User manual

# netFIELD OnPremise

**Hilscher Gesellschaft für Systemautomation mbH**
**www.hilscher.com**

DOC200901UM06EN | Revision 6 | English | 2023-05 | Released | Public

# Table of contents

# 1 Introduction

## 1.1 About this document

### 1.1.1 Description of the contents

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

### 1.1.2 List of revisions

| 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:<br>Section *Brief description* [▸ page 9] updated.<br>Section *LAN connectors* [▸ page 19] updated.<br>Section *LEDs of the Real-Time Ethernet interface* [▸ page 25] updated.<br>Section *Establish LAN connection and login to Local Device Manager* [▸ page 31] updated.<br>Section *"Onboard" (register) device in netFIELD Cloud* [▸ page 41] updated.<br>Section *Firewall* [▸ page 62] updated.<br>Section *Using the cifx0 interface (RTE)* removed (substituted by section *OT Interface (Using the cifx0 interface or RTE)* [▸ page 94]).<br>Section *Networking Services* [▸ page 78] added.<br>Section *Standard Docker* [▸ page 111] revised.<br>Section *IoT Edge Docker* [▸ page 117] revised.<br>Section *OT Interface (Using the cifx0 interface or RTE)* [▸ page 94] added.<br>Section *Remote Access* [▸ page 108] added. |

| Index | Date | Author | Revision |
|---|---|---|---|
| 3 | 2022-05-04 | MKE | Document revised and updated to netFIELD OS 2.3.<br>Section *Terms and abbreviations* [▸ page 8] revised.<br>Subsection *Services supported by netFIELD OS* in section *netFIELD OS: Industrial IoT Operating System* [▸ page 10] updated.<br>Section *Risk of denial of service due to extensive memory usage close to limits* [▸ page 15] added.<br>Subsection *Enabling access for application containers* in section *Serial interfaces COM1 and COM2* [▸ page 20] added.<br>Section *OT Interface (Using the cifx0 interface or RTE)* [▸ page 94] moved from *General Settings* to *Networking Services*.<br>Section *Connectivity Check* [▸ page 96] added.<br>Section *Login* [▸ page 110] added.<br>Section *OS Update* [▸ page 129] updated.<br>Section *Services* [▸ page 139] added.<br>Chapter *Decommissioning, dismounting and disposal* [▸ page 156] revised.<br>Section *Legal notes* [▸ page 159] updated. |
| 4 | 2022-12-16 | MKE | Document updated to netFIELD OS 2.4.<br>Sections *Onboarding using the “Basic” method* [▸ page 43] and *Onboarding (and offboarding)* [▸ page 98] updated (two-factor-authentication in Portal now supported).<br>Section *Docker Network Settings* [▸ page 104] updated and revised (DNS server configuration added).<br>Section *Accounts* [▸ page 123] updated (new roles added).<br>Section *Operating System* [▸ page 129] added.<br>Section *Backup & Restore* [▸ page 134] added.<br>Section *Factory Reset* [▸ page 137] added.<br>Chapter *Decommissioning, dismounting and disposal* [▸ page 156] revised. |
| 5 | 2023-02-10 | MKE | RAM in chapter *Technical data* [▸ page 154] updated. |
| 6 | 2023-05-02 | MKE | Download instructions in sections *OS Update* [▸ page 129] and *Device recovery via USB* [▸ page 143] updated. |

*Table 1: List of revisions*

### 1.1.3 Conventions in this document

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

**Notes**

**Important:**
<important note you must follow to avoid malfunction>

**Note:**
<general note>

<note on further information>

**Instructions**

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

**Results**

⤷ Intermediate result

⇨ Final result

## 1.2 Terms and abbreviations

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

*Table 2: Terms and abbreviations*

# 2 Brief description

## 2.1 Intended use

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

## 2.2 Key features

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

## 2.3 netFIELD OS: Industrial IoT Operating System

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

### Features

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

### Architecture

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

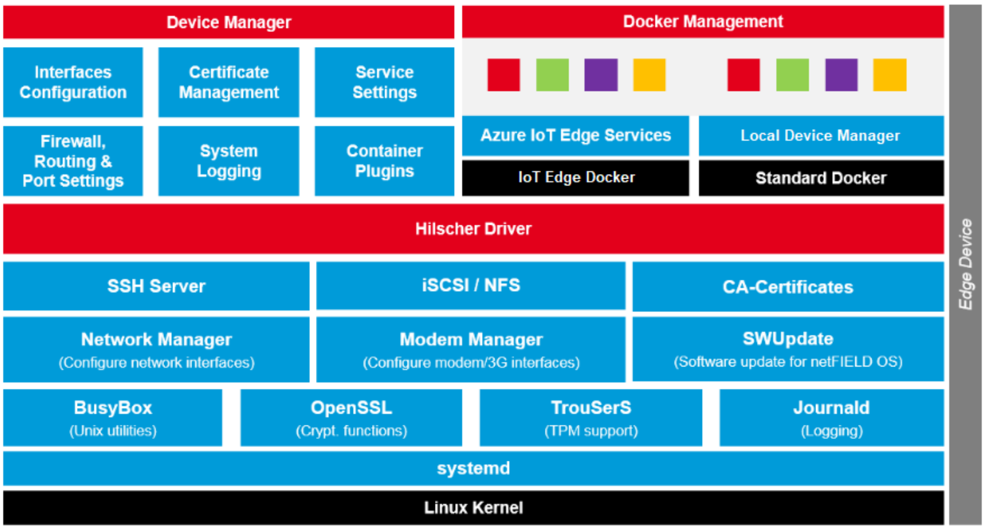


*Figure 1: netFIELD OS architecture*

### Core services

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

### Container management

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

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

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

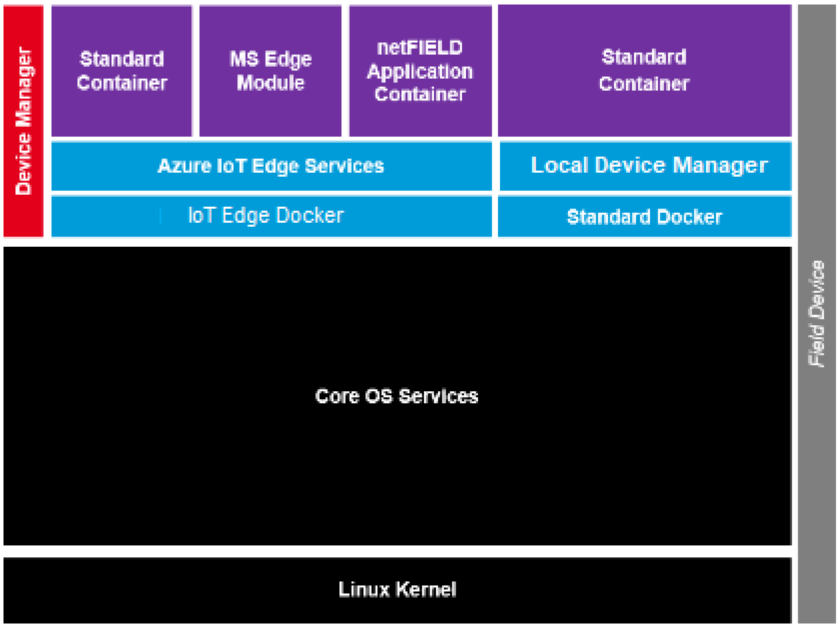


*Figure 2: netFIELD OS container management*

### Inter-container communication

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

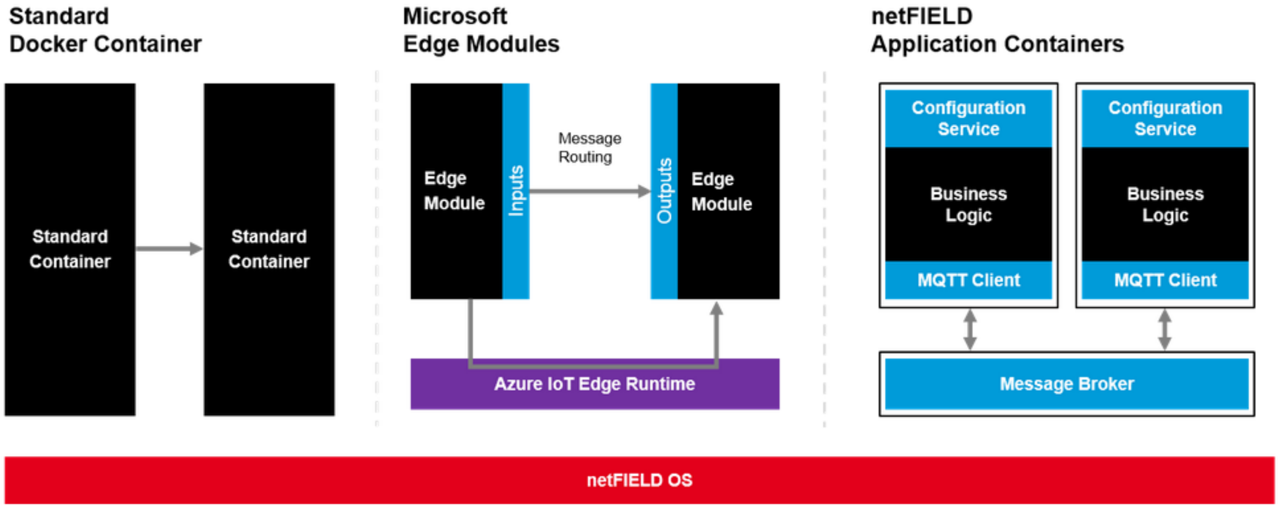


*Figure 3: netFIELD OS inter-container communication*

### Services supported by netFIELD OS

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

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

## 2.4 Depiction of netFIELD OnPremise SW architecture

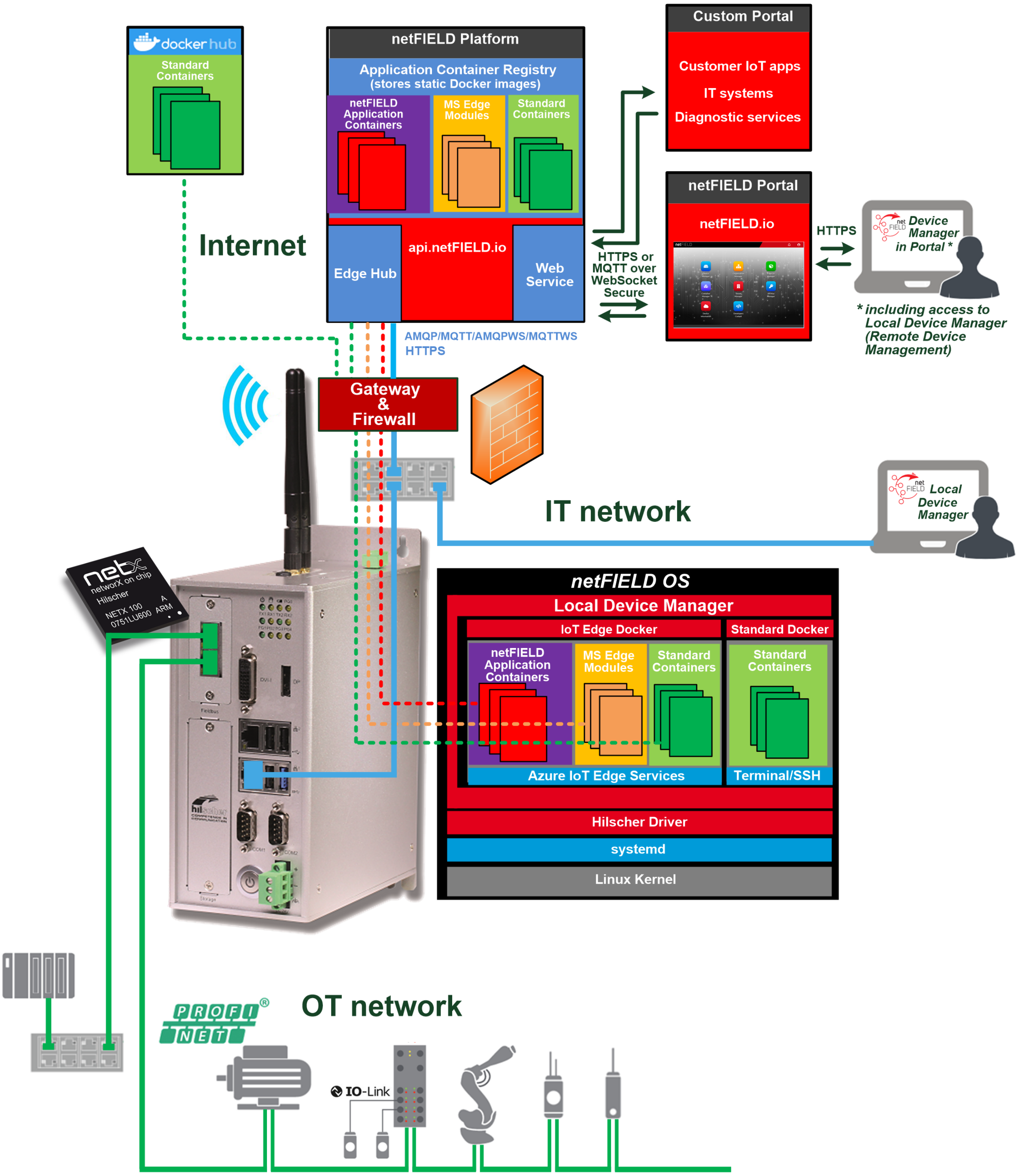


Figure 4: netFIELD OnPremise SW architecture

# 3 Safety

## 3.1 General note

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

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

Keep this manual for future reference.

## 3.2 Personnel qualification

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

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

## 3.3 Device destruction by exceeding the allowed supply voltage

Observe the following notes concerning the voltage supply:

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

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

Using applications that exceed the memory resources of the device can cause an out-of-memory situation (OOM) in the Linux kernel leading to temporary delayed application reaction times and limited overall device responsiveness.
You must therefore consider the memory requirements of your Docker containers carefully before deploying them on the device. We also recommend you to configure the logging behavior (e.g. log levels) of your containers accordingly.

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

# 4 Hardware description

## 4.1 Device drawings

### 4.1.1 Positions of the interfaces

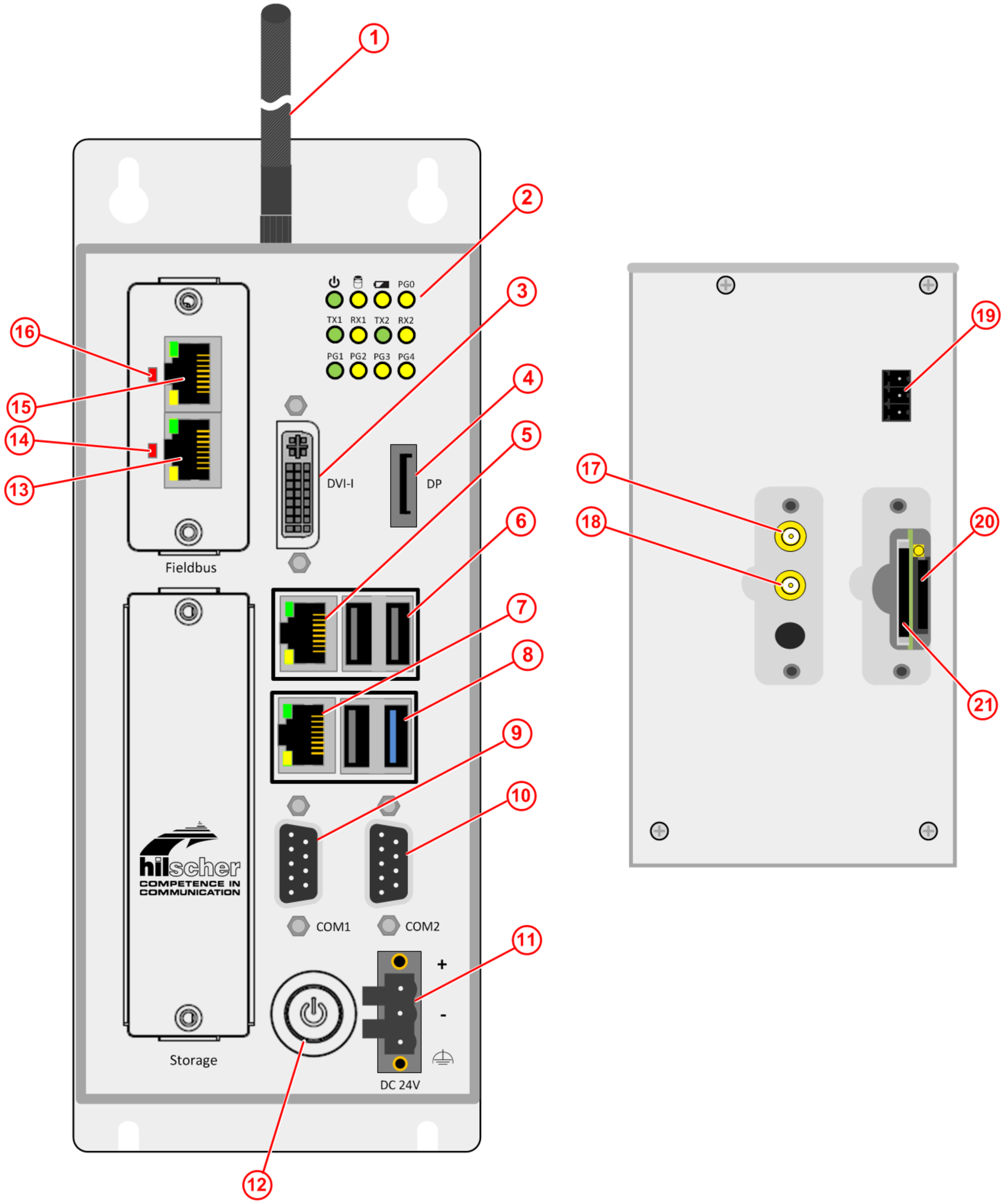


*Figure 5: Front and top view*

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

*Table 3: Positions of the interfaces*

## 4.1.2 Dimensions

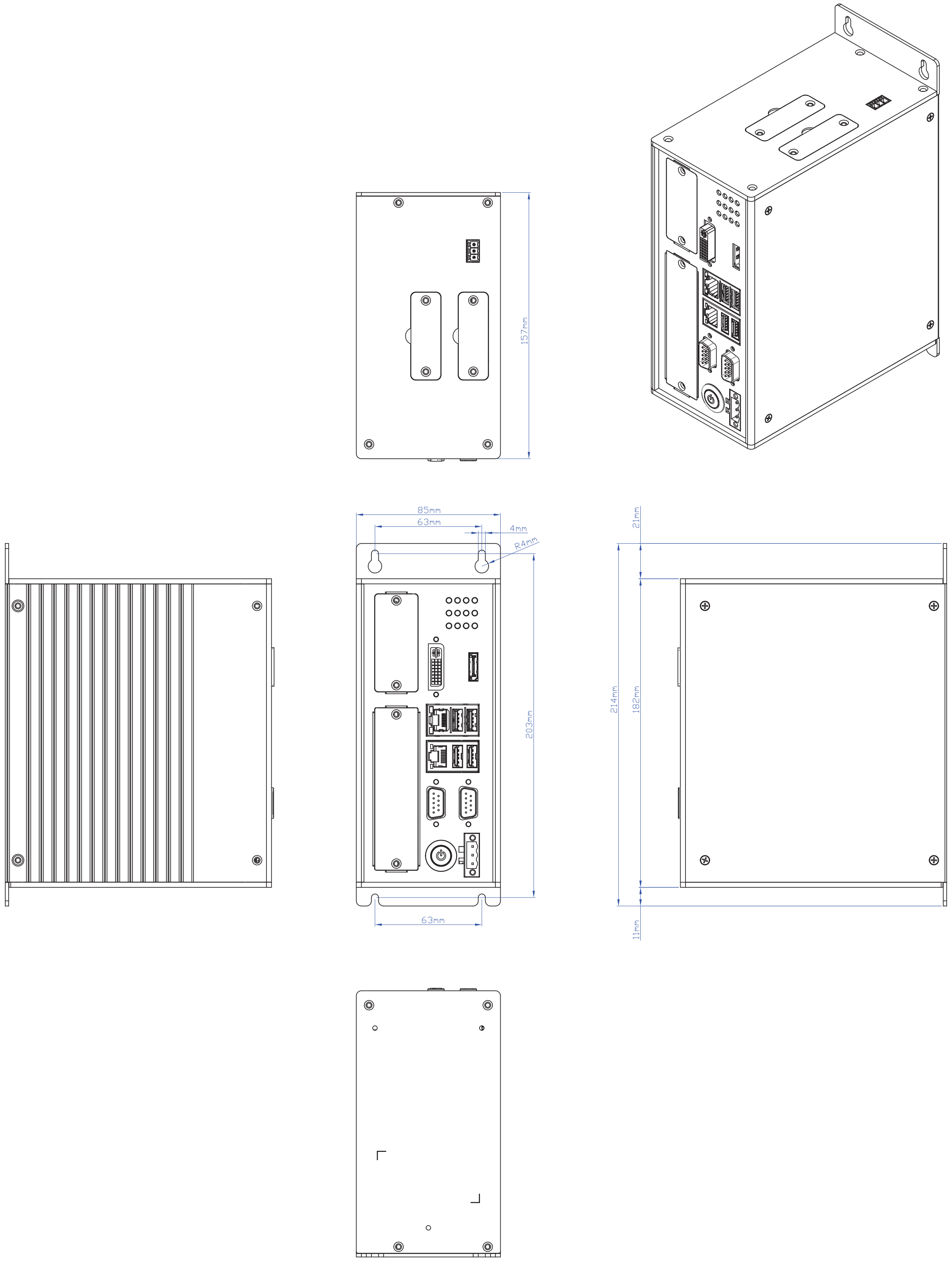


*Figure 6: Device dimensions*

# 4.2 Interfaces

## 4.2.1 Power supply

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

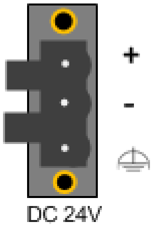
| DC 24V | Pin | Signal | Description |
|---|---|---|---|
|  | + | +24 V DC | +24 V DC |
| | - | GND | Ground (Reference potential) |
| | ⏚ | FE | Functional earth |

*Table 4: Power supply connector*

## 4.2.2 LAN connectors

The two RJ45 connectors (see positions (5) and (7) in section *Positions of the interfaces* [▸ page 16]) allow you to connect your device to your IT network, respectively to the cloud (e.g. the netFIELD Portal).
The MAC addresses of the LAN interfaces are printed on the device label.
Note that the “factory setting” for the IP address of the LAN port 1 (eth0) is DHCP mode (“fallback” is *link-local*, i.e. address block `169.254.0.0/16`).
The “factory setting” for the IP address of the LAN port 2 (eth1) is `192.168.253.1`
You can change the IP address settings in the Local Device Manager (see section *Networking* [▸ page 57]).

## 4.2.3 Real-Time Ethernet connectors

The two RJ45 connectors (see positions (13) and (15) in section *Positions of the interfaces* [▸ page 16]) allow you to connect your device to a Real-Time Ethernet network (OT network).
The MAC addresses of the RTE interfaces are printed on the device label (“Fieldbus MAC addr.”)
Note that you must deploy software containers featuring the corresponding applications (e.g. *netFIELD App PROFINET Device*) on the device in order to use the Real-Time Ethernet interface.

**Note:**
The RTE interface can also be used like a standard Ethernet TCP/IP interface with limited data throughput. (In this case, “multicasts” are not supported.)
If you want to do so, you can enable this option in the **Local Device Manager** under **Networking Services** > **OT Interface** (see section *OT Interface (Using the cifx0 interface or RTE)* [▸ page 94] for further information).

## 4.2.4 USB connectors

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

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

## 4.2.5 Serial interfaces COM1 and COM2

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

### Requirements for using the serial interfaces

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

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

### BIOS settings

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

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

*Table 5: Parameters of the serial interface*

### Enabling access for application containers

netFIELD OS supports the serial interfaces as standard Linux devices:
COM1: `/dev/ttyS0`
COM2: `/dev/ttyS1`
Docker application containers accessing the `ttyS0` or `ttyS1` interfaces must be either running as `root` user or as a member of the `dialout` group in Linux. If your container is not a `root` user, you can add the container to the `dialout` group with the `--group-add dialout` parameter in your `docker run` command during container deployment. Note that you must also map the `/dev/ttyS0` respectively `/dev/ttyS1` interface into the corresponding container.

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

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

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

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

### Pinning RS-232

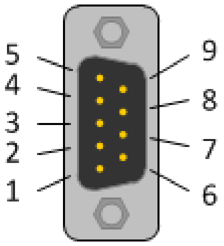
| RS-232 | Pin | Signal | Description |
|---|---|---|---|
|  | 1 | DCD | Data Carrier Detect |
| | 2 | RXD | Receive signal |
| | 3 | TXD | Send signal |
| | 4 | DTR | Data Terminal Ready |
| | 5 | ISO_GND | Ground (reference potential) |
| | 6 | DSR | Data Set Ready |
| | 7 | RTS | Request to Send |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

*Table 6: RS-232 D-Sub*

### Pinning RS-422

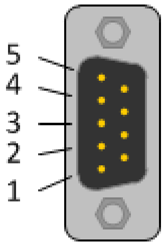
| RS-422 | Pin | Signal | Description |
|---|---|---|---|
|  | 1 | Tx- | Send signal negative |
| | 2 | Tx+ | Send signal positive |
| | 3 | Rx- | Receive signal negative |
| | 4 | Rx+ | Receive signal positive |
| | 5 | ISO_GND | Ground (reference potential) |
| | 6 | n.c. | - |
| | 7 | n.c. | - |
|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

*Table 7: RS-422 D-Sub*

**Pinning RS-485**

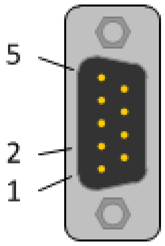
| RS-485 | Pin | Signal | Description |
|---|---|---|---|
|  | 1 | Rx/Tx- | Send/receive signal negative |
| | 2 | Rx/Tx+ | Send/receive signal positive |
| | 3 | n.c. | - |
| | 4 | n.c. | - |
| | 5 | ISO_GND | Ground (reference potential) |
| | 6 | n.c. | - |
| | 7 | n.c. | - |
| | 8 | n.c. | - |
|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

*Table 8: RS-485 D-Sub*

## 4.2.6 Wi-Fi

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

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

## 4.2.7 Monitor connectors

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

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

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

# 4.3 LEDs

## 4.3.1 Positions of the LEDs on the device

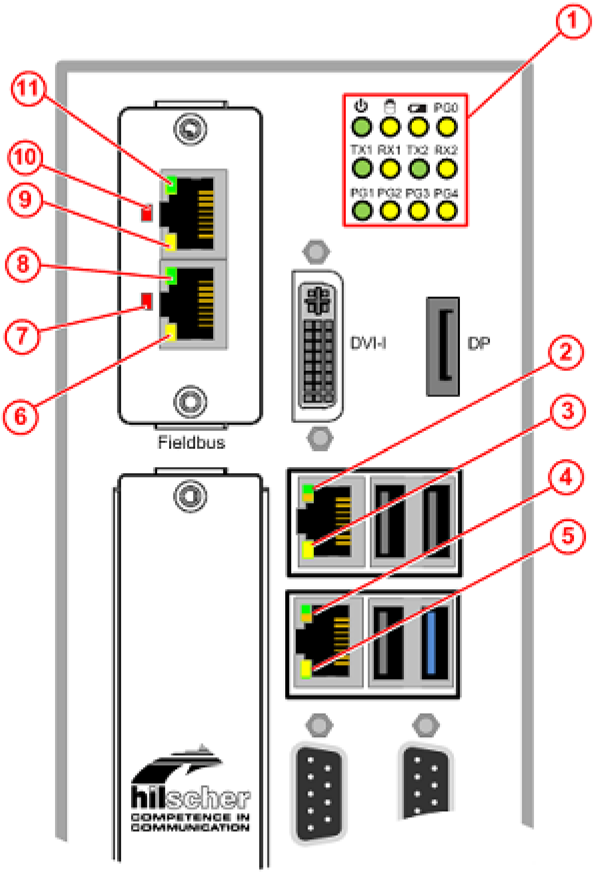


*Figure 7: LED positions on device*

## 4.3.2 Device status LEDs

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

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

*Table 9: Description of device status LEDs*

## 4.3.3 LEDs of the LAN interface

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

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

*Table 10: LEDs LAN interface*

## 4.3.4 LEDs of the Real-Time Ethernet interface

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

**Note:**
The COM LED (position (7) in section *Positions of the LEDs on the device* [▸ page 23]) shows steady red light if the TCP/IP channel of the cifx0 interface is enabled. See section *OT Interface (Using the cifx0 interface or RTE)* [▸ page 94] for further information.

# 5 Commissioning and first steps

## 5.1 Overview

### 5.1.1 netFIELD Portal user

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

| # | Step | For details see |
|---|---|---|
| 0 | Requirement:<br>• 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 31] |
| | | |
| 3 | Set local system time. | Section *Set system time* [▸ page 39] |
| | | |
| 4 | If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server. | Section *Network Proxy settings* [▸ page 72] |
| | | |
| 5 | If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings. | Section *Docker Network Settings* [▸ page 104] |
| | | |
| 6 | Optional: Configure netFIELD OS firewall.<br>**Note**: By default, the internal netFIELD OS firewall allows all traffic (“trusted zone”).<br>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 62] |
| | | |
| 7 | “Onboard” (register) device in netFIELD Portal.<br>**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.<br>MQTT: `8883`<br>MQTT over WebSocket: `443`<br>AMQP: `5671`<br>AMQP over WebSocket: `443` | Section *"Onboard" (register) device in netFIELD Cloud* [▸ page 41] |
| | | |
| 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)*

## 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 31] |
| | | |
| 3 | Set local system time. | Section *Set system time* [▸ page 39] |
| | | |
| 4 | If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server. | Section *Network Proxy settings* [▸ page 72] |
| | | |
| 5 | If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings. | Section *Docker Network Settings* [▸ page 104] |
| | | |
| 6 | Optional: Configure netFIELD OS firewall.<br>**Note**: By default, the internal netFIELD OS firewall allows all traffic (“trusted zone”).<br>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 62] |
| | | |
| 7 | Open Standard Docker and deploy and run container images. | Section *Standard Docker* [▸ page 111] |

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

# 5.2 Mounting

## 5.2.1 Attaching LED sticker (optional)

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

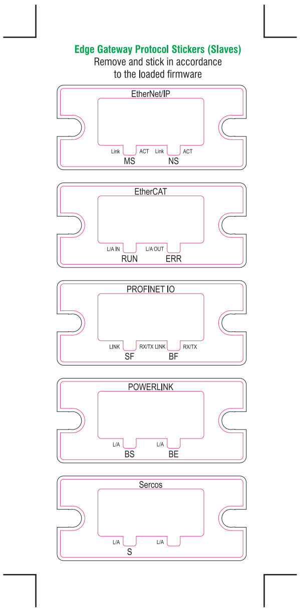


*Figure 8: LED sticker*

### 5.2.2 Mounting

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

The figure shows the distance of the mounting holes:

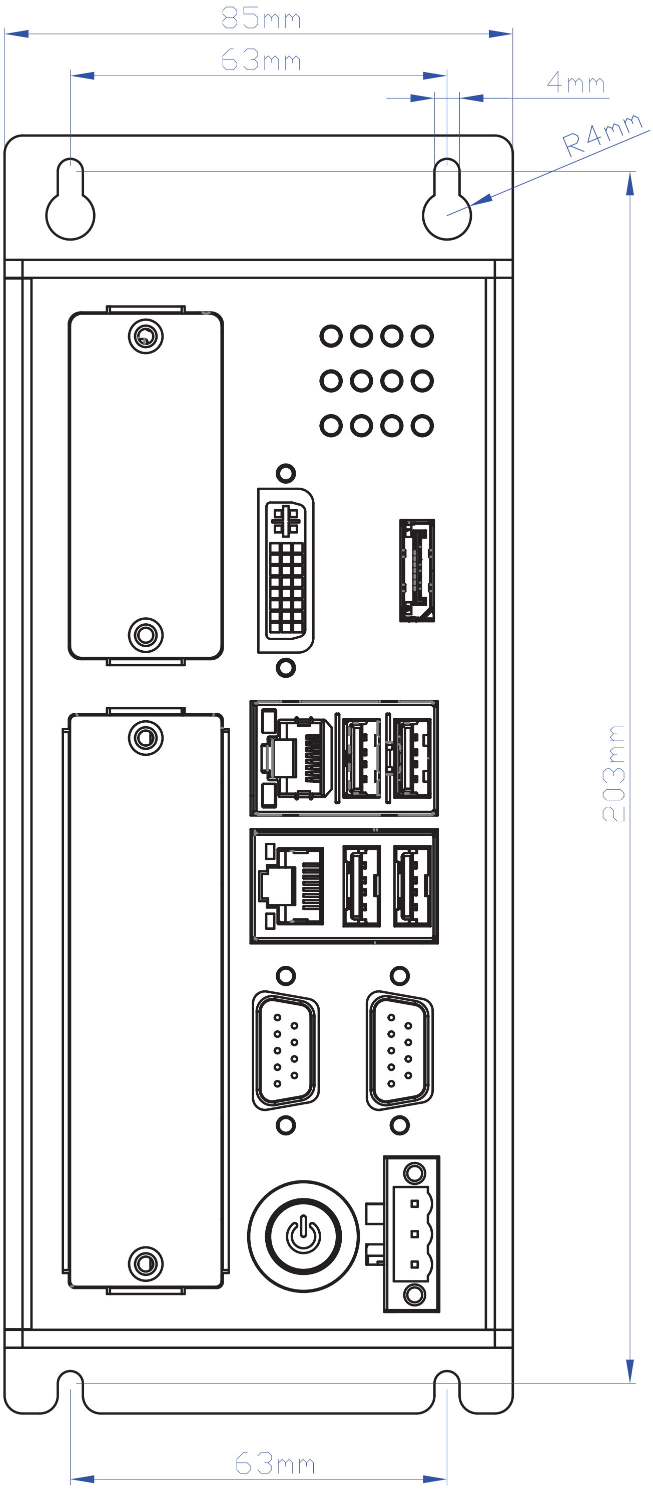


*Figure 9: Mounting holes*

### 5.2.3 Connecting Voltage suppy

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

**NOTICE**

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

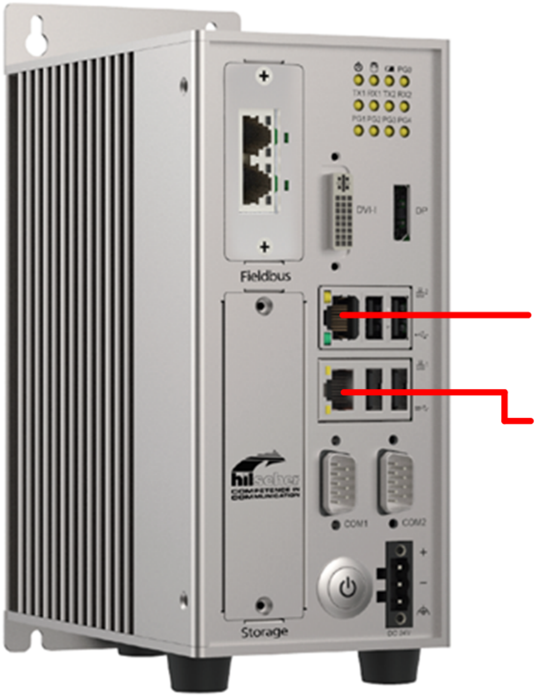
The supply voltage must not exceed 30 V; otherwise the device will be damaged.

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

### 5.3.1 Overview

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

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



**LAN port 2 (eth1) default IP address setting:** `192.168.253.1` `255.255.255.0`

**LAN port 1 (eth0) default IP address setting:** `DHCP`
**(Fallback: IPv4 link local)**

*Figure 10: Factory IP address settings of LAN interfaces*

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

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

### 5.3.2 Using DHCP server

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

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

- Make sure that a DHCP service is available in your local network.
- Plug an Ethernet cable into the LAN port 🖧1 on the front panel of the device (see position (7) in section *Positions of the interfaces* [▸ page 16]), to connect it to your local network and to the DHCP server.

➾ Your device should now automatically obtain an IP address from the DHCP server. This may take a few minutes.
If you know the IP address that the DHCP server has assigned to your device, you can now access the **Local Device Manager** directly by entering the assigned IP address into the address bar of your web browser. If you do not know the IP address, you can use the Windows network environment (see “Alternative A” below) or the “host name” of the device (see “Alternative B” below) to connect with it.

**Note:**
The device outputs its hostname and the IP address (which it has received from the DHCP server) at its display interfaces. Thus, connecting a monitor to one of its display interface (see positions (3) and (4) in section *Positions of the interfaces* [▸ page 16]) allows you to check the assigned IP address.
In case no DHCP service is available, the “fallback” IPv4 link local address of eth0 interface will also be output at the display ports.

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

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

**Note:**
The device contains a certificate issued by Hilscher. Your browser will therefore issue an "unsecure connection" warning message before directing you to the Sign-In page of the Local Device Manager.
You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).

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

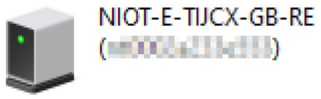
### Alternative A: Connecting via Windows network environment

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

**Note:**
Please make sure that the network discovery feature on your Windows PC is enabled for your security zone and that your PC and the device are located within the same subnet.
Note also that if a blocking or dropping zone was assigned to the LAN interface in the firewall, UPnP only works if port 80 (http) is allowed by your firewall settings.

➢ To display all devices in the network, open your **Windows Explorer** and select **Network**.

➯ You will find the device listed under **Other Devices**:

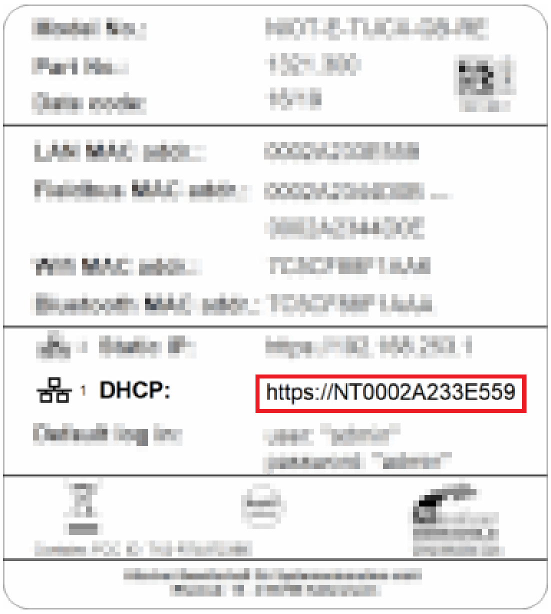


NIOT-E-TIJCX-GB-RE
([redacted])

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

### Alternative B: Connecting via host name

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



DHCP: https://NT0002A233E559

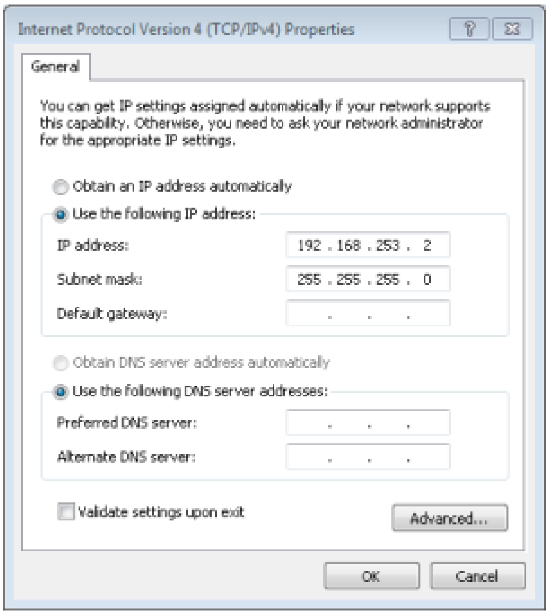
*Figure 11: Host name on device label (example)*

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

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

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

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 192 . 168 . 253 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

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

- ➢ Click **OK** and then **Close**.

3. Open browser and connect to device.

   ➢ You can now access the device from your PC or notebook via web browser by entering the following address into the address bar of your browser:
   `https://192.168.253.1`

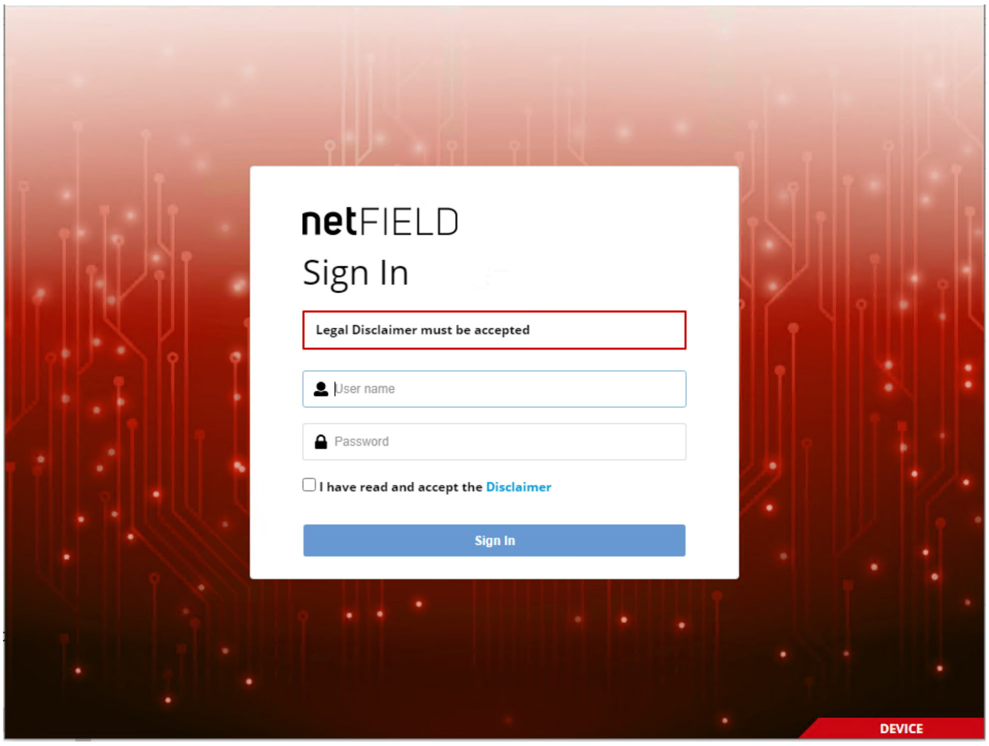
   ➯ A connection is established and the Local Device Manager opens in your browser window.

### 5.3.4 Login to Local Device Manager

**Note:**
When connecting to the device for the first time, your browser will probably issue a security warning before displaying the Login screen of the Local Device Manager.
You can ignore the warning and – depending on your browser model – select the option to continue to the device's website anyway (respectively add an "exception rule" for this website).

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

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



netFIELD

Sign In

Legal Disclaimer must be accepted

*Figure 13: Login Device Manager*

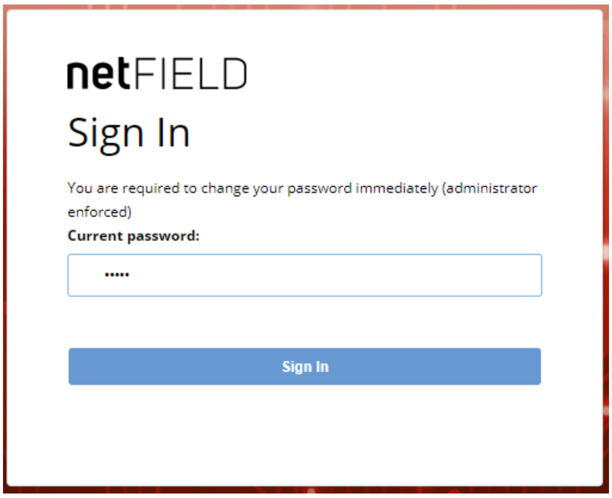
➢ In the **Sign In** dialog, enter the following default credentials:
**User name**: `admin`
**Password**: `admin`

➢ Read the **Disclaimer** then check the **I have read and accept the Disclaimer** box.

➢ Click **Sign In** button.

➩ For security reasons, you are now forced to change the default `admin` password immediately.

