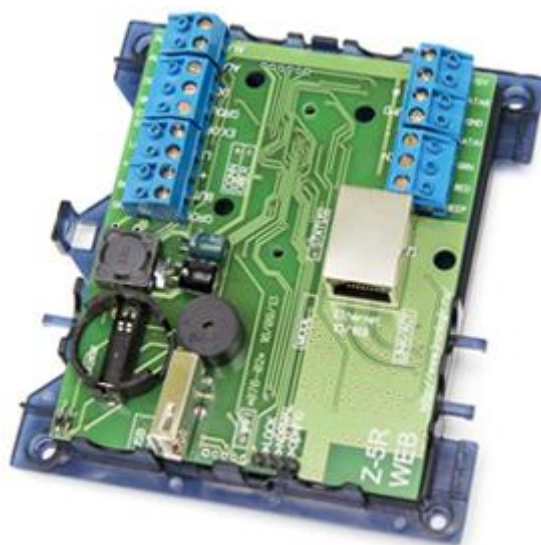


Instrukcja konfiguracji kontrolera sieciowego Z5R-WEB



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.....	5
3. MONTAŻ.....	5
4. KONFIGURACJA	11
5. INTERFEJS SIECIOWY	14
5.1 Wybór języka	15
5.2 Zakładka statusu	16
5.3. Zakładka konfiguracji połączenia	17
5.3.1. Ethernet	17
5.3.2. Wi-Fi	18
5.3.3. Modem 3G	20
5.3.4. Modem 4G.	21
5.4. Zakładka trybu połączenia dla oprogramowania sterującego	21
5.4.1. Sieć	22
5.4.2. Serwer	23
5.4.3. Klient	23
5.4.4. Tryb autonomiczny	24
5.5 Zakładka ustawień kontrolera.	26
5.5.1 Zakładka ustawień zaawansowanych.	27
5.5.2. Zakończenie pracy z interfejsem sieci Web	27
6. WŁĄCZENIE I ROZPOCZĘCIE PRACY.....	27
7. USTAWIENIE KONTROLERA PRZY POMOCY KLUCZA MASTER	28
7.1. Tryb dodawanie kluczy Normal.....	29
7.2. Tryb dodawania kluczy Master	29
7.3 Tryb usuwania kluczy Normal	30
7.4 Tryb usuwania całej pamięci.....	30
7.5 Ustawianie czasu otwarcia zamka.	30
7.6 Tryb Accept.	31
7.7. Tryby dostępu.	31
8. POŁĄCZENIE SIECI I TRYB AUTONOMICZNY.....	32
9. ZAWARTOŚĆ OPAKOWANIA.	32
10. WARUNKI PRACY.....	33
11. TRANSPORT I MAGAZYNOWANIE.....	33
12. PRZYKŁAD KONFIGURACJI Z5R-WEB Z USŁUGĄ GUARD-SAAS.	33

1. PRZEGLĄD

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

Kontroler może pracować w trybie autonomicznym lub sieciowym.

Podczas pracy w trybie autonomicznym, klucze są przechowywane w bazie danych za pomocą klucza Master.

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.

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

Jeśli podczas pracy w trybie sieciowym połączenie kontrolujące oprogramowanie zostanie utracone, kontroler nadal będzie funkcjonował w trybie autonomicznym, przechowując zdarzenia w lokalnym buforze zdarzeń.

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 kluczy będą określane później jako "klucze".

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

Klucze dostępu z kolei mogą być **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, te i tylko 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 rygla). Urządzenie blokujące oraz protokół połączenia zostają wybrane podczas instalacji i konfiguracji kontrolera.

Kontroler umożliwia przechowywanie 8192 zdarzeń w swoim buforze. Zdarzenia te obejmują uzyskanie kodu, operacje czujnika drzwi, generowanie sygnału sterującego itp.

W celu poprawienia funkcjonalności, kontrolera umożliwia:

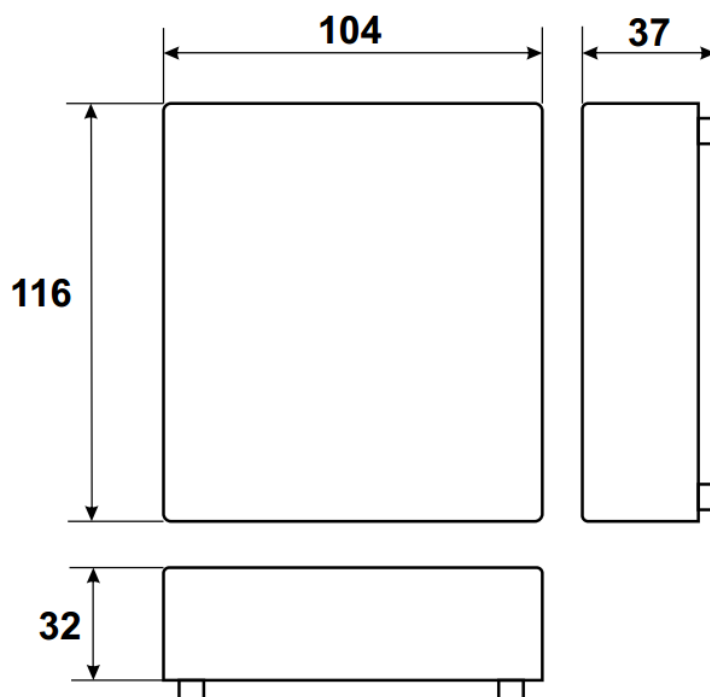
- Podłączenie czujnika drzwi w celu generowania zdarzenia "drzwi ominięte", a zmniejszenie czasu trwania alarmu "drzwi otwarte" (i ograniczenie czasu trwania sygnału odblokowania dla urządzenie blokującego).
- Podłączenie przycisku zwalniającego drzwi ("wyjście"), aby otworzyć drzwi bez kontroli dostępu.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

2. SPECYFIKACJA

Pamięć kluczy	2x 8168 kluczy
Pamięć zdarzeń	8192 zdarzeń
Ilość czytników	2
Protokoły czytników	Wiegand (-26, -34, -42, -50), iButton™
Audiowizualna kontrola zwrotna czytników	Czerwony i zielony LED, sygnał dźwiękowy
Zabezpieczenie czytników	200 mA
Moc wyjściowa prądu	5 A
Sygnał wyjściowy ALARMU	250 V, 100 mA, 35 Ohm, izolacja 1.5 kV
Zabezpieczenie	Optyczne
Ethernet	
Interfejs	RJ45 (10/100BASE-T) Auto MDI/MDIX
Obsługiwane rodzaje klatek	Ethernet II, IEEE 802.3
Obsługiwane protokoły	IP, ARP, TCP, SSH, ICMP, UDP, DHCP, HTTP
WI-FI	
Obsługiwane standardy	IEEE 802.11 b/g/n
Zakres częstotliwości	2.4-2.4835 GHz
Szybkość transmisji	802.11n: do 150 Mbps 802.11g: do 54 Mbps
Moc sygnału sieci bezprzewod.	Do 20 dBm (do 100 mW)
Tryby pracy bezprzewodowej	Punkt dostępu, Klient
Zabezpieczenia sieci bezprzewodowej	64/128/512-bit WEP, WPA, WPA-PSK, WPA2, WPA2-PSK
USB	
Typ złącza USB	USB Typ A
Wersja USB	USB 2.0
Tryb USB	Host, High Speed, Full Speed
Inne parametry	
Waga	150 g
Wymiary, mm	105 x 115 x 37
Montaż	Ścienny, 35mm szyna DIN(TH35)
Zasilanie	8 – 28 V
Prąd roboczy (at 12V)	Do 300 mA (bez czytników)

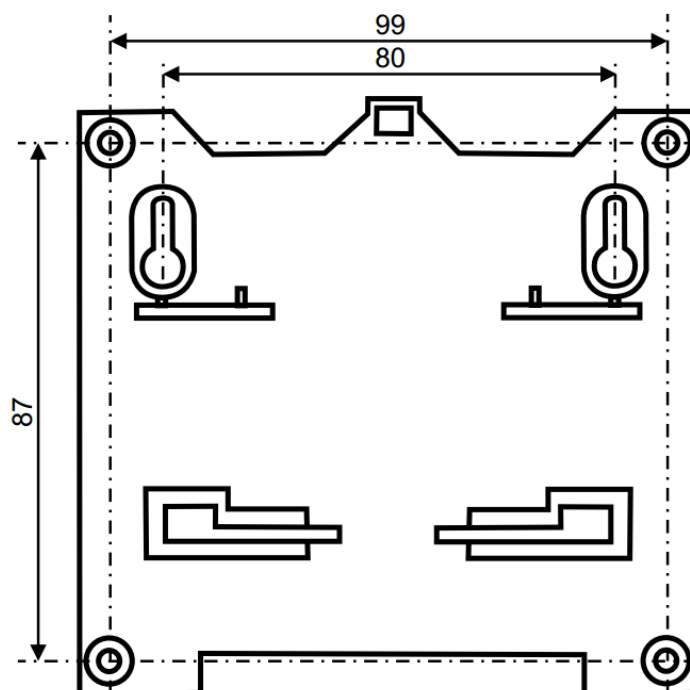
3. MONTAŻ

Wymiary kontrolera przedstawiono na rysunku poniżej:



Uwaga: Aby uniknąć ostrych krawędzi w obudowie kontrolera, użyj piły do wycięcia wypustek przykrywających otwory na przewody, zamiast wyłamywać je ręcznie.

