AXIS A1001 & AXIS Entry Manager

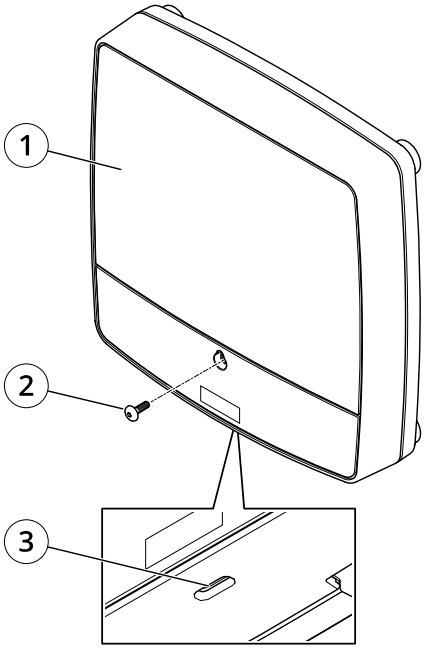
Podręcznik użytkownika

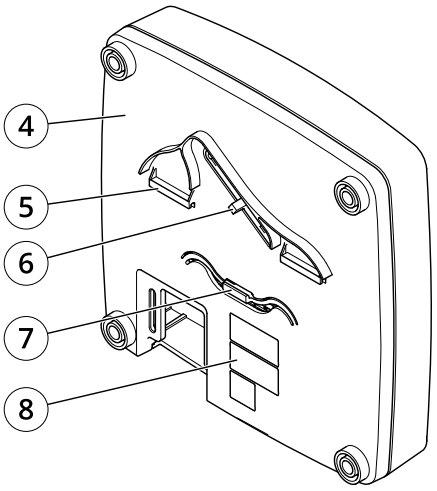
Spis treści

Spis treści

Informacje ogólne o produkcie

Informacje ogólne o produkcie

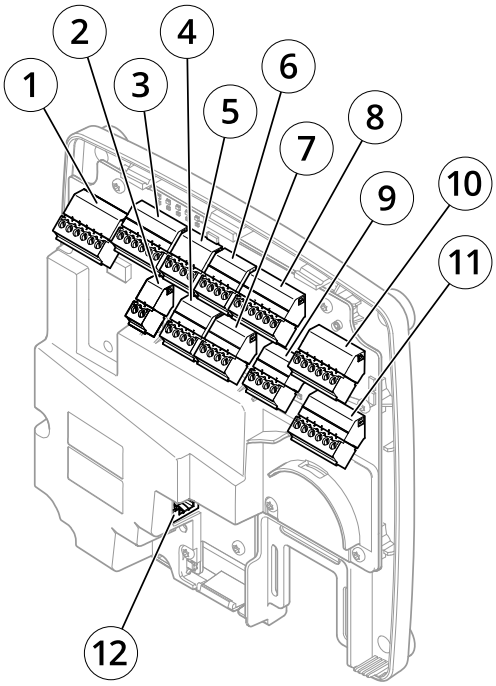




Przód i tył:

1 *Osłona*
2 *Osłona śruby*
3 *Otwór do podważania osłony*
4 *Podstawa*
5 *Klip DIN — górny*
6 *Przełącznik alarmu zabezpieczenia antysabotażowego – tył*
7 *Klip DIN – dolny*
8 *Numer części (P/N) i numer seryjny (S/N)*

Informacje ogólne o produkcie



Interfejs I/O:

1 *Złącze danych czytnika (CZYTNIK DANE 1)*
10 *Złącze danych czytnika (CZYTNIK DANE 2)*
3 *Złącze I/O czytnika (CZYTNIK I/O 1)*
8 *Złącze I/O czytnika (I/O CZYTNIKA 2)*
4 *Złącze drzwi (DRZWI WEJŚCIE 1)*
7 *Złącze drzwi (DRZWI WEJŚCIE 2)*
6 *Złącze pomocnicze (AUX)*
5 *Złącze audio (AUDIO) (nieużywane)*

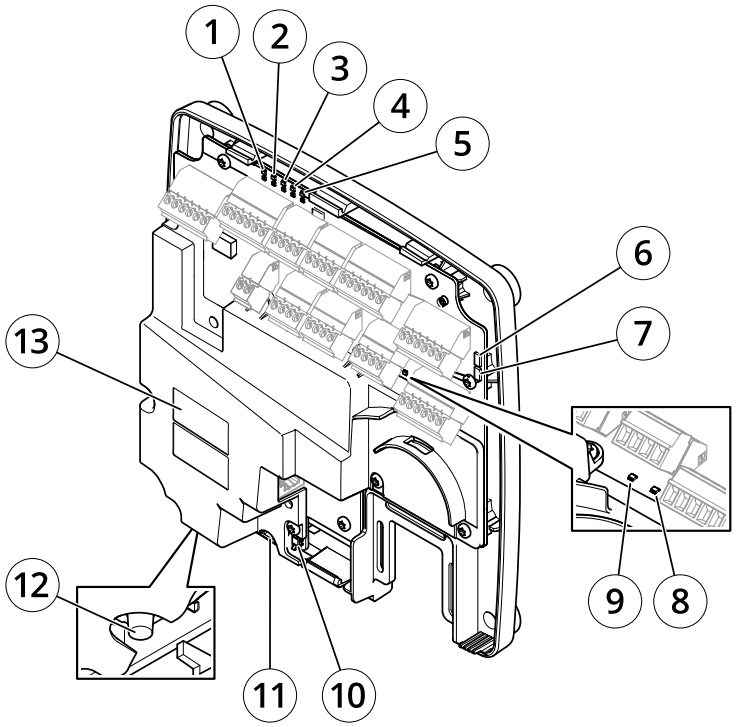
Zewnętrzne wejścia zasilania:

2 *Złącze zasilania (DC WEJŚCIE)*
12 *Złącze sieciowe (PoE)*

Wyjścia zasilania:

9 *Złącze zasilania zamka (ZAMEK)*
11 *Złącze zasilania i przekaźnika (ZASILANIE, PRZEKAŹNIK)*

Informacje ogólne o produkcie



Wskaźniki LED, przyciski i inny sprzęt:

1 *Wskaźnik LED zasilania*
2 *Wskaźnik LED stanu*
3 *Wskaźnik LED sieci*
4 *Wskaźnik LED czytnika 2 (nieużywany)*
5 *Wskaźnik LED czytnika 1 (nieużywany)*
6 *Złącze główkowe alarmu antysabotażowego – przód (TF)*
7 *Złącze główkowe alarmu antysabotażowego – tył (TB)*
8 *Wskaźnik LED zamka*
9 *Wskaźnik LED zamka*
10 *Czujnik alarmu antysabotażowego – przód*
11 *Gniazdo karty SD (microSDHC) (nieużywane)*
12 *Przycisk Control*
13 *Numer części (P/N) i numer seryjny (S/N)*

Wskaźniki LED

LED	Kolor	Wskazanie
Sieć	Zielony	Stałe światło przy podłączeniu do sieci 100 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Bursztynowy	Stałe światło przy podłączeniu do sieci 10 Mbit/s. Miga w przypadku wystąpienia aktywności sieciowej.
	Zgaszony	Brak połączenia z siecią.
Stan	Zielony	Stałe zielone światło przy normalnym działaniu.
	Bursztynowy	Stałe światło podczas uruchamiania i odtwarzania ustawień.
	Czerwony	Powolne miganie w przypadku niepowodzenia aktualizacji.

Zasilanie	Zielony	Normalne działanie.
	Bursztynowy	Miga na zielono/bursztynowo podczas aktualizacji oprogramowania sprzętowego.
Blokada	Zielony	Stałe światło bez podłączonego zasilania.
	Czerwony	Stałe światło z podłączonym zasilaniem.
	Zgaszony	Zmienne.

Uwaga

- Wskaźnik LED stanu można skonfigurować tak, by podczas aktywnego zdarzenia migał.
- Wskaźnik LED stanu można skonfigurować tak, by migał po rozpoznaniu jednostki. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.

Złącza i przyciski

Interfejs I/O

Złącza danych czytnika
Dwa 6-pinowe bloki złączy obsługujące protokoły RS485 i Wiegand do komunikacji z czytnikiem. Specyfikacja: *strona 67*.

Złącza I/O czytnika
Dwa 6-pinowe bloki złączy wejść i wyjść czytnika. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze I/O czytnika zapewnia interfejs do:

- Wejścia cyfrowego – na przykład do podłączenia alarmów sabotażu czytnika.
- Wyjścia cyfrowego – na przykład do podłączenia sygnałów dźwiękowych i diod LED czytnika.

Specyfikacja: *strona 67*.

Złącza drzwi
Dwa 4-pinowe bloki złączy do podłączania urządzeń monitorujących drzwi i urządzeń REX. Specyfikacja: *strona 68*.

Złącze pomocnicze
4-pinowy konfigurowalny blok złączy I/O. Złącze pomocnicze służy do obsługi urządzeń zewnętrznych w kombinacji przykładowo z alarmami sabotażowymi, wyzwalaniem zdarzeń i powiadomieniami o alarmach. Oprócz punktu odniesienia 0 V DC i zasilania (wyjście stałoprądowe) złącze pomocnicze zapewnia interfejs do:

- Wejście cyfrowe – wejście alarmowe do podłączenia urządzeń, które mogą przełączać się pomiędzy obwodem zamkniętym i otwartym, na przykład czujników PIR lub czujników wykrywania zbicia szyby.
- Wyjście cyfrowe – do podłączania urządzeń zewnętrznych, takich jak alarmy przeciwwłamaniowe, syreny lub światła. Podłączone urządzenia mogą być aktywowane przez interfejs programowania aplikacji VAPIX lub przez regułę akcji.

Specyfikacja: *strona 69*.

Zewnętrzne wejścia zasilania

POWIADOMIENIE

Ten produkt musi zostać podłączony przy pomocy kabla ekranowanego (STP). Wszystkie kable łączące produkt z siecią powinny być używane zgodnie z przeznaczeniem. Upewnij się, że urządzenia sieciowe zainstalowane są zgodnie z zaleceniami producenta. Informacje dotyczące wymogów regulacyjnych: .

Złącze zasilania
2-stykowy blok złączy wejścia zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤100 W lub nominalnym prądem ograniczonym do ≤5 A. Specyfikacja: *strona 69*.

Złącze sieciowe
złącze RJ45 Ethernet. Obsługuje Power over Ethernet (PoE). Specyfikacja: *strona 70*.

Wyjścia zasilania

Złącze zasilania zamka

4-pinowy blok złączy umożliwiający podłączenie jednego lub dwóch zamków. Złącza zamka można również użyć do zasilania urządzeń zewnętrznych. Specyfikacja: *strona 70*.

Złącze zasilania i przekaźnika

6-stykowy blok złączy do podłączenia zasilania i przekaźnika kontrolera drzwi do podłączania urządzeń zewnętrznych, takich jak zamki czy czujniki. Specyfikacja: *strona 70*.

Przyciski i inny sprzęt

Złącze główkowe alarmu antysabotażowego
2-pinowe złącza główkowe do odłączania przednich i tylnych alarmów antysabotażowych. Specyfikacja: *strona 71*.

Przycisk Control
Przycisk ten służy do:

- Przywracania domyślnych ustawień fabrycznych produktu. Patrz *strona 63*.
- Łączenia się z usługą AXIS Video Hosting System. Patrz *strona 57*. Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około jedną sekundę, aż dioda LED stanu zacznie migać na zielono.
- Łączenia się z usługą AXIS Internet Dynamic DNS Service. Patrz *strona 57*. Aby połączyć się z usługą, naciśnij i przytrzymaj przycisk przez około trzy sekundy.

Instalacja

Instalacja

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

help.axis.com/?&tpiaId=19467&section=product-overview

Film dotyczący instalacji produktu.

Uzyskiwanie dostępu do produktu

Aby zainstalować produkt Axis, skorzystaj z instrukcji instalacji dostarczonej z produktem.

Dostęp do urządzenia

1. Otwórz przeglądarkę i wprowadź adres IP lub nazwę hosta urządzenia Axis.

   Jeśli nie znasz adresu IP, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować urządzenie w sieci.

2. Wprowadź nazwę użytkownika oraz hasło. Jeżeli uzyskujesz dostęp do urządzenia po raz pierwszy, musisz ustawić hasło root. Patrz .

3. W przeglądarce zostanie otwarta aplikacja AXIS Entry Manager. Jeśli korzystasz z komputera, zostanie wyświetlona strona Informacje ogólne. Jeśli używasz urządzenia przenośnego, zostanie otwarta strona początkowa dla urządzeń mobilnych.

Informacje o stronie początkowej dla urządzeń mobilnych

Strona początkowa dla urządzeń mobilnych zawiera stan drzwi i zamków podłączonych do kontrolera drzwi. Można na niej przetestować odblokowywanie i blokowanie zamków. Odśwież stronę, aby zobaczyć wynik.

Można skorzystać z łącza, aby przejść do aplikacji do Axis Entry Manager.

Uwaga

- Aplikacja Axis Entry Manager nie obsługuje urządzeń mobilnych.
- Jeśli przejdziesz do aplikacji do Axis Entry Manager, nie będzie można wrócić do strony początkowej dla urządzeń mobilnych.

Uzyskiwanie dostępu do produktu przez internet

Router sieciowy umożliwia produktom w sieci prywatnej (LAN) współdzielić jedno połączenie internetowe. Odbywa się to poprzez przekazanie ruchu sieciowego z sieci prywatnej do internetu.

Większość routerów jest wstępnie skonfigurowana tak, aby zatrzymać próby uzyskania dostępu do sieci prywatnej (LAN) z sieci publicznej (internetu).

Użyj opcji **NAT traversal**, gdy produkt Axis jest podłączony do intranetu (LAN) i chcesz go udostępnić po drugiej stronie (WAN) routera NAT. Po prawidłowym skonfigurowaniu NAT traversal cały ruch HTTP do zewnętrznego portu HTTP w routerze NAT jest przekazywany do produktu.

Włączanie funkcji NAT traversal

- Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.
- Kliknij przycisk **Włącz**.
- Ręcznie skonfiguruj router NAT, aby umożliwić dostęp przez internet.

Patrz również AXIS Internet Dynamic DNS Service na stronie *www.axiscam.net*

Uwaga

- W tym kontekście router oznacza dowolne urządzenie działające jako router sieciowy, takie jak router NAT, router sieciowy, bramka internetowa, router szerokopasmowy, urządzenie do udostępniania szerokopasmowego lub oprogramowanie, takie jak zapora.
- Aby funkcja NAT traversal działała, produkt musi obsługiwać NAT traversal. Router musi również obsługiwać protokół UPnP®.

Uzyskiwanie dostępu do produktu

Ustawianie hasła root

Aby uzyskać dostęp do produktu Axis, należy ustawić hasło dla domyślnego administratora **root**. Można to zrobić w oknie dialogowym **Skonfiguruj hasło root**, które zostanie otwarte przy pierwszym dostępie do produktu.

Aby uniknąć podsłuchów sieciowych, hasło root można ustawić za pomocą zaszyfrowanego połączenia HTTPS, wymagającego certyfikatu HTTPS. HTTPS (Hypertext Transfer Protocol over SSL) to protokół używany do szyfrowania ruchu pomiędzy przeglądarkami i serwerami. Certyfikat HTTPS zapewnia szyfrowaną wymianę informacji. Patrz *HTTPS na stronie 53*.

Domyślna nazwa użytkownika dla administratora **root** jest stała i nie można jej usunąć. W razie utraty hasła dla użytkownika root należy przywrócić ustawienia fabryczne produktu. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 63*.

Aby ustawić hasło, wprowadź je bezpośrednio w oknie dialogowym.

Strona Informacje ogólne

Strona Informacje ogólne w programie AXIS Entry Manager zawiera informacje o nazwie kontrolera drzwi, jego adresie MAC, adresie IP i wersji oprogramowania sprzętowego. Umożliwia także identyfikację kontrolera drzwi w sieci lub w systemie.

Przy pierwszym dostępie do produktu Axis na stronie Informacje ogólne pojawi się monit o skonfigurowanie sprzętu, ustawienie daty i godziny, skonfigurowanie ustawień sieci oraz skonfigurowanie kontrolera drzwi jako części systemu lub jako autonomicznej jednostki. Więcej informacji na temat konfigurowania systemu: *Konfiguracja – krok po kroku na stronie 12*.

Aby powrócić do strony Informacje ogólne na innych stronach internetowych produktu, kliknij opcję **Informacje ogólne** na pasku menu.

Konfiguracja systemu

Aby otworzyć strony konfiguracji produktu, kliknij opcję **Ustawienia** w prawym górnym rogu strony Informacje ogólne.

Produkt Axis może być konfigurowany przez administratorów. Więcej informacji dotyczących użytkowników i administratorów: *strona 31*, *strona 39* i *strona 53*.

Konfiguracja – krok po kroku

Przed rozpoczęciem korzystania z systemu kontroli dostępu należy wykonać następujące etapy konfiguracji:

1. Jeśli na co dzień nie posługujesz się językiem angielskim, możesz wybrać inny język aplikacji AXIS Entry Manager. Patrz *Wybór języka na stronie 12*.
2. Ustaw datę i godzinę. Patrz *strona 12*.
3. Skonfiguruj ustawienia sieciowe. Patrz *strona 14*.
4. Skonfiguruj kontroler drzwi i podłączone urządzenia, takie jak czytniki, zamki i urządzenia request to exit (REX). Patrz *Konfigurowanie sprzętu na stronie 14*.
5. Zweryfikuj połączenia ze sprzętem. Patrz *strona 21*.
6. Skonfiguruj karty i formaty. Patrz *strona 21*.
7. Skonfiguruj system kontrolerów drzwi. Patrz *Zarządzanie sieciowymi kontrolerami drzwi na stronie 27*.

Informacje na temat tego, jak skonfigurować i zarządzać drzwiami systemu, harmonogramami, użytkownikami i grupami: *Zarządzanie dostępem na stronie 31*.

Informacje dotyczące zaleceń związanych z konserwacją: *Instrukcje konserwacji na stronie 29*.

Uwaga

Aby można było dodać lub usunąć kontrolery drzwi, aby dodać, usunąć lub edytować użytkowników oraz aby skonfigurować sprzęt, ponad połowa kontrolerów drzwi w systemie musi być w trybie **online**. Aby sprawdzić stan kontrolera drzwi, przejdź do menu **Ustawienia > Zarządzaj sieciowymi kontrolerami drzwi w systemie**.

Wybór języka

Domyślnym językiem aplikacji AXIS Entry Manager jest angielski, ale możesz przełączyć się na dowolny język skonfigurowany w urządzeniu. Informacje na temat najnowszego dostępnego oprogramowania sprzętowego można znaleźć na stronie *www.axis.com*.

Możesz zmienić język na dowolnej stronie internetowej produktu.

Aby zmienić język, kliknij listę rozwijaną języków  i wybierz język. Wszystkie strony internetowe i strony pomocy produktu będą wyświetlane w wybranym języku.

Uwaga

- Po zmianie języka format daty zmienia się również na format powszechnie używany w wybranym języku. Poprawny format jest wyświetlany w polach danych.
- Jeśli zresetujesz urządzenie do domyślnych ustawień fabrycznych, aplikacja AXIS Entry Manager przełączy się z powrotem na angielski.
- Jeśli przywrócisz ustawienia produktu, aplikacja AXIS Entry Manager będzie nadal używać wybranego języka.
- Jeśli przywrócisz lub ponownie uruchomisz produkt, aplikacja AXIS Entry Manager będzie nadal używać wybranego języka.
- Jeśli zaktualizujesz oprogramowanie sprzętowe, aplikacja AXIS Entry Manager będzie nadal używać wybranego języka.

Ustawianie daty i godziny

Jeśli kontroler drzwi stanowi część systemu, ustawienia daty i godziny zostaną przekazane wszystkim kontrolerom drzwi. Oznacza to, że ustawienia są narzucane innym kontrolerom w systemie, niezależnie od tego, czy zsynchronizujesz się z serwerem NTP, ustawisz datę i godzinę ręcznie, czy pobierzesz datę i godzinę z komputera. Jeśli nie widzisz zmian, spróbuj odświeżyć stronę w przeglądarce. Więcej informacji na temat zarządzania systemem kontrolerów drzwi: *Zarządzanie sieciowymi kontrolerami drzwi na stronie 27*.

Aby ustawić datę i godzinę produktu Axis, przejdź do menu **Ustawienia > Data i godzina**.

Datę i godzinę możesz ustawić w jeden z następujących sposobów:

- Pobierz datę i godzinę z serwera sieciowego protokołu synchronizacji czasu (NTP). Patrz *strona 13*.
- Ustaw datę i godzinę ręcznie. Patrz *strona 13*.
- Pobierz datę i godzinę z komputera. Patrz *strona 13*.

Aktualny czas kontrolera to aktualna data i godzina kontrolera drzwi (w formacie 24 h).

Te same opcje dla daty i godziny są również dostępne na stronach Opcji systemu. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Data i godzina**.

Pobieranie daty i godziny z serwera sieciowego protokołu synchronizacji czasu (NTP)

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Wybierz **Strefę czasową** z listy rozwijanej.
3. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
4. Wybierz opcję **Synchronizuj z NTP**.
5. Wybierz domyślny adres DHCP lub wprowadź adres serwera NTP.
6. Kliknij przycisk **Zapisz**.

Podczas synchronizacji z serwerem NTP data i godzina są aktualizowane w sposób ciągły, ponieważ dane są wysyłane z serwera NTP. Więcej informacji na temat ustawień NTP: *Konfiguracja NTP na stronie 58*.

W przypadku używania nazwy hosta dla serwera NTP należy skonfigurować serwer DNS. Patrz *Konfiguracja DNS na stronie 57*.

Ręczne ustawianie daty i godziny

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
3. Wybierz polecenie **Ustaw datę i godzinę ręcznie**.
4. Wprowadź żądaną datę i godzinę.
5. Kliknij przycisk **Zapisz**.

W przypadku ręcznego ustawiania daty i godziny data i godzina zostaną ustawione jednorazowo i nie będą automatycznie aktualizowane. Oznacza to, że jeśli będzie wymagana aktualizacja daty lub godziny, zmiany muszą zostać wprowadzone ręcznie, ponieważ nie ma połączenia z zewnętrznym serwerem NTP.

Pobieranie daty i godziny z komputera

1. Przejdź do menu **Ustawienia > Data i godzina**.
2. Jeśli w Twoim regionie stosowana jest zmiana czasu letniego, wybierz opcję **Dostosuj do zmiany czasu letniego**.
3. Wybierz polecenie **Ustaw datę i godzinę ręcznie**.

4. Kliknij przycisk **Zsynchronizuj i zapisz**.

Podczas korzystania z czasu komputera data i godzinę są synchronizowane z komputerem raz i nie będą aktualizowane automatycznie. Oznacza to, że zmiana daty i godziny w komputerze, który służy do zarządzania systemem, wymaga ponownej synchronizacji z urządzeniem.

Konfiguracja ustawień sieciowych

Aby skonfigurować podstawowe ustawienia sieciowe, przejdź do menu **Ustawienia > Ustawienia sieciowe** lub **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**.

Więcej informacji na temat ustawień sieciowych: *Sieć na stronie 55*.

Konfigurowanie sprzętu

Zanim będzie można zarządzać drzwiami i piętrami, sprzęt należy skonfigurować na stronach Konfiguracji sprzętowej.

Przed zakończeniem konfiguracji sprzętowej możesz podłączyć czytniki, blokady i inne urządzenia do produktu Axis. Jednak łatwiej będzie podłączyć urządzenia, jeśli najpierw zakończysz konfigurację sprzętową, ponieważ schemat styków sprzętu będzie dostępny po zakończeniu konfiguracji. Schemat styków sprzętu jest przewodnikiem po podłączaniu urządzeń do pinów i może służyć jako arkusz referencyjny do konserwacji. Aby uzyskać instrukcje dotyczące konserwacji, patrz *strona 29*.

Jeśli konfigurujesz sprzęt po raz pierwszy, wybierz jedną z następujących metod:

- Importowanie pliku konfiguracji sprzętowej. Patrz *strona 14*.
- Tworzenie nowej konfiguracji sprzętowej. Patrz *strona 15*.

Uwaga

Jeśli sprzęt danego produktu nie został uprzednio skonfigurowany lub został usunięty, opcja **Konfiguracja sprzętowa** będzie dostępna w panelu powiadomień na stronie Informacje ogólne.

Importowanie pliku konfiguracji sprzętowej

Konfigurację sprzętową produktu Axis można wykonać szybciej, importując plik konfiguracji sprzętowej.

Po wyeksportowaniu pliku z jednego produktu i zaimportowaniu go do innych można wykonać wiele kopii tej samej konfiguracji sprzętowej bez powtarzania tych samych kroków. Można także przechowywać eksportowane pliki jako kopie zapasowe i używać ich do przywracania poprzedniej konfiguracji sprzętowej. Więcej informacji: *Eksportowanie pliku konfiguracji sprzętowej na stronie 14*.

Importowanie pliku konfiguracji sprzętowej:

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa**.
2. Kliknij przycisk **Importuj konfigurację sprzętową** lub, jeśli konfiguracja sprzętowa już istnieje, **Zresetuj i zaimportuj konfigurację sprzętową**.
3. W wyświetlonym oknie dialogowym przeglądarki plików znajdź i wybierz plik konfiguracji sprzętowej (*.json) na swoim komputerze.
4. Kliknij przycisk **OK**.

Eksportowanie pliku konfiguracji sprzętowej

Konfigurację sprzętową produktu Axis można wyeksportować w celu wielokrotnego skopiowania tej samej konfiguracji sprzętowej. Można także przechowywać eksportowane pliki jako kopie zapasowe i używać ich do przywracania poprzedniej konfiguracji sprzętowej.

Uwaga

Konfiguracji sprzętowej pięter nie można wyeksportować.

Ustawienia zamków bezprzewodowych nie są uwzględniane podczas eksportowania konfiguracji sprzętowej.

Aby wyeksportować plik konfiguracji sprzętowej:

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa**.
2. Kliknij polecenie **Eksportuj konfigurację sprzętową**.
3. W zależności od przeglądarki konieczne może być przejście do okna dialogowego w celu dokończenia eksportu.

