



User manual  
netPI CORE  
NIOT-E-NPI3-EN  
V1.1.3



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

DOC181002UM01EN | Revision 1 | English | 2018-10 | Released | Public

# Table of contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
1.1	About the user manual	5
1.2	List of revisions	5
1.3	Further sources of information	5
<b>2</b>	<b>Brief description</b>	<b>6</b>
<b>3</b>	<b>Device drawings</b>	<b>7</b>
3.1	Positions of the interfaces	7
3.2	Dimensions	9
<b>4</b>	<b>Connectors and mounting</b>	<b>10</b>
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
<b>5</b>	<b>LEDs</b>	<b>12</b>
5.1	Positions of the LEDs on the gateway	12
5.2	Gateway status LEDs	13
5.3	LEDs of the LAN interface	13
<b>6</b>	<b>Commissioning the Edge Gateway</b>	<b>14</b>
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
<b>7</b>	<b>Edge Gateway Manager</b>	<b>17</b>
7.1	Calling the Edge Gateway Manager	17
7.2	Edge Gateway Manager web page	18
<b>8</b>	<b>Control Panel</b>	<b>20</b>
8.1	Opening the control panel	20
8.1.1	First login	20
8.1.2	Secure connection	22
8.2	Overview and main menu	25
8.3	System information and system time	26
8.3.1	Displaying system information	26
8.3.2	Displaying the system log files	27
8.3.3	Setting the system time	31
8.3.4	Rebooting the system	33
8.3.5	System shutdown	33
8.4	Packet management	34
8.4.1	Managing packets	34

8.5	Network.....	35
8.5.1	Configuring Ethernet communication (LAN) .....	35
8.5.2	Hostname.....	36
8.6	Services .....	37
8.6.1	Starting, stopping and configuring services .....	37
8.7	User management.....	38
8.7.1	Managing user roles .....	38
8.7.2	Managing user accounts.....	40
8.8	Security .....	41
8.8.1	Public Key Infrastructure.....	41
8.9	Help.....	44
8.10	Session .....	44
8.10.1	User profile.....	44
8.10.2	Logout.....	45
<b>9</b>	<b>Isolated application execution with Docker .....</b>	<b>46</b>
9.1	Docker, image, and container .....	46
9.2	Container for netPI: Examples .....	48
9.3	Working with Docker via the web GUI.....	50
9.3.1	The portainer.io interface .....	50
<b>10</b>	<b>Public Key Infrastructure .....</b>	<b>53</b>
10.1	Asymmetric encryption.....	53
10.2	Certificates and keys.....	55
10.2.1	Structure of a certificate according to X.509 .....	55
10.2.2	Hierarchy of trust.....	56
10.2.3	File formats for certificate and key files.....	57
10.3	Use cases .....	58
10.3.1	Use case 1: Verification of the authenticity of the communication partner (Server).....	58
10.3.2	Use case 2: Server certificates for Edge Gateway services .....	59
10.4	Verification of the authenticity of the communication partner using trustworthy certificates.....	61
10.4.1	Display the list of trustworthy root certificates stored within the Edge Gateway .. 61	61
10.4.2	Upload a trustworthy certificate into the Edge Gateway .....	62
10.4.3	Download of certificates from the Edge Gateway into a file.....	63
10.4.4	Removing certificates no longer considered as trustworthy.....	63
10.5	Working with server certificates for inbound connections .....	64
10.5.1	Uploading a a pair of certificate file and key file for HTTPS und OPC UA Server 64	64
10.5.2	Working with certificates for HTTPS and OPC UA Server.....	67
10.5.3	Working with key files for HTTPS and OPC UA Server .....	69
<b>11</b>	<b>Technical data.....</b>	<b>70</b>
11.1	Technical data NIOT-E-NPI3-EN .....	70
<b>12</b>	<b>Decommissioning, dismantling and disposal .....</b>	<b>72</b>
12.1	Putting the device out of operation.....	72
12.2	Disposal of waste electronic equipment.....	72
<b>13</b>	<b>Appendix.....</b>	<b>73</b>

---

13.1 Legal notes.....	73
<b>List of figures .....</b>	<b>77</b>
<b>List of tables.....</b>	<b>79</b>
<b>Contacts.....</b>	<b>80</b>

# 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

Revision	Date	Author	Change
1	2018-10-23	HHE	All sections created.

*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.

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

*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.

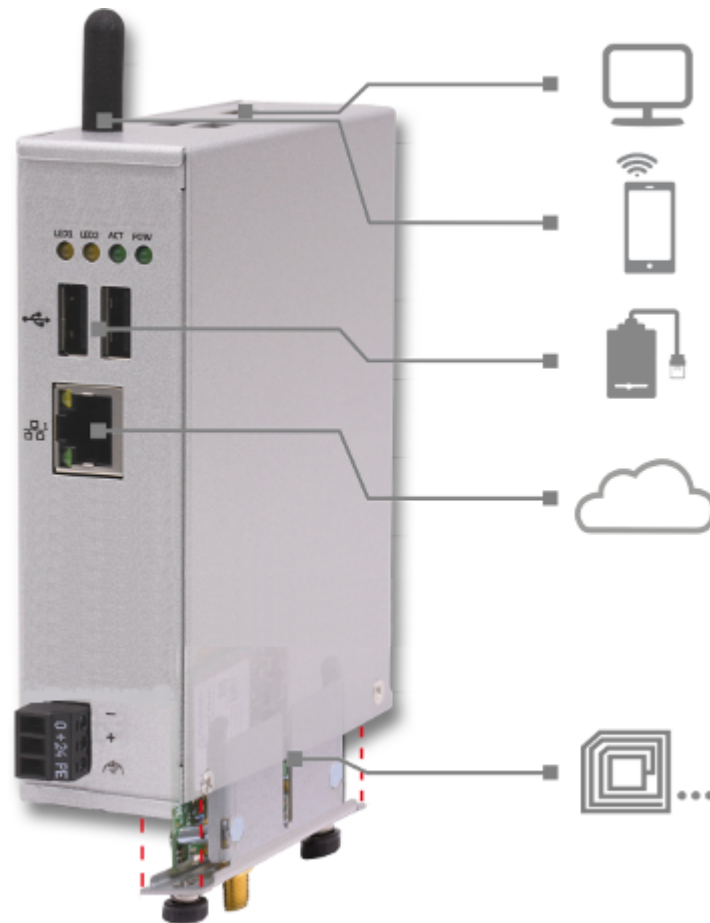


Figure 1: netPI CORE

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

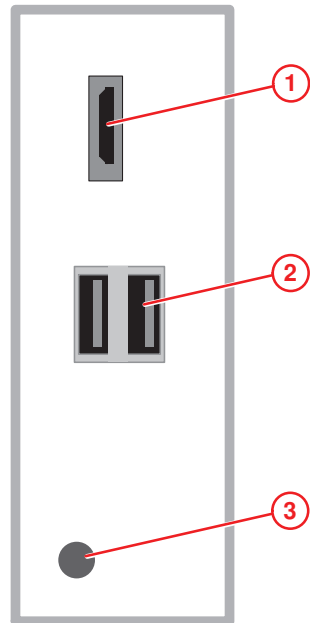


Figure 2: NIOT-E-NPI3-EN (Top view)

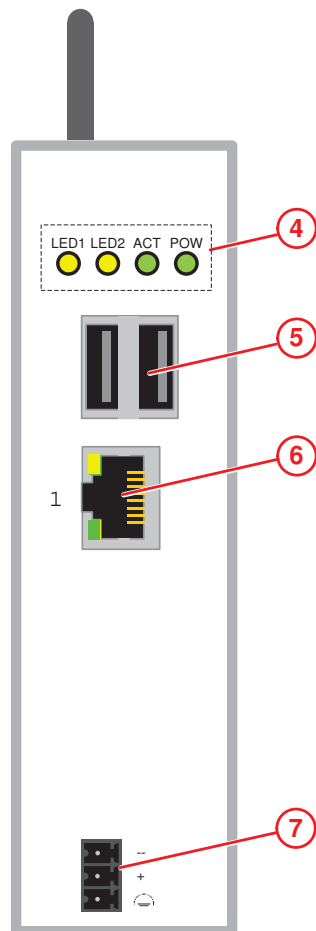


Figure 3: NIOT-E-NPI3-EN (Front view)

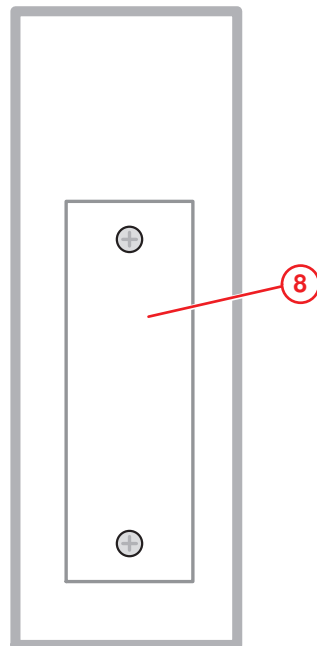


Figure 4: NIOT-E-NPI3-EN (Bottom view)

