# Table of contents

## 1 Introduction

1.1 About the user manual .......................................................... 5
1.2 List of revisions .................................................................. 5
1.3 Further sources of information ........................................... 5

## 2 Brief description ................................................................ 6

## 3 Device drawings ................................................................. 7

3.1 Positions of the interfaces .................................................. 7
3.2 Dimensions ....................................................................... 9

## 4 Connectors and mounting .................................................... 10

4.1 Mounting ......................................................................... 10
4.2 Power supply .................................................................... 10
4.3 LAN connectors ................................................................. 10
4.4 USB connectors ................................................................. 10
4.5 Wi-Fi ............................................................................... 10
4.6 HDMI connector ............................................................... 11
4.7 Slot for expansion modules ............................................... 11

## 5 LEDs .................................................................................. 12

5.1 Positions of the LEDs on the gateway ............................... 12
5.2 Gateway status LEDs ....................................................... 13
5.3 LEDs of the LAN interface ................................................ 13

## 6 Commissioning the Edge Gateway ........................................ 14

6.1 Establishing the IP address communication ....................... 14
6.2 Using the web browser to establish a connection with the Edge Gateway ......................................................... 15
6.2.1 Using the host name ................................................... 15
6.2.2 Access to the Edge Gateway in the Windows network environment .............................................................. 16

## 7 Edge Gateway Manager ....................................................... 17

7.1 Calling the Edge Gateway Manager .................................... 17
7.2 Edge Gateway Manager web page ....................................... 18

## 8 Control Panel ...................................................................... 19

8.1 Opening the control panel .................................................. 19
8.1.1 First login .................................................................. 20
8.1.2 Secure connection ...................................................... 21
8.2 Overview and main menu .................................................. 25
8.3 System information and system time .................................. 27
8.3.1 Displaying system information .................................... 27
8.3.2 Displaying the system log files .................................... 28
8.3.3 Setting the system time ............................................... 32
8.3.4 Configure ports for HTTP/HTTPS communication .......... 35
8.3.5 Rebooting the system .................................................. 36
8.3.6 System shutdown ....................................................... 37
8.4 Packet management .......................................................... 38
# Table of contents

## 8.5 Network
- 8.5.1 Configuring Ethernet communication (LAN) ................................................................. 39
- 8.5.2 Configuring wireless communication (Wi-Fi) ................................................................. 39
- 8.5.3 Configuring cellular communication .............................................................................. 41
- 8.5.4 Configuring IP Routes ..................................................................................................... 46
- 8.5.5 Configuring Firewall ..................................................................................................... 51
- 8.5.6 Hostname ..................................................................................................................... 53

## 8.6 Services
- 8.6.1 Starting, stopping and configuring services ................................................................. 54

## 8.7 User management
- 8.7.1 Managing user roles ..................................................................................................... 55
- 8.7.2 Managing user accounts .............................................................................................. 57

## 8.8 Security
- 8.8.1 Public Key Infrastructure ............................................................................................. 58

## 8.9 Help
- ........................................................................................................................................ 61

## 8.10 Session
- 8.10.1 User profile ................................................................................................................ 61
- 8.10.2 Logout ........................................................................................................................ 62

## 9 Isolated application execution with Docker ................................................................. 63
- 9.1 Docker, Image, Container and Repository ........................................................................ 63
- 9.2 Prerequisites for working with Docker ............................................................................ 65
- 9.3 Container for netPI: Examples ........................................................................................ 66
- 9.4 Working with Docker via the web GUI ............................................................................ 67
  - 9.4.1 The portainer.io interface ......................................................................................... 67
  - 9.4.2 Commissioning ......................................................................................................... 67
  - 9.4.3 Starting the portainer.io interface for working with the containers ......................... 69
  - 9.4.4 Functions for working with containers ..................................................................... 72
  - 9.4.5 User management ..................................................................................................... 73
  - 9.4.6 Registry management ............................................................................................... 76
  - 9.4.7 Stack management .................................................................................................... 85

## 10 Public Key Infrastructure ............................................................................................ 91
- 10.1 Asymmetric encryption ................................................................................................. 92
- 10.2 Certificates and keys ..................................................................................................... 94
  - 10.2.1 Structure of a certificate according to X.509 ............................................................ 94
  - 10.2.2 Hierarchy of trust ..................................................................................................... 95
  - 10.2.3 File formats for certificate and key files .................................................................. 96
- 10.3 Use cases ...................................................................................................................... 97
  - 10.3.1 Use case 1: Verification of the authenticity of the communication partner (Server) ......................... 97
  - 10.3.2 Use case 2: Server certificates for Edge Gateway services .................................... 98
- 10.4 Verification of the authenticity of the communication partner using trustworthy certificates .................................................................................................................. 100
  - 10.4.1 Display the list of trustworthy root certificates stored within the Edge Gateway .. 100
  - 10.4.2 Upload a trustworthy certificate into the Edge Gateway ......................................... 101
  - 10.4.3 Download of certificates from the Edge Gateway into a file .................................. 102
  - 10.4.4 Removing certificates no longer considered as trustworthy .................................. 102
- 10.5 Working with server certificates for inbound connections ........................................ 103
10.5.1 Uploading a pair of certificate file and key file for HTTPS und OPC UA Server  
10.5.2 Working with certificates for HTTPS and OPC UA Server ......................... 107  
10.5.3 Working with key files for HTTPS and OPC UA Server ........................... 109

11 Technical data ....................................................................................................... 110  
11.1 Technical data NIOT-E-NPI3-EN .................................................................... 110

12 Decommissioning, dismounting and disposal .................................................... 112  
12.1 Putting the device out of operation .................................................................. 112  
12.2 Disposal of waste electronic equipment ............................................................ 112

13 Appendix ............................................................................................................ 113  
13.1 Legal notes ..................................................................................................... 113

List of figures .......................................................................................................... 117

List of tables ........................................................................................................... 119

Contacts ............................................................................................................... 120
1 Introduction

1.1 About the user manual

This user manual describes the installation, configuration and functionality of the device NIOT-E-NPI3-EN.

In this description, the device NIOT-E-NPI3-EN is named **netPI** and **Edge Gateway** likewise. The name **netPI** is in reference to the Raspberry Pi function and **Edge Gateway** is in reference to the use on the “Edge” between the IT network and the OT network.

1.2 List of revisions

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring Ethernet communication (LAN) [↓ page 39] updated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>and DHCP server added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring cellular communication [↓ page 46] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring IP Routes [↓ page 47] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring Firewall [↓ page 51] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Chapter Isolated application execution with Docker [↓ page 63] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Technical data NIOT-E-NPI3-EN [↓ page 110]: Ratings added for UL-</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>conform usage.</td>
</tr>
</tbody>
</table>

Table 1: List of revisions

1.3 Further sources of information

The following table lists web addresses where you can get further information for netPI.

<table>
<thead>
<tr>
<th>Web address</th>
<th>This site offers you</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://www.netiot.com/netPI">https://www.netiot.com/netPI</a></td>
<td>Product presentation, documentation, tutorials, informationen</td>
</tr>
<tr>
<td></td>
<td>on expansion modules, blog, FAQ, and forum on netPI and IIoT.</td>
</tr>
<tr>
<td><a href="https://hub.docker.com/r/">https://hub.docker.com/r/</a></td>
<td>Docker hub with example images for netPI.</td>
</tr>
<tr>
<td>hilschernetpi/</td>
<td></td>
</tr>
<tr>
<td><a href="https://www.raspberrypi.org/">https://www.raspberrypi.org/</a></td>
<td>Information, blog, downloads, community, forum, and education</td>
</tr>
<tr>
<td></td>
<td>on Raspberry Pi.</td>
</tr>
</tbody>
</table>

Table 2: Further information
2 Brief description

netPI is a Raspberry Pi 3 architecture based platform for implementing Cloud, Internet of Things and Industry 4.0 customized Edge Automation projects safely. The device contains the original Raspberry Pi 3B circuitry.

The LAN interface connects to the IT network and is the interface for the device configuration via a web browser. With the WiFi antenna, the device supports also wireless network communication.

To expand the functional range of the device a slot for expansion modules is provided, e.g. a module for digital I/Os.

The system of netPI is based on an AppArmor-secured Yocto Linux build. The device boots secure, and only allows system changes with integrity-checked Hilscher software. User access is granted via a web browser over https-secured connections only.

The only preinstalled open source software „Docker“ by Docker, Inc. allows the user to execute own applications on the secured Linux operating system of the Edge Gateways while all protection mechanisms are fully preserved. The applications are executed in protected, isolated runtime environments. To accomplish this, Docker uses special techniques from virtualization of operating systems.
3 Device drawings

3.1 Positions of the interfaces

Figure 2: NIOT-E-NPI3-EN (Top view)

Figure 3: NIOT-E-NPI3-EN (Front view)
Figure 4: NIOT-E-NPI3-EN (Bottom view)

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Interface</th>
<th>For details see</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Connector for digital LCD display (HDMI)</td>
<td>HDMI connector [† page 11]</td>
</tr>
<tr>
<td>(2)</td>
<td>USB connectors (2x USB 2.0 on top of device)</td>
<td>USB connectors [† page 10]</td>
</tr>
<tr>
<td>(3)</td>
<td>Antenna (1 x Wi-Fi)</td>
<td>Wi-Fi [† page 10]</td>
</tr>
<tr>
<td>(4)</td>
<td>Gateway status LEDs (4 x)</td>
<td>Gateway status LEDs [† page 13]</td>
</tr>
<tr>
<td>(5)</td>
<td>USB connectors (2x USB 2.0 on front of device)</td>
<td>USB connectors [† page 10]</td>
</tr>
<tr>
<td>(6)</td>
<td>LAN connector (RJ45 jacket) port 1 / Eth0</td>
<td>LAN connectors [† page 10]</td>
</tr>
<tr>
<td>(7)</td>
<td>+24 V DC supply voltage connector (Mini Combicon)</td>
<td>Power supply [† page 10]</td>
</tr>
<tr>
<td>(8)</td>
<td>Slot for expansion module (Cover bolted)</td>
<td>Slot for expansion modules [† page 11]</td>
</tr>
</tbody>
</table>

Table 3: Positions of the interfaces
3.2 Dimensions

*Figure 5: Dimensions*
4 Connectors and mounting

4.1 Mounting

Mount the Edge Gateway on a DIN rail onto the wall of the cabinet.

4.2 Power supply

<table>
<thead>
<tr>
<th>DC 24V</th>
<th>Pin</th>
<th>Signal</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>GND</td>
<td>Ground</td>
<td>(Reference potential)</td>
</tr>
<tr>
<td>+</td>
<td>+24 V DC</td>
<td>+24 V DC</td>
<td></td>
</tr>
<tr>
<td>FE</td>
<td></td>
<td>Functional earth</td>
<td></td>
</tr>
</tbody>
</table>

*Table 4: Power supply connector*

4.3 LAN connectors

The Edge Gateway has one LAN connector for connecting it to the cloud network (IT network), position (6) (see section *Positions of the interfaces* [page 7]).

The MAC addresses of the LAN interfaces are printed on the device label.

Section *Configuring Ethernet communication (LAN)* [page 39] describes how you can set the IP address parameters of the LAN interfaces.

4.4 USB connectors

The Edge Gateway has - USB connectors (4 x USB 2.0), positions (2) and (5) (see section *Positions of the interfaces* [page 7]).

You can connect for example a USB stick, an external hard drive or a keyboard and use it together with a Docker image.

4.5 Wi-Fi

The Edge Gateway is equipped with a Wi-Fi interface. It supports 2 Wi-Fi operating modes: Access Point and Client. Operating mode Access Point allows the Edge Gateway to connect to other Wi-Fi devices in order to configure the Edge Gateway from a mobile device for example. Operating mode Client allows the Edge Gateway to be connected to any Wi-Fi Access Point.

Section *Configuring wireless communication (Wi-Fi)* [page 41] describes how you activate the antennas and how to set the Wi-Fi operating mode.
4.6 HDMI connector

The Edge Gateway has an HDMI-connection for a monitor (position (1)) which is not required for the operation of the Edge Gateway.

The HDMI interface is inactive by default and just outputs boot information during the boot process of the device. If you want to use it, find an example docker image with activated HDMI interface and desktop at https://hub.docker.com/r/hilschernetpi/.

4.7 Slot for expansion modules

To expand the functional range of the device a slot for expansion modules is provided, e.g. a module for digital I/Os.
5 LEDs

5.1 Positions of the LEDs on the gateway

Figure 6: LED positions

<table>
<thead>
<tr>
<th>Pos.</th>
<th>LED</th>
<th>For details see</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Gateway status LEDs (4 x)</td>
<td>Gateway status LEDs [13, page 13]</td>
</tr>
<tr>
<td>(2)</td>
<td>ACT / Rx/Tx LAN</td>
<td>LEDs of the LAN interface [13, page 13]</td>
</tr>
<tr>
<td>(3)</td>
<td>LINK LAN</td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Names of the LEDs
5.2 Gateway status LEDs

LEDs indicating the voltage supply and status information. The position of the LEDs is indicated by position (3) in section Positions of the LEDs on the gateway [† page 12].

![Gateway status LEDs]

Figure 7: Gateway status LEDs

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED1</td>
<td>(yellow)</td>
<td>-</td>
<td>GPIO12, programmable</td>
</tr>
<tr>
<td>LED2</td>
<td>(yellow)</td>
<td>-</td>
<td>GPIO13, programmable</td>
</tr>
<tr>
<td>ACT</td>
<td>(green)</td>
<td>Blinking</td>
<td>Activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Linux operating system is active.</td>
</tr>
<tr>
<td>POW</td>
<td>(green)</td>
<td>On</td>
<td>Supply voltage OK</td>
</tr>
<tr>
<td></td>
<td>(off)</td>
<td>Off</td>
<td>No supply voltage or supply voltage below 4.65 V.</td>
</tr>
</tbody>
</table>

Table 6: Description of gateway status LEDs

5.3 LEDs of the LAN interface

LEDs indicating state of the LAN communication. For the positions of the LAN LEDs, see section Positions of the LEDs on the gateway [† page 12].

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT / RX/TX</td>
<td>LED yellow</td>
<td>Flickering (load dependent)</td>
<td>The device sends/receives frames</td>
</tr>
<tr>
<td></td>
<td>(yellow)</td>
<td></td>
<td>The device does not send/receive frames.</td>
</tr>
<tr>
<td></td>
<td>(off)</td>
<td>off</td>
<td></td>
</tr>
<tr>
<td>LINK</td>
<td>LED green</td>
<td>On</td>
<td>100 MBit MBit network connection</td>
</tr>
<tr>
<td></td>
<td>(green)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(off)</td>
<td>off</td>
<td>10 MBit or no network connection</td>
</tr>
</tbody>
</table>

Table 7: LEDs LAN interface
6 Commissioning the Edge Gateway

6.1 Establishing the IP address communication

An IP address is required to address the Edge Gateway in the LAN network.

The following figure shows the factory setting of the LAN interface and the assignment to the connector.

![LAN interface and configuration](image)

**Figure 8: LAN interface and configuration**

**Network connection - DHCP server available**

If a DHCP server is available in the network:

- Use an Ethernet cable to connect the LAN connection port 1 (eth0) (see (6) in *Positions of the interfaces* [page 7]) with a network in which a DHCP server is available.

- The Edge Gateway obtains an IP address from the DHCP server. Access to the Edge Gateway is possible now.

---

**Note:**

The Edge Gateway sends a request to a DHCP server once after switching on the device or after each connection of the Ethernet cable, i.e. when the Edge Gateway detects a link signal. If you want to activate a request of the Edge Gateway to the DHCP server manually, pull off the Ethernet cable from the Edge Gateway and reconnect it to the Edge Gateway.

Read section *Using the web browser to establish a connection with the Edge Gateway* [page 15] to find out how to access the Edge Gateway.
6.2 Using the web browser to establish a connection with the Edge Gateway

You have three possibilities to access the Edge Gateway:

1. by means of the host name (see section Using the host name [page 15])
2. by access via the Windows network (see section Access to the Edge Gateway in the Windows network environment [page 16]),
3. by using the IP address (see section Using the IP address).