   Jeśli nie określono inaczej, wyeksportowany plik (*.json) zostanie zapisany w domyślnym folderze pobierania. Folder pobierania można wybrać w ustawieniach użytkownika przeglądarki internetowej.

Tworzenie nowej konfiguracji sprzętowej

Postępuj zgodnie z instrukcjami według wymogów:

- *Tworzenie nowej konfiguracji sprzętowej bez urządzeń peryferyjnych na stronie 15*
- *Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych na stronie 19*
- *Tworzenie nowej konfiguracji sprzętowej ze sterowaniem windą (AXIS A9188) na stronie 19*

Tworzenie nowej konfiguracji sprzętowej bez urządzeń peryferyjnych

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Wybierz liczbę podłączonych drzwi i kliknij przycisk **Dalej**.
4. Skonfiguruj monitory drzwi (czujniki położenia drzwi) i zamki wedle potrzeby, a następnie kliknij przycisk **Dalej**. Więcej informacji na temat dostępnych opcji: *Konfiguracja monitorów drzwi i zamków na stronie 15*.
5. Skonfiguruj używane czytniki i urządzenia REX, a następnie kliknij przycisk **Zakończ**. Więcej informacji na temat dostępnych opcji: *Konfiguracja czytników i urządzeń REX na stronie 18*.
6. Kliknij przycisk **Zamknij** lub łącze prowadzące do schematu styków sprzętu.

Konfiguracja monitorów drzwi i zamków

Po wybraniu opcji drzwi podczas nowej konfiguracji sprzętowej możesz skonfigurować monitory drzwi i zamki.

1. Jeśli będzie używany monitor drzwi, wybierz **Monitor drzwi**, a następnie wybierz opcję odpowiadającą temu, jak obwody monitora drzwi będą połączone.
2. Jeśli zamek drzwi ma być blokowany natychmiast po otwarciu drzwi, wybierz **Anuluj czas dostępu po otwarciu drzwi**.

   Jeśli chcesz opóźnić ponowne zablokowanie, ustaw wartość czasu opóźnienia w milisekundach w opcji **Czas ponownego zablokowania**.
3. Określ opcje czasu monitorowania drzwi lub jeśli żaden monitor drzwi nie będzie używany – opcje czasu zamka.
4. Wybierz opcje odpowiadające temu, jak obwody monitora drzwi będą połączone.
5. Jeśli będzie używany monitor zamka, wybierz **Monitor zamka**, a następnie wybierz opcję odpowiadającą temu, jak obwody monitora drzwi będą połączone.
6. Jeśli połączenia wejściowe z czytników, urządzeń REX i monitorów drzwi będą nadzorowane, wybierz opcję **Włącz nadzorowane wejścia**.

Więcej informacji: *Używanie nadzorowanych wejść na stronie 18*.

Uwaga

- Większość opcji blokady, monitora drzwi i czytnika można zmienić bez resetowania i uruchamiania nowej konfiguracji sprzętowej. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa**.
- Możesz połączyć jeden monitor zamka na kontroler drzwi. Jeśli więc używasz drzwi z podwójnym zamkiem, tylko jeden z zamków może mieć monitor zamka. Jeśli dwie pary drzwi są połączone z tym samym kontrolerem drzwi, nie można używać monitorów zamka.
- Mechaniczne zamki należy konfigurować jako drugie zamki.

Informacje o monitorze drzwi i opcjach ustawień czasu

Dostępne są następujące opcje dla monitora drzwi:

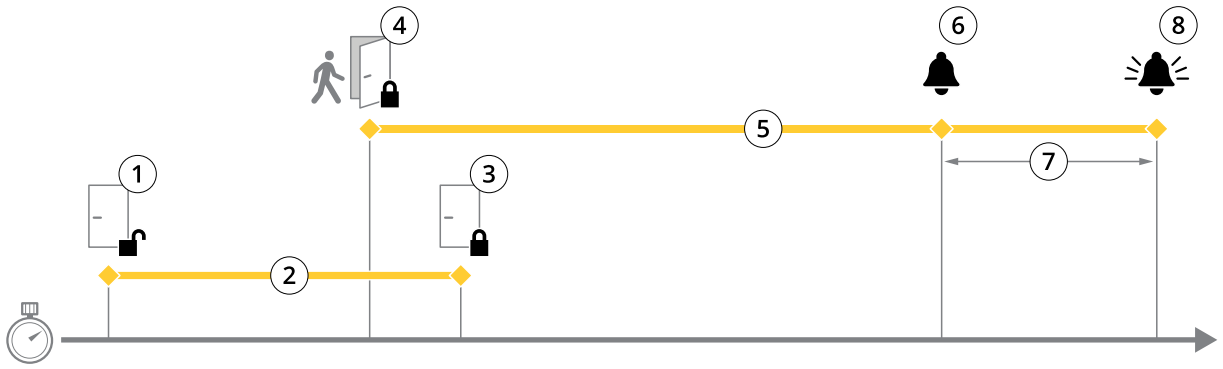
- **Monitor drzwi** – wybierany domyślnie. Każde drzwi mają własny monitor drzwi, który sygnalizuje, jeśli drzwi otworzono siłą lub jeśli zbyt długo pozostawały otwarte. Odznacz, jeśli monitor drzwi nie będzie używany.
  - **Obwód otwarty = Drzwi zablokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie otwarty. Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty.
  - **Obwód otwarty = Drzwi odblokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie zamknięty. Monitor drzwi wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor drzwi wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty.
- **Anuluj czas dostępu po otwarciu drzwi** – wybierz, aby zapobiec nieautoryzowanemu wjazdowi/wejściu. Zamek zostanie zablokowany, jak tylko monitor drzwi wskaże, że drzwi są odblokowane.

Następujące opcje ustawień czasu dla drzwi są zawsze dostępne:

- **Czas dostępu** – podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Drzwi pozostaną odblokowane do momentu ich otwarcia lub upłynięcia ustawionego czasu. Drzwi zostaną zablokowane po zamknięciu niezależnie od tego, czy czas dostępu upłynął, czy nie.
- **Długi czas dostępu** – podaj czas (w sekundach) odblokowania drzwi po uzyskaniu dostępu. Długi czas dostępu nadpisuje wcześniej ustawiony czas dostępu i zostanie włączony w przypadku użytkowników, dla których wybrano długi czas dostępu, patrz *Poświadczenia użytkowników na stronie 40*

Wybierz opcję **Monitor drzwi**, aby udostępnić następujące opcje ustawień czasu dla drzwi:

- **Otwarte zbyt długo** – podaj czas (w sekundach), przez jaki drzwi mogą być otwarte. Jeżeli po upłynięciu ustawionego czasu drzwi pozostają otwarte, wyzwalany jest alarm związany ze zbyt długim otwarciem drzwi. Ustaw regułę akcji, aby skonfigurować akcję, którą powinno wyzwolić zdarzenie zbyt długiego otwarcia drzwi.
- **Czas przed alarmem** – alarm wstępny to sygnał ostrzegawczy, wyzwalany po upłynięciu czasu ustawionego w opcji „Otwarte zbyt długo". Informuje on administratora i, w zależności od konfiguracji reguły akcji, ostrzega osobę wchodzącą przez drzwi, że drzwi należy zamknąć, aby uniknąć wyzwolenia alarmu. Podaj czas (w sekundach) przed wyzwoleniem alarmu związanego ze zbyt długim otwarciem drzwi, w którym system ma uruchomić sygnał ostrzegawczego alarmu wstępnego. Aby wyłączyć alarm wstępny, ustaw czas alarmu wstępnego jako 0.



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 *Uruchamiany jest alarm wstępny*
7 *Czas alarmu wstępnego*
8 *Otwarte zbyt długo – uruchamiany jest alarm*

Konfigurowanie reguł akcji: *Konfigurowanie reguł akcji na stronie 46*.

Informacje o opcjach zamków

Dostępne są następujące opcje obwodów zamków:

- 12 V
  - **Zabezpieczony podczas awarii** – wybierz dla zamków, które pozostają zamknięte podczas awarii zasilania. Po doprowadzeniu prądu elektrycznego zamek się otworzy.
  - **Odbezpieczony podczas awarii** – wybierz dla zamków, które pozostają otwarte podczas awarii zasilania. Po doprowadzeniu prądu elektrycznego zamek zostanie zablokowany.
- **Przekaźnik** – można go użyć tylko dla jednego zamka na kontroler drzwi. Jeśli z kontrolerem połączone są dwie pary drzwi, przekaźnika można użyć tylko dla zamka drugiej pary drzwi.
  - **Przekaźnik otwarty = Zablokowany** – wybierz dla zamków, które pozostają zamknięte przy otwartym przekaźniku (zabezpieczone podczas awarii). Po zamknięciu przekaźnika zamek się otworzy.
  - **Przekaźnik otwarty = Odblokowany** – wybierz dla zamków, które pozostają otwarte podczas awarii zasilania (odbezpieczone podczas awarii). Po zamknięciu przekaźnika zamek się zamknie.
- **Brak** – opcja dostępna tylko dla Zamka 2. Wybierz, jeśli będzie używany tylko jeden zamek.

Następujące opcje monitora zamka są dostępne dla konfiguracji z jedną parą drzwi:

- **Monitor zamka** – wybierz, aby udostępnić elementy sterowania monitorem zamka. Następnie wybierz zamek, który ma być monitorowany. Monitora zamka można używać tylko dla drzwi z podwójnym zamkiem, ale nie można go używać, jeśli dwie pary drzwi są połączone z kontrolerem drzwi.
  - **Obwód otwarty = Drzwi zablokowane** – wybierz, jeśli obwód monitora drzwi jest normalnie zamknięty. Monitor zamka wysyła sygnał odblokowanych drzwi, kiedy obwód jest zamknięty. Monitor zamka wysyła sygnał zablokowanych drzwi, kiedy obwód jest otwarty.
  - **Obwód otwarty = Odblokowany** – Wybierz, jeśli obwód monitora zamka jest normalnie otwarty. Monitor zamka wysyła sygnał odblokowanych drzwi, kiedy obwód jest otwarty. Monitor zamka wysyła sygnał zablokowanych drzwi, kiedy obwód jest zamknięty.

Konfiguracja czytników i urządzeń REX

Po przygotowaniu nowej konfiguracji sprzętowej monitorów drzwi i zamków można skonfigurować czytniki i urządzenia REX.

1. Jeżeli używany będzie czytnik, zaznacz pole wyboru i wybierz opcje pasujące do protokołu komunikacji czytnika.
2. Jeżeli używane będą takie urządzenia REX, jak przyciski, czujniki lub zamknięcia drążkowe, zaznacz pole wyboru i wybierz opcję pasującą do sposobu podłączenia obwodów urządzenia REX.

   Jeżeli sygnał REX nie wpływa na otwarcie drzwi (na przykład drzwi z mechanicznymi klamkami lub uchwytami drążkowymi), wybierz opcję **REX nie odblokowuje drzwi**.
3. Jeśli do kontrolera drzwi podłączasz więcej niż jeden czytnik/urządzenie REX, wykonaj powyższe czynności ponownie, tak aby każdy czytnik lub urządzenie REX miało poprawne ustawienia.

Informacje o opcjach czytnika i urządzenia REX

Dostępne są następujące opcje czytnika:

- **Wiegand** – wybierz dla czytników korzystających z protokołów Wiegand. Następnie wybierz kontrolkę LED obsługiwaną przez czytnik. Czytniki z pojedynczymi kontrolkami LED zwykle przełączają się między światłem czerwonym a zielonym. Czytniki z podwójnymi kontrolkami LED mają różne przewody dla czerwonych i zielonych diod LED. Oznacza to, że diody LED są sterowane niezależnie od siebie. Gdy obie diody LED są włączone, światło wydaje się pomarańczowe. Więcej informacji na temat tego, które kontrolki LED obsługuje czytnik, można znaleźć w instrukcji producenta.
- **OSDP, RS485 half duplex** – wybierz dla czytników RS485 z obsługą trybu half duplex (dwużyłowego). Więcej informacji na temat tego, które protokoły obsługuje czytnik, można znaleźć w instrukcji producenta.

Dostępne są następujące opcje urządzenia REX:

- **Aktywny niski** – wybierz, jeśli aktywacja urządzenia REX zamyka obwód.
- **Aktywny wysoki** – wybierz, jeśli aktywacja urządzenia REX otwiera obwód.
- **Sygnał REX nie odblokowuje drzwi** – wybierz, jeżeli sygnał REX nie wpływa na otwarcie drzwi (na przykład drzwi z mechanicznymi klamkami lub uchwytami drążkowymi). Jeżeli użytkownik otworzy drzwi w przewidzianym czasie dostępu, nie zostanie wyzwolony alarm „drzwi wyważone". Anuluj wybór, jeśli drzwi powinny automatycznie odblokowywać się, gdy użytkownik uruchomi urządzenie REX.

Uwaga

Większość opcji blokady, monitora drzwi i czytnika można zmienić bez resetowania i uruchamiania nowej konfiguracji sprzętowej. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa**.

Używanie nadzorowanych wejść

Nadzorowane wejścia informują o statusie połączenia między kontrolerem drzwi a czytnikami, urządzeniami REX i monitorami drzwi. Jeśli połączenie zostanie przerwane, zostanie aktywowane zdarzenie.

Aby użyć nadzorowanych wejść:

1. Zamontuj rezystory końca linii na wszystkich używanych nadzorowanych wejściach. Schemat połączeń: *strona 72*.
2. Przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa** i wybierz opcję **Włącz nadzorowane wejścia**. Możesz także włączyć nadzorowane wejścia podczas konfiguracji sprzętowej.

Informacje o zgodności wejść nadzorowanych

Następujące złącza obsługują wejścia nadzorowane:

- Złącze I/O czytnika – sygnał sabotażu. Patrz *strona 67*.
- Złącze drzwi. Patrz *strona 68*.

Czytniki i switche, których można używać z nadzorowanymi wejściami obejmują:

- Czytniki i switche z wewnętrznym napięciem1 kΩ do 5 V.
- Czytniki i przełączniki bez wewnętrznego napięcia.

Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych

1. Przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Z listy urządzeń peryferyjnych wybierz producenta bramki bezprzewodowej.
4. Jeśli chcesz podłączyć drzwi przewodowe, zaznacz pole wyboru **1 Drzwi** i kliknij przycisk **Dalej**. Jeżeli nie dołączono drzwi, kliknij przycisk **Zakończ**.
5. W zależności od producenta zamków, postępuj zgodnie z jednym z punktów:
   - **ASSA Aperio**: Kliknij łącze, aby wyświetlić schemat styków sprzętu lub kliknij przycisk **Zamknij** i przejdź do menu **Ustawienia > Ponowna konfiguracja sprzętowa**, aby zakończyć konfigurację; patrz *Dodaj drzwi i urządzenia Assa Aperio ™ na stronie 19*.
   - **SmartIntego**: Kliknij łącze, aby wyświetlić schemat styków sprzętu lub kliknij przycisk **Kliknij tutaj, aby wybrać bramkę bezprzewodową i skonfigurować drzwi**, aby zakończyć konfigurację; patrz *Informacje na temat konfiguracji SmartIntego na stronie 26*.

Dodaj drzwi i urządzenia Assa Aperio ™

Przed dodaniem drzwi bezprzewodowych do systemu należy sparować je z podłączonym koncentratorem komunikacyjnym Assa Aperio, używając narzędzia Aperio PAP (do programowania aplikacji Aperio).

Aby dodać drzwi bezprzewodowe:

1. Przejdź do menu **Ustawienia** > **Ponowna konfiguracja sprzętowa**.
2. W menu Drzwi i urządzenia bezprzewodowe kliknij opcję **Dodaj drzwi**.
3. W polu **Nazwa drzwi**: Wprowadź nazwę opisową.
4. W polu **ID** w menu **Zablokuj**: wprowadź sześcioznakowy adres urządzenia, które chcesz dodać. Adres urządzenia jest wydrukowany na etykiecie produktu.
5. Opcjonalnie w menu **Czujnik położenia drzwi**: wybierz opcję **Wbudowany czujnik położenia drzwi** lub **Czujnik położenia drzwi zewnętrznych**.

Uwaga

Jeśli korzystasz z zewnętrznego czujnika położenia drzwi (DPS), upewnij się, że urządzenie blokujące Aperio obsługuje wykrywanie stanu klamki drzwi przed jego skonfigurowaniem.

6. Opcjonalnie, w polu **ID** w menu **Czujnik położenia drzwi**: wprowadź sześcioznakowy adres urządzenia, które chcesz dodać. Adres urządzenia jest wydrukowany na etykiecie produktu.
7. Kliknij przycisk **Dodaj**.

Tworzenie nowej konfiguracji sprzętowej ze sterowaniem windą (AXIS A9188)

Ważne

Przed utworzeniem konfiguracji sprzętowej należy dodać użytkownika w module przekaźnikowym AXIS 9188 Network I/O Relay Module. Przejdź do interfejsu www A9188 > **Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika**.

Uwaga

Z każdym kontrolerem Axis Network Door Controller można połączyć maksymalnie dwa moduły przekaźnikowe AXIS 9188 Network I/O Relay Module.

1. W produkcie A1001 przejdź do menu **Ustawienia > Konfiguracja sprzętowa** i kliknij polecenie **Utwórz nową konfigurację sprzętową**.
2. Wprowadź nazwę produktu Axis.
3. Na liście urządzeń peryferyjnych wybierz **Sterowanie windą**, aby dołączyć moduł przekaźnikowy AXIS A9188 Network I/O Relay Module, a następnie kliknij przycisk **Dalej**.
4. Wprowadź nazwę podłączonego czytnika.
5. Wybierz używany protokół czytnika i kliknij przycisk **Zakończ**.
6. Kliknij opcję **Sieciowe urządzenia peryferyjne**, aby zakończyć konfigurację *Dodawanie i konfiguracja sieciowych urządzeń peryferyjnych na stronie 20*, lub kliknij łącze, aby przejść do schematu styków.

Dodawanie i konfiguracja sieciowych urządzeń peryferyjnych

Ważne

- Przed skonfigurowaniem sieciowych urządzeń peryferyjnych należy dodać użytkownika AXIS A9188 Network I/O Relay Module. Przejdź do interfejsu www AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika)**.
- Nie należy dodawać kolejnego kontrolera AXIS A1001 Network Door Controller jako sieciowego urządzenia peryferyjnego.

1. Przejdź do menu **Setup > Network Periphals (Ustawienia > Sieciowe urządzenia peryferyjne)**, aby dodać urządzenie.
2. Znajdź swoje urządzenie w obszarze **Discovered devices (Wykryte urządzenia)**.
3. Kliknij przycisk **Add this device (Dodaj to urządzenie)**.
4. Wprowadź nazwę urządzenia.
5. Wprowadź nazwę użytkownika i hasło produktu AXIS A9188.
6. Kliknij przycisk **Add (Dodaj)**.

Uwaga

Sieciowe urządzenia peryferyjne możesz dodać ręcznie, wprowadzając adres MAC lub adres IP w oknie dialogowym **Manually add device (Dodaj urządzenie ręcznie)**.

Ważne

Jeżeli chcesz usunąć harmonogram, upewnij się, że nie jest on używany przez sieciowy moduł przekaźnikowy I/O.

Konfigurowanie portów I/O oraz przekaźników w sieciowych urządzeniach peryferyjnych

Ważne

Przed skonfigurowaniem sieciowych urządzeń peryferyjnych należy dodać użytkownika AXIS A9188 Network I/O Relay Module. Przejdź do interfejsu www AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencje > Dodatkowa konfiguracja urządzenia > Ustawienia podstawowe > Użytkownicy > Dodaj > Ustawienia użytkownika)**.

1. Przejdź do menu **Setup > Network Peripherals (Ustawienia > Sieciowe urządzenia peryferyjne)** i kliknij wiersz **Added devices (Dodane urządzenia)**.
2. Wybierz porty I-O i przekaźniki do ustawienia jako piętro.

3. Kliknij przycisk **Set as floor (Ustaw jako piętro)** i wprowadź nazwę.
4. Kliknij przycisk **Add (Dodaj)**.

Piętro będzie teraz widoczne na karcie **Floor (Piętro)** w obszarze **Access Management (Zarządzanie dostępem)**.

Uwaga

W aplikacji AXIS Entry Manager można dodać maksymalnie 16 pięter.

Weryfikacja połączeń ze sprzętem

Po zakończeniu instalacji i konfiguracji sprzętu, a także w dowolnym momencie podczas eksploatacji kontrolera drzwi, można sprawdzić działanie podłączonych monitorów drzwi, sieciowych modułów przekaźnikowych I/O, zamków i czytników.

Aby zweryfikować konfigurację i przejść do elementów zarządzania weryfikacją, przejdź do menu **Ustawienia > Weryfikacja połączeń ze sprzętem**.

Zarządzanie weryfikacją drzwi

- **Status drzwi** – zweryfikuj bieżący status monitora drzwi, alarmów drzwi i zamków. Kliknij przycisk **Odczytaj bieżący status**.
- **Zablokuj** – ręcznie uruchom blokadę. Będzie to miało wpływ zarówno na zamki główne, jak i dodatkowe, jeśli są. Kliknij przycisk **Zablokuj** lub **Odblokuj**.
- **Zablokuj** – ręcznie uruchom blokadę, aby przyznać dostęp. Dotyczy to tylko zamków głównych. Kliknij opcję **Dostęp**.
- **Czytnik: informacja zwrotna** – sprawdź informacje zwrotne z czytnika, na przykład dźwięki i sygnały LED, dla różnych poleceń. Wybierz polecenie i kliknij przycisk **Testuj**. Dostępne rodzaje informacji zwrotnych zależą od czytnika. Więcej informacji: *Informacje zwrotne z czytnika na stronie 51*. Patrz także instrukcje producenta.
- **Czytnik: sabotaż** – uzyskaj informacje o ostatniej próbie ingerencji. Po zamontowaniu czytnika zostanie zarejestrowana pierwsza próba ingerencji. Kliknij opcję **Odczytaj ostatnią ingerencję**.
- **Czytnik: przeciągnięcie karty** – uzyskaj informacje na temat ostatniej przeciągniętej karty lub innego tokenu użytkownika zaakceptowanego przez czytnik. Kliknij opcję **Odczytaj ostatnie uprawnienia**.
- **REX** – uzyskaj informacje o ostatnim naciśnięciu przycisku żądania wyjścia (REX). Kliknij **Pobierz ostatni REX**.

Zarządzanie weryfikacją pięter

- **Status piętra** – zweryfikuj bieżący status dostępów do piętra. Kliknij przycisk **Odczytaj bieżący status**.
- **Blokada i odblokowanie piętra** – ręcznie wyzwalaj dostęp do piętra. Będzie to miało wpływ zarówno na zamki główne, jak i dodatkowe, jeśli są. Kliknij przycisk **Zablokuj** lub **Odblokuj**.
- **Dostęp do piętra** – ręczne udzielanie tymczasowego dostępu do piętra. Dotyczy to tylko zamków głównych. Kliknij opcję **Dostęp**.
- **Czytnik windy: informacja zwrotna** – sprawdź informacje zwrotne z czytnika, na przykład dźwięki i sygnały LED, dla różnych poleceń. Wybierz polecenie i kliknij przycisk **Testuj**. Dostępne rodzaje informacji zwrotnych zależą od czytnika. Więcej informacji: *Informacje zwrotne z czytnika na stronie 51*. Patrz także instrukcje producenta.
- **Czytnik windy: sabotaż** – uzyskaj informacje o ostatniej próbie ingerencji. Po zamontowaniu czytnika zostanie zarejestrowana pierwsza próba ingerencji. Kliknij opcję **Odczytaj ostatnią ingerencję**.
- **Czytnik windy: przeciągnięcie karty** – uzyskaj informacje na temat ostatniej przeciągniętej karty lub innego tokenu użytkownika zaakceptowanego przez czytnik. Kliknij opcję **Odczytaj ostatnie uprawnienia**.
- **REX** – uzyskaj informacje o ostatnim naciśnięciu przycisku żądania wyjścia (REX). Kliknij **Pobierz ostatni REX**.

Konfiguracja kart i formatów

Kontroler drzwi ma kilka wstępnie zdefiniowanych często stosowanych formatów kart, które można wykorzystać lub zmodyfikować według potrzeb. Można również tworzyć niestandardowe formaty kart. Każdy format karty ma inny zestaw reguł, mapy pól, sposób uporządkowania informacji przechowywanych na karcie. Dzięki zdefiniowaniu formatu karty system będzie wiedział, jak interpretować informacje, które kontroler pobiera z czytnika. Więcej informacji na temat tego, które formaty kart obsługuje czytnik, można znaleźć w instrukcji producenta.

Aby włączyć formaty kart:

1. Przejdź do menu **Ustawienia > Konfiguracja kart i formatów**.
2. Wybierz jeden lub więcej formatów kart, które pasują do formatu karty używanego przez podłączone czytniki.

Aby utworzyć nowe formaty kart:

1. Przejdź do menu **Ustawienia > Konfiguracja kart i formatów**.
2. Kliknij polecenie **Dodaj format karty**.
3. W oknie dialogowym **Dodaj format karty** wprowadź nazwę, opis i długość bitową formatu karty. Patrz *Opisy formatu karty na stronie 22*.
4. Kliknij polecenie **Dodaj mapę pola** i wprowadź wymagane informacje w polach. Patrz *Mapy pól na stronie 22*.
5. Aby dodać wiele map pól, powtórz poprzedni krok.

Aby rozwinąć element na liście **Formaty kart** i wyświetlić opisy formatów kart i mapy pól, kliknij .

Aby edytować format karty, kliknij i w razie potrzeby zmień opisy formatów kart i mapy pól. Następnie kliknij przycisk **Zapisz**.

Aby usunąć mapę pola, w oknie dialogowym **Edytuj format karty** lub **Dodaj format karty**, kliknij .

Aby usunąć format karty, kliknij .