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

Table 3: Positions of the interfaces



### 3.2 Dimensions

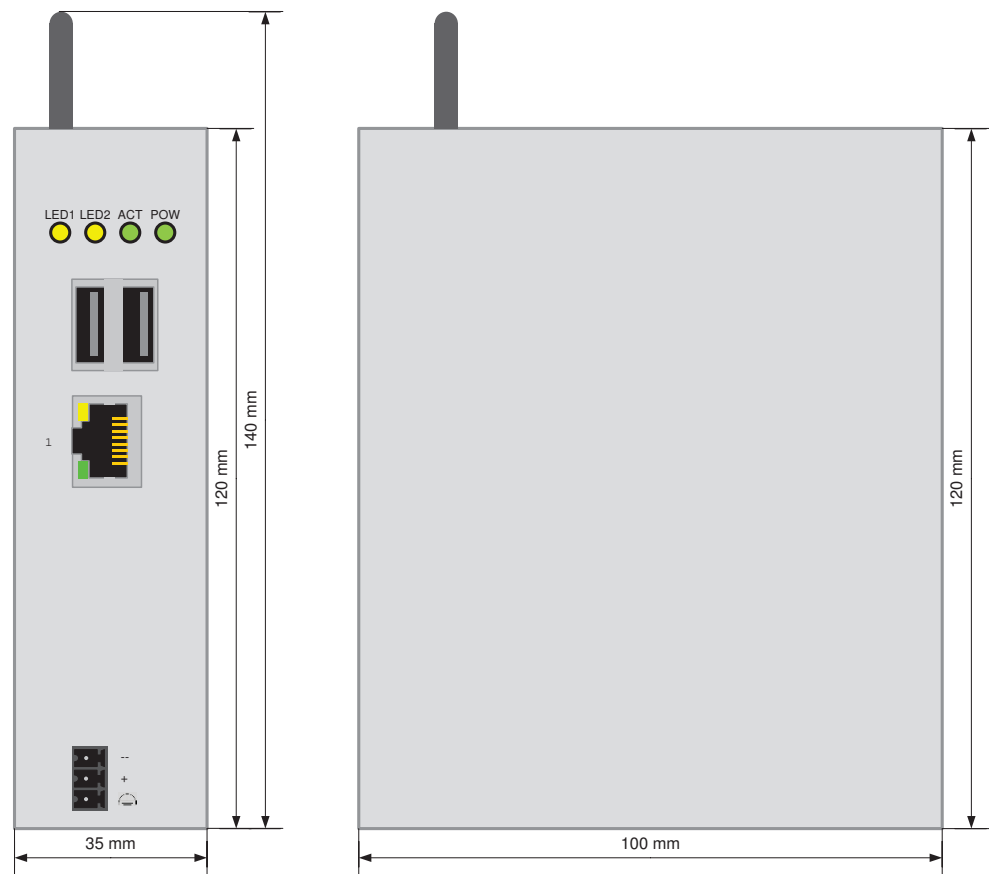


Figure 5: Dimensions

## 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



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

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 35] 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

You can use the Edge Gateway for wireless network communication. The Edge Gateway 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)* 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

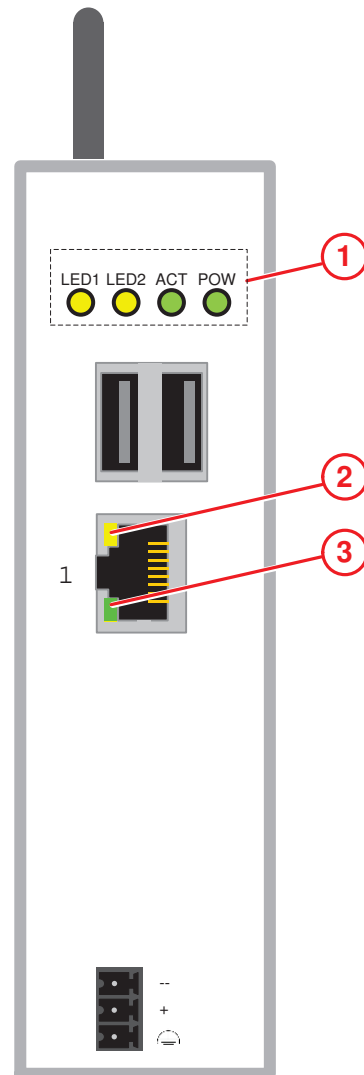


Figure 6: LED positions

Pos.	LED	For details see
(1)	Gateway status LEDs (4 x)	Gateway status LEDs [▶ page 13]
(2)	ACT / Rx/Tx LAN	LEDs of the LAN interface [▶ page 13]
(3)	LINK LAN	

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].

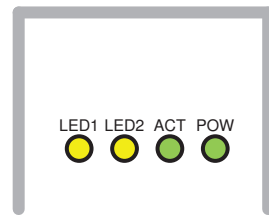


Figure 7: Gateway status LEDs

LED	Color	State	Meaning
LED1	● (yellow)	-	GPIO12, programmable
LED2	● (yellow)	-	GPIO13, programmable
ACT	☀ (green)	Blinking	Activity Linux operating system is active.
POW	● (green)	On	Supply voltage OK
	● (off)	Off	No supply voltage or supply voltage below 4.65 V.

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].

LED	Color	State	Meaning
<b>ACT / RX/TX</b>	<b>LED yellow</b>		
Position in the device drawing (2)	☀ (yellow)	Flickering (load dependent)	The device sends/receives frames
	● (off)	off	The device does not send/receive frames.
<b>LINK</b>	<b>LED green</b>		
Position in the device drawing (3)	● (green)	On	100 MBit network connection
	● (off)	off	10 MBit or no network connection

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.

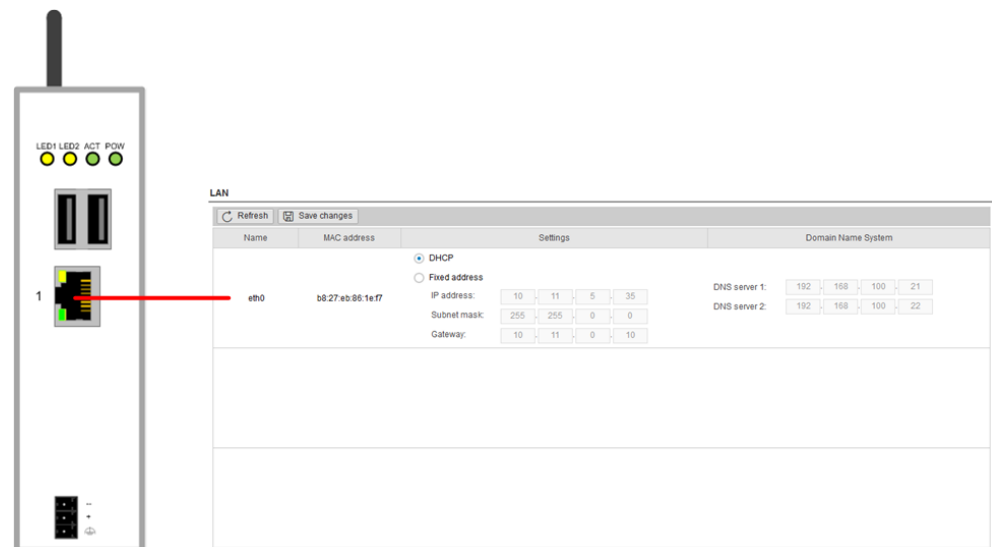


Figure 8: LAN interface and configuration

#### 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.

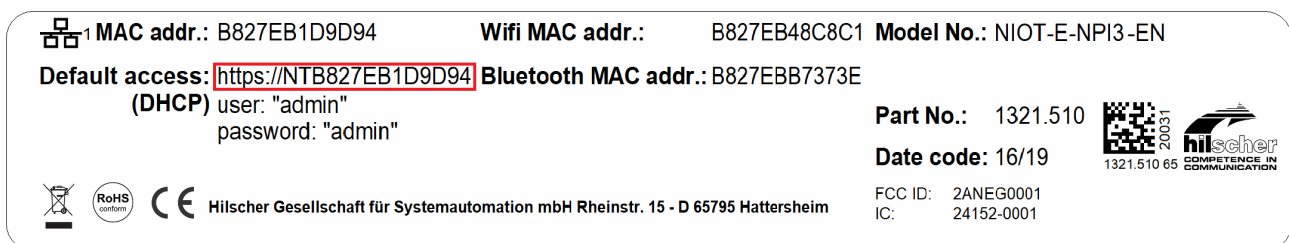


Figure 9: NIOT-E-NPI3-EN device label (Host name)

#### 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.

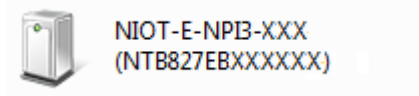
You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway Manager web page* [▶ page 18].

## 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**:



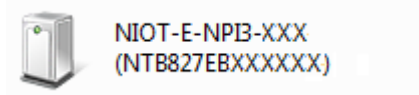
➤ Open the context menu of this entry and select **Properties**.

⇒ 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.



⇒ 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.

