AXIS Optimizer

AXIS Optimizer for XProtect®
AXIS Optimizer for Siemens Siveillance™

Podręcznik użytkownika

Spis treści

AXIS Optimizer 7
Przeznaczenie aplikacji AXIS Optimizer 7
Wymagania systemowe 7
Obsługa systemów sfederowanych 7
Obsługa systemów kompleksowych 7
Uwagi dot. wersji 7
Instalowanie i aktualizowanie aplikacji AXIS Optimizer 8
Instalowanie programu AXIS Optimizer 8
Które wersje są zainstalowane w moim systemie? 8
Zaawansowane opcje instalacji 8
Migracja systemu VMS 9
Sprawdzenie integralności pliku instalacyjnego 9
Aktualizacja aplikacji AXIS Optimizer 9
Ręczna aktualizacja 10
Automatyczne uaktualnianie systemu 10
Włączanie uaktualniania automatycznego 10
Wyłączanie automatycznego uaktualniania 11
Dowiedz się więcej 11
Odinstalowanie aplikacji AXIS Optimizer 11
Ustawienia fabryczne 11
Bezpieczne wycofanie z eksploatacji 12
Uprawnienia użytkowników 12
Dostęp do ustawień urządzenia 13
Asystent urządzeń 13
Konfigurowanie urządzenia Axis 13
Instalowanie aplikacji na urządzeniu Axis 13
Konfigurowanie aplikacji w urządzeniu Axis 13
Aktualizowanie aplikacji na urządzeniu Axis 13
Ponowne uruchamianie urządzenia Axis 14
Kopiowanie adresu IP urządzenia Axis 14
Wykonanie automatyzacji 15
Tworzenie akcji dla urządzeń Axis 15
Wtyczka serwera zdarzeń 15
Instalowanie wtyczki Serwer zdarzeń 15
Osuszanie wielu kamer jednym kliknięciem 15
Włączanie automatycznego regulowania ostrości jednym kliknięciem dla wielu kamer 16
Wyzwalanie kilku syren stroboskopowych za pomocą jednego kliknięcia 17
Automatyczne wyłączanie masek prywatności w wielu kamerach 18
Aktywowanie syreny stroboskopowej po wykryciu ruchu przez kamerę 20
Odtwarzanie klipów audio na głośnikach lub w strefie głośnika, gdy kamera wykryje ruch 22
Rozwiązywanie problemów z regułą 23
Centralnie zarządzanie listami tablic rejestracyjnych 23
Tworzenie listy 24
Konfigurowanie uprawnień do list 24
Edytowanie listy 24
Importowanie listy 25
Eksportowanie listy 26
Tu się dowiesz więcej o listach 26
Odpowiadanie na zdarzenia w czasie rzeczywistym 27
Używanie elementów sterujących urządzenia 27
Elementy sterujące operatora 27
Dostęp do elementów sterujących operatora 27
Zapisywanie obszaru ostrości kamery PTZ 27

Automatyczne ustawianie ostrości w kamerze 28
Włączanie szybkiego osuszania lub wycieraczki 28
Pomiar temperatury punktowej 29
Automatyczne przybliżanie i śledzenie ruchomego obiektu....29
Tworzenie niestandardowych elementów sterujących operatora 30
Konfigurowanie dostępu do elementów sterujących operatora 30
Interakcja za pośrednictwem głośników....31
Menedżer głośników 31
Tryby....31
Tryb AXIS Audio Manager Pro 31
Tryb AXIS Audio Manager Edge 33
Tryb zgodności wstecznej 34
Odtwarzanie dźwięku przez głośniki....35
Odtwarzanie dźwięku przez głośniki w widoku kamery....36
Odtwarzanie dźwięku przez głośniki w przypadku alarmów 36
Ustawienie zachowania wizualnego przy rozmowie przez głośnik 36
Zakładki nagrań fonicznych w obszarze obserwacji kamery lub w sekcji Alarmy....37
Zarządzanie osobami odwiedzającymi 37
Wtyczka interkomu....37
Konfigurowanie interkomu 37
Ustawianie uprawnień dla interkomu....38
Wykonywanie połączenia testowego....39
Eliminacja echa w trakcie połączeń 39
Sterowanie interkomem za pomocą podglądu na żywo 40
Odbieranie połączenia z okna podglądu na żywo....42
Wyświetlanie wielu kamer w oknie połączenia....43
Akcje okna wywołania....44
Wyświetlanie strony w oknie połączenia 44
Filtrowanie według numerów wewnętrznych 45
Wyświetlanie historii połączeń....45
Wyłączanie mikrofonu przy braku aktywnego połączenia 46
Generowanie alarmu po siłowym otwarciu drzwi....47
Włączanie alarmu w przypadku zbyt długiego otwarcia drzwi....47
Blokowanie odbierania połączeń w aplikacjach klienckich....47
Wizualizacja dźwięku 47
Widok mikrofonu....47
Konfiguracja VMS dla widoku mikrofonu....48
Dodawanie widoku mikrofonu do aplikacji Smart Client....48
Korzystanie z widoku mikrofonu....48
Jednoczesne słuchanie dźwięku z kilku mikrofonów....49
Wykrywanie zdarzeń z dźwiękiem....49
Analizowanie zdarzeń 49
Prace wyjaśniające....50
Prace wyjaśniające 50
Zanim rozpoczniesz 50
Konfigurowanie wyszukiwania do celów dochodzeniowych 50
Wyszukiwanie materiału....51
Zawężanie wyszukiwania....52
Ograniczenia....52
Wyszukiwanie pojazdów 53
Konfigurowanie wyszukiwania pojazdów....55
Wyszukiwanie pojazdu 55
Zawężanie wyszukiwania....55
Optymalizacja szybkości wyszukiwania 56
Zone speed search (Wyszukiwanie prędkości w strefie)....56
Konfiguracja wyszukiwania prędkości w strefie....56

Wyszukiwanie zdarzeń związanych z prędkością w strefie 57
Zawężanie wyszukiwania 57
Wyszukiwanie kontenerów 58
Konfigurowanie wyszukiwania kontenerów 58
Wyszukiwanie kontenerów 58
Zawężanie wyszukiwania 59
Tworzenie raportu PDF o wysokiej jakości 59
Axis license plates 59
Zanim rozpoczniesz 60
Konfigurowanie aplikacji Axis do tablic rejestracyjnych 60
Wyszukiwanie tablicy rejestracyjnej 60
Wyszukiwanie tablicy rejestracyjnej na żywo 60
Zawężanie wyszukiwania 61
Optymalizacja szybkości wyszukiwania 61
Eksportowanie wyników wyszukiwania tablic rejestracyjnych w formie raportu PDF 61
Eksportowanie wyników wyszukiwania tablic rejestracyjnych w formie raportu CSV 61
Funkcje analityczne Axis 62
Dostęp do aplikacji Axis insights 62
Utwórz nowy pulpit nawigacyjny 62
Konfiguracja listy rozwijalnej na pulpicie nawigacyjnym 63
Wyświetlanie wyników analiz dla danego widoku z kamery 63
Konfigurowanie funkcji analitycznych Axis 63
Rozwiązywanie problemów z aplikacją Axis insights 64
Korekcja obrazu wideo 65
Tworzenie widoku z korekcją krzywizn 65
Tworzenie widoku z korekcją krzywizn w przypadku wieloprzetwornikowych kamer panoramicznych 66
Widok szeroki 67
Ustawianie pozycji domowej 67
Zezwalanie operatorom na kontrolowanie i edytowanie widoków z korekcją krzywizn 68
Wydajność i rozwiązywanie problemów 68
Integracja urządzeń nasobnych 70
Dowiedz się więcej 70
Kontrola dostępu 71
Konfiguracja kontroli dostępu 71
Dodawanie sieciowego kontrolera drzwiowego Axis do systemu 71
Uaktywnienie licencji dot. drzwi 72
Skonfiguruj kontrolę dostępu 72
Integracja systemu kontroli dostępu 73
Drzwi i strefy 73
Przykład drzwi i stref 74
Dodaj drzwi 75
Ustawienia drzwi 76
Poziom zabezpieczeń drzwi 77
Opcje czasu 78
Dodawanie monitora drzwi 79
Dodawanie drzwi dozorujących 79
Dodawanie czytnika 80
Dodawanie urządzenia REX 81
Dodawanie strefy 82
Poziom zabezpieczeń strefy 82
Nadzorowane wejścia 83
Akcje wykonywane ręcznie 84
Formaty kart i kod PIN 84
Ustawienia formatu karty 86
Profile identyfikacji 88
Szyfrowana komunikacja 89

Bezpieczny kanał OSDP 89
Multiserwer BETA 89
Proces 90
Generowanie pliku konfiguracyjnego z serwera podrzędnego 90
Importowanie pliku konfiguracyjnego do serwera głównego 90
Unieważnianie serwera podrzędnego 90
Usuwanie serwera podrzędnego 90
Zarządzanie dostępem 91
Proces zarządzania dostępem 91
Dodawanie posiadacza karty 91
Dodaj poświadczenia 92
Dodawanie grupy 94
Dodaj regułę dostępu 95
Ręczne odblokowywanie drzwi i stref 95
Eksportowanie raportów konfiguracji systemu 96
Tworzenie raportów aktywności posiadaczy kart 96
Ustawienia zarządzania dostępem 97
Import i eksport 97
Kopia zapasowa i przywracanie 99
Zarządzanie dostępem w aplikacji Smart Client 99
Ustawienia ról w aplikacji AXIS Secure Entry 99
Zarządzanie systemem i kontrola bezpieczeństwa 101
Dostęp do ustawień funkcji dla operatorów 101
Ustawienia roli 101
Konfigurowanie ustawień ról 101
Zarządzanie urządzeniami 102
AXIS Device Manager Extend 102
Instalowanie hosta brzegowego 102
Przypisanie hosta na krawędzi systemu i synchronizacja urządzeń 103
Używanie AXIS Device Manager Extend do konfigurowania urządzeń 104
Rozwiązywanie problemów dotyczących dodawania urządzeń do hosta na krawędzi systemu 104
AXIS Site Designer: import 104
Importowanie projektu 104
Importowane ustawienia 105
Ograniczenia 105
Zarządzanie kontami 106
Łączenie się z urządzeniami za pomocą konta usługi XProtect 106
Axis events 106
Konfigurowanie zdarzenia dla wielu urządzeń 107
Informacje o wydarzeniach 107
Metadane i wyszukiwanie 107
Konfiguracja ustawień metadanych 107
Konfiguracja kategorii wyszukiwania Axis 108
Cyberbezpieczeństwo 109
Zarządzanie podatnościami 109
Powiadomienia dotyczące zabezpieczeń 109
Bezpieczny cykl eksploatacji produktu 109
Przewodnik dotyczący wzmacniania systemów 109
Potrzebujesz więcej pomocy? 111
Często zadawane pytania 111
Rozwiązywanie problemów 111
Kontakt z pomocą techniczną 111
Porady i wskazówki 112
Dodawanie strony internetowej w widoku klienta inteligentnego 112
Eksportowanie plików wideo z osadzonymi funkcjami wyszukiwania 112
Eksportowanie filmów w formacie XProtect 112

Odblokowywanie eksportu na komputerach odbiorczych 112
Odtwarzaj wyeksportowany widok skorygowany Axis 112

AXIS Optimizer

Aplikacja AXIS Optimizer pozwala korzystać z funkcji Axis bezpośrednio w oprogramowaniu XProtect i Siemens Siveillance Video. Optymalizuje ona działanie urządzeń Axis w tych systemach zarządzania materiałem wizyjnym, ograniczając czaso- i pracochłonność przy konfigurowaniu systemów i podczas codziennej eksploatacji. Aplikacja jest bezpłatna.

Przeznaczenie aplikacji AXIS Optimizer

Produkt ten jest przeznaczony dla specjalistów posiadających rozległą wiedzę w zakresie obsługi systemu zarządzania obrazem (VMS).

Wymagania systemowe

Aplikacja AXIS Optimizer jest w pełni obsługiwana na następujących platformach:

- XProtect Essential+
- XProtect Express+
- XProtect Professional+
- XProtect Expert
- XProtect Corporate
- Siemens Siveillance Video Pro
- Siemens Siveillance Video Advanced
- Siemens Siveillance Video Core Plus
- Siemens Siveillance Video Core

Zalecamy używanie najnowszych wersji klienta zarządzania i Smart Client. Najnowsza wersja aplikacji AXIS Optimizer jest zawsze przetestowana na zgodność z najnowszą wersją VMS. Więcej informacji, p. sekcja . *Uwagi dot. wersji, on page 7*

Uwaga

Minimalna obsługiwana platforma

- VMS w wersji 2019 R3.

Nawiązania do narzędzia Smart Client w pomocy dotyczą zarówno aplikacji XProtect Smart Client, jak i aplikacji Video Client w systemie Siemens.

Obsługa systemów sfederowanych

Aplikacja AXIS Optimizer jest w pełni obsługiwana w systemach sfederowanych.

Obsługa systemów kompleksowych

Aplikacja AXIS Optimizer w pełnym zakresie współpracuje z systemami kompleksowymi.

Uwaga

Wymagania

- Wersja systemu VMS 2022 R3 lub nowsza.

Uwagi dot. wersji

Aby zapoznać się z najnowszymi informacjami o wersji, przejdź do strony *axis.com/ftp/pub_soft/cam_srv/optimizer_milestone/latest/relnote.txt*.

Instalowanie i aktualizowanie aplikacji AXIS Optimizer

Instalowanie programu AXIS Optimizer



Uwaga

Aby zaktualizować aplikację AXIS Optimizer, trzeba mieć uprawnienia administratora.

1. Upewnij się, że masz poprawną wersję aplikacji klienckiej systemu VMS.
2. Zaloguj się na swoje konto MyAxis.
3. Ze strony *axis.com/products/axis-optimizer-for-milestone-xprotect* pobierz aplikację AXIS Optimizer do każdego urządzenia, na którym jest uruchomione oprogramowanie klienta zarządzania lub Smart Client.
4. Uruchom pobrany plik i postępuj zgodnie z instrukcjami krok po kroku.

Które wersje są zainstalowane w moim systemie?

W oknie **System overview (Przegląd systemu)** można zobaczyć, które wersje aplikacji AXIS Optimizer i AXIS Optimizer Body Worn Extension są zainstalowane na różnych serwerach i klientach w systemie.

Uwaga

Aby klienty i serwery były wyświetlane w oknie **System overview (Przegląd systemu)**, musi być na nich zainstalowane oprogramowanie AXIS Optimizer w wersji 3.7.17.0 lub nowszej albo oprogramowanie AXIS Optimizer Body Worn Extension w wersji 1.1.11.0 lub nowszej.

Aby wyświetlić aktywne serwery i klienty:

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > System overview (Nawigacja po witrynie > AXIS Optimizer > Przegląd systemu)**.

Aby uaktualnić określony serwer lub klienta:

1. Przejdź do tego konkretnego serwera lub klienta i uaktualnij jego oprogramowanie lokalnie.

Zaawansowane opcje instalacji

Jeżeli chcesz zainstalować aplikację AXIS Optimizer na kilku urządzeniach jednocześnie bez udziału użytkownika:

1. Kliknij prawym przyciskiem myszy menu **Start**.
2. Kliknij przycisk **Run (Uruchom)**.
3. Przejdź do pobranego pliku instalacyjnego i kliknij przycisk **Otwórz**.
4. Na końcu ścieżki dodaj jeden parametr lub więcej parametrów.

Parametr	Opis
`/SILENT`	Podczas instalacji dyskretnej nie jest wyświetlana instrukcja krok po kroku i okno tła. Widać jednak okno postępu instalacji.
`/VERYSILENT`	Podczas instalacji bardzo dyskretnej nie jest wyświetlana instrukcja krok po korku, okno tła ani okno postępu instalacji.

/FULL	Zainstaluj wszystkie komponenty, na przykład opcjonalną wtyczkę serwera zdarzeń i wtyczkę Secure Entry. Funkcja ta jest użyteczna w połączeniu z parametrem /VERYSILENT.
/SUPPRESSMSGBOXES	Wyłącz wszystkie okna komunikatów. W większości przypadków funkcja ta jest stosowana w połączeniu z parametrem /VERYSILENT.
/log=<filename>	Utwórz plik dziennika.
/NORESTART	Zapobiega ponownemu uruchomieniu komputera podczas instalacji.
/EVENTSERVERPLUGIN	Zainstaluj wtyczkę serwera zdarzeń, jeżeli komputer docelowy jest serwerem zdarzeń.
/SECUREENTRY	Zainstaluj usługę kontroli dostępu Secure Entry, jeżeli komputer docelowy jest serwerem zdarzeń.

5. Naciśnij klawisz **Enter**.

Przykład:
Instalacja Verysilent, zalogowanie do output.txt, bez ponownego uruchamiania komputera

```
.\AxisOptimizerXProtectSetup.exe /VERYSILENT /log=output.txt /NORESTART
```

Migracja systemu VMS

Aplikacja AXIS Optimizer przechowuje większość danych w bazie danych systemu VMS, dzięki czemu pozostają one zachowane w przypadku migracji systemu VMS na inny serwer.

Aby zmigrować system VMS na inny serwer, p. dokument *How to move an XProtect VMS installation/version from old servers to new servers* (Przenoszenie instalacji / wersji XProtect VMS ze starych serwerów na nowe).

Sprawdzenie integralności pliku instalacyjnego

Aby sprawdzić integralność pliku instalacyjnego aplikacji AXIS Optimizer:

1. Kliknij prawym przyciskiem myszy plik instalatora i wybierz **Properties** (Właściwości).
2. Przejdź do **Digital Signatures** (Podpisy cyfrowe), a następnie kliknij **Details** (Szczegóły).
3. Sprawdź, czy:
   - W sekcji **Digital Signature Information** (Informacje o podpisie cyfrowym) widnieje komunikat: This digital signature is OK (Ten podpis cyfrowy jest prawidłowy).
   - W sekcji **Signer information** > **Name** (Informacje o podpisującym > Nazwa) widnieje wpis Axis Communications AB.

Aktualizacja aplikacji AXIS Optimizer

Aplikacja AXIS Optimizer jest regularnie aktualizowana - wprowadzamy nowe funkcje, dokonujemy ulepszeń, udoskonalamy zabezpieczenia. AXIS Optimizer oferuje jedną ścieżkę wsparcia (najnowszą i najlepszą), tak że do pobrania ze strony axis.com jest tylko najnowsza wersja aplikacji. Najlepiej zawsze korzystać z najnowszej wersji aplikacji AXIS Optimizer.

Aplikacja AXIS Optimizer zawiera również funkcję pozwalającą zaktualizować wszystkie klienty w systemie VMS. Więcej informacji, p. sekcja *Automatyczna aktualizacja systemu*.

Uwaga

Aby zaktualizować aplikację AXIS Optimizer, trzeba mieć uprawnienia administratora.

Powiadomienia o aktualizacjach

Aplikacja AXIS Optimizer regularnie sprawdza dostępność swoich nowszych wersji i powiadamia o ich znalezieniu. Jeżeli Twoje urządzenie ma połączenie z siecią, powiadomienia o aktualizacjach otrzymasz w narzędziu Smart Client.

Aby zmienić rodzaj otrzymywanych powiadomień:

1. W aplikacji Smart Client przejdź do **Settings** > **Axis general options** > **Notification preference** (Ustawienia > Ogólne opcje Axis > Preferencje powiadomień).
2. Zaznacz opcję **All (Wszystkie)**, **Major (Główne)** lub **None (Brak)**.

Aby skonfigurować te powiadomienia dla wszystkich klientów w systemie VMS:

1. Przejdź do **Management Client** > **Site Navigation** > **AXIS Optimizer** > **System overview** (Management Client > Nawigacja po obiekcie) > AXIS Optimizer > Przegląd systemu).
2. Kliknij opcję **System upgrade settings (Ustawienia aktualizacji systemu)**.
3. Włącz lub wyłącz opcję **Show upgrade notifications on all clients (Pokazuj powiadomienia o uaktualnieniu na wszystkich klientach)**.

Ręczna aktualizacja

Aplikację AXIS Optimizer można aktualizować ręcznie z klienta zarządzania i Smart Client.

Uwaga

Aby zaktualizować aplikację AXIS Optimizer, trzeba mieć uprawnienia administratora.

W aplikacji Management Client

1. Wybierz kolejno opcje **Site Navigation > Basics > AXIS Optimizer (Nawigacja po witrynie > Podstawy > AXIS Optimizer)**.
2. Kliknij przycisk **Aktualizuj**.

W aplikacji Smart Client

1. Wybierz kolejno opcje **Settings > Axis general options (Ustawienia > Ogólne opcje Axis)**.
2. Kliknij przycisk **Aktualizuj**.

Automatyczne uaktualnianie systemu

Z serwera zarządzania systemu VMS można opublikować lokalną wersję aplikacji AXIS Optimizer do swojego systemu. Wykonanie tych czynności umożliwi automatyczne uaktualnianie programu AXIS Optimizer na wszystkich urządzeniach klienckich. Proces automatycznego uaktualnienia nigdy nie powoduje przerwania pracy operatora. Dyskretne instalacje są wykonywane podczas ponownego uruchamiania maszyny lub klienta VMS. Automatyczne uaktualnienie jest obsługiwane również wtedy, gdy klient nie ma połączenia z Internetem.

Uwaga

Funkcja automatycznego uaktualniania jest obsługiwana w przypadku klientów korzystających z programu AXIS Optimizer w wersji 4,4 lub nowszej.

Włączanie uaktualniania automatycznego



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

Uwaga

Wymagania

- System, w którym klient zarządzania działa na tym samym komputerze, co serwer zarządzania VMS.
- Uprawnienia administratora komputera na serwerze zarządzania VMS.

Aby włączyć funkcję automatycznego uaktualniania, należy opublikować w systemie określoną wersję programu AXIS Optimizer:

1. Na serwerze zarządzania systemu VMS zainstaluj wersję aplikacji AXIS Optimizer, którą chcesz opublikować w całym systemie.
2. Na komputerze serwera zarządzania systemu VMS otwórz aplikację Management Client.
3. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > System overview (Nawigacja po witrynie > AXIS Optimizer > Przegląd systemu)**.
4. Kliknij opcję **System upgrade settings (Ustawienia aktualizacji systemu)**.
5. Sprawdź, czy wersja w polu **Local version (Wersja lokalna)** jest poprawna, a następnie kliknij przycisk **Publish (Publikacja)**.
   Jeżeli jest już opublikowana jakaś wersja pakietu AXIS Optimizer, zostanie zastąpiona nową wersją.

Uwaga

Urządzenia klienckie z wersjami AXIS Optimizer w wersjach wcześniejszych niż 4.4 trzeba uaktualnić ręcznie.

Wyłączanie automatycznego uaktualniania

Aby wyłączyć automatyczne uaktualnianie, należy zresetować opublikowaną wersję:

1. Na komputerze serwera zarządzania systemu VMS otwórz aplikację Management Client.
2. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > System overview (Nawigacja po witrynie > AXIS Optimizer > Przegląd systemu)**.
3. Kliknij opcję **System upgrade settings > Reset published version** (Ustawienia aktualizacji systemu > Resetuj opublikowaną wersję).

Dowiedz się więcej

- Inteligentne klienty bez aplikacji AXIS Optimizer mogą uzyskać dostęp do pliku instalacyjnego opublikowanego na stronie internetowej serwera zarządzania (*http://[adresserwera]/installation/*), nawet jeśli nie mają połączenia z Internetem.
- Pakiet instalacyjny aplikacji AXIS Optimizer jest dostępny w menedżerze pobierania systemu VMS i można go tam konfigurować.
- W systemach sfederowanych i kompleksowych aplikację AXIS Optimizer należy opublikować na każdym serwerze zarządzania.
- Po opublikowaniu nowej wersji aplikacji AXIS Optimizer można monitorować, które oprogramowanie klienckie zostało uaktualnione do opublikowanej wersji. Obok urządzeń korzystających z opublikowanej wersji na stronie **System overview** (Przegląd systemu) będzie widoczny zielony symbol zaznaczenia.
- Funkcja automatycznego uaktualniania jest wyłączona w urządzeniach, w których uruchomiono serwer zarządzania systemu VMS.

Odinstalowanie aplikacji AXIS Optimizer

Ustawienia fabryczne

Aby przywrócić aplikację AXIS Optimizer do ustawień domyślnych, odinstaluj ją z systemu VMS i zainstaluj ponownie.

Bezpieczne wycofanie z eksploatacji

Aby całkowicie usunąć aplikację AXIS Optimizer oraz zapisane dane z systemu VMS, wykonaj najpierw poniższe czynności (w stosownych przypadkach), a dopiero potem usuń aplikację z komputera lokalnego.

1. Aby usunąć listy numerów tablic rejestracyjnych:
   - Otwórz aplikację Management Client i przejdź do **AXIS Optimizer** > **License plate lists** (AXIS Optimizer > Listy numerów tablic rejestracyjnych).
   - Usuń wszystkie obiekty z listy.
2. Aby odłączyć serwer AXIS Audio Manager Pro:
   - Otwórz aplikację Management Client i przejdź do **AXIS Optimizer** > **Speaker manager** (AXIS Optimizer > Menedżer głośników).
   - Kliknij **Disconnect (Odłącz)**.

Aby usunąć aplikację AXIS Optimizer oraz dane przechowywane lokalnie w komputerze:

1. Kliknij menu **Start** > **Ustawienia** > **Aplikacje** > **Zainstalowane aplikacje**.
2. Przejdź do **AXIS Optimizer**.
3. Kliknij p,255mm,sfx)=″graphics:graphicFE51463A3463EF1848C7CD2F60A78298″ i wybierz **Uninstall** (Odinstaluj).

Uwaga

Po odinstalowaniu aplikacji AXIS Optimizer niektóre usługi VMS będą musiały być ponownie uruchomione.

Uprawnienia użytkowników

Aplikacja AXIS Optimizer ma specjalną rolę użytkownika aplikacji Axis Optimizer. Ma ona ułatwiać administratorowi nadawanie użytkownikom uprawnień na inteligentnym kliencie wymaganych do używania funkcji i narzędzi aplikacji AXIS Optimizer.

W systemie XProtect 2018 R3 i starszych rola jest dostępna tylko w wersji XProtect Corporate.

W systemie XProtect 2019 R1 i nowszych rola jest dostępna w następujących wersjach:

- Firmowe
- Expert
- Professional+
- Essential+
- Express+

Jeżeli wolisz konfigurować uprawnienia ręcznie, użyj poniższej konfiguracji, aby umożliwić operatorowi narzędzia Smart Client korzystanie ze wszystkich funkcji aplikacji AXIS Optimizer:

- Sprzęt: Polecenia sterujące
- Kamery: Polecenia AUX

Uwaga

Opis bardziej zaawansowanej obsługi ról użytkowników znajduje się w temacie *Dostęp do ustawień funkcji dla operatorów, on page 101*.

Dostęp do ustawień urządzenia

Asystent urządzeń

Asystent urządzeń umożliwia łatwy dostęp do wszystkich ustawień urządzenia Axis bezpośrednio w kliencie do zarządzania systemami VMS. Wewnątrz systemu VMS można łatwo odszukać stronę WWW urządzenia Axis, przejść do niej i tam zmienić różne ustawienia urządzenia. Można również konfigurować aplikacje zainstalowane na urządzeniach.

Ważne

- Aby można było używać Asystenta urządzeń, urządzenie Axis musi być podłączone do tej samej sieci, co klient zarządzania.
- Asystent urządzeń nie jest obsługiwany w sieciach IPv6.

Konfigurowanie urządzenia Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Wybierz urządzenie i przejdź do ustawienia **Device settings (Ustawienia urządzenia)**. Zostanie otwarta strona webowa urządzenia.
3. Skonfiguruj żądane ustawienia.

Instalowanie aplikacji na urządzeniu Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Wybierz urządzenie i przejdź do ustawienia **Device settings (Ustawienia urządzenia)**. Zostanie otwarta strona webowa urządzenia.
3. Przejdź do menu **Apps (Aplikacje)**. Umiejscowienie menu **Apps (Aplikacje)** zależy od wersji oprogramowania urządzenia. Więcej informacji można znaleźć w pomocy urządzenia.
4. Zainstaluj żądane aplikacje.

Konfigurowanie aplikacji w urządzeniu Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Zaznacz urządzenie i przejdź do sekcji **Applications (Aplikacje)**. Jeżeli w urządzeniu są zainstalowane jakiekolwiek aplikacje, zobaczysz je tutaj.
3. Przejdź do odpowiedniej aplikacji, na przykład AXIS Object Analytics.
4. Skonfiguruj aplikację zgodnie z własnymi potrzebami.

Aktualizowanie aplikacji na urządzeniu Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Kliknij prawym przyciskiem myszy urządzenie i wybierz polecenie **Show updates (Pokaż aktualizacje)**. Jeżeli którekolwiek aplikacje mogą zostać zaktualizowane, zostanie wyświetlona lista dostępnych aktualizacji.
3. Pobierz plik aktualizacji.
4. Kliknij opcję **How to update (Procedura aktualizacji)** i postępuj zgodnie z instrukcjami.

Ponowne uruchamianie urządzenia Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Kliknij prawym przyciskiem myszy urządzenie i wybierz polecenie **Restart device (Uruchom ponownie urządzenie)**.

Kopiowanie adresu IP urządzenia Axis

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)**.
2. Kliknij prawym przyciskiem myszy urządzenie i wybierz polecenie **Copy device address (Kopiuj adres urządzenia)**.

Wykonanie automatyzacji

Tworzenie akcji dla urządzeń Axis

Wtyczka serwera zdarzeń

Wtyczka serwera zdarzeń w aplikacji AXIS Optimizer pozwala tworzyć niestandardowe zdarzenia dla urządzeń Axis. Używanie wspólnie silnika reguł systemu XProtect i wtyczki Serwer zdarzeń otwiera na przykład następujące możliwości:

- Wykonywanie niestandardowej akcji, gdy operator kliknie przycisk w aplikacji Smart Client. Przykład konfiguracji pokazano w temacie *Osuszanie wielu kamer jednym kliknięciem, on page 15*.
- Wykonywanie czynności bez udziału człowieka (automatyzacja). Przykład konfiguracji pokazano w temacie *Automatyczne wyłączanie masek prywatności w wielu kamerach, on page 18*.

Wtyczka Serwer zdarzeń składa się z dwóch części:

- Osobna wtyczka działająca na serwerze zdarzeń. Powoduje ona wypełnianie silnika reguł nowymi akcjami.
- Strona zatytułowana **Axis actions (Akcje Axis)** na serwerze zarządzania, gdzie można tworzyć nowe predefiniowane ustawienia akcji.

Niestandardowe akcje dostępne dla urządzeń Axis: Uruchamianie elementu sterującego operatora, Włączanie/wyłączanie radaru, Uruchamianie wywołania interkomu i Osuszanie kamery (szybkie osuszanie/wycieraczka).

Wtyczka Serwer zdarzeń jest dołączona w aplikacji AXIS Optimizer. W systemie wielokomputerowym należy zainstalować aplikację AXIS Optimizer na komputerach klienta zarządzania i serwera zdarzeń.

Instalowanie wtyczki Serwer zdarzeń

Wtyczka Serwer zdarzeń to opcjonalny składnik zawarty w pakiecie instalatora programu AXIS Optimizer. Można ją instalować tylko na serwerze zdarzeń systemu zarządzania materiałem wizyjnym (VMS). Jeżeli wymogi są spełnione, monit o zainstalowanie wtyczki Serwer zdarzeń zostanie wyświetlony podczas pracy instalatora aplikacji AXIS Optimizer.

Uwaga

Serwer zdarzeń systemu VMS będzie wymagał krótkiego ponownego uruchomienia podczas instalacji, a czasem również podczas aktualizowania aplikacji AXIS Optimizer. Zostanie wyświetlone odpowiednie powiadomienie.

Osuszanie wielu kamer jednym kliknięciem

Wtyczka Serwer zdarzeń umożliwia konfigurowanie niestandardowych reguł, które bardzo ułatwiają pracę operatorom. W tym przykładzie pokażemy, jak osuszyć wszystkie kamery w danym obszarze poprzez kliknięcie nakładkowego przycisku.



Uwaga

Wymagania

- Aplikacja AXIS Optimizer w wersji 4.0 lub nowszej na serwerze zdarzeń oraz aplikacja Management Client
- Co najmniej jedną kamerę z funkcją szybkiego osuszania lub wycieraczką, np. AXIS z serii Q86, Q87 lub Q61

1. Dodaj zdarzenie zdefiniowane przez użytkownika:
   1.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)**, a następnie prawym przyciskiem myszy kliknij opcję **User-defined Event (Zdarzenie zdefiniowane przez użytkownika)**.
   1.2. Wybierz opcję **Add User-defined Event (Dodaj zdarzenie zdefiniowane przez użytkownika)** i wprowadź nazwę, w tym przykładzie „Osuszanie wszystkich kamer".
2. Utwórz nową regułę:
   2.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)** i kliknij prawym przyciskiem myszy opcję **Rules (Reguły)**.
   2.2. Kliknij przycisk **Add Rule (Dodaj regułę)** i wprowadź nazwę, w tym przykładzie „Reguła Osuszanie wszystkich kamer".
   2.3. Wybierz **Perform an action on <event>** (Wykonaj działanie po wystąpieniu zdarzenia).
   2.4. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **event (zdarzenie)**.
   2.5. Wybierz kolejno opcje **Events > External Events > User-defined Events (Zdarzenia > Zdarzenia zewnętrzne > Zdarzenia zdefiniowane przez użytkownika)** i kliknij pozycję **Osuszanie wszystkich kamer**.
   2.6. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3: Actions** (Krok 3: działania).
   2.7. Wybierz działanie **Axis: Dry <camera>** (Axis: osusz kamerę).
   2.8. W polu **Edit the rule description** (Edytuj opis reguły) kliknij opcję **Axis: Dry camera** (Axis: osusz kamerę).
   2.9. W oknie **Select Triggering Devices (Wybierz urządzenia wyzwalające)** zaznacz opcję **Select devices (Wybierz urządzenia)** i kliknij przycisk **OK**.
   2.10. Zaznacz urządzenia, które mają wyzwalać akcję, a następnie kliknij kolejno przyciski **OK** i **Finish (Zakończ)**.
3. W aplikacji Smart Client dodaj zdarzenie zdefiniowane przez użytkownika jako nakładkowy przycisk w widoku mapy lub obrazu filmowego.
4. Kliknij nakładkowy przycisk i sprawdź, czy reguła działa zgodnie z oczekiwany sposób.

Włączanie automatycznego regulowania ostrości jednym kliknięciem dla wielu kamer

Wtyczka Serwer zdarzeń umożliwia konfigurowanie niestandardowych reguł, które bardzo ułatwiają pracę operatorom. W tym przykładzie pokażemy sposób włączania automatycznej regulacji ostrości jednym kliknięciem dla wszystkich kamer.

Uwaga

Wymagania

- Aplikację AXIS Optimizer w wersji 4.1 lub nowszej na serwerze zdarzeń i kliencie zarządzania
- Jedna lub kilka kamer obsługujących automatyczne ustawianie ostrości

1. Dodaj zdarzenie zdefiniowane przez użytkownika:
   1.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)**, a następnie prawym przyciskiem myszy kliknij opcję **User-defined Event (Zdarzenie zdefiniowane przez użytkownika)**.
   1.2. Wybierz opcję **Add User-defined Event (Dodaj zdarzenie zdefiniowane przez użytkownika)** i wprowadź nazwę, w tym przypadku „Automatyczna regulacja ostrości".
2. Utwórz nową regułę:
   2.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)** i kliknij prawym przyciskiem myszy opcję **Rules (Reguły)**.
   2.2. Wybierz opcję **Add Rule (Dodaj regułę)** i wprowadź nazwę, w tym przykładzie „Przeprowadzenie automatycznej regulacji ostrości".

2.3. Wybierz **Perform an action on <event>** (Wykonaj działanie po wystąpieniu zdarzenia).

2.4. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **event (zdarzenie)**.

2.5. Wybierz kolejno opcje **Events > External Events > User-defined Events (Zdarzenia > Zdarzenia zewnętrzne > Zdarzenia zdefiniowane przez użytkownika)** i kliknij pozycję **Automatyczna regulacja ostrości**. Kliknij **OK**.

2.6. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3: Actions** (Krok 3: działania).

2.7. Wybierz działanie **Axis: Run autofocus on <camera>** (Axis: uruchom automatyczne ogniskowanie w kamerze).

2.8. W polu **Edit the rule description** (Edytuj opis reguły) kliknij opcję **Axis: Run autofocus on camera** (Axis: uruchom automatyczne ogniskowanie w kamerze).

2.9. W oknie **Select Triggering Devices (Wybierz urządzenia wyzwalające)** zaznacz opcję **Select devices (Wybierz urządzenia)** i kliknij przycisk **OK**.

