optimize!
softing

User Guide

smartLink HW-PN

dataFLOW®

Version: 1.20-EN/2026-09-03

© Softing Industrial Automation GmbH

Disclaimer of liability

The information contained in these instructions corresponds to the technical status at the time of printing of it and is passed on with the best of our knowledge. Softing does not warrant that this document is error free. The information in these instructions is in no event a basis for warranty claims or contractual agreements concerning the described products, and may especially not be deemed as warranty concerning the quality and durability pursuant to Sec. 443 German Civil Code. We reserve the right to make any alterations or improvements to these instructions without prior notice. The actual design of products may deviate from the information contained in the instructions if technical alterations and product improvements so require.

Trademarks

PROFINET is a registered trademark of PROFIBUS Nutzerorganisation e.V. (PNO)

OpenSource

To comply with international software licensing terms, we offer the source files of open source software used in our products. For details see https://opensource.softing.com/

If you are interested in our source modifications and sources used, please contact: info@softing.com

Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6
85540 Haar / Germany
https://industrial.softing.com

+ 49 89 4 56 56-340

info.automation@softing.com
support.automation@softing.com

https://industrial.softing.com/support/support-form

Table of Contents

Chapter 1 About this guide 7
1.1 Read me first 7
1.2 Target audience 7
1.3 Typographic conventions 7
1.4 Document history 8
1.5 Related documentation 8
1.6 Document feedback 8
Chapter 2 About smartLink HW-PN 9
2.1 Intended use 9
2.2 Supported features 9
2.3 System requirements 9
2.4 Technical data 10
2.5 Hardware interfaces 12
2.5.1 Real-time clock 12
2.5.2 Safety precautions 12
2.6 Software interfaces 13
2.6.1 OPC UA 13
2.6.2 MQTT 13
2.6.3 HART-IP 13
2.7 LED status indicators 14
2.7.1 Status LEDs startup phase 15
2.7.2 Status LEDs – factory mode 15
2.7.3 Status LEDs – normal mode 16
Chapter 3 Installation 17
3.1 Hardware installation 17
3.1.1 Mounting and dismounting 17
3.1.2 Connections and nameplate 18
3.1.3 Power and alarm connectors 19
3.1.4 Installation positions 20
3.1.5 Connecting to the network 21
3.1.6 Powering up the device 21
3.1.7 Resetting the device 22
3.1.7.1 Soft reset 22
3.1.7.2 Hard reset 22
3.2 Software installation 24
3.2.1 Search and Configure tool 24
3.3 Commissioning 25
3.3.1 Prerequisites 25

3.3.2 Changing the IP address ... 25
3.3.2.1 Using the Search and Configure tool ... 26
3.3.3 Login to the user interface ... 28
3.3.4 Configuring PROFINET ... 28
3.3.5 Selection of services ... 28
Chapter 4 Security ... 29
Chapter 5 Working with the smartLink HW-PN ... 30
5.1 smartLink HW-PN user interface ... 30
5.1.1 General functions ... 30
5.1.2 Information ... 30
5.1.2.1 System ... 30
5.1.2.2 License ... 31
5.1.2.3 About ... 31
5.1.3 Settings ... 32
5.1.3.1 Network ... 32
5.1.3.2 User accounts ... 33
5.1.3.3 Firmware ... 35
5.1.3.4 Reset ... 37
5.1.3.5 Certificates ... 38
5.1.3.6 Time & Date ... 39
5.1.3.7 Licensing ... 40
5.1.4 Diagnosis ... 43
5.1.4.1 Settings ... 43
5.1.4.2 Log File ... 44
5.1.4.3 Threads ... 45
5.1.4.4 Status ... 45
5.1.4.5 Live List ... 46
5.1.5 PROFINET ... 49
5.1.6 HART-IP ... 50
5.1.6.1 Settings ... 50
5.1.6.2 Log ... 51
5.1.7 OPC UA ... 52
5.1.7.1 Settings ... 52
5.1.7.2 Security ... 52
5.1.8 MQTT ... 55
5.1.8.1 Settings ... 55
5.1.8.2 Log ... 56
5.2 Connecting to Emerson AMS Device Manager ... 57
5.2.1 Prerequisites ... 57

5.2.2 Network configuration - FDI ... 58
5.2.3 AMS Device Manager - FDI ... 61
5.2.4 Network configuration - HART-IP ... 62
5.2.5 AMS Device Manager - HART-IP ... 65
5.3 Connecting to ABB FIM ... 66
5.3.1 Prerequisites ... 66
5.3.2 Connecting to smartLink HW-PN ... 66
5.3.3 Importing an FDI package/FIMlet ... 71
5.3.4 Scanning for devices ... 72
5.4 Connecting to plantPerfect Monitor ... 73
5.4.1 Prerequisites ... 73
5.4.2 Connecting to an MQTT broker ... 73

Chapter 6 Performance ... 74

Chapter 7 Troubleshooting ... 75

Chapter 8 Declaration of conformity ... 77

Chapter 9 Glossary ... 79

Chapter 10 Appendix ... 80

10.1 MQTT payload ... 80
10.1.1 Object model and relationships ... 81
10.1.2 Server object ... 82
10.1.3 OnlineState object ... 83
10.1.4 Network object ... 84
10.1.5 Node object ... 84
10.1.6 Device object ... 85
10.1.7 Controller object ... 87
10.1.8 Interface object ... 89
10.1.9 EthernetInterface object ... 91
10.1.10 Port object ... 92
10.1.11 EthernetPort object ... 93
10.1.12 PortStatistics object ... 94
10.1.13 Diagnosis object ... 95

This page is intentionally left blank.

1 About this guide

1.1 Read me first

Please read this guide carefully before using the device to ensure safe and proper use. Softing does not assume any liability for damages due to improper installation or operation of this product.

This document is not warranted to be error-free. The information contained in this document is subject to change without prior notice. To obtain the most current version of this guide, visit the product website.

1.2 Target audience

This guide is intended for experienced operation personnel and network specialists responsible for configuring and maintaining field devices in process automation networks. Before installing and operating the smartLink HW-PN make sure that you have read and fully understood the safety requirements and working instructions in this guide.

1.3 Typographic conventions

The following conventions are used throughout Softing customer documentation:

Keys, buttons, menu items, commands and other elements involving user interaction are set in bold font and menu sequences are separated by an arrow	Open **Start → Control Panel → Programs**
Buttons from the user interface are enclosed in brackets and set to bold typeface	Press **[Start]** to start the application
Coding samples, file extracts and screen output is set in Courier font type	`MaxDlsapAddressSupported=23`
Filenames and directories are written in italic	Device description files are located in *C:\<Application name>\delivery\software\Device Description files*

CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, may result in damage or injury.

Note

This symbol is used to call attention to notable information that should be followed during installation, use, or servicing of this device.

Hint

This symbol is used when providing you with helpful user hints.

1.4 Document history

Document version	Changes since last version
1.00	First version
1.01	▪ Minor editorial changes
1.02	▪ Details on how to reset[22] the device added. ▪ New Live List[46] features.
1.03	▪ User interface chapters Settings → Certificates[38] and OPC UA → Security[29] added.
1.04	▪ Support of ABB FIM added. ▪ Support of AMS Device Manager added. ▪ Support for APL switches added: aplSwitch Field ((Softing), Ethernet-APL Rail Field Switch (Pepperl + Fuchs) and Ethernet-APL Field Switch (R.Stahl)
1.10	▪ Selection of services[28] added to Commissioning chapter ▪ MQTT[55] user interface menu explained ▪ MQTT payload[80] descriptions added ▪ Chapter Connecting to Softing plantPerfect Monitor added
1.20	▪ HART-IP support added. ▪ Setting HART-IP[50] in user interface explained.

1.5 Related documentation

See the following documents for further product information:

- plantPerfect Monitor User Guide
- data sheet and brochures

1.6 Document feedback

We would like to encourage you to provide feedback and comments to help us improve the documentation. You can write your comments and suggestions to the PDF file using the editing tool in Adobe Reader and email your feedback to support.automation@softing.com.

If you prefer to write your feedback directly as an email, please include the following information with your comments:

- document name
- document version (as shown on cover page)
- page number

2 About smartLink HW-PN

The Softing smartLink HW-PN provides access to the communication system and connects the higher-level network structure with the field level.

The default configuration allows for a start-up in only a few minutes. In order to prevent network disruptions by unauthorized configuration changes, all configuration functions are protected by user administration.

2.1 Intended use

The smartLink HW-PN is designed to be used as a secure access point to PROFINET networks. Any other use is deemed non-intended use.

CAUTION

Do not use this device in hazardous areas! See Section Technical Data 10 for permissible ambient conditions.

Note

Installation and operation of the smartLink HW-PN must be performed by qualified personnel only.

2.2 Supported features

<%PRODUCTNAME%> supports the following features:

- access to PROFINET devices
- access to PROFIBUS devices connected to supported PROFINET PROFIBUS proxies
- access to HART devices connected to supported PROFINET HART remote IOs
- PLC-independent access to PROFINET networks
- Asset Management connectivity via FDI (OPC UA) and HART-IP
- Network monitoring data over MQTT

2.3 System requirements

The following hardware and software components are required to install and operate your smartLink HW-PN:

- PC with web browser
- Ethernet cable
- PROFINET cable
- 18 VDC to 32 VDC power supply

2.4 Technical data

Hardware	**Processor**: Altera Cyclone V SoC with dual-core ARM Cortex-A9 **Status LEDs**: PWR, RUN, ERR, BUS Real-Time Clock: Real-Time clock with buffering, setting the time via browser or by NTP server (buffer time depends on conditions such as ambient temperature and duration of use)
Interfaces	**Ethernet:** 1 x IEEE802.3 10BASE-T/100BASE-TX/1000BASE-T, Connector: RJ45 **PROFINET**: 2 x IEEE802.3 10BASE-T/100BASE-TX, Connector: RJ45 Embedded PROFINET 2-port switch for line or ring topology Protocol: PROFINET RT / IRT, Support of PROFINET redundancy protocols
Supported communication protocols	PROFINET, PROFIBUS, FDI communication server (OPC UA), HART-IP, MQTT
Supported PROFINET-PROFIBUS proxies	Softing: pnGate PA, pnGate DP, aplSwitch Field PA Pepperl+Fuchs: Ethernet-APL Rail Field Switch (V1.31 and higher) R.Stahl: Ethernet-APL Field Switch
Supported Controllers and Remote IOs for HART ACCESS	**Siemens:** ET 200iSP: PROFINET IM152-1PN 6ES7152-1BA00-0AB0 (redundant) ET 200SP: PROFINET IM155-6PN (High Feature) 6ES7155-6AU01-0CN0 ET 200SP: PROFINET IM 155-6 PN/3 6ES7155-6AU30-0CN0 (redundant), ET 200SP: PROFINET IM 155-6 PN R1 6ES7155-6AU00-0HM0 (redundant) ET 200SP HA: PROFINET IM155-6PN 6DL1155-6AU00-0PM0 (redundant) ET 200M: PROFINET IM153-4 PN (High Feature) 6ES7153-4BA00-0XB0 ET200MP: 6ES7 155-5MU00-0CN0 CFU HART: 6ES7655-5PX41-1XX0
Supported PROFINET HART proxies	**Siemens:** ET 200iSP: 6ES7134-7TD00-0AB0, 6ES7134-7TD50-0AB0, 6ES7135-7TD00-0AB0, 6ES7138-7FA00-0AB0,6ES7138-7FA00-0AB0 ET 200SP: 6ES7134-6TD00-0CA1, 6ES7135-6TD00-0CA1 ET 200SP HA: 6DL1133-6EW00-0PH1, 6DL1133-6EW00-0EH16, DL1134-6TH00-0PH1, 6DL1134 6UD00-0PK0, 6DL1134-6TB00-0HX1, 6DL1135-6TF00-0PH1, 6DL1135-6UD00-0PK0, 6DL1136-6AA00-0PH1 with optional module redundancy ET 200M: 6ES7331-7TF01-0AB0, 6ES7332-8TF01-0AB0, 6ES7331-7TB10-0AB0, 6ES7332-5TB10-0AB0, 6ES7336-4GE00-0AB0, 6ES7336-4GE00-0AB0 , ET 200 MP: 6ES7531-7TF00-0AB0, 6ES7532-8TF00-0AB0
Supported asset management applications	Emerson AMS Device Manager (V14.5 and higher) ABB Field Information Manager (V3.3 and higher)
Dimensions (H x W x D)	120 mm x 28 mm x 110 mm
Weight	about 430g
Power Supply	18 VDC ... 32 VDC; SELV/PELV power supply mandatory, typical input current: 200 mA, maximum input current: 1 A (allowing for in-rush current at switch-on)
Typical Power Loss	5 W
Operating Temperature	-40 °C ... +65°C (see also Section Installation Positions 20)
Storage Temperature	-40 °C ... +85 °C
Relative humidity	10 % ... 95 %, non-condensing
Cooling	Convection, no fan

Mounting	DIN rail 35 mm
Protection	IP20
Altitude	intended use must not exceed 2000 m in altitude
Usage location	indoor use only; no direct sunlight

2.5 Hardware interfaces

2.5.1 Real-time clock

A real-time clock (RTC) is located on the device, which is used to validate the temporal validity when using certificates. The real-time clock is buffered so that the real-time clock continues to run in the event of a brief power failure. The buffer time is limited and depends on various parameters (ambient temperature, duration of use, ...) and can range from a few hours to several days.

During the initial installation and if the power failure lasts longer than the buffer time, the RTC can be set using a browser via the web server (see corresponding section: Setting the RTC via browser).

Therefore, a problem with the validity of a certificate may indicate that the real-time clock is not set. It is recommended to use a time server in the network (NTP server), then the device automatically fetches the current time (see corresponding section: Activating the NTP server).

2.5.2 Safety precautions

CAUTION

During operation, the device's surface will be heated up. Avoid direct contact. When servicing, turn off the power supply and wait until surface has cooled down.

CAUTION

The electronic components of the smartLink HW-PN are sensitive to electrostatic discharges. Damages due to electrostatic discharge can lead to premature failure of components or intermittent faults at a later stage. Before installing the smartLink HW-PN, divert the electrostatic discharge away from your body and the tools used.

Note

Do not open the housing of the smartLink HW-PN. It does not contain any parts that need to be maintained or repaired. In the event of a fault or defect, remove the device and return it to the vendor. Opening the device will void the warranty!

2.6 Software interfaces

2.6.1 OPC UA

The smartLink HW-PN has an OPC UA server integrated. This server implements the TCP based binary OPC UA protocol and allows OPC UA clients to connect to it.

FDI communication server

The FDI communication server supports both PROFINET (FCG_TS62769-103-4) and PROFIBUS (FCG_TS62769-103-1) profiles.

The OPC UA server of the smartLink HW-PN complies with the OPC 30080-7 / FCG TS62769-7 specification V1.3 "FDI Communication Devices". This specification can be found on the FieldComm Group web page (www.fieldcommgroup.org) and for download on the OPC Foundation web page (www.opcfoundation.org).

An example of an FDI communication client written in Python is available at: https://github.com/SoftingIndustrial/FDICommClient.

2.6.2 MQTT

The smartLink HW-PN has an integrated MQTT (Message Queuing Telemetry Transport) publisher. It publishes PROFINET network data to an MQTT broker.

The PROFINET network data is provided as a JSON-encoded payload within the MQTT messages. The payload structure is based on the objects and attributes defined in the OPC 30140 specification, OPC UA for PROFINET, version 1.00.

For more information, see the MQTT payload 80 section in the appendix, which contains a detailed description of the JSON-encoded data.

2.6.3 HART-IP

The smartLink HW-PN has an HART-IP server integrated and allows HART-IP clients to connect to it.

2.7 LED status indicators

smartLink HW-PN has four device status LEDs at the top, two connection status LEDs on the web server port and two on each PROFINET connection port:

PWR = power supply - refer to next section 15

RUN = running - refer to next section 15

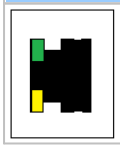
ERR = error - refer to next section 15

BUS = configuration - displays configuration upload - refer to next section 15

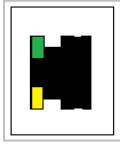
The device status LEDs are permanently on or flash in different colors and frequencies as indicated below:

Symbol	Color	Light
	none	off
	red	permanent
	green	permanent
	red	flashing (1 Hz)
	red	flashing quickly (5 Hz)
	green	flashing (1 Hz)
	green	flashing slowly (0.5 Hz)
	green	flashing quickly (5 Hz)
	orange (red/green)	permanent
	orange (red/green)	green permanent + red flashing (1 Hz)

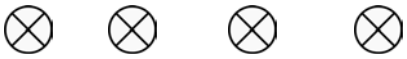
The **Ethernet port LEDs** indicate the following behaviour:

Ethernet port LEDs	Colour	Behaviour
	green	ON when port has an active link
	yellow	FLASHING when there is traffic on the port

The **PROFINET port LEDs** indicate the following behaviour:

PROFINET port LEDs	Colour	Behaviour
	green	ON when port has an active link and FLASHING when there is traffic on the port
	yellow	currently not in use

2.7.1 Status LEDs startup phase

LEDs	Meaning
PWR RUN ERR BUS 	**Power Off** – check Power supply.
PWR RUN ERR BUS	**Power On** - 24V DC power supply is ok.
PWR RUN ERR BUS	**Start up phase** (up to 30 seconds).
PWR RUN ERR BUS	**Start up phase finished** – check execution mode (normal or factory).

2.7.2 Status LEDs – factory mode

LEDs	Meaning
PWR RUN ERR BUS	Device running in factory mode.
PWR RUN ERR BUS	Firmware update is running.
PWR RUN ERR BUS	Request to execute factory reset.
PWR RUN ERR BUS	Device executes factory reset.
PWR RUN ERR BUS n.a	**Software error** - restart the device.
PWR RUN ERR BUS n.a	**Software error** - device restarted automatically and error is reported in log file.

2.7.3 Status LEDs – normal mode

LEDs				Meaning
PWR	**RUN**	**ERR**	**BUS**	Device running in Normal mode.
		n.a.	n.a.	
PWR	**RUN**	**ERR**	**BUS**	Firmware update is running.
		n.a.	n.a.	
PWR	**RUN**	**ERR**	**BUS**	Device is configuring for PROFINET.
		n.a.		
PWR	**RUN**	**ERR**	**BUS**	Device joined PROFINET and is online.
		n.a.		
PWR	**RUN**	**ERR**	**BUS**	**Software error** - restart the device.
			n.a.	
PWR	**RUN**	**ERR**	**BUS**	**Software error** - device restarted automatically and error is reported in log file.
			n.a.	
PWR	**RUN**	**ERR**	**BUS**	Flash LED operation is running (DCP-Signal).
			n.a.	

3 Installation

3.1 Hardware installation

Note

With an ambient temperature above 55 °C at the place of installation it is very likely that the temperatures of connecting cables will increase if the cables are installed in an unfavourable position. In such cases, measure the temperature to ensure that the service temperature of the cables is not exceeded or use cables sustaining high temperatures of at least 90 °C.

3.1.1 Mounting and dismounting

Note

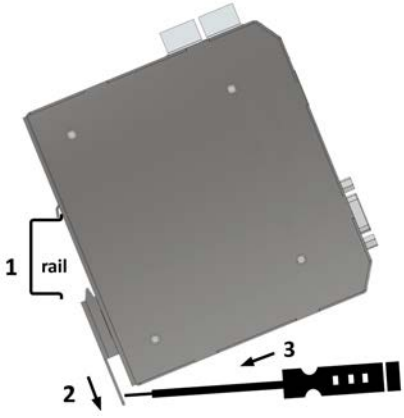
Make sure the smartLink HW-PN is mounted in such a way that the power supply can be easily disconnected. Depending on the installation position, the maximum ambient operating temperature may differ. See Section Installation positions 20 for details.

Installation and inspection

Installation and inspection must be carried out by qualified personnel only (personnel qualified according to the German standard TRBS 1203 - Technical Regulations for Operational Safety). The definition of terms can be found in IEC 60079-17.

Mounting

1. Hook the upper notch of the cut-out on the back of the device into a 35 mm DIN rail.
2. Leverage the screwdriver upwards, pull the locking bar downwards and move the device down towards the rail.
3. Press the gateway down towards the rail until it slides into place over the lip of the locking bar.



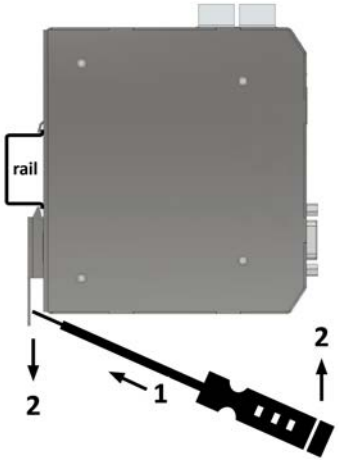
Note

Do not put stress on the system by bending or torsion.

Dismounting

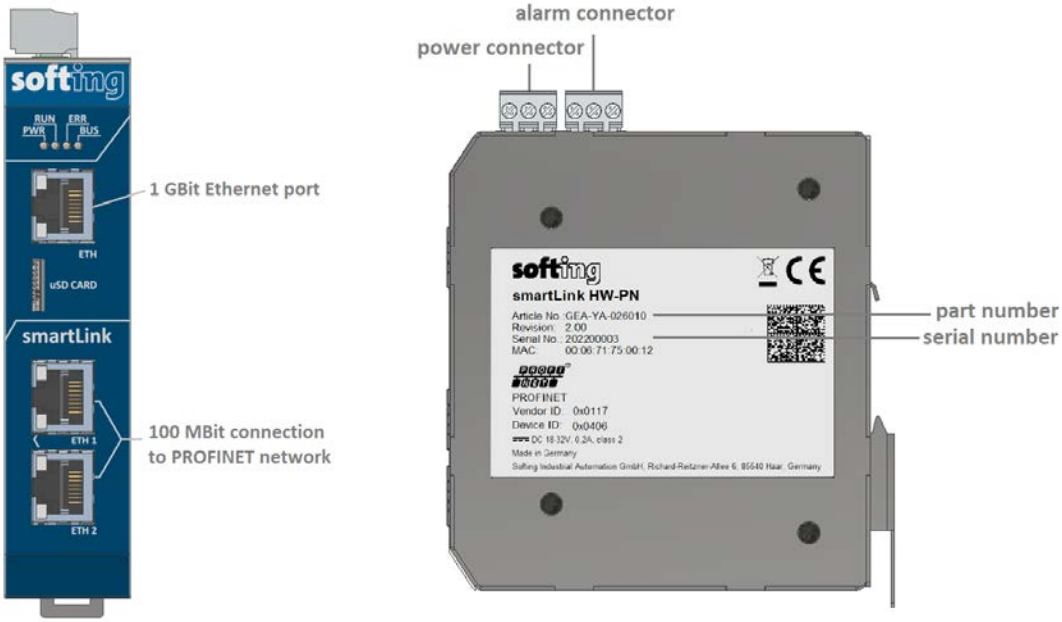
1. Slide a screwdriver diagonally under the housing into the locking bar.

