

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*.

Konfigurowanie kontroli dostępu

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

Kompletny proces konfigurowania sieciowego kontrolera drzwi Axis w oprogramowaniu AXIS Camera Station 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 sekcji **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
- Ustaw datę i godzinę kontrolera w oknie **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).
- Włącz obsługę protokołu HTTPS na kontrolerze w oknie **Configuration > Devices > Management** (Konfiguracja > Urządzenia > Zarządzanie).

Proces konfigurowania kontroli dostępu

1. Aby zmodyfikować predefiniowane profile identyfikacji lub utworzyć nowy profil identyfikacji, patrz *Profile identyfikacji, on page 18*.
2. Aby używać niestandardowej konfiguracji formatów kart i długości kodu PIN, patrz *Formaty kart i kod PIN, on page 20*.
3. Dodaj drzwi i zastosuj do nich profil identyfikacji. Patrz *Dodawanie drzwi, on page 5*.
4. Skonfiguruj drzwi.
 - *Dodawanie monitora drzwi, on page 11*
 - *Dodaj wejście awaryjne, on page 12*
 - *Dodawanie czytnika, on page 13*
 - *Dodawanie urządzenia REX, on page 15*
5. Dodaj strefę, a następnie drzwi do strefy. Patrz *Dodawanie strefy, on page 16*.

Zgodność oprogramowania urządzenia w przypadku kontrolerów drzwi

Ważne

W przypadku aktualizowania systemu AXIS OS w kontrolerze drzwi należy pamiętać o następujących kwestiach:

- **Obsługiwane wersje systemu AXIS OS:** Wymienione poniżej obsługiwane wersje systemu AXIS OS mają zastosowanie tylko w przypadku wykonywania aktualizacji z oryginalnej zalecanej wersji oprogramowania AXIS Camera Station Pro i gdy system zawiera drzwi. Jeśli system nie spełnia tych warunków, należy dokonać aktualizacji do wersji systemu AXIS OS zalecanej dla konkretnej wersji oprogramowania AXIS Camera Station Pro.
- **Minimalna obsługiwana wersja systemu AXIS OS:** Najstarsza wersja systemu AXIS OS zainstalowana w systemie określa minimalną obsługiwaną wersję AXIS OS — z ograniczeniem do dwóch wcześniejszych wersji. Załóżmy, że korzystasz z oprogramowania AXIS Camera Station Pro w wersji 6.5 i zaktualizujesz wszystkie urządzenia do zalecanej wersji systemu AXIS OS, czyli 12.0.86.2. Od tego momentu system AXIS OS w wersji 12.0.86.2 stanie się minimalną obsługiwaną wersją w Twoim systemie.
- **Aktualizacja przekraczająca zalecaną wersję systemu AXIS OS:** Załóżmy, że wykonasz aktualizację do wersji systemu AXIS OS przekraczającej wersję zalecaną dla danej wersji oprogramowania AXIS Camera Station Pro. Wówczas zawsze będzie można bez problemów obniżyć wersję z powrotem do zalecanej wersji systemu AXIS OS, o ile będzie się ona mieścić w limitach obsługi określonych dla danej wersji oprogramowania AXIS Camera Station Pro.
- **Przyszłe zalecenia dotyczące systemu AXIS OS:** Aby zapewnić stabilność systemu i pełną zgodność, należy zawsze przestrzegać wersji systemu AXIS OS zalecanej dla danej wersji oprogramowania AXIS Camera Station Pro.

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 6.15	12.5.68.1	12.8.55.1
Pro 6.14	12.5.68.1	12.8.55.1
Pro 6.13	12.5.68.1	12.6.102.1

W poniższej tabeli przedstawiono minimalną i zalecaną wersję systemu AXIS OS dla poszczególnych wersji programu AXIS Camera Station 5:

Wersja AXIS Camera Station	Zalecana wersja systemu AXIS OS
5.59	12.4.68.1
5.58	12.4.68.1
5.57	11.8.20.2

Drzwi i strefy

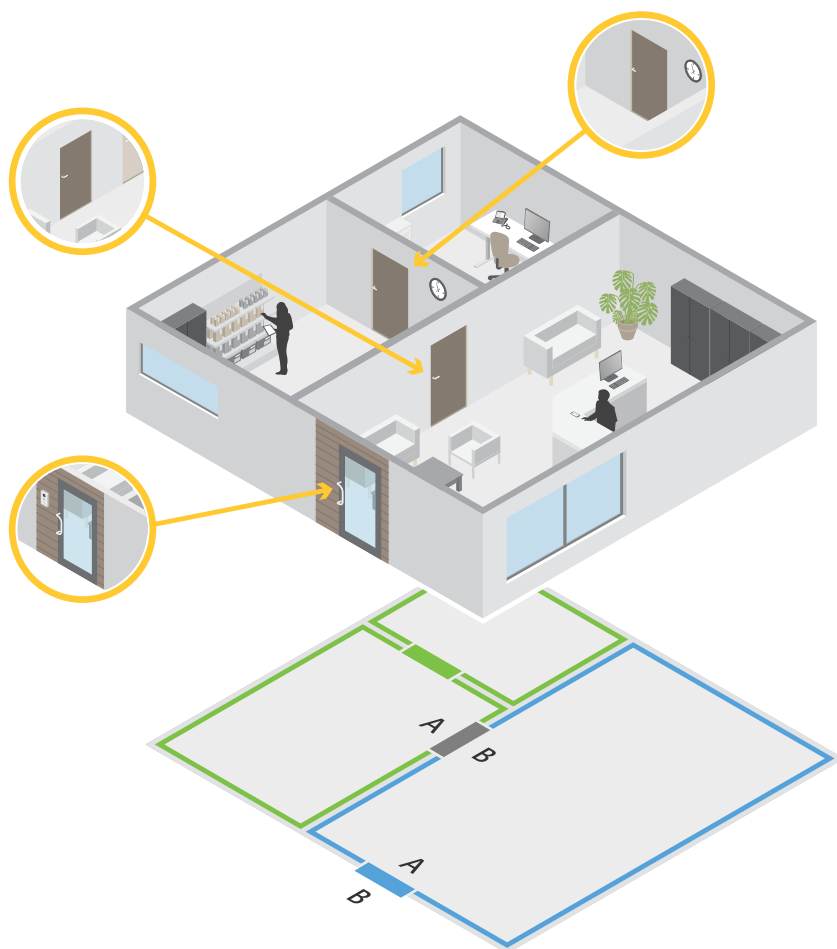
Wybierz kolejno opcje **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy), aby uzyskać przegląd oraz skonfigurować drzwi i strefy.

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

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

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

Przykład drzwi i stref



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

Dodawanie drzwi

Uwaga

- Kontroler drzwi można skonfigurować z jednymi drzwiami wyposażonymi w dwa zamki lub z dwoma drzwiami mającymi po jednym zamku.
- Jeśli kontroler drzwi nie ma drzwi i używasz nowej wersji aplikacji AXIS Camera Station Pro Secure Entry ze starszym oprogramowaniem sprzętowym w kontrolerze drzwi, system uniemożliwi dodanie drzwi. System zezwala jednak na tworzenie nowych drzwi na kontrolerach systemu ze starszym oprogramowaniem sprzętowym, jeśli są już istniejące drzwi.

