# Table of contents

1 **Introduction** .................................................................................................................................................. 7  
1.1 About the user manual ................................................................................................................................. 7  
1.2 List of revisions ............................................................................................................................................... 7  

2 **Brief description** ........................................................................................................................................... 8  

3 **Device drawings** .......................................................................................................................................... 10  
3.1 Positions of the interfaces ............................................................................................................................. 10  
3.2 Dimensions .................................................................................................................................................... 11  

4 **Connectors and mounting** ........................................................................................................................... 12  
4.1 Mounting ....................................................................................................................................................... 12  
4.2 Power supply .................................................................................................................................................. 12  
4.3 LAN connectors ............................................................................................................................................ 12  
4.4 Real-Time Ethernet connectors .................................................................................................................... 12  
4.5 USB connectors ............................................................................................................................................ 12  
4.6 Wi-Fi .............................................................................................................................................................. 13  
4.7 HDMI connector .......................................................................................................................................... 13  

5 **LEDs** ............................................................................................................................................................ 14  
5.1 Positions of the LEDs on the gateway ........................................................................................................... 14  
5.2 Gateway status LEDs ................................................................................................................................... 15  
5.3 LEDs of the LAN interface ............................................................................................................................ 15  
5.4 LEDs of the PROFINET IO Device interface ................................................................................................ 16  
5.5 LEDs of the EtherNet/IP Adapter interface .................................................................................................. 17  

6 **Commissioning the Edge Gateway** ........................................................................................................... 19  
6.1 Establishing the IP address communication ................................................................................................. 19  
6.2 Using the web browser to establish a connection with the Edge Gateway ................................................. 20  
6.2.1 Using the host name ................................................................................................................................... 20  
6.2.2 Access to the Edge Gateway in the Windows network environment ................................................ 21  

7 **Edge Gateway Manager** .................................................................................................................................. 22  
7.1 Calling the Edge Gateway Manager ........................................................................................................... 22  
7.2 Edge Gateway Manager web page ............................................................................................................... 23  

8 **Control Panel** ................................................................................................................................................. 25  
8.1 Opening the control panel ............................................................................................................................ 25  
8.1.1 First login ................................................................................................................................................. 26  
8.1.2 Secure connection ................................................................................................................................... 27  
8.2 Overview and main menu .............................................................................................................................. 31  
8.3 System information and system time ........................................................................................................... 33  
8.3.1 Displaying system information .................................................................................................................. 33  
8.3.2 License Manager ........................................................................................................................................ 35  
8.3.3 Displaying the system log files ................................................................................................................. 38  
8.3.4 Setting the system time ............................................................................................................................ 42  
8.3.5 Configure ports for HTTP/HTTPS communication ............................................................................... 44  
8.3.6 Backup and restore .................................................................................................................................. 46
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.3.7</td>
<td>Rebooting the system</td>
<td>53</td>
</tr>
<tr>
<td>8.3.8</td>
<td>System shutdown</td>
<td>54</td>
</tr>
<tr>
<td>8.4</td>
<td>Packet management</td>
<td>54</td>
</tr>
<tr>
<td>8.4.1</td>
<td>Managing packets</td>
<td>54</td>
</tr>
<tr>
<td>8.5</td>
<td>Network</td>
<td>55</td>
</tr>
<tr>
<td>8.5.1</td>
<td>Configuring Ethernet communication (LAN)</td>
<td>55</td>
</tr>
<tr>
<td>8.5.2</td>
<td>Configuring wireless communication (Wi-Fi)</td>
<td>58</td>
</tr>
<tr>
<td>8.5.3</td>
<td>Field</td>
<td>63</td>
</tr>
<tr>
<td>8.5.4</td>
<td>Configuring IP Routes</td>
<td>64</td>
</tr>
<tr>
<td>8.5.5</td>
<td>Configuring Firewall</td>
<td>68</td>
</tr>
<tr>
<td>8.5.6</td>
<td>Hostname</td>
<td>70</td>
</tr>
<tr>
<td>8.6</td>
<td>Services</td>
<td>71</td>
</tr>
<tr>
<td>8.6.1</td>
<td>Starting, stopping and configuring services</td>
<td>71</td>
</tr>
<tr>
<td>8.7</td>
<td>User management</td>
<td>75</td>
</tr>
<tr>
<td>8.7.1</td>
<td>Managing user roles</td>
<td>75</td>
</tr>
<tr>
<td>8.7.2</td>
<td>Managing user accounts</td>
<td>77</td>
</tr>
<tr>
<td>8.8</td>
<td>Security</td>
<td>78</td>
</tr>
<tr>
<td>8.8.1</td>
<td>Public Key Infrastructure</td>
<td>78</td>
</tr>
<tr>
<td>8.9</td>
<td>Help</td>
<td>81</td>
</tr>
<tr>
<td>8.10</td>
<td>Session</td>
<td>81</td>
</tr>
<tr>
<td>8.10.1</td>
<td>User profile</td>
<td>81</td>
</tr>
<tr>
<td>8.10.2</td>
<td>Logout</td>
<td>82</td>
</tr>
<tr>
<td>9</td>
<td>Node-RED - The wiring editor</td>
<td>83</td>
</tr>
<tr>
<td>9.1</td>
<td>Modelling IoT flows with nodes</td>
<td>84</td>
</tr>
<tr>
<td>9.2</td>
<td>Opening Node-RED</td>
<td>85</td>
</tr>
<tr>
<td>9.3</td>
<td>Graphical user interface</td>
<td>87</td>
</tr>
<tr>
<td>9.4</td>
<td>Working with Node-RED</td>
<td>89</td>
</tr>
<tr>
<td>9.4.1</td>
<td>Using Git hub repository to store flows (projects)</td>
<td>91</td>
</tr>
<tr>
<td>9.4.2</td>
<td>Menu Deploy</td>
<td>92</td>
</tr>
<tr>
<td>9.4.3</td>
<td>Dashboard</td>
<td>94</td>
</tr>
<tr>
<td>9.5</td>
<td>List of nodes</td>
<td>106</td>
</tr>
<tr>
<td>9.6</td>
<td>MQTT input node</td>
<td>109</td>
</tr>
<tr>
<td>9.7</td>
<td>MQTT output node</td>
<td>113</td>
</tr>
<tr>
<td>9.8</td>
<td>NPIX LEDs</td>
<td>115</td>
</tr>
<tr>
<td>9.9</td>
<td>Serial RS-232 send</td>
<td>116</td>
</tr>
<tr>
<td>9.10</td>
<td>Serial RS-232 receive</td>
<td>119</td>
</tr>
<tr>
<td>9.11</td>
<td>Serial inbound node RS-485</td>
<td>122</td>
</tr>
<tr>
<td>9.12</td>
<td>Serial outbound node RS-485</td>
<td>126</td>
</tr>
<tr>
<td>9.13</td>
<td>Digital I/O input node DIO in</td>
<td>130</td>
</tr>
<tr>
<td>9.14</td>
<td>Digital I/O output node DIO out</td>
<td>132</td>
</tr>
<tr>
<td>10</td>
<td>Examples for Node-RED</td>
<td>134</td>
</tr>
<tr>
<td>10.1</td>
<td>Example 1: Inject and debug node</td>
<td>134</td>
</tr>
<tr>
<td>10.2</td>
<td>Example 2: MQTT input node</td>
<td>136</td>
</tr>
<tr>
<td>10.3</td>
<td>Example 3: MQTT output node</td>
<td>140</td>
</tr>
<tr>
<td>10.4</td>
<td>Example 4: Fieldbus input node</td>
<td>144</td>
</tr>
</tbody>
</table>
## Table of contents

- **10.5** Example 5: Fieldbus output node ................................................................. 152

### 11 Configuring and using the fieldbus node ......................................................... 160

#### 11.1 Overview .................................................................................................... 160

#### 11.2 Configuring the fieldbus and defining the signals ...................................... 162

##### 11.2.1 Creating a new fieldbus configuration .................................................. 162

##### 11.2.2 Changing the existing fieldbus configuration ........................................ 167

### 12 Configuring PROFINET and defining signals ............................................... 173

#### 12.1 User interface ............................................................................................ 173

#### 12.2 Menu commands ....................................................................................... 173

##### 12.2.1 Project - Save ...................................................................................... 174

##### 12.2.2 GSDML Download .............................................................................. 174

##### 12.2.3 Printing the configuration ..................................................................... 174

##### 12.2.4 Help - Contents .................................................................................. 175

##### 12.2.5 Help - Information ............................................................................. 175

#### 12.3 Configuration tree ..................................................................................... 176

##### 12.3.1 PROFINET configuration ..................................................................... 176

##### 12.3.2 IO and signal configuration .................................................................. 177

##### 12.3.3 Signal definitions overview ................................................................. 186

##### 12.3.4 Download of the GSDML file............................................................. 187

##### 12.3.5 Help .................................................................................................... 187

### 13 Configuring EtherNet/IP and defining signals .............................................. 188

#### 13.1 User interface ............................................................................................ 188

#### 13.2 Menu commands ....................................................................................... 188

##### 13.2.1 Project - Save ...................................................................................... 189

##### 13.2.2 EDS Download .................................................................................... 189

##### 13.2.3 Printing the configuration ..................................................................... 190

##### 13.2.4 Help - Contents .................................................................................. 190

##### 13.2.5 Help - Information ............................................................................. 190

#### 13.3 Configuration tree ..................................................................................... 191

##### 13.3.1 EtherNet/IP configuration ..................................................................... 191

##### 13.3.2 IO and signal configuration .................................................................. 192

##### 13.3.3 Signal definitions overview ................................................................. 201

##### 13.3.4 Download of the EDS file .................................................................. 202

##### 13.3.5 Help .................................................................................................... 202

### 14 Edge Server .................................................................................................. 203

#### 14.1 Function principle ...................................................................................... 203

##### 14.1.1 Communication with IT-network and mobile devices ......................... 203

##### 14.1.2 Communication with the OT-network ................................................. 205

##### 14.1.3 Access rights to the REST API ............................................................. 205

##### 14.1.4 Functions of the Edge Server ............................................................... 206

##### 14.1.5 Internal structure of the Edge Server .................................................. 207

#### 14.2 Edge Server Control Center ...................................................................... 208

##### 14.2.1 Starting the Edge Server Control Center ............................................ 208

##### 14.2.2 Functions ............................................................................................ 208

##### 14.2.3 Service list .......................................................................................... 209

#### 14.3 Configuration of the Edge Server ............................................................... 211

##### 14.3.1 The configuration of IP address area ................................................... 211

##### 14.3.2 Selecting the protocols to scan for field devices ................................. 214
## Table of contents

19.1 Putting the device out of operation................................................................. 281
19.2 Removing device from top hat rail................................................................. 281
19.3 Disposal of waste electronic equipment....................................................... 281

20 Appendix.......................................................................................................... 282
  20.1 Legal notes................................................................................................... 282

List of figures ....................................................................................................... 286
List of tables ....................................................................................................... 291
Contacts............................................................................................................ 294
1 Introduction

1.1 About the user manual

This user manual describes the installation, configuration and functionality of the device NIOT-E-TPI51-EN-RE.

1.2 List of revisions

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Author</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2018-08-13</td>
<td>RGö, HHe</td>
<td>Section Displaying the system log files [→ page 38] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Security [→ page 78] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Public Key Infrastructure [→ page 244] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring wireless communication (Wi-Fi) [→ page 58] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section OPC UA input node updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section updated. OPC UA output node</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Public Key Infrastructure [→ page 244] updated.</td>
</tr>
<tr>
<td>5</td>
<td>2018-10-08</td>
<td>RGö, HHe</td>
<td>Section Configuring Ethernet communication (LAN) [→ page 55] updated and DHCP server added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring wireless communication (Wi-Fi) [→ page 58] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring cellular communication added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring IP Routes [→ page 64] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring Firewall [→ page 68] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Graphical user interface [→ page 87] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sections MQTT input node [→ page 109] and MQTT output node [→ page 113] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sections Example 4: Fieldbus input node [→ page 144] and Example 5: Fieldbus output node [→ page 152] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring the fieldbus and defining the signals [→ page 162] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Chapter Isolated application execution with Docker [→ page 215] updated.</td>
</tr>
<tr>
<td>6</td>
<td>2019-07-03</td>
<td>HHe, RGö, MKe</td>
<td>Section Configuring ports for HTTP/HTTPS communication [→ page 44] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Managing packets [→ page 54] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring Ethernet communication (LAN) [→ page 55] updated and DHCP server added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring wireless communication (Wi-Fi) [→ page 58] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring cellular communication added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring IP Routes [→ page 64] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring Firewall [→ page 68] added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Graphical user interface [→ page 87] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sections MQTT input node [→ page 109] and MQTT output node [→ page 113] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sections Example 4: Fieldbus input node [→ page 144] and Example 5: Fieldbus output node [→ page 152] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Section Configuring the fieldbus and defining the signals [→ page 162] updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Chapter Isolated application execution with Docker [→ page 215] updated.</td>
</tr>
<tr>
<td>7</td>
<td>2019-07-05</td>
<td>HHe</td>
<td>Section Technical data NIOT-E-TPI51-EN-RE [→ page 275]: Ratings added for UL-conform usage.</td>
</tr>
</tbody>
</table>

Table 1: List of revisions
2 Brief description

Hilscher’s netIOT Edge Gateway NIOT-E-TPI51-EN-RE securely connects Real-Time Ethernet automation networks with a “Cloud” or any IoT-directed application.

As a field device, it is performing a cyclic I/O data exchange with the PLC and communicates with further IoT-capable field devices within the automation network.

These key field data exchanged in real-time form the basis for intelligent higher-level IoT applications for cyber-physical processes and M2M solutions.

The gateway is designed for continuous operation in environments with permanent intranet or Internet connection. Security mechanisms such as the physical separation of automation and IT network, a secure operating system, the execution of signed firmware and packets, as well as encryption techniques of the latest standards secure the data integrity and offer protection against data theft.

The gateway base function forms the web-based Thing Wiring editor Node-RED, which serves to model the flows in the devices. Data apps and data profiles are created within minutes with predefined function blocks of the editor. OPC UA and MQTT functions address objects in IoT-capable field devices or in the cloud via standardized IoT protocols.

The Hilscher netIOT Service offers additional software packets to extend the Edge Gateway base functions by further applications or accesses to specific clouds.
The 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
### Table 2: Positions of the interfaces of NIOT-E-TPI51-EN-RE

<table>
<thead>
<tr>
<th>Pos.</th>
<th>Interface</th>
<th>For details see</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Connector for digital LCD display (HDMI)</td>
<td>HDMI connector [† page 13]</td>
</tr>
<tr>
<td>(2)</td>
<td>USB connectors (2x USB 2.0 on top of device)</td>
<td>USB connectors [† page 12]</td>
</tr>
<tr>
<td>(3)</td>
<td>Antenna (1 x Wi-Fi, for service only)</td>
<td>Wi-Fi [† page 13]</td>
</tr>
<tr>
<td>(4)</td>
<td>ERR/NS LED</td>
<td>LED for communication status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bus error (PROFINET) /</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network status (EtherNet/IP)</td>
</tr>
<tr>
<td>(5)</td>
<td>RUN/MS LED</td>
<td>LED for communication status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System error (PROFINET) /</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Module status (EtherNet/IP)</td>
</tr>
<tr>
<td>(6)</td>
<td>Gateway status LEDs (6 x)</td>
<td>Gateway status LEDs [† page 15]</td>
</tr>
<tr>
<td>(7)</td>
<td>USB connectors (2x USB 2.0 on front of device)</td>
<td>USB connectors [† page 12]</td>
</tr>
<tr>
<td>(8)</td>
<td>LAN connector (RJ45 jacket) port 1 / Eth0</td>
<td>LAN connectors [† page 12]</td>
</tr>
<tr>
<td>(9)</td>
<td>Real-Time Ethernet connector (RJ45 jacket) channel 0</td>
<td>Real-Time Ethernet connectors [† page 12]</td>
</tr>
<tr>
<td>(10)</td>
<td>Real-Time Ethernet connector (RJ45 jacket) channel 1</td>
<td>Real-Time Ethernet connectors [† page 12]</td>
</tr>
<tr>
<td>(11)</td>
<td>+24 V DC supply voltage connector (Mini Combicon)</td>
<td>Power supply [† page 12]</td>
</tr>
<tr>
<td>(12)</td>
<td>Cover at bottom of device (bolted)</td>
<td>-</td>
</tr>
</tbody>
</table>

#### 3.2 Dimensions

![Figure 2: Dimensions](image-url)
4 Connectors and mounting

4.1 Mounting

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

4.2 Power supply

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

Table 3: Power supply connector

4.3 LAN connectors

The Edge Gateway has one LAN connector for connecting it to the cloud network (IT network), position (8) (see section Positions of the interfaces [page 10]).

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

Section Configuring Ethernet communication (LAN) [page 55] describes, how you can set the IP address parameters of the LAN interfaces.

4.4 Real-Time Ethernet connectors

The Edge Gateway has 2 RJ45-connectors to connect the fieldbus to a Real-Time Ethernet network (OT network), positions (9) and (10) (see section Positions of the interfaces [page 10]).

For data exchange at the fieldbus, use the fieldbus input and output in node Node-RED. Sections Example 4: Fieldbus input node [page 144] and Example 5: Fieldbus output node [page 152] describe how to access the cyclic I/O data of the fieldbus in Node-RED.

4.5 USB connectors

The Edge Gateway has 4 USB connectors (4 x USB 2.0), positions (2) and (7) (see section Positions of the interfaces [page 10]).
4.6 Wi-Fi

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

Section *Configuring wireless communication (Wi-Fi)* [page 58] describes how you activate the antennas and how to set the Wi-Fi operating mode.

4.7 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/](https://hub.docker.com/r/hilschernetpi/).
5  LEDs

5.1  Positions of the LEDs on the gateway

Figure 3: NIO-E-TPI51-EN-RE LED positions
5.2 Gateway status LEDs

LEDs indicating communication status, system status, application status and voltage supply. The position of the LEDs is indicated by position (3) in section *Positions of the LEDs on the gateway* [p. page 14].

![Gateway status LEDs](image)

**Figure 4: Gateway state LEDs**

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR NS</td>
<td>(red)/ (green)</td>
<td>LED communication status Real-Time-Ethernet. Name and function depends on used RTE protocol: PROFINET IO Device = ERR (Bus failure) EtherNet/IP Adapter = NS (Network status) See section See section LEDs of the PROFINET IO Device interface [p. page 16] and section LEDs of the EtherNet/IP Adapter interface [p. page 17].</td>
</tr>
<tr>
<td>RUN MS</td>
<td>(red)/ (green)</td>
<td>LED communication status Real-Time-Ethernet. Name and function depends on used RTE protocol: PROFINET IO Device = RUN (System failure) EtherNet/IP Adapter = MS (Module status) See section LEDs of the PROFINET IO Device interface [p. page 16] and section LEDs of the EtherNet/IP Adapter interface [p. page 17].</td>
</tr>
<tr>
<td>APL</td>
<td>(yellow)</td>
<td>Application status</td>
</tr>
<tr>
<td>SYS</td>
<td>(yellow)/ (green)</td>
<td>System status</td>
</tr>
<tr>
<td>LED1</td>
<td>(yellow)</td>
<td>GPIO12: can be programmed, currently not used.</td>
</tr>
<tr>
<td>LED2</td>
<td>(yellow)</td>
<td>GPIO13: can be programmed, currently not used.</td>
</tr>
<tr>
<td>ACT</td>
<td>(green)</td>
<td>Activity</td>
</tr>
<tr>
<td>POW</td>
<td>(green)</td>
<td>Voltage supply is OK</td>
</tr>
</tbody>
</table>

**Table 4: 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* [p. page 14].

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACT / RX/TX</td>
<td>LED yellow</td>
<td>Flickering (load dependent)</td>
<td>The device sends/receives frames</td>
</tr>
<tr>
<td>Position in the device drawing (4)</td>
<td>(yellow)</td>
<td>off</td>
<td>The device does not send/receive frames.</td>
</tr>
<tr>
<td>LINK</td>
<td>LED green</td>
<td>On</td>
<td>100 MBit MBit network connection</td>
</tr>
<tr>
<td>Position in the device drawing (5)</td>
<td>(green)</td>
<td>off</td>
<td>10 MBit or no network connection</td>
</tr>
</tbody>
</table>

**Table 5: LEDs LAN interface**
## 5.4 LEDs of the PROFINET IO Device interface

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUN (System Failure)</td>
<td>Duo-LED red/green</td>
<td>⬿ (off) Off</td>
<td>No error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (red) Flasing (1 Hz, 3 s)</td>
<td>DCP signal service is initiated via the bus.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (red) On</td>
<td>Watchdog timeout; channel, generic or extended diagnosis present; system error.</td>
</tr>
<tr>
<td>ERR (Bus Failure)</td>
<td>Duo-LED red/green</td>
<td>⬿ (off) Off</td>
<td>No error</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (red) Flasing (2 Hz)</td>
<td>No data exchange</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (red) On</td>
<td>No configuration or low speed physical link or no physical link</td>
</tr>
<tr>
<td>LINK</td>
<td>LED green</td>
<td>⬤ (green) On</td>
<td>The device is linked to the Ethernet.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (off) Off</td>
<td>The device has no link to the Ethernet.</td>
</tr>
<tr>
<td>RX/TX</td>
<td>LED yellow</td>
<td>⬤ (yellow) Flickering (load dependent)</td>
<td>The device sends/receives Ethernet frames.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>⬤ (off) Off</td>
<td>The device does not send/receive Ethernet frames.</td>
</tr>
</tbody>
</table>

### Table 6: LED states for the PROFINET IO-Device protocol

<table>
<thead>
<tr>
<th>LED state</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flashing (1 Hz, 3 s)</td>
<td>The indicator turns on and off for 3 seconds with a frequency of 1 Hz: &quot;on&quot; for 500 ms, followed by &quot;off&quot; for 500 ms.</td>
</tr>
<tr>
<td>Flashing (2 Hz)</td>
<td>The indicator turns on and off with a frequency of 2 Hz: &quot;on&quot; for 250 ms, followed by &quot;off&quot; for 250 ms.</td>
</tr>
<tr>
<td>Flickering (load dependent)</td>
<td>The indicator turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: &quot;on&quot; for approximately 50 ms, followed by &quot;off&quot; for 50 ms. The indicator turns on and off in irregular intervals to indicate low Ethernet activity.</td>
</tr>
</tbody>
</table>

### Table 7: LED state definitions for the PROFINET IO-Device protocol
### 5.5 LEDs of the EtherNet/IP Adapter interface

<table>
<thead>
<tr>
<th>LED</th>
<th>Color</th>
<th>State</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MS</strong> (module status)</td>
<td>Duo LED red/green</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position in the device drawing: (2)</td>
<td>(green) On</td>
<td><strong>Device operational</strong>: The device is operating correctly.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(green) Flashing (1 Hz)</td>
<td><strong>Standby</strong>: The device has not been configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(green/red/green)</td>
<td><strong>Self-test</strong>: The device is performing its power-up testing.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flashing green/red/green</td>
<td></td>
<td>The module status indicator test sequence occurs before the network status indicator test sequence, according to the following sequence:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Network status LED off.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Module status LED turns green for approximately 250 ms, turns red for approximately 250 ms, and again turns green (and holds that state until the power-up test has completed).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Network status LED turns green for approximately 250 ms, turns red for approximately 250 ms, and then turns off (and holds that state until the power-up test has completed).</td>
</tr>
<tr>
<td></td>
<td>(red) Flashing (1 Hz)</td>
<td><strong>Major recoverable fault</strong>: The device has detected a major recoverable fault. E.g., an incorrect or inconsistent configuration can be considered a major recoverable fault.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(red) On</td>
<td><strong>Major unrecoverable fault</strong>: The device has detected a major unrecoverable fault.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(off) Off</td>
<td><strong>No power</strong>: The device is powered off.</td>
<td></td>
</tr>
<tr>
<td><strong>NS</strong> (Network status)</td>
<td>Duo LED red/green</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position in the device drawing: (1)</td>
<td>(green) On</td>
<td><strong>Connected</strong>: An IP address is configured, at least one CIP connection (any transport class) is established, and an Exclusive Owner connection has not timed out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(green) Flashing (1 Hz)</td>
<td><strong>No connections</strong>: An IP address is configured, but no CIP connections are established, and an Exclusive Owner connection has not timed out.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(green/red/off)</td>
<td><strong>Self-test</strong>: The device is performing its power-up testing. Refer to description for module status LED self-test.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Flashing green/red/off</td>
<td></td>
<td><strong>Connection timeout</strong>: An IP address is configured, and an Exclusive Owner connection for which this device is the target has timed out. The network status indicator returns to steady green only when all timed out Exclusive Owner connections are reestablished.</td>
</tr>
<tr>
<td></td>
<td>(red) Flashing (1 Hz)</td>
<td></td>
<td><strong>Duplicate IP</strong>: The device has detected that its IP address is already in use.</td>
</tr>
<tr>
<td></td>
<td>(red) On</td>
<td><strong>Not powered, no IP address</strong>: The device does not have an IP address (or is powered off).</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(off) (Off)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LINK</strong></td>
<td>LED green</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CH0 (6), CH1 (7)</td>
<td>(green) On</td>
<td>The device is linked to the Ethernet.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(off) Off</td>
<td>The device has no link to the Ethernet.</td>
<td></td>
</tr>
<tr>
<td><strong>ACT</strong></td>
<td>LED yellow</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CH0 (8), CH1 (9)</td>
<td>(yellow) Flickering (load dependent)</td>
<td>The device sends/receives Ethernet frames.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(off) Off</td>
<td>The device does not send/receive Ethernet frames.</td>
<td></td>
</tr>
</tbody>
</table>

*Table 8: LED states for the EtherNet/IP Adapter protocol*
<table>
<thead>
<tr>
<th>LED state</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flashing (1 Hz)</td>
<td>The indicator turns on and off with a frequency of 1 Hz: “on” for 500 ms, followed by “off” for 500 ms.</td>
</tr>
<tr>
<td>Flashing green/red/ green</td>
<td>The MS LED indicator turns on green on for 250 ms, then red on for 250 ms, then green on (until the test is completed).</td>
</tr>
<tr>
<td>Flashing green/red/off</td>
<td>The NS LED indicator turns on green on for 250 ms, then red on for 250 ms, then off (until the test is completed).</td>
</tr>
<tr>
<td>Flickering (load dependant)</td>
<td>The indicator turns on and off with a frequency of approximately 10 Hz to indicate high Ethernet activity: on for approximately 50 ms, followed by off for 50 ms. The indicator turns on and off in irregular intervals to indicate low Ethernet activity</td>
</tr>
</tbody>
</table>

Table 9: LED state definitions for the EtherNet/IP Adapter protocol
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.

![Default settings of the Ethernet network connectors](image)

**Figure 5: Default settings of the Ethernet network connectors**

**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 (8) in Positions of the interfaces [page 10]) 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 20] 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 20])
2. by access via the Windows network (see section Access to the Edge Gateway in the Windows network environment [page 21]),
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 6: Device label: Hostname](image)

**Establishing a connection with the host name**

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

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

- The Edge Gateway Manager opens.

You can now use the Edge Gateway manager to configure the device. For this purpose, read section *Edge Gateway Manager web page* [page 23].
6.2.2 Access to the Edge Gateway in the Windows network environment

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

- To display all devices in the network, click on **Network** in the Windows Explorer.
- You will find the Edge Gateway under **Other Devices**:

  ![Edge Gateway Icon](image1)

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

  ![Edge Gateway Icon](image2)

- 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 23].
7 Edge Gateway Manager

7.1 Calling the Edge Gateway Manager

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

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

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

---

**Note:**

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

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Control Panel icon" /></td>
<td>Opens the control panel of the Edge Gateway. The control panel configures the Edge Gateway and displays information on the system. Section <em>Control Panel</em> [page 25] describes the possibilities of configuration as well as the displayed information on the system.</td>
</tr>
<tr>
<td><img src="image" alt="Node-RED icon" /></td>
<td>Opens the wiring editor Node-RED. Section <em>Node-RED - The wiring editor</em> [page 83] describes how to create applications for the Edge Gateway.</td>
</tr>
<tr>
<td><img src="image" alt="Node-RED Dashboard icon" /></td>
<td>Opens the Node-RED Dashboard (graphical user interface).</td>
</tr>
<tr>
<td><img src="image" alt="netIOT Edge Server icon" /></td>
<td>Opens the Edge Server Control Center. See section <em>Edge Server</em> [page 203].</td>
</tr>
<tr>
<td><img src="image" alt="Docker Management icon" /></td>
<td>Opens the Docker management. See section <em>Isolated application execution with Docker</em> [page 215].</td>
</tr>
<tr>
<td><img src="image" alt="Documentation icon" /></td>
<td>Opens the Edge Gateway documentation stored in the device.</td>
</tr>
<tr>
<td><img src="image" alt="Device Information Portal icon" /></td>
<td>Opens the homepage of the Device Information Portal in the Internet. Requires a connection to the Internet.</td>
</tr>
<tr>
<td>Icon</td>
<td>Function</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>netIOT Platform Icon</td>
<td>Opens the homepage of the netIOT platform in the Internet. Requires a connection to the Internet.</td>
</tr>
<tr>
<td>Hilscher Homepage Icon</td>
<td>Opens the Hilscher homepage in the Internet. Requires a connection to the Internet.</td>
</tr>
</tbody>
</table>

*Table 10: Starting applications with the Edge Gateway Manager*
8 Control Panel

8.1 Opening the control panel

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

- Click the tile **Control Panel**.

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

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

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

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

![Figure 8: Edge Gateway Manager - Setting the administrator password](image)

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.

<table>
<thead>
<tr>
<th>Weak password</th>
<th>Mediocre password</th>
<th>Strong password</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Weak password" /></td>
<td><img src="image" alt="Mediocre password" /></td>
<td><img src="image" alt="Strong password" /></td>
</tr>
</tbody>
</table>
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 UPDATING AND INSTALLING OWN SECURITY CERTIFICATES).
8.1.2.1 Connection without certificate with Microsoft Internet Explorer

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

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

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

*Figure 9: 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:

![Your connection is not secure](image)

*Figure 10: 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**.

![Your connection is not secure](image)

*Figure 11: 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 12: Firefox dialog box: Adding exceptional safety rule

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

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

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

**Figure 13: Security error message of Google Chrome (1)**

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

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

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

**Figure 14: Security error message of Google Chrome (2)**

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

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

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

<table>
<thead>
<tr>
<th>Menu</th>
<th>Description</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>System &gt; Info Center</td>
<td>Displaying the system information, monitoring of the processor core temperature, and a system monitor for the usage of CPU, main memory, and SSD.</td>
<td>Displaying system information [† page 33]</td>
</tr>
<tr>
<td>System &gt; License Manager</td>
<td>Display of activated licenses, upload and download of the license file.</td>
<td>License Manager [† page 35]</td>
</tr>
<tr>
<td>System &gt; Syslog</td>
<td>Displaying the system log files.</td>
<td>Displaying the system log files [† page 38]</td>
</tr>
<tr>
<td>System &gt; Time</td>
<td>Settings of system time and time synchronization.</td>
<td>Setting the system time [† page 39]</td>
</tr>
<tr>
<td>System &gt; Port Settings</td>
<td>Port configuration for HTTP/HTTPS communication.</td>
<td>Configure ports for HTTP/HTTPS communication [† page 42]</td>
</tr>
<tr>
<td>System &gt; Backup and Restore</td>
<td>Backup and recovery of the files of the Linux operating system of the Edge Gateway.</td>
<td>Backup and restore [† page 46]</td>
</tr>
<tr>
<td>System &gt; Reboot</td>
<td>Rebooting the Linux operating system of the Edge Gateway</td>
<td>Rebooting the system [† page 53]</td>
</tr>
<tr>
<td>System &gt; Shutdown</td>
<td>Shutting down the Linux operating system of the Edge Gateway</td>
<td>System shutdown [† page 54]</td>
</tr>
<tr>
<td>Package Manager &gt; Packages</td>
<td>Managing the packages of the Linux-based operating system of the Edge Gateway.</td>
<td>Managing packets [† page 54]</td>
</tr>
<tr>
<td>Network &gt; LAN</td>
<td>Configuring the Ethernet interfaces to the IT network and OT network (fieldbus).</td>
<td>Configuring Ethernet communication (LAN) [† page 55]</td>
</tr>
<tr>
<td>Network &gt; Wi-Fi</td>
<td>Configuring the Wi-Fi communication</td>
<td>Configuring wireless communication (Wi-Fi) [† page 58]</td>
</tr>
<tr>
<td>Network &gt; Field</td>
<td>Configuring the operating mode of the fieldbus interface (Real-Time Ethernet).</td>
<td>Field [† page 63]</td>
</tr>
<tr>
<td>Network &gt; Routes</td>
<td>Configuration of interfaces or connections for certain IP destination addresses.</td>
<td>Configuring IP Routes [† page 64]</td>
</tr>
<tr>
<td>Network &gt; Firewall</td>
<td>Firewall configuration for each interface or connection.</td>
<td>Configuring Firewall [† page 68]</td>
</tr>
<tr>
<td>Network &gt; Hostname</td>
<td>Displaying and configuring the host name identifying the Edge Gateway in the network.</td>
<td>Hostname [† page 70]</td>
</tr>
<tr>
<td>Services &gt; Service List</td>
<td>Displaying, starting, and stopping the services of the Edge Gateway.</td>
<td>Starting, stopping and configuring services [† page 71]</td>
</tr>
<tr>
<td>User Management &gt; Roles</td>
<td>Displaying and configuring the permissions for user roles.</td>
<td>Managing user roles [† page 75]</td>
</tr>
<tr>
<td>User Management &gt; Accounts</td>
<td>Displaying user accounts and assigning user roles.</td>
<td>Managing user accounts [† page 77]</td>
</tr>
<tr>
<td>Security &gt; Public Key Infrastructure</td>
<td>Store and administer certificates and key files within the Public Key Infrastructure</td>
<td>Public Key Infrastructure [† page 78]</td>
</tr>
<tr>
<td>Help &gt; Info</td>
<td>Displaying current software version.</td>
<td>Help [† page 81]</td>
</tr>
<tr>
<td>Session &gt; User Profile</td>
<td>Displaying the permissions of the user.</td>
<td>User profile [† page 81]</td>
</tr>
<tr>
<td>Session &gt; Logout</td>
<td>Logout</td>
<td>Logout [† page 82]</td>
</tr>
</tbody>
</table>

Table 11: 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.

