NODER EE12/EWE4

Sieciowy sterownik systemów kontroli dostępu i sygnalizacji włamania i napadu

Instrukcja uruchomieniowo-konfiguracyjna

Ver.1.7_092025

1. Przed przystąpieniem do prac

Przed przystąpieniem do prac wdrożeniowych Sieciowy kontroler EE12/EWE4 musi być poprawnie zainstalowany, podłączony i uruchomiony zgodnie z DTR.

2. Opis urządzeń

Sieciowe sterowniki Systemu Kontroli Dostępu i Sygnalizacji Włamania i Napadu NODER są zaawansowanymi mikroprocesorowymi urządzeniami wejść/wyjść przeznaczonymi do zautomatyzowanej identyfikacji użytkowników. Mogą znaleźć zastosowanie w systemach bezpieczeństwa budynkowego, kontroli dostępu, rejestracji czasu pracy, obsługi obiektów hotelowych i rekreacyjnych. Systemem nadrzędnym i zarządzającym pracą sterowników jest oprogramowanie Axxon PSIM. Szczegóły na temat uruchomienia, konfiguracji ustawień sieciowych oraz podłączenia urządzeń do kontrolera znajdują się w dokumentacji technicznej kontrolerów.

3. Konfiguracja modułu Noder

W tym rozdziale zostaną opisane kolejne kroki konfiguracji modułu Noder.

3.1 Instalacja systemu

Systemy Kontroli Dostępu i Sygnalizacji Włamania i Napadu NODER działają pod oprogramowaniem Axxon PSIM. Za komunikację ze sterownikami odpowiedzialny jest dedykowany moduł „NoderEe12.run". Do poprawnej pracy z KD należy zainstalować na serwerze następujące komponenty:

Axxon PSIM Base version (w wersji 1.0.0.14 lub wyższej)
Access Control and Fire Alarm Module (w wersji 1.0.0.14 lub wyższej) z modułami:

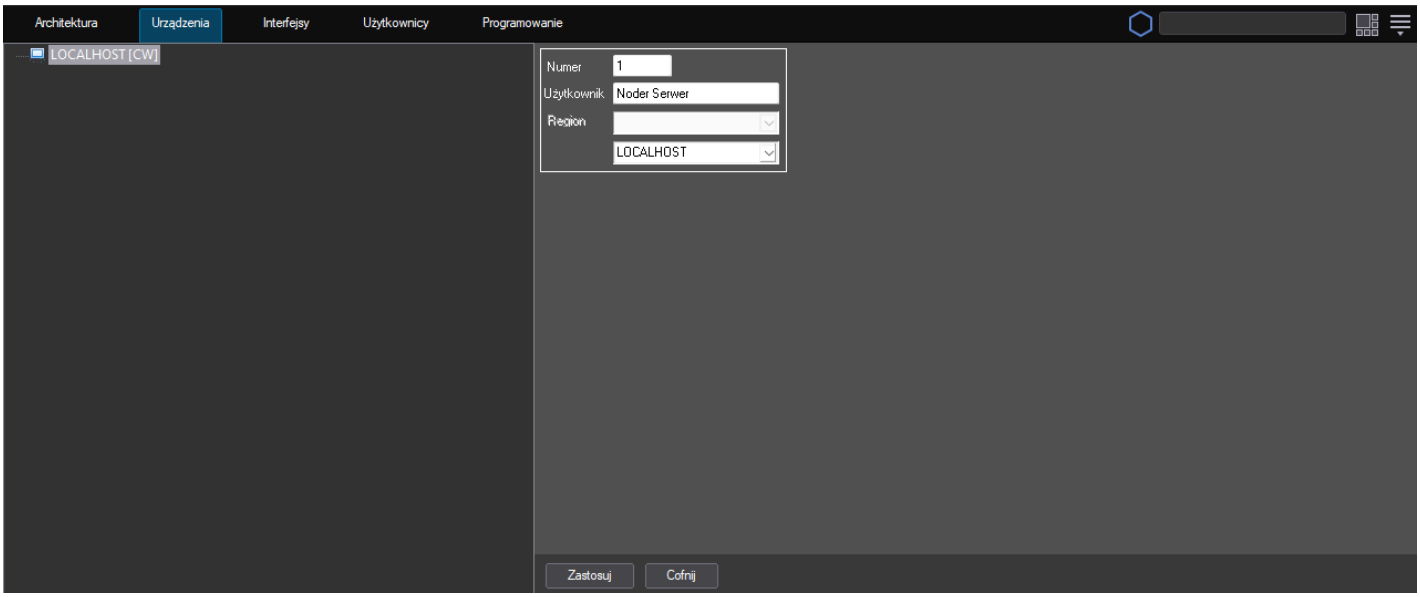
- ***Noder EE12/EWE4*** z katalogu Access Control Systems
- ***Access Manager*** z katalogu Application software

System Sygnalizacji Włamania i Napadu jest dostępny w kontrolerach EWE4 z płytkami od wersji 1.06 i EE12 od 1.08. Wersja modułu 2.1.1.204 lub wyższa, ID aktualizacji kontrolera 517 lub wyższa.

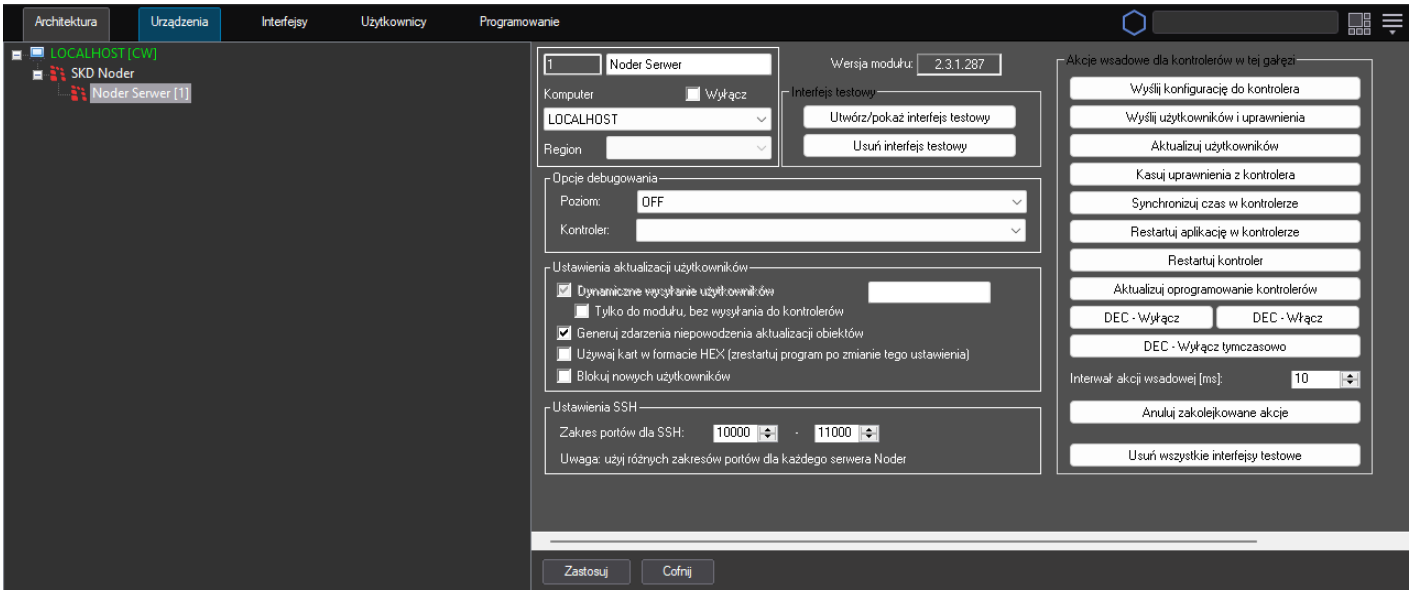
Instrukcja jest kompatybilna z kontrolerami EWE4 z płytkami od wersji 1.06 i EE12 z płytkami id wersji 1.08. Wersja modułu 2.3.1.287 lub wyższa, ID aktualizacji kontrolera 1135 lub wyższa.

3.2 Noder Serwer

Konfiguracja elementów systemu NODER odbywa się z panelu administracyjnego serwera PSIM. W zakładce ***Urządzenia*** na serwerze, na którym moduł ma pracować dodajemy nowy obiekt o nazwie ***Noder Serwer*** poprzez opcje ***Utwórz obiekt (prawy przycisk myszy na obiekt Serwer → Utwórz obiekt → Noder Serwer***. Nowy obiekt zostanie utworzony w katalogu o nazwie ***SKD Noder***.



Noder Serwer jest modułem odpowiedzialnym za komunikację z kontrolerami. ***Noder Serwer*** zawiera obiekty ***Noder Obiekt***.



Opcje debugowania – opcje dla programistów pozwalające na logowanie określonych zdarzeń z kontrolerów:

Poziom – opcja pozawala na wybranie typów logów zapisywanych do pliku.

Kontroler – opcja pozwala na wybranie kontrolera, z którego zbierane będą logi do pliku.

Ustawienia aktualizacji użytkowników:

Dynamiczne wysyłanie użytkowników – funkcjonalność umożliwia automatyczne wysyłanie użytkowników i poziomów dostępu, po każdorazowej zmianie w Menadżerze KD.

Tylko do modułu, bez wysyłania do kontrolerów – funkcja umożliwia zmianę uprawnień użytkownika, harmonogramów i poziomów dostępu, bez automatycznego wysłania zmian do kontrolera. Jeżeli opcja jest zaznaczona, każdorazową zmianę tych ustawień trzeba wysłać manualnie.

Generuj zdarzenia niepowodzenia aktualizacji obiektów– funkcja pozwala na wyświetlenie dodatkowego zdarzenia w systemie po wystąpieniu niepowodzenia przy aktualizacji obiektów.

Używaj kart w formacie HEX– funkcja pozwala zmianę zapisu numerów kart z decymalnego na szesnastkowy.

Blokuj nowych użytkowników – po zaznaczeniu opcji przy tworzeniu nowego użytkownika parametr Użytkownik zablokowany oznaczony jest jako **TAK**.

Ustawienia SSH:

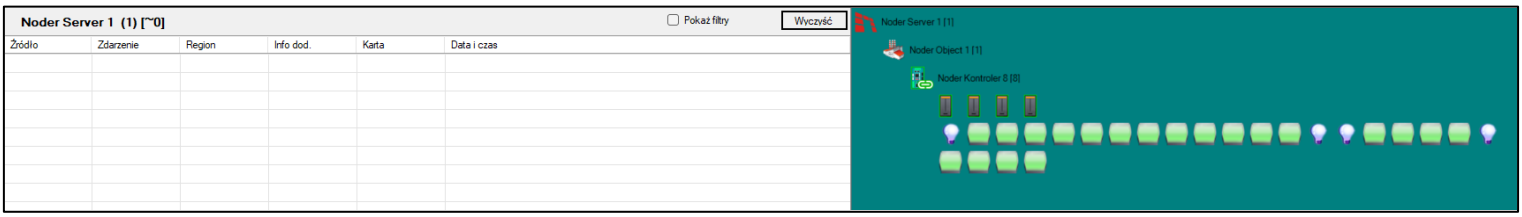
Zakres portów SSH – zakres porów używanych przy tunelowaniu SSH.

Wersja modułu – pole przedstawia aktualną wersję modułu.

Interfejsy:

Utwórz/pokaż interfejs testowy – tworzy interfejs kontrolera składający się z podglądu zdarzeń dotyczącego danego kontrolera oraz mapy z ikonami wszystkich czytników oraz wejść danego kontrolera. Jeżeli taki interfejs testowy został utworzony wcześniej ponowne wywołanie tej funkcji spowoduje odświeżenie mapy wg bieżącej konfiguracji i wyświetlenie interfejsu

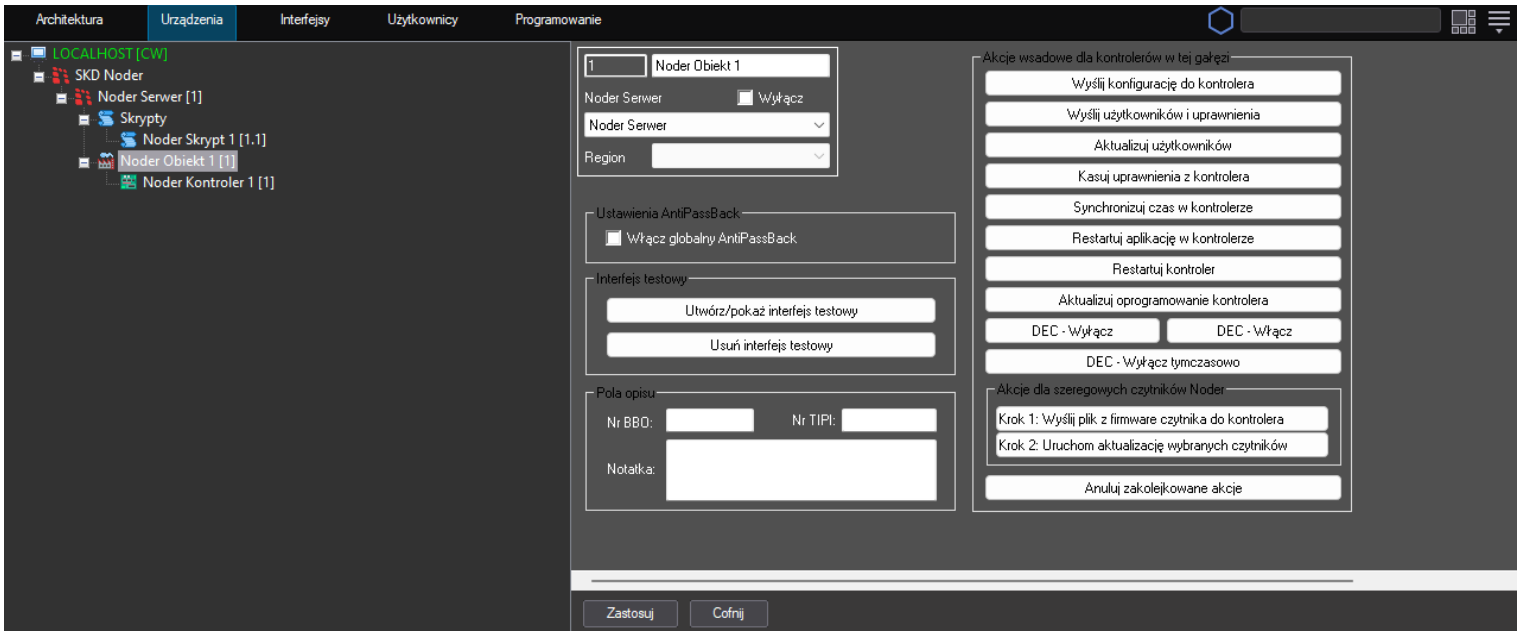
Usuń interfejs testowy – opcja usuwa utworzony wcześniej interfejs testowy.



Akcje wsadowe dla kontrolerów w tej gałęzi – sekcja pozwala na wykonanie akcji dla wszystkich kontrolerów przypisanych do serwera. W przypadku gdy jest ich więcej niż 50 akcje będą wykonywane sekwencyjnie. Informacje na temat znaczenia poszczególnych akcji opisano w rozdziale **3.4.1 Zakładka Akcje**.

3.3 Noder Obiekt

Noder Obiekt jest elementem logiczny umożliwiającym dzielenie systemu na części (piętra, budynki, działy) i zarządzanie nimi. Zawiera obiekty ***Noder Kontroler*** i ***Noder Strefa SSWiN***.



Włącz globalny AntiPassBack – opcja włącza globalny AntiPassBack na danym obiekcie. Aby działał on odpowiednio kontrolery, czytniki i użytkownicy muszą być poprawnie skonfigurowane (opisano w kolejnych rozdziałach).

Interfejsy:

Utwórz/pokaż interfejs testowy – tworzy interfejs kontrolera składający się z podglądu zdarzeń dotyczącego danego kontrolera oraz mapy z ikonami wszystkich czytników oraz wejść danego kontrolera. Jeżeli taki interfejs testowy został utworzony wcześniej ponowne wywołanie tej funkcji spowoduje odświeżenie mapy wg bieżącej konfiguracji i wyświetlenie interfejsu

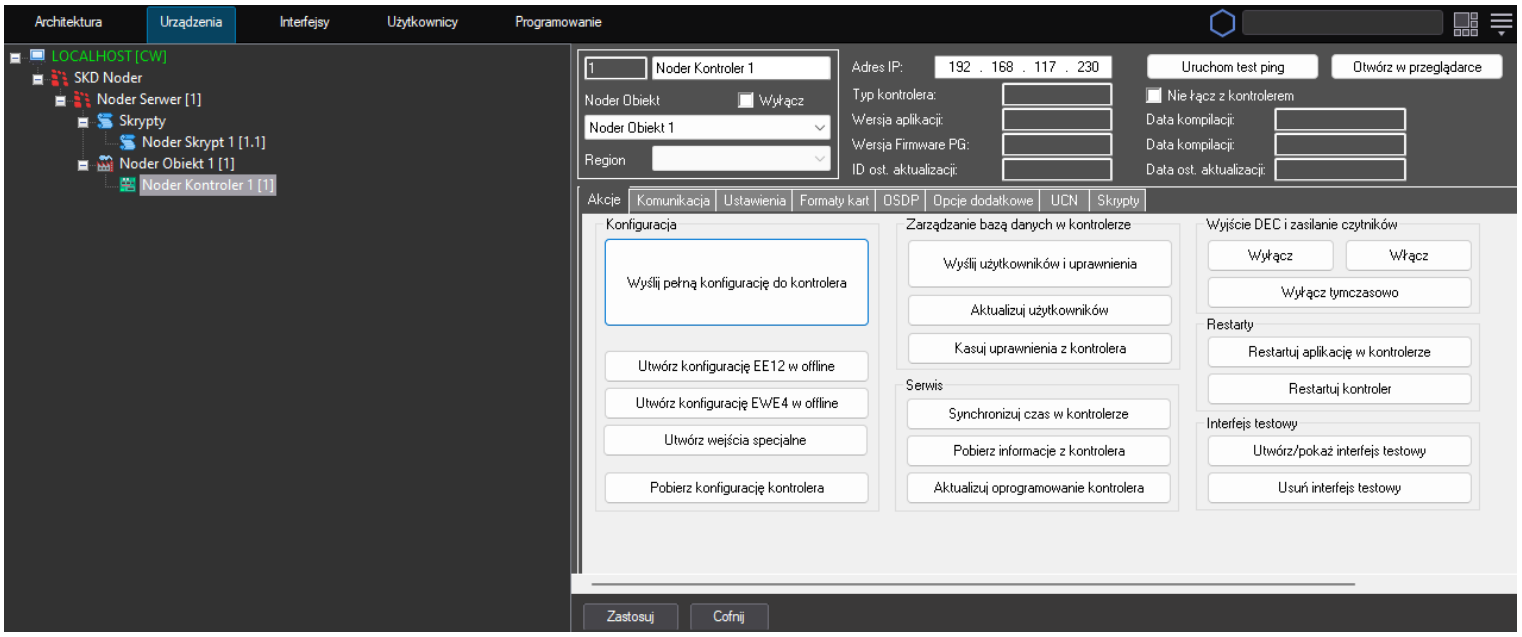
Usuń interfejs testowy – opcja usuwa utworzony wcześniej interfejs testowy.