Wymiary do montażu kontrolera:



Układ zacisków kontrolera:

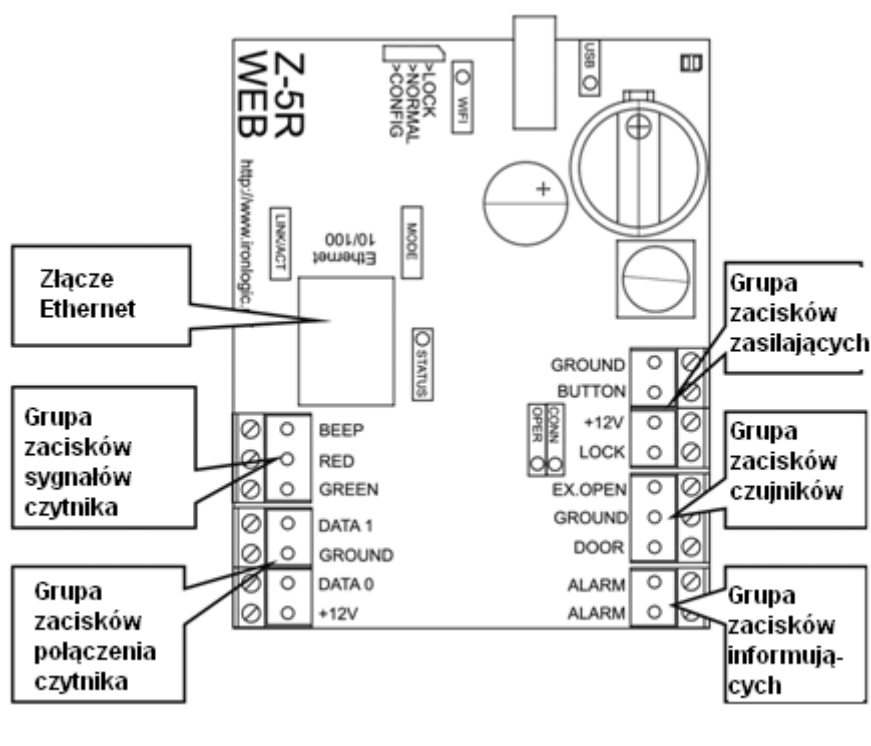


Tabela oznaczenia zacisków

Grupa zacisków zasilających

Nr	Oznaczenie	Przeznaczenie
1	GROUND	Miejsce podłączenia do ujemnego przewodu zasilania, drugi przewód dla przycisku wyjścia.
2	BUTTON	Wejście: Przycisk wyjścia. Zacisk ten jest wielofunkcyjny i pozwala na przeniesienie jego funkcji.
3	+12V	Dodatni przewód zasilający. Również dodatni przewód od zamka.
4	LOCK	Wyjście: Sygnał mocy wyjściowej. Drugi (ujemny) przewód idzie do zamka. Wyjście to tranzystor polowy.

Grupa zacisków czujników

Nr	Oznaczenie	Przeznaczenie
1	EX.OPEN	Wejście: tryb ewakuacyjny. Zwarcie tego sygnału z uziemieniem (GROUND) przełącza kontroler do trybu ewakuacji
2	GROUND	Przewód uziemienia sygnałów EX.OPEN i DOOR.
3	DOOR	Wejście: Czujnik drzwi. Kiedy drzwi są zamknięte, muszą być zwarte z uziemieniem. Zacisk ten jest wielofunkcyjny i pozwala na przeniesienie jego funkcji.

Grupa zacisków informacyjnych

Nr	Oznaczenie	Przeznaczenie
1	ALARM	Wyjście: Przełącznik kontaktronowy, łączący z systemami zabezpieczenia jako część obiegu bezpieczeństwa
2	ALARM	

Grupa zacisków podłączenia czytnika

Nr	Oznaczenie	Przeznaczenie
1	DATA1	- Tryb Wiegand: DATA1 dla sygnału wejściowego czytnika oraz DATA0 dla sygnału wyjściowego czytnika. - Tryb iButton™: Przewód sygnału wyjściowego czytnika (TM).
2	GROUND	Podłączenie uziemienia czytnika.
3	DATA0	- Tryb Wiegand: DATA0 dla sygnału wejściowego czytnika oraz DATA1 dla sygnału wyjściowego czytnika. - Tryb iButton: Przewód sygnału wejściowego czytnika (TM).
4	+12V	Zasilanie dla czytników. Wyjście jest zabezpieczone przed zwarcie do 200 mA.

Grupa zacisków sygnałów czytnika

No	Oznaczenie	Przeznaczenie
1	BEEP	Sygnał wyjściowy dla sterowania sygnałem dźwiękowym. Aktywny poziom sygnału jest niski.
2	RED	Sygnał wyjściowy dla sterowania czerwoną diodą LED czytnika. Aktywny poziom sygnału jest niski.
3	GREEN	Sygnał wyjściowy dla sterowania zieloną diodą LED czytnika. Aktywny poziom sygnału jest niski.

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

Układ wskaźników LED na płycie kontrolera

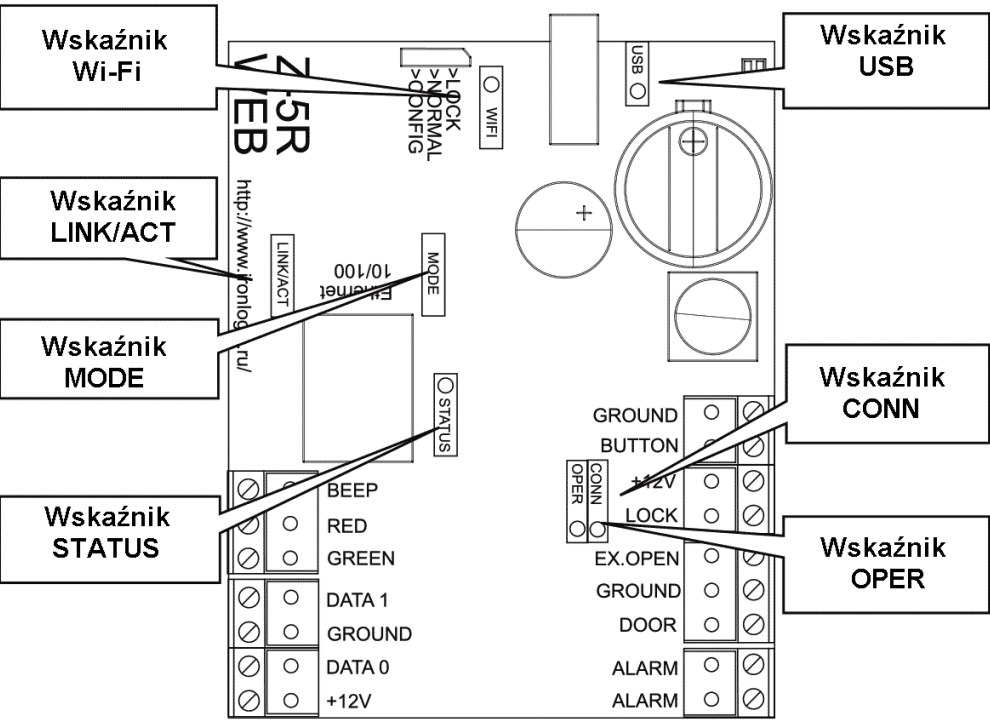


Tabela przeznaczenia wskaźników:

Oznaczenie	Kolor	Przeznaczenie
WIFI	Niebieski	Stan połączenia Wi-Fi: Stale wł. - sieć WiFi podłączona. Migający wł. - transfer danych w toku
USB	Zielony	Status USB: Stale wł. – urządzenie USB podłączone. Migający wł. – transfer danych w toku.
LINK/ACT	Zielony	Stan połączenia Ethernet: Stale wł. - Fizyczne połączenie Ethernet pomiędzy Z-5R WEB i urządzeniem na drugim końcu kabla (zwykle switch). Migający wł. - pakiety Ethernet odbierane.
		Stan łącza oprogramowania sterującego:

MODE	Żółty	Stale wł. - Połączenie TCP ustanowione z oprogramowaniem sterującym.
STATUS	Czerwony	Zdarzenia zewnętrzne: Migające wł. - czujnik(i) zmienił(y) stan (drzwi, zabezpieczenie, przycisk i odblokowanie awaryjne) lub uzyskiwanie kodu klucza.
CONN	Zielony	Status modułu połączeniowego: Migający często - moduł połączeniowy bez zasilania. Migający rzadko - Moduł połączeniowy uruchamiany. Stale wł. - moduł połączeniowy aktywny.
OPER	Żółty	Żądania z oprogramowania sterującego: Migający wł. - kontroler odbiera żądania z oprogramowania sterującego.