The Info Center displays the following information:

<table>
<thead>
<tr>
<th>System info</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware ident.</td>
<td>Serial number of the Edge Gateway</td>
</tr>
<tr>
<td>Model name</td>
<td>Model designation of the Edge Gateway (NIOT-E-TPI51-EN-RE)</td>
</tr>
<tr>
<td>Firmware version</td>
<td>Complete version designation of the firmware stored in the Edge Gateway</td>
</tr>
<tr>
<td>System time</td>
<td>Synchronization status of the internal clock of the Edge Gateway. When the clock is synchronized via the network, the IP address and the name of the time server used for synchronization will be displayed. The user has to configure the time zone.</td>
</tr>
<tr>
<td>Processor name</td>
<td>Name of the microprocessor (CPU) installed in the Edge Gateway.</td>
</tr>
</tbody>
</table>

*Table 12: Info Center: Area System info*
### Monitoring

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

*Table 13: Info Center: Area Monitoring*

### Temperature

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

*Table 14: Info Center: Area Temperature*

If the data of the area **Monitoring** cannot be read, this is grayed out.
8.3.2 License Manager

Open this page with System > License Manager.

The functionality of an Edge Gateway can be extended. The use of particular functions requires a license. On this page you can see which licenses are present in the device and you can transfer a license file into the device.

8.3.2.1 Which licenses are present in the device?

In order to display the licenses contained in the Edge Gateway, use the License Manager. You can open it as follows:

- Open the Control Panel.
- Select System>License Manager.

The window of the License Manager opens:

![License Manager](image)

Figure 17: License Manager with license for the passive mode of operation

The table License enabled Software Packages displays the currently available licenses, in the example a license for the passive mode of operation of the Edge Gateways is available.

Open Details window in the License Manager

To open the Details window:

- Click at the info button on the left edge of the line (within column Details).
The Details window opens:

![Details Window]

Figure 18: License information in window Details

For each license, it displays the license type (Column Type), a brief description (Column Description) and the expiration date (Column Expires). An expiration date will be displayed only, if the license has a runtime limit.

8.3.2.2 How to order and receive a license

The following instruction explains how to order a license for your Edge Gateway to be used in passive mode of operation and receive a license file.

If you order device and license together or after ordering the license, you receive a delivery note. After receiving the delivery note order the license file from Hilscher by e-mail. Specify the following information in your e-mail:

1. The denomination of the desired license
2. The number of your delivery note (for reference)
3. The LAN MAC address of your device (to be taken from the device label)
4. The e-mail address, to which the license download link shall be sent to.

Specify the following as the subject of your e-mail:

Request for a netIOT Licence

- Send the e-mail to Hilscher: vertrieb@hilscher.com
- Hilscher creates an individual license file for your Edge Gateway according to the information supplied by you.
- Hilscher sends this file back to you as an attachment within the answer e-mail. Consequently, this license file has to be transferred into the Edge Gateway as described in section How to transfer a license into the device? [page 37].
8.3.2.3  How to transfer a license into the device?

Load the individual license file received from Hilscher from your PC into the Edge Gateway. Do the upload as follows:

- Open the Control Panel in a web browser.
- Select System > License Manager.
- Click on Upload License.
- A file selection dialog opens.
- Select the license file. This file has the file extension *.LIC.
- Click on OK.
- The license file is transferred into the Edge Gateway. If the transfer is successful, the following message is displayed:

![Restart Now dialog]

*Figure 19: Message after the transfer of the license file into the Edge Gateway*

- To activate the license, a restart of the Edge Gateways is necessary.
- Click on OK.
- The license is installed now, but becomes active after the next restart of the Edge Gateways.
- For a restart, select System > Reboot.
- The license is activated.
8.3.3 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.

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.

**8.3.3.1 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), meanwhile it has been reworked and substituted by [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:

\[
\text{Priority} = 8 \times \text{Facility} + \text{Severity}
\]

The priority can be calculated from two numeric values:

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

*Table 15: Numeric coding of facility value in priority PRI*
The severity is coded according to the following table:

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

Table 16: Numeric coding of severity value in priority (PRI)

**VERSION**

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

**ISOTIMESTAMP**

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

Example

07/06/2018 15:59:41

**HOSTNAME**

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

**APPLICATION**

This part of the message line contains the name of the device or application originally generating the message. The length of APPLICATION is limited to 48 characters.

**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 name=value.

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:

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

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

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

Table 17: Assignment of parts of message line

8.3.3.2 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.
8.3.4 Setting the system time

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

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

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

You can set the system time in two ways:

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

*Table 18: Setting the system time*

![Time configuration page](image)

*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.

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.

8.3.5 Configure ports for HTTP/HTTPS communication

Open this page with System > Port Settings.

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

By default, the Edge Gateway Manager uses port 80 for its HTTP communication and port 443 for its HTTPS communication. In case of the ports being used otherwise, you can configure the Edge Gateway to use other ports. This situation applies, for instance, when using Docker (see Isolated application execution with Docker [page 215]) , if Docker containers are designed to serve HTTP and HTTPS requests only at the above mentioned standard ports.

![Port settings](image)

Figure 22: Port settings

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

Table 19: Default ports
Setting port address for HTTP
- Enter the port address for the communication of the Edge Gateway Manager over HTTP in input field **HTTP Port**.
- Store the port address as described subsequently. If a red error message box with the text *http port is not free* appears, the port is already used. In this case select another port.

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

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

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

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

Open this page by **System > Backup and Restore**.

You have to login as Administrator to use this function.

This page offers the possibility to store the complete system files of the Linux operating system of your Edge Gateway onto an external mass storage device and to restore it from there, if necessary.

**Backup**

Observe the following information:

- The duration of the backup depends on the quantity of data.
- A running backup cannot be interrupted.
- The backup can deteriorate the performance of the Edge Gateway.
- Save the backup on an external data carrier because any existing backup will be overwritten irrevocably without prior notice.

In order to create a backup of your system, proceed as follows:

> Select **System > Backup and Restore** in the control panel.

> The following screen is displayed:

![Figure 23: Backup and recovery](image)

> Click at **Create local backup**.
The following warning message is issued:

![Warning message]

Figure 24: Warning message

To improve the safety you can optionally define a password within input field **Password**. If a password has been specified, that password must be entered at each attempt to access the created backup file.

Furthermore, this warning message explains the above mentioned consequences of starting the backup process such as time expense, increased system load and missing possibility of abortion.

- In order to start the backup process, click at **Yes**.

- The following screen indicates the start of the backup process by the text **Backup in progress**:

![Backup in progress]

Figure 25: Backup in progress

- If the backup process has successfully been finished, the formerly grayed out button **Download local backup** is activated and the backup file is offered for possible download. This means, the backup of system files has been completed.
Recovery from internal backup

Choose this option to restore the system using the stored data, if already an internal backup has been performed within your device.

Take care of the following consequences of system recovery:

- that the former system is fully replaced and overwritten by the system stored in the backup file.
- that the system is stopped.
- that a new start of the system is initiated.
- that this process can last for a significant amount of time and cannot be interrupted.
- that you **must not interrupt power supply of the Edge Gateway** in any case.

In order to restore your system from a previous internal backup, proceed as follows.

- Select **System>Backup and Restore** within the Control Panel.
- The following screen appears:

![Backup and recovery](image)

*Figure 26: Backup and recovery*

- Click at **Restore from backup**.
- The following recovery dialog is displayed:

![Restore from backup](image)

*Figure 27: Recovery dialog*
If there is already an internal backup present in the system, you will notice that the button **Restore** is activated.

**Note:**
If a password has been specified at creation of the backup file to be restored, that password must be entered in input field **Password**!

- Click at **Restore**.
- The following security query is displayed:

![Security query prior to system recovery from internal backup file](image)

You are informed about the above mentioned consequences of system recovery.

- If you want to proceed taking into account these consequences, then click at **Yes**.
- The system on your device is restored from the system files stored within the internal backup. In any way, do not interrupt the power supply of the Edge Gateway during system recovery!
Recovery from external backup

Choose this option to restore the system using the stored data, if already an internal backup has been performed within your device and you have downloaded this backup to an external storage medium or device.

Take care of the following consequences of system recovery:

- that the former system is overwritten and fully replaced by the system stored in the backup file.
- that a new start of the system is initiated.
- that this process can last for a significant amount of time and cannot be interrupted.
- that you **must not interrupt power supply** of the Edge Gateway in any case.

In order to restore your system from a previous external backup (i.e. download of an internal backup), proceed as follows.

- Select **System>Backup and Restore** within the Control Panel.

The following screen appears:

![Backup and recovery](image-url)

*Figure 29: Backup and recovery*

- Click at **Restore from backup**.
The following recovery dialog appears:

![Recovery dialog (external source)](image)

**Note:**
If a password has been specified at creation of the backup file to be restored, that password must be entered in input field **Password**.

- Click at **Explorer**.
- A file selection dialog appears.
- Select the image file with your stored system (file extension is *.img*).
- The following message dialog is displayed:

![Message prior to starting recovery from external backup](image)

- You are informed about the above mentioned consequences of system recovery.
- If you want to proceed taking into account these consequences, then click at **Yes**.
- The selected file is checked for correctness. If the file is no image file, does not contain a backup or is defective in any other way, an error message is displayed. Otherwise your system is recovered from external backup. In any way, do not interrupt the power supply of the Edge Gateway during system recovery!
Delete local backup

If you want to delete a locally present internal backup, you can perform this as follows:

- Select menu entry **System>Backup and Restore** within the Control Panel.
- The following screen appears:

![Backup and restore when backup file is present](image)

*Figure 32: Backup and restore when backup file is present*

- Click at **Delete local backup**.
- The following safety query indicates the danger of possible data loss at deleting the backup, if it has not externally been saved via the download function.

![Safety query before deletion of local backup](image)

*Figure 33: Safety query before deletion of local backup*

- If you are still sure, that you really intend to delete the local backup, click at **Yes**.
- The local backup is internally deleted. Right of **Local backup** the text **No backup** is displayed now instead the name of the former backup.
Downloading a local backup

To download an existing local backup (image file) from the Edge Gateway to an external data carrier, proceed as follows:

- Select **System > Backup and Restore** in the control panel.
- The following screen will be displayed:

![Backup and Restore](image)

*Figure 34: Backup and Restore*

- Click **Download local backup**.
- Select a storage location.
- The download of your backup will be started and the backup will be stored on the external data carrier.

8.3.7 Rebooting the system

You have to login as Administrator to use this function.

To reboot the system:

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

![Warning](image)

*Figure 35: 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.
8.3.8 System shutdown

You have to login as Administrator to use this function.

In order to shut down the system:

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

![Warning](Figure 36: Warning for consequences of shutdown)

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

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

8.4 Packet management

8.4.1 Managing packets

Open this page with Package Manager > Packages.

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

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

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

**Note:**
You can install packages signed by Hilscher only!

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

8.5.1 Configuring Ethernet communication (LAN)

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

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

On this page you configure the Ethernet interfaces *eth0* (on the side of the cloud) and *cifx0* (on the side of the fieldbus).

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

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

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

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

![Figure 37: Default LAN-configuration](image-url)
<table>
<thead>
<tr>
<th>Column</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>-</td>
<td>displays the name of the LAN interface, e.g. <code>eth0</code>.</td>
</tr>
<tr>
<td>MAC address</td>
<td>-</td>
<td>displays the MAC address of the LAN interface.</td>
</tr>
<tr>
<td>Settings</td>
<td>Obtain an IP address automatically</td>
<td>Setting required so that the Edge Gateway automatically obtains the IP-address parameters from a DHCP server.</td>
</tr>
<tr>
<td></td>
<td>Use the following IP address</td>
<td>Setting required so that the user can enter the IP-address parameters manually. In addition, always enter the subnet mask and the Gateway address.</td>
</tr>
<tr>
<td></td>
<td>IP address, Subnet mask, Gateway</td>
<td>Automatically: Display of the IP-address parameters received from the DHCP server. Manually: Input fields for the IP-address parameters to be entered by the user.</td>
</tr>
<tr>
<td></td>
<td>Receive DNS address from DHCP server</td>
<td>✔️ DNS addresses (automatically) received from DHCP server. □ DNS addresses manually entered by the user.</td>
</tr>
<tr>
<td></td>
<td>DNS server 1, DNS server 2</td>
<td>Automatically: Display of the DNS addresses received from the DHCP server. Manually: Input fields for the DNS addresses to be entered by the user.</td>
</tr>
<tr>
<td>DHCP server settings</td>
<td>Enable</td>
<td>✔️ At this interface, the Edge Gateway provides a DHCP server. Prerequisite: The option „Use the following IP address“ is set. <strong>Note:</strong> In this subnetwork, no other DHCP server must be available. □ At this interface, the DHCP server is deactivated.</td>
</tr>
<tr>
<td></td>
<td>Start IP address, End IP address, Gateway, Subnet mask</td>
<td>Parameters for the integrated DHCP server of the Edge Gateway.</td>
</tr>
</tbody>
</table>

*Table 20: Table LAN: Description of the columns and elements*

To save your changes permanently, click **Save changes**.
Activating the Ethernet interface cifx0

1. Selecting the operating mode and firmware
   - Open the Fieldbus page with Network > Field.
   - The Fieldbus page is displayed.
   - Set the operating mode to Active.
   - Click Change mode and then Yes.
   - Under Firmware, select PROFINET IO Device or EtherNet/IP Adapter.
   - If you have changed the selection under Firmware, click Change mode to adopt your change and then click Yes.

2. Starting the Node-RED service.
   - Open the Service page with Services > Service List.
   - The Service page is displayed.
   - If the Node-RED service is in the state Stop (yellow), mark the service Node-RED.
   - Set the Autostart to enabled so that the Node-RED service will also be started with the next start of the device.
   - Click Apply and then Yes.
   - Under Operating status, click Start and then Yes.
   - The Node-RED service has been started and is displayed green.

3. Displaying the Ethernet interface cifx0
   - Open the LAN page with Network > LAN.
   - If the Node-RED-service has been started only a moment before, the Ethernet interface cifx0 is not displayed yet. The starting procedure may take up to 1 minute. To display cifx0, click Refresh.
   - The Ethernet interface cifx0 is activated and can be configured now.

Figure 38: LAN configuration(cifX0 activated)
8.5.2 Configuring wireless communication (Wi-Fi)

Open this page with Network > Wi-Fi.

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

Access onto Wi-Fi (wireless network)

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

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

Figure 39: Wi-Fi (default setting)

Wi-Fi modes of operation

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

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

Table 21: Wi-Fi modes of operation in selection list Mode

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

Table 22: Wi-Fi
Changing the operating mode:

You can change the operating mode via the Mode list.

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

Operating mode Access point

![Wi-Fi Settings](image)

Figure 41: Wi-Fi operating mode: Access point
The following table describes the parameters of the operating mode Access point.

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

*Table 23: Parameters of the operating mode Access point*
Operating mode: Client

The following table describes the parameters of the operating mode *Client*.

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

For each found client, the following data is shown in a separate column of the table:
- SSID (Service Set Identifier)
- MAC Address
- Quality (of radio signal)
- Wi-Fi protected access

**Scanning for a WLAN client**

- Click **Scan**.
- If a WLAN client is found, its data will be displayed in a line of the table **Client**.

**Establishing a connection to a WLAN client found**

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

**Delete stored connection**

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

**Saving the Wi-Fi settings**

To save the Wi-Fi settings, you need the access right 'Write' for the Wi-Fi page.

- Click **Save changes**.
- A security request box appears:
  - Click at **OK**.
- The Wi-Fi settings are saved.
8.5.3 Field

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

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

**Access to Field**

On this page you configure the operating mode of the fieldbus interface (Real-Time Ethernet). The fieldbus interface is deactivated when delivered (factory setting).

<table>
<thead>
<tr>
<th>Operating mode</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Active**     | In the operating mode **Active**, the device can send and receive data on the fieldbus interface. **Note:** The operating mode **Active** is required for the typical operation of the Edge Gateway. In this operating mode, select a firmware: PROFINET I/O Device or EtherNet/IP Adapter. **Note:** Do not use the PROFIBUS DP Slave firmware. In Node-RED use  
- the fieldbus input node to receive data from the fieldbus (see section **Example 4: Fieldbus input node** [page 144]) and  
- the fieldbus output node to send data to the fieldbus (see section **Example 5: Fieldbus output node** [page 152]). |
| **Inactive**   | The interface is deactivated. |

*Table 25: Operating mode fieldbus interface*
8.5.4 Configuring IP Routes

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

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

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

![Figure 43: Routes](image-url)
Current connection configuration

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection</strong></td>
<td>Physical or virtual interface</td>
</tr>
<tr>
<td>cifx0</td>
<td>Ethernet-LAN connection of the Real-Time Ethernet interface (Fieldbus). You can configure the IP address of cifx0 under <strong>Network &gt; LAN</strong> (you must first enable the cifx0 interface under <strong>Network &gt; Field</strong>).</td>
</tr>
<tr>
<td>eth0</td>
<td>LAN connection of the eth0 Ethernet interface (port 1). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>eth1</td>
<td>LAN connection of the eth1 Ethernet interface (port 2). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>cellular</td>
<td>Cellular communication interface (Modem). The IP address is assigned to the modem on establishment of the connection by the provider. <strong>Note</strong>: The Cellular modem is available only in the NIOT-E-TIJCX-GB-RE4EU variant.</td>
</tr>
<tr>
<td>wifi_client</td>
<td>Wi-Fi interface. You can configure the operating mode (&quot;Access Point&quot; or &quot;Client&quot;) and the IP address for the Wi-Fi interface under <strong>Network &gt; Wi-Fi</strong>. <strong>Note</strong>: The Wi-Fi interface is available only in the NIOT-E-TIJCX-GB-REWF variant.</td>
</tr>
<tr>
<td><strong>IP</strong></td>
<td>IP address of the connection in CIDR notation</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: In case no IP address is displayed although the interface has been activated:</td>
</tr>
<tr>
<td></td>
<td>• In case, the Ethernet interface has no link (then the operating system does not assign an IP address to this interface).</td>
</tr>
<tr>
<td></td>
<td>• In case, the Ethernet interface has a link but the Ethernet interface has not received an IP address from a DHCP server (then the operating system deactivates this interface).</td>
</tr>
<tr>
<td><strong>DHCP</strong></td>
<td>Indicates whether a DHCP service has been set for the connection.</td>
</tr>
</tbody>
</table>

*Table 26: Parameters of Current connection configuration table*
Static routes configuration

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

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

![Defined Routes](image1)

**Figure 44: Defined Routes**

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

Delete

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

**Table 27: Routes parameters**

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

![Create new route](image2)

**Figure 45: Create new route**
In the **Destination** field, overtype the `0.0.0.0/0` default value with your actual destination IP address. Use the CIDR notation.

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.1.1.1</td>
<td>192.168.253.254</td>
<td>1000</td>
</tr>
<tr>
<td>16.2.3.0/16</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>18.2.3.0/24</td>
<td>192.168.253.254</td>
<td>1000</td>
</tr>
</tbody>
</table>

![Figure 46: Define new route](image)

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

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

Click **Save** button.
8.5.5 Configuring Firewall

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

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

On this page, you can set individual firewall parameters for each connection/interface of the Edge Gateway separately.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>Physical or virtual interface</td>
</tr>
<tr>
<td>cfx0</td>
<td>Ethernet-LAN connection of the Real-Time Ethernet interface (fieldbus). You can configure the IP address of cfx0 under <strong>Network &gt; LAN</strong> (you must first enable the cfx0 interface under <strong>Network &gt; Field</strong>).</td>
</tr>
<tr>
<td>eth0</td>
<td>LAN connection of the eth0 Ethernet interface (port 1). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>eth1</td>
<td>LAN connection of the eth1 Ethernet interface (port 2). You can configure the IP address of eth0 under <strong>Network &gt; LAN</strong>.</td>
</tr>
<tr>
<td>cellular</td>
<td>Cellular communication interface (modem). The IP address is assigned to the modem on establishment of the connection by the provider. <strong>Note:</strong> The cellular modem is available only in the NIOT-E-TJJCX-GB-RE\4EU variant.</td>
</tr>
<tr>
<td>wifi_client</td>
<td>Wi-Fi interface. You can configure the operating mode (&quot;Access Point&quot; or &quot;Client&quot;) and the IP address for the Wi-Fi interface under <strong>Network &gt; Wi-Fi</strong>. <strong>Note:</strong> The Wi-Fi interface is available only in the NIOT-E-TJJCX-GB-RE\WF variant.</td>
</tr>
</tbody>
</table>

**Current firewall zone** | Current firewall settings for the connection/interface. |
**New firewall zone** | Here you can change the firewall setting for the connection/interface by clicking the arrow icon and selecting a new configuration setting from the drop-down list. |
| block | All packets reaching the interface will be dropped. The sender will be notified by an ICMP "unreachable" message. |
| drop | All packets reaching the interface will be "silently" dropped. |
| nat_drop | The source IP address of all outgoing IP packets is replaced by the assigned IP address of the interface. All incoming IP packets will be dropped. |
| nat_trusted | The source IP address of all outgoing IP packets is replaced by the assigned IP address of the interface. Incoming IP packets will be forwarded to the assigned IP address of the interface. |
| trusted | Default. All IP packets will be forwarded transparently (firewall is switched off). |

**Save:** Click this button to save new firewall settings.

---

**Important:**

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

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

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

*Access onto hostname of Edge Gateway*

On this page you configure the host name.

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

The default host name starts with the two letters "NT" followed by the LAN MAC address of the LAN connection port 1 of the Edge Gateway. Example `NT0002A233E559`. The default host name is printed on the label at the bottom of the Edge Gateway. With the host name you can access the Edge Gateway from your PC even without knowing the IP address of the Edge Gateway (also see *Using the web browser to establish a connection with the Edge Gateway* [page 20]).

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 Input field](image)

---

**Input field Hostname**

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

**Saving the host name**

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

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

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

8.6.1 Starting, stopping and configuring services

Open this page with Services > Service List.

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

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

The list of services is displayed at the left edge:

![Service 1]

![Service 2]

*Figure 49: List of default services*

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

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

*Table 29: Operating statuses of the services*

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

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

*Table 30: Operating and display elements*

A service can allow you individual settings.
8.6.1.1 Node-RED service

Deleting the current Node-RED flows

In case, the processing of a flow in the Edge Gateway takes a very long time (e.g. due to an endless loop) you can delete all flows. After deleting the flows there is no chance to restore these flows.

- Click **Delete all**.
- A security question is displayed.
- If you intend to delete all flows, click **Yes**.
- All Node-RED flows are deleted.

8.6.1.2 OPC UA Server for Edge

Figure 50: OPC-UA Server for Edge settings within the Control Panel, page **Network>Field**
The following table describes the parameters of the OPC UA Server for Edge.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Range of values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General communication parameters</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>The port used for communication by OPC UA</td>
<td>Valid port</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 4840</td>
</tr>
<tr>
<td>Server Name</td>
<td>The name of the OPC-UA Server (for the client)</td>
<td>Name consisting of:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a…z, A…Z, 0-9, space</td>
</tr>
<tr>
<td>Global discovery server URL</td>
<td>URL of a Discovery Server within the network to which the Edge Gateway is</td>
<td>Valid URL to a Discovery Server</td>
</tr>
<tr>
<td></td>
<td>connected. If there is a Global Discovery Server in your network, then</td>
<td>within the network.</td>
</tr>
<tr>
<td></td>
<td>specify the URL in Parameter <strong>Global discovery server URL</strong>. Using this</td>
<td></td>
</tr>
<tr>
<td></td>
<td>server, you can then access all OPC UA Servers listed there. If this is not</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the case, use the displayed default address: opc.tcp://127.0.0.1:4840/UAbl</td>
<td></td>
</tr>
<tr>
<td>Limitations</td>
<td>Max Sessions - Maximum number of sessions</td>
<td>1 … 10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td></td>
<td>Max connections per endpoint - Maximum number of connections per endpoint</td>
<td>1 … 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td></td>
<td>Max nodes per read - Maximum number of nodes per read</td>
<td>1 … 100</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td></td>
<td>Max nodes per browse - Maximum number of nodes per browse</td>
<td>1 … 200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 200</td>
</tr>
<tr>
<td>Min sampling interval Edge Server</td>
<td>Minimum sampling interval of the Edge Server, specified in milliseconds</td>
<td>&gt;= 1 000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 1000 [ms]</td>
</tr>
<tr>
<td>Min sampling interval</td>
<td>Minimum sampling interval of the passive fieldbus, specified in milliseconds</td>
<td></td>
</tr>
<tr>
<td>passive fieldbus</td>
<td></td>
<td>&gt;= 200</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: 200 [ms]</td>
</tr>
<tr>
<td><strong>Security settings (Security modes)</strong></td>
<td>At least one of these options must be checked. If multiple options are checked, the OPC UA Client may select a suitable of these options.</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>Unsigned communication without encryption</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Sign</td>
<td>Signed communication without encryption</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Sign &amp; Encrypt</td>
<td>Signed communication with encryption</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td><strong>Security settings (Security policies)</strong></td>
<td>At least one of these options must be checked. If multiple options are checked, the OPC UA Client may select a suitable of these options. For maximum security you should choose the security mode Sign &amp; Encrypt and the security policy Basic256Sha256.</td>
<td></td>
</tr>
<tr>
<td>None</td>
<td>No encryption useful at security mode None und Sign</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Basic128Rsa15</td>
<td>Encryption algorithm Basic128Rsa15, useful at security mode Sign &amp; Encrypt</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Basic256</td>
<td>Encryption algorithm Basic256, useful at security mode Sign &amp; Encrypt</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Basic256Sha256</td>
<td>Encryption algorithm Basic256Sha256, useful at security mode Sign &amp; Encrypt</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td><strong>Security settings (Access method to OPC UA Server)</strong></td>
<td>Anonymous access Anonymous access to the OPC UA Server (not secure)</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Anonymous access</td>
<td>Anonymous access to the OPC UA Server (not secure)</td>
<td>Checked / not checked</td>
</tr>
<tr>
<td>Passive mode of operation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 31: Parameters of the OPC UA Server for Edge

### Authentication in OPC UA

In general, OPC UA uses three methods for authentication.

1. Anonymous access
2. Access via username and password
3. Access via username, password, certificate and private key.

In order to allow anonymous access to the OPC UA Server, check checkbox **Allow anonymous access**. This mode does not provide any security and an OPC UA Client can connect via anonymous login. Otherwise an OPC UA Client can access the Edge Server via username and password.

### Storing the settings for the OPC UA Server for Edge

After you finished making your settings for the OPC UA Server for Edge, you have to store these as follows in order to make them effective.

- Click at **Save all**.
- A message indicates that the configuration of the OPC UA Servers will be changed on the next restart of the OPC UA Server.
- Click at **OK**.
- The following message appears: **OPC UA Server for Edge config settings are successfully saved**. The changes are stored in the Edge Gateway now. However, they will get effective after the next restart of the Edge Gateway.
- Click at **Stop**.
- Wait for some seconds.
- Click at **Start**.
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.

![Figure 51: Page for configuring roles](image)

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* [page 206]) is also a resource.
An access right can be assigned to the following single resources:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Access to resource via menu</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>System &gt; Time</td>
<td>Setting the system time [↑ page 42]</td>
</tr>
<tr>
<td>License management</td>
<td>System &gt; Licenses</td>
<td>License Manager [↑ page 35]</td>
</tr>
<tr>
<td>System log</td>
<td>System &gt; Syslog</td>
<td>Displaying the system log files [↑ page 38]</td>
</tr>
<tr>
<td>Packet management</td>
<td>Package Manager &gt; Packages</td>
<td>Managing packets [↑ page 54]</td>
</tr>
<tr>
<td>Network access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access to LAN (Ethernet network)</td>
<td>Network &gt; LAN</td>
<td>Configuring Ethernet communication (LAN) [↑ page 55]</td>
</tr>
<tr>
<td>Access onto Wi-Fi (wireless network)</td>
<td>Network &gt; Wi-Fi</td>
<td>Configuring wireless communication (Wi-Fi) [↑ page 58]</td>
</tr>
<tr>
<td>Access onto hostname of Edge Gateway</td>
<td>Network &gt; Hostname</td>
<td>Hostname [↑ page 70]</td>
</tr>
<tr>
<td>Access onto Field network (Ethernet network)</td>
<td>Network &gt; Field</td>
<td>Field [↑ page 63]</td>
</tr>
<tr>
<td>Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configure service &quot;XYZ&quot; (depends on installed services)</td>
<td>Services &gt; Service List &gt; Service &quot;XYZ&quot;</td>
<td>Starting, stopping and configuring services [↑ page 71]</td>
</tr>
<tr>
<td>Configure Docker</td>
<td>Services &gt; Service List &gt; Docker</td>
<td>Isolated application execution with Docker [↑ page 215]</td>
</tr>
</tbody>
</table>

Table 32: Access rights onto resources

Each resource may obtain one of the following access rights:

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

Table 33: Access rights to resources
Adding a new role

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

![Add new role dialog box](image)

- Enter a name for the role, e.g. User.
- Click Add.
- The role is added.

Setting the access rights of a role

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

8.7.2 Managing user accounts

Open this page with User Management > Accounts.

On this page you can
- add
- process
- delete user accounts.

![User account page](image)

Figure 52: 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.

Figure 53: Public Key Infrastructure for managing of certificates

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

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

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

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

File selection window for certificates and key files

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

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

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

- On selection of **Service Certificates** a tree structure is displayed.
Certificate Viewer

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 246].

Note:
For more information on the foundations of asymmetric encryption techniques and public key infrastructure, see sections Asymmetric encryption [page 244] and Certificates and keys [page 246].
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.

\[
\text{Info}
\]

Version 1.0200.776

*Figure 56: Info page*

8.10 Session

8.10.1 User profile

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

![User profile page]

*Figure 57: 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.

![Edit user account dialog](image)

Figure 58: 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 Node-RED - The wiring editor

The task of a gateway in the Internet of Things is to establish easy configurable flexible connections between different devices. The netIOT Edge Gateway uses Node-RED for this task, a very flexible visual wiring editor for the Internet of Things.

Node-RED was developed by IBM. It is a web-based graphical tool with an intuitive user interface for wiring nodes for an application-specific data flow. Nodes are wired by means of a mouse with drag and drop.

Node-RED is based on node.js a platform independent runtime environment to develop Web applications with server side java scripting.

This manual explains you how to use Node-RED for configuration and wiring of nodes within the netIOT Edge Gateway.

This manual refers to the following versions:

- Node-RED version 0.19.
- node.js minimal V4.x

Note:
9.1 Modelling IoT flows with nodes

To combine physics and logic, Node-RED models ("flows") and works with ("nodes") which represent objects in the Internet of Things. You can relate these objects to physical interfaces as well as to logic functions.

By means of Drag&Drop the nodes are interactively wired with one another to get flows, as shown in the following figure.

The following basic properties apply to one Node-RED node:

- A node fulfills a specific, defined task.
- A node has entry masks for setting the parameters.
- A node can have inputs and outputs.
- A node can be connected with other nodes via its inputs and outputs.
- A node can modify and overwrite data before passing the data on.
- A node transports data via the msg object in the JSON format.
The msg object always contains the objects .topic and .payload.

- .topic identifies the message.
- .payload contains the payload to be transported.

Node-RED has an ample library with already predefined nodes which are ready for immediate use.

Node-RED categorizes nodes. The following categories of nodes exist, e.g.:

- input
- output
- function
- social
- storage
- analysis
- advanced
- cloud
- modbus
- dashboard

Nodes offer functions, e.g.:

- Web-based communication
- TCP/UDP send/receive
- MQTT publish/subscribe
- Serial send/receive
- Time emitter

9.2 Opening Node-RED

This section describes how to call Node-RED for configuring the flow within the netIOT Edge Gateway.

Prerequisite: To login, you have to know your user name and password.

To open Node-RED, proceed as follows:

- Open the Edge Gateway manager (see Calling the Edge Gateway Manager [page 22])
- In the Edge Gateway manager click on the tile Node-RED.
The Node-RED start screen will be displayed.
- Enter your user name and password.

Click on Login.
- Node-RED asks you whether you want to use the projects function which allows you to store flows in a Git hub repository.
- If needed, you can setup the project function later. Click on Not right now.
- The Node-RED workspace will be displayed.

