

Network controller with built-in EM-Marine reader

Matrix II Wi-Fi

User Manual

1. GENERAL INFORMATION

Matrix II Wi-Fi network controller with built-in EM-Marine reader is a next generation model in Matrix-II product family. Initial model of EM-Marine proximity cards reader was Matrix-II. It was followed by successor model Matrix-II K reader, combined with stand-alone controller, and later by its network version Matrix-II Net, operating under RS-485 protocol. Further development of network device is Matrix II Wi-Fi, which represents the reader combined with a Wi-Fi network controller, and which is used in Access Control Systems (ACS) to operate a single access point. Integrated reader of this device is able to read EM-Marine proximity cards, but the device itself supports operating Mifare cards too if connected to an external reader.

Please refer to some operating facts about Matrix II Wi-Fi.

1. The term “Reader” is not an exact description of this device, as Matrix II Wi-Fi actually comprises two individual devices in one housing, EM-Marine proximity cards reader and a network controller. Therefore, it will be hereinafter referred to as “device”.

2. Two additional external readers can be connected to Matrix II Wi-Fi device, iButton protocol and Wiegand protocol are supported. Important: both additional external readers must be working under the same protocol. Hence, up to 3 readers (including one integrated iButton reader) can be connected to one controller. Controller will automatically recognize protocol of the external readers. DS1990A contactors may be installed instead of external readers.

3. ACS actions depend on the presence of the card ID in the controller's memory and on its status, as assigned to the card upon recording. “Card ID” is often called a “key”, therefore terms “card” and “key” will be considered as equivalent hereinafter (e.g. “touch with a card” or “touch with a key” mean the same). The full list of cards (keys), along with their statuses, is called “ACS database”.

4. Matrix II Wi-Fi device's “programming” hereinafter applies to the device's controller part only: e.g. initial card ID recording into controller's memory with its status assignment, deleting existing card ID from ACS database, etc. The reader part of the device, whether integrated or external, executes only procedures of reading the swiped card's ID and transmitting the acquired ID to the controller part.

5. To work with Matrix II Wi-Fi device, each new proximity card must be assigned a “status” (defined owner access rights). The status of the card is assigned upon its first swipe against the reader in programming mode. To change the card's status, such card's ID should first be removed from controller's memory, and then recorded again with different status.

There are several options of the card's status:

- Master-card – is used for programming of Matrix II Wi-Fi device and is not intended for access;
- Standard card (Access card) – is intended for passing through an access point (unless such access point is in “Block” mode);
- Blocking card – is intended for passing through an access point, including the one in “Block” mode, and for switching “Block mode” on/off at an access point. This card has a higher-level status than a Standard card. Blocking card opens the lock when it's removed from the reader.

6. In Standard access mode, Matrix II Wi-Fi device grants access for both Standard and Blocking cards (keys).

In “Block” access mode, the device grants access for Blocking cards only, while Standard cards are denied. For example, if common workers are given Standard cards and security staff are given Blocking cards, you can grant access to all employees with Standard mode during working hours, but restrict access to security staff only with Block mode at night.

After one of the device's readers is touched with a card, controller checks access rights: if the submitted card's ID is present in the database or not, and what the status of the card is. After that the controller sends control signal (lock/unlock power transistor) to the lock (electromechanical or electromagnetic lock or latch, or turnstile). Lock type and readers' protocol are defined during controller configuration.

Master-cards (Master-keys) are intended for programming the device's controller without computer connection. They are not intended for accessing. Master-keys are designated to: add/remove Standard, Blocking and Master keys records in device's database, set up unlocking interval, turn on/off "Accept" access mode.

In "Accept" access mode, any swiped key is treated as valid and is recorded into controller's memory with "Standard key" status. This mode is used to build up keys database during ACS installation where physical keys have already been distributed among users.

While "Accept" mode is running, controller collects information about submitted keys. After certain time it switches back to Standard mode and will grant access only to those keys, which have been recorded in its memory.

Please note that erasing Master-card record from the database is possible only when controller's memory is erased or overwritten, i.e. when whole ACS database is deleted.

7. Initially, Matrix II Wi-Fi device's memory is empty. The first thing to record in controller's memory is Master-card information. This card will subsequently be used for device's manual programming. Programming process will be described later.

Important! If the device operates in standalone mode, manual programming (recording keys database) is possible only via iButton protocol reader. Such reader may be integrated reader, or one of external readers connected via iButton protocol.

8. The following equipment can be connected to Matrix II Wi-Fi device:

- two external EM-Marine or Mifare proximity-card readers via iButton or Wiegand protocol (both readers must operate the same type of protocol), or two Dallas Touch Memory contactors to work with DS1990A keys;
- electromagnetic or electromechanical lock;
- lock release button ("Exit" button, normally-open type) – to open the door without checking access rights;
- external LED and external buzzer;
- door sensor (normally-open type) – to capture "passing completed" event, so that duration of door-unblocking sound alarm is reduced (duration of "open" signal to the lock is reduced).

Additionally, controller can receive external emergency unlock signal.

9. Matrix II Wi-Fi device can operate in standalone and network modes.

This device's installation and standalone operating is identical to those of Matrix II K, while network operating is identical to Z-5R Web.

10. Recording ACS database (keys database) in standalone mode is done with Master-card.

In network mode, device's operation and keys database recording is managed by external software via network connection. Apart from keys database management, network mode enables the following procedures: record events, set up local time in the device's controller, and define individual access time-slots for each card. Should Matrix II Wi-Fi device lose its connectivity with the management software while in network mode, it continues operating in standalone mode and records events off-line into events buffer. Controller's memory can hold up to 2048 events, like acquiring a card code, door sensor triggering, control signal output, etc.

2. SPECIFICATION

Integrated reader	
Working frequency, kHz:	125
ID type:	EM-Marine
Minimum reading distance, cm:	3
Controller's data-exchange protocol:	iButton (Dallas Touch Memory)
Connectible external readers (with same data-exchange output protocol only)	
ID type:	recognized by controller (EM-Marine, Mifare, etc.)
Connection protocol:	iButton or Wiegand
Maximum connection wiring length for iButton, m:	15
Maximum connection wiring length for Wiegand, m:	100
DS1990A contactors may be installed	

Controller	
Memory size for keys, no.:	2024
Memory size for events, no.:	2048
Maximum number of connectible external readers (contactors):	2
Connection protocols: for readers for contactors	iButton, Wiegand iButton
Readers' indicators control:	yes
Output type for lock connection:	MOS-transistor
Current for power output, A:	5
Jumper for lock type selection:	electromagnetic, electromechanical
Lock release duration timer, sec.:	0,1~1000 (factory default = 3)

Wi-Fi connection module	
Standards:	IEEE 802.11b, IEEE 802.11g
Frequency range:	2.4-2.4835 GHz
Maximum link rate	11g: 54Mbit/s 11b: 11Mbit/s
Transmitter power:	<20dBm (<100mW)
Operation modes:	Hotspot, Client
Security:	WPA/WPA2, WPA-PSK/WPA2-PSK
USB Interface	
Connector:	Micro USB, Type A
Version:	USB 2.0
Mode:	Device, Full/Low Speed

Other parameters	
Audio-visual indication of operation modes:	yes
Power supply operating voltage, V:	12 (within range 9~24)
Maximum operating current at 12V, mA:	100
Protection against wrong connection:	yes
Dimensions, mm:	85x44x18
Weight, g.:	100

3. CONNECTING EXTERNAL DEVICES

Dimensions and Terminals layout are shown on Figure 1.