4. KONFIGURACJA

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

Moduł sieciowy pozwala na:

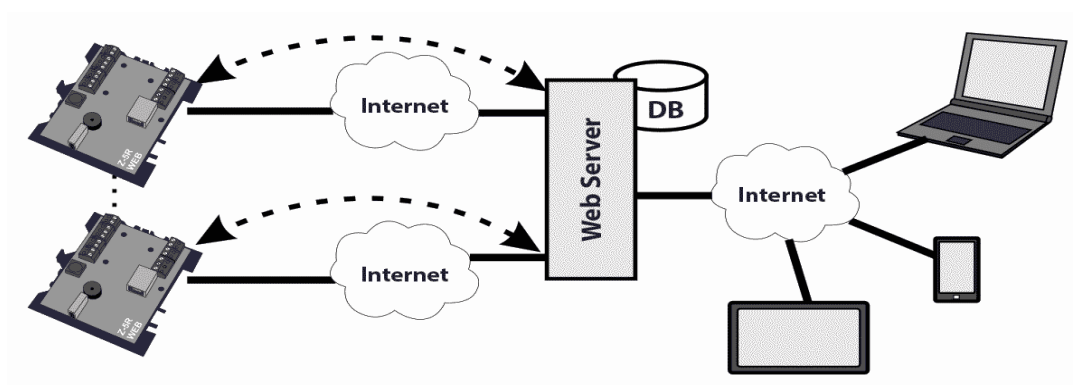
1) podłączenie kontrolera do sieci lokalnej LAN, za pośrednictwem jednego z następujących interfejsów:

Ethernet, Wi-Fi lub modemu USB.

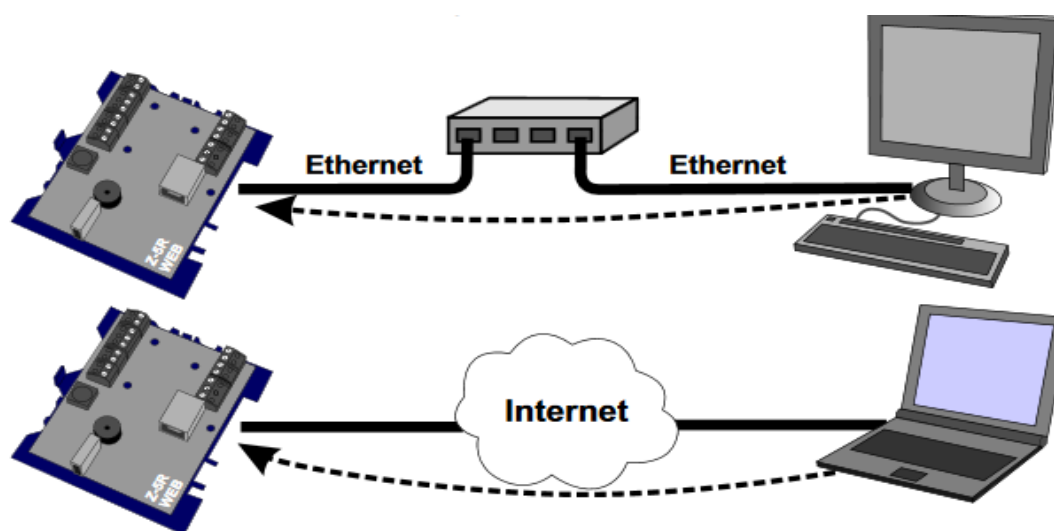
2) Podłączenie do komputera z zainstalowanym oprogramowaniem sterującym ACS, aby korzystać z funkcji kontroli dostępu (ładowanie bazy danych karty, zarządzanie kontrolą dostępu, pobieranie dziennika zdarzeń z bufora itp.)

Istnieją trzy tryby połączenia oprogramowania sterującego:

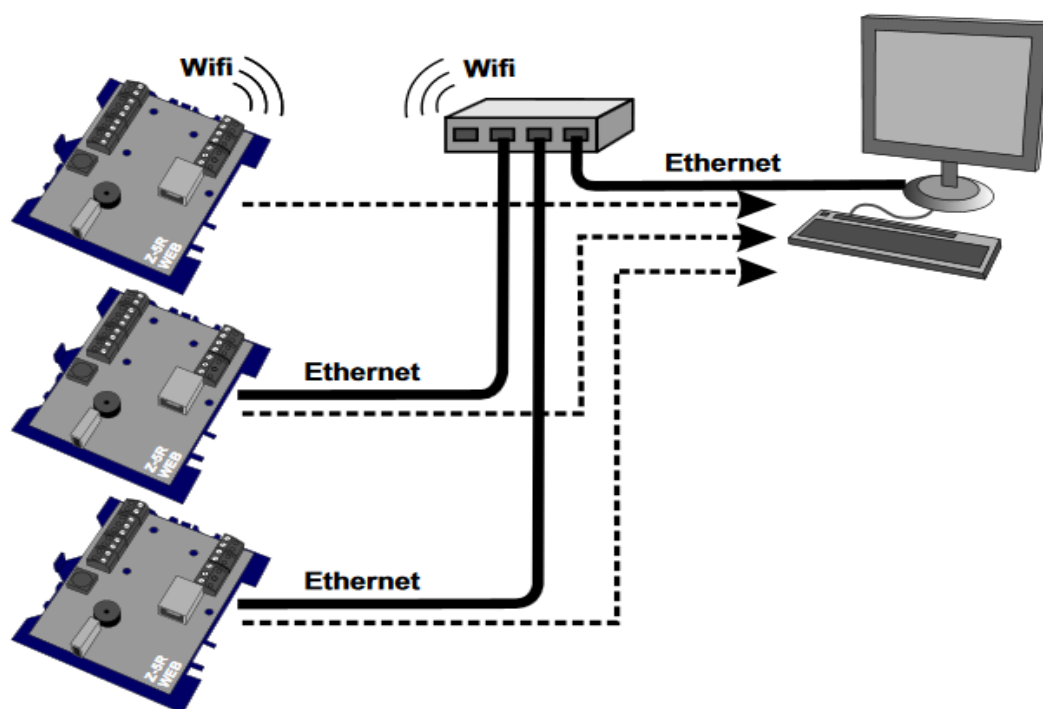
- Tryb połączenia **internetowego**. Moduł połączeniowy łączy się z serwerem WWW przez Internet, a kontroler jest zarządzany za pośrednictwem wewnętrznej witryny sieci Web.



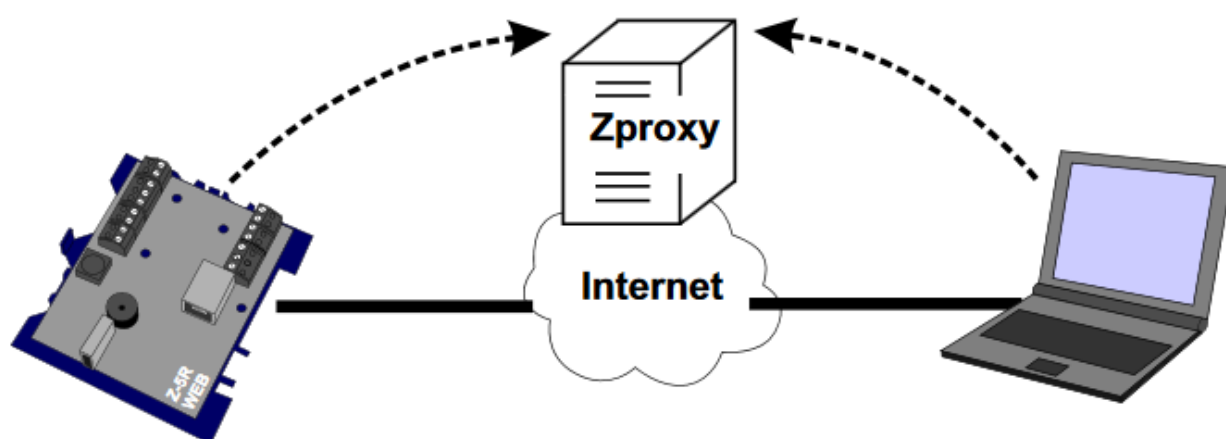
- Tryb połączenia z **serwerem**. Moduł połączeniowy oczekuje na połączenia przychodzące TCP / IP z oprogramowania sterującego PC (takiego jak GuardLight, GuardCommander, Avantgarde).