![Node-RED workspace](image)

**Figure 61: Node-RED workspace**

**Note:**
Remember that the secured HTTPS protocol is used here, not the widely spread HTTP protocol.

If the Node-RED workspace does not open, read the following sections in compliance with the browser used:

*Connection without certificate with Microsoft Internet Explorer [page 28]*
*Connection without certificate with Firefox [page 28]*
*Connection without certificate with Google Chrome [page 30]*
9.3 Graphical user interface

Graphical user interface

The following figure and table describe the elements of the user interface.

![Figure 62: Node-RED user interface](image)

<table>
<thead>
<tr>
<th>Position number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Worksheet which contains one or more flows. This worksheet has the name <strong>Flow 1</strong>.</td>
</tr>
<tr>
<td>(2)</td>
<td>Add worksheet</td>
</tr>
<tr>
<td>(3)</td>
<td>Deploy, to transfer the configuration (flows) into the device</td>
</tr>
<tr>
<td>(4)</td>
<td>Logout</td>
</tr>
<tr>
<td>(5)</td>
<td>Node-RED menu</td>
</tr>
<tr>
<td>(6)</td>
<td>Panel selection list, e.g. debug messages</td>
</tr>
<tr>
<td>(7)</td>
<td>Panel icons</td>
</tr>
<tr>
<td>(8)</td>
<td>Active panel</td>
</tr>
<tr>
<td></td>
<td>Selection of active panel with (6) or (7)</td>
</tr>
<tr>
<td>(9)</td>
<td>Sidebar</td>
</tr>
<tr>
<td></td>
<td>The sidebar can be switched on or off.</td>
</tr>
<tr>
<td>(10)</td>
<td>Zoom</td>
</tr>
<tr>
<td>(11)</td>
<td>Workspace which contains one or more worksheets.</td>
</tr>
<tr>
<td>(12)</td>
<td>Expand or collapse the node library</td>
</tr>
<tr>
<td>(13)</td>
<td>Node library</td>
</tr>
<tr>
<td>(14)</td>
<td>Node category</td>
</tr>
<tr>
<td>(15)</td>
<td>Nodes</td>
</tr>
<tr>
<td>(16)</td>
<td>Node filter</td>
</tr>
</tbody>
</table>

*Table 34: Node-RED user interface*
Nodes

The following figure and table describe the elements of a node.

![Node Diagram](image)

**Figure 63: Node**

<table>
<thead>
<tr>
<th>Position number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Node icon</td>
</tr>
<tr>
<td>(2)</td>
<td>Node name (editable)</td>
</tr>
<tr>
<td>(3)</td>
<td>The red triangle shows that a required parameter is not configured yet.</td>
</tr>
<tr>
<td>(4)</td>
<td>The blue circle shows that this node has been changed but not transmitted yet.</td>
</tr>
<tr>
<td>(5)</td>
<td>Output port (if available)</td>
</tr>
<tr>
<td>(6)</td>
<td>Node status (if available)</td>
</tr>
<tr>
<td>(7)</td>
<td>Input port (if available)</td>
</tr>
</tbody>
</table>

Table 35: Node elements
9.4 Working with Node-RED

In Node-RED you can process data using
1. Input nodes (nodes that read data),
2. Processing nodes and
3. Output nodes (nodes that write data).

You can wire nodes by connecting their input and output ports. By connecting the nodes you create a data flow that is simply called "flow" in the user interface. The flow direction is always fixed: From input node to output node. Insert the nodes in a worksheet, configure these nodes, connect them, and deploy the result to the Edge Gateway.

Procedure (overview)
1. Inserting a node from the library
2. Configuring node parameters:
   A node may require parameters that you can configure in an edit dialog. The fieldbus node is an example for a node which is configured via an edit dialog.
3. Connecting nodes to determine the flow:
   In Node-RED the data flow is realized as „flow“.
4. Using Deploy to activate the flow in the Edge Gateway:
   The flow in the workspace still has to be activated in the Edge Gateway. For this purpose Deploy is used to transmit the flow from the workspace to the Edge Gateway.

Procedure (step by step)
1. Inserting nodes from the library
   - Use the mouse to drag a node from the library and insert the node in the flow.
2. Configuring node parameters
   ➢ Double-click on the node.
   ➢ The edit dialog will be displayed.

3. Connecting nodes to determine the flow
   ➢ Connect the input node with the output node. For this purpose hold down the mouse button and draw a line (wire) from the output port of the node (in the example called „Hello World“-node) to the input port of the other node.

   ➢ Thus, the two nodes are connected by a line (wire) in the workspace, but they are not yet activated in the Edge Gateway.

4. Using Deploy to activate the flow in the Edge Gateway
   ➢ Click on **Deploy**.

   ➢ The flow will be deployed from the workspace to the Edge Gateway and activated.
9.4.1 Using GitHub repository to store flows (projects)

Node-RED offers you the projects function (optional). If you intend to use it, you first have to set it up. Then you can use Node-RED together with Git and can use the following functions:

- save flows in a repository,
- manage different versions of flows (version control), and
- collaborate with other persons on flows.

To setup a new project or to open an existing project, you have to specify or to know the following names:

- User name (for Git)
- Email address
- Project name
- Description for the project (optional)
- Flow file name
- The key, if encryption is used.

Starting from the Node-RED menu, use Projects > New to create a new project in Git and use Projects > Open to open an existing project in Git. To open the project settings, use Projects > Project Settings to display or change them and to use the version control.

**Note:**
For a description of the projects function, see https://nodered.org/docs/user-guide/projects/.
9.4.2 Menu Deploy

The menu Deploy offers further commands to control the deployment of the flow.

![Image of Menu Deploy]

Figure 64: Menu Deploy

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Deploys the entire workspace.</td>
</tr>
<tr>
<td>Modified Flows</td>
<td>Deploys only those flows which contain modified nodes.</td>
</tr>
<tr>
<td>Modified Nodes</td>
<td>Deploys only nodes that have been modified.</td>
</tr>
</tbody>
</table>

Table 36: Commands of menu Deploy

Procedure

- Click on the white arrow located at the right edge of the red button **Deploy**.
- The menu Deploy opens.
- Click on the menu command to be executed.
- The dialog box **Confirm Deploy** is displayed.
The dialog box **Confirm Deploy** is displayed.

A dialog box will indicate incorrectly configured nodes in the workspace, if there are any, and ask whether you really want to execute the deploy procedure.

- Click on **Cancel** to correct any possible errors.
- The flow has not been deployed to the Edge Gateway.

or

- Click on **Confirm deploy** to deploy the flow to the Edge Gateway and activate it.
- Thus, the flow is activated in the Edge Gateway.
9.4.3 Dashboard

Beginning with Version 0.14, Node-RED simply allows to design integrated graphical user interfaces. These graphical user interfaces are called dashboards and designed within the dashboard configuration using some special nodes.

These special nodes contain graphical elements for control and display, which are used for input and output purposes. These are called widgets.

<table>
<thead>
<tr>
<th>Node/Widget</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>button</td>
<td>Adds a button to the user interface</td>
</tr>
<tr>
<td>dropdown</td>
<td>Adds a dropdown list to the user interface</td>
</tr>
<tr>
<td>switch</td>
<td>Adds a switch to the user interface</td>
</tr>
<tr>
<td>slider</td>
<td>Adds a slider to the user interface</td>
</tr>
<tr>
<td>numeric</td>
<td>Adds a slider to the user interface</td>
</tr>
<tr>
<td>text input</td>
<td>Adds a widget for text input to the user interface</td>
</tr>
<tr>
<td>date picker</td>
<td>Adds a widget for date selection to the user interface</td>
</tr>
<tr>
<td>form</td>
<td>Adds a color picker to the user interface</td>
</tr>
<tr>
<td>text</td>
<td>Adds a widget for color selection to the user interface</td>
</tr>
<tr>
<td>gauge</td>
<td>Adds a form to the user interface</td>
</tr>
<tr>
<td>chart</td>
<td>Display of a non-editable text field on the user interface</td>
</tr>
<tr>
<td>notification</td>
<td>Adds a round gauge display to the user interface</td>
</tr>
<tr>
<td>chart</td>
<td>Adds a chart to the user interface (can be configured as line chart, bar chart or pie chart)</td>
</tr>
<tr>
<td>notification</td>
<td>Displays the contents of a message <code>msg.payload</code> as popup notification or as dialog box (Options <em>Ok</em> / <em>Cancel</em> on the user interface)</td>
</tr>
<tr>
<td>audio out</td>
<td>Adds audio output or speech output of text</td>
</tr>
<tr>
<td>ui control</td>
<td>Allows to control the dashboard dynamically</td>
</tr>
<tr>
<td>template</td>
<td>Adds directives or HTML code for further processing</td>
</tr>
</tbody>
</table>

Table 37: Kinds of widgets for use in dashboards

Widgets can be organized in groups. These groups together appear on worksheets which are called tabs.

9.4.3.1 Dashboard configuration (Overview)

The dashboard configuration occurs in register card *Dashboard* of the side bar. In the following the structure of and the functions provided by of the dashboard configuration are explained.

The register card *Dashboard* of the Edge Bar is itself divided into three register cards:

- Layout
- Theme
- Site
These register cards look as follows:

**Register card Layout**

- **Tabs**
  - Tab 1
  - Group 1
  - Gauge
  - Chat
  - Group 1
  - Slider

**Register card Theme**

- **Style**
  - Custom
- **Custom Profile**
  - Untitled Theme 1
- **Base Settings**
  - Colour
- **Page Settings**
  - Title Bar Background
  - Page Background
  - Side Bar Background
- **Group Settings**
  - Group Text
  - Group Border
  - Group Background

**Register card Site**

- **Title**
  - Node-RED Dashboard
- **Options**
  - Show the title bar
  - No swipe between tabs
- **Date Format**
  - DD/MM/YYYY

They consist of the following elements:

<table>
<thead>
<tr>
<th>Number</th>
<th>Area</th>
<th>Register card</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Button &quot;Show current dashboard in the browser within new register card&quot;</td>
<td>Layout, Theme, Site</td>
</tr>
<tr>
<td>(2)</td>
<td>Editable tree structure for creating tabs, groups and widgets. See sections Working with tabs [page 97], Working with groups [page 99] and Working with widgets [page 101].</td>
<td>Layout</td>
</tr>
<tr>
<td>(3)</td>
<td>Area for displaying messages</td>
<td>Layout</td>
</tr>
<tr>
<td>(4)</td>
<td>List field „Menu links“. See section Working with menu links [page 103].</td>
<td>Layout</td>
</tr>
<tr>
<td>(5)</td>
<td>Selection list &quot;Style&quot; - allows the selection of colors for background display (light or dark background or user-defined color display)</td>
<td>Theme</td>
</tr>
<tr>
<td>(6)</td>
<td>Input field „Custom Profile“ - allows to put in a name for a theme - is only displayed, if option „Custom“ has been chosen in selection list &quot;Style&quot;</td>
<td>Theme</td>
</tr>
<tr>
<td>(7)</td>
<td>Color selection field „Base Settings“</td>
<td>Theme</td>
</tr>
<tr>
<td>(8)</td>
<td>Color selection field „Page Settings“ - is only displayed, if option „Custom“ has been chosen in selection list &quot;Style&quot;</td>
<td>Theme</td>
</tr>
</tbody>
</table>
Table 38: Areas of the dashboard configuration

<table>
<thead>
<tr>
<th>Number</th>
<th>Area</th>
<th>Register card</th>
</tr>
</thead>
<tbody>
<tr>
<td>(9)</td>
<td>Color selection field „Group Settings” - is only displayed, if option „Custom“ has been chosen in selection list “Style”</td>
<td>Theme</td>
</tr>
<tr>
<td>(10)</td>
<td>Color selection field „Widget Settings“ - for the selection of text color, base color and background color for widgets - is only displayed, if option „Custom“ has been chosen in selection list “Style”</td>
<td>Theme</td>
</tr>
<tr>
<td>(11)</td>
<td>Input field „Title“ - for specifying the title of the dashboard</td>
<td>Site</td>
</tr>
<tr>
<td>(12)</td>
<td>Selection list „Options“ - showing or hiding the title bar - swiping over tabs</td>
<td>Site</td>
</tr>
<tr>
<td>(13)</td>
<td>Input field „Data Format“ - allows specifying the date format of your choice</td>
<td>Site</td>
</tr>
<tr>
<td>(14)</td>
<td>Input fields „Sizes“ for sizes and distances of widgets</td>
<td>Site</td>
</tr>
</tbody>
</table>

9.4.3.2 Display dashboard

You can visualize the dashboard currently configured in the active Node-RED flow and test it as follows:

- Click at the button right of the input field Title.
- In the browser a new register card is opened, in which the dashboard is displayed graphically.

9.4.3.3 Change title

You can change the title of a dashboard as follows:

- Specify the title of the dashboard in input field Title of register card Site.

![Title]

NodeRED-Test

9.4.3.4 Background

Select the background color (light or dark) of the dashboard as follows:

- In the selection list Style in register card Theme select option „Light(default)“ or „Dark“. The option Custom allows you to adjust additional color settings.
  - The background color is changed. However, the change will get effective at the next deploy operation.
9.4.3.5 Working with tabs

In this section, working with tabs is described, such as creating new tabs, changing tabs and deleting these.

Adding a tab

In this way you can add a tab to the dashboard:

- Click at icon (right of the text "Tabs").
- A new tab is added below the already preset ones.

Editing a tab

In this way, you edit a tab:

- Move your mouse cursor to the tab to be edited (within the tree structure).
- Icons and will become visible.
- Click at the icon (right of the name of the according tab).
- The dialog Edit dashboard tab node is opened.

![Figure 65: Dialog “Edit dashboard tab node”](image)

- Specify the desired name of the tab in field Name.
- If desired, specify the icon type within the field Icon, for instance, Dashboard.
- With field State, you can activate (option Enabled) or deactivate (option Disabled) the icon.
- In field Nav.Menu, you can set whether the tab is visible in the navigation menu (option Visible) or not (option Hidden).
In the dialog **Edit dashboard tab node**, click **Update** to save the settings.

The dialog **Edit dashboard tab node** is closed and the tab is adapted according to your specifications.

### Deleting a tab

So you can delete a tab:

- Click at the icon ![edit](right of the name of the according tab)
- The dialog **Edit dashboard tab node** is opened.

![Edit dashboard tab node](image)

**Figure 66: Dialog "Edit dashboard tab node"**

- Click **Delete** in the dialog **Edit dashboard tab node** to delete the tab.
- The dialog **Edit dashboard tab node** is closed and the tab is removed from the tree structure.
9.4.3.6 Working with groups

In this section, working with groups is described, such as creating new groups and changing and deleting groups.

**Adding a group to a tab**

So you can add a group to the dashboard within a tab:

- Click at the icon (right of the name of the according tab).
- A new group is added below the already present groups. If there is not any group, the new group is directly added below the tab.

**Editing a group**

In this way, you can edit a group of widgets:

- Click at the icon (right of the name of the according group).
- The dialog **Edit dashboard tab node** is opened.

---

**Figure 67: Dialog "Edit dashboard tab node"**

- Specify the desired name of the tab in field **Name**.
- If you want to change the relation of a group to a superordinated tab, you can select another tab from the selection list **Tab**. If you want to relate the group with a tab to be newly created, select entry **Add new ui_tab** at the end of the selection list. Then a new tab is created and the current group is related to this new tab.
- Specify the width of the group in field **Width**.
- You can control via the checkbox **Display Group Name** whether the name of the group as displayed in the field **Name** is displayed on the dashboard, or not.
Click **Update** in the dialog **Edit dashboard group node** to update the settings.

- The dialog **Edit dashboard tab node** is closed and the group is adapted according to your specifications.

### Deleting a group

In this way, you can delete a group (within a tab)

- Click at the icon ![edit](right of the name of the according tab).
- The dialog **Edit dashboard tab node** is opened.

![Edit dashboard group node dialog](image)

**Figure 68:** Dialog "Edit dashboard tab node"

- In order to delete a group, click at **Delete** in dialog **Edit dashboard tab node**.
- The dialog **Edit dashboard tab node** is closed and the group is removed from the tab.
9.4.3.7 Working with widgets

In this section, working with widgets is described, such as creating new widgets, changing widgets and deleting these.

Adding a widget to group

So you can add a widget of your choice to a group:

- Select a node for a widget from the node group dashboard out of the node library, for instance for a line chart, bar chart or pie chart the node for the widget Chart.
- Pull this node onto your worksheet using Drag&Drop.
- Double-click onto this node.
- The edit dialog of the node is opened. Name and contents of the edit dialog depend on the choice of the node. At its upper edge, this contains the three buttons Delete, Cancel und Done.

Note:
Further information can be found in the documentation of Node-RED. You can find it at https://github.com/node-red/node-red-dashboard.

- Configure the widget according to your needs.
- Select the group from the selection list, to which you want to add the widget having just been configured.
- Finish configuration by clicking at Done.
- The widget is stored including its configured settings and it is assigned to the selected group.

Editing a widget

In this way, you edit a widget:

- Click at the icon edit (right of the name of the according widget).
- The edit dialog of the widget to be edited is opened. The name and the contents of this edit dialog strongly depends on the type of the respective widget such as button, dropdown, switch, slider, numeric, textinput, form, colour picker, gauge, chart, audio out, notification, text, template or ui control.

Note:
Further information can be found in the documentation of Node-RED. You can find it at https://github.com/node-red/node-red-dashboard.

- Select the desired settings for your widget.
- Click at Done.
- The edit dialog is closed and the settings of your widget are stored.
Deleting a widget

So you can delete a widget:

- Click at the icon edit (right of the name of the according widget).
  - The edit dialog of the widget to be edited opens.

- Click at Delete.
  - The widget is deleted and removed from the group, to which it belonged previously.
9.4.3.8 Working with menu links

**Adding a link**

So you can add a further link to the dashboard:
- Click at icon (right of the text "Menu links").
- A new link is added at the end of the link list below "Menu links".

**Editing a link**

In this way, you edit a link within the link list:
- Click at the icon (right of the name of the according link).
- The dialog **Edit dashboard tab node** is opened.

![Edit dashboard tab node dialog](image)

*Figure 69: Dialog "Edit link node"*
- Specify the desired name of the tab in field **Name**.
- Specify the link address in the field **Link** (Protocol **http** or **https**).
- Specify in field **Icon**, how the link should be opened (Options **dashboard** or **open_in_browser**)
- Choose whether the link in the browser should be opened within a new tab (Option **New Tab**) or within an iframe (Option **iframe**).

- In order to store, click at **Update** in dialog **Edit link node**.
- The dialog **Edit link node** is closed and the link is adapted according to your specifications.
Deleting a link

So you can delete a link

- Click at the icon (right of the name of the according link).
- The dialog Edit dashboard tab node is opened.

In order to delete a link, click at in dialog Edit link node.
- The dialog Edit link node is closed and the link is removed from the link list.
## 9.5 List of nodes

The following table lists the nodes of the standard scope of delivery.

<table>
<thead>
<tr>
<th>Category</th>
<th>Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>inject</td>
</tr>
<tr>
<td></td>
<td>catch</td>
</tr>
<tr>
<td></td>
<td>status</td>
</tr>
<tr>
<td></td>
<td>link</td>
</tr>
<tr>
<td></td>
<td>mqtt</td>
</tr>
<tr>
<td></td>
<td>http</td>
</tr>
<tr>
<td></td>
<td>websocket</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
</tr>
<tr>
<td></td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>fieldbus</td>
</tr>
<tr>
<td></td>
<td>passive fieldbus</td>
</tr>
<tr>
<td></td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>s7comm</td>
</tr>
<tr>
<td></td>
<td>Watson IoT</td>
</tr>
<tr>
<td></td>
<td>serial</td>
</tr>
<tr>
<td>Output</td>
<td>debug</td>
</tr>
<tr>
<td></td>
<td>link</td>
</tr>
<tr>
<td></td>
<td>mqtt</td>
</tr>
<tr>
<td></td>
<td>http response</td>
</tr>
<tr>
<td></td>
<td>web socket</td>
</tr>
<tr>
<td></td>
<td>tcp</td>
</tr>
<tr>
<td></td>
<td>udp</td>
</tr>
<tr>
<td></td>
<td>fieldbus</td>
</tr>
<tr>
<td></td>
<td>LED</td>
</tr>
<tr>
<td></td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>s7comm</td>
</tr>
<tr>
<td></td>
<td>Watson IoT</td>
</tr>
<tr>
<td></td>
<td>serial</td>
</tr>
<tr>
<td>Category</td>
<td>Node</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Function</td>
<td>function</td>
</tr>
<tr>
<td></td>
<td>template</td>
</tr>
<tr>
<td></td>
<td>delay</td>
</tr>
<tr>
<td></td>
<td>trigger</td>
</tr>
<tr>
<td></td>
<td>comment</td>
</tr>
<tr>
<td></td>
<td>http request</td>
</tr>
<tr>
<td></td>
<td>tcp request</td>
</tr>
<tr>
<td></td>
<td>switch</td>
</tr>
<tr>
<td></td>
<td>change</td>
</tr>
<tr>
<td></td>
<td>range</td>
</tr>
<tr>
<td></td>
<td>split</td>
</tr>
<tr>
<td></td>
<td>join</td>
</tr>
<tr>
<td></td>
<td>sort</td>
</tr>
<tr>
<td></td>
<td>batch</td>
</tr>
<tr>
<td></td>
<td>csv</td>
</tr>
<tr>
<td></td>
<td>html</td>
</tr>
<tr>
<td></td>
<td>json</td>
</tr>
<tr>
<td></td>
<td>xml</td>
</tr>
<tr>
<td></td>
<td>yaml</td>
</tr>
<tr>
<td></td>
<td>sparkplug</td>
</tr>
<tr>
<td></td>
<td>rbe</td>
</tr>
<tr>
<td></td>
<td>serial request</td>
</tr>
<tr>
<td>Social</td>
<td>email in</td>
</tr>
<tr>
<td></td>
<td>email out</td>
</tr>
<tr>
<td></td>
<td>twitter in</td>
</tr>
<tr>
<td></td>
<td>twitter out</td>
</tr>
<tr>
<td>Storage</td>
<td>tail</td>
</tr>
<tr>
<td></td>
<td>file in</td>
</tr>
<tr>
<td></td>
<td>sqlite</td>
</tr>
<tr>
<td></td>
<td>file out</td>
</tr>
<tr>
<td></td>
<td>timeseries in</td>
</tr>
<tr>
<td></td>
<td>timeseries out</td>
</tr>
<tr>
<td></td>
<td>timeseries-- in</td>
</tr>
<tr>
<td></td>
<td>timeseries-- out</td>
</tr>
<tr>
<td>Analysis</td>
<td>sentiment</td>
</tr>
<tr>
<td>Advanced</td>
<td>watch</td>
</tr>
<tr>
<td></td>
<td>feedparse</td>
</tr>
<tr>
<td></td>
<td>exec</td>
</tr>
<tr>
<td>Cloud</td>
<td>azureiothub</td>
</tr>
<tr>
<td>IIoT</td>
<td>OPC UA nodes</td>
</tr>
<tr>
<td>Category</td>
<td>Node</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Modbus</td>
<td>Modbus Response</td>
</tr>
<tr>
<td></td>
<td>Modbus Read</td>
</tr>
<tr>
<td></td>
<td>Modbus Getter</td>
</tr>
<tr>
<td></td>
<td>Modbus Flex Getter</td>
</tr>
<tr>
<td></td>
<td>Modbus Write</td>
</tr>
<tr>
<td></td>
<td>Modbus Flex Write</td>
</tr>
<tr>
<td></td>
<td>Modbus Server</td>
</tr>
<tr>
<td></td>
<td>Modbus Flex Server</td>
</tr>
<tr>
<td></td>
<td>Modbus Queue Info</td>
</tr>
<tr>
<td></td>
<td>Modbus Flex Connector</td>
</tr>
<tr>
<td></td>
<td>Modbus Response Filter</td>
</tr>
<tr>
<td>Dashboard</td>
<td>button</td>
</tr>
<tr>
<td></td>
<td>dropdown</td>
</tr>
<tr>
<td></td>
<td>switch</td>
</tr>
<tr>
<td></td>
<td>slider</td>
</tr>
<tr>
<td></td>
<td>numeric</td>
</tr>
<tr>
<td></td>
<td>text input</td>
</tr>
<tr>
<td></td>
<td>date picker</td>
</tr>
<tr>
<td></td>
<td>colour picker</td>
</tr>
<tr>
<td></td>
<td>form</td>
</tr>
<tr>
<td></td>
<td>text</td>
</tr>
<tr>
<td></td>
<td>gauge</td>
</tr>
<tr>
<td></td>
<td>chart</td>
</tr>
<tr>
<td></td>
<td>audio out</td>
</tr>
<tr>
<td></td>
<td>notification</td>
</tr>
<tr>
<td></td>
<td>ui control</td>
</tr>
<tr>
<td></td>
<td>template</td>
</tr>
</tbody>
</table>

*Table 39: List of standard nodes*
9.6 MQTT input node

The MQTT input node enables you to receive data from an MQTT broker via the MQTT protocol using the MQTT function subscribe.

Figure 71: MQTT input node

Parameters of the MQTT input node

This section describes the parameters of the MQTT input node.

![Dialog box Edit MQTT in node](image)

Figure 72: Dialog box Edit MQTT in node

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Selection list</td>
<td>The selection list Server shows the MQTT broker to be used. If MQTT brokers are already defined, they will be listed here. The selection list Server always contains a further entry <strong>Add new mqtt-broker</strong> to add a new MQTT broker if no MQTT broker has been defined yet or if already existing brokers are not to be used.</td>
</tr>
<tr>
<td>Topic</td>
<td>Input field</td>
<td>In the input field Topic you can enter the topic for the MQTT communication. If no name has been entered, but an input has been made under Topic, this input will be used as node name in the Node-RED workspace. Topic # causes all topics of the broker to be received.</td>
</tr>
<tr>
<td>QoS</td>
<td>Selection list</td>
<td>You can set the selection list QoS (Quality of Service) to one of the three values 0, 1, and 2. The meaning of these values is as follows: 0 = At most once (no acknowledge by the receiver) 1 = At least once (the sender stores the message until it receives an acknowledge confirmation from the receiver) 2 = Exactly once (Sender and receiver acknowledge the message using additional acknowledge messages)</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here you enter the name of the MQTT input node that is displayed at the node in Node-RED and used for identification.</td>
</tr>
</tbody>
</table>

Table 40: Parameter MQTT input node
If you select *Add new mqtt-broker* in the list *Server* and click *Edit* thereafter, the dialog box *Add new mqtt-broker config node* will be displayed. In this dialog box you can configure the parameters for a connection to an MQTT broker.

*Figure 73: Dialog box MQTT broker config node – tab Connection*
**Tab Connection**

In the tab *Connection* you can configure the connection to the server.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Input field</td>
<td>Here you indicate with which MQTT broker the Node-RED MQTT input node shall communicate. For the communication with an external MQTT broker specify localhost (denoting the locally defined host computer) for addressing the integrated MQTT broker of the Edge Gateway.</td>
</tr>
<tr>
<td>Port</td>
<td>Input field</td>
<td>Here you enter the port via which Node-RED communicates with MQTT. Port 1883 (for standard MQTT) or 8883 (for MQTT with TLS encryption) is usually used here.</td>
</tr>
<tr>
<td>Enable secure (SSL/TLS) connection</td>
<td>Checkbox</td>
<td>If you check the box, the MQTT protocol will be transmitted via a secure connection with SSL/TLS encryption. For reasons of data security we recommend checking this box.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Input field</td>
<td>If the box Use clean session is not checked, you have to enter the client ID here to identify the client. If the box Use clean session is checked, no entry is required because in this case the client ID will be produced automatically.</td>
</tr>
<tr>
<td>Keep alive time</td>
<td>Input field</td>
<td>Here you enter the lifetime of the connection.</td>
</tr>
<tr>
<td>Use clean session</td>
<td>Checkbox</td>
<td>By checking this box you can activate a clean session during which the client ID is produced automatically.</td>
</tr>
<tr>
<td>Use legacy MQTT 3.1 support</td>
<td>Checkbox</td>
<td>By checking this box you can activate MQTT 3.1 support.</td>
</tr>
</tbody>
</table>

Table 41: Parameters in the tab Connection

**Tab Security**

In the tab *Security* you can configure the parameters for a secure connection, e.g. authentication and encryption.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Input field</td>
<td>Here you enter the user name for the connection.</td>
</tr>
<tr>
<td>Password</td>
<td>Input field</td>
<td>Here you enter the password for the connection.</td>
</tr>
</tbody>
</table>

Table 42: Parameters in the tab Security
Tab Messages

In the tab Messages you can configure the topics that will be sent in the following three cases:

- when a new connection is established (birth message).
- before a connection is disconnected (close message).
- when a connection is disconnection unexpectedly (will message).

![Dialog box MQTT broker config node - tab Messages](image)

Figure 75: Dialog box MQTT broker config node - tab Messages

The parameters are the same for all three types of messages.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topic</td>
<td>Input field</td>
<td>In the input field Topic you can enter the topic of the MQTT communication. If you leave this field blank, no Birth Message will be sent. In that case, all other parameters of this tab are meaningless.</td>
</tr>
<tr>
<td>Retain</td>
<td>Selection list</td>
<td>Here you can set whether the connection is to be maintained after use: TRUE: The connection is to be maintained. FALSE: The connection will be terminated.</td>
</tr>
<tr>
<td>Payload</td>
<td>Input field</td>
<td>Here you can enter the payload (text) to be transmitted in the Birth Message via MQTT.</td>
</tr>
<tr>
<td>QoS</td>
<td>Selection list</td>
<td>You can set the selection list QoS (Quality of Service) to one of the three values 0, 1, and 2. The meaning of these values is as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = At most once (no acknowledge by the receiver)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = At least once (the sender stores the message until it receives an acknowledge confirmation from the receiver)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Exactly once (Sender and receiver acknowledge the message using additional acknowledge messages)</td>
</tr>
</tbody>
</table>

Table 43: Parameters in the tab Messages
9.7 MQTT output node

The MQTT output node enables you to send data to an MQTT broker via the MQTT protocol using the MQTT function *publish*.

![MQTT output node](image)

**Figure 76: MQTT output node**

**Parameters of the MQTT output node**

This section describes the parameters of the MQTT output node.

![Dialog box MQTT output node](image)

**Figure 77: Dialog box MQTT output node**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Selection list</td>
<td>The selection list Server shows the MQTT broker to be used. If MQTT brokers are already defined, they will be listed here. The selection list Server always contains a further entry <strong>Add new mqtt-broker</strong> to add a new MQTT broker if no MQTT broker has been defined yet or if already existing brokers are not to be used.</td>
</tr>
<tr>
<td>Topic</td>
<td>Input field</td>
<td>In the input field Topic you can enter the topic of the MQTT communication. If no name has been entered, but an input has been made under Topic, this input will be used as node name in the Node-RED workspace.</td>
</tr>
<tr>
<td>QoS</td>
<td>Selection list</td>
<td>You can set the selection list QoS (Quality of Service) to one of the three values 0, 1, and 2. The meaning of these values is as follows: 0 = At most once (no acknowledge by the receiver) 1 = At least once (the sender stores the message until it receives an acknowledge from the receiver) 2 = Exactly once (Sender and receiver acknowledge the message using additional acknowledge messages)</td>
</tr>
<tr>
<td>Retain</td>
<td>Selection list</td>
<td>Here you can set whether the connection is to be maintained after use: TRUE: The connection is to be maintained. FALSE: The connection will be terminated.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here you enter the name of the MQTT output node that is displayed at the node in Node-RED and used for identification.</td>
</tr>
</tbody>
</table>

Table 44: Parameters of the Edit MQTT output node

If you select **Add new mqtt-broker** in the list Server and click Edit thereafter, the dialog box **Add new mqtt-broker config node** will be displayed. In this dialog box you can configure the parameters for a connection to an MQTT broker.

The parameters of tabs **Connection**, **Security**, **Birth Message**, and **Will Message** of the MQTT output and input node are identical and described in section **MQTT input node** [page 109].
9.8 NPIX LEDs

With the npix-leds node (RS-232) you can access the LEDs of the NPIX module from NodeRED.

**Figure 78: LED node**

**Parameter of the LED node**

This section describes the parameters of the LED node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LED</td>
<td>Selection list</td>
<td>Selection of LED to be controlled (COM0 / COM1, red / green)</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here specify the name to be displayed at the node</td>
</tr>
</tbody>
</table>

Table 45: Parameters of configuration dialog Edit serial rs232 node

Proceed as follows in order to configure the parameters of the LED node:

- Within Node-RED, double-click at the LED node to open it.
- The dialog window *Edit npix leds node* appears:

**Figure 79: Dialog window Edit npix leds node**

- From the selection list LED, choose that LED you intend to access. The following possibilities are available.

<table>
<thead>
<tr>
<th>LED Option</th>
<th>SIO: (2 x Duo LED yellow/green)</th>
<th>Accessed color</th>
</tr>
</thead>
<tbody>
<tr>
<td>COM0- LED0_GREEN</td>
<td>COM0</td>
<td>Green</td>
</tr>
<tr>
<td>COM0- LED0_RED</td>
<td>COM0</td>
<td>Red</td>
</tr>
<tr>
<td>COM1- LED1_GREEN</td>
<td>COM1</td>
<td>Green</td>
</tr>
<tr>
<td>COM1- LED1_RED</td>
<td>COM1</td>
<td>Red</td>
</tr>
</tbody>
</table>

Table 46: Options of selection list LED

- Specify in field Name the name to be displayed at the node.
- Now, the parameters of the LED node are configured.

