mbEDGE

Instructions for use

1.0 DR02 - EDG100 | July 10th, 2020

Table of Contents

1   Legal information

Qualified Personnel

This document is intended for software / web programmers and developers and requires good knowledge of the following products / systems:

- mbNET / mbNET.rokey
- Remote-Service-Portal mbCONNECT24
- Node-Red
- Programming and debugging Docker & Container applications
  (only in conjunction with an mbEDGE.advance license)

Proper use

The product / system associated with this documentation may only be used as described in this document.

License notice

The serial number of an mbEDGE card is linked to a license. The serial number / license may only be used in parallel in one device.

An mbEDGE card that has already been used can be transferred to another device.
See chapter "If you want to use the mbEDGE card in another mbNET".

Disclaimer

In this manual all technical information, data and instructions for installation, operation and maintenance are based on our previous experience and insights to the best knowledge and state of the art. For the details, illustrations and descriptions in these instructions, no claims can be deduced. We assume no liability for damage and / or data loss due to:

- Disregard of these operating instructions
- Improper use
- Technical modifications

Subject to technical and content changes.

Trademarks

The use of any trademark not listed herein is not an indication that it is freely available for use.

2   Use of open source software

General

Our products include, among other things, open source software, which is manufactured by a third party and has been published for free use by anyone. The open-source software is available under special open-source software licences and copyright of third parties. In principle, each customer can use open source software free of charge under the licence terms of the respective manufacturers. The customer's right to use the open source software for purposes other than those for which our products were intended is regulated in detail by the relevant open source software licences. The customer may freely use the open source software as set out in the respective valid licence, beyond the intended purpose of the open source software in our products. In the event that there is a contradiction between the licensing terms of one of our products and the respective open source software licence, the respective applicable open source software licence shall take priority over our licensing terms if the respective open source software is affected by this.

Use of the open source software is free of charge. We do not charge any usage fees or similar charges for the use of open source software included in our products. Customer use of open source software in our products is not part of the profit that we obtain from the contractual remuneration. All open source software programs contained in our products are in the available list. The most important open source software licenses are listed in the Licences section at the end of this publication.

If programs that are included in our products are under the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT), or other open source software license, which requires that the source code be made available, and this software was not already supplied with our product on a disk or in the source code, we will send this at any time upon request. If we are required to send this on a disk, there will be a flat rate charge of €35.00. Our offer to send the source code upon request, shall automatically end 3 years after delivery of the respective product to the customer.

Requests must, where possible, be sent to the following address with the product's serial number:
MB connect line GmbH Fernwartungssysteme · Winnettener Str. 6 · 91550 Dinkelsbühl GERMANY
Tel. +49 (0) 98 51/58 25 29 0 · Fax +49 (0) 98 51/58 25 29 99 · info@mbconnectline.com

Special liability provisions

We assume no responsibility or liability if the open-source software programs included in our products are used by customers in a manner that no longer corresponds to the purpose of the contract which serves as the basis for the purchase of our products. This applies in particular to any use of the open source software programs outside of our products. The warranty and liability provisions, which stipulate the applicable open source software license for the corresponding open source software, as listed below, apply to the use of open-source software beyond the contractual purpose. In particular, we are also not liable if the open source software in our products or the entire software configuration in our products is changed. The warranty contained in the contract, which forms the basis for the purchase of our products, applies only to unchanged open source software and the unchanged software configuration in our products.

Open source software used

For a list of the open source software used in our products, visit https://www.mbconnectline.com/downloads/open-source-software-licenses.txt.

3   General

Purpose of this documentation

This manual describes the use of the *mbEDGE* software toolkit.
Please read carefully and retain this information.

Target group

This document is intended for software / web programmers and developers and requires good knowledge of the following products / systems:

- mbNET / mbNET.rokey

- Remote-Service-Portal mbCONNECT24

- Node-Red

- Programming and debugging Docker & Container applications
  (only in conjunction with an mbEDGE.advance license)

Validity of this documentation

This manual is valid for mbEDGE.start (EDG 100) and mbEDGE.advanced (EDG 200).

Prerequisites / additional required components

Access to the mbEDGE functions is only possible with one of the following devices:

- Industrial router *mbNET* the 8xx series (MDH 810 - MDH 859) - from firmware version **6.0.6** and hardware version **HW 03**

- Industrial router *mbNET.rokey* (RKH210, RKH216, RKH235, RKH259)

- Cloud Gateway *mbXLINK* (XLH 100, XLH 110, XLH 120, XLH 130)

Release notes

Version	Date	Comment
V 1.0	Mar. 6th, 2019	Start version
V 1.0 DR01	May 20th, 2020	Chapter **Brief Description / Features**: - Information on free use of open source software. - Supplement to the list of pre-installed nodes.
V 1.0 DR02	July 10th, 2020	License notice in chapter "Legal information"

4   Scope of delivery

The delivery of mbEDGE takes place in the form of an SD card in a so-called DigiPack.

On the back of the packaging you will find all data for identifying your mbEDGE version.

- Designation
- Type
- Serial number
- Item number
- License code

Keep this information in a safe place!

Without the license code, you **can not** create a user backup key.

You need the user backup key if you want to use the mbEDGE card in another mbNET.