- 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, Avantgarde lub serwera Zproxy).



Serwer ZProxy umożliwia (przekierowywane) połączenie pomiędzy kontrolerem, a oprogramowaniem sterującym w przypadku, gdy bezpośrednie połączenie jest niemożliwe np. Jeśli kontroler oraz oprogramowanie są w różnych sieciach lokalnych. Jeśli dostęp do Internetu jest możliwy, 1) kontroler łączy się z serwerem ZProxy, 2) oprogramowanie sterujące łączy się również z tym serwerem oraz 3) za pomocą hasła, oprogramowanie sterujące żąda połączenia do wymaganego kontrolera.



Jeżeli nie ma połączenia z oprogramowaniem sterującym, kontroler będzie pracować w trybie **autonomicznym**.

Aby skonfigurować tryb kontrolera, należy użyć zworki na płycie PCB, którą można ustawić w następujący sposób:



- **CONFIG**: po włączeniu zasilania, kontroler wchodzi w tryb ustawień, aby skonfigurować parametry połączenia i typy sprzętu.
- **NORMAL**: Tryb normalny - moduł połączeniowy łączy się z siecią LAN jako skonfigurowany, kontroler podejmuje decyzje o kontroli dostępu. Istniejące parametry połączenia i podłączone urządzenia mogą być skonfigurowane poprzez lokalny adres IP.
- **LOCK**: taka sama operacja jak przy trybie Normal. Jednakże, zarówno interfejs WWW dla parametrów połączenia jak i konfiguracja podłączonego sprzętu oraz aktualizację danych w trybie połączenia internetowego, są **zablokowane**.

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)

Uruchom interfejs WWW w celu konfiguracji kontrolera według następującej kolejności:

1. Ustaw zworkę w pozycji **CONFIG** na płycie.
2. Włącz kontroler.
3. Połącz się z kontrolerem za pośrednictwem Wi-Fi lub Ethernet.

3.1. Wi-Fi:

3.1.1. Poczekaj, aż pojawi się niezabezpieczony punkt dostępu Wi-Fi o nazwie **Z5WEB_XXXXXX**.
(Trwa to do 45 s).

3.1.2. Połącz się do niezabezpieczonego połączenia Wi-Fi.

4.2. Ethernet:

4.2.1. Połącz urządzenie komputerowe i kontrolera za pomocą kabla RJ-45 Ethernet.

4.2.2. Poczekaj, aż urządzenie wykryje połączenie przewodowe LAN (trwa to do 45 s).

5. Przejdź do lub w nowszym firmware <http://192.168.10.1> (nie wymaga autoryzacji, logowania)

6. Przejdź przez wyświetlane menu karta po karcie i skonfiguruj parametry na każdej karcie. Proszę **zapisać** zmiany na każdej karcie!

Później, gdy konfiguracja jest zakończona, a kontroler Z-5R WEB jest podłączona do sieci LAN (zworka jest ustawiona na płycie w pozycji NORMAL lub LOCK), interfejs konfiguracyjny będzie nadal dostępny pod adresem IP poprzez przypisanie statyczne przy początkowej konfiguracji lub przypisanie automatyczne przez serwer DHCP podczas rejestracji LAN.

Jeśli interfejs WWW jest aktywowana poprzez adres IP kontrolera, pojawi się okno autoryzacji. Użyj loginu "**z5rweb**" (bez cudzysłówów), a jako hasło wartość 8 znaków AUTH_KEY znalezione albo na naklejce z tyłu obudowy kontrolera lub na końcu niniejszej instrukcji. Uwaga: Ważna jest wielkość liter w haśle - proszę wpisać **dokładnie** tak, jak pokazano na rysunku.

5.1 Wybór języka

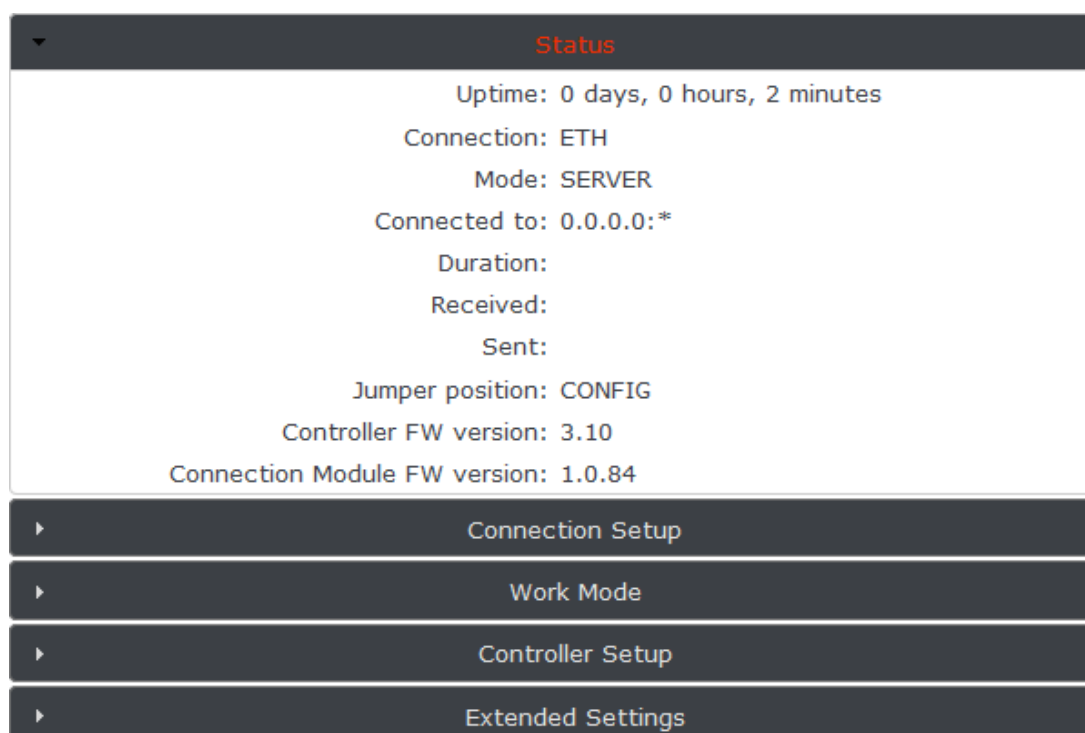


Z5-R WEB
SN: 40567



5.2 Zakładka statusu

Zakładka statusu wyświetla bieżący stan kontrolera.



LEGENDA:

Czas działania: czas, jaki upłynął od podłączenia kontrolera.

Połączenie: Kod trybu połączenia LAN (np. ETH przez Ethernet itd.)

Tryb: Tryb pracy kontrolera (www, Serwer, klient, Autonomiczny).

Połączony: W trybach klient i serwer, pokazuje adres IP podłączonego komputera z oprogramowaniem sterującym.

Czas trwania: W trybie klient i serwer, pokazuje aktualny czas trwania połączenia.

Rx: liczba bajtów odebranych podczas bieżącej sesji połączenia.

Tx: liczba bajtów przesyłanych w trakcie bieżącej sesji połączenia.

Pozycja zworki: Aktualna pozycja zworki: CONFIG, NORMAL lub LOCK.

