

**User manual**  
**netFIELD OnPremise**  
**NIOT-E-TIJCX-GB-RE/NFLD**



**Hilscher Gesellschaft für Systemautomation mbH**  
**[www.hilscher.com](http://www.hilscher.com)**

DOC200901UM07EN | Revision 7 | English | 2025-03 | Released | Public

# Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>5</b>
1.1	About this document .....	5
1.1.1	Description of the contents .....	5
1.1.2	List of revisions .....	5
1.1.3	Conventions in this document.....	7
1.2	Terms and abbreviations.....	8
<b>2</b>	<b>Brief description .....</b>	<b>9</b>
2.1	Intended use .....	9
2.2	Key features .....	9
2.3	netFIELD OS: Industrial IoT Operating System .....	10
2.4	Depiction of netFIELD OnPremise SW architecture .....	14
<b>3</b>	<b>Safety .....</b>	<b>15</b>
3.1	General note .....	15
3.2	Personnel qualification .....	15
3.3	Device destruction by exceeding the allowed supply voltage .....	15
3.4	Risk of denial of service due to extensive memory usage close to limits.....	15
<b>4</b>	<b>Hardware description .....</b>	<b>16</b>
4.1	Device drawings.....	16
4.1.1	Positions of the interfaces .....	16
4.1.2	Dimensions .....	18
4.2	Interfaces .....	19
4.2.1	Power supply .....	19
4.2.2	LAN connectors .....	19
4.2.3	Real-Time Ethernet connectors .....	19
4.2.4	USB connectors .....	20
4.2.5	Serial interfaces COM1 and COM2 .....	20
4.2.6	Wi-Fi.....	22
4.2.7	Monitor connectors .....	22
4.3	LEDs .....	23
4.3.1	Positions of the LEDs on the device .....	23
4.3.2	Device status LEDs.....	24
4.3.3	LEDs of the LAN interface .....	25
4.3.4	LEDs of the Real-Time Ethernet interface .....	25
<b>5</b>	<b>Commissioning and first steps .....</b>	<b>26</b>
5.1	Overview .....	26
5.1.1	netFIELD Portal user .....	26
5.1.2	Standard Docker user .....	27
5.2	Mounting .....	28
5.2.1	Attaching LED sticker (optional).....	28
5.2.2	Mounting .....	29
5.2.3	Connecting Voltage supply .....	30
5.3	Establish LAN connection and login to Local Device Manager.....	31
5.3.1	Overview .....	31
5.3.2	Using DHCP server.....	32
5.3.3	Establishing one-to-one connection to device (without DHCP server) .....	35

5.3.4	Login to Local Device Manager .....	36
5.4	Set system time.....	39
5.5	"Onboard" (register) device in netFIELD Cloud .....	41
5.5.1	Overview .....	41
5.5.2	Onboarding using the "Basic" method .....	43
5.5.3	Onboarding using the "Advanced" method .....	46
<b>6</b>	<b>Local Device Manager .....</b>	<b>52</b>
6.1	Overview .....	52
6.2	System .....	54
6.3	Networking .....	57
6.3.1	Overview .....	57
6.3.2	Firewall.....	62
6.3.3	Network Proxy settings .....	72
6.4	Networking Services .....	78
6.4.1	Wi-Fi.....	78
6.4.2	DHCP Server .....	90
6.4.3	OT Interface (Using the cfx0 interface or RTE).....	94
6.4.4	Connectivity Check .....	96
6.5	Onboarding (and offboarding).....	98
6.6	General Settings .....	101
6.6.1	Web Server (Port) Settings .....	101
6.6.2	Default MQTT Client Settings .....	102
6.6.3	Docker Network Settings .....	104
6.6.4	Remote Access .....	108
6.6.5	Login .....	110
6.7	Standard Docker .....	111
6.8	IoT Edge Docker .....	117
6.9	Accounts .....	123
6.10	Certificate .....	127
6.11	Terminal .....	128
6.12	Operating System .....	129
6.12.1	OS Update .....	129
6.12.2	Backup & Restore .....	134
6.12.3	Factory Reset.....	137
6.13	Logs .....	138
6.14	Services .....	139
<b>7</b>	<b>Good to know.....</b>	<b>143</b>
7.1	Device recovery via USB .....	143
7.1.1	Overview .....	143
7.1.2	Requirements.....	143
7.1.3	Step-by-step instructions .....	144
7.2	Useful CLI commands and parameters in Terminal.....	152
7.2.1	Network Manager.....	152
7.2.2	Show interface status.....	152
7.2.3	Activate interface .....	152
7.2.4	Docker Compose support for Standard Docker environment .....	152
7.2.5	Manage Standard Docker .....	152
7.2.6	Manage IoT Edge Docker .....	152

7.2.7 Enable/disable SSH Daemon (release port 22) ..... 153

7.2.8 External storage support using iSCSI ..... 153

7.2.9 Follow the system log via terminal CLI ..... 153

**8 Technical data ..... 154**

**9 Decommissioning, dismantling and disposal ..... 156**

9.1 Putting the device out of operation..... 156

9.2 Disposal and recycling ..... 156

9.2.1 Disposal of battery ..... 156

9.2.2 Removal of battery ..... 157

9.2.3 Disposal of device ..... 157

**10 Legal notes ..... 159**

**List of figures ..... 164**

**List of tables ..... 167**

**Contacts..... 168**



# 1 Introduction

## 1.1 About this document

### 1.1.1 Description of the contents

This user manual describes the hardware and the web-based management GUI (Local Device Manager) of the **netFIELD OnPremise** edge gateway (NIOT-E-TIJCK-GB-RE/NFLD) from Hilscher. Instructions on how to commission the gateway are also provided in this document. Note that for ease of reading, the edge gateway is referred to simply as "device" in this document.

### 1.1.2 List of revisions

Revision	Date	Change
1	2020-12-10	Document created.
2	2021-06-29	<p>Document revised and updated to netFIELD OS 2.2:</p> <p>Section <i>Brief description</i> [▶ page 9] updated.</p> <p>Section <i>LAN connectors</i> [▶ page 19] updated.</p> <p>Section <i>LEDs of the Real-Time Ethernet interface</i> [▶ page 25] updated.</p> <p>Section <i>Establish LAN connection and login to Local Device Manager</i> [▶ page 31] updated.</p> <p>Section <i>"Onboard" (register) device in netFIELD Cloud</i> [▶ page 41] updated.</p> <p>Section <i>Firewall</i> [▶ page 62] updated.</p> <p>Section <i>Using the cifx0 interface (RTE)</i> removed (substituted by section <i>OT Interface (Using the cifx0 interface or RTE)</i> [▶ page 94]).</p> <p>Section <i>Networking Services</i> [▶ page 78] added.</p> <p>Section <i>Standard Docker</i> [▶ page 111] revised.</p> <p>Section <i>IoT Edge Docker</i> [▶ page 117] revised.</p> <p>Section <i>OT Interface (Using the cifx0 interface or RTE)</i> [▶ page 94] added.</p> <p>Section <i>Remote Access</i> [▶ page 108] added.</p>

Revision	Date	Change
3	2022-05-04	<p>Document revised and updated to netFIELD OS 2.3.</p> <p>Section <i>Terms and abbreviations</i> [▸ page 8] revised.</p> <p>Subsection <i>Services supported by netFIELD OS</i> in section <i>netFIELD OS: Industrial IoT Operating System</i> [▸ page 10] updated.</p> <p>Section <i>Risk of denial of service due to extensive memory usage close to limits</i> [▸ page 15] added.</p> <p>Subsection <i>Enabling access for application containers</i> in section <i>Serial interfaces COM1 and COM2</i> [▸ page 20] added.</p> <p>Section <i>OT Interface (Using the cfx0 interface or RTE)</i> [▸ page 94] moved from <i>General Settings</i> to <i>Networking Services</i>.</p> <p>Section <i>Connectivity Check</i> [▸ page 96] added.</p> <p>Section <i>Login</i> [▸ page 110] added.</p> <p>Section <i>OS Update</i> [▸ page 129] updated.</p> <p>Section <i>Services</i> [▸ page 139] added.</p> <p>Chapter <i>Decommissioning, dismounting and disposal</i> [▸ page 156] revised.</p> <p>Section <i>Legal notes</i> [▸ page 159] updated.</p>
4	2022-12-16	<p>Document updated to netFIELD OS 2.4.</p> <p>Sections <i>Onboarding using the “Basic” method</i> [▸ page 43] and <i>Onboarding (and offboarding)</i> [▸ page 98] updated (two-factor-authentication in Portal now supported).</p> <p>Section <i>Docker Network Settings</i> [▸ page 104] updated and revised (DNS server configuration added).</p> <p>Section <i>Accounts</i> [▸ page 123] updated (new roles added).</p> <p>Section <i>Operating System</i> [▸ page 129] added.</p> <p>Section <i>Backup &amp; Restore</i> [▸ page 134] added.</p> <p>Section <i>Factory Reset</i> [▸ page 137] added.</p> <p>Chapter <i>Decommissioning, dismounting and disposal</i> [▸ page 156] revised.</p>
5	2023-02-10	RAM in chapter <i>Technical data</i> [▸ page 154] updated.
6	2023-05-02	Download instructions in sections <i>OS Update</i> [▸ page 129] and <i>Device recovery via USB</i> [▸ page 143] updated.
7	2025-03-05	<p>Onboarding/offboarding with netFIELD OS V2.5:</p> <p>Device authentication methods added to sections <i>Onboarding using the “Basic” method</i> [▸ page 43] and <i>Onboarding (and offboarding)</i> [▸ page 98].</p> <p>Section <i>Onboarding (and offboarding)</i> [▸ page 98] updated.</p>

Table 1: List of revisions

### 1.1.3 Conventions in this document

Notes, instructions and results of operating steps are marked as follows:

#### Notes



---

**Important:**

<important note you must follow to avoid malfunction>

---



---

**Note:**

<general note>

---



---

<note on further information>

---

#### Instructions

1. Operational step
  - Instruction
  - Instruction
2. Operational step
  - Instruction
  - Instruction

#### Results

↻ Intermediate result

⇒ Final result

## 1.2 Terms and abbreviations

Term	Description
Container	Executable software package including all components needed to run an application on a Docker engine.
Docker	Software for isolating applications using container virtualization. Docker enables the creation and operation of Linux containers. netFIELD OS provides two Docker runtime environments: <i>IoT Edge Docker</i> and <i>Standard Docker</i> . The <i>IoT Edge Docker</i> environment is managed remotely from the <i>netFIELD Platform</i> .
IIoT	Industrial Internet of Things.
IT network	Information technology network
Microsoft Azure IoT Edge	Features a deployable Docker-based runtime along with a public cloud-hosted backend logic for remote device servicing. It is the basic framework of the evolved netFIELD device-to-cloud communication infrastructure.
netFIELD App	netFIELD application Docker container from Hilscher. Runs in the <i>IoT Edge Docker</i> or <i>Standard Docker</i> of the netFIELD OS on the netFIELD Edge.
netFIELD Cloud	Internet-hosted platform providing APIs for cloud-to-cloud and cloud-to-edge communication. Based on <i>Microsoft Azure IoT Edge</i> . Consists of the netFIELD Platform (backend) and the netFIELD Portal (web-based user interface/frontend). The netFIELD Cloud is also referred to as <i>netFIELD.io</i> .
netFIELD Edge	Gateway devices or systems running the netFIELD OS, providing connectivity to the netFIELD Cloud. Cloud connectivity is based on <i>Microsoft Azure IoT Edge</i> .
netFIELD.io	Internet-hosted platform providing APIs for cloud-to-cloud and cloud-to-edge communication. Based on <i>Microsoft Azure IoT Edge</i> . Consists of the netFIELD Platform (backend) and the netFIELD Portal (web-based user interface/frontend). netFIELD.io is also referred to as <i>netFIELD Cloud</i> .
netFIELD OS	Cross-platform capable Linux operating system providing core OS functions plus optional connectivity to the netFIELD Cloud. Cloud connectivity is based on <i>Microsoft Azure IoT Edge</i> .
netFIELD Platform	Backend of the netFIELD Cloud, providing APIs for cloud-to-cloud and cloud-to-edge communication.
netFIELD Portal	Web-based user interface (frontend) of the netFIELD Cloud.
netX	Multi-protocol communication controller for OT networks
OT network	Operational technology network.

Table 2: Terms and abbreviations

## 2 Brief description

### 2.1 Intended use

netFIELD OnPremise is an edge gateway hosting the netFIELD OS for connecting an OT network – like e.g. PROFINET – with an IT network, the netFIELD Cloud or other custom IIoT services or applications.

### 2.2 Key features

- Physical separation of OT network and IT network by using two controllers:
  - Primary controller: Edge computing, IIoT functions and cloud connectivity are processed by the security-enhanced Yocto-Linux-based netFIELD OS on the main CPU.
  - Secondary controller: OT network connectivity (e.g. PROFINET) is processed by the netX 100 communication controller.
- Applications for data acquisition, analytics, processing or connectivity (to cloud or other enterprise systems) do not run natively under the netFIELD OS, but as “containers” in a Docker runtime. netFIELD OS provides two Docker runtimes that are running simultaneously on the device:
  - **IoT Edge Docker** for remote and automatic deployment and maintenance of containers. These containers are deployed (“pulled”) and managed over the netFIELD Platform. This requires your device to be onboarded in the *netFIELD Portal*. Note that you need an account/subscription for the *netFIELD Portal* (<https://www.netfield.io>) for this.
  - **Standard Docker** for manual and local deployment and maintenance of containers. Those containers can be pulled from official registries like Docker Hub (<https://hub.docker.com>) or any locally hosted Docker registry. In case you do not participate in the netFIELD device registration and onboarding process, the standard Docker is the only way to pull and run container applications on your device.
- The netFIELD OS features the **Local Device Manager**, which is a web-based GUI for local device parameterization.

## 2.3 netFIELD OS: Industrial IoT Operating System

The netFIELD OS supports scalable field device hardware depending on the customer's use case. In order to achieve this, applications do not run directly on the host system but instead as containers in a Docker runtime. Our OS is very lean and only supports the essential services required by the customer's network infrastructure.

### Features

- **Run containers:** Containers are revolutionizing connected IoT devices, and netFIELD OS is the perfect match to run them.
- **Manage device:** Manage your device locally with a web-based interface. It is easy to administer storage, configure networks, and more.
- **Build to last:** Build to survive in harsh environments like unexpected shutdowns with security in mind.
- **Easy to port:** Based on a Yocto project (<https://www.yoctoproject.org>) maintained Linux for easy porting to most capable device types across various CPU architectures.

### Architecture

Hilscher netFIELD OS is a secure operating system that makes it easy to program, deploy, connect and manage Edge Devices. Hilscher netFIELD OS extends the Linux kernel, with software libraries to securely connect operation technology like PLC, MES, Historians, Files or other on-premise systems with IT services like the netFIELD Portal. Our OS lets you innovate faster embracing container technologies managed by the netFIELD Portal from a central point or locally at the edge.

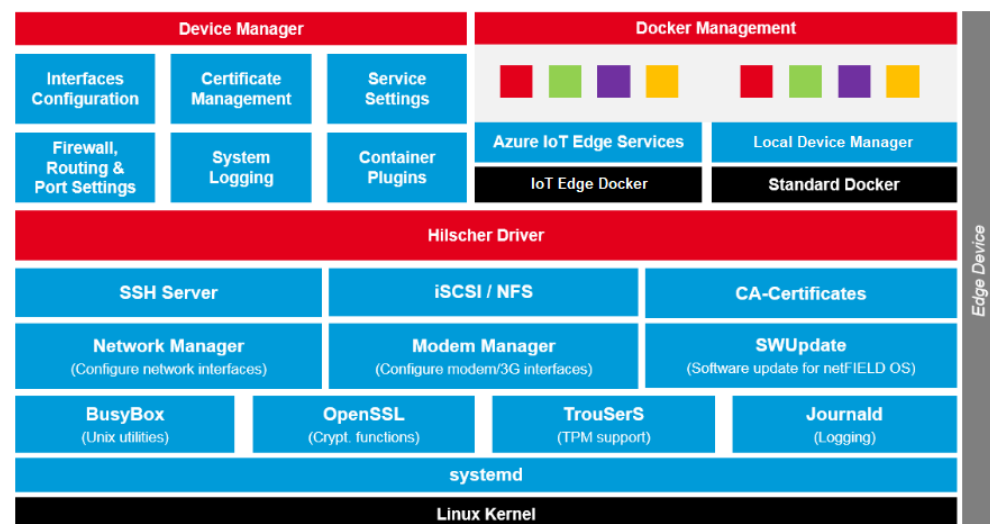


Figure 1: netFIELD OS architecture

Core services

The netFIELD OS core services include the support of hardware interfaces, the network environment, secure communication and system logging. In order to support the customer in setting up the gateway configuration, the Local Device Manager is coming along with the core services. With the open plug-in mechanism, the functionality of the Local Device Manager can be easily extended with the help of containerized applications.

Container management

Application containers can run in the IoT Edge Docker or Standard Docker environment and do contain business logic such as for data acquisition, analytics, processing or connectivity to cloud or enterprise systems.

The container management provides the functionality to pull and run containers on the device itself. Before a container can be run, its image needs to be pulled from a certain container registry. After that the container is created, the application can be then controlled by using the start / stop commands or by enabling the autostart option. Also, the deletion of containers and images is a part of container management. In order to enable the field devices for off- and online scenarios, netFIELD OS provides two Docker runtime environments at the same time.

The IoT Edge Docker environment is managed by the netFIELD.io (netFIELD Platform) remotely. That is why there is no need to have direct access to the netFIELD Edge Device, as long as the device can hold its connection to netFIELD.io. Administrators can be anywhere and have full management access to the device with the stored images and have the ability to control the application containers remotely. Otherwise, the Standard Docker can be used locally if the netFIELD Edge Device is not connected to netFIELD.io. In this case, the Standard Docker runtime environment can be managed by the Local Device Manager, by the netFIELD OS command line interface or by a web application like *portainer.io*, which can be deployed as container.

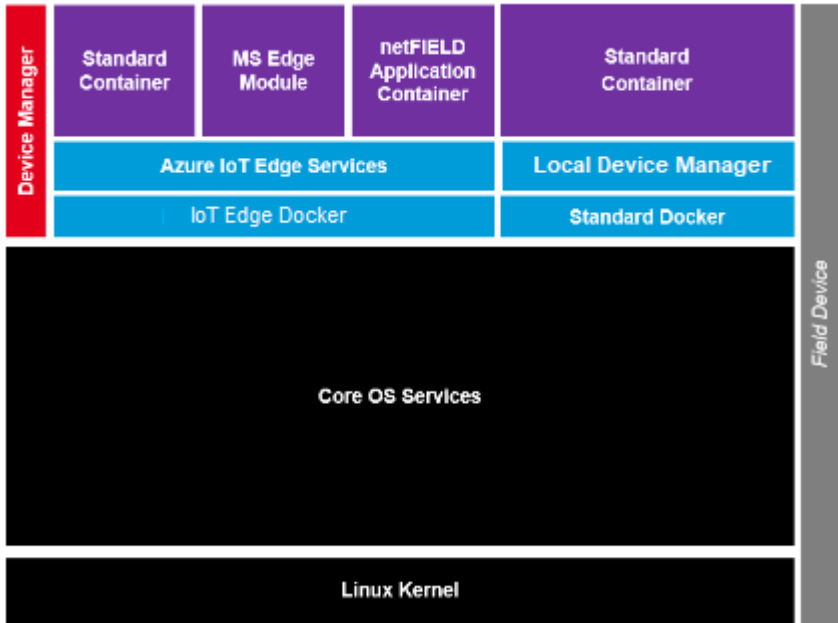


Figure 2: netFIELD OS container management

## Inter-container communication

Application containers usually focus on the dedicated business logic in order to avoid the development of unmaintainable software monoliths. In this scenario, multiple containers need to work together to realize customer use cases. Our powerful message and container-oriented architecture provide the highest level of flexibility and reusability when implementing customer solutions with individual requirements. This reduces IoT solution cost in development and operation.

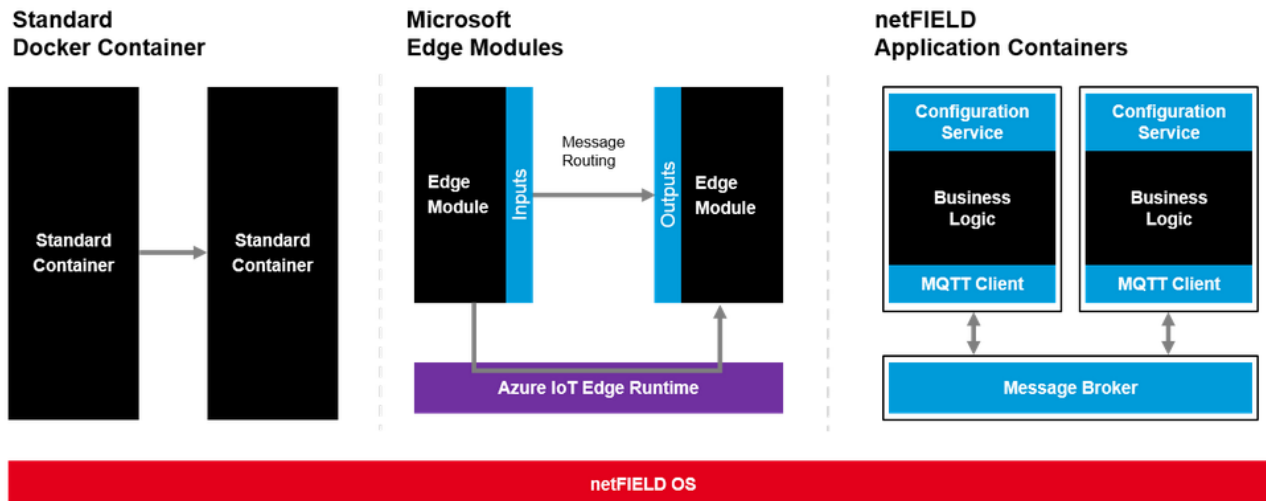


Figure 3: netFIELD OS inter-container communication

## Services supported by netFIELD OS

- Network interface configuration
- Firewall configuration (NAT, TCP/IP port management)
- Wi-Fi communication in “Client” or “Access Point” mode according to IEEE 802.11 (single band, 2.4 GHz). Client mode supports Personal and Enterprise WPA.
- HTTP(S) Proxy Server configuration
- Network storage (NFS, iSCSI) support
- Resources monitoring
- Access to netFIELD OS and Docker services via a web-terminal or over SSH
- Standard Docker instance for locally managed containers, including Docker Compose support
- IoT Edge Docker instance for application containers managed via netFIELD Cloud
- netFIELD OS update, backup & restore and “factory reset” (local/remote)
- User account management with pre-defined roles:
  - Network admin
  - Container admin
  - Container observer
  - Time admin



- System and container logging
- Onboarding in netFIELD Cloud
- Secure communication to the netFIELD Cloud services
- Remote device control/access via netFIELD Cloud, protected by “four-eyes principle”:  
Must be explicitly enabled by the user in the Local Device Manager
- Selection of upstream (device-to-cloud) protocol to the netFIELD Cloud: AMQP, AMQPWS, MQTT or MQTTWS. Note that the protocols use different ports, which is relevant to your firewall configuration
- Management of Linux services in Local Device Manager
- Connectivity check for IoT Edge Docker in Local Device Manager

## 2.4 Depiction of netFIELD OnPremise SW architecture

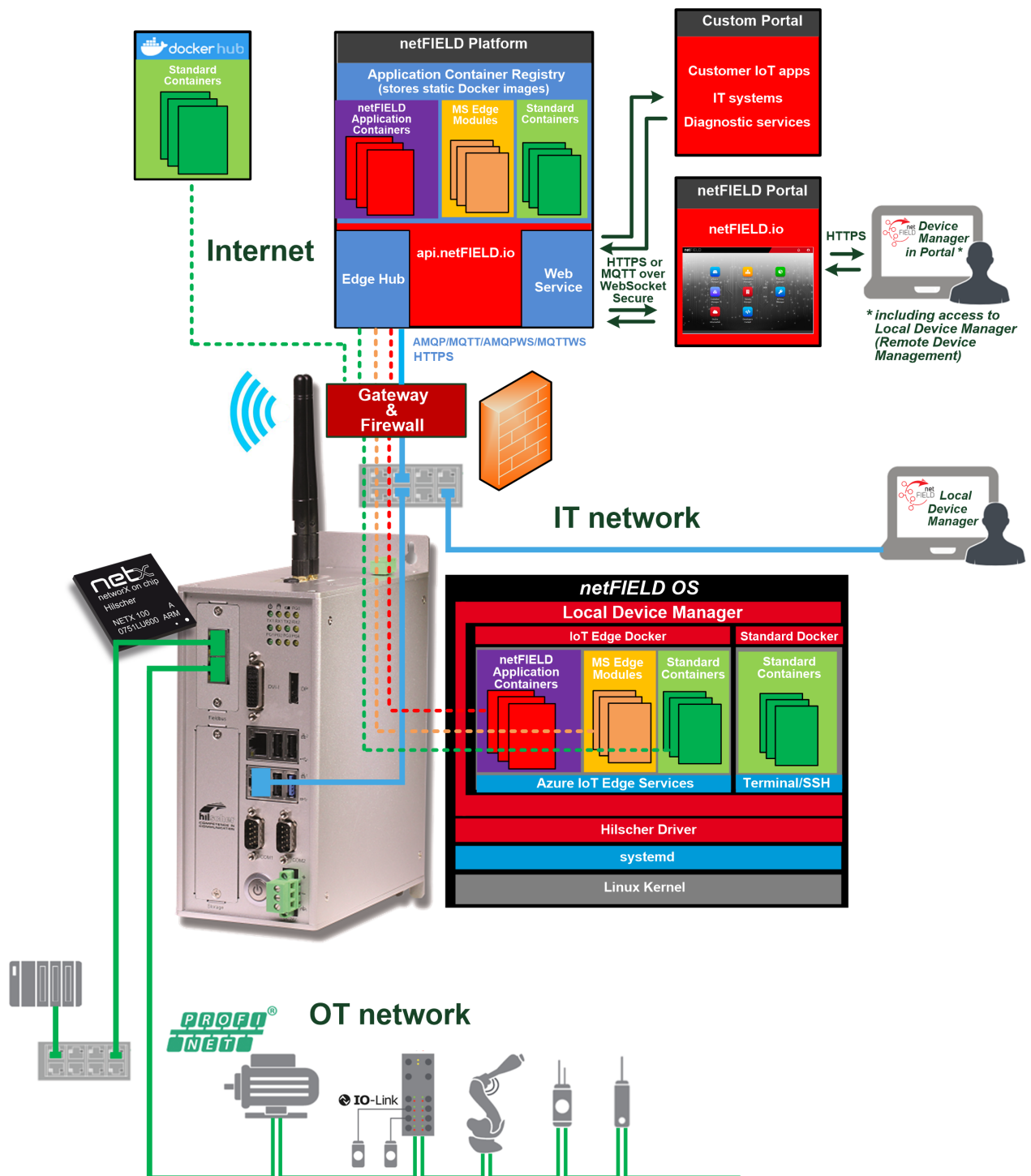


Figure 4: netFIELD OnPremise SW architecture

## 3 Safety

### 3.1 General note

To avoid personal injury or property damage to your system or to this product, you must read and understand all instructions in this manual before using the product.

This manual was written for the use of the product by educated personnel. When using the product, all safety instructions and all valid legal regulations have to be obeyed. Technical knowledge is presumed.

Keep this manual for future reference.

### 3.2 Personnel qualification

The device may only be installed, configured, operated and removed by qualified personnel. Job-specific technical skills for people professionally working with electricity must be present concerning the following topics:

- Safety and health at work
- Mounting and attaching of electrical equipment
- Measurement and analysis of electrical functions and systems
- Evaluation of the safety of electrical systems and equipment
- Installing and configuring IT

### 3.3 Device destruction by exceeding the allowed supply voltage

Observe the following notes concerning the voltage supply:

- The device may only be operated with the specified supply voltage of 24 V DC ( $\pm 4.8$  V DC). Make sure that the limits of the allowed range for the supply voltage are not exceeded.
- A supply voltage above the upper limit can cause severe damage to the device!
- A supply voltage below the lower limit can cause malfunction of the device.

### 3.4 Risk of denial of service due to extensive memory usage close to limits

Using applications that exceed the memory resources of the device can cause an out-of-memory situation (OOM) in the Linux kernel leading to temporary delayed application reaction times and limited overall device responsiveness.

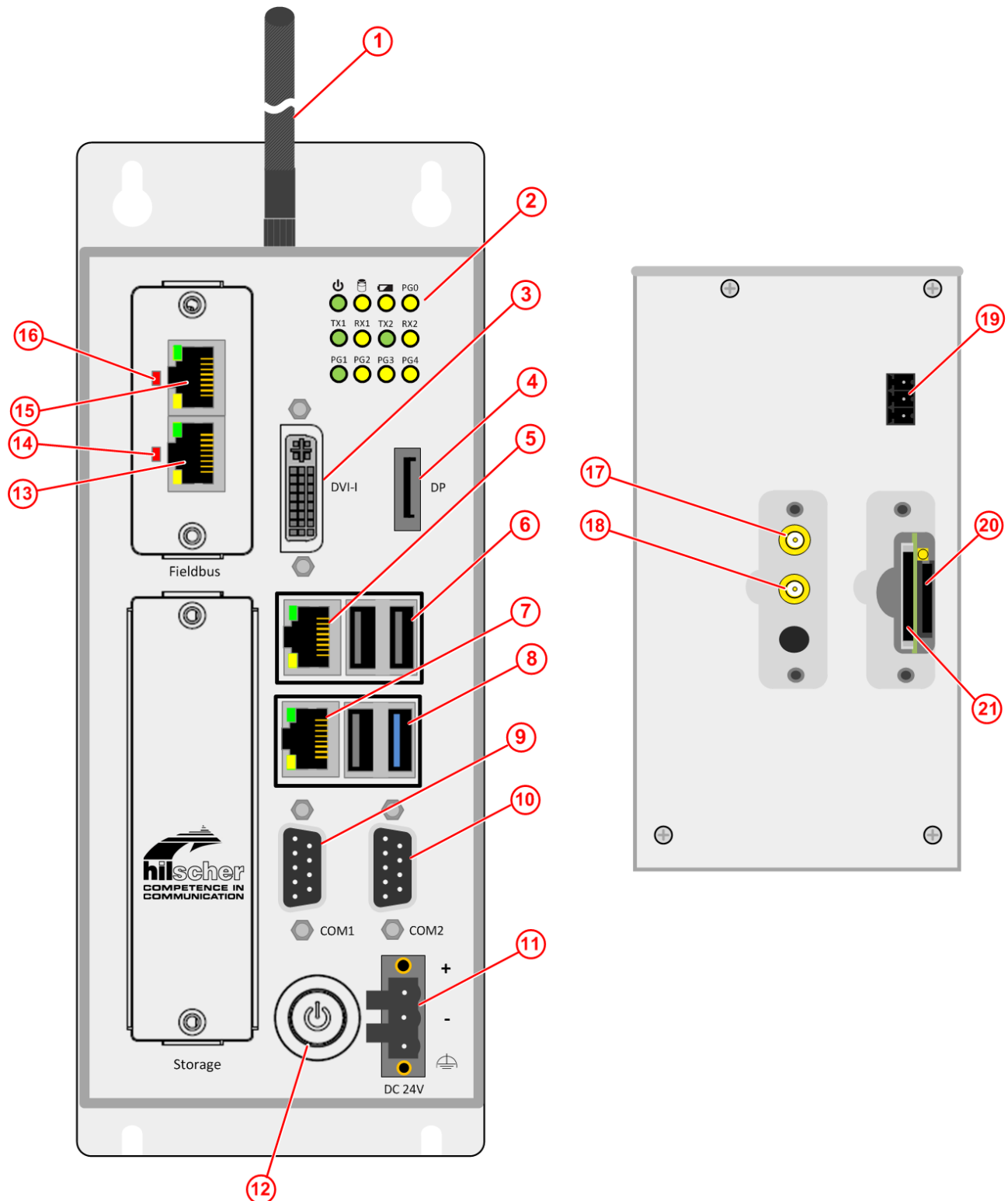
You must therefore consider the memory requirements of your Docker containers carefully before deploying them on the device. We also recommend you to configure the logging behavior (e.g. log levels) of your containers accordingly.

For information on the memory resources of the device, see section *Technical data* [► page 154].

## 4 Hardware description

### 4.1 Device drawings

#### 4.1.1 Positions of the interfaces



Pos.	Interface	For details see section
(1)	Antennas (Wi-Fi antennas are included in the delivery)	<i>Wi-Fi</i> [▶ page 22]
(2)	Device state LEDs (12 x)	<i>Device status LEDs</i> [▶ page 24]
(3)	DVI-I connector for external monitor	<i>Monitor connectors</i> [▶ page 22]
(4)	DisplayPort connector for external monitor	
(5)	LAN connector (RJ45 jacket) port 2 / Eth1	<i>LAN connectors</i> [▶ page 19]
(6)	USB connectors (3x USB 2.0)	<i>USB connectors</i> [▶ page 20]
(7)	LAN connector (RJ45 jacket) port 1 / Eth0	<i>LAN connectors</i> [▶ page 19]
(8)	USB connector (1x USB 3.0)	<i>USB connectors</i> [▶ page 20]
(9)	Serial interface connector COM1 (RS-232/422/485, can be configured)	<i>Serial interfaces COM1 and COM2</i> [▶ page 20]
(10)	Serial interface connector COM2 (RS-232/422/485, can be configured)	
(11)	+24 V DC supply voltage connector (Combicon)	<i>Power supply</i> [▶ page 19]
(12)	Power button On/Off	-
(13)	Real-Time Ethernet connector (RJ45 jacket) port 1 (channel 1)	<i>Real-Time Ethernet connectors</i> [▶ page 19]
(14)	LED for indicating the communication status of the Real-Time Ethernet interface.	<i>LEDs of the Real-Time Ethernet interface</i> [▶ page 25]
(15)	Real-Time Ethernet connector (RJ45 jacket) port 0 (channel 0)	<i>Real-Time Ethernet connectors</i> [▶ page 19]
(16)	LED for indicating the communication status of the Real-Time Ethernet interface.	<i>LEDs of the Real-Time Ethernet interface</i> [▶ page 25]
(17)	SMA connector for WiFi or cellular radio antenna	<i>Wi-Fi</i> [▶ page 22]
(18)	SMA connector for WiFi or cellular radio antenna	
(19)	Remote push button connector (without function)	-
(20)	SIM card holder (under removable cover)	-
(21)	SD card holder (under removable cover, without function)	-

Table 3: Positions of the interfaces

4.1.2 Dimensions

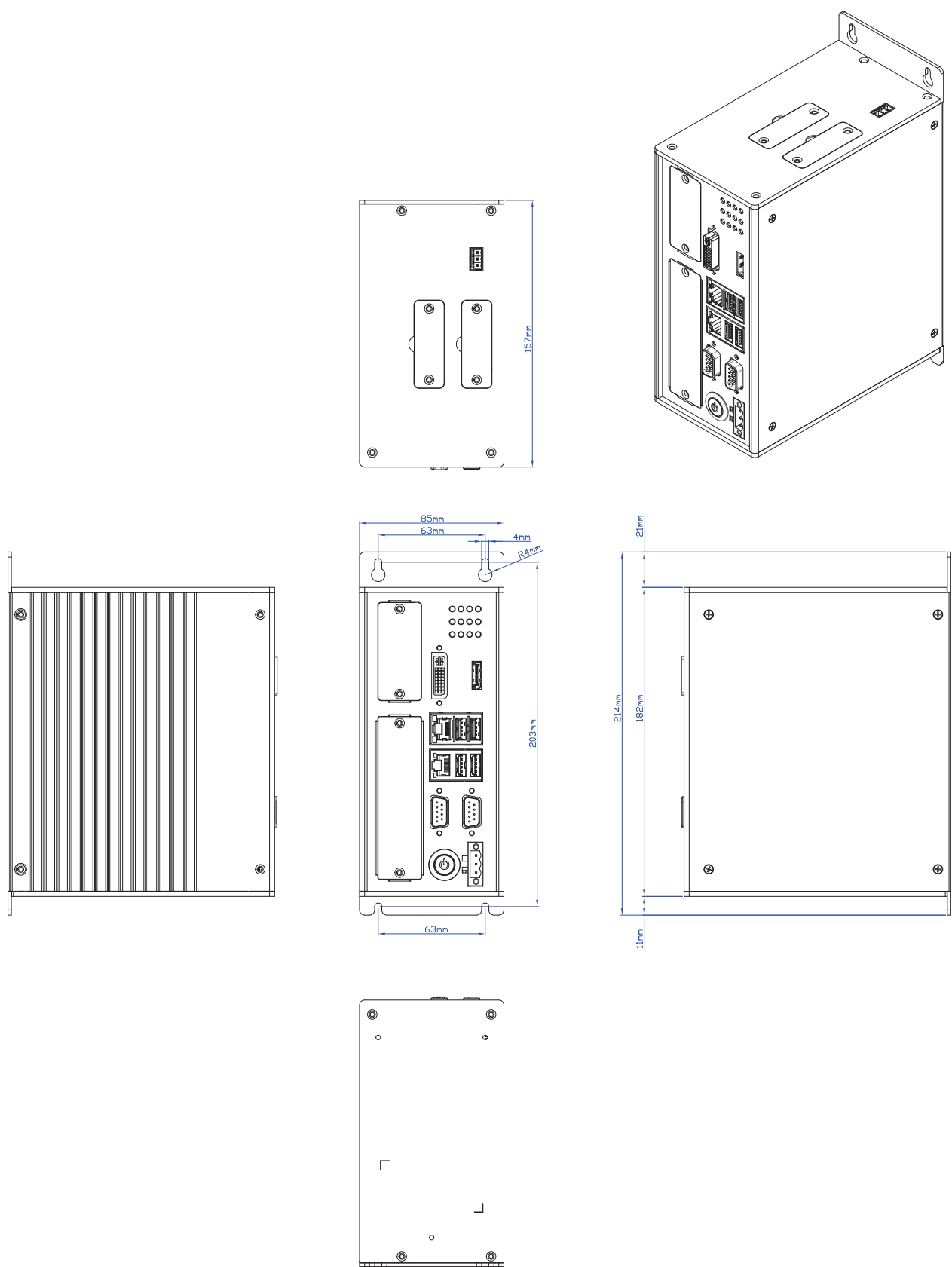


Figure 6: Device dimensions

## 4.2 Interfaces

### 4.2.1 Power supply

See position **(11)** in section *Positions of the interfaces* [► page 16].

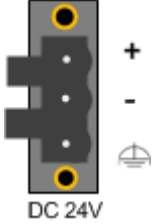

DC 24V	Pin	Signal	Description
	+	+24 V DC	+24 V DC
	-	GND	Ground (Reference potential)
		FE	Functional earth

Table 4: Power supply connector

### 4.2.2 LAN connectors

The two RJ45 connectors (see positions **(5)** and **(7)** in section *Positions of the interfaces* [► page 16]) allow you to connect your device to your IT network, respectively to the cloud (e.g. the netFIELD Portal).

The MAC addresses of the LAN interfaces are printed on the device label. Note that the “factory setting” for the IP address of the LAN port 1 (eth0) is DHCP mode (“fallback” is *link-local*, i.e. address block 169.254.0.0/16). The “factory setting” for the IP address of the LAN port 2 (eth1) is 192.168.253.1

You can change the IP address settings in the Local Device Manager (see section *Networking* [► page 57]).

### 4.2.3 Real-Time Ethernet connectors

The two RJ45 connectors (see positions **(13)** and **(15)** in section *Positions of the interfaces* [► page 16]) allow you to connect your device to a Real-Time Ethernet network (OT network).

The MAC addresses of the RTE interfaces are printed on the device label (“Fieldbus MAC addr.”)

Note that you must deploy software containers featuring the corresponding applications (e.g. *netFIELD App PROFINET Device*) on the device in order to use the Real-Time Ethernet interface.



**Note:**

The RTE interface can also be used like a standard Ethernet TCP/IP interface with limited data throughput. (In this case, “multicasts” are not supported.)

If you want to do so, you can enable this option in the **Local Device Manager** under **Networking Services > OT Interface** (see section *OT Interface (Using the cifx0 interface or RTE)* [► page 94] for further information).

## 4.2.4 USB connectors

The device is equipped with three USB 2.0 ports and one USB 3.0 port (see positions (6) and (8) in section *Positions of the interfaces* [▶ page 16]). For the maximum allowed output current, see section Technical data.

**Note:**

You do not need the USB connectors for the “normal” operation of the device.

You need the USB connectors e.g. for connecting a keyboard in order to access the terminal, to change BIOS settings or to perform a firmware recovery via USB stick.

## 4.2.5 Serial interfaces COM1 and COM2

The device has two configurable serial interfaces: COM1 and COM2 (see positions (9) and (10) in section *Positions of the interfaces* [▶ page 16]). Each serial interface can be used as RS-232, RS-422 or RS-485 interface.

### Requirements for using the serial interfaces

You have to set the interface type in the BIOS. For this, you need a keyboard with USB connector and a monitor with DVI-I or DP connector.

**Important:**

Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.

### BIOS settings

In the BIOS, select **Advanced > IT8786 Super IO Configuration > Serial Port 1 Configuration** for COM1 or **Serial Port 2 Configuration** for COM2.

Serial Port Configuration	Parameter
Serial Port	Enabled Disabled
Device Settings	Display only Serial Port 1 (COM1): IO=248h; IRQ=5 Serial Port 2 (COM2): IO=2F8h; IRQ=3
Onboard Serial Port Mode	RS232 RS422 RS485 (do not use this setting) RS485 Auto (use this setting for RS-485 only, because RTS control is active)

Table 5: Parameters of the serial interface



## Enabling access for application containers

netFIELD OS supports the serial interfaces as standard Linux devices:

COM1: /dev/ttyS0

COM2: /dev/ttyS1

Docker application containers accessing the `ttyS0` or `ttyS1` interfaces must be either running as `root` user or as a member of the `dialout` group in Linux. If your container is not a `root` user, you can add the container to the `dialout` group with the `--group-add dialout` parameter in your `docker run` command during container deployment. Note that you must also map the `/dev/ttyS0` respectively `/dev/ttyS1` interface into the corresponding container.

The following example shows a `docker run` command for a Node-RED container that would allow the container to access the COM1 interface:

```
docker run -d -p 1880:1880 --device=/dev/ttyS0:/dev/ttyS0 --group-add dialout nodered/node-red
```

If the container is deployed via Docker Compose, you would have to add the following lines in the `*.yaml` file:

```
devices:
  - "/dev/ttyS0:/dev/ttyS0"
group_add:
  - dialout
```

## Pinning RS-232

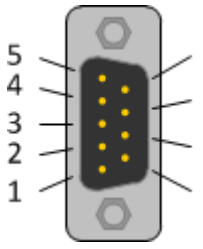
RS-232	Pin	Signal	Description
	1	DCD	Data Carrier Detect
	2	RXD	Receive signal
	3	TXD	Send signal
	4	DTR	Data Terminal Ready
	5	ISO_GND	Ground (reference potential)
	6	DSR	Data Set Ready
	7	RTS	Request to Send
	8	CTS	Clear to Send
	9	RI	Ring Indicator

Table 6: RS-232 D-Sub

## Pinning RS-422

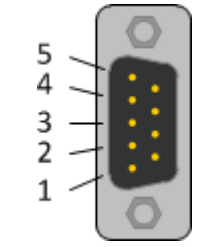
RS-422	Pin	Signal	Description
	1	Tx-	Send signal negative
	2	Tx+	Send signal positive
	3	Rx-	Receive signal negative
	4	Rx+	Receive signal positive
	5	ISO_GND	Ground (reference potential)
	6	n.c.	-
	7	n.c.	-
	8	n.c.	-
	9	n.c.	-

Table 7: RS-422 D-Sub

Pinning RS-485

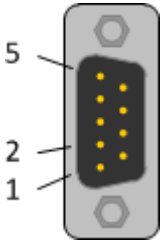
RS-485	Pin	Signal	Description
	1	Rx/Tx-	Send/receive signal negative
	2	Rx/Tx+	Send/receive signal positive
	3	n.c.	-
	4	n.c.	-
	5	ISO_GND	Ground (reference potential)
	6	n.c.	-
	7	n.c.	-
	8	n.c.	-
	9	n.c.	-

Table 8: RS-485 D-Sub

4.2.6 Wi-Fi

The device is equipped with a Wi-Fi interface according to IEEE 802.11. (For the position of the antennas, see position (1) in section *Positions of the interfaces* [► page 16].)

The Wi-Fi MAC address is printed on the device label.

The Wi-Fi interface supports two operating modes: **Access Point** and **Client**. In **Access Point** mode, the device acts as server allowing other Wi-Fi capable devices (e.g. smartphones or tablets) to connect to it. The **Client** mode allows the device to connect to any available Wi-Fi Access Point. The Wi-Fi functions (including a DHCP Server for Access Point mode) can be activated and configured in the **Local Device Manager** on the **Networking Services** page (see section *Networking Services* [► page 78]).

4.2.7 Monitor connectors

The device is equipped with a DVI-I socket (see position (3) in section *Positions of the interfaces* [► page 16]) and a DisplayPort (DP) [position (4)] to connect a monitor.



**Important:**

Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.



**Note:**

You do not need a monitor for the “normal” operation of the device. Connecting a monitor can be useful to access the terminal, to check the hostname and the IP address of the device (which the netFIELD OS outputs after booting) or for changing the BIOS settings in order to perform a firmware recovery via USB stick.

