ENGLISH

Anybus® Communicator™ - PROFINET to PROFINET

USER MANUAL

SCM-1202-235
Version 1.0
Publication date 2024-10-03

Important User Information

Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Copyright © 2024 HMS Networks

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface 1
1.1. About This Document 1
1.2. Document Conventions 1
1.3. Trademarks 2

2. Safety 3
2.1. Intended Use 3
2.2. General Safety 3

3. Cybersecurity 4
3.1. General Cybersecurity 4
3.2. Security Advisories 4
3.3. How to Report a Vulnerability 4
3.4. Product Cybersecurity Context 5
3.4.1. Security Defense in Depth Strategy 5
3.4.2. Purdue Model 6

4. Preparation 7
4.1. Support and Resources 7
4.2. Cabling 7
4.3. Mechanical Tools and Equipment 7
4.4. System Requirements 7
4.4.1. Supported Operating Systems 7
4.4.2. Supported Web Browsers 7
4.5. HMS Software Applications 8
4.6. Third-Party Software Applications 8
4.7. Software License Information 8

5. About Communicator Coupler 9
5.1. How the Communication Works 9
5.2. How the Data Exchange Works 10
5.3. Data Integrity 10

6. Installation 11
6.1. External Parts 11
6.2. DIN Rail Mounting 12
6.3. Connector Port Guide 13
6.4. Connect to Networks 14
6.5. Connect to Power 15
6.6. Security Switch 16
6.7. Lock the Cables 18
6.8. DIN Rail Demount 19

7. Communicator Configuration 21
7.1. Connect to Configure the Communicator 21
7.2. Access the Built-In Web Interface from HMS IPconfig 22
7.3. Access the Built-In Web Interface from a Web Browser 24
7.4. Communicator Built-In Web Interface Overview 25
7.5. Network Settings 26
7.5.1. Network Overview 26
7.5.2. IP Settings 27
7.6. Advanced Settings 29

7.6.1. Legacy Mode 29
7.7. I/O Configuration 29
7.7.1. Endian Swap 29
7.7.2. Convert Between Big-Endian and Little-Endian 30
7.7.3. Build Detailed Endian Swap 31
7.7.4. Process Data Settings 33
7.8. Configuration Notes 34
7.8.1. Add Configuration Note 34
7.8.2. View and Edit Configuration Notes 36
7.9. Apply Configuration 37
7.10. To Use an Existing Configuration 38

8. PLC Configuration 39
8.1. PLC Device Security 39
8.2. Export Product GSDML File 39

9. Verify Operation 40
9.1. Communicator Status Monitor 40
9.2. Communicator LED Indicators 42
9.3. Ethernet LED Indicators 43

10. Maintenance 44
10.1. Action on Fatal Error 44
10.2. Configuration Port IP Settings 45
10.3. Configuration File Handling 46
10.3.1. Export Configuration 46
10.3.2. Import Configuration 47
10.4. Clear and Revert Configuration 48
10.5. Firmware Management 49
10.5.1. View the Firmware Version 49
10.5.2. Firmware and Configuration Compatibility 49
10.5.3. Firmware File Validation 49
10.5.4. Update Firmware 50
10.6. Change Language 51

11. Troubleshooting 52
11.1. Diagnostics 52
11.1.1. I/O Data 52
11.1.2. Event Log 53
11.2. LED Status 54
11.3. Reset to Factory Settings 55
11.4. Firmware Upgrade Error Management 58
11.5. Support 60
11.5.1. Support Package 60

12. End Product Life Cycle 61
12.1. Secure Data Disposal 61

13. Technical Data 62
13.1. Technical Specification 62

1. Preface

1.1. About This Document

This document describes how to install and configure Anybus® Communicator™.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com.

1.2. Document Conventions

Lists

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information

User Interaction Elements

User interaction elements (buttons etc.) are indicated with bold text.

Program Code and Scripts

```
Program code and script examples
```

Cross-References and Links

Cross-reference within this document: Document Conventions (page 1)

External link (URL): www.hms-networks.com

Safety Symbols

DANGER
Instructions that must be followed to avoid an imminently hazardous situation which, if not avoided, will result in death or serious injury.

WARNING
Instructions that must be followed to avoid a potential hazardous situation that, if not avoided, could result in death or serious injury.

CAUTION
Instruction that must be followed to avoid a potential hazardous situation that, if not avoided, could result in minor or moderate injury.

IMPORTANT
Instruction that must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

Information Symbols

NOTE
Additional information which may facilitate installation and/or operation.

TIP
Helpful advice and suggestions.

1.3. Trademarks

Anybus® is a registered trademark of HMS Networks.

All other trademarks are the property of their respective holders.

2. Safety

2.1. Intended Use

The intended use of this equipment is as a communication interface and gateway.

The equipment receives and transmits data on various physical layers and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

2.2. General Safety

CAUTION
Ensure that the power supply is turned off before connecting it to the equipment.

CAUTION
This equipment contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.

CAUTION
To avoid system damage, the equipment should be connected to ground.

IMPORTANT
Using the wrong type of power supply can damage the equipment. Ensure that the power supply is connected properly and of the recommended type.

3. Cybersecurity

3.1. General Cybersecurity

IMPORTANT
It is important to maintain the cybersecurity of the Communicator.

Before connecting the Communicator to a PLC, ensure the PLC is configured and installed in accordance with the PLC supplier hardening guidelines.

IMPORTANT
To physically secure networks and equipment and to prevent unauthorized access, it is recommended to install the equipment in a locked environment.

IMPORTANT
After completing the configuration of the Communicator, lock the security switch to prevent unauthorized access to the Communicator built-in web interface.

IMPORTANT
To avoid exposure of sensitive data, always perform a factory reset before decommissioning the equipment.

Factory reset will reset any on site made configuration changes and set the Communicator to the same state as leaving HMS production.

See Reset to Factory Settings (page 55).

3.2. Security Advisories

For cybersecurity reasons, stay informed about new vulnerabilities and follow the recommended actions.

HMS Networks Security Advisories includes information about our product vulnerabilities and available solutions.

You find our Safety Advisories at www.hms-networks.com/cybersecurity/security-advisories.

3.3. How to Report a Vulnerability

HMS Networks place the utmost importance on the security of our products and systems, however, despite all the measures we take, it cannot be excluded that vulnerabilities persist.

To report a potential vulnerability in an HMS product or service, please visit www.hms-networks.com/cybersecurity/report-a-vulnerability and follow the instructions.

3.4. Product Cybersecurity Context

3.4.1. Security Defense in Depth Strategy

The defense in depth strategy of the Communicator includes the following security measures:

- Secure Boot: Security standard used to ensure that the Communicator boots using only software that is trusted by HMS Networks.
- Signed firmware: HMS Networks delivers digitally signed firmware. Before the firmware file is imported into the Communicator, the firmware upgrade function performs a validation of the file, to ensure that is authentic.
- Security switch: Used to lock unauthorized access to the Communicator built-in web interface.
- The Communicator is intended to be installed in a Process Control Network (PCN) environment. See Level 1 in the Purdue Model (page 6).
- To physically secure networks and equipment and to prevent unauthorized access, the Communicator is intended to be installed in a locked environment.

3.4.2. Purdue Model

The Communicator is intended to be part of the process control network in Level 1 (E), to enable communication between PLCs or between a PLC and peripheral devices.

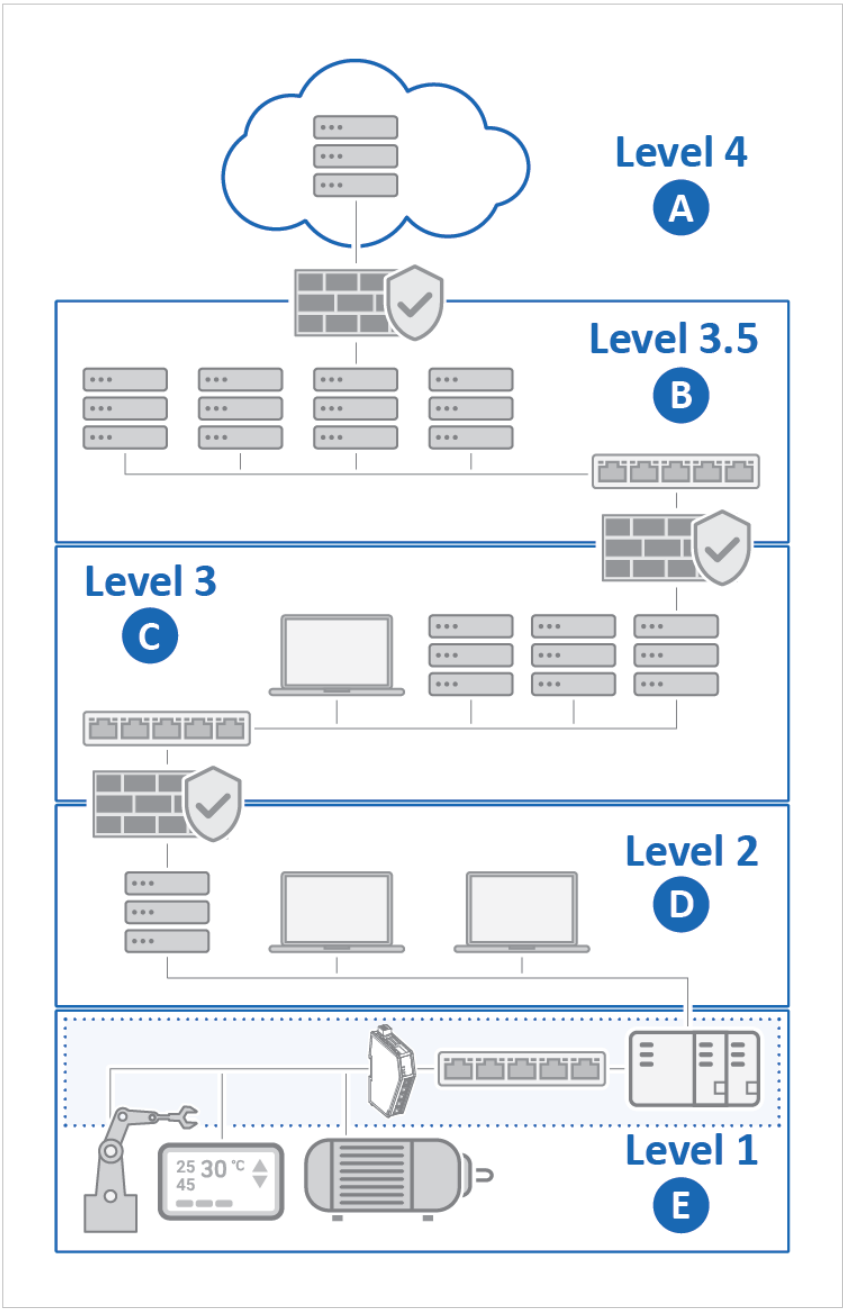


Figure 1. Purdue model, product security context

IT Network

A. **Level 4: Enterprise Network**
Example: Cloud solution, Business LAN (VPN)

B. **Level 3.5: Perimeter Network**
Example: Demilitarized Zone (DMZ)

OT Network

C. **Level 3: Advanced Control Network (ACN)**
Example: SCADA systems, Business control

D. **Level 2: Supervisory Control**
Example: Operator panels, Operator stations, Engineering stations

E. **Level 1: Process Control Network (PCN)**
Environment where the Communicator is installed
Example: Factory floor, Industrial product line

4. Preparation

4.1. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com.

TIP
Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.

4.2. Cabling

Have the following cables available:

- Ethernet cable for configuration.
- Ethernet cable x 2 for connecting to the networks.
- Power cable.

4.3. Mechanical Tools and Equipment

Have the following tools available:

- Flat-head screwdriver, size 5.5 mm
  Needed when removing the Communicator from DIN-rail.

4.4. System Requirements

4.4.1. Supported Operating Systems

Operating System	Description
Windows 7 SP1, 32-bit	Windows 7 32-bit with Service Pack 1
Windows 7 SP1, 64-bit	Windows 7 64-bit with Service Pack 1
Windows 10 64-bit	Windows 10 64-bit
Windows 11 64-bit	Windows 11 64-bit

4.4.2. Supported Web Browsers

The Communicator built-in web interface can be accessed from the following standard web browsers.

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

4.5. HMS Software Applications

Download the software installation files and user documentation from www.hms-networks.com.

HMS IPconfig

Use the software application HMS IPconfig and scan your network to discover and change the Communicator IP address and to access the Communicator built-in web interface.

NOTE
As an alternative, you can set a static IP address within the same IP address range as the Communicator IP address on the computer accessing the Communicator built-in web interface.

NOTE
HMS IPconfig is only available for Windows.

4.6. Third-Party Software Applications

Microsoft Excel

Microsoft Excel, or equivalent software application that supports the Office Open XML Workbook (xlsx) file format. Needed to open and read the **Event log** file.

4.7. Software License Information

For license agreements regarding the third-party software used in the Communicator, refer to the *LICENSE.txt* file(s) included in the Communicator firmware update package zip file.

To download the Communicator firmware update package zip file, please visit www.hms-networks.com.

TIP
Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.

5. About Communicator Coupler

5.1. How the Communication Works

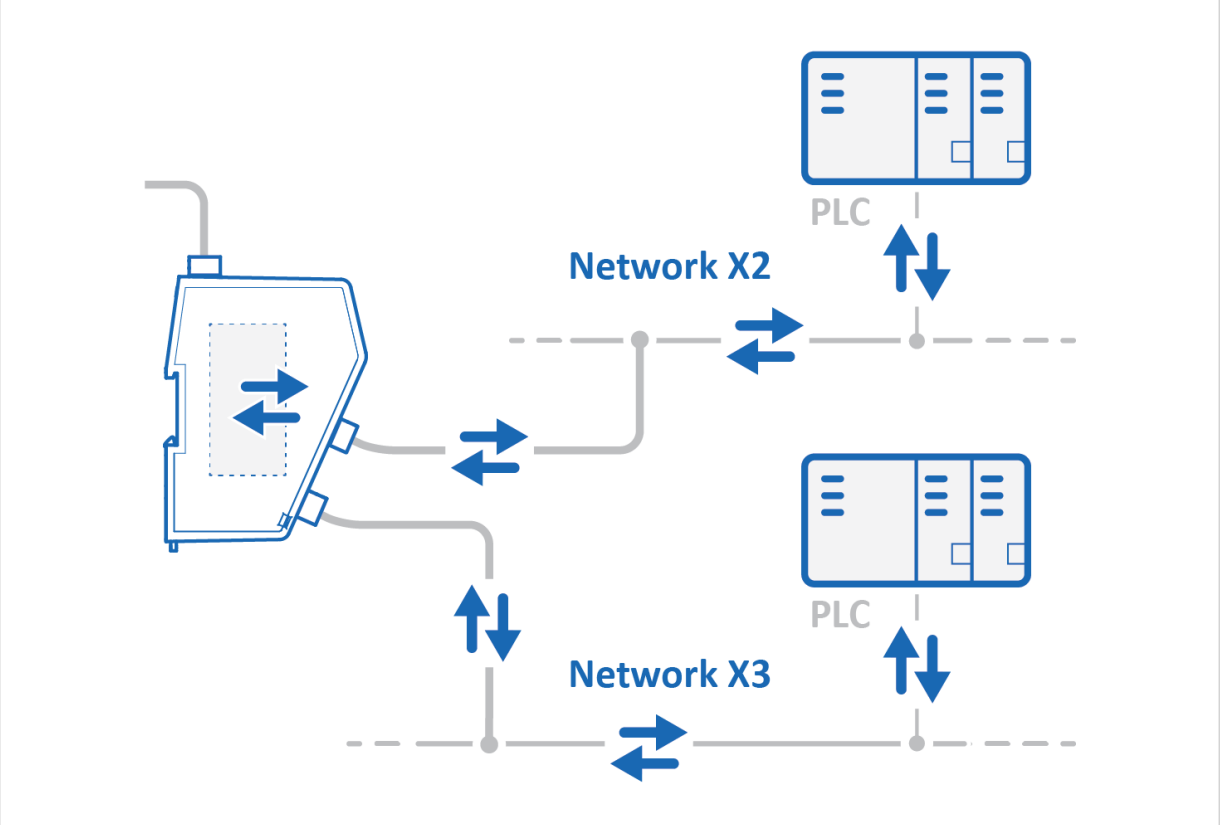


Figure 2. Process data traffic overview

The Communicator interconnects two network segments to facilitate data exchange.