Aby dodać drzwi poprzez utworzenie nowej konfiguracji drzwi:

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

Typy drzwi	
Drzwi	Zwykłe drzwi z monitorem drzwi obsługującym rygle i czytniki. Wymaga kontrolera drzwiowego.
Drzwi bezprzewodowe	Drzwi, które można skonfigurować za pomocą bezprzewodowych rygli i koncentratorów komunikacyjnych ASSA ABLOY Aperio®. Więcej informacji znajduje się w sekcji <i>Dodaj zamek bezprzewodowy, on page 10</i> .
Drzwi dozorujące	Drzwi, które mogą zgłaszać, czy są otwarte, czy zamknięte. Więcej informacji znajduje się w sekcji <i>Dodawanie drzwi dozorujących, on page 12</i> .
Drzwi zastępcze	Drzwi, które można dodać do systemu jako symbol zastępczy bez konieczności dobierania do nich osprzętu.
Piętro	Rodzaj drzwi do sterowania windą uwierzytelniający dostęp do pięter z windy za pomocą czytników kart. Więcej informacji znajduje się w sekcji .

3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami. Kontroler jest wyszarzony, gdy nie można dodać kolejnych drzwi, gdy jest offline lub serwer HTTPS nie jest aktywny.
4. Kliknij przycisk **Next (Dalej)**, aby przejść do strony konfiguracyjnej drzwi.
5. W rozwijalnym menu **Primary lock (Zamek główny)** wybierz port przekaźnika.
6. Aby skonfigurować dwa zamki w drzwiach, wybierz port przekaźnika z rozwijalnego menu **Secondary lock (Drugi zamek)**.
7. Wybierz profil identyfikacji. Patrz *Profile identyfikacji, on page 18*.
8. Skonfiguruj ustawienia drzwi. Zobacz *Ustawienia drzwi, on page 7*.
9. *Dodawanie monitora drzwi, on page 11*
10. *Dodaj wejście awaryjne, on page 12*
11. *Dodawanie czytnika, on page 13*
12. *Dodawanie urządzenia REX, on page 15*
13. Skonfiguruj poziom zabezpieczeń. Patrz *Poziom zabezpieczeń drzwi, on page 8*.
14. Kliknij przycisk **Zapisz**.

Aby dodać drzwi poprzez skopiowanie istniejącej konfiguracji drzwi:

1. Przejdź do **Configuration > Access control > Doors and zones** (Konfiguracja > Kontrola dostępu > Drzwi i strefy).
2. Kliknij **+** **Add door** (Dodaj drzwi).
3. Wpisz nazwę drzwi i wybierz kontroler drzwiowy z menu rozwijalnego **Device** (Urządzenie) celem powiązania go z drzwiami.
4. Kliknij **Next (Dalej)**.

5. Z rozwijalnego menu **Copy configuration (Kopiuje konfigurację)** wybierz istniejącą konfigurację drzwi. Pokazuje podłączone drzwi, a kontroler jest wyszarczony, jeśli został skonfigurowany z dwoma drzwiami lub jednym z dwoma zamkami.
6. W razie potrzeby zmień ustawienia.
7. Kliknij przycisk **Zapisz**.

Aby zmodyfikować drzwi:

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

Aby usunąć drzwi:

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



Dodawanie i konfigurowanie drzwi i stref

Ustawienia drzwi

1. Wybierz kolejno opcje **Configuration > Access control > Door and Zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**.
2. Wybierz drzwi, które chcesz edytować.
3. Kliknij  **Edit (Edytuj)**.

Czas dostępu (s)	Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Drzwi pozostają odblokowane do momentu ich otwarcia lub przez określony czas. Drzwi blokują się po zamknięciu, nawet jeśli nie upłynął limit czasu dostępu.
Open-too-long time (sec) (Przekroczony czas otwarcia drzwi (s))	Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączony alarm zbyt długiego otwarcia drzwi. Ustaw regułę akcji, aby skonfigurować akcję, którą powinno wyzwolić zdarzenie zbyt długiego otwarcia drzwi.
Długi czas dostępu (s)	Podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Po włączeniu tego ustawienia

	zastępuje ono czas dostępu obecnie ustawiony dla posiadaczy kart.
Long open-too-long time (sec) (Długi czas przekroczenia otwarcia drzwi (s))	Prawidłowy tylko w przypadku, gdy monitor drzwi jest skonfigurowany. Określ czas otwarcia drzwi w sekundach. Jeśli drzwi są otwarte po upływie ustawionego czasu, zostaje włączone zdarzenie zbyt długiego otwarcia drzwi. Długi czas przekroczenia otwarcia drzwi zastępuje już ustawiony czas otwarcia dla posiadaczy kart, jeśli włączona jest opcja Long access time (Długi czas dostępu) .
Czas opóźnienia do ponownego zablokowania (ms)	Ustaw czas w milisekundach, przez jaki drzwi pozostają odblokowane po ich otwarciu lub zamknięciu.
Ponowne zablokowanie	• After opening: (Po otwarciu) Dotyczy tylko scenariuszy z dodanym monitorem drzwi. • After closing: (Po zamknięciu) Dotyczy tylko scenariuszy z dodanym monitorem drzwi.
Drzwi wyważone	Wybierz, czy system ma wyzwać alarm w przypadku wyważenia drzwi.
Przekroczony czas otwarcia drzwi	Wybierz, czy system ma wyzwać alarm w przypadku, gdy drzwi pozostają zbyt długo otwarte.

Poziom zabezpieczeń drzwi

Do drzwi można dodać następujące zabezpieczenia:

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

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

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

Aby dodać regułę dwóch osób do istniejących drzwi:

1. 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.

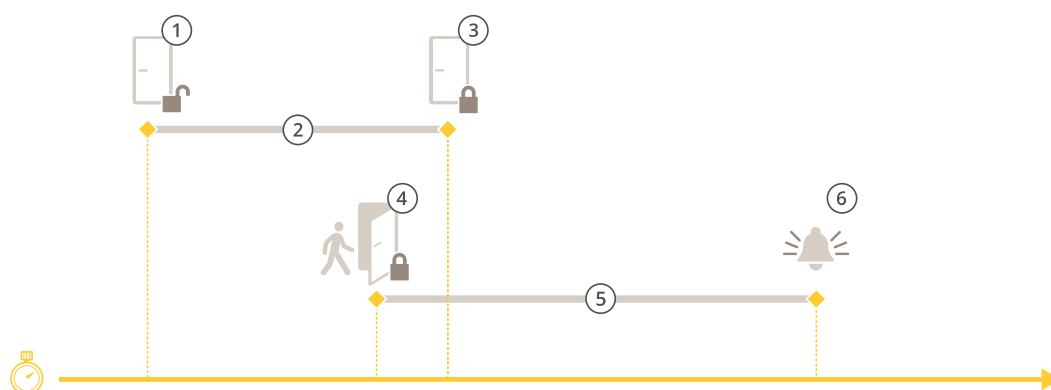
Harmonogramy	Wybierz, kiedy reguła jest aktywna.
Limit czasu (w sekundach)	Limit czasu to maksymalny dozwolony czas między przeciągnięciami kart lub innego rodzaju prawidłowymi poświadczeniami dostępu.

