

User Manual

M2M Industrial Router 2 SECURE



Rev: 1.00

2023-02-09



Document specifications

This document was completed for the **M2M Industrial Router 2 SECURE®** device and contains the hardware specification, with the most important information and software settings of the device.

Document category:	User Manual
Document subject:	M2M Industrial Router 2 SECURE®
Author:	WM Systems LLc
Document version No.:	REV 1.00
Number of pages:	27
Hardware Identifier No.:	BE0109D_ROUTER_9X60_7070_AXP
Firmware version:	202302061 or later
OpenWRT Linux Kernel version:	5.10.154
Document status:	Final
Last modified:	9 February, 2023
Approval date:	9 February, 2023



Table of contents

CHAPTER 1. Product information	5
CHAPTER 2. Technical data.....	6
2.1 Power voltage / Current ratings	6
2.2 Cellular modules (order options)	6
CHAPTER 3. Device exterior design and appearance	8
3.1 Safety cautions	9
3.2 Mounting, fastening	11
3.3 Antenna.....	12
3.4 Further accessories.....	12
CHAPTER 4. Software system.....	14
4.1 Operation system.....	14
4.2 LAN block feature	14
4.3 Device Manager platform.....	14
4.4 TLS protocol communication.....	15
4.5 Accessing the router (via SSH connection)	15
CHAPTER 5. Starting the device	16
5.1 Connecting the router	16
5.2 First start.....	17
5.3 Access via SSH connection	18
CHAPTER 6. Important notes.....	20
CHAPTER 7. Troubleshooting	21
CHAPTER 8. Support availability.....	26
8.1 Contact the support line	26
8.2 Product support.....	26
CHAPTER 9. Legal notice.....	27



Chapter 1. Product information

This secure and robust device features an Ethernet port, cellular module, and compact industrial design. It is currently available with LTE Cat.1 or LTE Cat.M/Cat.NB modules that provide enhanced coverage.

This product boasts special firmware that offers additional security features as required by the ENCS, the European Network for Cyber Security.

To meet ENCS standards, the device has been completely redesigned to enhance security. As a result, it has successfully passed all tests and offers improved processing speed with an eMMC chip for secure boot and encrypted data storage.

This device is designed for use in various smart grid and industrial M2M / IoT applications, including Automated Metering Infrastructure (AMI) and industrial automation projects. It is a preferred choice for securing critical smart grid infrastructure for some of the largest European utilities. The device offers all features required for the world of smart metering, smart grid, and industrial automation.

Ports / Interfaces

The device offers the following ports: Ethernet, and micro-USB port (for configuration).

System Software

The operating system is open-source OpenWRT® and the device is manageable through our state-of-the-art Device Manager® platform via TLS-secured communication. The solution enables clients to perform OTA firmware updates and mass deployments quickly and efficiently.

Secure storage / Secure Boot

The device has a built-in eMMC chip (4 or 8 GByte storage – by order option) for Secure Boot process / encrypted storage of all customer data. It uses an OTP-enabled memory chip.

The device is secured with Secure Boot system and secure storage mechanism. It uses an SHA-256 encrypted file system (with RSA and SHA-256 assignments).

The device operates with multiple encrypted partitions and file systems, which ensures the security of the device.



Security features

The device uses Secure Boot system with Secure Key Storage features (on encrypted eMMC memory chip).

The router continuously monitoring the operation parameters (QoS, module operation, vital signals, etc.).

It has detection of network interface connections / disconnections with an alarm event sending to the Device Manager® management platform.

The software of the router applies unique passwords, firewall and it has support for IPSec tunneling.

Management

Remote management of routers using Device Manager® software via a secure TLS v1.2 connection (by option) during the communication with the router.

The device has a secure Device Manager® connection (TLS protocol connection between the router and the remote management software.)

The router allows clients to do OTA firmware updates and mass deployments significantly faster via Device Manager® platform.