Wersja kontrolera FW: Wyświetla wersję oprogramowania kontrolera

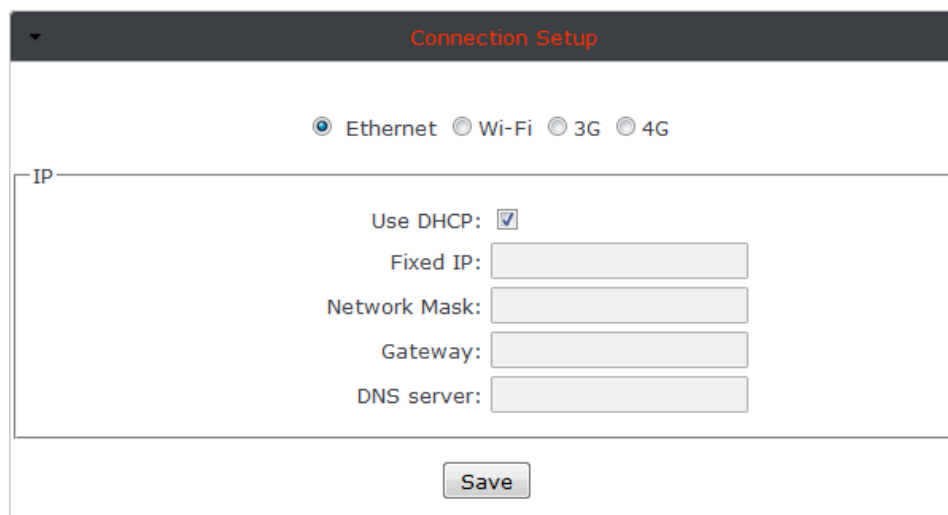
Wersja modułu połączenia FW: Wyświetla wersję oprogramowania modułu komunikacyjnego.

5.3. Zakładka konfiguracji połączenia

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

5.3.1. Ethernet

Jeśli wybrano typ połączenia Ethernet, interfejs wygląda następująco:



Connection Setup

☒ Ethernet ☐ Wi-Fi ☐ 3G ☐ 4G

IP

Use DHCP: ☒

Fixed IP:

Network Mask:

Gateway:

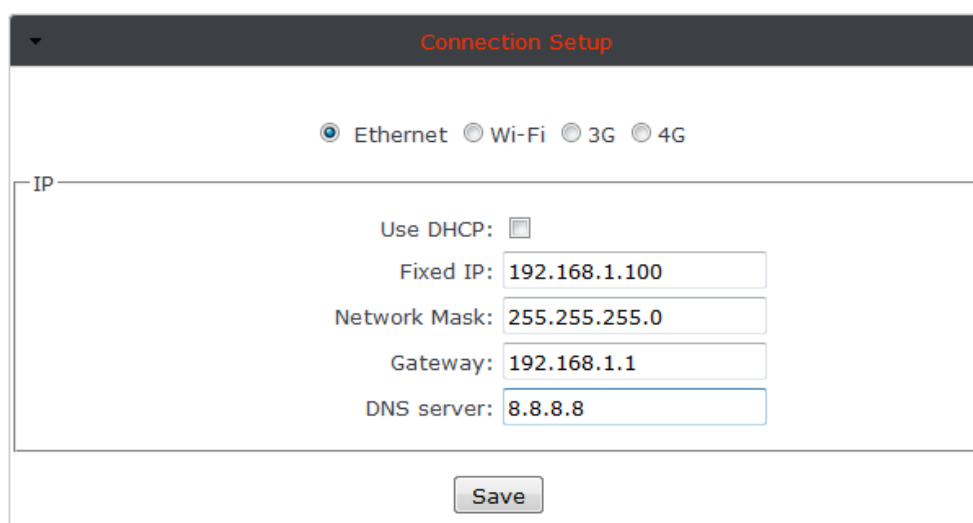
DNS server:

Save

Jeśli serwer DHCP jest obecny w sieci LAN, wszystkie ustawienia sieci kontrolera automatycznie są uzyskiwane od niego.

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

Brak DHCP: Ręczna konfiguracja parametrów sieci wymagany dla tej sieci LAN.



Connection Setup

☒ Ethernet ☐ Wi-Fi ☐ 3G ☐ 4G

IP

Use DHCP: ☐

Fixed IP:

Network Mask:

Gateway:

DNS server:

Save

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.

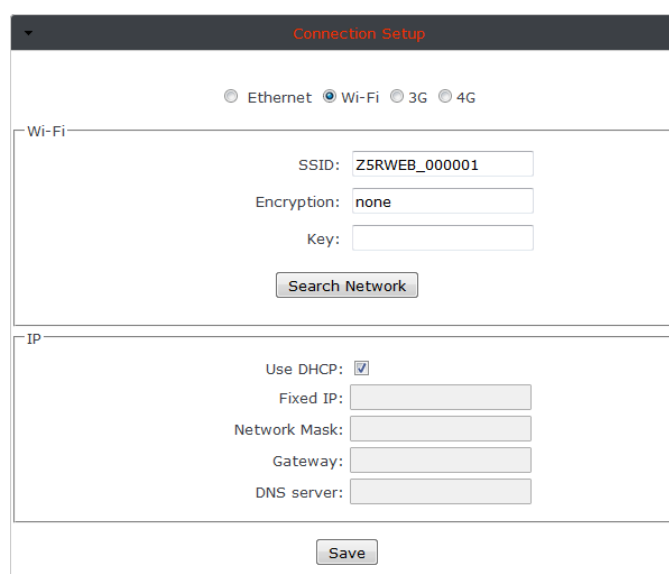
Serwer DNS: adres IP serwera DNS.

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**.

5.3.2. Wi-Fi

Jeśli wybrana jest typ połączenia **WiFi**, interfejs wygląda następująco:



The screenshot shows a web interface titled "Connection Setup". At the top, there are four radio buttons: "Ethernet", "Wi-Fi" (which is selected), "3G", and "4G". Below this, there are two main sections. The first section is labeled "Wi-Fi" and contains three input fields: "SSID" with the value "Z5RWEB_000001", "Encryption" with the value "none", and "Key" which is empty. Below these fields is a "Search Network" button. The second section is labeled "IP" and contains a "Use DHCP" checkbox which is checked. Below this checkbox are four input fields: "Fixed IP", "Network Mask", "Gateway", and "DNS server", all of which are empty. At the bottom of the form is a "Save" button.

SSID: Identyfikator SSID sieci WiFi do podłączenia kontroler.

Typ bezpieczeństwa: Typ bezpieczeństwa tej sieci WiFi (WPA, WPA2, żaden, itp)

Klucz bezpieczeństwa: klucz zabezpieczeń dla tej sieci Wi-Fi.

Szukanie sieci: Znajdź dostępne sieci Wi-Fi.

IP: Parametry konfiguracji sieci (jak dla typu połączenia Ethernet opisanego powyżej).

Po odnalezieniu sieci Wi-Fi, okno dialogowe pojawi się na liście dostępnych sieci, pozwalające wybrać żądaną sieć. Obok każdej nazwy sieci, pokazano jej poziom sygnału.

Connection Setup

☐ Ethernet ☒ Wi-Fi ☐ 3G ☐ 4G

Wi-Fi

SSID: Z5RWEB_000001

Encryption: none

IP

DNS server:

Save

Network Search

	SSID	Signal Level
☐	ironlogic2.ua	77%
☐	ironlogic.ua	64%

Select search again Close

Aby wybrać sieć, zaznacz ją na liście i naciśnij przycisk **Wybierz**. Po wybraniu tej opcji, SSID oraz typ zabezpieczeń dla tej sieci są wyświetlane w obszarze ustawień. Jeśli zabezpieczenie sieci jest włączone, wprowadź również klucz zabezpieczeń.