Aby dodać przeciągnięcie dwóch kart do istniejących drzwi:

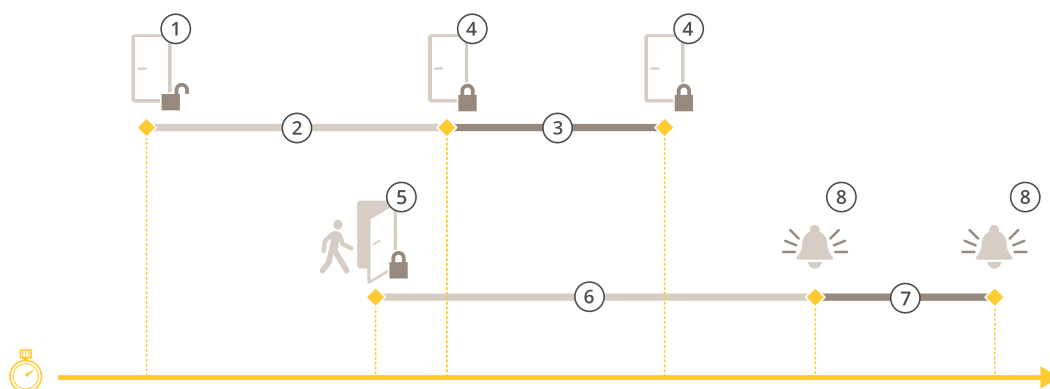
1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
2. Wybierz drzwi, dla których chcesz skonfigurować poziom zabezpieczeń.
3. Kliknij **Edit (Edycja)**.
4. Kliknij **Security level (Poziom zabezpieczeń)**.
5. Włącz **Double-swipe (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 poświadczeniami dostępu.

Opcje czasu



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



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

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 drzwi 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.
 - 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. Kliknij  **Add door (Dodaj drzwi)**.
 - 4.3. Wybierz kontroler drzwi podłączony do koncentratora komunikacyjnego **Aperio**, wybierz **Wireless door (Drzwi bezprzewodowe)** jako **Door type (Typ drzwi)**.
 - 4.4. Kliknij **Next (Dalej)**.
 - 4.5. Wybierz **Wireless lock (Zamek bezprzewodowy)**.
 - 4.6. Określ strony A i B drzwi i dodaj czujniki. Więcej informacji znajduje się w rozdziale *Drzwi i strefy, on page 4*.
 - 4.7. Kliknij przycisk **Zapisz**.

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

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

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

Dodawanie monitora drzwi

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

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 5*.
2. W obszarze **Sensors (Czujniki)** kliknij **Add (Dodaj)**.
3. Wybierz opcję **Door monitor sensor (Czujnik monitora drzwi)**.
4. Zaznacz port we/wy, do którego chcesz podłączyć monitor drzwi.

5. W obszarze **Door open if (Otwórz drzwi, jeśli)**, wybierz sposób podłączenia obwodów monitora drzwi.
6. Aby zmiany stanu cyfrowego wejścia były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu **Debounce time (Czas odbicia)**.
7. Aby przerwanie połączenia między kontrolerem drzwi i monitorem drzwi powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Patrz *Nadzorowane wejścia, on page 17*.

Drzwi otwarte, jeśli	
Obwód jest otwarty	Obwód monitora drzwi jest rozwierny (NC). Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty.
Obwód jest zamknięty	Obwód monitora drzwi jest zwierny (NO). Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty.

Dodawanie drzwi dozorujących

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

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

Uwaga

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

Aby skonfigurować drzwi dozorujące:

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

Dodaj wejście awaryjne

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

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

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

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

Dodawanie czytnika

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

Jeżeli do czytnika zastosujesz niestandardową konfigurację formatów kart lub długości numerów PIN, będzie to wyraźnie zaznaczone w kolumnie **Card formats (Formaty kart)** w oknie **Configuration > Access control > Doors and zones (Konfiguracja > Kontrola dostępu > Drzwi i strefy)**. Patrz *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 14.
 - Jeśli jako czytnik IP używany jest interkom sieciowy Axis, system używa konfiguracji kodu PIN ustawionej na stronie internetowej urządzenia.
1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi*, on page 5.
 2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
 3. Wybierz **Card reader (Czytnik kart)**.
 4. Wybierz **Reader type (Typ czytnika)**.
 5. Aby użyć niestandardowej konfiguracji długości kodu PIN tego czytnika.
 - 5.1. Kliknij przycisk **Advanced (Zaawansowane)**.
 - 5.2. Włącz opcję **Custom PIN length (Niestandardowa długość kodu PIN)**.
 - 5.3. Wypełnij pola **Min PIN length (Min. długość kodu PIN)**, **Max PIN length (Maks. długość kodu PIN)** i **End of PIN character (Koniec znaku kodu PIN)**.
 6. Aby użyć niestandardowego formatu karty tego czytnika.
 - 6.1. Kliknij przycisk **Advanced (Zaawansowane)**.

- 6.2. Włącz opcję **Custom card formats (Niestandardowe formaty kart)**.
- 6.3. Wybierz formaty karty na takie, których chcesz używać w czytniku. Jeżeli format karty o tej samej liczbie bitów jest już używany, należy go najpierw zdezaktywować. Gdy konfiguracja formatu karty różni się od skonfigurowanej konfiguracji systemu, w aplikacji klienckiej wyświetlana jest Ikona ostrzeżenia.
7. Kliknij **Dodaj**.
8. Aby dodać czytnik po drugiej stronie drzwi, wykonaj tę procedurę ponownie.

Aby dowiedzieć się, jak ustawić aplikację AXIS Barcode Reader, patrz *Konfigurowanie aplikacji AXIS Barcode Reader*.

Typ czytnika	
OSDP RS485 half duplex	Dla czytników RS485 należy wybrać OSDP RS485 half duplex i port czytnika.
Wiegand	W przypadku czytników używających protokołów Wiegand zaznacz opcję Wiegand oraz w sekcji Ogólne wybierz port dla czytnika.
Czytnik IP	W przypadku czytników sieciowych zaznacz opcję IP reader (Czytnik IP) i wybierz urządzenie z menu rozwijanego. Wymagania i obsługiwane urządzenia są opisane w temacie <i>Czytnik IP, on page 15</i> .