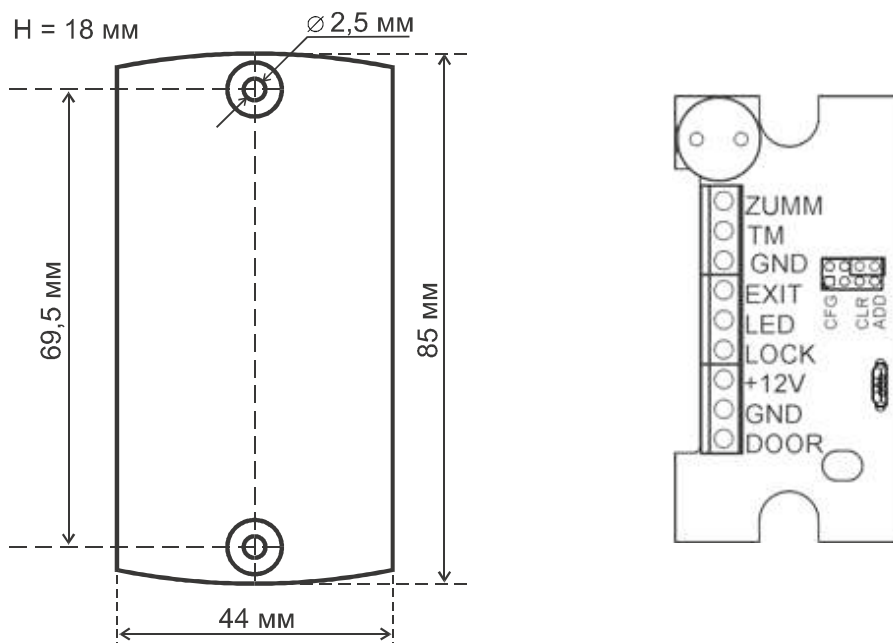


Figure 1. Dimensions and Terminals layout

Terminals definition is given in the table below:

ZUMM	External buzzer. Only a buzzer with integrated 12V generator with maximum operating current 200 mA should be used. Negative wire connects to this terminal, positive wire connects to +12V terminal.
TM	External reader or contactor.
GND	Signal earthing. To connect common wires from external reader, contactor, door sensor and lock release button.
EXIT	Lock release button. Closing the contact results in door unlocking. Recommended to connect with twisted pair.
LED	External reader's green LED control.
LOCK	Lock's negative winding wire.
+12V	+12V Power supply unit plus wire, lock's positive winding wire.
GND	Power earthing. Power supply unit minus wire.
DOOR	Door sensor. Twisted pair recommended. When the door sensor is triggered by door opening, it allows to switch off sound signal of controller earlier and to save power either by turning electromechanical lock off immediately after the door opens, by turning electromagnetic lock on only after the door closes.