Connection Setup

☐ Ethernet ☒ Wi-Fi ☐ 3G ☐ 4G

Wi-Fi

SSID: ironlogic

Encryption: mixed WPA/WPA2 PSK

Key: 123MyKey321

Search Network

IP

Use DHCP: ☐

Fixed IP: 10.10.1.100

Network Mask: 255.255.255.0

Gateway: 10.10.1.1

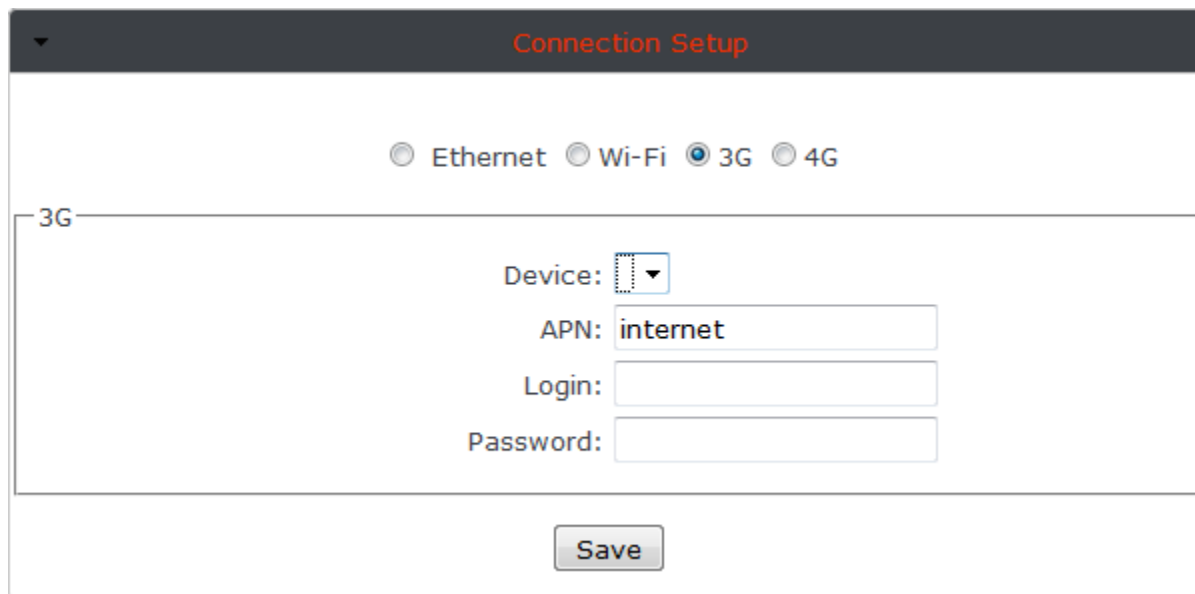
DNS server: 8.8.8.8

Save

Jeśli nie ma serwera DHCP w sieci LAN, parametry sieci należy skonfigurować ręcznie. Po zakończeniu ustawień, należy zapisać parametry naciskając przycisk **Zapisz**.

5.3.3. Modem 3G

Jeśli wybrany jest typ połączenia za pomocą **modemu 3G**, interfejs wygląda następująco:



Connection Setup

☐ Ethernet ☐ Wi-Fi ☒ 3G ☐ 4G

3G

Device:

APN:

Login:

Password:

Save

Gdzie:

Urządzenie: lista rozwijana wszystkich dostępnych modemów aktualnie podłączonych do portu USB urządzenia.

Pozostałe parametry muszą być ustawiona zgodnie z dokumentacją modemu 3G lub należy je uzyskać od operatora sieci komórkowej.

APN: Nazwa punktu dostępu .

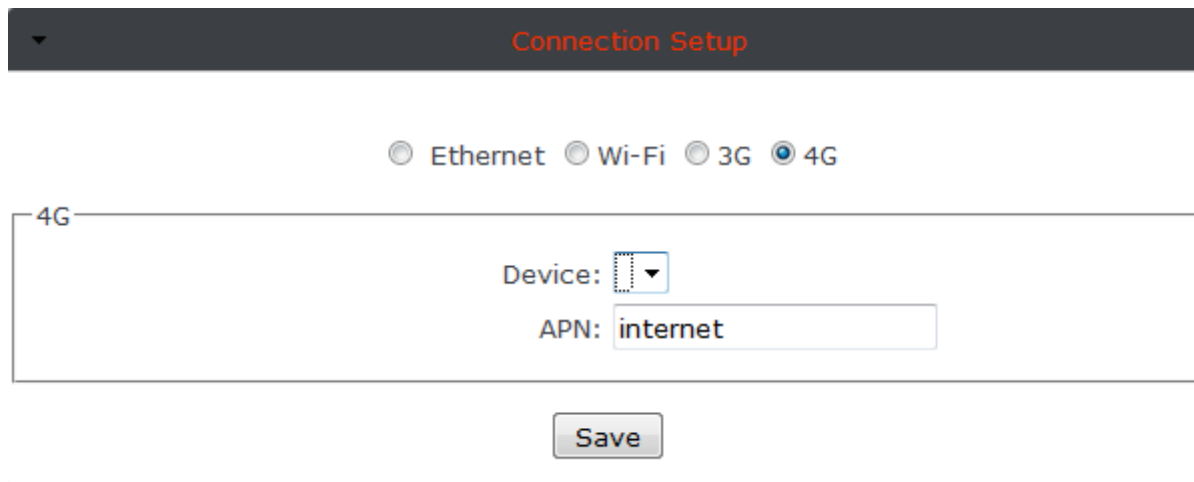
Login: login dostępu operatora komórkowego.

Hasło: hasło dostępu operatora komórkowego.

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

5.3.4. Modem 4G.

Jeśli wybrany jest typ połączenia za pomocą **modemu 4G**, interfejs wygląda następująco:



The screenshot shows the 'Connection Setup' window. At the top, there are radio buttons for 'Ethernet', 'Wi-Fi', '3G', and '4G', with '4G' selected. Below this, there is a section for '4G' configuration. It includes a 'Device:' dropdown menu, an 'APN:' text input field containing the value 'internet', and a 'Save' button at the bottom.

Gdzie:

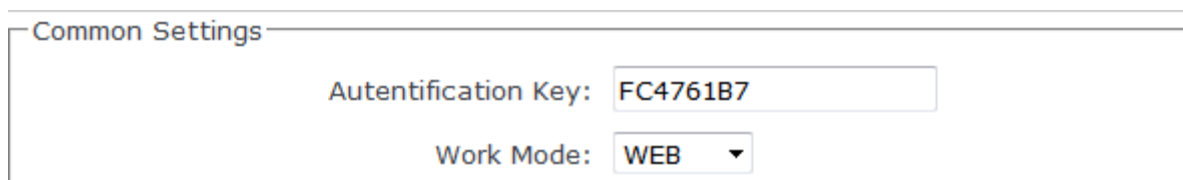
Device: lista rozwijana wszystkich dostępnych modemów aktualnie podłączonych do portu USB urządzenia.

APN: Nazwa punktu dostępu operator komórkowego. Można uzyskać go z dokumentacji modemu 4G lub należy go uzyskać od operatora sieci komórkowej.

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

5.4. Zakładka trybu połączenia dla oprogramowania sterującego

Jeśli Z-5R WEB 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.



The screenshot shows the 'Common Settings' window. It contains two configuration fields: 'Autentification Key:' with a text input field containing 'FC4761B7', and 'Work Mode:' with a dropdown menu currently set to 'WEB'.

Gdzie:

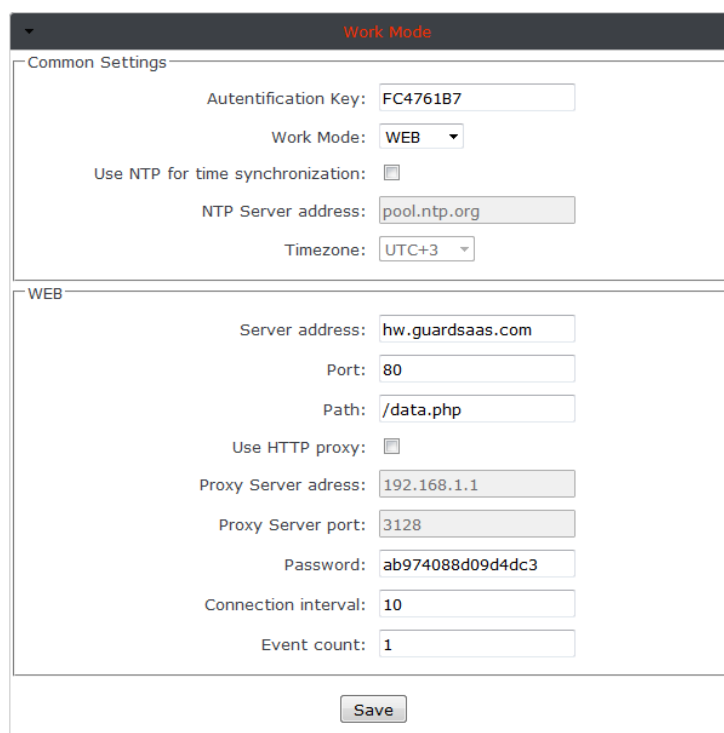
Klucz autoryzacji: Wymagane podczas łączenia się z serwerem internetowym lub podczas pracy poprzez serwer ZProxy i dostępu do interfejsu sieci kontrolera.

Początkowo to pole zawiera klucz fabrycznie ustawiony, obecny 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:



The screenshot displays the 'Work Mode' configuration window. It is divided into two main sections: 'Common Settings' and 'WEB'. In the 'Common Settings' section, the 'Authentication Key' is set to 'FC4761B7', 'Work Mode' is set to 'WEB', 'Use NTP for time synchronization' is unchecked, 'NTP Server address' is 'pool.ntp.org', and 'Timezone' is 'UTC+3'. The 'WEB' section contains fields for 'Server address' (hw.guardsaas.com), 'Port' (80), 'Path' (/data.php), 'Use HTTP proxy' (unchecked), 'Proxy Server address' (192.168.1.1), 'Proxy Server port' (3128), 'Password' (ab974088d09d4dc3), 'Connection interval' (10), and 'Event count' (1). A 'Save' button is located at the bottom of the window.