If one of these parts is missing or damaged when unpacking, please contact the following address:

MB connect line GmbH
Winnettener Str. 6
D-91550 Dinkelsbühl
GERMANY
Tel.: +49 (0)9851/282529-0
Fax: +49 (0)9851/282529-99

mbEDGE

5   Brief Description / Features

mbEDGE.start is a software kit that extends the industrial routers **mbNET** (from hardware version HW03 and firmware version from 6.0.6) and **mbNET.rokey** to an edge gateway.
Additional data collection and processing capabilities allow you to make your remote installations more versatile and flexible.
mbEDGE.start is based on recognized and proven standards such as docker / container technology and the **Node-RED** graphical development environment.
mbEDGE.start provides interfaces to different clouds and communication protocols such as OPC-UA and MQTT.

mbEDGE.start
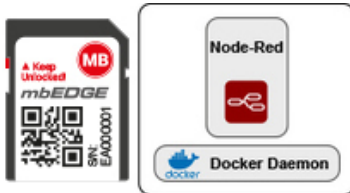
• **Read out and save PLC data**

• **Distributing the data to other media on the Internet**

• **Node-RED for easy programming**

  ○ Web-based programming user interface with Drag&Drop

  ○ Industrial protocols: MQTT, OPC-UA, Modbus, S7 and many more

  ○ Cloud-connectivity: Azure, IBM, Amazon and more

  ○ TCP/IP, HTTPs, E-Mail, Twitter and more

  ○ User-defined function blocks

  ○ **mbCONNECT24** node to connect with dashboards & widgets

• **Pre-installed Docker Engine**

Data stored on the SD card are encrypted (aes-xts-plain64:sha256):

- Encryption method: AES
- Encryption Mode: XTS-plain64
- Hash function: SHA256

8 GB industrial grade SD card (MLC NAND, UHS-I interface)

- Temperature (usage): -40 to 85°C
- Dimensions: 24mm x 32mm x 2,1mm
- 90 MB/s read and 20 MB/s write speed

NOTICE

Node-RED, Docker and Portainer.io are pre-installed open source applications. Use of the open source software is free of charge. We do not charge any usage fees or similar charges for the use of open source software included in our products. Customer use of open source software in our products is not part of the profit that we obtain from the contractual remuneration.

The following nodes are additionally available for the standard nodes in the Node-Red Edition mbEDGE.start:

Node-Red version 0.19.0 based on NodeJS 8.0

- node-red-contrib-azure-iot-hub
- node-red-contrib-aws
- node-red-contrib-scx-ibmiotapp
- node-red-contrib-ibm-watson-iot
- node-red-contrib-cumulocity
- node-red-contrib-aggregator
- node-red-contrib-ftp-sftp
- node-red-contrib-modbustcp
- node-red-contrib-s7
- node-red-contrib-iiot-opcua
- node-red-node-twitter
- node-red-node-email
- node-red-dashboard
- node-red-contrib-boolean-logic
- node-red-contrib-cloud
- node-red-contrib-device
- node-red-contrib-fieldbus
- node-red-contrib-mqtt-broker
- node-red-node-base64
- node-red-node-feedparser
- node-red-node-msgpack
- node-red-node-random
- node-red-node-rbe
- node-red-node-suncalc

Further information such as application examples, FAQs, videos and product information about **mbEDGE** can be found in our Helpdesk at www.mbconnectline.com

mbEDGE

6   Notes on handling the SD card

- All partitions on the SD card are encrypted (aes-xts-plain64:sha256):

  - Encryption method: AES

  - Encryption Mode: XTS-plain64

  - Hash function: SHA256

- The mbEDGE SD card is always bound to only one device - device card pairing.

- A card already paired with one device (mbNET) can not be used simultaneously in another device.

NOTICE

If the mbEDGE function has been activated on mbNET, the mbNET automatically detects the mbEDGE variant as soon as the device is ready for use and the SD card has been inserted.

Make sure the SD card is always unlocked.

NOTICE

Never remove the SD card from the device while the device is switched on and ready for use.

Otherwise, data on the SD card may be damaged or the device may not work.

To safely remove the SD card from the device, first turn off the device and then remove the SD card from the slot.

Further information for the use of mbEDGE

Further information such as application examples, FAQs, videos and product information about *mbEDGE* can be found in our Helpdesk at www.mbconnectline.com

7   If you are using mbEDGE for the first time in an mbNET

First of all, you must enable the mbEDGE functionality on the mbNET with which you want to operate mbEDGE. Otherwise, the mbEDGE card will not be recognized.

Please refer "Enable the mbEDGE functionality on the mbNET"

The mbEDGE card is split into an **Application folder** and a **User folder**. Both folders are grouped together in an encrypted container, so the information on the card is secure.
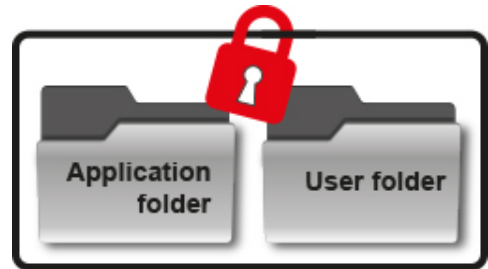
To decrypt the container (open and readable / writeable) are on the SD card three key memory.