Wiegand	
Sterowanie LED	Wybierz opcję Single wire (Pojedynczy przewód) lub Dual wire (R/G) (Podwójny przewód (R/G)) . Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED.
Powiadomienie o sabotażu	Określ, kiedy wejście wykrywania sabotażu w czytniku ma być aktywne. • Open circuit (Obwód otwarty): Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie otwarty. • Closed circuit (Obwód zamknięty): Czytnik wysyła sygnał próby sabotażu, kiedy obwód zostanie zamknięty.
Tamper debounce time (Czas odbicia zabezpieczenia sabotażowego)	Aby zmiany stanu wejścia wykrywania sabotażu w czytniku były ignorowane, zanim wejdzie ono w nowy stabilny stan, określ wartość w polu Tamper debounce time (Czas odbicia zabezp. przeciwsab.) .
Nadzorowane wejście	Włącz, aby wyzwolić zdarzenie, gdy występuje przerwa w połączeniu między kontrolerem drzwi i czytnikiem. Patrz <i>Nadzorowane wejścia, on page 17</i> .

Dodawanie czytnika Bluetooth

Czytnik AXIS A4612 Network Bluetooth Reader można zastosować do rozszerzenia limitów okablowanych drzwi w kontrolerach drzwiowych Axis, które umożliwiają przydzielenie maks. 16 takich czytników do odnośnych drzwi. Każdy czytnik może zarządzać rygłem drzwiowym, przyciskiem wyjścia (REX) i przełącznikiem pozycji drzwi (DPS).

Dodanie i stosowanie tych czytników nie wymaga dodatkowych licencji.

Aby dodać czytnik AXIS A4612 Network Bluetooth Reader do drzwi:

1. Sprawdź, czy czytnik AXIS A4612 został sparowany z kontrolerem drzwiowym. P. sekcja *Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth, on page 32.*
2. Przejdź do strony konfiguracyjnej drzwi. P. sekcja *Dodawanie drzwi, on page 5.*
3. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**, a następnie **Card reader (Czytnik kart)**.
4. Zaznacz **IP reader (Czytnik IP)** i wybierz sparowany czytnik AXIS A4612 z rozwijalnego menu. Jeżeli czytnik ten będzie stosowany do parowania poświadczeń, zaznacz go na potrzeby parowania. Kliknij **Dodaj**.
5. Na karcie **Overview (Przegląd)** zmień profil identyfikacji. Można użyć profili **Tap in app (Dotknij w aplikacji)** lub **Touch reader (Czytnik dotykowy)**, jeżeli czytnik AXIS A4612 jest dołączony po jednej stronie drzwi, a po drugiej stosowany jest przycisk wyjścia REX.

Czytnik IP

Interkomy sieciowe Axis mogą pełnić rolę czytników IP w aplikacji AXIS Camera Station Secure Entry.

Uwaga

- Potrzebna jest do tego aplikacja AXIS Camera Station w wersji 5.38 lub nowszej oraz kontroler drzwi Axis z oprogramowaniem sprzętowym w wersji 10.6.0.2 lub nowszej.
- Interkom nie wymaga żadnej specjalnej konfiguracji, aby mógł pełnić rolę czytnika IP.

Obsługiwane urządzenia:

- Wideodomofon sieciowy AXIS A8207-VE Network Video Door Station z oprogramowaniem sprzętowym w wersji 10.5.1 lub nowszej
- Wideodomofon sieciowy AXIS A8207-VE Mk II Network Video Door Station z oprogramowaniem sprzętowym w wersji 10.5.1 lub nowszej
- AXIS I8116-E Network Video Intercom

Dodawanie urządzenia REX

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

1. Przejdź do strony konfiguracyjnej drzwi. Patrz *Dodawanie drzwi, on page 5.*
2. Pod jedną stroną drzwi kliknij przycisk **Add (Dodaj)**.
3. Wybierz **REX device (Urządzenie REX)**.
4. Zaznacz port we/wy, na którym chcesz połączyć urządzenie REX. Jeżeli jest dostępny tylko jeden port, zostanie on wybrany automatycznie.
5. Wybierz **Action (Akcja)**, która ma być wyzwalana po odebraniu sygnału REX przez drzwi.
6. W obszarze **REX active (Aktywne REX)** wybierz połączenie obwodu monitora drzwi.
7. Aby zmiany stanu wejścia cyfrowego były ignorowane przed wejściem w nowy stan stabilny, ustaw **Debounce time (ms) (Czas odbicia) (ms)**.
8. Aby przerwanie połączenia między kontrolerem drzwi i urządzeniem REX powodowało zainicjowanie zdarzenia, włącz opcję **Supervised input (Nadzorowane wejście)**. Patrz *Nadzorowane wejścia, on page 17.*

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

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

Dodawanie strefy

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

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

Uwaga

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

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

Aby zmodyfikować strefę:

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

Aby usunąć strefę:

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

Poziom zabezpieczeń strefy

Do strefy można dodać następujące funkcje zabezpieczeń:

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

Uwaga

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

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

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

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

Nadzorowane wejścia

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

- Podłączenie między kontrolerem drzwi a monitorem drzwi. Patrz *Dodawanie monitora drzwi, on page 11*.
- Połączenie pomiędzy kontrolerem drzwi a czytnikiem używającym protokołów Wiegand. Patrz *Dodawanie czytnika, on page 13*.
- Podłączenie między kontrolerem drzwi a urządzeniem REX. Patrz *Dodawanie urządzenia REX, on page 15*.

Aby użyć nadzorowanych wejść:

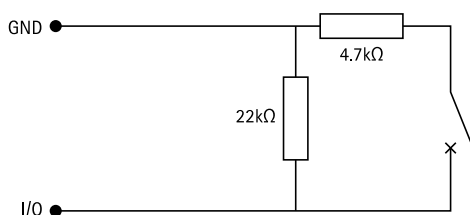
1. Zamontuj rezystory końca linii zgodnie ze schematem połączeń jak najbliżej urządzeń peryferyjnych.

- Przejdź do strony konfiguracyjnej czytnika, monitora drzwi lub urządzenia REX i włącz opcję **Supervised input (Nadzorowane wejście)**.
- Jeżeli zastosowano schemat pierwszego połączenia równoległego, wybierz opcję **Parallel first connection with a 22 K Ω parallel resistor and a 4.7 K Ω serial resistor (Pierwsze połączenie równoległe z 22 k Ω opornikiem równoległym i 4,7 k Ω opornikiem szeregowym)**.
- Jeżeli zastosowano schemat pierwszego połączenia szeregowego, zaznacz opcję **Serial first connection (Pierwsze połączenie szeregowe)**, a następnie z rozwijalnego menu **Resistor values (Wartości oporników)** wybierz wartość rezystora.

Schematy połączeń

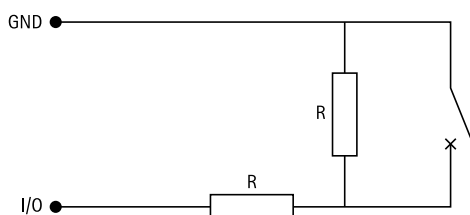
Pierwsze połączenie równoległe

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



Pierwsze połączenie szeregowe

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



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.

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

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

Aby wykonać akcję ręcznie:

- Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
- Wybierz drzwi lub strefę, dla których chcesz wykonać akcję ręcznie.
- Kliknij dowolną akcję wykonywaną ręcznie.