6.2.1 Using the host name

The Edge Gateway has a host name you can use to access the device.

Where do you find the host name on the device?

The device is delivered (factory setting) with a label printed at its bottom. In the figure below the host name has a red frame.

![Figure 9: NIOT-E-NPI3-EN device label (Host name)](image)

Establishing a connection with the host name

- Enter the following address in the address line of your browser:
  
  https://<hostname>

  **Example:** For the device with the host name NTB827EB1D9D94 enter
  
  https://NTB827EB1D9D94

- The Edge Gateway Manager opens.

You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway Manager web page* [page 18].
6.2.2 Access to the Edge Gateway in the Windows network environment

To be located easily in the network, the Edge Gateway uses the UPnP technology (Universal Plug and Play). This technology will display the Edge Gateway in the Windows network environment.

- To display all devices in the network, click on **Network** in the Windows Explorer.

- You will find the Edge Gateway under **Other Devices**:

  ![Edge Gateway icon](image)

  - Open the context menu of this entry and select **Properties**.
  - The menu provides information on the Edge Gateway, e.g. serial number, MAC address, host name or die IP address.
  - Click on the link under Device web page.
  - The Edge Gateway manager opens.
  - To open the Edge Gateway manager, you can also double-click on the device icon.

  ![Edge Gateway manager open](image)

  - The Edge Gateway manager opens.

You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway Manager web page* [page 18].
7 Edge Gateway Manager

7.1 Calling the Edge Gateway Manager

The Edge Gateway manager is a web page with tiles that allow rapid access to the applications integrated in the device or to external web pages.

The Edge Gateway uses the secured HTTPS protocol to access web pages stored in the Edge Gateway.

- To open the Edge Gateway manager, enter the following information in the address line of your browser:
  
  https://<Host name of the Edge Gateway>
  
  or
  
  https://<IP address of the Edge Gateway>
  
- Your browser displays the Edge Gateway manager.

Note: Remember that the secured HTTPS protocol is used here, not the widely spread HTTP protocol.
7.2 Edge Gateway Manager web page

The Edge Gateway Manager displays tiles that allow rapid access to the applications integrated in the device or external web pages.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Control Panel" /></td>
<td>Opens the control panel of the Edge Gateway. The control panel configures the Edge Gateway and displays information on the system. Section Control Panel [(\text{page } 19)] describes the possibilities of configuration as well as the displayed information on the system.</td>
</tr>
<tr>
<td><img src="image" alt="Docker Management" /></td>
<td>Opens the Docker management. See section Isolated application execution with Docker [(\text{page } 63)].</td>
</tr>
<tr>
<td><img src="image" alt="Documentation" /></td>
<td>Opens the Edge Gateway documentation stored in the device.</td>
</tr>
<tr>
<td><img src="image" alt="Device Information Portal" /></td>
<td>Opens the homepage of the Device Information Portal in the Internet. Requires a connection to the Internet.</td>
</tr>
<tr>
<td><img src="image" alt="netIOT Platform" /></td>
<td>Opens the homepage of the netIOT platform in the Internet. Requires a connection to the Internet.</td>
</tr>
<tr>
<td><img src="image" alt="Hilscher Homepage" /></td>
<td>Opens the Hilscher homepage in the Internet. Requires a connection to the Internet.</td>
</tr>
</tbody>
</table>

Table 8: Starting applications with the Edge Gateway Manager
8 Control Panel

8.1 Opening the control panel

With the control panel you can configure the Edge Gateway and display device-specific information.

- Click the tile **Control Panel**.

- The login screen for the **Control Panel** is displayed.

- Enter your user name and your password.
- Click at **Login**.
  - The **Control Panel** will be displayed.
8.1.1 First login

Setting the administrator password when the control panel is called for the first time

The dialog box **Set Administrator Password** is displayed when the control panel is called for the first time.

![Set Administrator Password](image)

*Figure 11: Edge Gateway Manager - Setting the administrator password*

To set a new administrator password, proceed as follows:

- Enter the preset password under **Current Password**. With the first commissioning, the password is: admin
- Enter the new administrator password. It must have at least 7 characters. For reasons of safety, Hilscher recommends using significantly more characters. A strong password consists of upper and lower case letters, digits and special characters. A quality indicator in the dialog box evaluates the password.
- Click **Change Password** only after the entered password has been evaluated as strong.
- The administrator password for the user account **Admin** has thus been changed.
As an administrator you can now use the control panel, create further users in the user management, and assign access rights.

8.1.2 Secure connection

Edge Gateways support web connections secured by SSH/TSL via https:// accesses only.

By definition, a secure connection can provide an efficient protection only if a certificate proves that the server is secure. Only then can running transactions of the initiating browser and the server be considered as protected against interception and data theft.

This is why the browser at first inquires a certificate of verification from the server (Gateway). This certificate proves that the issuer has verified the security of the server. Each browser provides a preinstalled list of known authorized issuers of certificates.

Each time the certificate of the server arrives at the browser, the browser compares the issuer of the certificate with the issuers stored in the list of known authorized issuers of certificates.

If the issuer of the certificate is not listed, the browser will signal a certificate error and request the user's confirmation to continue because it assumes that the connection is insecure.

As standard, Edge Gateways contain a certificate issued by Hilscher that is not on the list of the known authorized issuers of certificates. Due to that, the browser signals an insecure connection and requests the confirmation to continue. When this confirmation has been given once, any future connections will be established without further requests.

**Note:**
In the control panel you can replace this certificate any time by the certificate of a known authorized issuer of certificates, see section Uploading and installing own security certificates).
8.1.2.1 Connection without certificate with Microsoft Internet Explorer

**Microsoft Internet Explorer: Edge Gateway Manager will not be displayed**

If you use the Microsoft Internet Explorer and the following page is displayed, click the option **Continue to this web site (not recommended)**.

![Security error message of the Internet Explorer](image1)

*Figure 12: Security error message of the Internet Explorer*

8.1.2.2 Connection without certificate with Firefox

If you use Firefox as a browser, a self-signed certificate will cause the following error message:

![Security error message of the Firefox browser (1)](image2)

*Figure 13: Security error message of the Firefox browser (1)*

To avoid this message caused by a self-signed certificate, proceed as follows:

- To display the complete message, click **Advanced**.

![Security error message of the Firefox browser (2)](image3)

*Figure 14: Security error message of the Firefox browser (2)*

- To define an exceptional rule that enables the display of the user interface without repeated error messages, click **Add Exception**.
Figure 15: Firefox dialog box: Adding exceptional safety rule

- To save the setting permanently, check the box **Permanently store this exception.**
- To save the rule, click **Confirm Security Exception.**
- When you open the control panel in future, security messages will no longer be displayed.
8.1.2.3 Connection without certificate with Google Chrome

If you use Google Chrome as web browser, you will get the following error message due to a self-signed certificate.

![Security error message of Google Chrome (1)](image1)

Figure 16: Security error message of Google Chrome (1)

Proceed as follows in order to avoid the following message, which is caused by a self-signed certificate,

- Click at **ADVANCED** to display the complete message.

![Security error message of Google Chrome (2)](image2)

Figure 17: Security error message of Google Chrome (2)

- In order to continue, click at **Proceed to ... (unsafe)**.
- The Control Panel is displayed.
# 8.2 Overview and main menu

The following figure displays the main menu of the Control Panel.

![Main menu of the Control Panel](image)

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>System &gt; Info Center</td>
<td>Displaying the system information, monitoring of the processor core temperature, and a system monitor for the usage of CPU, main memory, and SSD.</td>
<td>Displaying system information [† page 27]</td>
</tr>
<tr>
<td>System &gt; Syslog</td>
<td>Displaying the system log files.</td>
<td>Displaying the system log files [† page 28]</td>
</tr>
<tr>
<td>System &gt; Time</td>
<td>Settings of system time and time synchronization.</td>
<td>Setting the system time [† page 28]</td>
</tr>
<tr>
<td>System &gt; Port Settings</td>
<td>Port configuration for HTTP/HTTPS communication.</td>
<td>Configure ports for HTTP/HTTPS communication [† page 32]</td>
</tr>
<tr>
<td>System &gt; Reboot</td>
<td>Rebooting the Linux operating system of the Edge Gateway</td>
<td>Rebooting the system [† page 33]</td>
</tr>
<tr>
<td>System &gt; Shutdown</td>
<td>Shutting down the Linux operating system of the Edge Gateway</td>
<td>System shutdown [† page 34]</td>
</tr>
<tr>
<td>Package Manager &gt; Packages</td>
<td>Managing the packages of the Linux-based operating system of the Edge Gateway.</td>
<td>Managing packets [† page 35]</td>
</tr>
<tr>
<td>Network &gt; LAN</td>
<td>Configuring the Ethernet interfaces to the IT network and OT network (fieldbus).</td>
<td>Configuring Ethernet communication (LAN) [† page 36]</td>
</tr>
<tr>
<td>Network &gt; Wi-Fi</td>
<td>Configuring the Wi-Fi communication</td>
<td>Configuring wireless communication (Wi-Fi) [† page 37]</td>
</tr>
<tr>
<td>Network &gt; Cellular</td>
<td>Configuration of the cellular interface.</td>
<td>Configuring cellular communication [† page 38]</td>
</tr>
<tr>
<td>Network &gt; Routes</td>
<td>Configuration of interfaces or connections for certain IP destination addresses.</td>
<td>Configuring IP Routes [† page 39]</td>
</tr>
<tr>
<td>Network &gt; Firewall</td>
<td>Firewall configuration for each interface or connection.</td>
<td>Configuring Firewall [† page 40]</td>
</tr>
<tr>
<td>Network &gt; Hostname</td>
<td>Displaying and configuring the host name identifying the Edge Gateway in the network.</td>
<td>Hostname [† page 41]</td>
</tr>
<tr>
<td>Services &gt; Service List</td>
<td>Displaying, starting, and stopping the services of the Edge Gateway.</td>
<td>Starting, stopping and configuring services [† page 42]</td>
</tr>
<tr>
<td>User Management &gt; Roles</td>
<td>Displaying and configuring the permissions for user roles.</td>
<td>Managing user roles [† page 43]</td>
</tr>
<tr>
<td>User Management &gt; Accounts</td>
<td>Displaying user accounts and assigning user roles.</td>
<td>Managing user accounts [† page 44]</td>
</tr>
<tr>
<td>Security &gt; Public Key Infrastructure</td>
<td>Store and administer certificates and key files within the Public Key Infrastructure</td>
<td>Public Key Infrastructure [† page 45]</td>
</tr>
<tr>
<td>Help &gt; Info</td>
<td>Displaying the current software version.</td>
<td>Help [† page 46]</td>
</tr>
<tr>
<td>Session &gt; User Profile</td>
<td>Displaying the permissions of the user.</td>
<td>User profile [† page 47]</td>
</tr>
<tr>
<td>Session &gt; Logout</td>
<td>Logout</td>
<td>Logout [† page 48]</td>
</tr>
</tbody>
</table>

Table 9: Functional overview of the Control Panel
For the pages which can be invoked via the Control Panel, the following applies:

If for the selected page, no access right for reading is present, this has the following implications:

- No data are displayed. All important controls and displays of the page are grayed out respectively inactive.
- The error message **Permission denied** is displayed when accessing the page.

If there is read but no write access right present, this has the following implications:

- The error message **Permission denied** is displayed when trying to make a change.
8.3 System information and system time

8.3.1 Displaying system information

Open this page with **System > Info Center**. No access rights are required in order to open this page. This page shows e.g. the firmware version and the serial number of the Edge Gateway.

![Figure 19: Page Info Center](image)

The Info Center displays the following information:

<table>
<thead>
<tr>
<th>System info</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware ident.</td>
<td>Serial number of the Edge Gateway</td>
</tr>
<tr>
<td>Model name</td>
<td>Model designation of the Edge Gateway (NIOT-E-NPI3-EN)</td>
</tr>
<tr>
<td>Firmware version</td>
<td>Complete version designation of the firmware stored in the Edge Gateway</td>
</tr>
<tr>
<td>System time</td>
<td>Synchronization status of the internal clock of the Edge Gateway. When the clock is synchronized via the network, the IP address and the name of the time server used for synchronization will be displayed. The user has to configure the time zone.</td>
</tr>
<tr>
<td>Processor name</td>
<td>Name of the microprocessor (CPU) installed in the Edge Gateway.</td>
</tr>
</tbody>
</table>

*Table 10: Info Center: Area System info*
<table>
<thead>
<tr>
<th>Monitoring</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU usage</td>
<td>Number of microprocessor cores plus clock frequency and average utilization of each core in the Edge Gateway</td>
</tr>
<tr>
<td>Memory utilization</td>
<td>Size and average utilization of the main memory in the Edge Gateway</td>
</tr>
<tr>
<td>Storage space</td>
<td>Display of available memory and the memory that is currently utilized on the integrated Solid-State-Disk of the Edge Gateway</td>
</tr>
</tbody>
</table>

Table 11: Info Center: Area Monitoring

<table>
<thead>
<tr>
<th>Temperature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU temperature</td>
<td>Display of the temperature of each processor core in the Edge Gateway</td>
</tr>
</tbody>
</table>

Table 12: Info Center: Area Temperature

If the data of the area Monitoring cannot be read, this is grayed out.

### 8.3.2 Displaying the system log files

**System log service and syslog file**

At any time, a Linux system executes many programs running in parallel within the background. Usually, these are denominated as services, servers or daemons. They perform a large part of the work of the operating system. As they run in the background, these programs do not have a GUI and so they are not able to manage output directly, for instance in case of events relevant for system administration.

Such messages originate from
1. the Linux kernel (the central part of the operating system)
2. the daemons (programs executing the system services)
3. user programs

Therefore, these messages are collected by a central system log service (syslog) and are distributed depending on their priority and origin according to a configurable set of rules.

So, for system supervision and safeguarding correct reaction on error situations, the file logging daemon syslogd (or an improved successor of it) runs on every Linux system. On the Edge Gateways from Hilscher, the widely-spread logging daemon Syslog-ng is used, which had been developed by BalaBit IT Security Ltd. (now: One Identity, [https://syslog-ng.org/](https://syslog-ng.org/)).

**Opening the system log**

To access the syslog files generated by Syslog-ng, open this page within the main menu of the control panel using System > Syslog. Read access rights are required to open this page. The page shows you a list of stored system logs covering different periods in time. This list also contains the last date of change and the file size specified in KB. Within this list, each line corresponds to a gzip-compressed system log file for a specific time period.
Select the desired entry within table **Syslog files**.

The selected line is highlighted instantly.

Click at button Download in the header of window **Syslog files**.

Your Web browser loads the file down from the Edge Gateway and offers options for further processing of the downloaded file such as Open, Open directory. The file has been compressed with the program gzip and must be unpacked prior to evaluation.

### 8.3.2.1 Structure of system log file

The structure of the entries has been originally defined by the IETF within RFC3164 ([https://tools.ietf.org/html/rfc3164](https://tools.ietf.org/html/rfc3164)), meanwhile it has been reworked and substituted by RFC5424 ([https://tools.ietf.org/html/rfc5424](https://tools.ietf.org/html/rfc5424)). The structure of the entries in the system log files of the Edge Gateways also follows this structure.

**HEADER**

The header starts with the priority, denominated as PRI within the standard. The priority is an integer number enclosed by angled brackets like `<45>`, for instance.

