



## User manual netFIELD Connect



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

DOC191101UM04EN | Revision 4 | English | 2021-06 | 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.....	6
1.2	Terms and abbreviations.....	7
<b>2</b>	<b>Brief description .....</b>	<b>8</b>
2.1	Intended use .....	8
2.2	Key features .....	8
2.3	netFIELD OS: Industrial IoT Operating System .....	9
2.4	Depiction of netFIELD Connect SW architecture .....	12
<b>3</b>	<b>Safety .....</b>	<b>13</b>
3.1	General note .....	13
3.2	Personnel qualification .....	13
3.3	Device destruction by exceeding the allowed supply voltage .....	13
3.4	Limitation of program/erase cycles of SD card .....	13
<b>4</b>	<b>Hardware description .....</b>	<b>14</b>
4.1	Device drawings.....	14
4.1.1	Positions of the interfaces .....	14
4.1.2	Dimensions .....	15
4.2	Interfaces .....	16
4.2.1	Power supply .....	16
4.2.2	LAN connector .....	16
4.2.3	Real-Time Ethernet connectors .....	16
4.2.4	USB connectors .....	17
4.2.5	Wi-Fi.....	17
4.2.6	HDMI connector .....	17
4.3	LEDs .....	18
4.3.1	Positions of the LEDs on the device .....	18
4.3.2	Device status LEDs.....	19
4.3.3	LEDs of the LAN interface .....	19
4.3.4	LEDs of the Real-Time Ethernet interface .....	20
<b>5</b>	<b>Commissioning and first steps .....</b>	<b>21</b>
5.1	Overview .....	21
5.1.1	netFIELD Portal user .....	21
5.1.2	Standard Docker user .....	22
5.2	Mounting .....	23
5.3	Establish LAN connection and login to Local Device Manager.....	23
5.4	Set system time.....	28
5.5	"Onboard" (register) device in netFIELD Portal .....	30
5.5.1	Overview .....	30
5.5.2	Onboarding using the "Basic" method .....	31
5.5.3	Onboarding using the "Advanced" method .....	33
<b>6</b>	<b>Local Device Manager .....</b>	<b>40</b>

6.1	Overview .....	40
6.2	System .....	42
6.3	Networking .....	45
6.3.1	Overview .....	45
6.3.2	Firewall.....	50
6.3.3	Network Proxy settings .....	59
6.4	Networking Services .....	65
6.4.1	Wi-Fi.....	65
6.4.2	DHCP Server .....	77
6.5	Onboarding (and offboarding) .....	81
6.6	Standard Docker .....	84
6.7	IoT Edge Docker .....	91
6.8	Accounts .....	97
6.9	Certificate .....	100
6.10	General Settings .....	101
6.10.1	Overview .....	101
6.10.2	Web Server (Port) Settings .....	102
6.10.3	Default MQTT Client Settings .....	103
6.10.4	Docker Network Settings .....	105
6.10.5	OT Interface (Using the cifx0 interface or RTE) .....	108
6.10.6	Remote Access .....	110
6.11	Terminal .....	112
6.12	System Update.....	113
6.13	Logs .....	117
<b>7</b>	<b>Good to know.....</b>	<b>118</b>
7.1	Device recovery via USB .....	118
7.2	Useful CLI commands and parameters in Terminal.....	122
7.2.1	Network Manager.....	122
7.2.2	Show interface status.....	122
7.2.3	Activate interface .....	122
7.2.4	Docker Compose Support for Standard Docker environment.....	122
7.2.5	Manage Standard Docker .....	122
7.2.6	Manage IoT Edge Docker .....	122
7.2.7	Enable/disable SSH Daemon (release port 22) .....	122
7.2.8	External storage support using iSCSI .....	123
7.2.9	Follow the system log via terminal CLI .....	123
<b>8</b>	<b>Technical data .....</b>	<b>124</b>
<b>9</b>	<b>Decommissioning, dismounting and disposal .....</b>	<b>126</b>
9.1	Putting the device out of operation.....	126
9.2	Removing device from top hat rail.....	126
9.3	Disposal of waste electronic equipment.....	126
<b>10</b>	<b>Appendix.....</b>	<b>127</b>
10.1	Approvals .....	127
10.1.1	Federal Communications Commission (FCC) .....	127
10.1.2	Industry Canada (IC).....	128
10.2	Legal notes.....	129

**List of figures ..... 133**

**List of tables ..... 136**

**Contacts..... 137**

# 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 Connect** device (NIOT-E-TPI51-EN-RE/NFLD) from Hilscher. Instructions on how to commission the device are also provided in this document.

### 1.1.2 List of revisions

Index	Date	Author	Revision
1	2020-04-17	MKE	Document created.
2	2020-05-11	MKE	Download links for netFIELD OS update/recovery files changed in sections and <i>System Update</i> [▶ page 113] and <i>Device recovery via USB</i> [▶ page 118].
3	2020-12-10	MKE	Document revised and updated to netFIELD OS 2.1: Section <i>Firewall</i> [▶ page 50] added. Section <i>Network Proxy settings</i> [▶ page 59] added. Section <i>Using the cifx0 interface (RTE)</i> added. Section <i>Docker Network Settings</i> [▶ page 105] added. Section <i>How to change the default Docker network configuration</i> removed (replaced by section <i>Docker Network Settings</i> [▶ page 105]).
4	2021-06-29	MKE	Document revised and updated to netFIELD OS 2.2: Section <i>Brief description</i> [▶ page 8] updated. Section <i>LAN connector</i> [▶ page 16] updated. Section <i>LEDs of the Real-Time Ethernet interface</i> [▶ page 20] updated. Section <i>Establish LAN connection and login to Local Device Manager</i> [▶ page 23] updated. Section <i>"Onboard" (register) device in netFIELD Portal</i> [▶ page 30] updated. Section <i>Firewall</i> [▶ page 50] updated. Section <i>Using the cifx0 interface (RTE)</i> removed (substituted by section <i>OT Interface (Using the cifx0 interface or RTE)</i> [▶ page 108]). Section <i>Networking Services</i> [▶ page 65] added. Section <i>Standard Docker</i> [▶ page 84] revised. Section <i>IoT Edge Docker</i> [▶ page 91] revised. Section <i>OT Interface (Using the cifx0 interface or RTE)</i> [▶ page 108] added. Section <i>Remote Access</i> [▶ page 110] added. Section <i>Technical data</i> [▶ page 124] updated.

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
IIoT	Industrial Internet of Things
IT network	Information technology network
OT network	Operational technology network
netFIELD App	netFIELD application container from Hilscher, deployable via netFIELD Platform and running in the IoT Edge Docker of the netFIELD OS
netFIELD OS	Cross-platform capable operating system with connection to the netFIELD Platform
netFIELD Edge	Devices or systems running the netFIELD OS
netFIELD Platform	Internet-hosted platform providing APIs for cloud-to-cloud and cloud-to-edge communication. Basis for the netFIELD Portal
netFIELD Portal	Web-based user interface for the netFIELD Platform services
netFIELD Cloud	netFIELD Platform and netFIELD Portal
netX	Multi-protocol communication controller for OT networks

Table 2: Terms and abbreviations

## 2 Brief description

### 2.1 Intended use

netFIELD Connect is an Edge Device hosting the netFIELD OS for connecting an OT network – like e.g. PROFINET – with an IT network, the netFIELD Platform 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 51 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, as a part of our technology portfolio, 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 Yocto 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.

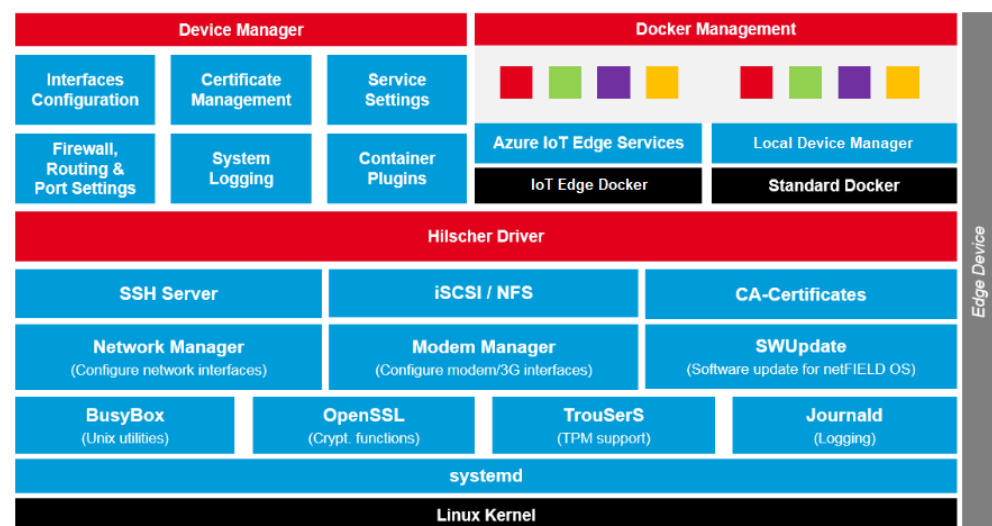


Figure 1: netFIELD OS architecture

## 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 platform remotely. That is why there is no need to have direct access to the netFIELD Device, as long as the device can hold his connection to netFIELD.io. Administrators can be anywhere and have full management access to the device with the stored images and has the ability to control the application containers remotely. Otherwise, the Standard Docker can be used locally if the netFIELD 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.

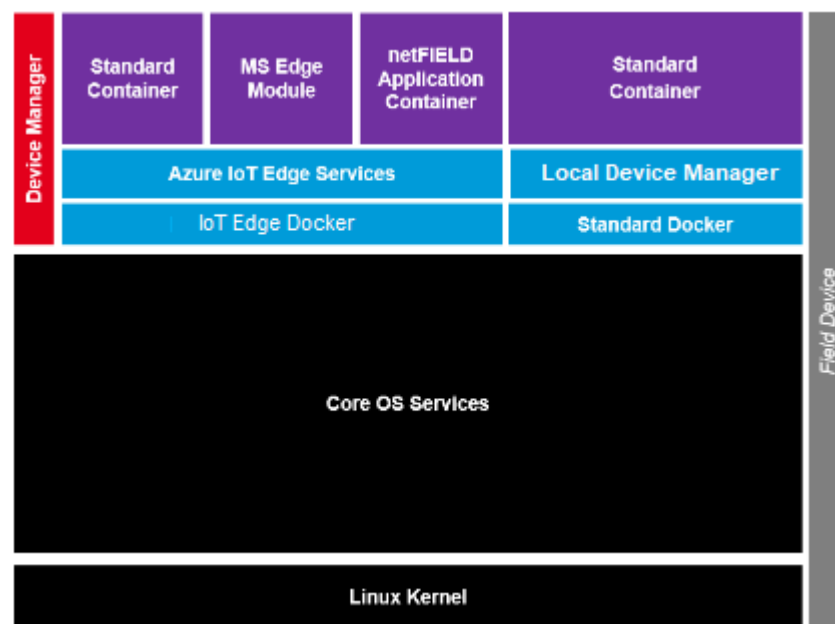


Figure 2: netFIELD OS container management

## 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.

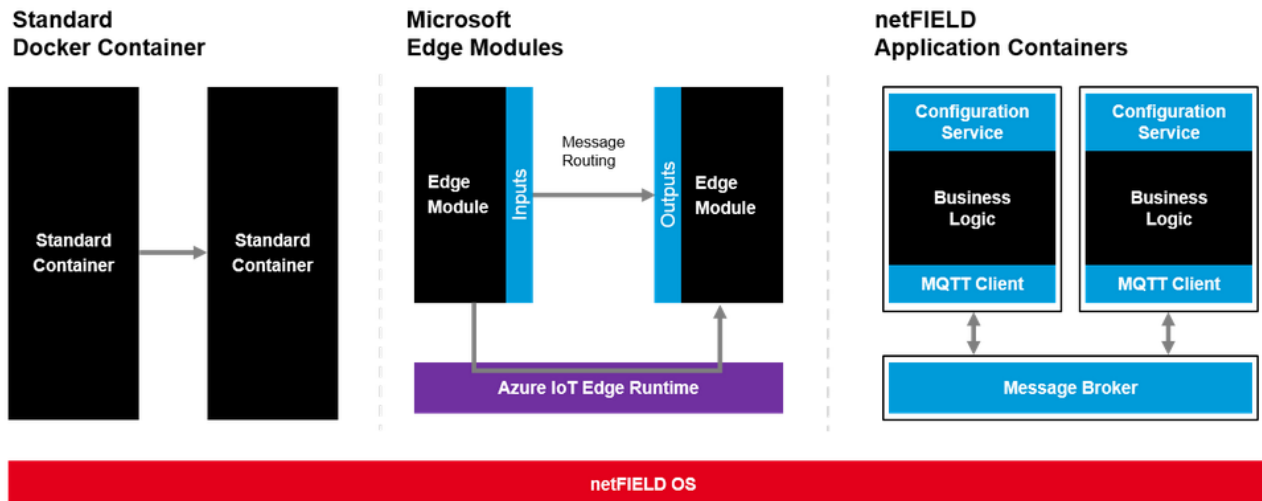


Figure 3: netFIELD OS inter-container communication

## Services supported by netFIELD OS

- Network interface configuration
- 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.
- Secure communication to the netFIELD Platform services
- Remote device control/access via netFIELD Portal (protected by "four-eyes principle", must be enabled in Local Device Manager)
- Firewall configuration (NAT, TCP/IP port management)
- HTTP(S) Proxy Server configuration
- IoT Edge Docker instance for application container managed via netFIELD Platform
- Additional Docker instance for locally managed containers, including Docker Compose support
- netFIELD OS update (local/remote) support
- Onboarding in netFIELD Portal
- Selection of upstream protocol to the netFIELD Platform (AMQP, AMQPWS, MQTT or MQTTWS)
- Network storage (NFS, iSCSI) support
- Resources monitoring
- Access to netFIELD OS and Docker services via a web-terminal or over SSH
- System and container logging

## 2.4 Depiction of netFIELD Connect SW architecture

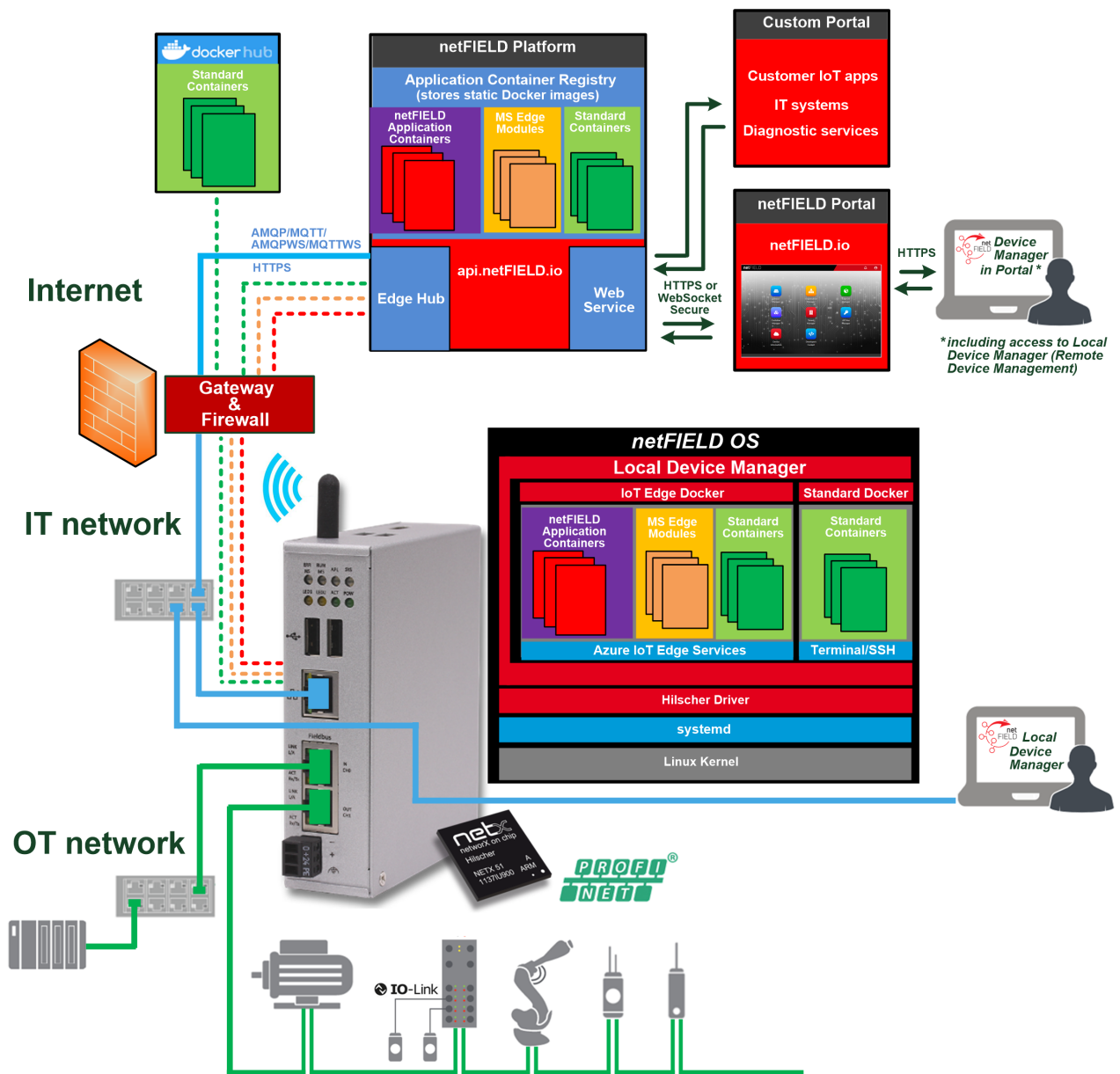


Figure 4: netFIELD Connect SW architecture

## 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 ( $\pm 6$  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 Limitation of program/erase cycles of SD card

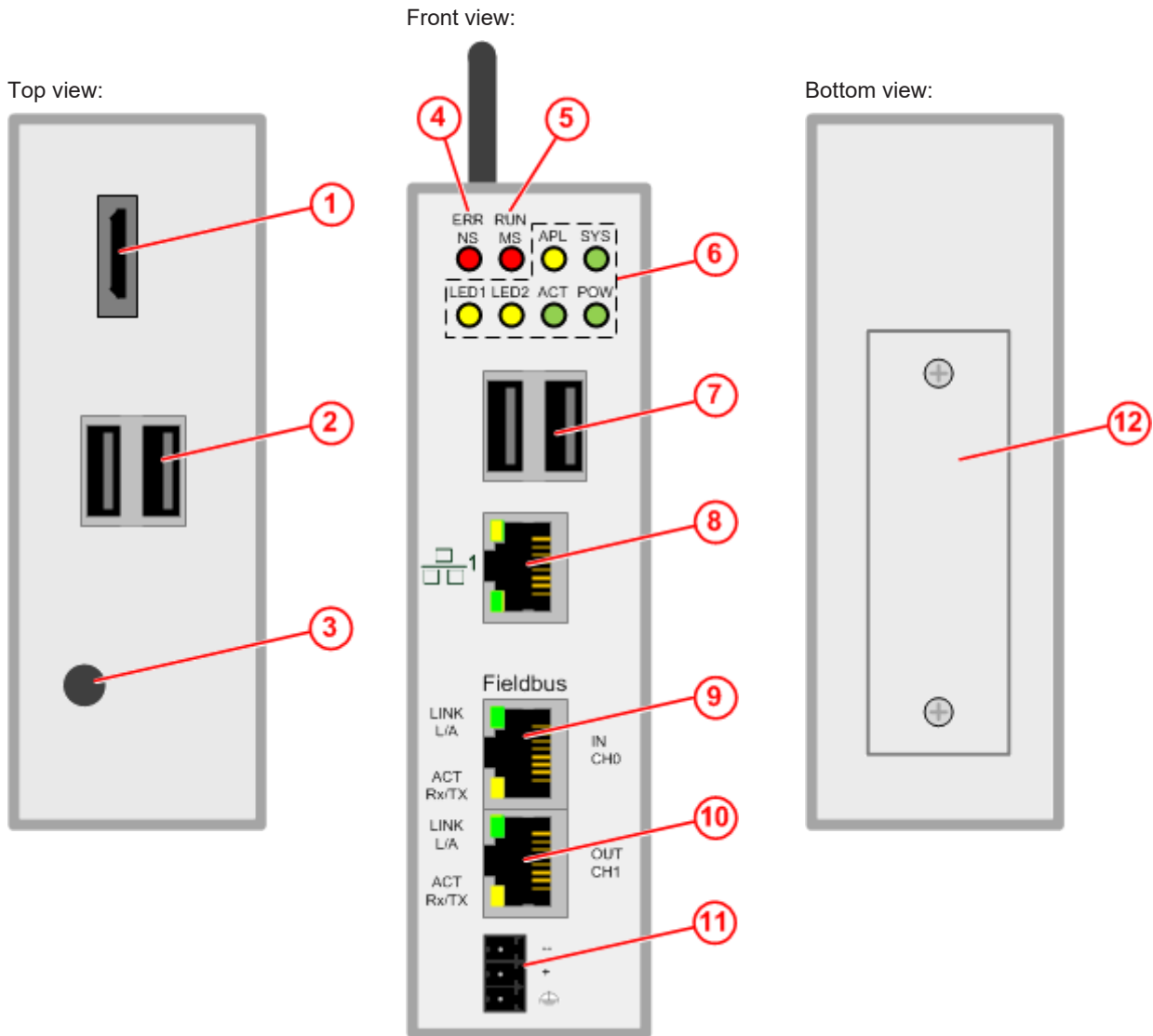
A microSD card supports only a certain amount of terabytes written (TBW) to its flash blocks. Keep this limitation in mind when planning your application, because applications involving frequent database usage may require more TBW than the card can endure.

For information on the capacity of the device's SD card, see section *Technical data* [► page 124].

## 4 Hardware description

### 4.1 Device drawings

#### 4.1.1 Positions of the interfaces



Pos.	Interface	For details see section
(1)	HDMI connector for external monitor	<i>HDMI connector</i> [▶ page 17]
(2)	USB connectors (2x USB 2.0 on top of device)	<i>USB connectors</i> [▶ page 17]
(3)	Antenna (WiFi/Bluetooth)	<i>Wi-Fi</i> [▶ page 17]
(4)	ERR/NS LED for indicating the communication status of the Real-Time Ethernet connection (OT network at "Fieldbus" connector).	<i>LEDs of the Real-Time Ethernet interface</i> [▶ page 20]
(5)	RUN/MS LED for indicating the communication status of the Real-Time Ethernet connection (OT network at "Fieldbus" connector).	
(6)	Device status LEDs (6 x)	<i>Device status LEDs</i> [▶ page 19]
(7)	USB connectors (2x USB 2.0 on front of device)	<i>USB connectors</i> [▶ page 17]
(8)	LAN connector (RJ45 jacket) port 1 / Eth0	<i>LAN connector</i> [▶ page 16]
(9)	Real-Time Ethernet connector (RJ45 jacket) channel 0	<i>Real-Time Ethernet connectors</i> [▶ page 16]
(10)	Real-Time Ethernet connector (RJ45 jacket) channel 1	
(11)	+24 V DC supply voltage connector (Mini Combicon)	<i>Power supply</i> [▶ page 16]
(12)	Cover of slot for NPIX Extension Modules	–

Table 3: Positions of the interfaces

### 4.1.2 Dimensions

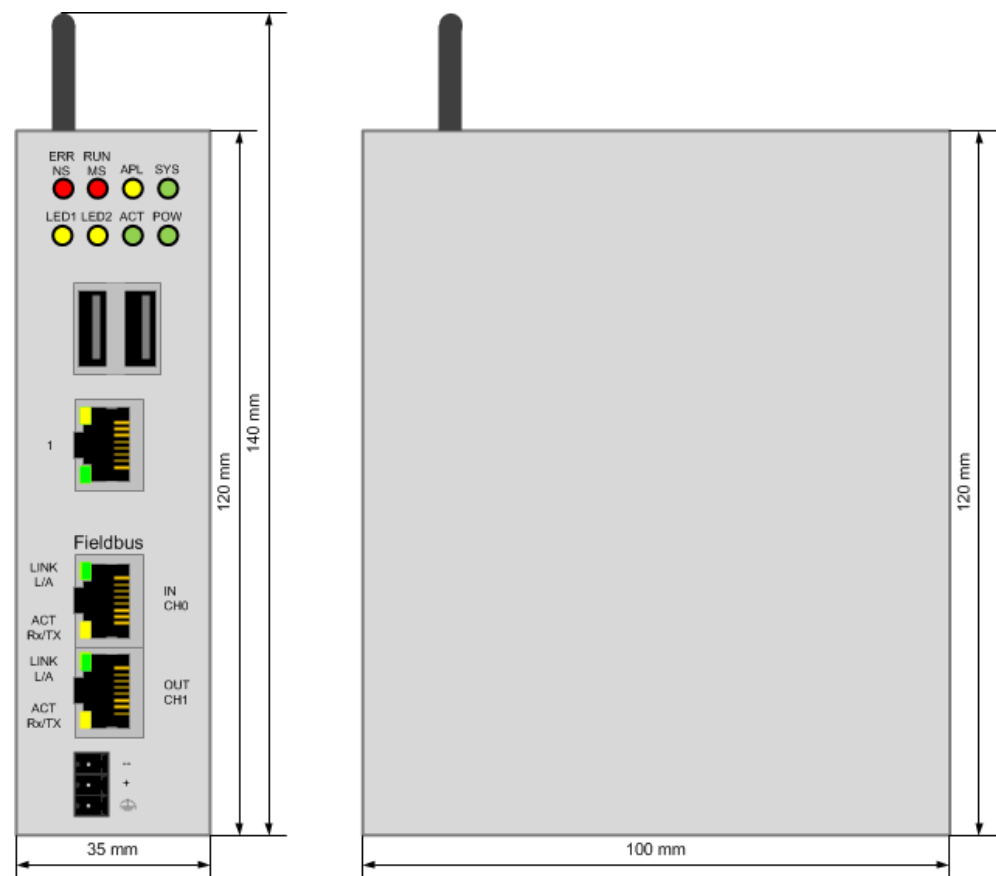


Figure 5: Device dimensions

## 4.2 Interfaces

### 4.2.1 Power supply

See position (11) in section *Positions of the interfaces* [► page 14].