Keystore setting at factory setting
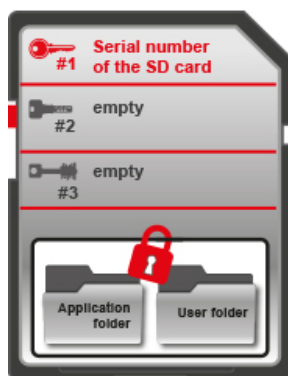
Keystore #	Setting on delivery
# 1	Initial key (Serial number * of the SD card)
# 2	empty
# 3	empty

* The serial number is no secret (it is on the back of the SD card). Thus, key memory # 1 can be opened at any time and described for initialization.
In the delivery (factory setting) of mbEDGE no sensitive data on the card are stored.

After you have inserted the mbEDGE card into the mbNET and the mbEDGE function has been activated, the card will be detected automatically.
The mbNET reads from the general SD card information, the serial number of the mbEDGE card (key memory # 1) and thus opens the container.
If keystores # 2 and # 3 are empty, the mbNET Secure Element generates a unique key. This key is written to the key store # 2.
At the same time, the content is deleted from keystore # 1.
From now on, only this mbNET can open the encrypted folder and read / write data (mbEDGE device pairing).
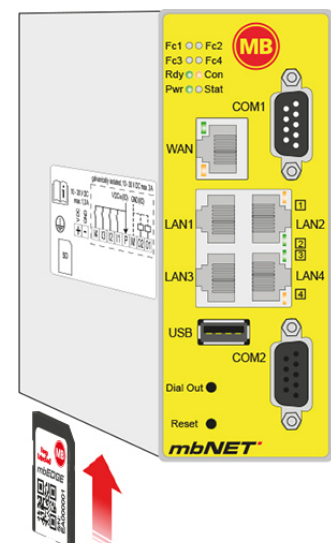
Keystore setting after mbEDGE device pairing
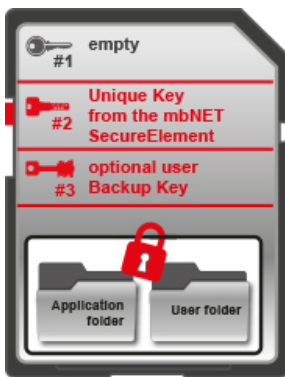
	Keystore #	State after mbEDGE devices pairing
	# 1	empty
	# 2	unique key from mb- NET Secure Element
	# 3	optional user Backup Key **

** The user backup key is required if you want to use the mbEDGE card in another mbNET
after mbEDGE device pairing.
Please refer "If you want to use the mbEDGE card in another mbNET"

NOTICE

Immediately after initializing the mbEDGE card, assign a user backup key to avoid data loss!
Please refer "Generate user backup key"

---

8   Enable the mbEDGE functionality on the mbNET

NOTICE

The mbEDGE functionality is **disabled** by default on mbNET.

Access to the mbEDGE functions is only possible with one of the following devices:

- Industrial router *mbNET* the 8xx series (MDH 810 - MDH 859) - from firmware version **6.0.6** and hardware version **HW 03**

- Industrial router *mbNET.rokey* (RKH210, RKH216, RKH235, RKH259)

- Cloud Gateway *mbXLINK* (XLH 100, XLH 110, XLH 120, XLH 130)

8.1   Activation via mbCONNECT24

NOTICE

The following steps for activating the mbEDGE functionality refer to the "Extended" view in your mbCONNECT24 user account.

View: Simple| **Extended**
mbCONNECT24 - V2.4.0 · 00000 · 25.02.2019 08:34 (UTC +01:00)
powered by mbconnectline

▶   Select the relevant device (mbNET / mbXLINK) from the device list or add a new device to your project.

▶   In the device settings (**Navigation**: Administration > Projects > *ProjectAlpha (selected project)* > *RouterAlpha (selected device)* > Interfaces) you will find the additional menu item "**IoT**"

▶   Click the edit icon to enable the IoT services.

Additionally, enable the "Docker management" if you have purchased an mbEDGE.advanced license and want to install additional Docker containers.

▶ Click "**IoT**" to make the following settings:
The settings in this menu are not mandatory for activation of mbEDGE.

- ° Create and edit **Tags** for the data exchange between mbCONNECT24 and Node-RED.

- ° Create and edit **Device User**s to access Node-Red. By default, the user admin is already created. admin is the default device user. The corresponding password is the default device password (default password) or the password that you have assigned in mbCONENCT24 for the user admin.

- ° Under **Network**, the IP address of the Docker Daemon (Runtimer for the IoT services and Nod-Red) is displayed.
  Default is 172.16.0.1/24.
  Adjust the IP address if an address conflict with other network settings is / can be expected.

- ° Here, you add Firewall Rules to open ports for Node-RED. By default, a network socket node in Node-RED has access only from the inside out. Therefore, any "listener socket" created in Node-RED is not accessible via LAN / WAN.
  For example, an OPC UA server can not be reached via LAN / WAN. Unless you release the OPC-UA server port here in a firewall rule. Enter the port number(s) and select the protocol (UDP or TCP).
  Multiple entries of port numbers must be separated by commas.

NOTICE

If you have not already done so, insert the mbEDGE SD card into the SD card slot of the mbNET.

▶ Now transfer the configuration to the mbNET.

NOTICE

The entire activation process of mbEDGE can take up to seven minutes.