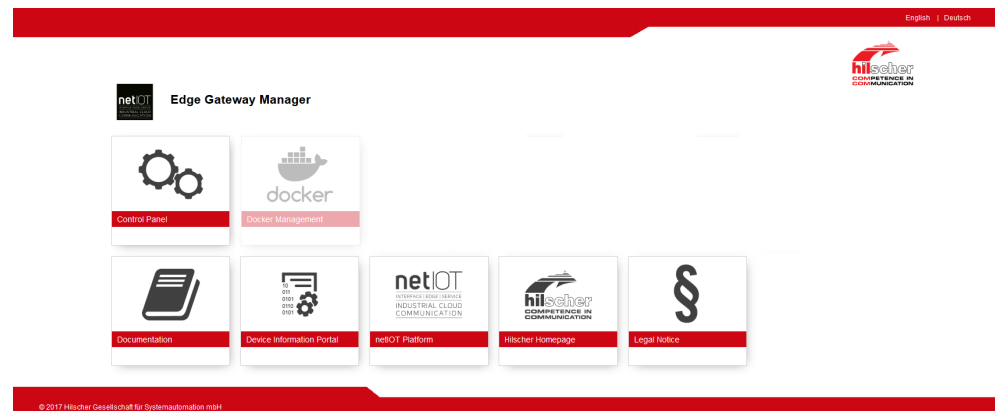


Figure 10: Edge Gateway Manager










#### 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.

Icon	Function
 Control Panel	<p>Opens the control panel of the Edge Gateway.</p> <p>The control panel configures the Edge Gateway and displays information on the system. Section <i>Control Panel</i> [▶ page 20] describes the possibilities of configuration as well as the displayed information on the system.</p>
 Docker Management	<p>Opens the Docker management.</p> <p>See section <i>Isolated application execution with Docker</i> [▶ page 46].</p>
 Documentation	<p>Opens the Edge Gateway documentation stored in the device.</p>
 Device Information Portal	<p>Opens the homepage of the Device Information Portal in the Internet.</p> <p>Requires a connection to the Internet.</p>
 netIOT Platform	<p>Opens the homepage of the netIOT platform in the Internet.</p> <p>Requires a connection to the Internet.</p>
 Hilscher Homepage	<p>Opens the Hilscher homepage in the Internet.</p> <p>Requires a connection to the Internet.</p>

Icon	Function
 <p data-bbox="454 201 710 432">The icon consists of a large black paragraph symbol (§) centered in the upper half. Below it is a solid red horizontal bar containing the text 'Legal Notice' in white. The entire icon is enclosed in a thin black border.</p>	<p data-bbox="710 201 1436 432">Opens legal information concerning the Edge Gateway. Requires a connection to the Internet.</p>

*Table 8: Starting applications with the Edge Gateway Manager*

## 8 Control Panel

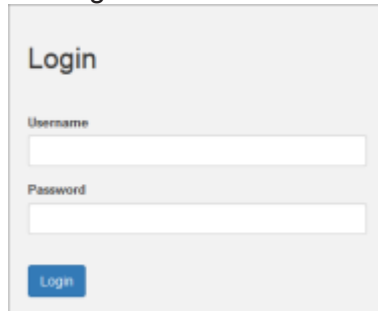
### 8.1 Opening the control panel

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.

A login screen with a light gray background. At the top, the word "Login" is displayed in a bold, dark font. Below it, there are two input fields: "Username" and "Password". Each field has a white background and a light gray border. Below the "Password" field is a blue button with the word "Login" in white text.

- 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.

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.

Weak password	Mediocre password	Strong 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)**.

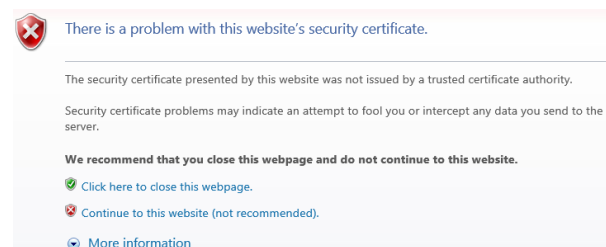


Figure 12: Security error message of the Internet Explorer

### 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:

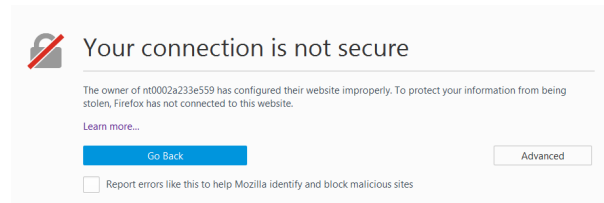


Figure 13: Security error message of the Firefox browser (1)

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

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

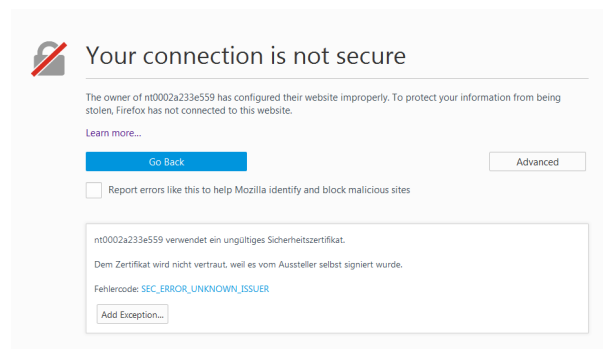


Figure 14: Security error message of the Firefox browser (2)

- To define an exceptional rule that enables the display of the user interface without repeated error messages, click **Add Exception**.

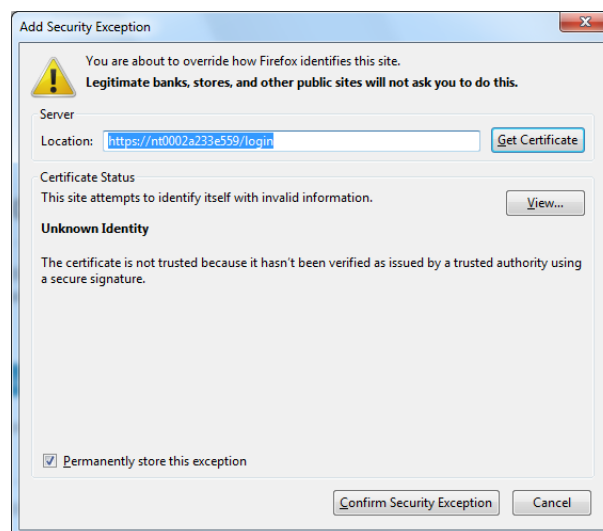


Figure 15: Firefox dialog box: Adding exceptional safety rule

- 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.

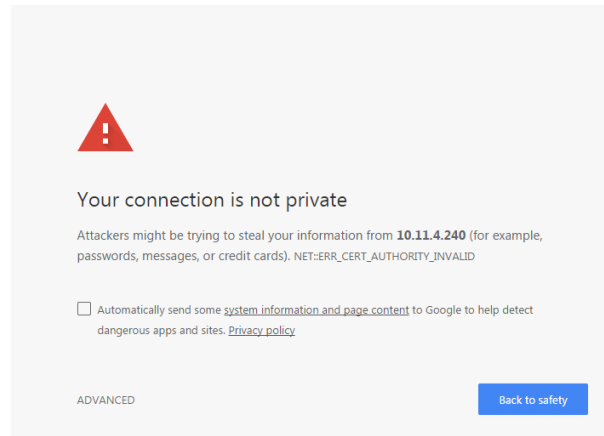


Figure 16: Security error message of Google Chrome (1)

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.

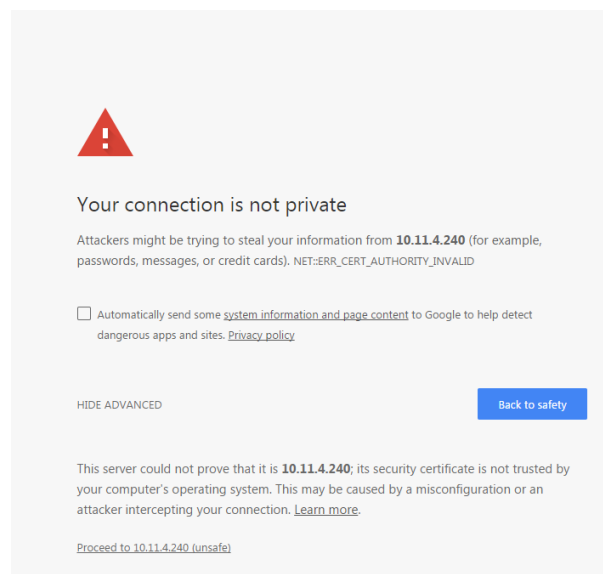


Figure 17: Security error message of Google Chrome (2)

- 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.

System ▾ Package Manager ▾ Network ▾ Services ▾ User Management ▾ Security ▾ Help ▾ Session ▾

Figure 18: Main menu of the Control Panel

Menu	Description	Details in section
System > Info Center	Displaying the system information, monitoring of the processor core temperature, and a system monitor for the usage of CPU, main memory, and SSD.	<i>Displaying system information</i> [▶ page 26]
System > Syslog	Displaying the system log files	<i>Displaying the system log files</i> [▶ page 27]
System > Time	Settings of system time and time synchronization.	<i>Setting the system time</i> [▶ page 31]
System > Reboot	Rebooting the Linux operating system of the Edge Gateway	<i>Rebooting the system</i> [▶ page 33]
System > Shutdown	Shutting down the Linux operating system of the Edge Gateway	<i>System shutdown</i> [▶ page 33]
Package Manager > Packages	Managing the packages of the Linux-based operating system of the Edge Gateway.	<i>Managing packets</i> [▶ page 34]
Network > LAN	Configuring the Ethernet interfaces to the IT network and OT network (fieldbus).	<i>Configuring Ethernet communication (LAN)</i> [▶ page 35]
Network > Wi-Fi	Configuring the Wi-Fi communication	Configuring wireless communication (WiFi)
Network > Hostname	Displaying and configuring the host name identifying the Edge Gateway in the network.	<i>Hostname</i> [▶ page 36]
Services > Service List	Displaying, starting, and stopping the services of the Edge Gateway.	<i>Starting, stopping and configuring services</i> [▶ page 37]
User Management > Roles	Displaying and configuring the permissions for user roles.	<i>Managing user roles</i> [▶ page 38]
User Management > Accounts	Displaying user accounts und assigning user roles.	<i>Managing user accounts</i> [▶ page 40]
Security > Public Key Infrastructure	Store and administer certificates and key files within the Public Key Infrastructure	<i>Public Key Infrastructure</i> [▶ page 41]
Help > Info	Displaying current software version.	<i>Help</i> [▶ page 44]
Session > User Profile	Displaying the permissions of the user.	<i>User profile</i> [▶ page 44]
Session > Logout	Logout	<i>Logout</i> [▶ page 45]

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.