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

Table 4: Power supply connector

### 4.2.2 LAN connector

The RJ45 LAN connector (see position (8) in section *Positions of the interfaces* [► page 14]) allows you to connect your device to your IT network, respectively to the cloud (e.g. the netFIELD Portal).

The MAC address of the LAN interface is printed on the device label.

Note that the “factory setting” for the IP address of the LAN port (eth0) is DHCP mode (“fallback” is *link-local*, i.e. address block 169.254.0.0/16).

You can set the IP address of the eth0 LAN port manually in the Local Device Manager (see section *Networking* [► page 45]).

### 4.2.3 Real-Time Ethernet connectors

The two RJ45 connectors (see positions (9) and (10) in section *Positions of the interfaces* [► page 14]) allow you to connect your device to a Real-Time Ethernet network (OT network) as a “slave” device.

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 **General Settings > OT Interface** (see section *OT Interface (Using the cfx0 interface or RTE)* [► page 108] for further information).



#### 4.2.4 USB connectors

The device is equipped with four USB 2.0 ports (see positions (2) and (7) in section *Positions of the interfaces* [► page 14]).  
For maximum allowed output current, see section *Technical data* [► page 124].

#### 4.2.5 Wi-Fi

The device is equipped with a single band 2.4 GHz Wi-Fi interface according to IEEE 802.11n.  
(For the position of the antenna, see position (3) in section *Positions of the interfaces* [► page 14].)

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 65]).

#### 4.2.6 HDMI connector

The device is equipped with an HDMI socket (see position (1) in section *Positions of the interfaces* [► page 14]).

Note that connecting a monitor here is optional and not required for the “normal” operation of the device.

Note also that the HDMI interface by default is deactivated during runtime, which means that it outputs only “boot information” during device booting. However, you can activate and use the HDMI interface if you deploy a software container featuring the corresponding application.

## 4.3 LEDs

### 4.3.1 Positions of the LEDs on the device

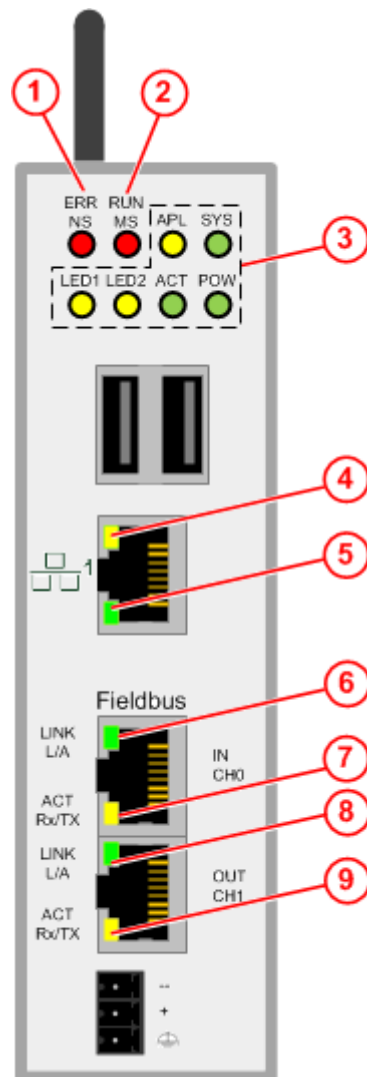


Figure 6: LED positions on device

### 4.3.2 Device status LEDs

LEDs indicating communication status, system status, application status and voltage supply (see position (3) in section *Positions of the LEDs on the device* [► page 18]).

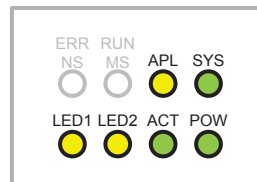


Figure 7: Gateway state LEDs

LED	Color	Meaning
APL	● (yellow)	Application status (of the netX) <b>Note:</b> This LED is controlled by the netX communication controller and is independent from the netFIELD OS operating system. This means that – as long as the device is powered – the LED might be active, even if the netFIELD OS has been shut down.
SYS	● (yellow)/ ● (green)	System status (of the netX) <b>Note:</b> This LED is controlled by the netX communication controller and is independent from the netFIELD OS operating system. This means that – as long as the device is powered – the LED might be active, even if the netFIELD OS has been shut down.
LED1	● (yellow)	GPIO12: can be programmed, currently not used.
LED2	● (yellow)	GPIO13: can be programmed, currently not used.
ACT	● (green)	Activity (of the Linux OS)
POW	● (green)	Voltage supply is OK

Table 5: Description of device's status LEDs

### 4.3.3 LEDs of the LAN interface

LEDs indicating state of the LAN communication (see positions (4) and (5) in section *Positions of the LEDs on the device* [► page 18]).

Pos.	LED	Color	State	Meaning
(4)	ACT / RX/TX	LED yellow		
		☀ (yellow)	Flickering (load dependent)	The device sends/receives frames
		● (off)	off	The device does not send/receive frames.
(5)	LINK	LED green		
		● (green)	On	100 MBit network connection
		● (off)	off	10 MBit or no network connection

Table 6: LEDs LAN interface

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

LEDs (1), (2), (6), (7), (8) and (9) in section *Positions of the LEDs on the device* [► page 18] 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, and are therefore not described in detail here.

Pos.	LED	Color	Meaning
(1)	ERR NS	● (red) / ● (green)	This LED is controlled by the netX communication controller and is independent from the netFIELD OS operating system. This means that – as long as the device is powered – the LED might be active, even if the netFIELD OS has been shut down. Note also that the LED will be showing red light until the device has been properly configured for Real-Time Ethernet communication (which requires the deployment of the appropriate software containers on the device). The LED also shows steady red if the TCP/IP channel of the Real-Time Ethernet interface is enabled (see section <i>OT Interface (Using the cifx0 interface or RTE)</i> [► page 108])
(2)	RUN MS	● (red) / ● (green)	This LED is controlled by the netX communication controller and is independent from the netFIELD OS operating system. This means that – as long as the device is powered – the LED might be active, even if the netFIELD OS has been shut down.

Table 7: LEDs of the Real-Time Ethernet interface

## 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 <i>Mounting</i> [► page 23]
2	Establish LAN connection and login to Local Device Manager	Section <i>Establish LAN connection and login to Local Device Manager</i> [► page 23]
3	Set local system time	Section <i>Set system time</i> [► page 28]
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 59]
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 105]
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 50]
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 Portal</i> [► page 30]
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 8: 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 <i>Mounting</i> [▶ page 23]
2	Establish LAN connection and login to Local Device Manager	Section <i>Establish LAN connection and login to Local Device Manager</i> [▶ page 23]
3	Set local system time	Section <i>Set system time</i> [▶ page 28]
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 59]
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 105]
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 50]
7	Open Standard Docker and deploy and run container images.	Section <i>Standard Docker</i> [▶ page 84]

Table 9: Tasks for commissioning the device (Standard Docker user)

## 5.2 Mounting

- Mount the device onto a DIN top hat rail in a cabinet.
- After mounting, connect the 24 V supply voltage to the device (see position (11) in section *Positions of the interfaces* [▶ page 14]).

---

### 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


In its state of delivery, the LAN interface of the device is preset to DHCP mode. You therefore need a DHCP server in your local network in order to establish a connection to your device.



#### Note:

If the device realizes that no DHCP service is available, it resets its 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 its *IPv4 link local* address at its HDMI port, therefore you can connect a monitor at its HDMI socket to find out the exact address.

1. Use DHCP Server to assign IP address to the LAN interface of the device.
  - Make sure that a DHCP service is available in your local network.
  - Plug an Ethernet cable into the  LAN connector on the front panel of the device (see position (8) in section *Positions of the interfaces* [▶ page 14]), 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, thus allowing you to access the **Local Device Manager**, which is the web-based management GUI of the device.  
If you know the IP address that the DHCP server has assigned to your device, you can now access it directly by entering its 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 HDMI port. Thus, connecting a monitor to the HDMI socket (see position (1) in section *Positions of the interfaces* [▶ page 14]) allows you to check the IP address. In case no DHCP service is available, its “fallback” IPv4 link local address will also be output at the HDMI port.

---

## 2. Establish connection to device.

- 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

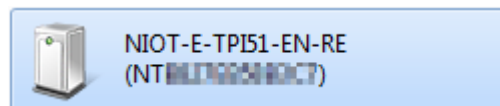
Because the device supports the UPnP technology (Universal Plug and Play), it will be displayed in the **Windows** network environment panel after having received its IP address from the DHCP server. This allows you to connect to it by simple mouse-click.

**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**:



- 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 with the device by entering its host name into the address bar of your browser. You will find the host name printed on the device label next to **Default access (DHCP)**, as shown in this example:



Figure 8: Host name on device label (example)

**Note:**

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

3. Login to **Local Device Manager**.

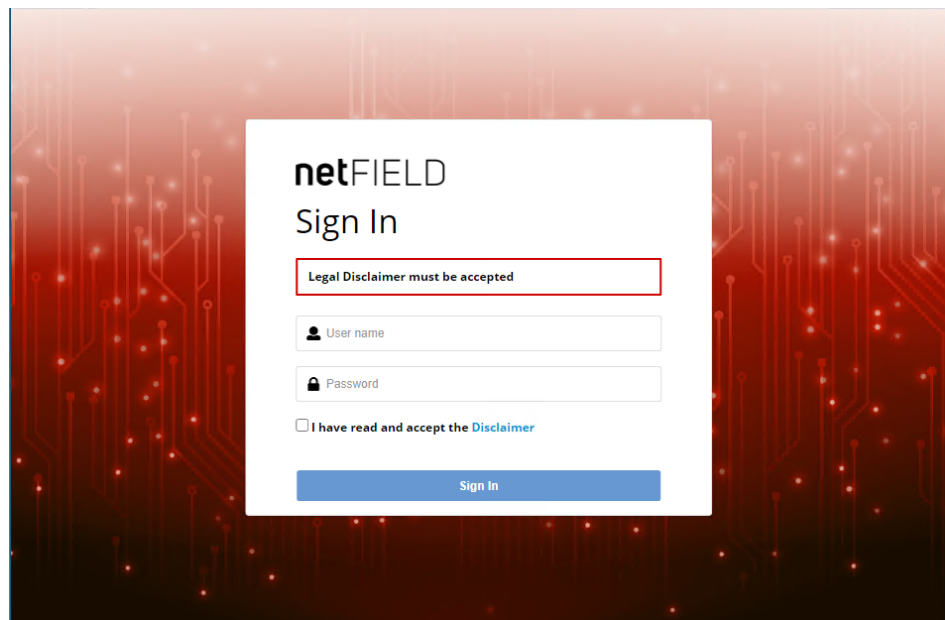


Figure 9: Login Device Manager

- 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:

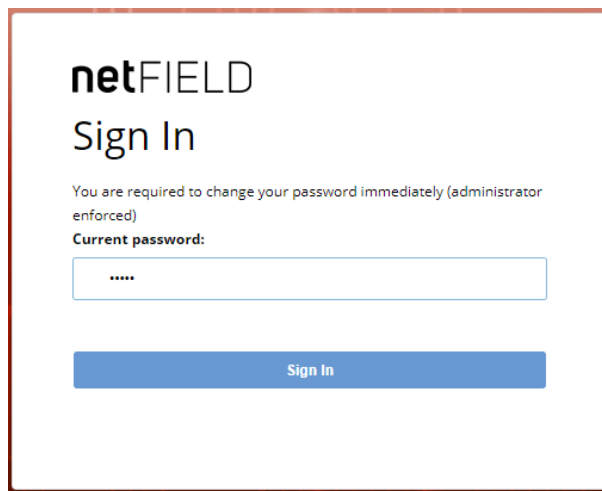
The image shows a web interface for 'netFIELD Sign In'. At the top, the text 'netFIELD Sign In' is displayed. Below it, a message states: 'You are required to change your password immediately (administrator enforced)'. Underneath this message is the label 'Current password:' followed by a text input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

Figure 10: 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 input field is now labeled 'New password:' and contains seven asterisks. The blue 'Sign In' button remains at the bottom.

Figure 11: 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 12: 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).

- 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**:

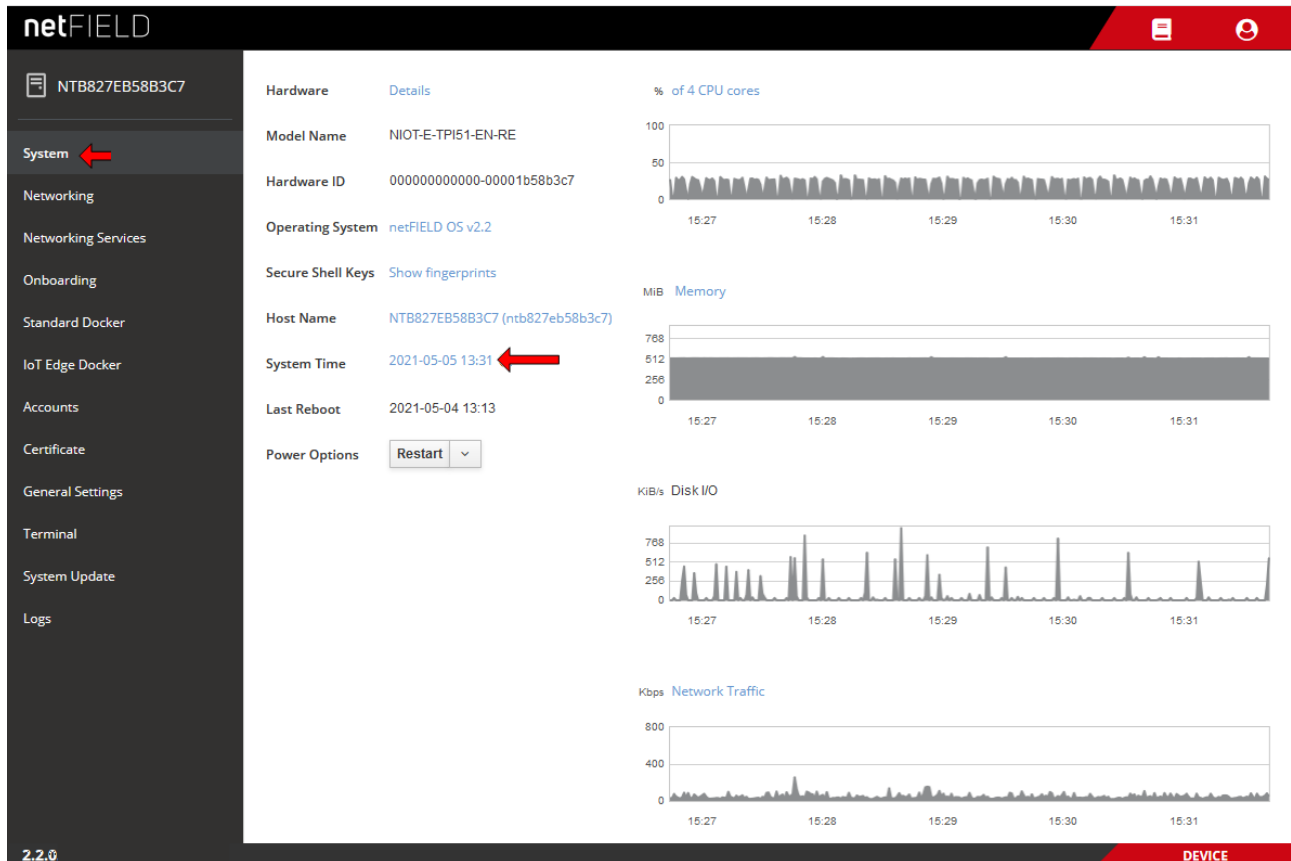


Figure 13: System time value

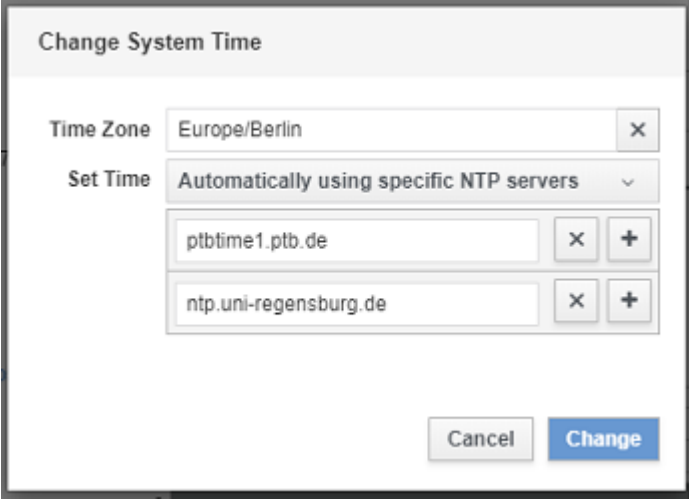
- The **Change System Time** dialog opens:

The dialog box is titled 'Change System Time'. It contains two fields: 'Time Zone' with a text input showing 'UTC' and a close button 'x'; and 'Set Time' with a dropdown menu showing 'Automatically using NTP'. At the bottom right are 'Cancel' and 'Change' buttons.

Figure 14: 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 a "Time Zone" dropdown menu set to "Europe/Berlin". Below it is a "Set Time" dropdown menu set to "Automatically using specific NTP servers". Under the "Set Time" dropdown, there are two input fields for NTP servers. The first field contains "ptbtime1.ptb.de" and the second field contains "ntp.uni-regensburg.de". Each input field has a delete button (x) and an add button (+). At the bottom of the dialog box are "Cancel" and "Change" buttons.

- 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 Portal

### 5.5.1 Overview

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

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:

Figure 15: “Basic” onboarding screen in Device Manager

- Open the **Basic** tab.
- In the **Environment** drop-down list, select the portal’s environment that you are using. Usually, this would be the `Production` environment.
- In the **Device Name** field, enter the name under which the device shall 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 **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*, DOC190701OlxxEN.

- In case your organization has a “Deployment Manifest” that you want to use for your device, select the **Use 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, DOC190701OlxxEN)

- Click **Onboard** button to start the onboarding process.
- ⇒ 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 displays the netFIELD Local Device Manager interface. On the left, a dark sidebar contains a navigation menu with items like System, Networking, and Onboarding. The 'Onboarding' item is highlighted with a red arrow. The main content area shows the 'Advanced' tab of the onboarding process. At the top, there are fields for 'Onboarding Method' (Manual), 'Status' (---), and 'API Endpoint' (---). To the right, the 'Hardware Id' is displayed as '000000000000-00001b58b3c7', with a red arrow pointing to it. Below these are input fields for 'API Endpoint', 'API Key', and 'Activation Code'. The 'Upstream Protocol' is set to 'AMQP'. At the bottom, there is an 'Onboard' button. The bottom of the interface shows the version '2.2.0' and a 'DEVICE' status indicator.

Figure 16: 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 17: 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).
- Keep all other parameters at their default settings. If necessary, you can reconfigure these parameters in the Portal later, after onboarding.



For information on how to configure these parameters, see section *Device Navigation: Edit device settings (Update mask)* in the netFIELD Portal manual (DOC1907010lxxEN).

- Click **Save** 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:

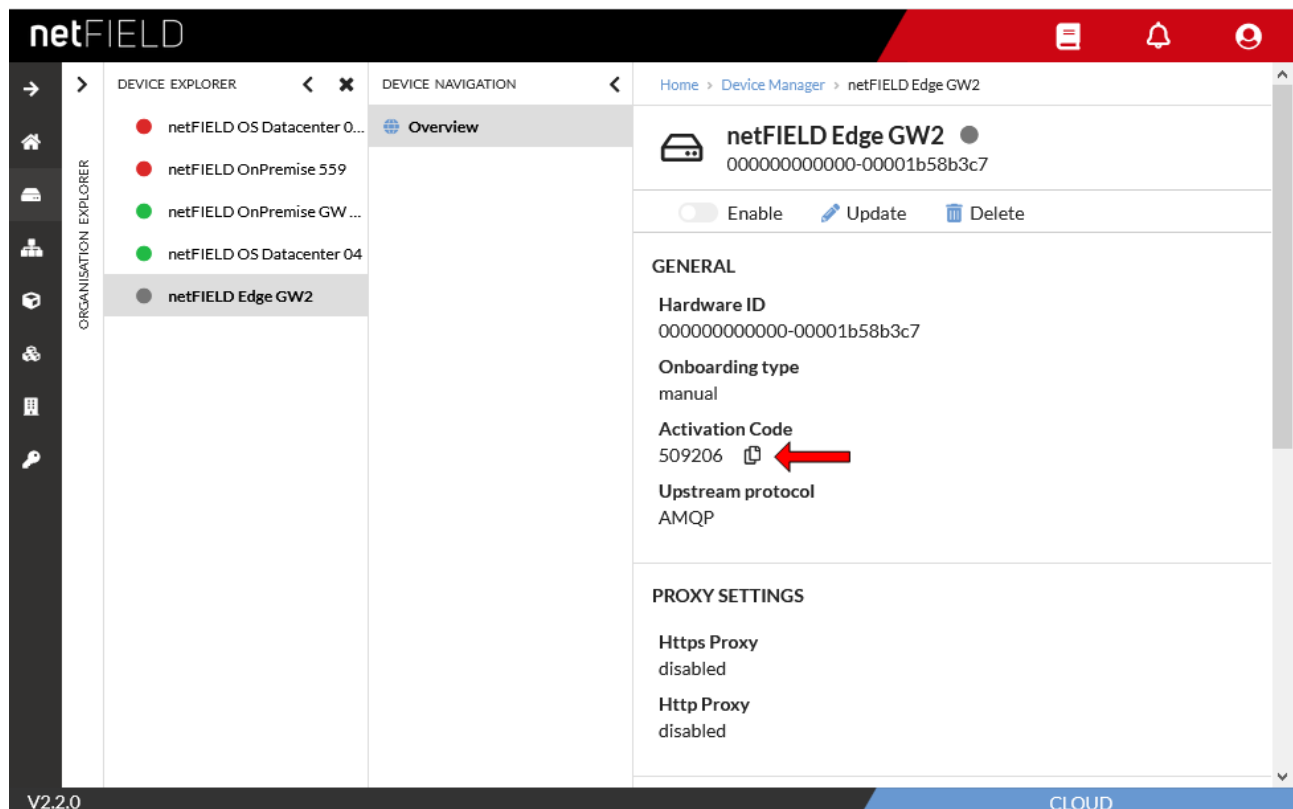


Figure 18: Activation Code in portal

- 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 shows the netFIELD Local Device Manager interface. The sidebar on the left lists various system settings, with 'Onboarding' selected. The main content area is titled 'Onboarding Method' and shows 'Manual' as the selected method. Below this, there are fields for 'Status', 'API Endpoint', 'Hardware Id', and 'Environment'. The 'API Endpoint' field is highlighted with a red asterisk, indicating it is required. The 'API Key' field also has a red asterisk. The 'Activation Code' field contains the value '509206'. The 'Upstream Protocol' is set to 'AMQP'. At the bottom, there is an 'Onboard' button.

Figure 19: 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 **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*, DOC1907010IxxEN.

- In case your organization has a "Deployment Manifest" that you want to use with your device, select the **Use 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, DOC1907010IxxEN)

- 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, DOC1907010IxxEN.

