

AXIS Secure Entry for XProtect

Spis treści

Kontrola dostępu	3
Konfiguracja kontroli dostępu.....	3
Dodawanie sieciowego kontrolera drzwiowego Axis do systemu	3
Uaktywnienie licencji dot. drzwi.....	4
Konfigurowanie kontroli dostępu.....	4
Integracja systemu kontroli dostępu.....	4
Drzwi i strefy.....	5
Przykład drzwi i stref.....	6
Dodawanie drzwi.....	6
Ustawienia drzwi.....	8
Poziom zabezpieczeń drzwi.....	8
Opcje czasu.....	10
Dodawanie monitora drzwi.....	10
Dodawanie drzwi dozorujących.....	11
Dodawanie czytnika.....	11
Dodawanie urządzenia REX.....	13
Dodawanie strefy.....	13
Poziom zabezpieczeń strefy	14
Nadzorowane wejścia	15
Akcje wykonywane ręcznie	16
Formaty kart i kod PIN	16
Ustawienia formatu karty.....	18
Profile identyfikacji	19
Szyfrowana komunikacja.....	21
Bezpieczny kanał OSDP	21
Multiserwer ^{BETA}	21
Proces	21
Generowanie pliku konfiguracyjnego z serwera podrzędnego.....	21
Importowanie pliku konfiguracyjnego do serwera głównego.....	22
Unieważnianie serwera podrzędnego	22
Usuwanie serwera podrzędnego	22
Zarządzanie dostępem	22
Proces zarządzania dostępem.....	22
Dodawanie posiadacza karty.....	23
Dodaj poświadczenia	24
Dodawanie grupy.....	26
Dodawanie reguły dostępu.....	26
Ręczne odblokowywanie drzwi i stref	27
Eksportowanie raportów konfiguracji systemu	27
Tworzenie raportów aktywności posiadaczy kart	28
Ustawienia zarządzania dostępem.....	28
Import i eksport.....	29
Kopia zapasowa i przywracanie.....	30
Zarządzanie dostępem w aplikacji Smart Client	30
Ustawienia ról w aplikacji AXIS Secure Entry.....	31

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 oprogramowania 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 4*.

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	12.9.65.3
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.

Konfigurowanie kontroli dostępu

1. Przejdź do **Site Navigation > AXIS Optimizer > Access control** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu).
2. Aby zmodyfikować predefiniowane profile identyfikacji lub utworzyć nowy profil identyfikacji, patrz *Profile identyfikacji, on page 19*.
3. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, patrz *Formaty kart i kod PIN, on page 16*.
4. Dodaj drzwi i zastosuj do nich profil identyfikacji. Patrz *Dodawanie drzwi, on page 6*.
5. Dodaj strefę, a następnie drzwi do strefy. Patrz *Dodawanie strefy, on page 13*.

Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

Ważne

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

- **Obsługiwane wersje systemu AXIS OS:** Wymienione powyżej obsługiwane wersje systemu (oprogramowania układowego) AXIS OS mają zastosowanie tylko w przypadku wykonywania aktualizacji z oryginalnej zalecanej wersji systemu 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 systemu AXIS OS:** Najstarsza wersja systemu AXIS OS zainstalowana w systemie określa minimalną obsługiwaną wersję AXIS OS – z ograniczeniem do dwóch wcześniejszych wersji.
- **Aktualizacja przekraczająca zalecaną wersję systemu AXIS OS:** Załóżmy, że wykonasz aktualizację do wersji oprogramowania AXIS OS przekraczającej wersję zalecaną dla danej 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 systemu 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** (Powyżaj 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