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

Port: port na którym chmura serwera internetowego jest przesyłana.

Ścieżka: Ścieżka do pliku przetwarzania danych na serwerze chmury internetowej.

Hasło: Hasło dostępu do danych na serwerze chmury internetowej.

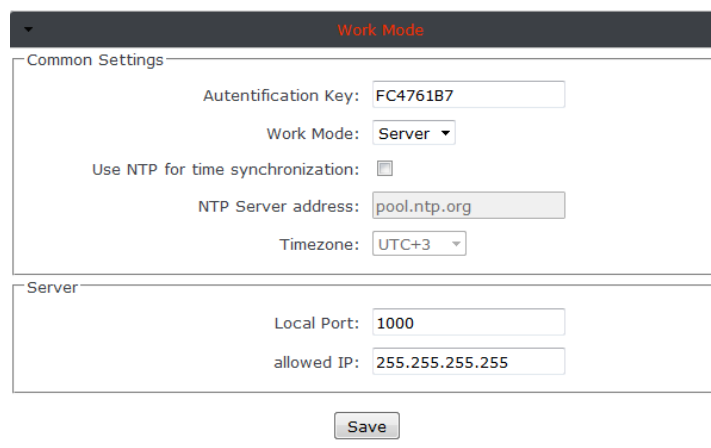
Interwał transmisji: Odstęp między okresowymi połączeniami z serwerem internetowym w sekundach.

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:



The screenshot shows a configuration window titled 'Work Mode'. It contains two main sections: 'Common Settings' and 'Server'. In the 'Common Settings' section, the 'Authentication Key' is set to 'FC4761B7', 'Work Mode' is set to 'Server', 'Use NTP for time synchronization' is unchecked, 'NTP Server address' is 'pool.ntp.org', and 'Timezone' is 'UTC+3'. In the 'Server' section, 'Local Port' is '1000' and 'allowed IP' is '255.255.255.255'. A 'Save' button is located at the bottom right of the window.

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 stara się regularnie, aby ustanowić połączenie z oprogramowaniem sterującym. Tryb ten powinien być również wybrana, jeśli kontroler łączy się z serwerem ZProxy. Następujące parametry muszą być spełnione:

The screenshot shows the 'Work Mode' configuration page. It has a dark header with 'Work Mode' in red. Below is a 'Common Settings' section with fields for 'Authentication Key' (FC4761B7), 'Work Mode' (Client), 'Use NTP for time synchronization' (checkbox), 'NTP Server address' (pool.ntp.org), and 'Timezone' (UTC+3). Below that is a 'Client' section with 'Server Address' (192.168.100.111) and 'Server Port' (0). A 'Save' button is at the bottom.

Gdzie:

Adres serwera: Zdalny adres IP lub nazwa serwera z zainstalowanym oprogramowaniem sterującym lub serwerem ZProxy.

Port serwera: Zdalny port TCP wyłapujący połączenia na serwerze.

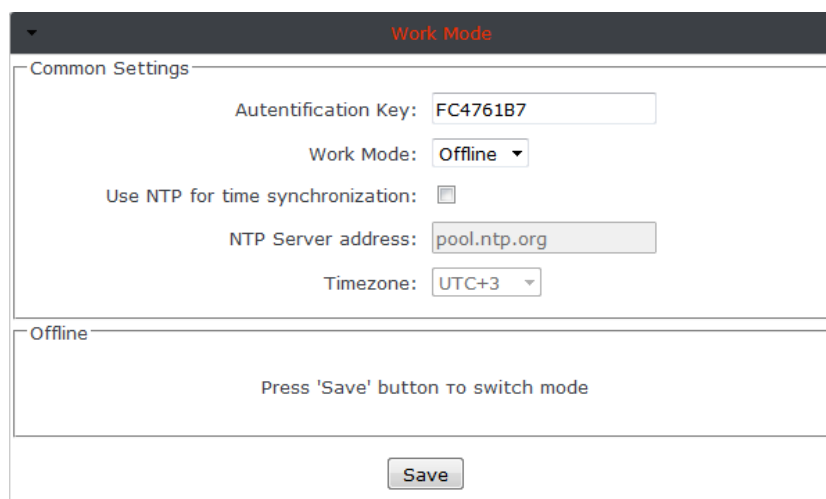
Klucz autoryzacji: Niezbędny do łączenia się z serwerem ZProxy. Oprogramowanie sterujące przekazuje je do serwera ZProxy, który z kolei łączy się z kontrolerem.

Po zakończeniu ustawień, należy zapisać parametry naciskając przycisk **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 potrzebnego klucza Master.

Tworzenie i modyfikacja bazy danych kluczy może się odbywać na dwa sposoby. Po pierwsze, poprzez interfejs sieci web. Po drugie, za pomocą specjalnej karty zbliżeniowej - klucza Master (patrz niżej jak zaprogramować kontroler z kluczem Master). Aby uzupełnić bazę danych kluczy, kontroler musi być podłączony do czytników. W trybie autonomicznym, oba banki pamięci są zarządzane w tym samym czasie. Wybierz tryb **autonomiczny** do konfiguracji bazy danych za pomocą interfejsu WWW. Interfejs wygląda następująco:



Work Mode

Common Settings

Authentication Key: FC4761B7

Work Mode: Offline ▼

Use NTP for time synchronization: ☐

NTP Server address: pool.ntp.org

Timezone: UTC+3 ▼

Offline

Press 'Save' button to switch mode

Save

Gdzie:

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

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

Tryb dodawania kluczy Master: Aktywuje tryb dodawania kluczy Master. Zobacz 7.2 po szczegóły.

Tryb usuwania kluczy: Usuwa klucze z bazy danych przez dotknięcie czytnika. Zobacz 7.3 po szczegóły.

Uwaga: W momencie wyboru trybu dodawania kluczy Master lub trybu usuwania kluczy, wyskoczy okno informując, że kontroler automatycznie opuści ten tryb, gdy przerwa między kluczami będzie wynosić 16 sekund.

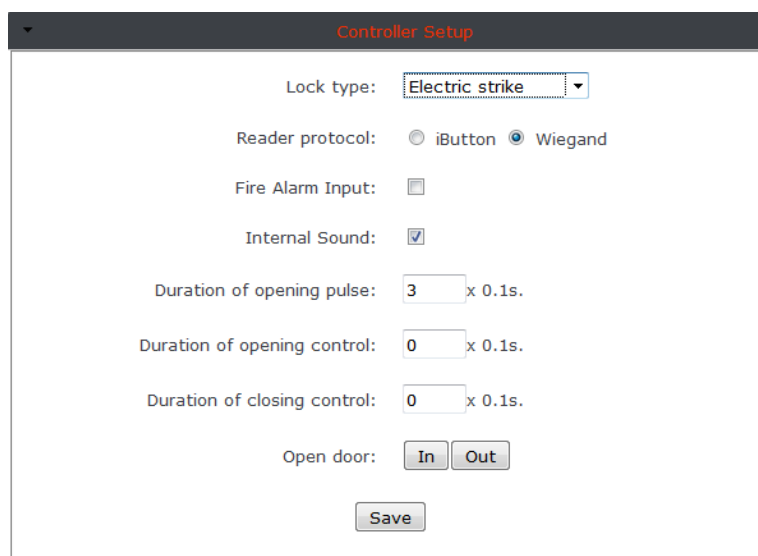
Eksport kluczy do pliku: Eksportuje bazę danych kluczy z pamięci kontrolera do pliku na lokalnym komputerze z interfejsem sieci web.

Przeglądaj ...: Wybieranie pliku na komputerze lokalnym przy kolejnym imporcie kluczy.

Importuj klucze z pliku: importuje (poprzednio wyeksportowane) plik do bazy danych kluczy kontrolera. Poprzednia zawartość bazy danych zostanie nadpisana i utracona.

5.5 Zakładka ustawień kontrolera.

Zakładka ustawień kontroler pozwala skonfigurować parametry operacyjne kontrolera.



Typ zamka: Elektryczny zatrzask, elektromagnetyczny lub elektromechaniczny.

Protokół czytników: Wybierz protokół transmisji kodu klucza. Dla protokołu Wiegand, kontroler automatycznie wykrywa szerokość bitową (26, 34, 42 lub 50).