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 or select the corresponding  button, then open its **Permissions** tab:

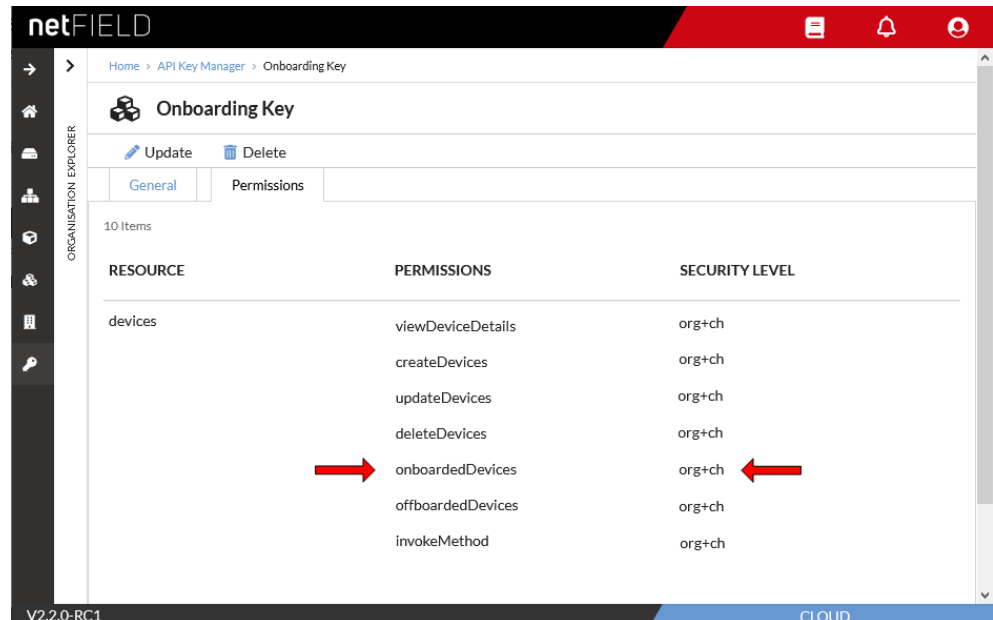

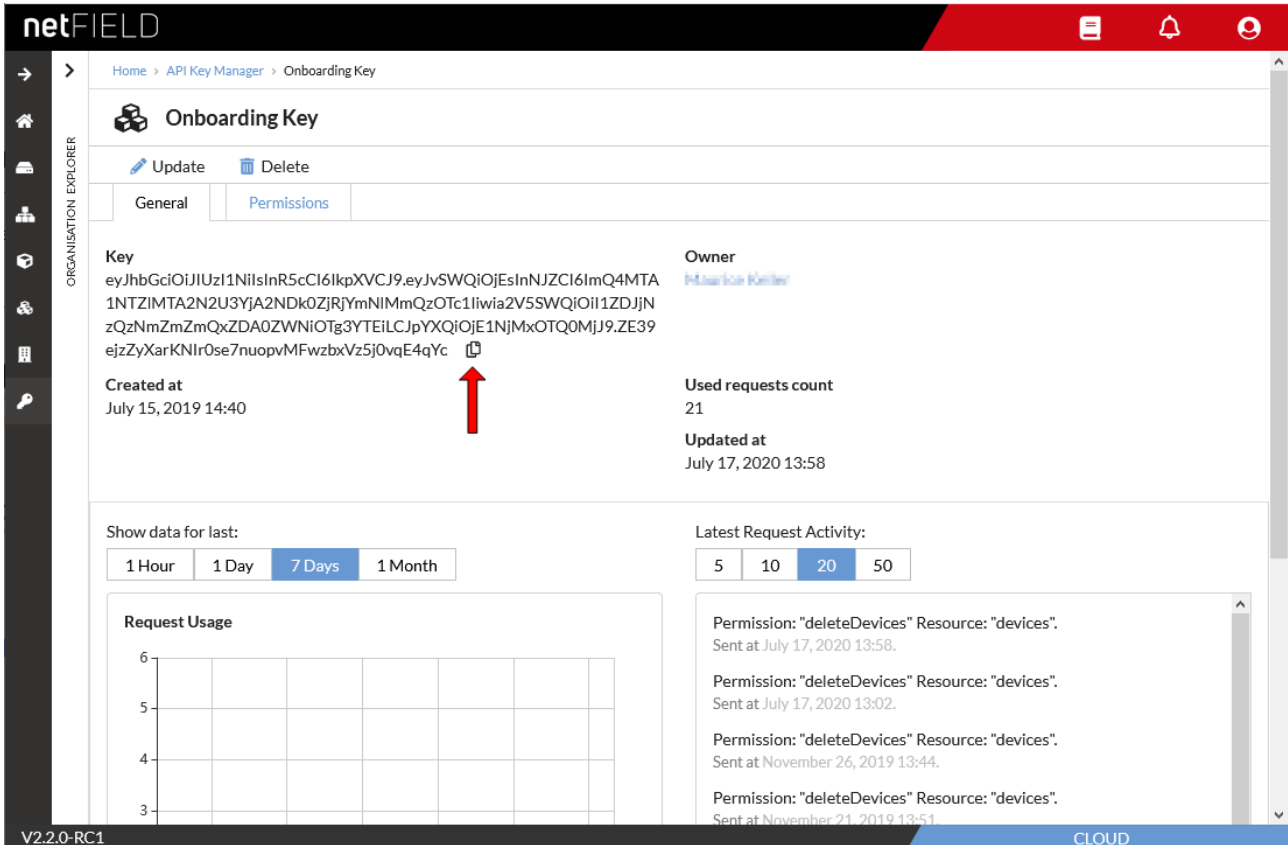


Figure 20: Example of an API Key permitting to onboard devices

- 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:



The screenshot shows the netFIELD API Key Manager interface. The 'Onboarding Key' tab is selected, displaying a long alphanumeric key. A red arrow points to the copy icon (two overlapping sheets) located at the end of the key string. Other details visible include the key's creation date (July 15, 2019 14:40), the owner (Hans-Joachim Kötter), the number of requests (21), and the last update date (July 17, 2020 13:58). Below the key, there are sections for 'Request Usage' (a line chart) and 'Latest Request Activity' (a list of recent requests).

Figure 21: 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 on your Edge 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 Edge 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

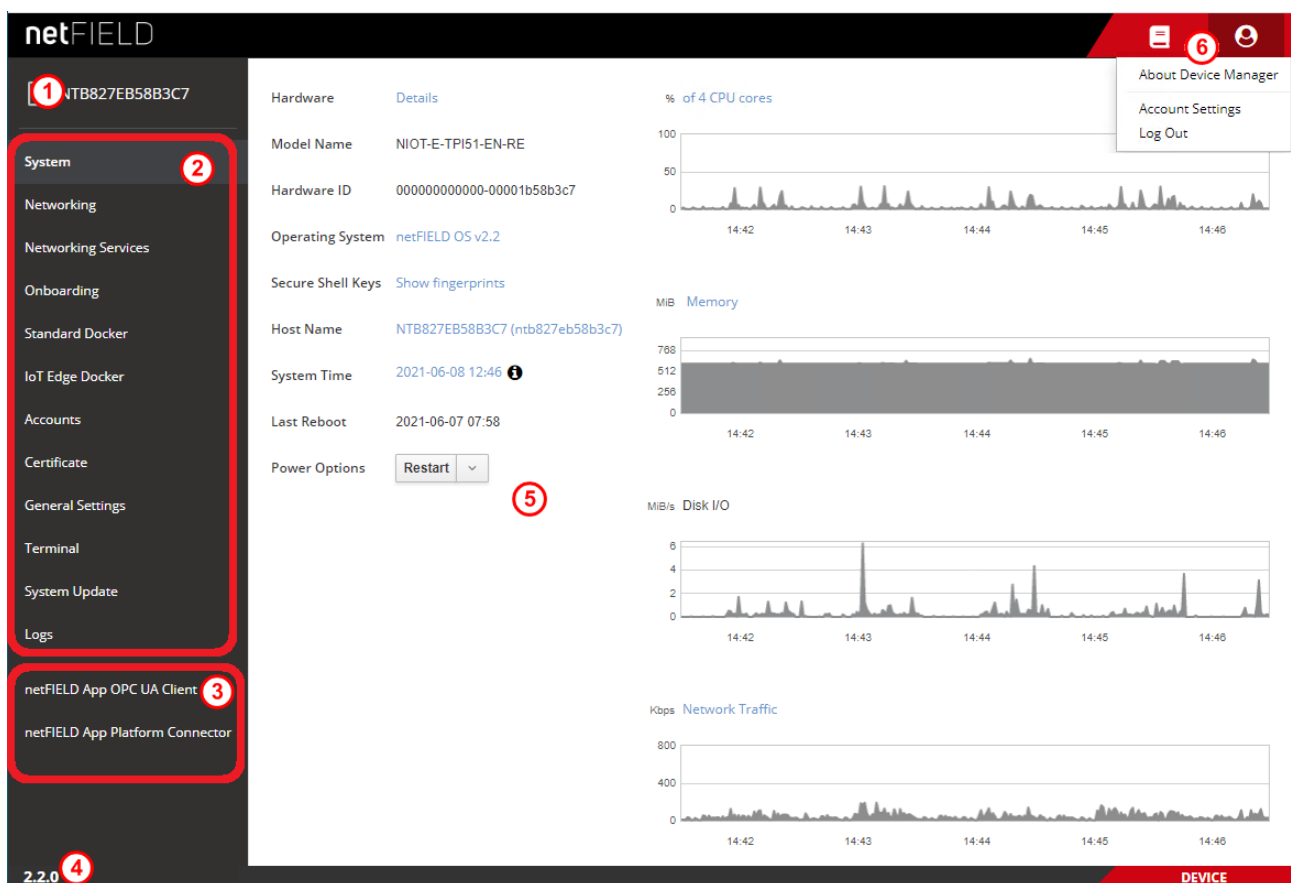


Figure 22: Overview Local Device Manager

(1) “Pretty” host name of the device (can be adapted by the user, see subsection *Host Name* in section *System* [▶ page 42])

(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 97] 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.

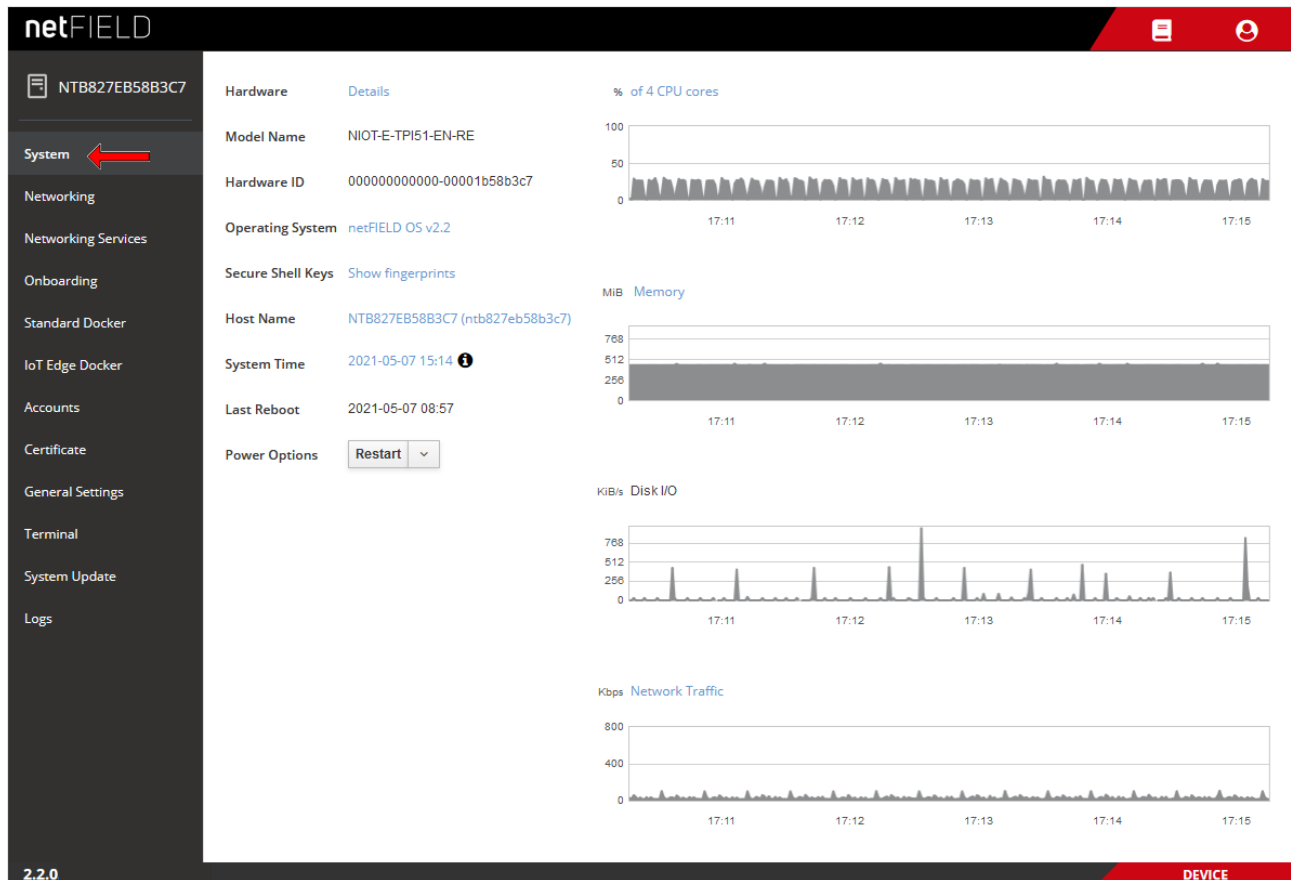


Figure 23: System page in Local Device Manager

### Hardware

Click on **Details** to open a page showing details about your device's hardware like processor cores, RAM, mass storage etc.

### 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 is also used in the netFIELD Portal as unique identifier of your device.

### Operating System

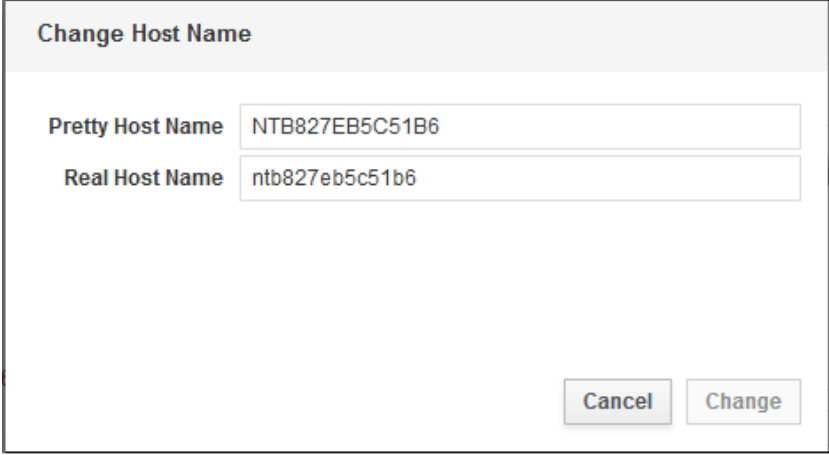
Name and version of the installed netFIELD OS. Click on the blue name to open a window showing further details (i.e. the exact firmware version).

### 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".

Change Host Name	
Pretty Host Name	NTB827EB5C51B6
Real Host Name	ntb827eb5c51b6
<div>Cancel Change</div>	


Figure 24: 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 28].

## 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 to shutdown the netFIELD OS.



### Note:

Note that the hardware and the netX communication controller of the device will not be powered down by using this function. The device itself can only be switched-off by manually removing the voltage supply.

This is the reason why the SYS and POW LEDs (and in some cases also the ERR/NS LED) remain on after using this function. If you want to restart the netFIELD OS after shutdown, briefly remove and reconnect the voltage supply.

## 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.

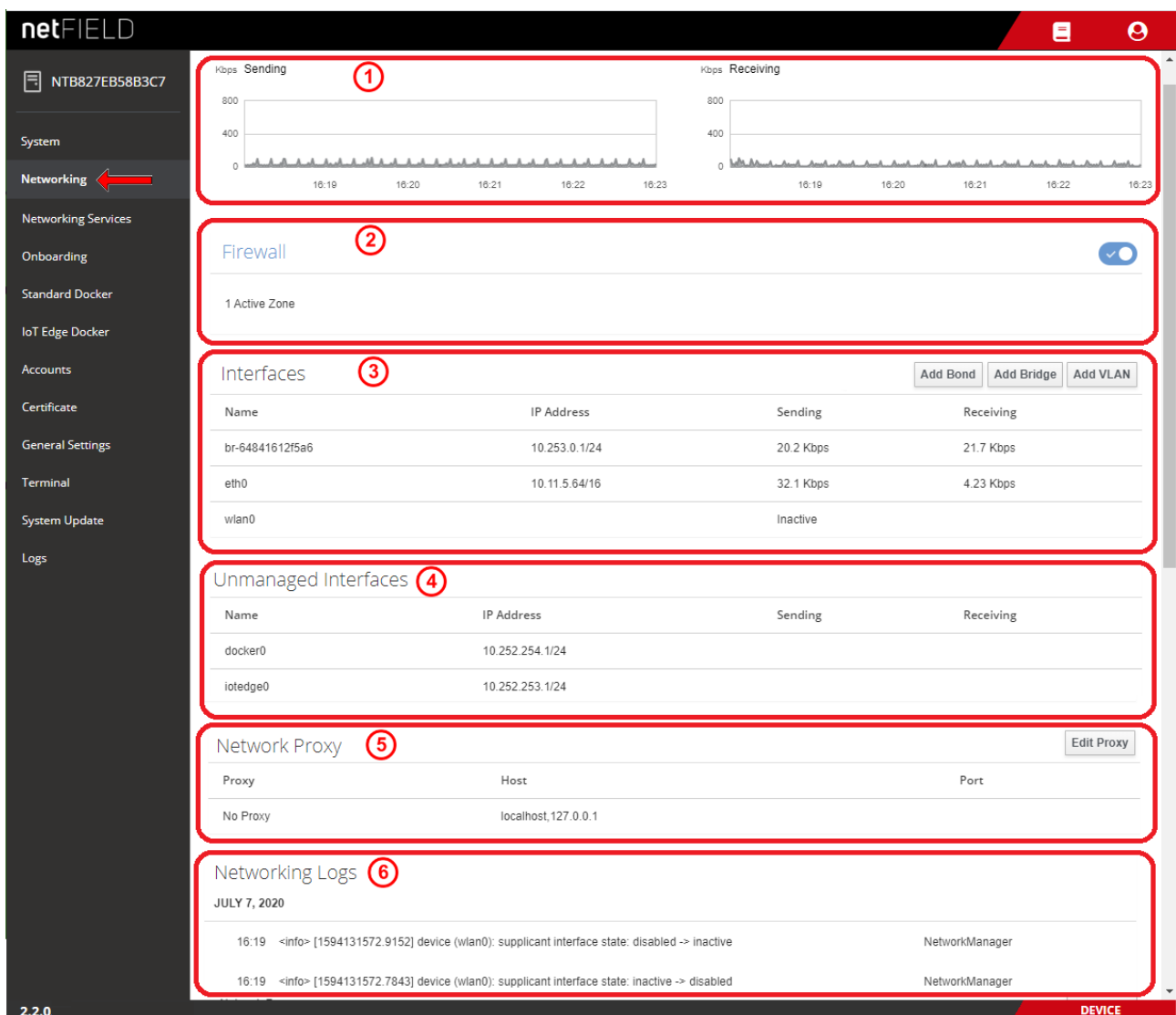


Figure 25: Networking page


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 50] 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 LAN interface of the device (for the location of the LAN connector on the device, see position (8) in section *Positions of the interfaces* [► page 14]).

**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 65]).

**cifx0**: This is the Standard TCP/IP interface of the OT network connectors of the device (see positions (9) and (10) in section *Positions of the interfaces* [► page 14]).



---

### 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 108].

---

### 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:

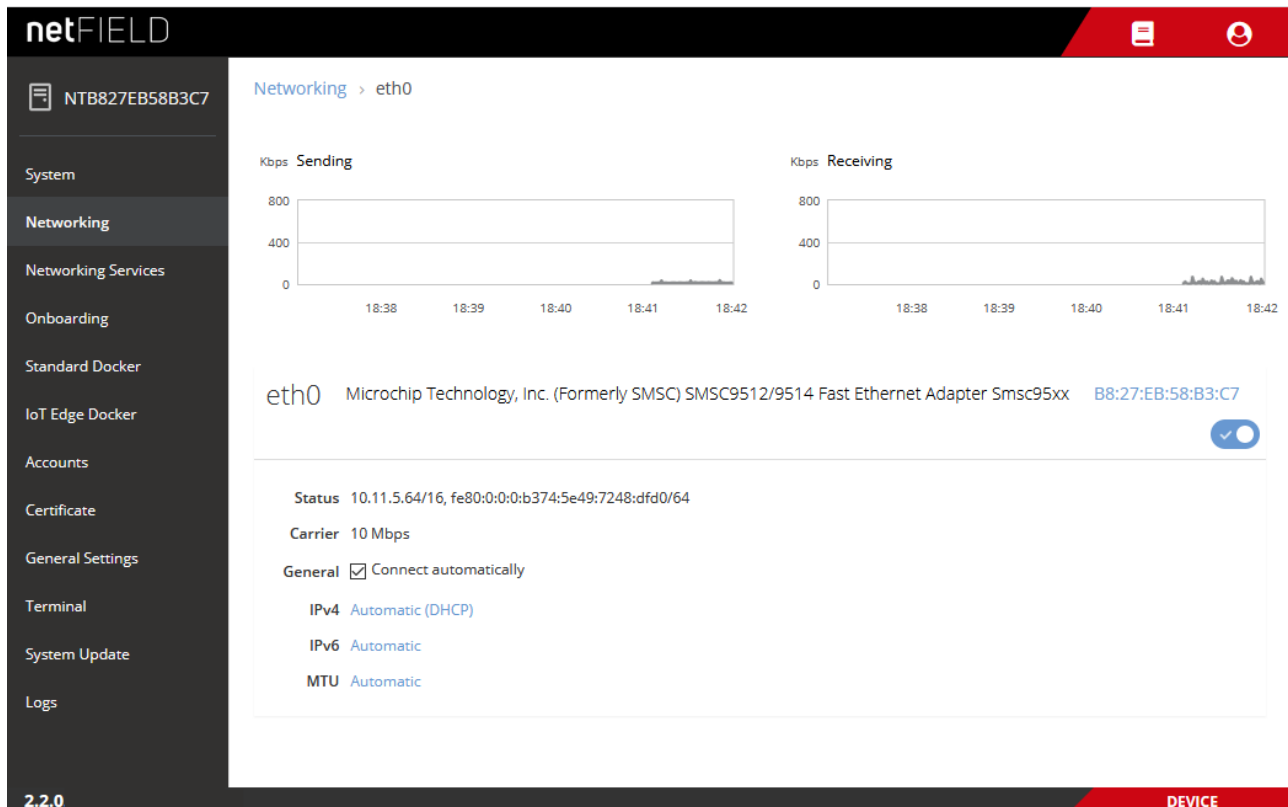



Figure 26: Details of LAN interface (eth0)



#### Important:

Be careful not to deactivate the **eth0** LAN interface by switching off the  toggle switch. Once you have deactivated the interface, the connection to your device via this interface will be lost. If you cannot reach the device via Wi-Fi, you will have to perform either a device recovery (see section *Device recovery via USB* [➤ page 118]) 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.

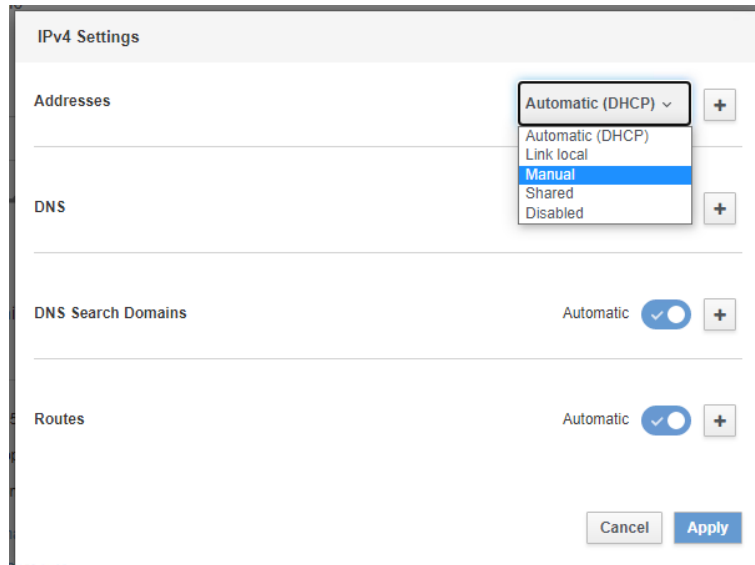


Figure 27: IPv4 Settings

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

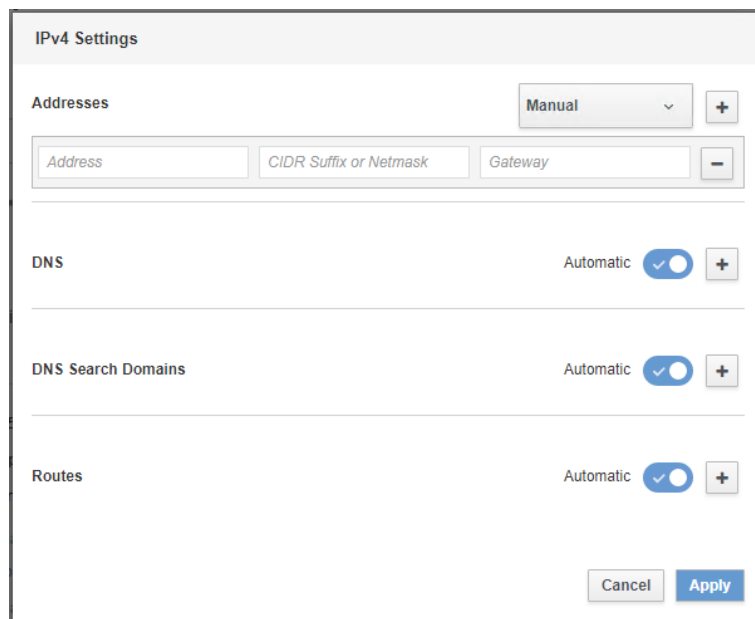


Figure 28: Manual IPv4 Settings

➤ 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 105] 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 59] 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 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.