Ważne

- Wszystkie zmiany formatów kart dotyczą całego systemu kontrolerów drzwi.
- Możesz włączać i wyłączać formaty kart tylko wtedy, gdy przynajmniej jeden kontroler drzwi w systemie został skonfigurowany z przynajmniej jednym czytnikiem. Patrz *Konfigurowanie sprzętu na stronie 14* i *Konfiguracja czytników i urządzeń REX na stronie 18*.
- Dwa formaty kart o tej samej długości bitów nie mogą być aktywne w tym samym czasie. Na przykład, jeśli zdefiniowano dwa 32-bitowe formaty kart, „Format A" i"Format B", a następnie włączono „Format A", nie można włączyć formatu „Format B" bez uprzedniego wyłączenia „Formatu A".
- Jeśli nie włączono formatów kart, do identyfikacji karty i udzielenia dostępu można użyć typów identyfikacji **Tylko dane karty** i **Tylko dane karty i PIN**. Nie jest to jednak zalecane, ponieważ różni producenci czytników lub ustawienia czytników mogą generować różne dane surowe karty.

Opisy formatu karty

- **Nazwa** (wymagana) – wprowadź nazwę opisową.
- **Opis** – wprowadź dodatkowe informacje według potrzeby. Informacje te są widoczne wyłącznie w oknach dialogowych **Edytuj format karty** i **Dodaj format karty**.
- **Liczba bitów** (wymagana) – wprowadź liczbę bitów formatu karty. Musi to być liczba pomiędzy 1 a 1 000 000 000.

Mapy pól

- **Nazwa** (wymagana) – wprowadź nazwę mapy pola bez spacji, na przykład `OddParity`.

  Przykłady często stosowanych map pól:

- `Parity` – bity parzystości są wykorzystywane do wykrywania błędów. Bity parzystości są zwykle dodawane na początku lub na końcu ciągu kodu binarnego i wskazują, czy liczba bitów jest parzysta, czy nieparzysta.
- `EvenParity` – bity parzystości zapewniają parzystą liczbę bitów w ciągu. Wliczane są bity o wartości 1. Jeśli wynik jest już parzysty, wartość bitu parzystości zostanie ustawiona na 0. Jeśli wynik jest nieparzysty, wartość bitu parzystości zostanie ustawiona na 1, co spowoduje, że całkowity wynik obliczeń będzie liczbą parzystą.
- `OddParity` – Bity nieparzyste zapewniają nieparzystą liczbę bitów w ciągu. Wliczane są bity o wartości 1. Jeśli wynik jest już nieparzysty, wartość bitu nieparzystości zostanie ustawiona na 0. Jeśli wynik jest parzysty, wartość bitu parzystości zostanie ustawiona na 1, co spowoduje, że całkowity wynik obliczeń będzie liczbą nieparzystą.
- `FacilityCode` – kody obiektu są czasem wykorzystywane w celu zweryfikowania, czy token jest zgodny z partią danych uwierzytelniających użytkownika końcowego. W starszych systemach kontroli dostępu kod obiektu był wykorzystywany do walidacji danych o obniżonej wartości, umożliwiając dostęp do danych każdego pracownika w partii danych uwierzytelniających, które zakodowano odpowiadającym kodem obiektu. Ta nazwa mapy pola, w której wielkość liter ma znaczenie, jest wymagana dla produktu, aby możliwa była walidacja kodu obiektu.
- `CrdNr` – numer karty lub ID użytkownika są najczęściej poddawane walidacji w systemach kontroli dostępu. Ta nazwa mapy pola, w której wielkość liter ma znaczenie, jest wymagana dla produktu, aby możliwa była walidacja numeru karty.
- `CardNrHex` – dane binarne numeru karty są zakodowane w produkcie w postaci liczb heksadecymalnych (małymi literami). Służą one przede wszystkim do rozwiązywania problemu w przypadku nieotrzymania oczekiwanego numeru karty z czytnika.

- **Range** (wymagane) – wprowadź zakres bitów dla mapy pola, na przykład 1, 2–17, 18–33 i 34.
- **Encoding** (wymagane) – wybierz rodzaj kodowania dla każdej mapy pola.
  - **BinLE2Int** – dane binarne są kodowane jako liczby całkowite z kolejnością bitów little endian. Liczba całkowita oznacza, że nie może to być ułamek. Kolejność bitów little endian oznacza kolejność, w której pierwszy bit jest najmniejszy (najmniej znaczący).
  - **BinBE2Int** – dane binarne są kodowane jako liczby całkowite z kolejnością bitów big endian. Liczba całkowita oznacza, że nie może to być ułamek. Kolejność bitów big endian oznacza kolejność, w której pierwszy bit jest największy (najistotniejszy).
  - **BinLE2Hex** – dane binarne są kodowane w postaci liczb heksadecymalnych (małymi literami) w kolejności little endian. System szesnastkowy, zwany również heksadecymalnym, składa się z 16 niepowtarzalnych znaków: cyfr od 0 do 9 i liter od a do f. Kolejność bitów little endian oznacza kolejność, w której pierwszy bit jest najmniejszy (najmniej znaczący).
  - **BinBE2Hex** – dane binarne są kodowane w postaci liczb heksadecymalnych (małymi literami) z kolejnością bitów big endian. System szesnastkowy, zwany również heksadecymalnym, składa się z 16 niepowtarzalnych znaków: cyfr od 0 do 9 i liter od a do f. Kolejność bitów big endian oznacza kolejność, w której pierwszy bit jest największy (najistotniejszy).
  - **BinLEIBO2Int** – dane binarne są kodowane w ten sam sposób, jak w przypadku BinLE2Int, ale dane nieprzetworzone z karty są odczytywane w odwróconej kolejności bitów w sekwencji wielobitowej przed wyodrębnieniem map pola w celu ich zakodowania.
  - **BinBEIBO2Int** – dane binarne są kodowane w podobny sposób, jak w przypadku BinBE2Int, ale dane nieprzetworzone z karty są odczytywane w odwróconej kolejności bitów w sekwencji wielobitowej przed wyodrębnieniem map pola w celu ich zakodowania.

Więcej informacji na temat tego, które mapy pól obsługuje dany format karty, można znaleźć w instrukcji producenta.

Wstępnie ustawiony kod obiektu

Kody obiektu są czasem wykorzystywane w celu zweryfikowania, czy token jest zgodny z systemem kontroli dostępu obiektu. Często wszystkie tokeny pojedynczego obiektu mają ten sam kod obiektu. Wprowadź wstępnie ustawiony kod obiektu, aby ułatwić

ręczną rejestrację partii kart. Wstępnie ustawiony kod obiektu jest automatycznie wypełniany podczas dodawania użytkowników, patrz *Poświadczenia użytkowników na stronie 40*.

Aby ustawić wstępnie ustawiony kod obiektu:

1. Przejdź do menu **Ustawienia > Konfiguracja kart i formatów**.
2. W opcji **Wstępnie ustawiony kod obiektu**: Wprowadź kod obiektu.
3. Kliknij przycisk **Ustaw kod obiektu**.

Konfiguracja usług

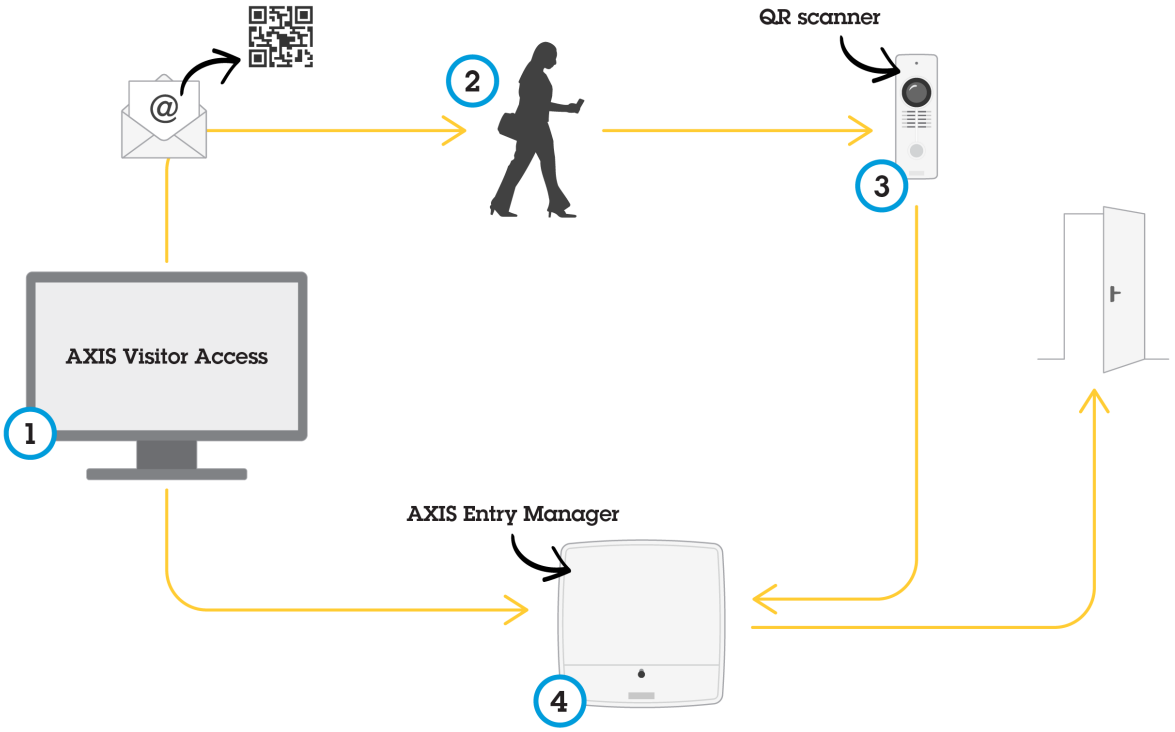
Opcja Skonfiguruj usługi na stronie Ustawienia służy do konfigurowania zewnętrznych usług dla kontrolera drzwi.

AXIS Visitor Access

Aplikacja AXIS Visitor Access umożliwia tworzenie tymczasowych poświadczeń w postaci kodu QR. Kod skanowany jest przez kamerę sieciową Axis lub wideodomofon podłączone do systemu kontroli dostępu.

Usługa składa się z:

- kontrolera drzwi Axis z aplikacją AXIS Entry Manager i oprogramowaniem sprzętowym w wersji 1.65.2 lub nowszej;
- kamery sieciowej lub wideodomofonu Axis z zainstalowaną aplikacją czytnika kodów QR;
- komputera PC z systemem Windows® i aplikacją AXIS Visitor Access.



Korzystanie z usługi AXIS Visitor Access

Konfiguracja systemu

Użytkownik tworzy zaproszenie w aplikacji AXIS Visitor Access (1) i wysyła zaproszenie na adres e-mail. Równocześnie tworzone są poświadczenia do odblokowania drzwi (przechowywane w kontrolerze drzwi Axis [4]). Goście skanują kod QR w kamerze lub wideodomofonie (3), które następnie przekazują polecenie odblokowania drzwi do kontrolera drzwi (4).

Kod QR jest zarejestrowanym znakiem towarowym Denso Wave, Inc.

Wymogi wstępne aplikacji AXIS Visitor Access

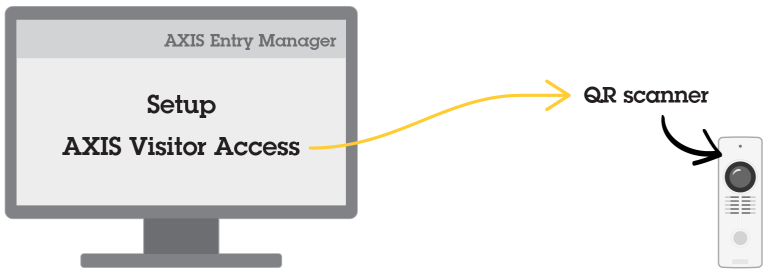
Zanim można będzie skorzystać z usługi AXIS Visitor Access, trzeba:

- skonfigurować sprzęt kontrolera drzwi;
- połączyć kamerę sieciową lub wideodomofonAxis z tą samą siecią, co kontroler drzwi, a następnie umieścić ją tak, aby mógł jej dosięgnąć odwiedzający;
- przygotować pakiet instalacyjny aplikacji AXIS Visitor Access. Pakiet można pobrać ze strony *axis.com*;
- utworzyć dwa konta użytkownika w kontrolerze drzwi, wykorzystywane tylko przez usługę AXIS Visitor Access. Jedno konto potrzebne jest do aplikacji AXIS Visitor Access, a drugie – do aplikacji czytnika kodów QR. Aby dowiedzieć się, jak utworzyć konta użytkowników, przejdź do *Użytkownicy na stronie 53*.

Ważne

- Usługi AXIS Visitor Access można użyć tylko w połączeniu z jednym kontrolerem drzwi w systemie.
- Usługa AXIS Visitor Access może być używana tylko dla drzwi z podłączonym kontrolerem. Nie można jej użyć dla innych drzwi w systemie.
- Użyj aplikacji AXIS Visitor Access do modyfikowania i usuwania odwiedzających. Nie używaj w tym celu aplikacji AXIS Entry Manager.
- Jeśli zmienisz hasło konta użytkownika aplikacji AXIS Visitor Access, musisz je również zmienić w aplikacji AXIS Visitor Access.
- Jeśli zmieniasz hasło konta użytkownika aplikacji czytnika kodów QR, musisz ponownie skonfigurować czytnik kodów QR.

Konfiguracja aplikacji AXIS Visitor Access



Aplikację QR Scanner instaluje się w kamerze sieciowej Axis lub wideodomofonie podczas konfiguracji usługi AXIS Visitor Access. Nie trzeba instalować jej oddzielnie.

1. Na stronie internetowej kontrolera drzwi przejdź do menu **Konfiguracja > Skonfiguruj usługi > Ustawienia**.
2. Kliknij przycisk **Rozpocznij nową konfigurację**.
3. Postępuj zgodnie z instrukcjami, aby przeprowadzić konfigurację.

Ważne

Jeśli chcesz wymuszać połączenie HTTPS, upewnij się, że kontroler drzwi komunikuje się z siecią za pośrednictwem protokołu HTTPS. W przeciwnym razie aplikacja nie będzie w stanie połączyć się z kontrolerem.

4. Na komputerze, który zostanie wykorzystany do tworzenia tymczasowych poświadczeń, zainstaluj i skonfiguruj aplikację AXIS Visitor Access.

SmartIntego

SmartIntego to bezprzewodowe rozwiązanie zwiększające liczbę drzwi obsługiwanych przez kontroler drzwi.

Wymogi wstępne SmartIntego

Przed konfiguracją SmartIntego należy spełnić następujące wymogi wstępne:

- Należy utworzyć plik CSV. Plik CSV zawiera informacje o tym, które opcje GatewayNode i drzwi są używane w rozwiązaniu SmartIntego. Plik zostaje utworzony w autonomicznym oprogramowaniu dostarczonym przez partnera SimonsVoss.
- Jeśli przeprowadzono konfigurację sprzętową SmartIntego: *Tworzenie nowej konfiguracji sprzętowej zamków bezprzewodowych na stronie 19*.

Uwaga

- Narzędzie do konfiguracji SmartIntego musi być w wersji 2.1.6452.23485, kompilacji 2.1.6452.23485 (8/31/2017 1:02:50 PM) lub nowszej.
- SmartIntego jest niekompatybilny z szyfrowaniem Advanced Encryption Standard (AES) i dlatego trzeba je wyłączyć w narzędziu do konfiguracji SmartIntego.

Informacje na temat konfiguracji SmartIntego

Uwaga

- Upewnij się, że spełniono podane wymogi wstępne.
- Aby stan akumulatora był lepiej widoczny, przejdź do menu **Ustawienia** > **Konfiguruj dzienniki zdarzeń i alarmów**, a następnie dodaj jako alarm opcje **Drzwi — alarm akumulatora** lub **IdPoint — alarm akumulatora**.
- Ustawienia monitorów drzwi pochodzą z zaimportowanego pliku CSV. W standardowej instalacji ustawienia tego nie trzeba zmieniać.

1. Kliknij przycisk **Przeglądaj...**, wybierz plik CSV i kliknij polecenie **Prześlij plik**.
2. Wybierz opcję GatewayNode i kliknij przycisk **Dalej**.
3. Zostanie wyświetlony podgląd nowej konfiguracji. W razie potrzeby wyłącz monitory drzwi.
4. Kliknij przycisk **Konfiguruj**.
5. Zostanie wyświetlony podgląd drzwi w konfiguracji. Kliknij opcję **Ustawienia**, aby skonfigurować każde drzwi oddzielnie.

Informacje na temat ponownej konfiguracji SmartIntego

1. W menu górnym kliknij opcję **Ustawienia**.
2. Kliknij opcję **Konfiguracja usług** > **Ustawienia**.
3. Kliknij przycisk **Konfiguruj ponownie**.
4. Kliknij przycisk **Przeglądaj...**, wybierz plik CSV i kliknij polecenie **Prześlij plik**.
5. Wybierz opcję GatewayNode i kliknij przycisk **Dalej**.
6. Zostanie wyświetlony podgląd nowej konfiguracji. W razie potrzeby wyłącz monitory drzwi.

Uwaga

Ustawienia monitorów drzwi pochodzą z zaimportowanego pliku CSV. W standardowej instalacji ustawienia tego nie trzeba zmieniać.

7. Kliknij przycisk **Konfiguruj**.
8. Zostanie wyświetlony podgląd drzwi w konfiguracji. Kliknij opcję **Ustawienia**, aby skonfigurować każde drzwi oddzielnie.

Zarządzanie sieciowymi kontrolerami drzwi

Strona Zarządzanie sieciowymi kontrolerami drzwi w systemie na stronie systemu zawiera informacje o kontrolerze drzwi, jego stanie w systemie i o tym, jakie inne kontrolery drzwi należą do systemu. Umożliwia ona również administratorowi zmianę konfiguracji systemu poprzez dodanie i usunięcie kontrolerów drzwi.

Ważne

Wszystkie kontrolery drzwi w systemie muszą być połączone z tą samą siecią i być skonfigurowane do stosowania w jednym obiekcie.

Aby zarządzać kontrolerami drzwi, przejdź do menu **Ustawienia > Zarządzaj sieciowymi kontrolerami drzwi w systemie**.

Strona Zarządzanie sieciowymi kontrolerami drzwi w systemie zawiera następujące panele:

- **Stan systemu tego kontrolera** – wyświetla stan systemu kontrolera drzwi i umożliwia przełączanie się pomiędzy trybami systemowymi i niezależnymi. Więcej informacji: *Status systemu kontrolerów drzwi na stronie 27*.
- **Sieciowe kontrolery drzwi w systemie** – wyświetla informacje o kontrolerach drzwi w systemie i obejmuje elementy sterowania umożliwiające dodawanie i usuwanie kontrolera z systemu. Więcej informacji: *Połączone kontrolery drzwi w systemie na stronie 27*.

Status systemu kontrolerów drzwi

To, czy kontroler drzwi może być częścią systemu kontrolerów, zależy od statusu systemu. Status systemu kontrolerów drzwi jest wyświetlany w panelu **Status tego kontrolera w systemie**.

Jeżeli kontroler drzwi nie pracuje w trybie autonomicznym, a chcesz zabezpieczyć go przed dodaniem do systemu, kliknij przycisk **Aktywuj tryb autonomiczny**.

Jeżeli kontroler pracuje w trybie autonomicznym, ale chcesz dodać go do systemu, kliknij przycisk **Dezaktywuj tryb autonomiczny** aby wyjść z trybu autonomicznego.

Tryby systemowe

- **Ten kontroler nie jest częścią systemu i nie jest w trybie autonomicznym** – kontroler drzwi nie został skonfigurowany jako część systemu i nie jest w trybie autonomicznym. Oznacza to, że kontroler drzwi jest otwarty i może być dodany do systemu przez dowolny inny kontroler drzwi w tej samej sieci. Aby zabezpieczyć kontroler drzwi przed dodaniem do systemu, włącz tryb autonomiczny.
- **Ten kontroler jest ustawiony w trybie autonomicznym** – kontroler drzwi nie jest częścią systemu. Nie może być dodany do systemu przez inne kontrolery drzwi w sieci ani dodawać innych kontrolerów drzwi. Tryb autonomiczny jest zwykle używany w małych układach z jednym kontrolerem drzwi i jedną lub dwiema parami drzwi. Aby umożliwić dodanie kontrolera drzwi do systemu, wyłącz tryb autonomiczny.
- **Ten kontroler jest częścią systemu** – kontroler drzwi jest częścią systemu rozproszonego. W systemie rozproszonym użytkownicy, grupy, drzwi i harmonogramy są współdzielone między podłączonymi kontrolerami.

Połączone kontrolery drzwi w systemie

Panel **Sieciowe kontrolery drzwi w systemie** zawiera elementy sterowania umożliwiające wprowadzenie następujących zmian w systemie:

- Dodawanie kontrolera drzwi do systemu, patrz *Dodawanie kontrolerów drzwi do systemu na stronie 28*.
- Usuwanie kontrolera drzwi z systemu, patrz *Usuwanie kontrolerów drzwi z systemu na stronie 29*.

Lista podłączonych kontrolerów drzwi

Panel **Sieciowe kontrolery drzwi w systemie** zawiera również listę z podanymi poniżej informacjami dotyczącymi identyfikatorów i statusu kontrolerów drzwi w systemie:

- **Nazwa** – zdefiniowana przez użytkownika nazwa kontrolera drzwi. Jeśli administrator nie ustawił nazwy podczas konfiguracji sprzętu, zostanie wyświetlona nazwa domyślna.
- **Adres IP**
- **Adres MAC**
- **Status** – kontroler drzwi, z którego uzyskujesz dostęp do systemu, ma status **Ten kontroler**. Pozostałe kontrolery drzwi w systemie mają status **Online**.
- **Wersja oprogramowania sprzętowego**

Aby otworzyć strony internetowe innego kontrolera drzwi, kliknij adres IP kontrolera.

Aby zaktualizować listę, kliknij polecenie **Odśwież listę kontrolerów**.

Uwaga

Wszystkie kontrolery w systemie zawsze muszą mieć tę samą wersję oprogramowania sprzętowego. Użyj aplikacji Axis Device Manager, aby jednocześnie zaktualizować oprogramowanie sprzętowe we wszystkich kontrolerach w całym systemie.

Dodawanie kontrolerów drzwi do systemu

Ważne

Podczas parowania kontrolerów drzwi wszystkie ustawienia zarządzania dostępem dla dodanego kontrolera drzwi zostaną skasowane i nadpisane ustawieniami zarządzania dostępem systemu.

Aby dodać do systemu kontroler drzwi z listy kontrolerów drzwi:

1. Przejdź do menu **Ustawienia > Zarządzaj sieciowymi kontrolerami drzwi w systemie**.
2. Kliknij polecenie **Dodaj kontrolery z listy do systemu**.
3. Wybierz kontroler drzwi, który chcesz dodać.
4. Kliknij przycisk **Dodaj**.
5. Aby dodać więcej kontrolerów drzwi, powtórz powyższe kroki.

Aby dodać kontroler drzwi do systemu z wykorzystaniem znanego adresu IP lub MAC:

1. Przejdź do opcji **Zarządzaj urządzeniami**.
2. Kliknij polecenie **Dodaj kontroler do systemu, podając adres MAC lub IP**.
3. Wprowadź adres IP lub MAC.
4. Kliknij przycisk **Dodaj**.
5. Aby dodać więcej kontrolerów drzwi, powtórz powyższe kroki.

Po zakończeniu parowania wszyscy użytkownicy, drzwi, harmonogramy i grupy będą współdzieleni przez wszystkie kontrolery drzwi w systemie.

Aby zaktualizować listę, kliknij polecenie **Odśwież listę kontrolerów**.

Usuwanie kontrolerów drzwi z systemu

Ważne

- Przed usunięciem kontrolera drzwi z systemu zresetuj jego konfigurację sprzętową. Jeśli pominiesz ten krok, wszystkie drzwi powiązane z usuniętym kontrolerem drzwi pozostaną w systemie i nie można będzie ich usunąć.
- Po usunięciu kontrolera drzwi z systemu z dwoma kontrolerami oba kontrolery automatycznie przełączą się w tryb autonomiczny.

Aby usunąć kontroler drzwi z systemu:

1. Uzyskaj dostęp do systemu za pośrednictwem kontrolera drzwi, który chcesz usunąć i przejdź do menu **Ustawienia > Konfiguracja sprzętowa**.
2. Kliknij polecenie **Resetuj konfigurację sprzętową**.
3. Po zresetowaniu konfiguracji sprzętowej przejdź do menu **Ustawienia > Zarządzaj sieciowymi kontrolerami drzwi w systemie**.
4. Na liście **Sieciowe kontrolery drzwi w systemie** znajdź kontroler drzwi, który chcesz usunąć i kliknij polecenie **Usuń z systemu**.
5. Zostanie otwarte okno dialogowe przypominające o konieczności zresetowania konfiguracji sprzętowej kontrolera drzwi. Kliknij polecenie **Usuń kontroler**, aby potwierdzić.
6. Zostanie otwarte okno dialogowe z informacją o konieczności potwierdzenia zamiaru usunięcia kontrolera drzwi. Kliknij przycisk **OK**, aby potwierdzić. Usunięty kontroler drzwi znajduje się obecnie w trybie autonomicznym.

Uwaga

- Po usunięciu kontrolera drzwi z systemu wszystkie jego ustawienia zarządzania dostępem zostaną wykasowane.
- Można usunąć tylko kontrolery drzwi dostępne online.

Tryb konfiguracji

Tryb konfiguracji to standardowy tryb używany podczas pierwszego dostępu do urządzenia. Po wyłączeniu trybu konfiguracji większość funkcji konfiguracji urządzenia zostanie ukryta.

Ważne

Wyłączenie trybu konfiguracji nie służy do zwiększania bezpieczeństwa. Ma to na celu zapobieganie błędom podczas konfiguracji, ale nie powstrzyma od złośliwej zmiany ważnych ustawień.

Wyłączanie trybu konfiguracji

1. Przejdź do menu **Ustawienia** > **Wyłącz tryb konfiguracji**.
2. Wprowadź kod PIN i naciśnij przycisk **OK**.

Uwaga

Kod PIN nie jest wymagany.

Włączanie trybu konfiguracji

1. Przejdź do menu **Ustawienia** > **Włącz tryb konfiguracji**.
2. Wprowadź PIN i naciśnij przycisk **OK**.

Uwaga

Jeżeli nie pamiętasz numeru PIN, możesz włączyć tryb konfiguracji na stronie `http://[adres IP]/webapp/pacs/index.shtml#resetConfigurationMode`.

Instrukcje konserwacji

Aby system kontroli dostępu działał poprawnie, firma Axis zaleca regularną konserwację systemu, w tym kontrolerów drzwi i podłączonych urządzeń.