## 4.3 LEDs

### 4.3.1 Positions of the LEDs on the device

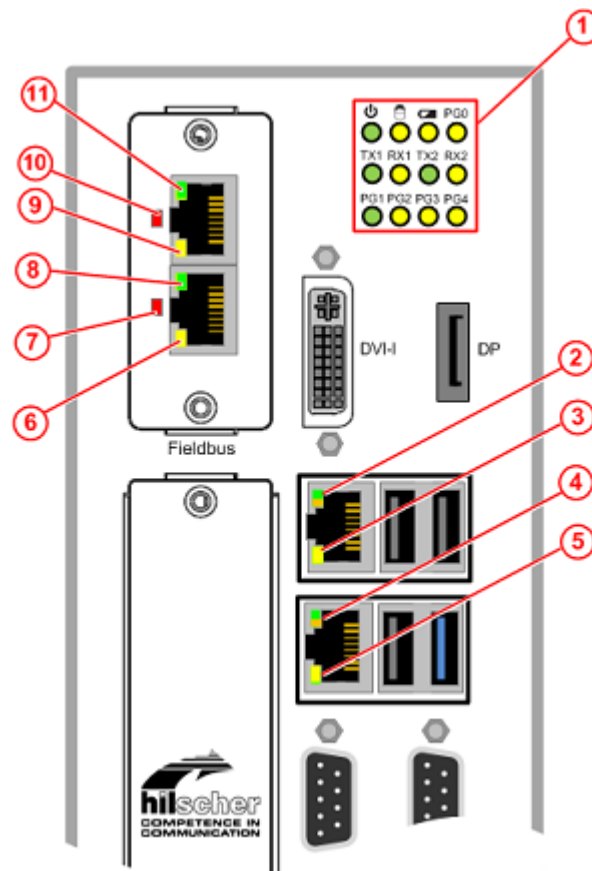


Figure 7: LED positions on device

### 4.3.2 Device status LEDs

LEDs indicating voltage supply, hard disk access, battery state and activity of operating system, serial interfaces and GPIOs. The position of the LEDs is indicated by position (1) in section *Positions of the LEDs on the device* [► page 23].













LED	Color	Meaning
	green	Voltage supply is OK
	yellow	Hard disk drive is accessed
	yellow	State of CMOS-RAM (BIOS) battery
PG0 	yellow	GPIO 4: can be programmed, currently not used.
TX1 	green	Transmission of data at serial interface COM1
RX1 	yellow	Receiving data at serial interface COM1
TX2 	green	Transmission of data at serial interface COM2
RX2 	yellow	Receiving data at serial interface COM2
PG1 	green	GPIO 0: Blinks when data is being copied from USB stick into device during firmware recovery.
PG2 	yellow	GPIO 1: can be programmed, currently not used.
PG3 	yellow	GPIO 2: can be programmed, currently not used.
PG4 	yellow	GPIO 3: can be programmed, currently not used.

Table 9: Description of device status LEDs

### 4.3.3 LEDs of the LAN interface

LEDs indicating state of the LAN communication (see section *Positions of the LEDs on the device* [► page 23]).







LED	Color	State	Meaning
<b>LINK</b> See positions (2) and (4)	<b>Duo LED green/orange</b>		
	 (green)	On	1 GBit network connection
	 (orange)	On	100 MBit network connection
	 (off)	Off	10 MBit or no network connection
<b>RX/TX</b> See positions (3) and (5)	<b>LED yellow</b>		
	 (yellow)	On	The device does not send/receive Ethernet frames.
	 (yellow)	Flickering (load dependent)	The device sends/receives frames.
	 (off)	Off	The device does not send/receive Ethernet frames.

Table 10: LEDs LAN interface

### 4.3.4 LEDs of the Real-Time Ethernet interface

LEDs (6) ... (11) in section *Positions of the LEDs on the device* [► page 23] relate to the Real-Time Ethernet network (OT network) that is connected to the RTE ports of the device (labelled as **Fieldbus** on the device housing). Names and functions of these LEDs depend on the protocol of the Real-Time Ethernet container that you have deployed on your device. They are therefore not described in detail here.



**Note:**

The COM LED (position (7) in section *Positions of the LEDs on the device* [► page 23]) shows steady red light if the TCP/IP channel of the cfx0 interface is enabled. See section *OT Interface (Using the cfx0 interface or RTE)* [► page 94] for further information.

## 5 Commissioning and first steps

### 5.1 Overview

#### 5.1.1 netFIELD Portal user

The following table shows the steps that you must perform in order to commission your device if you are a user of the netFIELD Portal.

#	Step	For details see
0	Requirement: • You have a netFIELD Portal account.	-
1	Mount the device.	Section Mounting
2	Establish LAN connection and login to Local Device Manager.	Section <i>Establish LAN connection and login to Local Device Manager</i> [► page 31]
3	Set local system time.	Section <i>Set system time</i> [► page 39]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section <i>Network Proxy settings</i> [► page 72]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section <i>Docker Network Settings</i> [► page 104]
6	Optional: Configure netFIELD OS firewall. <b>Note:</b> By default, the internal netFIELD OS firewall allows all traffic ("trusted zone"). When you assign an interface or subnet to the drop or block zone, make sure that you open the ports that are used by your application containers.	Section <i>Firewall</i> [► page 62]
7	"Onboard" (register) device in netFIELD Portal. <b>Note:</b> Make sure that your company's firewall does not block the TCP port (outgoing) of the upstream protocol (device-to-cloud communication) that you intend to use. MQTT: 8883 MQTT over WebSocket: 443 AMQP: 5671 AMQP over WebSocket: 443	Section <i>"Onboard" (register) device in netFIELD Cloud</i> [► page 41]
8	Optional: Deploy application container(s) from netFIELD Portal (if not already deployed through Deployment Manifest).	Section <i>Deploying containers on your device</i> in the operating instruction manual <i>netFIELD Portal</i> , DOC190701OIxxEN

Table 11: Tasks for commissioning the device (netFIELD Portal user)

## 5.1.2 Standard Docker user

The following table shows the steps that you must perform in order to commission your device if you use only the Standard Docker (*portainer*) for your application containers (i.e. if you are not a netFIELD Portal user).

#	Step	For details see
1	Mount the device.	Section Mounting
2	Establish LAN connection and login to Local Device Manager.	Section <i>Establish LAN connection and login to Local Device Manager</i> [▶ page 31]
3	Set local system time.	Section <i>Set system time</i> [▶ page 39]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section <i>Network Proxy settings</i> [▶ page 72]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section <i>Docker Network Settings</i> [▶ page 104]
6	Optional: Configure netFIELD OS firewall. <b>Note:</b> By default, the internal netFIELD OS firewall allows all traffic ("trusted zone"). When you assign an interface or subnet to the drop or block zone, make sure that you open the ports that are used by your application containers.	Section <i>Firewall</i> [▶ page 62]
7	Open Standard Docker and deploy and run container images.	Section <i>Standard Docker</i> [▶ page 111]

Table 12: Tasks for commissioning the device (Standard Docker user)

## 5.2 Mounting

### 5.2.1 Attaching LED sticker (optional)

Each Real-Time Ethernet protocol uses its own names for the LED indicators. Therefore, an LED sticker with the names of the respective RTE protocol is included in the delivery of the device. Stick the sticker of the RTE protocol to be used onto the shield of the **Fieldbus** interface of the device.

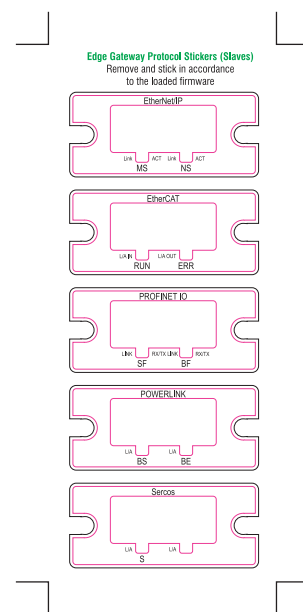


Figure 8: LED sticker



## 5.2.2 Mounting

- Mount the device with four screws into the control cabinet.

The figure shows the distance of the mounting holes:

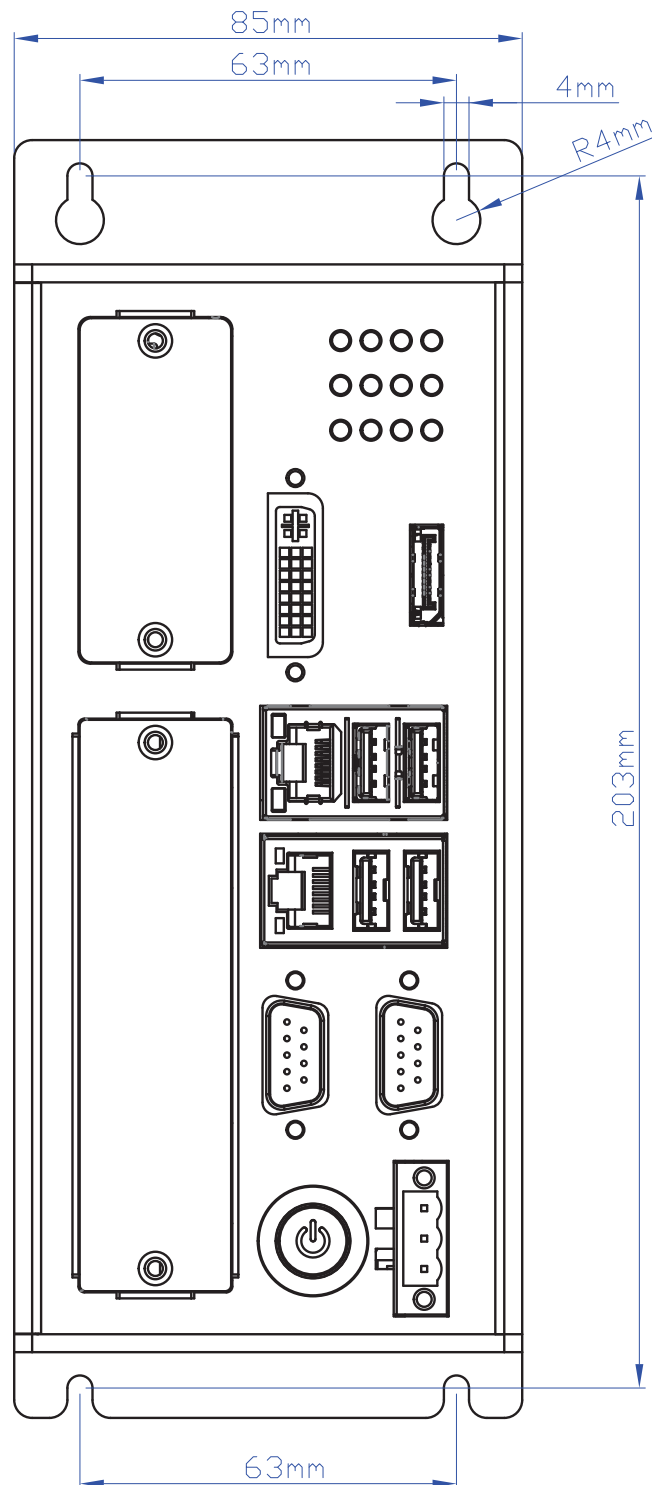


Figure 9: Mounting holes

### 5.2.3 Connecting Voltage supply

- After mounting, connect the 24 V supply voltage to the device (see position (11) in section *Positions of the interfaces* [▶ page 16]).

---

**NOTICE****Device Destruction by Exceeding the Allowed Supply Voltage!**

The supply voltage must not exceed 30 V; otherwise the device will be damaged.

---

## 5.3 Establish LAN connection and login to Local Device Manager

### 5.3.1 Overview

You have two possibilities to establish an initial LAN connection with the **Local Device Manager** (which is the web-based management GUI of the device):

- Via DHCP at LAN port 1 (eth0).  
(“Fallback” at LAN port 1 is *IPv4 link local*.)
- Via direct (one-to-one) connection at LAN port 2 (eth1)

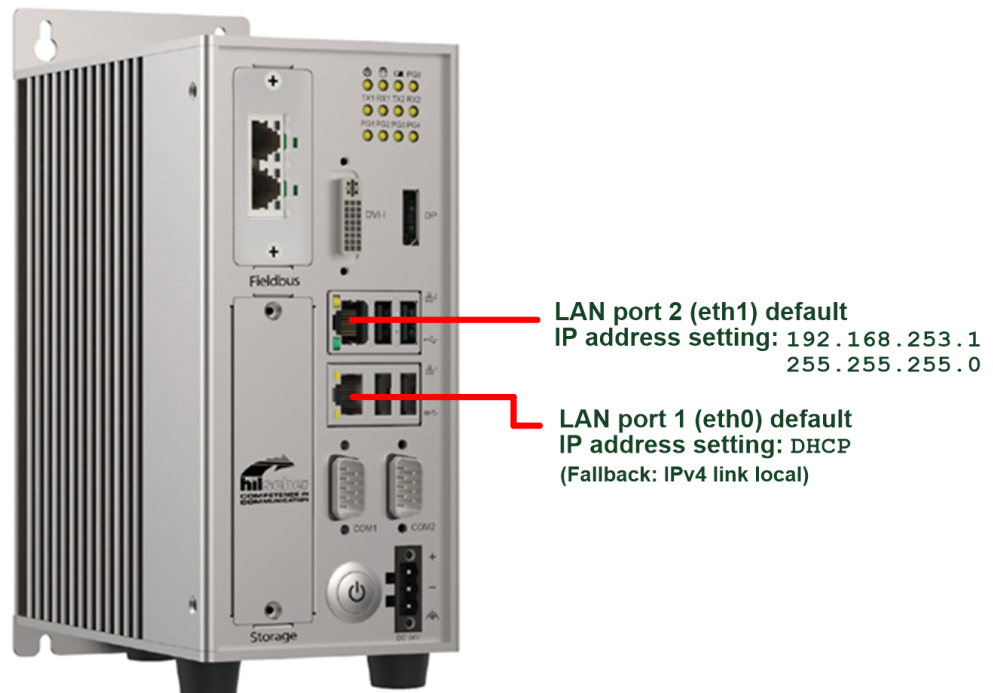


Figure 10: Factory IP address settings of LAN interfaces



#### Note:

The device contains a certificate issued by Hilscher. Therefore, your browser will probably issue an "unsecure connection" warning message when connecting to the device for the first time.

You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).

On the **Certificate** page of the device's **Local Device Manager**, you can upload your own certificate to the device.

Note that the automatically created certificate is valid for one year.

On the **Certificate** page of the **Local Device Manager**, you can upload your own certificate to the netFIELD OS. The corresponding root certificate should be rolled out on each of your PC/devices that you use for connecting to the netFIELD OS.

### 5.3.2 Using DHCP server


In its state of delivery, port 1 (eth0) of the LAN interface of the device is set to DHCP mode.

If a DHCP server is available in your local IT network, you can thus use the DHCP service it to assign an IP address to the LAN interface of the device.

**Note:**

If the device realizes that no DHCP service is available, it resets the port 1 (eth0) LAN interface address to *IPv4 link local* mode (“fallback” setting). *IPv4 link local* uses the address range from 169.254.0.0 to 169.254.255.255.

The device outputs the *IPv4 link local* address at its display interfaces, therefore you can connect a monitor at one of the display interfaces (e.g. DisplayPort) to find out the exact address.

- Make sure that a DHCP service is available in your local network.
- Plug an Ethernet cable into the LAN port <sup>1</sup> on the front panel of the device (see position (7) in section *Positions of the interfaces* [▶ page 16]), to connect it to your local network and to the DHCP server.
- Your device should now automatically obtain an IP address from the DHCP server. This may take a few minutes.  
If you know the IP address that the DHCP server has assigned to your device, you can now access the **Local Device Manager** directly by entering the assigned IP address into the address bar of your web browser. If you do not know the IP address, you can use the Windows network environment (see “Alternative A” below) or the “host name” of the device (see “Alternative B” below) to connect with it.

**Note:**

The device outputs its hostname and the IP address (which it has received from the DHCP server) at its display interfaces. Thus, connecting a monitor to one of its display interface (see positions (3) and (4) in section *Positions of the interfaces* [▶ page 16]) allows you to check the assigned IP address.

In case no DHCP service is available, the “fallback” IPv4 link local address of eth0 interface will also be output at the display ports.

- Enter into the address bar of your browser the IP address that the DHCP server has assigned to the device.

- Your browser connects to the **Local Device Manager**, which is the graphical user interface of the device.

**Note:**

The device contains a certificate issued by Hilscher. Your browser will therefore issue an "unsecure connection" warning message before directing you to the Sign-In page of the Local Device Manager.

You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).

Note that the automatically created certificate is valid for one year.

On the **Certificate** page of the **Local Device Manager**, you can upload your own certificate to the netFIELD OS. The corresponding root certificate should be rolled out on each of your PC/devices that you use for connecting to the netFIELD OS.

**Alternative A: Connecting via Windows network environment**

Because the device supports the UPnP technology (Universal Plug and Play), it will be displayed in the **Windows** network environment panel after having received its IP address from the DHCP server. This allows you to connect to it by simple mouse-click.

**Note:**

Please make sure that the network discovery feature on your Windows PC is enabled for your security zone and that your PC and the device are located within the same subnet.

Note also that if a blocking or dropping zone was assigned to the LAN interface in the firewall, UPnP only works if port 80 (http) is allowed by your firewall settings.

- To display all devices in the network, open your **Windows Explorer** and select **Network**.
- You will find the device listed under **Other Devices**:



NIOT-E-TIJCX-GB-RE  
(=0000000000000000)

- Double-click this entry to connect to the **Local Device Manager** of the device.

**Alternative B: Connecting via host name**

- As a second alternative, you can also connect to the **Local Device Manager** by entering the device's host name into the address bar of your browser. You will find the host name printed on the device label next to **DHCP**, as shown in this example:

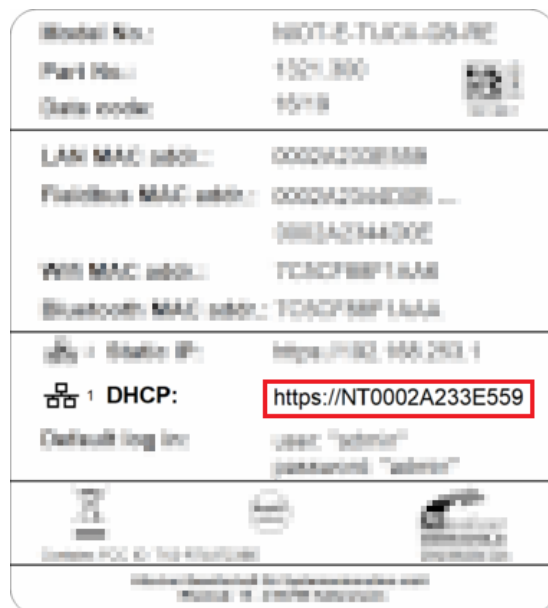


Figure 11: Host name on device label (example)

**Note:**

Your PC and your device must be located in the same subnet.

### 5.3.3 Establishing one-to-one connection to device (without DHCP server)

If no DHCP server is available in your network, you can connect your PC or notebook by Ethernet cable directly to the port 2 (eth1) LAN interface of the device (upper RJ45 socket of the two LAN interfaces).

For this, you must set an IP address on your PC or notebook that is compatible with the preset IP address and subnet mask of the port 2 (eth1) LAN interface of the gateway.

In its state of delivery, the preset IP address of the port 2/eth1 LAN interface is 192.168.253.1, the subnet mask is 255.255.255.0.

1. Connect Ethernet cable.
  - Use an Ethernet cable to connect the port 2 (eth1) LAN interface (upper socket) directly to your PC or notebook:
2. Set IP address on your PC or notebook (under Microsoft Windows).
  - Open the Windows **Control Panel**. (**Start** menu > **Windows System** > **Control Panel**)
  - In the **Control panel**, select **Network and Internet**, then **Network and Sharing Center**.
  - In the **Network and Sharing Center**, select **Change adapter settings**.
  - In the **Network Connections** window, double-click the name of your direct network connection, e.g. **Local Area Connection** or **Ethernet**. (The name of the network connection may be different on your PC.)
  - In the **General** dialog window, click **Properties**.
  - In the **Networking** tab of the **Properties** dialog window, double-click **Internet Protocol Version 4 (TCP/IPv4)**
  - In the **General** tab, set IP address 192.168.253.2 and subnet mask 255.255.255.0.

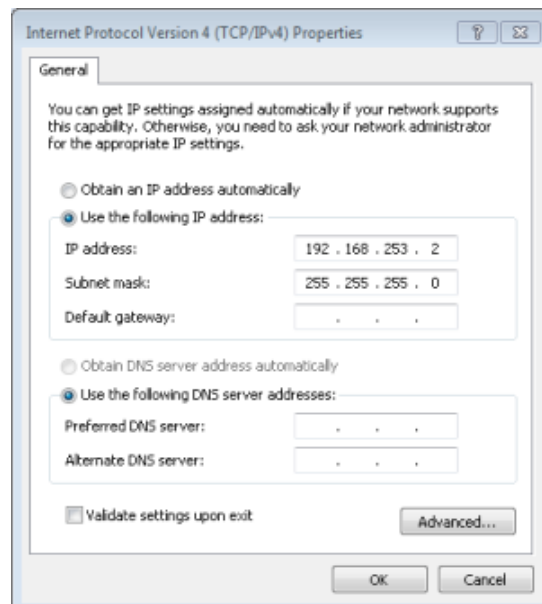


Figure 12: Setting IP address under Windows for direct LAN connection

- Click **OK** and then **Close**.

3. Open browser and connect to device.
  - You can now access the device from your PC or notebook via web browser by entering the following address into the address bar of your browser:  
`https://192.168.253.1`
  - A connection is established and the Local Device Manager opens in your browser window.

### 5.3.4 Login to Local Device Manager

**Note:**

When connecting to the device for the first time, your browser will probably issue a security warning before displaying the Login screen of the Local Device Manager.

You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an “exception rule” for this website).

Note that the automatically created certificate is valid for one year. On the **Certificate** page of the **Local Device Manager**, you should upload your own certificate to the netFIELD OS. The corresponding root certificate should be rolled out on each of your PC/devices that you use for connecting to the netFIELD OS.

After having established a LAN connection to the device, the **Sign In** dialog of the **Local Device Manager** appears:

Figure 13: Login Device Manager

- In the **Sign In** dialog, enter the following default credentials:  
**User name:** admin  
**Password:** admin



- Read the **Disclaimer** then check the **I have read and accept the Disclaimer** box.
- Click **Sign In** button.
- For security reasons, you are now forced to change the default `admin` password immediately.
- In the **Current password** field, enter `admin` once again, then click **Sign In** button:

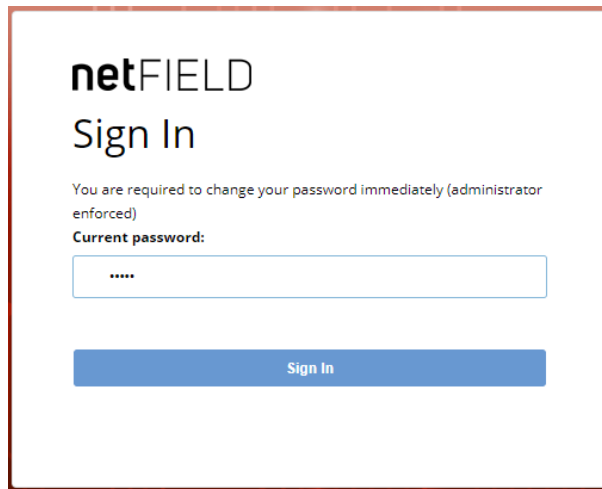
The image shows a web interface for 'netFIELD Sign In'. At the top, the text 'netFIELD Sign In' is displayed. Below it, a message states: 'You are required to change your password immediately (administrator enforced)'. Underneath this message is the label 'Current password:' followed by a text input field containing five asterisks. At the bottom of the form is a blue button labeled 'Sign In'.

Figure 14: Enter current password dialog

- The **New password** dialog opens:



The image shows the same 'netFIELD Sign In' web interface. The message 'You are required to change your password immediately (administrator enforced)' is still present. However, the label 'Current password:' has been replaced by 'New password:', and the text input field now contains seven asterisks. The blue 'Sign In' button remains at the bottom.

Figure 15: Enter new password dialog

- In the **New password** field, enter a new and safe password, then click **Sign In** button.  
Enter your new password again in the **Retype new password** field, then click **Sign In** button again.



**Note:**

You can change the password again later in the **Local Device Manager** under **Accounts > System Administrator > Set Password** or under  (user menu) > **Account Settings**.

- The **Re-Authentication required after password change** dialog opens:

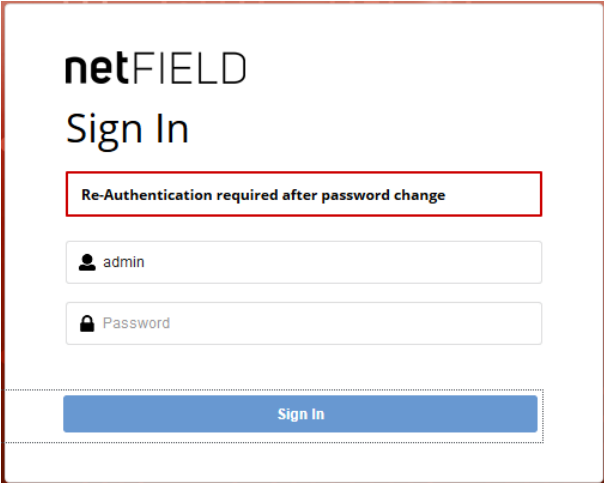
The image shows a web-based login interface for 'netFIELD'. At the top, the text 'netFIELD' is displayed in a bold, sans-serif font, followed by 'Sign In' in a slightly smaller font. Below this, a red rectangular box highlights the message 'Re-Authentication required after password change'. Underneath the message, there are two input fields: the first is labeled 'admin' with a user icon, and the second is labeled 'Password' with a lock icon. At the bottom of the form, there is a blue button with the text 'Sign In'.

Figure 16: Re-Authentication dialog

- Enter your new password once again, then click **Sign In** button
- The **Local Device Manager** opens.

## 5.4 Set system time

In the state of delivery of the device, the **Time Zone** of the system is set to **UTC** and the synchronization method (**Set Time**) to **Automatically using NTP (Network Time Protocol service)**.

**Note:**

You need `Server Administrator (admin user)` or `Time Administrator` rights to change the system time.

- To configure your local system time, open the **System** page of the **Local Device Manager**, then click the red date/time value next to **System Time**:

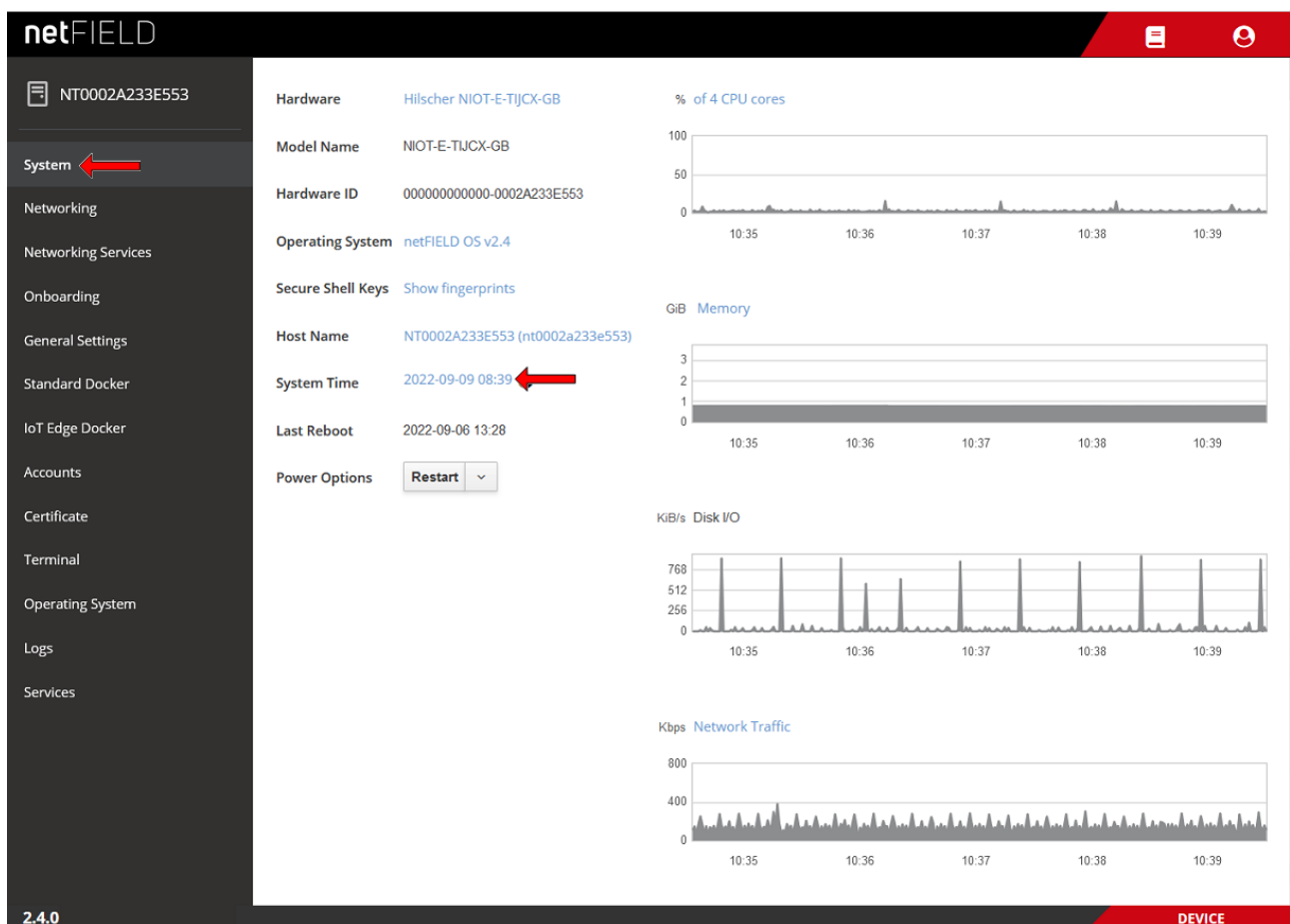


Figure 17: System time value

- The **Change System Time** dialog opens:

Figure 18: Change System Time dialog

- Click **x** button next to **Time Zone** field to delete the preset **UTC** value, then open the drop-down list and select the appropriate time zone region for your location (note that the list is searchable).
- To choose the synchronization method, choose one of the following options from the **Set Time** drop-down list:
  - **Manually:** Opens further fields for manually entering current date (yyyy-mm-dd) and time (hh:mm). Synchronization via NTP service will not be used.
  - **Automatically using NTP:** The system uses any available NTP server to obtain the correct time. (pool.ntp.org will be used by default).
  - **Automatically using specific NTP servers:** Opens further fields for entering the addresses of certain NTP servers that you want to use, e.g. ptbtime1.ptb.de.  
You can create a list of several servers; the system will use the first server in the list that delivers a valid response. Click the **+** button to add a server. Click the **x** button to remove a server.

The screenshot shows a dialog box titled "Change System Time". It contains two main sections: "Time Zone" and "Set Time". The "Time Zone" section has a text field with "Europe/Berlin" and a small "x" button to its right. The "Set Time" section has a dropdown menu currently showing "Automatically using specific NTP servers". Below this, there is a list of NTP servers. The first entry is "ptbtime1.ptb.de" with "x" and "+" buttons to its right. The second entry is "ntp.uni-regensburg.de" also with "x" and "+" buttons to its right. At the bottom of the dialog are two buttons: "Cancel" and "Change".

- Click **Change** button to save the new settings and close the dialog window.
- To update the display of the system time (to adapt it to the changed time zone), refresh the web page by pressing the **F5** key on your keyboard.

## 5.5 "Onboard" (register) device in netFIELD Cloud

### 5.5.1 Overview

If you connect your device via Internet to the netFIELD Cloud (<https://www.netfield.io>), you can install containers and manage your device from the netFIELD Portal, which is the web-based user interface of the netFIELD Cloud. You can also stream MQTT messages from your device to 3rd party applications via the *Data Service* of the netFIELD Platform, which is the backend of the netFIELD Cloud.

This section describes how to register your device in the netFIELD Portal.



---

**Note:**

Connecting your device to the netFIELD Cloud requires an account/subscription for the *netFIELD Cloud services*

<https://www.netfield.io>.

Contact your local Hilscher sales representative for information on terms and conditions.

---

Before your device can be managed from the portal, it must first complete a one-time registration process, called "onboarding".

This process is initialized by the device itself, not by the portal. There are three different onboarding methods: **Zero-Touch**, **Basic** and **Advanced**.

With the **Zero-Touch** method, the device registers itself automatically in the portal after it has been put into operation. Note that this method is implemented only in certain customer-specific Edge Device models.

With the **Basic** and **Advanced** methods, you start the registration process by locally entering authentication data in the **Onboarding** page of the **Local Device Manager**:

With the **Basic** method, you simply need to enter your netFIELD Portal's login credentials (if your user "role" in the portal entails permissions to "onboard" and "create" devices).

With the **Advanced** method (which allows onboarding in a certain separate instance of the netFIELD Portal), you must enter an `Activation Code`, an `API Key` and an `API End-Point URL`. You must research (respectively create) these parameters in the portal beforehand, then insert them in the **Onboarding** page of the Local Device Manager via clipboard ("copy and paste"). For the **Advanced** method, you therefore ideally need simultaneous access to the portal and the device in order to be able to copy the data from the portal conveniently into the corresponding fields of the **Onboarding** page of the Local Device Manager.

**Note:**

Before onboarding, make sure that your company's firewall does not block the TCP port (outgoing) of the upstream protocol (device-to-cloud communication) that you intend to use. The upstream protocol can be selected on the **Onboarding** page.

MQTT uses TCP port 8883

MQTT over WebSocket uses TCP port 443

AMQP (default protocol) uses TCP port 5671

AMQP over WebSocket uses TCP port 443

The following sections contain step-by-step instructions for the **Basic** and **Advanced** onboarding methods.

## 5.5.2 Onboarding using the “Basic” method

- In the navigation panel of the **Local Device Manager**, choose **Onboarding**.
- The **Onboarding** page opens:

The screenshot shows the netFIELD Local Device Manager interface. The left sidebar contains a navigation menu with items: System, Networking, Networking Services, Onboarding (highlighted with a red arrow), General Settings, Standard Docker, IoT Edge Docker, Accounts, Certificate, Terminal, Operating System, Logs, and Services. The main content area is titled 'Onboarding Method' and shows a 'Basic' tab selected. Below the tabs are several form fields: 'Environment' (a dropdown menu), 'Device Name' (a text input), 'E-Mail' (a text input), 'Password' (a text input), 'Device Authentication' (a dropdown menu), 'Upstream Protocol' (a dropdown menu), and a checkbox labeled 'Use Deployment Manifest'. At the bottom of the form is a blue 'Onboard' button. The top of the interface shows the netFIELD logo and some status indicators. The bottom of the interface shows the version '2.5.0.1.release' and the word 'DEVICE'.

Figure 19: “Basic” onboarding screen in Local Device Manager

- Open the **Basic** tab.
- In the **Environment** drop-down list, select the portal’s environment that you are using. Usually, this is the `Production` environment.
- In the **Device Name** field, enter the name under which the device is to be displayed in the portal.
- In the **E-Mail** and **Password** fields, enter the credentials of a user of the **portal** who possesses `createDevices` and `onboardedDevices` permissions.



### Note:

With these credentials (and the associated permissions), the device authenticates itself during onboarding in the portal and is automatically assigned to the organization or sub-organization of the user.

Ask your portal’s system administrator for the necessary credentials.

- In the **Device Authentication** field, select **Certificate based** or **Connection string based**. The certificate-based method uses digital certificates and is more secure than the connection-string-based method.
- In the **Upstream Protocol** drop-down list, select the protocol that the netFIELD OS shall use for sending data to the netFIELD Cloud (“device-to-cloud” communication).

**Note:**

Note that messaging over WebSocket causes more “overhead” per telegram. This might limit the performance if you want to stream large quantities of data.

- **MQTT** – Uses TCP port 8883
- **AMQP** – Default protocol (most commonly used). Uses TCP port 5671
- **MQTTWS** – MQTT over WebSocket. Uses TCP port 443 (same as HTTPS)
- **AMQPWS** – AMQP over WebSocket. Uses TCP port 443 (same as HTTPS)

**Important:**

Make sure that your company’s firewall does not block the TCP port (outgoing) of the selected upstream protocol.

**Note:**

If necessary, you can change the upstream protocol in the netFIELD Portal after onboarding. See section *Device Navigation: Edit device settings (Update mask)* in the operating instruction manual *netFIELD Portal*, DOC190701OIxxEN.

- In case your organization has a “Deployment Manifest” that you want to use for your device, select the **Use Deployment Manifest** option.

**Note:**

The deployment manifest causes certain software containers defined in the manifest to be automatically installed on your device. (For further information on deployment manifests, see section *Deployment Manifest* in the *netFIELD Portal* manual, DOC190701OIxxEN)

- Note: In case you are using the credentials (in the **E-Mail** and **Password** fields) of a netFIELD Portal user account that is protected by two-factor authentication (a.k.a 2FA), make sure that you have access to the corresponding “Time-based One-time Password (TOTP)” methods of the 2FA; i.e. the email account or the Authenticator app. This is because in this case you will also have to enter a 2FA passcode during onboarding.
- Click **Onboard** button to start the onboarding process.



- If the netFIELD Portal account is protected by 2FA, you will now have to select your 2FA method and enter the passcode.  
If the account is a member of other **Workspaces**, you will now also have to select the workspace in which you want to onboard the device.
- ⇒ The device connects to the portal, is registered there and assigned to your organization or sub-organization.  
If the process has been successful, the following message appears:  
**Success – Device is now onboarded.**  
From now on, the device will be listed in the portal's **Device Manager** and can be managed from there.



---

**Note:**

If the message “Something went wrong – Device has already been created” appears, the device had already been created in the **Device Manager** of the portal for the “Advanced” onboarding method.

In this case you can either use the “Advanced” onboarding method, or you can delete the device in the portal, and then start the “Basic” onboarding procedure here locally for a second time.

---

### 5.5.3 Onboarding using the “Advanced” method

#### Requirements

- You are logged-in to the Local Device Manager.
- You are also logged-in to the netFIELD Portal.
- You possess the following rights as portal user: `createDevices`, `onboardedDevices` and `getKeys`.

#### Step-by-step instructions

1. Copy **Hardware ID**.
  - In the navigation panel of the **Local Device Manager**, choose **Onboarding**, then open **Advanced** tab:

The screenshot shows the netFIELD Local Device Manager interface. On the left, a navigation sidebar lists various settings, with 'Onboarding' highlighted by a red arrow. The main panel displays the 'Onboarding Method' section, where the 'Advanced' tab is selected. A red arrow points to the 'Hardware ID' field, which contains the value '000000000000-0001C02E1F11'. Other fields visible include 'API Endpoint', 'API Key', 'Activation Code', 'Device Authentication', and 'Upstream Protocol'. An 'Onboard' button is located at the bottom of the form.

Figure 20: Research Hardware ID

- Select the **Hardware ID** and copy the string to your clipboard.
- Open a new tab in your browser and change to the portal, but do not close the connection to the **Local Device Manager** of your device in your first browser tab.

2. Add the device in the portal and create **Activation Code**.
  - In the portal, open the **Device Manager**.
  - On the start page (**Manage your devices**) of the **Device Manager**, select **+ Add** button.
  - The **Add Device** mask opens:

Figure 21: Add device mask in netFIELD Portal

- Copy the device's hardware ID from your clipboard into the **Hardware ID** field.
- In the **Name** field, enter a name for your device (optional but recommended).



For information on how to configure these parameters, see section *Device Navigation: Edit device settings (Update mask)* in the *netFIELD Portal* manual (DOC190701OIxxEN).

- Click **Next** button.
- The **Proxy Settings** tab opens.
- Use the default settings, if no proxy server is used. If a proxy server is used, enter the proxy settings.
- Click **Next** button.
- The **Remote Control Settings** tab opens.
- You can keep the default settings. If necessary, you can reconfigure these parameters in the Portal later, after onboarding.

- Click **Next** button.
- The **Environment Variables** tab opens.
- You can keep the default settings. If necessary, you can reconfigure these parameters in the Portal later, after onboarding.
- Click **Create** button.
- The mask closes, and the **Overview** page of the newly created device opens, showing the **Activation Code** that you will have to enter locally on your device:

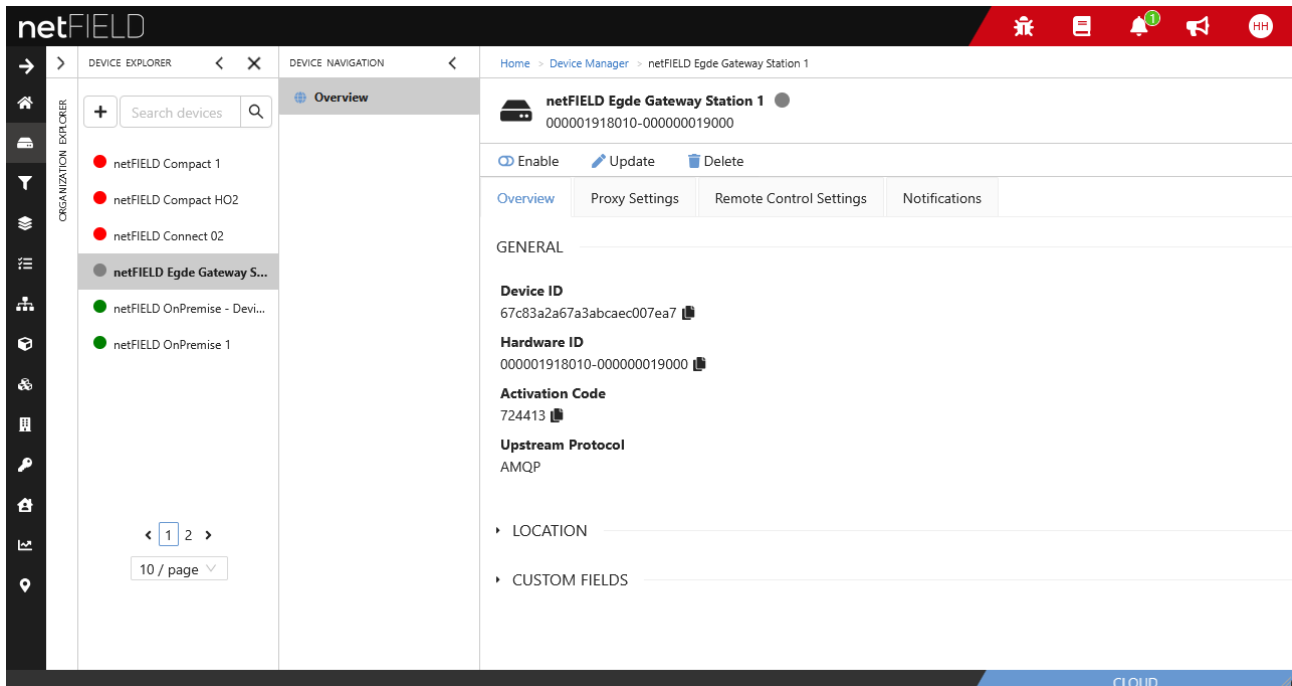


Figure 22: Activation Code in portal

- Copy the **Activation Code** to your clipboard.

3. Enter onboarding parameters in Local Device Manager.
  - Go back to the **Onboarding > Advanced** page in the **Local Device Manager** of your device.

The screenshot displays the 'netFIELD' Local Device Manager interface, specifically the 'Advanced' tab of the 'Onboarding' section. The left sidebar lists various system settings, with 'Onboarding' selected. The main area contains the following fields:

- Onboarding Method:** --
- Status:** --
- API Endpoint:** --
- Device Authentication Method:** --
- Hardware Id:** --
- Environment:** --
- Hub:** --

Below these are tabs for 'Basic' and 'Advanced', with 'Advanced' selected. The 'Advanced' tab contains:

- API Endpoint:** A text field containing 'api.netfield.io'.
- API Key:** A password field with a masked key.
- Hardware ID:** A text field containing '000001918010-000000019000'.
- Activation Code:** A text field containing '724413'.
- Device Authentication:** A dropdown menu set to 'Certificate based'.
- Upstream Protocol:** A dropdown menu set to 'AMQP'.
- ☐ Use Deployment Manifest

At the bottom left is an 'Onboard' button. The bottom status bar shows '2.5.0.0.release' on the left and 'DEVICE' on the right.

Figure 23: Advanced Onboarding tab in device

- In the **API Endpoint** field, enter the URL of the REST-API interface of the portal.  
For the Hilscher *netFIELD Portal*, this is: `api.netfield.io`  
If you are using a different instance of the portal, ask your portal's system administrator for the URL.
- In the **API KEY** field, enter an API Key that possesses the right to onboard devices. (See *Side note: How to copy an API Key for onboarding* below).
- Copy the activation code (which you have created in step 2) into the **Activation Code** field.
- In the **Device Authentication** field, select **Certificate based** or **Connection string based**. The certificate-based method uses digital certificates and is more secure than the connection-string-based method.
- In the **Upstream Protocol** drop-down list, select the protocol that the netFIELD OS shall use for sending data to the netFIELD Cloud ("device-to-cloud" communication).



**Note:**

Note that messaging over WebSocket causes more "overhead" per telegram. This might limit the performance if you want to stream large quantities of data.

- **MQTT** – Uses TCP port 8883
- **AMQP** – Default protocol (most commonly used). Uses TCP port 5671
- **MQTTWS** – MQTT over WebSocket. Uses TCP port 443 (same as HTTPS)
- **AMQPWS** – AMQP over WebSocket. Uses TCP port 443 (same as HTTPS)

**Important:**

Make sure that your company's firewall does not block the TCP port (outgoing) of the selected upstream protocol.

**Note:**

If necessary, you can change the upstream protocol in the netFIELD Portal after onboarding. See section *Device Navigation: Edit device settings (Update mask)* in the operating instruction manual *netFIELD Portal*, DOC190701OIxxEN.

- In case your organization has a "Deployment Manifest" that you want to use with your device, select the **Use Deployment Manifest** option.

