



**Operating instruction manual  
netFIELD OS Datacenter**

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

DOC200902OI02EN | Revision 2 | English | 2021-06 | Released | Public

# Table of contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
1.1	About this document .....	4
1.1.1	Description of the contents .....	4
1.1.2	List of revisions .....	4
1.1.3	Conventions in this document.....	5
1.2	Terms and abbreviations.....	6
<b>2</b>	<b>Brief description .....</b>	<b>7</b>
<b>3</b>	<b>System requirements for using netFIELD OS Datacenter .....</b>	<b>11</b>
<b>4</b>	<b>Commissioning and first steps .....</b>	<b>13</b>
4.1	Overview .....	13
4.1.1	netFIELD Portal user .....	13
4.1.2	Standard Docker user .....	14
4.2	Installation on KVM (Proxmox VE example) .....	15
4.3	Installation on VMware (ESXi) .....	30
4.4	Establish LAN connection and login to Local Device Manager.....	37
4.5	Set system time.....	41
4.6	"Onboard" (register) netFIELD OS in the netFIELD Portal .....	43
4.6.1	Overview .....	43
4.6.2	Onboarding using the "Basic" method .....	44
4.6.3	Onboarding using the "Advanced" method .....	46
<b>5</b>	<b>Local Device Manager .....</b>	<b>53</b>
5.1	Overview .....	53
5.2	System .....	55
5.3	Networking .....	58
5.3.1	Overview .....	58
5.3.2	Firewall.....	63
5.3.3	Network Proxy settings .....	72
5.4	Networking Services .....	78
5.5	Onboarding (and offboarding).....	78
5.6	Standard Docker .....	81
5.7	IoT Edge Docker .....	88
5.8	Accounts .....	94
5.9	Certificate .....	97
5.10	General Settings .....	98
5.10.1	Overview .....	98
5.10.2	Web Server (Port) Settings .....	99
5.10.3	Default MQTT Client Settings .....	100
5.10.4	Docker Network Settings .....	102
5.10.5	Remote Access.....	106
5.11	Terminal .....	108
5.12	System Update.....	109
5.13	Logs .....	112
<b>6</b>	<b>Good to know.....</b>	<b>113</b>

6.1	Useful CLI commands and parameters in Terminal.....	113
6.1.1	Network Manager.....	113
6.1.2	Show interface status.....	113
6.1.3	Activate interface .....	113
6.1.4	Docker Compose Support for Standard Docker environment.....	113
6.1.5	Manage Standard Docker .....	113
6.1.6	Manage IoT Edge Docker .....	113
6.1.7	Enable/disable SSH Daemon (release port 22) .....	113
6.1.8	External storage support using iSCSI .....	114
6.1.9	Follow the system log via terminal CLI .....	114
6.2	netFIELD OS: Industrial IoT Operating System .....	115
<b>7</b>	<b>Legal notes .....</b>	<b>118</b>
	<b>List of Figures .....</b>	<b>122</b>
	<b>List of Tables .....</b>	<b>125</b>
	<b>Contacts.....</b>	<b>126</b>

# 1 Introduction

## 1.1 About this document

### 1.1.1 Description of the contents

This document describes the **netFIELD OS Datacenter** from Hilscher and provides instructions on how to install it on KVM (Proxmox VE) or VMware VSpere ESXi virtualization platforms.

### 1.1.2 List of revisions

Index	Date	Author	Revision
1	2020-12-10	MKE	Document created
2	2021-06-29	MKE	Document revised and updated to netFIELD OS 2.2: Section <i>Brief description</i> [▶ page 7] updated. Section <i>Standard Docker user</i> [▶ page 14] added. Section <i>Establish LAN connection and login to Local Device Manager</i> [▶ page 37] updated. Section <i>"Onboard" (register) netFIELD OS in the netFIELD Portal</i> [▶ page 43] updated. Section <i>Firewall</i> [▶ page 63] updated. Section <i>Networking Services</i> [▶ page 78] added. Section <i>Standard Docker</i> [▶ page 81] revised. Section <i>IoT Edge Docker</i> [▶ page 88] revised. Section <i>Remote Access</i> [▶ page 106] added.

Table 1: List of revisions

### 1.1.3 Conventions in this document

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

#### Notes



---

**Important:**

<important note>

---



---

**Note:**

<simple note>

---



---

<note, where to find further information>

---

#### Operation instructions

1. <operational step>

➤ <instruction>

➤ <instruction>

2. <operational step>

➤ <instruction>

➤ <instruction>

#### Results

↻ <intermediate result>

⇒ <final result>

## 1.2 Terms and abbreviations

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

Table 2: Terms and abbreviations

## 2 Brief description

### Overview

**netFIELD OS Datacenter** is the netFIELD Operating System for virtual machines respectively virtualization environments. It runs on all hardware platforms supporting VMware® vSphere ESXi or KVM (Linux Kernel-based Virtual Machine) hypervisors.

It offers the same functions and features as the netFIELD OS running “natively” in netFIELD Connect and netFIELD OnPremise edge devices; but – being a virtual machine – allows you flexible assignment of hardware resources (like CPU cores, memory, data storage and network adapters) according to your needs.

It is thus an alternative to the netFIELD Connect and netFIELD OnPremise edge devices if your use case demands higher or scalable hardware capabilities.

### Key features of the netFIELD OS

- The netFIELD OS features the **Local Device Manager**, which is a web-based GUI for local device parameterization.
- 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 virtual machine:
  - **IoT Edge Docker** for remote and automatic deployment and maintenance of containers. These containers are deployed (“pulled”) and managed via the netFIELD Platform. This requires your netFIELD OS Datacenter 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 registration and onboarding process, the standard Docker is the only way to pull and run container applications on your netFIELD OS Datacenter.
- All i86-compliant netFIELD Apps are supported except for apps using netX resources. Apps that use netX resources and can thus currently not be used with the netFIELD OS Datacenter are:
  - netFIELD App PROFINET Device
  - netFIELD App EtherCAT Tap

**Services supported by the netFIELD OS**

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

## Software architecture

The following figure shows the software architecture of a netFIELD OS Datacenter that has a netFIELD Cloud connection and that is installed on a hardware with *VMware vSphere ESXi* ("bare metal" hypervisor):

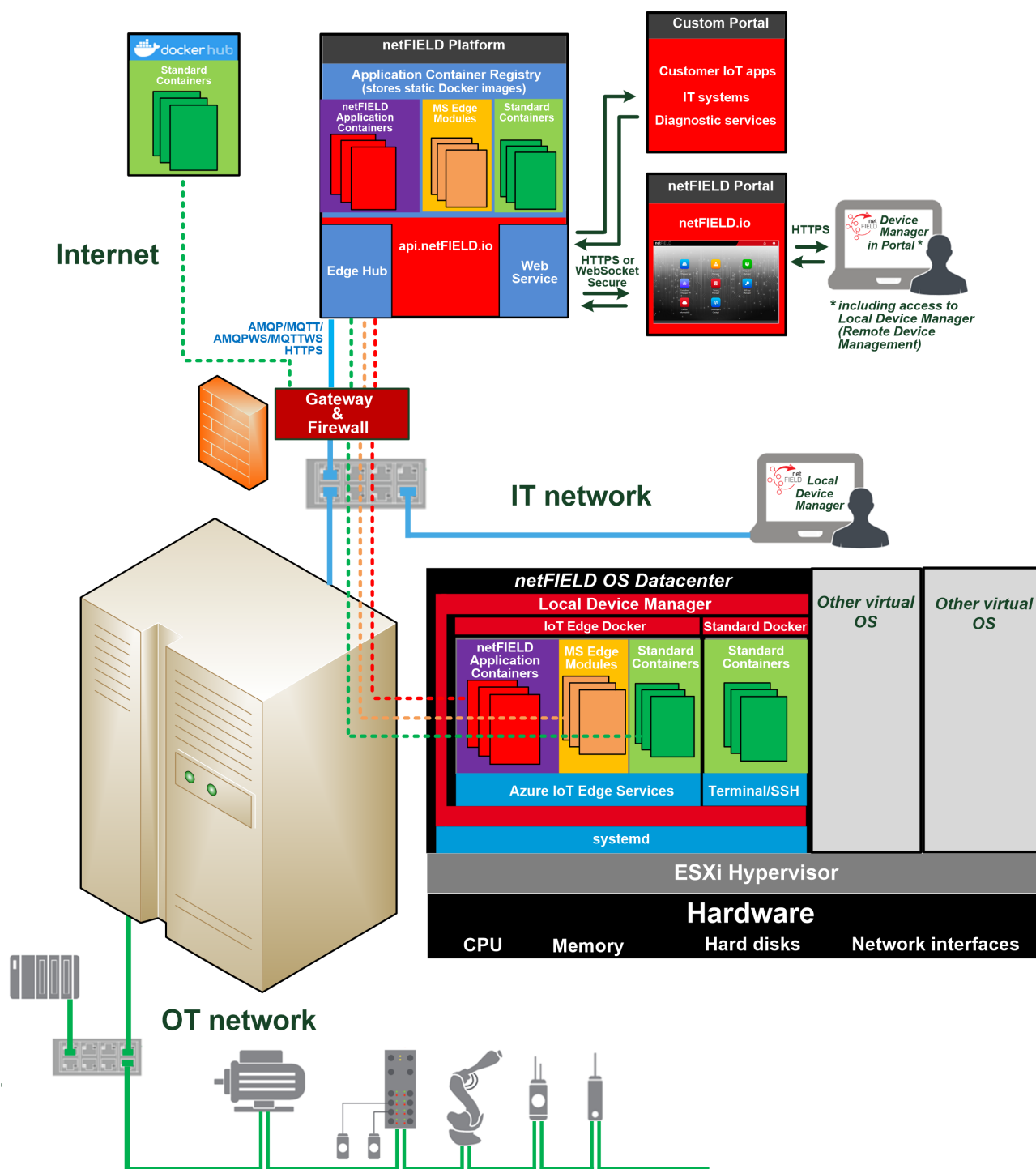


Figure 1: SW architecture with VMware ESXi

The following figure shows the software architecture of a netFIELD OS Datacenter that has a netFIELD Cloud connection and that is installed on a hardware with *KVM hypervisor* ("hosted" hypervisor):

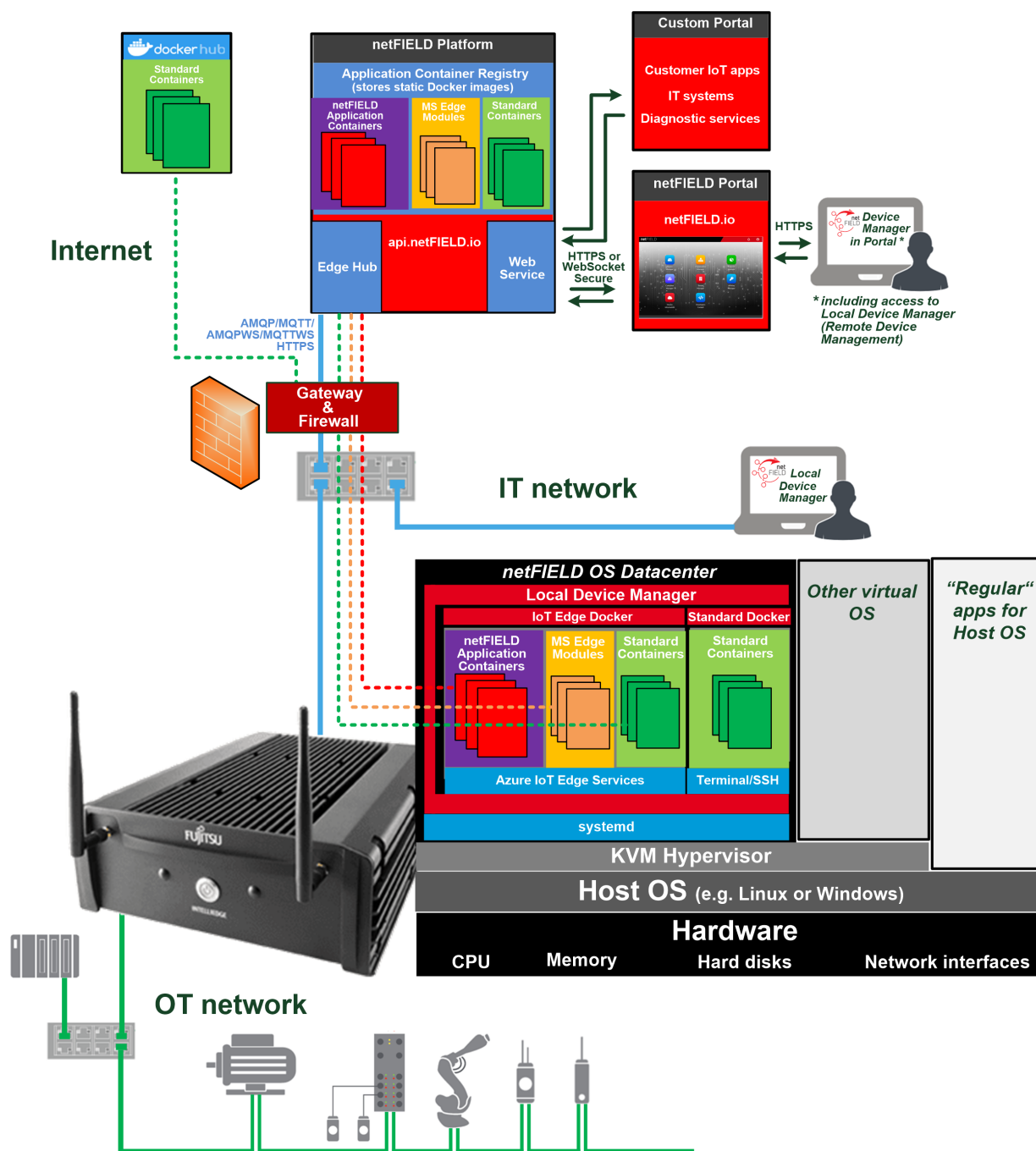


Figure 2: SW architecture with KVM

### 3 System requirements for using netFIELD OS Datacenter

#### Virtualization platforms

The netFIELD OS Datacenter is compatible with the following virtualization platforms:

Hypervisor/platform	Required features	Vendor/Distributor	Tested/verified with version	Note
KVM (Kernel-based virtual machines)	<ul style="list-style-type: none"> <li>• VirtIO support for virtual SCSI and Ethernet adapter</li> <li>• 16 GB virtual SATA disk</li> <li>• Virtual UEFI Bios</li> <li>• Virtual Machine Chipset Q35</li> <li>• 2 GB RAM</li> <li>• If Proxmox VE is used: Version 6.1-11 or higher</li> <li>• *.qcow2 file containing netFIELD OS image</li> <li>• DHCP service</li> </ul>	KVM kernel modules are contained in all major Linux community and enterprise distributions	Proxmox VE v6.1-11	Red Hat Enterprise and Proxmox VE provide user-friendly management GUIs. For information on hardware compliance, check the recommendations of the distribution's vendor.
VMware® VSphere ESXi	<ul style="list-style-type: none"> <li>• 16 GB virtual SATA disk</li> <li>• 4 vCPUs</li> <li>• 2 GB RAM</li> <li>• Virtual hardware &gt; v.10 (ESXi 5.5 or later)</li> <li>• VMXnet3 virtual Ethernet adapter</li> <li>• *.ova file containing netFIELD OS image</li> <li>• DHCP service</li> </ul>	VMware	ESXi 7.1	For information on hardware compliance, check the <a href="#">VMware Compatibility Guide</a> web page.
VMware® Workstation Player	Same as VMware® VSphere ESXi (see above)	VMware	≥ 6	Desktop application with limited functionalities for evaluating and testing virtual machines. For information on hardware compliance, check the <a href="#">System requirements for VMware Player and VMware Workstation Player</a> web page.

Table 3: Virtualization platforms for netFIELD OS Datacenter

### Minimum hardware resources requirements

netFIELD OS Datacenter requires the following minimum hardware resources on the host machine. (These values are also preset in the \*.qcow2 respectively \*.ova files)

- Memory: 2 GB
- CPU cores: 4
- Hard disk: 16 GB
- Network adapter: 1

**Note:**

Note that you can increase the size of the preset 16 GB virtual hard disk before the first start-up of the virtual machine. The partitioning of the virtual hard disk takes place during the first start-up of the virtual machine according to the default parameters preset in the \*.qcow2 respectively \*.ova files. Note that it is not possible to diminish the size of the virtual hard disk afterwards.

---

**Note:**

Note that a DHCP Server must be available in the network to which the netFIELD OS datacenter belongs. This ensures that the Local Device Manager of the netFIELD OS is accessible for initial configuration via web browser after having installed the netFIELD OS as virtual machine. Otherwise the netFIELD OS will randomly select its own IP address, which may not be reachable by the user via web browser.

---

## 4 Commissioning and first steps

### 4.1 Overview

#### 4.1.1 netFIELD Portal user

The following table shows the steps that you must perform to commission the netFIELD OS Datacenter if you are a user of the netFIELD Portal.

#	Step	For details see
1	Install netFIELD OS Datacenter on host system.	Section <i>Installation on KVM (Proxmox VE example)</i> [► page 15] respectively section <i>Installation on VMware (ESXi)</i> [► page 30]
2	Establish LAN connection and login to Local Device Manager.	Section <i>Establish LAN connection and login to Local Device Manager</i> [► page 37]
3	Set local system time.	Section <i>Set system time</i> [► page 41]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section <i>Network Proxy settings</i> [► page 72]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section <i>Docker Network Settings</i> [► page 102]
6	Optional: Configure netFIELD OS firewall <b>Note:</b> By default, the internal netFIELD OS firewall allows all traffic ("trusted zone"). When you assign an interface or subnet to the drop or block zone, make sure that you open the ports that are used by your application containers.	Section <i>Firewall</i> [► page 63]
7	"Onboard" (register) device in netFIELD Portal. <b>Note:</b> Make sure that your company's firewall does not block the TCP port (outgoing) of the upstream protocol (device-to-cloud communication) that you intend to use. MQTT: 8883 MQTT over WebSocket: 443 AMQP: 5671 AMQP over WebSocket: 443	Section <i>"Onboard" (register) netFIELD OS in the netFIELD Portal</i> [► page 43]
8	Deploy your desired application container(s) from netFIELD Portal (if not already deployed through Deployment Manifest).	Section <i>Deploying containers on your device</i> in the operating instruction manual <i>netFIELD Portal</i> , DOC190701OIxxEN

Table 4: Tasks for commissioning the netFIELD OS Datacenter (netFIELD Portal user)

### 4.1.2 Standard Docker user

The following table shows the steps that you must perform to commission the netFIELD OS Datacenter 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	Install netFIELD OS Datacenter on host system.	Section <i>Installation on KVM (Proxmox VE example)</i> [► page 15] respectively section <i>Installation on VMware (ESXi)</i> [► page 30]
2	Establish LAN connection and login to Local Device Manager.	Section <i>Establish LAN connection and login to Local Device Manager</i> [► page 37]
3	Set local system time.	Section <i>Set system time</i> [► page 41]
4	If applicable (if your LAN uses HTTP/HTTPS/FTP proxy servers): Configure netFIELD OS for using proxy server.	Section <i>Network Proxy settings</i> [► page 72]
5	If applicable (if the default Docker IP addresses are not compatible with your LAN): Customize Docker Network Settings.	Section <i>Docker Network Settings</i> [► page 102]
6	Optional: Configure netFIELD OS firewall <b>Note:</b> By default, the internal netFIELD OS firewall allows all traffic ("trusted zone"). When you assign an interface or subnet to the drop or block zone, make sure that you open the ports that are used by your application containers.	Section <i>Firewall</i> [► page 63]
7	Open Standard Docker and deploy and run container images.	Section <i>Standard Docker</i> [► page 81]

Table 5: Tasks for commissioning the netFIELD OS Datacenter (Standard Docker user)

## 4.2 Installation on KVM (Proxmox VE example)

This section describes how to install netFIELD OS Datacenter on KVM, using Proxmox VE as example.

1. Download the \*.qcow2 file from Hilscher to your local PC.
  - Go to the *netFIELD Software Overview* page <https://kb.hilscher.com/x/sSAfBw> and click on the link of the latest netFIELD OS version.  
Navigate to the *netFIELD OS Datacenter* section and download the netfield-image-niot-e-vm-en.wic.qcow2 file.
2. Create new virtual machine.
  - Connect to Proxmox VE.
  - In the **Resource tree**, select the node (i.e. the physical server) on which the netFIELD OS shall be installed, then click **Create VM** button in the header.

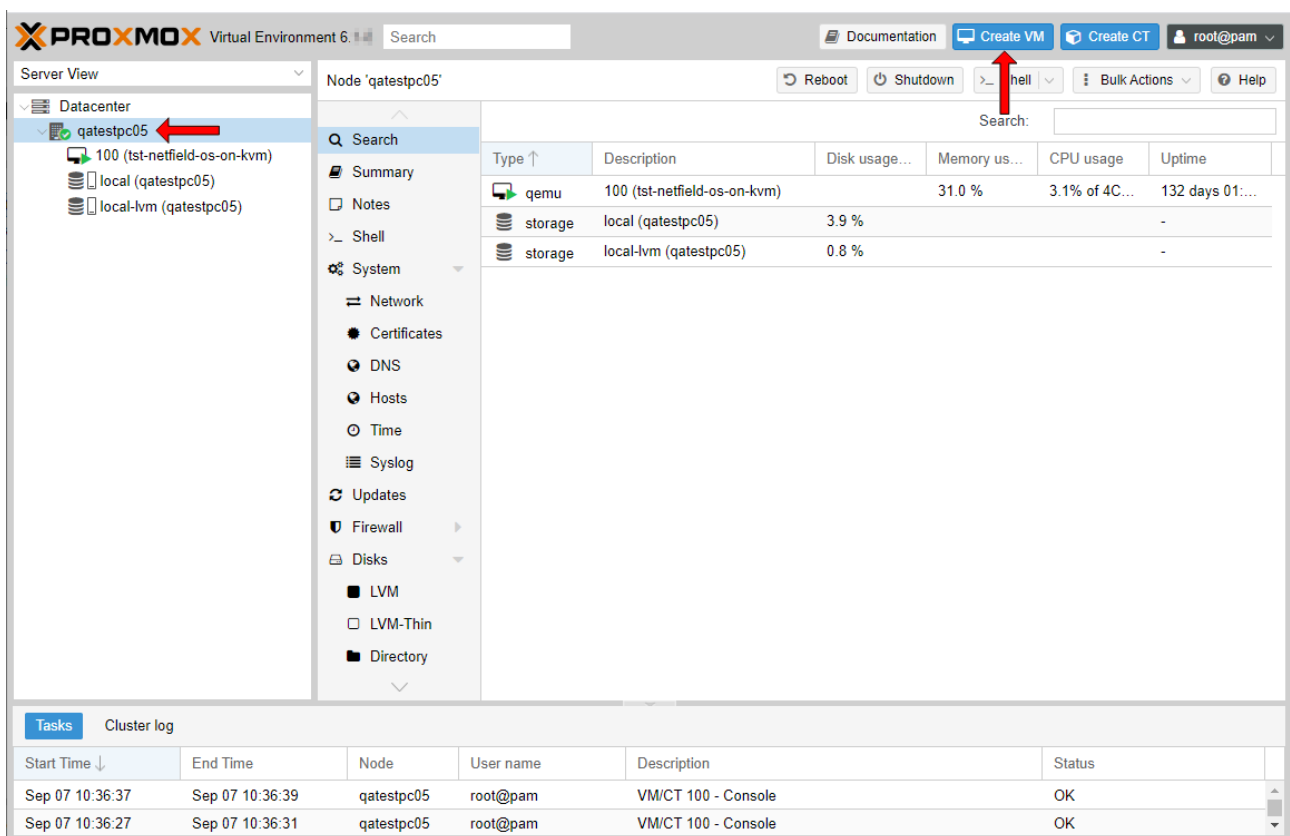
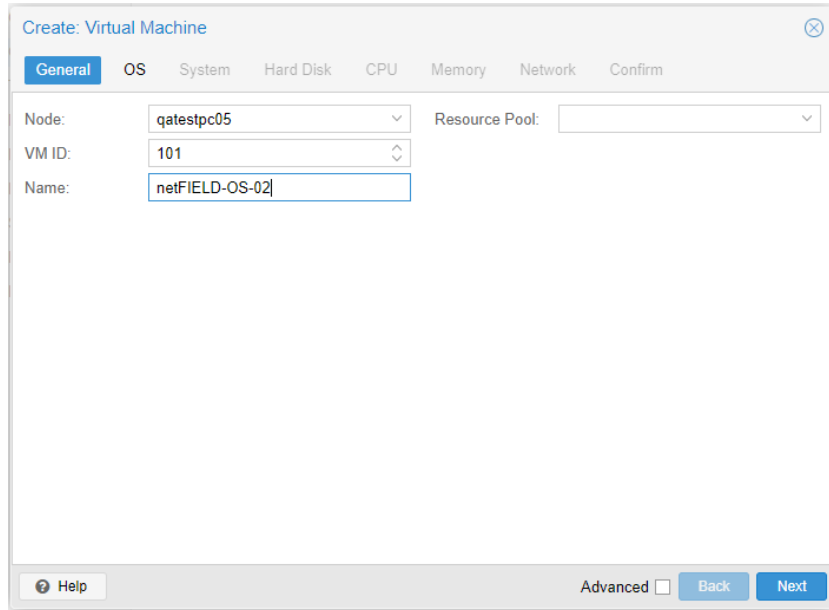


Figure 3: Proxmox VE

- The **Create Virtual Machine** wizard opens.

- In the **General** tab of the wizard, enter a **Name** for your virtual netFIELD OS:

The screenshot shows the 'Create: Virtual Machine' wizard with the 'General' tab selected. The 'Node' dropdown is set to 'qatestpc05', 'VM ID' is '101', and 'Name' is 'netFIELD-OS-02'. The 'Resource Pool' dropdown is empty. At the bottom, there is a 'Help' button, an 'Advanced' checkbox, and 'Back' and 'Next' buttons.

Create: Virtual Machine

General OS System Hard Disk CPU Memory Network Confirm

Node: qatestpc05 Resource Pool:

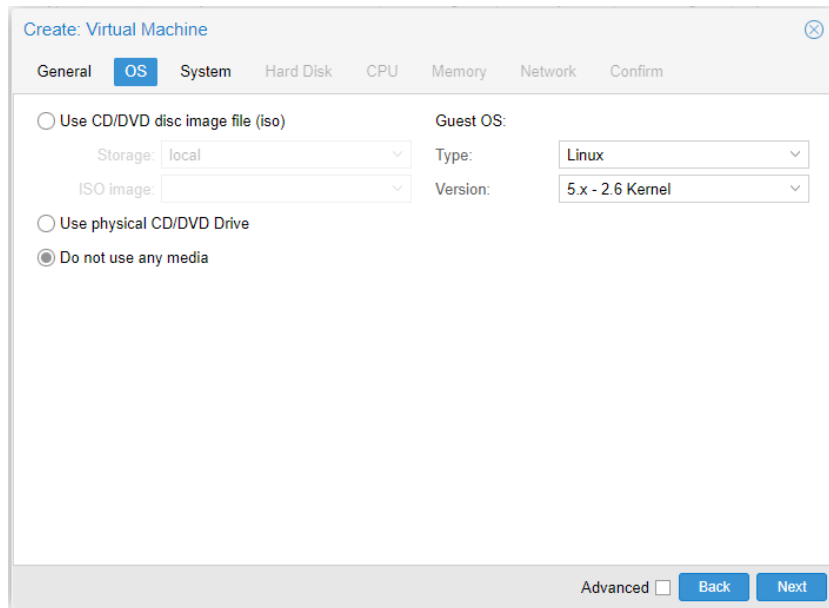
VM ID: 101

Name: netFIELD-OS-02

Help Advanced Back Next

Figure 4: General tab of Create Virtual Machine wizard

- In the **OS** tab of the wizard, select **Do not use any media** option (the netFIELD OS image will be imported and attached later). Leave the **Guest OS** parameters at their default settings (**Type**: Linux, **Version**: 5.x – 2.6 Kernel):

The screenshot shows the 'Create: Virtual Machine' wizard with the 'OS' tab selected. The 'Do not use any media' radio button is selected. The 'Guest OS' section shows 'Type' as 'Linux' and 'Version' as '5.x - 2.6 Kernel'. At the bottom, there is an 'Advanced' checkbox and 'Back' and 'Next' buttons.

Create: Virtual Machine

General OS System Hard Disk CPU Memory Network Confirm

☐ Use CD/DVD disc image file (iso)

Storage: local

ISO image:

☐ Use physical CD/DVD Drive

☒ Do not use any media

Guest OS:

Type: Linux

Version: 5.x - 2.6 Kernel

Advanced Back Next

Figure 5: OS tab of Create Virtual Machine wizard

- In the **System** tab of the wizard, leave the parameters at their default settings:

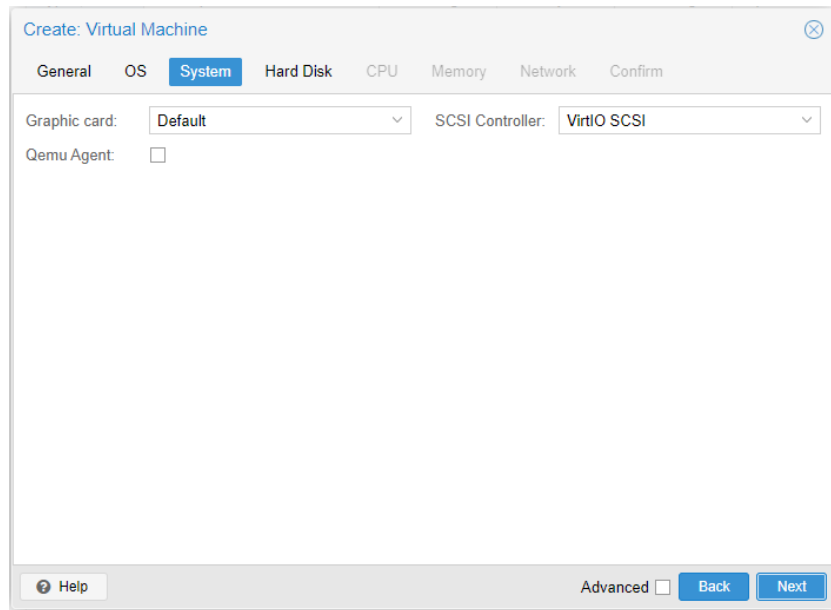


Figure 6: System tab of Create Virtual Machine wizard

- In the **Hard Disk** tab of the wizard, leave the parameters at their default settings.  
(This is only a dummy for now, which will be deleted later and then recreated after having imported the netFIELD OS \*.qcow2 file.)

