COMPETENCE IN COMMUNICATION

User manual

netFIELD OnPremise

Hilscher Gesellschaft für Systemautomation mbH
www.hilscher.com

DOC200901UM02EN | Revision 2 | English | 2021-06 | Released | Public

Table of contents

1 Introduction 5
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
2 Brief description 8
2.1 Intended use 8
2.2 Key features 8
2.3 netFIELD OS: Industrial IoT Operating System 9
2.4 Depiction of netFIELD OnPremise SW architecture 12
3 Safety 13
3.1 General note 13
3.2 Personnel qualification 13
3.3 Device destruction by exceeding the allowed supply voltage 13
4 Hardware description 14
4.1 Device drawings 14
4.1.1 Positions of the interfaces 14
4.1.2 Dimensions 16
4.2 Interfaces 17
4.2.1 Power supply 17
4.2.2 LAN connectors 17
4.2.3 Real-Time Ethernet connectors 17
4.2.4 USB connectors 18
4.2.5 Serial interfaces COM1 and COM2 18
4.2.6 Wi-Fi 20
4.2.7 Monitor connectors 20
4.3 LEDs 21
4.3.1 Positions of the LEDs on the device 21
4.3.2 Device status LEDs 22
4.3.3 LEDs of the LAN interface 23
4.3.4 LEDs of the Real-Time Ethernet interface 23
5 Commissioning and first steps 24
5.1 Overview 24
5.1.1 netFIELD Portal user 24
5.1.2 Standard Docker user 25
5.2 Mounting 26
5.2.1 Attaching LED sticker (optional) 26
5.2.2 Mounting 27
5.2.3 Connecting Voltage suppy 28
5.3 Establish LAN connection and login to Local Device Manager 29
5.3.1 Overview 29
5.3.2 Using DHCP server 30
5.3.3 Establishing one-to-one connection to device (without DHCP server) 33
5.3.4 Login to Local Device Manager 34

© Hilscher 2021

5.4 Set system time ... 37
5.5 "Onboard" (register) device in netFIELD Portal ... 39
5.5.1 Overview ... 39
5.5.2 Onboarding using the “Basic” method ... 40
5.5.3 Onboarding using the “Advanced” method ... 43

6 Local Device Manager ... 50

6.1 Overview ... 50
6.2 System ... 52
6.3 Networking ... 55
6.3.1 Overview ... 55
6.3.2 Firewall ... 60
6.3.3 Network Proxy settings ... 69
6.4 Networking Services ... 76
6.4.1 Wi-Fi ... 76
6.4.2 DHCP Server ... 88
6.5 Onboarding (and offboarding) ... 92
6.6 Standard Docker ... 95
6.7 IoT Edge Docker ... 102
6.8 Accounts ... 108
6.9 Certificate ... 111
6.10 General Settings ... 112
6.10.1 Overview ... 112
6.10.2 Web Server (Port) Settings ... 113
6.10.3 Default MQTT Client Settings ... 114
6.10.4 Docker Network Settings ... 116
6.10.5 OT Interface (Using the cifx0 interface or RTE) ... 119
6.10.6 Remote Access ... 121
6.11 Terminal ... 123
6.12 System Update ... 124
6.13 Logs ... 128

7 Good to know.. ... 129

7.1 Device recovery via USB ... 129
7.1.1 Overview ... 129
7.1.2 Requirements ... 129
7.1.3 Step-by-step instructions ... 130
7.2 Useful CLI commands and parameters in Terminal ... 138
7.2.1 Network Manager ... 138
7.2.2 Show interface status ... 138
7.2.3 Activate interface ... 138
7.2.4 Docker Compose Support for Standard Docker environment ... 138
7.2.5 Manage Standard Docker ... 138
7.2.6 Manage IoT Edge Docker ... 138
7.2.7 Enable/disable SSH Daemon (release port 22) ... 138
7.2.8 External storage support using iSCSI ... 139
7.2.9 Follow the system log via terminal CLI ... 139

8 Technical data ... 140

9 Decommissioning, dismounting and disposal ... 142

© Hilscher 2021

9.1 Putting the device out of operation 142
9.2 Removal of battery 142
9.3 Disposal of waste electronic equipment 143
10 Legal notes 144
List of figures 148
List of tables 151
Contacts 152

© Hilscher 2021

1 Introduction

1.1 About this document

1.1.1 Description of the contents

This user manual describes the hardware and the web-based management GUI (Local Device Manager) of the **netFIELD OnPremise** device (NIOT-E-TIJCK-GB-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	2020-12-10	MKE	Document created.
2	2021-06-29	MKE	Document revised and updated to netFIELD OS 2.2: Section *Brief description* [▷ page 8] updated. Section *LAN connectors* [▷ page 17] updated. Section *LEDs of the Real-Time Ethernet interface* [▷ page 23] updated. Section *Establish LAN connection and login to Local Device Manager* [▷ page 29] updated. Section *"Onboard" (register) device in netFIELD Portal* [▷ page 39] updated. Section *Firewall* [▷ page 60] updated. Section *Using the cifx0 interface (RTE)* removed (substituted by section *OT Interface (Using the cifx0 interface or RTE)* [▷ page 119]). Section *Networking Services* [▷ page 76] added. Section *Standard Docker* [▷ page 95] revised. Section *IoT Edge Docker* [▷ page 102] revised. Section *OT Interface (Using the cifx0 interface or RTE)* [▷ page 119] added. Section *Remote Access* [▷ page 121] added.

Table 1: List of revisions

© Hilscher 2021

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

© Hilscher 2021

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

© Hilscher 2021

2 Brief description

2.1 Intended use

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

2.2 Key features

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

© Hilscher 2021

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.

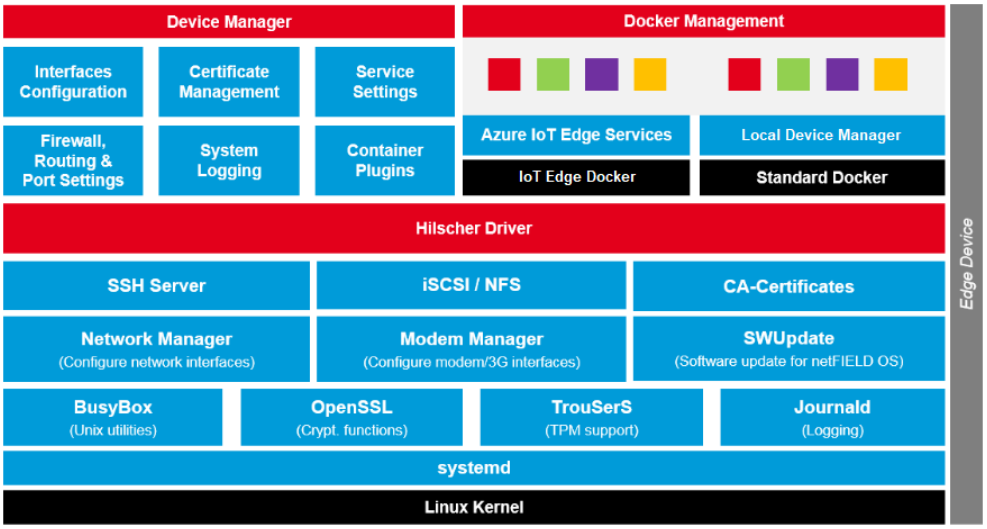


Figure 1: netFIELD OS architecture

© Hilscher 2021

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.

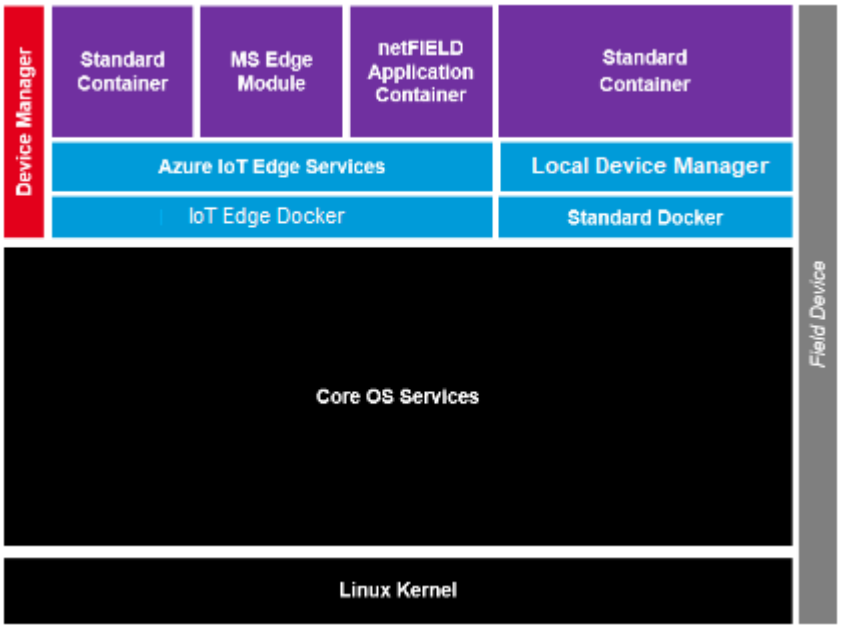


Figure 2: netFIELD OS container management

© Hilscher 2021

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.

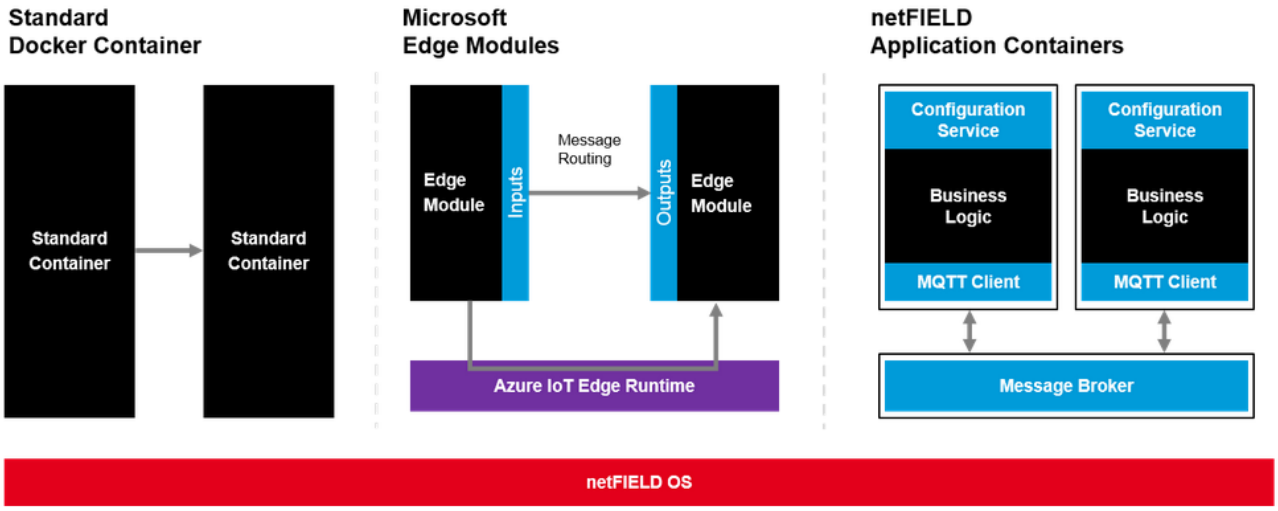


Figure 3: netFIELD OS inter-container communication

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

© Hilscher 2021

2.4 Depiction of netFIELD OnPremise SW architecture

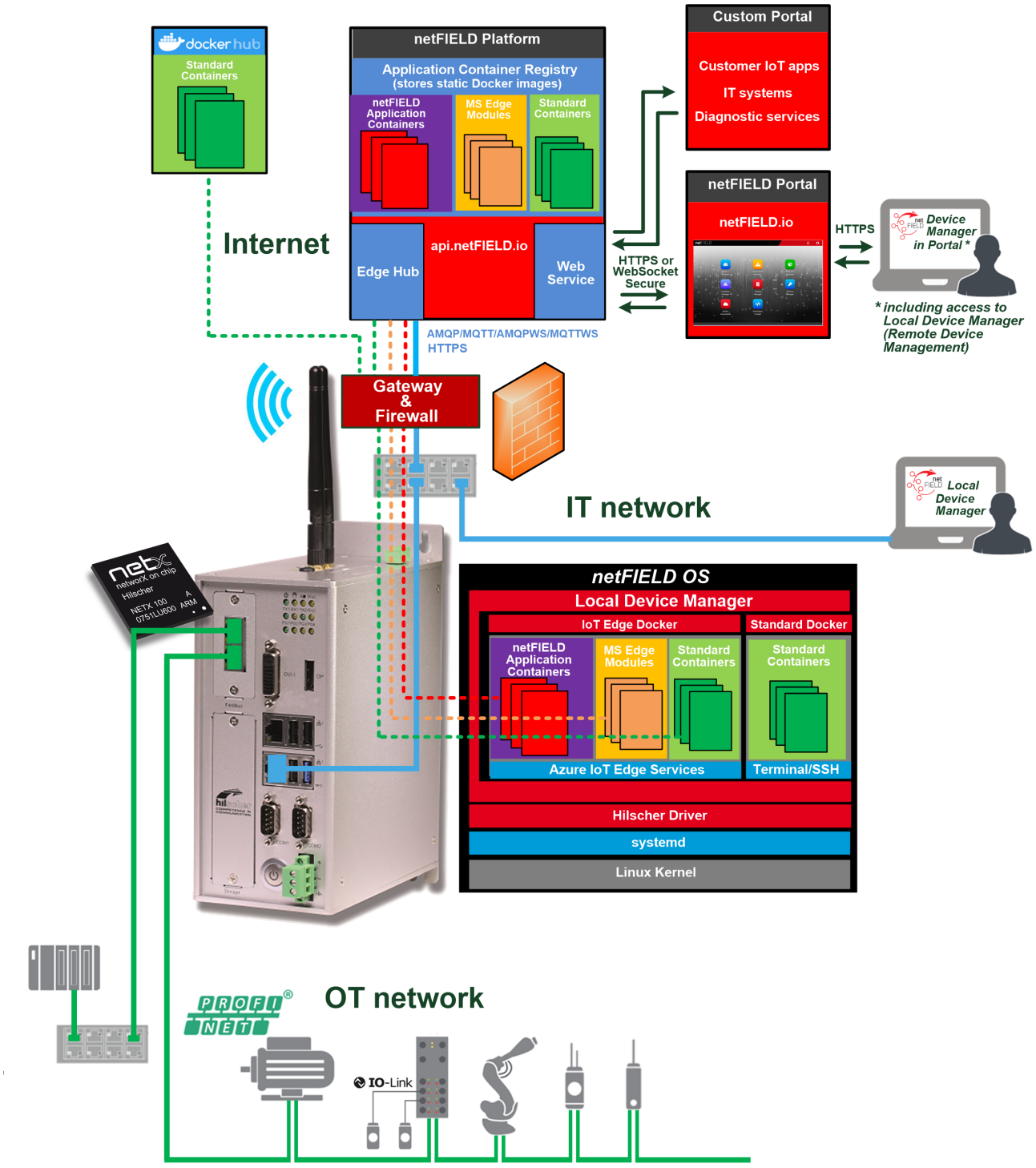


Figure 4: netFIELD OnPremise SW architecture

© Hilscher 2021

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 (± 4.8 V DC). Make sure that the limits of the allowed range for the supply voltage are not exceeded.
- A supply voltage above the upper limit can cause severe damage to the device!
- A supply voltage below the lower limit can cause malfunction of the device.

© Hilscher 2021

4 Hardware description

4.1 Device drawings

4.1.1 Positions of the interfaces

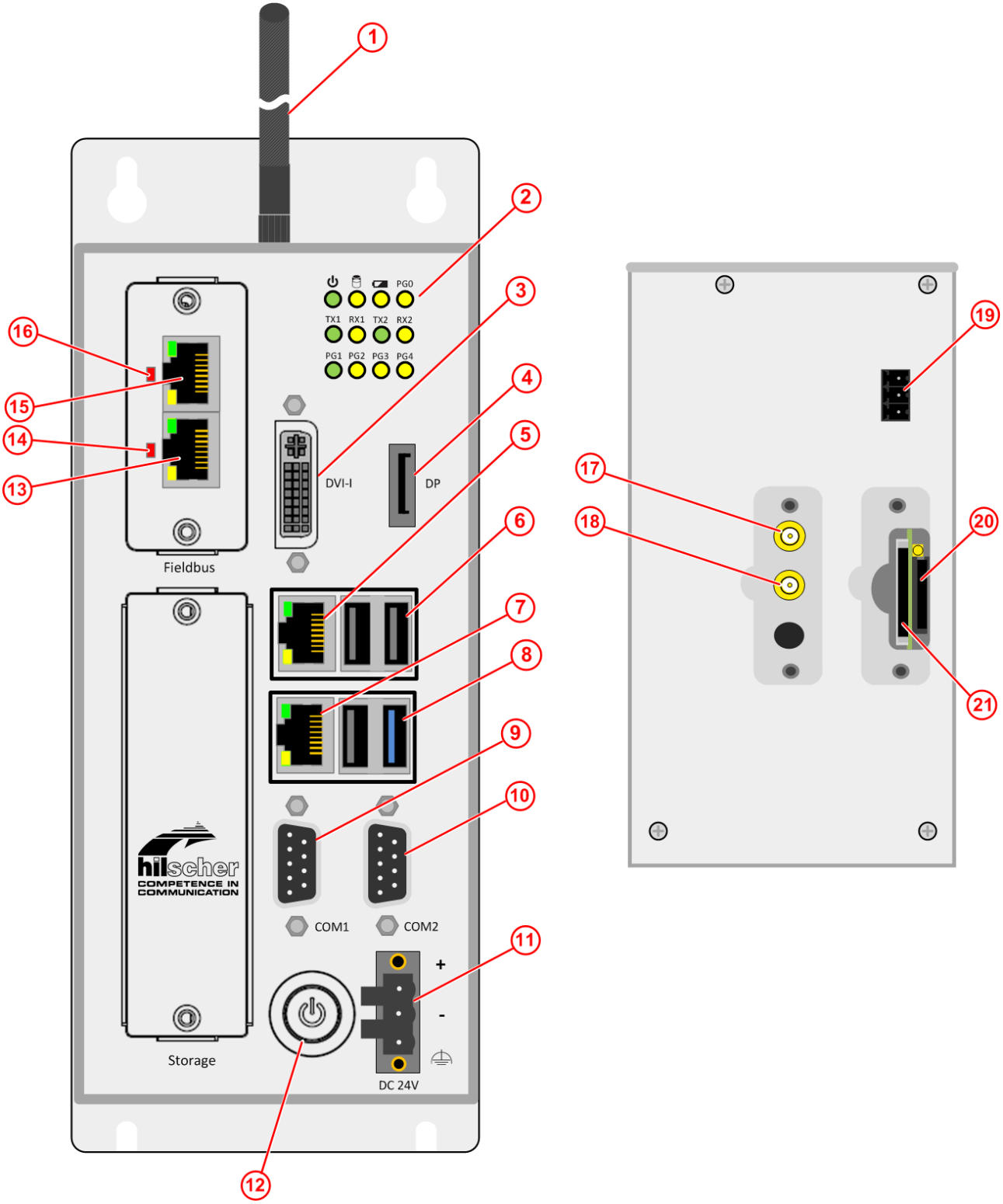


Figure 5: Front and top view

© Hilscher 2021

Pos.	Interface	For details see section
(1)	Antennas (Wi-Fi antennas are included in the delivery)	*Wi-Fi* [▷ page 20]
(2)	Device state LEDs (12 x)	*Device status LEDs* [▷ page 22]
(3)	DVI-I connector for external monitor	*Monitor connectors* [▷ page 20]
(4)	DisplayPort connector for external monitor	
(5)	LAN connector (RJ45 jacket) port 2 / Eth1	*LAN connectors* [▷ page 17]
(6)	USB connectors (3x USB 2.0)	*USB connectors* [▷ page 18]
(7)	LAN connector (RJ45 jacket) port 1 / Eth0	*LAN connectors* [▷ page 17]
(8)	USB connector (1x USB 3.0)	*USB connectors* [▷ page 18]
(9)	Serial interface connector COM1 (RS-232/422/485, can be configured)	*Serial interfaces COM1 and COM2* [▷ page 18]
(10)	Serial interface connector COM2 (RS-232/422/485, can be configured)	
(11)	+24 V DC supply voltage connector (Combicon)	*Power supply* [▷ page 17]
(12)	Power button On/Off	-
(13)	Real-Time Ethernet connector (RJ45 jacket) port 1 (channel 1)	*Real-Time Ethernet connectors* [▷ page 17]
(14)	LED for indicating the communication status of the Real-Time Ethernet interface.	*LEDs of the Real-Time Ethernet interface* [▷ page 23]
(15)	Real-Time Ethernet connector (RJ45 jacket) port 0 (channel 0)	*Real-Time Ethernet connectors* [▷ page 17]
(16)	LED for indicating the communication status of the Real-Time Ethernet interface.	*LEDs of the Real-Time Ethernet interface* [▷ page 23]
(17)	SMA connector for WiFi or cellular radio antenna	*Wi-Fi* [▷ page 20]
(18)	SMA connector for WiFi or cellular radio antenna	
(19)	Remote push button connector (without function)	-
(20)	SIM card holder (under removable cover)	-
(21)	SD card holder (under removable cover, without function)	-

Table 3: Positions of the interfaces

© Hilscher 2021

4.1.2 Dimensions

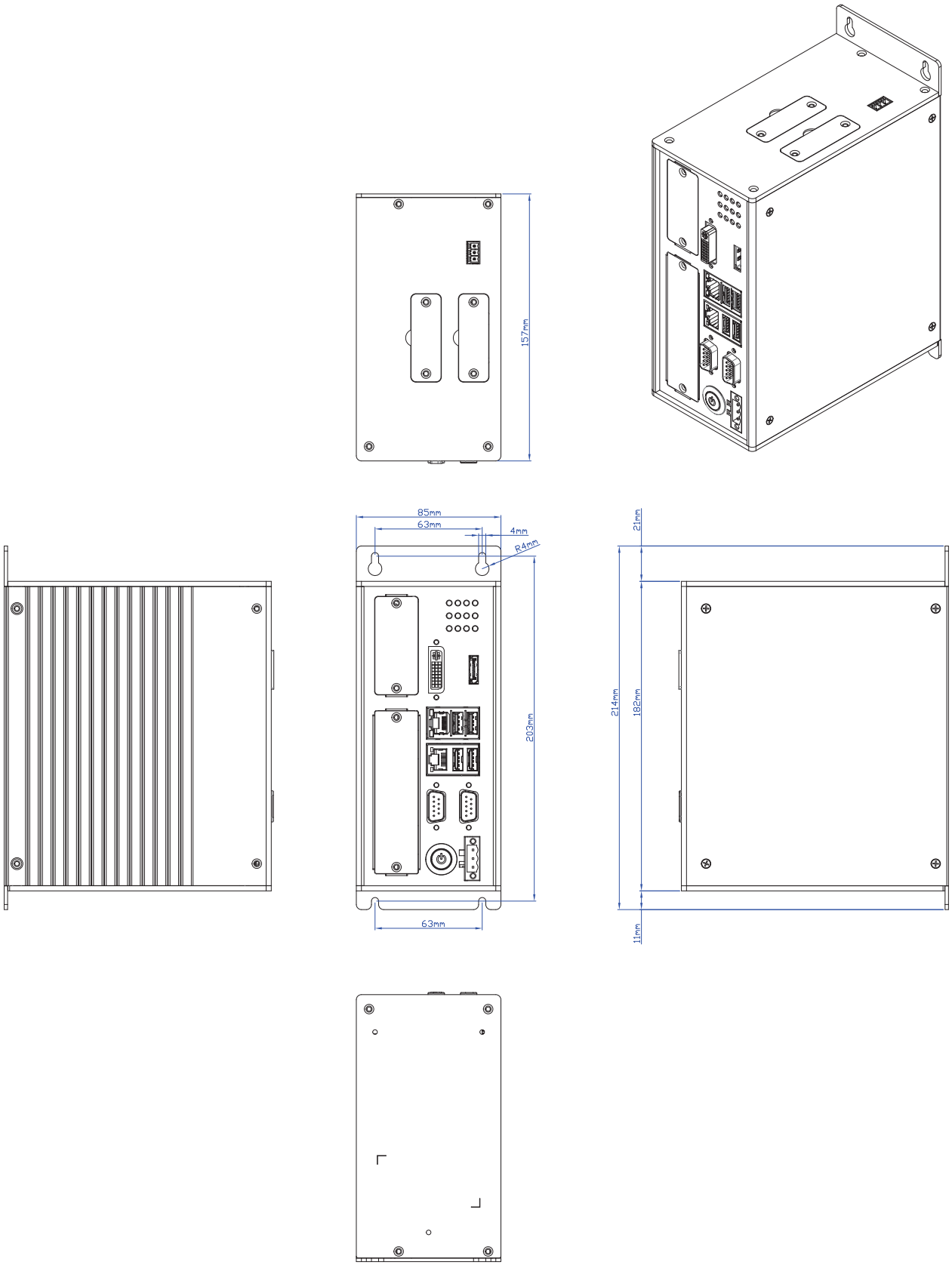


Figure 6: Device dimensions

© Hilscher 2021

4.2 Interfaces

4.2.1 Power supply

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

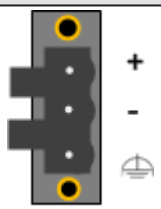
DC 24V	Pin	Signal	Description
	+	+24 V DC	+24 V DC
	-	GND	Ground (Reference potential)
	⏚	FE	Functional earth

Table 4: Power supply connector

4.2.2 LAN connectors

The two RJ45 connectors (see positions (5) and (7) in section *Positions of the interfaces* [page 14]) allow you to connect your device to your IT network, respectively to the cloud (e.g. the netFIELD Portal).
The MAC addresses of the LAN interfaces are printed on the device label.
Note that the “factory setting” for the IP address of the LAN port 1 (eth0) is DHCP mode (“fallback” is *link-local*, i.e. address block `169.254.0.0/16`).
The “factory setting” for the IP address of the LAN port 2 (eth1) is `192.168.253.1`
You can change the IP address settings in the Local Device Manager (see section *Networking* [page 55]).

4.2.3 Real-Time Ethernet connectors

The two RJ45 connectors (see positions (13) and (15) in section *Positions of the interfaces* [page 14]) allow you to connect your device to a Real-Time Ethernet network (OT network).
The MAC addresses of the RTE interfaces are printed on the device label (“Fieldbus MAC addr.”)
Note that you must deploy software containers featuring the corresponding applications (e.g. *netFIELD App PROFINET Device*) on the device in order to use the Real-Time Ethernet interface.

Note:
The RTE interface can also be used like a standard Ethernet TCP/IP interface with limited data throughput. (In this case, “multicasts” are not supported.)
If you want to do so, you can enable this option in the **Local Device Manager** under **General Settings** > **OT Interface** (see section *OT Interface (Using the cifx0 interface or RTE)* [page 119] for further information).

© Hilscher 2021

4.2.4 USB connectors

The device is equipped with three USB 2.0 ports and one USB 3.0 port (see positions (6) and (8) in section *Positions of the interfaces* [page 14]). For the maximum allowed output current, see section Technical data.

Note:
You do not need the USB connectors for the “normal” operation of the device.
You need the USB connectors e.g. for connecting a keyboard in order to access the terminal, to change BIOS settings or to perform a firmware recovery via USB stick.

4.2.5 Serial interfaces COM1 and COM2

The device has two configurable serial interfaces: COM1 and COM2 (see positions (9) and (10) in section *Positions of the interfaces* [page 14]). Each serial interface can be used as RS-232, RS-422 or RS-485 interface.

Requirements for using serial interface

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

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

BIOS settings

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

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

Table 5: Parameters of the serial interface

© Hilscher 2021

Pinning RS-232

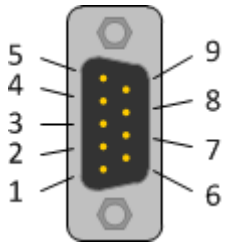
RS-232	Pin	Signal	Description
	1	DCD	Data Carrier Detect
	2	RXD	Receive signal
	3	TXD	Send signal
	4	DTR	Data Terminal Ready
	5	ISO_GND	Ground (reference potential)
	6	DSR	Data Set Ready
	7	RTS	Request to Send
	8	CTS	Clear to Send
	9	RI	Ring Indicator

Table 6: RS-232 D-Sub

Pinning RS-422

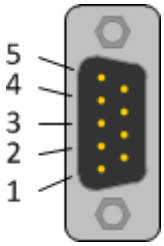
RS-422	Pin	Signal	Description
	1	Tx-	Send signal negative
	2	Tx+	Send signal positive
	3	Rx-	Receive signal negative
	4	Rx+	Receive signal positive
	5	ISO_GND	Ground (reference potential)
	6	n.c.	-
	7	n.c.	-
	8	n.c.	-
	9	n.c.	-

Table 7: RS-422 D-Sub

Pinning RS-485

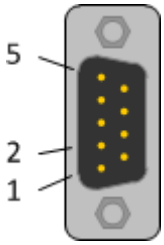
RS-485	Pin	Signal	Description
	1	Rx/Tx-	Send/receive signal negative
	2	Rx/Tx+	Send/receive signal positive
	3	n.c.	-
	4	n.c.	-
	5	ISO_GND	Ground (reference potential)
	6	n.c.	-
	7	n.c.	-
	8	n.c.	-
	9	n.c.	-

Table 8: RS-485 D-Sub

© Hilscher 2021

4.2.6 Wi-Fi

The device is equipped with a Wi-Fi interface according to IEEE 802.11. (For the position of the antennas, see position (1) in section *Positions of the interfaces* [page 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 76]).

4.2.7 Monitor connectors

The device is equipped with a DVI-I socket (see position (3) in section *Positions of the interfaces* [page 14]) and a DisplayPort (DP) [position (4)] to connect a monitor.

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

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

© Hilscher 2021

4.3 LEDs

4.3.1 Positions of the LEDs on the device

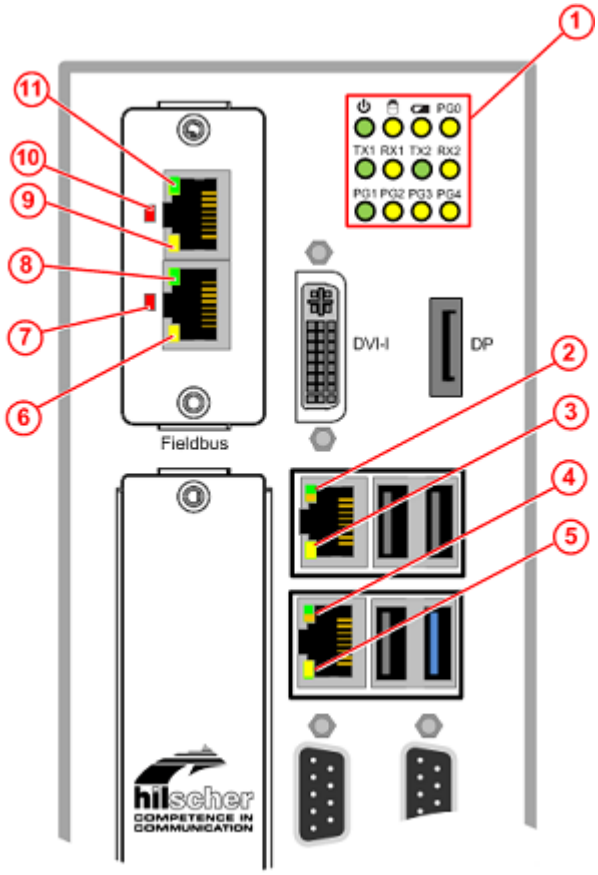


Figure 7: LED positions on device

© Hilscher 2021

4.3.2 Device status LEDs

LEDs indicating voltage supply, hard disk access, battery state and activity of operating system, serial interfaces and GPIOs. The position of the LEDs is indicated by position (1) in section *Positions of the LEDs on the device* [page 21].

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

Table 9: Description of device status LEDs

© Hilscher 2021

4.3.3 LEDs of the LAN interface

LEDs indicating state of the LAN communication (see section *Positions of the LEDs on the device* [page 21]).

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

Table 10: LEDs LAN interface

4.3.4 LEDs of the Real-Time Ethernet interface

LEDs (6) ... (11) in section *Positions of the LEDs on the device* [page 21] relate to the Real-Time Ethernet network (OT network) that is connected to the RTE ports of the device (labelled as **Fieldbus** on the device housing). Names and functions of these LEDs depend on the protocol of the Real-Time Ethernet container that you have deployed on your device. They are therefore not described in detail here.

Note:

The COM LED (position (7) in section *Positions of the LEDs on the device* [page 21]) shows steady red light if the TCP/IP channel of the cifx0 interface is enabled. See section *OT Interface (Using the cifx0 interface or RTE)* [page 119] for further information.

© Hilscher 2021

5 Commissioning and first steps

5.1 Overview

5.1.1 netFIELD Portal user

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

#	Step	For details see
0	Requirement: • You have a netFIELD Portal account.	-
1	Mount the device.	Section Mounting
2	Establish LAN connection and login to Local Device Manager.	Section *Establish LAN connection and login to Local Device Manager* [▷ page 29]
3	Set local system time.	Section *Set system time* [▷ page 37]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section *Network Proxy settings* [▷ page 69]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section *Docker Network Settings* [▷ page 116]
6	Optional: Configure netFIELD OS firewall. **Note**: 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 *Firewall* [▷ page 60]
7	“Onboard” (register) device in netFIELD Portal. **Note**: 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 *"Onboard" (register) device in netFIELD Portal* [▷ page 39]
8	Optional: Deploy application container(s) from netFIELD Portal (if not already deployed through Deployment Manifest).	Section *Deploying containers on your device* in the operating instruction manual *netFIELD Portal*, DOC190701OIxxEN

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

© Hilscher 2021

5.1.2 Standard Docker user

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

#	Step	For details see
1	Mount the device.	Section Mounting
2	Establish LAN connection and login to Local Device Manager.	Section *Establish LAN connection and login to Local Device Manager* [▷ page 29]
3	Set local system time.	Section *Set system time* [▷ page 37]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section *Network Proxy settings* [▷ page 69]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section *Docker Network Settings* [▷ page 116]
6	Optional: Configure netFIELD OS firewall. **Note**: 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 *Firewall* [▷ page 60]
7	Open Standard Docker and deploy and run container images.	Section *Standard Docker* [▷ page 95]

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

© Hilscher 2021

5.2 Mounting

5.2.1 Attaching LED sticker (optional)

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

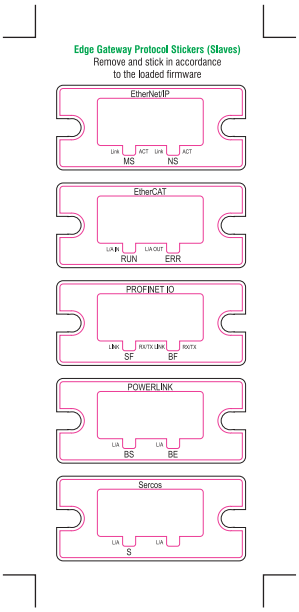


Figure 8: LED sticker

© Hilscher 2021

5.2.2 Mounting

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

The figure shows the distance of the mounting holes:

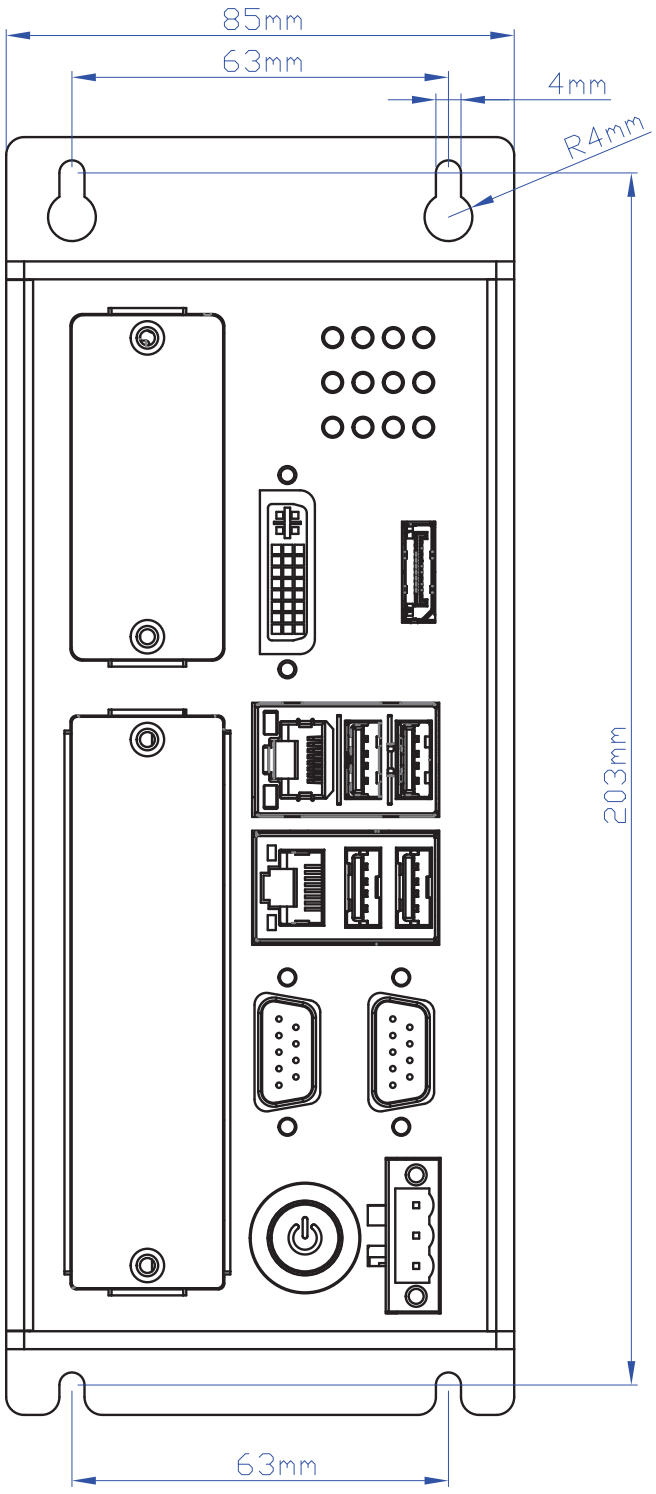


Figure 9: Mounting holes

© Hilscher 2021

5.2.3 Connecting Voltage suppy

➢ 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.