2. Leverage the screwdriver upwards, pull the locking bar downwards and move the gateway upwards off the rail.



3.1.2 Connections and nameplate

The following diagram shows the interfaces of the smartLink HW-PN. The device has one 1 GBit Ethernet port (ETH) connecting to your IT network and two 100 MBit Ethernet ports connecting to your PROFINET network and PLC. The connectors on the top are reserved for the supply voltage and alarm output. The uSD card slot is used for future service purposes and is not supported in the current version of the product.



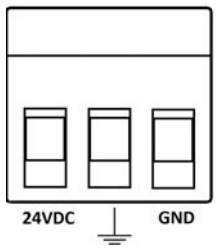
3.1.3 Power and alarm connectors

Connect the smartLink HW-PN to a 24 VDC power supply.

Note
smartLink HW-PN is intended for connection to a SELV/PELV circuitry only.

Power connector

The supply voltage (18 VDC .... 32 VDC) is connected by a 3-pole terminal block. The power supply is connected to the plug connector via flexible wires with a cross section of 0.75 to 1.5 mm². The ground connection wire must have a cross section of 1.5 mm².



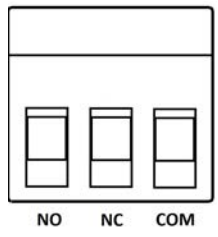
Signal	Description
24 VDC	24 VDC power supply
⏚	Functional earth
GND	Ground

Note
smartLink HW-PN offers reverse polarity protection in the specified DC supply voltage range (see Chapter Technical Data 10).

CAUTION
The Functional Earth (FE) connection of the device has to be connected at low inductance with the Protective Earth (PE) of the system.

Alarm connector

The alarm output has a voltage range of 0-32 V. Connect the positive supply voltage with the COM terminal to avoid damage when the connector accidentally mixed up.



Signal	Description
NO	Normally Open
NC	Normally Closed
COM	Common Terminal

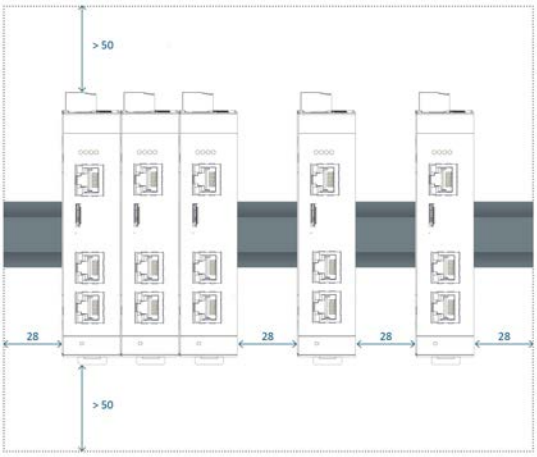
3.1.4 Installation positions

The smartLink HW-PN can be mounted horizontally and vertically. Depending on the installation position, different ambient operating temperatures (T_a) apply.

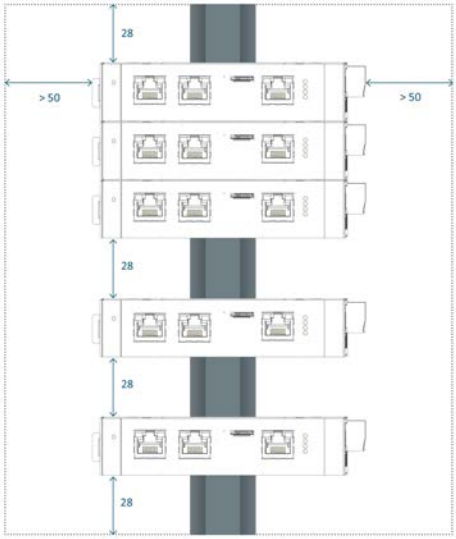
Minimum distance
Provide a minimum distance of 50 mm to the air inlet and air outlet to ensure natural convection.

Rotated installation position
The maximum permissible ambient temperature values also apply to a 180° rotated installation position.

Horizontal installation position



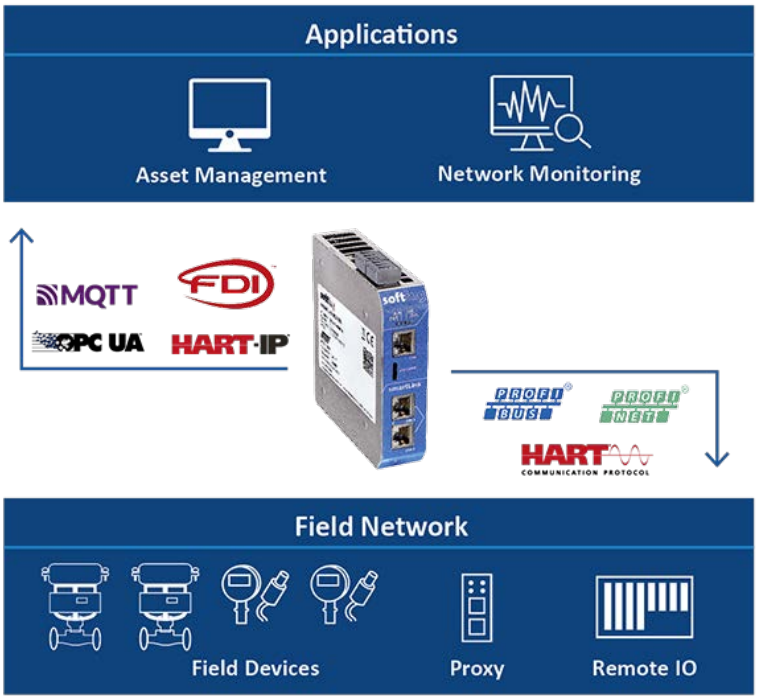
Vertical installation position



Max. ambient temperature (Ta)	Ta - no distance	Ta at 28mm distance between devices
horizontal	60 °C	65 °C
vertical	50 °C	60 °C

3.1.5 Connecting to the network

1. Connect your PC to the 1 GBit Ethernet (ETH) port of your smartLink HW-PN.
2. Connect your PROFINET network (with its Remote IOs, field devices and PLC) to the Ethernet ports (ETH1 and/or ETH2) of your smartLink HW-PN .



Note
The smartLink HW-PN can also be used in a PROFINET line or ring topology too. In this case it is best to locate it next to the controller.

Note
To access PROFIBUS devices, the PROFINET-PROFIBUS proxies have to be in the same PROFINET network as the smartLink HW-PN .

3.1.6 Powering up the device

Turn on the power supply. The boot process will take about 30 seconds. Refer to LED status indicators 14 for a detailed description of the LEDs and their behaviour.

3.1.7 Resetting the device

This chapter describes how to reset your smartLink HW-PN. By resetting your device you can restore previous settings or return to the original custom settings of your device, known as factory default.

3.1.7.1 Soft reset

A soft reset restarts the device through the user interface and clears all configuration data except the device IP address and associated licenses.

Action required:

See Section **Settings** → **Reset** 37 for details.

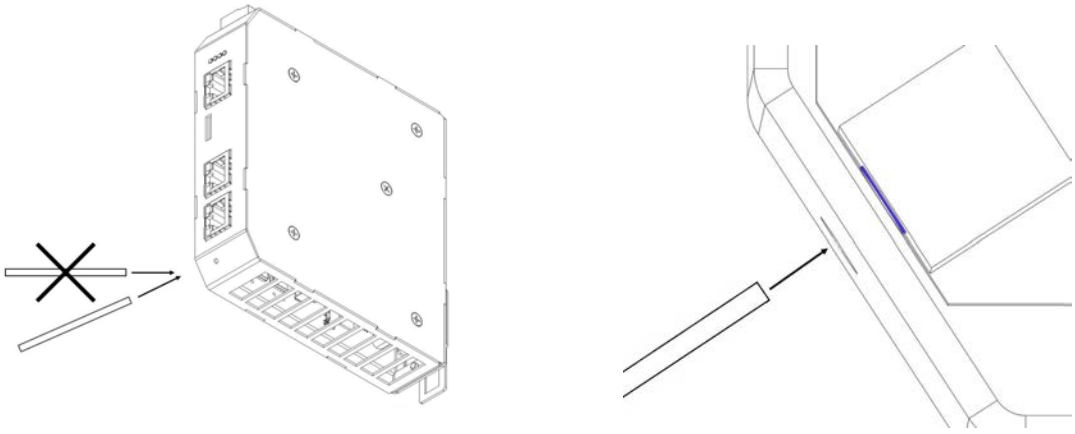
3.1.7.2 Hard reset

This type of reset is recommended if smartLink HW-PN is not responding, is malfunctioning or you simply cannot log on to the device because you have forgotten your login credentials. A hard reset deletes all device settings including the IP address and restores the factory default.

Example: You want to decommission a device because your plant is undergoing reconstruction and the network must be taken out of service.

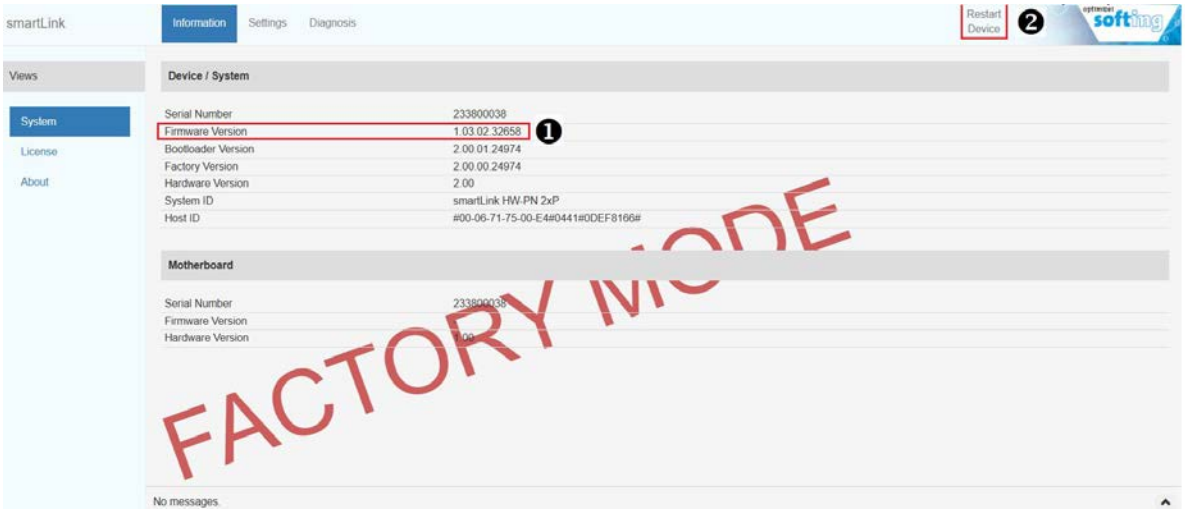
Action required:

1. Disconnect the power supply of your smartLink HW-PN.
2. Insert a thin screwdriver (1-2 mm) or a pin into the hole at the bottom of the front (as shown below).



3. Press the reset button carefully while reconnecting and powering up the device. The PWR LED lights orange. Hold the button until the RUN LED is flashing red (takes about 10 seconds).
4. Release the reset button. The smartLink HW-PN is now rebooting.
5. Open your Internet browser and enter the standard IP address to access the user interface of your smartLink HW-PN. The user interface shows that the device is now running in factory mode (watermarked diagonally across each menu).

Note
The factory mode indicates that the device has been reset to its original factory settings. The user interface shows only the menus Information, Setting and Diagnosis.



Note
Make sure that the firmware version shown on the **Information → System** page after the reset is the latest official version available for download from the product website. ❶

Note
If the smartLink HW-PN is running the latest firmware, proceed with step 8.

6. If the smartLink HW-PN is running an old firmware version, select **Settings → Choose Firmware File...** to update the device. See Chapter Firmware 35 for details.
7. When the firmware update has been successfully completed, the watermark FACTORY MODE is no longer shown and the version of the new firmware is shown on the **Information → System** page.
8. Alternatively, exit the factory mode and return to the fully featured user interface by restarting the device in the banner bar of the user interface. ❷

3.2 Software installation

When you install a Softing product for the first time, you will be asked if you trust the publisher. Activate the option Always trust software from Softing AG if you do not want to be asked in subsequent installations and select [Install] to start the installation.

Optionally, you can install the Windows *Search and Configure* tool to configure the IP address of the smartLink HW-PN.

3.2.1 Search and Configure tool

1. Go to the smartLink HW-PN product website to download the latest software (Search and Configure)*

2. Start by downloading and installing the **Search and Configure** tool.

3. Follow the on-screen installation instructions.

4. Read the license agreement carefully.
   If you have questions, you can **[Cancel]** the installation at this point and contact us. Click **[Print]** if you want to print the license agreement to a PDF or on a printer.

5. Select **I accept the terms in the license agreement** and click **[Next]**.

6. Click **[Install]** to install the selected software application on your PC.
   While the installation is in progress, the status bar of the installation wizard shows the different steps that are being executed. If you want to abort the installation, click **[Cancel]** button. The installation wizard will undo all modifications that have been made to your computer up to this point. Otherwise, wait until the installation is completed.

7. Press **[Finish]** to complete the installation and exit the wizard.

Note
Proceed with the installation of the other software packages.

* Search and Configure: discovery and IP-Configuration of smartLink HW-PN

3.3 Commissioning

The smartLink HW-PN comes with an integrated web server which is used to configure the device. The default IP address of the integrated web server is 192.168.0.10. To change the network settings of the smartLink HW-PN you can either change the IP address of the corresponding network adapter on your PC to access the integrated web server or use the Search and Configure tool. See section 3.3.2 25 on how to perform these two settings.

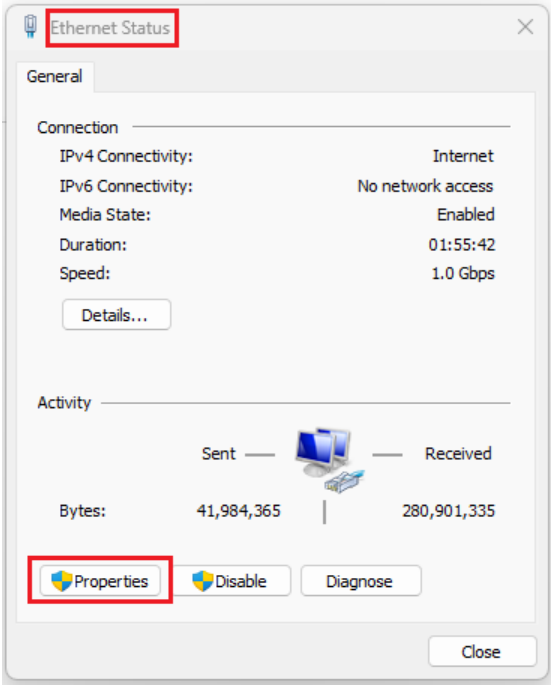
3.3.1 Prerequisites

- The smartLink HW-PN is connected with a PC which runs a Chrome, Microsoft Edge or Firefox web browser supporting JavaScript.

3.3.2 Changing the IP address

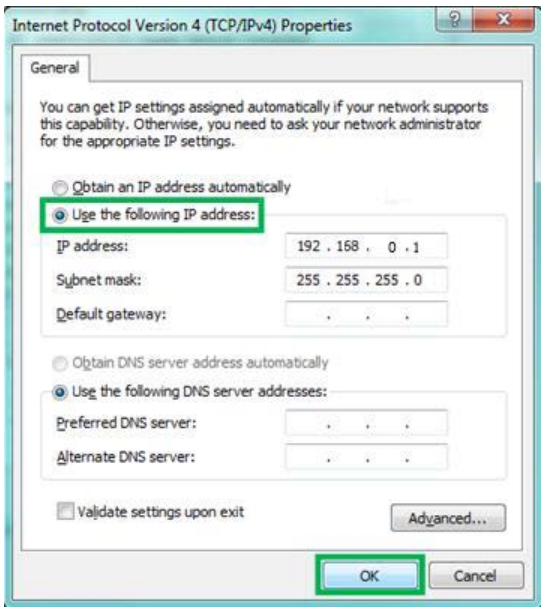
You can access the web interface of the smartLink HW-PN by changing the IP address of your PC. Using the web interface you can change the network settings of the smartLink HW-PN afterwards. The following chapter describes how to set a static IP address in Windows 11.

1. Click **Search** → **Control Panel** in your task bar.
2. Select **Network and Internet → Network and Sharing Center**.
   A new window opens where you can view your basic network information.
3. Select your Internet connection type (either Ethernet or Wireless) next to Connections under **View your active networks**.
   The connection status window opens.



4. Click **[Properties].**
   A new window opens.

5. Double-click the element **Internet Protocol Version 4 (TCP/IPv4)**.
   The following window opens.



6. Select **Use the following IP address** and enter a specific IP address and Subnet mask. In our example we use the following settings:
   IP address: 192.168.0.1
   Subnet mask: 255.255.255.0

7. Click **[OK]** to confirm.

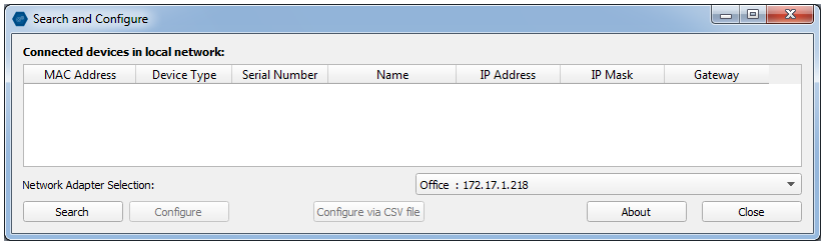
8. Adapt the network settings of your smartLink HW-PN as described in Section Network 32 .

3.3.2.1 Using the Search and Configure tool

Before you can operate the connected smartLink HW-PN you will have to change the default IP address of your gateway so that your PC can communicate with the integrated web server over the Local Area Network.

The following steps apply to Windows 11.

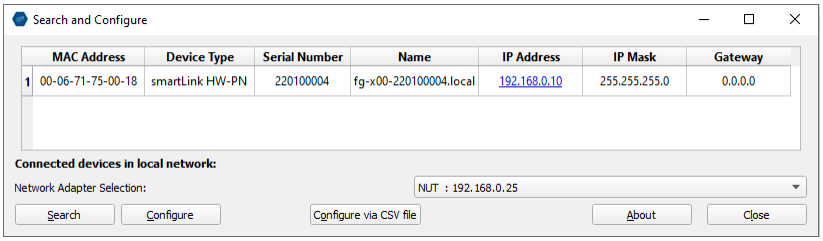
1. Click **Start → Softing → Search and Configure**.
   The application window is opened.



2. Click the dropdown list of the **Network Adapter Selection**.
   This selection menu shows all network adapters of your PC.

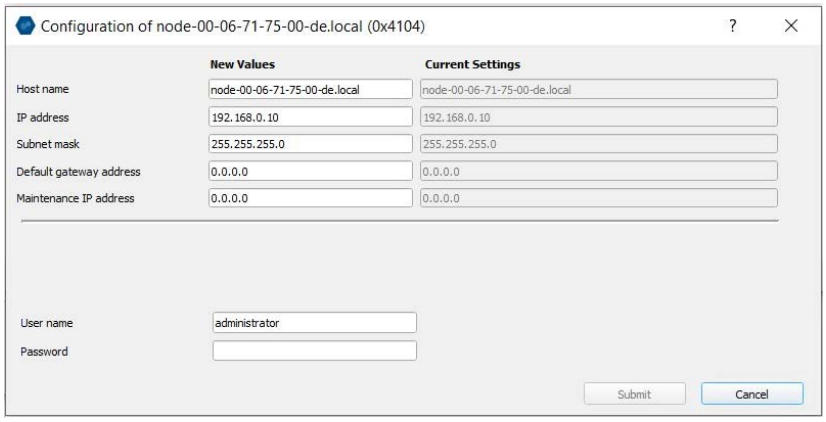
3. Select the network adapter which is connected to the smartLink HW-PN.

4. Click **[Search]** to start searching for connected devices.
   The search may take a moment.



5. Select the smartLink HW-PN.

6. Click **[Configure]** or double-click the device.
The configuration window opens. Here you can change the IP settings.



Note
You may also change the hostname. However, ensure that you follow hostname specifications RFC 952 and RFC 1123.

7. Enter a dedicated IP address and subnet mask or click **Use DHCP** to obtain the IP settings from a DHCP server.

8. Enter the **Password**.
Example: **GEA-YA-026010<serialnumber>**
The serial number can be found on the device, on the packaging and in the Search and Configure tool. See Section Login to user interface 28 for details.

9. Click **[Submit]**.
The changed settings are written to the device.

3.3.3 Login to the user interface

1. Open your Internet browser and enter the IP address of your smartLink HW-PN.

2. Enter **administrator** in the user field and the **password** below (example: *GEA-YA-026010<serialnumber>*). The **default password** (initial or after executing a factory reset) is a combination of the article number and the serial number which you find on the nameplate on the side of the device.

The web-based interface opens with the information page.

3.3.4 Configuring PROFINET

See Section PROFINET 49 in Chapter *Working with the user interface* for more details.

3.3.5 Selection of services

The smartLink HW-PN provides the following services:

OPC UA Server

The OPC UA Server enables Asset Management applications, such as Emerson AMS Device Manager or ABB FIM, to connect to the PROFINET network and its devices.

MQTT Publisher

The MQTT Publisher transfers PROFINET network data to plantPerfect Monitor, the OT network monitoring solution from Softing.

At least one of these services must be enabled to retrieve data from the PROFINET network.

HART-IP Server

The HART-IP Server enables Asset Management applications, such as Emerson AMS Device Manager, to connect to the HART devices attached to PROFINET remote IOs.

4 Security

The smartLink HW-PN is installed in level 0 of the Purdue reference model.

With its three Ethernet ports it resides in 2 network segments:

- The upper Ethernet port ETH is providing Software interfaces for asset management applications running in level 3.
- The PROFINET Ethernet ports (ETH1 / ETH2) must be part of the level 0 PROFINET network segment.

smartLink HW-PN upper Ethernet (ETH) services

Service	Port /Protocol	Description	Direction
OPC UA	4840 | TCP (configurable)	OPC UA Server	inbound to device
MQTT	1883/8883| TCP (configurable)	MQTT Publisher	outbound to MQTT broker
HTTPS	443 |TCP	HTTPS Server of integrated web server	inbound to device
HART-IP	5094/ alternate port | TCP	HART-IP Server	inbound to device

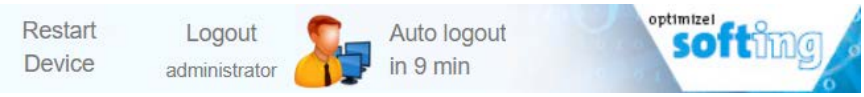
5 Working with the smartLink HW-PN

See Section Log in to user interface 28 for details on how to access the interface.