The Communicator has two PROFINET interfaces, each connected to a separate network segment.

This enables communication between Master devices connected to separate PROFINET network segments.

The Master device can, for example, be a PLC control system or a Gateway.

The Communicator main task is to transfer cyclic I/O data between the two network segments.

5.2. How the Data Exchange Works

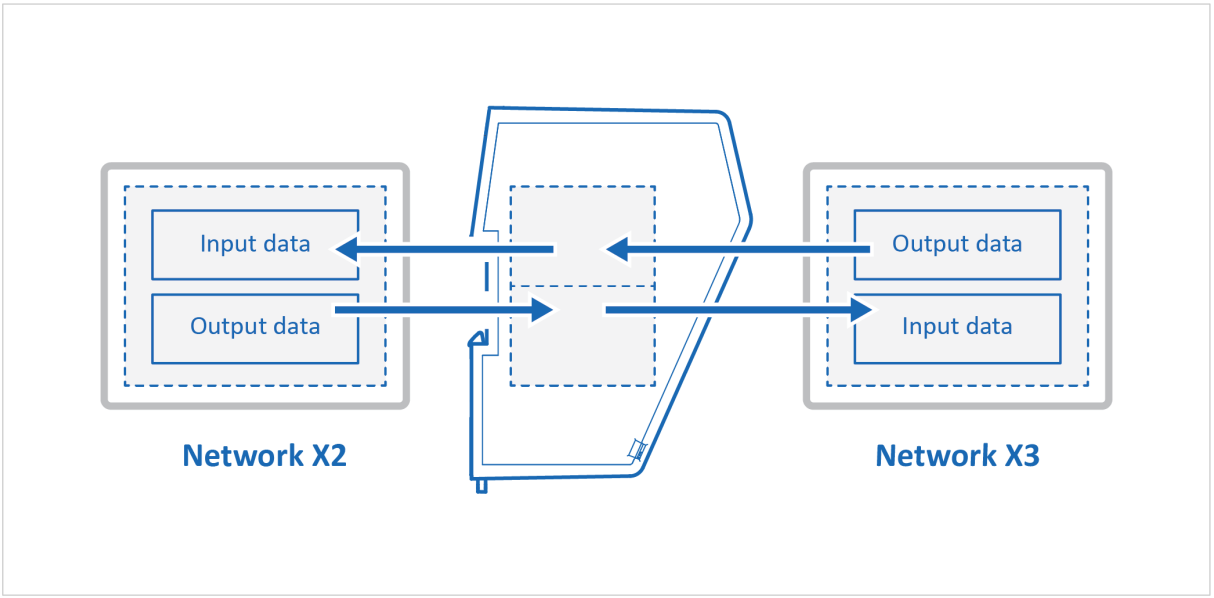


Figure 3. The Communicator internal memory areas

The data exchanged between the Communicator and the PROFINET networks, X2 and X3, resides in the Communicator internal memory buffer.

Input Data

This Input data area is read by the PROFINET.

Output Data

The Output data area is read/written by the PROFINET.

5.3. Data Integrity

A snapshot of the process data buffer between the PROFINET X2 network interface and the PROFINET X3 network interface is used during the operation of executing all the transactions within one cycle.

When the cycle is completed, the process data available on the network interfaces is updated and a new snapshot is created for the next cycle.

6. Installation

6.1. External Parts

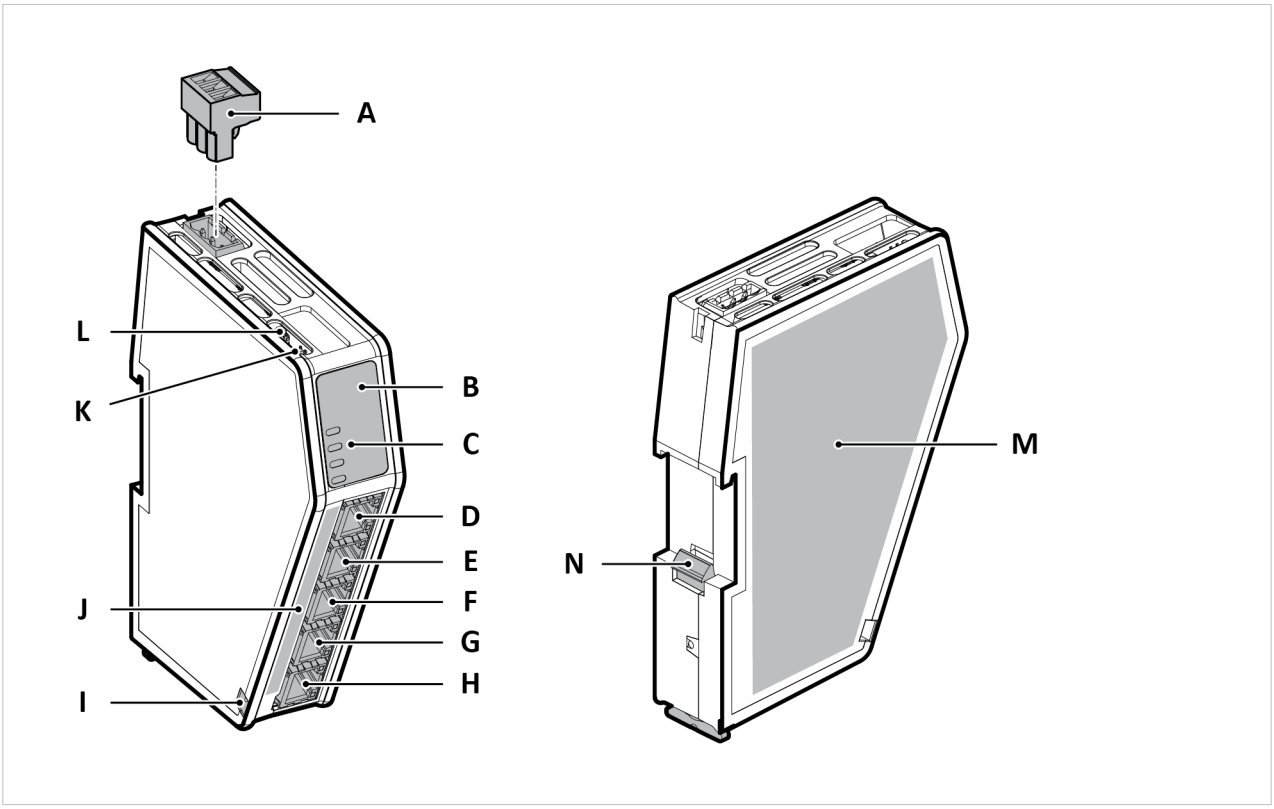


Figure 4. External parts

A. Power connector
B. Label with LED designation
C. Status LEDs
D. Configuration port
E. PROFINET port X2.1
F. PROFINET port X2.2
G. PROFINET port X3.1
H. PROFINET port X3.1
I. Cable tie mount
J. Laser engraved connectors designation
K. Security switch
L. Factory reset button
M. Laser engraved label with product information
N. DIN rail locking mechanism

6.2. DIN Rail Mounting

IMPORTANT
The equipment must be electrically grounded through the DIN rail for EMC compliance. Make sure that the equipment is correctly mounted on the rail and that the rail is properly grounded.

IMPORTANT
To physically secure networks and equipment and to prevent unauthorized access, it is recommended to install the equipment in a locked environment.

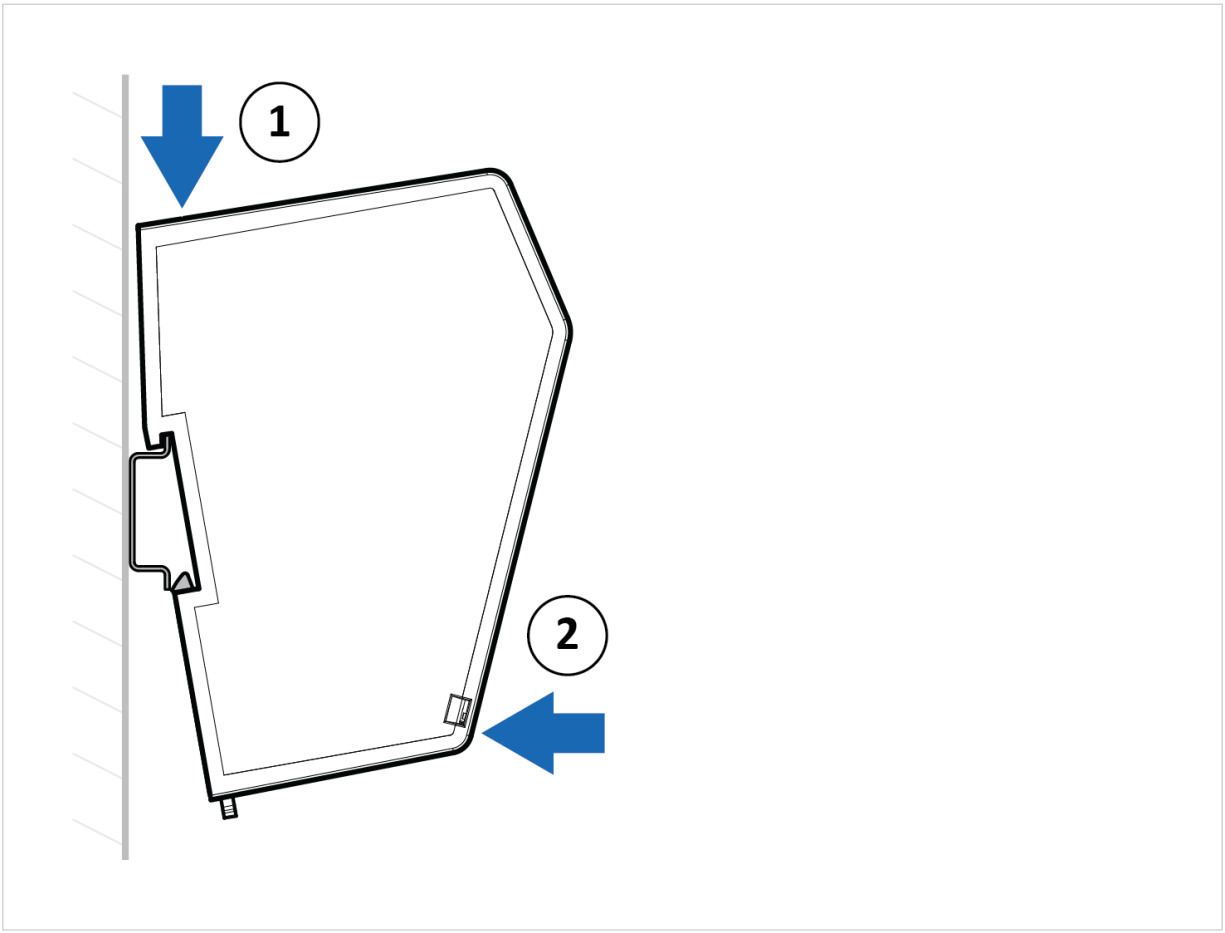


Figure 5. Attach the Communicator on the DIN rail

To attach the Communicator on the DIN rail:

1. Insert the upper end of the DIN rail clip into the DIN rail.
2. Push the bottom of the DIN rail clip into the DIN rail.

6.3. Connector Port Guide

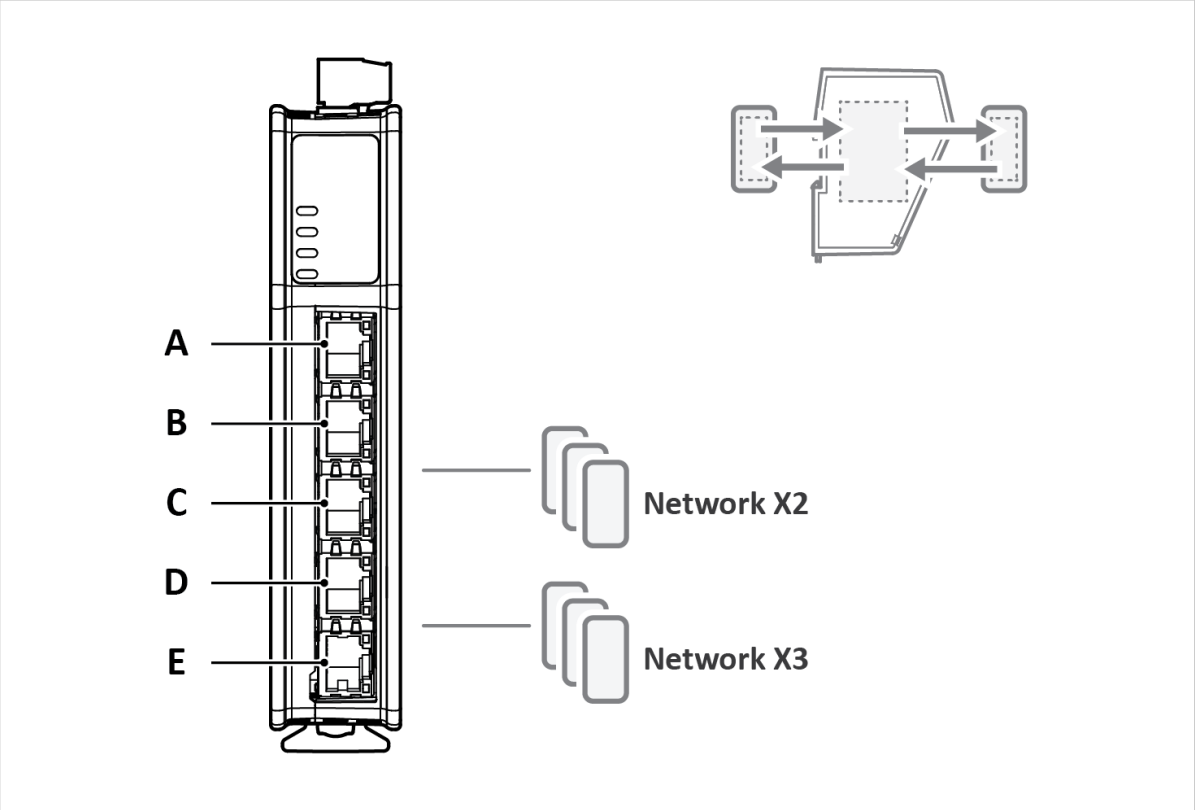


Figure 6. Communicator connector ports

Position	Network Number	Port Number	Connector Type	Port Usage
A	N/A	X1	Ethernet	Configuration port
B	Network X2	X2.1	Ethernet	PROFINET network
C	Network X2	X2.2	Ethernet	PROFINET network
D	Network X3	X3.1	Ethernet	PROFINET network
E	Network X3	X3.2	Ethernet	PROFINET network