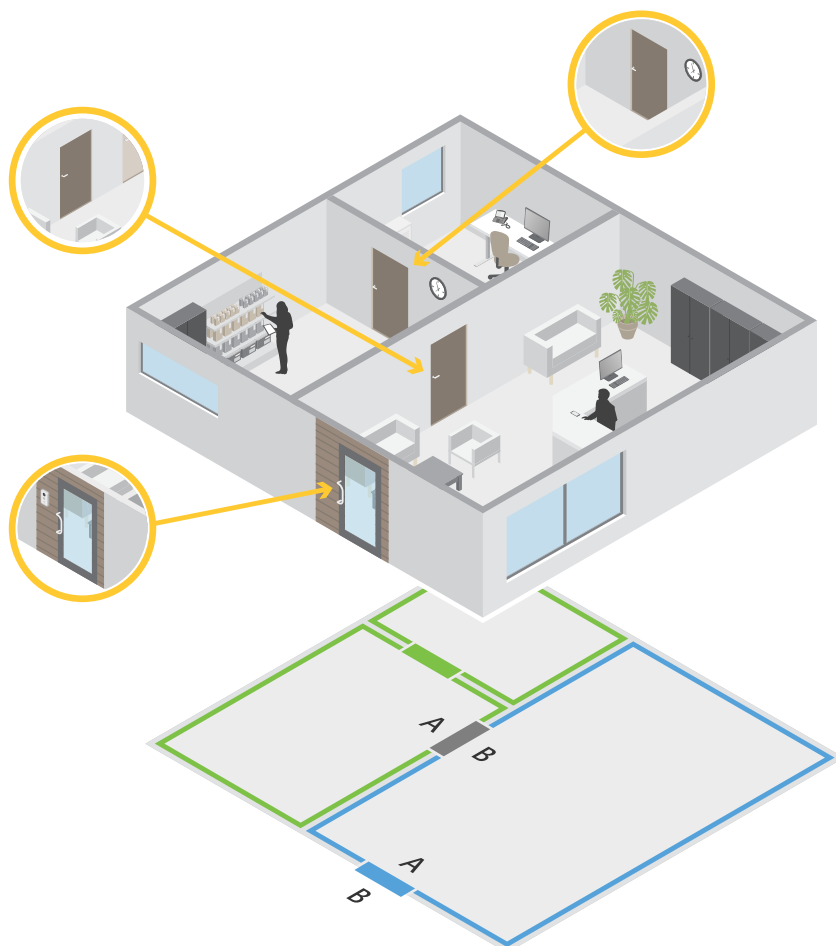
Przejdź do **Site Navigation > AXIS Optimizer > Access control > Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy), aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

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

Drzwi	
Nazwa	Nazwa drzwi.
Kontroler drzwi	Kontroler drzwi, z którym są połączone drzwi.
Strona A	Strefa, w której znajduje się strona A drzwi.
Strona B	Strefa, w której znajduje się strona B drzwi.
Profil identyfikacji	Profil identyfikacji przypisany do drzwi.
Formaty kart i kod PIN	Pokazuje typ formatów kart lub długość kodu PIN.
Status	Status drzwi. • Online: Drzwi są w trybie online i działają prawidłowo. • Czytnik offline: Czytnik podany w konfiguracji drzwi jest w trybie offline. • Błąd czytnika: Czytnik podany w konfiguracji drzwi nie obsługuje bezpiecznego kanału albo dla czytnika nie włączono bezpiecznego kanału.
Strefy	

Nazwa	Nazwa strefy.
Liczba drzwi	Liczba drzwi należących do strefy.

Przykład drzwi i stref



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

Dodawanie drzwi

Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku.
- 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. Patrz *Profile identyfikacji, on page 19*.
10. Skonfiguruj ustawienia drzwi. P. sekcja *Ustawienia drzwi, on page 8*.
11. Skonfiguruj drzwi dozorujące. P. sekcja *Dodawanie drzwi dozorujących, on page 11*.
12. Kliknij przycisk **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 (Kopiuje konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarzony, jeśli został skonfigurowany z dwoma drzwiami lub jednym z dwoma zamkami.
7. W razie potrzeby zmień ustawienia.
8. Kliknij przycisk **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)**.