➢ In the **Current password** field, enter `admin` once again, then click **Sign In** button:



netFIELD

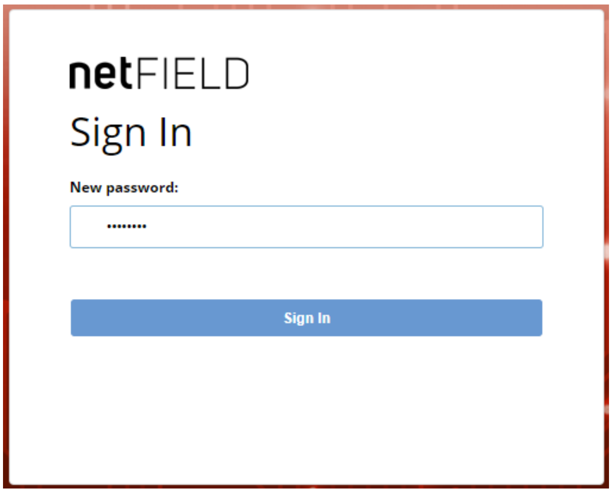
Sign In

You are required to change your password immediately (administrator enforced)

**Current password:** •••••

*Figure 14: Enter current password dialog*

➩ The **New password** dialog opens:



netFIELD

Sign In

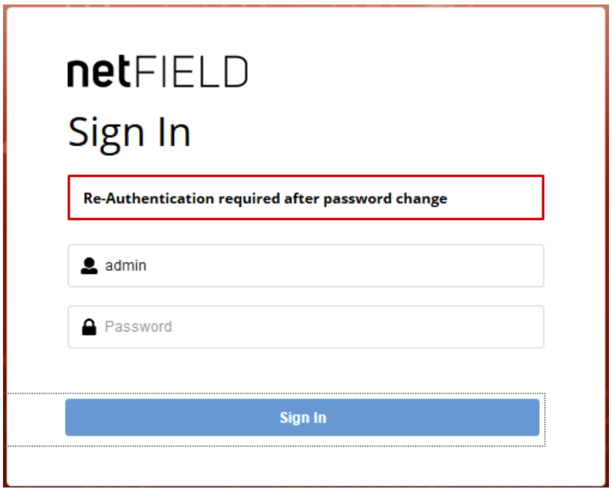
**New password:** ••••••••

*Figure 15: Enter new password dialog*

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

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

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



netFIELD

Sign In

Re-Authentication required after password change

admin

*Figure 16: Re-Authentication dialog*

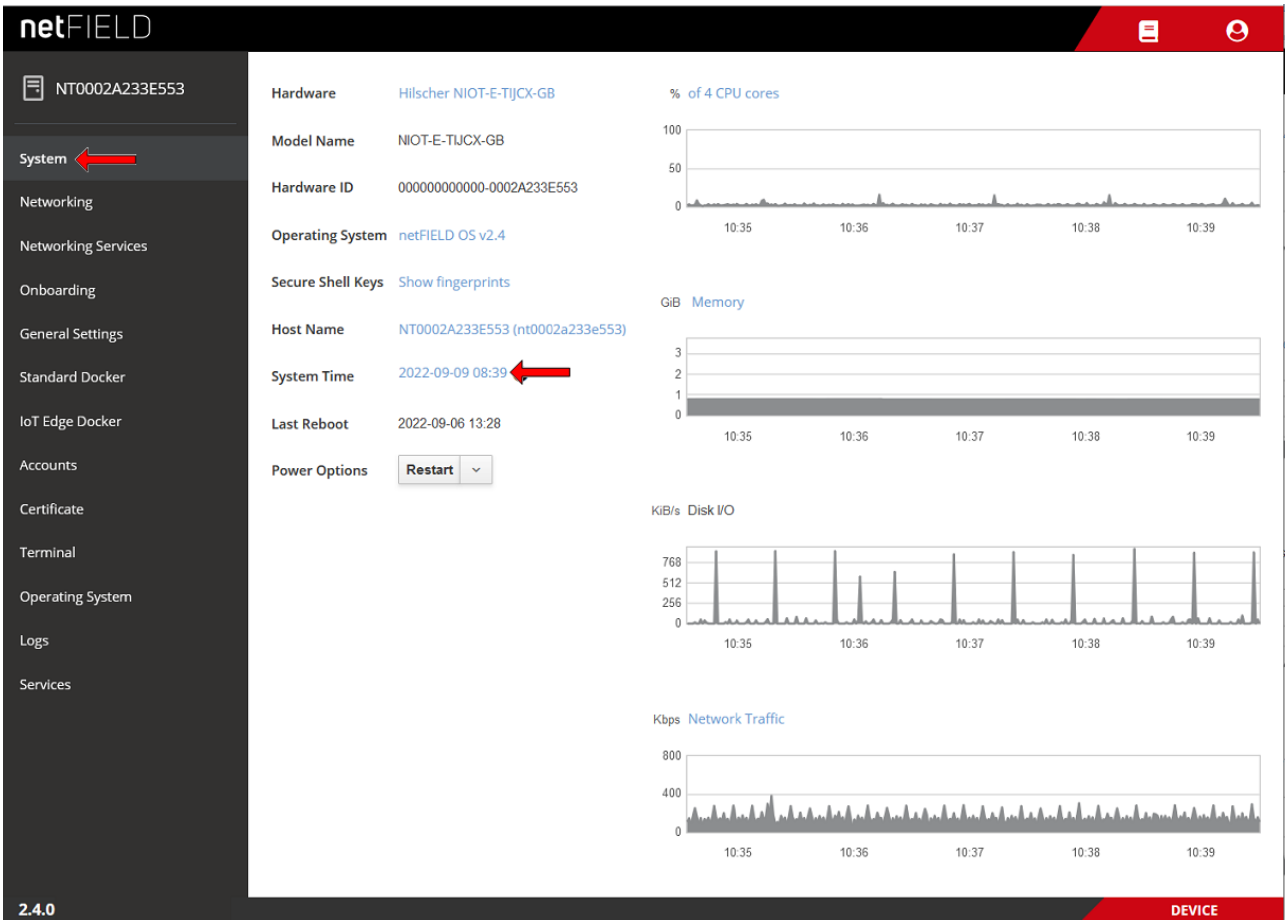
- Enter your new password once again, then click **Sign In** button
- The **Local Device Manager** opens.

## 5.4 Set system time

In the state of delivery of the device, the **Time Zone** of the system is set to **UTC** and the synchronization method (**Set Time**) to **Automatically using NTP** (**N**etwork **T**ime **P**rotocol service).

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

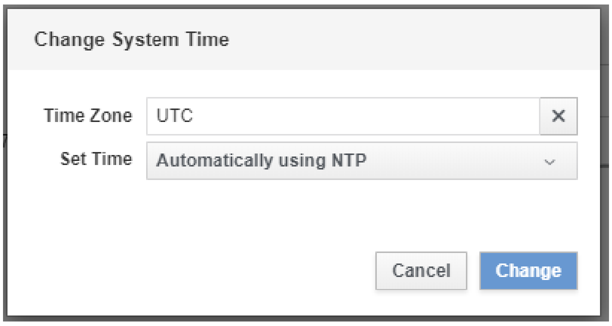
➢ To configure your local system time, open the **System** page of the **Local Device Manager**, then click the red date/time value next to **System Time**:



Hardware: Hilscher NIOT-E-TIJCX-GB
Model Name: NIOT-E-TIJCX-GB
Hardware ID: 000000000000-0002A233E553
Operating System: netFIELD OS v2.4
Secure Shell Keys: Show fingerprints
Host Name: NT0002A233E553 (nt0002a233e553)
System Time: 2022-09-09 08:39
Last Reboot: 2022-09-06 13:28
Power Options: Restart

*Figure 17: System time value*

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



Change System Time

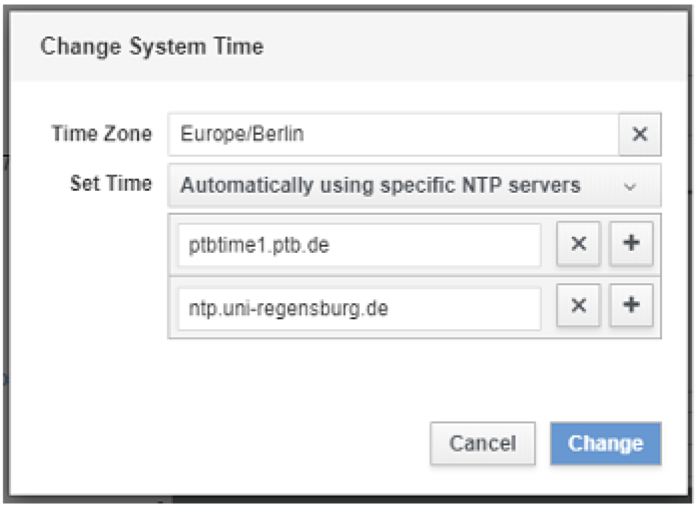
Time Zone: UTC

Set Time: Automatically using NTP

*Figure 18: Change System Time dialog*

- Click **x** button next to **Time Zone** field to delete the preset `UTC` value, then open the drop-down list and select the appropriate time zone region for your location (note that the list is searchable).
- To choose the synchronization method, choose one of the following options from the **Set Time** drop-down list:

- **Manually**: Opens further fields for manually entering current date (`yyyy-mm-dd`) and time (`hh:mm`). Synchronization via NTP service will not be used.
- **Automatically using NTP**: The system uses any available NTP server to obtain the correct time. (`pool.ntp.org` will be used by default).
- **Automatically using specific NTP servers**: Opens further fields for entering the addresses of certain NTP servers that you want to use, e.g. `ptbtime1.ptb.de`.
  You can create a list of several servers; the system will use the first server in the list that delivers a valid response. Click the **+** button to add a server. Click the **x** button to remove a server.



Change System Time

Time Zone: Europe/Berlin

Set Time: Automatically using specific NTP servers

ptbtime1.ptb.de

ntp.uni-regensburg.de

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

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

## 5.5.1 Overview

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

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

**Note:**
Connecting your device to the netFIELD Cloud requires an account/ subscription for the *netFIELD Cloud services* https://www.netfield.io.
Contact your local Hilscher sales representative for information on terms and conditions.

Before your device can be managed from the portal, it must first complete a one-time registration process, called “onboarding”.
This process is initialized by the device itself, not by the portal. There are three different onboarding methods: **Zero-Touch**, **Basic** and **Advanced**.

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

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

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

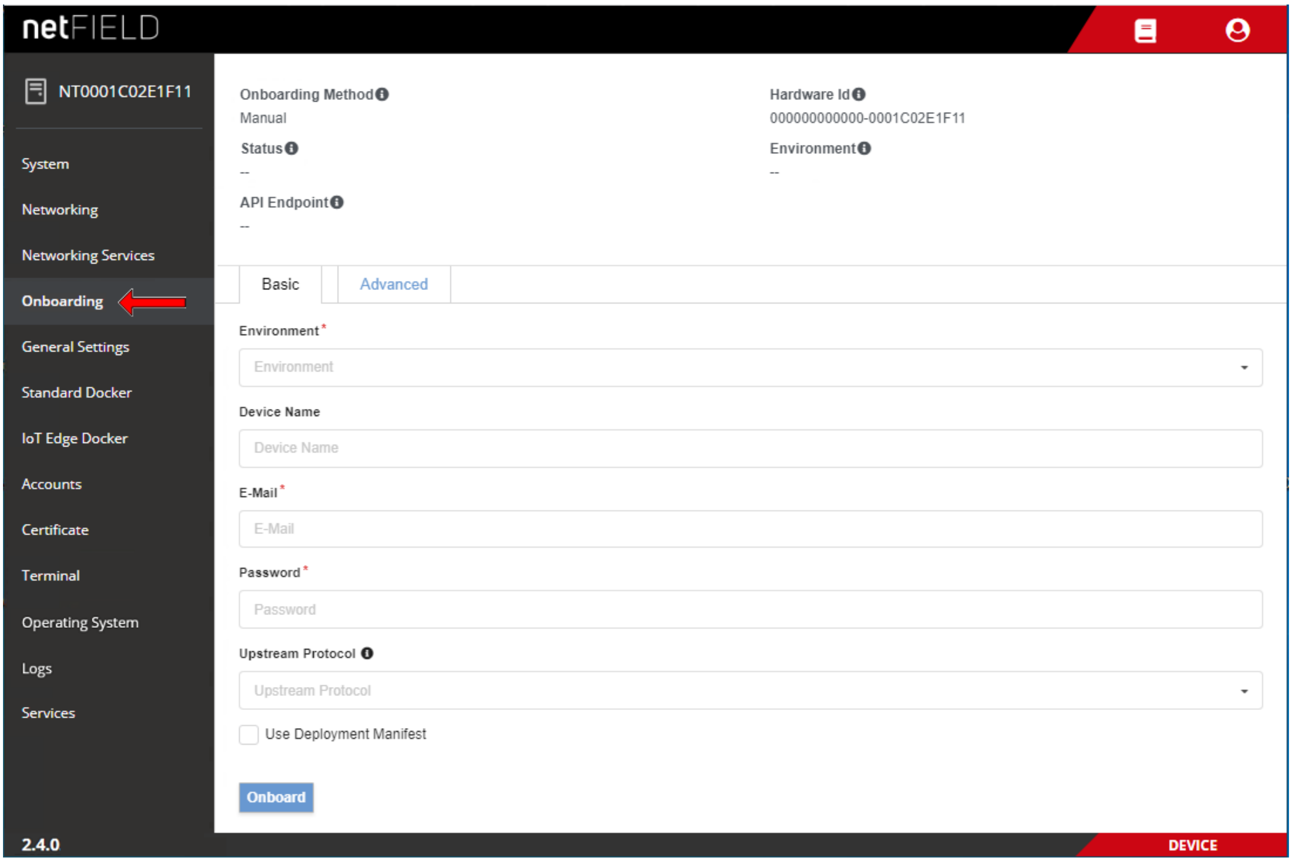
With the **Advanced** method (which allows onboarding in a certain separate instance of the netFIELD Portal), you must enter an `Activation Code`, an `API Key` and an `API End-Point` URL. You must research (respectively create) these parameters in the portal beforehand, then insert them in the **Onboarding**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

**Note:**
Before onboarding, make sure that your company's firewall does not block the TCP port (outgoing) of the upstream protocol (device-to-cloud communication) that you intend to use. The upstream protocol can be selected on the **Onboarding** page.
MQTT uses TCP port `8883`
MQTT over WebSocket uses TCP port `443`
AMQP (default protocol) uses TCP port `5671`
AMQP over WebSocket uses TCP port `443`

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

## 5.5.2 Onboarding using the “Basic” method

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



Onboarding Method: Manual
Hardware Id: 000000000000-0001C02E1F11
Status: --
Environment: --
API Endpoint: --

Environment*: Environment
Device Name: Device Name
E-Mail*: E-Mail
Password*: Password
Upstream Protocol: Upstream Protocol
□ Use Deployment Manifest

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

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

**Note:**
With these credentials (and the associated permissions), the device authenticates itself during onboarding in the portal and is automatically assigned to the organization or sub-organization of the user.
Ask your portal’s system administrator for the necessary credentials.

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

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

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

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

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

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

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

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

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

➢ If the netFIELD Portal account is protected by 2FA, you will now have to select your 2FA method and enter the passcode.
If the account is a member of other **Workspaces**, you will now also have to select the workspace in which you want to onboard the device.

⇨ The device connects to the portal, is registered there and assigned to your organization or sub-organization.
If the process has been successful, the following message appears:
**Success – Device is now onboarded**.
From now on, the device will be listed in the portal’s **Device Manager** and can be managed from there.

**Note:**
If the message “Something went wrong – Device has already been created” appears, the device had already been created in the **Device Manager** of the portal for the “Advanced” onboarding method.
In this case you can either use the “Advanced” onboarding method, or you can delete the device in the portal, and then start the “Basic” onboarding procedure here locally for a second time.

### 5.5.3 Onboarding using the “Advanced” method

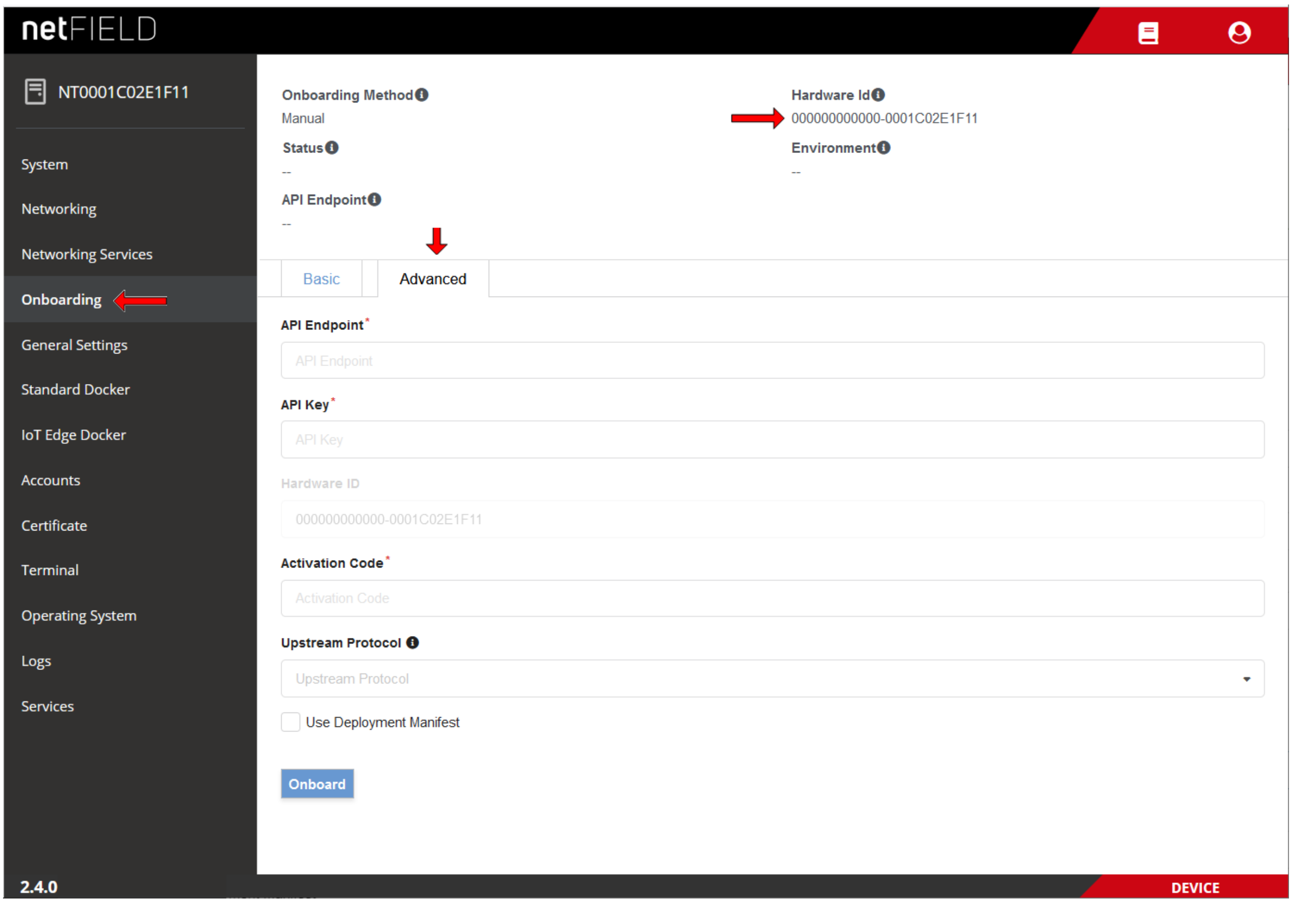
**Requirements**

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

**Step-by-step instructions**

1. Copy **Hardware ID**.

➢ In the navigation panel of the **Local Device Manager**, choose **Onboarding**, then open **Advanced** tab:



Onboarding Method
Manual

Status
--

API Endpoint
--

Hardware Id
000000000000-0001C02E1F11

Environment
--

API Endpoint*
API Endpoint

API Key*
API Key

Hardware ID
000000000000-0001C02E1F11

Activation Code*
Activation Code

Upstream Protocol
Upstream Protocol

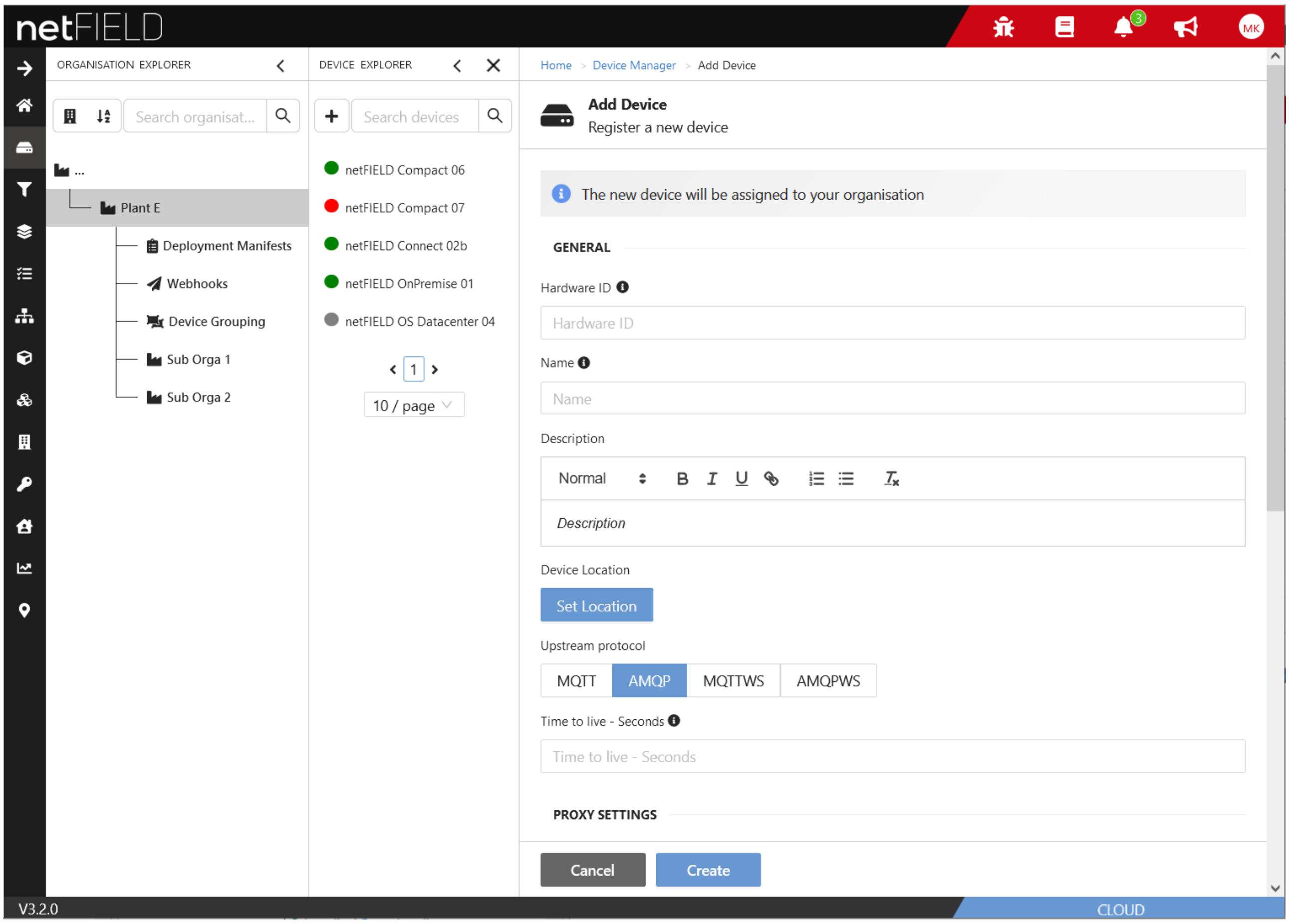
□ Use Deployment Manifest

*Figure 20: Research Hardware ID*

➢ Select the **Hardware ID** and copy the string to your clipboard.

- ⮚ Open a new tab in your browser and change to the portal, but do not close the connection to the **Local Device Manager** of your device in your first browser tab.

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



**Add Device**
Register a new device

The new device will be assigned to your organisation

GENERAL

Hardware ID: Hardware ID

Name: Name

Description: Normal — *Description*

Device Location: Set Location

Upstream protocol: MQTT [✓ AMQP] MQTTWS AMQPWS

Time to live - Seconds: Time to live - Seconds

PROXY SETTINGS

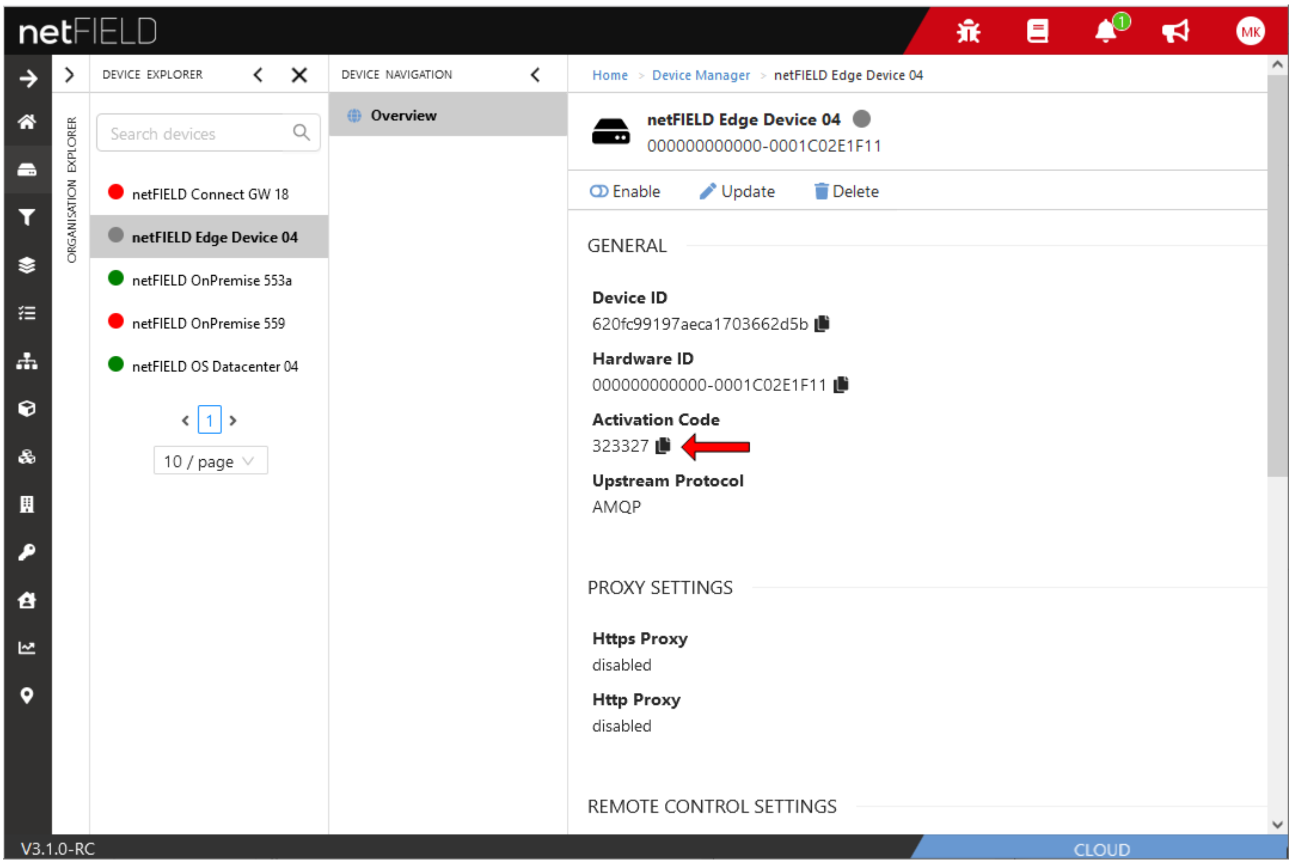
Cancel | Create

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



netFIELD Edge Device 04
000000000000-0001C02E1F11

GENERAL

Device ID
620fc99197aeca1703662d5b

Hardware ID
000000000000-0001C02E1F11

Activation Code
323327

Upstream Protocol
AMQP

PROXY SETTINGS

Https Proxy
disabled

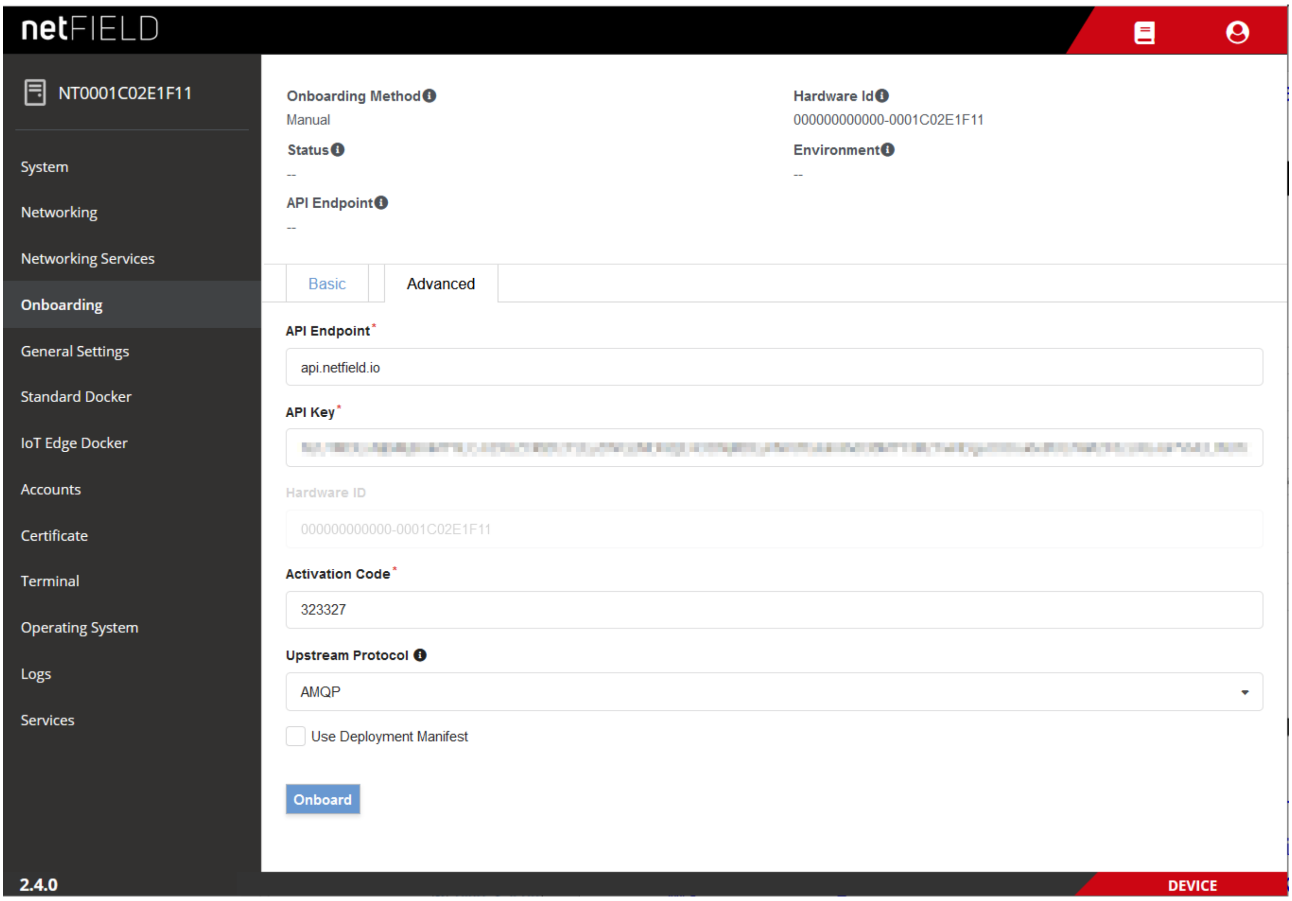
Http Proxy
disabled

REMOTE CONTROL SETTINGS

*Figure 22: Activation Code in portal*

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

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



Onboarding Method: Manual

Hardware Id: 000000000000-0001C02E1F11

Status: --

Environment: --

API Endpoint: --

API Endpoint*: api.netfield.io

API Key*: [redacted]

Hardware ID: 000000000000-0001C02E1F11

Activation Code*: 323327

Upstream Protocol: AMQP

□ Use Deployment Manifest

*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.

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

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

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

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

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

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

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

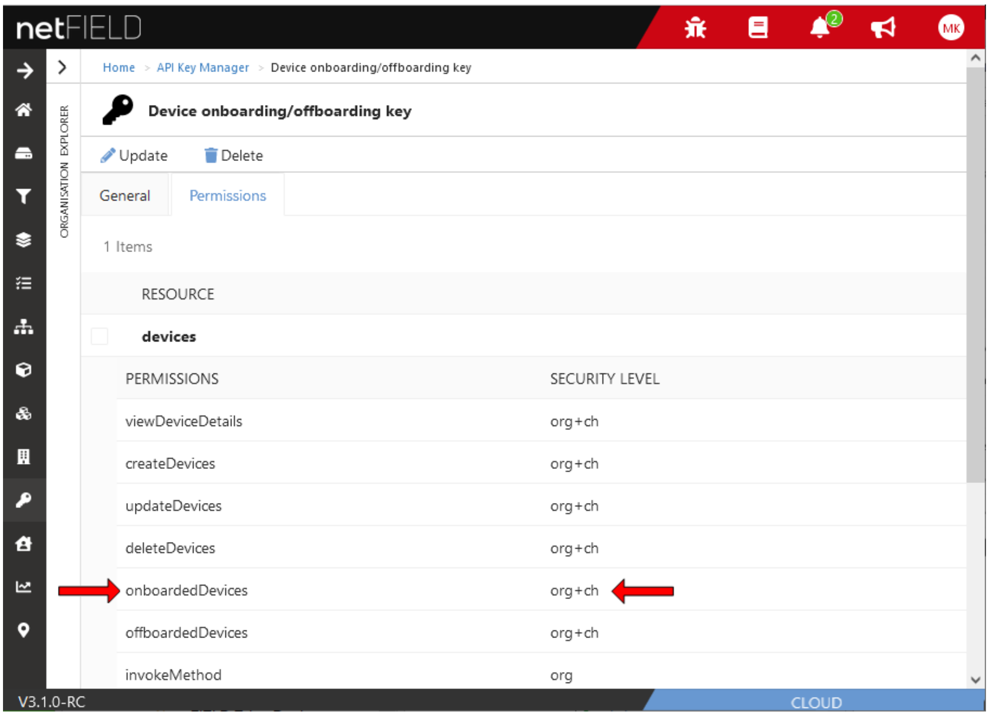
### Side note: How to copy an API Key for onboarding

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

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

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

To find out the permissions of an API Key, click on the key in the list, then open its **Permissions** tab:

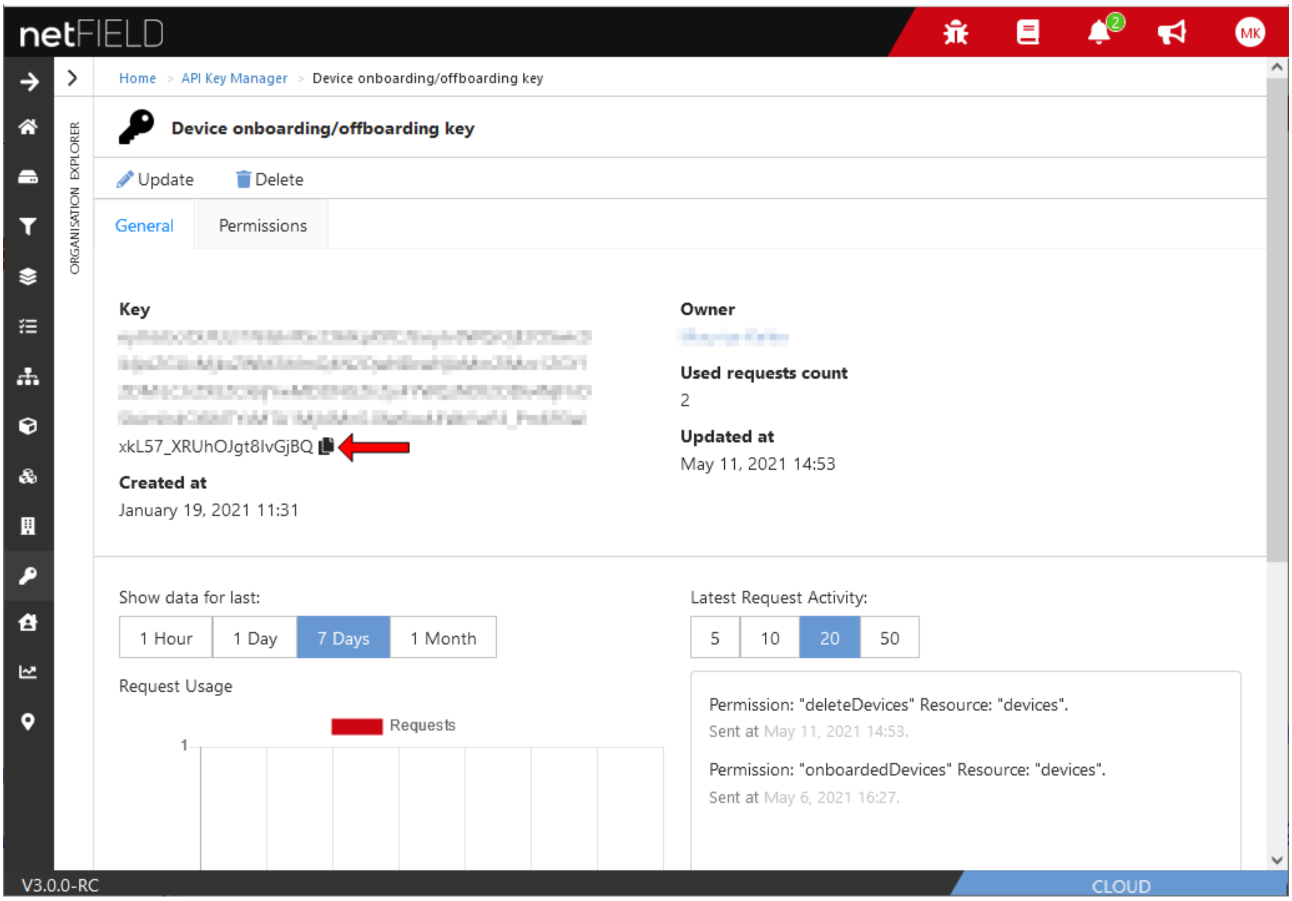


| PERMISSIONS | SECURITY LEVEL |
|---|---|
| viewDeviceDetails | org+ch |
| createDevices | org+ch |
| updateDevices | org+ch |
| deleteDevices | org+ch |
| onboardedDevices | org+ch |
| offboardedDevices | org+ch |
| invokeMethod | org |

*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.

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



Device onboarding/offboarding key

**Key**
[redacted]
xkL57_XRUhOJgt8IvGjBQ 🗐

**Created at**
January 19, 2021 11:31

**Owner**
[redacted]

**Used requests count**
2

**Updated at**
May 11, 2021 14:53

Show data for last: 1 Hour | 1 Day | 7 Days | 1 Month

Latest Request Activity: 5 | 10 | 20 | 50

Permission: "deleteDevices" Resource: "devices".
Sent at May 11, 2021 14:53.

Permission: "onboardedDevices" Resource: "devices".
Sent at May 6, 2021 16:27.

*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.

# 6 Local Device Manager

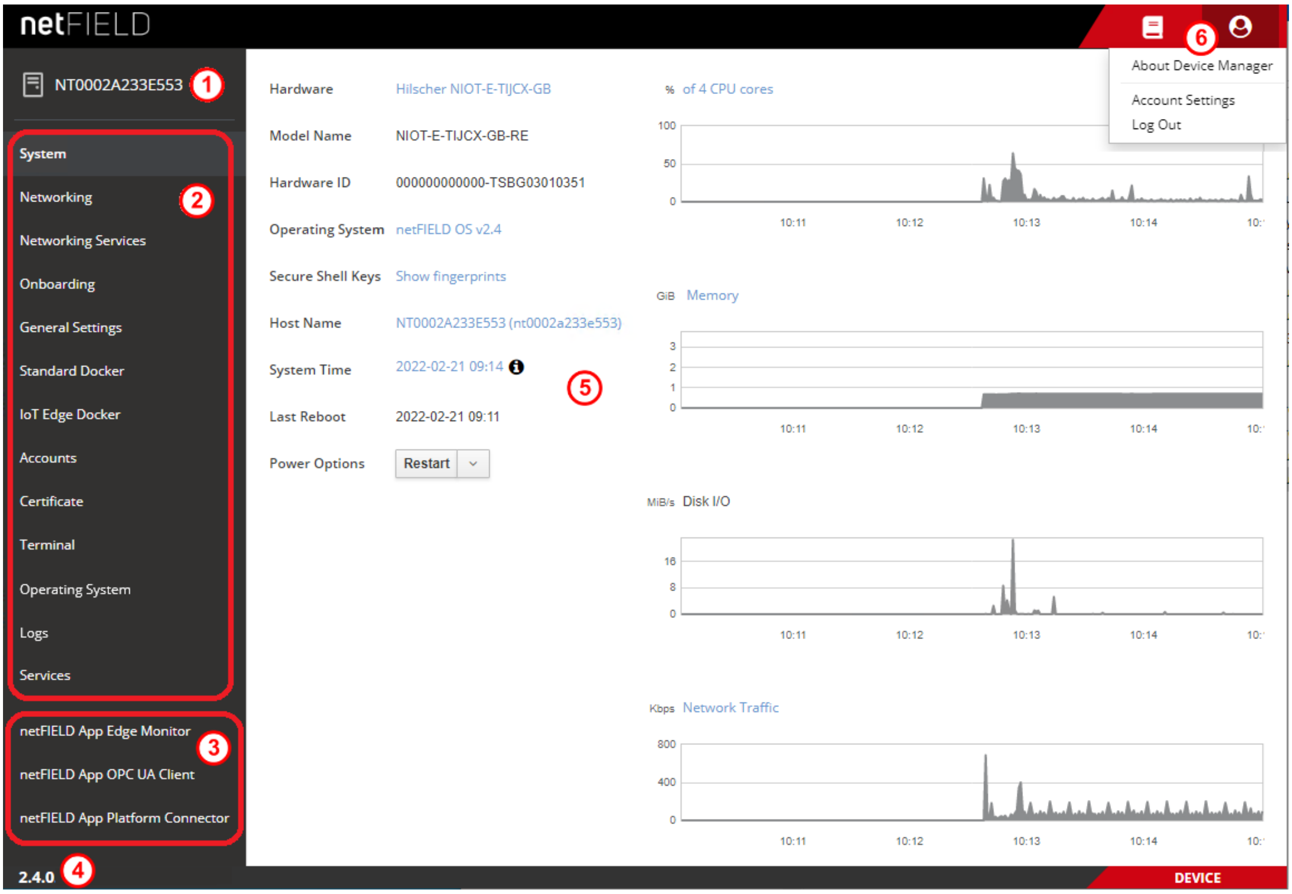
## 6.1 Overview

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

**Note:**

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

### Description of the GUI



Hardware Hilscher NIOT-E-TIJCX-GB

Model Name NIOT-E-TIJCX-GB-RE

Hardware ID 000000000000-TSBG03010351

Operating System netFIELD OS v2.4

Secure Shell Keys Show fingerprints

Host Name NT0002A233E553 (nt0002a233e553)

System Time 2022-02-21 09:14

Last Reboot 2022-02-21 09:11

Power Options Restart

*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 54])

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

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

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

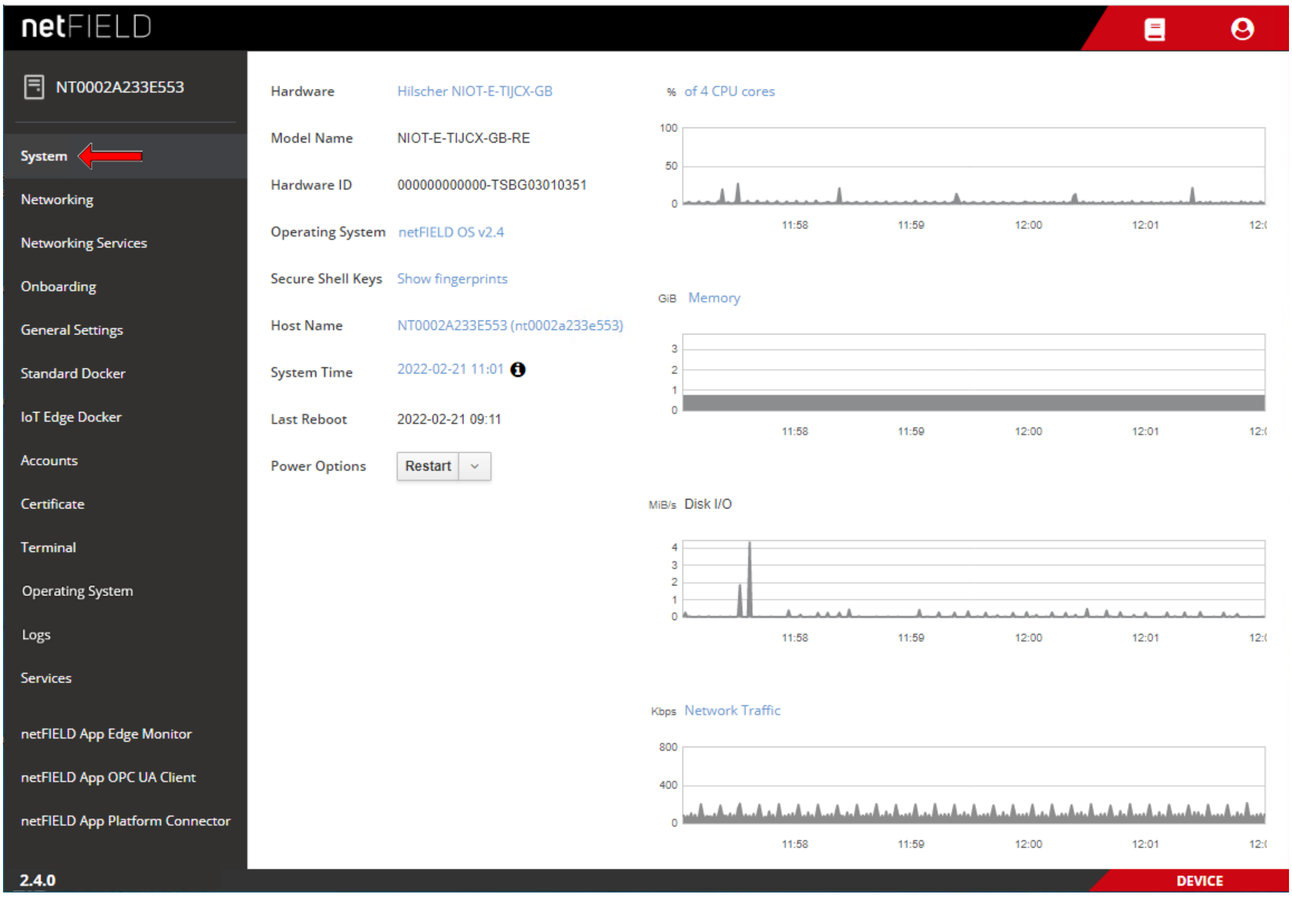
(5) Main screen displaying the management page that you have selected in the navigation panel.
Note that if a label, text or value is highlighted in blue, it contains a clickable link that opens a page or dialog box with further details or configuration options.