2.10. Zaznacz urządzenia, które mają wyzwalać akcję, a następnie kliknij kolejno przyciski **OK** i **Finish (Zakończ)**.

3. W aplikacji Smart Client dodaj zdarzenie zdefiniowane przez użytkownika „Automatyczna regulacja ostrości" jako nakładkowy przycisk w widoku mapy lub obrazu filmowego.

4. Kliknij nakładkowy przycisk i sprawdź, czy reguła działa zgodnie z oczekiwany sposób.

Wyzwalanie kilku syren stroboskopowych za pomocą jednego kliknięcia

Wtyczka Serwer zdarzeń umożliwia konfigurowanie niestandardowych reguł, które bardzo ułatwiają pracę operatorom. W tym przykładzie znajdują się instrukcje aktywacji kilku syren stroboskopowych jednym kliknięciem w programie Smart Client.

Uwaga

Wymagania

- Aplikację AXIS Optimizer w wersji 4.4 lub nowszej na serwerze zdarzeń i kliencie zarządzania
- Co najmniej jedną syrenę stroboskopową Axis
- Wyjście 1 sygnalizatora akustyczno-optycznego Axis włączone i dodane do urządzeń wyjściowych w aplikacji Management Client

1. Utwórz zdarzenie zdefiniowane przez użytkownika:

1.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)**, a następnie prawym przyciskiem myszy kliknij opcję **User-defined Event (Zdarzenie zdefiniowane przez użytkownika)**.

1.2. Wybierz **Add User-defined Event (Dodaj zdarzenie zdefiniowane przez użytkownika** i wprowadź nazwę, na przykład „Trigger all strobe sirens" („Wyzwalanie wszystkich syren stroboskopowych").

2. Włącz funkcję Device assistant (Asystent urządzenia) i utwórz profile syreny stroboskopowej:

2.1. Otwórz menu **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzenia)**.

2.2. Wybierz syrenę stroboskopową. Zostanie wyświetlona strona internetowa syreny stroboskopowej.

2.3. Przejdź do menu **Profiles** (Profile) i kliknij **Add profile** (Dodaj profil).

2.4. Ustaw reakcję syreny stroboskopowej na wyzwolenie przez operatora syren stroboskopowych w aplikacji Smart Client.

2.5. Utwórz te same profile w pozostałych syrenach stroboskopowych. W przypadku każdego urządzenia trzeba użyć tej samej nazwy profilu.

3. W menu Axis actions (Akcje Axis) utwórz prepozycję akcji:

3.1. Otwórz menu **Site Navigation > Rules and Events > Axis actions** (Nawigacja po witrynie > Reguły i zdarzenia > Działania Axis).

3.2. Kliknij polecenie **Add new preset (Dodaj nową prepozycję)**.

3.3. Otwórz menu **Select strobe siren (Wybierz syrenę stroboskopową)** i kliknij opcję **Strobe siren (Syrena stroboskopowa)**.

3.4. Wybierz syreny stroboskopowe, których chcesz używać, i kliknij przycisk **OK**.
Zostanie wyświetlona lista profili syren stroboskopowych.

3.5. Wybierz profil syreny stroboskopowej utworzony przez siebie w poprzednim kroku. Gotowe ustawienia działania zostaną automatycznie zapisane.

3.6. Naciśnij klawisz F5, aby odświeżyć konfigurację serwera. Teraz możesz rozpocząć korzystanie z utworzonej przez siebie nowej prepozycji akcji.

4. Utwórz regułę:

4.1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)** i kliknij prawym przyciskiem myszy opcję **Rules (Reguły)**.

4.2. Wybierz opcję **Add Rule (Dodaj regułę)** i wprowadź nazwę, np. „Trigger all strobe sirens rule" („Reguła wyzwalania wszystkich syren stroboskopowych").

4.3. Wybierz **Perform an action on <event>** (Wykonaj działanie po wystąpieniu zdarzenia).

4.4. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **event (zdarzenie)**.

4.5. Wybierz kolejno opcje **Events > External Events > User-defined Events (Zdarzenia > Zdarzenia zewnętrzne > Zdarzenia zdefiniowane przez użytkownika)** i kliknij pozycję **Trigger all strobe sirens (Wyzwalaj wszystkie syreny stroboskopowe)**.

4.6. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3**: Actions (Krok 3: działania).

4.7. Wybierz działanie **Axis: Run a profile on a strobe siren: <preset>** (Axis: uruchom profil w sygnalizatorze akustyczno-optycznym: gotowe ustawienie).

4.8. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **preset (prepozycja)**.

4.9. Wybierz prepozycje, których chcesz używać.

4.10. Kliknij przycisk **Next (Dalej)** i **Finish (Zakończ)**.

5. W aplikacji Smart Client dodaj zdarzenie zdefiniowane przez użytkownika jako nakładkowy przycisk w widoku mapy lub obrazu filmowego.

6. Kliknij nakładkowy przycisk i sprawdź, czy reguła działa zgodnie z oczekiwany sposób.

Automatyczne wyłączanie masek prywatności w wielu kamerach

Wtyczka Serwer zdarzeń umożliwia automatyzację pewnych działań. W tym przykładzie pokażemy, jak spowodować automatyczne wyłączanie masek prywatności w wielu kamerach w reakcji na wystąpienie zdarzenia analitycznego. W przykładzie zdarzenie polega na tym, że ludzie lub pojazdy wkraczają do obszaru, w którym normalnie nie powinni się znajdować. Chcemy automatycznego wyłączania masek prywatności, aby lepiej poznać obraz sytuacji.



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

Proces:

1. *Konfigurowanie scenariusza analizy, on page 19* w aplikacji AXIS Object Analytics (lub innej preferowanej aplikacji analitycznej)
2. *Dodawanie elementów sterujących operatora do odpowiednich kamer, on page 19*
3. *Tworzenie gotowych ustawień działań, on page 19*

4. *Tworzenie reguły wyłączania masek prywatności w reakcji na wystąpienie zdarzenia analitycznego, on page 19*
5. *Tworzenie reguły ponownego włączania masek prywatności, on page 20*
6. *Testowanie reguły, on page 20* i sprawdź, czy wszystko działa zgodnie z oczekiwaniami.

Uwaga

Wymagania

- Aplikacja AXIS Optimizer w wersji 4.0 lub nowszej na serwerze zdarzeń oraz aplikacja Management Client
- Kamery z systemem operacyjnym AXIS OS 7.40 lub nowszym
- Kamery zdolne generować zdarzenia, w tym przykładzie kamera z oprogramowaniem AXIS Object Analytics

Konfigurowanie scenariusza analizy

1. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)** i odszukaj urządzenie z funkcjami analitycznymi, których chcesz użyć.
2. Kliknij przycisk **Applications (Aplikacje)** i utwórz scenariusz analizy, który będzie inicjował akcję.
3. Wybierz kolejno opcje **Devices > Cameras (Urządzenia > Kamery)** i znajdź kamerę, dla której utworzono scenariusz analizy.
4. W oknie **Properties (Właściwości)** kliknij kolejno opcje **Events > Add (Zdarzenia > Dodaj)**.
5. Wybierz zdarzenie sterujące, w tym przykładzie „Object Analytics: Event test Rising (Analiza obiektów: Test zdarzenia narastająco)", i kliknij przycisk **OK**.
6. Kliknij przycisk **Add (Dodaj)** i wybierz zdarzenie sterujące „Object Analytics: Event test Failing (Analiza obiektów: Test zdarzenia opadająco)". Następnie kliknij przycisk **OK**.
7. Kliknij przycisk **Save (Zapisz)**.

Dodawanie elementów sterujących operatora do odpowiednich kamer

1. Wybierz kolejno opcje **AXIS Optimizer > Operator controls (AXIS Optimizer > Elementy sterujące operatora)** i otwórz bibliotekę elementów sterujących.
2. W oknie **Configuration (Konfiguracja)** zaznacz odpowiedni folder oraz aktywuj elementy sterujące **Turn off privacy mask (Wyłączanie maski prywatności)** i **Turn on privacy mask (Włączanie maski prywatności)**.

Tworzenie gotowych ustawień działań

1. Wybierz kolejno opcje **Rules and Events > Axis actions (Reguły i zdarzenia > Akcje Axis)** i kliknij przycisk **Add new preset (Dodaj nową prepozycję)**.
2. Kliknij pozycję **Cameras (Kamery)** i wybierz odpowiednie kamery. W tym przykładzie: AXIS P1375 i AXIS Q6075-E. Następnie wybierz element **Turn on privacy mask** (Włącz maskę prywatności).
3. Kliknij kolejno opcje **Add new preset > Cameras (Dodaj nową prepozycję > Kamery)** i wybierz odpowiednie kamery. W tym przykładzie: AXIS P1375 i AXIS Q6075-E. Następnie wybierz element **Turn off privacy mask** (Wyłącz maskę prywatności).

Tworzenie reguły wyłączania masek prywatności w reakcji na wystąpienie zdarzenia analitycznego

1. Wybierz kolejno opcje **Site Navigation > Rules and Events (Nawigacja po witrynie > Reguły i zdarzenia)** i kliknij prawym przyciskiem myszy opcję **Rules (Reguły)**.
2. Kliknij przycisk **Add Rule (Dodaj regułę)** i wprowadź nazwę, w tym przykładzie „Wyłączanie maski prywatności przy analizie".
3. Wybierz **Perform an action on <event>** (Wykonaj działanie po wystąpieniu zdarzenia).

4. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **event (zdarzenie)**. Kliknij kolejno **Devices > Configurable Events** (Urządzenia > Konfigurowane zdarzenia) i wybierz **Object Analytics: Event test Rising** (Analiza obiektów: test zdarzenia wznoszący).
5. W polu **Edit the rule description (Edytuj opis reguły)** zaznacz urządzenie, w tym przykładzie AXIS P1375.
6. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3: Actions** (Krok 3: działania).
7. Wybierz działanie **Axis: Run operator control: <preset>** (Axis: uruchom sterowanie przez operatora: gotowe ustawienie).
8. W polu **Edit the rule description (Edytuj opis reguły)** kliknij opcję **preset (prepozycja)**. Następnie dodaj docelową akcję **Turn on privacy mask on 2 cameras (Wyłączanie maski prywatności w 2 kamerach)** i kliknij przycisk **OK**.
9. Kliknij przycisk **Finish (Zakończ)**.

Tworzenie reguły ponownego włączania masek prywatności

1. Kliknij przycisk **Add Rule (Dodaj regułę)** i wprowadź nazwę, w tym przykładzie „Włączanie maski prywatności po zakończeniu analizy".
2. Wybierz **Perform an action on <event>** (Wykonaj działanie po wystąpieniu zdarzenia).
3. W sekcji **Edit the rule description (Edytuj opis reguły)** kliknij opcję **event (zdarzenie)**. Kliknij kolejno **Devices > Configurable Events** (Urządzenia > Konfigurowane zdarzenia) i wybierz **Object Analytics: Event test Falling** (Analiza obiektów: test zdarzenia opadający).
4. W sekcji **Edit the rule description (Edytuj opis reguły)** zaznacz urządzenie, w tym przykładzie AXIS P1375.
5. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3: Actions** (Krok 3: działania).
6. Wybierz działanie **Axis: Run operator control: <preset>** (Axis: uruchom sterowanie przez operatora: gotowe ustawienie).
7. W sekcji **Edit the rule description (Edytuj opis reguły)** kliknij opcję **preset (prepozycja)**. Następnie dodaj docelową akcję **Turn on privacy mask on 2 cameras (Włączanie maski prywatności w 2 kamerach)** i kliknij przycisk **OK**.
8. Kliknij przycisk **Finish (Zakończ)**.

Testowanie reguły

1. Wybierz kolejno opcje **AXIS Optimizer > Device assistant (AXIS Optimizer > Asystent urządzeń)** i odszukaj urządzenie z funkcjami analitycznymi użytymi do utworzenia automatyzacji. W tym przykładzie jest to AXIS P1375.
2. Otwórz odnośny scenariusz i kliknij przycisk **Test alarm (Testuj alarm)**.

Aktywowanie syreny stroboskopowej po wykryciu ruchu przez kamerę

Za pomocą wtyczki serwera można konfigurować niestandardowe reguły automatyzujące działania. W tym przykładzie zostały przedstawione instrukcje konfiguracji automatycznego uruchamiania syren stroboskopowych po wykryciu ruchu przez kamerę.

Uwaga

Wymagania

- Aplikację AXIS Optimizer w wersji 4.4 lub nowszej na serwerze zdarzeń i kliencie zarządzania
- Co najmniej jedną syrenę stroboskopową Axis
- Wyjście 1 sygnalizatora akustyczno-optycznego Axis włączone i dodane do urządzeń wyjściowych w aplikacji Management Client.
- W wersjach starszych niż VMS 2022 R2 akcje Axis nie mogą służyć do zatrzymywania. W takich wersjach należy utworzyć dwie osobne reguły do uruchamiania i zatrzymywania syreny stroboskopowej.

1. Utwórz profile syreny stroboskopowej:
   1.1. Otwórz menu **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzenia)**.
   1.2. Przejdź do sekcji **Axis output devices (Urządzenia wyjściowe Axis)** i wybierz syrenę stroboskopową. Zostanie wyświetlona strona internetowa syreny stroboskopowej.
   1.3. Przejdź do menu **Profiles** (Profile) i kliknij **Add profile** (Dodaj profil).
   1.4. Dla wszystkich syren koniecznie wybierz tę samą nazwę profilu.
   1.5. Ustaw reakcję syreny stroboskopowej po wykryciu ruchu.
2. Utwórz predefiniowane akcje uruchamiania i zatrzymywania:
   2.1. Otwórz menu **Site Navigation > Rules and Events > Axis actions** (Nawigacja po witrynie > Reguły i zdarzenia > Działania Axis).
   2.2. Aby utworzyć predefiniowaną akcję uruchamiania, przejdź do sekcji **Strobe siren (Syrena stroboskopowa)** i kliknij przycisk **Add new preset (Dodaj nową prepozycję)**.
   2.3. Otwórz menu **Select strobe siren (Wybierz syrenę stroboskopową)** i kliknij opcję **Strobe siren (Syrena stroboskopowa)**.
   2.4. Wybierz z listy jedną lub kilka syren stroboskopowych.
   2.5. Z listy wybierz utworzony wcześniej profil syreny. Gotowe ustawienia działania zostaną automatycznie zapisane.
   2.6. Aby utworzyć predefiniowaną akcję zatrzymywania, kliknij przycisk **Add new preset (Dodaj nową prepozycję)**.
   2.7. Otwórz menu **Select strobe siren (Wybierz syrenę stroboskopową)** i kliknij opcję **Strobe siren (Syrena stroboskopowa)**.
   2.8. Z listy wybierz te same syreny stroboskopowe, jak wybrane dla predefiniowanej akcji uruchamiania.
   2.9. Przejdź do sekcji **Select action (Wybierz akcję)** i zaznacz wartość **Stop (Zatrzymanie)**.
   2.10. Zaznacz ten sam profil syreny, jak utworzony dla akcji uruchamiania. Gotowe ustawienia działania zostaną automatycznie zapisane.
   2.11. Kliknij opcję **click to refresh** (kliknij, aby odświeżyć) lub naciśnij klawisz F5, aby odświeżyć konfigurację serwera.
3. Utwórz regułę:
   3.1. Otwórz menu **Site Navigation > Rules and Events > Rules** (Nawigacja po witrynie > Reguły i zdarzenia > Reguły).
   3.2. Kliknij prawym przyciskiem myszy pozycję **Rules** (Reguły), wybierz polecenie **Add Rule** (Dodaj regułę) i wprowadź nazwę.
   3.3. W obszarze **Edit the rule description** (Edytuj opis reguły) kliknij opcję **event** (zdarzenie).
   3.4. Otwórz menu **Devices > Predefined Events** (Urządzenia > Wstępnie zdefiniowane zdarzenia) i wybierz **Motion Started** (Aktywowane przez ruch).
   3.5. W sekcji **Edit the rule description** (Edytuj opis reguły) kliknij **devices/recording_server/management_server**.
   3.6. Wybierz kamerę, która będzie włączała syreny stroboskopowe.
   3.7. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3**: Actions (Krok 3: działania).
   3.8. Wybierz działanie **Axis: Start or stop a profile on a strobe siren: <preset>** (Axis: uruchom lub zatrzymaj profil w sygnalizatorze akustyczno-optycznym: gotowe ustawienie).
   3.9. W sekcji **Edit the rule description** (Edytuj opis reguły) kliknij opcję **preset** (gotowe ustawienie).
   3.10. Zaznacz utworzoną wcześniej predefiniowaną akcję uruchamiania.
   3.11. Kliknij przycisk **Dalej** i wybierz opcję **Perform stop action on <event>** (Wykonaj działanie zatrzymania po zdarzeniu).

3.12. Kliknij przycisk **Dalej** i wybierz opcję **Axis: Start or stop a profile on strobe siren: <event>** (Axis: uruchom lub zatrzymaj profil w sygnalizatorze akustyczno-optycznym: zdarzenie).

3.13. W sekcji **Edit the rule description** (Edytuj opis reguły) kliknij opcję **preset** (gotowe ustawienie).

3.14. Zaznacz utworzoną wcześniej predefiniowaną akcję zatrzymywania.

3.15. Kliknij przycisk **Zakończ**.

4. Sprawdź, czy syreny stroboskopowe działają poprawnie po wykryciu ruchu przez kamerę.

Odtwarzanie klipów audio na głośnikach lub w strefie głośnika, gdy kamera wykryje ruch



Za pomocą wtyczki serwera można konfigurować niestandardowe reguły automatyzujące działania zwane predefiniowanymi akcjami. W tym przykładzie zostały przedstawione instrukcje automatycznego odtwarzania klipu dźwiękowego z głośnika lub w strefie głośników, gdy kamera wykryje ruch.

Uwaga

Wymagania

- Aplikacja AXIS Optimizer w wersji 4.6 lub nowszej na serwerze zdarzeń oraz aplikacja Management Client.
- Co najmniej jeden dedykowany głośnik Axis lub co najmniej jednio urządzenie Axis wyposażone we wbudowane głośniki.
- Do odtworzenia pliku fonicznego w strefie głośnikowej wymagany jest prawidłowo skonfigurowany system AXIS Audio Manager Edge lub AXIS Audio Manager Pro. Więcej informacji o konfiguracji obu systemów, p. sekcja *Tryb konfiguracji, on page 31*.

1. Przesyłanie klipu audio:

1.1. W trybie systemu AXIS Audio Manager Edge lub Legacy klipy audio, które chcesz przesłać do głośników, umieść w domyślnym folderze **C:\Users\Public\Documents\AXIS Optimizer for Milestone XProtect - Audio Clips**.
W trybie AXIS Audio Manager Pro prześlij klipy audio za pośrednictwem interfejsu internetowego programu AXIS Audio Manager Pro.

1.2. W aplikacji Management Client przejdź do **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po obiekcie > AXIS Optimizer > Menedżer głośników) i wybierz głośnik, grupę urządzeń lub strefę głośnikową z listy.

Uwaga

Więcej informacji o wyborze trybu zarządzania głośnikami, p. sekcja *Tryb konfiguracji, on page 31*.

1.3. Przejdź do **Audio clips** (Klipy audio) i kliknij **+** przed klipem, który chcesz przesłać.

1.4. W trybie Legacy powtórz kroki 1.2 – 1.3 w zakresie każdego głośnika, przez który chcesz odtworzyć klip audio. Sprawdź, czy do każdego głośnika przesłałeś ten sam plik foniczny.

2. Aby utworzyć predefiniowane ustawienia akcji umożliwiające odtworzenie klipu audio na głośniku lub w strefie głośnika:

2.1. Przejdź do **Site Navigation** > **Rules and Events** > **Axis actions** (Nawigacja po obiekcie > Reguły i zdarzenia > Działania Axis).

2.2. Aby utworzyć predefiniowane działanie, przejdź do sekcji **Audio clips** (Klipy audio) i kliknij **Add new preset** (Dodaj nowe gotowe ustawienie).

2.3. W trybie AXIS Audio Manager Edge lub AXIS Audio Manager Pro przejdź do **Select playback destination** (Wybierz miejsce odtwarzania).

W trybie Legacy przejdź do **Select speaker** (Wybierz głośnik).

2.4. Wybierz głośnik lub strefę głośnika.

2.5. Z listy wybierz klip audio przesłany w kroku 1. Gotowe ustawienia działania zostaną automatycznie zapisane.

2.6. W trybie AXIS Audio Manager Pro przejdź do **Select visual profile** (Wybierz profil wizualny) i skonfiguruj profil wizualny oraz tekst.

Uwaga

Wybierz **Default** (Domyślne) na liście profili wizualnych, aby po wyzwoleniu działania związanego z klipem audio na serwerze AXIS Audio Manager Pro użyć domyślnego zachowania profilu wizualnego.

2.7. Kliknij opcję **odświeżania strony** lub naciśnij klawisz F5, aby odświeżyć konfigurację serwera.

3. Aby utworzyć regułę:

3.1. Przejdź do **Site Navigation** > **Rules and Events** > **Rules** (Nawigacja po obiekcie > Reguły i zdarzenia > Reguły).

3.2. Kliknij prawym przyciskiem myszy pozycję **Rules** (Reguły), wybierz polecenie **Add Rule** (Dodaj regułę) i wprowadź nazwę.

3.3. W obszarze **Edit the rule description** (Edytuj opis reguły) kliknij opcję **event** (zdarzenie).

3.4. Przejdź do **Devices** > **Predefined Events** (Urządzenia > Wstępnie zdefiniowane zdarzenia) i wybierz **Motion Started** (Aktywowane przez ruch).

3.5. W sekcji **Edit the rule description** (Edytuj opis reguły) kliknij **devices/recording_server/management_server**.

3.6. Wybierz kamerę, która ma wyzwalać prepozycje lub klip audio.

3.7. Klikaj **Dalej**, aż dotrzesz do punktu **Step 3**: Actions (Krok 3: działania).

3.8. Wybierz działanie **Axis: Play audio clip: <preset>** (Axis: odtwarzaj klip audio: gotowe ustawienie)).

3.9. W sekcji **Edit the rule description** (Edytuj opis reguły) kliknij opcję **preset** (gotowe ustawienie).

3.10. Wybierz prepozycję utworzoną przez siebie w poprzednim kroku.

3.11. Kliknij przycisk **Zakończ**.

4. Sprawdź, po wykryciu ruchu przez kamerę jest prawidłowo odtwarzany klip audio.

Rozwiązywanie problemów z regułą

Jeżeli reguła nie działa, najpierw w komunikatach serwera zdarzeń sprawdź, czy w ogóle jest uruchomiona usługa zdarzeń.

Można również sprawdzić dzienniki aplikacji AXIS Optimizer na serwerze zdarzeń. Jeżeli jest dostępna aplikacja Management Client lub Smart Client, to właśnie w nich można włączyć dzienniki i je zapisywać.

Centralnie zarządzanie listami tablic rejestracyjnych

Funkcja menedżera list w programie AXIS Optimizer umożliwia centralne zarządzanie listami tablic rejestracyjnych wszystkich kamer równocześnie. Listy elementów dozwolonych, blokowanych i niestandardowych można tworzyć bezpośrednio w systemie VMS i tam nimi zarządzać. System obsługuje łączenie list. Oznacza to, że można mieć globalną listę mającą zastosowanie do wszystkich kamer w systemie oraz listy lokalne, które dotyczą konkretnych kamer.

Centralne zarządzanie listami przydaje się na przykład wtedy, gdy trzeba zautomatyzować wjeżdżanie na parking i wyjeżdżanie z parkingu albo otrzymywać alarm, gdy system zarejestruje określoną tablicę rejestracyjną.

Aby tworzyć i edytować listy, trzeba być administratorem. Uprawnienia odczytu i edycji można przyznać również innym rolom, p. *Konfigurowanie uprawnień do list, on page 24*.

Tworzenie listy

Uwaga

Wymagania

- Aplikacja AXIS License Plate Verifier w wersji 1.8 lub nowszej uruchomiona na kamerach
- a jeśli chcesz utworzyć listy niestandardowe, potrzebujesz aplikacji AXIS License Plate Verifier w wersji 2.0 lub nowszej

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > AXIS Optimizer > License plate lists (Nawigacja po witrynie > AXIS Optimizer > Listy tablic rejestracyjnych)**.
2. Zaznacz kamery, które chcesz dodać do list elementów dozwolonych, blokowanych i niestandardowych.
3. (Opcjonalnie) Dodaj role użytkowników uprawnione do wyświetlania i edytowania list dozwolonych, blokowanych i niestandardowych.
4. Dodaj tablice rejestracyjne do listy dozwolonych, blokowanych i niestandardowych.
   Można również zaimportować istniejące listy tablic rejestracyjnych.
   Zmiana statusu listy na **Synchronized (Zsynchronizowana)** oznacza, że lista została wysłana do wybranych kamer.

Konfigurowanie uprawnień do list

Można wskazać role użytkowników uprawnione do edytowania list elementów dozwolonych, blokowanych i niestandardowych. Przydaje się to na przykład w sytuacjach, gdy administrator utworzył listy, ale operatorzy powinni mieć możliwość dodawania gości zgodnie z bieżącymi potrzebami.

W aplikacji Management Client

Wszystkie uprawnienia do wyświetlania i edytowania list można konfigurować indywidualnie dla każdej listy.

1. Przejdź do menu **Security > Roles (Zabezpieczenia > Role)** i wybierz rolę.
2. Przejdź do karty **AXIS Optimizer**.
3. Przejdź do pozycji **Role settings** > **AXIS Optimizer** > **License plate lists** (Ustawienia ról > AXIS Optimizer > Listy tablic rejestracyjnych).
4. Zaznacz opcję **Read** (Odczyt) w polu **License plate lists (node)** (Listy tablic rejestracyjnych (węzeł)).
5. Wybierz listę w pozycji **License plate lists** (Listy tablic rejestracyjnych) i zaznacz **Edit license plates** (Edytuj tablice rejestracyjne).
   - Wersje starsze niż XProtect 2023 R2 można uzyskać, przechodząc do menu **MIP > AXIS Optimizer > AXIS Optimizer Security > License plate lists (MIP > AXIS Optimizer > Zabezpieczenia aplikacji AXIS Optimizer > Listy tablic rejestracyjnych)** i wybierając polecenie **Edit license plate lists (Edytuj tablic rejestracyjnych)**.

Edytowanie listy

W aplikacji Management Client

1. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > License plate lists (Nawigacja po witrynie > AXIS Optimizer > Listy tablic rejestracyjnych)**.
2. Zaznacz lokalizację, którą chcesz edytować.
3. Odpowiednio zaktualizuj listę **Cameras (Kamery)** lub **License plates (Tablice rejestracyjne)**.
   Zmiana statusu listy na **Synchronized (Zsynchronizowana)** oznacza, że zmiany zostały wysłane do wybranych kamer.

W aplikacji Smart Client

1. Przejdź do aplikacji *Axis license plates, on page 59* i kliknij przycisk **License plate lists (Listy tablic rejestracyjnych)**.

Jeśli nie widzisz karty, wybierz kolejno opcje **Settings > Axis search options (Ustawienia > Opcje wyszukiwania Axis)** i kliknij opcję **Show license plate tab (Pokaż kartę tablic rejestracyjnych)**.

2. Zaznacz lokalizację, którą chcesz edytować.
3. Dodaj tablice rejestracyjne do listy dozwolonych, blokowanych i niestandardowych.
   Można również zaimportować istniejące listy tablic rejestracyjnych.
   Zmiana statusu listy na **Synchronized (Zsynchronizowana)** oznacza, że lista została wysłana do wybranych kamer.

Importowanie listy

Listy można importować w kilka formatach tekstowych lub CSV.

- Dozwolony format tekstowy: jedna tablica rejestracyjna w każdym wierszu
- Dozwolone formaty CSV:
  - Jedna tablica rejestracyjna w każdym wierszu
  - Dwa pola: tablica rejestracyjna i data
  - Trzy pola: tablica rejestracyjna, właściciel i komentarz
  - Cztery pola: tablica rejestracyjna, właściciel, komentarz i ciąg „Active (Aktywna)" lub „Inactive (Nieaktywna)". (taki sam format, jak przy eksportowaniu listy)

W aplikacji Management Client

1. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > License plate lists (Nawigacja po witrynie > AXIS Optimizer > Listy tablic rejestracyjnych)**.
2. Zaznacz lokalizację, którą chcesz edytować.
3. Przejdź do sekcji **Allowed (Dozwolone)**, **Blocked (Zablokowane)** lub **Custom (Niestandardowe)**.
4. Kliknij pozycję ⋮, a następnie wybierz opcję **Import to allow list** (Importuj do listy dozwolonych), **Import to block list** (Importuj do listy blokowanych) lub **Import to custom list** (Importuj do listy niestandardowych).
5. W oknie dialogowym **Reset list (Resetuj listę)**:
   - Kliknij **Yes (Tak)**, aby usunąć wszystkie istniejące tablice rejestracyjne i dodać do listy tylko nowo zaimportowane tablice rejestracyjne.
   - Kliknij **No (Nie)**, aby scalić nowo zaimportowane tablice rejestracyjne z istniejącymi tablicami rejestracyjnymi na liście.

W aplikacji Smart Client

1. Przejdź do aplikacji *Axis license plates, on page 59* i kliknij przycisk **License plate lists (Listy tablic rejestracyjnych)**.
   Jeśli nie widzisz karty, wybierz kolejno opcje **Settings > Axis search options (Ustawienia > Opcje wyszukiwania Axis)** i kliknij opcję **Show license plate tab (Pokaż kartę tablic rejestracyjnych)**.
2. Zaznacz lokalizację, którą chcesz edytować.
3. Przejdź do sekcji **Allowed (Dozwolone)**, **Blocked (Zablokowane)** lub **Custom (Niestandardowe)**.
4. Kliknij pozycję ⋮, a następnie wybierz opcję **Import to allow list** (Importuj do listy dozwolonych), **Import to block list** (Importuj do listy blokowanych) lub **Import to custom list** (Importuj do listy niestandardowych).
5. W oknie dialogowym **Reset list (Resetuj listę)**:
   - Kliknij **Yes (Tak)**, aby usunąć wszystkie istniejące tablice rejestracyjne i dodać do listy tylko nowo zaimportowane tablice rejestracyjne.
   - Kliknij **No (Nie)**, aby scalić nowo zaimportowane tablice rejestracyjne z istniejącymi tablicami rejestracyjnymi na liście.

Eksportowanie listy

Uwaga

Aby wyeksportować listy tablic rejestracyjnych, trzeba mieć uprawnienia administratora.

W aplikacji Management Client

1. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > License plate lists (Nawigacja po witrynie > AXIS Optimizer > Listy tablic rejestracyjnych)**.
2. Zaznacz lokalizację, którą chcesz edytować.
3. Przejdź do sekcji **Allowed (Dozwolone)**, **Blocked (Zablokowane)** lub **Custom (Niestandardowe)**.
4. Kliknij pozycję ⋮, a następnie wybierz opcję **Export to allow list** (Eksportuj do listy dozwolonych), **Export to block list** (Eksportuj do listy blokowanych) lub **Export to custom list** (Eksportuj do listy niestandardowych).
   Wyeksportowana lista będzie miała format CSV i następujące cztery pola: tablica rejestracyjna, właściciel, komentarz i status Active (Aktywna) lub Inactive (Nieaktywna).

W aplikacji Smart Client

1. Przejdź do aplikacji *Axis license plates, on page 59* i kliknij przycisk **License plate lists (Listy tablic rejestracyjnych)**.
   Jeśli nie widzisz karty, wybierz kolejno opcje **Settings > Axis search options (Ustawienia > Opcje wyszukiwania Axis)** i kliknij opcję **Show license plate tab (Pokaż kartę tablic rejestracyjnych)**.
2. Zaznacz lokalizację, którą chcesz edytować.
3. Przejdź do sekcji **Allowed (Dozwolone)**, **Blocked (Zablokowane)** lub **Custom (Niestandardowe)**.
4. Kliknij pozycję ⋮, a następnie wybierz opcję **Export to allow list** (Eksportuj do listy dozwolonych), **Export to block list** (Eksportuj do listy blokowanych) lub **Export to custom list** (Eksportuj do listy niestandardowych).
   Wyeksportowana lista będzie miała format CSV i następujące cztery pola: tablica rejestracyjna, właściciel, komentarz i status Active (Aktywna) lub Inactive (Nieaktywna).

Tu się dowiesz więcej o listach

- W programie można utworzyć kilka lokalizacji.
- Każda lokalizacja jest powiązana z jedną lub kilkoma kamerami, na których zainstalowano aplikację AXIS License Plate Verifier.
- Każda lokalizacja jest skojarzona z jedną lub kilkoma rolami użytkowników w systemie VMS. Rola użytkownika decyduje, kto może czytać i edytować listy tablic rejestracyjnych.
- Wszystkie listy są przechowywane w bazie danych VMS.
- Dodanie kamery do lokalizacji powoduje zastąpienie tablic rejestracyjnych już istniejących w kamerze.
- Jeżeli ta sama kamera występuje w kilku lokalizacjach, kamera otrzyma sumę wszystkich list.
- Jeżeli ta sama tablica rejestracyjna znajduje się na kilku listach, obecność na liście „zablokowane" ma najwyższy priorytet, na liście „dozwolone" średni priorytet, a na liście „niestandardowe" najniższy priorytet.
- Dla każdej tablicy rejestracyjnej można dodać informacje o właścicielu pojazdu. Informacje te nie są jednak synchronizowane z kamerami.

Odpowiadanie na zdarzenia w czasie rzeczywistym

Używanie elementów sterujących urządzenia

Elementy sterujące operatora

Elementy sterujące operatora umożliwiają korzystanie z funkcji specyficznych dla kamery Axis bezpośrednio z aplikacji Smart Client. Dostępność funkcji zależy od modeli kamer w systemie oraz od ich parametrów technicznych. Oprócz elementów sterujących instalowanych fabrycznie można tworzyć własne. Można również wskazać, których elementów operator będzie miał prawo używać.

Oto kilka przykładów elementów sterujących operatora:

- Włączanie i wyłączanie wycieraczki
- Włączanie i wyłączanie ogrzewacza
- Włączanie i wyłączanie promiennika podczerwieni
- Focus recall
- Włączanie i wyłączanie trybu WDR
- Włączanie i wyłączanie elektronicznej stabilizacji obrazu (EIS)
- Włączanie i wyłączanie masek prywatności

Więcej informacji o elementach sterujących operatora specyficznych dla kamery można znaleźć w opisie produktu.

Dostęp do elementów sterujących operatora

Uwaga

Wymagania

- Urządzenia Axis z systemem operacyjnym AXIS OS 7.10, 7.40 lub nowszym. (wersje 7.20 i 7.30 nie obsługują elementów sterujących operatora).

1. W aplikacji Smart Client kliknij opcję **Live (Na żywo)** i przejdź do kamery Axis.
2. Kliknij przycisk i wybierz funkcję, której chcesz używać.

Zapisywanie obszaru ostrości kamery PTZ

Funkcja przywracania ostrości umożliwia zapisywanie obszarów ostrości, do których kamera PTZ będzie wracać automatycznie po dotarciu do danego fragmentu sceny. Jest to szczególnie przydatne w warunkach słabego oświetlenia, gdzie kamera normalnie miałaby problemy z wyostrzeniem.



1. W aplikacji Smart Client przesuń kamerę w miejsce, na które chcesz ustawić ostrość.

Uwaga

Podczas ustawiania obszaru ostrości warunki oświetleniowe muszą być dobre.

2. Wyostrz kamerę.
3. Wybierz opcję **Add Focus Recall Zone (Dodaj strefę przywracania ostrości)**.

Gdy później obrócisz lub pochylisz kamerę, po czym przesuniesz widok na dany obszar, kamera automatycznie przywróci ostrość skonfigurowaną wcześniej dla tego widoku. Nawet po przybliżeniu lub oddaleniu widoku kamera zachowa tę samą pozycję ostrości.

Jeżeli strefa jest niepoprawnie skonfigurowana, wybierz opcję **Remove Focus Recall Zone (Usuń strefę przywracania ostrości)**.

Automatyczne ustawianie ostrości w kamerze



W kamerach z funkcją autofokusu ostrość można regulować ręcznie i mechanicznie, tak aby obraz pozostawał zawsze wyostrzony na obszar zainteresowania mimo zmiany widoku.

Ustawianie autofokusa kamery PTZ

1. W aplikacji Smart Client wybierz widok kamery.
2. Kliknij przycisk , a następnie wybierz kolejno opcje **Set Focus > AF** (Ustaw ogniskowanie > Automatyczne ogniskowanie).
   Funkcja **Focus Control (Sterowanie ostrością)** umożliwia przybliżanie i oddalanie punktu ostrości:
   - Aby wykonać duży krok, kliknij duży pasek.
   - Aby dokonać niewielkiej zmiany, kliknij mały pasek.