The priority can be calculated from two numeric values:

- the facility (signifying the origin of the message, located within the upper 5 Bits)
- the severity (signifying the urgency and importance of the message, located within the lower 3 Bits)

The following formula accomplishes this:

\[
\text{Priority} = 8 \times \text{Facility} + \text{Severity}
\]
The facility is coded according to the following table:

<table>
<thead>
<tr>
<th>Code</th>
<th>Facility (Origin of message)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Kernel messages</td>
</tr>
<tr>
<td>1</td>
<td>User-level message</td>
</tr>
<tr>
<td>2</td>
<td>Mail system</td>
</tr>
<tr>
<td>3</td>
<td>System daemons</td>
</tr>
<tr>
<td>4</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>5</td>
<td>Messages generated internally by syslogd</td>
</tr>
<tr>
<td>6</td>
<td>Line printer subsystem</td>
</tr>
<tr>
<td>7</td>
<td>Network news subsystem</td>
</tr>
<tr>
<td>8</td>
<td>UUCP subsystem</td>
</tr>
<tr>
<td>9</td>
<td>Clock daemon</td>
</tr>
<tr>
<td>10</td>
<td>Security/authorization messages</td>
</tr>
<tr>
<td>11</td>
<td>FTP daemon</td>
</tr>
<tr>
<td>12</td>
<td>NTP subsystem log audit</td>
</tr>
<tr>
<td>13</td>
<td>Log audit</td>
</tr>
<tr>
<td>14</td>
<td>Log alert</td>
</tr>
<tr>
<td>15</td>
<td>Clock daemon</td>
</tr>
<tr>
<td>16...23</td>
<td>Locally used facilities (local0-local7)</td>
</tr>
</tbody>
</table>

*Table 13: Numeric coding of facility value in priority PRI*

The severity is coded according to the following table:

<table>
<thead>
<tr>
<th>Code</th>
<th>Severity (Importance of message)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Emergency: System is currently in an unusable state</td>
</tr>
<tr>
<td>1</td>
<td>Alert: Immediate action required</td>
</tr>
<tr>
<td>2</td>
<td>Critical: The system is in a critical state</td>
</tr>
<tr>
<td>3</td>
<td>Error: Error messages are present</td>
</tr>
<tr>
<td>4</td>
<td>Warning: Warning messages are present</td>
</tr>
<tr>
<td>5</td>
<td>Notice: Normal state of operation, but there is an important Information</td>
</tr>
<tr>
<td>6</td>
<td>Informational: Informational messages are present</td>
</tr>
<tr>
<td>7</td>
<td>Debug: Messages on debug level are present</td>
</tr>
</tbody>
</table>

*Table 14: Numeric coding of severity value in priority (PRI)*

**VERSION**

Here the version number of the current syslog protocol standard is put out. As this is still in version 1, the version without any exception always equals to 1.

**ISOTIMESTAMP**

This part of the message line contains a timestamp in ISO 8601-compatible standard format (yyyy-mm-ddThh:mm:ss+-ZONE). This time stamp relates to the point in time at that the message has been generated.

Example

```
07/06/2018 15:59:41
```

**HOSTNAME**

This part of the message line contains the name of the machine originally sending the message. The length of HOSTNAME is limited to 255 characters.

**APPLICATION**

This part of the message line contains the name of the device or application originally generating the message. The length of APPLICATION is limited to 48 characters.
This part of the message line contains the name of the process or the process ID of the syslog application originally sending the message. This may not necessarily be the process ID of the application generating the message. The length of PID is limited to 128 characters.

This is the ID of the message itself. The length of MESSAGEID is limited to 32 characters.

This part of the message line may contain metadata on the message line or application-specific information such as counters or IP addresses. It consists of data blocks enclosed in angled brackets []. Each block contains an ID and one or more pairs of the form name=value.

Example

[meta sequenceId="1"]

This part of the message line contains the genuine text of the message. It can either be coded in UTF-8 (if a BOM character has been detected) or otherwise it is ASCII-coded.

Example of complete message line

A message line may look as follows:

```<45>1 2018-07-06T13:59:41+00:00 localhost syslog-ng 1524 - [meta sequenceId="1"] syslog-ng starting up; version='3.8.1'
```

The following table shows the assignment of the parts of this specific message line:

<table>
<thead>
<tr>
<th>Part of message line</th>
<th>Corresponding denomination</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;45&gt;</td>
<td>PRI (Priority)</td>
</tr>
<tr>
<td>1</td>
<td>VERSION (Versions number of current syslog protocol standard)</td>
</tr>
<tr>
<td>2018-07-06T13:59:41+00:00</td>
<td>ISOTIMESTAMP</td>
</tr>
<tr>
<td>localhost</td>
<td>HOSTNAME</td>
</tr>
<tr>
<td>syslog-ng</td>
<td>APPLICATION</td>
</tr>
<tr>
<td>1524</td>
<td>PID (Process name or process D of syslog application sending the message)</td>
</tr>
<tr>
<td>-</td>
<td>MESSAGEID</td>
</tr>
<tr>
<td>[meta sequenceId=&quot;1&quot;]</td>
<td>STRUCTURED-DATA (Meta information)</td>
</tr>
<tr>
<td>syslog-ng starting up; version='3.8.1'</td>
<td>MSG (Real message text)</td>
</tr>
</tbody>
</table>

Table 15: Assignment of parts of message line

8.3.2.2 Log rotation

The Edge Gateway is configured for a daily change of the logging file and to keep the files of the last seven days. This procedure is denominated as log rotation.
8.3.3 Setting the system time

Open this page with **System > Time**.

To access this page, you need rights for the resource: **Setting the system time**

On this page you can set the system time and the time zone this time relates to.

You can set the system time in two ways:

<table>
<thead>
<tr>
<th>Type</th>
<th>Selection</th>
<th>Method</th>
<th>Standard presetting</th>
</tr>
</thead>
<tbody>
<tr>
<td>manually</td>
<td>Manual selection</td>
<td>by entering date and time</td>
<td>no.</td>
</tr>
<tr>
<td>automatically</td>
<td>NTP synchronized</td>
<td>by means of a time server</td>
<td>yes</td>
</tr>
</tbody>
</table>

*Table 16: Setting the system time*

*Figure 21: Time configuration page*

**Note:**
When you change a system time setting, always reboot the Edge Gateway afterwards so that all software components in the Edge Gateway take the changed time: **System > Reboot**.
Setting the system time manually

- Click the option Manual.
- Enter the time in the input field Time in the format hh:mm:ss.
- Set the date using the calendar input field Date.
- Click Save changes.
- Reboot the device: System > Reboot in order that all software components in the Edge Gateway take the changed time.
- The system time is set.

Setting the system time automatically using a time server

You can synchronize the time using a time server that uses the Network Time Protocol (NTP). Under NTP synchronized there is a list where you can enter such time servers. The list of NTP servers will be worked off from top to bottom until a server gives a valid answer and synchronization occurs.

- Click the option NTP Synchronized.
- Click Add NTP server.
- The dialog box for entering the NTP server is displayed.

In the input field NTP server enter the address of a server which uses the NTP to synchronize the time:
E.g.: To add the server for time synchronization of the Physikalisch-Technische Bundesanstalt (the National Metrology Institute of Germany) to the list, enter the address ptbtime1.ptb.de in the input field NTP server.

- Click Add.
- Click Save changes.
- Reboot the device: System > Reboot in order that all software components in the Edge Gateway take the changed time.
- The system time is set via the NTP. As soon as the system time is set successfully, the following information will be displayed under Status:
Synchronized to time server <IP address of the time server>:<Port number of the time server > (<NTP address of the time server>)
Setting the time zone

With the selection list **Timezone** you can adjust the time zone to your local time in which the Edge Gateway is so that the set time can be interpreted correctly (e.g. summer time conversion). For this purpose, the selection list **Timezone** offers many setting options. The default value is **Universal**. For Central European Time set **CET**.

---

**Note:**

Once the system time has been set, system services and Node-RED flows which use the system time for synchronization loose their reference time, i.e. they refer to the new time set. When you change a system time setting, always reboot the Edge Gateway afterwards so that all software components in the Edge Gateway take the changed time.
8.3.4 Configure ports for HTTP/HTTPS communication

Open this page with System > Port Settings.

In order to open this page, no access rights are required.

By default, the Edge Gateway Manager uses port 80 for its HTTP communication and port 443 for its HTTPS communication. In case of the ports being used otherwise, you can configure the Edge Gateway to use other ports. This situation applies, for instance, when using Docker (see Isolated application execution with Docker [page 63]), if Docker containers are designed to serve HTTP and HTTPS requests only at the above mentioned standard ports.

![Port settings](image)

Figure 22: Port settings

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Default port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
</tr>
</tbody>
</table>

Table 17: Default ports

**Setting port address for HTTP**

- Enter the port address for the communication of the Edge Gateway Manager over HTTP in input field **HTTP Port**.
- Store the port address as described subsequently. If a red error message box with the text *http port is not free* appears, the port is already used. In this case select another port.

**Setting port address for HTTPS**

- Enter the port address for the communication of the Edge Gateway Manager over HTTPS in input field **HTTPS Port**.
- Store the port address as described subsequently. If a red error message box with the text *https port is not free* appears, the port is already used. In this case select another port.
Save changes of port addresses

- Click at **Save changes** in order to permanently store the port address.

**Note:**
Take care of this change not to have an immediate effect, but being effective after the next restart of the Edge Gateway.

**Refresh**

Clicking at the button **Refresh**, the currently configured values for the port addresses in the input fields **HTTP Port** and **HTTPS Port** are displayed.

8.3.5  Rebooting the system

You have to login as Administrator to use this function.

In order to reboot the system:

- Within the Control Panel select menu entry **System > Reboot**
- The following safety query is displayed:

  ![Warning](image)

  **Warning**
  Do you really want to reboot
  [Yes] [No]

  **Figure 23: Reboot safety query**

- If you really intend to reboot the system, answer to the safety query with **Yes**.
- The Linux operating system of your Edge Gateway is shut down and then immediately restarted.

**Note:**
Take care of the consequences of shutting down and restarting for your network, if you reboot the Edge Gateway.
8.3.6 System shutdown

You have to login as Administrator to use this function.

In order to shut down the system:

- Within the Control Panel select menu entry **System > Shutdown**.
- The following safety query is displayed:

![Warning](image)

*Figure 24: Warning for consequences of shutdown*

- If you really intend to shut down the system, answer to the safety query with **Yes**.
- The Linux operating system of your Edge Gateway is shut down.

**Note:**
Take care of the consequences for your network, if you shut down the Edge Gateway.
8.4 Packet management

8.4.1 Managing packets

Open this page with Package Manager > Packages.

In order to be allowed to install packages, you need access rights "Read & Write" for the resource "packages". In order to view the installed packages, you only need access right "Read".

This page serves for managing additionally installed packages of the Linux-based operating system of the Edge Gateway. The standard packages of the operating system will not be listed on this page. The page

- lists the additionally installed packages including version,
- adds new and signed packages or
- updates already installed signed packages.

---

**Note:**

You can install packages signed by Hilscher only!

Use the package management only when Hilscher requests you to use the package management.
8.5 Network

8.5.1 Configuring Ethernet communication (LAN)

Open this page with Network > LAN.

For editing the parameters, you need the access right „Read & Write“ to the resource „LAN“. For displaying the parameters, you need the access right „Read“.

When delivered, the Ethernet interface cifx0 is deactivated. Section „Activating the Ethernet interface cifx0“ (see below) describes how to activate this interface.

You can configure the setting of the IP-address for each Ethernet interface.

- The Edge Gateway obtains the IP-address parameters automatically from a DHCP server: Option „Obtain an IP address automatically“. The Edge Gateway is a DHCP client.
- The user enters the IP-address parameters manually: Option „Use the following IP address“. In this setting the Edge Gateway can be used as a DHCP server (optionally).

The IP-address parameters include the IP-address, the subnet mask, the Gateway address, and the IP-addresses of Domain Name Server 1 and 2.

Figure 25: Default LAN-configuration
<table>
<thead>
<tr>
<th>Column</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>-</td>
<td>displays the name of the LAN interface, e.g. eth0.</td>
</tr>
<tr>
<td>MAC address</td>
<td>-</td>
<td>displays the MAC address of the LAN interface.</td>
</tr>
<tr>
<td>Settings</td>
<td>Obtain an IP address automatically</td>
<td>Setting required so that the Edge Gateway automatically obtains the IP-</td>
</tr>
<tr>
<td></td>
<td>Use the following IP address</td>
<td>address parameters from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>IP address,</td>
<td>Automatically: Display of the IP-address parameters received from the DHCP</td>
</tr>
<tr>
<td></td>
<td>Subnet mask,</td>
<td>server.</td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td>Manually: Input fields for the IP-address parameters to be entered by the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>user.</td>
</tr>
<tr>
<td></td>
<td>Receive DNS address from DHCP server</td>
<td>✅ DNS addresses (automatically) received from DHCP server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ DNS addresses manually entered by the user.</td>
</tr>
<tr>
<td></td>
<td>DNS server 1,</td>
<td>Automatically: Display of the DNS addresses received from the DHCP server.</td>
</tr>
<tr>
<td></td>
<td>DNS server 2</td>
<td>Manually: Input fields for the DNS addresses to be entered by the user.</td>
</tr>
<tr>
<td>DHCP server settings</td>
<td>Enable</td>
<td>✅ At this interface, the Edge Gateway provides a DHCP server. Prerequisite:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The option „Use the following IP address” is set. Note: In this subnetwork,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>no other DHCP server must be available.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>☐ At this interface, the DHCP server is deactivated.</td>
</tr>
<tr>
<td></td>
<td>Start IP address,</td>
<td>Parameters for the integrated DHCP server of the Edge Gateway.</td>
</tr>
<tr>
<td></td>
<td>End IP address,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subnet mask</td>
<td></td>
</tr>
</tbody>
</table>

Table 18: Table LAN: Description of the columns and elements

To save your changes permanently, click Save changes.
8.5.2 Configuring wireless communication (Wi-Fi)

Open this page with **Network > Wi-Fi**.

To access this page, you need rights for the resource:

*Access onto Wi-Fi (wireless network)*

On this page, you configure the wireless network communication of the Edge Gateway (Wi-Fi / WLAN according to IEEE 802.11).

The Wi-Fi is deactivated when delivered (factory setting).

---

**Wi-Fi modes of operation**

The Edge Gateway offers 2 Wi-Fi operating modes. These can be selected via the selection list **Mode**, see following table.

<table>
<thead>
<tr>
<th>Operating mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
<td>Wi-Fi is deactivated.</td>
</tr>
<tr>
<td>Access Point</td>
<td>In the operating mode <em>Access point</em> the Edge Gateway enables other Wi-Fi-capable devices to establish a connection with the Edge Gateway and its peripheral devices.</td>
</tr>
<tr>
<td>Client</td>
<td>In the operating mode <em>Client</em> the Edge Gateway acts as WLAN Ethernet adapter. This allows the integration of the Edge Gateway into an already existing WLAN (Wireless Area Network).</td>
</tr>
</tbody>
</table>

---

**Table 19: Wi-Fi modes of operation in selection list Mode**

<table>
<thead>
<tr>
<th>Description</th>
<th>Operating mode</th>
<th>Name</th>
<th>MAC address</th>
</tr>
</thead>
<tbody>
<tr>
<td>displays the active operating mode.</td>
<td></td>
<td>displays the name of the Wi-Fi interface (wlan0).</td>
<td>displays the MAC address, if Wi-Fi is activated.</td>
</tr>
</tbody>
</table>

---

**Table 20: Wi-Fi**
Changing the operating mode:

You can change the operating mode via the Mode list.

- Specify the parameters for the new operation mode.
- Click at Change mode.
- A safety query, whether you want to really change the operation mode, appears
- Confirm the message with OK.
- The message *Wi-Fi Settings are successfully changed* is displayed.