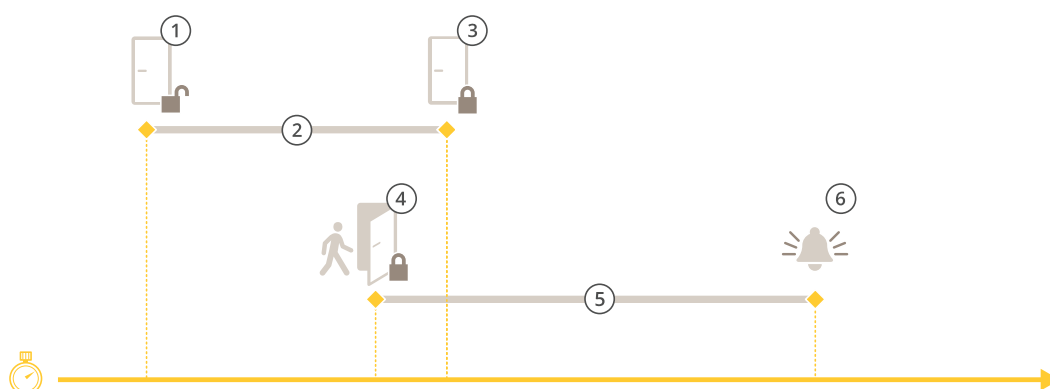
Reguła dwóch osób	
Side A (Strona A) i Side B (Strona B)	Wybierz, po których stronach drzwi ma być używana reguła.
Harmonogramy	Wybierz, kiedy reguła jest aktywna.
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi poświadczeniami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

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

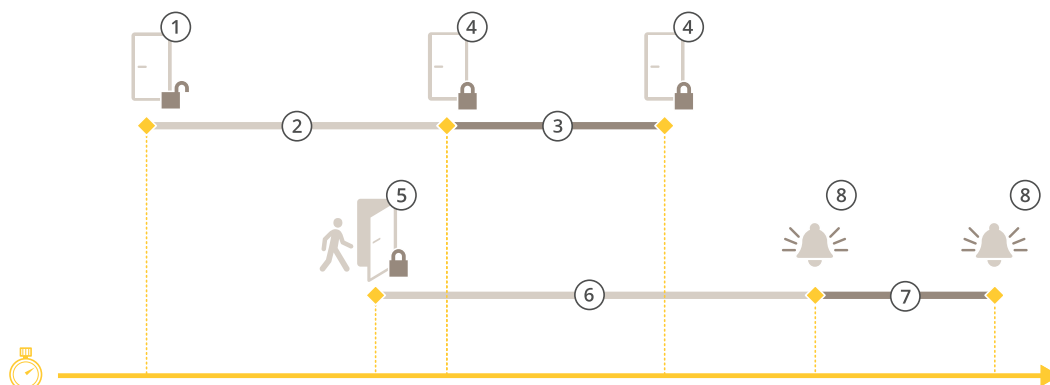
1. Przejdź do **Site Navigation > AXIS Optimizer > Access control > Doors and zones** (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Drzwi i strefy).
2. Wybierz drzwi, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom 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. Kliknij  przy posiadaczu karty, którego chcesz edytować, a następnie kliknij **Edit (Edytuj)**.
 - 7.3. Kliknij **More (Więcej)**.
 - 7.4. Wybierz **Allow double-swipe (Zezwól na przeciągnięcie dwóch kart)**.
 - 7.5. Kliknij przycisk **Apply (Zastosuj)**.

Dwukrotne przeciągnięcie	
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi 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 *Dodawanie drzwi*, on page 6
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.
3. Wybierz opcję **Door monitor sensor (Czujnik monitora drzwi)**.
4. Zaznacz port we/wy, do którego chcesz podłączyć monitor drzwi.

5. W obszarze **Door open if (Otwórz drzwi, jeśli)**, wybierz sposób podłączenia obwodów monitora drzwi.
6. Aby zmiany stanu cyfrowego wejścia były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Debounce time (Czas odbicia)**.
7. Aby przerwanie połączenia między kontrolerem drzwi i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. P. sekcja *Nadzorowane wejścia, on page 15*.

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 5*.

1. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodawanie drzwi, on page 6*.
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.) .
Nadzorowane wejście	Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. P. sekcja <i>Nadzorowane wejścia, on page 15</i> .

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 dźwawkowe.

1. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodawanie drzwi, on page 6*.
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 15*.

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

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

Dodawanie strefy

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

- **Perimeter door: (Drzwi na obwodzie)** Posiadacze kart wchodzą do strefy i wychodzą ze strefy przez te drzwi.
- **Drzwi wewnętrzne:** Wewnętrzne drzwi w strefie.

Uwaga

Drzwi obwodowe mogą należeć do dwóch stref. Drzwi wewnętrzne mogą należeć tylko do jednej strefy.

