio Manager Pro i dodanie do listy zaufanych certyfikatów serwera AXIS Camera Station Pro. Więcej informacji znajduje się w instrukcji obsługi aplikacji *AXIS Audio Manager Pro*.

Konfigurowanie funkcji Inteligentne wyszukiwanie 2

W funkcji Inteligentne wyszukiwanie 2 można ustawić filtry na potrzeby znajdowania ludzi i pojazdów w nagraniach z kamer Axis.



Wymagania, ograniczenia i zasady posługiwania się funkcją Smart Search 2 (Inteligentne wyszukiwanie 2) omówiono w temacie *Inteligentne wyszukiwanie 2*, on page 38.

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 obszarze **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 pojawiające się tylko przez chwilę, albo obiekty kołyszące się takie jak listowie.
Filtry funkcji inteligentnego wyszukiwania wykorzystują wszystkie istniejące filtry ustawień ruchu jako punkt wyjścia.
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. Zaznacz **Include periods with missing metadata (Uwzględnij okresy z brakującymi metadanymi)**, aby wyświetlić wyniki dotyczące okresów, dla których nie zapisano 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. Pojawia się w przypadku, 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.

Zdarzenia powodujące uruchomienie nagrywania

Możesz skonfigurować inteligentne filtry wyszukiwania jako wyzwalacze w regułach działań. Aby utworzyć wyzwalacz inteligentnego wyszukiwania:

1. Przejdź do **Configuration > Smart search 2 > Triggers (Konfiguracja > Inteligentne wyszukiwanie 2 > Wyzwalacze)**.
2. Kliknij polecenie **Create (Utwórz)**.
3. Ustaw filtr. Więcej informacji na temat filtrów inteligentnego wyszukiwania znajduje się w sekcji *Wyszukiwanie z filtrami, on page 38*.
4. Kliknij **Next (Dalej)**.
5. Dostosuj poziom **Confidence (Ufność)** wykrywania. Wyższy poziom ufności pozwala odfiltrować niepewne klasyfikacje, zmniejszając liczbę detekcji.
6. Kliknij **Next (Dalej)**.
7. Wpisz nazwę wyzwalacza i kliknij **Save (Zapisz)**.

Uwaga

- Funkcja Inteligentne wyszukiwanie 2 zazwyczaj potrzebuje kilku sekund po tym, jak obiekt opuścił pole widzenia kamery, aby przeanalizować materiał i zweryfikować detekcję. Na przykład, jeżeli ustawiłeś regułę działania tak, aby była wyzwalana po wykryciu czerwonego samochodu, działanie zostanie uruchomione dopiero kilka sekund po zniknięciu obiektu z pola widzenia kamery.
- Podobieństwo wizualne (**Visual similarity**) nie jest dostępne jako opcja dla wyzwalaczy funkcji Smart search 2.
- Utworzenie wyzwalacza dla kamery umożliwia serwerowi przetwarzanie wykrytych obiektów, nawet jeżeli dla tej kamery wyłączona jest funkcja **Enable background processing** (Włącz przetwarzanie w tle).
- Okresy opóźnionej detekcji (**Delayed detection periods**) to okresy charakteryzujące się dużym opóźnieniem przetwarzania, które powodują opóźnienie uruchomienia reguł działań. Jeżeli mają miejsce często, można zmienić konfigurację filtra wyzwalającego, aby obejmował mniej kamer, a także użyć filtrów kamer takich jak przekroczenie linii, obszar, wielkość i czas trwania, aby zmniejszyć opóźnienia przetwarzania.

Aby użyć wyzwalacza funkcji Smart search 2 w regule działania, p. sekcja *Tworzenie wyzwalaczy funkcji Smart search 2, on page 105*.

Konfigurowanie funkcji Monitorowanie stanu systemu ^{BETA}

Uwaga

- W przypadku aktywnego połączenia z wieloma serwerami AXIS Camera Station Pro można dokonać konfiguracji funkcji Monitorowanie stanu systemu na dowolnym połączonym serwerze. W tym celu wybierz serwer z rozwijalnego menu **Selected server (Wybrany serwer)**.
- Jeśli zarządzasz systemami w różnych sieciach, monitorowanie serwera w My Systems zapewnia tę samą funkcjonalność, ale za pośrednictwem chmury.

Ustawienia

Połączenie z chmurą	Jeżeli serwer został zarejestrowany w organizacji, możesz przeglądać dane dotyczące stanu systemu z dowolnego miejsca. Jeżeli nie masz jeszcze połączenia, kliknij Manage (Zarządzaj) i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
Częstotliwość odczytu danych	Wybierz niższą częstotliwość odczytu danych, aby wyeliminować ostrzeżenia dotyczące nieaktualnych danych lub ogólnych problemów z płynnością działania. W przypadku konfiguracji wielosystemowej zaleca się zastosowanie do podsystemu takiego samego lub wyższego ustawienia jak w przypadku jego systemu nadrzędnego. • Low (Niska) – w przypadku systemów z ponad 100 urządzeniami. • Medium (Średnia) – w przypadku systemów obejmujących 25 – 100 urządzeń. • High (Wysoka) – w przypadku systemów z mniej niż 25 urządzeniami.

Powiadomienia

Aby wysyłać powiadomienia pocztą elektroniczną:

1. Skonfiguruj serwer SMTP oraz serwer poczty e-mail, za pośrednictwem których będą wysyłane powiadomienia. Zob. *Ustawienia serwera, on page 127*

2. Skonfiguruj adresy e-mail, na które będą odbierane powiadomienia. Zob. *Konfigurowanie odbiorców poczty e-mail, on page 179*.
3. Skonfiguruj reguły powiadamiania. Zob. *Konfigurowanie reguł powiadamiania, on page 179*.

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**). Komunikat potwierdza wysłanie testowej wiadomości e-mail.

Konfigurowanie reguł powiadamiania

Domyślnie włączone są dwie reguły powiadamiania.

System nie działa – Wysyłanie powiadomienia, gdy system w konfiguracji jednokomputerowej lub dowolny system w konfiguracji wielokomputerowej nie działa przez czas dłuższy niż zwykle.

Urządzenie nie działa – Wysyłanie powiadomienia, gdy urządzenie wyszczególnione w oknie funkcji System Health Monitoring (Monitorowanie stanu systemu) nie działa przez czas dłuższy niż zwykle.

1. Wybierz kolejno opcje **Configuration > System Health Monitoring > Notifications** (**Konfiguracja > Monitorowanie stanu systemu > Powiadomienia**).
2. W obszarze **Notification rules** (Reguły powiadomień) możesz włączyć lub wyłączyć reguły powiadomień.
3. W obszarze **Applied rules** (Zastosowane reguły) zostanie wyświetlona lista systemów i urządzeń oraz zastosowanych do nich reguł powiadomień.

Multisystem



W funkcji Monitorowania stanu systemu z jednego systemu głównego można śledzić kondycję różnych systemów podrzędnych.

1. W systemie dodatkowym wygeneruj konfigurację systemu. Zob. *Generuj konfigurację systemu, on page 179*.
2. Na komputerze głównym wczytaj konfigurację systemu. Zob. *Pobierz dane z innych systemów, on page 180*.
3. Powtórz poprzednie czynności w pozostałych systemach podrzędnych.
4. Odtąd w systemie głównym można śledzić informacje o kondycji różnych komputerów podrzędnych. Zob. *Monitorowanie stanu systemu ^{BETA}, on page 197*.

Generuj konfigurację systemu

1. Wybierz kolejno opcje **Configuration > System Health Monitoring > Multisystem** (**Konfiguracja > Monitorowanie stanu systemu > Multisystem**).
2. Kliknij przycisk **Generate** (**Generuj**).
3. Kliknij **Copy** (**Kopiuj**), aby skopiować plik w celu przesłania do systemu głównego.

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 przesłaniu 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 konfigurację systemową systemu podległego można przesłać do głównego systemu.

1. Na głównym komputerze wybierz kolejno opcje **Configuration > System Health Monitoring > Multisystem (Konfiguracja > Monitorowanie stanu systemu > Multisystem)**.
2. Kliknij przycisk **Paste (Wklej)**, aby dodać informacje skopiowane z podległego systemu.
3. Sprawdź adres IP hosta i kliknij przycisk **Add (Dodaj)**.
Podrzędny system będzie wyświetlany w oknie **Available systems (Dostępne systemy)**.

Konfigurowanie funkcji analitycznych

AXIS Data Insights Dashboard

Pulpit **AXIS Data Insights Dashboard** przedstawia dane analityczne z urządzeń w postaci wykresów i tabel. Strona konfiguracji pulpitu **AXIS Data Insights Dashboard** pokazuje wszystkie obsługiwane aplikacje oraz scenariusze skonfigurowane w urządzeniach wchodzących w skład systemu. Przejdź do obszaru **Analytics (Analizy) > Data Insights Dashboard**, aby zyskać następujące możliwości:

- Wyświetlanie listy kamer i źródeł danych, w których są uruchomione obsługiwane aplikacje.
- Wyświetlanie listy obsługiwanych aplikacji i scenariuszy dla każdego urządzenia lub źródła danych. Obsługiwane są następujące aplikacje i scenariusze:
 - **AXIS Object Analytics** – zliczanie naruszeń i wykrywanie obecności w obszarze
 - **AXIS Audio Analytics**
 - **AXIS Image Health Analytics**
 - **AXIS People Counter**
 - **AXIS P8815-2 3D Counter**
 - Czujniki **AXIS Air Quality Sensor** (monitorowanie jakości powietrza)

Uwaga

Można przechowywać maksymalnie 100 MB danych, co ogranicza czas przechowywania w zasobie pamięci. Na przykład w przypadku czujnika jakości powietrza monitorującego wszystkie 12 typów danych czas przechowywania wynosi około 430 dni.

- Wybór scenariuszy do dodania na pulpicie nawigacyjnym.
- Oznaczenie scenariuszy do filtrowania danych na pulpicie nawigacyjnym, np. w celu zgrupowania kamer w tej samej lokalizacji.

Uwaga

Aby wyświetlić dane zliczania naruszeń linii w aplikacji **AXIS Object Analytics** w panelu **In and Out counting (Zliczanie wchodzących i wychodzących)**, wybierz kierunek scenariusza, zaznaczając opcję **In (Wchodzący)** lub **Out (Wychodzący)** w polu **Direction (Kierunek)**.

- Wyświetlanie stanu scenariuszy.

Dołącz	Włącz przełącznik w kolumnie Include (Uwzględnij) , aby wyświetlać dane scenariusza na pulpicie nawigacyjnym.
Znaczniki	Wybierz znaczniki z menu rozwijanego w kolumnie Tags (Tagi) , aby dodać je do scenariusza.

Aby dodać nowy tag:

1. Otwórz kartę **Tags (Tagi)**.
2. Nadaj tagowi nazwę.
3. Kliknij strzałkę.

Uwaga

- Aplikacja AXIS Data Insights wymaga protokołu TLS w wersji 1.2 lub nowszej do szyfrowania połączeń na serwerze Windows.
- Pulpit AXIS Data Insights Dashboard zastępuje wszelkie istniejące ustawienia MQTT w kamerze, jeśli:
 - Kamera nie ma skonfigurowanego klienta MQTT.
 - Zostanie ręcznie włączony scenariusz dla kamery połączonej z innym serwerem AXIS Camera Station Pro.
- Po nawiązaniu połączenia z pulpitem AXIS Data Insights klient MQTT w kamerze jest zarezerwowany dla pulpitu Data Insights.
- Kamery i serwer AXIS Camera Station Pro muszą się znajdować w tej samej sieci.
- Aby uzyskać optymalną wydajność, zalecany jest serwer z co najmniej 16 GB pamięci RAM do uruchamiania aplikacji AXIS Data Insights Dashboard w programie AXIS Camera Station Pro.
- Można przechowywać maksymalnie 100 MB danych, ale ogranicza to czas ich przechowywania z zasobie pamięci. Na przykład:
 - Szacowanie zajętości na parkingu wyposażonym w cztery kamery, z których każda jest skonfigurowana do detekcji w trybie 24/7 pięciu podklas pojazdów takich jak samochody osobowe i rowery / motocykle daje w rezultacie 260-dniowy okres przechowywania.
 - Zliczanie osób w sklepie detalicznym wyposażonym w osiem kamer i cechującym się ciągłym przepływem osób w okresie 12 godzin daje w rezultacie około 1270-dniowy okres przechowywania.
 - Kamera obsługująca scenariusz zliczania naruszeń linii z sześcioma klasami przy stałym zliczaniu przez 24 godziny daje w rezultacie około 860-dniowy okres przechowywania.

Aby się dowiedzieć, jak dodać pulpit do widoku dzielonego, zob. *Pulpit AXIS Data Insights w widoku dzielonym*, on page 20.



Jak włączyć pulpit AXIS Data Insights

License Plate Verifier do weryfikacji tablic rejestracyjnych

Na stronie License plate verifier (Weryfikator tablic rejestracyjnych) sprawdzisz stan działania aplikacji AXIS License Plate Verifier w poszczególnych kamerach i pogrupujesz kamery, co ułatwi zarządzanie listą.

Karta **Cameras (Kamery)** zawiera listę wszystkich podłączonych urządzeń z zainstalowaną aplikacją **AXIS License Plate Verifier**:

- **Camera (Kamera):** Nazwa kamery.
- **Version (Wersja):** Wersja aplikacji **AXIS License Plate Verifier** zainstalowana w kamerze.
- **Status:** Bieżący status aplikacji **AXIS License Plate Verifier**.
- **Latest event (Ostatnie zdarzenie):** Czas ostatniego zdarzenia zarejestrowanego przez kamerę.
- **Allowed (Dozwolone):** Liczba tablic rejestracyjnych umieszczonych na liście **Allowed (Dozwolone)** kamery.
- **Blocked (Zablokowane):** Liczba tablic rejestracyjnych umieszczonych na liście **Blocked (Zablokowane)** kamery.
- **Custom (Niestandardowe):** Liczba tablic rejestracyjnych umieszczonych na liście **Custom (Niestandardowe)** kamery.
- **Group (Grupa):** Grupa, do której należy kamera.

Na karcie **Groups (Grupy)** wyświetlone są wszystkie grupy kamer i kamery należące do każdej z nich. Na tej karcie można wykonać następujące operacje:

- Kliknij **New...** (Nowa...), aby dodać nową grupę.
- Kliknij **Delete (Usuń)**, aby usunąć istniejącą grupę.
- Zmień nazwę wybranej grupy w polu **Group name (Nazwa grupy)**.
- Kliknij **Add...** (Dodaj...), aby dodać kamerę do wybranej grupy.
- Kliknij **Remove (Usuń)**, aby usunąć kamerę z grupy.

Możesz tworzyć wspólne listy dla zgrupowanych kamer. Więcej informacji można znaleźć w temacie *Zarządzanie tablicami rejestracyjnymi, on page 206*.

Konfiguracja urządzenia nasobnego

Podłączanie systemu nasobnego

Podłącz system nasobny do programu **AXIS Camera Station Pro**, aby przesłać nagrania i metadane z kamer nasobnych.

1. Przejdź do **Configuration (Konfiguracja) > Body worn (Urządzenia nasobne) > Connect a body worn system (Podłączanie systemu nasobnego)**.
2. Wybierz preferowany sposób połączenia w sekcji **Connection method (Metoda połączenia)**:
 - **Connect directly (Połącz bezpośrednio):** Wpisz adres IP aplikacji **Body Worn Manager** i dane logowania.
 - **Generate connection file (Wygeneruj plik połączenia):** Utwórz plik konfiguracji do przesłania do aplikacji **Body Worn Manager**.

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 142*.