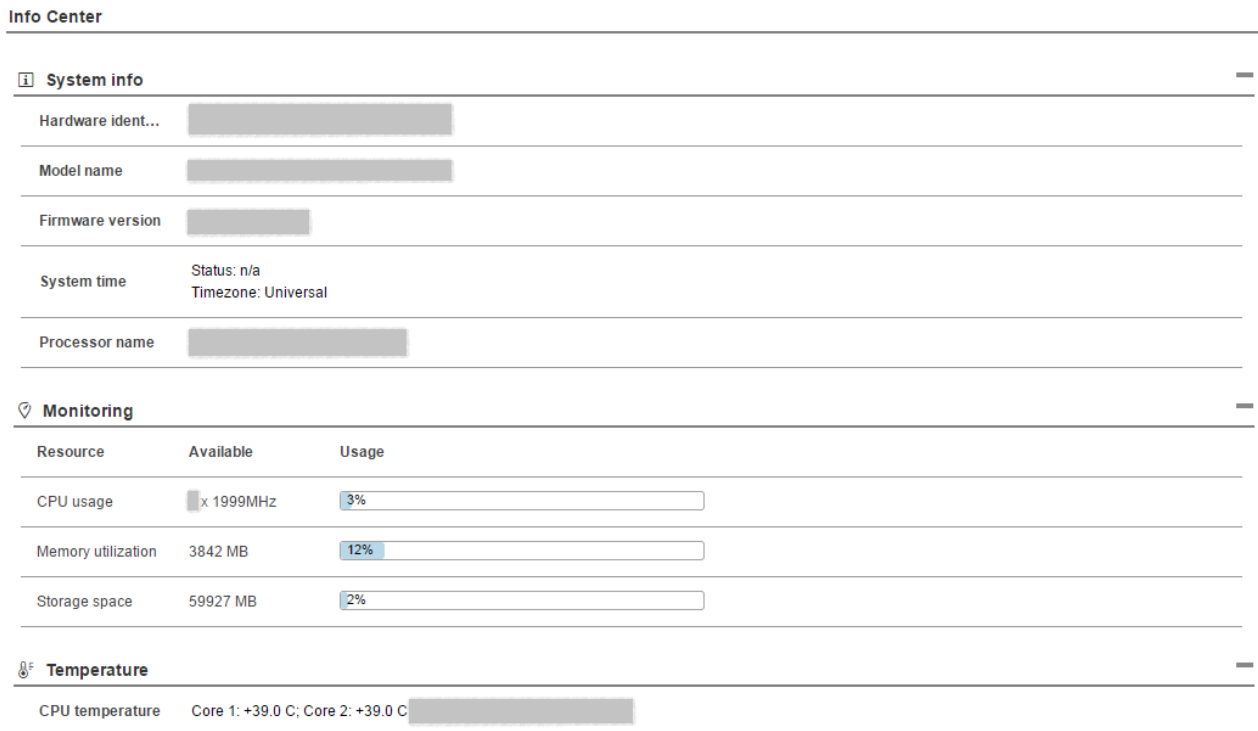


Figure 19: Page Info Center

The Info Center displays the following information:

System info	Description
Hardware ident.	Serial number of the Edge Gateway
Model name	Model designation of the Edge Gateway (NIOT-E-NPI3-EN)
Firmware version	Complete version designation of the firmware stored in the Edge Gateway
System time	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.
Processor name	Name of the microprocessor (CPU) installed in the Edge Gateway.

Table 10: Info Center: Area System info

Monitoring	Description
CPU usage	Number of microprocessor cores plus clock frequency and average utilization of each core in the Edge Gateway
Memory utilization	Size and average utilization of the main memory in the Edge Gateway
Storage space	Display of available memory and the memory that is currently utilized on the integrated Solid-State-Disk of the Edge Gateway

Table 11: Info Center: Area Monitoring

Temperature	Description
CPU temperature	Display of the temperature of each processor core in the Edge Gateway

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 nprograms

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/>).

### 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.

English

Control Panel

System Package Manager Network Services User Management

**Syslog**

Syslog Files

Download

Syslogs available	Modified	Size
syslog	Tue Jul 24 2018 11:07:52 GMT+0000 (UTC)	2626 KB
syslog-20180711.gz	Wed Jul 11 2018 07:30:01 GMT+0000 (UTC)	20 KB

Figure 20: Control Panel, page System > Syslog

- 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

PRI - Priority

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:

```
Priority = 8 * Facility + Severity
```

The facility is coded according to the following table:

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

Table 13: Numeric coding of facility value in priority PRI

The severity is coded according to the following table:

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

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

#### VERSION

Here the version number of the current sys'log 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.

PID	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.
MESSAGEID	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 <code>name=value</code> .

#### Example

```
[meta sequenceId="1"]
```

### MSG

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:

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

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**.

In order to access this page you require the following access right:

#### *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:

Type	Selection	Method	Standard presetting
manually	Manual selection	by entering date and time	yes
automatically	NTP synchronized	by means of a time server	no.

Table 16: Setting the system time

The screenshot shows the 'Time' configuration page. At the top, there is a 'Save changes' button. Below it, the 'Timezone' is set to 'Universal'. The 'Manual' option is selected, showing a 'Time' field with '14:51:57' and a 'Date' field with 'May 30, 2017'. The 'NTP synchronized' option is unselected, with a status of 'n/a'. Below this, there are buttons for '+ Add NTP server' and 'Delete'. A table lists the NTP server 'ptbtime1.ptb.de'.

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**.

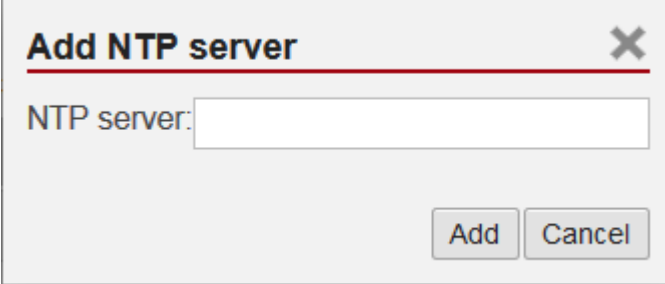
#### **Setting the system time manually**

- 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 lose 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 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:

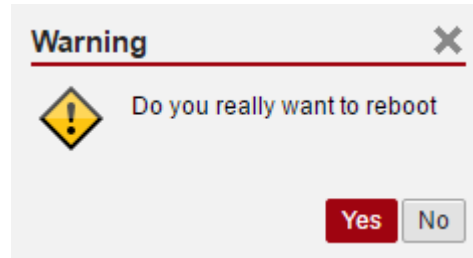


Figure 22: Reboot safety query

- 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.

---

### 8.3.5 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:

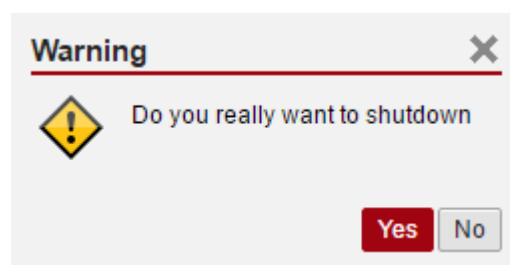


Figure 23: Warning for consequences of shutdown

- 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 access this page you require the following access right:

*Managing packets*

This page contains the package management of the Linux-based operating system of the Edge Gateway. This page

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



**Note:**

You can only install packages signed by Hilscher!

---

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**.

In order to access this page you require the following access right:

*Access to LAN (Ethernet network)*

The Ethernet interface `cifx0` is deactivated when delivered (factory setting). Section “Activating the Ethernet interface `cifx0`” (see below) describes how you can activate this interface.

For each Ethernet interface you can configure how to set the IP address:

- The Edge Gateway is to obtain the IP address parameters automatically from a DHCP server: Option DHCP.
- The IP address parameters are manually entered by the user: Option Fixed address.

The IP address parameters include the IP address, the subnet mask, the Gateway address, and the IP addresses of the 1st and 2nd domain name server.