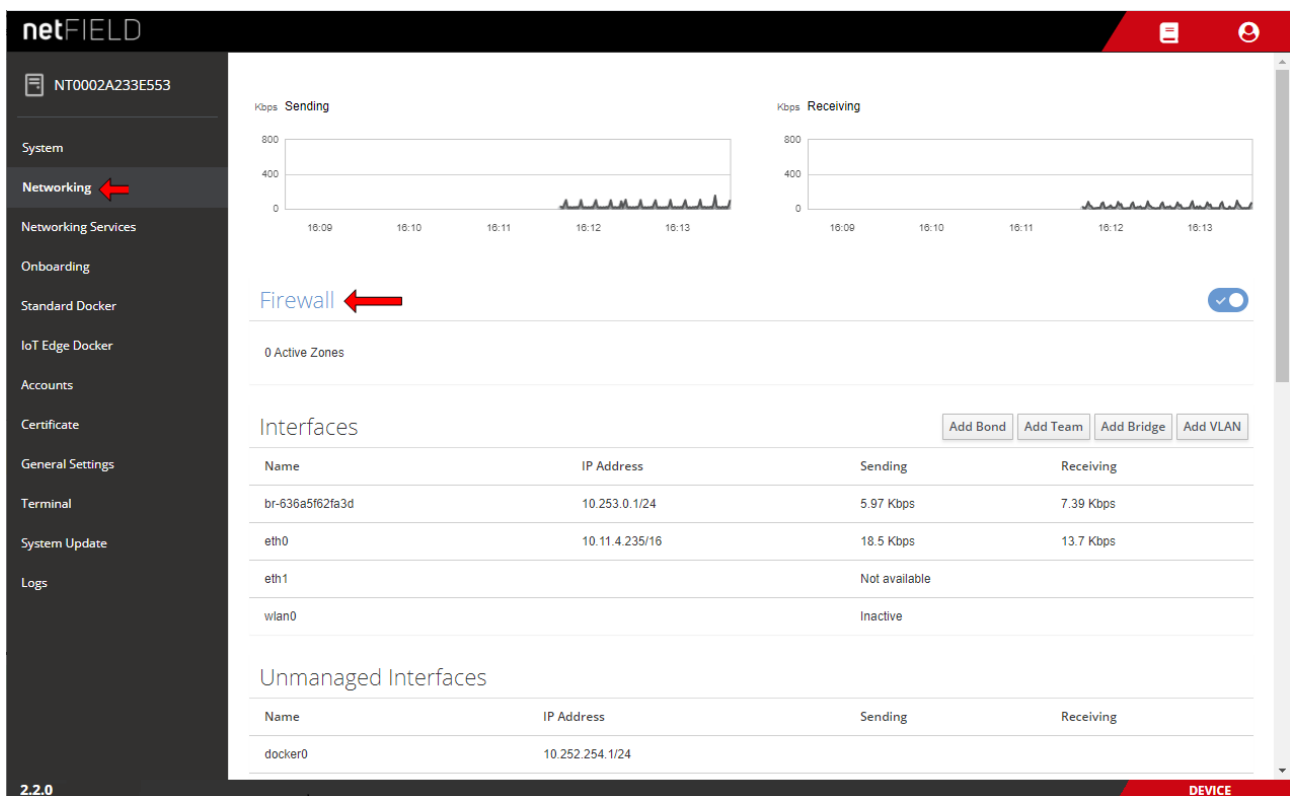


Figure 29: Open Firewall configuration page

- The Firewall configuration page opens:

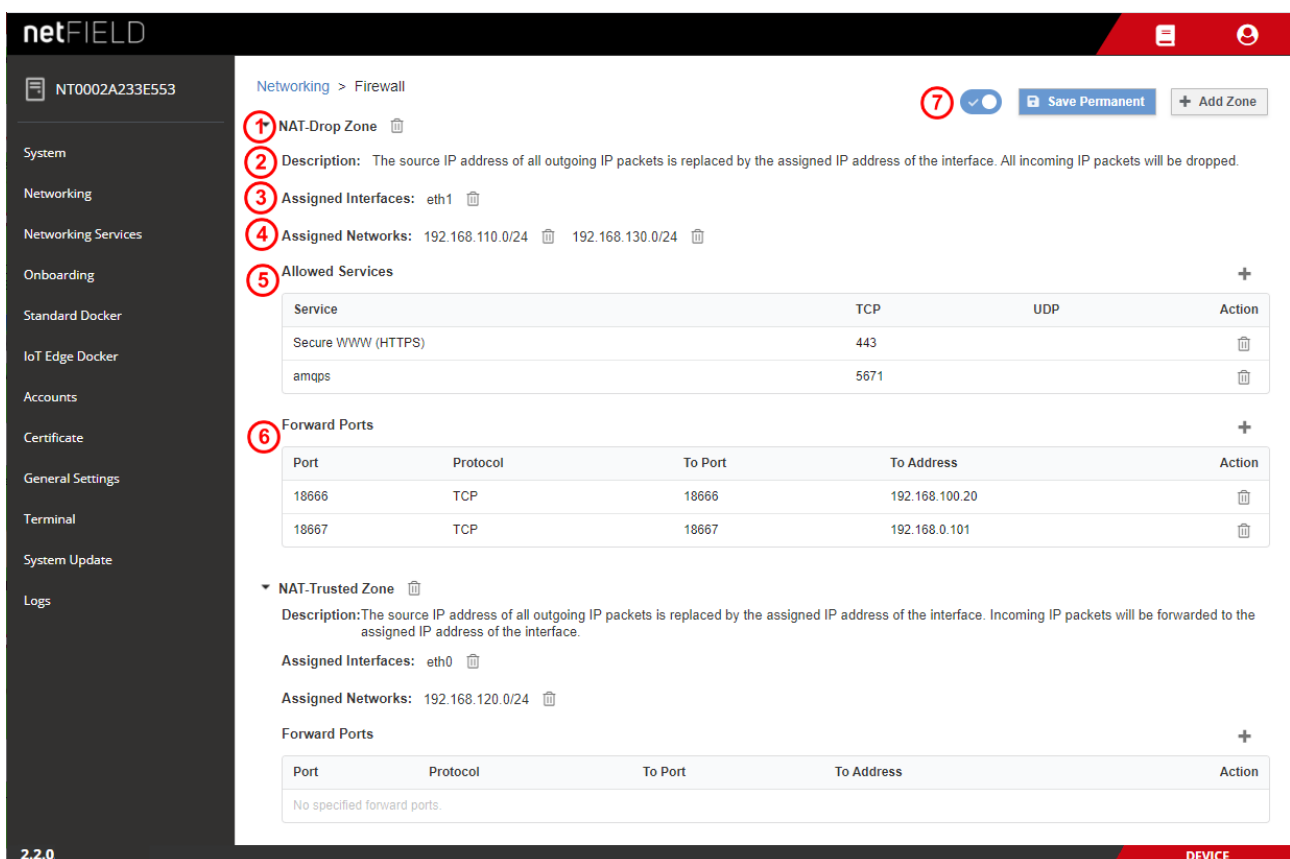



Figure 30: Elements on Firewall configuration page

## 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.
NAT-Drop	NAT = Network Address Translation, a.k.a. "masquerading". 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.
Block	All packets reaching the interface will be dropped. The sender will be notified by an ICMP "unreachable" message.
NAT-Trusted	NAT = Network Address Translation, a.k.a. "masquerading". 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 10: 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**  
☐ br-636a5f62fa3d
 ☐ eth0
 ☒ eth1
 ☐ wlan0

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

Cancel Add Zone

Figure 31: 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 11: 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 12: 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 32: 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 33: 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”). 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	+	Opens a dialog for adding a new port forwarding definition.
	🗑️	Deletes the port forwarding definition.

Table 13: 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:

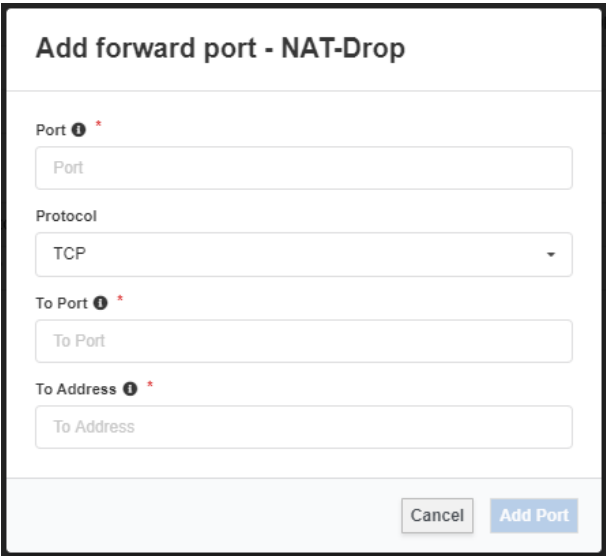


Figure 34: Add forward port dialog

- 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 14: 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 navigation links: System, **Networking** (highlighted with a red arrow), Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, and Logs. 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' with a date filter set to 'AUGUST 7, 2020'. The logs show several events related to the wlan0 interface state and MAC address configuration, all managed by NetworkManager.

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 35: 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 36: 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 two main sections: 'HTTP / HTTPS / FTP' and 'No Proxy'. In the 'HTTP / HTTPS / FTP' section, the 'Host' field contains 'HTTP://10.11.5.98' and the 'Port' field contains '3128'. There is a checked checkbox for 'Authentication required' with fields for 'Username' and 'Password'. Below that is another checked checkbox for 'Use this proxy server for all protocols'. The 'No Proxy' section has a 'Host' field containing 'localhost,127.0.0.1' and a note below it: '(e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)'. At the bottom right are 'Cancel' and 'Apply' buttons.

Figure 37: 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 proxy configuration: 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 'Host' input field with a placeholder 'localhost, 127.0.0.1' and a note '(e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)'. At the bottom right 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	localhost, 127.0.0.1 (e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)			

Figure 38: 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:

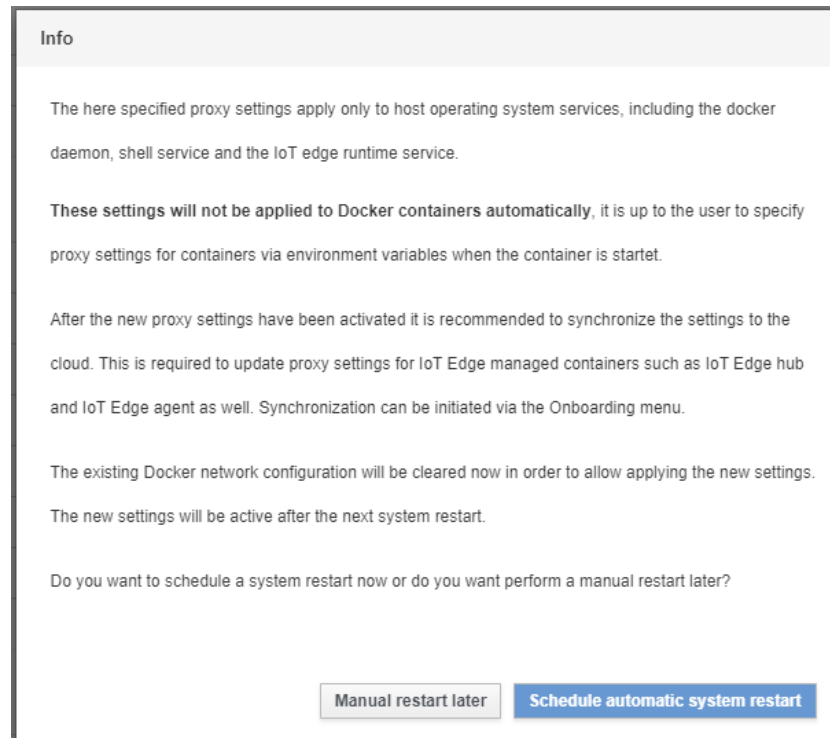


Figure 39: Restart dialog after changing proxy server configuration

- Read the note carefully.
- To apply the new settings, you must restart the netFIELD OS. Click **Schedule automatic system restart** to open the **Restart** dialog, in which you can restart the netFIELD OS immediately or specify a delayed restart.
- Click **Manual restart later** if you want to restart the netFIELD OS later on the **System** page (**System** > **Power Options** > **Restart**). If you choose this option, do not forget to restart later, otherwise the netFIELD OS will not be able to communicate via your new proxy server 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).

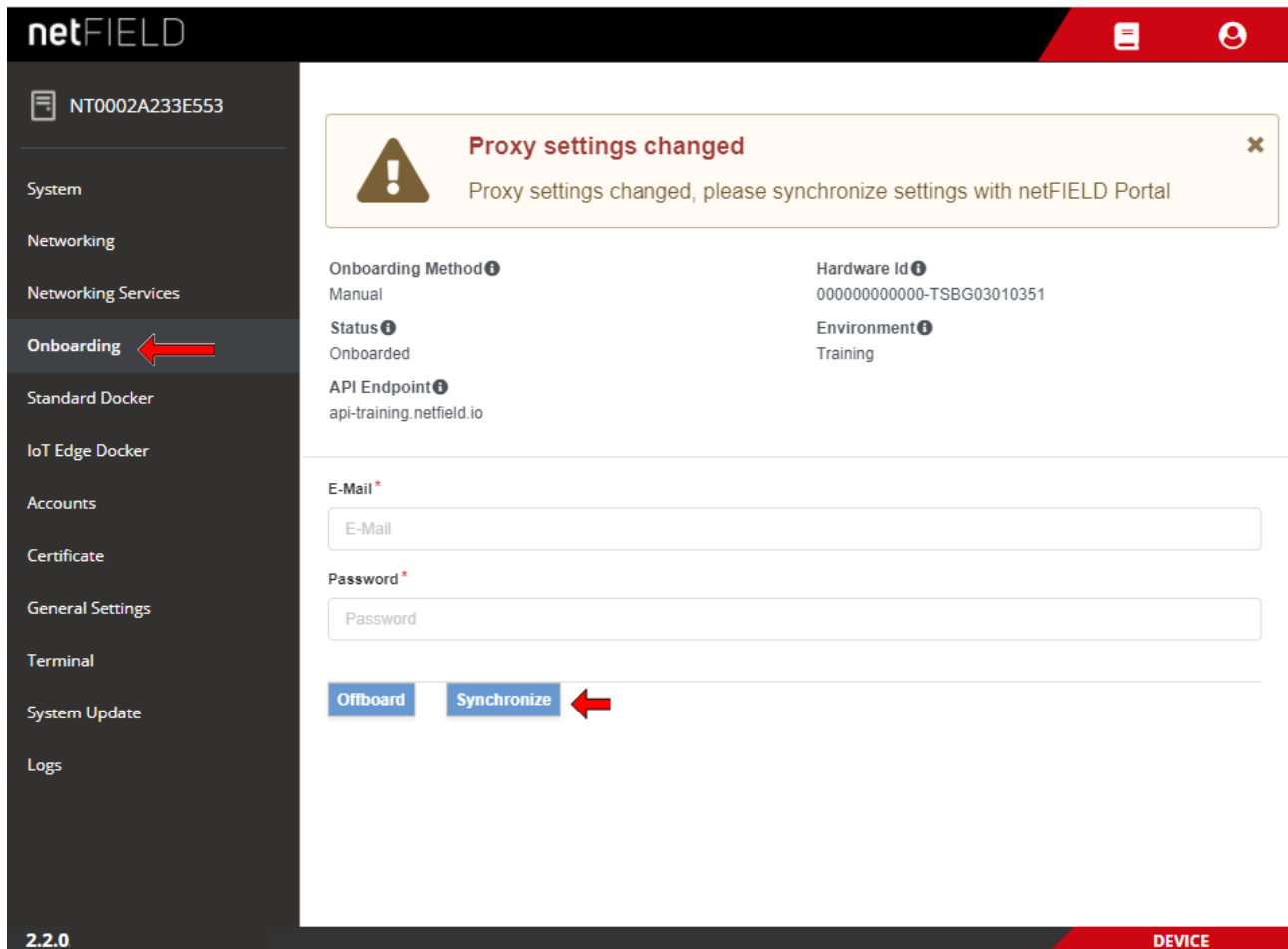


Figure 40: Synchronize proxy settings with netFIELD Portal

- 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. If configured accordingly, it can even route IP data from the clients to other connected subnets, e.g. to an Ethernet subnet connected at its **eth0** interface. The required “port forwarding” can be configured on the **Networking > Firewall** page (see section *Firewall* [► page 50]).



The screenshot shows the netFIELD web interface. The sidebar on the left contains navigation links: System, Networking, **Networking Services** (highlighted with a red arrow), Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, and Logs. The main content area is titled 'netFIELD' and has two tabs: 'WiFi' (selected) and 'DHCP Server'. Under the 'WiFi' tab, the 'Operation Mode' is set to 'Client Mode'. The 'Currently Connected Network' table shows one entry: 'HilscherGuests' with MAC address '82:2A:A8:54:66:41', Band '2.4 GHz', Channel '13', Protection Mode 'WPA2', and Signal Strength '63%'. The 'Visible Networks' table lists four networks: 'Deployment' (72% signal), 'HilscherGuests' (63% signal), 'HilscherIoT' (69% signal), and 'm0b1e@ndw' (22% signal). The 'Hidden Network' section has an SSID input field and a 'Connect' button. The 'Connection Profiles' table shows 'HilscherGuests' with a status of 'Connected' and 'Auto Connect' set to 'Yes'.

Figure 41: 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 67] 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 73] 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 15: Wi-Fi operating modes

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

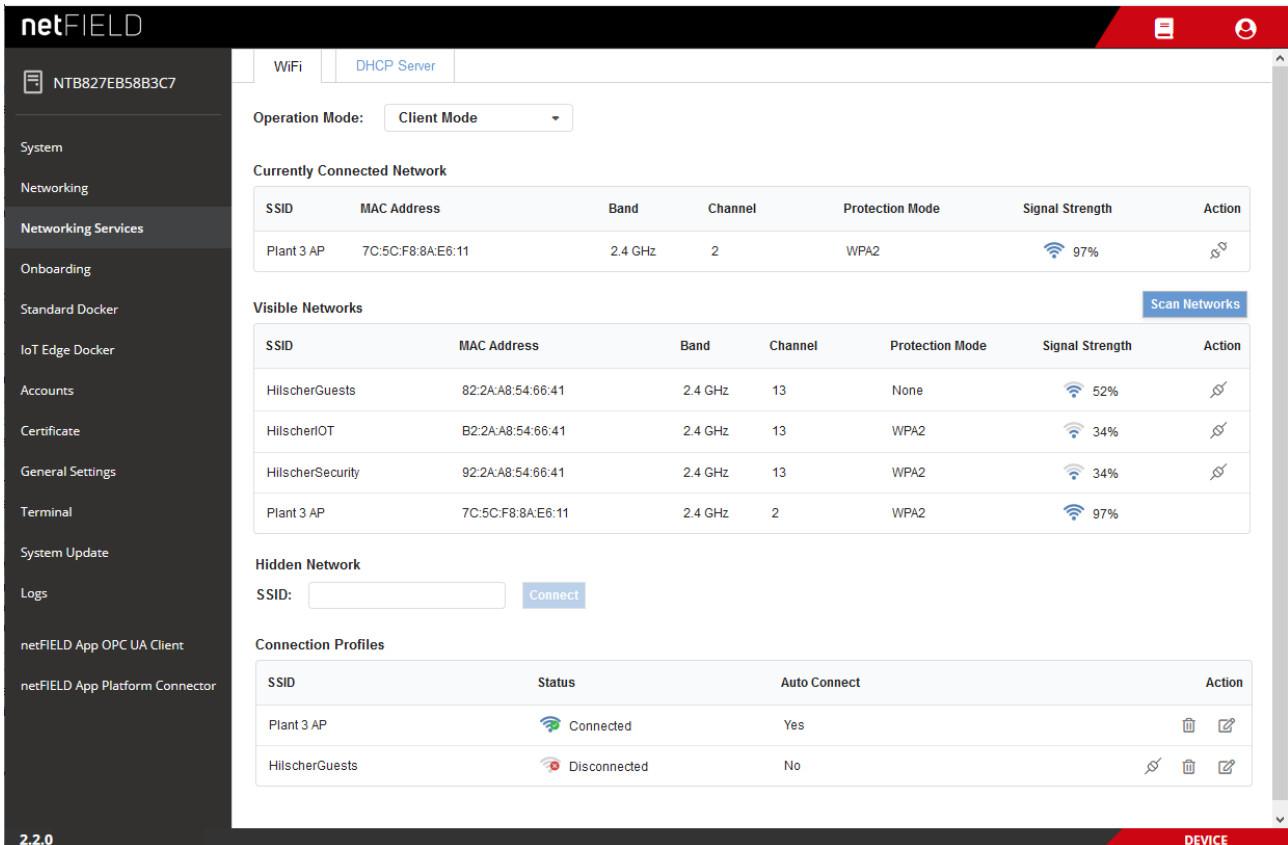
### 6.4.1.2 Client mode

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.



**netFIELD**

NTB827EB58B3C7

System

Networking

Networking Services

Onboarding

Standard Docker

IoT Edge Docker

Accounts

Certificate

General Settings

Terminal

System Update

Logs

netFIELD App OPC UA Client

netFIELD App Platform Connector

2.2.0

WiFi | DHCP Server

Operation Mode: Client Mode

Currently Connected Network

SSID	MAC Address	Band	Channel	Protection Mode	Signal Strength	Action
Plant 3 AP	7C:5C:F8:8A:E6:11	2.4 GHz	2	WPA2	97%	

Visible Networks Scan Networks

SSID	MAC Address	Band	Channel	Protection Mode	Signal Strength	Action
HilscherGuests	82:2A:A8:54:66:41	2.4 GHz	13	None	52%	
HilscherIoT	B2:2A:A8:54:66:41	2.4 GHz	13	WPA2	34%	
HilscherSecurity	92:2A:A8:54:66:41	2.4 GHz	13	WPA2	34%	
Plant 3 AP	7C:5C:F8:8A:E6:11	2.4 GHz	2	WPA2	97%	

Hidden Network

SSID:  Connect

Connection Profiles

SSID	Status	Auto Connect	Action
Plant 3 AP	Connected	Yes	
HilscherGuests	Disconnected	No	

DEVICE

Figure 42: 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 16: 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.


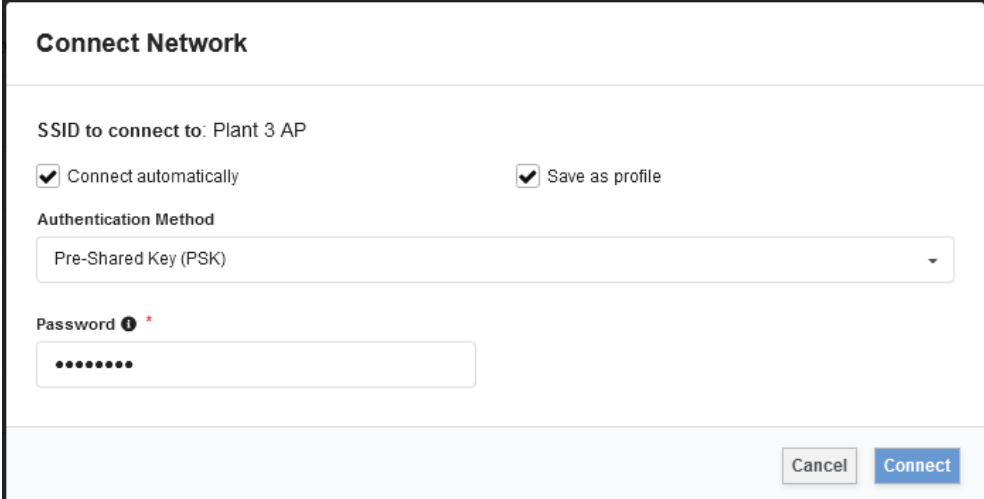
Parameter	Description	
SSID	SSID of the visible Wi-Fi network.	
MAC Address	MAC address of the Access Point of the visible Wi-Fi network	
Band	Radio waveband that the visible Wi-Fi connection uses.	
Channel	Channel that the visible Wi-Fi network uses.	
Protection Mode	Shows the Wi-Fi Protected Access 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 17: 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 43: 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 18: 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 19: Parameters in Connect Network dialog (2)

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

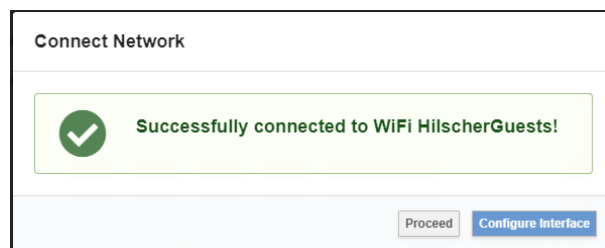


Figure 44: Connect network message

- 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 20: 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:

The screenshot shows the netFIELD web interface for device configuration. The left sidebar lists various system and networking options. The main content area is titled 'WiFi' and 'DHCP Server'. Under 'WiFi', the 'Operation Mode' is set to 'Access Point Mode'. Below this, there are configuration fields for 'Country' (set to Germany), 'Channel' (set to 1), 'SSID' (empty), a 'Hidden' checkbox, 'Protected Access' (set to WPA2), and a 'Pre-shared Key' field. A 'Save' button is located at the bottom of the configuration area.

Figure 45: Access Point Mode

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 21: Access Point parameters

## 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).

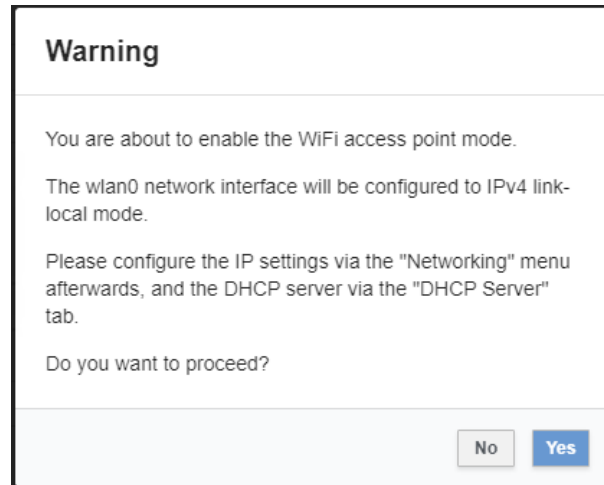


Figure 46: Warning note



### 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:

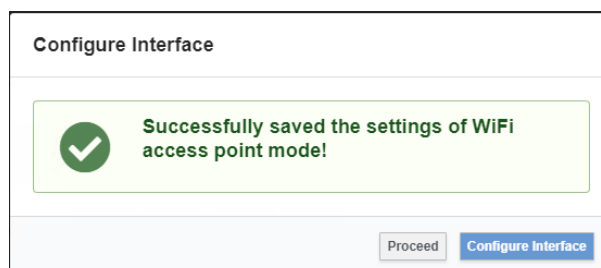


Figure 47: Configure Interface message

- 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.