Pola opisu – informacje o obiekcie mogą być tutaj przechowywane. Funkcjonalność ***nie wpływa na działanie kontrolera***.

Akcje wsadowe dla kontrolerów w tej gałęzi – sekcja pozwala na wykonanie akcji dla wszystkich kontrolerów przypisanych do obiektu. W przypadku gdy jest ich więcej niż 50 akcje będą wykonywane sekwencyjnie. Informacje na temat znaczenia poszczególnych akcji opisano w rozdziale **3.4.1 Zakładka Akcje**.

3.4 Noder Kontroler

Obiekt umożliwia połączenie się z kontrolerami EE12 lub EWE4. Pozwala na tworzenie jego konfiguracji i zarządzanie nim. Zawiera obiekty ***Noder Czytnik***, ***Noder Moduł IO16***, ***Noder Wejście***, ***Noder Wyjście***.

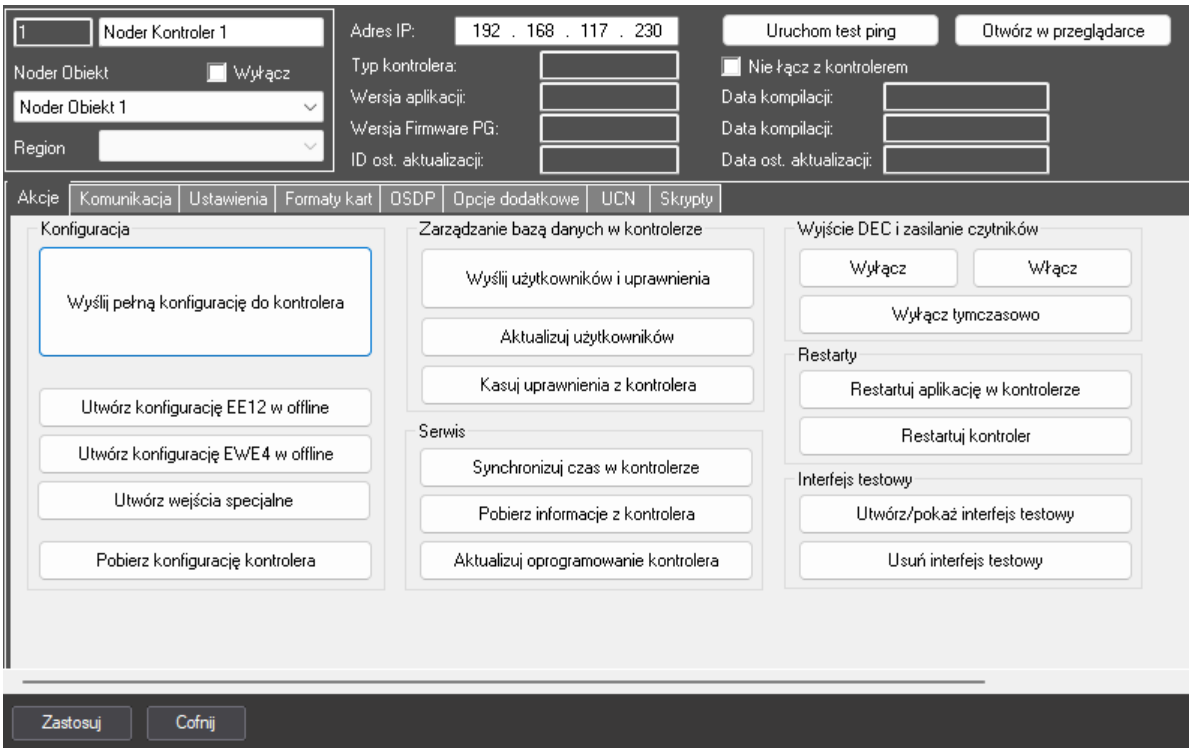


Po utworzeniu obiektu wyświetlone zostanie okno z otwartą zakładką ***Akcje***. Przed pierwszym połączeniem z urządzeniem pola ***Typ kontrolera***, ***Wersja aplikacji***, ***Data kompilacji***, ***Wersja Firmaware uC***, ***Data kompilacji***, ***ID ost. aktualizacji***, ***Data ost. aktualizacji*** pozostają puste.

Do połączenia z kontrolerem należy wpisać jego ***Adres IP***. Komenda ***Uruchom test ping*** uruchamia *Wiersz poleceń*, który monitoruje urządzenie protokołem ICMP. Opcja ***Otwórz w przeglądarce*** uruchamia domyślną przeglądarkę stron internetowych i załaduje stronę logowania do kontrolera.

3.4.1 Akcje

Zakładka umożliwia tworzenie, wysyłanie i sprawdzanie konfiguracji kontrolera i użytkowników. Pozwala na zdalny restart kontrolera i urządzeń peryferyjnych.



Konfiguracja:

Wyślij pełną konfigurację do kontrolera – opcja pozwala wysłać bieżące ustawienia do kontrolera. Opcja może być wykorzystana po utworzeniu konfiguracji w offline lub wymianie urządzenia. Jeżeli status oznaczony jako Połączony przy zmianie konfiguracji nie trzeba używać przycisku, ponieważ jest ona wysyłana dynamicznie.

Utwórz konfigurację EE12 w offline, Utwórz konfigurację EWE4 w offline – funkcja umożliwia łatwe utworzenie w konfiguracji wejść kontrolera i czytników (nawet bez jego fizycznego połączenia z Axxon PSIM), które mają być do niego podłączone. Dla kontrolera EWE4 utworzone zostanie 16 wejść i 4 czytniki, a dla EE12 20 wejść i 12 czytników. Wszystkie wejścia i czytniki będą domyślnie w stanie nieaktywnym.

Utwórz wejścia specjalne – opcja tworzy cztery predefiniowane wejścia sygnałów: rozładowania akumulatorów (BAT), braku zasilania 230V (AC), uszkodzenia zasilania 12V (TMP), naruszeniu tampera drzwiczek obudowy (DR). Wszystkie wejścia domyślnie ustawione są jako NC. Numery wejść specjalnych dla obu kontrolerów to 21-24.

Pobierz konfigurację kontrolera – opcja tworzy podstawową konfigurację kontrolera. Utworzone zostaną wejścia kontrolera w stanie wyłączonym i czytniki w stanie nieaktywnym. W przeciwieństwie do komend ***Utwórz konfigurację EE12 w offline, Utwórz konfigurację EWE4 w offline*** w przypadku braku połączenia konfiguracja nie zostanie utworzona.

Zarządzanie bazą danych w kontrolerze:

Wyślij użytkowników i uprawnienia – opcja tworzy bazę danych na nowo. Najpierw usuwani są użytkownicy i uprawnienia i wysyłani ponownie. Opcji należy używać po dodaniu nowego kontrolera do konfiguracji lub gdy zmiana konfiguracji odbywała się, gdy kontroler pracował w trybie offline. Przy dodawaniu użytkowników i uprawnień w poprawnie działającym systemie, są one wysyłane dynamicznie.

Aktualizuj użytkowników – opcja umożliwia aktualizację użytkowników. Należy jej użyć, gdy podczas aktualizacji użytkowników kontroler pracował w trybie offline.

Kasuj uprawnienia z kontrolera – opcja umożliwia usunięcie wszystkich użytkowników, poziomów dostępów i harmonogramów z bazy danych kontrolera.

Serwis:

Synchronizuj czas w kontrolerze – opcja umożliwia synchronizację czasu kontrolera z serwerem nim zarządzającym. Opcja wywoływana jest automatycznie w tle co 4 godziny.

Pobierz informacje z kontrolera – opcja umożliwia sprawdzenie informacji o kontrolerze (numer seryjny, firmware, wersja Linux), urządzeniach peryferyjnych do niego podłączonych (firmware czytników), ***napięcie zasilania kontrolera***.

Aktualizuj oprogramowanie kontrolera – opcja umożliwia aktualizację aplikacji i firmware kontrolera. Po wciśnięciu przycisku należy wskazać folder, w którym znajdują się pliki aktualizacyjne.

Wyjście DEC i zasilanie czytników:

Wyłącz – opcja pozwala na zdalne odłączenie napięcia od czytników i urządzeń peryferyjnych podłączonych do wyjścia napięciowego DEC

Włącz – opcja pozwala na zdalne podanie napięcia od czytników i urządzeń peryferyjnych podłączonych do wyjścia napięciowego DEC po jego wyłączeniu.

Wyłącz tymczasowo – opcja pozwala na czasowe wyłączenie wyjścia napięciowego DEC. Czas wyłączenia wyjścia można ustawić w zakładce ***Ustawienia*** w opcji ***Czas wyłączenia dla impulsu [s]***. Operator może wywołać akcję komendą ***Restart*** z menu kontekstowego kontrolera.

Restarty:

Restartuj aplikację w kontrolerze – opcja umożliwia ponowne uruchomienie aplikacji w kontrolerze (APK) odpowiadającej za logikę kontrolera

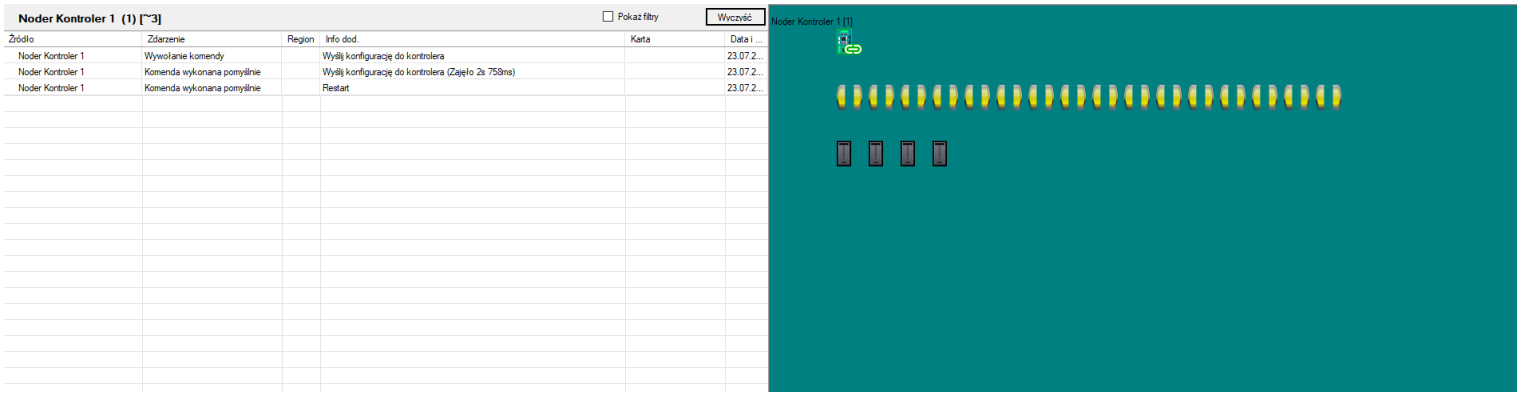
Restartuj kontroler – opcja umożliwia całkowity restart kontrolera.

Interfejsy:

Utwórz/pokaż interfejs testowy – tworzy interfejs kontrolera składający się z podglądu zdarzeń dotyczącego danego kontrolera oraz mapy z ikonami wszystkich czytników oraz wejść danego kontrolera. Jeżeli taki interfejs testowy został utworzony wcześniej ponowne wywołanie tej funkcji spowoduje odświeżenie mapy wg bieżącej konfiguracji i wyświetlenie interfejsu

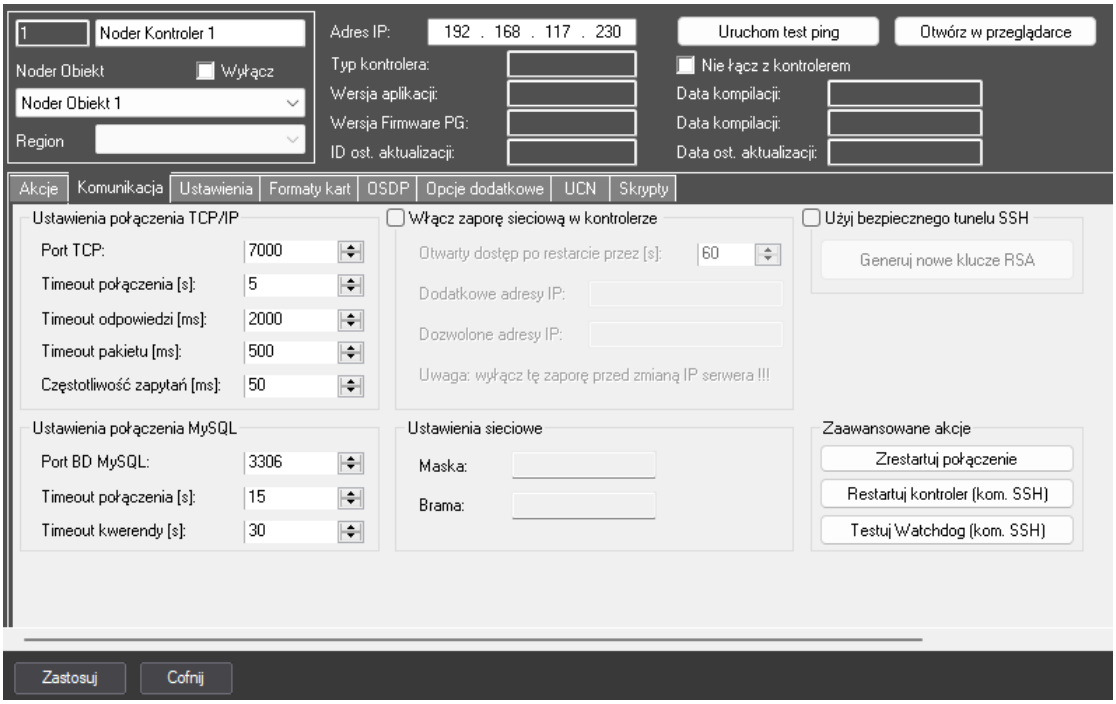
Usuń interfejs testowy – opcja usuwa utworzony wcześniej interfejs testowy.

Przykładowy interfejs testowy:



3.4.2 Komunikacja

Zakładka umożliwia konfigurację połączenia sieciowego, zapory sieciowej i tunelowania SSH.



Ustawienia połączenia TCP/IP:

Port TCP – port 7000 używany do połączenia TCP z kontrolerem.

Timeout połączenia [s] – maksymalny czas oczekiwania na odpowiedź kontrolera podczas połączenia. Zmniejszenie czasu przyspiesza ponowne połączenie.

Timeout odpowiedzi [ms] – maksymalny czas oczekiwania na odpowiedź kontrolera podczas komunikacji z nim. Zmniejszenie czasu przyspiesza ponowne połączenie.

Timeout pakietu [ms] – maksymalny czas odczytu odpowiedzi kontrolera. Zmniejszenie czasu przyspiesza ponowne połączenie.

Częstotliwość zapytań [ms] – czas pomiędzy ponownymi sprawdzaniami stanów i zdarzeń z kontrolera.

Ustawienia połączenia MySQL:

Port BD MySQL – port 3306 używany do bezpośredniego połączenia z bazą danych kontrolera. Pozwala na szybką aktualizację użytkowników (do 1000 na sekundę).

Timeout połączenia [s]– maksymalny czas oczekiwania na odpowiedź bazy danych kontrolera podczas połączenia.

Timeout kwerendy [s] – maksymalny czas oczekiwania na wykonanie zapytania SQL.

Włącz zaporę sieciową w kontrolerze – opcja uruchamia zaporę sieciową kontrolera. Należy pamiętać, aby ją wyłączyć przy zmianie adresu IP serwera. Jeżeli się tego nie zrobi utracone zostanie połączenie z kontrolerem.

Otwarty dostęp po restarcie przez [s] – gdy zapora jest włączona, urządzenia z niedozwolonymi adresami IP nie mogą połączyć się z kontrolerem. Opcja pozwala łączyć się z kontrolerem przez określony czas od uruchomienia APK kontrolera, nawet gdy znajduje się poza dozwolonymi adresami IP.

Dodatkowe adresy IP – administrator ma możliwość dodania dodatkowych adresów IP, które będą należeć do dozwolonych adresów IP. Przy dodawaniu kilku adresów IP należy użyć przecinka jako separatora np. 10.10.1.50,192.168.1.110,192.168.1.22.

Dozwolone adresy IP – podsumowanie z listą dozwolonych adresów IP. Oprócz niestandardowych (dodanych z ***Dodatkowe adresy IP***) będą wszystkie adresy IP komputera, do którego należy obiekt Noder serwer.

Ustawienia sieciowe – brama i maska kontrolera skonfigurowana w przeglądarce.

Użyj bezpiecznego tunelu SSH – funkcja umożliwiająca ustanowienie bezpiecznego kanału między serwerem a kontrolerem, a następnie przekierowanie całej komunikacji przez ten kanał.

Generuj nowe klucze RSA – przycisk do generowania par kluczy RSA (publiczny i prywatny) dla połączenia i poleceń SSH.

Połączenie SSH wykonywane jest na porcie 22. Gdy tunel SSH jest aktywny, zapora domyślnie jest włączona, a porty 3306 i 80 również są zamknięte. Port TCP 7000 jest używany tylko do pobrania wersji kontrolera, a następnie utworzony jest tunel SSH.

Połączenie od karty do serwera jest szyfrowane. Poniżej przedstawiono technologie zabezpieczające system:

- Zabezpieczenie połączenia serwer-klient → szyfrowanie TLS 1.2
- Zabezpieczenie serwer-kontroler → tunel SSH, zapora sieciowa w kontrolerze (dostęp do kontrolera wyłącznie z określonych adresów IP)
- Zabezpieczenie kontroler-czytnik → szyfrowanie AES-256
- Zabezpieczenie czytnik–karta Mifare DESFire 13.56 MHz → szyfrowanie AES-128

Zaawansowane akcje:

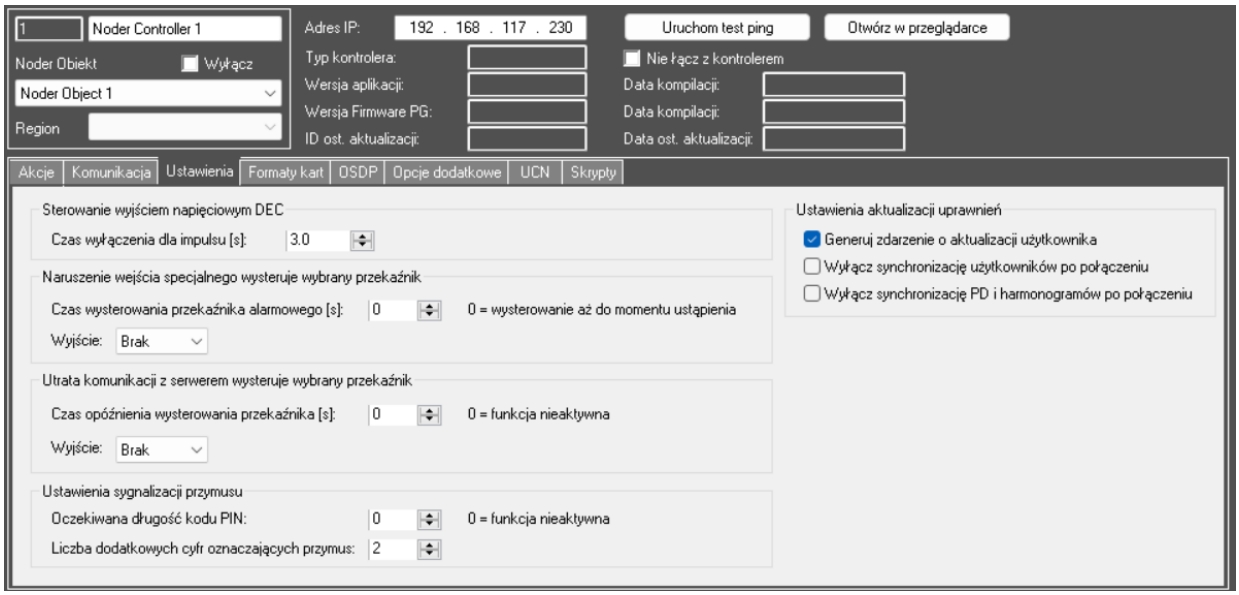
Zrestartuj połączenie – przycisk do rozłączenia z kontrolerem i ponownego połączenia.