1. 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 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 (wersji twardej)) tylko wtedy, gdy wszystkie drzwi w strefie mają czytniki po obu stronach.

Nadzorowane wejścia

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

- Podłączenie między kontrolerem drzwi a monitorem drzwi. P. sekcja *Dodawanie monitora drzwi, on page 10*.
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Zobacz *Dodawanie czytnika, on page 11*.
- Podłączenie między kontrolerem drzwi a urządzeniem REX. P. sekcja *Dodawanie urządzenia REX, on page 13*.

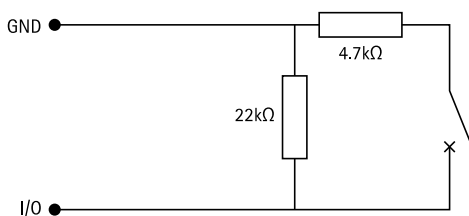
Aby użyć nadzorowanych wejść:

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 K Ω parallel resistor and a 4.7 K Ω serial resistor (Pierwsze połączenie równoległe z 22 k Ω opornikiem równoległym i 4,7 k Ω opornikiem szeregowym)**.
4. Jeżeli zastosowano schemat pierwszego połączenia szeregowego, zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z rozwijalnego menu **Resistor values (Wartości oporników)** wybierz wartość rezystora.

Schematy połączeń

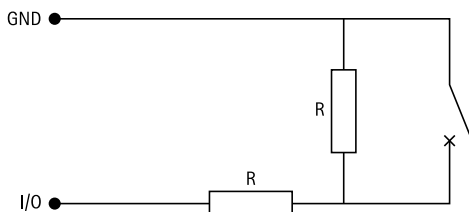
Pierwsze połączenie równoległe

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



Pierwsze połączenie szeregowo

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.

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

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

Aby wykonać akcję ręcznie:

1. 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 również pozycyjnym systemem liczbowym o podstawie 16 – składa się z 16 unikatowych symboli: cyfr 0–9 i liter a–f.
Kolejność bitów podzakresu	Wybierz kolejność bitów. Little endian : Pierwszy bit jest najmniejszy (najmniej znaczący). Big endian : Pierwszy bit jest największy (najbardziej znaczący).

Aby 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:

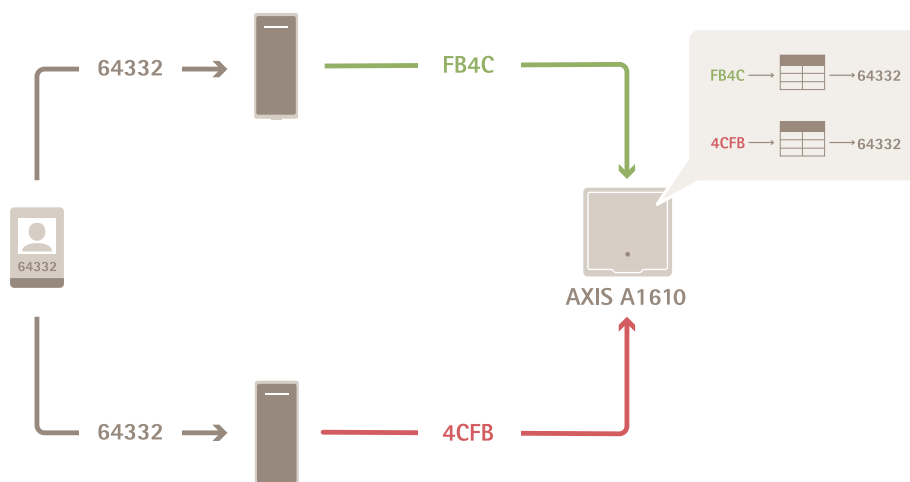
1. Przejdź do Site Navigation > AXIS Optimizer > Access control > Card formats and PIN (Nawigacja po obiekcie > AXIS Optimizer > Kontrola dostępu > Formaty kart i kod PIN).
2. Kliknij , aby w formacie karty przywrócić domyślną mapę pól.