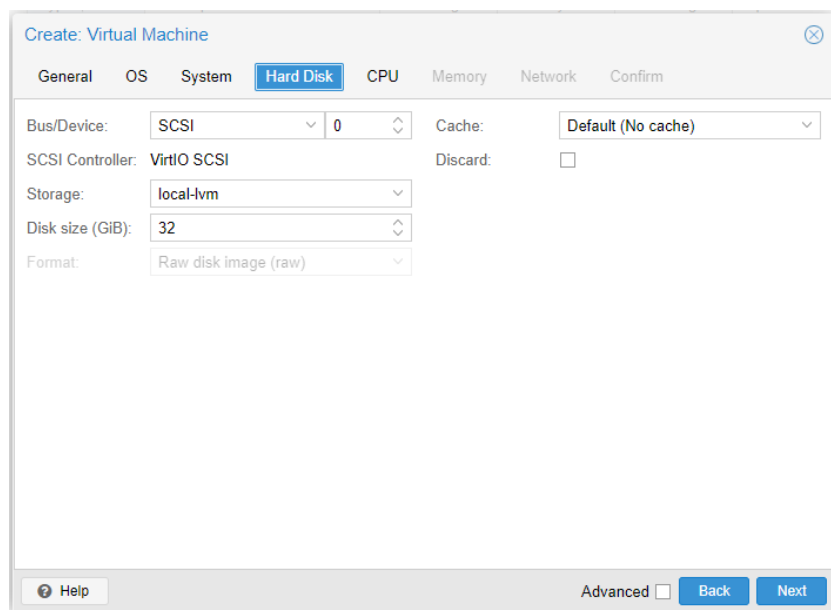


Figure 7: Hard Disk tab of Create Virtual Machine wizard

- In the **CPU** tab of the wizard, set four **Cores**. Leave the other parameters on their default settings:

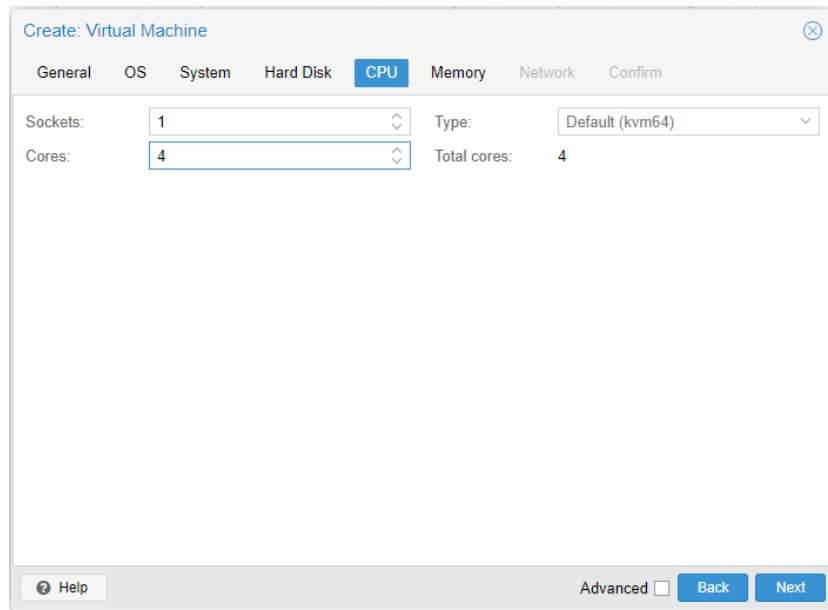


Figure 8: CPU tab of Create Virtual Machine wizard

- In the **Memory** tab of the wizard, set the amount of RAM that you want to allocate to the netFIELD OS (minimum 2016 MiB [2 GB]):

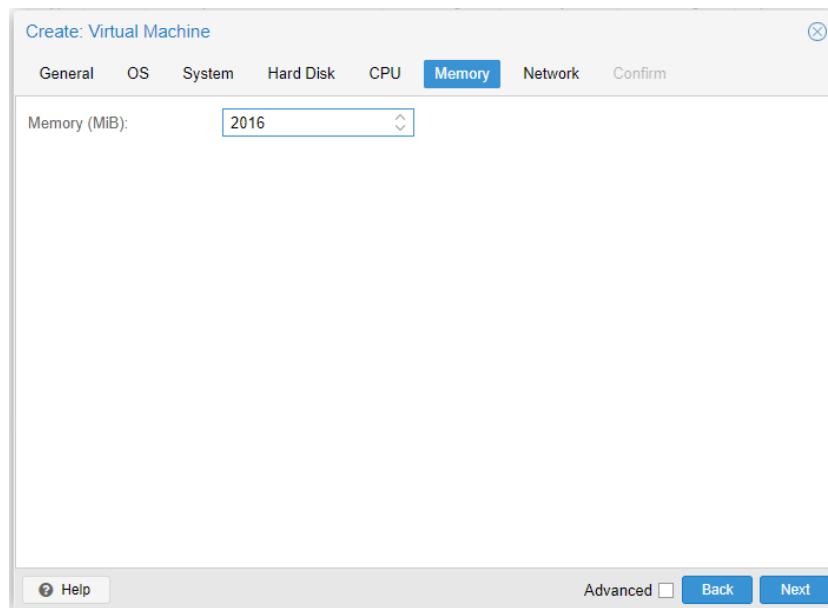


Figure 9: Memory tab of Create Virtual Machine wizard

- In the **Network** tab of the wizard, you must assign a **Bridge** that serves as a virtual connection of the netFIELD OS to a physical network interface device on your host system.

**Note:**

The bridge must be connected to a network in which a DHCP Server is available and it must be reachable from “outside” via TCP/IP. This means that you must configure the network environment of your host system (“node”) accordingly.

Note also that you can add further network interfaces/bridges (a.k.a “Network Devices”) to the virtual machine later, after having finished the wizard.

- Select a suitable **Bridge** in the drop-down menu. Leave the other parameters at their default settings.

Figure 10: Network tab of Create Virtual Machine wizard

- In the **Confirm** tab of the wizard, click **Finish**.

Key ↑	Value
cores	4
ide2	none,media=cdrom
memory	2016
name	netFIELD-OS-02
net0	virtio,bridge=vibr2,firewall=1
nodename	qatestpc05
numa	0
ostype	l26
scsi0	local-lvm:32
scsihw	virtio-scsi-pci
sockets	1
vmid	101

Figure 11: Confirm tab of Create Virtual Machine wizard

➤ The wizard closes and the new virtual machine is displayed in the **Resource tree**:

The screenshot shows the Proxmox VE web interface. On the left, the 'Server View' sidebar shows the 'Datacenter' with a tree structure where '101 (netFIELD-OS-02)' is highlighted under the 'qatestpc05' node. The main panel displays the 'Node: qatestpc05' summary for this VM. At the bottom, the 'Cluster log' table shows the creation of VM 101.

Type	Description	Disk usage...	Memory us...	CPU usage	Uptime
qemu	100 (tst-netfield-os-on-kvm)		31.0 %	3.3% of 4C...	132 days 19:...
qemu	101 (netFIELD-OS-02)				-
storage	local (qatestpc05)	4.3 %			-
storage	local-lvm (qatestpc05)	0.8 %			-

Start Time	End Time	Node	User name	Description	Status
Sep 08 10:04:38	Sep 08 10:04:39	qatestpc05	root@pam	VM 101 - Create	OK
Sep 08 03:04:43	Sep 08 03:04:44	qatestpc05	root@pam	Update package database	OK

Figure 12: New virtual machine

## 3. Adapt hardware configuration.

- Select the netFIELD OS virtual machine in the **Resource tree**, then select **Hardware** in the VM navigation:

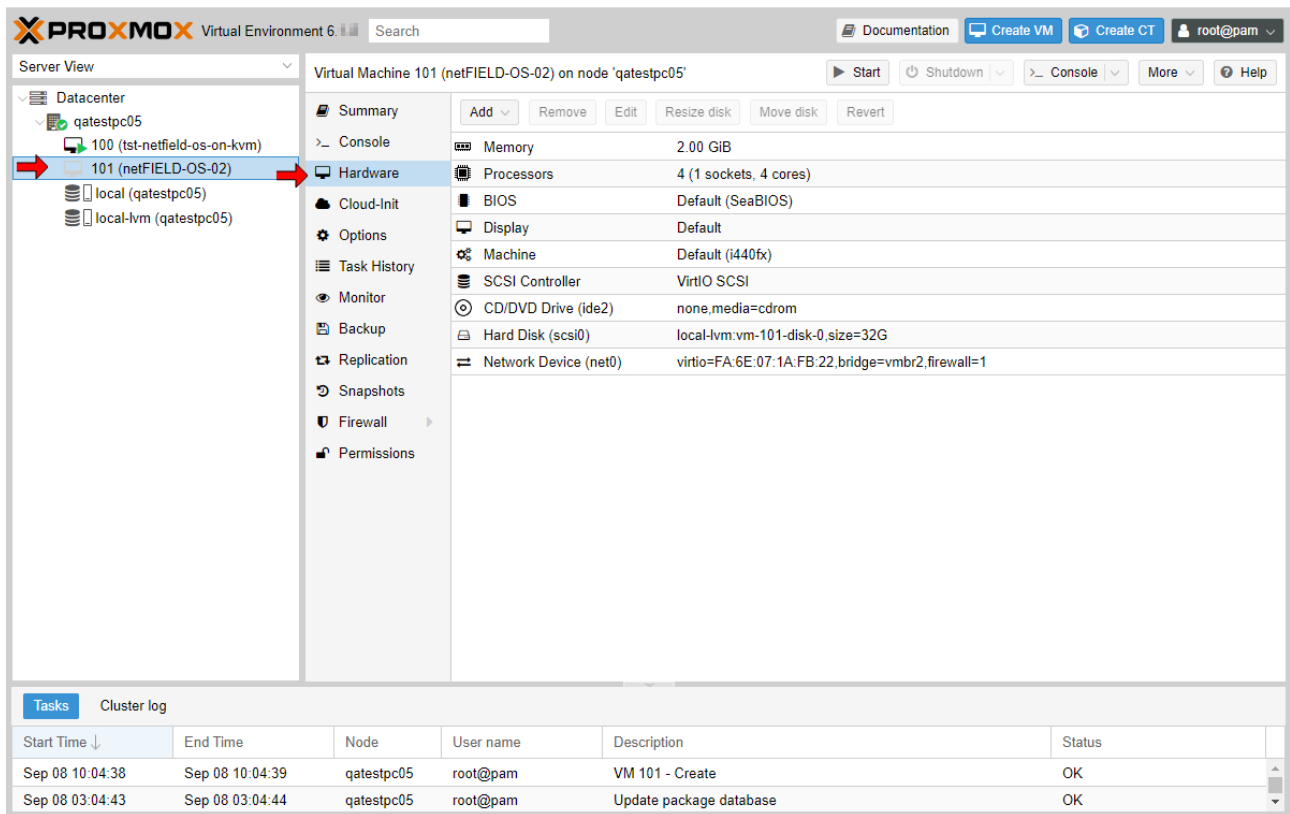
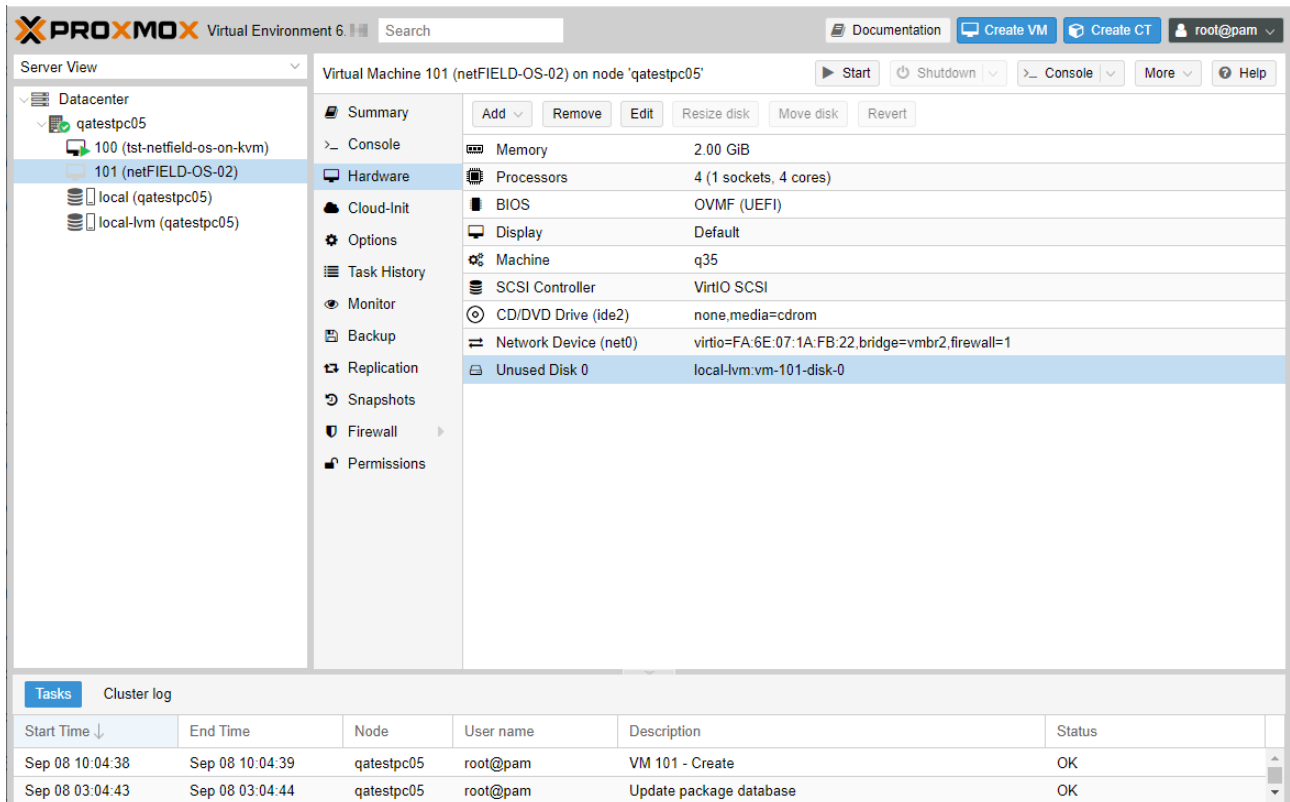


Figure 13: Hardware parameters VM

- Select the **BIOS** parameter, then click **Edit** button. In the **Edit BIOS** dialog, change the BIOS to **OVMF (UEFI)**.
- Select the **Machine** parameter, then click **Edit** button. In the **Edit Machine** dialog, change the Machine to **q35**.
- Select **Hard Disk** parameter, then click **Detach** button.

➤ The **Hard Disk** parameter is substituted by the **Unused Disk 0** entry:



Virtual Machine 101 (netFIELD-OS-02) on node 'qatestpc05'

Start | Shutdown | Console | More | Help

Summary | Add | Remove | Edit | Resize disk | Move disk | Revert

Hardware

Memory	2.00 GiB
Processors	4 (1 sockets, 4 cores)
BIOS	OVMF (UEFI)
Display	Default
Machine	q35
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	none,media=cdrom
Network Device (net0)	virtio=FA:6E:07:1A:FB:22.bridge=vmb2,firewall=1
Unused Disk 0	local-lvm:vm-101-disk-0

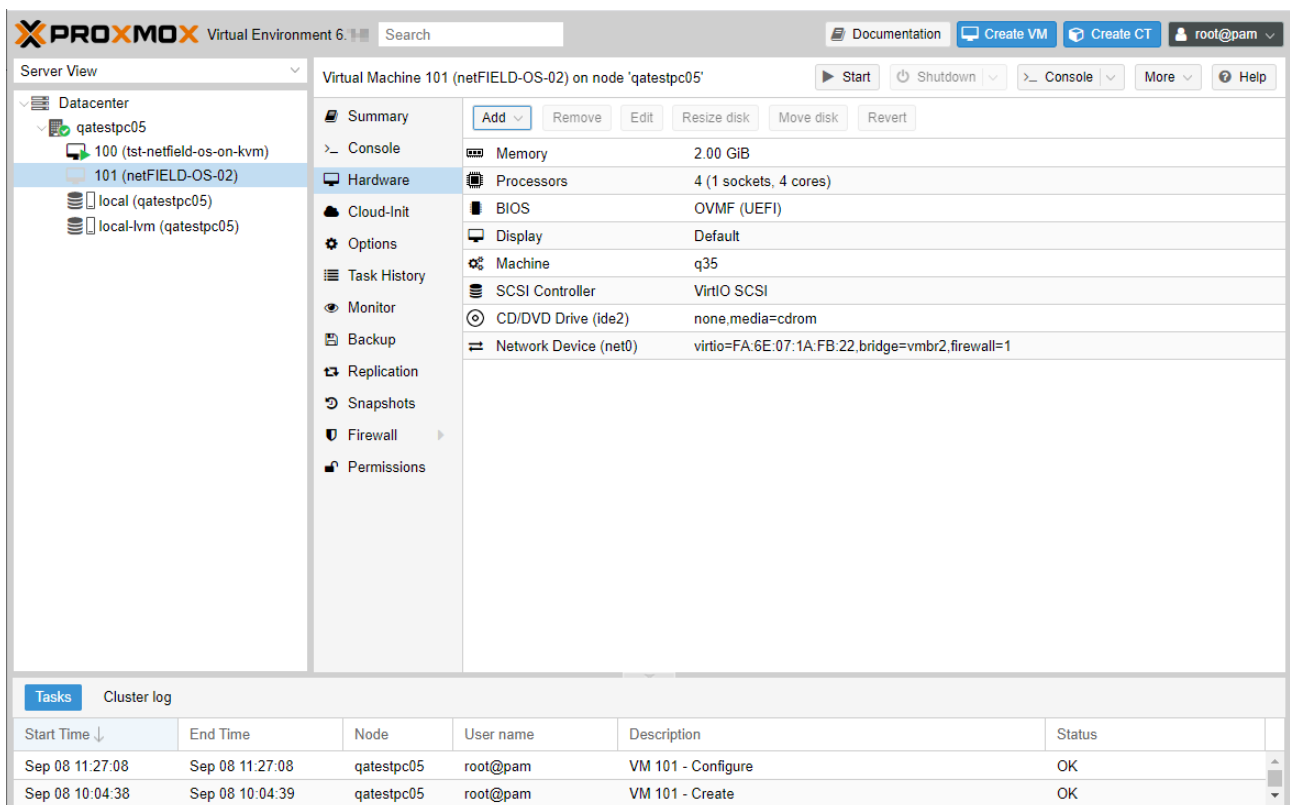
Tasks | Cluster log

Start Time ↓	End Time	Node	User name	Description	Status
Sep 08 10:04:38	Sep 08 10:04:39	qatestpc05	root@pam	VM 101 - Create	OK
Sep 08 03:04:43	Sep 08 03:04:44	qatestpc05	root@pam	Update package database	OK

Figure 14: Unused disk

➤ Select the **Unused Disk 0** entry, then click **Remove** button.

➤ The hardware parameters now look like this:



Virtual Machine 101 (netFIELD-OS-02) on node 'qatestpc05'

Start | Shutdown | Console | More | Help

Summary | Add | Remove | Edit | Resize disk | Move disk | Revert

Hardware

Memory	2.00 GiB
Processors	4 (1 sockets, 4 cores)
BIOS	OVMF (UEFI)
Display	Default
Machine	q35
SCSI Controller	VirtIO SCSI
CD/DVD Drive (ide2)	none,media=cdrom
Network Device (net0)	virtio=FA:6E:07:1A:FB:22.bridge=vmb2,firewall=1

Tasks | Cluster log

Start Time ↓	End Time	Node	User name	Description	Status
Sep 08 11:27:08	Sep 08 11:27:08	qatestpc05	root@pam	VM 101 - Configure	OK
Sep 08 10:04:38	Sep 08 10:04:39	qatestpc05	root@pam	VM 101 - Create	OK

Figure 15: New hardware parameters

#### 4. Upload the \*.qcow2 disk image file to Proxmox.

- Upload the \*.qcow2 file (which you have downloaded in step 1 from Hilscher) to the Proxmox host file system.  
You can use SSH or an SSH-based SCP tool like e.g. *WinSCP* to upload the file to the file directory of the host system, e.g.: /home/images:

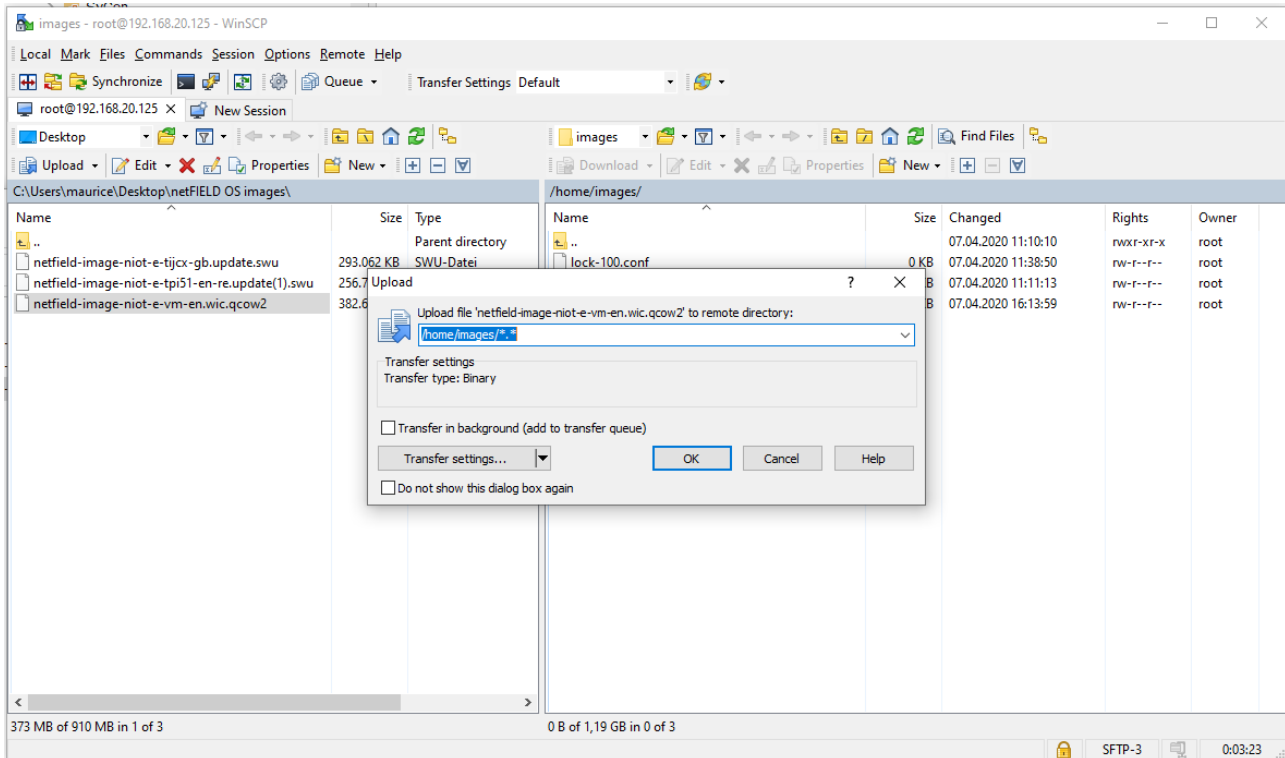


Figure 16: WinSCP upload

#### 5. Import the \*.qcow2 disk image file to the netFIELD OS.

- After uploading the image to the host system, you must import the image to the netFIELD OS virtual machine. Use an SSH terminal program like e.g. *Putty* for this.  
Enter the following command:

```
root@[node]:/[storage directory]# qm importdisk [ID of virtual machine] [name of the image file] local-lvm
```

In our example this is:

```
root@gatetpc05:/home/images# qm importdisk 101 netfield-image-niot-
e-vm-en.wic.qcow2 local-lvm
```

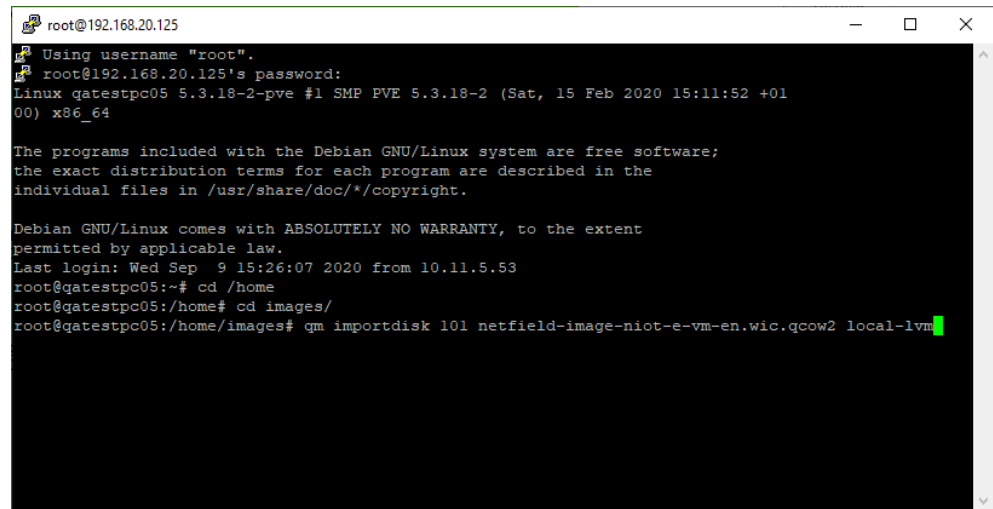


Figure 17: Using Putty to import the image

After successful import, the image is stored as `disk-0` for the virtual machine (`vm-101`) on the `local-lvm` mass storage disk of your node/host system:

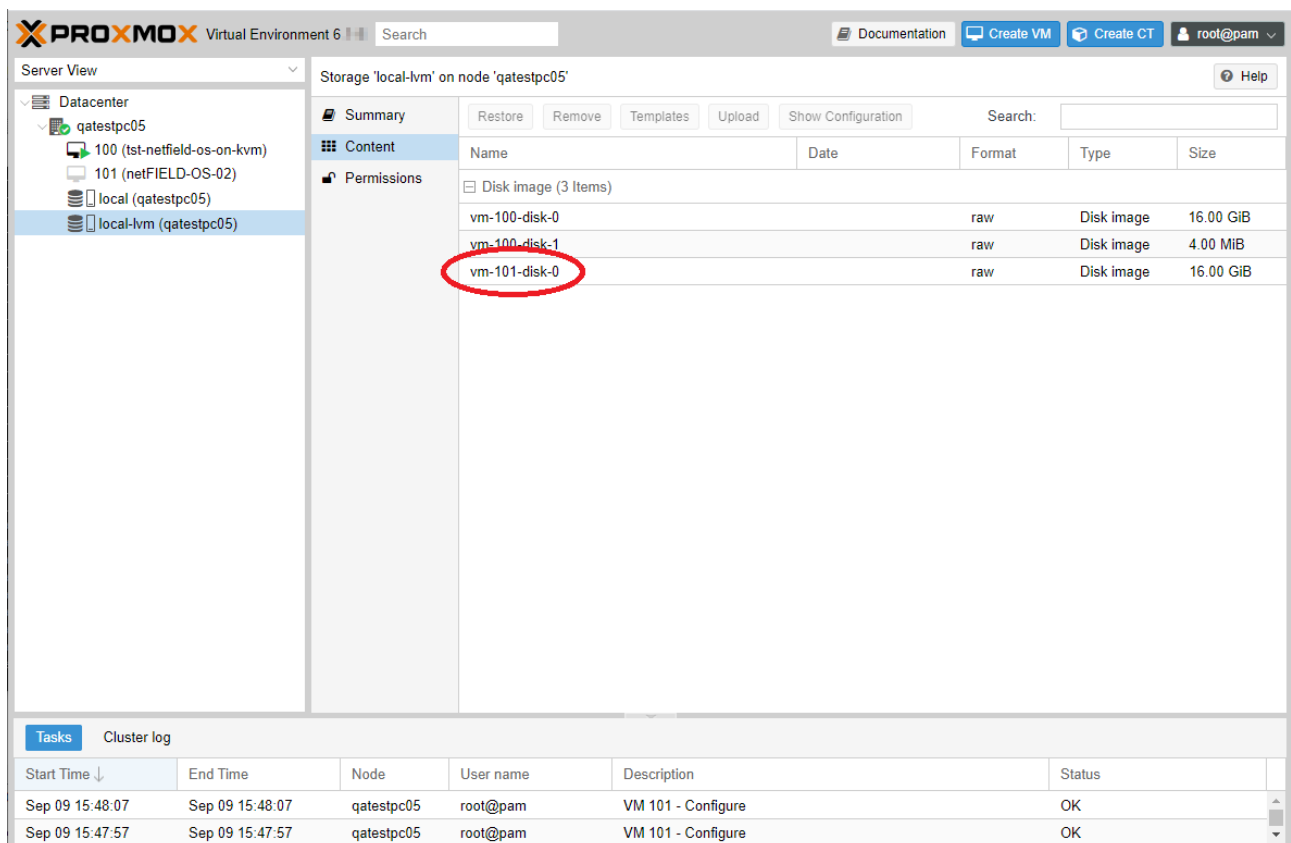
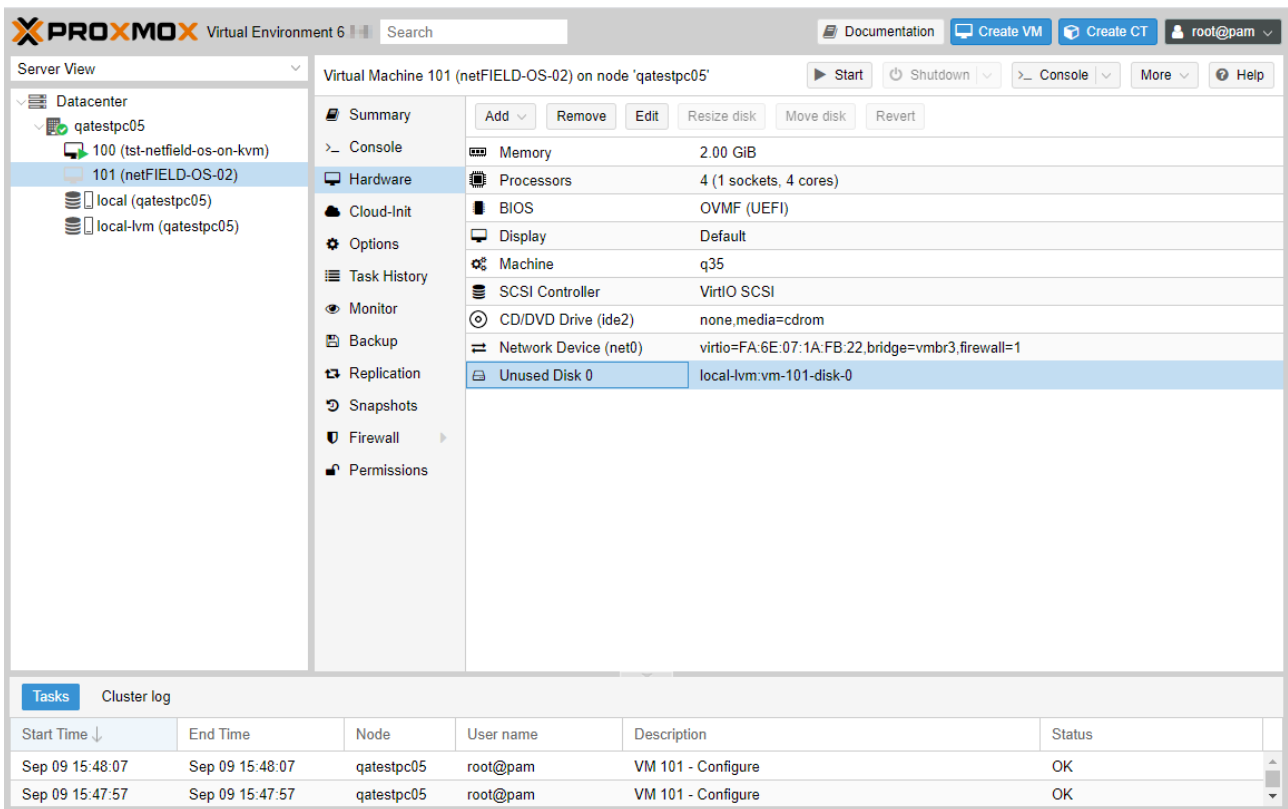


Figure 18: Imported image

It is also displayed as **Unused Disk 0** in the **Hardware** configuration panel of the netFIELD OS virtual machine:



The screenshot shows the Proxmox VE interface for Virtual Machine 101 (netFIELD-OS-02) on node 'qatestpc05'. The 'Hardware' tab is selected, displaying a list of hardware components. The 'Unused Disk 0' is highlighted, showing its path as 'local-lvm:vm-101-disk-0'.