5.1 smartLink HW-PN user interface

5.1.1 General functions

The banner bar of the user interface displays theses functions:



Restart Device
This function is available only when logged in as administrator or maintenance engineer and is used to restart the gateway remotely as instructed in this user guide or whenever required in ongoing operation.

Logout
Select this function to log out as an active user.

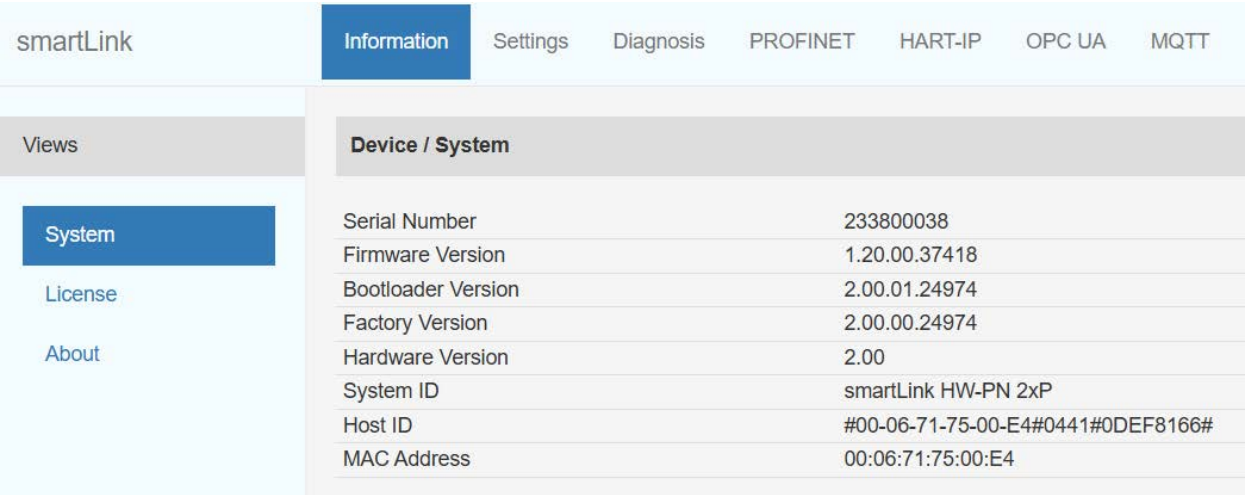
Auto logout
This default setting logs out the current user from the gateway if the interface has been inactive for 10 minutes.

5.1.2 Information

The **Information** window shows detailed product-related information in the menus **System**, **License** and **About.**

5.1.2.1 System

Select **Information** → **System** to view the hardware and software details of your device.



Parameter	Meaning
Serial Number	Serial number of the gateway.
Firmware Version	Version of the currently running firmware.
Bootloader Version	Version number of the boot loader.
Factory Version	Version number of the factory image.
Hardware Version	Version number of the hardware.
System ID	device type = smartLink HW-PN
Host ID	This is the ID you will need to request a license.

5.1.2.2 License

Select **Information → License** to view the licenses used by the gateway firmware under an open source license.

5.1.2.3 About

Select **Information → About** to show information about Softing and other useful information.

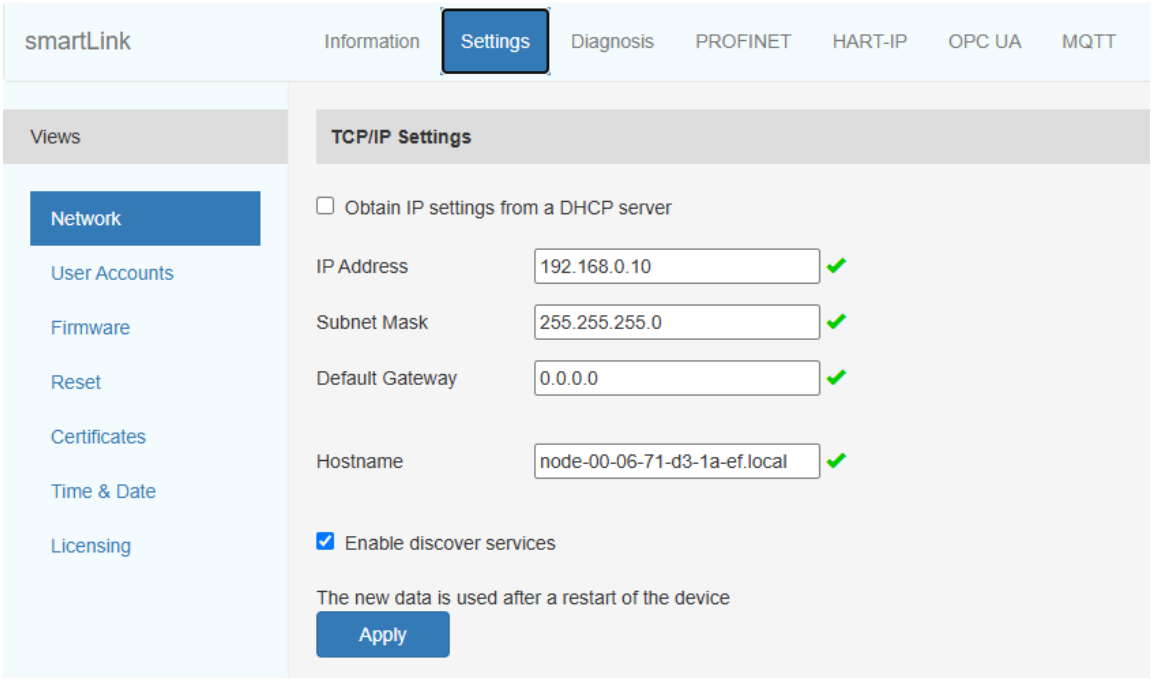
5.1.3 Settings

5.1.3.1 Network

Select **Settings → Network** to view and change the TCP/IP settings.

Note

You need to be logged in as Administrator or Maintenance[33] to change default settings. If you change the settings you must restart the gateway.

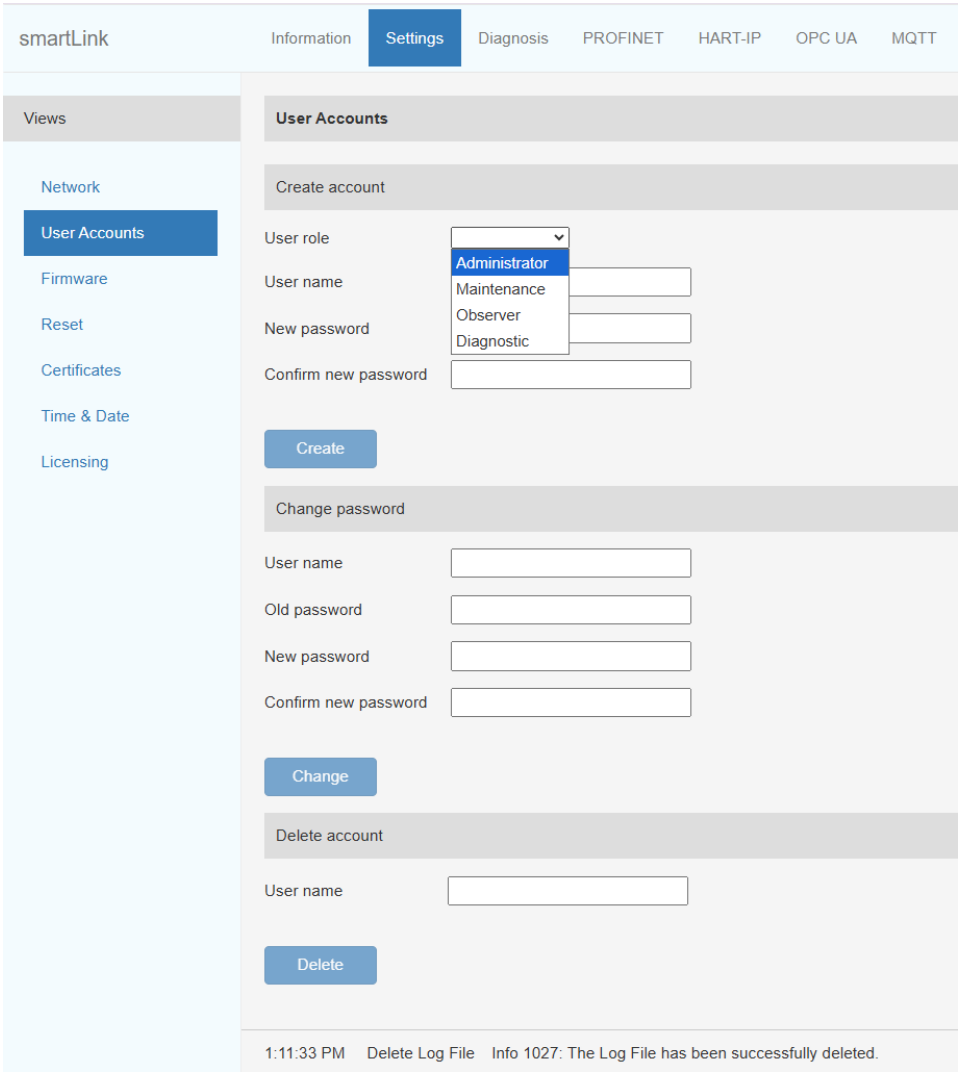


Parameter	Meaning
Obtain IP address from a DHCP server	The Dynamic Host Configuration Protocol (DHCP) is activated and the IP address is obtained from a DHCP server.
IP address	Internet Protocol (IP) address of the device used for web access.
Subnet mask	Subnet mask of the device used for web access.
Default gateway	Default gateway of the device used for web access.
Hostname	Name of the device used by a name server.
Enable discover services	Check the box to enable *Simple Service Discovery Protocol* (SSDP) *multicast DNS* (mDNS) and *SearchAndConfigure*.
Apply	Click [Apply] to confirm changes made in this window.

5.1.3.2 User accounts

In this section you will learn how to change accounts and passwords.

1. Select **Settings → User Accounts**.
   As **administrator** you can create and delete user accounts and also change passwords.



2. Select a user role in the dropdown menu, assign a user name and enter a **New password** in the corresponding fields according to the password rules.

3. Retype the password in the **Confirm new password** field and click **[Create]** to save the user and password settings.

Password rules

A password must contain between eight and 128 characters, including at least 1 lower case letter, 1 upper case letter, 1 number and 1 special character: !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~

Changing the password

1. Enter the user name of the account for which you want to change the password.
2. Enter the **Old password**.
3. Enter the **New password**.
4. Retype the password in the **Confirm new password** field and click **[Change]** to save the new password settings.

Deleting an account

1. Enter the user name of the account which you want to delete.
2. Click **[Delete]** to erase the account and remove the user.

The following table shows the user roles and corresponding permissions:

Permission	Administrator	Diagnostic	Maintenance	Observer
Create and delete accounts	☑	☑		
Change all passwords	☑	☑		
Change own password	☑	☑	☑	☑
Configuring gateway	☑	☑	☑	
Reading configuration	☑	☑	☑	☑
Reading diagnostics	☑	☑	☑	☑
Updating firmware	☑	☑		
Resetting gateway	☑	☑		
Managing certificates and security	☑	☑		

Note

The user role *Diagnostic* is not required for daily operations. It is reserved for internal purposes such as troubleshooting. Softing Support may ask you to add a user with this role to obtain more details of your smartLink HW-PN.

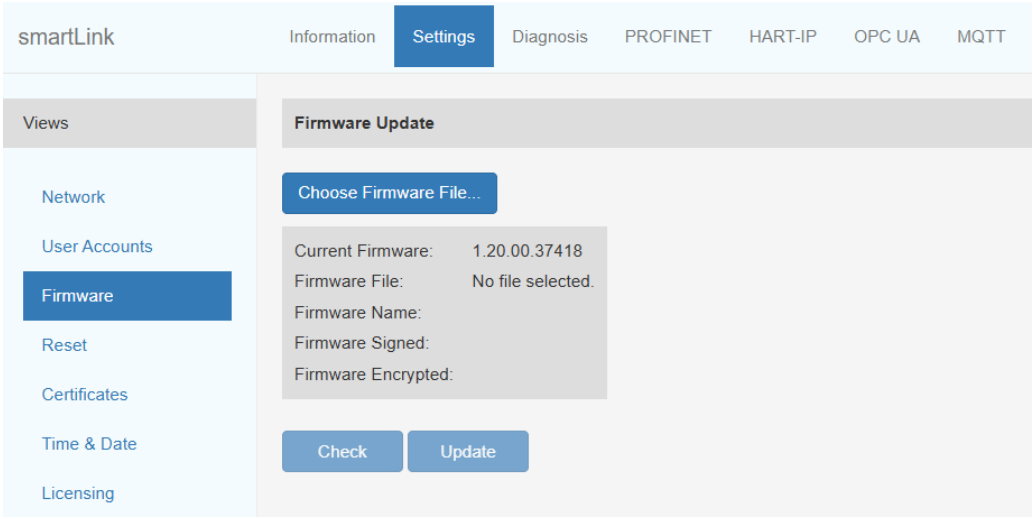
5.1.3.3 Firmware

The gateway comes with pre-installed firmware which is maintained and updated to continuously enhance the functionality of the device. To ensure that your smartLink HW-PN is running the latest firmware version check for the latest version in the Softing Download Center. Bear in mind that the smartLink HW-PN cannot be downgraded to a previous version.

Note

You need to be logged in as administrator[33] .

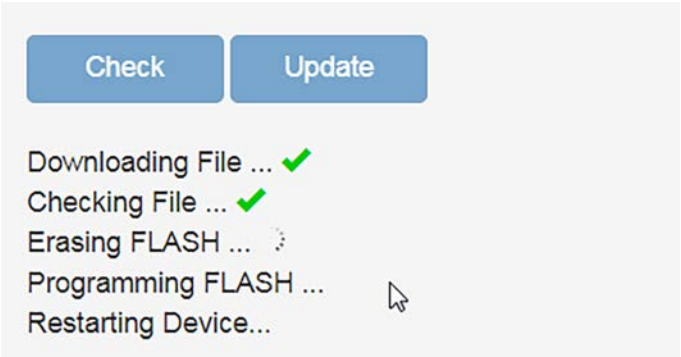
1. Download the firmware update to your computer.
   When you are downloading from this site for the first time you will have to register yourself in a few steps.
2. Log on to the web server of the smartLink HW-PN.
3. Select **Settings → Firmware** in the side bar navigation.
4. Click **[Choose Firmware File...]** and select the file *firmware.bin* from the firmware update you downloaded.



5. Click **[Update]** to install the latest firmware and **[OK]** in the message window. The update progress is shown beneath the update button.

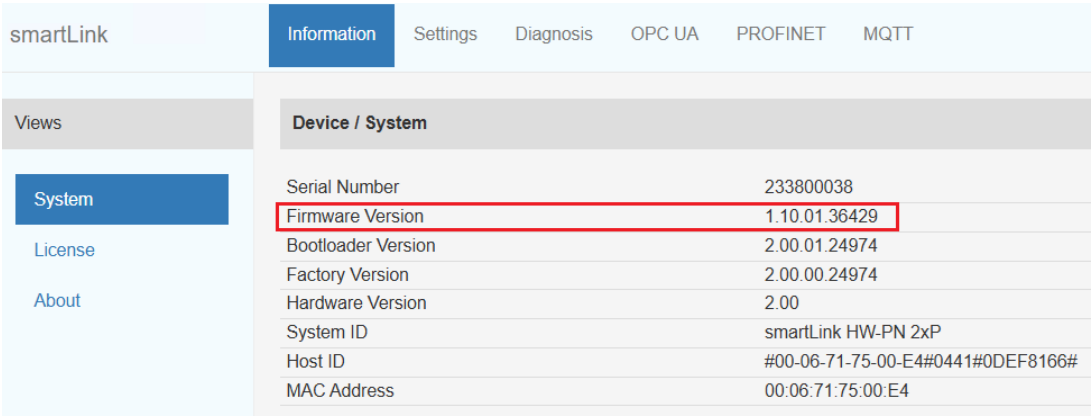
Hint

Click **[Check]** to verify, if the file you have chosen is a valid firmware file.



The system performs a firmware file check. The download starts automatically. When the download is completed, the smartLink HW-PN will be rebooted. You will be prompted to log in again to the user interface. When the boot process is completed, the RUN and the PWR LED are green.

You will now see the updated firmware version shown on the device information page.



Note
If the user login page of the user interface does not open automatically, press F5 to reload the page.

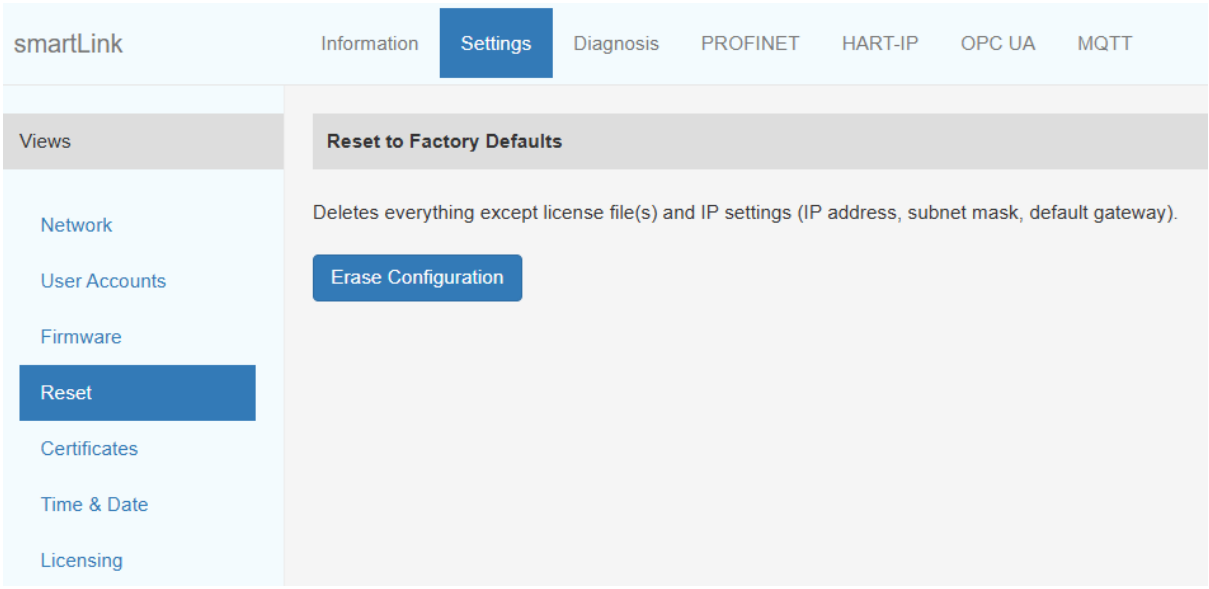
Note
If you encounter a problem during the update you can always repeat it.

5.1.3.4 Reset

Unlike the factory reset (hard reset) described in Chapter *Hardware Installation*[12], this soft reset deletes the configuration of your smartLink HW-PN and restores the factory settings of your gateway.

1. Select **Settings → Reset** in the side bar navigation
2. Select **[Erase Configuration]** to reset your device to default settings.

Note
You need to be logged in as administrator[33].



3. Click **[OK]** to confirm your selection.
Your smartLink HW-PN will be restarted with the default settings. License files and IP settings will not be deleted.

Note
The password is reset to the default password[28].

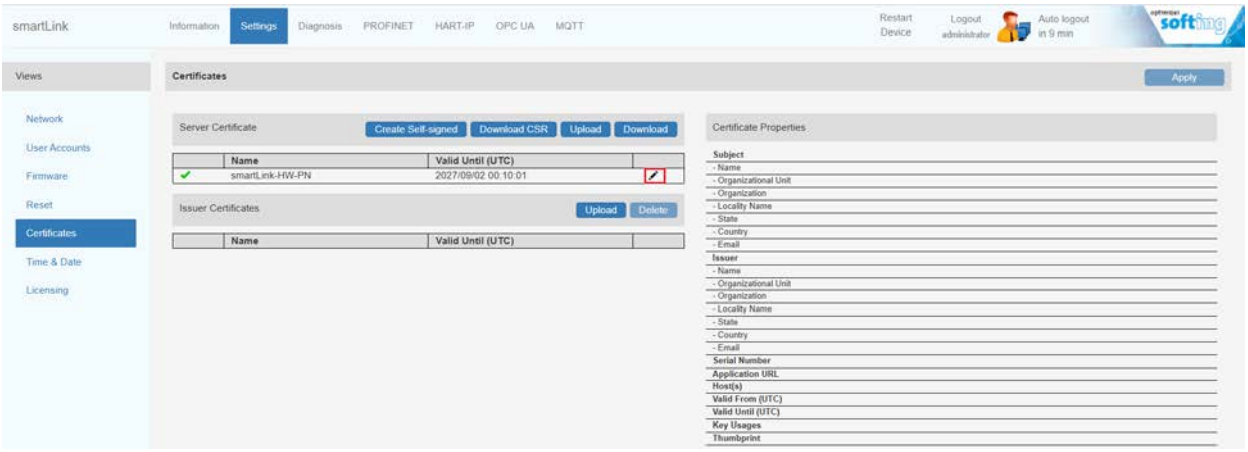
5.1.3.5 Certificates

A certificate is a digital document that is needed to identify and authenticate a website or server and to establish a secure communication (HTTPS) with the OPC UA server of the smartLink HW-PN.

Select **Settings → Certificates** to see the smartLink HW-PN X.509 server certificate and load issuer certificates which are used to validate the server certificate. The tables display the subject name and the expiration timestamp of the server and the issuer certificates. The first column either shows a checkmark indicating the certificate's status (✔ = valid, ⚠ = expired/not valid).

In the **Server Certificate** section you can create a new self-signed certificate, upload a new certificate and download the currently installed server certificate or a Certificate Signing Request (CSR). The downloaded server certificate can be passed on to the OPC UA client application to enable secure communication. The CSR can be forwarded to a Certificate Authority (CA) which may create a matching signed server certificate.

If you create a new self-signed certificate or change the existing server certificate, a pencil icon is shown in the right-most column of the server certificate list (see screenshot below). The icon indicates that the certificate settings have been changed but have not yet been applied and still need to be executed by clicking **[Apply]** in the top right corner.



In addition, intermediate issuer certificates can be uploaded to the **Issuer Certificates** section to configure a chain of trust for the issuer specified in the server or other intermediate certificates.

Note

Ensure that the clock on the smartLink HW-PN is properly set. Otherwise this could result in the creation or usage of certificates that have already expired. See **Settings → Time & date** for details.

