

# **AXIS Camera Station Pro Secure Entry**

### Informacje

Secure Entry jest komponentem programu AXIS Camera Station Pro. Użyj go do dodawania urządzeń i zarządzania harmonogramami. Więcej informacji znajduje się w *instrukcji obsługi programu AXIS Camera Station Pro*.

## Skonfiguruj kontrolę dostępu

Jeżeli do systemu dodano sieciowy kontroler drzwiowy Axis, można skonfigurować sprzęt kontroli dostępu w programie AXIS Camera Station w wersji 6.x lub nowszej.

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

### Uwaga

Na początek wykonaj następujące czynności:

- Zaktualizuj wersję systemu operacyjnego AXIS OS kontrolera w obszarze **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
- Ustaw datę i godzinę kontrolera w oknie **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
- Włącz obsługę protokołu HTTPS na kontrolerze w oknie **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).

### Proces konfigurowania kontroli dostępu

1. Aby zmodyfikować predefiniowane profile identyfikacji lub utworzyć nowy profil identyfikacji, p. sekcja *Profile identyfikacji*, on page 22.
2. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, zob. *Formaty kart i kod PIN*, on page 25.
3. Dodaj drzwi i zastosuj do nich profil identyfikacji. Zob. *Dodaj drzwi*, on page 8.
4. Skonfiguruj drzwi:
  - *Dodawanie czujnika pozycji drzwi*, on page 14
  - *Dodawanie czujnika awaryjnego*, on page 15
  - *Dodawanie czytnika*, on page 17
  - *Dodawanie urządzenia REX*, on page 18
5. Dodaj strefę, a następnie drzwi do strefy. Zob. *Dodawanie strefy*, on page 20.

## Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

### Ważne

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

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

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

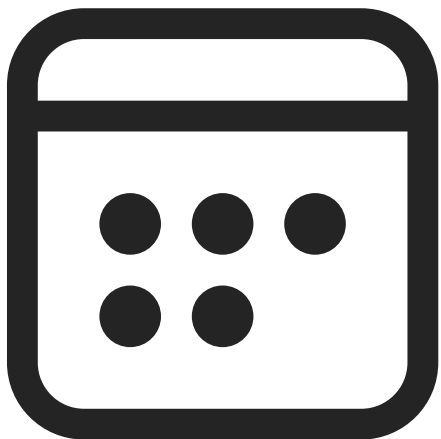
- **Przyszłe zalecenia dotyczące oprogramowania AXIS OS:** Aby zapewnić stabilność systemu i pełną zgodność, należy zawsze przestrzegać wersji oprogramowania AXIS OS zalecanej dla danej wersji programu AXIS Camera Station Pro Secure Entry.
- **Zmiana ścieżki:** Zmiana ścieżki oprogramowania układowego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

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

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

### Drzwi i strefy

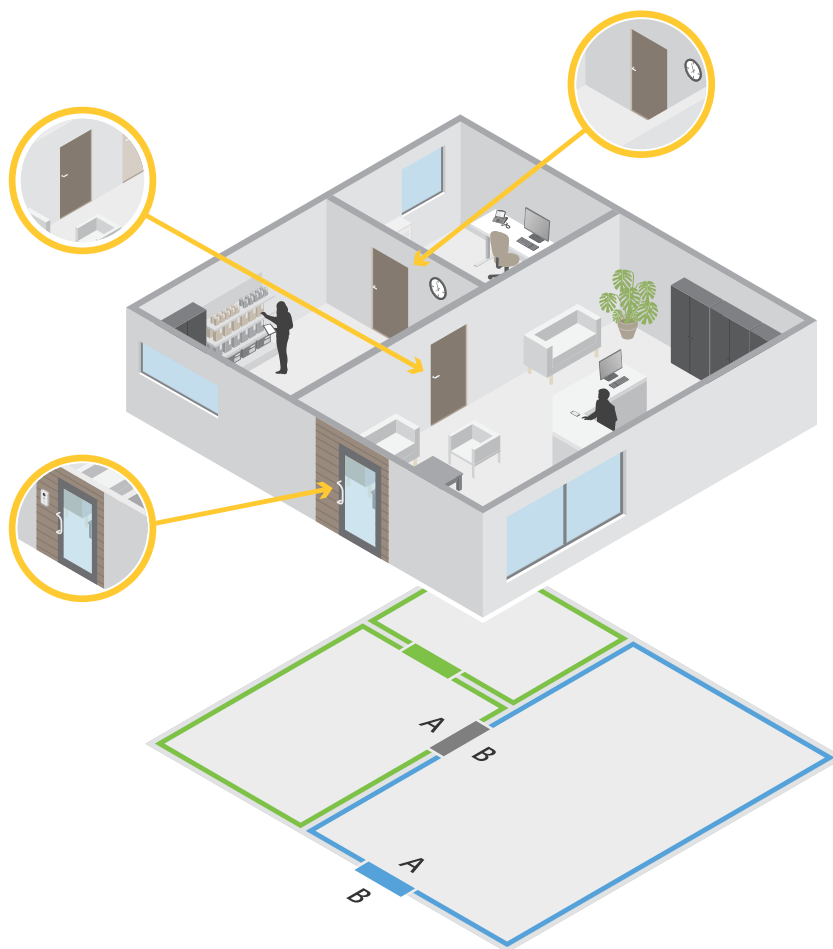
Wybierz kolejno opcje **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy), aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

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

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

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP address (Adres IP) | Adres IP sterownika drzwiowego dołączonego do drzwi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Strona A              | Strefa, w której znajduje się strona A drzwi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Strona B              | Strefa, w której znajduje się strona B drzwi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Profil identyfikacji  | Profil identyfikacji przypisany do drzwi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Akumulator            | Stan akumulatora kontrolera drzwi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Status                | <p>Stan drzwi.</p> <ul style="list-style-type: none"> <li>• <b>Online:</b> Drzwi są w trybie online i działają prawidłowo.</li> <li>• <b>Reader offline (Czytnik offline):</b> Czytnik w konfiguracji drzwi jest w trybie offline.</li> <li>• <b>Reader error (Błąd czytnika):</b> Czytnik nie obsługuje bezpiecznego kanału lub funkcja ta została dla niego wyłączona.</li> <li>• <b>Old firmware (Stare oprogramowanie układowe):</b> Urządzenie korzysta z przestarzałej wersji oprogramowania układowego. Zaktualizuj oprogramowanie układowe, aby zapewnić najlepsze działanie i bezpieczeństwo.</li> </ul> |
| <b>Strefy</b>         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Nazwa                 | Nazwa strefy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Liczba drzwi          | Liczba drzwi należących do strefy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Poziom zabezpieczeń   | Poziom zabezpieczeń zastosowany w tej strefie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Przykład drzwi i stref



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

## 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. Wybierz kolejno opcje **Configuration (Konfiguracja)** > **Access control (Kontrola dostępu)** > **Doors and zones (Drzwi i strefy)**.

2. Wybierz drzwi albo strefę.
3. Kliknij dowolną akcję wykonywaną ręcznie.

## Drzwi

### Dodaj drzwi

#### Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku. Kontrolery wielofunkcyjne obsługują dodatkowe konfiguracje zamków.

Aby dodać drzwi:

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

| Typy drzwi          |                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Drzwi               | Zwykłe drzwi z monitorem drzwi obsługującym rygle i czytniki. Wymaga kontrolera drzwiowego.                                                                                                                  |
| Piętro              | Rodzaj drzwi do sterowania windą uwierzytelniający dostęp do pięter z windy za pomocą czytników kart. Więcej informacji znajduje się w sekcji <i>Dodawanie piętra<sup>BETA</sup></i> , on page 9.            |
| Drzwi dozoruujące   | Drzwi, które mogą zgłaszać, czy są otwarte, czy zamknięte. Więcej informacji znajduje się w sekcji <i>Dodawanie drzwi dozoruujących</i> , on page 10.                                                        |
| Drzwi bezprzewodowe | Drzwi, które można skonfigurować za pomocą bezprzewodowych rygli i koncentratorów komunikacyjnych ASSA ABLOY Aperio®. Więcej informacji znajduje się w sekcji <i>Dodaj zamek bezprzewodowy</i> , on page 10. |
| Drzwi zastępcze     | Drzwi zastępcze, które możesz dodać do systemu bez wybierania sprzętu.                                                                                                                                       |

3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami. Sterownik jest wyszarzony, gdy nie można dodać kolejnych drzwi, gdy jest w trybie offline lub gdy nie jest włączony protokół HTTPS.
4. Kliknij przycisk **Next (Dalej)**, aby przejść do strony konfiguracyjnej drzwi.
5. W rozwijalnym menu **Primary lock (Zamek główny)** wybierz port przekaźnika.
6. Aby skonfigurować dwa zamki w drzwiach, wybierz port przekaźnika z rozwijalnego menu **Secondary lock (Drugi zamek)**.
7. Wybierz profil identyfikacji. Zob. *Profile identyfikacji*, on page 22.
8. Konfiguruj drzwi, dodając czujniki lub czytniki w obszarze **Sensors** (Czujniki), **Side A** (Strona A) i **Side B** (Strona B).
9. Skonfiguruj ustawienia właściwe dla drzwi. Zobacz *Ustawienia drzwi*, on page 12.
10. Kliknij przycisk **Save (Zapisz)**.

Kopiowanie konfiguracji drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **+** **Add (Dodaj)**.
3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device (Urządzenie)** celem powiązania go z drzwiami.
4. Kliknij **Next (Dalej)**.
5. Z rozwijalnego menu **Copy configuration (Kopiuje konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarzony, jeśli został skonfigurowany z dwoma drzwiami lub jednym drzwiami z dwoma zamkami.
6. W razie potrzeby zmień ustawienia.
7. Kliknij przycisk **Save (Zapisz)**.