© Hilscher 2021

5.3 Establish LAN connection and login to Local Device Manager

5.3.1 Overview

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

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

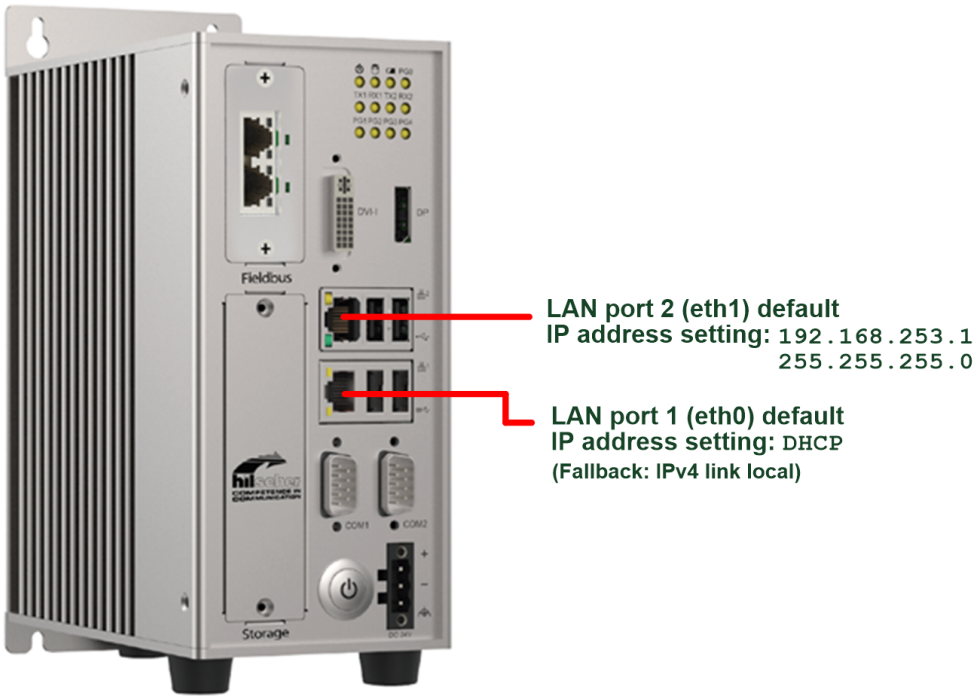


Figure 10: Factory IP address settings of LAN interfaces

Note:

The device contains a certificate issued by Hilscher. Therefore, your browser will probably issue an "unsecure connection" warning message when connecting to the device for the first time.
You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).

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

© Hilscher 2021

5.3.2 Using DHCP server

In its state of delivery, port 1 (eth0) of the LAN interface of the device is set to DHCP mode.
If a DHCP server is available in your local IT network, you can thus use the DHCP service it to assign an IP address to the LAN interface of the device.

Note:
If the device realizes that no DHCP service is available, it resets the port 1 (eth0) LAN interface address to *IPv4 link local* mode (“fallback” setting). *IPv4 link local* uses the address range from `169.254.0.0` to `169.254.255.255`.
The device outputs the *IPv4 link local* address at its display interfaces, therefore you can connect a monitor at one of the display interfaces (e.g. DisplayPort) to find out the exact address.

➢ Make sure that a DHCP service is available in your local network.

➢ Plug an Ethernet cable into the LAN port on the front panel of the device (see position (7) 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. This may take a few minutes.
If you know the IP address that the DHCP server has assigned to your device, you can now access the **Local Device Manager** directly by entering the assigned IP address into the address bar of your web browser. If you do not know the IP address, you can use the Windows network environment (see “Alternative A” below) or the “host name” of the device (see “Alternative B” below) to connect with it.

Note:
The device outputs its hostname and the IP address (which it has received from the DHCP server) at its display interfaces. Thus, connecting a monitor to one of its display interface (see positions (3) and (4) in section *Positions of the interfaces* [page 14]) allows you to check the assigned IP address.
In case no DHCP service is available, the “fallback” IPv4 link local address of eth0 interface will also be output at the display ports.

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

© Hilscher 2021

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.

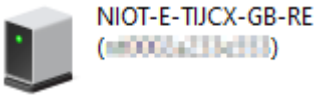
Alternative A: Connecting via Windows network environment

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.

© Hilscher 2021

Alternative B: Connecting via host name

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

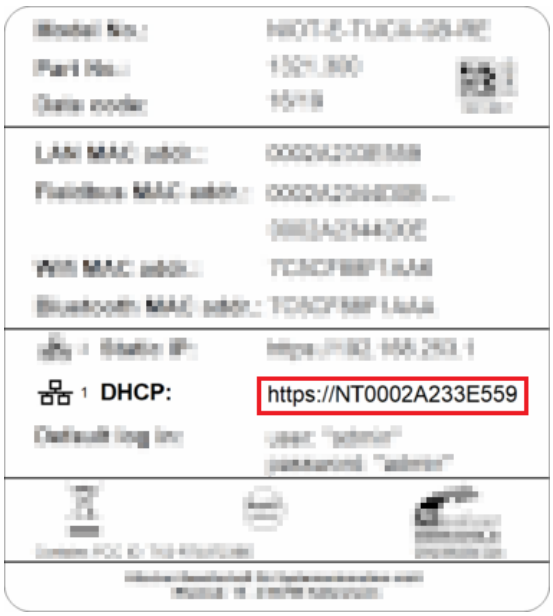


Figure 11: Host name on device label (example)

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

© Hilscher 2021

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

If no DHCP server is available in your network, you can connect your PC or notebook by Ethernet cable directly to the port 2 (eth1) LAN interface of the device (upper RJ45 socket of the two LAN interfaces).
For this, you must set an IP address on your PC or notebook that is compatible with the preset IP address and subnet mask of the port 2 (eth1) LAN interface of the gateway.
In its state of delivery, the preset IP address of the port 2/eth1 LAN interface is `192.168.253.1`, the subnet mask is `255.255.255.0`.

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

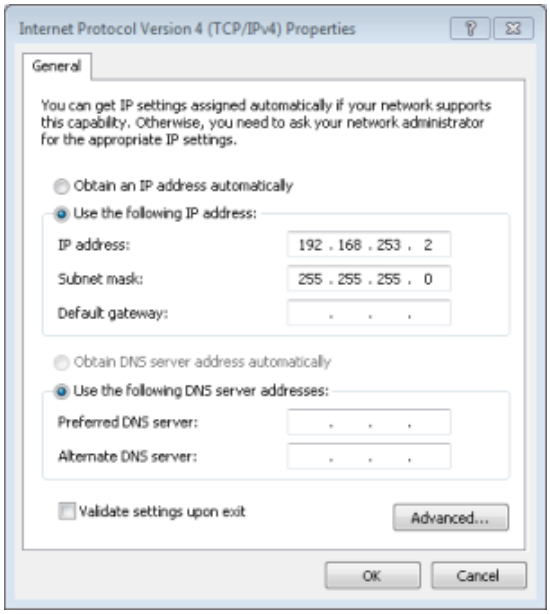


Figure 12: Setting IP address under Windows for direct LAN connection

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

© Hilscher 2021

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

5.3.4 Login to Local Device Manager

Note:
When connecting to the device for the first time, your browser will probably issue a security warning before displaying the Login screen of the Local Device Manager.
You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).
Note that the automatically created certificate is valid for one year. On the **Certificate** page of the **Local Device Manager**, you should upload your own certificate to the netFIELD OS. The corresponding root certificate should be rolled out on each of your PC/devices that you use for connecting to the netFIELD OS.

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

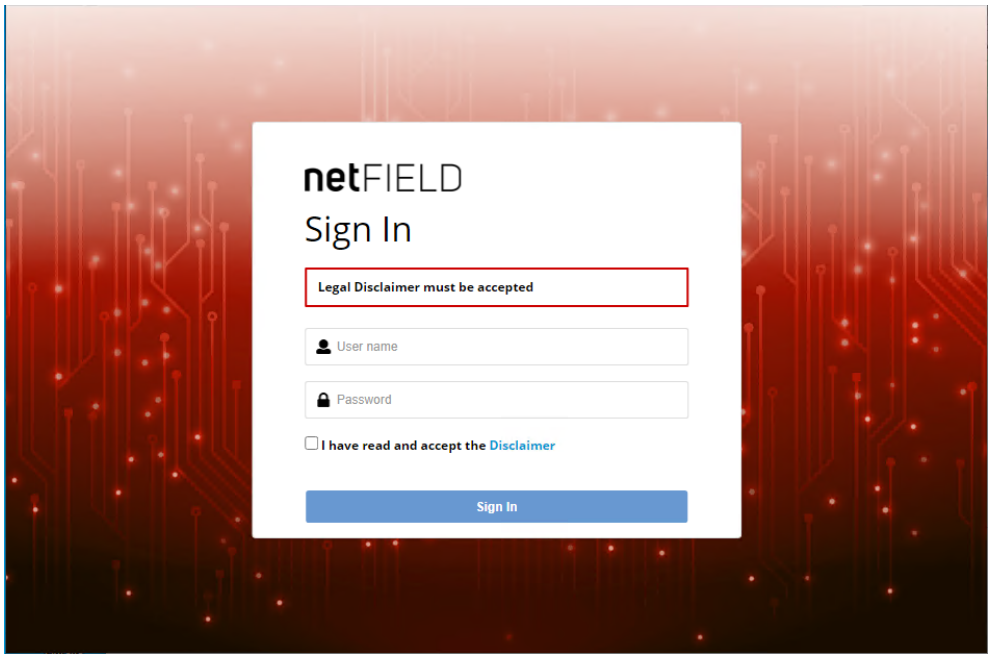


Figure 13: Login Device Manager

➢ In the **Sign In** dialog, enter the following default credentials:
User name: `admin`
Password: `admin`
➢ Read the **Disclaimer** then check the **I have read and accept the Disclaimer** box.
➢ Click **Sign In** button.

© Hilscher 2021

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:

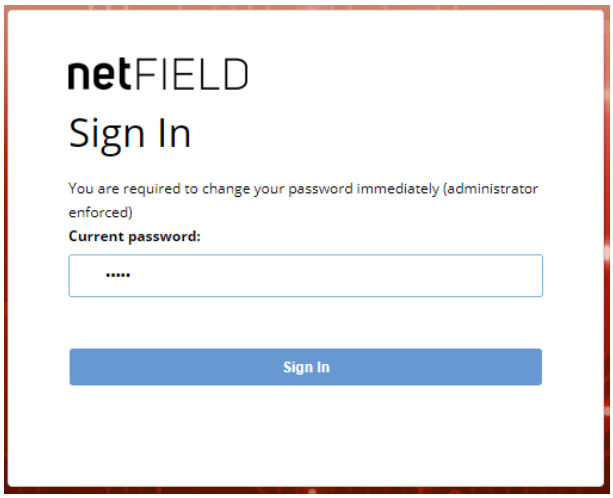


Figure 14: Enter current password dialog

The **New password** dialog opens:

Figure 15: Enter new password dialog

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

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

© Hilscher 2021

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

Figure 16: Re-Authentication dialog

➢ Enter your new password once again, then click **Sign In** button

↬ The **Local Device Manager** opens.

© Hilscher 2021

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** (**N**etwork **T**ime **P**rotocol 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**:

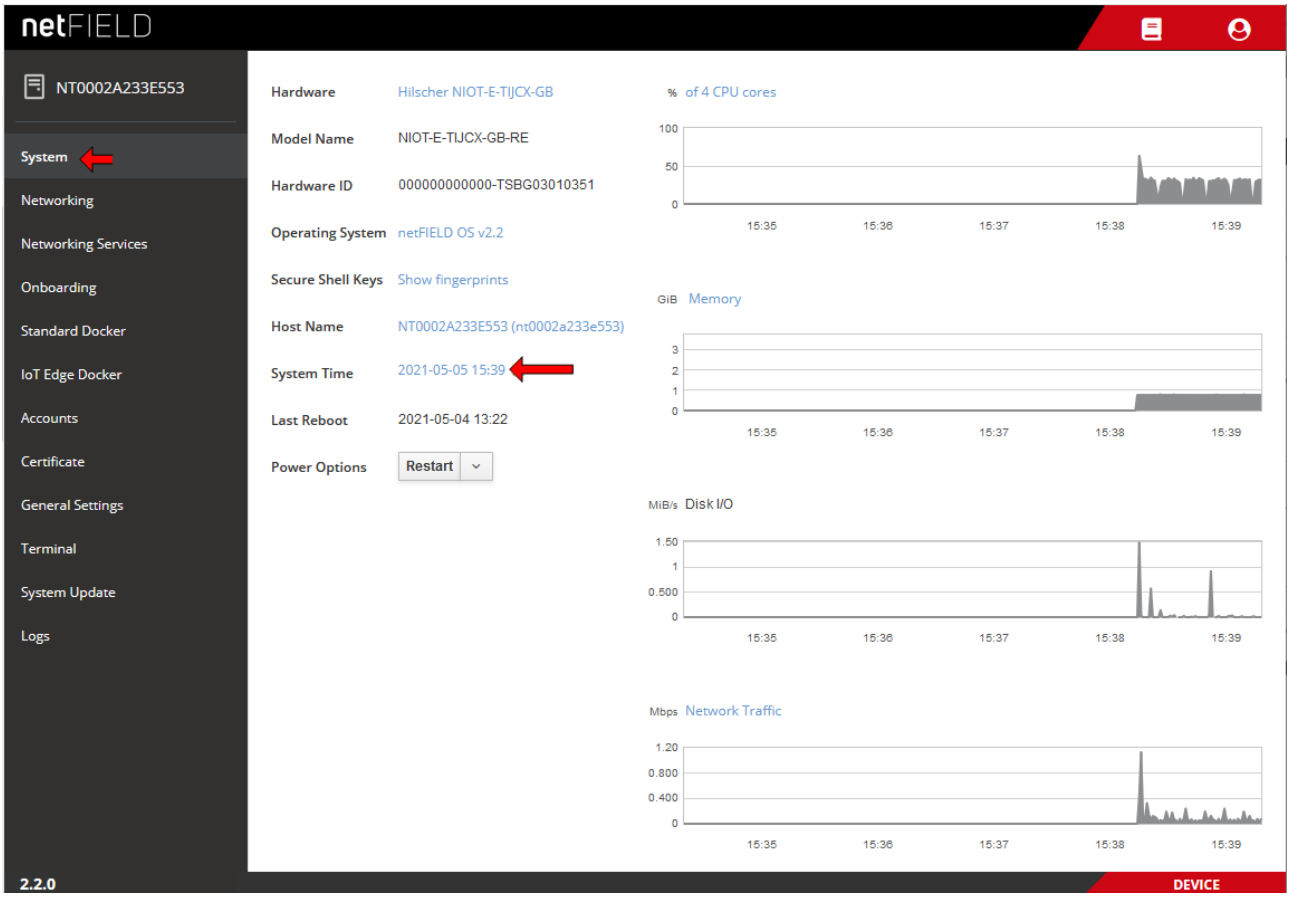


Figure 17: System time value

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

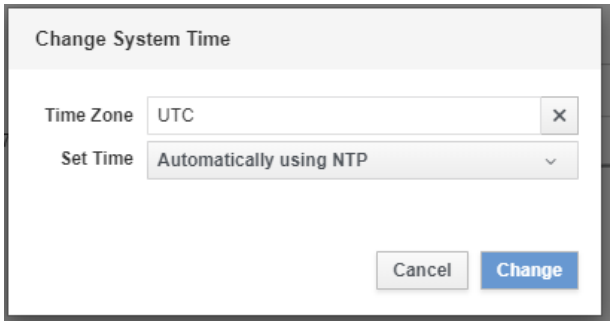


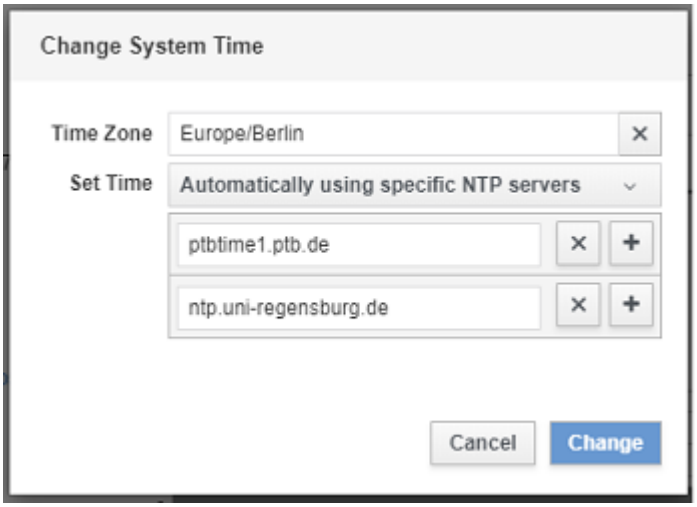
Figure 18: Change System Time dialog

➢ Click **x** button next to **Time Zone** field to delete the preset `UTC` value, then open the drop-down list and select the appropriate time zone region for your location (note that the list is searchable).

© Hilscher 2021

➢ 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.



➢ 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.

© Hilscher 2021

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.

© Hilscher 2021

5.5.2 Onboarding using the “Basic” method

➢ In the navigation panel of the **Local Device Manager**, choose **Onboarding**.

➢ The **Onboarding** page opens:

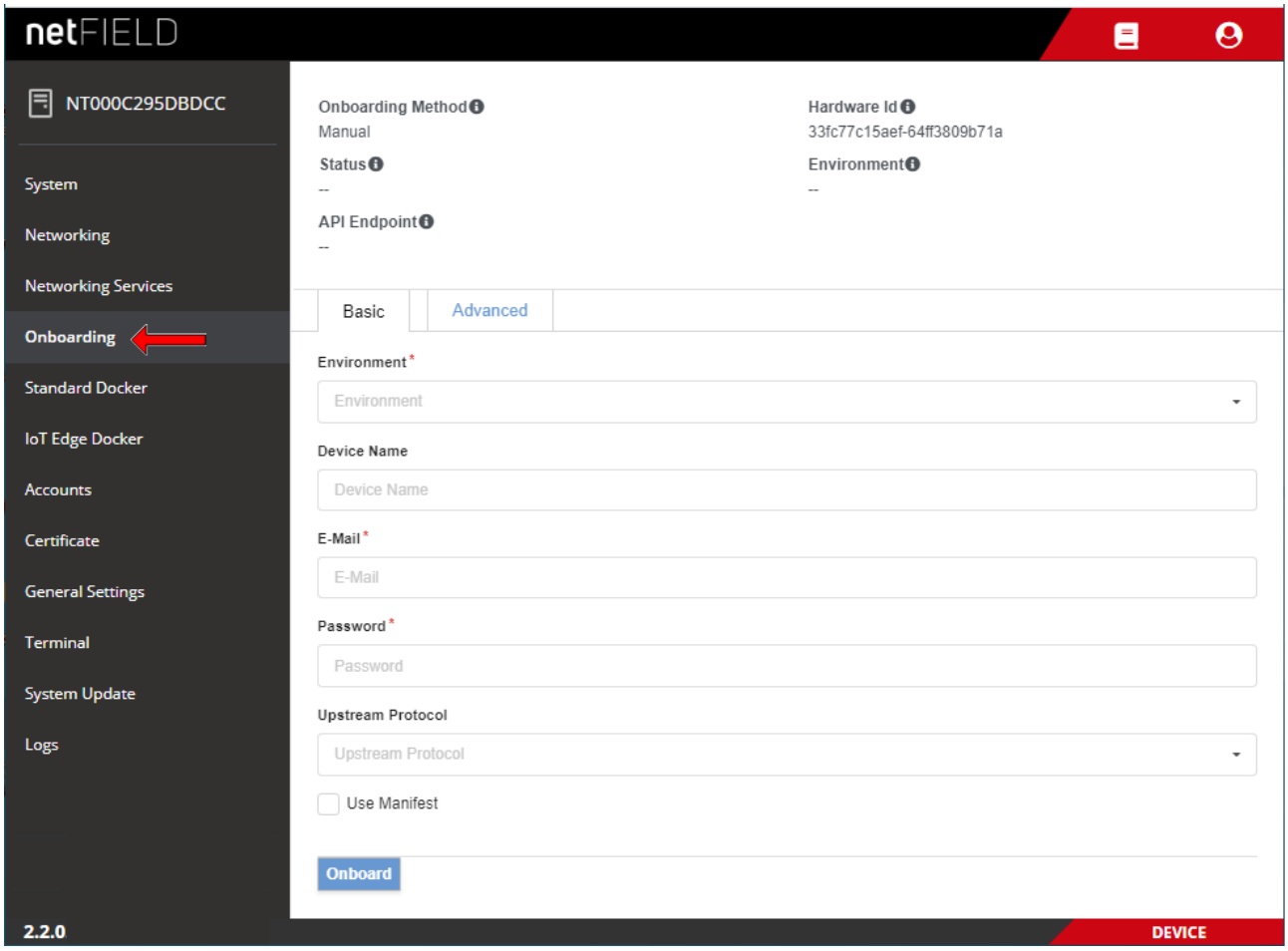


Figure 19: “Basic” onboarding screen in Device Manager

➢ 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.

© Hilscher 2021

➢ In the **Upstream Protocol** drop-down list, select the protocol that the netFIELD OS shall use for sending data to the netFIELD Cloud (“device-to-cloud” communication).

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

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

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

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

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

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

➢ 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.

© Hilscher 2021

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.

© Hilscher 2021

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:

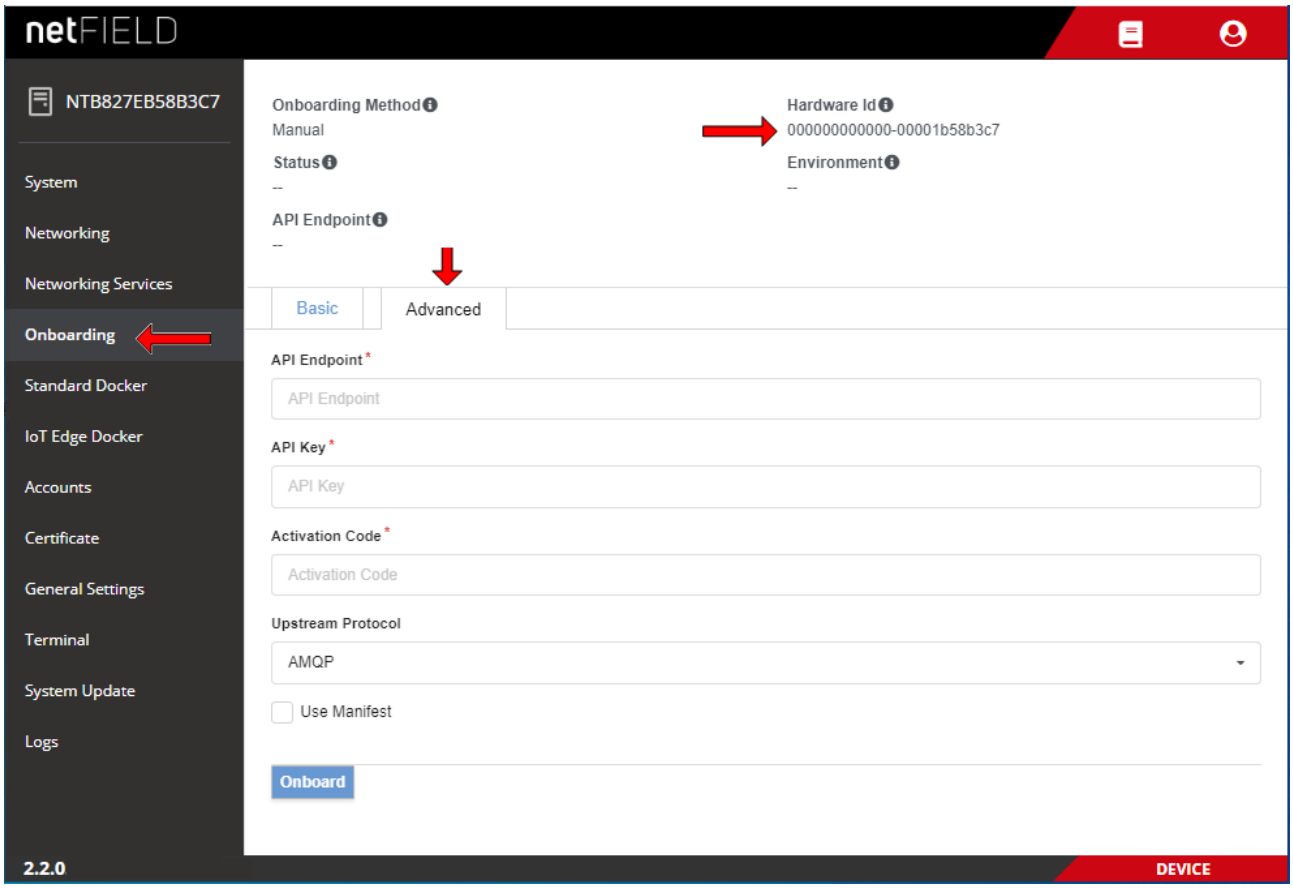


Figure 20: Research Hardware ID

   - ➢ Select the **Hardware ID** and copy the string to your clipboard.
   - ➢ Open a new tab in your browser and change to the portal, but do not close the connection to the **Local Device Manager** of your device in your first browser tab.
2. Add the device in the portal and create **Activation Code**.
   - ➢ In the portal, open the **Device Manager**.
   - ➢ On the start page (**Manage your devices**) of the **Device Manager**, select **+ Add** button.

© Hilscher 2021

The **Add Device** mask opens:

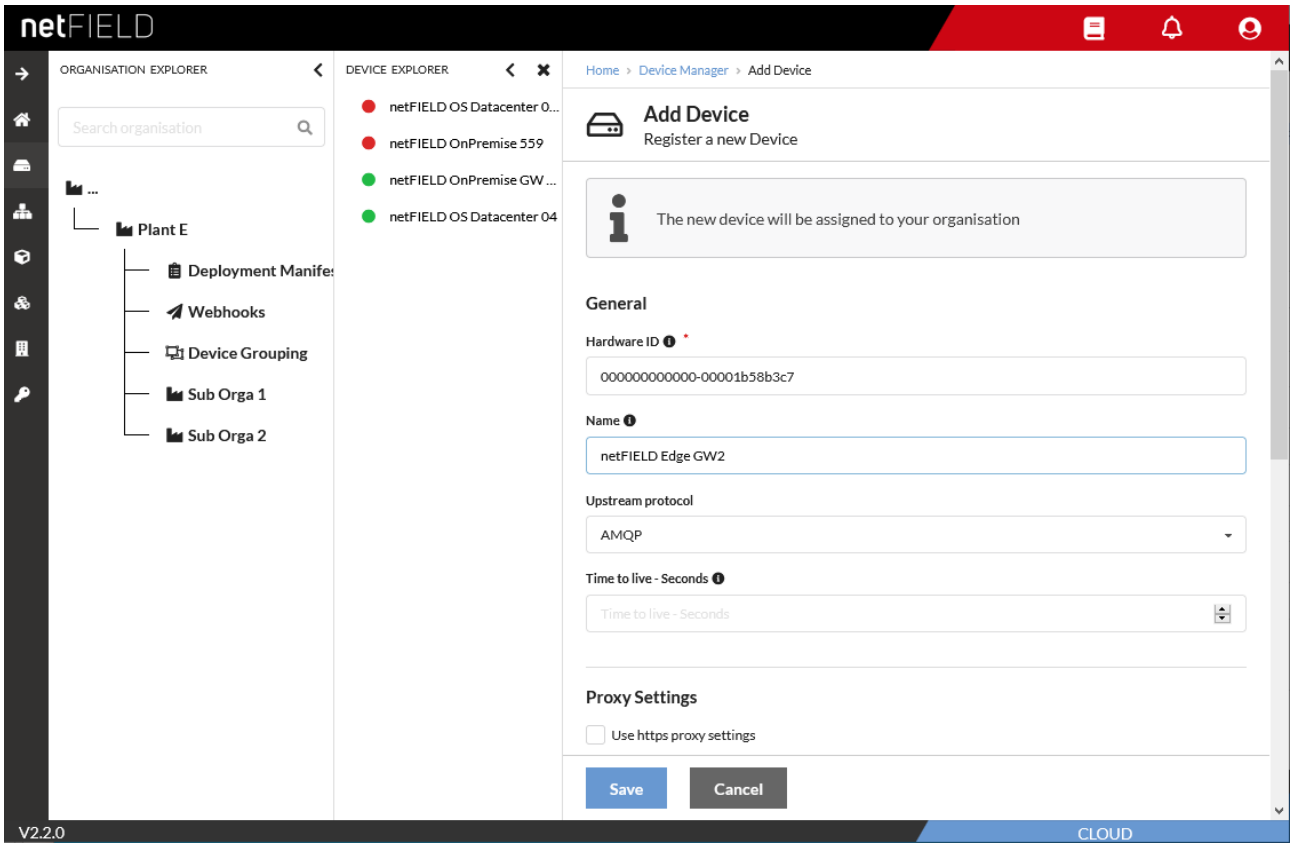


Figure 21: Add device mask in netFIELD Portal

- Copy the device's hardware ID from your clipboard into the **Hardware ID** field.
- In the **Name** field, enter a name for your device (optional but recommended).
- 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 (DOC190701OIxxEN).

- Click **Save** button.

© Hilscher 2021

The mask closes, and the **Overview** page of the newly created device opens, showing the **Activation Code** that you will have to enter locally on your device:

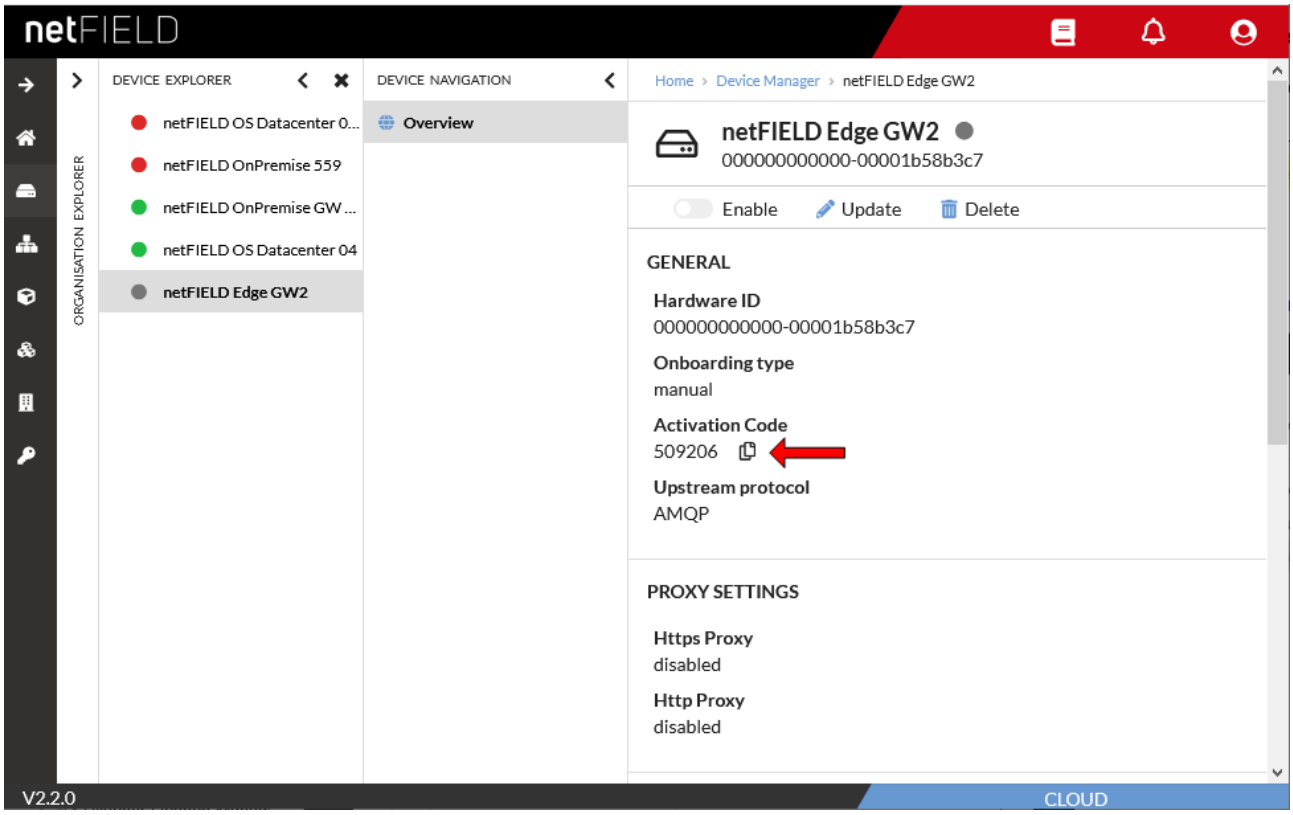


Figure 22: Activation Code in portal

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

© Hilscher 2021

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

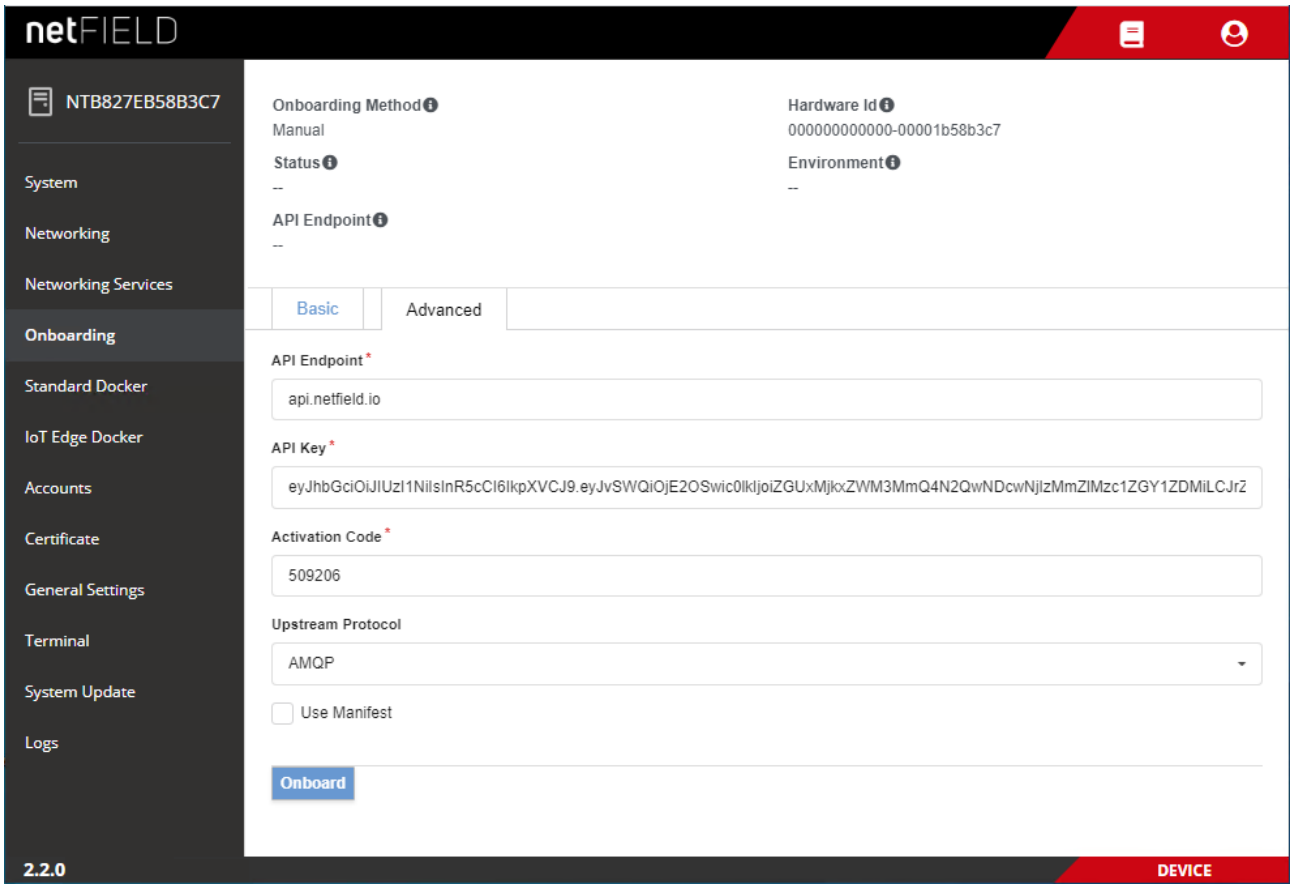


Figure 23: Advanced Onboarding tab in device

➢ In the **API Endpoint** field, enter the URL of the REST-API interface of the portal.
For the Hilscher *netFIELD Portal*, this is: `api.netfield.io`
If you are using a different instance of the portal, ask your portal's system administrator for the URL.