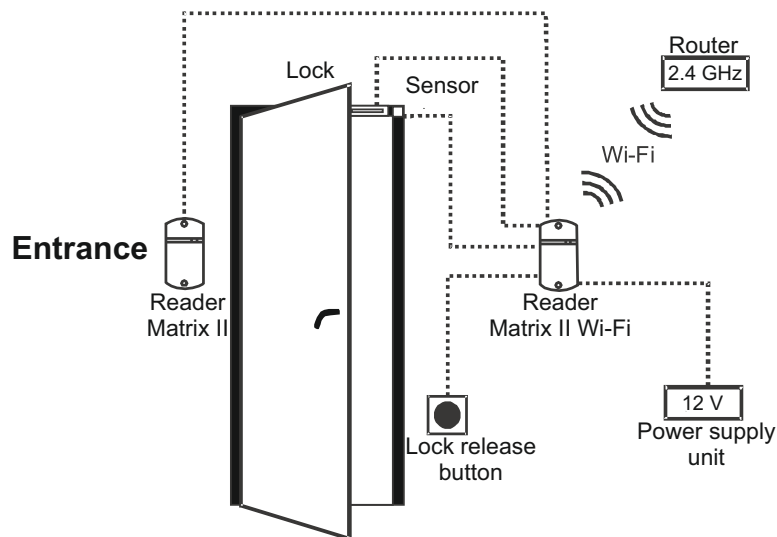


Figure 2. MATRIX II Wi-Fi connection diagram

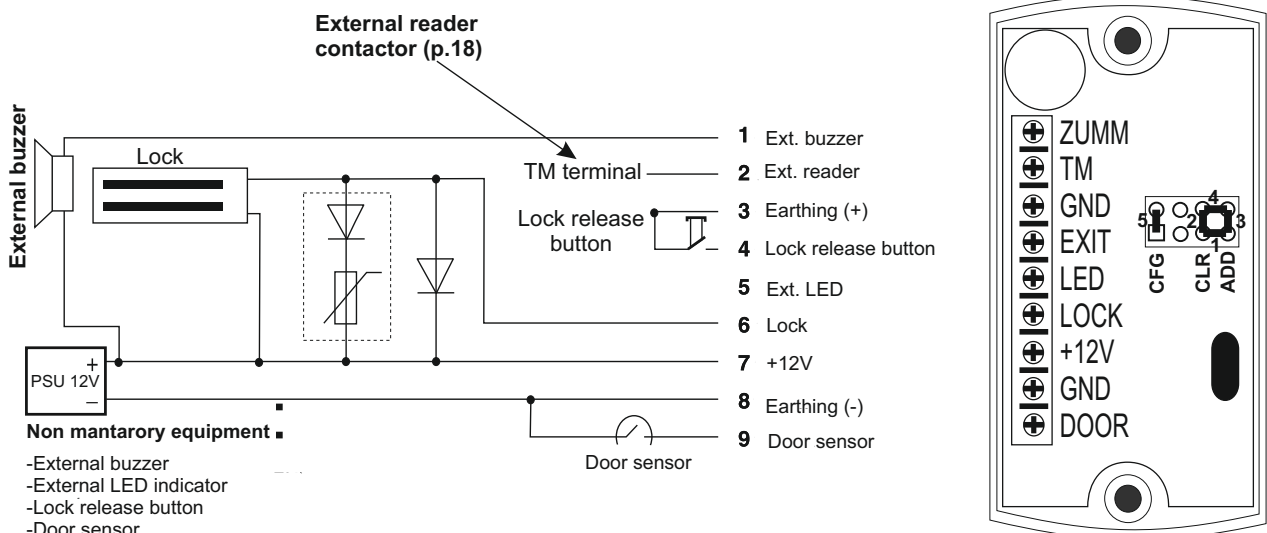


Figure 3. External devices connection diagram

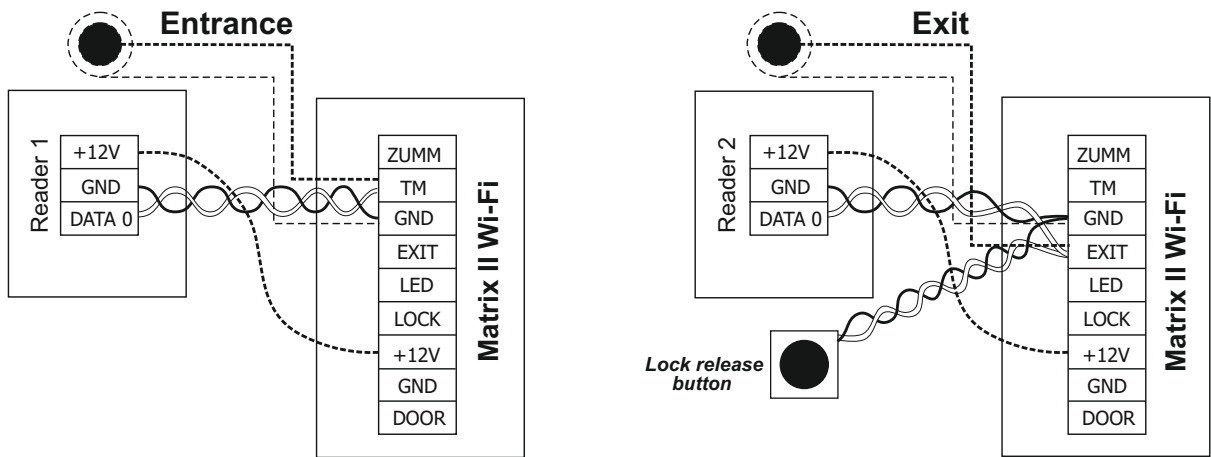


Figure 4. External readers connection diagram

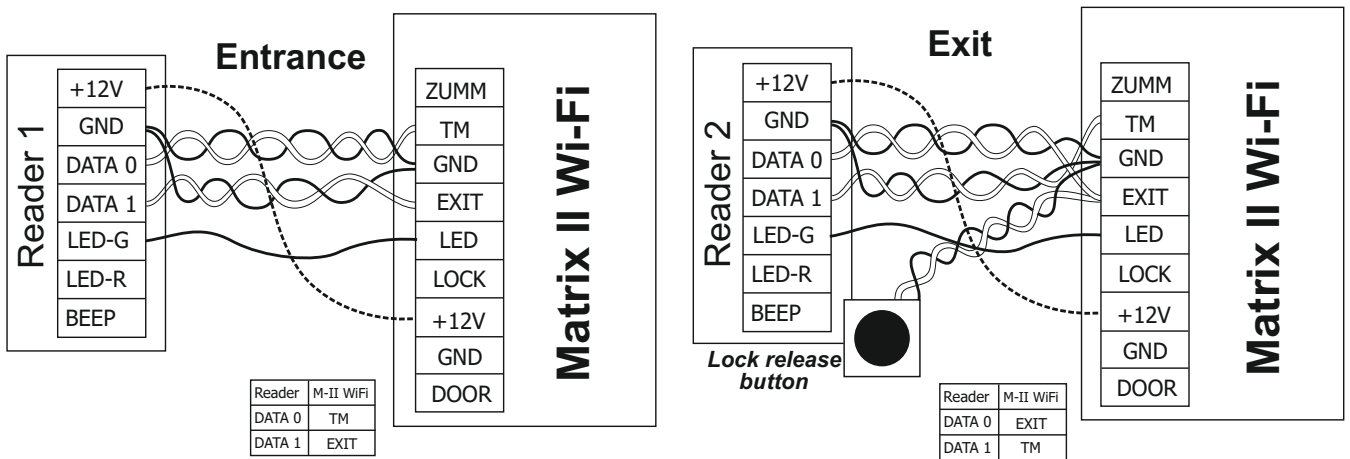


Figure 5. External Wiegand readers connection diagram

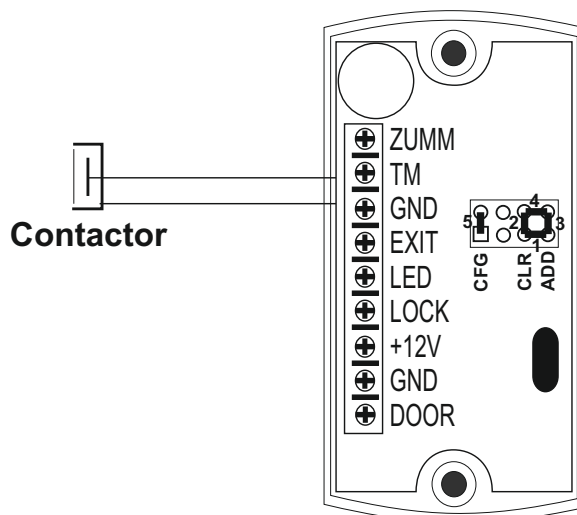


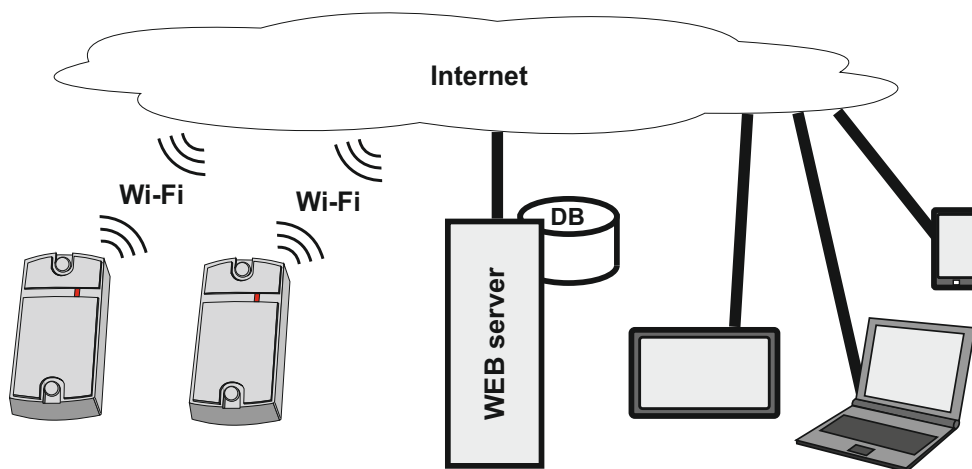
Figure 6. Contactor connection diagram

4. NETWORK CONNECTION MODES FOR MATRIX-II Wi-Fi DEVICE

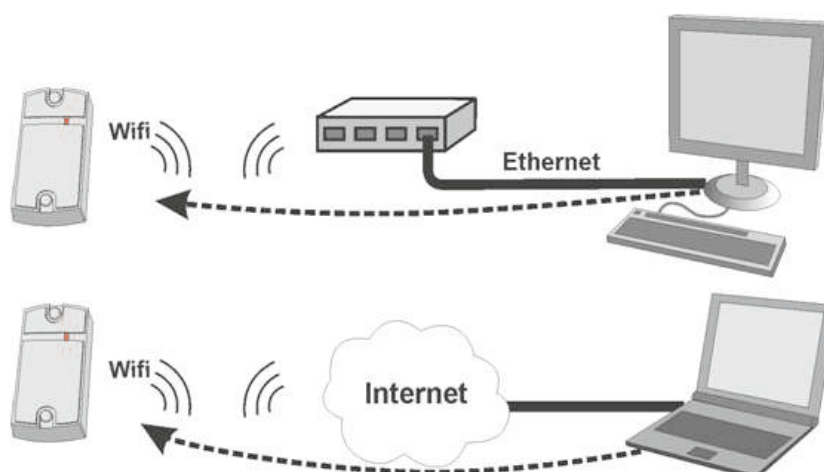
Wi-Fi network connection parameters must be set up to operate the device in network mode. When configuring the device, please note that Matrix II Wi-Fi device actually consists of three functional modules: integrated reader, ACS controller and Wi-Fi network connection module. The network module provides Wi-Fi connection of the device to facility's local network and establishes connectivity with local PC running ACS control software to manage access control functions (keys database management, definition of access rights, reading events from events buffer, etc.).

There are three modes of control software connection:

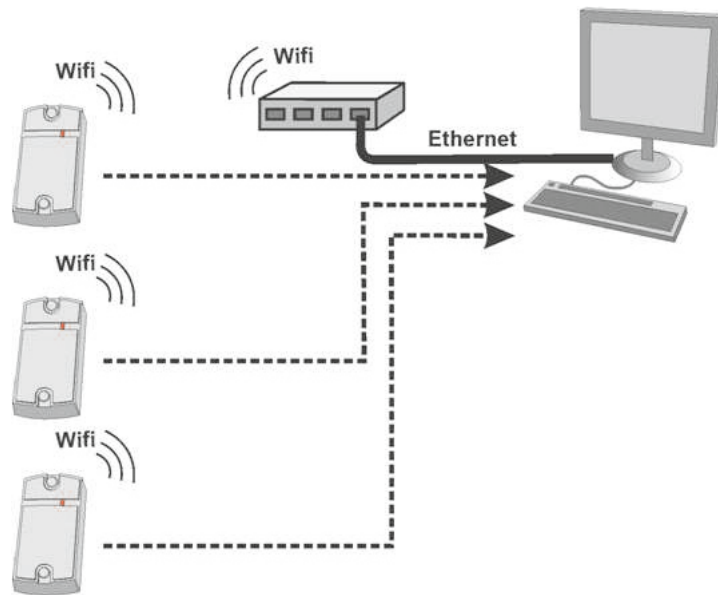
- **WEB** connection mode. In this mode, the connection module connects to a control Web server on the Internet, and the device is managed via a Web site (for example, Cloud ACS solution www.guardsaas.com);



- **Server** connection mode. In this mode, the connection module is listening for TCP/IP calls from the PC running control software (for example, GuardCommander, GuardLight, or Avantgarde [Авангард]);

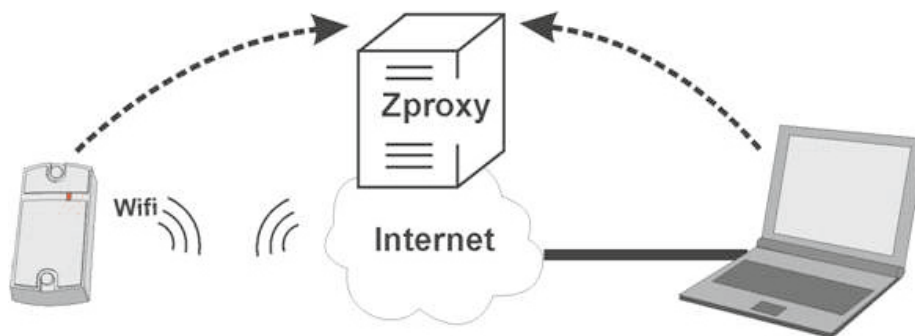