Via the node settings area you can access the inputs, outputs and icons.
Controlling the LED node

Controlling the LED node is done via msg.payload within the input message. Use the numerical value 0 to clear and value 1 to set the LED.

9.9 Serial RS-232 send

With the serial RS-232 inbound node you can read data, i.e. an attribute of an object, from a serial interface according to the RS-232 standard.

![RS-232-send](image)

*Figure 80: Serial inbound node RS-232 send*

Parameter of serial inbound node

This section describes the parameter of the serial RS-232 inbound node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port</td>
<td>Selection list (extendable)</td>
<td>Selection of RS-232 interface setting, with which the RS-232 node shall communicate.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here specify the name to be displayed at the node.</td>
</tr>
</tbody>
</table>

*Table 47: Parameters of configuration dialog Edit serial rs232 node*

In order to configure the node properties area to be used, proceed as follows:

- Within Node-RED, double-click at the serial RS-232 inbound node to open it.

![Edit serial rs232 node](image)

*Figure 81: Dialog window Edit serial rs232 node - node properties area*

- In selection list **Serial Port**, choose the desired one of the present interface settings by which the RS-232 shall communicate, or create a new interface setting with list entry **Add new serial port npix rs232**.
- By clicking at the pencil symbol you can display the dialog window **Edit serial port npix rs232 node**. In this dialog window you configure the parameters for the serial connection via the interface of the RS-232 module. For more information, see **Serial RS-232 send** page 117.
- After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.
- Specify in field **Name** the name to be displayed at the node.
- Now the area node properties is configured.
Via the node settings area you can access the inputs, outputs and icons.

The configuration of the parameters for serial connections over the interface of the RS232 module is done in dialog window Edit serial port npix rs232 node. In order to configure the parameters, proceed as follows:

- In dialog window **Edit serial rs232 node** right from Serial Port click at .
- The dialog window **Edit serial port npix rs232 node** is displayed.

![Dialog window „Edit serial port npix rs232 node“](image)

- Specify the name of the interface to be used in input field **Serial Port** (1). Here, the default is /dev/ttyS0.

- In selection list **Baud Rate** choose the desired baud rate (Interface speed). Possible values are:
  - 115200 Baud,
  - 57600 Baud,
  - 38400 Baud,
  - 19200 Baud,
  - 9600 Baud,
  - 4800 Baud,
  - 2400 Baud,
  - 1200 Baud.
  Here, the default value is 57600 Baud.

- Within the selection list **Data Bits** choose the number of desired data bits for the serial communication. Possible values are: 7 or 8 Bits. Here the default is 8 Bits.

- Within the selection list **Parity** choose the parity of the serial communication. Here the default is none. Other values are not supported as the mini-UART interface provides no parity support.

- Within the selection list **Stop Bits** choose the number of stop bits to be used in serial communication. Possible values are 1 or 2. Here the default is 1.
Within the selection list **Split input**

<table>
<thead>
<tr>
<th>Option</th>
<th>Criterion</th>
<th>Parameter out=</th>
</tr>
</thead>
<tbody>
<tr>
<td>on the character</td>
<td>Separation occurs if a specified separation character is encountered</td>
<td>char</td>
</tr>
<tr>
<td>after a timeout of</td>
<td>Separation after a fixed amount of time elapsed since the last separation</td>
<td>time</td>
</tr>
<tr>
<td>Into fixed length</td>
<td>Separation after a fixed number of characters has been transmitted.</td>
<td>cont</td>
</tr>
</tbody>
</table>

*Table 48: Options for Split input*

Depending on your choice at the last step, specify the following in the input field right beside:

- If **Character** has been chosen: The separation character. Here, the default is \n.
- If **Timeout** has been chosen: An integer value between 0 and 99999 for the Timeout period, after which the separation occurs.
- If **Number of chars** has been chosen: An integer value between 0 and 99999 for the fixed number of characters after that the separation occurs.

Within the selection list right of **and deliver**, choose how to interpret the payload: `bin = “true”` means that binary buffers should be applied. `bin = “false”` means that ASCII strings are used. Binary buffers can be managed using buffer objects.

Check the checkbox **add split character to output messages** only if the separation character shall also be used within the output messages.

Click at **Update** in order to store your choice and make it valid.
9.10 Serial RS-232 receive

With the serial RS-232 outbound node you can write data, i.e. an attribute of an object, to a serial interface according to the RS-232-Standard.

![Serial RS-232 receive](image)

**Figure 83: Serial outbound node RS-232 receive**

**Parameters of serial outbound node**

This section describes the parameters of the serial RS-232 outbound node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port</td>
<td>Selection list</td>
<td>Selection of RS-232 interface setting, with that the RS-232 node shall communicate.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here specify the name to be displayed at the node.</td>
</tr>
</tbody>
</table>

*Table 49: Parameters of configuration dialog Edit serial rs232 node.*

In order to configure the node properties area to be used, proceed as follows:

- Within Node-RED, double-click at the serial RS-232 outbound node to open it.
- In selection list **Serial Port**, choose the desired one of the present interface settings by which the RS-232 shall communicate, or create a new interface setting with list entry *Add new serial port npix rs232*.
- By clicking at the pencil symbol you can display the dialog window *Edit serial port npix rs232 node*. In this dialog window you configure the parameters for the serial connection via the interface of the RS-232 module. For more information, see *Serial RS-232 receive* [page 120].
- After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.
- Specify in field **Name** the name to be displayed at the node.
- Now the area **node properties** is configured.

Via the **node settings** area you can access the inputs, outputs and icons.
The configuration of the parameters for serial connections over the interface of the RS232 module is done in dialog window **Edit serial port npix rs232 node**. In order to configure the parameters, proceed as follows:

- In dialog window **Edit serial rs232 node** right from **Serial Port** click at .
- The dialog window **Edit serial port npix rs232 node** is displayed.

![Figure 85: Dialogf window „Edit serial port npix rs232 node“](image)

- Specify the name of the interface to be used in input field **Serial Port** (1) . Here, the default is `/dev/ttyS0`.

- In selection list **Baud Rate** choose the desired baud rate (Interface speed).
  Possible values are:
  - 115200 Baud,
  - 57600 Baud,
  - 38400 Baud,
  - 19200 Baud,
  - 9600 Baud,
  - 4800 Baud,
  - 2400 Baud,
  - 1200 Baud.
  Here, the default value is 57600 Baud.

- Within the selection list **Data Bits** choose the number of desired data bits for the serial communication. Possible values are: 7 or 8 Bits. Here the default is 8 Bits.

- Within the selection list **Parity** choose the parity of the serial communication. Here the default is *none*. Other values are not supported as the mini-UART interface provides no parity support.

- Within the selection list **Stop Bits** choose the number of stop bits to be used in serial communication. Possible values are 1 or 2. Here the default is 1.
Within the selection list **Split input**, choose one of the following three criteria for data separation:

<table>
<thead>
<tr>
<th>Option Split input</th>
<th>Criterion</th>
<th>Parameter out=</th>
</tr>
</thead>
<tbody>
<tr>
<td>on the character</td>
<td>Separation occurs if a specified separation character is encountered</td>
<td>char</td>
</tr>
<tr>
<td>after a timeout of</td>
<td>Separation after a fixed amount of time elapsed since the last separation</td>
<td>time</td>
</tr>
<tr>
<td>Into fixed length</td>
<td>Separation after a fixed number of characters has been transmitted.</td>
<td>cont</td>
</tr>
</tbody>
</table>

*Table 50: Options for Split input*

Depending on your choice at the last step, specify the following in the input field right beside:

- If **Character** has been chosen: The separation character. Here, the default is `\n`.
- If **Timeout** has been chosen: An integer value between 0 and 99999 for the Timeout period, after which the separation occurs.
- If **Number of chars** has been chosen: An integer value between 0 and 99999 for the fixed number of characters after that the separation occurs.

Within the selection list right of **and deliver**, choose how to interpret the payload: bin = “true” means that binary buffers should be applied. bin = “false” means that ASCII strings are used. Binary buffers can be managed using buffer objects.

Check the checkbox **add split character to output messages** only if the separation character shall also be used within the output messages.

Click at **Update** in order to store your choice and make it valid.
9.11 Serial inbound node RS-485

Using the serial RS-485 inbound node you can read data from a serial interface according to the RS-485 standard.

Figure 86: Serial inbound node RS-485 send

In this context, data means an attribute of a Node-RED object, specifically the attribute `payload` of the `msg` object.

The following prerequisite applies for using this node:

- In your Edge Gateway NIOT-E-TPI51-EN-RE an RS-485 interface module NIOT-E-NPIX-RS485 must have been mounted within the extension module bay located at the bottom of the Edge Gateway.

### Parameters of serial inbound node

This section describes the parameters of the serial RS-485 inbound node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port</td>
<td>Selection list (extendable)</td>
<td>Selection of desired configuration for the RS-485 communication of the interface module.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here specify the name to be displayed at the node</td>
</tr>
</tbody>
</table>

Table 51: Parameters of configuration dialog Edit serial rs485 node.

In order to configure the node properties area to be used, proceed as follows:

- To open the serial RS-485 inbound node within Node-RED, double-click at it.

  The dialog window **Edit serial port npix rs485 node** is displayed. Within this window, the node properties area is visible.

  [Figure 87: Dialog window Edit serial rs485 node - node properties area]

- In selection list **Serial Port**, choose the desired interface setting, or create a new interface setting with list entry **Add new serial port npix rs485**.

- For the desired interface setting, you can display the dialog window **Edit serial port npix rs485 node** by clicking at the pencil symbol (see below). Configure the parameters for a serial connection over the RS-485 interface of the module NIOT-E-NPIX-RS485 in this dialog window.

  After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.

- Specify in field **Name** the name to be displayed at the node.
Now the node properties area is configured.

Via the node settings area you can access the inputs, outputs and icons.

The configuration of the parameters for serial connections over the RS-485 interface of the module NIOT-E-NPIX-RS485 is done in dialog window Edit serial port npix rs485 node. In order to configure the parameters, proceed as follows:

- In dialog window Edit serial rs-485 node right from Serial Port, click at.

  The dialog window Edit serial port npix rs485 node is displayed.

- Specify the name of the desired interface in input field Serial Port\(^{(1)}\). Default value is /dev/ttyS0.

- In selection list Baud Rate\(^{(2)}\) choose the desired baud rate (interface speed). Possible values are: 115200 Baud, 57600 Baud, 38400 Baud, 19200 Baud, 9600 Baud, 4800 Baud, 2400 Baud, 1200 Baud.
  Other (%). Default value is 57600 Baud.

- Within the selection list Data Bits\(^{(3)}\), choose the number of desired data bits for the serial communication. Possible values are: 7 or 8 bits. Default value is 8 bits.

- Within the selection list Parity\(^{(4)}\), choose the parity of the serial communication. Here the default is none. Other values are not supported as the UART interface used in NIOT-E-TPI51-EN-RE does not provide parity support.
Within the selection list **Stop Bits** (5), choose the number of stop bits to be used in serial communication. Default value is 1 stop bit. Other values are not possible as the UART interface used in NIOT-E-TPI51-EN-RE does not support operation with 2 stop bits.

Within the selection list **Split input** (6), choose one of the following three criteria for data separation:

<table>
<thead>
<tr>
<th>Option Split input</th>
<th>Criterion</th>
<th>Parameter out</th>
</tr>
</thead>
<tbody>
<tr>
<td>on the character</td>
<td>Separation occurs if a specified separation character is encountered</td>
<td>char</td>
</tr>
<tr>
<td>after a timeout of</td>
<td>Separation after a fixed amount of time elapsed since the last separation</td>
<td>time</td>
</tr>
<tr>
<td>Into fixed length</td>
<td>Separation after a fixed number of characters has been transmitted.</td>
<td>cont</td>
</tr>
</tbody>
</table>

Table 52: Options for Split input

Depending on your choice at the last step, specify the following in the input field (7) right beside:

- If **Character** has been chosen: The separation character. Here, the default is \n.
- If **Timeout** has been chosen: This value indicates the time, after which the separation occurs. Specify an integer value between 0 and 99999 in units of milliseconds.
- If **Number of chars** has been chosen: An integer value between 0 and 99999 for the fixed number of characters after that the separation occurs.

Within the selection list right of **and deliver** (8), choose how to interpret the payload: `bin = “true”` means that binary buffers should be applied. `bin = “false”` means that ASCII strings are used. Binary buffers can be managed using buffer objects.

Check the checkbox **add split character to output messages** (9) only if the separation character shall also be used within the output messages.

Click at **Update** to store your choice and make it valid.
Timing behavior of the RS-485 interface in the context of switching between transmit and receive mode

Switching between transmit and receive mode of the RS-485 interface of the module NIOT-E-NPIX-RS485 is accomplished by a GPIO signal (GPIO 17, State High in send mode and Low in receive mode. Controlling GPIO 17 is done all in software causing a jitter.

Measurements using an oscilloscope have shown that the signal GPIO 17 is set to high state between 400 µsec and 1ms before the data is transmitted. It falls back to low state 5ms to 32ms after the last bit has been shifted out of the transmit shift register. Consider, that the module is able to receive data again only after that time has passed.

Fast devices (<32ms) sending back data over RS-486 in a request/response manner might not work with the RS-485 nodes.
9.12 Serial outbound node RS-485

With the serial RS-485 outbound node you can write data to a serial interface according to the RS-485-Standard.

![Node-RED serialization node](image)

**Figure 89: Serial outbound node RS-485 receive**

In this context, data means an attribute of a Node-RED object, specifically the attribute `payload` of the `msg` object.

The following prerequisite applies for using this node:

- In your Edge Gateway NIOT-E-TPI51-EN-RE an RS-485 interface module NIOT-E-NPIX-RS485 must have been mounted within the extension module bay located at the bottom of the Edge Gateway.

### Parameters of serial outbound node

This section describes the parameters of the serial RS-485 outbound node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Serial Port</td>
<td>Selection list (extensible)</td>
<td>Selection of desired configuration for the RS-485 communication of the interface module.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Here specify the name to be displayed at the node.</td>
</tr>
</tbody>
</table>

Table 53: Parameters of configuration dialog Edit serial node.

In order to configure the node properties area to be used, proceed as follows:

- To open the serial RS-485 outbound node within Node-RED, double-click at it.

  - The dialog window **Edit serial port npix rs485 node** is displayed. Within this window, the node properties area is visible.

  ![Node-RED configuration dialog](image)

  **Figure 90: Dialog window Edit serial rs485 node - node properties area**

- In selection list **Serial Port**, choose either the desired interface setting, or create a new interface setting with list entry **Add new serial port npix rs485**.

- For the desired interface setting, you can display the dialog window **Edit serial port npix rs485 node** by clicking at the pencil symbol. Configure the parameters for a serial connection over the RS-485 interface of the module NIOT-E-NPIX-RS485 in this dialog window.

  - After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.
Specify in field **Name** the name to be displayed at the node.

Now the **node properties** area is configured.

Via the **node settings** area you can access the inputs, outputs and icons.

The configuration of the parameters for serial connections over the RS-485 interface of the module NIOT-E-NPIX-RS485 is done in dialog window **Edit serial port npix rs485 node**. In order to configure the parameters, proceed as follows:

- In dialog window **Edit serial rs-485 node** right from **Serial Port**, click at .

The dialog window **Edit serial port npix rs485 node** is displayed.

![Edit serial port npix rs485 node dialog window](image)

**Figure 91: Dialog window „Edit serial port npix rs485 node“**

- Specify the name of the desired interface in input field **Serial Port** (1). Default value is `/dev/ttyS0`.

- In selection list **Baud Rate** (2) choose the desired baud rate (interface speed). Possible values are:
  - 115200 Baud,
  - 57600 Baud,
  - 38400 Baud,
  - 19200 Baud,
  - 9600 Baud,
  - 4800 Baud,
  - 2400 Baud,
  - 1200 Baud.

  Default value is 57600 Baud.

- Within the selection list **Data Bits** (3), choose the number of desired data bits for the serial communication. Possible values are: 7 or 8 bits. Default value is 8 bits.
Within the selection list **Parity(4)**, choose the parity of the serial communication. Here the default is *none*. Other values are not supported as the UART interface used in NIOT-E-TPI51-EN-RE does not provide parity support.

Within the selection list **Stop Bits(5)**, choose the number of stop bits to be used in serial communication. Default value is 1 stop bit. Other values are not possible as the UART interface used in NIOT-E-TPI51-EN-RE does not support operation with 2 stop bits.

Within the selection list **Split input(6)**, choose one of the following three criteria for data separation:

<table>
<thead>
<tr>
<th>Option Split input</th>
<th>Criterion</th>
<th>Parameter out=</th>
</tr>
</thead>
<tbody>
<tr>
<td>on the character</td>
<td>Separation occurs if a specified separation character is encountered</td>
<td>char</td>
</tr>
<tr>
<td>after a timeout of</td>
<td>Separation after a fixed amount of time elapsed since the last separation</td>
<td>time</td>
</tr>
<tr>
<td>Into fixed length</td>
<td>Separation after a fixed number of characters has been transmitted.</td>
<td>cont</td>
</tr>
</tbody>
</table>

**Table 54: Options for Split input**

Depending on your choice at the last step, specify the following in the input field (7) right beside:

- If **Character** has been chosen: The separation character. Here, the default is \n.
- If **Timeout** has been chosen: This value indicates the time, after which the separation occurs. Specify an integer value between 0 and 99999 in units of milliseconds.
- If **Number of chars** has been chosen: An integer value between 0 and 99999 for the fixed number of characters after which the separation occurs.

Within the selection list right of **and deliver(8)**, choose how to interpret the payload: `bin = “true”` means that binary buffers should be applied. `bin = “false”` means that ASCII strings are used. Binary buffers can be managed using buffer objects.

Check the checkbox **add split character to output messages(9)** only if the separation character shall also be used within the output messages.

Click at **Update** to store your choice and make it valid.
Timing behavior of the RS-485 interface in the context of switching between transmit and receive mode

Switching between transmit and receive mode of the RS-485 interface of the module NIOT-E-NPIX-RS485 is accomplished by a GPIO signal (GPIO 17, State High in send mode and Low in receive mode. Controlling GPIO 17 is done all in software causing a jitter.

Measurements using an oscilloscope have shown that the signal GPIO 17 is set to high state between 400 µsec and 1ms before the data is transmitted. It falls back to low state 5ms to 32ms after the last bit has been shifted out of the transmit shift register. Consider, that the module is able to receive data again only after that time has passed.

Fast devices (<32ms) sending back data over RS-486 in a request/response manner might not work with the RS-485 nodes.
9.13 Digital I/O input node DIO in

Using the digital I/O input node (DIO in) you can read data from a digital input line in order to process these further within a Node-RED flow.

![Digital I/O input node DIO in](image)

Figure 92: Digital I/O input node DIO in

In this context, data means an attribute of a Node-RED object, specifically the attribute `payload` of the `msg` object. This attribute will dynamically take the values 0 or 1 depending on the current state of the input pin of the selected digital input.

The following prerequisite applies for using this node:

- A digital input/output module NIOT-E-NPIX-I0 must have been mounted within the extension module bay located at the bottom of your Edge Gateway NIOT-E-TPI51-EN-RE behind a cover held by two screws. This module provides four digital inputs and outputs each (the inputs `dio in0`...`dio in3` and the outputs `dio out0`...`dio out3`).

**Parameters of the digital I/O input node**

The digital I/O input node provides the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input</td>
<td>Selection list</td>
<td>Selection of digital input line to be used (<code>dio in0</code>...<code>dio in3</code>), whose value is to be acquired in Node-RED.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Specify the name to be displayed at the node here.</td>
</tr>
</tbody>
</table>

Table 55: Parameters of configuration dialog Edit dio in node

In order to configure the `node properties` area to be used, proceed as follows:

- Within Node-RED, double-click at the digital I/O input node in order to open its configuration dialog.

![Dialog window Edit dio in node - node properties area](image)

Figure 93: Dialog window Edit dio in node - node properties area

- From selection list **Input** choose the desired one of the four present digital input lines (`dio in0`...`dio in3`) to receive data from using the digital IO input node.
- After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.
- In field **Name** specify the name to be displayed at the node.
- Now the area `node properties` of the configuration dialog is configured.
Via the *node settings* area you can access the inputs, outputs and icons, if present.

![Figure 94: Dialog window Edit dio in node - node settings area](image)

© Hilscher 2017 – 2019
9.14 Digital I/O output node DIO out

Using the digital I/O output node (DIO out) you can write data from the Node-RED flow to a digital output line for control purposes.

In this context, data means an attribute of a Node-RED object, specifically the attribute `payload` of the `msg` object. The state of the output pin of the selected digital output is set to low or high level depending on the current value of this attribute and is dynamically updated at any change of the attribute's value.

The following prerequisite applies for using this node:

- A digital input/ output module NIOT-E-NPIX-IO must have been mounted within the extension module bay located at the bottom of your Edge Gateway NIOT-E-TPI51-EN-RE behind a cover held by two screws. This module provides four digital inputs and outputs each (the inputs `dio in0`...`dio in3` and the outputs `dio out0`...`dio out3`).

Parameters of the digital I/O output node

The digital I/O output node provides the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output</td>
<td>Selection list</td>
<td>Selection of digital output line to be used (<code>dio out0</code>...<code>dio out3</code>), whose state is to be controlled from Node-RED.</td>
</tr>
<tr>
<td>Name</td>
<td>Input field</td>
<td>Specify the name to be displayed at the node here.</td>
</tr>
</tbody>
</table>

In order to configure the node properties area to be used, proceed as follows:

- Within Node-RED, double-click at the digital I/O output node in order to open its configuration dialog.

- From selection list **Output** choose the desired output of the four present digital output lines (`dio out0`...`dio out3`) to be controlled by the digital IO output node.

- After having clicked the **Update** button for saving or the **Cancel** button for cancelling, you return here.
Specify the name to be displayed at the node in field Name.

Now the area node properties of the configuration dialog is configured.

Via the node settings area you can access the inputs, outputs and icons, if present.

![Figure 97: Dialog window Edit dio out node - node settings area](image-url)
10 Examples for Node-RED

The following sections describe examples for data flows.

10.1 Example 1: Inject and debug node

This example shows a simple flow with an inject node (input node) and a debug node (output node).

The inject node allows you to insert messages into a flow, either by clicking once a button at the node or regularly by using a time interval between the sending of two messages.

The debug node allows you to display any messages (or the entire message object) in the sidebar. When the default settings of the debug node are used, the payload of the message will be displayed only.

Prerequisites
1. A connection with the Edge Gateway is established (see section Using the web browser to establish a connection with the Edge Gateway [page 20]).
2. The Node-RED workspace is open.

Step-by-step instructions
1. Inserting an inject node:
   - Drag an inject node from the node library and drop it in the worksheet.

2. Showing the sidebar:
   - Show the sidebar with the key combination Ctrl+spacebar or via the Node-RED menu View > Show Sidebar.
   - Click the tab Info.
   - Click the inject node to show its properties and function description in the tab Info.

3. Inserting a debug node:
   - Drag a debug node from the node library and drop it in the worksheet.

4. Connecting the nodes
   - To connect inject node and debug node, hold down the left mouse button and draw a connecting line (wire) from the output port of the inject node to the input port of the debug node.
   - The inject node can send messages to the debug node.
5. Deploy:
   - Click **Deploy** to transmit the nodes, that have so far existed in the editor only, to the device and activate them. This procedure is called deployment.
   - The flow is activated in the Edge Gateway.

---

**Note:**
For more information on Deploy, see section *Menu Deploy* [page 92].

---

The example for copying
```json
[{"id":"46ae085e.4fd768","type":"debug","z":"9deaf786.3854a","name":"","active":true,"console":"false","complete":"false","x":330,"y":200,"wires":[]},
 {"id":"b2605825.aea4d","type":"inject","z":"9deaf786.3854a","name":"","topic":"","payload":"","payloadType":"date","repeat":"","crontab":"","once":false,"x":138,"y":188.5,"wires":[]}]```

Testing the flow and displaying messages
   - Click the tab **Debug** in the sidebar.
   - Click the left button at the **inject** node.
   - The sidebar should display numbers. In the standard default setting, the inject node uses the quantity of milliseconds that have elapsed since January 1st, 1970, as payload.
10.2 Example 2: MQTT input node

The MQTT input node allows receiving data from an MQTT broker via the MQTT protocol and uses the MQTT function *subscribe* for this purpose.

![MQTT input node](image)

This example uses the MQTT input node together with a Debug node to receive data via MQTT and to display the data thereafter in the tab **Debug** of the Node-RED sidebar.

**Prerequisite**

1. A connection to the Edge Gateway is established (see section *Using the web browser to establish a connection with the Edge Gateway* [page 20])
2. The Node-RED workspace is open.

**Step-by-step instructions**

1. Inserting an MQTT input node:
   - Drag an **MQTT** input node from the node library and drop it in the worksheet.
   - The red triangle the MQTT input node is displayed with indicates that the node still needs some more parameters which you have to configure in the following steps.

2. Showing the sidebar:
   - Show the sidebar using the keyboard shortcut **Ctrl+spacebar** or via the Node-RED menu **View > Show Sidebar**.
   - Click the tab **Info**.
   - Click the **MQTT** input node to display its properties and a functional description in the tab **Info**.

3. Editing the MQTT input node:
   - To open the edit dialog, double-click on the MQTT input node.
   - The edit dialog for entering the parameters will be displayed.
4. Adding a broker:

- If you use an MQTT node for the first time, the **Server** list contains the entry **Add new mqtt-broker** only. In that case, click **Edit** to add an MQTT broker. As an alternative you can select a server from the list and continue with step 5.

- The dialog box **Add new mqtt-broker config node** will be displayed.

- Enter the name **localhost** in the field **Server** of the tab **Connection**. By means of **localhost** you address the MQTT broker integrated in the Edge Gateway.

- For this (simple) example you can adopt the preset parameters without having to enter any further parameters.

- Click **Add**.

- The MQTT broker is configured.

- The dialog box returns to the first edit dialog.

- Under **Server** the edit dialog shows the address and the port **localhost:1883**.
5. Configuring the MQTT input node:
   - Enter the name of the topic that you want to receive in the field **Topic**, e.g. **Timestamp1**. To receive all topics, enter #.
   - For **QoS** enter the value 1.
   - Enter the name of this node, e.g. **MySubscribingNode**, in the field **Name**.
   - All parameters are entered.
   - Click **Done**.
   - The configuration of the MQTT input node is completed and the red triangle has disappeared.

6. Inserting a Debug node:
   - Drag a **Debug** node from the node library and drop it in the worksheet.

7. Connecting the nodes:
   - To connect the **MQTT** node with the **Debug** node, hold down the left mouse button and draw a connecting line (wire) from the output port of the MQTT node to the input port of the Debug node.
8. Deploy:
   - Click Deploy to transmit the nodes, that have so far existed in the editor only, to the device and activate them.
   - The flow is activated in the Edge Gateway.
   - As soon as the topic Timestamp1 changes, the Debug output will display the new value.

The section MQTT input node [page 109] describes the parameters of the MQTT input node.

The example for copying

```json
[{
  "id": "4a22a8ea.115788","type": "mqtt-in","z": "6b03759e.b5eb4c","name": "MySubscribingNode","topic": "Timestamp1","qos": "1","broker": "55ba4653.6e07b8","x": 211,"y": 512,"wires": [
    ["2785278d.2d5bc8"]],
  ["id": "2785278d.2d5bc8","type": "debug","z": "6b03759e.b5eb4c","name": ",".,"active": true,"console": false,"complete": false,"x": 402,"y": 512,"wires": []],
  ["id": "55ba4653.6e07b8","type": "mqtt-broker","z": "localhost","port": "1883","clientid": ",","settls": false,"compatmode": true,"keepalive": "60","cleansession": true,"willTopic": ",","willQos": "0","willPayload": ",","birthTopic": ",","birthQos": "0","birthPayload": "]
}
```

Testing the flow and displaying messages

   - Click the tab Debug in the sidebar.
   - Use a device that is externally connected to the Edge Gateway to execute a publish with MQTT on topic Timestamp1.
     - or -
     - Copy and use the example MQTT output node (see section Example 3: MQTT output node [page 140]).
   - The Debug node displays messages of the MQTT input node as soon as the topic Timestamp1 changes.
10.3 Example 3: MQTT output node

The MQTT output node allows you to send data to an MQTT broker via the MQTT protocol and uses the MQTT function `publish` for this purpose.

This example uses the MQTT output node together with an Inject node to send data via MQTT.

Figure 99: MQTT output node

Prerequisites

1. A connection to the Edge Gateway is established (see section *Using the web browser to establish a connection with the Edge Gateway* [page 20]).
2. The Node-RED workspace is open.

Step-by-step instructions

1. Inserting an Inject node:
   - Drag an **Inject** node from the node library and drop it in the worksheet.

2. Inserting an MQTT output node:
   - Drag an **MQTT** output node from the node library and drop it in the worksheet.
   - The red triangle the MQTT output node is displayed with indicates that the node still needs some more parameters which you have to configure in the following steps.
3. Showing the sidebar:
   - Show the sidebar using the keyboard shortcut Ctrl+spacebar or via the Node-RED menu View > Show Sidebar.
   - Click the tab Info.
   - Click the MQTT output node to display its properties and a functional description in the tab Info.

4. Editing the MQTT output node:
   - To open the edit dialog, double-click on the MQTT output node.
     - The edit dialog for entering the parameters will be displayed.

5. Adding a broker:
   - If you use an MQTT node for the first time, the Server list contains the entry Add new mqtt-broker only. In that case, click Edit to add an MQTT broker. As an alternative you can select a server from the list and continue with step 6.
   - The dialog box Add new mqtt-broker config node will be displayed.
   - Enter the name localhost in the field Server of the tab Connection. By means of localhost you address the MQTT broker integrated in the Edge Gateway.
   - For this (simple) example you can adopt the preset parameters without having to enter any further parameters.
   - Click Add.
     - The MQTT broker is configured.
     - The dialog box returns to the first edit dialog.
Under **Server** the edit dialog shows the address and the port **localhost:1883**.

- **Server**
  - localhost:1883

- **Topic**
  - Topic

- **QoS**
  - 1

- **Name**
  - Name

6. Configuring the MQTT output node:
   - Enter the name of the topic that you want to send (publish) in the field **Topic**, e.g. **Timestamp1**.
   - For **QoS** enter the value **1**.
   - Enter the name of this node, e.g. **MyPublishingNode**, in the field **Name**.

   All parameters are entered.

   - **Server**
     - localhost:1883
   - **Topic**
     - Timestamp1
   - **QoS**
     - 1
   - **Name**
     - MyPublishingNode

   Click **Done**.

   The configuration of the MQTT output node is completed and the red triangle has disappeared.

7. Connecting the nodes:
   - To connect the **Inject** node with the **MQTT** node, hold down the left mouse button and draw a connecting line (wire) from the output port of the Inject node to the input port of the MQTT node.
8. Deploy:

- Click **Deploy** to transmit the nodes, that have so far existed in the editor only, to the device and activate them.

The flow is activated in the Edge Gateway.

The section *MQTT output node* [¶ page 113] describes the parameters of the MQTT output node.

The example for copying