**Note:**

The deployment manifest causes certain software containers defined in the manifest to be automatically installed on your device. (For further information about deployment manifests, see section *Deployment Manifest* in the *netFIELD Portal* manual, DOC190701OIxxEN)

- Click **Onboard** button, to start the onboarding process.
- ⇒ The device connects to the portal and is registered there. If the process has been successful, the following message appears: **Success – Device is now onboarded.**

**Side note: How to copy an API Key for onboarding**

For onboarding by "Advanced" method, you need an API Key, which you can copy to your clipboard in the **API Key Manager** of the netFIELD Portal, and then paste into the Local Device Manager of your device during onboarding.

The key must have the permissions (i.e. Security Level **org+ch** or **org**) for the **onboardedDevices** and **createDevices** functions of the **devices** resource of your organization.

You can use an already existing API key (which, for example, was created by the system administrator) or create a new API key yourself.

For information on how to create a new API Key, see section *Create/edit API key* in the *netFIELD Portal* manual, DOC190701OIxxEN.

API Keys are administered in the **API Key Manager** of the portal.

For accessing existing keys in the **API Key Manager**, you must at least have the permission to use the **getKeys** function of the **keys** resource.

For creating a new key, you must have the permission to use the **createKeys** function of the **keys** resource.

- Open the **API Key Manager** in the portal.
- On the start page (**Manage your API Keys**), select from the list a key that allows the **onboardedDevices** function of the **devices** resource.

To find out the permissions of an API Key, click on the key in the list, then open its **Permissions** tab. The permission `onboardedDevices` is required.


- To copy the API Key in order to use it in the Local Device Manager of the device for the advanced onboarding process, change into the **General** tab.
- In the **General** tab, click  icon to copy the key to your clipboard:



Figure 24: Copy key to clipboard

- Go to the **Onboarding > Advanced** page in the **Local Device Manager** of your local device and insert the key into the **API KEY** field.

## 6 Local Device Manager

### 6.1 Overview

The **Local Device Manager** is the web GUI for configuring and administering the netFIELD OS of your device. It is a customized version of the *Cockpit* web administration console for Linux server.



#### Note:

The Local Device Manager does not allow you direct management of the OT network connectivity (Real-Time Ethernet or “Fieldbus”) of your device, because the OT network is handled by a separate communication controller, the netX. From the netFIELD OS/Local Device Manager side, the netX can only be accessed via its Dual-Port Memory and the cifX API. This requires the deployment of special netFIELD application containers (featuring the required cifX API functions) on the device's **IoT Edge Docker**.

#### Description of the GUI

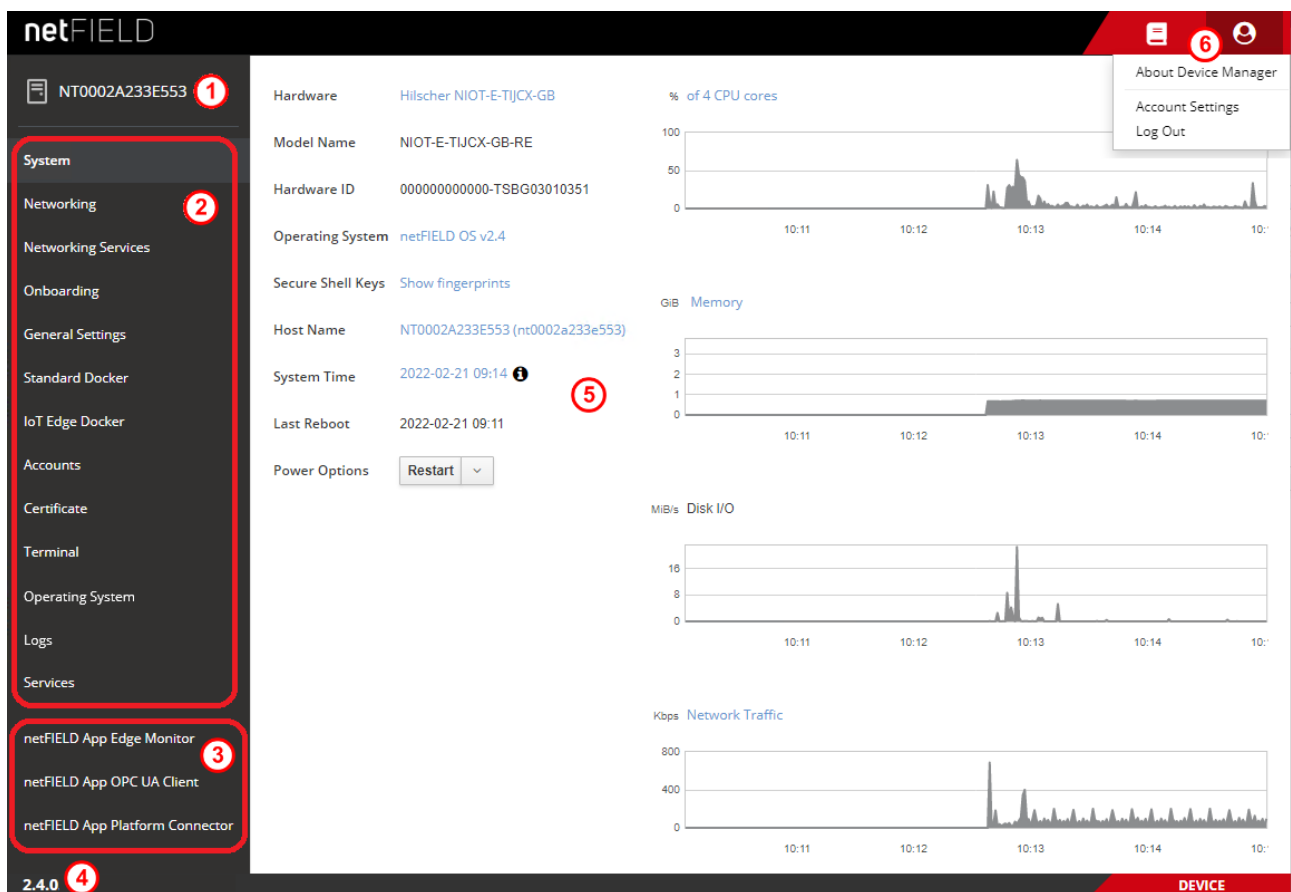


Figure 25: Overview Local Device Manager

(1) “Pretty” host name of the device (can be adapted by the user, see subsection *Host Name* in section *System* [▶ page 54])

(2) In the navigation panel on the left of the screen, you can select the available “standard” management pages.





(3) Many Hilscher netFIELD application containers like e.g. *netFIELD App Platform Connector* or *netFIELD App OPC UA Client* provide their own configuration GUI, which can be selected here (if deployed on your device). Note that the functions and the GUI of individual containers are not described in this manual. Consult the documentation of the individual container for more information.

(4) Shows the version of the netFIELD OS/Local Device Manager.

(5) Main screen displaying the management page that you have selected in the navigation panel.

Note that if a label, text or value is highlighted in blue, it contains a clickable link that opens a page or dialog box with further details or configuration options.

(6) Toolbar in the upper right corner of the screen:

- The  icon opens a page in the netFIELD Portal where you can find the currently available netFIELD documentation (including this user manual).
- The  icon opens the user menu:
  - **About Device Manager:** Shows information about the Local Device Manager.
  - **Account Settings:** Opens the configuration page of your currently used account (i.e. the account you are currently logged in with). See also *Accounts* [► page 123] section for further information.
  - **Log Out:** Logs you out of the Local Device Manager

## 6.2 System

The **System** page allows you to configure and monitor basic system parameters and resources.

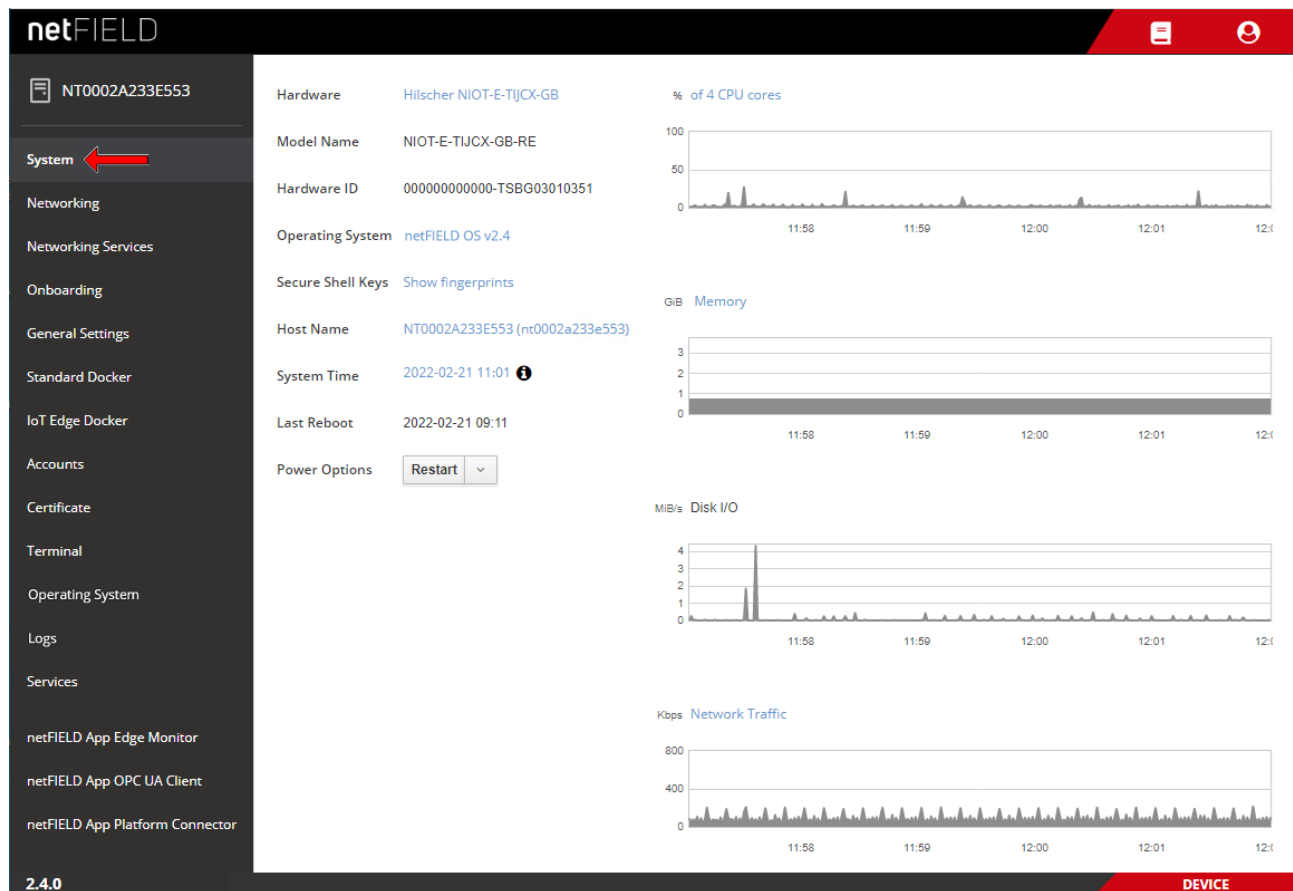


Figure 26: System page in Local Device Manager

### Hardware

Click on the blue name to open a page showing technical details about your device's hardware like processor(s), RAM, mass storage, OS kernel, temperature and PCI devices.

### Model Name

Model name of the device

### Hardware ID

Unique identification number of the device. To match the required format, the ID may be "filled up" with zeros. This ID can also be used in the netFIELD Portal as unique identifier of your device.

### Operating System

Name and version of the installed netFIELD OS. Click on the blue name to open a window showing further details (i.e. the exact firmware version).

## Secure Shell Keys

Click on **Show fingerprints** to open a window displaying the Machine SSH Key Fingerprints.

## Host Name

The host name identifies the device in a LAN or Wi-Fi network and can be used for connecting to the device. By default, the name consists of the letters `NT` followed by the MAC address of the LAN port of the device. If you want to change it, click on the blue name to open the **Change Host Name** dialog window.

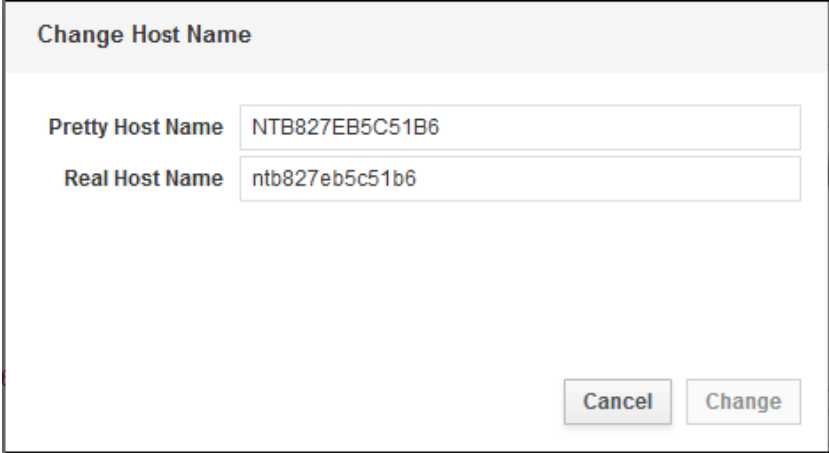
A dialog window titled "Change Host Name" with a light gray header. It contains two text input fields. The first field is labeled "Pretty Host Name" and contains the text "NTB827EB5C51B6". The second field is labeled "Real Host Name" and contains the text "ntb827eb5c51b6". At the bottom right of the dialog, there are two buttons: "Cancel" and "Change".


Figure 27: Change host name dialog

**Pretty Host Name:** Free-text (UTF8) name for presentation to the user. Will be displayed e.g. on top of the navigation panel in the Local Device Manager or as label in your browser tab.

**Real Host Name:** Equivalent to the transient host name which can be used to connect to the device and which can be changed by DHCP or mDNS at runtime. Can contain lower-case characters, digits, dashes and periods (with populated subdomains). Setting this value takes immediate effect and does not require a restart.

## System Time

Shows the system time of the device. By default, the time zone is set to UTC and the actual time is synchronized by an NTP (Network Time

Protocol) service. Hovering over the  icon opens a tooltip displaying details about the current settings, like e.g. the NTP service that was used for the synchronization.

For instructions on how to change the time settings, see section *Set system time* [► page 39].

## Last Reboot

Shows date and time of the last reboot (restart) of the netFIELD OS.

## Power Options

Use the drop-down button to restart or shutdown the netFIELD OS and the device.

To restart the device after shutdown, press the power button of the device (see position (12) in section *Positions of the interfaces* [► page 16]).

## CPU cores

The graph shows the combined load of the CPUs of the device during the last five minutes. Click on the blue % **of 4 CPU cores** link to open a page showing the share of certain process categories:

- Nice (`ni`): User space processes that have been “niced” (i.e. “prioritized”).
- User (`us`): User space processes (i.e. applications and processes that do not belong to the kernel processes)
- Kernel (`sy`): Linux kernel processes
- I/O Wait (`wa`): Idle while waiting for an I/O operation to complete

## Memory

The graph shows the usage of the RAM memory of the netFIELD OS during the last five minutes. Click on the blue **Memory** link to open a page showing actually used memory and cached memory.

## Disk I/O

The graph shows the data access rate to the mass storage drive/disk/device during the last five minutes.

## Network Traffic

The graph shows the network traffic rate during the last five minutes. Click on the blue **Network Traffic** link to open the **Networking** page providing further details about the physical and virtual network interfaces of the device.

## 6.3 Networking

### 6.3.1 Overview

The **Networking** page allows you to configure IP parameters and to monitor the amount of traffic of the physical and virtual/logical (i.e. of containers) network interfaces that are managed by the netFIELD OS. You can also configure your firewall and HTTPS/HTTP/FTP Proxy server settings here.

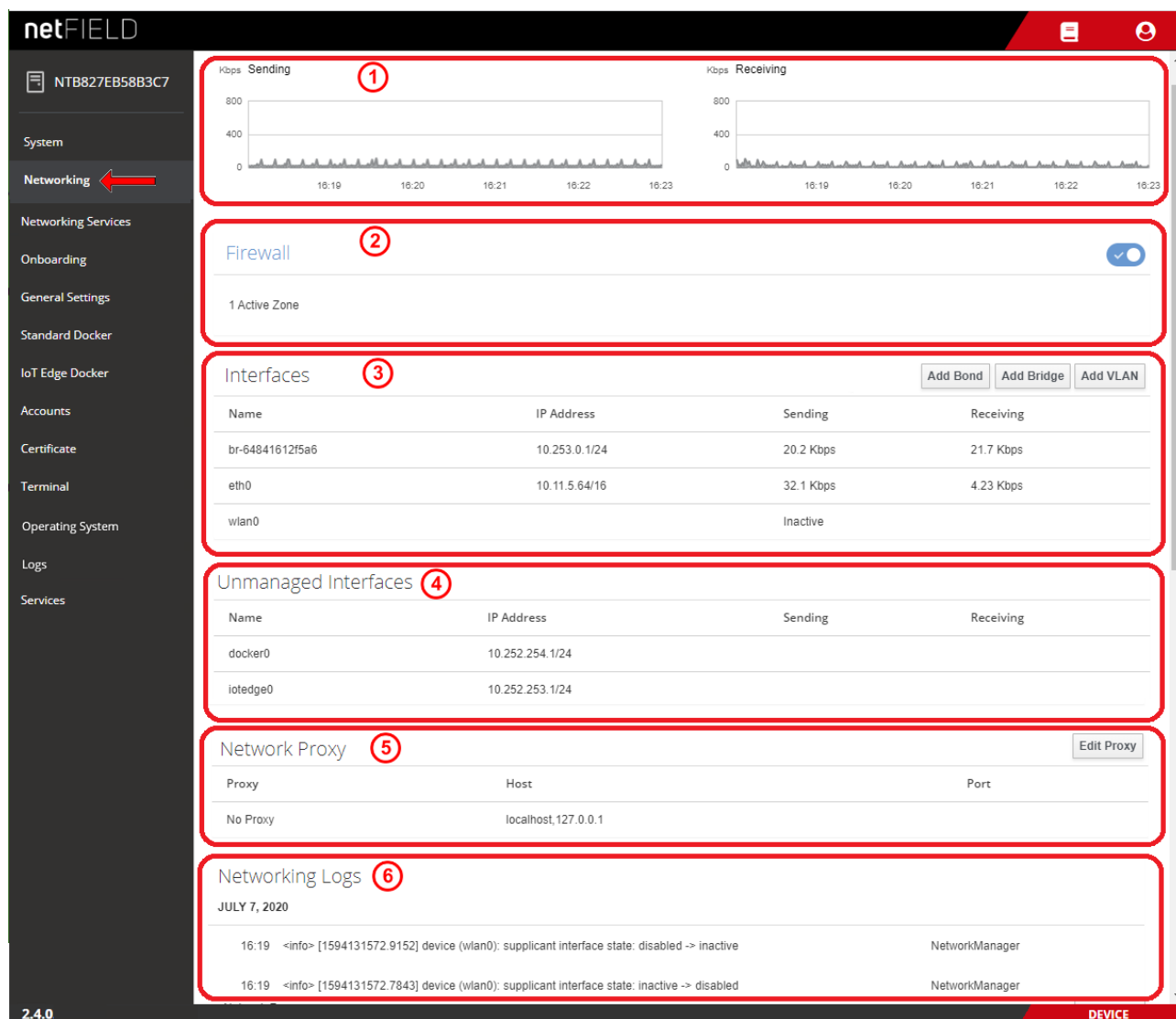


Figure 28: Networking page


The **Networking** page features the following sections:

#### Sending/Receiving

The graphs in the section on top (1) show the amount of network traffic (sending and receiving) for the last five minutes.

## Firewall

The **Firewall** section (2) shows the number of active firewall zones.

With the  toggle switch, you can deactivate the firewall all together. Click on the blue **Firewall** link to open the firewall configuration page. (See section *Firewall* [► page 62] for more details.)

## Interfaces

The **Interfaces** section (3) lists the interfaces that can be managed by the netFIELD OS, and shows their basic parameters (IP address, current volumes of sending and receiving).

**br-xxxxxxxxxxxx** : This is a “bridge” that was automatically created by the IoT Edge Docker after “onboarding” the device.

**eth0**: This is the port 1 LAN interface of the device (for the location of the LAN connector on the device, see position (7) in section *Positions of the interfaces* [► page 16]).

**eth1**: This is the port 2 LAN interface of the device (see position (5) in section *Positions of the interfaces* [► page 16]).

**wlan0**: This is the Wi-Fi interface of the device.

By clicking here, you can open its basic configuration page, where you can enable/disable the Wi-Fi interface and configure its IP address. Note that the Local Device Manager features a special Wi-Fi configuration page under **Networking Services > WiFi**, where you can make all other necessary configuration settings (see section *Wi-Fi* [► page 78]).

**cifx0**: This is the Standard TCP/IP interface of the OT network connectors of the device (see positions (13) and (15) in section *Positions of the interfaces* [► page 16]).



---

### Note:

For information on how to enable the **cifx0** interface for TCP/IP acyclic services, see section *OT Interface (Using the cifx0 interface or RTE)* [► page 94].

---

### Open details page of Ethernet interface (e.g. for changing IP settings)

- You can click on an interface, e.g. **eth0**, in order to display further details or to configure its IP settings:

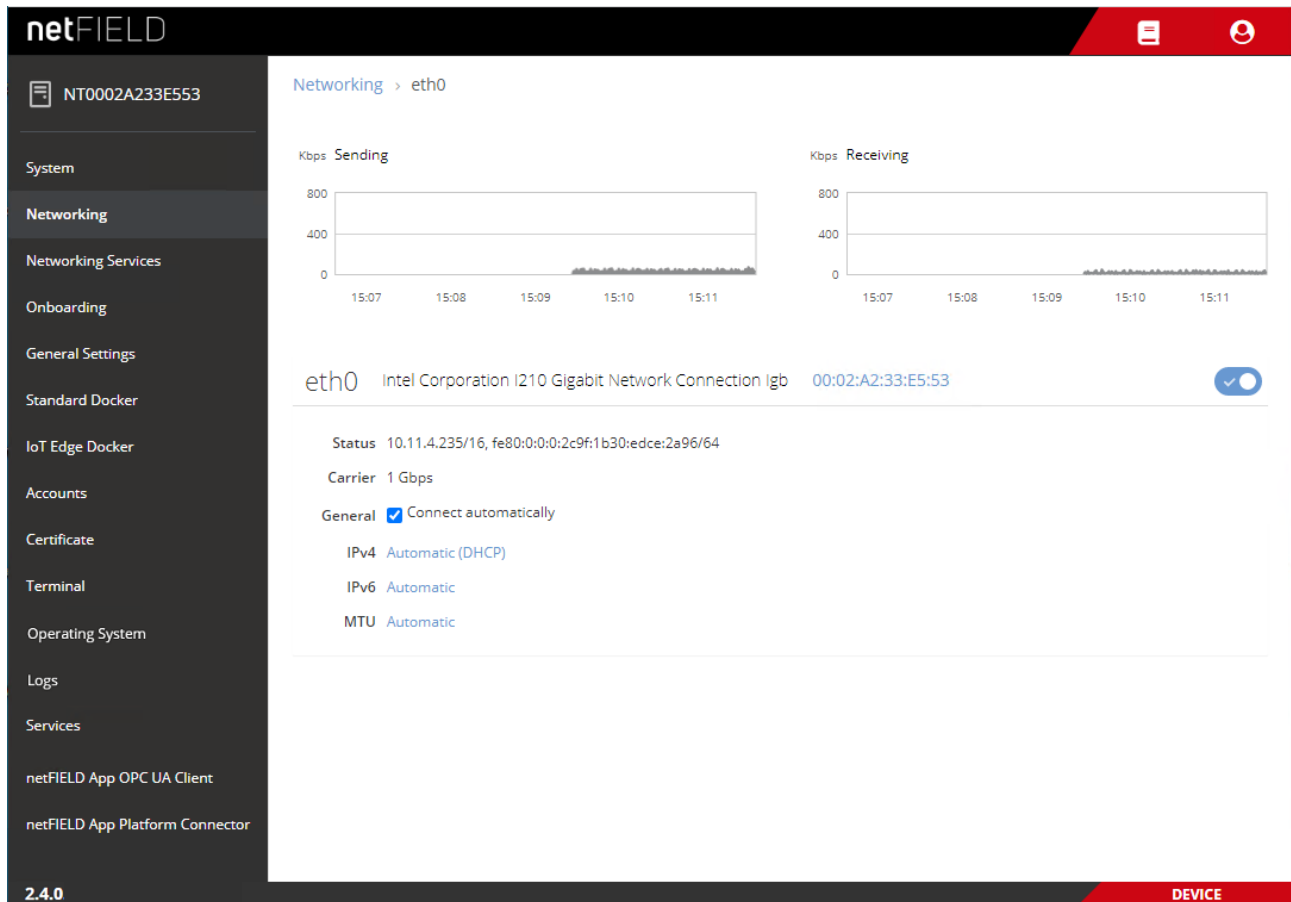



Figure 29: Details of LAN interface (eth0)



#### Important:

Be careful not to deactivate the **eth0** and the **eth1** LAN interfaces by switching them off with the  toggle switch. Once you have deactivated an interface, the connection to your device via this interface will be lost. If you have deactivated both LAN interfaces (and if you cannot reach the device via Wi-Fi), you will have to perform either a device recovery in order to be able to reconnect again (see section *Device recovery via USB* [➤ page 143]), or you can reactivate the interface via terminal (you have to connect a display and a keyboard to the device for accessing it via terminal). To query the connectivity states of the interfaces via terminal, use:

```
sudo nmcli dev status
```

To reactivate an interface (e.g. eth0) via terminal, use:

```
sudo nmcli con up ifname eth0
```

- To change the IP settings, e.g. to set a fixed IP address, click on **Automatic (DHCP)** next to **IPv4**.

➤ The **IPv4 Settings** page opens.

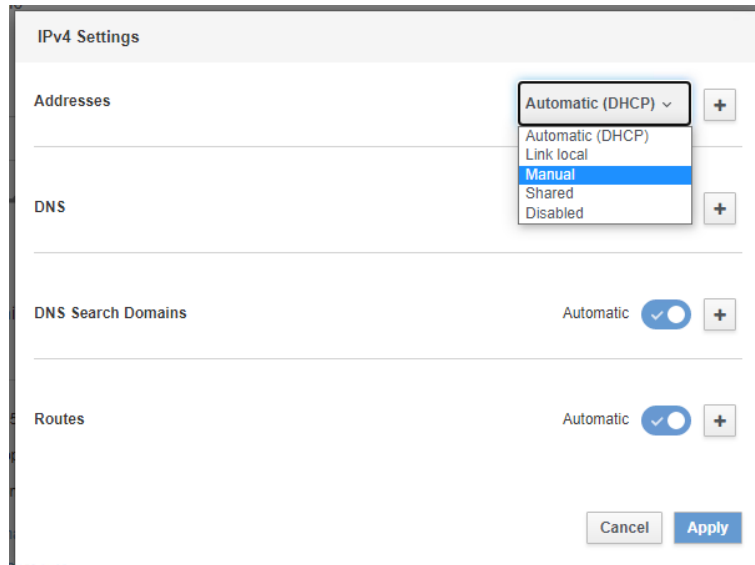


Figure 30: IPv4 Settings

➤ In the **Addresses** dropdown-list, select **Manual**.

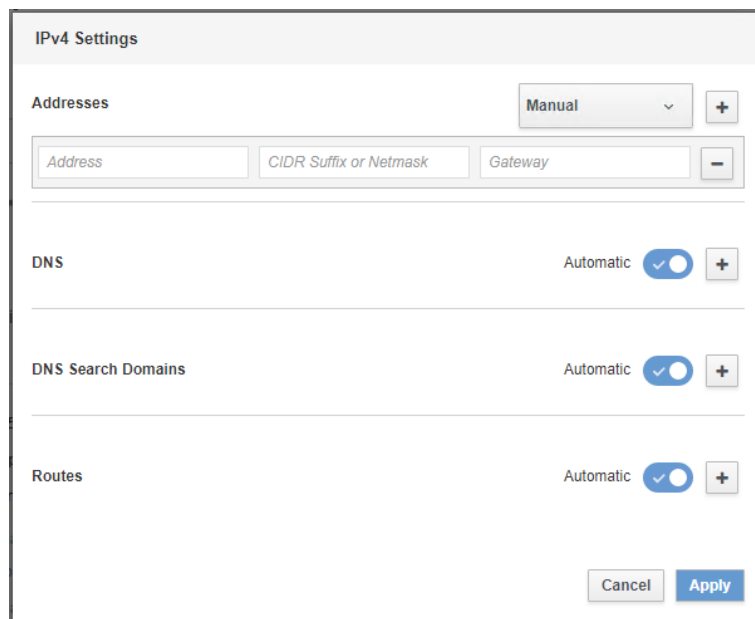


Figure 31: Manual IPv4 Settings

➤ Enter the address parameters, then click **Apply** button.

## Unmanaged Interfaces

The **Unmanaged Interfaces** section (4) lists virtual interfaces and their IP parameters (IP address, current send/receive volumes).

- **docker0**: Virtual interface (“bridge”) of the Standard Docker
- **l0tedge0**: Virtual interface (“bridge”) of the IoT Edge Docker
- **vethxxxxxxx**: Virtual interface (“virtual Ethernet device”) of a container in a Docker
- **sit0**: Tunneling protocol (“Simple internet transition”) for using IPv6 over an existing IPv4 connection.



**Note:**

The IP addresses of the “unmanaged interfaces” cannot be changed here. If you want to change the pre-configured IP address of the virtual interface of the Standard Docker (**docker0**) or of the IoT Edge Docker (**lotedge0**), e.g. because it conflicts with other IP addresses in your company network, see section *Docker Network Settings* [▶ page 104] for further information.

**Network Proxy**

The Network Proxy section (5) shows the HTTP/HTTPS/FTP proxy server settings of your netFIELD OS. Note that the **No Proxy** URIs `localhost` and `127.0.0.1` are “internal” destinations in the netFIELD OS and are therefore not to be addressed via Proxy server. They appear as **No Proxy** entries by default, even if you did not configure any Proxy server for your netFIELD OS. Do not edit or remove `localhost` and `127.0.0.1` from the **No Proxy** list.

To configure your network Proxy settings, click the **Edit Proxy** button to open the **Proxy Settings** dialog. (See section *Network Proxy settings* [▶ page 72] for more information.)

**NETWORKING LOGS**

The **NETWORKING LOGS** section (6) lists messages issued by the Network Manager of the system.

## 6.3.2 Firewall

### Overview

netFIELD OS is equipped with a firewall.

You can add firewall zones and assign interfaces and/or subnets or IP address ranges for which the rules of a zone shall apply. You can also configure “port forwarding” and define allowed services and ports that shall remain “open” in a Drop zone, NAT-Drop zone or Block zone.



#### Important:

Note that in its “state of delivery”, there is no active firewall zone configured, which means that by default, all traffic is allowed and none blocked or dropped until you have configured one or more active zone(s).



#### Note:

Be aware that containers running in the Standard Docker or in the IoT Edge Docker may require certain ports on the host system to be “open” in order to function and communicate properly.

Therefore, make sure that you add these ports to the **Allowed Services** list when you define Drop, NAT-Drop or Block zones. The required ports of a container are defined in its *Container Create Options*.

For example, the *mosquitto* container (which is an MQTT Broker) requires the TCP port 1883 for its `mqtt` service to be open.

To find out the services/ports that your containers use, go to the **Standard Docker** page respectively **IoT Edge Docker** page of the Local Device Manager and check out the container’s port settings by clicking on the corresponding image or container instance.

- To open the Firewall configuration page, click the **FIREWALL** link on the **Networking** page.

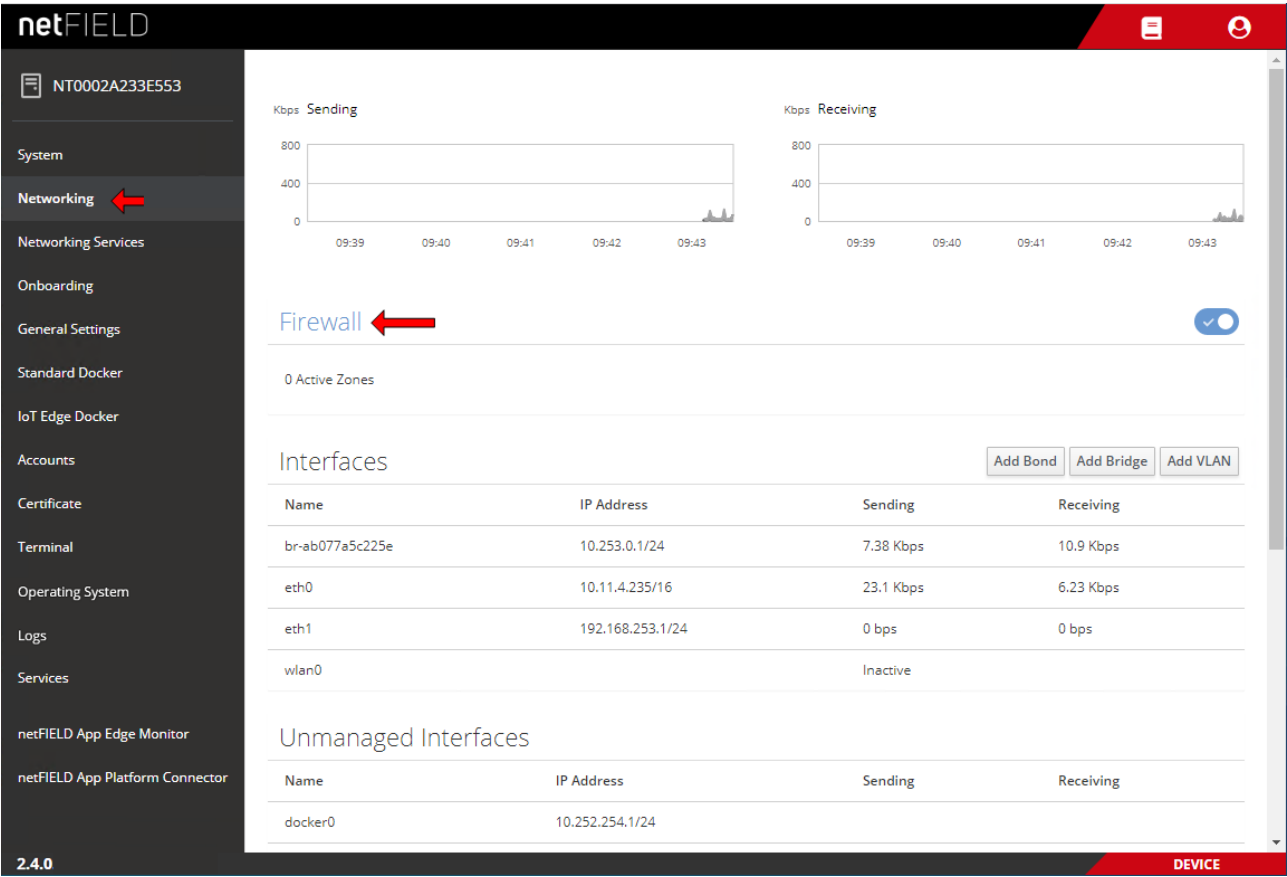


Figure 32: Open Firewall configuration page

The Firewall configuration page opens:

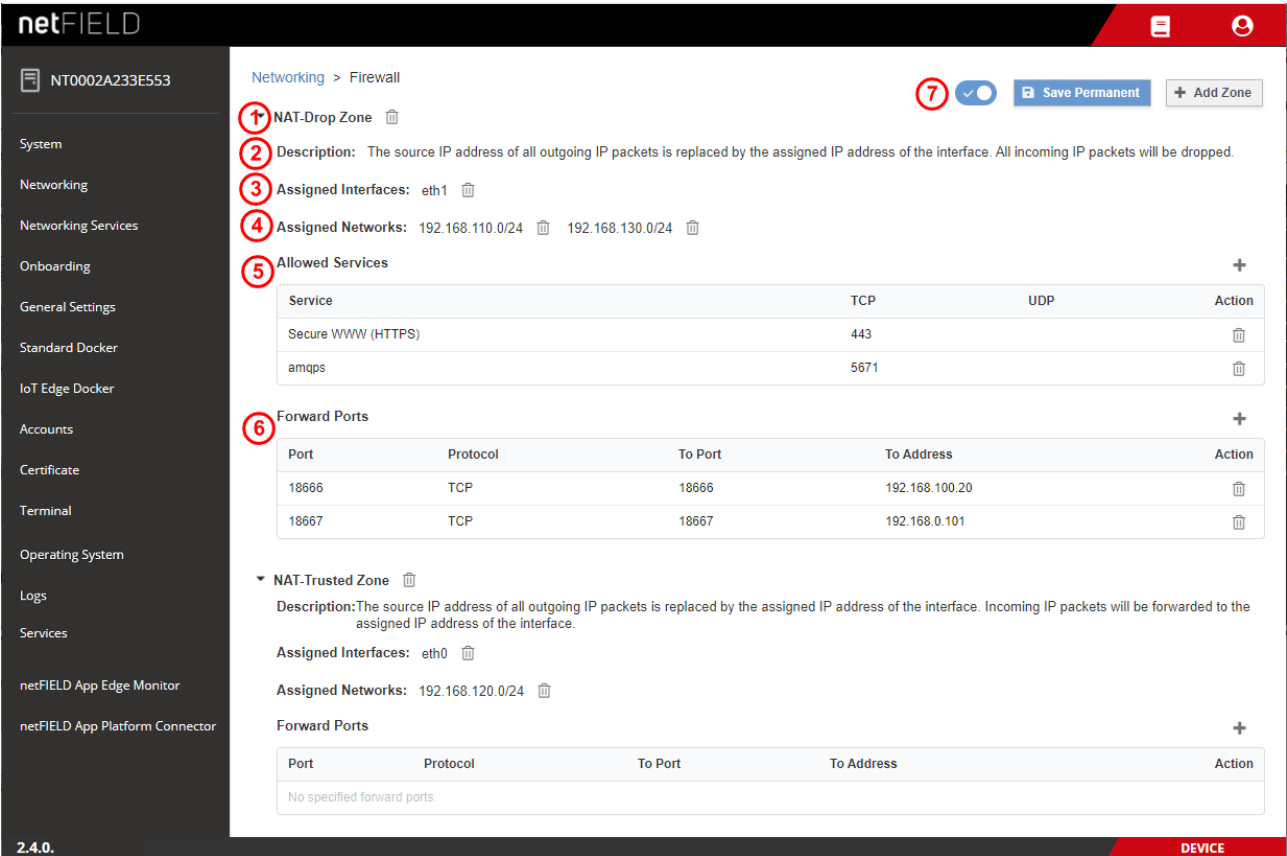




Figure 33: Elements on Firewall configuration page

## Zones

(1) All zones that have been added to your firewall configuration are listed on the **Firewall** page.

Click the  button (expand) in front of a zone's name to show the properties of the zone, like **Interfaces**, **Sources**, **Allowed Services**, **Forward ports** and a brief **Description**.

Click the  button (collapse) to hide the properties of the zone.

Zones can be removed from the firewall by clicking the  button.

You can add the following zones to your firewall by clicking the **+ Add Zone** button:

Zone *	Description
Drop	All packets reaching the interface will be “silently” dropped by default (except for the “allowed services”).
NAT-Drop	NAT = Network Address Translation, a.k.a. “masquerading”. Allows port forwarding between assigned interfaces. The source IP address of all outgoing IP packets is replaced by the assigned IP address of the interface. All incoming IP packets will be dropped by default (except for “allowed services” and forwarded ports).
Block	All packets reaching the interface will be dropped by default (except for the “allowed services”). The sender will be notified by an ICMP “unreachable” message.
NAT-Trusted	NAT = Network Address Translation, a.k.a. “masquerading”. Allows port forwarding between assigned interfaces. The source IP address of all outgoing IP packets is replaced by the assigned IP address of the interface. Incoming IP packets will be forwarded to the assigned IP address of the interface.
Trusted	All IP packets are forwarded transparently. There is no need to add allowed Services/ports to this zone because all services/ports are open anyway. Thus, there is no “Allowed Services” table for this zone.
* Sorted from “least trusted” to “most trusted”	

Table 13: Available Firewall zones

- To add a new zone or to assign new interfaces or subnet(s)/IP address range(s) to an existing zone, click **+ Add Zone** button.

➤ The **Add Zone** dialog opens:

### Add Zone

**Trust Level**  
Sorted from least trusted to most trusted

**Zones**

☐ Drop
 ☒ NAT-Drop
 ☐ Block
 ☐ NAT-Trusted
 ☐ Trusted

**Zone Description**  
The source IP address of all outgoing IP packets is replaced by the assigned IP address of the interface. All incoming IP packets will be dropped.

**Allowed Services**  
None  
The https service is automatically included

**Assign Interfaces**  
☐ cifx0
 ☐ eth0
 ☒ eth1
 ☐ wlan0

**Assign Networks**  
☒ Entire subnet of interface  
☐ Networks ⓘ

Figure 34: Add Zone dialog

Element	Description	
Trust Level	Explains the sorting of the zones under <b>Zones</b>	
Zones	Select here the zone that you want to add to your firewall configuration. If you want to assign <b>Interfaces</b> or <b>Networks</b> to an already existing zone (i.e. to a zone that has already been added to your firewall configuration), select here the corresponding zone to which you want to add the new parameters.	
Zone Description	Displays a brief description of the selected zone.	
Allowed Services	Shows the allowed services/ports of the selected zone. Note that HTTPS is allowed by default in all zones. You can add or delete allowed services to/from an existing zone in the <b>Allowed Services</b> table of the corresponding zone.	
Assign Interfaces	Select here the physical or virtual interface(s) that you want to assign to the selected zone. Note that each interface can be assigned to one zone only. Interfaces that have already been assigned to a different zone are not displayed here and thus cannot be selected here. If you want to reassign an interface from one zone to another, you will first have to remove the interface from the zone to which it is currently belonging.	
Assign Networks	Here you can define subnets or IP address ranges for which the rules of the zone shall apply.	
	Entire subnet of interface	Select this option if the rules shall apply to the entire subnet(s) of the assigned interface(s).
	Networks	Select this option to enter address ranges or subnets for which the rules of the zone shall apply. Enter the subnet mask as CIDR Suffix. Multiple entries must be separated with commas, e.g.: 192.168.1.0/24, 10.14.0.0/16

Table 14: Elements in Add Zone dialog

## Description


(2) Brief description of the function of the zone.

## Assigned Interfaces

(3) Physical or virtual interfaces that are assigned to the zone (i.e. these are the interfaces to which the rules of the zone apply).

You can assign interfaces to a zone in the **Add Zone** dialog when you add a new zone to your firewall.

Note that each interface can be assigned to *one zone* only.

Interface(s) can be removed from a zone by clicking the  button.

If you later want to add another interface to an already existing zone, proceed as follows:


- Click **+ Add Zone** button to open the **Add Zone** dialog.
- In the **Add Zone** dialog, select the existing zone in the **Zones** area.
- Select the new interface in the **Assign Interfaces** area.
- Click the **Add Zone** button in the footer.
- The **Add Zone** dialog closes and the new interface is added to the zone.

## Assigned Networks

(4) These are the subnet(s) or IP address ranges that are assigned to the zone (i.e. these are the subnet(s) respectively IP address ranges to which the rules of the zone apply).

You can assign networks to a zone in the **Add Zone** dialog when you add a new zone to your firewall. If no networks are assigned, the rules of the zone will apply to the entire subnet of the interface by default.

Note that each network can be assigned to *one zone* only.

Networks can be removed from a zone by clicking the  button.

If you later want to add networks to an already existing zone, proceed as follows:

- Click **+ Add Zone** button to open the **Add Zone** dialog.
- In the **Add Zone** dialog, select the existing zone in the **Zones** area.
- Select the **Networks** option in the **Assign Networks** area.
- Enter new subnet(s) or IP address range(s) into the **Networks** field. (Enter the subnet mask as CIDR Suffix and separate multiple entries with commas.)
- Click the **Add Zone** button in the footer.
- The **Add Zone** dialog closes and the network(s) are added to the zone.

## Allowed Services

(5) The **Allowed Services** table shows the network services and ports that remain “open” in a Drop, NAT-Drop or Block zone.



### Note:

**Secure WWW (HTTPS)/TCP port 443** is by default allowed for all zones and interfaces because this service/port is the standard means of communication of the web server of the netFIELD OS with the netFIELD Cloud. When you add a new zone, HTTPS will therefore be automatically included in the **Allowed Services** list.



### Important:

Be aware that if you delete **HTTPS** from the **Allowed Services** list, you might shut yourself out from the netFIELD OS.



Element	Description	
Service	Name of the service or alias of the custom port that is allowed in the zone.	
TCP	Number of the TCP port that is allowed in the zone.	
UDP	Number of the UDP port that is allowed in the zone.	
Action		Opens a dialog for adding allowed services respectively custom services (ports) to the zone (see below).
		Deletes the allowed service respectively port. <b>Note:</b> Deleting an allowed service/port from a Drop Zone, NAT-Drop Zone or Block Zone can cause loss of connection to your device (if the interface via which you are connected belongs to such a zone).

Table 15: Columns/elements in Allowed Services table

To add a new service respectively port to the **Allowed Services** list of a zone, proceed as follows:

- Click the **+** button above the **Action** column.



- The **Add Services** dialog opens. The dialog features a list of commonly used services and their standard TCP or UDP port numbers:

Service	TCP	UDP	Action
<input type="checkbox"/> Amanda Backup Client	10080	10080	
<input type="checkbox"/> Amanda Backup Client (kerberized)	10082		
<input checked="" type="checkbox"/> amqp	5672		
<input checked="" type="checkbox"/> amqps	5671		
<input type="checkbox"/> apcupsd	3551		
<input type="checkbox"/> Audit	60		
<input type="checkbox"/> Bacula	9101, 9102, 9103		
<input type="checkbox"/> Bacula Client	9102		
<input type="checkbox"/> RGP service listen	179		

Figure 35: Add services

- To find the service/port you are looking for, you can scroll through the list by using the scroll bar or you can enter the name of the service or the port number into the **Search** field.
- Select the service(s)/port(s) in the check box, then click **Add Services** in the footer.
- The dialog closes and the allowed services/ports are added to the zone.