Jeśli wybrano opcję **Connect directly (Połącz bezpośrednio)**:

3. W sekcji **Configure direct connection (Skonfiguruj połączenie bezpośrednie)** wprowadź **IP address (adres IP)**, **User name (Nazwa użytkownika)** oraz **Password (Hasło)** dla programu **Body Worn Manager**.
1. W razie potrzeby zmień **AXIS Camera Station system name (Nazwa systemu AXIS Camera Station)**. Nazwa ta określa miejsce docelowe do przechowywania skopiowanych i przesłanych nagrań.
2. Jeśli chcesz zamknąć wszystkie istniejące połączenia, wybierz opcję **End existing connections (Zakończ istniejące połączenia)**. Prześlij nowy plik połączenia do każdego kontrolera **AXIS Body Worn System**.

3. Kliknij przycisk **Połącz**.

Jeśli wybrano opcję **Generate connection file (Wygeneruj plik połączenia)**:

4. W sekcji **Generate connection file (Wygeneruj plik połączenia)** można w razie potrzeby zmienić **AXIS Camera Station system name (Nazwa systemu AXIS Camera Station)**. Pomaga ona określić, gdzie nagrania są kopiowane lub przesyłane.
 - 4.1. Jeśli chcesz zamknąć wszystkie istniejące połączenia, wybierz opcję **End existing connections (Zakończ istniejące połączenia)**. Prześlij nowy plik połączenia do każdego kontrolera AXIS Body Worn System.
 - 4.2. Kliknij opcję **Export (Eksportuj)** i zapisz plik połączenia.
 - 4.3. Prześlij plik połączenia do aplikacji Body Worn Manager.



Konfigurowanie systemu nasobnego Axis



Odtwarzane i eksportowane nagrania z kamery nasobnej Axis

Ujęcia

Automatycznie eksportuj ujęcia z zakładki kamer nasobnych do folderu podczas przesyłania nagrań do AXIS Camera Station Pro.

1. Przejdź do **Configuration (Konfiguracja) > Body worn (Urządzenia nasobne) > Snapshots (Ujęcia)**.
2. W lokalizacji pamięci masowej **Storage location** wpisz ścieżkę dostępu do folderu, w którym mają być zapisywane ujęcia.
3. Kliknij przycisk **Apply (Zastosuj)**.
4. Włącz opcję **Snapshot export (Eksport ujęć)**.

Integracja CAD

Zintegruj swój system komputerowego wspomagania dyspozytorów (CAD), aby automatycznie klasyfikować nagrania z kamer nasobnych na podstawie danych dyspozytorskich.

Aby skonfigurować integrację:

1. Przejdź do **Configuration (Konfiguracja) > Body worn (Urządzenia nasobne) > CAD integration (Integracja CAD)**.
2. Kliknij **Set up integration (Konfiguruj integrację)**.
3. Wybierz format pliku (CSV lub XML) i kliknij **Next (Dalej)**.
4. Jeśli plik CAD znajduje się na udostępnionym dysku sieciowym, włącz opcję **Shared network drive (Udostępniony dysk sieciowy)**.
5. Wprowadź ścieżkę do folderu zawierającego plik CAD, nazwę pliku (tylko w przypadku plików CSV) oraz separator kolumn.

6. Kliknij **Next (Dalej)**.
7. Przypisz każde pole do identyfikatora zgodnie z jego nazwą w pliku CAD:
 - **Officer name (Nazwa funkcjonariusza)**: musi odpowiadać nazwom kamer wirtualnych w AXIS Camera Station Pro. Jeśli nazwa nie jest zgodna, należy ją zaktualizować w programie Body Worn Manager, a nie w AXIS Camera Station Pro.
 - **Event ID (Identyfikator zdarzenia)**: unikalny identyfikator zgłoszenia.
 - **Kategoria zgłoszenia**: kategoria nagrania. Jeśli nie istnieje, zostanie utworzona.
 - **Czas zgłoszenia**: czas rozpoczęcia w formacie RFC 3339, np. „2025-11-25T09:49:17+01:00”.
 - **Czas zakończenia zgłoszenia**: czas zakończenia w formacie RFC 3339.
 - **Numer sprawy**: identyfikator sprawy powiązanej ze zgłoszeniem. Kolumna musi istnieć w pliku, ale wartość może pozostać pusta.
8. Kliknij **Finish (Zakończ)**, a następnie **Apply (Zastosuj)**.
9. Aby przejrzeć nagrania, kliknij **+** i wybierz **CAD recordings (Nagrania CAD)**, aby wyświetlić wszystkie automatycznie sklasyfikowane nagrania. Wyniki można filtrować według czasu lub nazwy funkcjonariusza.

Uwaga

Jeżeli nowe kategorie zostaną utworzone automatycznie, musisz ręcznie ustawić okres ich przechowywania.

Ograniczenia

Informacje mogą zostać utracone, jeśli:

- Program AXIS Camera Station Pro lub odpowiedni komponent nie jest uruchomiony.
- Pliki eksportu mają rozmiar większy niż 1 GB.
- Sieciowe dane uwierzytelniające wymagają aktualizacji.

Ustawienia urządzenia noszalnego

Skonfiguruj lokalizację pamięci dla nagrań z kamer noszonych.

Pamięć masowa nagrań

Wybierz domyślną lokalizację pamięci masowej do przechowywania nagrań z urządzeń noszonych dla nowych użytkowników systemu:

1. Przejdź do **Configuration (Konfiguracja) > Body worn (Urządzenia noszone) > Body worn settings (Ustawienia urządzeń noszonych)**.
2. W obszarze **Recording storage (Pamięć masowa nagrań)** wybierz dysk z listy rozwijalnej **Disk (Dysk)**.
3. Kliknij przycisk **Save (Zapisz)**.

Pamięć masowa odrzuconych nagrań

Wybierz lokalizację, w której będą przechowywane odrzucone treści z systemu noszonego:

1. W obszarze **Rejected recordings storage (Pamięć masowa odrzuconych nagrań)** wybierz dysk z listy rozwijalnej **Disk (Dysk)** i wprowadź nazwę folderu w polu **Folder**.
2. W polu **Number of days to keep rejected content from the body worn system (Liczba dni przechowywania odrzuconej zawartości z systemu noszonego)** ustaw liczbę dni, przez które ma być przechowywana odrzucona zawartość.
3. Kliknij przycisk **Save (Zapisz)**.

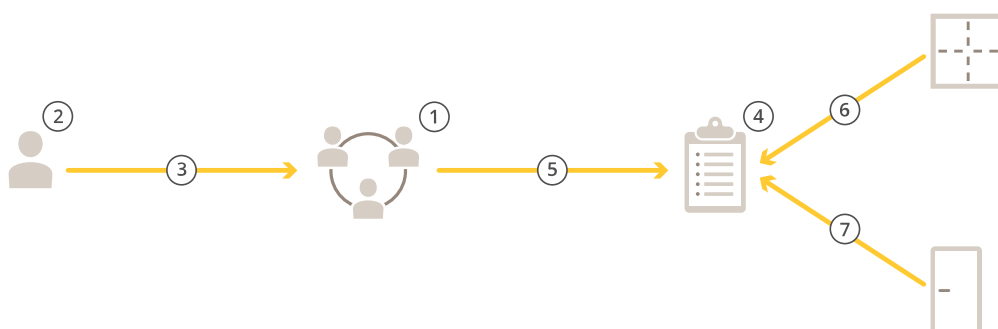
Zarządzanie dostępem

Użyj karty **Access management** (Zarządzanie dostępem) do konfigurowania i zarządzania posiadaczami kart, grupami i regułami dostępu w systemie.

Kompletny proces konfigurowania sieciowego kontrolera drzwi Axis w oprogramowaniu AXIS Camera Station Pro opisano w temacie *Konfigurowanie sieciowego kontrolera drzwi Axis*.

Proces zarządzania dostępem

Struktura zarządzania dostępem jest elastyczna, zatem możesz utworzyć schemat pracy, który najlepiej odpowiada potrzebom użytkownika. Przykładowy schemat pracy:



1. *Dodawanie grupy, on page 190.*
2. *Dodawanie posiadacza karty, on page 185.*
3. Dodaj posiadaczy kart do grup.
4. *Dodaj regułę dostępu, on page 190.*
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 użytkownika karty, podając dane uwierzytelniające pozwalające zidentyfikować daną osobę oraz określając, kiedy i w jaki sposób może ona uzyskać dostęp do drzwi.

Można również mapować użytkowników w bazie danych usługi Active Directory jako posiadaczy kart. Zob. *Ustawienia usługi Active directory^{BETA}, on page 175.*

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do **Cardholder management > Cardholders** (Zarządzanie posiadaczami kart > Posiadacze kart) i kliknij **+ Add** (Dodaj).
3. Wprowadź imię i nazwisko posiadacza karty. W razie potrzeby podaj dodatkowe dane posiadacza karty:
 - W polu **Email (Adres e-mail)** wpisz adres e-mail posiadacza karty.
 - W polu **Groups (Grupy)** wybierz grupy, do których chcesz dodać posiadacza karty.
 - W polu **Access rules (Reguły dostępu)** wybierz reguły dostępu, które chcesz zastosować do posiadacza karty.
4. Aby dodać zdjęcie, kliknij **Cardholder picture (Zdjęcie posiadacza karty)** i wybierz:
 - **Upload (Prześlij)**, aby dodać zdjęcie z urządzenia.

- **Capture (Zrób zdjęcie)**, aby zrobić zdjęcie bezpośrednio za pomocą aparatu.

Uwaga

Zdjęcie musi być w formacie JPG, PNG lub GIF. Zdjęcia są automatycznie konwertowane do maksymalnej rozdzielczości 700 x 700 pikseli i formatu JPG.

5. Kliknij **Advanced (Zaawansowane)**, aby skonfigurować dodatkowe opcje.
6. Dodaj poświadczenie do posiadacza karty. Zob. *Dodaj poświadczenia*, on page 187.
7. Kliknij przycisk **Save (Zapisz)**.
8. Aby wydrukować identyfikatory, wybierz jednego lub więcej posiadaczy kart i kliknij **Print Badge^{BETA}** (Drukuj identyfikator). Więcej informacji, p. sekcja *Drukowanie identyfikatorów^{BETA}*, on page 196.

Użyj pola wyszukiwania, aby wyszukać posiadacza karty według imienia lub nazwiska. Aby filtrować według źródła, kliknij opcję **Filter (Filtruj)**, a następnie **Local (Lokalne)**, **Global (Globalne)**, **AD** lub **Center (Centralne)**.

Zaawansowane	
Długi czas dostępu	Wybierz tę opcję, aby w sytuacji gdy jest zainstalowany monitor drzwi, posiadacz karty otrzymał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi.
Zawieś posiadacza karty	Wybierz, aby zawiesić posiadacza karty. Powoduje to tymczasowe zablokowanie dostępu dla posiadacza karty.
Zezwól na podwójne przeciągnięcie	Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Posiadacz karty może tego na przykład użyć do odblokowania drzwi poza regularnym harmonogramem.
Zwolnienie z blokady ogólnej	Zaznacz tę opcję, aby zapewnić posiadaczowi karty dostęp w okresie odcięcia obszaru.
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. Zob. <i>Multyserwer^{BETA}</i> , on page 173.



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:

- Poświadczenie w postaci kodu QR, on page 187
- Poświadczenie przez PIN, on page 187
- Poświadczenia mobilne, on page 188
- Poświadczenie kartą, on page 188
- Uwierzytelnienie tablicy rejestracyjnej, on page 188

Data wygaśnięcia	
Ważne od	Ustaw datę i godzinę, od kiedy uwierzytelnienie zacznie obowiązywać.
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 uwierzytelnienie będzie ważne po ostatnim użyciu. Wybierz dni, miesiące lub lata po ostatnim użyciu.

Poświadczenie w postaci kodu QR

Uwaga

Korzystanie z kodów QR jako uwierzytelnień wymaga zsynchronizowania czasu w kontrolerze systemowym i kamerze z aplikacją AXIS Barcode Reader. Zaleca się korzystanie z tego samego źródła czasu dla obu urządzeń, aby utrzymać synchronizację czasu.

Aby dodać do posiadacza karty poświadczenie w postaci kodu QR:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij  **Add** (Dodaj) i wybierz **QR-code** (Kod QR).
2. Wprowadź nazwę poświadczenia.
3. Domyślnie jest włączona opcja **Dynamic QR** (Dynamiczny kod QR). Musisz użyć jej z uwierzytelnieniem PIN.
4. Ustaw datę początkową i końcową poświadczenia.
5. Aby kod QR był wysyłany przez e-mail 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**.

Poświadczenie przez PIN

Aby dodać do posiadacza karty poświadczenie w postaci numeru PIN:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij  **Add** (Dodaj) i wybierz **PIN** (Kod PIN).
2. Wprowadź numer PIN.

3. Opcjonalnie, aby wywołać cichy alarm za pomocą odrębnego kodu PIN, włącz **Duress PIN** (Kod PIN pod przymusem) i wpisz kod PIN do podania w sytuacji zagrożenia.
4. Ustaw daty ważności poświadczenia: **Valid from** (Ważne od) i **Valid to** (Ważne do).
5. Kliknij **Dodaj**.

Poświadczenia mobilne

Uwaga

Posiadacz karty musi mieć adres e-mail, aby otrzymać poświadczenie mobilne.

Aby dodać poświadczenie mobilne do posiadacza karty:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij  **Add (Dodaj)** i wybierz **Mobile credential** (Uwierzytelnienia mobilne).
2. Wprowadź nazwę poświadczenia.
3. Ustaw datę początkową i końcową poświadczenia.
4. Wybierz **Send the mobile credential to the cardholder after saving** (Po zapisaniu wyślij poświadczenie mobilne do posiadacza karty). Posiadacz karty otrzyma wiadomość e-mail z instrukcją parowania.
5. Kliknij **Dodaj**.

Przykład, p. sekcja *Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth, on page 163*.

Poświadczenie kartą

Aby dodać do posiadacza karty poświadczenie w postaci karty:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij  **Add (Dodaj)** i wybierz **Card** (Karta).
2. Aby ręcznie wprowadzić dane karty, podaj nazwę karty, jej numer i liczbę bitów.

Uwaga

Liczbę bitów można określić tylko w przypadku tworzenia formatu karty o liczbie bitów, która nie jest jeszcze zdefiniowana w systemie.

3. Aby następowało automatyczne pobieranie danych ostatnio okazanej 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 readers** (Odczytaj dane ostatniej okazanej karty z czytników).

Uwaga

Do skanowania 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**.

Uwierzytelnienie tablicy rejestracyjnej

Aby dodać do posiadacza karty poświadczenie w postaci tablicy rejestracyjnej:

1. W obszarze **Credentials** (Uwierzytelnienia) 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**.

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 Pro. Zob. *Dodawanie urządzeń, on page 6*.
2. Uaktualnij oprogramowanie sprzętowe na nowych urządzeniach do najnowszej dostępnej wersji. Zob. *Aktualizuj oprogramowanie sprzętowe, on page 69*.
3. Dodaj nowe drzwi połączone z kontrolerem drzwi. Zob. *Dodaj drzwi, on page 152*.
 - 3.1. Dodaj czytnik w obszarze **Side A (Strona A)**. Zob. *Dodawanie czytnika, on page 161*.
 - 3.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
 - 3.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
 - 3.4. Kliknij przycisk **Ok**.
4. Zainstaluj i włącz w kamerze aplikację **AXIS License Plate Verifier**. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
5. Włącz aplikację **AXIS License Plate Verifier**.
6. Skonfiguruj aplikację **AXIS License Plate Verifier**.
 - 6.1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.
 - 6.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuje klucz)**.
 - 6.3. Otwórz aplikację **AXIS License Plate Verifier** z poziomu interfejsu WWW kamery.
 - 6.4. Pomiń kreatora konfiguracji.
 - 6.5. Przejdź do opcji **Settings (Ustawienia)**.
 - 6.6. W obszarze **Access control (Kontrola dostępu)** wybierz **Secure Entry (Bezpieczne wejście)** jako **Type (Typ)**.
 - 6.7. W obszarze **IP address (Adres IP)** wpisz adres IP kontrolera drzwi.
 - 6.8. W obszarze **Authentication key (Klucz uwierzytelniania)** wklej skopiowany wcześniej klucz uwierzytelniania.
 - 6.9. Kliknij przycisk **Połącz**.
 - 6.10. W obszarze **Door controller name (Nazwa kontrolera drzwi)** wybierz kontroler drzwi.
 - 6.11. W obszarze **Reader name (Nazwa czytnika)** wybierz czytnik dodany wcześniej.
 - 6.12. Włącz integrację.
7. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Zob. *Dodawanie posiadacza karty, on page 185*
8. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Zob. *Dodaj poświadczenia, on page 187*
9. Dodaj regułę dostępu. Zob. *Dodaj regułę dostępu, on page 190*.
 - 9.1. Dodaj harmonogram.
 - 9.2. Dodaj posiadacza karty, któremu chcesz przyznać dostęp na podstawie odczytu numeru tablicy rejestracyjnej.
 - 9.3. Dodaj drzwi z czytnikiem **AXIS License Plate Verifier**.