Ustawianie autofokusa stałopozycyjnej kamery typu box lub kopułkowej

1. W aplikacji Smart Client wybierz widok kamery.
2. Kliknij przycisk i wybierz opcję **Autofocus** (Automatyczne ogniskowanie).

Włączanie szybkiego osuszania lub wycieraczki



Funkcja szybkiego osuszania pozwala kopułce strząsnąć z siebie nadmiar wilgoci. Kopułka wpada w drgania o wysokiej częstotliwości, co powoduje przerwanie napięcia powierzchniowego wody i odpadnięcie kropel. Dzięki temu kamera może rejestrować ostre obrazy nawet w deszczowej pogodzie.

Aby włączyć funkcję szybkiego osuszania

1. W aplikacji Smart Client wybierz widok kamery.
2. Kliknij przycisk , a następnie wybierz kolejno opcje **PTZ > Speed Dry** (PTZ > Szybkie osuszanie).

Ważne

Funkcja szybkiego osuszania jest dostępna tylko w kamerach AXIS z serii Q61.

Aby włączyć funkcję wycieraczki

Wycieraczka usuwa nadmiar wody i opad deszczu z obiektywów kamer pozycjonujących Axis.

1. W aplikacji Smart Client wybierz widok kamery.

2. Kliknij .

Ważne

Funkcja wycieraczki jest dostępna tylko w kamerach AXIS z serii Q86.

Pomiar temperatury punktowej



Jeżeli w systemie znajduje się kamera wyposażona w funkcję punktowego odczytu temperatury, można zmierzyć temperaturę bezpośrednio w widoku kamery. Kamery AXIS z funkcją punktowego odczytu temperatury to AXIS Q1961-TE, AXIS Q2101-E oraz AXIS Q2901-E.

1. Przejdź do aplikacji Smart Client i otwórz widok kamery wyposażonej w funkcję punktowego odczytu temperatury.
2. Aby zmierzyć temperaturę punktową, kliknij i wybierz :
   - **Measure spot temperature (Pomiar temperatury w punkcie)** w przypadku AXIS Q2901-E.
   - **Enable temperature spot meter (Włącz termometr w punkcie)** w przypadku AXIS Q1961-TE i AXIS Q2101-E.
3. Kliknij dowolny obszar w widoku, a zobaczysz aktualną temperaturę w punkcie.
   W przypadku modeli Q1961-TE i AXIS Q2101-E kliknij przycisk **Done (Gotowe)**.
4. W przypadku modeli AXIS Q1961-TE oraz AXIS Q2101-E temperatura zmierzona w punkcie będzie wyświetlana na obrazie, chyba że ustawienie to zostanie wyłączone:
   - Wybierz > **Disable temperature spot meter** (Wyłącz termometr w punkcie).

Uwaga

W przypadku stosowania zoomu cyfrowego wyniki pomiarów temperatury mogą być błędne.

Automatyczne przybliżanie i śledzenie ruchomego obiektu

Automatyczne śledzenie ruchu

Po włączeniu automatycznego śledzenia ruchu kamera automatycznie przybliża i śledzi poruszające się obiekty, na przykład pojazd lub osobę. Można wybrać obiekt do śledzenia ręcznie lub skonfigurować obszary wyzwalania, w których kamera będzie wykrywała poruszające się obiekty. Kiedy kamera nie śledzi obiektu, po 5 s powraca do położenia wyjściowego.

- Skonfiguruj obszary wyzwalające w interfejsie sieciowym kamery PTZ.
- W aplikacji Smart Client widać następujące elementy:
  - Czerwony kwadrat: śledzony obiekt.
  - Niebieskie strefy: obiekty, które nie są śledzone, ale mogą być, o ile wejdą do strefy wyzwalania lub zostaną kliknięte prawym przyciskiem myszy.

Konfigurowanie automatycznego śledzenia

Uwaga

Wymagania

- AXIS OS 12.0
- Co najmniej jedna kamera Axis obsługująca funkcję Autotracking 2, na przykład sieciowa kamera kopułkowa AXIS Q6075 PTZ Dome Network Camera

1. Upewnij się, że kamera i urządzenia dostarczające metadane są włączone.
2. Wybierz dla kamery opcję Metadata 1 (Metadane 1) i kliknij przycisk **Settings (Ustawienia)**.
3. Wybierz kolejno opcje **Metadata stream > Event data (Strumień metadanych > Dane zdarzeń)** i kliknij przycisk **Yes (Tak)**.
4. Kliknij przycisk **Save (Zapisz)**.
5. Skonfiguruj funkcję automatycznego śledzenia w interfejsie sieciowym kamery PTZ.

Włączanie i wyłączanie automatycznego śledzenia

1. W aplikacji Smart Client kliknij przycisk .
2. Wybierz opcję **Turn on autotracking (Włącz automatyczne śledzenie)** lub **Turn off autotracking (Wyłącz automatyczne śledzenie)**.

Uwaga

Jeżeli jest kilka opcji włączania / wyłączania automatycznego śledzenia, użyj ostatniej opcji na liście.

Ręczne uruchamianie automatycznego śledzenia

Umieszczenie kursora myszy nad obiektem spowoduje wypełnienie nakładki. Następnie kliknięcie prawym przyciskiem myszy spowoduje ustawienie tego obiektu jako celu i kamera zacznie go śledzić. Jeżeli obiektu nie będzie można już śledzić, kamera zresetuje się po 5 s.

Kliknięcie prawym przyciskiem myszy poza niebieskimi polami zatrzymuje automatyczne śledzenie.

Tworzenie niestandardowych elementów sterujących operatora

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Operator controls (Nawigacja po witrynie > AXIS Optimizer > Elementy sterujące operatora)**.
2. Wybierz urządzenie lub grupę urządzeń.
3. Kliknij polecenie **Add new control (Dodaj nowy element sterujący)**.
4. Wypełnij pola **Name (Nazwa)** i **Description (Opis)**.
5. Jeżeli elementy sterujące operatora mają być dostępne tylko dla użytkowników z uprawnieniami administracyjnymi, zaznacz opcję **Administrator**.
6. Dodaj adres URL oprogramowania VAPIX dla wybranego elementu sterującego.
   Przykład: Aby dodać do elementów sterujących operatora funkcję Defog on (Wł. kompensacja mgły), wpisz adres URL: `/axis-cgi/param.cgi?action=update&imageSource.IO.Sensor.Defog=on`.
   Więcej informacji na temat interfejsów API urządzeń sieciowych Axis można znaleźć .
7. Przejdź do aplikacji Smart Client i sprawdź, czy element sterujący operatora działa w oczekiwany sposób.

Konfigurowanie dostępu do elementów sterujących operatora

Można wskazać elementy sterujące operatora, do których operator będzie miał dostęp w aplikacji Smart Client.

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Operator controls (Nawigacja po witrynie > AXIS Optimizer > Elementy sterujące operatora)**.
2. Wybierz urządzenie lub grupę urządzeń.
3. Zaznacz elementy sterujące operatora, których operatorzy będą mogli używać w aplikacji Smart Client.

Interakcja za pośrednictwem głośników

Menedżer głośników

Menedżer głośników integruje urządzenia audio Axis z systemem VMS, umożliwiając w ten sposób dostęp do wszystkich funkcji tych urządzeń.

- Dostęp do głośników współpracujących z kamerą
  Podłączanie kamer do głośników lub grup głośników oraz dostęp do głośników z okna podglądu na żywo. Nie trzeba już szukać głośników ręcznie.
- Wysyłanie dźwięku do grupy głośników
  Wysłanie dźwięku do wielu głośników jednym kliknięciem.
- Zarządzanie klipami audio
  Można łatwo zarządzać klipami audio.
- Błyskawiczne interweniowanie w razie problemów z głośnikami
  Szybkie reagowanie na alarmy bez opuszczania Menedżera alarmów.
- Synchronizowanie dźwięku między głośnikami
  Aby używać systemu audio do odtwarzania muzyki w tle, warto skorzystać z Menedżera głośników, ponieważ pomoże on skonfigurować strefy na potrzeby synchronizowania dźwięku pomiędzy głośnikami (tylko w trybach AXIS Audio Manager Pro i Edge).

Tryby

Menedżer głośników obsługuje trzy różne tryby dostosowane do różnych konfiguracji głośników.

- Oprogramowanie **Pro** dla systemów AXIS Audio Manager Pro
  Kompleksowe rozwiązanie przeznaczone do obsługi dużych lub zaawansowanych systemów nagłośnieniowych. Obsługuje ponad 5000 głośników i ponad 500 stref oraz oferuje elastyczne opcje licencjonowania i instalacji. Jest zalecane w przypadku większych systemów lub dla użytkowników o bardziej zaawansowanych wymaganiach dotyczących harmonogramów.
- Oprogramowanie **Edge** dla systemów AXIS Audio Manager Edge
  Zoptymalizowane rozwiązanie umożliwiające zarządzanie nawet 200 głośnikami w 20 strefach. Jest wbudowane bezpośrednio w głośniki sieciowe Axis i nie wymaga żadnych serwerów ani dodatkowych licencji. Jest zalecane w przypadku mniejszych systemów, które nie wymagają zaawansowanego harmonogramu.
- **Starszy**
  Tryb zgodności wstecznej wykorzystuje natywną integrację z głośnikami do przesyłania dźwięku do grupy głośników lub wyzwalania klipów audio. Nie obsługuje przesyłania zsynchronizowanego. Jest zalecany w przypadku systemów wyposażonych w pojedyncze głośniki w sytuacji, gdy nie jest wymagane zsynchronizowane przesyłanie dźwięku.

Tryb konfiguracji

Przy pierwszym wejściu na tę stronę pojawi się monit z prośbą o wybranie trybu, ale zmiany trybu można dokonać w każdej chwili. Ustawienia konfiguracji wprowadzone w każdym trybie są niezależne od pozostałych, ale przy przełączaniu się między trybami są zachowywane.

1. Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników).
2. W części **Mode (Tryb)** kliknij aktualnie wybrany tryb, a następnie wybierz żądany tryb w wyskakującym oknie.
3. Kliknij **Switch mode (Przełącz tryb)**.

Tryb AXIS Audio Manager Pro

Aby skorzystać z tego trybu:

- Zainstaluj oprogramowanie AXIS Audio Manager Pro na serwerze, na przykład na serwerze zapisu.
- Aktywuj licencję i skonfiguruj program AXIS Audio Manager Pro z dostępem do interfejsu API.
- Opcjonalnie: skonfiguruj certyfikat serwera dla interfejsu WWW; patrz *Certyfikaty*.
- W przypadku instalacji serwera AXIS Audio Manager Pro na komputerze z systemem VMS należy zmienić port 443.

W tym trybie nie ma potrzeby dodawania ani licencjonowania żadnych głośników w systemie VMS, jednak zostanie automatycznie utworzone urządzenie służące do połączenia z serwerem AXIS Audio Manager Pro (wymagana jest jedna licencja na urządzenie VMS). Więcej informacji o aplikacji AXIS Audio Manager Pro znajdziesz w jej *instrukcji obsługi*.

Uwaga

Tryb AXIS Audio Manager Pro obsługuje wyłącznie jedną lokalną lokalizację. Architektury obejmujące wiele lokalizacji, federacyjne oraz połączone ze sobą nie wchodzą w zakres niniejszej integracji.

Łączenie się z serwerem AXIS Audio Manager Pro w trybie Pro

1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer> Menedżer głośników).
2. Kliknij przycisk **Połącz**.
3. W oknie dialogowym:
   - Wybierz serwer zapisu, do którego ma zostać dodany sprzęt AXIS Audio Manager Pro.
   - Wprowadź adres i port HTTPS serwera AXIS Audio Manager Pro.
   - Wprowadź nazwę użytkownika i hasło API (dostęp przez API musi być włączony na serwerze AXIS Audio Manager Pro).
   - Kliknij przycisk **Połącz**.

Po lewej stronie wyświetlane są wszystkie lokalizacje docelowe i strefy dostępne w programie AXIS Audio Manager Pro. Po kliknięciu **AXIS Audio Manager Pro server (Serwer AXIS Audio Manager Pro)** po prawej stronie wyświetli się interfejs WWW programu AXIS Audio Manager Pro.

Uwaga

Aby uzyskać dostęp do interfejsu WWW, konieczne jest bezpośrednie połączenie między komputerem klienta zarządzania a serwerem AXIS Audio Manager Pro.

Jeżeli wprowadziłeś zmiany dotyczące stref, miejsc docelowych, klipów audio lub profili wizualnych w interfejsie internetowym programu AXIS Audio Manager Pro:

- Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników).
- Kliknij przycisk **Update (Aktualizuj)**

Kojarzenie kamery z lokalizacją docelową lub strefą

Można przypisać kamerę do konkretnego miejsca docelowego lub strefy i wyświetlać jej obraz bezpośrednio w widoku kamery w aplikacji Smart Client.

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i zaznacz lokalizację docelową lub strefę.
2. W oknie **Associated camera(s) (Powiązane kamery)** kliknij przycisk **Add cameras... (Dodaj kamery...)** i zaznacz kamery, z którymi chcesz powiązać lokalizację docelową lub strefę.

Gry kamera zostanie powiązana z lokalizacją docelową lub strefą, w aplikacji Smart Client w widoku kamery na pasku narzędzi pojawi się ikona .

Tworzenie profili wizualnych

- W kliencie zarządzania Management Client przejdź do **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po obiekcie > AXIS Optimizer > Menedżer głośników).
- Kliknij serwer **Audio Manager Pro**, aby wyświetlić interfejs internetowy.
- Kliknij **Visual profiles** (Profile wizualne), aby utworzyć lub edytować profile wizualne.

Więcej na temat profili wizualnych, p. *instrukcja obsługi programu AXIS Audio Manager Pro*.

Tryb AXIS Audio Manager Edge

Oprogramowanie AXIS Audio Manager Edge jest fabrycznie zainstalowane w większości głośników Axis i zostanie automatycznie wykryte po wybraniu tego trybu. Aby tryb AXIS Audio Manager Edge działał prawidłowo, do VMS należy dodać liderów lokalizacji, urządzenia pośredniczące dla źródła przywoływania i autonomiczne głośniki.

Uwaga

W trybie AXIS Audio Manager Edge nie można używać wbudowanych wyjść audio kamery ani innych niezgodnych urządzeń dźwiękowych.

Więcej informacji o aplikacji AXIS Audio Manager Edge znajdziesz w jej *instrukcji obsługi*.

Konfigurowanie głośników i stref w trybie AXIS Audio Manager Edge

Aby odtwarzać klipy dźwiękowe i mówić na żywo, trzeba najpierw włączyć funkcję przywoływania w strefach.

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **Devices** > **Speakers** (Nawigacja po witrynie > Urządzenia > Głośniki), a następnie dodaj grupy urządzeń albo dodaj i usuń głośniki z grup urządzeń.
2. Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i upewnij się, że wybrany jest tryb **Edge**.
   Menedżer głośników wyszuka wszystkie głośniki istniejące w systemie VMS oraz wyświetli wszystkie lokalizacje i strefy znane programowi AXIS Audio Manager Edge, których można używać w aplikacji Smart Client.
3. Na liście lokalizacji zaznacz strefę z wyłączoną funkcją przywoływania.
4. Wybierz opcję **Turn on paging for the zone (Włącz przywoływanie w strefie)**.

W przypadku wprowadzenia zmian w strefach lub źródłach przywoływania:

5. Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników).
6. Kliknij przycisk **Update (Aktualizuj)**

Uwaga

Jeżeli konfiguracja nie uda się, sprawdź konfigurację AXIS Audio Manager Edge i spróbuj ponownie.



Kojarzenie kamery z głośnikiem lub strefą

Aby w aplikacji Smart Client w widoku kamery był używany konkretny głośnik lub strefa, można powiązać te obiekty z kamerą.

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i zaznacz głośnik lub strefę.
2. W oknie **Associated cameras (Powiązane kamery)** kliknij przycisk **+ Add cameras (Dodaj kamery)** i zaznacz kamery, z którymi chcesz powiązać głośnik lub strefę.

Gry kamera zostanie powiązana z głośnikiem, grupą urządzeń lub strefą, w aplikacji Smart Client w widoku kamery na pasku narzędzi pojawi się ikona .

Przesyłanie klipów audio do głośników

Aby odtwarzać klipy audio z aplikacji Smart Client w głośniku lub strefie, trzeba najpierw przesłać klipy do głośników za pomocą aplikacji Management Client.

1. Klipy audio, które chcesz przesłać do głośników, umieść w domyślnym folderze **C:\Users\Public \Documents\AXIS Optimizer for Milestone XProtect – Audio Clips**.
2. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i zaznacz głośnik lub strefę.
3. Przejdź do obszaru **Audio clips (Klipy audio)** i kliknij symbol **+** przed klipami, które chcesz przesłać do głośników.

Tryb zgodności wstecznej

Tryb Legacy rozszerza natywną funkcjonalność głośników Axis oraz innych urządzeń Axis z obsługą dźwięku, które dodano do systemu VMS. W odróżnieniu od innych trybów Legacy nie obsługuje zsynchronizowanego rozgłaszania do wielu głośników.

Konfigurowanie głośników w trybie zgodności wstecznej

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **Devices** > **Speakers** (Nawigacja po witrynie > Urządzenia > Głośniki), a następnie dodaj grupy urządzeń albo dodaj i usuń głośniki z grup urządzeń.
2. Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i upewnij się, że wybrany jest tryb zgodności wstecznej.
3. Kliknij
   3.1. W oknie **Manage Side Panel (Zarządzaj panelem bocznym)** zaznacz głośniki, które mają być wyświetlane w aplikacji Smart Client.
   3.2. Kliknij kolejno przyciski **Add (Dodaj)** i **OK**.
   Głośniki znajdujące się w panelu **Visible (Widoczne)** będą teraz wyświetlane w aplikacji Smart Client wszystkim użytkownikom mającym dostęp do głośnika.
4. Aby usunąć głośniki:
   4.1. Wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i kliknij przycisk .
   4.2. W oknie **Manage Side Panel (Zarządzaj panelem bocznym)** zaznacz głośniki, które chcesz usunąć.
   4.3. Kliknij kolejno przyciski **Remove (Usuń)** i **OK**.

Kojarzenie kamery z głośnikiem lub grupą głośników

Można przypisać kamerę do konkretnego miejsca docelowego lub strefy i wyświetlać jej obraz bezpośrednio w widoku kamery w aplikacji Smart Client.

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i zaznacz głośnik lub grupę głośników.

2. W oknie **Associated camera(s) (Powiązane kamery)** kliknij przycisk **Add cameras... (Dodaj kamery...)** i zaznacz kamery, z którymi chcesz powiązać głośnik lub grupę głośników.

Gry kamera zostanie powiązana z głośnikiem lub grupą głośników, w aplikacji Smart Client w widoku kamery na pasku narzędzi pojawi się ikona .

Przesyłanie klipów audio do głośników

Aby odtwarzać klipy audio z aplikacji Smart Client w głośniku lub strefie, trzeba najpierw przesłać klipy do głośników za pomocą aplikacji Management Client.

1. Klipy audio, które chcesz przesłać do głośników, umieść w domyślnym folderze **C:\Users\Public \Documents\AXIS Optimizer for Milestone XProtect – Audio Clips**.
2. W aplikacji Management Client wybierz kolejno opcje **Site Navigation** > **AXIS Optimizer** > **Speaker manager** (Nawigacja po witrynie > AXIS Optimizer > Menedżer głośników) i zaznacz głośnik lub grupę głośników.
3. Przejdź do obszaru **Audio clips (Klipy audio)** i kliknij symbol **+** przed klipami, które chcesz przesłać do głośników.



Zmiana głośności

Tu opisano, jak zmienić natężenie dźwięku emitowanego przez głośniki:

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > Speaker manager (Nawigacja po witrynie > Menedżer głośników)** i zaznacz głośnik lub grupę głośników.
2. Przejdź do ustawienia **Volume (Głośność)** i ustaw żądany poziom głośności.



Odtwarzanie dźwięku przez głośniki

1. W aplikacji Smart Client wybierz kolejno opcje **Live** > **MIP plug-ins** > **Axis speaker control** (Na żywo > Wtyczki kamer MIP > Sterowanie głośnikami Axis), a następnie z listy rozwijanej wybierz głośnik lub strefę.
2. Wysyłanie dźwięku z mikrofonu do głośnika:
   2.1. W trakcie mówienia trzymaj wciśnięty przycisk .
   Upewnij się, że wskaźnik głośności mikrofonu pokazuje aktywność głosową.
3. Odtwarzanie klipu audio przez głośnik:
   3.1. Przejdź do obszaru **Media clip (Klip multimedialny)** i wybierz klip audio z listy rozwijanej.
   3.2. Aby rozpocząć odtwarzanie klipu audio przez wybrany głośnik, kliknij polecenie Play (Odtwórz).

Odtwarzanie dźwięku przez głośniki w widoku kamery

1. W aplikacji Smart Client przejdź do widoku kamery.
2. Jeżeli istnieje powiązanie z głośnikiem, grupą urządzeń lub strefą, na pasku narzędzi będzie widoczna ikona .
3. Kliknij przycisk , aby otworzyć okno **Axis speaker control** (Sterowanie głośnikami Axis).
4. Wysyłanie dźwięku z mikrofonu do głośnika:
   4.1. W trakcie mówienia trzymaj wciśnięty przycisk .
   Upewnij się, że wskaźnik głośności mikrofonu pokazuje aktywność głosową.
5. Odtwarzanie klipu audio przez głośnik:
   5.1. Przejdź do obszaru **Media clip (Klip multimedialny)** i wybierz klip audio z listy rozwijanej.
   5.2. Aby rozpocząć odtwarzanie klipu audio przez wybrany głośnik, kliknij polecenie Play (Odtwórz).

Odtwarzanie dźwięku przez głośniki w przypadku alarmów

1. W aplikacji Smart Client wybierz opcję **Alarms (Alarmy)**.
2. Wybierz alarm, którego źródłem jest kamera.
   Jeżeli istnieje powiązanie z głośnikiem lub strefą, widoczne będą opcje sterowania głośnikiem.
3. Wysyłanie dźwięku z mikrofonu do głośnika:
   – W trakcie mówienia trzymaj wciśnięty przycisk .
   Upewnij się, że wskaźnik głośności mikrofonu pokazuje aktywność głosową.
4. Odtwarzanie klipu audio przez głośnik:
   – Przejdź do obszaru **Media clip (Klip multimedialny)** i wybierz klip audio z listy rozwijanej.
   – Aby rozpocząć odtwarzanie klipu audio przez wybrany głośnik, kliknij polecenie Play (Odtwórz).

Ustawienie zachowania wizualnego przy rozmowie przez głośnik

W aplikacji Smart Client możesz ustawić zachowanie wizualne urządzenia w sekcji Axis speaker control (Sterowanie głośnikami Axis) bezpośrednio w widoku z kamery lub w Menedżerze alarmów.

Uwaga

Profile wizualne obsługiwane są wyłącznie w trybie AXIS Audio Manager Pro.

- W panelu bocznym sekcji **Axis speaker control** (Sterowanie głośnikami Axis):
  – Kliknij .
  – Wybierz profil wizualny z listy rozwijalnej.
  – Jeżeli chcesz zastąpić obecne teksty powiązane z wybranym profilem wizualnym, wpisz je w polu tekstowym.
- W widoku z kamery:
  – Przejdź do konkretnego widoku z kamery.
  – Jeżeli istnieje powiązanie z głośnikiem, grupą urządzeń lub strefą, na pasku narzędzi będzie widoczna ikona .
  – Kliknij przycisk , aby otworzyć okno **Axis speaker control** (Sterowanie głośnikami Axis).
  – Kliknij .
- W sekcji **Alarm Manager** (Menedżer alarmów):
  – Wybierz zdarzenie, przejdź do widoku z kamery i kliknij .

Zakładki nagrań fonicznych w obszarze obserwacji kamery lub w sekcji Alarmy

Po odtworzeniu pliku audio za pomocą elementów sterujących głośnikiem w obszarze obserwacji kamery lub w sekcji Alarmy tworzona jest zakładka zawierająca informacje o tym, kto i na jakim urządzeniu odtworzył ten plik audio.

Aby wyszukać zakładki nagrań fonicznych:

1. W aplikacji Smart Client kliknij przycisk **Search (Szukaj)**.
2. Wybierz przedział czasu oraz jedną lub kilka kamer.
3. Kliknij przycisk **Search for** > **Bookmarks** > **New search** (Szukaj > Zakładki > Nowe wyszukiwanie).

Zarządzanie osobami odwiedzającymi

Wtyczka interkomu

Interkomy sieciowe Axis łączą w jednym urządzeniu funkcje komunikacji, nadzoru wizyjnego i zdalnej kontroli wejścia. Aplikacja AXIS Optimizer ułatwia konfigurowanie i używanie interkomów Axis w systemie VMS. Na przykład pozwala odbierać połączenia i otwierać drzwi.

Konfigurowanie interkomu



Zazwyczaj zamek drzwi należy podłączyć do pierwszego przekaźnika interkomu. Na podstawie informacji w sekcji **Usage** (Zastosowanie) aplikacja AXIS Optimizer decyduje, który port wyjścia ma być używany. Będzie to pierwszy port, w którym ustawienie **Usage = Door (Zastosowanie = Drzwi)** (domyślnie przekaźnik RELAY1).

Uwaga

Wymagania

- Interkom Axis
- Mikrofon podłączony do komputera odbierającego połączenia
- Inteligentny klient skonfigurowany i uruchomiony

Uwaga

Od wersji 5.0.X.X i nowszych aplikacji AXIS Optimizer stosowana jest inna metoda konfiguracji domofonów w systemach VMS niż we wcześniejszych wersjach. Do wykrywania połączeń zamiast wejścia 1 może służyć urządzenie obsługujące metadane. Nadal obsługujemy dotychczasową metodę konfiguracji, jednak w przypadku nowych instalacji polecamy metodę nową.

1. Zainstaluj najnowszą wersję aplikacji AXIS Optimizer na wszystkich urządzeniach klienckich, na których mają być odbierane połączenia i kontrolowane drzwi.
2. Zaloguj się w aplikacji Management Client.
3. Dodaj interkom Axis do serwera zapisu.
4. W aplikacji Management Client włącz wszystkie potrzebne urządzenia. Aby móc odbierać połączenia w aplikacji Smart Client, potrzebujesz następujących elementów:
   - Kamera 1
   - Mikrofon
   - Głośnik
   - Metadane

- Wejście 2 (opcjonalne, jeśli interkom na porcie 2 ma podłączony przekaźnik zabezpieczający)
- Wyjście podłączone do drzwi. Jeśli wiesz, które wyjście jest połączone z drzwiami, wybierz właśnie je. Jeżeli nie wiesz, wybierz wszystkie wyjścia.

5. Przejdź do menu **Site Navigation > Devices > Metadata (Nawigacja po witrynie > Urządzenia > Metadane)**, a następnie wybierz urządzenie metadanych dla instalowanego interkomu.
6. Kliknij przycisk **Settings (Ustawienia)**.
7. Ustaw w opcji **Event data (Dane zdarzenia)** wartość **Yes (Tak)**.
8. Kliknij przycisk **Save (Zapisz)**.
9. Jeśli wejście 2 zostało włączone, trzeba je także skonfigurować.
   9.1. Przejdź do menu **Site Navigation > Devices > Input (Nawigacja po witrynie > Urządzenia > Wejście)** i wybierz Input 2 (Wejście 2).
   9.2. Kliknij kolejno opcje **Events (Zdarzenia)** i **Add (Dodaj)**.
   9.3. Zaznacz opcję **Input Falling event (Zdarzenie Spadek sygnału wejścia)** i dodaj to wejście do włączonych wejść. Powtórz te czynności dla opcji **Input Rising event (Zdarzenie Wzrost sygnału wejścia)**.
   9.4. Kliknij przycisk **Save (Zapisz)**.
10. Aby skonfigurować uprawnienia dla określonych ról, zobacz *Ustawianie uprawnień dla interkomu, on page 38*.
11. *Wykonywanie połączenia testowego, on page 39*.

Ustawianie uprawnień dla interkomu

Aby można było obsługiwać połączenia, trzeba najpierw włączyć uprawnienia.

1. Wybierz kolejno opcje **Site Navigation > Security > Roles (Nawigacja po witrynie > Zabezpieczenia > Role)**.
2. Wybierz rolę.
3. Przejdź do okna **Overall Security (Ogólna ochrona)**.
4. Upewnij się, że każda grupa zabezpieczeń ma ustawione wymagane uprawnienia. Przejdź do okna **Hardware (Sprzęt)** i wybierz opcję **Driver commands (Polecenia sterujące)**.
5. Aby ustawić uprawnienia na poziomie systemu, przejdź do okna **Overall Security (Ogólna ochrona)**. Aby ustawić uprawnienia na poziomie urządzenia, przejdź do okna **Device (Urządzenie)**.
6. Ustaw uprawnienia dla grup zabezpieczeń:
   6.1. Przejdź do okna **Cameras (Kamery)**. Wybierz kolejno **Read (Odczyt)** i **View live (Podgląd na żywo)**.
   6.2. Przejdź do okna **Microphones (Mikrofony)**. Wybierz kolejno **Read (Odczyt)** i **Listen (Słuchanie)**.
   6.3. W sekcji **Overall Security (Ogólna ochrona)** przejdź do okna **Speakers (Głośniki)**. Wybierz opcje **Read (Odczyt)** i **Speak (Mówienie)**.
   W oknie **Device (Urządzenie)** przejdź do ustawienia **Speakers (Głośniki)** i zaznacz wartość **Read (Odczyt)**. Następnie przejdź na kartę **Speech (Mowa)** i wybierz **Speak (Mówienie)**.
   6.4. Przejdź do okna **Metadata (Metadane)**. Wybierz opcje **Read (Odczyt)** i **Live (Na żywo)**.
   6.5. Przejdź do okna **Input (Wejście)**. Wybierz opcję **Read (Odczyt)**.
   6.6. Przejdź do opcji **Output (Wyjście)**. Wybierz opcje **Read (Odczyt)** i **Activate (Aktywacja)**.

Aby przypisać uprawnienia kontrolujące, którzy operatorzy mogą obsługiwać połączenia z konkretnych interkomów:

1. Dla urządzenia metadanych 1 konkretnego interkomu wybierz opcję **Read (Odczyt)**.
2. Wyczyść to uprawnienie dla wszystkich pozostałych ról. Użytkownicy niemający uprawnień nie będą mogli odbierać połączeń.

Aby przeglądać historię połączeń, potrzebujesz dodatkowych uprawnień.

1. Aby ustawić uprawnienia na poziomie systemu, przejdź do okna **Overall Security (Ogólna ochrona)**. Aby ustawić uprawnienia na poziomie urządzenia, przejdź do okna **Device (Urządzenie)**.
2. Wybierz poniższe uprawnienia dla grup zabezpieczeń:
   2.1. Przejdź do okna **Cameras (Kamery)**. Wybierz opcje **Playback (Odtwarzanie)** i **Read sequences (Odczyt sekwencji)**.
   2.2. Przejdź do okna **Microphones (Mikrofony)**. Wybierz opcje **Playback (Odtwarzanie)** i **Read sequences (Odczyt sekwencji)**.
   2.3. Przejdź do okna **Speakers (Głośniki)**. Wybierz opcje **Listen (Słuchanie)**, **Playback (Odtwarzanie)** i **Read sequences (Odczyt sekwencji)**.

Wykonywanie połączenia testowego

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options (Ustawienia > Opcje interkomu Axis)**.
2. Kliknij przycisk **Połączenie testowe**.
3. Wybierz interkom i kliknij **Make call (Wykonaj połączenie)**.

Eliminacja echa w trakcie połączeń

Funkcja push-to-talk umożliwia przesyłanie dźwięku przez interkom tylko w jednym kierunku naraz. Jeżeli słuchać echo w trakcie połączenia, możesz włączyć funkcję push-to-talk.

Aby włączyć **Push-to-talk**:

- W aplikacji Smart Client przejdź do **Settings** > **Axis intercom options** (Ustawienia > Opcje domofonu Axis).
- Przejdź do sekcji **Call** (Połączenie) i wybierz **Push-to-talk**.

Sterowanie interkomem za pomocą podglądu na żywo

Dla każdego domofonu i widoku domofonu kliknij opcję



, aby szybko przejąć kontrolę nad urządzeniem.

Jak...?	Instrukcje	Uwaga
Otwieranie zamka	Kliknij kolejno opcje  > **Access** (Dostęp) lub **Extended access** (Rozszerzony dostęp).	Po odblokowaniu zamka nie można kliknąć polecenia **Access (Dostęp)** ani **Extended access (Dostęp rozszerzony)**.
Sprawdzanie, czy drzwi są zablokowane, czy odblokowane	Kliknij opcję  i przeczytaj status na dole menu.	-

Jak...?	Instrukcje	Uwaga
Porozmawiać z osobą stojącą przed interkomem	Kliknij  > **Start call** (Rozpocznij połączenie).	Zostanie otwarte okno połączenia i system nawiąże dwukierunkową komunikację z interkomem.
Sprawdzanie, kto łączył się wczoraj	Kliknij  > **Call history** (Historia połączeń).	Zostanie wyświetlona lista połączeń wykonanych z bieżącym interkomem.

Odbieranie połączenia z okna podglądu na żywo

Gdy osoba odwiedzająca naciśnie przycisk połączenia na interkomie, na każdym uruchomionym inteligentnym kliencie zostanie wyświetlone okno połączenia. Zmiana rozmiaru okna połączenia automatycznie spowoduje wybór odpowiedniego widoku z kamery, na przykład widoku korytarza lub widoku poziomego.

Jak...?	Instrukcje	Uwaga
Odebrać połączenie	Kliknij przycisk **Akceptuj**	Zostanie otwarty dwukierunkowy kanał audio między operatorem a osobą przy interkomie.
Przekierować połączenie do innego operatora, ponieważ jestem zajęty/-a	Zamknij okno, klikając przycisk **X**	Gdy odrzucisz połączenie, inny operator może je odebrać na innym urządzeniu klienckim Interkom będzie emitował sygnały dźwiękowe i świetlne do momentu, aż ktoś odbierze połączenie. Jeżeli przez dłuższy czas połączenie nie zostanie odebrane, w historii połączeń otrzyma status nieodebrane.
Odrzucić połączenie, ponieważ drzwi zostały już otwarte po	Kliknij przycisk **Odrzuć**	Odrzucenie połączenia powoduje automatyczne zamknięcie jego okna na innych urządzeniach

Jak...?	Instrukcje	Uwaga
wizualnym potwierdzeniu i nie muszę rozmawiać z tą osobą Odrzucić połączenie, ponieważ nie chcę rozmawiać z niepożądanym gościem		klienckich. Żaden inny operator nie może odebrać połączenia. Interkom przestaje wysyłać sygnały dźwiękowe i świetlne, po czym okno połączenia się zamyka. W historii połączeń połączenie otrzymuje status odebrane.
Otwieranie drzwi	Kliknij **Access (Dostęp)**	Zamek interkomu zostanie otwarty na 7 s. Aby określić czas, przez jaki drzwi pozostają otwarte: 1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options > Door access (Ustawienia > Opcje interkomu Axis > Dostęp przez drzwi)**. 2. Zmień wartość w polu **Czas dostępu**.
Tymczasowo zatrzymać przekazywanie dźwięku od operatora do interkomu.	Kliknij polecenie **Wycisz**	-
Rozmowa z gościem, gdy włączona jest funkcja push-to-talk.	Kliknij **Talk (Rozmawiaj)**	Zwolnij przycisk rozmowy, aby słuchać gościa.
Zakończ połączenie.	Kliknij przycisk **Rozłącz**	Zgodnie z domyślnym ustawieniem automatycznego zamykania okno połączenia zamyka się po odrzuceniu lub rozłączeniu połączenia. Aby zmienić domyślne zachowanie okna połączenia: 1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options > Call (Ustawienia > Opcje interkomu Axis > Połączenie)**. 2. Wyczyść opcję **Auto-close window (Automatycznie zamknij okno)**.

Wyświetlanie wielu kamer w oknie połączenia

W oknie połączenia mogą być wyświetlane równocześnie nawet trzy kamery. Oznacza to, że w jednym oknie połączenia można widzieć strumień wideo z interkomu oraz dodatkowo strumienie wideo z dwóch innych kamer. Jest to przydatne na przykład wtedy, gdy chcesz widzieć doręczyciela i jednocześnie obszar wokół drzwi, przy których stoi ta osoba.

