

Instrukcja konfiguracji kontrolera sieciowego Z5R-WEB- Mini



WWW.HATPOL.PL

biuro@hatpol.pl

Proszę uważnie przeczytać instrukcję przed podejściem do zainstalowania urządzenia. HatPol nie bierze odpowiedzialności za złą interpretację poniższej instrukcji.

Spis treści

1. PRZEGLĄD	3
2. SPECYFIKACJA.....	4
3. PODŁĄCZENIE URZĄDZEŃ ZEWNĘTRZNYCH	5
4. KONFIGURACJA	8
5. INTERFEJS SIECIOWY	9
5.1 Wybór języka	9
5.2 Zakładka status	10
5.3 Zakładka konfiguracji połączenia	10
5.4 Zakładka trybu połączenia dla oprogramowania sterującego	11
5.4.1 Sieć	12
5.4.2. Serwer	13
5.4.3. Klient	13
5.4.4. Tryb autonomiczny	13
5.5 Zakładka ustawień kontrolera.	14
5.5.1 Zakładka ustawień zaawansowanych.	15
5.5.2. Wyłączanie interfejsu sieciowego.....	16
6. WŁĄCZENIE I ROZPOCZĘCIE PRACY.....	16
7. USTAWIENIE KONTROLERA PRZY POMOCY KLUCZA MASTER	17
7.1. Tryb dodawanie kluczy Normal	18
7.2. Tryb dodawania kluczy Master	18
7.3 Tryb usuwania wszystkich kluczy	19
7.5 Ustawianie czasu otwarcia zamka.	19
7.6 Tryb Accept.	19
7.7. Tryby dostępu.	20
8. POŁĄCZENIE SIECI I TRYB AUTONOMICZNY.....	20
9. AKTUALIZACJA LUB PRZYWRACANIE OPROGRAMOWANIA PRZEZ USB.....	21
10. ZAWARTOŚĆ OPAKOWANIA.	21
11. WARUNKI PRACY.....	21
12. TRANSPORT I MAGAZYNOWANIE.....	21
12. PRZYKŁAD KONFIGURACJI Z5R-WEB Z USŁUGĄ GUARD-SAAS.	22

1. PRZEGLĄD

Kontroler Z-5R WEB Mini jest używany w systemach kontroli dostępu (ACS) do kontroli pojedynczego punktu dostępu.

Kontroler może pracować w trybie autonomicznym lub sieciowym.

W trybie sieciowym, konieczne jest zewnętrzne oprogramowanie sterujące w celu obsługi i przechowywania kluczy kontrolera w bazie danych. Oprogramowanie umożliwia również czytanie dzienników zdarzeń, ustawienie czasu kontrolera i określenie okresów, kiedy dostęp jest umożliwiony dla każdej karty.

W obu trybach kontroler podejmuje decyzję o zezwoleniu na dostęp na podstawie wewnętrznej bazy kluczy oraz wybiera aktualny tryb działania niezależnie od połączenia z oprogramowaniem sterującym.

Aby działać w trybie sieciowym kontroler może zostać podłączony do sieci poprzez adapter sieciowy Wi-Fi.

W trybie konfiguracji kontroler staje się punktem dostępowym zapewniając możliwość komunikacji z istniejącą siecią Wi-Fi i konfigurację parametrów.

Decyzja o dostępie za pośrednictwem punktów dostępu zostanie dokonana poprzez analizę stanu kluczy znanych urządzeniu: karty zbliżeniowe, kluczy pamięci dotykowej lub kodów PIN. Wszystkie te klucze będą określane później jako "klucze".

Dzięki swojej funkcji, klucze wchodzą w kategorię kluczy programujących lub kluczy dostępu.

Klucze dostępu to klucze **Normal i Block**. Klucze Block mają więcej praw niż klucze Normal.

W trybie **Normal**, kontroler umożliwia dostęp dla obu kluczy - Normal i Block.

W trybie **Block**, dostęp jest możliwy tylko dla kluczy Block, a zablokowany dla kluczy Normal.

Przykład użycia: wszystkim pracownikom zostają przydzielone klucze Normal, a ochrona dostaje klucze Block.

W godzinach pracy, kontroler pracuje w trybie Normal i wszyscy pracownicy mogą uzyskać dostęp. Poza godzinami pracy, tryb Block jest włączony i tylko ochrona może mieć dostęp.

Klucze Master są to klucze, które programują kontroler. **Działają tylko w celu programowania kontrolera w trybie autonomicznym (samodzielnym) i nie mogą być stosowane w celu uzyskania dostępu.**

Klucze Master pozwalają na:

- Dodawanie i usuwanie kluczy Normal, Block i pozostałych kluczy Master;
- Ustawienie czasu sygnału otwarcia w urządzeniach zamykających (kontrola dostępu);
- Włączanie i wyłączanie trybu Accept.

W trybie Accept, każdy klucz ma możliwość dostępu i jest przechowywany w pamięci kontrolera jako klucz Normal. Tryb ten pomaga odzyskać bazy danych kluczy, w momencie gdy nowy system (ACS) jest instalowany na miejscu u klienta, a klucze dostępu zostały wcześniej wydane. W tym przypadku przez pewien czas kontroler jest wprowadzony do trybu Accept, co pozwala na zbieranie i przechowywanie kluczy w jego pamięci. Potem, gdy kontroler powraca do trybu Normal, wyłącznie te zapisane klucze mogą uzyskać dostęp.

W celu zebrania kodów kluczy, kontroler współpracuje z dwoma protokołami czytników (jednym do wejścia i jednym do wyjścia) poprzez Wiegand (-26, -34, -42 lub -50) lub iButton™ (Dallas Touch Memory). Każdy czytnik wykorzystuje osobne bazy danych kluczy w pamięci kontrolera. Po udzieleniu dostępu dla klucza, kontroler wysyła sygnał sterujący (otwarcia/zamknięcia tranzystora) do urządzenia blokującego (zamka elektromechanicznego lub elektromagnetycznego lub zatrasku lub bramki obrotowej). Urządzenie blokujące oraz protokół połączenia zostają wybrane podczas instalacji i konfiguracji kontrolera.

Kontroler umożliwia przechowywanie 2048 zdarzeń w swoim buforze. Zdarzenia te obejmują uzyskanie kodu, operacje czujnika drzwi, generowanie sygnału sterującego itp.

W celu poprawienia funkcjonalności, kontroler umożliwia:

- Podłączenie czujnika drzwi w celu zarejestrowania zdarzenia "nastąpiło przejście", a zmniejszenie czasu trwania alarmu "drzwi otwarte" (i ograniczenie czasu trwania sygnału odblokowania dla urządzenia blokującego).
- Podłączenie przycisku zwalniającego drzwi ("wyjście"), aby otworzyć drzwi bez kontroli dostępu.
- Podłączenie zewnętrznego sygnału odblokowania awaryjnego, tak aby drzwi mogły być otwierane w sytuacjach awaryjnych.

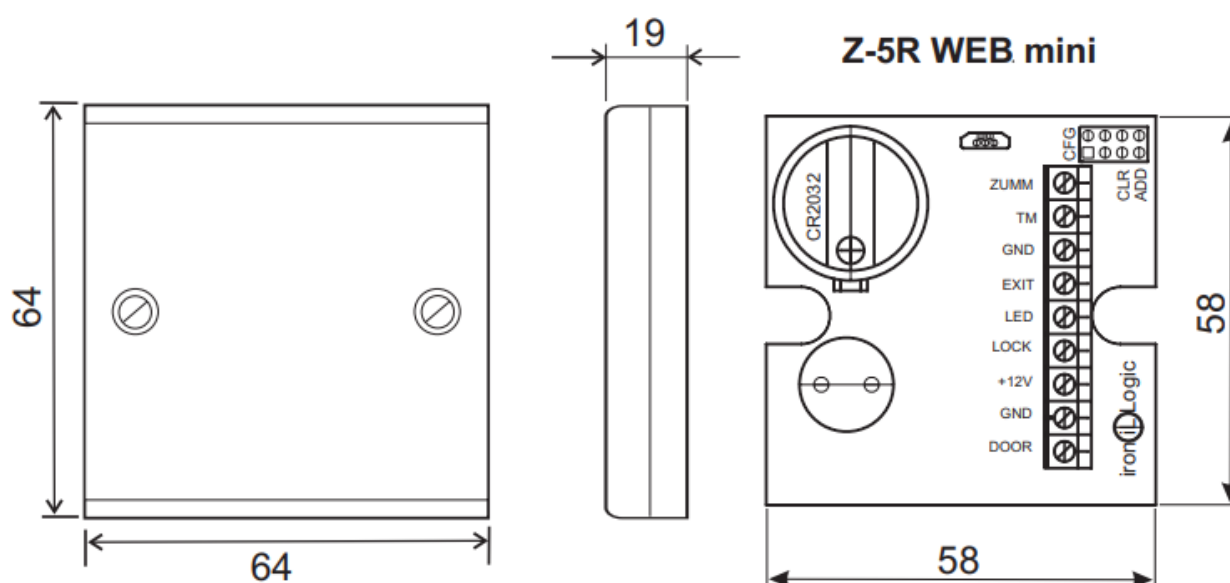
2. SPECYFIKACJA

Pamięć kluczy	2024 kluczy
Pamięć zdarzeń	2048 zdarzeń
Ilość czytników (max.)	2
Protokoły podłączenia czytników	Wiegand, iButton™
Kontrolka wskazań czytnika	tak
Wyjście do podłączenia zamka	Tranzystor MOS
Moc wyjściowa prądu	5 A
Zworka do wyboru typu zamka	Elektromagnetyczny, elektromechaniczny
Ustawienie czasu otwarcia zamka	0.1 s to 6,500s (wartość fabryczna: - 3)
Moduł komunikacyjny Wi-Fi	
Obsługiwane standardy	IEEE 802.11 b/g
Zakres częstotliwości	2.4-2.4835 GHz
Szybkość transmisji	11g: do 54 Mbit/s
	11b: do 11 Mbit/s