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

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

## 6.2 System

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



Hardware Hilscher NIOT-E-TIJCX-GB

Model Name NIOT-E-TIJCX-GB-RE

Hardware ID 000000000000-TSBG03010351

Operating System netFIELD OS v2.4

Secure Shell Keys Show fingerprints

Host Name NT0002A233E553 (nt0002a233e553)

System Time 2022-02-21 11:01

Last Reboot 2022-02-21 09:11

Power Options Restart

*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, temperature and PCI devices.

### Model Name

Model name of the device

### Hardware ID

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

### Operating System

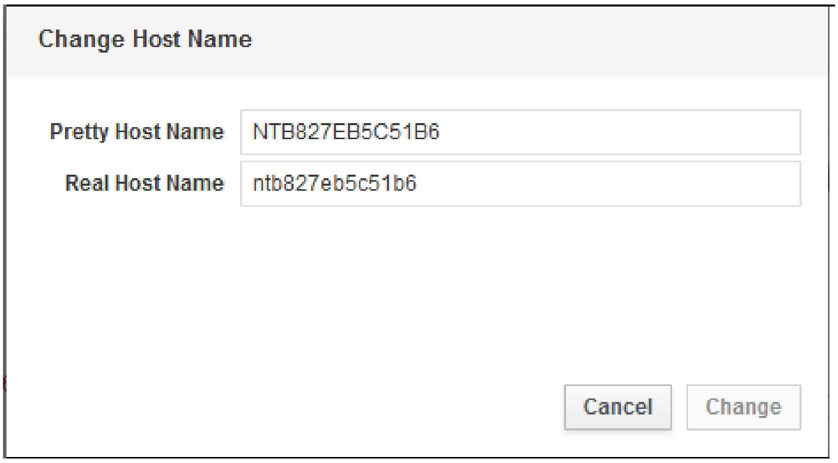
Name and version of the installed netFIELD OS. Click on the blue name to open a window showing further details (i.e. the exact firmware version).

### Secure Shell Keys

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

### Host Name

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



Change Host Name

Pretty Host Name: NTB827EB5C51B6

Real Host Name: ntb827eb5c51b6

*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 ℹ icon opens a tooltip displaying details about the current settings, like e.g. the NTP service that was used for the synchronization.
For instructions on how to change the time settings, see section *Set system time* [▸ page 39].

### Last Reboot

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

### Power Options

Use the drop-down button to restart or shutdown the netFIELD OS and the device.
To restart the device after shutdown, press the power button of the device (see position (12) in section *Positions of the interfaces* [▸ page 16]).

### CPU cores

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

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

### Memory

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

### Disk I/O

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

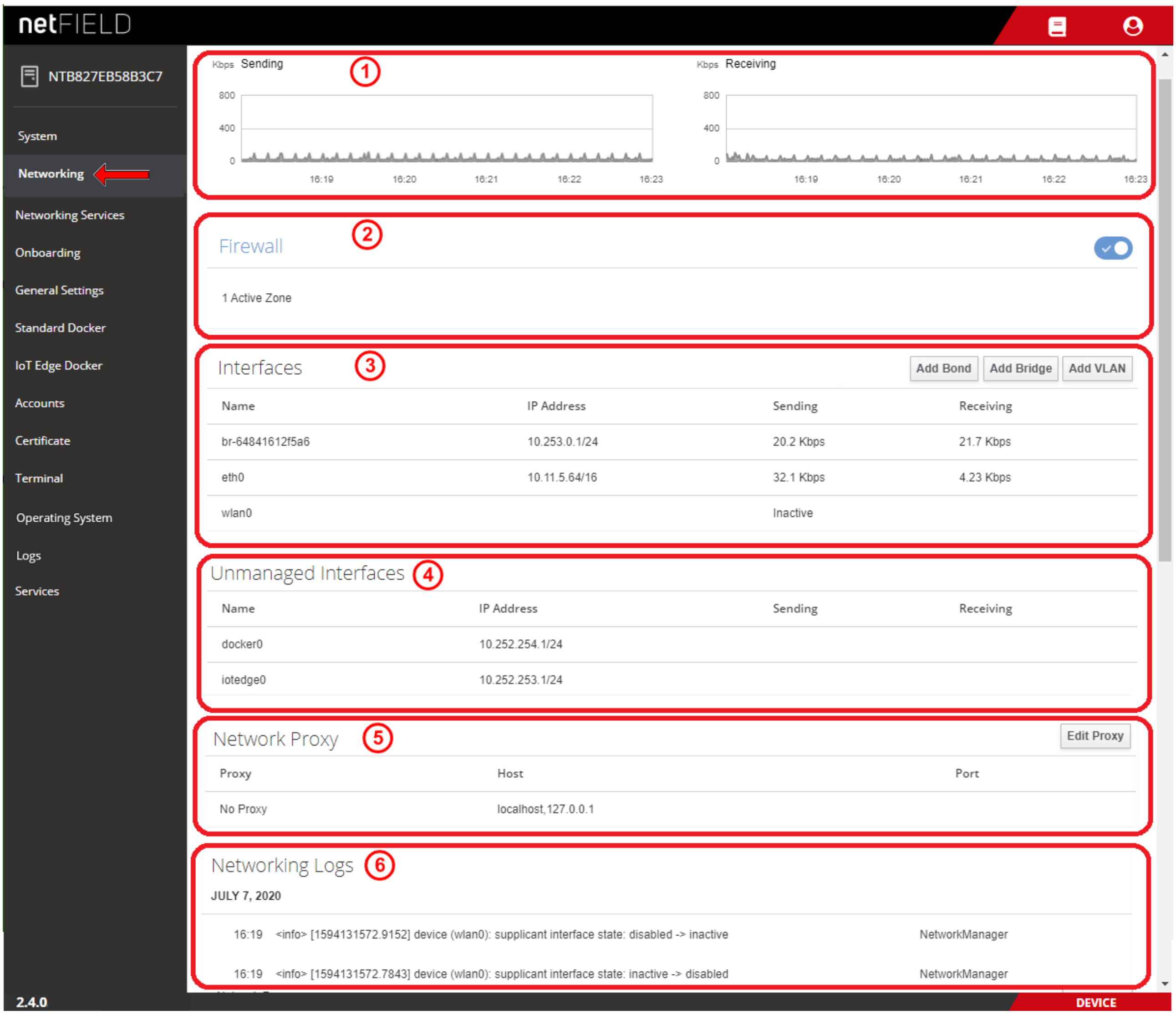
### Network Traffic

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

# 6.3 Networking

## 6.3.1 Overview

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



Firewall

1 Active Zone

Interfaces

| Name | IP Address | Sending | Receiving |
|---|---|---|---|
| br-64841612f5a6 | 10.253.0.1/24 | 20.2 Kbps | 21.7 Kbps |
| eth0 | 10.11.5.64/16 | 32.1 Kbps | 4.23 Kbps |
| wlan0 | | Inactive | |

Unmanaged Interfaces

| Name | IP Address | Sending | Receiving |
|---|---|---|---|
| docker0 | 10.252.254.1/24 | | |
| iotedge0 | 10.252.253.1/24 | | |

Network Proxy

| Proxy | Host | Port |
|---|---|---|
| No Proxy | localhost,127.0.0.1 | |

Networking Logs

JULY 7, 2020

```
16:19   <info> [1594131572.9152] device (wlan0): supplicant interface state: disabled -> inactive    NetworkManager
16:19   <info> [1594131572.7843] device (wlan0): supplicant interface state: inactive -> disabled    NetworkManager
```

*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.

### Firewall

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

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

### Interfaces

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

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

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

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

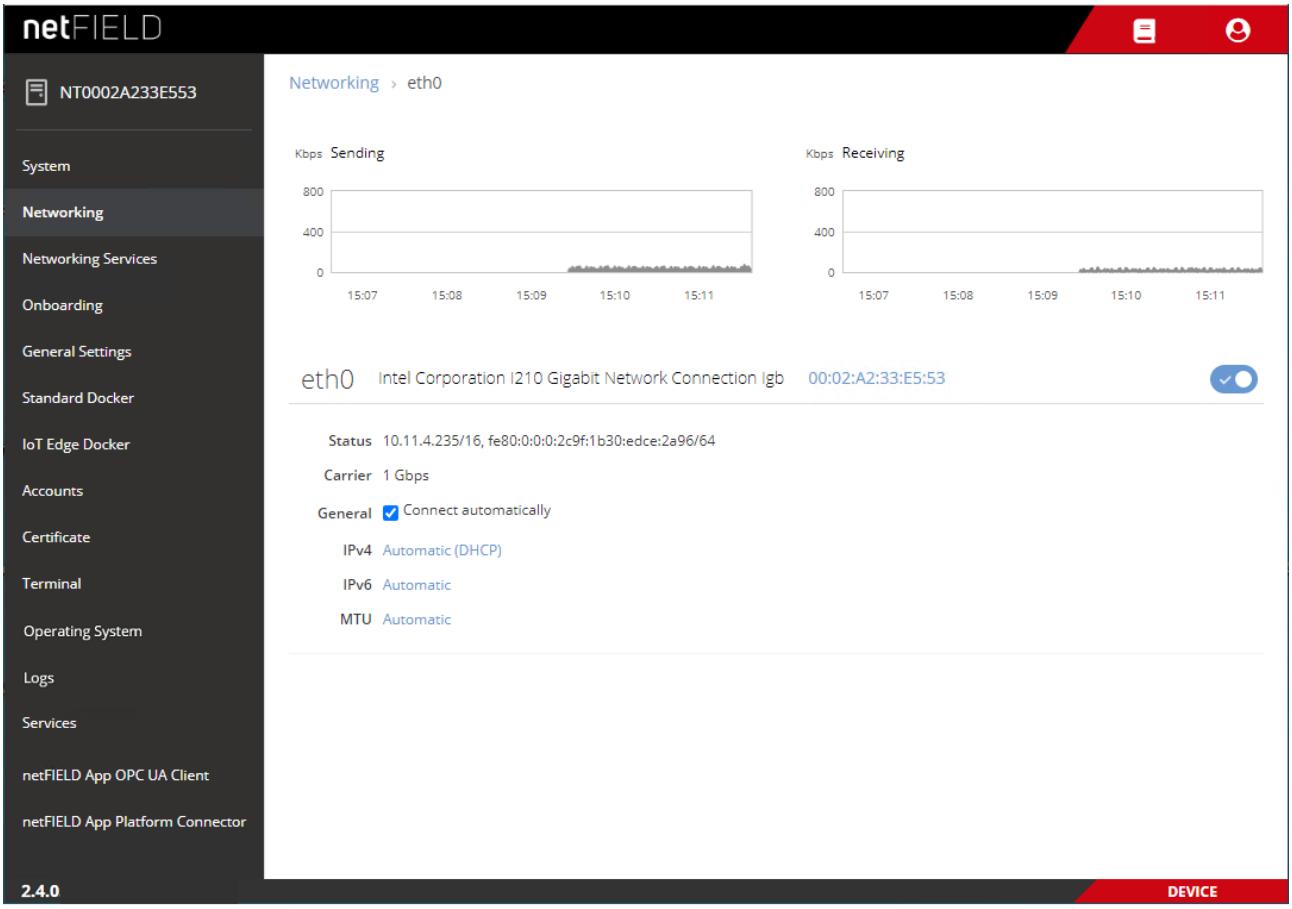
**wlan0**: This is the Wi-Fi interface of the device.
By clicking here, you can open its basic configuration page, where you can enable/disable the Wi-Fi interface and configure its IP address. Note that the Local Device Manager features a special Wi-Fi configuration page under **Networking Services** > **WiFi**, where you can make all other necessary configuration settings (see section *Wi-Fi* [▸ page 78]).

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

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

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

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



eth0 Intel Corporation I210 Gigabit Network Connection Igb 00:02:A2:33:E5:53

Status 10.11.4.235/16, fe80:0:0:0:2c9f:1b30:edce:2a96/64

Carrier 1 Gbps

General ☑ Connect automatically

IPv4 Automatic (DHCP)

IPv6 Automatic

MTU Automatic

*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 143]), or you can reactivate the interface via terminal (you have to connect a display and a keyboard to the device for accessing it via terminal).

To query the connectivity states of the interfaces via terminal, use:

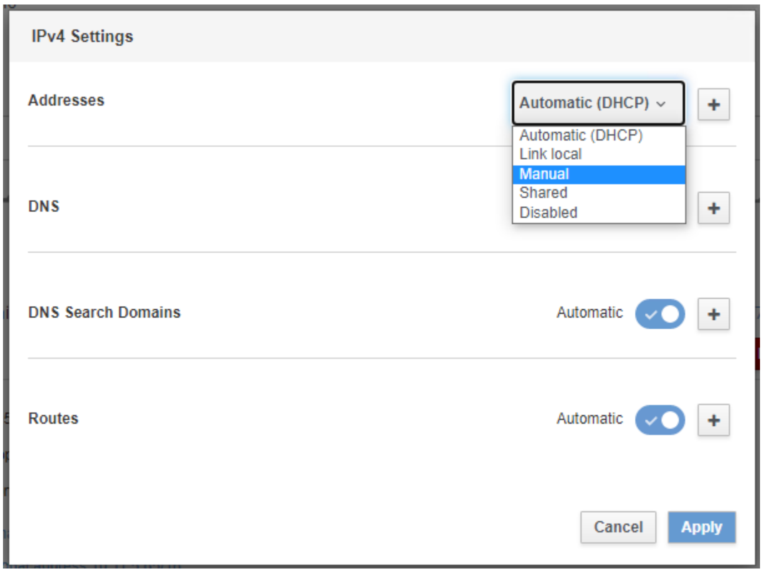
```
sudo nmcli dev status
```

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

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

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

➯ The **IPv4 Settings** page opens.



IPv4 Settings

Addresses: Automatic (DHCP)

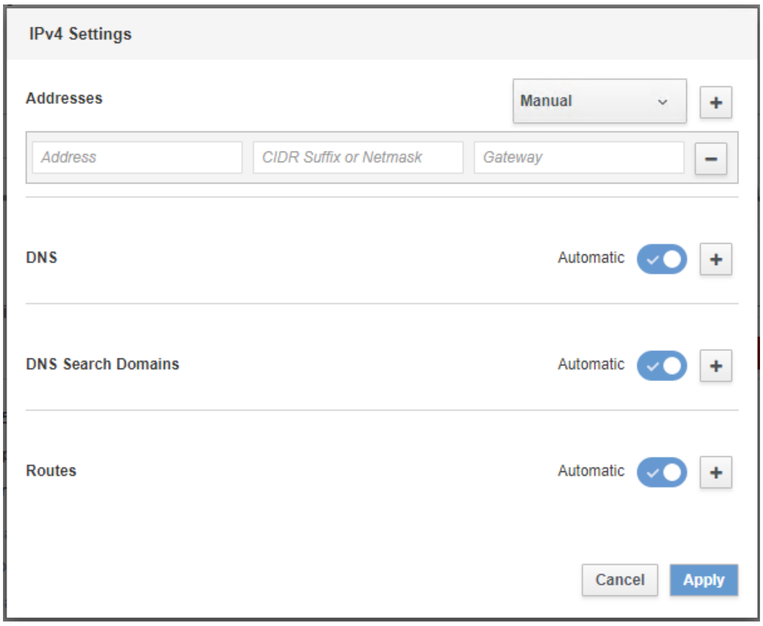
DNS

DNS Search Domains: Automatic

Routes: Automatic

*Figure 31: IPv4 Settings*

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



IPv4 Settings

Addresses: Manual

Address | CIDR Suffix or Netmask | Gateway

DNS: Automatic

DNS Search Domains: Automatic

Routes: Automatic

*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.

**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 104] for further information.

### Network Proxy

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

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

### NETWORKING LOGS

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

## 6.3.2 Firewall

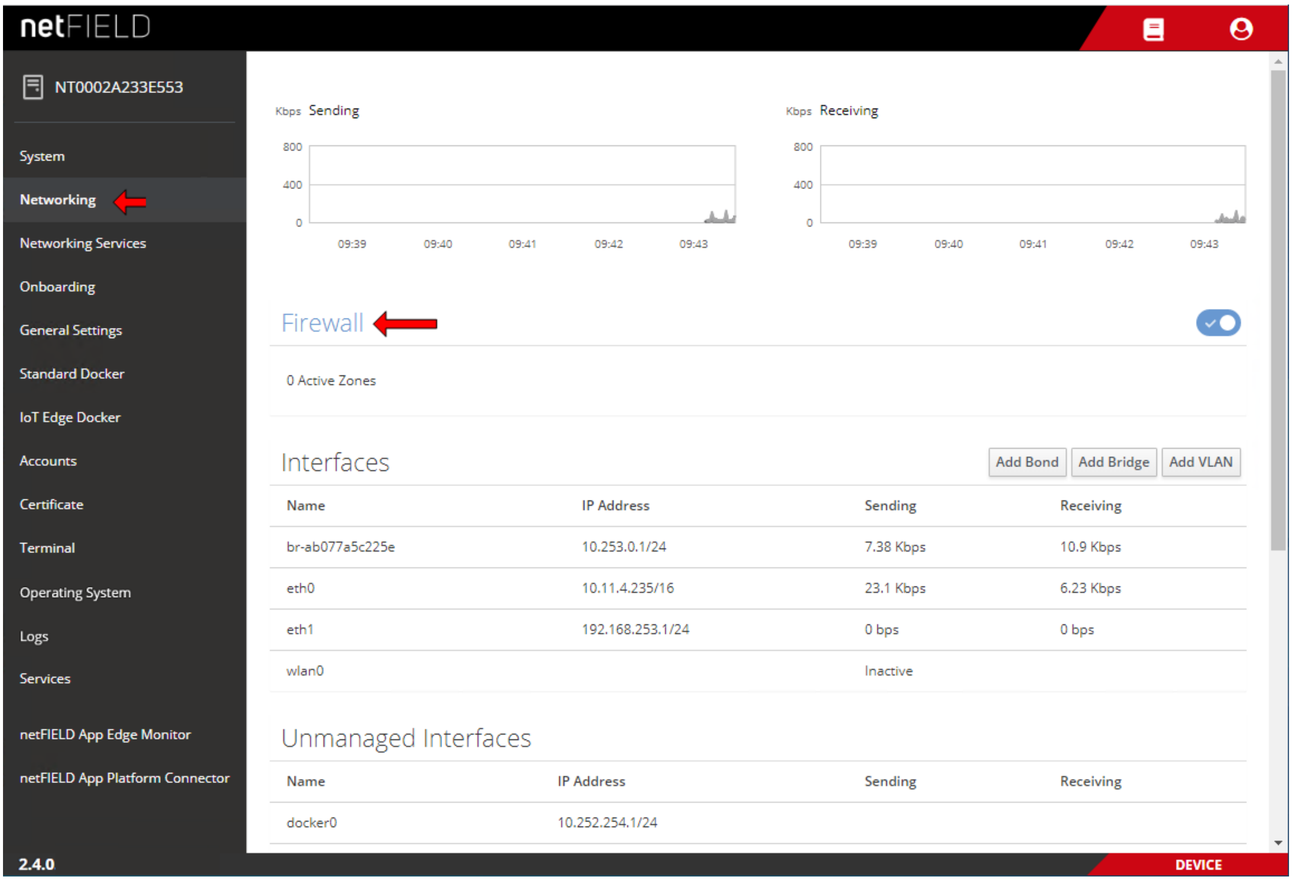
**Overview**

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

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

**Note:**
Be aware that containers running in the Standard Docker or in the IoT Edge Docker may require certain ports on the host system to be “open” in order to function and communicate properly.
Therefore, make sure that you add these ports to the **Allowed Services** list when you define Drop, NAT-Drop or Block zones.
The required ports of a container are defined in its *Container Create Options*.
For example, the *mosquitto* container (which is an MQTT Broker) requires the TCP port `1883` for its `mqtt` service to be open.
To find out the services/ports that your containers use, go to the **Standard Docker** page respectively **IoT Edge Docker** page of the Local Device Manager and check out the container’s port settings by clicking on the corresponding image or container instance.

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



Firewall

0 Active Zones

Interfaces

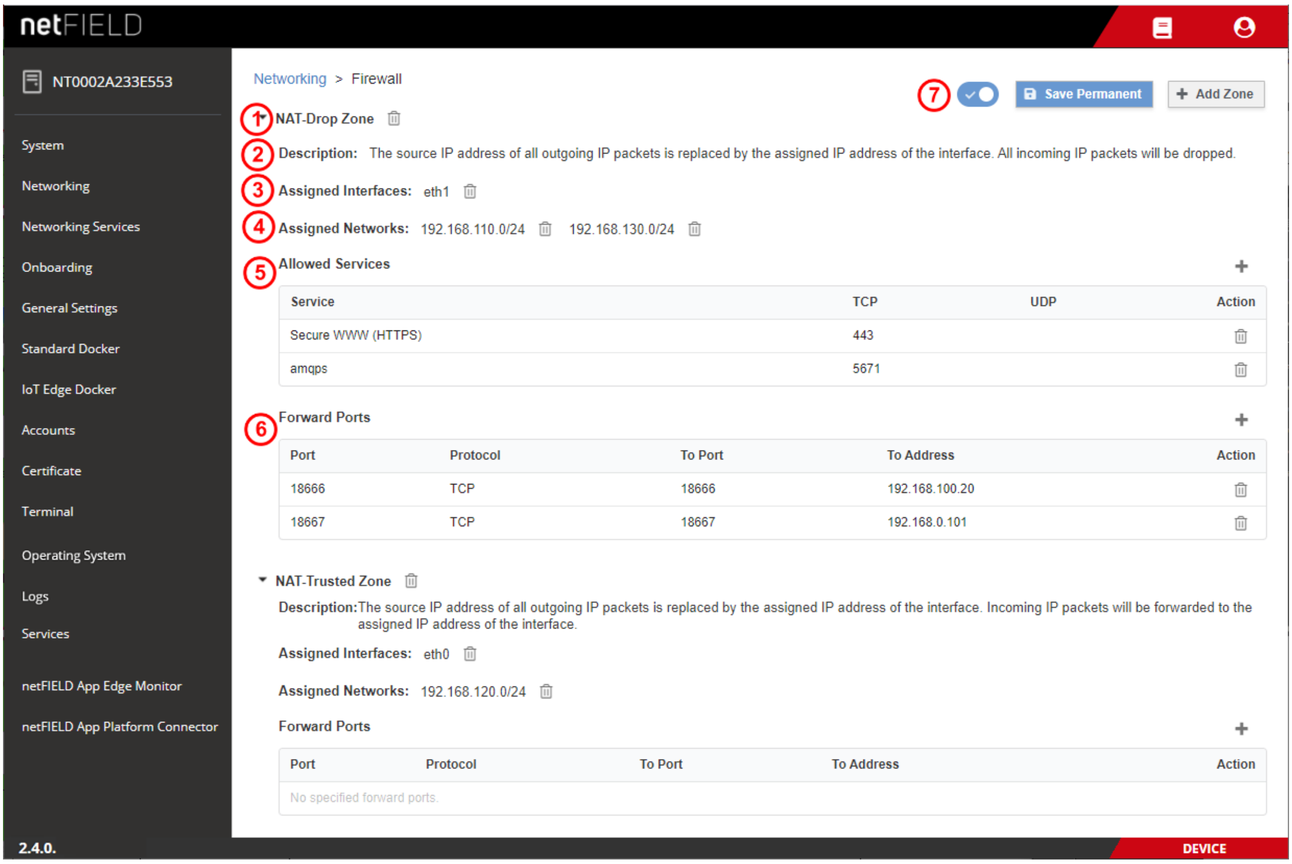
| Name | IP Address | Sending | Receiving |
|---|---|---|---|
| br-ab077a5c225e | 10.253.0.1/24 | 7.38 Kbps | 10.9 Kbps |
| eth0 | 10.11.4.235/16 | 23.1 Kbps | 6.23 Kbps |
| eth1 | 192.168.253.1/24 | 0 bps | 0 bps |
| wlan0 | | Inactive | |

Unmanaged Interfaces

| Name | IP Address | Sending | Receiving |
|---|---|---|---|
| docker0 | 10.252.254.1/24 | | |

*Figure 33: Open Firewall configuration page*

➯ The Firewall configuration page opens:



NAT-Drop Zone 🗑

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

**Assigned Interfaces:** eth1 🗑

**Assigned Networks:** 192.168.110.0/24 🗑 192.168.130.0/24 🗑

**Allowed Services** +

| Service | TCP | UDP | Action |
|---|---|---|---|
| Secure WWW (HTTPS) | 443 | | 🗑 |
| amqps | 5671 | | 🗑 |

**Forward Ports** +

| Port | Protocol | To Port | To Address | Action |
|---|---|---|---|---|
| 18666 | TCP | 18666 | 192.168.100.20 | 🗑 |
| 18667 | TCP | 18667 | 192.168.0.101 | 🗑 |

▾ NAT-Trusted Zone 🗑

**Description:** 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.

**Assigned Interfaces:** eth0 🗑

**Assigned Networks:** 192.168.120.0/24 🗑

**Forward Ports** +

| Port | Protocol | To Port | To Address | Action |
|---|---|---|---|---|
| No specified forward ports. | | | | |

*Figure 34: Elements on Firewall configuration page*

## Zones

(1) All zones that have been added to your firewall configuration are listed on the **Firewall** page.
Click the ▸ button (expand) in front of a zone's name to show the properties of the zone, like **Interfaces**, **Sources**, **Allowed Services**, **Forward ports** and a brief **Description**.
Click the ▾ button (collapse) to hide the properties of the zone.

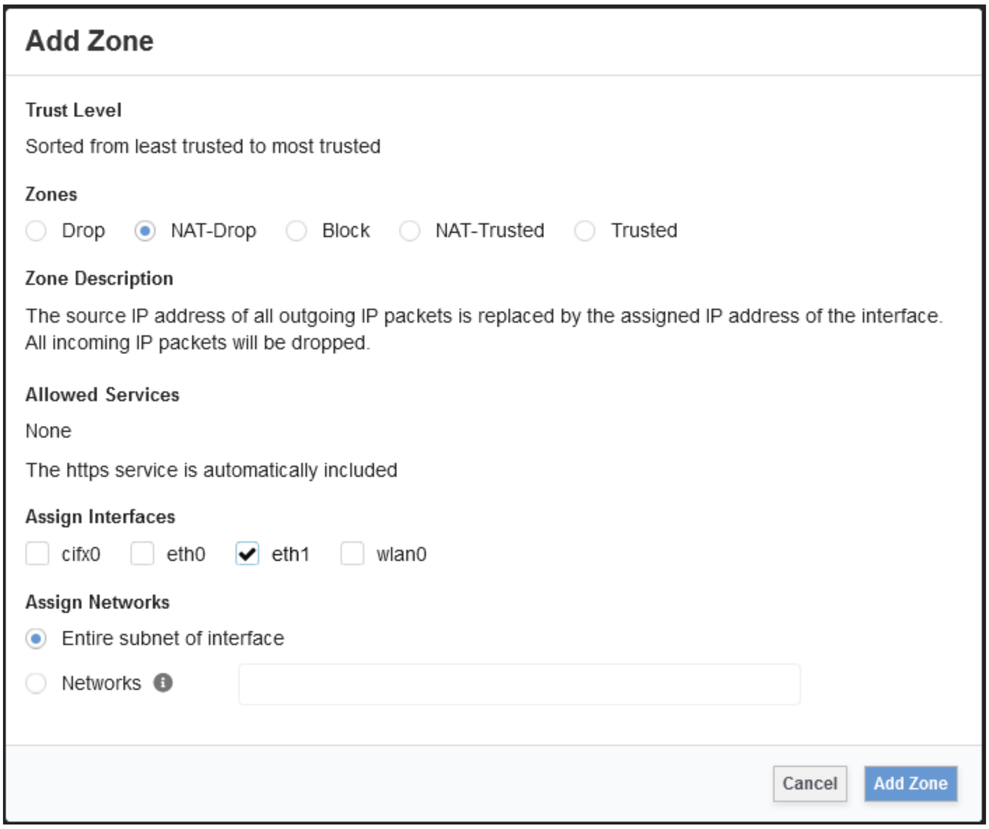
Zones can be removed from the firewall by clicking the 🗑 button.

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

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

*Table 13: Available Firewall zones*

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



Add Zone

Trust Level

Sorted from least trusted to most trusted

Zones

○ Drop ● NAT-Drop ○ Block ○ NAT-Trusted ○ Trusted

Zone Description

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

Allowed Services

None

The https service is automatically included

Assign Interfaces

□ cifx0 □ eth0 ☑ eth1 □ wlan0

Assign Networks

● Entire subnet of interface

○ Networks

*Figure 35: Add Zone dialog*

<table>
<tr><th>Element</th><th colspan="2">Description</th></tr>
<tr><td>Trust Level</td><td colspan="2">Explains the sorting of the zones under **Zones**</td></tr>
<tr><td>Zones</td><td colspan="2">Select here the zone that you want to add to your firewall configuration.<br>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.</td></tr>
<tr><td>Zone Description</td><td colspan="2">Displays a brief description of the selected zone.</td></tr>
<tr><td>Allowed Services</td><td colspan="2">Shows the allowed services/ports of the selected zone.<br>Note that HTTPS is allowed by default in all zones.<br>You can add or delete allowed services to/from an existing zone in the **Allowed Services** table of the corresponding zone.</td></tr>
<tr><td>Assign Interfaces</td><td colspan="2">Select here the physical or virtual interface(s) that you want to assign to the selected zone.<br>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.</td></tr>
<tr><td rowspan="3">Assign Networks</td><td colspan="2">Here you can define subnets or IP address ranges for which the rules of the zone shall apply.</td></tr>
<tr><td>Entire subnet of interface</td><td>Select this option if the rules shall apply to the entire subnet(s) of the assigned interface(s).</td></tr>
<tr><td>Networks</td><td>Select this option to enter address ranges or subnets for which the rules of the zone shall apply.<br>Enter the subnet mask as CIDR Suffix. Multiple entries must be separated with commas, e.g.:<br>`192.168.1.0/24,10.14.0.0/16`</td></tr>
</table>

*Table 14: Elements in Add Zone dialog*

### Description

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

### Assigned Interfaces

(3) Physical or virtual interfaces that are assigned to the zone (i.e. these are the interfaces to which the rules of the zone apply).
You can assign interfaces to a zone in the **Add Zone** dialog when you add a new zone to your firewall.
Note that each interface can be assigned to *one zone* only.
Interface(s) can be removed from a zone by clicking the 🗑 button.

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

➢ Click **+ Add Zone** button to open the **Add Zone** dialog.

➢ In the **Add Zone** dialog, select the existing zone in the **Zones** area.

➢ Select the new interface in the **Assign Interfaces** area.

➢ Click the **Add Zone** button in the footer.

⇨ The **Add Zone** dialog closes and the new interface is added to the zone.

### Assigned Networks

(4) These are the subnet(s) or IP address ranges that are assigned to the zone (i.e. these are the subnet(s) respectively IP address ranges to which the rules of the zone apply).
You can assign networks to a zone in the **Add Zone** dialog when you add a new zone to your firewall. If no networks are assigned, the rules of the zone will apply to the entire subnet of the interface by default.
Note that each network can be assigned to *one zone* only.
Networks can be removed from a zone by clicking the 🗑 button.

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

➢ Click **+ Add Zone** button to open the **Add Zone** dialog.

➢ In the **Add Zone** dialog, select the existing zone in the **Zones** area.

➢ Select the **Networks** option in the **Assign Networks** area.

➢ Enter new subnet(s) or IP address range(s) into the **Networks** field. (Enter the subnet mask as CIDR Suffix and separate multiple entries with commas.)

➢ Click the **Add Zone** button in the footer.

⇨ The **Add Zone** dialog closes and the network(s) are added to the zone.

### Allowed Services

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

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

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

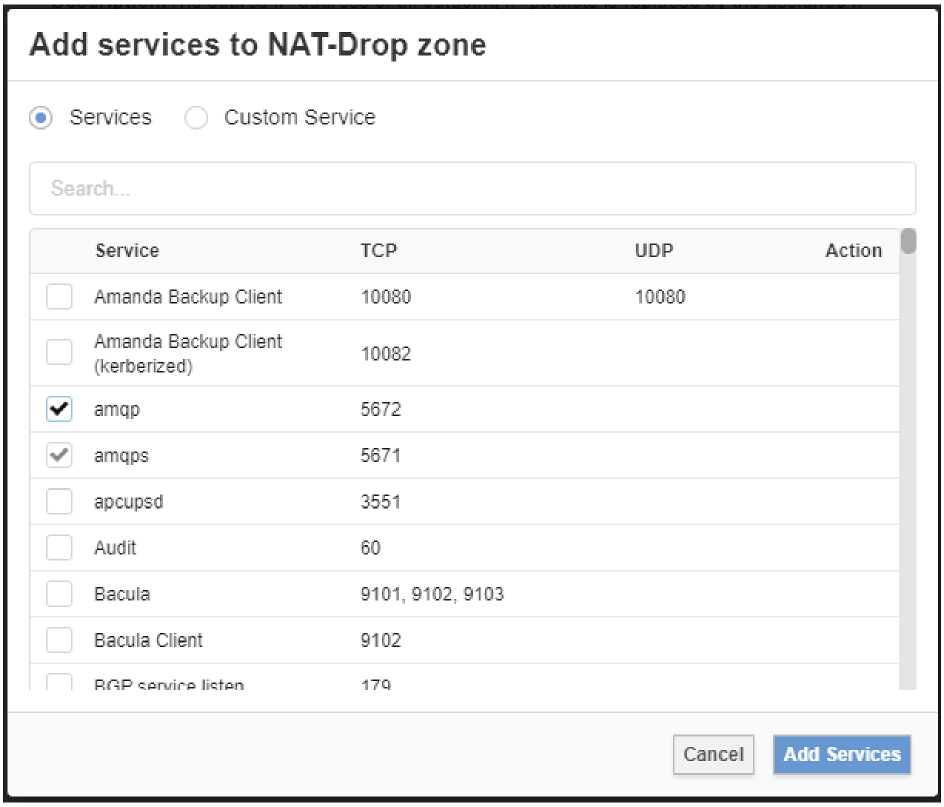
| Element | Description | |
|---|---|---|
| Service | Name of the service or alias of the custom port that is allowed in the zone. | |
| TCP | Number of the TCP port that is allowed in the zone. | |
| UDP | Number of the UDP port that is allowed in the zone. | |
| Action | + | Opens a dialog for adding allowed services respectively custom services (ports) to the zone (see below). |
| | 🗑 | Deletes the allowed service respectively port.<br>**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.

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



Add services to NAT-Drop zone

● Services ○ Custom Service

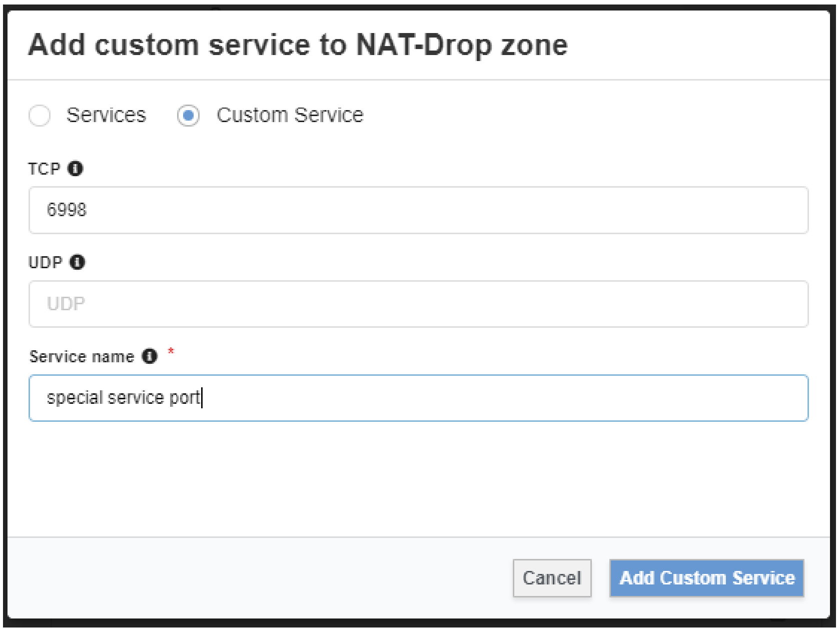
Search...

| | Service | TCP | UDP | Action |
|---|---|---|---|---|
| □ | Amanda Backup Client | 10080 | 10080 | |
| □ | Amanda Backup Client (kerberized) | 10082 | | |
| ☑ | amqp | 5672 | | |
| ☑ | amqps | 5671 | | |
| □ | apcupsd | 3551 | | |
| □ | Audit | 60 | | |
| □ | Bacula | 9101, 9102, 9103 | | |
| □ | Bacula Client | 9102 | | |
| □ | BGP service listen | 179 | | |

*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.

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


Add custom service to NAT-Drop zone

○ Services ● Custom Service

TCP: 6998

UDP: UDP

Service name *: special service port

*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”); i.e. the **NAT-Drop** or the **NAT-Trusted** zone. It allows traffic arriving at a certain port of an interface to be forwarded to a certain port of another interface, e.g. of an “internal” interface like a virtual container interface (“veth”), whose IP address is not “visible” to the “outside world”.

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

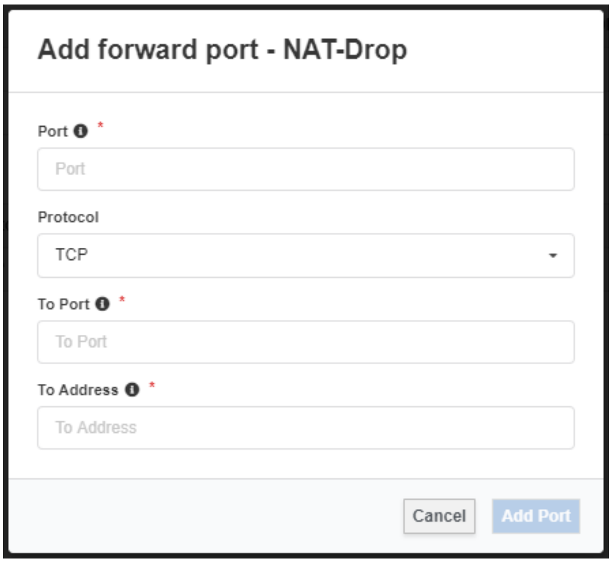
| Element | Description | |
|---|---|---|
| Port | Number of the port of the receiving interface from which the traffic is to be forwarded. | |
| Protocol | Protocol used by the service/port. | |
| To Port | Number of the port to which the traffic shall be forwarded. | |
| To Address | IP address of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

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



Add forward port - NAT-Drop

Port * : Port

Protocol: TCP

To Port * : To Port

To Address * : To Address

*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). |

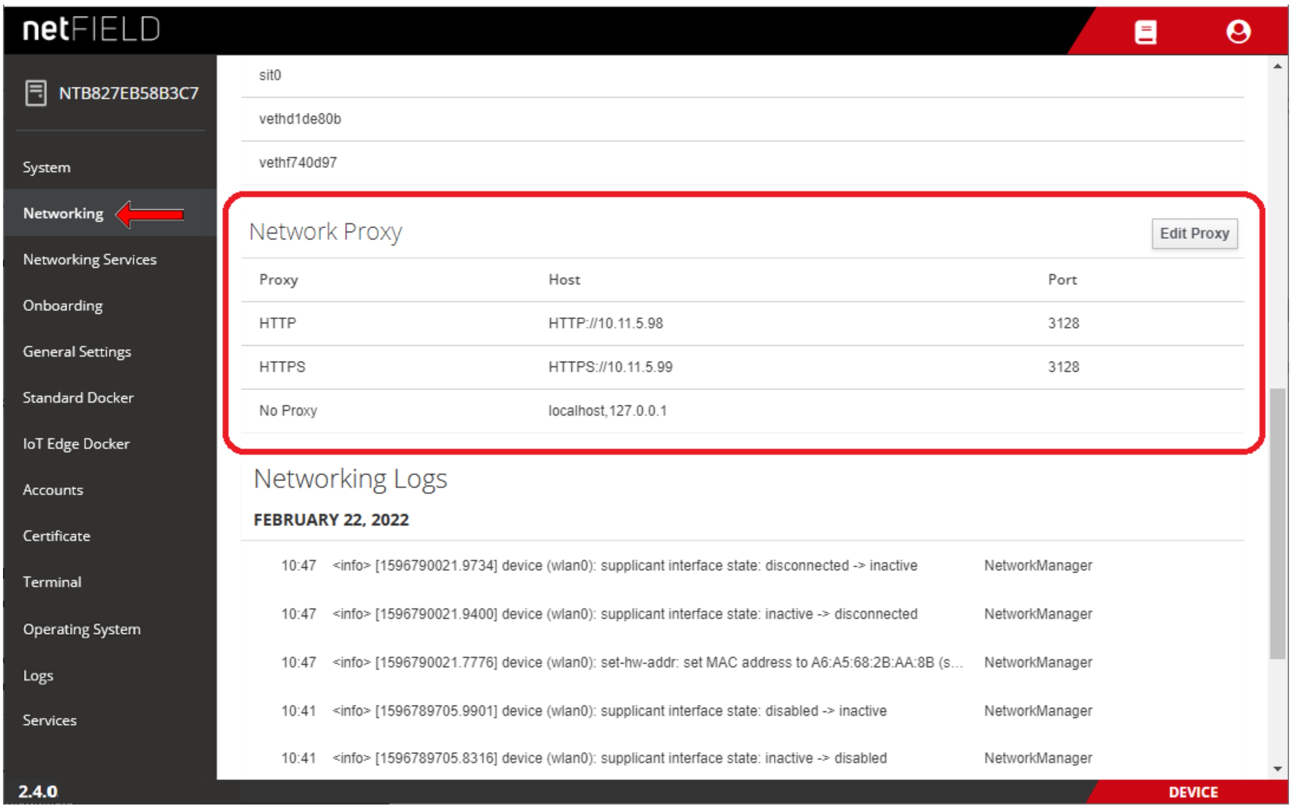
*Table 17: Control elements in main toolbar*

### 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.



Network Proxy

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

Networking Logs

FEBRUARY 22, 2022

```
10:47  <info> [1596790021.9734] device (wlan0): supplicant interface state: disconnected -> inactive   NetworkManager
10:47  <info> [1596790021.9400] device (wlan0): supplicant interface state: inactive -> disconnected   NetworkManager
10:47  <info> [1596790021.7776] device (wlan0): set-hw-addr: set MAC address to A6:A5:68:2B:AA:8B (s...  NetworkManager
10:41  <info> [1596789705.9901] device (wlan0): supplicant interface state: disabled -> inactive       NetworkManager
10:41  <info> [1596789705.8316] device (wlan0): supplicant interface state: inactive -> disabled       NetworkManager
```

*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.