```javascript
[{"id":"c28f8355.ed0b7","type":"inject","z":"6b03759e.b5eb4c","name":"","topic":"","payload":"","payloadType":"date","repeat":""},  
{"id":"9bc7b36a.df3c3","type":"mqtt out","z":"6b03759e.b5eb4c","name":"MyPublishingNode","topic":"Timestamp1","qos":"1","retain":"","broker":"cf82b7fc.b44d18","x":461,"y":163,"wires":[]},  
{"id":"cf82b7fc.b44d18","type":"mqtt broker","z":"6b03759e.b5eb4c","broker":"localhost","port":"1883","clientid":"","usetls":false,"compatmode":true,"keepalive":"60","cleansession":true,"willTopic":"","willQos":"0","willPayload":"","birthTopic":"","birthQos":"0","birthPayload":""}]
```

Testing the flow and displaying messages

- Use a device that is externally connected to the Edge Gateway to execute a **subscribe** with MQTT on topic Timestamp1.
  - or -
  Copy and use the example MQTT input node (see section *Example 2: MQTT input node* [¶ page 136]).

With each click on the button at the **Inject** node the topic Timestamp1 is sent to the MQTT broker. If you use this example together with the example MQTT input node, you can display the value of the topic Timestamp1 in the tab **Debug**.
10.4 Example 4: Fieldbus input node

The fieldbus input node allows you to receive data from the fieldbus, e.g. PROFINET, and uses signals to address this data. Before you can use the fieldbus input node, you have to configure the fieldbus and define the signals.

![Fieldbus input node](image)

This example uses the fieldbus input node together with a Debug node to receive fieldbus data (in this case PROFINET) and to display the data thereafter in the Debug tab of the Node-RED sidebar.

**Prerequisite**
1. A connection to the Edge Gateway is established (see section *Using the web browser to establish a connection with the Edge Gateway* [page 20]).
2. The Node-RED workspace is open.

**Step-by-step instructions**
1. Inserting the fieldbus input node:
   - Drag a fieldbus input node from the node library and drop it in the worksheet.
   - The red triangle the fieldbus node is displayed with indicates that the node still needs some more parameters which you have to configure in the following steps.

2. Showing the sidebar:
   - Show the sidebar using the keyboard shortcut `Ctrl+spacebar` or via the Node-RED menu `View > Show Sidebar`.
   - Click the tab `Info`.
   - Click the `fieldbus` input node to display its properties and a functional description in the tab `Info`. 
3. Editing the fieldbus input node:
   - To open the edit dialog, double-click on the fieldbus node.
   - The edit dialog for entering the parameters will be displayed.

4. Adding the fieldbus input node:
   - If you use a fieldbus node for the first time, (the fieldbus interface list displays **Add new fieldbus interface**), click **Edit** to add a new fieldbus interface.
   - The fieldbus configuration node will be displayed.
5. Selecting the fieldbus interface:
   - Check whether F displays the entry **PROFINET IO Device: Version ...**.
   - If it is not displayed, you first have to load the firmware for **PROFINET IO Device** in the control panel via the menu entry Network > Field (in the active mode).

6. Opening the fieldbus configurator (PROFINET configurator):
   - If **Fieldbus interface** does not yet display the entry **PROFINET IO Device**, repeat step 5.
   - If **Fieldbus interface** displays the entry **PROFINET IO Device**, click **Open Fieldbus Configurator**.
   - A new tab with the PROFINET configuration interface will be displayed.

7. Configuring PROFINET:
   - Click **IO and Signal configuration** in the configuration tree (left).
   - The page **IO Configuration** with the list of **Available IO items** will be displayed.
   - At first, double-click the entry **16 send byte (inputs)** in the list of **Available IO items**.
   - Then, double-click the entry **16 receive byte (outputs)** in the list of **Available IO items**.
   - The list of **IO items** displays 2 PROFINET modules.
8. Defining signal names for modules:
   - In the column Tag of the list IO items, click send_001 (index 001 named 16 send byte (inputs)).
   - Overwrite the available Tag name with the following new Tag name: toController.
   - In the column Tag of the list IO items, click receive_001 (index 002 named 16 receive byte (outputs)).
   - Overwrite the available Tag name with the following new Tag name: fromController.
   - The new Tag name which is part of the entire signal name is now displayed for each module.

9. Defining signals for module 1:
   - Select 001: 16 send byte (inputs) in the configuration tree.
   - The signal configuration page with information on module 001 will be displayed.
   - Mark the available signal in the signal list.
   - Click Delete selected items.
   - Click Add new signals.
   - The Add new signals dialog box will be displayed.
   - Select the data type: Signed16.
   - Select the quantity: 8.
   - Under tag name base enter Temperature.
   - Click Ok.
   - Column Tag displays Temperature_1 to Temperature_8. If required, you can adapt the signal names in the column Tag.
10. Defining signals for module 2:
   - Select **002: 16 receive byte (outputs)** in the configuration tree.
     - IO and signal configuration
       - 001: 16 send byte (inputs)
       - 002: 16 receive byte (outputs)
   - The signal configuration page with information on module 002 will be displayed.
   - Mark the available signal in the signal list.
   - Click **Delete selected items**.
   - Click **Add new signals**.
     - The Add new signals dialog box will be displayed.
     - Select the data type **Signed16**.
     - Select the quantity: 8.
     - Under tag name base enter **Set_temperature**.
     - Click **Ok**.
     - Column **Tag** displays **Set_temperature_1** to **Set_temperature_8**. If required, you can adapt the signal names in the column **Tag**.

11. Saving the configuration:
   - To save the configuration in the Edge Gateway, click **Project > Save** in the main menu of the PROFINET-configuration.
     - A message confirms that the configuration has been saved successfully.
   - Click **Ok**.
     - The PROFINET configuration and signal definition are saved in the Edge Gateway, but they are not activated yet.

12. Returning to Node-RED:
   - Return to the tab **Node-RED** in your browser.
   - To adopt a new/changed PROFINET configuration, click **Reconfigure interface**.
   - To add a new fieldbus interface, click **Add**.
     - or -
     - **Update** is offered as an alternative. Click **Update**, if only signal names have been extended or changed, whereas the PROFINET configuration has remained unchanged.
   - The display returns to the edit dialog.

13. Entering names:
   - Under Name enter a node name e.g. **MyInput**.
14. Selecting a signal:

- Use \( \text{Search} \) to open the signal list and select a **Signal** e.g. `input~fromController~Set_temperature_2`. If the **signal** is not displayed, close the edit dialog with **Done** and double-click to reopen the fieldbus node.

15. Finishing the fieldbus input node:

- Click **Done**.
  - The red triangle in the upper right corner has disappeared, i.e. the configuration of the fieldbus input node is completed, but not yet activated in the Edge Gateway.

16. Inserting a Debug node:

- Drag a **Debug** input node from the node library and drop it in the worksheet.

17. Connecting the nodes:

- To connect the **fieldbus** node with the **Debug** node, hold down the left mouse button and draw a connecting line (wire) from the output port of the fieldbus node to the input port of the Debug node.

18. Deploy:

- Click **Deploy** to transmit the nodes, that have so far existed in the editor only, to the device and activate them.
  - The flow is activated in the Edge Gateway.
  - As soon as the value of the signal changes, the Debug output will display the changed value/s and status information.
The example for copying

Note:
To configure the fieldbus (in this case PROFINET), it is simply not enough to copy this example. You have to perform steps 6 to 12 of the step-by-step instructions for this purpose.

```
{"id":"98832253.9224b","type":"fieldbus in","z":"ae0f59a7.16c008","name":"MyInput","FieldbusNodeVersion":"1.1.0","WrapperVersion":"1.1.0","WrapperCompileDate":"Sep 1 2016/08:37:12","MinExpectedNodeJSVersion":"4.5.0","selectedSignalPath":"input~fromController~Set_temperature_2","fieldbusObj":"e3a02a0f.a95938","x":179,"y":144,"wires": [{"id":"572ba7f6.f90c08","type":"debug","z":"ae0f59a7.16c008","name": "","active":true,"console":false,"complete":false,"x":361,"y":144,"wires":[]},{"id":"e3a02a0f.a95938","type":"fieldbus interface","z":"ae0f59a7.16c008","selectedConfigPath":"","currentFirmwareName":"PROFINET IO Device: Version(3.9, build 0, revision 6)","currentInterfaceName":"cifX0:PROFINET IO:Device","expectedInterfaceName":"cifX0:PROFINET IO:Device","expectedFirmwareName":"PROFINET IO Device: Version(3.9, build 0, revision 6)","expectedFirmwarePath":"","selectedChannelNumber":"2","selectedDeviceNumber":"1291105","selectedSerialNumber":"20726"}]
```

Testing the flow and displaying messages

For testing the flow you need a connection to a configured PROFINET IO Controller which cyclicly exchanges I/O-data with the Edge Gateway. At the PROFINET IO Controller you have to set output data so that the fieldbus input node can receive changed output data.

- Click the tab Debug in the sidebar.
- Set the output data at the PROFINET IO Controller: The example uses the signal **Set_temperature_2** and is byte 3 and 4 of module **16 receive byte (outputs)**. Byte 1 and 2 have been assigned by the configuration **Set_temperature_1**.
- The Debug node displays messages of the fieldbus input node as soon as the signal **Set_temperature_2** changes.

The following figure shows the value 123 for the signal **Set_temperature_2**. The value 0 for "Error" indicates that the cyclic PROFINET communication works without problems.

```
input~fromController~Set_temperature_2 : msg.payload : 
Object
{
"Error": 0, 
"DataType": "Signed16", 
"TimeStamp": "2016-09-08T16:33:34.375Z", 
"Value": 123 } 
```

*Figure 101: Message of the fieldbus input node (without error)*
The following figure displays a value for "Error" that is unequal to 0, i.e. the PROFINET communication does not work.

```json
    input-fromController->Set_temperature_2 : msg.payload :
        Object
            { "Error": -214697183, "DataType": "Signed16", "TimeStamp": "2016-09-08T16:31:51.232Z", "Value": 0 }
```

*Figure 102: Message of the fieldbus input node (with error)*
10.5 Example 5: Fieldbus output node

The fieldbus output node allows you to send data to the fieldbus, e.g. PROFINET, and uses signals to address this data. Before you can use the fieldbus output node, you have to configure the fieldbus and define the signals.

![Figure 103: Fieldbus output node](image)

This example uses the fieldbus output node together with two Inject nodes to send data to the fieldbus.

**Prerequisite**

1. A connection to the Edge Gateway is established (see section *Using the web browser to establish a connection with the Edge Gateway* [page 20]).
2. The Node-RED workspace is open.

**Step-by-step instructions**

1. Inserting the first Inject node:
   - Drag an **Inject** node from the node library and drop it in the worksheet.
2. Configuring Inject node:
   - To open the edit dialog, double-click on the **Inject** node.
   - The edit dialog for entering the parameters will be displayed.
   - Select from the **Payload** list the entry **number** and enter number **1**.
   - Enter in the field **Topic** the name of the topic, e.g. **Send1**.
   - Enter in the field **Name** the name for this node, e.g. **Send number 1**.
   - All parameters are entered.

3. Inserting the second Inject node:
   - Drag another **Inject** node from the node library and drop it in the worksheet.
4. Configuring the Inject node:
   - To open the edit dialog, double-click on the **Inject** node.
   - The edit dialog for entering the parameters will be displayed.
   - Select from the **Payload** list the entry **number** and enter number **2**.
   - Enter in the field **Topic** the name of the topic, e.g. **Send2**.
   - Enter in the field **Name** the name for this node, e.g. **Send number 2**.

   All parameters are entered.

5. Inserting the fieldbus output node:
   - Drag a fieldbus output node from the node library and drop it in the worksheet.
   - The red triangle the fieldbus node is displayed with indicates that the node still needs some more parameters which you have to configure in the following steps.
6. Showing the sidebar:
   - Show the sidebar using the keyboard shortcut Ctrl+spacebar or via the Node-RED menu View > Show Sidebar.
   - Click the tab Info.
   - Click the fieldbus output node to display its properties and a functional description in the tab Info.
   - The field Type of the tab Info shows the node type fieldbus.out.

7. Editing the fieldbus output node:
   - To open the edit dialog, double-click on the fieldbus node.
   - The edit dialog for entering the parameters will be displayed.

   ![Edit fieldbus out node](image)

8. Adding a fieldbus interface:
   - If you use an fieldbus node for the first time, (the fieldbus interface list displays Add new fieldbus interface), click Edit to add a new fieldbus interface.

9. Selecting the fieldbus interface:
   - Check whether F displays the entry PROFINET IO Device: Version ....
   - If it is not displayed, you first have to load the firmware for PROFINET IO Device in the control panel via the menu entry Network > Field (in the active mode).
10. Opening the fieldbus configurator (PROFINET configurator):
   - If Fieldbus interface does not yet display the entry PROFINET IO Device, repeat step 5.
   - If Fieldbus interface displays the entry PROFINET IO Device, click Open Fieldbus Configurator.
     - A new tab with the PROFINET configuration interface will be displayed.

11. Configuring PROFINET:
   - Click IO and Signal configuration in the configuration tree.
   - The page IO Configuration with the list of Available IO items will be displayed.
   - At first, double-click the entry 16 send byte (inputs).
   - Then, double-click the entry 16 receive byte (outputs).
   - The list of IO items displays 2 PROFINET modules.

12. Defining signal names for modules:
   - In the column Tag of the list IO items, click send_001 (index 001 named 16 send byte (inputs)).
   - Overwrite the available Tagname with the following new Tagname: toController.
   - In the column Tag of the list IO items, click receive_001 (index 002 named 16 receive byte (outputs)).
   - Overwrite the available Tagname with the following new Tagname: fromController.
   - The new Tagname which is part of the entire signal name is now displayed for each module.
13. Defining signals for module 1:
   - Select **001: 16 send byte (inputs)** in the configuration tree.
     - IO and signal configuration
     - **001: 16 send byte (inputs)**
     - **002: 16 receive byte (outputs)**
   - The signal configuration page with information on module 001 will be displayed.
   - Mark the available signal in the signal list.
   - Click **Delete selected items**.
   - Click **Add new signals**.
   - The **Add new signals** dialog box will be displayed.
   - Select the data type **Signed16**.
   - Select the quantity: 8.
   - Under tag name base enter **Temperature**.
   - Click **Ok**.
   - Column **Tag** displays **Temperature_1** to **Temperature_8**. If required, you can adapt the signal names in the column **Tag**.

14. Defining signals for module 2:
   - Select **002: 16 receive byte (outputs)** in the configuration tree.
     - IO and signal configuration
     - **001: 16 send byte (inputs)**
     - **002: 16 receive byte (outputs)**
   - The signal configuration page with information on module 002 will be displayed.
   - Mark the available signal in the signal list.
   - Click **Delete selected items**.
   - Click **Add new signals**.
   - The **Add new signals** dialog box will be displayed.
   - Select the data type **Signed16**.
   - Select the quantity: 8.
   - Under tag name base enter **Set_temperature**.
   - Click **Ok**.
   - Column **Tag** displays **Set_temperature_1** to **Set_temperature_8**. If required, you can adapt the signal names in the column **Tag**.

15. Saving the configuration:
   - To save the configuration in the Edge Gateway, click **Project > Save** in the main menu of the PROFINET configuration.
   - A message confirms that the configuration has been saved successfully.
   - Click **Ok**.
   - The PROFINET configuration and signal definition are saved in the Edge Gateway, but they are not activated yet.
16. Returning to Node-RED:
   - Return to the tab Node-RED in your browser.
   - To adopt a new/changed PROFINET configuration, click Reconfigure interface.
   - To add a new fieldbus interface, click Add - or - Update is offered as an alternative. Click Update, if only signal names have been extended or changed, whereas the PROFINET configuration has remained unchanged.
   - The display returns to the edit dialog.

17. Entering names:
   - Under Name enter a node name, e.g. MyOutput.

18. Selecting a signal:
   - Use to open the signal list and select a Signal e.g. output~toController~Temperature_2.
     If the signal is not displayed, close the edit dialog with Done and double-click to reopen the fieldbus node.

19. Finishing the fieldbus input node:
   - Click Done.
   - The configuration of the fieldbus input node is completed, but not yet activated in the Edge Gateway.

20. Connecting the nodes:
   - To connect the first Inject node with the fieldbus output node, hold down the left mouse button and draw a connecting line (wire) from the output port of the Inject node to the input port of the fieldbus node.
   - Connect the second Inject node with the fieldbus output node.
   - The nodes are connected.

21. Deploy:
   - Click Deploy to transmit the nodes, that have so far existed in the editor only, to the device and activate them.
   - The flow is activated in the Edge Gateway.
The example for copying

Note:
To configure the fieldbus (in this case PROFINET), it is simply not enough to copy this example. You have to perform steps 10 to 16 of the step-by-step instructions for this purpose.

Testing the flow and displaying messages

For testing the flow you need a connection to a configured PROFINET IO Controller which cyclicly exchanges I/O-data with the Edge Gateway. At the PROFINET IO Controller you have to display input data.

- Verify that the status of the fieldbus node MyOutput displays Communicating.
- Click the button to the left of Inject node 1.
  - Signal Temperature_2 is set to value 1 and transferred to the PROFINET IO Controller.
- Click the button to the left of Inject node 2.
  - Signal Temperature_2 is set to value 2 and transferred to the PROFINET IO Controller.
- At the PROFINET IO Controller, display the input data in a window.
11 Configuring and using the fieldbus node

11.1 Overview

The fieldbus input node allows you to receive data from the fieldbus system (e.g. PROFINET). The fieldbus output node allows you to send data to the fieldbus system. Each fieldbus node needs signals to address data. At first, configure the fieldbus system, then define the signals, and thereafter use signals for the fieldbus input node or the fieldbus output node.

### The fieldbus input node (fieldbus in)

**fieldbus input node** (fieldbus in) receives output data from the master:

Fieldbus master (e.g. PROFINET IO controller) → fieldbus input node

**Standard procedure**

1. Inserting the fieldbus input node
2. Configuring the fieldbus system (e.g. PROFINET)
3. Defining the signals
4. Configuring the fieldbus input node

### The fieldbus output node (fieldbus out)

**fieldbus output node** (fieldbus out) sends input data to the master:

Fieldbus output node → fieldbus master (e.g. PROFINET IO controller)

**Standard procedure**

1. Inserting the fieldbus output node
2. Configuring the fieldbus system (e.g. PROFINET)
3. Defining the signals
4. Configuring the fieldbus output node

Table 57: Standard procedure
The following table shows the sequence of the configuration steps:

1. Open fieldbus node
2. Open PROFINET configuration
3. Configure modules
4. Define signals
5. Project > Save
6. Fieldbus node (configured)
7. Reconfigure / Update
8. Deploy

Table 58: Configuration steps
11.2 Configuring the fieldbus and defining the signals

11.2.1 Creating a new fieldbus configuration

This section describes how to open the fieldbus configuration of the Edge Gateway from Node-RED using the PROFINET configuration as an example.

Prerequisite

The Node-RED workspace is open.

1. Inserting and opening the fieldbus node

   Ø Drag a fieldbus node from the node library and drop it in the workspace.

   Ø Double-click the fieldbus node.

   ⇒ The edit dialog **Edit fieldbus in node** will be displayed.

   ![Edit fieldbus in node dialog](image)

   **Figure 104: Edit dialog “Edit fieldbus in node”**

   Ø Click **Edit**.

   Ø The edit dialog **Add new fieldbus interface config node** will be displayed.

2. Opening the PROFINET configuration

   Ø Click the square to the right of fieldbus interface **.**
The dialog box *Add new fieldbus interface config node* opens. The fieldbus interface list is empty if no fieldbus interface has been defined yet.

![Diagram](image1.png)

*Figure 105: Dialog box "Add new fieldbus interface config node"

If one or several fieldbus interfaces have already been defined, the interface/s will be offered for selection in the list.

![Diagram](image2.png)

*Figure 106: Dialog box "Add new fieldbus interface config node"*
Determine the behavior of the output signals of the fieldbus node during the deploy process:

Check the box **Clear output on deploy** if the output signals of the fieldbus node, i.e. the data the master receives, are to be set to 0 during the deploy process. In this case, the Edge Gateway "cannot signal any valid data" to the master. Should the box for this option not be checked, the output data retains its last status during the deploy process. In this case, the master has no information that the Edge Gateway no longer processes the data received.

Click **Open**.

The user interface for the fieldbus configuration of the Edge Gateway will be opened in a new browser window: (the example shows the PROFINET configuration)
3. Configuring the modules

- Click **IO and signal configuration** in the configuration tree (left).
- The tables **Available IO items** and **IO items** will be shown in the display area and the workspace.

**Note:**
For more information on the tables **Available IO items** and **IO items** (example PROFINET), see **IO and signal configuration** [page 177].

- To select the inputs and outputs to be configured, double-click the appropriate entry in the upper table **Available IO items**, e.g. 4 byte input and 8 byte output.
  
  **Note:** Use the scroll bar to display further entries.

![Available IO items](image)

**Figure 108: Available IO items (Example in figure: PROFINET)**

- After each double-click, the corresponding entry for defining an input or output signal will be displayed immediately in a new line of the lower table **IO items**.

![IO items](image)

**Figure 109: IO items (Example: PROFINET)**
4. Defining signals

- As standard a signal definition is performed during which one single signal of the data type \textit{OctetString} will be defined which uses the entire available data length. If you wish to have another signal definition, you can delete this definition (with the button \textbf{Delete selected items}) and define new signals until the available data length is used up (with the button \textbf{Add new signals}).

- In the table columns \textbf{Tag} and \textbf{Description}, you can enter a short name and a description for each defined signal.

\textbf{Note:}
For more information on the signal definition, see section \textit{Defining signals (procedure)} [\textit{page 183}].

5. Saving the signal configuration

- Save your signal configuration via the menu function \textbf{Project > Save}.
- The configuration is prepared.
- Return to the Node-RED browser window that was originally used.

6. Storing the fieldbus configuration in NodeRED

- In the dialog \textit{Add new fieldbus interface config node} click the button \textit{Add}.
- This will transmit the fieldbus configuration into the device and update the signal definitions of the fieldbus node.

7. Deploy

- Perform a Deploy in the Node-RED. For this purpose, select one of the three options of the selection list \textit{Deploy} in the Node-RED window (top, right).
- The flow will thus be transmitted to the Edge Gateway, and the new configuration will be applied in the Edge Gateway.
Message received when the expected firmware deviates from the firmware actually determined

If you receive an error message similar to the one in the example when you open the user interface to the fieldbus configuration of the Edge Gateway, the expected firmware and the firmware actually determined do not match (in the example, PROFINET IO Device is expected, but EtherNet/IP Adapter is loaded):

![Error message](image)

In this case, check whether the desired firmware is really set in Fieldbus interface and in the control panel (menu Network > Field).

11.2.2 Changing the existing fieldbus configuration

This section describes how to change the existing fieldbus configuration (in this case PROFINET) of the Edge Gateway from Node-RED.

Prerequisites
1. The Node-RED workspace is open.
2. On the Node-RED screen, there must already be a flow whose workspace contains a fieldbus node. The node represents the previous fieldbus configuration of the Edge Gateway.

1. Opening the fieldbus node for changing
   - In the workspace, double-click on the fieldbus node to be changed. It is assumed that the node shown in the examples is preconfigured for PROFINET.

![Fieldbus node](image)
The edit dialog **Edit fieldbus in node** will be displayed.

![Image of edit fieldbus in node dialog](image1.png)

Figure 113: Dialog Edit fieldbus in node

The selection list **Fieldbus Interface** displays all fieldbus interfaces that are already configured. (In addition to that, there is an entry **Add new fieldbus interface** for adding a new fieldbus interface.)

![Image of edit fieldbus out node dialog](image2.png)

Figure 114: Dialog Edit fieldbus in node

- Select the interface to be changed (in the example this is `cifX0 PROFINET...`).
2. Opening the PROFINET configuration

- Click the square to the right of Fieldbus interface.
- The dialog box *Edit fieldbus interface node* opens.

![Edit fieldbus interface node dialog](image)

Determine the behavior of the output signals of the fieldbus node during the deploy process:

- Check the box **Clear output on deploy** if the output signals of the fieldbus node, i.e. the data the master receives, are to be set to 0 during the deploy process. In this case, the Edge Gateway "cannot signal any valid data" to the master. Should the box for this option not be checked, the output data retains its last status during the deploy process. In this case, the master has no information that the Edge Gateway no longer processes the data received.

- Click **Open fieldbus configurator**.

![Open fieldbus configurator button](image)
The user interface for fieldbus configuration of the currently loaded firmware of the Edge Gateway will be opened in a new browser window: If (as this example shows) PROFINET IO Device is the currently loaded firmware, the user interface for PROFINET configuration of the Edge Gateway will open, see figure:

![Figure 117: Start screen of the user interface for fieldbus configuration of the netIOT Edge Gateway (the example in the figure shows PROFINET)](image)

3. Configuring modules

- Make your changes in the fieldbus configuration. The possibilities you have for this purpose are described in the chapters Configuration tree [page 176] and Menu commands [page 173].

4. Defining signals

- If required, adapt the signal definitions as you desire.
5. Saving the signal configuration
   - Once you have made all desired changes, save your fieldbus configuration as described in section Project - Save [page 174]:
   - The steps to be made in the user interface for fieldbus configuration of the Edge Gateway are thus completed.
   - Return to the Node-RED browser window that was originally used.

6. Storing the fieldbus configuration in NodeRED
   - In the dialog Edit fieldbus interface node click the button Update.
   - This will transmit the fieldbus configuration (in this case PROFINET) into the device and update the signal definitions of the fieldbus node:

7. Deploy
   - Perform a Deploy in the Node-RED. For this purpose, select one of the three options of the selection list Deploy in the Node-RED window (top, right).
   - The flow will thus be transmitted to the netIOT Edge Gateway, and the new configuration will be applied in the Edge Gateway.
If the user interface cannot be started successfully, a message will be displayed that is similar to the following one:

```
Error in call to [checkExpectedFirmware]
Error number: [0x1]
Desc: [The firmware names do not match! expected is [PROFINET IO Device: Version(3.9, build 0, revision 6)] current is [EtherNet/IP Adapter: Version(2.10, build 0, revision 11)]]
Make sure you have the expected firmware loaded before proceeding!
```

Figure 119: Error message – Firmware does not match

This means that the expected firmware and the firmware actually determined do not match. In such a case, check your settings of the Fieldbus interface and the control panel (menu Network > Field)!
12 Configuring PROFINET and defining signals

12.1 User interface

The following figure and table describe the elements of the user interface.

![PROFINET user interface](image)

<table>
<thead>
<tr>
<th>Position number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Display area and workspace</td>
</tr>
<tr>
<td>(2)</td>
<td>Configuration tree</td>
</tr>
<tr>
<td>(3)</td>
<td>PROFINET configuration menu</td>
</tr>
</tbody>
</table>

Table 59: PROFINET configuration user interface

12.2 Menu commands

The menu bar of the PROFINET configuration of the netIOT Edge Gateway allows you to

- save the configuration in the Edge Gateway (see Project - Save [page 174]),
- download the GSDML-file from the Edge Gateway (see GSDML Download [page 174]),
- print the configuration (see Printing the configuration [page 174]),
- call the help page (see Help - Contents [page 175]), and
- display the software version of the configuration GUI (see Help - Information [page 175]).
12.2.1 Project - Save

To save the configuration in the device, proceed as follows:

- Click **Project > Save**
- The configuration is saved in the Edge Gateway.

12.2.2 GSDML Download

The GSDML file contains the PROFINET properties of the Edge Gateway and is required for configuring the PROFINET controller. Download the GSDML file from the Gateway so that you can use it in the configuration tool of the PROFINET controller.

To download the GSDML file, proceed as follows:

- Click **Download > GSDML**
- A dialog to save the GSDML file is displayed.
- Select a folder and click **Save**.
- Use the saved GSDML file to configure the PROFINET Controller.

12.2.3 Printing the configuration

To print configuration and signal definition, proceed as follows:

- Click **Print > Print configuration**
- The print dialog box will be displayed.
- Select a printer or an output file and set the printing parameters.
- The current configuration and signal definition will be printed.
12.2.4 Help - Contents

The Edge Gateway contains integrated documentation.

- Click Help > Contents.

- The integrated documentation is displayed

12.2.5 Help - Information

To display the version of the PROFINET configuration software of the netIOT Edge Gateway, proceed as follows:

- Click Help > Info.

- The version will be displayed.
12.3 Configuration tree

<table>
<thead>
<tr>
<th>Menu</th>
<th>Submenu</th>
<th>Description</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFINET configuration</td>
<td>-</td>
<td>Shows a note about how to set PROFINET name of station</td>
<td>PROFINET configuration [† page 176]</td>
</tr>
<tr>
<td>IO and signal configuration</td>
<td>-</td>
<td>Configuring input and output data.</td>
<td>IO and signal configuration [† page 177]</td>
</tr>
<tr>
<td></td>
<td>depends on configuration</td>
<td>Defining signal names.</td>
<td>Defining signals (procedure) [† page 183]</td>
</tr>
<tr>
<td>Signal definitions overview</td>
<td>-</td>
<td>Displaying defined signal names.</td>
<td>Signal definitions overview [† page 186]</td>
</tr>
<tr>
<td></td>
<td>Send signals</td>
<td>Displaying defined signal names.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Receive signals</td>
<td>Displaying defined input signal names.</td>
<td></td>
</tr>
<tr>
<td>GSDML file download</td>
<td>-</td>
<td>Download and displaying the GSDML file.</td>
<td>Download of the GSDML file [† page 187]</td>
</tr>
<tr>
<td>Help</td>
<td>Contents</td>
<td>Displaying help.</td>
<td>Help [† page 187]</td>
</tr>
<tr>
<td></td>
<td>Info</td>
<td>Displaying current software version.</td>
<td></td>
</tr>
</tbody>
</table>

Table 60: PROFINET configuration tree

12.3.1 PROFINET configuration

This page only contains a note on the setting of the PROFINET device name.

**PROFINET configuration**

*Note:* The PROFINET device name in factory state of this device is set to an empty string. The name must be assigned with a protocol known as PROFINET DCP from an engineering/standalone tool over any of its PROFINET ports.

Figure 121: Note: Name of station

**Note:**
In the factory setting of the Edge Gateway the PROFINET device name (Name of station) is an empty name. Via a PROFINET connection of the Edge Gateway you assign the PROFINET device name with an engineering tool of the PROFINET IO controller or a stand-alone tool. For this purpose the tools use the DCP protocol.
12.3.2 IO and signal configuration

On this page you configure the PROFINET input and output modules for the Edge Gateway. The Edge Gateway is a PROFINET IO device.

The upper table (Available IO items) shows the list of available input and output modules. The lower table (IO items) shows the PROFINET configuration and is empty at the beginning.

An “IO Item” corresponds to a PROFINET input or output module. The data length of PROFINET modules differs: Possible lengths are 1, 2, 3, 4, 8, 12, 16, 20, 32, 64, 128 and 256 bytes for input or output data. The configured modules (“IO Items” in the lower table) are the basis for the signal definition.

The table “Available IO Items” shows you the list of available input and output modules.

<table>
<thead>
<tr>
<th>Name</th>
<th>Length in bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 byte/inputs</td>
<td>1</td>
</tr>
<tr>
<td>2 byte/inputs</td>
<td>2</td>
</tr>
<tr>
<td>3 byte/inputs</td>
<td>3</td>
</tr>
<tr>
<td>4 byte/inputs</td>
<td>4</td>
</tr>
<tr>
<td>8 byte/inputs</td>
<td>8</td>
</tr>
<tr>
<td>12 byte/inputs</td>
<td>12</td>
</tr>
<tr>
<td>16 byte/inputs</td>
<td>16</td>
</tr>
</tbody>
</table>

Figure 122: List of the possible input and output modules

The table “IO items” shows you the configured PROFINET input or output modules.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the module index.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the module.</td>
</tr>
<tr>
<td>Tag</td>
<td>Editable short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Description</td>
<td>Editable description of the module</td>
</tr>
<tr>
<td>Length in bytes</td>
<td>Shows the module length in bytes.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address of the module (offset in bytes) in the input- and output data memory. The offset is calculated automatically.</td>
</tr>
</tbody>
</table>

Table 61: Contents of the table “IO items”
The column Tag is editable for each module. The Tag is an essential part of the signal name. The following characters are allowed only:

- Upper-case letters (A-Z),
- lower-case letters (a-z),
- numbers (0-9), and
- underscore.

Do not enter two or more underscores in succession.

To open the signal configuration of the respective module, double-click any line.

The following table lists the controls of the table IO Items.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Move up]</td>
<td>Moves the marked IO item (module) upward by one line.</td>
</tr>
<tr>
<td>![Move down]</td>
<td>Moves the marked IO item (module) downward by one line.</td>
</tr>
<tr>
<td>![Duplicate selected item]</td>
<td>Duplicates the marked IO item (module).</td>
</tr>
<tr>
<td>![Delete selected items]</td>
<td>Deletes the marked IO item (module).</td>
</tr>
<tr>
<td>![Send/Receive]</td>
<td>This selection allows you to filter the IO items.</td>
</tr>
<tr>
<td>![Aufsteigend sortieren]</td>
<td>Each column offers you sort and search functions.</td>
</tr>
<tr>
<td>![Absteigend sortieren]</td>
<td></td>
</tr>
<tr>
<td>![Filter]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Send/Receive</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>![Send]</td>
<td>Send/Receive shows you all IO items (modules).</td>
</tr>
<tr>
<td>![Receive]</td>
<td>Send shows you all send IO items (input modules).</td>
</tr>
<tr>
<td>![Receive]</td>
<td>Receive shows you all receive IO items (output module).</td>
</tr>
</tbody>
</table>

*Table 62: Controls of the table “IO Items”*
12.3.2.1  Signal definition page

On this page you can define the signals for the input and output modules of the PROFINET for the Edge Gateway. Signal names are required for the fieldbus node to address PROFINET data.

The table „IO item“ provides information on the selected IO item for which you define signals on this page.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the module index.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the module name.</td>
</tr>
<tr>
<td>Tag</td>
<td>Shows the short name required for the signal name.</td>
</tr>
<tr>
<td>Length in bytes</td>
<td>Shows the module length in bytes.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the module length in bits.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address of the module (offset in bytes) in the input and output data memory. The offset will be calculated automatically.</td>
</tr>
</tbody>
</table>

Table 63: Contents of table „IO item“

In the table Signals you can configure the signals for an IO item (module). The table shows you the current signal configuration and allows you to enter signal names, lengths and offset addresses.

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Tag</th>
<th>Description</th>
<th>Data type</th>
<th>Length in bits</th>
<th>Bit offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>SMsg_0</td>
<td>send_001</td>
<td>send_001</td>
<td>Unsigned8</td>
<td>16</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 124: Selected IO item (module) for which you define signals

Figure 125: List of the signal names of an IO item (module)
### Column name Description

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the module index.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the module name.</td>
</tr>
<tr>
<td>Tag</td>
<td>Editable short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Description</td>
<td>Editable module description.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the signal. You can set the data type only when you add a new signal.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the module length in bits.</td>
</tr>
<tr>
<td>Bit offset</td>
<td>Shows the configured start address of the module (offset in bytes) for a signal within a module.</td>
</tr>
</tbody>
</table>

**Table 64: Contents of the table „Signals“**

The column *Tag* is editable for each module. The *Tag* is an essential part of the signal name. The following characters are allowed only:

- Upper-case letters (A-Z),
- lower-case letters (a-z),
- numbers (0-9), and
- underscore.

Do not enter two or more underscores in succession.

The following table lists the controls of the table *Signals*.

<table>
<thead>
<tr>
<th>Controls</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>▲ Move up</td>
<td>Moves the marked signal upward by one line.</td>
</tr>
<tr>
<td>▼ Move down</td>
<td>Moves the marked signal downward by one line.</td>
</tr>
<tr>
<td>+ Add new signals</td>
<td>Adds a new signal. A dialog box for selecting the data type is displayed. You can set the data type of the signal in this dialog box only.</td>
</tr>
<tr>
<td>Delete selected items</td>
<td>Deletes the marked signal.</td>
</tr>
</tbody>
</table>

| ▲ Aufsteigend sortieren | Each column offers you sort and search functions. |
| ▼ Absteigend sortieren | To open the list to select from, click the column heading. To activate the filter function, enter the text in the filter input field and press the Enter key. You can use * as a wildcard for filtering. To deactivate the filter function again, delete any text you have entered in the filter input field and press the Enter key. |

**Table 65: Controls of the table „Signals“**
12.3.2.2 Data types for signal names

The following table lists the data types for signal names.

<table>
<thead>
<tr>
<th>Name of the data type</th>
<th>Description</th>
<th>Bit length</th>
<th>Value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bit list</td>
<td>List of individual bits The number of bits in a list must be a multiple of 8.</td>
<td>1</td>
<td>0 (false), 1 (true)</td>
</tr>
<tr>
<td>OctetString</td>
<td>Character sequence</td>
<td>8*(n+1)</td>
<td></td>
</tr>
<tr>
<td>Integer8</td>
<td>Short integer</td>
<td>8</td>
<td>-128 … 127</td>
</tr>
<tr>
<td>Integer16</td>
<td>Integer</td>
<td>16</td>
<td>-32768 … 32767</td>
</tr>
<tr>
<td>Integer32</td>
<td>Double integer</td>
<td>32</td>
<td>-2^{31} … +2^{31}-1</td>
</tr>
<tr>
<td>Unsigned8</td>
<td>Unsigned short integer</td>
<td>8</td>
<td>0 … 255</td>
</tr>
<tr>
<td>Unsigned16</td>
<td>Unsigned integer / Word</td>
<td>16</td>
<td>0 … 65535</td>
</tr>
<tr>
<td>Unsigned32</td>
<td>Unsigned double integer</td>
<td>32</td>
<td>0 … +2^{32}-1</td>
</tr>
<tr>
<td>Float32</td>
<td>Floating point</td>
<td>32</td>
<td>\approx \pm 10^{38}</td>
</tr>
<tr>
<td>Float64</td>
<td>Long Float</td>
<td>64</td>
<td>\approx \pm 10^{38}</td>
</tr>
</tbody>
</table>

Table 66: Data types for signal names

12.3.2.3 Structure of the signal names

Signal names address the fieldbus data.

General structure of the signal names

Signal names have the following structure:
- input~module_tag~signal_tag
- output~module_tag~signal_tag

For a bit list the signal names have the following structure:
- input~module_tag~bitlist_signal_tag
- output~module_tag~bitlist_signal_tag

Parts of the signal name

1. The prefix input or output is produced automatically.
2. The tilde (~) separates the prefix and the module_tag.
3. You can enter the name for module_tag as described in section Configuring I/O [page 182].
4. The tilde (~) separates the module_tag and the signal_tag or the module_tag and the bitlist_signal_tag.
5. You can enter the name for signal_tag or bitlist_signal_tag as described in section Defining signals (procedure) [page 183].
12.3.2.4 Configuring I/O

The upper table (*Available IO items*) displays the list of the possible (selectable) input and output modules. The lower table (*IO items*) displays the PROFINET configuration and is empty at the beginning.

1. Inserting the IO item (module):
   - To insert the required IO item into the „IO item“ list, double-click the IO item in the „Available IO item“ list.
   - The respective IO item will be inserted at the end of the list, if no „IO Item“ line has been marked, or before a marked „IO item“ line.

![Figure 126: List of the configured input and output modules](image)

2. Entering the tag for the IO item:
   - Enter a name for each IO item in the column *Tag* using the characters A-Z, a-z, 0-9 and _ (underscore) only.
   - The name (*Tag*) is used for the signal name to address the data.

3. Entering the description of the IO item (optional):
   - In the column *Description* you can enter a text (e.g. temperature sensor) which helps you describe the use of the data.
   - This description is used only if you print the signal list.

4. Configuring PROFINET:
   - Repeat steps 1-3 until all required IO items (modules) are inserted into the „IO Item“ list.
   - The PROFINET configuration is prepared.

5. Saving the configuration:
   - To save the PROFINET configuration in the Edge Gateway, click *Project > Save*.
   - The PROFINET configuration in the Edge Gateway is saved, but not active yet.
   - To activate the PROFINET configuration, you have to click *Reconfigure* in the fieldbus node as soon as you have finished the PROFINET configuration.

In the next step define the signal names as described in section *Defining signals (procedure)* [page 183].
12.3.2.5 Defining signals (procedure)

Each IO item (module) contains one or more bytes for input or output data. To enable the fieldbus node to access the input or output data, you have to select a signal at the fieldbus node. You can use the predefined signal name or define your own signal name.

The upper table (IO item) shows the IO item (module) for which you can define signals on this page. For defining signals, use the lower table (Signals).

Each IO item (module) already has a predefined signal. The predefined signal comprises and addresses the entire IO item (module). If you want to access a „part“ of the IO item, you can define a new signal for this purpose.

Example 1: The IO item contains 16 bytes. If you want to access each single byte, define 16 signals of data type byte each.

Example 2: The IO item contains 2 bytes that correspond to 16 digital input or outputs. If you want to access each single bit, define 16 signals of data type bit each.

Defining your own (new) signals

1. Selecting the IO item (module):
   - Select the IO item (module) for which you want to define signal names in the configuration tree under **IO and signal configuration**.
   - The selected IO item is displayed in the workspace.

2. Deleting the predefined signal:
   - Mark the predefined signal in the table **Signals**.
   - Click **Delete selected items**.
   - The predefined signal is deleted and you can define your own signals.
3. Adding new signals:
   - Click Add new signals.

   The dialog box Add new Signals for selecting the data type is displayed.

   ! Add new signals
   - Data type: Bit list
   - Quantity: 8
   - Tag name base: Sig
   - OK

4. Configuring signals:
   - Select the data type for the signal. The list of data types is described in section Data types for signal names [page 181].
   - Select the quantity. The possible values you can select depend on the selected data type and the number of input or output bytes to which no signal name has been assigned yet.
   - To have an identical beginning for all signal names, enter a text in the input field Tag name base. The extension "_1", "_2", etc. will be added automatically, if you have entered a value greater than 1 under "Quantity".
   - Click OK.
   - The new signal/s is/are defined and will be displayed in the table Signals.

5. Modifying signals subsequently:
   - If required, you can subsequently modify the signal names in the column Tag of the table Signals.
   - If required, you can enter a signal description in the column Description of the table Signals.

6. Defining signals:
   - Repeat steps 1-5 until you have defined all required signals.
   - The signal definition is prepared.
7. Saving the configuration and signal definition:
   - To save the configuration and signal definition in the Edge Gateway, click **Project > Save**.
   - The configuration and signal definition in the Edge Gateway is saved, but not active yet.
   - Click **Update** in the fieldbus node so that the fieldbus node reads the signal definition again.
   - To activate the configuration, click **Reconfigure** in the fieldbus node as soon as you have finished or changed the configuration.

The name in the column **Tag** is a part of the signal name and is described as **Signal_tag** or **Bitlist_signal_tag** in section *Structure of the signal names* [page 181].
12.3.3 Signal definitions overview

This page displays the list of the defined signals in the table „Send and Receive signals“. You can limit the display of the signals to send signals or receive signals. The signal names on these pages are not editable.

![Signal definitions overview](image)

Figure 127: List of the send and receive signals

If a module contains one or more signals, these signals will be displayed under the respective module.

<table>
<thead>
<tr>
<th>Column names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the index of the module (3-digit) or signal (1 to 3 digits).</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the module or signal.</td>
</tr>
<tr>
<td>Tag</td>
<td>Short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Data type</td>
<td>Shows the data type of the module or signal.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the length of the module or signal in bits.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address (offset in bytes) for a module in the input- or output data memory. The offset will be calculated automatically.</td>
</tr>
<tr>
<td>Bit offset</td>
<td>Shows the configured start address (bit offset) for a signal within a module.</td>
</tr>
</tbody>
</table>

Table 67: Columns of the table of the send and receive signals

You can print the table using **Print > Print configuration**.
12.3.4 Download of the GSDML file

On this page you can
- display the contents of the GSDML file and
- save the GSDML file on your PC (download).

The GSDML file contains the PROFINET properties of the Edge Gateway and is required for configuring the PROFINET controller. Download the GSDML file from the Gateway so that you can use it in the configuration tool of the PROFINET controller.

Display of the GSDML file

The GSDML file is not editable in this window. The contents of the GSDML file is represented in different colors:
- Violet: Names of elements.
- Black: Texts.
- Black and bold: Names of attributes.
- Red: Values of attributes.

Download of the GSDML file

- Click on the ZIP file. The ZIP file contains the device description file GSDML-V2.31-HILSCHER-NIOT-E-TPI51-EN-RE-xxxxxxxx.xml.
- Your PC displays a dialog for saving the GSDML file.
- Select a folder and click Save.
- Use the saved GSDML file to configure the PROFINET Controller.

12.3.5 Help

Contents

Page with the contents of the online help (currently empty)

Info

This page displays the version of the PROFINET configuration software.
13 Configuring EtherNet/IP and defining signals

13.1 User interface

The following figure and table describe the elements of the user interface.

![Figure 128: EtherNet/IP user interface](image)

<table>
<thead>
<tr>
<th>Position number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1)</td>
<td>Display area and workspace</td>
</tr>
<tr>
<td>(2)</td>
<td>Configuration tree</td>
</tr>
<tr>
<td>(3)</td>
<td>EtherNet/IP configuration menu</td>
</tr>
</tbody>
</table>

Table 68: EtherNet/IP configuration user interface

13.2 Menu commands

The menu bar of the EtherNet/IP configuration of the netIOT Edge Gateway allows you to

- save the configuration in the Edge Gateway (see Project - Save [page 189]),
- print the configuration (see Printing the configuration [page 190]),
- download the EDS file from the Edge Gateway (see EDS Download [page 189]),
- call the help page (see Help - Contents [page 190]), and
- display the software version of the configuration GUI (see Help - Information [page 190]).
13.2.1 Project - Save

To save the configuration data in the device, proceed as follows:

- Click **Project > Save**.

The configuration will be saved within the Edge Gateway.

13.2.2 EDS Download

The EDS file contains the Ethernet/IP properties of the Edge Gateway and is required for configuring the Ethernet/IP Scanner. Download the EDS file from the Edge Gateway in order to use it in the configuration tool of the Ethernet/IP Scanner.

To download the EDS file, proceed as follows:

- Click **Download > EDS**.

A dialog for saving the EDS file will be displayed.

- Select a folder and then click **Save**.
- Use the saved EDS file to configure the EtherNet/IP Scanner.
13.2.3 Printing the configuration

To print configuration and signal definition, proceed as follows:

- Click Print > Print configuration.

  ![Print configuration](image)

  The print dialog box will be displayed.

- Select a printer or an output file and set the printing parameters.

  The current configuration and signal definition will be printed.

13.2.4 Help - Contents

The Edge Gateway contains integrated documentation.

- Click Help > Contents.

  ![Contents](image)

  The integrated documentation is displayed.

13.2.5 Help - Information

To display the version of the EtherNet/IP configuration software of the netIOT Edge Gateway, proceed as follows:

- Click Help > Info.

  ![Info](image)

  The version will be displayed.
13.3 Configuration tree

<table>
<thead>
<tr>
<th>Menu</th>
<th>Submenu</th>
<th>Description</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>EtherNet/IP configuration</td>
<td>-</td>
<td>Setting IP address (using DHCP, BOOTP or direct input)</td>
<td>EtherNet/IP configuration [page 191]</td>
</tr>
<tr>
<td>IO and signal configuration</td>
<td>-</td>
<td>Configuring input and output data.</td>
<td>IO and signal configuration [page 192]</td>
</tr>
<tr>
<td>(depends on configuration)</td>
<td></td>
<td>Defining signal names.</td>
<td>Defining signals (procedure) [page 198]</td>
</tr>
<tr>
<td>Signal definitions overview</td>
<td>-</td>
<td>Displaying defined signal names.</td>
<td>Signal definitions overview [page 201]</td>
</tr>
<tr>
<td>Send signals</td>
<td></td>
<td>Displaying defined send signal names.</td>
<td></td>
</tr>
<tr>
<td>Receive signals</td>
<td></td>
<td>Displaying defined receive signal names.</td>
<td></td>
</tr>
<tr>
<td>EDS file download</td>
<td>-</td>
<td>Download of EDS file and contents of EDS file.</td>
<td>Download of the EDS file [page 202]</td>
</tr>
<tr>
<td>Help</td>
<td>Contents</td>
<td>Displaying online help.</td>
<td>Help [page 202]</td>
</tr>
<tr>
<td></td>
<td>Info</td>
<td>Displaying current software version.</td>
<td></td>
</tr>
</tbody>
</table>

Table 69: EtherNet/IP configuration tree

13.3.1 EtherNet/IP configuration

![IP Settings](image)

Figure 129: IP Settings

This page allows to define the method used for assigning an IP address to the Edge Gateway. This assignment can be accomplished either automatically via DHCP or BOOTP or manually by specifying the following information:

- IP address of Edge Gateway
- Network mask of Edge Gateway
- IP address of the gateway, to which the Edge Gateway is connected within the IP network
Parameters for setting the IP addresses

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Activate/deactivate DHCP protocol in order to configure the IP address via DHCP.</td>
</tr>
<tr>
<td>BootP</td>
<td>Activate/deactivate BootP protocol in order to configure the IP address via BootP.</td>
</tr>
<tr>
<td>Fixed Address</td>
<td>Activate/deactivate a fixed IP configuration</td>
</tr>
<tr>
<td>IP address</td>
<td>Specify the IP address of the Edge Gateway when configuring IP settings manually.</td>
</tr>
<tr>
<td>Network mask</td>
<td>Specify the network mask of the Edge Gateway when configuring IP settings manually.</td>
</tr>
<tr>
<td>Gateway</td>
<td>If necessary, specify the gateway address of the IP gateway here.</td>
</tr>
</tbody>
</table>

Table 70: Parameters for setting the IP addresses

If multiple options have been checked, these are evaluated in the following sequence:
1. DHCP
2. BOOTP
3. Fixed IP settings

13.3.2 IO and signal configuration

On this page, you configure the send and receive assemblies for EtherNet/IP within the Edge Gateway. The Edge Gateway works as an EtherNet/IP Adapter.

In the context of EtherNet/IP, an „IO Item“ corresponds to an EtherNet/IP send or receive assembly.

The upper table (Available IO items) displays the list of the possible (selectable) send and receive assemblies:
- The Send Assembly (IO item Send, Instance ID usually 100) acts as a producer and transmits data from the application to the network.
- The Receive Assembly (IO item Receive, Instance ID usually 101) acts as a consumer and transmits data from the network to the application.

At maximum, one send and one receive assembly can be configured. EtherNet/IP assemblies have a configurable data length: possible lengths range from 1 up to 504 Byte each for send and receive data (see columns Min_length and Max_length).

The lower table (IO items) displays the EtherNet/IP configuration and is empty at the beginning.
The configured assemblies („IO Items“ in the lower table) are the basis for the signal definition. They are displayed in the lower table below “IO Items”.

Figure 130: List of the possible send and receive assemblies

Figure 131: List of the configured send and receive assemblies

The table „IO items“ shows you the currently configured EtherNet/IP send and receive assemblies.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the index of the assembly.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the assembly.</td>
</tr>
<tr>
<td>Tag</td>
<td>Editable short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Description</td>
<td>Editable description of the assembly.</td>
</tr>
<tr>
<td>Data length</td>
<td>Contains the length of the assembly in bytes.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address of the assembly (offset in bytes) in the input- and output data memory. The offset is calculated automatically.</td>
</tr>
</tbody>
</table>

Table 71: Contents of the table „IO items“

The column Tag is editable for each assembly. The Tag is an essential part of the signal name. The following characters are allowed only:

- Upper-case letters (A-Z),
- lower-case letters (a-z),
- numbers (0-9), and
- the underscore.

Do not enter two or more underscores in succession.

To open the signal configuration of the respective assembly, double-click any line.
The following table lists the controls of the table *IO Items*.

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>☰ Move up</td>
<td>Moves the marked IO item (module) upward by one line.</td>
</tr>
<tr>
<td>☰ Move down</td>
<td>Moves the marked IO item (module) downward by one line.</td>
</tr>
<tr>
<td>☰ Duplicate selected item</td>
<td>Without function.</td>
</tr>
<tr>
<td>☰ Delete selected items</td>
<td>Deletes the marked IO item (module).</td>
</tr>
</tbody>
</table>

*Note:* This changes the EtherNet/IP configuration of the Edge Gateway and has to be taken into account when configuring the EtherNet/IP Scanner.

<table>
<thead>
<tr>
<th>Send/Receive</th>
<th>This selection allows you to filter the IO items.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Send/Receive shows you all IO items (modules).</td>
</tr>
<tr>
<td></td>
<td>• Send shows you all send IO items (input assemblies).</td>
</tr>
<tr>
<td></td>
<td>• Receive shows you all receive IO items (output assemblies).</td>
</tr>
</tbody>
</table>

Each column offers you sort and search functions.

To open the list to select from, click the column heading. To activate the filter function, enter the text in the filter input field and press the Enter key. You can use * as a wildcard for filtering. To deactivate the filter function again, delete any text entered in the filter input field and press the Enter key.

Table 72: Controls of the table *IO Items*”

13.3.2.1 Signal definition page

On this page, you can define the signals for the input and output assemblies of the EtherNet/IP for the Edge Gateway. Signal names are required for the fieldbus node to address EtherNet/IP data.

The table „IO item“ provides information on the selected IO item for which you define signals on this page.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the index of the assembly.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the assembly.</td>
</tr>
<tr>
<td>Tag</td>
<td>Editable short name required for the signal name.</td>
</tr>
<tr>
<td>Length in bytes</td>
<td>Contains the length of the assembly in bytes.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the length of the assembly in bits.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address of the assembly (offset in bytes) in the input- and output data memory. The offset is calculated automatically.</td>
</tr>
</tbody>
</table>

Table 73: Contents of the table „IO items”
In the table **Signals** you can configure the signals for one IO item (assembly). The table shows you the current signal configuration and allows you to enter signal names, lengths and offset addresses.

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Tag</th>
<th>Description</th>
<th>Data type</th>
<th>Length in bits</th>
<th>Bit offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sq_1</td>
<td>Sq_1_1</td>
<td></td>
<td>bit list</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>Sq_1_2</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>Sq_1_3</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td>Sq_1_4</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>Sq_1_5</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Sq_1_6</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>Sq_1_7</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>Sq_1_8</td>
<td></td>
<td></td>
<td>Bit</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Sq_2</td>
<td>Sq_2</td>
<td></td>
<td>string</td>
<td>2432</td>
<td>8</td>
</tr>
</tbody>
</table>

**Figure 133: List of the signal names of an IO item (assembly)**

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the index of the assembly.</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the assembly.</td>
</tr>
<tr>
<td>Tag</td>
<td>Editable short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Description</td>
<td>Editable description of the assembly.</td>
</tr>
<tr>
<td>Data type</td>
<td>Data type of the signal. You can set the data type only when you add a new signal.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the assembly length in bits.</td>
</tr>
<tr>
<td>Bit offset</td>
<td>Shows the configured start address for a signal within the assembly (offset in bytes).</td>
</tr>
</tbody>
</table>

**Table 74: Contents of the table „IO items“**

The column **Tag** is editable for each signal. The Tag is an essential part of the signal name. The following characters are allowed only:

- Upper-case letters (A-Z),
- lower-case letters (a-z),
- numbers (0-9), and
- the underscore.

Do not enter two or more underscores in succession.
The following table lists the controls of the table "Signals".

<table>
<thead>
<tr>
<th>Control</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>▲ Move up</td>
<td>Moves the marked signal upward by one line.</td>
</tr>
<tr>
<td>▼ Move down</td>
<td>Moves the marked signal downward by one line.</td>
</tr>
<tr>
<td>+ Add new signals</td>
<td>Adds a new signal. A dialog box for selecting the data type is displayed. You can set the data type of the signal only in this dialog box.</td>
</tr>
<tr>
<td>Delete selected items</td>
<td>Deletes the marked signal(s).</td>
</tr>
<tr>
<td>▲ Aufsteigend sortieren</td>
<td>Each column offers you sort and search functions.</td>
</tr>
<tr>
<td>▼ Absteigend sortieren</td>
<td>To open the list to select from, click the column heading. To activate the filter function, enter the text in the filter input field and press the Enter key. You can use * as a wildcard for filtering. To deactivate the filter function again, delete any text you have entered in the filter input field and press the Enter key.</td>
</tr>
</tbody>
</table>

Table 75: Controls of the table „Signals“

13.3.2.2 Data types for signal names

The following table lists the data types for signal names.

<table>
<thead>
<tr>
<th>Name of data type</th>
<th>Description</th>
<th>Length in bits</th>
<th>Allowed value range</th>
</tr>
</thead>
<tbody>
<tr>
<td>bit list</td>
<td>List of single bits</td>
<td>1</td>
<td>0 (false), 1 (true)</td>
</tr>
<tr>
<td>octetString</td>
<td>String of octets (bytes)</td>
<td>8*(n+1)</td>
<td></td>
</tr>
<tr>
<td>signed8</td>
<td>Short signed integer</td>
<td>8</td>
<td>-128 … 127</td>
</tr>
<tr>
<td>signed16</td>
<td>Signed integer</td>
<td>16</td>
<td>-32768 … 32767</td>
</tr>
<tr>
<td>signed32</td>
<td>Double signed integer</td>
<td>32</td>
<td>-2(^{31}) … +2(^{31})-1</td>
</tr>
<tr>
<td>unsigned8</td>
<td>Unsigned short integer</td>
<td>8</td>
<td>0 … 255</td>
</tr>
<tr>
<td>unsigned16</td>
<td>Unsigned integer / Word</td>
<td>16</td>
<td>0 … 65535</td>
</tr>
<tr>
<td>unsigned32</td>
<td>Unsigned double integer</td>
<td>32</td>
<td>0 … +2(^{32})-1</td>
</tr>
<tr>
<td>real32</td>
<td>Real (Floating point )</td>
<td>32</td>
<td>≈ +/- 10(^{38})</td>
</tr>
<tr>
<td>real64</td>
<td>Long real</td>
<td>64</td>
<td>≈ +/- 10(^{38})</td>
</tr>
</tbody>
</table>

Table 76: Data types for signal names
13.3.2.3 Structure of the signal names

Signal names address the fieldbus data.

**General structure of the signal names**

Signal names have the following structure:

- input~Modul_Tag~Signal_Tag
- output~Modultag~Signal_Tag

For a bit list, the signal names have the following structure:

- input~Modul_Tag~Bitlisten_Signal_Tag
- output~Modul_Tag~Bitlisten_Signal_Tag

**Parts of the signal name**

1. The prefix `input` or `output` is produced automatically.
2. The tilde (~) separates the prefix and the assembly_tag.
3. You can enter the name for `assembly_tag` as described in section Configuring I/O [page 197].
4. The tilde (~) separates the assembly_tag and the signal_tag or the assembly_tag and the bitlist_signal_tag.
5. You can enter the name for `signal_tag` or `bitlist_signal_tag` as described in section Defining signals (procedure) [page 198].

13.3.2.4 Configuring I/O

The upper table (Available IO items) displays the list of the possible (selectable) send and receive assemblies: The lower table (IO items) displays the EtherNet/IP configuration and is empty at the beginning.

1. Inserting the IO item (assembly):

   - To insert the required IO item into the „IO item“ list, double-click the IO item in the „Available IO item“ list.
   - The respective IO item will be inserted at the end of the list, if no „IO Item“ line has been marked, or before a marked „IO item“ line.

![IO Items Table](image)

**Figure 134: List of the configured send and receive assemblies**
2. Entering the tag for the IO item:
   - Enter a name for each IO item in the column Tag using the characters A-Z, a-z, 0-9 and _ (underscore) only.
   - The name (Tag) is used for the signal name to address the data.

3. Entering the description of the IO item (optional):
   - In the column Description you can enter a text (e.g. temperature sensor) which helps you describe the use of the data.
   - This description is used only if you print the signal list.

4. Configuring EtherNet/IP:
   - Repeat steps 1-3 until all required IO items (assemblies) are inserted into the „IO Item“ list.
   - The EtherNet/IP configuration is prepared.

5. Saving the configuration:
   - To save the EtherNet/IP configuration in the Edge Gateway, click Project > Save.
   - The EtherNet/IP configuration in the Edge Gateway is saved, but not active yet
   - To activate the EtherNet/IP configuration, you have to click Reconfigure in the fieldbus node as soon as you have finished the EtherNet/IP configuration.

In the next step define the signal names as described in section Defining signals (procedure) [page 198].

13.3.2.5 Defining signals (procedure)

Each IO item (assembly) contains one or more bytes for input or output data. To enable the fieldbus node to access the input or output data, you have to select a signal at the fieldbus node. You can use the predefined signal name or define your own signal name.

The upper table (IO item) shows the IO item (assembly) for which you can define signals on this page. For defining signals, use the lower table (Signals).

Each IO item (assembly) already has a predefined signal. The predefined signal comprises and addresses the entire IO item (assembly). If you want to access a „part“ of the IO item, you can define a new signal for this purpose.

Example 1: The IO item contains 16 bytes. If you want to access each single byte, define 16 signals of data type byte each.

Example 2: The IO item contains 2 bytes that correspond to 16 digital input or outputs. If you want to access each single bit, define 16 signals of data type bit each.
Defining your own (new) signals

1. Selecting the IO item:
   - Select the IO item for which you want to define signal names in the configuration tree under **IO and signal configuration**.
   - The selected IO item is displayed in the workspace.

2. Deleting the predefined signal:
   - Mark the predefined signal in the table **Signals**.
   - Click **Delete selected items**.
   - The predefined signal is deleted and you can define your own signals.

3. Adding new signals:
   - Click **Add new signals**.
   - The dialog box **Add new Signals** for selecting the data type is displayed.
   - Configuring signals:
     - Select the data type for the signal. The list of data types is described in section **Data types for signal names** [page 196].
     - Select the quantity. The possible values you can select depend on the selected data type and the number of input or output bytes to which no signal name has been assigned yet.
     - To have an identical beginning for all signal names, enter a text in the input field **Tag name base**. The extension "_1", "_2", etc. will be added automatically, if you have entered a value greater than 1 under "Quantity".
     - Click **OK**.
   - The new signal/s is/are defined and will be displayed in the table **Signals**.

4. Modifying signals subsequently:
   - If required, you can subsequently modify the signal names in the column **Tag** of the table **Signals**.
   - If required, you can enter a signal description in the column **Description** of the table **Signals**.

5. Defining signals:
   - Repeat steps 1-5 until you have defined all required signals.
   - The signal definition is prepared.
6. Saving the configuration and signal definition:

- To save the configuration and signal definition in the Edge Gateway, click **Project > Save**.
- The configuration and signal definition in the Edge Gateway is saved, but not active yet.
- Click Update in the fieldbus node so that the fieldbus node reads the signal definition again.
- To activate the configuration, click **Reconfigure** in the fieldbus node as soon as you have finished or changed the configuration.

The name in the column **Tag** is a part of the signal name and is described as **Signal_tag** or **Bitlist_signal_tag** in section *Structure of the signal names* [page 197].
13.3.3 Signal definitions overview

An overview on the current signal definitions is displayed on page “Signal Definitions Overview”. This page displays the list of the defined signals in the table „Send and Receive signals“. You can restrict the display of the signals to send signals or receive signals. The signal names on these pages are not editable.

![Signal definitions overview](image)

Figure 135: List of the send and receive signals

If an assembly contains one or more signals, these signals will be displayed under the respective assembly.

<table>
<thead>
<tr>
<th>Column names</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>Shows the index of the assembly (3-digit) or signal (1 to 3 digits).</td>
</tr>
<tr>
<td>Name</td>
<td>Shows the name of the assembly or signal.</td>
</tr>
<tr>
<td>Tag</td>
<td>Short name required for the signal name. The signal name addresses the data.</td>
</tr>
<tr>
<td>Data type</td>
<td>Shows the data type of the assembly or signal.</td>
</tr>
<tr>
<td>Length in bits</td>
<td>Shows the length of the assembly or signal in bits.</td>
</tr>
<tr>
<td>Byte offset</td>
<td>Shows the start address (offset in bytes) for an assembly in the input- or output data memory. The offset will be calculated automatically.</td>
</tr>
<tr>
<td>Bit offset</td>
<td>Shows the configured start address (bit offset) for a signal within an assembly.</td>
</tr>
</tbody>
</table>

Table 77: Columns of the table of the send and receive signals

You can print this table using Print > Print configuration.
13.3.4 Download of the EDS file

On this page you can
- display the contents of the EDS file and
- save the EDS file on your PC (download).

The EDS file contains the Ethernet/IP properties of the Edge Gateway and is required for configuring the Ethernet/IP Scanner. Download the EDS file from the Edge Gateway in order to use it in the configuration tool of the Ethernet/IP Scanner.

Display of the EDS file

The EDS file is not editable in this window.

Download of the EDS file

- Click the file with the extension .ZIP. The ZIP file contains the device description file HILSCHER NIOT-E-TPI51-EN-RE EIS V1.1.EDS
- A dialog for saving the ZIP file is displayed.
- Select Save and then click on OK.
- Select a folder and click Save.
- Extract the ZIP file to get the EDS file.
- Use this EDS file to configure the EtherNet/IP Scanner.

13.3.5 Help

Contents

Opens a page offering access to the contents of the online help system. See Help - Contents [page 190].

Info

This page only displays the current version of the EtherNet/IP configuration software. See Help - Information [page 190].
14 Edge Server

This chapter describes the Edge Server for Hilscher Edge Gateways Version 0.4.x and higher and explains the following topics:

- Communication, functions and internal structure of the Edge Server (see chapter *Function principle* [page 203])
- The *Edge Server Control Center* [page 208]
- The *Configuration of the Edge Server* [page 211]

14.1 Function principle

The Edge Server

- is a software component that has been developed by Hilscher and is executed under the Linux operating system of the Edge Gateway.