**Operating mode Access point**

![Figure 28: Wi-Fi operating mode: Access point](image)

**Table 1**

<table>
<thead>
<tr>
<th>Access point</th>
<th>Channel</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>hilscher-wg</td>
<td></td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>hilscher-wg-wlan</td>
<td></td>
</tr>
<tr>
<td>DHCP server</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Network Settings**

<table>
<thead>
<tr>
<th>Name</th>
<th>MAC address</th>
<th>Settings</th>
<th>Domain Name System</th>
</tr>
</thead>
<tbody>
<tr>
<td>wlan0</td>
<td>7C:SC:F8:BA:...</td>
<td>IP address: 192.168.250.10</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subnet mask: 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gateway:</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 28: Wi-Fi operating mode: Access point*
The following table describes the parameters of the operating mode Access point.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operation mode</td>
<td>Current mode of operation Access point.</td>
</tr>
<tr>
<td>Mode</td>
<td>Selection list for changing the mode of operation&lt;br&gt;Select the new operation mode from the selection list and then click at &lt;br&gt;<strong>Change mode.</strong></td>
</tr>
<tr>
<td>Name</td>
<td>displays the name of the Wi-Fi interface (<strong>wlan0</strong>).</td>
</tr>
<tr>
<td>MAC address</td>
<td>displays the MAC address, if Wi-Fi is activated.</td>
</tr>
<tr>
<td>IP address</td>
<td>Specify IP address of Edge Gateway.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Specify subnet mask of Edge Gateway.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Specify IP address of network gateway.</td>
</tr>
<tr>
<td>Channel</td>
<td>In the list <strong>Channel</strong> you can select the radio channel and, thus, determine the WLAN radio frequency in the 2.4 GHz band.</td>
</tr>
<tr>
<td>Country</td>
<td>In the list <strong>Country</strong> you can select the country in which you operate the radio network.</td>
</tr>
<tr>
<td>SSID</td>
<td>Specify Service Set Identifier of wireless network&lt;br&gt;Here you enter the SSID to be used in the wireless network (WLAN) of the Edge Gateway. &lt;br&gt;<strong>Note:</strong> Do not use the default SSID.&lt;br&gt;In order to use a WLAN connection, you have to specify the SSID at the Wi-Fi clients.</td>
</tr>
<tr>
<td>Wi-Fi protected access</td>
<td>displays the encryption method used in the wireless network.</td>
</tr>
<tr>
<td>Pre-shared key</td>
<td>Here you enter the key to be used in the wireless network (WLAN) of the Edge Gateway. In order to use a WLAN connection, you have to enter this key on any Wi-Fi client.&lt;br&gt;<strong>Note:</strong> Do not use the predefined default key.</td>
</tr>
<tr>
<td>DHCP Server</td>
<td>to activate/deactivate the DHCP server&lt;br&gt;Check this box whenever the Edge Gateway is to provide a DHCP server.</td>
</tr>
<tr>
<td>Start IP address</td>
<td>Here you have to enter the start IP address of the IP address range for the DHCP server if you have checked the box DHCP server.</td>
</tr>
<tr>
<td>End IP address</td>
<td>Here you have to enter the end IP address of the IP address range for the DHCP server if you have checked the box DHCP server.</td>
</tr>
</tbody>
</table>

*Table 21: Parameters of the operating mode Access point*
Operating mode: Client

Figure 29: Wi-Fi operating mode: Client
The following table describes the parameters of the operating mode **Client**.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mode</td>
<td>Current mode of operation: <strong>Client</strong>.</td>
</tr>
<tr>
<td>Mode</td>
<td>Selection list for changing the operation mode Select the new operation mode from the selection list and then click at <strong>Change mode</strong>.</td>
</tr>
<tr>
<td>Name</td>
<td>Displays the name of the Wi-Fi interface (<strong>wlan0</strong>).</td>
</tr>
<tr>
<td>MAC address</td>
<td>Displays the MAC address, if Wi-Fi is activated.</td>
</tr>
<tr>
<td>Obtain an IP address automatically</td>
<td>✓ The Edge Gateway obtains the IP address parameters from a DHCP server automatically. The Edge Gateway is a DHCP client. The user has to enter the IP address parameters manually.</td>
</tr>
<tr>
<td>IP address</td>
<td>Automatically: Display of the automatically received IP address. Manually: Enter the IP address.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Automatically: Display of the automatically received subnet mask. Manually: Enter the subnet mask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Automatically: Display of the automatically received gateway address. Manually: Enter the gateway address.</td>
</tr>
<tr>
<td>Receive DNS address through DHCP server</td>
<td>✓ To obtain the DNS server address 1 and 2 from a DHCP server automatically. Enter the DNS server address 1 and 2.</td>
</tr>
<tr>
<td>DNS server 1 and 2</td>
<td>Automatically: Display of the automatically received DNS server address 1 and 2. Manually: Enter the DNS server address 1 and 2.</td>
</tr>
<tr>
<td>Channel</td>
<td>Display of the used wireless channel.</td>
</tr>
<tr>
<td>SSID</td>
<td>Shows the SSID (Service Set Identifier) of the Access Point the Edge Gateway is connected to.</td>
</tr>
</tbody>
</table>

**Table 22: Parameters of the operating mode Client**

**Table Client**

For each found client, the following data is shown in a separate column of the table:

- SSID (Service Set Identifier)
- MAC Address
- Quality (of radio signal)
- Wi-Fi protected access

**Scanning for a WLAN client**

- Click **Scan**.
- If a WLAN client is found, its data will be displayed in a line of the table **Client**.
Establishing a connection to a WLAN client found
- Click a line in the table which shows data of a client found.
- Click at Connect.
  - A dialog to enter the password is displayed.
  - Enter the password and click Connect.
  - The Edge Gateway tries to establish a WLAN connection with the found client. If this does not succeed, an error message is displayed.

Delete stored connection
- In the table of the connections, click Delete in the row to be deleted.
  - The stored connection is deleted and the message Wi-Fi successfully disconnected is displayed.

Saving the Wi-Fi settings
To save the Wi-Fi settings, you need the access right ‘Write’ for the Wi-Fi page.
- Click Save changes.
  - A security request box appears:
  - Click at OK.
  - The Wi-Fi settings are saved.

8.5.3 Configuring cellular communication
Open this page with Network > Cellular.

In order to be allowed to edit these parameters, you need access rights “Read & Write” for the resource “Cellular”. In order to view these parameters, you only need access right “Read”.

On this page, you can configure the cellular interface of the Edge Gateway for transmitting data into the cloud via 2G/3G/4G standard.

In order that you can use the cellular interface, it has to be installed in the gateway. This page is empty if no cellular interface is installed and a Cellular interface not installed message will be displayed on opening this page.
8.5.4 Configuring IP Routes

Open this page with **Network > Routes**.

In order to be allowed to edit these parameters, you need access rights "Read & Write" for the resource "Routes". In order to view these parameters, you only need access right "Read".

On this page, you can configure the IP routing of the Edge Gateway; i.e. here you can specify which interfaces or connections are to be used to address certain IP destination addresses outside the Edge Gateway (e.g. on the Internet).

![Routes configuration](image)

**Figure 30: Routes**
### Current connection configuration

The **Current connection configuration** table shows the current IP settings of the network connections of the Edge Gateway:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection</strong></td>
<td>Physical or virtual interface</td>
</tr>
<tr>
<td>cifx0</td>
<td>Ethernet-LAN connection of the Real-Time Ethernet interface (Fieldbus). You can configure the IP address of cifx0 under <strong>Network &gt; LAN</strong> (you must first enable the cifx0 interface under <strong>Network &gt; Field</strong>).</td>
</tr>
<tr>
<td>eth0</td>
<td>LAN connection of the eth0 Ethernet interface (port 1). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>eth1</td>
<td>LAN connection of the eth1 Ethernet interface (port 2). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>cellular</td>
<td>Cellular communication interface (Modem). The IP address is assigned to the modem on establishment of the connection by the provider. <strong>Note</strong>: The Cellular modem is available only in the NIOT-E-TUCX-GB-RE\4EU variant.</td>
</tr>
<tr>
<td>wifi_client</td>
<td>Wi-Fi interface. You can configure the operating mode (&quot;Access Point&quot; or &quot;Client&quot;) and the IP address for the Wi-Fi interface under <strong>Network &gt; Wi-Fi</strong>. <strong>Note</strong>: The Wi-Fi interface is available only in the NIOT-E-TIJCX-GB-RE\WF variant.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>IP address of the connection in CIDR notation <strong>Note</strong>: In case no IP address is displayed although the interface has been activated:</td>
</tr>
<tr>
<td></td>
<td>• In case, the Ethernet interface has no link (then the operating system does not assign an IP address to this interface).</td>
</tr>
<tr>
<td></td>
<td>• In case, the Ethernet interface has a link but the Ethernet interface has not received an IP address from a DHCP server (then the operating system deactivates this interface).</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Indicates whether a DHCP service has been set for the connection.</td>
</tr>
</tbody>
</table>

*Table 23: Parameters of Current connection configuration table*
Static routes configuration

The Static routes configuration area displays already created routes, and you can also create new routes here.

- In the drop-down list, select a connection/interface, e.g. eth1, to display the IP destination addresses that are to be handled via this connection:

![Defined Routes](image)

**Figure 31: Defined Routes**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>IP destination address in CIDR notation</td>
</tr>
<tr>
<td>Gateway</td>
<td>Gateway serving as first “hop” of the connection/route. If empty, the standard gateway will be used as default.</td>
</tr>
<tr>
<td>Metric</td>
<td>If several routes have been defined for an IP destination address – e.g. a wired route via Ethernet (eth1) and an alternative wireless route via cellular connection (cellular) – the priority of the route can be defined here. The Edge Gateway always first uses the route with the lower value in the Metric field to reach the IP destination address. If this route is blocked (e.g. by pulled cable), the Edge Gateway will use the route with the next higher number defined in the Metric field (e.g. via cellular connection), etc.</td>
</tr>
</tbody>
</table>

Delete | Use the **Delete** button to delete the route.

**Table 24: Routes parameters**

- To define a new route, first select in the drop-down list the connection/interface that shall be used to contact the IP destination address.
- Click **Add** button.
- The table creates a new route with the default destination address 0.0.0.0/0:

![Create new route](image)

**Figure 32: Create new route**

- In the Destination field, overtype the 0.0.0.0/0 default value with your actual destination IP address. Use the CIDR notation.
Figure 33: Define new route

- In the **Gateway** field, enter the IP address of the gateway that shall be used as "first hop". The gateway should be located in the same network as the connection/interface of the Edge Gateway. If the field is left empty, the standard gateway will be used as default.

- If necessary (i.e. if more than one route has been defined for this IP destination address), define the priority of the route in the **Metric** field. The lower the number, the higher the priority.

- Click **Save** button.
8.5.5 Configuring Firewall

Open this page with **Network > Firewall**.

In order to be allowed to edit these parameters, you need access rights "Read & Write" for the resource "Firewall". In order to view these parameters, you only need access right "Read".

On this page, you can set individual firewall parameters for each connection/interface of the Edge Gateway separately.

![Firewall Configuration](image-url)

*Figure 34: Firewall*
## Parameters firewall

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection</strong></td>
<td>Physical or virtual interface</td>
</tr>
<tr>
<td>cifx0</td>
<td>Ethernet-LAN connection of the Real-Time Ethernet interface (fieldbus). You can configure the IP address of cifx0 under <strong>Network &gt; LAN</strong> (you must first enable the cifx0 interface under <strong>Network &gt; Field</strong>).</td>
</tr>
<tr>
<td>eth0</td>
<td>LAN connection of the eth0 Ethernet interface (port 1). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>eth1</td>
<td>LAN connection of the eth1 Ethernet interface (port 2). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>cellular</td>
<td>Cellular communication interface (modem). The IP address is assigned to the modem on establishment of the connection by the provider. <strong>Note:</strong> The cellular modem is available only in the NIOT-E-TIJCX-GB-RE4EU variant.</td>
</tr>
<tr>
<td>wifi_client</td>
<td>Wi-Fi interface. You can configure the operating mode (&quot;Access Point&quot; or &quot;Client&quot;) and the IP address for the Wi-Fi interface under <strong>Network &gt; Wi-Fi</strong>. <strong>Note:</strong> The Wi-Fi interface is available only in the NIOT-E-TIJCX-GB-REWIF variant.</td>
</tr>
<tr>
<td><strong>Current firewall zone</strong></td>
<td>Current firewall settings for the connection/interface.</td>
</tr>
<tr>
<td><strong>New firewall zone</strong></td>
<td>Here you can change the firewall setting for the connection/interface by clicking the arrow icon and selecting a new configuration setting from the drop-down list.</td>
</tr>
<tr>
<td>block</td>
<td>All packets reaching the interface will be dropped. The sender will be notified by an ICMP &quot;unreachable&quot; message.</td>
</tr>
<tr>
<td>drop</td>
<td>All packets reaching the interface will be “silently” dropped.</td>
</tr>
<tr>
<td>nat_drop</td>
<td>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.</td>
</tr>
<tr>
<td>nat_trusted</td>
<td>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.</td>
</tr>
<tr>
<td>trusted</td>
<td>Default. All IP packets will be forwarded transparently (firewall is switched off).</td>
</tr>
</tbody>
</table>

![Important:](image)

**Important:**

Note that you can no longer connect to the Edge Gateway Manager via a blocked interface. If you inadvertently block all active interfaces, the gateway is no longer accessible and must be reset to the factory settings via "Firmware Recovery" (see section Firmware recovery).
8.5.6 Hostname

Open this page with **Network > Hostname**.

To access this page, you need rights for the resource:

*Access onto hostname of Edge Gateway*

On this page you configure the host name.

The host name identifies the device via the Wi-Fi or LAN network.

The default host name starts with the two letters "NT" followed by the LAN MAC address of the LAN connection port 1 of the Edge Gateway. Example `NT0002A233E559`. The default host name is printed on the label at the bottom of the Edge Gateway. With the host name you can access the Edge Gateway from your PC even without knowing the IP address of the Edge Gateway (also see *Using the web browser to establish a connection with the Edge Gateway* [page 15]).

If the Edge Gateway does not obtain an IP address from a DHCP server, the system cannot translate the host name and you cannot access the device.

**Hostname**

![Hostname Input Field](image)

*Figure 35: Hostname*

**Input field Hostname**

A string of ASCII characters of arbitrary length can be entered into the input field **Hostname**.

**Saving the host name**

The hostname is saved by clicking at **Save changes**.

If storing the hostname has succeeded, the following message box is displayed:

![Hostname settings are successfully saved](image)
8.6 Services

8.6.1 Starting, stopping and configuring services

Open this page with Services > Service List.

For changing the settings of a service, you need the access right „Read & Write“ to this service. For displaying the settings you need the access right „Read“ to the service.

On this page you can

- display the list of the running services,
- display the operating status of each service,
- stop and start single services,
- activate/deactivate autostart.

The list of services is displayed at the left edge:

![Service 1](image1)
![Service 2](image2)

Figure 36: List of default services

For a quick overview, the operating status of each service is displayed in color.

<table>
<thead>
<tr>
<th>Color</th>
<th>Operating status</th>
</tr>
</thead>
<tbody>
<tr>
<td>green</td>
<td>The service is being executed.</td>
</tr>
<tr>
<td>yellow</td>
<td>The service is configured, but not executed.</td>
</tr>
<tr>
<td>red</td>
<td>The service is neither configured nor executed.</td>
</tr>
<tr>
<td>grey</td>
<td>No access right to this service</td>
</tr>
</tbody>
</table>

Table 26: Operating statuses of the services

The following table lists operating and display elements which are available for each service.

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating status</td>
<td>Displays the operating status of the service: “Stopped” or “Running”. Button to Start or Stop the service.</td>
</tr>
<tr>
<td>Autostart</td>
<td>Displays whether the service is automatically startet (enabled) or not started (disabled) when the Edge Gateway starts. “Apply” button to change the autostart setting.</td>
</tr>
</tbody>
</table>
| License status | Displays information about the license, if the execution of the service requires a license:  
- Required license available in the Edge Gateway: available / not available,  
- name of the license,  
- expiration date, if the license has a run-time limit. |

Table 27: Operating and display elements

A service can allow you individual settings.
8.7 User management

The administrator manages users by means of two configuration pages:

- User roles (determining new roles and assigning access rights) and
- User accounts (adding, processing, and deleting).

Defining a user account is accomplished by assigning a predefined role to the user.

8.7.1 Managing user roles

Open this page with User Management > Roles.