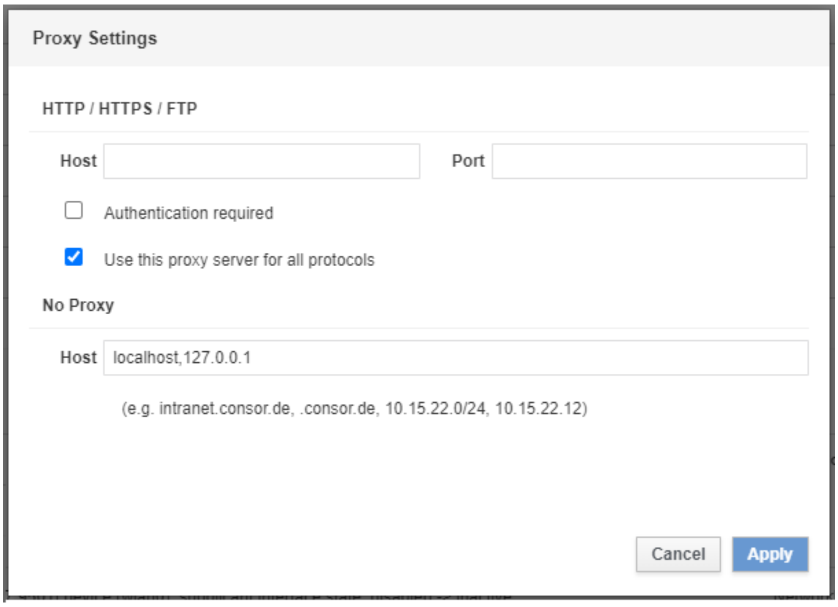
By default these are `localhost` and `127.0.0.1`, which are "internal" addresses of the netFIELD OS and are therefore not to be handled by a proxy server. The `localhost` and `127.0.0.1` entries appear in the **No Proxy** list even if you did not configure any Proxy Server for your netFIELD OS.
Do not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



Proxy Settings

HTTP / HTTPS / FTP

Host: (empty) Port: (empty)

□ Authentication required

☑ Use this proxy server for all protocols

No Proxy

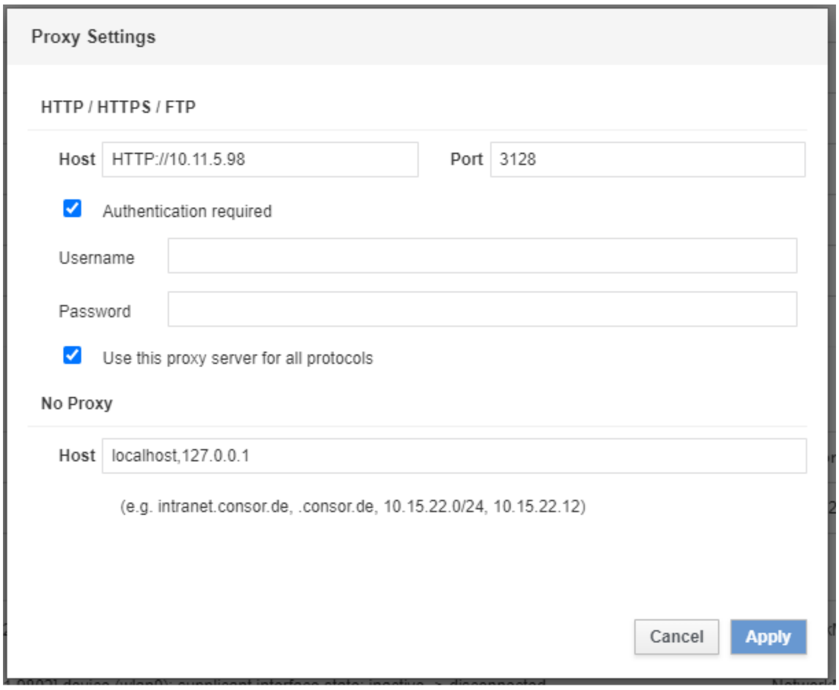
Host: localhost,127.0.0.1

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

*Figure 40: Proxy Settings dialog window*

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

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



Proxy Settings

HTTP / HTTPS / FTP

Host HTTP://10.11.5.98 Port 3128

☑ Authentication required

Username

Password

☑ Use this proxy server for all protocols

No Proxy

Host localhost,127.0.0.1

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

*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.

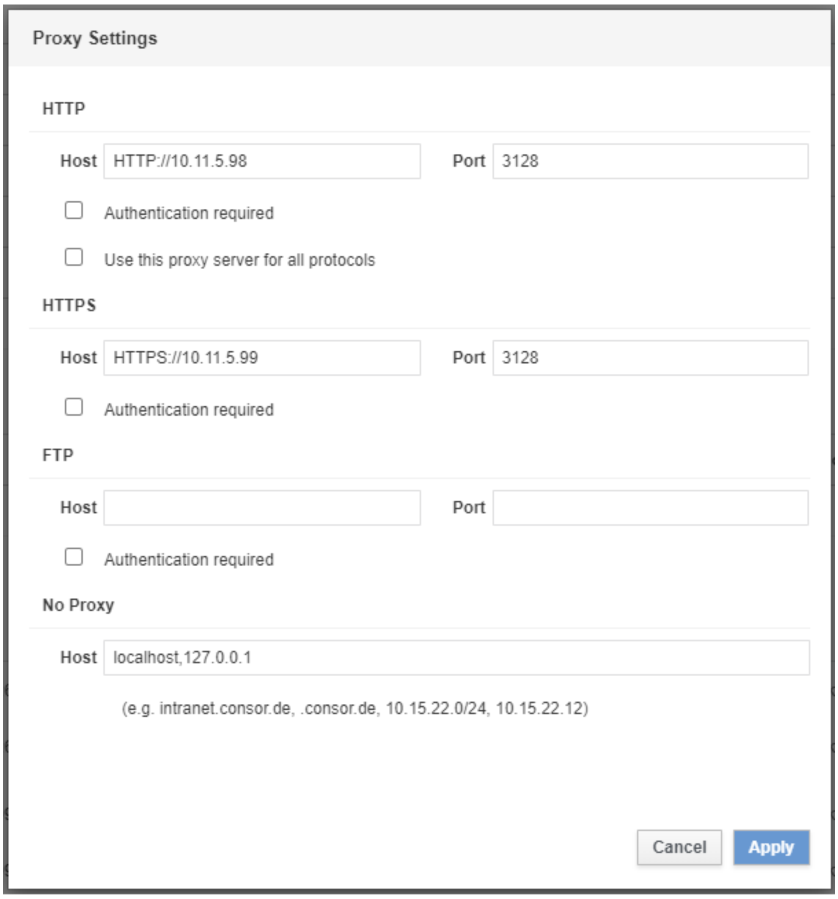
**Important:**

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.

**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:



Proxy Settings

HTTP

Host HTTP://10.11.5.98 Port 3128

□ Authentication required

□ Use this proxy server for all protocols

HTTPS

Host HTTPS://10.11.5.99 Port 3128

□ Authentication required

FTP

Host Port

□ Authentication required

No Proxy

Host localhost,127.0.0.1

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

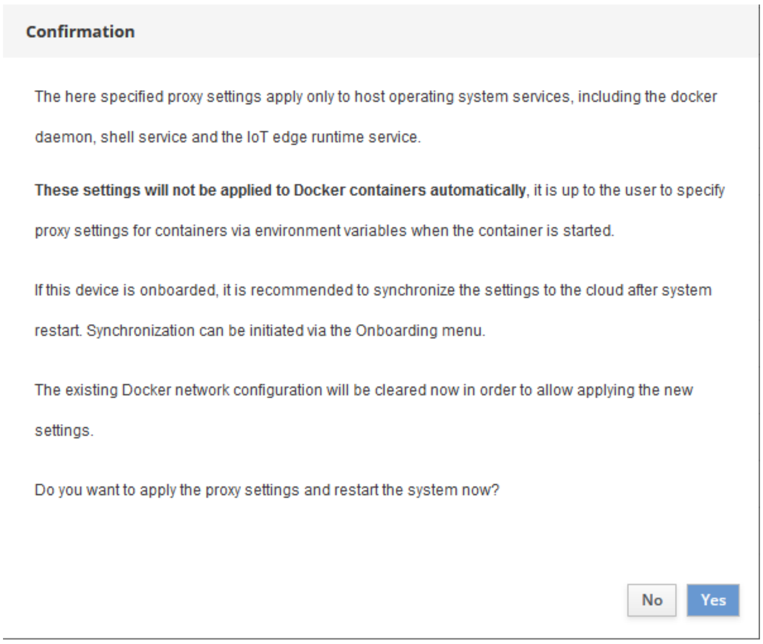
*Figure 42: Separate HTTP/HTTPS/FTP configuration*

➢ Enter the parameters of the individual proxy servers.

### Saving and restarting

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

➮ The following dialog appears:



**Confirmation**

The here specified proxy settings apply only to host operating system services, including the docker daemon, shell service and the IoT edge runtime service.

**These settings will not be applied to Docker containers automatically**, it is up to the user to specify proxy settings for containers via environment variables when the container is started.

If this device is onboarded, it is recommended to synchronize the settings to the cloud after system restart. Synchronization can be initiated via the Onboarding menu.

The existing Docker network configuration will be cleared now in order to allow applying the new settings.

Do you want to apply the proxy settings and restart the system now?

*Figure 43: Restart dialog after changing proxy server configuration*

➢ Read the note carefully.

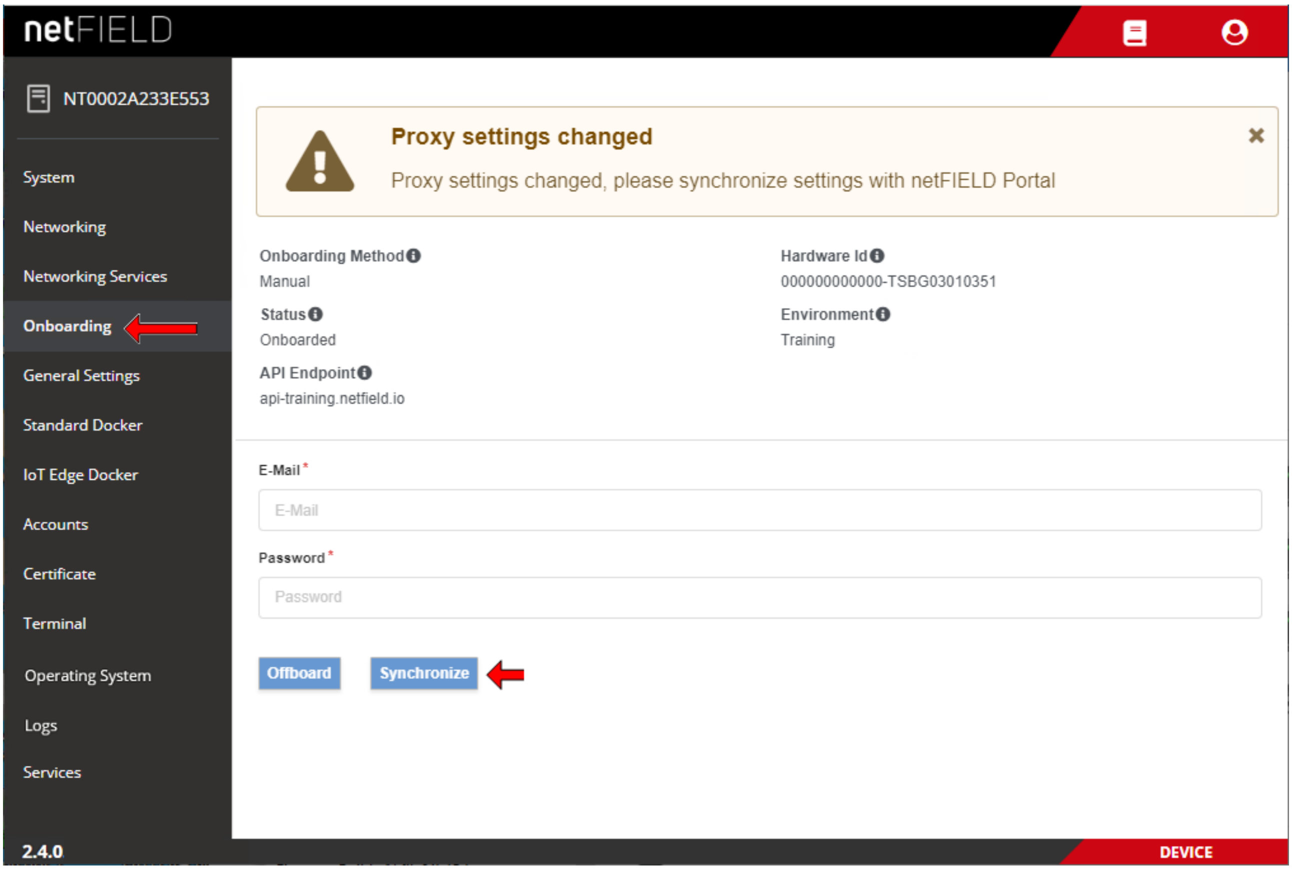
➢ To apply the new settings, you must allow the netFIELD OS to perform an immediate restart.
Click **Yes** to apply the new settings and restart the netFIELD OS.

➢ Click **No** to close the dialog without applying the new settings.

### Synchronizing new settings with the cloud

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

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



**Proxy settings changed**

Proxy settings changed, please synchronize settings with netFIELD Portal

Onboarding Method: Manual

Hardware Id: 000000000000-TSBG03010351

Status: Onboarded

Environment: Training

API Endpoint: api-training.netfield.io

E-Mail *

Password *

*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.

### Removing or editing existing Proxy server settings

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

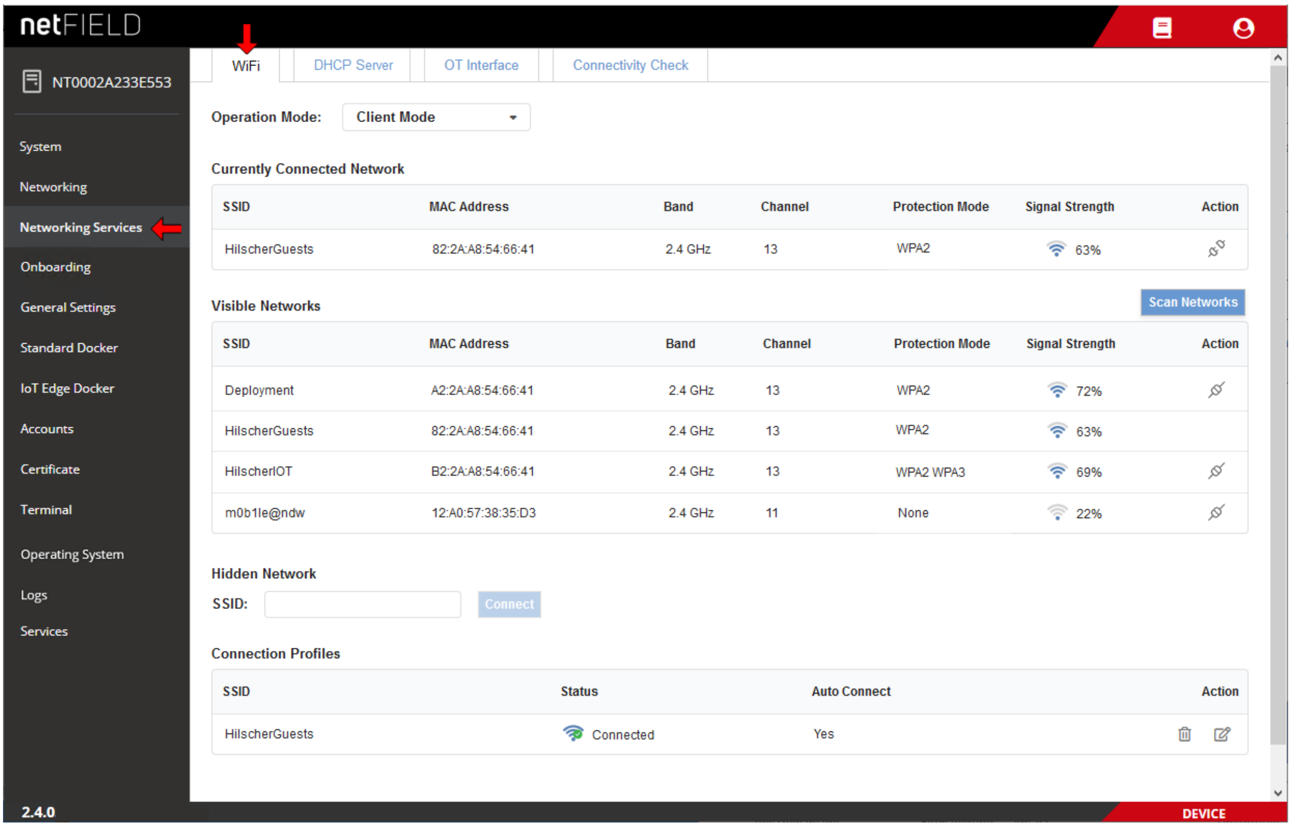
# 6.4 Networking Services

## 6.4.1 Wi-Fi

### 6.4.1.1 Overview

On the **WiFi** tab of the **Networking Services** page, you can configure the Wi-Fi functions of your device.
The netFIELD OS supports single band 2.4 GHz wireless network communication (Wi-Fi / WLAN) according to IEEE 802.11 and can either connect to an existing wireless network in “Client” mode or establish a new wireless network as “Access Point”.

Other clients connected to the same Wi-Fi network can thus access the **Local Device Manager** and/or other IP based services provided by the netFIELD OS on your device.
In Access Point mode, you can even route IP data from a connected Wi-Fi client to other connected subnets of your device (e.g. to an Ethernet subnet connected at its eth0 interface) by assigning both the Wi-Fi interface and the corresponding “target” interface (e.g. eth0) to the **NAT-Trusted** or the **NAT-Drop** zone of your firewall. The required NAT-Trusted respectively NAT-Drop zone can be created on the **Networking** > **Firewall** page (see section *Firewall* [▸ page 62]).
Routing from one Wi-Fi client to another connected Wi-Fi client is also possible.



Operation Mode: Client Mode

Currently Connected Network

| SSID | MAC Address | Band | Channel | Protection Mode | Signal Strength | Action |
|---|---|---|---|---|---|---|
| HilscherGuests | 82:2A:A8:54:66:41 | 2.4 GHz | 13 | WPA2 | 63% | 🔗 |

Visible Networks

Scan Networks

| SSID | MAC Address | Band | Channel | Protection Mode | Signal Strength | Action |
|---|---|---|---|---|---|---|
| Deployment | A2:2A:A8:54:66:41 | 2.4 GHz | 13 | WPA2 | 72% | 🔗 |
| HilscherGuests | 82:2A:A8:54:66:41 | 2.4 GHz | 13 | WPA2 | 63% | |
| HilscherIOT | B2:2A:A8:54:66:41 | 2.4 GHz | 13 | WPA2 WPA3 | 69% | 🔗 |
| m0b1le@ndw | 12:A0:57:38:35:D3 | 2.4 GHz | 11 | None | 22% | 🔗 |

Hidden Network

SSID: Connect

Connection Profiles

| SSID | Status | Auto Connect | Action |
|---|---|---|---|
| HilscherGuests | Connected | Yes | 🗑 ✎ |

*Figure 45: Wi-Fi Client Mode*

**Note:**
If the “WiFi hardware is not available or disabled” note is displayed, you have to enable the **wlan0** interface on the **Networking** page before you can select and configure your Wi-Fi mode here.
To do so, open the **Networking** page, click **wlan0 – Not available** entry (below **Interfaces**), then click the toggle switch (on the right side of the screen). After enabling, the toggle switch looks like this:

### Operation Mode

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

| Operation mode | Description | wlan0 interface default IP settings |
|---|---|---|
| Client Mode | This mode allows the netFIELD Edge device to connect to an already existing Wi-Fi network (2.4 GHz band) provided by a nearby access point.<br>Personal and Enterprise WPA is supported.<br>See section *Client mode* [▸ page 80] 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.<br>On the **Networking** > **Interfaces** > **wlan0** page, the **Status** parameter shows the IPv4 and IPv6 addresses assigned to the interface by the DHCP server.<br>**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).<br>See section *Access Point mode* [▸ page 86] for details. | After saving the Access Point configuration, the **IPv4** address configuration of the **wlan0** interface is by default set to *Link local*.<br>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).<br>**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*

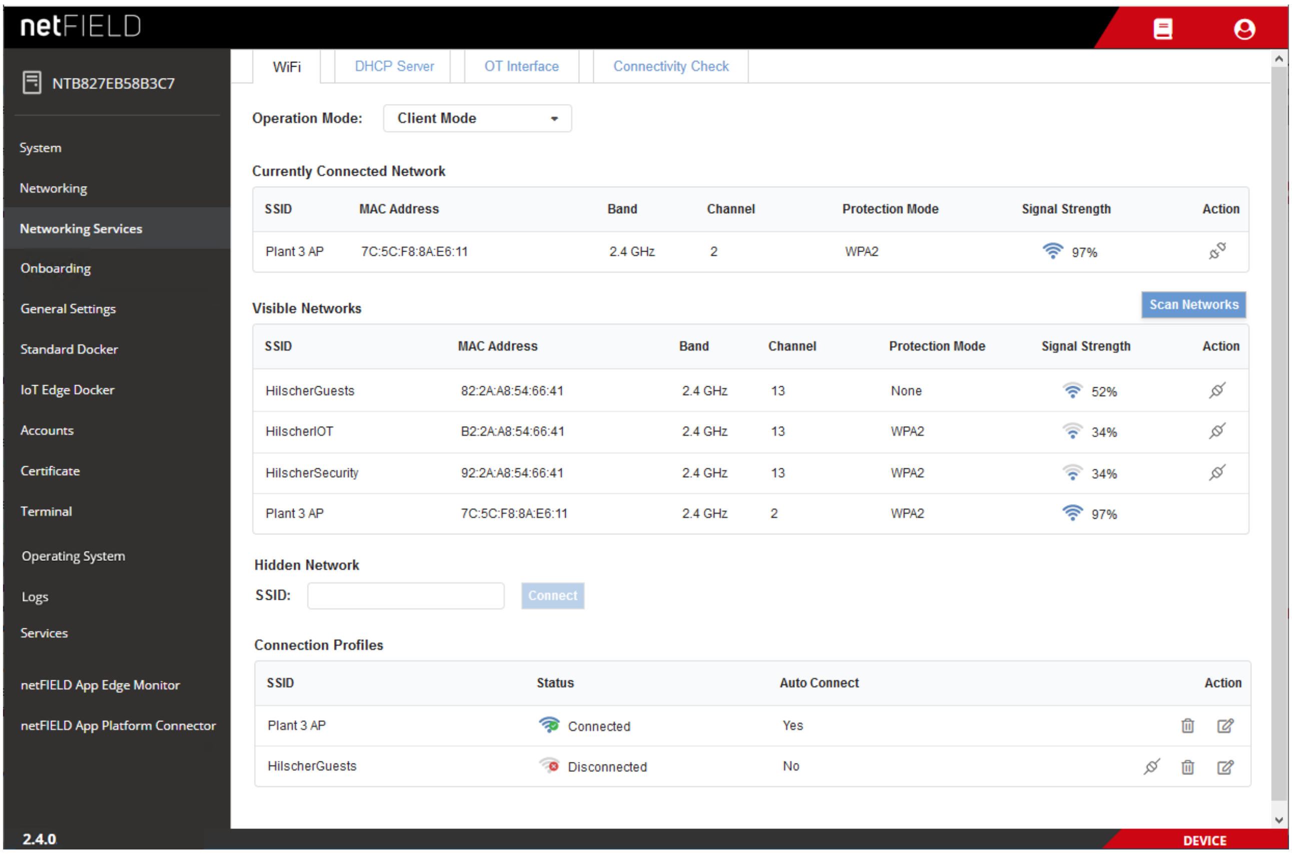
After having selected an **Operation Mode**, the configuration parameters of the selected mode are displayed.

### 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.



Operation Mode: Client Mode

Currently Connected Network

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

Visible Networks

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

Hidden Network

SSID:

Connection Profiles

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

*Figure 46: Client mode parameters*

### Currently Connected Network

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

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>SSID</td><td colspan="2">SSID (service set identifier) of the Wi-Fi network to which the device is connected.</td></tr>
<tr><td>MAC Address</td><td colspan="2">MAC address of the Access Point of the Wi-Fi network to which the device is connected.</td></tr>
<tr><td>Band</td><td colspan="2">Radio waveband that the Wi-Fi network uses.</td></tr>
<tr><td>Channel</td><td colspan="2">Channel that the Wi-Fi network uses.</td></tr>
<tr><td>Protection Mode</td><td colspan="2">Shows the Wi-Fi Protected Access mode (WPA) that the network uses.</td></tr>
<tr><td>Signal Strength</td><td colspan="2">Shows the signal strength of the Wi-Fi connection in percent.</td></tr>
<tr><td>Action</td><td>🔌</td><td>Disconnect from this Wi-Fi network.</td></tr>
</table>

*Table 19: Currently Connected Network*

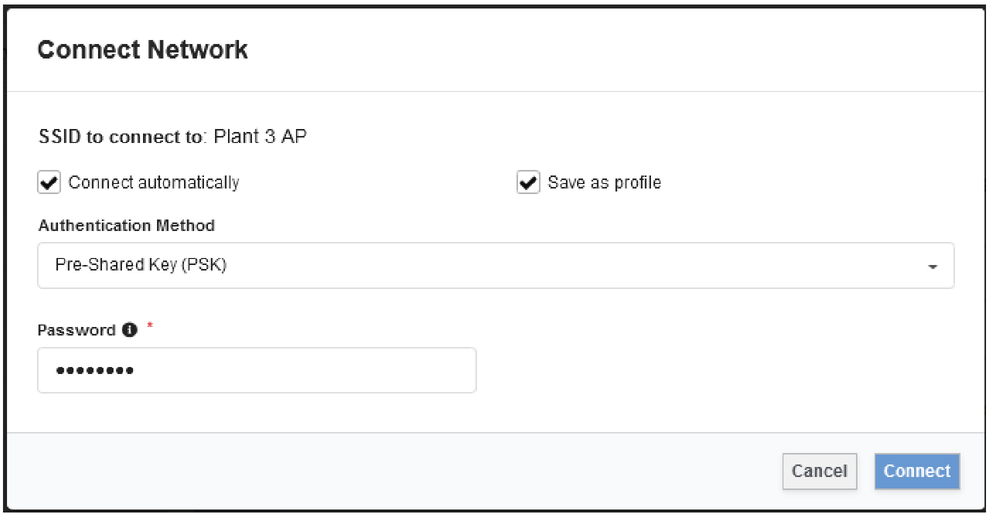
### Visible Networks

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.

<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>SSID</td><td colspan="2">SSID of the visible Wi-Fi network.</td></tr>
<tr><td>MAC Address</td><td colspan="2">MAC address of the Access Point of the visible Wi-Fi network</td></tr>
<tr><td>Band</td><td colspan="2">Radio waveband that the visible Wi-Fi connection uses.</td></tr>
<tr><td>Channel</td><td colspan="2">Channel that the visible Wi-Fi network uses.</td></tr>
<tr><td>Protection Mode</td><td colspan="2">Shows the Wi-Fi Protected Access mode (WPA) that the visible network uses.</td></tr>
<tr><td>Signal Strength</td><td colspan="2">Shows the signal strength of the visible Wi-Fi connection in percent.</td></tr>
<tr><td>Action</td><td>🔌</td><td>Connect to this Wi-Fi network. Opens the <b>Connect Network</b> dialog.<br><b>Note</b>: Establishing a new connection automatically terminates any other currently active Wi-Fi network connection.</td></tr>
</table>

*Table 20: Visible Networks*

### Connect Network dialog



Connect Network

SSID to connect to: Plant 3 AP

☑ Connect automatically ☑ Save as profile

Authentication Method

Pre-Shared Key (PSK)

Password *

••••••••

*Figure 47: Connect Network dialog*

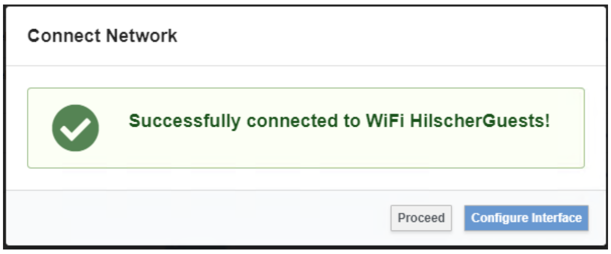
| Parameter | Description | | |
|---|---|---|---|
| Connect automatically | If you select this option, the device tries to automatically connect to this network each time after enabling the **Client mode**. | | |
| Save as profile | If you select this option, the connection parameters are saved as a 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.<br>**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.<br>**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).<br>**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)*

| 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).<br>**Note**: The certificate must be stored in the `/etc/wifi-certs/` directory of the netFIELD OS. |
| | | Client Private Key File | Client Private Key File.<br>**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).<br>**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:<br>MS-CHAP<br>MS-CHAP v2<br>CHAP |
| | | CA Certificate File | Click the 🗋 icon to select the root certificate of the Certification Authority that shall be used for authentication (optional).<br>**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.<br>**Note**: Establishing a new connection automatically terminates other current Wi-Fi network connections. | | |

*Table 22: Parameters in Connect Network dialog (2)*

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



Connect Network

Successfully connected to WiFi HilscherGuests!

*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.

### 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).

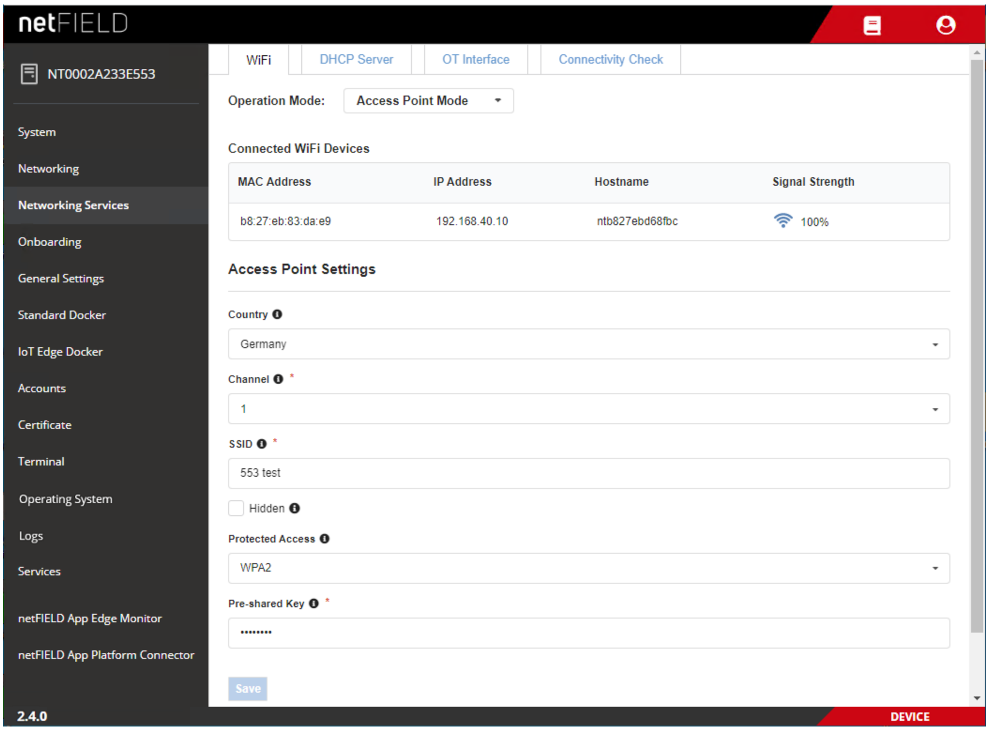
<table>
<tr><th>Parameter</th><th colspan="2">Description</th></tr>
<tr><td>SSID</td><td colspan="2">SSID of the Wi-Fi network.</td></tr>
<tr><td>Status</td><td colspan="2">Shows whether you are currently connected to the network.</td></tr>
<tr><td>Auto Connect</td><td colspan="2">Shows whether you have enabled the “Auto Connect” option for the network. In “Auto Connect” mode (“Connect automatically”) the device tries to automatically connect to this network after the <b>Client mode</b> has been enabled.<br><b>Note</b>: It is best practice to assign “Auto Connect” only to one SSID. If “Auto Connect” is assigned to more than one SSID, the device will pick the SSID with the highest signal strength.</td></tr>
<tr><td rowspan="3">Action</td><td>🔌</td><td>Connect to this Wi-Fi network using the profile settings.<br><b>Note</b>: Establishing a new connection automatically terminates other current Wi-Fi network connections.</td></tr>
<tr><td>🗑</td><td>Delete this profile.</td></tr>
<tr><td>✎</td><td>Edit this profile.</td></tr>
</table>

*Table 23: Connection Profiles*

### 6.4.1.3 Access Point mode

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

The Access Point configuration parameters are displayed:



Operation Mode: Access Point Mode

Connected WiFi Devices

| MAC Address | IP Address | Hostname | Signal Strength |
|---|---|---|---|
| b8:27:eb:83:da:e9 | 192.168.40.10 | ntb827ebd68fbc | 100% |

Access Point Settings

Country: Germany

Channel *: 1

SSID *: 553 test

□ Hidden

Protected Access: WPA2

Pre-shared Key *: ••••••••

*Figure 49: Access Point Mode*

## Connected WiFi Devices

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

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

*Table 24: Connected WiFi Devices*

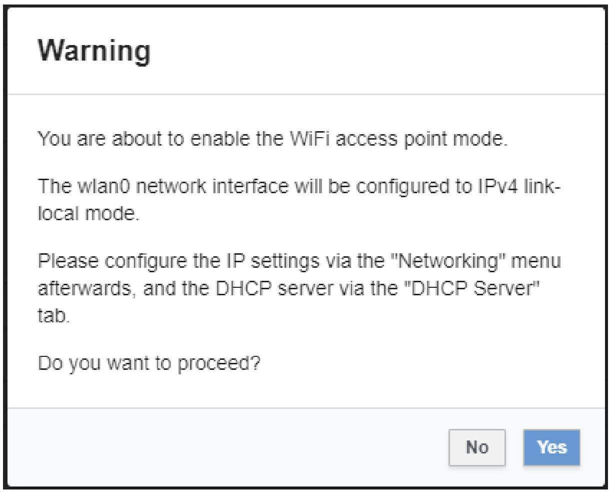
### Access Point Settings

| Parameter | Description |
|---|---|
| Country | In the drop-down list, select the country in which your device is operated.<br>**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:<br>- WPA<br>- WPA2<br>- 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).<br>The key may be entered either as a string of 64 hexadecimal digits or as a passphrase/password of 8 to 63 printable ASCII characters. |
| Save | Click this button to save your configuration. |

*Table 25: Access Point Settings*

### Reconfigure IP address of wlan0 interface

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



Warning

You are about to enable the WiFi access point mode.

The wlan0 network interface will be configured to IPv4 link-local mode.

Please configure the IP settings via the "Networking" menu afterwards, and the DHCP server via the "DHCP Server" tab.

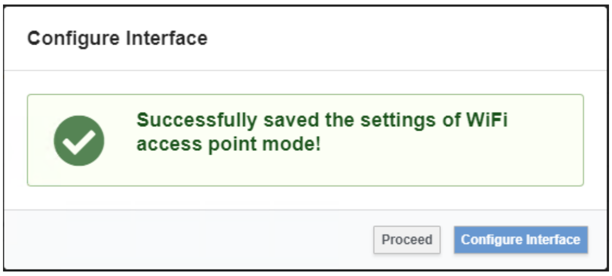
Do you want to proceed?

*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:



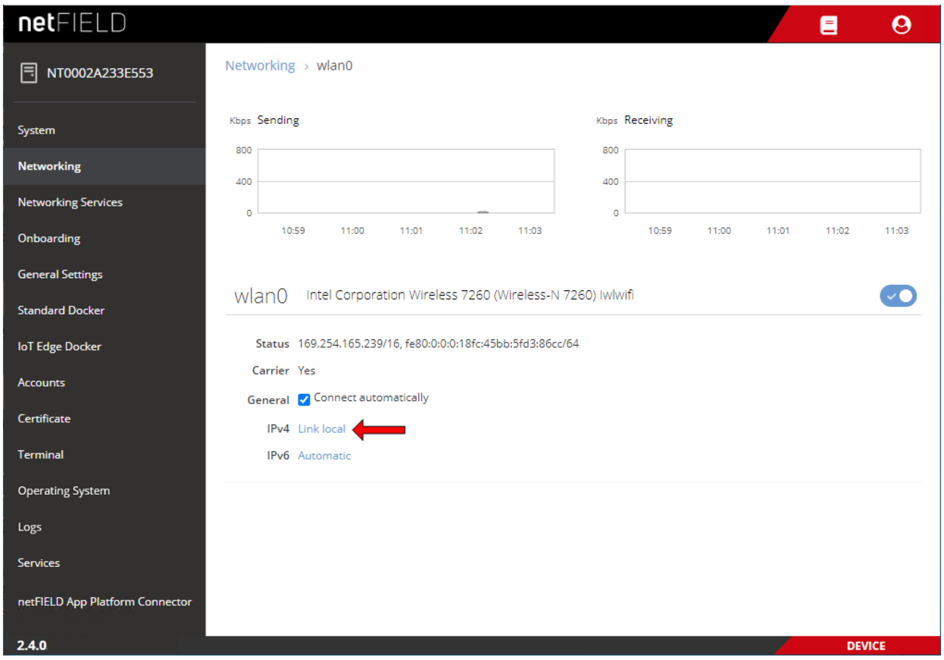
Configure Interface

Successfully saved the settings of WiFi access point mode!

*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**).

➢ 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.



wlan0 Intel Corporation Wireless 7260 (Wireless-N 7260) Iwlwifi

Status 169.254.165.239/16, fe80:0:0:0:18fc:45bb:5fd3:86cc/64

Carrier Yes

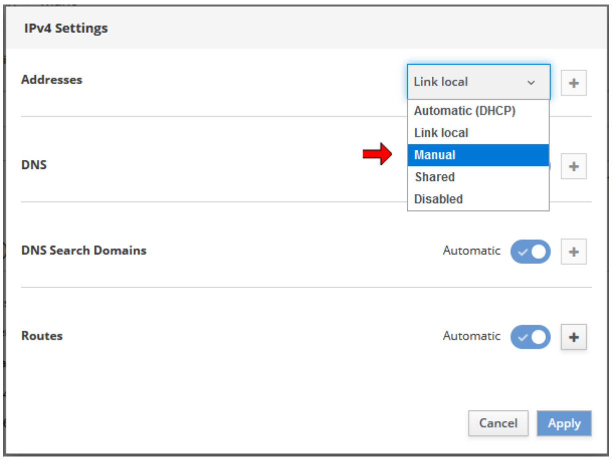
General ☑ Connect automatically

IPv4 Link local

IPv6 Automatic

*Figure 52: wlan0 configuration page*

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



IPv4 Settings

Addresses: Link local

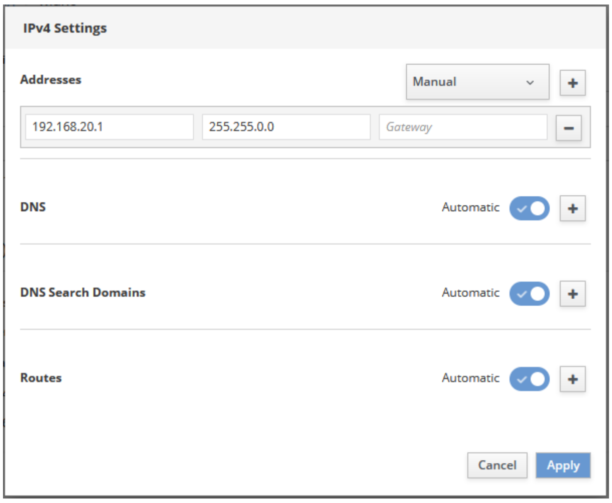
DNS

DNS Search Domains: Automatic

Routes: Automatic

*Figure 53: Set manual address in IPv4 Settings dialog*

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



IPv4 Settings

Addresses: Manual

192.168.20.1 | 255.255.0.0 | Gateway

DNS: Automatic

DNS Search Domains: Automatic

Routes: Automatic

*Figure 54: Enter Manual IP Address*

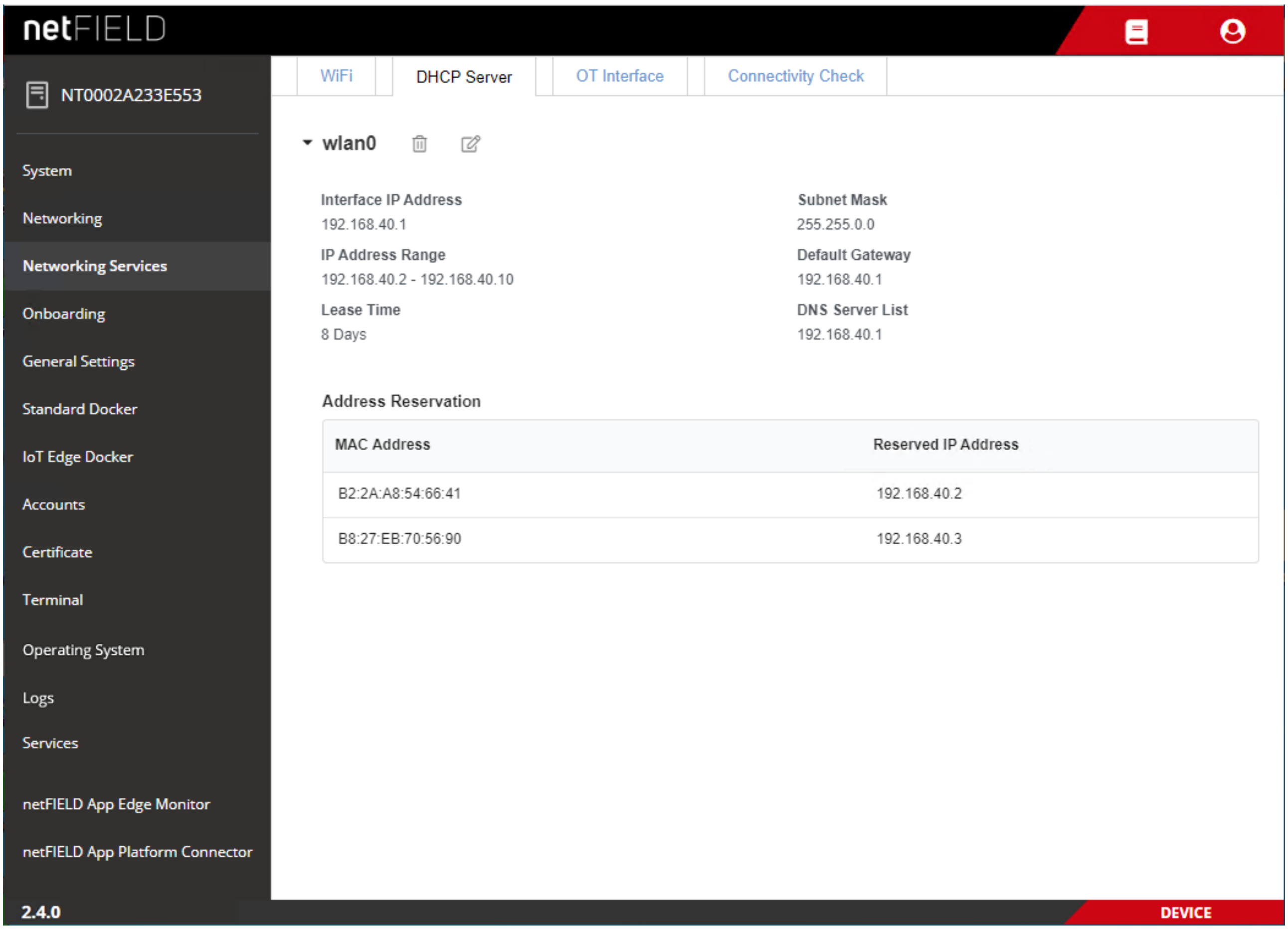
### Configure DHCP Server of Access Point

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).