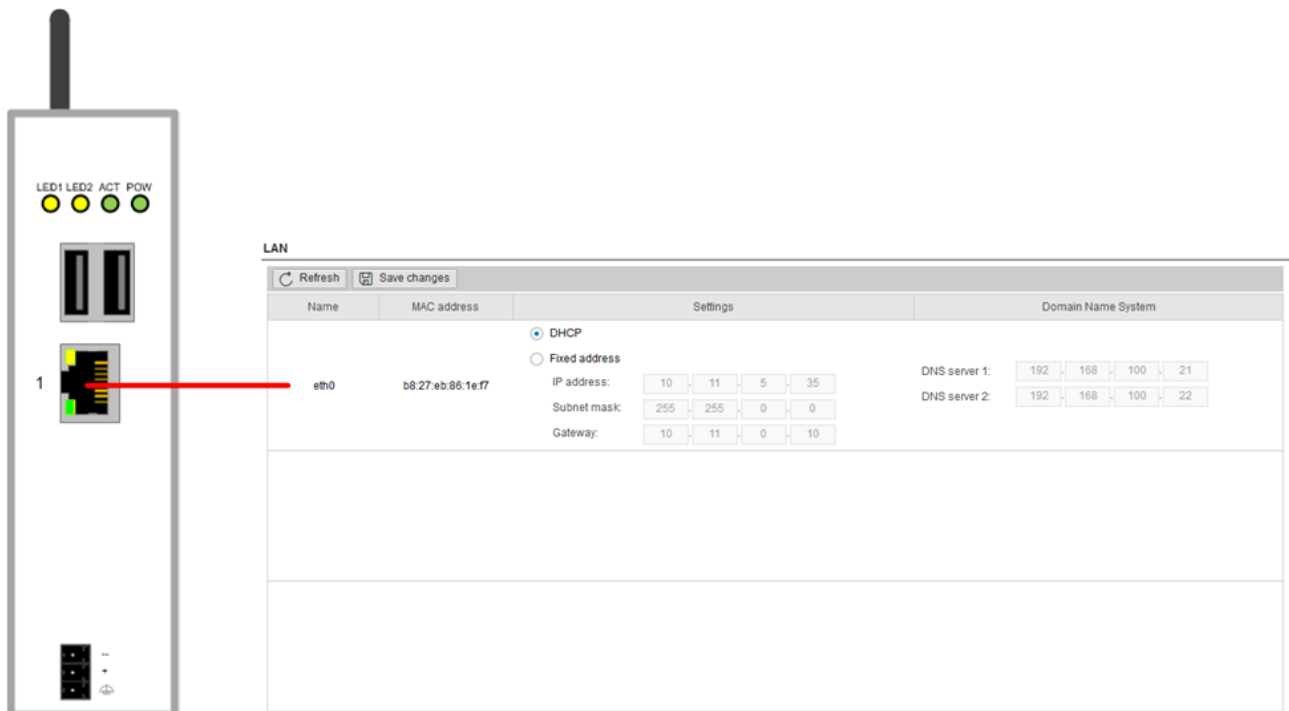


Figure 24: Default LAN configuration

Column	Meaning
Name	displays the name of the LAN interface.
MAC address	displays the MAC address of the LAN interface.
Settings	<p>Selecting the configuration method: Here you can select between</p> <ul style="list-style-type: none"> <li>• <i>DHCP</i> (IP address parameters automatically obtained from a DHCP server) or</li> <li>• <i>Fixed address</i> (IP address parameters entered by the user)</li> </ul> <p>If you enter the IP address manually, also always enter the subnet mask and the Gateway address.</p>
Domain Name System	If you enter the IP address parameters manually, enter the IP address of the 1st and 2nd domain name server.

Table 17: Table LAN: Meaning of the columns

If you want to save your changes permanent, click on **Save changes**.

## 8.5.2 Hostname

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

In order to access this page you require the following access right:

*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**

Figure 25: Hostname

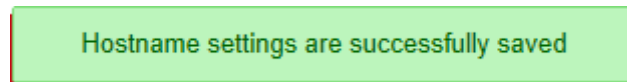
### Input field Hostname

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 .

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



## 8.6 Services

### 8.6.1 Starting, stopping and configuring services

Open this page with **Services > Service List**.

On this page you can

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

A service can allow you individual settings.

The list of services is displayed at the left edge:



Figure 26: List of default services

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

Color	Operating status
green	The service is being executed.
yellow	The service is configured, but not executed.
red	The service is neither configured nor executed.
grey	Right for accessing this service is missing

Table 18: Operating statuses of the services

## 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

Roles	
+ Create new role    Delete role	
Role	
Administrator	
View	
Save changes	
Resource	Access rights

Figure 27: 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:

Access right / Resource	Access to resource via menu	Usage
System		
Setting the system time	System > Time	<i>Setting the system time</i> [▶ page 31]
System log	System > Syslog	<i>Displaying the system log files</i> [▶ page 27]
Packet management		
Managing packets	Package Manager > Packages	<i>Managing packets</i> [▶ page 34]
Network access		
Access to LAN (Ethernet network)	Network > LAN	<i>Configuring Ethernet communication (LAN)</i> [▶ page 35]
Access onto Wi-Fi (wireless network)	Network > Wi-Fi	Configuring wireless communication (WiFi)
Access onto hostname of Edge Gateway	Network > Hostname	<i>Hostname</i> [▶ page 36]
Services		
Configure service "XYZ" (depends on installed services)	Services > Service "XYZ"	<i>Starting, stopping and configuring services</i> [▶ page 37]
Configure Docker	Services > Docker	<i>Isolated application execution with Docker</i> [▶ page 46]
Security		
Public Key Infrastructure (PKI)	Security > Public Key Infrastructure	<i>Public Key Infrastructure</i> [▶ page 41]

Table 19: Access rights onto resources

Each resource may obtain one of the following access rights:

Access rights onto resource	Checkbox
No access	None
Read access only	Read
Read and write access	Read, Write

Table 20: Access rights to resources

### Adding a new role

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

- 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.

#### User Accounts

+ Create new user account    ✎ Edit user account    🗑 Delete user account		
User name	Role	E-mail
admin	Administrator	

*Figure 28: User account page*

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*.

#### Public Key Infrastructure (PKI)

The screenshot shows the PKI management interface. At the top, there is a 'Certificate Type' dropdown menu with a red circle '1' next to it, containing options for 'Trusted Certification Authorities' and 'Service Certificates'. Below this is a toolbar with 'Upload', 'Download', 'Delete', and '+ Create' buttons. A list of certificates is displayed, with a red circle '2' next to the 'Certificates' header. The selected certificate is 'thawte\_Primary\_Root\_CA\_-\_G2.pem'. To the right, the 'Certificate Viewer' is open, showing details for the selected certificate, with a red circle '3' next to the viewer title. The viewer shows issuer information (country: 'US', organization: 'thawte, Inc.', organizationUnit: '(c) 2007 thawte, Inc. - For authorized use only', commonName: 'thawte Primary Root CA - G2', serial: '35.fc:26.5c:d9.84:4f:c9.3d:26.3d:57.9b:ae:d7.56', country: 'US', organization: 'thawte, Inc.', organizationUnit: '(c) 2007 thawte, Inc. - For authorized use only', commonName: 'thawte Primary Root CA - G2') and validity information (start: '2007-11-05T00:00:00.000Z', end: '2038-01-18T23:59:59.000Z', signatureAlgorithm: 'ecdsa-with-SHA384', publicKeySize: '384 bit').

Figure 29: 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

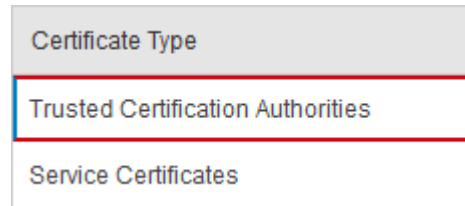


Figure 30: Certificate type selection list

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

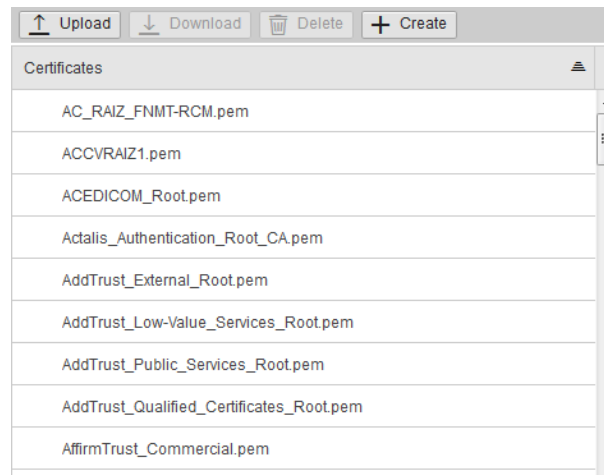
- certificates in the Trusted Certification Authorities or
- service certificates (server or client certificates for services in the Edge Gateway) for the communication using the HTTPS or OPC UA protocols.

### 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.

↑ Upload	↓ Download	🗑 Delete	+ Create
Certificates			
▼ nginx			
cert.pem			
key.pem			
▼ node-red			
node-opcuclient_cert.pem			
node-opcuclient_key.pem			
▼ opcuaserverforedge			
cert.pem			
key.pem			

### Certificate Viewer

📄 Copy path

Certificate Viewer - cert.pem

▼ issuer

country: "DE"

state: "Hessen"

locality: "Hattersheim"

organization: "Hilscher Gesellschaft fuer Systemautomation mbH"

commonName: "Hilscher OPC UA Server for Edge"

serial: "cb:e5:fd:1c:f8:b9:3d:be"

country: "DE"

state: "Hessen"

locality: "Hattersheim"

organization: "Hilscher Gesellschaft fuer Systemautomation mbH"

commonName: "Hilscher OPC UA Server for Edge"

san

▼ validity

start: "2018-07-06T13:59:40.000Z"

Figure 31: 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 55].



**Note:**

For more information on the foundations of asymmetric encryption techniques and public key infrastructure, see sections *Asymmetric encryption* [▶ page 53] and *Certificates and keys* [▶ page 55].

## 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

Version

Figure 32: 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**

[Edit user account](#)

User name

E-mail

Role

**Permissions**

Resource	Access
System	
• Time	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
Package Manager	
• Packages	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
Network	
• LAN	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
• WiFi	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
• Host Name	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
Services	
• Node-RED	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
• Secure shell (SSH)	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
• MQTT Broker	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
Security	
• SSL/TLS Certificate	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write
Edge Server	
• REST API	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read & Write

Figure 33: 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.