On this page, you can determine roles and assign access rights onto resources to these roles.

The roles Administrator and View are standard and cannot be deleted.

![Roles](image.png)

*Figure 37: Page for configuring roles*

An access right is set per resource. Each configuration page of the control panel which contains settable device parameters is a resource. Access via REST-API (see Functions of the Edge Server) is also a resource.
An access right can be assigned to the following single resources:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Access to resource via menu</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System &gt; Time</td>
<td>Setting the system time [(\rightarrow) page 32]</td>
</tr>
<tr>
<td>System log</td>
<td>System &gt; Syslog</td>
<td>Displaying the system log files [(\rightarrow) page 28]</td>
</tr>
<tr>
<td>Packet management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Managing packets</td>
<td>Package Manager &gt; Packages</td>
<td>Managing packets [(\rightarrow) page 38]</td>
</tr>
<tr>
<td>Network access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to LAN (Ethernet network)</td>
<td>Network &gt; LAN</td>
<td>Configuring Ethernet communication (LAN) [(\rightarrow) page 39]</td>
</tr>
<tr>
<td>Access onto Wi-Fi (wireless network)</td>
<td>Network &gt; Wi-Fi</td>
<td>Configuring wireless communication (Wi-Fi) [(\rightarrow) page 41]</td>
</tr>
<tr>
<td>Access onto hostname of Edge Gateway</td>
<td>Network &gt; Hostname</td>
<td>Hostname [(\rightarrow) page 53]</td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure service &quot;XYZ&quot; (depends on installed services)</td>
<td>Services &gt; Service List &gt; Service &quot;XYZ&quot;</td>
<td>Starting, stopping and configuring services [(\rightarrow) page 54]</td>
</tr>
<tr>
<td>Configure Docker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Note: The user rights in the role management relate only to the right to configure the Docker service in the Service List. The users of the Docker / container management will be registered in the portainer.io directly.</td>
<td></td>
<td>Isolated application execution with Docker [(\rightarrow) page 63]</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Public Key Infrastructure (PKI)</td>
<td>Security &gt; Public Key Infrastructure</td>
<td>Public Key Infrastructure [(\rightarrow) page 58]</td>
</tr>
</tbody>
</table>

Each resource may obtain one of the following access rights:

<table>
<thead>
<tr>
<th>Access rights onto resource</th>
<th>Checkbox</th>
</tr>
</thead>
<tbody>
<tr>
<td>No access</td>
<td>None</td>
</tr>
<tr>
<td>Read access only</td>
<td>Read</td>
</tr>
<tr>
<td>Read and write access</td>
<td>Read, Write</td>
</tr>
</tbody>
</table>

Table 29: Access rights to resources

Adding a new role

- **Click at Create new role.**
- The dialog box for entering the role name is displayed.

![Add new role dialog box](image)

- Enter a name for the role, e.g. **User**.
- **Click Add.**
- The role is added.
Setting the access rights of a role

- Click a role.
- The resources and access rights for this role will be displayed.
- Assign the access right per resource.
- Click Save changes.

8.7.2 Managing user accounts

Open this page with User Management > Accounts.

On this page you can

- add
- process
- delete user accounts.

Each user account has a user name, a password, and an assigned role.
8.8 Security

8.8.1 Public Key Infrastructure

For the protection of its communication using encryption, the Edge Gateway uses security certificates and keys based on modern asymmetric encryption techniques. The Edge Gateway can be integrated into a public key infrastructure. The menu Security > Public Key Infrastructure offers you the possibility to manage security certificates for several use cases, display the contents of certificates.

To display information related to certificates and the associated keys, you require access rights for reading on Public Key Infrastructure.

To add certificates and keys, you require access rights for writing on Public Key Infrastructure.

Figure 39: Public Key Infrastructure for managing of certificates

The GUI of the public key infrastructure consists of these areas:

1. Selection list for the certificate type (1): Trusted Certification Authorities or Service certificates
2. File selection area for certificate and key files (2)
3. Certificate Viewer (3)
Certificate type selection list

In the **Certificate Type** selection list (1), you can select whether you want to manage

- certificates in the Trusted Certification Authorities or
- service certificates (server or client certificates for services in the Edge Gateway) for the communication using the HTTPS or OPC UA protocols.

File selection window for certificates and key files

In this area (2), you can select a PEM file containing information about a certificate or a key. In case of selection of a certificate, important information about the selected certificate is displayed in the area Certificate Viewer (right side).

Depending on the selected certificate type (1), the file selection area for certificate and key files either displays a list structure or a tree structure:

On selection of **Root Certificates** the list structure of the Trusted CA Store in the Edge Gateway is displayed.
On selection of **Service Certificates** a tree structure is displayed.

![Certificate Viewer](image)

**Certificate Viewer**

The area Certificate Viewer (3) is used to display the structure of a certificate selected within the file selection area on the left side. The elements of the selected certificate according to the X.509 standard, such as information on the issuer, serial number, country, locality, organisation and organisation unit are displayed, see section *Structure of a certificate according to X.509* [† page 94].

**Note:**

For more information on the foundations of asymmetric encryption techniques and public key infrastructure, see sections *Asymmetric encryption* [† page 92] and *Certificates and keys* [† page 94].
8.9 Help

Open this page with Help > Info. No access rights are required in order to open this page.

This page displays the firmware version of the Edge Gateway.

![Info page](image)

**Figure 42: Info page**

8.10 Session

8.10.1 User profile

Open this page with Session > User Profile. No access rights are required in order to open this page.

![User profile page](image)

**Figure 43: User profile page**

On this page you can

- display the access rights of your user account,
- change your E-mail address, and
- change your password.
Changing the e-mail address
- Click at Edit user account.
- The dialog Edit user account is displayed.

![Figure 44: Dialog "Edit user account"](image)

- Specify your e-mail address at the input field E-mail.
- Click at Save changes.
- The specified e-mail address is stored.

Changing the password
- Click on Edit user account.
- The dialog Edit user account is displayed.
- Check change user password.
- Specify your password at the input field New Password.
- In order to confirm your input, specify your password again at the input field Confirm Password.
- Click on Save changes.
- The changed password is saved.

8.10.2 Logout

To log out from the Edge Gateway, use Session> Logout. No access rights are required to select this menu entry. Prior to accessing the Edge Gateway again, a new login (Specifying user name and password) is necessary.
Isolated application execution with Docker

The Edge Gateway enables the user to execute his own applications within the protected Linux operating system. A software platform becomes necessary to allow the execution of these applications without simultaneously opening the possibility of evading the safety mechanisms of the Linux operating system. For that purpose, the Edge Gateway uses the open-source software "Docker" from Docker Inc. (https://www.docker.com). Docker enables the isolated execution of applications by the creation of isolated execution environments (so called containers) for applications.

Note:
For more information on Docker, see the documentation of the Docker organization under https://docs.docker.com/.

9.1 Docker, Image, Container and Repository

In the following, the most important terms concerning Docker are explained:

Docker

Docker offers a platform for isolated execution of applications in protected environments and additionally a standard for software distribution. This platform allows Edge Gateway users to execute own application on the protected Linux operating system of the Edge Gateway without in any way being able to circumvent or deteriorate its security mechanisms.

To implement containers isolated from one another, Docker applies techniques originally developed for operating system virtualization. On the Edge Gateway, Docker runs as a service (the Docker daemon dockerd).

As common in Linux environments, Docker is usually controlled by commands from a command line interface.

However, due to the above mentioned security purposes, no command line service has been installed on the Edge Gateway. So, on the Edge Gateway Docker is not able to be controlled via a command line-oriented interface (CLI) as described within the official Docker documentation (https://docs.docker.com/). Instead of that, the easy-to-use GUI portainer.io has been installed on the Edge Gateway. Instead of the absent CLI, this GUI provides all necessary functions to administer the Docker services.

Note:
Further information concerning portainer.io can be found at http://portainer.io.
Image

An image is the basis for a container and includes only its program code and basic settings.

It does not include information the program code generates on a storage medium or RAM while it is running.

Moreover, it does not include any information on the environment the image is to be executed in, i.e. it is platform-neutral.

An image always relates to the defined processor architecture it is compiled for, e.g. x86, x64 or ARM. If a container is generated from an image, make sure that the image is suitable for the hardware platform used.

Note:
For more information on images, see the Docker documentation [https://docs.docker.com/engine/] and, in particular, its glossary [https://docs.docker.com/glossary/?term=image].

Container

A container is a runtime instance of an image.

A container represents an image being executed within an individual runtime environment of its own, comparable to a running process. Running an image in a container is commonly denominated as "starting" the container. The term "starting" implies that Docker transfers the image to an individual runtime environment to execute it there. This runtime environment is isolated both against the host machine and against the other containers present on this host machine. Access to resources of the host system as e.g. host files and ports only occurs, if explicitly configured.

A container consists of:
- a Docker image,
- a runtime environment, and
- a standard command architecture.

The runtime environment contains e.g. current information on configuration and status. For storing this information, Docker generates a virtual drive in the container, a so-called "volume"

Docker can start several containers, even containers originating from the same image.

Note:
For more information on containers, see the Docker documentation [https://docs.docker.com/get-started/#prerequisites] and, in particular, its glossary [https://docs.docker.com/glossary/?term=container].
Repository

For distributing images via the Internet, the Docker organization provides a special storage area, the so-called repository under https://hub.docker.com/. There, images can freely accessible be stored. Alternatively, you can administer own repositories there.

9.2 Prerequisites for working with Docker

In order to use the Docker functionality, both of the following conditions have to be fulfilled:

1. Read and write access rights at Docker UI are required. To examine whether you have these, you can use menu entry User profile [page 61]. Granting read and right access rights requires administrator rights and is described in section Managing user roles [page 55].

2. The Docker service must have been started on the Edge Gateway. In order to examine whether the service has been started or to start it, open the service list within the Control Panel as described in Starting, stopping and configuring services [page 54].
9.3 Container for netPI: Examples

The device contains a Docker host and allows you to load and execute own edge automation applications in safe containers. The Docker host within netPI does not allow you to create images on the device. As the security concept of netPI prohibits SSH services, you cannot use the "Docker build commands". However, you can develop images on a compatible hardware like the Raspberry Pi 3 instead on the netPI. The purchase of an inexpensive consumer Raspberry Pi 3 for little money is an investment free of any risk in order to get used with Docker or also to perform usability and performance tests prior to using the application on the professional netPI.

Docker Hub is the Internet platform for common usage of container images together with colleagues, customers and the Docker community. For netPI, there is a registration offering you ready-to-use examples like the wiring editor Node-RED or an HDMI desktop environment and much more. Use these images as a template for your own ideas as soon as you create your own images.

Address: https://hub.docker.com/r/hilschernetpi/

<table>
<thead>
<tr>
<th>Name</th>
<th>Container contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>netpi-desktop-hdmi</td>
<td>HDMI desktop environment. Activates the HDMI interface for connecting with a monitor and offers a desktop environment.</td>
</tr>
<tr>
<td>netpi-raspbian</td>
<td>Raspbian operating system. Raspbian (jessy)</td>
</tr>
<tr>
<td>netpi-nodered-fieldbus</td>
<td>Node-RED and fieldbus nodes. Processes I/O data of the real-time Ethernet with the wiring editor Node-RED. For instance, netPI can be used as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter.</td>
</tr>
<tr>
<td>netpi-netx-programming-examples</td>
<td>Programming example. Processes I/O data of the real-time Ethernet with access via the API. For instance, netPI can be used as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter.</td>
</tr>
<tr>
<td>netpi-nodered-fram</td>
<td>FRAM and Node-RED. Use of FRAM together with the wiring editor Node-RED.</td>
</tr>
<tr>
<td>netpi-container-build-environment</td>
<td>Container environment. Environment for the development of containers for netPI.</td>
</tr>
</tbody>
</table>

Table 30: Container for netPI: Examples

The following figure shows the possible use of containers.

Figure 45: netPI block diagram
9.4 Working with Docker via the web GUI

This section describes

- how to operate Docker via the portainer.io interface of the browser
- how to run additional software on the Edge Gateway with Docker (using the web server NGINX as an example).

9.4.1 The portainer.io interface

The portainer.io interface serves:

- to add new containers
- to configure the containers
- to provide functions for controlling the application execution such as Start, Stop, Kill, Restart, Pause, Resume, and Remove

9.4.2 Commissioning

In this section, you can learn how to start up the Docker service within the Control Panel and configure it in such a manner, that it will start automatically in future.

- Open the service list within the Control Panel as described in Starting, stopping and configuring services page 54.
- In the service list (to the left), select the entry Docker.
- At the Autostart option, click at the radio button enabled in order to set up automatic starting of the Docker service.
- Click at Apply.
- A security confirmation prompt appears and asks you whether you really request to change the state of Docker.
- Answer it with Yes.
- The button Apply is now displayed in red color.
- If the current status equals Stopped: Click at Start.
- The security confirmation prompt appears again.
- Again, answer with Yes.
- The status changes from Stopped to Running and the yellow icon at the Docker service within the services list changes to green, see figure.
Thus, the Docker service is started and the formerly deactivated grey tile for Docker within the Edge Gateway Manager (Docker Management) is activated enabling you to invoke the GUI portainer.io.

Note:
We urgently recommend you to set up an initial admin user account now. Otherwise, a user admin supplied with administrator rights will be established without any password, when the docker service is started. A potential offender could use this user account as an open entrance door. In order to avoid this, immediately continue to perform the initial set-up of portainer.io (Starting the portainer.io interface for working with the containers [→ page 69]) as subsequently described.
9.4.3 Starting the portainer.io interface for working with the containers

As the Edge Gateway, as explained above, does not provide any command line interface (CLI), the web-based GUI portainer.io represents the only possibility of access to Docker for working with containers.

To start the portainer.io interface, proceed as follows:

- Open the Edge Gateway Manager.
  - In this context, see Calling the Edge Gateway Manager [page 17].
- Click the tile Docker Management in the Edge Gateway Manager.

The portainer.io login screen will be displayed asking you to enter the username and password of an initial user with administrator rights.

portainer.io includes its own user administration working independently from the one implemented within Control Panel. Therefore, follow these steps precisely:

You are urged to specify the user name and twice the password for the first user with administrator rights.
In the field **Username** an arbitrary username can be specified. By default, *admin* is specified there as this is the only pre-defined username. We recommend you to use it and not to change it.

- At **Password**, specify the password for the username *admin* and repeat this at **Confirm Password**. Both specifications will be checked for equality.

---

**Note:**
This password is not identical to that of the user administration of the Edge Gateway Manager, see .

---

- Click at **Create user**.

Now, the following happens:

1. If the identical password has been specified twice and it conforms to the password rules, a new user named "admin" is created within the user administration of portainer.io .

---

**Note:**
Never skip configuring an initial administrator user, because otherwise a user admin with administrator rights and without any password will be generated.

2. Additionally, the start page „Home (Endpoints)“ of portainer.io is displayed.

---

![Figure 49: portainer.io - initial screen Home (Endpoints)](image)

- Click at entry "Dashboard" in the blue menu on the leftside .
- The page „Dashboard“ of portainer.io is displayed.
Isolated application execution with Docker

Figure 50: View of portainer.io dashboard

Note:
Inform yourself about the possibilities of managing containers and images within the current documentation of portainer.io (https://portainer.readthedocs.io/en/stable/).

➤ Click Containers in the menu on the left or Containers on the page "Dashboard".

➤ The page "Container list" will be displayed. This page contains a list with the name and status of all currently running or stopped containers and provides the functions for controlling application execution within containers.