Dodawanie grupy

Grupy umożliwiają zbiorcze zarządzanie posiadaczami kart i ich regułami dostępu.

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do **Cardholder management > Groups** (Zarządzanie posiadaczami kart > Grupy) i kliknij **+ Add** (Dodaj).
3. Wprowadź nazwę i opcjonalnie inicjały grupy.
4. Wybierz **Global group** (Grupa globalna), aby wyświetlić i monitorować posiadaczy kart na serwerach podległych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Zob. *Multiserwer^{BETA}, on page 173*.
5. Dodawanie posiadaczy kart do grupy:
 - 5.1. Kliknij **+ Add** (Dodaj).
 - 5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add** (Dodaj).
6. Kliknij przycisk **Save** (Zapisz).
7. Aby wydrukować identyfikatory dla wszystkich posiadaczy kart w grupie, wybierz grupę i kliknij opcję **Print Badge^{BETA}** (Drukuj identyfikator). Więcej informacji, p. sekcja *Drukowanie identyfikatorów^{BETA}, on page 196*.

Dodaj regułę 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.

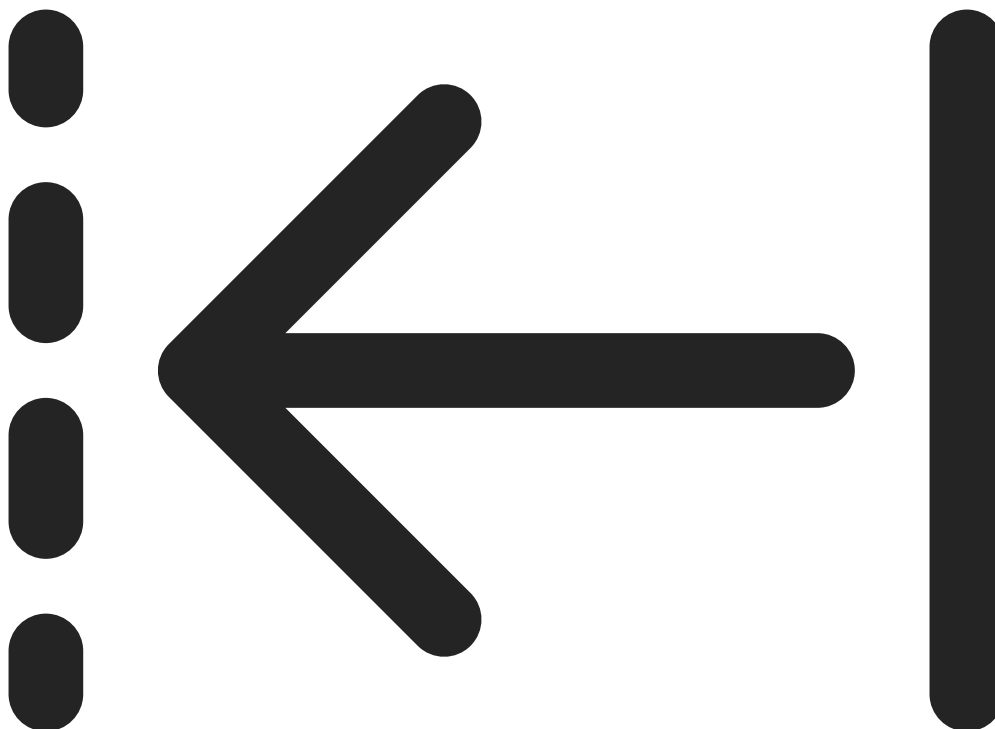
Drzwi i strefy – gdzie ma zostać przyznany dostęp.

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)**.

5.3. Można również przeciągnąć i upuścić posiadacza karty lub grupę bezpośrednio na regułę dostępu, aby ją zastosować. Podczas przeciągania elementów podświetlane są reguły dostępu, na które można je upuścić. W przypadku jednoczesnego przeciągnięcia wielu posiadaczy kart lub grup pojawi się liczba wskazująca przenoszoną ilość.

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 **Save (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)**.



Eksportowanie raportów konfiguracji systemu

Można eksportować raporty zawierające różne rodzaje informacji o systemie. AXIS Camera Station Pro eksportuje raporty jako plik CSV (zawierający wartości rozdzielone przecinkami) i zapisuje je 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.

Tworzenie raportów aktywności posiadaczy kart

Raport imienny zawiera listę posiadaczy kart przebywających w określonej strefie, ułatwiając ustalenie osób obecnych w danym momencie.

Raport ze zbiórki zawiera listę posiadaczy kart obecnych w określonej strefie, ułatwiając ustalenie, kto jest bezpieczny, a kto zaginął w sytuacji awaryjnej. Pomaga zarządcom budynków w lokalizacji pracowników i odwiedzających po ewakuacji. Miejsce zbiórki to wyznaczony czytnik, do którego pracownicy zgłaszają się w sytuacjach awaryjnych. System generuje raport dotyczący osób przebywających na terenie obiektu i poza nim.

System oznacza posiadaczy kart jako zaginionych, dopóki nie zameldują się w punkcie zbiórki lub dopóki inna osoba nie oznaczy ich ręcznie jako bezpiecznych.

Zarówno raporty imienne, jak i raporty ze zbiorów wymagają stref do śledzenia posiadaczy kart.

Aby utworzyć i uruchomić raport imienny lub ze zbiórki:

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Reports (Raporty) > Cardholder activity (Aktywność posiadaczy kart)**.
3. Kliknij **+ Add (Dodaj)** i wybierz **Roll call / Mustering (Imienny / Zbiórka)**.
4. Wprowadź nazwę raportu.
5. Wybierz strefy do uwzględnienia w raporcie.
6. Wybierz grupy do uwzględnienia w raporcie.
7. Jeżeli chcesz otrzymać raport ze zbiórki, wybierz **Mustering point (Punkt zbiórki)** i czytnik.
8. Wybierz ramy czasowe raportu.
9. Kliknij przycisk **Save (Zapisz)**.
10. Wybierz raport i kliknij **Run (Uruchom)**.

Stan w raporcie imiennym	Opis
Present (Obecny)	Posiadacz karty wszedł do określonej strefy i nie opuścił jej do czasu uruchomienia raportu.
Not present (Nieobecny)	Posiadacz karty opuścił określoną strefę i nie wszedł do niej ponownie do czasu uruchomienia raportu.

Stan w raporcie ze zbiórki	Opis
Safe (Bezpieczny)	Posiadacz karty przeciągnął swoją kartę w punkcie zbiórki.
Missing (Zaginiony)	Posiadacz karty nie przeciągnął swojej karty w punkcie zbiórki.

Import i eksport

Importuj posiadaczy kart

Ta opcja służy do importowania danych posiadaczy kart, grup, uwierzytelnień oraz zdjęć 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 wcześniej zapisaną konfigurację.

Można również mapować użytkowników w bazie danych usługi Active Directory jako posiadaczy kart. Zob. *Ustawienia usługi Active directory^{BETA}, on page 175*.

Opcje importu	
Nowość	Usuwa istniejące dane posiadaczy kart i dodaje nowych posiadaczy kart.
Aktualizuj	Aktualizuje dane istniejących posiadaczy kart i dodaje nowych posiadaczy kart.
Dodaj	Zachowuje istniejących posiadaczy kart i dodaje 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. Wybierz **New (Nowy)**, **Update (Aktualizuj)** lub **Add (Dodaj)**.
4. Kliknij **Next (Dalej)**.
5. Kliknij **Choose a file (Wybierz plik)**, zlokalizuj plik CSV, a następnie kliknij **Open (Otwórz)**.
6. Wprowadź separator kolumn, wybierz niepowtarzalny 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. Użyj tej opcji, aby zapobiec importowaniu zduplikowanych rekordów personelu.
Format numeru karty	Domyślnie włączona jest opcja Allow both hexadecimal and number (Zezwalaj na liczbę szesnastkową i dziesiętną) .

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 Pro 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.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Undo import (Cofnij import)**.
3. Kliknij **Tak**.

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 wpisz 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). Zob. *Profile identyfikacji, on page 167*.

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)**.

Szablony identyfikatorów ^{BETA}

Można dostosować szablony identyfikatorów, dodając informacje o posiadaczu karty, zdjęcia, logotypy i własne oznaczenia firmowe. Aby utworzyć nowy szablon:

1. Przejdź do **Access management > Settings > Badge templates ^{BETA} (Zarządzanie dostępem > Ustawienia > Szablony identyfikatorów)**.
2. Kliknij **Create new template (Utwórz nowy szablon)**.
3. Wprowadź nazwę w polu **Template name (Nazwa szablonu)**.
4. Aby ustawić ten szablon jako domyślny, wybierz **Use as default template for printing (Użyj jako domyślny szablon do drukowania)**.
5. Dostosuj wygląd identyfikatora:
 - Wybierz maks. pięć pól tekstowych, które mają być prezentowane na przedniej stronie, w tym wszelkie utworzone pola niestandardowe. Podczas drukowania na identyfikatorze znajdują się tylko wypełnione pola.
 - Wybierz czcionkę i kolor tekstu.
 - Dodaj kolor tła lub obraz.
 - Załącz logotyp swojej organizacji.
 - Na stronie tylnej dodaj kolor tła lub obraz.
6. Kliknij **Save (Zapisz)**, aby zapisać zmiany lub **Save as (Zapisz jako)**, aby utworzyć nowy szablon.

Uwaga

Utworzonego szablonu nie można edytować, można jedynie zmienić jego nazwę.

Drukowanie identyfikatorów ^{BETA}

Można drukować identyfikatory dla posiadaczy kart, korzystając ze skonfigurowanych szablonów identyfikatorów. Kodowanie kart nie jest obecnie obsługiwane. Zanim rozpoczniesz:

- Sprawdź, czy posiadacz karty ma co najmniej jedno uwierzytelnienie za pomocą karty. Nie można drukować identyfikatorów dla posiadaczy kart bez uwierzytelnień.
- Potrzebna jest drukarka obsługująca karty o rozmiarze CR80 i odpowiednie materiały do drukowania w rodzaju grubego kartonu.
- Skonfiguruj ustawienia drukowania w przeglądarce:
 1. Ustaw rozmiar strony na CR80 lub rozmiar niestandardowy odpowiadający wymiarom karty do wydrukowania.
 2. Ustaw orientację pionową.
 3. Wyłącz marginesy lub ustaw je na minimum.

Ważne

Aplikacja Secure Entry współpracuje z drukarkami działającymi w oparciu o sterowniki dla systemu Windows. Drukarki serii HID Fargo zostały sprawdzone pod kątem prawidłowości działania. Jeśli potrzebujesz sterownika do drukarki, skontaktuj się z jej dostawcą.

Aby wydrukować identyfikatory:

1. Przejdź do **Access management > Cardholder management > Cardholders** (Zarządzanie dostępem > Zarządzanie posiadaczami kart > Posiadacze kart).
2. Wybierz jednego lub kilku posiadaczy kart.
3. Kliknij **Print badge** ^{BETA} (Wydrukuj identyfikator).
4. Kliknij **Select template** (Wybierz szablon) i z menu rozwijalnego **Template** (Szablon) wybierz szablon identyfikatora, którego chcesz użyć.
5. Jeżeli posiadacz karty ma kilka uwierzytelnień za pomocą karty, wybierz jedno z menu rozwijalnego **Card** (Karta).
6. Kliknij przycisk **Drukuj**.

Uwaga

W przypadku drukarki nieobsługującej druku dwustronnego najpierw wydrukuj wszystkie przednie strony, a następnie odwróć plik kart i włóż je ponownie do podajnika, by wydrukować tylne strony.

Monitorowanie stanu systemu ^{BETA}

Za pomocą karty System Health Monitoring (Monitorowanie stanu systemu) monitoruj dane dotyczące stanu jednego lub kilku systemów AXIS Camera Station Pro w tej samej sieci.

Jeśli zarządzasz systemami w różnych sieciach, monitorowanie serwera w My Systems zapewnia tę samą funkcjonalność, ale za pośrednictwem chmury.

	Pokazuje podsumowanie urządzeń i systemów, do których masz dostęp. Zob. <i>Magazyn</i> , on page 197.
	Pokazuje podsumowanie informacji o pamięci masowej i szczegółów nagrywania dla wszystkich kamer z monitorowanych komputerów. Zob. <i>Pamięć masowa</i> , on page 198.
	Pokazuje dzienniki funkcji Monitorowanie stanu systemu z monitorowanych systemów. Zob. <i>Powiadomienia</i> , on page 199.

Ograniczenia

- W rejestratorach serii AXIS S30 i S40 Recorder nie ma możliwości monitorowania pamięci masowej na nagrania.
- Ustawienia powiadomień dotyczą tylko lokalnego serwera funkcji Monitorowanie stanu systemu.
- System oznacza nagrania, których rodzajem jest **None** (Brak), z wyjątkiem nagrań ciągłych i nagrań wyzwalanych detekcją ruchu.

Proces

1. *Konfigurowanie funkcji Monitorowanie stanu systemu ^{BETA}*, on page 178
 - 1.1. Skonfiguruj powiadomienia. Zob. *Powiadomienia*, on page 178.
 - 1.2. Skonfiguruj system wielokomputerowy. Zob. *Multisystem*, on page 179.
2. Monitoruj dane o kondycji z systemów AXIS Camera Station Pro.
 - 2.1. *Magazyn*, on page 197
 - 2.2. *Pamięć masowa*, on page 198
 - 2.3. *Powiadomienia*, on page 199

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 szczegóły systemu i serwera.
3. Aby wyświetlić podsumowanie informacji o urządzeniu w systemie, kliknij urządzenie na liście. W prawym panelu wyświetlane są informacje o urządzeniu i pamięci masowej, o ile urządzenie zawiera źródło wizyjne.
4. Aby pobrać raport systemowy, wybierz **AXIS Camera Station system report (Raport systemowy AXIS Camera Station)** z rozwijalnego menu **Create report (Utwórz raport)**. Zob. *Raport systemowy*, on page 211.
5. Aby pobrać raport funkcji Monitorowanie stanu systemu:

- 5.1. Z menu rozwijalnego **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.

Pamięć masowa

Strona Pamięć masowa zawiera podsumowanie informacji o pamięci masowej oraz szczegóły nagrywania na każdej kamerze należącej do monitorowanego systemu. Kliknij nagłówek kolumny, aby posortować dane według tej kolumny.

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. Zob. <i>Konfigurowanie pamięci masowej, on page 76</i> .
Lokalizacja	Ścieżka i nazwa pamięci masowej.
Łącznie	Łączna wielkość pamięci masowej. Odpowiada wartości Total size (Rozmiar na dysku) wyświetlanej we właściwościach systemu Windows dla danej lokalizacji pamięci masowej.
Przydzielone	Maksymalna ilość zasobu przeznaczona na nagrania.
Wykorzystane	Rozmiar pamięci masowej obecnie wykorzystywany na nagrania.
Data ostatniej aktualizacji	Data i godzina ostatniego zaktualizowania informacji.