➢ In the **API KEY** field, enter an API Key that possesses the right to onboard devices. (See *Side note: How to copy an API Key for onboarding* below).

➢ Copy the activation code (which you have created in step 2) into the **Activation Code** field.

➢ In the **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.

© Hilscher 2021

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

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

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

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

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

➢ Click **Onboard** button, to start the onboarding process.

⇨ The device connects to the portal and is registered there. If the process has been successful, the following message appears: **Success – Device is now onboarded**.

Side note: How to copy an API Key for onboarding

For onboarding by "Advanced" method, you need an API Key, which you can copy to your clipboard in the **API Key Manager** of the netFIELD Portal, and then paste into the Local Device Manager of your device during onboarding.
The key must have the permissions (i.e. Security Level **org+ch** or **org**) for the **onboardedDevices** and **createDevices** functions of the **devices** resource of your organization.
You can use an already existing API key (which, for example, was created by the system administrator) or create a new API key yourself.
For information on how to create a new API Key, see section *Create/edit API key* in the *netFIELD Portal* manual, DOC190701OIxxEN.

API Keys are administered in the **API Key Manager** of the portal.
For accessing existing keys in the **API Key Manager**, you must at least have the permission to use the **getKeys** function of the **keys** resource.
For creating a new key, you must have the permission to use the **createKeys** function of the **keys** resource.

© Hilscher 2021

- ➢ 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:

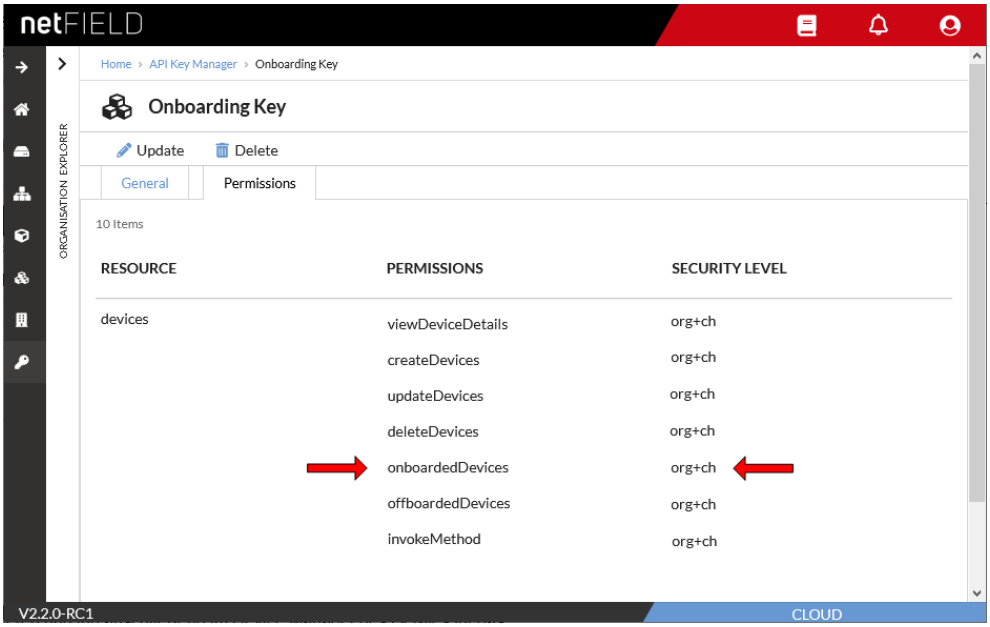


Figure 24: Example of an API Key permitting to onboard devices

- ➢ 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.

© Hilscher 2021

➢ In the **General** tab, click icon to copy the key to your clipboard:

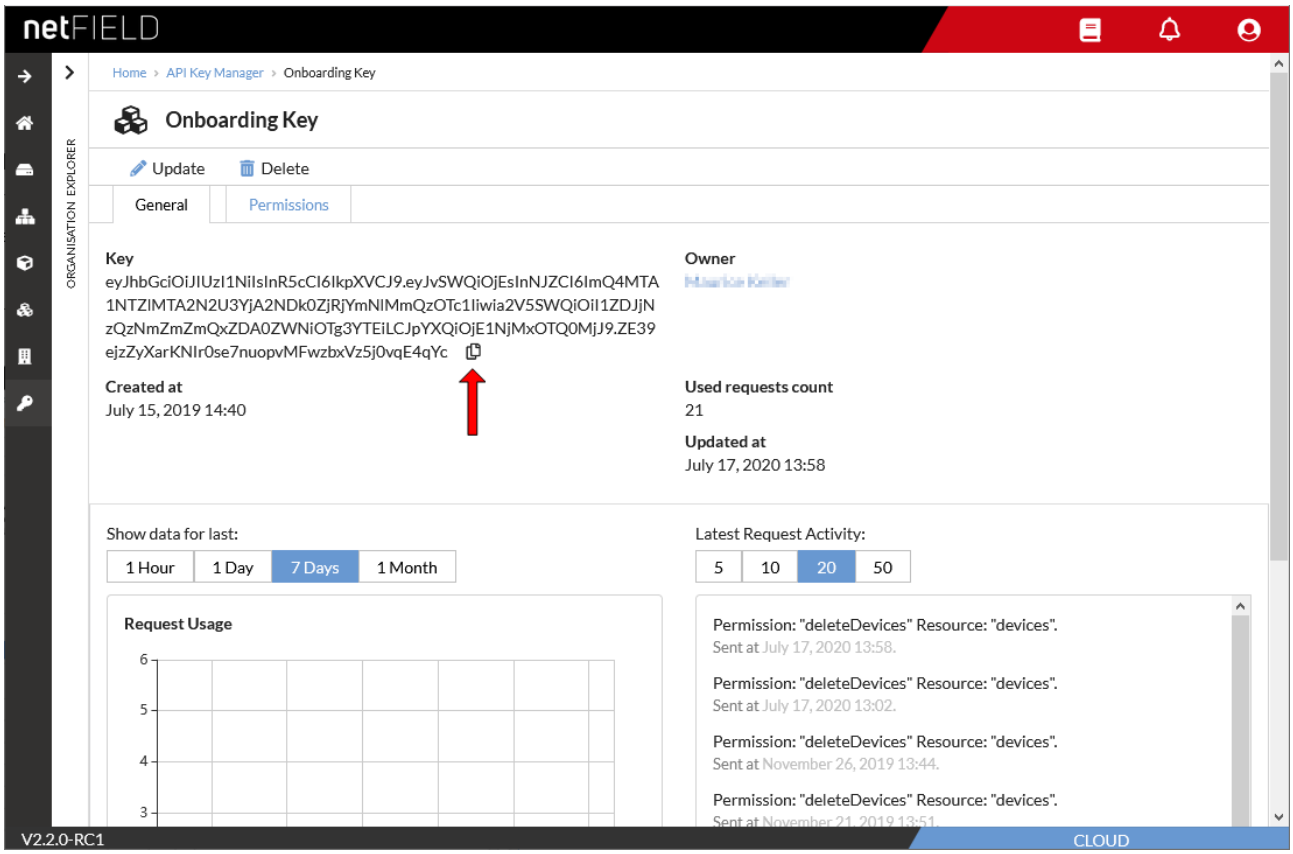


Figure 25: Copy key to clipboard

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

© Hilscher 2021

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

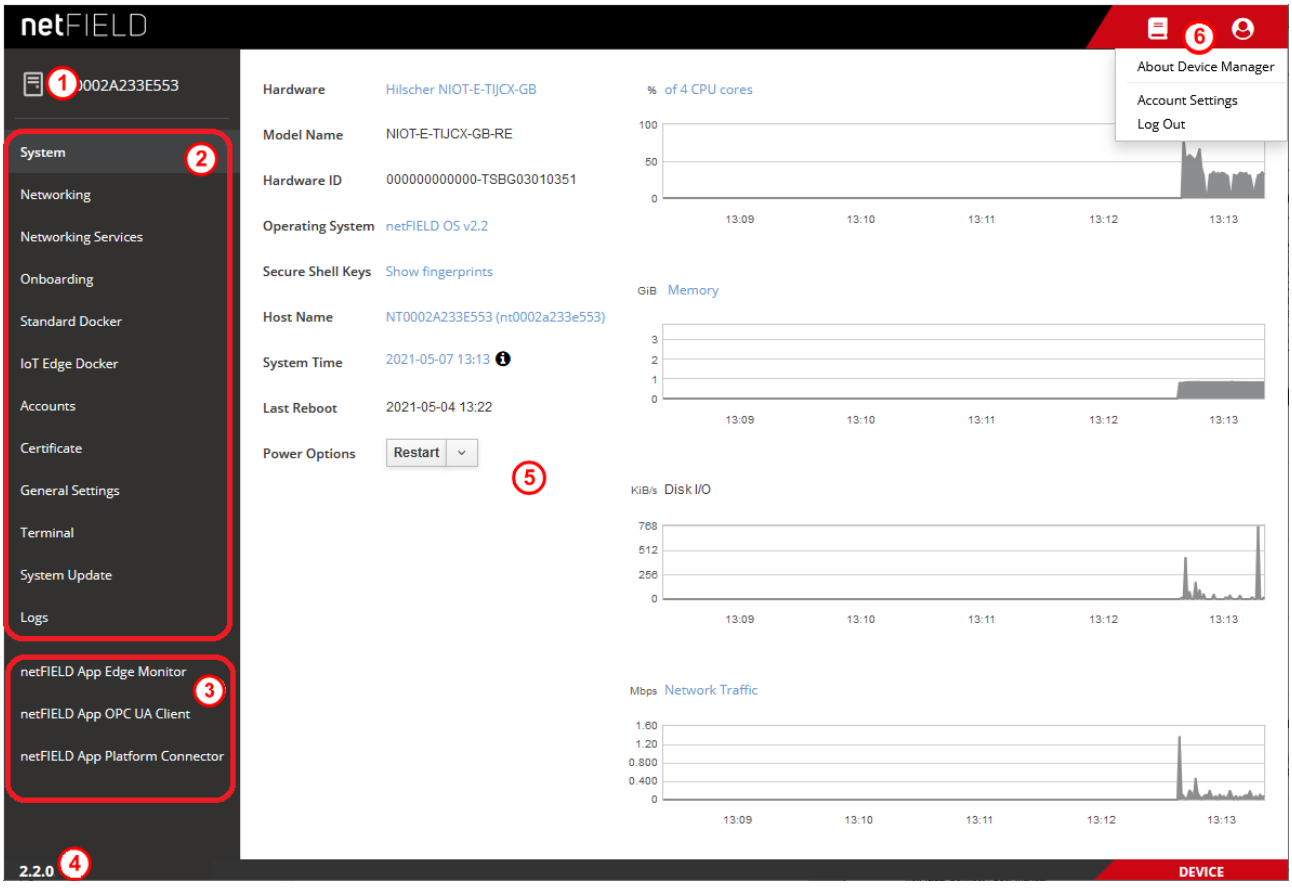


Figure 26: Overview Local Device Manager

(1) “Pretty” host name of the device (can be adapted by the user, see subsection *Host Name* in section *System* [page 52])

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

© Hilscher 2021

(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 108] section for further information.
  - **Log Out**: Logs you out of the Local Device Manager

© Hilscher 2021

6.2 System

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

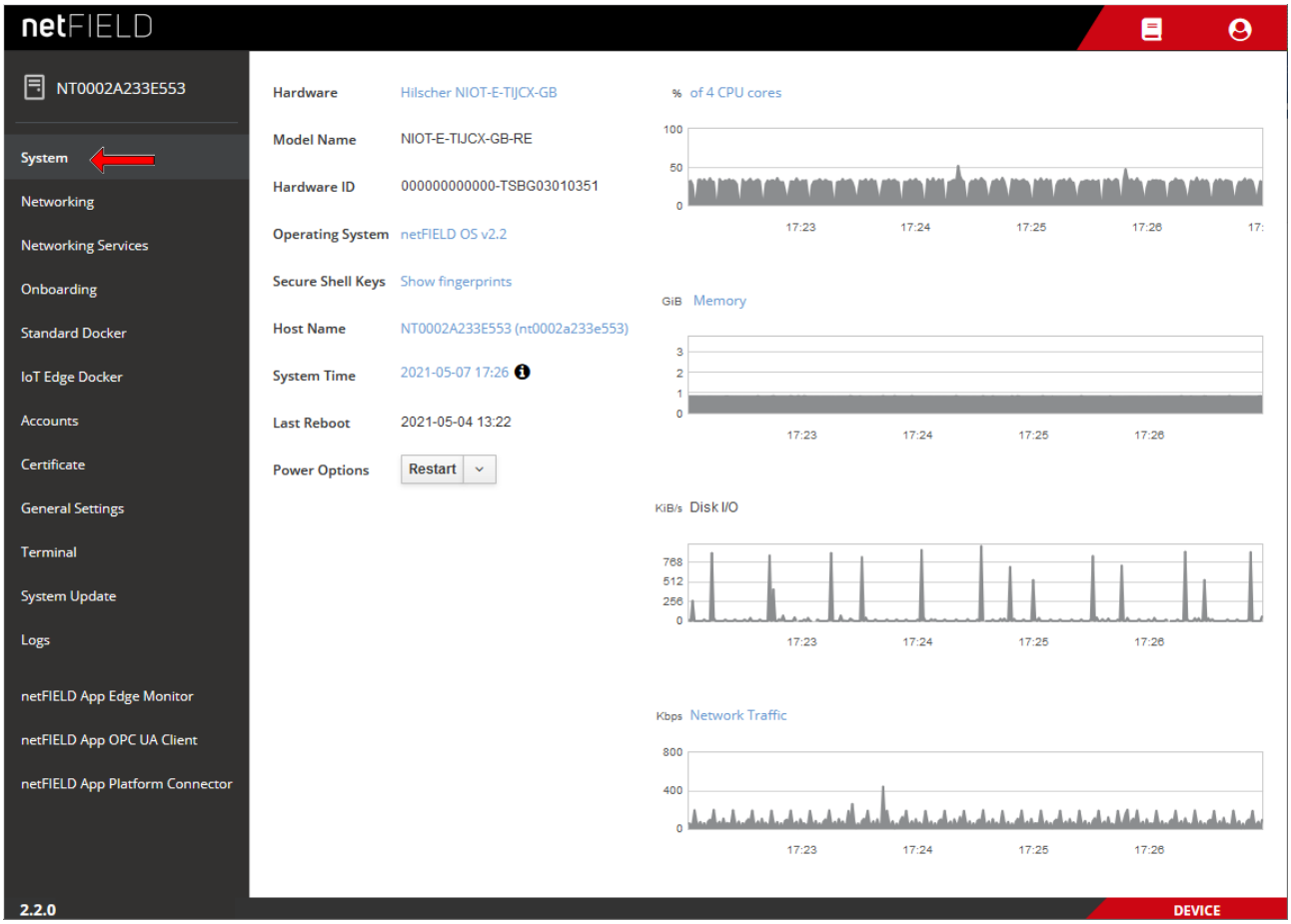


Figure 27: System page in Local Device Manager

Hardware

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

Model Name

Model name of the device

Hardware ID

Unique identification number of the device. To match the required format, the ID may be "filled up" with zeros. This ID 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).

© Hilscher 2021

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.

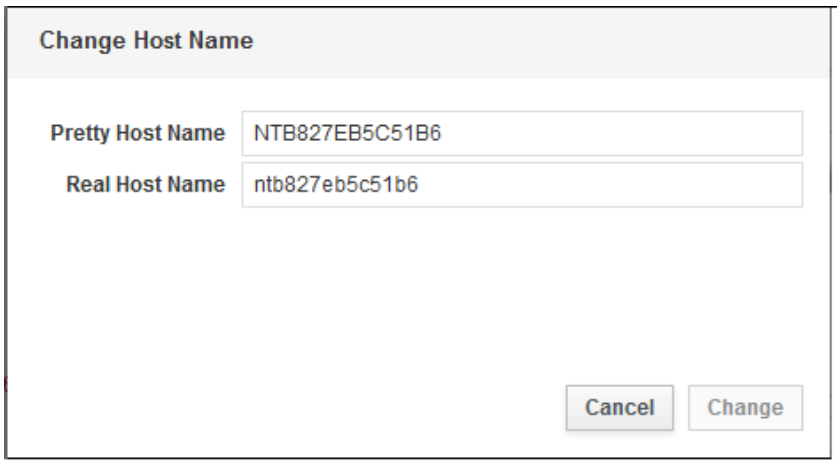


Figure 28: Change host name dialog

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 37].

Last Reboot

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

© Hilscher 2021

Power Options

Use the drop-down button to restart or shutdown the netFIELD OS and the device.
To restart the device after shutdown, press the power button (see position (12) in section *Positions of the interfaces* [page 14]).

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.

© Hilscher 2021

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.

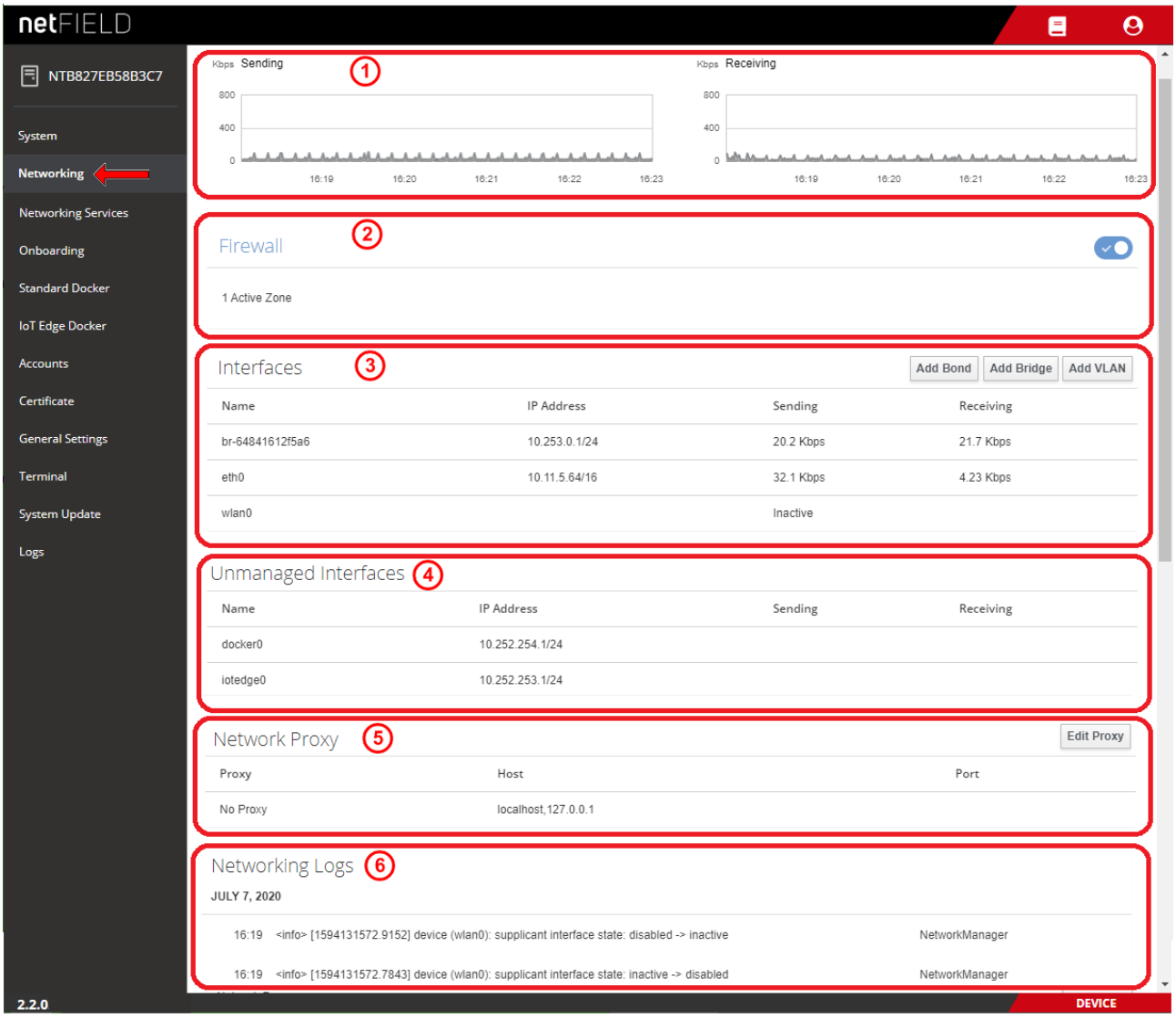


Figure 29: Networking page

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.

© Hilscher 2021

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 60] for more details.)

Interfaces

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

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

eth0: This is the port 1 LAN interface of the device (for the location of the LAN connector on the device, see position (7) in section *Positions of the interfaces* [page 14]).

eth1: This is the port 2 LAN interface of the device (see position (5) 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 76]).

cifx0: This is the Standard TCP/IP interface of the OT network connectors of the device (see positions (13) and (15) in section *Positions of the interfaces* [page 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 119].

© Hilscher 2021

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:

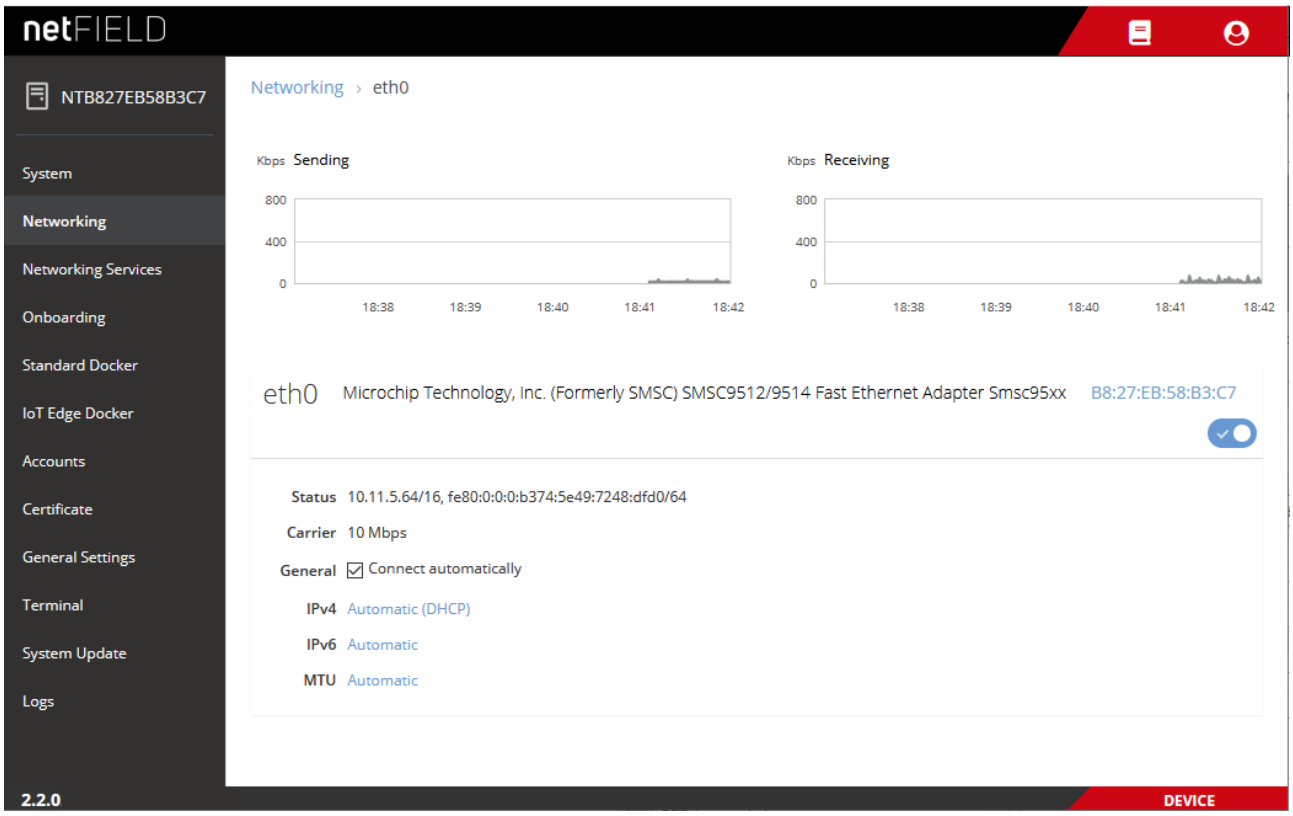


Figure 30: Details of LAN interface (eth0)

Important:
Be careful not to deactivate the **eth0** and the **eth1** LAN interfaces by switching them off with the toggle switch. Once you have deactivated an interface, the connection to your device via this interface will be lost. If you have deactivated both LAN interfaces (and if you cannot reach the device via Wi-Fi), you will have to perform either a device recovery in order to be able to reconnect again (see section *Device recovery via USB* [page 129]), 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**.

© Hilscher 2021

The **IPv4 Settings** page opens.

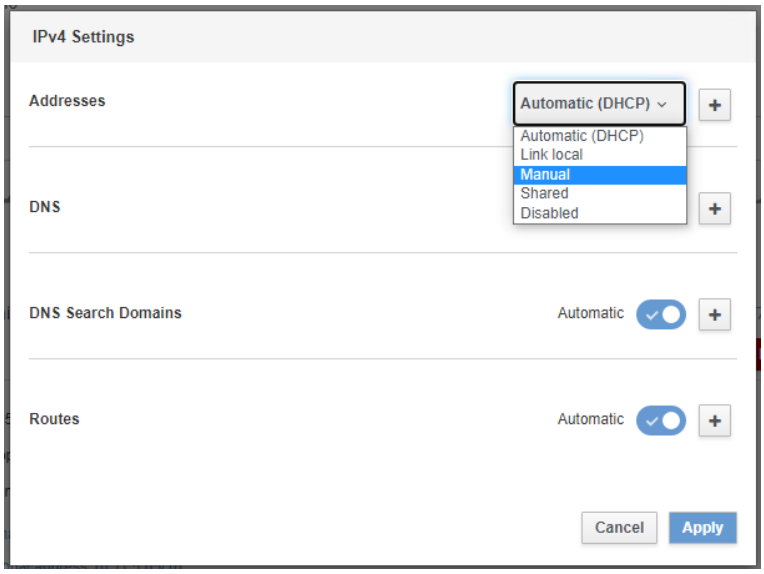


Figure 31: IPv4 Settings

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

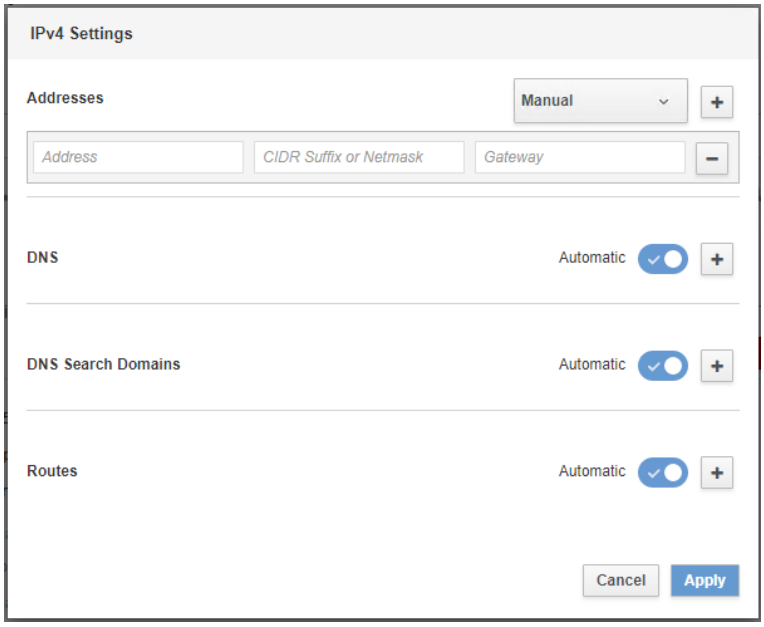


Figure 32: Manual IPv4 Settings

➢ 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
- **Iotedge0**: 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.

© Hilscher 2021

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 (**Iotedge0**), e.g. because it conflicts with other IP addresses in your company network, see section *Docker Network Settings* [page 116] 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 69] for more information.)

NETWORKING LOGS

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

© Hilscher 2021

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.

© Hilscher 2021

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

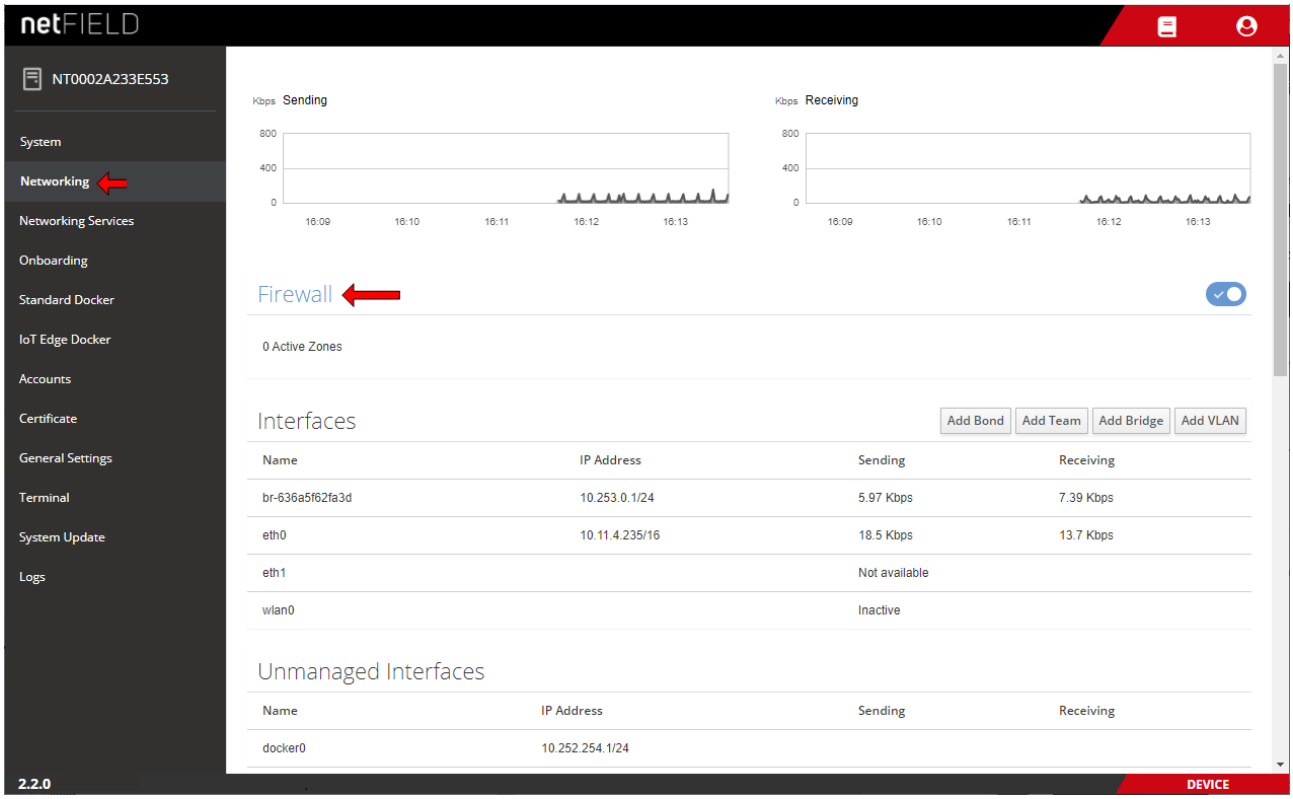


Figure 33: Open Firewall configuration page

➢ The Firewall configuration page opens:

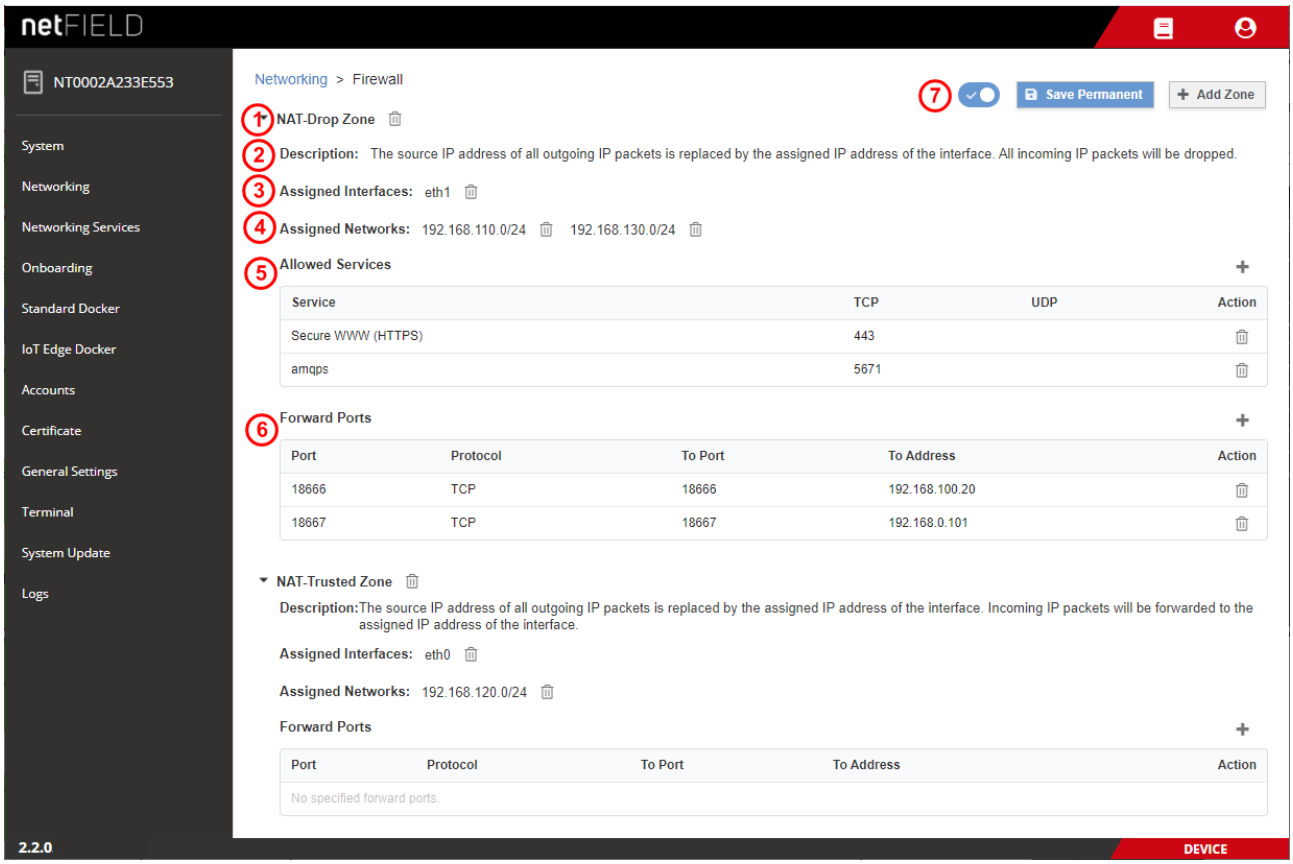


Figure 34: Elements on Firewall configuration page

© Hilscher 2021

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 13: Available Firewall zones

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

© Hilscher 2021

The **Add Zone** dialog opens:

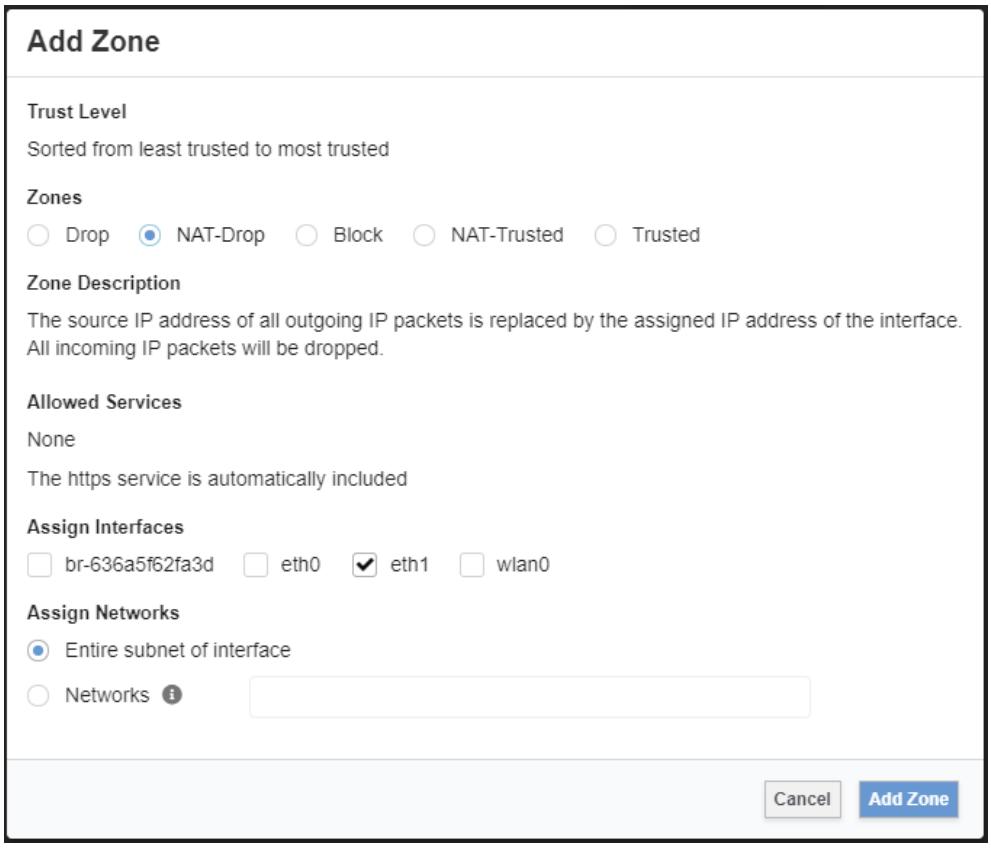


Figure 35: Add Zone dialog

Element	Description	
Trust Level	Explains the sorting of the zones under **Zones**	
Zones	Select here the zone that you want to add to your firewall configuration. If you want to assign **Interfaces** or **Networks** 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 **Allowed Services** table of the corresponding zone.	
Assign Interfaces	Select here the physical or virtual interface(s) that you want to assign to the selected zone. Note that each interface can be assigned to one zone only. Interfaces that have already been assigned to a different zone are not displayed here and thus cannot be selected here. If you want to reassign an interface from one zone to another, you will first have to remove the interface from the zone to which it is currently belonging.	
Assign Networks	Here you can define subnets or IP address ranges for which the rules of the zone shall apply.	
	Entire subnet of interface	Select this option if the rules shall apply to the entire subnet(s) of the assigned interface(s).
	Networks	Select this option to enter address ranges or subnets for which the rules of the zone shall apply. Enter the subnet mask as CIDR Suffix. Multiple entries must be separated with commas, e.g.: `192.168.1.0/24,10.14.0.0/16`

Table 14: Elements in Add Zone dialog

© Hilscher 2021

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.