- enables secure and capsuled access from the IT-network to functions and protocols embedded within the Edge Gateway via a REST API. From the IT network means here, e.g. from the cloud or an application on a mobile device (e.g. a mobile phone) or also from the Edge Gateway itself via functions of the integrated Node-RED application.
- is a secure link between Web-applications and the OT-network that allows only indirect access to the OT-network via the provided Edge Server services and functions. In any way, direct access to the OT-network, which would counteract the security concept of the Edge Gateway is not possible.
- allows access to processes having been prepared in an automated way, e.g.
  - the scan of the field devices of the OT-network (automation network)
  - or the identification of the topology.
- is used for acquiring the status of the OT network and the field devices connected with this network and to provide it in JSON format for applications performing further processing.

14.1.1 Communication with IT-network and mobile devices

A REST API (also called RESTful API or RESTful interface) is a programming interface (API) which uses HTTP-requests like GET, PUT, POST and DELETE to access data between a web-based client and a server. The abbreviation REST stands for *Representational State Transfer*, API for Application Programming Interface.

The Edge Server uses a REST API to provide the client with its services. The client application uses this REST API to communicate with the Edge Server. The Edge Server communicates exclusively via the secure Protocol HTTPS limiting the communication to the services GET, POST, and PUT.
The following figure shows the Edge Server structure:

![Edge Server structure](image)

**Figure 136: Edge Server structure**

---

**Note:**
14.1.2 Communication with the OT-network

To communicate with the connected OT-network the Edge Server uses, among other protocols, the protocols SNMP (Simple Network Management Protocol) and ARP (Address Resolution Protocol). In addition to this, PROFINET protocols are used for communication with PROFINET devices, and an IO-Link UDP protocol transmitting encapsulated IO-Link data is used for communication with IO-Link master devices in the OT-network.

Note:
see Configuration of the Edge Server [§ page 211]
Concerning ARP, see https://de.wikipedia.org/wiki/Address_Resolution_Protocol.

14.1.3 Access rights to the REST API

Access to the REST API is governed by rights as follows:

1. In order to request data from the Edge Server using the REST API (HTTP method GET), read access rights are required.

2. In order to make changes within the Edge Server using the REST API (HTTP methods PUT and POST), write access rights are required.

3. You can check whether you have the required access rights via the menu entry User profile [§ page 81].

4. Granting read and right access rights requires administrator rights and is described in section Managing user roles [§ page 75].
### 14.1.4 Functions of the Edge Server

Via its REST API the Edge Server provides functions from the groups DEVICE (device handling), FILE (file handling), GATEWAY (information on gateway), PROGRESS (information on progress), TOPOLOGY (information on topology), and USER (user login) for access from the IT-network:

<table>
<thead>
<tr>
<th>Group</th>
<th>Function</th>
<th>Method (HTTPS)</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEVICE</td>
<td>Reading device information</td>
<td>GET</td>
<td>/device/info</td>
</tr>
<tr>
<td>device handling</td>
<td>Setting device information</td>
<td>POST</td>
<td>/topology/device/info</td>
</tr>
<tr>
<td></td>
<td>Detailed device list with additional information</td>
<td>GET</td>
<td>/device/list</td>
</tr>
<tr>
<td></td>
<td>Reading parameters</td>
<td>GET</td>
<td>/device/parameter</td>
</tr>
<tr>
<td></td>
<td>Writing parameters</td>
<td>POST</td>
<td>/device/parameter</td>
</tr>
<tr>
<td></td>
<td>Reading parameter list</td>
<td>GET</td>
<td>/device/parameter/list</td>
</tr>
<tr>
<td></td>
<td>Cyclic reading of process data or reading of parameters</td>
<td>GET</td>
<td>/device/processData</td>
</tr>
<tr>
<td></td>
<td>Cyclic writing of process data or writing of parameters</td>
<td>POST</td>
<td>/device/processData</td>
</tr>
<tr>
<td></td>
<td>List of process data</td>
<td>GET</td>
<td>/device/processData/list</td>
</tr>
<tr>
<td>FILE</td>
<td>File-upload (firmware, configuration, device description files, general data)</td>
<td>PUT</td>
<td>/file</td>
</tr>
<tr>
<td>GATEWAY</td>
<td>Information on installed packages and internal modules</td>
<td>GET</td>
<td>/gateway/package/info</td>
</tr>
<tr>
<td></td>
<td>Access to product data</td>
<td>GET</td>
<td>/gateway/info</td>
</tr>
<tr>
<td>PROGRESS</td>
<td>Request of progress information on running tasks</td>
<td>GET</td>
<td>/progress</td>
</tr>
<tr>
<td>TOPOLOGY</td>
<td>List of topology scan results within a defined period</td>
<td>GET</td>
<td>/topology/networkScanList</td>
</tr>
<tr>
<td></td>
<td>Output of a network status list</td>
<td>GET</td>
<td>/topology/networkStatus/list</td>
</tr>
<tr>
<td>USER</td>
<td>Authentication of the app</td>
<td>POST</td>
<td>/user/login</td>
</tr>
<tr>
<td></td>
<td>Logout request</td>
<td>POST</td>
<td>/user/logout</td>
</tr>
</tbody>
</table>

Table 78: Functions of the Edge Server

---

**Note:**

For a detailed description of the functions and parameters provided by the netIOT Edge Server API, see [http://www.netiot.com/external/stkit-doku/](http://www.netiot.com/external/stkit-doku/).
14.1.5 Internal structure of the Edge Server

The following figure shows the environment of the Edge Server for the Edge Gateways:

![Edge Server environment](image)

*Figure 137: Edge Server environment*

The following figure shows the internal structure of the Edge Server for the Edge Gateways:

![Internal structure of the Edge Server](image)

*Figure 138: Internal structure of the Edge Server*
14.2 Edge Server Control Center

14.2.1 Starting the Edge Server Control Center

The Edge Server Control Center is a tool for commissioning and administrating the Edge Server. It can be started via the netIOT Edge Server Icon within the Edge Gateway Manager (see Edge Gateway Manager [page 22]).

Figure 139: netIOT Edge Server icon within the Edge Gateway Manager

14.2.2 Functions

The Edge Server Control Center provides the following functions:

- Information on the Edge Server
- Configuration of the Edge Server
- List of services
- Scan protocols of field devices
14.2.3 Service list

The service list contains valuable information on the components of the Edge Server. To display the service list, proceed as follows:

- Select entry Service list in menu Services.
- The service list is displayed. Each listed service represents an installed component of the Edge Server.

![Edge Server Control Center](image)

Figure 140: Edge Server Control Center

The left part of the window lists all services with their name and a symbol indicating the current state of operation of the service.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Green Circle" /></td>
<td>Running</td>
</tr>
<tr>
<td></td>
<td>Service is running</td>
</tr>
<tr>
<td><img src="image" alt="Blue Circle" /></td>
<td>Info</td>
</tr>
<tr>
<td></td>
<td>For this service, an informative message has been stored (see below).</td>
</tr>
<tr>
<td><img src="image" alt="Yellow Circle" /></td>
<td>Warning</td>
</tr>
<tr>
<td></td>
<td>For this service, a warning message has been stored.</td>
</tr>
<tr>
<td><img src="image" alt="Red Circle" /></td>
<td>Error</td>
</tr>
<tr>
<td></td>
<td>For this service, an error message has been stored.</td>
</tr>
</tbody>
</table>

Table 79: Symbols for the state of operation in the service list
You can select one of these services in the left part of the window. A blue bar marks the currently selected service. The right part of the window additionally shows the following data concerning the selected service:

- Name of service / component
- **Operating status** (displayed as text)
- Last information
- Version
- Description
- Information on the author
14.3 Configuration of the Edge Server

For the configuration of the Edge Server, the following two steps are necessary in this order:
1. The configuration of the used IP address area
   (see The configuration of IP address area [page 211])
2. The configuration of field devices
   (see Selecting the protocols to scan for field devices [page 214])

14.3.1 The configuration of IP address area

To configure the IP address range used, proceed as follows:
- Open the menu System in the Edge Server Control Center and select menu entry Configuration.
- The configuration screen page displays the settings for the server configuration.

Figure 141: Server configuration
- Click **Scanning** in the left column.
- The screen page for the scan settings (**Scanning**) is displayed:

![Figure 142: Configuration of the scan settings](image)

- Here you can define several address ranges. To create a new input line for entering an IP-address range click **Add new scan IP range**. Make sure, that an entered IP-address range falls into the IP-address range of the OT-network to allow the scanning of the connected devices.
- Under **Start address** enter the start address of the IP-address range, e.g. 192.168.0.1.
- Under **End address** enter the end address of the IP-address range, e.g. 192.168.0.8.

---

**Note:**
For configuring the Edge Gateway, we strongly recommend you to set **cifX0** to the IP-address 192.168.0.8. For the correct configuration of the IP-address range, the entered IP-addresses must fall into the range of the cifX0 network and its IP-address.
To save your settings in the Edge Server, click **Save changes**.

Now, the screen page for the scan settings should look like that:

![Figure 143: Correct configuration of the scan settings](image-url)
14.3.2 Selecting the protocols to scan for field devices

The protocols used to scan the individual field devices in the set IP-address range are set in the Edge Server Control Center.

To activate or deactivate individual protocols:

- Select menu entry **Scanning** in menu **Services** within the Edge Server Control Center
- The protocol configuration will be displayed:

![Scan protocol configuration](image)

**Figure 144: Scan protocol configuration**

- On this page, you can set the scan protocols to be active or inactive individually for each address of the configured IP-address range. For the basic registration of the field devices, you should activate the scan protocols SNMP and ARP.

**Note:**
Check the boxes IO-Link or PROFINET for IP-addresses in the configured IP-address range only if the corresponding IO-Link master devices or PROFINET devices are connected and configured.

- To save your settings in the Edge Server, click **Save changes**
- Thus, your scan protocol settings of the field devices are saved.
15 Isolated application execution with Docker

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

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

15.1 Docker, Image, Container and Repository

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

Docker

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

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

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

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

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

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

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

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

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

---

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

---

**Container**

A container is a runtime instance of an image.

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

A container consists of:

- a Docker image,
- a runtime environment, and
- a standard command architecture.

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

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

---

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

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

15.2 Prerequisites for working with Docker

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

1. Read and write access rights at Docker UI are required. To examine whether you have these, you can use menu entry User profile [page 81]. Granting read and right access rights requires administrator rights and is described in section Managing user roles [page 75].

2. The Docker service must have been started on the Edge Gateway. In order to examine whether the service has been started or to start it, open the service list within the Control Panel as described in Starting, stopping and configuring services [page 71].
15.3 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).

15.3.1 The portainer.io interface

The portainer.io interface serves:
- to add new containers
- to configure the containers
- to provide functions for controlling the application execution such as Start, Stop, Kill, Restart, Pause, Resume, and Remove

15.3.2 Commissioning

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

- Open the service list within the Control Panel as described in Starting, stopping and configuring services [page 71].
- In the service list (to the left), select the entry Docker.
- At the Autostart option, click at the radio button enabled in order to set up automatic starting of the Docker service.
- Click at Apply.
- A security confirmation prompt appears and asks you whether you really request to change the state of Docker.
- Answer it with Yes.
- The button Apply is now displayed in red color.
- If the current status equals Stopped: Click at Start.
- The security confirmation prompt appears again.
- Again, answer with Yes.
- The status changes from Stopped to Running and the yellow icon at the Docker service within the services list changes to green, see figure.
Thus, the Docker service is started and the formerly deactivated grey tile for Docker within the Edge Gateway Manager (Docker Management) is activated enabling you to invoke the GUI portainer.io.

**Note:**
We urgently recommend you to set up an initial admin user account now. Otherwise, a user admin supplied with administrator rights will be established without any password, when the docker service is started. A potential offender could use this user account as an open entrance door. In order to avoid this, immediately continue to perform the initial set-up of portainer.io (Starting the portainer.io interface for working with the containers [→ page 220]) as subsequently described.
15.3.3 Starting the portainer.io interface for working with the containers

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

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

- Open the Edge Gateway Manager.
  In this context, see Calling the Edge Gateway Manager [page 22].
- Click the tile Docker Management in the Edge Gateway Manager.

![Docker Management tile](image)

*Figure 146: Tile Docker in the Edge Gateway Manager*

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

![Portainer.io login screen](image)

*Figure 147: Initial call of portainer.io*
portainer.io includes its own user administration working independently from the one implemented within Control Panel. Therefore, follow these steps precisely:

You are urged to specify the user name and twice the password for the first user with administrator rights.

In the field **Username** an arbitrary username can be specified. By default, **admin** is specified there as this is the only pre-defined username. We recommend you to use it and not to change it.

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

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

- Click at **Create user**.

Now, the following happens:

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

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

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

Figure 148: portainer.io - initial screen Home (Endpoints)
Click at entry "Dashboard" in the blue menu on the leftside.

The page „Dashboard“ of portainer.io is displayed.

Figure 149: View of portainer.io dashboard

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

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

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

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

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

Table 80: Functions for working with containers
15.3.5 Example: Execute web server NGINX as a container

NGINX is an open source web server. As an example, how to execute an arbitrary application on the Edge Gateway using Docker, this section instructs you how to correctly execute the NGINX Webserver within a Docker container on the Edge Gateway.

Note:

Prerequisite

The following prerequisite has to be fulfilled:

- The GUI portainer.io is opened (see Starting the portainer.io interface for working with the containers [page 220]).

Steps

- Click at the lightblue button Add container on page „Container list“.
- The page “Create container” will be displayed.

Figure 151: NGINX Example- Screen page “Create container”

- Within field Name specify the name of your container, for instance MyFirstContainer.
- In field Image specify the name of the image to be executed within the container in the Image configuration area: nginx.
- The image is automatically searched for within the official Docker registry and loaded from the NGINX Repository having been installed there. The http address of the NGINX Repository is https://hub.docker.com/_/nginx/.
Always set swich **Always pull image** within area **Image configuration** to position **On** (i.e. switch is on the right position). This causes the image to be loaded automatically prior to the start. Manual loading via the option „Images“ of portainer.io is not necessary any more.

- Click at button **map additional port** in order to configure a network port transformation between the container and the Linux Host-System. Within the container, the default network port 80 of NGINX can be redirected to port 8080 and so be made accessible for the web browser.

- The fields **host** and **container** are shown on the page „Container list“.

- **Field host**: Here, specify the port to address NGINX via web browser. i.e. port 8080.

- **Field container**: Here, specify the port to be used by NGINX within the container, i.e. port 80.

- If necessary, adjust the **Advanced options** according to the documentation of the container to be started (here: Documentation of NGINX, [https://hub.docker.com/_/nginx/](https://hub.docker.com/_/nginx/)). However, for the current simple example, no further settings are required.

- Click at the light blue button **Start container**.

- Now, the container has been readily configured and set up for executing the NGINX web server. At first, Docker will load the image from the Registry (Duration approx. 2-3 Minuten), store it within the Edge Gateway and then transform it into a container. Then, this container will appear within the Container List and its status will change to **running**.

**Test**

In order to check for the correct installation of NGINX, proceed as follows:

- Specify the following address within the address line of your web browser:
  
  http://<IP address of your device>:8080

- If NGINX has been installed correctly, the NGINX splash screen will appear.

### 15.3.6 User management

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

**Note:**

The integrated user management of portainer.io may not be confused with the user management of the control panel.
15.3.6.1 Open screen Users

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

To open the screen *Users*, proceed as follows:
- If the portainer.io interface has not yet been opened, click at tile *Docker Management* within the Edge Gateway Manager.
- The portainer.io interface is opened.

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

*Figure 152: portainer.io - entry page Home*

- Within the darkblue menu on the left side click at Users in the SETTINGS area.
- The page for the user management within portainer.io is displayed (Users>User Management).
Figure 153: portainer.io - Page Users > User management

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

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

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

![User details](image)

*Figure 154: portainer.io - Display of User Details*

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

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

© Hilscher 2017 – 2019
15.3.7 Registry management

There are two ways to create a registry:

- Via Quay.io (pre-configured)
- As Custom Registry

15.3.7.1 Creating a registry with Quay.io

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

- Open the Edge Gateway Manager, if it is not already open. Also see Calling the Edge Gateway Manager [page 22].
- If the portainer.io interface has not yet been opened, click at tile Docker Management within the Edge Gateway Manager.

The portainer.io interface is opened.

- Within the darkblue menu on the left side, click at Registries within the SETTINGS area.
- The page Registries (Registry management) for the registry management in portainer.io is displayed.
This page consists of at least two areas:

- DockerHub
- Registries

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

Here you can enter the username within field **Username** and the password within field **Password**.
Within this area, you can find the buttons **Add Registry** and **Remove** for adding and removing registries (see *Creating a registry with Quay.io* [page 229], *Setting up a custom registry* [page 232] and *Deleting a registry* [page 236]) and a table of all current registries. This table consists of the following three columns:

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

Table 81: Meaning of columns of table of all current registries

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

To establish a custom registry, proceed as follows:

- Open the Edge Gateway Manager, if it is not already open. See *Calling the Edge Gateway Manager* [page 22].
- If the portainer.io interface has not yet been opened, click at tile **Docker Management** within the Edge Gateway Manager.

![Figure 160: Tile Docker within the Edge Gateway Manager](image1)

The portainer.io interface is opened.

![Figure 161: portainer.io - entry page Home](image2)

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

Figure 162: portainer.io - Page Registries (Registry management)

This page consists of at least two areas:

- DockerHub
- Registries

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

Figure 163: portainer.io - Page Registries (Registry-Management), Authentication has been activated

Here you can enter the username within field Username and the password within field Password.
Within this area, you can find the buttons **Add Registry** and **Remove** for adding and removing registries (see *Creating a registry with Quay.io* [page 229], *Setting up a custom registry* [page 232] and *Deleting a registry* [page 236]) and a table of all current registries. This table consists of the following three columns:

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

*Table 82: Meaning of columns of table of all current registries*

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

![Portainer.io - Page Create registry (Registries > Add registry)](image1)

- Click at the large blue button **Custom registry** at the right side.

![Portainer.io - Page Create registry (Registries > Add registry), Custom registry selected](image2)
Specify the name to be displayed at the node within field **Name**.

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

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

Click at the blue button **Add Registry**.

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

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

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

To delete a registry, proceed as follows:

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

15.3.7.4 Open registry access management

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

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

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

- The page Registry access (Registries > [Registry name] > Access Management) is being opened:
15.3.7.5 Registry access management

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

In area Access management users and teams of users are accepted or rejected.
Isolated application execution with Docker

To do so, there are two separate tables Users and teams (for users and teams without authorization) and Authorized Users and teams (for authorized users and teams).

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

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

15.3.8 Stack management

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

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

15.3.8.1 Preparations for creating a stack

Prerequisite: The GUI portainer.io is already opened.

Figure 169: portainer.io - Entry page Home

➤ Within the darkblue menu on the left side click at Stacks.

DDR The page Create Stacks (Stacks > Add Stack) for the stack management in portainer.io is displayed.
This page consists of at least four separate areas:

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

2. **Area Environment**
   If you want, you can additionally define environment variables here, which are supplied to the stack at execution time. See section *Set environment variables* [page 240].

3. **Area Access control**
   If you want, you can additionally define access restrictions here in order to allow access only to administrators, specific users or groups of users. See section *Define access control* [page 240].

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

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

- To do so, for each variable click exactly once a the dark grey button add environment variable.

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

15.3.8.3 Define access control

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

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

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

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

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

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

To create a stack via the integrated web editor:

- Proceed as described in Preparations for creating a stack [page 238].
- If necessary, set environment variables as described in Set environment variables [page 240].
- If required, restrict access as described in Define access control [page 240].
- In area Build method choose option Web Editor (left).

The additional area Web Editor is now displayed containing an editor window for entering Docker compose files according to the syntax described within the above mentioned documentation. It looks like this:

![Figure 171: Portainer.io - Creating a stack via web editor](image-url)
15.3.8.5 Creating a stack via upload of a Docker compose file

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

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

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

- Proceed as described in *Preparations for creating a stack* [page 238].
- If necessary, set environment variables as described in *Set environment variables* [page 240].
- If required, restrict access as described in *Define access control* [page 240].
- In area **Build method** choose option Upload (in the center).
  - The additional area **Upload** is now displayed. See the following figure.

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

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

To create a stack using GitHub:

- Proceed as described in Preparations for creating a stack [page 238].
- If necessary, set environment variables as described in Set environment variables [page 240].
- If required, restrict access as described in Define access control [page 240].
- In area Build method choose option Repository (right).
- The additional area Git Repository is now displayed.

![Portainer.io - Creating a stack using GitHub](image)

- Specify the URL of the Git repository in field Repository URL.
- Specify the reference of the Git repository in field Repository URL.
- Specify the path to your Docker compose file in field Compose path.
- All specifications for GitHub have been made now.
- Click at Deploy the stack in area Actions in order to create the stack
- If the stack has been created successfully, an according message is displayed.
16 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.

16.1 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.
1. The server has two keys
   - the **private key**
   - the **public key**
     - Both keys have a relation.
2. The client receives the certificate from the server which contains even the public key and a signature.
3. The client verifies the signature of the certificate using trustworthy certificates stored in its local directory of trustworthy certificates. Only if the authenticity check is ok, the client uses the received public key.
4. The client encrypts the message using the public key and sends the encrypted message to the server.
5. The server decrypt the message using his private key.
6. Client and server continue its encrypted communication using **one** new created protected transmitted key (symmetric communication).
16.2 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.

16.2.1 Structure of a certificate according to X.509

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

According to this, a certificate has the following constituents:

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

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

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

Table 83: Attributes concerning the issuer and owner of the certificate zum Zertifikats-Aussteller und Zertifikats-Inhaber
16.2.2 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.
16.2.3 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.
16.3 Use cases

<table>
<thead>
<tr>
<th>Use case</th>
<th>Details in section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root certificates</td>
<td>Use case 1: Verification of the authenticity of the communication partner (Server) [page 249]</td>
</tr>
<tr>
<td>Server certificates and private keys</td>
<td>Use case 2: Server certificates for Edge Gateway services [page 250]</td>
</tr>
<tr>
<td>Client certificates and private keys</td>
<td>Use case 3: Client certificates for specific servers [page 252]</td>
</tr>
</tbody>
</table>

*Table 84: Overview use cases*

16.3.1 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).

![Diagram](image.png)

*Figure 175: 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 247] 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 254].

16.3.2 Use case 2: Server certificates for Edge Gateway services

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

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

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

The file name for the private key is key.pem. The file name for the certificate is cert.pem. Both files have the PEM file format, see section File formats for certificate and key files [page 248].
The Nginx server is the access point for several Edge Gateway services. The pair of files (private key `key.pem` and the related server certificate `cert.pem`) is used among other services for the following services:

- Edge Gateway Manager
- Node-RED
- Edge Server and Rest API
- Portainer.io (Docker)
- AIN Connector

<table>
<thead>
<tr>
<th>Folder name (contains the pair of files)</th>
<th>Edge Gateway service</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx</td>
<td>The Nginx server is the access point for several Edge Gateway 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:</td>
</tr>
<tr>
<td>opcuaserverforedge</td>
<td>OPC UA for Edge</td>
</tr>
</tbody>
</table>

Table 85: 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 257].
16.3.3 Use case 3: Client certificates for specific servers

The Edge Gateway (client) is able to authenticate itself to a specific server. For this, you can store client certificates in the Edge Gateway. This use case extends use case 1 (The Edge Gateway uses server certificates, to identify a server and to encrypt messages). In case, you want to ensure that the server identifies the Edge Gateway, the Edge Gateway has to send his client certificate to the server.

From the point of view of the Edge Server, the client certificates relate to outbound HTTPS and OPC UA connections.

For each server the Edge Gateway should send an certificate for authentication, you have to upload a pair of files (private key `xyz_key.pem` and certificate `xyz_cert.pem`). The prefix (here `xyz_`) has to be identical for each file pair (you can freely choose the prefix).

You can upload and use client certificates in the Edge Gateway for Node-RED only.

---

**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.

---

**Node-RED**

You can upload several pairs of files (one pair for one server) in order to use the client certificate functionality. Use the same prefix for one pair of files. For each server, a separate pair of files is necessary.

For a Node-RED node, you need to use a path to the certification file as well as to the private key file:

- Mark the entry `xyz_cert.pem` and then click **Copy path**. Use the copied path in the Node-RED node for the path to the certificate.
- Mark the entry `xyz_key.pem` and then click **Copy path**. Use the copied path in the Node-RED node for the path to the private key.
**OPC UA Client in Node-RED**

The Edge Gateway is able to communicate with exactly one OPC UA Server using the authentication based-on client certificates. The file names are

- Certificate file `node-opcuaclient_cert.pem` and
- File with the private key `node-opcuaclient_key.pem`

For a OPC UA Client node, you need to use a path to the certification file as well as to the private key file.

- **Mark the entry** `node-opcuaclient_cert.pem` and then click **Copy path**. Use the copied path in the OPC UA Client node for the path to the certificate.

- **Mark the entry** `node-opcuaclient_key.pem` and then click **Copy path**. Use the copied path in the OPC UA Client node for the path to the private key.

How to work with client certificates, describes section *Working with client authentication certificates for outbound connections* [page 265].
16.4 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 249]. 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

16.4.1 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 79]).
- 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 246]).
16.4.2 Upload a trustworthy certificate into the Edge Gateway

To upload a trustworthy certificate from a file in *.pem format [page 248] 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 79]).
- 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 246] 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 248].
  - 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 53] for the changes to become effective.
16.4.3 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 79]).
- 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 246]).
- 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 248] format.

16.4.4 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 79]).
- 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 246]).
- 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.
16.5 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 250].

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.
16.5.1 Uploading 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 53] consequently if you upload a server certificate for communication with the HTTPS Server, Node-RED [page 83], the Edge Server [page 203] or the REST API [page 205] from a file into the Edge Gateway.
16.5.1.1 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 79]).

- 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 248].

- 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.
16.5.1.2 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 79]).

➢ 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 248].

➢ 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.
16.5.2 Working with certificates for HTTPS and OPC UA Server

16.5.2.1 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 260] beschrieben.

16.5.2.2 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 79]).
- 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 248] format.
16.5.2.3 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 79]).
- 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.
16.5.3 Working with key files for HTTPS and OPC UA Server

16.5.3.1 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 259].
16.5.3.2 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 79]).
- 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.
16.6 Working with client authentication certificates for outbound connections

For outbound connections, client authentication certificates can be stored within the Edge Gateway, as described in Use case 3: Client certificates for specific servers [page 252].

Here, a 1:n relation between server and client applies (i.e. per client one certificate and one corresponding key is stored for each server to which a secure connection shall be established).

In this context, the following actions can be performed for a specific server:

1. Uploading of a pair of client authentication certificate and corresponding key file from *.pem [page 248] files into the Edge Gateway
2. Download of a client authentication certificate from the Edge Gateway into a *.pem [page 248] file
3. Removing a certificate for client authentication for a specific server on the Edge Gateway
4. Copying the path to a certificate for client authentication for a specific server on the Edge Gateway
5. Downloading a key file for client authentication for a specific server from the Edge Gateway
6. Removing a key file for client authentication for a specific server on the Edge Gateway
7. Copying the path to a key file for client authentication for a specific server for further use within Node-RED on 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.
16.6.1 Uploading a pair of certificate and corresponding key file for client authentication

As certificates and the corresponding private keys are logically connected very tightly 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 node-opcuaclient_key.pem first and then the certificate file node-opcuaclient_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 be present, when this check takes place.

Note:
For the changes to become effective, it is necessary to reboot the Edge Gateway consequently if you upload a certificate for client authentication from a file into the Edge Gateway.
16.6.1.1 Step 1: Uploading a key file for client authentication for a specific server into the Edge Gateway

To upload a key file for client authorization for a specific server from a file into the Edge Gateway, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- In window Certificates, select the entry node-opcuaclient_key.pem below node-red.
- 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 248].
- The key file is checked for correctness. In case of error, a message indicating a defective file type is displayed 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 confirmation prompt whether you really intend to replace the key file is displayed.
- If you are really sure not to need the currently stored 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. A message is displayed indicating that the upload has been completed and the Edge Gateway requires a restart.
16.6.1.2 Step 2: Uploading a certificate for client authentication for a specific server on the Edge Gateway

To upload a certificate for client authentication for a specific server from a file into the Edge Gateway, proceed as follows:

- Select option **Service certificates** within selection list (Selection list for certificate type [page 79]).

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

- In window **Certificates**, select the entry **node-opcuaclient_cert.pem** below **node-red**.

- The window **Certificate Viewer** now shows the data of **node-opcuaclient_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 248].

- 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. 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 file is checked for matching the stored key file. In case of error, a message indicating that the certificate does not match with the private key is displayed.

- If this check is passed, the selected file is uploaded into the Edge Gateway. During this, the former certificate file is **irreversibly** overwritten. Thus, there is no possibility to recover this file if there is no suitable backup available. A message is displayed and informs you, that uploading has been completed and the Edge Gateway requires a restart.
16.6.2 Working with certificates for client authentication

16.6.2.1 Uploading a certificate for client authentication for a specific server into the Edge Gateway

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

To upload a certificate for client authentication for a specific server from a file into the Edge Gateway, proceed as described in section Step 2: Uploading a certificate for client authentication for a specific server on the Edge Gateway [page 268].

16.6.2.2 Downloading a certificate for client authentication for a specific server from the Edge Gateway

To download a certificate for client authentication for a specific server from the Edge Gateway into a file, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- In window Certificates, select the entry node-opcuaclient_cert.pem below node-red.
- The window Certificate Viewer now shows the data of node-opcuaclient_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 248] format.
16.6.2.3 Removing a certificate for client authentication for a specific server on the Edge Gateway

To remove a certificate for client authorization for a specific server from the Edge Gateway, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- Select option Service certificates from the selection list (Selection list for certificate type).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- In window Certificates select the entry node-opcuaclient_cert.pem below node-red.
- The window Certificate Viewer now shows the data of node-opcuaclient_cert.pem.
- Click at button Delete in the header of window Certificates.
- A confirmation prompt is displayed whether you really intend to delete the certificate file node-opcuaclient_cert.pem.
- If you are really sure not to need the currently stored certificate any longer, click at Yes.
- The selected certificate file is removed from the Edge Gateway.

**Note:**

If a 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 certificate is uploaded to the same position within the tree structure as that of the removed certificate.
16.6.2.4 Copying the path to a certificate for client authentication for a specific server on the Edge Gateway

To copy the path to the certificate for client authentication for a specific server, proceed as follows:

- Select option *Service Certificates* from the selection list (*Selection list for certificate type* [page 79]).
- Within window *Certificates*, a tree structure is displayed instead of the list of preinstalled certificates.
- In window *Certificates*, select the entry *node-opcuaclient_cert.pem* below *node-red*.
- The window *Certificate Viewer* now shows the data of *node-opcuaclient_cert.pem*.
- Click at button *Copy path* in the header of window *Certificate Viewer*.
- The path is now copied into the Windows clipboard. You can use it within Node-RED to open and configure the corresponding element within Node-RED.
16.6.3 Working with key files for client authentication

16.6.3.1 Uploading a key file for client authentication for a specific server into the Edge Gateway

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

To upload a key file for client authentication for a specific server from a file into the Edge Gateway, proceed as described in section Step 1: Uploading a key file for client authentication for a specific server into the Edge Gateway [page 267].
16.6.3.2 Downloading a key file for client authentication for a specific server from the Edge Gateway

To download a key file for client authentication for a specific server from the Edge Gateway into a file, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- In window Certificates, a tree structure is displayed.
- In window Certificates, select the entry node-opcuaclient_key.pem below node-red.