- **Client** connection mode. In this mode, the connection module attempts to connect to control software via TCP/IP. To configure this mode, provide the IP address and port number of a remote PC running the control software (for example, GuardLight, Avantgarde [Авангард], or Zproxy server).



- **Zproxy** Server (available at zproxy.con.ru) allows the (proxied) connection between the controller and the control software, where direct TCP/IP connection is impossible, e.g. if the controller and the software are in different LANs. If Internet access is available, the controller connects to ZProxy server, the control software connects to that server too and requests connection to the required controller using a password.

If no connection exists to control software, the controller will work in Standalone mode.



5. WEB INTERFACE

The Web interface is used to configure connection parameters and connected equipment. To run initial configuration, a device with Wi-Fi network connection (tablet, notebook, or smartphone) and with an integrated web-browser (Internet Explorer, FireFox, Opera, Chrome etc.) is required. Please follow these steps to access the Web interface of controller's preferences:

6. Set on-board jumper into CFG position (please refer to Section 6: "Power up and getting started");

7. Power up the device;

8. Connect to the device via Wi-Fi:

-Wait until a Wi-Fi access point with the name Matrix_II_WiFi_XXXXXX appears;

-Connect to that Wi-Fi;

Factory default password is called AUTH_KEY. It contains 8 characters and can be found either on the sticker on the back side of the device's housing, or in the end of this manual. Please note, that the AUTH_KEY password is case-sensitive, please type it exactly as shown.