© Hilscher 2021

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. **Note**: Deleting an allowed service/port from a Drop Zone, NAT-Drop Zone or Block Zone can cause loss of connection to your device (if the interface via which you are connected belongs to such a zone).

Table 15: Columns/elements in Allowed Services table

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

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

© Hilscher 2021

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

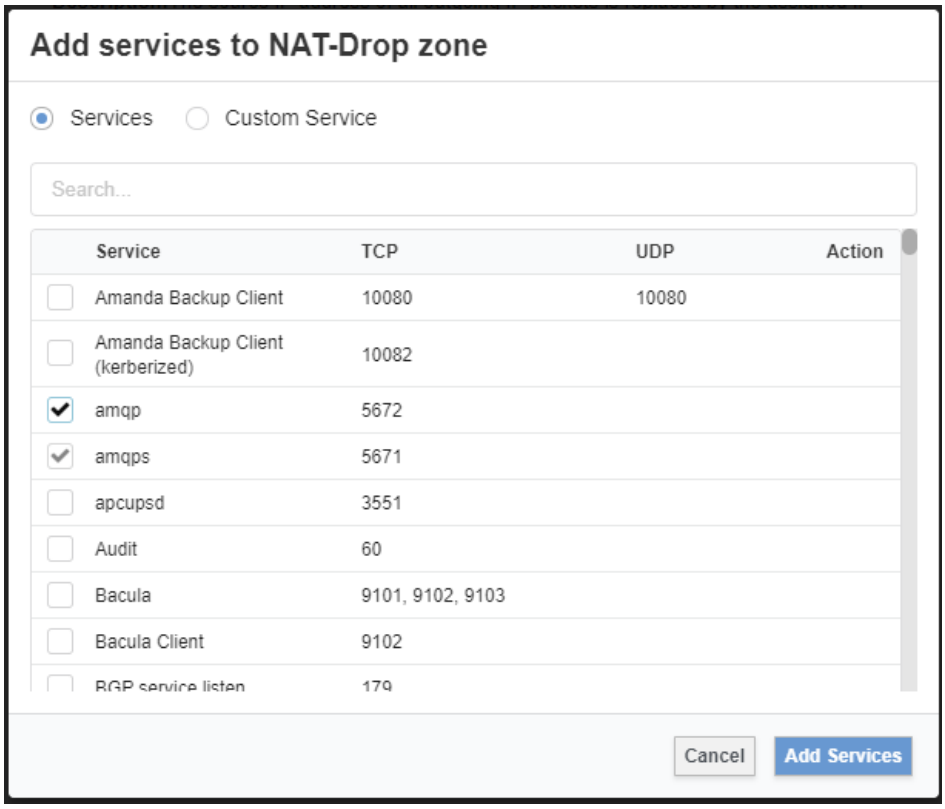


Figure 36: Add services

- 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.

© Hilscher 2021

➢ 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.

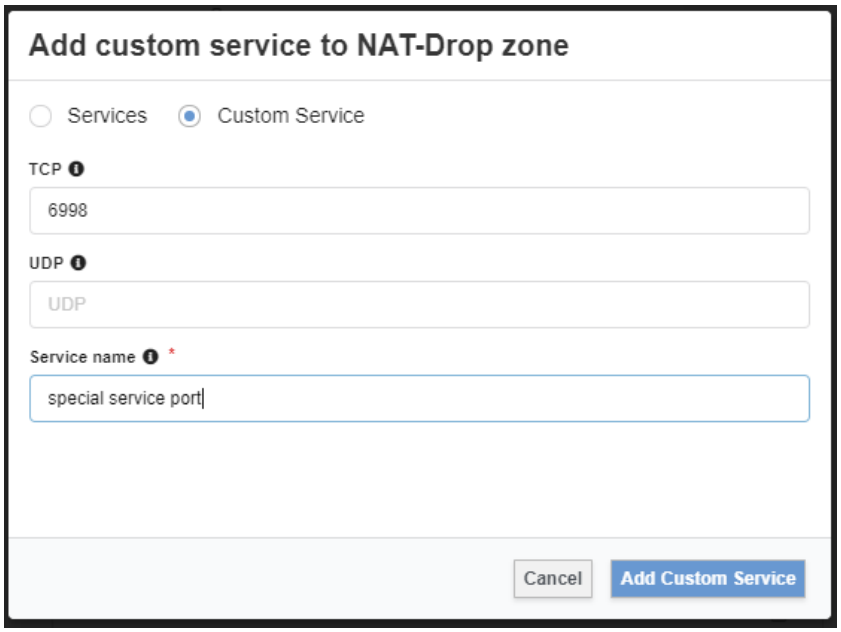


Figure 37: Add custom services dialog

➢ 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 16: Columns/elements in Forward Ports table

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

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

© Hilscher 2021

The **Add Forward Port** dialog opens:

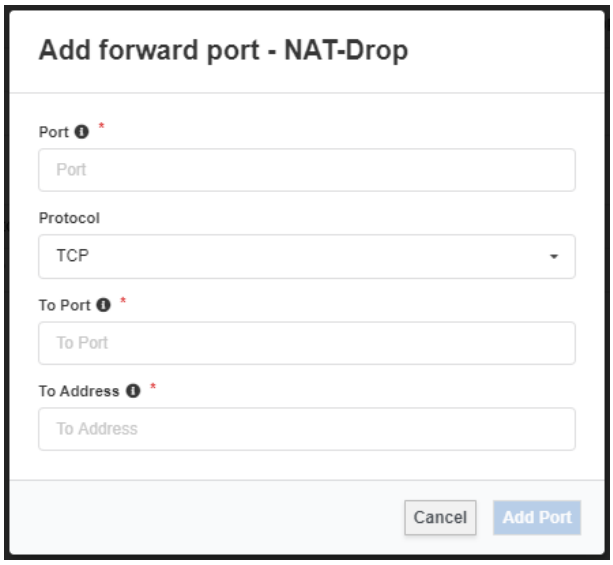


Figure 38: Add forward port dialog

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

Table 17: Control elements in main toolbar

© Hilscher 2021

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.

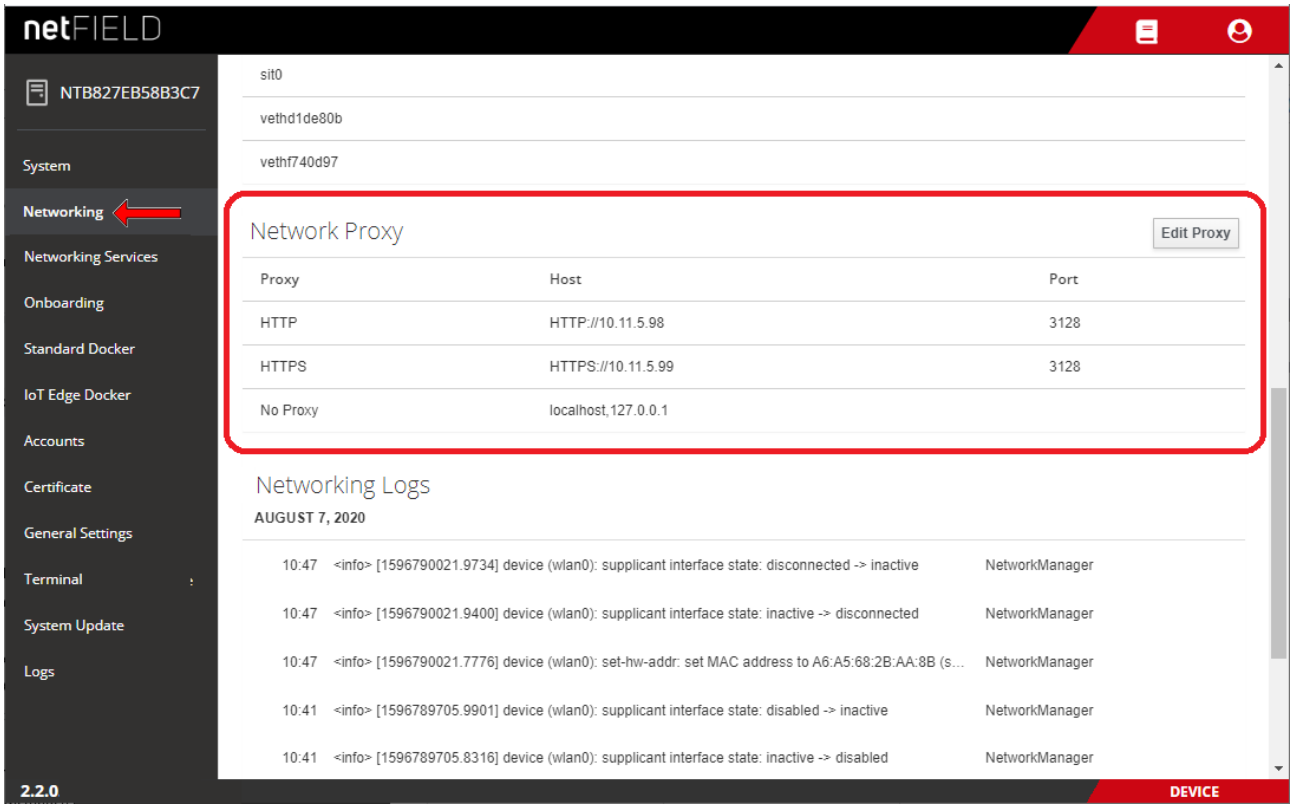


Figure 39: Network Proxy configuration

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.

© Hilscher 2021

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:

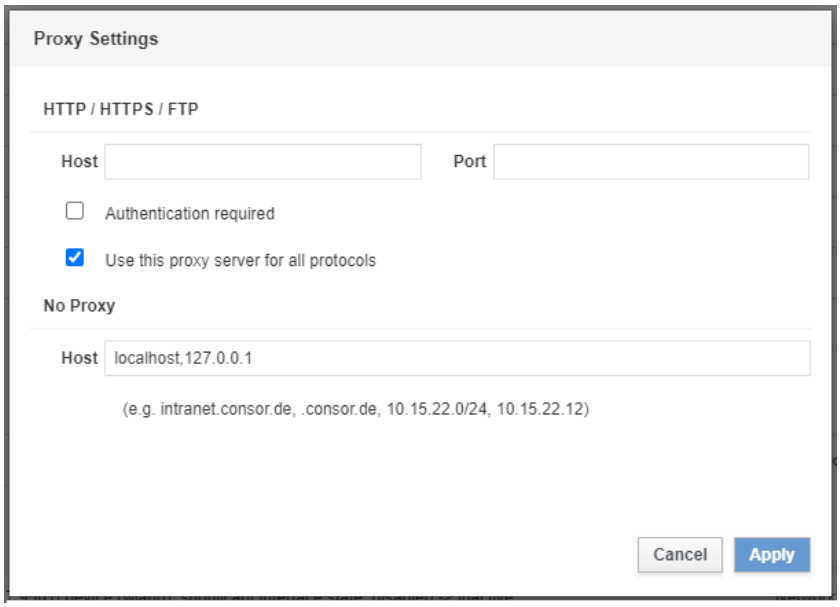


Figure 40: Proxy Settings dialog window

© Hilscher 2021

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.

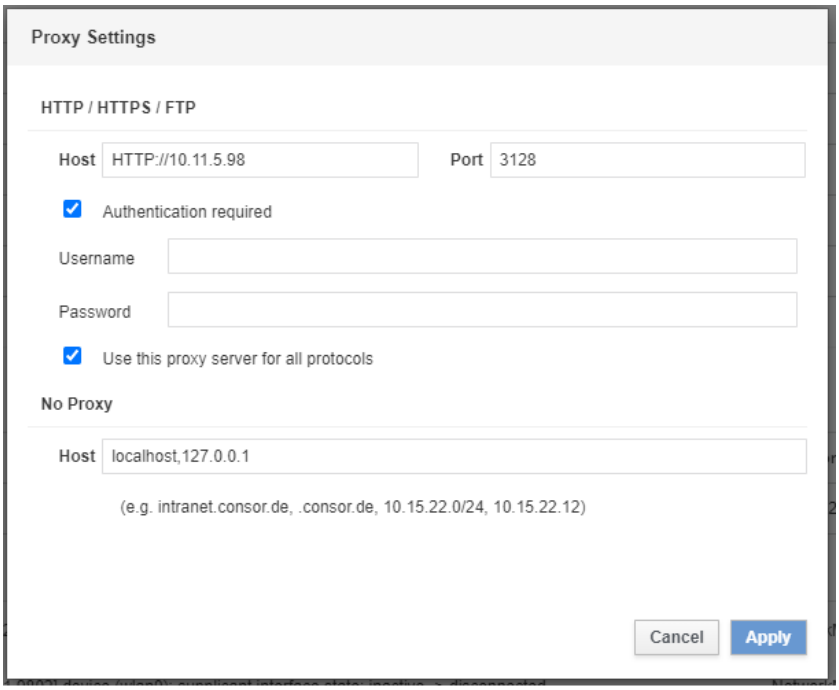


Figure 41: Using one Proxy server for all protocols

➢ 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.

© Hilscher 2021

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:

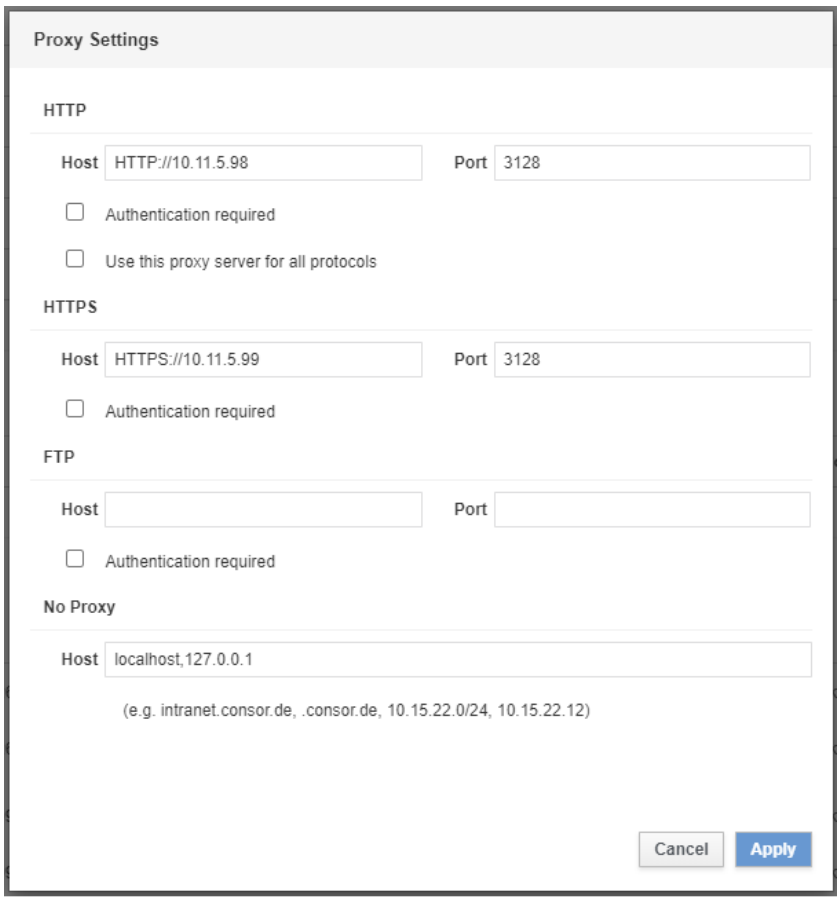


Figure 42: Separate HTTP/HTTPS/FTP configuration

➢ Enter the parameters of the individual proxy servers.

© Hilscher 2021

Saving and restarting

➢ To save your new proxy server configuration, click **Apply** button.

↬ The following dialog appears:

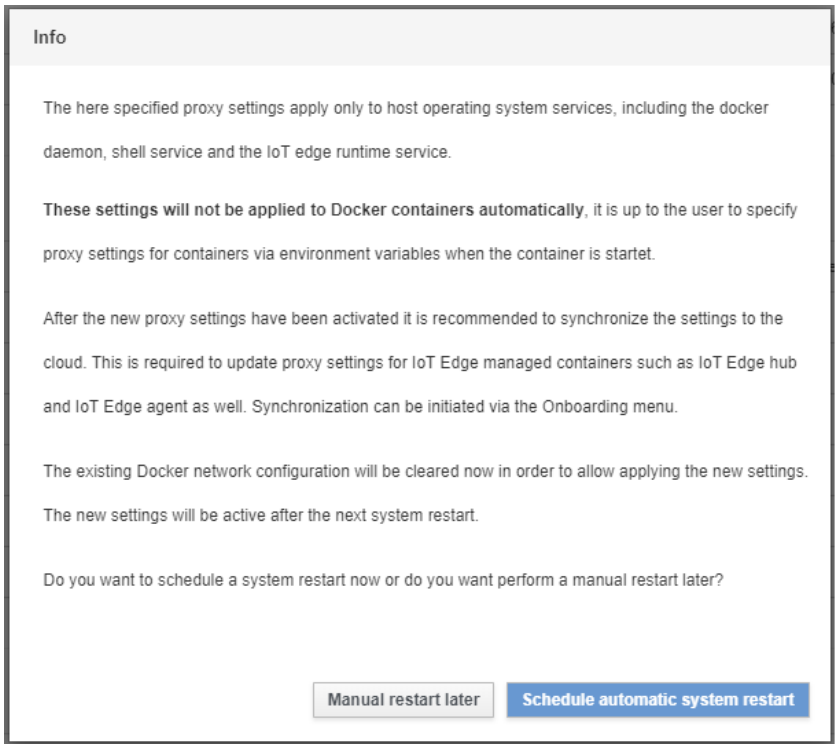


Figure 43: Restart dialog after changing proxy server configuration

➢ 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.

© Hilscher 2021

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).

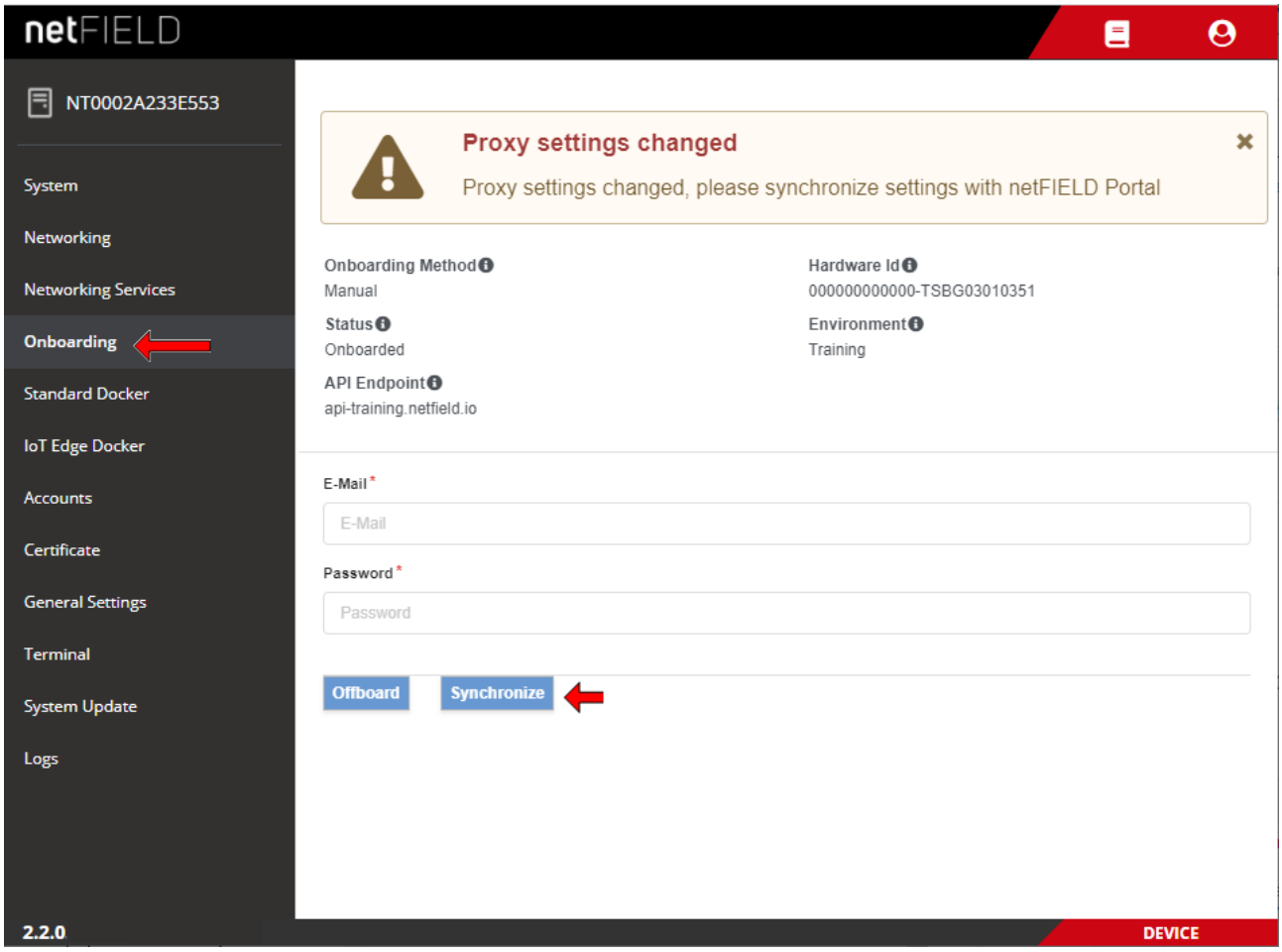


Figure 44: Synchronize proxy settings with netFIELD Portal

➢ 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.

© Hilscher 2021

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.

© Hilscher 2021

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 60]).

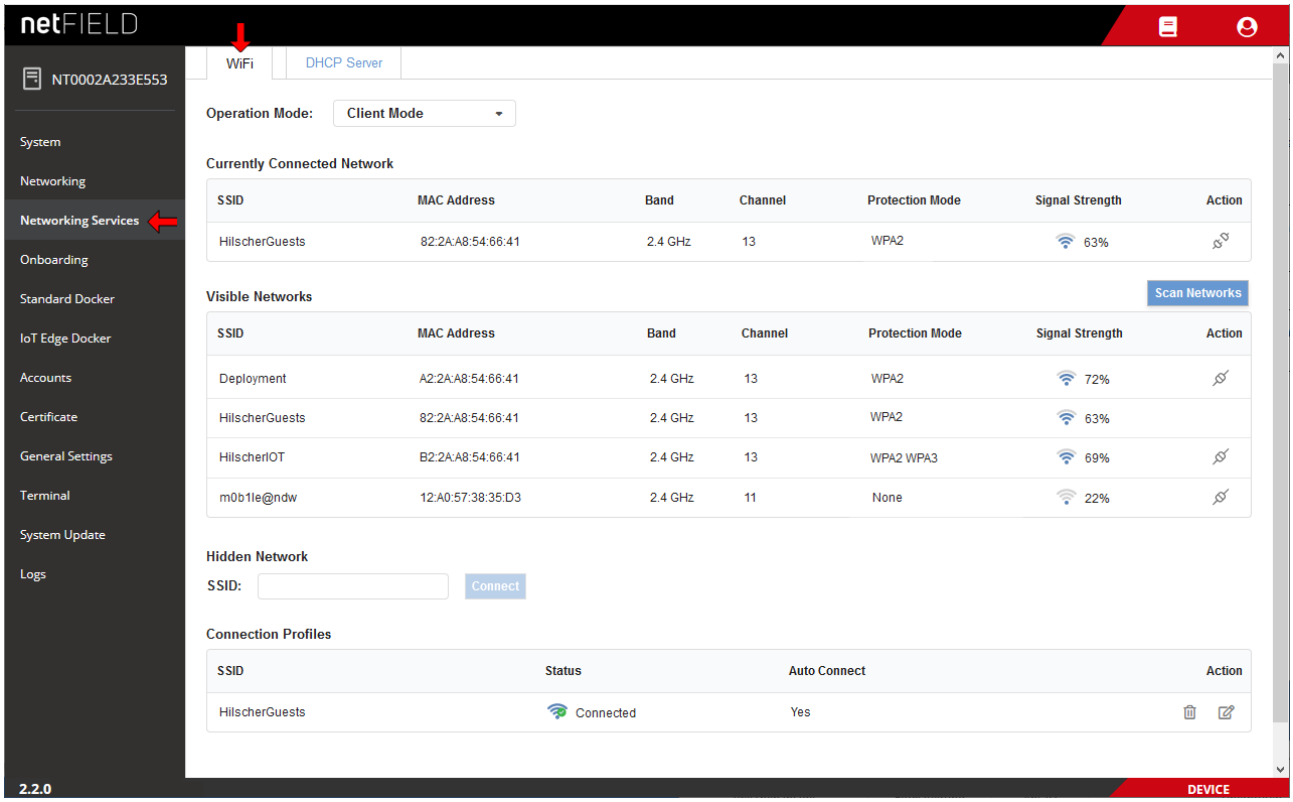


Figure 45: Wi-Fi Client Mode

© Hilscher 2021

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 *Client mode* [▷ page 78] for details.	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. On the **Networking** > **Interfaces** > **wlan0** page, the **Status** parameter shows the IPv4 and IPv6 addresses assigned to the interface by the DHCP server. **Note**: If you want to manually assign a fixed IP address, click on **Automatic (DHCP)** to open the **IPv4 Settings** dialog.
Access Point Mode	In this mode, the Wi-Fi interface (**wlan0**) of your device establishes a BSS (Basic Service Set) in the 2.4 GHz band, protected by WPA-PKS. Other Wi-Fi-capable can connect to it by using the Pre-shared Key (PKS). See section *Access Point mode* [▷ page 84] for details.	After saving the Access Point configuration, the **IPv4** address configuration of the **wlan0** interface is by default set to *Link local*. On the **Networking** > **Interfaces** > **wlan0** page, the **Status** 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). **Note**: 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 **Link local** to open the **IPv4 Settings** dialog.

Table 18: Wi-Fi operating modes

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

© Hilscher 2021

6.4.1.2 Client mode

After selecting **Client Mode** in the **Operation Mode** dropdown list, the device automatically scans its environment for “visible” Wi-Fi networks.

After scanning, you can connect to a visible network by clicking the button in the **Action** column.

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

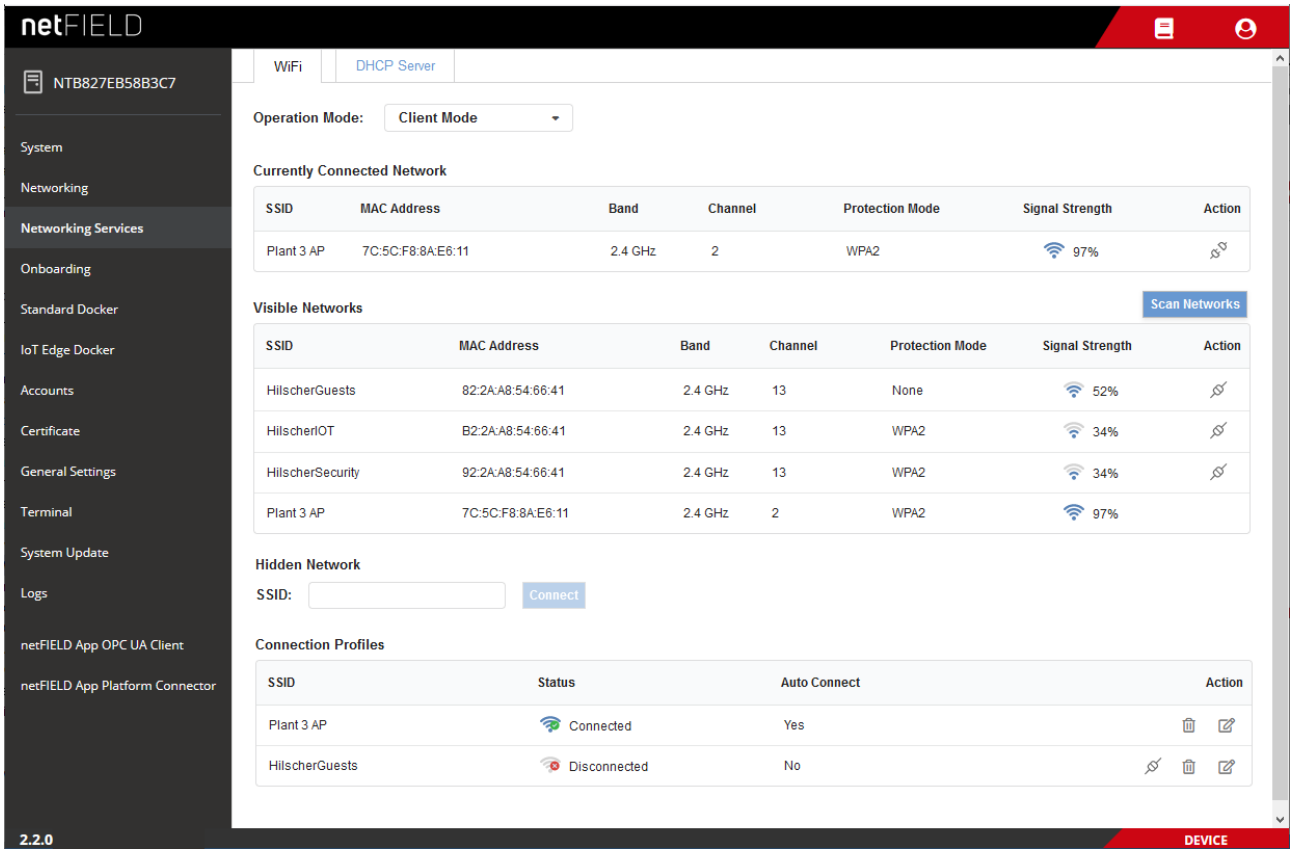


Figure 46: Client mode parameters

© Hilscher 2021

Currently Connected Network

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

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

Table 19: Currently Connected Network

Visible Networks

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

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

Table 20: Visible Networks

© Hilscher 2021

Connect Network dialog

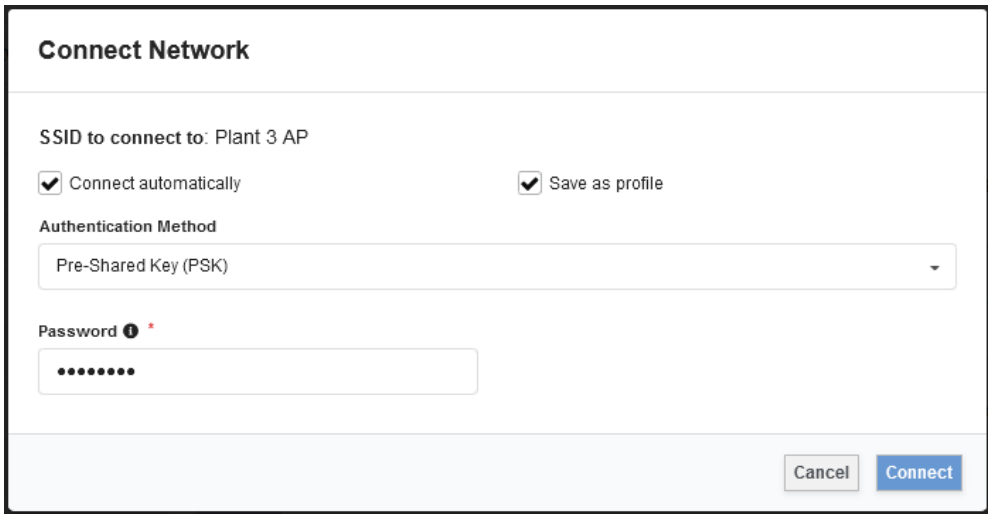


Figure 47: Connect Network dialog

Parameter	Description		
Connect automatically	If you select this option, the device tries to automatically connect to this network each time after enabling the **Client mode**.		
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 **Connection Profiles** 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. **Note**: 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. **Note**: 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). **Note**: The certificate must be stored in the `/etc/wifi-certs/` directory of the netFIELD OS. If not available, authentication will not be verified.