During the activation phase, the LED Fc4 of the mbNET flashes green at a frequency of 3 Hz (fast), after completion of activation at a frequency of 1.5 Hz (slow).
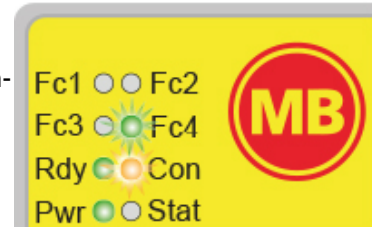
Once the mbNET is online and activation is complete, the IoT menu will show you whether your flows and dashboards are available through Web2go.

Further information such as application examples, FAQs, videos and product information about *mbEDGE* can be found in our Helpdesk at www.mbconnectline.com

mbEDGE

8.2 Activation via the mbNET web interface

NOTICE

Activate directly via the mbNET web interface **only** if you use the mbNET as a classic router without the use of the Remote Service Portal mbCONNECT24.

In all other cases, make activating the mbEDGE function via mbCONENCT24.

NOTICE

If you have not already done so, insert the mbEDGE SD card into the SD card slot of the mbNET.

▶ Call the administration interface (WebGUI) of the mbNET

Start the web browser of your PC and enter the required LAN IP address of the router in the address bar.

NOTICE

Please note that access to the web interface is only possible via the HTTPS protocol (eg https://192.168.0.100).

Log on to the router now - factory setting is:
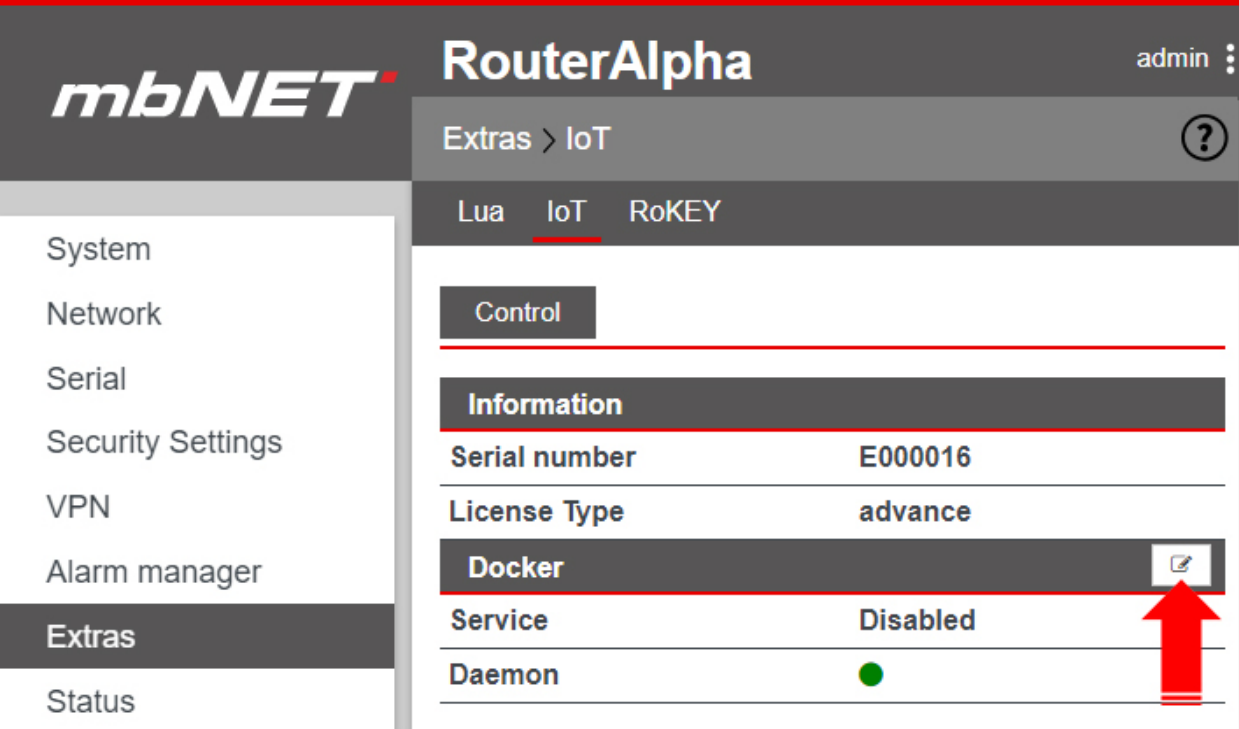
Username: admin

Password:
If you have not changed the default password yet, enter it here. The device password can be found on the back of the mbNET.

```
USER: admin
DEFAULT PASSWD:
47mxfFQrJ4
```

https://172.16.27.210/login

RouterAlpha

Login

Username

Password

Password

Log in
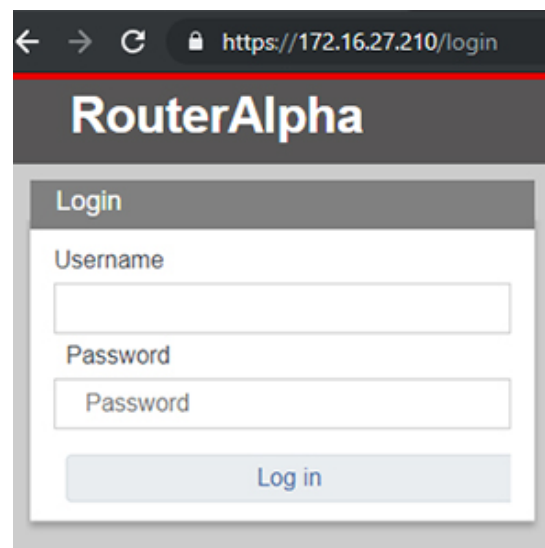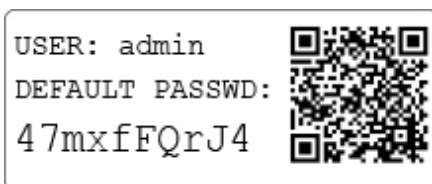
▶ Navigate to Extras > IoT > Control

▶ Click the edit icon to enable the Docker service.