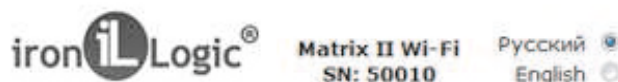
4. Browse <http://192.168.10.1> (login: **matrix**, password: AUTH_KEY);

5. Go through appearing menu tab by tab and configure parameters on each tab. Please do not forget to save the changes on each tab.

Once the configuration is complete, please remove the on-board jumper from CFG position and wait until Matrix II Wi-Fi device is connected to LAN. From this moment onwards, the preferences Web interface will still be available by the IP address as it was assigned during initial configuration (more details in Section 5.3 below), or the IP address will be automatically acquired from DHCP server when registering onto LAN.

5.1 Language Selection

On initial power up, the Web interface is set to work in English. Please select “Русский” (Russian) radio button in the upper-right corner of this Web interface to switch to Russian language:



5.2 Status Tab

The Status Tab displays the current status of the device:

Status	
Mode:	WEB
Connection:	
Elapsed Time:	0 days 00:01:01
Controller Software:	2.22
Connection Module Software:	1.09
CFG Jumper:	On

Legend:

Mode: Device operation mode (Web, Server, Client, Standalone).

Connection: In Client and Server operation modes, shows the IP address of connected PC running the control software.

Elapsed Time: Time elapsed since the controller was powered up.

Controller Software Version: Displays current version of controller's software.

Connection Module Software Version: Displays current version of connection module's software.

CFG Jumper: Shows if the on-board jumper is set to CFG position: On or Off.

5.3 Connection Setup Tab

Connection Setup Tab allows setting up network connection type and connection parameters. Parameters configuration is similar to that of an Internet router.

Connection Setup

Wi-Fi

SSID:

Password:

TCP/IP

Use DHCP:

Static IP:

Network Mask:

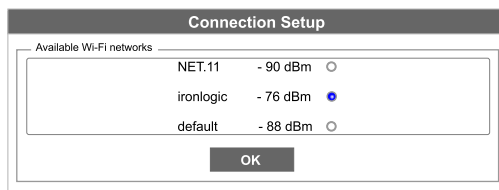
Gateway:

DNS Server:

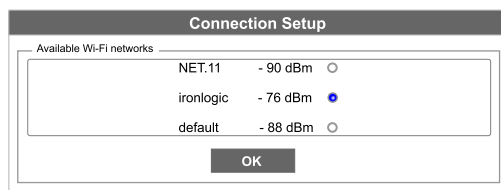
SSID: The SSID identifier of the Wi-Fi network to connect to.

Password: Security key (password) for this Wi-Fi network.

Search network: launch a search of currently available Wi-Fi networks. After available Wi-Fi networks are discovered, a dialog box will appear with the list of available networks. Next to each network name, its signal level is given:



To select a network, highlight it in the list and press OK button. When selected, SSID of that network will be displayed in settings area automatically. If a network is not broadcasting its SSID, it has to be manually inserted into the SSID textbox. If network security is enabled, enter the security key as well:



Test network: Check connectivity using current SSID and Password values. Even if the password is correct, router might reject connection due to missing MAC-address validation (if enabled).

Use DHCP: request DHCP server to provide IP address and other network parameters needed to work in this network.

In case if DHCP server is unavailable, following network parameters must be configured manually:

Static IP: a unique IP address assigned to all devices inside the network.

Network Mask: Subnet mask for this LAN segment.

Gateway: IP address of the gateway leading to other networks (including Internet).

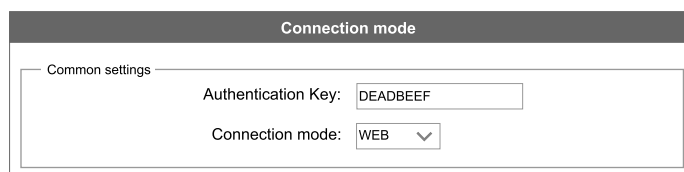
DNS Server: The DNS server IP address.

All network parameters must be configured for correct device operation. If any of those parameters are unknown, please refer to your network administrator.

After setting is complete, please save parameters by pressing **Save** button.

5.4 Connection Mode Tab

If Matrix II Wi-Fi device is intended to work in network mode, i.e. under external software control, then after completing LAN connection configuration, it is also necessary to set up the connection mode between control software and connection module. Connection mode to the control software is selected in Connection Mode Tab:



Where:

Authentication Key: it is required for connecting to a cloud-based internet server, when working via a ZProxy server, and for accessing WEB interface of the Matrix II Wi-Fi device.

Initially this field contains the factory pre-set key, found on a sticker on the back of the device housing (refer to AUTH_KEY). It is possible to change it at this stage, if necessary (Only alphanumeric characters allowed).

Connection mode: choose **Web**, **Server**, **Client** for network operation, or **Standalone** to operate without a control software connection.

5.4.1 Web

Web connection mode provides connection to a cloud SaaS (Security as a Service). To set it up, the following parameters are required from SaaS vendor:

WEB	
Server Address:	<input type="text" value="hw.guardsaas.com"/>
Use HTTP-proxy:	<input checked="" type="checkbox"/>
Proxy Server Address:	<input type="text" value="192.168.10.1"/>
Proxy Server Port:	<input type="text" value="3128"/>
Password:	<input type="text" value="ab974088d09d4dc3"/>
Transmission Interval:	<input type="text" value="10"/>
Number of events:	<input type="text" value="1"/>

Server Address: name or IP address of the cloud service Web server, where the controller should connect.

Use HTTP-proxy: specify if addressing a special local server for internet access is required.

Proxy Server Address: network address of the proxy server in local network.

Proxy Server Port: port ID for connecting to proxy server.

Password: data access password on the cloud Web server.

Transmission Interval: the interval between connections to the Web server in seconds.

Number of events: number of pending controller events that trigger an out-of-sequence data transmission to Web server, before the current Transmission Interval has elapsed.

After setting is complete, please save parameters by pressing **Save** button.

5.4.2 Server

In Server connection mode, the connection module is listening for control software connection on a local port. If this mode is selected, the following parameters must be specified:

Server	
Server Adress:	<input type="text" value="1000"/>
Allowed IP:	<input type="text" value="255.255.255.255"/>

Where:

Local Port: Local TCP port listening for control software connection.

Allowed IP: Source IP address from which control software can connect to controller. (To allow connections from any IP, please use 255.255.255.255 value).

After setting is complete, please save parameters by pressing **Save** button.