*Dodawanie i konfigurowanie drzwi i stref*

## **Dodawanie piętra<sup>BETA</sup>**

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

Zanim zaczniesz, potrzebujesz:

- Obsługiwanego sieciowego kontrolera drzwiowego dodanego do systemu np. *AXIS A1610*, *AXIS A1710-B* lub *AXIS A1810-B*.
- Modułu rozszerzeń we / wy na potrzeby współpracy z dodatkowymi przekaźnikami. Polecamy model *AXIS A9920*.

### **Uwaga**

Ta funkcja jest w fazie Beta i obecnie obsługuje jedynie maks. 64 piętra oraz czytniki kart.

Aby skonfigurować piętro:

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

### Uwaga

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

### Dodawanie drzwi dozorujących

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

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

### Uwaga

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

Aby skonfigurować drzwi dozorujące:

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

### Dodaj zamek bezprzewodowy

AXIS Camera Station Pro Secure Entry obsługuje zamki bezprzewodowe ASSA ABLOY Aperio® i koncentratory komunikacyjne. Zamek bezprzewodowy łączy się z systemem za pośrednictwem koncentratora komunikacyjnego Aperio podłączonego do złącza RS485 kontrolera drzwi. Do jednego kontrolera drzwi można podłączyć 16 zamków bezprzewodowych.



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

## Uwaga

- Konfiguracja wymaga, aby kontroler drzwi Axis miał system AXIS OS w wersji 11.6.16.1 lub nowszej.
  - Konfiguracja wymaga ważnej licencji AXIS Door Controller Extension.
  - Czas na kontrolerze drzwiowym Axis i serwerze AXIS Camera Station Pro Secure Entry musi być zsynchronizowany.
  - Przed rozpoczęciem skorzystaj z aplikacji Aperio obsługiwanej przez ASSA ABLOY, aby sparować zamki Aperio z koncentratorem Aperio.
  - Do każdego złącza RS485 można podłączyć tylko jeden koncentrator komunikacyjny Aperio. Technologia multi-drop nie jest obsługiwana.
  - Zamki bezprzewodowe nie działają zgodnie z harmonogramami odblokowywania, gdy są w trybie offline.
1. Otwórz kontroler drzwi.
    - 1.1. Wybierz kolejno opcje **Configuration > Devices > Other devices (Konfiguracja > Urządzenia > Inne urządzenia)**.
    - 1.2. Otwórz interfejs WWW kontrolera drzwi podłączonego do koncentratora komunikacyjnego Aperio.
  2. Włącz AXIS Door Controller Extension.
    - 2.1. W interfejsie WWW kontrolera drzwi przejdź do opcji **Apps (Aplikacje)**.
    - 2.2. Otwórz menu kontekstowe AXIS Door Controller Extension .
    - 2.3. Kliknij polecenie **Activate license with a key (Aktywuj licencję kluczem)** i wybierz licencję.
    - 2.4. Włącz **AXIS Door Controller Extension**.
  3. Podłącz zamek bezprzewodowy do kontrolera drzwi za pośrednictwem koncentratora komunikacyjnego.
    - 3.1. W interfejsie WWW kontrolera drzwi przejdź do menu **Access control > Wireless locks (Kontrola dostępu > Zamki bezprzewodowe)**.
    - 3.2. Kliknij polecenie **Connect communication hub (Połącz koncentrator komunikacyjny)**.
    - 3.3. Wprowadź nazwę koncentratora i kliknij przycisk **Connect (Połącz)**.
    - 3.4. Kliknij przycisk **Connect wireless lock (Podłącz zamek bezprzewodowy)**.
    - 3.5. Wybierz adres i funkcje zamka, który chcesz dodać, a następnie kliknij przycisk **Save (Zapisz)**.
  4. Dodaj i skonfiguruj drzwi z zamkiem bezprzewodowym.
    - 4.1. W sekcji AXIS Camera Station Pro Secure Entry wybierz kolejno **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
    - 4.2. W obszarze **Doors (Drzwi)** kliknij  **Add (Dodaj)**.
    - 4.3. Jako **Door type (Rodzaj drzwi)** wybierz **Wireless door (Drzwi bezprzewodowe)** i kontroler drzwiowy dołączony do koncentratora komunikacyjnego Aperio.
    - 4.4. Kliknij **Next (Dalej)**.
    - 4.5. Wybierz **Wireless lock (Zamek bezprzewodowy)**.
    - 4.6. Określ strony A i B drzwi i dodaj czujniki. Aby uzyskać dodatkowe informacje, zob. *Drzwi i strefy, on page 4*.
    - 4.7. Kliknij przycisk **Save (Zapisz)**.

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

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

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

### Ustawienia drzwi

Aby zmodyfikować drzwi:

1. Wybierz kolejno opcje **Configuration > Access control > Door and Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**.
2. Wybierz drzwi, które chcesz edytować.
3. Kliknij  **Edit (Edytuj)**.
4. W obszarze **Door settings (Ustawienia drzwi)** zmień dowolne ustawienia i kliknij **Save (Zapisz)**.

|                                                                             |                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Czas dostępu (s)                                                            | Ustaw, przez ile sekund drzwi pozostaną odblokowane po przyznaniu dostępu. Drzwi ponownie zaryglują się po zamknięciu, nawet gdy pozostał jeszcze czas.                                                                                                                                                                                              |
| Open-too-long time (sec) (Przekroczony czas otwarcia drzwi (s))             | Dotyczy tylko, gdy monitor drzwi jest skonfigurowany. Ustaw, przez ile sekund drzwi mogą pozostać otwarte. Jeżeli drzwi będą nadal otwarte po upływie określonego czasu, uruchomi się alarm sygnalizujący zbyt długie otwarcie drzwi. Skonfiguruj regułę działania, aby określić, co ma się stać po wystąpieniu tego zdarzenia będącego wyzwalaczem. |
| Długi czas dostępu (s)                                                      | Ustaw, przez ile sekund drzwi pozostają odblokowane po przyznaniu dostępu posiadaczom kart, u których ustawienie to jest dostępne. Ma to priorytet przed standardowym czasem dostępu.                                                                                                                                                                |
| Long open-too-long time (sec) (Długi czas przekroczenia otwarcia drzwi (s)) | Dotyczy tylko, gdy monitor drzwi jest skonfigurowany. Ustaw, przez ile sekund drzwi mogą pozostać otwarte dla posiadaczy kart z dostępną opcją <b>Long access time (Długi czas dostępu)</b> . Ma to priorytet przed standardowym czasem zbyt długiego otwarcia.                                                                                      |
| Czas opóźnienia do ponownego zablokowania (ms)                              | Ustaw, ile milisekund drzwi pozostają odblokowane po ich otwarciu lub zamknięciu.                                                                                                                                                                                                                                                                    |
| Ponowne zablokowanie                                                        | <ul style="list-style-type: none"> <li>• <b>After opening (Po otwarciu):</b> Dotyczy tylko scenariuszy z dodanym monitorem drzwi.</li> <li>• <b>After closing (Po zamknięciu):</b> Dotyczy tylko scenariuszy z dodanym monitorem drzwi.</li> </ul>                                                                                                   |

|                                  |                                                                                                                        |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Drzwi wyważone                   | Określ, czy system ma wyzwać alarm systemowy w przypadku wyważenia drzwi. Wymagany jest czujnik położenia drzwi (DPS). |
| Przekroczony czas otwarcia drzwi | Określ, czy system ma wyzwać alarm systemowy w przypadku pozostawienia na zbyt długo otwartych drzwi.                  |

Aby usunąć drzwi:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Doors (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Drzwi)**.
2. Wybierz drzwi z listy.
3. Kliknij  **Remove (Usuń)** i potwierdź.

### Poziom zabezpieczeń drzwi

Do drzwi można dodać następujące zabezpieczenia:

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

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

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

Aby dodać regułę dwóch osób do istniejących drzwi:

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

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

Aby dodać przeciągnięcie dwóch kart do istniejących drzwi:

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.

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

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

### Dodawanie czujnika pozycji drzwi

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

1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 8*.
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.
3. Wybierz **Door position sensor (Czujnik pozycji drzwi)**.
4. Zaznacz port we/wy, do którego chcesz podłączyć monitor drzwi.
5. W obszarze **Door open if (Otwórz drzwi, jeśli)**, wybierz sposób podłączenia obwodów monitora drzwi.
6. Aby zmiany stanu cyfrowego wejścia były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Debounce time (Czas odbicia)**.
7. Aby przerwanie połączenia między kontrolerem drzwiowym i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Zob. *Nadzorowane wejścia, on page 14*.

| 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.   |

### Nadzorowane wejścia

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

- Podłączenie między kontrolerem drzwi a monitorem drzwi. Zob. *Dodawanie czujnika pozycji drzwi, on page 14*.

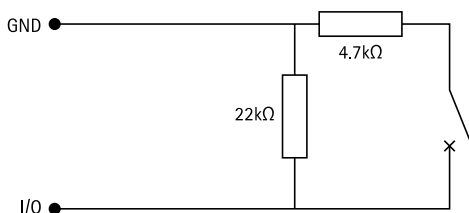
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Zob. *Dodawanie czytnika, on page 17.*
- Podłączenie między kontrolerem drzwi a urządzeniem REX. Zob. *Dodawanie urządzenia REX, on page 18.*

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

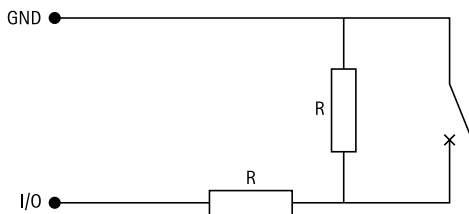
#### Pierwsze połączenie równoległe

Oporniki muszą mieć wartości 4,7 k $\Omega$  i 22 k $\Omega$ .



#### Pierwsze połączenie szeregowe

Oporniki muszą mieć takie same wartości w przedziale 1-10 k $\Omega$ .