Aby skonfigurować wyświetlanie wielu kamer w oknie połączenia:

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options (Ustawienia > Opcje interkomu Axis)**. Otwórz menu **Call > Intercom settings (Połączenie > Ustawienia interkomu)**.
2. Otwórz menu **Selected device (Wybrane urządzenie)** i wybierz urządzenie, które chcesz skonfigurować.
3. Przejdź do pozycji **Multiple cameras (Wiele kamer)**. Wybierz, który interkom ma być widoczny w oknie połączenia jako **camera 1 (kamera 1)**.
4. Wybierz skojarzone kamery, które mają być widoczne jako **camera 2 (kamera 2)** i **camera 3 (kamera 3)** w oknie połączenia, gdy zadzwoni interkom.
5. Zamknij okno **Intercom settings (Ustawienia interkomu)**.

Akcje okna wywołania

Akcje okna połączenia umożliwiają konfigurowanie zdarzeń zdefiniowanych przez użytkownika, które są powiązane z regułami w silniku reguł XProtect. To, które zdarzenia użytkownik może konfigurować i z których może korzystać, zależy od roli.

Aby skonfigurować akcje w oknie połączenia:

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options (Ustawienia > Opcje interkomu Axis)**.
2. Otwórz menu **Call > Intercom settings (Połączenie > Ustawienia interkomu)**.
3. Otwórz menu **Selected device (Wybrane urządzenie)** i wybierz urządzenie, które chcesz skonfigurować.
4. Przejdź do menu **Call window actions (Akcje okna połączenia)**, aby wybrać akcje okna połączenia, których chcesz używać.

Istnieją dwa typy akcji okna połączenia:

- **Access button action (Akcja przycisku dostępu)**: Skonfigurowanie akcji przycisku dostępu umożliwia zastąpienie domyślnej akcji przycisku **Access (Dostęp)**. Można na przykład skonfigurować otwieranie zestawu drzwi za pomocą przycisku **Access (Dostęp)**.
- **Custom action (Akcja niestandardowa)**: Po skonfigurowaniu akcji niestandardowej w oknie wywołania wyświetlany jest przycisk. Klikając ten przycisk, możesz uruchomić akcję niestandardową. Akcja niestandardowa to akcja, która niekoniecznie jest związana z dostępem do drzwi, np. wysyłanie wiadomości e-mail, wyzwalanie alarmów lub rozpoczynanie ciągłego nagrywania.

Wyświetlanie strony w oknie połączenia

Podczas korzystania z urządzenia AXIS I8307-VE Network Intercom można wyświetlać strony w oknie połączenia. Jest to przydatne do wyświetlania informacji, na przykład mapy lub godzin otwarcia, osobie stojącej przed interkomem.

Najpierw skonfiguruj te strony w interfejsie WWW interkomu, patrz *AXIS I8307-VE Network Intercom*.

W przypadku połączenia przychodzącego z interkomu:

1. Kliknij **Show page (Pokaż stronę)**, aby wyświetlić okno dialogowe zawierające wszystkie skonfigurowane strony w urządzeniu.
2. Kliknij **Load previews (Załaduj podglądy)**, aby wyświetlić podgląd wszystkich stron.
   Aby wyświetlić podgląd jednej skonfigurowanej strony, najedź kursorem na stronę i kliknij ikonę obrazu.
3. Kliknij skonfigurowaną stronę, aby wyświetlić ją na interkomie.

Można ustawić okno połączenia tak, aby wyświetlało zarówno obraz z kamery interkomu, jak i stronę przy użyciu różnych powiązanych kamer, tj. kamera 1 będzie wyświetlać obraz z kamery, a kamera 2 będzie wyświetlać stronę, patrz *Wyświetlanie wielu kamer w oknie połączenia, on page 43*.

Pamiętaj, że po zakończeniu połączenia strona zostanie zamknięta. Powtórz powyższe kroki, aby wyświetlić stronę podczas nowego połączenia.

Filtrowanie według numerów wewnętrznych

Domyślnie wszystkie komputery podłączone do interkomu odbierają połączenia. Dodając rozszerzenia połączeń i filtrując je w VMS, można skonfigurować interkomy tak, aby kierowały połączenia do określonych klientów Smart Client w VMS. Można konfigurować harmonogramy przekierowywania połączeń i dodawać kontakty rezerwowe. Można również przekierowywać połączenia do kontaktów opartych na protokole SIP i dodawać je jako kontakty rezerwowe.

W interfejsie WWW interkomu

1. Przejdź do pozycji **Communication** > **SIP** (Komunikacja > SIP).
2. Wybierz opcję **Enable SIP (Włącz SIP)**.
3. Kliknij przycisk **Save (Zapisz)**.
4. Przejdź do pozycji **Communication** > **VMS Calls** (Komunikacja > Połączenia VMS).
5. Sprawdź, czy jest włączona opcja **Allow calls in the video management system (VMS)** (Zezwalaj na połączenia w systemie zarządzania obrazem (VMS)).
6. Przejdź do pozycji **Communication** > **Contact list** (Komunikacja > Lista kontaktów).
7. W obszarze **Recipients** (Odbiorcy) kliknij +, aby dodać nowy kontakt. Wprowadź informacje o nowym kontakcie i kliknij przycisk **Save (Zapisz)**. Można dodać kilka kontaktów.
   - W polu **SIP address** (Adres SIP) wprowadź `VMS_CALL:<extension>`. Zastąp element `<extension>` (numer wewnętrzny) nazwą numeru wewnętrznego kontaktu, na przykład `ReceptionA`.
   - Aby skonfigurować harmonogram dla kontaktu, wybierz jego **Availability (Dostępność)**.
   - Możesz dodać kontakt rezerwowy, który odbierze połączenie, jeżeli żaden z pierwotnych kontaktów nie odpowiada, na przykład `ReceptionB`.
8. Przejdź do pozycji **Communication** > **Calls** (Komunikacja > Połączenia).
9. W przypadku urządzeń z oprogramowaniem układowym AXIS OS w wersji wcześniejszej niż 11.6 wyłącz opcję **Make calls in the video management system (VMS)** (Wykonuj połączenia w systemie zarządzania obrazem (VMS)).
10. W polu **Recipients** (Odbiorcy) usuń kontakt **VMS** i dodaj kontakt nowo utworzony.

W aplikacji Management Client

Zalecamy skonfigurowanie interkomów w VMS do korzystania z urządzenia metadanych do wykrywania połączeń. Zob. *Konfigurowanie interkomu, on page 37*.

W aplikacji Smart Client

Skonfiguruj rozszerzenie połączenia dla każdego użytkownika, który powinien odbierać połączenia. Ustawienie jest przechowywane na poziomie użytkownika. Oznacza to, że użytkownik będzie odbierał połączenia niezależnie od używanego komputera.

1. Zaloguj się do Smart Client jako użytkownik, który ma odbierać połączenia.
2. Wybierz kolejno opcje **Settings > Axis intercom options (Ustawienia > Opcje interkomu Axis)**.
3. W obszarze **Call > Call extension (Połączenie > Nr wewnętrzny)** wprowadź nazwę numeru wewnętrznego kontaktu, na przykład `ReceptionA`. Od tej chwili użytkownik będzie teraz odbierał połączenia tylko wtedy, gdy nr wewnętrzny będzie zgodny z wartością filtra.
   Jeżeli chcesz dodać kilka nazw numerów wewnętrznych, oddziel je średnikiem, na przykład `ReceptionA;ReceptionC`

Wyświetlanie historii połączeń

W historii połączeń można przejrzeć odebrane i nieodebrane połączenia oraz zdarzenia odryglowania drzwi. Można wybierać spośród połączeń oraz oglądać odnośny film przeznaczony do odtwarzania, jeśli jest dostępny.

1. Na inteligentnym kliencie przejdź do widoku interkomu.

2. Kliknij



> **Call history** (Historia połączeń).

Uwaga

Historia połączeń zawiera maksymalnie 39 połączeń i 1000 rekordów dziennika dostępu. Limit liczby połączeń może być jeszcze obniżony, jeśli rozmowa jest często wyciszana.

Aby rejestrować zdarzenia odblokowania drzwi, należy ustawić czas przechowywania (w dniach) dla interkomu Axis:

1. W aplikacji Management Client wybierz kolejno opcje **Tools > Options > Alarm and Events > Event retention (Narzędzia > Opcje > Alarmy i zdarzenia > Przechowywanie zdarzeń)**.
2. Ustaw czas w opcjach **Output Activated (Wyjście aktywowane)** i **Output Deactivated (Wyjście dezaktywowane)**.

Wyłączanie mikrofonu przy braku aktywnego połączenia

Gdy nie przychodzą żadne połączenia do interkomu Axis, można wyłączyć mikrofon. Mikrofon włączy się po zaistnieniu aktywnego połączenia.

Uwaga

- Do wyłączenia mikrofonu trzeba mieć uprawnienia administratora.
- Nie jest to obsługiwane w sfederowanej architekturze ani w przypadku korzystania z kontaktów rezerwowych.

1. W aplikacji Smart Client przejdź do **Settings** > **Axis intercom options** (Ustawienia > Opcje domofonu Axis).
2. Zaznacz opcję **Turn off intercom microphone when no active call (Wyłącz mikrofon interkomu w razie braku aktywnych połączeń)**.

Generowanie alarmu po siłowym otwarciu drzwi

Jeżeli drzwi mają przekaźnik zabezpieczający (wejście 2), nakładka drzwi w oknie połączenia na inteligentnym kliencie pokazuje moment otwarcia lub zamknięcia drzwi. Oznacza to, że gdy ktoś otworzy drzwi siłą w czasie, gdy są one zablokowane, można otrzymać o tym alarm.

Uwaga

Aby można było odebrać taki alarm, musi być uruchomiony przynajmniej jeden inteligentny klient.

Aby skonfigurować alarm:

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options > Administrator options (Ustawienia > Opcje interkomu Axis > Opcje administratora)**.
2. Zaznacz opcję **Trigger an alarm when a door has been forced open (Wyzwalaj alarm po siłowym otwarciu drzwi)**.

Włączanie alarmu w przypadku zbyt długiego otwarcia drzwi

Jeżeli drzwi mają przekaźnik zabezpieczający (wejście 2), nakładka drzwi w oknie połączenia na inteligentnym kliencie pokazuje moment otwarcia lub zamknięcia drzwi. Oznacza to, że gdy ktoś otworzy drzwi i zbyt długo pozostaną one otwarte, zostanie wygenerowany alarm.

Uwaga

Aby można było odebrać taki alarm, musi być uruchomiony przynajmniej jeden inteligentny klient.

Aby skonfigurować alarm:

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options > Administrator options (Ustawienia > Opcje interkomu Axis > Opcje administratora)**.
2. Wybierz opcję **Trigger an alarm when a door has been open longer than (s) (Wyzwalaj alarm, gdy drzwi pozostają otwarte dłużej niż (s))**.
3. Wpisz, po jakim czasie otwarcia drzwi ma być emitowany alarm.

Blokowanie odbierania połączeń w aplikacjach klienckich

Administrator może określić, że klienty nie będą odbierały żadnych połączeń. Wtedy gdy ktoś wykonuje połączenie, na danym kliencie nie otworzy się okno połączenia.

1. W aplikacji Smart Client wybierz kolejno opcje **Settings > Axis intercom options > Call (Ustawienia > Opcje interkomu Axis > Połączenie)**.
2. Wyczyść pole wyboru **Receive calls on this client (Odbieraj połączenia na tym kliencie)**.

Wizualizacja dźwięku

Widok mikrofonu

W systemie można wizualizować dźwięk, dodając jeden lub kilka widoków mikrofonu do Smart Client. Następnie można monitorować dźwięk zarówno w podglądzie na żywo, jak i z odtworzenia. Za pomocą funkcji wykrywania dźwięku w urządzeniu Axis można sprawdzić, kiedy poziomy dźwięku podnoszą się powyżej określonego poziomu. Typowe przypadki użycia tej funkcjonalności obejmują:

- *Jednoczesne słuchanie dźwięku z kilku mikrofonów, on page 49*
- *Wykrywanie zdarzeń z dźwiękiem, on page 49*

- *Analizowanie zdarzeń, on page 49*

Uwaga

Wymagania

- VMS Smart Client w wersji 2020 R2 lub nowszej.

Konfiguracja VMS dla widoku mikrofonu

1. Ustaw poziomy detekcji:
   1.1. Na kliencie zarządzania wybierz kolejno opcje **Site Navigation > AXIS Optimizer > Device assistant (Nawigacja po witrynie > AXIS Optimizer > Asystent urządzeń)** i wybierz urządzenie.
   1.2. Otwórz ustawienia opcji **Detectors (Detektory)**. Sposób otwierania tych ustawień zależy od wersji oprogramowania urządzenia.
   1.3. Przejdź do menu **Audio detection (Wykrywanie dźwięku)** i dostosuj **Input 1 sound level (Poziom sygnału dźwiękowego 1)** do swoich potrzeb.
2. Pobieranie zdarzeń z kamery do systemu VMS:
   2.1. W kliencie zarządzania wybierz kolejno opcje **Site Navigation > Devices > Microphones (Nawigacja po witrynie > Urządzenia > Mikrofony)**.
   2.2. Kliknij swój mikrofon, a następnie kliknij opcję **Events (Zdarzenia)**.
   2.3. Dodaj zdarzenia **Audio Falling (Opadanie dźwięku)** i **Audio Rising (Wznoszenie dźwięku)**.
3. Ustaw okres przechowywania w systemie metadanych dotyczących wykrytych dźwięków:
   3.1. Przejdź do menu **Tools > Options > Alarm and Events > Device events** (Narzędzia > Opcje > Alarm i zdarzenia > Zdarzenia urządzenia).
   3.2. Znajdź **Audio Falling (Opadanie dźwięku)** i ustaw czas przechowywania.
   3.3. Znajdź **Audio Raising (Wznoszenie dźwięku)** i ustaw czas przechowywania.
4. Sprawdź, czy zapis dźwięku został skonfigurowany. Można ustawić ciągłe nagrywanie dźwięku lub utworzyć reguły nagrywania na podstawie zdarzeń opadania lub wznoszenia dźwięku.
5. Powtórz kroki opisane wyżej dla każdego mikrofonu, którego chcesz używać z widokiem mikrofonu.
6. W narzędziu Smart Client przejdź do **Settings > Timeline > Additional data (Ustawienia > Oś czasu > Dodatkowe dane)** i wybierz opcję **Show (Pokaż)**.

Dodawanie widoku mikrofonu do aplikacji Smart Client

1. Otwórz narzędzie Smart Client i kliknij opcję **Setup (Ustawienia)**.
2. Przejdź do obszaru **Views (Widoki)**.
3. Kliknij polecenie **Create new view (Utwórz nowy widok)** i wybierz format.
4. Przejdź do menu **System overview > AXIS Optimizer (Przegląd systemu > AXIS Optimizer)**.
5. Kliknij opcję **Microphone view (Widok mikrofonu)** i przeciągnij ją do widoku.
6. Wybierz mikrofon.
7. Kliknij opcję **Setup (Ustawienia)**.

Korzystanie z widoku mikrofonu

- Podgląd na żywo
  - Poziomy dźwięku są wyświetlane w formie wykresu słupkowego; po prawej stronie jest widoczny bieżący poziom, a po lewej — do 60 sekund historii.
  - Kliknij w widoku, aby słuchać dźwięku z mikrofonu.
  - W każdym z widoków mikrofonu jest widoczna ikona słuchawki. Kliknięcie tej ikony umożliwia wyciszenie lub ponowne włączenie dźwięku w każdym widoku — bez wybierania samego widoku. Dzięki temu można słuchać dźwięku z kilku mikrofonów naraz.

- Odtwarzanie
  - W przypadku wykrycia dźwięku dostępnego dla mikrofonu nastąpi podświetlenie ikony.
  - Żółte paski oznaczają, że dźwięk został wykryty zgodnie z poziomami wykrywania ustawionymi w urządzeniu.
  - Kliknij w widoku, aby słuchać dźwięku z mikrofonu.
  - W każdym z widoków mikrofonu jest widoczna ikona słuchawki. Kliknięcie tej ikony umożliwia wyciszenie lub ponowne włączenie dźwięku w każdym widoku — bez wybierania samego widoku. Dzięki temu można słuchać dźwięku z kilku mikrofonów naraz.

Jednoczesne słuchanie dźwięku z kilku mikrofonów

Widok mikrofonu umożliwia jednoczesne słuchanie dźwięku z kilku mikrofonów, za zarówno w trybie podglądu na żywo, jak i odtwarzania.

1. *Konfiguracja VMS dla widoku mikrofonu, on page 48*.
2. Otwórz narzędzie Smart Client i kliknij opcję **Setup (Ustawienia)**.
3. Przejdź do obszaru **Views (Widoki)**.
4. Kliknij polecenie **Create new view (Utwórz nowy widok)** i wybierz widok podzielony.
5. Przejdź do menu **System overview > AXIS Optimizer (Przegląd systemu > AXIS Optimizer)**.
6. W przypadku każdego mikrofonu, z którego dźwięku chcesz słuchać:
   6.1. Kliknij opcję **Microphone view (Widok mikrofonu)** i przeciągnij ją do widoku.
   6.2. Wybierz mikrofon.
7. Kliknij opcję **Setup (Ustawienia)**.
8. W przypadku każdego mikrofonu określ, czy chcesz go wyciszyć lub włączyć. W tym celu klikaj ikony słuchawek w widokach mikrofonu. Teraz możliwe jest jednoczesne słuchanie dźwięku ze wszystkich niewyciszonych mikrofonów.

Wykrywanie zdarzeń z dźwiękiem

Może być konieczne monitorowanie działań w miejscach, w których nie wolno instalować kamer, np. w toaletach. W widoku mikrofonu można szybko sprawdzić, kiedy poziom dźwięku przekroczy poziomy detekcji.

1. *Konfiguracja VMS dla widoku mikrofonu, on page 48*. Należy pamiętać o ustawieniu odpowiednich poziomów detekcji dla urządzenia i obszaru, który ma być monitorowany.
2. Dodaj widok mikrofonu z urządzeniem do podglądu na żywo w narzędziu Smart Client, p. *Dodawanie widoku mikrofonu do aplikacji Smart Client, on page 48*.

Analizowanie zdarzeń

Po wystąpieniu zdarzenia na osi czasu można szybko zidentyfikować okresy odtwarzania, w których dźwięk był wykrywany przez mikrofony.

1. *Konfiguracja VMS dla widoku mikrofonu, on page 48*.
2. Można dodać jeden lub kilka widoków mikrofonu z odpowiednimi urządzeniami do odtwarzania przy użyciu narzędzia Smart Client, p. *Dodawanie widoku mikrofonu do aplikacji Smart Client, on page 48*.

Prace wyjaśniające

Aplikacja AXIS Optimizer oferuje cztery kategorie centralnego wyszukiwania urządzeń Axis:

- *Prace wyjaśniające, on page 50* (wyszukiwanie obiektów)
- *Wyszukiwanie pojazdów, on page 53*
- *Zone speed search (Wyszukiwanie prędkości w strefie), on page 56*
- *Wyszukiwanie kontenerów, on page 58*

W aplikacji Smart Client można również dodać osobną kartę wyszukiwania tablic rejestracyjnych, p. *Axis license plates, on page 59*.

Te kategorie wyszukiwania można skonfigurować w centralnym panelu, zobacz *Konfiguracja kategorii wyszukiwania Axis, on page 108*.

Prace wyjaśniające

Kamery Axis z systemem AXIS OS 9.50 lub nowszym generują metadane, które opisują obiekty poruszające się w danej chwili w polu widzenia kamery. Dane te mogą być rejestrowane przez VMS wraz z odpowiadającym im obrazem wizyjnym i dźwiękiem. Funkcja Wyszukiwanie do celów dochodzeniowych dostępna w aplikacji AXIS Optimizer pozwala analizować i przeszukiwać te dane. Za pomocą tej funkcji można uzyskać całościowy obraz aktywności w scenie albo szybko znaleźć konkretny obiekt lub zdarzenie.

Zanim rozpoczniesz

1. Upewnij się, że w kamerze jest zainstalowana najnowsza wersja systemu AXIS OS.
2. Upewnij się, że używasz prawidłowej wersji systemu VMS:
   - Corporate 2019 R3 lub nowsze albo Expert 2019 R3 lub nowsze
   - Professional+ 2022 R3 lub nowsze albo Express+ 2022 R3 lub nowsze
3. Czas kamery musi być zsynchronizowany z usługą NTP.
4. Aby filtrować obiekty według typów **Człowiek**, **Pojazd**, **Rower**, **Autobus**, **Samochód osobowy** lub **Samochód ciężarowy**:
   4.1. korzystaj z urządzenia Axis z obsługą AXIS Object Analytics. Patrz Filtr analityczny w *Selektorze produktów*.
   4.2. Przejdź do menu **System > Analytics metadata (System > Metadane analityczne)** i włącz **Analytics Scene Description (Opis sceny analityki)** na stronie internetowej kamery.
5. Aby filtrować według **koloru** pojazdu, **koloru górnej części ubioru** lub **koloru dolnej części ubioru**:
   5.1. korzystaj z urządzenia Axis z obsługą AXIS Object Analytics. Patrz Filtr analityczny w *Selektorze produktów*.
   5.2. używaj urządzenia Axis z ARTPEC-8 lub CV25. P. filtr System-on-chip w narzędziu wyboru produktów *Product selector*.

Konfigurowanie wyszukiwania do celów dochodzeniowych



1. W aplikacji Management Client upewnij się, że urządzenie dostarczające metadane jest włączone dla kamer.

2. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
3. Wybierz kolejno opcje **Site Navigation > Devices > Metadata (Nawigacja po witrynie > Urządzenia > Metadane)**.
4. Zaznacz swoje urządzenie i kliknij przycisk **Record (Rejestruj)**. Upewnij się, że funkcja **Recording (Zapis)** jest włączona.
   Domyślnie metadane są rejestrowane tylko wtedy, gdy system VMS wykryje ruch w scenie. Dlatego zalecamy takie wyregulowanie progu ruchu w środowisku, aby nie ominąć żadnego ruchu obiektu.
5. Kliknij **Settings** (Ustawienia) i sprawdź, czy jest włączona opcja **Analytics data** (Dane analityczne).
6. W aplikacji Smart Client otwórz podgląd na żywo i upewnij się, że widać ramki wokół obiektów i czy są one wyświetlane poprawnie.
   Przystosowanie się zegara do czasu NTP może nieco potrwać.
7. Zaczekaj co najmniej 15 minut, aż system zarejestruje wideo i metadane. Następnie możesz rozpocząć korzystanie z funkcji wyszukiwania, p. *Wyszukiwanie materiału, on page 51*.
8. Włącz **Consolidated metadata (Skonsolidowane metadane)**, aby zwiększyć szybkość wyszukiwania na urządzeniach z systemem AXIS OS 11.10 lub nowszym. Patrz *Metadane i wyszukiwanie, on page 107*.

Wyszukiwanie materiału



Uwaga

Korzystanie z funkcji wyszukiwania wymaga jej skonfigurowania w aplikacji Management Client. Instrukcje konfiguracji, p. *Konfigurowanie wyszukiwania do celów dochodzeniowych, on page 50*.

1. W aplikacji Smart Client kliknij przycisk **Search (Szukaj)**.
2. Wybierz przedział czasu oraz jedną lub kilka kamer.
3. Kliknij kolejno opcje **Search for > Forensic search > New search (Wyszukaj > Wyszukiwanie do celów dochodzeniowych > Nowe wyszukiwanie)**. Dla każdego wyniku wyszukiwania zobaczysz obiekt oraz jego ścieżkę ruchu w miniaturze.
   - Miniatura wyświetla klatkę wideo, w której obiekt był najbardziej widoczny.
   - Zielony punkt wskazuje miejsce, w którym kamera po raz pierwszy wykryła obiekt.
   - Czerwony punkt wskazuje miejsce, w którym kamera po raz ostatni wykryła obiekt.
   - Aby zobaczyć pełną sekwencję wideo dla wyników wyszukiwania, zaznacz ją i kliknij **Play forward (Odtwórz do przodu)** w panelu podglądu.
   - Aby ukryć nakładki graficzne, przejdź do ustawienia **Bounding boxes (Obwódki)** i wybierz opcję **Hide (Ukryj)**.

   Uwaga

   Aplikacje analityczne działające w kamerze, takie jak AXIS Object Analytics i AXIS Loitering Guard, mogą również wypalać nakładki na obrazie wizyjnym. Aby usunąć te nakładki, przejdź na stronę internetową konfiguracji aplikacji.
4. Zaznacz filtry wyszukiwania, aby zawęzić listę zwracanych wyników.
   Aby dowiedzieć się więcej o stosowaniu różnych filtrów, p. *Zawężanie wyszukiwania, on page 52*.

5. Zaznacz wyniki wyszukiwania, którym chcesz się dokładniej przyjrzeć. Można na przykład dodać je do zakładek albo wykonać operacje opisane w temacie *Tworzenie raportu PDF o wysokiej jakości, on page 59*.

Zawężanie wyszukiwania

Aby zawęzić wyniki wyszukiwania, można zastosować jeden lub kilka filtrów wyszukiwania.

- **Region of interest (Obszar zainteresowania)**
  Detekcja obiektów, które się poruszyły w granicach określonego obszaru.
- **Object direction (Kierunek obiektu)**
  Detekcja obiektów, które przebyły określoną trasę w scenie: w lewo, w prawo, w dół lub w górę.
- **Typ obiektu**
  Detekcja obiektów określonego typu: człowiek, pojazd, rower, autobus, samochód lub ciężarówka.

Uwaga

- Prędkość (km/h lub mph) i tablica rejestracyjna są obsługiwane tylko przez kamerę AXIS Q1686-DLE Radar-Video Fusion Camera.
- Aby korzystać z tych funkcji, trzeba włączyć prędkość (km/h lub mph) i tablicę rejestracyjną. Instrukcje znajdziesz w temacie *Konfiguracja kategorii wyszukiwania Axis, on page 108*.
- **Prędkość (km/h lub mph)**
  Pozwala wykrywać pojazdy poruszające się z określoną prędkością.
- **Tablica rejestracyjna**
  Pozwala wykrywać pojazdy z konkretną tablicą rejestracyjną. Tej funkcji można też używać do wyszukiwania tablic rejestracyjnych zawierających określone litery lub cyfry.
- **Kolor pojazdu**
  Detekcja pojazdów o wybranym kolorze.
- **Upper body clothing color (Kolor górnej część ubioru)**
  Detekcja ubrania w określonym kolorze na górnej części ciała.
- **Lower body clothing color (Kolor dolnej część ubioru)**
  Detekcja ubrania w określonym kolorze na dolnej ciała.
- **Godzina dnia**
  Detekcja obiektów wykrytych w określonej porze dnia. Ten filtr przydaje się przy wyszukiwaniu w okresie kilku dni, ale tylko w określonej porze, na przykład po południu.
- **Minimum time in scene (s) (Minimalny czas w scenie (s))**
  Detekcja obiektów wykrytych i śledzonych przez ustawioną minimalną liczbę sekund. Ten filtr odsiewa obiekty nieinteresujące dla użytkownika, na przykład znajdujące się obiekty i pozorne (efekty oświetleniowe). Wartość domyślna to 1 s. Oznacza to, że kiedy filtr jest ustawiony, wyklucza obiekty o czasie trwania przekraczającym 1 s.
- **Swaying objects (% of image) (Kołyszące się obiekty (% obrazu))**
  Wykluczanie obiektów, które się poruszyły tylko w ograniczonym obszarze, na przykład flag lub drzew poruszających się na wietrze. Wartość domyślna 5-100%. Oznacza to, że gdy filtr jest ustawiony, wyklucza obiekty, których zakres ruchu nie przekroczył 5% powierzchni obrazu.

Ograniczenia

- Uzyskanie prawidłowego materiału wideo w wynikach wyszukiwania wymaga odpowiedniej synchronizacji zegara.
- Informacje analizowane przez funkcję wyszukiwania do celów dochodzeniowych nie uwzględniają perspektywy sceny. W związku z tym wielkość i prędkość poruszającego się obiektu różnią się w zależności od jego odległości od kamery.
- Na dokładność wykrywania mogą mieć wpływ warunki atmosferyczne, takie jak ulewny deszcz lub śnieg.
- Analizy są tym dokładniejsze, im lepszy jest kontrast obiektu w scenach ze słabym oświetleniem.

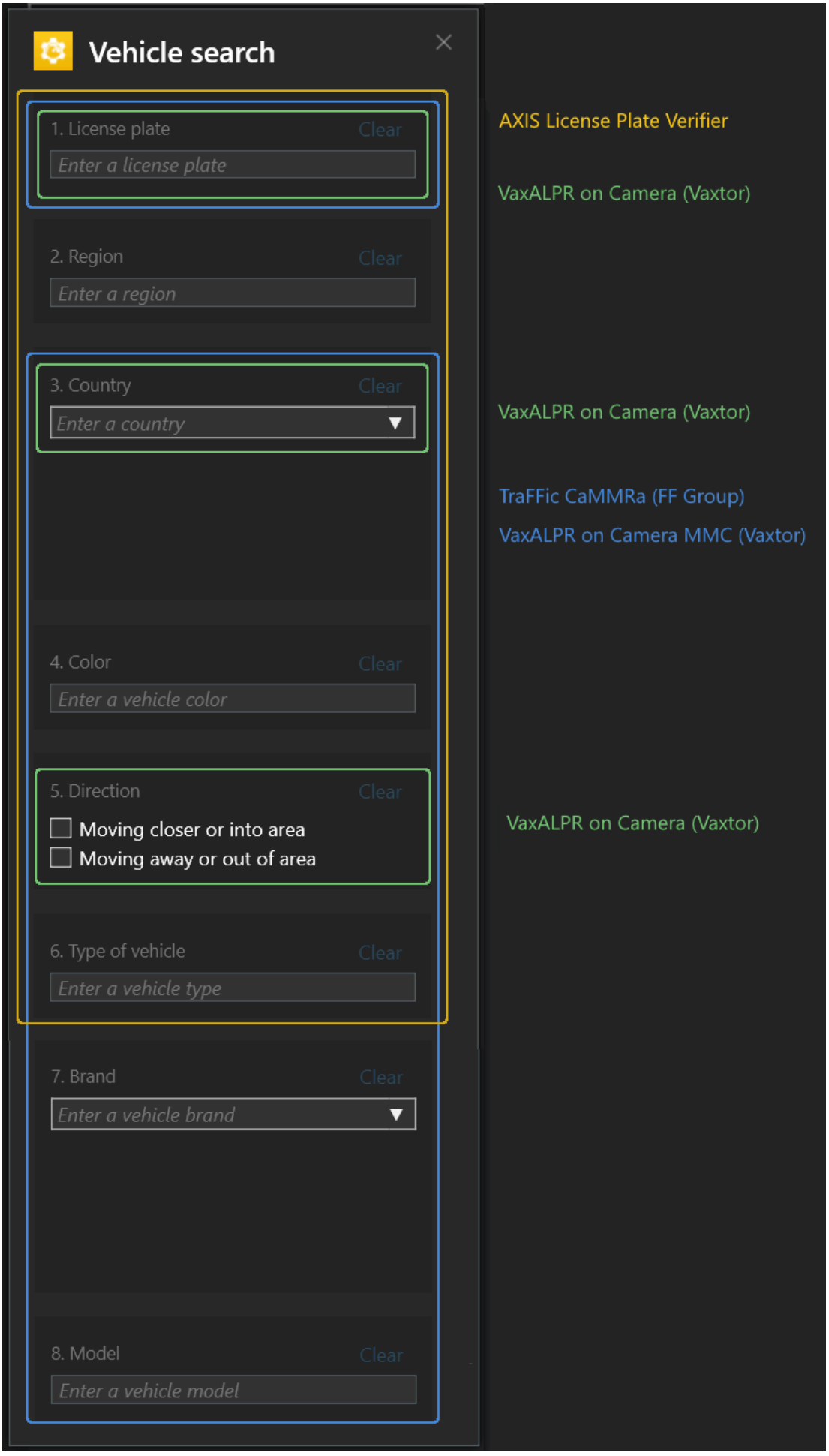
- Czasami jeden obiekt może generować kilka wyników. Może się tak zdarzyć, np. wtedy, gdy śledzenie obiektu zostanie przerwane z powodu zasłonięcia go przez inny obiekt.
- Nakładki mogą się różnić w zależności od wersji oprogramowania XProtect. Na przykład: obsługa nakładek w podglądzie wideo wymaga oprogramowania XProtect 2020 R3, a obsługa kolorów nakładek wymaga oprogramowania XProtect 2020 R2.
- Aby funkcja wyszukiwania do celów dochodzeniowych działała na strumieniach wideo obróconych o 180 stopni, należy:
  - zainstalować w kamerach system AXIS OS 10.6 lub nowszy, albo
  - zainstalować na serwerze zapisu oprogramowanie Device Pack 11.0 lub nowsze
- Warunkiem skutecznego wykrywania kolorów jest prawidłowe ustawienie balansu bieli w kamerze

Wyszukiwanie pojazdów

Używając aplikacji AXIS Optimizer wspólnie z niektórymi innymi aplikacjami zainstalowanymi w kamerze, można wyszukiwać, identyfikować i udostępniać wizyjny materiał dowodowy o pojazdach. Funkcja wyszukiwania pojazdów obsługuje dane tablic rejestracyjnych pochodzące z następujących aplikacji:

- *AXIS License Plate Verifier* firmy Axis Communications
- *CAMMRA AI* firmy FF Group (wymagana wersja 1.3 lub nowsza)
- *VaxALPR On Camera* firmy Vaxtor Recognition Technologies
- *VaxALPR On Camera MMC* firmy Vaxtor Recognition Technologies

Dostępność filtrów wyszukiwania zależy od aplikacji zainstalowanych w kamerach, p. *Zawężanie wyszukiwania, on page 55*.


Vehicle search
1. License plate
Clear
Enter a license plate
2. Region
Clear
Enter a region
3. Country
Clear
Enter a country
4. Color
Clear
Enter a vehicle color
5. Direction
Clear
Moving closer or into area
Moving away or out of area
6. Type of vehicle
Clear
Enter a vehicle type
7. Brand
Clear
Enter a vehicle brand
8. Model
Clear
Enter a vehicle model
AXIS License Plate Verifier
VaxALPR on Camera (Vaxtor)
VaxALPR on Camera (Vaxtor)
TraFFic CaMMRa (FF Group)
VaxALPR on Camera MMC (Vaxtor)
VaxALPR on Camera (Vaxtor)

Konfigurowanie wyszukiwania pojazdów

Uwaga

Wymagania

- System VMS:
  - Corporate lub Expert w wersji 2019 R3 lub nowszej
  - Professional+ lub Express+ w wersji 2022 R3 lub nowszej
- Czas kamery zsynchronizowany z NTP
- Jedna z aplikacji wymienionych w sekcji .

1. W aplikacji Management Client dodaj kamerę, na której jest uruchomiona wybrana aplikacja.
2. Włącz wszystkie potrzebne urządzenia. Aby można było korzystać z aplikacji AXIS License Plate Verifier, muszą być włączone pozycje Camera 1 i Metadata 1.
3. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
4. Konfigurowanie metadanych:
   4.1. Wybierz kolejno opcje **Site Navigation > Recording Server (Nawigacja po witrynie > Serwer zapisu)** i odszukaj urządzenie.
   4.2. Wybierz pozycję Metadata 1 (Metadane 1) i kliknij przycisk **Settings (Ustawienia)**.
   4.3. Wybierz kolejno opcje **Metadata stream > Event data (Strumień metadanych > Dane zdarzeń)** i kliknij przycisk **Yes (Tak)**.
5. Przejdź do karty **Record settings (Ustawienia zapisu)** i upewnij się, że włączono zapis metadanych.
6. Kliknij przycisk **Save (Zapisz)**.
7. Konfigurowanie aplikacji dla standardowego użytkownika:
   7.1. Dodaj uprawnienia odczytu i odtwarzania do konkretnej kamery i użytkownika.
   7.2. Dodaj uprawnienia odczytu i odtwarzania metadanych do konkretnej kamery i użytkownika.

Wyszukiwanie pojazdu

1. W aplikacji Smart Client kliknij przycisk **Search (Szukaj)**.
2. Wybierz przedział czasu oraz jedną lub kilka kamer.
3. Kliknij kolejno opcje **Search for > Vehicle search > New search (Wyszukaj > Wyszukiwanie pojazdu > Nowe wyszukiwanie)**.
4. Zaznacz filtry wyszukiwania, aby zawęzić listę zwracanych wyników.
   Aby dowiedzieć się więcej o różnych filtrach, p. *Zawężanie wyszukiwania, on page 55*.
5. Zaznacz wyniki wyszukiwania, którym chcesz się dokładniej przyjrzeć. Można na przykład dodać je do zakładek albo wykonać operacje opisane w temacie *Tworzenie raportu PDF o wysokiej jakości, on page 59*.