Moc sygnału sieci bezprzewod.	Do 20 dBm (do 100 mW)
Tryby pracy bezprzewodowej	Punkt dostępu, Klient
Zabezpieczenia sieci bezprzewodowej	PA/WPA2, WPAPSK/WPA2-PSK
USB	
Typ złącza USB	USB Typ micro A
Wersja USB	USB 2.0
Tryb USB	Device, Full/Low Speed
Inne parametry	
Waga	150 g
Wymiary, mm	64x64x19
Zabezpieczenie przed nieprawidłowym podłączeniem	tak
Zasilanie	12 V (dozwolone 9-24)
Prąd roboczy (12V)	Do 300 mA (bez czujników)
Audiowizualna kontrola zwrotna trybów pracy	tak
Maksymalny pobór prądu przy 12V	100mA

3. PODŁĄCZENIE URZĄDZEŃ ZEWNĘTRZNYCH

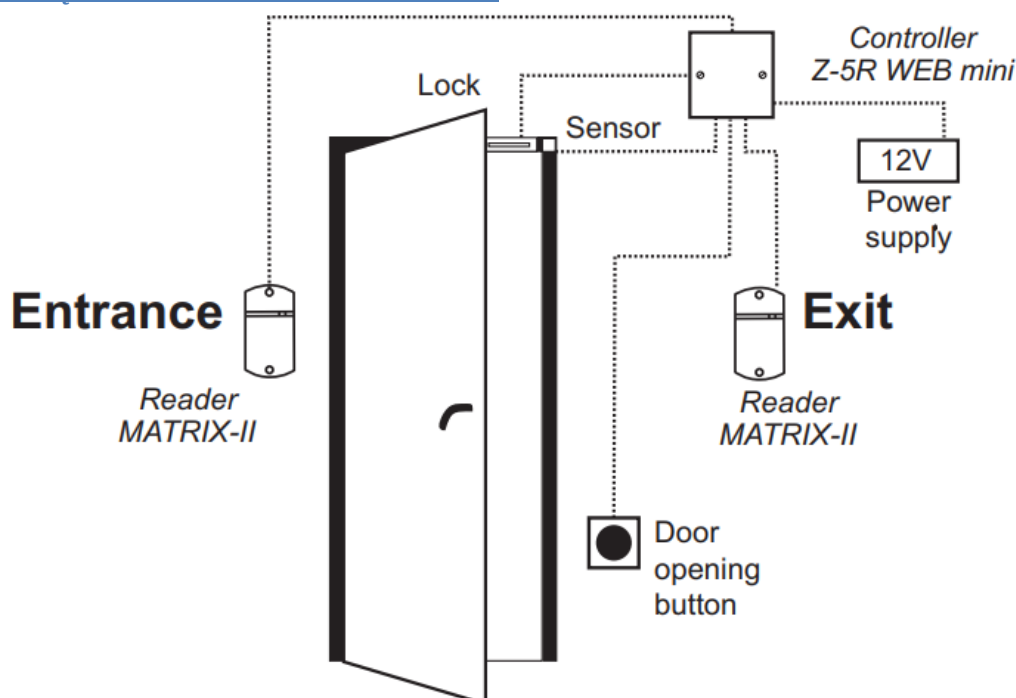
Rysunek przedstawia wymiary urządzenia oraz układ zacisków na płycie głównej.



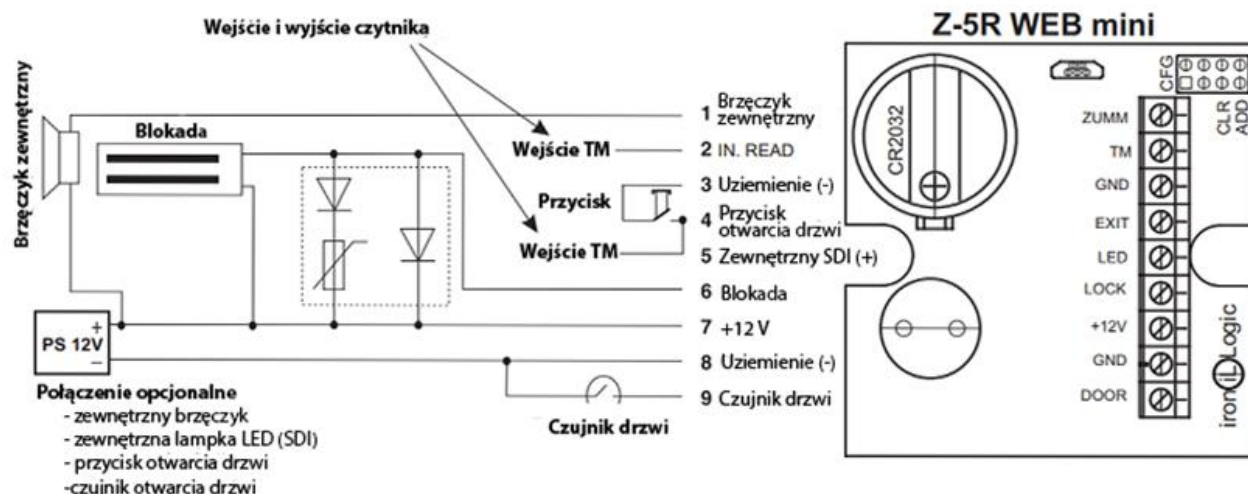
Przeznaczenie terminali przedstawia poniższa tabela

ZUMM	Do podłączenia zewnętrznego brzęczyka. Niezbędne jest użycie brzęczyka z wbudowanym generatorem na napięcie 12 V i poborem prądu nie większym niż 200mA. Dodatni pin powinien być podłączony do zacisku +12V, a ujemny do tego zacisku.
TM	Zewnętrzny czytnik lub stycznik w trybie Wiegand: sygnał DATA0.
GND	Uziemienie sygnału. Aby podłączyć wspólne przewody czytnika zewnętrznego, stycznika, czujnik położenia drzwi i przycisk otwierania drzwi.
EXIT	Przycisk otwierania drzwi. Czytnik wewnętrzny lub stycznik można podłączyć jednocześnie. W trybie Wiegand: sygnał DATA1.
LED	Kontrolka zielonej diody LED czytnika zewnętrznego.
LOCK	Zacisk do podłączenia ujemnego przewodu uzwojenia zamka (Wyjście: Sygnał mocy wyjściowej. Drugi (ujemny) przewód idzie do zamka. Wyjście to tranzystor polowy.)
+12	Dodatni przewód zasilający. Również dodatni przewód od zamka.
GND	Uziemienie zasilania. Podłączenie ujemnego pinu zasilacza
DOOR	Wejście: Czujnik drzwi. Kiedy drzwi są zamknięte, muszą być zwarte z uziemieniem. Zacisk ten jest wielofunkcyjny i pozwala na przeniesienie jego funkcji. Podłączenie czujnika położenia drzwi. Zalecana jest skrętka. Kiedy drzwi są otwarte czujnik pozwala na włączenie z wyprzedzeniem dźwięku na sterowniku. Umożliwia także oszczędzanie energii poprzez włączenie blokady elektromechanicznej natychmiast po otwarciu drzwi lub włączeniu zamka elektromagnetycznego tylko wtedy, gdy drzwi są już zamknięte.