- If you want to add a port that is not bound to a specific service, you can select the **Custom Service** option and enter the port number in the **TCP** respectively **UDP** field. For reference, you should also enter a name for your custom service/port in the **Name** field. You can add several ports at once by separating the entries with a comma.

**Add custom service to NAT-Drop zone**

☐ Services
 ☒ Custom Service

TCP ⓘ

6998

UDP ⓘ

UDP

Service name ⓘ \*

special service port

Cancel Add Custom Service

Figure 36: Add custom services dialog

- Click **Add Custom Service** in the footer.
- The dialog closes and the allowed custom service/port is added to the zone.

## Forward Ports

(6) The firewall supports “port forwarding”, which is commonly used together with NAT zones (NAT = Network Address Translation, a.k.a. “masquerading”); i.e. the **NAT-Drop** or the **NAT-Trusted** zone. It allows traffic arriving at a certain port of an interface to be forwarded to a certain port of another interface, e.g. of an “internal” interface like a virtual container interface (“veth”), whose IP address is not “visible” to the “outside world”.

Port forwarding settings are displayed in the **Forward Ports** table of the zone.

Element	Description
Port	Number of the port of the receiving interface from which the traffic is to be forwarded.
Protocol	Protocol used by the service/port.
To Port	Number of the port to which the traffic shall be forwarded.
To Address	IP address of the interface to which the traffic shall be forwarded.
Action	+
	Deletes the port forwarding definition.

Table 16: Columns/elements in Forward Ports table

To add a new port forwarding definition to a zone, proceed as follows:

- Click the **+** button above the **Action** column.

➤ The **Add Forward Port** dialog opens:

Figure 37: Add forward port dialog

- In the **Port** field, enter the number of the port of the receiving interface from which the traffic is to be forwarded.
  - In the **Protocol** drop-down list, select the corresponding protocol.
  - In the **To Port** field, enter the number of the port to which the traffic shall be forwarded.
  - In the **To Address** field, enter the IP address of the interface to which the traffic shall be forwarded.
  - Click the **Add Port** button in the footer.
- The **Add Forward Port** dialog closes and the new port forwarding definition is added to the existing zone.

### Control elements in main toolbar

(7) The main toolbar on top of the **Firewall** configuration page features the following control elements:

Element	Description
	Toggle switch to deactivate the firewall.
<b>Save Permanent</b>	Saves your new firewall configuration settings.
<b>+ Add Zone</b>	Opens the <b>Add Zone</b> dialog. In the <b>Add Zone</b> dialog, you can add a new active zone to your firewall configuration, or you can assign new interfaces or “networks” (subnets/IP address ranges) for an already existing active zone (i.e. for a zone that has already been added to your firewall).

Table 17: Control elements in main toolbar

### 6.3.3 Network Proxy settings

If your local IT network uses proxy server(s) for HTTP, HTTPS, or FTP communication, you must configure the **Network Proxy** settings of the netFIELD OS accordingly.



#### Note:

To ensure that the device will be able to communicate with the cloud, we strongly recommend you to configure the proxy settings *before onboarding* your device. The local proxy settings of the device will be transferred to the netFIELD Portal during onboarding and will be stored there.

The container images that you then deploy from the Portal can thus take over these proxy settings and use them for their own communication when they run on the device after their deployment. Note also that if you change the proxy settings locally on your device *after onboarding*, you must “synchronize” the settings with the netFIELD Portal in order to keep the settings there “up-to-date” (to synchronize, open the **Onboarding** page in the Local Device Manager, then click **Synchronize** button).

You can find the **Network Proxy** settings on the **Networking** page.

The screenshot displays the netFIELD web interface. On the left, a sidebar contains various menu items: System, **Networking** (highlighted with a red arrow), Networking Services, Onboarding, General Settings, Standard Docker, IoT Edge Docker, Accounts, Certificate, Terminal, Operating System, Logs, and Services. The main content area shows the 'Network Proxy' configuration page. At the top, there are input fields for 'sit0', 'vethd1de80b', and 'vethf740d97'. Below these is a table titled 'Network Proxy' with columns 'Proxy', 'Host', and 'Port'. The table contains three rows: HTTP (Host: HTTP://10.11.5.98, Port: 3128), HTTPS (Host: HTTPS://10.11.5.99, Port: 3128), and No Proxy (Host: localhost, 127.0.0.1). An 'Edit Proxy' button is located to the right of the table. Below the table is a section titled 'Networking Logs' for 'FEBRUARY 22, 2022', showing a list of log entries with timestamps, log levels, messages, and sources (NetworkManager). The bottom of the interface shows the version '2.4.0' and a 'DEVICE' label.

Proxy	Host	Port
HTTP	HTTP://10.11.5.98	3128
HTTPS	HTTPS://10.11.5.99	3128
No Proxy	localhost, 127.0.0.1	

Figure 38: Network Proxy configuration

The **Network Proxy** table shows the current Proxy server settings of your netFIELD OS. The protocols for which a Proxy server is being used are listed in the **Proxy** column, the **Host** column shows the IP address or host name of the corresponding proxy server and the **Port** column shows the port number that the proxy server uses for the protocol.

The **No Proxy** entries designate destinations that shall not be addressed via Proxy server.

By default these are `localhost` and `127.0.0.1`, which are “internal” addresses of the netFIELD OS and are therefore not to be handled by a proxy server. The `localhost` and `127.0.0.1` entries appear in the **No Proxy** list even if you did not configure any Proxy Server for your netFIELD OS.

Do not edit or remove `localhost` and `127.0.0.1` from the **No Proxy** list.

To configure your network proxy settings, proceed as follows:

**Note:**

Ask your local network administrator for the parameters (IP address, ports, passwords etc.) of your local proxy server(s).

➤ Click the **Edit Proxy** button.

🔗 The **Proxy Settings** dialog opens:

Figure 39: Proxy Settings dialog window

**Use case a: Using one proxy server for multiple protocols.**

- If the HTTP, HTTPS and/or FTP communication in your local network is handled by a single proxy server, select the **Use this proxy server for all protocols** option.

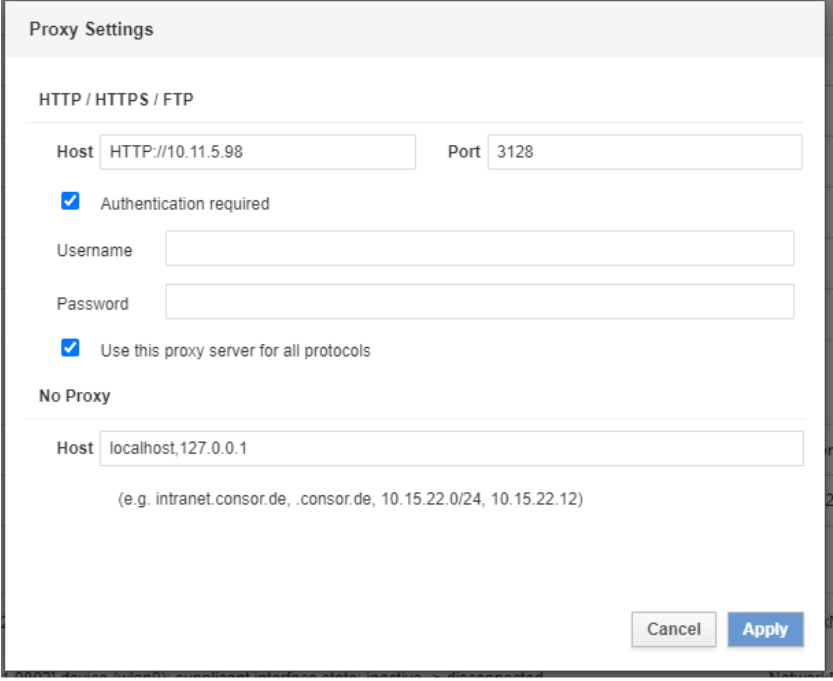
The image shows a 'Proxy Settings' dialog box. It has a title bar 'Proxy Settings'. Below it is a section 'HTTP / HTTPS / FTP'. In this section, there are two input fields: 'Host' with the value 'HTTP://10.11.5.98' and 'Port' with the value '3128'. Below these are two checkboxes: 'Authentication required' (checked) and 'Use this proxy server for all protocols' (checked). There are also input fields for 'Username' and 'Password'. Below the 'HTTP / HTTPS / FTP' section is a section 'No Proxy'. It has a 'Host' input field with the value 'localhost,127.0.0.1'. Below this field is a hint text: '(e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)'. At the bottom right of the dialog are 'Cancel' and 'Apply' buttons.

Figure 40: Using one Proxy server for all protocols

- In the **Host** field, enter the appropriate prefix of the protocol that the proxy server is using, followed by its IP address or host name, e.g.: `http://192.168.20.122`
- In the **Port** field, enter the number of the port that the proxy server is using.
- If your proxy server requires authentication, select the **Authentication required** option and enter **Username** and **Password** of the server.
- In the **No Proxy** section, you can specify destinations that shall not be handled by the proxy server(s). Multiple entries in the **Host** field must be separated by comma.

**Important:**

Do not change or remove the `localhost` and `127.0.0.1` entries in the **No Proxy** section. These are “internal” addresses of the netFIELD OS that cannot be handled by a proxy server because they are required for internal communication. You can, however, add further exceptions in the **Host** field.

**Use case b: Using separate proxy servers for different protocols.**

- If the HTTP, HTTPS and/or FTP communication in your local network is handled by separate proxy servers, uncheck the **Use this proxy server for all protocols** option.
- This enables separate configuration fields for the **HTTP**, **HTTPS** and **FTP** protocols:

The image shows a 'Proxy Settings' dialog box with a light gray header. It contains three sections for protocol-specific settings: HTTP, HTTPS, and FTP. Each section has a 'Host' and 'Port' input field, and two checkboxes: 'Authentication required' and 'Use this proxy server for all protocols'. The 'No Proxy' section at the bottom has a single 'Host' input field. The 'Host' fields are pre-filled with 'HTTP://10.11.5.98', 'HTTPS://10.11.5.99', and 'localhost, 127.0.0.1' respectively. The 'Port' fields are pre-filled with '3128'. The 'Authentication required' checkboxes are unchecked. The 'Use this proxy server for all protocols' checkbox is also unchecked. At the bottom right, there are 'Cancel' and 'Apply' buttons.

Protocol	Host	Port	Authentication required	Use this proxy server for all protocols
HTTP	HTTP://10.11.5.98	3128	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	HTTPS://10.11.5.99	3128	<input type="checkbox"/>	<input type="checkbox"/>
FTP			<input type="checkbox"/>	<input type="checkbox"/>

**No Proxy**

Host
localhost, 127.0.0.1

(e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)

Cancel Apply

Figure 41: Separate HTTP/HTTPS/FTP configuration

- Enter the parameters of the individual proxy servers.

## Saving and restarting

- To save your new proxy server configuration, click **Apply** button.
- The following dialog appears:

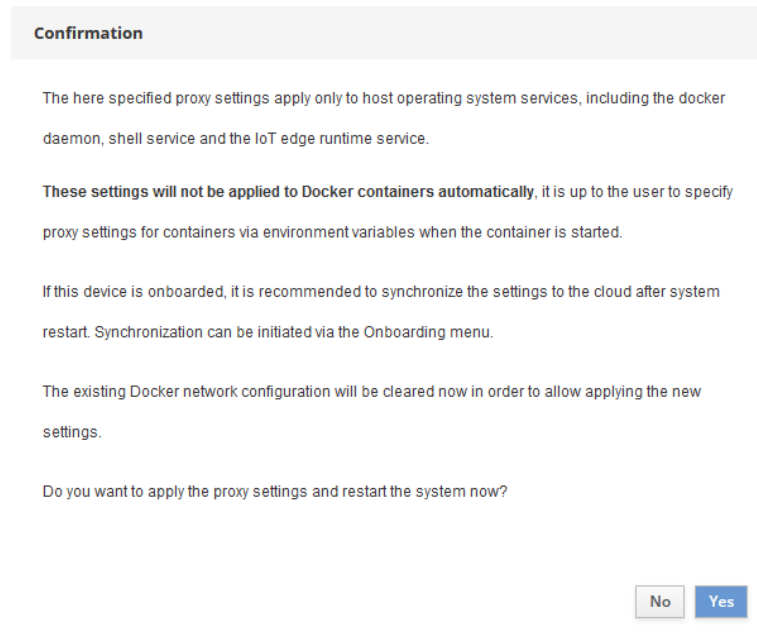


Figure 42: Restart dialog after changing proxy server configuration

- Read the note carefully.
- To apply the new settings, you must allow the netFIELD OS to perform an immediate restart.  
Click **Yes** to apply the new settings and restart the netFIELD OS.
- Click **No** to close the dialog without applying the new settings.

## Synchronizing new settings with the cloud

- If your device was already onboarded in the netFIELD Portal before changing the settings, you must “synchronize” the new proxy server settings with the corresponding data set of the “device twin” in the cloud.  
To do so, open the **Onboarding** page of the netFIELD OS.



- After having changed the proxy settings of an onboarded device, the **Onboarding** page should now display a **Proxy settings changed** note and the **Synchronize** button (if not, refresh the page by pressing **F5** on your keyboard).

The screenshot shows the netFIELD Onboarding page for device NT0002A233E553. A notification banner at the top states "Proxy settings changed" with the instruction "Proxy settings changed, please synchronize settings with netFIELD Portal". The page displays the following information:

<b>Onboarding Method</b> Manual	<b>Hardware Id</b> 000000000000-TSBG03010351
<b>Status</b> Onboarded	<b>Environment</b> Training
<b>API Endpoint</b> api-training.netfield.io	

Below this information are input fields for "E-Mail" and "Password". At the bottom, there are two buttons: "Offboard" and "Synchronize". A red arrow points to the "Synchronize" button.

Figure 43: Synchronize proxy settings with netFIELD Portal

- In the **E-Mail** and **Password** fields, enter the credentials of a user of the **portal** who possesses the `updateDevices` permission.
- Click **Synchronize** button.
- If the credentials have been correct, the “**Device proxy settings were updated**” message appears. The proxy server settings of your device in the cloud are now identical with your local settings. You can check the new settings in the Device Manager of the netFIELD Portal under **Device Manager** > **[your device]** > **Overview**. The new settings should be displayed there.

### Removing or editing existing Proxy server settings

If you are not using proxy server(s) in your local IT network any more, you can simply open the **Proxy Settings** dialog window and delete (or edit) the entries in the corresponding fields. After clicking the **Apply** button, the proxy server will be removed from the configuration and the new settings will become effective after restarting the netFIELD OS. If your device is onboarded in the netFIELD Portal, do not forget to synchronize the new settings.

## 6.4 Networking Services

### 6.4.1 Wi-Fi

#### 6.4.1.1 Overview

On the **WiFi** tab of the **Networking Services** page, you can configure the Wi-Fi functions of your device.

The netFIELD OS supports single band 2.4 GHz wireless network communication (Wi-Fi / WLAN) according to IEEE 802.11 and can either connect to an existing wireless network in “Client” mode or establish a new wireless network as “Access Point”.

Other clients connected to the same Wi-Fi network can thus access the **Local Device Manager** and/or other IP based services provided by the netFIELD OS on your device.

In Access Point mode, you can even route IP data from a connected Wi-Fi client to other connected subnets of your device (e.g. to an Ethernet subnet connected at its eth0 interface) by assigning both the Wi-Fi interface and the corresponding “target” interface (e.g. eth0) to the **NAT-Trusted** or the **NAT-Drop** zone of your firewall. The required NAT-Trusted respectively NAT-Drop zone can be created on the **Networking > Firewall** page (see section *Firewall* [▶ page 62]).

Routing from one Wi-Fi client to another connected Wi-Fi client is also possible.

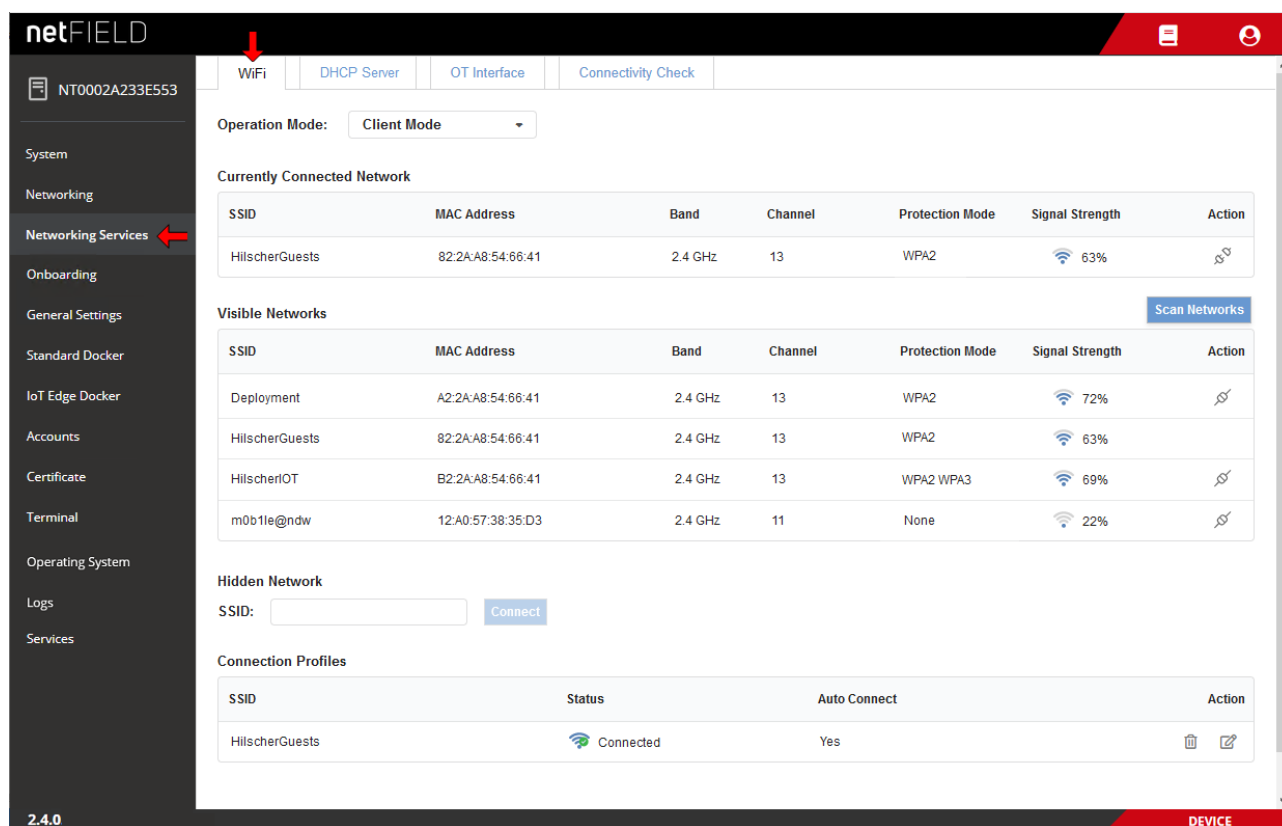




Figure 44: Wi-Fi Client Mode

**Note:**

If the “WiFi hardware is not available or disabled” note is displayed, you have to enable the **wlan0** interface on the **Networking** page before you can select and configure your Wi-Fi mode here.

To do so, open the **Networking** page, click **wlan0 – Not available**

entry (below **Interfaces**), then click the toggle switch  (on the right side of the screen). After enabling, the toggle switch looks like this: 

## Operation Mode


➤ Select the **Operation Mode** in the dropdown-list.

Operation mode	Description	wlan0 interface default IP settings
Client Mode	This mode allows the netFIELD Edge device to connect to an already existing Wi-Fi network (2.4 GHz band) provided by a nearby access point. Personal and Enterprise WPA is supported. See section <i>Client mode</i> [▶ page 80] for details.	After connecting to an access point, the <b>IPv4</b> address configuration of the <b>wlan0</b> interface is by default set to <i>Automatic (DHCP)</i> . The interface thus uses the IP address assigned to it by the DHCP server of the Access Point. On the <b>Networking &gt; Interfaces &gt; wlan0</b> page, the <b>Status</b> parameter shows the IPv4 and IPv6 addresses assigned to the interface by the DHCP server. <b>Note:</b> If you want to manually assign a fixed IP address, click on <b>Automatic (DHCP)</b> to open the <b>IPv4 Settings</b> dialog.
Access Point Mode	In this mode, the Wi-Fi interface ( <b>wlan0</b> ) of your device establishes a BSS (Basic Service Set) in the 2.4 GHz band, protected by WPA-PSK. Other Wi-Fi-capable can connect to it by using the Pre-shared Key (PSK). See section <i>Access Point mode</i> [▶ page 86] for details.	After saving the Access Point configuration, the <b>IPv4</b> address configuration of the <b>wlan0</b> interface is by default set to <i>Link local</i> . On the <b>Networking &gt; Interfaces &gt; wlan0</b> page, the <b>Status</b> parameter shows the IPv4 Link local address, which was automatically assigned by the netFIELD OS. IPv4 Link local uses address block 169.254.0.0/16 (i.e. from 169.254.0.0 to 169.254.255.255). <b>Note:</b> IPv4 Link local address are generally not routed (because they are not guaranteed to be unique beyond their network segment), therefore we strongly recommend you to manually assign a more appropriate IPv4 address. To do so, click on <b>Link local</b> to open the <b>IPv4 Settings</b> dialog.

Table 18: Wi-Fi operating modes

After having selected an **Operation Mode**, the configuration parameters of the selected mode are displayed.

6.4.1.2 Client mode

After selecting **Client Mode** in the **Operation Mode** dropdown list, the device automatically scans its environment for “visible” Wi-Fi networks. After scanning, you can connect to a visible network by clicking the  button in the **Action** column.



**Note:**  
If the device detects a network for which an “Auto Connect” profile exists, it automatically connects to it.

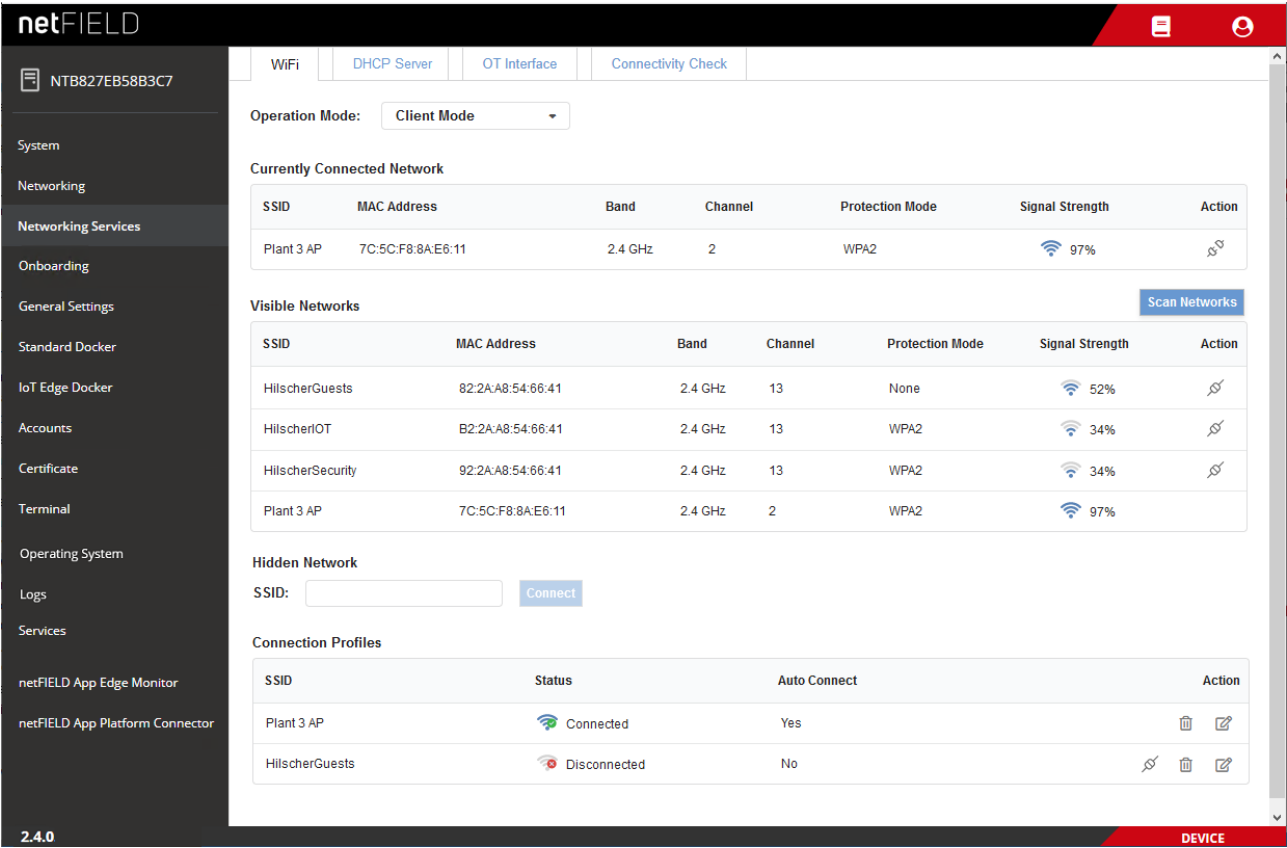


Figure 45: Client mode parameters

## Currently Connected Network

This table shows the Wi-Fi network to which the device is currently connected.


Parameter	Description	
SSID	SSID (service set identifier) of the Wi-Fi network to which the device is connected.	
MAC Address	MAC address of the Access Point of the Wi-Fi network to which the device is connected.	
Band	Radio waveband that the Wi-Fi network uses.	
Channel	Channel that the Wi-Fi network uses.	
Protection Mode	Shows the Wi-Fi Protected Access mode (WPA) that the network uses.	
Signal Strength	Shows the signal strength of the Wi-Fi connection in percent.	
Action		Disconnect from this Wi-Fi network.

Table 19: Currently Connected Network

## Visible Networks

This table shows the visible (i.e. “not hidden”) Wi-Fi networks that are currently within reach of the device. Click **Scan Networks** button to rescan for visible networks.


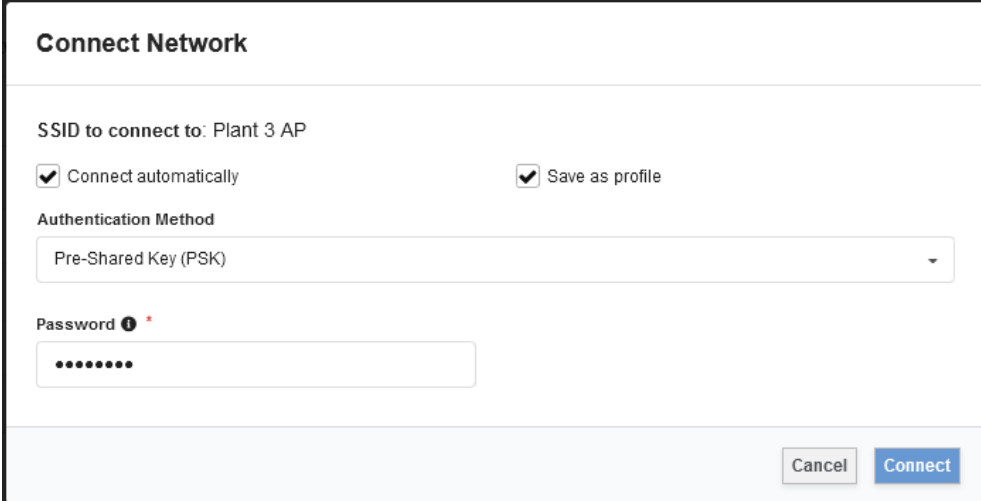
Parameter	Description	
SSID	SSID of the visible Wi-Fi network.	
MAC Address	MAC address of the Access Point of the visible Wi-Fi network	
Band	Radio waveband that the visible Wi-Fi connection uses.	
Channel	Channel that the visible Wi-Fi network uses.	
Protection Mode	Shows the Wi-Fi Protected Access mode (WPA) that the visible network uses.	
Signal Strength	Shows the signal strength of the visible Wi-Fi connection in percent.	
Action		Connect to this Wi-Fi network. Opens the <b>Connect Network</b> dialog. <b>Note:</b> Establishing a new connection automatically terminates any other currently active Wi-Fi network connection.

Table 20: Visible Networks

## Connect Network dialog




**Connect Network**

SSID to connect to: Plant 3 AP

☒ Connect automatically ☒ Save as profile

Authentication Method

Pre-Shared Key (PSK)

Password  \*

••••••••

Cancel Connect

Figure 46: Connect Network dialog


Parameter	Description	
Connect automatically	If you select this option, the device tries to automatically connect to this network each time after enabling the <b>Client mode</b> .	
Save as profile	If you select this option, the connection parameters are saved as a connection profile, which means that you will not have to re-enter them again when you connect via profile in future. Saved profiles are listed and can be selected in the <b>Connection Profiles</b> table.	
Authentication Method	Select in the drop-down list the authentication method that the access point requires. Depending on the method, further parameters might be displayed.	
	None	No authentication required (network provides no access protection).
	Flexible Authentication via Secure Tunneling (FAST)	EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified. Use of server certificates is optional. EAP-FAST can be used without PAC files, falling back to normal TLS.
		Identity Identity string for EAP authentication methods. This is often the user's user name or login name.
		Anonymous Identity Anonymous identity string for EAP authentication methods. Used as the unencrypted identity with EAP types that support different tunneled identities like EAP-TTLS.
		Password The password used for EAP authentication methods.
		Inner Authentication Method "802.1x phase 2" authentication method. <b>Note:</b> Preset to MS-CHAP v2
	Protected Extensible Authentication Protocol (PEAP)	Allows chaining of multiple EAP mechanisms.
		Identity Identity string for EAP authentication methods. This is often the user's user name or login name.
		Anonymous Identity Anonymous identity string for EAP authentication methods. Used as the unencrypted identity with EAP types that support different tunneled identities like EAP-TTLS.
		Password The password used for EAP authentication methods.
		Inner Authentication Method "802.1x phase 2" authentication method. <b>Note:</b> For PEAP only MS-CHAP v2 is allowed.
		CA Certificate File Click the  icon to select the root certificate of the Certification Authority that shall be used for authentication (optional). <b>Note:</b> The certificate must be stored in the <code>/etc/wifi-certs/</code> directory of the netFIELD OS. If not available, authentication will not be verified.

Table 21: Parameters in Connect Network dialog (1)



Parameter	Description		
Authentication Method	Pre-Shared Key (PSK)	Authentication only via PSK (does not require public-key infrastructure).	
		Password	Enter here the pre-shared key string (password or passphrase)
	Transport Layer Security (TLS)	EAP using the TLS protocol.	
		Identity	Identity string for EAP authentication methods. This is often the user's user name or login name.
		Client Key Password	Password used to decrypt the client private key file.
		Client Certificate File	Click the  icon to select the file containing the client certificate that shall be used for authentication (mandatory). <b>Note:</b> The certificate must be stored in the <code>/etc/wifi-certs/</code> directory of the netFIELD OS.
		Client Private Key File	Client Private Key File. <b>Note:</b> The private key file must be stored in the <code>/etc/wifi-certs/</code> directory of the netFIELD OS.
	CA Certificate File	Root certificate of the Certification Authority that shall be used for authentication (optional). <b>Note:</b> The certificate must be stored in the <code>/etc/wifi-certs/</code> directory of the netFIELD OS. If not available, authentication will not be verified.	
	Tunneled Transport Layer Security (TTLS)	EAP using "tunneled" TLS protocol.	
		Identity	Identity string for EAP authentication methods. This is often the user's user name or login name.
		Anonymous Identity	Anonymous identity string for EAP authentication methods. Used as the unencrypted identity with EAP types that support different tunneled identities like EAP-TTLS.
		Password	The password used for EAP authentication methods.
		Inner Authentication Method	Select in the drop-down list the "802.1x phase 2" authentication method: MS-CHAP MS-CHAP v2 CHAP
CA Certificate File		Click the  icon to select the root certificate of the Certification Authority that shall be used for authentication (optional). <b>Note:</b> The certificate must be stored in the <code>/etc/wifi-certs/</code> directory of the netFIELD OS. If not available, authentication will not be verified.	
Cancel	Click this button to close the dialog without connecting to the Wi-Fi network.		
Connect	Click this button to connect to the Wi-Fi network. <b>Note:</b> Establishing a new connection automatically terminates other current Wi-Fi network connections.		

Table 22: Parameters in Connect Network dialog (2)

After having connected to a network the **Connect Network** message appears:

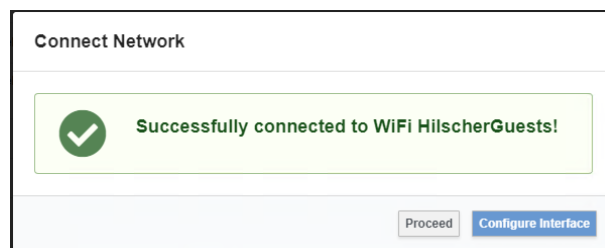


Figure 47: Connect network message

➤ Click **Proceed** to go back to the Wi-Fi page.



#### Note:

After connecting to an access point, the IPv4 address configuration of the **wlan0** interface is by default set to *Automatic (DHCP)*. The interface thus uses the IP address assigned to it by the DHCP server of the Access Point. If you want to manually define a fixed IP address (e.g. because a DHCP service is not available), click **Configure Interface** to open the **wlan0** interface configuration page where you can reconfigure its IP settings.

### Hidden Network

If you want to connect to a “hidden” network (i.e. that cannot be detected and displayed under **Visible Networks**) and you know its SSID, you can enter it into the **SSID** field, then click **Connect** button.

In the **Connect Network** dialog, you can save the connection as profile, so that you do not have to memorize the “hidden” SSID for future use.



## Connection Profiles

This table shows your stored network connection profiles. A profile can be created and stored by selecting the **Save as profile** option in the **Connect Network** dialog. You can store multiple profiles, including profiles of “hidden” networks. However, only a successfully established connection can be stored as “profile”.

When you connect to a network by using its connection profile, you do not have to re-enter the authentication parameters again (because they were stored in the profile).




Parameter	Description	
SSID	SSID of the Wi-Fi network.	
Status	Shows whether you are currently connected to the network.	
Auto Connect	Shows whether you have enabled the “Auto Connect” option for the network. In “Auto Connect” mode (“Connect automatically”) the device tries to automatically connect to this network after the <b>Client mode</b> has been enabled. <b>Note:</b> It is best practice to assign “Auto Connect” only to one SSID. If “Auto Connect” is assigned to more than one SSID, the device will pick the SSID with the highest signal strength.	
Action		Connect to this Wi-Fi network using the profile settings. <b>Note:</b> Establishing a new connection automatically terminates other current Wi-Fi network connections.
		Delete this profile.
		Edit this profile.

Table 23: Connection Profiles

6.4.1.3 Access Point mode

To operate your device as Wi-Fi Access Point (single band 2.4 GHz), select **Access Point Mode** in the **Operation Mode** dropdown list.

The Access Point configuration parameters are displayed:

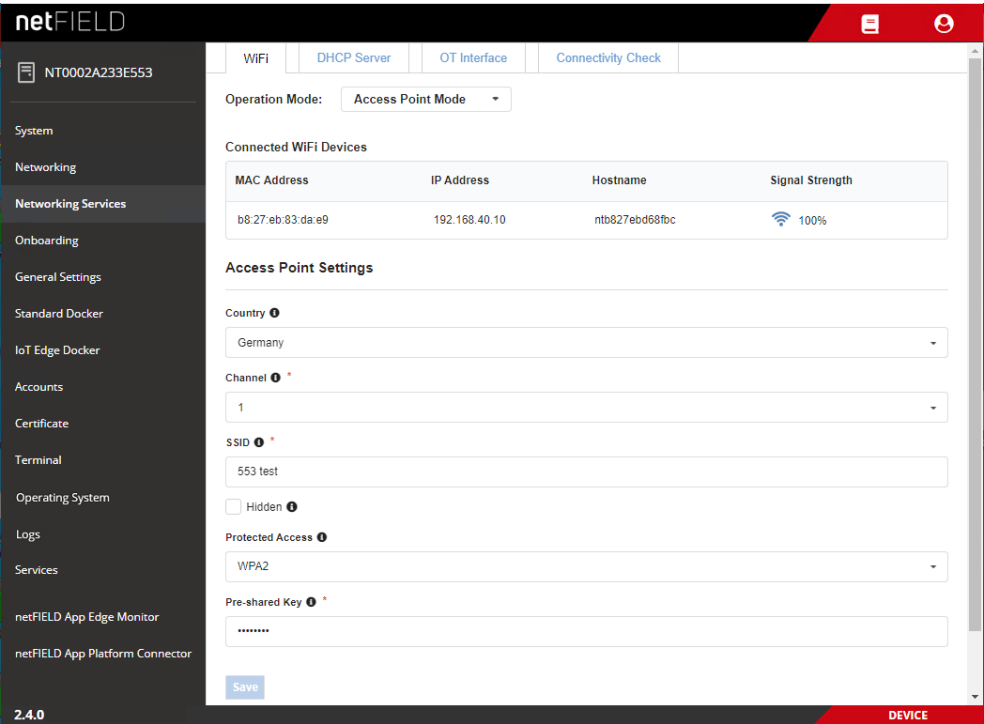


Figure 48: Access Point Mode

Connected WiFi Devices

This table shows the devices that are currently connected to your Access Point.

Parameter	Description
MAC Address	MAC address of the connected device.
IP Address	IP address of the connected device.
Hostname	Hostname of the connected device.
Signal Strength	Shows the signal strength of the Wi-Fi connection in percent.

Table 24: Connected WiFi Devices

## Access Point Settings

Parameter	Description
Country	In the drop-down list, select the country in which your device is operated. <b>Important:</b> This is necessary to ensure that the Wi-Fi interface operates in compliance with your national/regional regulations!
Channel	In the drop-down list, select the channel that your access point shall use.
SSID	Enter here the SSID (service set identifier) of the Wi-Fi network of your access point.
Hidden	Select this option if you want to "hide" the SSID broadcast of your access point. Nearby client devices scanning for available Wi-Fi networks will thus not be able to detect your SSID/network. Clients that know about your access point and want to connect to it will have to enter the SSID and the pre-shared key deliberately in their connection dialog.
Protected Access	In the drop-down list, select the Wi-Fi Protected Access standard (WPA). The Access Point mode of the netFIELD OS supports the so-called <i>WPA-Personal</i> (WPA-PSK) modes: - WPA - WPA2 - WPA / WPA2
Pre-shared Key	Define here the key for the protected access (WPA-PSK). This will be the "shared" key that clients must know in order to connect to your access point (this is also the key used for encrypting the wireless communication). The key may be entered either as a string of 64 hexadecimal digits or as a passphrase/password of 8 to 63 printable ASCII characters.
Save	Click this button to save your configuration.

Table 25: Access Point Settings

## Reconfigure IP address of wlan0 interface

After saving a new access point configuration, a message warns you that you are about to enable the wlan0 interface of the netFIELD OS in Wi-Fi access point mode and that its IP configuration will be set to IPv4 **link-local** (default).

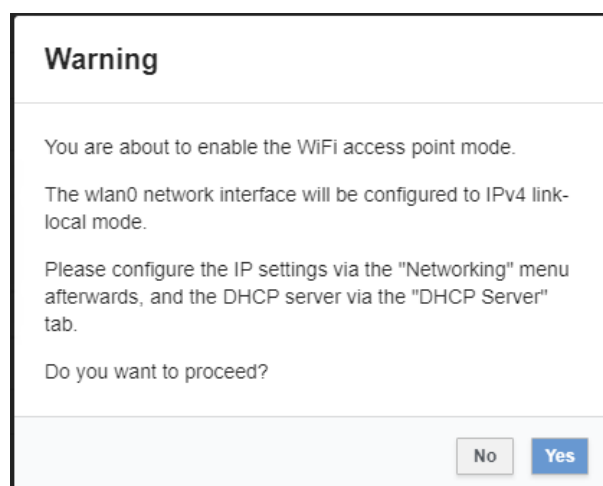


Figure 49: Warning note

**Note:**

By default, the IPv4 address configuration of the **wlan0** interface is automatically set to **link-local** by the netFIELD OS each time when you save your Access Point mode settings.

IPv4 link-local addresses are assigned using address block 169.254.0.0/16 (i.e. from 169.254.0.0 to 169.254.255.255).

Note that IPv4 link-local address are generally not routed (because they are not guaranteed to be unique beyond their network segment), therefore we strongly recommend you to assign a more appropriate IPv4 address to your **wlan0** interface.

- Acknowledge the warning with **Yes**.
- After a few seconds, the **Configure Interface** message appears:

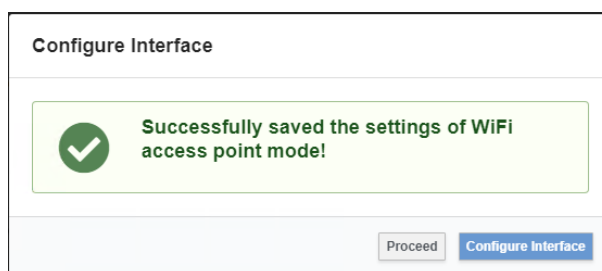


Figure 50: Configure Interface message

- To open the **wlan0** interface configuration page, click **Configure Interface** (as an alternative, you can click **Proceed** to go back to the Wi-Fi page and navigate later to the wlan0 interface configuration page via **Networking > Interfaces > wlan0**).
- On the **wlan0** interface configuration page, click on the blue **Link local** entry next to **IPv4** to open the **IPv4 Settings** dialog to replace the **link-local** address with a more appropriate IP address.

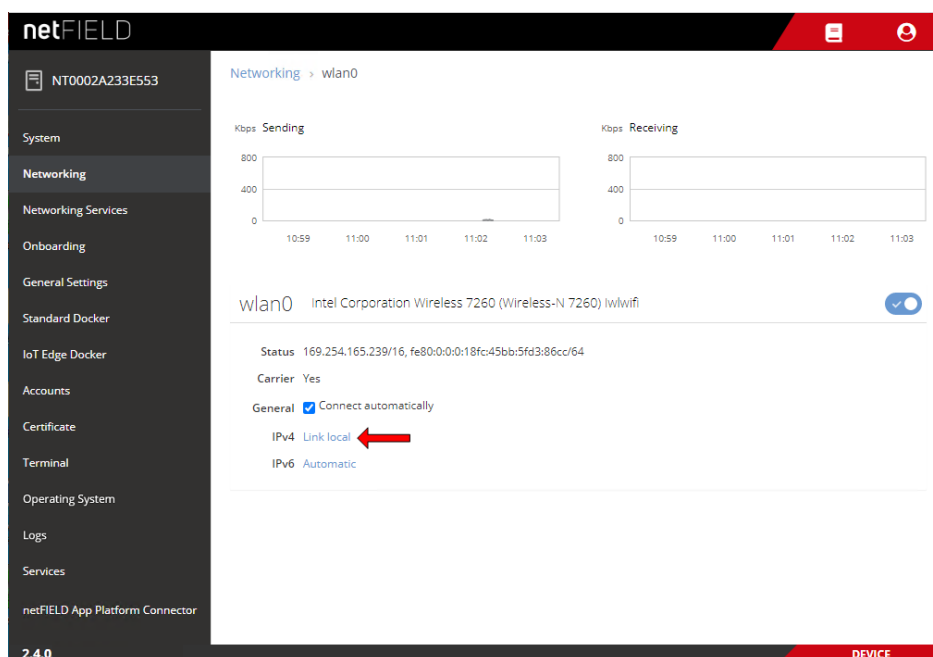


Figure 51: wlan0 configuration page

- In the **IPv4 Settings** dialog, select **Manual** in the **Addresses** drop-down list:

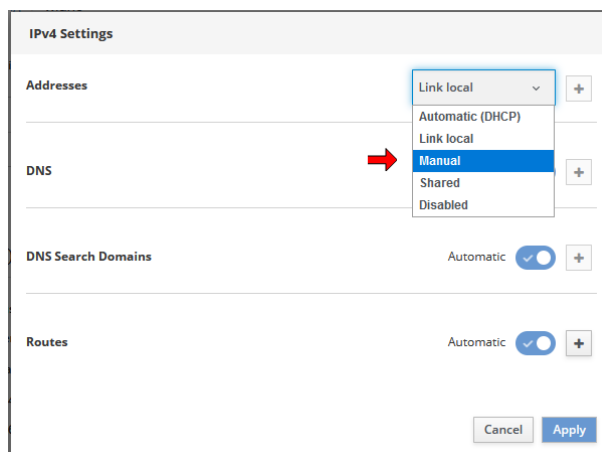


Figure 52: Set manual address in IPv4 Settings dialog

- Enter your new IP address parameters, then click **Apply** button.

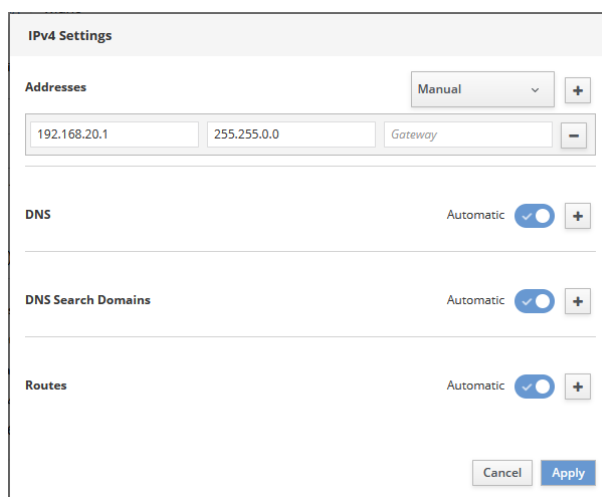


Figure 53: Enter Manual IP Address

## Configure DHCP Server of Access Point

To allow clients to connect easily to your Access Point, you should now also configure a DHCP service on the **DHCP Server** tab accordingly (see section below).