6.4. Connect to Networks

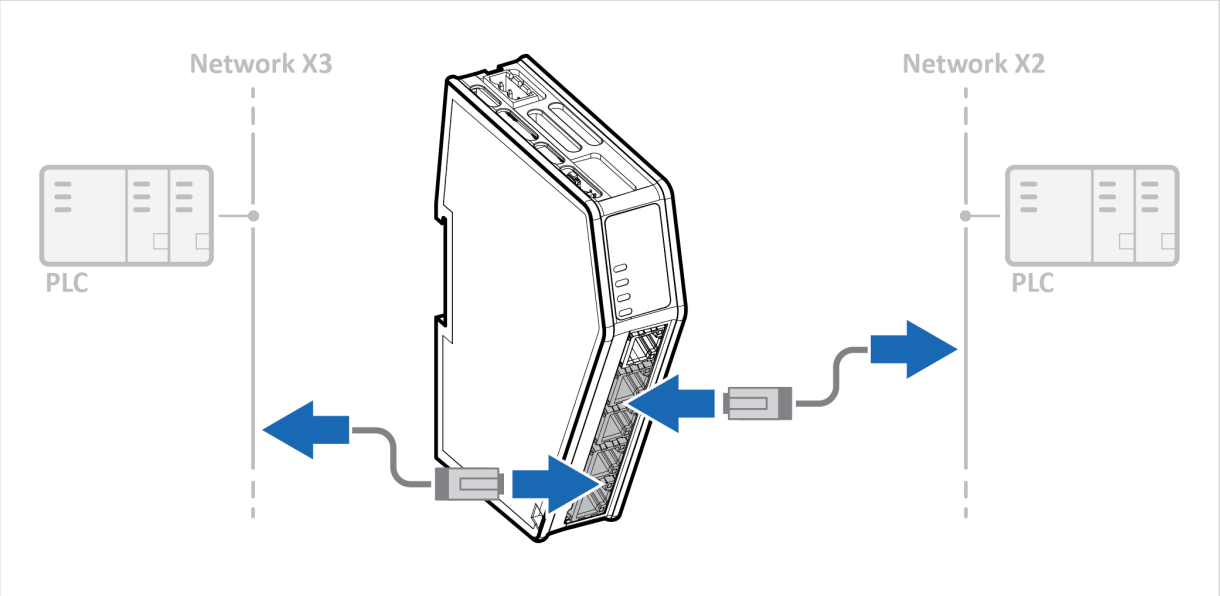
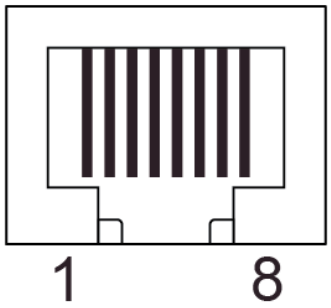


Figure 7. Connect to networks

Connect the Communicator to your PROFINET and PROFINET networks.

Ethernet RJ45 Connector Pinout

Ethernet RJ45 Connector	Pin	Description
	1	TD+
	2	TD-
	3	RD+
	4	Not used
	5	Not used
	6	RD-
	7	Not used
	8	Not used

6.5. Connect to Power

CAUTION
Ensure that the power supply is turned off before connecting it to the equipment.

IMPORTANT
Using the wrong type of power supply can damage the equipment. Ensure that the power supply is connected properly and of the recommended type.

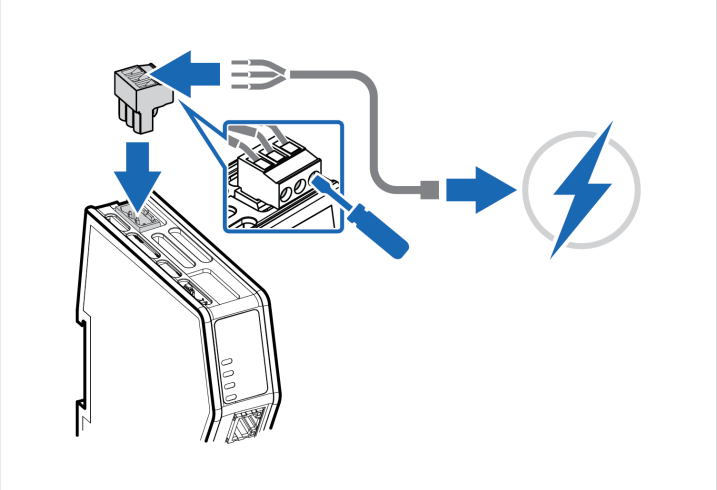
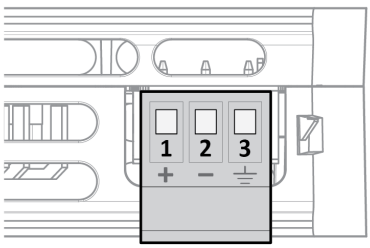


Figure 8. Connect to power

Power Connector Pinout

Power port	Pin	Description
	1	12-30 VDC Power Connector
	2	Ground (GND)
	3	Functional Earth (FE)

Procedure

1. Insert the cable wires to the terminal block and tighten the wire clamp screws.
2. Connect the terminal block to the Communicator.
3. Connect the Communicator to a power supply.
4. Turn on the power supply.

6.6. Security Switch

IMPORTANT
After completing the configuration of the Communicator, lock the security switch to prevent unauthorized access to the Communicator built-in web interface.

When the security switch is in its locked position, the Communicator built-in web interface cannot be accessed, and the Communicator cannot be configured using the built-in web interface. Network specific parameters, configured via the PLC is still available.

To Lock and Unlock the Security Switch

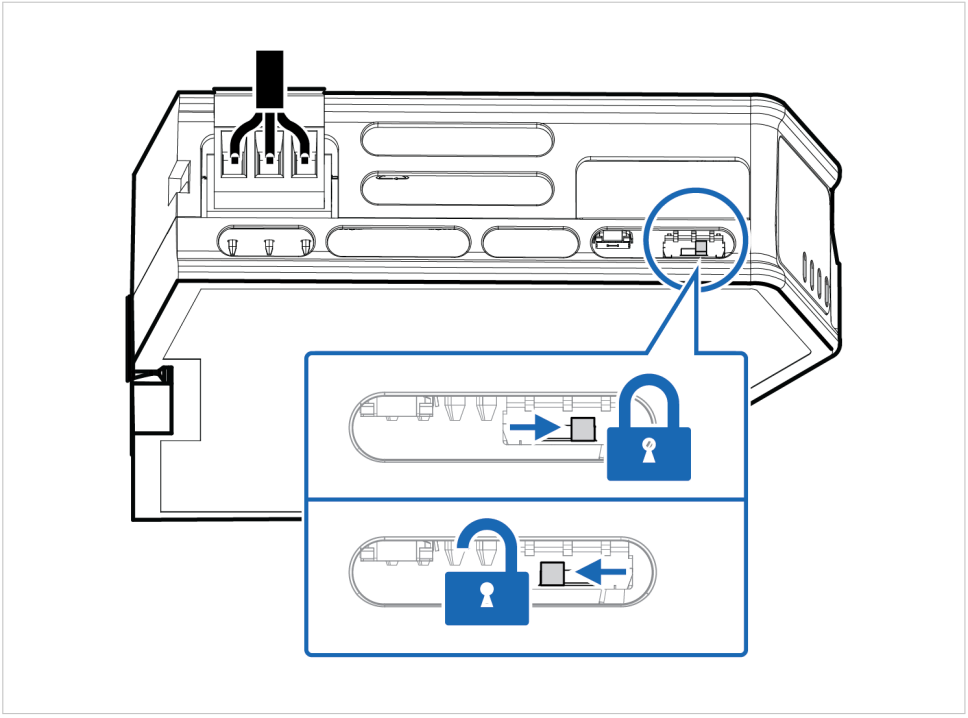


Figure 9. Security switch in locked and unlocked position

Use a pointed object, such as a ballpoint pen.

- To **lock** the security switch, push the toggle towards the **Communicator front**.
- To **unlock** the security switch, push the toggle towards the **Communicator back**.

Security Switch Status LED

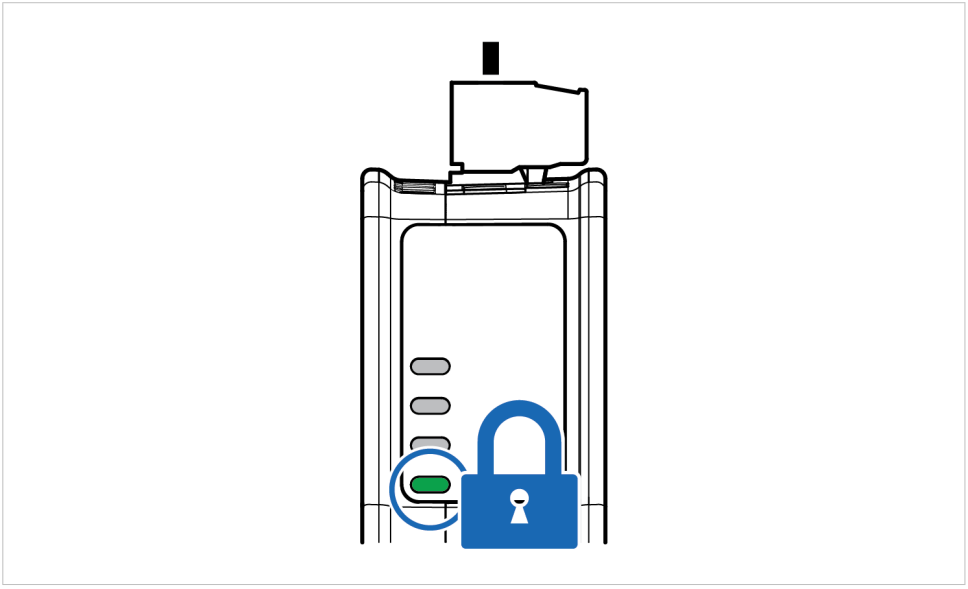


Figure 10. Security switch locked status LED

When the security switch is in its:

- locked position, the security switch status LED turn solid green.
- unlocked position, the security switch status LED is turned off.

6.7. Lock the Cables

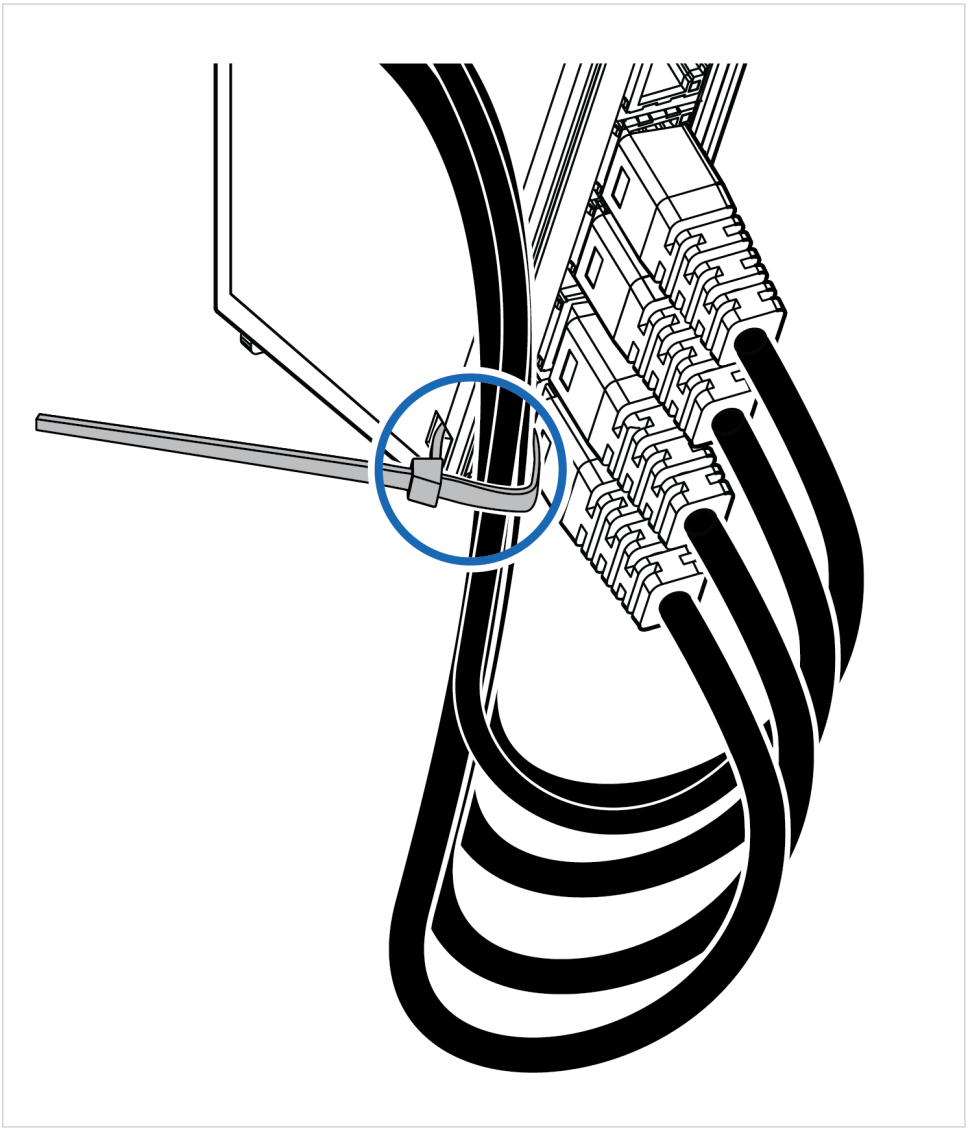


Figure 11. Lock the cables

To strain relieve the cables, place a cable tie in the holder and lock the cables.

6.8. DIN Rail Demount

Before You Begin

IMPORTANT
Be careful when removing the Communicator from the DIN-rail. If not removed properly, the DIN rail locking mechanism and the product cover can break.

Have a flat-blade screwdriver, size 5.5 mm, available.

Procedure

Remove the Communicator from the DIN rail:

1. Insert the screwdriver into the Communicator DIN rail locking mechanism.
2. To unlock the Communicator DIN rail locking mechanism, turn the screwdriver clockwise.