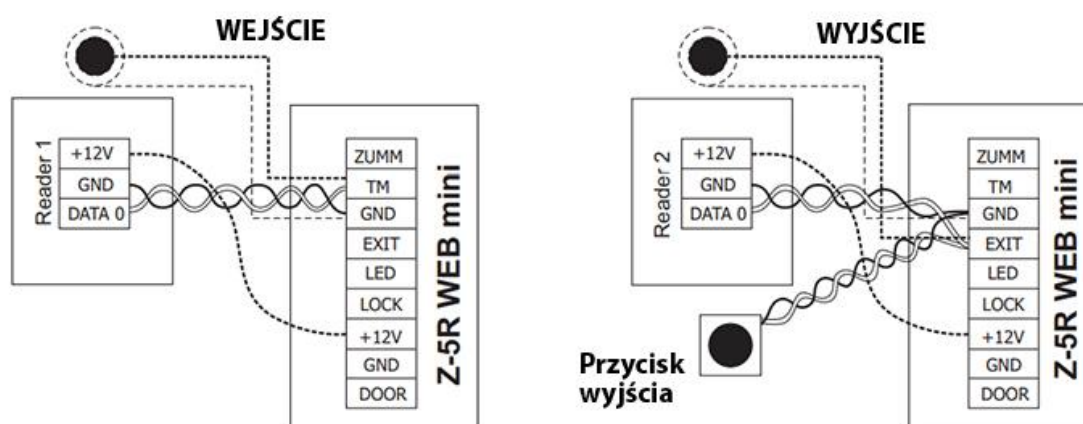
Schemat podłączenia dla Z5R- Web-Mini



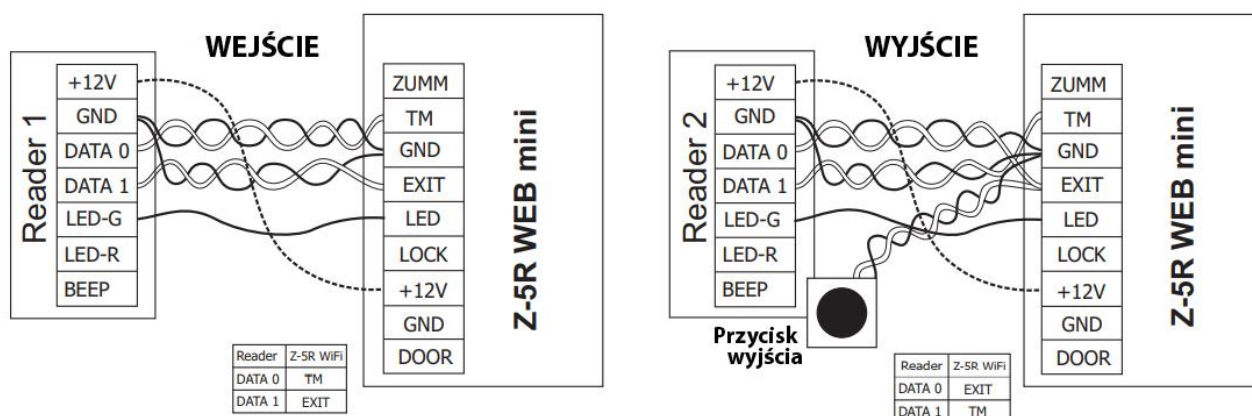
Schemat podłączenia urządzeń zewnętrznych



Schemat podłączenia czytników zewnętrznych poprzez protokół iButton

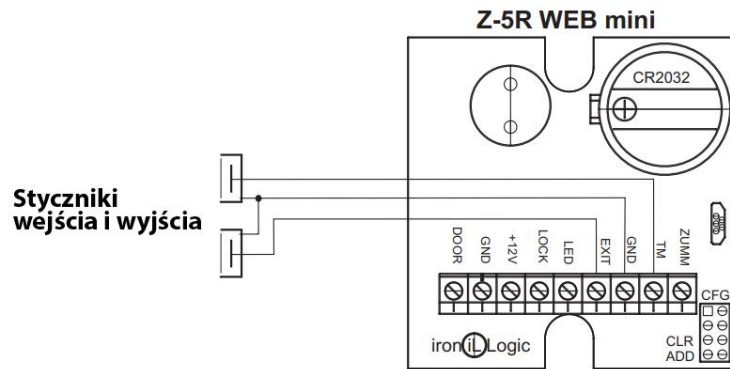


Schemat podłączenia czytników zewnętrznych poprzez protokół Wiegand



Uwaga: Należy podłączyć oba czytniki do tego samego protokołu! Sterowanie sygnałem czytnika jest wspólne dla obu czytników.

Schemat podłączenia styczników



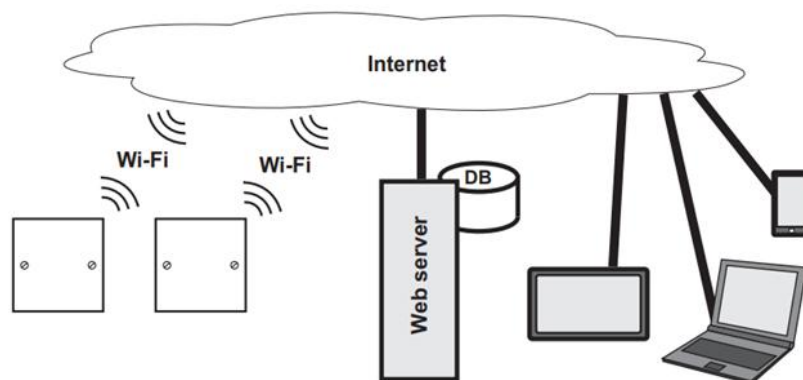
4. KONFIGURACJA

Ważne: Podczas konfigurowania kontrolera Z-5R Web Mini, należy pamiętać, że w rzeczywistości składa się on z dwóch modułów: kontrolera ACS oraz modułu połączenia sieciowego.

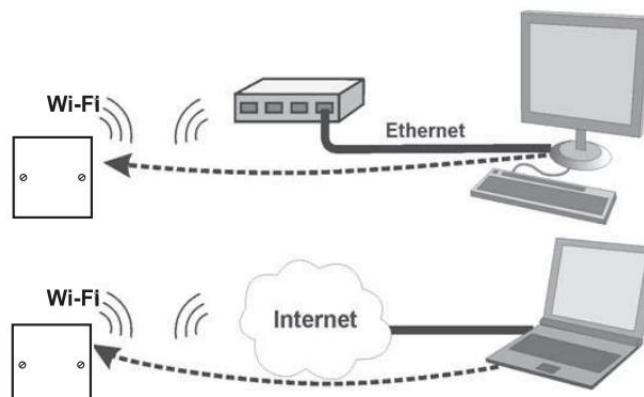
Moduł sieciowy pozwala na podłączenie do komputera z zainstalowanym oprogramowaniem sterującym ACS, aby korzystać z funkcji kontroli dostępu (ładowanie bazy danych karty, zarządzanie kontrolą dostępu, pobieranie dziennika zdarzeń z bufora itp.)

Istnieją trzy tryby połączenia oprogramowania sterującego:

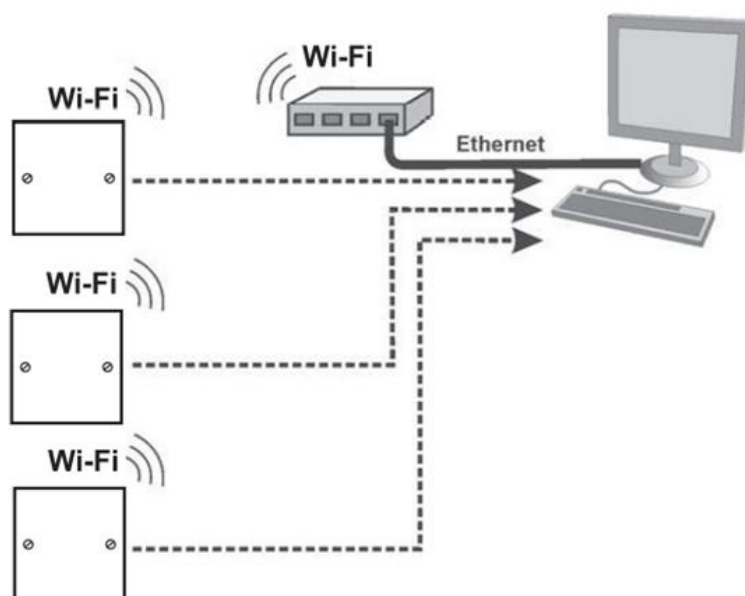
- Tryb połączenia **internetowego**. Moduł połączeniowy łączy się z serwerem WWW przez Internet, a kontroler jest zarządzany za pośrednictwem wewnętrznej witryny sieci Web (np. „chmura ACS- WWW.guardsaas.com)



- Tryb połączenia z **serwerem**. Moduł połączeniowy oczekuje na połączenia przychodzące TCP / IP z oprogramowania sterującego PC (takiego jak GuardLight, GuardCommander, Avantgarde).