Zawężanie wyszukiwania

Aby zawęzić wyniki wyszukiwania, można zastosować jeden lub kilka filtrów wyszukiwania. Różne aplikacje oferują różne opcje filtrowania.

- **Tablica rejestracyjna**
  Znajdowanie konkretnego numeru tablicy rejestracyjnej.
  Aplikacja: AXIS License Plate Verifier, VaxALPR On Camera, CAMMRA AI lub VaxALPR On Camera MMC.
- **Region**

Znajdowanie pojazdów z określonego regionu.
Aplikacja: AXIS License Plate Verifier 2.9.19.

Uwaga

Określ lokalizację kamery w ustawieniach aplikacji AXIS License Plate Verifier, aby uzyskać optymalne rozpoznawanie regionu.

- **Kraj**
  Znajdowanie pojazdów z pewnego kraju.
  Aplikacja: AXIS License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI lub VaxALPR On Camera MMC.
- **Kolor**
  Znajdowanie pojazdów w określonym kolorze.
  Aplikacja: AXIS License Plate Verifier 2.9.19, CAMMRA AI lub VaxALPR On Camera MMC.
- **Kierunek**
  Znajdowanie pojazdów poruszających się w określonym kierunku.
  Aplikacja: AXIS License Plate Verifier 2.9.19, VaxALPR On Camera, CAMMRA AI lub VaxALPR On Camera MMC.
- **Typ pojazdu**
  Znajdowanie określonego typu pojazdu.
  Aplikacja: AXIS License Plate Verifier 2.9.19, CAMMRA AI lub VaxALPR On Camera MMC.
- **Marka**
  Znajdowanie określonej marki pojazdu.
  Aplikacja: CAMMRA AI lub VaxALPR On Camera MMC.
- **Model**
  Znajdowanie określonego modelu pojazdu.
  Aplikacja: CAMMRA AI lub VaxALPR On Camera MMC.

Optymalizacja szybkości wyszukiwania

Możesz zwiększyć szybkość wyszukiwania, kontrolując dane przechowywane przez system na urządzeniu VMS obsługującym metadane.

- Jeżeli nie potrzebujesz danych analitycznych, możesz je wyłączyć.
  - Otwórz menu **Devices (Urządzenia)** > **Metadata (Metadane)** i wybierz odpowiednie urządzenie.
  - Kliknij **Settings** (Ustawienia) i wyłącz **Analytics data** (Dane analityczne).
- Jeżeli potrzebujesz danych analitycznych, możesz skorzystać z zagregowanych metadanych, o ile są dostępne. Patrz *Metadane i wyszukiwanie, on page 107*.
- Wyłącz niepotrzebne zdarzenia w aplikacji AXIS License Plate Verifier. Aby działała aplikacja AXIS Optimizer, potrzebne jest jedynie zdarzenie **Lost** (Utracone). P. aplikacja *AXIS License Plate Verifier*.
- Upewnij się, że korzystasz z oprogramowania AXIS OS w wersji 12.8 lub nowszej.

Zone speed search (Wyszukiwanie prędkości w strefie)

W programie AXIS Optimizer można użyć funkcji wyszukiwania prędkości w strefie do wyszukiwania pojazdów przekraczających prędkość wykrytych podczas wjazdu do wcześniej określonej strefy w widoku kamery. Strefowe wyszukiwanie prędkości działa razem z aplikacją *AXIS Speed monitor* w celu wizualizacji prędkości pojazdów w strefie detekcji radarowej w podglądzie na żywo kamery. Dzięki funkcji AXIS Zone speed search można ustawić określone filtry w celu zawężenia wyników, a także eksportować i udostępniać dowody wideo podczas dochodzeń.

Konfiguracja wyszukiwania prędkości w strefie

Uwaga

Wymagania

- System VMS:

  - Corporate lub Expert w wersji 2019 R3 lub nowszej
  - Professional+ lub Express+ w wersji 2022 R3 lub nowszej
- Czas kamery zsynchronizowany z NTP

1. W aplikacji Management Client dodaj kamerę, na której jest uruchomiona wybrana aplikacja.
2. Włącz wszystkie potrzebne urządzenia. Aby można było korzystać z funkcji wyszukiwania prędkości w strefie dostępnej w rozwiązaniu AXIS, muszą być włączone pozycje Camera 1 i Metadata 1.
3. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
4. Aby skonfigurować metadane:
   4.1. Wybierz kolejno opcje **Site Navigation > Recording Server (Nawigacja po witrynie > Serwer zapisu)** i odszukaj urządzenie.
   4.2. Wybierz pozycję Metadata 1 (Metadane 1) i kliknij przycisk **Settings (Ustawienia)**.
   4.3. Wybierz kolejno opcje **Metadata stream > Event data (Strumień metadanych > Dane zdarzeń)** i kliknij przycisk **Yes (Tak)**.
5. Przejdź do karty **Record settings (Ustawienia zapisu)** i upewnij się, że włączono zapis metadanych.
6. Kliknij przycisk **Save (Zapisz)**.
7. Aby skonfigurować aplikację dla standardowego użytkownika:
   7.1. Dodaj uprawnienia odczytu i odtwarzania do konkretnej kamery i użytkownika.
   7.2. Dodaj uprawnienia odczytu i odtwarzania metadanych do konkretnej kamery i użytkownika.

Wyszukiwanie zdarzeń związanych z prędkością w strefie



1. W aplikacji Smart Client kliknij przycisk **Search (Szukaj)**.
2. Wybierz przedział czasu oraz jedną lub kilka kamer.
3. Kliknij kolejno opcje **Search for > Zone speed search > New search (Wyszukaj > Wyszukiwanie prędkości w strefie > Nowe wyszukiwanie)**.
4. Zaznacz filtry wyszukiwania, aby zawęzić listę zwracanych wyników.
   Aby dowiedzieć się więcej o różnych filtrach, p. *Zawężanie wyszukiwania, on page 57*.
5. Zaznacz wyniki wyszukiwania, którym chcesz się dokładniej przyjrzeć. Można na przykład dodać je do zakładek albo wykonać operacje opisane w temacie *Tworzenie raportu PDF o wysokiej jakości, on page 59*.

Zawężanie wyszukiwania

Aby zawęzić wyniki wyszukiwania zdarzeń przekroczenia prędkości, można zastosować jeden lub kilka filtrów wyszukiwania.

- **Max Speed (Prędkość maksymalna)**
  Filtrowanie maksymalnej prędkości dowolnego obiektu w strefie w czasie trwania zdarzenia. Można ustawić zarówno dolną, jak i górną granicę prędkości.

- **Typ obiektu**
  W przypadku wybrania obiektu **Vehicle (Pojazd)** narzędzie wyszukiwania pokaże tylko te zdarzenia przekroczenia prędkości, w których najszybszy obiekt w strefie został sklasyfikowany jako pojazd.
- **Nazwa strefy**
  Wyszukiwanie i filtrowanie stref według nazw.

Wyszukiwanie kontenerów

Używając aplikacji AXIS Optimizer wspólnie z niektórymi innymi aplikacjami, można wyszukiwać, identyfikować i udostępniać wizyjny materiał dowodowy o kontenerach. Funkcja wyszukiwania kontenerów obsługuje dane z następującej aplikacji:

- *VaxOCR Containers* firmy Vaxtor Recognition Technologies

Konfigurowanie wyszukiwania kontenerów

Uwaga

Wymagania

- System VMS:
  - Corporate lub Expert w wersji 2019 R3 lub nowszej
  - Professional+ lub Express+ w wersji 2022 R3 lub nowszej
- Czas kamery zsynchronizowany z NTP
- Aplikacja wymieniona w sekcji .

1. W aplikacji Management Client dodaj kamerę, na której jest uruchomiona wybrana aplikacja.
2. Włącz wszystkie potrzebne urządzenia.
3. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
4. Konfigurowanie metadanych:
   4.1. Wybierz kolejno opcje **Site Navigation > Recording Server (Nawigacja po witrynie > Serwer zapisu)** i odszukaj urządzenie.
   4.2. Wybierz pozycję Metadata 1 (Metadane 1) i kliknij przycisk **Settings (Ustawienia)**.
   4.3. Wybierz kolejno opcje **Metadata stream > Event data (Strumień metadanych > Dane zdarzeń)** i kliknij przycisk **Yes (Tak)**.
5. Przejdź do karty **Record settings (Ustawienia zapisu)** i upewnij się, że włączono zapis metadanych.
6. Kliknij przycisk **Save (Zapisz)**.
7. Konfigurowanie aplikacji dla standardowego użytkownika:
   7.1. Dodaj uprawnienia odczytu i odtwarzania do konkretnej kamery i użytkownika.
   7.2. Dodaj uprawnienia odczytu i odtwarzania metadanych do konkretnej kamery i użytkownika.

Wyszukiwanie kontenerów

1. W aplikacji Smart Client kliknij przycisk **Search (Szukaj)**.
2. Wybierz przedział czasu oraz jedną lub kilka kamer.
3. Kliknij kolejno opcje **Search for > Container search > New search (Wyszukaj > Wyszukiwanie kontenerów > Nowe wyszukiwanie)**.
4. Zaznacz filtry wyszukiwania, aby zawęzić listę zwracanych wyników.
   Aby dowiedzieć się więcej o różnych filtrach, p. *Zawężanie wyszukiwania, on page 59*.

5. Zaznacz wyniki wyszukiwania, którym chcesz się dokładniej przyjrzeć. Można na przykład dodać je do zakładek albo wykonać operacje opisane w temacie *Tworzenie raportu PDF o wysokiej jakości, on page 59*.

Zawężanie wyszukiwania

Aby zawęzić wyniki wyszukiwania, można zastosować jeden lub kilka filtrów wyszukiwania. Wszystkie opcje filtrowania pochodzą z aplikacji VaxOCR Containers.

- **Kod kontenera**
  Znajdowanie określonego kodu kontenera.
- **Właściciel**
  Znajdowanie kontenerów należących do określonego właściciela.
- **Owner code (Kod właściciela)**
  Znajdowanie kontenerów należących do określonego właściciela.
- **Rozmiar**
  Znajdowanie kontenerów o określonej wielkości i konkretnym typie.
- **Size code (Kod rozmiaru)**
  Znajdowanie kontenerów o określonej wielkości i konkretnym typie.
- **City or country (Miejscowość lub kraj)**
  Znajdowanie kontenerów z określonej miejscowości lub kraju.
- **Sprawdzanie**
  Znajdowanie kontenerów, które zostały już zweryfikowane na podstawie kodu właściciela lub cyfry kontrolnej.

Tworzenie raportu PDF o wysokiej jakości



Utwórz raport na podstawie wyników wyszukiwania. Funkcja pozwala dołączyć obrazy o wysokiej rozdzielczości do wyniku.

1. W aplikacji Smart Client wykonaj wyszukiwanie.
2. Zaznacz wyniki wyszukiwania, które chcesz uwzględnić w raporcie.
3. Kliknij kolejno opcje p,255mm,sfx)=″graphics:graphicFE51463A3463EF1848C7CD2F60A78298″ **> Create high quality PDF report** (Utwórz raport PDF w wysokiej jakości).
4. (Opcjonalnie) Wypełnij pola **Report name (Nazwa raportu)**, **Report destination (Lokalizacja docelowa raportu)** i **Notes (Uwagi)**.
5. Dla każdego wyniku wyszukiwania wybierz ramkę, jaką chcesz dołączyć do raportu. Aby powiększyć obraz, kliknij go dwukrotnie.
6. Kliknij polecenie **Create (Utwórz)**. Kiedy raport będzie gotowy, otrzymasz powiadomienie.

Axis license plates

W aplikacji Smart Client można dodać osobną kartę z funkcjami wyszukiwania tablic rejestracyjnych i zarządzania nimi. Karta centralizuje wszystkie zadania wykonywane przez operatora w zakresie zarządzania tablicami rejestracyjnymi, ich wyszukiwania i eksportowania na podstawie informacji dostarczanych przez kamery Axis wyposażone w funkcjonalność rozpoznawania tablic rejestracyjnych (LPR).



Zanim rozpoczniesz

- Upewnij się, że używasz systemu VMS w wersji 2018 R3 lub nowszej
- Upewnij się, że używasz VMS Device Pack w wersji 10.1 lub nowszej
- Czas kamery musi być zsynchronizowany z usługą NTP
- Użyj jednej z aplikacji wymienionych w sekcji .

Konfigurowanie aplikacji Axis do tablic rejestracyjnych

1. W aplikacji Management Client dodaj kamerę, na której jest uruchomiona wybrana aplikacja.
2. Włącz wszystkie potrzebne urządzenia. Aby można było korzystać z aplikacji AXIS License Plate Verifier, muszą być włączone pozycje Camera 1 i Metadata 1.
3. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
4. Konfigurowanie metadanych:
   4.1. Wybierz kolejno opcje **Site Navigation > Recording Server (Nawigacja po witrynie > Serwer zapisu)** i odszukaj urządzenie.
   4.2. Wybierz pozycję Metadata 1 (Metadane 1) i kliknij przycisk **Settings (Ustawienia)**.
   4.3. Wybierz kolejno opcje **Metadata stream > Event data (Strumień metadanych > Dane zdarzeń)** i kliknij przycisk **Yes (Tak)**.
5. Przejdź do karty **Record settings (Ustawienia zapisu)** i upewnij się, że włączono zapis metadanych.
6. Kliknij przycisk **Save (Zapisz)**.

Wyszukiwanie tablicy rejestracyjnej

1. W aplikacji Smart Client przejdź do aplikacji **Axis license plates**.
   Jeśli nie widzisz karty, wybierz kolejno opcje **Settings > Axis search options (Ustawienia > Opcje wyszukiwania Axis)** i kliknij opcję **Show license plate tab (Pokaż kartę tablic rejestracyjnych)**.
2. Kliknij przycisk **Add camera... (Dodaj kamerę)** i wybierz odpowiednie kamery > kliknij **Close (Zamknij)**.
   Tylko administrator może dodawać kamery do systemu. Gdy kamera wykryje tablice rejestracyjne, od razu pojawią się na liście wraz z przyciętymi obrazami tablic rejestracyjnych przechwyconych przez kamerę. Wynik wyszukiwania będzie zawierał maksymalnie 5000 pozycji.
3. Wprowadź numer rejestracyjny i kliknij przycisk **Time interval (Przedział czasowy)**, aby wyfiltrować wynik wyszukiwania.
   - W polu **Time interval (Przedział czasowy)** wprowadź niestandardową wartość z ustawionego zakresu, aby wyfiltrować wynik wyszukiwania.

Wyszukiwanie tablicy rejestracyjnej na żywo

1. W aplikacji Smart Client przejdź do aplikacji **Axis license plates**.
   Jeśli nie widzisz karty, wybierz kolejno opcje **Settings > Axis search options (Ustawienia > Opcje wyszukiwania Axis)** i kliknij opcję **Show license plate tab (Pokaż kartę tablic rejestracyjnych)**.

2. Kliknij przycisk **Add camera... (Dodaj kamerę)** i wybierz odpowiednie kamery > kliknij **Close (Zamknij)**. Tylko administrator może dodawać kamery do systemu. Gdy kamera wykryje tablice rejestracyjne, od razu pojawią się na liście wraz z przyciętymi obrazami tablic rejestracyjnych przechwyconych przez kamerę. Wynik wyszukiwania będzie zawierał maksymalnie 5000 pozycji.
3. Wprowadź numer rejestracyjny i kliknij kolejno opcje **Time interval (Przedział czasowy)** > **Live (Na żywo)**, aby filtrować wynik wyszukiwania.

Zawężanie wyszukiwania

Aby zawęzić wyniki wyszukiwania, można zastosować jeden lub kilka filtrów wyszukiwania.

- **Przedział czasowy**
  Filtrowanie na podstawie trafień wyszukiwania w określonym przedziale czasowym.
- **Tablica rejestracyjna**
  Filtrowanie częściowe lub pełne tekstu na tablicy rejestracyjnej.
- **Kamery**
  Filtrowanie na podstawie trafień wyszukiwania wykrytych przez określone kamery.
- **Kierunek**
  Filtrowanie według pojazdów poruszających się w określonym kierunku.
- **Listy**
  Filtrowanie trafień wyszukiwania w określonych lokalizacjach oraz filtrowanie trafień wyszukiwania na listach obiektów dozwolonych, blokowanych i niestandardowych. Więcej informacji na temat konfiguracji list, p. *Centralnie zarządzanie listami tablic rejestracyjnych, on page 23*.

Optymalizacja szybkości wyszukiwania

Możesz zwiększyć szybkość wyszukiwania, kontrolując dane przechowywane przez system na urządzeniu VMS obsługującym metadane.

- Jeżeli nie potrzebujesz danych analitycznych, możesz je wyłączyć.
  - Otwórz menu **Devices (Urządzenia)** > **Metadata (Metadane)** i wybierz odpowiednie urządzenie.
  - Kliknij **Settings** (Ustawienia) i wyłącz **Analytics data** (Dane analityczne).
- Jeżeli potrzebujesz danych analitycznych, możesz skorzystać z zagregowanych metadanych, o ile są dostępne. Patrz *Metadane i wyszukiwanie, on page 107*.
- Wyłącz niepotrzebne zdarzenia w aplikacji AXIS License Plate Verifier. Aby działała aplikacja AXIS Optimizer, potrzebne jest jedynie zdarzenie **Lost** (Utracone). P. aplikacja *AXIS License Plate Verifier*.
- Upewnij się, że korzystasz z oprogramowania AXIS OS w wersji 12.8 lub nowszej.

Eksportowanie wyników wyszukiwania tablic rejestracyjnych w formie raportu PDF

Ta funkcja umożliwia skompilowanie wybranych wyników wyszukiwania w postaci raportu PDF zawierającego obrazy o wysokiej jakości.

1. Kliknij przycisk **Export... (Eksportuj)**.
2. Zaznacz opcję **PDF...**.
3. (Opcjonalnie) Wypełnij pola **Report name (Nazwa raportu)**, **Report destination (Lokalizacja docelowa raportu)** i **Notes (Uwagi)**.
4. Dla każdego wyniku wyszukiwania wybierz ramkę, jaką chcesz dołączyć do raportu. Aby powiększyć obraz, kliknij go dwukrotnie.
5. Kliknij polecenie **Create (Utwórz)**. Kiedy raport będzie gotowy, otrzymasz powiadomienie.

Eksportowanie wyników wyszukiwania tablic rejestracyjnych w formie raportu CSV

Ta funkcja umożliwia skompilowanie dużej liczby wyników wyszukiwania w postaci raportu CSV.

1. Kliknij przycisk **Export... (Eksportuj)**.
2. Zaznacz opcję **CSV...**.
3. Wybierz lokalizację docelową dla eksportowanego pliku.

Funkcje analityczne Axis

Funkcje analityczne Axis zapewniają przegląd danych z urządzeń za pomocą wykresów i pulpitów nawigacyjnych. Możesz dzięki temu przeglądać metadane wszystkich posiadanych urządzeń. Możesz przeglądać dane o wykrytych obiektach, zidentyfikowanych pojazdach i alarmach. Możesz również tworzyć nowe pulpity nawigacyjne i udostępniać je innym użytkownikom.

Funkcje analityczne Axis są dostępne w domyślnych widokach administratora i operatora. W aplikacji Axis insights domyślny widok administratora jest dostępny wyłącznie dla użytkowników z uprawnieniami administratora, natomiast domyślny widok operatora - dla wszystkich operatorów posiadających odpowiednie uprawnienia. Zobacz *Konfigurowanie ustawień ról, on page 101*. Widok operatora udostępnia określone dane z wybranych skonfigurowanych widoków kamer, natomiast widok administratora udostępnia przegląd całego systemu.

Dostęp do aplikacji Axis insights

- Przejdź do aplikacji **Smart Client** i kliknij **Axis insights**.
- **Dashboard** (Pulpit nawigacyjny): Wybierz pulpit nawigacyjny z listy rozwijalnej.
- **Camera view (Widok kamery)**: Wybierz określony widok z kamery w celu uzyskania przeglądu danych.
- **Time range (Zakres czasu)**: Wybierz określony zakres czasu.
- **Auto update (Aktualizacja automatyczna)**: Włącz, aby automatycznie odświeżać dane.

••• Menu kontekstowe zawiera opcje:

- **Edit dashboard** (Edytuj pulpit nawigacyjny): Edytuj, udostępnij lub usuń pulpit nawigacyjny.
- **Add chart** (Dodaj wykres): Utwórz nowy wykres na pulpicie.
- **About Axis insights** (Informacje o Axis insights): Zapoznaj się w informacjami o aplikacji Axis insights.

••• Menu kontekstowe każdego wykresu zawiera następujące pozycje:

- **Maximize chart (Zmaksymalizuj wykres)**: Kliknij, aby powiększyć wykres.
- **Copy as image (Kopiuj jako obraz)**: Kliknij, aby skopiować wykres do schowka.
- **Export (Eksportuj)**: Kliknij, aby wyeksportować wykres w formacie PNG lub CSV.
- **Edit chart** (Edytuj wykres): Kliknij, aby edytować wykres.
- **Remove chart** (Usuń wykres): Kliknij, aby usunąć wykres.

Uwaga

- W przypadku niektórych wykresów można kliknąć ilustrację, aby wyświetlić dodatkowe informacje.
- : Przedstawia wybrane zaznaczenia dotyczące każdego wykresu na pulpicie nawigacyjnym.

Utwórz nowy pulpit nawigacyjny

1. **Dashboard** (Pulpit nawigacyjny): Wybierz **Add dashboard** (Pulpit nawigacyjny) z listy rozwijalnej.
2. Kliknij **Empty** (Pusty), aby utworzyć nowy pulpit nawigacyjny, lub kliknij **From existing dashboard** (Z istniejącego pulpitu nawigacyjnego), aby utworzyć pulpit nawigacyjny podobny do jednego z dostępnych w systemie.
3. **Name (Nazwa)**: Wpisz nazwę pulpitu nawigacyjnego.

4. **Allow other users to view this dashboard** (Zezwól innym użytkownikom na wyświetlanie tego pulpitu nawigacyjnego): Kliknij, aby udostępnić swój pulpit nawigacyjny innym użytkownikom w trybie tylko do odczytu.
5. Kliknij przycisk **Apply (Zastosuj)**.
6. **Add chart** (Dodaj wykres): Kliknij, aby dodać nowy wykres.
   - **Select chart type** (Wybierz rodzaj wykresu): Wybierz potrzebny rodzaj wykresu i kliknij **Next** (Dalej). Rodzaj wykresu można wyszukać za pomocą znaczników lub nazw wykresów, takich jak analiza obrazu, pojazdy, wykresy liniowe itp.
   - **Modify data selections** (Zmień wybór danych): Wybierz odpowiednie filtry w każdej kategorii.
   - **Adjust appearance** (Dostosuj wygląd): Edytuj teksty i wybierz wielkość wykresu.

Konfiguracja listy rozwijalnej na pulpicie nawigacyjnym

Uwaga

- Domyślnie widoczne są tylko utworzone przez użytkownika pulpity nawigacyjne.

Aby wyświetlić pulpity nawigacyjne udostępnione przez innych użytkowników na liście rozwijanej **Dashboard** (Pulpity nawigacyjne):

1. Przejdź do **Shared dashboards** (Udostępnione pulpity nawigacyjne).
2. Włącz przełącznik obok każdego udostępnionego pulpitu nawigacyjnego, który chcesz dodać do listy rozwijalnej.

Wyświetlanie wyników analiz dla danego widoku z kamery

Przy podglądzie na żywo bądź odtwarzaniu nagrania z kamery możesz otworzyć aplikację Axis Insights z automatycznie wybranym aktywnym widokiem z kamery.

Aby otworzyć Axis Insights dla konkretnego obszaru obserwacji kamery:

1. Przejdź do **Smart Client** i otwórz obszar obserwacji.
2. Kliknij **Show insights (Pokaż statystyki)**.

Konfigurowanie funkcji analitycznych Axis

1. Sprawdź, czy kamera obsługuje oprogramowanie Axis Object Analytics. Zobacz funkcje analityczne w *Selektorze produktów Axis*.
2. Sprawdź, czy data i godzina w kamerze są ustawione prawidłowo.
3. W aplikacji Management Client upewnij się, że urządzenie dostarczające metadane jest włączone dla kamer.
4. Sprawdź, czy urządzenie generujące metadane jest powiązane z kamerą:
   - Przejdź do pozycji **Devices** > **Camera** (Urządzenia > Kamera) i wybierz urządzenie.
   - Przejdź do karty **Client** (Klient) i sprawdź, czy w obszarze **Related metadata** (Powiązane metadane) wybrane jest urządzenie generujące metadane kamery.
5. Aby wyświetlić wszystkie dostępne dane w aplikacji Axis Insights, włącz analizę sceny w kamerze za pomocą aplikacji *AXIS Scene Metadata*:
   5.1. Otwórz menu **Devices (Urządzenia)** > **Metadata (Metadane)** i wybierz odpowiednie urządzenie.
      - Kliknij polecenie **Record (Nagrywaj)** i upewnij się, że jest aktywna funkcja **Recording (Nagrywanie)**.
      - Kliknij **Settings** (Ustawienia) i sprawdź, czy jest włączona opcja **Analytics data** (Dane analityczne).

   5.1. Włącz **Consolidated metadata (Skonsolidowane metadane)**, aby skrócić czas ładowania, jeśli opcja ta jest dostępna. Patrz *Metadane i wyszukiwanie, on page 107*.

6. Aby włączyć dane dla rodzajów wykresów przy użyciu aplikacji *AXIS Object Analytics*, *AXIS Image Health Analytics* lub funkcji *Environmental sensors* (Czujniki środowiskowe):
   - Otwórz menu **Devices (Urządzenia)** > **Metadata (Metadane)** i wybierz odpowiednie urządzenie.
   - Kliknij polecenie **Record (Nagrywaj)** i upewnij się, że jest aktywna funkcja **Recording (Nagrywanie)**.
   - Kliknij **Settings (Ustawienia)** i upewnij się, że jest zaznaczona opcja **Event data (Dane zdarzenia)**.
   - Zaleca się utworzenie reguły w systemie VMS, aby zawsze zapisywać metadane z tego urządzenia.
7. Ustaw uprawnienia dla grup zabezpieczeń:
   7.1. Wybierz kolejno opcje **Site Navigation (Nawigacja w lokalizacji)** > **Security (Zabezpieczenia)** > **Roles (Role)**.
   7.2. Wybierz rolę.
   7.3. Przejdź do okna **Cameras (Kamery)**. Wybierz opcję **Read (Odczyt)**.
   7.4. Przejdź do okna **Metadata (Metadane)**. Wybierz opcje **Read (Odczyt)**, **Live (Na żywo)** i **Playback (Odtwarzanie)**.
8. Aby dowiedzieć się, jak dodać metadane tablicy rejestracyjnej do statystyk Axis, zob. *Konfigurowanie aplikacji Axis do tablic rejestracyjnych, on page 60*

Rozwiązywanie problemów z aplikacją Axis insights

Problem	Rozwiązanie
Na wykresach widać „brak danych".	Należy skonfigurować aplikację Axis Insights. Patrz *Konfigurowanie funkcji analitycznych Axis, on page 63*.
Wczytywanie widoku operatora trwa bardzo długo.	• Zmniejsz zakres czasu. • Utwórz obszar obserwacji kamery z mniejszą ilością liczbą kamer do analizy scen. • Aby włączyć skonsolidowane metadane, patrz: *Metadane i wyszukiwanie, on page 107*.

Korekcja obrazu wideo

Funkcja korekcji zniekształceń spłaszcza i koryguje perspektywę geometrycznie zniekształconego obrazu powstałego wskutek użycia obiektywu szerokokątnego lub typu „rybie oko". Funkcja korekcji zniekształceń Axis w systemie VMS może współpracować z dowolną kamerą panoramiczną Axis o kącie widzenia 360°. Usuwanie zniekształceń odbywa się bezpośrednio w kamerze lub w aplikacji Smart Client.

Więcej informacji o usuwaniu zniekształceń:

- Stosowanie korekcji zniekształceń po stronie klienta pozwala uzyskać płynne usuwanie zniekształceń w obrazie filmowym na żywo i nagrywanym.
- Powrót do widoku powoduje automatyczne przejście do ostatniej lokalizacji korygowania zniekształceń.
- Korekcja zniekształceń jest uruchamiana automatycznie podczas eksportowania materiału filmowego.
- Aby zapisać pozycję domową, p. *Ustawianie pozycji domowej, on page 67*.
- Można pozwolić lub zabronić operatorom kontrolowania i edytowania widoków skorygowanych, p. *Zezwalanie operatorom na kontrolowanie i edytowanie widoków z korekcją krzywizn, on page 68*.

Tworzenie widoku z korekcją krzywizn

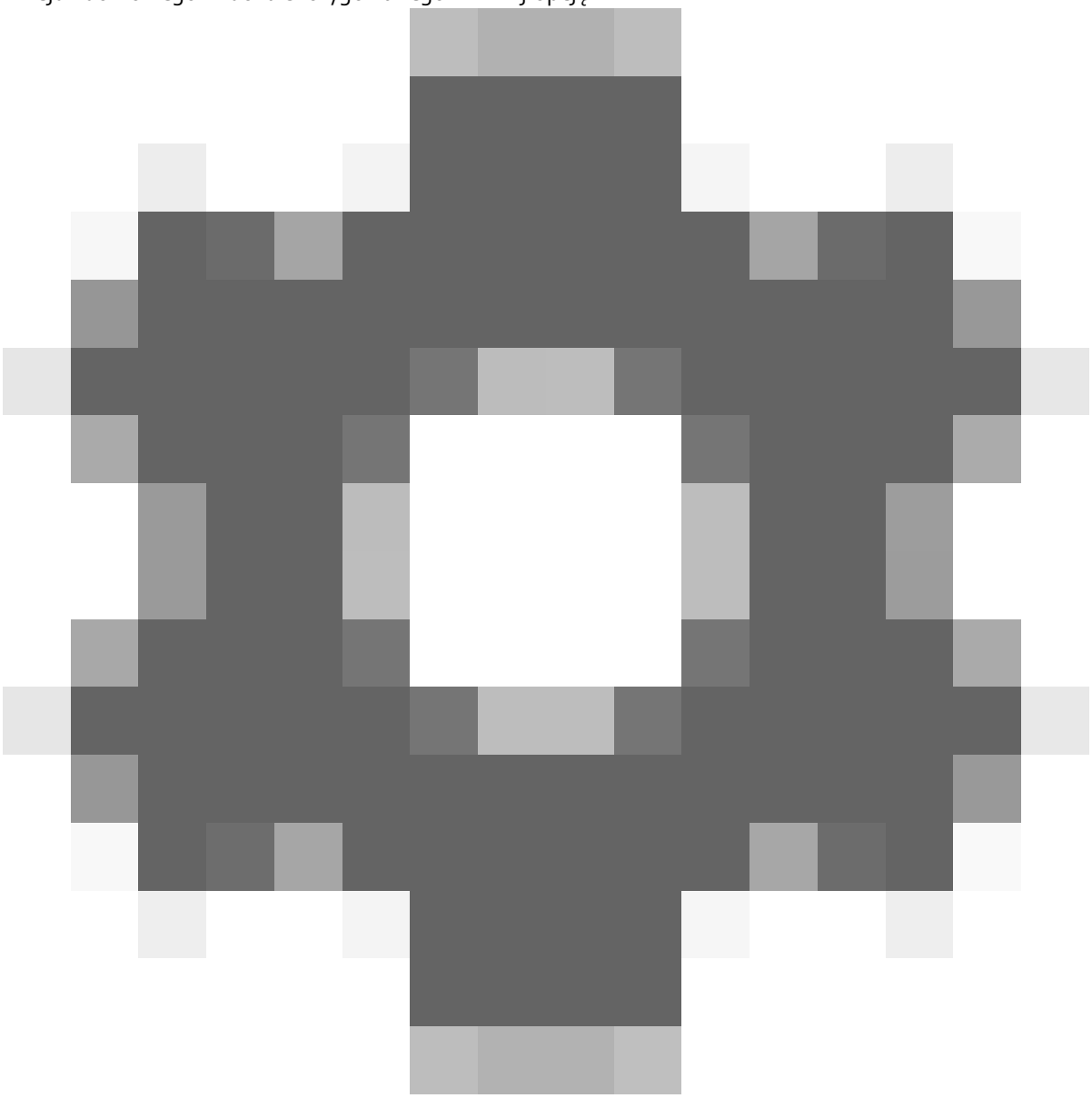


Uwaga

Aby zoptymalizować strumień służący usuwaniu zniekształceń obrazu, wybierz maksymalną dostępną rozdzielczość w ustawieniu **Video stream 1 (Strumień wideo 1)** w obszarze **Camera 1 (Kamera 1)** w aplikacji Management Client. Aby uzyskać dodatkowe informacje, zob. *Wydajność i rozwiązywanie problemów, on page 68*.

1. Otwórz narzędzie Smart Client i kliknij opcję **Setup (Ustawienia)**.
2. Przejdź do obszaru **Views (Widoki)**.
3. Kliknij polecenie **Create new view (Utwórz nowy widok)** i wybierz format.
4. Przejdź do menu **System overview > AXIS Optimizer (Przegląd systemu > AXIS Optimizer)**.
5. Kliknij opcję **Dewarping view (Widok korekcji zniekształceń)** i przeciągnij ją do widoku.
6. Wybierz kamerę i obecną pozycję montażową kamery.
7. Kliknij opcję **Setup (Ustawienia)**.

8. Przejdź do nowego widoku skorygowanego i kliknij opcję



.

9. Kliknij przycisk **Set view type (Ustaw typ widoku)** i wybierz jedną z opcji. Zależnie od sposobu zamontowania kamery można wybrać ustawienie **Quad (Poczwórny)**, **Normal (Normalny)**, **Normal with overview (Normalny z całościowym podglądem)** lub **Panorama**.

Uwaga

Zalecamy używanie rozdzielczości DPI 100%. Przy rozdzielczości innej niż 100% korekcja zniekształcenia Axis na drugim monitorze może nie być w pełni widoczna.

W przypadku używania innych ustawień DPI okno usuwania zniekształceń może być widoczne tylko częściowo. Aby rozwiązać ten problem, postępuj zgodnie z instrukcjami zawartymi w tych zewnętrznych artykułach:

- *Problemy z systemem XProtect na ekranach o wysokiej rozdzielczości (4K i wyższej)*
- *Skalowanie interfejsu GUI urządzenia klienckiego na ekranach o dużej wartości DPI*

Tworzenie widoku z korekcją krzywizn w przypadku wieloprzetwornikowych kamer panoramicznych

Widoki korekcji zniekształceń można tworzyć dla wieloprzetwornikowych kamer panoramicznych, takich jak AXIS P3807-PVE Network Camera i AXIS Q3819-PVE Panoramic Camera.

- Łączenie obrazów po stronie klienta. Jeżeli w kamerze zostanie włączony tryb rejestracji Client Dewarp (Korekcja po stronie klienta), aplikacja AXIS Optimizer połączy wszystkie cztery obrazy w jedną płynną panoramę (tylko w kamerach AXIS P3807-PVE).
- Korekta horyzontu. Istnieje możliwość korygowania horyzontu panoramy. Może to być przydatne, jeżeli kamera jest pochylona w stronę podłoża, a ziemski horyzont ma zakrzywienie. Korekta pozwoli również bardziej intuicyjnie sterować wirtualnymi ustawieniami PTZ.
- Sterowanie PTZ. Umożliwia przybliżanie/oddalanie widoku i poruszanie się po nim analogicznie jak w prawdziwej kamerze PTZ.



Uwaga

Wymagania

- Użytkownicy posiadający jedno z następujących uprawnień:
  - Rola optymalizatora
  - Hardware > Driver commands = Allow (Sprzęt > Polecenia sterujące = Zezwalaj)
- Wieloprzetwornikowa kamera panoramiczna Axis

1. W razie potrzeby w trakcie początkowego konfigurowania urządzenia ustaw tryb rejestrowania **Client Dewarp (Korekcja po stronie klienta)**.
2. Otwórz narzędzie Smart Client i kliknij opcję **Setup (Ustawienia)**.
3. Przejdź do obszaru **Views (Widoki)**.
4. Kliknij polecenie **Create new view (Utwórz nowy widok)** i wybierz format.
5. Przejdź do menu **System overview > AXIS Optimizer (Przegląd systemu > AXIS Optimizer)**.
6. Kliknij opcję **Dewarping view (Widok korekcji zniekształceń)** i przeciągnij ją do widoku.
7. Wybierz wieloprzetwornikową kamerę panoramiczną.
   Gdy wieloprzetwornikowa kamera panoramiczna jest dodawana do widoku korekcji zniekształceń po raz pierwszy, nad widokiem pojawia się okno kalibracji horyzontu.
8. Kliknij strzałki, aby wyrównać czerwoną linię do ziemskiego horyzontu.
9. Kliknij przycisk **Done (Gotowe)**, aby zapisać ustawienia i wyjść z trybu kalibracji.