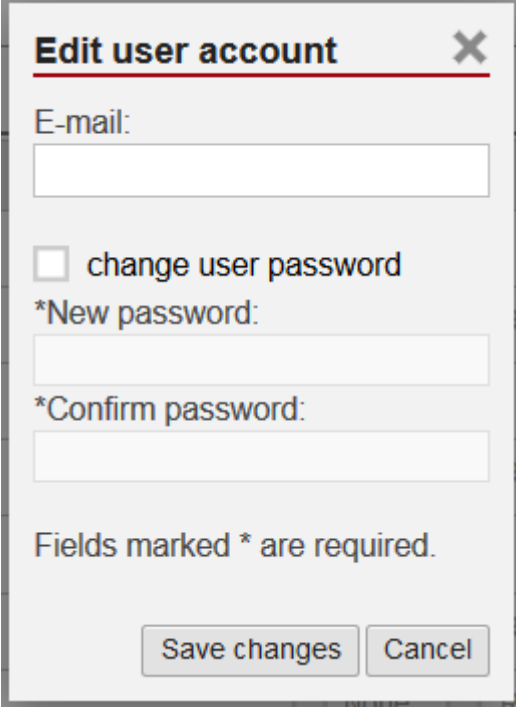


Figure 34: Dialog "Edit user account"

- 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.

## 9 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 said 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/>).

In order to work with Docker, read and write access rights at Docker UI are required. You can check whether you have the required access rights via the menu entry *User profile* [▶ page 44]. Granting read and right access rights requires administrator rights and is described in section *Managing user roles* [▶ page 38].

**Note:**

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

---

### 9.1 Docker, image, and container

#### Docker

Docker offers a platform for the isolated execution of applications within protected environments and, moreover, a standard for the distribution of software. This platform allows Edge Gateway users to run their own applications within the protected Linux operating system without being able to weaken or evade its safety mechanisms.

For realizing containers, Docker internally uses techniques from operating system virtualization. On the Edge Gateway, Docker is running as a service (Docker daemon `dockerd`).

As standard with Linux, Docker is controlled by entering commands via the command line. For reasons of safety, a command line service is not installed on the Edge Gateway.

Thus, Docker cannot be operated via a CLI (Command Line Interface) as described in the official Docker documentation (<https://docs.docker.com/>). An easy-to-use GUI (Graphical User Interface) `portainer.io` is installed instead. This GUI provides the essential functions for managing the Docker services.

**Note:**

For more information on `portainer.io`, see <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.

For distributing images via the Internet, the Docker organization provides a so-called repository under <https://hub.docker.com/>. Images stored there are freely accessible. Users can also manage their own repositories.



### Note:

For more information on images, see the Docker documentation <https://docs.docker.com/engine/docker-overview/%23docker-objects> 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 that is being executed in its individual runtime environment and can be compared with 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 against host machine and other containers, i.e. neither host machine nor other containers can influence it. Access to resources of the host system as e.g. host files and ports occurs only 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>).

---

## 9.2 Container for netPI: Examples

The device contains a Docker host enabling the deploy of own Edge automation applications to execute them in safe containers. Since netPI is a Docker host only, you cannot build images on-board. netPI's security concept prohibits SSH servicing and hence you cannot get access to "Docker build commands". Since containers run the same on any compatible hardware use a Raspberry Pi 3 instead for image development. Buying the consumer Pi for a low price is a riskless invest for getting familiar with Docker, making usability and performance tests of applications before moving them onto the professional netPI.

Docker hub is an Internet platform to share container images with co-workers, customers and the Docker community. For netPI there is a registry as well providing you examples for immediate use, such as the Thing Editor Node-RED or a HDMI desktop environment and many more. Use them also as templates for your own ideas when starting creating own images.

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



Name	Container contains
netpi-desktop-hdmi	HDMI desktop environment Activates the HDMI interface to connect a monitor and has a desktop.
netpi-raspbian	Raspbian-Betriebssystem Raspbian (jessy)
netpi-nodered-fieldbus	Node-RED and fieldbus node Processes I/O data of the Real-Time Ethernet using the Thing Editor Node-RED. netPI can be used for example as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter.
netpi-netx-programming-examples	Programming example Processes I/O data of the Real-Time Ethernet using access over the API. netPI can be used for example as PROFINET IO Device, EtherCAT Slave or EtherNet/IP Adapter.
netpi-nodered-fram	FRAM and Node-RED Using the FRAM with the Thing Editor Node-RED.
netpi-container-build-environment	Container environment Environment to develop container for netPI.

Table 21: Container for netPI: Examples

The following figure shows a possible usage of containers.

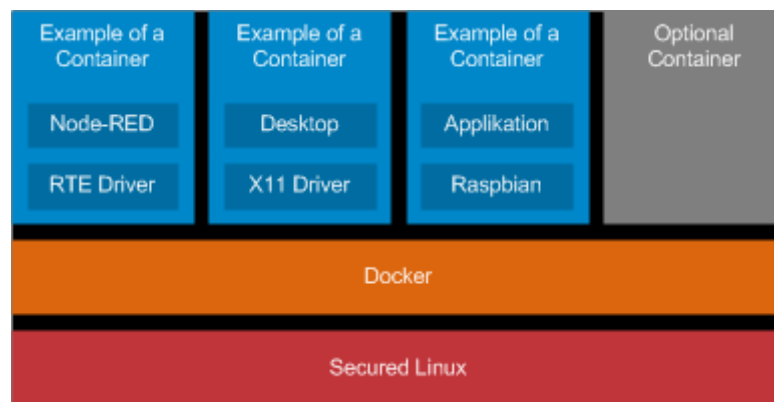


Figure 35: netPI block diagram

## 9.3 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).

### 9.3.1 The portainer.io interface

#### Tasks of the portainer.io interface

The portainer.io interface serves:

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

#### Starting the portainer.io interface for working with the containers

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

- Open the Edge Gateway Manager, if it is not already open.  
For this purpose see *Calling the Edge Gateway Manager* [▶ page 17]
- Click the tile *Docker Management* in the *Edge Gateway Manager*..



Figure 36: Tile Docker in the Edge Gateway Manager

- The portainer.io login screen will be displayed. In the field **Username**, *admin* is already entered. This is the only predefined user name.
- Enter the password for the user name *admin*. This password is set in the user management of the Edge Gateway Manager, see *User management* [▶ page 38].
- The start page "Dashboard" of the user interface portainer.io will be displayed.

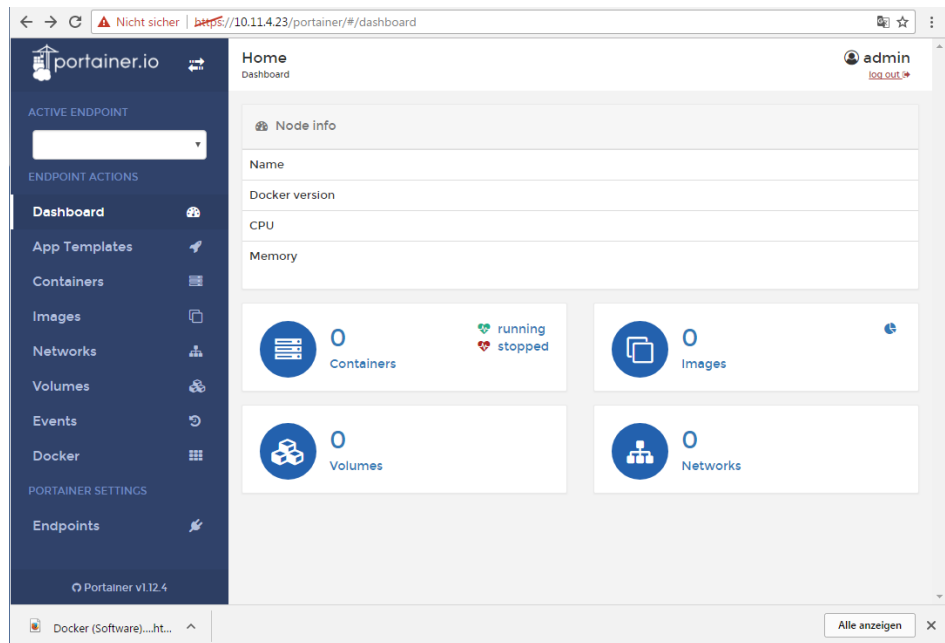


Figure 37: View of portainer.io dashboard

- Click **Containers** in the menu on the left or **Containers** on the page "Dashboard".
- ⇒ The page "Container list" will be displayed. This list contains the names and statuses of all currently known containers and provides the functions for controlling the code execution.