Start Time	End Time	Node	User name	Description	Status
Sep 09 15:48:07	Sep 09 15:48:07	qatestpc05	root@pam	VM 101 - Configure	OK
Sep 09 15:47:57	Sep 09 15:47:57	qatestpc05	root@pam	VM 101 - Configure	OK

Figure 19: Unused Disk

6. Attach the \*.qcow2 disk image file to the netFIELD OS virtual machine.
  - Select the **Unused Disk 0** entry, then click **Edit** button. In the **Add Unused Disk** dialog, change the **Bus/Device** parameter to **SATA**.
  - The **Unused Disk 0** entry has changed into the **Hard Disk (sata0)** parameter:

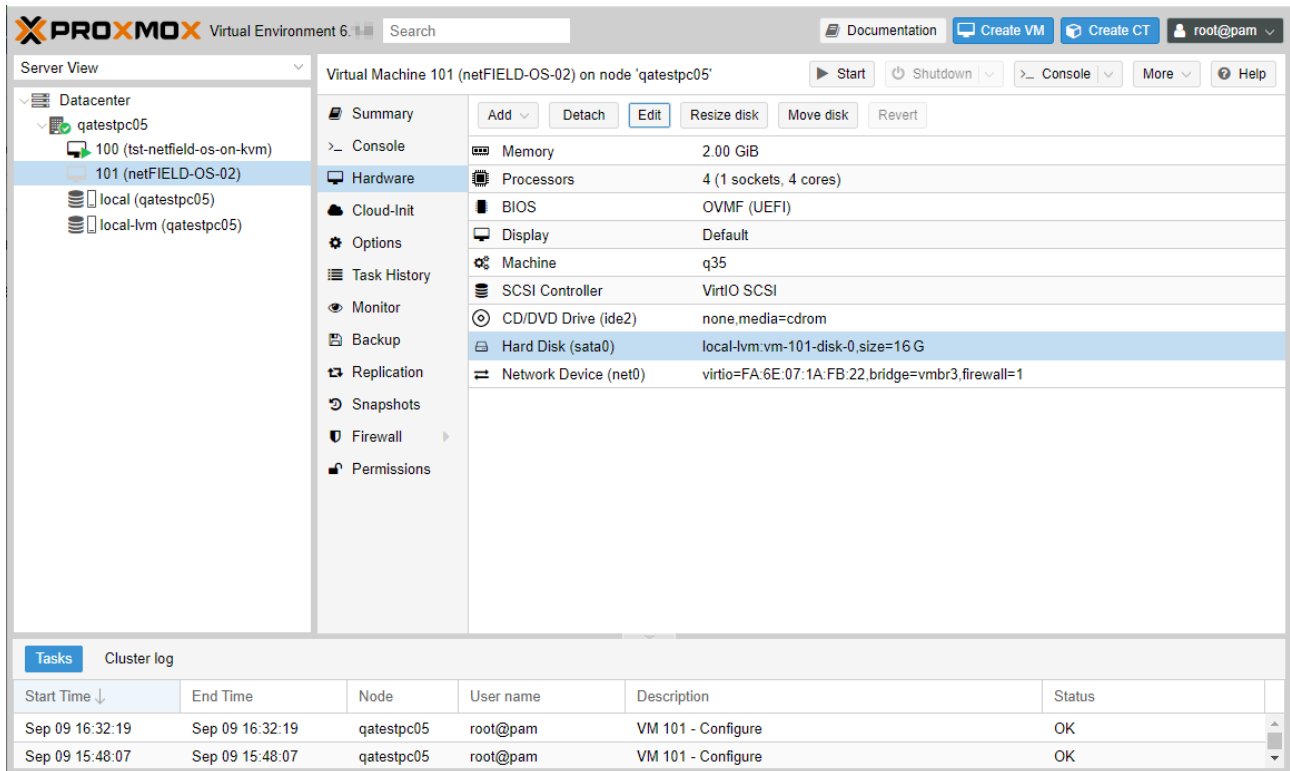


Figure 20: Attached hard disk

7. Add EFI disk.
  - In the **Hardware** panel of the netFIELD OS virtual machine, click **Add** button and select **EFI Disk** from the drop-down list. In the **Edit EFI Disk** dialog, select `local-lvm` as **Storage**.

8. Check boot order (first boot device must be **Disk 'sata0'**).

- Open the **Options** panel of the netFIELD OS virtual machine and check if **Disk 'sata0'** is the first entry for the **Boot Order** parameter:

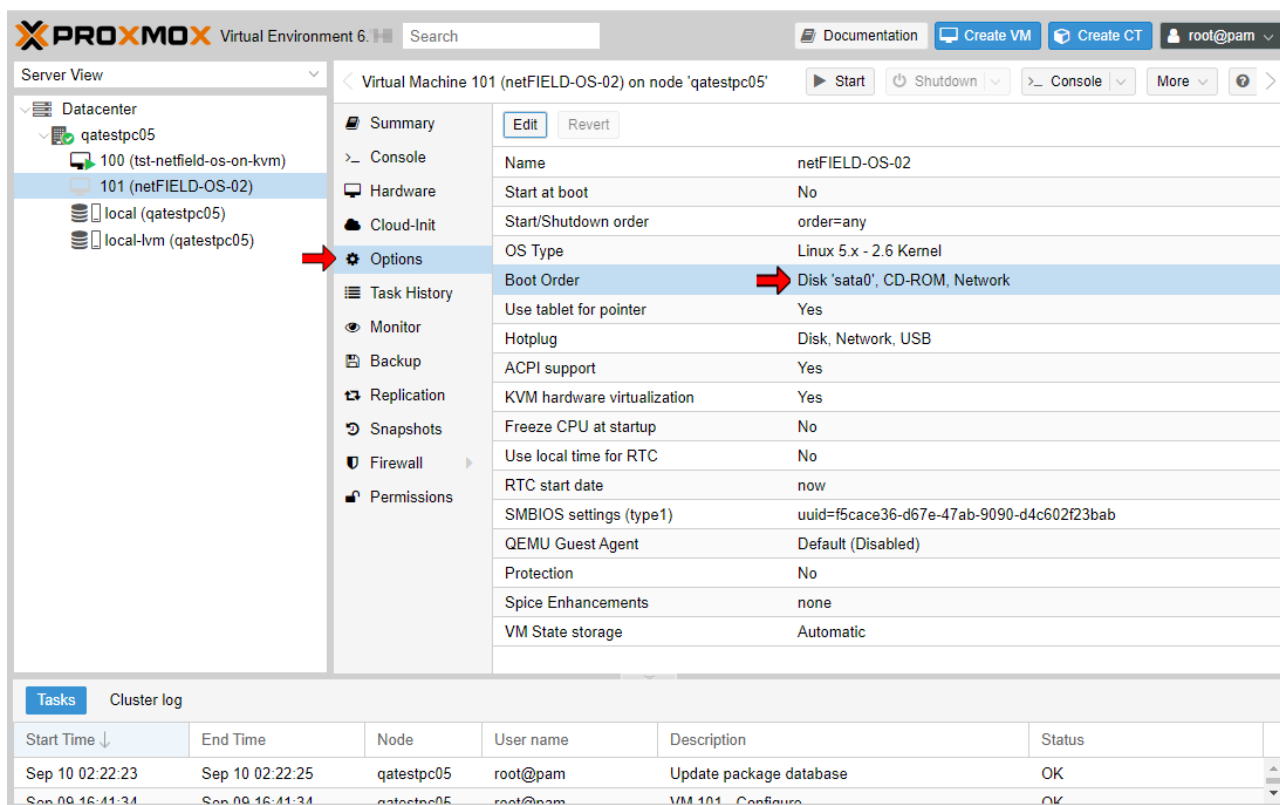


Figure 21: Check boot order

- If this is not the case, select the **Boot Order** parameter, click **Edit** button and select **Disk 'sata0'** for **Boot device 1** in the **Edit Boot Order** dialog:

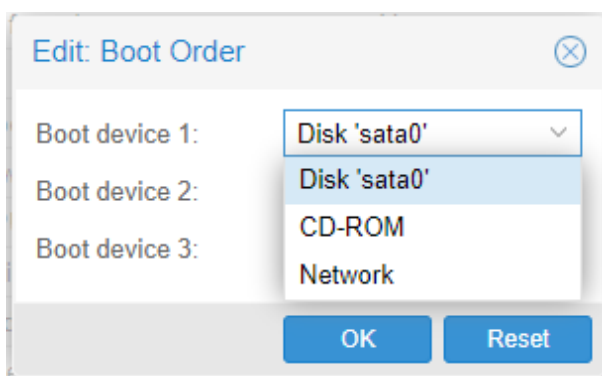


Figure 22: Edit boot order dialog

## 9. Change disk size (optional).

**Note:**

If you want to allow the netFIELD OS Datacenter more (or less) hard disk storage capacity, you must resize the Hard Disk *before starting* the virtual machine for the first time. This is because the hard disk gets partitioned on first starting-up of the virtual machine. If you want to diminish the hard disk storage capacity, we recommend you to allow at least 10 GB.

- In the **Hardware** panel of the netFIELD OS virtual machine, select the **Hard Disk (sata0)** parameter, then click **Resize disk** button. In the **Resize disk** dialog, increment or diminish the size according to your needs.
10. Start the netFIELD OS virtual machine.
- Click **Start** button then wait for a few seconds until the green arrow head next to the netFIELD OS virtual machine entry in the resources tree indicates that the machine is running.

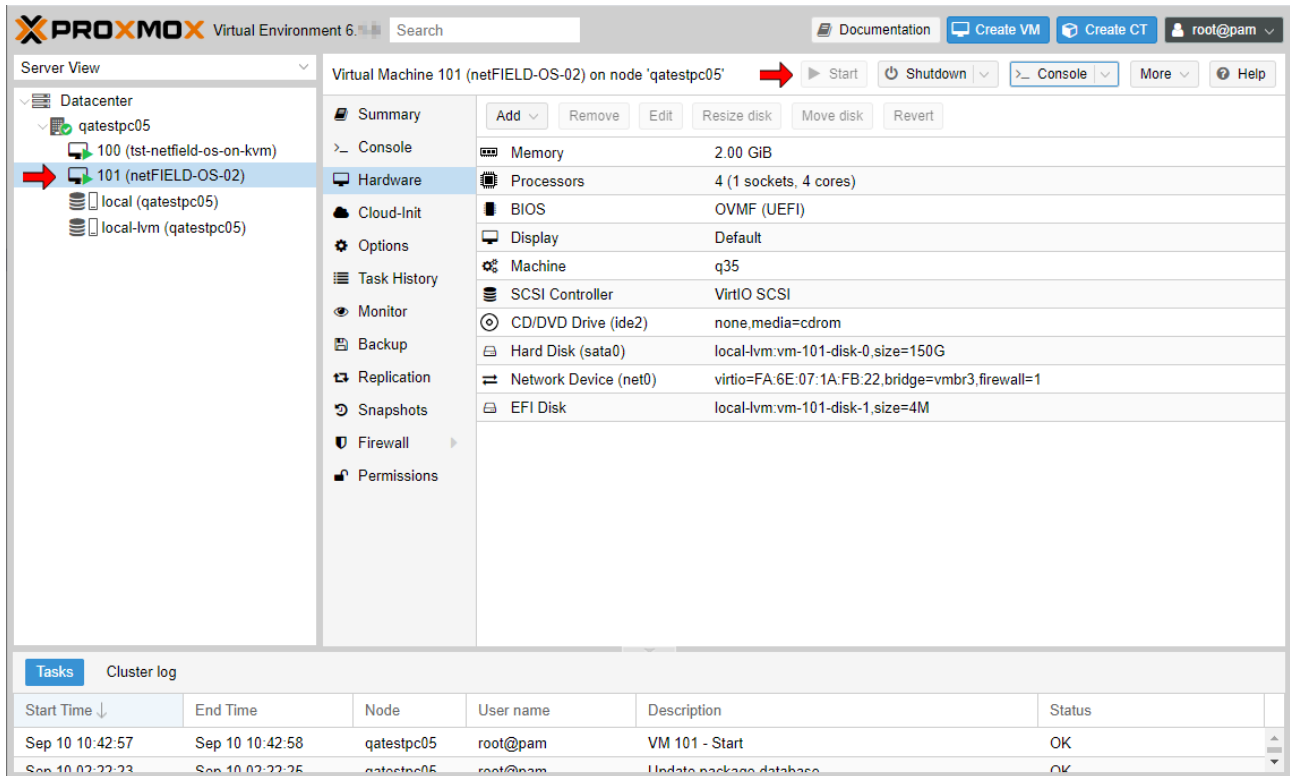


Figure 23: VM started

11. Open Console and display IP Address of the netFIELD OS.

- Click **Console** button to open the console.
- ⇒ At first – depending on the current booting stage of the netFIELD OS – the console may only display booting information. Wait a short while until the netFIELD OS displays its static “welcome screen” showing its basic identification parameters along with its IP address and host name:

```
-----  
Welcome to netFIELD OS version 2.1.0.0  
  
Model Name : NIOT-E-UM-EN  
Hardware ID: b3175c7bc38b-7e3985ae8f60  
Host Name  : ntfa6e071afb22  
  
Please use your web browser for configuration - connect to:  
  
https://192.168.20.56  
https://ntfa6e071afb22  
  
-----  
  
ntfa6e071afb22 login:
```

Figure 24: Console

- ⇒ You have installed the netFIELD OS Datacenter under Proxmox VE. You can now connect to the Local Device Manager of the netFIELD OS with your web browser (see section *Establish LAN connection and login to Local Device Manager* [► page 37]).

## 4.3 Installation on VMware (ESXi)

This section describes how to install netFIELD OS Datacenter on VMware VSphere ESXi.

1. Download the \*.ova file from Hilscher to your local PC.
  - Go to the *netFIELD Software Overview* page <https://kb.hilscher.com/x/sSAfBw> and click on the link of the latest netFIELD OS version. Navigate to the *netFIELD OS Datacenter* section and download the netfield-image-niot-e-vm-en.ova file.
2. Create new virtual machine.
  - Connect to VMware ESXi.
  - In the **Navigator**, select **Host** or **Virtual Machines**, then click **Create/ Register VM** button in the header.

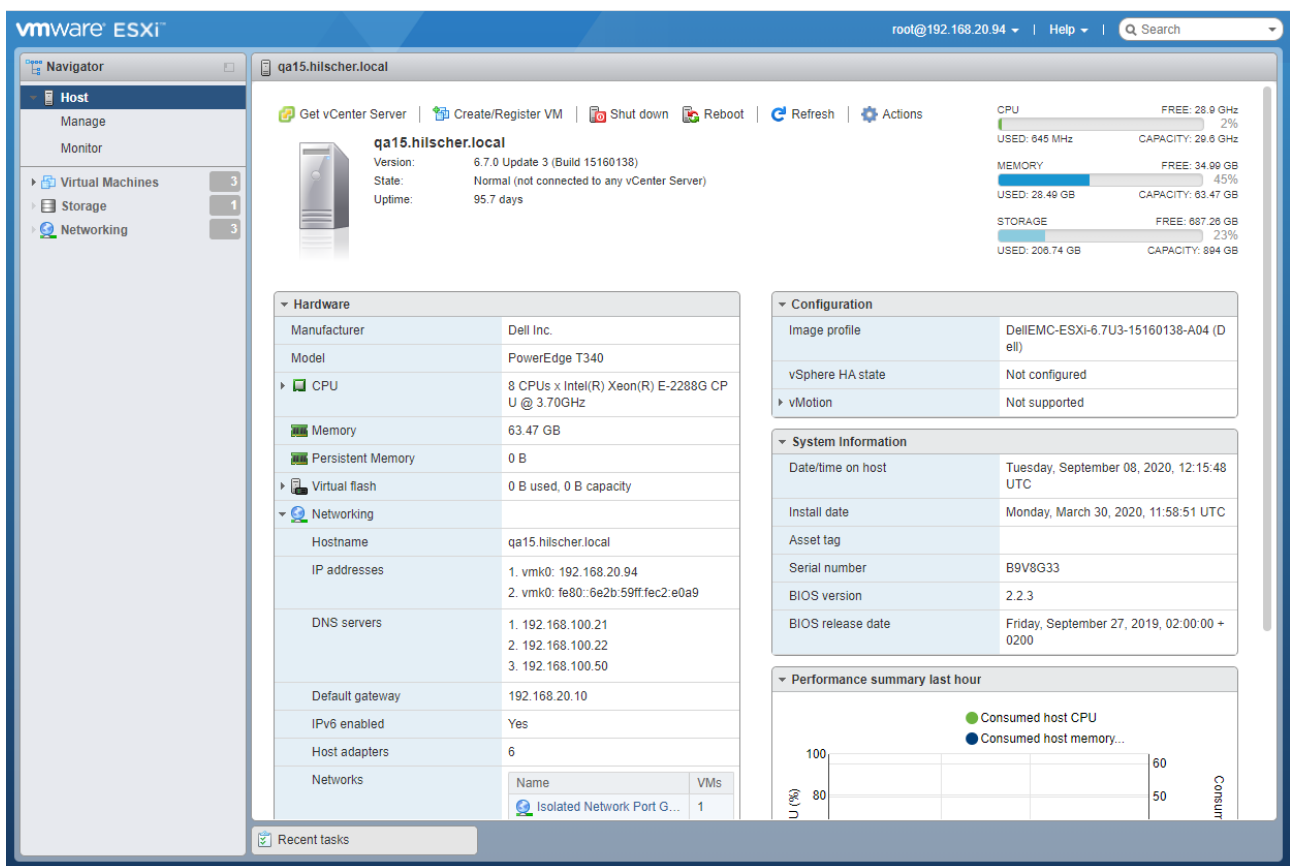


Figure 25: ESXi

- The **New virtual machine** wizard opens.

- In the **Select creation type** tab of the wizard, select **Deploy a virtual machine from an OVF or OVA** option.

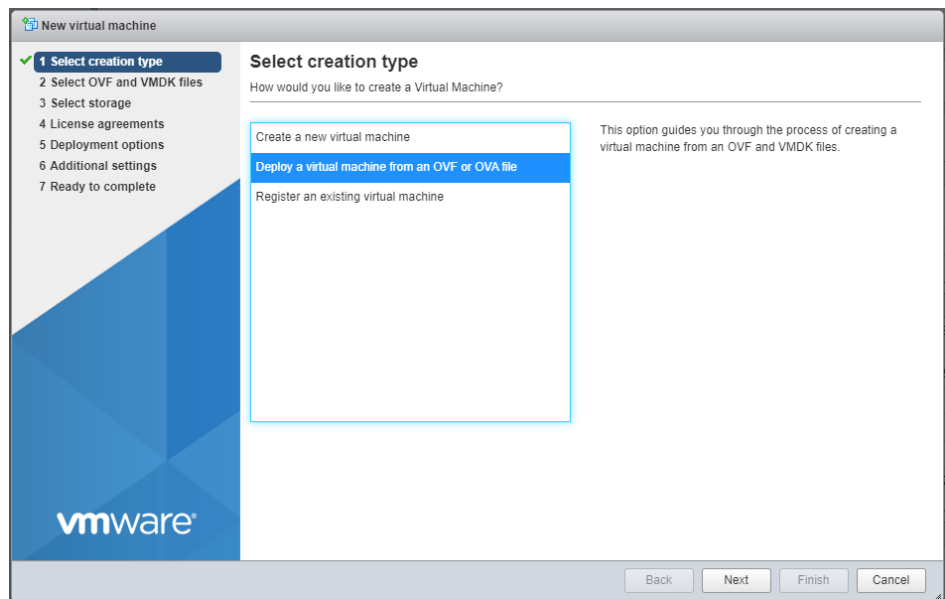


Figure 26: Select creation type

- In the **Select OVF and VMDK files** tab of the wizard, enter a name for the virtual machine and add the \*.ova file that you have downloaded from Hilscher.

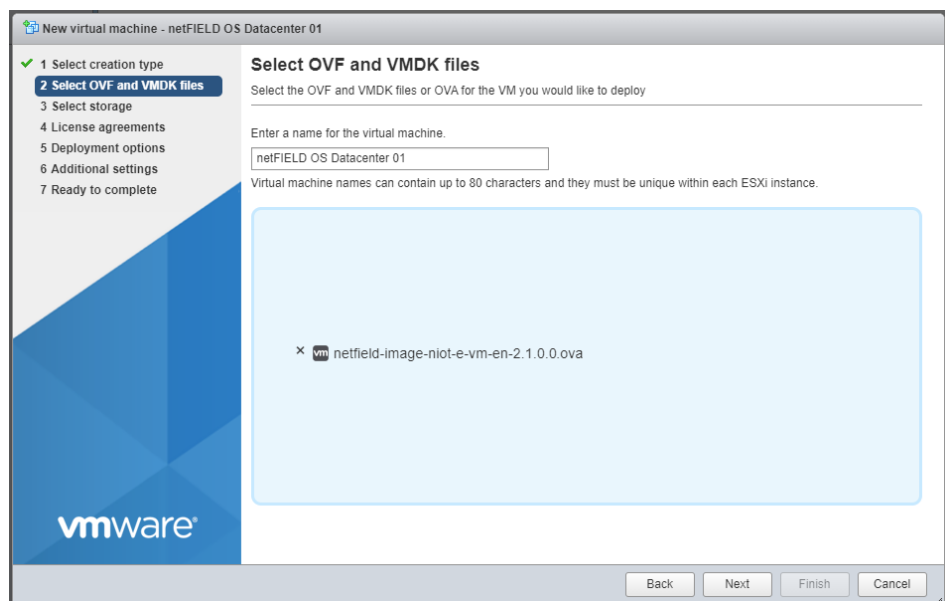


Figure 27: Select OVF and VMDK files

- In the **Select storage** tab of the wizard, select the storage location for your netFIELD OS virtual machine.

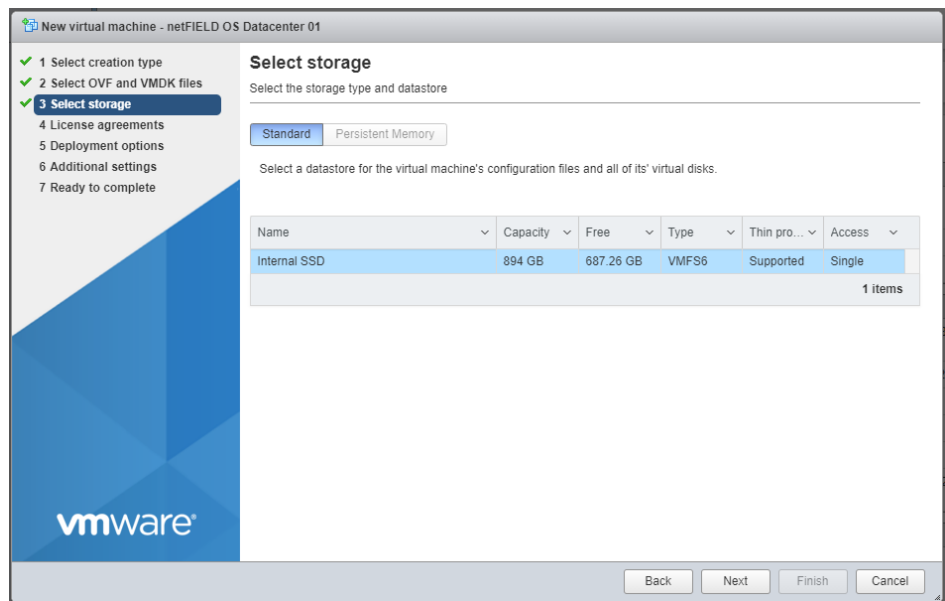


Figure 28: wizard3

- In the **Deployment options** tab of the wizard, you must assign to your netFIELD OS a suitable virtual network in the **VM Network** drop-down menu. This virtual network serves as a connection between the netFIELD OS to a physical network interface device on your host system.



**Note:**

The assigned network must be connected to a DHCP Server and it must be reachable from “outside” via TCP/IP. This means that you must configure the network environment of your host system accordingly.

Note also that you can add further network interfaces to the virtual machine later, after having finished the wizard.

- Leave the **Disk provisioning** parameter at their default setting *Thin*.

**Important:**

If you want to allow the netFIELD OS Datacenter more (or less) than the 16 GB hard disk storage capacity predefined in the \*.ova file, you must uncheck the **Power on automatically** option. You do not want the automatic power-on in this case because you must reconfigure the hard disk storage capacity *before starting* the virtual machine for the first time. (The hard disk gets partitioned on first starting-up of the virtual machine, which allows no subsequent reconfiguration). Note that you should allow at least 10 GB of hard disk storage.

The screenshot shows the 'New virtual machine - netFIELD OS Datacenter' wizard. On the left, a progress bar indicates the steps: 1 Select creation type, 2 Select OVF and VMDK files, 3 Select storage, 4 Deployment options (selected), and 5 Ready to complete. The main area is titled 'Deployment options' and contains a table with the following settings:

Select deployment options	
Network mappings	VM Network: VM Network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick
Power on automatically	<input checked="" type="checkbox"/>

At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

Figure 29: Deployment options

- In the **Ready to complete** tab, click Finish button.

The screenshot shows the 'New virtual machine - netFIELD OS Datacenter 01' wizard. On the left, the progress bar shows steps 1 through 5, with '5 Ready to complete' selected. The main area is titled 'Ready to complete' and contains a table summarizing the settings:

Review your settings selection before finishing the wizard	
Product	netFIELD OS
VM Name	netFIELD OS Datacenter 01
Files	netfield-image-niot-e-vm-en-2.1.0.0.debug.nightly-389-20200908185247-disk1.vmdk
Datastore	Internal SSD
Provisioning type	Thin
Network mappings	VM Network: VM Network
Guest OS Name	Unknown

Below the table, there is a yellow warning triangle icon and the text: 'Do not refresh your browser while this VM is being deployed.' At the bottom right, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'.

Figure 30: Ready to complete

- The wizard closes and after a short while the new virtual machine is displayed in the **Virtual Machines** list:

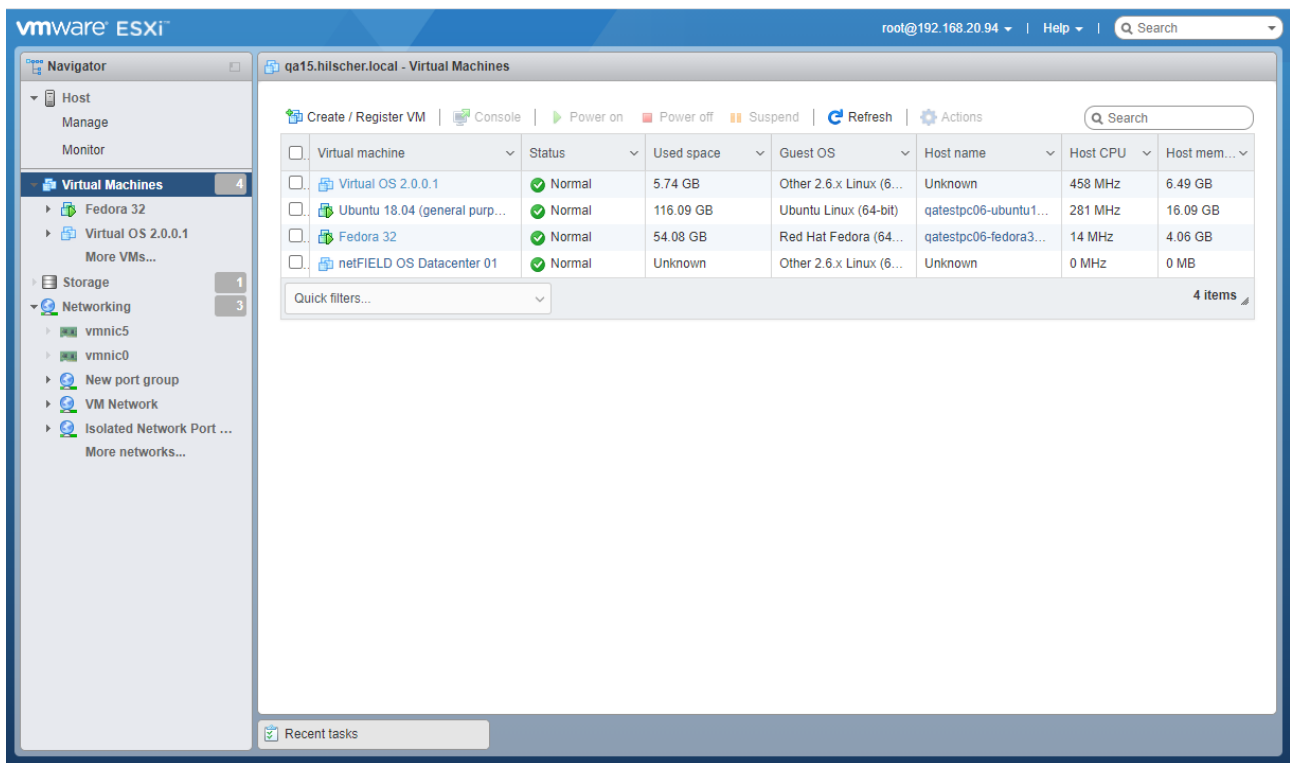




Figure 31: New virtual machine created

- If you have selected the **Power on automatically** option in the wizard, the blue power icon next to the virtual machine will change after a short while from blue  to green , indicating that the netFIELD OS Datacenter is up and running. You can now proceed to open the console and check the assigned IP address of the netFIELD OS (see step 4: *Open Console and display IP Address of the netFIELD OS virtual machine*).