#### Dodawanie czujnika awaryjnego

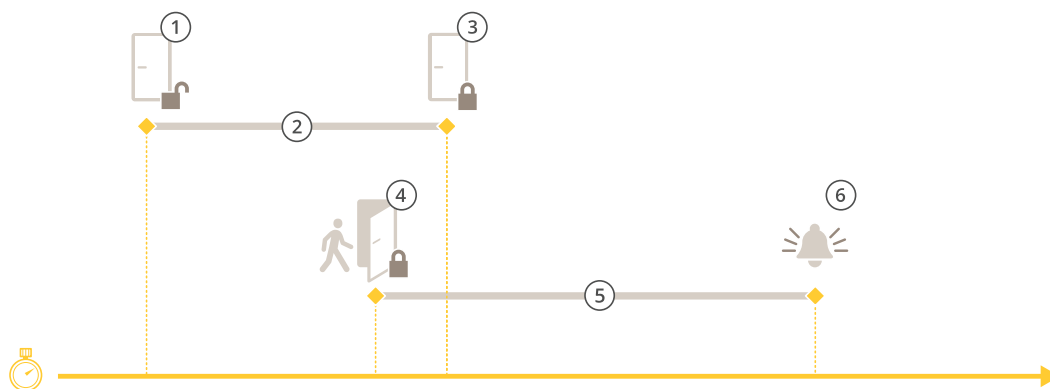
Można dodać i skonfigurować wejście awaryjne, aby zainicjować akcję blokującą lub odblokowującą drzwi. Można również skonfigurować sposób łączenia obwodu.

1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 8.*
2. W obszarze **Sensors (Czujniki)** kliknij **+ Add (Dodaj)**.
3. Wybierz opcję **Emergency input (Wejście awaryjne)**.
4. W obszarze **Emergency state (Stan awaryjny)** wybierz połączenie obwodu.
5. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
6. Wybierz **Emergency action (Akcję awaryjną)**, która ma być wyzwalana po odebraniu przez drzwi sygnału stanu awaryjnego.

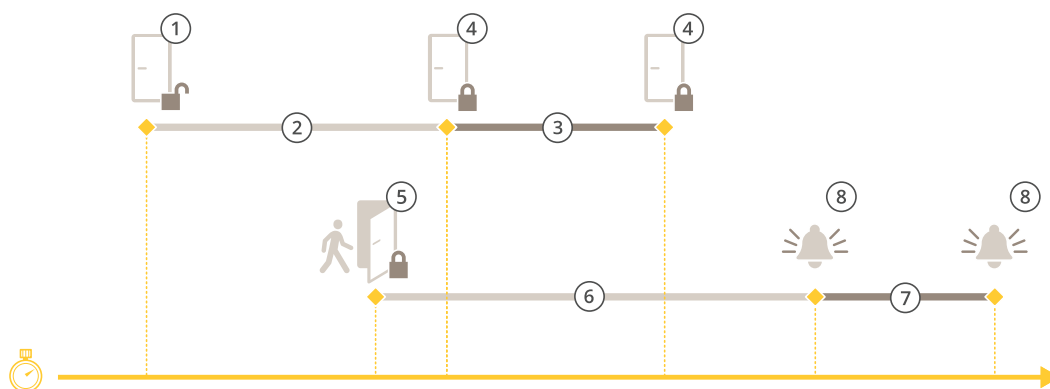
| Stan awaryjny        |                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Obwód jest otwarty   | Obwód wejścia awaryjnego jest rozwierny (NC). Wejście awaryjne będzie wysyłać sygnał stanu awaryjnego, gdy obwód zostanie otwarty. |
| Obwód jest zamknięty | Obwód wejścia awaryjnego jest zwierny (NO). Wejście awaryjne będzie wysyłać sygnał stanu awaryjnego, gdy obwód zostanie zamknięty. |

| Działanie awaryjne |                                                               |
|--------------------|---------------------------------------------------------------|
| Odblokuj drzwi     | Drzwi odblokowują się po otrzymaniu sygnału stanu awaryjnego. |
| Zablokuj drzwi     | Drzwi blokują się po otrzymaniu sygnału stanu awaryjnego.     |

### Opcje czasu



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



- 1 Dostęp przyznany – zamek odblokowany

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

## Dodawanie czytnika

Kontroler drzwiowy można skonfigurować tak, aby obsługiwał kilka czytników przewodowych. Czytniki można dodać po jednej lub obu stronach drzwi.

Jeżeli do czytnika zastosujesz niestandardową konfigurację formatów kart lub długości kodów PIN, pojawi się to w kolumnie **Card formats** (Formaty kart) w obszarze **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy). Zob. *Drzwi i strefy, on page 4*.

### Uwaga

- Do kontrolera drzwiowego można również dołączyć maks. 16 czytników Bluetooth. Więcej informacji znajduje się w sekcji *Dodawanie czytnika Bluetooth, on page 19*.
  - Jeżeli jako czytnik IP używany jest domofon sieciowy Axis, system używa konfiguracji kodu PIN ustawionej na stronie internetowej urządzenia.
1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 8*.
  2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
  3. Wybierz **Card reader (Czytnik kart)**.
  4. Wybierz **Reader type (Typ czytnika)**.
  5. Aby użyć niestandardowej długości kodu PIN dla tego czytnika.
    - 5.1. Kliknij przycisk **Advanced (Zaawansowane)**.
    - 5.2. Włącz opcję **Custom PIN length (Niestandardowa długość kodu PIN)**.
    - 5.3. Wypełnij pola **Min PIN length (Min. długość kodu PIN)**, **Max PIN length (Maks. długość kodu PIN)** i **End of PIN character (Koniec znaku kodu PIN)**.
  6. Aby użyć niestandardowego formatu karty tego czytnika:
    - 6.1. Kliknij przycisk **Advanced (Zaawansowane)**.
    - 6.2. Włącz opcję **Custom card formats (Niestandardowe formaty kart)**.
    - 6.3. Wybierz formaty karty na takie, których chcesz używać w czytniku. Jeżeli format karty o tej samej liczbie bitów jest już używany, należy go najpierw zdezaktywować. Gdy konfiguracja formatu karty różni się od poczynionej w konfiguracji systemu, w aplikacji klienckiej pojawia się ikona ostrzeżenia.
  7. Kliknij **Dodaj**.
  8. Aby dodać czytnik po drugiej stronie drzwi, powtórz tę procedurę.

Aby uzyskać informacje o instalacji czytnika kodów kreskowych AXIS Barcode Reader, p. sekcja *Instalowanie aplikacji AXIS Barcode Reader, on page 24*.

| Typ czytnika           |                                                                                  |
|------------------------|----------------------------------------------------------------------------------|
| OSDP RS485 half duplex | Dla czytników RS485 należy wybrać <b>OSDP RS485 half duplex</b> i port czytnika. |

|            |                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wiegand    | W przypadku czytników używających protokołów Wiegand zaznacz opcję <b>Wiegand</b> oraz w sekcji Ogólne wybierz port dla czytnika.                                                 |
| Czytnik IP | W przypadku czytników sieciowych zaznacz opcję <b>IP reader (Czytnik IP)</b> i wybierz urządzenie z menu rozwijanego. Domofony sieciowe Axis możesz wykorzystać jako czytniki IP. |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wiegand                                                         |                                                                                                                                                                                                                                                                                                                                                          |
| Sterowanie LED                                                  | Wybierz opcję <b>Single wire (Pojedynczy przewód)</b> lub <b>Dual wire (R/G) (Podwójny przewód (R/G))</b> . Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED.                                                                                                                                               |
| Powiadomienie o sabotażu                                        | Wybierz stan obwodu, który uaktywnia wejście sabotażu w czytniku. <ul style="list-style-type: none"> <li>• <b>Open circuit (Obwód otwarty)</b>: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie otwarty.</li> <li>• <b>Closed circuit (Obwód zamknięty)</b>: Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie zamknięty.</li> </ul> |
| 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 <b>Tamper debounce time (Czas odbicia zabezp. przeciwsab.)</b> .                                                                                                                                                  |
| Wejście nadzorowane                                             | Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. Zob. <i>Nadzorowane wejścia, on page 14</i> .                                                                                                                                                                                                   |

### Dodawanie urządzenia REX

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

1. Przejdź do strony konfiguracyjnej drzwi. Zob. *Dodaj drzwi, on page 8*.
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **REX device (Urządzenie REX)**.
4. Zaznacz port we / wy, do którego chcesz dołączyć urządzenie REX. Jeżeli dostępny jest tylko jeden port, zostanie on wybrany automatycznie.
5. Wybierz **Action (Akcja)**, która ma być wyzwalana po odebraniu sygnału REX przez drzwi.
6. W obszarze **REX active (Aktywne REX)** wybierz połączenie obwodu monitora drzwi.
7. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
8. Aby przerwanie połączenia między kontrolerem drzwiowym i urządzeniem REX powodowało wyzwolenie zdarzenia, włącz **Supervised input (Nadzorowane wejście)**. Zob. *Nadzorowane wejścia, on page 14*.

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

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

### Dodawanie czytnika IP

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

#### Uwaga

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

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

Po dodaniu urządzenie możesz przydzielić do drzwi. Zobacz *Dodawanie czytnika, on page 17*.

### Dodawanie czytnika Bluetooth

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

Instalacja i stosowanie tych czytników nie wymaga dodatkowych licencji.