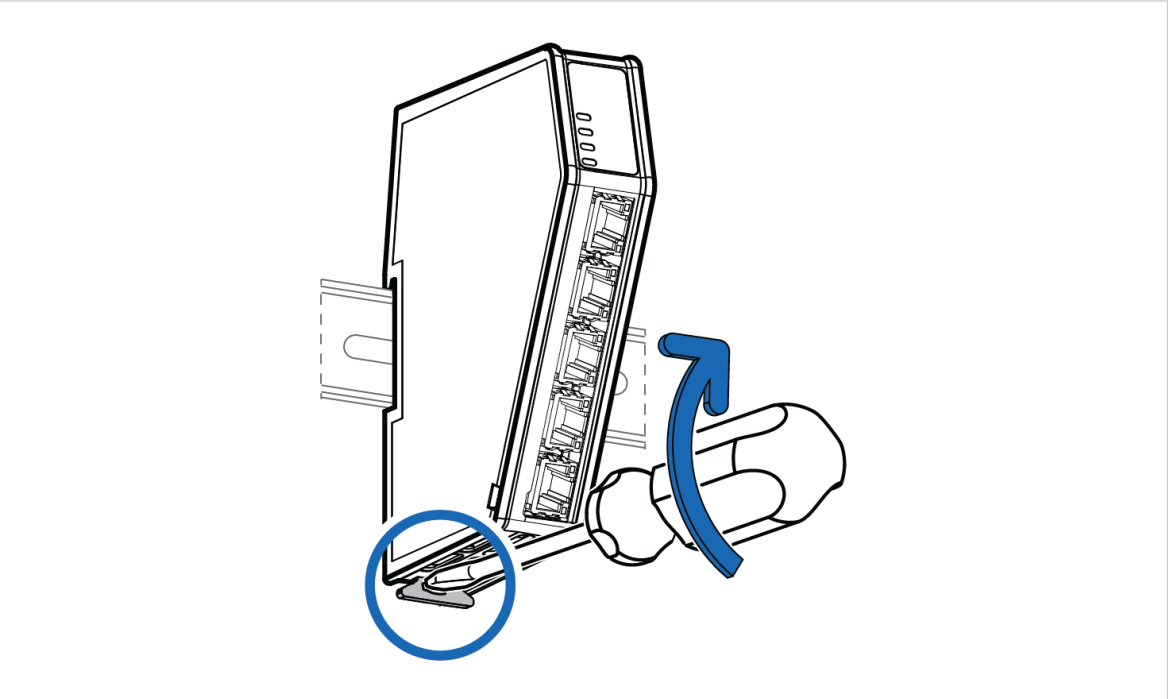


Figure 12. Unlock the Communicator

3. Hold the screwdriver in the DIN rail locking mechanism while you unhook the Communicator from the DIN rail.

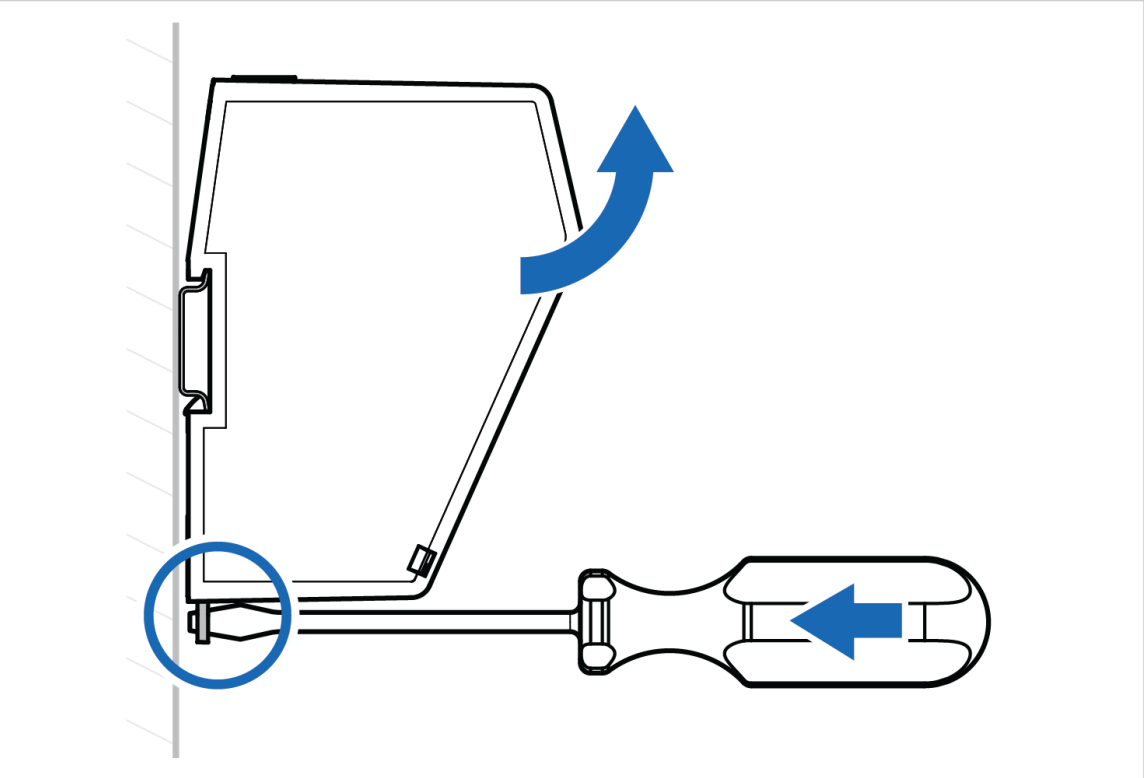


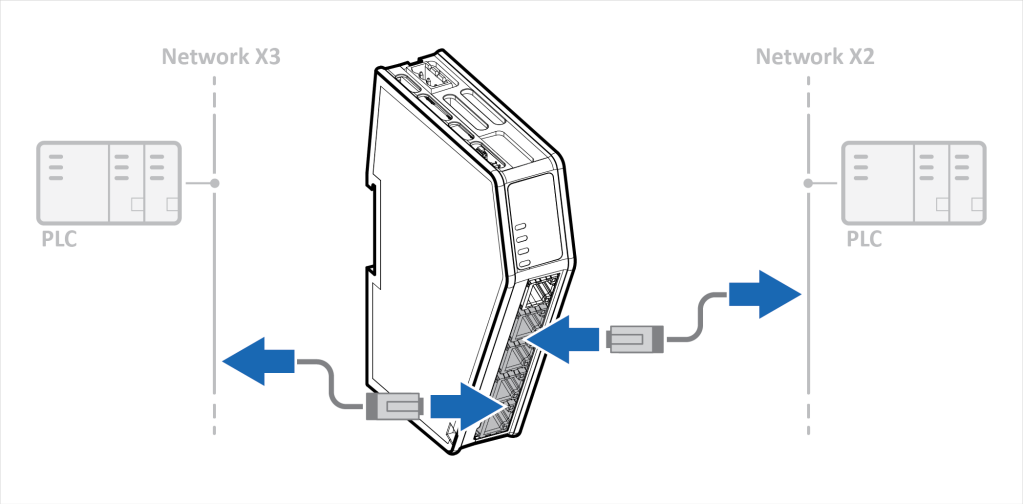
Figure 13. Unhook the Communicator

7. Communicator Configuration

7.1. Connect to Configure the Communicator

Procedure

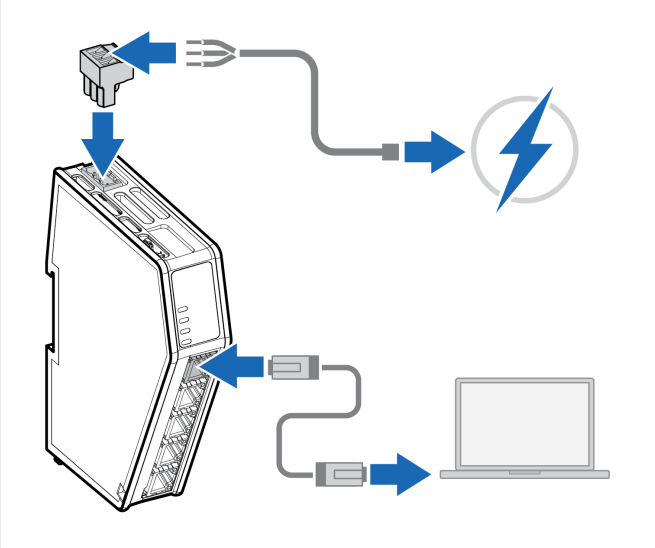
Connect to PROFINET network and PROFINET network



Network X2 = PROFINET Network X3= PROFINET

1. Connect the Communicator, upper connector, to the PROFINET X2 network.
2. Connect the Communicator, lower connector, to the PROFINET X3 network.

Connect to PC and Power



1. Connect an Ethernet cable between the Communicator and your PC.
2. Connect the Communicator to a power supply.

7.2. Access the Built-In Web Interface from HMS IPconfig

Before You Begin

Download the software application HMS IPconfig installation files and user documentation from www.hms-networks.com.

NOTE
The Communicator default IP address is 192.168.0.10.

NOTE
To access the Communicator built-in web interface, ensure that Port 80 TCP is open in your Firewall. This applies to any Firewall between the web browser and the gateway.

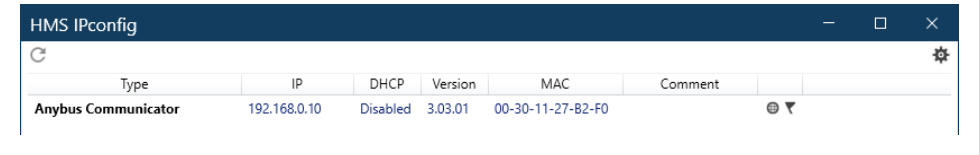
NOTE
To access the Communicator built-in web interface from HMS IPconfig, ensure that Port 3250 UDP is open in your PC Windows Firewall.

NOTE
Ensure that the security switch is unlocked. HMS IPconfig cannot configure the Communicator if the security switch is locked.

TIP
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System** > **Configuration port** page.

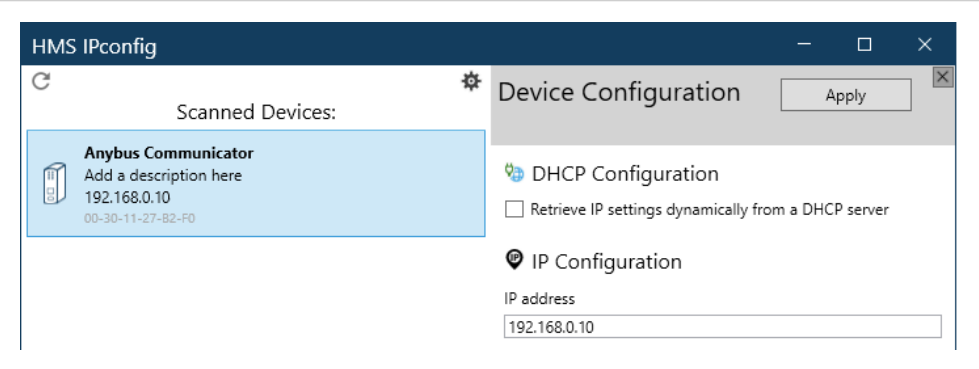
Procedure

1. Install HMS IPconfig on your PC.
2. Open HMS IPconfig.

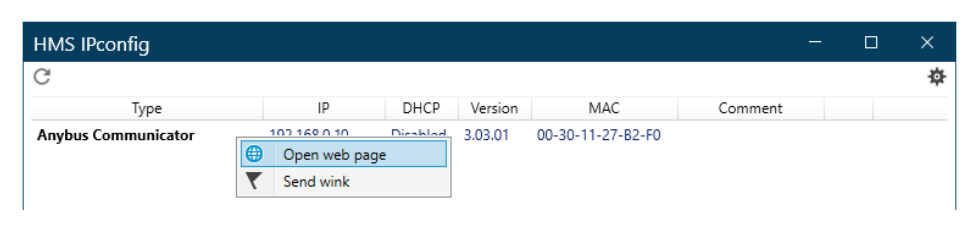


   - HMS IPconfig automatically starts scanning for compatible and active HMS devices.
   - Found HMS devices are added to the device list.
3. To open the settings pane, click on the Communicator in the device list.

4. Change the Communicator configuration port IP address to one within the same IP address range as your PC.

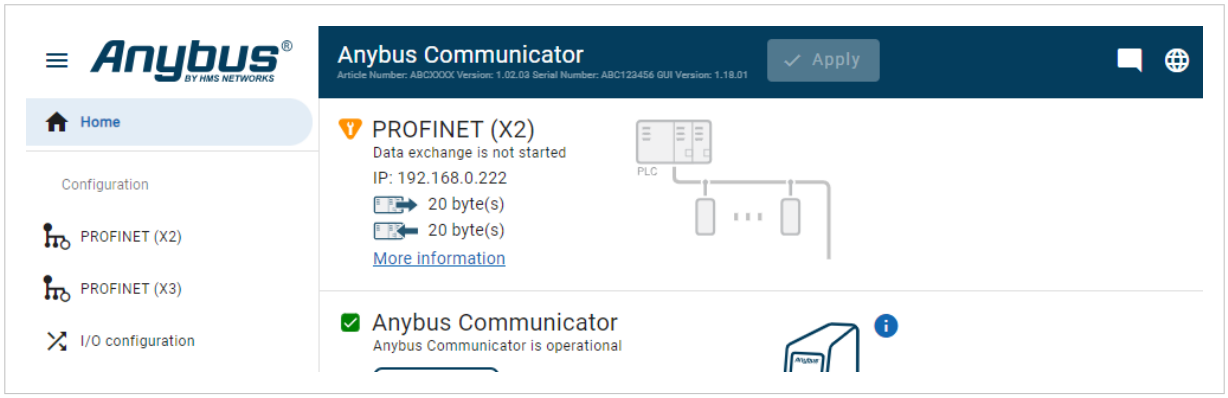


5. To open the **Open web page** built-in web interface, click Communicator.



Result

You are redirected to the Communicator built-in web interface **Home** page.



7.3. Access the Built-In Web Interface from a Web Browser

Before You Begin

NOTE
The Communicator configuration port default IP address is 192.168.0.10.

NOTE
To access the Communicator built-in web interface, ensure that Port 80 TCP is open in your Firewall. This applies to any Firewall between the web browser and the gateway.

NOTE
When you change to a static IP address on your computer, internet access may be lost.

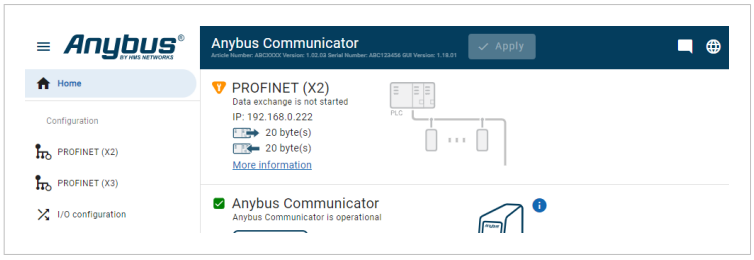
TIP
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System** > **Configuration port** page.

Procedure

1. On the PC accessing the Communicator built-in web interface, set a static IP address within the same IP address range as the Communicator IP address.

2. Open a web browser.
3. Click to select the **Address bar** and enter the Communicator IP address.

4. To open the built-in web interface **Home** page, press **Enter**.



7.4. Communicator Built-In Web Interface Overview

Use the Communicator built-in web interface to configure, maintain and troubleshoot the Communicator.