Kamera	
Status	(puste): Stan normalny. Ikona ostrzeżenia: Kryterium czasu przechowywania nie zostało spełnione. 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 obszarze Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór).
Bieżące przechowywanie	Liczba dni, przez które nagrania były przechowywane w pamięci masowej.
Najstarsze nagranie	Godzina wykonania najstarszego nagrania z kamery w pamięci masowej.
Najnowsze nagranie	Godzina wykonania najnowszego nagrania z kamery w pamięci masowej.
Lokalizacja	Lokalizacja pamięci masowej wykorzystywana przez kamerę.
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. Kliknij nagłówek kolumny, aby posortować dane według tej kolumny.

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 <code>device down</code> (Urządzenie niedziałające) lub <code>system</code> w przypadku powiadomień wyzwalanych regułą <code>system down</code> (System niedziałający).
System	Nazwa systemu, w którym wystąpiło zdarzenie.
Reguła	Reguła, która wyzwoliła powiadomienie: <code>System down</code> (System niedziałający) lub <code>Device down</code> (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 Pro.

- 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
- Położenia zaprogramowane PTZ
- Nagrania
- Sekwencje
- Widok dzielony
- Karta
- Inne

W kategoriach Navigate to cameras (Przejdź do kamer) i Navigate to views (Przejdź do widoków) działania te musisz przypisać 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 działania powodującego konflikt. Naciśnij klawisz ESC, aby anulować. Naciśnij klawisz ENTER, aby użyć klawisza skrótu i usunąć jego powiązanie z innym działaniem.
- 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 działania jest pusta, kliknij puste pole i dodaj żądany klawisz skrótu do tego działania. - Aby dodać klawisz skrótu za pomocą klawiatury, naciśnij klawisz Ctrl i co najmniej jeden inny klawisz lub klawisz funkcyjny F2 – F12. - Aby dodać klawisz skrótu używający elementu klawiatury numerycznej, naciśnij żadaną kombinację klawiszy numerycznych lub jeden z klawiszy funkcyjnych F1–F5. - Aby dodać klawisz skrótu używający joysticka lub pokrętła, naciśnij przycisk joysticka lub pokrętła, który ma zostać przypisany.
Edycja klawisza skrótu	Kliknij wartość klawiatury danego działania, aby je edytować.
Usuwanie klawisza skrótu	Kliknij wartość klawiatury danego działania, aby je usunąć.
	Kliknij, aby wydrukować tabelę klawiszy skrótów klawiaturowych.
	Kliknij, aby przywrócić domyślne wartości wszystkich klawiszy skrótu.

Klawisze panelu sterowania dozoru 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 **Logs** (Dzienniki) są wyświetlane alarmy na żywo, zdarzenia i dzienniki kontroli. Można również wyszukiwać poprzednie dzienniki. W obszarze **Configuration > Server > Settings** (Konfiguracja > Serwer > Ustawienia) można określić liczbę dni przechowywania dzienników.

Godzina	Data i godzina działania.
Type (Typ):	Rodzaj działania: alarm, zdarzenie lub kontrola.
Kategoria	Kategoria akcji.
Wiadomość	Krótki opis akcji.
Użytkownik	Użytkownik AXIS Camera Station Pro wykonujący działanie.
Komputer	Komputer (nazwa domeny systemu Windows), na którym zainstalowano AXIS Camera Station Pro. Wartość ta jest podawana przez klienta i nie może zostać niezależnie zweryfikowana przez serwer.
Użytkownik systemu Windows	Użytkownik systemu Windows z rolą administratora AXIS Camera Station Pro. Wartość ta jest podawana przez klienta i nie może zostać niezależnie zweryfikowana przez serwer. W kolumnie User (Użytkownik) wyświetlany jest uwierzytelniony użytkownik.
Serwer	Widoczna tylko w przypadku połączenia z wieloma serwerami. 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 Pro przeszukuje listę dzienników oprócz **Time** (Godzina) i pokazuje wyniki zawierające wszystkie słowa kluczowe. Obsługiwane operatory wyszukiwania są opisane w temacie *Optymalizowanie wyszukiwania, on page 45*.
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 **Alarms** (Alarmy) są wyświetlane alarmy systemowe oraz alarmy wygenerowane przez reguły i funkcję detekcji ruchu. Na liście są też takie informacje, jak data i godzina wystąpienia alarmu, kategoria alarmu i komunikat alarmu. Zob. *Alarmy*.

	Kliknij alarm i  , aby otworzyć kartę Recordings (Nagrania) i rozpocząć odtwarzanie, jeżeli 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 potwierdzeniu alarmów.
	Kliknij alarm i  , aby wyeksportować dziennik do pliku tekstowego.

Dziennik zdarzeń

W dzienniku **Events** (Zdarzenia) na liście są wyświetlane zdarzenia dotyczące kamer i serwera, na przykład nagrań, 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 kontroli

W dzienniku **Audit** (Kontrola) są widoczne wszystkie działania podjęte przez użytkownika, takie jak zapis uruchamiany ręcznie, rozpoczęcie lub zatrzymanie strumieniowania wizyjnego, uaktywnianie reguł działań, utworzenie drzwi i utworzenie posiadacza karty. Zaznacz dzienniki kontroli i na pasku narzędzi kliknij  , aby wyeksportować je w postaci pliku tekstowego.

Zarządzanie tablicami rejestracyjnymi

Aby zarządzać listami tablic rejestracyjnych w oprogramowaniu AXIS Camera Station Pro, otwórz kartę **License plate management (Zarządzanie tablicami rejestracyjnymi)**.

Na tej karcie można edytować trzy listy tablic rejestracyjnych dla poszczególnych kamer lub grup kamer:

1. Wybierz grupę lub kamerę z listy **Groups (Grupy)** i **Cameras (Kamery)**.
2. Wybierz listę, którą chcesz edytować. Domyślnie trzy listy, które można edytować, noszą nazwy: **Allow list (Lista dozwolonych)**, **Block list (Lista blokowanych)** i **Custom list (Lista niestandardowa)**.
3. Wprowadź zmiany na liście:
 - Aby edytować nazwę listy, kliknij **Edit list name (Edytuj nazwę listy)**.
 - Aby dodać nowy numer tablicy rejestracyjnej, wpisz go w kolumnie **License plate (Numer tablicy rejestracyjnej)** i opcjonalnie dodaj opis w kolumnie **Description (Opis)**. Kliknij **Dodaj**.
 - Aby edytować lub usunąć istniejący numer tablicy rejestracyjnej, zaznacz go i kliknij **Edit (Edytuj)** lub **Remove (Usuń)**.
 - Aby zaimportować listę numerów tablic rejestracyjnych z pliku CSV, kliknij **Import (Importuj)** i wybierz plik. Spowoduje to nadpisanie obecnej listy, więc jeżeli chcesz zachować jej kopię, najpierw wyeksportuj listę.
 - Aby wyeksportować listę numerów tablic rejestracyjnych do pliku CSV, kliknij **Export (Eksportuj)**.
4. Kliknij **Apply (Zastosuj)**, aby zapisać zmiany.

Uwaga

Po zastosowaniu zmian program AXIS Camera Station Pro przejmuje zarządzanie listami numerów tablic rejestracyjnych dla danej grupy lub kamery. Każdej nocy aktualizujemy ustawienia kamery zgodnie z listami zapisanymi w programie AXIS Camera Station Pro, co powoduje nadpisanie wszelkich numerów tablic rejestracyjnych zapisanych bezpośrednio w kamerze.

AXIS Audio Manager Pro

Użyj karty **AXIS Audio Manager Pro**, aby uzyskać bezpośredni dostęp do interfejsu serwera AXIS Audio Manager Pro z programu AXIS Camera Station Pro. Więcej informacji na temat interfejsu serwera znajduje się w instrukcji obsługi programu *AXIS Audio Manager Pro*.

Karta ta pojawia się dopiero po nawiązaniu połączenia z serwerem AXIS Audio Manager Pro w programie AXIS Camera Station Pro. Więcej informacji znajduje się w sekcji *Konfiguracja programu AXIS Audio Manager Pro*, on page 175.

Ważne

Nie można uzyskać dostępu do interfejsu serwera AXIS Audio Manager Pro za pomocą Secure Remote Access v2.

Integracja umożliwia również:

- *Tworzenie wyzwalaczy aplikacji AXIS Audio Manager, on page 105.*
- *Tworzenie działań aplikacji AXIS Audio Manager, on page 115.*
- *Dodaj strefy nagłośnieniowe do map. Patrz Mapa, on page 23.*
- *Korzystanie z interfejsów przywołań w widokach dzielonych, on page 21.*
- *Ustaw uprawnienia użytkownika związane z programem AXIS Audio Manager Pro w programie AXIS Camera Station Pro. P. sekcja Uprawnienia użytkownika/grupy, on page 140.*
- *Wybierz urządzenia audio z serwera AXIS Audio Manager Pro jako urządzenia audio powiązane z kamerą. P. sekcja Edytowanie profili strumienia, on page 55.*

Alarms

Na karcie Alarms (Alarmsy), dostępnej w dolnej części okna klienta AXIS Camera Station Pro, wyświetlane są wyzwalane zdarzenia oraz alarmy systemowe. Informacje na temat tworzenia alarmów: *Reguły akcji*. Więcej informacji o alarmie „Database maintenance is required” (Wymagana jest konserwacja bazy danych) można znaleźć w temacie *Konserwacja bazy danych, on page 229*.

Godzina	Godzina wystąpienia alarmu.
Kategoria	Kategoria zainicjowanego alarmu.
Opis	Krótki opis alarmu.
Serwer	Opcja dostępna w przypadku połączenia z wieloma serwerami. Serwer AXIS Camera Station Pro, który wysłał alarm.
Element	Element, który wyzwał alarm.
	Pokazuje procedurę postępowania w razie wystąpienia alarmu. Opcja widoczna tylko, jeżeli alarm zawiera procedurę alarmową.
	Przejdź do nagrań. Opcja widoczna tylko, jeżeli alarm zawiera nagranie.
	Potwierdź wybrany alarm
	Usuń alarm. Alarm zostanie usunięty tylko tymczasowo, o ile najpierw go nie potwierdzisz.

Aby zareagować na konkretny alarm:

1. Kliknij  Alarms and Tasks (Alarmy i zadania) w dolnej części okna klienta AXIS Camera Station Pro 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 potwierdzeniu 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 Pro.

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
- Eksportowanie nagrań

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.
- Anuluj lub spróbuj ponownie wykonać rozpoczęte zadania. 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.
Rozpocznij	Godzina rozpoczęcia zadania.
Wiadomość	Wyświetla status lub informacje o zadaniu. Możliwe statusy: • Canceling (Anulowanie): Czyszczenie przed anulowaniem zadania. • Canceled (Anulowano): Czyszczenie zostało ukończone, a zadanie anulowane. • Error (Błąd): Zadanie nie zostało wykonane na co najmniej jednym urządzeniu. • Finished (Ukończono): Zadanie ukończone. • Finished during lost connection (Ukończono przy utraconym połączeniu): Zadanie zostało ukończone w czasie braku połączenia z serwerem. Nie można ustalić statusu zadania. • Lost connection (Utracono połączenie): Podczas wykonywania zadania komputer kliencki utracił połączenie z serwerem. Nie można ustalić statusu zadania. • Running (Wykonywanie): Zadanie jest w trakcie realizacji. • 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 Pro, 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 Pro i kliknij kartę **Tasks (Zadania)**.

2. Wybierz zadania i kliknij jedno z działań

	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. Przejrzyj i skonfiguruj ręcznie wszystkie operacje zakończone niepowodzeniem.

W przypadku większości zadań są wyświetlane informacje wymienione poniżej. W przypadku zadań takich jak eksportowanie nagrań (**Export recordings**) czy raport systemowy (**System report**) dwukrotne kliknięcie zadania 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: • Finished (Ukończono): Zadanie ukończone. • Error (Błąd): Nie można było ukończyć zadania w urządzeniu. • Canceled (Anulowano): 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 przegląd konfiguracji systemu klienta w standardzie HTML:

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 działań, harmonogramach, pamięci masowej nagrań, urządzeniach dodatkowych i licencjach. Przydaje się przy rozwiązywaniu problemów oraz kontaktowaniu z działem wsparcia technicznego.

Aby wyświetlić przegląd konfiguracji systemu serwera w standardzie HTML:

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  > **Help > System report**. (Pomoc > Raport systemowy).
2. Jeżeli chcesz zmienić automatycznie wygenerowaną nazwę pliku, wyedytuj ją.
3. Kliknij przycisk **Browse** (Przeglądaj) i wskaż miejsce, gdzie chcesz zapisać raport systemowy.
4. Wybierz preferowane ustawienia:
 - **Automatically open folder when report is ready** (Automatyczne otwieranie folderu, gdy raport jest gotowy), aby otworzyć go 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 ze wszystkich monitorów), aby ułatwić analizę raportu systemowego.
5. Kliknij **OK**.



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

Generowanie raportu systemowego

Uwaga

- Jeżeli serwer się nie uruchomi, możesz pobrać uproszczony raport systemowy z karty **Tools** (Narzędzia) w aplikacji **AXIS Camera Station Service Control**.
- Jeżeli klient nie może zalogować się na serwer, dział obsługi klienta Axis może poprosić o udostępnienie dzienników klienta. Znajdziesz je w folderze właściwym dla danej wersji klienta: `C:\ProgramData\Axis Communications\AXIS Camera Station\Core\Client 6.xx`.
- W zależności od problemu może być również konieczne zebranie dzienników zdarzeń systemu Windows. W tym celu otwórz przeglądarkę zdarzeń, przejdź do **Windows Logs** (Dzienniki systemu Windows), a następnie kliknij prawym przyciskiem myszy **Application** (Aplikacja) i wybierz **Save all events as** (Zapisz wszystkie zdarzenia jako). Te same czynności wykonaj dla **Systemu**.

W takich przypadkach dział obsługi klienta Axis będzie również potrzebował standardowych dzienników serwera na potrzeby przeprowadzenia analizy.

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)	Testowanie strumieniowania i zapisu danych przy użyciu bieżących ustawień systemu w programie AXIS Camera Station Pro . Rezultaty wyświetlane są jako „zaliczone” lub „niezaliczone”.
Złe oświetlenie	Testowanie strumieniowania i zapisu danych z wykorzystaniem ustawień zoptymalizowanych pod kątem typowych warunków złego oświetlenia. Rezultaty wyświetlane są jako „zaliczone” lub „niezaliczone”.
Test obciążenia	Testy, w których strumieniowanie danych i wykorzystanie pamięci masowej są stopniowo zwiększane aż do osiągnięcia przez system maksymalnego ograniczenia. Rezultaty przedstawiają maksymalne możliwości 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 Pro** 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 otworzyć raport, lub przycisk **Save report (Zapisz raport)**, aby go zapisać.

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 obszarze **Latest export (Ostatni eksport)** zostanie wyświetlone lub uaktualnione łącze do pliku.
5. Kliknięcie łącza spowoduje przejście do lokalizacji pliku.

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)**.

Aplikacja AXIS Camera Station Pro Service Control

Serwer używa aplikacji AXIS Camera Station Pro Service Control do uruchamiania się, wyłączania oraz zmieniania 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 i wybierz **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 aplikację Service Control z menu Start:

Przejdź do menu **Start** i wybierz kolejno **All Programs > Tools > Service Control** (Wszystkie programy > Narzędzia > Kontrola usług).