Profile identyfikacji

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

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

Obsługiwane typy identyfikacji: karta, numer PIN, urządzenie REX, statyczne kody QR i dynamiczne kody QR.

Uwaga

Dynamicznych kodów QR i PIN należy używać razem.

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

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

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

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

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

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

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

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

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 obsługujący poświadczenia przy użyciu urządzenia mobilnego.

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

Aby utworzyć profil identyfikacji:

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

Aby zmodyfikować profil identyfikacji:

1. Wybierz kolejno opcje **Configuration > Access control > Identification profiles (Konfiguracja > Kontrola dostępu > Profile identyfikacji)**.
2. Zaznacz profil identyfikacji i kliknij .
3. Aby zmienić nazwę profilu identyfikacji, wpisz nową nazwę.
4. Wprowadź zmiany z boku drzwi.

5. Aby zmodyfikować profil identyfikacji po drugiej stronie drzwi, powtórz poprzednie kroki.
6. Kliknij **OK**.

Aby usunąć profil identyfikacji:

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

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



Konfigurowanie profilu identyfikacji

Formaty kart i kod PIN

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

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

Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN** (Konfiguracja > kontroli dostępu > Formaty kart i kod PIN), aby utworzyć, edytować lub aktywować formaty kart. Można również skonfigurować numer PIN.

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

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

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

Aby utworzyć format karty:

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

Uwaga

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

	Kliknij  , aby zobaczyć przykład rezultatu odwrócenia kolejności bitów.
Zasięg	Ustaw zakres bitów danych dla pola danych. Musi się on mieścić w przedziale określonym w polu Bit length (Liczba bitów) .
Format wyjściowy	Wybierz format wyjściowy danych dla pola danych. Decimal (Dziesiętny): Nazywany jest również „pozycyjnym systemem liczbowym o podstawie 10”, są używane cyfry 0–9. Hexadecimal (Szesnastkowy): nazywany również pozycyjnym systemem liczbowym o podstawie 16 – składa się z 16 unikatowych symboli: cyfr 0–9 i liter a–f.
Kolejność bitów podzakresu	Wybierz kolejność bitów. Little endian: Pierwszy bit jest najmniejszy (najmniej znaczący). Big endian: Pierwszy bit jest największy (najbardziej znaczący).

Aby edytować format karty:

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

4. Kliknij **OK**.

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

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

Aby zresetować wstępnie zdefiniowany format karty:

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

Aby skonfigurować długość numeru PIN:

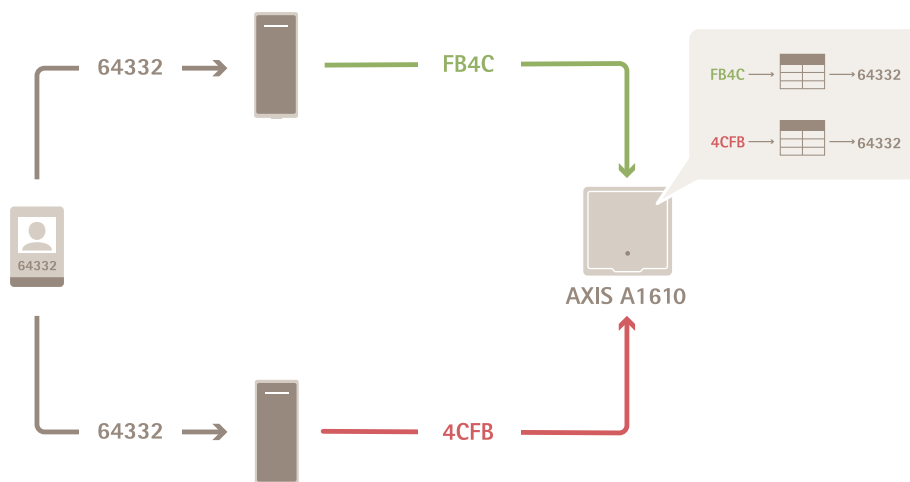
1. Wybierz kolejno opcje **Configuration > Access Control > Card formats and PIN (Konfiguracja > Kontrola dostępu > Formaty kart i kod PIN)**.
2. W obszarze **PIN configuration (Konfiguracja kodu PIN)** kliknij .
3. Wypełnij pola **Min. długość kodu PIN**, **Maks. długość kodu PIN** i **Koniec znaku kodu PIN**.
4. Kliknij **OK**.



Konfigurowanie formatów kart

Ustawienia formatu karty

Informacje ogólne



- Numer karty w zapisie dziesiętnym ma wartość 64332.
- Jeden czytnik przekształca numer karty na liczbę szesnastkową FB4C. Drugi czytnik przekształca go na liczbę szesnastkową 4CFB.

- Kontroler AXIS A1610 Network Door Controller odbiera wartość FB4C i przekształca ją na wartość dziesiętną 64332 zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.
- Kontroler AXIS A1610 Network Door Controller odbiera wartość 4CFB, zmienia ją na FB4C, odwracając porządek bajtów, i przekształca na wartość dziesiętną 64332 zgodnie z ustawieniami formatu karty skonfigurowanymi dla czytnika.

Odwróć kolejność bitów

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

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 FFFFFFF NNNNNNNNNNNNNNNN P
 (1) (2) (3) (4)

- 1 Parzystość wiodąca
- 2 Kod obiektu
- 3 Numer karty
- 4 Parzystość końcowa

Szyfrowana komunikacja

Bezpieczny kanał OSDP

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

Włączanie bezpiecznego kanału OSDP dla całego systemu:

- 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:

- 4.1. W obszarze OSDP Secure Channel (Bezpieczny kanał OSDP) kliknij  .

- 4.2. Wyczyść opcję **Use main encryption key to generate OSDP Secure Channel key** (Użyj głównego klucza szyfrowania, aby wygenerować klucz bezpiecznego kanału OSDP).
- 4.3. Wpisz klucz bezpiecznego kanału OSDP, a następnie kliknij **OK**.

Aby włączyć lub wyłączyć bezpieczny kanał OSDP dla konkretnego czytnika, zobacz *Drzwi i strefy*.

AXIS Barcode Reader

AXIS Barcode Reader to aplikacja, którą można instalować w kamerach Axis. Kontroler drzwi Axis może uwierzytelniać aplikację AXIS Barcode Reader poprzez używanie klucza uwierzytelniania do przyznania dostępu. Kompletny proces konfigurowania aplikacji AXIS Barcode Reader opisano w temacie *Konfigurowanie aplikacji AXIS Barcode Reader*.

Aby utworzyć połączenie między kontrolerem drzwi a aplikacją AXIS Barcode Reader:

1. W aplikacji 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. 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).
 - 2.4. Włącz opcję **AXIS Camera Station Secure Entry**.
 - 2.5. Kliknij przycisk **Add** (Dodaj), a następnie wprowadź adres IP kontrolera drzwi i wklej klucz uwierzytelniania.
 - 2.6. Z rozwijanego menu wybierz czytnik, który ma służyć do skanowania kodów kreskowych.