Figure 51: Container list (portainer.io)
9.4.4 Functions for working with containers

Docker provides the following functions for application execution control within containers:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Start]</td>
<td>Start</td>
<td>Starting a container</td>
</tr>
<tr>
<td>![Stop]</td>
<td>Stop</td>
<td>Stopping a container</td>
</tr>
<tr>
<td>![Kill]</td>
<td>Kill</td>
<td>Aborting the execution of a container</td>
</tr>
<tr>
<td>![Restart]</td>
<td>Restart</td>
<td>Repeated starting of a container</td>
</tr>
<tr>
<td>![Pause]</td>
<td>Pause</td>
<td>Interrupting the execution of a container temporarily</td>
</tr>
<tr>
<td>![Resume]</td>
<td>Resume</td>
<td>Continuing the execution of a container after an interruption</td>
</tr>
<tr>
<td>![Remove]</td>
<td>Remove</td>
<td>Removing, i.e. deleting a container</td>
</tr>
</tbody>
</table>

Table 31: Functions for working with containers
9.4.5 User management

This section describes the integrated user management of portainer.io.

**Note:**
The integrated user management of portainer.io may not be confused with the user management of the control panel.

9.4.5.1 Open screen Users

The user administration of the portainer.io interface is done via the screen *Users*.

To open the screen *Users*, proceed as follows:

- If the portainer.io interface has not yet been opened, click at tile *Docker Management* within the Edge Gateway Manager.
- The portainer.io interface is opened.

Within the darkblue menu on the left side click at Users in the SETTINGS area.

The page for the user management within portainer.io is displayed (Users>User Management).
Figure 53: portainer.io - Page Users > User management

The figure shows an example configuration with a user admin being defined with assigned administrator rights and with another user named default_user being defined without any administrator rights.
### 9.4.5.2 Display of User Details

In order to display (or change) detailed information concerning a specific user from the list, proceed as follows:

- Within Users, click at the desired entry within the table of users
- The user details of the desired user are displayed.

![Portainer User Details](image)

*Figure 54: portainer.io - Display of User Details*

The screen "User details" allows you to perform the following actions within the user administration of portainer.io:

- Remove user (click at **Remove**)
- Grant administrator rights
  (Set slider right of Administrator to position „right“)
- Revoke administrator rights
  (Set slider right of Administrator to position „right“)
- Change password (Specify password twice in the input fields at **New password** und bei **Confirm password**)

9.4.6 Registry management

There are two ways to create a registry:
- Via Quay.io (pre-configured)
- As Custom Registry

9.4.6.1 Creating a registry with Quay.io

In order to create a registry with Quay.io, proceed as follows.

- Open the Edge Gateway Manager, if it is not already open. Also see Calling the Edge Gateway Manager [page 17].
- If the portainer.io interface has not yet been opened, click at tile **Docker Management** within the Edge Gateway Manager.

![Tile Docker within the Edge Gateway Manager](image)

*Figure 55: Tile Docker within the Edge Gateway Manager*

- The portainer.io interface is opened.

![portainer.io - entry page Home](image)

*Figure 56: portainer.io - entry page Home*

- Within the darkblue menu on the left side, click at **Registries** within the SETTINGS area.
- The page Registries (Registry management) for the registry management in portainer.io is displayed.
Isolated application execution with Docker

Figure 57: portainer.io - Page Registries (Registry management)

This page consists of at least two areas:

- DockerHub
- Registries

The DockerHub registry can generally be used by any arbitrary user. In DockerHub area, the slide switch **Authentication** determines, whether username and password have to be specified (Slider set to the right position), or not (Slider set to the left position). If the slide switch is set to the right position, the page changes as follows:

Figure 58: portainer.io - Page Registries (Registry-Management), Authentication has been activated

Here you can enter the username within field **Username** and the password within field **Password**.
Within this area, you can find the buttons **Add Registry** and **Remove** for adding and removing registries (see *Creating a registry with Quay.io* [page 76], *Setting up a custom registry* [page 79] and *Deleting a registry* [page 83]) and a table of all current registries. This table consists of the following three columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of registry</td>
</tr>
<tr>
<td>URL</td>
<td>URL of registry</td>
</tr>
<tr>
<td>Action</td>
<td>Contains a <strong>button Manage access</strong> for accessing the registry</td>
</tr>
</tbody>
</table>

**Table 32:** Meaning of columns of table of all current registries

- Click at the blue button **Add Registry**.
- The page Create registry (Registries > Add registry) appears.

- If the large field Quay.io at the left side has not already be marked click there.
- Click at the blue button **Add Registry**.
- If the registry has successfully been established, a success message is displayed.
- Furthermore the page Registries (Registry-Management) is displayed again. In the table within the lower area at Registries you can find an additional entry containing the information specified by you.
- In case of a URL conflict the message **Failure – A registry with the same URL already exists** is displayed. In that case choose another URL.
9.4.6.2 Setting up a custom registry

To establish a custom registry, proceed as follows:

- Open the Edge Gateway Manager, if it is not already open.
  See Calling the Edge Gateway Manager [page 17].
- If the portainer.io interface has not yet been opened, click at tile Docker Management within the Edge Gateway Manager.

![Docker Management](image)

*Figure 60: Tile Docker within the Edge Gateway Manager*

- The portainer.io interface is opened.

![Portainer.io - entry page Home](image)

*Figure 61: portainer.io - entry page Home*

- Within the darkblue menu on the left side, click at Registries within the SETTINGS area.
- The page Registries (Registry management) for the registry management in portainer.io is displayed.
Isolated application execution with Docker

Figure 62: portainer.io - Page Registries (Registry management)

This page consists of at least two areas:

- DockerHub
- Registries

The DockerHub registry can generally be used by any arbitrary user. In DockerHub area, the slide switch **Authentication** determines, whether username and password have to be specified (Slider set to the right position), or not (Slider set to the left position). If the slide switch is set to the right position, the page changes as follows:

Figure 63: portainer.io - Page Registries (Registry-Management), Authentication has been activated

Here you can enter the username within field **Username** and the password within field **Password**.
Within this area, you can find the buttons Add Registry and Remove for adding and removing registries (see Creating a registry with Quay.io [page 76], Setting up a custom registry [page 79] and Deleting a registry [page 83]) and a table of all current registries. This table consists of the following three columns:

<table>
<thead>
<tr>
<th>Column</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of registry</td>
</tr>
<tr>
<td>URL</td>
<td>URL of registry</td>
</tr>
<tr>
<td>Action</td>
<td>Contains a button Manage access for accessing the registry</td>
</tr>
</tbody>
</table>

Table 33: Meaning of columns of table of all current registries

1. Click at the blue button Add Registry.
2. The page Create registry (Registries > Add registry) appears.

1. Click at the large blue button Custom registry at the right side.

Figure 64: Portainer.io - Page Create registry (Registries > Add registry)

Figure 65: Portainer.io - Page Create registry (Registries > Add registry), Custom registry selected
Specify the name to be displayed at the node within field Name.

Specify the URL to be displayed at the node within field Registry URL of the Custom Registry.

If the Custom Registry is password-protected, set the slide switch right of Authentication to the right. Then to additional fields Username and Password are opened, into which you can enter the username and the (hidden) password for accessing the Custom Registry.

Click at the blue button Add Registry.

If the registry has successfully been established, the success message „Registry successfully created“ is displayed.

Furthermore the page Registries (Registry-Management) is displayed again. In the table within the lower area at Registries you can find an additional entry containing the information specified by you.

In case of a URL conflict the message Failure – A registry with the same URL already exists is displayed.
9.4.6.3 Deleting a registry

To delete a registry, proceed as follows:

- Below Registries, check the checkbox of the registry to be deleted within the table of the current registries.
- Click at the light red button *Remove*.
- A confirmation prompt asking whether the selected registries should really be deleted, appears.
- Confirm this by clicking at the light red button *Remove*.
- The selected registry is deleted. For a short time, also a confirmation message is displayed.

9.4.6.4 Open registry access management

To get to the page of the registry access management, proceed as follows:

- Go to page Registries (Registry management), see above.
- Click at *Manage access* in the line belonging to the desired registry within the table below Registries (Column Actions).

![Portainer.io - Page Registries (Registry-Management)](image)

- The page Registry access (Registries > [Registry name] > Access Management) is being opened:
Isolated application execution with Docker

Figure 67: Portainer.io - Registry access

9.4.6.5 Registry access management

Figure 68: Portainer.io - Registry access

In the area Registry (above), there are non-editable fields for displaying the name (Field Name) and the URL (Field URL) of the registry.

In area Access management users and teams of users are accepted or rejected.
To do so, there are two separate tables Users and teams (for users and teams without authorization) and Authorized Users and teams (for authorized users and teams).

Users and teams can be moved from one of these groups to the other one by simply shifting them.

Furthermore, there are the buttons Authorize all and Deny all. With those, one can authorize (Button Authorize all) or exclude (Button Deny all) all users and teams with a single click.

9.4.7 Stack management

A stack in the sense of Docker provides an execution environment in which some task and services may be present. For this environment you can define access control and supply environment variables. There are three different methods to create a stack:

1. Via the integrated web editor
2. Via upload of a Docker compose file
3. Using GitHub

9.4.7.1 Preparations for creating a stack

Prerequisite: The GUI portainer.io is already opened.

![portainer.io - Entry page Home](image)

- Within the darkblue menu on the left side click at Stacks.
- The page Create Stacks (Stacks > Add Stack) for the stack management in portainer.io is displayed.
This page consists of at least four separate areas:

1. **Bereich Build method:**
   Here you can choose the method, how the stack is created.

2. **Area Environment**
   If you want, you can additionally define environment variables here, which are supplied to the stack at execution time. See section *Set environment variables* [page 87].

3. **Area Access control**
   If you want, you can additionally define access restrictions here in order to allow access only to administrators, specific users or groups of users. See section *Define access control* [page 87].

4. **Area Actions**
   Here the deployment of the stack can be started.
9.4.7.2 Set environment variables

If you want so,, you can set one or more environment variables within the area Environment variables, which are valid within the stack to be created.

- To do so, for each variable click exactly once a the dark grey button add environment variable.
- For each environment variable, a new line is created within the area Environment variables. There, the name of the environment variable can be specified within field name (left side) and its value within field value (right side). At the right edge of each line there is a lightred button. If this button is clicked, the line will be removed with out any confirmation prompt.

9.4.7.3 Define access control

In area Access control, restrictions of access to stacks can be defined. In general, there are three possibilities:

1. There is no access control at all. To accomplish this option, set the slide switch right of Enable access control onto the left position. (Then no additional fields will be displayed within area Access control.)

2. Access is restricted to administrators only. To accomplish this option, set the slide switch right of Enable access control onto the right position and then click at the left field Administrators.

3. Access is restricted to specific users and teams. To accomplish this option, set the slide switch right of Enable access control onto the right position and then click at the left field Restricted. You can choose one or multiple users in the selection list Select one or more users right of Authorized users. Similarly, you can select the user groups in selection list Select one or more teams right of Authorized teams. This implies, that users or teams have already been defined.
Creating a stack via the integrated web editor

The Web GUI portainer.io contains an integrated Web editor allowing you to enter Docker compose files.

**Note:**
Concerning the syntax, the meaning and possibilities read section *Overview of Docker Compose* in the original Docker documentation at https://docs.docker.com/compose/overview/. There you will also find a command reference.

To create a stack via the integrated web editor:

- Proceed as described in *Preparations for creating a stack* [page 85].
- If necessary, set environment variables as described in *Set environment variables* [page 87].
- If required, restrict access as described in *Define access control* [page 87].
- In area Build method choose option Web Editor (left).
- The additional area Web Editor is now displayed containing an editor window for entering Docker compose files according to the syntax described within the above mentioned documentation. It looks like this:

![Portainer.io - Creating a stack via web editor](image)

**Figure 71: Portainer.io - Creating a stack via web editor**

- Specify your Docker compose file there.
- Click at **Deploy the stack** in area **Actions** in order to create the stack.
If the stack has been created successfully, an according message is displayed.

9.4.7.5 Creating a stack via upload of a Docker compose file

To create a stack via upload of a Docker compose file:

- Proceed as described in *Preparations for creating a stack* [page 85].
- If necessary, set environment variables as described in *Set environment variables* [page 87].
- If required, restrict access as described in *Define access control* [page 87].
- In area **Build method** choose option Upload (in the center).
- The additional area **Upload** is now displayed. See the following figure.

![portainer.io - Area "Upload"](image)

- Click at the blue button **Select file**.
- A file selection dialog opens. Select a valid Docker compose file there. This is required before the next step can be executed.
- Click at **Deploy the stack** in area **Actions** in order to create the stack.
- If the stack has been created successfully, an according message is displayed.
9.4.7.6 Creating a stack using GitHub

Alternatively, it is possible to create a stack within Docker by accessing a GitHub repository.

To create a stack using GitHub:

- Proceed as described in Preparations for creating a stack [page 85].
- If necessary, set environment variables as described in Set environment variables [page 87].
- If required, restrict access as described in Define access control [page 87].
- In area Build method choose option Repository (right).
- The additional area Git Repository is now displayed.

Specify the URL of the Git repository in field Repository URL.

Specify the reference of the Git repository in field Repository URL.

Specify the path to your Docker compose file in field Compose path.

All specifications for GitHub have been made now.

Click at Deploy the stack in area Actions in order to create the stack.

If the stack has been created successfully, an according message is displayed.
10 Public Key Infrastructure

This chapter explains, how a Public Key Infrastructure (PKI) for storing and administration of certificates and (private) keys can be established with the Edge gateway in order to provide protected data communication. First, the method of asymmetric encryption providing the logical foundation of the PKI is described, and the single members of the PKI are introduced. Then, certificates and keys are explained in more detail. Finally, all actions concerning PKI which are executable within the Control Panel of the Edge Gateway are explained within a step-by-step description.

Public Key Infrastructure (PKI) means a system to protect data communication based on asymmetric encryption that maintains digital certificates by creation, distribution, and checking. The Edge Gateway stores and checks digital certificates and can be integrated into a Public Key Infrastructure.
10.1 Asymmetric encryption

Asymmetric encryption uses a pair of keys consisting of a public key and a private key.

The private key is used to
- create signatures and
- decrypt messages.

The public key is used to
- verify signatures and
- encrypt messages.

A server provides the public key within a certificate. Beside the public key, a certificate includes even a signature and many more information. With a certificate, a client can identify a server and can encrypt messages (data) using the public key and send it to the server. The client does an authenticity check of the certificate of the server using one or more trustworthy root certificates which the client has stored in local directory of trustworthy certificates.

**Process of asymmetric encryption**

![Diagram of asymmetric encryption process](image)

*Figure 74: Process of asymmetric encryption*
1. The server has two keys
   – the **private key**
   – the **public key**
   – Both keys have a relation.
2. The client receives the certificate from the server which contains even the public key and a signature.
3. The client verifies the signature of the certificate using trustworthy certificates stored in its local directory of trustworthy certificates. Only if the authenticity check is ok, the client uses the received public key.
4. The client encrypts the message using the public key and sends the encrypted message to the server.
5. The server decrypt the message using his private key.
6. Client and server continue its encrypted communication using **one** new created protected transmitted key (symmetric communication).
10.2 Certificates and keys

A certificate can be considered as the digital confirmation of authenticity for the public key contained therein. For the time of its validity, the certificate connects the identity of the certificate owner owning the private key on one hand with the public key on the other hand. An advantage of the usage of certificates is that the effort of password administration is no longer necessary by creating a state of trust between the host and the issuer of the certificate.

10.2.1 Structure of a certificate according to X.509

The structure of a certificate corresponds to the standard X.509 issued by ITU-T or the equivalent ISO/IEC 9594-8 standard.