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.

$$64332 = 1111\ 1011\ 0100\ 1100 \longrightarrow 0011\ 0010\ 1101\ 1111 = 13023$$

$\longrightarrow$ Read from left Read from right $\longleftarrow$

Odwróć kolejność bajtów

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

$$64\ 332 = \begin{matrix} 1111 & 1011 & 0100 & 1100 \\ \text{F} & \text{B} & 4 & \text{C} \end{matrix} \longrightarrow \begin{matrix} 0100 & 1100 & 1111 & 1011 \\ 4 & \text{C} & \text{F} & \text{B} \end{matrix} = 19707$$

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** (Profil 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.

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 21*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. P. sekcja *Importowanie pliku konfiguracyjnego do serwera głównego, on page 22*.
3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. P. sekcje *Dodawanie posiadacza karty, on page 23* i *Dodawanie grupy, on page 26*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz *Zarządzanie dostępem, on page 22*.

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:

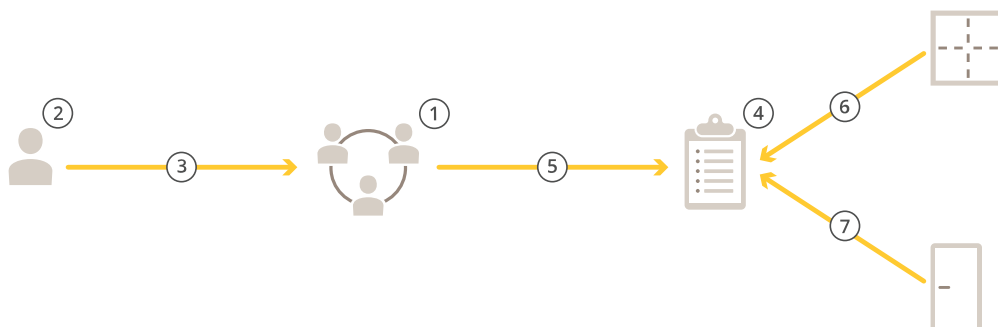
1. Na serwerze głównym:
 - 1.1. Przejdź do **Access management > Dashboard** (Zarządzanie dostępem > Pulpit nawigacyjny).
 - 1.2. Zmień globalnych posiadaczy kart i grupy na lokalnych posiadaczy kart i grupy.
 - 1.3. Przejdź do **AXIS Optimizer > Access control > Multi server** (AXIS Optimizer > Kontrola 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. Patrz *Dodawanie grupy*, on page 26.
2. Dodaj posiadaczy kart. Patrz *Dodawanie posiadacza karty*, on page 23.
3. Dodaj posiadaczy kart do grup.
4. Dodaj reguły dostępu. Patrz *Dodawanie reguły dostępu*, on page 26.
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. Patrz *Dodaj poświadczenia*, on page 24
6. Kliknij przycisk **Zapisz**.
7. Dodaj posiadacza karty do grupy.
 - 7.1. W obszarze **Groups** (Grupy) wybierz grupę, do której chcesz dodać posiadacza karty, i kliknij **Edit** (Edytuj).
 - 7.2. Kliknij **+ Add** (+ Dodaj) i wybierz posiadacza karty, którego chcesz dodać do grupy. Można wybrać wielu posiadaczy kart.
 - 7.3. Kliknij **Dodaj**.
 - 7.4. Kliknij przycisk **Zapisz**.

Zaawansowane	
Długi czas dostępu	Wybierz tę opcję, aby w sytuacji, gdy jest zainstalowany monitor drzwi, posiadacz karty miał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi.
Zawieś posiadacza karty	Wybierz, aby zawiesić posiadacza karty.
Zezwól na podwójne przeciągnięcie	Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Mogą go na

Zaawansowane	
	przykład użyć do odblokowania drzwi poza regularnym harmonogramem.
Zwolnienie z blokady ogólnej	Zaznacz, aby zezwolić posiadaczowi karty na dostęp podczas blokady.
Exempt from anti-passback (Zwolnienie z reguły anti-passback)	Wybierz tę opcję, aby przyznać zwolnić posiadacza karty z reguły anti-passback. Reguła Anti-passback uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Zanim takie poświadczenia będą mogły zostać użyte ponownie, posiadacz kart z tymi danymi musi najpierw opuścić obszar.
Globalny posiadacz karty	Zaznacz tę opcję, aby możliwe było wyświetlanie i monitorowanie posiadacza karty na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Patrz .