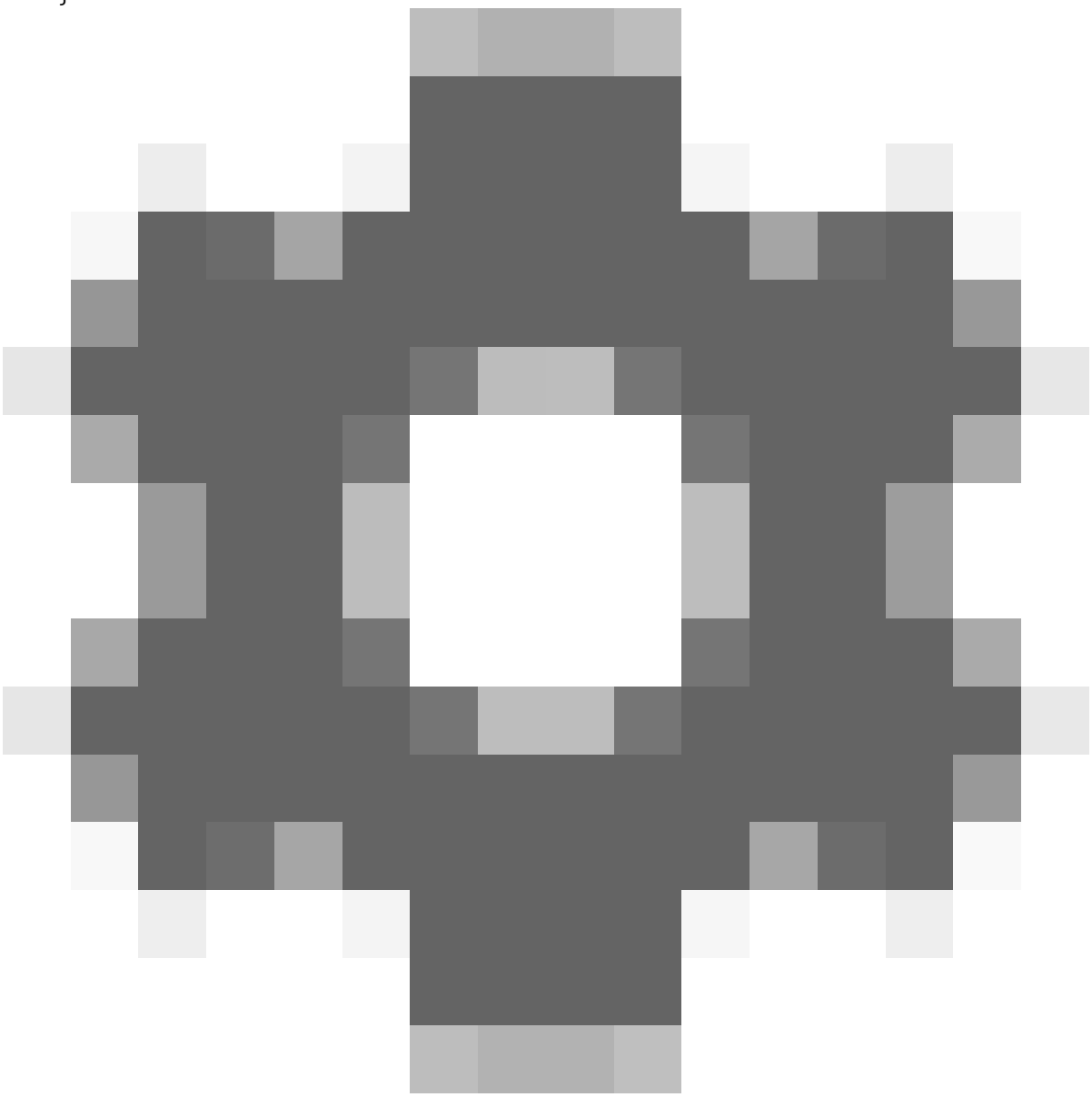
Widok szeroki

Widok szeroki jest przeznaczony do wieloprzetwornikowych kamer panoramicznych. Włącz **wide view (widok szeroki)**, jeśli normalne pole widzenia 120° nie wystarczy. W przypadku widoku szerokiego obraz będzie zawsze pozbawiony zniekształceń. Wyłącz **wide view (widok szeroki)**, aby przejść do normalnego widoku po całkowitym pomniejszeniu.

Ustawianie pozycji domowej

1. W aplikacji Smart Client otwórz widok korekcji zniekształceń.
2. Przejdź do położenia, które chcesz zapisać jako pozycję domową.

3. Kliknij



, a następnie **Set home position** (Ustaw pozycję domową).

Zezwalanie operatorom na kontrolowanie i edytowanie widoków z korekcją krzywizn

Można pozwolić lub zabronić operatorom kontrolowania i edytowania widoków skorygowanych, p. *Dostęp do ustawień funkcji dla operatorów, on page 101*.

Wydajność i rozwiązywanie problemów

Kwestie wydajności

- W miarę możliwości korekcja zniekształceń obrazu filmowego Axis odbywa się w procesorze graficznym (GPU), ale w pewnym stopniu obciąża również główny procesor komputera (CPU).
- Aby poklatkowość nie spadała w dużym widoku z wieloma widokami korekcji zniekształceń, należy wziąć pod uwagę następujące kwestie:
  - Rozdzielczość kamery. Wysoka rozdzielczość kamery, na przykład 2880 x 2880, wymaga znacznie więcej mocy obliczeniowej niż na przykład rozdzielczość 1920 x 1920.
  - Poklatkowość kamery. Jeżeli nie potrzebujesz wysokiej poklatkowości, ustaw niższą, co zapobiegnie zacinaniu się obrazu w widoku korekcji zniekształceń i innych widokach.

– Rozdzielczość monitora. Monitory o wysokiej rozdzielczości, na przykład 4K, potrzebują dużo zasobów do wyświetlania obrazu filmowego. Jeżeli nie potrzebujesz tak wysokiej rozdzielczości, lepiej używać mniejszej, ponieważ więcej widoków z korekcją zniekształceń będzie wyświetlanych bez zacinania.

Rozdzielczość dynamiczna

- W miarę możliwości strumień wideo będzie przesyłany w niższej rozdzielczości bez pogarszania jakości obrazu. Może to usprawnić wyświetlanie widoków korekcji zniekształceń.
- Jeżeli podczas przybliżania z widoku ogólnego występuje migotanie, warto spróbować wyłączyć rozdzielczość dynamiczną.
- Aby włączyć lub wyłączyć rozdzielczość dynamiczną: w aplikacji Smart Client przejdź do **Settings > Axis dewarping options > Rendering options** (Ustawienia > Opcje widoku skorygowanego Axis > Opcje renderowania) i wybierz lub usuń zaznaczenie **Dynamic resolution** (Rozdzielczość dynamiczna).
- Domyślnie opcja **Dynamic resolution (Rozdzielczość dynamiczna)** jest włączona.

Renderowanie w zgodności

- Jeżeli na obrazie poddanym korekcji zniekształceń występują jakieś problemy wizualne, na przykład okno jest całe czarne, lub jeśli korekcja trwa dłużej niż oczekiwano, można włączyć funkcję renderowania w zgodności. Należy pamiętać, że funkcja ta może również powodować efekt negatywny polegający na migotaniu przy przechodzeniu między widokami oraz szybkim podglądzie podczas odtwarzania.
- Aby włączyć lub wyłączyć renderowanie w zgodności: w aplikacji Smart Client przejdź do **Settings > Axis dewarping options > Rendering options** (Ustawienia > Opcje widoku skorygowanego Axis > Opcje renderowania) i wybierz lub usuń zaznaczenie **Use compatibility rendering** (Użyj renderowania w zgodności).
- Domyślnie funkcja **Use compatibility rendering (Użyj renderowania w zgodności)** jest wyłączona.

Czego się spodziewać

W systemie referencyjnym zawierającym procesor Intel i7 8700, kartę graficzną NVIDIA Geforce 1050 GTX i trzy monitory o rozdzielczości 1920x1080 można oczekiwać następujących zachowań:

- 7 widoków korekcji zniekształceń przy rozdzielczości 1920x1920 i klatkażu 25 kl./s może być generowanych bez gubienia klatek, lub
- 4 widoki korekcji zniekształceń przy rozdzielczości 2880x2880 i klatkażu 25 kl./s

Jeżeli jeden z trzech monitorów pracuje w rozdzielczości 4K zamiast 1920x1080, można się spodziewać następujących zachowań:

- 5 widoków korekcji zniekształceń przy rozdzielczości 1920x1920 i klatkażu 25 kl./s może być generowanych bez gubienia klatek, lub
- 3 widoki korekcji zniekształceń przy rozdzielczości 2880x2880 i klatkażu 25 kl./s Jeden widok korekcji zniekształceń na każdym monitorze.

Skale poklatkowości i rozdzielczości są liniowe. Komputer zdolny obsłużyć 5 widoków korekcji zniekształceń z klatkażem 30 kl./s obsłuży 10 widoków po zmniejszeniu klatkażu do 15 kl./s.

Integracja urządzeń nasobnych

Aplikacja AXIS Optimizer Body Worn Extension umożliwia kamerze pracującej w terenie nagrywanie, oznaczanie i udostępnianie filmów śledczym w biurze, którzy następnie w systemie VMS mogą wyszukiwać dowody wizualne i nimi zarządzać. Usługa zapewnia bezpieczne połączenie i przesyłanie danych między systemem nasobnym Axis a systemem VMS. AXIS Body Worn Extension to bezpłatna samodzielna usługa (aplikacja), którą należy zainstalować na serwerze zapisu.

Uwaga

Obsługiwane wersje:

- VMS w wersji 2020 R1 Corporate lub nowszej
- VMS w wersji 2020 R1 Professional+ lub nowszej
- VMS w wersji 2020 R1 Expert lub nowszej

Zawsze używaj najnowszych poprawek technicznych VMS i zbiorczych instalatorów poprawek.

Dowiedz się więcej

- Aby pobrać samą usługę lub przeczytać przewodnik po integracji i uwagi do rozwiązania, przejdź do witryny *axis.com*.
- Aby przeczytać podręcznik użytkownika, przejdź do witryny *axis.help.com*.

Kontrola dostępu

Kontrola dostępu to rozwiązanie łączące fizyczną kontrolę dostępu z dozorem wizyjnym. Takie połączenie umożliwia skonfigurowanie systemu kontroli dostępu Axis bezpośrednio z poziomu aplikacji Management Client. System bezproblemowo integruje się z oprogramowaniem XProtect, dzięki czemu operatorzy mają możliwość monitorowania dostępu i wykonywania działań związanych z kontrolą dostępu w aplikacji Smart Client.

Uwaga

Wymagania

- Wersja systemu VMS 2024 R1 lub nowsza.
- Licencje dostępowe do oprogramowaniem XProtect, p. pkt *Licencje dostępowe*.
- Zainstaluj aplikację AXIS Optimizer na serwerze zdarzeń i kliencie Management Client.

Porty 53459 i 53461 zostaną otwarte dla ruchu przychodzącego (TCP) przy instalacji aplikacji AXIS Optimizer poprzez aplikację AXIS Secure Entry.

Aby korzystać z funkcji obsługi drzwi w systemie AXIS Secure Entry, uzyskaj licencję na każde drzwi, p. sekcja *Uaktywnienie licencji dot. drzwi, on page 72*.

Konfiguracja kontroli dostępu

Uwaga

Na początek wykonaj następujące czynności:

- Zaktualizuj oprogramowanie układowe kontrolera drzwiowego. W poniższej tabeli przedstawiono minimalną i zalecaną wersję oprogramowania układowego AXIS OS dla danej wersji programu VMS.
- Sprawdź, czy data i godzina są prawidłowe.

AXIS Optimizer w wersji	Minimalna wersja systemu AXIS OS	Zalecana wersja systemu AXIS OS
6.0	12.6.94.1	12.10.73.4
5.8	12.6.94.1	12.8.55.1
5.6	12.6.94.1	12.6.94.1

Dodawanie sieciowego kontrolera drzwiowego Axis do systemu

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu).
2. W sekcji **Configuration** (Konfiguracja) wybierz **Devices** (Urządzenia).
3. Wybierz **Discovered devices** (Wykryte urządzenia), aby wyświetlić listę urządzeń, które można dodać do systemu.
4. Wybierz urządzenia, które chcesz dodać.
5. Kliknij **+ Add** (Dodaj) w wyskakującym okienku i podaj dane uwierzytelniające dla kontrolera.

Uwaga

- Dodane kontrolery powinny być widoczne na karcie **Management** (Zarządzanie).
- Aby ręcznie dodać kontroler do systemu, kliknij przycisk **+ Add** (Dodaj) na karcie **Management** (Zarządzanie).
- Aby uwzględnić zmiany w systemie VMS za każdym razem, gdy dodajesz, usuwasz lub edytujesz nazwę kontrolera drzwiowego:
  - Przejdź do **Site Navigation** > **Access control** (Nawigacja po obiekcie > Kontrola dostępu) i kliknij Access Control integration (Integracja kontroli dostępu).
  - Kliknij **Refresh Configuration** (Odśwież konfigurację) na karcie **General settings** (Ustawienia ogólne).

Uaktywnienie licencji dot. drzwi

Drzwi będziesz mógł dodać po uaktywnieniu posiadanych w systemie licencji.

1. W sekcji **Site Navigation** (Nawigacja po obiekcie) przejdź do **License Information** (Informacje o licencji).
2. Kliknij **Activate License Manually** (Uaktywnij licencję ręcznie) i wybierz **Online** lub **Offline**.
3. Aby uaktywnić licencje dot. drzwi w trybie online:
   – Wprowadź swoją nazwę użytkownika i hasło.
4. Aby uaktywnić licencje dot. na drzwi w trybie offline, p. sekcja *Uaktywnienie licencji w trybie offline*.

Jeżeli chcesz zmienić liczbę licencji dot. drzwi, które mają zostać uaktywnione:

1. Przejdź do **AXIS Optimizer** > **Access control** (AXIS Optimizer > Kontrola dostępu).
2. W sekcji **Configuration** (Konfiguracja) wybierz **Devices** (Urządzenia).
3. Przejdź do **Allocated door licenses** > **Custom license allocation** (Przydzielone licencje dot. drzwi > Przydzielanie licencji niestandardowych) i wpisz liczbę licencji dot. drzwi, z których chcesz korzystać.
4. Kliknij przycisk **Apply (Zastosuj)**.
5. Przejdź do **License Information** (Informacje o licencji) i ponownie uaktywnij swoje licencje.

Skonfiguruj kontrolę dostępu

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu).
2. Aby edytować predefiniowane profile identyfikacji lub utworzyć nowy profil identyfikacji, zob. *Profile identyfikacji, on page 88*.
3. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, zob. *Formaty kart i kod PIN, on page 84*.
4. Dodaj drzwi i zastosuj do nich profil identyfikacji. Zob. *Dodaj drzwi, on page 75*.
5. Dodaj strefę, a następnie drzwi do strefy. Zob. *Dodawanie strefy, on page 82*.

Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

Ważne

Przy aktualizowaniu systemu AXIS OS w kontrolerze drzwiowym pamiętaj o następujących kwestiach:

- **Obsługiwane wersje oprogramowania układowego AXIS OS**: Wymienione powyżej obsługiwane wersje systemu (oprogramowania układowego) AXIS OS mają zastosowanie tylko w przypadku wykonywania aktualizacji z oryginalnej zalecanej wersji programu VMS i gdy system zawiera drzwi. Jeżeli system nie spełnia tych warunków, należy dokonać aktualizacji do wersji systemu AXIS OS zalecanej dla konkretnej wersji systemu VMS.
- **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 aplikacji AXIS Optimizer w wersji 6.0 i aktualizujesz wszystkie urządzenia do zalecanej wersji oprogramowania układowego AXIS OS 12.10.73.4. W związku z tym wersja oprogramowania AXIS OS 12.6.94.1 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 systemu VMS. 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 systemu VMS.
- **Przyszłe zalecenia dotyczące oprogramowania AXIS OS**: Aby zapewnić stabilność systemu i pełną zgodność, należy zawsze przestrzegać wersji oprogramowania AXIS OS zalecanej dla danej wersji systemu VMS.

Integracja systemu kontroli dostępu

Aby zintegrować system kontroli dostępu z systemem VMS:

1. Przejdź do **Site Navigation** > **Access Control** (Nawigacja po obiekcie > Kontrola dostępu).
2. Kliknij prawym przyciskiem myszy **Access Control** (Kontrola dostępu) i kliknij **Create new...** (Utwórz nową...).
3. W oknie dialogowym **Create Access Control System Integration** (Utwórz integrację systemu kontroli dostępu):
   - Wpisz nazwę integracji.
   - Z rozwijalnego menu w pozycji **Integration plug-in** (Wtyczka integracji) wybierz **AXIS Secure Entry**.
   - Klikaj **Next** (Dalej), aż pojawi się okno dialogowe **Associate cameras** (Powiąż kamery).
     Aby powiązać kamery z punktami dostępowymi drzwi:
     - Kliknij urządzenie w sekcji **Cameras** (Kamery), aby wyświetlić listę kamer skonfigurowanych w systemie XProtect.
     - Zaznacz kamerę i przeciągnij ją do punktu dostępowego, z którym chcesz ją powiązać.
     - Kliknij **Close** (Zamknij), aby zamknąć okno dialogowe.

Uwaga

- Więcej informacji na temat integracji systemu kontroli dostępu w oprogramowaniu XProtect znajduje się w sekcji *Korzystanie z systemu kontroli dostępu w kliencie XProtect Smart Client*.
- Więcej informacji na temat właściwości systemu kontroli dostępu, takich jak ustawienia ogólne, drzwi i powiązane kamery, zdarzenia kontroli dostępu itp., znajduje się w sekcji *Właściwości kontroli dostępu*.

Drzwi i strefy

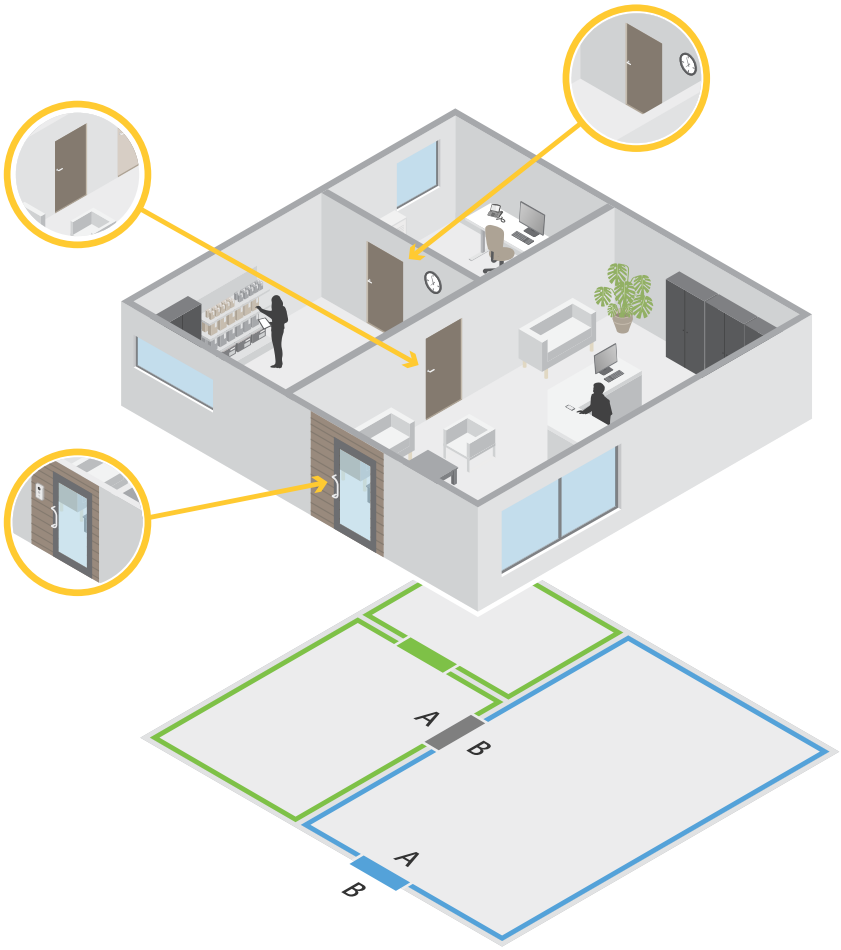
Przejdź do **Site Navigation** > **AXIS Optimizer** >**Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy), aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

Przypnij wykres	Wyświetlić schemat styków kontrolera drzwi. Jeżeli chcesz wydrukować tabelę rozkładu styków, kliknij **Print** (Drukuj).
Profil identyfikacji	Zmień profil identyfikacji w drzwiach.
Bezpieczny kanał	Włącz lub wyłącz bezpieczny kanał OSDP dla konkretnego czytnika.

Drzwi	
Nazwa	Nazwa drzwi.
Kontroler drzwi	Kontroler drzwi, z którym są połączone drzwi.
Strona A	Strefa, w której znajduje się strona A drzwi.
Strona B	Strefa, w której znajduje się strona B drzwi.
Profil identyfikacji	Profil identyfikacji przypisany do drzwi.
Formaty kart i kod PIN	Pokazuje typ formatów kart lub długość kodu PIN.
Status	Status drzwi. • **Online:** Drzwi są w trybie online i działają prawidłowo. • **Reader offline (Czytnik w trybie offline):** Czytnik podany w konfiguracji drzwi jest w trybie offline.

	• **Reader error (Błąd czytnika):** Czytnik podany w konfiguracji drzwi nie obsługuje bezpiecznego kanału albo dla czytnika nie włączono bezpiecznego kanału.
Strefy	
Nazwa	Nazwa strefy.
Liczba drzwi	Liczba drzwi należących do strefy.

Przykład drzwi i stref



- Istnieją dwie strefy: zielona i niebieska.
- Istnieje troje drzwi: zielone, niebieskie i brązowe.
- Zielone drzwi są wewnętrznymi drzwiami w zielonej strefie.
- Niebieskie drzwi są drzwiami obwodowymi wyłącznie niebieskiej strefy.
- Brązowe drzwi są drzwiami obwodowymi stref zielonej i niebieskiej.

Dodaj drzwi

Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku.
- Jeżeli kontroler drzwiowy nie ma drzwi, a Ty używasz nowej wersji aplikacji Axis Optimizer ze starszym oprogramowaniem w kontrolerze drzwiowym, system uniemożliwi dodanie drzwi. System zezwala jednak na tworzenie nowych drzwi na kontrolerach systemu ze starszym oprogramowaniem, jeżeli drzwi już istnieją.

Aby dodać drzwi poprzez utworzenie nowej konfiguracji drzwi:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **Add door (Dodaj drzwi)**.
3. Wprowadź nazwę drzwi.
4. Z rozwijalnego menu **Controller (Kontroler)** wybierz kontroler drzwi. Kontroler jest wyszarzony, gdy nie można dodać kolejnych drzwi, gdy jest offline lub serwer HTTPS nie jest aktywny.
5. W rozwijalnym menu **Door type (Typ drzwi)** wybierz typ drzwi, które chcesz utworzyć.
6. Kliknij przycisk **Next (Dalej)**, aby przejść do strony konfiguracyjnej drzwi.
7. W rozwijalnym menu **Primary lock (Zamek główny)** wybierz port przekaźnika.
8. Aby skonfigurować dwa zamki w drzwiach, wybierz port przekaźnika z rozwijalnego menu **Secondary lock (Drugi zamek)**.
9. Wybierz profil identyfikacji. Zob. *Profile identyfikacji, on page 88*.
10. Skonfiguruj ustawienia drzwi. P. sekcja *Ustawienia drzwi, on page 76*.
11. Skonfiguruj drzwi dozorujące. P. sekcja *Dodawanie drzwi dozorujących, on page 79*.
12. Kliknij przycisk **Save (Zapisz)**.

Aby dodać drzwi poprzez skopiowanie istniejącej konfiguracji drzwi:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **Add door (Dodaj drzwi)**.
3. Wprowadź nazwę drzwi.
4. Z rozwijalnego menu **Controller (Kontroler)** wybierz kontroler drzwi.
5. Kliknij **Next (Dalej)**.
6. Z rozwijalnego menu **Copy configuration (Kopiuj konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarzony, jeśli został skonfigurowany z dwoma drzwiami lub jednymi drzwiami z dwoma zamkami.
7. W razie potrzeby zmień ustawienia.
8. Kliknij przycisk **Save (Zapisz)**.

Aby zmodyfikować drzwi:

1. Przejdź do **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy > Drzwi).
2. Wybierz drzwi z listy.
3. Kliknij **Edit (Edytuj)**.
4. Zmień ustawienia i kliknij przycisk **Save (Zapisz)**.

Aby usunąć drzwi:

1. Przejdź do **Site Navigation** > **AXIS Optimizer**> **Access control** > **Doors and zones** > **Doors** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy > Drzwi).
2. Wybierz drzwi z listy.
3. Kliknij **Remove (Usuń)**.
4. Kliknij **Tak**.

Aby uwzględnić zmiany w systemie VMS za każdym razem, gdy dodajesz, usuwasz lub edytujesz nazwę drzwi:

1. Przejdź do **Site Navigation** > **Access control** (Nawigacja po obiekcie > Kontrola dostępu) i kliknij Access Control integration (Integracja kontroli dostępu).
2. Kliknij **Refresh Configuration** (Odśwież konfigurację) na karcie **General settings** (Ustawienia ogólne).

Ustawienia drzwi

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Wybierz drzwi, które chcesz edytować.
3. Kliknij **Edit (Edytuj)**.

Czas dostępu (s)	Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Drzwi pozostają odblokowane do momentu ich otwarcia lub przez określony czas. Drzwi blokują się po zamknięciu, nawet jeśli nie upłynął limit czasu dostępu.
Open-too-long time (sec) (Przekroczony czas otwarcia drzwi (s))	Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączony alarm zbyt długiego otwarcia drzwi. Ustaw regułę akcji, aby skonfigurować akcję, którą powinno wyzwolić zdarzenie zbyt długiego otwarcia drzwi.
Długi czas dostępu (s)	Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Po włączeniu tego ustawienia zastępuje ono czas dostępu obecnie ustawiony dla posiadaczy kart.
Long open-too-long time (sec) (Długi czas przekroczenia otwarcia drzwi (s))	Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączone zdarzenie zbyt długiego otwarcia drzwi. Długi czas przekroczenia otwarcia drzwi zastępuje już ustawiony czas otwarcia dla posiadaczy kart, jeśli włączona jest opcja **Long access time (Długi czas dostępu)**.
Czas opóźnienia do ponownego zablokowania (ms)	Ustaw czas w milisekundach, przez jaki drzwi pozostają odblokowane po ich otwarciu lub zamknięciu.
Ponowne zablokowanie	• **After opening** (Po otwarciu): Dotyczy tylko scenariuszy z dodanym monitorem drzwi. • **After closing** (Po zamknięciu): Dotyczy tylko scenariuszy z dodanym monitorem drzwi.

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 pozwala posiadaczowi karty zmienić bieżący stan drzwi. Może to służyć na przykład do blokowania lub odblokowywania drzwi poza regularnym harmonogramem, co jest wygodniejsze niż wchodzenie do systemu w celu odblokowania drzwi. Przeciągnięcie dwóch kart nie ma wpływu na istniejący harmonogram. Jeśli na przykład drzwi mają zostać zablokowane o godzinie zamknięcia, a pracownik wyjdzie na przerwę obiadową, drzwi nadal zostaną zablokowane zgodnie z harmonogramem.

Poziom zabezpieczeń można skonfigurować podczas dodawania nowych drzwi lub można to zrobić dla już istniejących drzwi.

Aby dodać **regułę dwóch osób** do istniejących drzwi:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > 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)**.

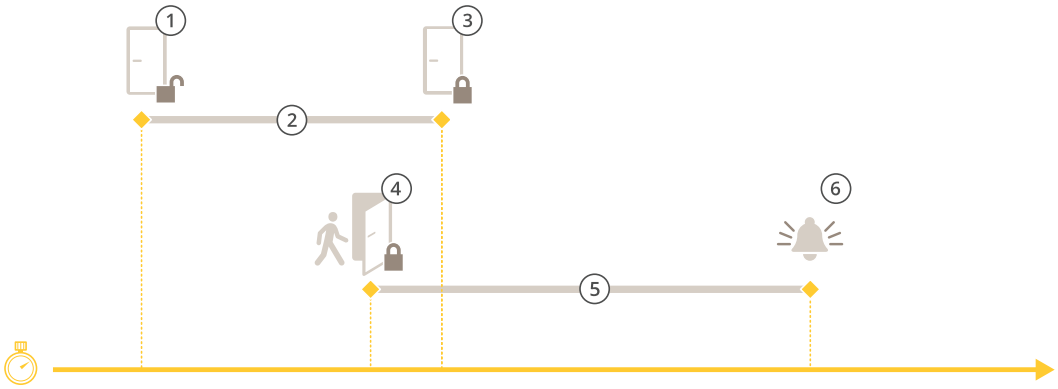
Reguła dwóch osób	
Side A (Strona A) i **Side B (Strona B)**	Wybierz, po których stronach drzwi ma być używana reguła.
Harmonogramy	Wybierz, kiedy reguła jest aktywna.
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi poświadczeniami dostępu.

Aby dodać **przeciągnięcie dwóch kart** do istniejących drzwi:

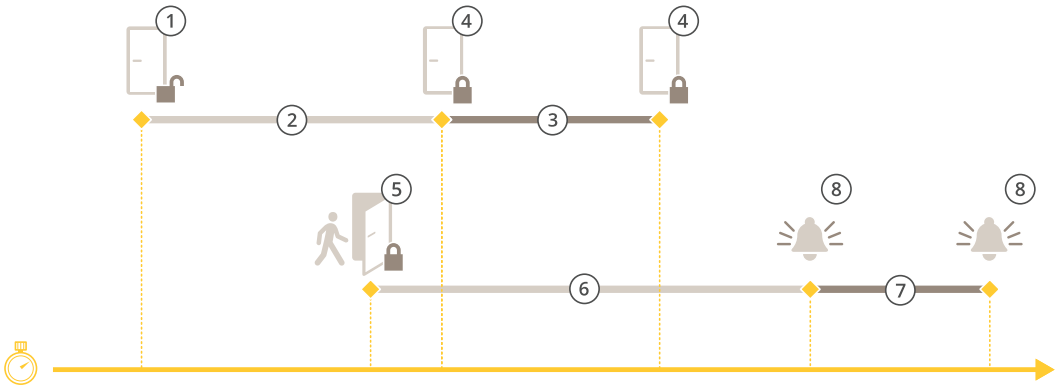
1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Wybierz drzwi, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (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. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)**.
   7.2. Wybierz posiadacza karty, którego dane chcesz edytować, i kliknij **Edit** (Edytuj).
   7.3. Kliknij przycisk **Advanced (Zaawansowane)**.
   7.4. Wybierz **Allow double-swipe (Zezwól na przeciągnięcie dwóch kart)**.
   7.5. Kliknij przycisk **Save (Zapisz)**.

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

Opcje czasu



1 Dostęp przyznany – zamek odblokowany
2 Czas dostępu
3 Nie podjęto żadnych działań – zamek zablokowany
4 Podjęto działanie (otwarto drzwi) – zamek zablokowany lub pozostaje odblokowany do momentu zamknięcia drzwi
5 Przekroczony czas otwarcia drzwi
6 Otwarte zbyt długo – uruchamiany jest alarm



1 Dostęp przyznany – zamek odblokowany
2 Czas dostępu
3 2+3: Długi czas dostępu
4 Nie podjęto żadnych działań – zamek zablokowany
5 Podjęto działanie (otwarto drzwi) – zamek zablokowany lub pozostaje odblokowany do momentu zamknięcia drzwi
6 Przekroczony czas otwarcia drzwi
7 6+7: Długi czas przekroczenia otwarcia drzwi
8 Otwarte zbyt długo – uruchamiany jest alarm

Dodawanie monitora drzwi

Monitor drzwi to przełącznik położenia drzwi, który monitoruje fizyczny stan drzwi. Po dodaniu monitora do drzwi można określić sposób podłączenia jego obwodów.

1. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodaj drzwi, on page 75*
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 drzwi i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. P. sekcja *Nadzorowane wejścia, on page 83*.

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, 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 systemie VMS przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > 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 sekcji **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 czytnika

Kontroler drzwiowy można skonfigurować tak, aby wykorzystywał dwa czytniki przewodowe. Czytniki można dodać po jednej lub obu stronach drzwi.

Jeżeli do czytnika zastosujesz niestandardową konfigurację formatów kart lub długości numerów PIN, będzie to wyraźnie zaznaczone w kolumnie **Card formats (Formaty kart)** w oknie **Configuration > Access control > Doors and zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**. P. sekcja *Drzwi i strefy, on page 73*.

1. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodaj drzwi, on page 75*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **Card reader (Czytnik kart)**.
4. Wybierz **Reader type (Typ czytnika)**.
5. Aby użyć niestandardowej konfiguracji długości kodu PIN tego czytnika.
   5.1. Kliknij przycisk **Advanced (Zaawansowane)**.
   5.2. Włącz opcję **Custom PIN length (Niestandardowa długość kodu PIN)**.
   5.3. Wypełnij pola **Min PIN length (Min. długość kodu PIN)**, **Max PIN length (Maks. długość kodu PIN)** i **End of PIN character (Koniec znaku kodu PIN)**.
6. Aby użyć niestandardowego formatu karty tego czytnika.
   6.1. Kliknij przycisk **Advanced (Zaawansowane)**.
   6.2. Włącz opcję **Custom card formats (Niestandardowe formaty kart)**.
   6.3. Wybierz formaty karty na takie, których chcesz używać w czytniku. Jeżeli format karty o tej samej liczbie bitów jest już używany, należy go najpierw zdezaktywować. Gdy konfiguracja formatu karty różni się od skonfigurowanej konfiguracji systemu, w aplikacji klienckiej wyświetlana jest Ikona ostrzeżenia.
7. Kliknij **Dodaj**.
8. Aby dodać czytnik po drugiej stronie drzwi, wykonaj tę procedurę ponownie.

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.

Wiegand	
Sterowanie LED	Wybierz opcję **Single wire (Pojedynczy przewód)** lub **Dual wire (R/G) (Podwójny przewód (R/G))**. Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED.
Powiadomienie o sabotażu	Określ, kiedy wejście wykrywania sabotażu w czytniku ma być aktywne.

	• **Open circuit (Obwód otwarty)**: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie otwarty. • **Closed circuit (Obwód zamknięty)**: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie zamknięty.
Tamper debounce time (Czas odbicia zabezpieczenia sabotażowego)	Aby zmiany stanu wejścia wykrywania sabotażu w czytniku były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Tamper debounce time (Czas odbicia zabezp. przeciwsab.)**.
Wejście nadzorowane	Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. P. sekcja *Nadzorowane wejścia, on page 83*.

Dodawanie urządzenia REX

Urządzenie REX (żądanie wyjścia) można dodać z jednej lub obu stron drzwi. Rolę urządzenia REX może pełnić czujnik PIR, przycisk REX lub zamknięcie drążkowe.

1. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodaj drzwi, on page 75*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **REX device (Urządzenie REX)**.
4. Zaznacz port we/wy, na którym chcesz połączyć urządzenie REX. Jeżeli jest dostępny tylko jeden port, zostanie on wybrany automatycznie.
5. Wybierz **Action (Akcja)**, która ma być wyzwalana po odebraniu sygnału REX przez drzwi.
6. W obszarze **REX active (Aktywne REX)** wybierz połączenie obwodu monitora drzwi.
7. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
8. Aby przerwanie połączenia między kontrolerem drzwi i urządzeniem REX powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. P. sekcja *Nadzorowane wejścia, on page 83*.

Akcja	
Odblokuj drzwi	Wybierz tę opcję, aby odblokować drzwi po odebraniu sygnału REX.
Brak	Wybierz, jeśli po odebraniu przez drzwi sygnału REX nie ma być wykonywane żadne działanie.

Urządzenie REX aktywne	
Obwód jest otwarty	Wybierz, jeżeli obwód REX jest rozwierny. Urządzenie REX wysyła sygnał po otwarciu obwodu.
Obwód jest zamknięty	Wybierz, jeżeli obwód REX jest zwierny. Urządzenie REX wysyła sygnał po zamknięciu obwodu.