- Tryb połączenia z **klientem**. Moduł połączeniowy próbuje połączyć się z oprogramowaniem sterującym za pośrednictwem protokołu TCP/IP. Aby skonfigurować połączenie, należy podać adres IP i numer portu komputera z oprogramowaniem sterującym (takie jak GuardLight lub Avangarde).



5. INTERFEJS SIECIOWY

Interfejs WWW służy do konfigurowania parametrów połączenia i podłączonych urządzeń. Wymagane jest połączenie urządzenia z siecią Wi-Fi (smartfon, tablet lub laptop) oraz przeglądarki internetowej (Internet Explorer, Firefox, Opera, Chrome itd.)

Aby uzyskać dostęp do interfejsu sieciowego należy wykonać następujące czynności:

1. Ustaw zworkę w pozycji **CFG** (patrz punkt 6 „Włączanie urządzenia i rozpoczęcie pracy”);
2. Włącz zasilanie;
3. Połącz urządzenie z Wi-Fi:
 - Poczekaj na pojawienie się sieci Wi-Fi o nazwie Z-5R WiFi_XXXXXX;
 - Połącz się z tą siecią (hasło: AUTH_KEY);
 - **AUTH_KEY** znajduje się na etykiecie obudowy lub PCB urządzenia – fabryczna wartość ma 8 znaków i uwzględnia wielkość liter;
4. Za pomocą przeglądarki otwórz stronę pod adresem: <http://192.168.10.1> (**login:** z5rwebmini, **hasło:** AUTH_KEY);
5. Przejdź przez wyświetlane menu karta po karcie i skonfiguruj parametry na każdej z kart (należy pamiętać, aby za każdym razem nacisnąć „Zapisz” na każdej stronie).

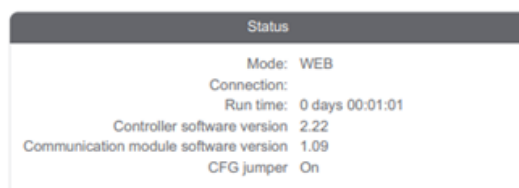
Po zakończeniu konfiguracji należy usunąć zworkę z pozycji **CFG**, uruchomić ponownie kontroler i poczekać, aż połączy się z siecią lokalną. Teraz interfejs sieciowy będzie dostępny pod adresem IP, który został nadany podczas konfiguracji (opis poniżej w punkcie 5.3) lub otrzymany z routera (serwer DHCP) podczas rejestracji w sieci lokalnej.

5.1 Wybór języka

Przy pierwszej aktywacji w interfejsie sieciowym ustawiony jest język angielski.

5.2 Zakładka status

Wyświetla aktualny status kontrolera.



Status	
Mode:	WEB
Connection:	
Run time:	0 days 00:01:01
Controller software version	2.22
Communication module software version	1.09
CFG jumper	On

Legenda:

Mode (Tryb pracy urządzenia): WEB, serwer, klient, autonomiczny

Connection (Połączenie): W trybach Klient i Serwer wyświetla adres IP komputera, z którym nawiązywane jest połączenie

Run time (Czas pracy): Czas pracy urządzenia od momentu włączenia zasilania.

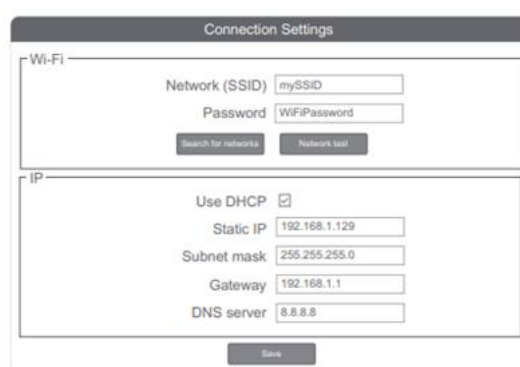
Controler software version (Wersja oprogramowania kontrolera): Wyświetla aktualną wersję oprogramowania kontrolera

Communication module software version (Wersja oprogramowania modułu komunikacyjnego): Wyświetla aktualną wersję oprogramowania modułu komunikacyjnego

CFG Jumper (Zworka CFG): wyświetla stan zworki: włączona- zainstalowana, wyłączona- usunięta

5.3 Zakładka konfiguracji połączenia

Zakładka konfiguracji połączenia pozwala na ustawienie typu połączenia i parametrów połączenia sieciowego. Konfiguracja parametrów jest podobna do tych co routera internetowego.

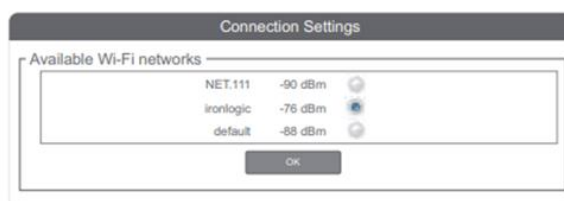


Connection Settings	
Wi-Fi	
Network (SSID)	mySSID
Password	WiFiPassword
Search for networks Network test	
IP	
Use DHCP	☒
Static IP	192.168.1.129
Subnet mask	255.255.255.0
Gateway	192.168.1.1
DNS server	8.8.8.8
Save	

Sieć (SSID): nazwa sieci Wi-Fi, do której zostanie podłączone urządzenie.

Hasło: Klucz szyfrowania (hasło) używany w powyższej sieci Wi-Fi.

Szukanie sieci: Aktywacja wyszukiwania aktualnie dostępnych sieci Wi-Fi. Po tym jak wyszukiwanie dostępnych sieci zostanie zakończone, pojawi się lista znalezionych sieci z wyświetloną siłą sygnału.



Aby wybrać podświetl żądaną sieć, a następnie naciśnij OK. Potem nazwa sieci pojawi się automatycznie w ustawieniach. Jeśli sieć nie wyświetla swojej nazwy, należy ją ręcznie wprowadzić w polu Sieć (SSID). Podczas używania szyfrowania należy wprowadzić klucz szyfrowania.

Test sieci: Weryfikacja łączności na podstawie aktualnych wartości sieci Wi-Fi i hasła. Jeśli pomimo poprawnego hasła nie można się połączyć z routerem należy sprawdzić adres MAC urządzenia.

Użyj DHCP: serwer DHCP automatycznie zapewnia adres IP i inne parametry sieciowe niezbędne do pracy w tej sieci LAN.

W przypadku braku serwera DHCP należy poprawnie skonfigurować następujące ustawienia sieciowe:

Statyczne IP: Unikalny adres IP przypisany do kontrolera.

Maska sieci: Maska podsieci używana w tym segmencie sieci LAN.

Brama domyślna: Adres IP bramy prowadzącej do innych sieci, w tym Internetu.

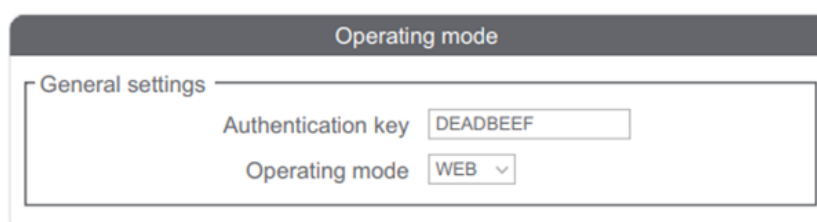
Serwer DNS: adres IP serwera DNS.

Dla prawidłowej pracy kontrolera, należy skonfigurować wszystkie parametry sieci. Jeśli nie znasz wszystkich tych parametrów należy odnieść się do administratora sieci.

Zapisz wszystkie ustawienia na tej karcie za pomocą przycisku **Zapisz**.

5.4 Zakładka trybu połączenia dla oprogramowania sterującego

Jeśli Z-5R WEB-Mini ma pracować w trybie sieciowym, to znaczy na zasadzie zewnętrznego oprogramowania sterującego to po zakończeniu połączenia z siecią LAN, konieczne jest również, aby skonfigurować tryb połączenia pomiędzy modułem połączeniowym i oprogramowaniem sterującym. Zakładka ta pozwala na wybór trybu połączenia dla oprogramowania sterującego.



Gdzie:

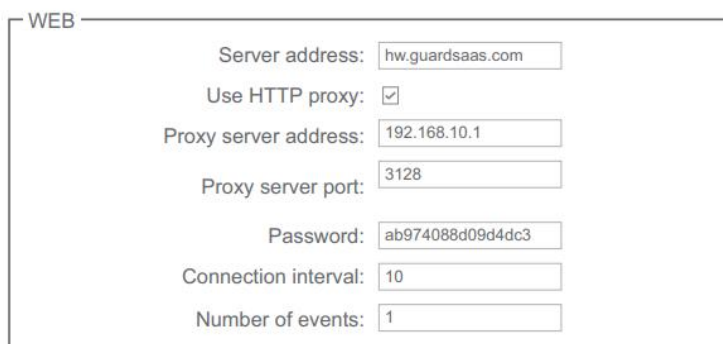
Klucz autoryzacji jest wymagany do połączenia z serwerem internetowym, w chmurze SaaS, w trybie WEB podczas pracy przez serwer, a także dostęp do interfejsu sieciowego kontrolera.