Aby dodać czytnik AXIS A4612 Network Bluetooth Reader do drzwi:

1. Sprawdź, czy czytnik AXIS A4612 został sparowany z kontrolerem drzwiowym. P. sekcja *Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth, on page 19*.
2. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodaj drzwi, on page 8*.
3. Pod jedną stroną drzwi kliknij **+ Add** (Dodaj), a następnie **Card reader** (Czytnik kart).
4. Zaznacz **IP reader** (Czytnik IP) i wybierz sparowany czytnik AXIS A4612 z rozwijalnego menu. Jeżeli czytnik ten jest stosowany do parowania uwierzytelnień, zaznacz go na potrzeby parowania. Kliknij **Dodaj**.
5. Na karcie **Overview** (Przegląd) zmień profil identyfikacji. Można użyć profili **Tap in app** (Dotknij w aplikacji) lub **Touch reader** (Czytnik dotykowy), jeżeli czytnik AXIS A4612 jest dołączony po jednej stronie drzwi, a po drugiej stosowany jest przycisk wyjścia REX.

### Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth

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

1. Zainstaluj czytnik Bluetooth i podłącz go do kontrolera drzwi.

2. Dodaj czytnik Bluetooth w interfejsie WWW kontrolera drzwi.
  - 2.1. Uzyskaj dostęp do kontrolera drzwi i przejdź do sekcji **Peripherals (Urządzenia peryferyjne) > Readers (Czytniki)**.
  - 2.2. Kliknij **Add reader (Dodaj czytnik)**.
  - 2.3. Wprowadź wymagane informacje w oknie dialogowym **Add Bluetooth reader (Dodaj czytnik Bluetooth)**.
  - 2.4. Kliknij **Dodaj**.
3. Dodaj czytnik Bluetooth do drzwi w programie AXIS Camera Station Pro Secure Entry.
  - 3.1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
  - 3.2. Wybierz drzwi, do których chcesz dodać czytnik Bluetooth, i kliknij **Edit (Edytuj)**.
  - 3.3. Kliknij **+ Add (Dodaj)** po stronie drzwi, gdzie znajduje się czytnik Bluetooth.
  - 3.4. Wybierz **Card reader (Czytnik kart)**.
  - 3.5. W sekcji **Add IP reader (Dodaj czytnik IP)** wybierz **IP reader (Czytnik IP)**.
  - 3.6. W sekcji **Select IP reader (Wybierz czytnik IP)** wybierz czytnik Bluetooth.
  - 3.7. Kliknij **Dodaj**.
4. Wybierz czytnik Bluetooth do sparowania. Należy je przeprowadzić w przypadku co najmniej jednego czytnika Bluetooth w systemie.
  - 4.1. Wybierz nowo dodany czytnik Bluetooth.
  - 4.2. Kliknij **Edit (Edycja)**.
  - 4.3. W sekcji **Edit bluetooth reader (Edytuj czytnik Bluetooth)** wybierz **Use this reader for pairing (Użyj tego czytnika do parowania)**.
  - 4.4. Kliknij przycisk **Apply (Zastosuj)**.
5. Wybierz profil identyfikacji **Tap in app (Dotknij w aplikacji)** lub **Touch reader (Dotknij czytnika)**. Więcej informacji p. *Profile identyfikacji, on page 22*.
6. Dodaj mobilne poświadczenia do posiadacza karty. Zob. *Dodaj poświadczenia, on page 33*.
7. Sparuj mobilne poświadczenia z czytnikiem z włączonym trybem parowania:
  - 7.1. Zbliz telefon komórkowy posiadacza karty do czytnika Bluetooth z włączonym trybem parowania.
  - 7.2. Postępuj zgodnie z instrukcjami podanymi w e-mailu wysłanym do posiadacza karty.

## Strefy

### 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. Patrz punkt *Przykład drzwi i stref, on page 7*, gdzie znajduje się ogólny przegląd.

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Kliknij **+ Add zone (Dodaj strefę)**.

3. Wprowadź nazwę strefy.
4. Kliknij **Add door (Dodaj drzwi)**.
5. Zaznacz drzwi, które chcesz dodać do strefy, i kliknij przycisk **Add (Dodaj)**.
6. Domyślnie drzwi zostaną ustawione jako obwodowe. Aby to zmienić, z menu rozwijanego wybierz pozycję **Internal door (Drzwi wewnętrzne)**.
7. Drzwi na obwodzie domyślnie jako wejścia do strefy używają strony A. Aby to zmienić, z menu rozwijanego wybierz opcję **Leave (Opuść)**.
8. Aby usunąć drzwi ze strefy, zaznacz ją i kliknij przycisk **Remove (Usuń)**.
9. Kliknij przycisk **Save (Zapisz)**.

Aby zmodyfikować strefę:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Wybierz strefę z listy.
3. Kliknij  **Edit (Edytuj)**.
4. Zmień ustawienia i kliknij przycisk **Save (Zapisz)**.

Aby usunąć strefę:

1. Wybierz kolejno opcje **Configuration > Access control > Doors and zones > Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy > Strefy)**.
2. Wybierz strefę z listy.
3. Kliknij  **Remove (Usuń)**.
4. Kliknij **Tak**.

### Poziom zabezpieczeń strefy

Do strefy można dodać następujące funkcje zabezpieczeń:

**Anti-passback** – Uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Aby ponownie skorzystać z uwierzytelnień, osoba musi najpierw opuścić obszar.

#### Uwaga

- W przypadku korzystania z funkcji anti-passback wszystkie drzwi w strefie muszą być wyposażone w czujniki położenia drzwi, aby system był w stanie zarejestrować, że użytkownik otworzył drzwi po przeciągnięciu karty.
- Jeśli kontroler drzwi przejdzie w tryb offline, funkcja anti-passback będzie nadal działać, pod warunkiem, że wszystkie drzwi w strefie należą do tego samego kontrolera drzwi. Jeśli jednak drzwi w strefie należą do różnych kontrolerów drzwi, które przejdą w tryb offline, funkcja anti-passback przestanie działać.

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

1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
2. Wybierz strefę, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz zabezpieczenia, które chcesz dodać do strefy.
6. Kliknij przycisk **Apply (Zastosuj)**.

| Anti-passback                                                            |                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log violation only (Soft) (Tylko rejestrowanie naruszeń (wersja miękka)) | Zaznacz tę opcję, aby umożliwić drugiej osobie wejście przy użyciu uwierzytelnień, których użyła pierwsza osoba. Ta opcja powoduje tylko wywołanie alarmu systemowego.                                                                                                                                                                                                           |
| Deny access (Hard) (Odmowa dostępu (wersja twarda))                      | Zaznacz tę opcję, aby uniemożliwić wejście drugiej osobie, jeżeli korzysta z uwierzytelnień, których użyła pierwsza osoba. Ta opcja powoduje także wywołanie alarmu systemowego.                                                                                                                                                                                                 |
| Limit czasu (w sekundach)                                                | Czas, po którym system zezwoli użytkownikowi na ponowne wejście. Wpisz 0, aby wyłączyć limit czasu, co oznacza, że funkcja anti-passback będzie obowiązywać do momentu opuszczenia strefy przez użytkownika. Użyj limitu czasu 0 z opcją <b>Deny access (Hard) (Odmowa dostępu (w wersji twardej))</b> tylko wtedy, gdy wszystkie drzwi w strefie mają czytniki po obu stronach. |

## Profile identyfikacji

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

### Uwaga

Dynamicznych kodów QR i PIN należy używać razem.

Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**, a zostanie wyświetlone okno, w którym można tworzyć, edytować i usuwać profile identyfikacji.

Dostępne profile identyfikacji:

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

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

**Kod PIN** – Aby uzyskać dostęp do drzwi, posiadacz karty musi wpisać kod PIN.

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

**Kod QR** – Aby uzyskać dostęp do drzwi, posiadacz kart musi okazać kod QR Code® do kamery. Profil identyfikacji Kod QR jest używany do statycznych i dynamicznych kodów QR.

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

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

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

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

## Tworzenie profilu identyfikacji

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.

2. Kliknij **+** **Create identification profile** (Utwórz profil identyfikacyjny).
3. Wpisz nazwę profilu identyfikacji.
4. Zaznacz opcję **Include facility code for card validation** (Uwzględnij kod obiektu w celu weryfikacji karty), aby używać kodu obiektu jako jednego z pól służących do weryfikacji poświadczeń. To pole jest dostępne tylko po włączeniu ustawienia **Facility code (Kod obiektu)** w obszarze **Access management > Settings (Zarządzanie dostępem > Ustawienia)**.
5. W przypadku strony A (Side A) kliknij **+** **Add (Dodaj)**, a następnie wybierz rodzaj identyfikacji i harmonogram.
  - Aby wymagać od posiadaczy kart użycia więcej niż jednego rodzaju identyfikacji, zaznacz kilka rodzajów w tym samym wierszu.
  - Aby umożliwić posiadaczom kart korzystanie z obu rodzajów, kliknij ponownie **+** **Add (Dodaj)** i dodaj kolejny wiersz.
6. W przypadku strony B (Side B) kliknij **+** **Add (Dodaj)**, a następnie wybierz rodzaj identyfikacji i harmonogram.
7. Kliknij **OK**.



*Konfigurowanie profilu identyfikacji*

## Edycja profilu identyfikacji

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles** (Konfiguracja > Kontrola dostępu > Profile identyfikacji).
2. Zaznacz profil identyfikacji i kliknij .
3. Aby zmienić nazwę profilu identyfikacji, wpisz nową nazwę.
4. Wprowadź zmiany z boku drzwi.
5. Aby zmodyfikować profil identyfikacji po drugiej stronie drzwi, powtórz poprzednie kroki.
6. Kliknij **OK**.

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

## Usuwanie profilu identyfikacji

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles** (Konfiguracja > Kontrola dostępu > Profile identyfikacji).
2. Zaznacz profil identyfikacji i kliknij .
3. Jeżeli profil identyfikacji został zastosowany do drzwi, wybierz dla nich inny profil identyfikacji.
4. Kliknij **OK**.

## Resetowanie wstępnie zdefiniowanego formatu karty

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN** (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN).
2. Kliknij , aby w formacie karty przywrócić domyślną mapę pól.