Last GASP – notification of power outage

The device has built-in supercapacitor parts with LastGASP feature (in case of a power outage, the router is operating further, while an immediate notification will be sent from the event to the Device Manager® software).



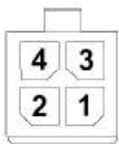
Chapter 2. Technical data

2.1 Power voltage / Current ratings

- **Power Voltage / Ratings:** • 12V DC, 1A power supply (9-32VDC) – powered via Microfit 4-pins power input connection (from external 12V DC power adapter)
- **Current / Consumption:** Average: 200mA - 260mA, 12VDC (according to module version) / 2.4W – 3.1W, 12VDC

For the connection it is recommended to use the DC microfit connection power adapter or a 12V DC supply according to the pinout which can be seen on the next figure.

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

Pin number	Name	Functions
3	POWER -	DC power negative input
4	POWER+	DC power positive input

2.2 Cellular modules (order options)

- **LTE Cat.1 / 450 MHz module with 2G „fallback”**

Module:

- SIMCOM A7676E

Bands:

- LTE Cat.1 / 450MHz: B1/B3/B8/B20/B31/B72
- GSM/EGPRS: 900/1800MHz

- **LTE Cat.M / Cat.NB / 450 MHz module with 2G „fallback”**

Module:

- SIMCOM SIM 7070E



Bands:

- LTE Cat.M / 450MHz:
1/B2/B3/B4/B5/B8/B12/B13/B14/B18/B19/B20/B25/B26/B27/B28/
B31/B66/B72/B85
- LTE Cat.NB: B1/B2/B3/B4/B5/B8/B12/B13/B18/B19/B20/B25/B26/B28/B31/
B66/B85
- GSM/EGPRS: 850/900/1800/1900MHz



Chapter 3. Device exterior design and appearance



*Industrial secure router, assembled in aluminum casing
with interface connectors / ports*

- 1 – POWER (9-32V DC): Microfit 4-pin power connector (for DC power/adapter)
- 2 – *SIM card slot (2FF)
- 3 – micro-USB connector (for configuration)
- 4 – Reset button (hole)
- 5 – Ethernet (RJ45, 10/100 Mbit)
- 6 – Antenna connector (SMA-M, 50 Ohm)
- 7 – 3 Operation LEDs

** SIM insertion: push the APN-activated SIM into the SIM tray (2) - the SIM chip surface must be look to top and the cutted edge of the SIM must be look to the router – then push the SIM until it will be fixed and closed (you will hear a soft click sound).*



*Industrial secure router, assembled in aluminum casing,
attachable to 35mm DIN rail(with an adapter)*

3.1 Safety cautions

The device must be used and operated according to the user manual provided.

Only a responsible and skilled person with adequate experience and knowledge in wiring and installing a router device, as instructed by the service team, should carry out the installation.

It is forbidden for the user to touch or alter the wiring or installation. The device enclosure should not be opened during operation or when connected to power, and the device PCB should not be removed or modified. No modification or repair should



be made without the manufacturer's permission, as this will result in the loss of product warranty.

CAUTION! Only certified experts or the manufacturer are authorized to open the device enclosure.

The device uses 9-32V DC power supply within the enclosure, and the enclosure should NOT be opened or the PCB touched.

Router current and consumption

- Power voltage: 9..32 VDC
- Current average: 200mA, 12V DC
- Consumption: 1.9W (during 2G/3G communication), 3.1W (during LTE or Cat.1 / LTE Cat.M communication)

The IP51 immunity protection will only be effective if the device is used under normal conditions and with undamaged hardware in the provided enclosure / chassis.

Any deliberate damage or malfunction of the device will result in the loss of product warranty.

To ensure safety, the following guidelines should be followed:

- Keep the chassis area clean and free of dust during and after installation.
- Wear appropriate clothing to avoid loose clothing getting caught in the chassis.
- Avoid actions that could cause a hazard to people or equipment.