After you have saved your input, you can activate / edit further services in the now expanded menu.

▶ Click the edit icon in the **Flows and Dashboard** submenu and enable this service.

Only activate Docker Management if you have purchased an mbEDGE.**advance** license.

Docker Management Settings

Enable	☐

Save   Close

Check the network settings for the Docker interface

In the **Extras > IoT** menu, switch to the submenu **Network**

RouterAlpha   admin ⋮

Extras ⟩ IoT   ?

Lua   IoT   RoKEY

Control   **Network**   Key Management   Firmware

Docker Interface   ✎

Docker IP Address	172.16.0.1
Subnetmask	255.255.255.0

Firewall Settings for Node-Red   ✎

Allow following TCP ports	
Allow following UDP ports	

This displays the IP address of the Docker daemon (IoT services runtimer and NodRed).
Default setting is 172.16.0.1/24
Adjust the IP address if an address conflict with other network settings is / can be expected.

The Docker Daemon's IP address must be neither in the LAN nor in the WAN address range of the router.

To change the network settings, click the edit icon ✎

Set firewall rules for Node-Red

Menu: **Extras > IoT** > **Network**

Here you add firewall rules to open ports for Node-RED.
By default, a network socket node in Node-RED has internal-to-outside access only. Therefore, any "listener socket" created in Node-RED is not accessible over LAN / WAN.
For example, an OPC UA server can not be reached via LAN / WAN. Unless you release the OPC UA server port here in a firewall rule.

To do this, click on the edit icon

Enter the port number for the respective protocol (UDP or TCP) here.

NOTICE

If you use multiple ports together, the port numbers must be entered separated by commas.

Create user for Node-Red (optional)

Switch to the menu **System** > **User**

Here are two new fields added:

- Flows (Node Red) Admin
- Docker Management Admin

For the administrator (admin), these two fields are enabled by default.

When you have finished with all settings, you need to **apply the changes**.
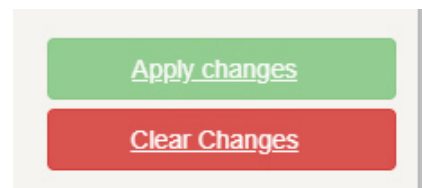
NOTICE

The mbEDGE service is now started. This may take a few minutes at the first activation.

When "Daemon" displays a green LED icon, the service is running.

"Flows" und "Dashboard" are ready when the link buttons appear black instead of grayed out.

mbEDGE

9   Access to (Node-Red) flows

Node-RED allows you to edit your flows or access the dashboards of Node-RED applications.

There are two ways to access Node-RED:

   a) via Web2go from your mbCONNECT24 account

   b) directly via the web interface of the mbNET
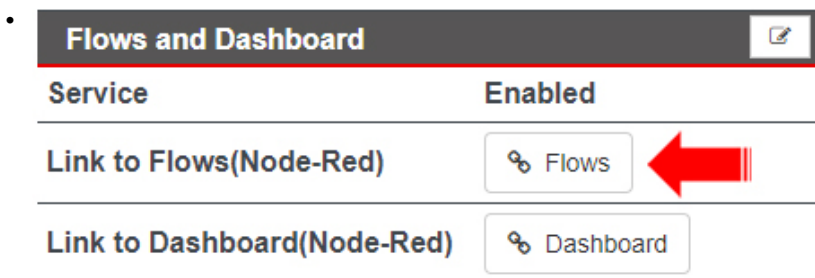
Access via Web2go from mbCONNECT24