6.4.2 DHCP Server

On the **DHCP Server** tab of the **Networking Services** page, you can configure the DHCP service for your **wlan0** interface, thus allowing nearby Wi-Fi clients to connect easily to your Access Point.



**Note:**  
DHCP service for the **eth0** and **eth1** Ethernet interfaces of the device is not yet supported by the current netFIELD OS.

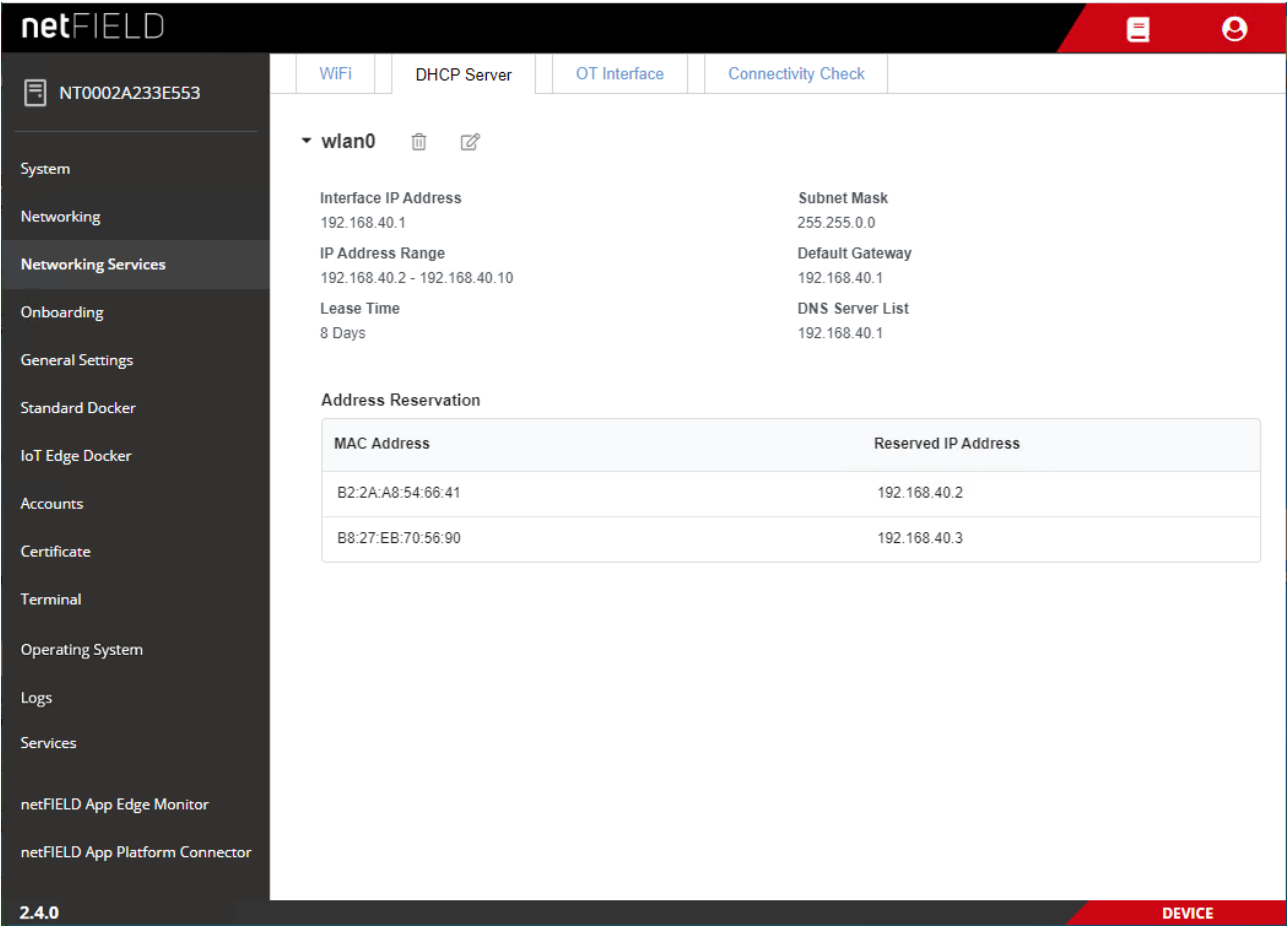



Figure 54: Configured DHCP service

Element/Parameter	Description
	Click here to delete the DHCP Server configuration.
	Click here to open the <b>DHCP Server Configuration</b> dialog where you can add a new DHCP Server configuration or edit your existing configuration.
Interface IP address	IP address of your wlan0 interface/access point. <b>Note:</b> IP address settings of the wlan0 interface must be defined under <b>Networking &gt; Interfaces &gt; wlan0</b> .
Subnet Mask	Subnet mask of your wlan0 interface/access point (which is also the subnet of your Wi-Fi network). <b>Note:</b> The IP address settings of the wlan0 interface can be defined under <b>Networking &gt; Interfaces &gt; wlan0</b> .
IP Address Range	Address range that the DHCP server uses.
Default Gateway	Default gateway (for routing IP traffic to other subnets). If no other router is present, this should be the IP address of the wlan0 interface/access point.

Element/Parameter	Description
Lease Time	Specifies how long an IP address assigned by the DHCP server is valid. After this period, the client device asks the DHCP server for a renewal of the lease respectively for a new IP address assignment.
DNS Server List	IP address(es) of the dynamic name servers to be used. If no other DNS server is specified, this should be the IP address of the wlan0 interface/access point. (The netFIELD OS will automatically forward DNS requests.)
Address Reservation	Shows reserved IP address(es) for certain client devices (identified by their MAC address).

Table 26: Elements/Parameters on DHCP Server page

- Click on the  button to open the **DHCP Server Configuration** dialog where you can add a new DHCP Server configuration or edit your existing configuration.



**Note:**

Note that after activating the Access Point mode, the IP address configuration of the wlan0 interface is automatically set to IPv4 **link-local** (which uses a default address range from 169.254.0.0 to 169.254.255.255). Addresses in the link-local range cannot be routed, therefore make sure that you have replaced the link-local address of the wlan0 interface with your own adequate IP address settings before you configure the DHCP server. To check or change the wlan0 IP address settings, go to **Networking > Interfaces > wlan0**.

## DHCP Server Configuration dialog

### DHCP Server Configuration for wlan0

Interface IP Address ⓘ  
192.168.40.1

Subnet Mask ⓘ  
255.255.255.0

IP Address Range - Start Address ⓘ \*

192.168.40.2

IP Address Range - End Address ⓘ \*

192.168.40.10

Default Gateway ⓘ \*

192.168.40.1

DNS Server List ⓘ \*

192.168.40.1

Lease Time ⓘ

☐ Infinite Time
 ☒ User Defined Time

8

Days

Address Reservation ⓘ

+

MAC Address	Reserved IP Address	Action
B2:2A:A8:54:66:41	192.168.40.2	
B8:27:EB:70:56:90	192.168.40.3	
MAC address	IP address	

Cancel

Save

Figure 55: DHCP Server Configuration dialog

Parameter	Description
Interface IP address	IP address of your wlan0 interface/access point. <b>Note:</b> IP address settings of the wlan0 interface must be defined under <b>Networking &gt; Interfaces &gt; wlan0</b> .
Subnet Mask	Subnet mask of your wlan0 interface/access point (which is also the subnet of your Wi-Fi network). <b>Note:</b> The IP address settings of the wlan0 interface must be defined under <b>Networking &gt; Interfaces &gt; wlan0</b> .
IP Address Range – Start Address	Enter here the start of the address range that the DHCP server shall use for assigning IP addresses to clients.
IP Address Range – End Address	Enter here the end of the address range that the DHCP server shall use for assigning IP addresses to clients.
Default Gateway	Enter here the IP address of the default gateway that the DHCP server shall assign to the clients. If no other router/gateway is available, enter here the IP address of your wlan0 interface/access point.
DNS Server List	Enter here the IP address(es) of the DNS Server(s) that the DHCP server shall assign to the clients. If no other DNS Server(s) are available, enter here the IP address of your wlan0 interface/access point. (The netFIELD OS will automatically forward DNS requests.) Separate multiple entries with commas.




Parameter	Description
Lease Time	Specifies here how long an IP address assigned by the DHCP server shall remain valid. After this period, the client device must ask the DHCP server for a new IP address assignment.
	Infinite Time      Lease remains valid until revoked.
	User Defined Time      Selecting this option allows you to define a certain period of minutes, hours or days.
Address Reservation	<p>Here you can ensure that certain client devices will always receive the same IP address when they request a lease.</p> <p>Click the <b>+</b> symbol above <b>Action</b> to add a reservation. To delete a reservation, click the  symbol.</p> <p>In the <b>MAC Address</b> field, enter the MAC address of the client device for which you want to reserve a certain IP Address, which is to be entered into the <b>Reserved IP Address</b> field.</p>
Cancel	Click this button to close the dialog without saving the DHCP configuration.
Save	Click this button to save the DHCP configuration. The DHCP service of your access point is immediately started. Wi-Fi clients can now connect to your Access Point.

Table 27: Parameters of DHCP Server Configuration dialog

### 6.4.3 OT Interface (Using the cifx0 interface or RTE)

On the **OT Interface** tab of the **Networking Services** page, you can enable or disable the TCP/IP channel of the cifx0 interface. Enabling the TCP/IP channel allows you to use the RTE ports (see positions (13) and (15) in section *Positions of the interfaces* [▶ page 16]) as standard Ethernet TCP/IP interface for acyclic services (“multicasts” are not supported).

Thus you could e.g. access the **Local Device Manager** via the RTE (“Fieldbus”) interfaces instead of the LAN interfaces of the device. (Note that in this case, the UPnP service cannot be used for connecting to the device, because it is not supported by the cifx0 interface.)



#### Important:

If you want to use a Real-Time Ethernet Docker Container (like e.g. the **netFIELD App PROFINET Device**), make sure that the **RTE Port TCP/IP Channel** option here is *disabled*.



#### Note:

Enabling the **RTE Port TCP/IP Channel** will cause the COM LED of the Real-Time Ethernet interface (see position (14) in section *Positions of the interfaces* [▶ page 16]) to show steady red light.

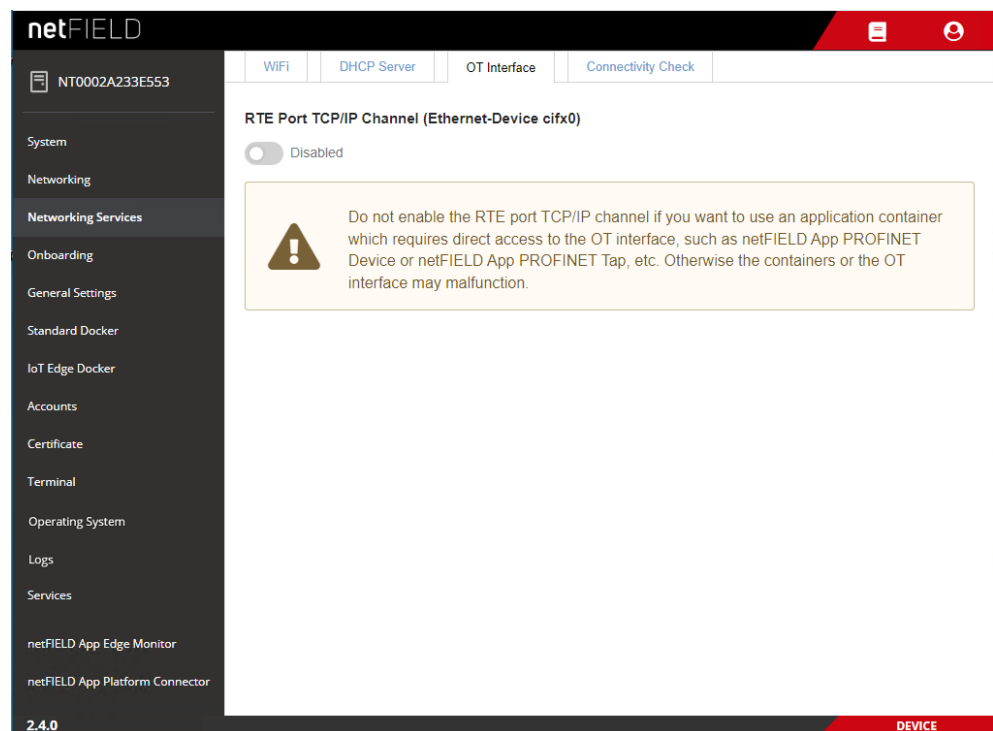


Figure 56: OT interface tab

**Note the following about the OT Interface**

The cfx0/Real Time Ethernet interface physically provides two separate Ethernet interfaces, which also have two different MAC addresses at network level. Both interfaces are controlled by a common driver, which cannot be used by more than one application at the same time.

Either the netFIELD OS uses the driver and provides the LAN interface **cfx0**, or a Docker Container uses the driver, for example to manage the RTE interface. Parallel access to the driver by the netFIELD OS and simultaneously by a Docker Container is not possible.

Therefore, you have to make sure that the **RTE Port TCP/IP Channel** option on this page is *disabled* if you want to use a Real-Time Ethernet Docker Container, like e.g. the **netFIELD App PROFINET Device** offered by Hilscher.

The netFIELD App PROFINET Device initializes the driver for the operation of both interfaces, i.e. as cfx0 (LAN) *and* as a Real-Time Ethernet device (in this case PROFINET Device).

Note that the **cfx0** and the RTE interface must receive their own individual IP configuration. While the **cfx0** interface is configured in the Local Device Manager (on the **Networking** page), the RTE interface is usually configured by the PLC e.g. via PROFINET DCP.

## 6.4.4 Connectivity Check

On the **Connectivity Check** tab of the **Networking Services** page, you can test the connectivity of the cloud communication channels that are used by the netFIELD OS-underlying Linux and the *Azure IoT Edge runtime* of the IoT Edge Docker. Some other configuration settings that are relevant for proper connectivity (like the local host time and the Docker's DNS settings) are also checked here.

The cloud connectivity checking functions are provided by the *iotedge check* tool (version 1.2.5) of the IoT Edge runtime, which uses the *azureiotedge-diagnostics* container for this.

Therefore, your device must be onboarded in the netFIELD Cloud (which enables the IoT Edge Docker and the IoT Edge runtime) for using this function. However, using only the **Ping** test works without the device being onboarded.



For more information on the *iotedge check* tool, see <https://docs.microsoft.com/en-us/azure/iot-edge/troubleshoot?view=iotedge-2020-11> and <https://github.com/Azure/iotedge/blob/main/doc/troubleshoot-checks.md>

The screenshot shows the netFIELD interface with the 'Connectivity Check' tab selected. The left sidebar lists various system settings, and the main area displays a 'Cloud Connectivity' table with columns for 'Check' and 'Result'.

Check	Result
Host can connect to and perform TLS handshake with iotHub AMQP port	Success (Green dot)
Container on the default network can connect to upstream AMQP port	Success (Green dot)
Container on the IoT Edge module network can connect to upstream AMQP port	Success (Green dot)
Host can connect to and perform TLS handshake with iotHub HTTPS / WebSockets port	Success (Green dot)
Container on the default network can connect to upstream HTTPS / WebSockets port	Success (Green dot)
Container on the IoT Edge module network can connect to upstream HTTPS / WebSockets port	Success (Green dot)
Host can connect to and perform TLS handshake with iotHub MQTT port	Failure (Red dot)
Could not connect to eplOTHub-Training.azure-devices.net : could not complete TLS handshake	
Container on the default network can connect to upstream MQTT port	Success (Green dot)
Container on the IoT Edge module network can connect to upstream MQTT port	Success (Green dot)
Host time is close to reference time	Success (Green dot)
<b>DNS server</b> Container engine is not configured with DNS server setting, which may impact connectivity to IoT Hub. Please see <a href="https://aka.ms/iotedge-prod-checklist-dns">https://aka.ms/iotedge-prod-checklist-dns</a> for best practices. You can ignore this warning if you are setting DNS server per module in the Edge deployment.	Warning (Yellow dot)

Figure 57: Connectivity Check tab

### LAN/Internet ping

To test the LAN respectively Internet connection, enter the IP address or the hostname of an endpoint in the **Ping** field, then click **Ping** button.

### Cloud Connectivity

To test the connectivity of the components that are involved in connecting the IoT Edge runtime to the netFIELD Cloud, click **Check** button.

The result is indicated with a dot:

- OK (available)
- Warning
- Error (not available)



For more information on the checks that are being performed, see <https://github.com/Azure/iotedge/blob/main/doc/troubleshoot-checks.md>

Note that the current netFIELD OS uses the *iotedge check* tool version 1.2.5.

---

## 6.5 Onboarding (and offboarding)

The **Onboarding** page allows you to “register” your device in the netFIELD Portal. For a detailed description of the onboarding process and the parameters on this page, see section *“Onboard” (register) device in netFIELD Cloud* [▶ page 41]. You can also “offboard” your device here.

If you have changed the HTTP/HTTPS/FTP proxy server settings of your device *after onboarding*, you can also “synchronize” these new settings here with the netFIELD Portal by clicking the **Synchronize** button. (The **Synchronize** button will only be visible if you have actually changed the proxy server settings. See also section *Network Proxy settings* [▶ page 72] for further information.)

The screenshot displays the netFIELD Onboarding interface. On the left is a dark sidebar with a menu including 'System', 'Networking', 'Networking Services', 'Onboarding' (indicated by a red arrow), 'General Settings', 'Standard Docker', 'IoT Edge Docker', 'Accounts', 'Certificate', 'Terminal', 'Operating System', 'Logs', and 'Services'. The main content area has a header 'netFIELD' and a red bar with icons. Below the header, there's a table with columns for 'Onboarding Method', 'Status', 'API Endpoint', 'Device Authentication Method', 'Hardware Id', 'Environment', and 'Hub'. The 'Onboarding' tab is active, showing a 'Basic' settings form. The form includes fields for 'Environment' (a dropdown), 'Device Name', 'E-Mail', 'Password', 'Device Authentication' (a dropdown), and 'Upstream Protocol' (a dropdown). There is a checkbox for 'Use Deployment Manifest' and an 'Onboard' button at the bottom. The footer shows '2.5.0.1.release' and 'DEVICE'.

Figure 58: Basic Onboarding page

Once your device has been onboarded, the page changes and shows the parameters for “offboarding” the device. By offboarding it, the device will be “deleted” in the portal and removed from the device list of the portal’s **Device Manager**:

## Offboarding after having used the Basic Onboarding method

Figure 59: Offboarding “Basic”

- In the **E-Mail** and **Password** fields, enter the credentials of a user of the **netFIELD Portal** who possesses `deleteDevices` and `offboardedDevices` permissions.
- Note: In case you are using the credentials (in the **E-Mail** and **Password** fields) of a netFIELD Portal user account that is protected by two-factor authentication (a.k.a 2FA), make sure that you have access to the corresponding “Time-based One-time Password (TOTP)” methods, i.e. the email account or the Authenticator app. This is because in this case you will also have to enter a 2FA passcode during offboarding.
- Click **Offboard** button.
- If the netFIELD Portal account is protected by 2FA, you will now have to select your 2FA method and enter the passcode.  
If the account is a member of other **Workspaces**, you will now also have to select the workspace from which you want to offboard the device.
- After successful offboarding, the following message appears: **Success – Device is now deleted.**

## Offboarding after having used the Advanced Onboarding method

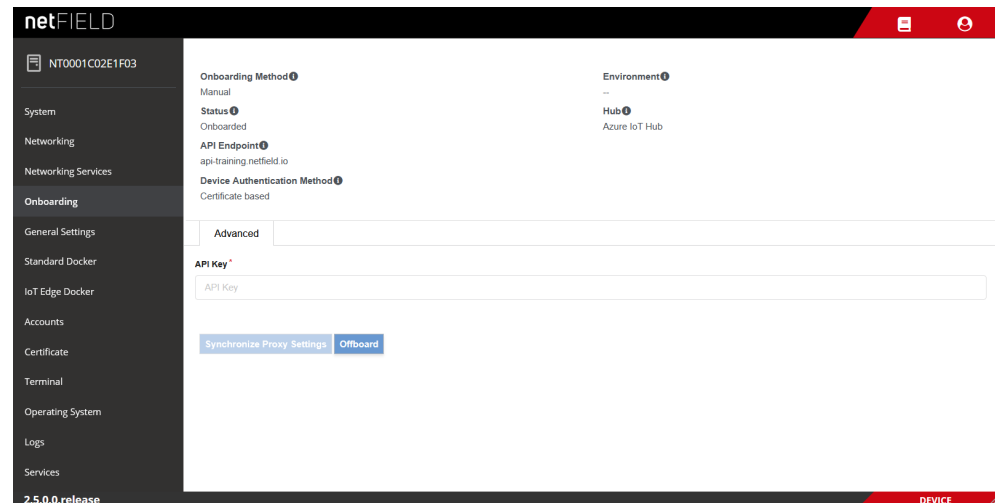


Figure 60: Offboarding “Advanced”

- In the **API KEY** field, enter an API Key that possesses the right to offboard devices. I.e. this key must have **Security Level** `org+ch` or `org` for the `deleteDevices` and `offboardedDevices` functions of the **devices** resource.
- Click **Offboard** button.
- ⇒ After successful offboarding, the following message appears: **Success – Device is now deleted.**



### Note:

After offboarding, all application containers managed by the netFIELD Portal are automatically deleted. However, the Docker images will still present on the device.



## 6.6 General Settings

### 6.6.1 Web Server (Port) Settings

On the **Web Server** tab of the **General Settings** page, you can change the TCP ports of the web server of the netFIELD OS.

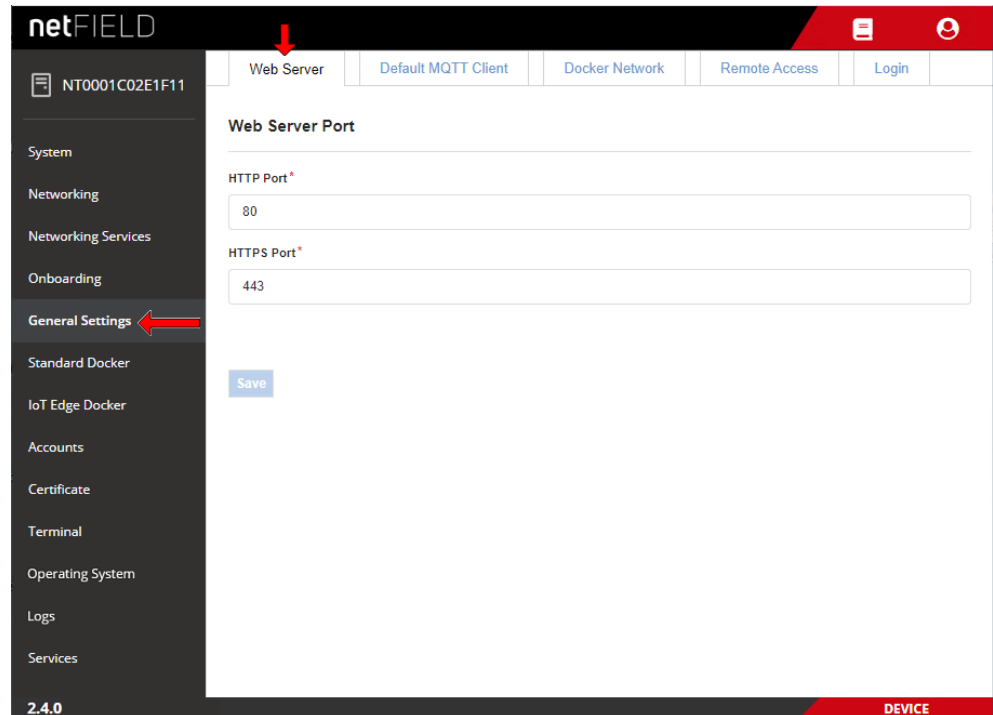


Figure 61: Web Server Settings tab

By default, the netFIELD OS uses port 80 for its HTTP communication and port 443 for its HTTPS communication.



#### Important:

The new settings become immediately effective after saving and confirming the changes, which means that your current HTTP/HTTPS connection to the netFIELD OS respectively Local Device Manager will be lost.

You will have to reconnect by specifying the new port number after the IP address in the address bar of your web browser.



#### Note:

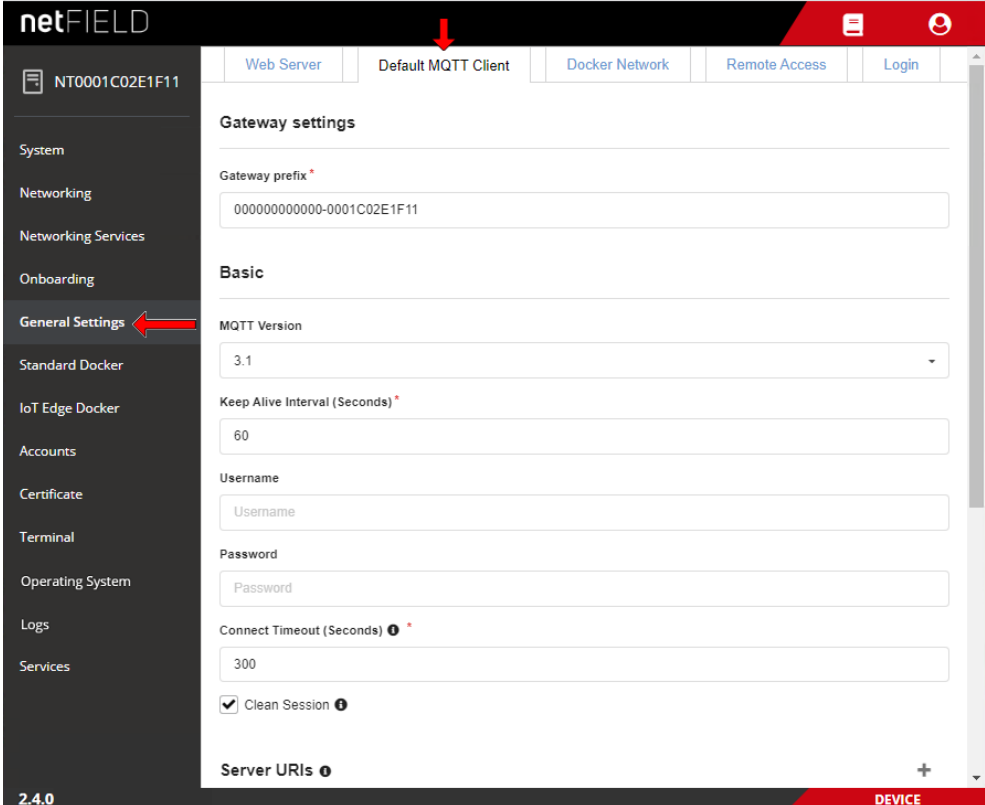
Changing the web server port settings will have no effect on the **Remote Control** function that allows you to access the Local Device Manager from the netFIELD Portal via “web tunnel”. For more information about the Remote Control function, see *netFIELD Portal* operating instructions manual, DOC190701OIxxEN.

- Click **Save** button to save your new Web Server Settings.

## 6.6.2 Default MQTT Client Settings

On the **Default MQTT Client** tab of the **General Settings** page, you can change the MQTT Client configuration parameters that shall be used by the Docker containers that are running on your netFIELD OS. These settings are stored in a JSON configuration file in the netFIELD OS (`/etc/gateway/mqtt-config.json`).

By default, all Hilscher netFIELD Apps use this configuration file. Other containers (i.e. non-Hilscher application containers) that do not require their own customized MQTT client settings, can also use these settings here if the configuration file is referenced accordingly in the container image (e.g. in the *Container Create Options* of the netFIELD Portal, see *netFIELD Portal* operating instructions manual, DOC190701OIxxEN).



The screenshot displays the netFIELD web interface. The left sidebar contains a menu with 'General Settings' highlighted by a red arrow. The top navigation bar shows 'Default MQTT Client' as the active tab, also indicated by a red arrow. The main content area is titled 'Gateway settings' and includes the following fields:

- Gateway prefix \***: A text input field containing '00000000000-0001C02E1F11'.
- Basic**: A section header.
- MQTT Version**: A dropdown menu set to '3.1'.
- Keep Alive Interval (Seconds) \***: A text input field containing '60'.
- Username**: A text input field containing 'Username'.
- Password**: A text input field containing 'Password'.
- Connect Timeout (Seconds) ⓘ \***: A text input field containing '300'.
- Clean Session ⓘ**: A checked checkbox.
- Server URIs ⓘ**: A section header with a plus icon for adding more URIs.

The bottom of the interface shows the version '2.4.0' and a 'DEVICE' label.

Figure 62: Default MQTT Settings

Element		Description	
Gateway settings	Gateway prefix	Identifies the device. By default, this is the Hardware ID of the device.	
Basic	MQTT Version	MQTT version to be used (depending on the MQTT broker).	
	Keep Alive Interval	Defines the maximum length of time in seconds that the broker and client may not communicate with each other.	
	Username	User name for authentication at the broker (if implemented and required by the broker). Note that the <i>netFIELD App MQTT Broker</i> from the netFIELD Portal does not require login authentication.	
	Password	Password for authentication at the broker (if implemented and required by the broker). Note that the <i>netFIELD App MQTT Broker</i> from the netFIELD Portal does not require login authentication.	
	Connect Timeout	Defines the maximum length of time in seconds that is allowed for completing the connection process.	
	Clean session	If <b>Clean session</b> is selected, the client does not want a persistent session (meaning that if the client disconnects for any reason, all information and messages that are queued from a previous persistent session are lost). If <b>Clean session</b> is unchecked, the broker creates a persistent session for the client.	
Server URIs		Server URI or FQDN of the MQTT broker <b>Note:</b> When multiple server URIs are specified, the client will try to connect to each server one after the other, starting with the first server in the list. If a server connection was established successfully, only this connection will be used. The client will not open multiple connections to multiple servers simultaneously.	
Last Will and Testament		Select this option if you want to use the “last will and testament” (LWT) feature of MQTT. (I.e. to notify other clients about an unexpected loss of connection to the broker)	
		Topic Name	Topic name of LWT message
		Retained	“Retained” flag of LWT message
		Quality of Service	QoS of LWT message
		Message	Message text, e.g. “unexpected loss of connection”
SSL / TLS		Select this option if you want to use SSL/TLS encryption for creating a secure connection to the MQTT broker. <b>Note:</b> This option is for expert users only! In the standard use case, in which the <i>netFIELD App MQTT Broker</i> and the Docker containers are running on the same device, a secure SSL/TLS connection is not necessary (the overhead of the secure connection can thus be avoided).	
		File name and path to private key in PEM format	Enter here the complete path to the private key on the device.
		File name and path to certificate chains in PEM format	Enter here the complete path to the certificate chains on the device.
		Override the trusted CA certificates in PEM format	Enter here the complete path to override the trusted CA certificates on the device.
		Enable verification of the server certificate	If this option is disabled, the Docker containers will also accept invalid certificates from the broker (not recommended).

Table 28: Default MQTT Client Settings

➤ Click **Save** button to save your new Default MQTT Client Settings.

## 6.6.3 Docker Network Settings

On the **Docker Network** tab of the **General Settings** page, you can change the network address settings of the Standard Docker and of the IoT Edge Docker.

You can also add addresses of external DNS server(s) for Standard Docker and IoT Edge Docker containers here.



### Important:

These network address settings are predefined by Hilscher. Change these default addresses only if they are not compatible with your company's LAN address configuration, i.e. to avoid an address conflict.

Note that after changing the address settings of the Standard and/or IoT Edge Docker all containers running on the corresponding Docker will be stopped and deleted and the netFIELD OS will be automatically restarted. After restart, you might have to re-deploy the deleted containers that are not automatically re-deployed via the netFIELD Portal.

The screenshot displays the 'Docker Network' settings page in the netFIELD interface. The left sidebar shows the navigation menu with 'General Settings' highlighted. The top navigation bar includes tabs for 'Web Server', 'Default MQTT Client', 'Docker Network' (selected), 'Remote Access', and 'Login'. The main content area is divided into two sections: 'Standard Docker' and 'IoT Edge Docker'. Each section contains fields for 'Bridge IP', 'CIDR Suffix or Netmask', and 'DNS Server List'. Below these fields is a table for 'Default address pools' with columns for 'IP Address', 'CIDR Suffix or Netmask', 'Network Size', and 'Action'. A 'Save' button is located at the bottom left of the page.

IP Address	CIDR Suffix or Netmask	Network Size	Action
10.254.0.1	16	24	[Delete Icon]

Figure 63: Docker Network Settings

## Standard Docker

The **docker0** bridge is a virtual default interface created by the Standard Docker.

By default, it uses the address 10.252.254.1/24 (“private range” as defined in RFC 1918) if the address is not already used on the host machine.

If not configured otherwise, a container deployed in the Standard Docker connects to this **docker0** bridge by default. The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. “masquerading”) created by the Standard Docker to communicate with destinations outside the netFIELD OS.

Note that the **docker0** default bridge does not provide internal or external DNS resolution for its containers. However, you can specify external DNS server(s) to be used by the containers in the Standard Docker.



### Note:

According to the Docker documentation (<https://docs.docker.com/network/bridge/>), the default **docker0** bridge network is considered a “legacy detail” of Docker and is not recommended for production use. If you are using the Standard Docker, we strongly recommend you to create your own custom bridge network(s) for your containers instead of using the **docker0** default bridge, because custom bridges provide automatic DNS resolution between containers (which docker0 does not).

Element	Description
Bridge IP	IP address of the <b>docker0</b> bridge. Default: 10.252.254.1 <b>Note:</b> Do not change the default address, unless this is necessary to avoid an address conflict with your LAN. Do not use the same Bridge IP address for both Standard and IoT Edge Docker.
CIDR Suffix or Netmask	Subnet mask of the <b>docker0</b> bridge as CIDR Suffix or in “dotted decimal notation”. Default (CIDR Suffix): 24 Default (dotted decimal notation): 255.255.255.0
DNS Server List	Enter here the IPv4 address of the DNS server that the containers in the Standard Docker shall use. You can specify more than one server. Enter first the address of the primary server then use a comma to separate the address of the secondary server etc.
Default address pools	Here you can define “reserve” address pools (subnets) for your Docker custom bridge networks (a.k.a user defined bridges). The default pool consisting of the IP address/CIDR Suffix 10.254.0.1/16 with network size 24 means that the first additional custom network bridge interface will be created with the IP address/CIDR Suffix 10.254.0.1/24, the second will be 10.254.1.1/24, the third will be 10.254.2.1/24, and so on.
	IP address      Reserved IP address for custom bridge networks.
	CIDR Suffix or Netmask      Subnet mask for the custom bridge networks as CIDR Suffix or in “dotted decimal notation”.
	Network Size      Number of bits used as the netmask for further custom bridge networks.
	Action       Opens a dialog for adding a new pool of reserved addresses.
	Deletes the address pool.

Table 29: Standard Docker Network Settings

## IoT Edge Docker

The **iotedge0** bridge is a virtual default interface created by the IoT Edge Docker.

By default, it uses the address 10.252.253.1/24 ("private range" as defined in RFC 1918) if the address is not already used on the host machine.

If not configured otherwise, a container deployed in the IoT Edge Docker connects to this **iotedge0** bridge by default. (Note that most netFIELD App containers deployed from the netFIELD Portal are configured to connect themselves either to the *azure-iot-edge* bridge network or to the host network.)

The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. "masquerading") created by the IoT Edge Docker to communicate with destinations outside the netFIELD OS.

Note that the **iotedge0** default bridge does not provide internal or external DNS resolution for its containers. However, you can specify external DNS server(s) to be used by the containers in the IoT Edge Docker.



Element	Description
Bridge IP	IP address of the <b>iotedge0</b> bridge. Default: 10.252.253.1 <b>Note:</b> Do not change the default address, unless this is necessary to avoid an address conflict with your LAN. Do not use the same Bridge IP address for both Standard and IoT Edge Docker.
CIDR Suffix or Netmask	Subnet mask of the <b>iotedge0</b> bridge as CIDR Suffix or in "dotted decimal notation". Default (CIDR Suffix): 24 Default (dotted decimal notation): 255.255.255.0
DNS Server List	Enter here the IPv4 address of the DNS server that the containers in the IoT Edge Docker shall use. You can specify more than one server. Enter first the address of the primary server then use a comma to separate the address of the secondary server etc.
Default address pools	Here you can define "reserve" address pools (subnets) for your IoT Edge Docker custom bridge networks (a.k.a user-defined bridges). The default pool consisting of the IP address/CIDR Suffix 10.253.0.1/16 with network size 24 means that the first additional custom network bridge interface will be created with the IP address/CIDR Suffix 10.253.0.1/24, the second will be 10.253.1.1/24, the third will be 10.253.2.1/24, and so on.
	IP address      Reserved IP address for IoT Edge Docker custom bridge networks.
	CIDR Suffix or Netmask      Subnet mask for IoT Edge Docker custom bridge networks as CIDR Suffix or in "dotted decimal notation".
	Network Size      Number of bits used as the netmask for further IoT Edge Docker custom bridge networks.
	Action  Opens a dialog for adding a new pool of reserved addresses.
	 Deletes the address pool.

Table 30: IoT Edge Docker Network Settings

➤ Click **Save** button to save your new Docker Network Settings.

The following picture shows an example of a typical Docker network setup. The default bridge networks (**docker0** and **iotedge0**) are indicated in blue, the user-defined custom bridge networks are indicated in green:

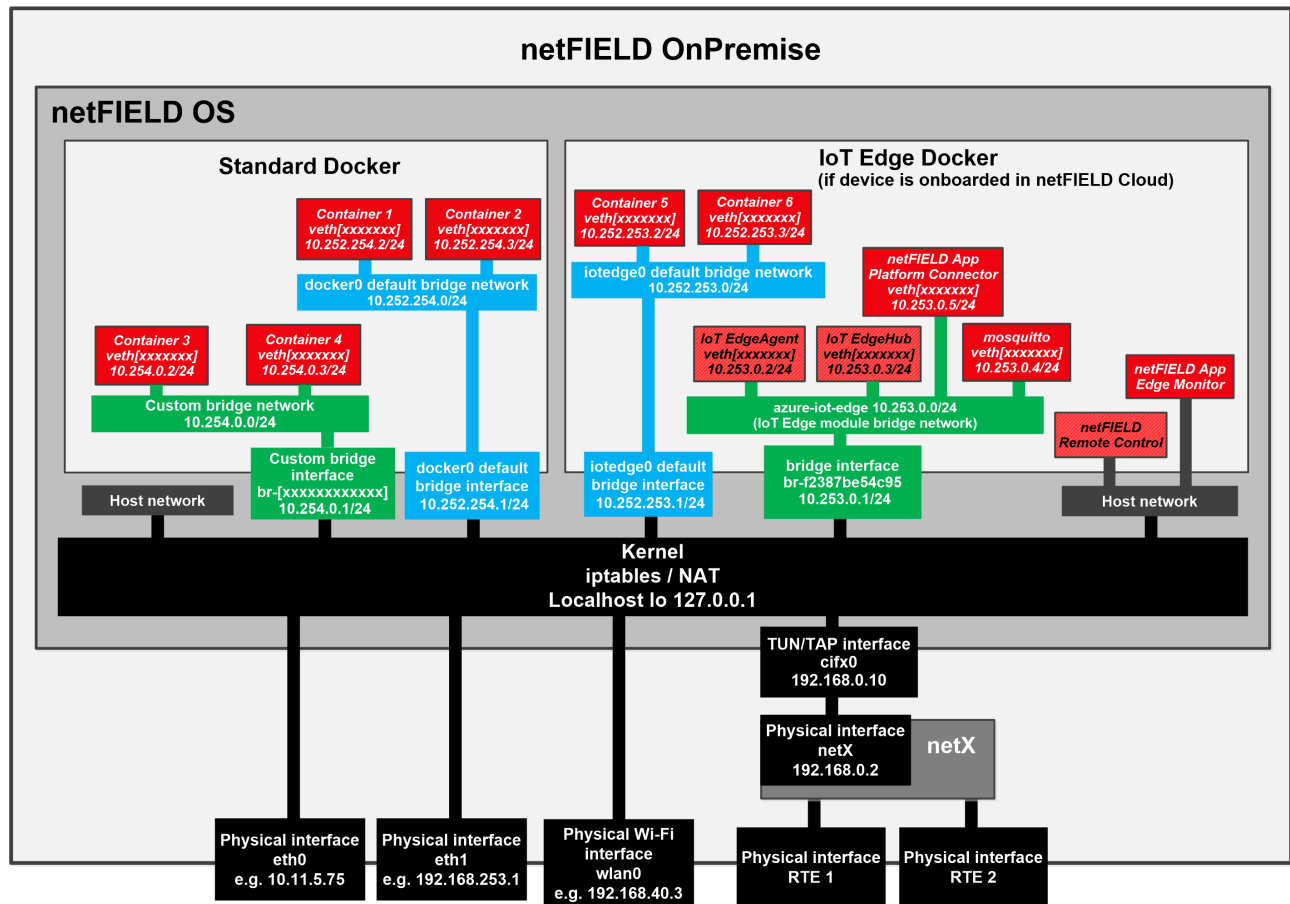


Figure 64: Default docker network configuration

## 6.6.4 Remote Access

On the **Remote Access** tab of the **General Settings** page, you can enable (on) or disable (off) *Remote Control* access from the netFIELD Portal to your device.



---

**Note:**

Note that your device must be onboarded in the netFIELD Cloud and connected to the Internet in order to use the remote control functions.

Contact your local Hilscher sales representative for information on the terms and conditions of an account/subscription for the *netFIELD Cloud services* (<https://www.netfield.io>).

---

For security reasons, remote control access is by default switched off. To allow remote control of your device, you must enable it here in the Local Device Manager *and* in the netFIELD Portal (“four-eyes-principle”).

Note that if you have updated your device from an older netFIELD OS version to version  $\geq 2.2$ , the remote access remains by default enabled (for compatibility reasons) until it is switched off by the user.



**Note:**

The “Remote Control” functions of the Portal allow you to access IP services (like e.g. HTTP(S), SSH, VNC, RDP or other TCP-based services) running on your netFIELD Edge Device/netFIELD OS (or on other devices connected to a network that is accessible by the netFIELD Edge Device/netFIELD OS) from a remote PC via a HTTPS tunnel. The HTTPS tunnel is established by the remote agent container, which is automatically downloaded and started on your device/netFIELD OS when you click the **Enable Remote Control** button on the **Overview** page of your device in the Portal for the first time.

For a detailed description of the remote control functions, see section *Remote Control* in the *netFIELD Portal* manual, DOC1907010lxxEN).

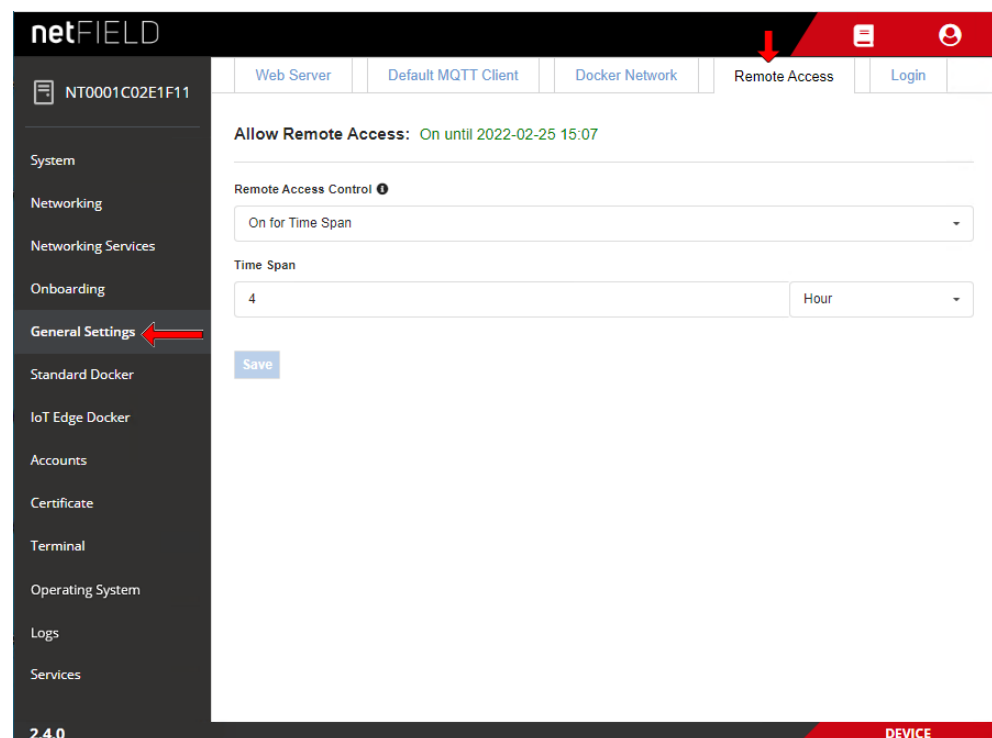


Figure 65: Remote Access tab

- In the **Remote Access Control** dropdown-list, enable (**on**) or disable (**off**) the remote access according to your use case. You can also define time limits (**On for Time Span**) for allowing remote access to the device.

**Important:**

Be aware that disabling the Remote Access and clicking the **Save** button will instantly cut off your remote connection from the netFIELD Portal to your device. Accessing the netFIELD OS will then be possible via local LAN, Wi-Fi or SSH connection only.

- Click **Save**.

## 6.6.5 Login

On the **Login** tab of the **General Settings** page, you can define a message that will be displayed on the login screen of the Local Device Manager. This allows you e.g. to implement a “system use notification” in accordance with IEC 62443.