Safety precautions for Electricity

- Read all safety warnings before working on equipment powered by electricity.
- Locate the emergency power-off switch for quick access in case of an electrical accident.
- Disconnect all power before installing or removing a chassis, working near power supplies, or inserting a SIM card.



- Look for potential hazards in your work area, such as moist floors, ungrounded power cables, frayed cords, and missing safety grounds.
- Never work alone if hazardous conditions exist.
- Always verify that power is disconnected from a circuit before working on it.
- Do not open the internal power supply enclosure of the router.
- In case of an electrical accident, follow these steps:
 - Use caution to avoid becoming a victim.
 - Turn off power to the device.
 - If possible, send someone for medical aid. If not, assess the victim's condition and call for help.
 - Determine if rescue breathing or external cardiac compressions are needed, and take appropriate action.

Preventing Electrostatic Discharge Damage

- Electrostatic discharge (ESD) can cause damage to equipment and impair electrical circuitry.
- Always follow ESD prevention procedures when removing and replacing modules:
 - Ensure that the router chassis is grounded.
 - Wear an ESD-preventive wrist strap and connect it to an unpainted surface of the chassis frame to safely channel ESD voltages to ground.
 - If a wrist strap is not available, ground yourself by touching a metal part of the chassis.

3.2 Mounting, fastening

The device's bopla aluminum enclosure can be fixed to a DIN-rail using the optional AB800MKL fixation part, or mounted to a wall, placed in a server rack, or fixed in a similar manner.





The device enclosure can be mounted using either the AB-MKL one-sided DIN-rail adapter (left) or the AB800MKL adapter (right) on a wall or DIN-rail.

These accessories can be ordered - more information:

<https://m2mserver.com/en/product/din-rail-mount-unit-two-sided/>

<https://m2mserver.com/en/product/din-rail-mount-unit-one-sided/>

3.3 Antenna

Please be aware that the presence of metal parts in close proximity, the metal material of the cabinet, and industrial conditions such as the use of high power levels or exposure to external radio frequency signals can cause radio interference and result in weak wireless signals during transmission or reception, as well as reduced signal quality. In these cases, we recommend testing the wireless signal reception and quality. If necessary, you can improve reception by using an external magnetic mount antenna that is mounted outside of the cabinet and placed on its surface.



3.4 Further accessories

The following accessories are not part of the product, these are order options.



Microfit power cable:

Type: min. 70 cm, OMYA type, 2 x 1 mm², halogen free, double insulated wires, min. 24 V DC voltage, wires are marked by colors and blanked.

Connector type: 4-pins Microfit (2-pins are wired)

Feature: to provide 9..32V DC power supply connecting for the router (12V DC 1A).

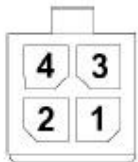
For the wiring and assuring the power supply you should take note to the following figure.



More information:

<https://m2mserver.com/en/product/microfit-psu-cable/>

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

Pin number	Name	Functions
3	POWER -	DC power negative input
4	POWER+	DC power positive input

DC power adapter:

Connector: 4-pins microfit

Function: 12V DC 1A power voltage for the router

More information:

<https://m2mserver.com/en/product/universal-power-supply-12v-1a/>

UTP (Ethernet) cable:

Type: Cat5e UTP PVC

Connector: RJ45



Chapter 4. Software system

4.1 Operation system

The device runs on OpenWRT® system with a micro Linux microkernel. The secure boot system is integrated into the hardware-level eMMC secure chip and partitions are encrypted by secure boot.

The router comes with a pre-installed system, which is tailored to the customer's requirements and includes the operating system, software, and a factory default configuration. The device uses Linux-based and UCI commands at the command line, which can be accessed through SSHv2 connection.

4.2 LAN block feature

If the Ethernet (LAN) cable is disconnected from the router or the device it's connected to, the router will notify of the event and the LAN controller will be stopped for security reasons. This can occur at the router or the connected device. The LAN controller can be re-enabled from the Device Manager®.