Konserwację należy przeprowadzać przynajmniej raz w roku. Sugerowana procedura konserwacji obejmuje, ale nie ogranicza się do następujących kroków:

- Upewnij się, że wszystkie połączenia między kontrolerem drzwi a urządzeniami zewnętrznymi są zabezpieczone.
- Sprawdź wszystkie połączenia sprzętowe. Patrz *Zarządzanie weryfikacją drzwi na stronie 21*.
- Sprawdź, czy system, w tym podłączone urządzenia zewnętrzne, działa poprawnie.
    - Przeciągnij kartę i przetestuj czytniki, drzwi i zamki.
    - Jeśli system zawiera urządzenia REX, czujniki lub inne urządzenia, również należy je przetestować.
    - Jeśli alarm przeciwsabotażowy jest włączony, sprawdź go.

Jeśli w wyniku powyższych sprawdzeń stwierdzona zostanie awaria lub nieprzewidziane zachowanie:

- Sprawdź sygnały przewodów za pomocą odpowiedniego sprzętu i sprawdź, czy przewody lub kable nie są w jakikolwiek sposób uszkodzone.
- Wymień wszystkie uszkodzone lub wadliwe kable i przewody.
- Po wymianie kabli i przewodów sprawdź ponownie wszystkie połączenia sprzętowe. Patrz *Zarządzanie weryfikacją drzwi na stronie 21*.

- Upewnij się, że wszystkie harmonogramy dostępu, drzwi, grupy i użytkownicy są aktualne.
- Jeśli kontroler drzwi nie działa zgodnie z oczekiwaniami, więcej informacji możesz znaleźć w *Rozwiązywanie problemów na stronie 64* i *Konserwacja na stronie 61*.

Zarządzanie dostępem

Informacje o użytkownikach

W aplikacji AXIS Entry Manager użytkownicy to osoby, które zarejestrowano jako właścicieli jednego lub więcej tokenów (typów identyfikacji). Każda osoba musi mieć własny profil użytkownika, aby uzyskać dostęp do drzwi w systemie kontroli dostępu. Profil użytkownika składa się z poświadczeń, które informują system o tożsamości użytkownika i o tym, kiedy i w jaki sposób użytkownik może uzyskać dostęp do drzwi. Więcej informacji: *Tworzenie i edytowanie użytkowników na stronie 39*.

Użytkowników w tym kontekście nie można mylić z administratorami. Administratorzy mają nieograniczony dostęp do wszystkich ustawień. W kontekście zarządzania systemem kontroli dostępu i stronami WWW produktu (AXIS Entry Manager) administratorzy są czasami określani nazwą użytkownicy. Więcej informacji: *Użytkownicy na stronie 53*.

Strona zarządzania dostępem

Strona zarządzania dostępem umożliwia konfigurację i zarządzanie użytkownikami, grupami, drzwiami i harmonogramami w systemie. Aby otworzyć stronę zarządzania dostępem, kliknij przycisk **Zarządzanie dostępem**.

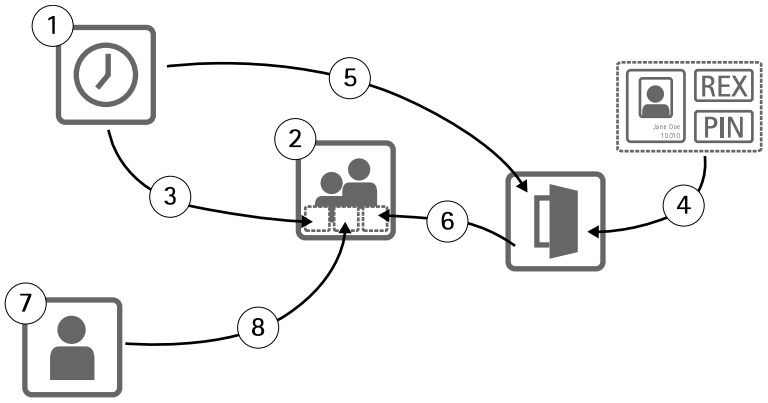
Aby dodać użytkowników do grup i zastosować harmonogramy dostępu i dodać drzwi, przeciągnij odpowiednie elementy w odpowiednie miejsca na listach **Grupy** i **Drzwi**.

Uwaga

Komunikaty, które wymagają działania, są wyświetlane na czerwono.

Wybór przepływu pracy

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



1. Utwórz harmonogramy dostępu. Patrz *strona 32*.
2. Utwórz grupy. Patrz *strona 34*.
3. Zastosuj harmonogramy dostępu do grup.
4. Dodaj typy identyfikacji do drzwi lub pięter. Patrz *strona 34* i *strona 35*.
5. Zastosuj harmonogramy dostępu do każdego typu identyfikacji.
6. Zastosuj drzwi lub piętra do grup.
7. Utwórz użytkowników. Patrz *strona 39*.

8. Dodaj użytkowników do grup.

Stosowane przykłady tego przepływu pracy: *Przykładowe kombinacje harmonogramów dostępu na stronie 42*.

Tworzenie i edytowanie harmonogramów dostępu

Harmonogramy dostępu są wykorzystywane w celu zdefiniowania ogólnych reguł dostępu do drzwi. Są one również używane do definiowania reguł dostępu do drzwi w systemie przez grupy. Więcej informacji: *Typy harmonogramów dostępu na stronie 32*.

Aby utworzyć nowy harmonogram dostępu:

1. Przejdź do opcji **Zarządzanie dostępem**.
2. Na karcie **Harmonogramy dostępu** kliknij polecenie **Dodaj nowy harmonogram**.
3. W oknie dialogowym **Dodaj harmonogram dostępu** wprowadź nazwę harmonogramu.
4. Aby utworzyć harmonogram regularnego dostępu, wybierz opcję **Harmonogram dodawania**.

   Aby utworzyć harmonogram odejmowania, wybierz opcję **Harmonogram odejmowania**.

   Więcej informacji: *Typy harmonogramów dostępu na stronie 32*.
5. Kliknij przycisk **Zapisz**.

Aby rozwinąć element na liście **Harmonogramy dostępu**, kliknij . Harmonogramy dodawania są zaznaczone zieloną czcionką, a harmonogramy odejmowania – ciemnoczerwoną.

Aby przejrzeć kalendarz harmonogramu dostępu, kliknij .

Aby edytować nazwę harmonogramu dostępu lub element dostępu, kliknij i wprowadź zmiany. Następnie kliknij przycisk **Zapisz**.

Aby usunąć harmonogram dostępu, kliknij .

Uwaga

Kontroler drzwi ma kilka wstępnie zdefiniowanych często stosowanych harmonogramów dostępu, które można wykorzystać jako przykłady lub zmodyfikować według potrzeb. Jednak wstępnie zdefiniowanego harmonogramu dostępu **Zawsze** nie można zmodyfikować ani usunąć.

Typy harmonogramów dostępu

Istnieją dwa rodzaje harmonogramów dostępu:

- **Harmonogram dodawania** - regularne harmonogramy dostępu określające, kiedy drzwi są dostępne. Typowe harmonogramy dodawania to godziny pracy, godziny otwarcia, po godzinach pracy lub godziny nocne.
- **Harmonogram odejmowania** – wyjątki od zwykłych harmonogramów dostępu. Są one zwykle używane do ograniczania dostępu w określonym przedziale czasowym w regularnym harmonogramie (harmonogram dodawania). Harmonogramy odejmowania mogą być używane do odmowy użytkownikom dostępu do budynku podczas wolnego w dni powszednie.

Oba typy harmonogramów dostępu mogą być używane na dwóch poziomach:

- **Harmonogramy typów identyfikacji** – określ, kiedy i jak czytniki mają przyznawać użytkownikom dostęp do drzwi. Każdy typ identyfikacji musi być połączony z harmonogramem dostępu, który informuje system, kiedy udzielić użytkownikom z tym konkretnym typem identyfikacji dostępu. Do każdego typu identyfikacji można dodać wiele harmonogramów dodawania i odejmowania. Informacje na temat typów identyfikacji: *strona 35*.
- **Harmonogramy grup** – określ, kiedy (ale nie w jaki sposób) członkowie grupy mają uzyskać dostęp do drzwi. Każda grupa musi być połączona z jednym lub kilkoma harmonogramami dostępu, które informują system, kiedy przyznać dostęp użytkownikom. Do każdej grupy można dodać wiele harmonogramów dodawania i harmonogramów odejmowania. Informacje o grupach: *strona 34*.

Harmonogramy grup mogą ograniczać uprawnienia dostępu, ale nie rozszerzają praw dostępu do wejść i wyjść poza uprawnienia harmonogramów typów identyfikacji. Innymi słowy, jeśli harmonogram typu identyfikacji ogranicza dostęp do wejścia lub wyjścia w określonych momentach, harmonogram grupy nie może nadpisać harmonogramu typu identyfikacji. Jeśli jednak harmonogram grup jest bardziej restrykcyjny niż harmonogram typu identyfikacji, harmonogram grupy nadpisze harmonogram typu identyfikacji.

Harmonogramy typów identyfikacji i harmonogramy grup można łączyć na kilka sposobów w celu uzyskania różnych wyników. Przykładowe kombinacje harmonogramów dostępu: *strona 42*.

Dodawanie elementów harmonogramu

Zarówno harmonogramy dodawania, jak i harmonogramy odejmowania, mogą być jednorazowymi (pojedynczymi) lub powtarzalnymi zdarzeniami.

Dodawanie elementu harmonogramu do harmonogramu dostępu:

1. Rozwiń harmonogram dostępu na liście **Harmonogramy dostępu**.
2. Kliknij polecenie **Dodaj element harmonogramu**.
3. Wprowadź nazwę elementu harmonogramu.
4. Wybierz opcję **Jednorazowo** lub **Cyklicznie**.
5. Wprowadź czas trwania w polach czasu. Patrz *Opcje czasu na stronie 33*.
6. Dla cyklicznych zdarzeń harmonogramu wybierz parametry **Wzorzec powtarzania** i **Zakres powtarzania**. Patrz *Opcje wzorca powtórzeń na stronie 33* i *Opcje zakresu powtarzania na stronie 33*.
7. Kliknij przycisk **Zapisz**.

Opcje czasu

Dostępne są następujące opcje czasu:

- **Cały dzień** – wybierz w przypadku zdarzeń trwających 24 godziny w ciągu doby. Następnie wprowadź żądaną datę **początku**.
- **Początek** – kliknij pole czasu i wybierz żądaną godzinę. W razie potrzeby kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.
- **Koniec** – kliknij pole czasu i wybierz żądaną godzinę. W razie potrzeby kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.

Opcje wzorca powtórzeń

Dostępne są następujące opcje wzorca powtórzeń:

- **Co rok** – wybierz tę opcję, aby powtarzać zdarzenie co rok.
- **Co tydzień** – wybierz tę opcję, aby powtarzać zdarzenie co tydzień.
- Co tydzień w **poniedziałek**, **wtorek**, **środę**, **czwartek**, **piątek**, **sobotę**, i **niedzielę** – wybierz dni, w które ma być powtarzane zdarzenie.

Opcje zakresu powtarzania

Dostępne są następujące opcje zakresu powtarzania:

- **Pierwsze wystąpienie** – kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.
- **Brak daty zakończenia** – wybierz tę opcję, aby powtarzać wystąpienie bezterminowo.

- **Koniec przed** – kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.

Tworzenie i edytowanie grup

Grupy pozwalają zarządzać użytkownikami i ich prawami dostępu zbiorowo i skutecznie. Grupa obejmuje poświadczenia, które informują system, z których użytkowników składa się grupa, oraz kiedy i w jaki sposób członkowie grupy mają dostęp do drzwi.

Każdy użytkownik musi należeć do co najmniej jednej grupy. Aby dodać użytkownika do grupy, przeciągnij i upuść użytkownika do żądanej grupy na liście **Grupy**. Więcej informacji: *Tworzenie i edytowanie użytkowników na stronie 39*.

Tworzenie nowej grupy:

1. Przejdź do opcji **Zarządzanie dostępem**.
2. Na karcie **Grupy** kliknij **Dodaj nową grupę**.
3. W oknie dialogowym **Dodaj grupę** wprowadź poświadczenia grupy. Patrz *Poświadczenia grupy na stronie 34*.
4. Kliknij przycisk **Zapisz**.

Aby rozwinąć pozycję na liście **Grupy** i wyświetlić jej członków, prawa dostępu do drzwi i harmonogramy, kliknij przycisk .

Aby edytować nazwę grupy lub datę ważności, kliknij przycisk i wprowadź zmiany. Następnie kliknij przycisk **Zapisz**.

Aby sprawdzić, kiedy i jak grupa może uzyskać dostęp do niektórych drzwi, kliknij .

Aby usunąć grupę lub członków grupy, drzwi lub harmonogramy z grupy, kliknij .

Poświadczenia grupy

Dla grup dostępne są następujące rodzaje poświadczeń:

- **Nazwa** (wymagana)
- **Ważny od** i **Ważny do** – wprowadź daty ważności poświadczeń grupy. Kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.
- **Biała lista** – użytkownicy w grupie białej listy zawsze mają dostęp do drzwi w grupie, nawet w przypadku awarii sieci lub zasilania. Ponieważ użytkownicy w grupie zawsze mają dostęp do drzwi, harmonogramy ani daty ważności nie mają zastosowania. Opcja Długi czas dostępu nie jest obsługiwana dla użytkownika, który otwiera drzwi w grupie białej listy. Tylko drzwi z zamkami bezprzewodowymi obsługującymi funkcję białej listy mogą być dodawane do grupy.

Uwaga

- Aby móc zapisać grupę, musisz wprowadzić **nazwę** grupy.
- Daty ważności dla użytkownika nie maja zastosowania przy dodawaniu użytkownika do grupy białej listy.
- Synchronizacja białych list uwierzytelniających z blokadą bezprzewodową zajmuje trochę czasu i zakłóca zwykłe procedury otwierania drzwi. Unikaj dodawania lub usuwania dużej liczby poświadczeń w systemie w godzinach szczytu. Po zakończeniu synchronizacji zaktualizowanych poświadczeń z blokadą w dzienniku zdarzeń zostanie wyświetlone polecenie `SyncOngoing: fałsz` dla zamka.

Zarządzanie drzwiami

Ogólnymi regułami dotyczącymi poszczególnych drzwi można zarządzać na karcie **Drzwi**. Reguły obejmują dodawanie typów identyfikacji, które określają, w jaki sposób użytkownicy będą mieli dostęp do drzwi, i harmonogramy dostępu, które określają, kiedy dany typ identyfikacji jest ważny. Więcej informacji: *Typy identyfikacji na stronie 35* i *Tworzenie i edytowanie harmonogramów dostępu na stronie 32*.

Aby zarządzać drzwiami, trzeba je dodać do systemu kontroli dostępu, przeprowadzając procedurę konfiguracji sprzętowej; patrz *Konfigurowanie sprzętu na stronie 14*.

Zarządzanie dostępem

Zarządzanie drzwiami:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Drzwi**.
2. Na liście **Drzwi** kliknij obok tych drzwi, które chcesz edytować.
3. Przeciągnij drzwi do co najmniej jednej grupy. Jeśli lista **Grupy** jest pusta, utwórz nową grupę. Patrz *Tworzenie i edytowanie grup na stronie 34*.
4. Kliknij polecenie **Dodaj typ identyfikacji** i wybierz, które poświadczenia użytkownicy muszą wprowadzić do czytnika, aby uzyskać dostęp do drzwi. Patrz *Typy identyfikacji na stronie 35*.

   Dodaj co najmniej jeden typ identyfikacji do każdych drzwi.
5. Aby dodać wiele typów identyfikacji, powtórz poprzedni krok.

   Jeśli dodano oba typy identyfikacji **Tylko numer karty** i **Tylko PIN**, użytkownicy mogą albo przeciągnąć kartę, albo wprowadzić numer PIN, aby uzyskać dostęp do drzwi. Jeśli jednak dodano tylko typ identyfikacji **Numer karty i PIN**, użytkownicy muszą przeciągnąć kartę i wprowadzić kod PIN, aby uzyskać dostęp do drzwi.
6. Aby określić, kiedy poświadczenia są ważne, przeciągnij harmonogram do każdego typu identyfikacji.

Aby ręcznie odblokować lub zablokować drzwi albo zezwolić na tymczasowy dostęp, kliknij jedną z ręcznych akcji związanych z drzwiami. Patrz *Używanie ręcznej obsługi drzwi na stronie 36*.

Uwaga

Dla drzwi/urządzeń bezprzewodowych nie ma możliwości ręcznego odblokowywania lub zablokowywania drzwi albo udzielania dostępu.

Aby rozwinąć element na liście **Drzwi**, kliknij .

Aby edytować nazwę drzwi lub czytnika, kliknij i wprowadź zmiany. Następnie kliknij przycisk **Zapisz**.

Aby zweryfikować czytnik, typ identyfikacji i kombinacje harmonogramów dostępu, kliknij .

Aby zweryfikować działanie zamków podłączonych do drzwi, kliknij elementy sterowania procesem weryfikacji. Patrz *Zarządzanie weryfikacją drzwi na stronie 21*.

Aby usunąć typy identyfikacji lub harmonogramy dostępu, kliknij .

Typy identyfikacji

Typy identyfikacji to przenośne urządzenia do przechowywania poświadczeń, fragmenty zapamiętanych informacji lub różne ich połączenia, które określają, w jaki sposób użytkownicy uzyskają dostęp do drzwi. Typowe typy identyfikacji obejmują tokeny, takie jak karty lub breloczki, osobiste numery identyfikacyjne (PIN) i urządzenia Request to Exit (REX).

Więcej informacji dotyczących poświadczeń: *Poświadczenia użytkowników na stronie 40*.

Dostępne są następujące typy identyfikacji:

- **Tylko kod obiektu** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik.
- **Tylko numer karty** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik. Numer karty jest unikalnym numerem zazwyczaj nadrukowanym na karcie. Informacje o lokalizacji numeru karty podaje producent. Numer karty można również pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**.
- **Tylko dane karty** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik. Informacje są przechowywane jako surowe dane na karcie. Surowe dane na karcie można

pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**. Tego typu identyfikacji używaj tylko wtedy, gdy nie można znaleźć numeru karty.

- **Tylko PIN** – użytkownik może uzyskać dostęp do drzwi za pomocą czterocyfrowego numeru PIN.
- **Kod obiektu i PIN** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu z kodem obiektu wraz z numerem PIN akceptowanym przez czytnik. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).
- **Numer karty i PIN** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu wraz z numerem PIN akceptowanym przez czytnik. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).
- **Tylko dane karty i PIN** – użytkownik może uzyskać dostęp do drzwi za pomocą karty lub innego tokenu wraz z numerem PIN akceptowanym przez czytnik. Tego typu identyfikacji używaj tylko wtedy, gdy nie można znaleźć numeru karty. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).
- **REX** – użytkownik może uzyskać dostęp do drzwi, aktywując urządzenie REX, takie jak przycisk, czujnik lub zamknięcie drążkowe.
- **Tylko tablica rejestracyjna** – użytkownik może uzyskać dostęp do drzwi tylko za pomocą numeru tablicy rejestracyjnej pojazdu.

Dodawanie stanów zaplanowanego odblokowania

Aby automatycznie pozostawić drzwi odblokowane na określony czas, możesz dodać stan **Zaplanowanego odblokowania** do drzwi oraz zastosować harmonogram dostępu.

Na przykład, aby drzwi pozostawały odblokowane w godzinach pracy biura:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Drzwi**.
2. Kliknij ▶ obok elementu na liście **Drzwi**, który chcesz edytować.
3. Kliknij polecenie **Dodaj zaplanowane odblokowanie**.
4. Wybierz **Stan odblokowania** (**odblokowane** lub **odblokuj oba zamki**, w zależności do tego, czy drzwi mają jeden zamek, czy dwa).
5. Kliknij przycisk **OK**.
6. Zastosuj wstępnie zdefiniowany harmonogram dostępu **Godziny pracy** do stanu **Zaplanowane odblokowanie**.

Aby zweryfikować, kiedy drzwi będą odblokowane, kliknij .

Aby usunąć stan zaplanowanego odblokowania lub harmonogram dostępu, kliknij .

Używanie ręcznej obsługi drzwi

Drzwi można odblokować lub zablokować, a tymczasowego dostępu można udzielić, przechodząc do karty **Drzwi** i wybierając opcję **Ręczna obsługa drzwi**. To, które działania w ramach ręcznej obsługi drzwi są dostępne dla określonych drzwi, zależy od przeprowadzonej konfiguracji drzwi.

Aby skorzystać z ręcznej obsługi drzwi:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Drzwi**.
2. Na liście **Drzwi** kliknij ▶ obok tych drzwi, które chcesz kontrolować.
3. Kliknij wymaganą akcję drzwi. Patrz *Ręczna obsługa drzwi na stronie 37*.

Uwaga

Aby skorzystać z ręcznej obsługi drzwi, trzeba otworzyć stronę Zarządzanie dostępem za pośrednictwem tego kontrolera drzwi, do którego są podłączone konkretne drzwi. Jeśli otworzysz stronę Zarządzanie dostępem za pośrednictwem innego kontrolera drzwi, zamiast ręcznej obsługi drzwi pojawi się łącze do strony Informacje ogólne tego kontrolera drzwi, do którego są podłączone konkretne drzwi. Kliknij łącze, przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Drzwi**.

Ręczna obsługa drzwi

Dostępne są następujące działania:

- **Odczytaj status drzwi** – zweryfikuj bieżący status monitora drzwi, alarmów drzwi i zamków.
- **Dostęp** – opcja ta umożliwia udzielenie użytkownikom dostępu do drzwi. Stosowane jest ograniczenie czasu dostępu. Patrz *Konfiguracja monitorów drzwi i zamków na stronie 15*.
- **Odblokuj** (jeden zamek) lub **Odblokuj oba zamki** (dwa zamki) – wybierz, aby odblokować drzwi. Drzwi pozostają odblokowane do momentu naciśnięcia przycisku **Zablokuj** lub **Zablokuj oba zamki**, aktywacji zaplanowanego statusu drzwi lub zrestartowania kontrolera drzwi.
- **Zablokuj** (jeden zamek) lub **Zablokuj oba zamki** (dwa zamki) – wybierz, aby zablokować drzwi.
- **Odblokuj drugi zamek i zablokuj zamek główny** – ta opcja jest dostępna tylko wtedy, gdy drzwi skonfigurowano z drugim zamkiem. Odblokuj drzwi. Drugi zamek pozostaje odblokowany do momentu naciśnięcia **Oba zamki zablokowane** lub aktywacji zaplanowanego statusu drzwi.

Zarządzanie piętrami

Jeśli zainstalowano moduł przekaźnikowy AXIS 9188 Network I/O Relay Module, możesz zarządzać piętrami w podobny sposób, w jaki zarządza się drzwiami.

Uwaga

Jeśli używasz A1001 w trybie klastra z włączonymi zdarzeniami globalnymi, upewnij się, że używasz unikalnych opisowych nazw dla każdego piętra. Na przykład *„Winda A, Piętro 1"*.

Uwaga

Z każdym kontrolerem A1001 Network Door Controller można połączyć maksymalnie dwa moduły przekaźnikowe AXIS 9188 Network I/O Relay Module.

Ogólnymi regułami dla każdego piętra zarządza się na karcie **Piętra**. Reguły obejmują dodawanie typów identyfikacji, które określają, w jaki sposób użytkownicy będą mieli dostęp do pięter, i harmonogramy dostępu, które określają, kiedy dany typ identyfikacji jest ważny. Więcej informacji: *Typy identyfikacji pięter na stronie 38* i *Tworzenie i edytowanie harmonogramów dostępu na stronie 32*.

Aby zarządzać piętrem, trzeba je dodać do systemu kontroli dostępu, przeprowadzając procedurę konfiguracji sprzętowej; patrz *Konfigurowanie sprzętu na stronie 14*.

Zarządzanie piętrem:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Piętra**.
2. Na liście **Piętra** kliknij ▶ obok tego piętra, które chcesz edytować.
3. Przeciągnij piętro do co najmniej jednej grupy. Jeśli lista **Grupy** jest pusta, utwórz nową grupę. Patrz *Tworzenie i edytowanie grup na stronie 34*.
4. Kliknij polecenie **Dodaj typ identyfikacji** i wybierz, które poświadczenia użytkownicy muszą wprowadzić do czytnika, aby uzyskać dostęp do piętra. Patrz *Typy identyfikacji pięter na stronie 38*.

   Dodaj co najmniej jeden typ identyfikacji do każdego piętra.
5. Aby dodać wiele typów identyfikacji, powtórz poprzedni krok.

Jeśli dodano oba typy identyfikacji **Tylko numer karty** i **Tylko PIN**, użytkownicy mogą albo przeciągnąć kartę, albo wprowadzić numer PIN, aby uzyskać dostęp do drzwi. Jeśli jednak dodano tylko typ identyfikacji **Numer karty i PIN**, użytkownicy muszą przeciągnąć kartę i wprowadzić kod PIN, aby uzyskać dostęp do drzwi.

6. Aby określić, kiedy poświadczenia są ważne, przeciągnij harmonogram do każdego typu identyfikacji.

Aby ręcznie odblokować lub zablokować piętra albo zezwolić na tymczasowy dostęp, kliknij jedną z ręcznych akcji związanych z drzwiami. Patrz *Używanie ręcznej obsługi pięter na stronie 39*.

Uwaga

Dla drzwi/urządzeń bezprzewodowych nie ma możliwości ręcznego odblokowywania lub zablokowywania drzwi albo udzielania dostępu.

Aby rozwinąć element na liście **Piętra**, kliknij .

Aby edytować nazwę piętra lub czytnika, kliknij i wprowadź zmiany. Następnie kliknij przycisk **Zapisz**.

Aby zweryfikować czytnik, typ identyfikacji i kombinacje harmonogramów dostępu, kliknij .

Aby zweryfikować działanie zamków połączonych z piętrami, kliknij elementy sterowania procesem weryfikacji. Patrz *Zarządzanie weryfikacją pięter na stronie 21*.

Aby usunąć typy identyfikacji lub harmonogramy dostępu, kliknij .