### 3. Change hard disk size (optional).



#### Note:

If you have unchecked the **Power on automatically** option in the wizard because you want to allow the netFIELD OS Datacenter more hard disk storage capacity, you can now resize the hard disk (this must be done *before starting* the virtual machine for the first time because the hard disk gets partitioned on first starting-up of the virtual machine.)

- Select the netFIELD OS virtual machine, then click **Edit** button in the header.

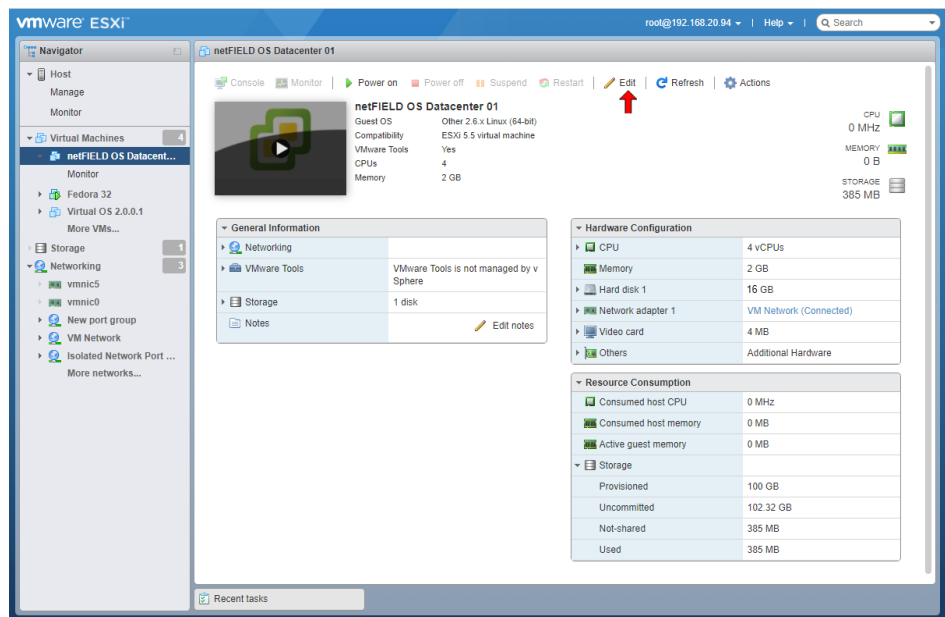


Figure 32: Edit VM

- In the **Edit settings** dialog, enter the new size in the **Hard disk** field, then click **Save** button.

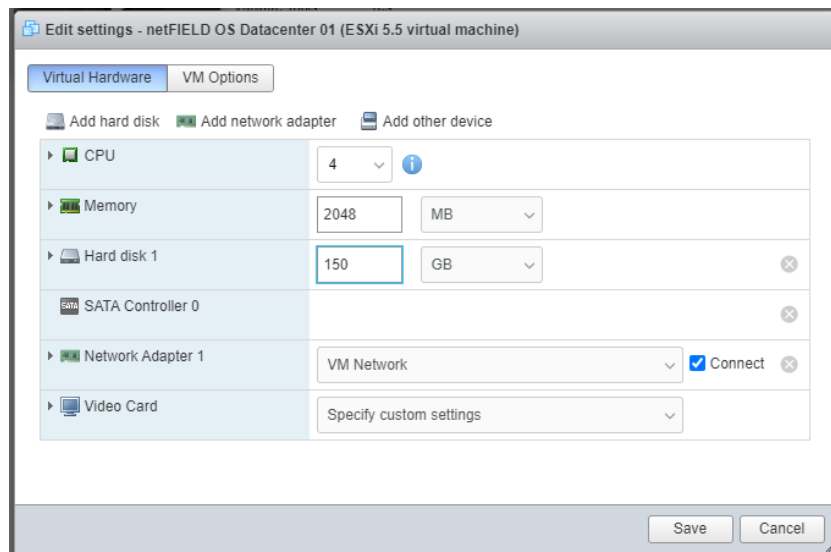


Figure 33: Edit hard disk size

- After having resized the hard disk, you can now start the netFIELD OS virtual machine by clicking the **Power on** button in the header.
4. Open Console and display IP Address of the netFIELD OS virtual machine.
    - Click the **Console** button and select e.g. **Open browser console** from the drop-down menu.

- ⇒ At first – depending on the current booting stage of the netFIELD OS – the console may only display booting information. Wait a short while until the netFIELD OS displays its static “welcome screen” showing its basic identification parameters with its IP address and host name:

```
-----  
Welcome to netFIELD OS version 2.1.0.0.debug.nightly-389  
  
Model Name : NIOT-E-VM-EN  
Hardware ID: 33fc77c15aef-64ff3809b71a  
Host Name  : nt000c295dbdcc  
  
Please use your web browser for configuration - connect to:  
  
https://192.168.20.57  
https://nt000c295dbdcc  
  
-----  
  
nt000c295dbdcc login:
```

Figure 34: Console

- ⇒ You have installed the netFIELD OS Datacenter under VMware ESXi. You can now connect to the Local Device Manager of the netFIELD OS with your web browser (see section *Establish LAN connection and login to Local Device Manager* [▶ page 37]).

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

The netFIELD OS virtual machine should have obtained an IP address from the DHCP server after start-up, which allows you to access the web-based management GUI of the netFIELD OS, called **Local Device Manager**. If you know the IP address that the DHCP server has assigned to your netFIELD OS virtual machine, you can now access it directly by entering its IP address into the address bar of your web browser. If you do not know the IP address, you can use the Windows network environment to connect with it.



---

**Note:**

If the netFIELD OS realizes that no DHCP service is available, it switches the port 1 (eth0) LAN interface address configuration to *IPv4 link local* mode ("fallback" setting). An IPv4 link local address uses an address range from 169.254.0.0 to 169.254.255.255. The netFIELD OS outputs its hostname and its IP address (the IPv4 link local address or the address which it has received from the DHCP server) at the console.

---

1. Establish connection to the netFIELD OS.

- Enter into your web browser the IP address that the DHCP server assigned to the netFIELD OS virtual machine.
- Your browser connects to the **Local Device Manager**, which is the graphical user interface of the netFIELD OS.



---

**Note:**

The netFIELD OS contains a certificate issued by Hilscher. Your browser will therefore issue an "unsecure connection" warning 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 netFIELD OS 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: Connecting via Windows network environment

Because the netFIELD OS 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 netFIELD OS virtual machine 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/virtual machines in the network, open your **Windows Explorer** and select **Network**.
- You will find the netFIELD OS virtual machine listed under **Other Devices**:



NIOT-E-VM-EN  
(ntfa6e071afb22)

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

#### 2. Login to the **Local Device Manager**.



Figure 35: Sign In dialog of Local Device Manager

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

- For security reasons, you are now forced to change the default `admin` password immediately.
- In the **Current password** field, enter `admin` once again, then click **Sign In** button:

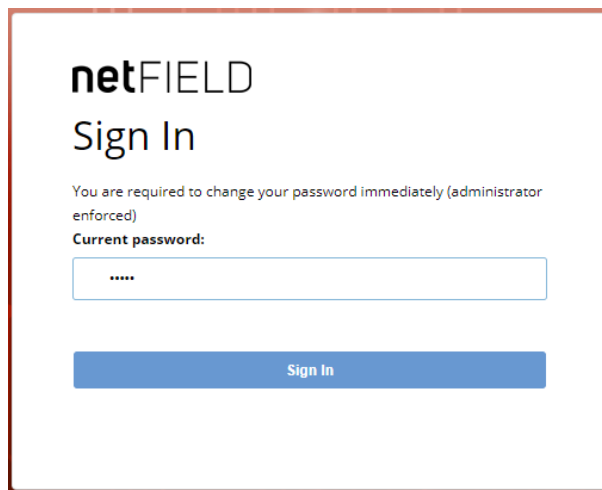
The image shows a web interface for 'netFIELD Sign In'. At the top, the text 'netFIELD Sign In' is displayed. Below it, a message states: 'You are required to change your password immediately (administrator enforced)'. Underneath this message is the label 'Current password:' followed by a text input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

Figure 36: Enter current password dialog

- The **New password** dialog opens:


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

Figure 37: Enter new password dialog

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



**Note:**

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

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

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

Figure 38: Re-Authentication dialog

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

## 4.5 Set system time

By default, the **Time Zone** of the netFIELD OS is set to **UTC** and the synchronization method (**Set Time**) to **Automatically using NTP** (Network Time Protocol service).

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

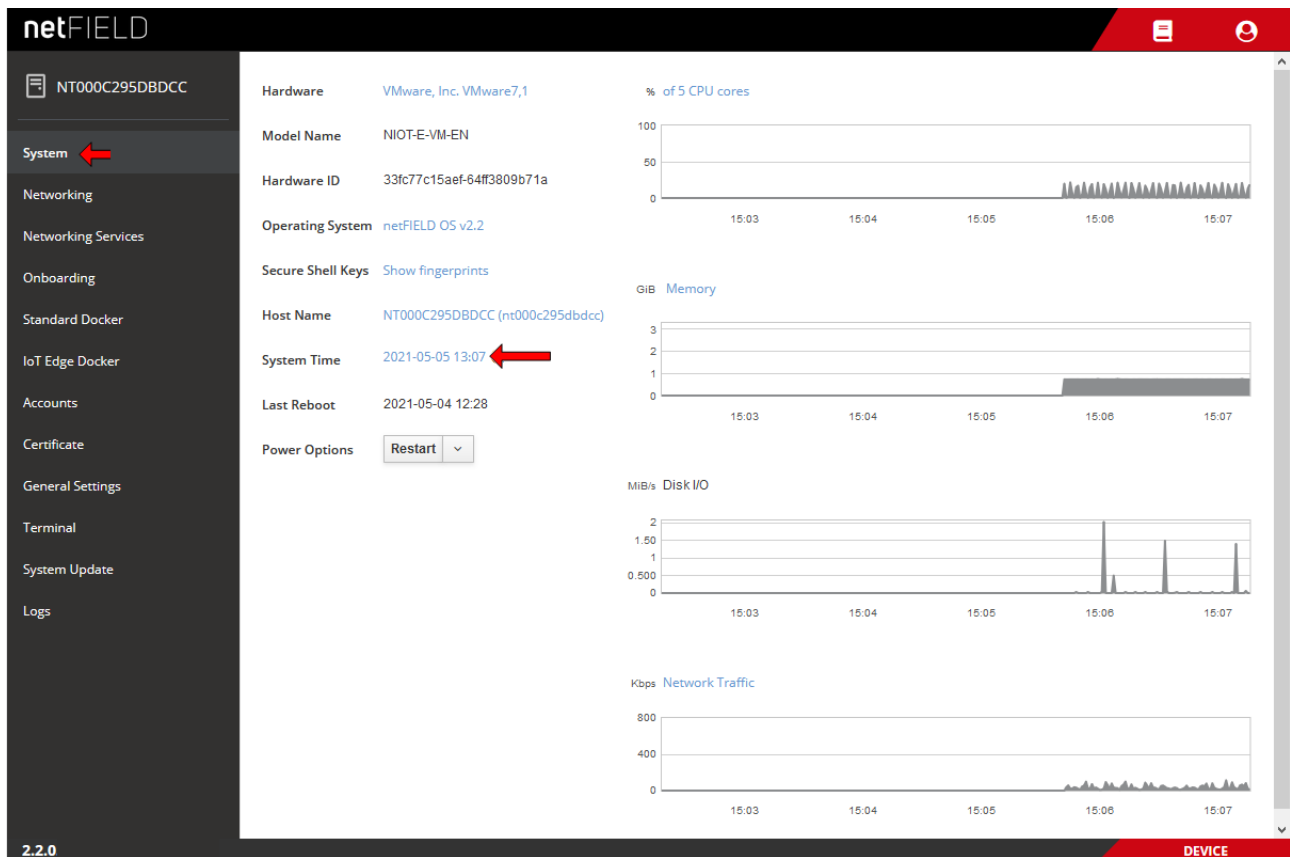


Figure 39: System time value

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

Figure 40: Change System Time dialog

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

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

The screenshot shows a web-based dialog titled "Change System Time". It contains a "Time Zone" dropdown menu currently showing "Europe/Berlin". Below it is a "Set Time" dropdown menu showing "Automatically using specific NTP servers". Underneath the "Set Time" menu is a list of NTP servers. The first entry is "ptbtime1.ptb.de" and the second is "ntp.uni-regensburg.de". Each entry has a small "x" button to its right for removal and a small "+" button for adding more servers. At the bottom of the dialog are two buttons: "Cancel" and "Change".

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

## 4.6 "Onboard" (register) netFIELD OS in the netFIELD Portal

### 4.6.1 Overview

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

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

This process is initialized by the netFIELD OS itself, not by the portal.

There are three different onboarding methods: **Zero-Touch**, **Basic** and **Advanced**.

With the **Zero-Touch** method, the netFIELD OS 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, not in the netFIELD OS Datacenter.

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 netFIELD OS on the local level, 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 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.

## 4.6.2 Onboarding using the “Basic” method

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

The screenshot displays the 'netFIELD' Local Device Manager interface. On the left, a dark sidebar contains a navigation menu with items like System, Networking, Onboarding (highlighted with a red arrow), Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, and Logs. The main area is titled 'Onboarding Method' and shows 'Manual' as the selected method. It also displays 'Status' as '--', 'API Endpoint' as '--', 'Hardware Id' as '33fc77c15aef-64ff3809b71a', and 'Environment' as '--'. Below this, there are tabs for 'Basic' and 'Advanced'. The 'Basic' tab is active, showing fields for 'Environment' (a dropdown menu), 'Device Name', 'E-Mail', 'Password', and 'Upstream Protocol' (a dropdown menu). There is also a checkbox for 'Use Manifest'. At the bottom of the form is a blue 'Onboard' button. The bottom of the page shows the version '2.2.0' on the left and 'DEVICE' on the right.

Figure 41: “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 netFIELD OS shall be displayed in the portal (in the portal, the netFIELD OS virtual machine is labelled and handled as “device”).
- 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 netFIELD OS 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*, DOC1907010IxxEN.

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

**Note:**

The deployment manifest causes certain software containers defined in the manifest to be automatically installed on your netFIELD OS. (For further information on deployment manifests, see section *Deployment Manifest* in the *netFIELD Portal* manual, DOC1907010IxxEN)

- Click **Onboard** button to start the onboarding process.
- ⇒ The netFIELD OS 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 netFIELD OS will be listed in the portal’s **Device Manager** as “device” and can be managed from there.

**Note:**

If the message “Something went wrong – Device has already been created” appears, the netFIELD OS “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 netFIELD OS “device” in the portal, and then start the “Basic” onboarding procedure here locally for a second time.

### 4.6.3 Onboarding using the “Advanced” method

**Requirements**

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

**Step-by-step instructions**

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

The screenshot shows the netFIELD Local Device Manager interface. The left sidebar contains a navigation menu with the following items: System, Networking, Networking Services, Onboarding (highlighted with a red arrow), Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, and Logs. The main content area is titled 'Onboarding Method' and shows the 'Advanced' tab selected. The 'Hardware Id' field is highlighted with a red arrow and contains the value '33fc77c15aef-64ff3809b71a'. Below this, there are input fields for 'API Endpoint', 'API Key', and 'Activation Code', and a dropdown for 'Upstream Protocol' set to 'AMQP'. A red arrow points to the 'Onboard' button at the bottom.

Figure 42: Copy 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 netFIELD OS in your first browser tab.
- 2. Add the netFIELD OS as “device” in the portal and create **Activation Code**.
  - In the portal, open the **Device Manager**.
  - On the start page (**Manage your devices**) of the **Device Manager**, select **+ Add** button.
  - The **Add Device** mask opens:

Figure 43: “Add device” mask in netFIELD Portal

- Copy the netFIELD OS’s hardware ID from your clipboard into the **Hardware ID** field.
- In the **Name** field, enter a name for your netFIELD OS (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 operating instruction manual *netFIELD Portal*, DOC190701OIxxEN.

- Click **Save** button.

- The mask closes, and the **Overview** page of the newly created netFIELD OS “device” opens, showing the **Activation Code** that you will have to enter locally in your netFIELD OS:

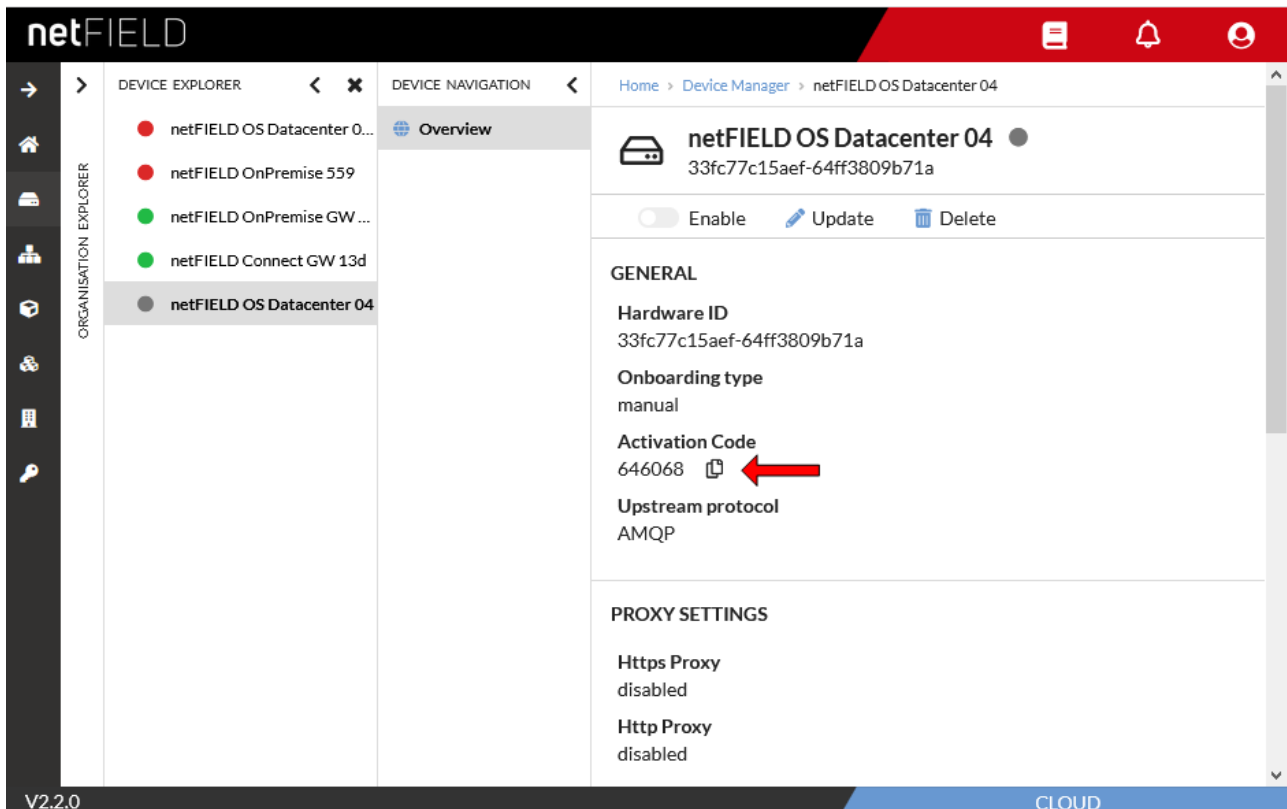



Figure 44: Activation Code in portal

- Copy the **Activation Code** to your clipboard. You can use the  button for this.



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

**Important:**

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

**Note:**

If necessary, you can change the upstream protocol in the netFIELD Portal after onboarding. See section *Device Navigation: Edit device settings (Update mask)* in the operating instruction manual *netFIELD Portal*, DOC1907010IxxEN.

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

**Note:**

The deployment manifest causes certain software containers defined in the manifest to be automatically installed on your netFIELD OS. (For further information about deployment manifests, see section *Deployment Manifest* in the *netFIELD Portal* manual, DOC1907010IxxEN)

- Click **Onboard** button, to start the onboarding process.
- ⇒ The netFIELD OS connects to the portal and is registered there as new "device". 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 netFIELD OS during onboarding.

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

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


For information on how to create a new API Key, see section *Create/edit API key* in the *netFIELD Portal* manual, DOC1907010IxxEN.

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

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

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

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

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

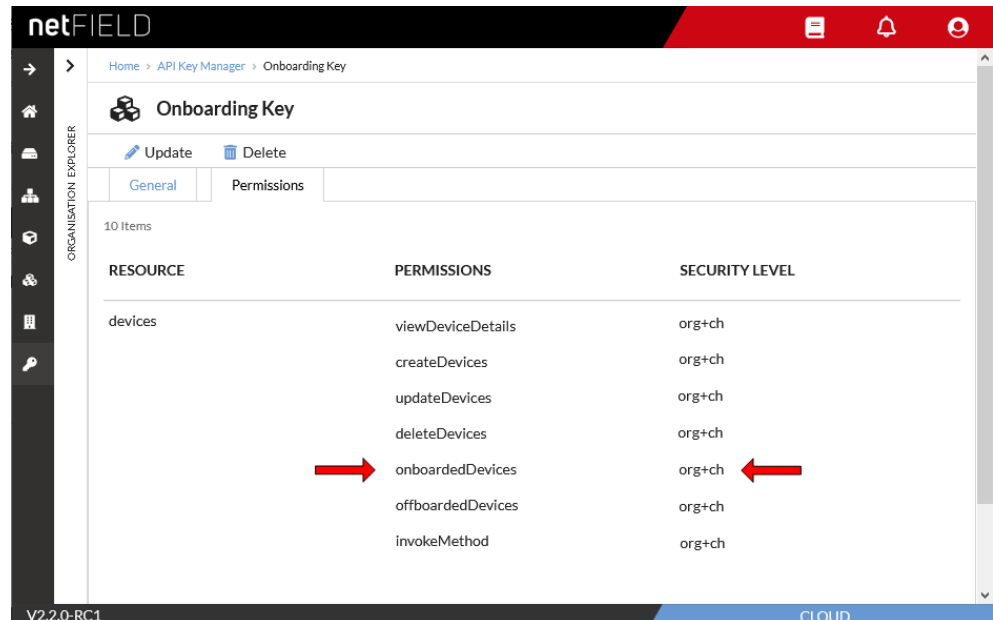

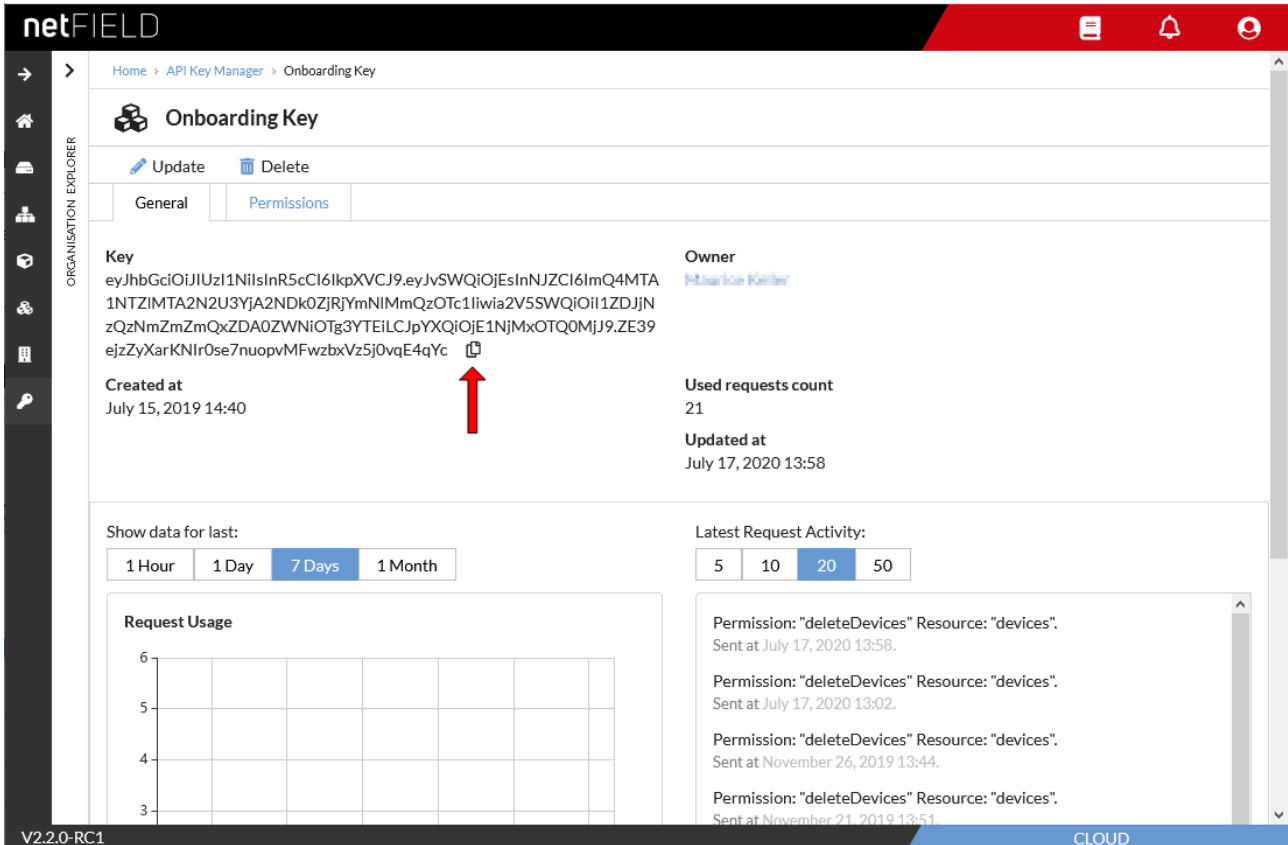


Figure 46: Example of an API Key permitting to onboard devices

- To copy the API Key in order to use it in the Local Device Manager of the netFIELD OS for the advanced onboarding process, change into the **General** tab.

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



The screenshot shows the netFIELD web interface. The breadcrumb navigation is Home > API Key Manager > Onboarding Key. The page title is 'Onboarding Key'. There are 'Update' and 'Delete' buttons. The 'General' tab is selected. The 'Key' field contains a long alphanumeric string: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJvSWQoOiJEsInNJZCI6ImQ4MTA1NTZIMTA2N2U3YjA2NDk0ZjRjYmNIMmQzOTc1Iiwia2V5SWQoOiI1ZDJjNzQzNmZmZmQxZDA0ZWNiOTg3YTEILCJpYXQiOiJ1NjMxOTQ0MjJ9.ZE39ejzZyXarKNlr0se7nuopvMFwzbxVz5j0vqE4qYc. A red arrow points to the copy icon next to this key. The 'Owner' is 'Markus Reiter'. The 'Created at' date is 'July 15, 2019 14:40'. The 'Used requests count' is '21'. The 'Updated at' date is 'July 17, 2020 13:58'. Below this, there are filters for 'Show data for last:' (1 Hour, 1 Day, 7 Days, 1 Month) and 'Latest Request Activity:' (5, 10, 20, 50). The 'Request Usage' section shows a grid with 6 rows and 7 columns. The 'Latest Request Activity' section shows a list of requests with permission 'deleteDevices' and resource 'devices'.

Figure 47: Copy key to clipboard

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

## 5 Local Device Manager

### 5.1 Overview

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



**Note:**

In this *Local Device Manager* chapter, the netFIELD OS Datacenter is sometimes referred to as “device”.