Początkowo to pole zawiera klucz fabrycznie ustawiony, widoczny na naklejce z tyłu obudowy urządzenia, pod etykietą AUTH_KEY. Jeśli jest to konieczne, klucz może zostać zmieniony w tym momencie. (Tylko znaki alfanumeryczne są dozwolone).

Tryb połączenia oprogramowania: Wybierz **sieć**, **serwer**, **klienta** dla funkcjonowania sieci lub tryb **autonomiczny** w celu obsługi bez połączenia oprogramowania sterującego.

5.4.1 Sieć

Tryb połączenia sieci Web służy do podłączenia do chmury obliczeniowej SaaS. W celu konfiguracji, następujące parametry są wymagane od dostawcy SaaS:



WEB

Server address:	hw.guardsaas.com
Use HTTP proxy:	☒
Proxy server address:	192.168.10.1
Proxy server port:	3128
Password:	ab974088d09d4dc3
Connection interval:	10
Number of events:	1

Adres serwera: Nazwa DNS lub adres IP serwera sieci Web, gdzie kontroler będzie się łączyć.

Użyj serwera proxy HTTP: Należy zaznaczyć tej checkbox, jeśli jest potrzeba, by połączyć się ze specjalnym serwerem sieciowym.

Adres serwera Proxy: adres sieciowy serwera Proxy w sieci lokalnej.

Port serwera Proxy: port do połączenia z serwerem Proxy.

Hasło: hasło dostępu do danych na serwerze WEB.

Interwał transmisji: Odstęp między okresowymi połączeniami z serwerem internetowym w sekundach.

Ilość zdarzeń: Ilość oczekujących zdarzeń kontrolera, które powodują losową transmisję danych do serwera sieciowego, zanim skończy się aktualny przedział transmisji.

Po zakończeniu ustawień, należy zapisać parametry naciskając przycisk Zapisz.

5.4.2. Serwer

W trybie połączenia z serwerem, moduł połączeniowy wyłapuje połączenia oprogramowania sterującego do portu lokalnego. W tym trybie, następujące parametry muszą być spełnione:

Server	Local port:	1000
	Allowed IP:	255.255.255.255

Gdzie:

Port lokalny: Lokalny port TCP wyłapujący połączenia oprogramowania sterującego.

Dozwolone IP: Źródłowy adres IP, z którego oprogramowanie może połączyć się z kontrolerem. (Aby umożliwić dowolne IP, należy użyć wartości 255.255.255.255).

Po zakończeniu ustawień, należy zapisać parametry naciskając przycisk **Zapisz**.

5.4.3. Klient

W trybie połączenia klienta, moduł połączeniowy będzie regularnie starał się nawiązać połączenie z oprogramowaniem sterującym. Następujące parametry muszą być spełnione:

Client	Server address:	192.168.1.10
	Server port:	25000

Gdzie:

Adres serwera: adres IP komputera, z którym urządzenie powinno się połączyć w celu komunikacji z oprogramowaniem sterującym.

Port serwera: Port IP z którym należy nawiązać połączenie. Po skonfigurowaniu wszystkich parametrów należy nacisnąć „zapisz”.

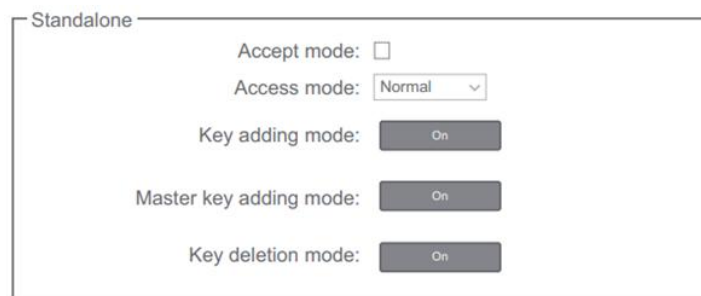
5.4.4. Tryb autonomiczny

Wstępna konfiguracja ACS, dokonywana przez zworki na innych kontrolerach na danym urządzeniu przechodzi w tryb **autonomiczny**. Współpracuje z bazą danych kluczy kontrolera poprzez interfejs sieciowy, bez konieczności użycia klucza Master.

Tworzenie i modyfikacja bazy danych kluczy może się odbywać na dwa sposoby:

- użycie czytnika zewnętrznego podłączonego do urządzenia Z5R-Web-Mini przez protokół iButton (konfiguracja bazy kluczy za pomocą czytnika podłączonego przez protokół Wiegand nie jest obsługiwana).

- przez tryb pracy autonomicznej. Należy wybrać ten tryb w przypadku sterowania pracą urządzenia przez interfejs WWW. Interfejs wygląda następująco:



The screenshot shows a web interface titled "Standalone". It contains the following settings:

- Accept mode: ☐
- Access mode: Normal (dropdown menu)
- Key adding mode: On (button)
- Master key adding mode: On (button)
- Key deletion mode: On (button)

Gdzie:

Tryb Accept: Włącza tryb Accept, w którym wszystkie nowe klucze będą przechowywane w pamięci jako klucze Normal.

Tryb dostępu: możliwa wartość do wybrania: Normal (normalny tryb przejścia).

Tryb Block: przejście jest możliwe dla użytkowników kart Block; **Free** (przejście jest otwarte), **Oczekiwanie** (ustawiane tylko przez interfejs sieciowy, kiedy punkt dostępu jest ustawiony w tryb Block, więc pierwsza zeskanowana karta (**Normal lub Block, ale nie karta główna Master**) przełączy tryb dostępu na pozycję **Free**).

Tryb dodawania kluczy: Aktywuje tryb dodawania kluczy Normal i Block na kontrolerze. Zobacz szczegóły w punkcie 7.1

Tryb dodawania klucza głównego (Master): Aktywuje tryb dodawania kluczy głównych (Master). Zobacz szczegóły w punkcie 7.2.

Tryb usuwania kluczy: Usuwa klucze Normal i Block z bazy danych. Zobacz szczegóły punkcie 7.3 . Klucze główne (Master) nie są usuwane w tym trybie.

Po włączeniu trybów „Dodawanie kluczy”, „Dodawanie klucza głównego” i „Usuwanie klucza” na przycisku pojawi się licznik informujący, ile czasu pozostało do momentu, kiedy kontroler automatycznie opuści ten tryb.

5.5 Zakładka ustawień kontrolera.

Zakładka ustawień kontroler pozwala skonfigurować parametry operacyjne kontrolera.

Typ zamka: Elektryczny zatrzask, elektromagnetyczny lub elektromechaniczny.

Jeśli typ zamka jest konfigurowany przez oprogramowanie sterujące, nie będzie możliwa zmiana typu zamka, do czasu przywrócenia ustawień fabrycznych z poziomu interfejsu sieciowego lub zworki. Wówczas to pole wyświetla nazwę skonfigurowanego punktu przejścia.

Dźwięk wewnętrzny: służy do włączenia/wyłączenia zintegrowanego źródła dźwięku.

Wskaźnik Wi-Fi: pokazuje status połączenia z siecią poprzez migające niebieskie światło. Opis wskazania:

- ciągłe miganie- wyszukiwanie i łączenie się z siecią Wi-Fi;
- 3 mignięcia z rzędu- przejście w tryb konfiguracji (zworka CFG jest zainstalowana);
- 2 mignięcia z rzędu- nawiązywane jest połączenie z oprogramowaniem sterującym (serwerem);
- Pojedyncze mignięcie- oczekiwanie na połączenie z oprogramowaniem sterującym
- **Interwały otwarcia:** czas trwania impulsu wysyłanego do urządzenia wyłączającego, w celu odblokowania przejścia. W zależności od rodzaju zamka może to być zarówno odłączenie napięcia lub zasilania.

Kontrolowany czas otwarcia - Maksymalny czas po udzieleniu dostępu, gdy drzwi są otwarte. Jeśli po tym okresie drzwi zostaną otwarte, będzie to uważane za sforsowanie. Jeśli kontrolowany czas otwarcia jest krótszy niż czas otwarcia - czas otwarcia jest używany dla tej funkcji.

Kontrolowany czas zamknięcia: Maksymalny czas, gdy drzwi pozostają otwarte. Jeżeli w ciągu kontrolowanego czasu zamknięcia drzwi nie zostaną zamknięte, w dzienniku zostanie wygenerowane zdarzenie o pozostawieniu otwartych drzwi. Aby wyłączyć kontrolowany czas zamknięcia, ustaw wartość na zero.

Synchronizacja czasu przez NTP: umożliwia dostęp do serwera NTP, w celu synchronizacji zegara w urządzeniu.