	Uruchomiona
	Rozpoczynanie
	Zatrzymane

Modify Settings (Zmień ustawienia)	Wybierz, aby zmienić ustawienia serwera.
Restore Default Settings (Przywróć ustawienia domyślne)	Kliknij tę opcję, aby przywrócić wszystkie ustawienia domyślne.
Rozpocznij	Kliknij tę opcję, aby zmienić stan serwera.
Zatrzymaj	
Rozpocznij ponownie	Kliknij tę opcję, aby zrestartować serwer.

Ogólne ustawienia serwera

W aplikacji AXIS Camera Station Pro Service Control kliknij **Modify settings (Modyfikuj ustawienia)**, a następnie **General (Ogólne)**, aby zmienić ogólne ustawienia serwera.

Nazwa serwera	Nazwa serwera. Nazwa serwera pojawia się w oprogramowaniu klienckim. Domyślnie nazwą serwera jest nazwa komputera. Nazwa ta nie ulegnie zmianie w przypadku zmiany nazwy komputera.
Web client port (Port klienta sieci Web)	Jest to portu używany przez klient sieci Web programu AXIS Camera Station.
Ports range (Zakres portów)	Określ zakres portów. Pozostałe porty zmieniają się automatycznie.
Allow AXIS Camera Station Pro to add exceptions to the Windows Firewall (Zezwalaj aplikacji na dodawanie wyjątków do Zapory systemu Windows)	Wybierz, aby zezwolić programowi AXIS Camera Station Pro na automatyczne dodawanie wyjątków do Zapory systemu Windows, jeżeli użytkownik zmieni zakres portów.

Uwaga

- Jeżeli między serwerem a klientem istnieje brama NAT, zaporą sieciową lub podobne rozwiązanie, skonfiguruj przepuszczanie ruchu wykorzystującego te porty.
- Numery portów muszą być w zakresie 1024–65534.

Lista portów dotycząca AXIS Camera Station Pro

W poniższych tabelach opisano, z jakich portów i protokołów korzysta aplikacja AXIS Camera Station Pro. Może być konieczne zezwolenie na nie w zaporze w celu uzyskania optymalnej wydajności i użyteczności. Numery portów są obliczane na podstawie głównego portu HTTP 29200. W niektórych sekcjach wymieniono zarówno porty wymagane, jak i opcjonalne. Aby program AXIS Camera Station Pro działał poprawnie, wymagane porty muszą być zawsze otwarte. Jeżeli opcjonalne porty nie są dozwolone, powiązane funkcje nie będą działać.

Serwer do urządzeń

Wymagane				
Port	Liczba	Protokół	Kierunek	Opis
Główny port HTTP i HTTPS	443	HTTPS	Wychodzący	Używany do uaktywniania licencji, pobierania oprogramowania układowego i do połączonych usług.

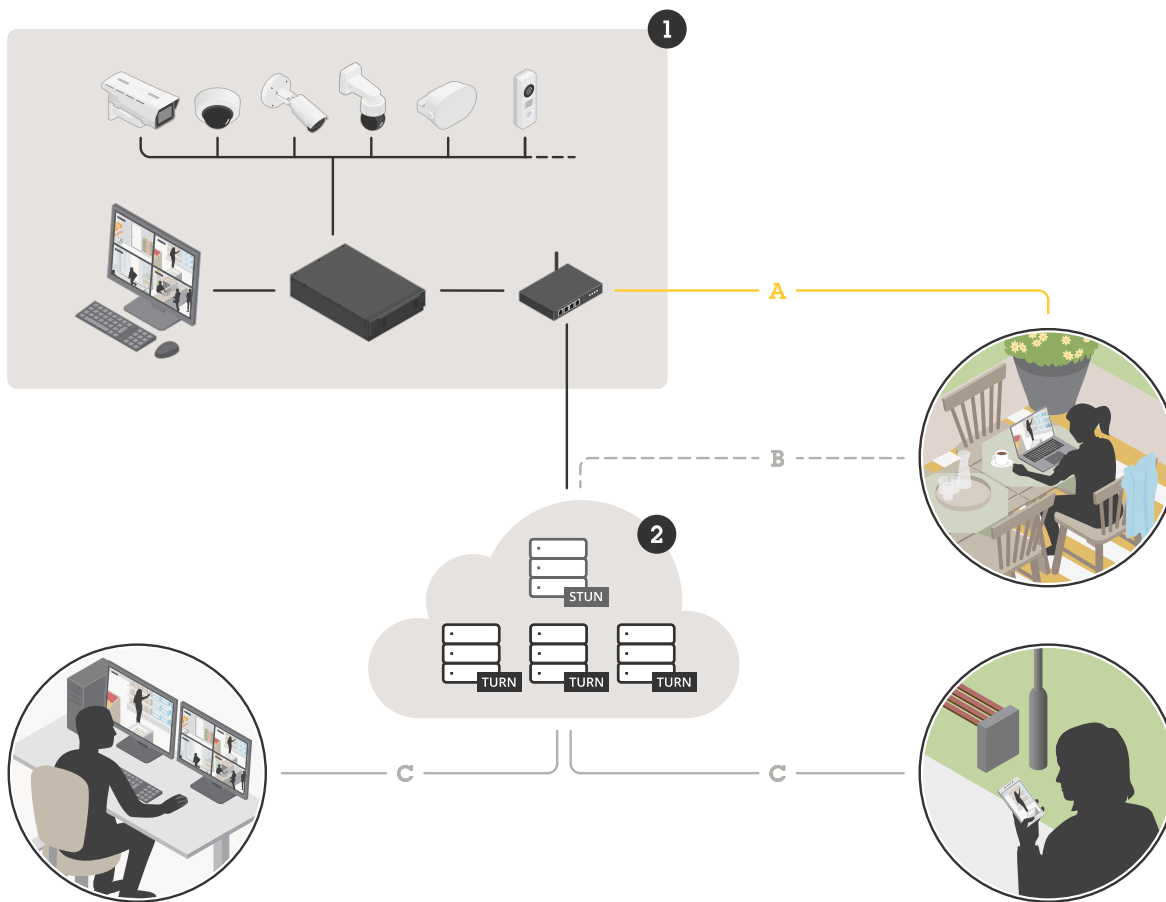
Opcjonalnie				
Domyślny port protokołu WS-Discovery	3702	UDP	Przychodzące i wychodzące	Usługi internetowe z użyciem protokołu WS-Discovery służące do wykrywania urządzeń ONVIF. Multiemisja na adresie 239.255.255.250.
Domyślny port protokołu Bonjour	5353	UDP	Przychodzące i wychodzące	Służy do wykrywania urządzeń za pomocą protokołu mDNS (Bonjour). Multiemisja na adresie 224.0.0.251. Jeżeli domyślny port jest niedostępny, być może korzysta z niego inna aplikacja i nie udostępnia go. W takiej sytuacji stosowany będzie zamiennie losowy port. Urządzenia z adresami lokalnymi nie są wykrywalne przez protokół Bonjour w przypadku stosowania losowego portu.

Klient do serwera

Wymagane są wszystkie porty					
Port	Liczba	Protokół	Kierunek	Komunikacja między	Opis
Główny port HTTP i port strumieniowania HTTP	29200	HTTP	Przychodzący	Serwer i klient ACS	Używany do strumieniowania obrazu, dźwięku i metadanych (szyfrowanie AES).
Główny port TCP	29202	TCP	Przychodzący	Serwer i klient ACS	Od wersji 6.17 służy wyłącznie do przełączania klientów. Wcześniej był to główny port TCP.

Port serwera internetowego interfejsu API ACS	29204	HTTPS	Przychodzący	Serwer ACS i aplikacja mobilna	Służy do przesyłania danych aplikacji oraz strumieniowania obrazu w standardzie MP4 poprzez protokół HTTPS.
Lokalny port HTTP serwera proxy	29206	TCP	Przychodzący	Wewnętrznie w serwerze ACS	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.
Port punktu końcowego internetowego serwera proxy	29207	TCP	Przychodzący	Serwer ACS i jego komponenty	Używany do bezpiecznej komunikacji między składnikami a urządzeniami.

Domeny i porty dotyczące funkcji Secure Remote Access v2



Rysunek: Przegląd funkcji rozwiązania Axis Secure Remote Access v2 w programie AXIS Camera Station Pro

1. Monitorowany obiekt w sieci lokalnej z lokalnym klientem podglądu

- A – Połączenie zdalne (peer-to-peer)
- B – Połączenie tymczasowe STUN / TURN z usługami Axis Cloud Connected Services

Nazwa lub rodzaj	Adres	Numer portu	Protokół	Kierunek
SRA v2 – logowanie do My Axis	eu.login.connect.axis.com	443	TCP	Przychodzące i wychodzące
SRA v2 – komunikacja Cloud Service	eu.cs.connect.axis.com	443	TCP	Przychodzące i wychodzące
SRA v2 – komunikacja API Cloud Service	api.vms.axis.cloud	443	TCP	Przychodzące i wychodzące
Komponent łączy w górę	acspro.mysystems.axis.com	443	-	Przychodzące i wychodzące
Komponent EdgeHost	75.2.119.140	443, 8443	-	Przychodzące i wychodzące
Komponent EdgeHost	99.83.133.42	443, 8443	-	Przychodzące i wychodzące
Komponent EdgeHost	cep.connect.axis.com	443, 8443	-	Przychodzące i wychodzące

2. Usługi Axis Cloud Connected Services

- C – Zdalne połączenie TURN z usługami Axis Cloud Connected Services

Nazwa lub rodzaj	Adres	Numer portu	Protokół	Kierunek
Komunikacja między serwerem proxy P2P a komponentem WebRTC	wss://signaling.prod.webrtc.connect.axis.com	443	TCP	Przychodzące i wychodzące
Komunikacja między serwerem proxy P2P a komponentem WebRTC	https://*.turn.prod.webrtc.connect.axis.com	443, 3478, 5349, 49152-65535	TCP	Przychodzące i wychodzące

Zarezerwowane dla składników

Wymagane						
Element	Nasłuchuje na interfejsie	Liczba	Protokół	Kierunek	Komunikacja między	Opis
Lokalny serwer sygnalizacji WebRTC	host lokalny	29227	WSS	Przychodzący	Klient z opcją osadzenia, WebClient i WebRTC Streamer do serwera sygnalizacyjnego	Część komponentu WebRTC w środowisku lokalnym.
Lokalna konfiguracja WebRTC	host lokalny	29229	HTTPS	Przychodzący	Klient ACS (strona internetowa)	Służy do hostowania konfiguracji WebRTC, strony internetowej i backendu. Część komponentu WebRTC w środowisku lokalnym.
Serwer lokalny TURN	Wszystkie (0.0.0.0/INADDR_ANY)	29230	UDP	Przychodzące i wychodzące	Klient z opcją osadzenia / WebClient to serwera TURN	Używany do „pojedynczego portu WebRTC” w lokalnym systemie ACS.
Local-IAM (IDP)	0.0.0.0	29232	HTTPS	Przychodzący	Reverse proxy i lokalne zarządzanie dostępem i tożsamościami Local-	Publiczny port IDP_OIDC.

					IAM, klient ACS Windows i lokalne zarządzanie dostępem i tożsamościami Local-IAM	
Local-IAM (IDP)	0.0.0.0	29233	HTTPS	Przychodzący	Usługi innych firm	Port administratora mTLS.
Local-IAM (IDP)	127.0.0.1	29234	HTTPS	Przychodzący	Usługi innych firm	Port tokenizera.
WebRTC	host lokalny	29235	HTTPS	Przychodzący	Składnik chmurowy	Służy przy włączeniu do sieci IP celem skonfigurowania połączenia z chmurą WebRTC. Część składnika WebRTC.
Interfejs API usługi	127.0.0.1	29244	NATS	Przychodzący	Pomiędzy ACS a komponentami i pomiędzy samymi komponentami przez NATS.	Broker NATS.

Opcjonalnie

Secure Entry (AC-MSM)	127.0.0.1	29214	HTTPS (WS)	Przychodzący	Klient ACS (strona internetowa) i komponent	Z możliwością konfigurowania za pomocą podstawowego portu ACS. Starsze instalacje korzystały z portu 8081.
Secure Entry (AC-MSM)	Wszystkie (0.0.0.0/INADDR_ANY)	29215	HTTPS (WS)	Przychodzący	Komponenty Secure Entry w różnych lokalizacjach	Z możliwością konfigurowania za pomocą podstawowego portu ACS.

Monitorowanie stanu systemu	Wszystkie (0.0.0.0/INADDR_ANY)	29216	HTTPS	Przychodzący	ACS (strona internetowa), SHM backend (komponent)	Używany do hostowania strony internetowej funkcji Monitorowanie stanu systemu oraz do udostępniania danych w konfiguracji wielosystemowej.
Usługa chmurowa Monitorowania stanu systemu / Usługa chmurowa	host lokalny	29217	HTTPS	Przychodzący	ACS (strona internetowa) i backend usługi chmurowej (komponent)	Wykorzystywane w usługach chmurowych.
Inteligentne wyszukiwanie 2	host lokalny	29218	HTTPS	Przychodzący	Klient ACS (karta na stronie internetowej Inteligentne wyszukiwanie) oraz backend Inteligentnego wyszukiwania (komponent)	Używany do hostowania interfejsu API Inteligentnego wyszukiwania oraz do obsługi strony internetowej klienta.
Interfejs API VMS	127.0.0.1, ::1	29219	GraphQL	Przychodzący	Klienty API VMS i GraphQL	Służy do udostępniania systemu ACS jako interfejsu programowania aplikacji (API) GraphQL klientowi.
Klient internetowy	host lokalny	29223	HTTPS	Przychodzący	WebClient to VMS API/Embeddable Client	Backend działa jako serwer proxy przed konfigurowalnym interfejsem API VMS.
Klient z opcją osadzenia	host lokalny	29224	HTTPS	Przychodzący	Klient z opcją osadzenia w interfejsie API VMS,	Backend działa jako serwer proxy przed

					WebRTC Streamer oraz serwerze sygnalizacyjnym	interfejsem API VMS.
Konfiguracja klienta internetowego	host lokalny	29225	HTTPS	Przychodzący	Klient ACS (strona internetowa)	Służy do hostowania strony internetowej i backendu konfiguracji klienta internetowego.
Konfiguracja klienta z opcją osadzenia	host lokalny	29226	HTTPS	Przychodzący	Klient ACS (strona internetowa)	Służy do hostowania strony internetowej i backendu konfiguracji klienta internetowego z opcją osadzenia.
Opentelemetry	127.0.0.1	29236	gRPC	Przychodzący	Usługi innych firm (ACS i inne komponenty)	Port gRPC.
Opentelemetry	127.0.0.1	29237	HTTPS	Przychodzący	Usługi innych firm (ACS i inne komponenty)	Port HTTP.
Audio Manager		29238	HTTPS	Przychodzący	Usługi i komponenty integracyjne innych firm	Port serwera www.
Data Insights Dashboard	host lokalny	29241	HTTPS	Przychodzący		Port serwera internetowego odbiornika.
Data Insights Dashboard	0.0.0.0	29242	MQTT	Przychodzące i wychodzące	Odbiornik komunikatów o zdarzeniach kamer	Broker Mosquitto.
Opentelemetry	127.0.0.1	29245	HTTP	Przychodzący	Monitorowanie punktu końcowego w celu pobrania metryk z otwartego modułu OpenTelemetry collector	Port HTTP.