Table 21: Parameters in Connect Network dialog (1)

© Hilscher 2021

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). **Note**: The certificate must be stored in the `/etc/wifi-certs/` directory of the netFIELD OS.
		Client Private Key File	Client Private Key File. **Note**: The private key file must be stored in the `/etc/wifi-certs/` directory of the netFIELD OS.
		CA Certificate File	Root certificate of the Certification Authority that shall be used for authentication (optional). **Note**: The certificate must be stored in the `/etc/wifi-certs/` 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). **Note**: The certificate must be stored in the `/etc/wifi-certs/` 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. **Note**: Establishing a new connection automatically terminates other current Wi-Fi network connections.		

Table 22: Parameters in Connect Network dialog (2)

© Hilscher 2021

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

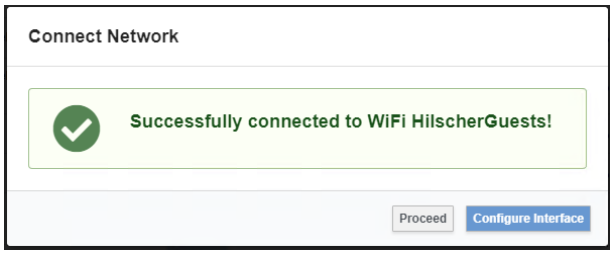


Figure 48: Connect network message

➢ 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.

© Hilscher 2021

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 **Client mode** has been enabled. **Note**: 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. **Note**: Establishing a new connection automatically terminates other current Wi-Fi network connections.
		Delete this profile.
		Edit this profile.

Table 23: Connection Profiles

© Hilscher 2021

6.4.1.3 Access Point mode

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

The Access Point configuration parameters are displayed:

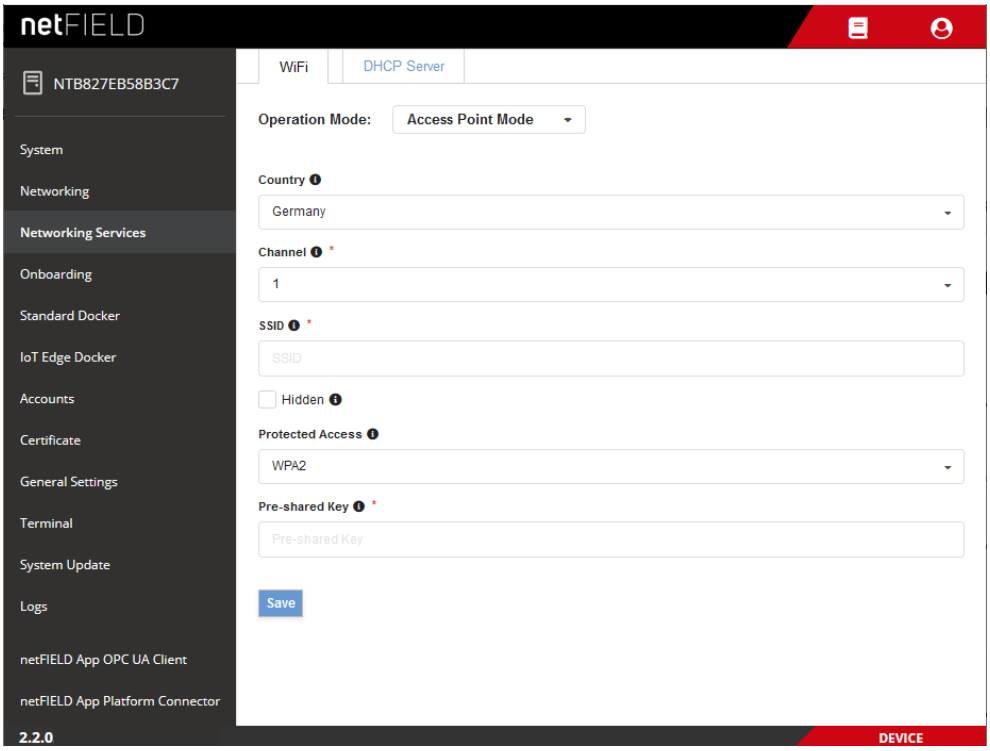


Figure 49: Access Point Mode

Parameter	Description
Country	In the drop-down list, select the country in which your device is operated. **Important**: 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 *WPA-Personal* (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 24: Access Point parameters

© Hilscher 2021

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).

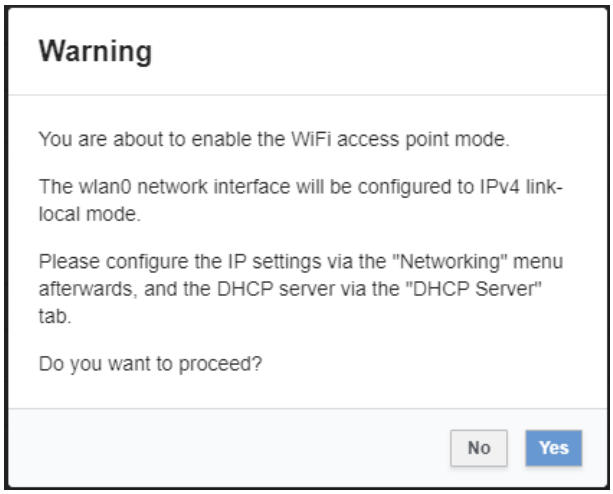


Figure 50: Warning note

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:

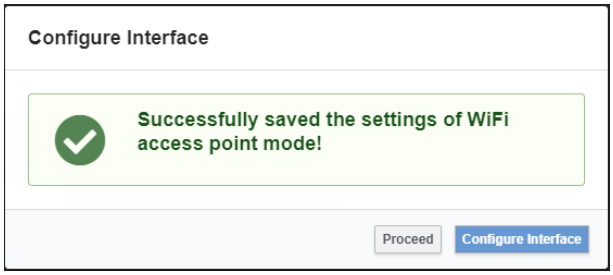


Figure 51: Configure Interface message

➢ 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**).

© Hilscher 2021

➢ 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.

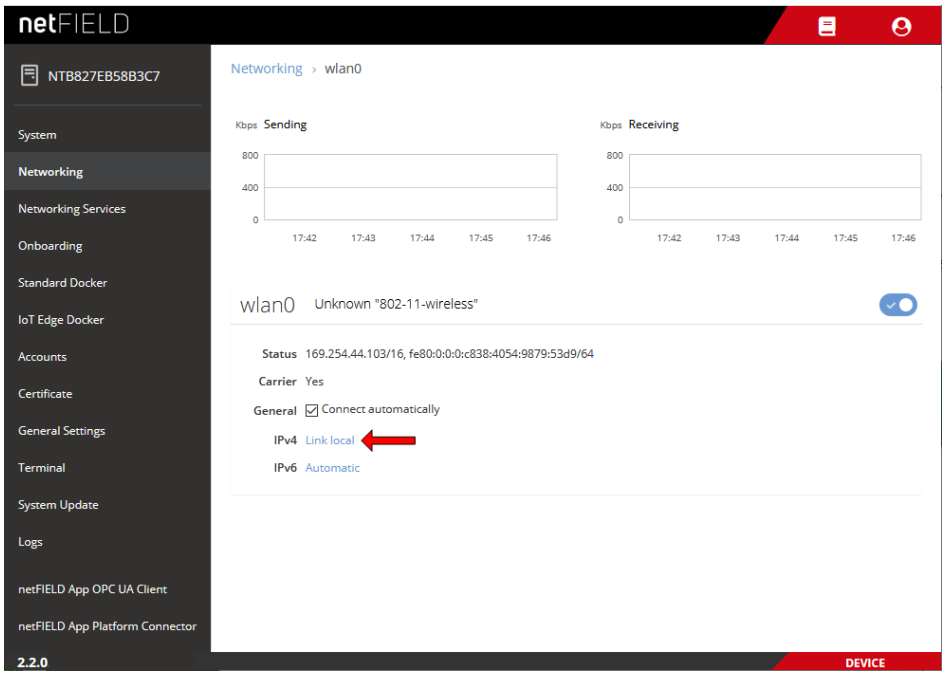


Figure 52: wlan0 configuration page

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

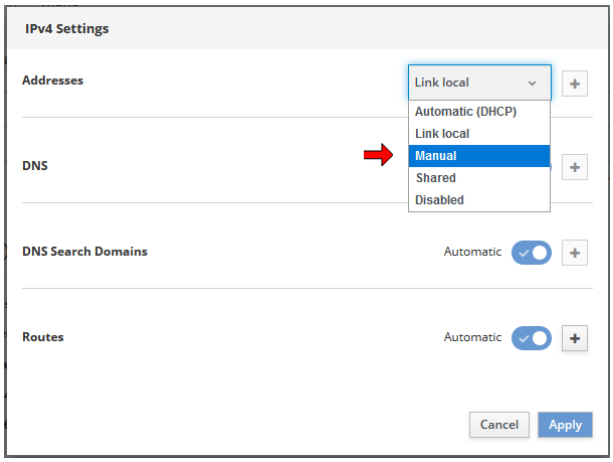


Figure 53: Set manual address in IPv4 Settings dialog

© Hilscher 2021

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

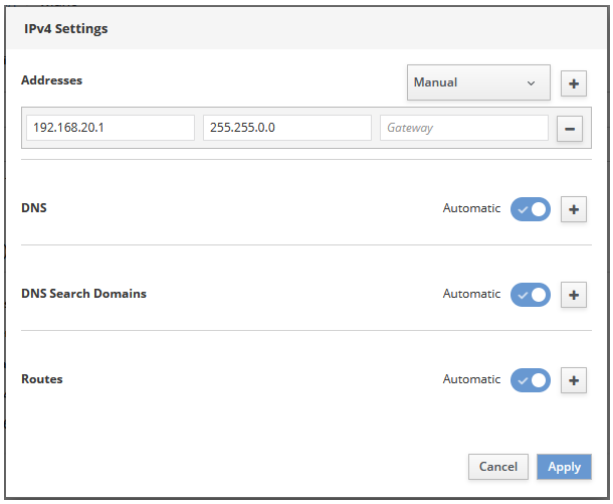


Figure 54: Enter Manual IP Address

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).

© Hilscher 2021

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** and **eth1** Ethernet interfaces of the device is not yet supported by the current netFIELD OS.

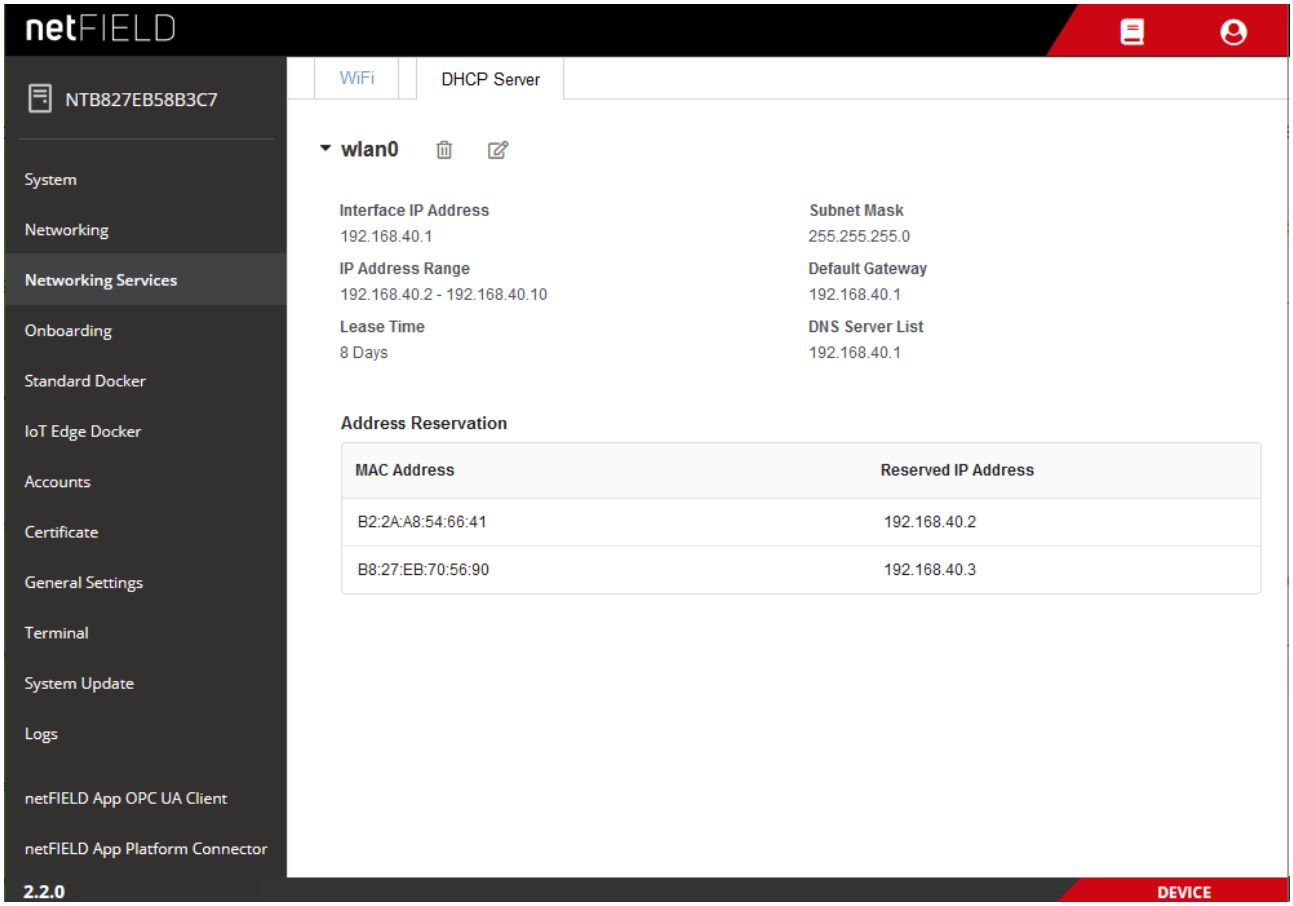


Figure 55: Configured DHCP service

Element/Parameter	Description
	Click here to delete the DHCP Server configuration.
	Click here to open the **DHCP Server Configuration** 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. **Note**: IP address settings of the wlan0 interface must be defined under **Networking** > **Interfaces** > **wlan0**.
Subnet Mask	Subnet mask of your wlan0 interface/access point (which is also the subnet of your Wi-Fi network). **Note**: The IP address settings of the wlan0 interface can be defined under **Networking** > **Interfaces** > **wlan0**.
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.

© Hilscher 2021

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 25: 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**.

© Hilscher 2021

DHCP Server Configuration dialog

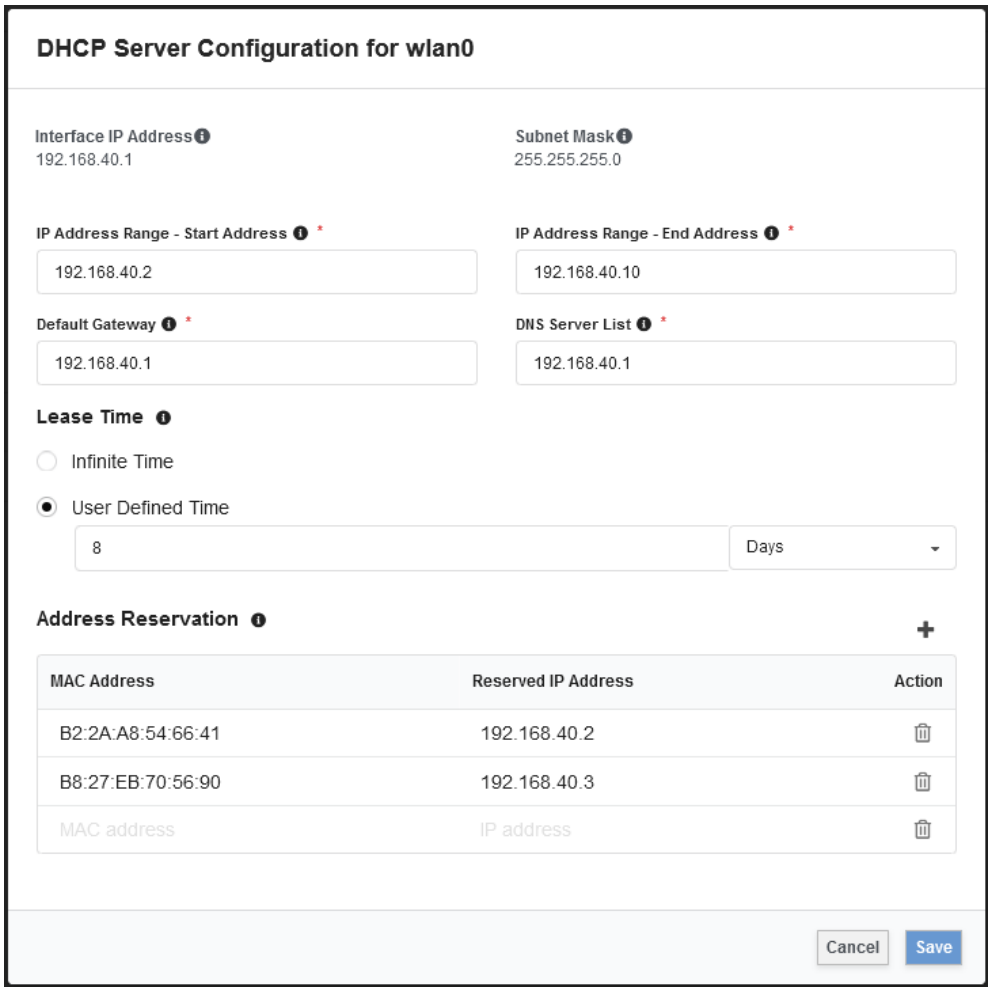


Figure 56: DHCP Server Configuration dialog

Parameter	Description
Interface IP address	IP address of your wlan0 interface/access point. **Note**: IP address settings of the wlan0 interface must be defined under **Networking** > **Interfaces** > **wlan0**.
Subnet Mask	Subnet mask of your wlan0 interface/access point (which is also the subnet of your Wi-Fi network). **Note**: The IP address settings of the wlan0 interface must be defined under **Networking** > **Interfaces** > **wlan0**.
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.

© Hilscher 2021

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	Here you can ensure that certain client devices will always receive the same IP address when they request a lease. Click the **+** symbol above **Action** to add a reservation. To delete a reservation, click the symbol. In the **MAC Address** 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 **Reserved IP Address** field.	
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 26: Parameters of DHCP Server Configuration dialog

© Hilscher 2021

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 39]. 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 69] for further information.)

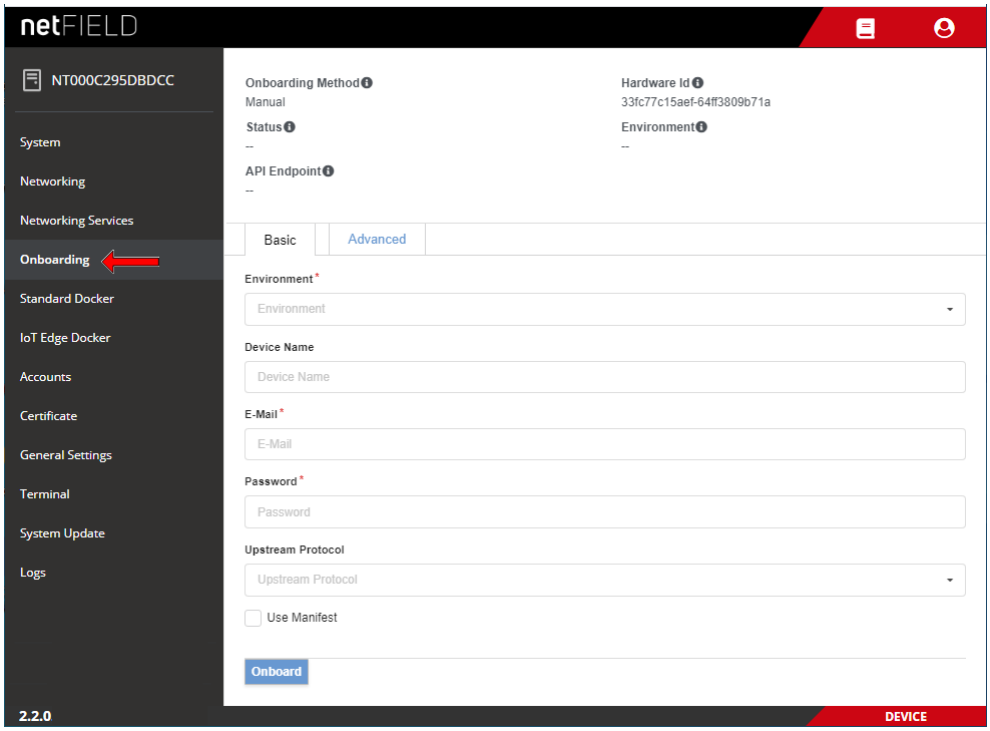


Figure 57: Basic Onboarding page

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**:

© Hilscher 2021

Offboarding after having used the Basic Onboarding method

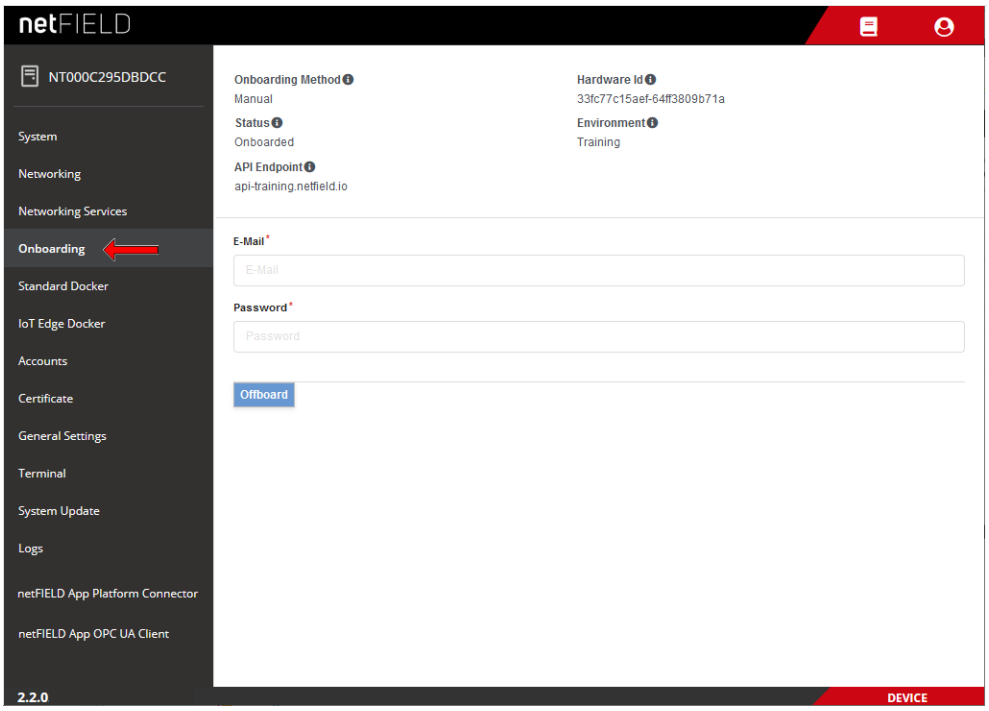


Figure 58: Offboarding "Basic"

- 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

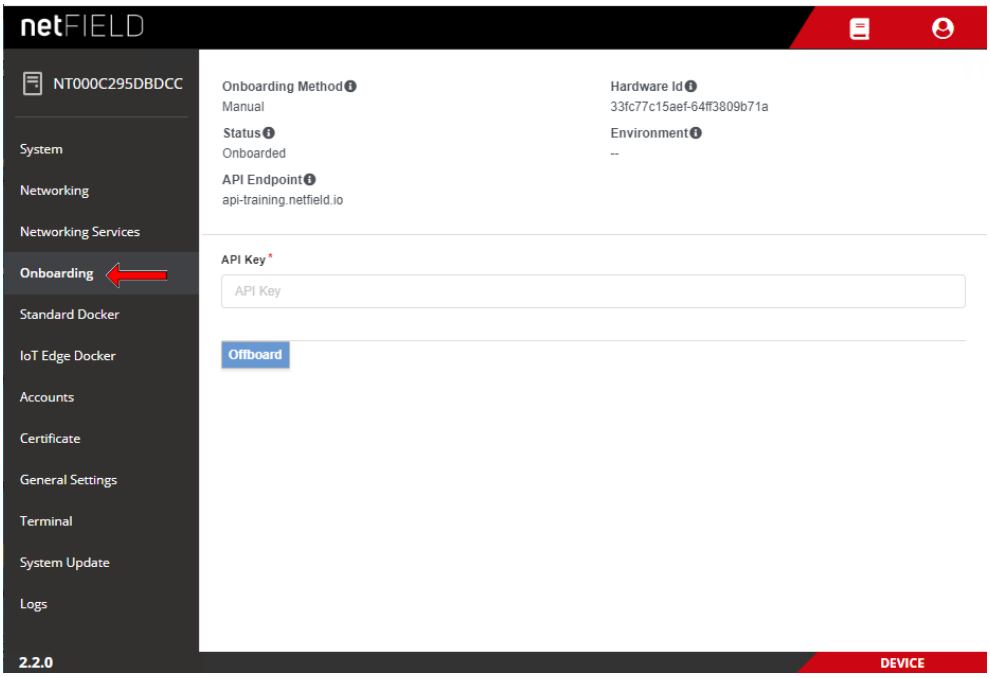


Figure 59: Offboarding "Advanced"

© Hilscher 2021

- 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.

© Hilscher 2021

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 116]).

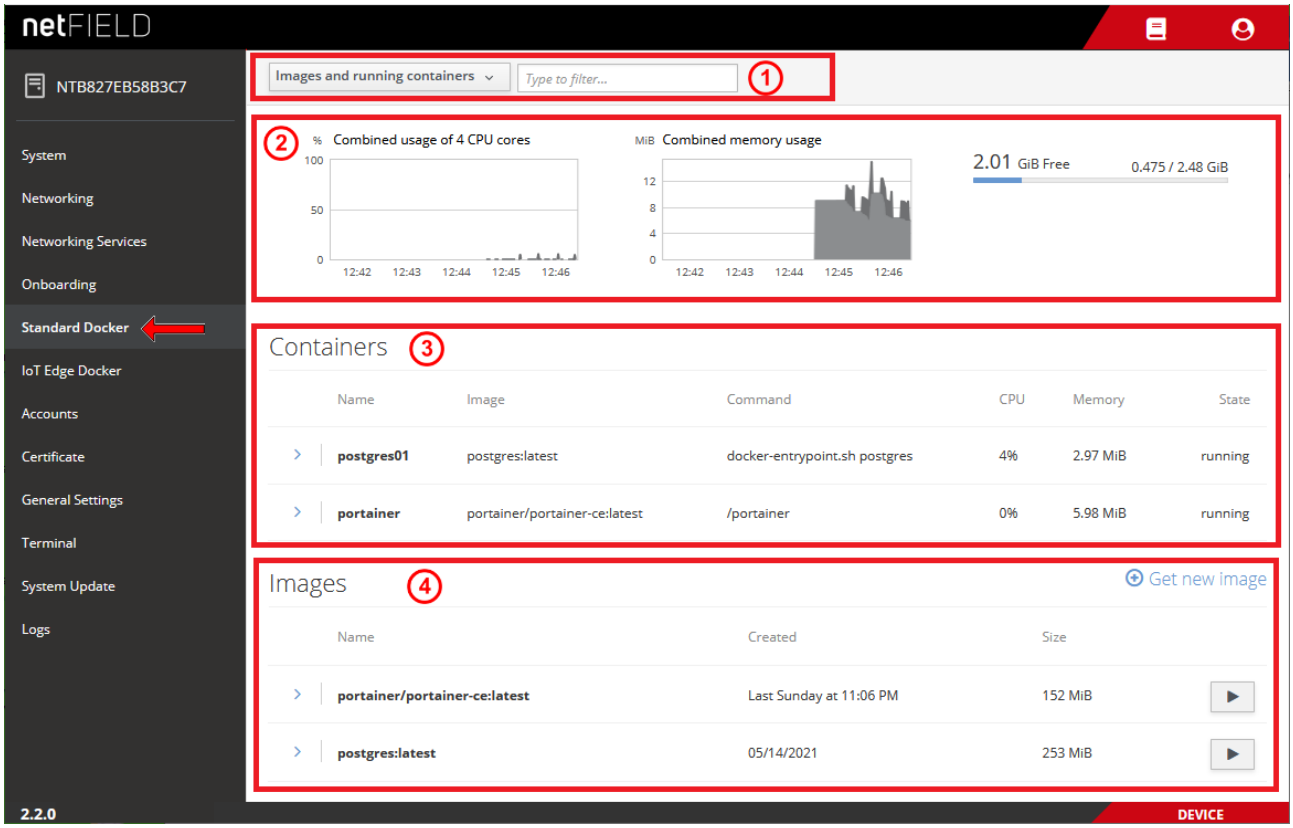


Figure 60: Standard Docker

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.

© Hilscher 2021

Graphs

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

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

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

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

Containers

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

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

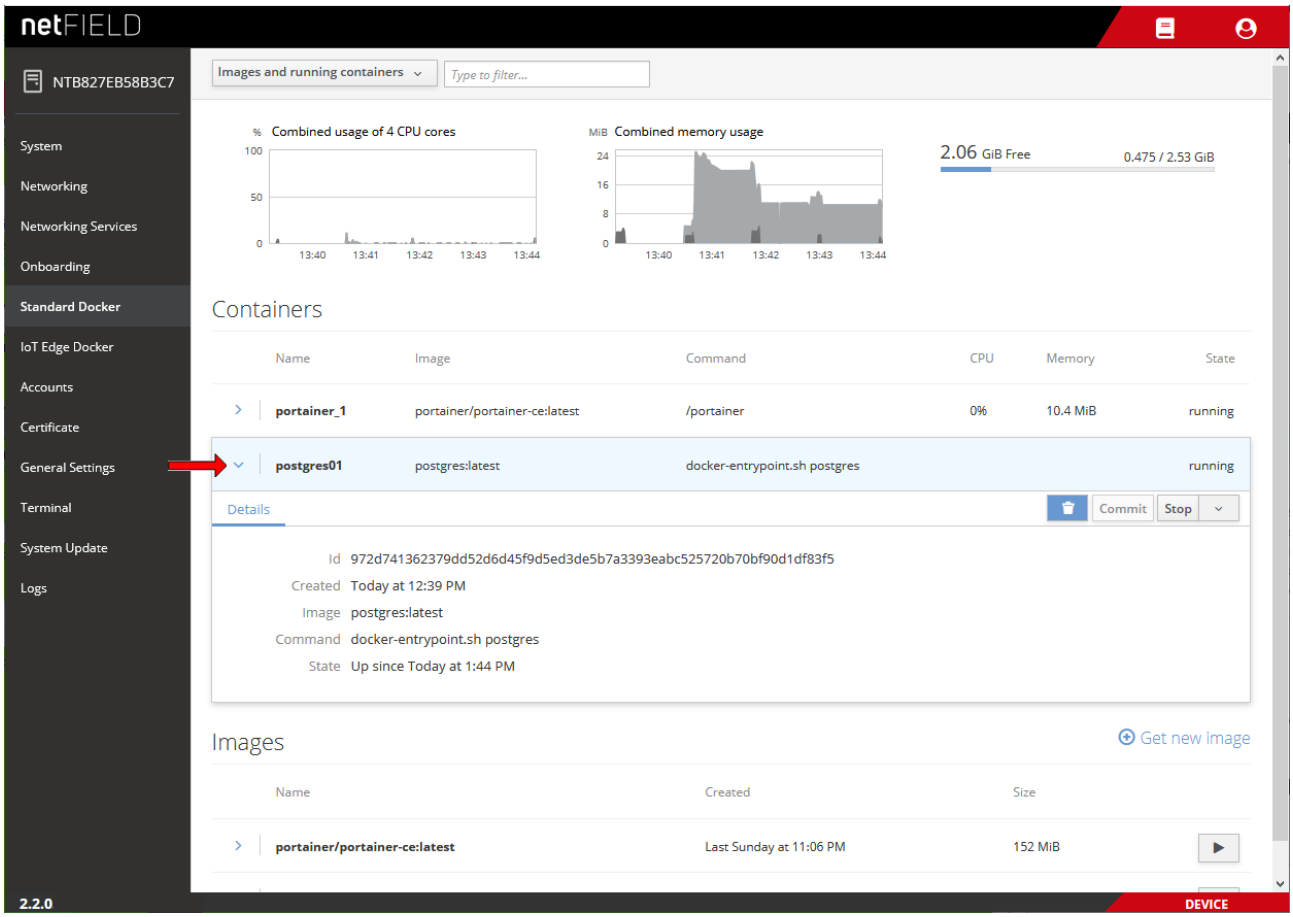


Figure 61: Expand concise container details

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

© Hilscher 2021

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:

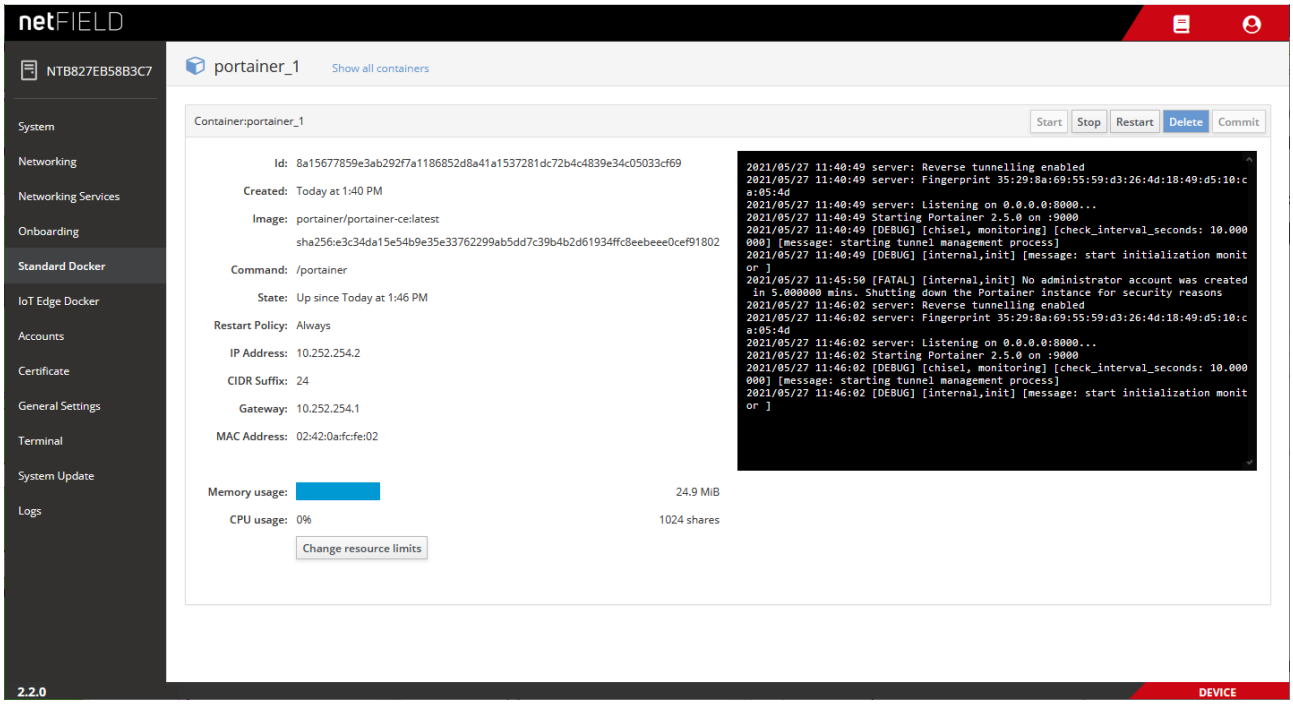


Figure 62: Container parameters with terminal window

➢ 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.