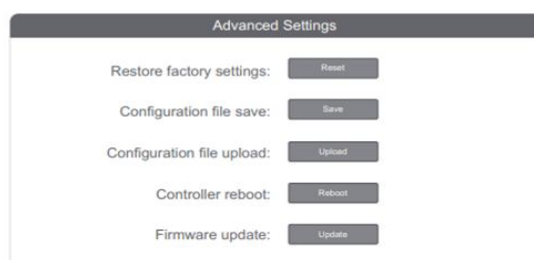
Serwer NTP: adres serwera NTP używanego do synchronizacji czasu.

Strefa czasowa: wskazuje strefę czasową używaną podczas synchronizacji czasu.

Otwarcie drzwi: przyciski otwierające wejście lub wyjście. Po skonfigurowaniu wszystkich parametrów należy wybrać „zapisz”.

5.5.1 Zakładka ustawień zaawansowanych.

Ustawienia zaawansowane umożliwiają: eksportowanie i importowanie konfiguracji do/z pliku, aktualizację oprogramowania kontrolera, zresetowanie kontrolera do ustawień fabrycznych i uruchomienie ponowne kontrolera.



Przywracanie ustawień fabrycznych: przywraca ustawienia domyślne.

Zapis pliku konfiguracyjnego: zapisuje ustawienia sterownika do pliku używanego do konfiguracji urządzenia.

Przesyłanie pliku konfiguracyjnego: przesyła zapisane ustawienia z pliku konfiguracyjnego do kontrolera.

Ponowne uruchomienie kontrolera: Uruchamia ponownie urządzenie, aby wczytać zapisane zmiany ustawień.

Aktualizacja oprogramowania: umożliwia aktualizację oprogramowania kontrolera i modułu komunikacyjnego.

5.5.2. Wyłączanie interfejsu sieciowego.

Aby wyłączyć interfejs sieciowy należy usunąć zworkę z pozycji CFG (jeśli była zainstalowana). Wybierz zakładkę „Ustawienia zaawansowane” i naciśnij przycisk „Uruchom ponownie” w menu kontrolera.

6. WŁĄCZENIE I ROZPOCZĘCIE PRACY.

Podłącz urządzenia zewnętrzne do kontrolera zgodnie z punktem 3. Domyślne ustawienia fabryczne modułu Z-5R-Web-Mini, są następujące:

- **nazwa sieci:** „mySSID”
- **hasło:** „WiFiPassword”
- **protokół:** Wi-Fi
- **tryb:** DHCP;
- **tryb nawiązywania połączenia:** WEB
- **serwer:** hw.guardsaas.com.

Uwaga: Zmiana ustawień modułu komunikacyjnego jest możliwa tylko przez interfejs sieciowy.

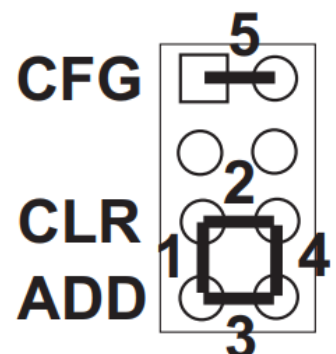
Jeśli zamierzasz używać urządzenia w trybie sieciowym, z parametrami sieci innymi niż ustawienia fabryczne, zmień je zgodnie z punktem 5 niniejszej instrukcji. Za pomocą interfejsu internetowego można również skonfigurować ustawienia w trybie autonomicznym. Aby urządzenie pracowało w tym trybie, konieczne jest wybranie w interfejsie sieciowym menu „Tryb operacyjny” i uruchomienie opcji „Autonomiczny” oraz utworzenie co najmniej jednego klucza głównego (patrz punkt 7). Następnie pozostając w trybie autonomicznym, wyjdź z interfejsu sieciowego i utwórz klucze dla przejścia.

Po dokonaniu zmiany ustawień wyłącz zasilanie. Usuń zworkę z pozycji CFG i ustaw ją zgodnie z typem wybranego zamka. Następnie włącz zasilanie. Urządzenie jest gotowe do pracy w trybie zdefiniowanym w ustawieniach. Jeśli urządzenie ma być używane tylko w trybie autonomicznym, zworka znajdująca się na płycie głównej urządzenia służy do jej konfiguracji:

Układ zworki:

Zworka może znajdować się w jednej z pięciu pozycji:

- **Pozycja nr 1-** wybór zamka elektromechanicznego (w pozycji „zamknięty” napięcie jest odłączane od zamka (patrz uwaga 1)
- **Pozycja nr 2 CLR (wyczyść)-** służy do kasowania pamięci (bazy danych) kontrolera i przywracania ustawień fabrycznych modułu komunikacyjnego. Aby użyć tej opcji, wyłącz zasilanie, ustaw zworkę, a następnie włącz zasilanie. Po skasowaniu zostanie wygenerowana seria krótkich sygnałów dźwiękowych. Wszystkie klucze oraz zaprogramowany czas otwarcia drzwi zostaną usunięte (fabryczna wartość tego parametru to 3 sekundy).



- **Pozycja nr 3 ADD (dodaj)**- służy do dodania kluczy Normal i Block do pamięci kontrolera bez konieczności użycia karty głównej. W tym celu wyłącz zasilanie, załóż zworkę i włącz zasilanie. Kontroler wyda sygnał dźwiękowy, po czym przejdzie w tryb dodawania kluczy Normal. Możesz dodawać klucze Normal (skanowanie krótkoterminowe) oraz Block (skanowanie długoterminowe), bez konieczności użycia karty głównej (Master). Po 16 sekundach po zeskanowaniu ostatniej karty, kontroler wyjdzie z menu dodawania kart (urządzenie wyda serię krótkich sygnałów dźwiękowych).
- **Pozycja nr 4**- wybór zamka elektromagnetycznego (w pozycji „zamknięty” napięcie jest dostarczane do zamka). Jeżeli zworka nie jest zamontowana, uważa się ją za ustawioną w pozycji nr 4, tj. wybrane jest połączenie zamka elektromagnetycznego (patrz uwagi 1 i 2).
- **Pozycja nr 5 (CFG)**- Gdy dostarczane jest zasilanie kontroler rozpoczyna komunikację i konfigurację parametrów podłączonego sprzętu (patrz punkt 5). W tym trybie do zamka nie jest dostarczane napięcie.

Uwaga 1: Jeśli typ zamka został skonfigurowany za pomocą interfejsu internetowego lub oprogramowania sterującego np. GuardLight), to ustawienie zworki w pozycji 1 lub 4 nie ma wpływu na wybór typu zamka, aż do momentu przywrócenia ustawień fabrycznych za pomocą interfejsu internetowego lub zworki (pozycja 2).

Uwaga 2: Przy dużej ilości przejść (np. co 10 sekund), obwód wyjściowy może się przegrzewać. W celu ochrony obwodu przejścia muszą być wyposażone w diody bocznikujące równolegle do uzwojenia zamka. Następnie czas otwarcia klucza elektromagnetycznego może wzrosnąć o 1-3 sekund. Jeśli taki czas zwłoki jest niedopuszczalny, zaleca się montaż rezystora zmiennego, połączonego szeregowo z diodą na napięciu 14V i energia rozproszona do 0,7 J (zalecane V8ZA2P). Patrz schemat 3.

Sygnalizacja świetlna i dźwiękowa pracy kontrolera Z5R-Web-Mini

Czerwona dioda LED sygnalizuje stan pracy i zasilanie. Po zbliżeniu karty do czytnika możliwe są następujące reakcje:

- karta znajduje się w bazie kontrolera: miga zielona dioda, kontroler wydaje sygnał dźwiękowy, zamek jest otwarty przez zdefiniowany czas lub do momentu uruchomienia czujnika pozycji drzwi,
- karty nie ma w bazie kontrolera: miga zielona i czerwona dioda, kontroler wydaje 2 krótkie sygnały dźwiękowe.

Gdy włączona jest opcja „Wskaźnik Wi-Fi” (patrz punkt 5.5), powyższe wskazanie będzie przerywane przez mignięcia niebieskiej diody LED, pokazującej stan połączenia z siecią Wi-Fi.

7. USTAWIENIE KONTROLERA PRZY POMOCY KLUCZA MASTER

Aby zarządzać kontrolerem poprzez klucz Master (należy przełączyć na żądany tryb programowania - w celu utworzenia lub usunięcia kluczy Normal lub Block, aktywować tryb Accept itd.), używane są dwa typy dotknięcia kluczem Master. Krótki dotyk jest do 1 sek., a długi dotyk to około 6 sekund. Aby korzystać z programowania klucza Master, podłącz czytniki poprzez protokół **iButton™**.

Uwaga: do sterowania („programowania”) urządzenia nie należy wykorzystywać czytników podłączonych przez protokół Wiegand, ponieważ nie jest on obsługiwany.