Restartuj połączenie (kom. SSH) – Zabezpieczone polecenie na 22 porcie do ponownego uruchomienia kontrolera (działa nawet, gdy kontroler jest odłączony z oprogramowaniem Axxon PSIM).

Testuj Watchdog (kom. SSH) – opcja powoduje zrestartowanie kontrolera poprzez krótkie przerwy w zasilaniu. Po wydaniu komendy połączenie zostanie utracone za około. 2 minuty. Jest to zabezpieczone polecenie na 22 porcie działające nawet jeśli kontroler jest rozłączony z oprogramowaniem Axxon PSIM. *Nie uruchamiaj tego polecenia, jeśli masz starą płytę główną bez zainstalowanego zewnętrznego watchdoga*.

3.4.3 Ustawienia

Zakładka umożliwia konfigurację wyjścia napięciowego DEC oraz wyjść przekaźnikowych w przypadku naruszenia lub utraty komunikacji z serwerem.



Sterowanie wyjściem napięciowym DEC:

Czas wyłączenia dla impulsu – opcja umożliwia ustawienie czasu ***Wyłączenia tymczasowego*** wyjścia napięciowego DEC, a tym samym wyłączenia na ten czas czytników i urządzeń peryferyjnych zasilonych z tego wyjścia.

Ustawienia aktualizacji uprawnień:

Generuj zdarzenie o aktualizacji użytkownika – zaznaczenie opcji powoduje generowanie zdarzenia ***Zaktualizowano użytkownika: Nazwa użytkownika [ID użytkownika]***, po zmianie informacji o nim lub uprawnień.

Wyłącz synchronizację użytkowników po połączeniu – zaznaczenie opcji powoduje wyłączenie synchronizacji użytkowników po połączeniu z oprogramowanie Axxon PSIM.

Wyłącz synchronizację PD i harmonogramów po połączeniu – zaznaczenie opcji powoduje wyłączenie synchronizacji PD i harmonogramów po połączeniu z oprogramowanie Axxon PSIM.

Naruszenie wejścia specjalnego wysteruje wybrany przekaźnik:

Czas wysterowania przekaźnika – czas na jaki wyjście przekaźnikowe będzie aktywowane po naruszeniu wejścia specjalnego (21-24). Gdy wartość ustawiona jest na 0, wyjście będzie aktywne do czasu ustania naruszenia.

Wyjście – numer wyjścia przekaźnikowego kontrolera

Utrata komunikacji z serwerem wysteruje wybrany przekaźnik:

Czas opóźnienia wysterowania – czas po jakim wyjście przekaźnikowe zostanie aktywowane po utracie połączenia z serwerem. Gdy wartość ustawiona jest na 0, funkcja nie będzie aktywna.

Wyjście – numer wyjścia przekaźnikowego kontrolera

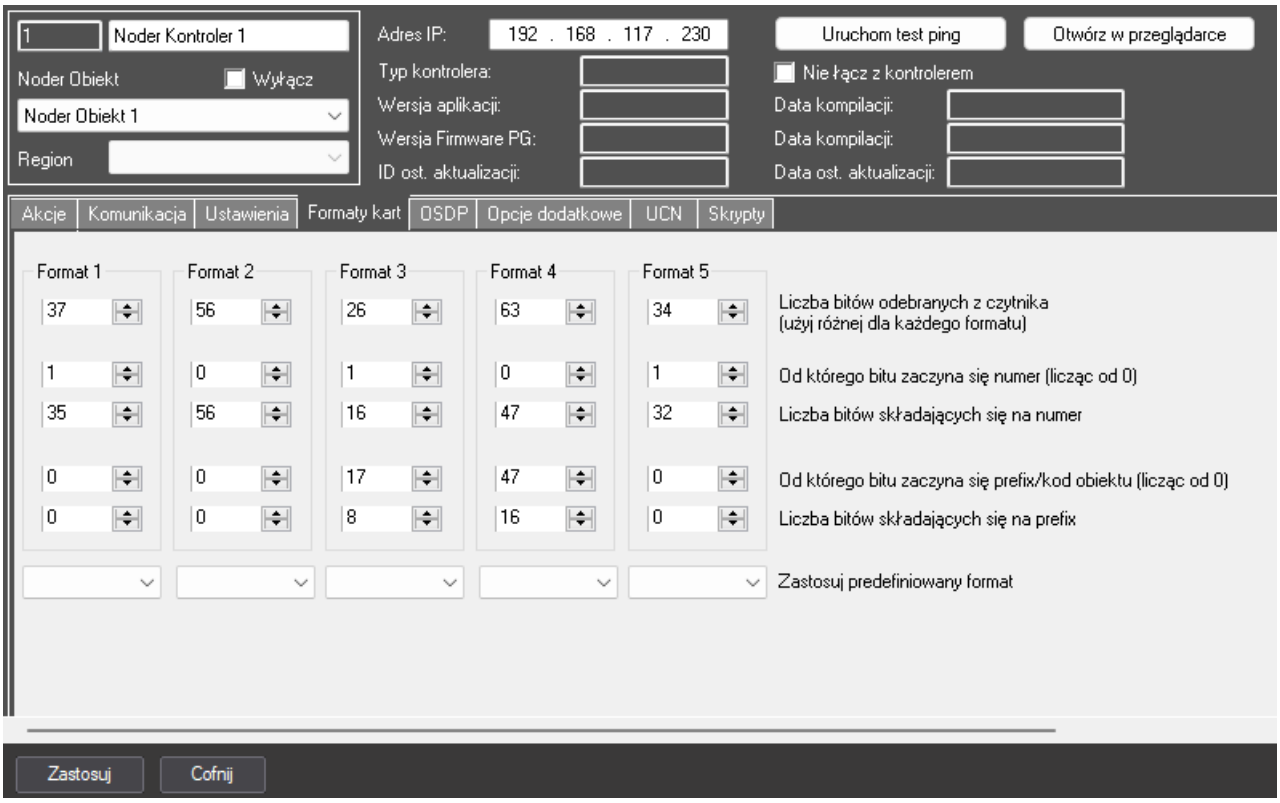
Utrata sygnalizacji przymusu – włącznie opcji generuje dodatkowy log w systemie *„Cichy alarm !!! Zastosowano kod przymusu !!!”* po wpisaniu kodu PIN zawierającego większą ilość znaków

Oczekiwana długość kodu PIN– liczba cyfr w kodzie PIN przypisywana użytkownikom w systemie

Liczba dodatkowych cyfr oznaczających przymus – ilość dodatkowych cyfr do wprowadzenia, które wygenerują log o przymusie (np. PIN 4-cyfrowy, Liczba dodatkowych cyfr oznaczających przymus-2. Do wygenerowania alarmu należy wprowadzić 6 cyfr i zatwierdzić # na klawiaturze czytnika)

3.4.4 Formaty kart

Ustawienie różnych formatów kart daje możliwość podłączenia do jednego kontrolera czytników o różnych parametrach odczytywanych kart.



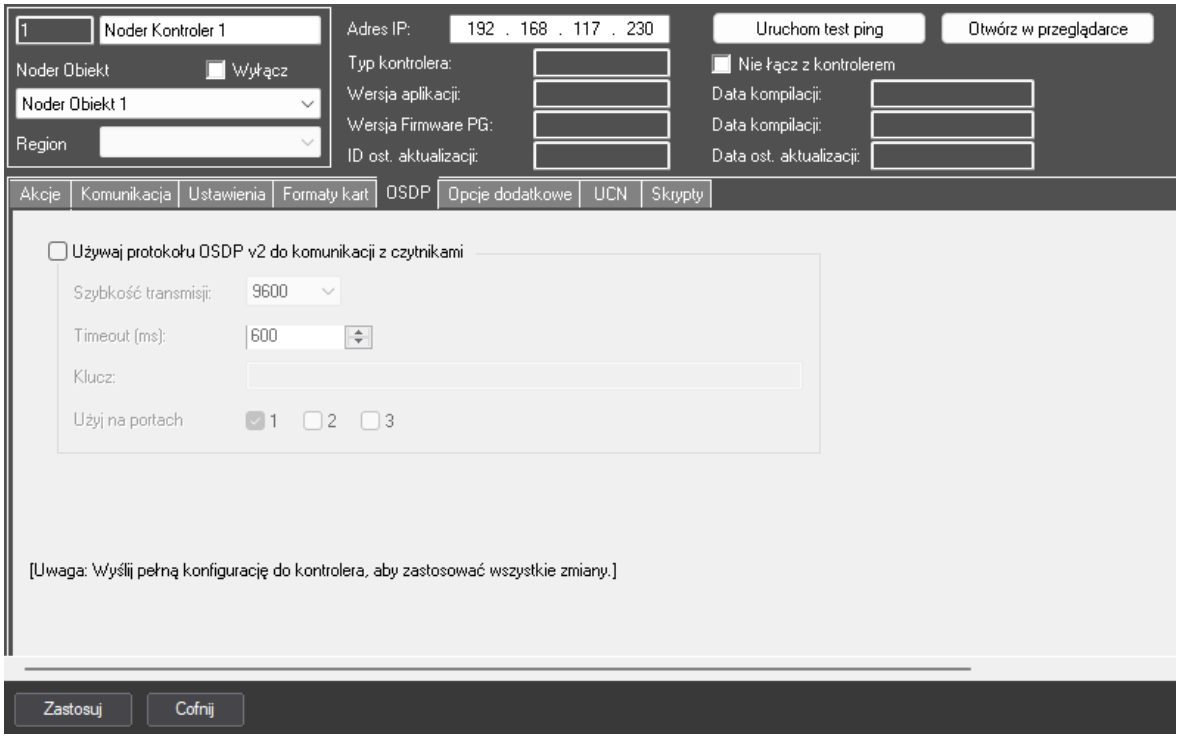
Kontroler może obsługiwać 5 formatów kart w oparciu o liczbę odebranych bitów. Axxon PSIM daje możliwość wyboru predefiniowanych formatów kart lub ich ręcznej konfiguracji.

Użycie karty z nieokreśloną liczbą bitów w formatach kart wygeneruje w systemie zdarzenie ***Odczytano niezdefiniowaną liczbę bitów*** z informacją, ile bitów zostało odczytanych.

Źródło	Zdarzenie	Region	Info dod.
Noder Czytnik 1.1	Odczytano niezdefiniowaną liczbę bitów		37

3.4.5 OSDP

Kontrolery NODER EE12 i EWE4 umożliwiają komunikację z czytnikami przez protokół OSDP v2.



Używaj protokołu OSDP v2 do komunikacji z czytnikami – zaznaczenie opcji pozwala połączyć się z czytnikami po protokole OSDP v2. Gdy opcja jest odznaczona kontroler pracuje na domyślnym protokole ***RS485***:

Szybkość transmisji – szybkość transmisji zgodna z ustawioną na czytniku. Do wyboru 9600, 19200, 38400, 57600, 115200.

Timeout – czas odpowiedzi czytnika podczas komunikacji z kontrolerem.

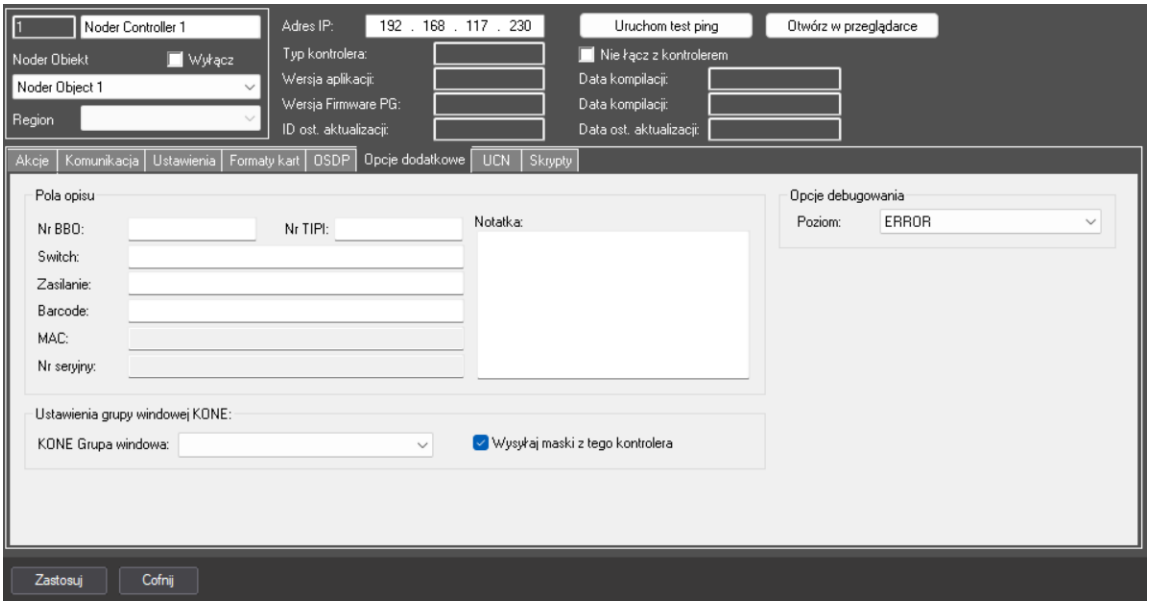
Klucz – 128 bitowy klucz w zapisie heksadecymalnym (32 znaki). Przykładowy klucz dla czytników HID w trybie Install Mode: 303132333435363738393A3B3C3D3E3F.

Używaj na portach – opcja pozwala włączyć OSDP v2 na poszczególnych portach RS485 kontrolera. Kontroler EE12 umożliwia na jednoczesne używanie RS485 i OSDP v2 na różnych magistralach (np. 1 port – OSDP v2, 2 port – RS485, port 3 – RS485).

OSDPv2 zaimplementowane w kontrolerze jest zgodne ze wspieranym protokołem OSDP zaimplementowanym w czytnikach HID, Elatec, ISBC ESMART. W czytnikach należy ustawić adres z zakresu od 1 do 4. W czytniku musi zostać ustawiona opcja ***Compliance*** na 0x02 (kontroler ***nie wspiera OSDP v1***)

3.4.6 Opcje dodatkowe

Zakładka umożliwia konfigurację dodatkowych ustawień kontrolera.



Pola opisu – informacje o sieci, infrastrukturze elektrycznej oraz inne informacje na temat kontrolera mogą być tu przechowywane. Przechowywane tutaj informacje nie mają wpływu na działanie kontrolera.

Ustawienia grupy windowej KONE:

KONE Grupa windowa – należy wybrać grupę windową do zarządzania nią z danego kontrolera.

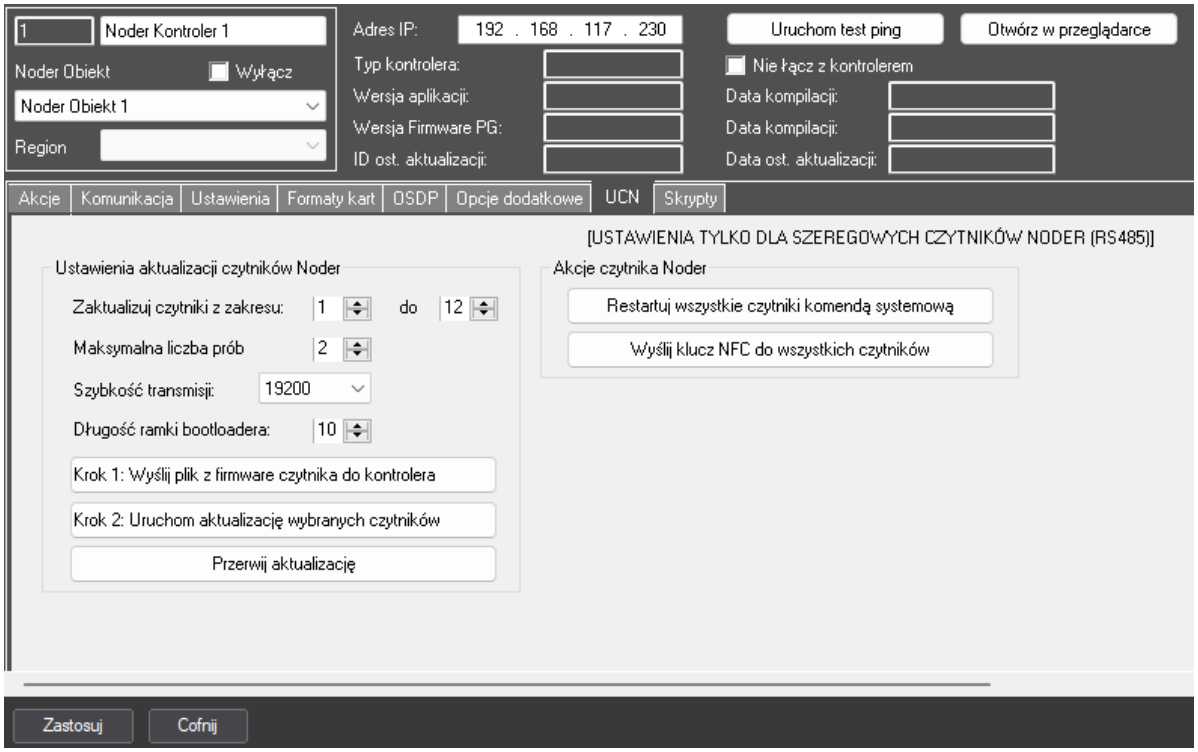
Wysyłaj maski z tego kontrolera – zaznaczenie opcji powoduje wysyłanie masek określonych w grupie windowej.

Ustawienia debugowania:

Poziom – opcja pozawala na wybranie typów logów zapisywanych do pliku.

3.4.7 UCN

Zakładka umożliwia wgranie plików oraz aktualizację czytników Noder do obsługi technologii NFC.



Ustawienia aktualizacji czytników NODER:

Zaktualizuj czytniki z zakresu – opcja umożliwia zbiorową akcję aktualizacji czytników na wybranych adresach podłączonych do kontrolera.