## 6.4.2 DHCP Server

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

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



wlan0

Interface IP Address
192.168.40.1

Subnet Mask
255.255.0.0

IP Address Range
192.168.40.2 - 192.168.40.10

Default Gateway
192.168.40.1

Lease Time
8 Days

DNS Server List
192.168.40.1

Address Reservation

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

*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.<br>**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).<br>**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. |

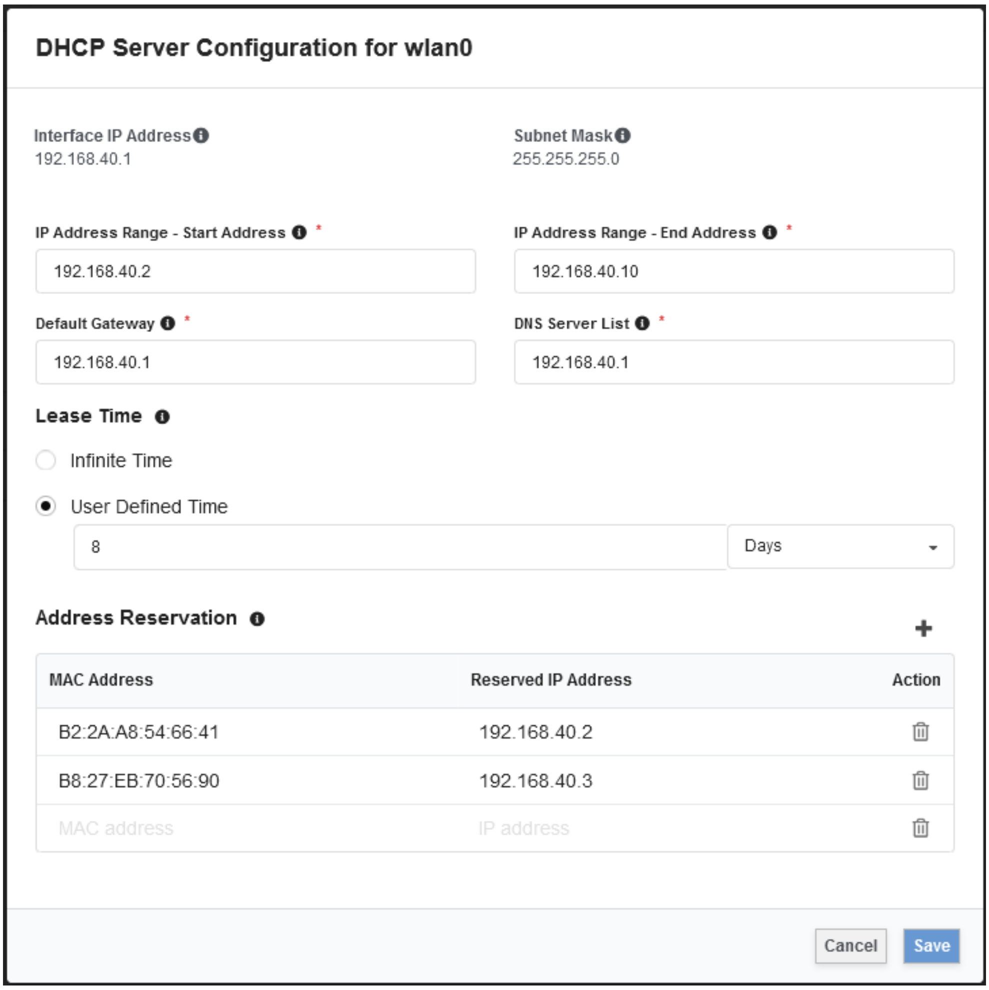
| Element/Parameter | Description |
|---|---|
| Lease Time | Specifies how long an IP address assigned by the DHCP server is valid. After this period, the client device asks the DHCP server for a renewal of the lease respectively for a new IP address assignment. |
| DNS Server List | IP address(es) of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

*Table 26: Elements/Parameters on DHCP Server page*

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

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

### DHCP Server Configuration dialog



DHCP Server Configuration for wlan0

Interface IP Address: 192.168.40.1

Subnet Mask: 255.255.255.0

IP Address Range - Start Address *: 192.168.40.2

IP Address Range - End Address *: 192.168.40.10

Default Gateway *: 192.168.40.1

DNS Server List *: 192.168.40.1

Lease Time

○ Infinite Time

● User Defined Time

8 Days

Address Reservation

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

*Figure 56: DHCP Server Configuration dialog*

| Parameter | Description |
|---|---|
| Interface IP address | IP address of your wlan0 interface/access point.<br>**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).<br>**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. |

| 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.<br>Click the **+** symbol above **Action** to add a reservation. To delete a reservation, click the 🗑 symbol.<br>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.<br>Wi-Fi clients can now connect to your Access Point. | |

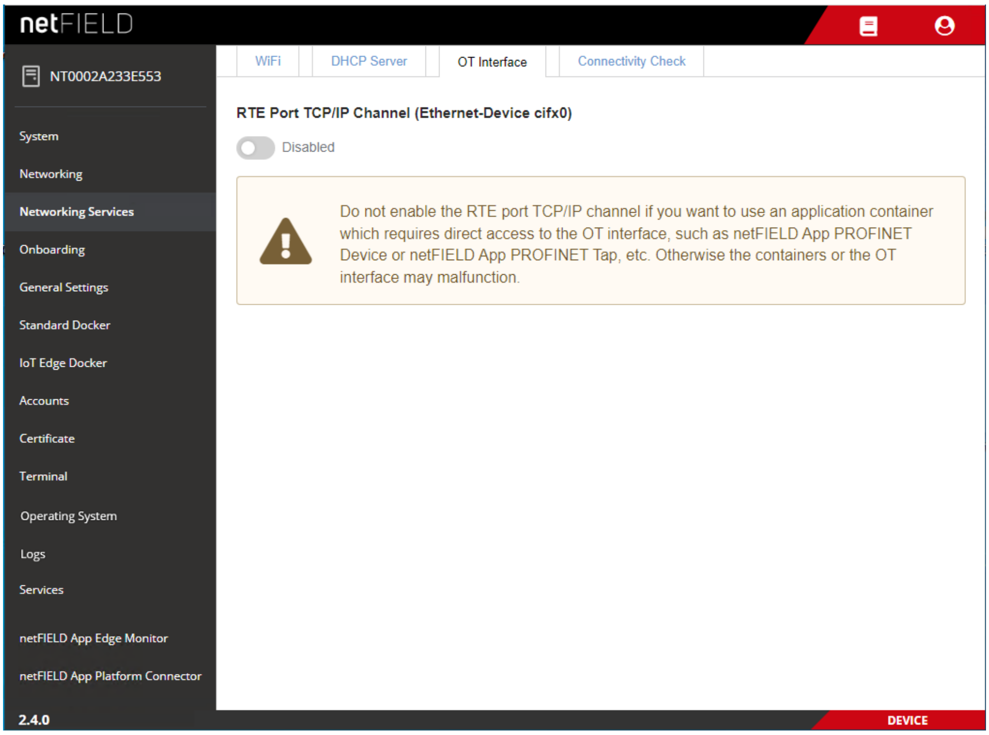
*Table 27: Parameters of DHCP Server Configuration dialog*

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

On the **OT Interface** tab of the **Networking Services** page, you can enable or disable the TCP/IP channel of the cifx0 interface.
Enabling the TCP/IP channel allows you to use the RTE ports (see positions (13) and (15) in section *Positions of the interfaces* [▸ page 16]) as standard Ethernet TCP/IP interface for acyclic services ("multicasts" are not supported).
Thus you could e.g. access the **Local Device Manager** via the RTE ("Fieldbus") interfaces instead of the LAN interfaces of the device. (Note that in this case, the UPnP service cannot be used for connecting to the device, because it is not supported by the cifx0 interface.)

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

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



RTE Port TCP/IP Channel (Ethernet-Device cifx0)

○ Disabled

Do not enable the RTE port TCP/IP channel if you want to use an application container which requires direct access to the OT interface, such as netFIELD App PROFINET Device or netFIELD App PROFINET Tap, etc. Otherwise the containers or the OT interface may malfunction.

*Figure 57: OT interface tab*

**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.

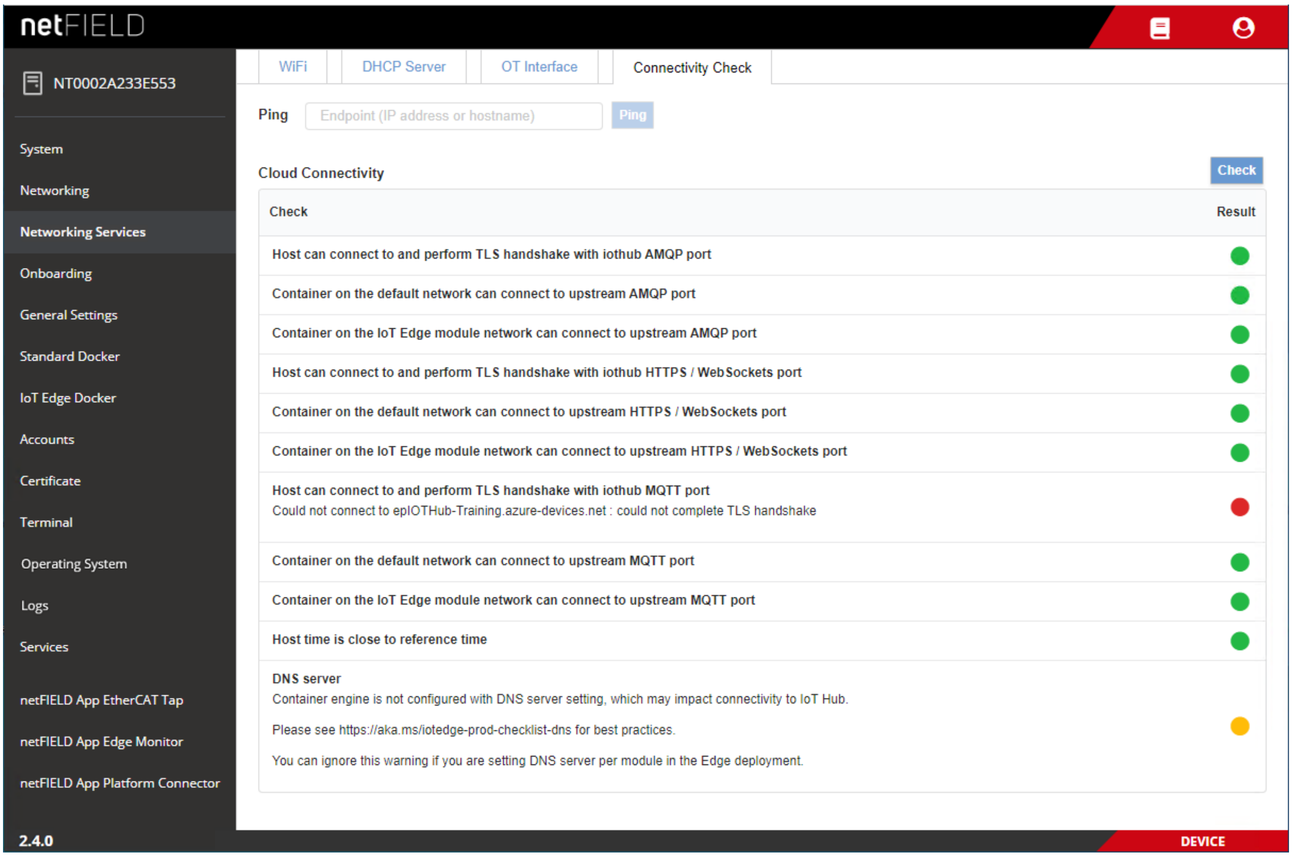
## 6.4.4 Connectivity Check

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

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

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

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



Cloud Connectivity

| Check | Result |
|---|---|
| Host can connect to and perform TLS handshake with iothub AMQP port | 🟢 |
| Container on the default network can connect to upstream AMQP port | 🟢 |
| Container on the IoT Edge module network can connect to upstream AMQP port | 🟢 |
| Host can connect to and perform TLS handshake with iothub HTTPS / WebSockets port | 🟢 |
| Container on the default network can connect to upstream HTTPS / WebSockets port | 🟢 |
| Container on the IoT Edge module network can connect to upstream HTTPS / WebSockets port | 🟢 |
| Host can connect to and perform TLS handshake with iothub MQTT port<br>Could not connect to epIOTHub-Training.azure-devices.net : could not complete TLS handshake | 🔴 |
| Container on the default network can connect to upstream MQTT port | 🟢 |
| Container on the IoT Edge module network can connect to upstream MQTT port | 🟢 |
| Host time is close to reference time | 🟢 |
| DNS server<br>Container engine is not configured with DNS server setting, which may impact connectivity to IoT Hub.<br>Please see https://aka.ms/iotedge-prod-checklist-dns for best practices.<br>You can ignore this warning if you are setting DNS server per module in the Edge deployment. | 🟡 |

*Figure 58: Connectivity Check tab*

### LAN/Internet ping

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

### Cloud Connectivity

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

The result is indicated with a dot:

🟢 OK (available)

🟠 Warning

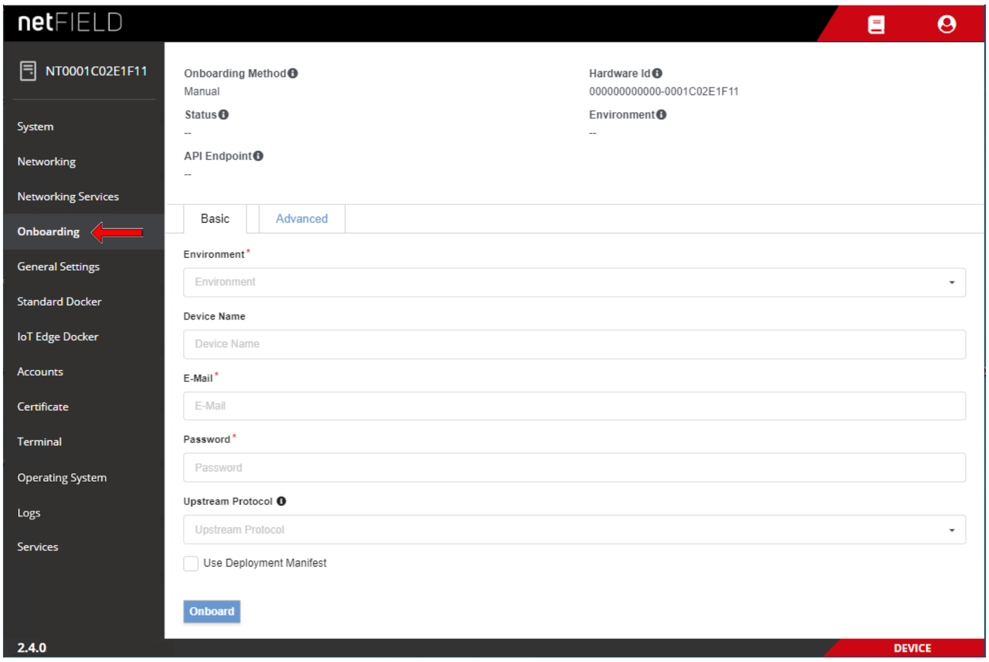
🔴 Error (not available)

For more information on the checks that are being performed, see https://github.com/Azure/iotedge/blob/main/doc/troubleshoot-checks.md
Note that the current netFIELD OS uses the *iotedge check* tool version 1.2.5.

## 6.5 Onboarding (and offboarding)

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

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



Onboarding Method: Manual

Hardware Id: 000000000000-0001C02E1F11

Status: --

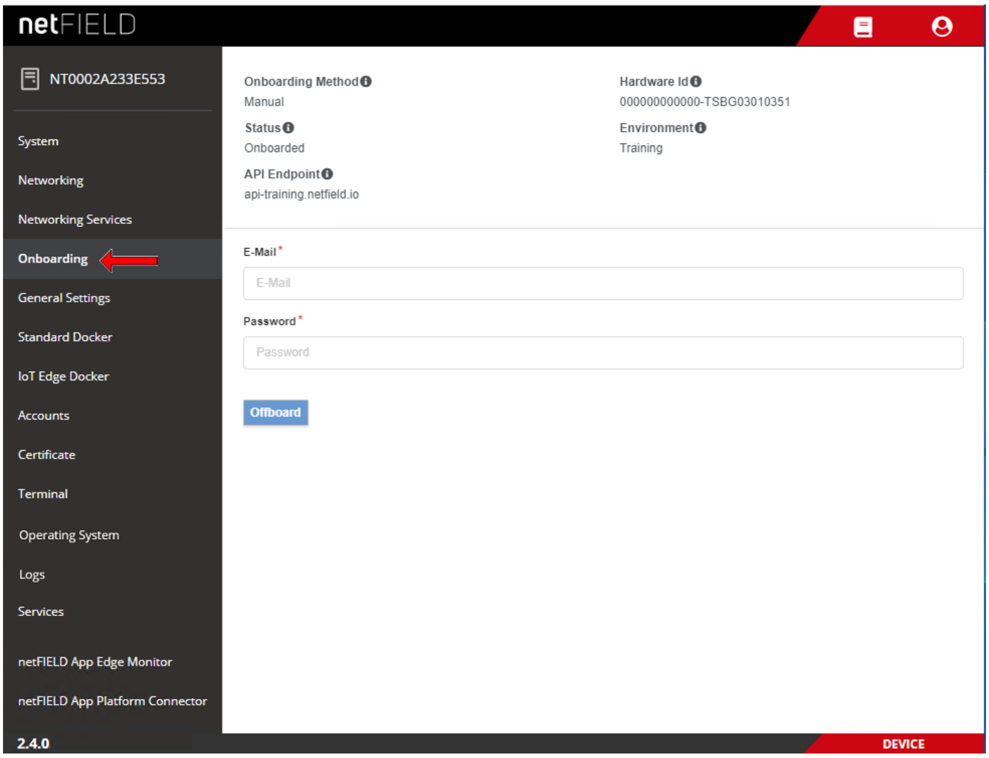
Environment: --

API Endpoint: --

*Figure 59: Basic Onboarding page*

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

### Offboarding after having used the Basic Onboarding method



Onboarding Method: Manual

Hardware Id: 000000000000-TSBG03010351

Status: Onboarded

Environment: Training

API Endpoint: api-training.netfield.io

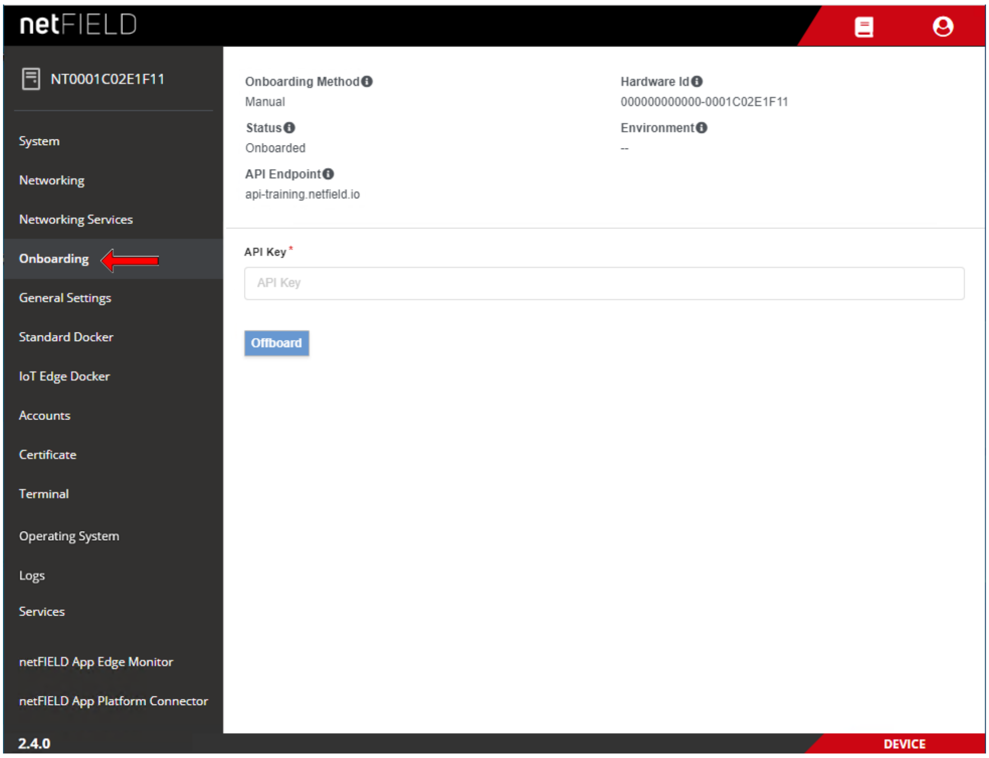
E-Mail *: E-Mail

Password *: Password

*Figure 60: Offboarding “Basic”*

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

### Offboarding after having used the Advanced Onboarding method



Onboarding Method: Manual

Hardware Id: 000000000000-0001C02E1F11

Status: Onboarded

Environment: --

API Endpoint: api-training.netfield.io

API Key *

*Figure 61: Offboarding “Advanced”*

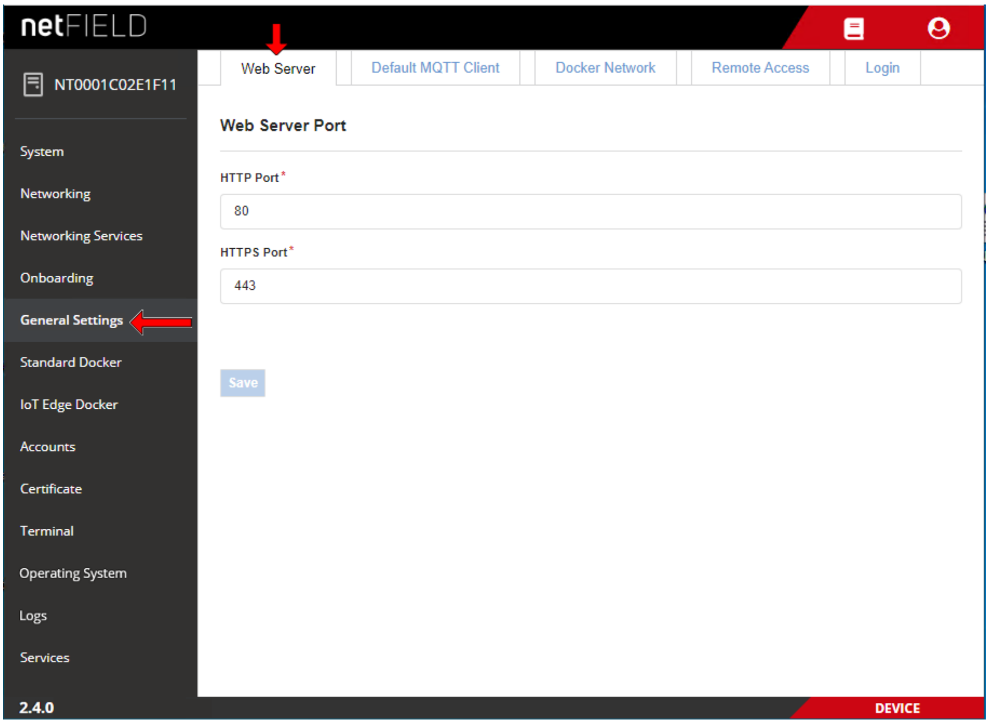
- ➢ In the **API KEY** field, enter an API Key that possesses the right to offboard devices. I.e. this key must have **Security Level** `org+ch` or `org` for the `deleteDevices` and `offboardedDevices` functions of the **devices** resource.
- ➢ Click **Offboard** button.
- ⇨ After successful offboarding,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

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

# 6.6 General Settings

## 6.6.1 Web Server (Port) Settings

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



Web Server Port

HTTP Port*: 80

HTTPS Port*: 443

*Figure 62: Web Server Settings tab*

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

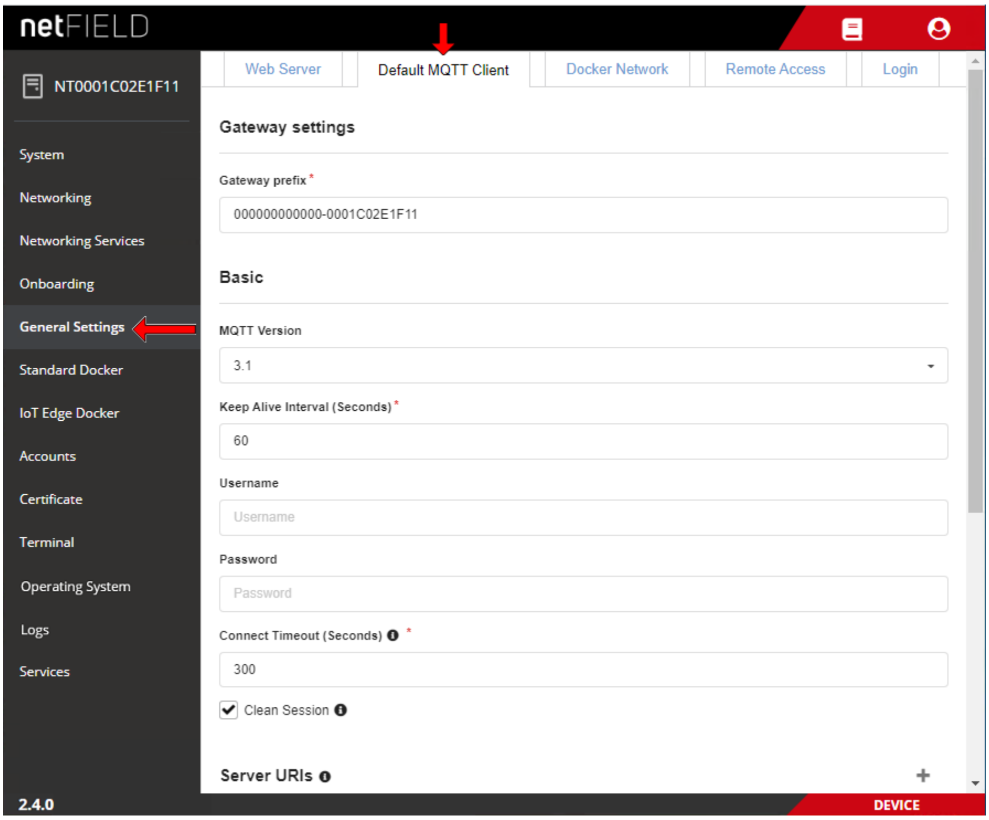
**Important:**
The new settings become immediately effective after saving and confirming the changes, which means that your current HTTP/ HTTPS connection to the netFIELD OS respectively Local Device Manager will be lost.
You will have to reconnect by specifying the new port number after the IP address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

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

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

### 6.6.2 Default MQTT Client Settings

On the **Default MQTT Client** tab of the **General Settings** page, you can change the MQTT Client configuration parameters that shall be used by the Docker containers that are running on your netFIELD OS. These settings are stored in a JSON configuration file in the netFIELD OS (`/etc/gateway/mqtt-config.json`).
By default, all Hilscher netFIELD Apps use this configuration file. Other containers (i.e. non-Hilscher application containers) that do not require their own customized MQTT client settings, can also use these settings here if the configuration file is referenced accordingly in the container image (e.g. in the *Container Create Options* of the netFIELD Portal, see *netFIELD Portal* operating instructions manual, DOC190701OIxxEN).



Gateway settings

Gateway prefix *
000000000000-0001C02E1F11

Basic

MQTT Version
3.1

Keep Alive Interval (Seconds) *
60

Username
Username

Password
Password

Connect Timeout (Seconds) *
300

☑ Clean Session

Server URIs +

*Figure 63: Default MQTT Settings*

| Element | | Description | |
|---|---|---|---|
| Gateway settings | Gateway prefix | Identifies the device. By default, this is the Hardware ID of the device. | |
| Basic | MQTT Version | MQTT version to be used (depending on the MQTT broker). | |
| | Keep Alive Interval | Defines the maximum length of time in seconds that the broker and client may not communicate with each other. | |
| | Username | User name for authentication at the broker (if implemented and required by the broker).<br>Note that the *netFIELD App MQTT Broker* from the netFIELD Portal does not require login authentication. | |
| | Password | Password for authentication at the broker (if implemented and required by the broker).<br>Note that the *netFIELD App MQTT 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.<br>If **Clean session** is unchecked, the broker creates a persistent session for the client. | |
| Server URIs | | Server URI or FQDN of the MQTT broker<br>**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.<br>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.<br>**Note**: This option is for expert users only! In the standard use case, in which the *netFIELD App MQTT 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). |

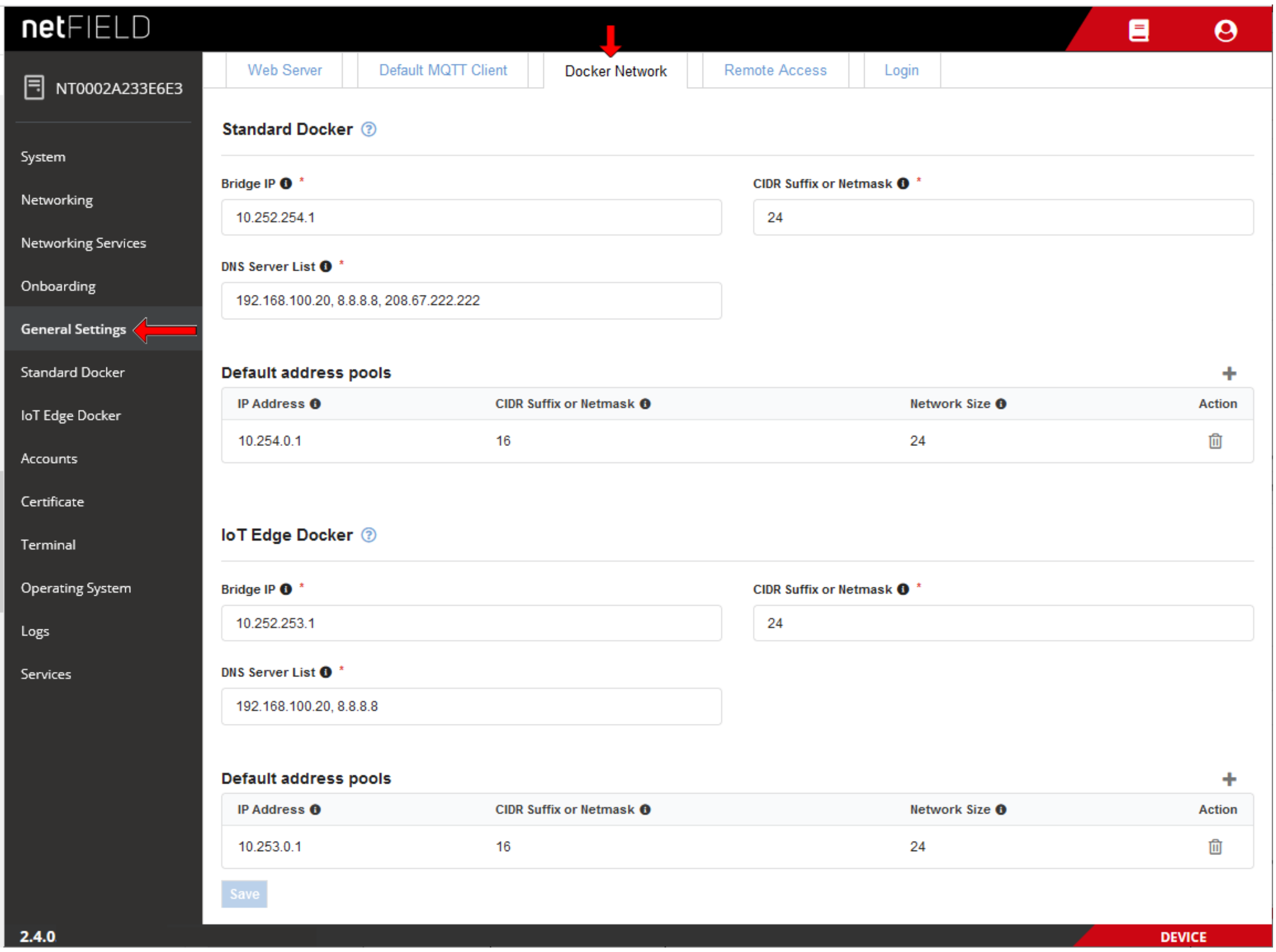
*Table 28: Default MQTT Client Settings*

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

### 6.6.3 Docker Network Settings

On the **Docker Network** tab of the **General Settings** page, you can change the network address settings of the Standard Docker and of the IoT Edge Docker.
You can also add addresses of external DNS server(s) for Standard Docker and IoT Edge Docker containers here.

**Important:**
These network address settings are predefined by Hilscher. Change these default addresses only if they are not compatible with your company's LAN address configuration, i.e. to avoid an address conflict.
Note that after changing the address settings of the Standard and/or IoT Edge Docker all containers running on the corresponding Docker will be stopped and deleted and the netFIELD OS will be automatically restarted. After restart, you might have to re-deploy the deleted containers that are not automatically re-deployed via the netFIELD Portal.



Standard Docker

Bridge IP *: 10.252.254.1
CIDR Suffix or Netmask *: 24
DNS Server List *: 192.168.100.20, 8.8.8.8, 208.67.222.222

Default address pools

| IP Address | CIDR Suffix or Netmask | Network Size | Action |
|---|---|---|---|
| 10.254.0.1 | 16 | 24 | 🗑 |

IoT Edge Docker

Bridge IP *: 10.252.253.1
CIDR Suffix or Netmask *: 24
DNS Server List *: 192.168.100.20, 8.8.8.8

Default address pools

| IP Address | CIDR Suffix or Netmask | Network Size | Action |
|---|---|---|---|
| 10.253.0.1 | 16 | 24 | 🗑 |

*Figure 64: Docker Network Settings*

### Standard Docker

The **docker0** bridge is a virtual default interface created by the Standard Docker.
By default, it uses the address `10.252.254.1/24` (“private range” as defined in RFC 1918) if the address is not already used on the host machine.
If not configured otherwise, a container deployed in the Standard Docker connects to this **docker0** bridge by default. The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. “masquerading”) created by the Standard Docker to communicate with destinations outside the netFIELD OS.
Note that the **docker0** default bridge does not provide internal or external DNS resolution for its containers. However, you can specify external DNS server(s) to be used by the containers in the Standard Docker.

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

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

*Table 29: Standard Docker Network Settings*

### IoT Edge Docker

The **iotedge0** bridge is a virtual default interface created by the IoT Edge Docker.
By default, it uses the address `10.252.253.1/24` (“private range” as defined in RFC 1918) if the address is not already used on the host machine.
If not configured otherwise, a container deployed in the IoT Edge Docker connects to this **iotedge0** bridge by default. (Note that most netFIELD App containers deployed from the netFIELD Portal are configured to connect themselves either to the *azure-iot-edge* bridge network or to the host network.)
The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. “masquerading”) created by the IoT Edge Docker to communicate with destinations outside the netFIELD OS.
Note that the **iotedge0** default bridge does not provide internal or external DNS resolution for its containers. However, you can specify external DNS server(s) to be used by the containers in the IoT Edge Docker.

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

*Table 30: IoT Edge Docker Network Settings*

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

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

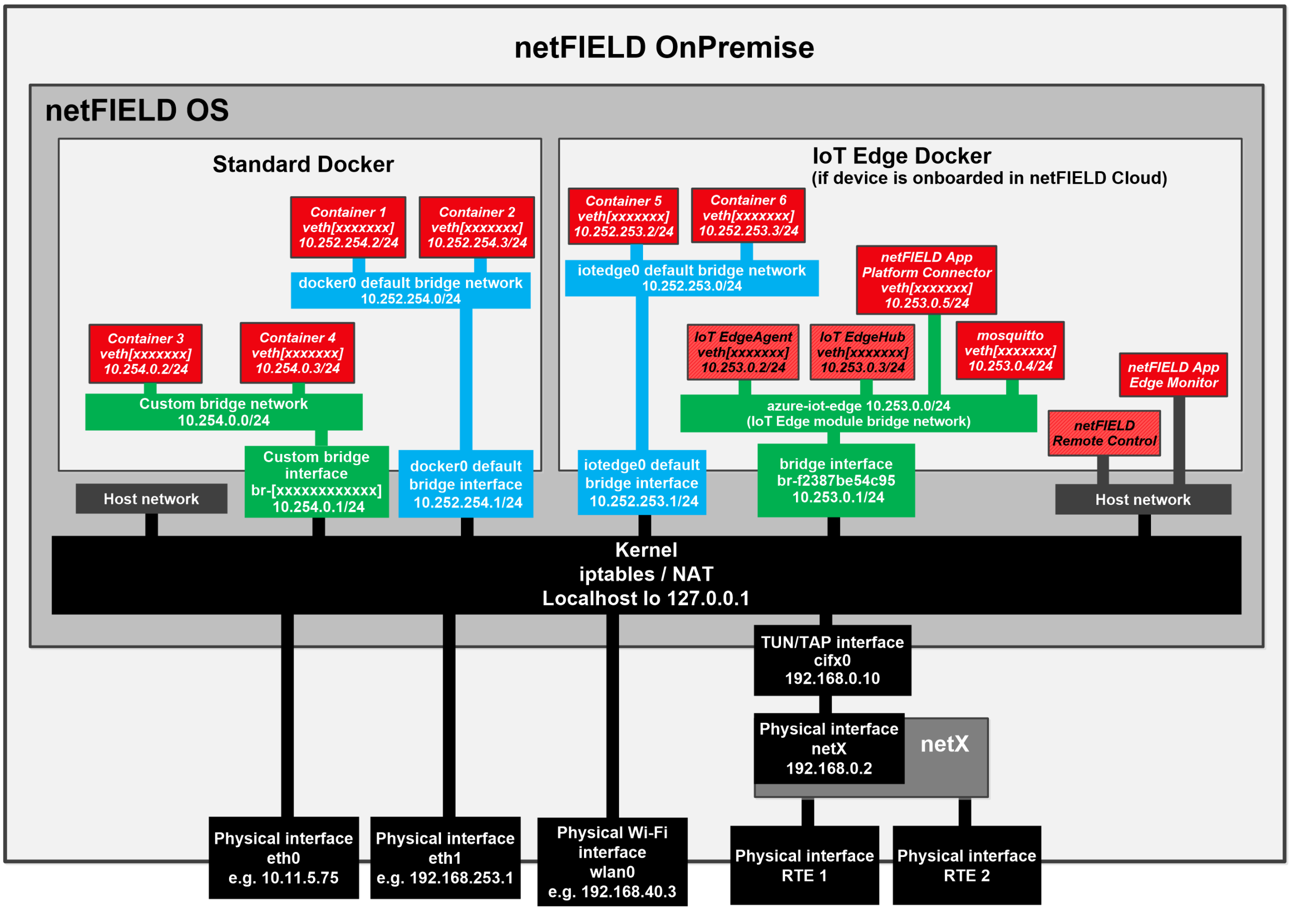

netFIELD OnPremise
netFIELD OS
Standard Docker
Container 1 veth[xxxxxxx] 10.252.254.2/24
Container 2 veth[xxxxxxx] 10.252.254.3/24
docker0 default bridge network 10.252.254.0/24
Container 3 veth[xxxxxxx] 10.254.0.2/24
Container 4 veth[xxxxxxx] 10.254.0.3/24
Custom bridge network 10.254.0.0/24
Custom bridge interface br-[xxxxxxxxxxxx] 10.254.0.1/24
docker0 default bridge interface 10.252.254.1/24
Host network
IoT Edge Docker
(if device is onboarded in netFIELD Cloud)
Container 5 veth[xxxxxxx] 10.252.253.2/24
Container 6 veth[xxxxxxx] 10.252.253.3/24
iotedge0 default bridge network 10.252.253.0/24
netFIELD App Platform Connector veth[xxxxxxx] 10.253.0.5/24
IoT EdgeAgent veth[xxxxxxx] 10.253.0.2/24
IoT EdgeHub veth[xxxxxxx] 10.253.0.3/24
mosquitto veth[xxxxxxx] 10.253.0.4/24
netFIELD App Edge Monitor
azure-iot-edge 10.253.0.0/24 (IoT Edge module bridge network)
netFIELD Remote Control
iotedge0 default bridge interface 10.252.253.1/24
bridge interface br-f2387be54c95 10.253.0.1/24
Host network
Kernel
iptables / NAT
Localhost lo 127.0.0.1
TUN/TAP interface cifx0 192.168.0.10
Physical interface netX 192.168.0.2
netX
Physical interface eth0 e.g. 10.11.5.75
Physical interface eth1 e.g. 192.168.253.1
Physical Wi-Fi interface wlan0 e.g. 192.168.40.3
Physical interface RTE 1
Physical interface RTE 2

*Figure 65: Default docker network configuration*

### 6.6.4 Remote Access

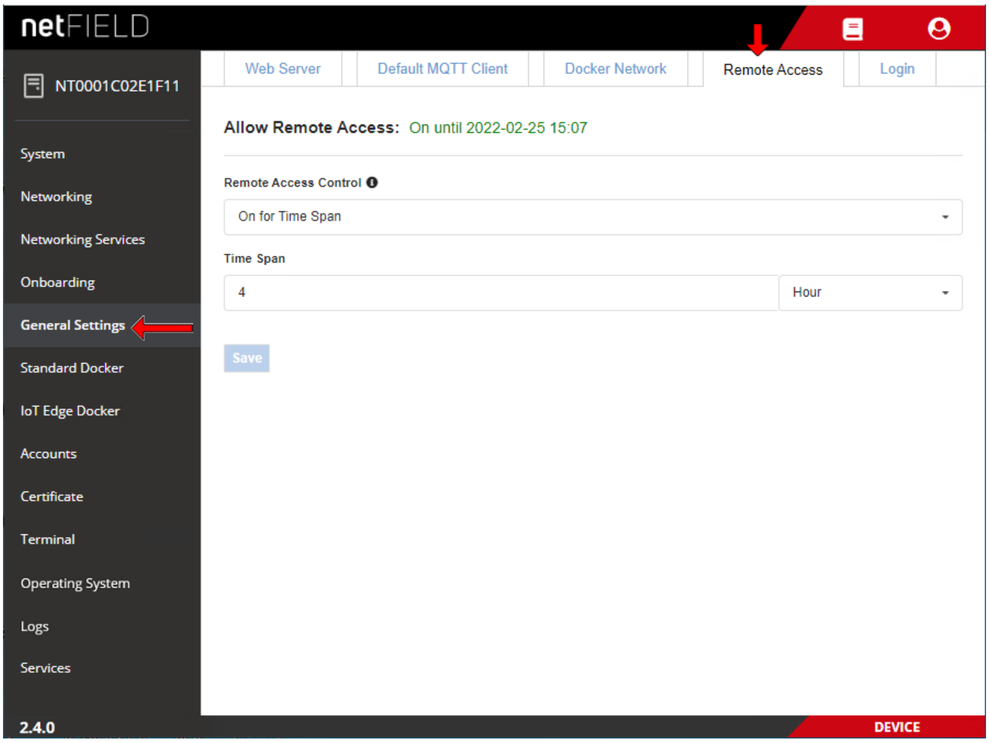
On the **Remote Access** tab of the **General Settings** page, you can enable (on) or disable (off) *Remote Control* access from the netFIELD Portal to your device.

**Note:**
Note that your device must be onboarded in the netFIELD Cloud and connected to the Internet in order to use the remote control functions.
Contact your local Hilscher sales representative for information on the terms and conditions of an account/subscription for the *netFIELD Cloud services* (https://www.netfield.io).

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

Note that if you have updated your device from an older netFIELD OS version to version ≥ 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).