Wejście alarmu pożarowego: Umożliwia odblokowanie drzwi awaryjnych, gdy sygnał wejściowy EX.OPEN został aktywowany.

Wbudowana brzęczyk: włączenie/wyłączenie wbudowanego sygnalizatora.

Czas otwarcia: Okres odblokowania zamka w celu otwarcia drzwi. W zależności od typu blokady, impuls może być aktywny-niski lub aktywny-wysoki.

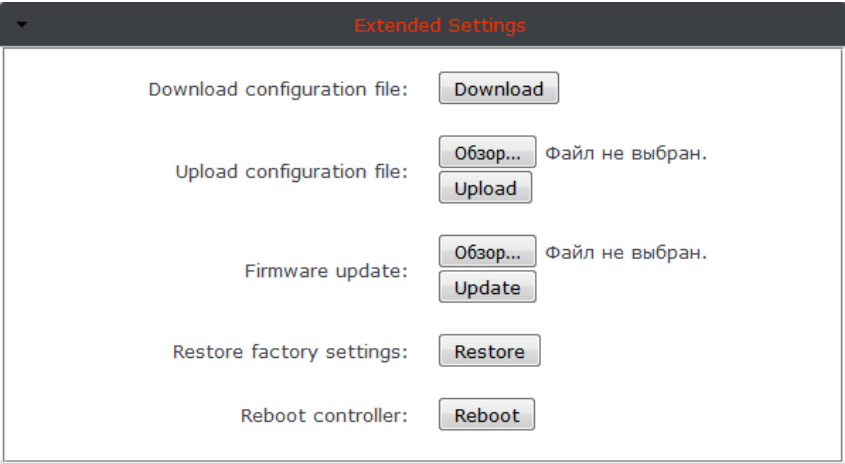
Kontrolowany czas otwarcia - Maksymalny czas po udzieleniu dostępu, gdy drzwi są otwarte. Jeśli po tym okresie drzwi zostaną otwarte, będzie to uważane za sforsowanie. Jeśli kontrolowany czas otwarcia jest krótszy niż czas otwarcia, - czas otwarcia jest używany dla tej funkcji.

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

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

5.5.1 Zakładka ustawień zaawansowanych.

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



Eksport konfiguracji do pliku: Eksportuje bieżącą konfigurację kontrolera do pliku na lokalnym komputerze z interfejsem WWW.

Import konfiguracji z pliku: Importuje konfigurację kontrolera z pliku na lokalnym komputerze z interfejsem WWW. Wybierz plik konfiguracyjny za pomocą przycisku **Przeglądaj....**

Aktualizacja oprogramowania: Aktualizacja oprogramowania kontrolera. Wybierz plik zawierający nowe oprogramowanie za pomocą przycisku Przeglądaj

Przywracanie ustawień fabrycznych: Przywraca wszystkie ustawienia do wartości domyślnych, obecna konfiguracja jest nadpisana i utracona.

Restart kontrolera: restart kontrolera w celu uaktualnienia zmiany ustawień sieciowych.

5.5.2. Zakończenie pracy z interfejsem sieci Web

Aby zakończyć pracę z interfejsem, należy zmienić położenie zworki z CONFIG na NORMAL lub LOCK, przejść do zakładki Ustawienia zaawansowane i wybrać tam funkcję **reset kontrolera**.

6. WŁĄCZENIE I ROZPOCZĘCIE PRACY.

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

- **Użycie** serwera DHCP;
- **Konfiguracja** połączenia Ethernet;
- **Wyłączenie** protokołu **Wi-Fi**;
- Tryb oprogramowania **serwera**, port lokalny - 1000.

Uwaga: Możliwe jest tylko, aby zmienić konfigurację modułu podłączenia poprzez interfejs sieciowy.

Zmiana ustawień fabrycznych jest opisana w punkcie 5 tej instrukcji. Proszę ustawić ustawienia fabryczne zgodnie z wybranym trybem.

Wyłącz kontroler. Ustaw zworkę w pozycji NORMAL lub LOCK. Włącz zasilanie kontrolera. Kontroler jest gotowy do pracy w wybranym trybie.

Aby używać kontrolera w trybie **autonomicznym**, uruchom interfejs sieci Web, a następnie wybierz zakładkę trybu połączenia dla oprogramowania sterującego, ustaw tryb połączenia na **autonomiczny** i utwórz co najmniej jeden klucz Master.

Pozostań w trybie **autonomicznym**, wyjdź z interfejsu i utwórz klucze Normal.

7. USTAWIENIE KONTROLERA PRZY POMOCY KLUCZA MASTER

Aby zarządzać kontrolerem poprzez klucz Master (tj 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. We wszystkich trybach programowania, istnieje funkcja przekroczenia czasu: po 16 sek. po ostatnim dotyku, kontroler opuści tryb programowania, emitując cztery krótkie sygnały dźwiękowe.

Uwaga 1: Kontroler zawiera dwie bazy danych klawiszy. W trybie autonomicznym, są one zapełniane i usuwane równocześnie.

Uwaga 2: Aby korzystać z programowania klucza Master, podłącz czytniki poprzez protokół **iButton™**.

Możliwe są następujące tryby programowania:

- **Dodawanie klucza Normal - 1 długi dotyk;**
- **Dodawanie klucza Master - 1 krótki dotyk, 1 długi dotyk;**
- **Usuwanie klucza Normal- 2 krótkie dotyki, 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. 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 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 kluczy Normal

Zbliż klucz Master na krótko do czytnika. 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. Nie później niż 6 sekund po tym, dotknij i przytrzymaj klucz Master do czytnika (długi dotyk). Przy trzecim kontakcie, kontroler wyda trzy krótkie sygnały dźwiękowe, a po 6 sek. jeden sygnał oznaczający przejście w tryb usuwania kluczy Normal. Teraz odsuń klucz Master od czytnika. Aby usunąć klucze Normal i Block, zbliżaj je jeden po drugim, upewniając się, że odstęp pomiędzy dotknięciami nie przekracza 16 s.

Przy każdym dotknięciu, skuteczne usunięcie klucza zostanie potwierdzone krótkim sygnałem dźwiękowym; jeśli klucz nie istnieje w pamięci, zostaną wyemitowane dwa dźwięki. Aby wyjść z tego trybu, albo odczekaj 16 s po ostatnim dotknięciu klucza, albo dotknij czytnik kluczem Master. Kontroler potwierdzi wyjście z trybu programowania czterema krótkimi sygnałami.

7.4 Tryb usuwania całej pamięci

Zbliż klucz Master na krótko do czytnika trzykrotnie. Kontroler wyemituje krótki sygnał dźwiękowy potwierdzający rozpoznanie klucza Master. Przy drugim kontakcie, kontroler wyda dwa krótkie sygnały oznaczające przejście klucza Master w tryb programowania. Przy trzecim kontakcie, kontroler wyda trzy krótkie sygnały oznaczające trzecie poprawne zbliżenie klucza Master.

Nie później niż 6 sekund po tym, dotknij i przytrzymaj klucz Master przy czytniku (długie dotknięcie). Przy czwartym dotknięciu, kontroler wyemituje cztery krótkie sygnały dźwiękowe, a po 6 sek. - serie krótkich sygnałów oznaczających kasowanie pamięci kontrolera i automatyczne wyjście z trybu programowania.

Teraz można odsunąć klucz główny od czytnika.

Uwaga: Gdy baza kluczy jest kasowana przez klucz Master, zaprogramowany czas otwarcia zamka (blokady) 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

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 kluczem Master krótko pięciokrotnie czytnika. 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 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 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 blokujący 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. ZAWARTOŚĆ OPAKOWANIA.

- Kontroler Z-5R WEB - 1
- Zestaw montażowy - 1
- Bateria CR2032 (typu zegarkowego)- 1
- Instrukcja obsługi - 1

10. WARUNKI PRACY

Dopuszczalna temperatura pracy: +5°C do +40°C

Wilgotność: nieprzekraczająca 80% 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 w pełni poprawnie podczas pracy w warunkach innych niż zalecane.

11. 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.

Prezentujemy 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:



Pozbycie 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.

WARUNKI GWARANCJI

Producent udziela gwarancji na okres 24 miesięcy 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 rma.hatpol.pl. Reklamowany sprzęt klient musi dostarczyć do serwisu HatPol na własny koszt. Przesyłkę powrotną przyjętego do reklamacji pokrywa firma HatPol, 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 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, 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 w każdej chwili warunków gwarancyjnych, 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: www.hatpol.pl/rma

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