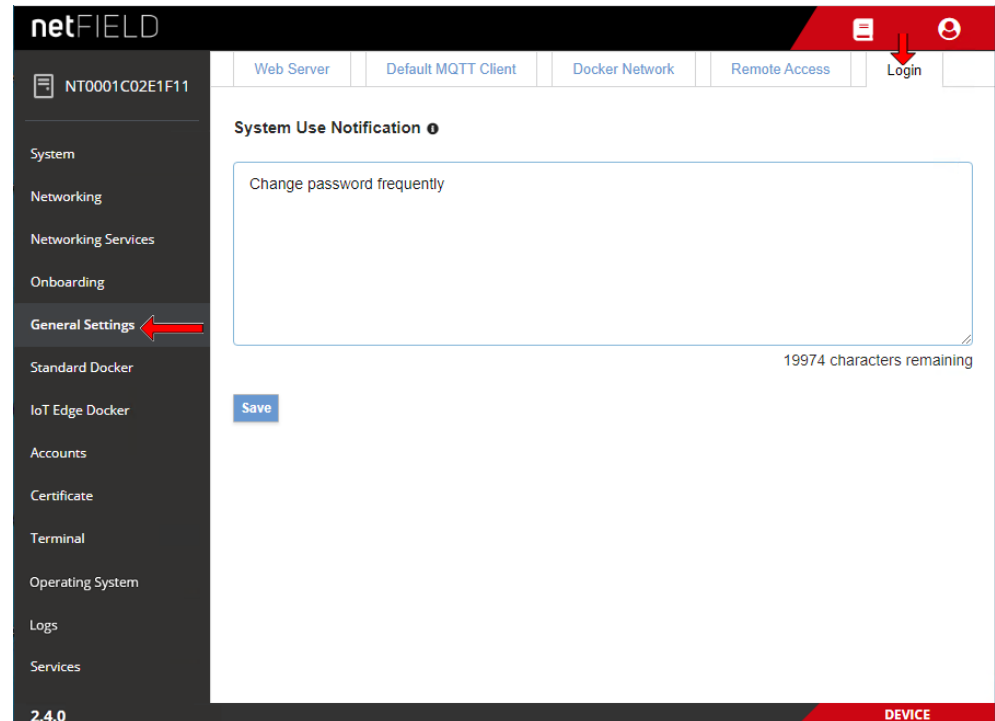


Figure 66: Login tab

- In the text field, enter the message that shall be displayed, then click **Save** button.
- The message will be displayed in the *Sign In* dialog of the Local Device Manager:

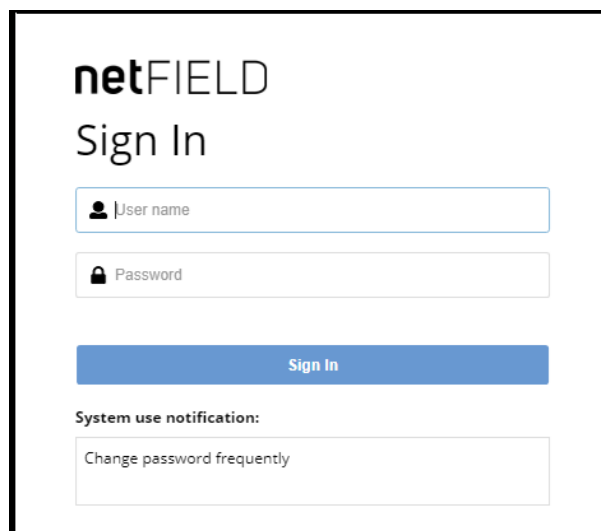


Figure 67: Notification on Sign In dialog

- To remove the message from the *Sign In* dialog again, go to **General Settings > Login** and delete the message from the text field, then click **Save** button.

## 6.7 Standard Docker

The **Standard Docker** page allows you to manage Docker images and containers from the “standard” Docker Hub or from a local repository. It lists all containers that were deployed on the device; except for those that were deployed from the netFIELD Cloud via netFIELD Portal (containers deployed from the netFIELD Cloud are listed on the **IoT Edge Docker** page – see section *IoT Edge Docker* [► page 117]).

Unlike the **IoT Edge Docker**, the Standard Docker can be used without having to “onboard” the device in the portal beforehand.

If your device is connected to the Internet, you can pull here images directly from the Docker Hub by clicking the **Get new image** link on this page.



### Note:

The network address settings of the Standard Docker can be managed under **General Settings > Docker Network Settings** (see section *Docker Network Settings* [► page 104]).

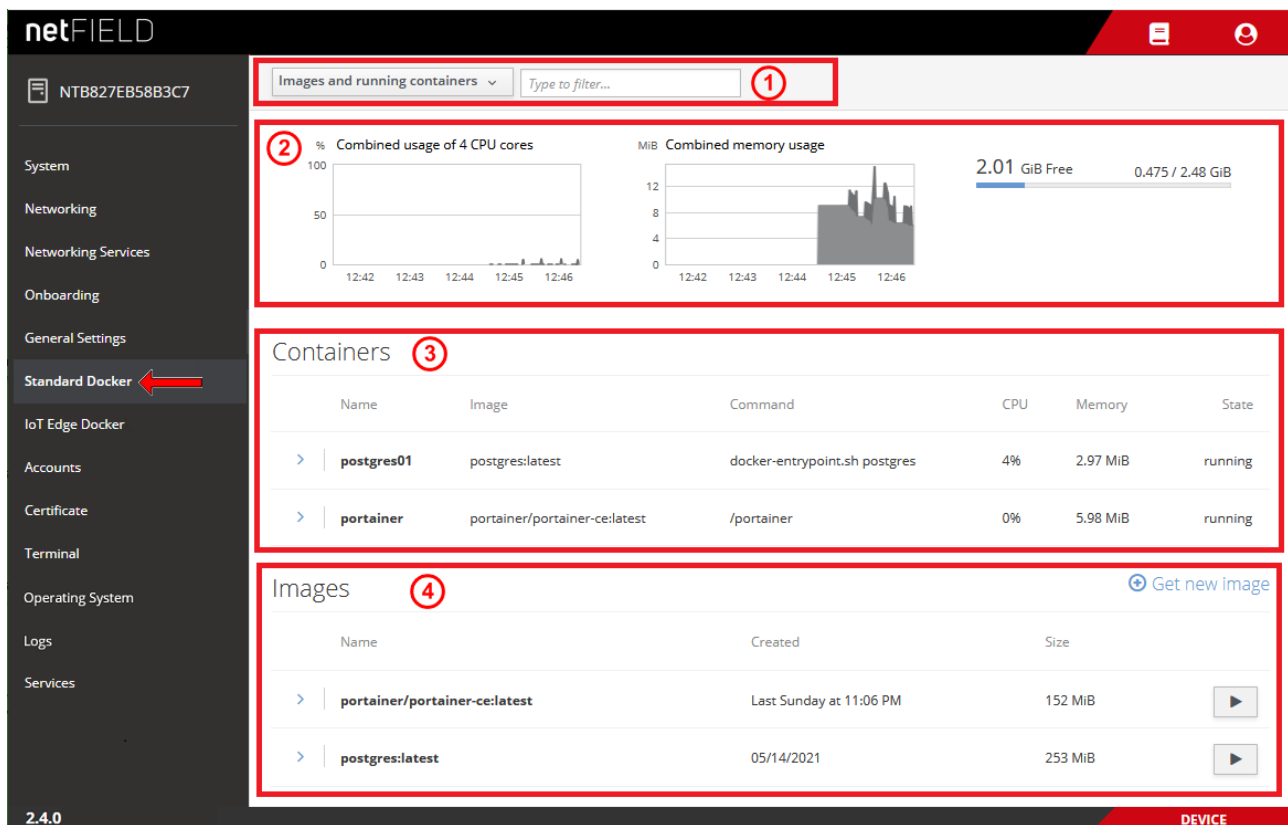


Figure 68: Standard Docker

### Filter options in header

The elements in the header (1) allow you to filter the display of containers and images.

You can choose in the drop-down list:

- **Images and running containers** – All downloaded Docker images and currently running containers are displayed (default).
- **Everything** - All Docker images and containers are displayed (including stopped containers).

Use the **Filter** field to display only certain containers.

## Graphs

The graphs (2) show you the load of the containers on the system resources.

**Combined usage of 4 CPU cores:** Load of the containers on the CPUs.

**Combined memory usage:** Load of the containers on the memory.

The graph in the upper right corner shows the amount of mass storage memory taken by the images and containers (blue bar) and the amount of mass storage left available.

## Containers

The **Containers** area (3) lists the container instances of the Docker images according to your Filter options settings in the header (1).

- To expand a box showing concise container details, or to display control buttons to restart, stop or delete it, click on the blue > arrow icon on the left of the container in the list:

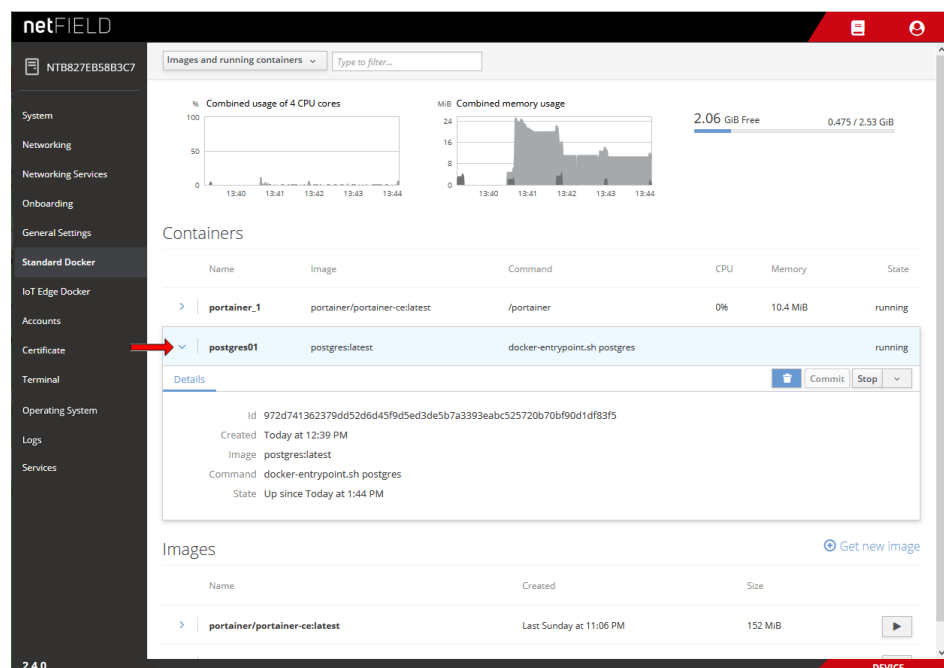


Figure 69: Expand concise container details

- To manage a container, click on it in the list.

- A page featuring detailed container information opens. Depending on its configuration, the page also includes a terminal or a “console output” window for the running container. Here you can also start, stop, restart, delete or commit the container, or change its resource limits:

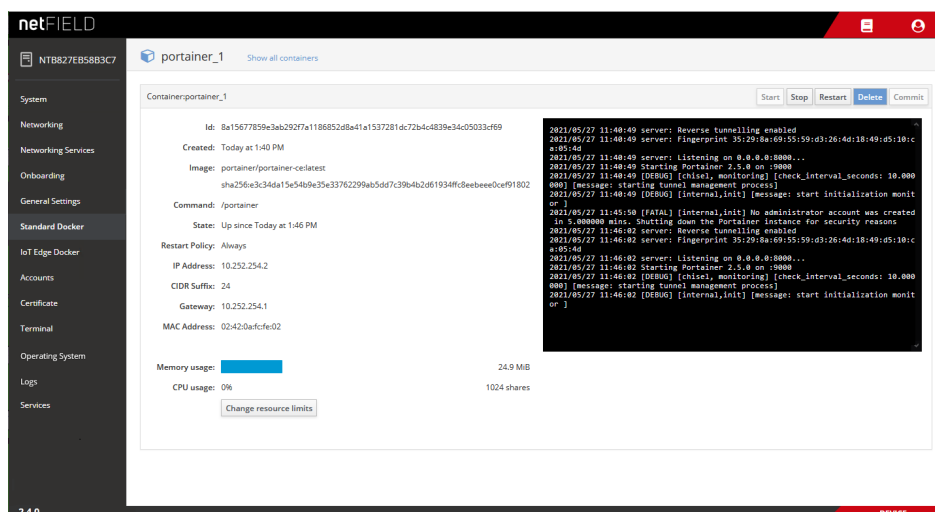


Figure 70: Container parameters with terminal window

- To go back to the **Standard Docker** overview page, click the blue **Show all containers** link in the page header.

## Images

The **Images** area (4) lists the Docker images that you have downloaded from the “standard” Docker Hub.

- You can download a Docker image by clicking the **Get new image** link.
- The **Image Search** dialog opens, allowing you to search the Docker Hub registry:

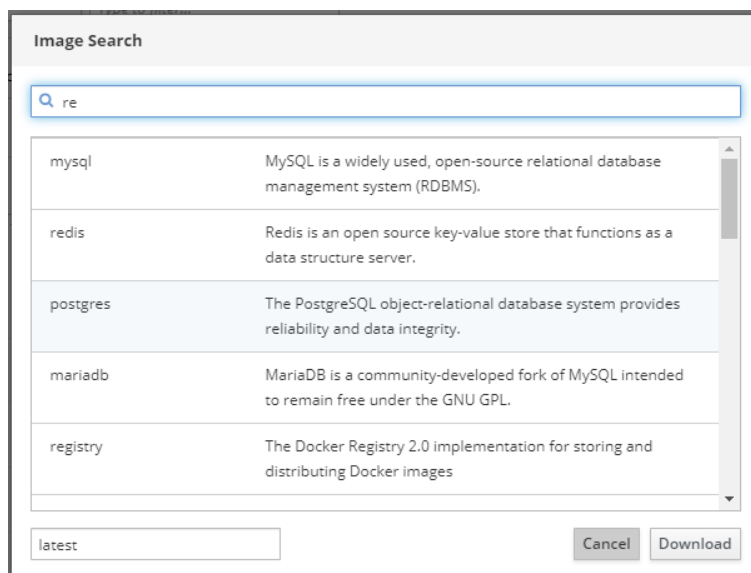

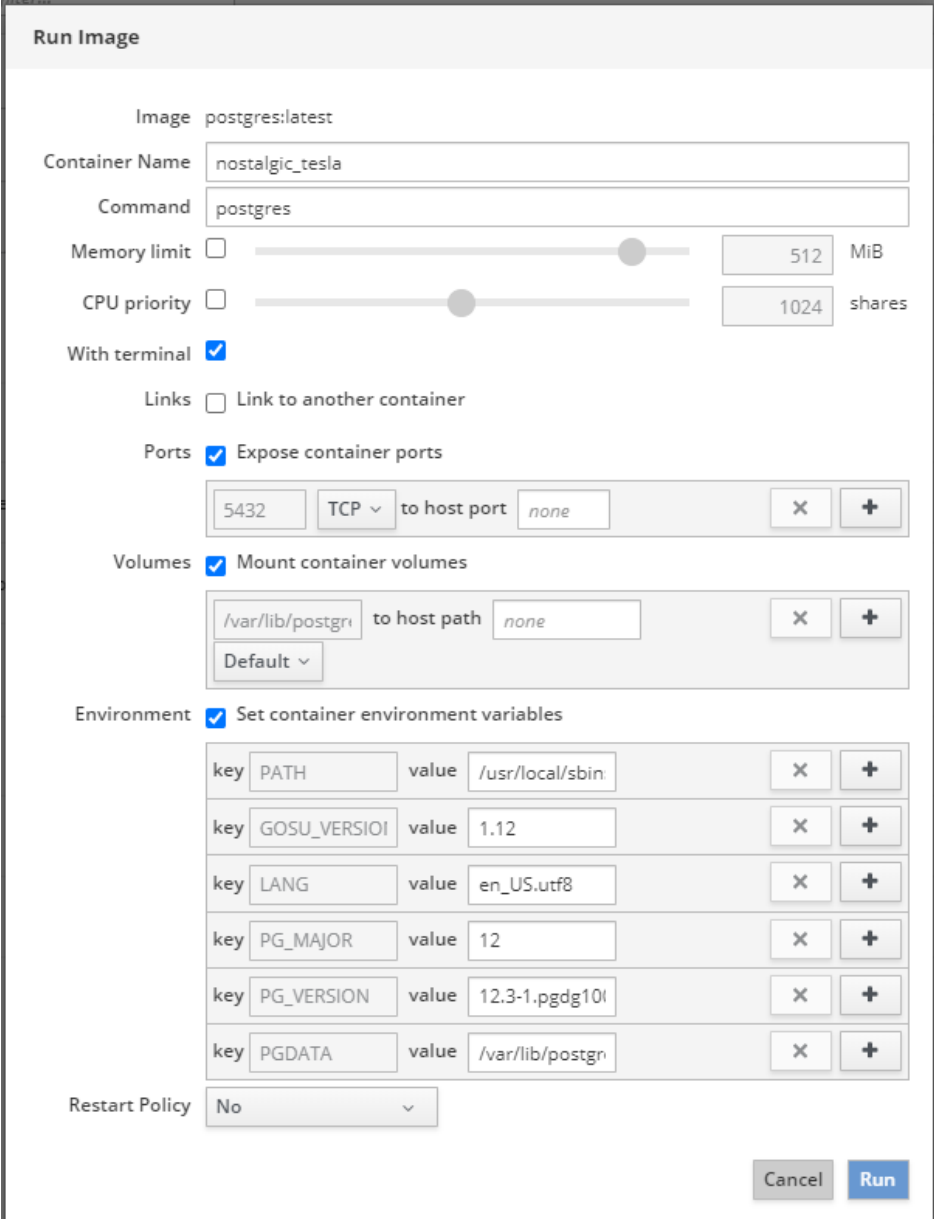


Figure 71: Image Search dialog of Standard Docker

- In the search field, type-in a name or search string, then press **Enter** on your keyboard.
- A list featuring the search results is displayed.
- Select an image in the list, then click **Download** button.
- The image is downloaded, extracted and displayed in the **Images** area.

### Starting a container

- You can start a container (i.e. run an instance of the program contained in the image), by clicking the  button on the right side of the image in the list.
- The **Run Image** dialog opens, in which you can configure the container before running it:



The **Run Image** dialog box is used to configure a container before running it. It contains the following sections:

- Image:** postgres:latest
- Container Name:** nostalgic\_tesla
- Command:** postgres
- Memory limit:** ☐ (slider set to 512) MiB
- CPU priority:** ☐ (slider set to 1024) shares
- With terminal:** ☒
- Links:** ☐ Link to another container
- Ports:** ☒ Expose container ports
  - 5432 TCP to host port none
- Volumes:** ☒ Mount container volumes
  - /var/lib/postgres to host path none
  - Default
- Environment:** ☒ Set container environment variables
 

key	value
PATH	/usr/local/sbin
GOSU_VERSION	1.12
LANG	en_US.utf8
PG_MAJOR	12
PG_VERSION	12.3-1.pgdg10l
PGDATA	/var/lib/postgres
- Restart Policy:** No

Buttons: Cancel, Run

Figure 72: Run Image dialog

**Note:**

For information about the configuration parameters and environment variables that the container requires, consult the documentation or description of the image on Docker Hub.

- To expand a box showing concise image details, or to display a control button to delete it, click on the blue > arrow icon on the left of the image in the list:

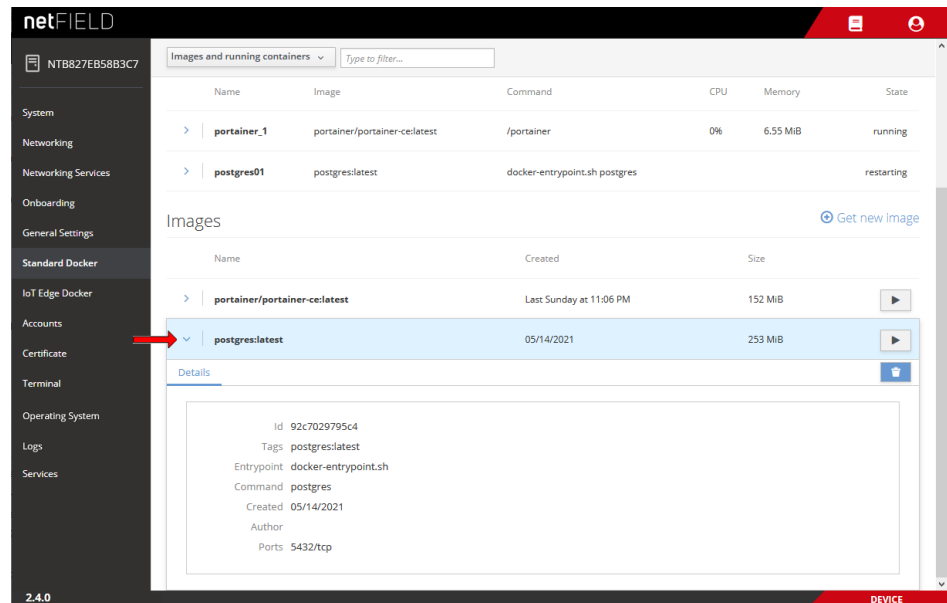


Figure 73: Expand image details

- To manage an image, click on it in the list.

➤ A page featuring detailed information opens:

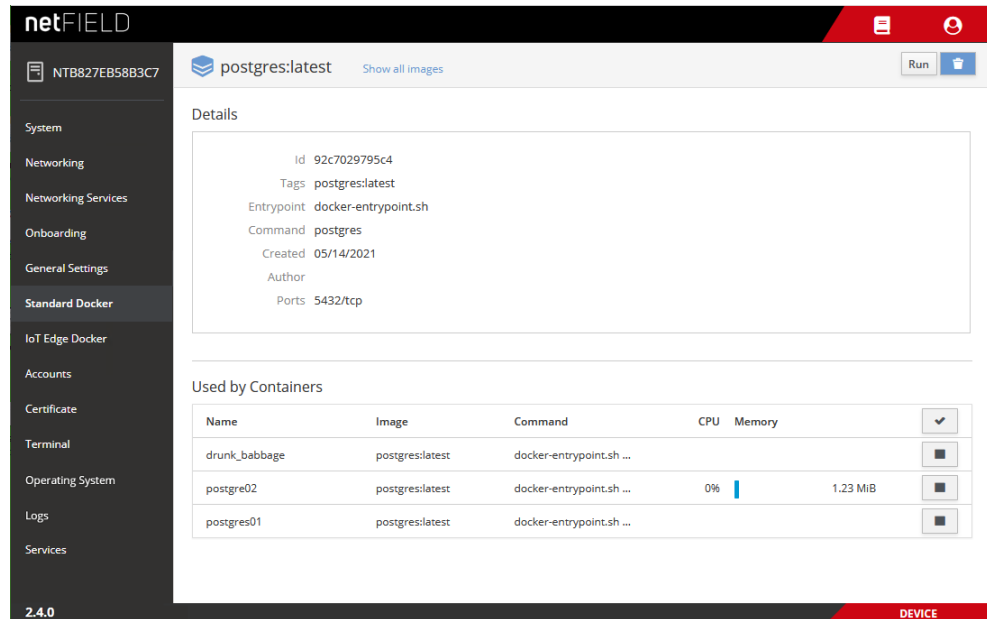





Figure 74: Image details

Here you can also start a new container for the image (by clicking the **Run** button in the header) or delete the image altogether (by clicking the  button in the header).

The **Used by Containers** area shows the containers that are running on the image (you can create more than one container of the same image), and the resources they consume. You can start or stop a container with the  and  buttons, or open the details page of the container by clicking on it in the list.

- To go back to the **Standard Docker** overview page, click the blue **Show all images** link in the page header.



#### Note:

The Standard Docker can also be managed by using Docker commands on the embedded **Terminal** page of the Local Device Manager (see section *Terminal* [▶ page 128]) or via SSH client connection (e.g. with PuTTY). For examples (e.g. “Docker Compose” support), see section *Useful CLI commands and parameters in Terminal* [▶ page 152].

You can also use the **Portainer.io** container as an additional tool for managing your Standard Docker images and containers. The Portainer.io provides a well-documented web-based management GUI that can be deployed here in the Standard Docker like any other container from the Docker Hub.



## 6.8 IoT Edge Docker

On the **IoT Edge Docker** page, you can monitor the Docker images and containers that were deployed from the netFIELD Cloud via the netFIELD Portal.

Note that you have to “onboard” your device (see section *“Onboard” (register) device in netFIELD Cloud* [▶ page 41]) before you can access this page.

Note also that you have only limited control over the images and containers here (i.e. you cannot download, configure, start or stop them here), because they are managed exclusively from the netFIELD Cloud, respectively netFIELD Portal (where you can e.g. define environment variables for a container before or after its deployment). This distinguishes the IoT Edge Docker from the Standard Docker, which allows the parameterization of containers before they are started (see section *Standard Docker* [▶ page 111]).

Here you can, however, change the limits of the resources (memory and CPU priority) that your application container is allowed to consume on the device.

You can also “remove” an obsolete container image here, but only if you have deleted it in the Device Manager of the portal beforehand. (If you delete an image only locally on the device without having deleted it in the portal beforehand, the image will be automatically deployed again).



### Note:

The network address settings of the IoT Edge Docker can be managed under **General Settings > Docker Network Settings** (see section *Docker Network Settings* [▶ page 104]).

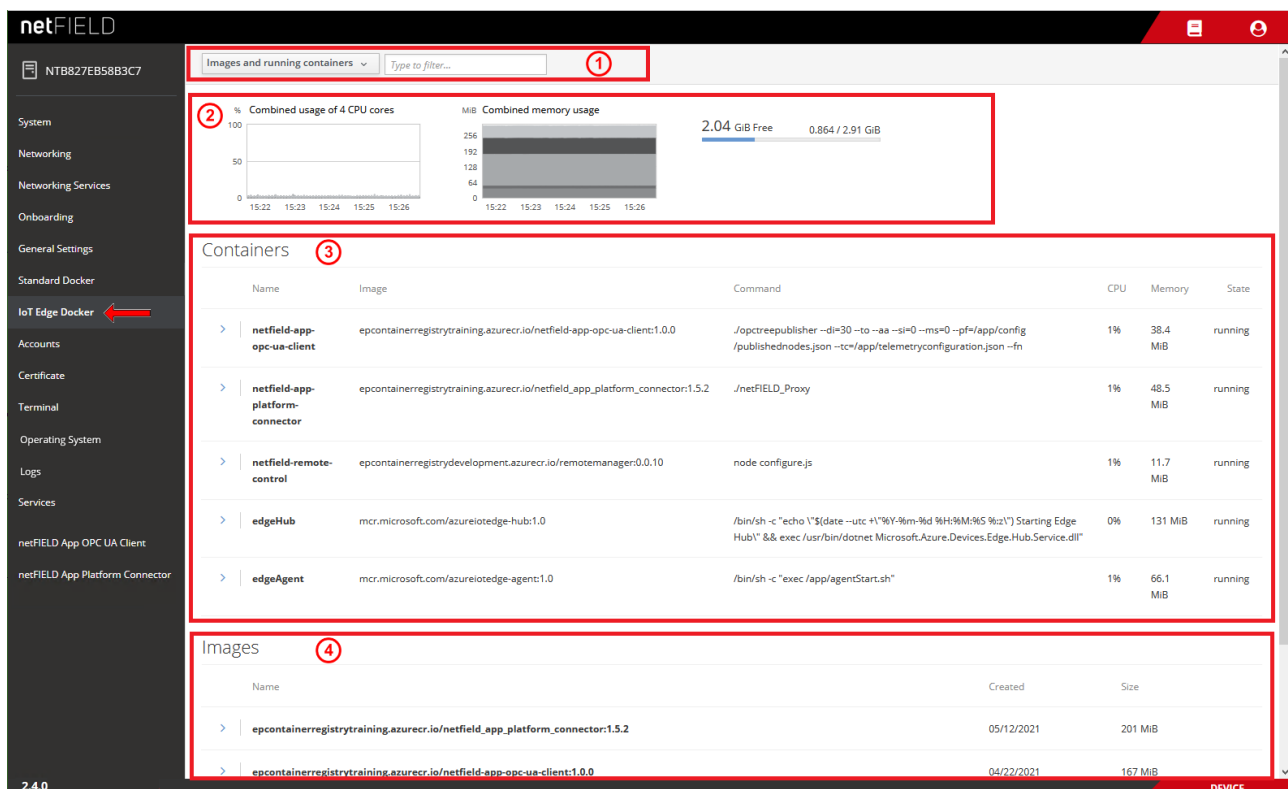


Figure 75: IOT Edge Docker

**Note:**

The *edgeHub* and *edgeAgent* are Microsoft images/containers (called “modules” in Microsoft terms) that make up the Azure IoT Edge runtime, which is necessary for connecting your device to the netFIELD Cloud (which uses the Azure cloud).

The *edgeAgent* is automatically downloaded and instantiated on the device after onboarding; the *edgeHub* is automatically downloaded and instantiated when you deploy a container from the portal for the first time.

**Filter options in header**

The elements in the header (1) allow you to filter the display of containers and images.

You can choose in the drop-down list:

- **Images and running containers** – All downloaded Docker images and currently running containers are displayed (default).
- **Everything** - All Docker images and containers are displayed (including stopped containers).

Use the **Filter** field to display only certain containers.

**Graphs**

The graphs (2) show you the load of the containers on the system resources.

**Combined usage of 4 CPU cores:** Load of the containers on the CPUs.

**Combined memory usage:** Load of the containers on the memory.

The graph in the upper right corner shows the amount of mass storage memory taken by the images and containers (blue bar) and the amount of mass storage left available.

## Containers

The **Containers** area (3) lists the container instances of the Docker images according to your Filter options settings in the header (1).

- To expand a box showing concise container details, or to display a control button to restart it, click on the blue ➤ arrow icon on the left:

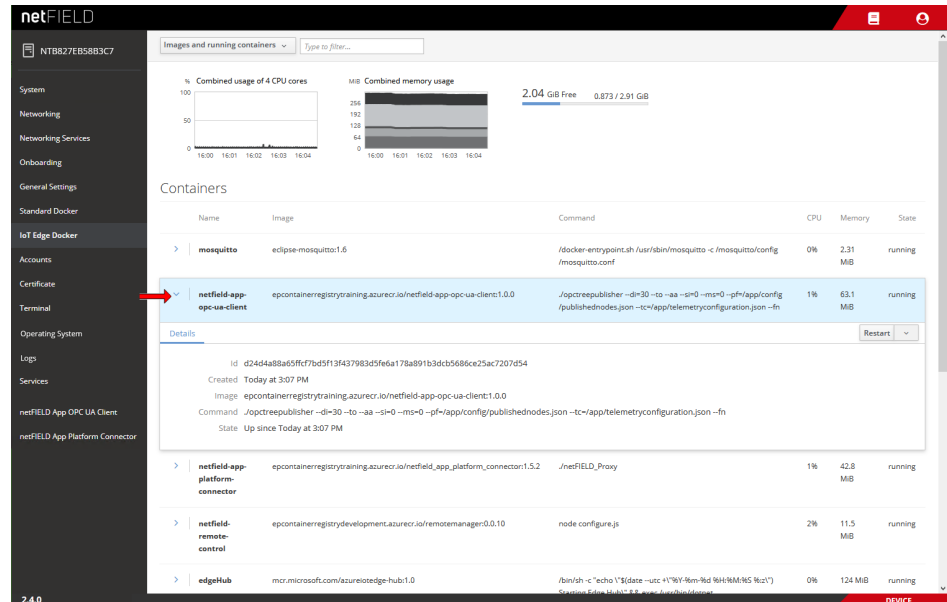


Figure 76: Container details expanded

- To display more details of the container, click on it in the list.

- A page featuring detailed information including a “console output” opens. Here you can also restart the container or change its resource limits:

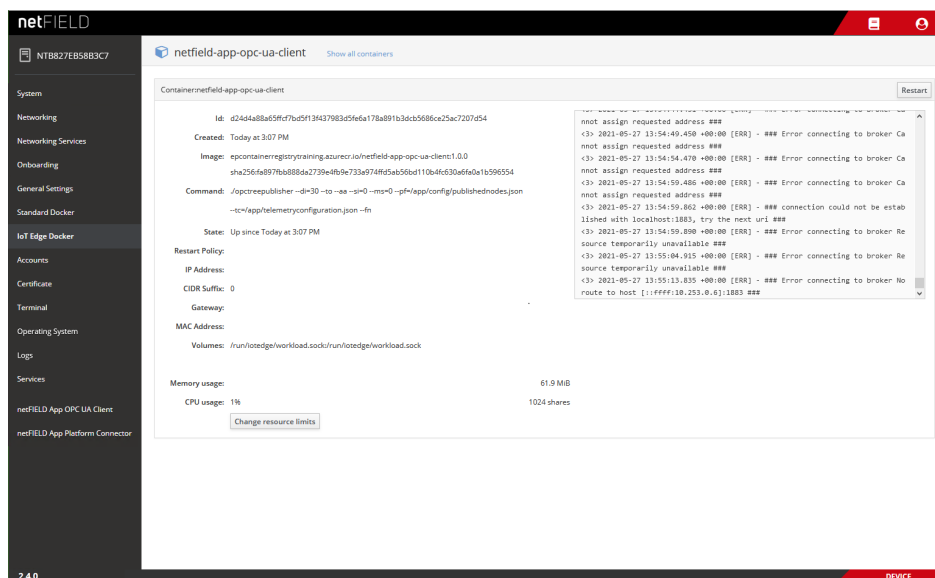


Figure 77: Container parameters

- To go back to the **IoT Edge Docker** overview page, click the blue **Show all containers** link in the page header.

## Images

The **Images** area (4) lists the Docker images that were deployed from the netFIELD Portal.



### Note:

To remove an image and its container from the device, you must first delete the container in the **Device Manager** of the portal. If you delete it only locally (i.e. here on the IoT Edge Docker page by clicking the  button) while the container is still “deployed” from the portal, the image will be automatically downloaded to the device again.

- To expand a box showing concise image details, or to display a control button to delete it, click on the blue > arrow icon on the left:

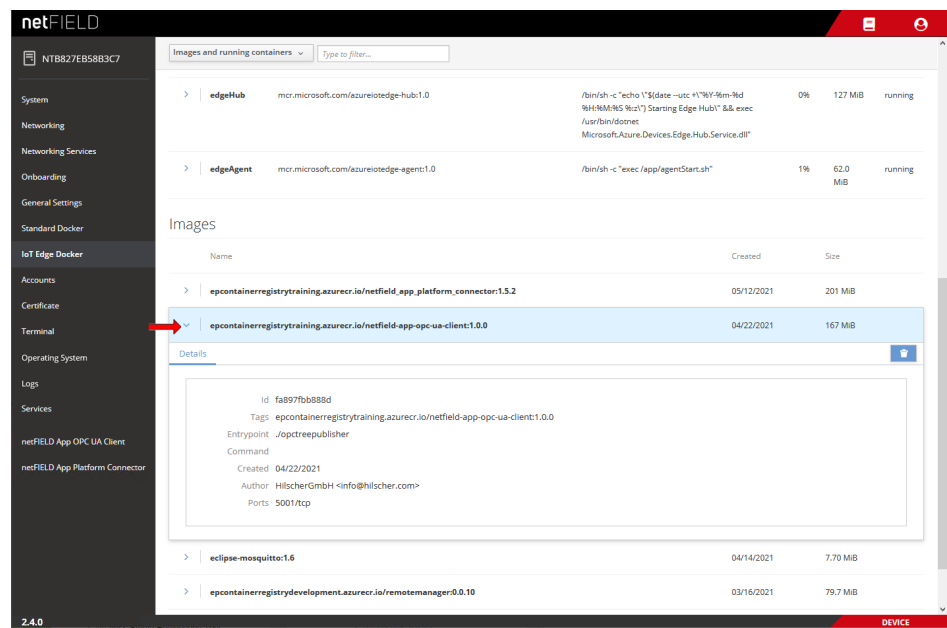


Figure 78: IoT image expanded

- To show more details of an image, click on it in the list.

➤ A page featuring detailed information opens:

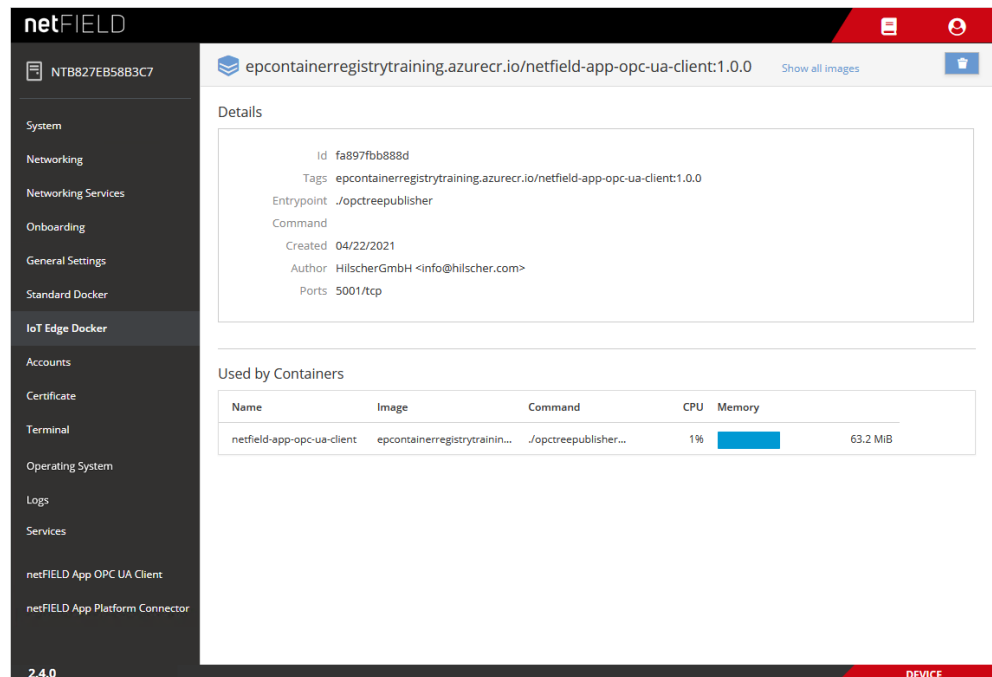


Figure 79: Details of netFIELD Proxy image

Here you can delete the image by clicking the  button.

The **Used by Containers** area shows the containers that are running on the image, and the resources they consume. You can open the details page of the container by clicking on it in the list.

- To go back to the **IoT Edge Docker** overview page, click the blue **Show all images** link in the page header.



#### Note:

The IoT Edge Docker can also be managed (with the same limitations as in the UI) by using docker commands with the CLI in the Terminal.

See section *Useful CLI commands and parameters in Terminal* [▶ page 152] for examples.

## 6.9 Accounts

On the **Accounts** page, you can manage the user accounts of the netFIELD OS.

You can create new users, change passwords and assign user roles (i.e. access rights) here. Note that only the `admin` user (*System Administrator* a.k.a *Server Administrator*) of the netFIELD OS can create new accounts and assign roles. The admin user can also arbitrarily change the passwords of all users.

However, as a “low-level” user (e.g. Container Admin) without *Server Administrator* privileges, you are allowed to change your password here.

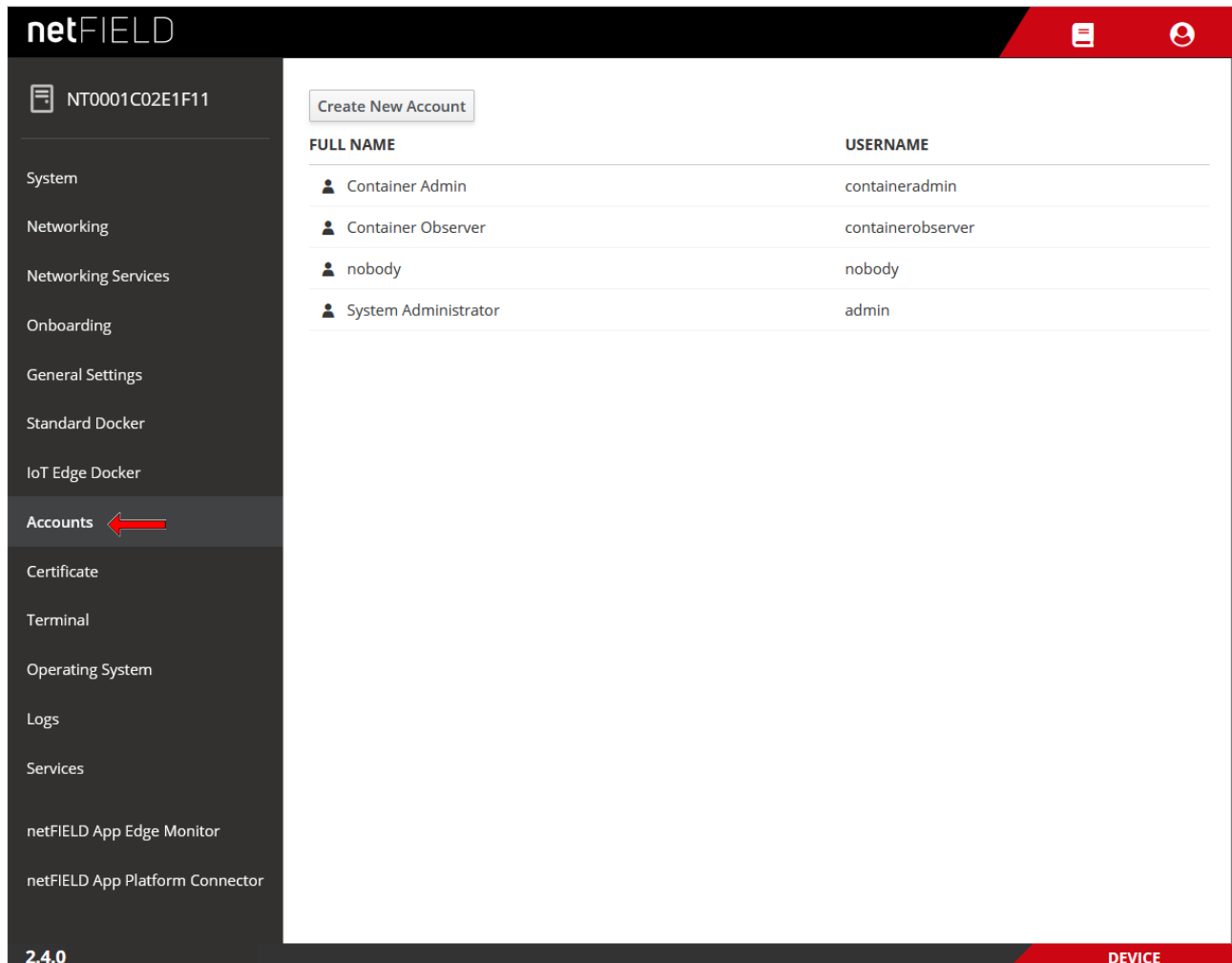
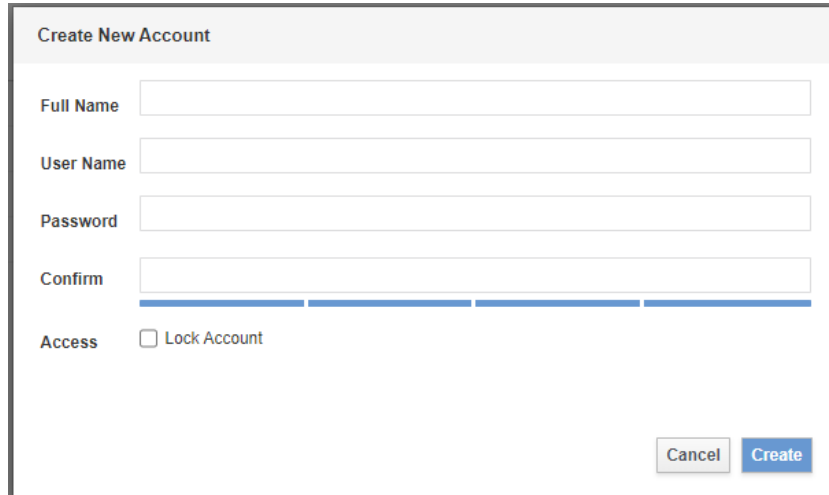


Figure 80: Accounts

- To create a new user account, click on the **Create New Account** button.

➤ The **Create New Account** dialog opens:

A dialog box titled "Create New Account" with a light gray header. It contains five input fields: "Full Name", "User Name", "Password", and "Confirm". Below the "Confirm" field is a blue progress bar. At the bottom left, there is an "Access" section with a checkbox labeled "Lock Account". At the bottom right, there are two buttons: "Cancel" and "Create".