To block the LAN interface, go to the Device Manager software, access the **Device config** tab, and allow it in the router's configuration. If the Ethernet removal event occurs, it will be signaled in the Device Manager and the LAN controller will be disabled, stopping LAN traffic immediately. After restarting the device, the router will still not be able to communicate on the LAN interface until you allow usage again from the Device Manager® platform.

4.3 Device Manager platform

The Device Manager® software can be used for the remote management of the routers. The application allows for remote maintenance and reconfiguration of the routers, as well as continuous monitoring of operating characteristics such as network access, field strength, runtime, and QoS.

You can also replace and install firmware on the device and manage thousands of routers from this program, allowing for remote control and execution of tasks on the device. In the Device Manager software, individual or group settings can be made. Legacy or TLS communication can also be allowed in the Device Manager software during the M2M Industrial Router 2's communication.



4.4 TLS protocol communication

TLS v1.2 protocol communication can be activated between the router and the Device Manager® from the software side, by choosing TLS mode or legacy communication. The router uses the mbedTLS library and the Device Manager uses the OpenSSL library. The encrypted communication is double encrypted using a TLS socket for added security.

The TLS solution uses mutual authentication to identify the two parties involved in communication. Both sides have a private-public key pair, with the private key visible only to the DM and router, and the public key in the form of a certificate. The router firmware includes a factory default key and certificate, and until a custom certificate from the DM is received, the router will authenticate itself with the embedded certificate. The router only implements factory default, so any TLS connection can be established with any certificate, including self-signed, as long as the encryption inside TLS is known. Access requires knowledge of the encryption and a successful self-authentication with the root password.

4.5 Accessing the router (via SSH connection)

The router can be accessed via an ssh connection, either remotely through the cellular network (LTE Cat.1, Cat.M or Cat.NB) within the IP address range of the SIM card on the WAN interface or via the local Ethernet interface (LAN). Access is protected with RSA2 key.



Chapter 5. Starting the device

5.1 Connecting the router

1. Ensure that the router is not under power voltage, therefore the power adapter cable is removed from the **POWER** titled microfit connector (1) – or the adapter is not connecting to the power network. Ensure, that all the 3 LEDs (7) are blank.
2. **Mount** a proper **LTE antenna** to the left **SMA connector** (6).



3. **Insert an activated SIM card** to the SIM slot (2) - the SIM chip surface must be look to top and the cutted edge of the SIM must be look to the router – then push the SIM until it will be fixed and closed (you will hear a soft click sound). (In case of necessary of SIM removal you have to power off the router and push the SIM a bit, while it will be released and can be removed).
4. **Connect an UTP cable** to the router's **Ethernet** titled RJ45 port (6). During the configuration the cable's opposite connector must be connected to the PC's Ethernet port. (After the configuration connect it to the network- or industrial device's RJ45 port.)
5. You can also configure the router through the **micro-USB slot** (4) by a microUSB-USB cable of the PC connection.

5.2 First start

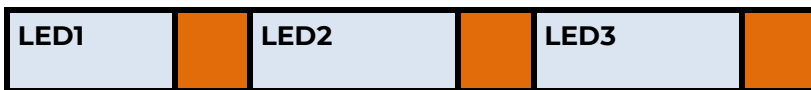
The router is provided with pre-installed system (which contains the operating firmware and a Linux-based command line with UCI command line interface).

The router is accessible via ssh connection.

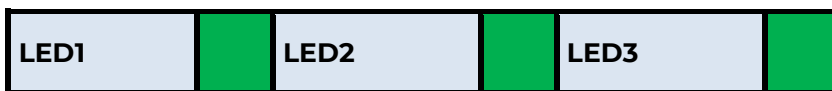
1. Connect the *microfit* connection **power connector** (1) when the router begins its operation, where the LED lights will be signing and inform you about the current status of the device.