Tworzenie połączenia z kontrolerem drzwi

1. W aplikacji 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. 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).
 - 2.4. Włącz opcję **AXIS Camera Station Secure Entry**.
 - 2.5. Kliknij przycisk **Add** (Dodaj), a następnie wprowadź adres IP kontrolera drzwi i wklej klucz uwierzytelniania.

- 2.6. Z rozwijalnego menu wybierz czytnik, który ma służyć do skanowania kodów kreskowych.

Multiserwer ^{BETA}

W konfiguracji wieloserwerowej globalni posiadacze kart i grupy posiadaczy kart zdefiniowane na serwerze głównym mogą być wykorzystywane na połączonych serwerach podrzędnych.

Uwaga

- Jeden system może obsługiwać do 64 serwerów podrzędnych.
- Wymagane jest oprogramowanie AXIS Camera Station w wersji 5.47 lub nowszej.
- Serwer główny i podrzędne muszą się znajdować w tej samej sieci.
- Na serwerze głównym i podrzędnych konieczne w Zaporze systemu Windows włączyć zezwalanie na przychodzące połączenia TCP na porcie bezpiecznego wchodzenia. Domyślnie jest to port 55767. Niestandardowe konfiguracje portów są omówione w temacie .

Proces

1. Skonfiguruj serwer jako podrzędny i wygeneruj plik konfiguracyjny. Patrz *Generowanie pliku konfiguracyjnego z serwera podrzędnego, on page 25*.
2. Skonfiguruj serwer jako główny i zaimportuj pliki konfiguracyjne serwerów podrzędnych. Patrz *Importowanie pliku konfiguracyjnego do serwera głównego, on page 25*.
3. Na serwerze głównym skonfiguruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz *Dodawanie posiadacza karty, on page 28* i *Dodawanie grupy, on page 33*.
4. Na serwerach podrzędnych oglądaj i monitoruj globalnych posiadaczy kart i grupy posiadaczy kart. Patrz .

Generowanie pliku konfiguracyjnego z serwera podrzędnego

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

Importowanie pliku konfiguracyjnego do serwera głównego

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

Unieważnianie serwera podrzędnego

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

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

Teraz można skonfigurować ten serwer jako główny lub podrzędny.

Usuwanie serwera podrzędnego

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

Aby usunąć serwer podrzędny:

1. Na serwerze głównym:
 - 1.1. Wybierz kolejno opcje **Access management > Dashboard (Zarządzanie dostępem > Pulpit nawigacyjny)**.
 - 1.2. Zmień globalnych posiadaczy kart i grupy na lokalnych posiadaczy kart i grupy.
 - 1.3. Przejdź do menu **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
 - 1.4. Kliknij **Main server (Główny serwer)** w celu wyświetlenia listy serwerów podrzędnych.
 - 1.5. Zaznacz serwer podrzędny i kliknij przycisk **Delete (Usuń)**.
2. Na serwerze podrzędnym:
 - Przejdź do menu **Configuration > Access control > Multi server (Konfiguracja > Kontrola dostępu > Multiserwer)**.
 - Kliknij polecenie **Sub server (Serwer podrzędny)** i kliknij przycisk **Revoke server (Unieważnij serwer)**.

Ustawienia usługi Active directory^{BETA}

Uwaga

Konta użytkowników w systemie Microsoft Windows oraz użytkownicy i grupy Active Directory mogą uzyskać dostęp do AXIS Camera Station Pro Secure Entry. Sposób dodawania użytkowników w systemie Windows różni się w zależności od wersji. Więcej informacji można uzyskać na stronie support.microsoft.com. Jeżeli korzystasz z sieci domeny Active Directory, skonsultuj się z administratorem sieci.

Gdy po raz pierwszy otworzysz ustawienia usługi Active Directory, będziesz mieć możliwość zaimportowania użytkowników Microsoft Active Directory do obszaru posiadaczy kart w AXIS Camera Station Pro Secure Entry. Patrz *Importowanie użytkowników usługi Active Directory, on page 26*.

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)^{BETA}**.
2. Kliknij **Set up import (Konfiguruj importowanie)**.
3. Postępuj zgodnie z instrukcjami na ekranie, aby wykonać następujące trzy główne kroki:
 - 3.1. Wybierz użytkownika z usługi Active Directory, który posłuży za szablon mapowania danych.

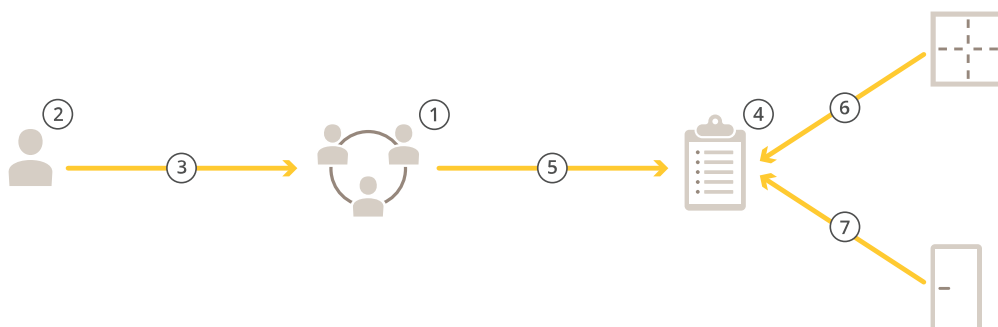
- 3.2. Mapuj dane użytkowników z bazy danych usługi Active Directory do właściwości posiadaczy kart.
- 3.3. Utwórz nową grupę posiadaczy kart w systemie zarządzania dostępem i wybierz grupy Active Directory do zaimportowania.

Nie można zmienić żadnych zaimportowanych danych użytkownika, ale można dodać poświadczenia do zaimportowanego posiadacza karty – zob. *Dodaj poświadczenia, on page 29*.

Konfigurowanie zarządzania dostępem

Proces zarządzania dostępem

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



1. Dodaj grupy. Patrz *Dodawanie grupy*, on page 33.
2. Dodaj posiadaczy kart. Patrz *Dodawanie posiadacza karty*, on page 28.
3. Dodaj posiadaczy kart do grup.
4. Dodaj reguły dostępu. Patrz *Dodawanie reguły dostępu*, on page 33.
5. Przypisz grupy do reguł dostępu.
6. Przypisz strefy do reguł dostępu.
7. Przypisz drzwi do reguł dostępu.

Dodawanie posiadacza karty

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

Można również wybrać opcję zamapowania użytkowników w bazie danych usługi Active Directory jako posiadaczy kart, patrz *Ustawienia usługi Active directory^{BETA}*, on page 26.

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)** > **Cardholders (Posiadacze kart)** i kliknij **+ Add (+ Dodaj)**.
3. Wprowadź imię i nazwisko posiadacza karty i kliknij **Next (Dalej)**.
4. Opcjonalnie kliknij **Advanced (Zaawansowane)** i wybierz dowolne opcje.
5. Dodaj poświadczenie do posiadacza karty. Patrz *Dodaj poświadczenia*, on page 29
6. Kliknij przycisk **Zapisz**.
7. Dodaj posiadacza karty do grupy.
 - 7.1. W obszarze **Groups (Grupy)** wybierz grupę, do której chcesz dodać posiadacza karty, i kliknij **Edit (Edytuj)**.
 - 7.2. Kliknij **+ Add (+ Dodaj)** i wybierz posiadacza karty, którego chcesz dodać do grupy. Można wybrać wielu posiadaczy kart.
 - 7.3. Kliknij **Dodaj**.
 - 7.4. Kliknij przycisk **Zapisz**.