Maksymalna liczba prób – opcja umożliwia wskazanie ilości prób aktualizacji czytników.

Szybkość transmisji – opcja pozwala na wybranie szybkości transmisji przy aktualizacji czytnika. Domyślna wartość to 19200.

Długość ramki bootloadera – opcja umożliwia ustawienie wielkości pakietów danych wysyłanych do czytnika. Domyślna wartość to 10.

Krok 1: Wyślij plik z firmware czytnika do kontrolera – po kliknięciu w przycisk, otwarte zostaje okno, w którym należy wskazać folder z plikami aktualizacyjnymi czytnika. Wgranie plików jest niezbędne do uruchomienia NFC w czytnikach.

Krok 2: Uruchom aktualizację wybranych czytników – po ustawieniu parametrów aktualizacji i wgraniu plików z firmware czytnika można rozpocząć aktualizację klikając w ten przycisk.

Przerwij aktualizację – opcja umożliwia przerwanie aktualizacji.

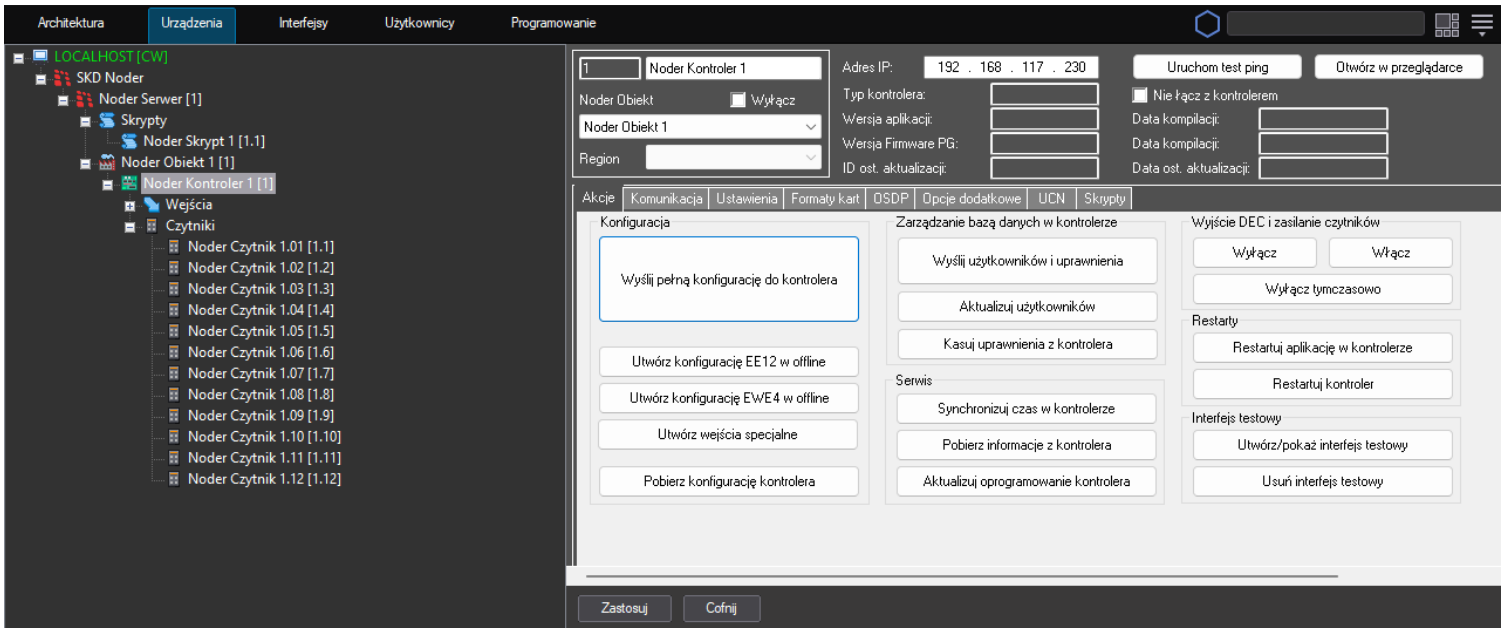
Akcje czytnika NODER:

Restartuj wszystkie czytniki komendą systemową – opcja pozwala zrestartować wszystkie czytniki podłączone do kontrolera przy pomocy komendy systemowej (nie jest odłączane od nich napięcie jak w przypadku restartu przez wyjście DEC).

Wyślij klucz NFC do wszystkich czytników – opcja umożliwia wysłanie kluczy NFC do czytników. Należy pamiętać o wcześniejszym ustawieniu ich dla każdego czytnika.

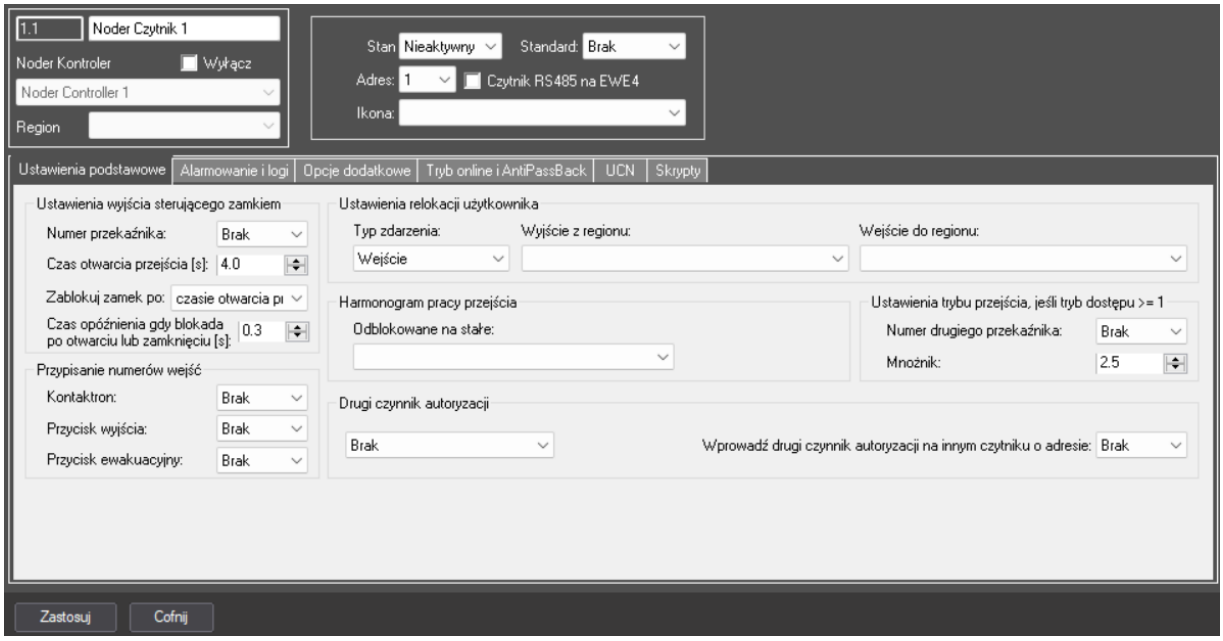
3.5 Czytniki

Przy pierwszym uruchomieniu kontrolera należy pobrać jego konfigurację klikając na przycisk ***Pobierz konfigurację kontrolera***.



Po pobraniu konfiguracji z kontrolera utworzone zostaną ***Czytniki*** i ***Wejścia***. Dla kontrolera EE12 będzie to 12 czytników i 20 wejść, a dla EWE4 – 4 czytniki i 16 wejść. Następnie należy je skonfigurować według potrzeb systemu. ***Nieużywane obiekty należy usunąć i wysłać konfigurację do kontrolera*** (przycisk ***Wyślij pełną konfigurację do kontrolera***).

Do połączenia z czytnikiem należy skonfigurować jego ***Stan***, ***Adres*** i ***Typ***:



Stan:

Nieaktywny – stan, w którym wyłączana jest komunikacja z czytnikiem. W tym stanie operator nie ma możliwości sprawdzenia czy czytnik jest fizycznie podłączony do kontrolera.

Aktywny – stan normalnej pracy czytnika

Zablokowany – stan, w którym czytnik jest zablokowany. Komunikacja z czytnikiem powinna się odbywać poprawnie. Dioda na czytniku zablokowanym przez administratora jest wygaszona w normalnym stanie. Po przyłożeniu uprawnionej/nieuprawnionej karty pomarańczowa dioda mignie 2 razy, a z nią beeper. Komendy z mapy nie zmieniają stanu czytnika. Gdy jeden z czytników przejścia dwustronnego jest zablokowany to drugi działa prawidłowo. Dla przejścia jednostronnego przycisk wyjścia działa poprawnie.

Adres – z listy rozwijanej należy wybrać adres czytnika z zakresu 1-12. Kontroler EWE4 wykorzystuje adresy 1-4, a EE12 obsługuje adresy 1-12. Adresowanie czytników odbywa się za pomocą kart programujących nadając im adresy 1-4 (po podaniu zasilania na czytnik adres czytnika wskazywany jest przez ilość piknięć beepera). Adresy dla kontrolera EE12 przeliczane są następująco.

Adres czytnika	*Port*	*Adres logiczny w kontrolerze*
1	**1**	**1**
2	**1**	**2**
3	**1**	**3**
4	**1**	**4**
1	**2**	**5**
2	**2**	**6**
3	**2**	**7**
4	**2**	**8**
1	**3**	**9**
2	**3**	**10**
3	**3**	**11**
4	**3**	**12**

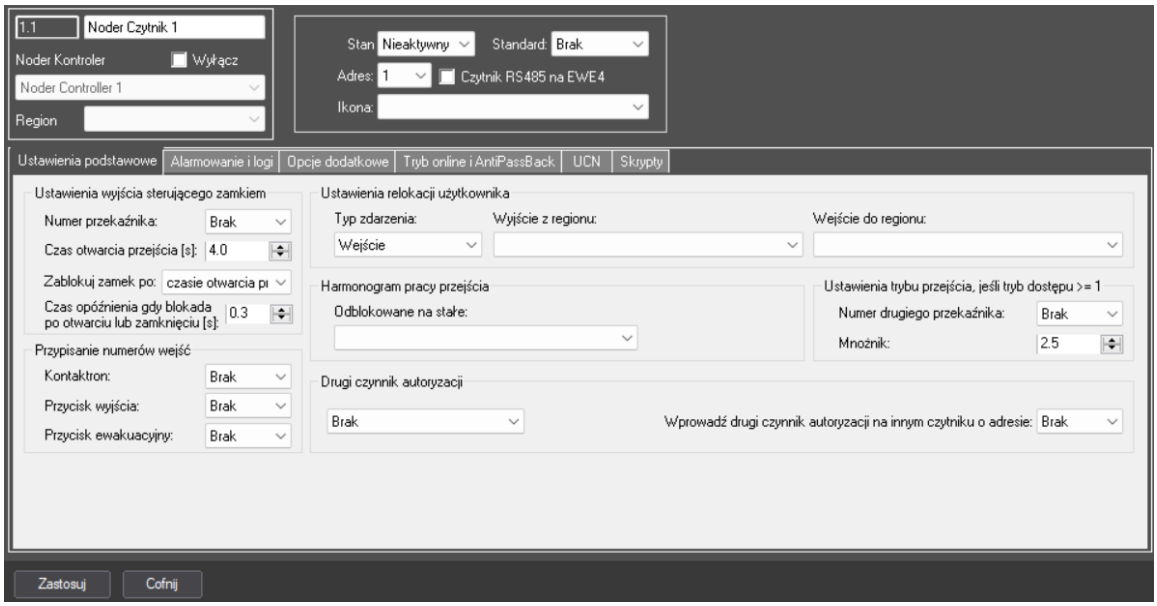
Kontroler EWE4 umożliwia podpięcie 4 czytników (zarówno Wiegand jak i RS485 w dowolnej konfiguracji: np. 1 czytnik Wiegand i 3 czytniki RS485). Czytniki NODER RS-485 powinny być adresowane kartami programującymi, w celu nadania im adresu i kluczy, a czytniki Wiegand kartą programującą na adresie 1, w celu nadania im kluczy (adres nie jest potrzebny).

Ikona – rodzaj ikony, który będzie wyświetlany na wizualizacji

Czytnik RS na EWE4 – opcję należy zaznaczyć, gdy do kontrolera EWE4 podłączony na danym adresie jest czytnik RS485 lub OSDPv2.

3.5.1 Ustawienia podstawowe

Zakładka używana jest do konfiguracji przejścia. Pozwala przypisać do danego czytnika wejścia i wyjścia kontrolera.



Ustawienia wyjścia sterującego zamkiem:

Numer przekaźnika – numer wyjścia przekaźnikowego, który ma być przypisany do czytnika. Dla kontrolera EWE4 należy wybrać przekaźnik 1-6, a dla EE12 przekaźnik 1-16.

Czas otwarcia przejścia [s] – czas przez, który przekaźnik będzie wysterowany po przyłożeniu uprawnionej karty, wciśnięciu przycisku wyjścia lub wywołaniu komendy ***Otwórz jednorazowo***.

Zablokuj zamek po – przejście może być blokowane po ***czasie otwarcia przejścia***, ***otwarciu przejścia*** lub ***zamknięciu przejścia***. Dla opcji ***otwarciu przejścia***, ***zamknięciu przejścia*** jego zablokowanie nastąpi w przypadku braku akcji po ***Czasie otwarcia przejścia [s]***.

Czas opóźnienia, gdy blokada po otwarciu lub zamknięciu [s] – opcja pozwala ustawić dodatkowy czas po jakim będzie blokowany rygiel dla opcji ***Zablokuj zamek po: otwarciu przejścia/zamknięciu przejścia***. Maksymalny czas możliwy do ustawienia wynosi 2 sekundy.

Przypisanie numerów wejść:

Kontaktron – numer wejścia kontrolera, do którego przypisano kontaktron dla danego przejścia.

Przycisk wyjścia – numer wejścia kontrolera, do którego przypisano przycisk wyjścia dla danego przejścia.

Przycisk ewakuacyjny – numer wejścia kontrolera, do którego przypisano przycisk ewakuacyjny dla danego przejścia.

Ustawienia relokacji użytkownika:

Typ zdarzenia – do wyboru: ***Wejście, Wyjście, Wejście służbowe, Wyjście służbowe, Wejście prywatne, Wyjście prywatne, Wjazd, Wyjazd, Patrol***. Zdarzenia będą pojawiać się po przyłożeniu karty do czytnika i skorzystaniu z przejścia.

Wyjście z regionu/Wejście do regionu – są to regiony używane przez system AntiPassBack do logicznej mapy systemu i kontrolowania obecności użytkownika w danym regionie oraz możliwości jego przejścia tylko do sąsiednich regionów. Bez ustawienia tych regionów nie ma możliwości używania globalnego AntiPassBack'u. Dzięki po ustawieniu regionów operator ma możliwość sprawdzenia aktualnego położenia użytkownika.

Harmonogram pracy przejścia:

Odblokowane na stałe – administrator systemu ma możliwość odblokowania danego przejścia na według utworzonego harmonogramu w Access Managerze. *Należy pamiętać, że zmiana stanu czytniku na nieaktywny (np. przy odłączeniu go od systemu) nie wyłącza harmonogramu. Taki harmonogram należy ustawić na „pusty" przed zmianą stanu czytnika. W przeciwnym wypadku przekaźnik zostanie wysterowany po jego rozpoczęciu.*

Drugi czynnik autoryzacji:

Brak – drugi czynnik autoryzacji jest nieaktywny.

Żądaj kodu PIN – po wybraniu opcji, po przyłożeniu karty czytnik będzie oczekiwał na wpisanie kodu PIN na nim.

Żądaj numeru karty – po wybraniu opcji, po przyłożeniu karty system będzie oczekiwał na ten sam numer karty na innym czytniku (Wprowadź drugi czynnik autoryzacji na innym czytniku). Jeżeli nie jest on wybrany drugi czynnik autoryzacji jest nieaktywny.

Kod dostępu zamiast karty – po wybraniu tej opcji, można przeprowadzić autoryzację za pomocą kodu dostępu przypisanego do użytkownika w polu „Kod dostępu" w Menadżerze KD.

Wprowadź drugi czynnik autoryzacji na innym czytniku:

- ***Brak*** – oczekiwanie na drugi czynnik autoryzacji odbywa się na tym samym czytniku, do którego przyłożono kartę.
- ***1-12*** – adres czytnika na tym samym kontrolerze, na którym będzie podany drugi czynnik autoryzacji.
- ***13*** – opcja używana w kontrolerze EE12. Pozwala na to, aby drugi czynnik autoryzacji odbywał się na 4 porcie kontrolera. Opcja używana jest dla urządzeń specjalnych (np. czytnik biometryczny twarzy)

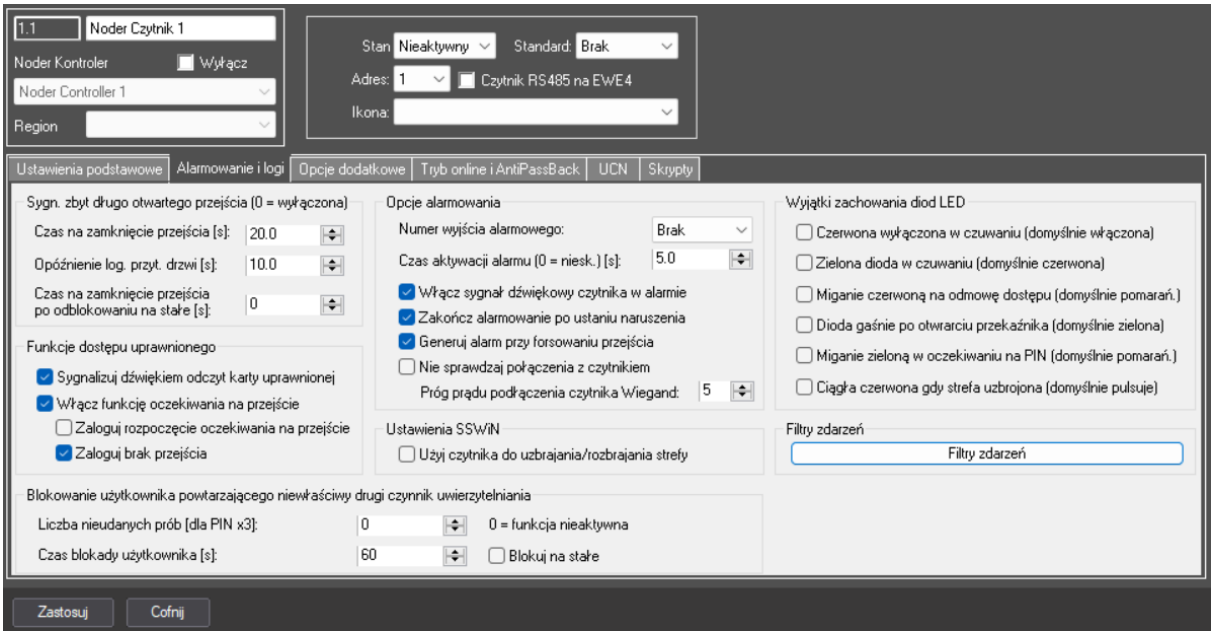
Ustawienia trybu przejścia, jeśli tryb dostępu >=1 – opcja wykorzystywana w przejściach, które wymagają wydłużenia czasu otwarcia dla poszczególnych grup użytkowników (np. osoby niepełnosprawne)***:***

Numer drugiego przekaźnika – po przyłożeniu karty przez użytkownika z trybem dostępu >=1, otwierany jest wybrany przekaźnik.