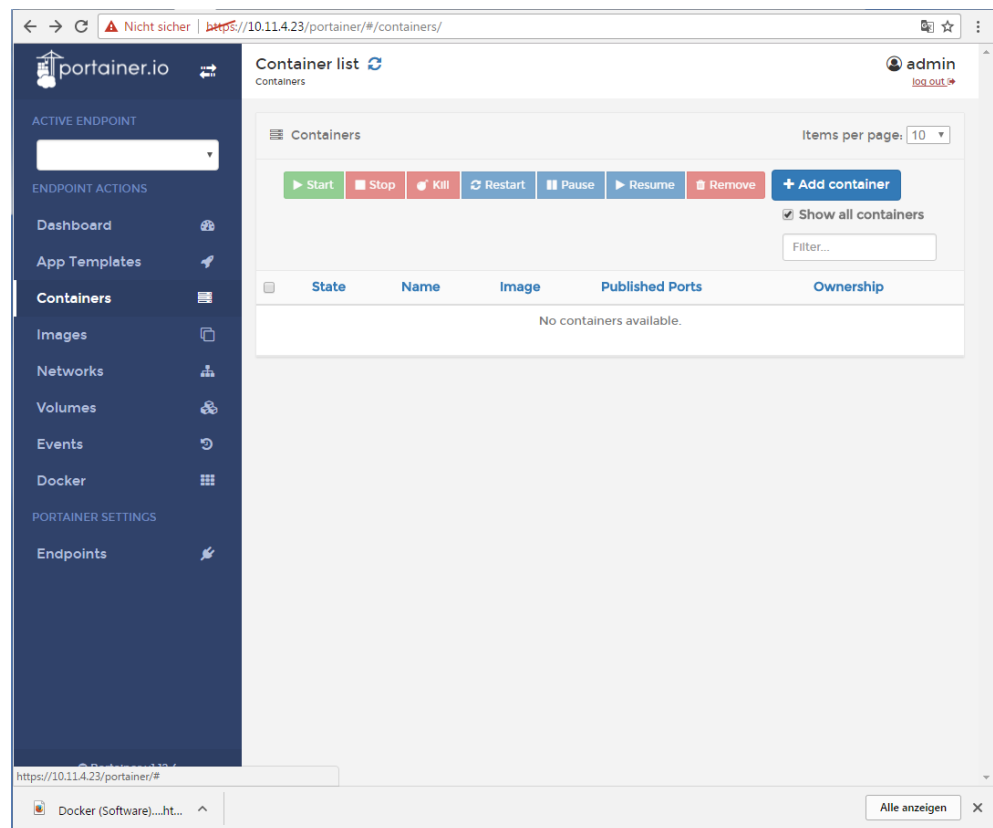


Figure 38: Container list (portainer.io)

## Functions for working with containers

Docker provides the following functions for controlling the code execution:






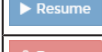
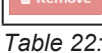
Icon	Function	Meaning
 Start	Start	Starting a container
 Stop	Stop	Stopping a container
 Kill	Kill	Aborting the execution of a container
 Restart	Restart	Repeated starting of a container
 Pause	Pause	Interrupting the execution of a container temporarily
 Resume	Resume	Continuing the execution of a container after an interruption
 Remove	Remove	Deleting a container

Table 22: Functions for working with containers

## 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

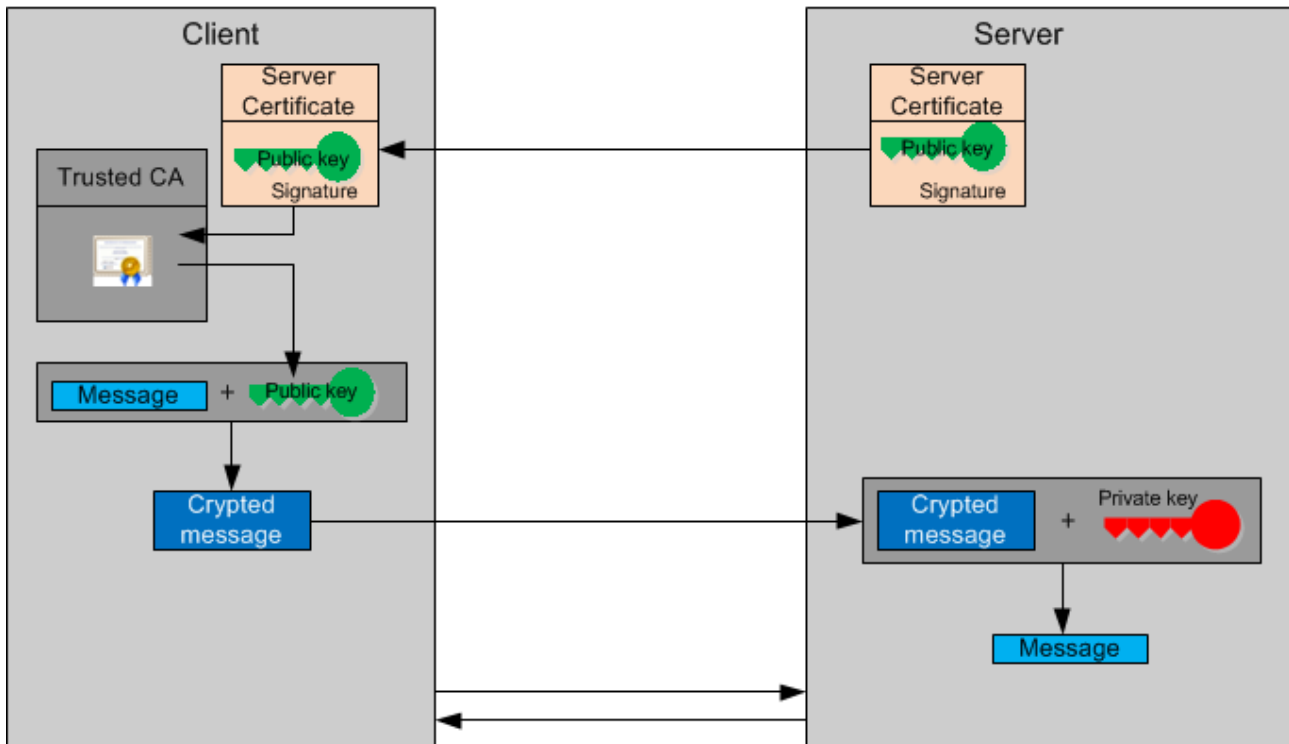


Figure 39: Process of asymmetric encryption

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 decrypts 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:

Attribute	Meaning
CN	Common name
O	Organisation
OU	Organisational unit
C	Country or region
ST	State
L	Location

*Table 23: 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) 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/>. 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.
- DChange the file extension \*.CER or \*.CRT to \*.PEM.

### 10.3 Use cases

Use case	Details in section
Root certificates	Use case 1: Verification of the authenticity of the communication partner (Server) [▶ page 58]
Server certificates and private keys	Use case 2: Server certificates for Edge Gateway services [▶ page 59]

Table 24: 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).

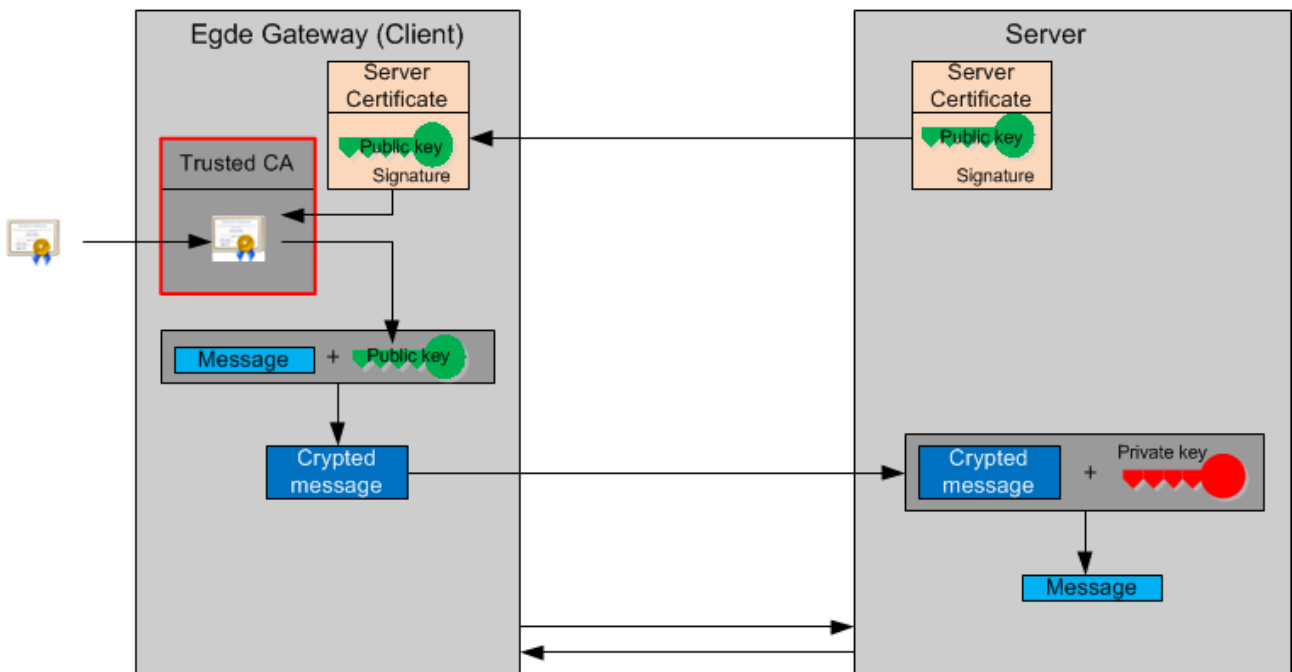


Figure 40: Use case 1: Verification of the authenticity of the communication partner (Server)

A trustworthy certificate can require another trustworthy certificate to verify authenticity. Consequently, a so called *Hierarchy of trust* [▶ page 56] is established. For verification, the Edge Gateway requires all trustworthy

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 61].