## AXIS Barcode Reader

AXIS Barcode Reader to aplikacja, którą można instalować w kamerach Axis. Kontroler drzwiowy Axis wykorzystuje klucz uwierzytelniający urządzenia peryferyjnego do przyznawania dostępu oraz uwierzytelniania czytnika AXIS Barcode Reader i aplikacji AXIS License Plate Verifier. Kompletny proces konfigurowania aplikacji AXIS License Plate Verifier w ramach programu AXIS Camera Station Pro opisano w sekcji .

### Instalowanie aplikacji AXIS Barcode Reader

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

### Konfigurowanie aplikacji AXIS Barcode Reader

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

### Tworzenie połączenia z kontrolerem drzwi

1. W programie AXIS Camera Station Pro Secure Entry:
  - 1.1. Przejdź do **Configuration > Access control > Encrypted communication** (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana).

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

## Formaty kart i kod PIN

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

Wybierz kolejno opcje Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN). Strona zawiera dwie zakładki:

**Konfiguracja kodu PIN** – Ustawienie długości kodu PIN oraz znaku kończącego kod PIN.

**Formaty kart** – Wyświetlanie, tworzenie, edytowanie, usuwanie i aktywowanie formatów kart.

### Formaty kart

W tabeli wymieniono wszystkie dostępne formaty kart wraz z następującymi informacjami:

|                     |                                                                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| W użyciu            | Czy format jest aktywny. W danym momencie na daną liczbę bitów aktywny może być tylko jeden format.                                                 |
| Nazwa formatu karty | Nazwa formatu karty.                                                                                                                                |
| Liczba bitów        | Liczba bitów formatu karty.                                                                                                                         |
| Pochodzenie         | Bez względu na to czy format jest domyślnym formatem systemu (System default) czy formatem niestandardowym (Custom), który samodzielnie utworzyłeś. |

### Dodawanie formatu karty

1. Wybierz kolejno opcje Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN).
2. Kliknij  Add (Dodaj).
3. Wprowadź nazwę oraz długość w bitach z zakresu od 1 do 256.
4. Zaznacz opcję Invert bit order (Odwróć kolejność bitów), jeżeli chcesz odwracać kolejność bitów w danych odbieranych z czytnika kart.
5. 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.
6. Włącz opcję Card number (Numer karty), Facility code (Kod obiektu) lub obie te opcje. Przynajmniej jedna z nich musi być aktywna w danym formacie kart.

7. Ustaw zakres bitów danych dla pola danych. Musi się mieścić w przedziale określonym dla liczby bitów.
8. Wybierz format wyjściowy danych dla pola danych.
  - Dziesiętny: System liczbowy o podstawie 10. Wykorzystuje cyfry od 0 do 9.
  - Hexadecimal (Szesnastkowy): System liczbowy o podstawie 16. Wykorzystuje 16 symboli: cyfry od 0 do 9 i litery od a do f.
9. Wybierz kolejność bitów.
  - Little-endian: Pierwszy bit jest najmniejszy lub najmniej znaczący.
  - Big-endian: Pierwszy bit jest największy lub najbardziej znaczący.
10. Kliknij **OK**.

#### **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.
- Można edytować predefiniowane formaty kart, ale nie można ich usuwać. Aby cofnąć wszelkie zmiany wprowadzone w predefiniowanym formacie, wybierz ikonę resetowania celem przywrócenia jego ustawień domyślnych. Możesz usunąć utworzone przez siebie formaty kart.



*Konfigurowanie formatów kart*

#### **Edycja formatu karty**

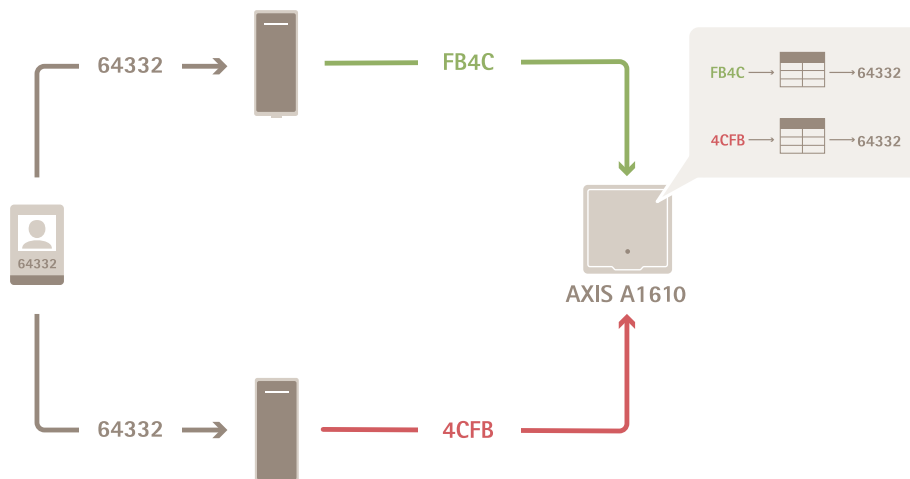
1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Wybierz format karty i kliknij .
3. W przypadku edytowania wstępnie zdefiniowanego formatu karty można edytować tylko opcje **Invert bit order (Odwracanie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

Usuwać można tylko niestandardowe formaty kart. Aby usunąć niestandardowy format karty:

1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. Zaznacz niestandardowy format karty, a następnie kliknij  i **Yes (Tak)**.

#### **Ustawienia formatu karty**

#### **Informacje ogólne**



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

### Odwróć kolejność bitów

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

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

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

### Odwróć kolejność bajtów

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

64 332 = 1111 1011 0100 1100  $\longrightarrow$  0100 1100 1111 1011 = 19707

F B 4 C                      4 C F B

### 26-bitowy standardowy format karty Wiegand

P FFFFFF NNNNNNNNNNNNNNNN P

①      ②                      ③                      ④

- 1 Parzystość wiodąca
- 2 Kod obiektu

- 3 Numer karty
- 4 Parzystość końcowa

## Kod PIN

Ustaw minimalną i maksymalną długość kodu PIN. Jeśli ustawiasz różne wartości długości minimalnej i maksymalnej, określ znak kończący kod PIN, który będzie sygnalizował zakończenie wprowadzania kodu PIN.

- Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN > PIN configuration** (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN > Konfiguracja kodu PIN).
- Wprowadź **Minimalną długość kodu PIN** i **Maksymalną długość kodu PIN**.
- W razie potrzeby wprowadź **Znak kończący kod PIN**.
- Kliknij **OK**.

## Szyfrowana komunikacja

### Bezpieczny kanał OSDP

AXIS Camera Station Secure Entry obsługuje bezpieczny kanał OSDP (Open Supervised Device Protocol), który umożliwia szyfrowanie komunikacji pomiędzy kontrolerem i czytnikami Axis.

Włączanie bezpiecznego kanału OSDP dla całego systemu:

- Przejdź do **Configuration > Access control > Encrypted communication** (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana).
- Podaj główny klucz szyfrowania i kliknij **OK**.
- Włącz **OSDP Secure Channel (Bezpieczny kanał OSDP)**. Opcja ta jest dostępna tylko po wprowadzeniu głównego klucza szyfrowania.
- Domyślnie główny klucz szyfrowania generuje klucz bezpiecznego kanału OSDP. Aby ręcznie ustawić klucz bezpiecznego kanału OSDP:
  - W obszarze **OSDP Secure Channel (Bezpieczny kanał OSDP)** kliknij .
  - Wyczyść opcję **Use main encryption key to generate OSDP Secure Channel key** (Użyj głównego klucza szyfrowania, aby wygenerować klucz bezpiecznego kanału OSDP).
  - 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.
- Wymagane jest oprogramowanie AXIS Camera Station w wersji 5.47 lub nowszej.
- Serwer główny i podrzędne muszą się znajdować w tej samej sieci.
- Na serwerze głównym i podrzędnych konieczne w Zaporze systemu Windows włączyć zezwalanie na przychodzące połączenia TCP na porcie bezpiecznego wchodzenia. Domyślny port to 55767. Aby dowiedzieć się więcej o dostosowywaniu konfiguracji portów, p. sekcja *Ogólne ustawienia serwera*.
- Dołączenie serwera podrzędnego do serwera głównego powoduje zastąpienie klucza czytnika, a w konsekwencji utratę ważności wszelkich danych uwierzytelniających Bluetooth. Aby do tego nie doszło, utwórz dane uwierzytelniające Bluetooth na serwerze głównym zamiast na serwerze podrzędnym.

## Proces

1. Skonfiguruj serwer jako podrzędny i wygeneruj plik konfiguracyjny. Zob. *Generowanie pliku konfiguracyjnego z serwera podrzędnego, on page 29*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. Zob. *Importowanie pliku konfiguracyjnego do serwera głównego, on page 29*.
3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. Zob. *Dodawanie posiadacza karty, on page 31* i *Dodawanie grupy, on page 35*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Zob. *Zarządzanie dostępem, on page 31*.

## Generowanie pliku konfiguracyjnego z serwera podrzędnego

1. Na serwerze podrzędnym wybierz kolejno opcje **Configuration > Access control > Multi server** (Konfiguracja > Kontrola dostępu > Multiserwer).
2. Kliknij opcję **Sub server** (Serwer podrzędny).
3. Kliknij przycisk **Generate** (Generuj). Generuje plik konfiguracyjny w formacie .json.
4. Kliknij przycisk **Download** (Pobierz) i wybierz lokalizację, w której ma zostać zapisany plik.

## Importowanie pliku konfiguracyjnego do serwera głównego

1. Na serwerze głównym wybierz kolejno opcje **Configuration > Access control > Multi server** (Konfiguracja > Kontrola dostępu > Multiserwer).
2. Kliknij opcję **Main server** (Główny serwer).
3. Kliknij przycisk **+ Add** (Dodaj) i przejdź do pliku konfiguracyjnego wygenerowanego na serwerze podrzędnym.
4. Wprowadź nazwę, adres IP i numer portu serwera podrzędnego.
5. Kliknij przycisk **Import** (Importuj), aby dodać serwer podrzędny.
6. Stan serwera podrzędnego będzie widoczny jako **Connected** (Połączony).