Inteligentne wyszukiwanie 2	host lokalny	29247	gRPC	Przychodzący	VMS API core i Smart Search resolver	Smart Search Resolver.
Brama interfejsu programowania aplikacji (API)	0.0.0.0	29248	HTTPS	Przychodzący	Host brzegowy i brama interfejsu API	Port awaryjny bramy interfejsu API używany przez host brzegowy.
Brama interfejsu programowania aplikacji (API)	0.0.0.0	29250	HTTPS	Przychodzący	Klienty ACS i brama interfejsu API	Port awaryjny dla ruchu HTTP i HTTPS na portach 80 i 443. Różni się od +48, jako że +48 wykorzystuje certyfikaty komponentów, ten zaś certyfikaty serwerowe.
Monitorowanie stanu systemu	127.0.0.1	29251	gRPC	Przychodzący	Serwer ACS i ewentualnie inne komponenty połączone z kolektorem SHM	Użytkowany przez aplikacje wytwarzające dane o stanie systemu do przesyłania danych do kolektora SHM.
Monitorowanie stanu systemu	127.0.0.1	29252	HTTPS	Przychodzący	Serwer ACS i ewentualnie inne komponenty połączone z kolektorem SHM	Użytkowany przez aplikacje wytwarzające dane o stanie systemu do przesyłania danych do kolektora SHM.
Odbiornik AXIS Body Worn Live Receiver	127.0.0.1	29254	TCP	Przychodzący	Serwer strumieniowania na żywo obsługujący żądania HTTPS z serwera ACS	Serwer strumieniowania na żywo.

Inne porty
Wymagane

Port	Liczba	Protokół	Kierunek	Komunikacja między	Opis
Port HTTP	80	HTTP	Wychodzący	Serwer ACS i urządzenia oraz klient ACS i serwer ACS z dostępem do internetu	Służy do uaktywnienia licencji, pobierania oprogramowania układowego oraz korzystania z połączonych usług.
Port HTTP	80	HTTP	Przychodzący	Klient ACS i serwer ACS	Używany do strumieni wideo i danych urządzeń.
HTTPS port (Port HTTPS):	443	TCP	Przychodzący	Klienty ACS i serwer ACS	Używany do strumieni wideo i danych urządzeń.
Port UDP stanu aktualizacji	15156	UDP	Przychodzące i wychodzące	Serwer ACS i sterowanie usługą ACS	Sterowanie usługą ACS nasłuchuje na porcie, a serwer ACS rozgłasza status trwającej aktualizacji.
PostgreSQL	29210	TCP	Przychodzące i wychodzące	PostgreSQL i dowolny konsument	Do bieżących konsumentów należą: Data Insights Dashboard, komponent AXIS Audio Manager Pro oraz komponent AXIS Body Worn.

Opcjonalnie

Usługi pokładowe	29253	UDP	Przychodzący	Odbiornik GNSS jako komponent usług pokładowych	
Port HTTP	80	HTTP	Wychodzący	Serwer ACS i urządzenia, klient ACS oraz serwer ACS z dostępem do internetu	Używany do aktywowania licencji, pobierania oprogramowania sprzętowego, połączonych usług itd.
Port HTTP	80	HTTP	Przychodzący	Klient ACS i serwer ACS	Używany do strumieni wideo i danych urządzeń.

Baza danych

Pliki baz danych

Podstawowe pliki baz danych

AXIS Camera Station Pro 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 Pro 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\INTERNAL\main_db.

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

System tworzy kopię zapasową bazy danych każdej nocy, a także przed każdą aktualizacją. W aplikacji AXIS Camera Station Pro 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 Pro w celu zastosowania wprowadzonej zmiany. Jeżeli ścieżka folderu kopii zapasowej jest nieprawidłowa lub AXIS Camera Station Pro 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. Można wybrać dowolną liczbę 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 uaktualnieniu bazy danych. Możesz zobaczyć zdarzenia, które wystąpiły od ostatniego ponownego uruchomienia aplikacji AXIS Camera Station Pro 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. W obszarze **Configuration > Storage** (Konfiguracja > Pamięć masowa) określ lokalizację pamięci masowej i utwórz osobne kopie zapasowe nagrań.
- Ustawienia serwera i bazy danych w aplikacji AXIS Camera Station Pro Service Control nie zostały zapisane.

Kopia zapasowa systemu

System automatycznie zapisuje kopię zapasową systemu w folderze określonym na karcie **Database** (Baza danych). Zob. *Ustawienia bazy danych, on page 226*. Kopia zapasowa systemu zawiera podstawowe pliki bazy danych oraz pliki baz danych składników. Zob. *Pliki baz danych, on page 226*.

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 korzystania z komponentu, przykładowo, AXIS Camera Station Secure Entry lub funkcji inteligentnego wyszukiwania. • webrtc: W tym folderze znajdują się pliki konfiguracyjne WebRTC. • ACMSM: Folder ten zawiera plik bazy danych programu AXIS Camera Station Secure Entry SecureEntry.db oraz zdjęcia posiadaczy kart. • smartsearch: Folder ten zawiera plik bazy danych funkcji Inteligentnego wyszukiwania smartSearch-backup-yyyyMMddHHmmssfff.sqlite3.
backup_summary.json	Ten plik zawiera dokładniejsze informacje o kopii zapasowej.
_cluster_yyyyMMddHHmmssfff.dbcbackup	Plik ten zawiera logiczną kopię zapasową klastra bazy danych PostgreSQL, który obejmuje dane dotyczące całego klastra, takie jak role i tablice.

Konserwacyjne kopie zapasowe

Określ folder kopii zapasowych do przechowywania konserwacyjnych kopii zapasowych na karcie **Database** (Baza danych). Zob. *Ustawienia bazy danych, on page 226*. 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 Pro.
- Po ręcznym uruchomieniu narzędzia do konserwacji bazy danych **Database maintainer** w aplikacji AXIS Camera Station Pro Service Control. Zob. *Konserwacja bazy danych, on page 229*.
- Automatycznie przez zaplanowane zadanie konserwacji bazy danych skonfigurowane w harmonogramie zadań systemu Windows. Zob. *Narzędzia, on page 231*.

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.

Istnieją dwa sposoby ręcznego wykonania kopii zapasowej:

- **Opcja 1:** Przejdź do folderu `C:\ProgramData\AXIS Communications\AXIS Camera Station Server` i wykonaj kopię plików bazy danych. Następnie wykonaj kopię zapasową klastra bazy danych PostgreSQL:
 1. Otwórz terminal jako administrator w katalogu, w którym chcesz zapisać kopię zapasową.
 2. Uruchom "`C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe`" `backup -cluster`
 3. Kopia zapasowa zapisywana jest w folderze o nazwie `yyyyMMddHHmmssfff` w katalogu, w którym otworzyłeś terminal.
- **Opcja 2:** Utwórz raport systemowy i zaznacz opcję **Include all databases** (Uwzględnij wszystkie bazy danych), aby uwzględnić pliki kopii zapasowych baz danych. Zob. *Raport systemowy, on page 211*.

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, p. sekcja *Przygotuj kopię zapasową bazy danych, on page 227*.

Uwaga

Baza danych nie przechowuje nagrań. W obszarze **Configuration > Storage** (Konfiguracja > Pamięć masowa) określ lokalizację pamięci masowej i utwórz osobne kopie zapasowe nagrań.

Aby przywrócić bazę danych:

1. Przejdź do aplikacji AXIS Camera Station Pro Service Control i kliknij przycisk **Stop (Zatrzymaj)**, aby zatrzymać usługę.
2. Przejdź do plików kopii zapasowych bazy danych. Zob. *Przygotuj kopię zapasową bazy danych, on page 227*.
3. Wyodrębnij pliki.
4. Przywróć klaster bazy danych PostgreSQL:
 - 4.1. Otwórz terminal jako administrator w wyodrębnionym katalogu.

- 4.2. Uruchom "C:\Program Files\Axis Communications\AXIS Camera Station\Core\DbConsole\DbConsole.exe" restore -backup-file _cluster_yyyyMMddHHmmssfff.dbcbakup
- 4.3. Kliknij **y**, gdy pojawi się monit o potwierdzenie, że masz zaufanie do źródła pliku kopii zapasowej.
5. 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.

6. Jeżeli używasz programu AXIS Camera Station Secure Entry, postępuj zgodnie z instrukcjami w pliku RESTORE_INSTRUCTIONS.txt znajdującym się w folderze C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry 2\INTERNAL\main_db.
7. 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.
8. Jeżeli korzystasz z klienta internetowego programu VMS, skopiuj wszystkie pliki z folderu webrtc do C:\ProgramData\Axis Communications\AXIS Camera Station\Components\WebRTC.
9. Wróć do aplikacji AXIS Camera Station Pro 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 231*.

Uwaga

AXIS Camera Station Secure Entry wykorzystuje narzędzie DB Janitor do monitorowania plików bazy danych i ich zmniejszania w razie potrzeby. W przypadku wystąpienia wymuszonego zmniejszenia plików 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 antywirusowego bazy danych, ponieważ niektóre programy antywirusowe mogą uszkodzić bazę danych. Jeżeli używasz zewnętrznego systemu przechowywania kopii zapasowych, nie twórz kopii zapasowej 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 Pro 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”, aby sprawdzić, czy nie występują błędy pamięci RAM.

Certyfikaty

Użyj karty **Certificates** (Certyfikaty) do zarządzania certyfikatami serwerowymi w programie AXIS Camera Station Pro. Można wyświetlić informacje o bieżącym certyfikacie serwera, sprawdzić datę jego wygaśnięcia, a także wygenerować i importować nowe certyfikaty serwera albo wyeksportować certyfikat aktualny. Certyfikaty serwera znajdują się w folderze `C:\ProgramData\Axis Communications\AXIS Camera Station One Server\certs`.

Certyfikat serwera

Wygeneruj	Tworzenie nowego samopodpisanego certyfikatu serwera. Utworzony certyfikat zastępuje poprzednio używany przez serwer; wymagane jest ponowne uruchomienie serwera, by certyfikat zaczął obowiązywać.
Importuj...	Import certyfikatu serwera z pliku. Obsługiwane formaty plików to PEM i PFX / PKCS12. Obsługiwane są wyłącznie klucze RSA o długości co najmniej 2048 bitów.

Uwaga

Podczas importowania certyfikatu z certyfikatami pośrednimi w formacie PEM wszystkie certyfikaty pośrednie muszą znajdować się w pliku z rozszerzeniem .cer. Jeżeli tworzysz własne certyfikaty, p. sekcja *Przygotowanie certyfikatów pośrednich do importowania*, on page 230.

Aktualny certyfikat

Wyświetla informacje o aktualnym certyfikacie serwerowym. Służy do ręcznego sprawdzenia, czy klient połączył się z właściwym serwerem.

Wyświetl	Wyświetl więcej szczegółowych informacji na temat certyfikatu serwera.
Eksportuj...	Wyeksportuj certyfikat serwera jako plik PFX.

Generowanie nowego certyfikatu serwera

- Naciśnij klawisze Windows + S, aby wyszukać i otworzyć moduł sterowania usługą AXIS Camera Station Pro.
- Na karcie **Certificates** (Certyfikaty) kliknij **Generate** (Generuj), aby wygenerować nowy certyfikat serwera.
- Aby zastosować nowy certyfikat serwera, uruchom ponownie serwer.

Przygotowanie certyfikatów pośrednich do importowania

Aby zaimportować certyfikat z certyfikatami pośrednimi do programu AXIS Camera Station Pro, połącz certyfikat serwera i certyfikat pośredni w jeden plik:

- Otwórz jeden z certyfikatów serwera oraz certyfikat pośredni w Notatniku. Zawartość będzie mieć następującą strukturę:

```
cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
```

2. Skopiuj i wklej zawartość jednego certyfikatu do drugiego, a następnie zmień pierwszy wiersz na `combined_cert.cer`:

```
combined_cert.cer
-----BEGIN CERTIFICATE-----
MIIFTDCCB....
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIE+zCCA+OgA.....
-----END CERTIFICATE-----
```
3. Zapisz plik.

Narzędzia

W aplikacji AXIS Camera Station Pro Service Control wybierz **Modify settings** (Zmień ustawienia), a następnie kliknij **Tools** (Narzędzia), aby przeprowadzić konserwację bazy danych, utworzyć częściowy raport systemowy, włączyć rejestrację ruchu sieciowego lub zresetować urządzenie certyfikacji.

Narzędzie konserwacji bazy danych

Aby uruchomić narzędzie konserwacji bazy danych Database maintainer:

1. Otwórz aplikację AXIS Camera Station Pro Service Control.
2. Kliknij **Tools** (Narzędzia).
3. W obszarze **Database maintainer** (Narzędzie konserwacji bazy danych) kliknij **Run** (Uruchom).
4. Wyświetla się szacowany czas przestoju. Kliknij przycisk **Yes** (Tak), aby kontynuować. Uruchomionego procesu nie można anulować.

Uwaga

- Serwer AXIS Camera Station Pro i wszystkie bieżące nagrania są zatrzymywane na czas konserwacji. Po zakończeniu konserwacji serwer uruchamia się automatycznie.
- Podczas konserwacji nie wyłączaj 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.

Konieczne 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 Pro Database Maintenance” (Konserwacja bazy danych). Możesz edytować ustawienia wyzwalacza, aby ustawić kiedy i jak często ma być uruchamiana konserwacja bazy danych.

Rejestracja ruchu sieciowego

Aby uruchomić rejestrację ruchu sieciowego:

1. Otwórz aplikację AXIS Camera Station Pro Service Control.
2. Kliknij **Tools** (Narzędzia).
3. W obszarze **Network logging** (Rejestracja ruchu sieciowego) kliknij łącze, aby pobrać aplikację analizatora protokołów sieciowych.
4. Po jej zainstalowaniu kliknij **Start**, aby uruchomić aplikację.

Częściowy 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, p. sekcja *Raport systemowy*, on page 211.

Aby utworzyć częściowy raport systemowy:

1. Otwórz program AXIS Camera Station Pro service control.
2. Kliknij **Tools (Narzędzia)**.
3. W obszarze **Częściowy raport systemowy** kliknij **Run...** (Uruchom).
4. Wybierz i wprowadź wymagane informacje w oknie dialogowym.
5. Kliknij **Generate report (Generuj raport)**.

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 Pro i sposobów ich rozwiązywania. Zagadnienia pogrupowane są według tematów, co ma ułatwiać ich wyszukiwanie. Tematem może być na przykład dźwięk lub podgląd na żywo. Każde zagadnienie zawiera propozycję rozwiązania.

Aby uzyskać więcej materiałów, w tym wymagania sprzętowe, aktualizacje oprogramowania i samouczki, p. strona axis.com/support.

Jeżeli wystąpią ogólne problemy, przed podjęciem dalszych działań spróbuj ponownie uruchomić usługę serwera AXIS Camera Station Pro:

1. Przejdź do obszaru **Configuration (Konfiguracja) > Server (Serwer) > Diagnostics (Diagnostyka)**.
2. Kliknij **Restart AXIS Camera Station server service (Uruchom ponownie usługę serwera AXIS Camera Station)**.

Uwaga

Ponowne uruchamianie usługi serwera może trochę potrwać, a samej operacji ponownego uruchomienia nie można anulować. Serwer jest niedostępny, a wszystkie dołączone urządzenia tracą połączenie na czas jego ponownego uruchomienia.

Usługa AXIS Camera Station Pro

Usługa często uruchamia się ponownie

Serwer może być przeciążony, co wydłuża kolejkę zadań i zagraża integralności bazy danych.

- Sprawdź, czy program AXIS Camera Station Pro lub jakakolwiek inna aplikacja zużywa zbyt dużo zasobów.
- Uruchom narzędzie do konserwacji bazy danych Database maintainer. P. sekcja *Konserwacja bazy danych*, on page 229.

Jeżeli żadne z powyższych działań nie pomoże, skontaktuj się z pomocą techniczną Axis. Przejdź do *Proces eskalacji*, on page 249.