Allow Remote Access: On until 2022-02-25 15:07

Remote Access Control: On for Time Span

Time Span: 4 Hour

Figure 66: Remote Access tab

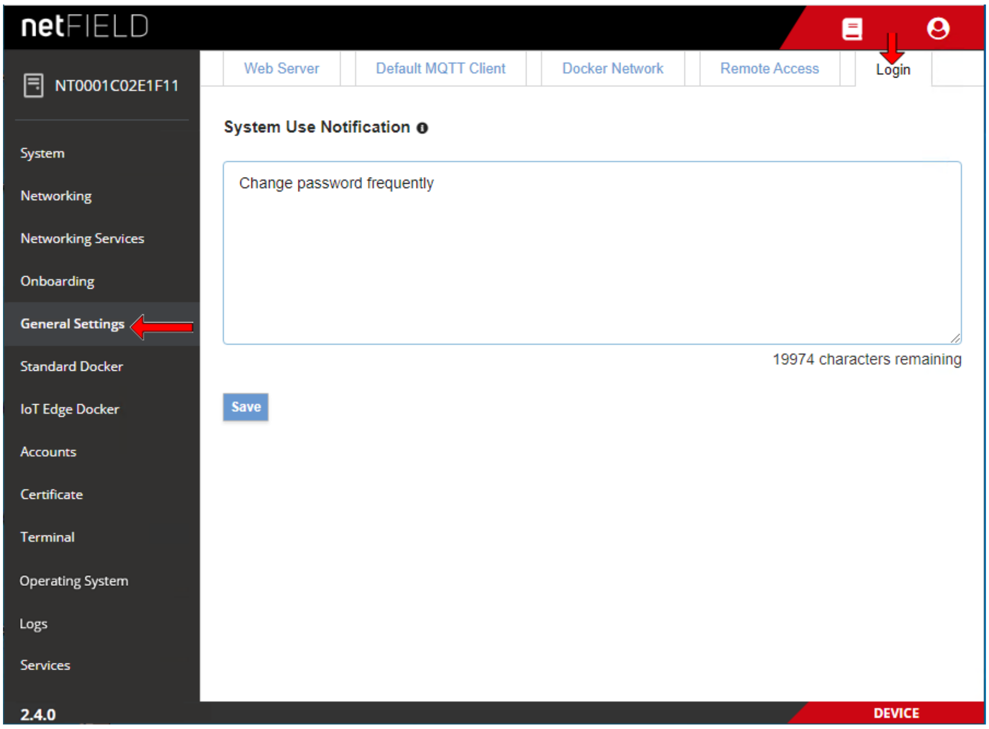
- In the **Remote Access Control** dropdown-list, enable (**on**) or disable (**off**) the remote access according to your use case. You can also define time limits (**On for Time Span**) for allowing remote access to the device.

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

- Click **Save**.

## 6.6.5 Login

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



System Use Notification

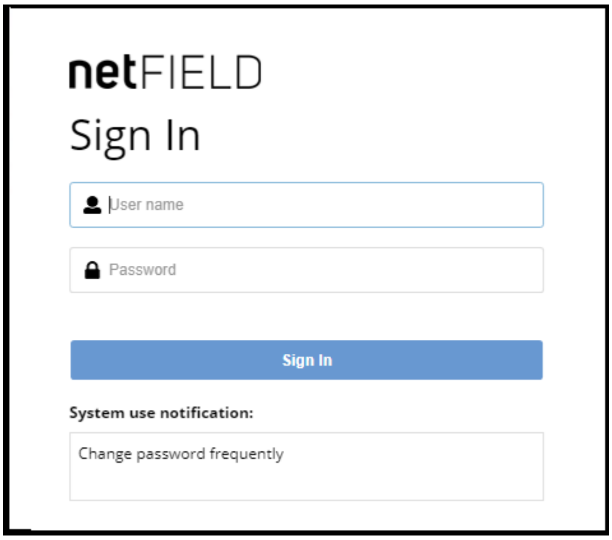
Change password frequently

19974 characters remaining

Figure 67: Login tab

➢ In the text field, enter the message that shall be displayed, then click **Save** button.

➩ The message will be displayed in the *Sign In* dialog of the Local Device Manager:



System use notification:

Change password frequently

Figure 68: Notification on Sign In dialog

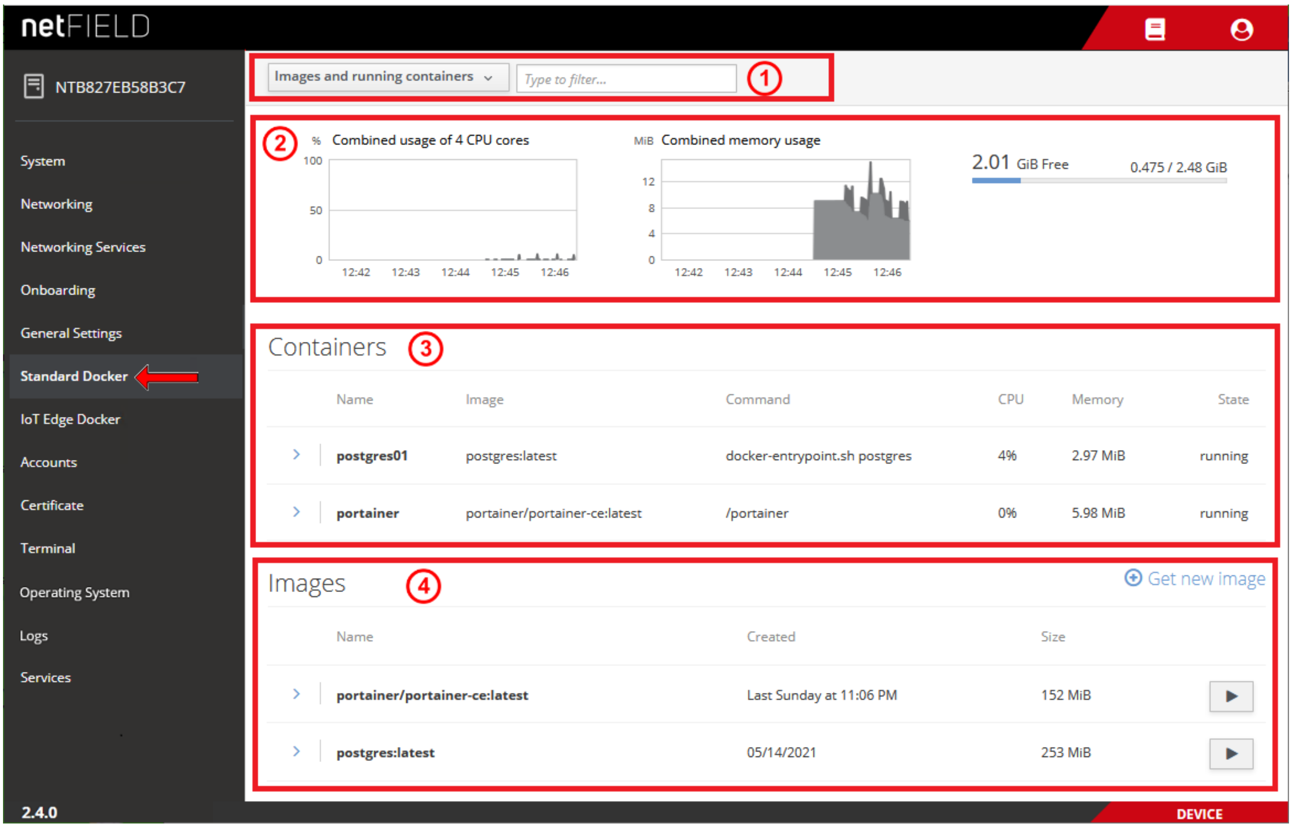
➢ To remove the message from the *Sign In* dialog again, go to **General Settings** > **Login** and delete the message from the text field, then click **Save** button.

## 6.7 Standard Docker

The **Standard Docker** page allows you to manage Docker images and containers from the “standard” Docker Hub or from a local repository. It lists all containers that were deployed on the device; except for those that were deployed from the netFIELD Cloud via netFIELD Portal (containers deployed from the netFIELD Cloud are listed on the **IoT Edge Docker** page – see section *IoT Edge Docker* [▹ page 117]).
Unlike the **IoT Edge Docker**, the Standard Docker can be used without having to “onboard” the device in the portal beforehand.

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

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



Containers

| Name | Image | Command | CPU | Memory | State |
|---|---|---|---|---|---|
| postgres01 | postgres:latest | docker-entrypoint.sh postgres | 4% | 2.97 MiB | running |
| portainer | portainer/portainer-ce:latest | /portainer | 0% | 5.98 MiB | running |

Images

| Name | Created | Size |
|---|---|---|
| portainer/portainer-ce:latest | Last Sunday at 11:06 PM | 152 MiB |
| postgres:latest | 05/14/2021 | 253 MiB |

*Figure 69: Standard Docker*

### Filter options in header

The elements in the header (1) allow you to filter the display of containers and images.
You can choose in the drop-down list:

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

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

### Graphs

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

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

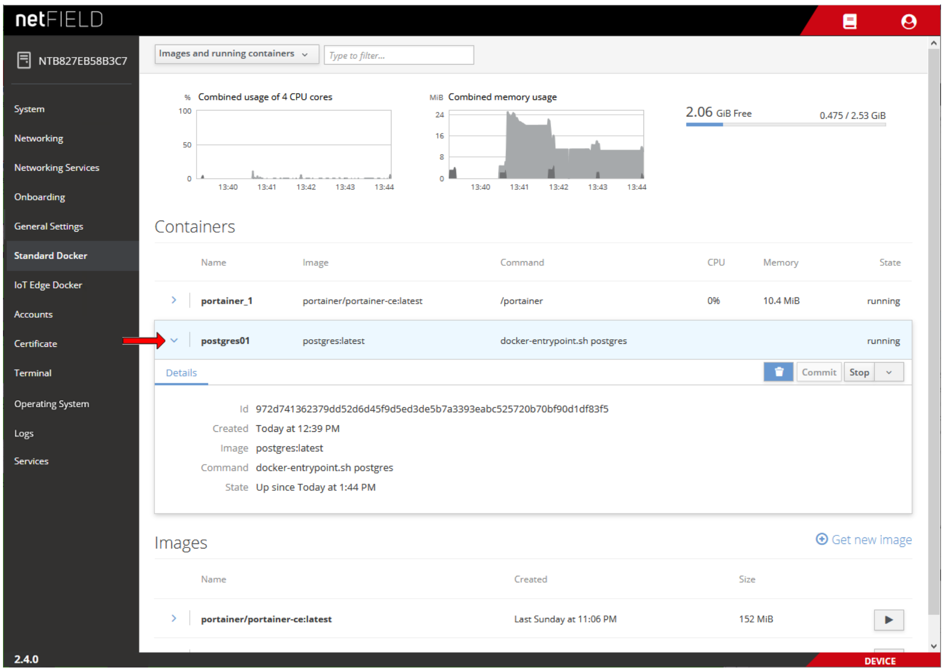
**Combined memory usage**: Load of the containers on the memory.

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

### Containers

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

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



Containers

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

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

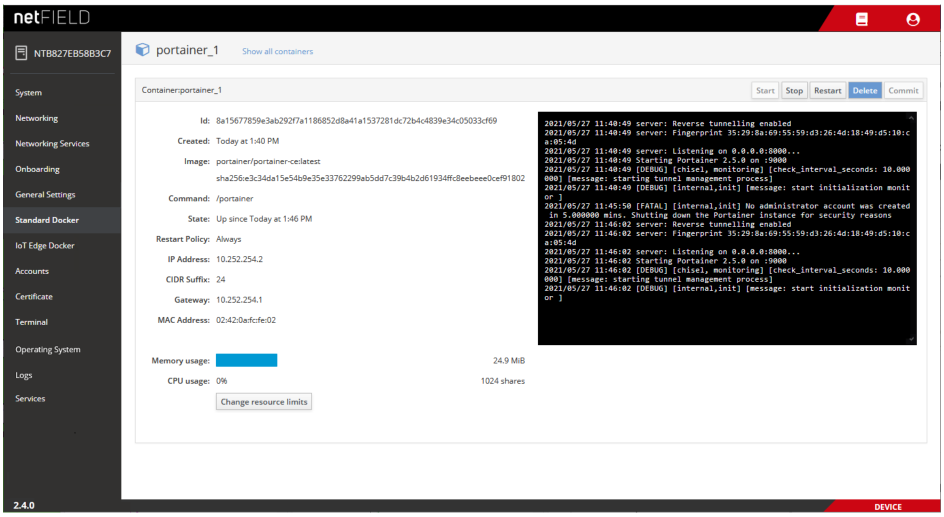
Images

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

*Figure 70: Expand concise container details*

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

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



Container:portainer_1

Id: 8a15677859e3ab292f7a1186852d8a41a1537281dc72b4c4839e34c05033cf69
Created: Today at 1:40 PM
Image: portainer/portainer-ce:latest
sha256:e3c34da15e54b9e35e33762299ab5dd7c39b4b2d61934ffc8eebeee0cef91802
Command: /portainer
State: Up since Today at 1:46 PM
Restart Policy: Always
IP Address: 10.252.254.2
CIDR Suffix: 24
Gateway: 10.252.254.1
MAC Address: 02:42:0a:fc:fe:02

Memory usage: 24.9 MiB
CPU usage: 0% 1024 shares

```
2021/05/27 11:40:49 server: Reverse tunnelling enabled
2021/05/27 11:40:49 server: Fingerprint 35:29:8a:69:55:59:d3:26:4d:18:49:d5:10:c
a:05:4d
2021/05/27 11:40:49 server: Listening on 0.0.0.0:8000...
2021/05/27 11:40:49 Starting Portainer 2.5.0 on :9000
2021/05/27 11:40:49 [DEBUG] [chisel, monitoring] [check_interval_seconds: 10.000
000] [message: starting tunnel management process]
2021/05/27 11:40:49 [DEBUG] [internal,init] [message: start initialization monit
or ]
2021/05/27 11:45:50 [FATAL] [internal,init] No administrator account was created
 in 5.000000 mins. Shutting down the Portainer instance for security reasons
2021/05/27 11:46:02 server: Reverse tunnelling enabled
2021/05/27 11:46:02 server: Fingerprint 35:29:8a:69:55:59:d3:26:4d:18:49:d5:10:c
a:05:4d
2021/05/27 11:46:02 server: Listening on 0.0.0.0:8000...
2021/05/27 11:46:02 Starting Portainer 2.5.0 on :9000
2021/05/27 11:46:02 [DEBUG] [chisel, monitoring] [check_interval_seconds: 10.000
000] [message: starting tunnel management process]
2021/05/27 11:46:02 [DEBUG] [internal,init] [message: start initialization monit
or ]
```

*Figure 71: Container parameters with terminal window*

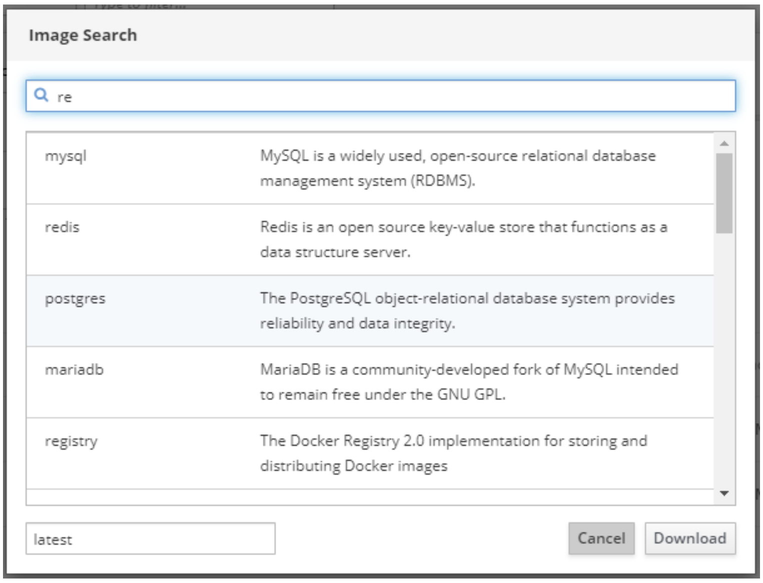
➢ To go back to the **Standard Docker** overview page, click the blue **Show all containers** link in the page header.

### Images

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

➢ You can download a Docker image by clicking the **Get new image** link.

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



re

| | |
|---|---|
| mysql | MySQL is a widely used, open-source relational database management system (RDBMS). |
| redis | Redis is an open source key-value store that functions as a data structure server. |
| postgres | The PostgreSQL object-relational database system provides reliability and data integrity. |
| mariadb | MariaDB is a community-developed fork of MySQL intended to remain free under the GNU GPL. |
| registry | The Docker Registry 2.0 implementation for storing and distributing Docker images |

latest

*Figure 72: Image Search dialog of Standard Docker*

➢ In the search field, type-in a name or search string, then press **Enter** on your keyboard.

➾ A list featuring the search results is displayed.

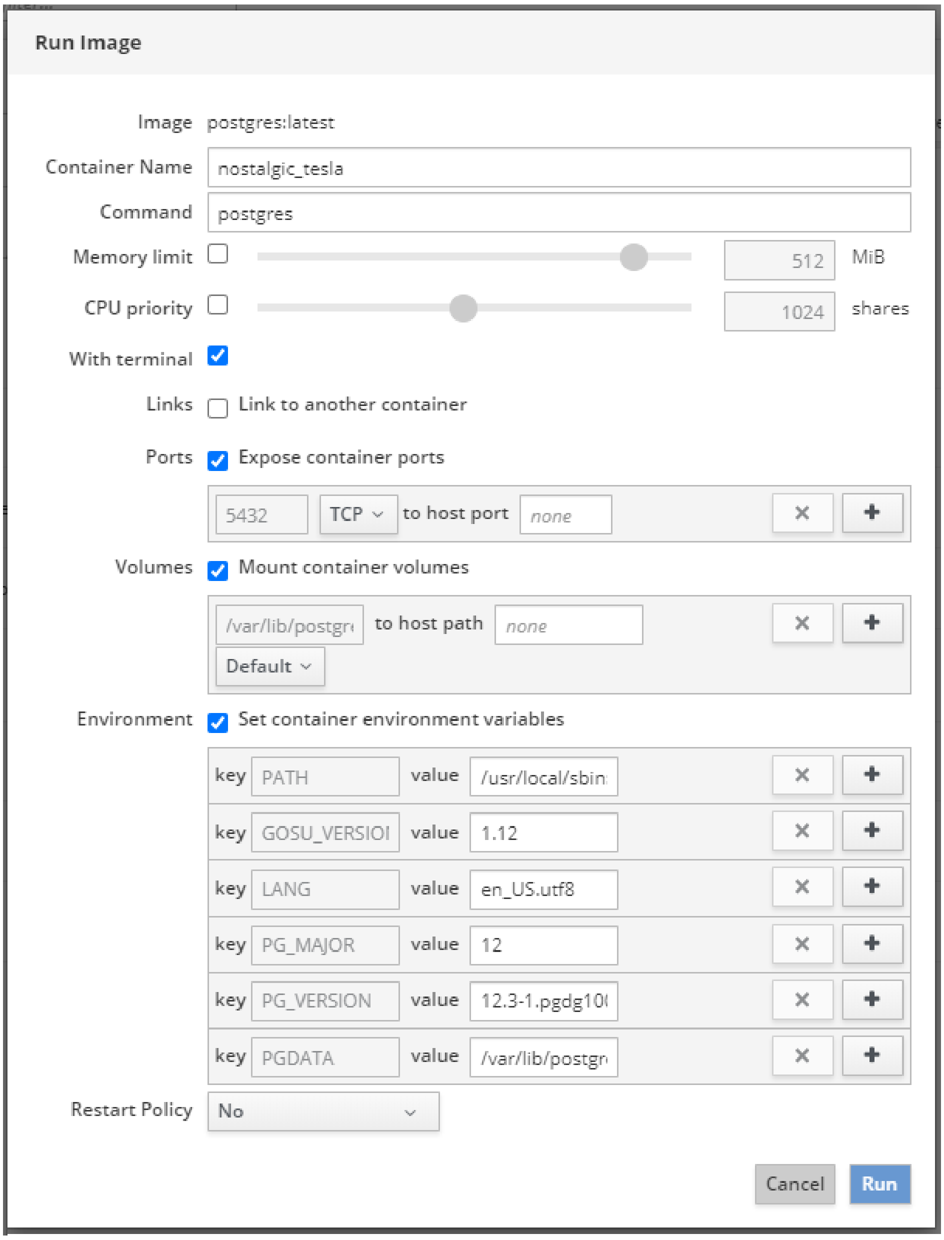
➢ Select an image in the list, then click **Download** button.

➾ The image is downloaded, extracted and displayed in the **Images** area.

### Starting a container

➢ You can start a container (i.e. run an instance of the program contained in the image), by clicking the ▶ button on the right side of the image in the list.

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



Run Image

Image postgres:latest

Container Name nostalgic_tesla

Command postgres

Memory limit □ 512 MiB

CPU priority □ 1024 shares

With terminal ☑

Links □ Link to another container

Ports ☑ Expose container ports

5432 TCP to host port none ✕ +

Volumes ☑ Mount container volumes

/var/lib/postgr to host path none ✕ +
Default

Environment ☑ Set container environment variables

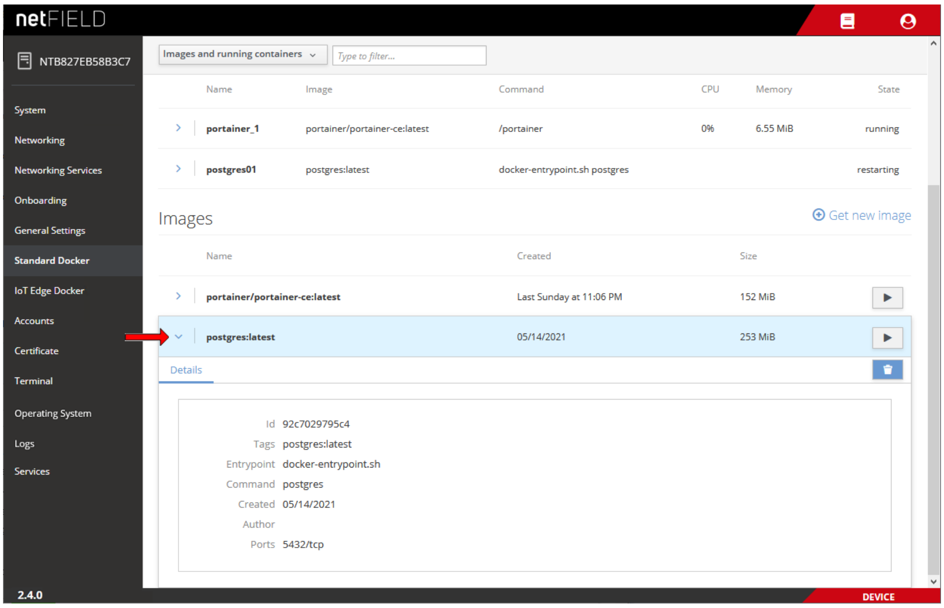
| | | | | | |
|---|---|---|---|---|---|
| key | PATH | value | /usr/local/sbin | ✕ | + |
| key | GOSU_VERSIOI | value | 1.12 | ✕ | + |
| key | LANG | value | en_US.utf8 | ✕ | + |
| key | PG_MAJOR | value | 12 | ✕ | + |
| key | PG_VERSION | value | 12.3-1.pgdg10( | ✕ | + |
| key | PGDATA | value | /var/lib/postgr | ✕ | + |

Restart Policy No

*Figure 73: Run Image dialog*

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

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



| Name | Image | Command | CPU | Memory | State |
|---|---|---|---|---|---|
| portainer_1 | portainer/portainer-ce:latest | /portainer | 0% | 6.55 MiB | running |
| postgres01 | postgres:latest | docker-entrypoint.sh postgres | | | restarting |

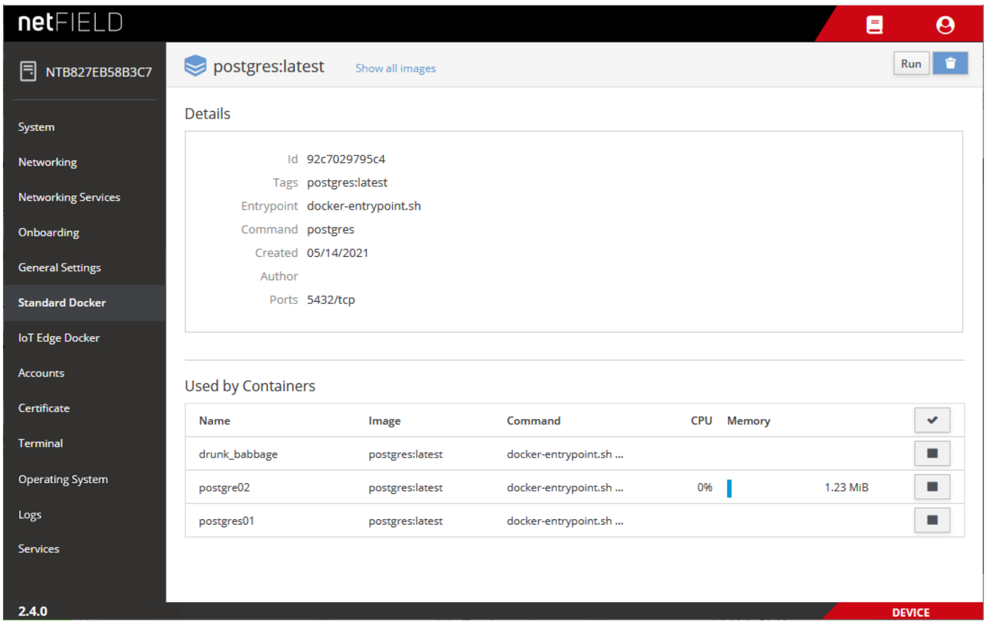
| Name | Created | Size |
|---|---|---|
| portainer/portainer-ce:latest | Last Sunday at 11:06 PM | 152 MiB |
| postgres:latest | 05/14/2021 | 253 MiB |

Id 92c7029795c4
Tags postgres:latest
Entrypoint docker-entrypoint.sh
Command postgres
Created 05/14/2021
Author
Ports 5432/tcp

*Figure 74: Expand image details*

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

➩ A page featuring detailed information opens:



Details

| | |
|---|---|
| Id | 92c7029795c4 |
| Tags | postgres:latest |
| Entrypoint | docker-entrypoint.sh |
| Command | postgres |
| Created | 05/14/2021 |
| Author | |
| Ports | 5432/tcp |

Used by Containers

| Name | Image | Command | CPU | Memory | ✓ |
|---|---|---|---|---|---|
| drunk_babbage | postgres:latest | docker-entrypoint.sh ... | | | ■ |
| postgre02 | postgres:latest | docker-entrypoint.sh ... | 0% | 1.23 MiB | ■ |
| postgres01 | postgres:latest | docker-entrypoint.sh ... | | | ■ |

*Figure 75: Image details*

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

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

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

**Note:**

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

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

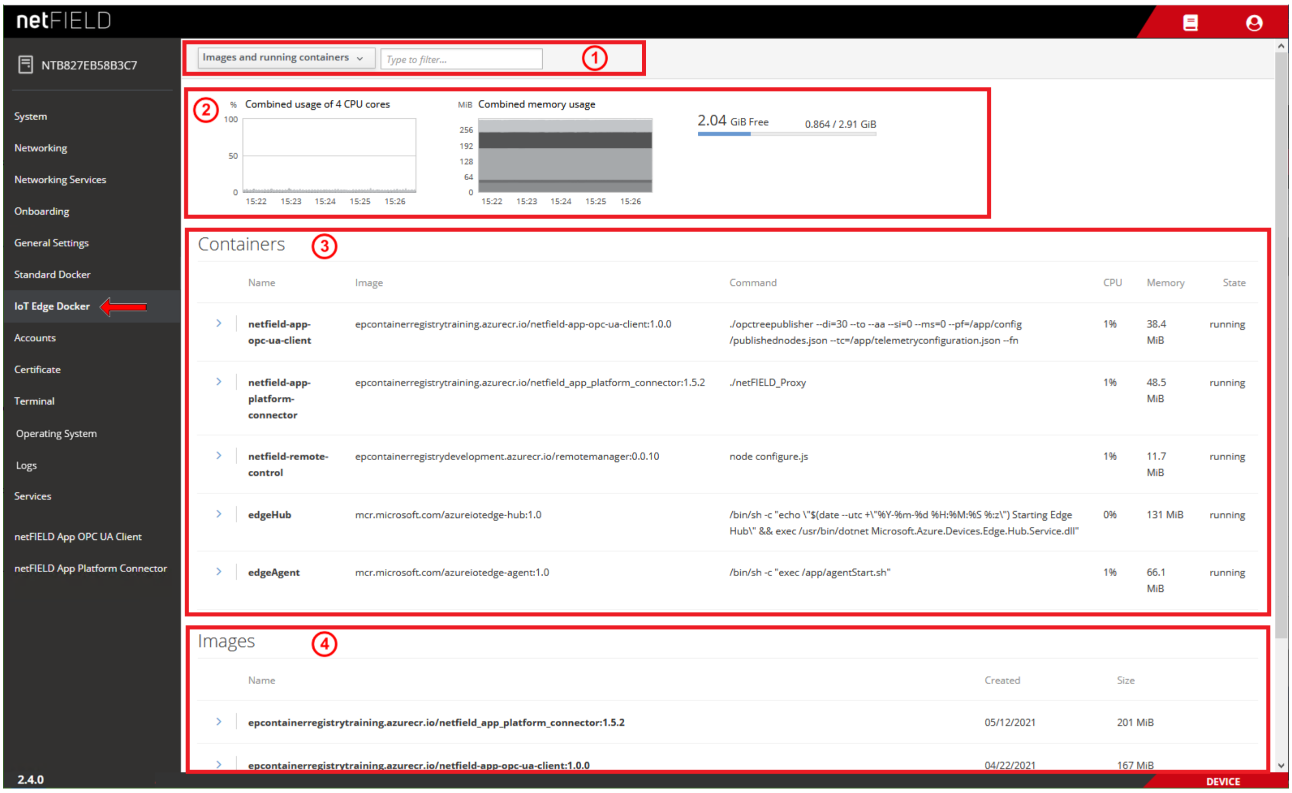
## 6.8 IoT Edge Docker

On the **IoT Edge Docker** page, you can monitor the Docker images and containers that were deployed from the netFIELD Cloud via the netFIELD Portal.
Note that you have to “onboard” your device (see section *"Onboard" (register) device in netFIELD Cloud* [▸ page 41]) before you can access this page.

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

Here you can, however, change the limits of the resources (memory and CPU priority) that your application container is allowed to consume on the device.
You can also “remove” an obsolete container image here, but only if you have deleted it in the Device Manager of the portal beforehand. (If you delete an image only locally on the device without having deleted it in the portal beforehand, the image will be automatically deployed again).

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



Containers

| Name | Image | Command | CPU | Memory | State |
|---|---|---|---|---|---|
| netfield-app-opc-ua-client | epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0 | ./opctreepublisher --di=30 --to --aa --si=0 --ms=0 --pf=/app/config /publishednodes.json --tc=/app/telemetryconfiguration.json --fn | 1% | 38.4 MiB | running |
| netfield-app-platform-connector | epcontainerregistrytraining.azurecr.io/netfield_app_platform_connector:1.5.2 | ./netFIELD_Proxy | 1% | 48.5 MiB | running |
| netfield-remote-control | epcontainerregistrydevelopment.azurecr.io/remotemanager:0.0.10 | node configure.js | 1% | 11.7 MiB | running |
| edgeHub | mcr.microsoft.com/azureiotedge-hub:1.0 | /bin/sh -c "echo \"$(date --utc +\"%Y-%m-%d %H:%M:%S %:z\") Starting Edge Hub\" && exec /usr/bin/dotnet Microsoft.Azure.Devices.Edge.Hub.Service.dll" | 0% | 131 MiB | running |
| edgeAgent | mcr.microsoft.com/azureiotedge-agent:1.0 | /bin/sh -c "exec /app/agentStart.sh" | 1% | 66.1 MiB | running |

Images

| Name | Created | Size |
|---|---|---|
| epcontainerregistrytraining.azurecr.io/netfield_app_platform_connector:1.5.2 | 05/12/2021 | 201 MiB |
| epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0 | 04/22/2021 | 167 MiB |

*Figure 76: IOT Edge Docker*

**Note:**
The *edgeHub* and *edgeAgent* are Microsoft images/containers (called “modules” in Microsoft terms) that make up the Azure IoT Edge runtime, which is necessary for connecting your device to the netFIELD Cloud (which uses the Azure cloud).
The *edgeAgent* is automatically downloaded and instantiated on the device after onboarding; the *edgeHub* is automatically downloaded and instantiated when you deploy a container from the portal for the first time.

### Filter options in header

The elements in the header (1) allow you to filter the display of containers and images.
You can choose in the drop-down list:

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

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

### Graphs

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

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

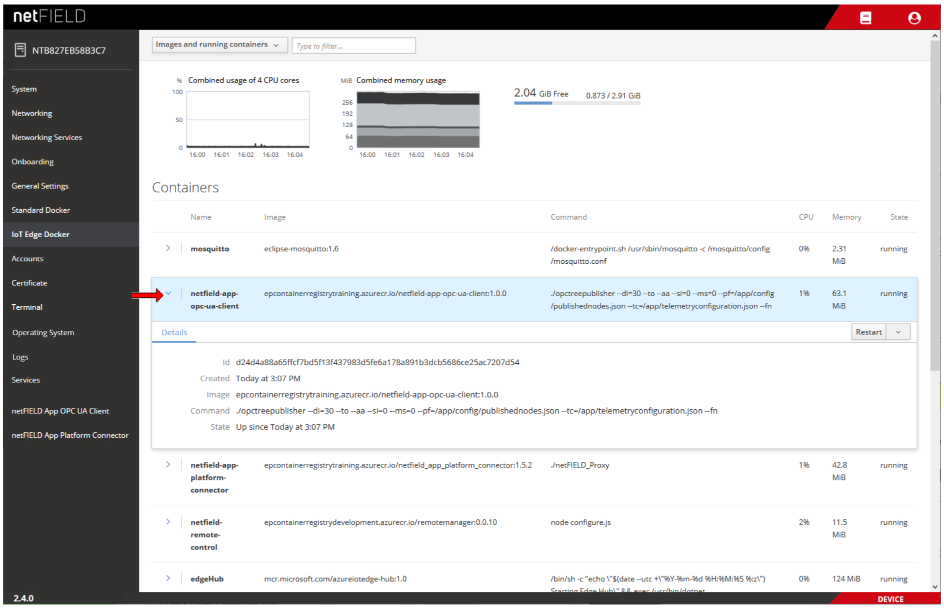
**Combined memory usage**: Load of the containers on the memory.

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

### Containers

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

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



Containers

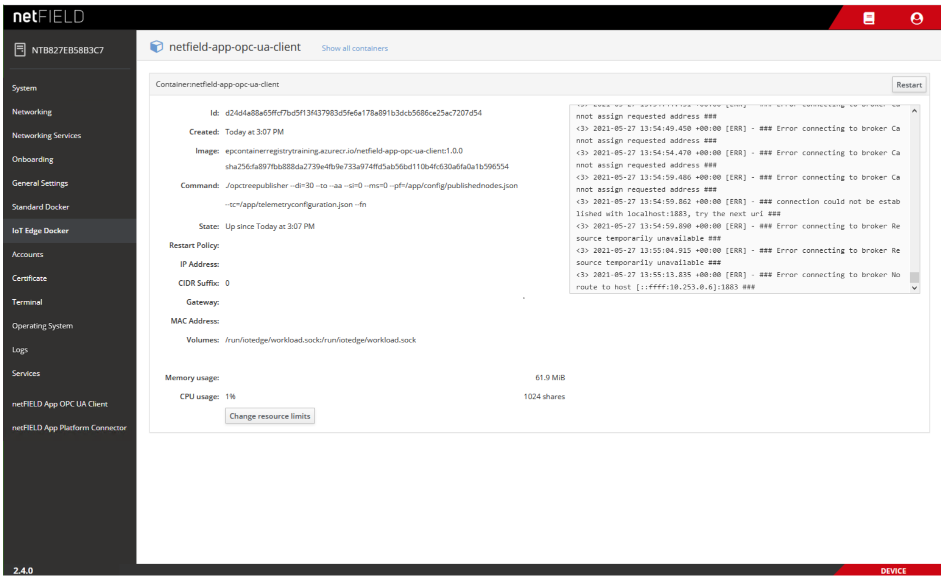
| Name | Image | Command | CPU | Memory | State |
|---|---|---|---|---|---|
| mosquitto | eclipse-mosquitto:1.6 | /docker-entrypoint.sh /usr/sbin/mosquitto -c /mosquitto/config /mosquitto.conf | 0% | 2.31 MiB | running |
| netfield-app-opc-ua-client | epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0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

Id d24d4a88a65ffcf7bd5f13f437983d5fe6a178a891b3dcb5686ce25ac7207d54
Created Today at 3:07 PM
Image epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0
Command ./opctreepublisher --di=30 --to --aa --si=0 --ms=0 --pf=/app/config/publishednodes.json --tc=/app/telemetryconfiguration.json --fn
State Up since Today at 3:07 PM

*Figure 77: Container details expanded*

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

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



netfield-app-opc-ua-client

Container:netfield-app-opc-ua-client

Id: d24d4a88a65ffcf7bd5f13f437983d5fe6a178a891b3dcb5686ce25ac7207d54
Created: Today at 3:07 PM
Image: epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0
sha256:fa897fbb888da2739e4fb9e733a974ffd5ab56bd110b4fc630a6fa0a1b596554
Command: ./opctreepublisher --di=30 --to --aa --si=0 --ms=0 --pf=/app/config/publishednodes.json
--tc=/app/telemetryconfiguration.json --fn
State: Up since Today at 3:07 PM
Restart Policy:
IP Address:
CIDR Suffix: 0
Gateway:
MAC Address:
Volumes: /run/iotedge/workload.sock:/run/iotedge/workload.sock

Memory usage: 61.9 MiB
CPU usage: 1% 1024 shares

```
nnot assign requested address ###
<3> 2021-05-27 13:54:49.450 +00:00 [ERR] - ### Error connecting to broker Ca
nnot assign requested address ###
<3> 2021-05-27 13:54:54.470 +00:00 [ERR] - ### Error connecting to broker Ca
nnot assign requested address ###
<3> 2021-05-27 13:54:59.486 +00:00 [ERR] - ### Error connecting to broker Ca
nnot assign requested address ###
<3> 2021-05-27 13:54:59.862 +00:00 [ERR] - ### connection could not be estab
lished with localhost:1883, try the next uri ###
<3> 2021-05-27 13:54:59.890 +00:00 [ERR] - ### Error connecting to broker Re
source temporarily unavailable ###
<3> 2021-05-27 13:55:04.915 +00:00 [ERR] - ### Error connecting to broker Re
source temporarily unavailable ###
<3> 2021-05-27 13:55:13.835 +00:00 [ERR] - ### Error connecting to broker No
route to host [::ffff:10.253.0.6]:1883 ###
```

*Figure 78: Container parameters*

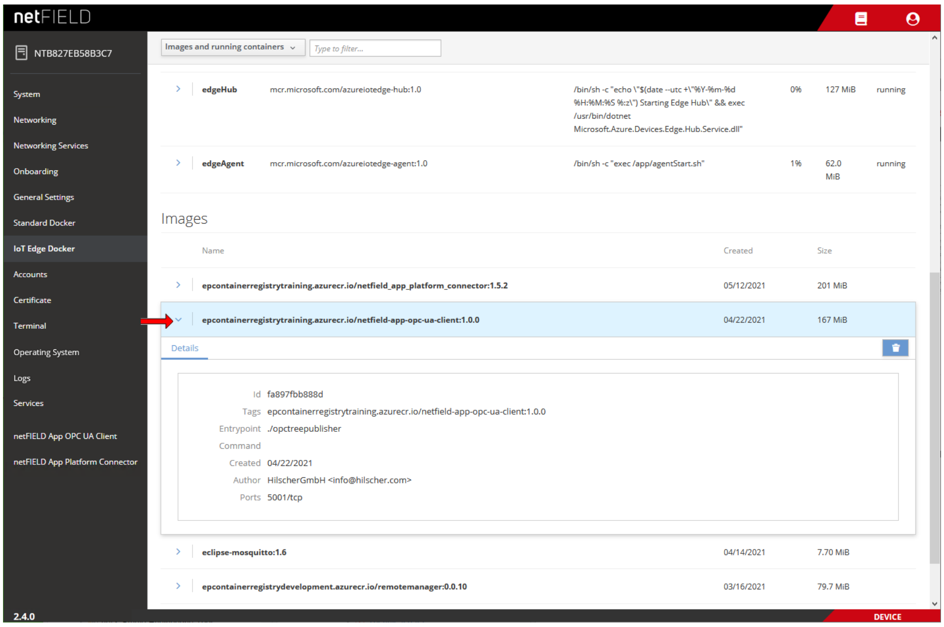
- ➢ To go back to the **IoT Edge Docker** overview page, click the blue **Show all containers** link in the page header.

## Images

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

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

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



| | | | | | |
|---|---|---|---|---|---|
| edgeHub | mcr.microsoft.com/azureiotedge-hub:1.0 | /bin/sh -c "echo \"$(date --utc +\"%Y-%m-%d %H:%M:%S %:z\") Starting Edge Hub\" && exec /usr/bin/dotnet Microsoft.Azure.Devices.Edge.Hub.Service.dll" | 0% | 127 MiB | running |
| edgeAgent | mcr.microsoft.com/azureiotedge-agent:1.0 | /bin/sh -c "exec /app/agentStart.sh" | 1% | 62.0 MiB | running |

Images

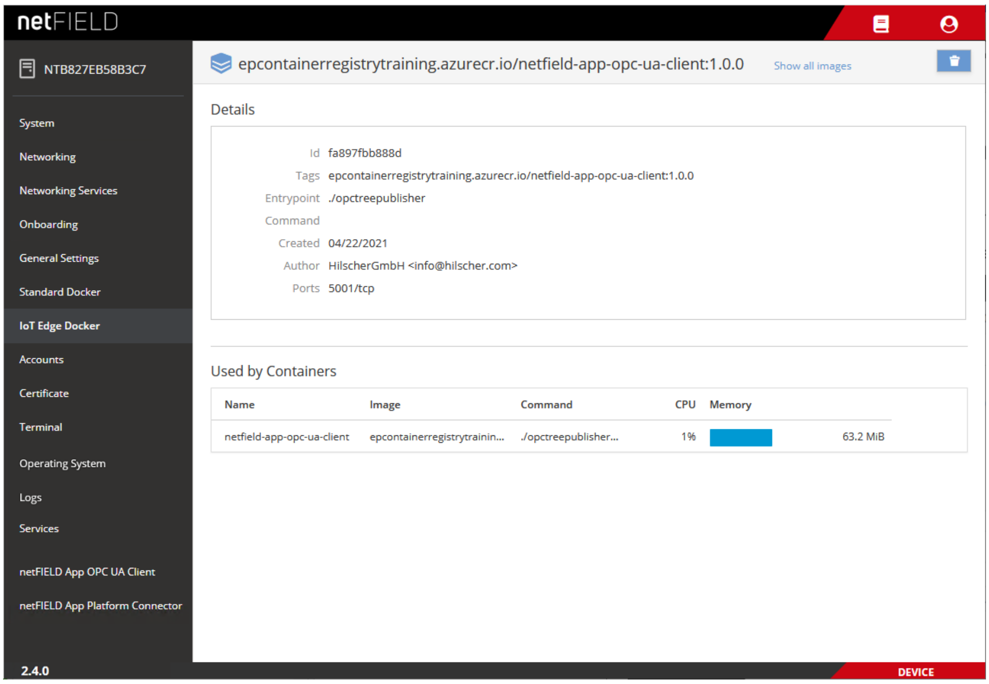
| Name | Created | Size |
|---|---|---|
| epcontainerregistrytraining.azurecr.io/netfield_app_platform_connector:1.5.2 | 05/12/2021 | 201 MiB |
| epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0 | 04/22/2021 | 167 MiB |
| eclipse-mosquitto:1.6 | 04/14/2021 | 7.70 MiB |
| epcontainerregistrydevelopment.azurecr.io/remotemanager:0.0.10 | 03/16/2021 | 79.7 MiB |

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

*Figure 79: IoT image expanded*

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

➯ A page featuring detailed information opens:



epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0

Details

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

Used by Containers

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

*Figure 80: Details of netFIELD Proxy image*

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

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

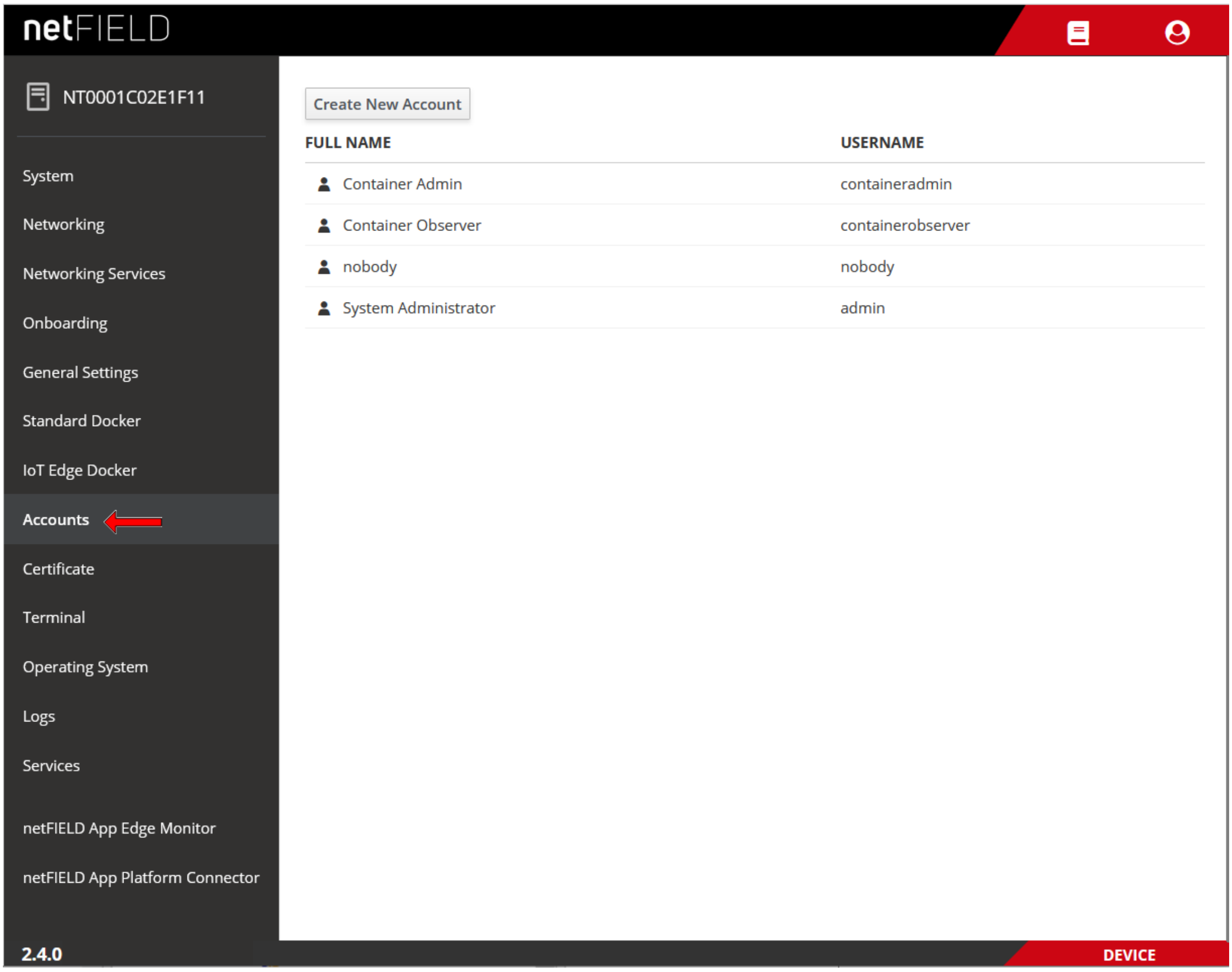
**Note:**
The IoT Edge Docker can also be managed (with the same limitations as in the UI) by using docker commands with the CLI in the Terminal.
See section *Useful CLI commands and parameters in Terminal* [▷ page 152] for examples.