#### Description of the GUI

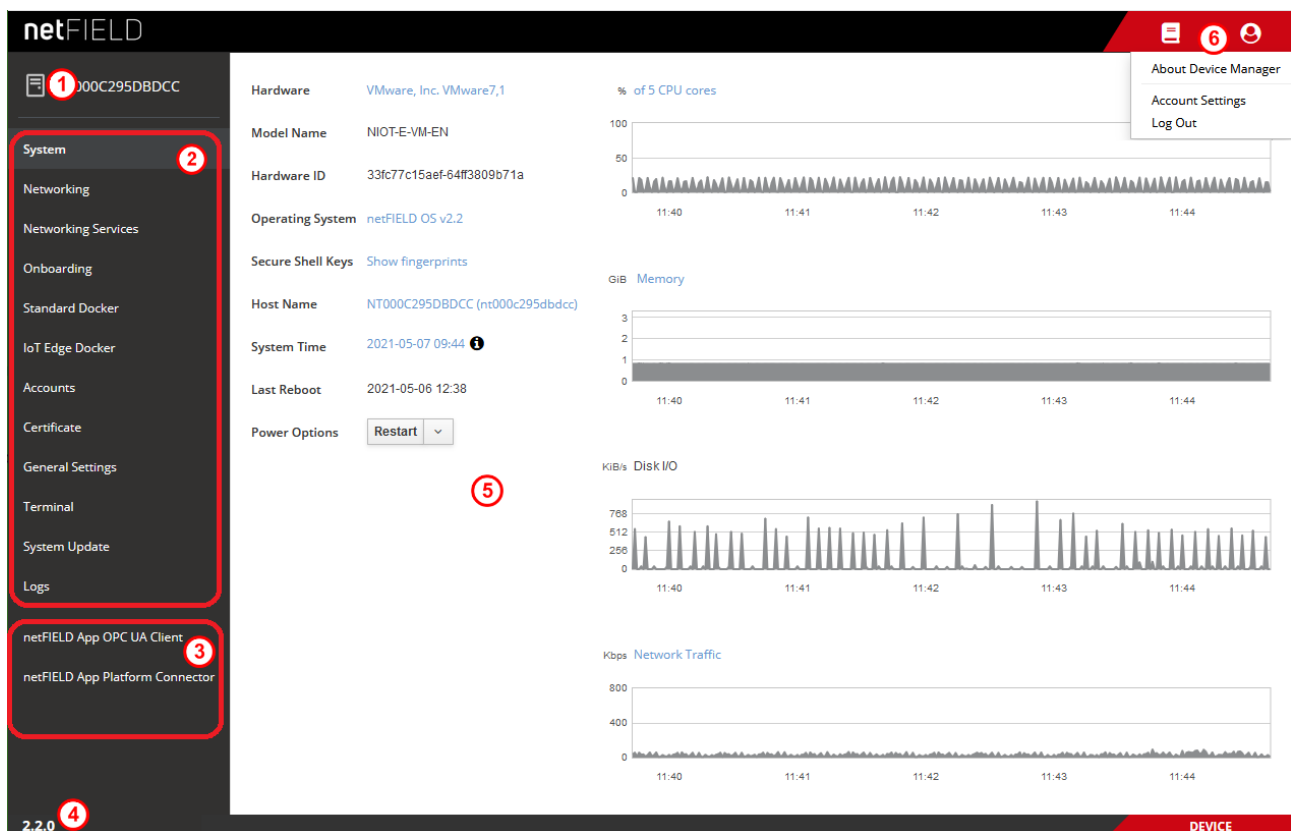


Figure 48: Overview Local Device Manager



- (1) “Pretty” host name of the device (can be adapted by the user, see subsection *Host Name* in section *System* [▶ page 55])
- (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 94] section for further information.
  - **Log Out:** Logs you out of the Local Device Manager

## 5.2 System

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

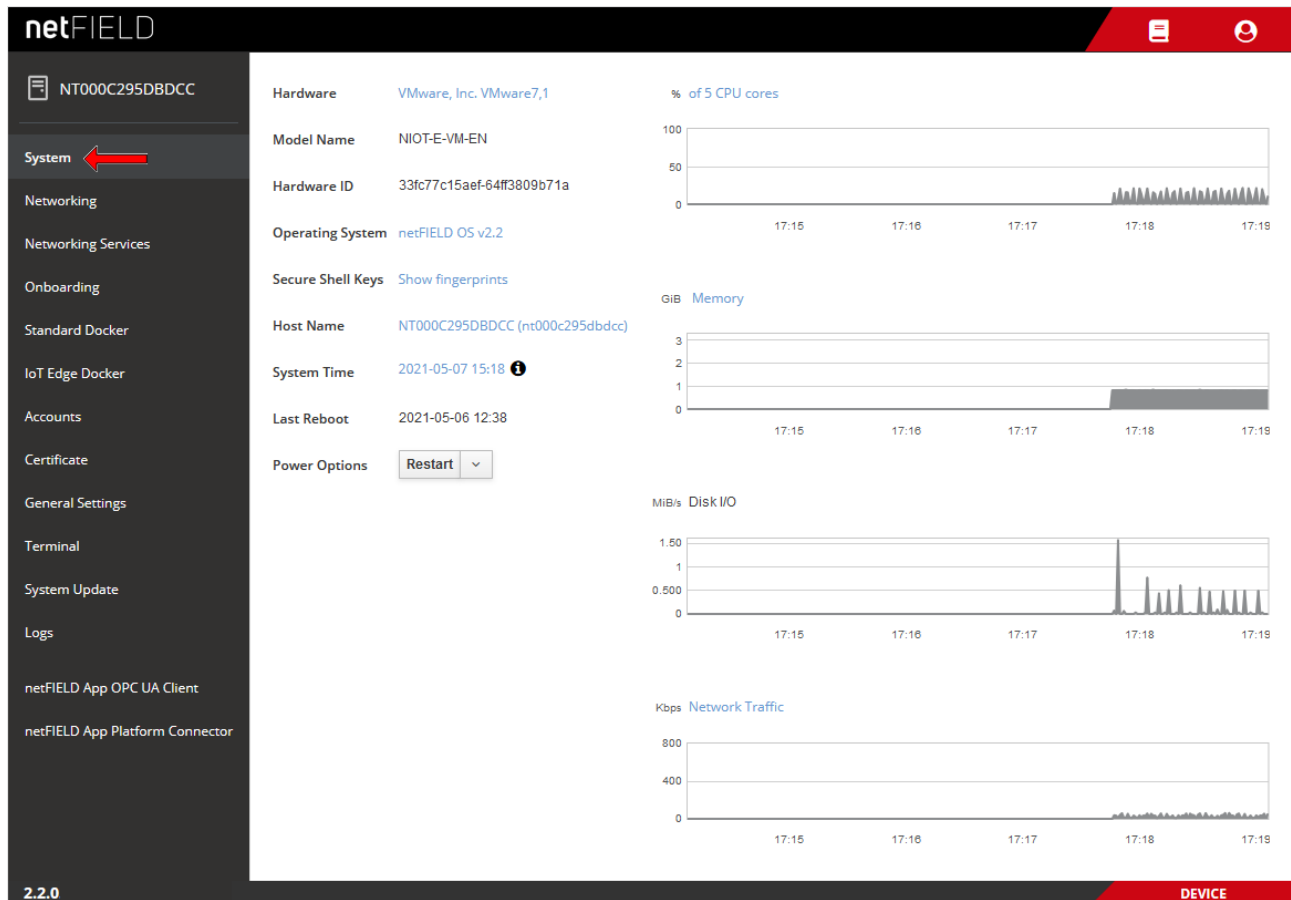


Figure 49: System page in Local Device Manager

### Hardware

Click on the blue name to open a page showing details about the hardware resources allocated to the netFIELD OS Datacenter; like CPU cores, RAM, mass storage, PCI etc. Information on the kernel version of the netFIELD OS is also displayed.

The hardware resources can be configured in the hypervisor of your virtualization environment (e.g. ESXi or Proxmox VE).

### Model Name

The netFIELD OS Datacenter can be identified by its model name **NIOT-E-VM-EN**.

### Hardware ID

Unique identification number of the netFIELD OS Datacenter “virtual machine”, randomly generated by the netFIELD OS itself. This ID is also used in the netFIELD Portal as unique identifier of your netFIELD OS Datacenter.

## 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 netFIELD OS Datacenter in a LAN or Wi-Fi network and can be used for connecting to it. By default, the name consists of the letters **NT** followed by the MAC address of the virtual network interface or bridge of the netFIELD OS.

If you want to change it, click on the blue name to open the **Change Host Name** dialog window.

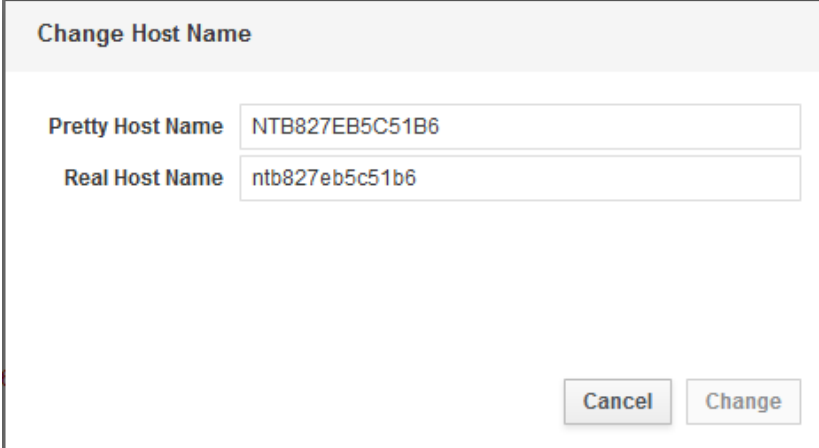
A dialog window titled "Change Host Name" with a light gray header. It contains two text input fields. The first field is labeled "Pretty Host Name" and contains the text "NTB827EB5C51B6". The second field is labeled "Real Host Name" and contains the text "ntb827eb5c51b6". At the bottom right of the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

Figure 50: 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 the tab of your browser.

**Real Host Name:** Equivalent to the transient host name which can be used to connect to the netFIELD OS and which can be changed by DHCP or mDNS at runtime. Can contain lower-case characters, digits, dashes and periods (with populated subdomains).

Setting this value takes immediate effect and does not require a restart.

## System Time

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

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

For instructions on how to change the time settings, see section Set system time.

### Last Reboot

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

### Power Options

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

### CPU cores

The graph shows the combined load of the allocated CPUs of the netFIELD OS during the last five minutes. Click on the blue **% of x 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 virtual network interfaces of the netFIELD OS.

## 5.3 Networking

### 5.3.1 Overview

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

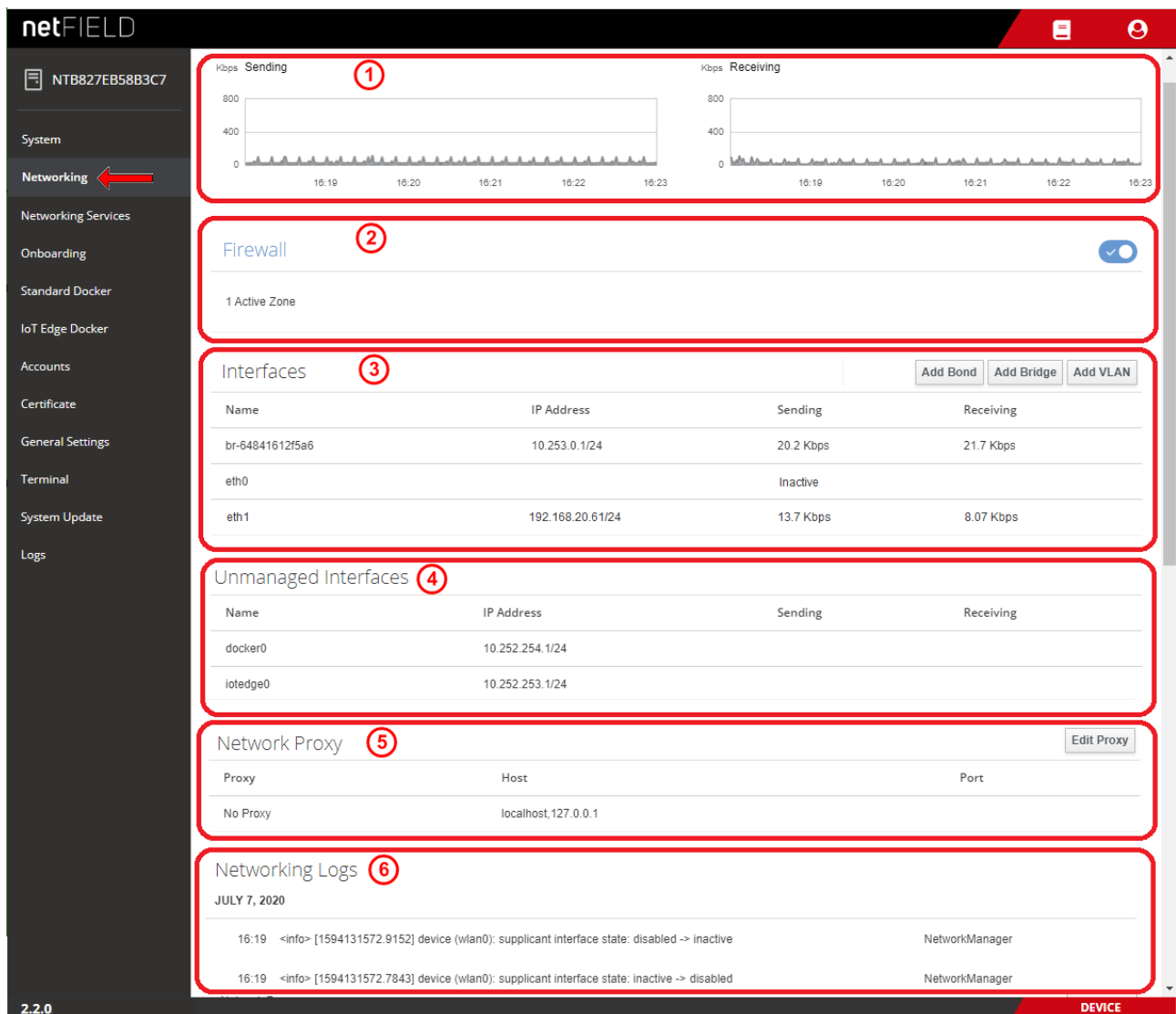


Figure 51: Networking page


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 63] 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, eth1 [...]**: These are the network interfaces that were assigned to the netFIELD OS Datacenter by the hypervisor.

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

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

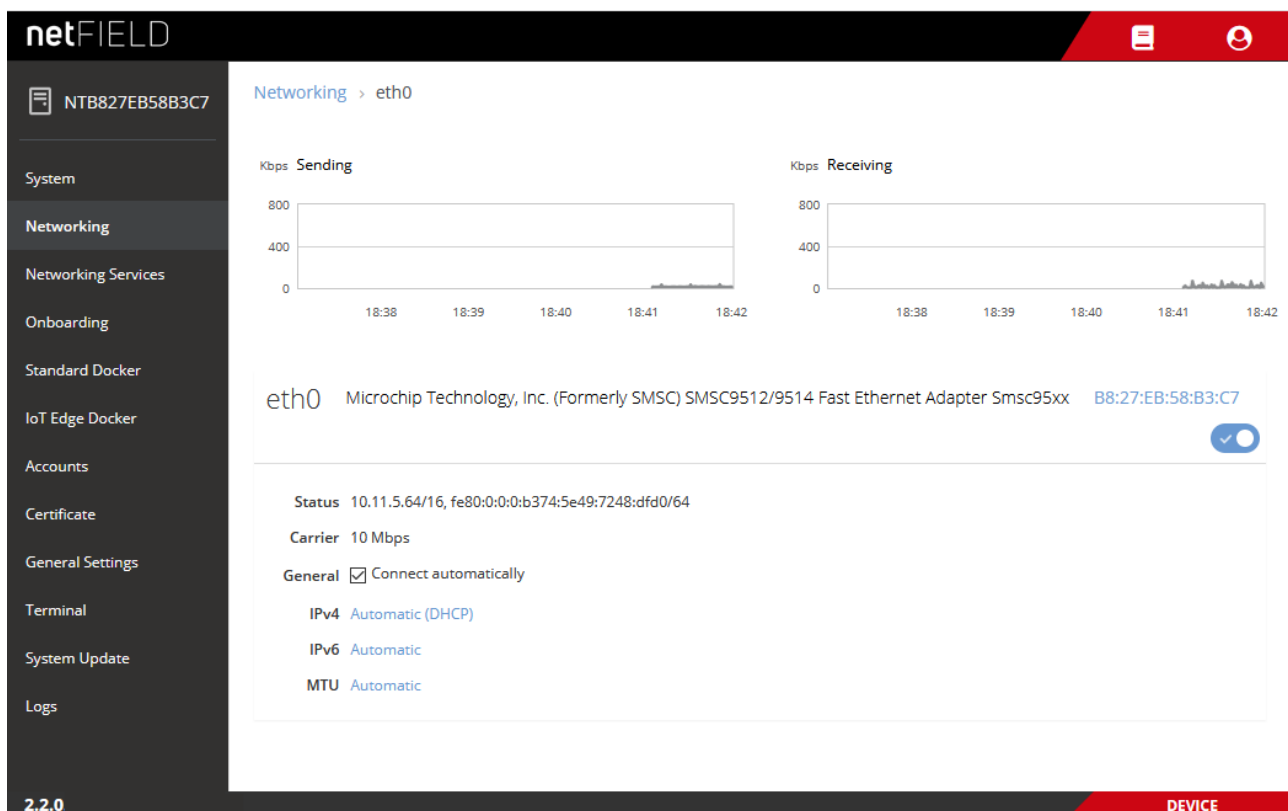



Figure 52: Details of LAN interface (eth0)

**Important:**

Be careful not to deactivate a network interface by switching it off with the  toggle switch. Once you have deactivated an interface, the connection to the netFIELD OS via this interface will be lost.

If you have deactivated all **eth** interfaces here (or if you have deactivated one interface without having configured the other interfaces properly), you can still reach the netFIELD OS via the virtual terminal (console) in the hypervisor.

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

```
sudo nmcli dev status
```

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

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

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

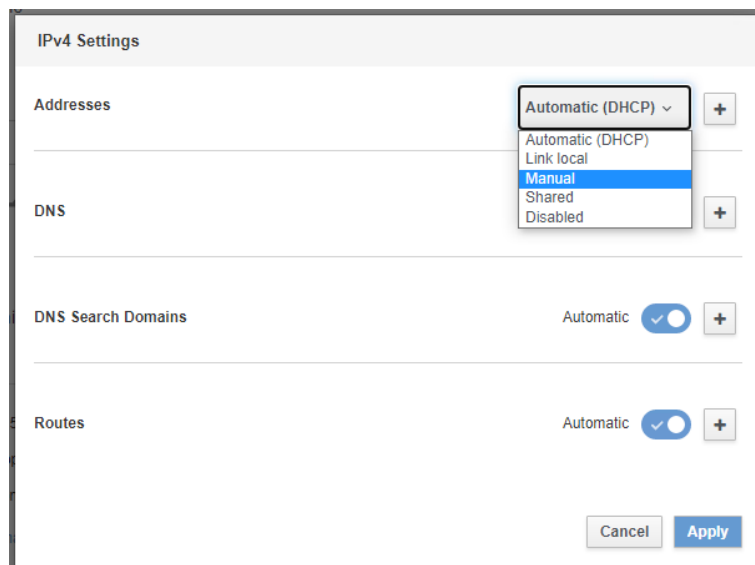


Figure 53: IPv4 Settings

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

The screenshot shows the 'IPv4 Settings' window. At the top, the 'Addresses' dropdown menu is open, showing 'Manual' as the selected option. Below this, there are three input fields: 'Address', 'CIDR Suffix or Netmask', and 'Gateway'. The 'DNS' section has a toggle switch labeled 'Automatic' which is turned on. The 'DNS Search Domains' section also has a toggle switch labeled 'Automatic' which is turned on. The 'Routes' section has a toggle switch labeled 'Automatic' which is turned on. At the bottom right, there are 'Cancel' and 'Apply' buttons.

Figure 54: 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
- **lotedge0**: Virtual interface (“bridge”) of the IoT Edge Docker
- **vethxxxxxxx**: Virtual interface (“virtual Ethernet device”) of a container in a Docker
- **sit0**: Tunneling protocol (“Simple internet transition”) for using IPv6 over an existing IPv4 connection.



#### Note:

The IP addresses of the “unmanaged interfaces” cannot be changed here. If you want to change the pre-configured IP address of the virtual interface of the Standard Docker (**docker0**) or of the IoT Edge Docker (**lotedge0**), e.g. because it conflicts with other IP addresses in your company network, see section *Docker Network Settings* [▶ page 102] 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.

## 5.3.2 Firewall

### Overview

netFIELD OS is equipped with a firewall.

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



---

#### Important:

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

---



---

#### Note:

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

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

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

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

---

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

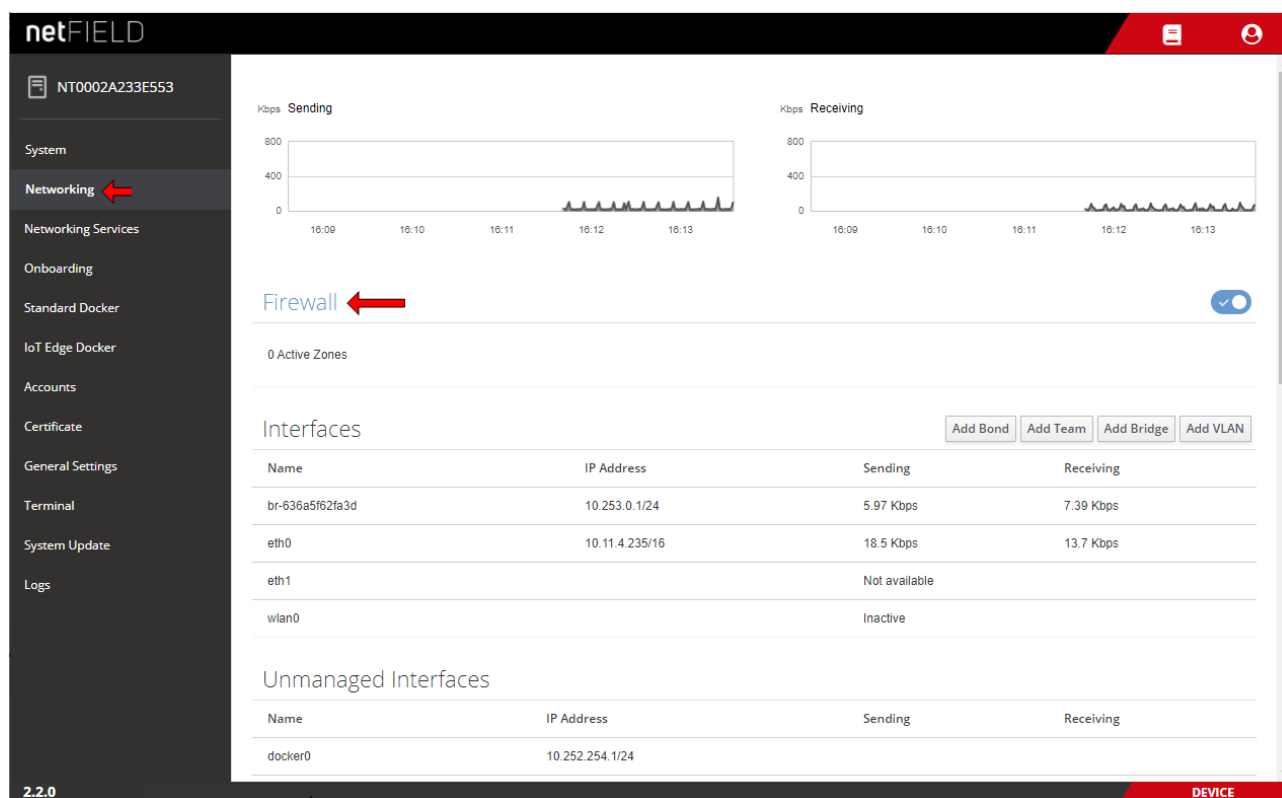


Figure 55: Open Firewall configuration page

- The Firewall configuration page opens:

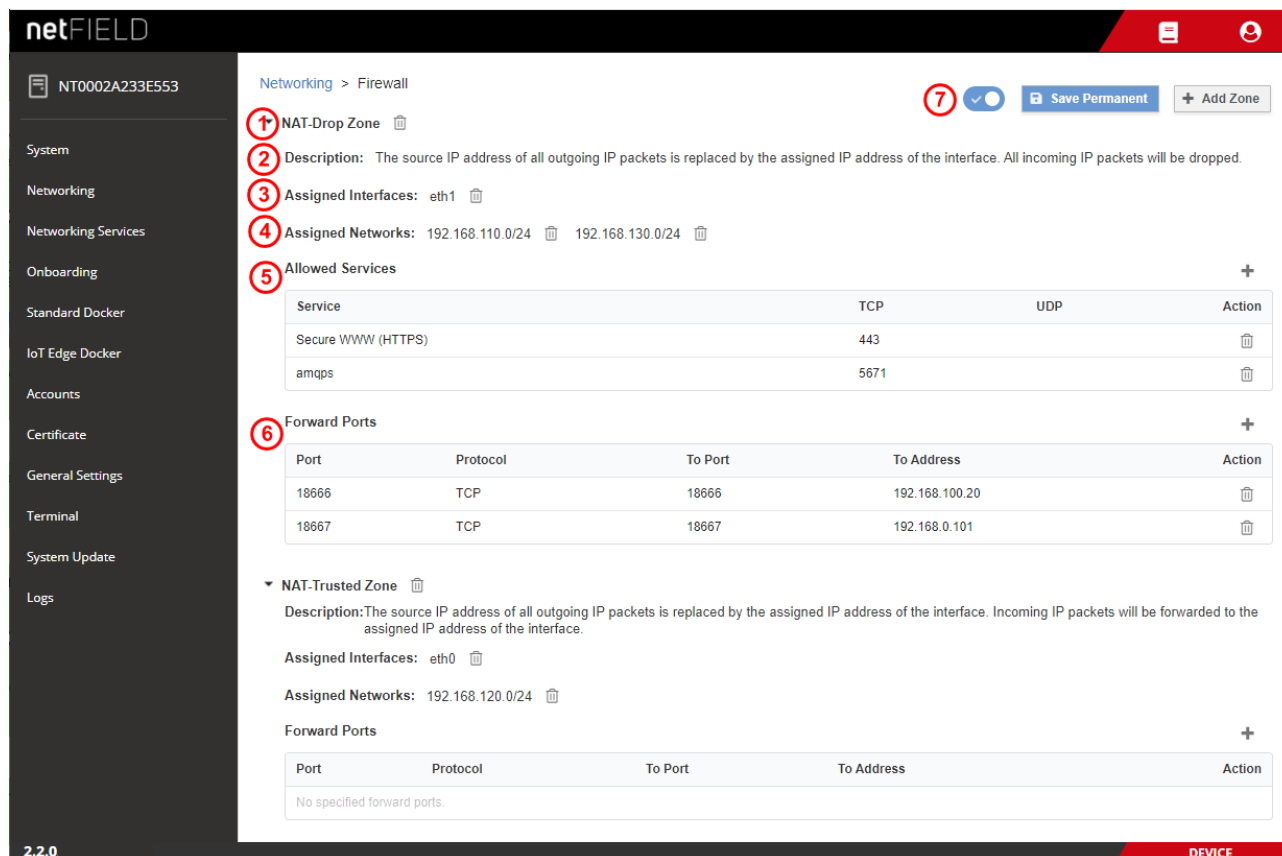


Figure 56: Elements on Firewall configuration page

## Zones

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

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

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

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

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

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

Table 6: Available Firewall zones

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

➤ The **Add Zone** dialog opens:

**Add Zone**

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

**Zones**  
☐ Drop
 ☒ NAT-Drop
 ☐ Block
 ☐ NAT-Trusted
 ☐ Trusted

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

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

**Assign Interfaces**  
☐ br-636a5f62fa3d
 ☐ eth0
 ☒ eth1
 ☐ wlan0

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

Cancel Add Zone

Figure 57: Add Zone dialog

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

Table 7: Elements in Add Zone dialog

## Description


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

## Assigned Interfaces

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

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

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

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

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


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

## Assigned Networks

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

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

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

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

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

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

## Allowed Services

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



### Note:

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



### Important:

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

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

Table 8: Columns/elements in Allowed Services table

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

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

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

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

Figure 58: Add services

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

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

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

☐ Services
 ☒ Custom Service

TCP ⓘ

6998

UDP ⓘ

UDP

Service name ⓘ \*

special service port

Cancel
 Add Custom Service

Figure 59: Add custom services dialog

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

## Forward Ports

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

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

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

Table 9: 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

Cancel

Add Port

Figure 60: 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 <b>Add Zone</b> dialog. In the <b>Add Zone</b> dialog, you can add a new active zone to your firewall configuration, or you can assign new interfaces or “networks” (subnets/IP address ranges) for an already existing active zone (i.e. for a zone that has already been added to your firewall).

Table 10: Control elements in main toolbar

### 5.3.3 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 your netFIELD OS will be able to communicate with the cloud, we strongly recommend you to configure the proxy settings *before onboarding* the netFIELD OS. The local proxy settings of the netFIELD OS 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 in the netFIELD OS after their deployment.

Note also that if you change the proxy settings locally in your netFIELD OS *after onboarding*, you must “synchronize” the settings with the netFIELD Portal in order to keep the settings there “up-to-date” (to synchronize, open the **Onboarding** page in the Local Device Manager, then click **Synchronize** button).

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

The screenshot displays the netFIELD OS interface. On the left, a sidebar menu lists various system settings, with 'Networking' highlighted by a red arrow. The main content area shows the 'Network Proxy' configuration page, which is also outlined in red. This page includes an 'Edit Proxy' button and a table of proxy settings. Below the table is a 'Networking Logs' section showing a list of system messages dated August 7, 2020.

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**  
AUGUST 7, 2020

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 61: Network Proxy configuration

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

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

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

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

To configure your network proxy settings, proceed as follows:



**Note:**

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

➤ Click the **Edit Proxy** button.

➤ The **Proxy Settings** dialog opens:

Figure 62: Proxy Settings dialog window

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

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

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

Figure 63: Using one Proxy server for all protocols

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

**Important:**

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

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

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

The image shows a 'Proxy Settings' dialog box with a light gray header. It contains three sections for protocol-specific proxy configuration: HTTP, HTTPS, and FTP. Each section has a 'Host' and 'Port' input field, and two checkboxes: 'Authentication required' and 'Use this proxy server for all protocols'. The 'No Proxy' section at the bottom has a 'Host' input field with a default value 'localhost, 127.0.0.1' and a note '(e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)'. At the bottom right are 'Cancel' and 'Apply' buttons.

Protocol	Host	Port	Authentication required	Use this proxy server for all protocols
HTTP	HTTP://10.11.5.98	3128	<input type="checkbox"/>	<input type="checkbox"/>
HTTPS	HTTPS://10.11.5.99	3128	<input type="checkbox"/>	<input type="checkbox"/>
FTP			<input type="checkbox"/>	<input type="checkbox"/>
No Proxy	localhost, 127.0.0.1 (e.g. intranet.consor.de, .consor.de, 10.15.22.0/24, 10.15.22.12)			

Figure 64: Separate HTTP/HTTPS/FTP configuration

- Enter the parameters of the individual proxy servers.

## Saving and restarting

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

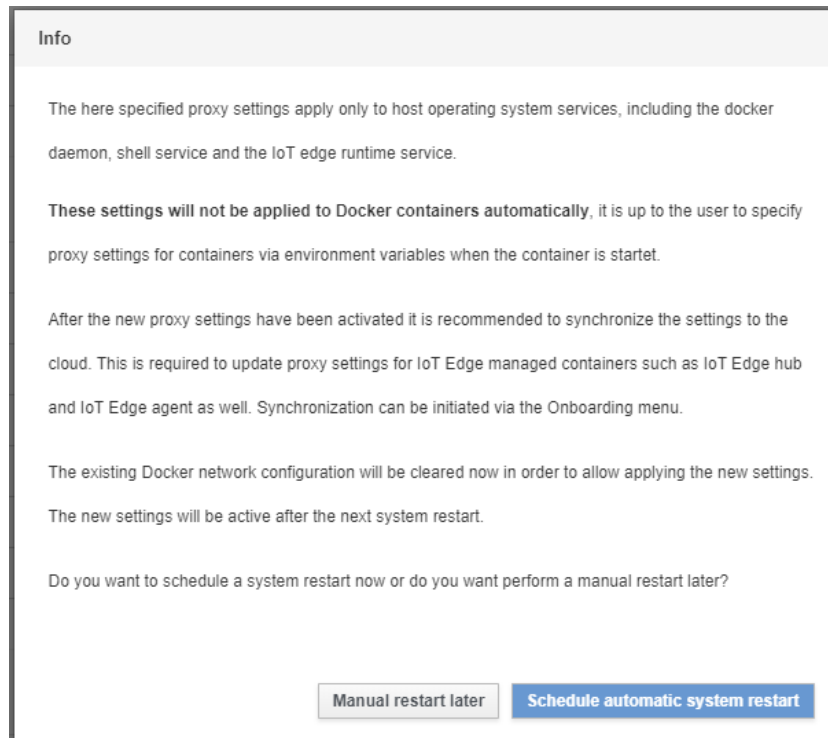


Figure 65: Restart dialog after changing proxy server configuration

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

## Synchronizing new settings with the cloud

- If your netFIELD OS 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” of the netFIELD OS in the cloud. To do so, open the **Onboarding** page of the netFIELD OS.