Urządzenia w systemie VMS

Typowe problemy

Wymienione kamery nie zostały dodane, ponieważ system VMS nie może nawiązać połączenia z kamerą	1. Sprawdź, czy kamera ma połączenie sieciowe i zasilanie oraz czy działa. 2. Wybierz kolejno opcje Configuration > Add devices (Konfiguracja > Dodaj urządzenia) i spróbuj ponownie dodać kamerę.
Wymienione kamery nie zostały dodane, ponieważ użytkownik anulował instalację	Aby dodać kamery, wybierz kolejno opcje Configuration > Add devices (Konfiguracja > Dodaj urządzenia) .
Nie można ustawić hasła dostępu do kamer widocznych na liście	1. Aby ręcznie ustawić hasło, przejdź do Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie). 2. Kliknij kamerę prawym przyciskiem myszy i wybierz User Management > Set password (Zarządzanie użytkownikami > Ustaw hasło).

Nie można dodać urządzenia

Urządzenie było używane w innym systemie przed dodaniem do AXIS Camera Station Pro	• Przywróć ustawienia fabryczne w urządzeniu. • Spróbuj dodać urządzenie do aplikacji AXIS Device Manager.
Zamiast wybranego urządzenia dodano inny model urządzenia	Może występować problem ze zgodnością. Zawsze korzystaj z najnowszej wersji AXIS Camera Station Pro.
Nie można dodać innego modelu urządzenia	Rozwiąż problemy z kamerą, p. strona axis.com/support/troubleshooting .

Nie można zaktualizować oprogramowania układowego urządzenia za pomocą AXIS Camera Station Pro

Oprogramowania układowego kamery nie można zaktualizować za pomocą interfejsu internetowego	Rozwiąż problemy z kamerą, p. strona axis.com/support/troubleshooting .
Nie na wszystkich urządzeniach można zaktualizować oprogramowanie układowe	• Sprawdź, czy masz połączenie sieciowe. • Jeżeli nie chodzi o problem z siecią IP, skontaktuj się z pomocą techniczną Axis. Przejdź do <i>Proces eskalacji</i>, on page 249.
Nie można zaktualizować oprogramowania sprzętowego konkretnych modeli	Może występować problem ze zgodnością. Kontakt z pomocą techniczną Axis. Przejdź do <i>Proces eskalacji</i> , on page 249.

Nie znaleziono urządzeń

System zarządzania obrazem automatycznie wyszukuje w sieci dołączone kamery i kodery wizyjne, ale nie znajduje żadnych.

- Sprawdź, czy 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.
 - Zmień NAT lub system zabezpieczeń, jeśli NAT lub system zabezpieczeń oddziela klienta od serwera. Zezwól na ruch przechodzący przez system zabezpieczeń lub NAT na porcie HTTP, porcie TCP (Transmission Control Protocol) i porcie strumieniowania, które określono w usłudze AXIS Camera Station Service Control. Aby wyświetlić pełną listę portów, p. sekcja *Lista portów dotycząca AXIS Camera Station Pro*, on page 216.
- Dodaj ręcznie kamery. Przejdź do sekcji *Dodawanie urządzeń*, on page 6.

Powtarzający się komunikat „Ponowne połączenie z kamerą za 15 s”

Możliwe problemy:

- Przeciążenie sieci.
- Kamera jest niedostępna. Sprawdź, czy kamera ma połączenie sieciowe.
- 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. Wybierz tę opcję w sekcji **Graphics card** (Karta graficzna) w obszarze **Hardware decoding** (Dekodowanie sprzętowe). Ustawienie znajdziesz w obszarze **Configuration > Client > Streaming** (Konfiguracja > Klient > Strumieniowanie).
- Dostosuj ustawienia obrazu i dźwięku. Na przykład zoptymalizuj ustawienia profilu na potrzeby niskiej przepustowości.

Nagrania

Typowe problemy

Zapis ciągły nie jest włączony	1. Aby wyłączyć nagrywanie ciągłe, przejdź do menu Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania). 2. Wybierz kamerę i włącz ustawienie Continuous (Ciągły).
Nie można nagrywać na określonym napędzie	1. Aby użyć innej pamięci masowej, wybierz kolejno opcje Configuration > Storage > management (Konfiguracja > Pamięć masowa > Zarządzanie). 2. Dodaj zasób pamięci i skonfiguruj jego ustawienia dla kamer.
Nie można zainstalować aplikacji AXIS Video Content Stream	1. Aby zainstalować aplikację ręcznie, wybierz kolejno opcje Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie). 2. Zaznacz kamerę i kliknij .

Nagrywanie nie rozpoczyna się

Jeżeli zapis nie rozpoczyna się albo zatrzymuje po kilku sekundach, oznacza to, że dysk jest zapełniony lub występuje zbyt duża ilość kolidujących danych.

- W 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. P. sekcja *Konfigurowanie pamięci masowej, on page 76*.

Przerwy w nagrywaniu podczas ciągłego nagrywania

Przerwy powodują wygenerowanie alarmów oznaczonych jako **Recording errors** (Błędy zapisu). Przerwy w nagrywaniu mogą wynikać z różnych przyczyn, takich jak:

- Przeciążenie serwera
- Problem z siecią
- Przeciążenie kamery
- Przeciążenie dysku

Sprawdź, czy przerwy w zapisie występują we wszystkich kamerach. Niewystępowanie przerw we wszystkich kamerach może wskazywać na przeciążenie kamery. Skorzystaj z poniższych pytań, aby określić przyczynę:

- 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 któryś z zasobów sprzętowych nie jest wykorzystywany w stopniu większym niż zwykle. Jeżeli dysk wykazuje oznaki przeciążenia, dodaj więcej dysków i ustaw w niektórych kamerach zapis na nowych dyskach.
- Zmniejsz ilość danych zapisywanych na dysku (ustawienia wizyjne, Zipstream, częstotliwość odświeżania, rozdzielczość). Weź pod uwagę przepustowość szacowaną przez aplikację AXIS Site Designer, p. strona axis.com/support/tools/axis-site-designer.

Aby uzyskać dodatkowe informacje, zob. *Jakość widoku na żywo i odtwarzania*, on page 237.

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, p. sekcja *Odtwarzanie i weryfikacja zapisów w AXIS File Player*, on page 7.

Uwaga

AXIS File Player automatycznie otwiera wszystkie nagrania znajdujące się w tym samym folderze co odtwarzacz.

Znikające nagrania

System przechowuje nagrania tylko przez określoną liczbę dni. Aby zmienić tę liczbę dni, wybierz kolejno opcje **Configuration > Storage > Selection (Konfiguracja > Pamięć masowa > Wybór)**.

Jeżeli pamięć masowa jest zapełniona, system może usunąć nagrania przed upływem okresu przechowywania. Aby uniknąć zapełnienia pamięci masowej, wypróbuj 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 Pro. Wybierz kolejno opcje **Configuration > Storage > Management (Konfiguracja > Pamięć masowa > Zarządzanie)**.
- Zmniejsz rozmiar nagrywanych plików, zmieniając na przykład rozdzielczość lub częstotliwość odświeżania. Wybierz kolejno opcje **Configuration > Devices > Stream profiles (Konfiguracja > Urządzenia > Profile strumieni)**.
 - Do zapisu należy stosować standard H.264. Standard M-JPEG wymaga dużo więcej pamięci masowej.
 - Aby jeszcze bardziej zmniejszyć rozmiary nagrań, użyj technologii Zipstream.

Problemy z zapisem awaryjnym

Przepustowość sieci łączącej kamerę z serwerem jest niewystarczająca do przesłania nagrania	Zwiększ przepustowość.
W okresie braku połączenia kamera nie zapisywała nagrań na karcie SD	• Zobacz raport serwera kamery. Zobacz na stronie axis.com/support/troubleshooting. • 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 skonfigurowania serwera NTP na potrzeby przyszłych nagrań. • Zsynchronizuj czas kamery z serwerem lub użyj tego samego serwera NTP w kamerze, co na serwerze.

Uwaga

Zapis awaryjny nie działa podczas kontrolowanego wyłączenia serwera ani w przypadku przerw w połączeniu trwających krócej niż 10 s.

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 Pro.

Urządzenie klienckie

Sprawdź, czy sterowniki karty graficznej lub karty sieciowej są aktualne.

1. Otwórz narzędzie diagnostyczne DirectX (wyszukaj dxdiag na komputerze).
2. Sprawdź w witrynie producenta urządzenia, czy masz najnowszy sterownik dla używanego systemu operacyjnego.
3. Sprawdź, czy aplikacje kliencka i serwera działają na tym samym komputerze.
4. Spróbuj uruchomić klienta na dedykowanym komputerze.

Sprawdź liczbę monitorów

Nie zaleca się dołączania więcej niż dwóch monitorów do jednej karty graficznej.

Uwaga

Uruchamianie klienta na maszynie wirtualnej nie jest obsługiwane.

Karta graficzna nie obsługuje standardu kodowania skonfigurowanego w **Configuration > Devices > Stream Profiles** (Konfiguracja > Urządzenia > Profile strumieniowania)

- Sprawdź, czy karta graficzna obsługuje standard kodowania strumieni.
- Spróbuj użyć różnych standardów kodowania.
- Jeżeli obsługiwany standard kodowania nie działa zgodnie z oczekiwaniami w kilku kamerach, sprawdź, czy sterowniki karty graficznej są zaktualizowane.

Dołączone 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. Patrz <i>Server requirements (Wymagania dotyczące serwera)</i> w przewodniku po instalacji i migracji oprogramowania AXIS Camera Station Pro.
Kamera jest podłączona do innego systemu zarządzania materiałem wizyjnym niż AXIS Camera Station Pro	Odłącz kamerę od innego klienta i ustaw ją jako domyślną, zanim ją połączysz z AXIS Camera Station Pro.
Jedna kamera wykorzystuje wiele różnych strumieni, zwłaszcza wysokiej rozdzielczości:	Może to stanowić problem zwłaszcza w przypadku niektórych kamer serii M-Line lub kamer wieloprzetwornikowych. Zmień strumień na ten sam profil strumieniowania lub ustaw niższą rozdzielczość. P. sekcja <i>Profile strumieniowania, on page 55</i>.

Przeciążenie serwera

Nietypowe wykorzystanie procesora lub pamięci RAM równoległe z występowaniem problemu	Sprawdź, czy żadna inna aplikacja obciążająca procesor lub pamięć RAM nie działa w tym samym czasie.
---	--

Problem z siecią

Nietypowe wykorzystanie przepustowości równoległe z występowaniem problemu	Sprawdź, czy żadna inna aplikacja, która zajmuje dużo przepustowości, nie działa w tym samym czasie.
Wystarczająca przepustowość / zdalna lub lokalna sieć IP	- Zapoznaj się z topologią sieci. - 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 jest domyślnie ustawione na **Auto**. P. Dekodowanie sprzętowe w sekcji *Przesyłanie strumieniowe, on page 123*.
- Jeżeli masz zainstalowane oprogramowanie antywirusowe, może ono blokować strumień na żywo lub foldery i procesy AXIS Camera Station Pro. P. sekcja *Najczęściej zadawane pytania*.

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 serwera kamer. Przejdź do axis.com/support/troubleshooting.
- Sprawdź, czy zaporą sieciowa nie blokuje połączeń na określonych portach, p. sekcja *Ogólne ustawienia serwera, on page 216*.
- Sprawdź, czy została zainstalowana aplikacja Desktop Experience do obsługiwanych wersji systemu Windows Server. P. sekcja *Zaplanowany eksport, on page 132*.
- Sprawdź, czy strumień o niższej rozdzielczości jest poprawnie odtwarzany.

Jeżeli żadne z opisanych wyżej rozwiązań nie pomoże, przejdź do sekcji *Proces eskalacji*, on page 249.

Wydajność dekodowania sprzętowego

Skorzystaj z niniejszego przewodnika dotyczącego rozwiązywania problemów w przypadku zauważenia opóźnień, zacięć lub przerywanego obrazu, wysokiego obciążenia procesora przy podglądzie na żywo lub częstych komunikatów "Reconnecting to camera" (Ponowne łączenie z kamerą).

1. Zaktualizuj sterowniki karty graficznej. Nieaktualne sterowniki są najczęstszą przyczyną problemów z przyspieszeniem sprzętowym. Wejdź na stronę internetową producenta (NVIDIA, AMD lub Intel) i pobierz najnowszy sterownik odpowiedni dla modelu posiadanej karty graficznej.
2. Zmień tryb dekodowania sprzętowego. Przejdź do **Configuration > Client > Streaming** (Konfiguracja > Klient > Strumieniowanie):
 - Jeżeli tryb ustawiony jest na **Automatic** (Automatyczny) lub **On** (Włączony) i występują problemy, ustaw go na **Off** (Wyłączony). Jeżeli wydajność wzrosła, może się okazać, że procesor graficzny nie ma wystarczającej mocy obliczeniowej, by obsłużyć bieżące obciążenie wynikające z odtwarzania strumienia. P. krok 6.
 - Jeżeli tryb jest wyłączony (**Off**), a obciążenie procesora graficznego wysokie, spróbuj ustawić tryb **Automatic** (Automatyczny) lub **On** (Wł.) – o ile dysponujesz wydajnym procesorem graficznym.
3. Monitoruj zasoby systemowe. Otwórz Menedżera zadań Windows (Ctrl + Shift + Esc) i przejdź do karty **Performance** (Wydajność):
 - Wykorzystanie procesora utrzymujące się na poziomie powyżej ~80% przy braku dekodowania sprzętowego sugeruje, że system może nie mieć wystarczającej mocy obliczeniowej do obsługi danej liczby lub rozdzielczości strumienia.
 - Wykorzystanie dedykowanej pamięci procesora graficznego na poziomie zbliżonym do maksymalnego przy włączonym dekodowaniu sprzętowym wskazuje na wąskie gardło tego procesora.
4. Zmniejsz liczbę kamer wyświetlanych jednocześnie lub przełącz je na profile strumieniowania o niższej rozdzielczości celem zmniejszenia obciążenia systemu.
5. Sprawdź, czy kamery strumieniają w standardzie H.264 lub AV1. Inne kodeki nie korzystają z dekodowania sprzętowego.
6. Oceń możliwości procesora graficznego. Nawet karta graficzna obsługująca dekodowanie sprzętowe może mieć ograniczenia w zakresie rozdzielczości lub częstotliwości odświeżania. W przypadku konfiguracji z wieloma strumieniami o wysokiej rozdzielczości zapoznaj się z *wymaganiami klienta AXIS Camera Station Pro* i rozważ modernizację karty graficznej do modelu z większą pamięcią VRAM i wyższą przepustowością dekodowania.
7. Jeżeli żadne z powyższych rozwiązań nie pomoże, skontaktuj się z *działem pomocy technicznej Axis* i przygotuj następujące informacje:
 - Sprzęt systemowy (procesor, karta graficzna, pamięć RAM).
 - Wersja systemu operacyjnego.
 - Wersja sterownika karty graficznej.
 - Wersja programu AXIS Camera Station Pro.
 - Objawy i kroki odtworzenia problemu.

Pamięć masowa

Pamięć sieciowa jest nieosiągalna

W przypadku używania lokalnego konta systemowego do logowania się w aplikacji AXIS Camera Station Pro 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 Pro 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 siecią 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 siecią pamięcią masową za pomocą nowej nazwy użytkownika i hasła.

Detekcja ruchu

Typowe problemy

Nie można zainstalować aplikacji AXIS Video Motion Detection	Aby zainstalować aplikację ręcznie, przejdź do <i>Instalowanie aplikacji do kamery, on page 70</i> .
Nie można pobrać aktualnych danych detekcji ruchu	Przywróć ustawienia fabryczne kamery: 1. Przejdź do menu Configuration > Devices > Management (Konfiguracja > Urządzenia > Zarządzanie). 2. Kliknij prawym przyciskiem myszy kamerę, z którą występuje problem, i kliknij Restore the camera to factory settings (Przywróć ustawienia fabryczne kamery). W czasie resetowania kamera jest niedostępna. Ustawienia IP i HTTPS pozostaną bez zmian. Po zakończeniu resetowania w kolumnie stanu wyświetla się komunikat Set password (Ustaw hasło). Kliknij Set password (Ustaw hasło), aby ponownie połączyć kamerę z serwerem.