According to this, a certificate has the following constituents:

- Version
- Serial number
- Algorithm ID
- Time period of validity (specifications of begin and end)
- Specifications concerning the issuer of the certificate (see below)
- Specifications concerning the owner of the certificate (see below)
- Key information concerning the certificate owner
- Optional: Unique ID of the issuer of the certificate
- Optional: Unique ID of the owner of the certificate
- Signature algorithm
- Signature
- Extensions

The specifications concerning the issuer and the owner of the certificate may each have the following attributes:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>Common name</td>
</tr>
<tr>
<td>O</td>
<td>Organisation</td>
</tr>
<tr>
<td>OU</td>
<td>Organisational unit</td>
</tr>
<tr>
<td>C</td>
<td>Country or region</td>
</tr>
<tr>
<td>ST</td>
<td>State</td>
</tr>
<tr>
<td>L</td>
<td>Location</td>
</tr>
</tbody>
</table>

Table 34: Attributes concerning the issuer and owner of the certificate zum Zertifikats-Aussteller und Zertifikats-Inhaber
10.2.2 Hierarchy of trust

Certificates link with other certificates for authentication, that have been issued by an instance classified as being trustworthy. Such a certificate itself can link to another one, etc. So, a chain of concatenated certificates linked pair-wise is generated. This chain is denominated as the hierarchy of trust. One certificate is located at the end of this chain. This one is denominated as the root certificate. It is not linked to another certificate, but to itself, thus putting an end to the chain of certificates. Such certificates are denominated as self-signed certificates. You will only trust a self-signed certificate, if it has been signed by an extraordinarily trustworthy authority. For this purpose, Certificate Authorities (CAs)s have been established who sign certificate requests, who issue certificates and who check the identity and authority of the requestors. Usually, these are renowned official institutions, clubs or companies..

Consequently, the authenticity check of a certificate is practically done in that way, that the complete hierarchy of trust is tracked up to the root certificate, whose issuer is determined and a list of well-known trustworthy root certificates is searched whether it contains the root certificate at the end of the hierarchy of trust. Such lists are maintained by all browser manufacturers within the scope of special membership programmes and may be found within browsers, operating systems and mobile devices.

On the Edge Gateway the operating system Linux is run, which itself maintains such a list of root certificates of renowned CAs. This list is denominated as the Linux Trust Store and thus constitutes the Root Certificate Store of Linux.

---

**Note:**

A list of trustworthy root certificates is maintained by the Mozilla organisation under the denomination *Mozilla CA Certificate Store*, see [https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/](https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/). The display of root certificates in the Control Panel of the Edge Gateway follows this list.
10.2.3 File formats for certificate and key files

The Edge Gateway uses the PEM file format (Privacy Enhanced Mail according to RFC1421 to 1424) to store certificate and key files.

**PEM file format**

Certificate and key files for use in the PKI of the Edge Gateway use the Base64-coded PEM file format. Within this format, the genuine Base64-coded certificate data are surrounded by

```
-----BEGIN CERTIFICATE-----
at the beginning and
-----END CERTIFICATE-----
at the end of the PEM file.
```

Similarly, key data are surrounded by

```
-----BEGIN RSA PRIVATE KEY-----
and
-----END RSA PRIVATE KEY-----
```

You can convert a Base64-coded *.CER or *.CRT file into the *.PEM format, by following these steps:

- Surround the Base64-coded genuine certificate data with
  ```
  -----BEGIN CERTIFICATE-----
  at the beginning and
  -----END CERTIFICATE-----
  at the end.
  ```

- Surround the Base64-coded genuine key data with
  ```
  -----BEGIN RSA PRIVATE KEY-----
  at the beginning and
  -----END RSA PRIVATE KEY-----
  at the end.
  ```

- Change the file extension *.CER or *.CRT to *.PEM.
10.3 Use cases

<table>
<thead>
<tr>
<th>Use case</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificates</td>
<td>Use case 1: Verification of the authenticity of the communication partner (Server) [† page 97]</td>
</tr>
<tr>
<td>Server certificates and private keys</td>
<td>Use case 2: Server certificates for Edge Gateway services [† page 98]</td>
</tr>
</tbody>
</table>

Table 35: Overview use cases

10.3.1 Use case 1: Verification of the authenticity of the communication partner (Server)

The Edge Gateway (Client) can communicate in a protected (i.e. encrypted) way with a specific server. For this, the Edge Gateway needs the public key of the server, which the server provides within a certificate. This server certificate contains the public key and a signature (among other information). The signature serves the Edge Gateway to verify the server certificate. The client verifies the signature of the certificate using trustworthy root certificates which the Edge Gateway has stored in its local directory of trustworthy certificates. Only if the verification results in a valid authenticity, the Edge Gateway uses the received key.

When the Edge Gateway is delivered, it already has a directory with trustworthy certificates (Trusted Certification Authorities). You can add more trustworthy certificates or delete them. The preinstalled certificates originate from the Mozilla CA Store (https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/, e.g. List of included root certificates).

A trustworthy certificate can require another trustworthy certificate to verify authenticity. Consequently, a so called Hierarchy of trust [† page 95] is established. For verification, the Edge Gateway requires all trustworthy certificates.
certificates related to a specific server certificate. For this, if applicable, you have to load more trustworthy certificates into the directory of trustworthy certificates (Trusted Certification Authorities) of the Edge Gateway.

For details about “How to work with the certificates of this list (Upload, Download, Removal, Creation, Show List)” see section Verification of the authenticity of the communication partner using trustworthy certificates [page 100].

10.3.2 Use case 2: Server certificates for Edge Gateway services

In the role as a server, the Edge Gateway provides server certificates which contain the public key. An external client can encrypt the communication to the Edge Gateway with the public key and verify the authenticity of the Edge Gateway.

In the Edge Gateway, you can manage the private key and the related server certificate for a service. Each service of the Edge Gateway uses a separate pair consisting of private key and certificate. This certificate contains the public key, a signature and furthermore information.

From the point of view of the Edge Gateway, server certificates apply to inbound connections (e.g. HTTPS).

The file name for the private key is `key.pem`. The file name for the certificate is `cert.pem`. Both files have the PEM file format, see section File formats for certificate and key files [page 96].
Folder name (contains the pair of files) | Edge Gateway service
---|---
nginx | The Nginx server is the access point for several Edge Gateways services. The pair of files (private key `key.pem` and the related server certificate `cert.pem`) is used among other services for the following services:
- Edge Gateway Manager
- Portainer.io (Docker)

**Table 36: Edge Gateway Services**

**Note:**
The certificate (containing the public key) and the private key are stored in two separated files and uploaded individually into the Edge Gateway. As the user, you are solely responsible that the file with the certificate matches with the file containing the private key, which you have uploaded into the Edge gateway.

For details about “How to work with the certificates and key files (Upload, Download, Removal, Creation)”, see section *Working with server certificates for inbound connections* [page 103].
10.4 Verification of the authenticity of the communication partner using trustworthy certificates

Certificates from trustworthy sources can be used for verification of the authenticity of the communication partner using the hierarchy of trust as described within section Use case 1: Verification of the authenticity of the communication partner (Server) [page 97]. Within the Edge Gateway, a list of certificates of trustworthy issuers (Trusted Certification Authorities) is stored which can be adapted if required. The following actions can be performed:

1. Display list of trustworthy root certificates issued by Trusted Certification Authorities stored within the Edge Gateway
2. Upload a trustworthy certificate into the Edge Gateway
3. Download of certificates from the Edge Gateway into a file
4. Removing certificates/CAs that are no longer considered as trustworthy
5. Adding a new trustworthy certificate to the Linux trust store of the Edge Gateway

10.4.1 Display the list of trustworthy root certificates stored within the Edge Gateway

To display the list of trustworthy certificates within the Edge Gateway, which have been issued by Trusted Certification Authorities, proceed as follows:

- Select option Trusted Certification Authorities in selection list (Selection list for certificate type [page 59]).
- In window Certificates the list of trustworthy certificates within the Edge Gateway, which have been issued by Trusted Certification Authorities, is displayed (containing certificates originating from the Mozilla CA Certificate Shop, see https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/).

- Select the desired entry within window Certificates
- The window Certificate Viewer now shows the data of the selected certificate (Structure according to X.509 [page 94]).
10.4.2 Upload a trustworthy certificate into the Edge Gateway

To upload a trustworthy certificate from a file in *.pem format [page 96] and update it within the list of the Trusted Certification Authorities of the Edge Gateway, proceed as follows:

➢ Select option Trusted Certification Authorities within selection list (Selection list for certificate type [page 59]).

➢ In window Certificates, the list of trustworthy certificates within the Edge Gateway, which have been issued by Trusted Certification Authorities, is displayed (containing certificates originating from the Mozilla CA Certificate Store).

➢ Select the desired entry within window Certificates

➢ The window Certificate Viewer now shows the data of the selected certificate (Structure according to X.509 [page 94] standard).

➢ Click at button Upload in the header of window Certificates.

➢ A file selection dialog appears:

➢ Within that dialog, select the certificate file to be uploaded! This file must be present in the *.pem file format [page 96].

➢ The certificate file is checked for correctness. In case of error, a message indicating a defective file type appears and further processing is terminated. For instance, this occurs in case of the file not having the extension *.pem or the file contents is not coded in *.pem format. However, in case of success a security query appears whether you really intend to replace the certificate file.

➢ If you are really sure not to need the current certificate file any longer, click at Yes.

➢ The selected certificate file is uploaded into the Edge Gateway. During this, the formerly existing certificate within the Edge Gateway is irreversibly destroyed. Thus, there is no possibility to restore this certificate if no suitable backup is available. After some seconds, a message is displayed indicating that the upload has been completed and the Edge Gateway requires a restart according to the following note.

Note:
If you upload a trustworthy certificate from a file into the Edge Gateway, it is necessary to consequently perform a reboot of the Edge Gateway [page 36] for the changes to become effective.
10.4.3 Download of certificates from the Edge Gateway into a file

To download a trustworthy certificate from the list of the Trusted Certification Authorities of the Edge Gateway into a file in *.pem format, proceed as follows:

- Select option **Trusted Certification Authorities** within selection list (*Selection list for certificate type* [page 59]).
- In window **Certificates**, the list of trustworthy certificates within the Edge Gateway, which have been issued by Trusted Certification Authorities, is displayed (containing certificates originating from the Mozilla CA Certificate Store).
- Select the desired entry within window **Certificates**.
- The window **Certificate Viewer** now shows the data of the selected certificate (*Structure according to X.509 standard* [page 94]).
- Click at button **Download** in the header of window **Certificates**.
- A dialog box depending on the browser of your choice is displayed and asks you whether the file should be opened or stored.
- Select **Save** and then click on **OK**.
- The file is stored in *.pem* [page 96] format.

10.4.4 Removing certificates no longer considered as trustworthy

If you no longer trust the certificate or its issuer, proceed as follows to remove a certificate from the list of Trusted Certification Authorities of the Edge Gateway,

- Select option **Trusted Certification Authorities** within selection list (*Selection list for certificate type* [page 59]).
- In window **Certificates**, the list of trustworthy certificates within the Edge Gateway, which have been issued by Trusted Certification Authorities, is displayed (containing certificates originating from the Mozilla CA Certificate Store).
- Select the entry of the certificate to be removed in window **Certificates**.
- The window **Certificate Viewer** now shows the data of the selected certificate (*Structure according to X.509 standard* [page 94]).
- Click at button **Delete** in the header of window **Certificates**.
- A security query is displayed and warns against possible malfunction of the related application caused by the removal of certificates
- If you are really sure not to need the current certificate file any longer, click at **Yes**.
- The selected certificate file is being removed from the Edge Gateway.
10.5 Working with server certificates for inbound connections

For inbound connections, certificates can be stored within the Edge Gateway as described in *Use case 2: Server certificates for Edge Gateway services* [](#) page 98).

There is a 1:1-Relation between client and server (this means, exactly one certificate and one matching private key are required per client).

In this context, the following actions can be performed:

1. Uploading a pair consisting of a server certificate and the corresponding key file in *.*.pem format into the Edge Gateway
2. Downloading the server certificate from the Edge Gateway into a *.*.pem file
3. Removing a server certificate from the Edge Gateway
4. Removing a key corresponding to a server certificate from the Edge Gateway

---

**Note:**

The certificate (containing the public key) and the private key are stored in two separated files and uploaded individually into the Edge Gateway. As the user, you are solely responsible that the file with the certificate matches with the file containing the private key, which you have uploaded into the Edge gateway.
10.5.1 Uploading a pair of certificate file and key file for HTTPS and OPC UA Server

As certificates and the corresponding private keys are logically connected very firmly and must always be uploaded or changed together, uploading of an entire certificate-key-pair is described here within a single step description consisting of two separate consecutive steps of work. Nevertheless, uploading both of these separately is possible, but does not make very much sense.

---

**Note:**
Always take care of the order and upload the private key file `key.pem` first and then the certificate file `cert.pem` into the Edge Gateway as described below. This execution sequence is necessary as a check whether certificate and key match is performed every time a certificate file is uploaded and the key must already be present when this check takes place.

---

**Note:**
For the changes to become effective it is necessary to reboot the Edge Gateway [page 36] consequently if you upload a server certificate for communication with the HTTPS Server, Node-RED, the Edge Server or the REST API from a file into the Edge Gateway.
10.5.1.1 Step 1: Uploading a key file belonging to a server certificate into the Edge Gateway

To upload a key file belonging to a server certificate for the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API from a file into the Edge Gateway, proceed as follows.

- Select option Service certificates within selection list (Selection list for certificate type [page 59]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.

If the server certificate applies to the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API:

- Within window Certificates, select the entry key.pem below nginx.

Alternatively: If the server certificate applies to the communication with the OPC UA-Server:

- Within window Certificates, select the entry key.pem below opcua.
- In both cases, the window Certificate Viewer is empty now (Text No data).

- Click at button Upload in the header of window Certificates.

- A file selection dialog appears.

- Within that dialog, select the key file to be uploaded! This file must be present in the *.pem file format [page 96].

- The key file is checked for correctness. In case of error, a message appears indicating a defective file type and further processing of the key file is terminated. For instance, this occurs if the file does not have the extension *.pem or the contents of the file is not coded in *.pem format. However, in case of success a security query appears whether you really intend to replace the key file.

- If you are really sure not to need the current key file any longer, click at Yes.

- The selected key file is uploaded into the Edge Gateway. During this, the formerly existing key within the Edge Gateway is irreversibly destroyed. Thus, there is no possibility to restore this key if no suitable backup is available. After a short delay, a message is displayed indicating that the upload has been completed and the Edge Gateway requires a restart.
Step 2: Uploading the server certificate from a file into the Edge Gateway

To upload a server certificate for the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API from a file into the Edge Gateway, if the corresponding key file has already been uploaded, proceed as follows.

- Select option Service certificates within selection list (Selection list for certificate type [† page 59]).

Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.

If the server certificate applies to the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API:

- Within window Certificates, select the entry cert.pem below nginx.

Alternatively: If the server certificate applies to the communication with the OPC UA-Server:

- Within window Certificates, select the entry cert.pem below opcua.

In both cases, the window Certificate Viewer now displays the data of cert.pem.

- Click at button Upload in the header of window Certificates.

A file selection dialog appears:

- Within that dialog, select the certificate file to be uploaded! This file must be present in the *.pem file format [† page 96].

The certificate file is checked for correctness. In case of error, a message appears indicating a defective file type and further processing of the certificate file is terminated. For instance, this occurs if the file does not have the extension *.pem or the contents of the file is not coded in *.pem format. In case of success a security query appears whether you really intend to replace the key file.

- If you are really sure not to need the current certificate file any longer, click at Yes.

- If this check is passed, the selected file is uploaded into the Edge Gateway. During this, the formerly existing certificate within the Edge Gateway is irreversibly destroyed. Thus, there is no possibility to restore this certificate if no suitable backup is available. After a short delay, a message is displayed indicating that the upload has been completed and the Edge Gateway requires a restart.
10.5.2 Working with certificates for HTTPS and OPC UA Server

10.5.2.1 Uploading the server certificate from a file into the Edge Gateway

As described above, it should usually not be necessary to upload a server certificate without a corresponding key file. If you nevertheless require this functionality:

To upload a server certificate for the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API from a file into the Edge Gateway, proceed exactly as described in section *Step 2: Uploading the server certificate from a file into the Edge Gateway* [page 106] described.

10.5.2.2 Downloading the server certificate from the Edge Gateway into a file

To download a server certificate for the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API from the Edge Gateway into a file, proceed as follows.

- Select option *Service certificates* within selection list (*Selection list for certificate type* [page 59]).
- Within window *Certificates*, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.

If the server certificate applies to the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API:

- Within window *Certificates*, select the entry *cert.pem* below nginx.