Note

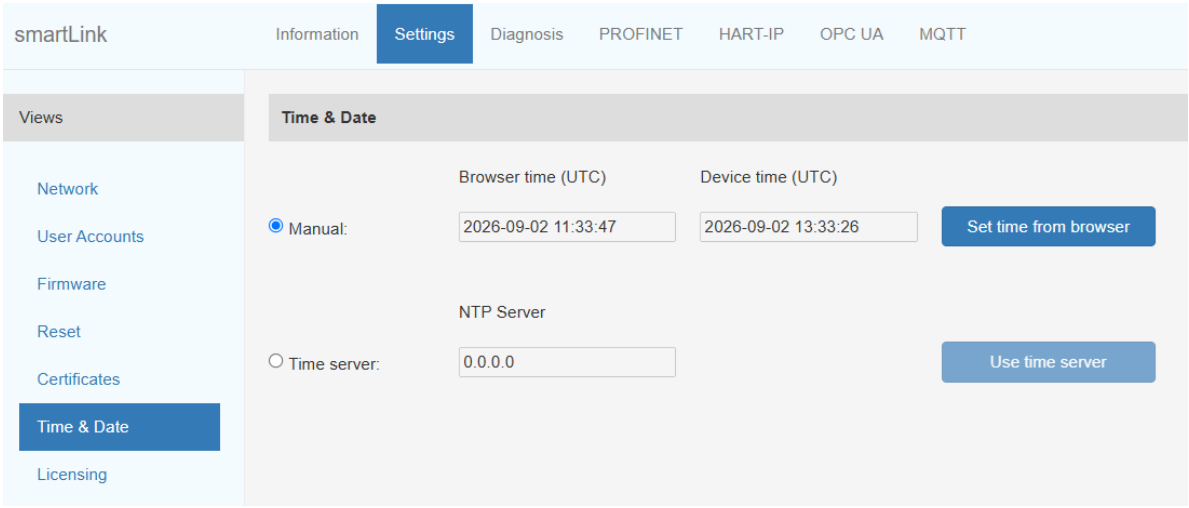
Your changes are not executed immediately but have to be confirmed by clicking **[Apply]** in the top right corner of the page. This will restart the OPC UA server component of smartLink HW-PN. Any clients connected at that time will lose their connection but typically will automatically reconnect.

Parameter		Meaning
Server Certificate	Create self-signed	Creates a new self-signed certificate.
	Download CSR	Sends a Certificate Signing Request (CSR) for a new server certificate. The signed server certificate must then be uploaded.
	Upload	Uploads the a signed server certificate to the smartLink HW-PN.
	Download	Downloads the server certificate currently used by the smartLink HW-PN and upload it to e.g. an OPC UA client.
Issuer Certificate	Upload	Uploads the an issuer certificate to the smartLink HW-PN.
	Delete	Deletes the an issuer server certificate from the smartLink HW-PN.

5.1.3.6 Time & Date

Select **Settings → Time & Date** in the side bar navigation to set the time and date of your smartLink HW-PN.

1. Click **[Set time from browser]** to synchronize the gateway with the PC date and time manually.
2. Click **[Use time server]** and enter the IP address of your time server to synchronize date and time automatically.



Parameter	Meaning
Browser time (UTC)	The time set on the PC.
Device time (UTC)	The time set on the gateway.
NTP server	IP address of a Network Time Protocol (NTP) server used for time synchronisation.
Time server	The time can be set either manually or using a time server.

5.1.3.7 Licensing

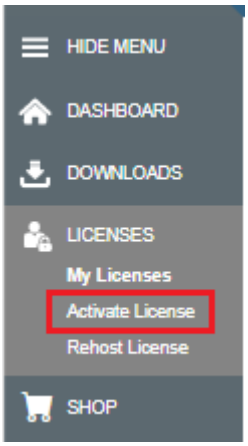
Licenses are needed for PROFINET Device Support by any Asset Management Tool to parametrize and monitor PROFINET devices and to retrieve process data and diagnosis data via OPC UA. Each license is tied to one PROFINET slave and can be used for Asset Management and for OPC UA at the same time.
You will most likely have purchased your smartLink HW-PN with one or more PROFINET licenses installed. You will need a license for each field device to which you wish to connect over the PROFINET network. A license is a unique key tied to the serial number of your gateway. It cannot be migrated or run on another smartLink HW-PN.

If your smartLink HW-PN has no license or you wish to connect to more PROFINET devices than previously licensed, please contact Softing Support.

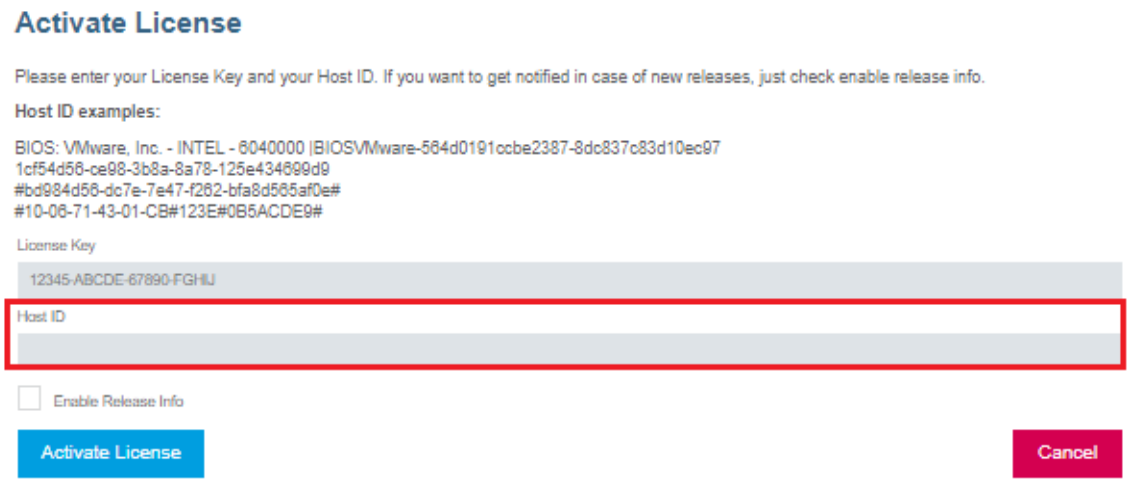
How to activate a license

1. Go to the Softing Industrial website and click the icon in the upper right corner to register yourself or select this My Softing Portal link. When you are registered and logged in you are directed to the **My Softing Dashboard**.

2. Select **Licenses → Activate License** in the side menu.



3. Enter the license key from your License Certificate in the license key input field.
You will find the license key on the certificate you have received by email.



4. Select **Information → System**[30].

5. Highlight and copy the Host ID from the Device/System table.

6. Paste the Host ID into the **Host ID** field of the Activate License form.

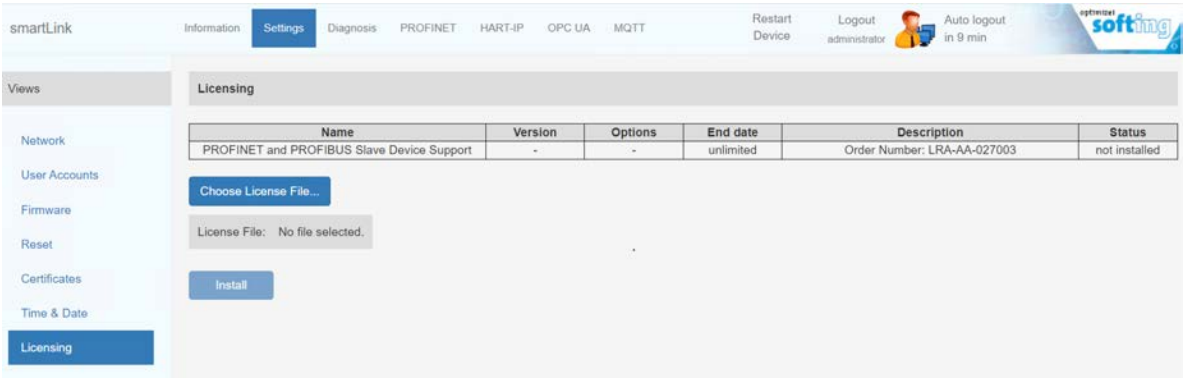
7. Click **[Activate License]**.
   A license file is generated and downloaded to your PC.

Note
The license file is assigned to the device and can therefore only be used with this device.

How to install a license

To install a license file follow these steps:

1. Select **Settings → Licensing** in the side bar navigation.

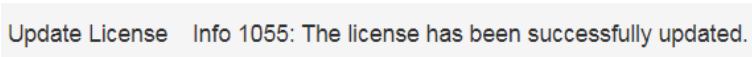


2. Click **[Choose License File**].
   Windows Explorer (file explorer) will open.

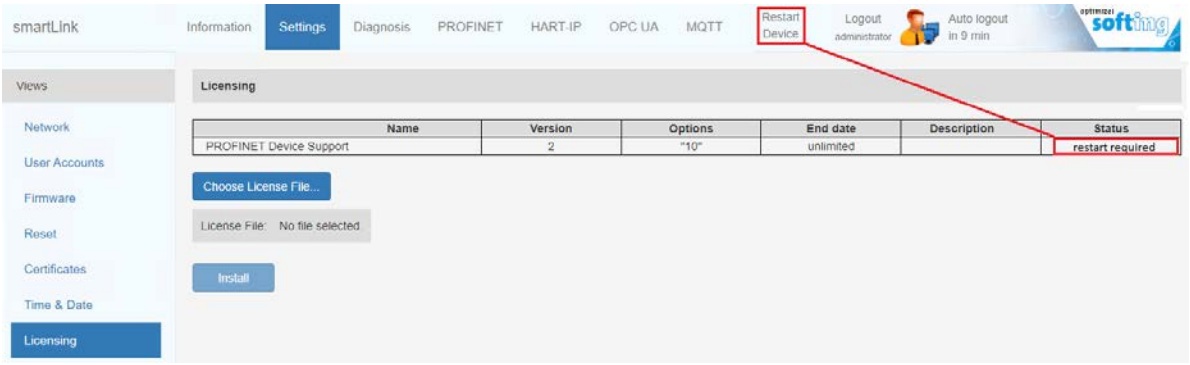
3. Go to the directory to which you have saved the file.

4. Select the license file and click **[Open]** in Windows Explorer.
   The license file is now shown underneath the **[Choose License File]** button.

5. Click **[Install**].
   When the license has been installed, the following message appears at the bottom of the window.

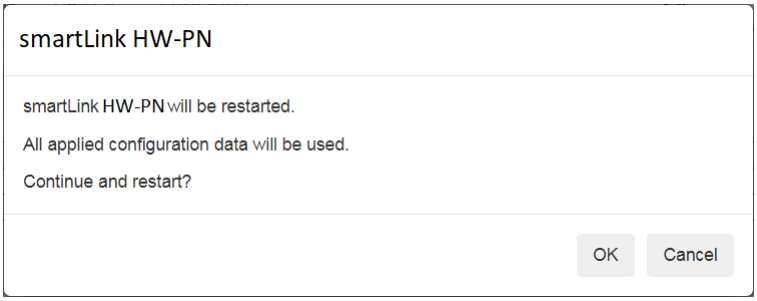


In the Licensing window, the table entries for PROFINET Device Support will have changed.

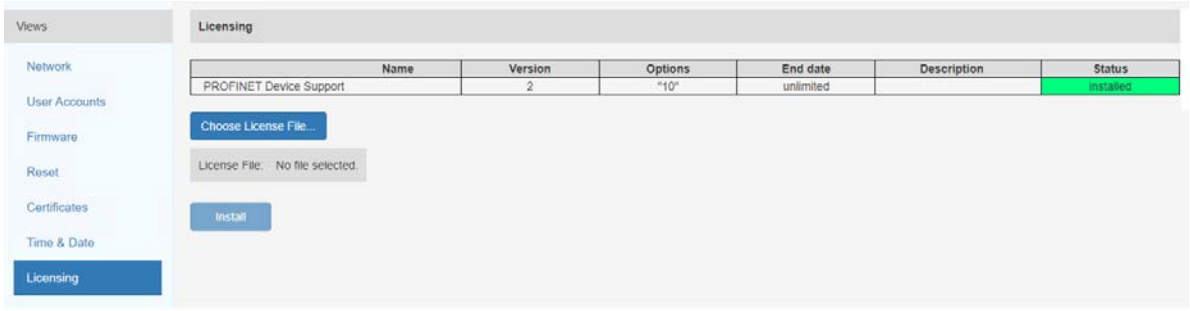


Parameter	Meaning
Version	A support number (for internal use only).
Options	Total number of supported PROFINET devices.
End date	The date on which the license expires. Generally all licenses are unlimited.
Description	Before a license is installed, this field displays the order number for a license for this specific gateway.
Status	Before a license is installed, this field displays "not installed". When a license has been installed it shows "restart required" against a yellow background. After the gateway has been restarted it shows "installed" against a green background

6. Click **Restart Device** in the top menu of the window.
The following message will appear.



7. Click **[OK].**
The status column now shows "installed" meaning the license is activated on your smartLink HW-PN device.



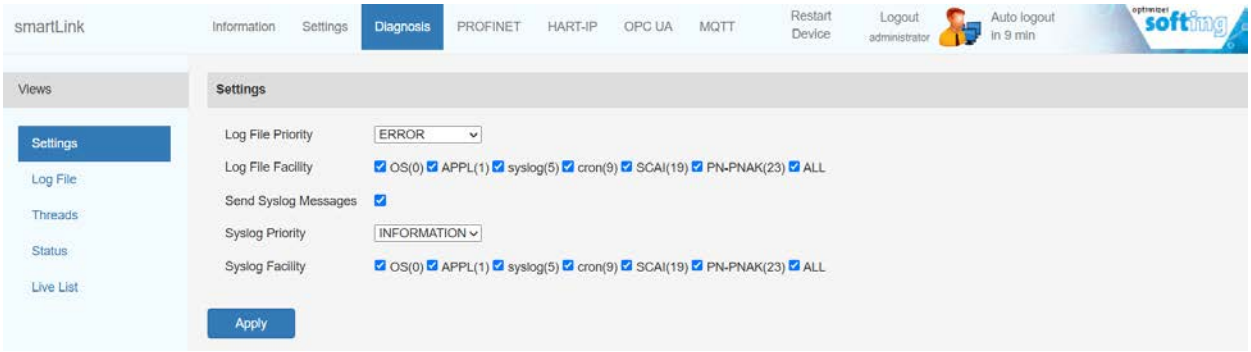
5.1.4 Diagnosis

Note

The submenus **Settings, Log File, Threads and Status** are of particular interest for Softing Support.

5.1.4.1 Settings

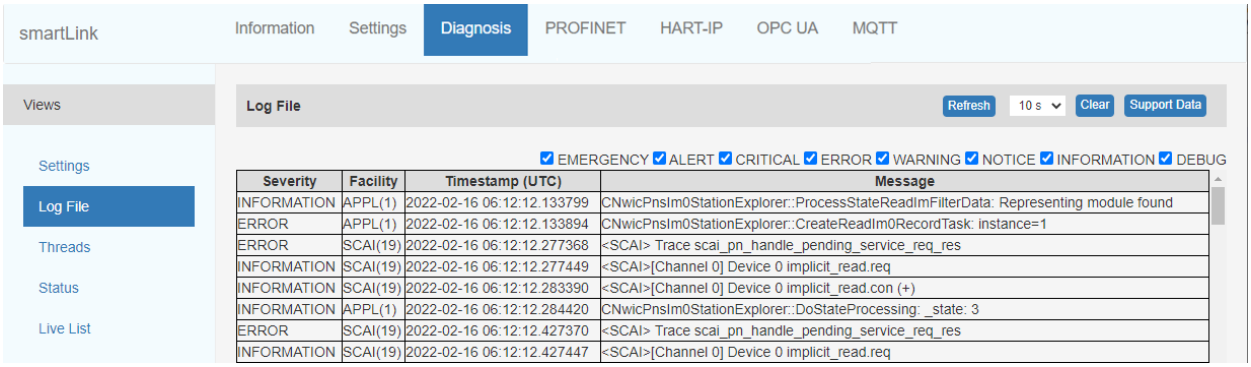
Select **Diagnosis → Settings** to view logging settings. The settings can be viewed in any role. To change the settings you must have administration rights.



Parameters/Actions	Meaning
Log File Priority	Available values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATION. All messages with the set priority or higher are logged. The log file is shown under **Diagnosis → Log File**
Log File Facility	Tick the checkbox for the protocol layer you wish to write to the log file.
Send Syslog Messages	Enables additional Log File Priority DEBUG and sends the information to the network. The syslog can be logged with wireshark, Visual Syslog Server or similar.
Syslog Priority	Available values: EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATION. All messages with the set priority or higher are logged.
Syslog Facility	Tick the checkbox for the protocol layer you wish to write to the syslog file.
Apply	Click **[Apply]** to save your changes in the system. If you do not click apply the changes will not be saved.

5.1.4.2 Log File

Select **Diagnosis → Log File** to view the log file. You can also filter the diagnostic log by ticking and unticking the checkboxes for each notification priority. Filtering only affects the display of the log and not the log file priority set under **Diagnosis → Settings**.



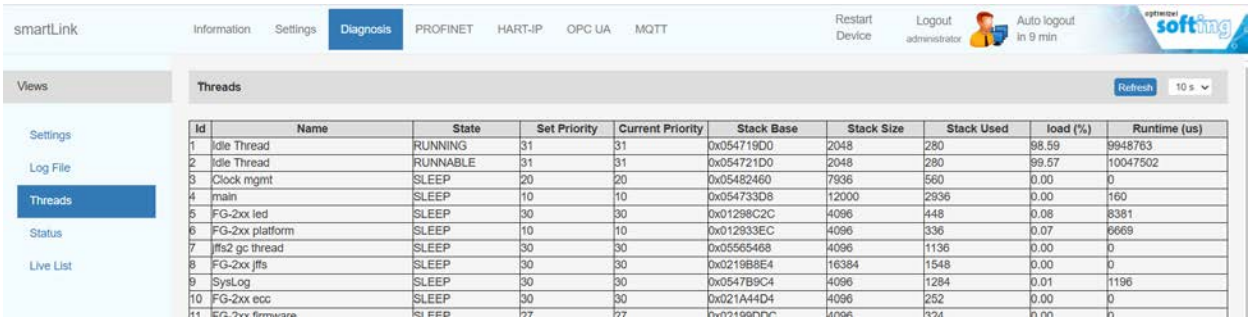
Note

If you are facing problems with your smartLink HW-PN, use the button **[Support Data]** to create a support file. The information contained in this file helps Softing Support address and fix potential issues.

Parameters / Actions	Meaning
EMERGENCY; ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATION, DEBUG	Tick the check boxes to set a display filter.
Clear	Click this button to delete the log file entries.
Refresh	Click this button to update the message log entries based on the filter settings.
Support Data	Click this button to upload a collection of all available logs for support requests.

5.1.4.3 Threads

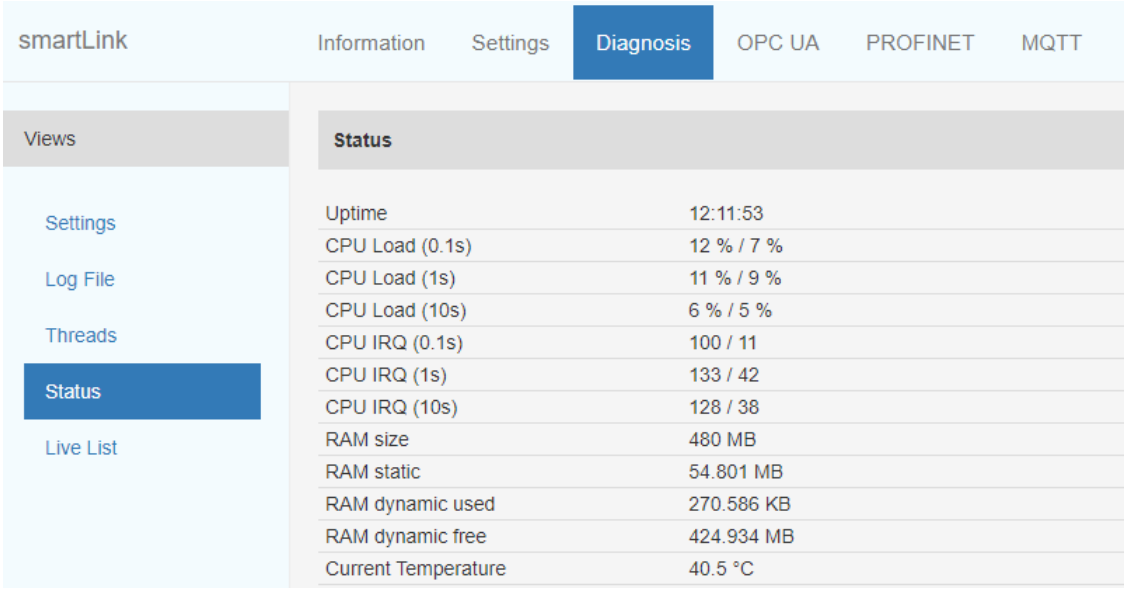
Select **Diagnosis → Threads** to view the current state of the threads. The list you will see and the details contained may not be of any use to you but helps Softing support to diagnose device and performance errors.



Id	Name	State	Set Priority	Current Priority	Stack Base	Stack Size	Stack Used	load (%)	Runtime (us)
1	Idle Thread	RUNNING	31	31	0x054719D0	2048	280	98.59	9948763
2	Idle Thread	RUNNABLE	31	31	0x054721D0	2048	280	99.57	10047502
3	Clock mgmt	SLEEP	20	20	0x05482460	7936	560	0.00	0
4	main	SLEEP	10	10	0x054733D8	12000	2936	0.00	160
5	FG-2xx led	SLEEP	30	30	0x01298C2C	4096	448	0.08	8381
6	FG-2xx platform	SLEEP	10	10	0x012933EC	4096	336	0.07	6669
7	jffs2 gc thread	SLEEP	30	30	0x05565468	4096	1136	0.00	0
8	FG-2xx jffs	SLEEP	30	30	0x0219B8E4	16384	1548	0.00	0
9	SysLog	SLEEP	30	30	0x0547B9C4	4096	1284	0.01	1196
10	FG-2xx ecc	SLEEP	30	30	0x021A44D4	4096	252	0.00	0
11	FG-2xx firmware	SLEEP	27	27	0x02199DDC	4096	324	0.00	0

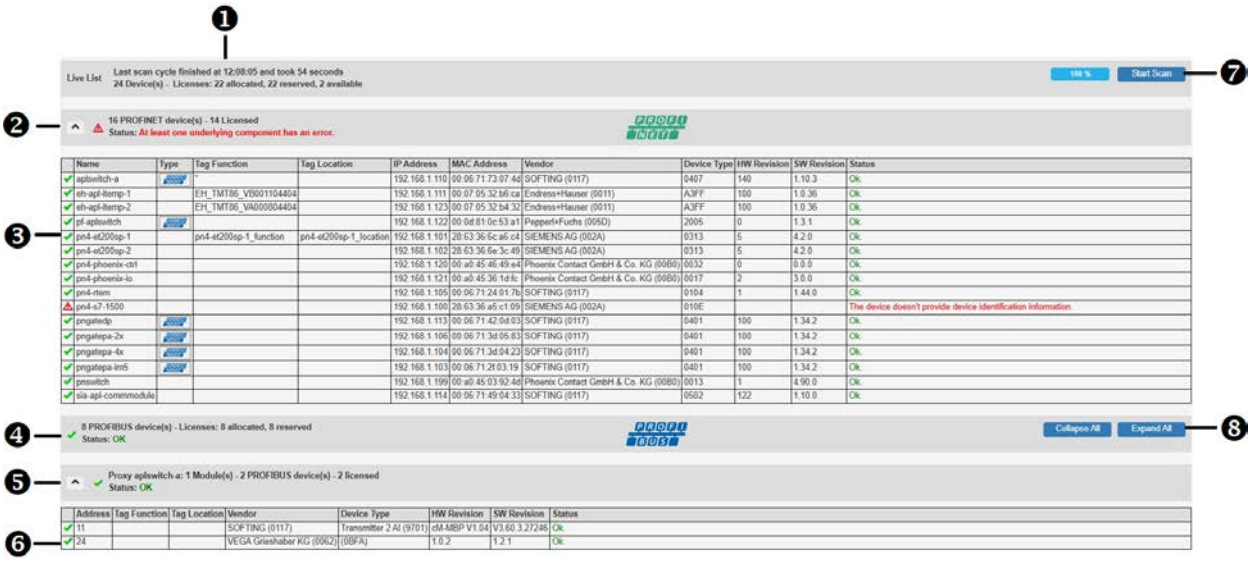
5.1.4.4 Status

Select **Diagnosis → Status** to view gateway diagnostics.