Typy identyfikacji pięter

Typy identyfikacji to przenośne urządzenia do przechowywania poświadczeń, fragmenty zapamiętanych informacji lub różne ich połączenia, które określają, w jaki sposób użytkownicy uzyskają dostęp do pięter. Typowe typy identyfikacji obejmują tokeny, takie jak karty lub breloczki, osobiste numery identyfikacyjne (PIN) i urządzenia Request to Exit (REX).

Więcej informacji dotyczących poświadczeń: *Poświadczenia użytkowników na stronie 40*.

Dostępne są następujące typy identyfikacji:

- **Tylko kod obiektu** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik.
- **Tylko numer karty** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik. Numer karty jest unikalnym numerem zazwyczaj nadrukowanym na karcie. Informacje o lokalizacji numeru karty podaje producent. Numer karty można również pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**.
- **Tylko dane karty** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu z kodem obiektu akceptowanym przez czytnik. Informacje są przechowywane jako surowe dane na karcie. Surowe dane na karcie można pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**. Tego typu identyfikacji używaj tylko wtedy, gdy nie można znaleźć numeru karty.
- **Tylko PIN** – użytkownik może uzyskać dostęp do piętra za pomocą czterocyfrowego numeru PIN.
- **Kod obiektu i PIN** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu z kodem obiektu wraz z numerem PIN akceptowanym przez czytnik. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).
- **Numer karty i PIN** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu wraz z numerem PIN akceptowanym przez czytnik. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).
- **Tylko dane karty i PIN** – użytkownik może uzyskać dostęp do piętra za pomocą karty lub innego tokenu wraz z numerem PIN akceptowanym przez czytnik. Tego typu identyfikacji używaj tylko wtedy, gdy nie można znaleźć numeru karty. Użytkownik musi przedstawić poświadczenia w określonej kolejności (najpierw karta, potem PIN).

- **REX** – użytkownik może uzyskać dostęp do piętra, aktywując urządzenie REX, takie jak przycisk, czujnik lub zamknięcie drążkowe.

Dodawanie stanów zaplanowanego odblokowania

Aby automatycznie ustawić piętro jako dostępne dla wszystkich osób w konkretnych godzinach, możesz dodać stan **Zaplanowane odblokowanie** do piętra, a następnie zastosować harmonogram dostępu.

Na przykład, aby udostępnić piętro dla wszystkich podczas godzin pracy:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Piętra**.
2. Kliknij obok elementu na liście **Piętra**, który chcesz edytować.
3. Kliknij polecenie **Dodaj zaplanowane odblokowanie**.
4. Wybierz **Stan odblokowania** (**odblokowane** lub **odblokuj oba zamki**, w zależności do tego, czy drzwi do piętra mają jeden zamek, czy dwa).
5. Kliknij przycisk **OK**.
6. Zastosuj wstępnie zdefiniowany harmonogram dostępu **Godziny pracy** do stanu **Zaplanowane odblokowanie**.

Aby sprawdzić, kiedy piętro jest dostępne, kliknij przycisk .

Aby usunąć stan zaplanowanego odblokowania lub harmonogram dostępu, kliknij .

Używanie ręcznej obsługi pięter

Piętra mogą mieć różne dostępności, być ograniczone lub dostępne dla każdego. Tymczasowego dostępu można udzielić, przechodząc do karty**Piętra** i wybierając opcję **Ręczna obsługa pięter**. To, które działania w ramach ręcznej obsługi pięter są dostępne dla określonego piętra, zależy od przeprowadzonej konfiguracji piętra.

Aby skorzystać z ręcznej obsługi pięter:

1. Przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Piętra**.
2. Na liście **Piętra** kliknij obok tego piętra, które chcesz kontrolować.
3. Kliknij wymaganą akcję piętra. Patrz *Ręczna obsługa pięter na stronie 39*.

Uwaga

Aby skorzystać z ręcznej obsługi pięter, trzeba otworzyć stronę stronę Zarządzanie dostępem za pośrednictwem tego kontrolera piętra, do którego jest podłączone konkretne piętro. Jeśli otworzysz stronę Zarządzanie dostępem za pośrednictwem innego kontrolera piętra, zamiast ręcznej obsługi pięter pojawi się łącze do strony Informacje ogólne tego kontrolera piętra, do którego jest podłączone konkretne piętro. Kliknij łącze, przejdź do opcji **Zarządzanie dostępem** i wybierz kartę **Piętra**.

Ręczna obsługa pięter

Dostępne są następujące działania:

- **Odczytaj status piętra** – opcja ta umożliwia zweryfikowanie bieżącego stanu przekaźnika podłączonego do piętra.
- **Dostęp** – opcja ta umożliwia udzielenie użytkownikom dostępu do piętra. Stosowane jest ograniczenie czasu dostępu. Patrz *Konfiguracja monitorów drzwi i zamków na stronie 15*.
- **Odblokuj** – piętro pozostanie dostępne dla wszystkich do momentu naciśnięcia przycisku **Zablokuj**, aktywacji zaplanowanego statusu piętra lub ponownego uruchomienia kontrolera drzwi.
- **Zablokuj** – piętro pozostanie zablokowane do momentu naciśnięcia przycisku **Odblokuj**, aktywacji zaplanowanego statusu piętra lub ponownego uruchomienia kontrolera drzwi.

Tworzenie i edytowanie użytkowników

Każda osoba musi mieć własny profil użytkownika, aby uzyskać dostęp do drzwi w systemie kontroli dostępu. Profil użytkownika składa się z poświadczeń, które informują system o tożsamości użytkownika i o tym, kiedy i w jaki sposób użytkownik może uzyskać dostęp do drzwi.

Każdy użytkownik musi należeć do co najmniej jednej grupy, aby można było skutecznie zarządzać uprawnieniami. Więcej informacji: *Tworzenie i edytowanie grup*.

Tworzenie nowego profilu użytkownika:

1. Przejdź do opcji **Zarządzanie dostępem**.
2. Wybierz kartę **Użytkownicy** i kliknij opcję **Dodaj nowego użytkownika**.
3. W oknie dialogowym **Dodaj użytkownika** wprowadź poświadczenia użytkownika. Patrz *Poświadczenia użytkowników na stronie 40*.
4. Kliknij przycisk **Zapisz**.
5. Przeciągnij użytkownika do jednej lub więcej grup na liście **Grupy**. Jeśli lista **Grupy** jest pusta, utwórz nową grupę. Patrz *Tworzenie i edytowanie grup na stronie 34*.

Aby rozwinąć element na liście **Użytkownicy** i wyświetlić poświadczenia użytkownika, kliknij .

Aby znaleźć określonego użytkownika, wprowadź filtr w polu użytkowników. Aby wymusić dokładne dopasowanie, umieść filtrowany tekst w prostym cudzysłowie, na przykład "John", "Potter, Virginia".

Aby edytować poświadczenia użytkownika, kliknij i zmień poświadczenia zgodnie z wymaganiami. Następnie kliknij przycisk **Zapisz**.

Aby usunąć użytkownika, kliknij .

Ważne

Jeżeli użytkownika utworzono w aplikacji AXIS Visitor Manager, nie można go edytować ani usunąć w aplikacji AXIS Entry Manager. Więcej informacji na temat AXIS Visitor Manager i usługi czytnika kodów QR: *AXIS Visitor Access na stronie 24*.

Poświadczenia użytkowników

Dla użytkowników dostępne są następujące rodzaje poświadczeń:

- **Imię** (wymagane)
- **Nazwisko**
- **Ważny od** i **Ważny do** – wprowadź daty ważności poświadczeń użytkownika. Kliknij pole daty i wybierz żądany miesiąc, dzień i rok. Możesz również wpisać datę bezpośrednio w polu.
- **Zawieś poświadczenia** – wybierz tę opcję, aby zawiesić poświadczenie. Po zawieszeniu użytkownik nie może uzyskać dostępu do żadnych drzwi w systemie z użyciem tego poświadczenia. Odznacz tę opcję, aby ponownie przydzielić użytkownikowi dostęp. Zawieszenie ma charakter tymczasowy. Jeśli użytkownik ma zostać pozbawiony dostępu na stałe, najlepiej usunąć profil użytkownika.
- **PIN** (wymagany, jeśli nie jest używany numer karty lub tylko dane karty) – wprowadź czterocyfrowy osobisty numer identyfikacyjny (PIN) przydzielony użytkownikowi lub przez niego wybrany.
- **Kod obiektu** – wprowadź kod, aby zweryfikować system kontroli dostępu do obiektu. Jeśli wprowadzono wstępnie ustawiony kod obiektu, to pole zostanie wypełnione automatycznie, patrz *Wstępnie ustawiony kod obiektu na stronie 23*.
- **Numer karty** (wymagany, jeśli nie jest używany numer karty lub tylko dane karty) – wprowadź numer karty. Informacje o lokalizacji numeru karty podaje producent. Numer karty można również pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**.

- **Tylko dane karty** (wymagany, jeśli nie jest używany PIN lub numer karty) – wprowadź surowe dane karty. Surowe dane karty można pobrać z systemu. Przeciągnij kartę przez czytnik podłączony do systemu, wybierz czytnik z listy i kliknij polecenie **Pobierz**. Tego typu identyfikacji używaj tylko wtedy, gdy nie można znaleźć numeru karty.
- **Długi czas dostępu** – wybierz, aby zastąpić istniejący czas dostępu i umożliwić użytkownikowi pozostawienie drzwi otwartych przez dłuższy czas, patrz *Informacje o monitorze drzwi i opcjach ustawień czasu na stronie 16*.
- **Tablica rejestracyjna** (to poświadczenie nie jest dostępne w domyślnej wersji instalacyjnej kontrolerów drzwi) – po aktywacji tego poświadczenia przez oprogramowanie partnerskie wprowadź numer tablicy rejestracyjnej pojazdu użytkownika. Tego poświadczenia można używać tylko razem z oprogramowaniem partnerskim Axis i kamerą z oprogramowaniem do rozpoznawania tablic rejestracyjnych. Aby uzyskać więcej informacji, skontaktuj się z partnerem Axis lub lokalnym biurem sprzedaży firmy Axis.

Uwaga

Przycisk **Pobierz** jest dostępny tylko wtedy, gdy zakończono proces konfiguracji sprzętowej i jeden lub więcej czytników jest podłączonych do kontrolera.

Importowanie użytkowników

Użytkownicy mogą być dodawani do systemu poprzez importowanie pliku tekstowego w formacie CSV (wartości oddzielonych przecinkami). Zaleca się importowanie użytkowników, gdy trzeba dodać wielu użytkowników naraz.

Przed zaimportowaniem użytkowników należy utworzyć i zapisać plik (*.csv lub *.txt) w odpowiednim formacie CSV. Oddzielaj wartości przecinkami, bez spacji, i oddzielaj każdego użytkownika podziałem linii.

Przykład

```
jane,doe,1234,12345678,abc123
john,doe,5435,87654321,cde321
```

Aby zaimportować użytkowników:

1. Przejdź do **Ustawienia > Importuj użytkowników**.
2. Zlokalizuj i wybierz plik *.csv lub *.txt, który zawiera listę użytkowników.
3. Wybierz poprawną opcję poświadczeń dla każdej kolumny.
4. Aby zaimportować użytkowników do systemu, kliknij opcję **Importuj użytkowników**.
5. Sprawdź, czy każda kolumna zawiera poprawny typ poświadczenia.
6. Jeśli kolumny są poprawne, kliknij opcję **Rozpocznij importowanie użytkowników**. Jeśli kolumny są niepoprawne, kliknij przycisk **Anuluj** i rozpocznij od nowa.
7. Po zakończeniu importu kliknij przycisk **OK**.

Dostępne są następujące opcje poświadczeń:

- **Imię**
- **Nazwisko**
- **Kod PIN**
- **Numer karty**
- **Tablica rejestracyjna**
- **Nieprzydzielone** – wartości, które nie zostaną zaimportowane. Wybierz tę opcję, aby pominąć określoną kolumnę.

Więcej informacji dotyczących poświadczeń: *Tworzenie i edytowanie użytkowników*.

Eksportowanie użytkowników

Na stronie eksportowania jest wyświetlana lista zawierająca wartości rozdzielane przecinkami (CSV) przedstawiająca wszystkich użytkowników w systemie. Tę listę można wykorzystać do importowania użytkowników do innego systemu.

Aby eksportować listę użytkowników:

1. Otwórz zwykły edytor tekstu i utwórz nowy dokument.
2. Przejdź do menu **Ustawienia > Eksportuj użytkowników**.
3. Zaznacz wszystkie wartości na stronie i skopiuj je.
4. Wklej wartości w dokumencie tekstowym.
5. Zapisz dokument jako plik z wartościami rozdzielanymi przecinkami (*.csv) oraz jako plik tekstowy (*.txt).

Przykładowe kombinacje harmonogramów dostępu

Harmonogramy typów identyfikacji i harmonogramy grup można łączyć na kilka sposobów w celu uzyskania różnych wyników. Poniższe przykłady są zgodne z przepływem pracy opisanym tutaj: *strona 31*.

Przykład

Aby utworzyć kombinację harmonogramów, która

- zapewnia pracownikom ochrony dostęp do drzwi przez cały czas,
  - za pomocą karty w godzinach pracy (poniedziałek–piątek, od 6:00 do 16:00.),
  - za pomocą karty i numeru PIN poza godzinami pracy;
- która zapewnia pracownikom dziennej zmiany dostęp do tych samych drzwi
  - za pomocą karty tyko w godzinach pracy:

1. Utwórz **Harmonogram dodawania** o nazwie **Godziny zmiany dziennej**. Patrz *strona 32*.
2. Utwórz **Element harmonogramu** godzin pracy zmiany dziennej powtarzający się od poniedziałku do piątku od 6:00 do 16:00.
3. Utwórz dwie grupy: **Grupa Strażnicy** i **Grupa Personel zmiany dziennej**. Patrz *strona 34*.
4. Przeciągnij wstępnie zdefiniowany harmonogram dostępu **Zawsze** do grupy **Strażnicy**.
5. Przeciągnij harmonogram dostępu **Godziny zmiany dziennej** do grupy **Personel zmiany dziennej**.
6. Dodaj **Numer karty i PIN** oraz **Tylko numer karty** jako typy identyfikacji dla czytnika przy drzwiach.
7. Przeciągnij wstępnie zdefiniowany harmonogram dostępu **Zawsze** do typu identyfikacji **Numer karty i PIN**.
8. Przeciągnij harmonogram dostępu **Godziny zmiany dziennej** do typu identyfikacji **Tylko numer karty**.
9. Przeciągnij drzwi do obu grup. Następnie dodaj użytkowników do grup. Patrz *strona 39*.

Przykład

Aby utworzyć kombinację harmonogramów, która

- zapewnia pracownikom ochrony dostęp do drzwi przez cały czas,
  - za pomocą karty w godzinach pracy (poniedziałek–piątek, od 6:00 do 16:00.),
  - za pomocą karty i numeru PIN poza godzinami pracy;
- która zapewnia pracownikom dziennej zmiany dostęp do tych samych drzwi od 6:00 do 16:00,

- za pomocą karty tyko w godzinach pracy;
- za pomocą karty i numeru PIN w nocy i w weekendy:

1. Utwórz **Harmonogram dodawania** o nazwie **Godziny zmiany dziennej**. Patrz *strona 32*.
2. Utwórz **Element harmonogramu** godzin pracy zmiany dziennej powtarzający się od poniedziałku do piątku od 6:00 do 16:00.
3. Utwórz **Harmonogram odejmowania** o nazwie **Noce i weekendy**.
4. Utwórz **Element harmonogramu** godzin pracy zmiany nocnej powtarzający się od niedzieli do soboty od 16:00 do 6:00.
5. Przeciągnij wstępnie zdefiniowany harmonogram **Zawsze** i harmonogram dostępu **Noce i weekendy** do grupy **Personel zmiany dziennej**.
6. Utwórz dwie grupy: **Grupa Strażnicy** i **Grupa Personel zmiany dziennej**. Patrz *strona 34*.
7. Przeciągnij wstępnie zdefiniowany harmonogram dostępu **Zawsze** do grupy **Strażnicy** i grupy **Personel zmiany dziennej**.
8. Przeciągnij harmonogram dostępu **Noce i weekendy** do grupy **Personel zmiany dziennej**.
9. Dodaj **Numer karty i PIN** oraz **Tylko numer karty** jako typy identyfikacji dla czytnika przy drzwiach.
10. Przeciągnij wstępnie zdefiniowany harmonogram dostępu **Zawsze** do typu identyfikacji **Numer karty i PIN**.
11. Przeciągnij harmonogram dostępu **Godziny zmiany dziennej** do typu identyfikacji **Tylko numer karty**.
12. Przeciągnij drzwi do obu grup. Następnie dodaj użytkowników do grup. Patrz *strona 39*.

Konfiguracja alarmów i zdarzeń

Zdarzenia zachodzące w systemie, na przykład kiedy użytkownik przeciągnie kartę lub kiedy aktywuje się urządzenie REX, są rejestrowane w dzienniku zdarzeń. Zarejestrowane zdarzenia można skonfigurować tak, aby wyzwalały alarmy, które będą rejestrowane w dzienniku alarmów.

- Wyświetlanie dziennika zdarzeń. Patrz *strona 44*.
- Eksportowanie dziennika zdarzeń. Patrz *strona 44*
- Wyświetlanie dziennika alarmów. Patrz *strona 45*.
- Konfigurowanie dzienników zdarzeń i alarmów. Patrz *strona 45*.

Alarmy można również skonfigurować tak, aby wyzwalały akcje, takie jak powiadomienia e-mail. Więcej informacji: *Konfigurowanie reguł akcji na stronie 46*.

Wyświetlanie dziennika zdarzeń

Aby wyświetlić zarejestrowane zdarzenia, przejdź do opcji **Dziennik zdarzeń**.

Jeśli włączone są zdarzenia globalne, można otworzyć dziennik zdarzeń z poziomu dowolnego kontrolera drzwi w systemie. Więcej informacji na temat zdarzeń globalnych: *Konfigurowanie dzienników zdarzeń i alarmów na stronie 45*.

Aby rozwinąć element w dzienniku zdarzeń i wyświetlić szczegóły zdarzeń, kliknij  .

Zastosowanie filtrów do dziennika zdarzeń ułatwia znalezienie określonych zdarzeń. Aby odfiltrować listę, wybierz jeden lub kilka filtrów zdarzeń i kliknij przycisk **Zastosuj filtry**. Więcej informacji: *Filtry dziennika zdarzeń na stronie 44*.

Jako administrator możesz bardziej interesować się szczególnymi typami zdarzeń. Możesz więc wybrać, które zdarzenia mają być rejestrowane dla poszczególnych kontrolerów. Więcej informacji: *Opcje dziennika zdarzeń na stronie 45*.

Filtry dziennika zdarzeń

Możesz zawęzić zakres dziennika zdarzeń, wybierając co najmniej jeden z następujących filtrów:

- Użytkownik – filtruje zdarzenia związane z wybranym użytkownikiem.
- Drzwi i piętro – filtruje zdarzenia związane z konkretnymi drzwiami lub piętrem.
- Temat – filtruje typy zdarzeń.
- Źródło – filtruje zdarzenia z wybranego kontrolera. Filtr dostępny tylko w przypadku grupy kontrolerów oraz gdy zdarzenia globalne są włączone.
- Data i godzina – filtruje dziennik zdarzeń według przedziału dat i czasu.

Eksportowanie dziennika zdarzeń

Aby eksportować zarejestrowane zdarzenia, przejdź do opcji **Dziennik zdarzeń**:

1. Kliknij  .
2. Wybierz format eksportowanego pliku z menu podręcznego, aby rozpocząć eksportowanie.

Uwaga

Format CSV obsługują wszystkie przeglądarki, format XLSX obsługują przeglądarki Chrome™ oraz Internet Explorer®.

Uwaga

Po wyeksportowaniu pliku przycisk eksportu zmieni się z  na  . Aby rozpocząć nowy eksport, odśwież stronę internetową. Przycisk eksportu ponownie zmieni się na  .

Wyświetlanie dziennika alarmów

Aby wyświetlić wyzwolone alarmy, przejdź do opcji **Dziennik alarmów**. Jeśli włączone są zdarzenia globalne, można otworzyć dziennik alarmów z poziomu dowolnego kontrolera drzwi w systemie. Więcej informacji na temat zdarzeń globalnych: *Konfigurowanie dzienników zdarzeń i alarmów na stronie 45*.

Aby rozwinąć element w dzienniku alarmów i wyświetlić szczegóły alarmów, takie jak identyfikator drzwi i ich stan, kliknij  .

Aby usunąć alarm z listy po zweryfikowaniu jego przyczyny, kliknij polecenie **Potwierdź**. Aby usunąć wszystkie alarmy, kliknij polecenie **Potwierdź wszystkie alarmy**.

Jako administrator możesz potrzebować pewnych zdarzeń, aby wyzwalać alarmy. Możesz więc wybrać, które zdarzenia mają wyzwalać alarmy dla poszczególnych kontrolerów. Więcej informacji: *Opcje dziennika alarmów na stronie 46*.

Konfigurowanie dzienników zdarzeń i alarmów

Strona Konfiguracja dzienników zdarzeń i alarmów umożliwia określenie zdarzeń, które będą rejestrowane w dzienniku i wyzwalać alarmy.

Aby udostępniać zdarzenia i alarmy pomiędzy wszystkie podłączone kontrolery, wybierz **Zdarzenia globalne**. Gdy zdarzenia globalne są włączone, wystarczy otworzyć jedną stronę Dziennika zdarzeń i jedną stronę Dziennika alarmów, aby zarządzać jednocześnie zdarzeniami i alarmami wszystkich kontrolerów drzwi w systemie. Zdarzenia globalne są domyślnie włączone.

Jeśli wyłączysz zdarzenia globalne, konieczne będzie otwieranie jednej strony Dziennika zdarzeń i jednej strony Dziennika alarmów dla każdego kontrolera drzwi i osobne zarządzanie ich zdarzeniami i alarmami.

Ważne

Za każdym razem, gdy włączysz lub wyłączysz zdarzenia globalne, dziennik zdarzeń zostanie wyczyszczony. Oznacza to, że wszystkie zdarzenia sprzed tego momentu są usuwane, a rejestrowanie zdarzeń w dzienniku zdarzeń rozpoczyna się od nowa.

Alarmy można również skonfigurować tak, aby wyzwalały akcje, takie jak powiadomienia e-mail. Więcej informacji: *Konfigurowanie reguł akcji na stronie 46*.

Opcje dziennika zdarzeń

By zdefiniować, jakie zdarzenia powinny znaleźć się w dzienniku zdarzeń, przejdź do menu **Ustawienia > Skonfiguruj dzienniki zdarzeń i alarmów**.

Dostępne są następujące opcje rejestrowania zdarzeń:

- **Brak rejestracji** – wyłącz rejestrowanie zdarzeń. Zdarzenie nie zostanie zarejestrowane ani włączone do dziennika zdarzeń.
- **Rejestruj dla wszystkich źródeł** – włącz rejestrowanie zdarzeń we wszystkich kontrolerach drzwi. Zdarzenie zostanie zarejestrowane dla wszystkich kontrolerów i uwzględnione w dzienniku zdarzeń.
- **Rejestruj dla wybranych źródeł** – włącz rejestrowanie zdarzeń w wybranych kontrolerach drzwi. Zdarzenie zostanie zarejestrowane dla wszystkich wybranych kontrolerów i uwzględnione w dzienniku zdarzeń. Wybierz tę opcję dla zdarzeń, które będą połączone z opcją dziennika alarmów **Brak alarmów** lub **Rejestruj alarm dla wybranych kontrolerów**.

  Na liście **Skonfiguruj rejestrowanie zdarzeń** kliknij opcję **Wybierz kontrolery** pod elementem dziennika zdarzeń, które chcesz włączyć. Zostanie otwarte okno dialogowe **Rejestracja zdarzeń w urządzeniu**. W menu **Rejestruj zdarzenie** wybierz kontrolery, dla których włączone ma być rejestrowanie alarmów, i kliknij przycisk **Zapisz**.

Opcje dziennika alarmów

By zdefiniować, jakie zdarzenia powinny wyzwolić alarm, przejdź do menu **Ustawienia > Skonfiguruj dzienniki zdarzeń i alarmów**.

Dostępne są następujące opcje wyzwalania i rejestracji alarmów:

- **Brak alarmów** – służy do włączania rejestrowania alarmów. Zdarzenie nie wyzwoli żadnych alarmów i nie zostanie ujęte w dzienniku alarmów.
- **Zarejestruj alarmy ze wszystkich źródeł** – włącz rejestrowanie alarmów we wszystkich kontrolerach drzwi. Zdarzenie wyzwoli alarm i zostanie ujęte w dzienniku alarmów.
- **Zarejestruj alarm z wybranych źródeł** – włącz rejestrowanie alarmów w wybranych kontrolerach drzwi. Zdarzenie wyzwoli alarm i zostanie ujęte w dzienniku alarmów.

  Na liście **Skonfiguruj rejestrowanie alarmów** kliknij opcję **Wybierz źródła** pod elementem dziennika alarmów, których chcesz włączyć. Zostanie otwarte okno dialogowe **Wyzwalanie alarmu w urządzeniu**. W opcji **Wyzwól alarm** wybierz kontrolery drzwi, w których rejestrowanie alarmów ma być włączone, i kliknij przycisk **Zapisz**.

Konfigurowanie reguł akcji

Na stronach zdarzeń można skonfigurować produkt Axis tak, aby wykonywał akcje po wystąpieniu różnych zdarzeń. Produkt można na przykład wysłać powiadomienie emailem lub aktywować port wyjścia po wyzwoleniu alarmu. Zestaw warunków określających, w jaki sposób i kiedy wyzwalana jest akcja, nazywamy regułą akcji. Jeśli określono wiele warunków, to do wyzwolenia akcji konieczne jest spełnienie wszystkich z nich.

Więcej informacji dotyczących dostępnych wyzwalaczy i akcji: *Wyzwalacze na stronie 47* i *Akcje na stronie 49*.

W poniższym przykładzie opisano, jak skonfigurować regułę akcji, aby po wyzwoleniu alarmu zostało wysłane pocztą e-mail powiadomienie.