### 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).

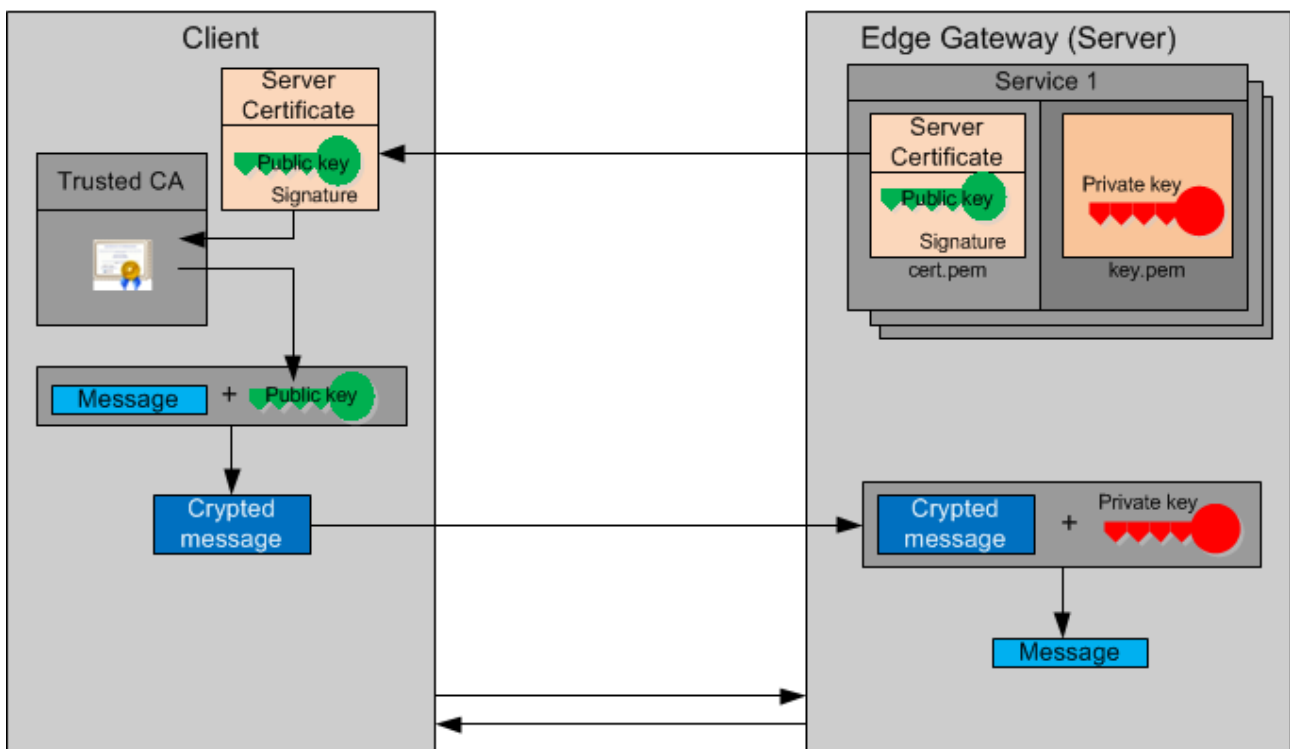


Figure 41: Use case 2: Server certificates for Edge Gateway services

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 57].

Folder name (contains the pair of files)	Edge Gateway service
nginx	<p>The Nginx server is the access point for several Edge Gateways services. The pair of files (private key <code>key.pem</code> and the related server certificate <code>cert.pem</code>) is used among other services for the following services:</p> <ul style="list-style-type: none"> <li>• Edge Gateway Manager</li> <li>• Portainer.io (Docker)</li> </ul>

Table 25: 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 64].

## 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 58]. 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 42]).
- ⇒ 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 55]).

## 10.4.2 Upload a trustworthy certificate into the Edge Gateway

To upload a trustworthy certificate from a file in *\*.pem format* [▶ page 57] 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 42]).
- ↗ 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 55] 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 57].
- ↗ 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 33] 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 42]).
- 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 55]).
- 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 57] 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 42]).
- 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 55]).
- 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 59].

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 a pair of certificate file and key file for HTTPS und 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 33] 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 42]).
- ⇒ 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 57].
- ⇒ 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

### 10.5.1.2 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 42]).
- ⇒ 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 57].
- ⇒ 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 66] beschrieben.

### 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 42]).
- ↗ 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 57] 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 42]).
- ↗ 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 65].

### 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 42]).
- ⇒ 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

NIOT-E-NPI3-EN	Parameter	Value
Product	Part number	1321.510
	Application	IoT and Industry 4.0 Edge automation projects
Processors	CPU	Broadcom BCM2837 1.2 GHz, 64 bit, 4 cores
Integrated memory	RAM	1 GByte
	FLASH	8 GByte MLC NAND (3000 w/e)
Power	Power supply	18 V DC ... 30 V DC
	Typical/maximum current (at 24 V)	170 mA / 400 mA
	Power consumption	Min. 4.2 W (no USB) Max. 9 W (USB with 1 A)
	Connector	3-pin terminal block (3.5 mm)
LAN interface	Interface type	10BASE-T/100BASE-TX, potential free
	Connector	1 x RJ45 socket
Interfaces	USB	4 x USB 2.0, max. 500 mA max. 1 A for all USB, type A
	Wireless	1 x WiFi, single-band 2.4 GHz IEEE 802.11b/g/n (BCM43438)
	Display connector	1 x HMDI (default: inactive)
	Expansion module	1 x slot for NPIX modules, 52 pins
Software	Operating system	Yocto Linux, AppArmor sicher
	Docker	Docker with Portainer.io Web GUI
Security	Access	HTTPS
Display	LED display	4 LEDs (2 programable)
Real-time clock	Buffering	Capacitor buffered, max. 7 days backup, maintenance free
Environment	Ambient temperature range for operation	-20°C ... +60°C
	Ambient temperature range for storage	-40°C ... +85°C
Device	Dimensions (H x W x L)	140 x 35 x 105 mm
	Weight	400 g
	Housing	Metal
	Mounting	DIN top hat rail
	Degree of protection	IP 20
Approvals	FCC ID (Federal Communications Commission)	2ANEG0001
	IC (Industry Canada)	24152-0001
Conformity	RoHS	Ja
Conformance with EMC directives	CE sign	Yes
	Emission	EN 55011:2009
	Immunity	IEC 61000-6-2/3, EN 61131-2
	Electrostatic discharge (ESD) (air and contact discharge method)	EN 61000-4-2
	Fast transient interferences (Burst)	EN 61000-4-4
	Surge voltage	EN 61000-4-5

NIOT-E-NPI3-EN	Parameter	Value
Tests	Shock	IEC 60068-2-27 Ea
	Vibration	IEC 60068-2-6 Fc

*Table 26: Technical data NIOT-E-NPI3-EN*

## 12 Decommissioning, dismantling 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 uninterrupted or the hardware and/or software is fault-free.

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

### **Confidentiality**

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

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

The customer must not allow any third party to become knowledgeable of this expertise and shall only provide knowledge thereof to authorized users as appropriate and necessary. Companies associated with the customer shall not be deemed third parties. The customer must obligate authorized

users to confidentiality. The customer should only use the confidential information in connection with the performances specified in this agreement.

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

### **Export provisions**

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

### **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 .....	21
Figure 12:	Security error message of the Internet Explorer .....	22
Figure 13:	Security error message of the Firefox browser (1) .....	23
Figure 14:	Security error message of the Firefox browser (2) .....	23
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 .....	26
Figure 20:	Control Panel, page System > Syslog .....	28
Figure 21:	Time configuration page .....	31
Figure 22:	Reboot safety query .....	33
Figure 23:	Warning for consequences of shutdown .....	33
Figure 24:	Default LAN configuration .....	35
Figure 25:	Hostname .....	36
Figure 26:	List of default services .....	37
Figure 27:	Page for configuring roles .....	38
Figure 28:	User account page .....	40
Figure 29:	Public Key Infrastructure for managing of certificates .....	41
Figure 30:	Certificate type selection list .....	42
Figure 31:	Certificate Viewer .....	43
Figure 32:	Info page .....	44
Figure 33:	User profile page .....	44
Figure 34:	Dialog "Edit user account" .....	45
Figure 35:	netPI block diagram .....	49
Figure 36:	Tile Docker in the Edge Gateway Manager .....	50
Figure 37:	View of portainer.io dashboard .....	51
Figure 38:	Container list (portainer.io) .....	51
Figure 39:	Process of asymmetric encryption .....	54

---

Figure 40:	Use case 1: Verification of the authenticity of the communication partner (Server).....	58
Figure 41:	Use case 2: Server certificates for Edge Gateway services.....	59

## 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.....	26
Table 11:	Info Center: Area Monitoring.....	26
Table 12:	Info Center: Area Temperature .....	27
Table 13:	Numeric coding of facility value in priority PRI.....	29
Table 14:	Numeric coding of severity value in priority (PRI).....	29
Table 15:	Assignment of parts of message line.....	30
Table 16:	Setting the system time .....	31
Table 17:	Table LAN: Meaning of the columns.....	36
Table 18:	Operating statuses of the services .....	37
Table 19:	Access rights onto resources.....	39
Table 20:	Access rights to resources.....	39
Table 21:	Container for netPI: Examples .....	49
Table 22:	Functions for working with containers.....	52
Table 23:	Attributes concerning the issuer and owner of the certificate zum Zertifikats- Aussteller und Zertifikats-Inhaber .....	55
Table 24:	Overview use cases.....	58
Table 25:	Edge Gateway Services .....	60
Table 26:	Technical data NIOT-E-NPI3-EN.....	70

# Contacts

## HEADQUARTERS

### Germany

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

### Support

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

## SUBSIDIARIES

### China

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

### Support

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

### France

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

### Support

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

### India

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

### Italy

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

### Support

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

### Japan

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

### Support

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

### Korea

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

### Switzerland

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

### Support

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

### USA

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

### Support

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