Detekcja ruchu nie jest skonfigurowana	1. Aby ręcznie skonfigurować funkcjonalność wykrywania ruchu, wybierz kolejno opcje Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania). 2. Zaznacz kamerę i kliknij Motion settings (Ustawienia ruchu), aby skonfigurować detekcję ruchu.
Detekcja ruchu nie jest włączona	1. Wybierz kolejno opcje Configuration > Recording and events > Recording method (Konfiguracja > Zapis i zdarzenia > Metoda zapisywania). 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. P. sekcja <i>Edytowanie ustawień aplikacji AXIS Video Motion Detection 2 i 4, on page 89.</i>
Wbudowana funkcja detekcji ruchu	Można skonfigurować okna uwzględniane i pomijane. P. sekcja <i>Edytowanie wbudowanej funkcji detekcji ruchu, on page 90.</i>

Wyreguluj okres wyzwalacza

Okres wyzwalacza to odstęp czasu pomiędzy kolejnymi wyzwalaczami. Ustawienie to służy do zmniejszania liczby następujących po sobie nagrań. Jeżeli w tym odstępie czasu wystąpi dodatkowy wyzwalacz, zapis będzie kontynuowany, a okres wyzwalacza zostanie uruchomiony ponownie.

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.

Reguły akcji

Nieoczekiwane zdarzenia wyzwalaczy WE/WY

Jeśli około 1:15 w nocy występują nieoczekiwane zdarzenia wejścia/wyjścia, należy zastąpić istniejące wyzwalacze WE/WY wyzwalaczami opartymi na zdarzeniach w urządzeniu.

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 menu rozwijalnego **Microphone** (Mikrofon).
5. Z menu rozwijalnego **Use microphone for** (Użyj mikrofonu przy) wybierz, kiedy ma być używany dźwięk.
6. W razie potrzeby wybierz głośnik z menu rozwijalnego **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 Pro.

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. Więcej informacji, p. sekcja *Profile strumieniowania*, on page 55.

Brak dźwięku podczas odtwarzania

Dźwięk jest dostępny podczas odtwarzania, jeżeli obsługa dźwięku była włączona w profilu używanym podczas zapisu.

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 i będzie wyświetlać status połączenia na pasku stanu. Aby uzyskać więcej informacji o statusie połączenia, p. sekcja *Status połączenia, on page 134*.

Nazwa użytkownika lub hasło są niepoprawne	• Sprawdź pisownię lub użyj innego konta. • Sprawdź, czy użytkownik ma uprawnienia dostępu do serwera AXIS Camera Station Pro. • Zegary serwera i klienta AXIS Camera Station Pro muszą być zsynchronizowane. W przypadku użytkowników domenowych zegar serwera domeny musi być zsynchronizowany z serwerem i klientem. • Użytkownik, który nie został dodany do serwera, a należy do lokalnej grupy administratorów, musi uruchomić klienta jako administrator. • Więcej o uprawnieniach dostępu użytkowników, p. sekcja <i>Uprawnienia użytkownika, on page 138</i>.
Użytkownik nie ma uprawnień do zalogowania się na serwerze	Dodaj użytkownika w oknie dialogowym User permissions (Uprawnienia użytkownika).
Nie można zweryfikować zabezpieczeń wiadomości	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	• Sprawdź, czy serwer może połączyć się z siecią. • Upewnij się, że komputer serwera jest uruchomiony. • Upewnij się, że zapora jest poprawnie skonfigurowana. • Sprawdź pisownię adresu serwera.

	• Sprawdź ustawienia proxy klienta.
Brak odpowiedzi z serwera	Upewnij się, że łączysz się z właściwym komputerem i że serwer AXIS Camera Station Pro jest uruchomiony.
Klient nie może połączyć się z serwerem	Upewnij się, że sieć jest poprawnie skonfigurowana: • Sprawdź, czy system operacyjny jest obsługiwany. Aby uzyskać pełną listę obsługiwanych systemów operacyjnych, przejdź do <i>informacji o wersji</i>. • Z poziomu aplikacji Service Control sprawdź, czy serwer AXIS Camera Station Pro jest uruchomiony, albo uruchom go w razie potrzeby. • Sprawdź, czy klient i serwer są połączone z tą samą siecią. Jeżeli nie, klient powinien używać zewnętrznego adresu IP serwera. • Na komputerze pełniącym rolę serwera skonfiguruj ustawienia serwera proxy w oknie Opcje internetowe systemu Windows. • Skonfiguruj ustawienie serwera proxy klienta na stronie logowania, wybierz Change proxy settings (Zmień ustawienia serwera proxy). • Na komputerze klienckim skonfiguruj ustawienia serwera proxy klienta w oknie Opcje internetowe systemu Windows.
Nie można połączyć się z serwerem	• Sprawdź, czy adres i port serwera AXIS Camera Station Pro są prawidłowe. Sprawdź, czy zakres portów jest prawidłowo ustawiony w aplikacji Service Control. • Sprawdź, czy żadna brama NAT, zaporą sieciową ani oprogramowanie antywirusowe nie blokują połączenia z serwerem. Więcej informacji znajduje się w sekcji <i>Domeny i porty dotyczące funkcji Secure Remote Access v2, on page 219</i>. • Skorzystaj z aplikacji AXIS Camera Station Pro Service Control, aby sprawdzić, czy serwer jest uruchomiony. – Otwórz program AXIS Camera Station Pro Service Control, p. sekcja <i>Aplikacja AXIS Camera Station Pro Service Control, on page 214</i>. – Wyświetl stan serwera na karcie General (Ogólne). Jeśli serwer ma stan Stopped (Zatrzymany), kliknij Start, aby uruchomić serwer.
Nie można znaleźć serwera	• Upewnij się, czy serwer może połączyć się z siecią. • Sprawdź, czy adres i port serwera AXIS Camera Station Pro są prawidłowe. • Sprawdź, czy żadna brama NAT, zaporą sieciową ani oprogramowanie antywirusowe nie blokują połączenia z serwerem. • Sprawdź, czy ustawienia DNS klienta są prawidłowe. • Sprawdź, czy na serwerze DNS znajduje się wpis zawierający nazwę hosta i adres IP serwera.
Nie można połączyć się z serwerem	Sprawdź, czy komputer serwera i sieć IP nie są przeciążone.
Wersje serwera i klienta są różne	Uaktualnij serwer, aby używał tej samej wersji, co klient.

Lokalny serwer AXIS Camera Station Pro nie jest uruchomiony	Użyj aplikacji Service Control, aby uruchomić AXIS Camera Station Pro, lub wybierz serwer zdalny, do którego chcesz się zalogować.
Na tym komputerze nie zainstalowano serwera AXIS Camera Station Pro	Zainstaluj serwer AXIS Camera Station Pro albo wybierz inny serwer.
Wybrana lista serwerów jest 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:

- Upewnij się, że system jest zarejestrowany dla organizacji.
- Przejdź do **Configuration (Konfiguracja)** i sprawdź, czy opcja **Automatic licensing (Automatyczne licencjonowanie)** jest włączona. P. sekcja *Zarządzaj licencjami, on page 136*.
- Sprawdź, czy czas serwera jest aktualny.

Więcej informacji można znaleźć w *Przewodniku po instalacji i migracji aplikacji AXIS Camera Station Pro*.

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 Pro** 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

Nierozwiązany błąd certyfikatu uniemożliwia komunikację z **AXIS Camera Station Pro**.

Możliwe błędy	
Certificate Not Found (Nie znaleziono certyfikatu)	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: • Urządzenie zresetowano do ustawień fabrycznych. • Wyłączono funkcję bezpiecznej komunikacji przy użyciu protokołu HTTPS. • Nieuprawniona osoba uzyskała dostęp do urządzenia i zmieniła jego ustawienia.
Niezaufany certyfikat	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

Jeżeli w programie AXIS Camera Station Pro znajduje się urząd certyfikacji bez zapisanego hasła, pojawi się następujący 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 Pro traci połączenie z urządzeniami, a niektóre składniki systemu uruchamiają się ponownie.

Aby umożliwić aplikacji AXIS Camera Station Pro 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 Pro traci połączenie z urządzeniami, a niektóre składniki systemu uruchamiają się ponownie.

Synchronizacja czasu

Usługa Czas systemu Windows nie działa

Usługa Czas systemu Windows i serwer NTP nie są zsynchronizowane. Przyczyną może być fakt, że usługa Czas systemu Windows nie może nawiązać połączenia z serwerem NTP.

- Sprawdź, czy serwer NTP jest online.
- Sprawdź, czy ustawienia zapory sieciowej są prawidłowe.
- Sprawdź, czy 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 zapisu 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. Sprawdź, czy urządzenie ma dostęp do określonego 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 wysłało odpowiedniej ilości danych niezbędnych do synchronizowania czasu.

- 3.1. Aby wyłączyć generowanie alarmów, usuń zaznaczenie opcji **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.

Secure Remote Access v2

Nie można nawiązać lokalnego połączenia z usługami w chmurze

Aby rozwiązać problemy z łącznością z usługami w chmurze:

1. Otwórz program AXIS Camera Station Pro i przejdź do **Configuration > Connected services > Management** (Konfiguracja > Połączone usługi > Zarządzanie).
2. Sprawdź, czy **Status** jest wyświetlany na zielono. Jeśli nie, sprawdź połączenie internetowe.
3. Jeśli problem nie ustąpi, skontaktuj się z pomocą techniczną Axis w celu uzyskania wsparcia.

Nie można nawiązać zdalnego połączenia z usługami w chmurze

W oprogramowaniu AXIS Camera Station Pro:

1. Przejdź do obszaru **Menu > Help (Pomoc)** i kliknij **Status of Axis services (Status usług Axis)**. Spowoduje to otwarcie strony statusu <https://status.axis.com>, na której można sprawdzić ewentualne powiadomienia o konserwacji lub zaplanowanym przestoju.
2. W sekcji AXIS Camera Station Pro rozwiń listę rozwijalną, aby sprawdzić, czy usługi w chmurze są dostępne.
3. Sprawdź, czy Twoje konto My Axis zostało zaproszone do prawidłowej organizacji.

W aplikacji mobilnej AXIS Camera Station Pro:

1. Przejdź do sekcji **More (Więcej) > Help (Pomoc)** i kliknij **Status of Axis services (Status usług Axis)**. Spowoduje to otwarcie strony statusu <https://status.axis.com>, na której można sprawdzić ewentualne powiadomienia o konserwacji lub zaplanowanym przestoju.
2. Upewnij się, że masz stabilne połączenie internetowe. Spróbuj wykonać test na innym urządzeniu mobilnym, aby zidentyfikować przyczynę problemu.
3. Sprawdź, czy Twoje konto My Axis zostało zaproszone do prawidłowej organizacji.

Jeśli problem nie ustąpi, skontaktuj się z pomocą techniczną Axis w celu uzyskania wsparcia.

Ogólne problemy z utratą pakietów, opóźnieniami lub nieprawidłowym routingiem

1. Upewnij się, że masz dostęp do Internetu. Głównymi używanymi portami są porty 80 i 443, które powinny być również otwarte dla ruchu wychodzącego.
2. W zależności od routera może być konieczne otwarcie następujących dodatkowych domen z portami:
 - <https://eu.login.connect.axis.com> z portem 433
 - <https://eu.cs.connect.axis.com> z portem 433
 - <https://api.vms.axis.cloud> z portem 433
 - wss://signaling.prod.webrtc.connect.axis.com z portem 433
 - https://*.turn.prod.webrtc.connect.axis.com z portami 443, 3478, 5349 i 49152–65535

Uwaga

Gwiazdka „*” ma charakter dynamiczny i składa się z kombinacji regionu i niestatycznego identyfikatora serwera.

W celu uzyskania dalszego wsparcia skontaktuj się z działem pomocy technicznej Axis.

Wsparcie techniczne

Wsparcie techniczne jest dostępne dla klientów mających licencjonowaną wersję aplikacji AXIS Camera Station

Pro. Aby skontaktować się z działem pomocy technicznej, przejdź do  > Help > Online Support (Pomoc > Wsparcie online) lub 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 *wsparcia technicznego online 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.
- Czas wystąpienia problemu oraz, w stosownych przypadkach, nazwa lub adres IP kamery, której dotyczy problem.
- Raport systemowy AXIS Camera Station Pro generowany bezpośrednio po wystąpieniu problemu. Raport systemowy musi zostać wygenerowany przez klienta lub serwer, na którym odtworzono problem. Jeżeli problem powtarza się w przewidywalny sposób, włącz rejestrowanie na potrzeby usuwania błędów (debugowania) zarówno na serwerze, jak i na kliencie, aby dokładniej zidentyfikować przyczynę problemu. Po zakończeniu pamiętaj, aby wyłączyć rejestrowanie na potrzeby usuwania błędów.

W niektórych przypadkach zespół pomocy technicznej może poprosić o dodatkowe informacje.

Uwaga

Jeżeli rozmiar pliku (na przykład trasa sieciowa lub plik bazy danych) przekracza 1 GB, użyj zaufanej usługi bezpiecznego udostępniania plików.

Informacje dodatkowe	
Dzienniki poziomu debugowania	Dzienniki poziomu debugowania są domyślnie wyłączone, ponieważ wielkość pliku dziennika jest ograniczona. Jeżeli rejestrowanie poziomu debugowania jest włączone, pamiętaj, aby je wyłączyć po wygenerowaniu raportu systemowego. Server: Configuration > Server > Settings > Enable debug logging (Konfiguracja > Serwer > Ustawienia > Włącz rejestrowanie debugowania) Klient: Configuration > Client > Settings > Enable debug logging (Konfiguracja > Klient > Ustawienia > Włącz rejestrowanie debugowania)
Nakładanie debugowania przy podglądzie na żywo i odtwarzaniu	W przypadku wystąpienia problemu z podglądem na żywo lub odtwarzaniem pomocne jest nagranie ekranu przedstawiające nakładanie debugowania. Nagranie to powinno obejmować cały ekran łącznie z zegarem systemowym, aby pomoc techniczna mogła prześledzić problem w logach. • Naciśnij klawisze Ctrl + I raz, aby wyświetlić dane nałożenia w podglądzie na żywo. • Naciśnij klawisze Ctrl + I dwa razy, aby dodać informacje dotyczące usuwania błędów.

Informacje dodatkowe	
	Naciśnij klawisze Ctrl + I trzy razy, aby ukryć nałożenie.
Pliki baz danych	Użyj, gdy musimy sprawdzić lub ręcznie naprawić bazę danych. Przed wygenerowaniem raportu systemowego zaznacz opcję Include database in the report (Dołącz bazę danych do raportu) . Uwzględnij to za każdym razem, gdy pojawia się problem z uruchomieniem usługi AXIS Camera Station Service.
Zrzuty ekranu	Dodając zrzuty ekranu, ujmij cały ekran, aby przedstawić pełen kontekst. Jeżeli w Twojej ocenie zrzut ekranu w trybie pełnoekranowym jest niejednoznaczny, za pomocą strzałek zaznacz obszar będący punktem zainteresowania.
Nagrania ekranu	Korzystaj z nagrań ekranu, gdy problem trudno opisać słowami, na przykład gdy odtworzenie błędu wymaga wielu interakcji z interfejsem użytkownika.
Pliki nagrań	Dział pomocy technicznej może poprosić o dostarczenie przykładowych plików .acsm i .acsi, których program AXIS Camera Station używa do przechowywania nagrań. Dotyczy to sytuacji, gdy występują problemy z odtwarzaniem lub eksportowaniem nagrań albo gdy występują problemy z aplikacją AXIS File Player. Pliki te można znaleźć w lokalizacji pamięci masowej wybranej dla każdej kamery.

T10196821_pl

2026-07 (M33.8)

© 2023 – 2026 Axis Communications AB