1. Skonfiguruj alarmy. Patrz *Konfigurowanie dzienników zdarzeń i alarmów na stronie 45*.
2. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Reguły akcji** i kliknij przycisk **Dodaj**.
3. Wybierz opcję **Włącz regułę** i wprowadź nazwę opisową reguły.
4. Z listy rozwijanej **Wyzwalacz** wybierz opcję **Rejestr zdarzeń**.
5. Możesz opcjonalnie wybrać **Harmonogram** i **Dodatkowe warunki**. Patrz poniżej.
6. W poleceniu **Akcje** wybierz opcję **Wyślij powiadomienie** z listy rozwijanej **Typ**.
7. Z listy rozwijanej wybierz odbiorcę wiadomości e-mail. Patrz *Dodawanie odbiorców na stronie 49*.

W poniższym przykładzie opisano, jak skonfigurować regułę akcji, aby po otwarciu drzwi siłą został aktywowany port wyjścia.

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Porty i urządzenia > Porty I/O**.
2. Wybierz **Wyjście** z listy rozwijanej **Typ portu I/O** i wprowadź nazwę w polu **Nazwa**.
3. Wybierz **Stan normalny** portu I/O i kliknij przycisk **Zapisz**.
4. Przejdź do menu **Zdarzenia > Reguły akcji** i kliknij przycisk **Dodaj**.
5. Z listy rozwijanej **Wyzwalacz** wybierz opcję **Drzwi**.
6. Wybierz **Alarm drzwi** z listy rozwijanej.
7. Wybierz żądane drzwi z listy rozwijanej.
8. Wybierz **DrzwiOtwarteSiłą** z listy rozwijanej.
9. Możesz opcjonalnie wybrać **Harmonogram** i **Dodatkowe warunki**. Patrz poniżej.

10. W poleceniu **Akcje** wybierz opcję **Port wyjścia** z listy rozwijanej **Typ**.
11. Wybierz żądany port wyjścia z listy rozwijanej **Port**.
12. Ustaw stan jako **Aktywne**.
13. Wybierz **Czas trwania** i wartość **Przejdź do przeciwnego stanu po**. Wprowadź żądany czas trwania akcji.
14. Kliknij przycisk **OK**.

Aby użyć więcej niż jednego wyzwalacza dla reguły akcji, wybierz opcję **Dodatkowe warunki** i kliknij przycisk **Dodaj**, aby dodać dodatkowe wyzwalacze. Jeśli określono wiele warunków, to do wyzwolenia akcji konieczne jest spełnienie wszystkich z nich.

Aby zapobiec wielokrotnemu wyzwalaniu akcji, możesz ustawić wartość opcji **Odczekaj przynajmniej**. Wprowadź w godzinach, minutach i sekundach czas, podczas którego wyzwalacz powinien zostać zignorowany przed ponowną aktywacją reguły akcji.

Więcej informacji znajduje się we wbudowanej pomocy produktu.

Wyzwalacze

Dostępne **wyzwalacze** i **warunki** obejmują:

- **Punkt dostępu**
  - **Punkt dostępu włączony** – wyzwala regułę akcji, gdy skonfigurowane jest urządzenie punktu dostępu, takie jak czytnik lub urządzenie REX, na przykład po zakończeniu konfiguracji sprzętu lub dodaniu typu identyfikacji.
- **Konfiguracja**
  - **Zmieniono punkt dostępu** – wyzwala regułę akcji, gdy konfiguracja urządzenia punktu dostępu, takiego jak czytnik lub urządzenie REX, ulega zmianie, na przykład po skonfigurowaniu sprzętu lub edycji typu identyfikacji, zmieniającego sposób dostępu do drzwi.
  - **Usunięto punkt dostępu** – wyzwala regułę akcji, gdy konfiguracja sprzętowa urządzenia punktu dostępu, takiego jak czytnik lub urządzenie REX, zostanie zresetowana.
  - **Obszar zmieniony** — opcja niedostępna w tej wersji aplikacji AXIS Entry Manager. Opcję tę należy skonfigurować przez klienta, na przykład system zarządzania dostępem, interfejs oprogramowania VAPIX® obsługujący tę funkcję i pracujący z urządzeniami, które mogą dostarczyć wymagany sygnał. Opcja ta wyzwala regułę akcji po zmianie obszaru dostępu.
  - **Obszar usunięty** — opcja niedostępna w tej wersji aplikacji AXIS Entry Manager. Opcję tę należy skonfigurować przez klienta, na przykład system zarządzania dostępem, interfejs oprogramowania VAPIX® obsługujący tę funkcję i pracujący z urządzeniami, które mogą dostarczyć wymagany sygnał. Opcja ta wyzwala regułę akcji po usunięciu obszaru dostępu z systemu.
  - **Drzwi zmienione** – wyzwala regułę akcji, gdy ustawienia konfiguracji drzwi, na przykład nazwa drzwi, zostaną zmienione lub kiedy drzwi zostaną dodane do systemu. Opcji tej można użyć na przykład do wysłania powiadomienia o instalacji i konfiguracji drzwi.
  - **Drzwi usunięte** – wyzwala regułę akcji, gdy drzwi zostaną usunięte z systemu. Opcji tej można użyć na przykład do wysłania powiadomienia o usunięciu drzwi z systemu.
- **Drzwi**
  - **Alarm akumulatora** – wyzwala regułę akcji, gdy stan naładowania akumulatora w drzwiach podłączonych bezprzewodowo jest niski lub kiedy akumulator się wyczerpie.
  - **Alarm drzwi** – wyzwala regułę akcji, gdy monitor drzwi zasygnalizuje, że drzwi zostały otwarte, są otwarte zbyt długo lub że wystąpiła awaria/uszkodzenie drzwi. Opcji tej można użyć na przykład do wysłania powiadomienia o próbie włamania.
  - **Monitor podwójnej blokady drzwi** – wyzwala regułę akcji tylko wtedy, gdy dodatkowy zamek zmieni status na zablokowany lub odblokowany.

  - **Monitor blokady drzwi** – wyzwala regułę akcji, gdy standardowy zamek zmieni status na zablokowany lub odblokowany. Na przykład kiedy czujnik drzwi wykryje otwarcie drzwi, pomimo że są one zamknięte, wyzwalany jest alarm usterki.

  - **Door Mode (Tryb drzwi)** – wyzwala regułę akcji, gdy drzwi zmieniają stan, na przykład, gdy uzyskano dostęp do drzwi lub gdy drzwi zostały zablokowane albo są w trybie blokady. Szczegółowe opisy tych trybów znajdują się w pomocy online.

  - **Monitor drzwi** – wyzwala regułę akcji, gdy zmienia się status drzwi. Opcji tej można użyć na przykład do wysłania powiadomienia o wykryciu otwarcia lub zamknięcia drzwi przez czujnik.

  - **Sabotaż drzwi** – wyzwala regułę akcji, gdy monitor drzwi wykryje, że połączenie zostało przerwane, na przykład gdy ktoś odetnie przewody monitora drzwi. Aby użyć tego wyzwalacza, należy się upewnić, że wybrano opcję **Włącz nadzorowane wejścia**, a rezystory końcowe zamontowano na odpowiednich portach wejścia złącza drzwi. Więcej informacji: *Używanie nadzorowanych wejść na stronie 18*.

  - **Ostrzeżenie o drzwiach** – wyzwala regułę akcji przed uruchomieniem się alarmu zbyt długiego czasu otwarcia drzwi. Opcji tej można użyć na przykład do wysłania ostrzeżenia, że kontroler drzwi aktywuje alarm zbyt długiego czasu otwarcia drzwi, jeśli drzwi nie zostaną zamknięte w ciągu określonego czasu. Więcej informacji o zbyt długim czasie otwarcia drzwi: *Konfiguracja monitorów drzwi i zamków na stronie 15*.

  - **Blokada zamka** – wyzwala regułę akcji po fizycznym zablokowaniu zamka bezprzewodowego drzwi.

- **Rejestr zdarzeń** — funkcja ta umożliwia śledzenie wszystkich zdarzeń dotyczących kontrolera drzwi, na przykład przeciągnięcia karty lub otwarcia drzwi przez użytkownika. Jeżeli włączono opcję **Zdarzenia globalne**, rejestrowane są wszystkie zdarzenia dla wszystkich kontrolerów w systemie. Aby ustawić alarmy i zdarzenia, które mogą wyzwalać reguły akcji, przejdź do **Konfiguracja > Konfiguruj dzienniki zdarzeń i alarmów**. Rejestr zdarzeń jest wspólny dla całego systemu i może przechowywać maksymalnie 30 000 zdarzeń. Po osiągnieciu tego limitu rejestr zdarzeń używa reguły first in first out (FIFO). Oznacza to, że najpierw nadpisywane są najstarsze zdarzenia.

  - **Alarm** – wyzwala regułę akcji po wyzwoleniu jednego z alarmów. Administrator systemu może wybrać zdarzenia ważniejsze od innych i zdecydować, czy dane zdarzenie ma wyzwalać alarm.

  - **Pominięte alarmy** – wyzwala regułę akcji, gdy nowych alarmów nie można zapisać w dzienniku alarmów. Tak może dziać się w przypadku, gdy wystąpi wiele alarmów w tym samym czasie i rejestr nie nadąży ich zapisywać. W przypadku pominięcia alarmu do operatora wysyłane jest powiadomienie.

  - **Pominięte zdarzenia** – wyzwala regułę akcji, gdy nowych zdarzeń nie można zapisać w dzienniku zdarzeń. Tak może dziać się w przypadku, gdy wystąpi wiele zdarzeń w tym samym czasie i rejestr nie nadąży ich zapisywać. W przypadku pominięcia zdarzenia do operatora wysyłane jest powiadomienie.

- **Sprzęt**

  - **Sieć** – wyzwala regułę akcji po utracie połączenia sieciowego. Wybierz opcję **Tak**, aby wyzwolić regułę akcji po utracie połączenia sieciowego. Wybierz opcję **Nie**, aby wyzwolić regułę akcji po przywróceniu połączenia sieciowego. Wybierz opcję **Usunięto adres IPv4/v6** lub **Nowy adres IPv4/v6**, aby wyzwolić akcję po zmianie adresu IP.

  - **Połączenie równorzędne** – wyzwala regułę akcji, gdy produkt Axis nawiąże połączenie z innym kontrolerem drzwi, jeśli połączenie sieciowe między urządzeniami zostanie przerwane lub jeśli parowanie kontrolerów drzwi się nie powiodło. Opcji tej można użyć na przykład do wysłania powiadomienia o utracie połączenia sieciowego przez kontroler drzwi.

- **Sygnał wejściowy**

  - **Port wejścia cyfrowego** – wyzwala regułę akcji po odebraniu przez port I/O sygnału z podłączonego urządzenia. Patrz *Porty I/O na stronie 61*.

  - **Wyzwalacz ręczny** – wyzwala regułę akcji po aktywacji wyzwalacza ręcznego. Opcja ta może być wykorzystana przez klienta, na przykład system zarządzania dostępem, przez interfejs oprogramowania VAPIX®, do ręcznego rozpoczęcia i zakończenia reguły akcji.

  - **Wejścia wirtualne** – wyzwala regułę akcji, gdy jedno z wejść wirtualnych zmieni stan. Opcja ta może być wykorzystywana przez klienta, na przykład system zarządzania dostępem, poprzez API VAPIX®, do wyzwalania

akcji. Wejścia wirtualne mogą na przykład być podłączone do przycisków w interfejsie użytkownika systemu zarządzania dozorem.

- **Harmonogram**
  - **Przedział czasowy** – wyzwala regułę akcji na początku harmonogramu i pozostaje aktywna do zakończenia.
  - **Jednorazowo** – wyzwala regułę akcji po wystąpieniu zdarzenia jednorazowego. Oznacza to zdarzenie, które występuje w konkretnym momencie i nie ma określonego czasu trwania.
- **System**
  - **Gotowość systemu** – wyzwala regułę akcji po uzyskaniu przez system stanu gotowości. Produkt Axis może wykryć na przykład stan sytemu i wysłać powiadomienie do operatora o jego uruchomieniu.

    Zaznacz przycisk opcji **Tak**, aby wyzwolić regułę akcji po wejściu produktu w stan gotowości. Reguła ta zostanie wyzwolona tylko wtedy, gdy uruchomione zostaną wszystkie wymagane usługi, takie jak system wykrywania zdarzeń.
- **Czas**
  - **Cyklicznie** – wyzwala regułę akcji poprzez monitorowanie utworzonych zdarzeń cyklicznych. Tego wyzwalacza można użyć do inicjowania cyklicznych akcji, takich jak wysyłanie powiadomień co godzinę. Wybierz wzorzec powtórzeń lub utwórz nowy. Więcej informacji na temat konfiguracji wzorców powtórzeń: *Konfiguracja powtórzeń na stronie 50*.
  - **Użyj harmonogramu** – wyzwala regułę akcji zgodnie z harmonogramem. Patrz *Jak stworzyć harmonogram na stronie 50*.

Akcje

Można skonfigurować następujące akcje:

- **Port wyjścia** – aktywuj port I/O sterujący urządzeniem zewnętrznym.
- **Wyślij powiadomienie** – wyślij powiadomienie do odbiorcy.
- **Wskaźnik LED** — wskaźnik LED można ustawić tak, aby migał podczas wykonywania reguły akcji lub przez ustaloną liczbę sekund. Wskaźnika można użyć podczas instalacji i konfiguracji, aby potwierdzić, że ustawienia wyzwalacza (na przykład zbyt długiego czasu otwarcia drzwi) są prawidłowe. Aby ustawić kolor migającej diody LED, wybierz **Kolor LED** z listy rozwijanej.

Dodawanie odbiorców

Produkt może wysyłać wiadomości w celu powiadamiania odbiorców o zdarzeniach i alarmach. Aby produkt mógł wysyłać powiadomienia, trzeba zdefiniować co najmniej jednego odbiorcę. Więcej informacji na temat dostępnych opcji: *Typy odbiorców na stronie 50*.

Aby dodać odbiorcę:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Odbiorcy** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową.
3. Wybierz **Typ** odbiorcy.
4. Wprowadź informacje potrzebne w przypadku danego typu odbiorcy.
5. Kliknij przycisk **Test**, aby przetestować połączenie z odbiorcą.
6. Kliknij przycisk **OK**.

Typy odbiorców

Dostępne są następujące typy odbiorców:

HTTP

HTTPS

Poczta e-mail

TCP

Konfiguracja odbiorców wiadomości e-mail

Adresatów wiadomości e-mail można skonfigurować, wybierając jednego z wymienionych dostawców poczty e-mail lub określając serwer SMTP, port i metodę uwierzytelnienia używane na przykład przez firmowy serwer poczty e-mail.

Uwaga

Niektórzy dostawcy usług poczty elektronicznej stosują filtry bezpieczeństwa, uniemożliwiające odbiór lub przeglądanie dużych załączników, odbieranie wiadomości cyklicznych itp. Sprawdź zasady zabezpieczeń dostawcy poczty elektronicznej, aby uniknąć problemów z dostarczaniem e-maili i zablokowania konta.

Aby skonfigurować adresata wiadomości e-mail przy użyciu jednego z wymienionych dostawców:

1. Przejdź do menu **Zdarzenia > Odbiorcy** i kliknij przycisk **Dodaj**.
2. Wprowadź **Nazwę** i wybierz **E-mail** z listy **Typ**.
3. Wprowadź adresy e-mail, na które chcesz wysłać e-maile, w polu **Do**. Aby wprowadzić wiele adresów e-mail, oddziel je przecinkami.
4. Wybierz dostawcę poczty elektronicznej z listy **Dostawca**.
5. Wprowadź identyfikator użytkownika i hasło do konta e-mail.
6. Kliknij przycisk **Testuj**, aby wysłać testową wiadomość e-mail.

Aby skonfigurować adresata wiadomości e-mail przy użyciu na przykład firmowego serwera poczty e-mail, postępuj zgodnie z instrukcjami powyżej, ale wybierz **Użytkownik zdefiniowany** jako **Dostawca**. Wprowadź adres e-mail, który ma być wyświetlany jako adres nadawcy w polu **Od**. Wybierz **Ustawienia zaawansowane** i podaj adres serwera SMTP, port i metodę uwierzytelniania. Opcjonalnie wybierz opcję **Użyj szyfrowania**, aby wysyłać wiadomości e-mail przez połączenie szyfrowane. Certyfikat serwera można sprawdzić za pomocą certyfikatów dostępnych w produkcie Axis. Informacje na temat przesyłania certyfikatów: *Certyfikaty na stronie 54*.

Jak stworzyć harmonogram

Harmonogramów można użyć jako dodatkowego warunku wyzwalania reguł akcji. Użyj jednego ze wstępnie zdefiniowanych harmonogramów lub utwórz nowy harmonogram zgodnie z opisem poniżej.

Aby utworzyć nowy harmonogram:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Harmonogramy** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową oraz informacje niezbędne w przypadku harmonogramu dziennego, tygodniowego, miesięcznego lub rocznego.
3. Kliknij przycisk **OK**.

Aby użyć harmonogramu w reguła akcji, wybierz harmonogram z listy rozwijanej **Harmonogram** na stronie Konfiguracja reguł akcji.

Konfiguracja powtórzeń

Powtórzenia służą do powtarzania wyzwalania reguł akcji, na przykład co pięć minut lub co godzinę.

Konfigurowanie powtórzenia:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Zdarzenia > Powtórzenia** i kliknij przycisk **Dodaj**.
2. Wprowadź nazwę opisową i wzorzec powtórzenia.
3. Kliknij przycisk **OK**.

Aby użyć powtórzenia w regule akcji, wybierz najpierw opcje **Godzina** na liście rozwijanej **Wyzwalacz** na stronie Konfiguracja reguł akcji, a następnie wybierz powtórzenie z listy rozwijanej.

Aby zmodyfikować lub zmienić powtórzenie, wybierz je z listy **Lista powtórzeń** i kliknij przycisk **Zmień** lub **Usuń**.

Informacje zwrotne z czytnika

Czytniki używają diod LED i sygnałów dźwiękowych do przekazywania informacji zwrotnych użytkownikom (osobom uzyskującym lub próbującym uzyskać dostęp do drzwi). Kontroler drzwi może wyzwolić kilka komunikatów zwrotnych, a niektóre z nich są wstępnie skonfigurowane w kontrolerze drzwi i obsługiwane przez większość czytników.

Czytniki mają różne konfiguracje działania diod LED, ale zazwyczaj korzystają z różnych sekwencji stałego i migającego czerwonego, zielonego i bursztynowego światła.

Czytniki mogą również wykorzystywać sygnały dźwiękowe do przesyłania komunikatów, używając różnych sekwencji krótszych i dłuższych sygnałów.

Poniższa tabela zawiera zdarzenia wstępnie skonfigurowane w kontrolerze drzwi tak, aby wyzwolić komunikat zwrotny z czytnika i typowy sygnał informacji zwrotnej. Sygnały zwrotne czytników AXIS znajdują się w Instrukcji instalacji dostarczonej z czytnikiem AXIS.

Zdarzenie	Wiegand dwie diody LED	Wiegand jedna dioda LED	OSDP	Wzorzec sygnału dźwiękowego	Stan
Bezczynność[1]	Wył.	Czerwony	Czerwony	Bez dźwięku	Normalny
WymagajPIN	Migający czerwony/zielony	Migający czerwony/zielony	Migający czerwony/zielony	Dwa krótkie sygnały	Wymagany PIN
Przyznano dostęp	Zielony	Zielony	Zielony	Sygnał dźwiękowy	Przyznano dostęp
Odmowa dostępu	Czerwony	Czerwony	Czerwony	Sygnał dźwiękowy	Odmowa dostępu

1. Stan bezczynności rozpoczyna się po zamknięciu drzwi i zablokowaniu zamka.

Komunikaty zwrotne inne niż wymienione powyżej należy skonfigurować przez klienta, na przykład system zarządzania dostępem, interfejs oprogramowania VAPIX® obsługujący tę funkcję i pracujący z czytnikami, które mogą dostarczyć wymagany sygnał. Więcej informacji znajduje się w informacjach o użytkownikach dostarczonych przez deweloperów systemu zarządzania dostępem i producenta czytnika.

Raporty

Strona Raporty umożliwia przeglądanie, drukowanie i eksport raportów zawierających różne rodzaje informacji o systemie. Więcej informacji na temat dostępnych raportów: *Typy raportów na stronie 52*.

Przeglądanie, drukowanie i eksportowanie raportów

Aby otworzyć stronę Raporty, kliknij opcję **Raporty**.

Aby obejrzeć raport, kliknij polecenie **Pokaż i wydrukuj**.

Aby wydrukować raport:

1. Kliknij polecenie **Pokaż i wydrukuj**.
2. Wybierz kolumny, które powinny znaleźć się w raporcie. Domyślne wybierane są wszystkie kolumny.
3. Jeśli chcesz zawęzić zakres raportu, wprowadź filtr w odpowiednim polu filtra. Na przykład możesz filtrować użytkowników według grupy, do której należą, drzwi według ich harmonogramu lub grupy według drzwi, do których mają dostęp.

   Aby wymusić dokładne dopasowanie, umieść filtrowany tekst w prostym cudzysłowie, na przykład "John".
4. Jeśli chcesz posortować elementy raportu w innej kolejności, kliknij  w odpowiedniej kolumnie. Aby zmienić kolejność ze standardowej na odwróconą lub odwrotnie, przełącz przyciski sortowania.

   ▲ służy do wyświetlania elementów w standardowej kolejności (rosnąco).

   ▼ służy do wyświetlania elementów w odwróconej kolejności (malejąco).
5. Kliknij polecenie **Drukuj wybrane kolumny**.

Aby eksportować raport, kliknij polecenie **Eksportuj plik CSV**.

Raport zostanie wyeksportowany jako plik zawierający wartości rozdzielane przecinkami (CSV) i będzie zawierać wszystkie możliwe dla danego rodzaju raportu kolumny i elementy. Jeśli nie określono inaczej, wyeksportowany plik (*.csv) zostanie zapisany w domyślnym folderze pobierania. Folder pobierania można wybrać w ustawieniach użytkownika przeglądarki internetowej.

Uwaga

W raportach są wyświetlani wyłącznie użytkownicy z poświadczeniami.

Typy raportów

Dostępne są następujące typy raportów:

- Harmonogramy dostępu. Więcej informacji dotyczących typów i opcji harmonogramów dostępu: *strona 32* i *strona 33*.
- Grupy. Więcej informacji dotyczących danych uwierzytelniających grup: *strona 34*.
- Drzwi. Więcej informacji dotyczących drzwi i typów identyfikacji: *strona 34* i *strona 35*.
- Użytkownicy. Więcej informacji dotyczących danych uwierzytelniających użytkowników: *strona 40*.
- Kontrolery drzwi. Więcej informacji dotyczących podłączonych kontrolerów i typów ich identyfikatorów: *strona 28*. Więcej informacji dotyczących opcji czasu monitorowania drzwi: *strona 17*.

Opcje systemu

Zabezpieczenia

Użytkownicy

Kontrola dostępu użytkowników jest domyślnie włączona i można ją skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > Użytkownicy**. Administrator może skonfigurować innych użytkowników, nadając im nazwy użytkowników i przydzielając hasła.

Lista użytkowników zawiera autoryzowanych użytkowników i grupy użytkowników (poziomy dostępu):

- **Administratorzy** mają nieograniczony dostęp do wszystkich ustawień. Administrator może dodawać, modyfikować i usuwać innych użytkowników.

Uwaga

Należy pamiętać, że po wybraniu opcji **Zaszyfrowane i niezaszyfrowane**, serwer WWW zaszyfruje hasło. Jest to domyślna opcja dla nowego urządzenia lub urządzenia zresetowanego do domyślnych ustawień fabrycznych.

W opcji **Ustawienia hasła HTTP/RTSP** wybierz typ dozwolonego hasła. Może być konieczne zezwolenie na używanie niezaszyfrowanych haseł, jeśli istnieją klienty, które nie obsługują szyfrowania, lub jeśli zaktualizowano oprogramowanie sprzętowe, a istniejące klienty obsługują szyfrowanie, ale konieczne jest ponowne zalogowanie i konfiguracja, aby można było użyć tej funkcji.

ONVIF

ONVIF to otwarte forum branżowe zapewniające i promujące standardowe interfejsy zapewniające skuteczne współdziałanie produktów bezpieczeństwa fizycznego opartych na protokole IP.

Utworzenie użytkownika powoduje automatyczne włączenie komunikacji ONVIF. Nazwy użytkownika i hasła należy używać podczas komunikacji ONVIF z urządzeniem. Więcej informacji znajduje się na stronie *www.onvif.org*

Filtr adresów IP

Filtrowanie adresów IP można włączyć w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > Filtr adresów IP**. Po włączeniu tej funkcji adresy IP z listy mogą uzyskać dostęp do produktu Axis (lub otrzymać komunikat odmowy dostępu). Wybierz opcję **Zezwalaj** lub **Odmów** z listy i kliknij przycisk **Zastosuj**, aby włączyć filtrowanie adresów IP.

Administrator może dodać maksymalnie 256 adresów IP do listy (jeden wpis może zawierać wiele adresów IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer lub HTTP over SSL) to protokół sieciowy zapewniający szyfrowane przeglądanie. Protokół HTTPS może być również używany przez użytkowników i klienty w celu sprawdzenia, czy uzyskiwany jest dostęp do właściwego urządzenia. Poziom bezpieczeństwa zapewniany przez HTTPS jest uważany za odpowiedni dla większości komercyjnych wymian danych.

Produkt Axis można skonfigurować tak, aby wymagał protokołu HTTPS podczas logowania administratora.

Aby móc korzystać z protokołu HTTPS, najpierw trzeba zainstalować certyfikat HTTPS. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > Certyfikaty**. Patrz *Certyfikaty na stronie 54*.

Aby włączyć HTTPS w produkcie Axis:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > HTTPS**.
2. Wybierz certyfikat HTTPS z listy zainstalowanych certyfikatów.
3. Możesz również kliknąć opcję **Szyfr** i wybrać algorytmy szyfrowania dla SSL.
4. Ustaw **Zasady połączenia HTTPS** dla różnych grup użytkowników.

5. Kliknij **Zapisz**, aby włączyć ustawienia.

Aby uzyskać dostęp do produktu Axis za pośrednictwem pożądanego protokołu, w polu adresu przeglądarki wpisz `https://` dla protokołu HTTPS i `http://` dla protokołu HTTP.

Port HTTPS można zmienić na stronie **Opcje systemu > Sieć >TCP/IP > Zaawansowane**.