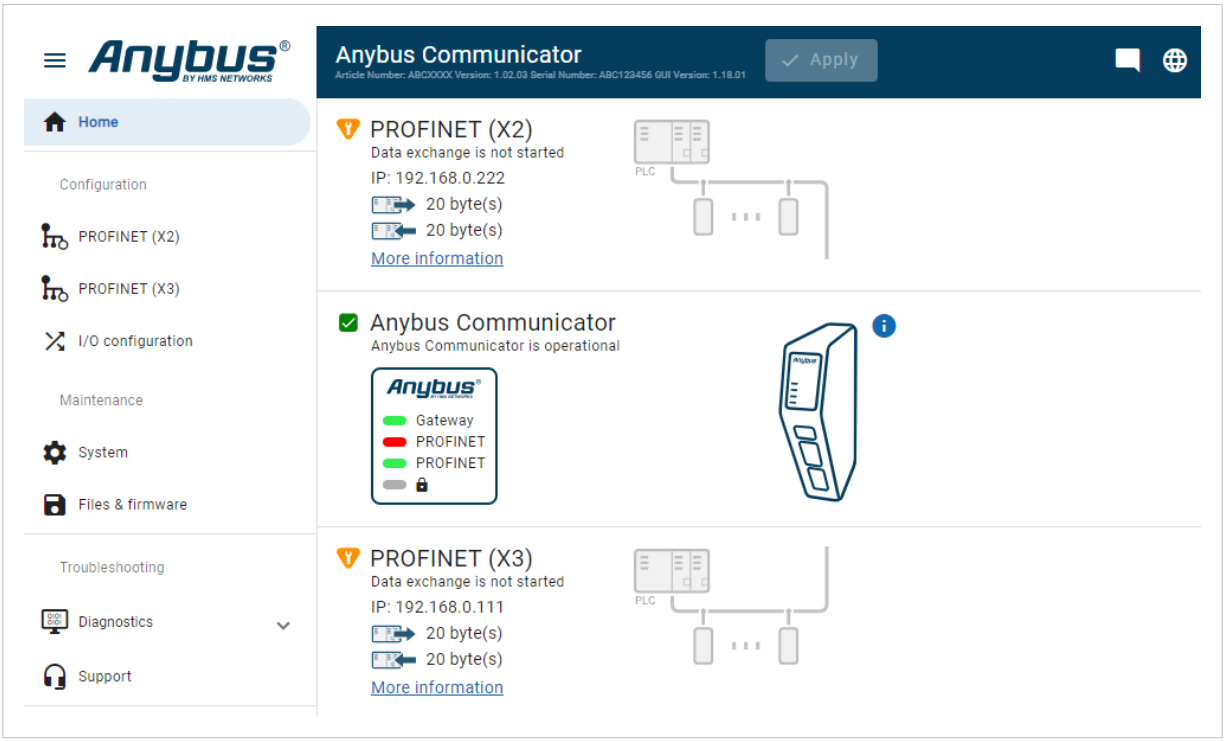


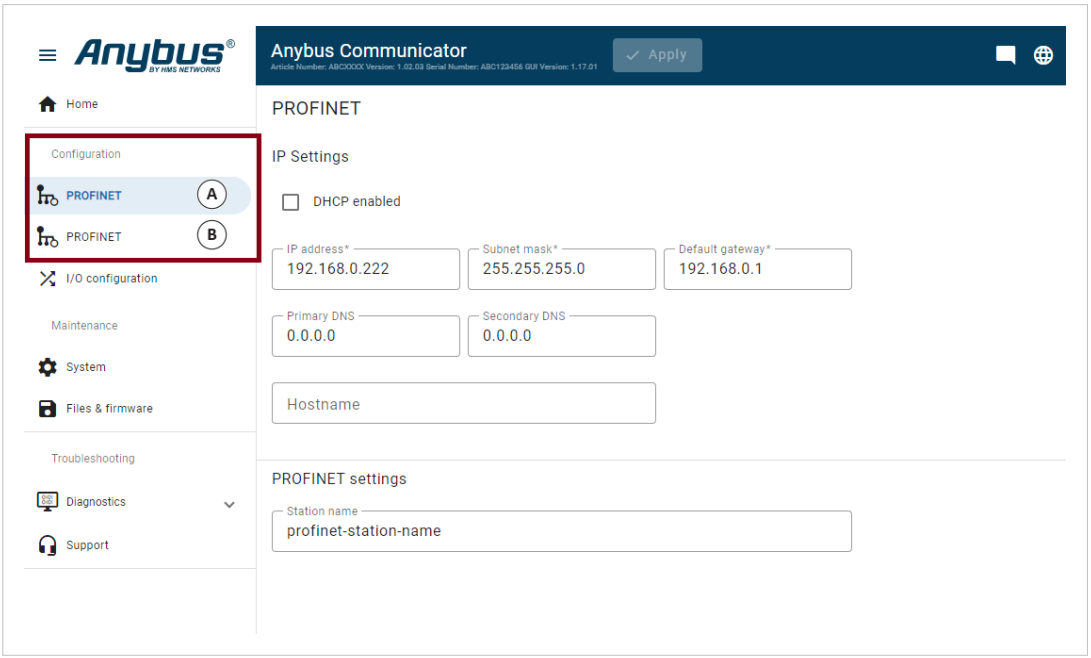
Figure 14. The Communicator built-in web interface Home page

Menu item	Description
Home	View the Communicator, network and node status.
Apply	After configuration changes are made and verified, press Apply to make the settings take effect.
PROFINET (X2)	Configure the network settings for the PROFINET (X2) network.
PROFINET (X3)	Configure the network settings for the PROFINET (X3) network.
I/O configuration	Configure input and output data sizes and endian conversion. Configure status byte and clear data settings.
System	Define how the device should behave if a serious error occurs. Configure the Communicator configuration port IP settings.
Files & firmware	Save settings in a configuration files, upload configuration files and upgrade firmware.
Diagnostics	Monitor and troubleshoot the Communicator.
Support	Contains Communicator product information, Anybus contact information, link to Anybus support website, and product file for download. Here you can generate a support package with product information, to send to your Anybus support technician.

7.5. Network Settings

7.5.1. Network Overview

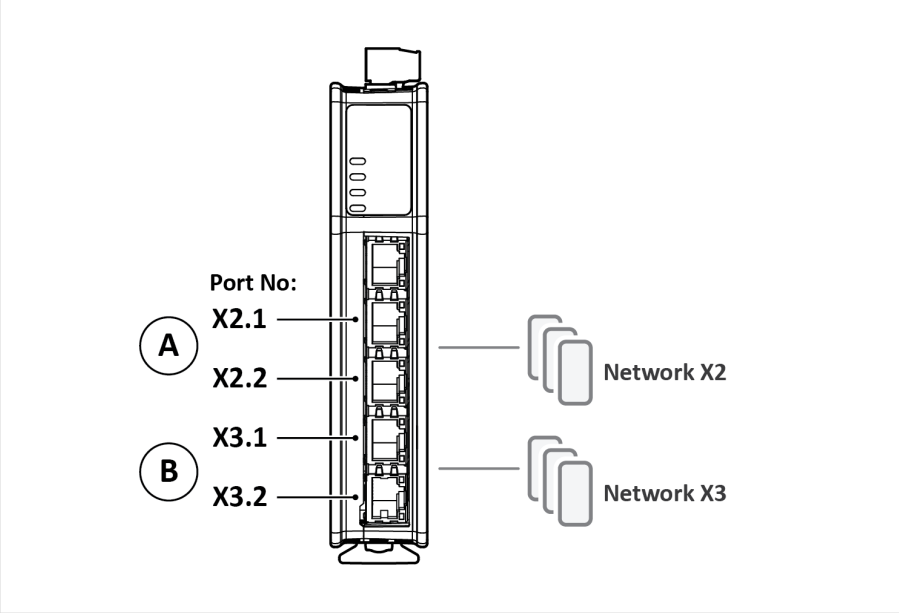
Configure the network settings for each network connected to the Communicator.



A. **PROFINET (X2)** page

B. **PROFINET (X3)** page

Figure 15. Communicator built-in web interface network settings



A. The upper PROFINET ports X2.1 and X2.2 corresponds to the **PROFINET (X2)** web page.

B. The lower PROFINET ports X3.1 and X3.2 corresponds to the **PROFINET (X3)** web page.

Figure 16. Communicator ports

7.5.2. IP Settings

To Configure IP Settings Manually

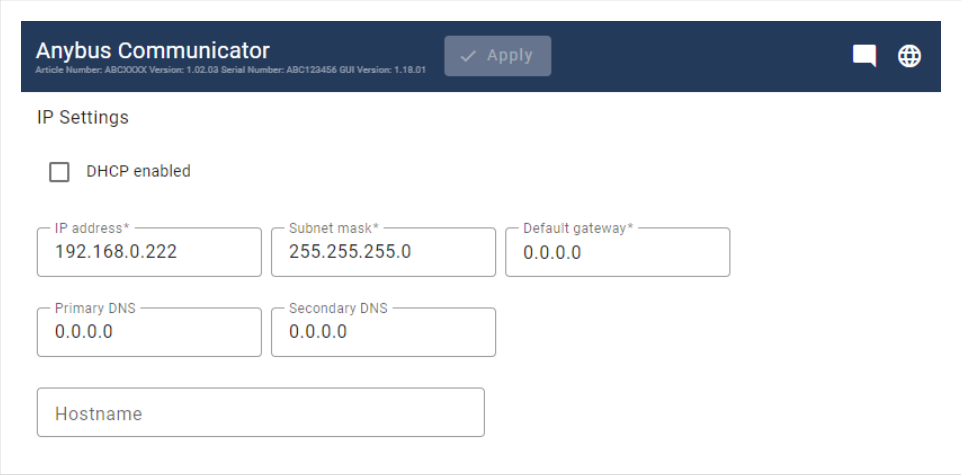


Figure 17. IP Settings, DCHP disabled

1. Ensure that the **DHCP enabled** checkbox is deselected.

2. Configure the IP settings.

Setting	Description
IP address	The PROFINET network IP address in IPv4 dot-decimal notation
Subnet mask	The PROFINET network Subnet mask in IPv4 dot-decimal notation.
Gateway address	The PROFINET network Gateway address in IPv4 dot-decimal notation. If there is no gateway available, set the Gateway address to: 0.0.0.0
Primary DNS	The PROFINET network Primary DNS in IPv4 dot-decimal notation.
Secondary DNS	The PROFINET network Secondary DNS in IPv4 dot-decimal notation.
Hostname	You can label the Communicator. Maximum length is 64 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Hostname as one single word.
Station name	To identify the Communicator in the PROFINETnetwork, enter a Station name. Maximum length is 240 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Station name as one single word.

Naming the Host

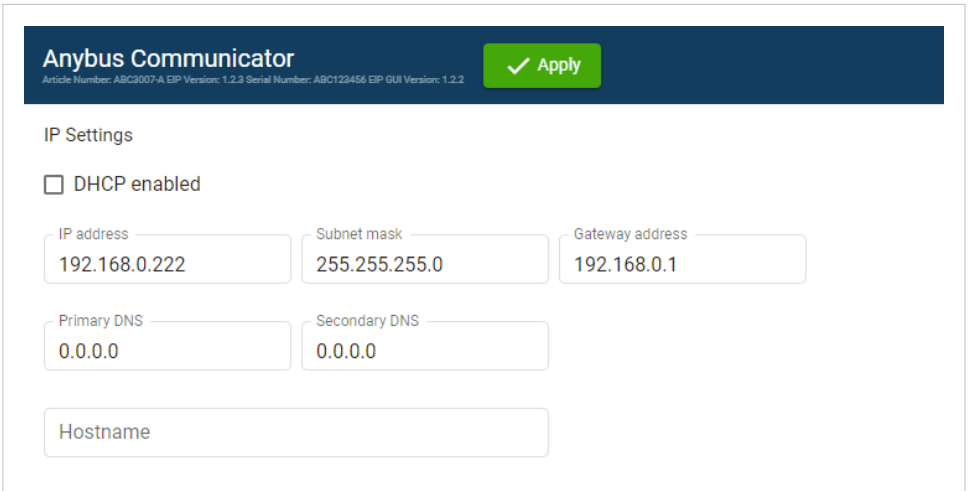


Figure 18. IP Settings Hostname

You can label the Communicator.

- The maximum allowed length of the Hostname is 64 characters.
- No symbol characters, punctuation characters, or whitespace are permitted.
- Write the Hostname as one single word.

7.6. Advanced Settings

7.6.1. Legacy Mode

Advanced settings option for PROFINET.

Before You Begin

If you already have an Anybus X-gateway GSDML (Generic Station Description Markup Language) file installed in your PLC, legacy mode allows you to continue using the settings from the GSDML file for the new Communicator.

IMPORTANT

Legacy mode does not support acyclic communication.

Compatible Product Variants GSDML Files

The GSDML file for the following Anybus X-gateway variants are compatible with the new Communicator:

AB7651-F - Anybus X-gateway – PROFINET-IO Device – PROFINET-IO Device

Procedure

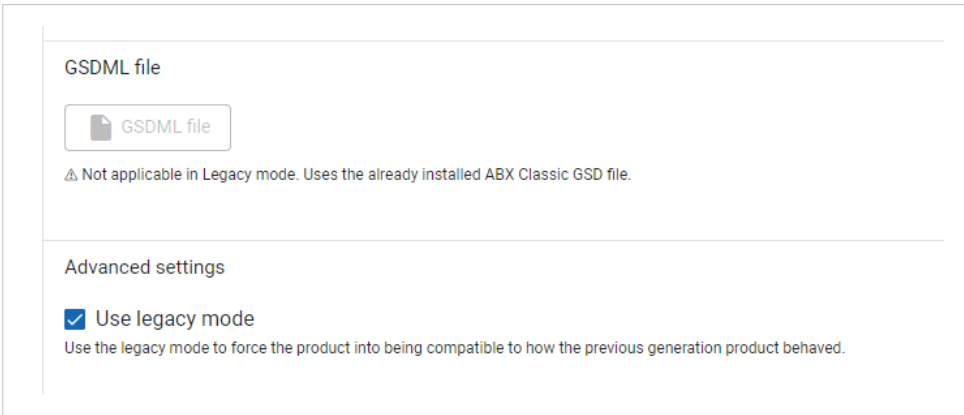


Figure 19. Advanced settings > Use legacy mode

To enable the legacy mode, select the **Use legacy mode** checkbox.

When Use legacy mode is enabled, the **GSDML file** download becomes inactive.

7.7. I/O Configuration

7.7.1. Endian Swap

By default, Communicator uses **No swapping**.

About Endianness

Big-endian (BE)

The big-endian format places the most significant byte of the data at the byte with the lowest memory address.

Little-endian (LE)

The little-endian format places the least significant byte of the data at the byte with the lowest memory address.

7.7.2. Convert Between Big-Endian and Little-Endian

To convert between big-endian and little-endian you must reverse the byte order.

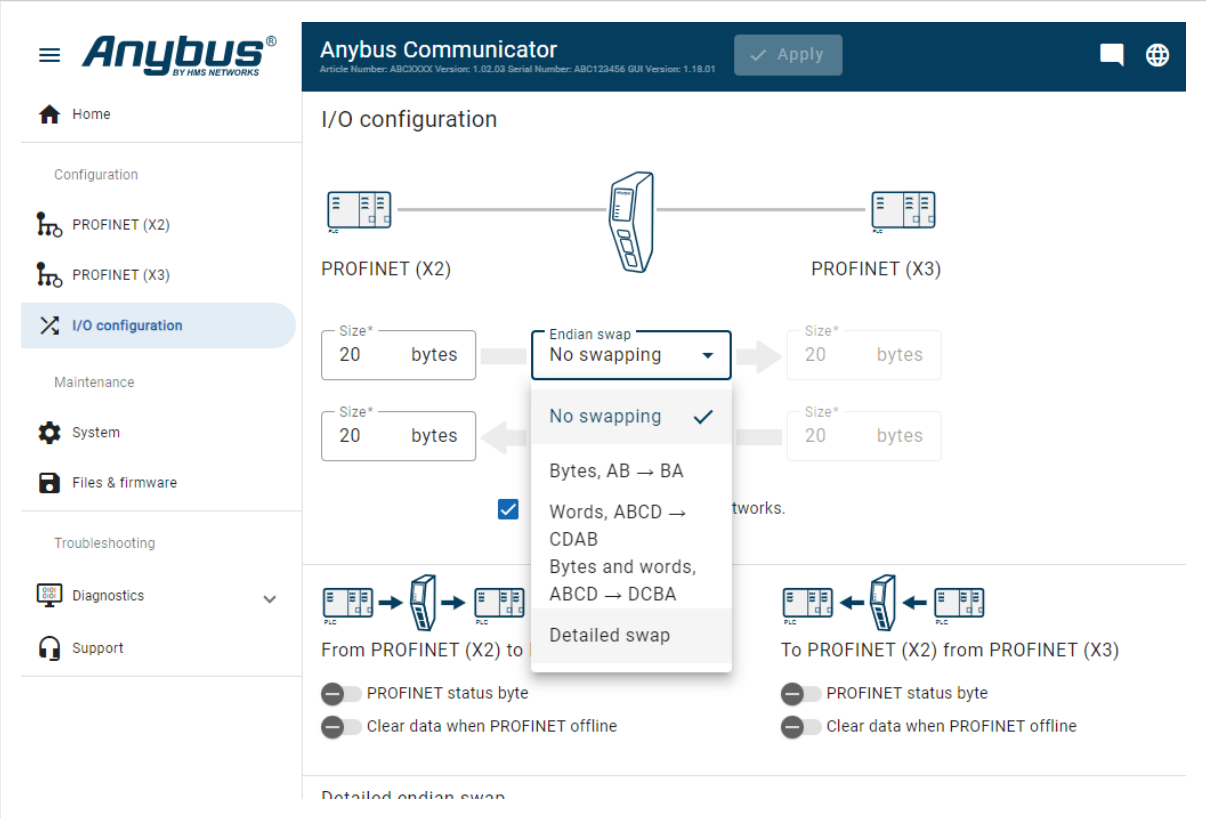


Figure 20. **I/O configuration** page, Endian swap

To reverse the byte order:

1. In the web-interface left sidebar menu, click **I/O configuration**.
2. In the data map, select the transaction for which you want to do swap the byte order.
3. Select the endian swap type from the **Endian swap** drop-down menu.