Mnożnik – administrator może wybrać, ile razy zostanie wydłużony czas otwarcia przejścia dla użytkownika z trybem dostępu >=1. (np. dla mnożnika 2.5 czas otwarcia zostanie wydłużony z 4s na 10s)

3.5.2 Alarmowanie i logi

Zakładka pozwala konfigurować alarmy i zdarzenia generowane w systemie.



Sygnalizacja zbyt długo otwartego przejścia:

Czas na zamknięcie przejścia [s] – czas po otwarciu drzwi, po którym generowane jest ostrzeżenie (zdarzenie w systemie nie jest wtedy generowane) o przytrzymaniu drzwi. Sygnalizowane jest to beeperem i pomarańczową diodą z częstotliwością 1Hz. Długość czasu ostrzegania o alarmie jest równy ***Opóźnieniu log. przyt. drzwi [s].*** W tym czasie, aby zapobiec wywołaniu alarmu należy zamknąć drzwi lub ponownie otrzymać dostęp (np. przykładając identyfikator). Ustawienie wartości 0 powoduje, że funkcja jest nieaktywna.

Opóźnienie log. przyt. drzwi [s] – czas, którego odliczanie rozpoczyna się po ***Czasie na zamknięcie przejścia [s]***, gdy generowane jest ostrzeżenie o przytrzymaniu drzwi. Po jego upłynięciu generowany jest alarm na czytniku sygnalizowany beeperem i pomarańczową diodą z częstotliwością 2.5Hz. Zakończenie alarmowania jest zależne od ustawień ***Opcji alarmowania***. Ustawienie wartości 0 powoduje natychmiastowe generowanie alarmu po upłynięciu ***Czasu na zamknięcie przejścia [s]***.

Czas na zamknięcie przejścia po odblokowaniu na stałe [s] – czas, po jakim wygenerowane zostanie zdarzenie ***Zbyt długo otwarte przejście na stałe i reakcja*** po wykonaniu przez operatora komendy na czytniku ***Otwórz na stałe***.

Funkcje dostępu uprawnionego:

Sygnalizuj dźwiękiem odczyt karty uprawnionej – odznaczenie opcji spowoduje, że po odczycie uprawnionej karty, czytnik zmieni jedynie kolor diody na zielony. Sygnalizacja dźwiękowa będzie w tym przypadku wyłączona.

Włącz funkcję oczekiwania na przejście – odznaczenie opcji spowoduje, że po przyłożeniu uprawnionej karty będzie generowane zdarzenie ***Zaliczono przejście*** bez sprawdzenia jego fizycznego otwarcia przejścia.

- ***Zaloguj rozpoczęcie oczekiwania na przejście*** – zaznaczenie opcji powoduje, że po przyłożeniu uprawnionej karty generowane jest zdarzenie ***Dostęp przyznano – oczekiwanie na przejście***.
- ***Zaloguj brak przejścia*** – zaznaczenie opcji powoduje, że po przyłożeniu uprawnionej karty użytkownik nie otworzy przejścia to po ***Czasie otwarcia przejścia [s]*** generowane jest zdarzenie ***Brak wejścia po karcie uprawnionej***.

Opcje alarmowania:

Numer wyjścia alarmowego – numer przekaźnika, który zostanie wysterowany po wystąpieniu alarmu w systemie (forsowanie lub zbyt długo otwarte przejście).

Czas aktywacji alarmu [s] – czas, przez który będzie wysterowany przekaźnik po wystąpieniu alarmu. Parametr określa również czas przez jaki alarm będą sygnalizowały czytniki. Gdy czas ustawiony jest na 0 alarmowanie trwa do ustania przyczyny (opcja ***Zakończ alarmowanie po ustaniu naruszenia*** w tym wypadku musi być zaznaczona) lub do przyłożenia uprawnionej karty/reakcji operatora. Sygnalizacja alarmowania na czytniku:

- ***Forsowanie przejścia*** – ciągły sygnał dźwiękowy, pomarańczowa dioda migająca z częstotliwością 1.5Hz
- ***Zbyt długo otwarte przejście*** – podczas ostrzegania o alarmie beeper i pomarańczowa dioda z częstotliwością 1Hz, podczas alarmu beeper i dioda z częstotliwością 2.5Hz

Włącz sygnał dźwiękowy czytnika w alarmie – gdy opcja nie jest zaznaczona, alarm na czytniku jest sygnalizowany wyłącznie miganiem diody na pomarańczowo.

Zakończ alarmowanie po ustaniu naruszenia – gdy opcja jest zaznaczona, to w przypadku wystąpienia alarmu (forsowania lub zbyt długo otwartego przejścia) sygnalizacja dźwiękowa i świetlna kasowana jest natychmiast po ustaniu przyczyny alarmu (zamknięciu przejścia). Niezaznaczenie opcji spowoduje, że alarmowanie będzie trwało do czasu ustania naruszenia i przyłożeniu uprawnionej karty/reakcji operatora. Poniżej opisano dokładnie reakcje czytnika przy zaznaczonej i niezaznaczonej opcji:

<u>**Opcja zaznaczona:**</u>

- ***Forsowanie przejścia*** – ciągły sygnał dźwiękowy przez ***Czas aktywacji alarmu [s]***, pomarańczowa dioda migająca z częstotliwością 1.5Hz do ustania naruszenia (zamknięcie przejścia). Sygnalizacja alarmu na czytniku (dźwiękowa i świetlna) ustaje natychmiast po zamknięciu przejścia.
- ***Zbyt długo otwarte przejście*** – po rozpoczęciu alarmu (po zakończeniu ostrzeżenia o przytrzymaniu drzwi) generowany jest sygnał dźwiękowy i świetlny (pomarańczowa dioda) z częstotliwością 2.5Hz. Zakończenie alarmowania następuje natychmiast po zamknięciu przejścia lub ukończeniu ***czasu aktywacji alarmu [s]*** (zarówno dioda jak i beeper)

Opcja odznaczona:

- ***Forsowanie przejścia*** – ciągły sygnał dźwiękowy przez ***Czas aktywacji alarmu [s]***, pomarańczowa dioda migająca z częstotliwością 1.5Hz do przyłożenia uprawnionej karty lub reakcji operatora (np. „Otwórz jednorazowo"). Sygnalizacja alarmu na czytniku (dźwiękowa i świetlna) nie ustaje po zamknięciu przejścia.
- ***Zbyt długo otwarte przejście*** – po rozpoczęciu alarmu (po zakończeniu ostrzeżenia o przytrzymaniu drzwi) generowany jest sygnał dźwiękowy i świetlny (pomarańczowa dioda) z częstotliwością 2.5Hz. Zakończenie alarmowania następuje po ukończeniu ***czasu aktywacji alarmu [s]*** (zarówno dioda jak i beeper). Sygnalizacja nie ustaje po zamknięciu przejścia.

Generuj alarm przy forsowaniu przejścia – odznaczenie opcji wyłącza generowanie alarmu w przypadku nieautoryzowanego otwarcia przejścia. Odznaczenie opcji nie wpłynie na działanie alarmowania przy ***Zbyt długo otwartym przejściu***.

Nie sprawdzaj połączenia z czytnikiem – opcja dla urządzeń połączonych przez magistralę Wiegand. Jeżeli urządzenie podłączone jest do innego źródła zasilania, kontroler nie będzie miał informacji o połączeniu z nim mimo poprawnej komunikacji (kontroler wykrywa połączenie z urządzeniem po obciążeniu portu magistrali). Zaznaczenie opcji pozwala na ustawienie na stałe stanu normalnego dla urządzenia na wizualizacji.

Próg prądu podłączenia czytnika Wiegand – opcja umożliwia ustawienie poziomu poboru prądu, od którego wykrywany będzie czytnik na magistrali Wiegand w kontrolerze EWE4. Funkcja przydatna jest przy czytnikach, które mają niski pobór prądu.

Ustawienia SSWiN:

Użyj czytnika do uzbrajania/rozbrajania strefy – opcja używana w SSWiN. Pozwala na uzbrojenie/rozbrojenie strefy po przyłożeniu karty do czytnika. Do uzbrojenia strefy należy przyłożyć uprawnioną kartę dwukrotnie w odstępie krótszym niż 2.5s. Do rozbrojenia strefy należy przyłożyć uprawnioną kartę jednokrotnie. Uzbrojenie strefy jest sygnalizowane 2-krotnym piknięciem czytnika po czym zaczyna migać pomarańczowa dioda z częstotliwością 0.5Hz do czasu jej rozbrojenia.

Blokowanie użytkownika powtarzającego niewłaściwy drugi czynnik uwierzytelniania:

Liczba nieudanych prób [dla PIN x3] – parametr, w którym administrator określa liczbę prób wpisania kodu PIN lub odczytu twarzy/odcisku palca, po których użytkownik zostanie zablokowany.

Czas blokady użytkownika [s] – parametr, w którym administrator określa czas blokowania użytkownika po wystąpieniu ***Liczba nieudanych prób [dla PIN x3].*** Jeżeli zaznaczona zostanie opcja ***Blokuj na stałe*** do skorzystania z przejścia operator będzie musiał zmienić jego status w Menedżerze KD na ***Zablokowany*** – „Nie"

Wyjątki zachowania diod LED – ustawienia zachowania diod LED pozwalają spersonalizować kolorystykę diod według potrzeb systemu:

Czerwona wyłączona w czuwaniu (domyślnie włączona)– pozwala wyłączyć czerwoną diodę, gdy czytnik jest w normalnym stanie.

Zielona dioda w czuwaniu (domyślnie czerwona)– pozwala włączyć zieloną diodę, gdy czytnik jest w normalnym stanie.

Miganie czerwoną na odmowę dostępu (domyślnie pomarańczowa)– pozwala migać czerwoną diodą zamiast pomarańczową po odmowie dostępu.

Dioda gaśnie po otwarciu przekaźnika (domyślnie zielona)– pozwala wyłączyć diodę po otrzymaniu dostępu, otwarciu przejścia na stałe itp.

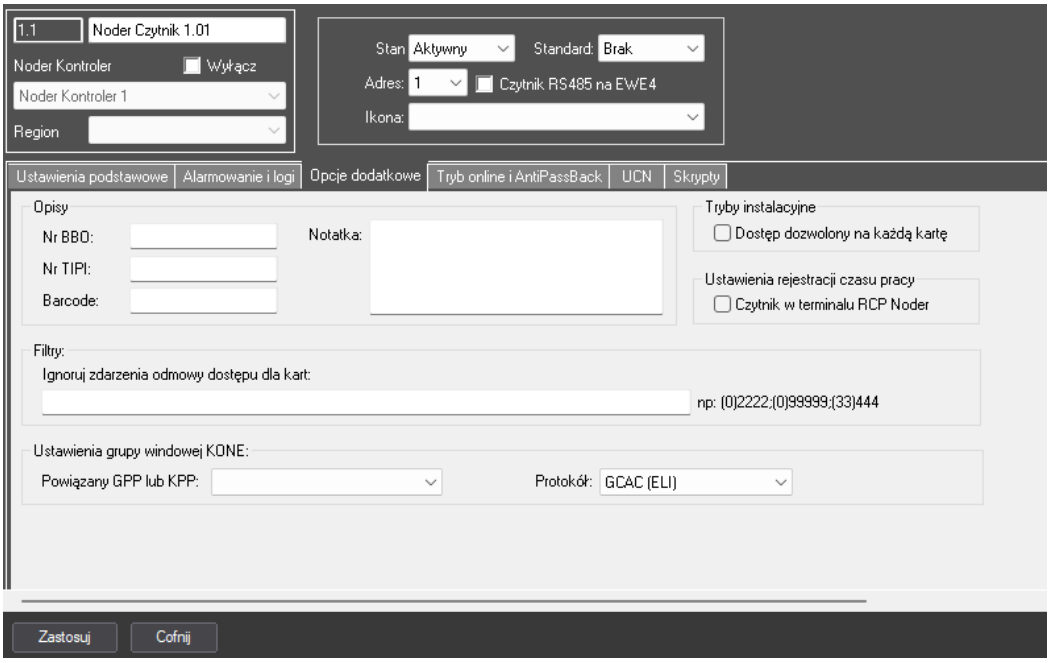
Miganie zieloną w oczekiwaniu na PIN (domyślnie pomarańczowa)– pozwala migać zieloną diodą zamiast pomarańczową po przyłożeniu karty, gdy rozpocznie się czas oczekiwania na wpisanie kodu PIN.

Ciągła czerwona, gdy strefa uzbrojona (domyślnie pulsuje)– pozwala włączyć czerwoną diodę po uzbrojeniu strefy.

Filtry zdarzeń – opcja umożliwia wyłączenie logowania wybranych zdarzeń z bazy danych kontrolera.

3.5.3 Opcje dodatkowe

Zakładka umożliwia konfigurację dodatkowych funkcjonalności czytnika.



Opisy – pola pozwalające przypisać dodatkowe informacje o kontrolerze. Nie wpływają one na działanie kontrolera.

Filtry:

Ignoruj zdarzenia odmowy dostępu dla kart – numery kart, które nie będą rejestrowane w systemie po otrzymaniu zdarzenia o nieuprawnionym dostępie. Kolejne numery należy oddzielać średnikiem.

Ustawienia grupy windowej KONE (tylko jeżeli jest używana):

Powiązany GPP lub KPP – należy przypisać czytnik do Grupowego Panelu Przywoławczego lub Kabinowego Panelu Przywoławczego.

Protokół – należy wybrać protokół komunikacji z listy rozwijanej:

- GCAC (ELI) – protokół do *zarządzania dostępem z GPP lub KPP*.
- RCGIF (Piętro domowe) – protokół do wywoływania piętra domowego z tripoda.

Tryby instalacyjne:

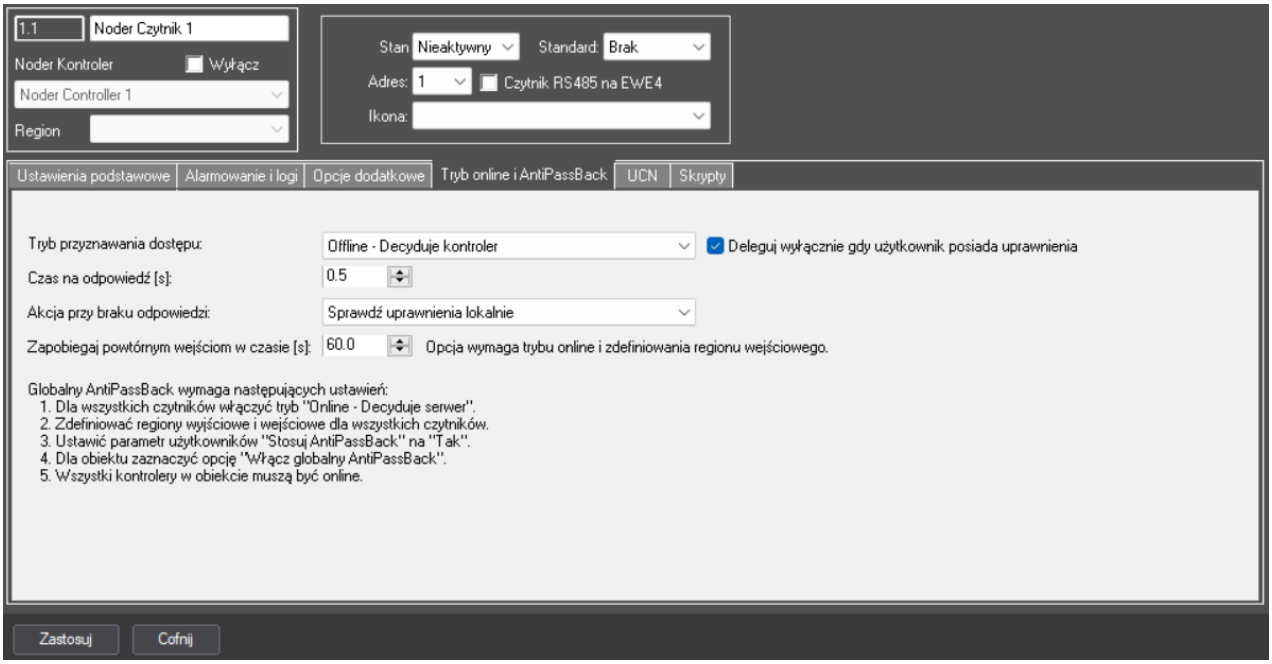
Dostęp dozwolony na każdą kartę – użycie dowolnej karty odczytywanej przez czytnik, odblokuje przejście.

Ustawienia rejestracji czasu pracy:

Czytnik w terminalu RCP Noder – opcję należy zaznaczyć, gdy czytnik NODER RCP-1 jest przypisany do danego adresu w kontrolerze. Jeżeli opcja nie zostanie zaznaczona nie będzie można połączyć się z terminalem

3.5.4 Tryb online i AntiPassBack

Zakładka używana jest do konfiguracji trybu pracy, w którym ma pracować czytnik.



Tryb przyznawania dostępu:

- ***Offline – Decyduje kontroler*** – przyznanie dostępu odbywa się poprzez wewnętrzną bazę danych kontrolera. Wybranie tej opcji wyłączy globalny AntiPassBack na tym czytniku.
- ***Offline – Decyduje skrypt***– przyznanie dostępu odbywa się na podstawie logiki skryptu.
- ***Online – Decyduje serwer*** – opcja przełącza czytnik w tryb pracy online. Przyznanie dostępu po przyłożeniu karty odbywa się automatycznie przez serwer. Włączenie tej funkcji umożliwi włączenie globalnego AntiPassBack na czytniku.
- ***Online – Decyduje operator*** – opcja przełącza czytnik w tryb pracy online. Przyznanie dostępu po przyłożeniu karty wykonywane jest przez operatora na przygotowanym wcześniej interfejsie. Włączenie tej funkcji umożliwi włączenie globalnego AntiPassBack na czytniku.
- ***Online – Decyduje serwer, następnie skrypt*** – opcja przełącza czytnik w tryb pracy online. Przyznanie dostępu po przyłożeniu karty odbywa się automatycznie przez serwer. Włączenie tej funkcji umożliwi włączenie globalnego AntiPassBack na czytniku. W przypadku braku reakcji ze strony serwera tryb zmieniany jest na ***Decyduje skrypt***.
- ***Online – Decyduje serwer*** – opcja przełącza czytnik w tryb pracy online. Przyznanie dostępu po przyłożeniu karty wykonywane jest przez operatora na przygotowanym wcześniej interfejsie. Włączenie tej funkcji umożliwi włączenie globalnego AntiPassBack na czytniku. W przypadku braku reakcji ze strony serwera tryb zmieniany jest na ***Decyduje skrypt***.

Deleguj wyłączenie, gdy użytkownik posiada uprawnienia – opcja wykorzystywana jest w trybie ***Online – decyduje operator***. Po zaznaczeniu jej zapytania użytkowników z dostępem będą potwierdzane przez operatora. Użytkownicy bez uprawnień otrzymają od razu odmowę dostępu na czytniku.