## Unieważnianie serwera podrzędnego

Serwer podrzędny można unieważnić tylko zanim jego plik konfiguracyjny zostanie zaimportowany do serwera głównego.

1. Na serwerze głównym wybierz kolejno opcje **Configuration > Access control > Multi server** (Konfiguracja > Kontrola dostępu > Multiserwer).
2. Zaznacz opcję **Serwer podrzędny** i kliknij przycisk **Unieważnij serwer**. Teraz można skonfigurować ten serwer jako główny lub podrzędny.

## Usuwanie serwera podrzędnego

Po zaimportowaniu pliku konfiguracyjnego serwera podrzędnego ów serwer zostanie połączony z serwerem głównym.

Aby usunąć serwer podrzędny:

1. Na serwerze głównym:
  - 1.1. Wybierz kolejno opcje **Access management > Dashboard** (Zarządzanie dostępem > Pulpit nawigacyjny).
  - 1.2. Zmień globalnych posiadaczy kart i grupy na lokalnych posiadaczy kart i grupy.
  - 1.3. Przejdź do menu **Configuration > Access control > Multi server** (Konfiguracja > Kontrola dostępu > Multiserwer).

- 1.4. Kliknij **Main server (Główny serwer)** w celu wyświetlenia listy serwerów podrzędnych.
- 1.5. Zaznacz serwer podrzędny i kliknij przycisk **Delete (Usuń)**.
2. Na serwerze podrzędnym:
  - Przejdź do menu **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
  - Kliknij polecenie **Sub server (Serwer podrzędny)** i kliknij przycisk **Revoke server (Unieważnij serwer)**.

## **Ustawienia usługi Active directory<sup>BETA</sup>**

### **Uwaga**

Konta użytkowników w systemie Microsoft Windows oraz użytkownicy i grupy Active Directory mogą uzyskać dostęp do AXIS Camera Station Pro Secure Entry. Sposób dodawania użytkowników w systemie Windows różni się w zależności od wersji. Więcej informacji, p. strona [support.microsoft.com](http://support.microsoft.com). Jeżeli korzystasz z sieci domeny Active Directory, skonsultuj się z administratorem sieci.

Gdy po raz pierwszy otworzysz ustawienia usługi Active Directory, będziesz mieć możliwość zaimportowania użytkowników Microsoft Active Directory do obszaru posiadaczy kart w AXIS Camera Station Pro Secure Entry. Zob. *Importowanie użytkowników usługi Active Directory, on page 30*.

Po wstępnej konfiguracji na stronie ustawień usługi Active Directory pojawią się następujące opcje.

- Tworzenie i zarządzanie grupami posiadaczy kart w oparciu o grupy w Active Directory.
- Skonfiguruj zaplanowaną synchronizację między Active Directory a systemem zarządzania dostępem.
- Zsynchronizuj manualnie, aby zaktualizować dane wszystkich posiadaczy kart zaimportowanych z usługi Active Directory.
- Zarządzaj mapowaniem danych między danymi użytkownika z Active Directory a właściwościami posiadacza karty.

## **Importowanie użytkowników usługi Active Directory**

Aby zaimportować użytkowników usługi Active Directory do obszaru posiadaczy kart w AXIS Camera Station Pro Secure Entry:

1. W obszarze **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Active directory settings (Ustawienia usługi Active Directory)<sup>BETA</sup>**.
2. Kliknij **Set up import (Konfiguruj importowanie)**.
3. Postępuj zgodnie z instrukcjami na ekranie, aby wykonać następujące trzy główne kroki:
  - 3.1. Wybierz użytkownika z usługi Active Directory, który posłuży za szablon mapowania danych.
  - 3.2. Mapuj dane użytkowników z bazy danych usługi Active Directory do właściwości posiadaczy kart.
  - 3.3. Utwórz nową grupę posiadaczy kart w systemie zarządzania dostępem i wybierz grupy Active Directory do zaimportowania.

Nie można zmienić żadnych zaimportowanych danych użytkownika, ale można dodać poświadczenia do zaimportowanego posiadacza karty – zob. *Dodaj poświadczenia, on page 33*.

### **Ważne**

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

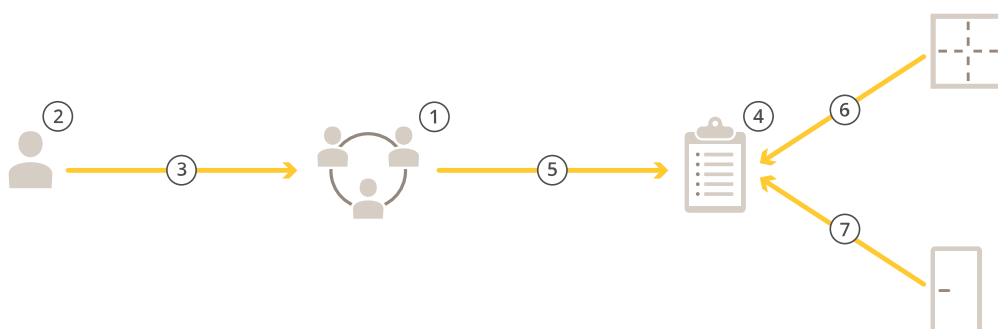
## Zarządzanie dostępem

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

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

### Proces zarządzania dostępem

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



1. *Dodawanie grupy, on page 35.*
2. *Dodawanie posiadacza karty, on page 31.*
3. Dodaj posiadaczy kart do grup.
4. *Dodaj regułę dostępu, on page 36.*
5. Przypisz grupy do reguł dostępu.
6. Przypisz strefy do reguł dostępu.
7. Przypisz drzwi do reguł dostępu.

### Dodawanie posiadacza karty

Posiadacz karty to osoba posiadająca unikatowy identyfikator zarejestrowany w systemie. Skonfiguruj użytkownika karty, podając dane uwierzytelniające pozwalające zidentyfikować daną osobę oraz określając, kiedy i w jaki sposób może ona uzyskać dostęp do drzwi.

Można również mapować użytkowników w bazie danych usługi Active Directory jako posiadaczy kart. Zob. *Ustawienia usługi Active directory<sup>BETA</sup>, on page 30.*

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

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

**Uwaga**

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

5. Kliknij **Advanced (Zaawansowane)**, aby skonfigurować dodatkowe opcje.
6. Dodaj poświadczenie do posiadacza karty. Zob. *Dodaj poświadczenia*, on page 33.
7. Kliknij przycisk **Save (Zapisz)**.
8. Aby wydrukować identyfikatory, wybierz jednego lub więcej posiadaczy kart i kliknij **Print Badge<sup>BETA</sup>** (Drukuj identyfikator). Więcej informacji, p. sekcja *Drukowanie identyfikatorów<sup>BETA</sup>*, on page 42.

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

| Zaawansowane                                                  |                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Długi czas dostępu                                            | Wybierz tę opcję, aby w sytuacji gdy jest zainstalowany monitor drzwi, posiadacz karty otrzymał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi.                                                                                                                                                                                     |
| Zawieś posiadacza karty                                       | Wybierz, aby zawiesić posiadacza karty. Powoduje to tymczasowe zablokowanie dostępu dla posiadacza karty.                                                                                                                                                                                                                                            |
| Zezwól na podwójne przeciągnięcie                             | Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Posiadacz karty może tego na przykład użyć do odblokowania drzwi poza regularnym harmonogramem.                                                                                                                                                                       |
| Zwolnienie z blokady ogólnej                                  | Zaznacz tę opcję, aby zapewnić posiadaczowi karty dostęp w okresie odcięcia obszaru.                                                                                                                                                                                                                                                                 |
| Exempt from anti-passback (Zwolnienie z reguły anti-passback) | Wybierz tę opcję, aby przyznać zwolnić posiadacza karty z reguły anti-passback. Reguła Anti-passback uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Zanim takie poświadczenia będą mogły zostać użyte ponownie, posiadacz kart z tymi danymi musi najpierw opuścić obszar. |
| Globalny posiadacz karty                                      | Zaznacz tę opcję, aby możliwe było wyświetlanie i monitorowanie posiadacza karty na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Zob. <i>Multiserwer<sup>BETA</sup></i> , on page 28.                                                                                                    |



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

*Dodawanie posiadaczy kart i grup*

## Dodaj poświadczenia

Do posiadacza karty można dodać następujące typy poświadczeń:

- Poświadczenie w postaci kodu QR, on page 33
- Poświadczenie przez PIN, on page 33
- Poświadczenie kartą, on page 34
- Uwierzytelnienie tablicy rejestracyjnej, on page 34

| Data wygaśnięcia |                                                                      |
|------------------|----------------------------------------------------------------------|
| Ważne od         | Ustaw datę i godzinę, od kiedy uwierzytelnienie zacznie obowiązywać. |
| Ważne do         | Wybierz opcję z menu rozwijanego.                                    |

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

## Poświadczenie w postaci kodu QR

### Uwaga

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

Aby dodać do posiadacza karty poświadczenie w postaci kodu QR:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij  **Add (Dodaj)** i wybierz **QR-code** (Kod QR).
2. Wprowadź nazwę poświadczenia.
3. Domyślnie jest włączona opcja **Dynamic QR** (Dynamiczny kod QR). Musisz użyć jej z uwierzytelnieniem PIN.
4. Ustaw datę początkową i końcową poświadczenia.
5. Aby kod QR był wysyłany przez e-mail automatycznie po zapisaniu posiadacza karty, zaznacz opcję **Send QR code to cardholder when credential is saved** (Po zapisaniu poświadczenia wyślij kod QR do posiadacza karty).
6. Kliknij **Dodaj**.