Dodawanie strefy

Strefa to konkretny fizyczny obszar zawierający grupę drzwi. Można tworzyć strefy oraz dodawać do nich drzwi. Istnieją dwa rodzaje drzwi:

- **Perimeter door** (Drzwi na obwodzie): Posiadacze kart wchodzą do strefy bądź wychodzą z niej 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.

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy > Strefy).
2. Kliknij **Add zone (Dodaj strefę)**.
3. Wprowadź nazwę strefy.
4. Kliknij **Add door (Dodaj drzwi)**.
5. Zaznacz drzwi, które chcesz dodać do strefy, i kliknij przycisk **Add (Dodaj)**.
6. Domyślnie drzwi zostaną ustawione jako obwodowe. Aby to zmienić, z menu rozwijanego wybierz pozycję **Internal door (Drzwi wewnętrzne)**.
7. Drzwi obwodowe domyślnie jako wejścia do strefy używają drzwi A. Aby to zmienić, z menu rozwijanego wybierz opcję **Leave (Opuść)**.
8. Aby usunąć drzwi ze strefy, zaznacz ją i kliknij przycisk **Remove (Usuń)**.
9. Kliknij przycisk **Save (Zapisz)**.

Aby zmodyfikować strefę:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Nawigacja po obiekcie > AXIS Optimizer > 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. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** > **Zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy > Strefy).
2. Wybierz strefę z listy.
3. Kliknij **Remove (Usuń)**.
4. Kliknij **Tak**.

Poziom zabezpieczeń strefy

Do strefy można dodać następujące funkcje zabezpieczeń:

Anti-passback – Uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Wymusza on, że dana osoba musi najpierw opuścić obszar, zanim będzie mogła ponownie użyć swoich poświadczeń.

Uwaga

- W przypadku korzystania z funkcji anti-passback wszystkie drzwi w strefie muszą być wyposażone w

czujniki położenia drzwi, aby system był w stanie zarejestrować, że użytkownik otworzył drzwi po przeciągnięciu karty.

- Jeśli kontroler drzwi przejdzie w tryb offline, funkcja anti-passback będzie nadal działać, pod warunkiem, że wszystkie drzwi w strefie należą do tego samego kontrolera drzwi. Jeśli jednak drzwi w strefie należą do różnych kontrolerów drzwi, które przejdą w tryb offline, funkcja anti-passback przestanie działać.

Poziom zabezpieczeń można skonfigurować podczas dodawania nowej strefy lub w istniejącej strefie. Aby dodać poziom zabezpieczeń do istniejącej strefy:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Wybierz strefę, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz zabezpieczenia, które chcesz dodać do drzwi.
6. Kliknij przycisk **Apply (Zastosuj)**.

Anti-passback	
Log violation only (Soft) (Tylko rejestrowanie naruszeń (wersja miękka))	Użyj tej opcji, jeśli chcesz, aby druga osoba mogła wejść przez drzwi przy użyciu tych samych poświadczeń, co pierwsza osoba. Ta opcja powoduje tylko wywołanie alarmu systemowego.
Deny access (Hard) (Odmowa dostępu (wersja twarda))	Użyj tej opcji, jeśli chcesz uniemożliwić drugiej osobie wejście przez drzwi, jeśli używa on tych samych poświadczeń, co pierwsza osoba. Ta opcja powoduje także wywołanie alarmu systemowego.
Limit czasu (w sekundach)	Czas, po którym system zezwoli użytkownikowi na ponowne wejście. Wprowadź 0, jeśli nie chcesz ustawiać limitu czasu. Oznacza to, że w strefie obowiązuje zasada anti-passback do momentu opuszczenia jej przez użytkownika. Użyj limitu czasu **0** z opcją **Deny access (Hard) (Odmowa dostępu (w wersji twardej)** tylko wtedy, gdy wszystkie drzwi w strefie mają czytniki po obu stronach.

Nadzorowane wejścia

Nadzorowane wejścia mogą wyzwalać zdarzenie w przypadku przerwy w połączeniu z kontrolerem drzwi.

- Podłączenie miedzy kontrolerem drzwi a monitorem drzwi. P. sekcja *Dodawanie monitora drzwi, on page 79*.
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Zobacz *Dodawanie czytnika, on page 80*.
- Podłączenie miedzy kontrolerem drzwi a urządzeniem REX. P. sekcja *Dodawanie urządzenia REX, on page 81*.

Aby użyć nadzorowanych wejść:

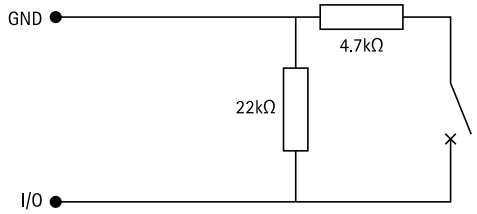
1. Zamontuj rezystory końca linii zgodnie ze schematem połączeń jak najbliżej urządzeń peryferyjnych.
2. Przejdź do strony konfiguracyjnej czytnika, monitora drzwi lub urządzenia REX i włącz opcję **Supervised input (Nadzorowane wejście)**.
3. Jeżeli zastosowano schemat pierwszego połączenia równoległego, wybierz opcję **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Pierwsze połączenie równoległe z 22 kΩ opornikiem równoległym i 4,7 kΩ opornikiem szeregowym)**.

4. Jeżeli zastosowano schemat pierwszego połączenia szeregowego, zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z rozwijalnego menu **Resistor values (Wartości oporników)** wybierz wartość rezystora.

Schematy połączeń

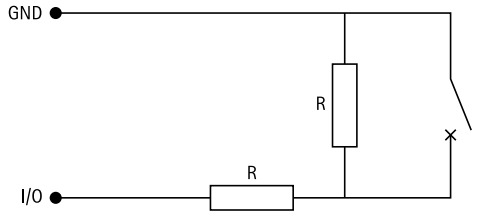
Pierwsze połączenie równoległe

Oporniki muszą mieć wartości 4,7 kΩ i 22 kΩ.



Pierwsze połączenie szeregowe

Oporniki muszą mieć takie same wartości w przedziale 1-10 kΩ.



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.

Zablokuj – 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. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Wybierz drzwi lub strefę, dla których chcesz wykonać akcję ręcznie.
3. Kliknij dowolną akcję wykonywaną ręcznie.

Uwaga

Drzwi pozostaną w trybie obsługi ręcznej, zwanym również trybem ręcznego sterowania, dopóki nie przywrócisz ich do normalnego harmonogramu działania.

Formaty kart i kod PIN

Format karty decyduje o sposobie przechowywania danych na karcie. Jest to tabela translacji między danymi przychodzącymi a zweryfikowanymi danymi w systemie. Każdy format karty ma inny zestaw reguł i sposób uporządkowania informacji przechowywanych na karcie. Dzięki zdefiniowaniu formatu karty system będzie wiedział, jak interpretować informacje, które kontroler pobiera z czytnika kart.

Istnieje kilka predefiniowanych powszechnie używanych schematów kart, których można używać w istniejącej postaci lub zmodyfikować. Można również tworzyć niestandardowe formaty kart.

Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Formaty kart i kod PIN), aby utworzyć, edytować lub uaktywnić formaty kart. Można również skonfigurować numer PIN.

Niestandardowe formaty kart mogą zawierać następujące pola danych służące do weryfikowania poświadczeń:

Numer karty – Podzbiór binarnych danych poświadczenia, które są zakodowane jako liczby dziesiętne lub szesnastkowe. Numer karty służy do identyfikowania konkretnej karty lub jej posiadacza.

Kod obiektu – Podzbiór binarnych danych poświadczenia, które są zakodowane jako liczby dziesiętne lub szesnastkowe. Kod obiektu służy do identyfikowania określonego klienta końcowego lub lokalizacji.

Aby utworzyć format karty:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Formaty kart i kod PIN).
2. Kliknij polecenie **Add card format (Dodaj format karty)**.
3. Wprowadź nazwę formatu karty.
4. W polu **Bit length (Liczba bitów)** wpisz liczbę bitów między 1 i 256.
5. Zaznacz opcję **Invert bit order (Odwróć kolejność bitów)**, jeżeli chcesz odwracać kolejność bitów w danych odbieranych z czytnika kart.
6. Zaznacz opcję **Invert byte order (Odwróć kolejność bajtów)**, jeżeli chcesz odwracać kolejność bajtów w danych odbieranych z czytnika kart. Ta opcja jest dostępna tylko w przypadku określenia liczby bitów, którą można podzielić przez osiem.
7. Wybierz i skonfiguruj pola danych, które mają być aktywne w formacie karty. W formacie karty koniecznie musi być aktywne pole **Card number (Numer karty)** lub **Facility code (Kod obiektu)**.
8. Kliknij **OK**.
9. Aby aktywować format karty, zaznacz pole wyboru przed jego nazwą.

Uwaga

- Dwa formaty kart o tej samej długości bitów nie mogą być aktywne w tym samym czasie. Na przykład, jeśli zdefiniowano dwa formaty kart 32-bitowych, tylko jeden z nich może być aktywny. Dezaktywuj jeden format karty, aby aktywować drugi.
- Możesz aktywować i dezaktywować formaty kart tylko wtedy, gdy kontroler drzwi w systemie został skonfigurowany z przynajmniej jednym czytnikiem.

ⓘ	Kliknij ⓘ, aby zobaczyć przykład rezultatu odwrócenia kolejności bitów.
Zasięg	Ustaw zakres bitów danych dla pola danych. Musi się on mieścić w przedziale określonym w polu **Bit length (Liczba bitów)**.

Format wyjściowy	Wybierz format wyjściowy danych dla pola danych. **Decimal (Dziesiętny)**: Nazywany jest również „pozycyjnym systemem liczbowym o podstawie 10", są używane cyfry 0–9. **Hexadecimal (Szesnastkowy)**: Nazywany jest również „pozycyjnym systemem liczbowym o podstawie 16", są używane symbole 16-tkowe: cyfry od 0 do 9 i litery od a do f.
Kolejność bitów podzakresu	Wybierz kolejność bitów. **Little endian**: Pierwszy bit jest najmniejszy (najmniej znaczący). **Big endian**: Pierwszy bit jest największy (najbardziej znaczący).

Aby edytować format karty:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > 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. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Formaty kart i kod PIN).
2. Zaznacz niestandardowy format karty, a następnie kliknij i **Yes (Tak)**.

Aby zresetować wstępnie zdefiniowany format karty:

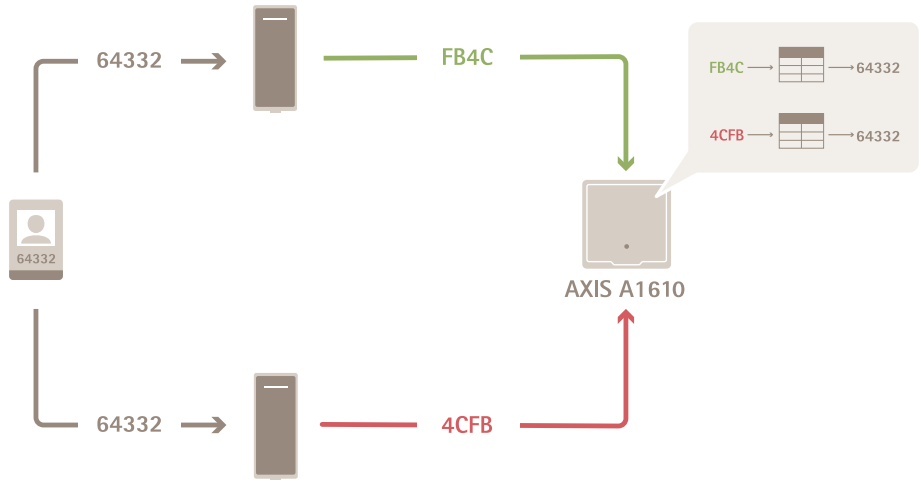
1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Formaty kart i kod PIN).
2. Kliknij , aby w formacie karty przywrócić domyślną mapę pól.

Aby skonfigurować długość numeru PIN:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Card formats and PIN** (Nawigacja po obiekcie > AXIS Optimizer > 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**.

Ustawienia formatu karty

Informacje ogólne



- Numer karty w zapisie dziesiętnym ma wartość `64332`.
- Jeden czytnik przekształca numer karty na liczbę szesnastkową `FB4C`. Drugi czytnik przekształca go na liczbę szesnastkową `4CFB`.
- Kontroler AXIS A1610 Network Door Controller odbiera wartość `FB4C` i przekształca ją na wartość dziesiętną `64332` zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.
- Kontroler AXIS A1610 Network Door Controller odbiera wartość `4CFB`, zmienia ją na `FB4C`, odwracając porządek bajtów, i przekształca na wartość dziesiętną `64332` zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.

Odwróć kolejność bitów

Po odwrócenia kolejności bitów dane karty odebrane od czytnika są odczytywane bit po bicie od prawej do lewej.



Odwróć kolejność bajtów

Grupa ośmiu bitów tworzy bajt. Po odwrócenia kolejności bajtów dane karty odebrane od czytnika są odczytywane bajt po bajcie od prawej do lewej.



26-bitowy standardowy format karty Wiegand



1 Parzystość wiodąca
2 Kod obiektu

3 *Numer karty*
4 *Parzystość końcowa*

Profile identyfikacji

Profil identyfikacji to połączenie typów i harmonogramów identyfikacji. Do jednych lub większej liczby drzwi można zastosować profil identyfikacji, aby określić, jak i kiedy posiadacz karty może uzyskać dostęp do drzwi.

Typy identyfikacji to nośniki informacji o poświadczeniach niezbędnych do uzyskania dostępu do drzwi. Typowe typy identyfikacji to tokeny, osobiste numery identyfikacyjne (PIN), linie papilarne, skany twarzy oraz urządzenia REX. Typ identyfikacji może zawierać jeden lub więcej typów informacji.

Harmonogramy, noszące również nazwę **Time profiles** (Profile czasowe), tworzone są w aplikacji Management Client. Aby skonfigurować profile czasowe, p. *Profile czasowe (wyjaśnienie)*.

Obsługiwane typy identyfikacji: Karta, kod PIN i urządzenie REX.

Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Profile identyfikacji).

Istnieje pięć domyślnych profili identyfikacji, których można używać w niezmienionej lub zmodyfikowanej postaci.

Karta – Aby uzyskać dostęp do drzwi, posiadacz karty musi przeciągnąć kartę przez czytnik.

Karta i PIN – Aby uzyskać dostęp do drzwi, posiadacz karty musi przeciągnąć kartę i wpisać numer PIN.

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.

Tablica rejestracyjna – Posiadacz karty musi jechać w kierunku kamery pojazdem z zatwierdzoną tablicą rejestracyjną.

Aby utworzyć profil identyfikacji:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Profile identyfikacji).
2. Kliknij **Create identification profile (Utwórz profil identyfikacji)**.
3. Nadaj nazwę profilowi identyfikacji.
4. Zaznacz opcję **Include facility code for card validation (Uwzględnij kod obiektu w celu weryfikacji karty)**, aby używać kodu obiektu jako jednego z pól służących do weryfikacji poświadczeń. To pole jest dostępne tylko po włączeniu ustawienia **Facility code (Kod obiektu)** w obszarze **Access management > Settings (Zarządzanie dostępem > Ustawienia)**.
5. Skonfiguruj profil identyfikacji po jednej stronie drzwi.
6. Po drugiej stronie drzwi powtórz poprzednie kroki.
7. Kliknij **OK**.

Aby zmodyfikować profil identyfikacji:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Profile identyfikacji).
2. Zaznacz profil identyfikacji i kliknij .
3. Aby zmienić nazwę profilu identyfikacji, wpisz nową nazwę.
4. Wprowadź zmiany z boku drzwi.
5. Aby zmodyfikować profil identyfikacji po drugiej stronie drzwi, powtórz poprzednie kroki.
6. Kliknij **OK**.

Aby usunąć profil identyfikacji:

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Identification profiles** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Profile identyfikacji).
2. Zaznacz profil identyfikacji i kliknij .
3. Jeżeli profil identyfikacji został zastosowany do drzwi, wybierz dla nich inny profil identyfikacji.
4. Kliknij **OK**.

Edytuj profil identyfikacji	
×	Aby usunąć typ identyfikacji i powiązany z nim harmonogram.
Typ identyfikacji	Aby zmienić typy identyfikacji, zaznacz je na liście rozwijanej **Identification type (Typ identyfikacji)**.
Schedule	Aby zmienić harmonogramy, zaznacz je z menu rozwijanego **Schedule (Harmonogram)**.
+ **Dodaj**	Dodaj typ identyfikacji i powiązany z nim harmonogram, kliknij przycisk **Add (Dodaj)**, a następnie skonfiguruj żądane typy identyfikacji i harmonogramy.

Szyfrowana komunikacja

Bezpieczny kanał OSDP

Aplikacja 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 **Site Navigation** > **AXIS Optimizer** > **Access control** > **Encrypted communication** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Szyfrowana komunikacja).
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*.

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.
- 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 53461.

Proces

1. Skonfiguruj serwer jako podrzędny i wygeneruj plik konfiguracyjny. P. sekcja *Generowanie pliku konfiguracyjnego z serwera podrzędnego, on page 90*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. P. sekcja *Importowanie pliku konfiguracyjnego do serwera głównego, on page 90*.
3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. P. sekcje *Dodawanie posiadacza karty, on page 91* i *Dodawanie grupy, on page 94*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz *Zarządzanie dostępem, on page 91*.

Generowanie pliku konfiguracyjnego z serwera podrzędnego

1. Na serwerze podrzędnym przejdź do **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer > 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 przejdź do **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer > 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 przejdź do **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer > 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:

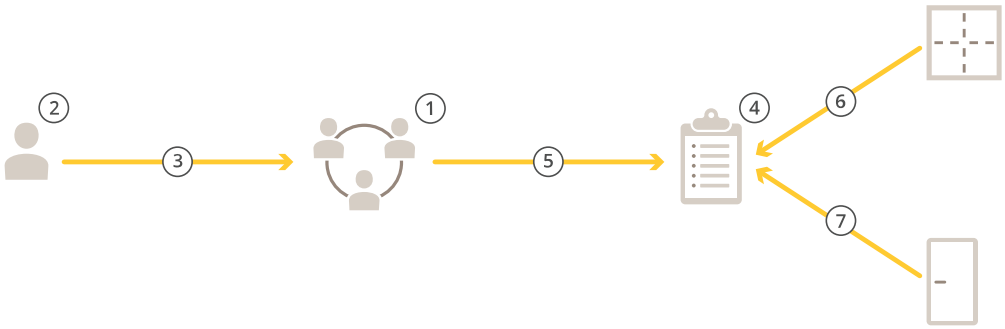
1. Na serwerze głównym:
   1.1. Przejdź do **Access management** > **Dashboard** (Zarządzanie dostępem > Pulpit nawigacyjny).
   1.2. Zmień globalnych posiadaczy kart i grupy na lokalnych posiadaczy kart i grupy.
   1.3. Przejdź do **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer > 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 **AXIS Optimizer** > **Access control** > **Multi server** (AXIS Optimizer > Kontrola dostępu > Multiserwer).
   – Kliknij polecenie **Sub server (Serwer podrzędny)** i kliknij przycisk **Revoke server (Unieważnij serwer)**.

Zarządzanie dostępem

Karta Access management (Zarządzanie dostępem) umożliwia konfigurowanie posiadaczy kart, grup i reguł dostępu w systemie oraz zarządzanie nimi.

Proces zarządzania dostępem

Struktura zarządzania dostępem jest elastyczna i pozwala utworzyć przepływ pracy, który najlepiej odpowiada potrzebom użytkownika. Oto przykład przepływu pracy:



1. Dodaj grupy. Zob. *Dodawanie grupy, on page 94*.
2. Dodaj posiadaczy kart. Zob. *Dodawanie posiadacza karty, on page 91*.
3. Dodaj posiadaczy kart do grup.
4. Dodaj reguły dostępu. Zob. *Dodaj regułę dostępu, on page 95*.
5. Przypisz grupy do reguł dostępu.
6. Przypisz strefy do reguł dostępu.
7. Przypisz drzwi do reguł dostępu.

Dodawanie posiadacza karty

Posiadacz karty to osoba posiadająca unikatowy identyfikator zarejestrowany w systemie. Skonfiguruj posiadacza karty z poświadczeniami osoby oraz czas i sposób udzielania temu posiadaczowi karty dostępu do drzwi.

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Zarządzanie posiadaczami kart).
2. Przejdź do **Cardholders** (Posiadacze kart) i kliknij **+ Add** (Dodaj).

3. Wprowadź imię i nazwisko posiadacza karty i kliknij **Next (Dalej)**.
4. Opcjonalnie kliknij **Advanced (Zaawansowane)** i wybierz dowolne opcje.
5. Dodaj poświadczenie do posiadacza karty. Zob. *Dodaj poświadczenia, on page 92*
6. Kliknij przycisk **Save (Zapisz)**.
7. Dodaj posiadacza karty do grupy.
   7.1. W obszarze **Groups (Grupy)** wybierz grupę, do której chcesz dodać posiadacza karty, i kliknij **Edit (Edytuj)**.
   7.2. Kliknij **+ Add (+ Dodaj)** i wybierz posiadacza karty, którego chcesz dodać do grupy. Można wybrać wielu posiadaczy kart.
   7.3. Kliknij **Dodaj**.
   7.4. Kliknij przycisk **Save (Zapisz)**.

Zaawansowane	
Długi czas dostępu	Wybierz tę opcję, aby w sytuacji, gdy jest zainstalowany monitor drzwi, posiadacz karty miał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi.
Zawieś posiadacza karty	Wybierz, aby zawiesić posiadacza karty.
Zezwól na podwójne przeciągnięcie	Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Mogą go na przykład użyć do odblokowania drzwi poza regularnym harmonogramem.
Zwolnienie z blokady ogólnej	Zaznacz, aby zezwolić posiadaczowi karty na dostęp podczas blokady.
Exempt from anti-passback (Zwolnienie z reguły anti-passback)	Wybierz tę opcję, aby przyznać zwolnić posiadacza karty z reguły anti-passback. Reguła Anti-passback uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Zanim takie poświadczenia będą mogły zostać użyte ponownie, posiadacz kart z tymi danymi musi najpierw opuścić obszar.
Globalny posiadacz karty	Zaznacz tę opcję, aby możliwe było wyświetlanie i monitorowanie posiadacza karty na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Zob. .

Dodaj poświadczenia

Do posiadacza karty można dodać następujące typy poświadczeń:

- Kod PIN
- Karta
- Tablica rejestracyjna
- Tel. komórkowy

Aby dodać do posiadacza karty poświadczenie w postaci tablicy rejestracyjnej:

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **License plate (Tablica rejestracyjna)**.

2. Wprowadź nazwę poświadczenia opisującą dany pojazd.
3. Wprowadź numer tablic rejestracyjnych dla pojazdu.
4. Ustaw datę początkową i końcową poświadczenia.
5. Kliknij **Dodaj**.

Zobacz przykład w temacie *Używanie numeru rejestracyjnego jako poświadczenia, on page 94*.

Aby dodać do posiadacza karty poświadczenie w postaci numeru PIN:

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **PIN**.
2. Wprowadź numer PIN.
3. Aby używać kodu PIN na wypadek zagrożenia w celu inicjowania cichego alarmu, włącz opcję **Duress PIN (PIN na wypadek zagrożenia)** i wprowadź odpowiedni numer PIN.
4. Kliknij **Dodaj**.

Poświadczenia przez PIN jest zawsze ważne. Można również skonfigurować PIN na wypadek zagrożenia, który otwiera drzwi oraz dodatkowo wyzwala cichy alarm w systemie.

Aby dodać do posiadacza karty poświadczenie w postaci karty:

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

Uwaga

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

3. Aby następowało automatyczne pobieranie danych ostatnio przeciągniętej karty:
   3.1. W menu rozwijanym **Select reader (Wybierz czytnik)** zaznacz czytnik.
   3.2. Przeciągnij kartę w czytniku podłączonym do tych drzwi.
   3.3. Kliknij **Get last swiped card data from the door's reader(s) (Odczytaj dane ostatniej przeciągniętej karty z czytnika)**.
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**.

Data wygaśnięcia	
Ważne od	Ustaw datę i godzinę ważności poświadczeń.
Ważne do	Wybierz opcję z menu rozwijanego.

Ważne do	
Brak daty zakończenia	Poświadczenie nigdy nie wygasa.
Data	Ustaw datę i godzinę wygaśnięcia poświadczenia.
Od pierwszego użycia	Określ, jak długo poświadczenie będzie ważne po pierwszym użyciu. Może to być liczba dni, miesięcy lub lat albo liczba razy po pierwszym użyciu.
Od ostatniego użycia	Określ, jak długo poświadczenie będzie ważne po ostatnim użyciu. Wybierz dni, miesiące lub lata po ostatnim użyciu.

Używanie numeru rejestracyjnego jako poświadczenia

W tym przykładzie pokazano, jak użyć kontrolera drzwi, kamery z AXIS License Plate Verifier i numeru rejestracyjnego pojazdu jako danych uwierzytelniających do przyznania dostępu.

1. Dodaj kontroler drzwi i kamerę do AXIS Optimizer.
2. Ustaw datę i godzinę dla nowych urządzeń, wybierając polecenie **Synchronize with server computer time (Synchronizuj z czasem serwera)**.
3. Uaktualnij oprogramowanie w nowych urządzeniach do najnowszej dostępnej wersji.
4. Dodaj nowe drzwi połączone z kontrolerem drzwi. Zob. *Dodaj drzwi, on page 75*.
   4.1. Dodaj czytnik na **Side A** (Strona A). P. sekcja *Dodawanie czytnika, on page 80*.
   4.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
   4.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
   4.4. Kliknij przycisk **Ok**.
5. Zainstaluj i włącz w kamerze aplikację AXIS License Plate Verifier. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
6. Włącz aplikację AXIS License Plate Verifier.
7. Skonfiguruj aplikację AXIS License Plate Verifier.
   7.1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.
   7.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuj klucz)**.
   7.3. Otwórz aplikację AXIS License Plate Verifier z poziomu interfejsu WWW kamery.
   7.4. Nie przeprowadzaj konfiguracji.
   7.5. Przejdź do opcji **Settings (Ustawienia)**.
   7.6. W obszarze **Access control (Kontrola dostępu)** wybierz **Secure Entry (Bezpieczne wejście)** jako **Type (Typ)**.
   7.7. W obszarze **IP address (Adres IP)** wpisz adres IP kontrolera drzwi.
   7.8. W obszarze **Authentication key (Klucz uwierzytelniania)** wklej skopiowany wcześniej klucz uwierzytelniania.
   7.9. Kliknij przycisk **Połącz**.
   7.10. W obszarze **Door controller name (Nazwa kontrolera drzwi)** wybierz kontroler drzwi.
   7.11. W obszarze **Reader name (Nazwa czytnika)** wybierz czytnik dodany wcześniej.
   7.12. Włącz integrację.
8. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Zob. *Dodawanie posiadacza karty, on page 91*.
9. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Zob. *Dodaj poświadczenia, on page 92*.
10. Dodaj regułę dostępu. Zob. *Dodaj regułę dostępu, on page 95*.
    10.1. Dodaj harmonogram.
    10.2. Dodaj posiadacza karty, któremu chcesz przyznać dostęp do tablicy rejestracyjnej.
    10.3. Dodaj drzwi z czytnikiem AXIS License Plate Verifier.

Dodawanie grupy

Grupy pozwalają zarządzać posiadaczami kart oraz regułami ich dostępu zbiorowo i skutecznie.

1. Przejdź do **Site Navigation** > **AXIS Optimizer** > **Access control** > **Cardholder management** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Zarządzanie posiadaczami kart).
2. Przejdź do **Groups** (Grupy) i kliknij **+ Add** (Dodaj).
3. Wprowadź nazwę i opcjonalnie inicjały grupy.
4. Zaznacz opcję **Global group (Grupa globalna)**, aby posiadaczy kart można było wyświetlać i monitorować na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. P. sekcja *Multiserwer BETA, on page 89*.
5. Dodawanie posiadaczy kart do grupy:
   5.1. Kliknij **+ Dodaj**.
   5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add (Dodaj)**.
6. Kliknij przycisk **Save (Zapisz)**.

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. Przejdź do **Access control** > **Cardholder management** (Kontrola dostępu > Zarządzanie posiadaczami kart).
2. W obszarze **Access rules (Reguły dostępu)** kliknij **+ Add (+ Dodaj)**.
3. Wprowadź nazwę reguły dostępu i kliknij **Next (Dalej)**.
4. Skonfiguruj posiadaczy kart i grupy:
   4.1. W obszarze **Cardholders (Posiadacze kart)** lub **Groups (Grupy)** kliknij **+ Add (+ Dodaj)**.
   4.2. Wybierz posiadaczy kart lub grupy i kliknij **Add (Dodaj)**.
5. Konfiguracja drzwi i stref:
   5.1. W obszarze **Doors (Drzwi)** lub **Zones (Strefy)** kliknij **+ Add (+ Dodaj)**.
   5.2. Wybierz drzwi lub strefy i kliknij **Add (Dodaj)**.
6. Konfiguracja harmonogramów:
   6.1. W obszarze **Schedules (Harmonogramy)** kliknij **+ Add (+ Dodaj)**.
   6.2. Wybierz jeden lub więcej harmonogramów i kliknij **Add (Dodaj)**.
7. 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)**.

Ręczne odblokowywanie drzwi i stref

Aby uzyskać informacje na temat czynności wykonywanych ręcznie, takich jak ręczne odblokowywanie drzwi, p. sekcja *Akcje wykonywane ręcznie, on page 84*.

Aby uzyskać informacje na temat czynności wykonywanych ręcznie, takich jak ręczne odblokowywanie strefy, p. sekcja *Akcje wykonywane ręcznie, on page 84*.

Eksportowanie raportów konfiguracji systemu

Można eksportować raporty zawierające różne rodzaje informacji o systemie. AXIS Optimizer eksportuje raport jako plik CSV (zawierający wartości rozdzielone przecinkami) i zapisuje go w domyślnym folderze pobierania. Aby wyeksportować raport:

1. Przejdź do obszaru **Reports (Raporty)** > **System configuration (Konfiguracja systemu)**.
2. Wybierz raporty, które chcesz wyeksportować, i kliknij **Download (Pobierz)**.

Dane posiadaczy kart	Zawiera informacje o posiadaczach kart, poświadczeniach, weryfikacjach kart i ostatnich transakcjach.
Dostęp posiadaczy kart	Zawiera informacje o posiadaczu karty, grupach posiadaczy kart, regułach dostępu, drzwiach i strefach powiązanych z posiadaczami kart.
Dostęp 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.
Reguła dostępu	Zawiera nazwę reguły dostępu oraz informacje o posiadaczach kart, grupach posiadaczy kart, drzwiach i strefach, z którymi jest powiązana reguła dostępu.
Dostęp do drzwi	Zawiera nazwę drzwi oraz informacje o posiadaczach kart, grupach posiadaczy kart, regułach dostępu i strefach, z którymi są powiązane drzwi.
Dostęp 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 on zarządcom budynków w odszukiwaniu pracowników i gości po ewakuacji. Punkt zbiórki to wyznaczony czytnik, do którego pracownicy zgłaszają się w sytuacji awaryjnej, umożliwiając wygenerowanie raportu z listą osób znajdujących się na miejscu 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 zbiórek wymagają stref do śledzenia posiadaczy kart.

Aby utworzyć i uruchomić raport imienny lub ze zbiórki:

1. Przejdź do obszaru **Reports (Raporty)** > **Cardholder activity (Aktywność posiadaczy kart)**.
2. Kliknij **+ Add (+ Dodaj)** i wybierz **Roll call / Mustering (Imienny / Zbiórka)**.
3. Wprowadź nazwę raportu.
4. Wybierz strefy do uwzględnienia w raporcie.
5. Wybierz grupy do uwzględnienia w raporcie.
6. Jeśli chcesz otrzymać raport ze zbiórki, wybierz **Mustering point (Punkt zbiórki)** i czytnik odpowiadający punktowi zbiórki.
7. Wybierz ramy czasowe raportu.

8. Kliknij przycisk **Save (Zapisz)**.
9. 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 rapocie ze zbiórki	Opis
Safe (Bezpieczny)	Posiadacz karty przeciągnął swoją kartę w punkcie zbiórki.
Missing (Zaginiony)	Posiadacz karty nie przeciągnął swojej karty w punkcie zbiórki.

Ustawienia zarządzania dostępem

Aby dostosować pola posiadacza karty używane na pulpicie nawigacyjnym dostępu:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia)** > **Custom cardholder fields (Niestandardowe pola posiadacza karty)**.
2. Kliknij **+ Add (+ Dodaj)** i wprowadź nazwę. Można dodać maksymalnie 6 pól niestandardowych.
3. Kliknij **Dodaj**.

Aby używać kodu obiektu do weryfikowania systemu kontroli dostępu:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia)** > **Facility code (Kod obiektu)**.
2. Wybierz **Facility code on (Kod obiektu włączony)**.

Uwaga

Podczas konfigurowania profili identyfikacji zaznacz również opcję **Include facility code for card validation** (Dołącz kod obiektu do sprawdzania poprawności karty). Zob. .

Import i eksport

Importuj posiadaczy kart

Ta opcja służy do importowania danych posiadaczy kart i grup posiadaczy karty, poświadczeń oraz zdjęć posiadaczy kart z pliku CSV. Aby można było zaimportować zdjęcia posiadaczy kart, serwer musi mieć dostęp do tych zdjęć.

Po zaimportowaniu posiadaczy kart system zarządzania dostępem automatycznie zapisuje konfigurację systemu, w tym całą konfigurację sprzętową, i usuwa wszystkie wcześniejsze ustawienia.

Opcje importu	
Nowość	Ta opcja powoduje usunięcie istniejących posiadaczy kart i dodanie nowych.
Aktualizuj	Opcja ta pozwala zaktualizować dane istniejących posiadaczy kart i dodanie nowych posiadaczy kart.
Dodaj	Ta opcja powoduje zachowanie istniejących posiadaczy kart i dodanie nowych. Numery kart i identyfikatory posiadaczy kart są unikatowe i można ich użyć tylko raz.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Import cardholders (Importuj posiadaczy kart)**.
3. Kliknij przycisk **New (Nowy)**, **Update (Aktualizuj)** lub **Add (Dodaj)**.
4. Kliknij **Next (Dalej)**.
5. Kliknij **Choose a file (Wybierz plik)** i przejdź do pliku CSV. Kliknij przycisk **Otwórz**.
6. Wprowadź separator kolumn i wybierz unikatowy identyfikator, a następnie kliknij **Next (Dalej)**.
7. Przypisz nagłówek do każdej kolumny.
8. Kliknij przycisk **Import (Importuj)**.

Ustawienia importu	
Pierwszy wiersz to nagłówek	Wybierz, czy plik CSV zawiera nagłówek kolumny.
Ogranicznik kolumny	Wprowadź format ogranicznika kolumn w pliku CSV.
Unikalny identyfikator	Do identyfikowania posiadacza karty system domyślnie używa **Cardholder ID (Identyfikatora posiadacza karty)**. Możesz również użyć imienia i nazwiska lub adresu e-mail. Unikatowy identyfikator zapobiega importowaniu duplikatów rekordów personelu.
Format numeru karty	Domyślnie jest zaznaczona opcja **Allow both hexadecimal and number (Zezwalaj na liczbę szesnastkową i liczbową)**.

Eksportowanie danych posiadaczy kart

Ta opcja powoduje wyeksportowanie zapisanych w systemie danych posiadacza karty do pliku CSV.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Export cardholders (Eksportuj posiadaczy kart)**.
3. Wybierz lokalizację pobierania i kliknij **Save (Zapisz)**.

AXIS Optimizer aktualizuje zdjęcia posiadaczy kart w katalogu `C:\ProgramData\Axis Communications\AXIS Camera Station\Components\AXIS Secure Entry\Cardholder photos` przy każdej zmianie konfiguracji.

Cofanie importu

System automatycznie zapisuje własną konfigurację w momencie importowania posiadaczy kart. Opcja **Undo import (Cofnij import)** powoduje przywrócenie danych posiadaczy kart i całej konfiguracji sprzętowej do stanu sprzed ostatniego importu posiadaczy kart.

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Import and export (Import i eksport)**.
2. Kliknij **Undo import (Cofnij import)**.
3. Kliknij **Tak**.

Kopia zapasowa i przywracanie

Automatyczne kopie zapasowe wykonywane są co noc. Trzy najnowsze pliki kopii zapasowych są przechowywane w folderze C:\ProgramData\Axis Communications\AXIS Optimizer Secure Entry\backup. Aby przywrócić te pliki:

1. Przenieś plik kopii zapasowej do katalogu C:\ProgramData\AXIS Communications\AXIS Optimizer Secure Entry\restore.
2. Uruchom ponownie aplikację AXIS Secure Entry, korzystając z jednej z poniższych metod:
   - Uruchom program MSC (Services), znajdź „AXIS Optimizer Secure Entry Service" i uruchom ponownie.
   - Uruchom ponownie komputer.
3. Ponownie uruchom instalator aplikacji AXIS Optimizer na komputerze pełniącym rolę serwera zdarzeń.