Create New Account

Full Name

User Name

Password

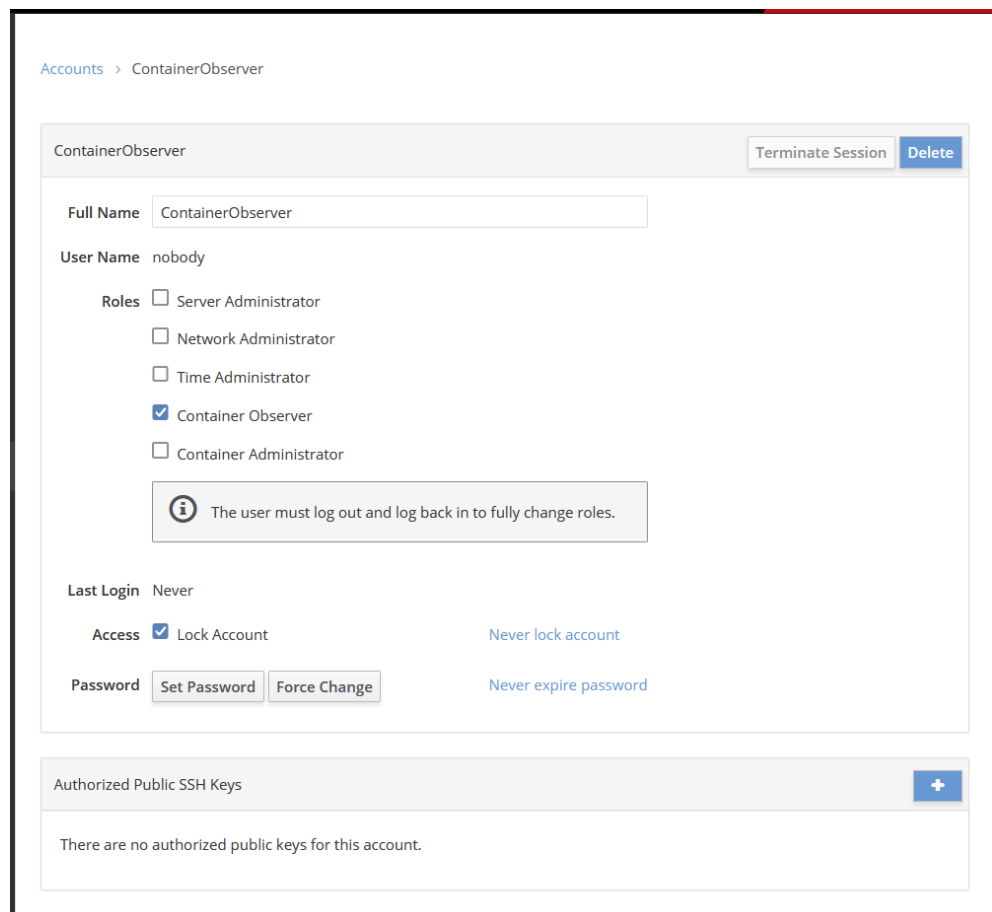
Confirm

Access ☐ Lock Account

Cancel Create

Figure 81: Create new account

- Fill in the form, then click **Create** button.
  - To configure an account (e.g. assign roles, change password or lock account), click on the name in the list.
- The configuration dialog for the account opens:

A web page titled "Accounts > ContainerObserver". It features a header bar with "ContainerObserver" and buttons for "Terminate Session" and "Delete". The main content area includes fields for "Full Name" (ContainerObserver) and "User Name" (nobody). Under "Roles", there are checkboxes for "Server Administrator", "Network Administrator", "Time Administrator", "Container Observer" (checked), and "Container Administrator". A message box states: "The user must log out and log back in to fully change roles." Below this, "Last Login" is "Never". The "Access" section has a checked "Lock Account" checkbox and a link "Never lock account". The "Password" section has "Set Password" and "Force Change" buttons, and a link "Never expire password". At the bottom, there is a section for "Authorized Public SSH Keys" with a "+" button and a message: "There are no authorized public keys for this account.".

Accounts > ContainerObserver

ContainerObserver Terminate Session Delete

Full Name ContainerObserver

User Name nobody

Roles ☐ Server Administrator  
☐ Network Administrator  
☐ Time Administrator  
☒ Container Observer  
☐ Container Administrator

*i* The user must log out and log back in to fully change roles.

Last Login Never

Access ☒ Lock Account Never lock account

Password Set Password Force Change Never expire password


Authorized Public SSH Keys +

There are no authorized public keys for this account.

Figure 82: Edit account



**Note:**

You can open the configuration dialog for your currently used account (i.e. the account you are currently logged in with) also by selecting  > **Account Settings** in the toolbar.

**Roles**

- The **Server Administrator** has full access rights to all functions of the netFIELD OS. This role adds the user to the Linux `sudo` group.
- The **Network Administrator** has full access rights to the functions of the **Networking** and **Networking Services** pages of the netFIELD OS. In addition to this, this role allows changing the **Web Server** and the **Default MQTT Client** configuration under **General Settings**. This role adds the user to the Linux `netadmin` group.  
Note that configuring the **Docker Network** under **General Settings** requires the **Network Administrator** and the **Container Administrator** roles.
- The **Time Administrator** is allowed to configure the **System Time** and define an NTP server. This role adds the user to the Linux `timeadmin` group.
- The **Container Observer** has “read” access to the functions of the **Standard Docker** and **IoT Edge Docker** of the netFIELD OS, but is not allowed to change containers or Docker settings. This role adds the user to the Linux `docker-readonly` group.
- The **Container Administrator** has full access rights to the containers and functions of the **Standard Docker** and **IoT Edge Docker**. This role adds the user to the Linux `docker` group.  
The **Container Administrator** can download container images in the **Standard Docker**, and can also start and stop the containers.  
Note that the containers running in the **IoT Edge Docker** are deployed and managed exclusively from the netFIELD Cloud, respectively netFIELD Portal. As **Container Administrator** you can, however, “clean” a netFIELD container image from the netFIELD OS after it has been deleted in the *Device Manager of the Portal*. (If you delete an image only locally on the netFIELD OS without having deleted it in the Portal beforehand, the image will be automatically deployed again).  
Note also that configuring the **Docker Network** under **General Settings** requires the **Container Administrator** and the **Network Administrator** roles.

If you assign **no role** to an account, this user will have no or only “read” access to the netFIELD OS configuration web pages.

**Note:**

Note, however, that all users who login to the **Local Device Manager** have full read and write access to the plug-in dashboards of netFIELD application containers (like e.g. *netFIELD App Platform Connector*) – regardless of the roles assigned to the user.

### Authorized Public SSH Keys

This area lists the SSH keys assigned to this account.

With a SSH key pair (private and public key), you can login (e.g. with a terminal program like *PuTTY*) to your account via netFIELD OS SSH shell by using your private key. The password is replaced by the private key, and you only have to specify a valid netFIELD OS account name (e.g. “*admin*”) for authentication when you login.

- Click on the  button to add an SSH key.

## 6.10 Certificate

On the **Certificate** page, you can manage the web server certificate of the device's web UI and turn it into a trusted one. You can display details of your currently installed certificate and upload a new certificate and the corresponding private key file in \*.pem format to the netFIELD OS.

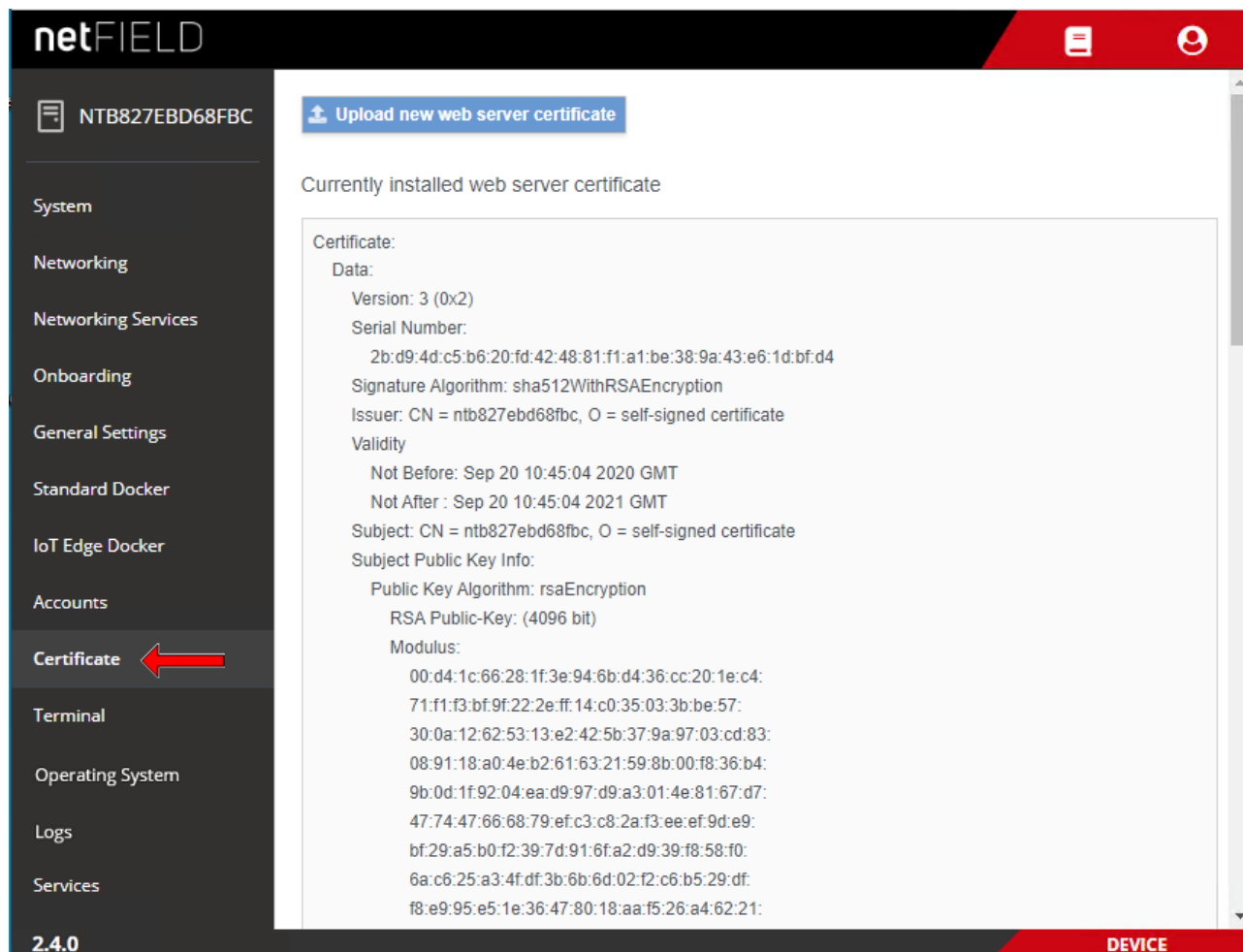


Figure 83: Web Server Certificate page



### Note:

The netFIELD OS contains a certificate issued by Hilscher. Note that the automatically created certificate is valid for one year. You can upload your own certificate to the netFIELD OS here. The corresponding root certificate should be rolled out on each of your PC/devices that you use for connecting to the netFIELD OS.

## 6.11 Terminal

The “in-browser” **Terminal** page allows command line-based administration of the netFIELD OS. Note that this is for Linux experts only.

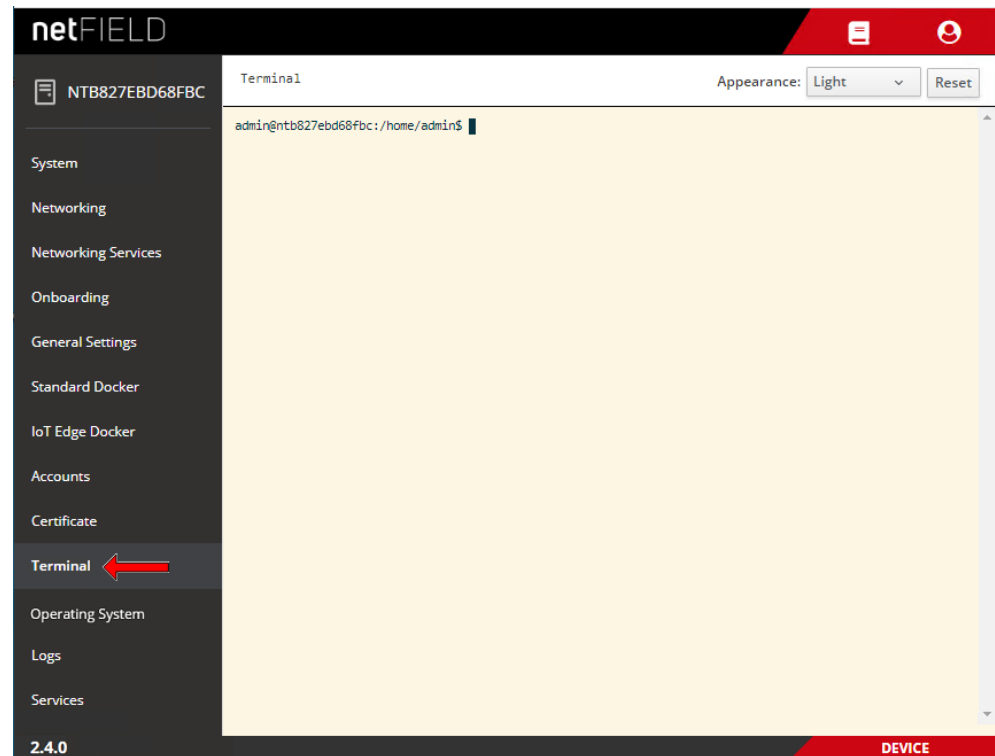


Figure 84: Terminal



### Note:

As an alternative, you can also access the netFIELD OS command line interface by using an external SSH Client (like e.g. PuTTY) via standard port 22. File transfer via SCP protocol is also supported.

For working with root privileges in the CLI, use “`sudo`”.

Examples of commands and parameters are provided in section *Useful CLI commands and parameters in Terminal* [► page 152].

## 6.12 Operating System

### 6.12.1 OS Update

The **OS Update** tab of the **Operating System** page of the Local Device Manager allows you to update the netFIELD operating system (netFIELD OS) by uploading an `swu` update file.

You can also perform an OS “Recovery” here by uploading a recovery image (also in `swu` format) instead of an update file.



---

**Important:**

Be aware of the difference between an OS *update* and a *recovery*: In an *update*, bug fixes and/or new functions will be added to the existing netFIELD OS. Your device’s configuration settings, containers, user accounts, passwords and its cloud registration (“onboarding”) will thereby be preserved.

In a *recovery*, the currently installed OS and all its settings will be fully replaced by the new recovery image, which means that individual configurations settings, containers, user accounts and passwords will be lost. After a *recovery*, you will have to reconfigure and “onboard” your device again. In this respect, the recovery is like the factory reset (see section *Factory Reset* [► page 137]), with the difference that the recovery process uses a completely new OS version, whereas the factory reset restores the “pristine” state of the currently installed OS version (by deleting all user configurations). Note that if you cannot connect to the netFIELD OS via Ethernet (e.g. because you have locked yourself out), you can perform a device recovery via USB, as described in section *Device recovery via USB* [► page 143].

---

Note that it is not possible to “downgrade” your OS; i.e. the installation of an OS version that is “older” than the currently installed OS version will be denied.

**Note:**

The netFIELD OS update process requires a certain amount of free RAM on your device. If you are running application containers with extensive memory usage, we recommend you to stop these containers before you start the update process, in order to “free” the required RAM for the process. You can restart the containers after having finished the OS Update.

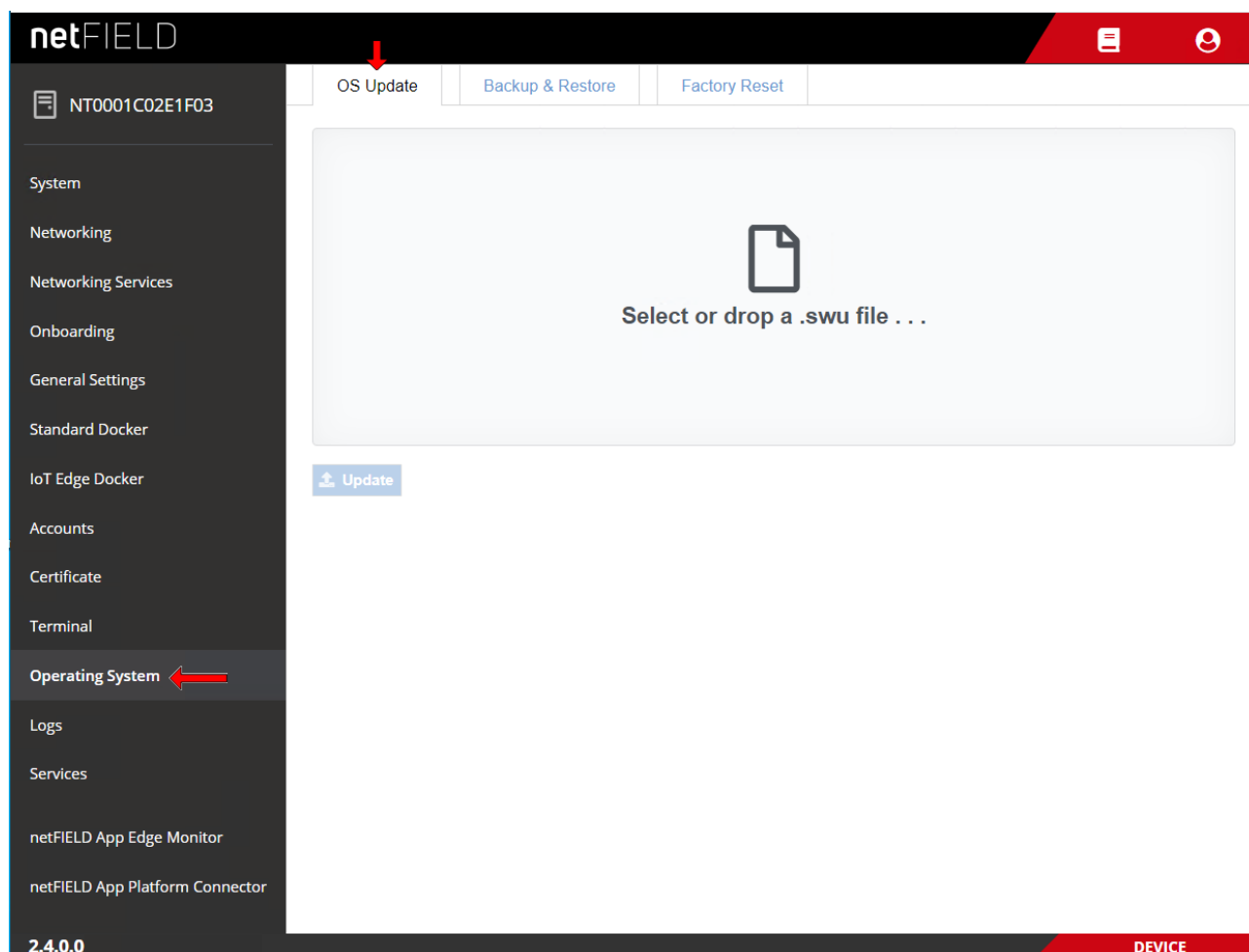


Figure 85: OS update page

**Note:**

As an alternative to using the Local Device Manager for your OS update, it is also possible to update your device’s OS from the netFIELD Portal in the cloud. However, this requires access to the portal (i.e. an account) and the deployment of the *netFIELD App Platform Connector* on your device.

Note also that you cannot update the firmware of the netX communication controller here. Updating the netX firmware requires the deployment of special containers that feature the corresponding cifX API functions.

**To update the operating system, proceed as follows:**

1. Download the update file (or recovery file) from Hilscher to your local PC.
  - Go to the **netFIELD OS Version history** page  
<https://hilscher.atlassian.net/l/cp/SBeH8aq2>  
and click on the link under **Current version**.  
On the **netFIELD OS Version [x.x]** page, scroll down to the **Downloads - netFIELD OS Edge** table and look for the **Model Name NIOT-E-TIJCX-GB-RE/NFLD**. Download the [...] **.update.swu** file that is linked under **Update via device's Web UI**.  
(Note: If you want to perform a "recovery", download the [...] **.recovery.swu** file that is linked under **Recovery with factory reset via device's Web UI**.)
2. Upload the \*.swu file from your local PC to the device.
  - On the **System Update** page, simply drag and drop the \*.swu file from your local PC onto the **Select or drop a .swu file...** field, or click into the field to open a file selection dialog.

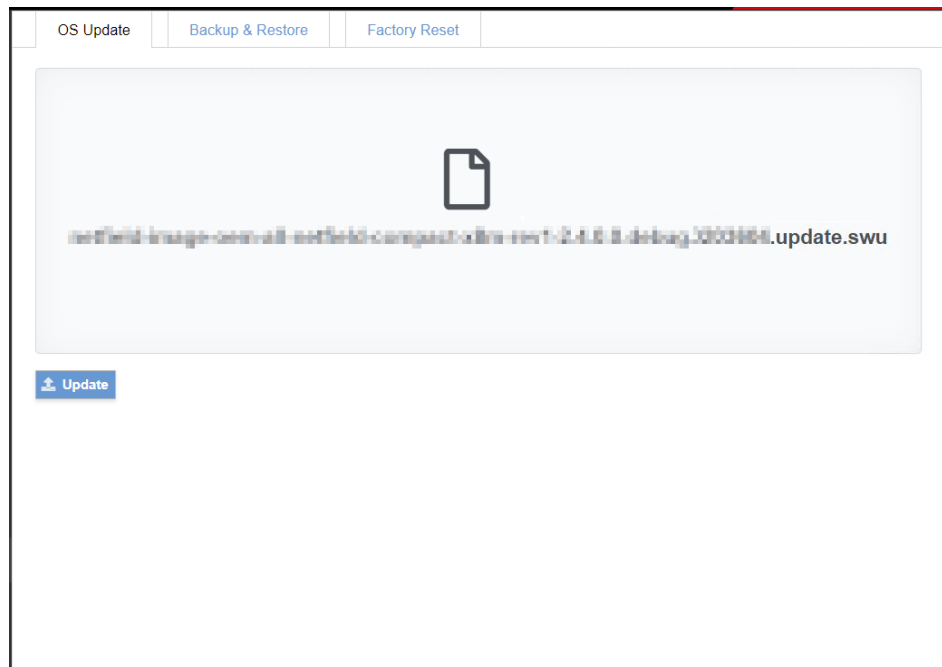


Figure 86: Selected OS update image

- After having added the update file to the field, click **Update** button.
- The **Confirmation** dialog appears.
- Because the update process cannot be aborted after confirmation, you should now check carefully whether you have selected the right update file (and not a recovery file for instance, which would delete all your configuration settings and containers).  
Click **Yes** if you want to start the update.

- The image is uploaded to the device. This might take a few minutes. After uploading has been finished, the following screen appears:

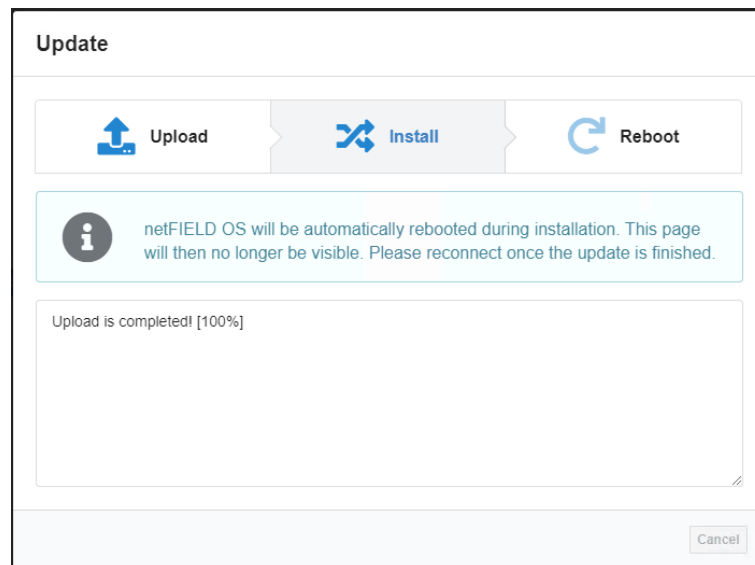


Figure 87: Upload finished message



**Note:**

If you receive an error message, this may be because of a lack of sufficient free storage memory on the hard drive. To remedy this, restart the netFIELD OS, then try again. The restart will clear remanent data from the hard drive and provide sufficient space for buffering the update file.

The installation process (i.e. the actual update of the OS) is automatically started. The device reboots and closes the LAN connection.

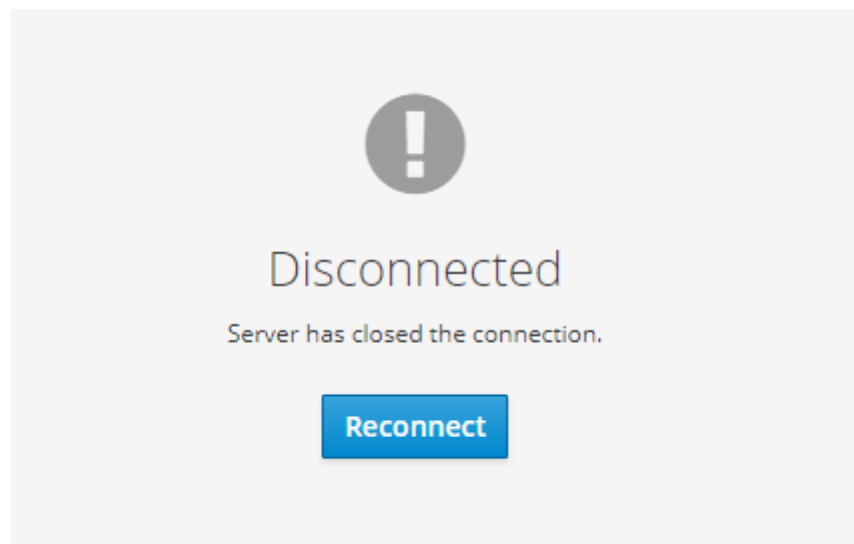


Figure 88: OS update “Disconnected” message

- Click **Reconnect** button.
- ⇒ You have updated the OS of your device. You can now sign-in again with your usual login credentials. The new firmware version is indicated in the bottom left corner of the **Local Device Manager** screen.



**Note:**

If you have performed a *recovery* (by uploading and installing a recovery image) instead of an *update*, all configuration settings have been deleted, and you now must commission the device again (see chapter *Commissioning and first steps* [▶ page 26]).

## 6.12.2 Backup & Restore

The **Backup & Restore** tab of the **Operating System** page of the Local Device Manager allows you to save (backup) and restore the current configuration (including Docker containers) or the full system (including the netFIELD OS/firmware) of your netFIELD Edge Gateway.

You can store the backup files either on the designated backup partition on the device itself and/or download the backup files e.g. to your engineering PC.

You can create as many backups as you like; note however, that each device has a limited amount of designated backup storage capacity (which is indicated in the upper right corner of the screen); therefore it might be prudent to delete old obsolete backup files on your device or download and store them on your engineering PC instead.

The screenshot shows the netFIELD Local Device Manager interface. The sidebar on the left lists various system settings, with 'Operating System' highlighted. The top navigation bar has three tabs: 'OS Update', 'Backup & Restore' (selected), and 'Factory Reset'. The main content area is divided into three sections:

- Available Backup Files:** A table showing existing backup files with columns for File Name, Size, Date, and Action.
- Create System Backup:** A section for creating a new backup, including fields for File Name, Password, and Confirm Password, and a 'Create' button.
- Restore a System Backup:** A section for restoring a backup, featuring a file selection area and a Password field.



File Name	Size	Date	Action
NT0001C02E1F11_config_august_22_pw-protected.fsa	578 MB	2022-08-01 16:05:38	
NT0001C02E1F11_config_sept_22_no_pw.fsa	578 MB	2022-09-01 15:34:35	
NT0001C02E1F11_full_backup_sept_pw-protected.fsa	877 MB	2022-09-01 16:01:06	

Figure 89: Backup and Restore tab

**NOTICE****Risk of device destruction by using the wrong backup file for system restoration!**

When restoring your device, make sure to use a backup file that was created for your *netFIELD OnPremise* hardware model.

Using a backup file that was made for a different netFIELD Edge Gateway model can damage your device.

Element	Description	
Available Backup Files	The table displays the backup files that have already been created.	
	File Name	Name of the backup file.
	Size	Size of the backup file.
	Date	Date and time of the creation of the backup file.
	Action	<div>  Delete backup file. </div> <div>  Download backup file. </div>
Free disk space	Indicates the available space for storing backup files on the device (designated backup partition). The green value in brackets shows the percentage of the designated backup space that is already consumed.	
Create System Backup	Create here new backup files.	
	File Name	Enter here a name for the backup file that you want to create. <b>Note:</b> The name must end with the suffix <code>.fsa</code> Blank spaces and special characters are not allowed. We recommend you to use a "telling" name, indicating a device ID and the backup type, e.g. <code>NT0002A233E553_full_backup_august_2022_pw-protected.fsa</code>
	Password	Enter here a password if you want to encrypt and protect the backup file with a password. <b>Note:</b> In this case, you will have to provide the same password again when you are restoring your system with the backup file.
	Confirm Password	Re-enter here your password.
	Mode	Select here the backup type. <div> Backup configuration only <div> This option saves all user-made settings and application data of your netFIELD Edge Gateway, including <ul style="list-style-type: none"> <li>• Docker containers</li> <li>• User accounts</li> <li>• Network settings</li> <li>• Onboarding</li> <li>• Log files</li> </ul> </div> </div> <div> Backup full system <div> This option saves all user-made settings and application data plus the currently installed netFIELD OS itself. </div> </div>
	Create	Click here to create the backup file.

Element	Description
Restore a System Backup	<p><b>Note:</b> In order to restore your system, you have to upload the corresponding backup file from your engineering PC. If you want to use a backup file from your <b>Available Backup Files</b> list, you have to download it to your engineering PC first, before you can upload it to use it to restore your system.</p>
Select or drop a backup file	Click here to open the upload dialog of your browser, in which you can select your backup file. As an alternative, you can also drag & drop the file from your desktop onto this field.
Password	If your backup file was created with password protection, enter here the corresponding password.
Upload & Restore	<p>Click here to upload the backup file and restore your system with it.</p> <p><b>NOTICE</b> Using the wrong backup file can damage your Edge Gateway!</p> <p>Make sure that you have selected the appropriate backup file for your Edge Gateway hardware model!</p>

Table 31: Elements in Backup &amp; Restore tab

**Note:**

If you cannot connect to the netFIELD OS via Ethernet (e.g. because you have locked yourself out), you can perform a device recovery via USB, as described in section *Device recovery via USB* [► page 143].

## 6.12.3 Factory Reset

The **Factory Reset** tab of the **Operating System** page of the Local Device Manager allows you to restore the currently installed OS version to its original “pristine” state.



### Important:

Note that thereby all individual configuration settings, Docker containers, user accounts and passwords will be lost and you will have to commission, reconfigure and “onboard” your device again (see chapter *Commissioning and first steps* [► page 26]). The password of the admin user will be reset to `admin` again.

We recommend you to create configuration backup files (see section *Backup & Restore* [► page 134]) before performing the factory reset. Note that the backup files stored on your device will “survive” the factory reset. After having reconnected to the device after the reset, you can use a configuration backup file to restore your device to the backed-up state (including onboarding and container deployment).

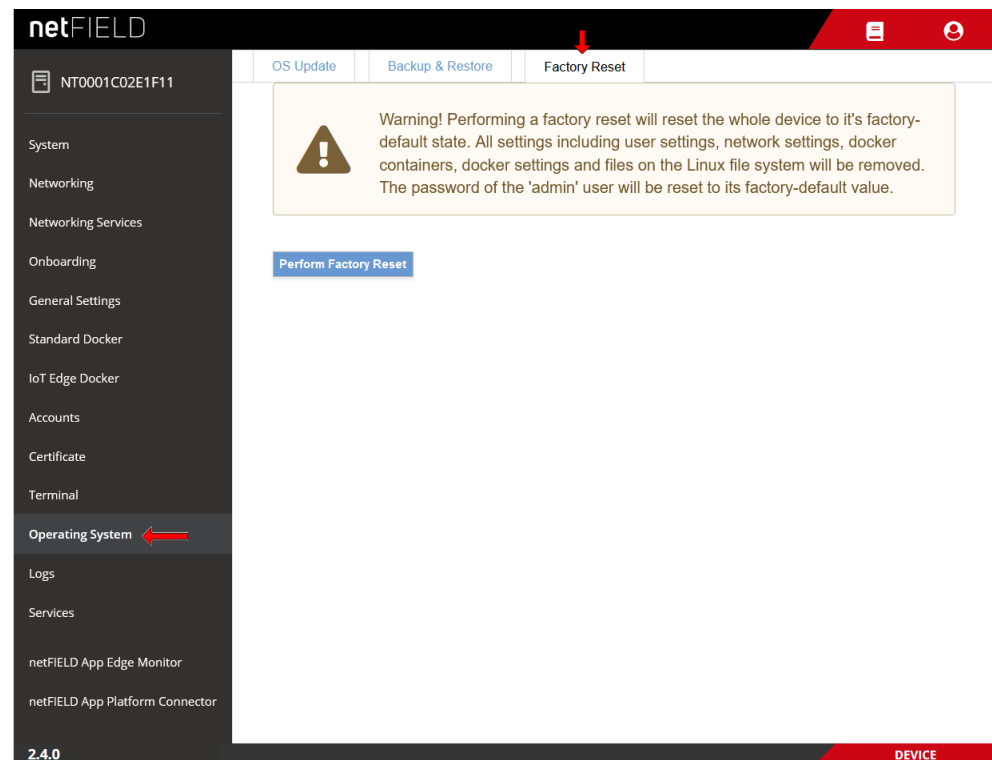


Figure 90: Factory Reset



### Note:

If you cannot connect to the netFIELD OS via Ethernet (e.g. because you have locked yourself out), you can perform a device recovery via USB, as described in section *Device recovery via USB* [► page 143].

## 6.13 Logs

The **Logs** page allows you to monitor the messages produced by the `systemd journal`.

- In the drop-down lists in the header, you can filter the messages by time/date, **Severity** (type) and **Service** (i.e. the “service” that issued the message).
- Click on a message in the list to display the information in full detail.

The screenshot shows the netFIELD web interface. On the left, a dark sidebar contains a menu with items like System, Networking, and Logs. A red arrow points to the 'Logs' item. The main content area is titled 'FEBRUARY 28, 2022' and shows a list of log entries. At the top of this area are filters for date (February 28, 2022), severity (Warning and above), and service (All). The log entries include timestamps, messages, and service names like 'cockpit-bridge'. The bottom of the interface shows the version '2.4.0' and a 'DEVICE' button.

Figure 91: Logs

## 6.14 Services

### Overview

The **Services** page allows you to manage and monitor services of the netFIELD OS.



#### Important:

Note that this feature is for expert users only! Changing the state or the startup settings of a service here can lead to malfunctioning of the netFIELD OS respectively of your device!

NAME	DESCRIPTION	STATE	AUTOMATIC STARTUP
alsa-restore.service	Save/Restore Sound Card State	inactive (dead)	Static
alsa-state.service	Manage Sound Card State (restore and store)	inactive (dead)	Static
apparmor.service	AppArmor initialization	active (exited)	Enabled
auditd.service	Security Auditing Service	active (running)	Enabled
autovt@.service	autovt@.service Template		
avahi-daemon.service	Avahi mDNS/DNS-SD Stack	active (running)	Enabled
aziot-certd.service	Azure IoT Certificates Service	active (running)	Disabled
aziot-edged.service	Azure IoT Edge daemon	active (running)	Enabled
aziot-identityd.service	Azure IoT Identity Service	active (running)	Disabled
aziot-keyd.service	Azure IoT Keys Service	active (running)	Disabled
aziot-tpmd.service	Azure IoT TPM Service	inactive (dead)	Disabled
blk-availability.service	Availability of block devices	inactive (dead)	Disabled
bluetooth-start.service	Run hciattach when HCI UART device becomes available	inactive (dead)	Disabled
bluetooth.service	Bluetooth service	inactive (dead)	Enabled
busybox-klogd.service	Kernel Logging Service	inactive (dead)	Disabled
busybox-syslog.service	System Logging Service	inactive (dead)	Disabled
cifxeth.service	LSB: Raise and configure the netX based virtual ethernet interfaces	inactive (dead)	Static

Figure 92: Services page

- (1) Click the tabs in the header to select a service type.
- (2) In the filter field, you can perform a text search for name and description of a service.  
To remove the filter, delete the text in the field.
- (3) In the drop-down list, you can filter the services by their automatic startup setting; i.e. **Static**, **Enabled** and **Disabled**.
- (4) List of services showing their current states and automatic startup settings.

## Service details/settings page

- Click on a service in the list to display further information (including the service logs) and/or to change its running state or startup settings.
- 🔗 The details/settings page of the service opens:

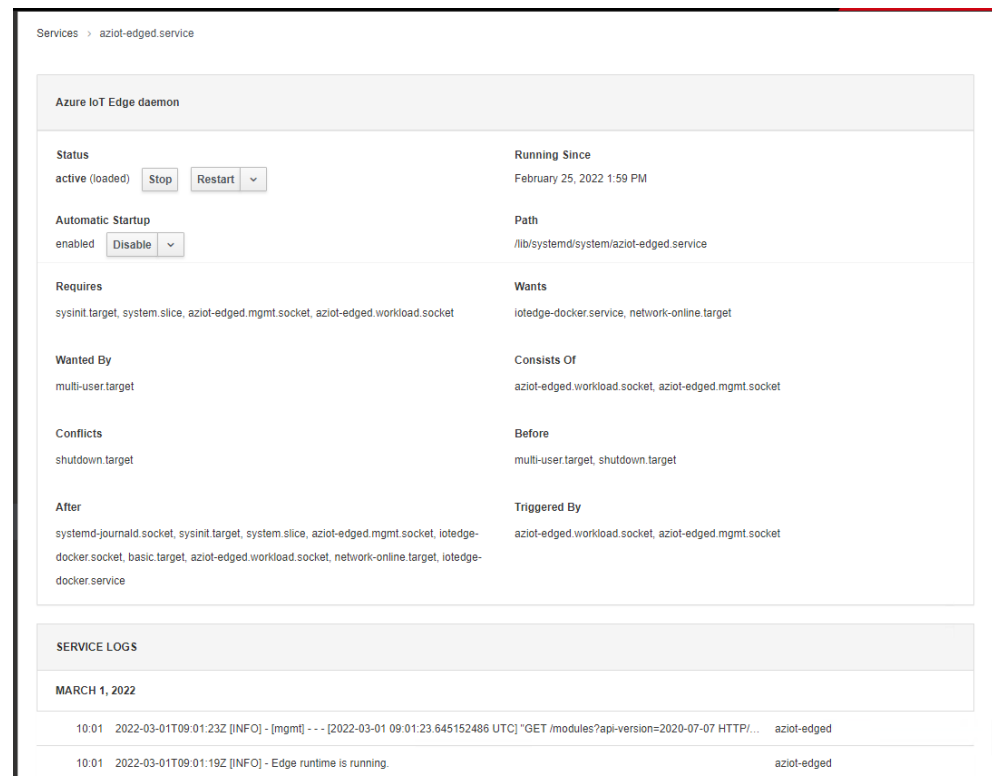


Figure 93: Service details and settings page

The buttons in the **Status** section allow you to **Stop/Start** or **Restart/Reload** the service.

The drop-down button in the **Automatic Startup** section allows you to configure the startup behavior of the service like e.g. “masking” it in order to prevent the service from running.

Other services that are related to the service (e.g. required services displayed under **Requires**) are displayed as clickable links.

The log messages of the service are displayed under **SERVICE LOGS** in the footer.



Managing Timers

On the **Timers** tab, you can display existing timers and create new timer units. A timer allows you to execute a certain command at a certain time.

TargetsSystem ServicesSocketsTimersPaths

Create Timer

Filter by name or description...All

NAME	DESCRIPTION	NEXT RUN	LAST TRIGGER	STATE	AUTOMATIC STARTUP
flush-journal.timer	Weekly flushing of journal			inactive (dead)	Enabled
logrotate.timer	Daily rotation of log files	Sat, 03 Sep 2022 00:00:00 CEST	Fri, 02 Sep 2022 08:28:44 CEST	active (waiting)	Enabled
systemd-tmpfiles-clean.timer	Daily Cleanup of Temporary Directories	Sat, 03 Sep 2022 12:06:32 CEST	Fri, 02 Sep 2022 12:06:33 CEST	active (waiting)	Static

Figure 94: Service types: Timers

- Click on a timer in the list to display further information and/or to change its running state or startup settings.
- To configure a new timer, click **Create Timer** button in the header.
- The **Create Timers** dialog opens:

Create Timers

Service nameflush-journal

DescriptionWeekly flushing of journal

Commandsystemd-journal-flush.service

RunAt specific time

Repeat Weekly

Monday11:00

CancelSave

Figure 95: Create timer dialog

- In the **Command** field, enter the name of the service that shall be triggered by the timer.
- Set all desired parameters, then click **Save** button.

**Note:**

Note that you can create but cannot delete timers here. (You can however stop a timer here by opening its details/settings page, then clicking the **Stop** button in the **Status** section).

To remove a timer completely, you have to use the **Terminal** to delete it manually in the corresponding `systemd` configuration.

## 7 Good to know...

### 7.1 Device recovery via USB

#### 7.1.1 Overview

This section describes how to reset the netFIELD OS of your device by installing a “recovery” image firmware from a USB stick.

A device recovery via USB can be necessary if the netFIELD OS has become instable or corrupted, or if you have “locked yourself out” of the **Local Device Manager** because you have deactivated or misconfigured its LAN or Wi-Fi interfaces (eth0, eth1 and wlan0), or if you have forgotten the administrator’s password.

Note that it is not possible to “downgrade” your OS; i.e. the installation of an OS version that is “older” than the currently installed OS version is not supported.



---

**Important:**

Note that in a recovery, all configuration settings, user accounts and deployed containers of the current netFIELD OS will be deleted. This means that you will have to commission and configure your device again after the recovery procedure.

Note also that the firmware of the netX communication controller will not be affected by the recovery.

---

#### 7.1.2 Requirements

- USB stick with a minimum of 500 MByte storage capacity, FAT32 formatted



---

**Note:**

USB sticks with a storage capacity of more than 64 GByte cannot be easily formatted under Windows in FAT32. If you intend to use such a high-capacity stick, use a tool like e. g. HP USB STICK FORMAT to format the stick under Windows.

---

- USB keyboard
- Monitor with DVI-I or DP connector



---

**Important:**

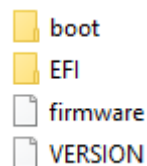
Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the gateway.

---

- You have downloaded the recovery image from Hilscher to your local PC (see step-by-step instructions for details).
- You have physical access to the device (in order to plug-in the USB stick and to connect keyboard and monitor).

### 7.1.3 Step-by-step instructions

1. Download the zip archive containing the recovery image from Hilscher to your local PC and unpack it.
  - Go to the **netFIELD OS Version history** page  
<https://hilscher.atlassian.net/l/cp/SBeH8aq2>  
 and click on the link under **Current version**.  
 On the **netFIELD OS Version [x.x]** page, scroll down to the **Downloads - netFIELD OS Edge** table.
  - Look for the **Model Name NIOT-E-TIJCX-GB-RE/NFLD** and download the [...] **.recovery.zip** file that is linked under **Recovery/Upgrade with factory reset via USB memory stick**.
  - Use a tool like **7-Zip** to unpack the downloaded zip archive on your local PC.
  - The unpacked folder contains the following folders and files, which you will later have to copy onto the USB stick (after having formatted the stick):



2. Format and rename USB stick.
  - Connect the USB stick to your Windows PC.



#### Note:

USB sticks with a storage capacity of more than 64 GByte cannot be easily formatted under Windows in FAT32. If you intend to use such a high-capacity stick, use a tool like e. g. HP USB STICK FORMAT to format the stick under Windows.

- Open the Windows Explorer.
- Select the USB stick and choose **Format...** from the context menu.

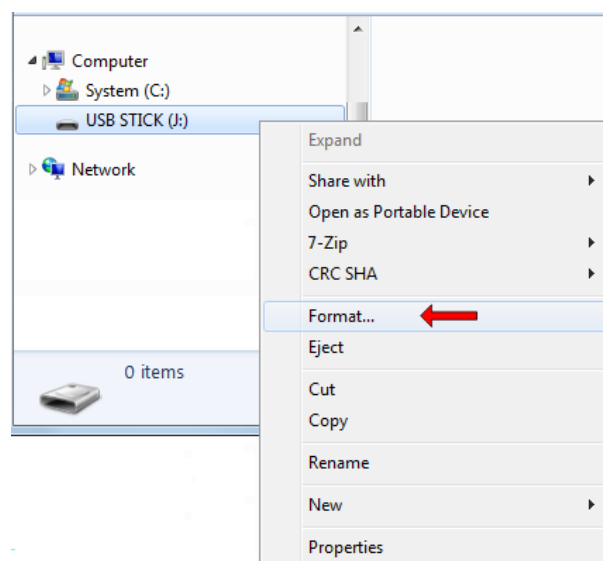


Figure 96: Formatting USB stick

- The **Format USB STICK** dialog window opens:

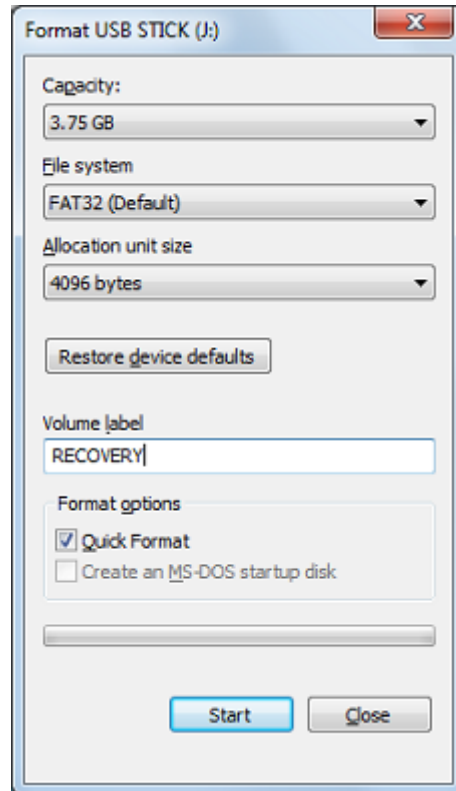


Figure 97: Format USB STICK dialog window

- In the **File system** drop-down list, select **FAT32 (Default)** option.
- In the **Volume label** field, enter the name `RECOVERY`.



#### Important:

The volume label name `RECOVERY` is mandatory. Do not use any other name, otherwise the procedure will fail.

- Under **Format options**, check **Quick Format** option.
- Click **Start** button.
- Acknowledge the warning message with **OK**.
- After formatting is finished, the USB stick is labelled in the Windows Explorer by its new name "RECOVERY".