Czas na odpowiedź [s] – czas oczekiwania kontrolera na odpowiedź od serwera/operatora w trybie online. Po tym czasie wykonana zostanie ***Akcja przy braku odpowiedzi***.

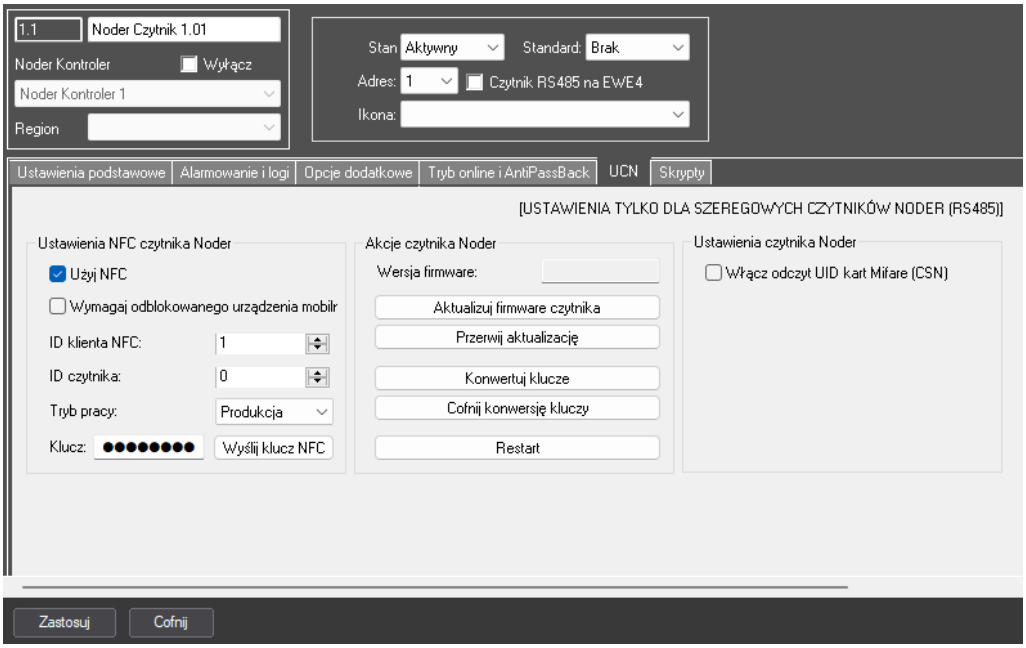
Akcja przy braku odpowiedzi – w przypadku braku odpowiedzi od serwera/operatora w trybie online wykonana zostanie akcja:

- ***Sprawdź uprawnienia lokalnie*** – po utracie połączenia z serwerem i użyciu uprawnionej karty, przyznanie dostępu będzie sprawdzone po sprawdzeniu uprawnień użytkownika w wewnętrznej bazie danych kontrolera.
- ***Zaloguj brak dostępu*** – po utracie połączenia z serwerem i użyciu uprawnionej karty, nastąpi odmowa dostępu.

Zapobiegaj powtórnym przejściom w czasie – administrator ma możliwość ustawienia czasu, po którym użytkownik będzie mógł ponownie skorzystać z przejścia.

3.5.5 UCN

Zakładka używana jest do konfiguracji NFC w czytniku oraz umożliwia jego zdalną aktualizację.



Ustawienia NFC czytnika Noder:

Użyj NFC – zaznaczenie opcji włącza funkcję NFC w czytniku.

Wymagaj odblokowanego urządzenia mobilnego– po zaznaczeniu opcji, użytkownik będzie musiał odblokować smartfon przed przyłożeniem go do czytnika. Jeżeli tego nie zrobi czytnik nie zareaguje.

ID klienta NFC – indywidualny numer klienta nadawany przy tworzeniu kluczy NFC

ID czytnika– numer ID czytnika. Opcję należy ustawić na wartość 0.

Tryb pracy– tryb pracy należy ustawić na ***Produkcja***. Opcje ***Testy*** i ***Rozwój*** wykorzystywane są do testowania funkcjonalności.

Klucz– indywidualny klucz tworzony dla klienta. Po wprowadzeniu go przed wykonaniem komendy ***Wyślij klucz NFC*** należy kliknąć ***Zastosuj***.

Funkcjonalności związane z NFC (***Klucz***, ***ID klienta NFC*** itp.) należy wgrywać po aktualizacji czytnika.

Akcje czytnika Noder:

Wersja firmware – wyświetlany jest firmware ostatnio podłączonego czytnika na określonym adresie do kontrolera.

Aktualizuj firmware czytnika – opcja pozwala zaktualizować czytnik. Należy pamiętać o wcześniejszym wgraniu plików aktualizacyjnych przed rozpoczęciem akcji.

Przerwij aktualizację –opcja pozwala przerwać aktualizację czytnika. W niektórych sytuacjach po przerwaniu aktualizacji może być potrzeba zrestartowania kontrolera.

Konwertuj klucze – opcja wykorzystywana jest w czytnikach, których firmware jest starszy od R409 (MD-R) i R509 (MDK-R). Należy użyć jej, gdy nie podczas aktualizacji nie zostanie wykonana automatycznie konwersja kluczy. Objawem braku konwersji kluczy jest niedziałająca funkcja NFC w czytniku.

Cofnij konwersję kluczy – opcja pozwala cofnąć konwersję kluczy. Może być używana, gdy omyłkowo wykonano ją ręcznie klikając Konwertuj klucze po aktualizacji czytnika z firmware np. R411 lub R511. Po konwersji kluczy na takim czytniku nie będzie można odczytać karty.

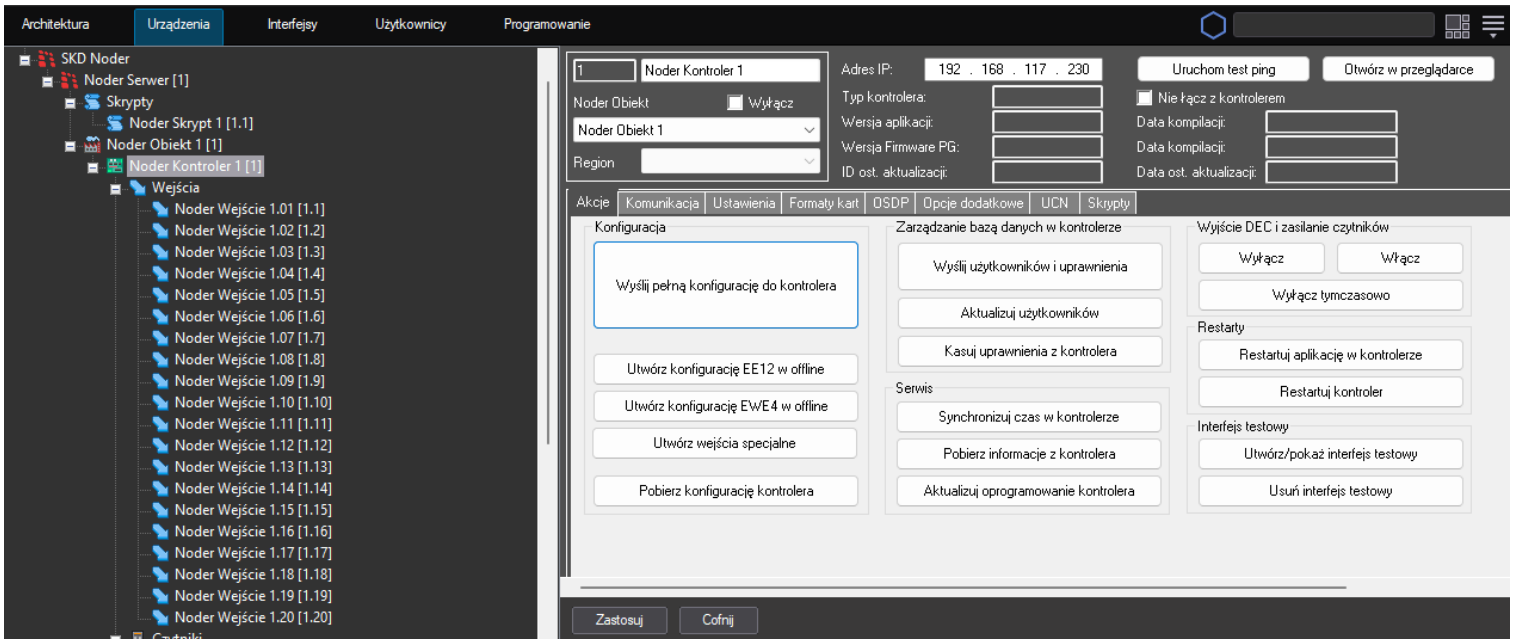
Restart – opcja pozwala wykonać systemowy restart czytnika.

Ustawienia czytnika Noder:

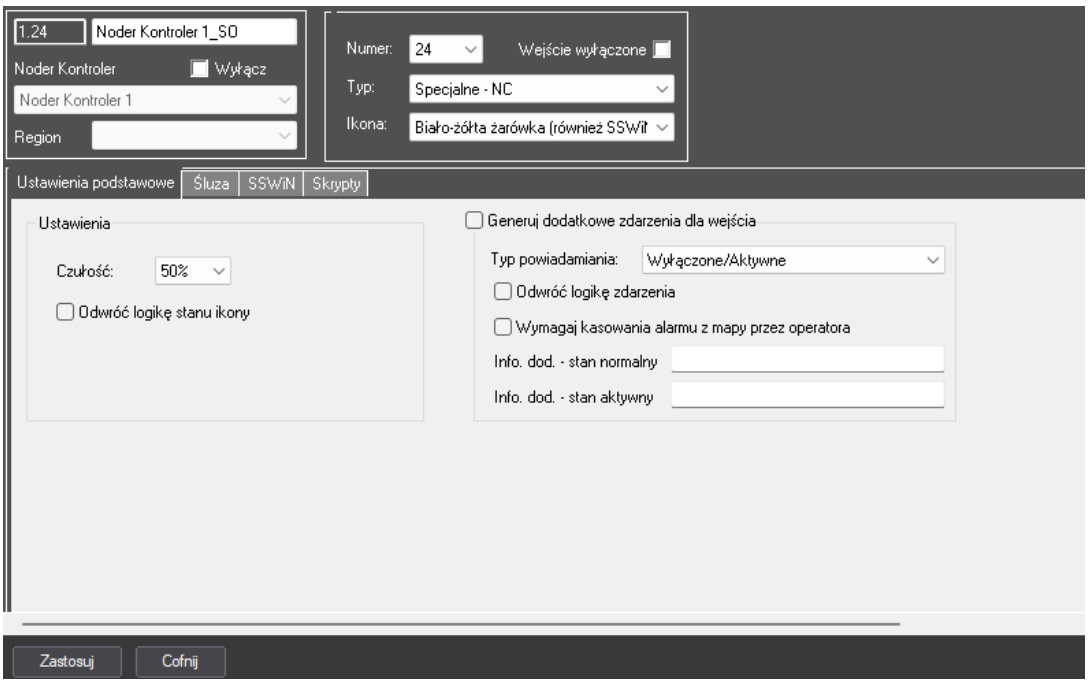
Włącz odczyt UID kart Mifare (CSN) – opcja pozwala uruchomić odczyt numerów seryjnych (CSN). CSN będzie odczytywany, gdy klucze wgrane do czytnika będą różniły się z kluczami wgranymi do identyfikatora lub ich nie było.

3.6 Wejścia

Pobranie konfiguracji z kontrolera automatycznie utworzy poza czytnikami utworzy 16 wejść dla kontrolera EWE4 i 20 wejść dla EE12. Po pobraniu konfiguracji typ wejścia będzie oznaczony jako Wyłączone. W celu wykorzystania wejścia w systemie oprócz przypisania numeru wejścia (np. kontaktron lub przycisk wyjścia) należy je odpowiednio skonfigurować.



Kontrolery EWE4 i EE12 posiadają wejścia specjalne (wejścia 21-24). Klikając ***Utwórz wejścia specjalne*** tworzona jest domyślna konfiguracja z 4 wejściami o typie Specjalne NC:



Na kontrolerze opisane są następująco:

BAT – sygnał rozładowanych akumulatorów,

AC – brak zasilania 230 V,

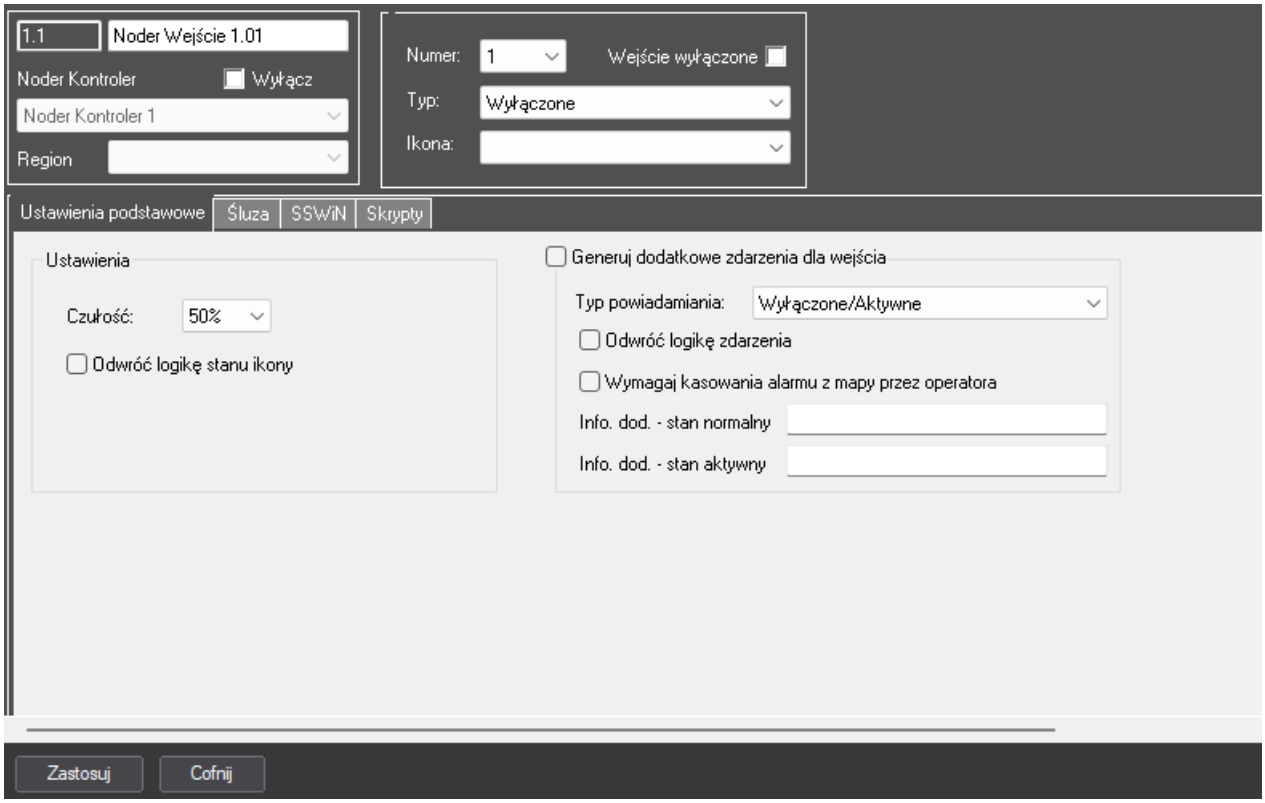
TMP – uszkodzenie zasilacza 12V DC,

DR – szeregowe połączenie wszystkich tamperów drzwi szafek oraz montażu naściennego.

Po utworzeniu wejść specjalnych ich typ ustawia się automatycznie na: ***Specjalne – NC***. Konfiguracja wejść specjalnych może być konfigurowana według potrzeb systemu, umożliwiając monitorowanie elementów zasilających i zabezpieczających zasilacz.

3.6.1 Konfiguracja wejść

Okno konfiguracji wejść pozwala skonfigurować wejścia według potrzeb systemu.



Wejście wyłączone – stan wejścia nie jest sprawdzany w systemie.

Ustawienia:

Numer – numer wejścia kontrolera

Czułość – opcja pozwala ustawić czas przez jaki wejście musi być aktywne do zarejestrowania tego w systemie. Czułość wejścia należy ustawić w zakresie 10-100%.

Typ – należy wybrać typ wejścia z listy rozwijanej. Jeżeli wejście jest używane jedynie w Systemie Kontroli dostępu należy wybrać typ wejścia „SKD”. Jeżeli typ wejście jest używane jedynie w Systemie

Sygnalizacji Włamania i Napadu należy wybrać typ wejścia „SSWiN”. Jeżeli wejście będzie wykorzystywane w obu systemach to należy wybrać typ „SKD+SSWiN”. Schematy i zastosowanie wejść SKD i SSWiN opisano w rozdziałach **3.6.2** i **3.6.3**. Typy wejść:

- ***Wyłączone*** – wejście wyłączone, jego stan nie jest sprawdzany w systemie.
- ***SKD – NO***
- ***SKD – NC***
- ***SKD – EOL/NO***
- ***SSWiN – NO***
- ***SSWiN – NC***
- ***SSWiN – EOL/NO***
- ***SSWiN – EOL/NO***
- ***SSWiN – 2EOL/NO***
- ***SSWiN – 2EOL/NC***
- ***SKD+SSWiN – NO***
- ***SKD+SSWiN – NC***
- ***SKD+SSWiN – EOL/NO***
- ***SKD+SSWiN – EOL/NC***
- ***SKD+SSWiN – 2EOL/NO***
- ***SKD+SSWiN – 2EOL/NC***
- ***Specjalne – NO*** – wejście specjalne używane dla wejść 21-24 kontrolera w logice normalnie otwartej.
- ***Specjalne – NC*** – wejście specjalne używane dla wejść 21-24 kontrolera w logice normalnie zamkniętej.

Ikona – ikona reprezentująca wejście na wizualizacji.

Odwróć logikę – zaznaczenie opcji spowoduje, że stan ikony na wizualizacji będzie odwrotny do rzeczywistego.

Generuj dodatkowe zdarzenia dla wejścia – wybranie opcji wygeneruje dodatkowe zdarzenie po aktywacji wejścia:

Typ powiadomienia – typ powiadomienia jakie zostanie wyświetlone na mapie w zależności od stanu wejścia:

- ***Wyłączone/Aktywne***
- ***Normalny/Alarm***
- ***Normalny/Uszkodzenie***

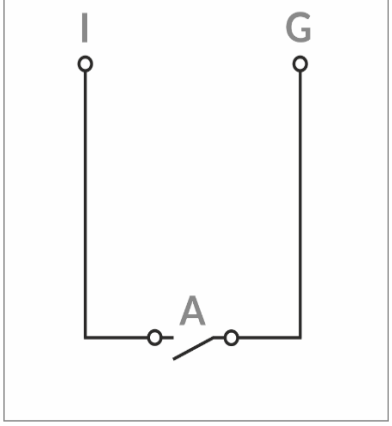
Odwróć logikę zdarzenia – wybranie opcji odwróci logikę generowanych zdarzeń w systemie w stosunku do rzeczywistego stanu.