5.1.4.5 Live List

Select **Diagnosis → Live List** to see a table with all PROFINET, APL and PB devices connected to Softing APL switches, pnGate PA, pnGate DP and HART devices connected to supported HART RIOs. The page is divided into several sections, from general scan information to dedicated sections for PROFINET, PROFIBUS, and HART devices.



❶ **Results of the last scan**: The general information includes the timestamp and the duration of the last completed scan, the total number of detected and licensed devices and the number of reserved and remaining licenses.

- **device(s) =** number of PROFINET, PROFIBUS and HART devices in the PROFINET segment
- **allocated =** number of licenses used by a device in the live list
- **reserved =** like allocated but including devices that were deleted from the live list because they are no longer responding
- **available =** number of licenses still available

NOTE: Once a license is assigned to a device, it remains associated with that device even if the device becomes unavailable and is removed from the Live List. The license is released only after all services (such as HART-IP, OPC UA and MQTT) have been deactivated.

❷ **Summary of PROFINET scans**: This header displays the number of detected and licensed PROFINET devices. If PROFINET communication is not working correctly or an error occurs while scanning a PROFINET device, an error icon ⚠ is displayed in the Status column together with the corresponding error information. To show or hide the PROFINET device details, click the arrow icon (⌄) to the left of the header.

❸ **Details of PROFINET scans:** The table lists all scanned PROFINET devices together with their properties, such as name, tag, function, location, IP address, and MAC address. The Type column indicates whether a device has one or more PROFIBUS or HART segments by displaying the corresponding PROFIBUS icon or HART icon. Click the icon to navigate to the corresponding section, where the associated device table is displayed. If an error occurs while scanning a PROFINET device, an error icon is displayed in the leftmost column, and the corresponding error message is shown in the Status column.

❹ **Summary of PROFINET, PROFIBUS and HART proxy scans:** This header sums up the number of detected and licensed PROFIBUS, PROFIBUS and HART devices. A scanning error is indicated by an error icon and the specific error is displayed in the Status.

❺ **Details of PROFINET, PROFIBUS and HART proxies:** The header view shows all proxies of a segment.

❻ **Details of devices:** The table includes all successfully scanned devices with additional properties such as channel number, tag function and location, vendor, device type, hardware and software revision numbers, status. To the left of the device name you may see one of the following icons:
✔ = device is licensed and ⚠ = error occurred during scan of the device

❼ **Scan progress bar (%)**
Indicates the progress of a running scan process.

Start Scan
A scan is started cyclically. The default cycle time is 15 minutes and can be configured on the PROFINET settings page 49. By pressing this button you can invoke a manual scan. When a scan is in progress this button is disabled.

❽ **Collapse All**
Hides all tables with details of connected PROFIBUS devices.

Expand All
Expands all tables with details of connected PROFIBUS devices.

PROFINET table column headers explained

Column Header	Meaning
Name	The device name of the PROFINET device
Type	Indicates if the PROFINET device has a proxy functionality. If so, a corresponding icon is displayed. By clicking on the icon you are navigated to the corresponding proxy section.
Tag Function	Displays the Tag Function contained in the device.
Tag Location	Displays the Tag Location contained in the device.
Address	The Internet Protocol Address is a set of four numbers separated by periods identifying a device in your network.
MAC Address	The Medium Access Control Address is the unique 12-digit hexadecimal device number assigned by device manufacturer.
Vendor	This column displays in brackets the manufacturer Identification code as a hexadecimal value. A vendor name is shown only if this value can be resolved.
Device Type	Displays the type of the PROFINET device as a hexadecimal value.
HW Revision	Displays the hardware revision of the PROFINET device.
SW Revision	Displays the software revision of the PROFINET device.
Status	It is either shown as "OK" (when a PROFINET device has been successfully scanned) or with a red error text describing the error detected during the scan process.

PROFIBUS table column headers explained

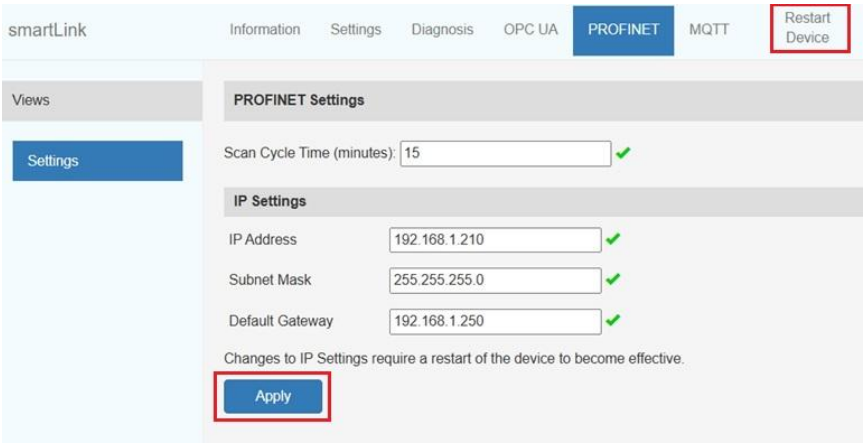
Column Header	Meaning
Address	Displays the address of the PROFIBUS device.
Tag Function	Displays the Tag Function contained in the device.
Tag Location	Displays the Tag Location contained in the device.
Vendor	This column displays in brackets the manufacturer Identification code as a hexadecimal value. A vendor name is shown only if this value can be resolved.
Device Type	Displays the type of the PROFIBUS device as a hexadecimal value in brackets. A device type name is shown if this value can be resolved.
HW Revision	Displays the hardware revision of the PROFIBUS device.
SW Revision	Displays the software revision of the PROFIBUS device.
Status	It is either shown as "OK" (when a PROFIBUS device has been successfully scanned) or with a red error text describing the error detected during the scan process.

HART table column headers explained

Column Header	Meaning
Channel	Wiring position on which the HART device is connected to the module. Values are in the range 0 .. <number of module channels> - 1
Long Tag / Message	For HART devices with HART revision 6 and later, the Long Tag ( )contained in the device is shown. For HART devices with HART revision 5 and earlier, the Message ( )contained in the device is shown.
Vendor	This column displays in brackets the Manufacturer Identification code as a hexadecimal value. A vendor name is shown if this value can be resolved.
Device Type	This column displays in brackets the type of the HART device as a hexadecimal value. A device type name is shown if this value can be resolved.
HART Revision	The HART protocol Major Revision number.
Device Revision	This column displays in brackets the type of the HART device as a hexadecimal value. A device type name is shown if the value can be resolved.
HART Long Address	The unique long address of the HART device.
Status	Licensing state of HART device.

5.1.5 PROFINET

1. Select **PROFINET → Settings** to enter the IP settings that the smartLink HW-PN will use in the PROFINET network.
2. Click **[Apply]** to confirm and activate your settings.
3. Select **Restart Device** in the menu bar to activate the new IP settings.



Parameter	Meaning
Scan Cycle Time	This field defines the scan interval used by the smartLink HW-PN to rescan the PROFINET network.
IP Address	The IP Address used by the smartLink HW-PN in the PROFINET network.
Subnet Mask	The subnet used by the smartLink HW-PN in the PROFINET network.
Default Gateway	The default gateway used by the smartLink HW-PN in the PROFINET network.

5.1.6 HART-IP

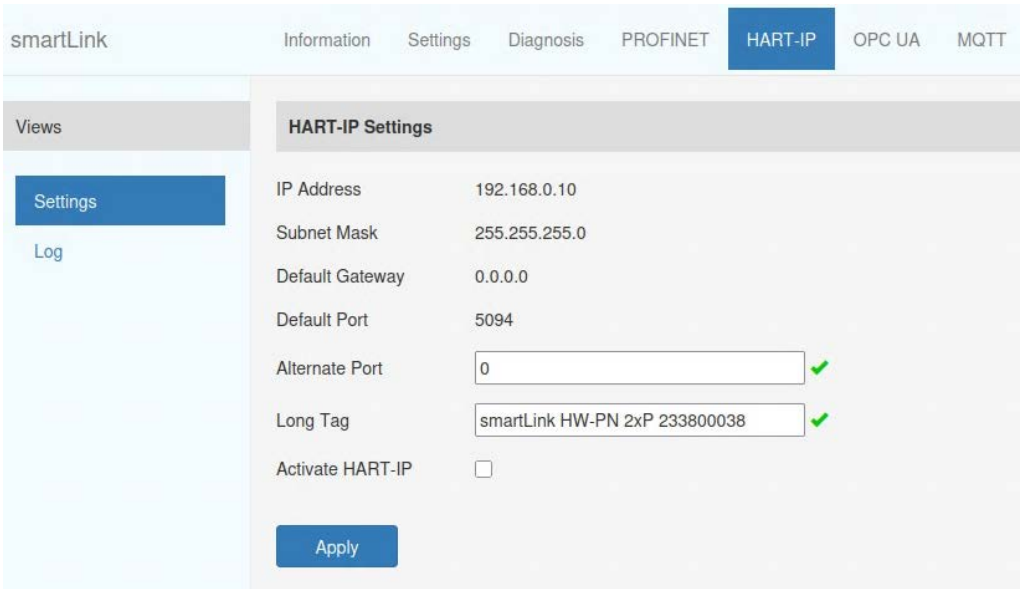
The smartLink HW-PN includes an integrated HART-IP server that provides standardized access to HART field devices connected through supported PROFINET HART proxies.

Asset Management Systems supporting the HART-IP protocol can directly communicate with connected HART devices without using the FDI communication server. For details on connecting an Asset Management System using HART-IP, see Section Network Configuration - HART-IP 62

5.1.6.1 Settings

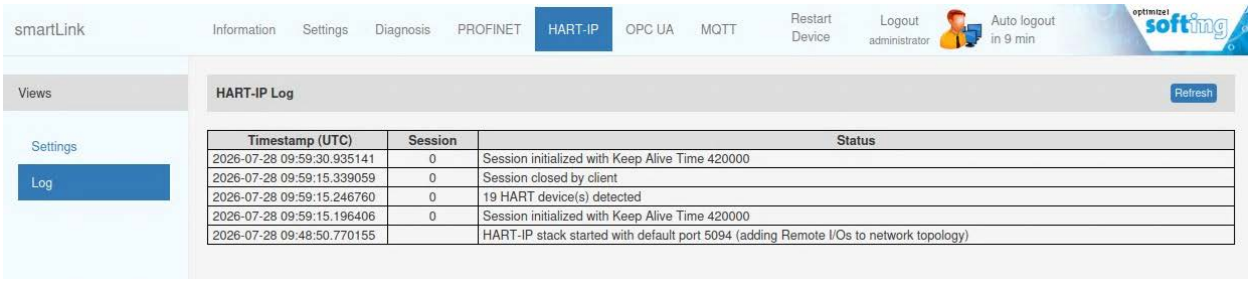
The HART-IP server can be enabled and configured in the HART-IP menu.

1. Select **HART-IP** → **Settings** to see the current settings.
2. Configure the TCP port. The communication is typically run on the default port **5094**.
3. Set the alternate port to use a different port if the default port is already occupied by another protocol.
4. Configure the Long Tag of the smartLink HW-PN .
5. Tick the checkbox **Activate HART-IP** to start the HART-IP server.
6. Click **[Apply]** to confirm and activate your settings.



5.1.6.2 Log

Select **HART-IP → Log** to see details of the HART-IP communication activity. This log file is typically used by Softing support for troubleshooting a problem.



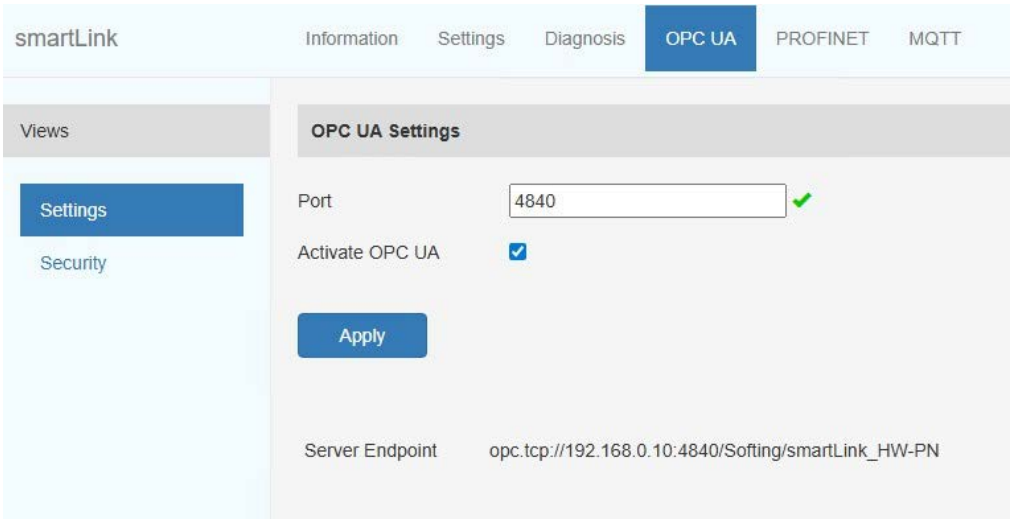
Timestamp (UTC)	Session	Status
2026-07-28 09:59:30.935141	0	Session initialized with Keep Alive Time 420000
2026-07-28 09:59:15.339059	0	Session closed by client
2026-07-28 09:59:15.246760	0	19 HART device(s) detected
2026-07-28 09:59:15.196406	0	Session initialized with Keep Alive Time 420000
2026-07-28 09:48:50.770155		HART-IP stack started with default port 5094 (adding Remote I/Os to network topology)

5.1.7 OPC UA

5.1.7.1 Settings

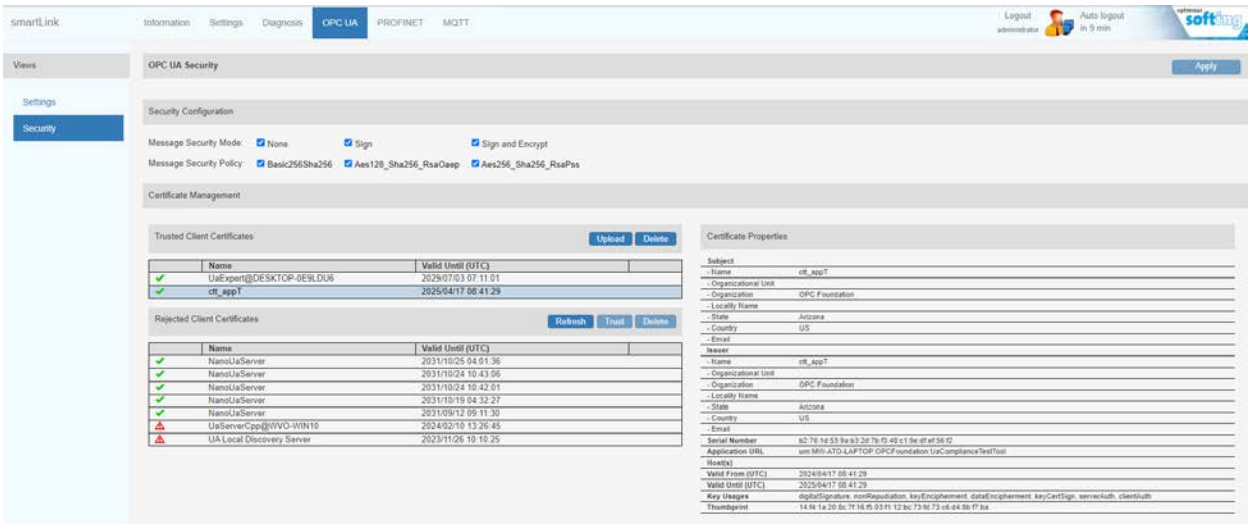
Select **OPC UA → Settings** to configure the OPC UA server and see the server endpoint.

1. Select **OPC UA → Settings** to see the server endpoint.
2. Keep the default port number 4840 or enter another number.
   The valid value range is [1..65535].
3. Tick the checkbox **Activate OPC UA** to start the OPC UA server.
   A pencil icon appears.
4. Click **[Apply]** to confirm the settings.
   The pencil icon is no longer visible.

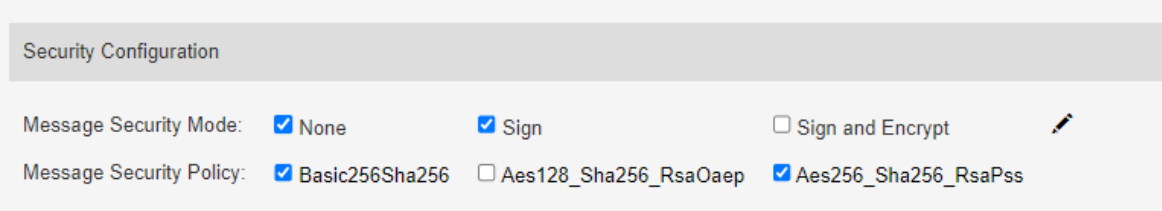


5.1.7.2 Security

Select **OPC UA → Security** to configure a secure communication between the smartLink HW-PN (OPC UA server) and the OPC UA client application.



In the **Security Configuration** window frame, smartLink HW-PN offers three encryption modes supported by three security policies for secure OPC UA communication:



If you have changed any of the security configuration setting, a pencil icon is shown to indicate that the settings have been changed but have not yet been applied and the changes still need to be executed by clicking **[Apply]** in the top right corner.

Message Security Modes	Meaning
None	Don't use any encryption. No certificate exchange is needed between smartLink HW-PN and a client. Be aware that communication on the network is readable by others. This might be a security risk.
Sign	Messages sent from smartLink HW-PN or the OPC UA client are signed with the private key of the sender. The receiving entity can validate the origin of the message using the public key of the sending entity. Nevertheless, messages are not encrypted.
Sign and Encrypt	Message are signed as in the Sign mode and additionally encrypted with the public key of the receiving entity. On the receiver side the message can be decrypted using its private key.

If you check **None**, no security policy must be selected. For the modes **Sign** and/or **Sign and Encrypt** at least one policy must be chosen. Although any combination of modes and policies is possible, it is recommended to restrict the configuration to the one that the OPC UA client application is expected to use. For further details see the documentation of the client application.

To establish a secure OPC UA communication smartLink HW-PN and the OPC UA client application have to exchange their public keys. For this they store a certificate of the communication partner in their Public Key Infrastructure (PKI). The OPC UA client application typically receives the public key of smartLink HW-PN by calling the OPC UA service **GetEndpoints**. Alternatively, it can be exported from smartLink HW-PN (**Settings → Certificates → Server Certificate → Download**) and imported manually in the client application. See also the OPC UA client application documentation for more information on how to store the smartLink HW-PN certificate in the **Trusted** section of its PKI.

The **Certificate Management** window frame shows all certificates that are trusted or have been rejected (as a result of an unsuccessful connection attempt from the client application). When an OPC UA client application attempts to open a secure connection to a smartLink HW-PN it submits its client certificate. smartLink HW-PN stores this certificate in the **Rejected Client Certificates** table (see screenshot above). Before a connection between the smartLink HW-PN and the client can be established you have to confirm that you trust this certificate. If the certificate is available as a file, you may upload it directly to the **Trusted Client Certificates**.

The tables include the subject name and the expiration timestamp of each certificate. The first column either shows a checkmark indicating that the certificate's status (= valid, = expired/not valid). You can upload new or delete existing client certificates to the **Trusted Client Certificates** and move client certificates from the **Rejected Client Certificates** table the **Trusted** section or simply delete them from the PKI.

Note

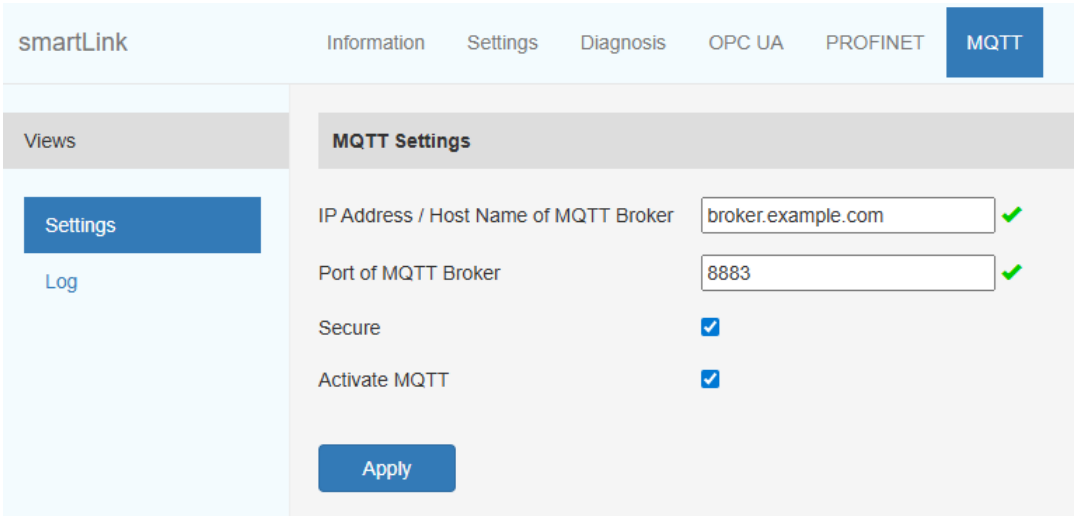
Your changes are not executed immediately but have to be confirmed by clicking **[Apply]** in the top right corner of the page. This will restart the OPC UA server component of smartLink HW-PN. Any clients connected at that time will lose their connection but typically will automatically reconnect.

For a detailed view of the common client certificate properties, select and highlight a certificate in either table as shown in the screenshot above (example certificate: *ctt_appT*).