   Navigation: Administration > Projects > Project Alpha *(selected project)* > RouterAlpha *(selected device)* > Interfaces
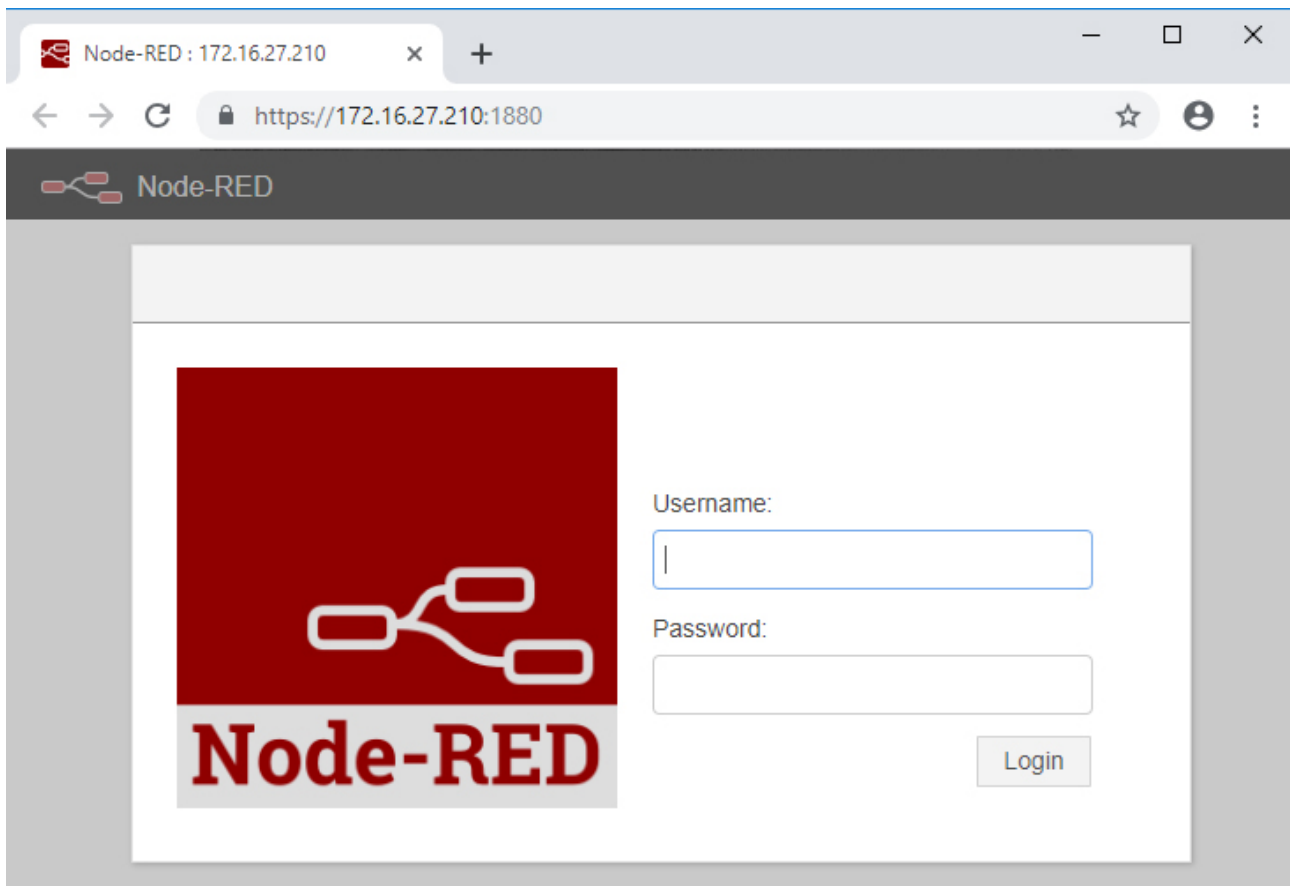
   •
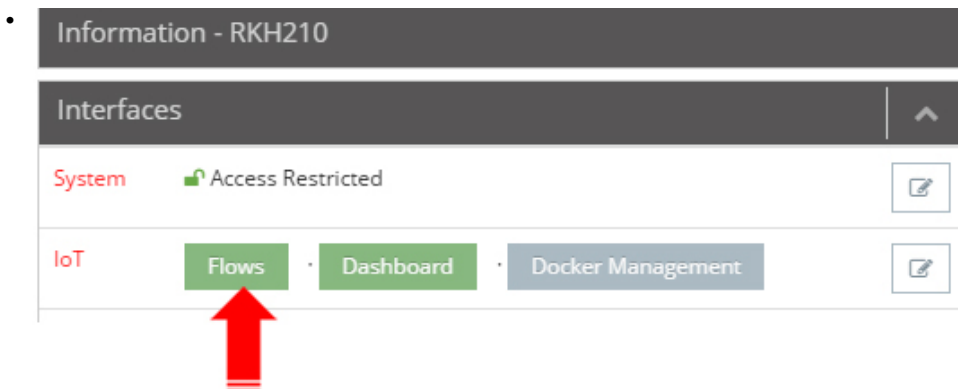
   In the device settings, click on the "Flows" button in the "**IoT**" menu item.

Access via the mbNET web interface

   Navigation: Extras > IoT > Control

   •

   Click on the "Flows" button

A new browser window, with a login, will open.

The access data for this are:

    a) User name and password for the user you created in the user management for accessing Node-Red

      or

    b) the current user data for the administrator (device access data)
      standard user name = admin
      standard password = the respective device password of the mbNET (see label on the back of the mb-NET)

Further information such as application examples, FAQs, videos and product information about *mbEDGE* can be found in our Helpdesk at www.mbconnectline.com
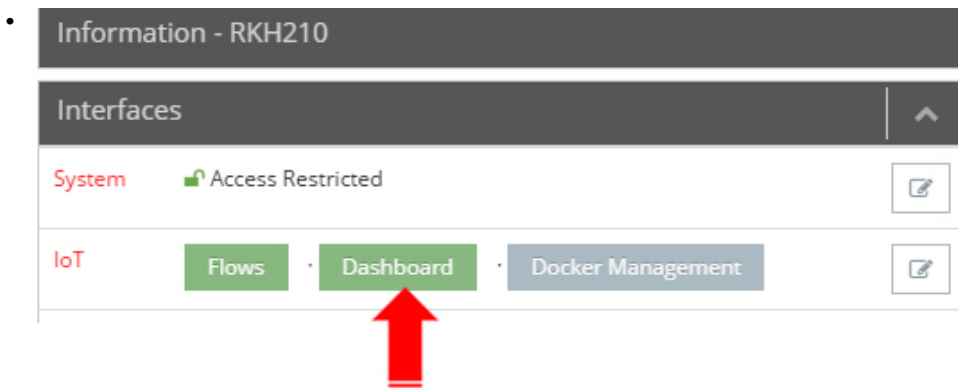
mbEDGE