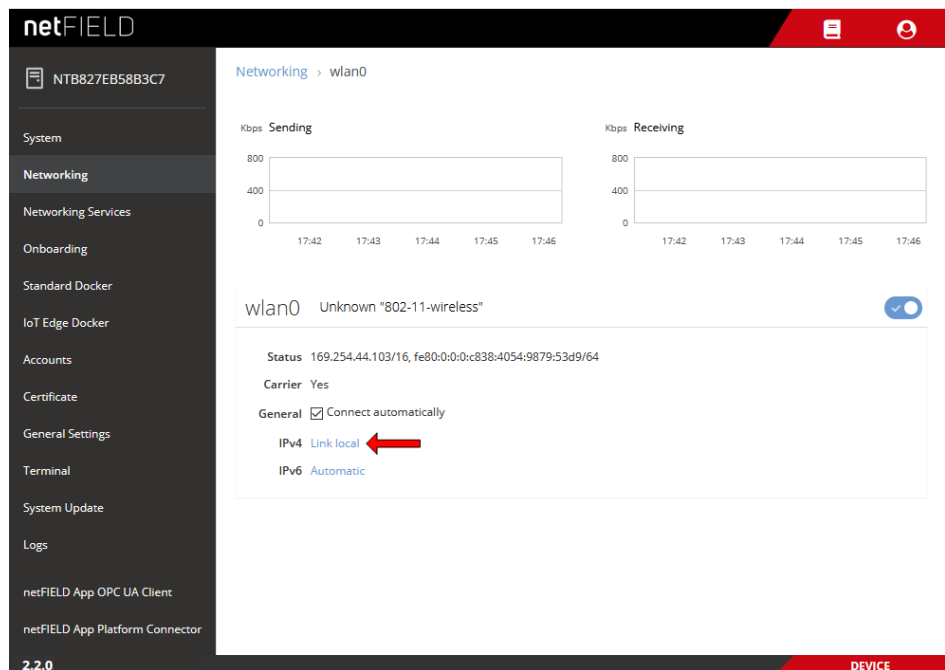


Figure 48: wlan0 configuration page

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

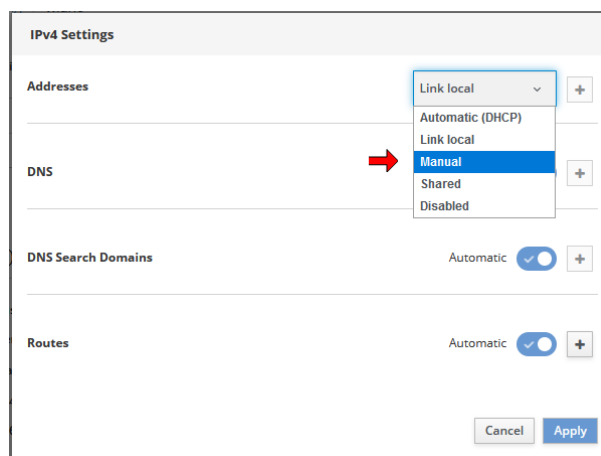
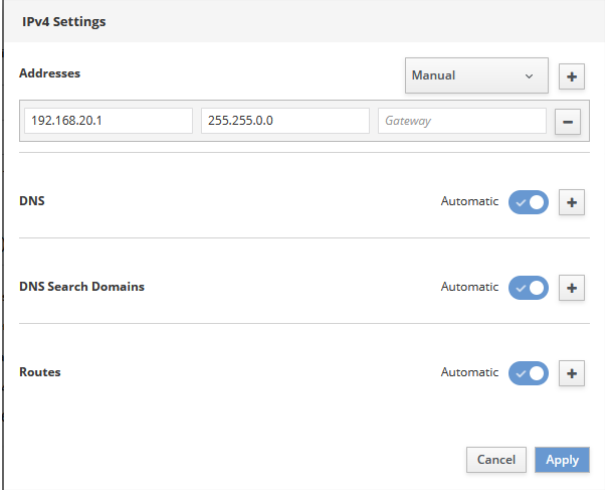


Figure 49: Set manual address in IPv4 Settings dialog

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



The image shows the 'IPv4 Settings' dialog box. It has a title bar 'IPv4 Settings'. Below it, there's a section 'Addresses' with a dropdown menu set to 'Manual' and a '+' button. Below this, there are three input fields: the first contains '192.168.20.1', the second contains '255.255.0.0', and the third is labeled 'Gateway' and is empty. There's a '-' button to the right of the 'Gateway' field. Below the 'Addresses' section, there are three sections: 'DNS', 'DNS Search Domains', and 'Routes'. Each section has a toggle switch set to 'Automatic' (indicated by a blue circle with a checkmark) and a '+' button. At the bottom right, there are 'Cancel' and 'Apply' buttons.

Figure 50: 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, 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** Ethernet interface of the device is not yet supported by the current netFIELD OS.

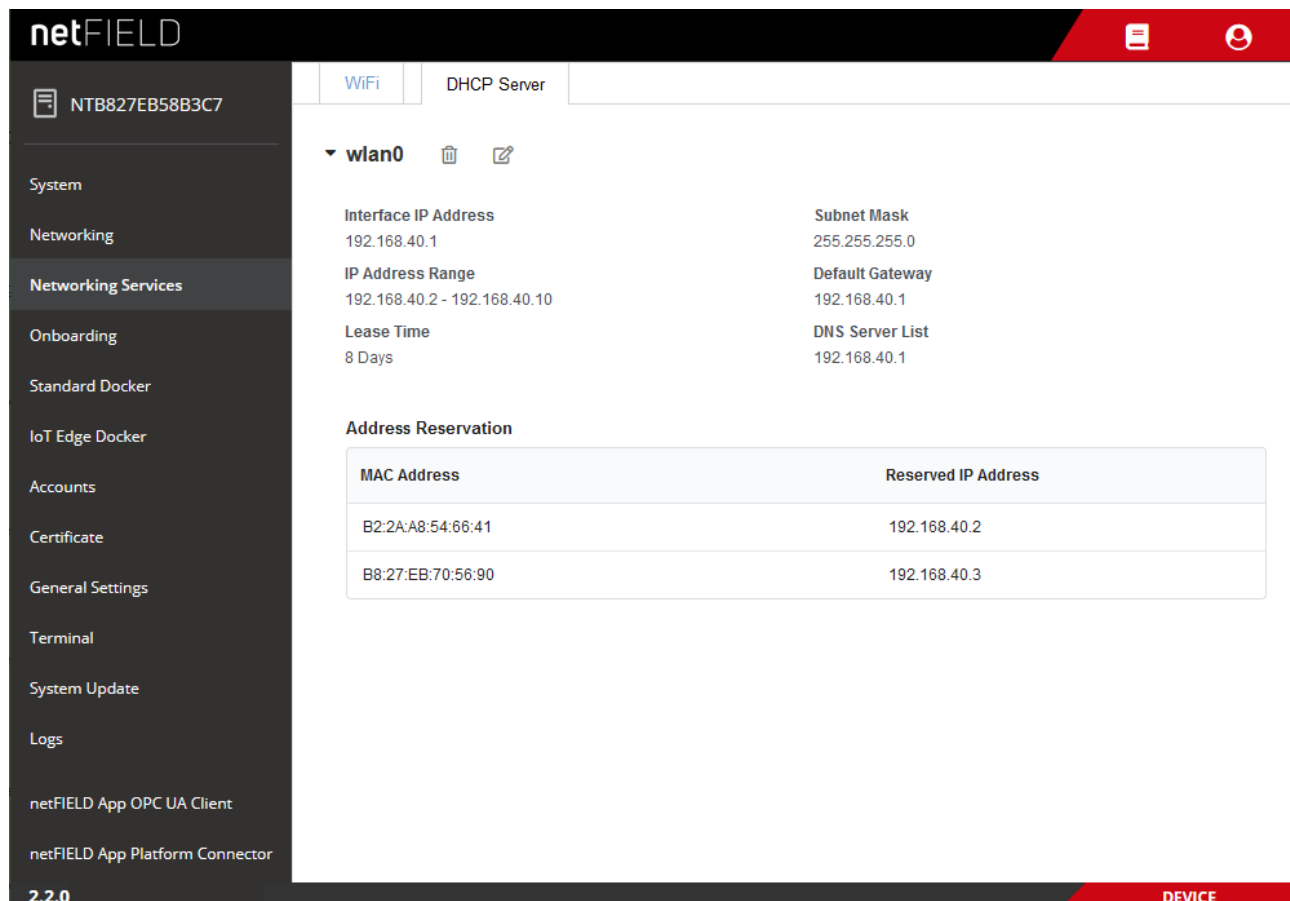



Figure 51: Configured DHCP service

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 22: 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 52: 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 23: Parameters of DHCP Server Configuration dialog



## 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 Portal* [▶ page 30]. 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 59] for further information.)

netFIELD

NT000C295DBDCC

System

Networking

Networking Services

**Onboarding**

Standard Docker

IoT Edge Docker

Accounts

Certificate

General Settings

Terminal

System Update

Logs

2.2.0

Onboarding Method ⓘ

Manual

Status ⓘ

--

API Endpoint ⓘ

--

Hardware Id ⓘ

33fc77c15aef-64ff3809b71a

Environment ⓘ

--

Basic Advanced

Environment \*

Environment

Device Name

Device Name

E-Mail \*

E-Mail

Password \*

Password

Upstream Protocol

Upstream Protocol

☐ Use Manifest

Onboard

DEVICE

Figure 53: 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

netFIELD

NT000C295DBDCC

System

Networking

Networking Services

**Onboarding**

Standard Docker

IoT Edge Docker

Accounts

Certificate

General Settings

Terminal

System Update

Logs

netFIELD App Platform Connector

netFIELD App OPC UA Client

2.2.0

Onboarding Method ⓘ  
Manual

Status ⓘ  
Onboarded

API Endpoint ⓘ  
api-training.netfield.io

Hardware Id ⓘ  
33fc77c15aef-64ff3809b71a

Environment ⓘ  
Training

E-Mail \*

E-Mail

Password \*

Password

Offboard

DEVICE

Figure 54: 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.
- Click **Offboard** button.
- After successful offboarding, the following message appears: **Success – Device is now deleted.**

## Offboarding after having used the Advanced Onboarding method

netFIELD

NT000C295DBDCC

System

Networking

Networking Services

**Onboarding**

Standard Docker

IoT Edge Docker

Accounts

Certificate

General Settings

Terminal

System Update

Logs

2.2.0

Onboarding Method ⓘ  
Manual

Status ⓘ  
Onboarded

API Endpoint ⓘ  
api-training.netfield.io

Hardware Id ⓘ  
33fc77c15aef-64ff3809b71a

Environment ⓘ  
—

API Key \*

API Key

Offboard

DEVICE

Figure 55: 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 are still present on the device. They can be deleted manually on the **IoT Edge Docker** page of the Local Device Manager.

---

## 6.6 Standard Docker

The **Standard Docker** page allows you to download and manage Docker images and containers from the “standard” Docker Hub (i.e. images/containers that are not “deployed” from the *netFIELD Portal*).

Unlike the **IoT Edge Docker** (which manages images/containers from the *netFIELD Portal*), the Standard Docker can be used without having to “onboard” the device in the portal beforehand.



### Note:

The network address settings of the Standard Docker can be managed under **General Settings > Docker Network Settings** (see section *Docker Network Settings* [▶ page 105]).

The screenshot displays the netFIELD Standard Docker management interface. The left sidebar contains navigation links for various system functions. The main area is titled 'Standard Docker' and includes a filter dropdown (1) set to 'Images and running containers'. Below this, there are performance graphs (2) for CPU and memory usage. The 'Containers' section (3) shows a table with two running containers: 'postgres01' and 'portainer'. The 'Images' section (4) shows a table with two downloaded images: 'portainer/portainer-ce:latest' and 'postgres:latest'. A 'Get new image' link is available in the top right of the Images section.

Figure 56: 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:

The screenshot shows the netFIELD web interface. On the left is a sidebar with navigation options: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings (highlighted with a red arrow), Terminal, System Update, and Logs. The main area is titled 'Containers' and shows a table of running containers. The 'postgres01' container is selected, and its details are expanded. The details panel shows the container ID, creation time, image, command, and state. Below the details is a section for 'Images' showing the 'portainer/portainer-ce:latest' image. At the top of the main area, there are two graphs: '% Combined usage of 4 CPU cores' and 'MiB Combined memory usage'. A status bar at the top right shows '2.06 GiB Free' and '0.475 / 2.53 GiB'.

Name	Image	Command	CPU	Memory	State
portainer_1	portainer/portainer-ce:latest	/portainer	0%	10.4 MiB	running
postgres01	postgres:latest	docker-entrypoint.sh postgres			running

**Container Details for postgres01:**

- Id: 972d741362379dd52d6d45f9d5ed3de5b7a3393eabc525720b70bf90d1df83f5
- Created: Today at 12:39 PM
- Image: postgres:latest
- Command: docker-entrypoint.sh postgres
- State: Up since Today at 1:44 PM

**Images:**

Name	Created	Size
portainer/portainer-ce:latest	Last Sunday at 11:06 PM	152 MiB

Figure 57: 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:

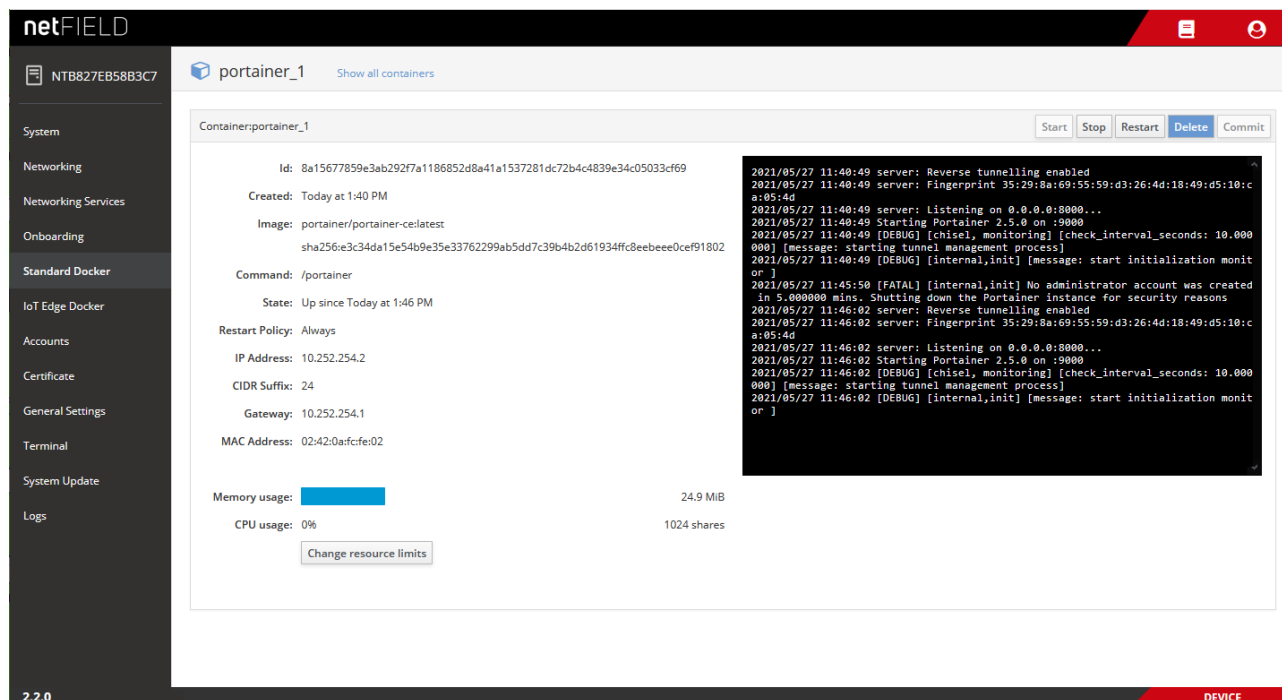


Figure 58: Container parameters with terminal window

- 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:

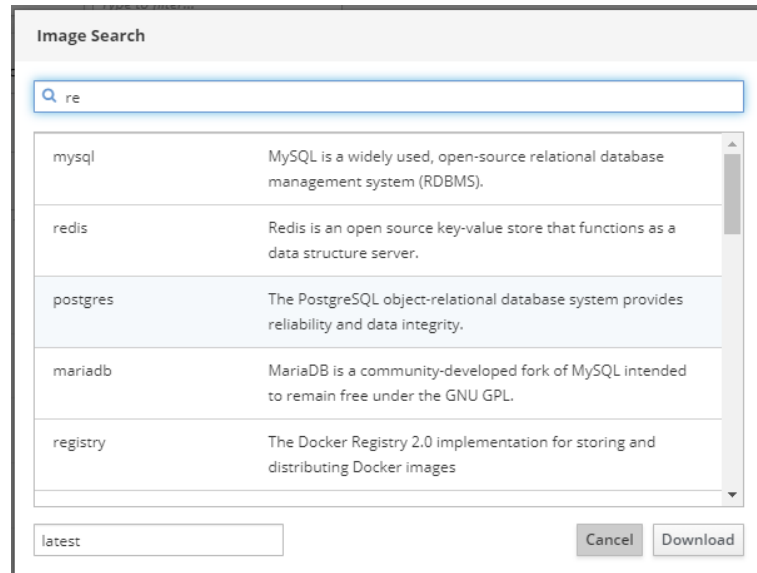

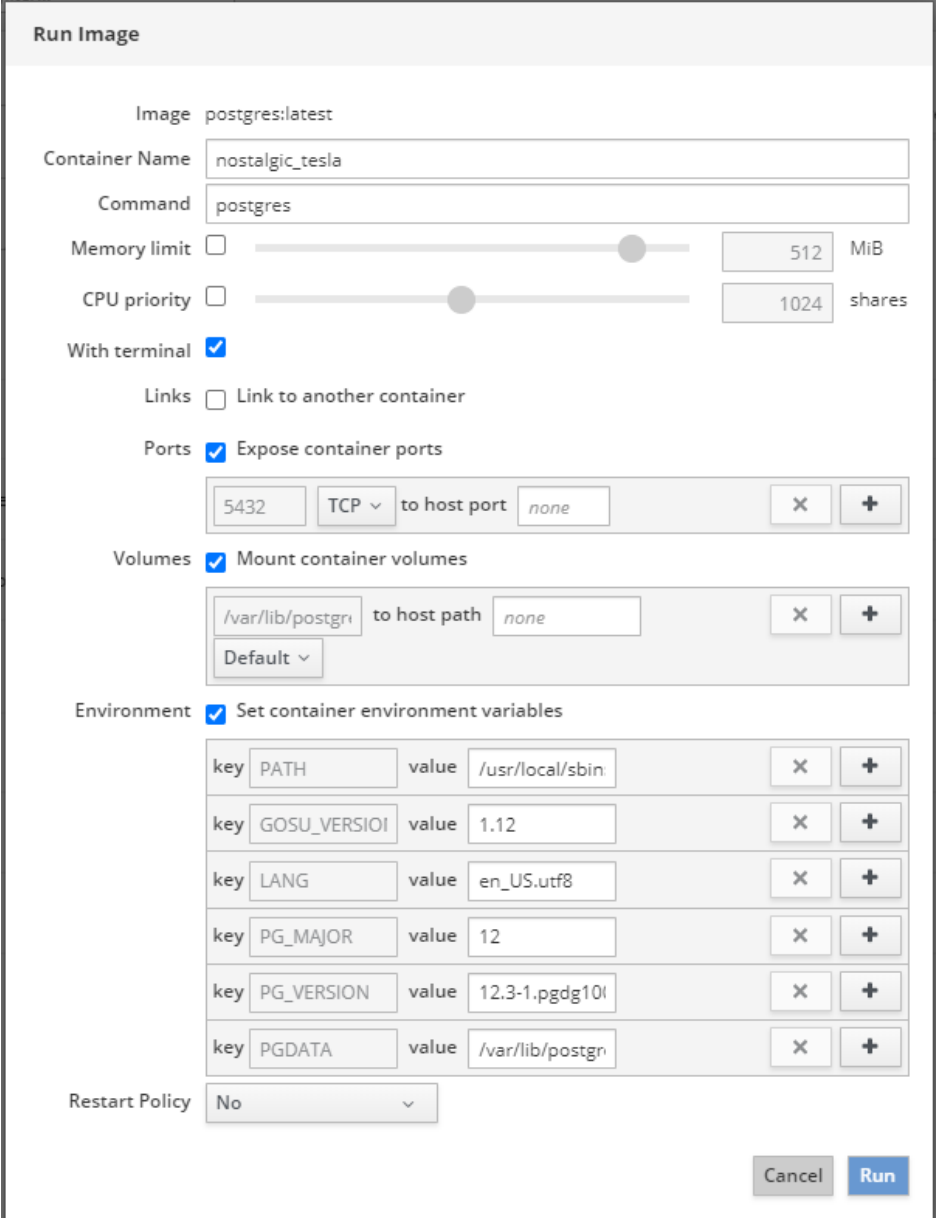


Figure 59: Image Search dialog of Standard Docker

- 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 includes 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	X	+
GOSU_VERSION	1.12	X	+
LANG	en_US.utf8	X	+
PG_MAJOR	12	X	+
PG_VERSION	12.3-1.pgdg10l	X	+
PGDATA	/var/lib/postgres	X	+
- Restart Policy:** No

Buttons: Cancel, Run

Figure 60: 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:

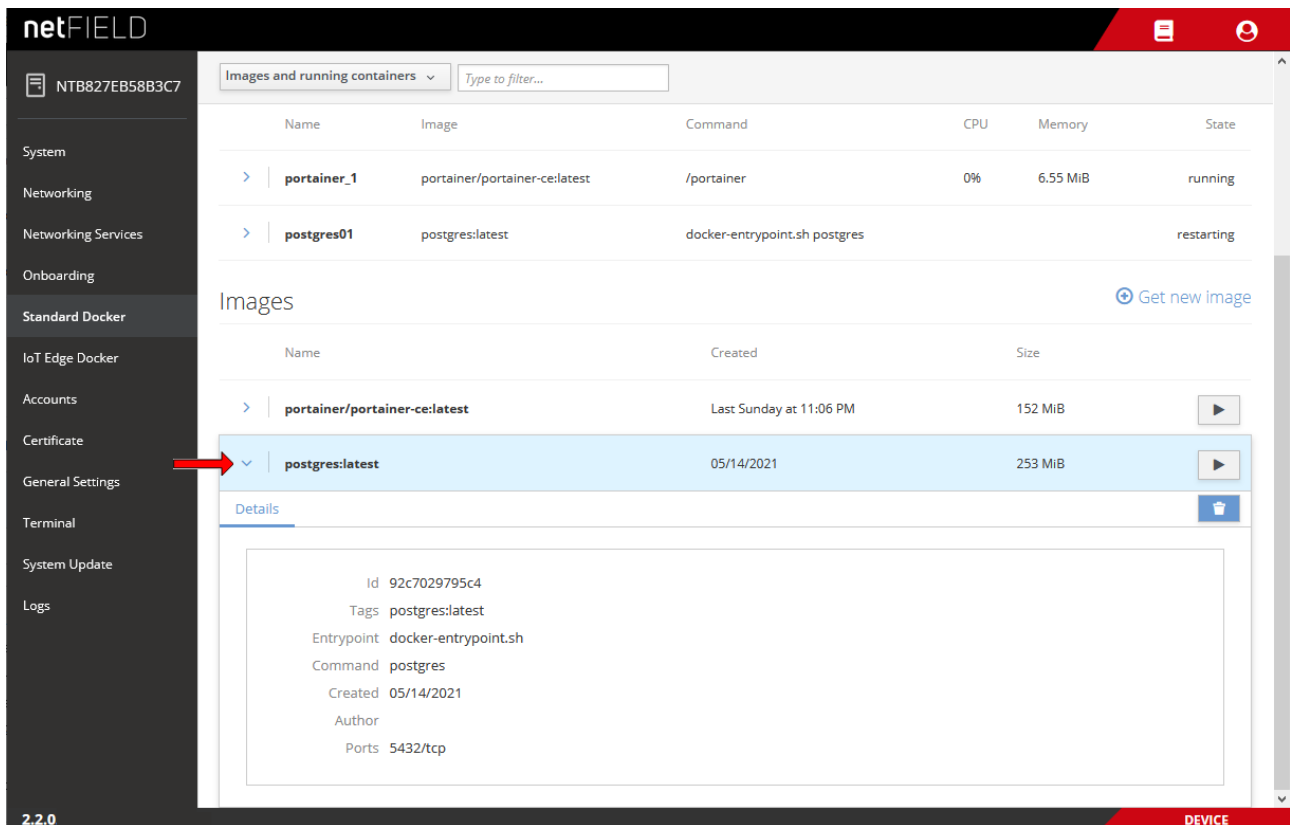


Figure 61: Expand image details

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

➤ A page featuring detailed information opens:

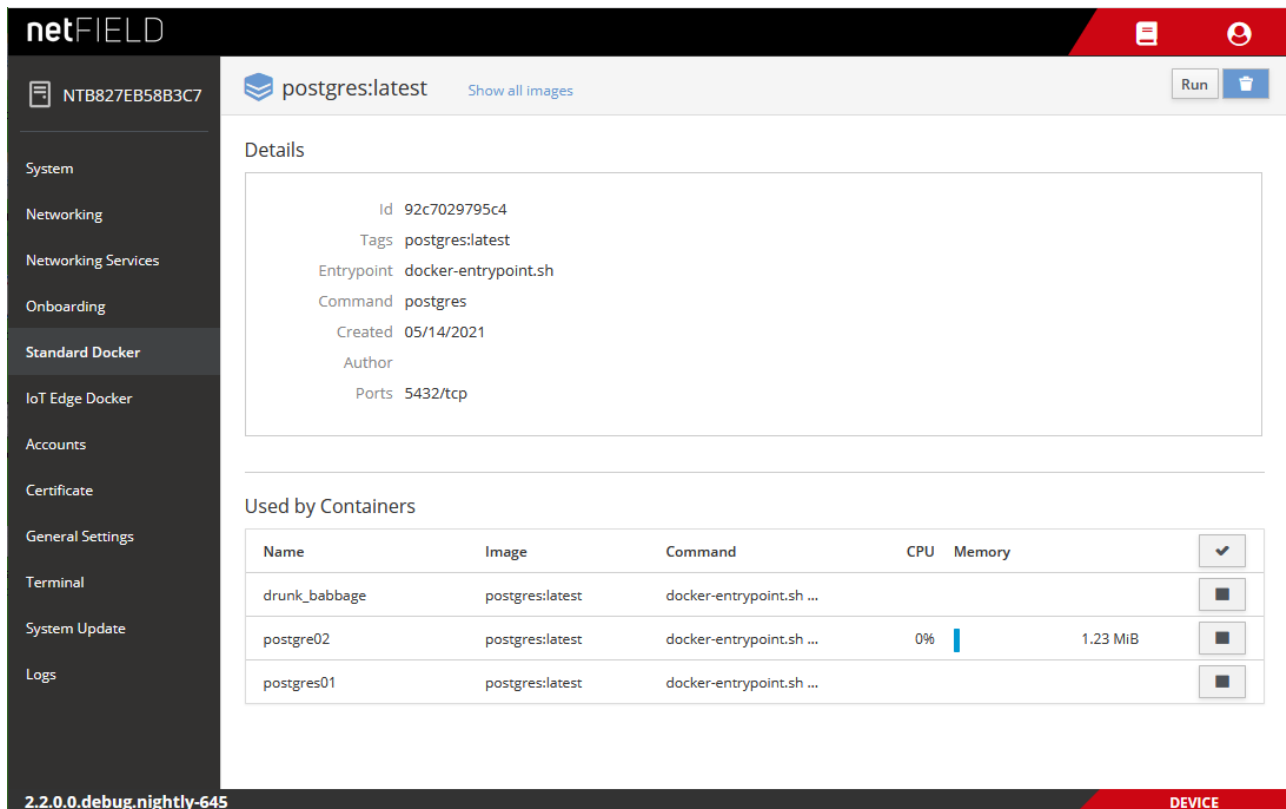





Figure 62: Image details

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 with the CLI in the **Terminal**. See section *Useful CLI commands and parameters in Terminal* [▶ page 122] for examples, e.g. for “Docker Compose” support.