5.4.3 Client

In Client connection mode, the connection module regularly attempts to establish connection to the control software. Also select this mode, if the controller connects to a ZProxy server. The following parameters have to be provided:

Client	
Server Address:	<input type="text" value="192.168.1.10"/>
Allowed IP:	<input type="text" value="25000"/>

Where:

Server Address: IP address of a target server system running the control software, or IP address or server name of a **ZProxy** server (zproxy.con.ru).

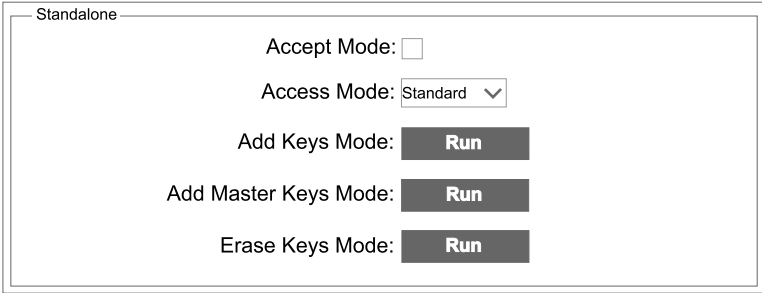
Server Port: TCP port on the server listening for connections (25000 for **Zproxy**).

After setting is complete, please save parameters by pressing **Save** button.

5.4.4 Standalone

The initial ACS setup, done by jumpers on other controllers (like on Z-5R controller), is performed in Standalone mode on this device. This mode is intended to operate controller keys database via Web interface, without using the Master key. Recording and modifying the keys database can thus be done in two ways. First is via Web interface, second is using a special Proximity card called a Master key (controller programming with a Master key will be explained later). It is possible to use either integrated or external iButton reader to operate keys database of Matrix II Wi-Fi device. Operating keys database via Wiegand reader is not supported!

Please select **Standalone** mode to configure keys database via Web interface. The interface will look as follows:



Standalone

Accept Mode:

Access Mode: Standard ▾

Add Keys Mode: **Run**

Add Master Keys Mode: **Run**

Erase Keys Mode: **Run**

Accept Mode: activates Accept mode, where all new keys will be stored into memory as new Standard keys.

Access mode: available access modes: **Standard mode** (regular access mode),

Block mode (access granted to Blocking cards), **Free access** (doors unlocked), **Waiting** (can be turned on only via Web interface; when an access point is in Block mode, and Waiting mode is turned on, the first submitted Standard or Blocking card (but not Master card!) will convert access mode into **Free access**).

Add Keys Mode: activates Add Standard and Blocking Keys mode on the device (more details in Section 7.1).

Add Master Keys Mode: activates Add Master Keys mode on the device (more details in Section 7.2).

Erase Keys Mode: erases Standard and Blocking keys touching the reader from the keys database (more details in Section 7.2).

Master keys can't be erased in this mode.

When Add Keys, Add Master Keys or Erase Keys mode is selected, an additional pop-up will display a timer, showing remaining time before this mode gets automatically terminated.

5.5 Controller Setup Tab

Controller Setup tab allows to set up controller operational parameters of Matrix II Wi-Fi device:

The screenshot shows a web interface for configuring a controller. The title is "Controller Setup". The fields are as follows:

- Lock Type: Electromagnetic (dropdown)
- Integrated Beeper:
- Wi-Fi Indication:
- Opening Time: 10 x 0.1s.
- Opening Check Time: 30 x 0.1s.
- Closing Check Time: 0 x 0.1s.
- Synchronize time with NTP:
- NTP-server: pool.ntp.org
- Time zone: UTC+3 (dropdown)
- Open doors: Entrance, Exit (buttons)
- Save (button)

Lock Type: Electric Latch, Electromagnetic, or Electromechanical.

If the lock type is regulated by control software, then this field shows the name of the defined access point, and its adjustment is not possible until resetting the device to factory default settings via Web-interface or via on-board jumper (position #2, please refer to p. 50).

Integrated Beeper: enables/disables the built-in beeper.

Wi-Fi Indication: enables/disables Wi-Fi connectivity status notification, which blinks with blue light indicator. Indications legend: continuous blinking – searching and connecting to a Wi-Fi network; blinking with 3 flashes – configuration mode is on (on-board jumper is set to CFG position); blinking with 2 flashes – connection with control software (server) is established; single flashes – waiting for control software (server) connection.

Opening Time: Duration of the impulse sent into the lock to unlock the door. Depending on Lock Type, the impulse can apply voltage or remove it.

Opening Check Time: Maximum time after access has been granted till the door is open. The door opened after this interval is considered as Forced. If Opening Check Time is shorter than “Opening Time”, then “Opening Time” is used for this function.

Closing Check Time: Maximum time while the door stays open. If within Closing Check Time the door has not closed, a “Door Held” event is generated into the log. To disable Closing Check, set this parameter to 0.

Synchronize time with NTP: Allows connection to a NTP time server to synchronize device's time settings.

NTP-server: IP address of a NTP server, which is used for time synchronization.

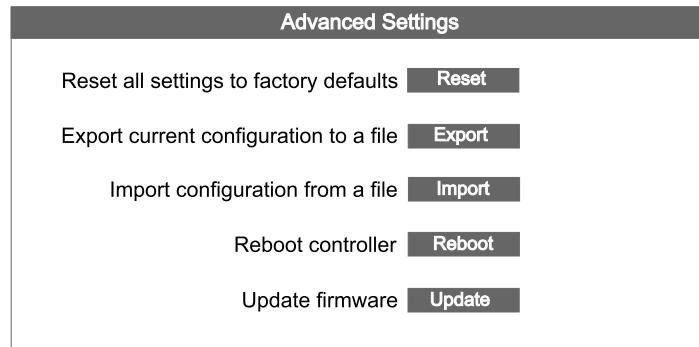
Time zone: identifies the time zone in which the time is synchronized.

Open doors: Lock release buttons on entrance or on exit.

After setting is complete, please save parameters by pressing Save button.

5.6 Advanced Settings tab

Advanced Settings tab allows to install software updates, export and import configuration to/from a file, update the device firmware, reset the controller to factory defaults and reboot Matrix II Wi-Fi device:



Reset to Factory Defaults: resets all settings to factory defaults.

Export Config to File: exports the current controller configuration to a file on the local computer running the Web interface.

Import Config from File: imports the controller configuration from a file on the local computer running the Web interface.

Reboot Controller: reboots the controller to apply the changed network settings.

Firmware Update: allows to update both controller's and connection module's firmware.

5.7 Ending Web interface operation

To finish working with the Web interface, please remove the on-board jumper from CFG position, if present (please refer to Section 6: “Power up and getting started”), go to Advanced Settings tab and choose the Reboot Controller function there.