10   Access to (Node-Red) dashboards

There are two ways to access dashboards:

    a) via Web2go from your mbCONNECT24 account

    b) directly via the web interface of the mbNET
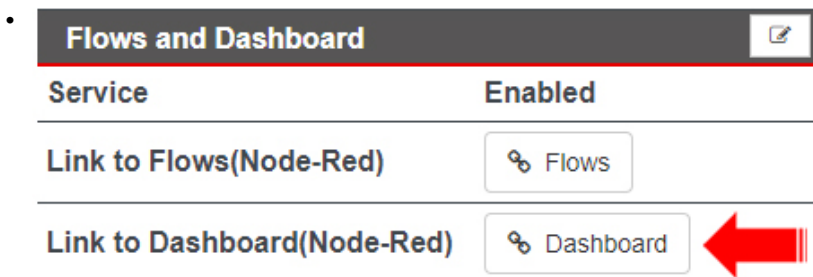
Access via Web2go from mbCONNECT24

Navigation: Adminstration > Projects > Project Alpha *(selected project)* > RouterAlpha *(selected device)* > Interfaces
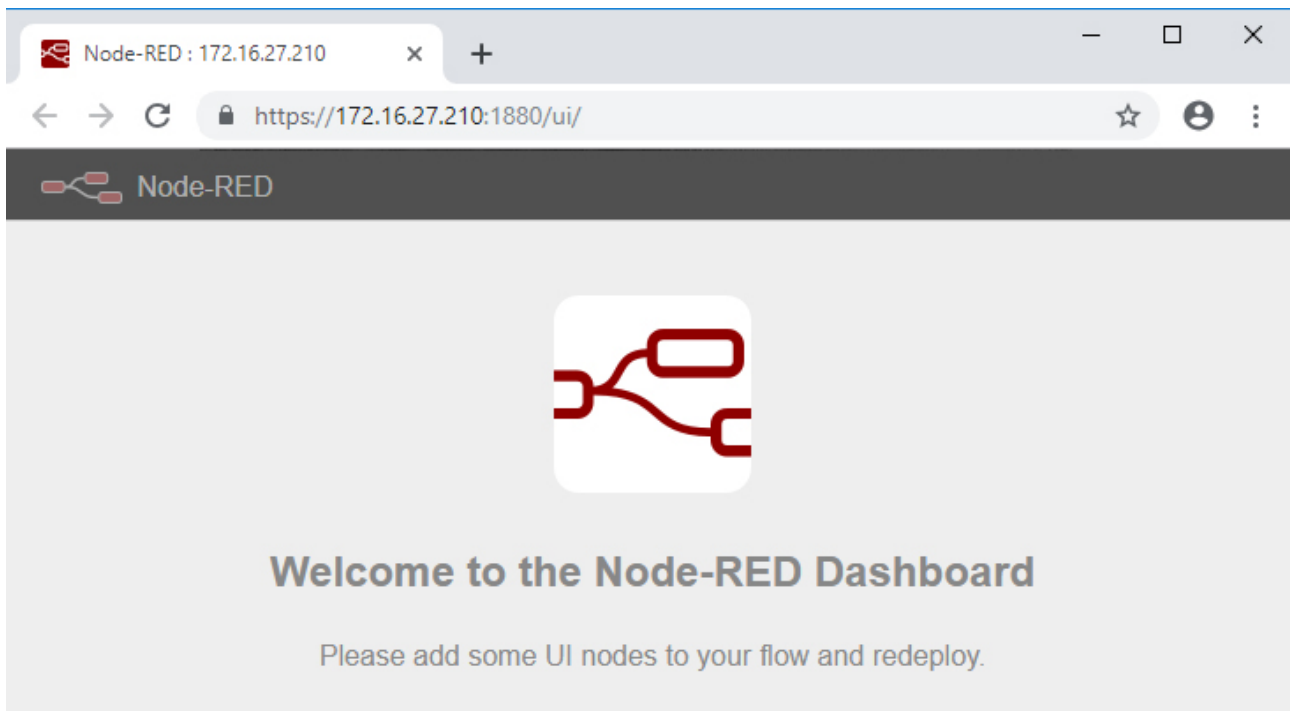
-

    In the device settings, click on the "Dashboard" button in the "**IoT**" menu item.

Access via the mbNET web interface

Navigation: Extras > IoT > Control

-

    Click on the "Dashboard" button

A new browser window will open with a Node Red dashboard.

NOTICE
As a dashboard of a flow out is generated, the display of a dashboard without access is possible.

As long as you have not created / configured a flow, you will be prompted to add some UI nodes to a flow and redeploy it.

Further information such as application examples, FAQs, videos and product information about *mbEDGE* can be found in our Helpdesk at www.mbconnectline.com

11   Generate user backup key

Only the mbNET with which the mbEDGE card is paired can open the encrypted container. So that you can access your data at any time, even if the mbNET is no longer available (eg in the event of a device failure or device replacement), a user backup key is required.

If the mbNET is no longer reachable before you have generated the user backup key (eg in the event of total failure due to damage), there is no way to access the card.

NOTICE

Immediately after initializing the mbEDGE card, assign a user backup key to avoid data loss!