Zarządzanie dostępem w aplikacji Smart Client

Za pośrednictwem aplikacji Smart Client operatorzy mogą wykonywać działania związane z systemem kontroli dostępu. Większość funkcji związanych z kontrolą dostępu, takich jak ręczne sterowanie drzwiami, jest dostępna w aplikacji Smart Client. Więcej informacji na temat tych funkcji znajduje się w sekcji *Korzystanie z systemu kontroli dostępu w aplikacji Smart Client*.

Zarządzać dostępem można bezpośrednio w aplikacji Smart Client. Następujące funkcje w aplikacji Management Client dostępne są również w aplikacji Smart Client:

- Zarządzanie użytkownikami
- Ustawienia ogólne
- Pola niestandardowe posiadacza karty
- Kod obiektu
- Szablony e-mail
- Szablony identyfikatorów BETA

Aby wyświetlić kartę zarządzania dostępem Axis w aplikacji Smart Client:

1. Zainstaluj aplikację AXIS Optimizer na komputerze zawierającym aplikację Smart Client.
2. Uaktywnij licencję na jedne drzwi, o ile żadna nie została jeszcze uaktywniona. Aby uaktywnić licencję dot. drzwi, p. sekcja *Uaktywnienie licencji dot. drzwi, on page 72*.
3. Sprawdź, czy zalogowany użytkownik ma uprawnienia do zarządzania dostępem, p. sekcja *Ustawienia ról w aplikacji AXIS Secure Entry, on page 99*.

Ustawienia ról w aplikacji AXIS Secure Entry

1. W aplikacji Management Client przejdź do **Site Navigation** > **Security** > **Roles** (Nawigacja po obiekcie > Bezpieczeństwo > Role).
2. Wybierz konkretną rolę w systemie.
3. Wybierz **AXIS Optimizer**.
4. Rozwiń listę i kliknij **Access control** (Kontrola dostępu).
5. Wybierz **Read** (Czytaj) w przypadku ustawień bezpieczeństwa kontroli dostępu.
6. Kliknij funkcję, do której rola ma mieć uprawnienia, a następnie wybierz **Grant** (Przyznaj uprawnienia).

- **Access control configuration** (Konfiguracja kontroli dostępu): Nadaje roli operatora uprawnienia do wszystkich funkcji na karcie Configuration (Konfiguracja).
- **Access management** (Zarządzanie dostępem): Nadaje roli operatora uprawnienia do wszystkich funkcji na karcie Access Management (Zarządzanie dostępem).

Zarządzanie systemem i kontrola bezpieczeństwa

Dostęp do ustawień funkcji dla operatorów

Ustawienia roli

Domyślnie operator ma dostęp do wszystkich funkcji aplikacji AXIS Optimizer features w Smart Client, o ile ma on również dostęp do urządzenia w systemie VMS. Jednak w aplikacji Management Client za pomocą funkcji Role settings (Ustawienia ról) można wybrać funkcje, do których operator będzie mieć dostęp.

Konfigurowanie ustawień ról

Włącz funkcję **Role settings (Ustawienia ról)**:

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > Security > AXIS Optimizer Security (Nawigacja po witrynie > Zabezpieczenia > Zabezpieczenia w aplikacji AXIS Optimizer)**.

Uwaga

Ustawień ról nie można wyłączyć po ich włączeniu. Ustawienie jest trwałe.

2. Wybierz **Turn on role settings** (Włącz ustawienia ról).
3. Uruchom ponownie aplikację Management Client.

Konfigurowanie opcji w oknie **Role settings (Ustawienia ról)**:

1. W aplikacji Management Client wybierz kolejno opcje **Site Navigation > Security > Roles (Nawigacja po witrynie > Zabezpieczenia > Role)**.
2. Zaznacz rolę i przejdź do okna **Overall security (Ogólna ochrona)**.
3. Kliknij pozycję **AXIS Optimizer Security (Zabezpieczenia w aplikacji AXIS Optimizer)**.
4. Zaznacz funkcje, do których rola powinna mieć dostęp.
   - **Full control (Pełna kontrola)**Daje użytkownikowi z rolą operatora pełny dostęp do wszystkich funkcji aplikacji AXIS Optimizer.
   - **Edit (not applicable) (Edycja (nie dotyczy))**Funkcja systemu VMS, która nie ma zastosowania do ustawień ról w aplikacji AXIS Optimizer.
   - **Access AXIS Optimizer in Management Client (Dostęp do aplikacji AXIS Optimizer w kliencie zarządzania)**Rola operatora umożliwia korzystanie ze wszystkich funkcji administracyjnych pakietu AXIS Optimizer w aplikacji Management Client.
   - **Manage AXIS Optimizer security (Zarządzanie zabezpieczeniami aplikacji AXIS Optimizer)** Operator może zmieniać ustawienia w obszarze **Site Navigation> Security > AXIS Optimizer Security (Nawigacja po witrynie > Zabezpieczenia > Zabezpieczenia w aplikacji AXIS Optimizer)**.
   - **Dynamic camera operator controls (Dynamiczne elementy sterujące operatora w kamerze)** Operator ma dostęp do wszystkich preinstalowanych funkcji, które system znajdzie na urządzeniu.
   - **Remote focus operator control (Elementy sterujące operatora do zdalnego ustawiania ostrości)**Operator może zdalnie regulować ostrość stałopozycyjnych kamer kopułkowych.
   - **PTZ operator controls (Elementy sterujące operatora PTZ)**Posiadacz roli operatora ma dostęp do wybranych elementów sterujących operatora służących ustawianiu obrotu, pochylenia i powiększenia (PTZ): regulacja ostrości, prepozycje PTZ, elementy sterujące operatora dla aplikacji automatycznego śledzenia Autotracking 2, myjka i przycisk szybkiego osuszania/wycieraczki.
   - **Temperature spot measurement control (Kontrola punktowego pomiaru temperatury)**Operator może mierzyć temperaturę punktową w kamerze AXIS Q2901-E.
   - **Speaker operator control (Elementy sterujące operatora dla głośnika)**Operator ma dostęp do wszystkich funkcji menedżera głośników w aplikacji Smart Client.

- **Access visitor management (Zarządzanie dostępem gości)**Operator ma dostęp do wszystkich opcji zarządzania dostępem osób odwiedzających, np. może odebrać połączenie i otworzyć drzwi w podglądzie na żywo.
- **Access call history (Dostęp do historii połączeń)**Operator ma dostęp do historii połączeń interkomu. Aby używać tego ustawienia, należy włączyć uprawnienie **Access visitor management (Zarządzanie dostępem gości)**.
- **Extended search functions (Rozszerzone funkcje wyszukiwania)**W przypadku wybrania opcji **Deny** karta aplikacji AXIS License Plate Verifier będzie ukryta w aplikacji Smart Client. Ponadto nie będzie można używać funkcji wyszukiwania pojazdów ani kontenerów w mechanizmie centralnego wyszukiwania.
- **Control dewarping view (Kontrola widoku skorygowanego)**Operator może się poruszać po widokach z korekcją krzywizn.
- **Edit a dewarping view's home position (Edycja pozycji domowej widoku skorygowanego)**Rola operatora umożliwia edycję pozycji domowej kamery.
- **Web page (Strona internetowa)**Użytkownik z rolą operatora może utworzyć widok przy użyciu przeglądarki internetowej.
- **Axis insights dashboard (Pulpit nawigacyjny funkcji analitycznych Axis)**
  Osoba z rolą operatora ma dostęp do pulpitu nawigacyjnego funkcji analitycznych Axis.

5. Kliknij przycisk **Save (Zapisz)**.
6. Zrestartuj wszystkie uruchomione inteligentne klienty w systemie.

Zarządzanie urządzeniami

AXIS Device Manager Extend

W narzędziu AXIS Optimizer można użyć AXIS Device Manager Extend do zarządzania urządzeniami z wielu lokalizacji. Dzięki skonfigurowaniu hostów na krawędzi systemu na serwerach zapisu AXIS Device Manager Extend może łączyć się z urządzeniami w systemie VMS. Ułatwia to przeglądanie informacji gwarancyjnych i przeprowadzanie aktualizacji oprogramowania w wielu urządzeniach i lokalizacjach za pomocą jednego interfejsu użytkownika.

Więcej informacji na temat AXIS Device Manager Extend znajduje się w *instrukcji obsługi*.

Uwaga

Wymagania

- Zaloguj się na swoje *konto MyAxis*.
- Serwery zapisów muszą mieć połączenie z Internetem.
- Obsługiwane tylko na urządzeniach z systemem AXIS OS 6.50. Aby dowiedzieć się, które urządzenia są obsługiwane, p. *często zadawane pytania*.

Instalowanie hosta brzegowego

Host na krawędzi systemu to usługa zarządzania lokalnego, która umożliwia AXIS Device Manager Extend komunikację z lokalnymi urządzeniami w systemie VMS.

Aby móc korzystać z AXIS Device Manager Extend w VMS, musisz zainstalować hosta na krawędzi systemu i klienta na komputer stacjonarny. Zarówno host na krawędzi systemu, jak i klient komputerowy, wchodzą w skład instalatora AXIS Device Manager Extend.

1. Pobierz *plik instalacyjny* aplikacji AXIS Device Manager Extend.
   Host na krawędzi systemu musi być zainstalowany na serwerach zapisów VMS.
2. Uruchom instalator na serwerze zapisu i wybierz instalację tylko hosta na krawędzi systemu.

Przeczytaj *instrukcję obsługi do Axis Device Manager Extend* w celu uzyskania dodatkowych informacji o otwartych portach sieciowych i innych wymaganiach.

Przypisanie hosta na krawędzi systemu i synchronizacja urządzeń



1. Otwórz aplikację Management Client.
2. Wybierz kolejno opcje **Site Navigation > AXIS Optimizer > System overview (Nawigacja po witrynie > AXIS Optimizer > Przegląd systemu)**.
3. Wybierz i zaloguj się w MyAxis.
4. Kliknij kafelek serwera zapisu z zainstalowanym hostem na krawędzi systemu, który jest gotowy do przypisania.
5. Na pasku bocznym utwórz nową organizację lub wybierz wcześniej utworzoną organizację.
6. Kliknij i przypisz hosta na krawędzi systemu.
7. Poczekaj na ponowne wczytanie strony i kliknij **Synchronize (Synchronizuj)**.
   Wszystkie urządzenia Axis na serwerze rejestrującym zostaną teraz dodane do hosta brzegowego i będą przynależeć do wybranej organizacji.

Uwaga

AXIS Device Manager Extend musi mieć dostęp do sprzętu w VMS. Więcej informacji o obsługiwanych urządzeniach, p. sekcja *Rozwiązywanie problemów dotyczących dodawania urządzeń do hosta na krawędzi systemu, on page 104*.

8. W przypadku dodania nowych urządzeń do serwera nagrań lub zmiany informacji o urządzeniu wykonaj ponownie krok 7, aby zsynchronizować zmiany z systemem AXIS Device Manager Extend.
9. Powtórz kroki 4–7 dla wszystkich serwerów zapisów z urządzeniami, które chcesz dodać do AXIS Device Manager Extend.

Status hosta na krawędzi systemu

Na każdym serwerze zapisów w oknie **System overview (Przegląd systemu)** można sprawdzić, czy host na krawędzi systemu został już zainstalowany lub przypisany. Można włączyć opcję **Show machines that need edge host action (Pokaż maszyny wymagające akcji po stronie hosta na krawędzi systemu)** w celu filtrowania widoku.

- – nie znaleziono hosta na krawędzi systemu na serwerze zapisów.
  - Jeżeli host na krawędzi systemu nie został zainstalowany, pobierz go i zainstaluj na serwerze zapisów. Zob. *Instalowanie hosta brzegowego, on page 102*.
  - Jeśli host na krawędzi systemu jest zainstalowany, musisz zalogować się na konto MyAxis, aby go wykryć.
- – host na krawędzi systemu jest zainstalowany, ale nie został przypisany. Przypisz hosta na krawędzi systemu, tworząc nową organizację lub wybierając wcześniej utworzoną organizację. Zob. *Przypisanie hosta na krawędzi systemu i synchronizacja urządzeń, on page 103*.
- – host na krawędzi systemu został zainstalowany i przypisany, ale jest nieosiągalny. Sprawdź, czy serwer nagrań ma dostęp do Internetu.
- – host na krawędzi systemu jest zsynchronizowany.

-  – host na krawędzi systemu wymaga synchronizacji. Mogą to być nowe urządzenia w VMS, które można dodać do hosta na krawędzi systemu lub zaktualizowane informacje o urządzeniu, które należy zsynchronizować.

Używanie AXIS Device Manager Extend do konfigurowania urządzeń

Po zsynchronizowaniu urządzeń z hostem na krawędzi systemu można skonfigurować te urządzenia w narzędziu AXIS Device Manager Extend. Można to zrobić za pomocą dowolnego komputera połączonego z Internetem.

Uwaga

Jeżeli chcesz również zarządzać urządzeniami za pomocą połączenia zdalnego, musisz włączyć *zdalny dostęp na każdym hoście brzegowym*.

1. Zainstaluj i otwórz aplikację komputerową *AXIS Device Manager Extend*.
2. Wybierz organizację, która została użyta do przypisania hosta na krawędzi systemu.
3. Zsynchronizowane urządzenia można znaleźć w lokalizacji o tej samej nazwie co serwer zapisów VMS.

Rozwiązywanie problemów dotyczących dodawania urządzeń do hosta na krawędzi systemu

Jeżeli masz problemy z dodawaniem urządzeń do hosta na krawędzi systemu, upewnij się, że:

- AXIS Optimizer doda tylko włączony sprzęt z VMS.
- Połączenie ze sprzętem nie jest zerwane w VMS.
- Urządzenie ma zainstalowany system AXIS OS 6.50 lub nowszy.
- Urządzenie jest ustawione na uwierzytelnianie szyfrowane. Domyślnie AXIS Device Management nie obsługuje uwierzytelniania podstawowego.
- Spróbuj dodać urządzenia bezpośrednio z aplikacji AXIS Device Manager Extend.
- Zbierz dzienniki z AXIS Device Manager Extend i skontaktuj się z działem pomocy technicznej Axis.
  1. W aplikacji AXIS Device Manager Extend przejdź do wybranej lokalizacji na serwerze zapisów, na którym zainstalowano kamerę.
  2. Przejdź do menu **Settings (Ustawienia)** i kliknij **Download sitelog (Pobierz dziennik lokalizacji)**.

AXIS Site Designer: import

AXIS Optimizer umożliwia zaimportowanie projektu AXIS Site Designer i zastosowanie konfiguracji do systemu VMS w jednym łatwym procesie importu. Zaprojektuj i skonfiguruj swój system za pomocą aplikacji *AXIS Site Designer*. Gdy projekt będzie gotowy, używając aplikacji AXIS Optimizer, możesz zaimportować ustawienia wszystkich kamer i innych urządzeń z aplikacji AXIS Site Designer Management Client.

Aby dowiedzieć się więcej na temat aplikacji AXIS Site Designer, przeczytaj *instrukcję obsługi*.

Uwaga

Wymagania

- Wersja VMS 2020 R2 lub nowsza

Importowanie projektu



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

W aplikacji AXIS Site Designer

1. Utwórz projekt i skonfiguruj urządzenia.
2. Po utworzeniu projektu wygeneruj kod lub pobierz plik ustawień.

Uwaga

Jeżeli wprowadzisz jakiekolwiek zmiany w projekcie, wygeneruj nowy kod lub pobierz nowy plik ustawień.

W aplikacji Management Client

1. Upewnij się, że odpowiednie urządzenia zostały dodane do systemu VMS.
2. Przejdź do menu **Site Navigation > AXIS Optimizer > Import design project (Nawigacja po witrynie > AXIS Optimizer > Importuj projekt)**.
3. Zostanie otwarty przewodnik krok po kroku. Wybierz projekt, który chcesz zaimportować, wprowadzając kod dostępu lub zaznaczając plik ustawień projektu. Kliknij **Next (Dalej)**.
4. W sekcji **Project overview** (Przegląd projektu) widać informacje o liczbie urządzeń znalezionych w projekcie AXIS Site Designer i liczbie urządzeń znalezionych w systemie VMS. Kliknij **Next (Dalej)**.
5. W następnym kroku następuje dopasowanie urządzeń w VMS do urządzeń w projekcie AXIS Site Designer. Urządzenia z tylko jednym możliwym dopasowaniem są wybierane automatycznie. Zostaną zaimportowane tylko dopasowane urządzenia. Gdy dopasowywanie zostanie zakończone, kliknij przycisk **Next (Dalej)**.
6. Nastąpi zaimportowanie i zastosowanie ustawień wszystkich dopasowanych urządzeń w systemie VMS. Zależnie od wielkości projektu może to potrwać nawet kilka minut. Kliknij **Next (Dalej)**.
7. W obszarze **Results of import (Wyniki importu)** można znaleźć szczegółowe informacje o poszczególnych krokach procesu importu. W przypadku braku możliwości zaimportowania niektórych ustawień rozwiąż problemy i uruchom importowanie ponownie. Aby zapisać listę wyników jako plik, kliknij przycisk **Export... (Eksportuj...)**. Aby zamknąć przewodnik krok po kroku, kliknij przycisk **Done (Gotowe)**.

Importowane ustawienia

Import obejmuje wyłącznie urządzenia dopasowane między VMS i projektem. Następujące ustawienia są importowane i stosowane do VMS dla wszystkich typów urządzeń:

- Nazwa urządzenia użyta w projekcie
- Opis urządzenia użytego w projekcie
- Ustawienia geolokalizacji, jeżeli urządzenie jest umieszczone na mapie

W przypadku urządzeń z obsługą wideo stosowane są również następujące ustawienia:

- Jeden lub dwa strumienie wideo skonfigurowane w VMS (rozdzielczość, poklatkowość, kodek, kompresja i ustawienia Zipstream)
  - Strumień wideo 1 jest skonfigurowany pod kątem podglądu na żywo i nagrywania.
  - Strumień wideo 2 jest skonfigurowany pod kątem nagrywania, jeśli ustawienia strumienia w projekcie różnią się w podglądzie na żywo i nagraniu.
- Zasady detekcji ruchu lub ciągłego nagrywania są ustawiane zgodnie z projektem. Wykorzystywana jest wbudowana detekcja ruchu VMS, tworzone są profile czasowe dla reguł, a na serwerach nagrań tworzone są profile zasobów dla różnych czasów przechowywania.
- Mikrofon jest włączany lub wyłączany zgodnie z ustawieniami audio projektu.

Ograniczenia

W VMS obowiązują ograniczenia dotyczące importu projektów z AXIS Site Designer.

- Domyślna reguła nagrywania ruchu w VMS może zastąpić reguły nagrywania utworzone przez import. Wyłącz wszystkie reguły powodujące konflikty lub wyklucz z nich urządzenia, których one dotyczą.

- W przypadku nagrań wyzwalanych ruchem w VMS ich oszacowania mogą być niedokładne.
- Bieżąca wersja nie obsługuje planów pięter.
- Jeśli w projekcie skonfigurowano zarówno nagrywanie wyzwalane ruchem, jak i nagrywanie ciągłe, będzie stosowana wyłącznie konfiguracja przesyłania strumieniowego z ustawień nagrywania wyzwalanego ruchem.
- W VMS nie ma możliwości ustawienia minimalnej poklatkowości dla technologii Zipstream.

Zarządzanie kontami

Zarządzanie kontami pomaga zarządzać kontami i hasłami na wszystkich urządzeniach Axis używanych przez XProtect.

Zgodnie z wytycznymi Axis nie należy używać konta root do łączenia się z urządzeniami. Zarządzanie kontem pozwala utworzyć konto usługi XProtect. Dla każdego urządzenia tworzone są unikalne hasła złożone z 16 znaków. Urządzenia, które mają już konto XProtect, otrzymają nowe hasła.

Łączenie się z urządzeniami za pomocą konta usługi XProtect

1. Przejdź do menu **Site Navigation > AXIS Optimizer > Account management (Nawigacja po witrynie > Optymalizator AXIS > Menedżer kont)**.
   Wykres pokazuje, ile urządzeń jest w trybie online, ile z nich ma konto usługi XProtect, a ile nie ma konta usługi XProtect.
2. Kliknij **Show device details (Pokaż szczegóły urządzenia)**, aby uzyskać więcej informacji o urządzeniach. Urządzenia będące w trybie online są wyświetlane na górze listy. Możesz wybrać urządzenia, dla których chcesz wygenerować hasła. Jeśli nie zostanie wybrane żadne urządzenie, nowe hasła otrzymają wszystkie urządzenia będące online. Kliknij **OK**.

Uwaga

Jeśli w konfiguracji sprzętu zostanie wybrany protokół HTTP, hasła będą przesyłane między serwerem rejestrującym a urządzeniem Axis w postaci zwykłego tekstu. Zalecamy skonfigurowanie protokołu HTTPS w celu zabezpieczenia komunikacji między systemem VMS a urządzeniem.

3. Kliknij polecenie **Generate passwords (Generuj hasła)**. Wygenerowane hasło zawiera losowy tekst składający się z 16 znaków ASCII z zakresu od 32 do 126.
   Kliknij polecenie **Show device details (Pokaż szczegóły urządzenia)**, aby w czasie rzeczywistym obserwować aktualizacje statusu procesu. W trakcie tego procesu nastąpi krótka przerwa w dostępie do aktywnych podglądów na żywo i trwających nagrań.
4. Urządzenia będące online otrzymają konto usługi XProtect i nowe hasła. Urządzenia online mające już konto usługi XProtect otrzymują tylko nowe hasła.

Axis events

Funkcja „Axis events" zapewnia przegląd zdarzeń urządzeń Axis w VMS. Można testować zdarzenia na określonym urządzeniu, wyświetlać szczegółowe informacje o zdarzeniach i dodawać zdarzenia do wielu urządzeń.

Otwórz menu **Site Navigation (Nawigacja po witrynie)** i przejdź kolejno do **Rules and Events > Axis events (Reguły i zdarzenia > Zdarzenia Axis)**. Lista wszystkich dostępnych zdarzeń zostanie wyświetlona w oknie **Configuration (Konfiguracja)**. Widać, które zdarzenia są aktywne w systemie, a które nie.

Dla każdego zdarzenia można zobaczyć nazwy urządzeń, do których zdarzenie zostało dodane. Można również sprawdzić nazwę wyświetlaną zdarzenia, stan zdarzenia i czas jego ostatniego wyzwolenia.

Uwaga

Wymagania

- Wersja VMS 2023 R2 lub nowsza.

Konfigurowanie zdarzenia dla wielu urządzeń

1. Przejdź do **Configuration (Konfiguracja)** i wybierz zdarzenie.
2. Kliknij opcję **Add devices (Dodaj urządzenia)** .
3. W oknie **Add devices (Dodaj urządzenia)** zostanie wyświetlona lista urządzeń, do których można dodać zdarzenie. Wybierz jedno lub więcej urządzeń i kliknij **Add devices (Dodaj urządzenia)**.

Aby usunąć zdarzenie z urządzenia, kliknij **Remove (Usuń)**.

Informacje o wydarzeniach

W obszarze Zdarzenia Axis można wyświetlić ostatnie znane wystąpienie, stan zdarzeń i aktualizacje w czasie rzeczywistym w interfejsie użytkownika. W tym celu należy ustawić czas przechowywania w aplikacji Management Client.

1. Wybierz kolejno opcje **Tools > Options > Alarm and Events > Event retention (Narzędzia > Opcje > Alarmy i zdarzenia > Przechowywanie zdarzeń)**.
2. Ustaw czas przechowywania dla całej grupy zdarzeń urządzenia lub określonych zdarzeń w grupie.

Metadane i wyszukiwanie

Metadane i wyszukiwanie zapewniają przegląd wszystkich urządzeń dodanych do systemu VMS, możliwości metadanych oraz kategorii wyszukiwania Axis, które są widoczne dla operatorów.

Metadane i wyszukiwanie umożliwiają włączenie określonych funkcji dla tych urządzeń, tj. można włączyć dane zdarzeń, dane analityczne i skonsolidowane dane dla wielu urządzeń, a także wyświetlić funkcje analityczne obsługiwane przez urządzenia. Dzięki kategoriom wyszukiwania Axis można kontrolować opcje wyszukiwania dla wszystkich operatorów, aby odzwierciedlić dostępne funkcje analityczne w systemie VMS. Obsługa kategorii wyszukiwania i filtrów różni się w zależności od modelu kamery i zainstalowanych aplikacji analitycznych.

Konfiguracja ustawień metadanych

1. Wybierz kolejno opcje **Management Client (Management Client)** > **Site Navigation (Nawigacja po witrynie)** > **AXIS Optimizer (AXIS Optimizer)** > **Metadata and search (Metadane i wyszukiwanie)**.
   - **Event data (Dane o zdarzeniu)**: Włącz tę opcję, aby system VMS pobierał dane zdarzeń z urządzenia. Jest to potrzebne do korzystania z różnych funkcji aplikacji AXIS Optimizer.
   - **Analytics data (Dane analityczne)**: Włącz tę opcję, aby korzystać z funkcji wyszukiwania materiałów dowodowych i wyświetlać obwódki w podglądzie na żywo i odtwarzaniu.
   - **Analytics features (Funkcje analizy)**: Wyświetl funkcje analizy wideo obsługiwane obecnie przez urządzenie, takie jak typ obiektu (ludzie, samochody) i kolor obiektu. Aktualizacja oprogramowania urządzenia może rozszerzyć dostęp do kolejnych funkcji analitycznych.
   - **Consolidated metadata (Skonsolidowane metadane)**: Ta opcja pozwala przyspieszyć wyszukiwanie podczas postępowania wyjaśniającego i skrócić czas ładowania w funkcjach analitycznych Axis.

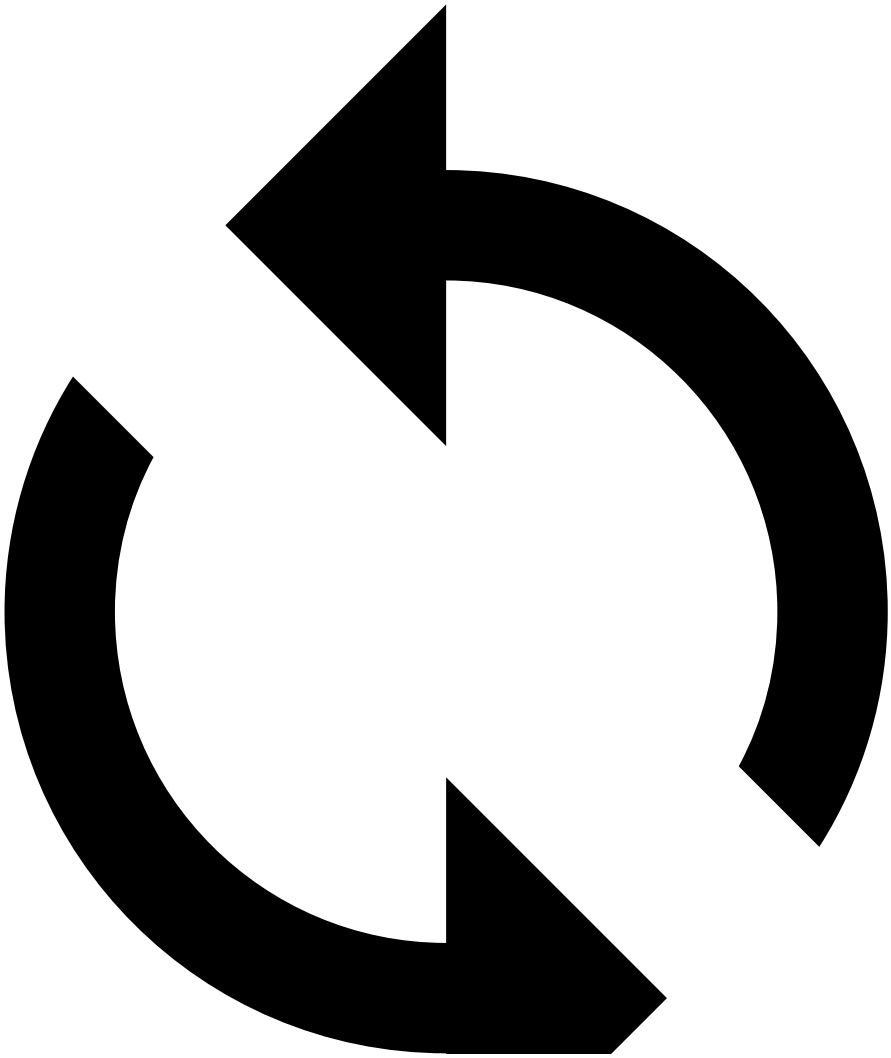
Uwaga

Skonsolidowane wymogi dotyczące metadanych

- Urządzenia Axis z systemem AXIS OS 11.10 lub nowszym.

Ograniczenia skonsolidowanych metadanych

- Obwódki w podglądzie na żywo i nagraniu oraz wbudowane opcje wyszukiwania VMS nie są dostępne.

– 
: Kliknij, aby wczytać ponownie po wprowadzeniu zmian w konfiguracji urządzenia.

Konfiguracja kategorii wyszukiwania Axis

1. Wybierz kolejno opcje **Management Client (Management Client)** > **Site Navigation (Nawigacja po witrynie)** > **AXIS Optimizer (AXIS Optimizer)** > **Metadata and search (Metadane i wyszukiwanie)**.
2. W oknie dialogowym **Kategorie wyszukiwania Axis** włącz kategorie wyszukiwania, których chcesz używać:
   - Prace wyjaśniające
   - Wyszukiwanie pojazdów
   - Zone speed search (Wyszukiwanie prędkości w strefie)
   - Wyszukiwanie kontenerów
3. Wybierz odpowiednie filtry w każdej kategorii wyszukiwania.

Uwaga

Wymagania dotyczące kategorii wyszukiwania Axis

- AXIS Optimizer w wersji 5.3 lub nowszej w Smart Client.

Cyberbezpieczeństwo

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

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

Zarządzanie podatnościami

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

Powiadomienia dotyczące zabezpieczeń

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

Bezpieczny cykl eksploatacji produktu

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

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

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

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

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

Przewodnik dotyczący wzmacniania systemów

Jako integralna część infrastruktury systemu VMS aplikacja AXIS Optimizer wymaga określonych konfiguracji w celu zapewnienia bezpieczeństwa środowiska. Przestrzeganie zalecanych ustawień jest konieczne do zabezpieczenia haseł urządzeń, ochrony danych osobowych oraz zapobiegania dostępowi osób nieuprawnionych do systemu.

- Przy dodawaniu urządzeń Axis do systemu VMS korzystaj z protokołu HTTPS.
- Włącz szyfrowanie pomiędzy klientami a serwerami systemu VMS.
- Włącz przechowywanie szyfrowanych danych w pamięci masowej systemu VMS.

- Przejrzyj wszystkie role w systemie VMS i sprawdź, czy nie mają przyznanych uprawnień wykraczających poza niezbędny zakres.

Potrzebujesz więcej pomocy?

Często zadawane pytania

Pytanie	Odbierz
Jak zaktualizować aplikację AXIS Optimizer, gdy komputer kliencki nie ma dostępu do Internetu?	Opublikuj nową wersję na serwerze zarządzania systemu VMS, p. *Automatyczne uaktualnianie systemu, on page 10*.
Czy przed aktualizacją do nowej wersji aplikacji AXIS Optimizer trzeba wykonać kopię zapasową ustawień?	Nie. Uaktualnienie do nowej wersji nie spowoduje zmiany żadnych danych.
Mam ponad 30 komputerów klienckich z oprogramowaniem AXIS Optimizer. Czy trzeba je uaktualniać jeden po drugim?	Oprogramowanie klienckie można uaktualniać osobno. Można także automatycznie wymusić uaktualnienia poprzez opublikowanie w systemie lokalnej wersji aplikacji AXIS Optimizer, p. *Automatyczne uaktualnianie systemu, on page 10*.
Czy można oddzielnie włączać i wyłączać wtyczki w aplikacji AXIS Optimizer?	Nie, ale kiedy nie są aktywnie używane, nie używają żadnych zasobów.
Których portów używa aplikacja AXIS Optimizer?	Porty 80 i 443 są niezbędne do komunikowania się z witryną axis.com. To za ich pośrednictwem system może otrzymywać informacje o nowych wersjach i pobierać aktualizacje. Porty 53459 i 53461 są otwarte dla ruchu przychodzącego (TCP) po zainstalowaniu aplikacji AXIS Optimizer poprzez aplikację AXIS Secure Entry.

Rozwiązywanie problemów

W razie wystąpienia problemów technicznych włącz rejestrowanie debugowania, odtwórz problem, a następnie udostępnij te dzienniki działowi pomocy technicznej Axis. Rejestrowanie debugowania można włączyć w aplikacji Management Client lub Smart Client.

W aplikacji Management Client:

1. Wybierz kolejno **Site Navigation (Nawigacja po witrynie)** > **Basics (Podstawy)** > **AXIS Optimizer**.
2. Wybierz **Turn on debug logging (Włącz rejestrowanie debugowania)**.
3. Kliknij **Save report (Zapisz raport)**, aby zapisać dzienniki na urządzeniu.

W aplikacji Smart Client:

1. Wybierz kolejno **Settings (Ustawienia)** > **Axis general options (Ogólne opcje Axis)**.
2. Wybierz **Turn on debug logging (Włącz rejestrowanie debugowania)**.
3. Kliknij **Save report (Zapisz raport)**, aby zapisać dzienniki na urządzeniu.

Kontakt z pomocą techniczną

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

Porady i wskazówki

Dodawanie strony internetowej w widoku klienta inteligentnego

Aplikacja AXIS Optimizer umożliwia wyświetlanie niemal każdej strony internetowej, nie tylko w formacie HTML, bezpośrednio w narzędziu Smart Client. Ten widok WWW jest renderowany przez nowoczesny silnik przeglądarki i obsługuje większość stron internetowych. Przydaje się to na przykład wtedy, gdy chcesz uzyskać dostęp do aplikacji AXIS Body Worn Manager bezpośrednio z narzędzia Smart Client albo wyświetlać pulpit z aplikacji AXIS Store Reporter bezpośrednio obok podglądów na żywo.

1. W narzędziu Smart Client kliknij opcję **Setup (Ustawienia)**.
2. Przejdź do obszaru **Views (Widoki)**.
3. Utwórz nowy widok lub wybierz istniejący.
4. Przejdź do menu **System overview > AXIS Optimizer (Przegląd systemu > AXIS Optimizer)**.
5. Kliknij opcję **Web view (Widok WWW)** i przeciągnij ją do widoku.
6. Wprowadź adres i kliknij przycisk **OK**.
7. Kliknij opcję **Setup (Ustawienia)**.

Eksportowanie plików wideo z osadzonymi funkcjami wyszukiwania

Eksportowanie filmów w formacie XProtect

Aby odtwarzać obraz z osadzonymi funkcjami wyszukiwania aplikacji AXIS Optimizer lub możliwościami korekty obrazu Axis, należy wyeksportować pliki wizyjne w formacie XProtect. Może to być pomocne na przykład do demonstracji.

Uwaga

W przypadku aplikacji AXIS Optimizer w wersji 5.3 lub nowszej należy rozpocząć od kroku 3.

1. W aplikacji Smart Client wybierz kolejno opcje **Settings (Ustawienia)** > **Axis search options (Opcje wyszukiwania Axis)**.
2. Włącz opcję **Include search plugins in exports (Uwzględniaj wtyczki wyszukiwania w eksportowanych materiałach)**.
3. Jeżeli tworzysz eksport w aplikacji Smart Client, zaznacz opcję **XProtect format (Format XProtect)**.

Odblokowywanie eksportu na komputerach odbiorczych

Aby pomyślnie używać eksportu na innym komputerze, trzeba koniecznie odblokować archiwum plików eksportu.

1. Na komputerze odbiorczym kliknij prawym przyciskiem myszy plik eksportu (.zip) i wybierz **Properties** (Właściwości).
2. W sekcji **General** (Ogólne) kliknij kolejno **Unblock** (Odblokuj) > **OK**.
3. Wyodrębnij plik eksportu „SmartClient-Player.exe" i go otwórz.

Odtwarzaj wyeksportowany widok skorygowany Axis

1. Otwórz wyeksportowany projekt.
2. Wybierz widok, który zawiera widok skorygowany Axis.

T10134385_pl

2026-09 (M61.2)

© 2021 – 2026 Axis Communications AB