© Hilscher 2021

↬ The **Image Search** dialog opens, allowing you to search the Docker Hub registry:

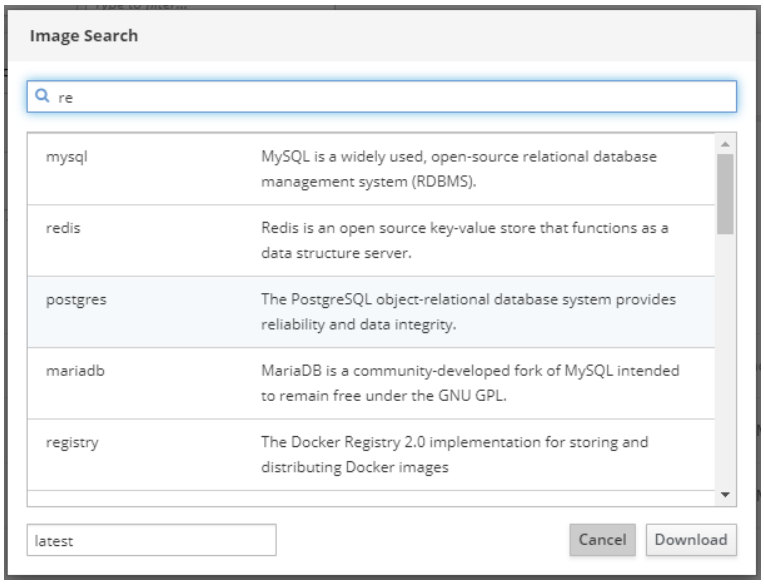


Figure 63: Image Search dialog of Standard Docker

➢ 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.

© Hilscher 2021

The **Run Image** dialog opens, in which you can configure the container before running it:

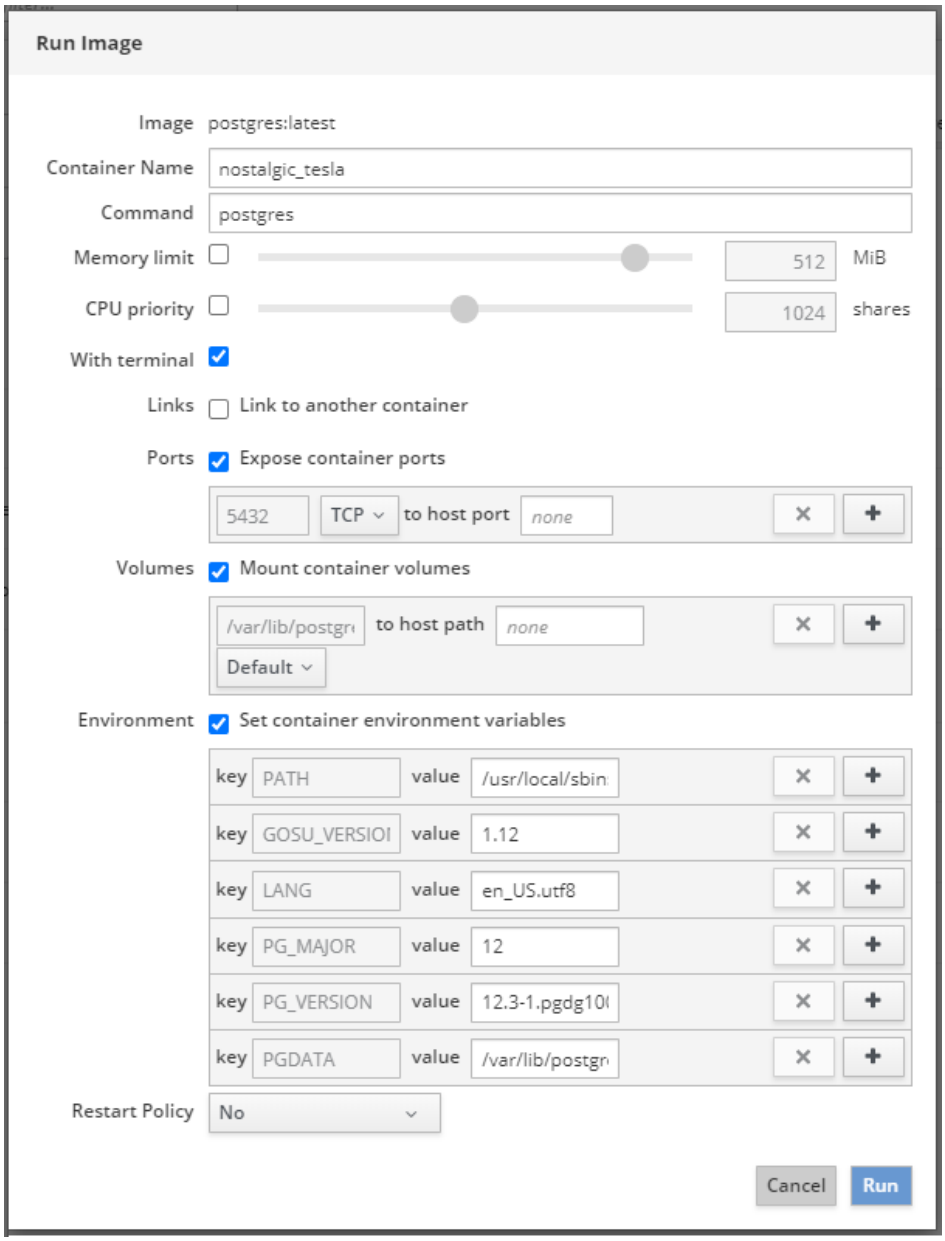


Figure 64: Run Image dialog

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.

© Hilscher 2021

➢ 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:

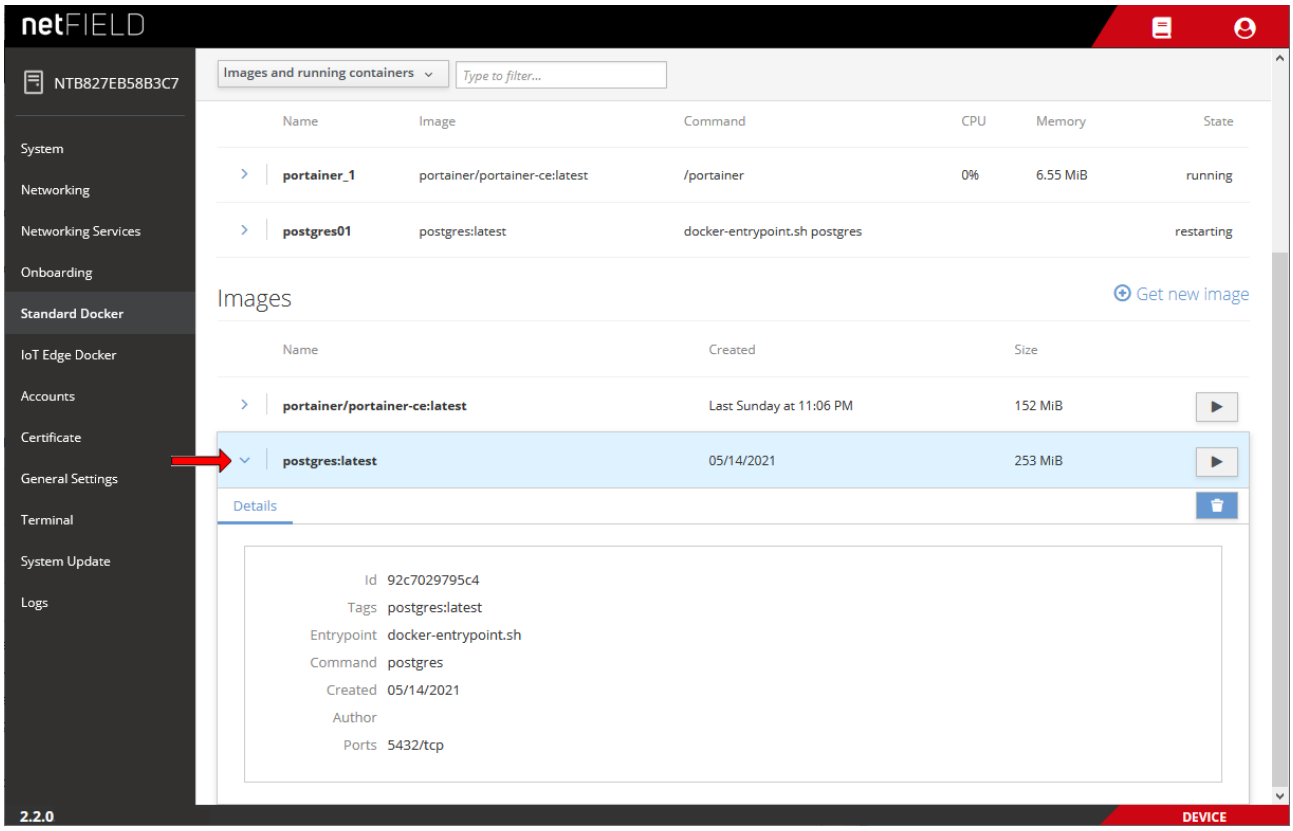


Figure 65: Expand image details

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

© Hilscher 2021

A page featuring detailed information opens:

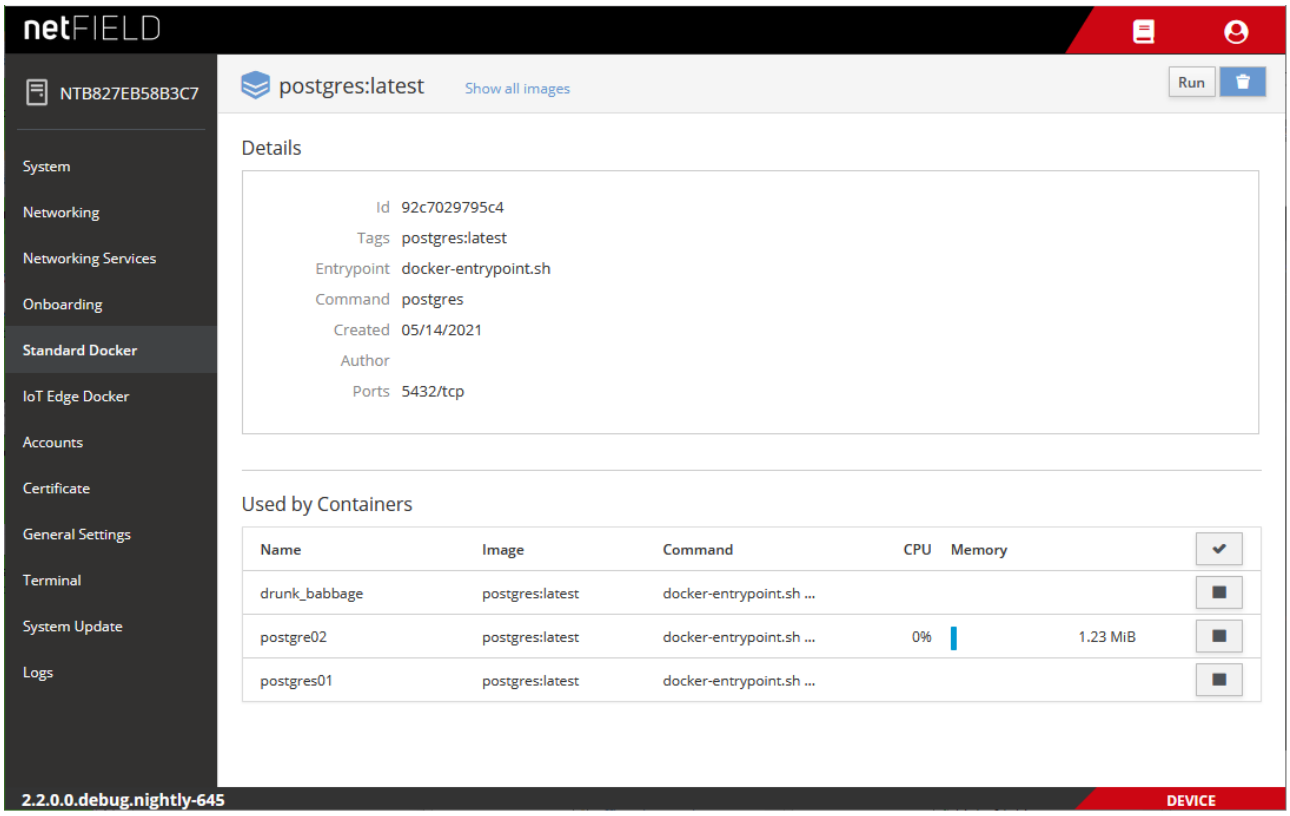


Figure 66: Image details

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 138] 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.

© Hilscher 2021

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 39]) 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 95]).

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 116]).

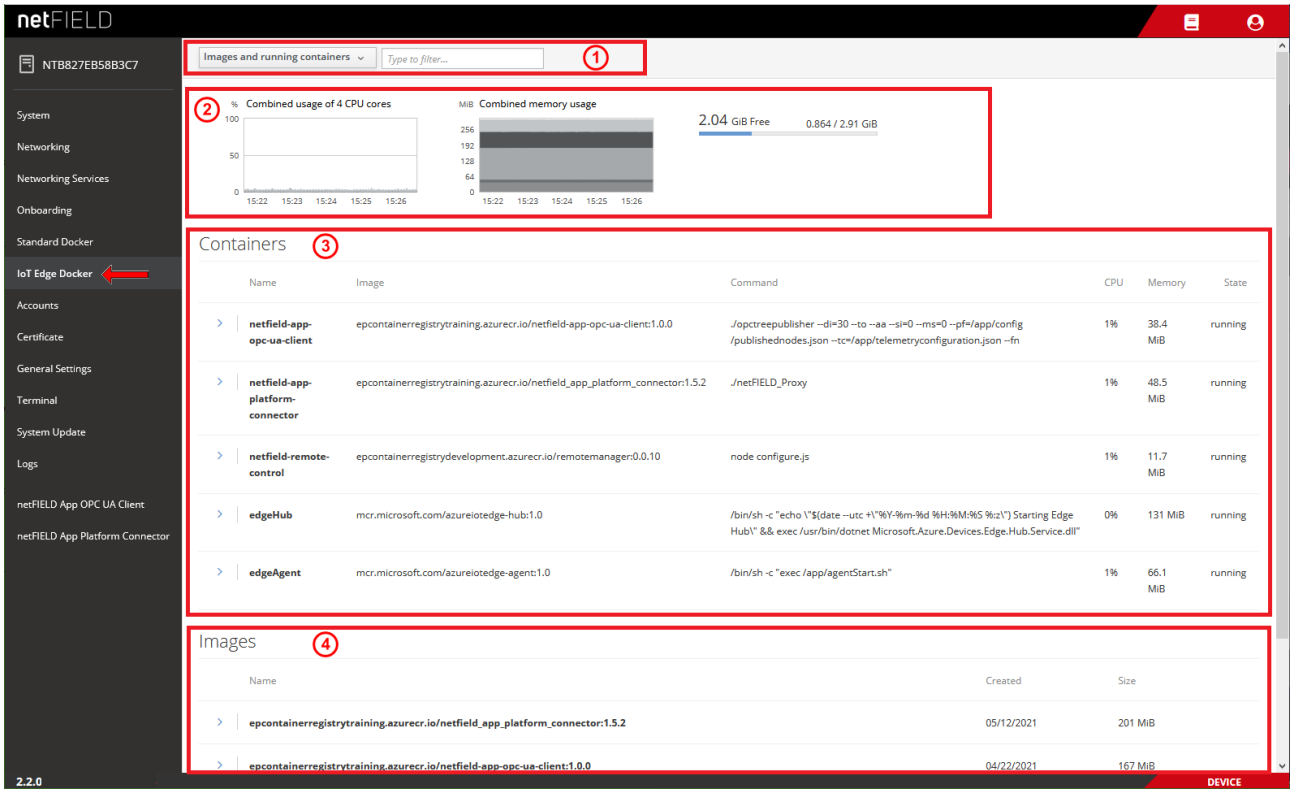


Figure 67: IOT Edge Docker

© Hilscher 2021

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.

© Hilscher 2021

Containers

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

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

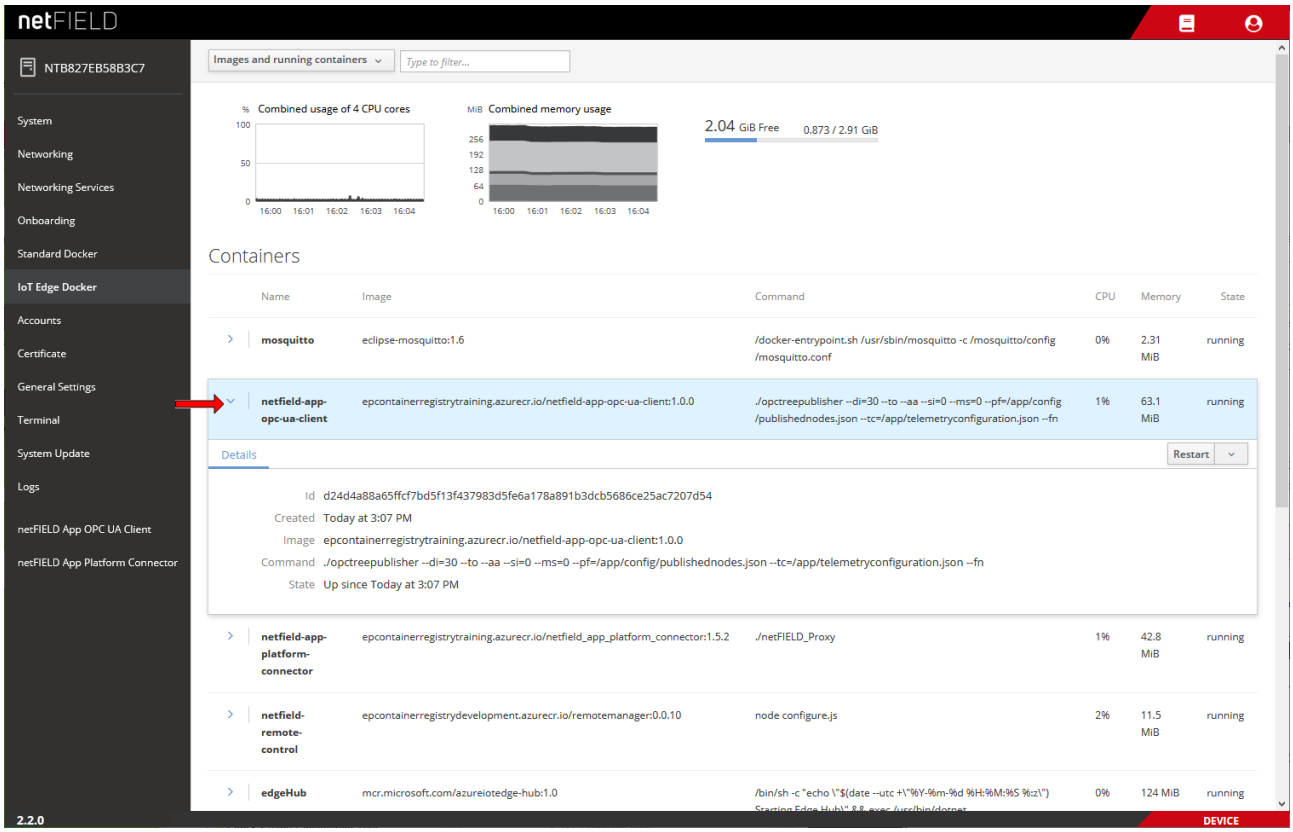


Figure 68: Container details expanded

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

© Hilscher 2021

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

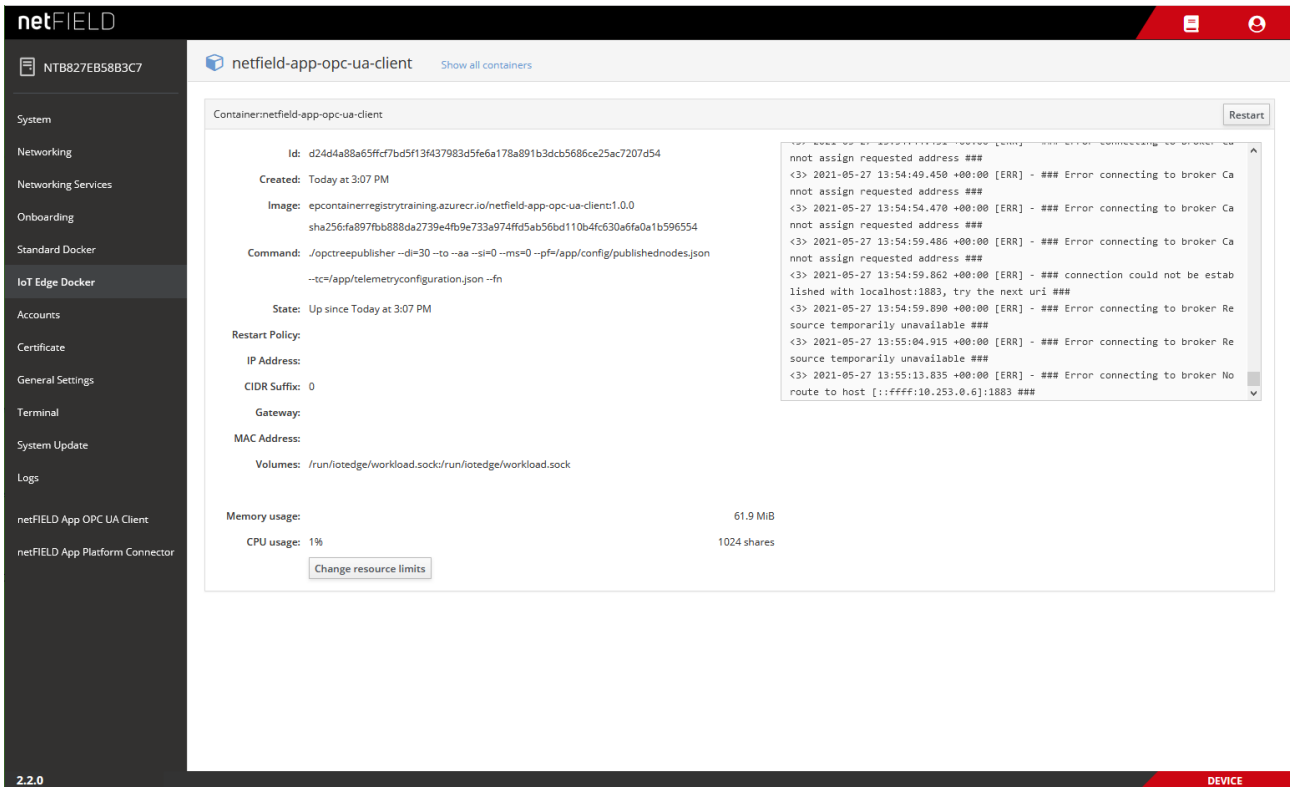


Figure 69: Container parameters

➢ 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.

© Hilscher 2021

➢ 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:

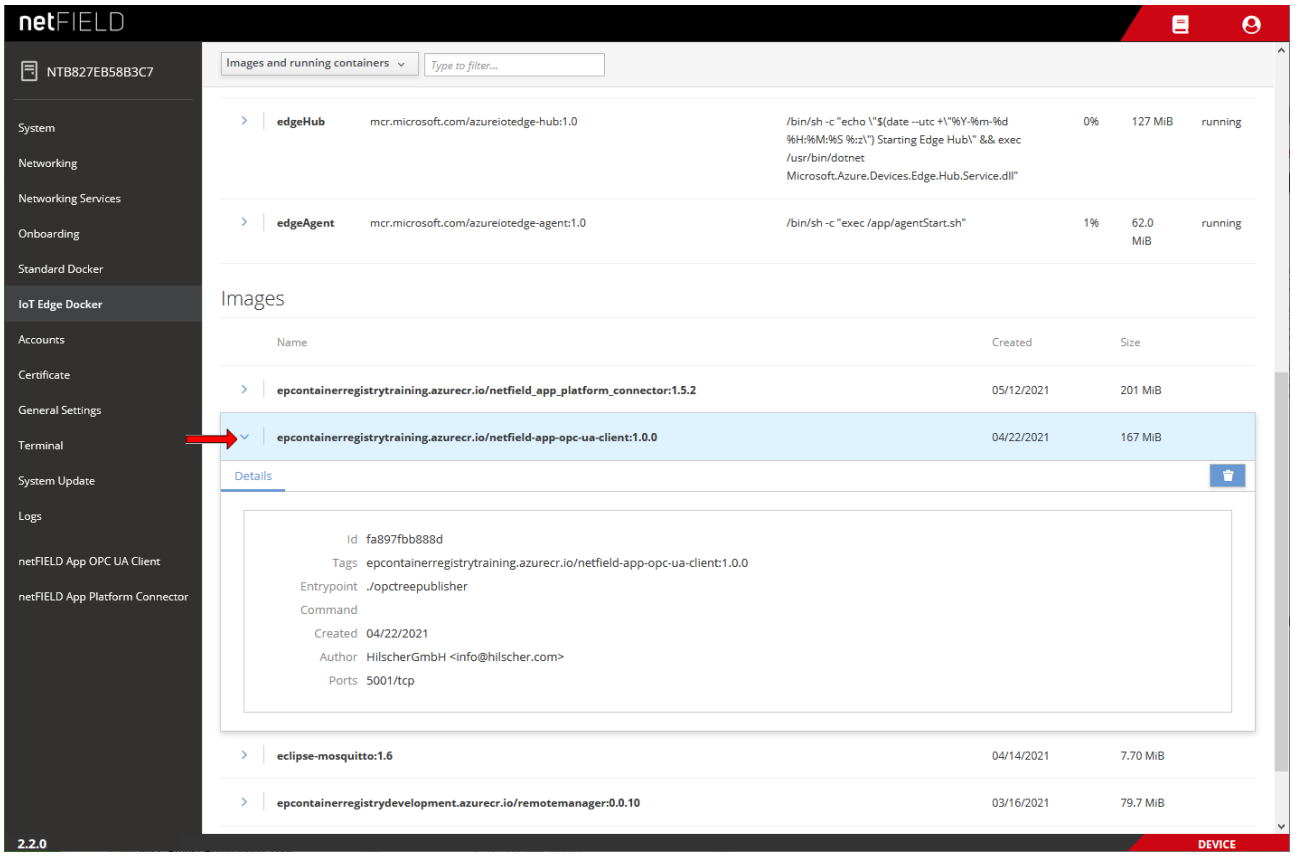


Figure 70: IoT image expanded

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

© Hilscher 2021

A page featuring detailed information opens:

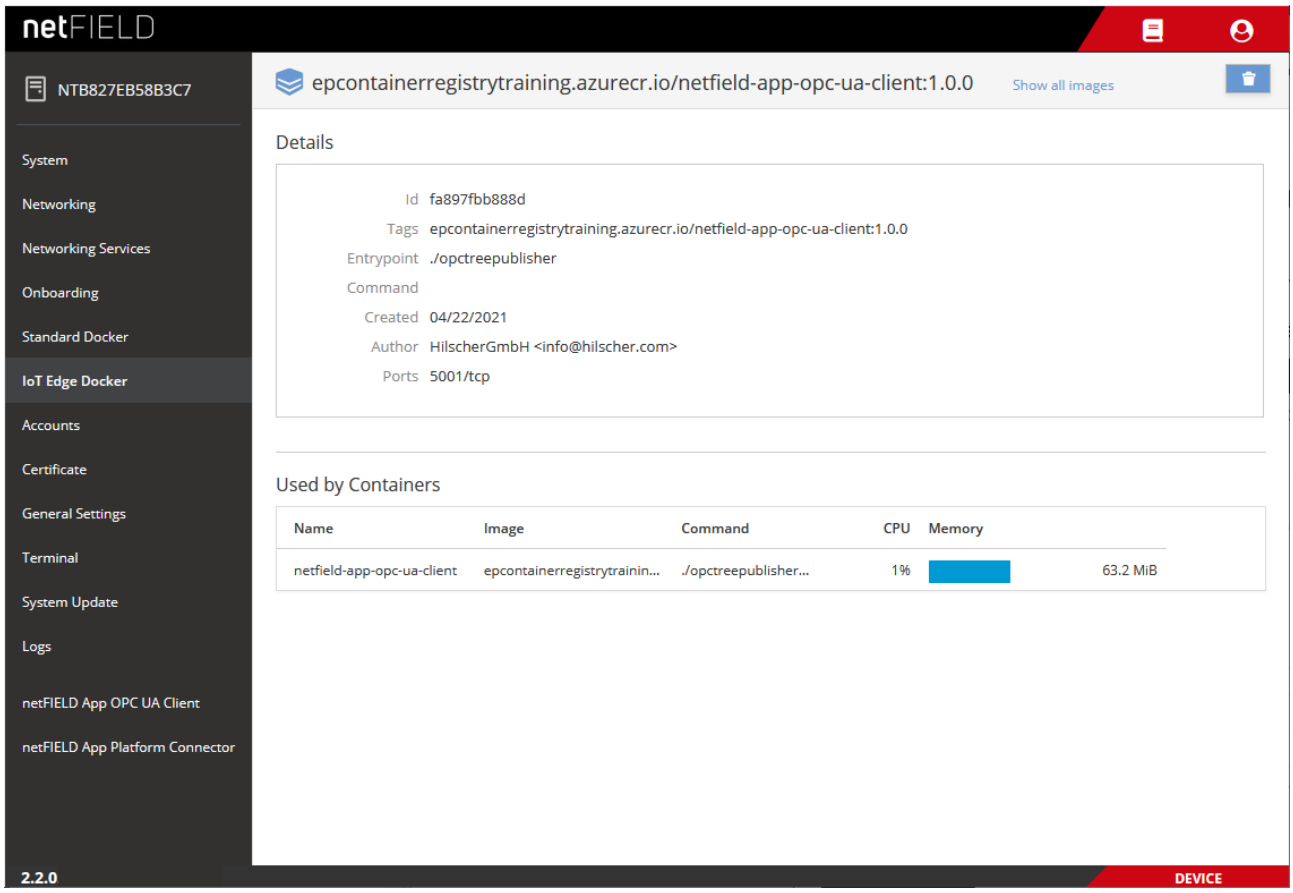


Figure 71: Details of netFIELD Proxy image

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 138] for examples.

© Hilscher 2021

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”).

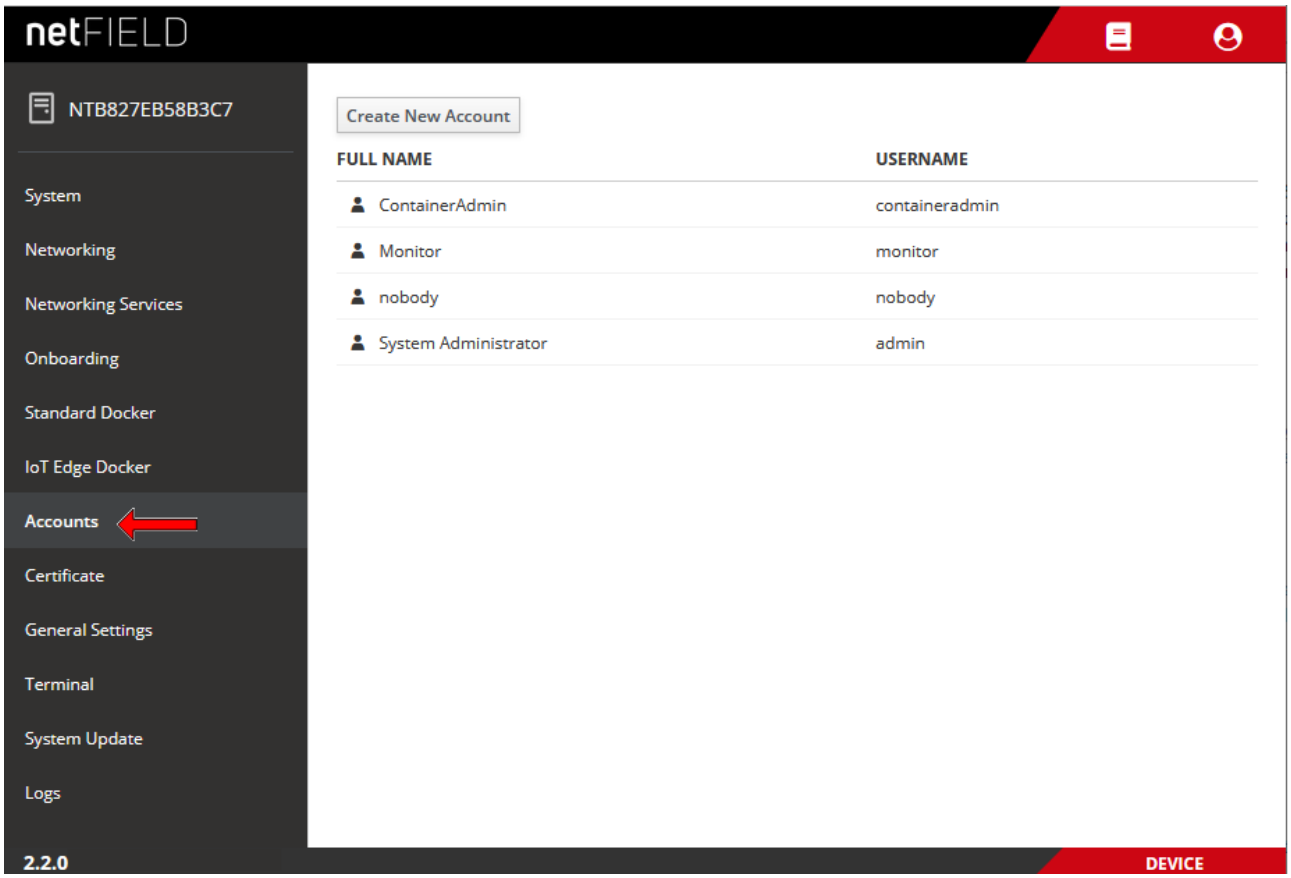


Figure 72: Accounts

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

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

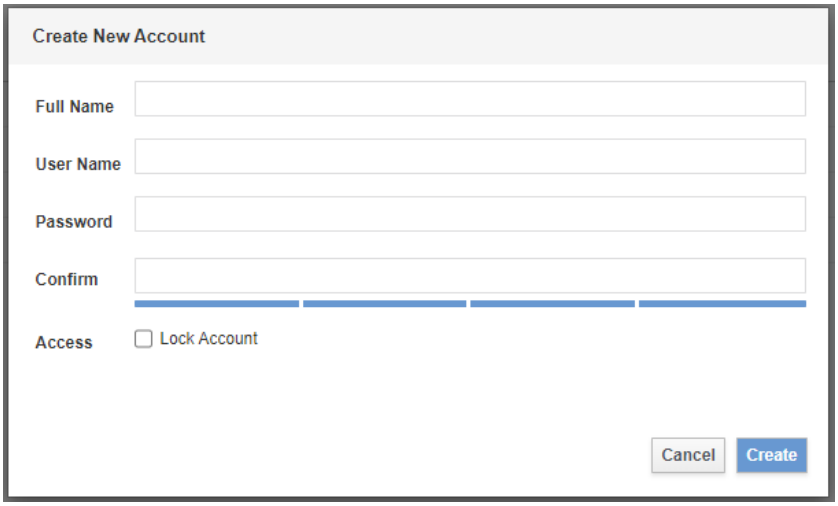


Figure 73: Create new account

➢ Fill in the form, then click **Create** button.