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.

## 6.7 IoT Edge Docker

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

Note that you have to “onboard” your device (see section *"Onboard" (register) device in netFIELD Portal* [▶ page 30]) 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 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 84]).

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 105]).

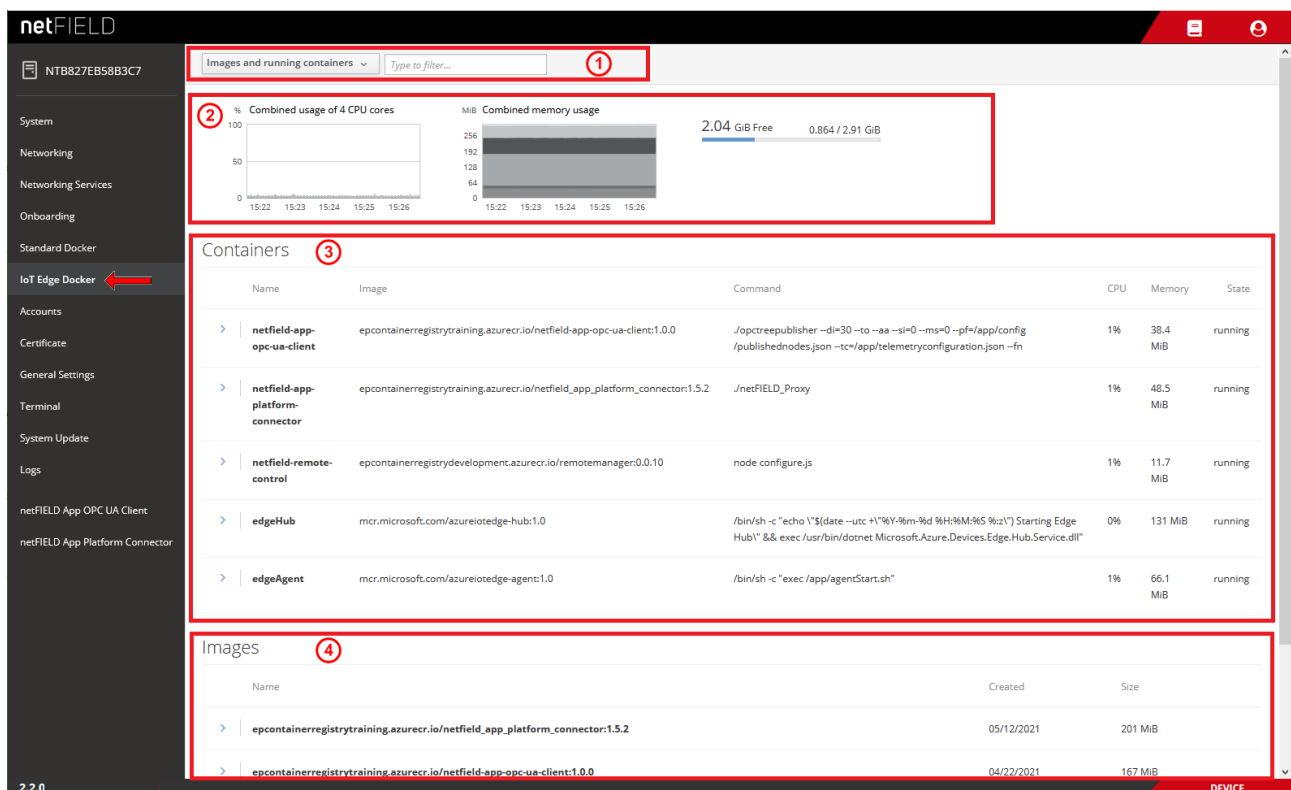


Figure 63: IOT Edge Docker

**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 Azure cloud (respectively to the netFIELD Portal).

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:

The screenshot shows the netFIELD web interface. On the left is a sidebar with navigation options: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, Logs, netFIELD App OPC UA Client, and netFIELD App Platform Connector. The main area is titled 'Images and running containers' with a filter input. It displays two graphs: '% Combined usage of 4 CPU cores' and 'MiB Combined memory usage'. Below these is a table of containers. The 'netfield-app-opc-ua-client' container is selected, and its details are expanded. The details show the container ID, creation time, image, command, and state. A 'Restart' button is visible next to the container name in the table.

Name	Image	Command	CPU	Memory	State
mosquitto	eclipse-mosquitto:1.6	/docker-entrypoint.sh /usr/sbin/mosquitto -c /mosquitto/config/mosquitto.conf	0%	2.31 MiB	running
netfield-app-opc-ua-client	epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0	/opctreepublisher --di=30 --to --aa --si=0 --ms=0 --pf=/app/config/publishednodes.json --tc=/app/telemetryconfiguration.json --fn	1%	63.1 MiB	running
netfield-app-platform-connector	epcontainerregistrytraining.azurecr.io/netfield_app_platform_connector:1.5.2	/netFIELD_Proxy	1%	42.8 MiB	running
netfield-remote-control	epcontainerregistrydevelopment.azurecr.io/remotemanager:0.0.10	node configure.js	2%	11.5 MiB	running
edgeHub	mcr.microsoft.com/azureiotedge-hub:1.0	/bin/sh -c "echo \"\$(date --utc +%Y-%m-%d %H:%M:%S %z)\"; Stapsio Edge Hub\" && exec /usr/bin/docker	0%	124 MiB	running

Figure 64: 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:

The screenshot shows the netFIELD IoT Edge Docker interface. On the left is a sidebar with navigation options: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker (selected), Accounts, Certificate, General Settings, Terminal, System Update, Logs, netFIELD App OPC UA Client, and netFIELD App Platform Connector. The main panel displays details for the container 'netfield-app-opc-ua-client'. It includes a 'Restart' button, a 'Show all containers' link, and a 'Container: netfield-app-opc-ua-client' header. Below this, various parameters are listed: Id, Created (Today at 3:07 PM), Image (epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0), Command (/optreepublisher --di=30 --to --aa --si=0 --ms=0 --pf=/app/config/publishednodes.json --tc=/app/telemetryconfiguration.json --fn), State (Up since Today at 3:07 PM), Restart Policy, IP Address, CIDR Suffix (0), Gateway, MAC Address, Volumes (/run/iotedge/workload.sock:/run/iotedge/workload.sock), Memory usage (61.9 MiB), and CPU usage (1% / 1024 shares). A 'Change resource limits' button is at the bottom. A console output window on the right shows error logs related to broker connections.

Figure 65: 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:

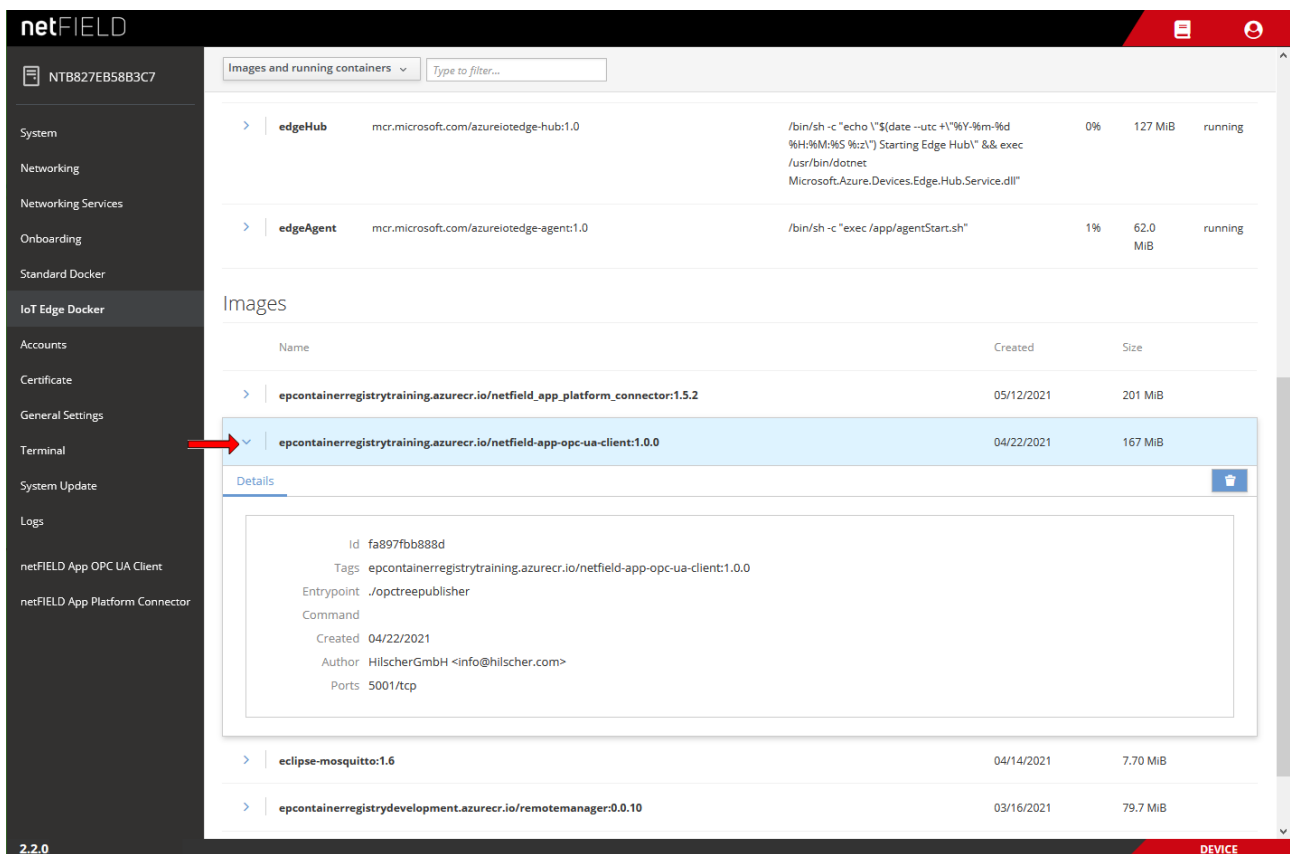


Figure 66: IoT image expanded

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

➤ A page featuring detailed information opens:

The screenshot shows the netFIELD IoT Edge Docker interface. On the left is a sidebar with navigation options: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker (selected), Accounts, Certificate, General Settings, Terminal, System Update, Logs, netFIELD App OPC UA Client, and netFIELD App Platform Connector. The main area displays details for the image 'epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0'. Below the details is a table titled 'Used by Containers' showing one container running on the image.

**Details:**

- Id: fa897fbb888d
- Tags: epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0
- Entrypoint: ./opctreepublisher
- Command: (empty)
- Created: 04/22/2021
- Author: HilscherGmbH <info@hilscher.com>
- Ports: 5001/tcp

**Used by Containers:**

Name	Image	Command	CPU	Memory
netfield-app-opc-ua-client	epcontainerregistrytrainin...	./opctreepublisher...	1%	63.2 MiB

Figure 67: 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 122] for examples.



## 6.8 Accounts

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

You can create new users and define passwords and access right (“roles”).

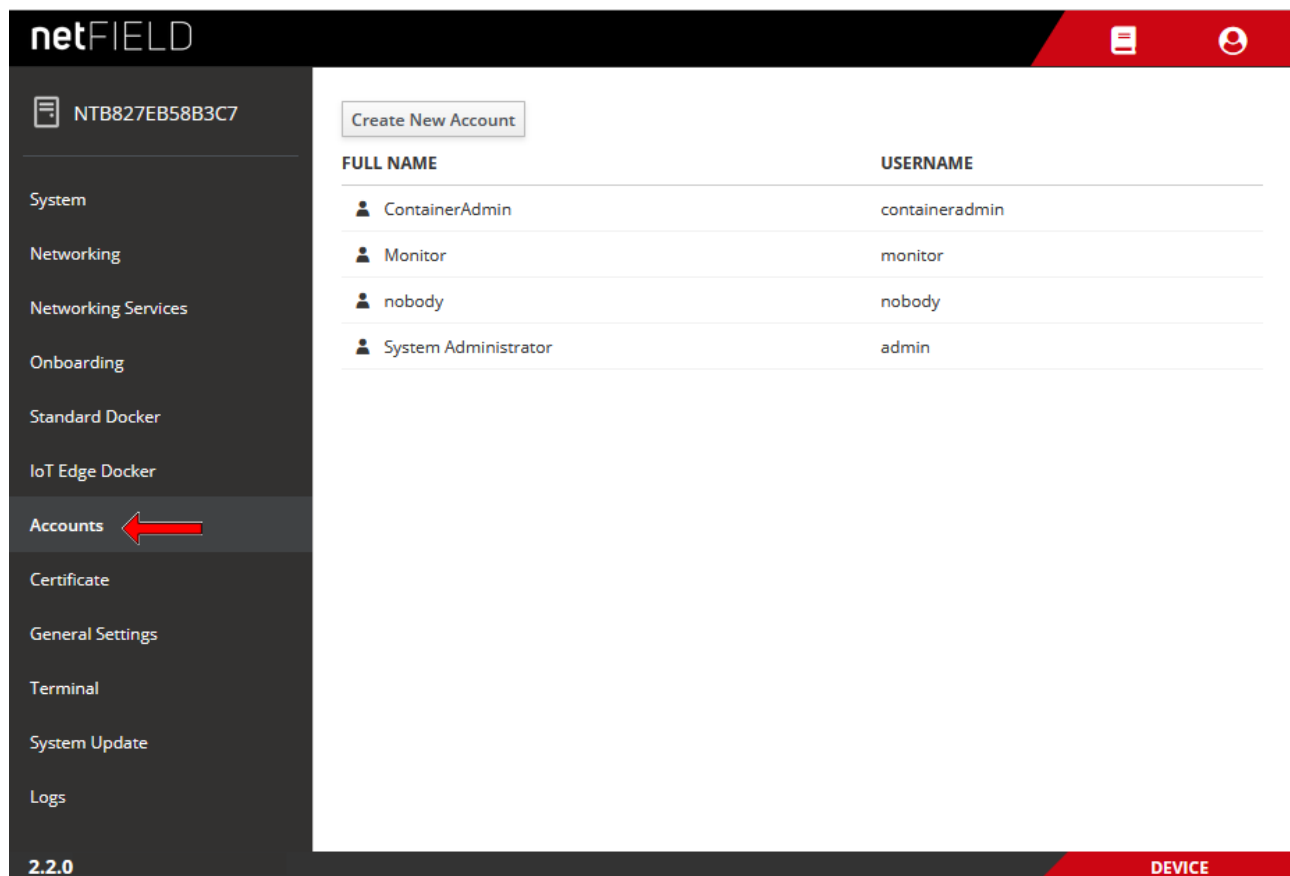


Figure 68: Accounts

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

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

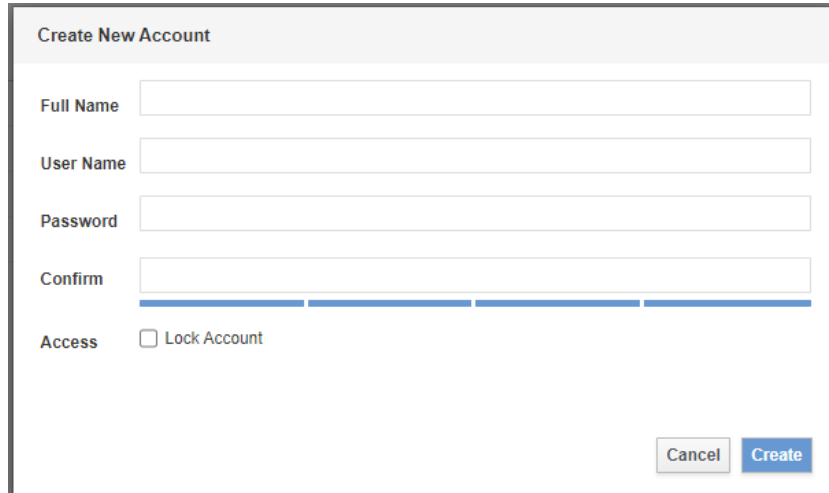
A dialog box titled "Create New Account" with a light gray header. It contains four text input fields: "Full Name", "User Name", "Password", and "Confirm". Below the "Confirm" field is a blue progress bar. At the bottom left, there is an "Access" section with a checkbox labeled "Lock Account". At the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

Figure 69: 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:

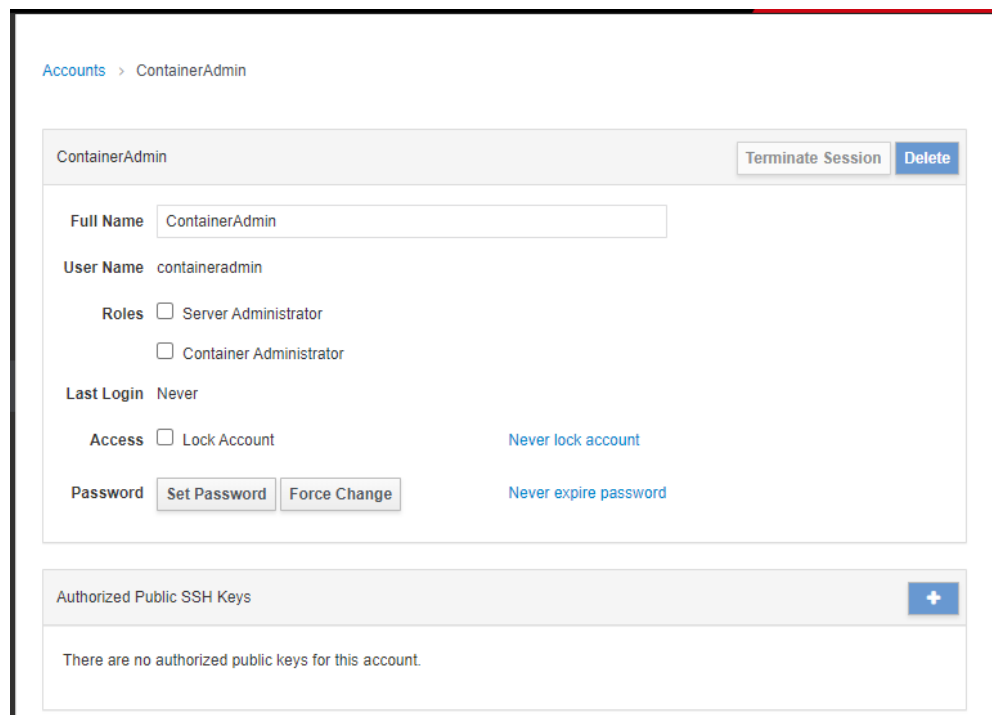

A configuration dialog for the "ContainerAdmin" account. The title bar shows "Accounts > ContainerAdmin". The main content area has a header "ContainerAdmin" with "Terminate Session" and "Delete" buttons. Below are fields for "Full Name" (ContainerAdmin), "User Name" (containeradmin), "Roles" (Server Administrator and Container Administrator checkboxes), "Last Login" (Never), "Access" (Lock Account checkbox), and "Password" (Set Password and Force Change buttons). To the right of the "Access" and "Password" sections are links: "Never lock account" and "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."

Figure 70: 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 (including Standard Docker and IoT Edge Docker).

The **Container Administrator** has access to the **Standard Docker** and **IoT Edge Docker**, but is otherwise not allowed to make any changes to the netFIELD OS settings.

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 device after it has been deleted in the *Device Manager of the Portal*. (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).

If you assign **neither role** to an account, the user has only “read” access to the netFIELD OS functions respectively to the host configuration.

Furthermore, a user without a role will have no access to the Standard Docker or to IoT Edge Docker (not even “read” access).

Note, however, that this user will have access to the plug-in dashboards of the netFIELD application containers in the Local Device Manager.

## Authorized Public SSH Keys

This area lists the SSH keys assigned to this account.

Click on the  button to add an SSH key.



### Note:

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.

## 6.9 Certificate

On the **Certificate** page, you can manage your web server certificate. 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.

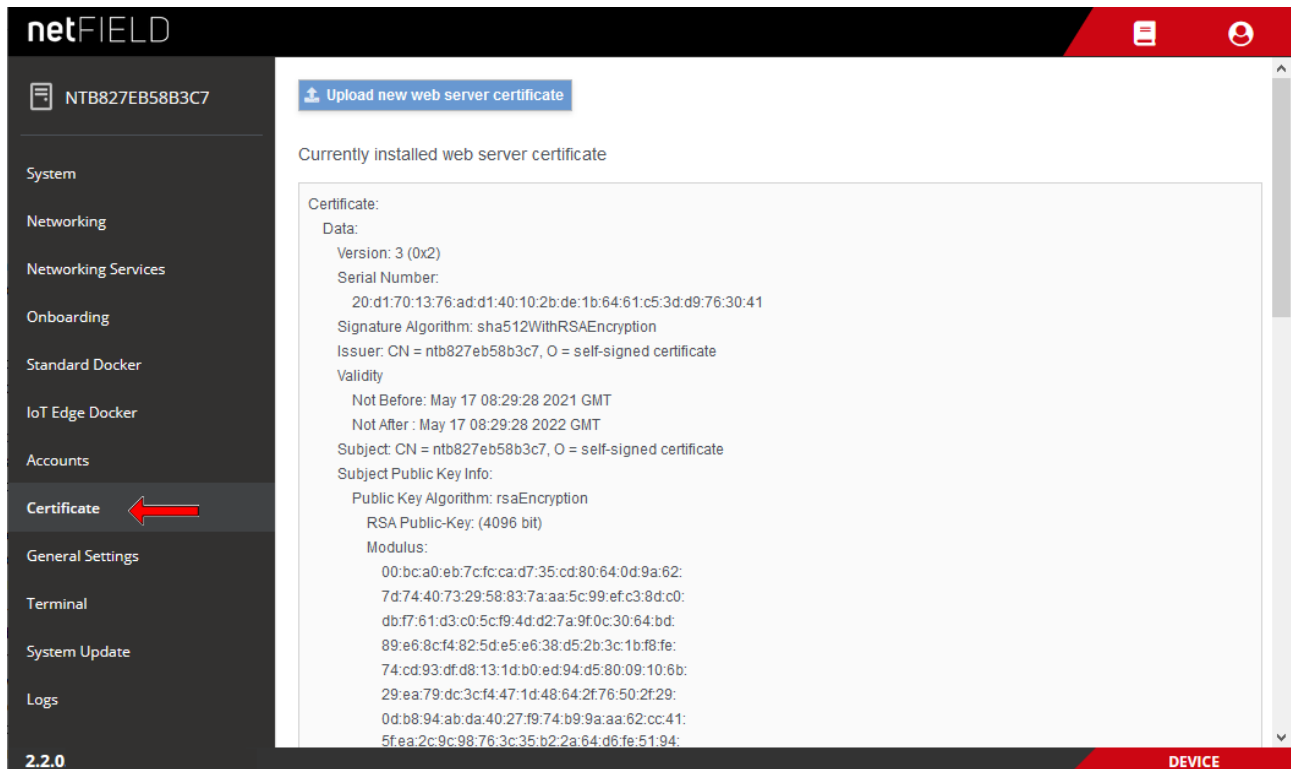


Figure 71: Web Server Certificate page



### 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.

## 6.10 General Settings

### 6.10.1 Overview

Under **General Settings** page, you can change various configuration settings of the netFIELD OS.

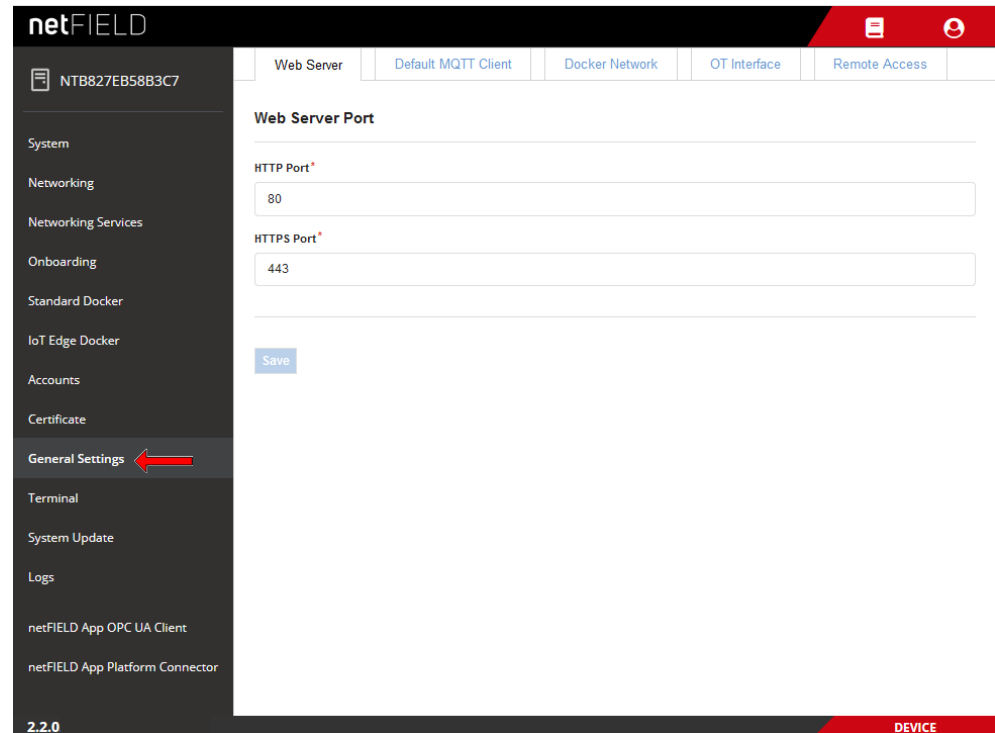


Figure 72: General Settings

## 6.10.2 Web Server (Port) Settings

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

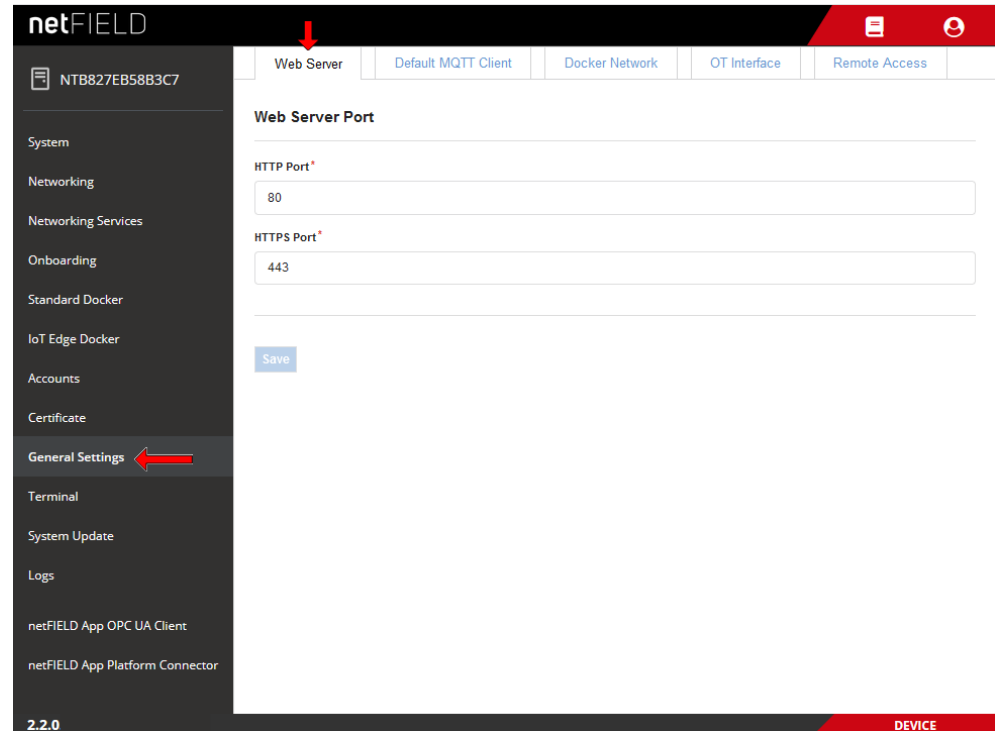


Figure 73: Web Server Settings tab

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, DOC1907010IxxEN.