▶   Go to the administration interface of the mbNET

a) directly via a web browser or

b) from mbCONNECT24 via Web2go

and navigate to the **Extras > IoT > Key Management** menu
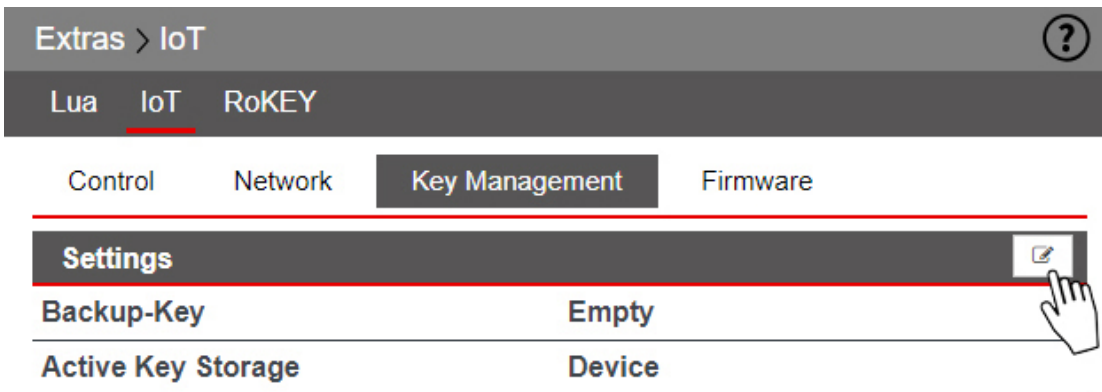
▶   Click on the edit button

and fill out the input fields under **Key Settings**.

The "**Backup-Key"** must be at least 8 characters long.
The **license code** can be found on the back of the mbEDGE packaging.

After you have saved your entries, you can always assign a new user backup key.

## 12 If you want to use the mbEDGE card in another mbNET

Relocation of the mbEDGE card from mbNET1 to mbNET2

mbNET 1   **mbNET 2**

NOTICE

If you want to operate an already paired mbEDGE card in another mbNET (card migration from mbNET 1 to mbNET 2), you need a user backup key. Ideally, the key was already created during the initialization of the mbEDGE card with mbNET 1, as recommended.

If this has not already been done, you must now generate the user backup key.

Please refer "Generate user backup key"
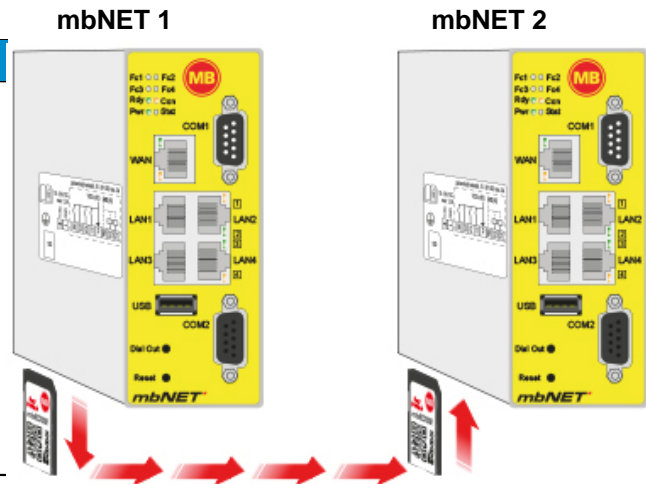
NOTICE

If mbNET 1 is no longer reachable before you have generated the user backup key (eg in the event of total failure due to damage), there is no way to access the card.

If you have created a user backup key:

▸ Remove the mbEDGE card from mbNET 1 and insert the card into the SD card slot of mbNET 2.

NOTICE

ATTENTION: Threatening data loss! Never remove the SD card from the device while the device is ready for use.

Data can be damaged or the device may no longer work.

First switch off the device and then remove the SD card from the slot.

▸ Call the administration interface of mbNET 2

    a) directly via a web browser or

    b) from mbCONNECT24 via Web2go

    and navigate to **Extras > IoT > Key Management**

▸ Here you will receive a message that the card can not be accessed and you will be asked to enter a user Backup Key.

▸ After entering the valid user Backup Key, you have access to the mbEDGE card.

Now there are two ways to operate the mbEDGE card in mbNET 2

- Temporary use

  - during temporary use of the mbEDGE card, no mbEDGE device pairing takes place.
    After each restart of mbNET 2, the user backup key must be reentered.

- Permanent use - new mbEDGE device pairing

  - if you want to permanently use the mbEDGE card in mbNET 2, you must use the mbNET security
    element to generate a new key store # 2.
    The mbEDGE card is then paired with mbNET 2.

MB connect line GmbH offers universal solutions for
worldwide remote maintenance of machines and equipment.
The specialists at MB connect line can draw on years of
experience and extensive know-how.

MB connect line GmbH
Fernwartungssysteme
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

Phone+49 (0) 700 MBCONNECT
+49 (0) 700 622 666 32

MB connect line Inc.
4320 Winfield Road, Suite 200
Warrenville, IL 60555
USA
Phone +1-630-797-0093
center.usa@mbconnectline.com

info@mbconnectline.com
www.mbconnectline.com

Despite a detailed description of the device and its functions, we cannot be held liable for the correctness of the content.
The latest information can be obtained on our homepage. We welcome any comments or suggestions for improvement.