6. POWER-UP AND GETTING STARTED

Connect external devices to your controller as per Section 3 of this manual. Factory default settings of Matrix II Wi-Fi device network module are as follows:

Network name: «mySSID»;

Password: «WiFiPassword»;

Wi-Fi and DHCP enabled;

Connection mode: WEB, server: hw.guardsaas.com.

Important! Changing the connection module configuration is only possible via Web-interface.

To use the device in network mode with network settings, different to factory defaults, please adjust settings as described in Section 5 of this manual.

To use the controller in Standalone mode, launch the Web interface and select Control Software Connection Mode tab, set the connection mode there to Standalone and create at least one Master key (please refer to Section 7).

Stay in Standalone mode, exit the Web interface and create all needed keys for access.

After saving the changed settings, turn power off. Remove on-board jumper from CFG position and install it according to the used lock type. Turn power on. The device is ready to operate in a mode defined during configuration.

To use the device in standalone mode only, on-board jumper may be used to set the device up:

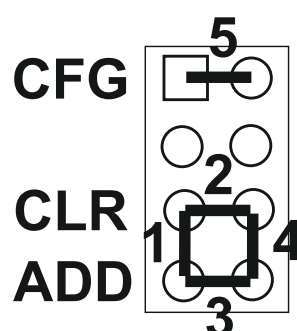


Figure 7. On-board jumper

This jumper may be installed in one of five different positions:

Position #1 - Electromechanical lock (the lock is closed, when the voltage is off) (see **Remark 1**).

Position #2 CLR (clear) - to clear controller memory (database) and reset network module factory defaults.

To do so, power off the device, install the jumper into Position #2 and power it on. When erasing is complete, the device will produce a series of short beep sounds. All keys are erased and programmed door release timer is reset to factory default (3 s)

Position #3 ADD (adding) - to add Standard and Blocking cards into controller memory without using the Master card. Power off the controller, install the jumper into Position #3 and power it back on. After a sound signal, the controller switches to Add Standard and Blocking Cards Mode. A short touch adds a Standard card, and a long touch adds a Blocking card, without need for using a Master card. 16 seconds after the last card touch, the controller exits this mode (accompanied by a series of sound beeps).

Position #4 - Electromagnetic lock (the lock is closed, when the voltage is on). If the jumper is not installed at all, it is considered as if set on Position #4, i.e. Electromagnetic lock (see **Remarks 2 & 3**).

Position #5 CFG (configure) – the device launches connection parameters and connected equipment configuration mode when powered on (please refer to Section 5). The lock is powered down in this mode.

Remark 1. If the lock type setting was done via Web interface or via control software (e.g. GuardLight), then installing the jumper onto Positions #1 or #4 does not affect the lock type selection until factory default settings are reset via Web interface or by installing the jumper onto Position #2.

Remark 2. Since an electromagnetic lock opens only after cessation of its coil current, the door's opening is delayed depending on the current's drop rate. To minimize this rate, a current's drop circuit is integrated in controller. It converts "excessive" lock coil's current into heat, which dramatically reduces the lock Opening Time.

However, the capacity of the circuit is not unlimited, and it can break down due to overheating if the traffic is over 25 passages in 5 minutes. To protect the current's drop circuit in such access points, mounting of bypass diode parallel to lock coil is required. This might trigger electromagnetic lock Opening Time increase by 1-3 seconds as compared with existing current's drop circuit. If such response time increase is unacceptable, we recommend mounting a varistor with operating voltage up to 14V and energy dissipation over 0.7J (V8ZA2P recommended) in series with the bypass diode (Please refer to Figure 6).

Audio-visual status indication for the Matrix II Wi-Fi device.

In standby mode, the red LED is lit, to signal that power is supplied. When a card is submitted to the reader, following options are possible:

- **the card is present in device database** - the green LED blinks, the buzzer rings, the lock is released for the defined Lock Opening Time (or until the door sensor is triggered);
- **the card is missing in device database** – the LED blinks (green and red), the buzzer produces two short ringing sounds.

When the "**Wi-Fi indication**" option is enabled (see section 5.5.), The above indication will be interrupted by the blue LED flashes indicating the status of the Wi-Fi network connection.

7. SETTING UP DEVICE WITH A MASTER KEY

To manage the device (transfer to the desired programming mode: Create / delete simple and / or blocking cards, enable the "Accept" mode, etc.), short (less than 1 sec) and long (about 6 sec) presentations (touches) of the master are used - cards (master key) either to the built-in reader or to an external reader connected via the iButton protocol.

Important: for control, or as they often say - "programming", **reader devices connected via the Wiegand protocol are not supported due to the peculiarities of the protocol.**

There is a time limit for operation in each programming mode after the last presentation of the card to the reader (about 16 seconds), after which the device exits the programming mode, informing with a series of 4 short signals.

The following programming modes are possible:

- **Adding Standard keys – 1 long touch.**
- **Adding Master keys – 1 short tap and 1 long touch.**
- **Erasing Standard keys – 2 short taps and 1 long touch.**
- **Erasing all keys (whole keys database) – 3 short taps and 1 long touch.**
- **Setting Door Opening Time – 4 short taps.**
- **Activate “Accept” mode – 5 short taps.**
- **Deactivating “Accept” mode – 1 short tap.**

7.1 Adding Standard Keys

Touch and hold the reader with a Master key (long touch). The controller will emit a short beep acknowledging the Master key, and after 6 seconds one more beep indicating that controller has switched to Add Standard Keys mode. Take the Master key away from the reader. To add new keys, swipe them against the reader one after another, ensuring that the interval between the swipes is less than 16 seconds. Each new swipe will be acknowledged by the controller with a short beep. Hold a new key against the reader for over 3 seconds to record it as a Blocking key. If the submitted key is already present in the memory, the controller will emit two short beeps. To exit this mode, either wait for 16 seconds after last key touch, or touch the reader with a Master key. The controller will acknowledge exit from programming by 4 short beeps.

7.2 Adding Master Keys

Make a short tap (tap) on the reader with a Master key. The Controller will emit a short beep acknowledging the Master key. Within next 6 seconds, touch and hold the Master key at the reader (long touch). The controller then will emit two short beeps indicating second Master key touch in programming mode, and after 6 seconds more, one beep indicating that controller switched to Add Master Keys mode. Now take the Master key away from the reader. To add new Master keys, swipe them against the reader one after another, ensuring that interval between the swipes is less than 16 seconds. Each new swipe will be acknowledged by the controller with a short beep. However, if the presented key already exists in controller memory as a Master key, there will be no signals. To exit this mode, wait for 16 seconds after last key touch. The controller will acknowledge exit from programming by four short beeps.