© Hilscher 2021

➢ 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:

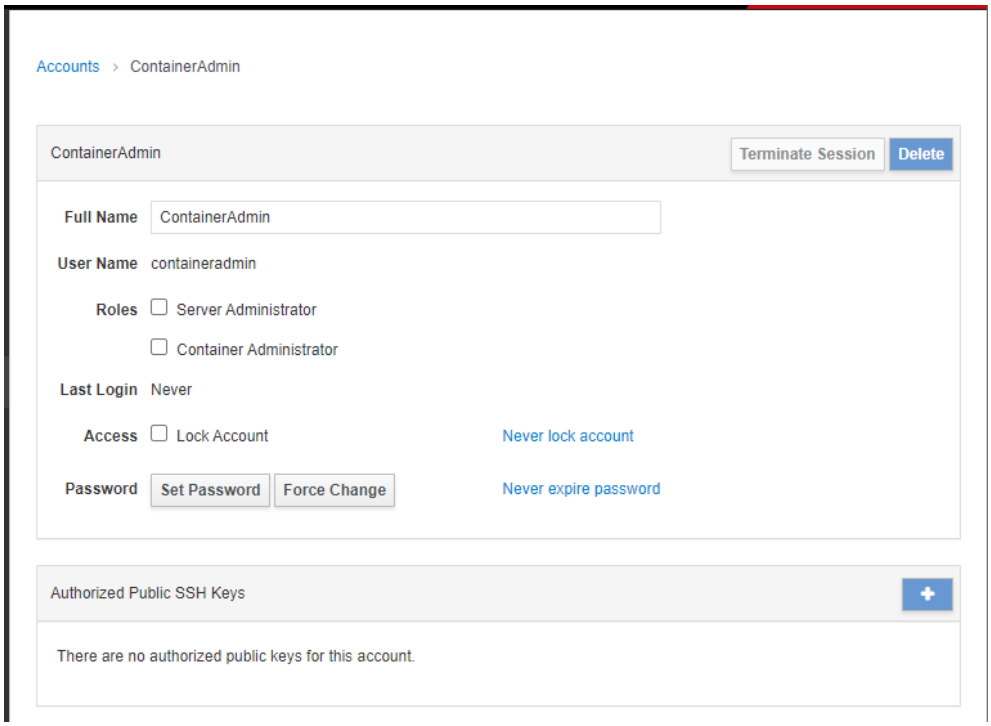


Figure 74: Edit account

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).

© Hilscher 2021

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.

© Hilscher 2021

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.

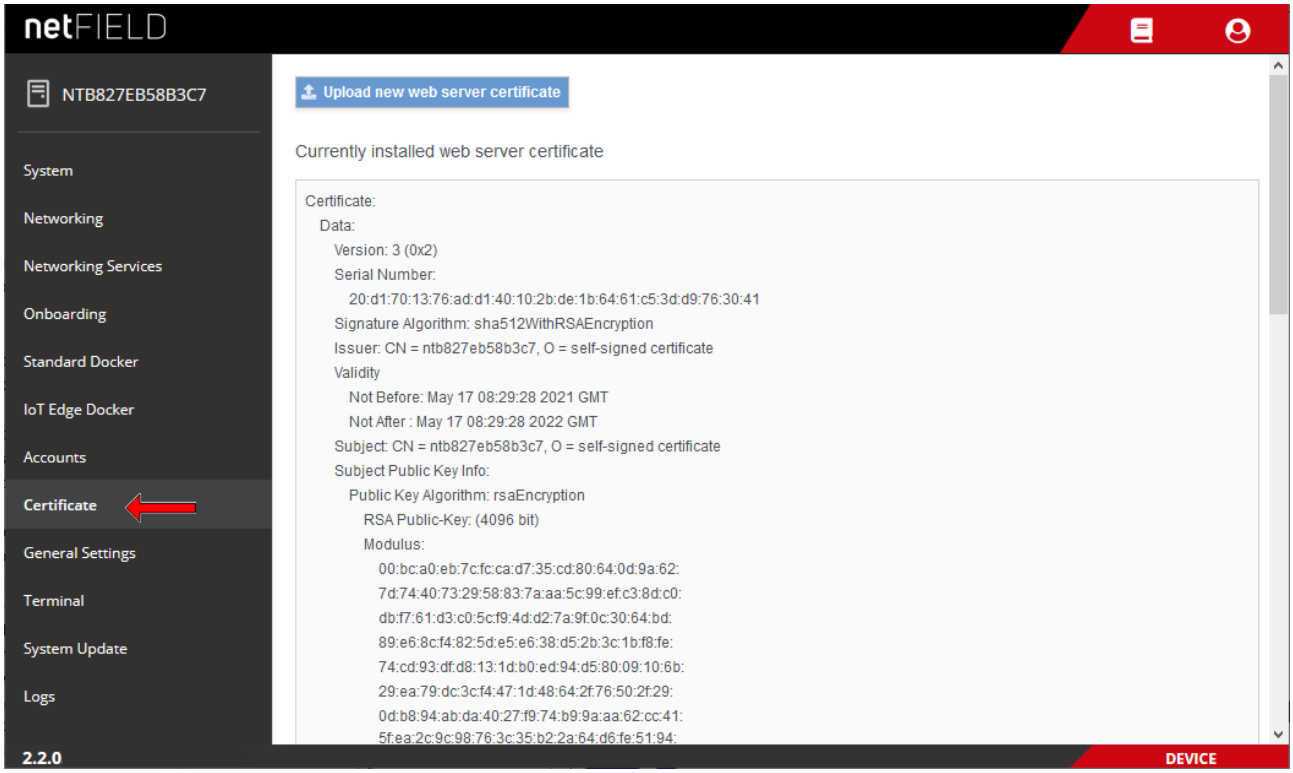


Figure 75: Web Server Certificate page

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.

© Hilscher 2021

6.10 General Settings

6.10.1 Overview

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

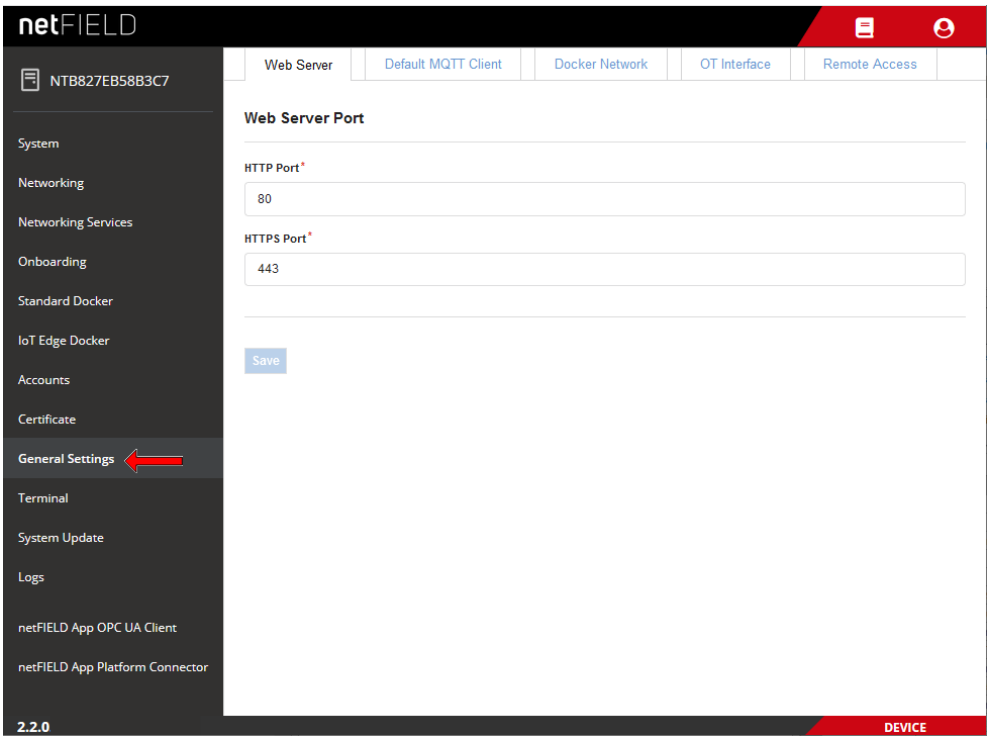


Figure 76: General Settings

© Hilscher 2021

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.

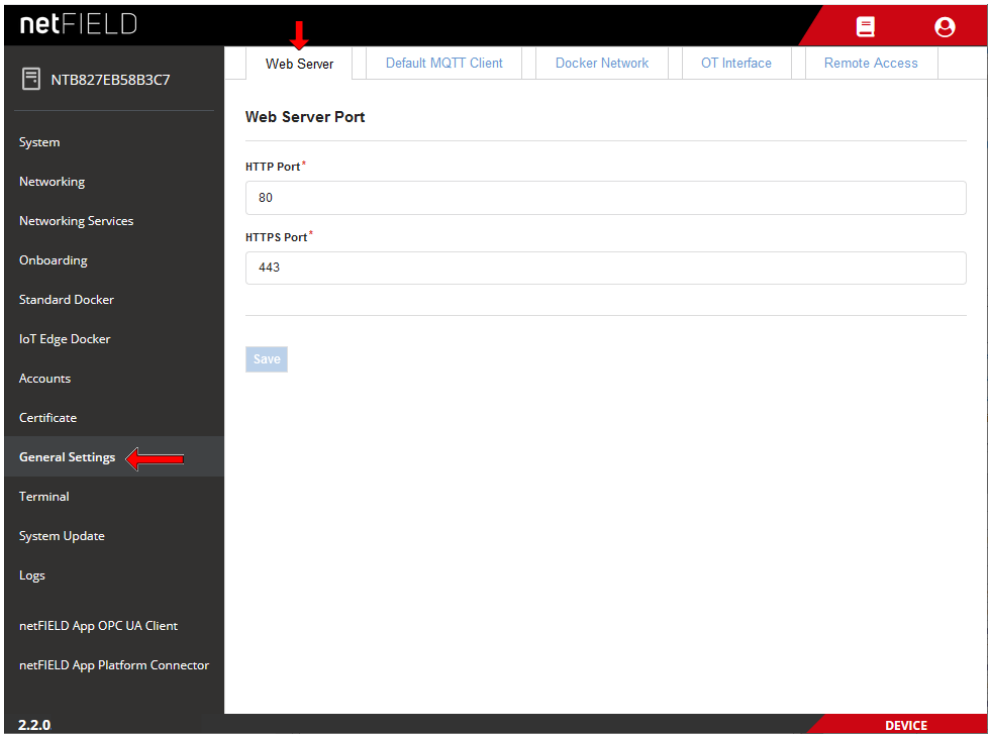


Figure 77: Web Server Settings tab

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

Important:
The new settings become immediately effective after saving and confirming the changes, which means that your current HTTP/ HTTPS connection to the netFIELD OS respectively Local Device Manager will be lost.
You will have to reconnect by specifying the new port number after the IP address in the address bar of your web browser.

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

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

© Hilscher 2021

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, DOC190701OIxxEN).

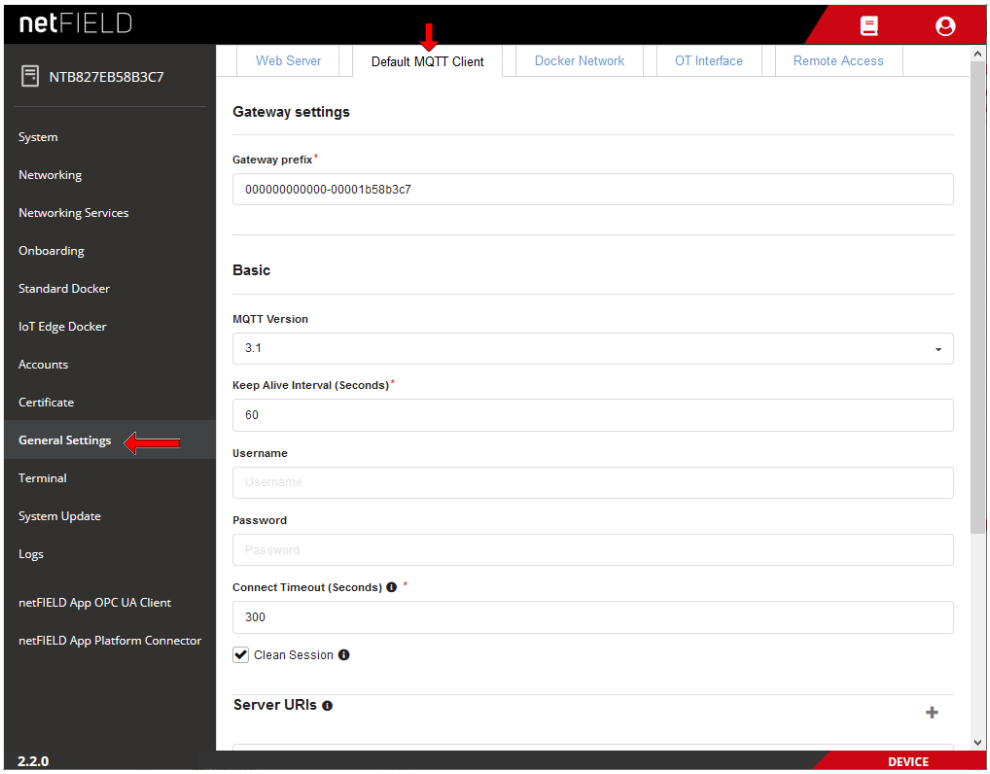


Figure 78: Default MQTT Settings

© Hilscher 2021

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 **Clean session** 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 **Clean session** is unchecked, the broker creates a persistent session for the client.	
Server URIs		Server URI or FQDN of the MQTT Broker **Note**: 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. **Note**: 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 27: Default MQTT Client Settings

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

© Hilscher 2021

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.

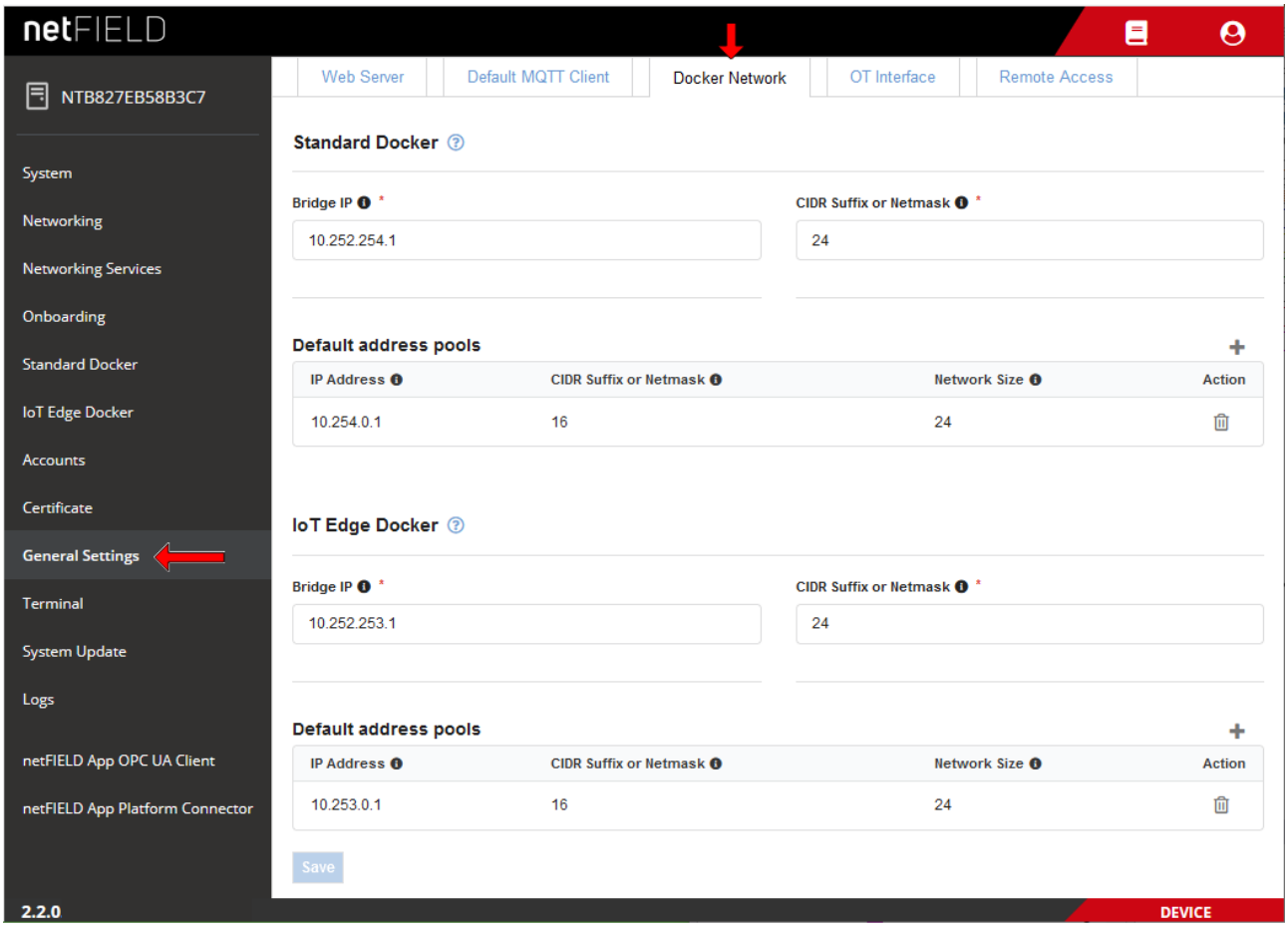


Figure 79: Docker Network Settings

© Hilscher 2021

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 **docker0** bridge. Default: `10.252.254.1` **Note**: 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 **docker0** 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		Opens a dialog for adding a new pool of reserved addresses.
			Deletes the address pool.

Table 28: Standard Docker Network Settings

© Hilscher 2021

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 **iotedge0** bridge. Default: `10.252.253.1` **Note**: 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 **iotedge0** 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.		
	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	+	Opens a dialog for adding a new pool of reserved addresses.
		🗑	Deletes the address pool.

Table 29: Standard Docker Network Settings

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

The following pictures illustrates the default Docker network configuration:

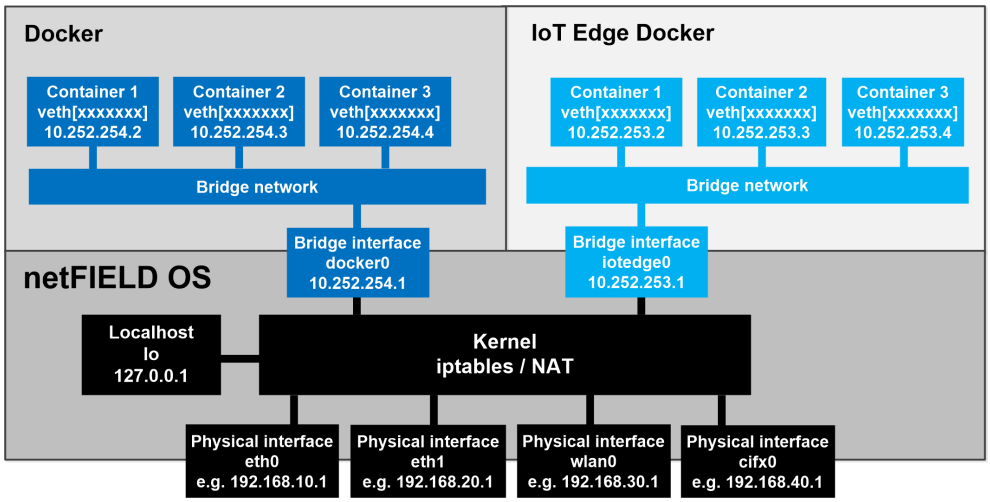


Figure 80: Default docker network configuration

© Hilscher 2021

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 (13) and (15) 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 interfaces of the device. (Note that in this case, the UPnP service cannot be used for connecting to the device, because it is not supported by the cifx0 interface.)

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

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

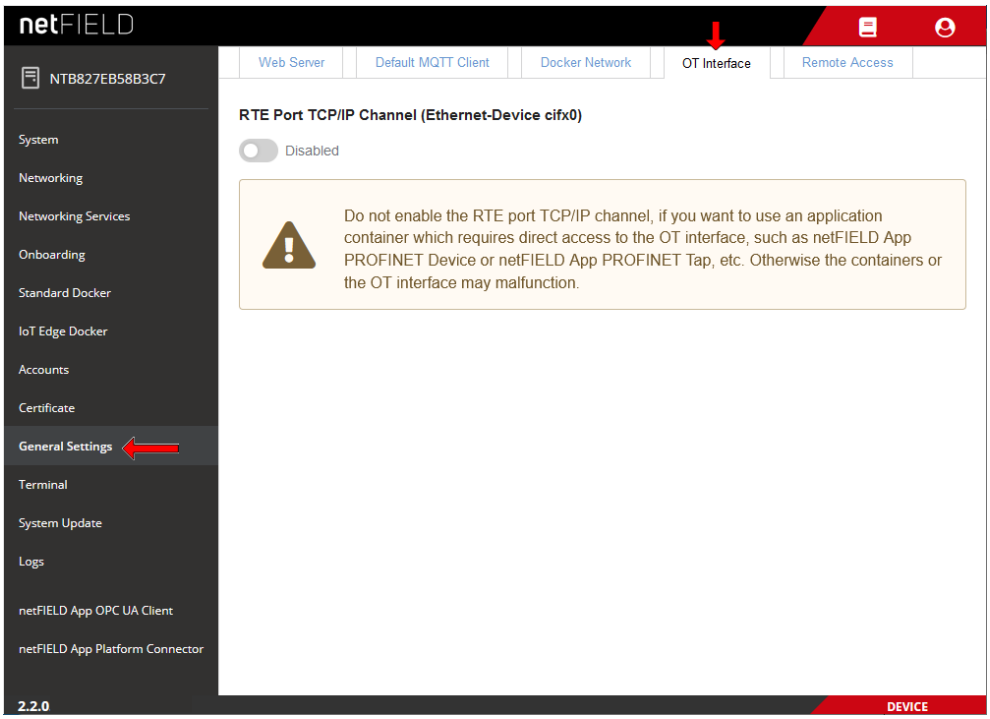


Figure 81: OT interface

© Hilscher 2021

Note the following about the OT Interface

The cifx0/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 **cifx0**, 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 cifx0 (LAN) *and* as a Real-Time Ethernet device (in this case PROFINET Device).
Note that the **cifx0** and the RTE interface must receive their own individual IP configuration. While the **cifx0** 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.

© Hilscher 2021

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 ≥ 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, DOC190701OIxxEN).

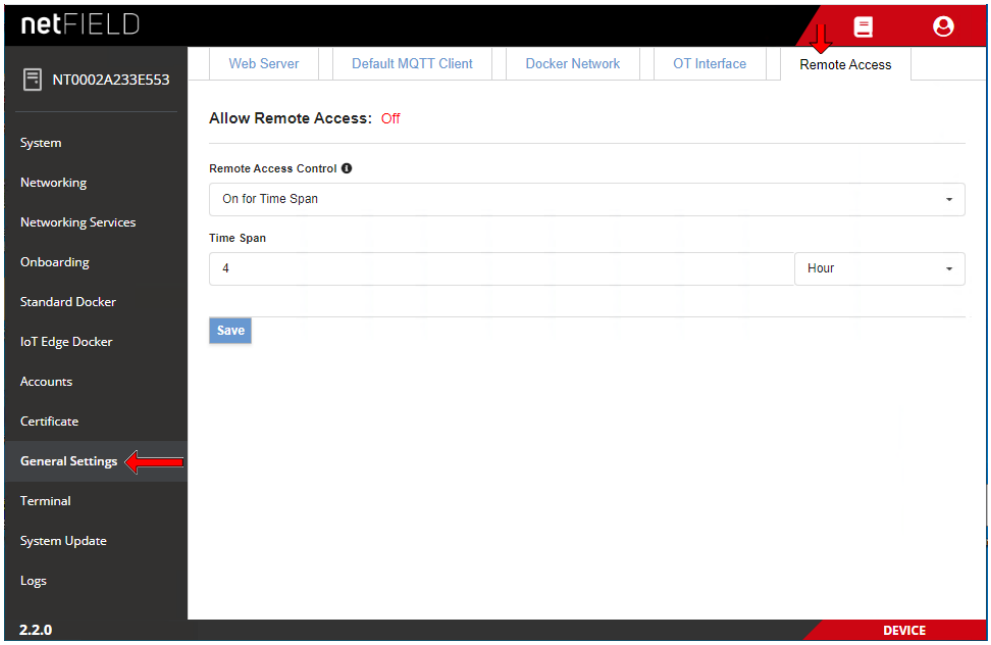


Figure 82: Remote Access tab

© Hilscher 2021

- 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**.

© Hilscher 2021

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.

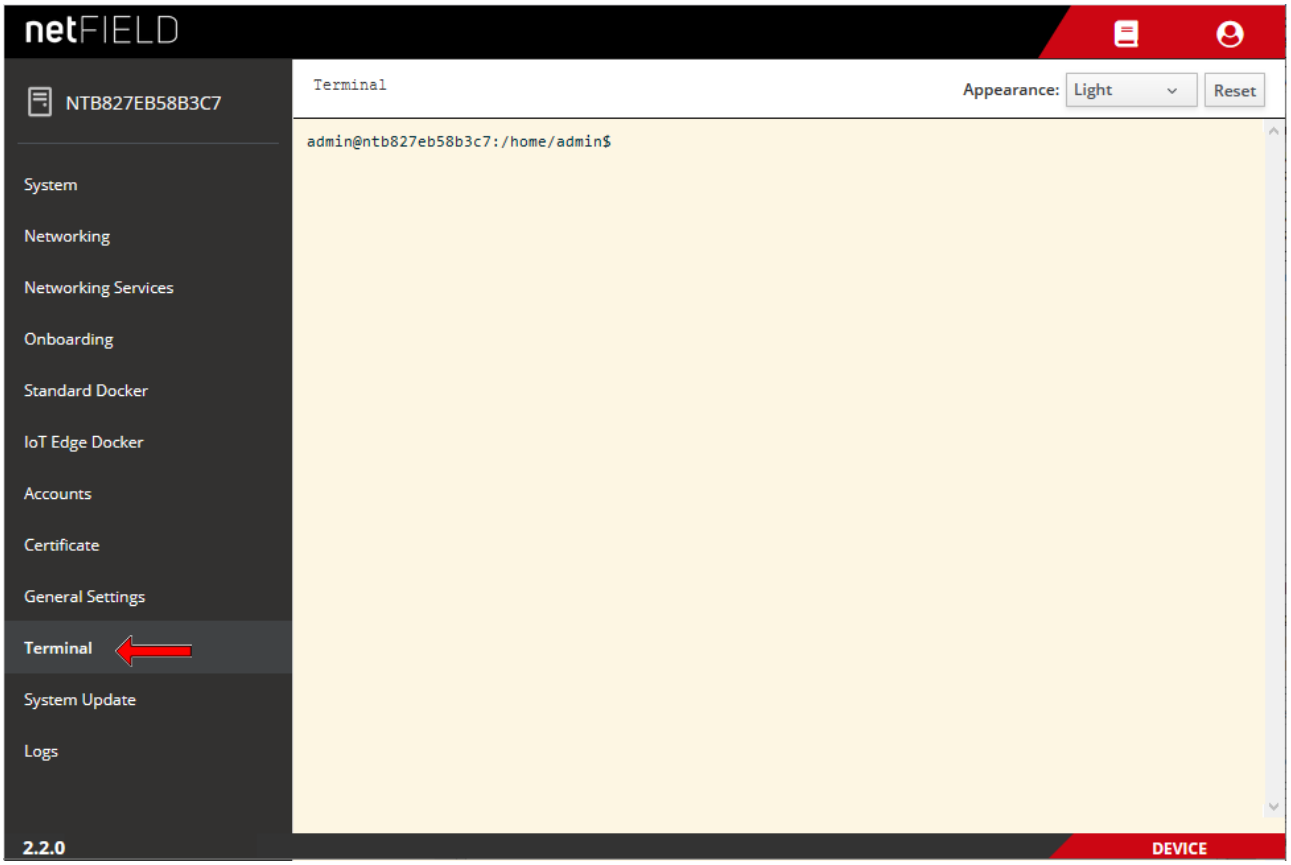


Figure 83: Terminal

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 138].

© Hilscher 2021

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.

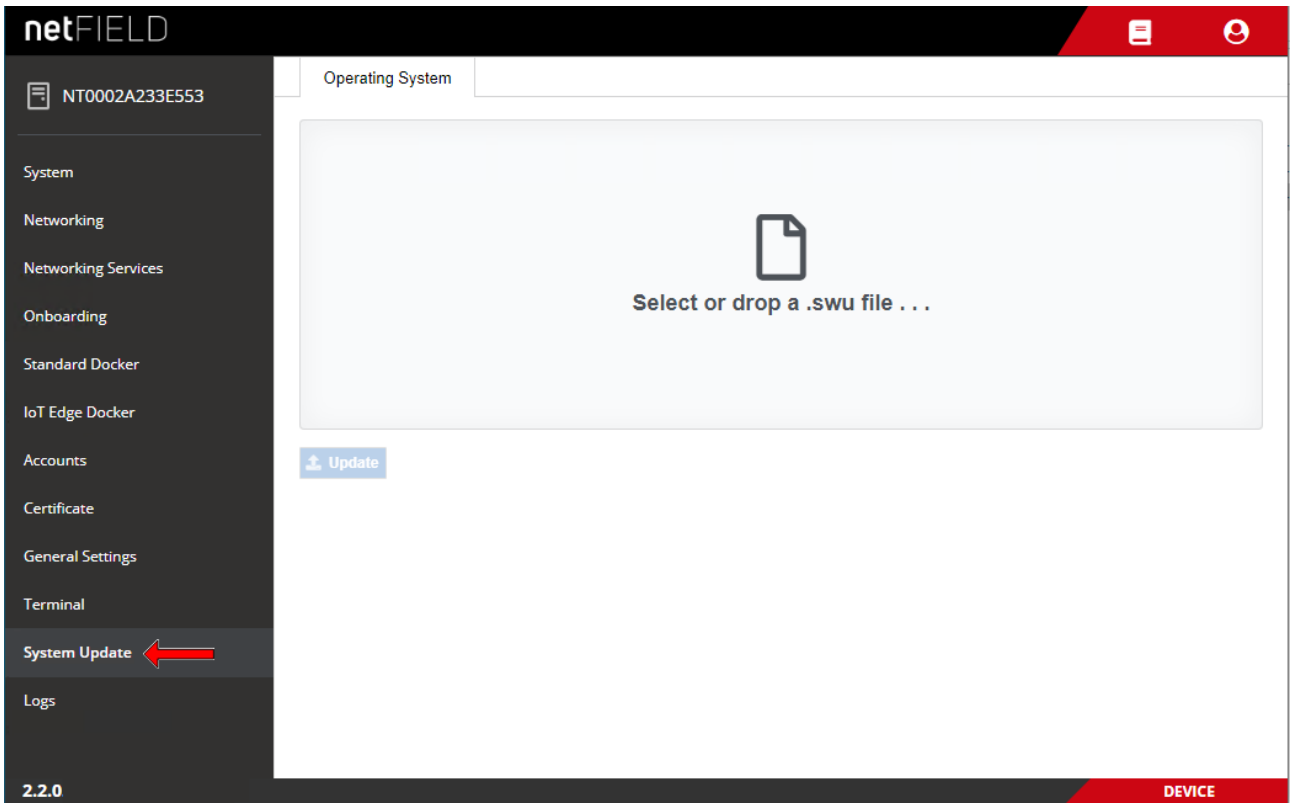


Figure 84: OS update page

© Hilscher 2021

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 OnPremise device.
     In the *Software* table, go to the *Update via local Device Manager* entry and download the `niot-e-tijcx-gb-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-tijcx-gb-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.

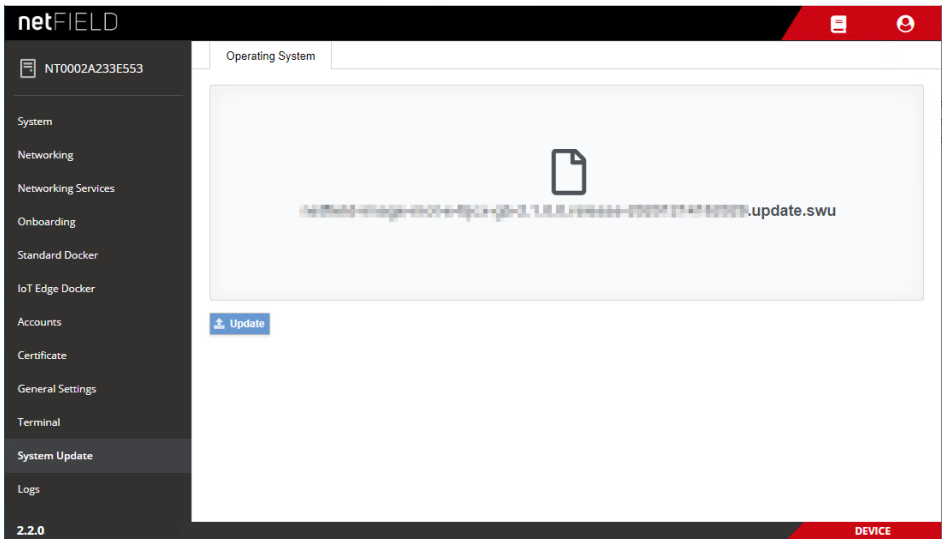


Figure 85: Selected OS update image

   - ➢ After having added the update file to the field, click **Update** button.

© Hilscher 2021

- 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:

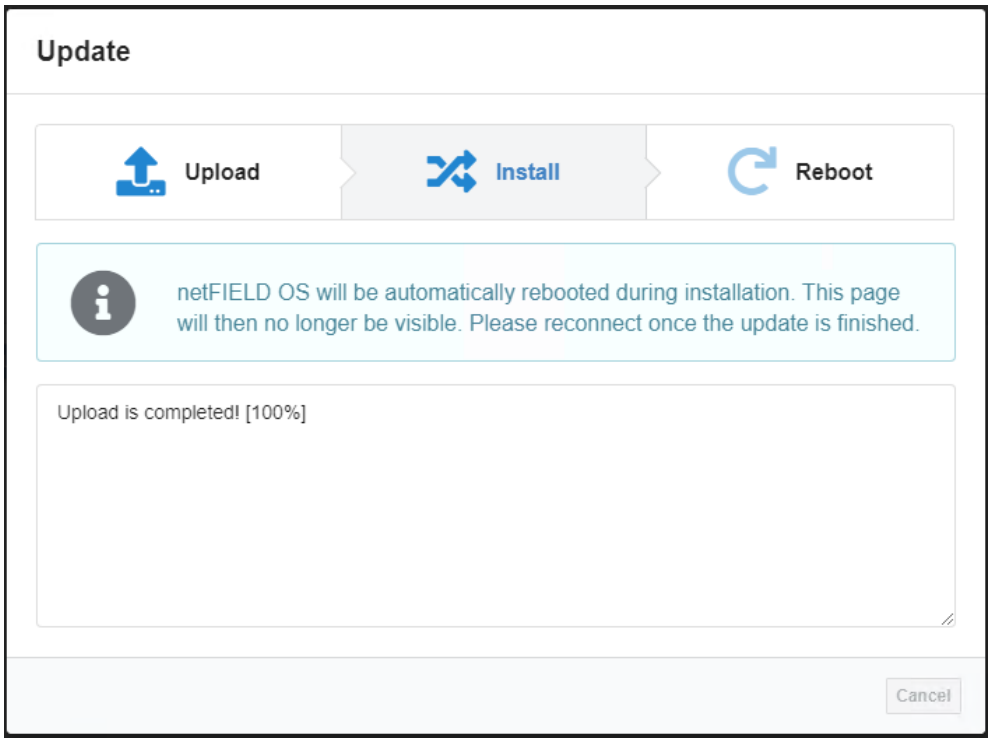


Figure 86: Upload finished message

© Hilscher 2021

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

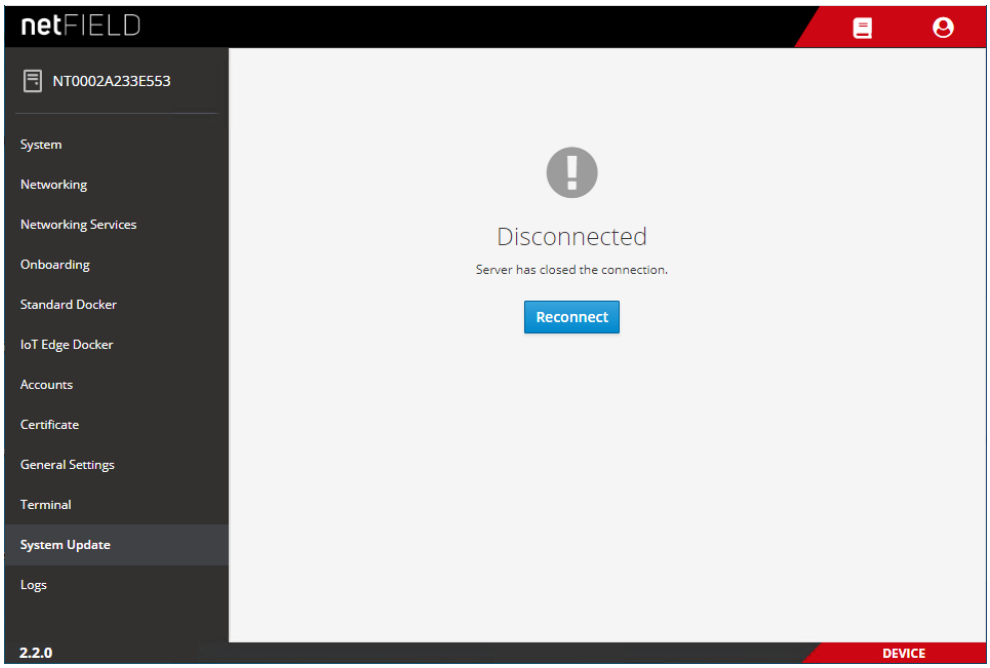


Figure 87: OS update “Disconnected” message

➢ 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 24]).