- The window Certificate Viewer now shows the data of node-opcuaclient_key.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 248] format.

16.6.3.3 Removing a key file for client authentication for a specific server on the Edge Gateway

To remove a key file for client authentication for a specific server from the Edge Gateway, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- In window Certificates, select the entry node-opcuaclient_key.pem below node-red.
- The window Certificate Viewer now shows the data of node-opcuaclient_key.pem.
- Click at button Delete in the header of window Certificates.
- A confirmation prompt whether you really intend to delete the key file node-opcuaclient_key.pem 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 Gateway.

Note:
If a key file 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.
16.6.3.4 Copying the path to a key file for client authentication for a specific server on the Edge Gateway

You might need the path to the certificate for client authentication for a specific server later on within Node-RED in order to open and configure the corresponding element.

To copy the path to a key file for client authentication for a specific server from the Edge Gateway into a file, proceed as follows:

- Select option Service certificates within selection list (Selection list for certificate type [page 79]).
- Within window Certificates, a tree structure is displayed instead of the list of preinstalled trustworthy certificates.
- In window Certificates, select the entry node-opcuaclient_key.pem below node-red.
- The window Certificate Viewer is empty now (Text No data).
- Click at button Copy path in the header of window Certificate Viewer.
- The path to the key file is now copied into Windows clipboard. You can use it within Node-RED to open and configure the corresponding Node-RED element.
17 Technical data

17.1 Technical data NIOT-E-TPI51-EN-RE

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
<td><strong>Part number</strong> 1321.400</td>
</tr>
<tr>
<td><strong>Application</strong></td>
<td>For IoT applications with limited quantity scale. Data mining and data processing/distribution with Node-RED scope of functions only.</td>
</tr>
<tr>
<td><strong>Functions</strong></td>
<td><strong>Services for IoT data mining and distribution</strong> Node-RED: MQTT client, OPC UA client MQTT broker</td>
</tr>
<tr>
<td></td>
<td><strong>Data connection, processing and cloud connectivity</strong> Node-RED, IBM Watson, Azure IoT Hub</td>
</tr>
<tr>
<td></td>
<td><strong>Web services (REST)</strong> OT network scan, diagnostics, device status</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td><strong>Boot</strong> Booting of signed software</td>
</tr>
<tr>
<td></td>
<td><strong>Access</strong> HTTPS, TLS</td>
</tr>
<tr>
<td><strong>Processors</strong></td>
<td><strong>CPU</strong> Broadcom BCM2837 1.2 GHz, 64 bit, 4 cores</td>
</tr>
<tr>
<td></td>
<td><strong>Communication controller</strong> netX 51</td>
</tr>
<tr>
<td><strong>Software</strong></td>
<td><strong>Operating system</strong> Security Enhanced Linux</td>
</tr>
<tr>
<td><strong>Memory</strong></td>
<td><strong>RAM</strong> 1 GB DDR3 RAM</td>
</tr>
<tr>
<td></td>
<td><strong>SD card</strong> 8 GB MLC NAND (3000 w/e), Micro SD card (sealed): 4 GB application, 4 GB backup</td>
</tr>
<tr>
<td><strong>Power</strong></td>
<td><strong>Voltage</strong> 24 V DC ± 6 V DC For UL conform usage: powered by class 2 source, Overvoltage Category II</td>
</tr>
<tr>
<td></td>
<td><strong>Current (at 24 V DC)</strong> Without USB: 170 mA (typical) With USB: max. 400 mA</td>
</tr>
<tr>
<td></td>
<td><strong>Power of the used power supply unit</strong> Min. 4.2 W (no USB) 9 W (USB with 1 A)</td>
</tr>
<tr>
<td></td>
<td><strong>Connector</strong> 3-pin terminal block (3.5 mm)</td>
</tr>
<tr>
<td><strong>IT interface</strong></td>
<td><strong>Interface type</strong> 1 x 10/100 Mbit, Mircochip LAN9514</td>
</tr>
<tr>
<td></td>
<td><strong>LAN connector</strong> 1 x RJ45 socket</td>
</tr>
<tr>
<td><strong>OT interface</strong></td>
<td><strong>Interface type</strong> 10BASE-T/100BASE-TX, potential free, Hilscher netX 51</td>
</tr>
<tr>
<td></td>
<td><strong>Connector</strong> 2 x RJ45 socket</td>
</tr>
<tr>
<td></td>
<td><strong>OT networks</strong> PROFINET I/O-Device, EtherNet/IP Adapter</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td><strong>USB</strong> 4 x USB 2.0, max. 500 mA max. 1 A over all USBs, Type A</td>
</tr>
<tr>
<td></td>
<td><strong>Wi-Fi</strong> 1 x WiFi, single band 2.4 GHz IEEE 802.11n (BCM43438), fixed antenna</td>
</tr>
<tr>
<td></td>
<td><strong>Display connection</strong> 1 x HDMI (inaktive)</td>
</tr>
<tr>
<td><strong>Display</strong></td>
<td><strong>LED display</strong> 8 LEDs (2 programmable)</td>
</tr>
<tr>
<td><strong>Real-time clock</strong></td>
<td><strong>Buffering</strong> Capacitor buffered, max. 7 days backup, maintenance free</td>
</tr>
</tbody>
</table>
### Technical data

<table>
<thead>
<tr>
<th>Parameter</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environment</strong></td>
<td></td>
</tr>
<tr>
<td>Ambient temperature range for operation</td>
<td>-20°C ... +60°C</td>
</tr>
<tr>
<td>Ambient temperature range for storage</td>
<td>-40°C ... +85°C</td>
</tr>
<tr>
<td>Humidity range</td>
<td>10 % … 95 % (95 % at 40°C) relative humidity (non-condensing)</td>
</tr>
<tr>
<td>Pollution degree</td>
<td>For UL compliant usage: The device must be used in a pollution degree 2 environment.</td>
</tr>
<tr>
<td>Altitude</td>
<td>Max. 2000 m</td>
</tr>
<tr>
<td>Use</td>
<td>Indoor use</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td></td>
</tr>
<tr>
<td>Dimensions</td>
<td>140 mm (H) x 35 mm (W) x 105 mm (L)</td>
</tr>
<tr>
<td>Weight</td>
<td>400 g</td>
</tr>
<tr>
<td>Housing</td>
<td>Metal</td>
</tr>
<tr>
<td>Mounting</td>
<td>DIN top hat rail</td>
</tr>
<tr>
<td>Degree of protection</td>
<td>IP20</td>
</tr>
<tr>
<td><strong>Approvals</strong></td>
<td></td>
</tr>
<tr>
<td>FCC ID (Federal Communications Commission)</td>
<td>2ANEG0001</td>
</tr>
<tr>
<td>IC (Industry Canada)</td>
<td>24152-0001</td>
</tr>
<tr>
<td><strong>UL certification</strong></td>
<td></td>
</tr>
<tr>
<td>UL-File-Nr</td>
<td>E221530 Vol D1</td>
</tr>
<tr>
<td><strong>Conformity</strong></td>
<td></td>
</tr>
<tr>
<td>RoHS</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Conformance with EMC directives</strong></td>
<td></td>
</tr>
<tr>
<td>CE sign</td>
<td>Yes</td>
</tr>
<tr>
<td>Emission</td>
<td>EN 55011:2009</td>
</tr>
<tr>
<td>Immunity</td>
<td>IEC 61000-6-2/3, EN 61131-2</td>
</tr>
<tr>
<td>Electrostatic discharge (ESD) (air and contact discharge method)</td>
<td>EN 61000-4-2</td>
</tr>
<tr>
<td>Fast transient interferences (Burst)</td>
<td>EN 61000-4-4</td>
</tr>
<tr>
<td>Surge voltage</td>
<td>EN 61000-4-5</td>
</tr>
<tr>
<td><strong>Tests</strong></td>
<td></td>
</tr>
<tr>
<td>Shock</td>
<td>IEC 60068-2-27 Ea</td>
</tr>
<tr>
<td>Vibration</td>
<td>IEC 60068-2-6 Fc</td>
</tr>
</tbody>
</table>

*Table 86: Technical data NIOT-E-TPI51-EN-RE*
## 17.2 Technical data PROFINET IO Device

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of cyclic input data</td>
<td>1440 Bytes</td>
</tr>
<tr>
<td>Maximum number of cyclic output data</td>
<td>1440 Bytes</td>
</tr>
<tr>
<td>Maximum number of submodules</td>
<td>255 submodules per Application Relation at the same time, 1000 submodules can be configured</td>
</tr>
<tr>
<td>Multiple Application Relations (AR)</td>
<td>The Stack can handle up to 2 IO-ARs, one Supervisor AR and one Supervisor-DA AR at the same time.</td>
</tr>
</tbody>
</table>
| Supported protocols | RTC – Real Time Cyclic Protocol, Class 1 (unsynchronized), Class 3 (synchronized)  
RTA – Real Time Acyclic Protocol  
DCP – Discovery and configuration Protocol  
CL-RPC – Connectionless Remote Procedure Call  
LLDP – Link Layer Discovery Protocol  
SNMP – Simple Network Management Protocol  
MRP – MRP Client |
| Topology recognition | LLDP, SNMP V1, MIB2, physical device |
| Identification & Maintenance | Read and write of I&M1-4 |
| Minimum cycle time | 1 ms for RT_CLASS_1  
250 µs for RT_CLASS_3 |
| IRT Support | RT_CLASS_3 |
| Media redundancy | MRP client is supported |
| Additional features | DCP, VLAN- and priority-tagging, Shared Device |
| Baud rate | 100 MBit/s |
| Data transport layer | Ethernet II, IEEE 802.3 |
| PROFINET IO specification | V2.2 (legacy startup) and V2.3 (but advanced startup only for RT) are supported. |
| Limitations | RT over UDP not supported.  
Multicast communication not supported.  
DHCP is not supported.  
FastStartUp is not supported.  
The amount of configured IO-data influences the minimum cycle time that can be reached.  
Only 1 Input-CR and 1 Output-CR are supported.  
Using little endian (LSB-MSB) byte order for cyclic process data instead of default big endian (MSB-LSB) byte order may have a negative impact on minimum reachable cycle time.  
System Redundancy (SR-AR) and Configuration-in-Run (CiR) are not supported.  
Max. 255 submodules can be used simultaneously within one specific Application Relation.  
Advanced Startup according Profinet specification V2.3 is NOT yet supported for IRT.  
As there is no official certification available for Profinet IO specification V2.3 at the time of release of the stack there is no guarantee that this implementation will pass such a certification once it is available. |
| Reference to stack version | V3.9 |

*Table 87: Technical data PROFINET IO RT IRT Device Protocol*
17.3 Technical data EtherNet/IP Adapter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of input data</td>
<td>504 bytes</td>
</tr>
<tr>
<td>Maximum number of output data</td>
<td>504 bytes</td>
</tr>
<tr>
<td>I/O Connection (implicit)</td>
<td>1 Exclusive Owner, 1 Listen Only, 1 Input only</td>
</tr>
<tr>
<td>I/O Connection type</td>
<td>'Cyclic', minimal 1 ms*</td>
</tr>
<tr>
<td></td>
<td>* depending on number of connections and number of input and output data used</td>
</tr>
<tr>
<td>UCMM</td>
<td>Supported</td>
</tr>
<tr>
<td>Predefined standard objects</td>
<td>Identity-Objekt</td>
</tr>
<tr>
<td></td>
<td>Message-Router-Objekt</td>
</tr>
<tr>
<td></td>
<td>Assembly-Objekt</td>
</tr>
<tr>
<td></td>
<td>Connection-Manager-Objekt</td>
</tr>
<tr>
<td></td>
<td>Ethernet-Link-Objekt</td>
</tr>
<tr>
<td></td>
<td>TCP/IP-Objekt</td>
</tr>
<tr>
<td>Topology</td>
<td>Tree, Line, Ring</td>
</tr>
<tr>
<td>DLR (Device Level Ring)</td>
<td>Beacon based 'Ring Node'</td>
</tr>
<tr>
<td>ACD (Address Conflict Detection)</td>
<td>Supported</td>
</tr>
<tr>
<td>DHCP</td>
<td>Supported</td>
</tr>
<tr>
<td>BOOTP</td>
<td>Supported</td>
</tr>
<tr>
<td>Baud rate</td>
<td>10 and 100 MBit/s</td>
</tr>
<tr>
<td>Data transport layer</td>
<td>Ethernet II, IEEE 802.3</td>
</tr>
<tr>
<td>Switch function</td>
<td>Supported</td>
</tr>
<tr>
<td>integrated</td>
<td>Quick Connect not supported.</td>
</tr>
<tr>
<td></td>
<td>The Edge Gateway is designed for cyclic data exchange. Acyclic communication for user data transfer can not be used.</td>
</tr>
<tr>
<td></td>
<td>CIP Sync Services are not implemented.</td>
</tr>
<tr>
<td></td>
<td>TAGs are not supported.</td>
</tr>
<tr>
<td>Reference to stack version</td>
<td>V2.10</td>
</tr>
</tbody>
</table>

*Table 88: Technical data EtherNet/IP Adapter protocol*
18 Approvals

18.1 Federal Communications Commission (FCC)

**FCC ID: 2ANEG0001**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

*Figure 177: FCC label*

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
18.2 Industry Canada (IC)

This device contains license-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s license-exempt RSS(s). Operation is subject to the following two conditions: (1) This device may not cause interference. (2) This device must accept any interference, including interference that may cause undesired operation of the device.

L’émetteur/récepteur exempt de licence contenu dans le présent appareil est conforme aux CNR d’Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes : (1) L’appareil ne doit pas produire de brouillage; (2) L’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

Cet équipement est conforme aux limites d'exposition aux radiations IC CNR-102 établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec une distance minimale de 20 cm entre le radiateur et votre corps.

![Figure 178: IC on the device label](image-url)
19 Decommissioning, dismounting and disposal

19.1 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.

19.2 Removing device from top hat rail

- Before dismounting the Edge Gateway from the top hat rail, first remove the power supply cable and all data cables from the device.
- Put a screw driver into the slot of the latch at the bottom of the device.
- To disengage the lock of the hook, pull down the latch with the screw driver.
- Take the device off the top hat rail.

19.3 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.
20 Appendix

20.1 Legal notes

Copyright

© Hilscher Gesellschaft für Systemautomation mbH
All rights reserved.

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

Important notes

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

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

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

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

It is hereby expressly agreed upon in particular that any use or utilization of the hardware and/or software in connection with
- Flight control systems in aviation and aerospace;
- Nuclear fusion processes in nuclear power plants;
- Medical devices used for life support and
- Vehicle control systems used in passenger transport
shall be excluded. Use of the hardware and/or software in any of the following areas is strictly prohibited:
- For military purposes or in weaponry;
- For designing, engineering, maintaining or operating nuclear systems;
- In flight safety systems, aviation and flight telecommunications systems;
- In life-support systems;
- In systems in which any malfunction in the hardware and/or software may result in physical injuries or fatalities.

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

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

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

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

Costs of support, maintenance, customization and product care

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

Additional guarantees

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

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

The customer hereby expressly acknowledges that this document contains trade secrets, information protected by copyright and other patent and ownership privileges as well as any related rights of Hilscher Gesellschaft für Systemautomation mbH. The customer agrees to treat as confidential all of the information made available to 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: Edge Gateway communication structure .......................................................... 8
Figure 2: Dimensions ..................................................................................................... 11
Figure 3: NIOT-E-TPI51-EN-RE LED positions .............................................................. 14
Figure 4: Gateway state LEDs ...................................................................................... 15
Figure 5: Default settings of the Ethernet network connectors ....................................... 19
Figure 6: Device label: Hostname .................................................................................. 20
Figure 7: Edge Gateway Manager .................................................................................. 22
Figure 8: Edge Gateway Manager - Setting the administrator password ..................... 26
Figure 9: Security error message of the Internet Explorer ............................................... 28
Figure 10: Security error message of the Firefox browser (1) ......................................... 28
Figure 11: Security error message of the Firefox browser (2) ......................................... 28
Figure 12: Firefox dialog box: Adding exceptional safety rule .......................................... 29
Figure 13: Security error message of Google Chrome (1) .............................................. 30
Figure 14: Security error message of Google Chrome (2) .............................................. 30
Figure 15: Main menu of the Control Panel .................................................................. 31
Figure 16: Page Info Center .......................................................................................... 33
Figure 17: License Manager with license for the passive mode of operation .................. 35
Figure 18: License information in window Details ......................................................... 36
Figure 19: Message after the transfer of the license file into the Edge Gateway ................ 37
Figure 20: Control Panel, page System > Syslog ............................................................. 38
Figure 21: Time configuration page ............................................................................... 42
Figure 22: Port settings ................................................................................................. 44
Figure 23: Backup and recovery .................................................................................... 46
Figure 24: Warning message ......................................................................................... 47
Figure 25: Backup in progress ....................................................................................... 47
Figure 26: Backup and recovery .................................................................................... 48
Figure 27: Recovery dialog ........................................................................................... 48
Figure 28: Security query prior to system recovery from internal backup file .................. 49
Figure 29: Backup and recovery .................................................................................... 50
Figure 30: Recovery dialog (external source) ................................................................ 51
Figure 31: Message prior to starting recovery from external backup ............................ 51
Figure 32: Backup and restore when backup file is present ........................................... 52
Figure 33: Safety query before deletion of local backup ................................................. 52
Figure 34: Backup and Restore .................................................................................... 53
Figure 35: Reboot safety query ..................................................................................... 53
Figure 36: Warning for consequences of shutdown ....................................................... 54
Figure 37: Default LAN-configuration .......................................................................... 55
Figure 38: LAN configuration(cifX0 activated) ............................................................... 57
Figure 39: Wi-Fi (default setting) .................................................................................. 58
Figure 40: Wi-Fi modes of operation in selection list Mode ........................................... 58
List of figures

Figure 41: Wi-Fi operating mode: Access point................................................................. 59
Figure 42: Wi-Fi operating mode: Client ........................................................................ 61
Figure 43: Routes ........................................................................................................... 64
Figure 44: Defined Routes ............................................................................................ 66
Figure 45: Create new route ......................................................................................... 66
Figure 46: Define new route .......................................................................................... 67
Figure 47: Firewall ......................................................................................................... 68
Figure 48: Hostname ....................................................................................................... 70
Figure 49: List of default services .................................................................................. 71
Figure 50: OPC-UA Server for Edge settings within the Control Panel, page Network>Field................................................................. 72
Figure 51: Page for configuring roles................................................................................ 75
Figure 52: User account page ......................................................................................... 77
Figure 53: Public Key Infrastructure for managing of certificates ................................ 78
Figure 54: Certificate type selection list ......................................................................... 79
Figure 55: Certificate Viewer ........................................................................................ 80
Figure 56: Info page ........................................................................................................ 81
Figure 57: User profile page .......................................................................................... 81
Figure 58: Dialog "Edit user account" .......................................................................... 82
Figure 59: Comparison of the physical and logic view ................................................... 84
Figure 60: Wiring the nodes ........................................................................................... 84
Figure 61: Node-RED workspace ................................................................................... 86
Figure 62: Node-RED user interface .............................................................................. 87
Figure 63: Node ............................................................................................................... 88
Figure 64: Menu Deploy ................................................................................................. 92
Figure 65: Dialog "Edit dashboard tab node" .................................................................. 97
Figure 66: Dialog "Edit dashboard tab node" .................................................................. 98
Figure 67: Dialog "Edit dashboard tab node" .................................................................. 99
Figure 68: Dialog "Edit dashboard tab node" ................................................................ 100
Figure 69: Dialog "Edit link node" ................................................................................ 103
Figure 70: Dialog "Edit link node" ................................................................................ 105
Figure 71: MQTT input node ........................................................................................ 109
Figure 72: Dialog box Edit MQTT in node ................................................................. 109
Figure 73: Dialog box MQTT broker config node – tab Connection ......................... 110
Figure 74: Dialog box MQTT broker config node - tab Security ................................. 111
Figure 75: Dialog box MQTT broker config node - tab Messages .............................. 112
Figure 76: MQTT output node ...................................................................................... 113
Figure 77: Dialog box MQTT output node .................................................................... 113
Figure 78: LED node..................................................................................................... 115
Figure 79: Dialog window Edit npix leds node ............................................................ 115
Figure 80: Serial inbound node RS-232 send .............................................................. 116
Figure 81: Dialog window Edit serial rs232 node - node properties area .................. 116
List of figures

Figure 82: Dialog window „Edit serial port npix rs232 node“ .............................................................. 117
Figure 83: Serial outbound node RS-232 receive .................................................................................. 119
Figure 84: Dialog window Edit serial rs232 node - node properties area .............................................. 119
Figure 85: Dialog window „Edit serial port npix rs232 node“ .............................................................. 120
Figure 86: Serial inbound node RS-485 send ....................................................................................... 122
Figure 87: Dialog window Edit serial rs485 node - node properties area ........................................... 122
Figure 88: Dialog window „Edit serial port npix rs485 node“ .............................................................. 123
Figure 89: Serial outbound node RS-485 receive .................................................................................. 126
Figure 90: Dialog window Edit serial rs485 node - node properties area ........................................... 126
Figure 91: Dialog window „Edit serial port npix rs485 node“ .............................................................. 127
Figure 92: Digital I/O input node DIO in ............................................................................................... 130
Figure 93: Dialog window Edit dio in node - node properties area ..................................................... 130
Figure 94: Dialog window Edit dio in node - node settings area .......................................................... 131
Figure 95: Digital I/O output node DIO out ......................................................................................... 132
Figure 96: Dialog window Edit dio out node - node properties area ................................................... 132
Figure 97: Dialog window Edit dio out node - node settings area ....................................................... 133
Figure 98: MQTT input node .............................................................................................................. 136
Figure 99: MQTT output node ........................................................................................................... 140
Figure 100: Fieldbus input node ........................................................................................................ 144
Figure 101: Message of the fieldbus input node (without error) ........................................................... 150
Figure 102: Message of the fieldbus input node (with error) ............................................................... 151
Figure 103: Fieldbus output node ...................................................................................................... 152
Figure 104: Edit dialog “Edit fieldbus in node” .................................................................................... 162
Figure 105: Dialog box "Add new fieldbus interface config node" ....................................................... 163
Figure 106: Dialog box "Add new fieldbus interface config node" ....................................................... 163
Figure 107: PROFINET configuration ................................................................................................. 164
Figure 108: Available IO items (Example in figure: PROFINET) ........................................................... 165
Figure 109: IO items (Example: PROFINET) ....................................................................................... 165
Figure 110: Dialog „Add new fieldbus interface config node“ .............................................................. 166
Figure 111: Error message – Firmware does not match ........................................................................ 167
Figure 112: Fieldbus_node ................................................................................................................. 167
Figure 113: Dialog Edit fieldbus in node .............................................................................................. 168
Figure 114: Dialog Edit fieldbus in node .............................................................................................. 168
Figure 115: Dialog “Edit fieldbus interface config node” ................................................................. 169
Figure 116: Button Open fieldbus configurator ................................................................................. 169
Figure 117: Start screen of the user interface for fieldbus configuration of the netIOT Edge Gateway (the example in the figure shows PROFINET) .......................................................... 170
Figure 118: Edit fieldbus interface config node .................................................................................... 171
Figure 119: Error message – Firmware does not match ...................................................................... 172
Figure 120: PROFINET user interface ............................................................................................... 173
Figure 121: Note: Name of station .................................................................................................... 176
Figure 122: List of the possible input and output modules ................................................................. 177
List of figures

Figure 123: List of the configured input and output modules .......................................................... 177
Figure 124: Selected IO item (module) for which you define signals ........................................... 179
Figure 125: List of the signal names of an IO item (module) ........................................................... 179
Figure 126: List of the configured input and output modules .......................................................... 182
Figure 127: List of the send and receive signals ............................................................................ 186
Figure 128: EtherNet/IP user interface ............................................................................................ 188
Figure 129: IP Settings ................................................................................................................. 191
Figure 130: List of the possible send and receive assemblies ......................................................... 193
Figure 131: List of the configured send and receive assemblies ..................................................... 193
Figure 132: Selected IO item (assembly) for which you define signals ....................................... 194
Figure 133: List of the signal names of an IO item (assembly) ....................................................... 195
Figure 134: List of the configured send and receive assemblies .................................................... 197
Figure 135: List of the send and receive signals ............................................................................ 201
Figure 136: Edge Server structure ................................................................................................. 204
Figure 137: Edge Server environment ........................................................................................... 207
Figure 138: Internal structure of the Edge Server ......................................................................... 207
Figure 139: netIOT Edge Server icon within the Edge Gateway Manager ...................................... 208
Figure 140: Edge Server Control Center ....................................................................................... 209
Figure 141: Server configuration ................................................................................................. 211
Figure 142: Configuration of the scan settings ............................................................................. 212
Figure 143: Correct configuration of the scan settings .................................................................. 213
Figure 144: Scan protocol configuration ......................................................................................... 214
Figure 145: After the start of the Docker-Service within the Control Panel .................................... 219
Figure 146: Tile Docker in the Edge Gateway Manager ................................................................. 220
Figure 147: Initial call of portainer.io .............................................................................................. 220
Figure 148: portainer.io - initial screen Home (Endpoints) ............................................................. 221
Figure 149: View of portainer.io dashboard ................................................................................... 222
Figure 150: Container list (portainer.io) ......................................................................................... 223
Figure 151: NGINX Example- Screen page "Create container" ....................................................... 224
Figure 152: portainer.io - entry page Home ................................................................................... 226
Figure 153: portainer.io - Page Users > User management ............................................................. 227
Figure 154: portainer.io - Display of User Details ......................................................................... 228
Figure 155: Tile Docker within the Edge Gateway Manager ............................................................ 229
Figure 156: portainer.io - entry page Home ................................................................................... 229
Figure 157: portainer.io - Page Registries (Registry management) ................................................ 230
Figure 158: portainer.io - Page Registries (Registry-Management), Authentication has been activated ........................................................................................................... 230
Figure 159: Portainer.io - Page Create registry (Registries > Add registry) .................................... 231
Figure 160: Tile Docker within the Edge Gateway Manager ............................................................. 232
Figure 161: portainer.io - entry page Home ................................................................................... 232
Figure 162: portainer.io - Page Registries (Registry management) ................................................ 233
List of figures

Figure 163: portainer.io - Page Registries (Registry-Management), Authentication has been activated ................................................................. 233
Figure 164: Portainer.io - Page Create registry (Registries > Add registry) .................. 234
Figure 165: Portainer.io - Page Create registry (Registries > Add registry), Custom registry selected ............................................................... 234
Figure 166: portainer.io - Page Registries (Registry-Management) .................................. 236
Figure 167: Portainer.io - Registry access ..................................................................... 237
Figure 168: Portainer.io - Registry access ..................................................................... 237
Figure 169: portainer.io - Entry page Home ................................................................. 238
Figure 170: portainer.io - Page Create Stacks (Stacks > Add Stack) ......................... 239
Figure 171: Portainer.io - Creating a stack via web editor ........................................... 241
Figure 172: portainer.io - Area "Upload" .................................................................... 242
Figure 173: Portainer.io - Creating a stack using GitHib ............................................. 243
Figure 174: Process of asymmetric encryption ............................................................ 245
Figure 175: Use case 1: Verification of the authenticity of the communication partner (Server) ................................................................. 249
Figure 176: Use case 2: Server certificates for Edge Gateway services ....................... 250
Figure 177: FCC label .................................................................................................. 279
Figure 178: IC on the device label ................................................................................ 280
# List of tables

<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table 1</td>
<td>List of revisions</td>
<td>7</td>
</tr>
<tr>
<td>Table 2</td>
<td>Positions of the interfaces of NIOT-E-TPI51-EN-RE</td>
<td>11</td>
</tr>
<tr>
<td>Table 3</td>
<td>Power supply connector</td>
<td>12</td>
</tr>
<tr>
<td>Table 4</td>
<td>Description of gateway status LEDs</td>
<td>15</td>
</tr>
<tr>
<td>Table 5</td>
<td>LEDs LAN interface</td>
<td>15</td>
</tr>
<tr>
<td>Table 6</td>
<td>LED states for the PROFINET IO-Device protocol</td>
<td>16</td>
</tr>
<tr>
<td>Table 7</td>
<td>LED state definitions for the PROFINET IO-Device protocol</td>
<td>16</td>
</tr>
<tr>
<td>Table 8</td>
<td>LED states for the EtherNet/IP Adapter protocol</td>
<td>17</td>
</tr>
<tr>
<td>Table 9</td>
<td>LED state definitions for the EtherNet/IP Adapter protocol</td>
<td>18</td>
</tr>
<tr>
<td>Table 10</td>
<td>Starting applications with the Edge Gateway Manager</td>
<td>23</td>
</tr>
<tr>
<td>Table 11</td>
<td>Functional overview of the Control Panel</td>
<td>31</td>
</tr>
<tr>
<td>Table 12</td>
<td>Info Center: Area System info</td>
<td>33</td>
</tr>
<tr>
<td>Table 13</td>
<td>Info Center: Area Monitoring</td>
<td>34</td>
</tr>
<tr>
<td>Table 14</td>
<td>Info Center: Area Temperature</td>
<td>34</td>
</tr>
<tr>
<td>Table 15</td>
<td>Numeric coding of facility value in priority PRI</td>
<td>39</td>
</tr>
<tr>
<td>Table 16</td>
<td>Numeric coding of severity value in priority (PRI)</td>
<td>40</td>
</tr>
<tr>
<td>Table 17</td>
<td>Assignment of parts of message line</td>
<td>41</td>
</tr>
<tr>
<td>Table 18</td>
<td>Setting the system time</td>
<td>42</td>
</tr>
<tr>
<td>Table 19</td>
<td>Default ports</td>
<td>44</td>
</tr>
<tr>
<td>Table 20</td>
<td>Table LAN: Description of the columns and elements</td>
<td>56</td>
</tr>
<tr>
<td>Table 21</td>
<td>Wi-Fi modes of operation in selection list Mode</td>
<td>58</td>
</tr>
<tr>
<td>Table 22</td>
<td>Wi-Fi</td>
<td>58</td>
</tr>
<tr>
<td>Table 23</td>
<td>Parameters of the operating mode Access point</td>
<td>60</td>
</tr>
<tr>
<td>Table 24</td>
<td>Parameters of the operating mode Client</td>
<td>61</td>
</tr>
<tr>
<td>Table 25</td>
<td>Operating mode fieldbus interface</td>
<td>63</td>
</tr>
<tr>
<td>Table 26</td>
<td>Parameters of Current connection configuration table</td>
<td>65</td>
</tr>
<tr>
<td>Table 27</td>
<td>Routes parameters</td>
<td>66</td>
</tr>
<tr>
<td>Table 28</td>
<td>Parameters firewall</td>
<td>69</td>
</tr>
<tr>
<td>Table 29</td>
<td>Operating statuses of the services</td>
<td>71</td>
</tr>
<tr>
<td>Table 30</td>
<td>Operating and display elements</td>
<td>71</td>
</tr>
<tr>
<td>Table 31</td>
<td>Parameters of the OPC UA Server for Edge</td>
<td>73</td>
</tr>
<tr>
<td>Table 32</td>
<td>Access rights onto resources</td>
<td>76</td>
</tr>
<tr>
<td>Table 33</td>
<td>Access rights to resources</td>
<td>76</td>
</tr>
<tr>
<td>Table 34</td>
<td>Node-RED user interface</td>
<td>87</td>
</tr>
<tr>
<td>Table 35</td>
<td>Node elements</td>
<td>88</td>
</tr>
<tr>
<td>Table 36</td>
<td>Commands of menu Deploy</td>
<td>92</td>
</tr>
<tr>
<td>Table 37</td>
<td>Kinds of widgets for use in dashboards</td>
<td>94</td>
</tr>
<tr>
<td>Table 38</td>
<td>Areas of the dashboard configuration</td>
<td>95</td>
</tr>
<tr>
<td>Table 39</td>
<td>List of standard nodes</td>
<td>106</td>
</tr>
<tr>
<td>Table 40</td>
<td>Parameter MQTT input node</td>
<td>109</td>
</tr>
<tr>
<td>Table 41:</td>
<td>Parameters in the tab Connection</td>
<td>111</td>
</tr>
<tr>
<td>Table 42:</td>
<td>Parameters in the tab Security</td>
<td>111</td>
</tr>
<tr>
<td>Table 43:</td>
<td>Parameters in the tab Messages</td>
<td>112</td>
</tr>
<tr>
<td>Table 44:</td>
<td>Parameters of the Edit MQTT output node</td>
<td>114</td>
</tr>
<tr>
<td>Table 45:</td>
<td>Parameters of configuration dialog Edit serial rs232 node</td>
<td>115</td>
</tr>
<tr>
<td>Table 46:</td>
<td>Options of selection list LED</td>
<td>115</td>
</tr>
<tr>
<td>Table 47:</td>
<td>Parameters of configuration dialog Edit serial rs232 node</td>
<td>116</td>
</tr>
<tr>
<td>Table 48:</td>
<td>Options for Split input</td>
<td>118</td>
</tr>
<tr>
<td>Table 49:</td>
<td>Parameters of configuration dialog Edit serial rs232 node</td>
<td>119</td>
</tr>
<tr>
<td>Table 50:</td>
<td>Options for Split input</td>
<td>121</td>
</tr>
<tr>
<td>Table 51:</td>
<td>Parameters of configuration dialog Edit serial rs485 node</td>
<td>122</td>
</tr>
<tr>
<td>Table 52:</td>
<td>Options for Split input</td>
<td>124</td>
</tr>
<tr>
<td>Table 53:</td>
<td>Parameters of configuration dialog Edit serial rs485 node</td>
<td>126</td>
</tr>
<tr>
<td>Table 54:</td>
<td>Options for Split input</td>
<td>128</td>
</tr>
<tr>
<td>Table 55:</td>
<td>Parameters of configuration dialog Edit dio in node</td>
<td>130</td>
</tr>
<tr>
<td>Table 56:</td>
<td>Parameters of configuration dialog Edit dio out node</td>
<td>132</td>
</tr>
<tr>
<td>Table 57:</td>
<td>Standard procedure</td>
<td>160</td>
</tr>
<tr>
<td>Table 58:</td>
<td>Configuration steps</td>
<td>161</td>
</tr>
<tr>
<td>Table 59:</td>
<td>PROFINET configuration user interface</td>
<td>173</td>
</tr>
<tr>
<td>Table 60:</td>
<td>PROFINET configuration tree</td>
<td>176</td>
</tr>
<tr>
<td>Table 61:</td>
<td>Contents of the table “IO items”</td>
<td>177</td>
</tr>
<tr>
<td>Table 62:</td>
<td>Controls of the table “IO Items”</td>
<td>178</td>
</tr>
<tr>
<td>Table 63:</td>
<td>Contents of table „IO item“</td>
<td>179</td>
</tr>
<tr>
<td>Table 64:</td>
<td>Contents of the table „Signals“</td>
<td>180</td>
</tr>
<tr>
<td>Table 65:</td>
<td>Controls of the table „Signals“</td>
<td>180</td>
</tr>
<tr>
<td>Table 66:</td>
<td>Data types for signal names</td>
<td>181</td>
</tr>
<tr>
<td>Table 67:</td>
<td>Columns of the table of the send and receive signals</td>
<td>186</td>
</tr>
<tr>
<td>Table 68:</td>
<td>EtherNet/IP configuration user interface</td>
<td>188</td>
</tr>
<tr>
<td>Table 69:</td>
<td>EtherNet/IP configuration tree</td>
<td>191</td>
</tr>
<tr>
<td>Table 70:</td>
<td>Parameters for setting the IP addresses</td>
<td>192</td>
</tr>
<tr>
<td>Table 71:</td>
<td>Contents of the table „IO items“</td>
<td>193</td>
</tr>
<tr>
<td>Table 72:</td>
<td>Controls of the table „IO Items“</td>
<td>194</td>
</tr>
<tr>
<td>Table 73:</td>
<td>Contents of the table „IO items“</td>
<td>194</td>
</tr>
<tr>
<td>Table 74:</td>
<td>Contents of the table „IO items“</td>
<td>195</td>
</tr>
<tr>
<td>Table 75:</td>
<td>Controls of the table „Signals“</td>
<td>196</td>
</tr>
<tr>
<td>Table 76:</td>
<td>Data types for signal names</td>
<td>196</td>
</tr>
<tr>
<td>Table 77:</td>
<td>Columns of the table of the send and receive signals</td>
<td>201</td>
</tr>
<tr>
<td>Table 78:</td>
<td>Functions of the Edge Server</td>
<td>206</td>
</tr>
<tr>
<td>Table 79:</td>
<td>Symbols for the state of operation in the service list</td>
<td>209</td>
</tr>
<tr>
<td>Table 80:</td>
<td>Functions for working with containers</td>
<td>223</td>
</tr>
<tr>
<td>Table 81:</td>
<td>Meaning of columns of tab le of all current registries</td>
<td>231</td>
</tr>
</tbody>
</table>
List of tables

Table 82:  Meaning of columns of table of all current registries ........................................ 234
Table 83:  Attributes concerning the issuer and owner of the certificate zum Zertifikats-Aussteller und Zertifikats-Inhaber ................................................................. 246
Table 84:  Overview use cases............................................................................................ 249
Table 85:  Edge Gateway services ..................................................................................... 251
Table 86:  Technical data NIOT-E-TPI51-EN-RE .............................................................. 275
Table 87:  Technical data PROFINET IO RT IRT Device Protocol .................................. 277
Table 88:  Technical data EtherNet/IP Adapter protocol .................................................. 278
Contacts

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

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

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

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

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

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

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

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

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