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

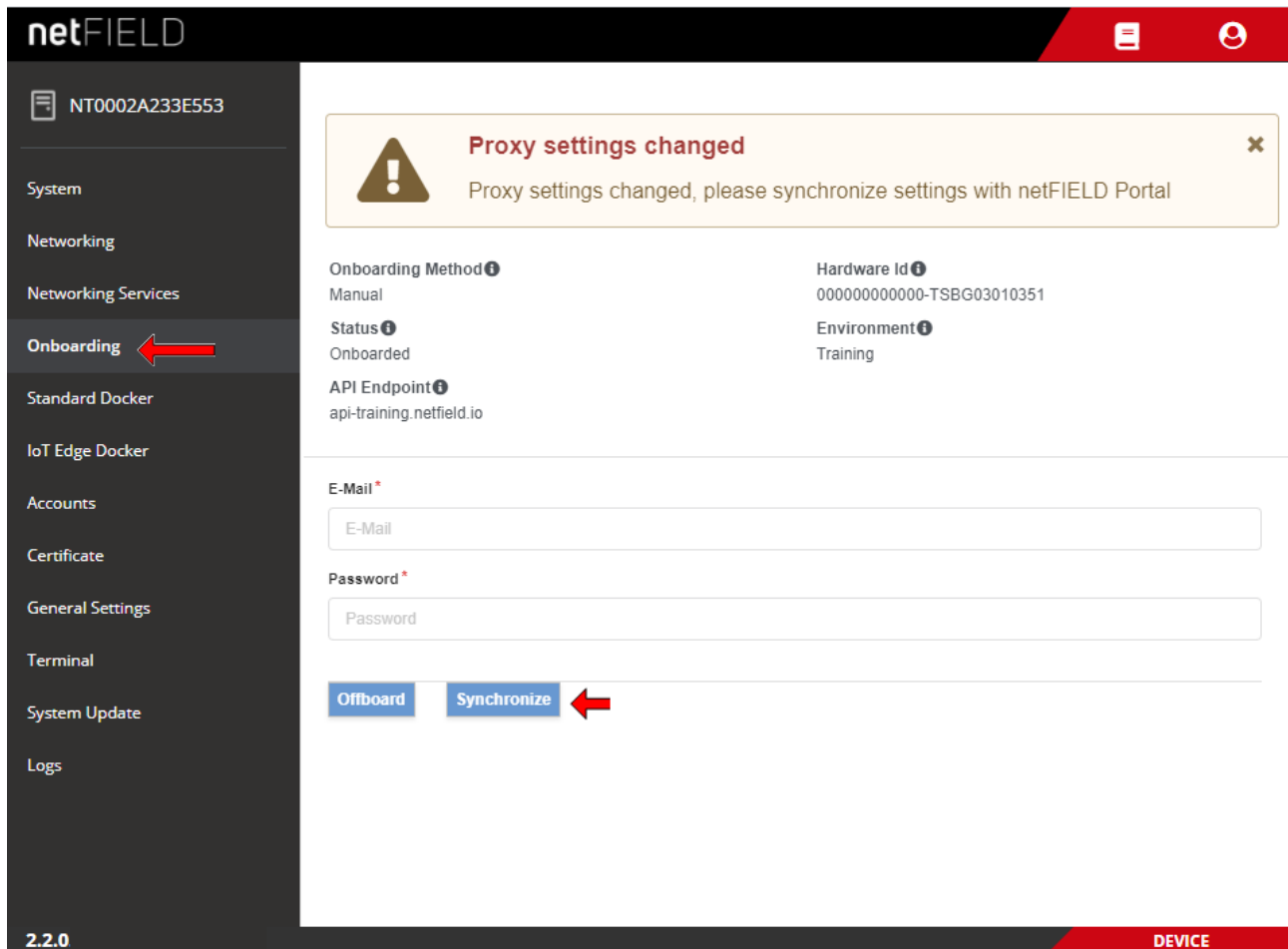


Figure 66: Synchronize proxy settings with netFIELD Portal

- 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 netFIELD OS is onboarded in the netFIELD Portal, do not forget to synchronize the new settings.

## 5.4 Networking Services

By default, the netFIELD OS Datacenter does not support Wi-Fi and DHCP Services for Access Point mode. The **Wi-Fi** tab and the **DHCP Server** tab are therefore disabled.

## 5.5 Onboarding (and offboarding)

The **Onboarding** page allows you to “register” your netFIELD OS Datacenter in the netFIELD Portal. For a detailed description of the onboarding process and the parameters on this page, see section *“Onboard” (register) netFIELD OS in the netFIELD Portal* [▶ page 43]. Note that the netFIELD OS Datacenter will be labelled as “device” in the Portal.

You can also “offboard” your netFIELD OS here.

If you have changed the HTTP/HTTPS/FTP proxy server settings of your netFIELD OS *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.)

netFIELD

NT000C295DBDCC

System

Networking

Networking Services

**Onboarding**

Standard Docker

IoT Edge Docker

Accounts

Certificate

General Settings

Terminal

System Update

Logs

2.2.0

Onboarding Method ⓘ

Manual

Status ⓘ

API Endpoint ⓘ

Hardware Id ⓘ

33fc77c15aef-64ff3809b71a

Environment ⓘ

--

Basic | Advanced

Environment \*

Environment

Device Name

Device Name

E-Mail \*

E-Mail

Password \*

Password

Upstream Protocol

Upstream Protocol

☐ Use Manifest

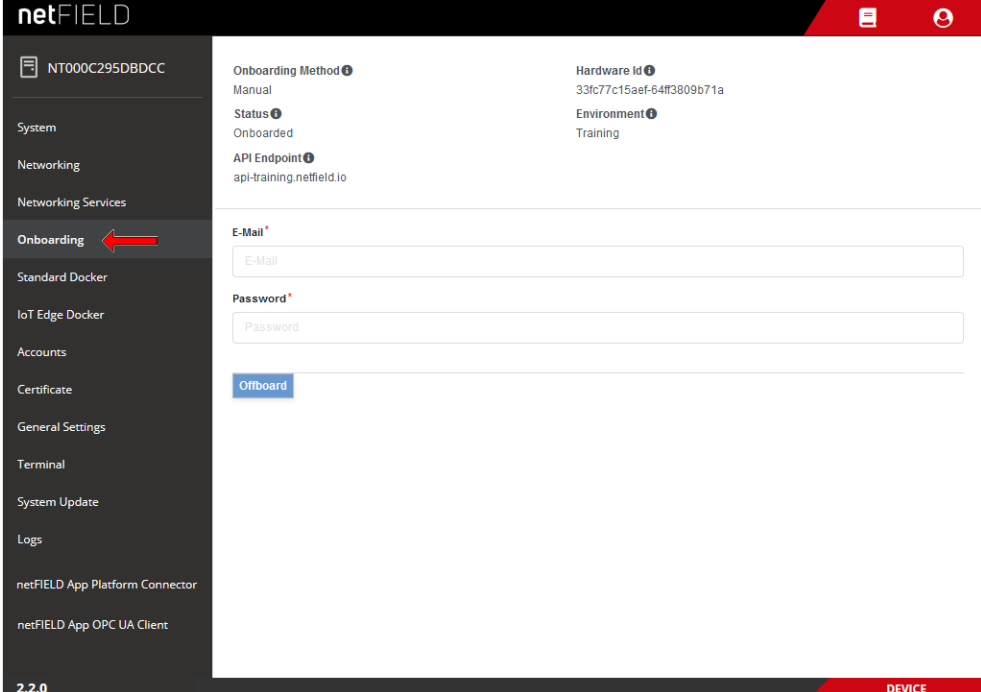
Onboard

DEVICE

Figure 67: Basic Onboarding page

Once your netFIELD OS has been onboarded, the page changes and shows the parameters for “offboarding” it. By offboarding it, the netFIELD OS 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



The screenshot shows the netFIELD portal interface. The left sidebar contains a list of settings: System, Networking, Networking Services, **Onboarding** (highlighted with a red arrow), Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, Logs, netFIELD App Platform Connector, and netFIELD App OPC UA Client. The main content area displays the following information:

Onboarding Method	Hardware Id
Manual	33fc77c15aef-64ff3809b71a

Below this, the status is shown as "Onboarded" and the API Endpoint as "api-training.netfield.io". The Environment is set to "Training".

The offboarding section includes two input fields: "E-Mail" and "Password", both marked with an asterisk (\*). Below these fields is a blue "Offboard" button.

The bottom of the interface shows the version "2.2.0" and the label "DEVICE".

Figure 68: Offboarding “Basic”

- In the **E-Mail** and **Password** fields, enter the credentials of a user of the **netFIELD Portal** who possesses `deleteDevices` and `offboardedDevices` permissions.
- Click **Offboard** button.
- After successful offboarding, the following message appears: **Success – Device is now deleted.**

## Offboarding after having used the Advanced Onboarding method

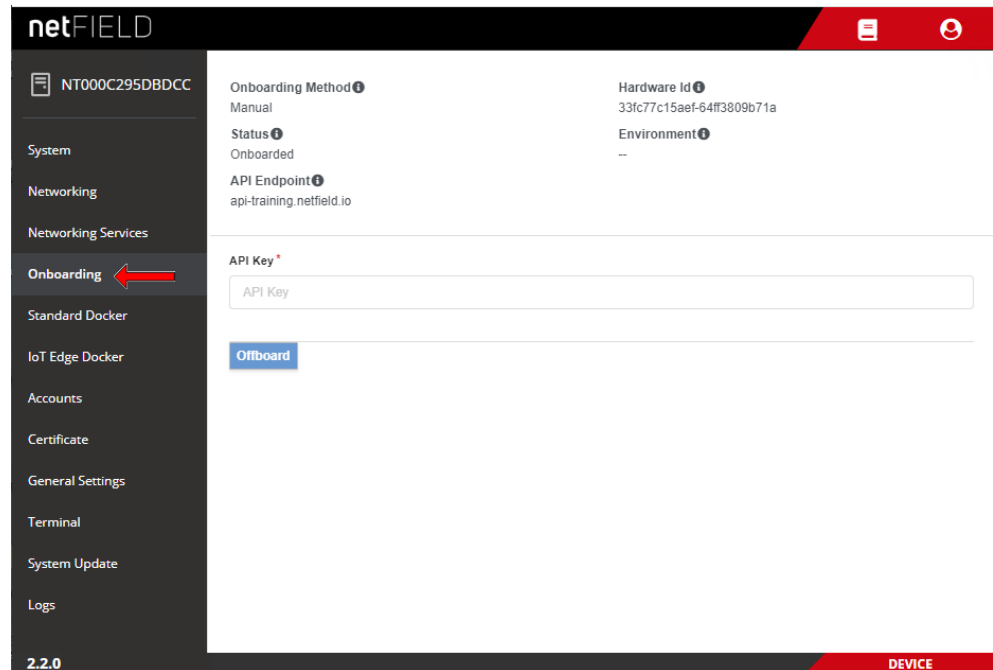


Figure 69: Offboarding “Advanced”

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



### Note:

After offboarding, all application *containers* managed by the netFIELD Portal are automatically deleted. However, the Docker *images* are still present in the netFIELD OS. They can be deleted manually on the **IoT Edge Docker** page of the Local Device Manager.

## 5.6 Standard Docker

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

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



### Note:

The network address settings of the Standard Docker can be managed under **General Settings > Docker Network Settings** (see section *Docker Network Settings* [▶ page 102]).

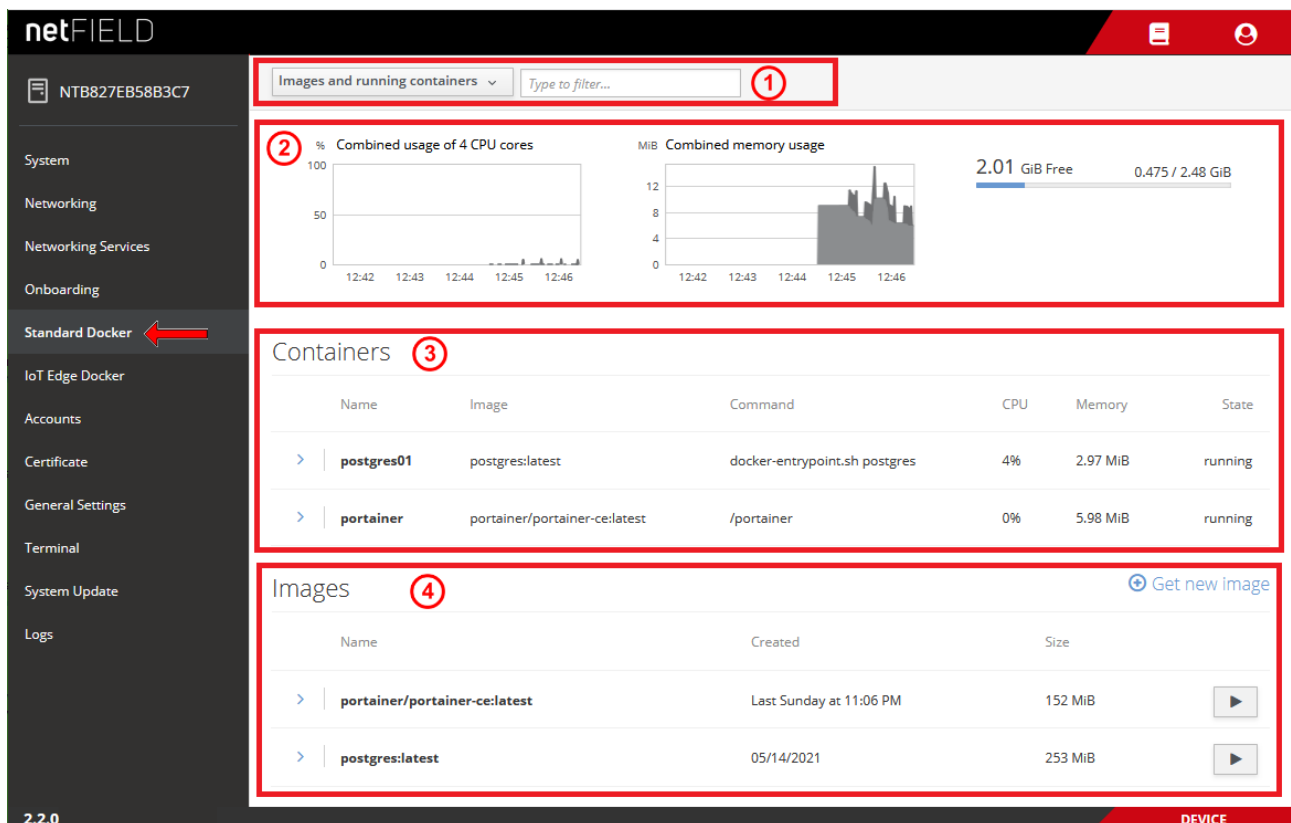


Figure 70: Standard Docker

### Filter options in header

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

You can choose in the drop-down list:

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

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

## Graphs

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

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

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

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

## Containers

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

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

The screenshot shows the netFIELD web interface. On the left is a sidebar with navigation links: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, and Logs. A red arrow points to the 'General Settings' link. The main content area is titled 'Containers' and shows a table of running containers. The table has columns for Name, Image, Command, CPU, Memory, and State. Two containers are listed: 'portainer\_1' and 'postgres01'. The 'postgres01' container is selected, and its details are expanded below the table. The details show the container ID, creation time, image, command, and state. To the right of the container list, there are buttons for 'Commit', 'Stop', and a dropdown menu. Below the container details is a section for 'Images' with a table showing the 'portainer/portainer-ce:latest' image and its size. At the bottom left, the version '2.2.0' is displayed, and at the bottom right, the word 'DEVICE' is shown.

Figure 71: Expand concise container details

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

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

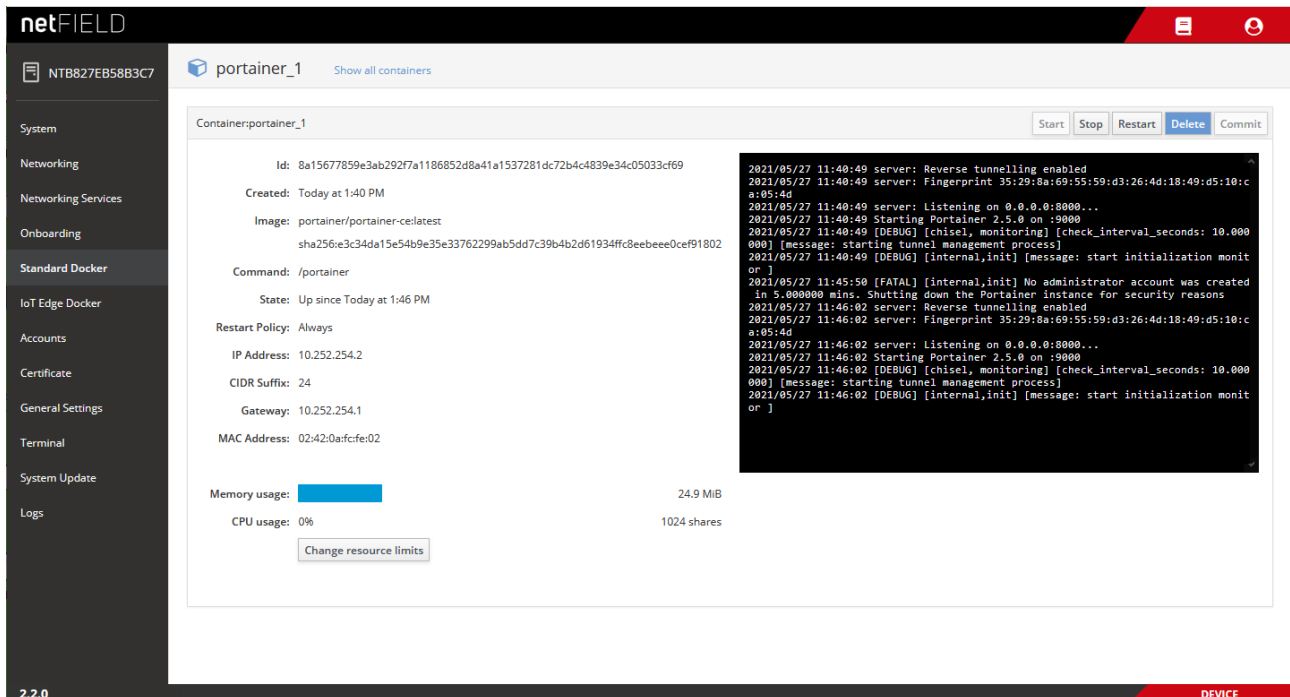


Figure 72: Container parameters with terminal window

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

## Images

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

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

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

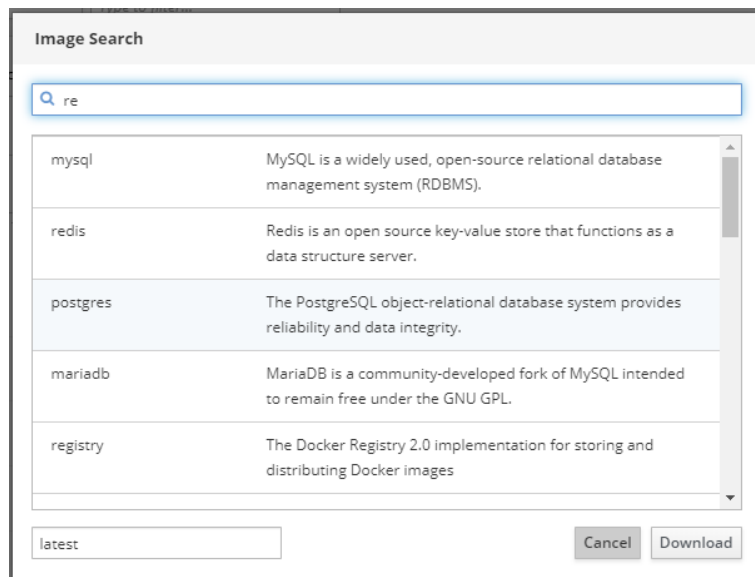



Figure 73: Image Search dialog of Standard Docker

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

### Starting a container

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

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

The **Run Image** dialog box is used to configure a container before running it. The configuration includes:

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

key	value
PATH	/usr/local/sbin
GOSU_VERSION	1.12
LANG	en_US.utf8
PG_MAJOR	12
PG_VERSION	12.3-1.pgdg10i
PGDATA	/var/lib/postgres
- Restart Policy:** No

Buttons: Cancel, Run

Figure 74: Run Image dialog



#### Note:

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

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

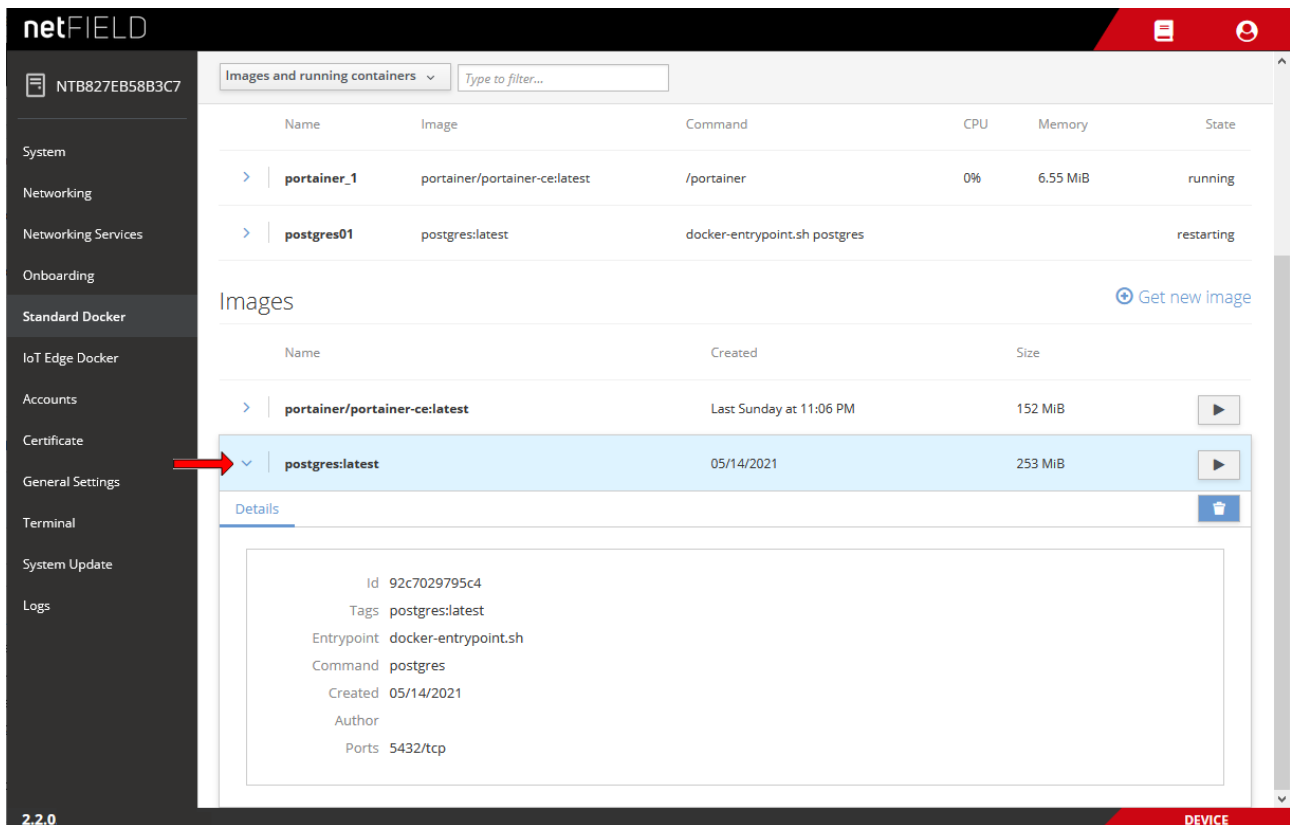


Figure 75: Expand image details

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

➤ A page featuring detailed information opens:

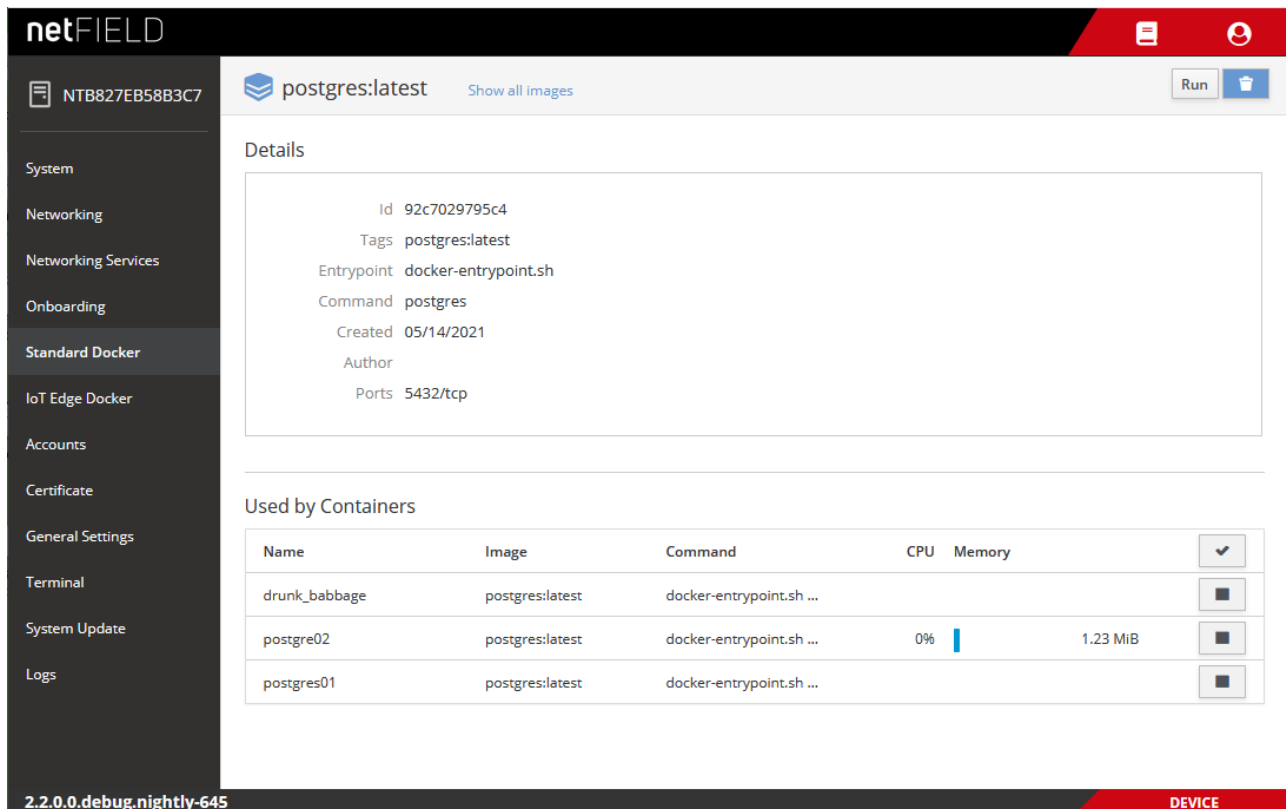





Figure 76: Image details

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

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

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



#### Note:

The Standard Docker can also be managed by using Docker commands with the CLI in the **Terminal**. See section *Useful CLI commands and parameters in Terminal* [▶ page 113] for examples, e.g. for “Docker Compose” support.

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

## 5.7 IoT Edge Docker

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

Note that you have to “onboard” your netFIELD OS (see section *"Onboard" (register) netFIELD OS in the netFIELD Portal* [▶ page 43]) before you can access this page.

Note also that you have only limited control over the images and containers here (i.e. you cannot download, configure, start or stop them here), because they are managed exclusively from the netFIELD Cloud, respectively netFIELD Portal (where you can e.g. define environment variables for a container before its deployment). This distinguishes the IoT Edge Docker from the Standard Docker, which allows the parameterization of containers before they are started (see section *Standard Docker* [▶ page 81]).

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

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 in the netFIELD OS 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 102]).

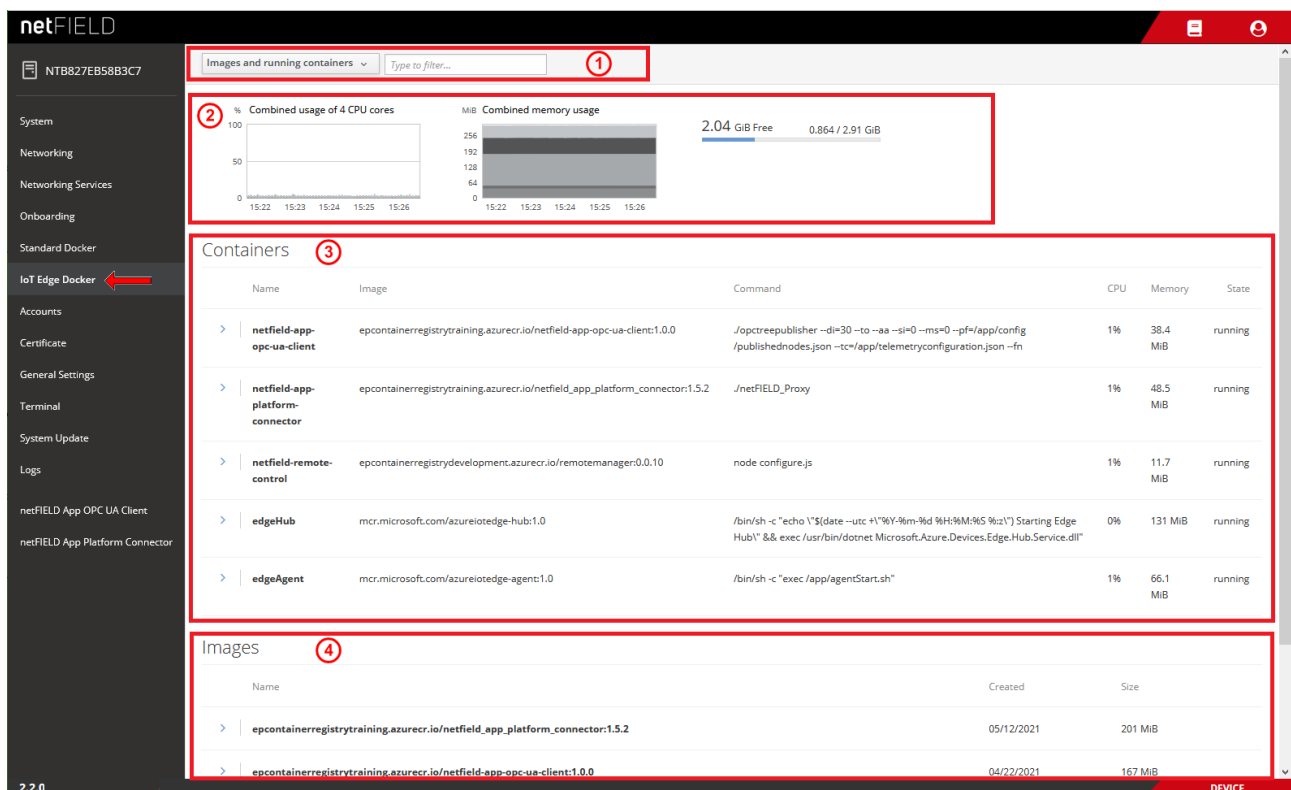


Figure 77: IOT Edge Docker

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

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

**Filter options in header**

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

You can choose in the drop-down list:

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

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

**Graphs**

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

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

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

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

## Containers

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

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

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

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

Figure 78: Container details expanded

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

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

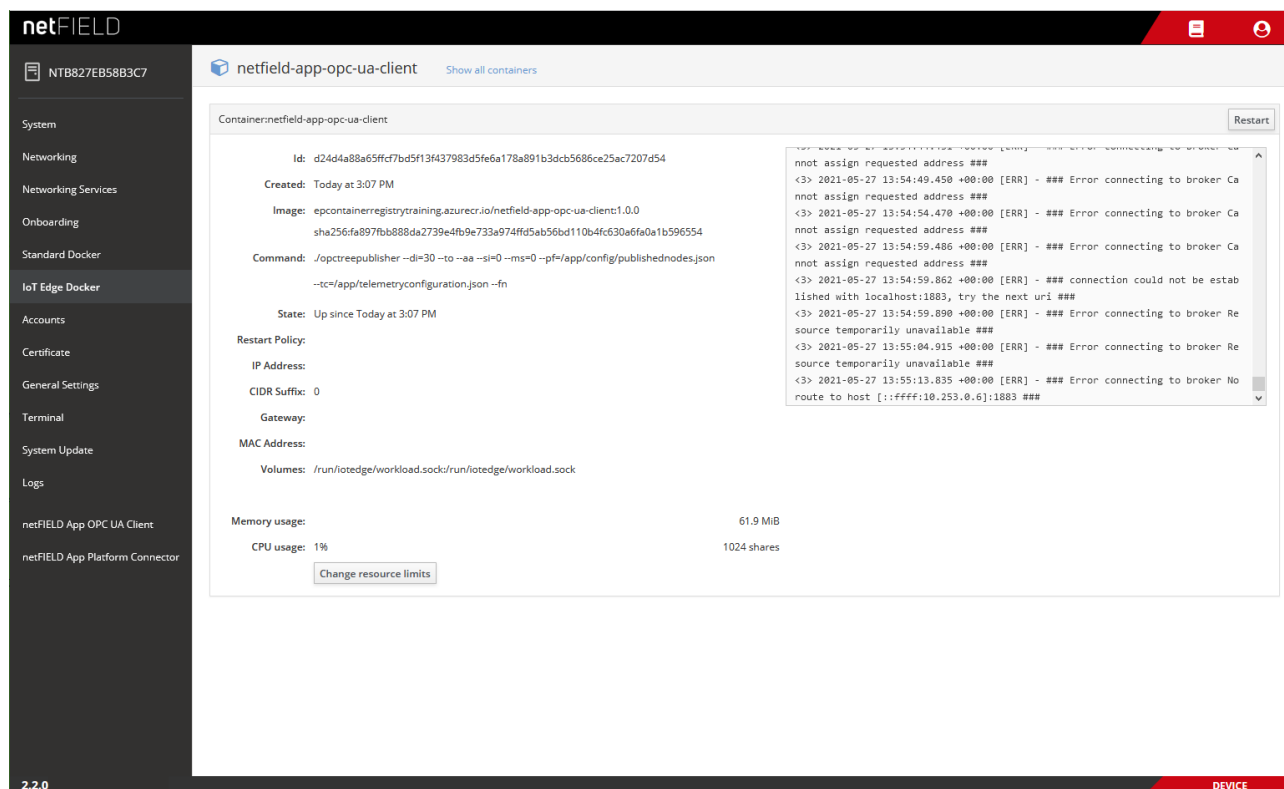


Figure 79: Container parameters


- 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 netFIELD OS, 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 netFIELD OS again.