## Poświadczenie przez PIN

Aby dodać do posiadacza karty poświadczenie w postaci numeru PIN:

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

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

### Poświadczenia mobilne

#### Uwaga

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

### Poświadczenie kartą

Aby dodać do posiadacza karty poświadczenie w postaci karty:

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

#### Uwaga

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

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

#### Uwaga

Do sczytania danych karty można użyć biurkowego czytnika kart USB marki 2N. Więcej informacji znajdziesz w temacie *Konfigurowanie biurkowego czytnika kart USB firmy 2N*.

4. Wprowadź kod obiektu. To pole jest dostępne tylko po włączeniu ustawienia **Facility code** (Kod obiektu) w obszarze **Access management > Settings** (Zarządzanie dostępem > Ustawienia).
5. Ustaw datę początkową i końcową poświadczenia.
6. Kliknij **Dodaj**.

### Uwierzytelnienie tablicy rejestracyjnej

Aby dodać do posiadacza karty poświadczenie w postaci tablicy rejestracyjnej:

1. W obszarze **Credentials** (Uwierzytelnienia) kliknij **+ Add** (Dodaj) i wybierz **License plate** (Tablica rejestracyjna).
2. Wprowadź nazwę poświadczenia opisującą dany pojazd.
3. Wprowadź numer tablic rejestracyjnych dla pojazdu.
4. Ustaw datę początkową i końcową poświadczenia.
5. Kliknij **Dodaj**.

### Używanie numeru rejestracyjnego jako poświadczenia

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

1. Dodaj kontroler drzwi i kamerę do AXIS Camera Station Pro Secure Entry. Patrz *Dodawanie urządzeń*.
2. Uaktualnij oprogramowanie sprzętowe na nowych urządzeniach do najnowszej dostępnej wersji. Patrz *Aktualizowanie oprogramowania sprzętowego*.
3. Dodaj nowe drzwi połączone z kontrolerem drzwi. Zob. *Dodaj drzwi, on page 8*.

- 3.1. Dodaj czytnik w obszarze **Side A (Strona A)**. Zob. *Dodawanie czytnika, on page 17*.
- 3.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
- 3.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
- 3.4. Kliknij przycisk **Ok**.
4. Zainstaluj i włącz w kamerze aplikację **AXIS License Plate Verifier**. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
5. Włącz aplikację **AXIS License Plate Verifier**.
6. Skonfiguruj aplikację **AXIS License Plate Verifier**.
  - 6.1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.
  - 6.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuje klucz)**.
  - 6.3. Otwórz aplikację **AXIS License Plate Verifier** z poziomu interfejsu **WWW** kamery.
  - 6.4. Pomiń kreatora konfiguracji.
  - 6.5. Przejdź do opcji **Settings (Ustawienia)**.
  - 6.6. W obszarze **Access control (Kontrola dostępu)** wybierz **Secure Entry (Bezpieczne wejście)** jako **Type (Typ)**.
  - 6.7. W obszarze **IP address (Adres IP)** wpisz adres IP kontrolera drzwi.
  - 6.8. W obszarze **Authentication key (Klucz uwierzytelniania)** wklej skopiowany wcześniej klucz uwierzytelniania.
  - 6.9. Kliknij przycisk **Połącz**.
  - 6.10. W obszarze **Door controller name (Nazwa kontrolera drzwi)** wybierz kontroler drzwi.
  - 6.11. W obszarze **Reader name (Nazwa czytnika)** wybierz czytnik dodany wcześniej.
  - 6.12. Włącz integrację.
7. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Zob. *Dodawanie posiadacza karty, on page 31*
8. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Zob. *Dodaj poświadczenia, on page 33*
9. Dodaj regułę dostępu. Zob. *Dodaj regułę dostępu, on page 36*.
  - 9.1. Dodaj harmonogram.
  - 9.2. Dodaj posiadacza karty, któremu chcesz przyznać dostęp na podstawie odczytu numeru tablicy rejestracyjnej.
  - 9.3. Dodaj drzwi z czytnikiem **AXIS License Plate Verifier**.

## Dodawanie grupy

Grupy umożliwiają zbiorcze zarządzanie posiadaczami kart i ich regułami dostępu.

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do **Cardholder management > Groups (Zarządzanie posiadaczami kart > Grupy)** i kliknij  **Add (Dodaj)**.
3. Wprowadź nazwę i opcjonalnie inicjały grupy.
4. Wybierz **Global group (Grupa globalna)**, aby wyświetlić i monitorować posiadaczy kart na serwerach podległych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Zob. *Multiserwer<sup>BETA</sup>, on page 28*.

5. Dodawanie posiadaczy kart do grupy:
  - 5.1. Kliknij  **Add (Dodaj)**.
  - 5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add (Dodaj)**.
6. Kliknij przycisk **Save (Zapisz)**.
7. Aby wydrukować identyfikatory dla wszystkich posiadaczy kart w grupie, wybierz grupę i kliknij opcję **Print Badge<sup>BETA</sup>** (Drukuj identyfikator). Więcej informacji, p. sekcja *Drukowanie identyfikatorów<sup>BETA</sup>*, on page 42.

## **Dodaj regułę dostępu**

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

Reguła dostępu zawiera następujące elementy:

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

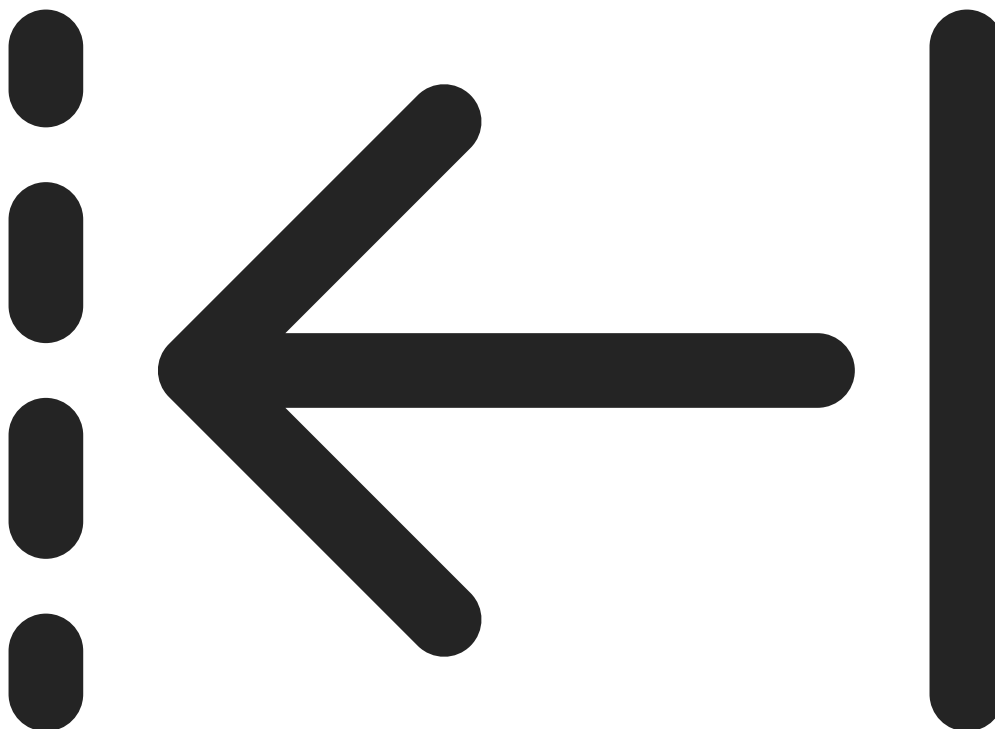
**Drzwi i strefy** – gdzie ma zostać przyznany dostęp.

**Harmonogramy** – kiedy ma zostać przyznany dostęp.

Aby dodać regułę dostępu:

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)**.

3. W obszarze Access rules (Reguły dostępu)



kliknij **+** Add (Dodaj).

4. Wprowadź nazwę reguły dostępu i kliknij **Next (Dalej)**.

5. Skonfiguruj posiadaczy kart i grupy:

5.1. W obszarze **Cardholders** (Posiadacze kart) lub **Groups** (Grupy) kliknij **+** Add (Dodaj).

5.2. Wybierz posiadaczy kart lub grupy i kliknij **Add (Dodaj)**.

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

6. Konfiguracja drzwi i stref:

6.1. W obszarze **Doors** (Drzwi) lub **Zones** (Strefy) kliknij **+** Add (Dodaj).

6.2. Wybierz drzwi lub strefy i kliknij **Add (Dodaj)**.

7. Konfiguracja harmonogramów:

7.1. W obszarze **Schedules** (Harmonogramy) kliknij **+** Add (Dodaj).

7.2. Wybierz jeden lub więcej harmonogramów i kliknij **Add (Dodaj)**.

8. Kliknij przycisk **Save (Zapisz)**.

Reguła dostępu, w której brakuje co najmniej jednego z opisanych powyżej składników, jest niekompletna. Wszystkie niekompletne reguły dostępu można obejrzeć na karcie **Incomplete (Niekompletne)**.