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

### 6.10.3 Default MQTT Client Settings

In this tab, 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, DOC1907010IxxEN).

The screenshot displays the netFIELD web interface for configuring the Default MQTT Client. The sidebar on the left lists various system settings, with 'General Settings' highlighted by a red arrow. The main content area, titled 'Default MQTT Client', is divided into several sections:

- Gateway settings**: Includes a 'Gateway prefix' field with the value '000000000000-00001b58b3c7'.
- Basic**: Includes a 'MQTT Version' dropdown set to '3.1', a 'Keep Alive Interval (Seconds)' field set to '60', a 'Username' field with the placeholder 'Username', and a 'Password' field with the placeholder 'Password'.
- Connect Timeout (Seconds)**: A field set to '300'.
- Clean Session**: A checkbox that is checked.
- Server URIs**: A section with a plus icon to add new URIs.

At the bottom of the sidebar, the version '2.2.0' is displayed. The bottom right corner of the interface shows the word 'DEVICE'.

Figure 74: 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 Mosquitto Broker 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 Mosquitto Broker 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 Mosquitto Broker 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 24: Default MQTT Client Settings

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



## 6.10.4 Docker Network Settings

On this tab, you can change the network address settings of the Standard Docker and of the IoT Edge Docker.



### 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.

The screenshot displays the netFIELD Docker Network Settings interface. The left sidebar contains a menu with items: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings (highlighted with a red arrow), Terminal, System Update, Logs, netFIELD App OPC UA Client, and netFIELD App Platform Connector. The main content area has tabs for Web Server, Default MQTT Client, Docker Network (selected), OT Interface, and Remote Access. The Docker Network tab is divided into two sections: Standard Docker and IoT Edge Docker. Each section contains fields for Bridge IP and CIDR Suffix or Netmask, and a table for Default address pools. The Standard Docker section shows a Bridge IP of 10.252.254.1 and a CIDR Suffix or Netmask of 24. The IoT Edge Docker section shows a Bridge IP of 10.252.253.1 and a CIDR Suffix or Netmask of 24. Both sections have a table for Default address pools with columns for IP Address, CIDR Suffix or Netmask, Network Size, and Action. The Standard Docker table has one entry with IP Address 10.254.0.1, CIDR Suffix or Netmask 16, and Network Size 24. The IoT Edge Docker table has one entry with IP Address 10.253.0.1, CIDR Suffix or Netmask 16, and Network Size 24. A red arrow points to the 'General Settings' menu item in the sidebar.

Figure 75: Docker Network Settings

## Standard Docker

The **docker0** bridge is a virtual 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.

All containers running on the Standard Docker connect 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.



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 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	
Default address pools	Here you can define "reserve" address pools (subnets) for the internal Docker bridge networks. The default pool consisting of the IP address/CIDR Suffix 10.254.0.1/16 with network size 24 means that the first additional Docker 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 of the internal Docker bridge network.
	CIDR Suffix or Netmask	Subnet mask of the internal Docker bridge network as CIDR Suffix or in "dotted decimal notation".
	Network Size	Number of bits used as the netmask for further Docker bridge networks.
	Action	<div>  Opens a dialog for adding a new pool of reserved addresses. </div> <div>  Deletes the address pool. </div>

Table 25: Standard Docker Network Settings

## IoT Edge Docker

The **iotedge0** bridge is a virtual 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.

All containers running on the IoT Edge Docker connect to this **iotedge0** bridge by default. 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.

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 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								
Default address pools	Here you can define “reserve” address pools (subnets) for the internal IoT Edge Docker bridge networks. The default pool consisting of the IP address/CIDR Suffix 10.253.0.1/16 with network size 24 means that the first additional IoT Edge Docker 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.								
	<table> <tr> <td>IP address</td><td>Reserved IP address of the internal IoT Edge Docker bridge network.</td></tr> <tr> <td>CIDR Suffix or Netmask</td><td>Subnet mask of the internal IoT Edge Docker bridge network as CIDR Suffix or in “dotted decimal notation”.</td></tr> <tr> <td>Network Size</td><td>Number of bits used as the netmask for further IoT Edge Docker bridge network.</td></tr> <tr> <td>Action</td><td> <div>+</div> Opens a dialog for adding a new pool of reserved addresses. <div>🗑️</div> Deletes the address pool. </td></tr> </table>	IP address	Reserved IP address of the internal IoT Edge Docker bridge network.	CIDR Suffix or Netmask	Subnet mask of the internal IoT Edge Docker bridge network as CIDR Suffix or in “dotted decimal notation”.	Network Size	Number of bits used as the netmask for further IoT Edge Docker bridge network.	Action	<div>+</div> Opens a dialog for adding a new pool of reserved addresses. <div>🗑️</div> Deletes the address pool.
IP address	Reserved IP address of the internal IoT Edge Docker bridge network.								
CIDR Suffix or Netmask	Subnet mask of the internal IoT Edge Docker bridge network as CIDR Suffix or in “dotted decimal notation”.								
Network Size	Number of bits used as the netmask for further IoT Edge Docker bridge network.								
Action	<div>+</div> Opens a dialog for adding a new pool of reserved addresses. <div>🗑️</div> Deletes the address pool.								

Table 26: Standard Docker Network Settings

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

The following pictures illustrates the default Docker network configuration:

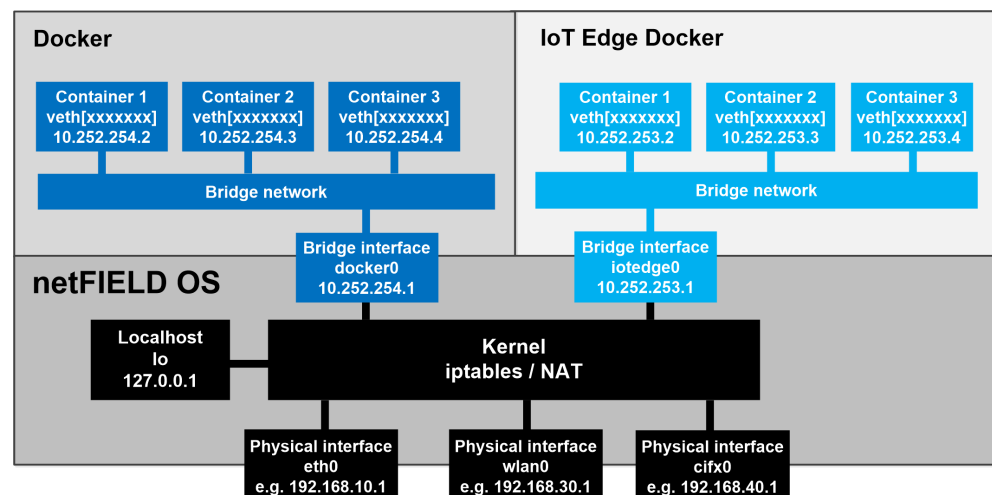


Figure 76: Default docker network configuration

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

On the **OT Interface** tab, 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 (9) and (10) in section *Positions of the interfaces* [▶ page 14]) 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 interface 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 **ERR/NS** LED (see position (4) in section *Positions of the interfaces* [▶ page 14]) to show steady red light.

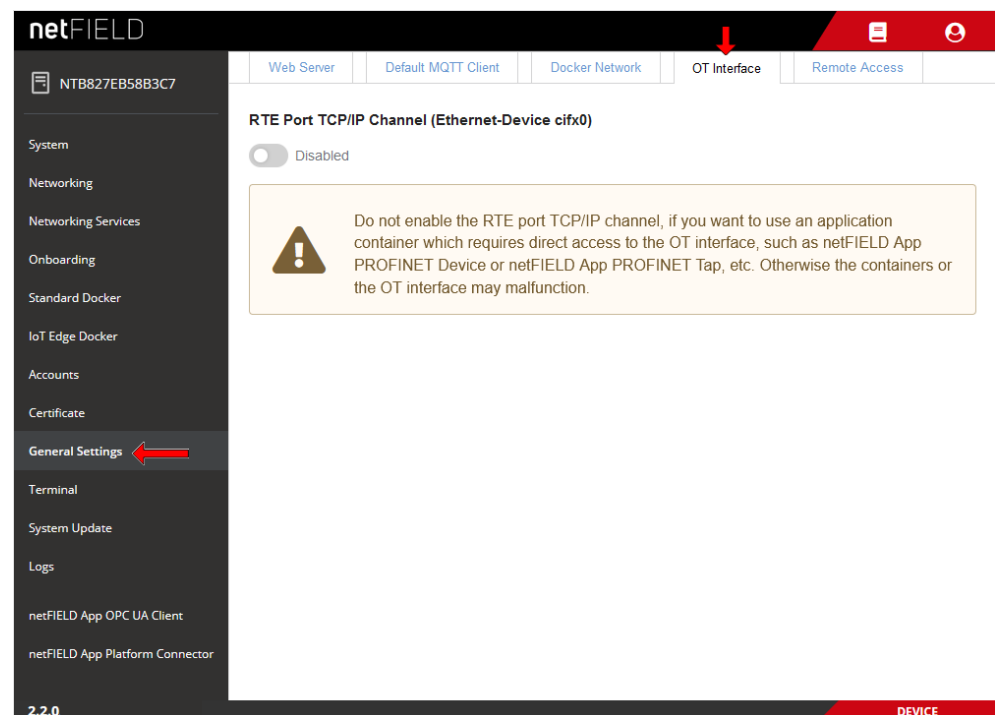


Figure 77: OT interface

**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.

## 6.10.6 Remote Access

On this tab you can enable (on) or disable (off) *Remote Control* access from the netFIELD Portal to your device respectively to your netFIELD OS Datacenter.

For security reasons, remote control access is by default switched off. To allow remote control for 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, DOC1907010IxxEN).

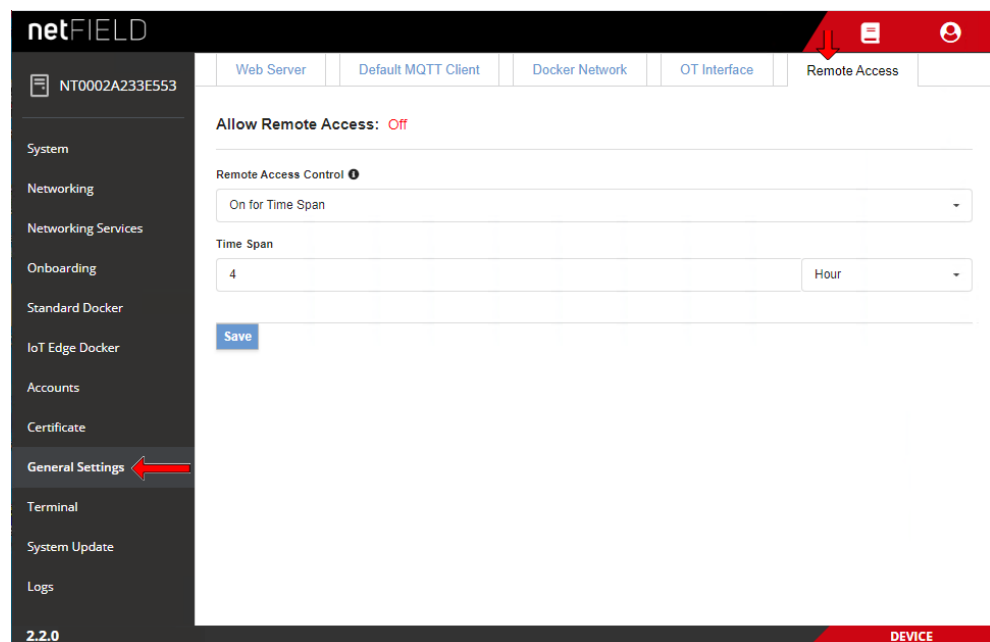


Figure 78: Remote Access tab

- 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**.

## 6.11 Terminal

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

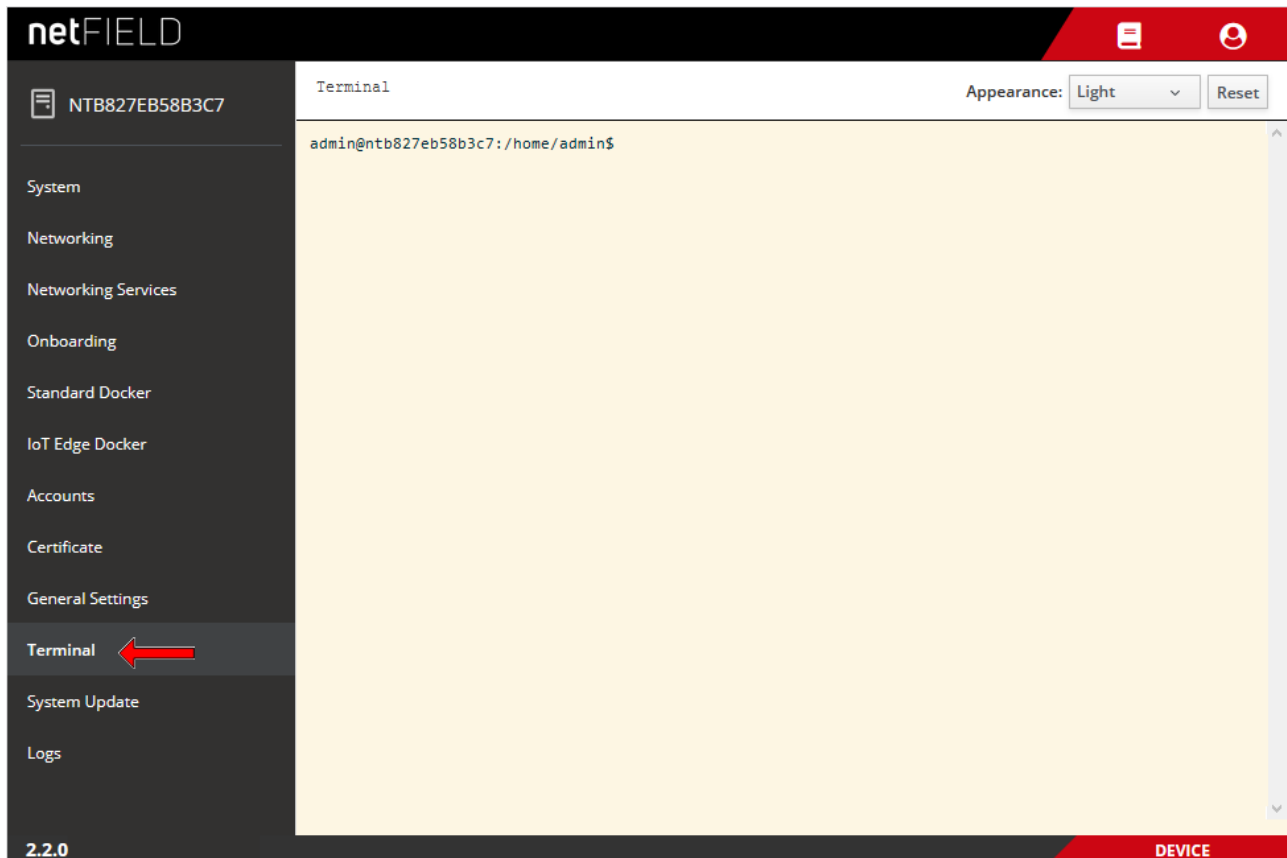


Figure 79: Terminal



**Note:**

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

Note that in order to work with root privileges in the CLI, “sudo” has to be used.

Examples of commands and parameters are provided in section *Useful CLI commands and parameters in Terminal* [► page 122].



## 6.12 System Update

You can update the netFIELD operating system (netFIELD OS) by simply uploading an `swu` update file on the **System Update** page of the Local Device Manager.

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 will be fully replaced by the new recovery image. This restores the “factory settings” of the device, which means that individual configurations settings, containers, user accounts and passwords will be lost. Therefore, you will have to reconfigure and “onboard” your device again after a *recovery*.

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.

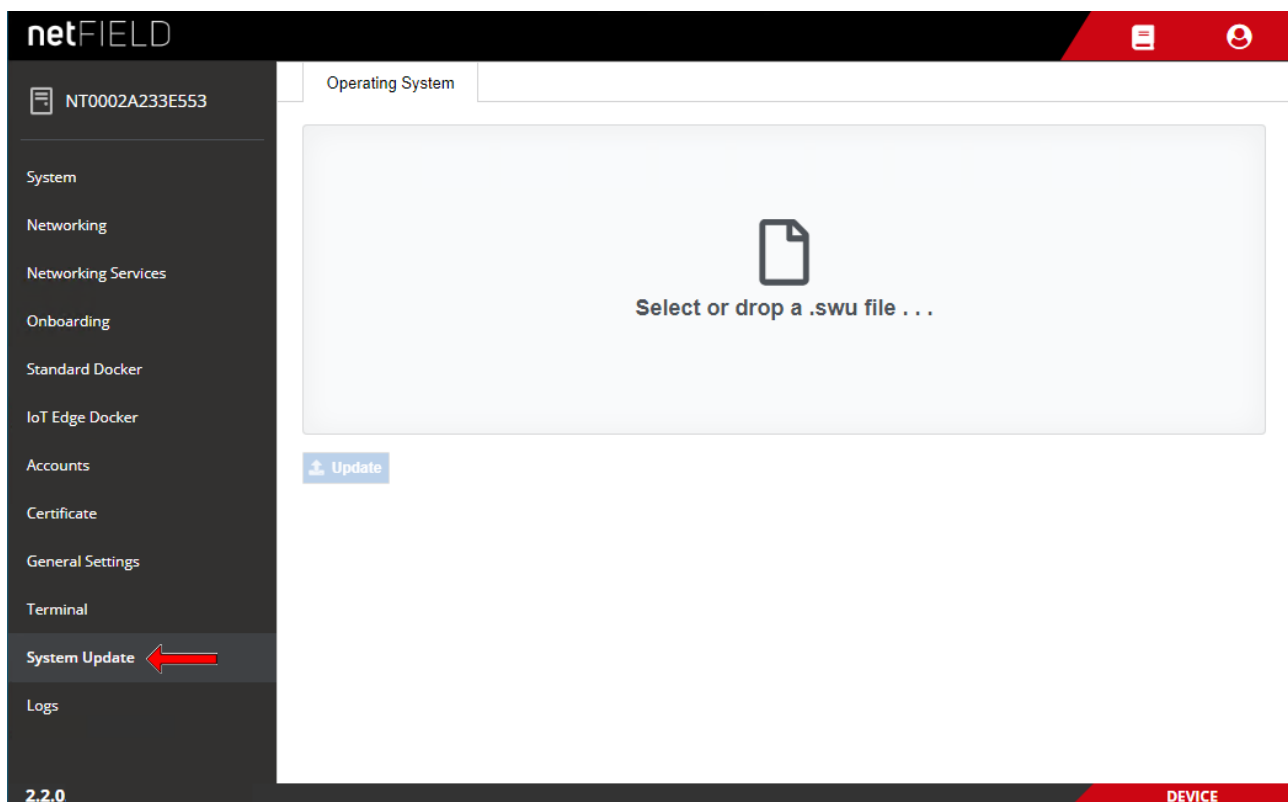


Figure 80: OS update page

**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 Software Overview* page <https://kb.hilscher.com/x/sSAfBw> and navigate to the latest netFIELD OS version for the netFIELD Connect device. In the *Software* table, go to the *Update via local Device Manager* entry and download the `niot-e-tpi51-en-re-2.x.x.x.release-update.swu` file. (If you want to perform a "recovery", go to the *Recovery (factory reset) via local Device Manager* entry and download the `niot-e-tpi51-en-re-2.x.x.x.release-recovery.swu` file.)
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.

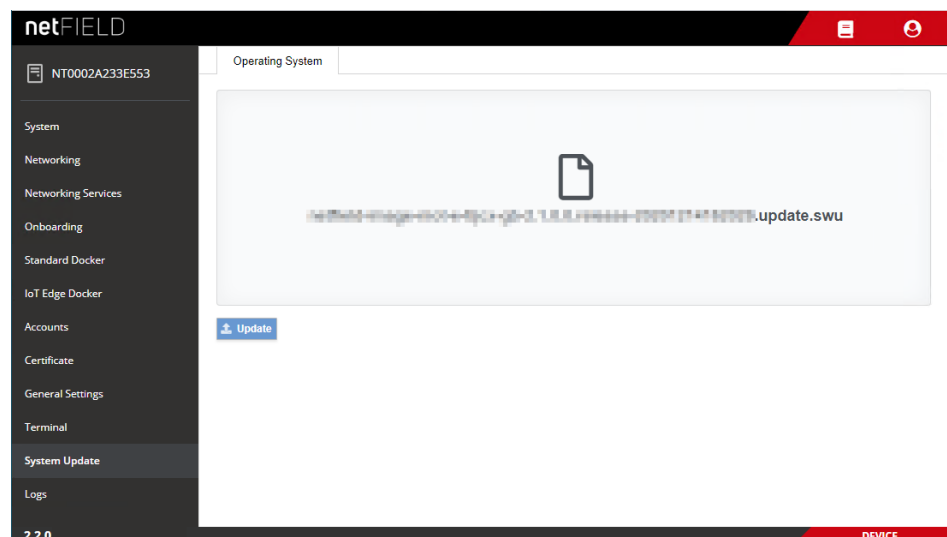


Figure 81: Selected OS update image

- 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:

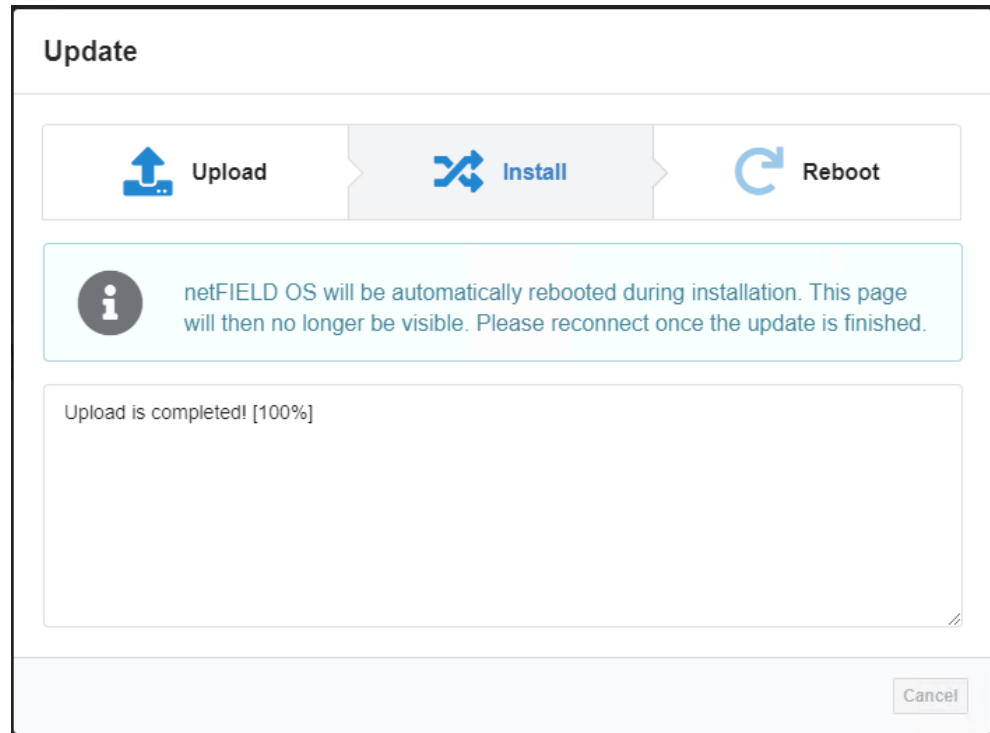


Figure 82: Upload finished message



**Note:**

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

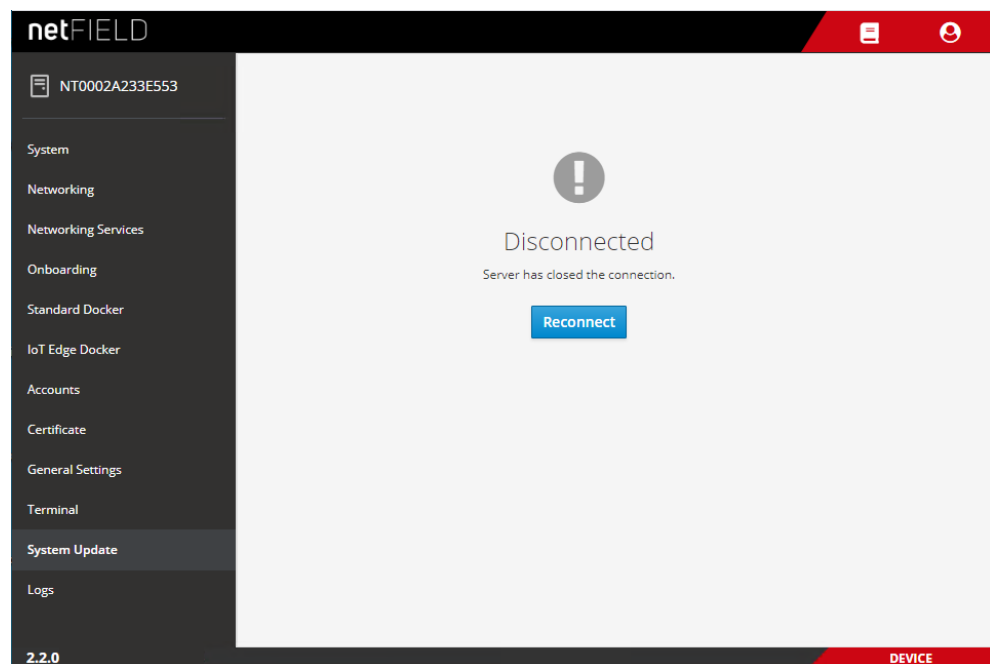


Figure 83: OS update “Disconnected” message

- 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.