Wymagaj kasowania alarmu z mapy przez operatora – po wybraniu opcji operator po wystąpieniu alarmu będzie musiał kasować go z mapy, żeby przywrócić wejście do normalnego stanu.

Info. dod. – stan normalny/aktywny – dodatkowe informacje wyświetlane w Event Viewer po zmianie stanu wejścia w kolumnie ***Info. dod***.

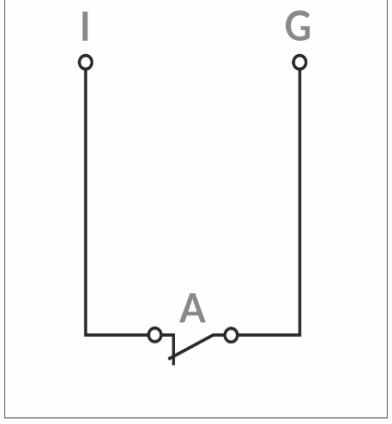
3.6.2 Schematy podłączeniowe dla SKD

NO



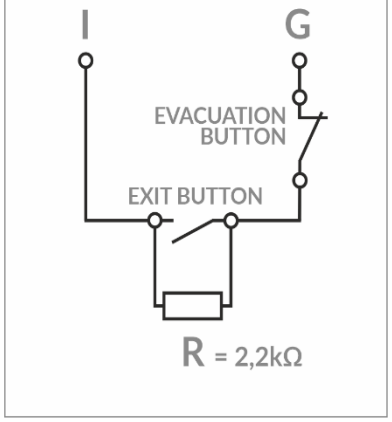
Typ wejścia NO używany jest np. jako przycisk wyjścia. Po wciśnięciu go, przekaźnik zostaje wysterowany i zdarzenie „Otwarcie z przycisku" zostanie wygenerowane

NC



Typ wejścia NC używany jest jako kontaktron lub przycisk ewakuacyjny. Kontaktron informuje aktualnym stanie przejścia (otwarte/zamknięte). Po wciśnięciu przycisku ewakuacyjnego generowany jest alarm i zdarzenie „Wciśnięty przycisk ewakuacyjny".

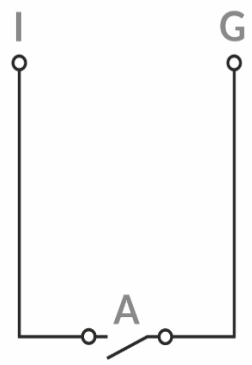
EOL/NO



Wejście skonfigurowane jako NO z rezystorem parametryzującym (2,2kOhm) końca linii. Po wciśnięciu przycisku wyjścia otrzymywane jest zdarzenie „Otwarcie z przycisku". Po wciśnięciu przycisku ewakuacyjnego otrzymywane jest zdarzenie „Wciśnięty przycisk ewakuacyjny".

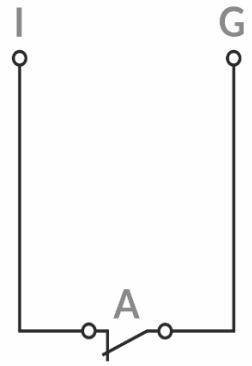
3.6.3 Schematy podłączeniowe dla SSWiN

NO



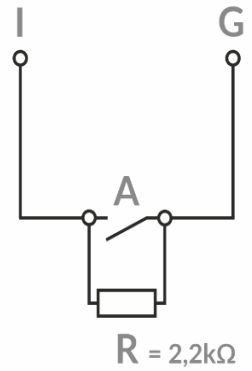
Używany dla czujek z wyjściem NO. Zamknięcie obwodu (**A**) generuje alarm. Ten typ wejścia nie pozwala otrzymywać alarmów sabotażu i uszkodzenia.

NC



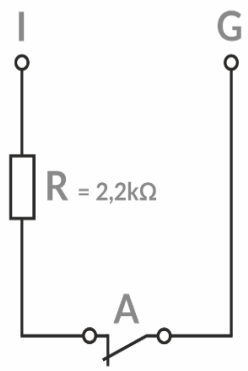
Używany dla czujek z wyjściem NC. Otwarcie obwodu (**A**) generuje alarm. Ten typ wejścia nie pozwala otrzymywać alarmów sabotażu i uszkodzenia.

EOL/NO



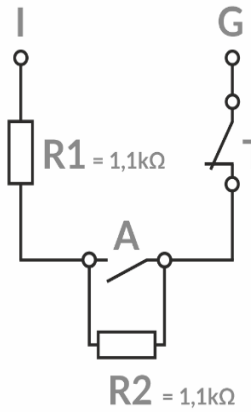
Używany dla czujek z rezystorem parametryzującym (2,2kOhm) końca linii. Zamknięcie obwodu (**A**) generuje alarm. Odłączenie wejścia kontrolera (np. odcięcie kabla czujki) generuje alarm sabotażu.

EOL/NC



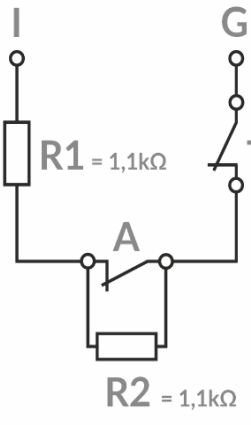
Używany dla czujek z rezystorem parametryzującym (2,2kOhm) końca linii. Otwarcie obwodu (**A**) generuje alarm. Bezpośrednie zwarcie wejścia do masy generuje alarm uszkodzenia.

2EOL/NO



Używany dla czujek z dwoma rezystorami parametryzującymi (2x1,1kOhm) końca linii. Zamknięcie obwodu (**A**) generuje alarm. Bezpośrednie zwarcie wejścia do masy generuje alarm uszkodzenia. Odłączenie wejścia kontrolera (np. odcięcie kabla) (**T**) generuje alarm sabotażu.

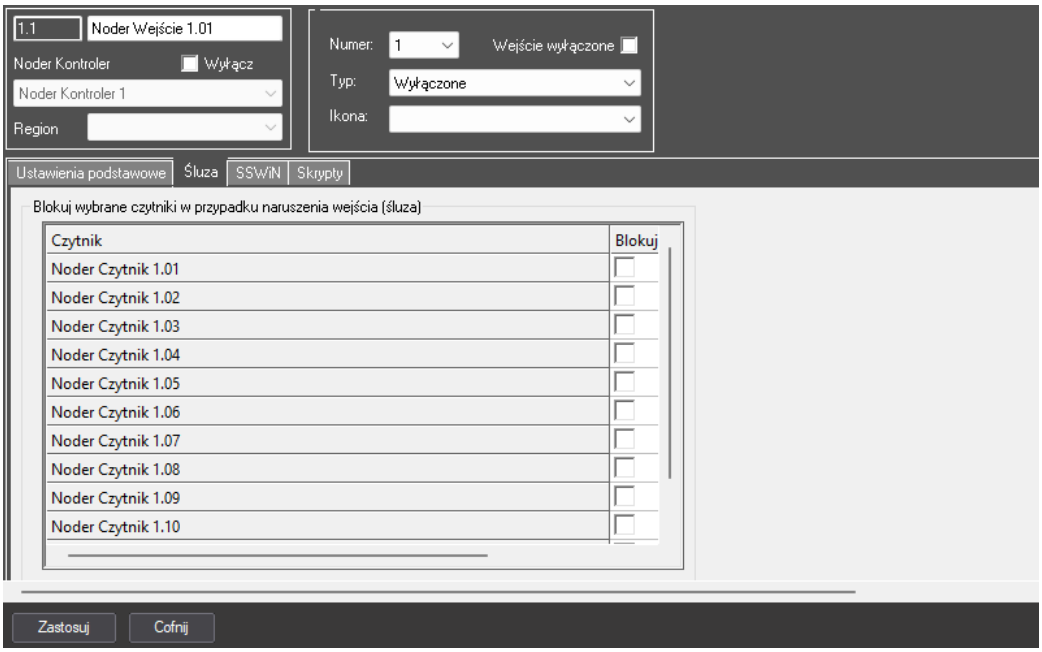
2EOL/NC



Używany dla czujek z dwoma rezystorami parametryzującymi (2x1,1kOhm) końca linii. Otwarcie obwodu (**A**) generuje alarm. Bezpośrednie zwarcie wejścia do masy generuje alarm uszkodzenia. Odłączenie wejścia kontrolera (np. odcięcie kabla) (**T**) generuje alarm sabotażu.

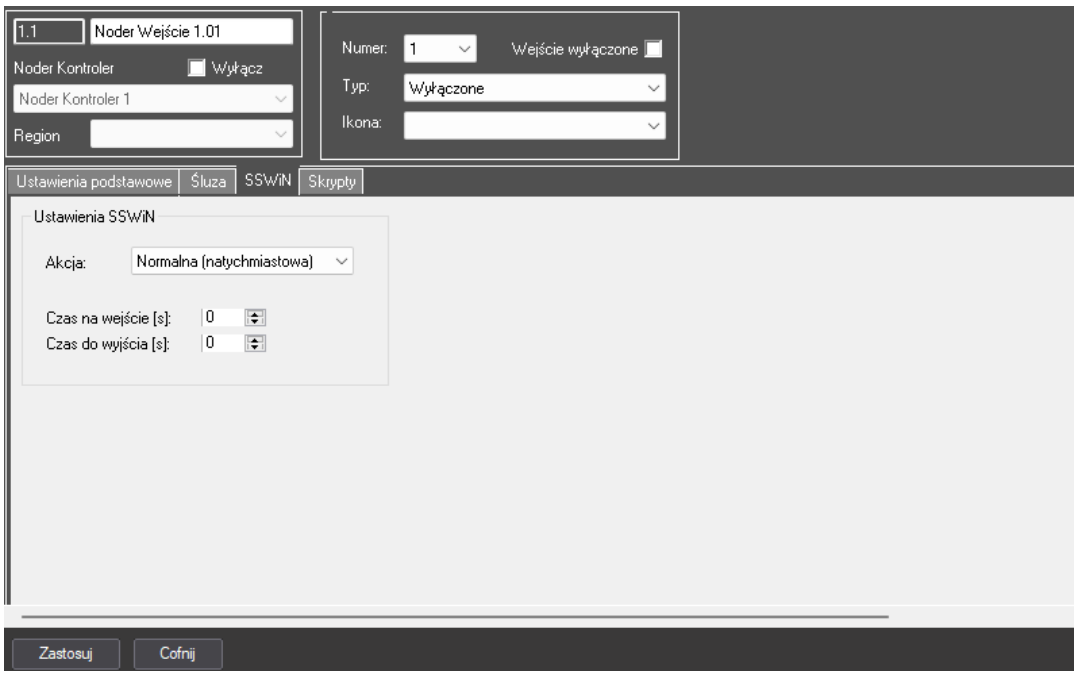
3.6.4 Śluza

Administrator dzięki opcji śluzy ma możliwość wyboru, które czytniki będą blokowane po aktywacji wybranego wejścia. Przyciski wyjścia należące do poszczególnych przejść również będą blokowane.



3.6.5 SSWiN

Jeżeli wejście ma być wykorzystane w SSWiN NODER, to administrator ma możliwość skonfigurowania logiki jego działania



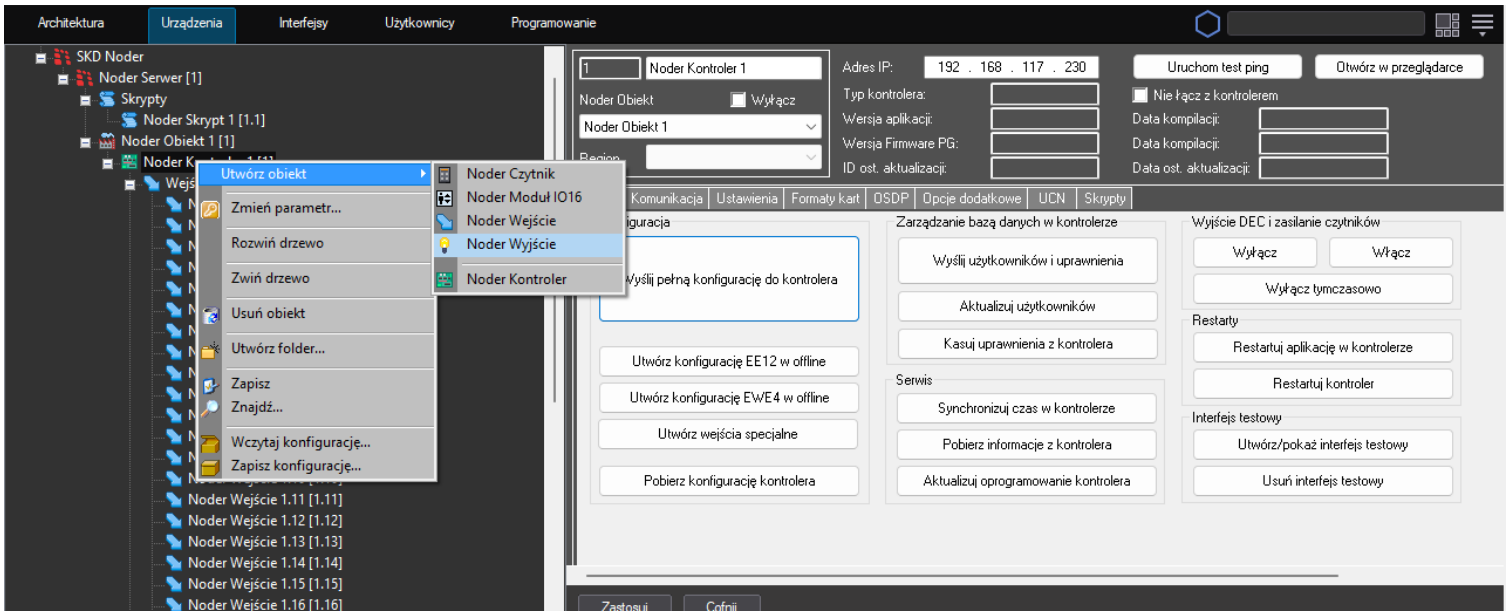
Ustawienia SSWiN – funkcja będzie działać poprawnie, jeżeli typ wejścia to „SSWiN" lub „SKD + SSWiN"

Akcja – z listy rozwijanej należy wybrać akcję jaka ma się wykonać po aktywacji wejścia:

- ***Normalna (natychmiastowa)*** – alarm zostanie aktywowany po uzbrojeniu strefy i aktywacji wejścia
- ***Wejście/Wyjście (opóźniona)*** – przy uzbrojonej strefie po aktywacji wejścia użytkownik ma ***Czas na wejście [s]*** (czas na rozbrojenie strefy)/***Czas na wyjście [s]*** ze strefy. Po tym czasie aktywowany jest alarm. Funkcjonalność jest przydatna w miejscach, gdzie strefa jest uzbrajana i rozbrajana (np. czujka ruchu wykrywająca człowieka przed rozbrojeniem strefy)
- ***24h*** – alarm aktywowany jest po każdorazowym wysterowaniu wejścia (nawet gdy strefa jest rozbrojona)
- ***24h cichy alarm*** – cichy alarm aktywowany jest po każdorazowym wysterowaniu wejścia (nawet gdy strefa jest rozbrojona). Czytniki ani wyjścia przekaźnikowe po aktywacji alarmu nie zmienią swojego stanu
- ***Napadowa –*** każde wysterowanie wejścia spowoduje aktywację alarmu napadowego (nawet jeżeli strefa jest rozbrojona)
- ***Napadowa cicha*** – każde wysterowanie wejścia spowoduje aktywację cichego alarmu napadowego (nawet jeżeli strefa jest rozbrojona). Czytniki ani wyjścia przekaźnikowe po aktywacji alarmu nie zmienią swojego stanu
- ***Techniczne – awaria zasilacza AC –*** każde wysterowanie wejścia generuje cichy alarm awarii zasilacza AC (nawet jeżeli strefa jest rozbrojona). Czytniki i wyjścia po aktywacji alarmu nie zmieniają swojego stanu.
- ***Techniczne – awaria akumulatora*** – każde wysterowanie wejścia generuje cichy alarm awarii akumulatora (nawet jeżeli strefa jest rozbrojona). Czytniki i wyjścia po aktywacji alarmu nie zmieniają swojego stanu.
- ***Uzbrajająca*** – aktywacja wejścia uzbraja strefę.
- ***Rozbrajająca*** – aktywacja wejścia rozbraja strefę.
- ***Uzbrajająco-rozbrajająca monostabilna*** – zmiana stanu na uzbrojony/rozbrojony odbywa się po podaniu zbocza narastającego na wejście (wejście nieaktywne → wejście aktywne).
- ***Uzbrajająco-rozbrajająca bistabilna*** – zmiana stanu na uzbrojony/rozbrojony odbywa się po każdorazowej zmianie stanu wejścia.
- ***Resetująca alarm*** – aktywacja wejścia resetuje alarm

3.7 Wyjścia

Aby utworzyć wyjście należy na obiekcie kontrolera kliknąć prawym przyciskiem myszy i wybrać obiekt ***Noder Wyjście***. Po przypisaniu do numeru i nazwy okno jego ustawień zostanie otwarte.



Obiekt może być używany w SSWiN (po utworzeniu go, będzie on widoczny w ustawieniach strefy SSWiN). Można przypisać go do strefy i wysterować po określonej akcji.

Ustawienia podstawowe:

Numer zacisku – numer przekaźnika na kontrolerze

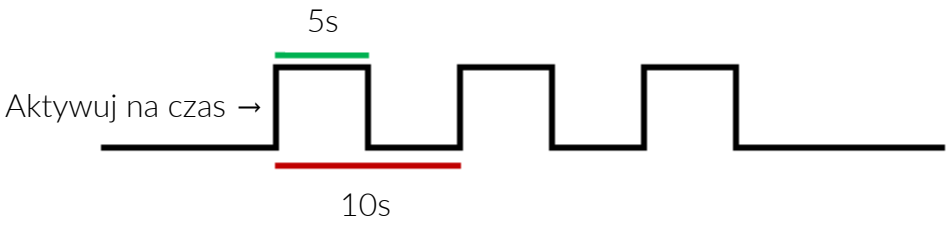
Ikona – ikona, która będzie reprezentować wyjście na wizualizacji.

Odwróć logikę – wybranie opcji odwróci logikę wyświetlania stanu wyjścia na wizualizacji.

Domyślne wartości komendy „Aktywuj na czas”:

Czas pojedynczego impulsu [s] – czas wysterowania pojedynczego impulsu po komendzie „Aktywuj na czas” (w przykładzie ***Czas pojedynczego impulsu [s]*** = 5.)