## Eksportowanie raportów konfiguracji systemu

Można eksportować raporty zawierające różne rodzaje informacji o systemie. AXIS Camera Station Pro Secure Entry eksportuje raporty jako plik CSV (zawierający wartości rozdzielone przecinkami) i zapisuje je w domyślnym folderze pobierania. Aby wyeksportować raport:

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

|                                      |                                                                                                                                                                 |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Raport szczegółów posiadaczy kart    | Zawiera informacje o posiadaczach kart, poświadczeniach, weryfikacjach kart i ostatnich transakcjach.                                                           |
| Dziennik dostępu posiadaczy kart     | Zawiera informacje o posiadaczu karty, grupach posiadaczy kart, regułach dostępu, drzwiach i strefach powiązanych z posiadaczami kart.                          |
| Raport dostępu grupy posiadaczy kart | Zawiera nazwę grupy posiadaczy kart oraz informacje o posiadaczach kart, regułach dostępu, drzwiach i strefach, z którymi jest powiązana grupa posiadaczy kart. |
| Raport reguły dostępu                | Zawiera nazwę reguły dostępu oraz informacje o posiadaczach kart, grupach posiadaczy kart, drzwiach i strefach, z którymi jest powiązana reguła dostępu.        |
| Raport dostępu do drzwi              | Zawiera nazwę drzwi oraz informacje o posiadaczach kart, grupach posiadaczy kart, regułach dostępu i strefach, z którymi są powiązane drzwi.                    |
| Raport dostępu do strefy             | Zawiera nazwę strefy oraz informacje o posiadaczach kart, grupach posiadaczy kart, regułach dostępu i drzwiach, z którymi jest powiązana strefa.                |

## Tworzenie raportów aktywności posiadaczy kart

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

Raport ze zbiórki zawiera listę posiadaczy kart obecnych w określonej strefie, ułatwiając ustalenie, kto jest bezpieczny, a kto zaginął w sytuacji awaryjnej. Pomaga zarządcom budynków w lokalizacji pracowników i odwiedzających po ewakuacji. Miejsce zbiórki to wyznaczony czytnik, do którego pracownicy zgłaszają się w sytuacjach awaryjnych. System generuje raport dotyczący osób przebywających na terenie obiektu i poza nim.

System oznacza posiadaczy kart jako zaginionych, dopóki nie zameldują się w punkcie zbiórki lub dopóki inna osoba nie oznaczy ich ręcznie jako bezpiecznych.

Zarówno raporty imienne, jak i raporty ze zbiórek wymagają stref do śledzenia posiadaczy kart.

Aby utworzyć i uruchomić raport imienny lub ze zbiórki:

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Reports (Raporty) > Cardholder activity (Aktywność posiadaczy kart)**.
3. Kliknij **+ Add (Dodaj)** i wybierz **Roll call / Mustering (Imienny / Zbiórka)**.
4. Wprowadź nazwę raportu.
5. Wybierz strefy do uwzględnienia w raporcie.
6. Wybierz grupy do uwzględnienia w raporcie.
7. Jeżeli chcesz otrzymać raport ze zbiórki, wybierz **Mustering point (Punkt zbiórki)** i czytnik.
8. Wybierz ramy czasowe raportu.
9. Kliknij przycisk **Save (Zapisz)**.
10. Wybierz raport i kliknij **Run (Uruchom)**.

| Stan w raporcie imiennym       | Opis                                                                                                  |
|--------------------------------|-------------------------------------------------------------------------------------------------------|
| <b>Present (Obecny)</b>        | Posiadacz karty wszedł do określonej strefy i nie opuścił jej do czasu uruchomienia raportu.          |
| <b>Not present (Nieobecny)</b> | Posiadacz karty opuścił określoną strefę i nie wszedł do niej ponownie do czasu uruchomienia raportu. |

| Stan w raporcie ze zbiórki | Opis                                                            |
|----------------------------|-----------------------------------------------------------------|
| <b>Safe (Bezpieczny)</b>   | Posiadacz karty przeciągnął swoją kartę w punkcie zbiórki.      |
| <b>Missing (Zaginiony)</b> | Posiadacz karty nie przeciągnął swojej karty w punkcie zbiórki. |

## Import i eksport

### Importuj posiadaczy kart

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

Po zaimportowaniu posiadaczy kart system zarządzania dostępem automatycznie zapisuje konfigurację systemu, w tym całą konfigurację sprzętową, i usuwa wcześniej zapisaną konfigurację.

Można również mapować użytkowników w bazie danych usługi Active Directory jako posiadaczy kart. Zob. *Ustawienia usługi Active directory<sup>BETA</sup>, on page 30.*

| Opcje importu |                                                                                                                                               |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Nowość        | Usuwa istniejące dane posiadaczy kart i dodaje nowych posiadaczy kart.                                                                        |
| Aktualizuj    | Aktualizuje dane istniejących posiadaczy kart i dodaje nowych posiadaczy kart.                                                                |
| Dodaj         | Zachowuje istniejących posiadaczy kart i dodaje nowych. Numery kart i identyfikatory posiadaczy kart są unikatowe i można ich użyć tylko raz. |

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

| Ustawienia importu          |                                                                                                                                                                                                                                                            |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pierwszy wiersz to nagłówek | Wybierz, czy plik CSV zawiera nagłówek kolumny.                                                                                                                                                                                                            |
| Ogranicznik kolumny         | Wprowadź format ogranicznika kolumn w pliku CSV.                                                                                                                                                                                                           |
| Unikalny identyfikator      | Do identyfikowania posiadacza karty system domyślnie używa <b>Cardholder ID (Identyfikatora posiadacza karty)</b> . Możesz również użyć imienia i nazwiska lub adresu e-mail. Użyj tej opcji, aby zapobiec importowaniu zduplikowanych rekordów personelu. |
| Format numeru karty         | Domyślnie włączona jest opcja <b>Allow both hexadecimal and number (Zezwalaj na liczbę szesnastkową i dziesiętną)</b> .                                                                                                                                    |

## **Eksportowanie danych posiadaczy kart**

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

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

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

## **Cofanie importu**

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

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

## **Ustawienia zarządzania dostępem**

Aby dostosować pola posiadacza karty używane na pulpicie nawigacyjnym dostępu:

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

Aby używać kodu obiektu do weryfikowania systemu kontroli dostępu:

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

### **Uwaga**

Podczas konfigurowania profili identyfikacji zaznacz również opcję **Include facility code for card validation (Dołącz kod obiektu do sprawdzania poprawności karty)**. Zob. *Profile identyfikacji, on page 22*.

Aby zmodyfikować szablon wiadomości e-mail służący do wysłania poświadczeń QR lub mobilnych:

1. Na karcie **Access management (Zarządzanie dostępem)** kliknij **Settings (Ustawienia) > Email templates (Szablony e-mail)**.
2. Zmodyfikuj szablon i kliknij **Update (Aktualizuj)**.

## **Szablony identyfikatorów <sup>BETA</sup>**

Można dostosować szablony identyfikatorów, dodając informacje o posiadaczu karty, zdjęcia, logotypy i własne oznaczenia firmowe. Aby utworzyć nowy szablon:

1. Przejdź do **Access management > Settings > Badge templates <sup>BETA</sup> (Zarządzanie dostępem > Ustawienia > Szablony identyfikatorów)**.
2. Kliknij **Create new template (Utwórz nowy szablon)**.
3. Wprowadź nazwę w polu **Template name (Nazwa szablonu)**.
4. Aby ustawić ten szablon jako domyślny, wybierz **Use as default template for printing (Użyj jako domyślny szablon do drukowania)**.
5. Dostosuj wygląd identyfikatora:
  - Wybierz maks. pięć pól tekstowych, które mają być prezentowane na przedniej stronie, w tym wszelkie utworzone pola niestandardowe. Podczas drukowania na identyfikatorze znajdują się tylko wypełnione pola.
  - Wybierz czcionkę i kolor tekstu.
  - Dodaj kolor tła lub obraz.
  - Załącz logotyp swojej organizacji.
  - Na stronie tylnej dodaj kolor tła lub obraz.
6. Kliknij **Save (Zapisz)**, aby zapisać zmiany lub **Save as (Zapisz jako)**, aby utworzyć nowy szablon.

### **Uwaga**

Utworzonego szablonu nie można edytować, można jedynie zmienić jego nazwę.

### Drukowanie identyfikatorów <sup>BETA</sup>

Można drukować identyfikatory dla posiadaczy kart, korzystając ze skonfigurowanych szablonów identyfikatorów. Kodowanie kart nie jest obecnie obsługiwane. Zanim rozpoczniesz:

- Sprawdź, czy posiadacz karty ma co najmniej jedno uwierzytelnienie za pomocą karty. Nie można drukować identyfikatorów dla posiadaczy kart bez uwierzytelnień.
- Potrzebna jest drukarka obsługująca karty o rozmiarze CR80 i odpowiednie materiały do drukowania w rodzaju grubego kartonu.
- Skonfiguruj ustawienia drukowania w przeglądarce:
  1. Ustaw rozmiar strony na CR80 lub rozmiar niestandardowy odpowiadający wymiarom karty do wydrukowania.
  2. Ustaw orientację pionową.
  3. Wyłącz marginesy lub ustaw je na minimum.

#### Ważne

Aplikacja Secure Entry współpracuje z drukarkami działającymi w oparciu o sterowniki dla systemu Windows. Drukarki serii HID Fargo zostały sprawdzone pod kątem prawidłowości działania. Jeśli potrzebujesz sterownika do drukarki, skontaktuj się z jej dostawcą.

Aby wydrukować identyfikatory:

1. Przejdź do **Access management > Cardholder management > Cardholders** (Zarządzanie dostępem > Zarządzanie posiadaczami kart > Posiadacze kart).
2. Wybierz jednego lub kilku posiadaczy kart.
3. Kliknij **Print badge** <sup>BETA</sup> (Wydrukuj identyfikator).
4. Kliknij **Select template** (Wybierz szablon) i z menu rozwijalnego **Template** (Szablon) wybierz szablon identyfikatora, którego chcesz użyć.
5. Jeżeli posiadacz karty ma kilka uwierzytelnień za pomocą karty, wybierz jedno z menu rozwijalnego **Card** (Karta).
6. Kliknij przycisk **Drukuj**.

#### Uwaga

W przypadku drukarki nieobsługującej druku dwustronnego najpierw wydrukuj wszystkie przednie strony, a następnie odwróć plik kart i włóż je ponownie do podajnika, by wydrukować tylne strony.



T10231644\_pl

2026-07 (M8.5)

© 2025 – 2026 Axis Communications AB