5.1.8 MQTT

5.1.8.1 Settings

1. Select **MQTT → Settings** to set the broker parameters.
   When you have changed the values in the input field, a pencil icon is shown.
2. Enter the **IP address** or **Host Name** of the broker if you intend to activate MQTT.
   The host name must conform to the standard IP host name rules defined in RFC 952 and RFC 1123. See details below.
3. Keep the default port number 1883 or set another number.
   The valid value range is [1..65535]. The default port for unsecured MQTT communication is 1883. The default port for secured MQTT communication is 8883.
4. Tick the checkbox **Secure** to establish a secure connection to the broker via TLS.
5. Tick the checkbox **Activate MQTT** to start the MQTT client.
   A pencil icon appears.
6. Click **[Apply]** to confirm the settings to the desired values.
   The pencil icon is no longer shown.



Host name rules

Allowed characters
- Letters: a-z (case-insensitive)
- Digits: 0-9
- Hyphen: -

Hyphen restrictions
- A label must not start or end with a hyphen (for example `host.example-.com` is invalid)

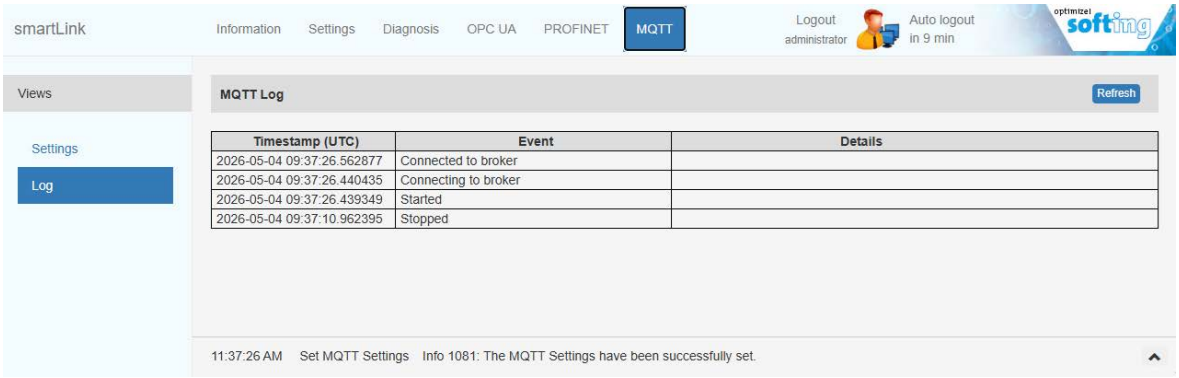
Length limits
- Max 63 characters per label
- Max 253 characters total (including dots)

Empty labels
- A label must not be empty (for example `host..com` is invalid)

Numeric only labels
- A label must not consist solely of digits (for example `123.example.com` is invalid)

5.1.8.2 Log

Select **MQTT → Log** to see details of the MQTT communication activity. This log file is typically used by Softing support for troubleshooting a problem.



5.2 Connecting to Emerson AMS Device Manager

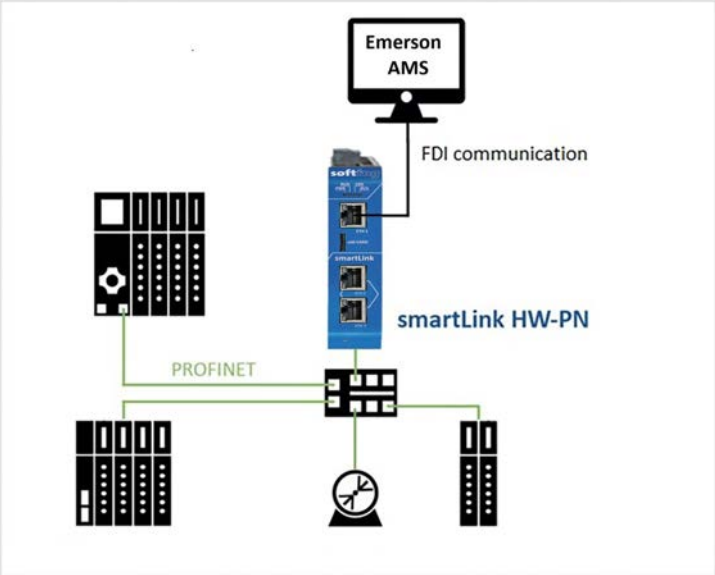
The Emerson AMS Device Manager is a software platform used for managing and maintaining field devices in industrial automation systems. It is part of Emerson's broader suite of asset management solutions, designed to help operators and maintenance engineers optimize the performance, reliability, and lifespan of their instrumentation and control devices.

The smartLink HW-PN supports two different communication methods for connecting Emerson AMS Device Manager to field devices:

- FDI communication using the integrated OPC UA server
- HART-IP communication using the integrated HART-IP server

Both methods provide access to connected field devices. The recommended communication path depends on the supported functionality of the Asset Management application and the connected devices. For details on configuring the HART-IP server, see Section HART-IP 50 .

The Emerson Asset Management System and FDI Communication



The following section describes how to configure your network using the Emerson Asset Management System. For details see also the Emerson installation guide provided with the AMS (Chapter Prerequisites 57). Changes to the I&M data (Identification and Maintenance) of PROFINET and PROFIBUS devices connected to the network are automatically displayed in the Live List 46 of the smartLink HW-PN user interface.

5.2.1 Prerequisites

Emerson AMS

- AMS version 15.0 or later must be installed on your PC.
- The FDI Communication Server must be enabled. See the Installation Guide PDF file for details (**AMS Devices Manager → Installation Guide**).

smartLink HW-PN

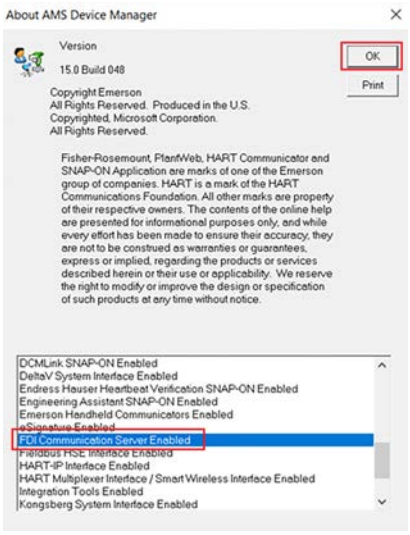
- Your smartLink HW-PN is properly commissioned (see Chapter Commissioning 25).
- Your smartLink HW-PN has sufficient licenses available (see Chapter Licensing 40).

- OPC UA Security must be enabled in the user interface. See **OPC UA** 52 → **Security** 52 .
- **HART-IP server** is activated for Segment DP1 (see **HART IP Settings** 55).
- **Add Remote IOs to Network Topology** is activated.

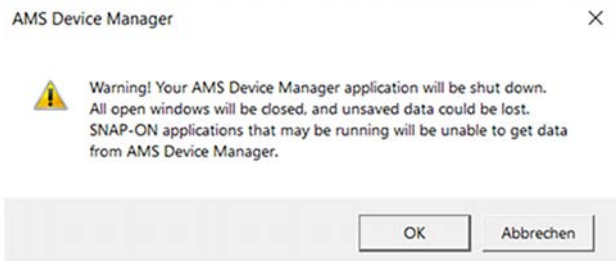
Note
The time of your smartLink HW-PN must have been updated and the validity of your server certificate must have been checked before setting up the OPC UA security.

5.2.2 Network configuration - FDI

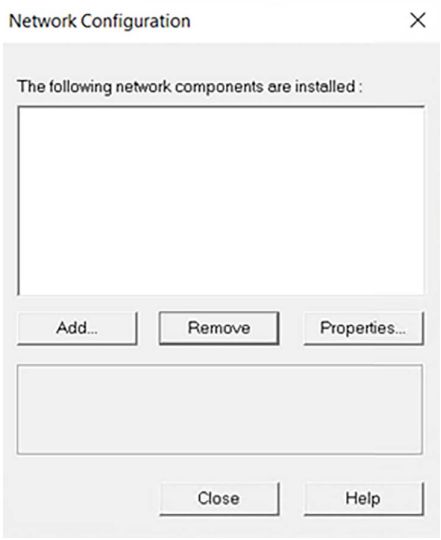
1. Click **Windows Start → AMS Devices Manager → About AMS Device Manager**.
   The following window opens.



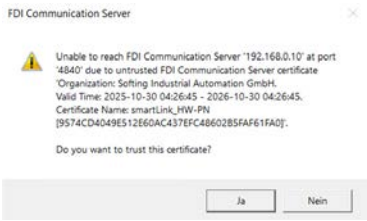
2. Verify that **FDI Communication Server Enabled** is shown .
3. Click **[OK]**.
4. Click **Windows Start → AMS Devices Manager → Terminate Servers** to stop the AMS Devices Manager.
5. Click **[OK]** in the Warning pop-up window.



6. Click **Windows Start → AMS Devices Manager → Network Configuration**.
   The AMS network configuration window opens.



7. Click **[Add]**.
8. Select the component **FDI Communication Server Network or HART-IP Network (**from the list.
9. Click **[Install...]** and follow the on-screen instructions.
10. Enter a unique **Network Name.**
    The name you enter here (e.g. smartLink HW-PN) will later appear under the physical networks the AMS Device Manager.
11. Click **[Next]**.
12. Enter the DNS or IP address of your smartLink HW-PN and the port configured in the OPC UA settings 52.
13. Click **[Finish]**.
    A dialog window opens.



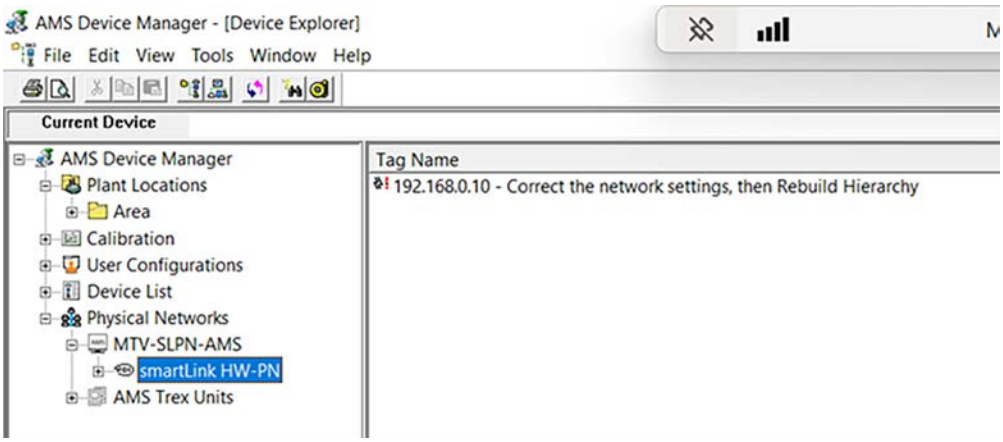
14. Click **[Yes]** to confirm that you trust the server certificate of the smartLink HW-PN.
    Your smartLink HW-PN is now shown as available network components by the network name you entered above.

15. Click **[Close]**.

5.2.3 AMS Device Manager - FDI

1. Click **Windows Start → AMS Devices Manager → AMS Devices Manager**.
   The AMS device manager window opens.

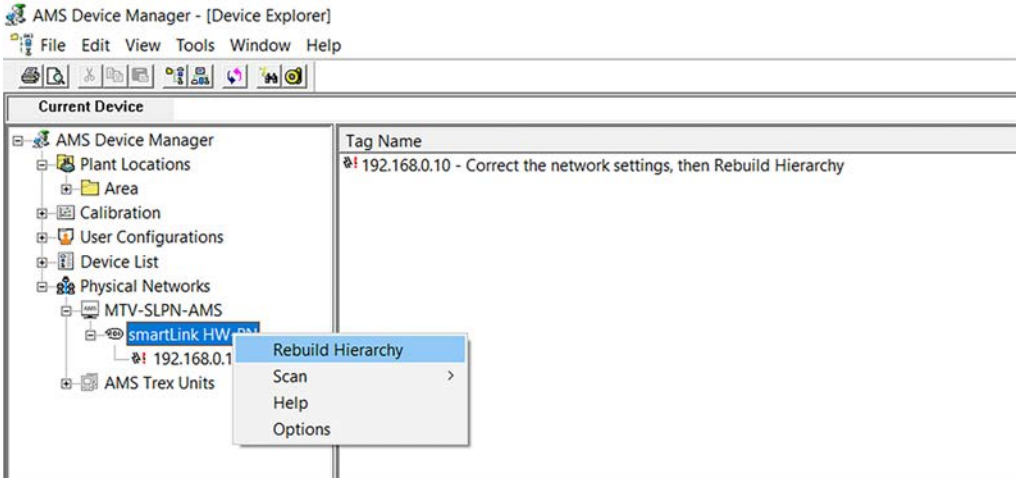
2. Expand **Physical Networks** in the navigation tree on the left.



3. Expand the node for your local PC under Physical Networks (here *MTV-SLPN-AMS*).

4. Select the FDI Communication Server Network node name you entered previously (here *smartLink HW-PN*).

5. Right-click the node name and select **Rebuild Hierarchy**.



Note
The connection is rejected by the smartLink HW-PN as it is not yet trusted.

6. Open the smartLink HW-PN user interface[28] and log in as administrator.

7. Select **OPC UA**[52] → **Security**[52].
   In the section Rejected Client Certificates you should now see the new entry FDICommServer.

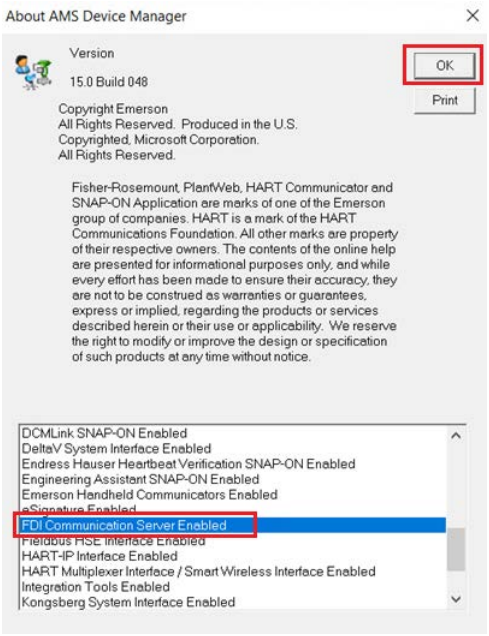
8. Select **FDICommServer** and click **[Trust]**.

9. Click **[Apply]** in the right top corner to confirm the settings on the OPC UA Security page.

10. Return to the AMS Device Manager and repeat steps 4 and 5 above.
    The connection is now established.

5.2.4 Network configuration - HART-IP

1. Click **Windows Start → AMS Device Manager → About AMS Device Manager** to verify, whether your AMS version supports HART-IP network components. The following window opens.

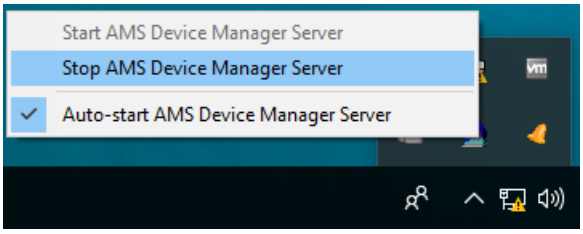


2. Scroll down in the drop-down list to see if you can find **HART-IP Interface Enabled**.

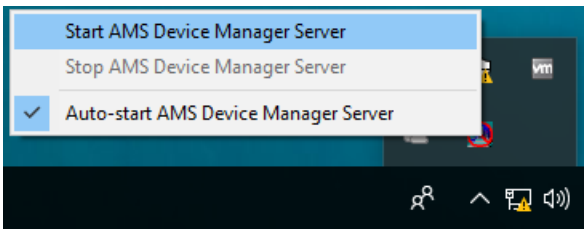
Note

You will not be able to configure HART-IP if your AMS version does not have a HART-IP licence.

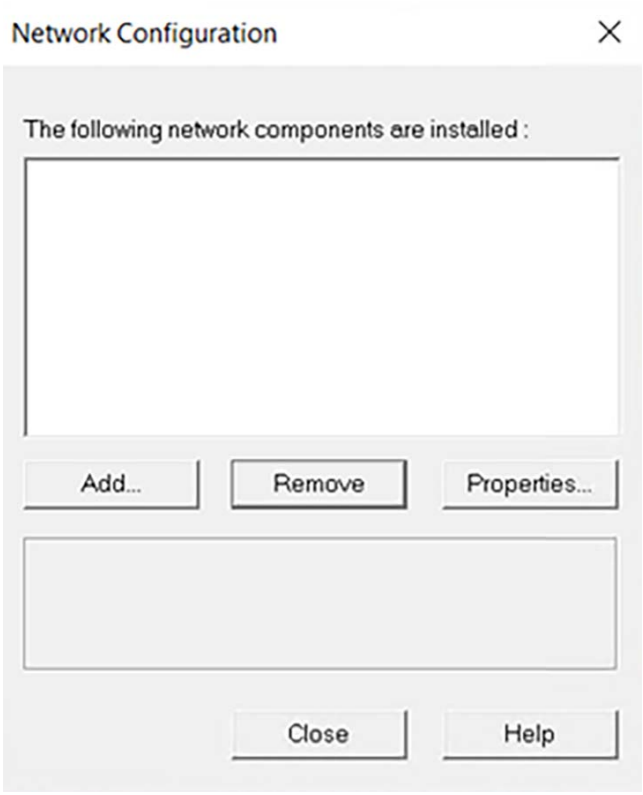
3. Click **[OK]**.
4. Right-click the icon at the bottom of your screen and select **Stop the AMS Device Manager Server**.



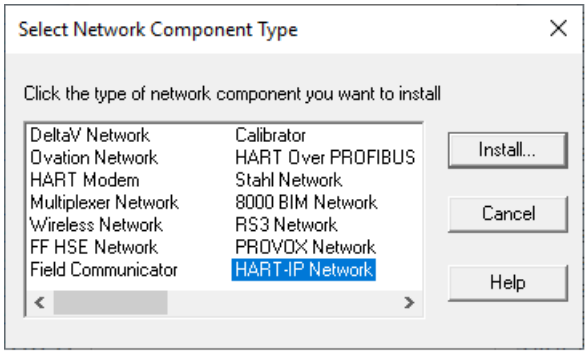
5. Wait a second.
6. Now right-click the icon at the bottom of your screen again and select **Start the AMS Device Manager Server**.



7. Click **Windows Start → AMS Devices Manager → Network Configuration**.
   The AMS network configuration window opens.

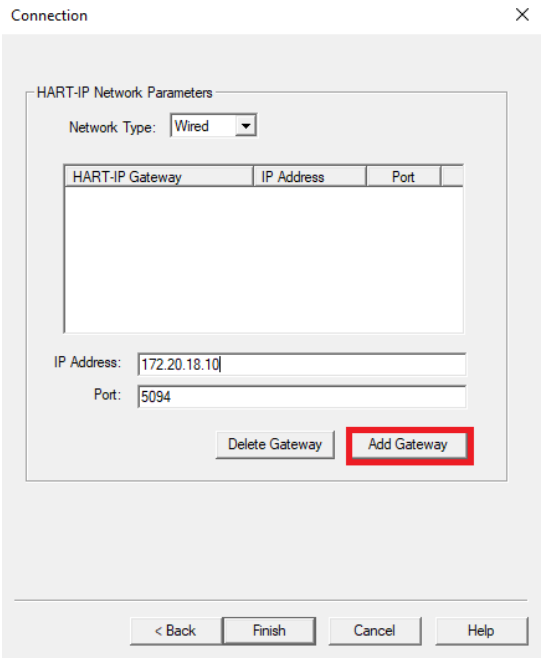


8. Click **[Add]**.
9. Select the component **HART-IP Network** from the list.
10. Click **[Install...]** and follow the wizard on-screen instructions.



11. Enter a unique name in the Network Name input field and click **[Next]**.

12. Enter the IP address of your smartLink HW-PN.
    Keep the default port 5094.



13. Click **[Add Gateway]**.
    The added gateway is shown with the corresponding IP address.

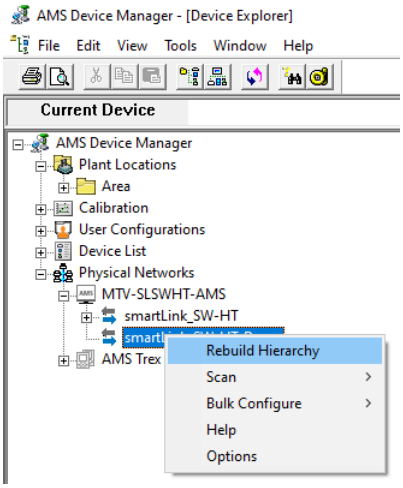
14. Click **[Finish]**.
    Your smartLink HW-PN is now shown as available network component by the name and the corresponding IP address you entered.

15. Click **[Close]**.

5.2.5 AMS Device Manager - HART-IP

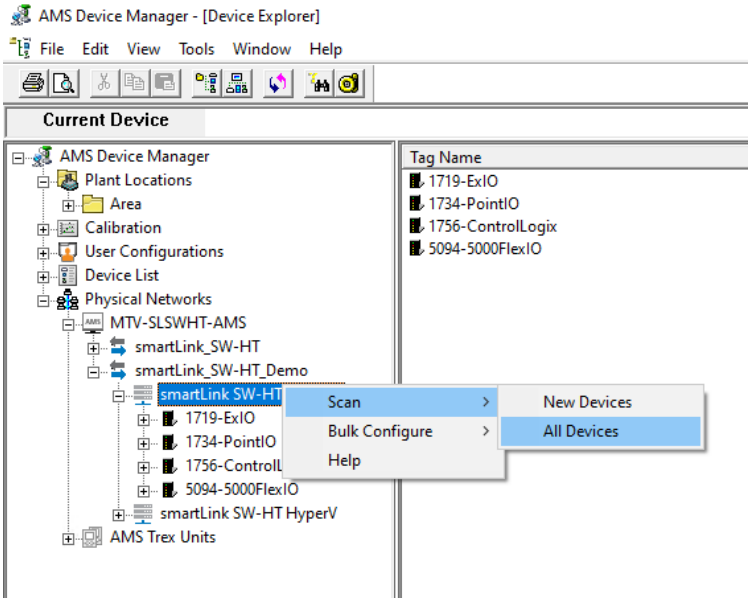
For details on how to connect your smartLink HW-PN over HART-IP with an Asset Management System (AMS) see also section HART-IP 50.

1. Click **Windows Start → AMS Device Manager → AMS Device Manager**.
   The AMS device manager window opens.



2. Right-click a smartLink HW-PN and select **Rebuild Hierarchy**.
   The device returns the configured HART IO modules as HART Cards.