## 6.9 Accounts

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

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

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

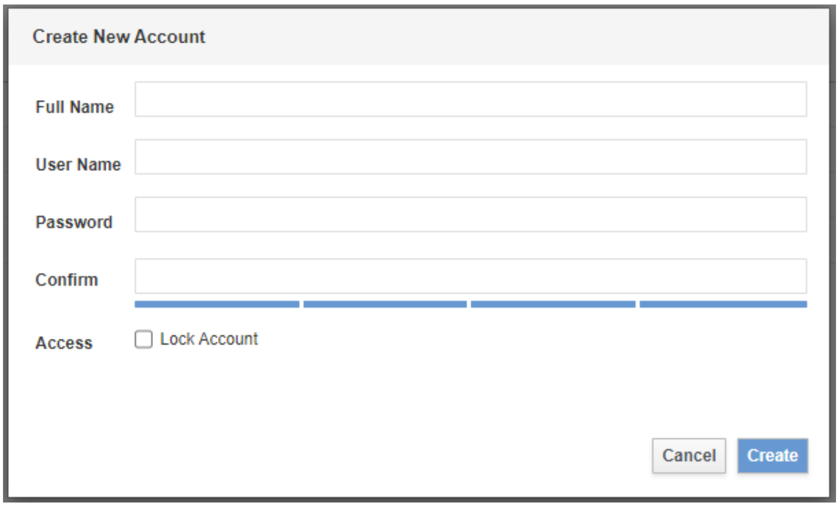


| FULL NAME | USERNAME |
|---|---|
| Container Admin | containeradmin |
| Container Observer | containerobserver |
| nobody | nobody |
| System Administrator | admin |

*Figure 81: Accounts*

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

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



Create New Account

Full Name

User Name

Password

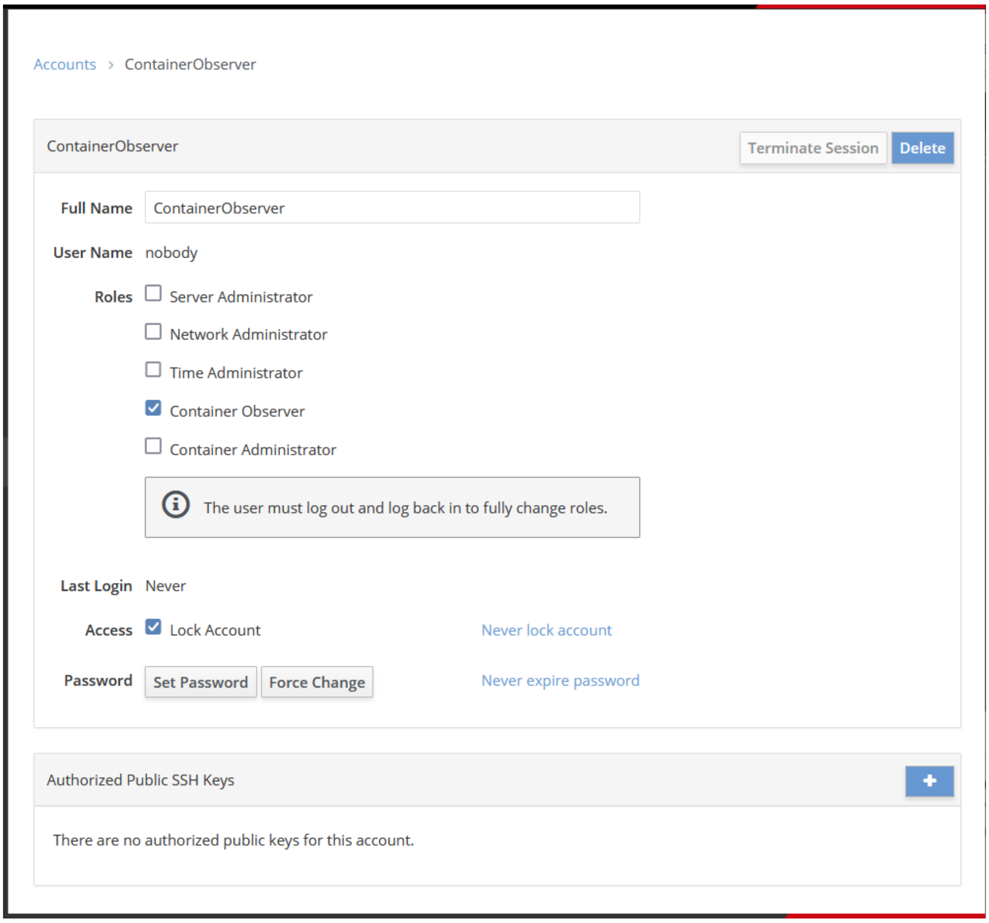
Confirm

Access □ Lock Account

*Figure 82: Create new account*

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

⮊ The configuration dialog for the account opens:



Full Name ContainerObserver

User Name nobody

Roles □ Server Administrator
□ Network Administrator
□ Time Administrator
☑ Container Observer
□ Container Administrator

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

Last Login Never

Access ☑ Lock Account

There are no authorized public keys for this account.

*Figure 83: Edit account*

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

### Roles

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

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

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

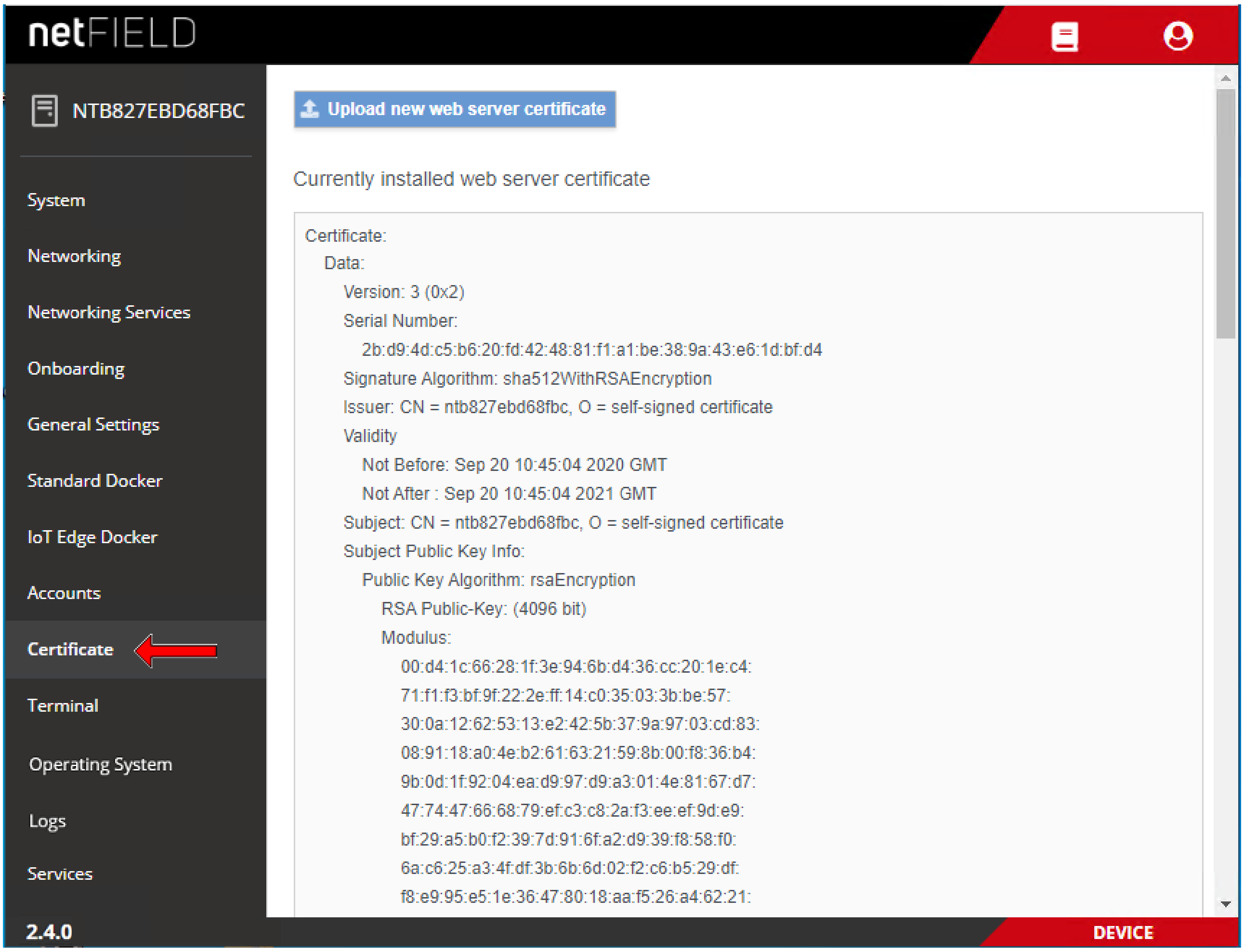
### Authorized Public SSH Keys

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

➢ Click on the ➕ button to add an SSH key.

## 6.10 Certificate

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



Currently installed web server certificate

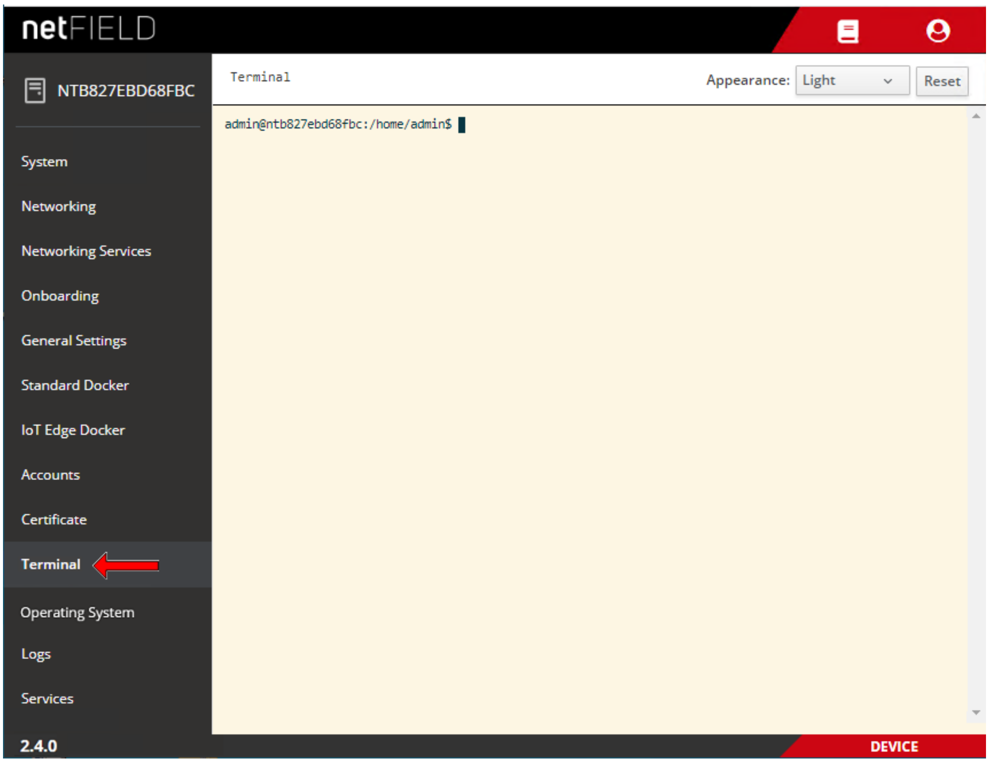
```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2b:d9:4d:c5:b6:20:fd:42:48:81:f1:a1:be:38:9a:43:e6:1d:bf:d4
    Signature Algorithm: sha512WithRSAEncryption
    Issuer: CN = ntb827ebd68fbc, O = self-signed certificate
    Validity
      Not Before: Sep 20 10:45:04 2020 GMT
      Not After : Sep 20 10:45:04 2021 GMT
    Subject: CN = ntb827ebd68fbc, O = self-signed certificate
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        RSA Public-Key: (4096 bit)
        Modulus:
          00:d4:1c:66:28:1f:3e:94:6b:d4:36:cc:20:1e:c4:
          71:f1:f3:bf:9f:22:2e:ff:14:c0:35:03:3b:be:57:
          30:0a:12:62:53:13:e2:42:5b:37:9a:97:03:cd:83:
          08:91:18:a0:4e:b2:61:63:21:59:8b:00:f8:36:b4:
          9b:0d:1f:92:04:ea:d9:97:d9:a3:01:4e:81:67:d7:
          47:74:47:66:68:79:ef:c3:c8:2a:f3:ee:ef:9d:e9:
          bf:29:a5:b0:f2:39:7d:91:6f:a2:d9:39:f8:58:f0:
          6a:c6:25:a3:4f:df:3b:6b:6d:02:f2:c6:b5:29:df:
          f8:e9:95:e5:1e:36:47:80:18:aa:f5:26:a4:62:21:
```

*Figure 84: Web Server Certificate page*

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

## 6.11 Terminal

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



```
admin@ntb827ebd68fbc:/home/admin$
```

*Figure 85: Terminal*

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

For working with root privileges in the CLI, use “`sudo`”.
Examples of commands and parameters are provided in section *Useful CLI commands and parameters in Terminal* [▸ page 152].

# 6.12 Operating System

## 6.12.1 OS Update

The **OS Update** tab of the **Operating System** page of the Local Device Manager allows you to update the netFIELD operating system (netFIELD OS) by uploading an `swu` update file.
You can also perform an OS “Recovery” here by uploading a recovery image (also in `swu` format) instead of an update file.

! **Important:**
Be aware of the difference between an OS *update* and a *recovery*:
In an *update*, bug fixes and/or new functions will be added to the existing netFIELD OS. Your device’s configuration settings, containers, user accounts, passwords and its cloud registration (“onboarding”) will thereby be preserved.
In a *recovery*, the currently installed OS and all its settings will be fully replaced by the new recovery image, which means that individual configurations settings, containers, user accounts and passwords will be lost. After a *recovery*, you will have to reconfigure and “onboard” your device again. In this respect, the recovery is like the factory reset (see section *Factory Reset* [▸ page 137]), with the difference that the recovery process uses a completely new OS version, whereas the factory reset restores the “pristine” state of the currently installed OS version (by deleting all user configurations).
Note that if you cannot connect to the netFIELD OS via Ethernet (e.g. because you have locked yourself out), you can perform a device recovery via USB, as described in section *Device recovery via USB* [▸ page 143].

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

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

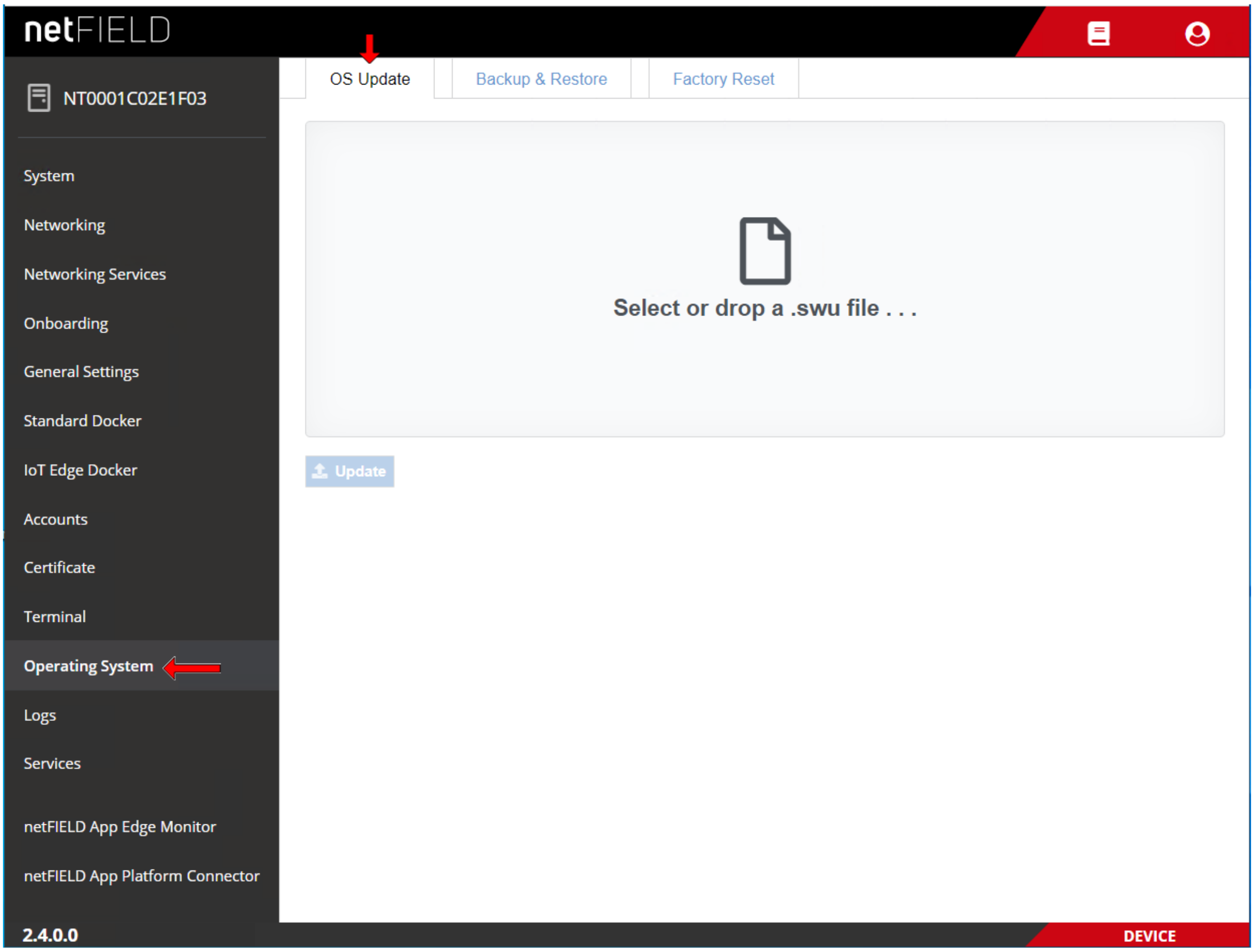


*Figure 86: OS update page*

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

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

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

1. Download the update file (or recovery file) from Hilscher to your local PC.

   ➢ Go to the **netFIELD OS Version history** page
   [https://hilscher.atlassian.net/l/cp/SBeH8aq2](https://hilscher.atlassian.net/l/cp/SBeH8aq2)
   and click on the link under **Current version**.
   On the **netFIELD OS Version [x.x]** page, scroll down to the **Downloads - netFIELD OS Edge** table and look for the **Model Name** *NIOT-E-TIJCX-GB-RE/NFLD*. Download the `[...].update.swu` file that is linked under **Update via device's Web UI**.
   (Note: If you want to perform a "recovery", download the `[...].recovery.swu` file that is linked under **Recovery with factory reset via device's Web UI**.)

2. Upload the `*.swu` file from your local PC to the device.

   ➢ On the **System Update** page, simply drag and drop the `*.swu` file from your local PC onto the **Select or drop a .swu file...** field, or click into the field to open a file selection dialog.

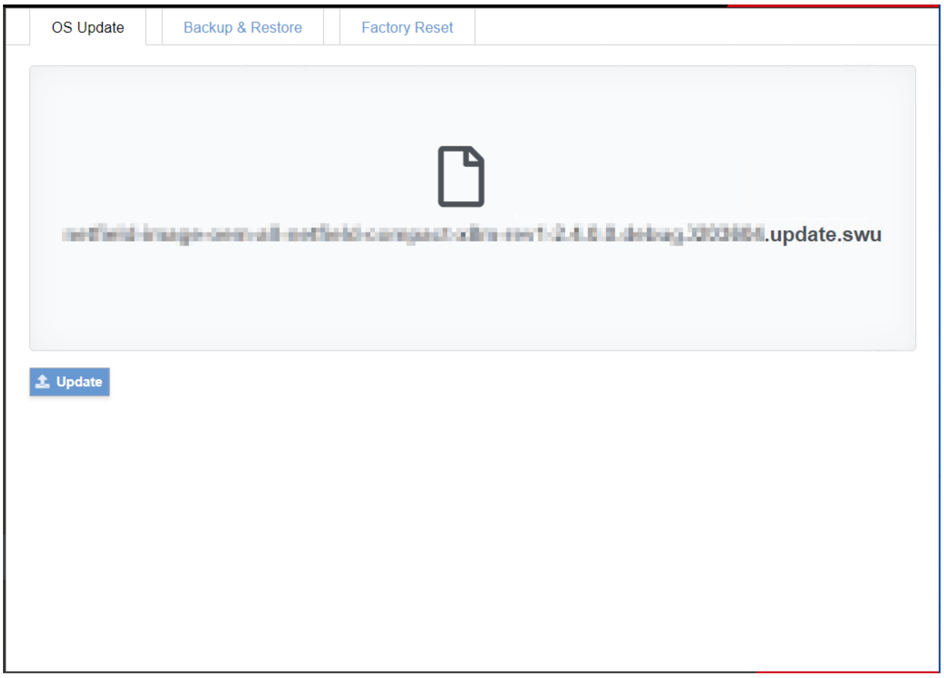
   

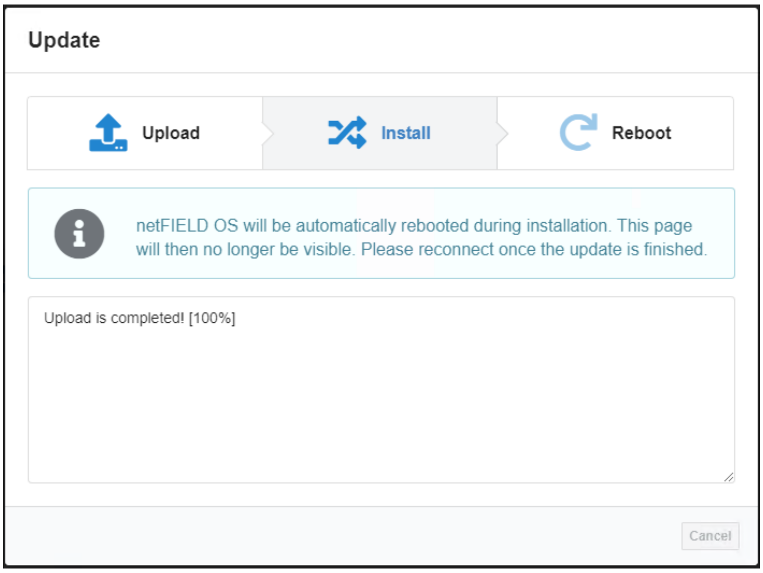
   *Figure 87: Selected OS update image*

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

   ➯ The **Confirmation** dialog appears.

   ➢ Because the update process cannot be aborted after confirmation, you should now check carefully whether you have selected the right update file (and not a recovery file for instance, which would delete all your configuration settings and containers).
   Click **Yes** if you want to start the update.

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



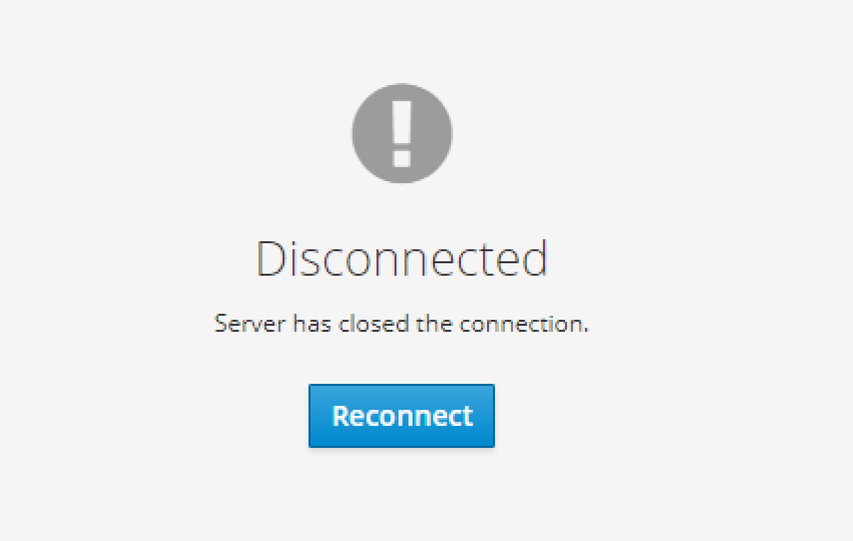
netFIELD OS will be automatically rebooted during installation. This page will then no longer be visible. Please reconnect once the update is finished.

Upload is completed! [100%]

*Figure 88: Upload finished message*

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

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



Disconnected

Server has closed the connection.

*Figure 89: OS update “Disconnected” message*

➢ Click **Reconnect** button.

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

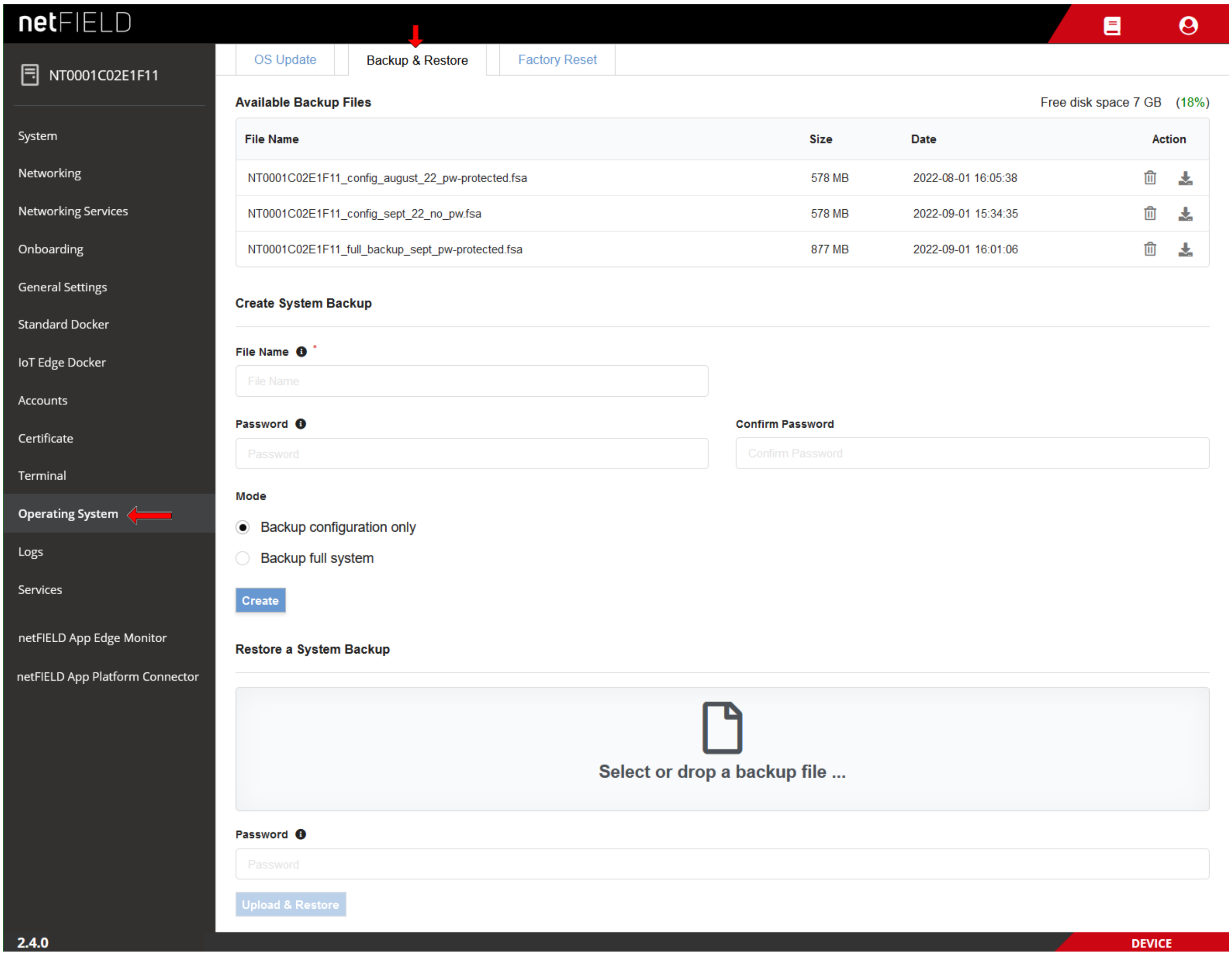
**Note:**
If you have performed a *recovery* (by uploading and installing a recovery image) instead of an *update*, all configuration settings have been deleted, and you now must commission the device again (see chapter *Commissioning and first steps* [▸ page 26]).

## 6.12.2 Backup & Restore

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

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

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



**Available Backup Files** Free disk space 7 GB (18%)

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

**Create System Backup**

File Name *: File Name

Password: Password

Confirm Password: Confirm Password

Mode

● Backup configuration only

○ Backup full system

Create

**Restore a System Backup**

Select or drop a backup file ...

Password: Password

Upload & Restore

*Figure 90: Backup and Restore tab*

**NOTICE**

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

When restoring your device, make sure to use a backup file that was created for your *netFIELD OnPremise* hardware model.
Using a backup file that was made for a different netFIELD Edge Gateway model can damage your device.

| Element | | Description | |
|---|---|---|---|
| Available Backup Files | The table displays the backup files that have already been created. | | |
| | File Name | Name of the backup file. | |
| | Size | Size of the backup file. | |
| | Date | Date and time of the creation of the backup file. | |
| | Action | 🗑 | Delete backup file. |
| | | ⤓ | Download backup file. |
| Free disk space | Indicates the available space for storing backup files on the device (designated backup partition). The green value in brackets shows the percentage of the designated backup space that is already consumed. | | |
| Create System Backup | Create here new backup files. | | |
| | File Name | Enter here a name for the backup file that you want to create.<br>**Note**: The name must end with the suffix `.fsa`<br>Blank spaces and special characters are not allowed. We recommend you to use a “telling” name, indicating a device ID and the backup type, e.g. `NT0002A233E553_full_backup_august_2022_pw-protected.fsa` | |
| | Password | Enter here a password if you want to encrypt and protect the backup file with a password.<br>**Note**: In this case, you will have to provide the same password again when you are restoring your system with the backup file. | |
| | Confirm Password | Re-enter here your password. | |
| | Mode | Select here the backup type. | |
| | | Backup configuration only | This option saves all user-made settings and application data of your netFIELD Edge Gateway, including<br>• Docker containers<br>• User accounts<br>• Network settings<br>• Onboarding<br>• Log files |
| | | Backup full system | This option saves all user-made settings and application data plus the currently installed netFIELD OS itself. |
| | Create | Click here to create the backup file. | |

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

*Table 31: Elements in Backup & Restore tab*

**Note:**

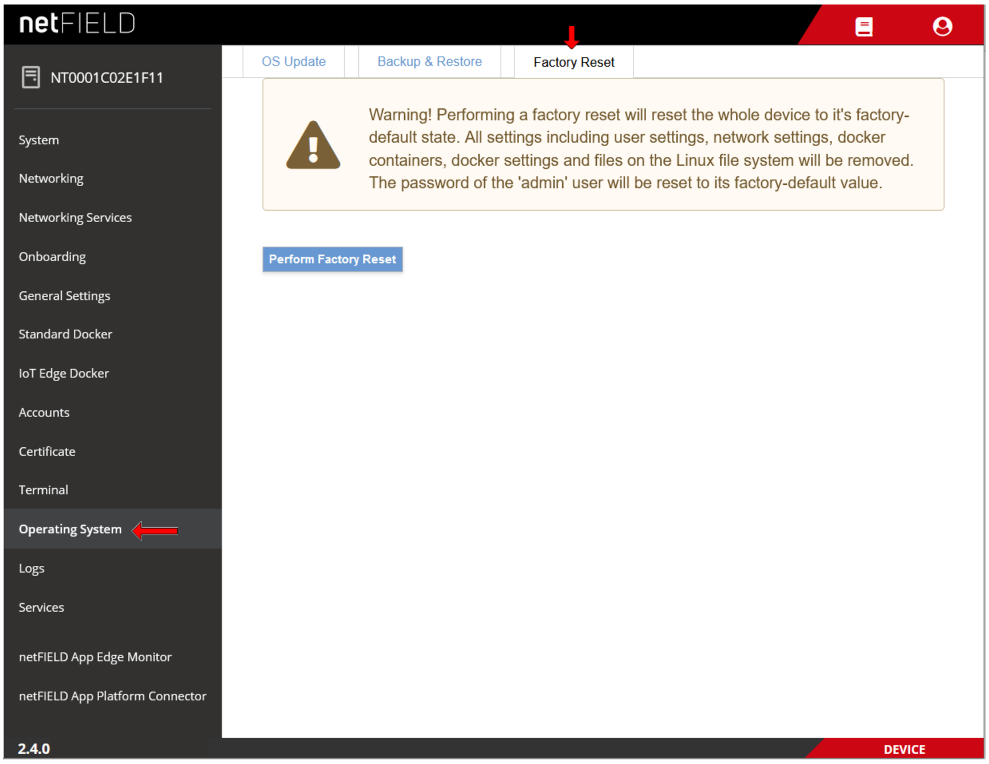
If you cannot connect to the netFIELD OS via Ethernet (e.g. because you have locked yourself out), you can perform a device recovery via USB, as described in section *Device recovery via USB* [▸ page 143].

### 6.12.3 Factory Reset

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

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

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



Warning! Performing a factory reset will reset the whole device to it's factory-default state. All settings including user settings, network settings, docker containers, docker settings and files on the Linux file system will be removed. The password of the 'admin' user will be reset to its factory-default value.

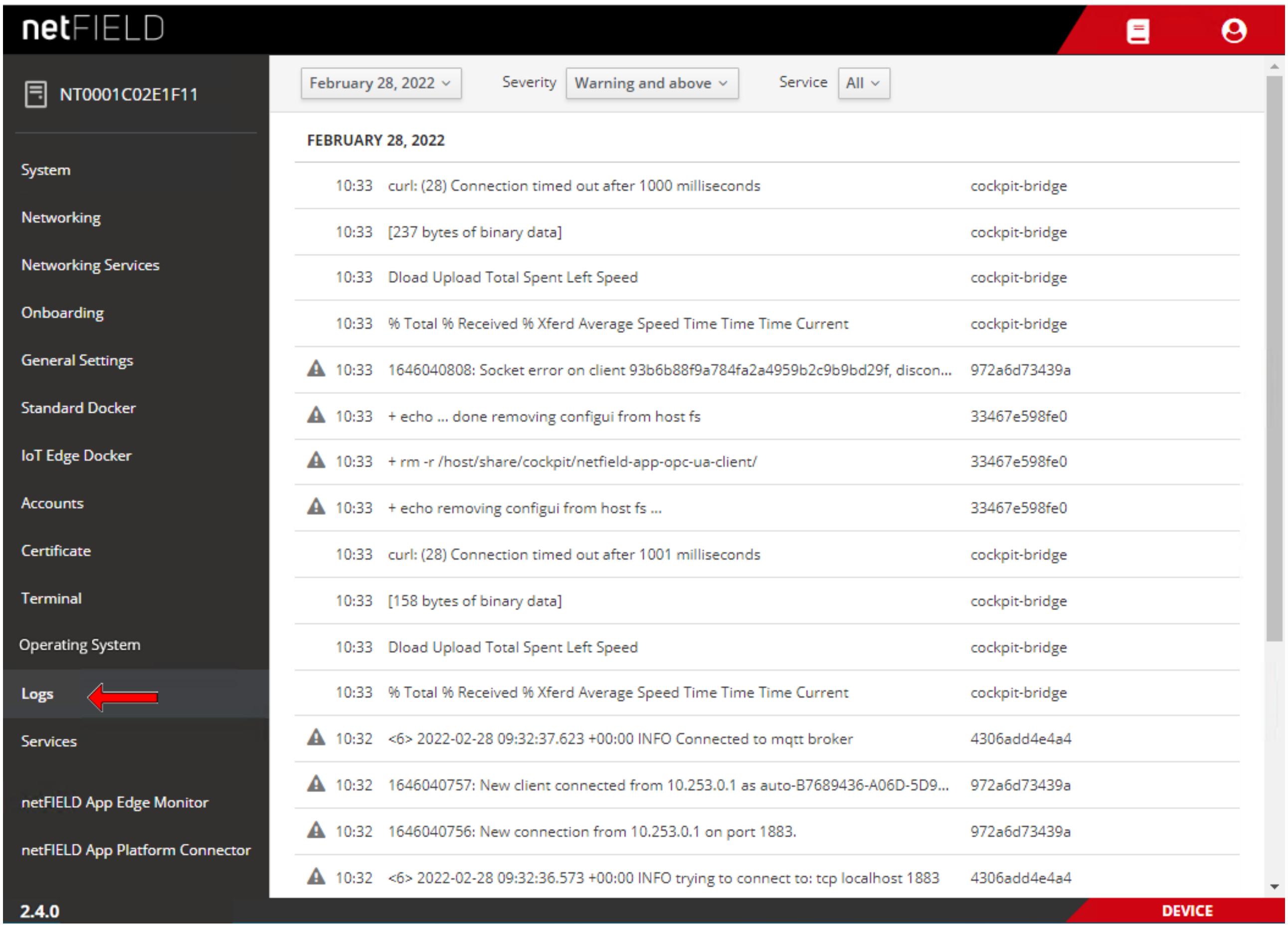
*Figure 91: Factory Reset*

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

## 6.13 Logs

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

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



February 28, 2022 | Severity: Warning and above | Service: All

FEBRUARY 28, 2022

```
   10:33  curl: (28) Connection timed out after 1000 milliseconds                             cockpit-bridge
   10:33  [237 bytes of binary data]                                                          cockpit-bridge
   10:33  Dload Upload Total Spent Left Speed                                                 cockpit-bridge
   10:33  % Total % Received % Xferd Average Speed Time Time Time Current                     cockpit-bridge
⚠  10:33  1646040808: Socket error on client 93b6b88f9a784fa2a4959b2c9b9bd29f, discon...     972a6d73439a
⚠  10:33  + echo ... done removing configui from host fs                                      33467e598fe0
⚠  10:33  + rm -r /host/share/cockpit/netfield-app-opc-ua-client/                             33467e598fe0
⚠  10:33  + echo removing configui from host fs ...                                           33467e598fe0
   10:33  curl: (28) Connection timed out after 1001 milliseconds                             cockpit-bridge
   10:33  [158 bytes of binary data]                                                          cockpit-bridge
   10:33  Dload Upload Total Spent Left Speed                                                 cockpit-bridge
   10:33  % Total % Received % Xferd Average Speed Time Time Time Current                     cockpit-bridge
⚠  10:32  <6> 2022-02-28 09:32:37.623 +00:00 INFO Connected to mqtt broker                    4306add4e4a4
⚠  10:32  1646040757: New client connected from 10.253.0.1 as auto-B7689436-A06D-5D9...      972a6d73439a
⚠  10:32  1646040756: New connection from 10.253.0.1 on port 1883.                            972a6d73439a
⚠  10:32  <6> 2022-02-28 09:32:36.573 +00:00 INFO trying to connect to: tcp localhost 1883   4306add4e4a4
```

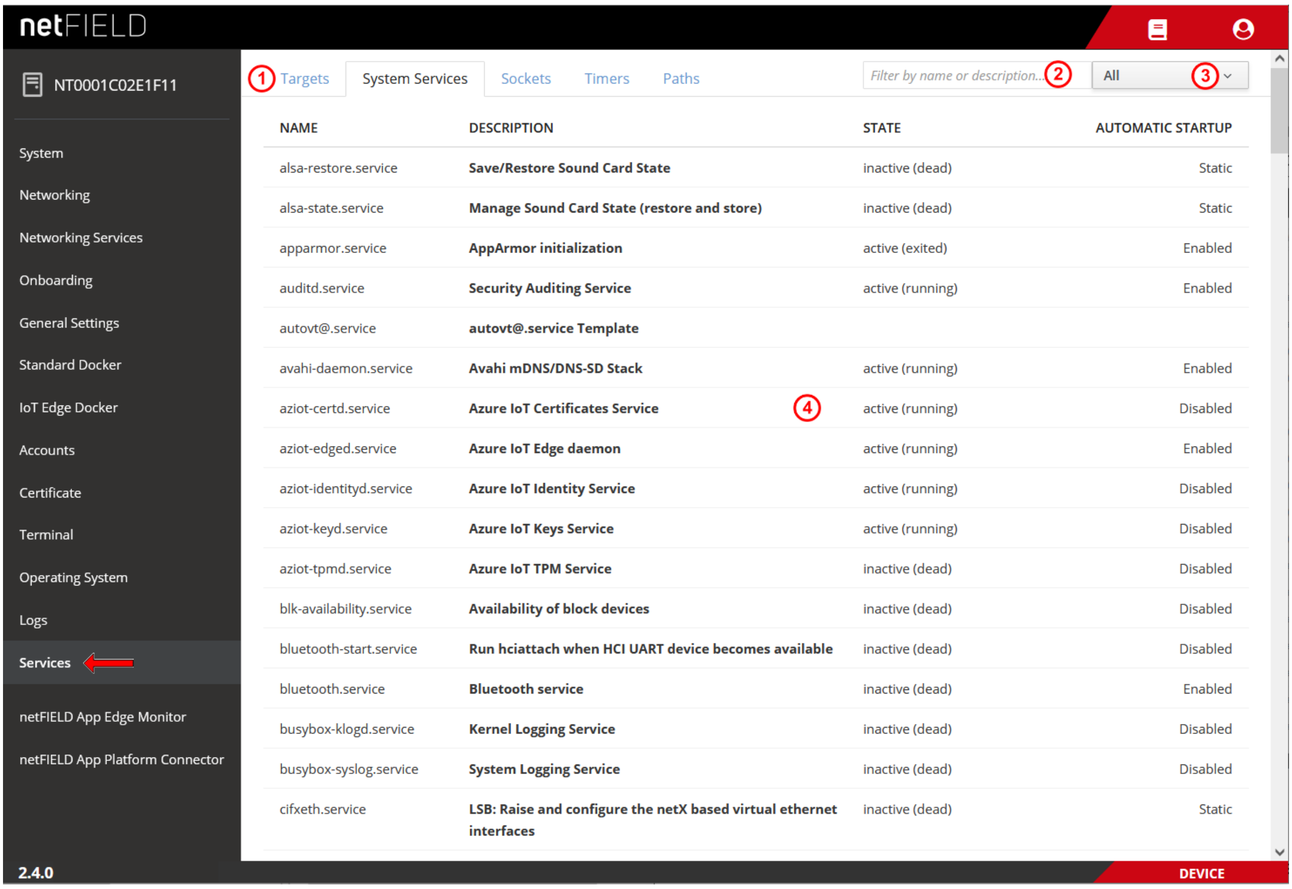
*Figure 92: Logs*

## 6.14 Services

### Overview

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

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



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

*Figure 93: Services page*

(1) Click the tabs in the header to select a service type.