9-32V DC power voltage input (interface nr. 1) should be used by the DC powering with the microfit connection 12V DC power adapter, or you can use alternatively 9-32V DC power voltage with own cabling (follow the pinout hints).

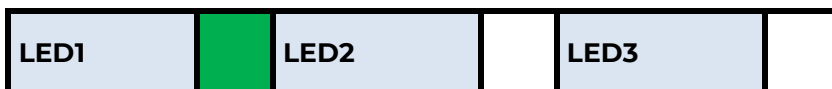
2. **After long time off, when powering the device on**, all 3 LEDs will active with **red** / **orange** color for a few seconds. this means that the charging of the supercapacitor has began.



Normally, in case of rebooting, the supercapacitors are already charged, therefore **LEDs** will be active with **green**.



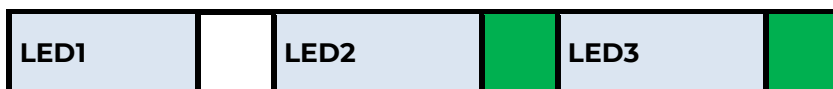
3. Then the **LED1** light is lighting continously by **green**, which signs that the system is during loading (boot progress).



4. The system start requires about 1-2 minutes, while the device loads the necessary modules or the operation and prepares the login command line user interface – the **LED2** will sign it. Then you can log in.



5. **Configure the device's wireless internet module settings** (SIM and APN) **for the cellular internet connection** – otherwise the router will be restarting in ever 10 minutes.
6. The module registration to the cellular network is signed by the **LED3** flashing after the settings. If it was succesful (to register the SIM card data to the network) then the **LED2** will lighting, which shows that the router can access the cellular network already.



7. If you notice an unusual LED sign or other operation misbehaviour symphthoms, read the **Troubleshooting** chapter.
8. If you'd like to make the router settings via USB connection (micro-USB port) then install the **USB Ethernet / RNDIS Gadget** driver to your computer by using your web browser: https://m2mserver.com/m2m-downloads/RNDIS_win10.ZIP

5.3 Connect to the router

1. To connect to the router, allow the router IP address for the Ethernet connector interface in the Windows®'s network settings (IP address for Ethernet connection: 192.168.127.100, Subnet mask: 255.255.255.0)
2. In case of USB connection, you have to setup the **USB Ethernet / RNDIS Gadget** virtual interface to the following IP: 192.168.10.100, subnet mask: 255.255.255.0
3. By default, the **Ethernet** port's IP address is **19.168.127.1**
The **USB** connection the IP address of the router is **192.168.10.1**
4. Connect via SSHv2 to the router (e.g. **192.168.127.1:22**. Then the router's local command line interface will appear where you can login.

5. **Accept** the security risk (RSA token) encryption key usage warning notice (visible at first time only).

Login information

■ **Username:** *root*

■ **Password:** *wmrpwd*

At the Linux command line you can use standard Uc Linux kernel 5.10 compatible commands and execute scripts on the device.

You can also use **UCI command line interface** commands here. The UCI® (Unified Configuration Interface) is an OpenWrt® API utility that allows centralized configuration and management of the OpenWrt® operation system, configuration of the router.

To review the UCI commands and options that can be used, we recommend to read UCI Reference Guide, which can be downloaded from our website.

https://m2mserver.com/m2m-downloads/UCI_Command_Line_Reference_v3.pdf

E.g. you can make a query to ask the current setting of a service (openvpn, ser2net, ddns, etc. by using the following command from command line):

```
#uci show service_name
```

You can also having the option to make detailed settings of a service by using the UCI interface.



Chapter 6. Important notes

- For security reasons, we do recommend to **change the password** immediately for accessing the administration user interface.
- The parameters that can be used for the APN settings are always provided by the SIM card issuer (mobile service provider). Contact them for **APN**, SIM **PIN**, **PAP/CHAP username** **username**, **PAP/CHAP password** and other information.
- The router constantly checks the interfaces and the viability of the connections. In the event of a power failure or power failure, the network and data connections are automatically reconnected after the conditions are restored.