Setting	Description
No swapping	Default setting No swapping is performed on the data.
Bytes	Swap 2 bytes A B C D becomes B A D C
Words	Swap 4 bytes A B C D becomes C D A B
Bytes and words	A B C D becomes D C B A

4. To apply the settings, click **Apply** in the web-interface header, and follow the instructions.

7.7.3. Build Detailed Endian Swap

If you have multiple data types, you can use the **Detailed endian swap** to change different parts of the data area in different ways.

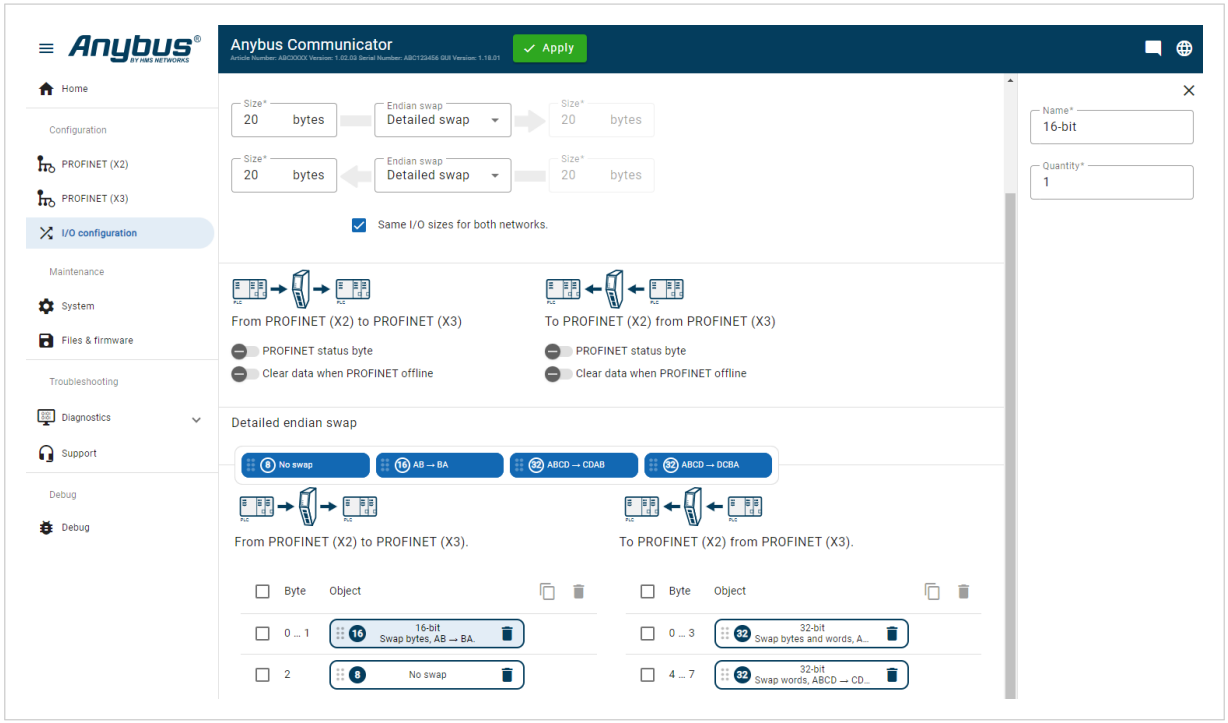


Figure 21. Detailed endian swap example

1. In the **Endian swap** drop-down menu for the desired network(s), select **Detailed swap**.
2. Build the detailed endian swap.

- To add an endian swap object: Drag and drop the desired endian swap object from the toolbar into the drag and drop fields.

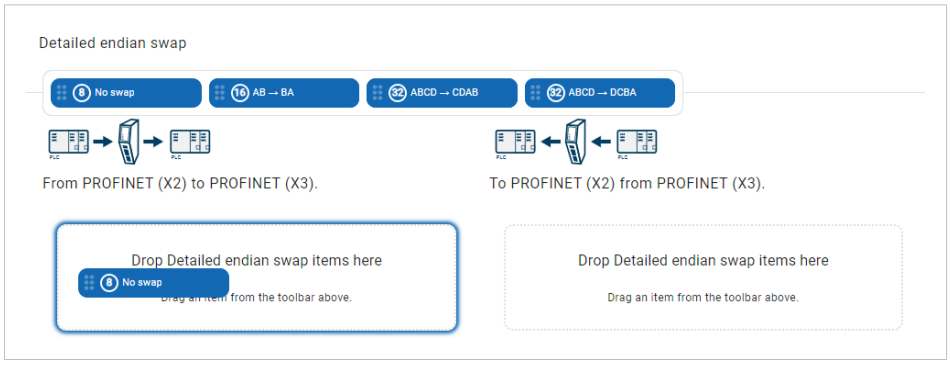


Figure 22. Add endian swap object(s)

- To duplicate an endian swap object: Select the checkbox in front of the endian swap object that you want to duplicate and click the **Duplicate selected** button.
  You can select multiple endian swap objects and duplicate the group.

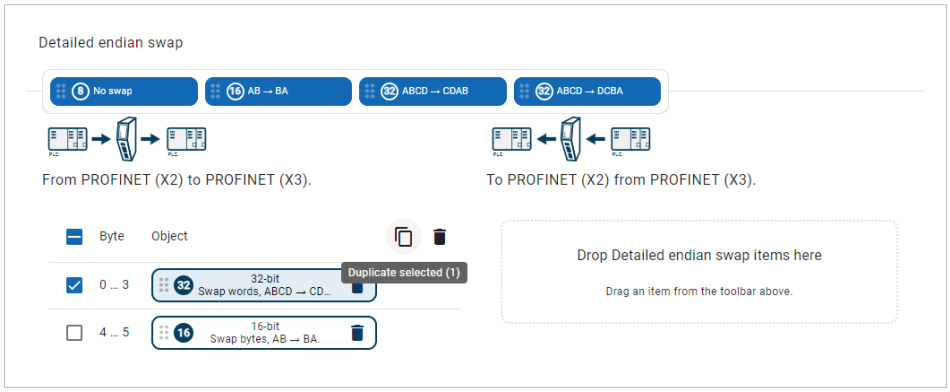


Figure 23. Duplicate endian swap object

- To change the order of the endian swap objects, drag and drop the endian swap objects in the list.

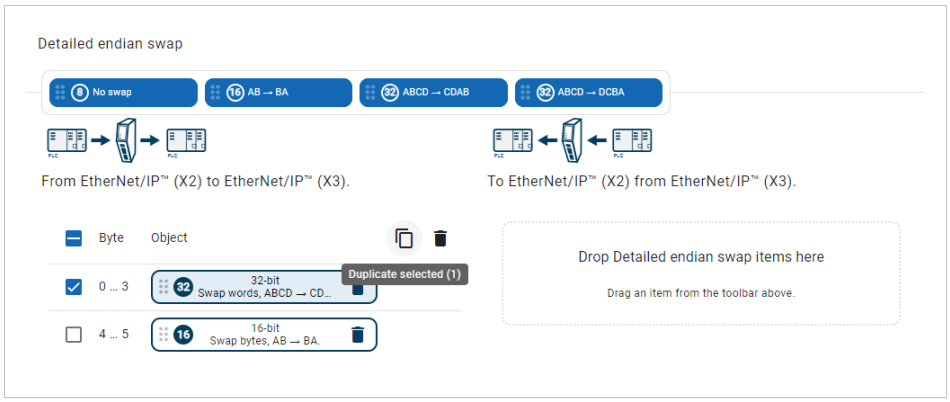


Figure 24. Change endian swap objects order

7.7.4. Process Data Settings

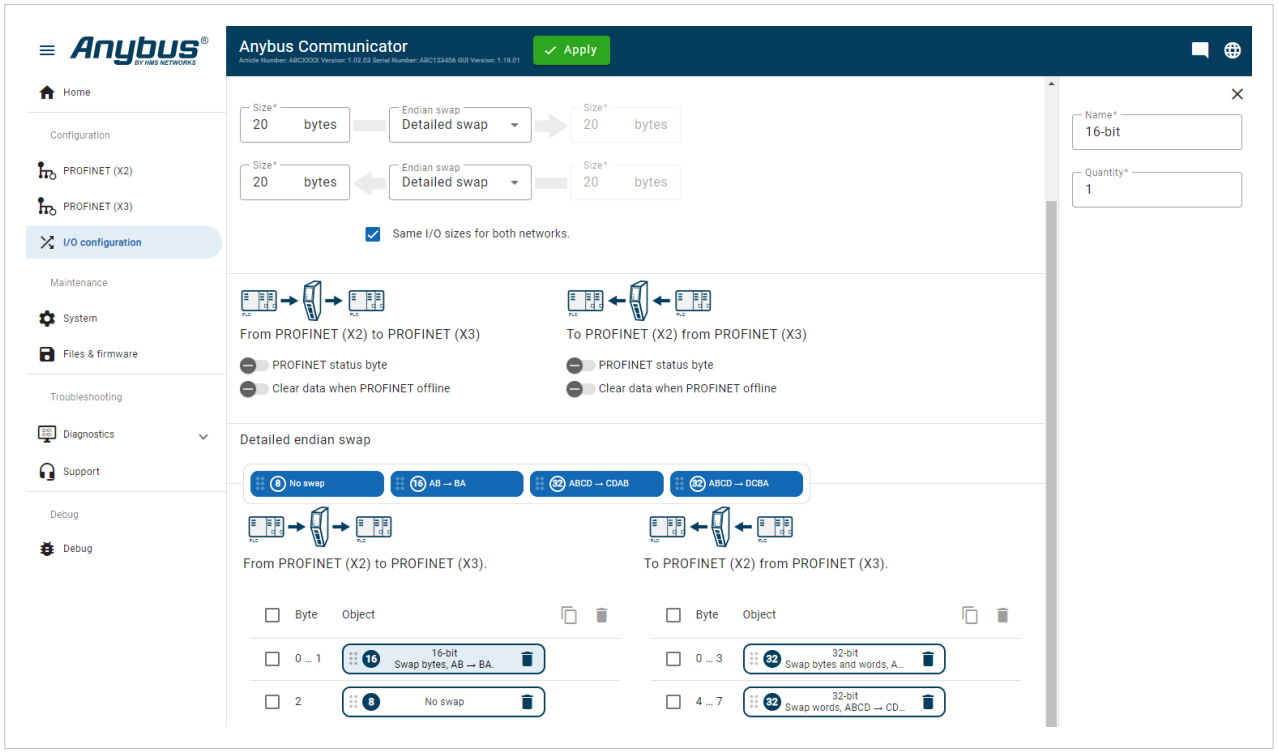


Figure 25. I/O configuration page

Status Byte

> **IMPORTANT**
> Adding a status byte to the I/O area after the data swap can cause data to be overwritten.

A status byte is used where a bit is:

- 1 if the corresponding network is online
- 0 if the corresponding network is not online

When status byte is enabled, it replaces the first data position in the data packet.

By default the status byte settings are disabled.

To enable **PROFINET status byte** and/or **PROFINET status byte**, click the slide toggle(s).

Clear Data

When clear data is enabled, any data sent to/from the Communicator while the network is offline is reset to zero.

By default the clear data settings are disabled.

To enable clear data, click the slide toggle for each network.

7.8. Configuration Notes

You can add notes to describe the Communicator configuration.

7.8.1. Add Configuration Note

Procedure

1. To open the **Configuration Notes** window, click on the **comments** icon .

Figure 26. Configuration note, comment icon

2. To add a new configuration note, click **Add**.

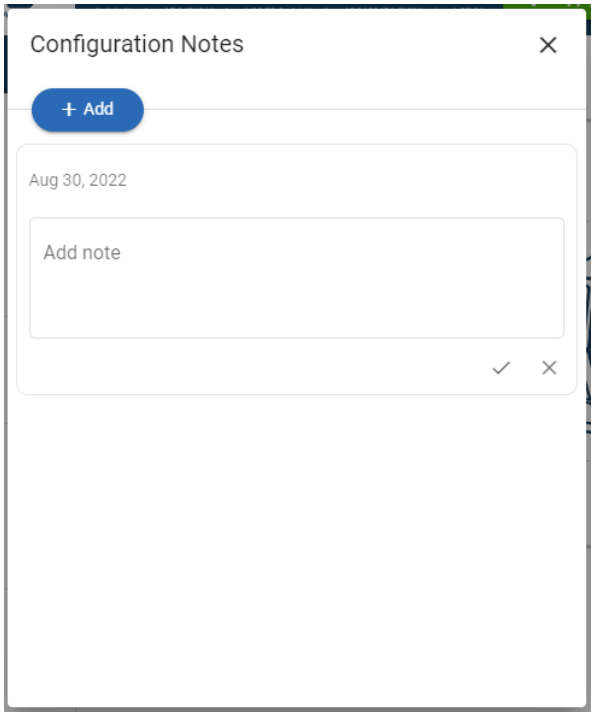


Figure 27. Add new configuration note

3. Write your configuration note and click **accept** ✓.

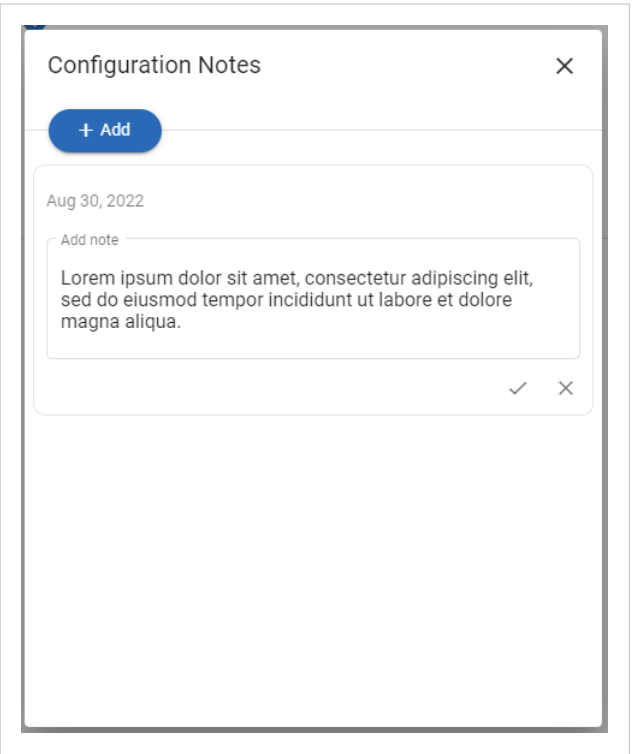


Figure 28. Write a configuration note

The configuration note is added to the list.

4. To close the window, click **close** ×.
5. To save the configuration note, click **Apply** in the web-interface header, and follow the instructions.

7.8.2. View and Edit Configuration Notes

To view and/or edit a note, click on the **comments** icon .