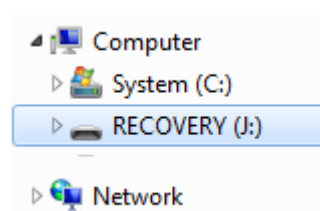


Figure 98: Formatted USB stick

### 3. Copy recovery files onto the USB stick.

- Open the unpacked `recovery` archive folder and copy the `boot` and `efi` folders and the `firmware` and `VERSION` files onto the USB stick.
- The USB stick with the copied firmware image must now feature the following elements:

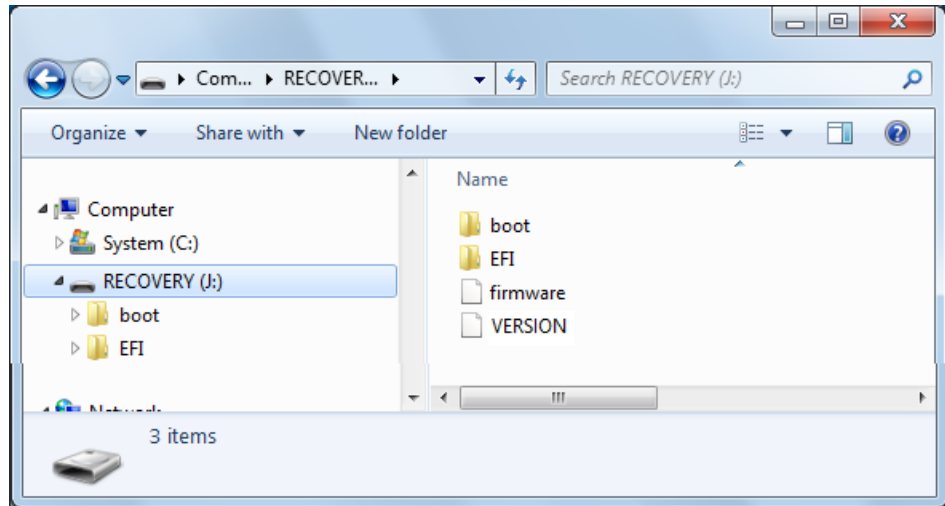


Figure 99: Prepared USB stick


- Remove the USB stick from your Windows PC.



#### Important:

Please note that the firmware recovery procedure clears all contents on the main storage memory of the device. All existing projects and configuration files in the device will thus be deleted.

### 4. Prepare netFIELD OnPremise device

- Make sure that the device is switched off (the green Status LED below  indicating power must be dark).
- Connect the USB keyboard with one of the USB sockets of the device (for the positions of the USB sockets, see section *Positions of the interfaces* [▶ page 16]).
- Connect the monitor with the DVI-I socket (see position (3) in section *Positions of the interfaces* [▶ page 16]) or with the DP socket (see Position (4)) [according to your monitor type].



#### Important:

Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.

- Plug the prepared USB stick into one of the USB sockets of the device (for the positions of the USB sockets, see section *Positions of the interfaces* [▶ page 16]).

5. Configure USB Device as boot drive in BIOS setup.

- Turn-on the device by pressing the power button (see position (12) in section *Positions of the interfaces* [▶ page 16]).
- After a few seconds, the device beeps and the BIOS start screen appears on the monitor:



Figure 100: BIOS start screen

- To open the BIOS setup menu, press **Del** on your keyboard immediately.



**Note:**

If you have missed the time slot for opening the BIOS setup menu, the device boots in its usual mode. In this case, turn the device off and on again, then try once more to open the BIOS setup menu by pressing the **Del** key.

- The BIOS setup menu opens:

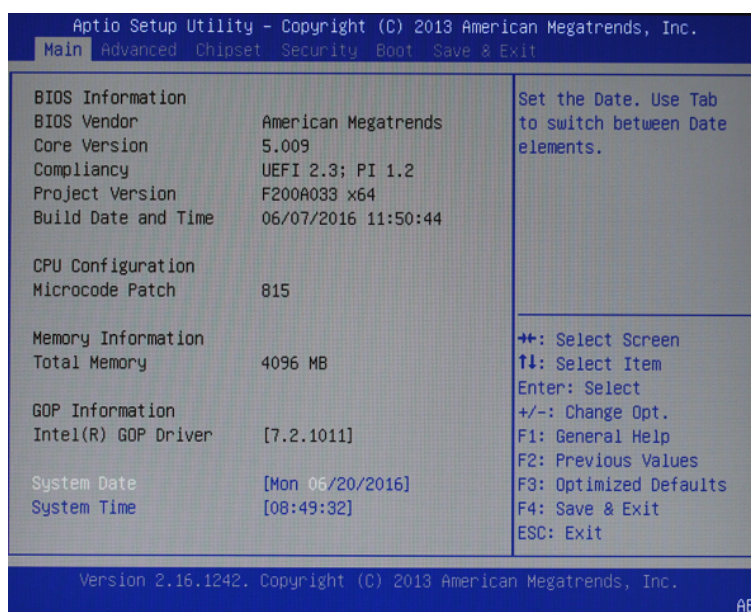


Figure 101: BIOS setup menu



- In the main menu, use the right arrow key to navigate and open the **Boot** tab:

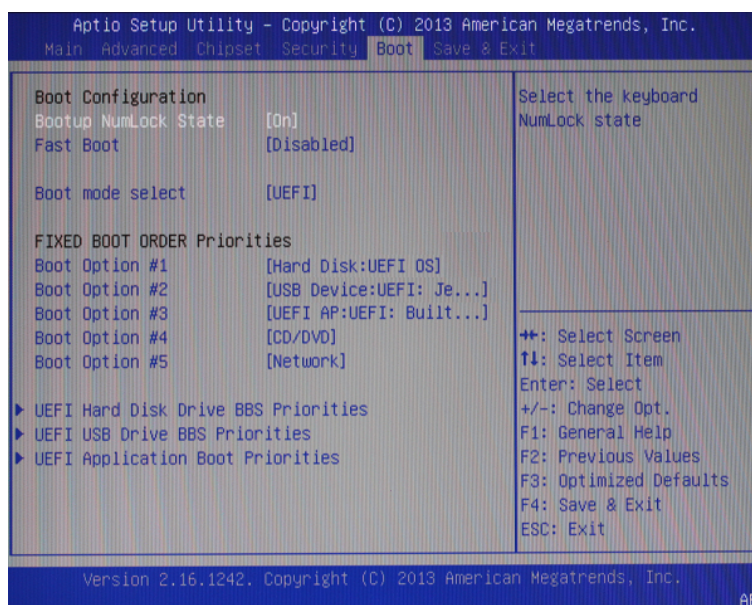


Figure 102: Boot options tab in BIOS setup menu

- Use the downwards arrow key to navigate to the **FIXED BOOT ORDER Priorities** area and select **Boot Option #1**.

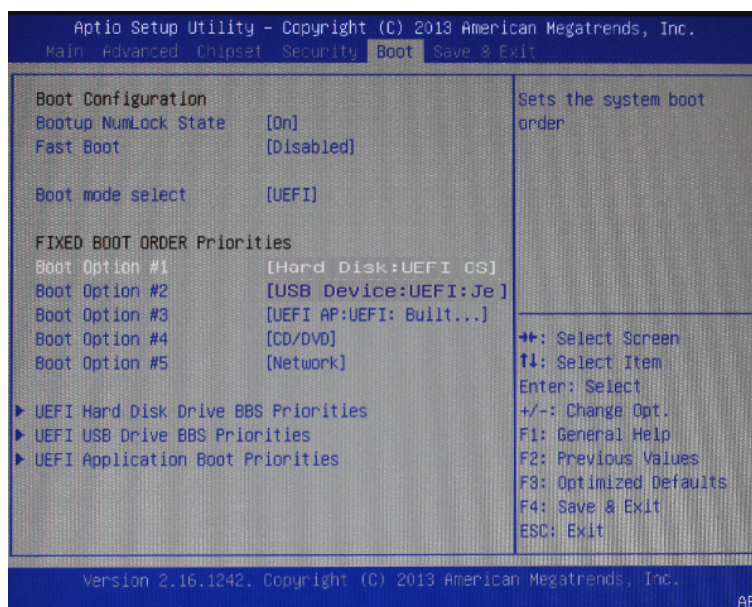


Figure 103: Boot option #1 in BIOS setup menu

- Press **Enter** key to open the **Boot Option #1** list.



- Use the downwards arrow key to select **USB Device:UEFI: [Name of your USB stick]**:

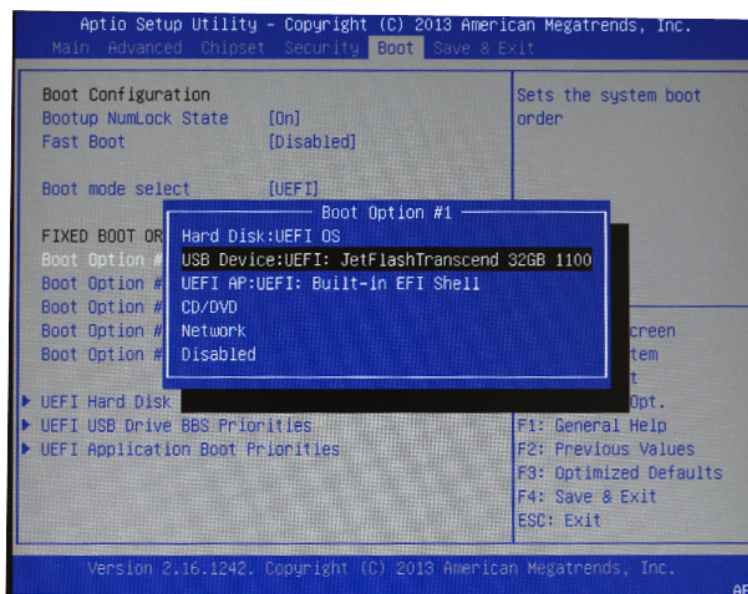


Figure 104: List for boot option #1

- Press **Enter** key to take over this option.
- Use the upwards arrow key to navigate to the main menu, then use the right arrow key to open the **Save & Exit** tab.

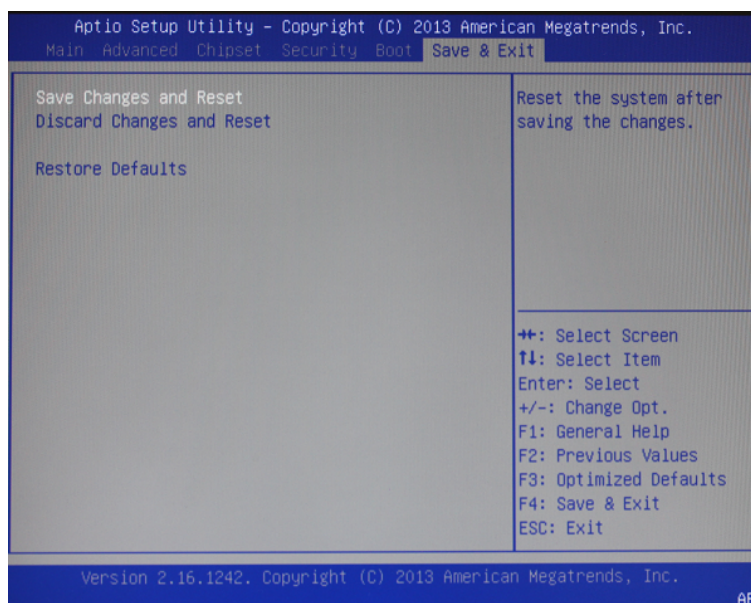


Figure 105: Save & Exit tab

- In the **Save & Exit** tab, select **Save Changes and Reset** option, then press **Enter** key.

## 6. Restart booting (reset).

- In the **Save & reset** security window, select **Yes**, then press **Enter** key.

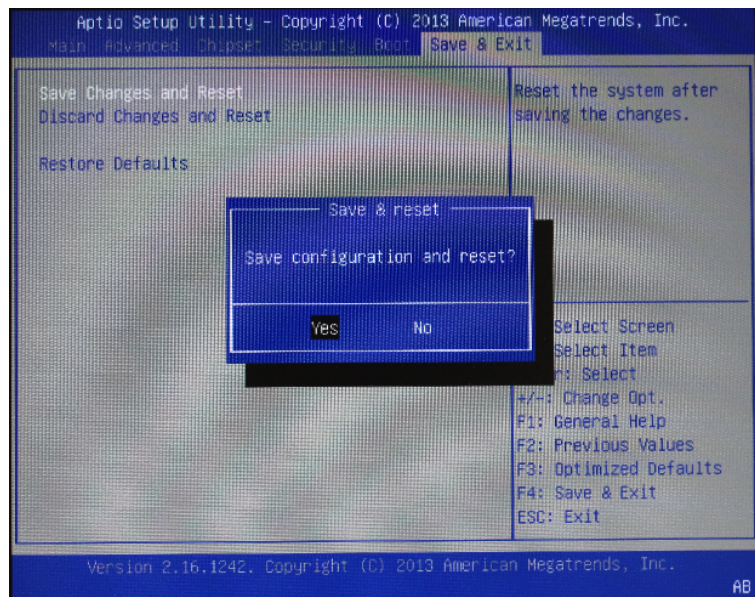


Figure 106: Save &amp; Reset security question

- The device restarts and boots from the connected USB stick. The following boot option question appears:

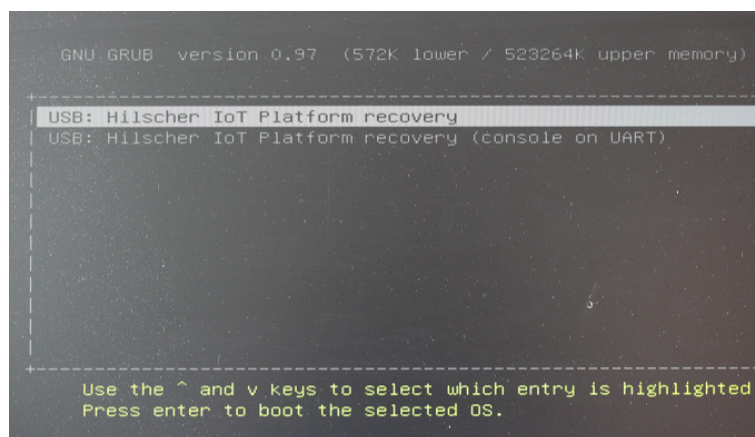


Figure 107: Boot options question

- Ignore the question, respectively leave the option at **USB: Hilscher IoT Platform recovery**.

- ⇒ The device updates its firmware. This is indicated by a progress bar at the bottom of the monitor screen:

```

Updating the X509 certificate ... Can't update variable in their mode without a key
Updating the PK certificate ... Can't update variable in their mode without a key
Updating the PK certificate ... Cannot write to PK, wrong file system permissions
[ 1.426781] tsc: refined tsc clocksource calibration: 1999.799 MHz
[ 1.427453] clocksource tsc: mask: 0xffffffffffffff max_cycles: 0x2b05d4f227, max_idle_ns: 881590665980 ns
[ 1.698136] random: uchange: urandom read with 6 bits of entropy available
[ 1.705966] usb 1-1.2: new high-speed USB device number 3 using ehci-pci
[ 2.001066] iscsi volume(s) is volume group "rootfs" now active
[ 1.947181] hub 1-1.2.1.0: 4 ports detected
[ 1.929154] usb 1-1.4: new full-speed USB device number 4 using ehci-pci
[ 2.136941] usb 1-1.2.1: new high-speed USB device number 5 using ehci-pci
[ 2.221955] usb-storage 1-1.2.1.1.0: USB Mass Storage device detected
[ 2.226294] scsi host2: usb-storage 1-1.2.1.1.0
[ 2.232453] usb 1-1.2.2: new low-speed USB device number 6 using ehci-pci
[ 2.363780] input: DELL Dell USB Entry Keyboard as /devices/pci0000:00/0000:00:14.0/usb1/1-1/1-1.2/1-1.2.2/1-1.2.2.1/6-0003:413C:2167.0001/input/input7
[ 2.476293] hid-generic 0003:413C:2167.0001: input: USB HID v1.11 Keyboard [DELL Dell USB Entry Keyboard] on usb-0000:00:14.0-1.2.2/input6
[ 2.489463] Switched to clocksource tsc
[ 3.486534] sd 2:0:0:0: Direct Access JetFlash Transcend 32GB 1190 PQ: 0 ANSI: 6
[ 3.613221] sd 2:0:0:0: Attached SCSI generic sgl type 9
[ 3.612755] sd 2:0:0:0: (sdb) 61702144 512-byte logical blocks: CH 6 GB/29.4 GiB
[ 3.615177] sd 2:0:0:0: (sdb) Write Protect: is off
[ 3.615171] sd 2:0:0:0: (sdb) Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[ 3.621401] sdb: sdb
[ 3.687465] sd 2:0:0:0: (sdb) Attached SCSI removable disk
Searching for initrd.spl at /dev/sdb1 ... not found
Searching for firmware at /dev/sdb1 ... found (media/sdb1/firmware)
[ 4.251492] random: smunlocking pool is initialized
Verifying the signature ... done
Extracting the archive ... done
Cleaning up ... done
Processing script 1.sh ...
=====
#
# Firmware update
#
=====
Searching update device ... done (/dev/sda)
Checking the BIOS name ... done
Replaying firmware/Allwinner-jetex-image-mling1z1and-64-20160617110302_rootfs.tar.bz2 to /dev/sda ...
Application: deploy.sh (20160511)
=====
Creating a bootable device /dev/sda
- Checking the target device /dev/sda ... done
- Clearing partition table at /dev/sda ... done
- Creating partition table at /dev/sda for target ... 0 logical volume(s) is volume group "rootfs" now active
[ 21.236538] sda: sda1 sda2
- Formatting /dev/sda1 (vfat) ... done
- Preparing physical device "/dev/sda2" for LHM usage ... done
- Creating logical volume "SYSTEM" with size 5368 ... done
- Creating Backup-Partition "BACKUP" ... done
- Formatting /dev/mapper/rootfs-BACKUP (ext4) ... done
- Formatting /dev/mapper/rootfs-SYSTEM (ext4) ... done
- Mounting /dev/sda1 ... done
- Mounting /dev/mapper/rootfs-SYSTEM ... [ 22.404051] EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts: (null)
done
Replaying firmware/Allwinner-jetex-image-mling1z1and-64-20160617110302_rootfs.tar.bz2 to /dev/mapper/rootfs-SYSTEM ...
[201610 0:01:42 (2.59118s)] [=====] 100%
done

```

Figure 108: Firmware update in progress

- ⇒ After the recovery procedure is finished, the device automatically switches itself off.
- Wait until the device has switched itself off, then **remove the USB stick** from the device.



#### Note:

If you don't remove the USB stick, the firmware will be updated again after re-powering the device.

- ⇒ You have finished the firmware recovery procedure and the device has recovered its "factory settings".

## 7.2 Useful CLI commands and parameters in Terminal

### 7.2.1 Network Manager

```
sudo nmcli ...
```

### 7.2.2 Show interface status

```
sudo nmcli dev status
```

### 7.2.3 Activate interface

(Re)activate interface, e.g. eth0:

```
sudo nmcli con up ifname eth0
```

### 7.2.4 Docker Compose support for Standard Docker environment

```
docker-compose <commands>
```

#### Examples

Show the version of Docker Compose:

```
docker-compose version
```

Start container(s) via Docker Compose file:

```
docker-compose -file <docker compose file.yml> up -d
```

Stop container(s) via Docker Compose file:

```
docker-compose -file <docker compose file.yml> down
```

### 7.2.5 Manage Standard Docker

```
docker <docker commands>
```

#### Examples

List all created containers of the Standard Docker instance:

```
docker ps
```

List all bridges of the Standard Docker instance:

```
docker network ls
```

### 7.2.6 Manage IoT Edge Docker

```
docker-iotedge <docker commands>
```

#### Example

To list all created containers for the IoT Edge Docker instance:

```
docker-iotedge ps -a
```



## 7.2.7 Enable/disable SSH Daemon (release port 22)

Disable autostart:

```
sudo systemctl disable sshd.socket
```

Stop SSH Daemon:

```
sudo systemctl stop sshd.socket
```

## 7.2.8 External storage support using iSCSI

Enable iSCSI service:

```
sudo systemctl enable iscsi-initiator
```

Start iSCSI service:

```
sudo systemctl start iscsi-initiator
```

Target discovery and connection administration:

```
sudo iscsiadm <parameter>
```

Configuration files:

```
initiatorname.iscsi  
iscsid.conf
```

## 7.2.9 Follow the system log via terminal CLI

```
sudo journalctl -f
```

## 8 Technical data

Category	Parameter/item	Value/description
Product	Part number	1321.300/NFLD
	Product name	NIOT-E-TIJCX-GB-RE/NFLD
	Application	IT/OT Edge device for data-intensive and complex IoT applications with demand on maximum performance, connectivity and memory size.
Functions	IoT Edge Docker	Docker for remote and automatic deployment and maintenance of containers
	Standard Docker	Docker for manual and local deployment and maintenance of containers
	Local Device Manager	Web-based GUI for local device parameterization
Security	Boot	Bootimg of signed software
	Access	HTTPS, TLS
Processors	CPU	2 GHz Celeron®, Intel® J1900
	Communication controller	netX 100
Software	Operating system	netFIELD OS based on Security Enhanced Linux
Memory	RAM	8 GB DDR3 RAM
	Hard drive	128 GB solid state disk drive: 64 GB application 64 GB backup
Power	Voltage	24 V DC $\pm$ 4.8 V DC
	Current (at 24 V DC)	Without USB: 420 mA (typical) With USB: max. 2.5 A
	Power of the used power supply unit	60 W
	Connector	3-pin terminal block
IT interface	Interface type	2 x 10/100/1000 Mbit, Intel® I210AT
	LAN connector	2 x RJ45 socket
OT interface	Interface type	10BASE-T/100BASE-TX, potential free, Hilscher netX 100
	Connector	2 x RJ45 socket
	Supported protocols	PROFINET IO Device, EtherNet/IP Adapter, Standard TCP/IP (limited throughput). In listening ("passive") mode: PROFINET, EtherCAT, Ethernet
Additional interfaces	USB	3 x USB 2.0 (500 mA) 1 x USB 3.0 (900 mA) All USB max. 2 A
	Wi-Fi	Single band 2.4 GHz IEEE 802.11n, 2 x flexible antenna connection
	Serial interface	2 x RS-232/422/485 (can be configured)
	Display connectors	DVI-I and DP (DisplayPort) <b>Note:</b> Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.
Display	LED indicators	12 LEDs
Real-time clock	Buffering	Yes, battery (service interval 10 years)
Environment	Ambient temperature range for operation	0°C ... +50°C
	Ambient temperature range for storage	-20°C ... +80°C
	Humidity range	10 % ... 93 % relative humidity (non-condensing)

Category	Parameter/item	Value/description
Device	Dimensions	214 mm (H) x 85 mm (W) x 157 mm (D)
	Weight	2.3 kg
	Housing	Metal
	Mounting	Screws
Conformity	RoHS	Yes
Conformance with EMC directives	CE sign	Yes
Shock and vibration resistance	Shock resistance	50 G, half sine, 11 ms, IEC 60068-2-27
	Vibration resistance	Random: 2 Grms @ 5~500 Hz, IEC 60068-2-64 Sinusoidal: 2 Grms @ 5~500 Hz, IEC 60068-2-64

Table 32: Technical data netFIELD OnPremise (NIOT-E-TIJCX-GB-RE/NFLD)

## 9 Decommissioning, dismounting and disposal

### 9.1 Putting the device out of operation

---

**NOTICE****Danger of Unsafe System Operation!**

To prevent personal injury or property damage, make sure that the removal of the device from your plant during operation will not affect the safe operation of the plant.

- Disconnect all communication cables from the device.
  - Disconnect the power supply plug.
  - Remove the device from the cabinet.
- 

### 9.2 Disposal and recycling

#### 9.2.1 Disposal of battery

This product contains a battery:

KTS CR2032W Lithium coin cell battery (or equivalent).

The battery requires special handling when it is replaced or when the device is disposed of after having reached its end-of-use.



---

**Waste electronic equipment**

This battery must not be disposed of with household waste.

Dispose of this battery in accordance with local regulations in your country.

---

When disposing of the battery, observe the following:

- Observe the national and local regulations for the disposal of batteries.
- Dispose of this product in an environmentally friendly manner at a local collection point for batteries.

Alternatively, you can return our products to us for disposal. The prerequisite is that no additional foreign substances are contained. Before returning, please contact us via the Return Merchandise Authorization (RMA) form on [www.hilscher.com](http://www.hilscher.com).

In Europe, the directive 2006/66/EG batteries and accumulators and waste batteries and accumulators applies. Different policies and laws may apply nationally.



## 9.2.2 Removal of battery

If you do not want to return the device to Hilscher, you have to remove the battery and dispose of it properly prior to the disposal of the device.

To remove the battery, proceed as follows:

- Open the housing of the device by unscrewing the fastening screws.
- Remove the battery from the device. The mounting position of the battery is marked in the following photo of the opened device by the yellow rectangle:

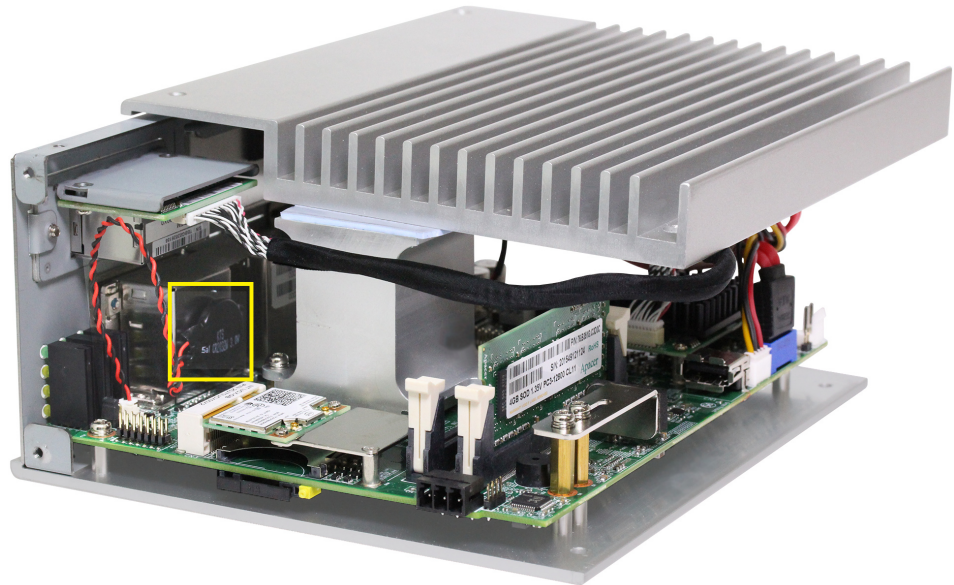


Figure 109: NIOT-E-TIJCX-GB-RE/NFLD battery

## 9.2.3 Disposal of device

Waste electronic equipment must be disposed of properly after the end of use.



### Waste electronic equipment

This product must not be disposed of with household waste.

Dispose of this product in accordance with local regulations in your country.

When disposing of the product, observe the following:

- Observe national and local regulations for the disposal of waste electronic equipment, batteries and packaging.
- Delete personal data stored in the waste electronic device.
- Remove the battery from the waste electronic device and dispose it separately.
- Dispose of this product in an environmentally friendly manner at a local collection point for waste electronic equipment.
- Dispose of packaging in such a way that a high level of recycling is possible.

Alternatively, you can return our products to us for disposal. The prerequisite is that no additional foreign substances are contained. Before returning, please contact us via the Return Merchandise Authorization (RMA) form on [www.hilscher.com](http://www.hilscher.com).

In Europe, the directive 2012/19/EU waste electrical and electronic equipment applies. Different policies and laws may apply nationally.

## 10 Legal notes

### Terms and conditions

Please read the terms and conditions under  
<https://www.netfield.io/termsOfUse>.

### netFIELD OS

netFIELD OS is a YOCTO project based Linux operating system released and licensed by Hilscher.

netFIELD OS is released under the

[HILSCHER netFIELD Source Code/Software LICENSE AGREEMENT](#).

netFIELD OS may include 3rd party software or software declared as Open Source. The licensing information of all included software components are provided in textual form in the netFIELD OS under the folder `/usr/share/common-licenses` and subfolders.

Open Source software is released under Open Source License usually.

The official verbatim texts can be read and checked under

<https://opensource.org/licenses>.

### Copyright

© Hilscher Gesellschaft für Systemautomation mbH

All rights reserved.

The images, photographs and texts in the accompanying materials (in the form of a user's manual, operator's manual, Statement of Work document and all other document types, support texts, documentation, etc.) are protected by German and international copyright and by international trade and protective provisions. Without the prior written consent, you do not have permission to duplicate them either in full or in part using technical or mechanical methods (print, photocopy or any other method), to edit them using electronic systems or to transfer them. You are not permitted to make changes to copyright notices, markings, trademarks or ownership declarations. Illustrations are provided without taking the patent situation into account. Any company names and product designations provided in this document may be brands or trademarks by the corresponding owner and may be protected under trademark, brand or patent law. Any form of further use shall require the express consent from the relevant owner of the rights.

**Important notes**

Utmost care was/is given in the preparation of the documentation at hand consisting of a user's manual, operating manual and any other document type and accompanying texts. However, errors cannot be ruled out.

Therefore, we cannot assume any guarantee or legal responsibility for erroneous information or liability of any kind. You are hereby made aware that descriptions found in the user's manual, the accompanying texts and the documentation neither represent a guarantee nor any indication on proper use as stipulated in the agreement or a promised attribute. It cannot be ruled out that the user's manual, the accompanying texts and the documentation do not completely match the described attributes, standards or any other data for the delivered product. A warranty or guarantee with respect to the correctness or accuracy of the information is not assumed.

We reserve the right to modify our products and the specifications for such as well as the corresponding documentation in the form of a user's manual, operating manual and/or any other document types and accompanying texts at any time and without notice without being required to notify of said modification. Changes shall be taken into account in future manuals and do not represent an obligation of any kind, in particular there shall be no right to have delivered documents revised. The manual delivered with the product shall apply.

Under no circumstances shall Hilscher Gesellschaft für Systemautomation mbH be liable for direct, indirect, ancillary or subsequent damage, or for any loss of income, which may arise after use of the information contained herein.

**Liability disclaimer**

The hardware and/or software was created and tested by Hilscher Gesellschaft für Systemautomation mbH with utmost care and is made available as is. No warranty can be assumed for the performance or flawlessness of the hardware and/or software under all application conditions and scenarios and the work results achieved by the user when using the hardware and/or software. Liability for any damage that may have occurred as a result of using the hardware and/or software or the corresponding documents shall be limited to an event involving willful intent or a grossly negligent violation of a fundamental contractual obligation. However, the right to assert damages due to a violation of a fundamental contractual obligation shall be limited to contract-typical foreseeable damage.

It is hereby expressly agreed upon in particular that any use or utilization of the hardware and/or software in connection with

- Flight control systems in aviation and aerospace;
- Nuclear fission processes in nuclear power plants;
- Medical devices used for life support and
- Vehicle control systems used in passenger transport

shall be excluded. Use of the hardware and/or software in any of the following areas is strictly prohibited:

- For military purposes or in weaponry;
- For designing, engineering, maintaining or operating nuclear systems;
- In flight safety systems, aviation and flight telecommunications systems;
- In life-support systems;
- In systems in which any malfunction in the hardware and/or software may result in physical injuries or fatalities.

You are hereby made aware that the hardware and/or software was not created for use in hazardous environments, which require fail-safe control mechanisms. Use of the hardware and/or software in this kind of environment shall be at your own risk; any liability for damage or loss due to impermissible use shall be excluded.

## Warranty

Hilscher Gesellschaft für Systemautomation mbH hereby guarantees that the software shall run without errors in accordance with the requirements listed in the specifications and that there were no defects on the date of acceptance. The warranty period shall be 12 months commencing as of the date of acceptance or purchase (with express declaration or implied, by customer's conclusive behavior, e.g. putting into operation permanently).

The warranty obligation for equipment (hardware) we produce is 36 months, calculated as of the date of delivery ex works. The aforementioned provisions shall not apply if longer warranty periods are mandatory by law pursuant to Section 438 (1.2) BGB, Section 479 (1) BGB and Section 634a (1) BGB [Bürgerliches Gesetzbuch; German Civil Code] If, despite of all due care taken, the delivered product should have a defect, which already existed at the time of the transfer of risk, it shall be at our discretion to either repair the product or to deliver a replacement product, subject to timely notification of defect.

The warranty obligation shall not apply if the notification of defect is not asserted promptly, if the purchaser or third party has tampered with the products, if the defect is the result of natural wear, was caused by unfavorable operating conditions or is due to violations against our operating regulations or against rules of good electrical engineering practice, or if our request to return the defective object is not promptly complied with.

## Costs of support, maintenance, customization and product care

Please be advised that any subsequent improvement shall only be free of charge if a defect is found. Any form of technical support, maintenance and customization is not a warranty service, but instead shall be charged extra.

## Additional guarantees

Although the hardware and software was developed and tested in-depth with greatest care, Hilscher Gesellschaft für Systemautomation mbH shall not assume any guarantee for the suitability thereof for any purpose that was not confirmed in writing. No guarantee can be granted whereby the hardware and software satisfies your requirements, or the use of the hardware and/or software is uninterrupted or the hardware and/or software is fault-free.

It cannot be guaranteed that patents and/or ownership privileges have not been infringed upon or violated or that the products are free from third-party influence. No additional guarantees or promises shall be made as to whether the product is market current, free from deficiency in title, or can be integrated or is usable for specific purposes, unless such guarantees or promises are required under existing law and cannot be restricted.

## **Confidentiality**

The customer hereby expressly acknowledges that this document contains trade secrets, information protected by copyright and other patent and ownership privileges as well as any related rights of Hilscher Gesellschaft für Systemautomation mbH. The customer agrees to treat as confidential all of the information made available to customer by Hilscher Gesellschaft für Systemautomation mbH and rights, which were disclosed by Hilscher Gesellschaft für Systemautomation mbH and that were made accessible as well as the terms and conditions of this agreement itself.

The parties hereby agree to one another that the information that each party receives from the other party respectively is and shall remain the intellectual property of said other party, unless provided for otherwise in a contractual agreement.

The customer must not allow any third party to become knowledgeable of this expertise and shall only provide knowledge thereof to authorized users as appropriate and necessary. Companies associated with the customer shall not be deemed third parties. The customer must obligate authorized users to confidentiality. The customer should only use the confidential information in connection with the performances specified in this agreement.

The customer must not use this confidential information to his own advantage or for his own purposes or rather to the advantage or for the purpose of a third party, nor must it be used for commercial purposes and this confidential information must only be used to the extent provided for in this agreement or otherwise to the extent as expressly authorized by the disclosing party in written form. The customer has the right, subject to the obligation to confidentiality, to disclose the terms and conditions of this agreement directly to his legal and financial consultants as would be required for the customer's normal business operation.

## **Export provisions**

The delivered product (including technical data) is subject to the legal export and/or import laws as well as any associated regulations of various countries, especially such laws applicable in Germany and in the United States. The products / hardware / software must not be exported into such countries for which export is prohibited under US American export control laws and its supplementary provisions. You hereby agree to strictly follow the regulations and to yourself be responsible for observing them. You are hereby made aware that you may be required to obtain governmental approval to export, reexport or import the product.



## List of figures

Figure 1:	netFIELD OS architecture .....	10
Figure 2:	netFIELD OS container management .....	11
Figure 3:	netFIELD OS inter-container communication .....	12
Figure 4:	netFIELD OnPremise SW architecture .....	14
Figure 5:	Front and top view .....	16
Figure 6:	Device dimensions .....	18
Figure 7:	LED positions on device .....	23
Figure 8:	LED sticker .....	28
Figure 9:	Mounting holes .....	29
Figure 10:	Factory IP address settings of LAN interfaces .....	31
Figure 11:	Host name on device label (example) .....	34
Figure 12:	Setting IP address under Windows for direct LAN connection .....	35
Figure 13:	Login Device Manager .....	36
Figure 14:	Enter current password dialog .....	37
Figure 15:	Enter new password dialog .....	37
Figure 16:	Re-Authentication dialog .....	38
Figure 17:	System time value .....	39
Figure 18:	Change System Time dialog .....	39
Figure 19:	“Basic” onboarding screen in Local Device Manager .....	43
Figure 20:	Research Hardware ID .....	46
Figure 21:	Add device mask in netFIELD Portal .....	47
Figure 22:	Activation Code in portal .....	48
Figure 23:	Advanced Onboarding tab in device .....	49
Figure 24:	Copy key to clipboard .....	51
Figure 25:	Overview Local Device Manager .....	52
Figure 26:	System page in Local Device Manager .....	54
Figure 27:	Change host name dialog .....	55
Figure 28:	Networking page .....	57
Figure 29:	Details of LAN interface (eth0) .....	59
Figure 30:	IPv4 Settings .....	60
Figure 31:	Manual IPv4 Settings .....	60
Figure 32:	Open Firewall configuration page .....	63
Figure 33:	Elements on Firewall configuration page .....	64
Figure 34:	Add Zone dialog .....	65
Figure 35:	Add services .....	69
Figure 36:	Add custom services dialog .....	70
Figure 37:	Add forward port dialog .....	71
Figure 38:	Network Proxy configuration .....	72
Figure 39:	Proxy Settings dialog window .....	73
Figure 40:	Using one Proxy server for all protocols .....	74



Figure 41:	Separate HTTP/HTTPS/FTP configuration .....	75
Figure 42:	Restart dialog after changing proxy server configuration .....	76
Figure 43:	Synchronize proxy settings with netFIELD Portal.....	77
Figure 44:	Wi-Fi Client Mode .....	78
Figure 45:	Client mode parameters .....	80
Figure 46:	Connect Network dialog .....	82
Figure 47:	Connect network message .....	84
Figure 48:	Access Point Mode .....	86
Figure 49:	Warning note .....	87
Figure 50:	Configure Interface message .....	88
Figure 51:	wlan0 configuration page.....	88
Figure 52:	Set manual address in IPv4 Settings dialog .....	89
Figure 53:	Enter Manual IP Address.....	89
Figure 54:	Configured DHCP service .....	90
Figure 55:	DHCP Server Configuration dialog.....	92
Figure 56:	OT interface tab .....	94
Figure 57:	Connectivity Check tab .....	96
Figure 58:	Basic Onboarding page .....	98
Figure 59:	Offboarding “Basic” .....	99
Figure 60:	Offboarding “Advanced” .....	100
Figure 61:	Web Server Settings tab.....	101
Figure 62:	Default MQTT Settings .....	102
Figure 63:	Docker Network Settings .....	104
Figure 64:	Default docker network configuration .....	107
Figure 65:	Remote Access tab .....	109
Figure 66:	Login tab .....	110
Figure 67:	Notification on Sign In dialog .....	110
Figure 68:	Standard Docker.....	111
Figure 69:	Expand concise container details .....	112
Figure 70:	Container parameters with terminal window.....	113
Figure 71:	Image Search dialog of Standard Docker.....	113
Figure 72:	Run Image dialog .....	114
Figure 73:	Expand image details .....	115
Figure 74:	Image details .....	116
Figure 75:	IOT Edge Docker .....	117
Figure 76:	Container details expanded.....	119
Figure 77:	Container parameters .....	120
Figure 78:	IoT image expanded.....	121
Figure 79:	Details of netFIELD Proxy image .....	122
Figure 80:	Accounts.....	123
Figure 81:	Create new account.....	124

Figure 82:	Edit account.....	124
Figure 83:	Web Server Certificate page .....	127
Figure 84:	Terminal.....	128
Figure 85:	OS update page .....	130
Figure 86:	Selected OS update image.....	131
Figure 87:	Upload finished message .....	132
Figure 88:	OS update “Disconnected” message.....	132
Figure 89:	Backup and Restore tab .....	134
Figure 90:	Factory Reset .....	137
Figure 91:	Logs.....	138
Figure 92:	Services page .....	139
Figure 93:	Service details and settings page.....	140
Figure 94:	Service types: Timers .....	141
Figure 95:	Create timer dialog .....	141
Figure 96:	Formatting USB stick .....	144
Figure 97:	Format USB STICK dialog window.....	145
Figure 98:	Formatted USB stick.....	145
Figure 99:	Prepared USB stick .....	146
Figure 100:	BIOS start screen .....	147
Figure 101:	BIOS setup menu .....	147
Figure 102:	Boot options tab in BIOS setup menu .....	148
Figure 103:	Boot option #1 in BIOS setup menu .....	148
Figure 104:	List for boot option #1 .....	149
Figure 105:	Save & Exit tab .....	149
Figure 106:	Save & Reset security question.....	150
Figure 107:	Boot options question .....	150
Figure 108:	Firmware update in progress.....	151
Figure 109:	NIOT-E-TIJCX-GB-RE/NFLD battery .....	157

## List of tables

Table 1:	List of revisions .....	5
Table 2:	Terms and abbreviations .....	8
Table 3:	Positions of the interfaces.....	17
Table 4:	Power supply connector .....	19
Table 5:	Parameters of the serial interface .....	20
Table 6:	RS-232 D-Sub .....	21
Table 7:	RS-422 D-Sub .....	21
Table 8:	RS-485 D-Sub .....	22
Table 9:	Description of device status LEDs .....	24
Table 10:	LEDs LAN interface .....	25
Table 11:	Tasks for commissioning the device (netFIELD Portal user).....	26
Table 12:	Tasks for commissioning the device (Standard Docker user) .....	27
Table 13:	Available Firewall zones .....	65
Table 14:	Elements in Add Zone dialog .....	66
Table 15:	Columns/elements in Allowed Services table .....	68
Table 16:	Columns/elements in Forward Ports table .....	70
Table 17:	Control elements in main toolbar .....	71
Table 18:	Wi-Fi operating modes.....	79
Table 19:	Currently Connected Network.....	81
Table 20:	Visible Networks .....	81
Table 21:	Parameters in Connect Network dialog (1).....	82
Table 22:	Parameters in Connect Network dialog (2).....	83
Table 23:	Connection Profiles.....	85
Table 24:	Connected WiFi Devices .....	86
Table 25:	Access Point Settings .....	87
Table 26:	Elements/Parameters on DHCP Server page .....	90
Table 27:	Parameters of DHCP Server Configuration dialog .....	92
Table 28:	Default MQTT Client Settings .....	103
Table 29:	Standard Docker Network Settings .....	105
Table 30:	IoT Edge Docker Network Settings .....	106
Table 31:	Elements in Backup & Restore tab .....	135
Table 32:	Technical data netFIELD OnPremise (NIOT-E-TIJCX-GB-RE/NFLD) .....	154

# Contacts

## HEADQUARTER

### Germany

Hilscher Gesellschaft für  
Systemautomation mbH  
Rheinstraße 15  
65795 Hattersheim  
Phone: +49 (0) 6190 9907-0  
Fax: +49 (0) 6190 9907-50  
E-mail: [info@hilscher.com](mailto:info@hilscher.com)

### Support

Phone: +49 (0) 6190 9907-990  
E-mail: [hotline@hilscher.com](mailto:hotline@hilscher.com)

## SUBSIDIARIES

### China

Hilscher Systemautomation (Shanghai) Co. Ltd.  
200010 Shanghai  
Phone: +86 (0) 21-6355-5161  
E-mail: [info@hilscher.cn](mailto:info@hilscher.cn)

### Support

Phone: +86 (0) 21-6355-5161  
E-mail: [cn.support@hilscher.com](mailto:cn.support@hilscher.com)

### France

Hilscher France S.a.r.l.  
69800 Saint Priest  
Phone: +33 (0) 4 72 37 98 40  
E-mail: [info@hilscher.fr](mailto:info@hilscher.fr)

### Support

Phone: +33 (0) 4 72 37 98 40  
E-mail: [fr.support@hilscher.com](mailto:fr.support@hilscher.com)

### India

Hilscher India Pvt. Ltd.  
Pune, Delhi, Mumbai, Bangalore  
Phone: +91 8888 750 777  
E-mail: [info@hilscher.in](mailto:info@hilscher.in)

### Support

Phone: +91 020-24243777  
E-mail: [info@hilscher.in](mailto:info@hilscher.in)

### Italy

Hilscher Italia S.r.l.  
20090 Vimodrone (MI)  
Phone: +39 02 25007068  
E-mail: [info@hilscher.it](mailto:info@hilscher.it)

### Support

Phone: +39 02 25007068  
E-mail: [it.support@hilscher.com](mailto:it.support@hilscher.com)

### Japan

Hilscher Japan KK  
Tokyo, 160-0022  
Phone: +81 (0) 3-5362-0521  
E-mail: [info@hilscher.jp](mailto:info@hilscher.jp)

### Support

Phone: +81 (0) 3-5362-0521  
E-mail: [jp.support@hilscher.com](mailto:jp.support@hilscher.com)

### Republic of Korea

Hilscher Korea Inc.  
13494, Seongnam, Gyeonggi  
Phone: +82 (0) 31-739-8361  
E-mail: [info@hilscher.kr](mailto:info@hilscher.kr)

### Support

Phone: +82 (0) 31-739-8363  
E-mail: [kr.support@hilscher.com](mailto:kr.support@hilscher.com)

### Austria

Hilscher Austria GmbH  
4020 Linz  
Phone: +43 732 931 675-0  
E-mail: [sales.at@hilscher.com](mailto:sales.at@hilscher.com)

### Support

Phone: +43 732 931 675-0  
E-mail: [at.support@hilscher.com](mailto:at.support@hilscher.com)

### Switzerland

Hilscher Swiss GmbH  
4500 Solothurn  
Phone: +41 (0) 32 623 6633  
E-mail: [info@hilscher.ch](mailto:info@hilscher.ch)

### Support

Phone: +41 (0) 32 623 6633  
E-mail: [support.swiss@hilscher.com](mailto:support.swiss@hilscher.com)

### USA

Hilscher North America, Inc.  
Lisle, IL 60532  
Phone: +1 630-505-5301  
E-mail: [info@hilscher.us](mailto:info@hilscher.us)

### Support

Phone: +1 630-505-5301  
E-mail: [us.support@hilscher.com](mailto:us.support@hilscher.com)