Chapter 7. Troubleshooting

LED activity

Can you see any LED activity (flashing, lighting)?

After ca. 2 minutes inactivity of the LEDs could mean the router has a failure (configuration or firmware trouble).

First you should ensure about the router is still under starting / booting phase or not.

Please wait 2-3 minutes, then check the LED signals again. If the **LED1..LED2..LED3** are blank, then the device hasn't got its power supply or it has some trouble.

Connect the power source and if it does not helps, ask our support, please.

In case of LED blinking after restart

After ca. 2 minutes of the router start the **LED1** will be blank and the **LED3** starts to flashing by **green**. This signs that the router begins try to connect to the cellular network (logins to the APN and builds the connection).

After 1 or 2 minutes, the **LED2** must be lighting continuously, which signs the successful modem network connection and the available ppp (**WAN**) connection.

(in case of 4G version the **LED2** does not lighting here.)

The device is communicating on the network and will send a couple of minutes later proper *RSSI* values and life signals. Meanwhile the **LED1** will flashing once in every 10 seconds - which means it is operating properly.

Power source

Check that the router can get any power through its microfit connector (**POWER**) – power adapter is connected to the router microfit connector and the adapter to the 230V AC plug.

When it receives 12V DC power, the LED signals will sign it: *all the three LEDs will light for a short period*, then the **LED1 (green)** will lighting for 2 or 3 minutes, then after that only blinks once in every 10 seconds. The router is booting and just started.

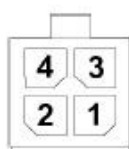
(Wait for 1-2 minutes, while the router is registering to the wireless network then check the life signals in Device Manager®).



In case of failure, check the power supply connection at the socket plug side and on the microfit connector at the router side. The top 2-pins of the microfit plugin are wired only, the left pin is the negative.

Check the next figure for the pinout and check the 12V DC voltage on the microfit connector (by a multimeter) of the power adapter that it provides 12V or not. If not, than remove the 12V DC adapter and get another one with the proper pinout and voltage.

4-PIN connector (Power Input)



Pin assignment of 4-pin connector

Pin number	Name	Functions
3	POWER -	DC power negative input
4	POWER+	DC power positive input

Connecting to the router, checking connection

Set the IP address of the **Ethernet interface** on the PC where it can be reached (in the Microsoft Windows®: **Control panel / Network / Network Adapter / Adapter settings**). Ping the router IP address.

If you can connect, you can ping an IP address out of the OpenWrt interface to check network access on the mobile Internet.

Ethernet connection

Check or connect the RJ45 UTP6a type cable to the **ETHERNET** port. When the router is operating, the **Ethernet** port LEDs must sign the network activities. If you do not have an Ethernet cable connection, you can use a micro USB connection for the bridge connection to access the router.

When you cannot access router through SSH

Download the micro-USB cable **driver** from here:

http://www.wmsystems.hu/m2m-downloads/USB_Ethernet_RNDIS_DRIVER.zip

Unzip the downloaded zip file into a directory and install.



Establish a USB connection between the PC and the router with a micro-USB cable connected to the socket marked **USB**. (The driver must be installed on the PC according to the **Installation Guide**).

Set the IP address of the **USB-Ethernet interface** on the PC for the “**USB Ethernet / RNDIS Gadget**” network connection (**Control Panel / Network / Network Adapter / Adapter Settings**). You can also voltage the device on the **USB** connection at the IP address.

Enable the access to the router's IP address in the browser (from the computer on the USB network interface it should always appear as **192.168.10.10** IP address, Subnet mask: 255.255.255.0 - this is set in **Control Panel / Network and Sharing Center / Adapter Settings / Under Network Connections**, to the **USB Ethernet / RNDIS Gadget Interface**.)