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

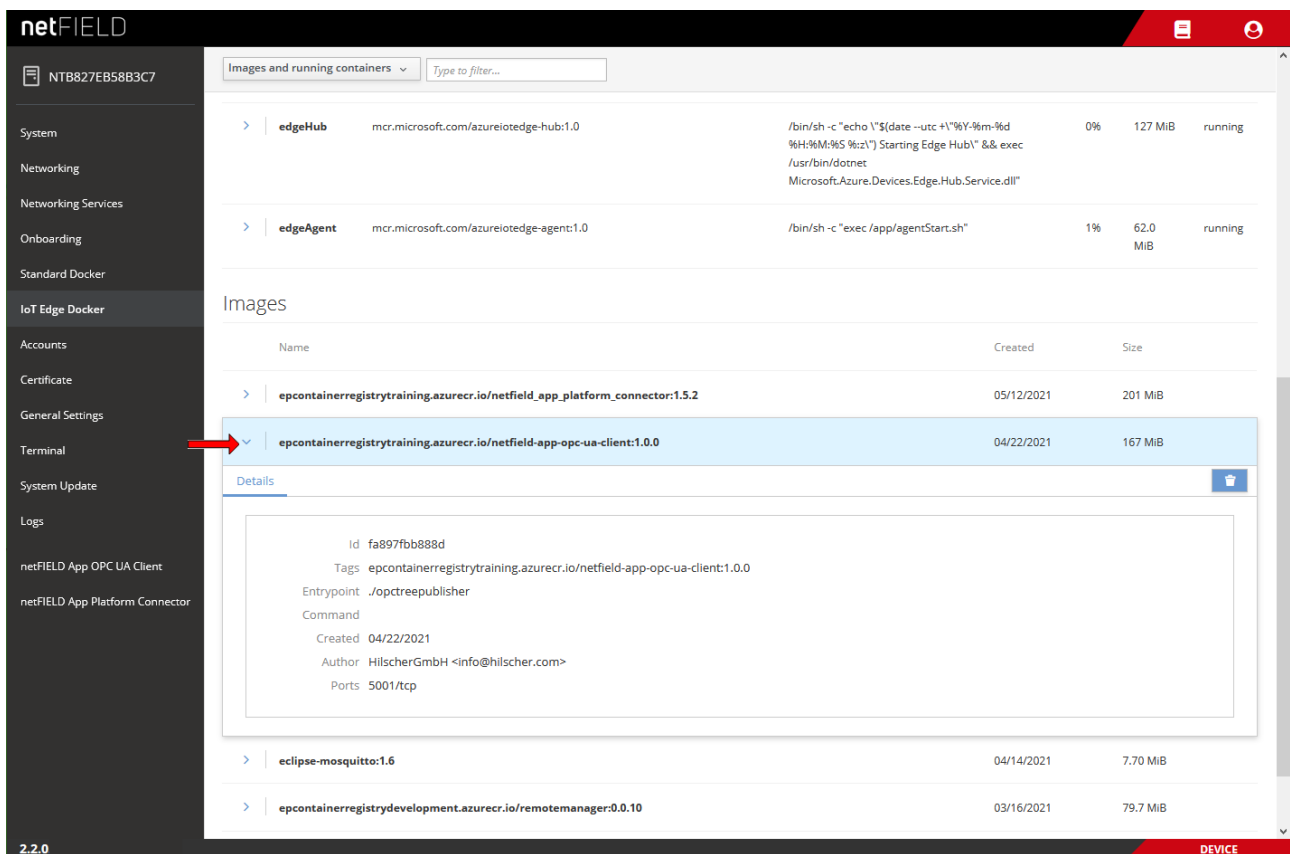


Figure 80: IoT image expanded

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

➤ A page featuring detailed information opens:

The screenshot shows the netFIELD interface. The sidebar on the left contains navigation links: System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker (highlighted), Accounts, Certificate, General Settings, Terminal, System Update, Logs, netFIELD App OPC UA Client, and netFIELD App Platform Connector. The main content area displays the details of the image 'epcontainerregistrytraining.azurecr.io/netfield-app-opc-ua-client:1.0.0'. The details section includes fields for Id, Tags, Entrypoint, Command, Created, Author, and Ports. Below this is a table titled 'Used by Containers' showing the resources consumed by the 'netfield-app-opc-ua-client' container.

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

Figure 81: 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 113] for examples.

## 5.8 Accounts

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

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

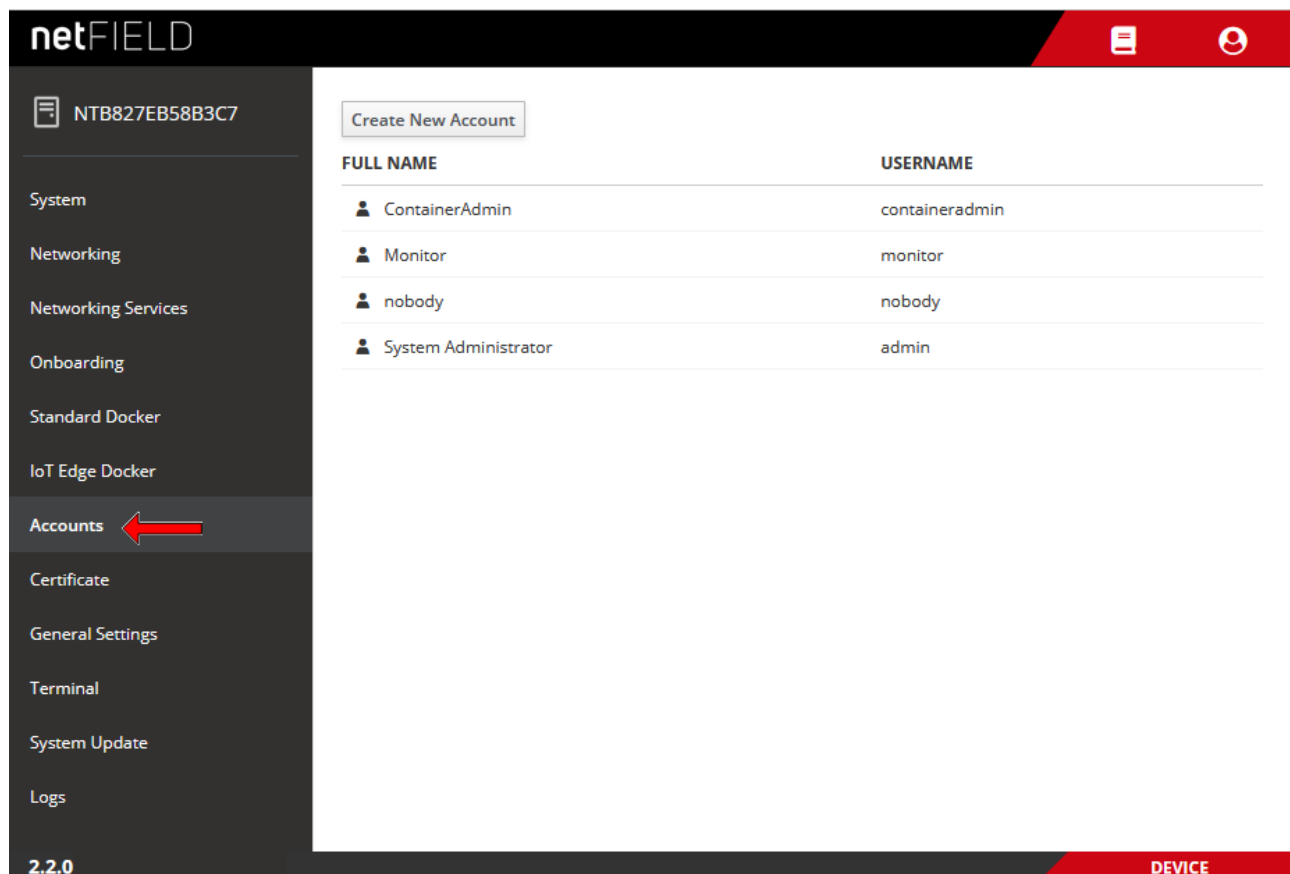


Figure 82: Accounts

- 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

Cancel Create

Figure 83: 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:

The screenshot shows the 'Edit account' configuration dialog for the 'ContainerAdmin' account. The breadcrumb path is 'Accounts > ContainerAdmin'. The account name 'ContainerAdmin' is displayed at the top, with 'Terminate Session' and 'Delete' buttons. Below this, the 'Full Name' is 'ContainerAdmin' and the 'User Name' is 'containeradmin'. Under 'Roles', there are two checkboxes: 'Server Administrator' and 'Container Administrator', both of which are currently unchecked. The 'Last Login' status is 'Never'. In the 'Access' section, the 'Lock Account' checkbox is unchecked, with a link 'Never lock account' to its right. The 'Password' section includes 'Set Password' and 'Force Change' buttons, with a link 'Never expire password' to its right. At the bottom, there is a section for 'Authorized Public SSH Keys' with a '+' button to add keys. Below this section, a message states: 'There are no authorized public keys for this account.'

Figure 84: Edit account



#### Note:

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

## Roles

The **Server Administrator** has full access rights to all functions of the netFIELD OS (including Standard Docker and IoT Edge Docker).

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

The **Container Administrator** can download container images in the **Standard Docker**, and can also start and stop the containers.

Note that the containers running in the **IoT Edge Docker** are deployed and managed exclusively from the netFIELD Cloud, respectively netFIELD Portal. As **Container Administrator** you can, however, “clean” a netFIELD container image from the 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).

If you assign **neither role** to an account, the user has only “read” access to the netFIELD OS functions respectively to the host configuration. Furthermore, a user without a role will have no access to the Standard Docker or to IoT Edge Docker (not even “read” access). Note, however, that this user will have access to the plug-in dashboards of the netFIELD application containers in the Local Device Manager.

### Authorized Public SSH Keys

This area lists the SSH keys assigned to this account.

Click on the  button to add an SSH key.



---

**Note:**

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

---

## 5.9 Certificate

On the **Certificate** page, you can manage your web server certificate. You can display details of your currently installed certificate and upload a new certificate and the corresponding private key file in \*.pem format to the netFIELD OS.

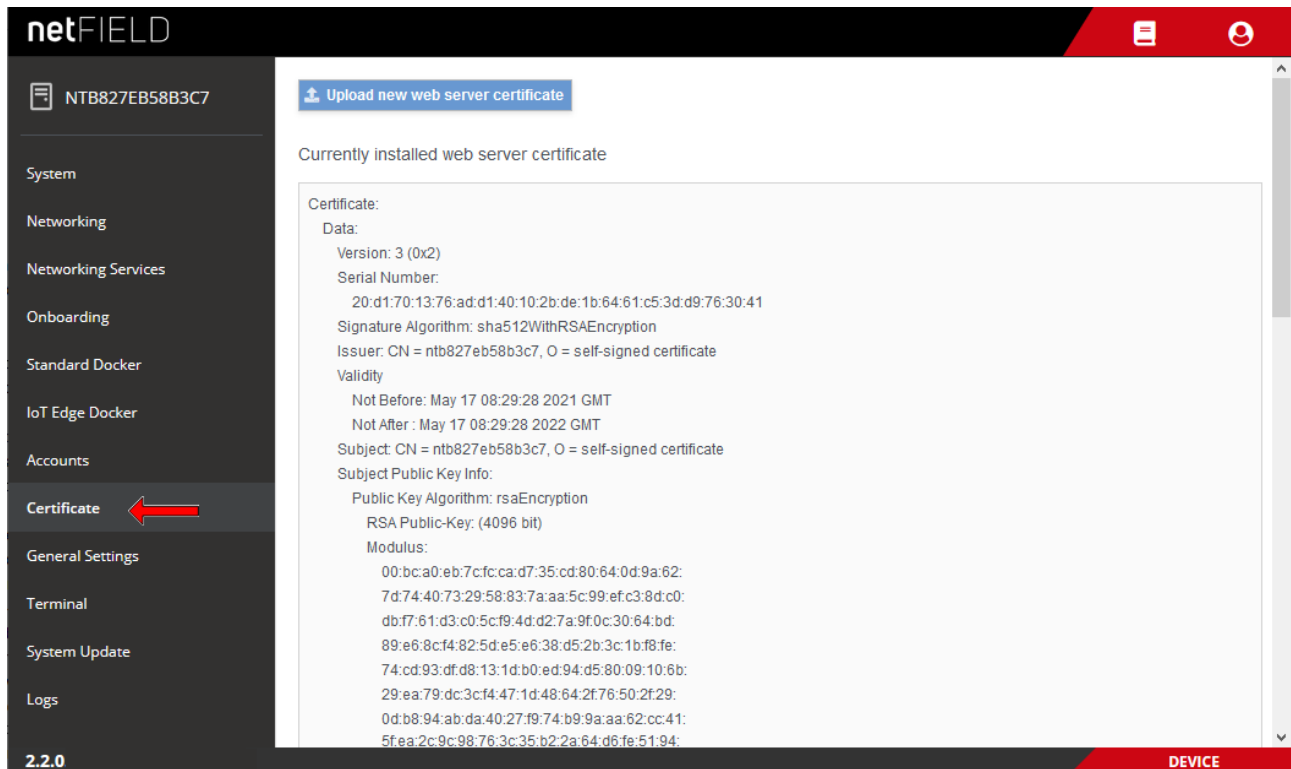


Figure 85: Web Server Certificate page



### 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.

## 5.10 General Settings

### 5.10.1 Overview

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

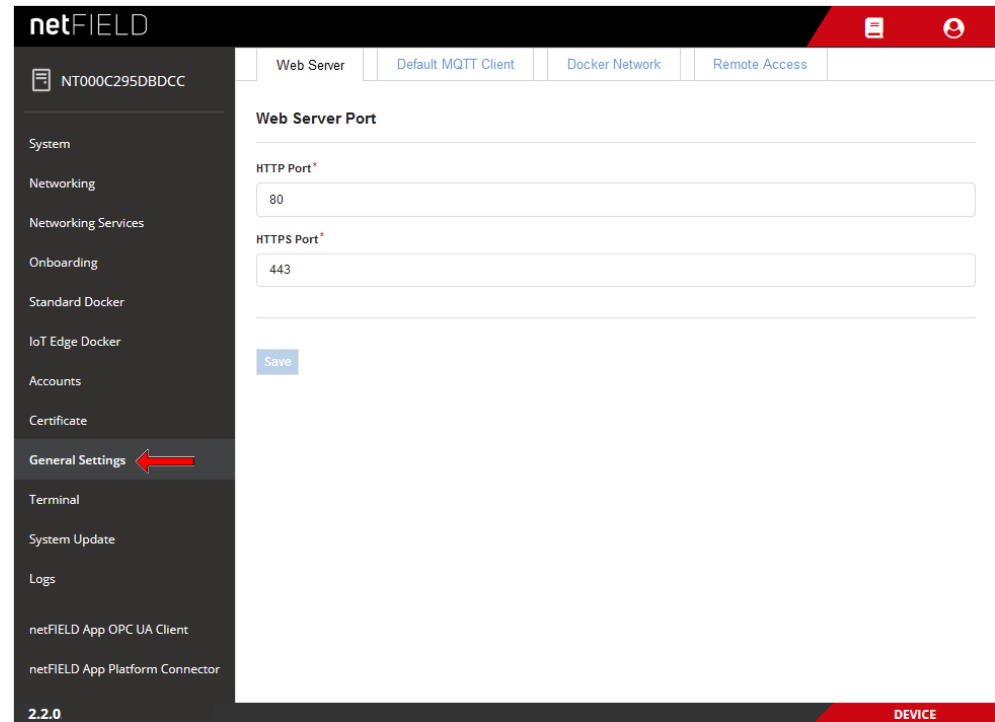


Figure 86: General Settings

## 5.10.2 Web Server (Port) Settings

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

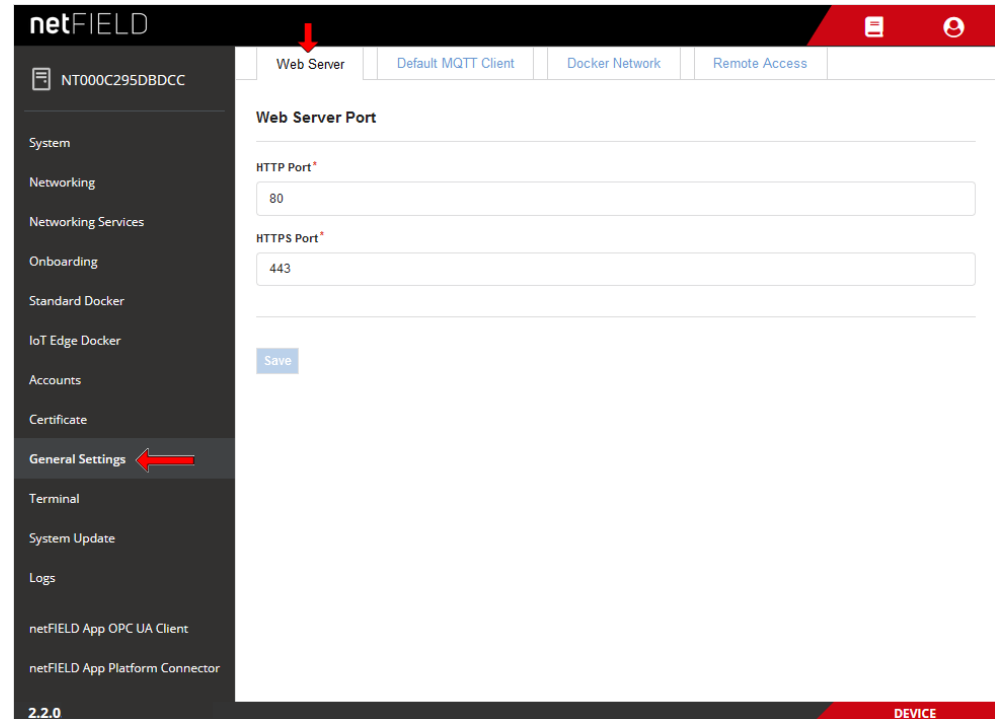


Figure 87: Web Server Settings tab

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:

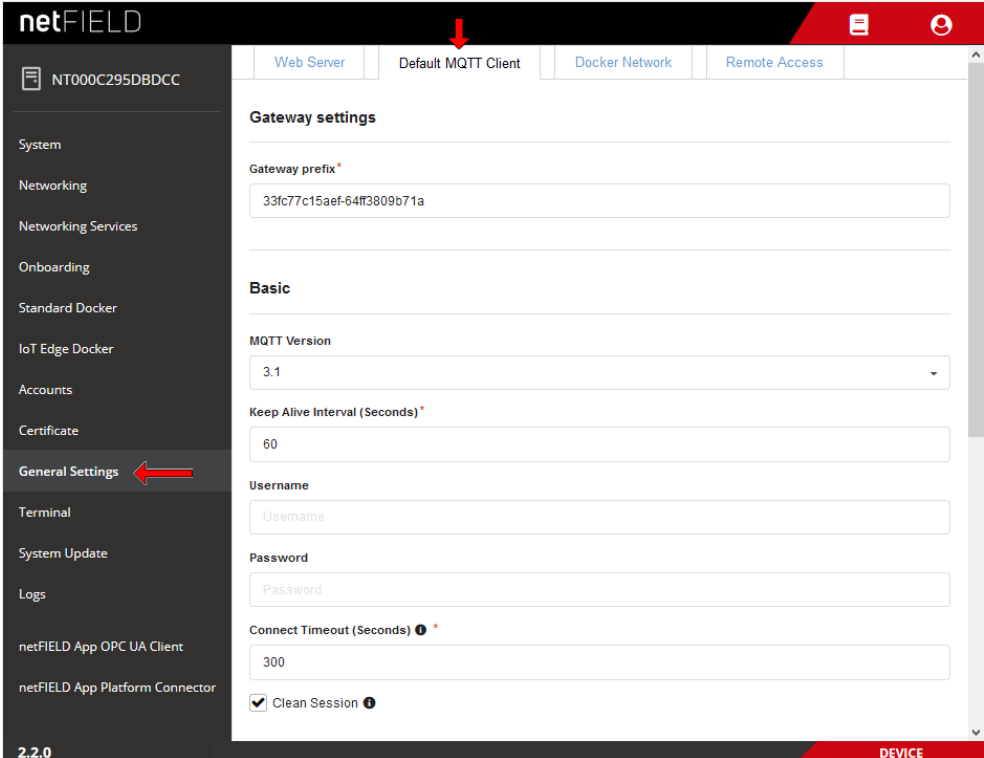
Changing the web server port settings will have no effect on the **Remote Control** function that allows you to access the Local Device Manager from the netFIELD Portal via “web tunnel”. For more information about the Remote Control function, see *netFIELD Portal* operating instructions manual, DOC1907010lxxEN.

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

### 5.10.3 Default MQTT Client Settings

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

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



The screenshot displays the netFIELD web interface. The top navigation bar includes tabs for 'Web Server', 'Default MQTT Client' (selected), 'Docker Network', and 'Remote Access'. A red arrow points to the 'Default MQTT Client' tab. The left sidebar lists various system settings, with 'General Settings' highlighted by a red arrow. The main content area shows the 'Default MQTT Client' settings, which are divided into 'Gateway settings' and 'Basic' sections. The 'Gateway settings' section includes a 'Gateway prefix\*' field with the value '33fc77c15aef-64ff3809b71a'. The 'Basic' section includes a 'MQTT Version' dropdown menu set to '3.1', a 'Keep Alive Interval (Seconds)\*' field with the value '60', a 'Username' field with the value 'Username', a 'Password' field with the value 'Password', a 'Connect Timeout (Seconds) ⓘ \*' field with the value '300', and a 'Clean Session ⓘ' checkbox that is checked. The bottom of the interface shows the version '2.2.0' and the label 'DEVICE'.

Figure 88: Default MQTT Settings

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

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

## 5.10.4 Docker Network Settings

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



### Important:

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

Note that after changing the address settings of the Standard and/or IoT Edge Docker all containers running on the corresponding Docker will be stopped and deleted and the netFIELD OS will be automatically restarted. After restart, you might have to re-deploy the deleted containers.

The screenshot displays the netFIELD web interface for configuring Docker network settings. The left sidebar contains a menu with items like System, Networking, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings (highlighted with a red arrow), Terminal, System Update, and Logs. The main content area has tabs for Web Server, Default MQTT Client, Docker Network (active), and Remote Access. Under the Docker Network tab, there are two sections: Standard Docker and IoT Edge Docker. Each section includes input fields for Bridge IP and CIDR Suffix or Netmask, and a table for Default address pools. The Standard Docker section shows a Bridge IP of 10.252.254.1 and a CIDR Suffix of 24. The IoT Edge Docker section shows a Bridge IP of 10.252.253.1 and a CIDR Suffix of 24. Both sections have a table with columns for IP Address, CIDR Suffix or Netmask, Network Size, and Action. A 'Save' button is located at the bottom left of the IoT Edge Docker section.

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

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

Figure 89: Docker Network Settings

## Standard Docker

The **docker0** bridge is a virtual interface created by the Standard Docker. By default, it uses the address 10.252.254.1/24 ("private range" as defined in RFC 1918) if the address is not already used on the host machine.

All containers running on the Standard Docker connect to this **docker0** bridge by default. The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. "masquerading") created by the Standard Docker to communicate with destinations outside the netFIELD OS.



Element	Description	
Bridge IP	IP address of the <b>docker0</b> bridge. Default: 10.252.254.1 <b>Note:</b> Do not change the default address unless necessary to avoid an address conflict with your LAN. Do not use the same Bridge IP address for both Standard and IoT Edge Docker.	
CIDR Suffix or Netmask	Subnet mask of the <b>docker0</b> bridge as CIDR Suffix or in "dotted decimal notation". Default (CIDR Suffix): 24 Default (dotted decimal notation): 255.255.255.0	
Default address pools	Here you can define "reserve" address pools (subnets) for the internal Docker bridge networks. The default pool consisting of the IP address/CIDR Suffix 10.254.0.1/16 with network size 24 means that the first additional Docker network bridge interface will be created with the IP address/CIDR Suffix 10.254.0.1/24, the second will be 10.254.1.1/24, the third will be 10.254.2.1/24, and so on.	
	IP address	Reserved IP address of the internal Docker bridge network.
	CIDR Suffix or Netmask	Subnet mask of the internal Docker bridge network as CIDR Suffix or in "dotted decimal notation".
	Network Size	Number of bits used as the netmask for further Docker bridge networks.
	Action	<div>  Opens a dialog for adding a new pool of reserved addresses.           </div> <div>  Deletes the address pool.           </div>

Table 12: Standard Docker Network Settings

## IoT Edge Docker

The **iotedge0** bridge is a virtual interface created by the IoT Edge Docker. By default, it uses the address 10.252.253.1/24 (“private range” as defined in RFC 1918) if the address is not already used on the host machine.

All containers running on the IoT Edge Docker connect to this **iotedge0** bridge by default. The containers can use the iptables/NAT rules (NAT = Network Address Translation, a.k.a. “masquerading”) created by the IoT Edge Docker to communicate with destinations outside the netFIELD OS.

Element	Description	
Bridge IP	IP address of the <b>iotedge0</b> bridge. Default: 10.252.253.1 <b>Note:</b> Do not change the default address unless necessary to avoid an address conflict with your LAN. Do not use the same Bridge IP address for both Standard and IoT Edge Docker.	
CIDR Suffix or Netmask	Subnet mask of the <b>iotedge0</b> bridge as CIDR Suffix or in “dotted decimal notation”. Default (CIDR Suffix): 24 Default (dotted decimal notation): 255.255.255.0	
Default address pools	Here you can define “reserve” address pools (subnets) for the internal IoT Edge Docker bridge networks. The default pool consisting of the IP address/CIDR Suffix 10.253.0.1/16 with network size 24 means that the first additional IoT Edge Docker network bridge interface will be created with the IP address/CIDR Suffix 10.253.0.1/24, the second will be 10.253.1.1/24, the third will be 10.253.2.1/24, and so on.	
	IP address	Reserved IP address of the internal IoT Edge Docker bridge network.
	CIDR Suffix or Netmask	Subnet mask of the internal IoT Edge Docker bridge network as CIDR Suffix or in “dotted decimal notation”.
	Network Size	Number of bits used as the netmask for further IoT Edge Docker bridge network.
	Action	<div> <div>+</div> <div>Opens a dialog for adding a new pool of reserved addresses.</div> </div> <div> <div>🗑</div> <div>Deletes the address pool.</div> </div>

Table 13: Standard Docker Network Settings

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

The following pictures illustrates the default Docker network configuration:

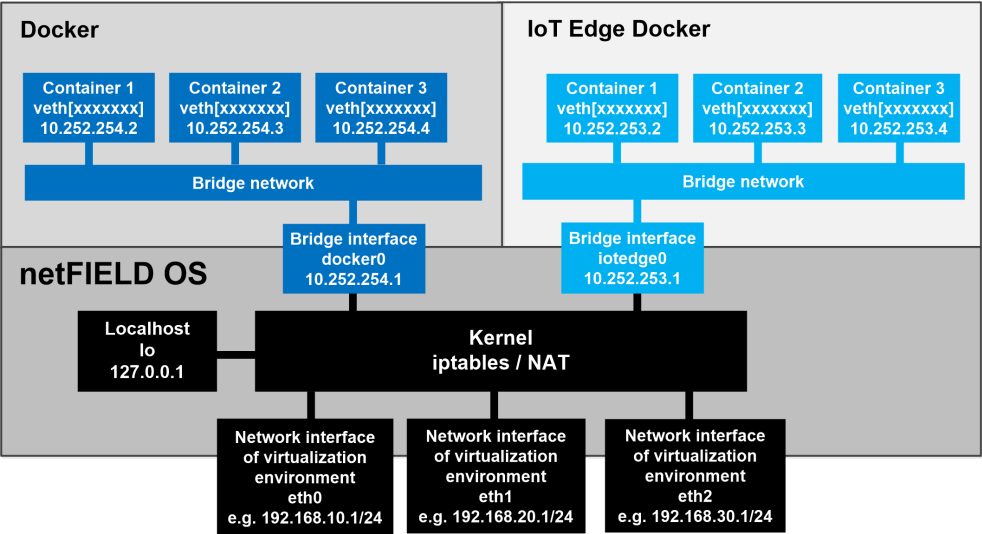


Figure 90: Default docker network configuration

## 5.10.5 Remote Access

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

For security reasons, remote control access is by default switched off. To allow remote control for your netFIELD OS Datacenter, 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 netFIELD OS Datacenter from an older netFIELD OS version to version  $\geq 2.2$ , the remote access remains by default enabled (for compatibility reasons) until it is switched off by the user.