Zaawansowane	
Długi czas dostępu	Wybierz tę opcję, aby w sytuacji, gdy jest zainstalowany monitor drzwi, posiadacz karty miał długi czas dostępu oraz długi czas zbyt długiego otwarcia drzwi.
Zawieś posiadacza karty	Wybierz, aby zawiesić posiadacza karty.
Zezwól na podwójne przeciągnięcie	Wybierz, aby zezwolić posiadaczowi karty na zastąpienie bieżącego stanu drzwi. Mogą go na przykład użyć do odblokowania drzwi poza regularnym harmonogramem.
Zwolnienie z blokady ogólnej	Zaznacz, aby zezwolić posiadaczowi karty na dostęp podczas blokady.
Exempt from anti-passback (Zwolnienie z reguły anti-passback)	Wybierz tę opcję, aby przyznać zwolnić posiadacza karty z reguły anti-passback. Reguła Anti-passback uniemożliwia użycie tych samych danych uwierzytelniających, które zostały użyte osoby, które weszły na obszar wcześniej. Zanim takie poświadczenia będą mogły zostać użyte ponownie, posiadacz kart z tymi danymi musi najpierw opuścić obszar.
Globalny posiadacz karty	Zaznacz tę opcję, aby możliwe było wyświetlanie i monitorowanie posiadacza karty na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Patrz <i>Multiserwer^{BETA}</i> , on page 25.



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:

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

Aby dodać poświadczenie mobilne do posiadacza karty:

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **Mobile credential (Poświadczenie mobilne)**.
2. Wprowadź nazwę poświadczenia.
3. Ustaw datę początkową i końcową poświadczenia.

4. Wybierz **Send the mobile credential to the cardholder after saving** (Po zapisaniu wyślij poświadczenie obsługiwane za pomocą urządzenia mobilnego do posiadacza karty). Posiadacz karty otrzyma wiadomość e-mail z instrukcją parowania.
5. Kliknij **Dodaj**.

Zobacz przykład w temacie *Używanie aplikacji AXIS Mobile Credential jako poświadczeń Bluetooth, on page 32*.

Aby dodać do posiadacza karty poświadczenie w postaci tablicy rejestracyjnej:

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

Zobacz przykład w temacie *Używanie numeru rejestracyjnego jako poświadczenia, on page 31*.

Aby dodać do posiadacza karty poświadczenie w postaci numeru PIN:

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

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

Aby dodać do posiadacza karty poświadczenie w postaci karty:

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

Uwaga

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

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

Uwaga

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

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

Aby dodać do posiadacza karty poświadczenie w postaci kodu QR:

Uwaga

Korzystanie z kodów QR jako poświadczeń wymaga zsynchronizowania czasu na kontrolerze systemu i kamerze z aplikacją **AXIS Barcode Reader**. Aby uzyskać idealną synchronizację czasu, zaleca się korzystanie z tego samego źródła czasu dla obu urządzeń.

1. W obszarze **Credentials (Poświadczenia)** kliknij **+ Add (+ Dodaj)** i wybierz **QR-code (Kod QR)**.
2. Wprowadź nazwę poświadczenia.
3. Domyślnie jest włączona opcja **Dynamic QR (Dynamiczny kod QR)**. Używanie dynamicznego kodu QR wymaga podania kodu PIN.
4. Ustaw datę początkową i końcową poświadczenia.
5. Aby kod QR był wysyłany automatycznie po zapisaniu posiadacza karty, zaznacz opcję **Send QR code to cardholder when credential is saved (Po zapisaniu poświadczenia wyślij kod QR do posiadacza karty)**.
6. Kliknij **Dodaj**.

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

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

Używanie numeru rejestracyjnego jako poświadczenia

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

1. Dodaj kontroler drzwi i kamerę do AXIS Camera Station Pro Secure Entry. Patrz
2. Ustaw datę i godzinę dla nowych urządzeń, wybierając polecenie **Synchronize with server computer time (Synchronizuj z czasem serwera)**. Patrz .
3. Uaktualnij oprogramowanie sprzętowe na nowych urządzeniach do najnowszej dostępnej wersji. Patrz .
4. Dodaj nowe drzwi połączone z kontrolerem drzwi. Patrz *Dodawanie drzwi, on page 5*.
 - 4.1. Dodaj czytnik w obszarze **Side A (Strona A)**. Zob. *Dodawanie czytnika, on page 13*.
 - 4.2. W obszarze **Door settings (Ustawienia drzwi)** wybierz **AXIS License Plate Verifier** jako **Reader type (Typ czytnika)** i wpisz nazwę czytnika.
 - 4.3. Opcjonalnie dodaj czytnik lub urządzenie REX w obszarze **Side B (Strona B)**.
 - 4.4. Kliknij **OK**.
5. Zainstaluj i włącz w kamerze aplikację **AXIS License Plate Verifier**. Zobacz *Podręcznik użytkownika oprogramowania AXIS License Plate Verifier*.
6. Włącz aplikację **AXIS License Plate Verifier**.
7. Skonfiguruj aplikację **AXIS License Plate Verifier**.
 - 7.1. Przejdź do **Configuration > Access control > Encrypted communication (Konfiguracja > Kontrola dostępu > Komunikacja szyfrowana)**.

- 7.2. W obszarze **External Peripheral Authentication Key (Klucz uwierzytelniania zewnętrznego urządzenia peryferyjnego)** kliknij polecenie **Show authentication key (Pokaż klucz uwierzytelniania)** oraz **Copy key (Kopiuje klucz)**.
- 7.3. Otwórz aplikację **AXIS License Plate Verifier** z poziomu interfejsu WWW kamery.
- 7.4. Nie przeprowadzaj konfiguracji.
- 7.5. Przejdź do opcji **Settings (Ustawienia)**.
- 7.6. W obszarze **Access control (Kontrola dostępu)** wybierz **Secure Entry (Bezpieczne wejście)** jako **Type (Typ)**.
- 7.7. W obszarze **IP address (Adres IP)** wpisz adres IP kontrolera drzwi.
- 7.8. W obszarze **Authentication key (Klucz uwierzytelniania)** wklej skopiowany wcześniej klucz uwierzytelniania.
- 7.9. Kliknij przycisk **Połącz**.
- 7.10. W obszarze **Door controller name (Nazwa kontrolera drzwi)** wybierz kontroler drzwi.
- 7.11. W obszarze **Reader name (Nazwa czytnika)** wybierz czytnik dodany wcześniej.
- 7.12. Włącz integrację.
8. Dodaj posiadacza karty, któremu chcesz przyznać dostęp. Patrz *Dodawanie posiadacza karty, on page 28*
9. Dodaj poświadczenia tablic rejestracyjnych do nowego posiadacza karty. Patrz *Dodaj poświadczenia, on page 29*
10. Dodaj regułę dostępu. Patrz *Dodawanie reguły dostępu, on page 33*.
 - 10.1. Dodaj harmonogram.
 - 10.2. Dodaj posiadacza karty, któremu chcesz przyznać dostęp do tablicy rejestracyjnej.
 - 10.3. Dodaj drzwi z czytnikiem **AXIS License Plate Verifier**.