W każdym trybie programowania obowiązuje limit czasowy od zeskanowania ostatniej karty (16 sekund). Po tym czasie urządzenie wyjdzie z trybu programowania, potwierdzając tę operację serią 4 krótkich sygnałów. Dostępne są następujące tryby programowania:

- **Dodawanie klucza Normal - 1 długi dotyk;**
- **Dodawanie klucza Master - 1 krótki dotyk, 1 długi dotyk;**
- **Usuwanie klucza Normal- 2 krótkie dotknięcia, 1 długi dotyk;**
- **Usuwanie całej pamięci - 3 krótkie dotknięcia, 1 długi dotyk;**
- **Ustawienie czasu otwarcia drzwi - 4 krótkie dotknięcia;**
- **Aktywacja trybu Accept - 5 krótkich dotknięć;**
- **Dezaktywacja trybu Accept - 1 krótki dotyk.**

7.1. Tryb dodawanie kluczy Normal

Dotknij i przytrzymaj klucz Master przy czytniku (długi dotyk). Kontroler będzie emitował krótki sygnał dźwiękowy akceptujący klucz Master, a po 6 sek., kolejny sygnał wskazujący, że kontroler został przełączony w tryb dodawania kluczy Normal. Odsuń klucz Master od czytnika.

Aby dodać nowe klucze, zbliżaj klucze do czytnika jeden po drugim, upewniając się, że odstęp pomiędzy dotknięciami nie przekracza 16 s. Czytnik potwierdzi każdy nowy dotyk krótkim sygnałem dźwiękowym. Jeśli nowy klucz będzie zbliżony do czytnika na 3 sekundy i więcej, to zostanie utworzony jako klucz Block. Jeżeli przedstawiony klucz już istnieje w pamięci, kontroler wyda dwa krótkie sygnały dźwiękowe. Aby wyjść z tego trybu, należy albo odczekać 16 sek. po ostatnim zbliżeniu klucza lub dotknij czytnik krótko za pomocą klucza Master. Kontroler potwierdzi wyjście z trybu programowania czterema krótkimi sygnałami.

7.2. Tryb dodawania kluczy Master

Zbliż na krótko klucz Master do czytnika. Kontroler będzie emitował krótki sygnał dźwiękowy potwierdzający rozpoznanie klucza Master. Nie później niż 6 sekund po tym, dotknij i przytrzymaj klucz Master przy czytniku. Kontroler wyemituje dwa krótkie sygnały oznaczające przejście w trybie programowania klucza Master, a po 6 sekundach - jeden sygnał oznaczający, że kontroler został przełączony w tryb dodawania kluczy Master. Teraz odsuń klucz Master od czytnika.

Aby dodać nowe klucze Master, zbliżaj je do czytnika, upewniając się, że odstęp pomiędzy dotknięciami nie przekracza 16 s. Czytnik potwierdzi każdy nowy dotyk krótkim sygnałem dźwiękowym, jednak jeżeli przedstawiony klucz już istnieje w pamięci kontrolera, nie będzie żadnych sygnałów.

Aby wyjść z tego trybu, należy odczekać 16 sekund po ostatnim dotknięciu. Kontroler potwierdzi wyjście z trybu programowania czterema krótkimi sygnałami.

7.3 Tryb usuwania wszystkich kluczy

Zbliż trzykrotnie na krótko do czytnika klucz Master. Kontroler będzie emitował krótki sygnał dźwiękowy potwierdzający rozpoznanie klucza Master. Przy drugim kontakcie, kontroler wyda dwa krótkie sygnały oznaczające, że klucz Master jest w trybie programowania. W chwili trzeciego dotknięcia kontroler wyda trzy krótkie dźwięki wskazujące na trzecie poprawne zbliżenie klucza. Nie później niż 6 sekund po tym umieść i przytrzymaj klucz Master na czytniku (długie dotknięcie). Przy czwartym dotknięciu kontroler wyda cztery krótkie sygnały, a po 6 sekundach zasygnalizuje skasowanie pamięci kontrolera i wyjście z trybu programowania. Po tej operacji klucz główny należy odsunąć od czytnika.

*- W przypadku kasowania całej bazy danych za pomocą klucza głównego, zaprogramowany czas otwarcia zamka nie jest usuwany.

7.5 Ustawianie czasu otwarcia zamka.

Zbliż klucz Master na krótko do czytnika cztery razy. Przy każdym kontakcie, kontroler potwierdzi klucz Master, emitując tyle krótkich sygnałów dźwiękowych co liczba dotknięć (jeden przy jednym dotknięciu, dwa przy dwóch itd.) Przy czwartym dotyku, kontroler wyemituje cztery krótkie sygnały dźwiękowe i przejdzie w tryb programowania czasu otwarcia zamka.

Nie później niż 6 sekund po tym, należy nacisnąć i przytrzymać przycisk zwalniający drzwi na długość czasu potrzebną do otwarcia. Gdy przycisk odblokowania drzwi zostanie zwolniony, kontroler wyda sygnał dźwiękowy i ustawi czas na jaki został wciśnięty przycisk jako nowy czas otwarcia drzwi.

Dla dokładnego zaprogramowania czasu zalecamy korzystanie z interfejsu sieciowego.

7.6 Tryb Accept.

Trybu Accept należy używać, aby zapisać do pamięci wszystkie klucze zbliżane do czytnika. Dowolny klucz zbliżony do czytnika odblokuje drzwi i będzie przechowywany w pamięci kontrolera, jeżeli tam jeszcze nie był zapisany.

Ten tryb służy do odzyskiwania bazy danych kluczy kontrolera bez konieczności zbierania wszystkich kluczy wydanych dla użytkowników. Klucz Master jest konieczny, aby uaktywnić ten tryb.

Dotknij krótko pięciokrotnie czytnika kluczem Master. Przy każdym zbliżeniu, kontroler potwierdzi rozpoznanie klucza Master, emitując tyle krótkich sygnałów dźwiękowych co liczba dotknięć (jeden dla jednego zbliżenia, dwa do dwóch itd.) Przy piątym dotknięciu, kontroler wyda pięć krótkich sygnałów i po kilku sekundach długi sygnał, który potwierdzi aktywację trybu Accept.

Aby wyłączyć tryb Accept, należy zbliżyć do czytnika klucz Master ponownie; seria krótkich sygnałów dźwiękowych potwierdzi wyjście z tego trybu.

Uwaga: Jeśli zasilanie zostanie odłączone podczas aktywnego trybu Accept, to pozostaje on aktywny po przywróceniu zasilania.

7.7. Tryby dostępu.

Kontroler obsługuje trzy tryby dostępu.

- **Tryb Normal:** klucze Normal i Block mają dostęp.
- **Tryb Block:** Tylko klucze Block mają dostęp.
- **Tryb Free:** zamek pozostaje odblokowany.

Tryb Block oraz tryb Free są aktywowane za pomocą klucza Block (patrz 7.1. w jaki sposób dodawać), przez dotknięcie i przytrzymanie go przy czytniku przez 3 sekundy lub dłużej (długie dotknięcie). Jeśli drzwi były otwarte podczas tej sekwencji, tryb Free jest aktywowany, a jeśli były zamknięte włącza się tryb Block. Jeśli tryb Block lub tryb Free jest już aktywny, to samo działanie go dezaktywuje i tryb Normal jest przywracany.

Uwaga: W przypadku korzystania z klucza Block, dostęp jest możliwy w momencie odsunięcia klucza od czytnika.

W trybie Block, gdy stosuje się klucz Normal, dostęp jest zabroniony i fakt ten jest potwierdzony serią krótkich sygnałów.

W trybie Free, wszystkie zbliżone klucze są rejestrowane w pamięci w celu dalszego przetwarzania przez program sterujący.

Uwaga: Jeśli zasilanie zostanie wyłączone, gdy tryb Block jest włączony, to pozostaje on aktywny po przywróceniu zasilania.

8. POŁĄCZENIE SIECI I TRYB AUTONOMICZNY.

Uwaga 1: Gdy zasilanie zostanie przywrócone po awarii zasilania kontroler zachowuje tryb aktywny przed awarią. Wyjątek: Tryby dodawania/usuwania kluczy nie są zachowywane po przywróceniu zasilania, a tryb Normal jest reaktywowany.

Uwaga 2: Podczas przełączania z trybu autonomicznego na tryb sieciowy, oprogramowanie sterujące zwykle nadpisuje istniejące bazy kluczy na nowe bazy kluczy z komputera sterującego. Dlatego zaleca się, aby zapisać bazę danych istniejących kluczy przed podłączeniem kontrolera do oprogramowania sterującego, dzięki czemu może być później przywrócona lub wyeksportowana do oprogramowania sterującego.