Alternatively: If the server certificate applies to the communication with the OPC UA-Server:

- Within window *Certificates*, select the entry *cert.pem* below opcua.
- In both cases, the window *Certificate Viewer* now displays the data of *cert.pem*.
- Click at button *Download* in the header of window *Certificates*.
- A dialog box depending on the browser of your choice is displayed and asks you whether the file should be opened or stored.
- Select *Save* and then click on *OK*.
- The file is stored in *.*.pem [page 96] format.
10.5.2.3 Removing a server certificate from the Edge Gateway

To remove a server certificate from the Edge Gateway, proceed as follows.

- Select option Service certificates within selection list (Selection list for certificate type [page 59]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.

If the server certificate applies to the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API:

- Within window Certificates, select the entry cert.pem below nginx.

Alternatively: If the server certificate applies to the communication with the OPC UA-Server:

- Within window Certificates, select the entry cert.pem below opcua.
- In both cases, the window Certificate Viewer now displays the data of cert.pem.

- Click at button Delete in the header of window Certificates
- A security query whether you really intend to delete the server certificate file Cert.pem is displayed.
- If you are really sure not to need the currently stored certificate any longer, click at Yes.
- The selected file is removed from the Edge Gateway.

Note:

If a server certificate related to a specific service (for instance OPC UA Server), is removed, then the affected service will not be available until an according certificate is uploaded to the same position within the tree structure as that of the removed certificate.
10.5.3 Working with key files for HTTPS and OPC UA Server

10.5.3.1 Uploading a key file for a server certificate into the Edge Gateway

As described above, it should usually not be necessary to upload a key file belonging to a server certificate without the corresponding server certificate itself. If you nevertheless require this functionality:

To upload a key file into the Edge Gateway, proceed as described in section Step 1: Uploading a key file belonging to a server certificate into the Edge Gateway [page 105].

10.5.3.2 Removing a key file for a server certificate on the Edge Gateway

To remove a key file corresponding to a server certificate on the Edge Gateway, proceed as follows.

- Select option Service certificates within selection list (Selection list for certificate type [page 59]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.

If the server certificate corresponding to the key file applies to the communication with the HTTPS server nginx, Node-RED, the Edge Server or the REST API:

- Within window Certificates, select the entry key.pem below nginx.

Alternatively: If the server certificate corresponding to the key file applies to the communication with the OPC UA-Server:

- Within window Certificates, select the entry key.pem below opcua.
- In both cases, the window Certificate Viewer is empty now (Text No data).
- Click at button Delete in the header of window Certificates.
- A confirmation prompt whether you really intend to delete the key file key.pem corresponding to the server certificate, is displayed.
- If you are really sure not to need the current key file any longer, click at Yes.
- The key file is removed from the Edge Gateways.

Note:

If a server certificate related to a specific service such as OPC UA Client or Server, is removed, then the affected service will not be available until an according key for this certificate is uploaded to the same position within the tree structure as that of the formerly removed key.
11 Technical data

11.1 Technical data NIOT-E-NPI3-EN

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product</td>
<td>1321.510</td>
</tr>
<tr>
<td>Application</td>
<td>IoT and Industry 4.0 Edge automation projects</td>
</tr>
<tr>
<td>Processors</td>
<td>CPU</td>
</tr>
<tr>
<td>Integrated memory</td>
<td>RAM</td>
</tr>
<tr>
<td></td>
<td>FLASH</td>
</tr>
<tr>
<td>Power</td>
<td>Power supply</td>
</tr>
<tr>
<td></td>
<td>Typical/maximum current (at 24 V)</td>
</tr>
<tr>
<td></td>
<td>Power consumption</td>
</tr>
<tr>
<td></td>
<td>Connector</td>
</tr>
<tr>
<td>LAN interface</td>
<td>Interface type</td>
</tr>
<tr>
<td></td>
<td>Connector</td>
</tr>
<tr>
<td>Interfaces</td>
<td>USB</td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
</tr>
<tr>
<td></td>
<td>Display connector</td>
</tr>
<tr>
<td></td>
<td>Expansion module</td>
</tr>
<tr>
<td>Software</td>
<td>Operating system</td>
</tr>
<tr>
<td></td>
<td>Docker</td>
</tr>
<tr>
<td>Security</td>
<td>Access</td>
</tr>
<tr>
<td>Display</td>
<td>LED display</td>
</tr>
<tr>
<td>Real-time clock</td>
<td>Buffering</td>
</tr>
<tr>
<td>Environment</td>
<td>Ambient temperature range for operation</td>
</tr>
<tr>
<td></td>
<td>Ambient temperature range for storage</td>
</tr>
<tr>
<td></td>
<td>Humidity</td>
</tr>
<tr>
<td></td>
<td>Pollution degree</td>
</tr>
<tr>
<td></td>
<td>Altitude</td>
</tr>
<tr>
<td></td>
<td>Use</td>
</tr>
<tr>
<td>Device</td>
<td>Dimensions (H x W x L)</td>
</tr>
<tr>
<td></td>
<td>Weight</td>
</tr>
<tr>
<td></td>
<td>Housing</td>
</tr>
<tr>
<td></td>
<td>Mounting</td>
</tr>
<tr>
<td></td>
<td>Degree of protection</td>
</tr>
<tr>
<td>Approvals</td>
<td>FCC ID (Federal Communications Commission)</td>
</tr>
<tr>
<td></td>
<td>IC (Industry Canada)</td>
</tr>
<tr>
<td>UL certification</td>
<td>UL-File-Nr</td>
</tr>
<tr>
<td>Conformity</td>
<td>RoHS</td>
</tr>
</tbody>
</table>
### Table 37: Technical data NIOT-E-NPI3-EN

<table>
<thead>
<tr>
<th>NIOT-E-NPI3-EN</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conformance with EMC directives</td>
<td>CE sign</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Emission</td>
<td>EN 55011:2009</td>
</tr>
<tr>
<td></td>
<td>Immunity</td>
<td>IEC 61000-6-2/3, EN 61131-2</td>
</tr>
<tr>
<td></td>
<td>Electrostatic discharge (ESD) (air and contact discharge method)</td>
<td>EN 61000-4-2</td>
</tr>
<tr>
<td></td>
<td>Fast transient interferences (Burst)</td>
<td>EN 61000-4-4</td>
</tr>
<tr>
<td></td>
<td>Surge voltage</td>
<td>EN 61000-4-5</td>
</tr>
<tr>
<td>Tests</td>
<td>Shock</td>
<td>IEC 60068-2-27 Ea</td>
</tr>
<tr>
<td></td>
<td>Vibration</td>
<td>IEC 60068-2-6 Fc</td>
</tr>
</tbody>
</table>
12 Decommissioning, dismounting and disposal

12.1 Putting the device out of operation

**NOTICE**

Danger of Unsafe System Operation!

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

- Disconnect all communication cables from the device.
- Disconnect the power supply plug.
- Remove the device from the DIN top hat rail.

12.2 Disposal of waste electronic equipment

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

**Waste electronic equipment**

**Art und Quelle der Gefahr**

This product must not be treated as household waste.

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

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

13.1 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 fusion processes in nuclear power plants;
- Medical devices used for life support and
- Vehicle control systems used in passenger transport
shall be excluded. Use of the hardware and/or software in any of the following areas is strictly prohibited:
- For military purposes or in weaponry;
- For designing, engineering, maintaining or operating nuclear systems;
- In flight safety systems, aviation and flight telecommunications systems;
- In life-support systems;
- In systems in which any malfunction in the hardware and/or software may result in physical injuries or fatalities.

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

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

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

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

Costs of support, maintenance, customization and product care

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

Additional guarantees

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

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

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

Terms and conditions

Please read the notes about additional legal aspects on our netIOT web site under http://www.netiot.com/netiot/netiot-edge/terms-and-conditions/.
List of figures

Figure 1: netPI CORE ................................................................. 6
Figure 2: NIOT-E-NPI3-EN (Top view) ......................................... 7
Figure 3: NIOT-E-NPI3-EN (Front view) ........................................ 7
Figure 4: NIOT-E-NPI3-EN (Bottom view) ...................................... 8
Figure 5: Dimensions .................................................................. 9
Figure 6: LED positions ............................................................ 12
Figure 7: Gateway status LEDs ...................................................... 13
Figure 8: LAN interface and configuration ....................................... 14
Figure 9: NIOT-E-NPI3-EN device label (Host name) ...................... 15
Figure 10: Edge Gateway Manager ................................................ 17
Figure 11: Edge Gateway Manager - Setting the administrator password .... 20
Figure 12: Security error message of the Internet Explorer ............... 22
Figure 13: Security error message of the Firefox browser (1) .......... 22
Figure 14: Security error message of the Firefox browser (2) .......... 22
Figure 15: Firefox dialog box: Adding exceptional safety rule .......... 23
Figure 16: Security error message of Google Chrome (1) ............... 24
Figure 17: Security error message of Google Chrome (2) ............... 24
Figure 18: Main menu of the Control Panel .................................... 25
Figure 19: Page Info Center ........................................................ 27
Figure 20: Control Panel, page System > Syslog .............................. 29
Figure 21: Time configuration page ............................................... 32
Figure 22: Port settings ................................................................ 35
Figure 23: Reboot safety query ..................................................... 36
Figure 24: Warning for consequences of shutdown ......................... 37
Figure 25: Default LAN-configuration .......................................... 39
Figure 26: Wi-Fi (default setting) ................................................. 41
Figure 27: Wi-Fi modes of operation in selection list Mode .............. 41
Figure 28: Wi-Fi operating mode: Access point .............................. 42
Figure 29: Wi-Fi operating mode: Client ....................................... 44
Figure 30: Routes ..................................................................... 47
Figure 31: Defined Routes .......................................................... 49
Figure 32: Create new route ........................................................ 49
Figure 33: Define new route ........................................................ 50
Figure 34: Firewall ..................................................................... 51
Figure 35: Hostname .................................................................. 53
Figure 36: List of default services .................................................. 54
Figure 37: Page for configuring roles .......................................... 55
Figure 38: User account page ....................................................... 57
Figure 39: Public Key Infrastructure for managing of certificates ....... 58
Figure 40: Certificate type selection list ........................................ 59
List of figures

- **Figure 41:** Certificate Viewer ................................................................. 60
- **Figure 42:** Info page.................................................................................. 61
- **Figure 43:** User profile page ..................................................................... 61
- **Figure 44:** Dialog "Edit user account"...................................................... 62
- **Figure 45:** netPI block diagram................................................................. 66
- **Figure 46:** After the start of the Docker-Service within the Control Panel .. 68
- **Figure 47:** Tile Docker in the Edge Gateway Manager .......................... 69
- **Figure 48:** Initial call of portainer.io......................................................... 69
- **Figure 49:** portainer.io - initial screen Home (Endpoints) ....................... 70
- **Figure 50:** View of portainer.io dashboard............................................... 71
- **Figure 51:** Container list (portainer.io)...................................................... 71
- **Figure 52:** portainer.io - entry page Home............................................... 73
- **Figure 53:** portainer.io - Page Users > User management...................... 74
- **Figure 54:** portainer.io - Display of User Details ..................................... 75
- **Figure 55:** Tile Docker within the Edge Gateway Manager .................... 76
- **Figure 56:** portainer.io - entry page Home............................................... 76
- **Figure 57:** portainer.io - Page Registries (Registry management) .......... 77
- **Figure 58:** portainer.io - Page Registries (Registry-Management), Authentication has been activated .............................................................. 77
- **Figure 59:** Portainer.io - Page Create registry (Registries > Add registry) . 78
- **Figure 60:** Tile Docker within the Edge Gateway Manager ........................ 79
- **Figure 61:** portainer.io - entry page Home............................................... 79
- **Figure 62:** portainer.io - Page Registries (Registry management) .......... 80
- **Figure 63:** portainer.io - Page Registries (Registry-Management), Authentication has been activated .............................................................. 80
- **Figure 64:** Portainer.io - Page Create registry (Registries > Add registry) . 81
- **Figure 65:** Portainer.io - Page Create registry (Registries > Add registry), Custom registry selected .............................................................. 81
- **Figure 66:** portainer.io - Page Registries (Registry-Management).......... 83
- **Figure 67:** Portainer.io - Registry access .................................................. 84
- **Figure 68:** Portainer.io - Registry access .................................................. 84
- **Figure 69:** portainer.io - Entry page Home .............................................. 85
- **Figure 70:** portainer.io - Page Create Stacks (Stacks > Add Stack)......... 86
- **Figure 71:** Portainer.io - Creating a stack via web editor....................... 88
- **Figure 72:** portainer.io - Area "Upload"...................................................... 89
- **Figure 73:** Portainer.io - Creating a stack using GitHub......................... 90
- **Figure 74:** Process of asymmetric encryption......................................... 92
- **Figure 75:** Use case 1: Verification of the authenticity of the communication partner (Server) .............................................................. 97
- **Figure 76:** Use case 2: Server certificates for Edge Gateway services ....... 98
List of tables

Table 1: List of revisions ................................................................. 5
Table 2: Further information .......................................................... 5
Table 3: Positions of the interfaces .................................................. 8
Table 4: Power supply connector ..................................................... 10
Table 5: Names of the LEDs .......................................................... 12
Table 6: Description of gateway status LEDs ................................. 13
Table 7: LEDs LAN interface .......................................................... 13
Table 8: Starting applications with the Edge Gateway Manager ........... 18
Table 9: Functional overview of the Control Panel ............................ 25
Table 10: Info Center: Area System info. .......................................... 27
Table 11: Info Center: Area Monitoring ........................................... 28
Table 12: Info Center: Area Temperature ......................................... 28
Table 13: Numeric coding of facility value in priority PRI .................... 30
Table 14: Numeric coding of severity value in priority (PRI) ................. 30
Table 15: Assignment of parts of message line ................................. 31
Table 16: Setting the system time ................................................... 32
Table 17: Default ports .................................................................. 35
Table 18: Table LAN: Description of the columns and elements ............ 40
Table 19: Wi-Fi modes of operation in selection list Mode ..................... 41
Table 20: Wi-Fi ............................................................................. 41
Table 21: Parameters of the operating mode Access point .................... 43
Table 22: Parameters of the operating mode Client ............................. 45
Table 23: Parameters of Current connection configuration table ............. 48
Table 24: Routes parameters ........................................................... 49
Table 25: Parameters firewall .......................................................... 52
Table 26: Operating statuses of the services ....................................... 54
Table 27: Operating and display elements .......................................... 54
Table 28: Access rights onto resources .............................................. 56
Table 29: Access rights to resources ................................................ 56
Table 30: Container for netPI: Examples .......................................... 66
Table 31: Functions for working with containers ................................. 72
Table 32: Meaning of columns of table of all current registries .............. 78
Table 33: Meaning of columns of table of all current registries .............. 81
Table 34: Attributes concerning the issuer and owner of the certificate zum Zertifikats-Aussteller und Zertifikats-Inhaber 94
Table 35: Overview use cases .......................................................... 97
Table 36: Edge Gateway Services ..................................................... 99
Table 37: Technical data NIOT-E-NPI3-EN ....................................... 110
Contacts

HEADQUARTERS
Germany
Hilscher Gesellschaft für Systemautomation mbH
Rheinstrasse 15
65795 Hattersheim
Phone: +49 (0) 6190 9907-0
Fax: +49 (0) 6190 9907-50
E-mail: info@hilscher.com
Support
Phone: +49 (0) 6190 9907-99
E-mail: de.support@hilscher.com

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

France
Hilscher France S.a.r.l.
69500 Bron
Phone: +33 (0) 4 72 37 98 40
E-mail: info@hilscher.fr
Support
Phone: +33 (0) 4 72 37 98 40
E-mail: fr.support@hilscher.com

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

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

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

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

Switzerland
Hilscher Swiss GmbH
4500 Solothurn
Phone: +41 (0) 32 623 6633
E-mail: info@hilscher.ch
Support
Phone: +49 (0) 6190 9907-99
E-mail: ch.support@hilscher.com

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