IEEE 802.1X

IEEE 802.1X to standard dla kontroli dostępu sieciowego opartej na portach, zapewniający bezpieczne uwierzytelnianie przewodowych i bezprzewodowych urządzeń sieciowych. IEEE 802.1X jest oparty na protokole EAP (Extensible Authentication Protocol).

Aby uzyskać dostęp do sieci zabezpieczonej IEEE 802.1X, urządzenia sieciowe muszą być uwierzytelnione. Do uwierzytelnienia służy serwer, zazwyczaj **RADIUS**, taki jak FreeRADIUS i Microsoft Internet Authentication Server.

W instalacjach firmy Axis urządzenia Axis i serwer uwierzytelniający używają do identyfikacji certyfikatów cyfrowych z użyciem EAP-TLS (Extensible Authentication Protocol - Transport Layer Security). Certyfikaty są dostarczane przez **jednostkę certyfikującą** (CA). Potrzebujesz:

- certyfikatu CA w celu uwierzytelnienia serwera uwierzytelniania;
- certyfikatu klienta podpisanego przez CA w celu uwierzytelnienia produktu Axis.

Aby utworzyć i zainstalować certyfikaty, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Bezpieczeństwo > Certyfikaty**. Patrz *Certyfikaty na stronie 54*.

Aby umożliwić produktowi dostęp do sieci chronionej przez IEEE 802.1X:

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > IEEE 802.1X**.
2. Wybierz **Certyfikat CA** i **Certyfikat klienta** z list zainstalowanych certyfikatów.
3. W opcji **Ustawienia** wybierz wersję EAPOL i podaj tożsamość EAP powiązaną z certyfikatem klienta.
4. Zaznacz to pole, aby włączyć IEEE 802.1X i kliknij przycisk **Zapisz**.

Uwaga

Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w produkcie Axis powinny być zsynchronizowane z serwerem NTP. Patrz *Data i godzina na stronie 55*.

Certyfikaty

Certyfikaty służą do uwierzytelniania urządzeń w sieci. Typowe zastosowania certyfikatów obejmują szyfrowane przeglądanie stron internetowych (HTTPS), ochronę sieci za pośrednictwem IEEE 802.1X i wysyłanie powiadomień, na przykład pocztą e-mail. Urządzenia Axis mogą używać dwóch rodzajów certyfikatów:

Certyfikaty serwera/klienta – Służą do uwierzytelniania produktów Axis. Certyfikat **serwera/klienta** może mieć własny podpis lub podpis jednostki certyfikującej (CA). Certyfikaty z własnym podpisem oferują ograniczoną ochronę i można je wykorzystywać do momentu uzyskania certyfikatu CA.

Certyfikaty CA – Certyfikaty te służą do uwierzytelniania innych certyfikatów, na przykład certyfikatu serwera uwierzytelniającego w przypadku podłączenia urządzenia Axis do sieci zabezpieczonej IEEE 802.1X. Urządzenia Axis mają kilka zainstalowanych wstępnie certyfikatów CA.

Uwaga

- Po przywróceniu fabrycznych ustawień domyślnych urządzenia usuwane są wszystkie certyfikaty, poza zainstalowanymi wstępnie certyfikatami CA.
- Po przywróceniu fabrycznych ustawień domyślnych urządzenia wstępnie zainstalowane certyfikaty CA, które usunięto, zostaną zainstalowane ponownie.

Tworzenie certyfikatu z własnym podpisem

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Bezpieczeństwo > Certyfikaty**.
2. Kliknij przycisk **Utwórz certyfikat z własnym podpisem** i podaj wymagane informacje.

Tworzenie i instalowanie certyfikatu z podpisem CA

1. Tworzenie certyfikatu z własnym podpisem: .
2. Przejdź do menu **Setup > Additional Controller Configuration > System Options > Security > Certificates (Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Bezpieczeństwo > Certyfikaty)**.
3. Kliknij przycisk **Utwórz żądanie podpisania certyfikatu** i podaj wymagane informacje.
4. Skopiuj żądanie w formacie PEM i wyślij do wybranego organu certyfikującego (CA).
5. Po otrzymaniu podpisanego certyfikatu kliknij przycisk **Zainstaluj certyfikat** i wczytaj certyfikat.

Instalowanie dodatkowych certyfikatów CA

1. Przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Bezpieczeństwo > Certyfikaty**.
2. Kliknij polecenie **Instaluj certyfikat** i wczytaj certyfikat.

Data i godzina

Ustawienia daty i godziny produktu Axis można skonfigurować w pozycji menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Data i godzina**.

Bieżący czas serwera wyświetla aktualną datę i godzinę (w formacie 24-godzinnym).

Aby zmienić ustawienia daty i godziny, wybierz preferowany **Tryb wyświetlania czasu** w opcji **Nowy czas serwera**:

- **Zsynchronizuj z czasem komputera** – ustawia datę i godzinę zgodnie z zegarem komputera. Przy tej opcji data i godzina zostaną ustawione jednorazowo i nie będą automatycznie aktualizowane.
- **Zsynchronizuj z serwerem NTP** – pobiera datę i godzinę z serwera NTP. Przy tej opcji data i godzina są na bieżąco aktualizowane. Więcej informacji na temat ustawień NTP: *Konfiguracja NTP na stronie 58*.

  W przypadku używania nazwy hosta dla serwera NTP należy skonfigurować serwer DNS. Patrz *Konfiguracja DNS na stronie 57*.
- **Ustaw ręcznie** – umożliwia ręczne ustawienie daty i godziny.

W przypadku używania serwera NTP wybierz swoją **Strefę czasową** z listy rozwijanej. Jeśli jest to wymagane, zaznacz **Automatycznie dostosuj do zmiany czasu letniego**.

Sieć

Podstawowe ustawienia TCP/IP

Produkt Axis obsługuje wersję 4 IP (IPv4).

Produkt Axis może uzyskać adres IPv4 na następujące sposoby:

- **Dynamiczny adres IP** – domyślnie wybraną opcją jest **Uzyskaj adres IP przez DHCP**. Oznacza to, że produkt Axis jest ustawiony tak, aby uzyskiwać adres IP automatycznie za pośrednictwem protokołu Dynamic Host Configuration Protocol (DHCP).

  DHCP pozwala administratorom sieci zarządzać centralnie adresami IP i automatyzować ich przypisywanie.

- **Statyczny adres IP** – aby użyć statycznego adresu IP, wybierz opcję **Użyj następującego adresu IP** i podaj adres IP, maskę podsieci i domyślny router. Następnie kliknij przycisk **Zapisz**.

DHCP należy włączać tylko w razie używania powiadomień dynamicznych adresów IP lub wtedy, gdy DHCP może aktualizować serwer DNS, co umożliwia dostęp do produktu Axis według nazwy (nazwy hosta).

Jeśli włączono DHCP i nie można uzyskać dostępu do produktu, należy uruchomić narzędzie AXIS IP Utility, aby wyszukać w sieci podłączone produkty Axis, lub zresetować produkt do domyślnych ustawień fabrycznych, a następnie wykonać ponowną instalację. Informacje dotyczące przywracania domyślnych ustawień fabrycznych: *strona 63*.

ARP/Ping

Adres IP produktu można przypisywać za pomocą ARP i Ping. Instrukcje: *Przypisywanie adresu IP z użyciem ARP/Ping na stronie 56*.

Usługa ARP/Ping jest domyślnie włączona, ale jest automatycznie wyłączana po upływie dwóch minut od uruchomienia produktu lub zaraz po przypisaniu adresu IP. Aby ponownie przypisać adres IP za pomocą ARP/Ping, należy ponownie uruchomić produkt, włączając tym samym usługę ARP/Ping na dodatkowe dwie minuty.

Aby wyłączyć usługę, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe** i wyczyść opcję **Włącz ustawianie adresu IP przez usługę ARP/Ping**.

Wysyłanie poleceń ping do produktu jest nadal możliwe, gdy usługa jest wyłączona.

Przypisywanie adresu IP z użyciem ARP/Ping

Adres IP urządzenia można przypisać z użyciem ARP/Ping. Polecenie należy wprowadzić w ciągu dwóch minut od podłączenia zasilania.

1. Uzyskaj wolny statyczny adres IP w tym samym segmencie sieci, w którym znajduje się komputer.
2. Znajdź numer seryjny (S/N) na etykiecie urządzenia.
3. Otwórz wiersz polecenia i wprowadź następujące polecenia:

   Składnia Linus/Unix

   ```
   arp -s <adres IP> <numer seryjny> temp
   ping -s 408 <adres IP>
   ```

   Przykład Linux/Unix

   ```
   arp-s 192.168.0.125 00:40:8c:18:10:00 temp
   ping -s 408 192.168.0.125
   ```

   Składnia Windows (może być wymagane uruchomienie wiersza polecenia z konta administratora)

   ```
   arp-s <adres IP> <numer seryjny>
   ping -i 408 -t <adres IP>
   ```

   Przykład Windows (może być wymagane uruchomienie wiersza polecenia z konta administratora)

   ```
   arp -s 192.168.0.125 00-40-8c-18-10-00
   ping -l 408 -t 192.168.0.125
   ```

4. Uruchom ponownie urządzenie poprzez odłączenie i ponowne podłączenie złącza sieciowego.
5. Zamknij wiersz polecenia, kiedy urządzenie wyśle następującą lub podobną odpowiedź `Reply from 192.168.0.125:....`
6. Otwórz przeglądarkę i wpisz `http://<adres IP>` w polu adresu.

Inne metody przypisywania adresu IP opisano w dokumencie *Przypisywanie adresu IP i uzyskiwanie dostępu do urządzenia* na stronie *www.axis.com/support*

Uwaga

- Aby otworzyć wiersz polecenia w systemie Windows, otwórz menu **Start** i wyszukaj `cmd`.
- Aby użyć polecenia ARP w systemach Windows 8/Windows 7/Windows Vista, kliknij prawym przyciskiem myszy wiersz polecenia i wybierz **Uruchom jako administrator**.
- Aby otworzyć wiersz polecenia w systemie Mac OS X, otwórz **Narzędzie terminal** w menu **Aplikacja > Narzędzia**.

AXIS Video Hosting System (AVHS)

System AVHS w połączeniu z usługą AVHS zapewnia łatwe i bezpieczne połączenie z internetem w celu zarządzania kontrolerami i dziennikami z dowolnej lokalizacji. Aby uzyskać więcej informacji znaleźć lokalnego dostawcę usług AVHS, odwiedź stronę www.axis.com/hosting

Ustawienia AVHS można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**. Możliwość połączenia z usługą AVHS jest włączona domyślnie. Aby ją wyłączyć, wyczyść pole **Włącz AVHS**.

Włączona obsługa jednym kliknięciem – Naciśnij i przytrzymaj przycisk Control produktu (patrz *Informacje ogólne o produkcie na stronie 4*) przez około trzy sekundy, aby połączyć się z usługą AVHS przez internet. Po rejestracji funkcja **Zawsze** będzie włączona, a produkt Axis pozostanie podłączony do usługi AVHS. Jeśli produkt nie zostanie zarejestrowany w ciągu 24 godzin od naciśnięcia przycisku, produkt zostanie odłączony od usługi AVHS.

Zawsze – Produkt Axis stale próbuje połączyć się z usługą AVHS przez internet. Po zarejestrowaniu produkt pozostanie podłączony do usługi. Ta opcja może być używana, gdy produkt jest już zainstalowany i nie można korzystać z instalacji jednym kliknięciem lub jest to niewygodne.

Uwaga

Wsparcie AVHS zależy od dostępności subskrypcji od usługodawców.

Usługa AXIS Internet Dynamic DNS Service

Usługa AXIS Internet Dynamic DNS Service przypisuje nazwę hosta, aby umożliwić łatwy dostęp do produktu. Więcej informacji: *www.axiscam.net*

Aby zarejestrować produkt Axis w usłudze AXIS Internet Dynamic DNS Service, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**. W menu **Usługi** kliknij przycisk **Ustawienia** usługi AXIS Internet Dynamic DNS Service (wymaga dostępu do Internetu). Nazwę domeny zarejestrowaną aktualnie w usłudze AXIS Internet Dynamic DNS Service dla danego produktu można w dowolnym momencie usunąć.

Uwaga

Usługa AXIS Internet Dynamic DNS Service wymaga protokołu IPv4.

Zaawansowane ustawienia TCP/IP

Konfiguracja DNS

Usługa DNS (Domain Name Service) zapewnia tłumaczenie nazw hostów na adresy IP. Ustawienia DNS można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.

Wybierz polecenie **Uzyskaj adres serwera DNS za pośrednictwem DHCP**, aby wykorzystać ustawienia DNS dostarczone przez serwer DHCP.

Aby wprowadzić ustawienia ręczne, wybierz **Użyj następującego adresu serwera DNS** i określ następujące ustawienia:

Nazwa domeny – Wprowadź domenę (domeny), aby wyszukać nazwę hosta używaną przez produkt Axis. Nazwy domen można oddzielić średnikami. Nazwa hosta jest zawsze pierwszą częścią pełnej nazwy domeny, na przykład `myserver` to nazwa hosta w pełnej nazwie domeny `myserver.mycompany.com`, gdzie `mycompany.com` jest nazwą domeny.

Podstawowy/dodatkowy serwer DNS – Wprowadź adresy IP podstawowego i dodatkowego serwera DNS. Dodatkowy serwer DNS jest opcjonalny i będzie używany, jeśli podstawowy jest niedostępny.

Opcje systemu

Konfiguracja NTP

Protokół NTP (Network Time Protocol) służy do synchronizacji czasu zegarów urządzeń w sieci. Ustawienia NTP można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.

Wybierz polecenie **Uzyskaj adres serwera NTP za pośrednictwem DHCP**, aby wykorzystać ustawienia NTP dostarczone przez serwer DHCP.

Aby wprowadzić ustawienia ręczne, wybierz opcję **Użyj następującego adresu serwera NTP** i wprowadź nazwę hosta lub adres IP serwera NTP.

Konfiguracja nazwy hosta

Dostęp do produktu Axis można uzyskać przy użyciu nazwy hosta zamiast adresu IP. Nazwa hosta jest zwykle taka sama jak przypisana nazwa DNS. Nazwę hosta można skonfigurować w menu **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced** .

Wybierz opcję **Uzyskaj nazwę hosta za pośrednictwem IPv4 DHCP**, aby używać nazwy hosta dostarczonej przez serwer DHCP bazujący na protokole IPv4.

Wybierz opcję **Użyj nazwy hosta**, aby ręcznie ustawić nazwę hosta.

Wybierz opcję **Włącz dynamiczne aktualizacje DNS**, aby dynamicznie aktualizować lokalne serwery DNS za każdym razem, gdy zmienia się adres IP produktu Axis. Więcej informacji można znaleźć w pomocy online.

Adres IPv4 lokalnego powiązania

Adres lokalnego powiązania jest domyślnie włączony i powoduje przypisanie produktowi Axis dodatkowego adresu IP, który może służyć do dostępu do produktu z innych hostów należących do tego samego segmentu sieci lokalnej. Produkt może mieć równocześnie adres IP lokalnego powiązania oraz adres statyczny i dynamiczny (DHCP).

Funkcję tę można wyłączyć w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.

HTTP

Port HTTP używany przez produkt Axis można zmienić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**. Oprócz ustawienia domyślnego (czyli 80) można używać dowolnego portu w zakresie 1024–65535.

HTTPS

Numer portu HTTPS używanego przez produkt Axis można zmienić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**. Oprócz ustawienia domyślnego (czyli 443) można używać dowolnego portu w zakresie 1024–65535.

Aby włączyć HTTPS, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zabezpieczenia > HTTPS**. Więcej informacji: *HTTPS na stronie 53*.

NAT traversal (mapowanie portów) dla IPv4.

Router sieciowy umożliwia urządzeniom w sieci prywatnej (LAN) współdzielić jedno połączenie internetowe. Odbywa się to poprzez przekazanie ruchu sieciowego z sieci prywatnej „na zewnątrz", czyli do internetu. Bezpieczeństwo w sieci prywatnej (LAN) jest większe, ponieważ większość routerów jest wstępnie skonfigurowana tak, aby zatrzymać próby uzyskania dostępu do sieci prywatnej (LAN) z sieci publicznej (internetu).

Użyj opcji **NAT traversal**, gdy produkt Axis jest podłączony do intranetu (LAN) i chcesz go udostępnić po drugiej stronie (WAN) routera NAT. Po prawidłowym skonfigurowaniu NAT traversal cały ruch HTTP do zewnętrznego portu HTTP w routerze NAT jest przekazywany do produktu.

Ustawienia NAT traversal można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.

Uwaga

- Aby ta funkcja działała, produkt musi obsługiwać NAT traversal. Router musi również obsługiwać protokół UPnP®.
- W tym kontekście router oznacza dowolne urządzenie działające jako router sieciowy, takie jak router NAT, router sieciowy, bramka internetowa, router szerokopasmowy, urządzenie do udostępniania szerokopasmowego lub oprogramowanie, takie jak zapora.

Włącz/Wyłącz – Po włączeniu produkt Axis próbuje skonfigurować mapowanie portów w routerze NAT w sieci przy użyciu UPnP. Protokół UPnP musi być włączony w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > UPnP**.

Korzystanie z ręcznie wybranego routera NAT – Wybierz tę opcję, aby ręcznie wybrać router NAT i wprowadź w polu adres IP routera. Jeśli nie zostanie określony router, urządzenie automatycznie wyszuka routery NAT w sieci. Jeśli zostanie wykryty więcej niż jeden router, wybrany zostanie domyślny router.

Alternatywny port HTTP – Wybierz tę opcję, aby ręcznie zdefiniować zewnętrzny port HTTP. Wprowadź numer portu z zakresu 1024–65535. Jeśli pole portu jest puste lub zawiera ustawienie domyślne, czyli 0, numer portu jest wybierany automatycznie po włączeniu NAT traversal.

Uwaga

- Alternatywny port HTTP może być używany lub aktywny, nawet wtedy, gdy opcja NAT traversal jest wyłączona. Jest to przydatne wtedy, gry router NAT nie obsługuje UPnP i trzeba ręcznie skonfigurować przekazywanie portów w routerze NAT.
- Jeśli spróbujesz ręcznie wprowadzić port, który jest już w użyciu, automatycznie wybrany zostanie inny dostępny port.
- Automatycznie wybrany port jest wyświetlany w tym polu. Aby to zmienić, wprowadź nowy numer portu i kliknij przycisk **Zapisz**.

FTP

Serwer FTP produktów Axis umożliwia wczytywanie nowego oprogramowania sprzętowego, niestandardowych aplikacji itp. Można go wyłączyć w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**.

RTSP

Serwer RTSP produktu Axis umożliwia podłączającemu się klientowi przesyłanie zdarzeń strumieniowo. Numer portu RTSP można zmienić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Zaawansowane**. Domyślny port to 554.

Uwaga

Przesyłanie zdarzeń strumieniowo nie będzie dostępne, jeśli serwer RTSP zostanie wyłączony.

SOCKS

SOCKS to protokół sieciowy serwera proxy. Produkt Axis można skonfigurować tak, do dostępu do sieci po drugiej stronie zapory lub serwera proxy używał serwera SOCKS. Funkcja ta jest przydatna, jeśli produkt Axis znajduje się w sieci lokalnej za zaporą, a do miejsca przeznaczenia spoza sieci lokalnej (na przykład internetu) konieczne jest przesyłanie powiadomień, plików, alarmów itp.

SOCKS konfiguruje się w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > SOCKS**. Więcej informacji można znaleźć w pomocy online.

QoS (Quality of Service)

Protokół QoS (Quality of Service) gwarantuje określony poziom konkretnego zasobu na potrzeby wybranego ruchu w sieci. Sieć obsługująca protokół QoS nadaje priorytet ruchowi w sieci i zapewnia większą niezawodność dzięki kontrolowaniu przepustowości, jaką może wykorzystywać aplikacja.

Ustawienia QoS można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > QoS**. Korzystając z wartości DSCP (Differentiated Services Codepoint), produkt Axis może oznaczać ruch związany ze zdarzeniem/alarmem i ruch związany z zarządzaniem.

Opcje systemu

SNMP

Protokół zarządzania urządzeniami sieciowymi Simple Network Management Protocol (SNMP) umożliwia zdalne zarządzanie urządzeniami sieciowymi. Społeczność SNMP to grupa urządzeń i stacja zarządzająca z ustanowionym protokołem SNMP. Do identyfikacji grup używa się nazw społeczności.

Aby włączyć i skonfigurować SNMP w produkcie Axis, przejdź do strony **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > SNMP**.

Zależnie od wymaganego poziomu bezpieczeństwa wybierz wersję SNMP, której chcesz użyć.

Pułapki są wykorzystywane przez produkt Axis, aby wysyłać do systemu zarządzania komunikaty dotyczące ważnych zdarzeń i zmian stanu. Zaznacz pole **Włącz pułapki** i wprowadź adres IP lokalizacji, do której ma zostać przesłany komunikat pułapki oraz **Społeczność pułapki**, która powinna otrzymać komunikat.

Uwaga

Jeśli włączono HTTPS, SNMP v1 i SNMP v2c należy wyłączyć.

Pułapki dla SNMP v1/v2 są wykorzystywane przez produkt Axis, aby wysyłać do systemu zarządzania komunikaty dotyczące ważnych zdarzeń i zmian stanu. Zaznacz pole **Włącz pułapki** i wprowadź adres IP lokalizacji, do której ma zostać przesłany komunikat pułapki oraz **Społeczność pułapki**, która powinna otrzymać komunikat.

Dostępne są następujące pułapki:

- Zimny rozruch
- Ciepły rozruch
- Powiąż
- Niepowodzenie uwierzytelniania

SNMP v3 zapewnia szyfrowanie i bezpieczne hasła. Aby można było korzystać z pułapek z SNMP v3, wymagana jest aplikacja do zarządzania SNMP v3.

Aby można było korzystać z SNMP v3, należy włączyć HTTPS, patrz *HTTPS na stronie 53*. Aby włączyć SNMP v3, zaznacz pole i wprowadź wstępne hasło użytkownika.

Uwaga

Wstępne hasło można ustawić tylko raz. W przypadku utraty hasła produkt Axis należy zresetować do domyślnych ustawień fabrycznych, patrz *Przywróć domyślne ustawienia fabryczne na stronie 63*.

UPnP

Produkt Axis obsługuje protokół UPnP®. Protokół UPnP jest domyślnie włączony, a produkt jest automatycznie wykrywany przez systemy operacyjny i klienty obsługujące ten protokół.

Protokół UPnP można wyłączyć w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > UPnP**.

Bonjour

Produkt Axis obsługuje protokół Bonjour. Protokół Bonjour jest domyślnie włączony, a produkt jest automatycznie wykrywany przez systemy operacyjny i klienty obsługujące ten protokół.

Protokół Bonjour można wyłączyć w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > Bonjour**.

Opcje systemu

Porty i urządzenia

Porty I/O

Złącze pomocnicze produktu Axis zapewnia dwa konfigurowalne porty wejścia i wyjścia do podłączania urządzeń zewnętrznych. Informacje na temat podłączania urządzeń zewnętrznych znajdują się w instrukcji instalacji dostępnej na stronie *www.axis.com*.

Porty I/O można skonfigurować w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Porty i urządzenia > Porty I/O**. Wybierz kierunek portu (**Wejście** lub **Wyjście**). Portom można nadać nazwy opisowe, a ich **Stany normalne** można skonfigurować jako **Obwód otwarty** lub **Obwód uziemienia**.

Status portu

Lista na stronie **Opcje systemu > Porty i urządzenia > Status portu** informuje o statusie portów wejścia i wyjścia produktu.

Konserwacja

Produkt Axis ma kilka funkcji służących do konserwacji. Są one dostępne w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.

Gdy produkt Axis działa niezgodnie z oczekiwaniami, kliknij przycisk **Uruchom ponownie**, aby ponownie uruchomić produkt. Nie wpłynie to na żadne bieżące ustawienia.

Uwaga

Ponowne uruchomienie spowoduje skasowanie wszystkich wpisów w raporcie o serwerze.

Kliknij przycisk **Przywróć**, aby zresetować większość ustawień do domyślnych wartości fabrycznych. Nie ma to wpływu na następujące ustawienia:

- protokół uruchamiania (DHCP lub stały adres),
- stały adres IP,
- router domyślny,
- maska podsieci,
- czas systemowy,
- ustawienia 802.1X,

Kliknij przycisk **Domyślne**, aby zresetować większość ustawień, w tym adres IP, do domyślnych wartości fabrycznych. Tego przycisku należy używać z rozwagą. Produkt Axis można również przywrócić do domyślnych ustawień fabrycznych za pomocą przycisku Control, patrz *Przywróć domyślne ustawienia fabryczne na stronie 63*.

Informacje dotyczące aktualizacji oprogramowania sprzętowego: *Aktualizacja oprogramowania sprzętowego na stronie 64*.

Tworzenie kopii zapasowej danych aplikacji

Przejdź do menu **Setup > Create a backup (Konfiguracja > Utwórz kopię zapasową)**, aby utworzyć kopię zapasową danych aplikacji. Dane w kopii zapasowej obejmują użytkowników, poświadczenia, grupy i harmonogramy. Podczas tworzenia kopii zapasowej plik zawierający dane jest zapisywany lokalnie na komputerze.

Przejdź do menu **Setup > Upload a backup (Konfiguracja > Wczytaj kopię zapasową)**, aby użyć utworzonego wcześniej pliku kopii zapasowej w celu przywrócenia danych aplikacji. Przed wczytaniem pliku kopii zapasowej należy przywrócić domyślne ustawienia fabryczne urządzenia. Instrukcje: *Przywróć domyślne ustawienia fabryczne na stronie 63*.

Support (Pomoc techniczna)

Informacje ogólne o pomocy technicznej

Jeśli potrzebujesz pomocy technicznej, na stronie **Ustawienia > Dodatkowa konfiguracja sterowników > Opcje systemu > Pomoc techniczna > Informacje ogólne o pomocy technicznej** znajdują się informacje na temat rozwiązywania problemów i dane kontaktowe.

Patrz także *Rozwiązywanie problemów na stronie 64*.

Przegląd systemu

Aby wyświetlić ogólny status produktu Axis i jego ustawienia, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Pomoc techniczna > Przegląd systemu**. Można tutaj znaleźć takie informacje, jak wersja oprogramowania sprzętowego, adres IP, ustawienia sieci i zabezpieczeń, ustawienia zdarzeń i najnowsze wpisy do dziennika.