(2) In the filter field, you can perform a text search for name and description of a service.
To remove the filter, delete the text in the field.

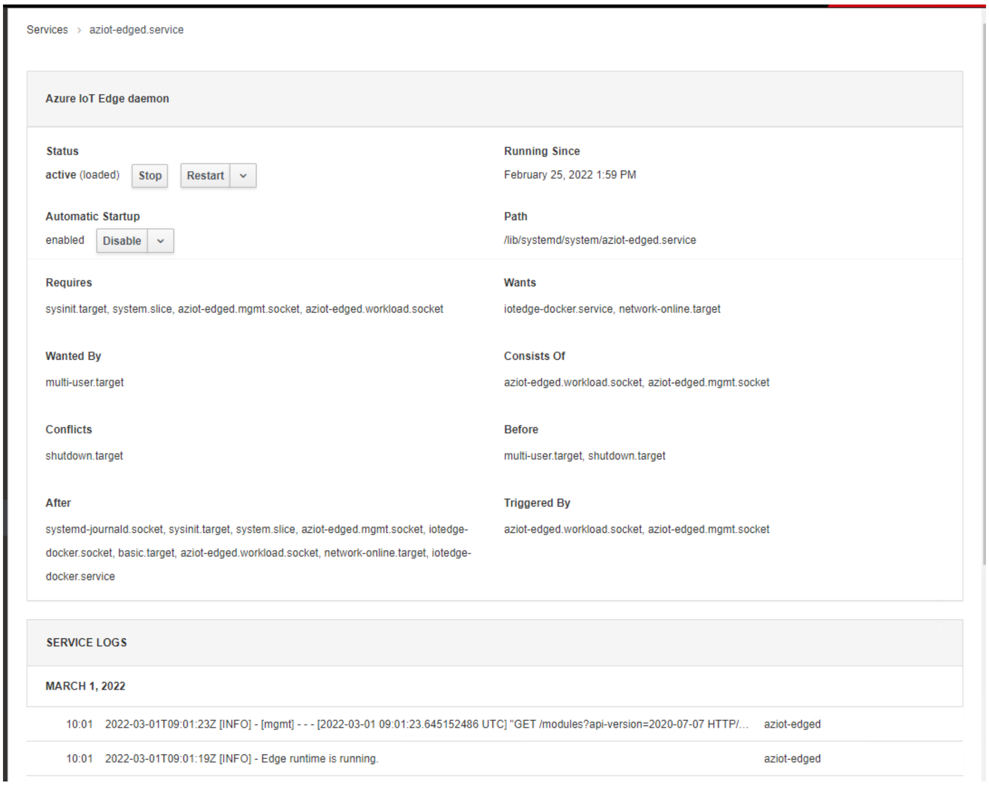
(3) In the drop-down list, you can filter the services by their automatic startup setting; i.e. **Static**, **Enabled** and **Disabled**.

(4) List of services showing their current states and automatic startup settings.

### Service details/settings page

➢ Click on a service in the list to display further information (including the service logs) and/or to change its running state or startup settings.

⮱ The details/settings page of the service opens:



Azure IoT Edge daemon

**Status**
active (loaded)

**Running Since**
February 25, 2022 1:59 PM

**Automatic Startup**
enabled

**Path**
/lib/systemd/system/aziot-edged.service

**Requires**
sysinit.target, system.slice, aziot-edged.mgmt.socket, aziot-edged.workload.socket

**Wants**
iotedge-docker.service, network-online.target

**Wanted By**
multi-user.target

**Consists Of**
aziot-edged.workload.socket, aziot-edged.mgmt.socket

**Conflicts**
shutdown.target

**Before**
multi-user.target, shutdown.target

**After**
systemd-journald.socket, sysinit.target, system.slice, aziot-edged.mgmt.socket, iotedge-docker.socket, basic.target, aziot-edged.workload.socket, network-online.target, iotedge-docker.service

**Triggered By**
aziot-edged.workload.socket, aziot-edged.mgmt.socket

SERVICE LOGS

MARCH 1, 2022

```
10:01   2022-03-01T09:01:23Z [INFO] - [mgmt] - - - [2022-03-01 09:01:23.645152486 UTC] "GET /modules?api-version=2020-07-07 HTTP/...   aziot-edged
10:01   2022-03-01T09:01:19Z [INFO] - Edge runtime is running.                                                                     aziot-edged
```

*Figure 94: Service details and settings page*

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

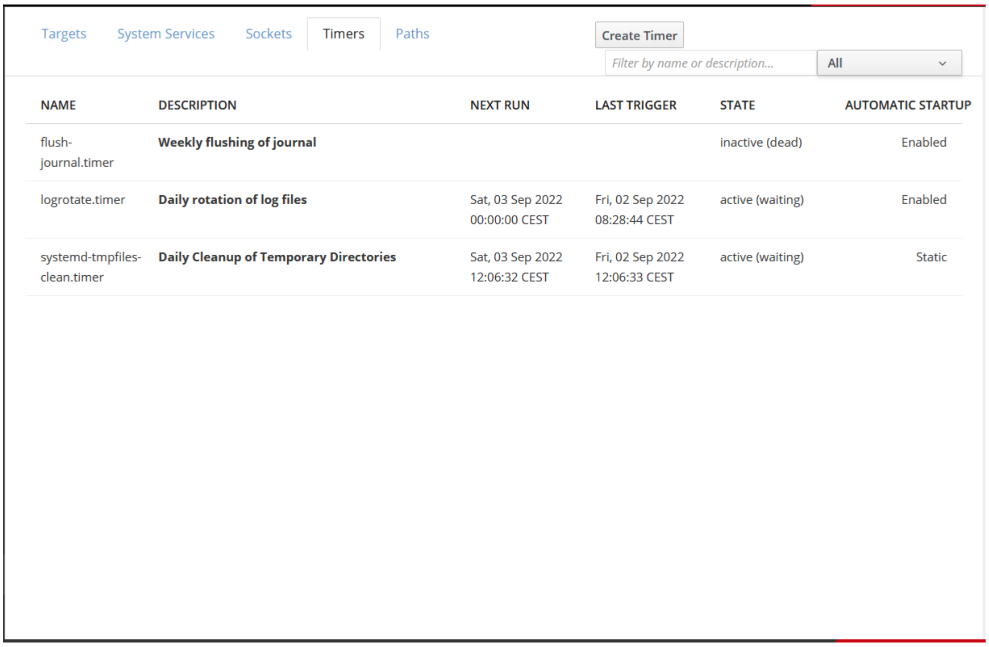
The drop-down button in the **Automatic Startup** section allows you to configure the startup behavior of the service like e.g. “masking“ it in order to prevent the service from running.

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

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

### Managing Timers

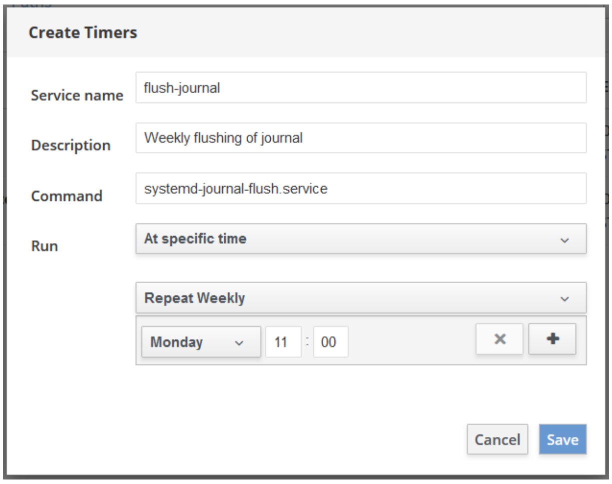
On the **Timers** tab, you can display existing timers and create new timer units. A timer allows you to execute a certain command at a certain time.



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

*Figure 95: Service types: Timers*

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


**Create Timers**

Service name: flush-journal

Description: Weekly flushing of journal

Command: systemd-journal-flush.service

Run: At specific time

Repeat Weekly

Monday 11 : 00

*Figure 96: Create timer dialog*

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

**Note:**
Note that you can create but cannot delete timers here. (You can however stop a timer here by opening its details/settings page, then clicking the **Stop** button in the **Status** section).
To remove a timer completely, you have to use the **Terminal** to delete it manually in the corresponding `systemd` configuration.

# 7 Good to know...

## 7.1 Device recovery via USB

### 7.1.1 Overview

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

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

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

### 7.1.2 Requirements

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

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

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

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

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

### 7.1.3 Step-by-step instructions

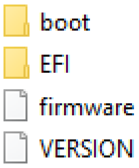
1. Download the zip archive containing the recovery image from Hilscher to your local PC and unpack it.

➢ Go to the **netFIELD OS Version history** page
[https://hilscher.atlassian.net/l/cp/SBeH8aq2](https://hilscher.atlassian.net/l/cp/SBeH8aq2)
and click on the link under **Current version**.
On the **netFIELD OS Version [x.x]** page, scroll down to the **Downloads - netFIELD OS Edge** table.

➢ Look for the **Model Name** *NIOT-E-TIJCX-GB-RE/NFLD* and download the `[...].recovery.zip` file that is linked under **Recovery/Upgrade with factory reset via USB memory stick**.

➢ Use a tool like **7-Zip** to unpack the downloaded zip archive on your local PC.

➯ The unpacked folder contains the following folders and files, which you will later have to copy onto the USB stick (after having formatted the stick):



boot
EFI
firmware
VERSION

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.

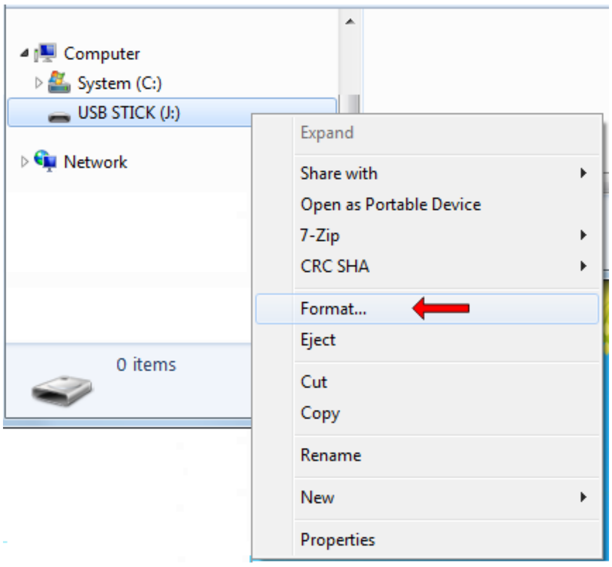
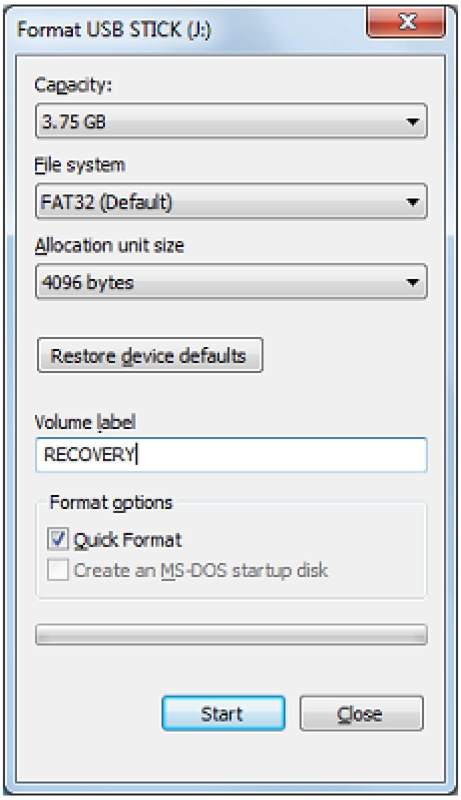


*Figure 97: Formatting USB stick*

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



Format USB STICK (J:)

Capacity: 3.75 GB

File system: FAT32 (Default)

Allocation unit size: 4096 bytes

Volume label: RECOVERY

Format options

☑ Quick Format

□ Create an MS-DOS startup disk

*Figure 98: 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”.

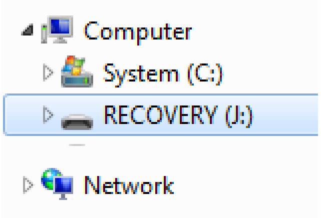


*Figure 99: Formatted USB stick*

3. Copy recovery files onto the USB stick.

   ➢ Open the unpacked `recovery` archive folder and copy the `boot` and `efi` folders and the `firmware` and `VERSION` files onto the USB stick.

   ➪ The USB stick with the copied firmware image must now feature the following elements:

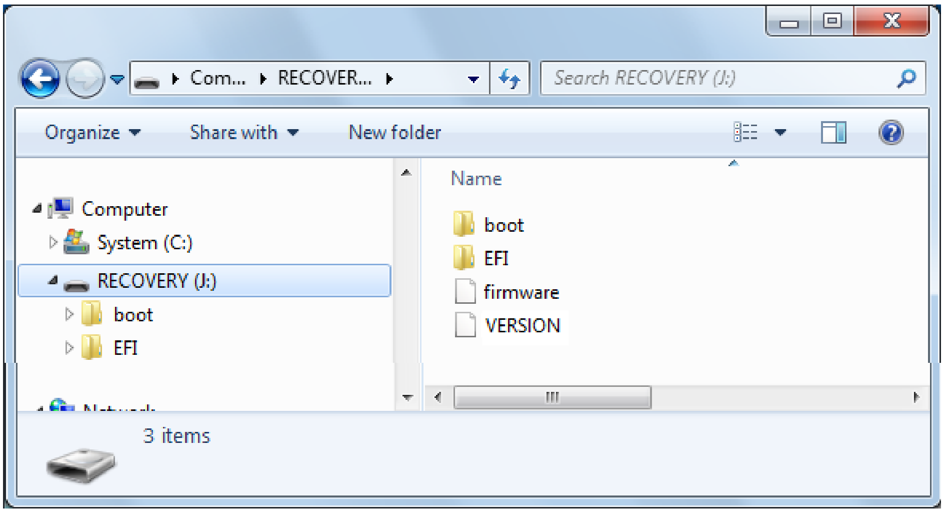


*Figure 100: Prepared USB stick*

   ➢ Remove the USB stick from your Windows PC.

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

4. Prepare netFIELD OnPremise device

   ➢ Make sure that the device is switched off (the green Status LED below ⏻ indicating power must be dark).

   ➢ Connect the USB keyboard with one of the USB sockets of the device (for the positions of the USB sockets, see section *Positions of the interfaces* [▹ page 16]).

   ➢ Connect the monitor with the DVI-I socket (see position (3) in section *Positions of the interfaces* [▹ page 16]) or with the DP socket (see Position (4)) [according to your monitor type].

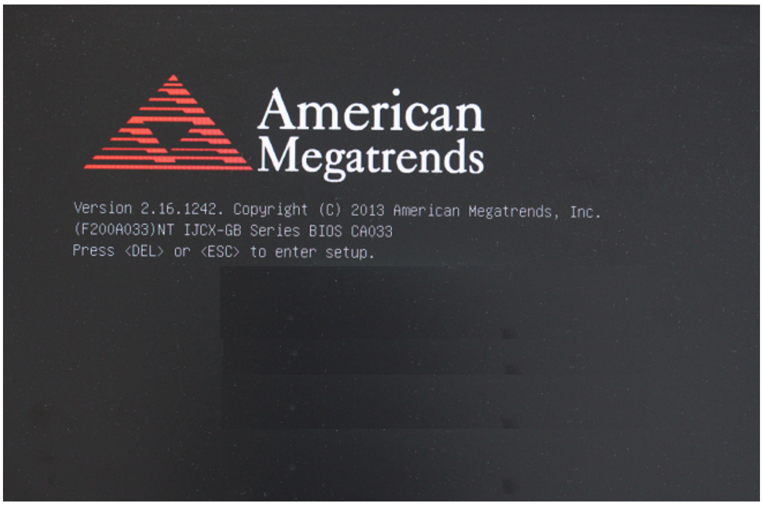
**Important:**
Use only 1:1 DVI or DP connectors. Adapters like DVI-I to VGA or DP to VGA are not supported by the device.

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

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

➢ Turn-on the device by pressing the power button (see position (12) in section *Positions of the interfaces* [▸ page 16]).

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



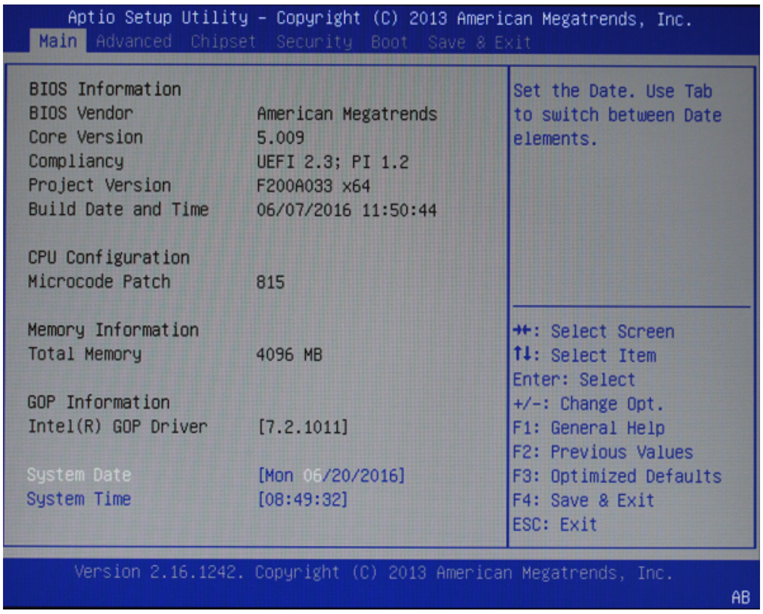
```
Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
(F200A033)NT IJCX-GB Series BIOS CA033
Press <DEL> or <ESC> to enter setup.
```

*Figure 101: 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.

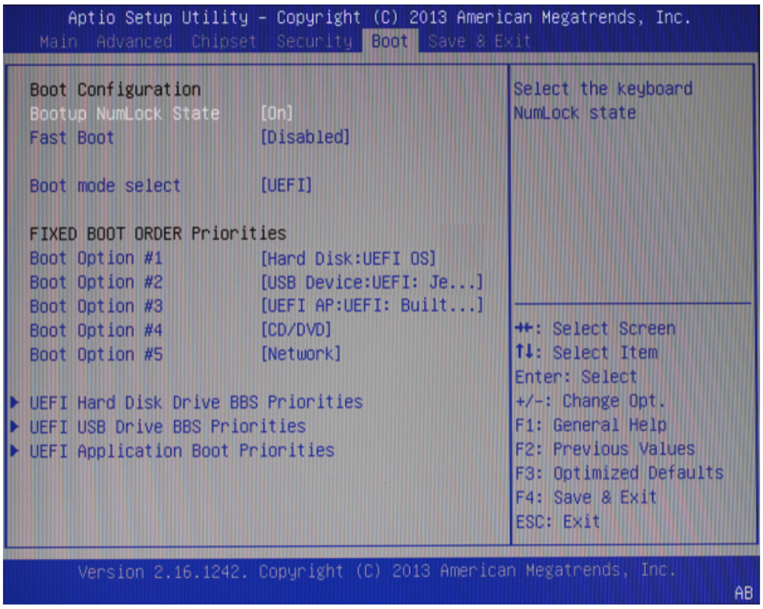
➪ The BIOS setup menu opens:



```
      Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
   Main  Advanced  Chipset  Security  Boot  Save & Exit

  BIOS Information                                         Set the Date. Use Tab
  BIOS Vendor             American Megatrends              to switch between Date
  Core Version            5.009                            elements.
  Compliancy              UEFI 2.3; PI 1.2
  Project Version         F200A033 x64
  Build Date and Time     06/07/2016 11:50:44

  CPU Configuration
  Microcode Patch         815

  Memory Information                                       →←: Select Screen
  Total Memory            4096 MB                          ↑↓: Select Item
                                                           Enter: Select
  GOP Information                                          +/-: Change Opt.
  Intel(R) GOP Driver     [7.2.1011]                       F1: General Help
                                                           F2: Previous Values
  System Date             [Mon 06/20/2016]                 F3: Optimized Defaults
  System Time             [08:49:32]                       F4: Save & Exit
                                                           ESC: Exit

        Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                          AB
```

*Figure 102: BIOS setup menu*

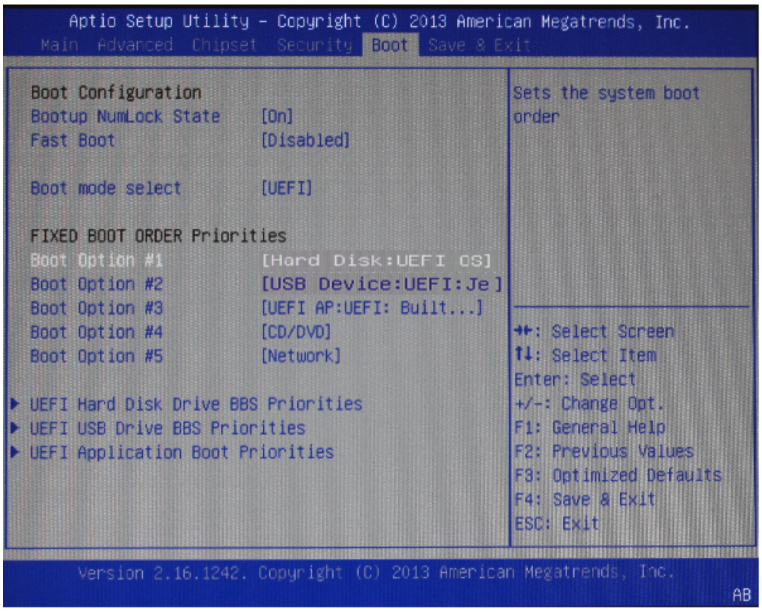
- ➢ In the main menu, use the right arrow key to navigate and open the **Boot** tab:



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.

Boot Configuration                                  Select the keyboard
Bootup NumLock State       [On]                     NumLock state
Fast Boot                  [Disabled]

Boot mode select           [UEFI]

FIXED BOOT ORDER Priorities
Boot Option #1             [Hard Disk:UEFI OS]
Boot Option #2             [USB Device:UEFI: Je...]
Boot Option #3             [UEFI AP:UEFI: Built...]
Boot Option #4             [CD/DVD]                 ↔: Select Screen
Boot Option #5             [Network]                ↑↓: Select Item
                                                    Enter: Select
▶ UEFI Hard Disk Drive BBS Priorities               +/-: Change Opt.
▶ UEFI USB Drive BBS Priorities                     F1: General Help
▶ UEFI Application Boot Priorities                  F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                  AB
```

*Figure 103: 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**.

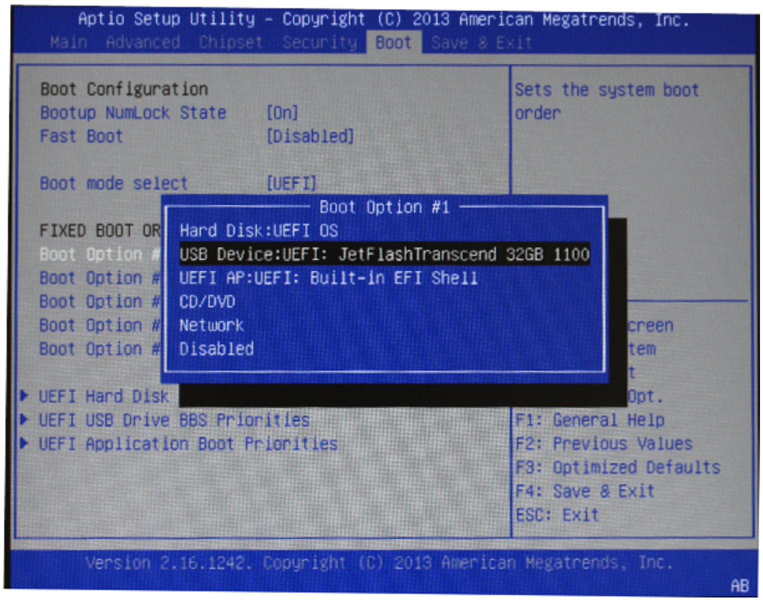


```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.

Boot Configuration                                  Sets the system boot
Bootup NumLock State       [On]                     order
Fast Boot                  [Disabled]

Boot mode select           [UEFI]

FIXED BOOT ORDER Priorities
Boot Option #1             [Hard Disk:UEFI OS]
Boot Option #2             [USB Device:UEFI:Je]
Boot Option #3             [UEFI AP:UEFI: Built...]
Boot Option #4             [CD/DVD]                 ↔: Select Screen
Boot Option #5             [Network]                ↑↓: Select Item
                                                    Enter: Select
▶ UEFI Hard Disk Drive BBS Priorities               +/-: Change Opt.
▶ UEFI USB Drive BBS Priorities                     F1: General Help
▶ UEFI Application Boot Priorities                  F2: Previous Values
                                                    F3: Optimized Defaults
                                                    F4: Save & Exit
                                                    ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                  AB
```

*Figure 104: Boot option #1 in BIOS setup menu*

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

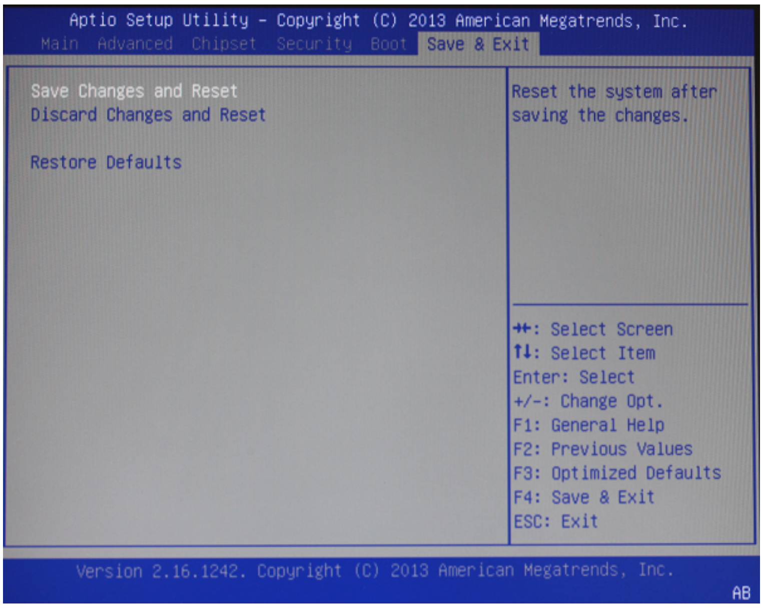
- ➢ Use the downwards arrow key to select **USB Device:UEFI: [Name of your USB stick]**:



```
         Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

 Boot Configuration                               Sets the system boot
 Bootup NumLock State        [On]                 order
 Fast Boot                   [Disabled]

 Boot mode select            [UEFI]
                     ──── Boot Option #1 ────
 FIXED BOOT OR  Hard Disk:UEFI OS
 Boot Option #  USB Device:UEFI: JetFlashTranscend 32GB 1100
 Boot Option #  UEFI AP:UEFI: Built-in EFI Shell
 Boot Option #  CD/DVD
 Boot Option #  Network                                creen
 Boot Option #  Disabled                               tem
                                                       t
▶ UEFI Hard Disk                                       Opt.
▶ UEFI USB Drive BBS Priorities                   F1: General Help
▶ UEFI Application Boot Priorities                F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit

         Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                        AB
```

*Figure 105: 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.



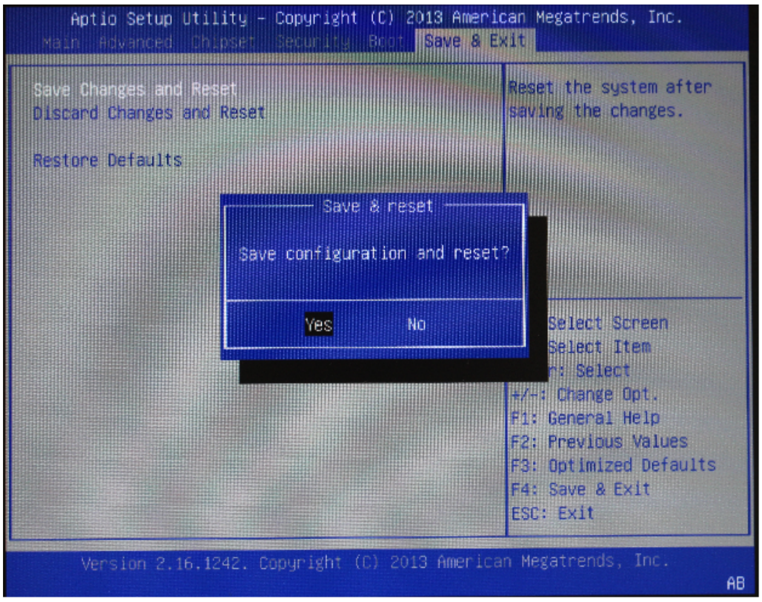
```
         Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
    Main  Advanced  Chipset  Security  Boot  Save & Exit

 Save Changes and Reset                           Reset the system after
 Discard Changes and Reset                        saving the changes.

 Restore Defaults




                                                  →←: Select Screen
                                                  ↑↓: Select Item
                                                  Enter: Select
                                                  +/-: Change Opt.
                                                  F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit

         Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                        AB
```

*Figure 106: Save & Exit tab*

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

6. Restart booting (reset).

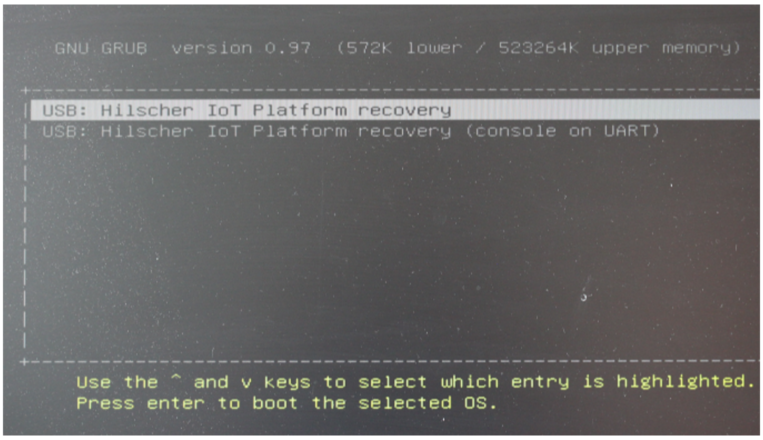
➢ In the **Save & reset** security window, select **Yes**, then press **Enter** key.



```
Aptio Setup Utility - Copyright (C) 2013 American Megatrends, Inc.
Main  Advanced  Chipset  Security  Boot  Save & Exit

Save Changes and Reset                          Reset the system after
Discard Changes and Reset                       saving the changes.

Restore Defaults
                    Save & reset
          Save configuration and reset?

              Yes            No
                                                 Select Screen
                                                 Select Item
                                                 : Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

Version 2.16.1242. Copyright (C) 2013 American Megatrends, Inc.
                                                                 AB
```

*Figure 107: Save & Reset security question*

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

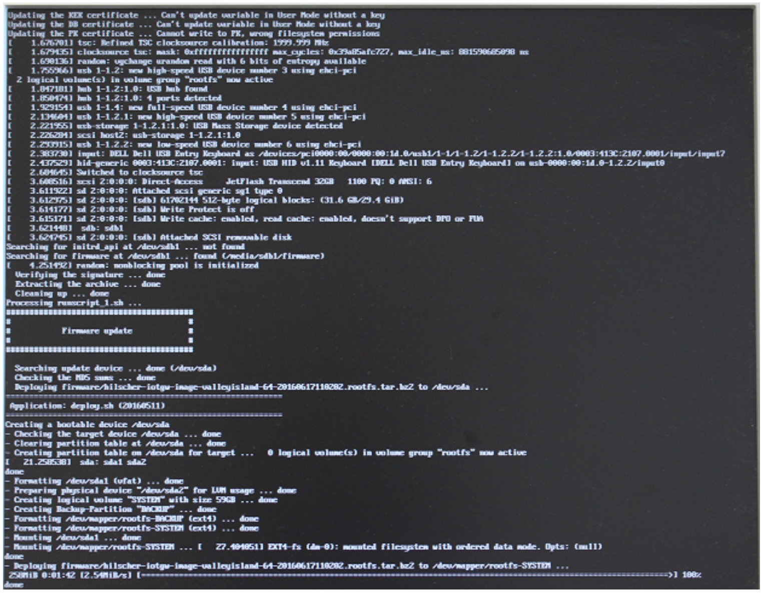


```
GNU GRUB  version 0.97  (572K lower / 523264K upper memory)

 USB: Hilscher IoT Platform recovery
 USB: Hilscher IoT Platform recovery (console on UART)

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS.
```

*Figure 108: Boot options question*

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

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



```
Updating the KEK certificate ... Can't update variable in User Mode without a key
Updating the DB certificate ... Can't update variable in User Mode without a key
Updating the PK certificate ... Cannot write to PK, wrong filesystem permissions
[    1.676701] tsc: Refined TSC clocksource calibration: 1999.999 MHz
[    1.679435] clocksource tsc: mask: 0xffffffffffffffff max_cycles: 0x39a85afc727, max_idle_ns: 881590685098 ns
[    1.690136] random: ugchange urandom read with 6 bits of entropy available
[    1.755966] usb 1-1.2: new high-speed USB device number 3 using ehci-pci
  2 logical volume(s) in volume group "rootfs" now active
[    1.847181] hub 1-1.2:1.0: USB hub found
[    1.850474] hub 1-1.2:1.0: 4 ports detected
[    1.929154] usb 1-1.4: new full-speed USB device number 4 using ehci-pci
[    2.134604] usb 1-1.2.1: new high-speed USB device number 5 using ehci-pci
[    2.221955] usb-storage 1-1.2.1:1.0: USB Mass Storage device detected
[    2.226284] scsi host2: usb-storage 1-1.2.1:1.0
[    2.293915] usb 1-1.2.2: new low-speed USB device number 6 using ehci-pci
[    2.383730] input: DELL Dell USB Entry Keyboard as /devices/pci0000:00/0000:00:1d.0/usb1/1-1/1-1.2/1-1.2.2/1-1.2.2:1.0/0003:413C:2107.0001/input/input7
[    2.437529] hid-generic 0003:413C:2107.0001: input: USB HID v1.11 Keyboard [DELL Dell USB Entry Keyboard] on usb-0000:00:1d.0-1.2.2/input0
[    2.604645] Switched to clocksource tsc
[    3.608516] scsi 2:0:0:0: Direct-Access     JetFlash Transcend 32GB   1100 PQ: 0 ANSI: 6
[    3.611922] sd 2:0:0:0: Attached scsi generic sg1 type 0
[    3.612975] sd 2:0:0:0: [sdb] 61702144 512-byte logical blocks: (31.6 GB/29.4 GiB)
[    3.614177] sd 2:0:0:0: [sdb] Write Protect is off
[    3.615171] sd 2:0:0:0: [sdb] Write cache: enabled, read cache: enabled, doesn't support DPO or FUA
[    3.621440]  sdb: sdb1
[    3.624745] sd 2:0:0:0: [sdb] Attached SCSI removable disk
Searching for initrd_api at /dev/sdb1 ... not found
Searching for firmware at /dev/sdb1 ... found (/media/sdb1/firmware)
[    4.251492] random: nonblocking pool is initialized
  Verifying the signature ... done
  Extracting the archive ... done
  Cleaning up ... done
Processing runscript_1.sh ...
########################################
#                                      #
#           Firmware update            #
#                                      #
########################################

  Searching update device ... done (/dev/sda)
  Checking the MD5 sums ... done
  Deploying firmware/hilscher-iotgw-image-valleyisland-64-20160617110202.rootfs.tar.bz2 to /dev/sda ...
==============================================================
 Application: deploy.sh (20160511)
==============================================================
Creating a bootable device /dev/sda
- Checking the target device /dev/sda ... done
- Clearing partition table at /dev/sda ... done
- Creating partition table on /dev/sda for target ...   0 logical volume(s) in volume group "rootfs" now active
[   21.258538]  sda: sda1 sda2
done
- Formatting /dev/sda1 (vfat) ... done
- Preparing physical device "/dev/sda2" for LVM usage ... done
- Creating logical volume "SYSTEM" with size 59GB ... done
- Creating Backup-Partition "BACKUP" ... done
- Formatting /dev/mapper/rootfs-BACKUP (ext4) ... done
- Formatting /dev/mapper/rootfs-SYSTEM (ext4) ... done
- Mounting /dev/sda1 ... done
- Mounting /dev/mapper/rootfs-SYSTEM ... [   27.404051] EXT4-fs (dm-0): mounted filesystem with ordered data mode. Opts: (null)
done
- Deploying firmware/hilscher-iotgw-image-valleyisland-64-20160617110202.rootfs.tar.bz2 to /dev/mapper/rootfs-SYSTEM ...
 258MiB 0:01:42 [2.54MiB/s] [==================================================================================================>] 100%
done
```

*Figure 109: Firmware update in progress*

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

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

**Note:**

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

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

# 7.2 Useful CLI commands and parameters in Terminal

## 7.2.1 Network Manager

```
sudo nmcli …
```

## 7.2.2 Show interface status

```
sudo nmcli dev status
```

## 7.2.3 Activate interface

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

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

## 7.2.4 Docker Compose support for Standard Docker environment

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

**Examples**

Show the version of Docker Compose:

```
docker-compose version
```

Start container(s) via Docker Compose file:

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

Stop container(s) via Docker Compose file:

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

## 7.2.5 Manage Standard Docker

```
docker <docker commands>
```

**Examples**

List all created containers of the Standard Docker instance:

```
docker ps
```

List all bridges of the Standard Docker instance:

```
docker network ls
```

## 7.2.6 Manage IoT Edge Docker

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

**Example**

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

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

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

Disable autostart:

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

Stop SSH Daemon:

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

### 7.2.8 External storage support using iSCSI

Enable iSCSI service:

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

Start iSCSI service:

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

Target discovery and connection administration:

```
sudo iscsiadm <parameter>
```

Configuration files:

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

### 7.2.9 Follow the system log via terminal CLI

```
sudo journalctl -f
```

# 8 Technical data

| Category | Parameter/item | Value/description |
|---|---|---|
| Product | Part number | 1321.300/NFLD |
| | Product name | NIOT-E-TIJCX-GB-RE/NFLD |
| | Application | IT/OT Edge device for data-intensive and complex IoT applications with demand on maximum performance, connectivity and memory size. |
| Functions | IoT Edge Docker | Docker for remote and automatic deployment and maintenance of containers |
| | Standard Docker | Docker for manual and local deployment and maintenance of containers |
| | Local Device Manager | Web-based GUI for local device parameterization |
| Security | Boot | 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 | 8 GB DDR3 RAM |
| | Hard drive | 128 GB solid state disk drive:<br>64 GB application<br>64 GB backup |
| Power | Voltage | 24 V DC ± 4.8 V DC |
| | Current (at 24 V DC) | Without USB: 420 mA (typical)<br>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).<br>In listening (“passive”) mode: PROFINET, EtherCAT, Ethernet |
| Additional interfaces | USB | 3 x USB 2.0 (500 mA)<br>1 x USB 3.0 (900 mA)<br>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)<br>**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) |

| 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<br>Sinusoidal: 2 Grms @ 5~500 Hz, IEC 60068-2-64 |

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

# 9 Decommissioning, dismounting and disposal

## 9.1 Putting the device out of operation

**NOTICE**

**Danger of Unsafe System Operation!**

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

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

## 9.2 Disposal and recycling

### 9.2.1 Disposal of battery

This product contains a battery:
KTS CR2032W Lithium coin cell battery (or equivalent).

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

**Waste electronic equipment**

This battery must not be disposed of with household waste.

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

When disposing of the battery, observe the following:

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

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

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

### 9.2.2 Removal of battery

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

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

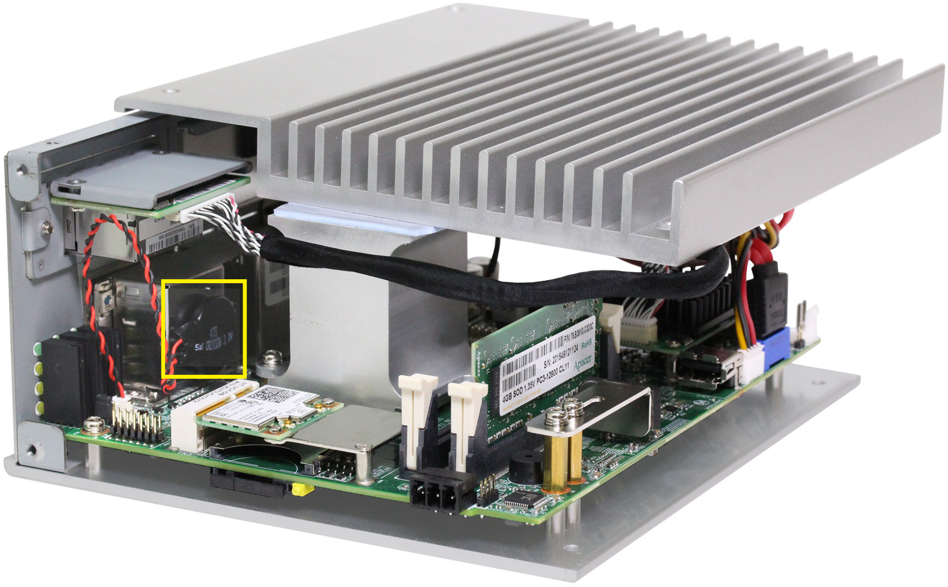


*Figure 110: NIOT-E-TIJCX-GB-RE/NFLD battery*

### 9.2.3 Disposal of device

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

**Waste electronic equipment**

This product must not be disposed of with household waste.

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

When disposing of the product, observe the following:

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

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

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

# 10 Legal notes

### Terms and conditions

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

### netFIELD OS

netFIELD OS is a YOCTO project based Linux operating system released and licensed by Hilscher.
netFIELD OS is released under the HILSCHER netFIELD Source Code/Software LICENSE AGREEMENT.
netFIELD OS may include 3rd party software or software declared as Open Source. The licensing information of all included software components are provided in textual form in the netFIELD OS under the folder `/usr/share/common-licenses` and subfolders.
Open Source software is released under Open Source License usually.
The official verbatim texts can be read and checked under https://opensource.org/licenses.

### Copyright

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

### Important notes

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

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

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

### Liability disclaimer

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

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

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

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

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

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

### Warranty

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

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

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

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

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

### Additional guarantees

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

### Confidentiality

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

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

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

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

### Export provisions

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

# List of figures

# List of tables

# Contacts

### HEADQUARTER

**Germany**

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

**Support**

Phone: +49 (0) 6190 9907-990
E-mail: hotline@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, Bangalore
Phone: +91 8888 750 777
E-mail: info@hilscher.in

**Support**

Phone: +91 8108884011
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

**Republic of Korea**

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

**Support**

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

**Austria**

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

**Support**

Phone: +43 732 931 675-0
E-mail: at.support@hilscher.com

**Switzerland**

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

**Support**

Phone: +41 (0) 32 623 6633
E-mail: support.swiss@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