If the router is not starting

It is possible that there is no uploaded software available on the router. Ask our support line!

Periodic restart of the router (by 10 minutes periods)

When router was not be configured properly for the ppp/wan connection or the modem was not started then the router will be restarted within in 10 minutes.

You can also configure the periodic ping interval from the LuCi / OpenWrt.

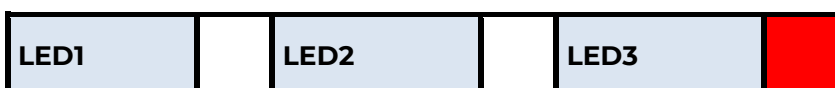
Restart of the router

Restart the router by pushing its **Reset** button on its interface / port side. Push this button for 10 seconds, by a sharp and thin object. Then the router will be restarted.

Shutdown / halt the router

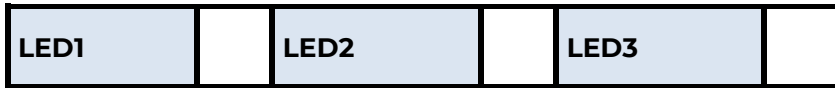
Pull out the power connector from the 230V AC electricity plug.

Then the **LED3** will be lighting by **red** color.



Note, that the router will not powered off immediately, due to it have supercapacitor components inside. Therefore, the router will getting enough spare power (ca. for up to 10 seconds) to close every connection, interfaces and ports and shutdown the device safely.

When the **LED3** will be blank, then the router was turned off and its not under power further.



Antenna

Use the proper antenna type regarding the used cellular module and mobile network.

Connect the SMA antenna properly to the antenna connector by mounting to the antenna interface.



In case of using LTE 4G or Cat.M, Cat.NB

(Narrow Band) networks – always use the proper antenna which is harmonizing to the frequency/band. In other way the router will not abble to access the cellular network.

SIM/APN failure

It means a SIM or APN failure, if the **LED2** will not light for minutes.

If the device is not registering to the network, then the modem was not initiated properly, and the router will restart itself after 10 minutes. This could caused by a not proper APN setting.

Check with your mobile service provider that issues your SIM card for the APN names and passwords you are using.

After turning off the router, insert a working SIM properly, start the router, configure the APN and SIM settings on the router.

If the problem persists, contact your mobile service provider for the SIM card and the APN settings that you can use.

SIM card cannot be detected

Turn off the router - unplug the power plug from the **POWER** connector of the device. Then, make sure that there is a SIM card in the **SIM** slot with the chip facing up and the bevelled corner facing inward, and then push the card in until it stops. Check with your mobile service provider that the SIM card is active and ready to use data packet (IP communication).

Restart the router by reconnecting the power connector.



Chapter 8. Support availability

If you have any questions concerning the use of the device, contact us at the following address:

E-mail: support@wmsystems.hu

Phone: +36 20 333 1111

8.1 Contact the support line

For the proper identification of the router you should use the sticker on the device, which contains important information for the call center.

Attach the OpenWrt related important information – marked - of modem identifiers to the problem ticket, which will help resolving the problem! Thank you!

8.2 Product support

Documentation and released firmware for the product can be accessed via the following link.

<https://m2mserver.com/en/product/m2m-industrial-router-2-secure/>

Online product support can be required here:

<https://www.m2mserver.com/en/support/>



Chapter 9. Legal notice

©2023. WM Systems LLC.

The content of this documentation (all information, pictures, tests, descriptions, guides, logos) is under copyright protection. Copying, using, distributing and publishing it is only permitted with the consent of WM Systems LLC., with clear indication of the source.

The pictures in the user guide are only for illustration purposes.

WM Systems LLC. does not acknowledge or accept responsibility for any mistakes in the information contained in the user guide.

The published information in this document is subject to *change without notice*.

All data contained in the user guide is for information purposes only. For further information, please, contact our colleagues.

Warning

Any errors occurring during the program update process may result in failure of the device.