Liczba impulsów – liczba impulsów po komendzie „Aktywuj na czas” (w przykładzie ***Liczba impulsów*** = 3)

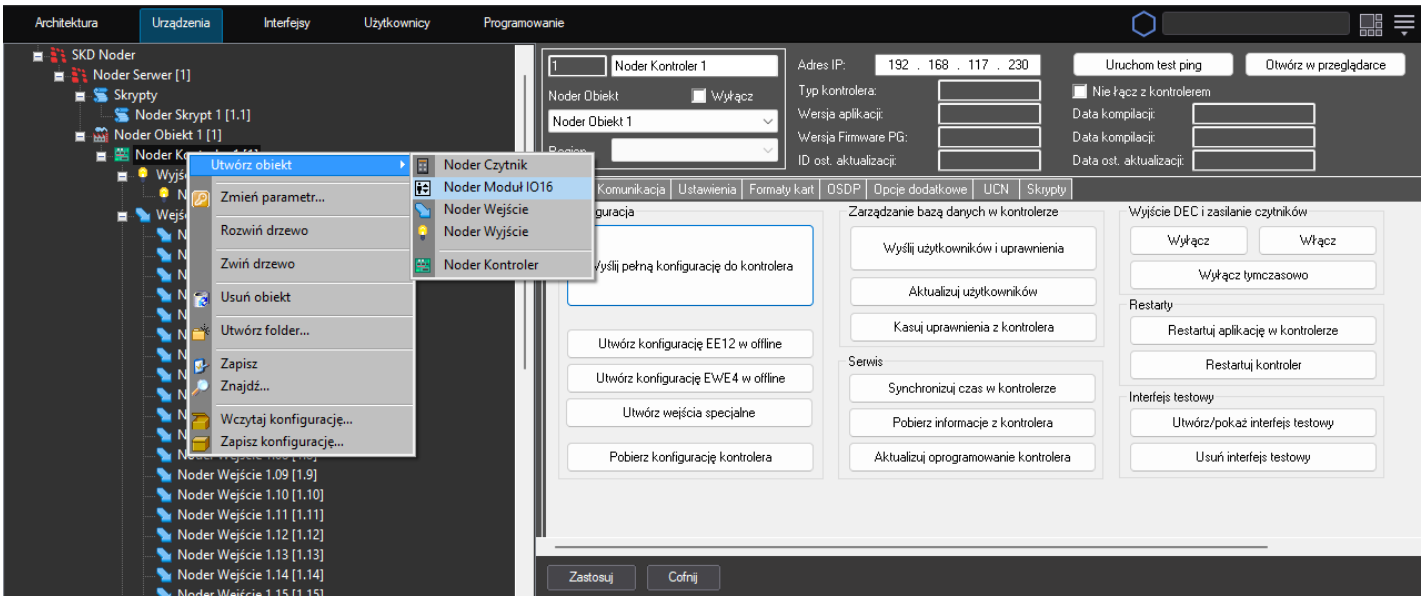


3.8 Moduł IO16

Po połączeniu i skonfigurowaniu kontrolera, administrator może dodać moduł IO16RS.

3.8.1 Konfiguracja Modułu IO16

Aby utworzyć obiekt należy kliknąć prawym przyciskiem myszy na kontrolerze, do którego jest on fizycznie podłączony i wybrać ***Noder Moduł IO16***.



Po wybraniu obiektu otwarte zostanie okno, w którym można mu przypisać numer i nazwę. Po zatwierdzeniu wyświetlone zostanie poniższe okno.

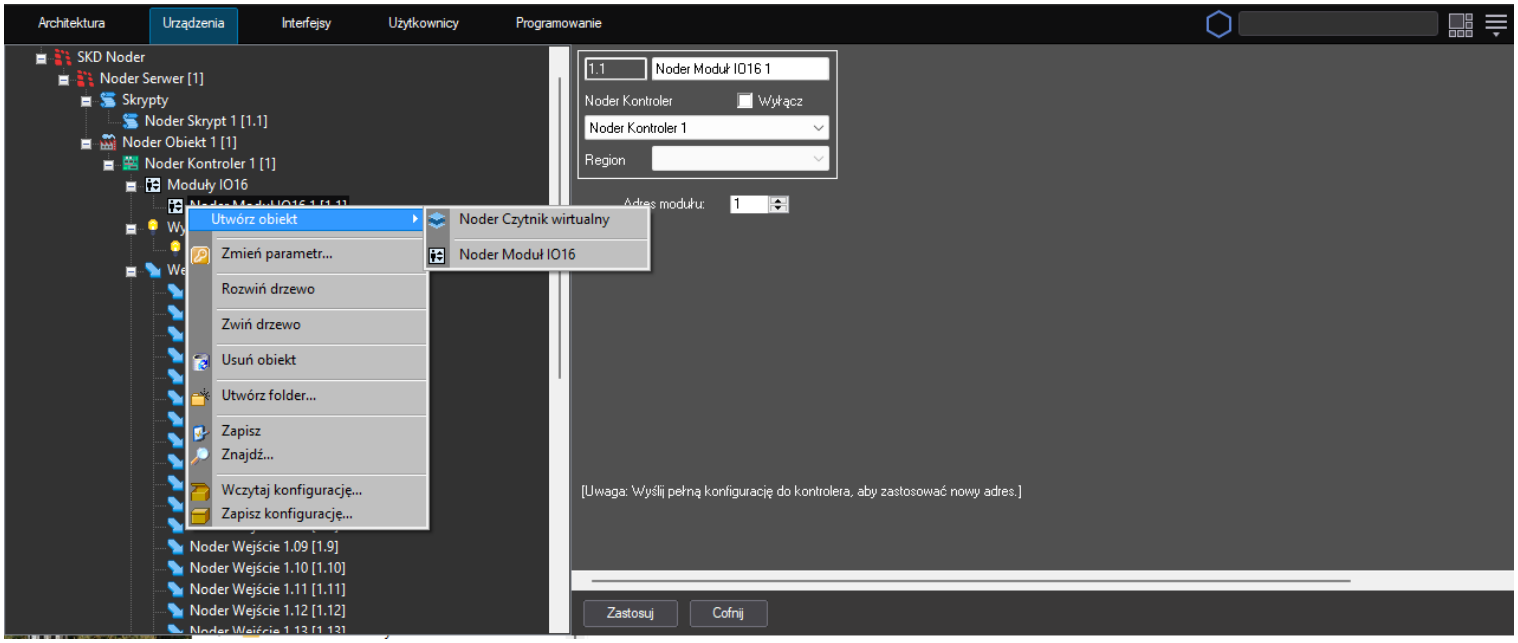
Adres obiektu musi być taki sam jak ustawiony na DIP switchu modułu. Adresacje modułu opisano w dokumencie *Noder DTR-IO16RS*. Do jednego kontrolera EE12 i EWE4 może być podłączone po 4 moduły. W przypadku kontrolera EE12 należy podłączyć moduł do magistrali rozszerzeń (port 4), a dla EWE4 do magistrali RS485. Na magistrali RS485 może działać jeden typ urządzeń, dlatego EWE4 obsługuje tylko czytniki na magistrali Wiegand razem z IO16.

Po nadaniu adresu należy kliknąć ***Zastosuj*** i wysłać konfigurację do kontrolera klikając ***Wyślij pełną konfigurację do kontrolera*** w jego ustawieniach. W tym momencie urządzenie powinno nawiązać połączenie. Diody komunikacji RX i TX na kontrolerze i module powinny zacząć migać z częstotliwością 10Hz.

Do sprawdzenia połączenia można utworzyć interfejs testowy. Przy poprawnym połączeniu w Podglądzie zdarzeń wyświetlone zostanie zdarzenie „Połączono” i ikona modułu będzie świeciła na zielono.

3.8.2 Konfiguracja Czytnika wirtualnego

IO16RS posiada 16 wyjść przekaźnikowych, które mają reprezentować poszczególne piętra budynku. Do utworzenia obiektu należy kliknąć prawym przyciskiem myszy na obiekcie ***Noder Moduł IO16*** i wybrać ***Noder Czytnik wirtualny***.



Po przypisaniu numeru i nazwy do piętra otwarte zostanie okno jego konfiguracji.

Adres – unikalny adres dla piętra numerowany od 1000 dla każdego obiektu Noder Czytnik wirtualny.

Czytnik – fizyczny czytnik w windzie, który powinien być przypisany do każdego piętra, do którego winda ma dostęp. Po przyłożeniu do niego uprawnionej karty moduł windowy wysteruje przekaźniki IO16RS (reprezentujące piętra), do których uprawniony jest użytkownik.
Numer wyjścia – numer wyjścia przekaźnikowego przypisanego do piętra.

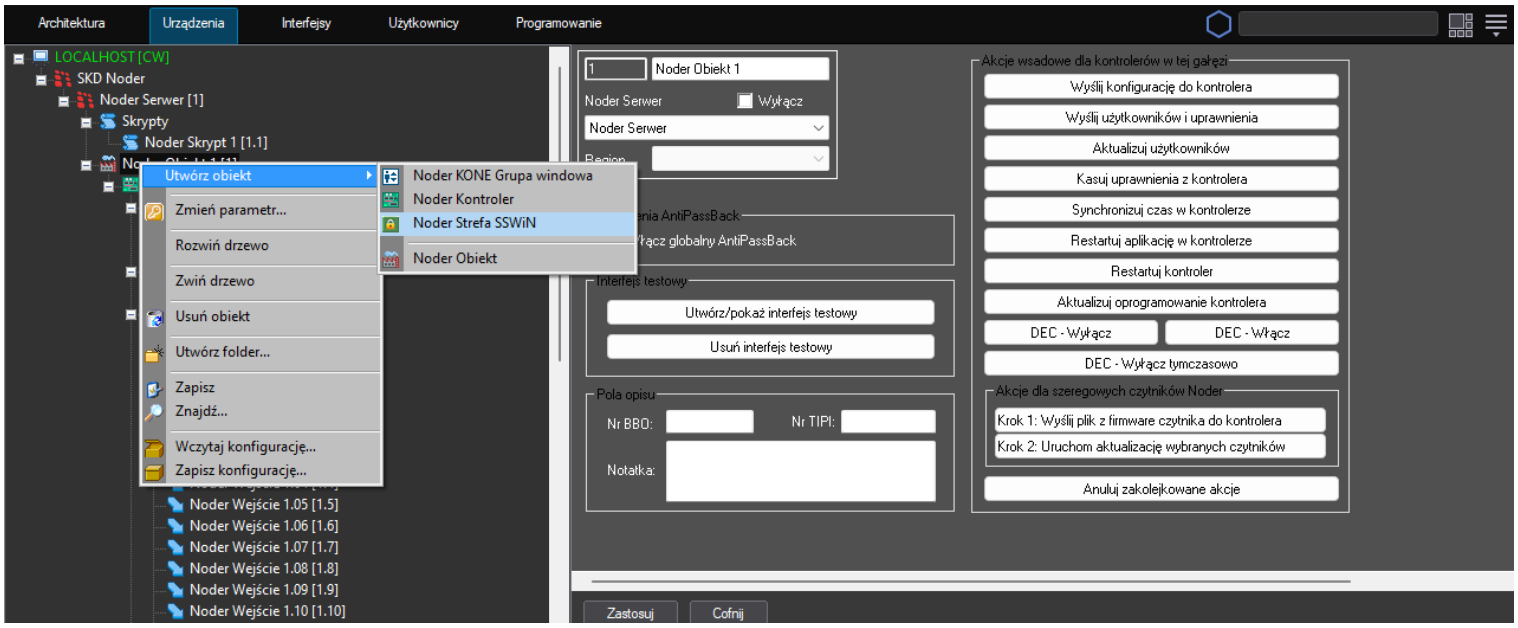
Czas otwarcia styku – czas wysterowania styku przekaźnika po przyłożeniu uprawnionej karty lub po komendzie operatora „Otwórz jednorazowo".

Ikona – ikona reprezentująca piętro na wizualizacji

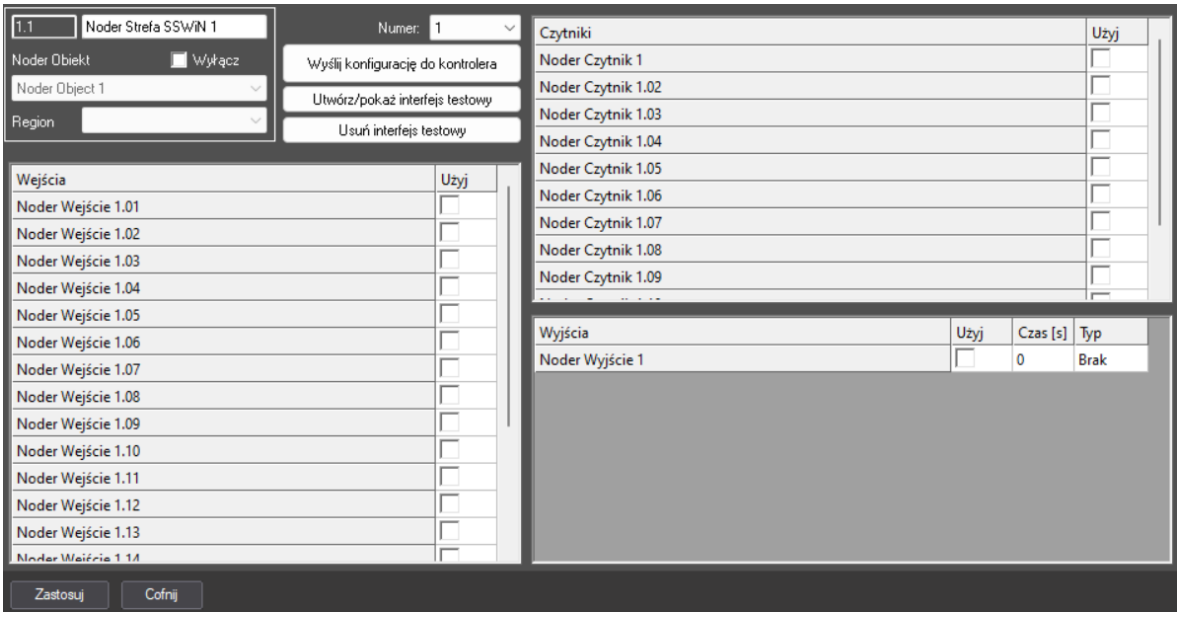
Należy pamiętać, aby po każdorazowej zmianie konfiguracji zastosować zmiany klikając ***Zastosuj*** *i wysłać pełną konfigurację do kontrolera klikając* ***Wyślij pełną konfigurację do kontrolera*** *w jego ustawieniach.*

3.9 Noder Strefa SSWiN

Do utworzenia obiektu należy kliknąć prawym przyciskiem myszy na obiekt ***Noder Obiekt***, do którego będzie przypisana strefa i wybrać ***Noder Strefa SSWiN***.

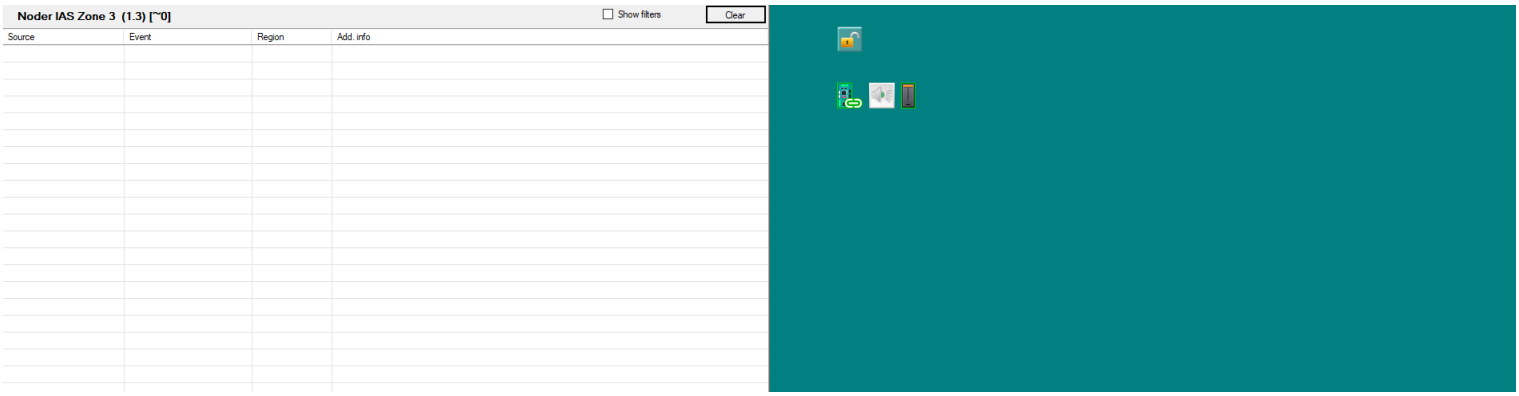


Po przypisaniu nazwy i numeru do strefy, wyświetlone zostanie okno jej konfiguracji.



Wyślij konfigurację – opcja wysyła aktualną konfigurację strefy do wszystkich kontrolerów znajdujących się na obiekcie.

Utwórz/pokaż interfejs testowy – tworzy interfejs kontrolera składający się z podglądu zdarzeń dotyczącego danej strefy oraz mapy z ikonami wszystkich czytników, wejść i wyjść danego kontrolera w strefie. Jeżeli taki interfejs testowy został utworzony wcześniej ponowne wywołanie tej funkcji spowoduje odświeżenie mapy wg bieżącej konfiguracji i wyświetlenie interfejsu:



Usuń interfejs testowy – opcja usuwa utworzony wcześniej interfejs testowy.

Wejścia – po wybraniu wejść i wysłaniu konfiguracji zostaną one przypisane do strefy. Ich konfiguracja została opisana w rozdziale Wejścia.

Czytniki – po wybraniu czytników i wysłaniu konfiguracji zostaną przypisane do strefy. W przypadku wystąpienia alarmu (nie dotyczy cichego alarmu) lub sabotażu rozpoczną alarmowanie. Czytnik przypisany do strefy może być również używana do uzbrajania/rozbrajania strefy. Zachowanie czytnika:

Strefa rozbrojona – czerwona dioda na czytniku (normalny stan czytnika)

Strefa uzbrojona – czerwona dioda migająca z częstotliwością 0.5Hz

Uzbrajanie strefy – 3xbeeper z częstotliwością 2.5Hz. Gdy strefa jest ***Niegotowa do uzbrojenia*** przy próbie uzbrojenia – pomarańczowa dioda i ciągły sygnał przez 1s.

Rozbrajanie strefy – 2xbeeper z częstotliwością 1Hz.

Alarm – beeper z częstotliwością 2.5Hz przez ***Czas aktywacji alarmu [s]*** i czerwona dioda z częstotliwością 2.5Hz do resetu alarmu.

Reset alarmu – beeper z częstotliwością 2.5Hz przez ***Czas aktywacji alarmu [s]*** i czerwona dioda z częstotliwością 2.5Hz do resetu alarmu → czerwona dioda na czytniku.

Wyjścia – po wybraniu wyjścia i wysłaniu konfiguracji będzie ono należeć do strefy. Aby mogło ono działać poprawnie należy wybrać typ akcji i czas wysterowania przekaźnika.

4. Zarządzanie użytkownikami

Zarządzanie użytkownikami oraz poziomami dostępu jest możliwe przy użyciu Menadżera KD (Access Manager). Menadżer KD jest elementem Interfejsu. Do zarządzania użytkownikami kontroli dostępu powinien zostać stworzony specjalny użytkownik o odpowiednich uprawnieniach.

Szczegóły dotyczące obsługi użytkowników, poziomów dostępu oraz SKD i SSWiN NODER znajdują się w Instrukcji Operatora Kontroli Dostępu, która jest dostępna pod https://noder.systems/materialy-techniczne/.