### Note:

The “Remote Control” functions of the Portal allow you to access IP services (like e.g. HTTP(S), SSH, VNC, RDP or other TCP-based services) running on your netFIELD OS (or on other devices connected to a network that is accessible by the netFIELD OS Datacenter) 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 netFIELD OS when you click the **Enable Remote Control** button on the **Overview** page of your device in the Portal for the first time.

For a detailed description of the remote control functions, see section *Remote Control* in the *netFIELD Portal* manual, DOC1907010IxxEN).

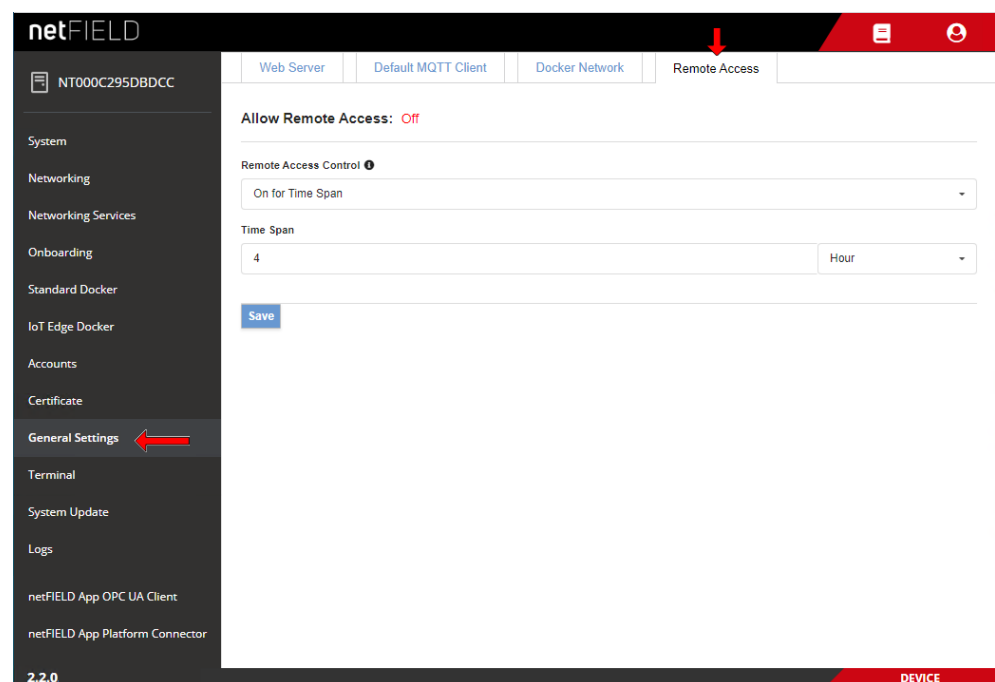


Figure 91: Remote Access tab

- 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 netFIELD OS.

**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 netFIELD OS. Accessing the netFIELD OS will then be possible via local LAN, Wi-Fi or SSH connection only.

- 
- Click **Save**.

## 5.11 Terminal

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

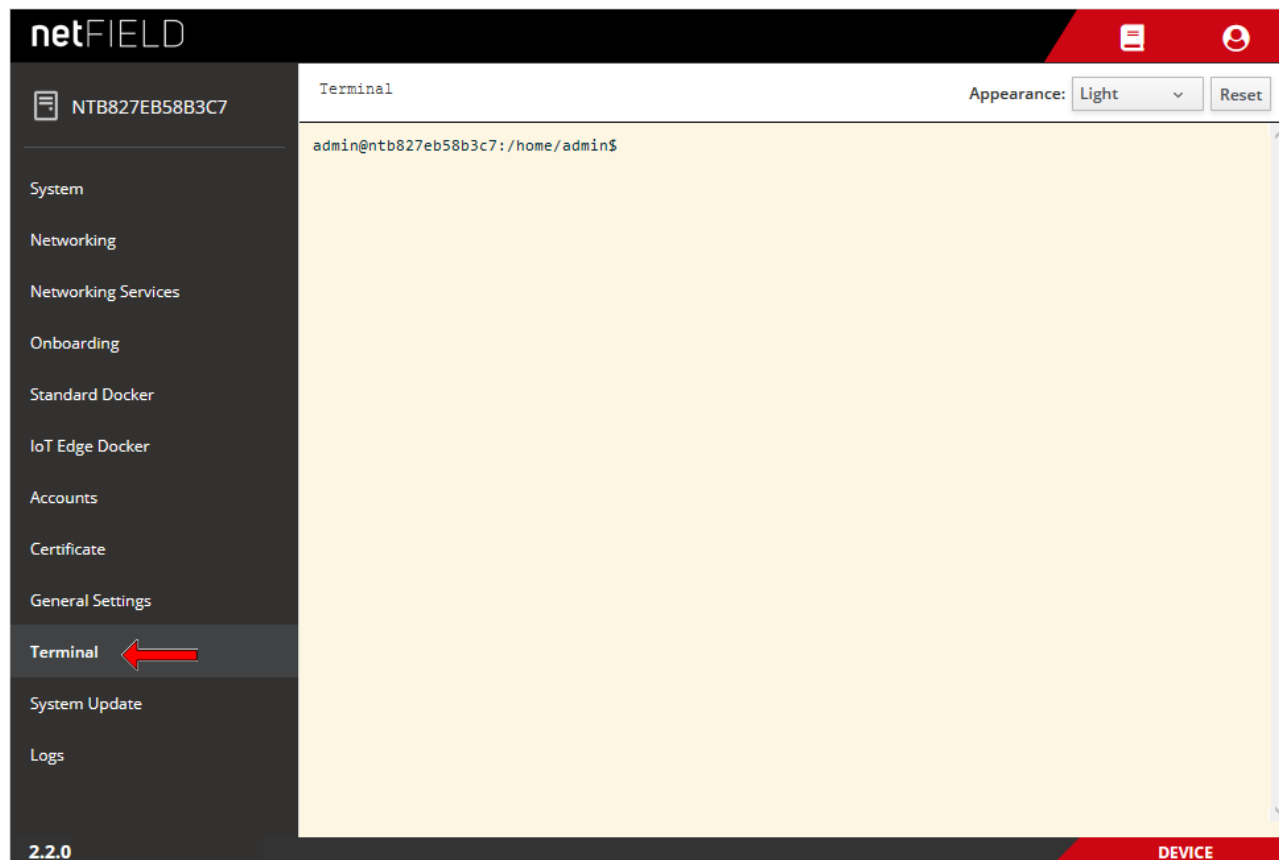


Figure 92: Terminal



**Note:**

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

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

Examples of commands and parameters are provided in section *Useful CLI commands and parameters in Terminal* [► page 113].

## 5.12 System Update

You can update the netFIELD OS Datacenter by simply uploading an `.swu` update file to the **System Update** page of the Local Device Manager. In the update, bug fixes and/or new functions will be added to the existing netFIELD OS, but its configuration settings, containers, user accounts, passwords and cloud registration (onboarding) will be preserved. You do not need to perform any action in the hypervisor of your virtualization environment for this.

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

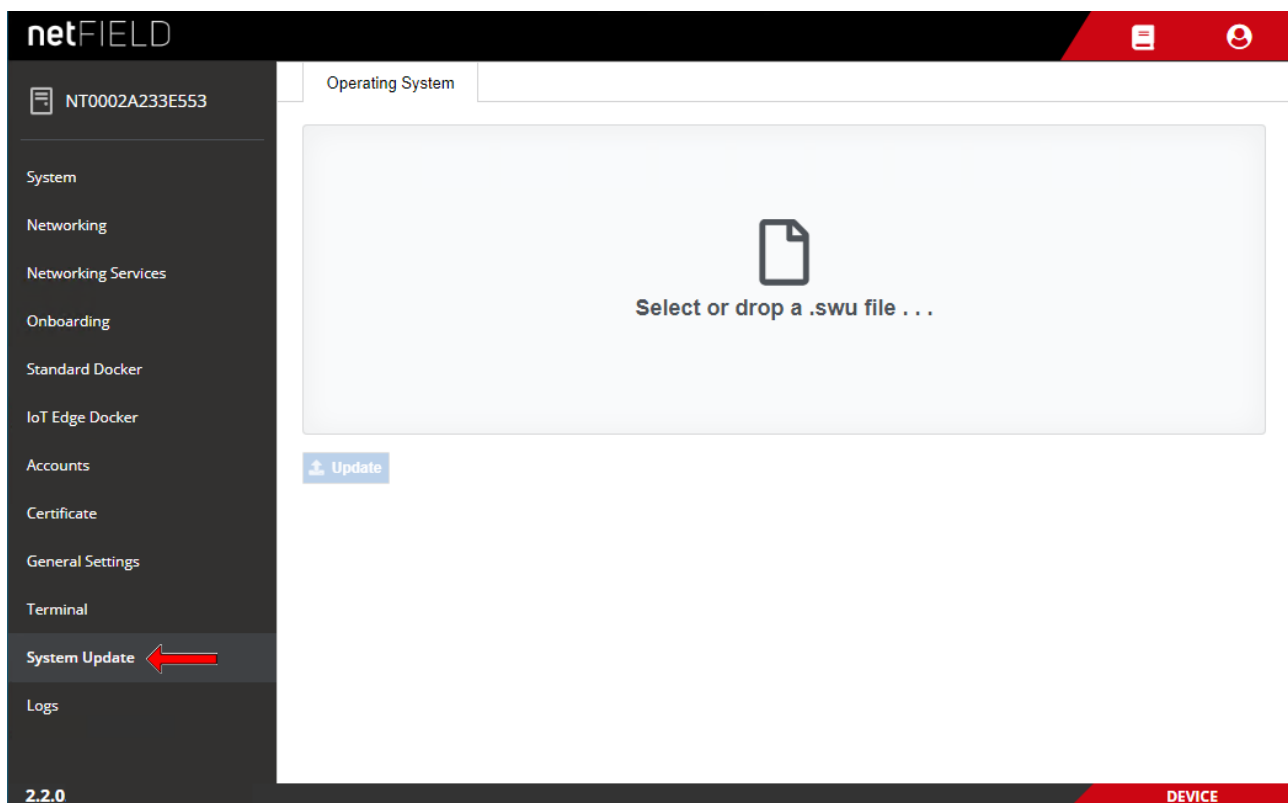


Figure 93: OS update page



### Note:

As an alternative to using the Local Device Manager for your netFIELD OS update, it is also possible to update it 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 netFIELD OS.

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

1. Download the update file from Hilscher to your local PC.
  - Go to the *netFIELD Software Overview* page <https://kb.hilscher.com/x/sSAfBw> and navigate to the latest netFIELD OS Datacenter version.  
In the *Software* table, go to the *Update via local Device Manager* entry and download the `niot-e-vm-en-2.x.x.x.release-update.swu` file.
2. Upload the \*.swu file from your local PC to the device.
  - On the **System Update** page, simply drag and drop the \*.swu file from your local PC onto the **Select or drop a .swu file...** field, or click into the field to open a file selection dialog.

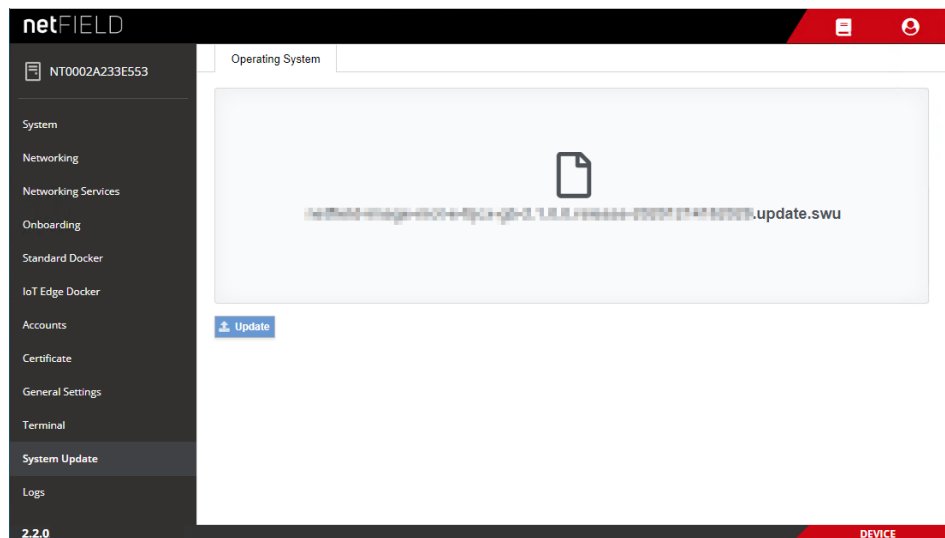


Figure 94: Selected OS update image

- 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.  
Click **Yes** if you want to start the update.

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

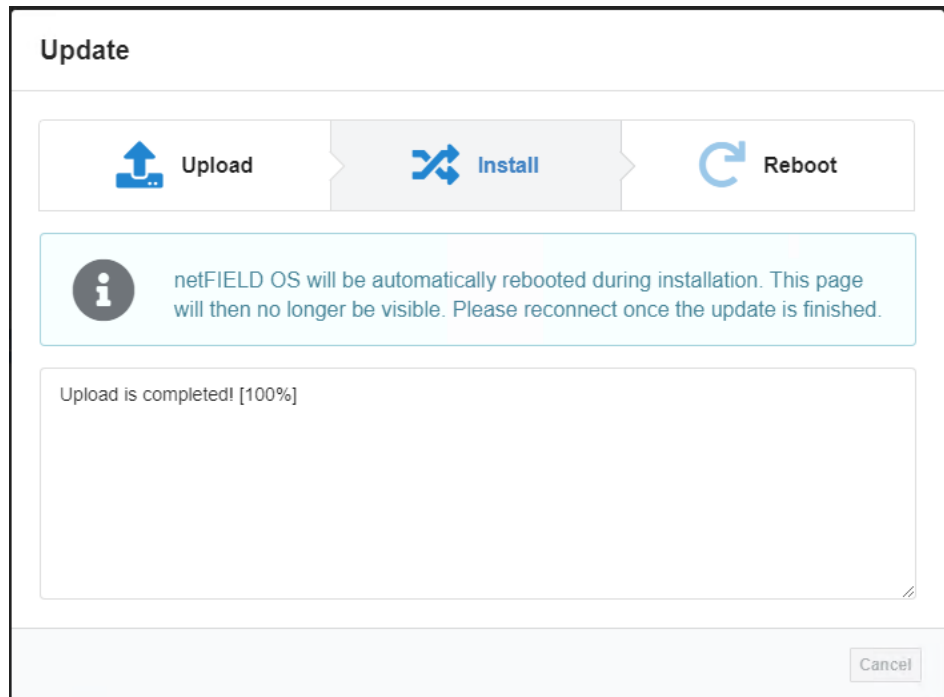


Figure 95: Upload finished message

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

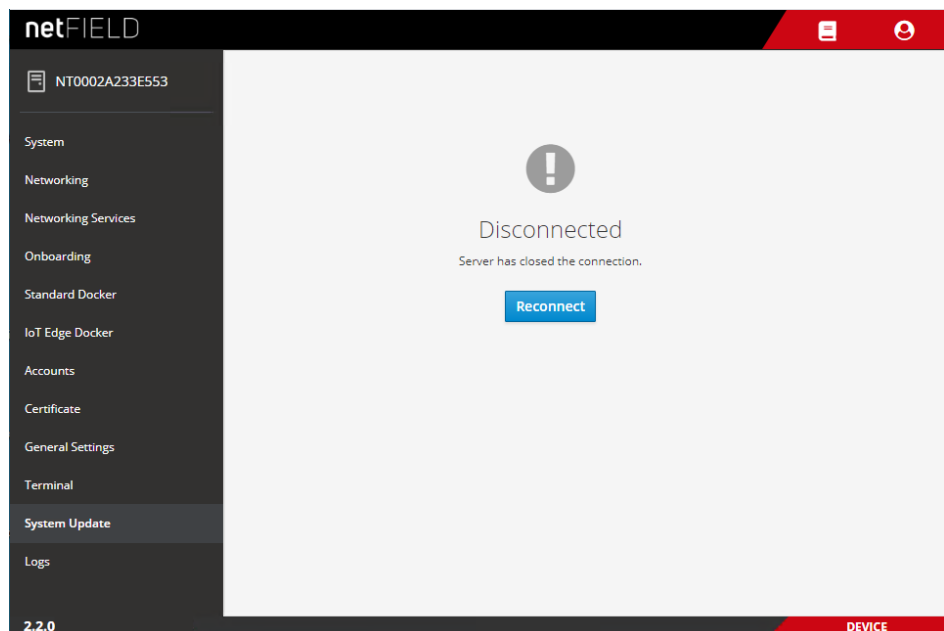


Figure 96: OS update "Disconnected" message

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

## 5.13 Logs

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

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

The screenshot shows the netFIELD web interface. On the left is a sidebar with a menu including System, Networking, Networking Services, Onboarding, Standard Docker, IoT Edge Docker, Accounts, Certificate, General Settings, Terminal, System Update, Logs (highlighted with a red arrow), netFIELD App OPC UA Client, and netFIELD App Platform Connector. The top header shows the device ID NTB827EB58B3C7. The main content area is titled 'MAY 31, 2021' and contains a table of log entries. The table has columns for time, message content, and service. The log entries include messages from cockpit-bridge, kernel, pkexec, and polkitd. A red bar at the bottom right indicates the device status.

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

Figure 97: Logs

## 6 Good to know...

### 6.1 Useful CLI commands and parameters in Terminal

#### 6.1.1 Network Manager

```
sudo nmcli ...
```

#### 6.1.2 Show interface status

```
sudo nmcli dev status
```

#### 6.1.3 Activate interface

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

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

#### 6.1.4 Docker Compose Support for Standard Docker environment

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

##### Example

To show the version of Docker Compose:

```
docker-compose version
```

#### 6.1.5 Manage Standard Docker

```
docker <docker commands>
```

##### Example

To list all created containers for the Standard Docker instance:

```
docker ps -a
```

#### 6.1.6 Manage IoT Edge Docker

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

##### Example

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

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

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

Disable autostart:

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

Stop SSH Daemon:

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

## 6.1.8 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
```

## 6.1.9 Follow the system log via terminal CLI

```
sudo journalctl -f
```

## 6.2 netFIELD OS: Industrial IoT Operating System

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

### Features

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

### Architecture

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

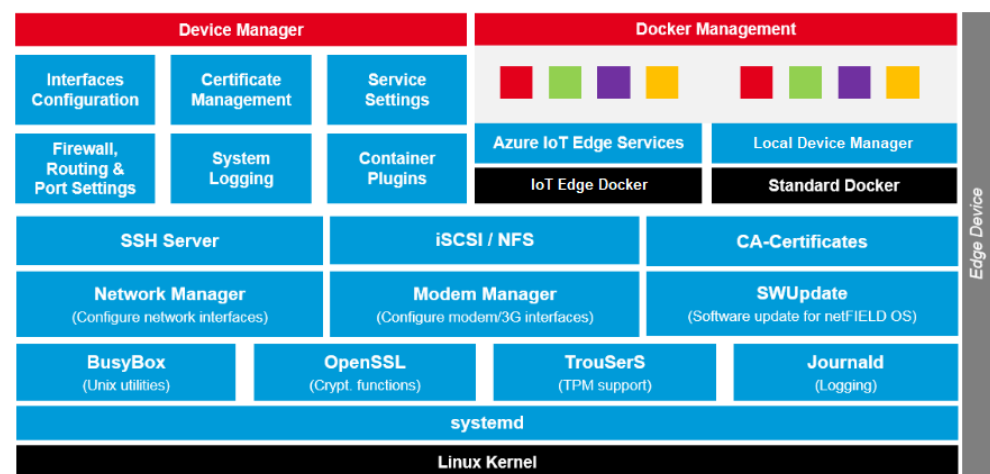


Figure 98: netFIELD OS architecture

### Core Services

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

## Container Management

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

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

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

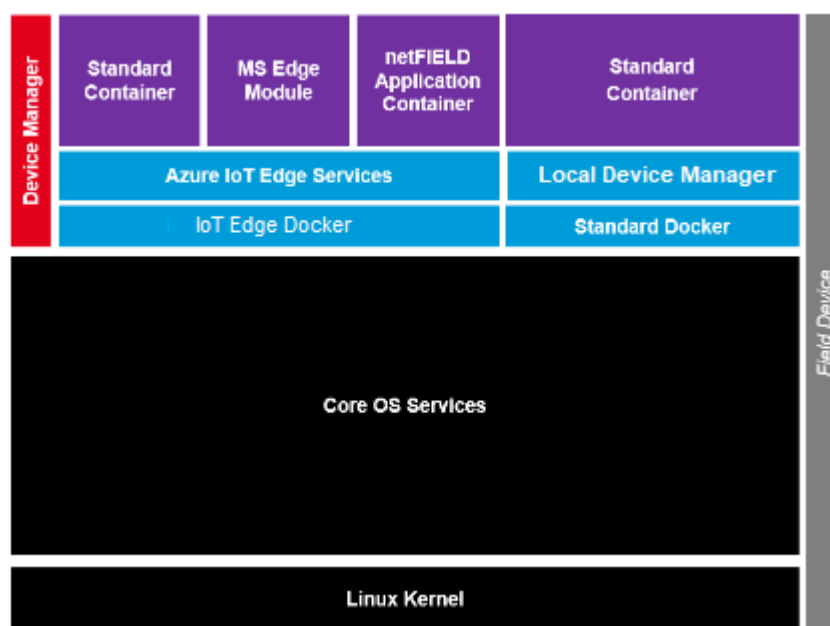


Figure 99: netFIELD OS container management

## 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.

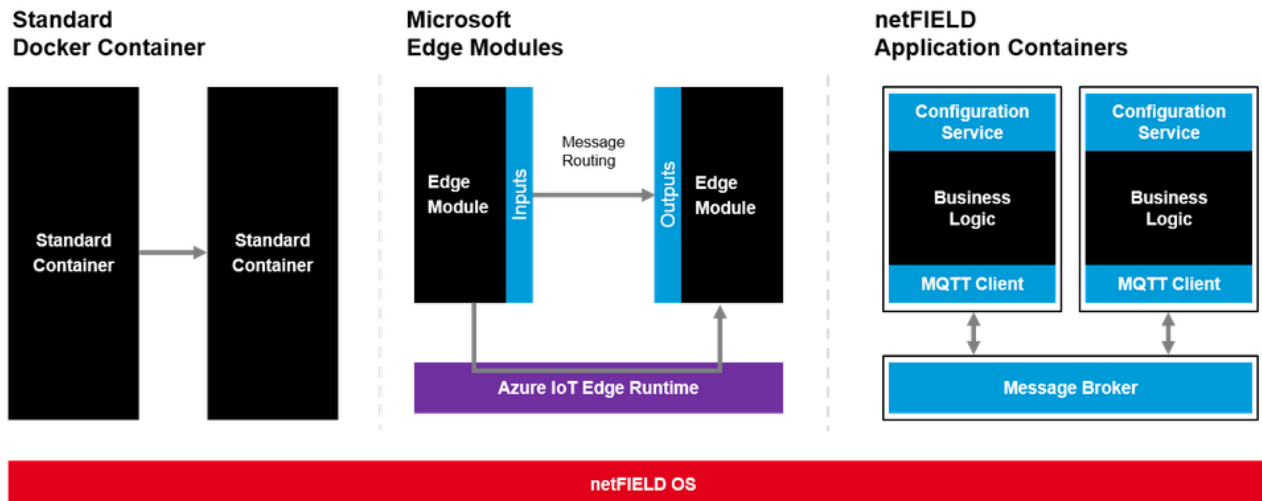


Figure 100: netFIELD OS inter-container communication

## Services supported by netFIELD OS

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

## 7 Legal notes

### Copyright

© Hilscher Gesellschaft für Systemautomation mbH

All rights reserved.

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

### Important notes

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

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

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

### Liability disclaimer

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

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

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

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

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

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

## Warranty

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

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

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

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

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

## Additional guarantees

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

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

## **Confidentiality**

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

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

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

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

## **Export provisions**

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

## List of Figures

Figure 1:	SW architecture with VMware ESXi .....	9
Figure 2:	SW architecture with KVM.....	10
Figure 3:	Proxmox VE.....	15
Figure 4:	General tab of Create Virtual Machine wizard.....	16
Figure 5:	OS tab of Create Virtual Machine wizard .....	16
Figure 6:	System tab of Create Virtual Machine wizard.....	17
Figure 7:	Hard Disk tab of Create Virtual Machine wizard.....	17
Figure 8:	CPU tab of Create Virtual Machine wizard .....	18
Figure 9:	Memory tab of Create Virtual Machine wizard.....	18
Figure 10:	Network tab of Create Virtual Machine wizard .....	19
Figure 11:	Confirm tab of Create Virtual Machine wizard .....	19
Figure 12:	New virtual machine .....	20
Figure 13:	Hardware parameters VM .....	21
Figure 14:	Unused disk.....	22
Figure 15:	New hardware parameters .....	22
Figure 16:	WinSCP upload .....	23
Figure 17:	Using Putty to import the image .....	24
Figure 18:	Imported image.....	24
Figure 19:	Unused Disk .....	25
Figure 20:	Attached hard disk.....	26
Figure 21:	Check boot order .....	27
Figure 22:	Edit boot order dialog .....	27
Figure 23:	VM started .....	28
Figure 24:	Console .....	29
Figure 25:	ESXi.....	30
Figure 26:	Select creation type .....	31
Figure 27:	Select OVF and VMDK files .....	31
Figure 28:	wizard3 .....	32
Figure 29:	Deployment options.....	33
Figure 30:	Ready to complete.....	33
Figure 31:	New virtual machine created .....	34
Figure 32:	Edit VM.....	35
Figure 33:	Edit hard disk size .....	35
Figure 34:	Console .....	36
Figure 35:	Sign In dialog of Local Device Manager .....	38
Figure 36:	Enter current password dialog.....	39
Figure 37:	Enter new password dialog .....	39
Figure 38:	Re-Authentication dialog .....	40
Figure 39:	System time value .....	41
Figure 40:	Change System Time dialog .....	41

Figure 41:	“Basic” onboarding screen in Local Device Manager .....	44
Figure 42:	Copy Hardware ID .....	46
Figure 43:	“Add device” mask in netFIELD Portal .....	47
Figure 44:	Activation Code in portal.....	48
Figure 45:	Advanced Onboarding tab in netFIELD OS.....	49
Figure 46:	Example of an API Key permitting to onboard devices .....	51
Figure 47:	Copy key to clipboard .....	52
Figure 48:	Overview Local Device Manager.....	53
Figure 49:	System page in Local Device Manager .....	55
Figure 50:	Change host name dialog.....	56
Figure 51:	Networking page.....	58
Figure 52:	Details of LAN interface (eth0) .....	59
Figure 53:	IPv4 Settings .....	60
Figure 54:	Manual IPv4 Settings.....	61
Figure 55:	Open Firewall configuration page.....	64
Figure 56:	Elements on Firewall configuration page.....	64
Figure 57:	Add Zone dialog .....	66
Figure 58:	Add services .....	69
Figure 59:	Add custom services dialog.....	70
Figure 60:	Add forward port dialog .....	71
Figure 61:	Network Proxy configuration.....	72
Figure 62:	Proxy Settings dialog window.....	73
Figure 63:	Using one Proxy server for all protocols.....	74
Figure 64:	Separate HTTP/HTTPS/FTP configuration .....	75
Figure 65:	Restart dialog after changing proxy server configuration .....	76
Figure 66:	Synchronize proxy settings with netFIELD Portal.....	77
Figure 67:	Basic Onboarding page .....	78
Figure 68:	Offboarding “Basic”.....	79
Figure 69:	Offboarding “Advanced” .....	80
Figure 70:	Standard Docker.....	81
Figure 71:	Expand concise container details .....	82
Figure 72:	Container parameters with terminal window.....	83
Figure 73:	Image Search dialog of Standard Docker.....	84
Figure 74:	Run Image dialog .....	85
Figure 75:	Expand image details .....	86
Figure 76:	Image details .....	87
Figure 77:	IOT Edge Docker.....	88
Figure 78:	Container details expanded.....	90
Figure 79:	Container parameters .....	91
Figure 80:	IoT image expanded.....	92
Figure 81:	Details of netFIELD Proxy image .....	93

Figure 82:	Accounts.....	94
Figure 83:	Create new account.....	94
Figure 84:	Edit account.....	95
Figure 85:	Web Server Certificate page .....	97
Figure 86:	General Settings.....	98
Figure 87:	Web Server Settings tab.....	99
Figure 88:	Default MQTT Settings .....	100
Figure 89:	Docker Network Settings .....	102
Figure 90:	Default docker network configuration .....	105
Figure 91:	Remote Access tab .....	106
Figure 92:	Terminal.....	108
Figure 93:	OS update page .....	109
Figure 94:	Selected OS update image.....	110
Figure 95:	Upload finished message .....	111
Figure 96:	OS update “Disconnected” message.....	111
Figure 97:	Logs.....	112
Figure 98:	netFIELD OS architecture .....	115
Figure 99:	netFIELD OS container management .....	116
Figure 100:	netFIELD OS inter-container communication .....	117

## List of Tables

Table 1:	List of revisions .....	4
Table 2:	Terms and abbreviations .....	6
Table 3:	Virtualization platforms for netFIELD OS Datacenter .....	11
Table 4:	Tasks for commissioning the netFIELD OS Datacenter (netFIELD Portal user) ....	13
Table 5:	Tasks for commissioning the netFIELD OS Datacenter (Standard Docker user)...	14
Table 6:	Available Firewall zones .....	65
Table 7:	Elements in Add Zone dialog .....	66
Table 8:	Columns/elements in Allowed Services table .....	68
Table 9:	Columns/elements in Forward Ports table .....	70
Table 10:	Control elements in main toolbar .....	71
Table 11:	Default MQTT Client Settings .....	101
Table 12:	Standard Docker Network Settings .....	103
Table 13:	Standard Docker Network Settings .....	104

# Contacts

## HEADQUARTERS

### Germany

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

### Support

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

## SUBSIDIARIES

### China

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

### Support

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

### France

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

### Support

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

### India

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

### Italy

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

### Support

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

### Japan

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

### Support

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

### Korea

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

### Switzerland

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

### Support

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

### USA

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

### Support

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