© Hilscher 2021

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.

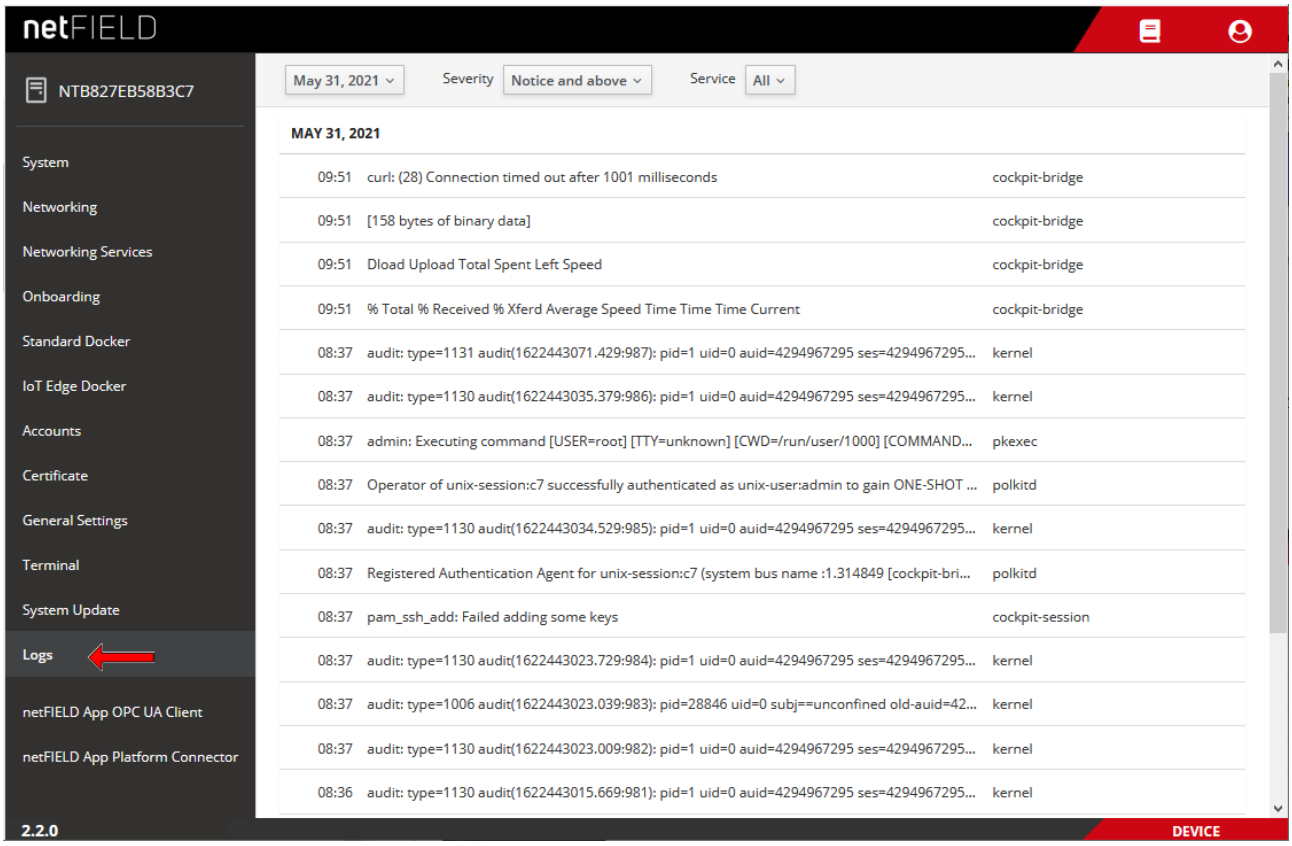


Figure 88: Logs

© Hilscher 2021

7 Good to know...

7.1 Device recovery via USB

7.1.1 Overview

This section describes how to reset the netFIELD OS of your device by installing a “recovery” image firmware from a USB stick.
A device recovery via USB can be necessary if the netFIELD OS has become instable or corrupted, or if you have “locked yourself out” of the **Local Device Manager** because you have deactivated or misconfigured its LAN or Wi-Fi interfaces (eth0, eth1 and wlan0), or if you have forgotten the administrator’s password.

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

Important:
Note that in a recovery, all configuration settings, user accounts and deployed containers of the current netFIELD OS will be deleted. This means that you will have to commission and configure your device again after the recovery procedure.
Note also that the firmware of the netX communication controller will not be affected by the recovery.

7.1.2 Requirements

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

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

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

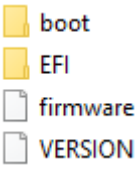
Important:
Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the gateway.

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

© Hilscher 2021

7.1.3 Step-by-step instructions

1. Download the zip archive containing the recovery image from Hilscher to your local PC and unpack it.
   - ➢ Go to the *netFIELD Software Overview* page https://kb.hilscher.com/x/sSAfBw and navigate to the latest netFIELD OS version for the netFIELD OnPremise device.
   - ➢ In the *Software* table, go to the *Recovery (factory reset) via USB memory stick* entry and download the `niot-e-tijcx-gb-2.x.x.x.release-recovery.zip`.
   - ➢ Use a tool like **7-Zip** to unpack the downloaded zip archive on your local PC.
   - ↬ The unpacked folder contains the following folders and files, which you will later have to copy onto the USB stick (after having formatted the stick):



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

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

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

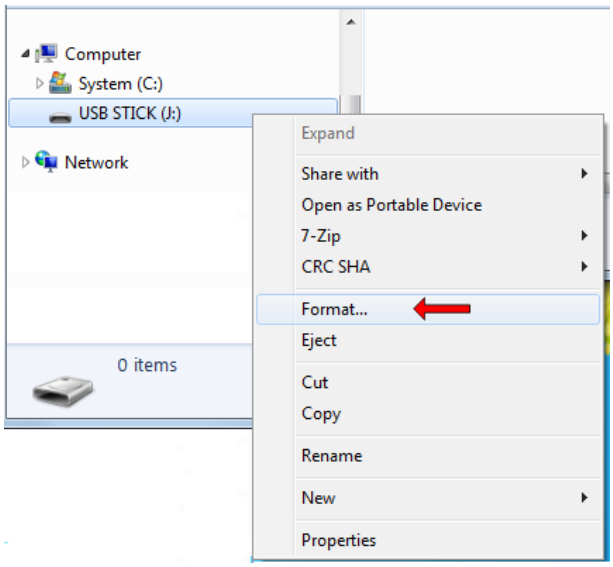


Figure 89: Formatting USB stick

© Hilscher 2021

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

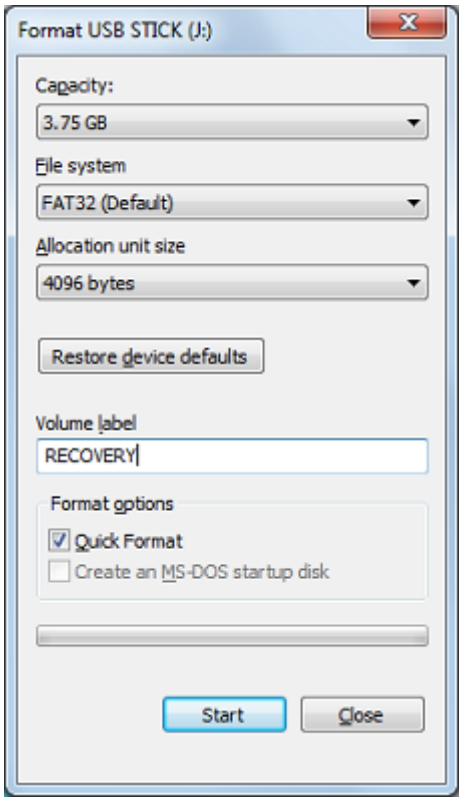


Figure 90: Format USB STICK dialog window

- 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”.

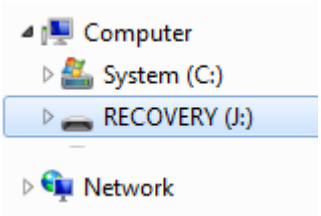


Figure 91: Formatted USB stick

© Hilscher 2021

3. Copy recovery files onto the USB stick.
   - ➢ Open the `niot-e-tijcx-gb-2.x.x.x.release-recovery` folder and copy the `boot` and `efi` folders and the `firmware` and `VERSION` files onto the USB stick.
   - ➢ The USB stick with the copied firmware image must now feature the following elements:

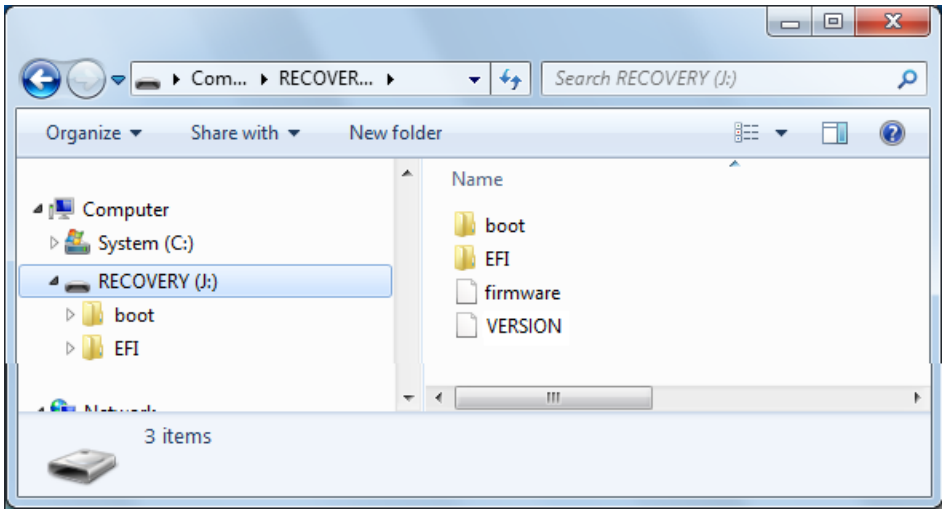


Figure 92: Prepared USB stick

   - ➢ Remove the USB stick from your Windows PC.

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

4. Prepare netFIELD OnPremise device
   - ➢ Make sure that the device is switched off (the green Status LED below ⏻ indicating power must be dark).
   - ➢ Connect the USB keyboard with one of the USB sockets of the device (for the positions of the USB sockets, see section *Positions of the interfaces* [▸ page 14]).
   - ➢ Connect the monitor with the DVI-I socket (see position (3) in section *Positions of the interfaces* [▸ page 14]) or with the DP socket (see Position (4)) [according to your monitor type].

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

   - ➢ Plug the prepared USB stick into one of the USB sockets of the device (for the positions of the USB sockets, see section *Positions of the interfaces* [▸ page 14]).

© Hilscher 2021

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

   ➢ Turn-on the device by pressing the power button (see position (12) in section *Positions of the interfaces* [page 14]).

   ➢ After a few seconds, the device beeps and the BIOS start screen appears on the monitor:

Figure 93: BIOS start screen

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

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

   ➢ The BIOS setup menu opens:

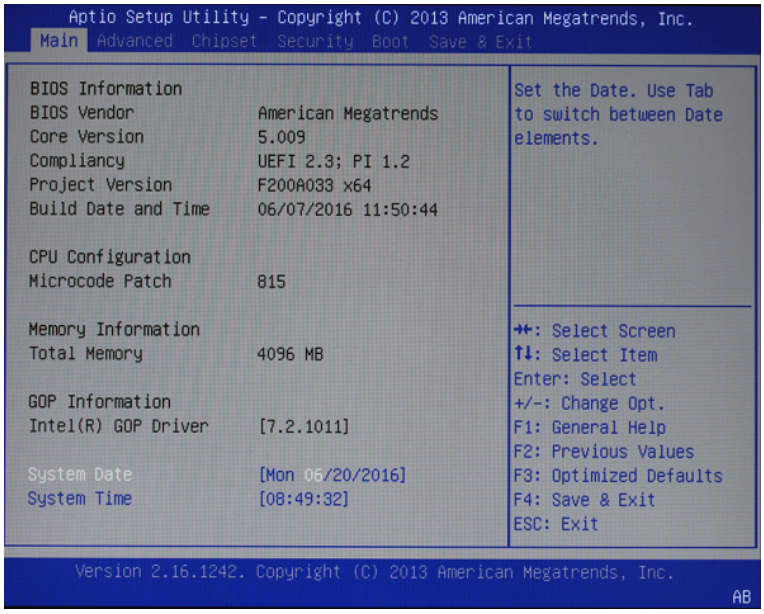


Figure 94: BIOS setup menu

© Hilscher 2021

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

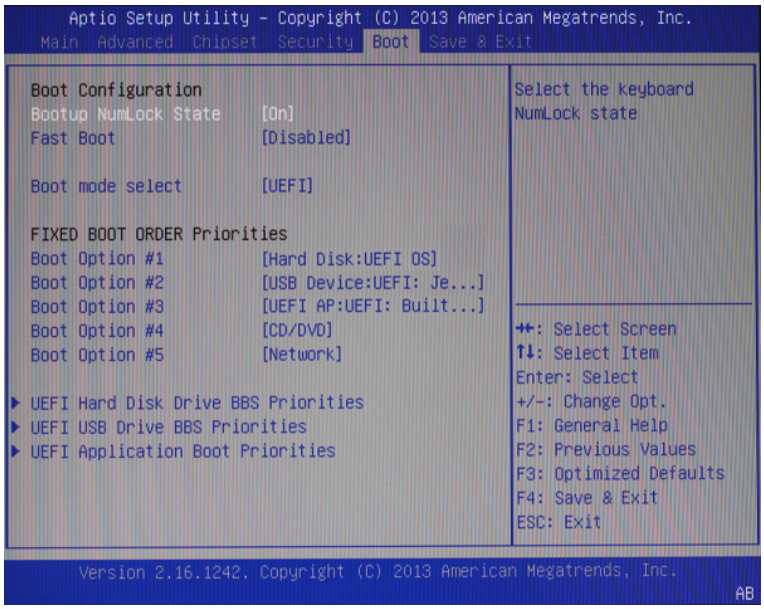


Figure 95: Boot options tab in BIOS setup menu

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

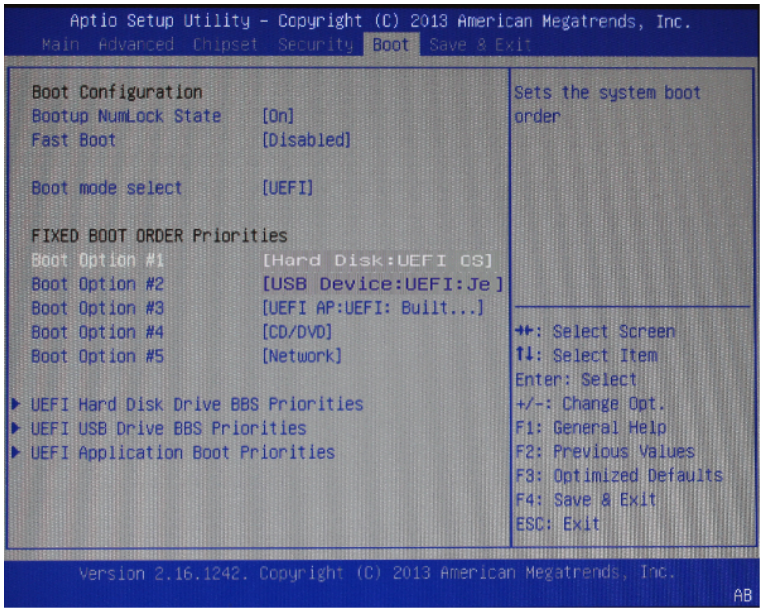


Figure 96: Boot option #1 in BIOS setup menu

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

© Hilscher 2021

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

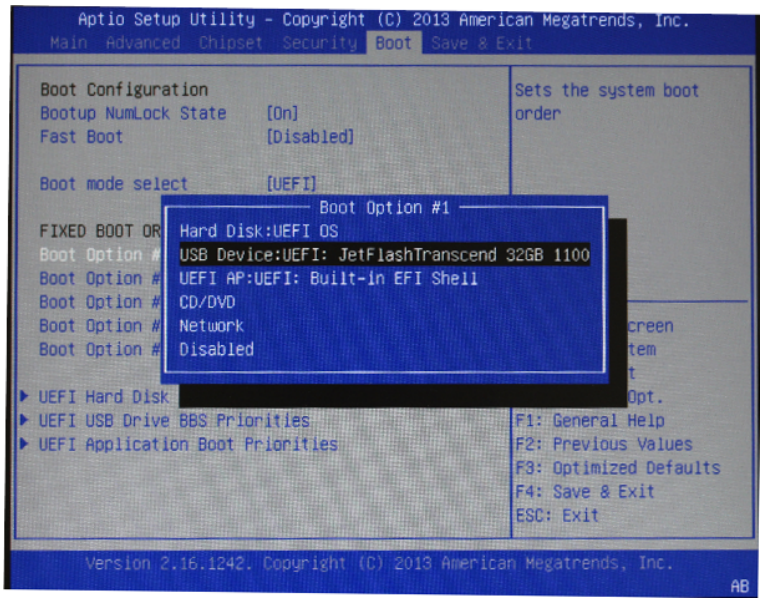


Figure 97: List for boot option #1

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

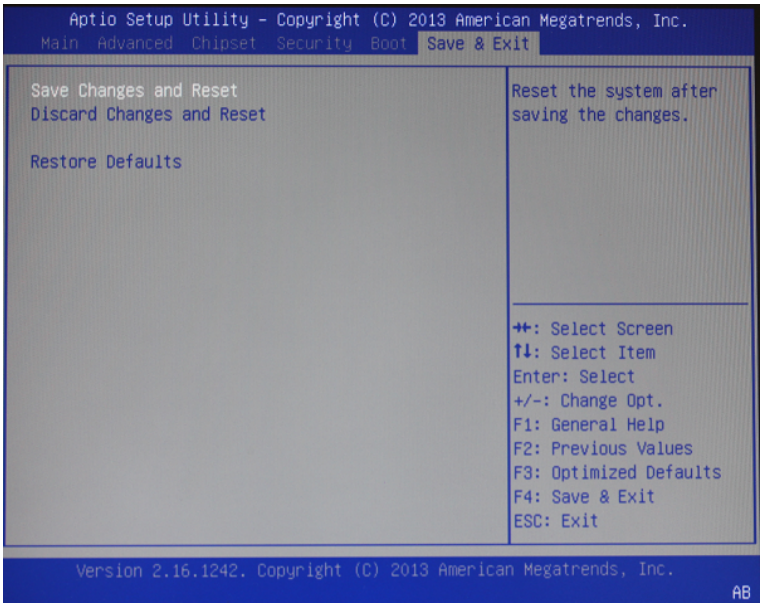


Figure 98: Save & Exit tab

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

© Hilscher 2021

6. Restart booting (reset).

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

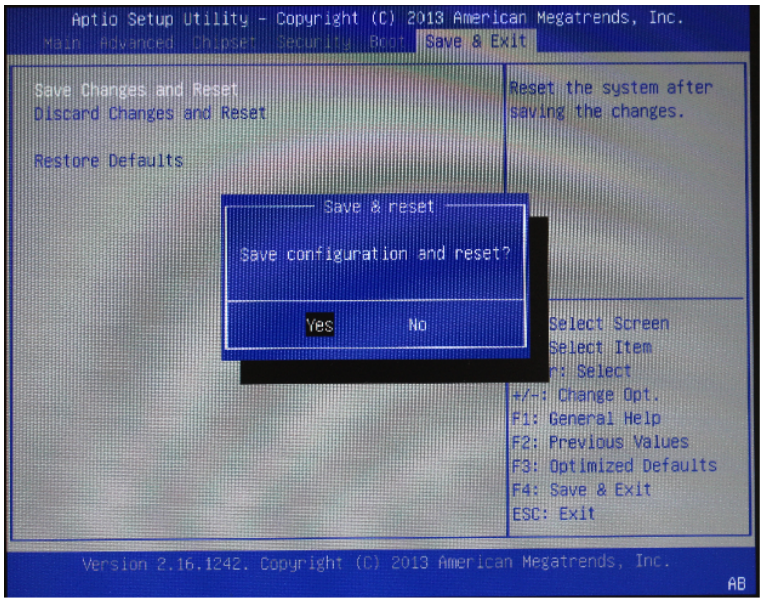


Figure 99: Save & Reset security question

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

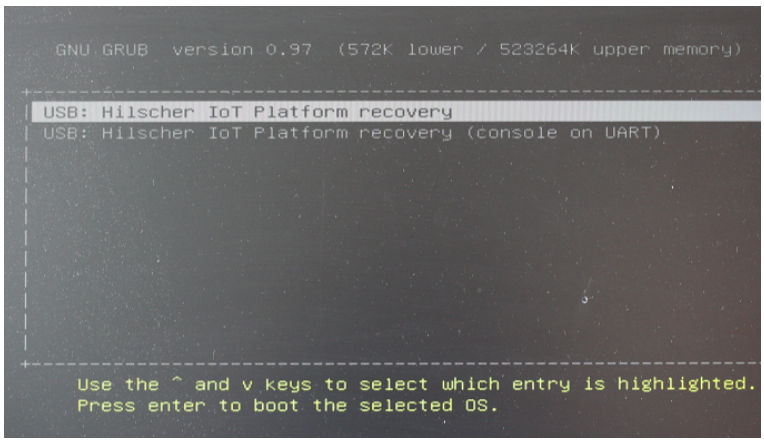


Figure 100: Boot options question

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

© Hilscher 2021

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

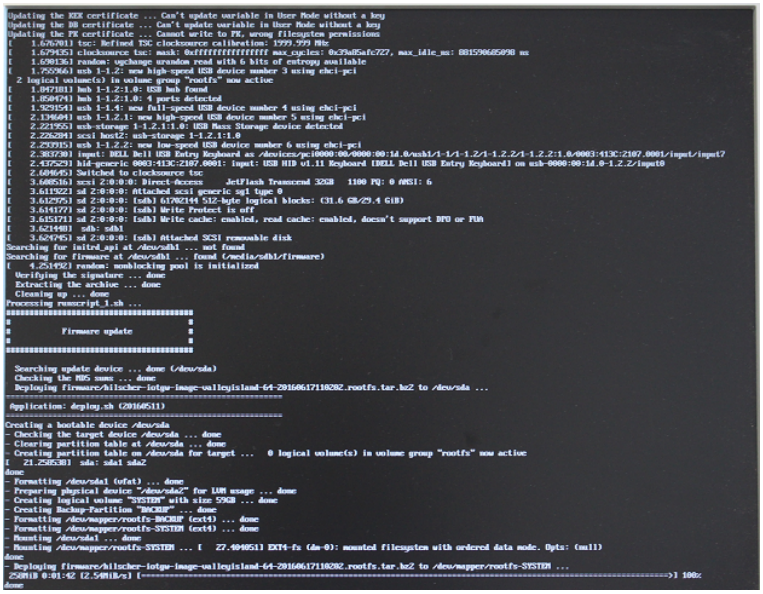


Figure 101: Firmware update in progress

After the recovery procedure is finished, the device automatically switches itself off.

Wait until the device has switched itself off, then **remove the USB stick** from the device.

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

You have finished the firmware recovery procedure and the device has recovered its “factory settings”.

© Hilscher 2021

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
```


© Hilscher 2021

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
```


© Hilscher 2021

8 Technical data

Category	Parameter/item	Value/description
Product	Part number	1321.300/NFLD
	Product name	NIOT-E-TIJCX-GB-RE/NFLD
	Application	IT/OT Edge device for data-intensive and complex IoT applications with demand on maximum performance, connectivity and memory size.
Functions	IoT Edge Docker	Docker for remote and automatic deployment and maintenance of containers
	Standard Docker	Docker for manual and local deployment and maintenance of containers
	Local Device Manager	Web-based GUI for local device parameterization
Security	Boot	Booting of signed software
	Access	HTTPS, TLS
Processors	CPU	2 GHz Celeron®, Intel® J1900
	Communication controller	netX 100
Software	Operating system	netFIELD OS based on Security Enhanced Linux
Memory	RAM	4 GB DDR3 RAM
	Hard drive	128 GB solid state disk drive: 64 GB application 64 GB backup
Power	Voltage	24 V DC ± 4.8 V DC
	Current (at 24 V DC)	Without USB: 420 mA (typical) With USB: max. 2.5 A
	Power of the used power supply unit	60 W
	Connector	3-pin terminal block
IT interface	Interface type	2 x 10/100/1000 Mbit, Intel® I210AT
	LAN connector	2 x RJ45 socket
OT interface	Interface type	10BASE-T/100BASE-TX, potential free, Hilscher netX 100
	Connector	2 x RJ45 socket
	Supported protocols	PROFINET IO Device, EtherNet/IP Adapter, Standard TCP/IP (limited throughput). In listening (“passive”) mode: PROFINET, EtherCAT, Ethernet
Additional interfaces	USB	3 x USB 2.0 (500 mA) 1 x USB 3.0 (900 mA) All USB max. 2 A
	Wi-Fi	Single band 2.4 GHz IEEE 802.11n, 2 x flexible antenna connection
	Serial interface	2 x RS-232/422/485 (can be configured)
	Display connectors	DVI-I and DP (DisplayPort) **Note**: Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.
Display	LED indicators	12 LEDs
Real-time clock	Buffering	Yes, battery (service interval 10 years)
Environment	Ambient temperature range for operation	0°C ... +50°C
	Ambient temperature range for storage	-20°C ... +80°C
	Humidity range	10 % … 93 % relative humidity (non-condensing)

© Hilscher 2021

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

Table 30: Technical data netFIELD OnPremise (NIOT-E-TIJCX-GB-RE/NFLD)

© Hilscher 2021

9 Decommissioning, dismounting and disposal

9.1 Putting the device out of operation

NOTICE

Danger of Unsafe System Operation!

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

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

9.2 Removal of battery

Waste electronic equipment

Removal of battery

According to European Directive 2006/66/EU batteries may not be treated as household waste. As a consumer, you are legally obliged to dispose of batteries according to national and local regulations, for instance at the public collection sites for waste batteries.

Prior to the disposal of the device, you have to remove the battery for buffering the real-time-clock and to dispose it properly according to the applicable rules. In order to do so, follow the subsequent instructions.

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

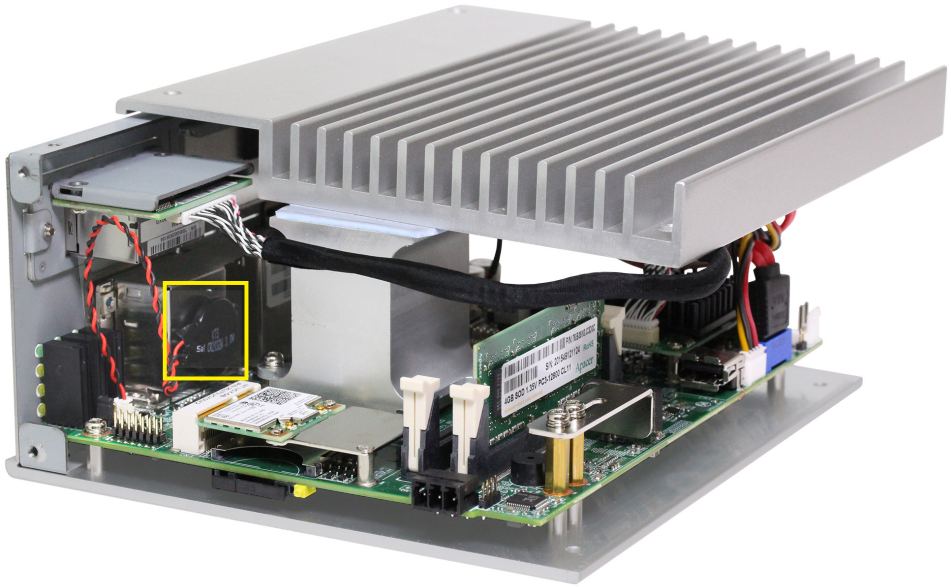


Figure 102: NIOT-E-TIJCX-GB-RE/NFLD battery

© Hilscher 2021

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.

© Hilscher 2021

10 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.

© Hilscher 2021

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 uninterruptable 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.

© Hilscher 2021

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.

© Hilscher 2021

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 OnPremise SW architecture ... 12
Figure 5: Front and top view ... 14
Figure 6: Device dimensions ... 16
Figure 7: LED positions on device ... 21
Figure 8: LED sticker ... 26
Figure 9: Mounting holes ... 27
Figure 10: Factory IP address settings of LAN interfaces ... 29
Figure 11: Host name on device label (example) ... 32
Figure 12: Setting IP address under Windows for direct LAN connection ... 33
Figure 13: Login Device Manager ... 34
Figure 14: Enter current password dialog ... 35
Figure 15: Enter new password dialog ... 35
Figure 16: Re-Authentication dialog ... 36
Figure 17: System time value ... 37
Figure 18: Change System Time dialog ... 37
Figure 19: “Basic” onboarding screen in Device Manager ... 40
Figure 20: Research Hardware ID ... 43
Figure 21: Add device mask in netFIELD Portal ... 44
Figure 22: Activation Code in portal ... 45
Figure 23: Advanced Onboarding tab in device ... 46
Figure 24: Example of an API Key permitting to onboard devices ... 48
Figure 25: Copy key to clipboard ... 49
Figure 26: Overview Local Device Manager ... 50
Figure 27: System page in Local Device Manager ... 52
Figure 28: Change host name dialog ... 53
Figure 29: Networking page ... 55
Figure 30: Details of LAN interface (eth0) ... 57
Figure 31: IPv4 Settings ... 58
Figure 32: Manual IPv4 Settings ... 58
Figure 33: Open Firewall configuration page ... 61
Figure 34: Elements on Firewall configuration page ... 61
Figure 35: Add Zone dialog ... 63
Figure 36: Add services ... 66
Figure 37: Add custom services dialog ... 67
Figure 38: Add forward port dialog ... 68
Figure 39: Network Proxy configuration ... 69
Figure 40: Proxy Settings dialog window ... 70

© Hilscher 2021

Figure 41: Using one Proxy server for all protocols ... 71
Figure 42: Separate HTTP/HTTPS/FTP configuration ... 72
Figure 43: Restart dialog after changing proxy server configuration ... 73
Figure 44: Synchronize proxy settings with netFIELD Portal ... 74
Figure 45: Wi-Fi Client Mode ... 76
Figure 46: Client mode parameters ... 78
Figure 47: Connect Network dialog ... 80
Figure 48: Connect network message ... 82
Figure 49: Access Point Mode ... 84
Figure 50: Warning note ... 85
Figure 51: Configure Interface message ... 85
Figure 52: wlan0 configuration page ... 86
Figure 53: Set manual address in IPv4 Settings dialog ... 86
Figure 54: Enter Manual IP Address ... 87
Figure 55: Configured DHCP service ... 88
Figure 56: DHCP Server Configuration dialog ... 90
Figure 57: Basic Onboarding page ... 92
Figure 58: Offboarding “Basic” ... 93
Figure 59: Offboarding “Advanced” ... 93
Figure 60: Standard Docker ... 95
Figure 61: Expand concise container details ... 96
Figure 62: Container parameters with terminal window ... 97
Figure 63: Image Search dialog of Standard Docker ... 98
Figure 64: Run Image dialog ... 99
Figure 65: Expand image details ... 100
Figure 66: Image details ... 101
Figure 67: IOT Edge Docker ... 102
Figure 68: Container details expanded ... 104
Figure 69: Container parameters ... 105
Figure 70: IoT image expanded ... 106
Figure 71: Details of netFIELD Proxy image ... 107
Figure 72: Accounts ... 108
Figure 73: Create new account ... 108
Figure 74: Edit account ... 109
Figure 75: Web Server Certificate page ... 111
Figure 76: General Settings ... 112
Figure 77: Web Server Settings tab ... 113
Figure 78: Default MQTT Settings ... 114
Figure 79: Docker Network Settings ... 116
Figure 80: Default docker network configuration ... 118
Figure 81: OT interface ... 119

© Hilscher 2021

Figure 82: Remote Access tab 121
Figure 83: Terminal 123
Figure 84: OS update page 124
Figure 85: Selected OS update image 125
Figure 86: Upload finished message 126
Figure 87: OS update “Disconnected” message 127
Figure 88: Logs 128
Figure 89: Formatting USB stick 130
Figure 90: Format USB STICK dialog window 131
Figure 91: Formatted USB stick 131
Figure 92: Prepared USB stick 132
Figure 93: BIOS start screen 133
Figure 94: BIOS setup menu 133
Figure 95: Boot options tab in BIOS setup menu 134
Figure 96: Boot option #1 in BIOS setup menu 134
Figure 97: List for boot option #1 135
Figure 98: Save & Exit tab 135
Figure 99: Save & Reset security question 136
Figure 100: Boot options question 136
Figure 101: Firmware update in progress 137
Figure 102: NIOT-E-TIJCX-GB-RE/NFLD battery 142

© Hilscher 2021

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 17
Table 5: Parameters of the serial interface 18
Table 6: RS-232 D-Sub 19
Table 7: RS-422 D-Sub 19
Table 8: RS-485 D-Sub 19
Table 9: Description of device status LEDs 22
Table 10: LEDs LAN interface 23
Table 11: Tasks for commissioning the device (netFIELD Portal user) 24
Table 12: Tasks for commissioning the device (Standard Docker user) 25
Table 13: Available Firewall zones 62
Table 14: Elements in Add Zone dialog 63
Table 15: Columns/elements in Allowed Services table 65
Table 16: Columns/elements in Forward Ports table 67
Table 17: Control elements in main toolbar 68
Table 18: Wi-Fi operating modes 77
Table 19: Currently Connected Network 79
Table 20: Visible Networks 79
Table 21: Parameters in Connect Network dialog (1) 80
Table 22: Parameters in Connect Network dialog (2) 81
Table 23: Connection Profiles 83
Table 24: Access Point parameters 84
Table 25: Elements/Parameters on DHCP Server page 88
Table 26: Parameters of DHCP Server Configuration dialog 90
Table 27: Default MQTT Client Settings 115
Table 28: Standard Docker Network Settings 117
Table 29: Standard Docker Network Settings 118
Table 30: Technical data netFIELD OnPremise (NIOT-E-TIJCX-GB-RE/NFLD) 140

© Hilscher 2021

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

Support

Phone: +49 (0) 6190 9907-99
E-mail: de.support@hilscher.com

SUBSIDIARIES

China

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

Support

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

France

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

Support

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

India

Hilscher India Pvt. Ltd.
Pune, Delhi, Mumbai
Phone: +91 8888 750 777
E-mail: info@hilscher.in

Italy

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

Support

Phone: +39 02 25007068
E-mail: it.support@hilscher.com

Japan

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

Support

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

Korea

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

Switzerland

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

Support

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

USA

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

Support

Phone: +1 630-505-5301
E-mail: us.support@hilscher.com

© Hilscher 2021