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 aplikacji **AXIS Camera Station Pro**.
 - 3.1. Wybierz kolejno opcje **Configuration (Konfiguracja) > Access control (Kontrola dostępu) > Doors and zones (Drzwi i strefy)**.
 - 3.2. Wybierz drzwi, do których chcesz dodać czytnik **Bluetooth**, i kliknij **Edit (Edytuj)**.
 - 3.3. Kliknij **+ Add (Dodaj)** z boku 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: *Profile identyfikacji, on page 18*.
6. Dodaj mobilne poświadczenia do posiadacza karty. Patrz *Dodaj poświadczenia, on page 29*.
7. Sparuj mobilne poświadczenia z czytnikiem z włączonym trybem parowania.
 - 7.1. Zbliź telefon komórkowy posiadacza karty do czytnika Bluetooth z włączonym trybem parowania.
 - 7.2. Postępuj zgodnie z instrukcjami podanymi w e-mailu wysłanym do posiadacza karty.

Dodawanie grupy

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

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)** > **Groups (Grupy)** i kliknij **+ Add (+ Dodaj)**.
3. Wprowadź nazwę i opcjonalnie inicjały grupy.
4. Zaznacz opcję **Global group (Grupa globalna)**, aby posiadaczy kart można było wyświetlać i monitorować na serwerach podrzędnych. Ta opcja jest dostępna tylko dla posiadaczy kart utworzonych na serwerze głównym. Patrz *Multiserwer BETA, on page 25*.
5. Dodawanie posiadaczy kart do grupy:
 - 5.1. Kliknij **+ Dodaj**.
 - 5.2. Wybierz posiadaczy kart, których chcesz dodać, i kliknij **Add (Dodaj)**.
6. Kliknij przycisk **Zapisz**.

Dodawanie reguły dostępu

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

Reguła dostępu zawiera następujące elementy:

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

Drzwi i strefy – gdzie ma zostać przyznany dostęp.

Harmonogramy – kiedy ma zostać przyznany dostęp.

Aby dodać regułę dostępu:

1. Otwórz kartę  zarządzania dostępem.
2. Przejdź do obszaru **Cardholder management (Zarządzanie posiadaczami kart)**.
3. W obszarze **Access rules (Reguły dostępu)** kliknij **+ Add (+ Dodaj)**.
4. Wprowadź nazwę reguły dostępu i kliknij **Next (Dalej)**.
5. Skonfiguruj posiadaczy kart i grupy:
 - 5.1. W obszarze **Cardholders (Posiadacze kart)** lub **Groups (Grupy)** kliknij **+ Add (+ Dodaj)**.

- 5.2. Wybierz posiadaczy kart lub grupy i kliknij **Add (Dodaj)**.
6. Konfiguracja drzwi i stref:
 - 6.1. W obszarze **Doors (Drzwi)** lub **Zones (Strefy)** kliknij **+ Add (+ Dodaj)**.
 - 6.2. Wybierz drzwi lub strefy i kliknij **Add (Dodaj)**.
7. Konfiguracja harmonogramów:
 - 7.1. W obszarze **Schedules (Harmonogramy)** kliknij **+ Add (+ Dodaj)**.
 - 7.2. Wybierz jeden lub więcej harmonogramów i kliknij **Add (Dodaj)**.
8. Kliknij przycisk **Zapisz**.

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



Eksportowanie raportów konfiguracji systemu

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

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

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

Tworzenie raportów aktywności posiadaczy kart

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

Raport ze zbiórki zawiera listę posiadaczy kart obecnych w określonej strefie, ułatwiając ustalenie, kto jest bezpieczny, a kto zaginął w sytuacji awaryjnej. Pomaga on zarządcom budynków w odszukiwaniu pracowników i gości po ewakuacji. Punkt zbiórki to wyznaczony czytnik, do którego pracownicy zgłaszają się w sytuacji awaryjnej, umożliwiając wygenerowanie raportu z listą osób znajdujących się na miejscu i poza nim. System oznacza posiadaczy kart jako zaginionych, dopóki nie zameldują się w punkcie zbiórki lub dopóki inna osoba nie oznaczy ich ręcznie jako bezpiecznych.

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

Aby utworzyć i uruchomić raport imienny lub ze zbiórki:

1. 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. Jeśli chcesz otrzymać raport ze zbiórki, wybierz **Mustering point (Punkt zbiórki)** i czytnik odpowiadający punktowi zbiórki.
8. Wybierz ramy czasowe raportu.
9. Kliknij przycisk **Zapisz**.
10. Wybierz raport i kliknij **Run (Uruchom)**.

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

Stan w raporcie ze zbiórki	Opis
Safe (Bezpieczny)	Posiadacz karty przeciągnął swoją kartę w punkcie zbiórki.
Missing (Zaginiony)	Posiadacz karty nie przeciągnął swojej karty w punkcie zbiórki.

Ustawienia zarządzania dostępem

Aby dostosować pola posiadacza karty używane na pulpicie nawigacyjnym dostępu:

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

Aby używać kodu obiektu do weryfikowania systemu kontroli dostępu:

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

Uwaga

Podczas konfigurowania profili identyfikacji należy również zaznaczyć opcję **Include facility code for card validation (Dołącz kod obiektu do sprawdzania poprawności karty)**. Patrz *Profile identyfikacji, on page 18*.

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

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

Import i eksport

Importuj posiadaczy kart

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

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

Można również wybrać opcję zamapowania użytkowników w bazie danych usługi Active Directory jako posiadaczy kart, patrz *Ustawienia usługi Active directory^{BETA}, on page 26*.

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

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

Ustawienia importu	
Pierwszy wiersz to nagłówek	Wybierz, czy plik CSV zawiera nagłówek kolumny.
Ogranicznik kolumny	Wprowadź format ogranicznika kolumn w pliku CSV.

Ustawienia importu	
Unikalny identyfikator	Do identyfikowania posiadacza karty system domyślnie używa Cardholder ID (Identyfikatora posiadacza karty) . Możesz również użyć imienia i nazwiska lub adresu e-mail. Unikatowy identyfikator zapobiega importowaniu duplikatów rekordów personelu.
Format numeru karty	Domyślnie jest zaznaczona opcja Allow both hexadecimal and number (Zezwalaj na liczbę szesnastkową i liczbową) .

Eksportowanie danych posiadaczy kart

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

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

AXIS 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 posiadaczy kart.

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

T10231644_pl

2026-02 (M4.3)

© 2025 – 2026 Axis Communications AB