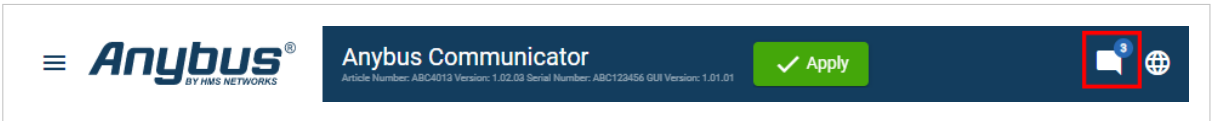


Figure 29. Example: The comment icon indicates that there are three added notes

The configuration notes are listed in the **Configuration Note** window.

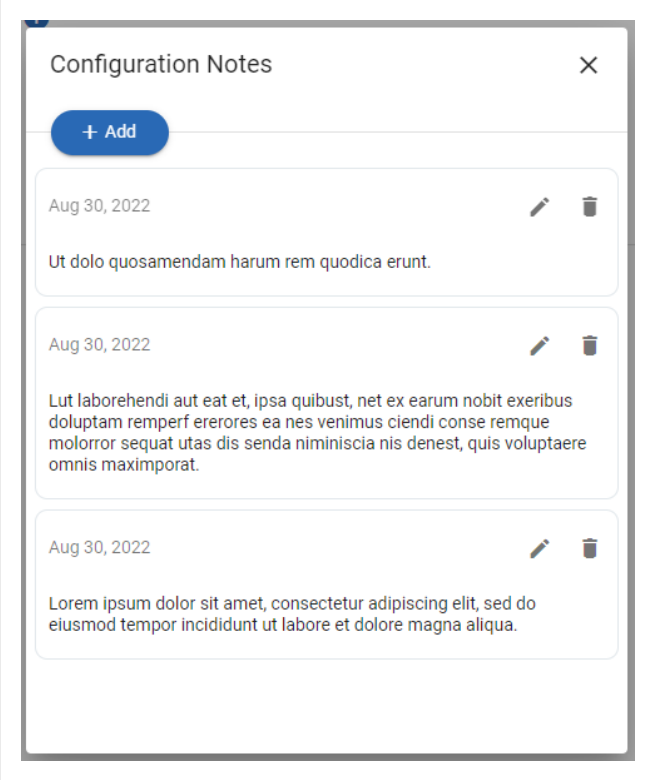


Figure 30. Example: The Configuration Notes window with added notes

7.9. Apply Configuration

Before You Begin

NOTE
When you apply the configuration, any existing configuration is overwritten.

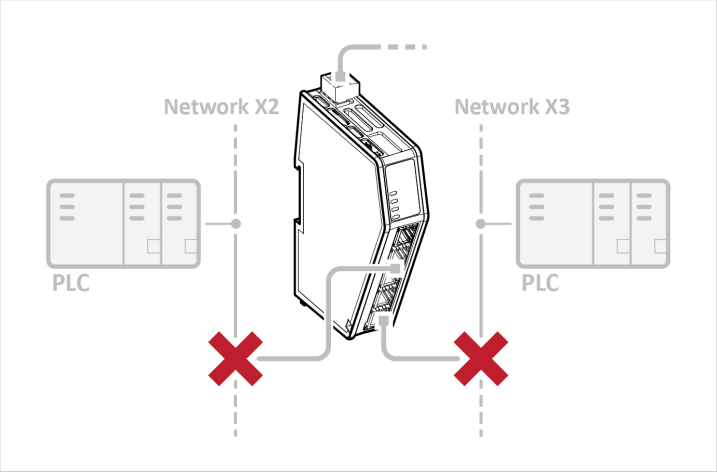


Figure 31. Disconnect the Communicator from the networks

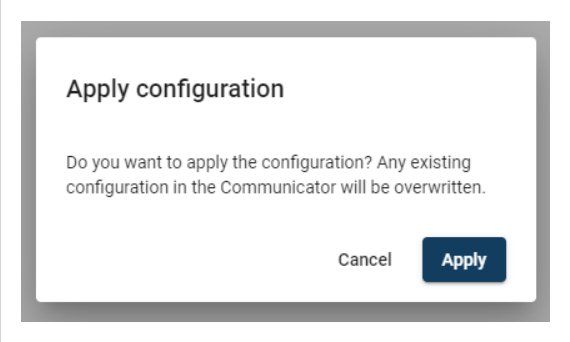
Before you can apply the configuration, ensure that there is no active communication on the PROFINET network or the PROFINET network where the Communicator is connected.

Procedure

To make the settings take effect, download the configuration to the Communicator:

1. In the web-interface header, click **Apply**

2. To confirm download, click **Apply**.
   The configured settings are downloaded and applied to the system.



7.10. To Use an Existing Configuration

When you have configured a Communicator and want to use the same settings to configure additional Communicator, do the following.

Procedure

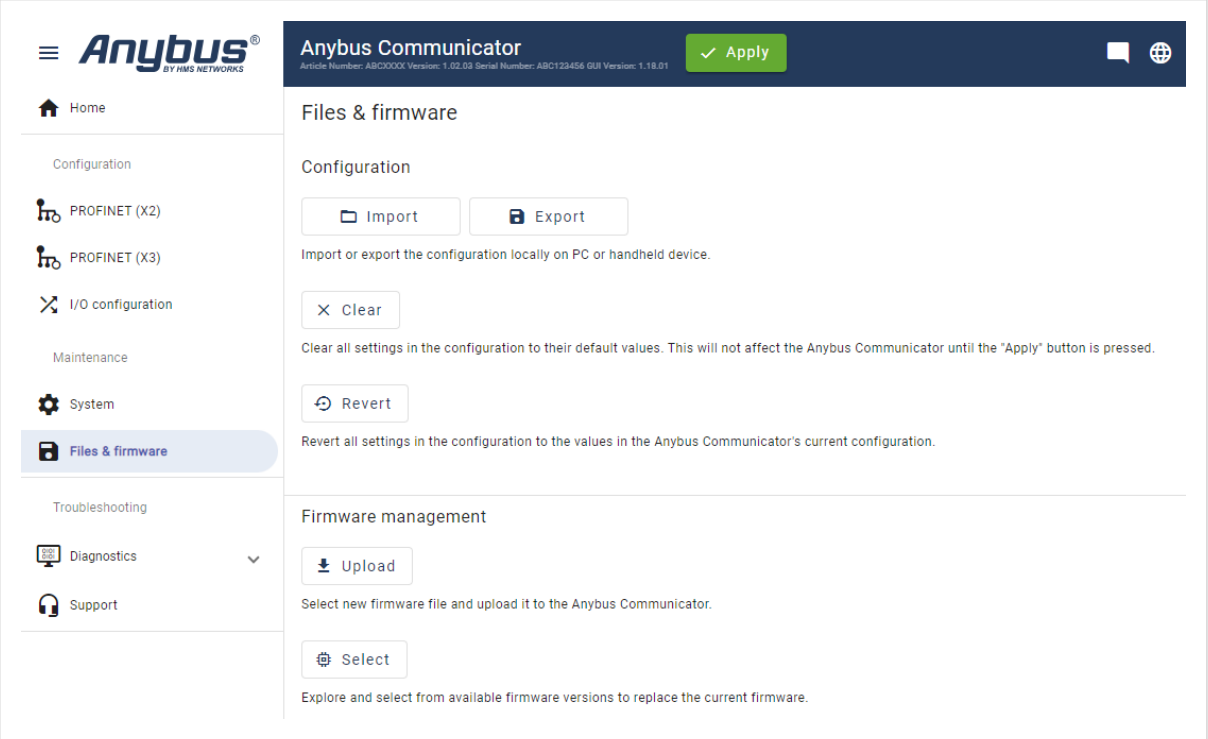


Figure 32. **Files & firmware** page

In the built-in web-interface of the Communicator with the configuration you want to use:

1. On the **Files & firmware** page, click **Export**
   The configuration is saved in a configuration file and downloaded to your PC.

In the built-in web-interface of the new Communicator to be configured:

2. On the **Files & firmware** page, click **Import**
3. In the Import configuration window, click **Select file (.conf)**.
4. In the Open dialog box, browse to and select the configuration file and click **Open**.
5. To import the configuration file, click **Import**.

Result

All the configuration settings are imported.

To apply the settings, click **Apply** in the web-interface header, and follow the instructions.

8. PLC Configuration

8.1. PLC Device Security

IMPORTANT
It is important to maintain the cybersecurity of the Communicator.

Before connecting the Communicator to a PLC, ensure the PLC is configured and installed in accordance with the PLC supplier hardening guidelines.

8.2. Export Product GSDML File

Option if the PLC program requires a product file, GSDML (Generic Station Description Markup Language) file, describing how the Communicator can be used on the high level network.

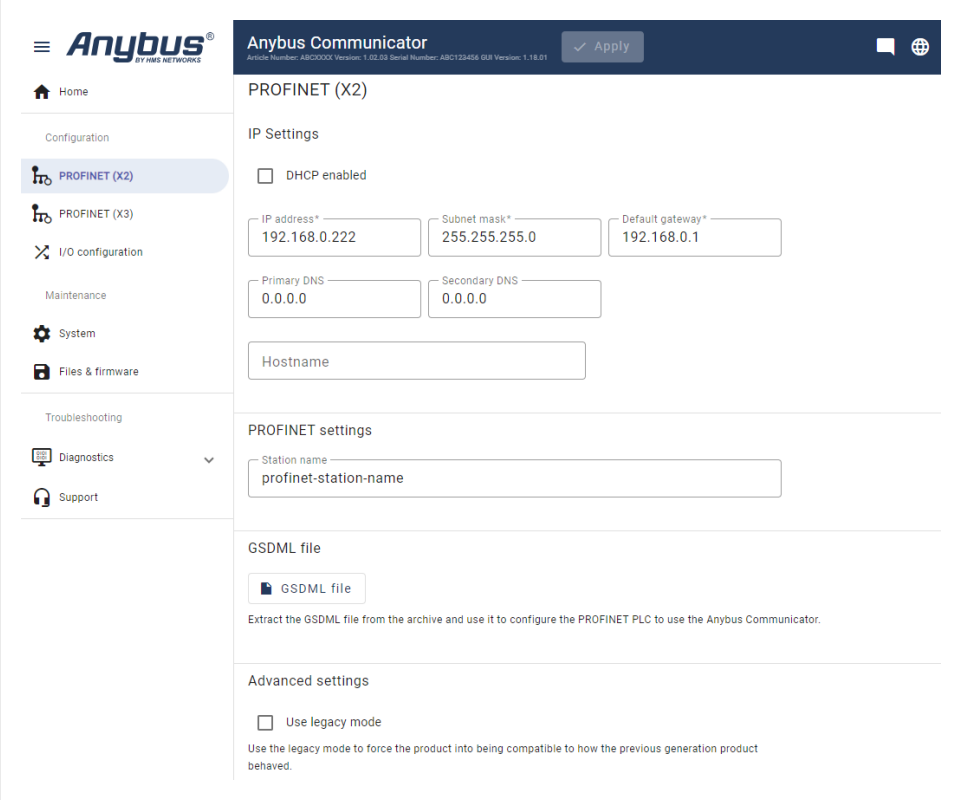


Figure 33. Files & firmware page, PROFINET GSDML file

You find the *PROFINET GSDML* file on the Communicator built-in web interface **PROFINET (X2)** and **PROFINET (X3)** pages.

To export the GSDML file:

- Click **GSDML** file.
  The GSDML file is downloaded to your PC.

9. Verify Operation

9.1. Communicator Status Monitor

On the Home page, you can get a quick overview of the network and the Communicator operating status.

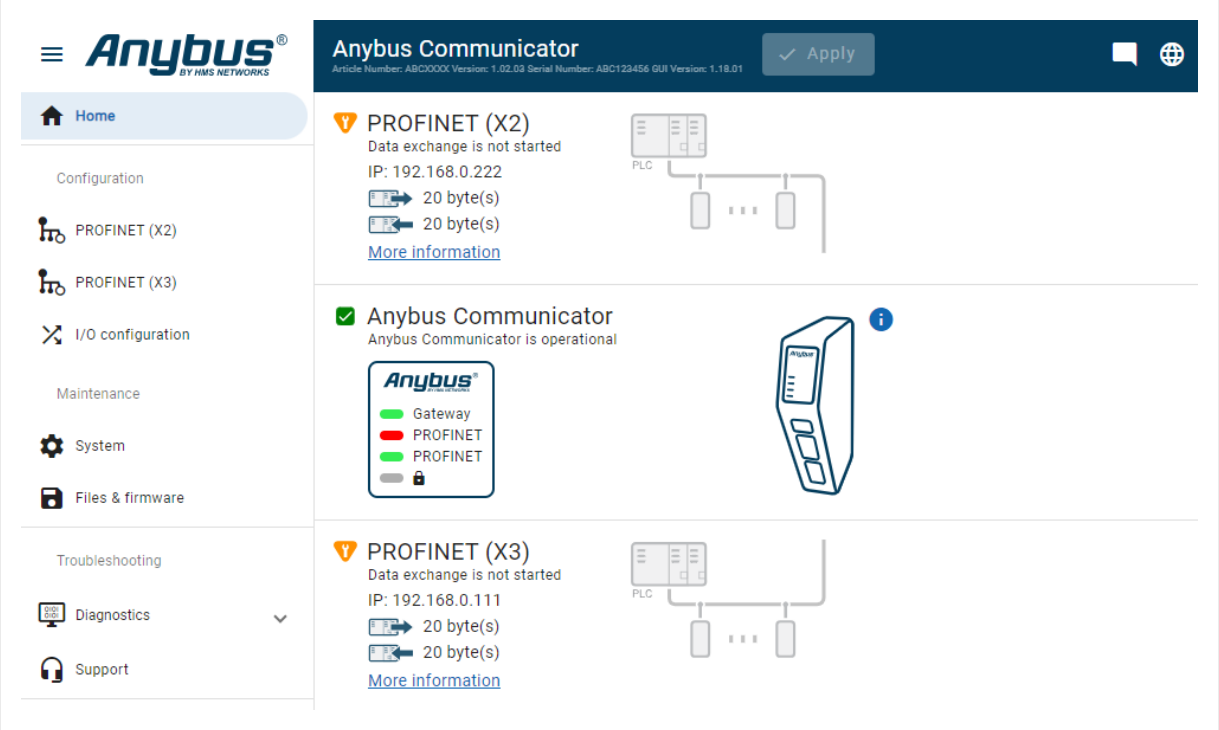


Figure 34. Home page

Gateway status

Overview the Communicator LED indications remotely.

Refer to Communicator LED Indicators (page 42).

Network Status and Settings

Overview communication status and the current networks settings.

Status Symbols

Symbol	Description
	Internal error has occurred, and operation cannot be guaranteed.
	Out of Specification.
	Check Function: • Initial state where non network components are started and configured. • Network startup in progress. • Invalid configuration detected.
	Normal operation.