7.3 Erasing Standard Keys

Make two short taps (tap) on the reader with a Master key. The controller will emit a short beep acknowledging the Master key on the first tap. On the second tap, the controller will emit two short beeps indicating second Master key touch in programming mode. Within next 6 seconds, touch and hold the Master key at the reader (long touch). On the third touch, the controller will emit three short beeps, and after 6 seconds more, one beep indicating switch to Erase Standard Keys mode. Now take the Master key away from the reader. To erase Standard and Blocking keys, swipe them against the reader one after another, ensuring that the interval between the swipes is less than 16 seconds. On each swipe, successful erasing of a key will be acknowledged by the controller with a short beep. If a key is missing in memory, two beeps will follow. To exit this mode, either wait for 16 seconds after last key touch, or touch the reader with a Master key. The controller will acknowledge exit from programming by four short beeps.

7.4 Erasing All Keys (Controller Memory)

Make three short taps (tap) on the reader with a Master key. The controller will emit a short beep

acknowledging the Master key on the first tap. On the second tap, the controller will emit two short beeps, indicating the second Master key touch in programming mode. On the third tap, the controller will emit three short beeps indicating the third Master key touch. Within next 6 seconds, touch and hold the Master key at the reader (long touch). On the fourth touch, the controller will emit four short beeps, and after 6 seconds more, a series of short beeps indicating controller memory erase and automatic exit from programming mode. Now take the Master key away from the reader.

Note: When keys database is erased via the Master key, the existing programmed Lock Opening Time setting is not erased.

7.5 Setting Lock Opening Time

Make four short taps (tap) on the reader with a Master key. On each tap, the controller will acknowledge the Master key, emitting short beeps. Number of short beeps will correspond with the tap number (one beep for the first touch, two beeps for the second, etc.). On the fourth tap, the controller will respectively emit four short beeps and will switch to Lock Opening Time programming mode. Within next 6 seconds after that, please press and hold the door release button for as long, as the time required for door opening. After the door button is released, the controller will emit a beep and record the new lock opening time. For precise time programming, we recommend using the Web interface.

7.6 Enabling/Disabling “Accept” Mode

Use the Accept mode to store all keys touching the reader into memory. Any key touching the reader will unlock the door and will be stored into controller memory if it's missing there. This mode is used to recover controller's keys database without having to collect all the keys previously distributed to users. A Master key is needed to activate this mode. Make five short taps (tap) on the reader with a Master key. On each tap, the controller will acknowledge the Master key, emitting short beeps. Number of short beeps will correspond with the tap number (one beep for the first touch, two beeps for the second, etc.). On the fifth tap, the controller will respectively emit five short beeps and, in few seconds, a long beep, which acknowledges Accept mode activation. To deactivate Accept mode, touch the reader with a Master key again; a series of short beeps will acknowledge the exit from this mode.

Note: If the power supply fails while Accept mode is active, it remains active after the power is back on.

7.7 Access modes

The controller supports the following access modes:

- Normal access mode – both Standard and Blocking keys grant access;
- Blocking mode – only Blocking keys grant access;
- All-pass mode – the lock stays open.

The Blocking and All-Pass modes are activated with a Blocking key (please see Section 7.1. on how to add one), by touching and holding it against the reader for more than 3 seconds (long touch). If the door is open during this procedure, the All-Pass mode is activated, and if it is closed, the Blocking mode. If Blocking or All-Pass mode is already active, the same action (or touching the reader with a Master key) deactivates it and Normal Access mode is restored regardless of door's position.

Important! When using a Blocking key, the access is granted at the moment when the key is removed from the reader.

In Blocking mode, when a Normal key is used, access is denied and a series of short beeps is produced.

In All-Pass mode, all keys that have touched the reader, are registered in memory for further processing by control software.

Note: If the power supply fails while “Blocking” mode is active, it remains active after the power is back on.

8. CONNECTION BETWEEN NETWORK AND STANDALONE MODES

Note 1: When the power is back after a power failure, the Controller remains in the mode that was active before the failure. Exception: Add/Erase Keys modes do not persist after power is back on, but normal operation mode is reactivated instead.

Note 2: When switching from standalone mode to network mode, the control software usually overwrites existing keys database with the new keys database from the control computer. Therefore, we recommend saving existing keys database before connecting the controller to control software, so it can later be restored, or exported into control software.

Note 3: If while in network or Web mode, a Master key is presented to the controller, most probably nothing happens, because the network software removes all existing Master keys and forbids creating new keys. To enter a new key into networked system while in network mode, use the control software.

Note 4: If after the controller is configured in standalone mode, it will need to be accessed via software (e.g. GuardCommander) over the network, then please use the Web interface to configure the controller for network operation.

9. UPDATING OR RESTORING FIRMWARE VIA USB

Controller may be connected to a PC via USB interface in case if firmware update is not possible via Web interface. Once the device is connected to a PC with a USB cable, it is powered from USB bus, hence external power supply is not needed.

Once connected, the system will recognize a new serial port. Drivers installation might be required, which can be found on www.ironlogic.me website. Software utility for controller's firmware update is also available on this website.

10. PACKAGE CONTENTS

Matrix II Wi-Fi device - 1 pce.
Mounting kit.....- 1 pce.
User manual- 1 pce.

11. OPERATING CONDITIONS

Ambient temperature:.....-40°C... +50°C.

Humidity:.....not exceeding 98% at 25°C.

Device specifications may not fully be as specified, when operating under non-recommended conditions.

The controller should not be operated where the following exists: atmospheric precipitation, direct sunlight, sand, dust and moisture condensation.

12. LIMITED WARRANTY

Device is covered by limited warranty for 24 months.

The warranty becomes void if:

- this Manual is not followed;
- device has physical damage;
- device has visible traces of aggressive chemicals exposure;
- device circuits have visible traces of tamper by unauthorized parties.

While covered, the Manufacturer will repair the device or replace any broken parts, free of charge, where fault is caused by manufacturer's defect.

Product lifetime – 6 years.

13. CONTACTS

Authorized representative in the European Union

ICONCONTROL SIA

1B Balta Street, LV - 1055, Riga, Latvia

E-mail: info@iconcontrol.lv

Phone: +371 24422922

www.iconcontrol.lv



The symbol of crossed-through waste bin on wheels means that the product must be disposed of at a separate collection point. This also applies to the product and all accessories marked with this symbol. Products labeled as such must not be disposed of with normal household waste, but should be taken to a collection point for recycling electrical and electronic equipment. Recycling helps to reduce the consumption of raw materials, thus protecting the environment.