Dzienniki i raporty

Na stronie **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Pomoc techniczna > Dzienniki i raporty** można wygenerować dzienniki i raporty umożliwiające analizę systemu oraz rozwiązywanie problemów. W przypadku kontaktu z działem wsparcia technicznego Axis należy dołączyć raport systemowy do zgłoszenia.

Dziennik systemu – Zawiera informacje o zdarzeniach systemowych.

Dziennik dostępu – Zawiera wykaz wszystkich nieudanych prób dostępu do produktu. Dziennik dostępu można również skonfigurować tak, aby wyświetlić listę wszystkich połączeń z produktem (patrz poniżej).

Wyświetl raport o serwerze – Opcja ta służy do wyświetlenia statusu produktu w oknie wyskakującym. W raporcie o serwerze automatycznie umieszczany jest dziennik dostępu.

Pobierz raport o serwerze – Opcja ta służy do utworzenia pliku ZIP, który zawiera pełny raport o serwerze w pliku tekstowym w formacie UTF–8. Aby dołączyć zrzut ekranu ze strony podglądu na żywo produktu, wybierz opcję **Dołącz ujęcie z podglądu na żywo**. Plik ZIP należy zawsze dołączać do korespondencji z działem pomocy technicznej.

Lista parametrów – Wyświetla parametry produktów i ich bieżące ustawienia. Lista ta może być szczególnie przydatna podczas rozwiązywania problemów lub korespondencji z działem pomocy technicznej Axis.

Lista połączeń – Lista wszystkich klientów mających bieżący dostęp do strumieni mediów.

Raport o awarii – Opcja ta służy do generowania archiwum z informacjami o usuwaniu błędów. Wygenerowanie tego raportu trwa kilka minut.

Poziomy dzienników systemu i dostępu można ustawić w menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Pomoc techniczna > Dzienniki i raporty > Konfiguracja**. Dziennik dostępu można skonfigurować tak, aby wyświetlić listę wszystkich połączeń z produktem (wybierz opcję Krytyczne, Ostrzeżenia i informacje).

Zaawansowane

Używanie skryptów

Dzięki skryptom doświadczeni użytkownicy mogą personalizować i wykorzystywać własne skrypty.

POWIADOMIENIE

Nieprawidłowe korzystanie z tej funkcji może spowodować nieoczekiwane zachowanie i utratę kontaktu z produktem Axis.

Axis stanowczo odradza korzystanie z tej funkcji użytkownikom, którzy nie rozumieją konsekwencji. Dział wsparcia technicznego Axis nie zapewnia pomocy w razie problemów ze spersonalizowanymi skryptami.

Aby otworzyć Edytor skryptów, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zaawansowane > Skrypty**. Jeśli skrypt powoduje problemy, zresetuj produkt do domyślnych ustawień fabrycznych: *strona 63*.

Więcej informacji: *www.axis.com/developer*

Przesyłanie plików

Pliki, na przykład strony internetowe i obrazy, można przesłać do produktu Axis i użyć jako opcji ustawień domyślnych. Aby przesłać plik, przejdź do menu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Zaawansowane > Przesyłanie plików**.

Dostęp do przesłanych plików można uzyskać pod adresem `http://<ip address>/local/<user>/<file name>`, gdzie `<user>` to wybrana grupa użytkowników (administratorzy) przesłanego pliku.

Przywróć domyślne ustawienia fabryczne

Ważne

Przywracanie domyślnych ustawień fabrycznych należy stosować rozważnie. Opcja resetowania do domyślnych ustawień fabrycznych powoduje przywrócenie wszystkich domyślnych ustawień fabrycznych produktu, włącznie z adresem IP.

Przywracanie domyślnych ustawień fabrycznych produktu:

1. Odłącz zasilanie produktu.
2. Naciśnij i przytrzymaj przycisk Control i włącz zasilanie. Patrz *Informacje ogólne o produkcie na stronie 4*.
3. Przytrzymuj przycisk Control przez 25 sekund, aż wskaźnik LED stanu ponownie zmieni kolor na bursztynowy.
4. Zwolnij przycisk Control. Proces zostanie zakończony, gdy wskaźnik LED stanu zmieni kolor na zielony. Produkt zostanie zresetowany do domyślnych ustawień fabrycznych. Jeśli w sieci brak serwera DHCP, domyślny adres IP to `192.168.0.90`.
5. Użyj narzędzi do instalacji i zarządzania, aby przypisać adres IP, ustawić hasło i uzyskać dostęp do produktu.

Parametry można również zresetować do domyślnych ustawień fabrycznych przez interfejs WWW. Wybierz kolejno **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Ustawienia > Konfiguracja dodatkowego sterownika > Konfiguracja > Opcje systemu > Konserwacja)** i kliknij opcję **Default (Domyślne)**.

Rozwiązywanie problemów

Sprawdzanie bieżącej wersji oprogramowania sprzętowego

Oprogramowanie sprzętowe określa dostępne funkcje urządzeń sieciowych. Podczas rozwiązywanie problemów należy zawsze najpierw sprawdzić bieżącą wersję oprogramowani sprzętowego. Najnowsza wersja może zawierać poprawki, które rozwiążą problem.

Bieżąca wersja oprogramowania sprzętowego produktu Axis wyświetlana jest na stronie przeglądu systemu.

Aktualizacja oprogramowania sprzętowego

Ważne

- Sprzedawca zastrzega sobie prawo do naliczenia opłaty za wszelkie naprawy spowodowane nieprawidłowym przeprowadzeniem aktualizacji przez użytkownika.
- Wstępnie skonfigurowane i spersonalizowane ustawienia są zapisywane podczas aktualizacji oprogramowania sprzętowego (pod warunkiem że funkcje te są dostępne w nowym oprogramowaniu sprzętowym), choć Axis Communications AB tego nie gwarantuje.
- Po zainstalowaniu poprzedniej wersji oprogramowania sprzętowego trzeba przywrócić domyślne ustawienia fabryczne produktu.

Uwaga

- Po zakończeniu aktualizacji produkt automatycznie uruchomi się ponownie. Jeżeli będziesz uruchamiać produkt po aktualizacji ręcznie, odczekaj 5 minut, nawet jeśli podejrzewasz niepowodzenie aktualizacji.
- Pierwsze uruchomienie może potrwać kilka minut, ponieważ po aktualizacji oprogramowania sprzętowego bazy danych użytkowników, grup, ich dane uwierzytelniające i inne dane są aktualizowane. Wymagany czas zależy od ilości danych.
- Aktualizacja produktu Axis do najnowszej wersji oprogramowania sprzętowego umożliwia uaktualnienie produktu o najnowsze funkcje. Przed aktualizacją oprogramowania sprzętowego zawsze należy przeczytać instrukcje dotyczące aktualizacji oraz informacje o wersji dostępne z każdą nową wersją.

Kontrolery drzwi w trybie autonomicznym:

1. Pobierz na komputer najnowszy plik oprogramowania sprzętowego dostępny bezpłatnie na stronie *www.axis.com/support*
2. Przejdź do strony internetowej produktu **Ustawienia > Dodatkowa konfiguracja kontrolera > Opcje systemu > Konserwacja**.
3. W opcji **Aktualizuj serwer** kliknij polecenie **Wybierz plik** i wyszukaj plik na komputerze.
4. Jeżeli produkt ma automatycznie przywrócić domyślne ustawienia fabryczne po aktualizacji, zaznacz pole wyboru **Domyślne**.
5. Kliknij **Aktualizuj**.
6. Odczekaj około 5 minut na aktualizację i ponowne uruchomienie produktu. Następnie wyczyść pamięć podręczną przeglądarki.
7. Zaloguj się do produktu.

Kontrolery drzwi w systemie:

Aby zaktualizować wszystkie kontrolery drzwi w systemie, możesz użyć aplikacji AXIS Device Manager lub AXIS Camera Station. Więcej informacji znajduje się na stronie *www.axis.com*.

Ważne

- Nie wybieraj aktualizacji sekwencyjnych.

Uwaga

- Wszystkie kontrolery w systemie zawsze muszą mieć tę samą wersję oprogramowania sprzętowego.
- Aby zaktualizować wszystkie kontrolery drzwi w systemie, użyj opcji aktualizacji jednoczesnej aplikacji AXIS Device Manager lub AXIS Camera Station.

Awaryjna procedura przywracania

Jeśli podczas aktualizacji nastąpi utrata zasilania lub połączenia sieciowego, proces się nie powiedzie i produkt może przestać reagować. Migający na czerwono wskaźnik stanu wskazuje na nieudaną aktualizację. Aby przywrócić działanie produktu, wykonaj poniższe czynności. Numer seryjny jest wydrukowany na etykiecie produktu.

1. W systemie **UNIX/Linux** wprowadź następujące polecenie z wiersza poleceń:

   ```
   arp -s <adres IP> <numer seryjny> temp
   ping -l 408 <adres IP>
   ```

   W systemie **Windows** wprowadź następujące polecenie w wierszu poleceń / okienku DOS (może to wymagać uruchomienia wiersza poleceń jako administrator):

   ```
   arp-s <adres IP> <numer seryjny>
   ping -i 408 -t <adres IP>
   ```

2. Jeśli produkt nie odpowie w ciągu 30 sekund, uruchom go ponownie i poczekaj na odpowiedź. Naciśnij CTRL+C, aby zatrzymać proces Ping.
3. Otwórz przeglądarkę i wpisz adres IP produktu. Na stronie, która się otworzy, użyj przycisku **Przeglądaj**, aby wybrać plik aktualizacji, którego chcesz użyć. Następnie kliknij **Wczytaj**, aby wznowić proces aktualizacji.
4. Po zakończeniu aktualizacji (1-10 minut) urządzenie automatycznie uruchomi się ponownie i zacznie świecić na zielono na wskaźniku stanu.
5. Zainstaluj ponownie produkt, korzystając z podręcznika instalacji.

Jeśli awaryjna procedura przywracania nie spowoduje ponownego uruchomienia produktu, skontaktuj się z działem pomocy firmy Axis pod adresem *www.axis.com/support*

Objawy, możliwe przyczyny i sposoby naprawy

Problemy z aktualizacją oprogramowania sprzętowego	
Niepowodzenie podczas aktualizacji oprogramowania sprzętowego	Jeśli aktualizacja oprogramowania sprzętowego zakończy się niepowodzeniem, produkt załaduje ponownie poprzednią wersję oprogramowania sprzętowego. Sprawdź plik oprogramowania sprzętowego i spróbuj ponownie.

Problemy z ustawieniem adresu IP	
Podczas korzystania z ARP/Ping	Spróbuj ponownej instalacji. Adres IP należy ustawić w ciągu dwóch minut po doprowadzeniu zasilania do produktu. Upewnij się, że długość Ping jest równa 408. Instrukcje znajdują się w instrukcji instalacji na stronie produktu w witrynie *axis.com*.
Produkt należy do innej podsieci	Jeśli adres IP przeznaczony dla danego produktu oraz adres IP komputera używanego do uzyskania dostępu do produktu należą do różnych podsieci, ustawienie adresu IP będzie niemożliwe. Skontaktuj się z administratorem sieci, aby uzyskać adres IP.

Rozwiązywanie problemów

Adres IP jest używany przez inne urządzenie	Odłącz produkt Axis od sieci. Uruchom polecenie Ping (w oknie polecenia/DOS wpisz `ping` oraz adres IP produktu): • Jeśli otrzymasz odpowiedź: `Reply from <adres IP>: bytes=32; time=10...`, oznacza to, że ten adres IP może już być używany przez inne urządzenie w sieci. Poproś administratora sieci o nowy adres IP i zainstaluj ponownie produkt. • Jeśli otrzymasz odpowiedź: `Request timed out`, oznacza to, że ten adres IP jest dostępny do wykorzystania przez produkt Axis. Sprawdź całe okablowanie i zainstaluj produkt ponownie.
Możliwy konflikt adresów IP z innym urządzeniem w tej samej podsieci	Zanim serwer DHCP ustawi adres dynamiczny, używany jest statyczny adres IP produktu Axis. Oznacza to, że jeśli ten sam domyślny statyczny adres IP jest używany także przez inne urządzenie, mogą wystąpić problemy podczas uzyskiwania dostępu do produktu.

Nie można uzyskać dostępu do produktu przez przeglądarkę

Nie można się zalogować	Jeśli protokół HTTPS jest włączony, trzeba upewnić się, że podczas logowania używany jest właściwy protokół (HTTP lub HTTPS). Może zajść konieczność ręcznego wpisania `http` lub `https` w polu adresu przeglądarki. W razie utraty hasła dla użytkownika root należy przywrócić ustawienia fabryczne produktu. Patrz *Przywróć domyślne ustawienia fabryczne na stronie 63*.
Serwer DHCP zmienił adres IP	Adresy IP otrzymane z serwera DHCP są dynamiczne i mogą się zmieniać. Jeśli adres IP został zmieniony, użyj narzędzia AXIS IP Utility lub AXIS Device Manager, aby zlokalizować produkt w sieci. Znajdź produkt przy użyciu nazwy modelu lub numeru seryjnego produktu bądź nazwy DNS (jeśli skonfigurowano tę nazwę). W razie potrzeby można przydzielić samodzielnie statyczny adres IP. Instrukcje znajdują się w dokumencie *Jak przypisać adres IP i uzyskać dostęp do urządzenia* na stronie produktu w witrynie *axis.com*
Błąd certyfikatu podczas korzystania ze standardu IEEE 802.1X	Aby uwierzytelnianie działało prawidłowo, ustawienia daty i godziny w produkcie Axis powinny być zsynchronizowane z serwerem NTP. Patrz *Data i godzina na stronie 55*.

Dostęp do produktu można uzyskać lokalnie, ale nie z zewnątrz

Konfiguracja routera	Aby skonfigurować router i umożliwić przesyłanie danych do produktu Axis, włącz funkcję NAT-traversal (przechodzenie portów), która spróbuje automatycznie skonfigurować router, umożliwiając dostęp do produktu Axis; patrz *NAT traversal (mapowanie portów) dla IPv4. na stronie 58*. Router musi obsługiwać protokół UPnP®.
Zapora	Poproś administratora sieci, aby sprawdził, czy problemem nie jest zapora internetowa.
Wymagane domyślne routery	Sprawdź, czy należy skonfigurować ustawienia routera w menu **Ustawienia > Ustawienia sieciowe** lub **Konfiguracji > Dodatkowa konfiguracja kontrolera > Opcje systemu > Sieć > TCP/IP > Podstawowe**.

Diody LED statusu i sieci szybko migają na czerwono

Awaria sprzętu	Skontaktuj się z resellerem Axis.

Produkt nie uruchamia się

Produkt nie uruchamia się	Jeżeli nie można uruchomić produktu, nie odłączaj kabla sieciowego i ponownie włóż przewód zasilania do zasilacza midspan.

Specyfikacje

Złącza

Informacji na temat położenia złączy: .

Schematy połączeń i informacje o schemacie styków sprzętu wygenerowanym w konfiguracji sprzętu: *Schematy połączeń na stronie 71* i *Konfigurowanie sprzętu na stronie 14*.

Poniżej opisano specyfikacje złączy.

Złącze danych czytnika

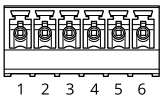
6-pinowy blok złączy obsługujący protokoły RS485 i Wiegand do komunikacji z czytnikiem.

Porty RS485 obsługują:

- RS485 half duplex (dwużyłowy)
- RS485 full duplex (czterożyłowy)

Porty Wiegand obsługują:

- Wiegand (dwużyłowy)



Funkcja		Styk	Uwagi
RS485	A-	1	Full duplex RS485 Half duplex RS485
	B+	2	
RS485	A-	3	Full duplex RS485 Half duplex RS485
	B+	4	
Wiegand	D0 (Dane 0)	5	Wiegand
	D1 (Dane 1)	6	

Ważne

Porty RS485 mają stałą prędkość transmisji wynoszącą 9600 Bit/s.

Ważne

Zalecana maksymalna długość kabla wynosi 30 m (98,4 ft).

Ważne

Obwody wyjściowe w tej sekcji mają ograniczenie mocy klasy 2.

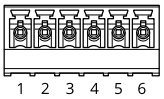
Złącze I/O czytnika

6-pinowy blok złączy na potrzeby:

- Dodatkowego zasilania (wyjście DC)
- Wejścia cyfrowego

- Wyjścia cyfrowego
- 0 V DC (-)

Styk 3 na złączach I/O czytnika może być nadzorowany. Jeśli połączenie zostanie przerwane, zostanie aktywowane zdarzenie. Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii. Dla wejść nadzorowanych użyj schematu połączeń. Patrz *strona 72*.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wyjście DC	2	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	12 V DC Maks. obciążenie = 300 mA
Konfigurowalne (wejście lub wyjście)	3–6	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 40 V DC
		Wyjście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. W przypadku stosowania z obciążeniem indukcyjnym, np przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 40 V DC, otwarty dren maks. 100 mA

Ważne

Zalecana maksymalna długość kabla wynosi 30 m (98,4 ft).

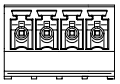
Ważne

Obwody wyjściowe w tej sekcji mają ograniczenie mocy klasy 2.

Złącze drzwi

Dwa 4-pinowe bloki złączy do urządzeń monitorujących drzwi (wejście cyfrowe).

Wszystkie styki wejściowe drzwi mogą być nadzorowane. Alarm wyzwalany jest po przerwaniu połączenia. Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii. Dla wejść nadzorowanych użyj schematu połączeń. Patrz *strona 72*.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1, 3		0 V DC
Wejście	2, 4	Do komunikacji z monitorem drzwi. Wejście cyfrowe — podłącz do styku 1 lub 3, aby aktywować lub pozostaw rozłączone, aby dezaktywować. Uwaga: ten styk może być używany tylko jako wejście.	Od 0 do maks. 40 V DC

Ważne

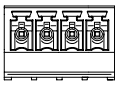
Zalecana maksymalna długość kabla wynosi 30 m (98,4 ft).

Złącze pomocnicze

4-pinowy konfigurowalny blok złączy I/O na potrzeby:

- Dodatkowego zasilania (wyjście DC)
- Wejścia cyfrowego
- Wyjścia cyfrowego
- 0 V DC (-)

Przykładowy schemat połączeń: *Schematy połączeń na stronie 71*.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wyjście DC	2	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	3,3 V DC Maks. obciążenie = 100 mA
Konfigurowalne (wejście lub wyjście)	3–4	Wejście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować.	Od 0 do maks. 40 V DC
		Wyjście cyfrowe — podłącz do styku 1, aby aktywować lub pozostaw rozłączone, aby dezaktywować. W przypadku stosowania z obciążeniem indukcyjnym, np przekaźnikiem, konieczne jest szeregowe podłączenie diody w celu zabezpieczenia przed stanami przejściowymi napięcia.	Od 0 do maks. 40 V DC, otwarty dren maks. 100 mA

Ważne

Zalecana maksymalna długość kabla wynosi 30 m (98,4 ft).

Ważne

Obwody wyjściowe w tej sekcji mają ograniczenie mocy klasy 2.

Złącze zasilania

2-pinowy blok złączy na wejście zasilania DC. Używaj urządzenia LPS zgodnego z SELV z nominalną mocą wyjściową ograniczoną do ≤100 W lub nominalnym prądem ograniczonym do ≤5 A.

Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1		0 V DC
Wejście DC	2	Do zasilania kontrolera, gdy nie jest używane zasilanie Power over Ethernet. Uwaga: ten styk może być używany tylko jako wejście zasilania.	10–28 V DC, maks. 36 W Maks. obciążenie wyjść = 14 W

Specyfikacje

Złącze sieciowe

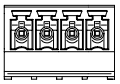
Złącze RJ45 Ethernet. Użyj kabli kategorii 5e lub wyższej.

Funkcja	Specyfikacje
Zasilanie i Ethernet	Power over Ethernet IEEE 802.3af/802.3at typ 1 klasa 3, 44–57 V DC Maks. obciążenie wyjść = 7,5 W

Złącze zasilania zamka

4-pinowy blok złączy umożliwiający podłączenie jednego lub dwóch zamków do zasilania prądem stałym. Złącza zamka można również użyć do zasilania urządzeń zewnętrznych.

Podłącz zamki i zasilanie zgodnie ze schematem styków sprzętu wygenerowanym przez konfigurację sprzętową.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1, 3		0 V DC
0 V DC, rozłączone, lub 12 V DC	2, 4	Do sterowania maksymalnie dwoma zamkami 12 V. Użyj schematu styków sprzętu. Patrz *Konfigurowanie sprzętu na stronie 14*.	12 V DC Maks. obciążenie łączne = 500 mA

POWIADOMIENIE

Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

Ważne

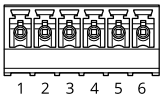
Obwody wyjściowe w tej sekcji mają ograniczenie mocy klasy 2.

Złącze zasilania i przekaźnika

6-pinowy blok złączy z wbudowanym przekaźnikiem na potrzeby:

- Urządzeń zewnętrznych
- Dodatkowego zasilania (wyjście DC)
- 0 V DC (-)

Podłącz zamki i zasilanie zgodnie ze schematem styków sprzętu wygenerowanym przez konfigurację sprzętową.



Funkcja	Styk	Uwagi	Specyfikacje
0 V DC (-)	1, 4		0 V DC

Przekaźnik	2–3	Do podłączania urządzeń przekaźnikowych. Użyj schematu styków sprzętu. Patrz *Konfigurowanie sprzętu na stronie 14*. Obwód przekaźnika jest odizolowany galwanicznie od pozostałych obwodów.	Maks. prąd = 700 mA Maks. napięcie = +30 V DC
12 V DC	5	Do zasilania urządzeń dodatkowych. Uwaga: ten styk może być używany tylko jako wyjście zasilania.	Maks. natężenie = +12 V DC Maks. obciążenie = 500 mA
24 V DC	6	Nieużywane	

POWIADOMIENIE

Jeśli zamek nie jest spolaryzowany, zalecamy dodanie zewnętrznej diody typu flyback.

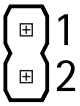
Ważne

Obwody wyjściowe w tej sekcji mają ograniczenie mocy klasy 2.

Złącze główkowe alarmu antysabotażowego

Dwa 2-pinowe złącza główkowe do obchodzenia:

- Tylnego alarmu antysabotażowego (TB)
- Przedniego alarmu antysabotażowego (TF)



Funkcja	Styk	Uwagi
Tylny alarm antysabotażowy	1–2	Aby obejść jednocześnie przedni i tylny alarm antysabotażowy, połącz zworki odpowiednio pomiędzy TB 1, TB 2 i TF 1, TF 2. Obejście alarmów antysabotażowych oznacza, że system nie wykryje prób sabotażu.
Przedni alarm antysabotażowy	1–2	

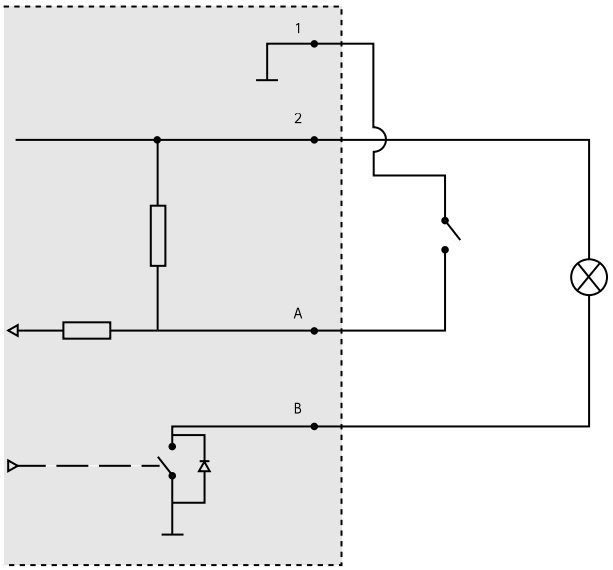
Uwaga

Zarówno przedni, jak i tylny alarm antysabotażowy są podłączone domyślnie. Wyzwalacz otwarcia obudowy można skonfigurować, aby wykonywał akcję, kiedy kontroler drzwi zostanie otwarty lub usunięty ze ściany lub sufitu. Informacje na temat konfiguracji alarmów i zdarzeń: *Konfiguracja alarmów i zdarzeń na stronie 44*.

Schematy połączeń

Podłącz urządzenia zgodnie ze schematem styków sprzętu wygenerowanym przez konfigurację sprzętową. Więcej informacji na temat konfiguracji sprzętowej i schematu styków sprzętu: *Konfigurowanie sprzętu na stronie 14*.

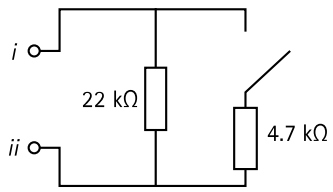
Złącze pomocnicze



1 0 V DC (-)
2 Wyjście DC: 3,3 V, maks. 100 mA
A I/O skonfigurowane jako wejście
B I/O skonfigurowane jako wyjście

Nadzorowane wejścia

Aby móc korzystać z nadzorowanych wejść, zamontuj rezystory końca linii zgodnie ze schematem poniżej.



i Wejście
ii 0 V DC (-)

Uwaga

Zaleca się korzystanie ze skrętek ekranowanych. Podłącz ekranowanie do 0 V DC.

Informacje dotyczące bezpieczeństwa

Poziomy zagrożenia

⚠NIEBEZPIECZEŃSTWO

Wskazuje zagrożenie, które spowoduje zgon lub ciężkie obrażenia.

⚠OSTRZEŻENIE

Wskazuje zagrożenie, które może spowodować zgon lub ciężkie obrażenia.

⚠UWAGA

Wskazuje zagrożenie, które może spowodować niewielkie lub umiarkowane obrażenia.

POWIADOMIENIE

Wskazuje zagrożenie, które może spowodować uszkodzenie mienia.

Inne poziomy komunikatów

Ważne

Wskazuje istotne informacje niezbędne do poprawnego działania produktu.

Uwaga

Wskazuje przydatne informacje, które ułatwiają wykorzystanie możliwości produktu.

Podręcznik użytkownika
AXIS A1001 & AXIS Entry Manager

Wer. M25.2
Data: Grudzień 2023
Numer części T10010336