Uwaga 3: W przypadku, gdy będąc w sieci lub w trybie sieciowym, klucz Master zostanie zbliżony do kontrolera, najprawdopodobniej nic się nie będzie działo, ponieważ oprogramowanie sieciowe usuwa wszystkie istniejące klucze Master i zakazuje tworzenia nowych kluczy. Aby wprowadzić nowy klucz do systemu sieciowego w trybie sieciowym, należy skorzystać z oprogramowania sterującego.

Uwaga 4: Jeśli kontroler jest konfigurowany w trybie autonomicznym, to należy do niego wchodzić za pośrednictwem oprogramowania (np. Guard Commander) w sieci, a następnie użyć interfejsu sieciowego, aby skonfigurować kontroler do pracy w sieci.

9. AKTUALIZACJA LUB PRZYWRACANIE OPROGRAMOWANIA PRZEZ USB.

Jeśli nie jest możliwe zaktualizowanie oprogramowania przez interfejs sieciowy, kontroler może połączyć się z komputerem przez USB. Aby to zrobić, należy podłączyć urządzenie do komputera za pomocą kabla USB. W tym trybie urządzenie jest zasilane przez magistralę USB, więc nie jest konieczne dodatkowe zewnętrzne źródło zasilania. Po podłączeniu w systemie pojawia się nowy port szeregowy. Może być konieczne zainstalowanie sterowników, które można pobrać ze strony: hatpol.pl. Można także pobrać oprogramowanie narzędziowe, aby zaktualizować firmware kontrolera.

10. ZAWARTOŚĆ OPAKOWANIA.

- Kontroler Z-5R WEB-Mini - 1
- Zestaw montażowy - 1
- Bateria CR2032 - 1
- Instrukcja obsługi - 1

11. WARUNKI PRACY

- Dopuszczalna temperatura pracy: -40°C do +40°C
- Wilgotność: nieprzekraczająca 98% w temperaturze +25°C
- Kontroler nie powinien być eksploatowany w warunkach, których mamy do czynienia z: opadami atmosferycznymi, bezpośrednim nasłonecznieniem, piaskiem, kurzem i skraplanie się wody.
- Kontroler może nie działać poprawnie podczas pracy w warunkach innych niż zalecane.

12. TRANSPORT I MAGAZYNOWANIE.

Zapakowane urządzenie może być transportowane w każdym zadaszonym pojeździe w zakresie temperatur od -50°C do +50°C, unikając bezpośredniego działania promieni słonecznych czy opadów deszczu oraz transportowane bezpiecznie zgodnie z ogólnymi zasadami bezpieczeństwa dla tego rodzaju transportu, zgodnie ze standardem przemysłowym GOST 23088-80.

Urządzenie musi być przechowywane w warunkach grupy L zgodnie ze standardem przemysłowym GOST 15150-69 (o temperaturze od +5°C do +40°C, wilgotność do 98%).

12. PRZYKŁAD KONFIGURACJI Z5R-WEB Z USŁUGĄ GUARD-SAAS.

Przedstawiamy film instruktażowy podłączenia kontrolera Z5R-WEB z oprogramowaniem kontroli dostępu oraz rejestracji czasu pracy GuardSaaS.

Bezpośredni link: <https://www.youtube.com/watch?v=YGGQwuRLej4>

Możesz również zeskanować kod QR telefonem, aby przejść do odtwarzania materiału szkoleniowego:



Pozbądź się zużytego sprzętu elektronicznego.



Urządzenia oznaczone są zgodnie z ustawą o zużytym sprzęcie elektrycznym i elektronicznym symbolem przekreślonego kosza na odpady. Oznakowanie takie informuje, że sprzęt ten, po okresie jego użytkowania nie może być umieszczany w koszu łącznie z innymi odpadami pochodzącymi z gospodarstwa domowego. Użytkownik jest zobowiązany do oddania go firmom, bądź instytucjom prowadzącym zbieranie zużytego sprzętu elektrycznego i elektronicznego. Prowadzący zbieranie, w tym lokalne punkty zbiórki, sklepy czy gminne jednostki, tworzą odpowiedni system umożliwiający oddanie tego sprzętu. Właściwe postępowanie ze zużytymi urządzeniami elektrycznymi i elektronicznymi przyczynia się do uniknięcia szkodliwych dla zdrowia ludzi i środowiska naturalnego konsekwencji, wynikających z obecności składników niebezpiecznych oraz niewłaściwego przetwarzania i składowania takich urządzeń.

Szanowni Państwo

Dziękujemy za dokonanie zakupu produktów dystrybutora HatPol oraz gratulujemy trafnego wyboru.

Jesteśmy wśród największych producentów systemów kontroli dostępu na świecie,

Działamy od 1992 roku i ciągle się rozwijamy oferując Klientom produkty najwyższej klasy,

Produkty są zgodne z normami europejskimi – CE,

Gwarantujemy najlepszy serwis gwarancyjny i pogwarancyjny.

WARUNKI GWARANCJI

Producent udziela gwarancji na okres 24 miesiące od daty sprzedaży przez HatPol.

1. Data, od której zaczyna się okres gwarancyjny, jest datą wystawienia faktury bądź paragonu.
2. Gwarancja nie obejmuje czynności związanych z instalacją, montażem urządzenia bądź oprogramowania.
3. Reklamowany sprzęt należy zgłosić poprzez formularz na stronie „<https://rma.hatpol.pl/>”. Reklamowany sprzęt klient musi dostarczyć do serwisu HatPol na własny koszt. Przesyłkę powrotną przyjętego do reklamacji pokrywa firma HatPol, ale pod warunkiem, że urządzenie nie jest uszkodzone z powodu czynników zewnętrznych tj. zły montaż, wylądowania atmosferyczne itp.
4. Sprzęt zostanie przyjęty do serwisu tylko wtedy, gdy na pudełku w widocznym miejscu znajdować się będzie numer RMA nadany przez serwis HatPol podczas zgłoszenia na [hatpol.pl/rma](https://rma.hatpol.pl/), a wewnątrz opakowania znajdować się będzie dowód zakupu (faktura, paragon) oraz karta gwarancyjna lub kopie tych dokumentów.
5. Jeżeli sprzęt będzie zapakowany w nieoryginalny karton, bądź źle zapakowany (brak odpowiedniego styropianu, tektury itp.) serwis HatPol nie odpowiada za uszkodzenia powstałe w wyniku złego opakowania (pęknięcia, rysy, otarcia itp.)
6. Serwis HatPol nie uwzględnia uszkodzeń mechanicznych powstałych w wyniku transportu z winy przewoźnika bądź przez użytkownika.
7. Dostarczony sprzęt musi posiadać nieuszkodzone plomby gwarancyjne i czytelne numery seryjne.
8. Reklamowany sprzęt musi być dostarczony do serwisu HatPol kompletny np. monitor, panel, zasilacz.
9. Montaż należy wykonywać zgodnie ze schematem i wskazówkami w instrukcji danego sprzętu oraz przez doświadczonego monter z odpowiednią wiedzą i umiejętnościami.
10. Jeżeli reklamowany sprzęt dostarczony do serwisu okaże się sprawny, serwisant może obciążyć kosztami sprawdzania oraz przesyłki osobę bądź firmę reklamującą towar.
11. Gwarancja nie obejmuje uszkodzeń powstałych w wyniku złego montażu lub niewłaściwej obsługi sprzętu.
12. Koszty odesłania naprawionego na gwarancji sprzętu ponosi firma HatPol.
13. Serwis HatPol nie ma obowiązku informować reklamującego o stanie naprawy sprzętu, klient może sam śledzić stan swojej naprawy na [hatpol.pl/rma](https://rma.hatpol.pl/), tam również może wprowadzać swoje komentarze.
14. Naprawa gwarancyjna będzie trwać 19dni roboczych, jednak z przyczyn niezależnych od HatPol czas naprawy może zostać przedłużony maksymalnie do 3 miesięcy (w praktyce czas reklamacji średnio trwa 3dni robocze).
15. HatPol nie ponosi odpowiedzialności za serwis gwarancyjny, jeżeli wymagane naprawy nie będą mogły być wykonane z powodu restrykcji importowo-exportowych.
16. Serwis HatPol zastrzega sobie prawo do zmiany warunków gwarancyjnych w każdej chwili, które będą miały moc działania wstecz.
17. Prawa i obowiązki stron regulują niniejsze warunki gwarancji, z którymi klient winien się zapoznać i zatwierdzić własnoręcznym podpisem.

Model urządzenia i nr seryjny	Data sprzedaży, pieczęć i podpis sprzedawcy



Strony producenta: ironlogic.pl

Strona wyłącznego dystrybutora: <https://hatpol.pl/>

E-mail serwisu: serwis@hatpol.pl

Strona zgłoszeń reklamacji: rma.hatpol.pl

Nr telefonu do serwisu: (18) 414-47-83