3. Right-click a smartLink HW-PN and select **Scan → All Devices** to identify connected HART devices.



4. When the scan has finished you can continue configuring the HART Devices.

Note

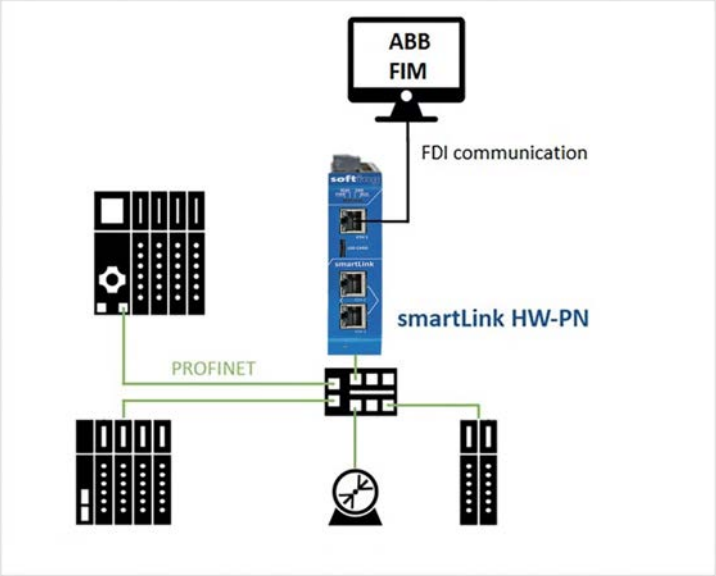
Proceed by following the instructions in the Emerson AMS manual.

5.3 Connecting to ABB FIM

The following chapter describes how to connect with the ABB Field Information Manager (FIM) to configure, parameterize, troubleshoot and maintain field devices.

For more information on managing your network assets in FIM, refer to the ABB Ability™ Field Information Manager User Guide.

Asset Management and Parameterization of PROFINET Devices

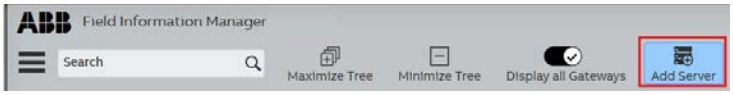


5.3.1 Prerequisites

- Your smartLink HW-PN is properly commissioned (see Chapter Commissioning 25).
- Your smartLink HW-PN has sufficient licenses available (see Chapter Licensing 40).
- The ABB Field Information Manager (FIM) version 3.3 or higher is installed.

5.3.2 Connecting to smartLink HW-PN

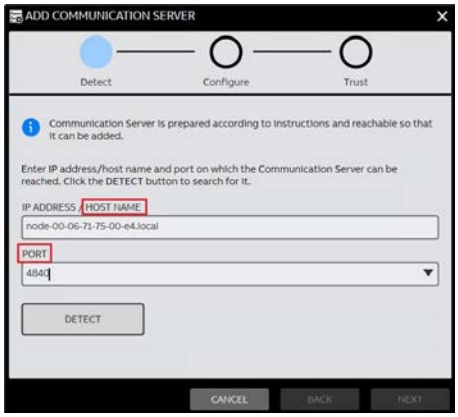
1. Go to the product page of smartLink HW-PN and download the latest FDI package.
2. Right-click the ABB FIM icon to start the application.
3. Import the downloaded FDI package in ABB FIM as described in Importing an FDI package/FIMlet 71 .
4. Select **Add Server** in the FIM menu.



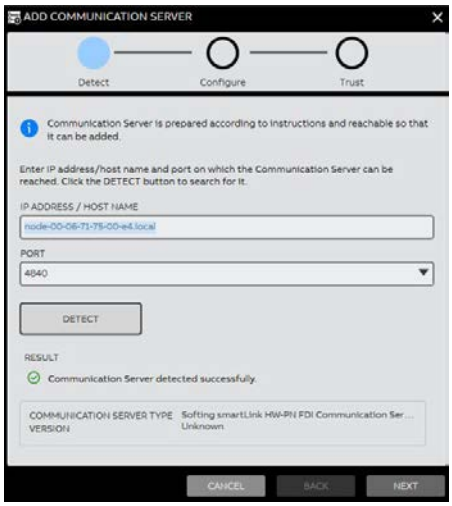
The **ADD COMMUNICATION SERVER** popup window appears. Here you are prompted to enter the hostname (see Settings 32 → Network 32) and the port configured in OPC UA settings 52 .

Note

For security reasons, FIM currently does not support connections using an IP address. Please use the host name of the smartLink HW-PN.



5. Click **[DETECT]** to continue.



6. Click **[NEXT]** if the smartLink HW-PN was detected.

7. Enter a unique name in the DISPLAY NAME field representing the smartLink HW-PN in the FIM client.
   The smartLink HW-PN will be shown under this name in the FIM topology view.

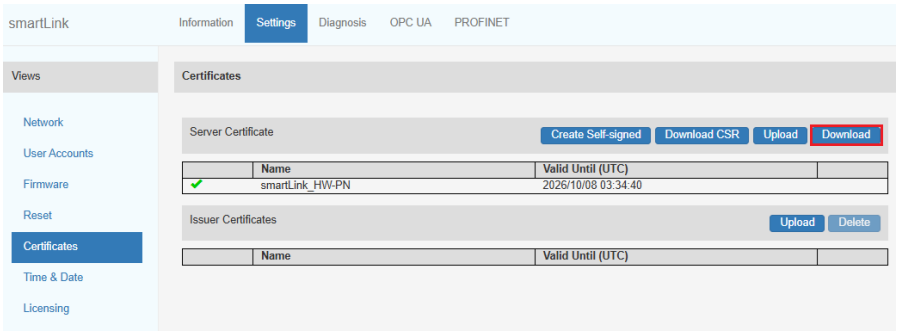
8. If no Trust relationship is required, click **[ADD]** to finalize establishing a connection to the smartLink HW-PN in ABB FIM and continue with scanning for devices 72 .

9. If a Trust relationship is required, click **[NEXT]** and continue with the steps below.

   a) Log in to web server of smartLink HW-PN .

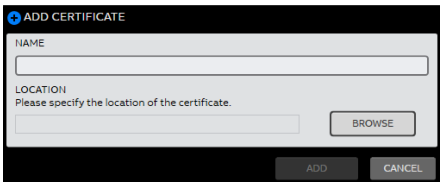
   b) Go to page Certificates[38] → Time & Date[39] and verify that the time of your smartLink HW-PN is correctly set. If the time /date is incorrect, the server certificate may be outdated and invalid. In this case it is recommended to create a new server certificate.

   c) Go to page Settings[32] → Certificates[38] and click **[Download]** to save the server certificate on your PC.



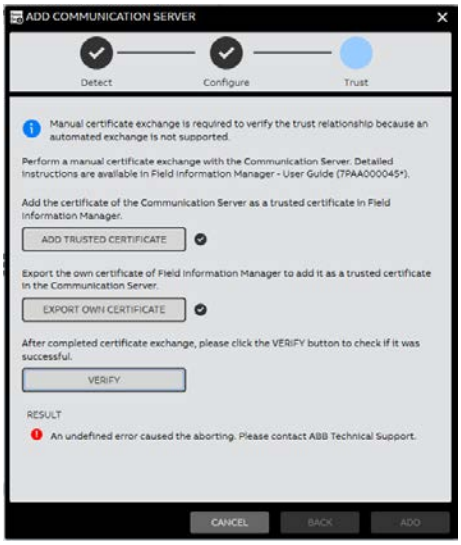
10. Return to the ABB FIM application

11. Click **[ADD TRUSTED CERTIFICATE]**.

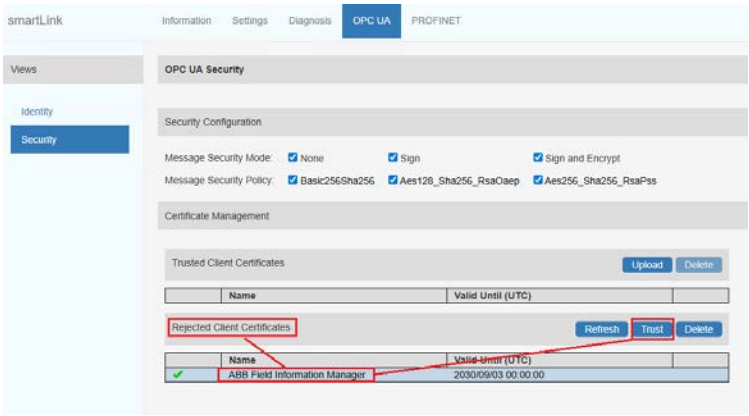


12. Click **[Browse],** select the previously downloaded server certificate of the smartLink HW-PN and click **[Add]**.

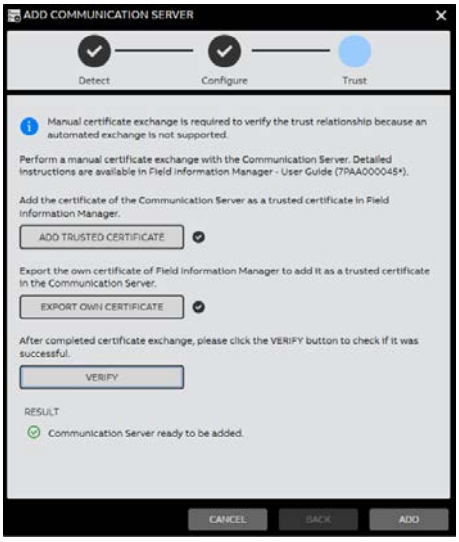
13. Click **[VERIFY]** to check if the certificates have been added successfully.
    The verification will fail because ABB FIM is not yet trusted by smartLink HW-PN.



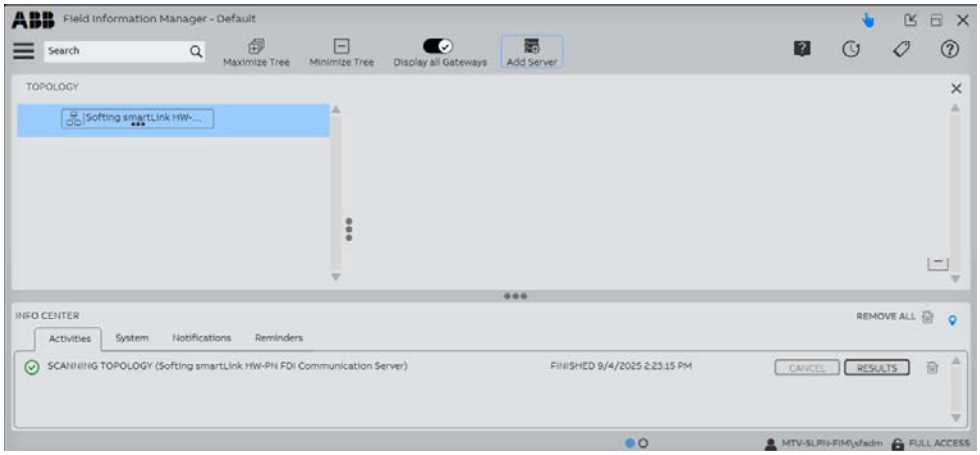
14. Return to the smartLink HW-PN user interface and select OPC UA [52] → Security [52].
15. In the section **Rejected Client Certificates**, select the **ABB Field Information Manager** certificate and click **[Trust]**.



16. Click **[Apply]** in the right top corner to confirm the settings on the OPC UA Security page.
17. Return to the configuration settings in the **ADD Communication Server** window of the ABB FIM.
18. Click **[VERIFY]** to ensure that the certificate exchange with the smartLink HW-PN is successful.



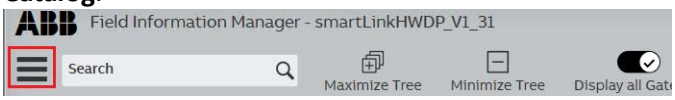
19. Click **[ADD]** to finalize the connection setup to smartLink HW-PN.
The FIM topology view will open automatically.



5.3.3 Importing an FDI package/FIMlet

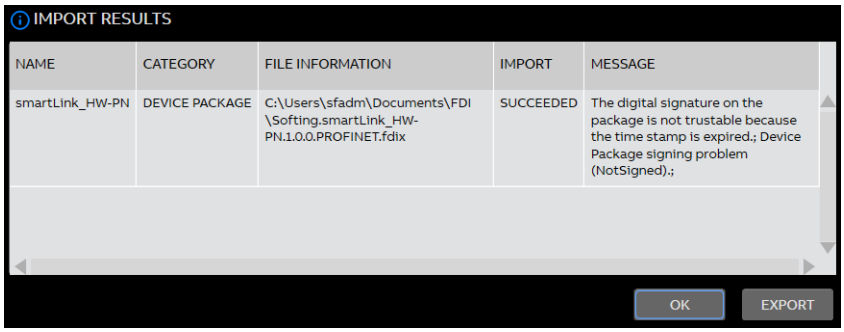
1. Double-click the **ABB FIM** icon to start the application.

2. Select the burger **Menu** icon in the top left corner and select the menu option **Device Catalog**.



3. Click **[Import]** and select the corresponding file with the .fdi extension to import the FDI package or FIMlet in ABB FIM.

4. Click **[Import]**.
When successfully imported the file will be shown in the Import Results window.

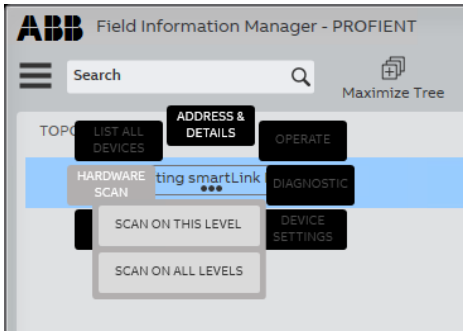


5.3.4 Scanning for devices

Note

If you are using an APL switch or a pnGate and want to scan for the connected PROFIBUS devices you have to download the device package or FIMLET from the corresponding product page and import it in ABB FIM as described in the previous Chapter Importing an FDI package/FIMlet 71.

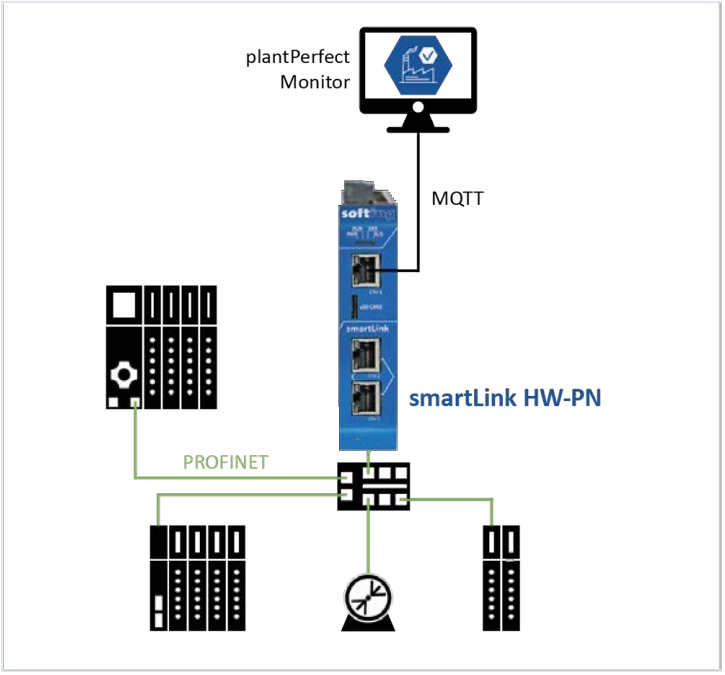
1. Open the ABB FIM Topology view.
2. Click the ellipsis icon ••• in the device tile representing the smartLink HW-PN in the Topology view.



3. Select the option **HARDWARE SCAN → SCAN ON ALL LEVELS** to scan for the available PROFINET and PROFIBUS devices.

5.4 Connecting to plantPerfect Monitor

plantPerfect Monitor is a Softing OT network monitoring tool for centralized, plant-wide monitoring of PROFINET and PROFIBUS networks.



Note

For details on how to connect your smartLink HW-PN to the plantPerfect Monitor, see the Section MQTT[55] and the plantPerfect Monitor user guide available for download from the plantPerfect Monitor product website.

5.4.1 Prerequisites

- Your smartLink HW-PN is properly commissioned (see Chapter Commissioning[25])
- Your smartLink HW-PN has sufficient licenses available (see Chapter Licensing[40])
- plantPerfect Monitor is installed.

5.4.2 Connecting to an MQTT broker

To establish a connection to plantPerfect Monitor, configure the MQTT broker of the plantPerfect Monitor in the MQTT Settings[55] of the smartLink HW-PN.

- Enter IP address and port of the MQTT broker.
- Tick the checkbox for **Activate MQTT** in the MQTT Settings menu.

6 Performance

The table below shows the average response time in seconds for HART requests to devices connected through supported PROFINET HART proxies, based on performance tests.

During the tests, HART-IP requests were sent to HART devices using HART commands without a request payload (1, 3, 7, 8, 13, 14, 16, and 48). The measured response time represents the elapsed time between sending a request to the smartLink HW-PN and receiving the corresponding response.

The measured values depend on the type of HART device, the connected PROFINET HART proxy, and the device's internal processing time. Therefore, the values shown below should be regarded as typical reference values rather than guaranteed response times.

Response times may increase when multiple HART requests are processed simultaneously on the same PROFINET HART proxy or HART I/O module.

Note

To optimize HART communication performance, disable unused HART channels in the engineering configuration of the corresponding PROFINET HART proxy whenever possible.

Siemens	Duration in sec
CFU Compact Field Unit HART (6ES7655-5PX41-1XX0)	1.4
ET200IM AI 4xI 2-wire HART	1.5
ET200IM AQ 4xI HART	1.5
ET200iSP 4AO HART, 4-20 mA (6ES7135-7TD00-0AB0)	2.6
ET200iSP 4AI HART, 2DMU (6ES7134-7TD00-0AB0)	1.7
ET200iSP 4AI HART, 4DMU (6ES7134-7TD50-0AB0)	2.2
ET200iSP 4F-AI HART Ex (6ES7138-7FA00-0AB0)	2.2
ET200M SM 331, 2AE, 0/4 - 20mA HART (6ES7331-7TB10-0AB0)	0.9
ET200M SM 332, 2AA, 0/4 - 20mA HART (6ES7332-5TB10-0AB0)	1.1
ET200M SM 331, 8AE, 0/4 - 20mA HART (6ES7331-7TF01-0AB0)	2.3
ET200M SM 332, 8AA, 0/4 - 20mA HART (ES7332-8TF01-0AB0)	2.0
ET200M SM 336, F-AI 6x, 0/4-20 mA HART (6ES7336-4GE00-0AB0)	1.8
ET200MP AQ 8xHART HF (6ES7532-8TF00-0AB0)	1.2
ET200MP AI 8xHART HF (6ES7531-7TF00-0AB0)	2.6
ET200R1 AI 4xI 2-wire HART HF (6ES7134-6TD00-0CA1)	1.4
ET200S2 AO 4xI HART HF (6ES7135-6TD00-0CA1)	1.5
ET200SP HA AI 16xI 2-wire HART HA (6DL1134-6TH00-0PH1)	1.2
ET200SP HA F-AI 8x, 2-/4-wire HART (6DL1136-6AA00-0PH1)	2.5
ET200SP HA AI 4xI 2-/4-Wire HART ISOL (6DL1134-6UD00-0PK0)	1.4
ET200SP HA AI-DI/DQ 16/16x24VDC HART (6DL1133-6EW00-0PH1)	1.2
ET200SP HA AI-DI/DQ 16/16x24VDC HART (6DL1133-6EW00-0PH1)	1.5
ET200SP HA AQ 4xI HART ISOL (6DL1135-6UD00-0PK0)	1.2
ET200SP HA Ex-AI 2xI 2-wire HART (6DL1134-6TB00-0HX1)	1.7
ET200SP HA Ex-AQ 2xI 2-wire HART (6DL1135-6TB00-0HX1)	2.1

7 Troubleshooting

smartLink HW-PN generates status messages displayed in the live list of the user interface (select **Diagnosis → Live List**). The table below explains the possible cause for each message and where applicable, provides a corresponding corrective action.

Status	Possible Cause	Solution/Required Action
Failed to read I&M1 parameter.	The device is busy, or the live list scan has not yet completed.	Wait until the live list scan has completed, or verify that the device supports the I&M1 feature.
PROFINET Service Error.	The same IP address is assigned to multiple devices on the PROFINET network.	Check the PROFINET network for duplicate IP addresses and assign a unique IP address to each device.
The station IP address is not set.	The IP address has not yet been assigned to the device by the controller, or it was lost following a reboot.	Ensure that an IP address is assigned to the PROFINET device and remains configured after a reboot.
The device doesn't provide device identification information.	The device does not permit its actual identification information to be read. Therefore, no identification information is published for this device via MQTT.	N/A
The station did not report any head-module interfaces.	The station did not report a valid PROFINET head-module interface.	Check the PROFINET interface configuration and the station firmware.
The query IP address is assigned to multiple reported head-module interfaces.	The queried IP address is assigned to multiple reported interfaces.	Check the network for duplicate IP addresses and correct the station configuration.
The query IP address is not assigned to any reported head-module interface.	The queried IP address does not correspond to a reported PROFINET interface.	Verify the station IP address and correct the IP configuration if required.
The station reported conflicting basic identification information.	The station reported inconsistent identification data.	Check the station configuration and firmware. Restart the station and retry.
The station failed to provide I&M0 filter data.	The station did not provide the expected I&M0 filter information.	Check I&M support and firmware. If I&M0 is not required, the warning can normally be ignored.
The station failed to provide I&M0 data.	The station did not provide I&M0 identification data.	Check whether I&M2 is supported and configured. Configure it if required.
The station failed to provide I&M1 data.	The station did not provide I&M1 data.	Check whether I&M1 is supported and configured. Configure it if required.
The station failed to provide I&M2 data.	The station did not provide I&M2 data.	Check whether I&M2 is supported and configured. Configure it if required.
The station failed to provide I&M3 data.	The station did not provide I&M3 data.	Check whether I&M3 is supported and configured. Configure it if required.
The station failed to provide I&M4 data.	The station did not provide I&M4 data.	Check whether I&M4 is supported and configured. Configure it if required.

Status	Possible Cause	Solution/Required Action
An OPC UA connection cannot be established, or access via HTTPS is not possible.	The device's time settings under Settings →Time & Date are incorrect, have been reset, or the device was switched off for an extended period and its time settings were lost.	Reset the time under Settings →Time & Date 39 . Check under OPC UA → Security 52 whether the certificate has been listed as Rejected as a result of the incorrect time settings. If so, select the certificate under Rejected Client Certificates and click Delete to remove it from the list. Verify that the certificate is now listed only under Trusted Client Certificates.

8 Declaration of conformity

This device is compliant with EC directive 2014/30/EG, "Electromagnetic Compatibility" (EMC directive) and meets the following requirements:

- EN 55011 Industrial, scientific and medical (ISM) devices - radio disturbance - limits and methods of measurement
- EN 55032 Electromagnetic compatibility of multimedia equipment (MME) and interference emission
- EN 61000-6-4 Electromagnetic compatibility (EMC); Part 6-4: generic standard – emission for industrial environments
- EN 61000-6-2 Electromagnetic compatibility (EMC); Part 6-2: generic standard - immunity for industrial environments

Note
To fulfill the EMC requirements, the other components of your installation (DC adapter, Industrial Ethernet devices, etc.) also have to meet the EMC requirements. A shielded cable must be used. In addition, the cable shield must be grounded properly.