Dodaj poświadczenia

Do posiadacza karty można dodać następujące typy poświadczeń:

- 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 25*.

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 Secure Entry for XProtect.
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. Patrz *Dodawanie drzwi, on page 6*.
 - 4.1. Dodaj czytnik na **Side A (Strona A)**. P. sekcja *Dodawanie czytnika, on page 11*.
 - 4.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
 - 4.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
 - 4.4. Kliknij **OK**.
5. Zainstaluj i włącz w kamerze aplikację **AXIS License Plate Verifier**. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
6. Włącz aplikację **AXIS License Plate Verifier**.
7. Skonfiguruj aplikację **AXIS License Plate Verifier**.

- 7.1. Przejdź do **Configuration > Access control > Encrypted communication** (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana).
- 7.2. W obszarze **External Peripheral Authentication Key** (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego) kliknij polecenie **Show authentication key** (Pokaż klucz uwierzytelniania) oraz **Copy key** (Kopiuj klucz).
- 7.3. Otwórz aplikację **AXIS License Plate Verifier** z poziomu interfejsu WWW kamery.
- 7.4. Nie przeprowadzaj konfiguracji.
- 7.5. Przejdź do opcji **Settings** (Ustawienia).
- 7.6. W obszarze **Access control** (Kontrola dostępu) wybierz **Secure Entry** (Bezpieczne wejście) jako **Type** (Typ).
- 7.7. W obszarze **IP address** (Adres IP) wpisz adres IP kontrolera drzwi.
- 7.8. W obszarze **Authentication key** (Klucz uwierzytelniania) wklej skopiowany wcześniej klucz uwierzytelniania.
- 7.9. Kliknij przycisk **Połącz**.
- 7.10. W obszarze **Door controller name** (Nazwa kontrolera drzwi) wybierz kontroler drzwi.
- 7.11. W obszarze **Reader name** (Nazwa czytnika) wybierz czytnik dodany wcześniej.
- 7.12. Włącz integrację.
8. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Patrz *Dodawanie posiadacza karty, on page 23*.
9. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Patrz *Dodaj poświadczenia, on page 24*.
10. Dodaj regułę dostępu. Patrz *Dodawanie reguły dostępu, on page 26*.
 - 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 21*.
5. Dodawanie posiadaczy kart do grupy:
 - 5.1. Kliknij **+ Dodaj**.
 - 5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add** (Dodaj).
6. Kliknij przycisk **Zapisz**.

Dodawanie reguły dostępu

Reguła dostępu określa warunki, które muszą zostać spełnione w celu udzielenia dostępu.

Reguła dostępu zawiera następujące elementy:

Posiadacze kart i ich grupy – komu ma zostać przyznany dostęp.

Drzwi i strefy – gdzie ma zostać przyznany dostęp.

Harmonogramy – kiedy ma zostać przyznany dostęp.

Aby dodać regułę dostępu:

1. 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 **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 16*.

Aby uzyskać informacje na temat czynności wykonywanych ręcznie, takich jak ręczne odblokowywanie strefy, p. sekcja *Akcje wykonywane ręcznie, on page 16*.

Eksportowanie raportów konfiguracji systemu

Można eksportować raporty zawierające różne rodzaje informacji o systemie. AXIS Secure Entry for XProtect 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 **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 raporcie ze zbiórki	Opis
Safe (Bezpieczny)	Posiadacz karty przeciągnął swoją kartę w punkcie zbiórki.
Missing (Zaginiony)	Posiadacz karty nie przeciągnął swojej karty w punkcie zbiórki.

Ustawienia zarządzania dostępem

Aby dostosować pola posiadacza karty używane na pulpicie nawigacyjnym dostępu:

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

Aby używać kodu obiektu do weryfikowania systemu kontroli dostępu:

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

Uwaga

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

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 nagłówki 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.

Ustawienia importu	
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 Secure Entry for XProtect 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 4*.
3. Sprawdź, czy zalogowany użytkownik ma uprawnienia do zarządzania dostępem, p. sekcja *Ustawienia ról w aplikacji AXIS Secure Entry, on page 31*.

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

T10234037_pl

2026-06 (M4.6)

© 2025 – 2026 Axis Communications AB