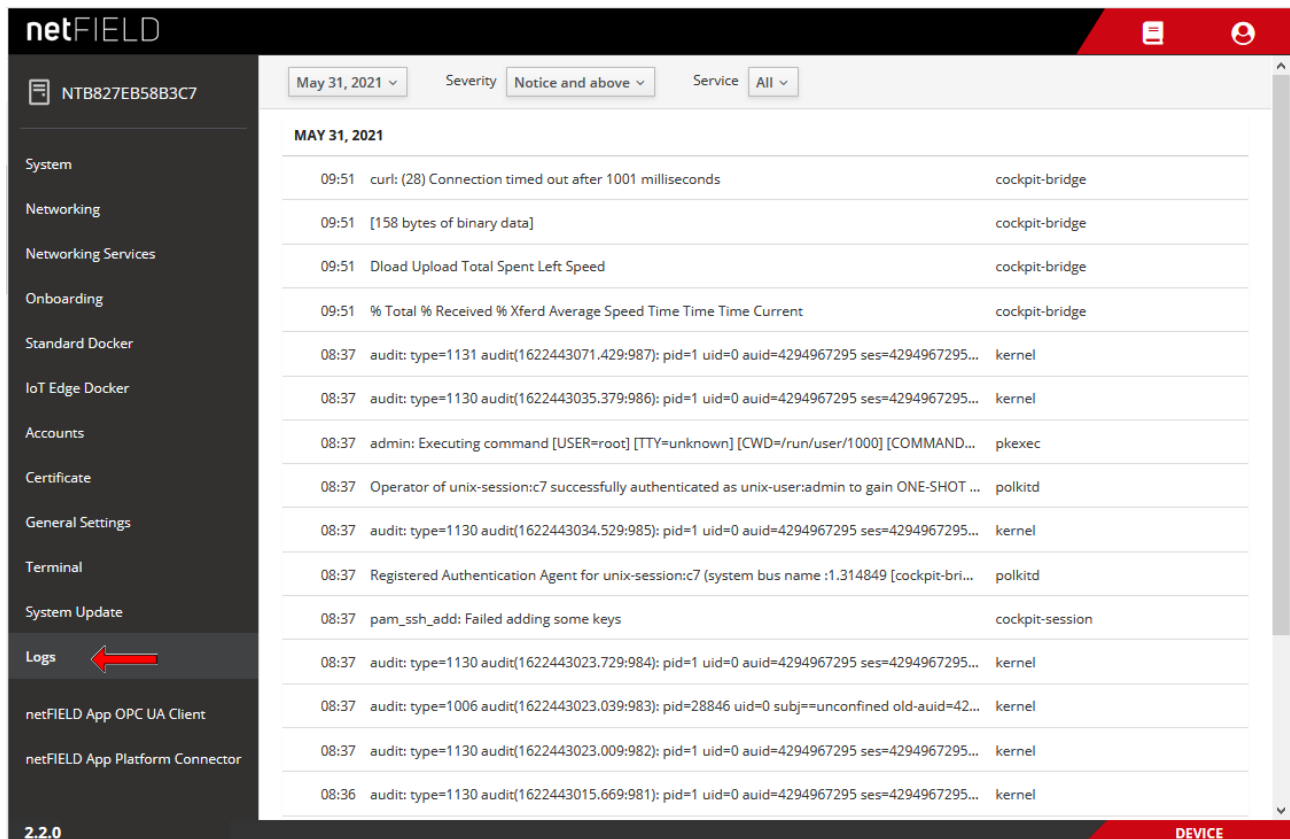
**Note:**

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 21]).

## 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 is a dark sidebar with a menu. The 'Logs' option is highlighted with a red arrow. The main area displays log messages for May 31, 2021. At the top of the main area are filters for date (May 31, 2021), severity (Notice and above), and service (All). The log messages are listed in a table with columns for time, message content, and service.

Time	Message	Service
09:51	curl: (28) Connection timed out after 1001 milliseconds	cockpit-bridge
09:51	[158 bytes of binary data]	cockpit-bridge
09:51	Dload Upload Total Spent Left Speed	cockpit-bridge
09:51	% Total % Received % Xferd Average Speed Time Time Time Current	cockpit-bridge
08:37	audit: type=1131 audit(1622443071.429:987): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel
08:37	audit: type=1130 audit(1622443035.379:986): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel
08:37	admin: Executing command [USER=root] [TTY=unknown] [CWD=/run/user/1000] [COMMAND=...]	pkexec
08:37	Operator of unix-session:c7 successfully authenticated as unix-user:admin to gain ONE-SHOT ...	polkitd
08:37	audit: type=1130 audit(1622443034.529:985): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel
08:37	Registered Authentication Agent for unix-session:c7 (system bus name :1.314849 [cockpit-bri...]	polkitd
08:37	pam_ssh_add: Failed adding some keys	cockpit-session
08:37	audit: type=1130 audit(1622443023.729:984): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel
08:37	audit: type=1006 audit(1622443023.039:983): pid=28846 uid=0 subj==unconfined old-auid=42...	kernel
08:37	audit: type=1130 audit(1622443023.009:982): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel
08:36	audit: type=1130 audit(1622443015.669:981): pid=1 uid=0 auid=4294967295 ses=4294967295...	kernel

Figure 84: Logs

## 7 Good to know...

### 7.1 Device recovery via USB

#### 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 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.

#### 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.

- You have downloaded the recovery image from Hilscher to your local PC (see below for instructions).
- You have physical access to the device (in order to plug-in the USB stick).

### 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 Software Overview* page <https://kb.hilscher.com/x/sSAfBw>, navigate to the latest netFIELD OS version for the netFIELD Connect device, then to the *Recovery (factory reset) via USB memory stick* section and download the `niot-e-tpi51-en-re-2.x.x.x.release-recovery.zip`.
  - Unpack the downloaded zip archive on your local PC.
  - The unpacked `niot-e-tpi51-en-re-2.x.x.x.release-recovery` folder contains the following files, which you will later have to copy to the USB stick (after having formatted the stick):

- boot-fit
- firmware
- fitImage
- VERSION

2. Format and rename USB stick.
  - Connect the USB stick to your Windows PC.
  - Open the Windows Explorer.
  - Select the USB stick and choose **Format...** from the context menu.

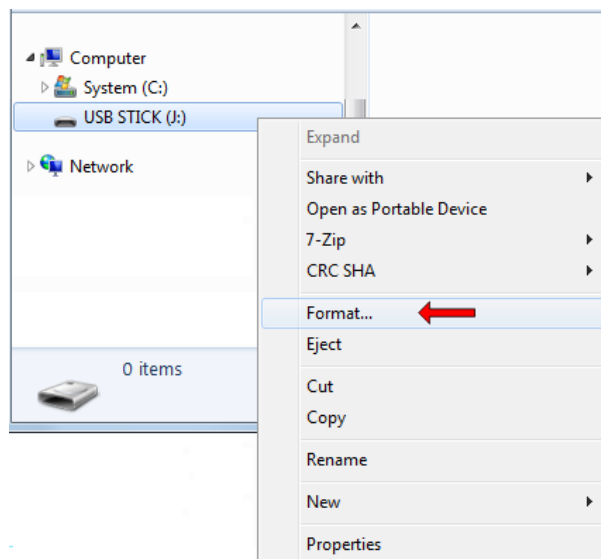


Figure 85: Formatting USB stick

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

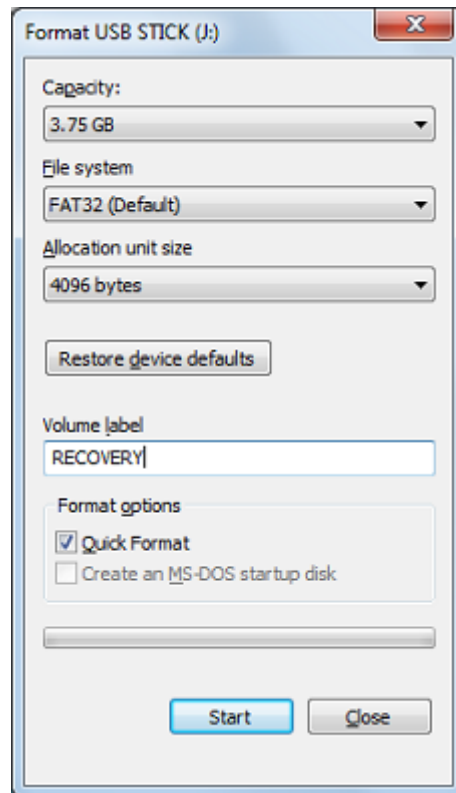


Figure 86: Format USB STICK dialog window

- 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".

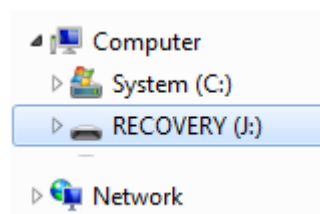


Figure 87: Formatted USB stick



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

- Open the `niot-e-tpi51-en-re-2.x.x.x.release-recovery` folder and copy the `boot-fit`, `firmware`, `fitImage` and `VERSION` files onto the USB stick.
- ⇒ The USB stick with the copied recovery image files must now feature the following elements:

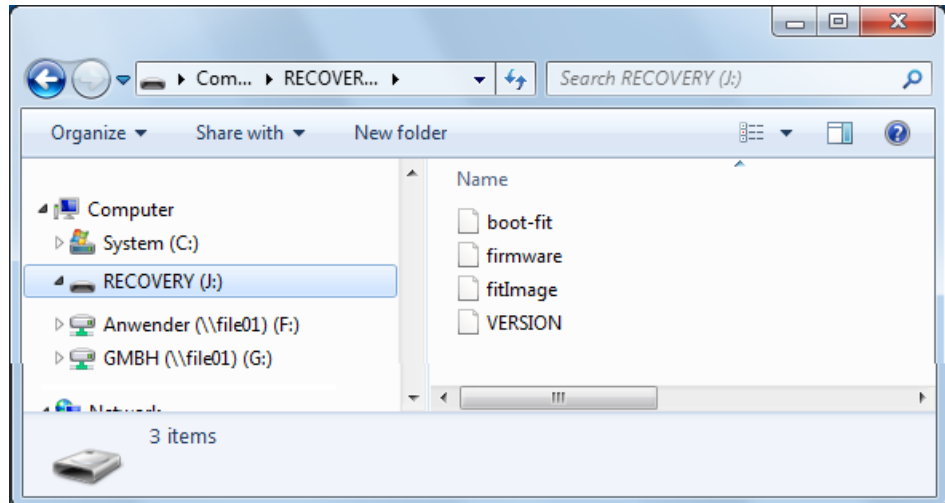


Figure 88: Recovery image on USB stick

- Remove the USB stick from your Windows PC.
- ### 4. Start recovery.
- Plug the prepared USB stick into one of the USB sockets of the device.
  - Start a hardware power cycle by briefly removing the voltage supply.
  - ⇒ The device restarts and boots from the connected USB stick (this is the default BIOS boot setting). It then installs the new netFIELD OS from the USB stick. This might take a few minutes. The installation process is indicated by a flickering ACT LED. After the installation is finished, the ACT LED briefly lights up and then eventually goes off.
  - Wait until the ACT LED is off, then remove the USB stick, then start a new power cycle by briefly removing the voltage supply.
  - ⇒ You have finished the netFIELD OS recovery procedure. The device is reset to its factory settings (LAN interface is enabled and set to DHCP, default administrator password is set to `admin`). You can now reconnect to the device as described in chapter *Commissioning and first steps* [▶ page 21].

## 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>
```

#### Example

To show the version of Docker Compose:

```
docker-compose version
```

### 7.2.5 Manage Standard Docker

```
docker <docker commands>
```

#### Example

To list all created containers for the Standard Docker instance:

```
docker ps -a
```

### 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	1321.400/NFLD
	Product name	NIOT-E-TPI51-EN-RE/NFLD
	Application	IT/OT Edge device for IoT, Industry 4.0, Integrated Industry and Automation projects
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	Bootling of signed software
	Access	HTTPS, TLS
Processors	CPU	Broadcom BCM2837 1.2 GHz, 64 bit, 4 cores
	Communication controller	netX 51
Software	Operating system	netFIELD OS, based on Security Enhanced Linux
Memory	RAM	1 GB DDR3 RAM
	SD card	NIOT-E-TPI51-EN-RE/NFLD: 8 GB MLC NAND Micro SD card, 384 TBW (Terabytes Written)
		NIOT-E-TPI51-EN-RE\32HE/NFLD: 32 GB SLC Micro SD card, 1920 TBW (Terabytes Written)
Power	Voltage	24 V DC $\pm$ 6 V DC For UL conform usage: powered by class 2 source, Overvoltage Category II
	Current (at 24 V DC)	Without USB: 170 mA (typical) With USB: max. 400 mA Important: Maximum load over all four USB ports is 1 A
	Power of the used power supply unit	Min. 4.2 W (no USB) 9 W (USB with 1 A)
	Connector	3-pin terminal block (3.5 mm)
IT interface	Interface type	1 x 10/100 Mbit, Microchip LAN9514
	LAN connector	1 x RJ45 socket
OT interface	Interface type	10BASE-T/100BASE-TX, potential free, Hilscher netX 51
	Connector	2 x RJ45 socket
	Supported protocols	PROFINET IO Device, EtherNet/IP Adapter, EtherCAT Slave, Standard TCP/IP (limited throughput).
Additional interfaces	USB	4 x USB 2.0, max. 500 mA max. 1 A over all USBs, Type A
	Wi-Fi	1 x Wi-Fi, single band 2.4 GHz IEEE 802.11n (BCM43438), fixed antenna.
	Bluetooth	BT 4.1 Inactive by default, can be activated by software.
	Display connector	1 x HDMI Inactive by default, can be activated by software.
	Communication module interface	Slot for NPIX Extension Modules
Display	LED indicators	8 LEDs (2 programmable)
Real-time clock	Buffering	Capacitor buffered, max. 7 days backup, maintenance free

Category	Parameter/item	Value/description
Environment	Ambient temperature range for operation	-20°C ... +60°C
	Ambient temperature range for storage	-40°C ... +85°C
	Humidity range	10 % ... 95 % (95 % at 40°C) relative humidity (non-condensing)
	Pollution degree	For UL compliant usage: The device must be used in a pollution degree 2 environment.
	Altitude	Max. 2000 m
	Use	Indoor use
Device	Dimensions	140 mm (H) x 35 mm (W) x 105 mm (L)
	Weight	400 g
	Housing	Metal
	Mounting	DIN top hat rail
	Degree of protection	IP20
Approvals	FCC ID (Federal Communications Commission)	2ANEG0001
	IC (Industry Canada)	24152-0001
UL certification	UL-File-Nr	E221530 Vol D1
Conformity	Wi-Fi / Bluetooth	EN 300 328 V2.2.2
	RoHS	Yes
Conformance with EMC directives	CE sign	Yes
	Emission	EN 55011:2009
	Immunity	IEC 61000-6-2/3, EN 61131-2
	Electrostatic discharge (ESD) (air and contact discharge method)	EN 61000-4-2
	Fast transient interferences (Burst)	EN 61000-4-4
	Surge voltage	EN 61000-4-5
Mechanical tests	Shock	IEC 60068-2-27 Ea
	Vibration	IEC 60068-2-6 Fc

Table 27: Technical data netFIELD Connect (NIOT-E-TPI51-EN-RE/NFLD)

## 9 Decommissioning, dismantling 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 DIN top hat rail.
- 

### 9.2 Removing device from top hat rail

- Before dismantling the device from the top hat rail, first remove the power supply cable and all data cables from the device.
- Put a screwdriver into the slot of the latch at the bottom of the device.
- To disengage the lock of the hook, pull down the latch with the screwdriver.
- Take the device off the top hat rail.

### 9.3 Disposal of waste electronic equipment

Important notes from the European Directive 2012/16/EU "Waste Electrical and Electronic Equipment (WEEE)"



---

**Waste electronic equipment**

This product must not be treated as household waste.

This product must be disposed of at a designated waste electronic equipment collecting point.

---

Waste electronic equipment may not be disposed of as household waste. As a consumer, you are legally obliged to dispose of all waste electronic equipment according to national and local regulations.

## 10 Appendix

### 10.1 Approvals

#### 10.1.1 Federal Communications Commission (FCC)

**FCC ID: 2ANEG0001**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

*Figure 89: FCC label*

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## 10.1.2 Industry Canada (IC)

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference. (2) This device must accept any interference, including interference that may cause undesired operation of the device.

L'émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) L'appareil ne doit pas produire de brouillage; (2) L'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Cet équipement est conforme aux limites d'exposition aux radiations IC CNR-102 établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

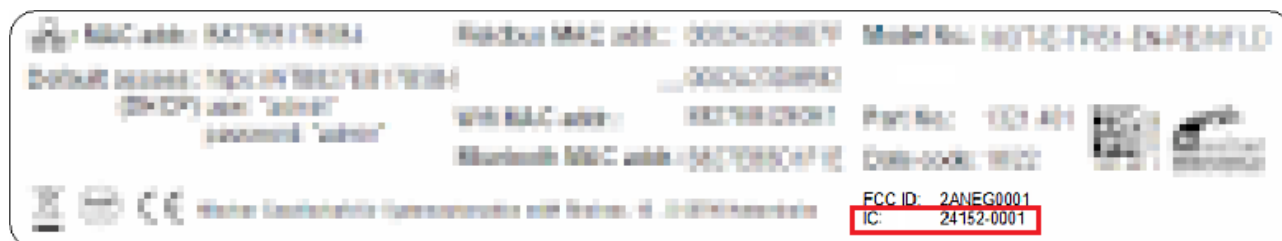


Figure 90: IC number on device label



## 10.2 Legal notes

### 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 .....	9
Figure 2:	netFIELD OS container management .....	10
Figure 3:	netFIELD OS inter-container communication .....	11
Figure 4:	netFIELD Connect SW architecture .....	12
Figure 5:	Device dimensions .....	15
Figure 6:	LED positions on device .....	18
Figure 7:	Gateway state LEDs .....	19
Figure 8:	Host name on device label (example) .....	25
Figure 9:	Login Device Manager.....	25
Figure 10:	Enter current password dialog.....	26
Figure 11:	Enter new password dialog .....	26
Figure 12:	Re-Authentication dialog .....	27
Figure 13:	System time value .....	28
Figure 14:	Change System Time dialog .....	28
Figure 15:	“Basic” onboarding screen in Device Manager.....	31
Figure 16:	Research Hardware ID .....	33
Figure 17:	Add device mask in netFIELD Portal.....	34
Figure 18:	Activation Code in portal.....	35
Figure 19:	Advanced Onboarding tab in device.....	36
Figure 20:	Example of an API Key permitting to onboard devices .....	38
Figure 21:	Copy key to clipboard .....	39
Figure 22:	Overview Local Device Manager.....	40
Figure 23:	System page in Local Device Manager .....	42
Figure 24:	Change host name dialog.....	43
Figure 25:	Networking page.....	45
Figure 26:	Details of LAN interface (eth0) .....	47
Figure 27:	IPv4 Settings .....	48
Figure 28:	Manual IPv4 Settings.....	48
Figure 29:	Open Firewall configuration page.....	51
Figure 30:	Elements on Firewall configuration page.....	51
Figure 31:	Add Zone dialog .....	53
Figure 32:	Add services .....	56
Figure 33:	Add custom services dialog.....	57
Figure 34:	Add forward port dialog .....	58
Figure 35:	Network Proxy configuration.....	59
Figure 36:	Proxy Settings dialog window.....	60
Figure 37:	Using one Proxy server for all protocols.....	61
Figure 38:	Separate HTTP/HTTPS/FTP configuration .....	62
Figure 39:	Restart dialog after changing proxy server configuration .....	63
Figure 40:	Synchronize proxy settings with netFIELD Portal.....	64

Figure 41:	Wi-Fi Client Mode .....	65
Figure 42:	Client mode parameters .....	67
Figure 43:	Connect Network dialog .....	69
Figure 44:	Connect network message .....	71
Figure 45:	Access Point Mode .....	73
Figure 46:	Warning note .....	74
Figure 47:	Configure Interface message .....	74
Figure 48:	wlan0 configuration page.....	75
Figure 49:	Set manual address in IPv4 Settings dialog .....	75
Figure 50:	Enter Manual IP Address.....	76
Figure 51:	Configured DHCP service .....	77
Figure 52:	DHCP Server Configuration dialog.....	79
Figure 53:	Basic Onboarding page .....	81
Figure 54:	Offboarding "Basic" .....	82
Figure 55:	Offboarding "Advanced" .....	82
Figure 56:	Standard Docker.....	84
Figure 57:	Expand concise container details .....	85
Figure 58:	Container parameters with terminal window.....	86
Figure 59:	Image Search dialog of Standard Docker.....	87
Figure 60:	Run Image dialog .....	88
Figure 61:	Expand image details .....	89
Figure 62:	Image details .....	90
Figure 63:	IOT Edge Docker.....	91
Figure 64:	Container details expanded.....	93
Figure 65:	Container parameters .....	94
Figure 66:	IoT image expanded.....	95
Figure 67:	Details of netFIELD Proxy image .....	96
Figure 68:	Accounts.....	97
Figure 69:	Create new account.....	98
Figure 70:	Edit account.....	98
Figure 71:	Web Server Certificate page .....	100
Figure 72:	General Settings.....	101
Figure 73:	Web Server Settings tab.....	102
Figure 74:	Default MQTT Settings .....	103
Figure 75:	Docker Network Settings .....	105
Figure 76:	Default docker network configuration .....	107
Figure 77:	OT interface.....	108
Figure 78:	Remote Access tab .....	110
Figure 79:	Terminal.....	112
Figure 80:	OS update page .....	113
Figure 81:	Selected OS update image.....	114

Figure 82:	Upload finished message .....	115
Figure 83:	OS update “Disconnected” message.....	116
Figure 84:	Logs.....	117
Figure 85:	Formatting USB stick .....	119
Figure 86:	Format USB STICK dialog window.....	120
Figure 87:	Formatted USB stick.....	120
Figure 88:	Recovery image on USB stick .....	121
Figure 89:	FCC label.....	127
Figure 90:	IC number on device label.....	128

## List of tables

Table 1:	List of revisions .....	5
Table 2:	Terms and abbreviations .....	7
Table 3:	Positions of the interfaces.....	15
Table 4:	Power supply connector .....	16
Table 5:	Description of device's status LEDs .....	19
Table 6:	LEDs LAN interface .....	19
Table 7:	LEDs of the Real-Time Ethernet interface .....	20
Table 8:	Tasks for commissioning the device (netFIELD Portal user).....	21
Table 9:	Tasks for commissioning the device (Standard Docker user) .....	22
Table 10:	Available Firewall zones .....	52
Table 11:	Elements in Add Zone dialog.....	53
Table 12:	Columns/elements in Allowed Services table .....	55
Table 13:	Columns/elements in Forward Ports table.....	57
Table 14:	Control elements in main toolbar .....	58
Table 15:	Wi-Fi operating modes.....	66
Table 16:	Currently Connected Network.....	68
Table 17:	Visible Networks .....	68
Table 18:	Parameters in Connect Network dialog (1).....	69
Table 19:	Parameters in Connect Network dialog (2).....	70
Table 20:	Connection Profiles.....	72
Table 21:	Access Point parameters .....	73
Table 22:	Elements/Parameters on DHCP Server page .....	77
Table 23:	Parameters of DHCP Server Configuration dialog .....	79
Table 24:	Default MQTT Client Settings .....	104
Table 25:	Standard Docker Network Settings .....	106
Table 26:	Standard Docker Network Settings .....	107
Table 27:	Technical data netFIELD Connect (NIOT-E-TPI51-EN-RE/NFLD).....	124



# Contacts

## HEADQUARTERS

### 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 9907-99  
E-mail: [de.support@hilscher.com](mailto:de.support@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.  
69500 Bron  
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  
Phone: +91 8888 750 777  
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)

### Korea

Hilscher Korea Inc.  
Seongnam, Gyeonggi, 463-400  
Phone: +82 (0) 31-789-3715  
E-mail: [info@hilscher.kr](mailto:info@hilscher.kr)

### Switzerland

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

### Support

Phone: +49 (0) 6190 9907-99  
E-mail: [ch.support@hilscher.com](mailto:ch.support@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)