CAUTION
This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures!

CE
The CE marking indicates conformity with the above standards in a Declaration of Conformity which can be requested from Softing Industrial Automation GmbH.

RoHS
This product is compliant the Restriction of Hazardous Substances under Directive 2002/95/EC.

FCC
This equipment has been tested and found to comply with the limits for a Class A digital device, under part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications.

VCCI
This Class A product conforms to the regulations of Voluntary Control Council for Interference (VCCI) by Information Technology Equipment.

WEEE
Electrical and electronic equipment must be disposed of separately from normal waste at the end of its operational lifetime in compliance with Waste Electrical & Electronic Equipment (WEEE) Directive 2002/96/EC. Packaging material and worn components shall be disposed of according to the regulations applicable in the country of installation.

EU-Konformitätserklärung
EU Declaration of Conformity

Wir
We

Softing Industrial Automation GmbH
Richard-Reitzner-Allee 6
D-85540 Haar

erklären hiermit in alleiniger Verantwortung, dass das Produkt.
declare under our sole responsibility that the product.

Modell / Typ
Model / Type

smartLink HW-PN (GEA-YA-026010)

mit den Anforderungen der folgenden Richtlinien übereinstimmt
complies with the requirements of the following directives:

EMV Richtlinie 2014/30/EU
EMC Directive 2014/30/EU

ROHS-Richtlinie 2011/65/EU, ergänzt um Delegierte Richtlinie (EU) 2015/863
ROHS directive 2011/65/EU, amended by commission delegated directive (EU) 2015/863

Angewandte harmonisierte Normen
Applied harmonized standards:

EN 55011:2016 + A11:2020 group 1 class A
EN 55032:2015 + A11:2020 class A
EN 61000-6-2:2005 + AC:2005; EN IEC 61000-6-2 :2019
EN 61000-6-4:2007 + A1:2011; EN IEC 61000-6-4 :2019
EN 61326-1:2013; EN IEC 61326-1:2021
EN IEC 63000:2018

Haar, 04.06.2024
Ort, Datum
Place, Date

Geschäftsführer
Managing Director

Dokumentvorlage/Template: EU-Konformitätserklärung_V1.13.docx Version: 1.00
Datei: EU-Konformitätserklärung_smartLink-HW-PN.docx Datum: 10.05.24

9 Glossary

Abbreviations	Definition
CA	Certificate Authority
CSR	Certificate Signing Request
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung
DP	Decentralised Peripherals
ETH	Ethernet
Ex	Explosion protection
FDI	Field Device Integration
GND	Ground
HTTPS	Hypertext Transfer Protocol Secure
I/O	Input/Output
IP	Internet Protocol
MQTT	Message Queuing Telemetry Transport. A lightweight messaging protocol designed for devices that have limited bandwidth
MQTT broker	The broker is the central server that receives messages from publishers and forwards them to subscribers. It is the middleman that manages who gets what message.
MQTT server	Another expression for an MQTT broker running on a server machine
MQTT last will message	A LWL message is a predefined message registered by a client when connected to a broker. If the client disconnects unexpectedly, the broker automatically publishes that “last will” message on behalf of the client. It is often used to signal offline status or failure.
MQTT topic	A structured communication channel used for publishing and subscribing to messages.
NTP	Network Time Protocol
OPC UA	Open Platform Communications Unified Architecture
PA	Process Automation
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PN	PROFINET
pnGate	Softing PROFINET Gateway
RIO	Remote Input / Output
RPP	Reverse Polarity Protection
RTC	real-time clock
T	Temperature

10 Appendix

10.1 MQTT payload

This section describes the MQTT communication model used by the smartLink HW-PN and explains the concept of the MQTT objects, topics, payloads, and object relationships published to the MQTT broker. The smartLink HW-PN publishes information about monitored PROFINET networks, devices, interfaces, ports, diagnostics, and communication states using structured MQTT topics and JSON payloads.

Note
Throughout the sections below, any mention of OPC 30140 (for example "IPnEquipmentType OPC 30410") refers to the OPC UA for PROFINET Companion Specification.

MQTT Broker

When the smartLink HW-PN establishes a connection to the MQTT broker, all available objects are updated and published. This ensures that the broker always contains the latest state information for all monitored assets. Objects are only published after all required object data is available and complete. To indicate the connection status of the smartLink HW-PN, an MQTT Last Will Message (LWT) is configured in addition to the regular connect and disconnect messages. This mechanism allows subscribers to monitor the availability of the smartLink HW-PN. The Last Will Message is published to the topic `{server}/OnlineState` .

The message is retained by the MQTT broker so that newly connected subscribers immediately receive the current online status.

MQTT Attributes

All MQTT messages are published with the MQTT retain flag enabled. This ensures that the latest object state remains available on the broker even if no subscribers are currently connected. Object attributes are transferred as JSON payloads and contain the current state and properties of the represented object.

MQTT Topics

All MQTT messages are published to object-specific subtopics below the default smartLink HW-PN topic hierarchy.

The MQTT topic syntax is defined as `{server}/{path}`

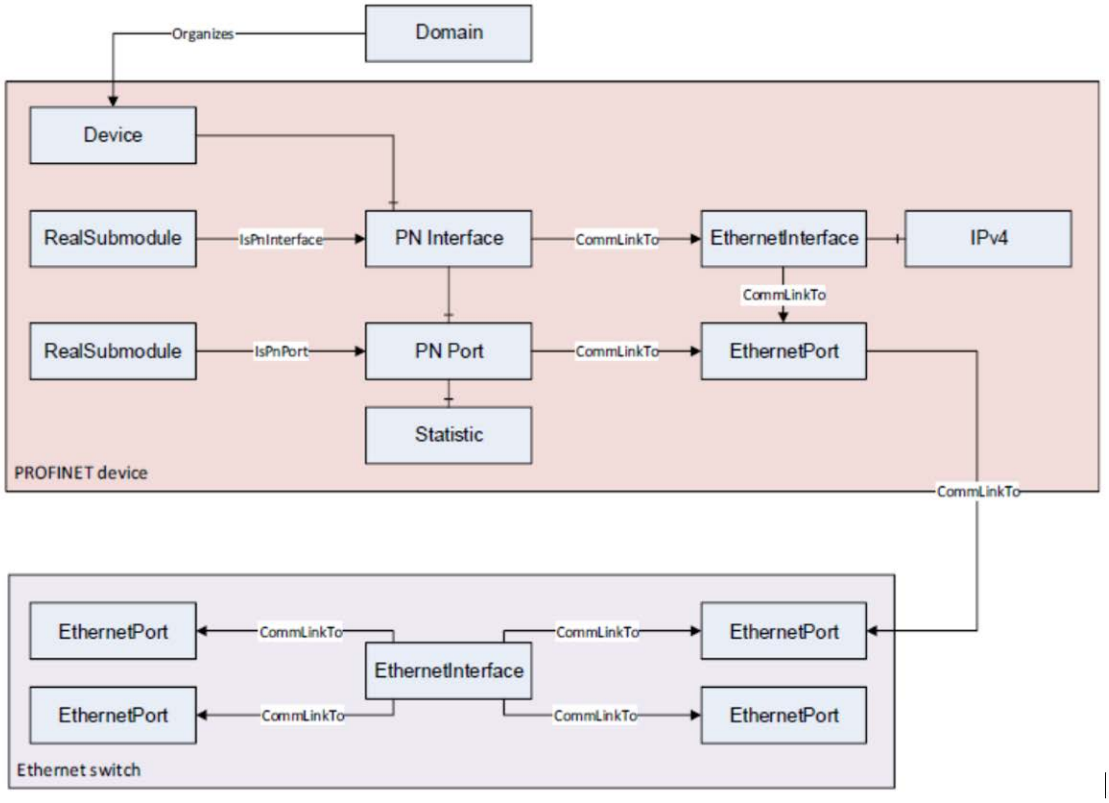
Where:
- `{server}` = smartLink server UID
- `{path}` = object-specific NodeId path

Examples:
- `04AF0CC1630F/NS/PN1`
- `04AF0CC1630F/DS/PN1/pndev`

10.1.1 Object model and relationships

The smartLink MQTT model consists of hierarchical objects representing PROFINET networks and their components. Objects reference related objects using MQTT payload references.

The following object types are supported:



10.1.2 Server object

The Server object represents a smartLink instance.

The object contains:

- The list of monitored networks
- General smartLink identification information

Field Name	Field Value
NodeId	{server} where: {server} is the smartLink's server UID
ObjectType	smartLink
BrowseName	{server UID}
Model	"smartLink HW-PN" or "smartLink SW-PN"
SoftwareRevision	version of the smartLink software
HardwareRevision	version of the smartLink hardware (optional)
SerialNumber	serial number of the smartLink hardware (optional)

Example


```
{
  "Server": "smartLink HW-PN 214000398",
  "NodeId": "04AF0CC1630F",
  "ObjectType": "smartLink",
  "BrowseName": "04AF0CC1630F",
  "Model": "smartLink HW-PN",
  "SoftwareRevision": "V1.04.00.34003",
  "HardwareRevision": "V2.00",
  "SerialNumber": "233800036",
  "Networks": {
    "References": [
      {
        "ReferenceType": "HasComponent",
        "Target": "04AF0CC1630F#NS|PN1"
      }
    ]
  },
  "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```

10.1.3 OnlineState object

The OnlineState object represents the connection state of the smartLink to the MQTT broker.

The following states are supported:

State	Description
ONLINE	smartLink is connected to the broker
OFFLINE	smartLink disconnected normally
CONNECTION_LOST	Unexpected connection loss

The smartLink publishes:

- ONLINE after successfully connecting
- OFFLINE before disconnecting
- CONNECTION_LOST via the MQTT Last Will Message

Field Name	Field Value
NodeId	server} where: {server} is the smartLink's server UID
ObjectType	OnlineState
BrowseName	OnlineState
OnlineState	OFFLINE, ONLINE, CONNECTION_LOST

Example

```
{
    "Server": "smartLink HW-PN 214000398",
    "NodeId": "04AF0CC1630F|OnlineState",
    "ObjectType": "OnlineState",
    "BrowseName": "OnlineState",
    "OnlineState": "ONLINE"
}
```

10.1.4 Network object

The Network object represents a monitored PROFINET network segment.

The object contains references to:

- Connected nodes
- Connected interfaces

Field Name	Field Value
NodeId	{server}#NS|{segment} where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1).
ObjectType	PnDomain
BrowseName	{segment}

Example


```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#NS|PN1",
 "ObjectType": "PnDomain",
 "BrowseName": "PN1",
 "Nodes":
 {
  "References":
  [
   {
    "ReferenceType": "HasComponent",
    "Target": "04AF0CC1630F#DS|PN1|pndev"
   }
  ]
 },
 "Interfaces":
 {
  "References":
  [
  {
   "ReferenceType": "ConnectsTo",
   "Target": "04AF0CC1630F#DS|PN1|pndev|IF1"
  }
 ]
},
 "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```


10.1.5 Node object

Node objects represent PROFINET assets within the monitored network.

Two node types are supported:

- PnDevice
- PnController

10.1.6 Device object

The Device object represents a monitored PROFINET device.

The object contains:

- device asset properties like vendor id or serial number.
- list of diagnosis entries which are active for the device (object references)
- list of interfaces of the object (object references)

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation} where: {server} is the smartLink's server UID and{segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network
ObjectType	PnDevice
BrowseName	{nameofstation}
Vendor	DCP device vendor code - IPnEquipmentType of OPC 30410
State	Device state - IPnDeviceType of OPC 30410
Manufacturer	Device manufacturer name
Model	Device model name
IM	PROFINET IM data - PnIdentificationType of OPC 30410

Example


```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#DS|PN1|pndev",
 "ObjectType": "PnDevice",
 "BrowseName": "pndev",
 "State": "ONLINE_2",
 "Vendor": "",
 "IM":
 {
   "VendorId": 0,
   "OrderId": "",
   "SerialNumber": "",
   "SoftwareRevision": "",
   "HardwareRevision": "",
   "ProfileId": 0,
   "ProfileSpecificType": 0,
   "Version": "",
   "RevisionCounter": 0,
   "IMSupported":
   {
    "IM1": true,
    "IM2": true,
    "IM3": true,
    "IM4": true,
    "IM5": true
   },
    "TagFunction": "",
    "TagLocation": "",
    "Date": "0000-01-01 00:00",
    "Descriptor": "",
```

```
    "Signature": "",
    "IM5":
         [
     {
      "Annotation": "",
      "VendorId": 0,
      "OrderId": "",
      "SerialNumber": "",
      "SoftwareRevision": "",
      "HardwareRevision": ""
     }
           ]
    },
    "Manufacturer": "",
    "Model": "",
    "Network":
    {
     "References":
     [
       {
        "ReferenceType": "ComponentOf",
        "Target": "04AF0CC1630F#NS|PN1"
       }
      ]
     },
     "Interfaces":
     {
     "References":
      [
       {
        "ReferenceType": "HasPnInterface",
         "Target": "04AF0CC1630F#DS|PN1|pndev|IF1"
       }
      ]
     },
     "Diagnosis":
     {
      "References":
      [
       {
        "ReferenceType": "HasComponent",
        "Target": "04AF0CC1630F#DS|PN1|pndev|DG"
       }
      ]
    },
    "TimeStamp": "2025-03-06T15:38:25.075Z"
  }
```

10.1.7 Controller object

The Controller object represents a monitored PROFINET controller.

The object contains:

- device asset properties like vendor id or serial number
- list of interfaces of the object (object references)

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation} where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network
ObjectType	PnController
BrowseName	{nameofstation}
Vendor	DCP device vendor code - IPnEquipmentType of OPC 30410
Manufacturer	Device manufacturer name
Model	Device model name
IM	PROFINET IM data - PnIdentificationType of OPC 30410

Example


```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#DS|PN1|pncon",
 "ObjectType": "PnController",
 "BrowseName": "pncon",
 "Vendor": "",
 "IM":
 {
  "VendorId": 0,
  "OrderId": "",
  "SerialNumber": "",
  "SoftwareRevision": "",
  "HardwareRevision": "",
  "ProfileId": 0,
  "ProfileSpecificType": 0,
  "Version": "",
  "RevisionCounter": 0,
  "IMSupported":
  {
   "IM1": true,
   "IM2": true,
   "IM3": true,
   "IM4": true,
   "IM5": true
  },
  "TagFunction": "",
  "TagLocation": "",
  "Date": "0000-01-01 00:00",
  "Descriptor": "",
  "Signature": "",
  "IM5":
          [
    {
```

```
            "Annotation": "",
            "VendorId": 0,
            "OrderId": "",
            "SerialNumber": "",
            "SoftwareRevision": "",
            "HardwareRevision": ""
          }
                ]
      },
      "Manufacturer":
      "Model":
      "Network":
      {
       "References":
      [
        {
           "ReferenceType": "ComponentOf",
           "Target": "04AF0CC1630F#NS|PN1"
        }
      ]
    },
    "Interfaces":
    {
      "References":
     [
      {
        "ReferenceType": "HasPnInterface",
        "Target": "04AF0CC1630F#DS|PN1|pncon|IF1"
      }
     ]
    },
     "TimeStamp": "2025-03-06T15:38:25.075Z"
   }
```

10.1.8 Interface object

The Interface object represents a PROFINET interface of a node.

The object contains:

- Interface properties (name of station or the device role)
- Port references (list of ports of the object)
- Ethernet interface references

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|IF{interfacenumber} where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network {interfacenumber} is the number of the interface starting with 1
ObjectType	PnInterface
BrowseName	{interfacenumber}
<interface properties>	IPnInterfaceType of OPC 30410

Example


```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#DS|PN1|pndev|IF1",
 "ObjectType": "PnInterface",
 "BrowseName": "1",
 "NameOfStation": "pndev",
 "DeviceRole": ["IO_DEVICE"],
 "DeviceVendor": "X",
 "VendorId": 0,
 "DeviceId": 0,
 "DeviceInstance": 0,
 "OEMVendorId": 0,
 "OEMDeviceId": 0,
 "Node":
 {
  "References":
  [
   {
     "ReferenceType": "ComponentOf",
     "Target": "04AF0CC1630F#DS|PN1|pndev"
   }
  ]
 },
 "Network":
 {
  "References":
  [
   {
     "ReferenceType": "ConnectsTo",
     "Target": "04AF0CC1630F#NS|PN1"
   }
  ]
},
"EthernetInterface":
{
```

```
    "References":
    [
     {
      "ReferenceType": "CommLinkTo",
      "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|EIF"
     }
    ]
  },
  "Ports":
  {
    "References":
   [
    {
     "ReferenceType": "HasPnPort"
     "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|P1"
    }
   ]
  },
  "TimeStamp": "2025-03-06T15:38:25.075Z"
 }
```

10.1.9 EthernetInterface object

The EthernetInterface object represents an Ethernet communication interface.

The object contains:

- MAC address information
- IPv4 configuration
- Ethernet port references

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|IF{interfacenumber} where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network {interfacenumber} is the number of the interface starting with 1
ObjectType	EnInterface
BrowseName	EIF
Enabled	Enabled flag - NetworkComponentType of OPC 30410
MacAddress	Ethernet MAC address - EthernetInterfaceType of OPC 30410
IPv4	IP V4 properties - IPv4FeatureType of OPC 30410

Example


```
{
  "Server": "smartLink HW-PN 214000398",
  "NodeId": "04AF0CC1630F#DS|PN1|pndev|IF1|EIF",
  "ObjectType": "EnInterface",
  "BrowseName": "EIF",
  "Enabled" : true,
  "MacAddress": "00:00:00:00:00:00",
  "IPv4" :
  {
    "IpAddress": "192.168.0.10",
    "SubnetMask": "255.255.255.0",
    "DefaultGateway": "192.168.0.1",
    "DhcpEnabled": false
  },
  "EthernetPorts" :
  {
   "References":
   [
    {
     "ReferenceType": "CommLinkTo",
     "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|P1|EP"
    }
   ]
 },
 "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```

10.1.10 Port object

The port object represents a PROFINET port of an interface of a node monitored by smartLink.

The object contains:

- port properties like link state and port state
- link to the Ethernet port object

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|IF{interfacenumber}|P{portnumber} where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network {interfacenumber} is the number of the interface starting with 1 {portnumber} is the number of the port starting with 1
ObjectType	PnPort
BrowseName	{portnumber}
<port properties>	see PnPortType of OPC 30410

Example


```
{
  "Server": "smartLink HW-PN 214000398",
  "NodeId": "04AF0CC1630F#DS|PN1|pndev|IF1|P1",
  "ObjectType": "PnPort",
  "BrowseName": "1",
  "LinkState": "UP_1",
  "PortState": "LISTENING_3",
  "MAUType": 0,
  "CableDelay": 0,
  "PowerBudget": 0,
  "IsWireless": false,
  "Statistic":
  {
   "References":
   [
    {
     "ReferenceType": "HasComponent",
     "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|P1|ST"
    }
   ]
  },
   "EthernetPort" :
   {
    "References":
    [
     {
      "ReferenceType": "CommLinkTo",
      "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|P1|EP"
     }
    ]
  },
   "TimeStamp": "2025-03-06T15:38:25.075Z"
 }
```

10.1.11 EthernetPort object

The EthernetPort object represents a physical Ethernet port.

The object contains:

- Ethernet port properties like the physical address
- Ethernet port object of another node (object reference) - This link represents the Ethernet cable

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|IF{interfacenumber}|P{portnumber}|EP where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network {interfacenumber} is the number of the interface starting with 1 {portnumber} is the number of the port starting with 11
ObjectType	EnPort
BrowseName	EP
<ethernet port properties>	see EthernetPortType

Example

```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#DS|PN1|pndev|IF1|P1|EP",
 "ObjectType": "EnPort",
 "BrowseName": "EP",
 "Enabled" : true,
 "PhysAddress": "00:00:00:00:00:00",
 "EthernetPort" :
 {
  "References":
  [
   {
    "ReferenceType": "CommLinkTo",
    "Target": "04AF0CC1630F#DS|PN1|pncon|IF1|P1|EP"
   }
  ]
 },
 "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```

10.1.12 PortStatistics object

The PortStatistics object contains Ethernet and PROFINET traffic statistics for a port.

The object includes:

- port statistics properties

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|IF{interfacenumber}|P{portnumber}|ST where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network {interfacenumber} is the number of the interface starting with 1 {portnumber} is the number of the port starting with 1
ObjectType	PnPortStatistics
BrowseName	ST
<port statistics properties>	see PnPortStatisticType

Example


```
{
  "Server": "smartLink HW-PN 214000398",
  "NodeId": "04AF0CC1630F#DS|PN1|pndev|IF1|P1|ST",
  "ObjectType": "PnPortStatistics",
  "BrowseName": "ST",
  "InOctets" : 0,
  "OutOctets" : 0,
  "InDiscards" : 0,
  "OutDiscards" : 0,
  "InErrors" : 0,
  "OutErrors" : 0,
  "Port":
  {
   "References":
   [
    {
     "ReferenceType": "ComponentOf",
     "Target": "04AF0CC1630F#DS|PN1|pndev|IF1|P1"
    }
   ]
  },
  "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```

10.1.13 Diagnosis object

The Diagnosis object contains active diagnostic entries for a monitored device.

The object includes:

- an array of diagnostics entries

Field Name	Field Value
NodeId	{server}#DS|{segment}|{nameofstation}|DG where: {server} is the smartLink's server UID and {segment} is the PROFINET segment short name (e.g. PN1) and {nameofstation} is the name of the device as configured in the PROFINET network
ObjectType	PnDiagnosis
BrowseName	DG
<diagnostics properties>	PnDeviceDiagnosisDataType of OPC 30410

Example


```
{
 "Server": "smartLink HW-PN 214000398",
 "NodeId": "04AF0CC1630F#DS|PN1|pndev|DG",
 "ObjectType": "PnDiagnosis",
 "BrowseName": "DG",
 "Diagnosis":
 [
  {
   "API" : 0,
   "Slot": 0,
   "Subslot" : 0,
   "ChannelNumber": 0,
   "Type":  "16BIT_5",
   "Accumulative" : "SINGLE_0",
   "Maintenance" : "MAINTENANCE_REQUIRED_512",
   "Specifier" : "APPEARS_2048",
   "Direction": "INPUT_CHANNEL_8192",
   "UserStructureIdentifier": 0,
   "ChannelErrorType" : 0,
   "ExtChannelErrorType" : 0,
   "ExtChannelAddValue" : 0,
   "QualifiedChannelQualifier": 0,
   "ManufacturerData" : "0001",
   "Message": "",
   "HelpText": "",
   "Severity": 1000
  }
 ],
 "TimeStamp": "2025-03-06T15:38:25.075Z"
}
```

Softing Industrial Automation GmbH

Richard-Reitzner-Allee 6
85540 Haar / Germany
https://industrial.softing.com

+ 49 89 45 656-340
info.automation@softing.com