9.2. Communicator LED Indicators

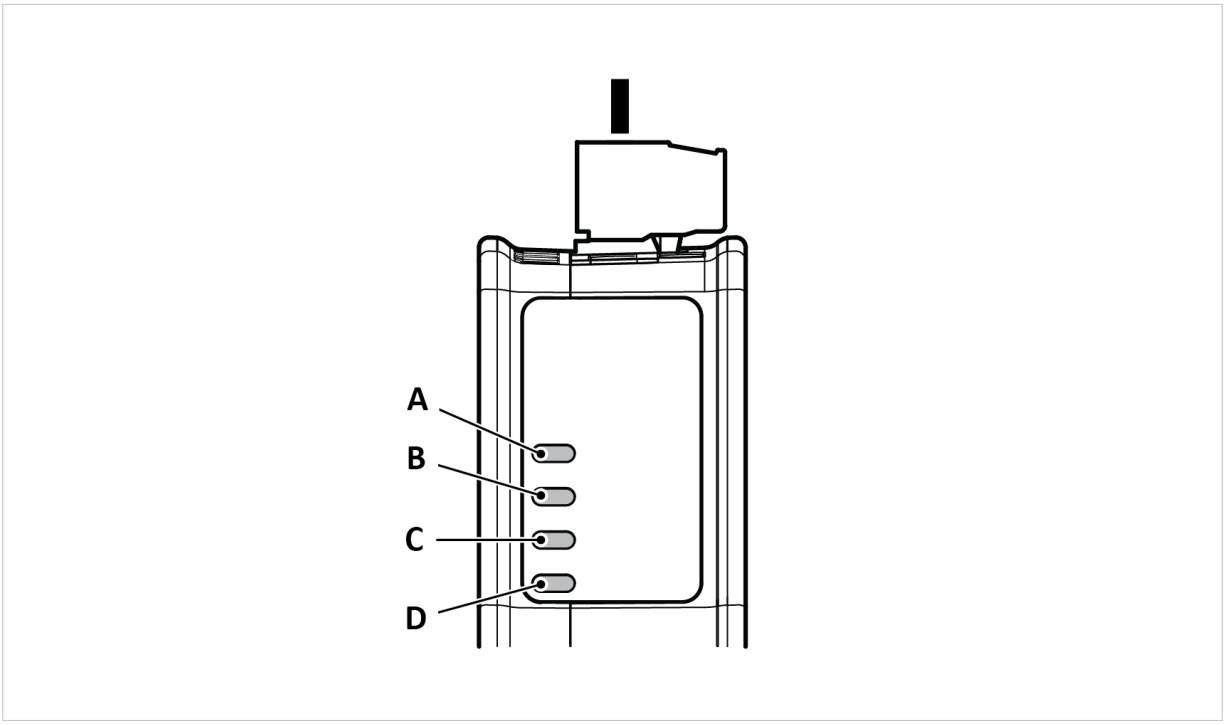


Figure 35. Gateway status (A), Upper connector (B), Lower connector (C) and Security Switch (D)

LED A - Gateway status	
Operation Status	**Description**
Off	No power
Green, flashing	Startup phase
Green, solid	Operational
Red, flashing	Invalid configuration
Green/Red, flashing	Power up self-test/Firmware update/Firmware recovery

LED B - PROFINET, Upper connectors **LED C - PROFINET, Lower connectors**	
Operation Status	**PROFINET**
Off	No power/No connection with IO controller
Green, flashing	Used by engineering tools to identify the node on the network
Green, one flash	Connection with IO controller establishedIO controller in STOP state or IO data bad
Green, solid	PROFINET online, one or more connections established
Red, solid	FATAL event
Red, one flash	Station name not set
Red, two flash	IP address not set
Red, three flash	Expected Identification differs from Real Identification
Red, flashing	One or more connections timed out

Security switch - LED D	
Operation status	**Description**
Off	No power/Security switch is unlocked/Exception/Fatal error
Green	Security switch is locked

9.3. Ethernet LED Indicators

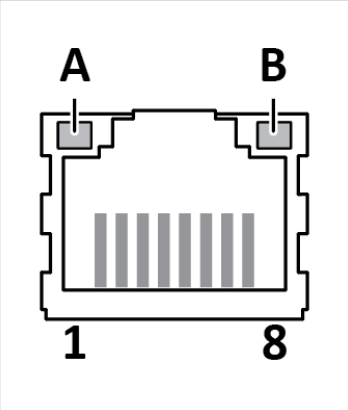


Figure 36. LED A. Activity LED B. Not used

LED A	Function
Off	No link (or no power)
Green	Link (100 Mbit/s) established
Green, flashing	Activity (100 Mbit/s)
Yellow	Link (10 Mbit/s) established
Yellow, flashing	Activity (10 Mbit/s)

LED B	Function
Off	Not used

10. Maintenance

10.1. Action on Fatal Error

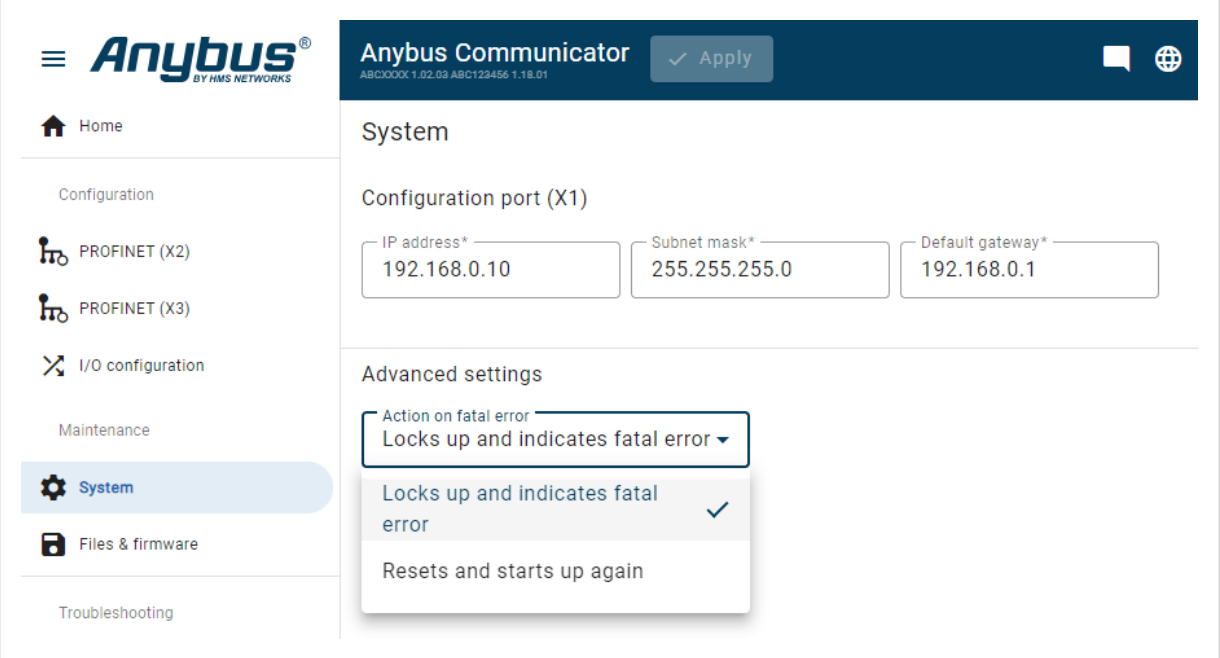


Figure 37. System page, Action on fatal error menu

A fatal error causes the Communicator firmware application to crash in an uncontrolled manner.

You can configure how the Communicator should behave if a fatal error occurs.

In the **Action on fatal error** menu, select one of the following settings:

- **Locks up and indicates fatal error**: Default setting, the Communicator locks up and the LED indicators indicates a fatal error.
- **Resets and starts up again**: The Communicator is rebooted to reset the system and return to normal operation.

10.2. Configuration Port IP Settings

On the **System** page you can change the IP address of the Communicator configuration port.

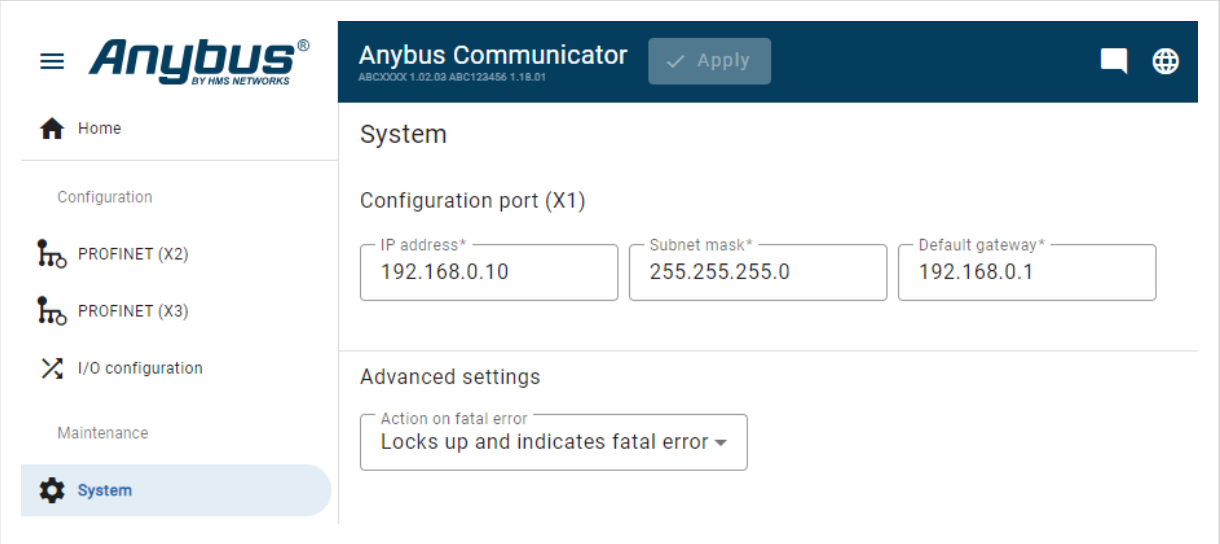


Figure 38. System page, Configuration port settings

Default Configuration Port IP settings

Setting	Default value
IP address	192.168.0.10
Subnet mask	255.255.255.0
Gateway	There is no default Gateway address.

10.3. Configuration File Handling

10.3.1. Export Configuration

You can export the current configuration, to import and use the same settings to configure additional Communicator.

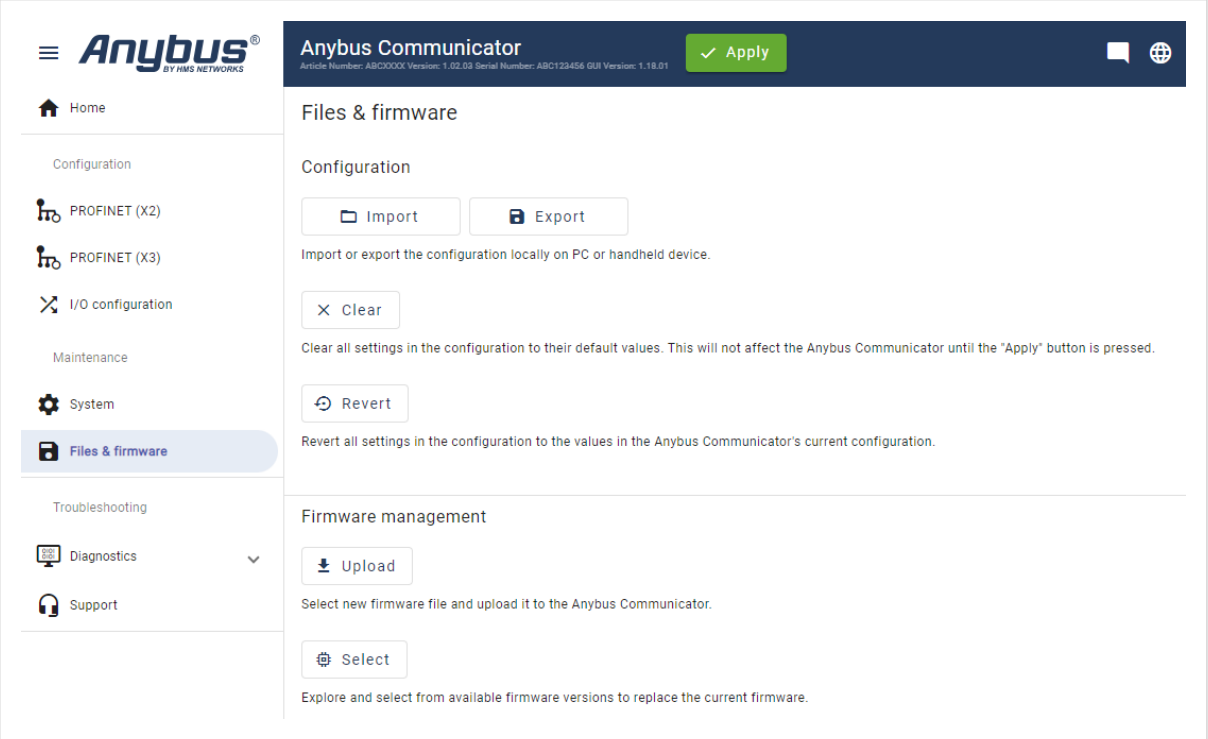


Figure 39. Files & firmware page

To export a configuration file:

In **Files & firmware**, click **Export**.

The configuration settings are stored in a .conf file and downloaded to your PC.

10.3.2. Import Configuration

To easily configure multiple Communicator with the same settings, you can import a configuration file.

Before You Begin

NOTE
Importing a configuration replaces the current applied configuration.

The supported file format is .conf.

Procedure

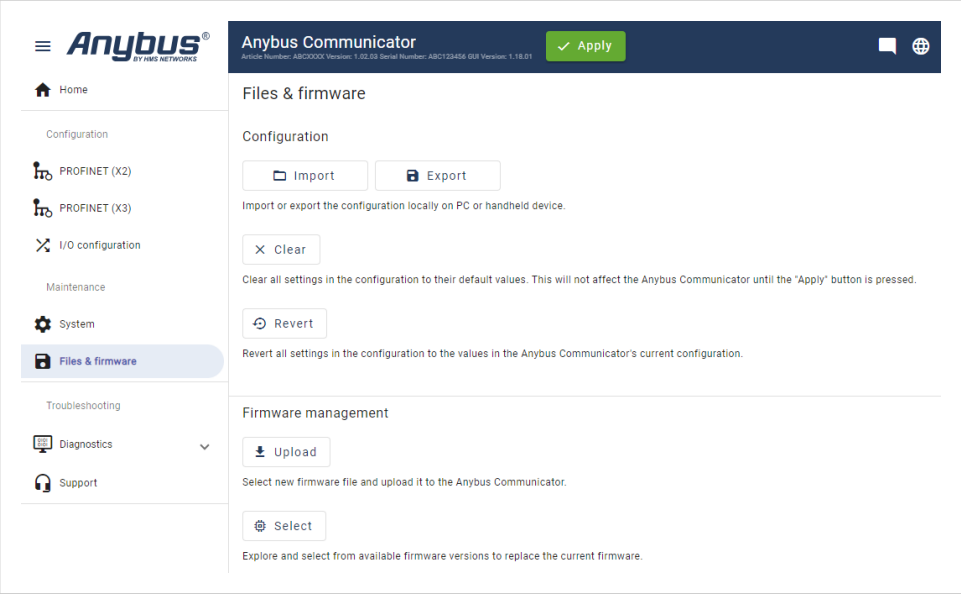


Figure 40. Files & firmware page

Import configuration file:

1. On the **Files & firmware** page, click **Import**.
2. In the Import configuration window, click **Select file (.conf)**.
3. In the Open dialog box, browse to and select the configuration file and click **Open**.
4. In the Import configuration window, click **Import**.
5. In the Communicator address settings window:
   - To import IP settings from the selected configuration file, click **Imported settings**.
     All configuration settings are imported.
   - To continue using the current IP settings, click **Configured settings**.
     All configuration settings except the IP settings are imported.
6. The configuration file is parsed.
   - If the configuration is compatible, the settings are imported.
   - If any compatibility mismatches occur, a message about the mismatch appears.
7. To apply the settings, click **Apply** in the web-interface header, and follow the instructions.

10.4. Clear and Revert Configuration

You can restore all settings in a configuration to the default settings.

Procedure

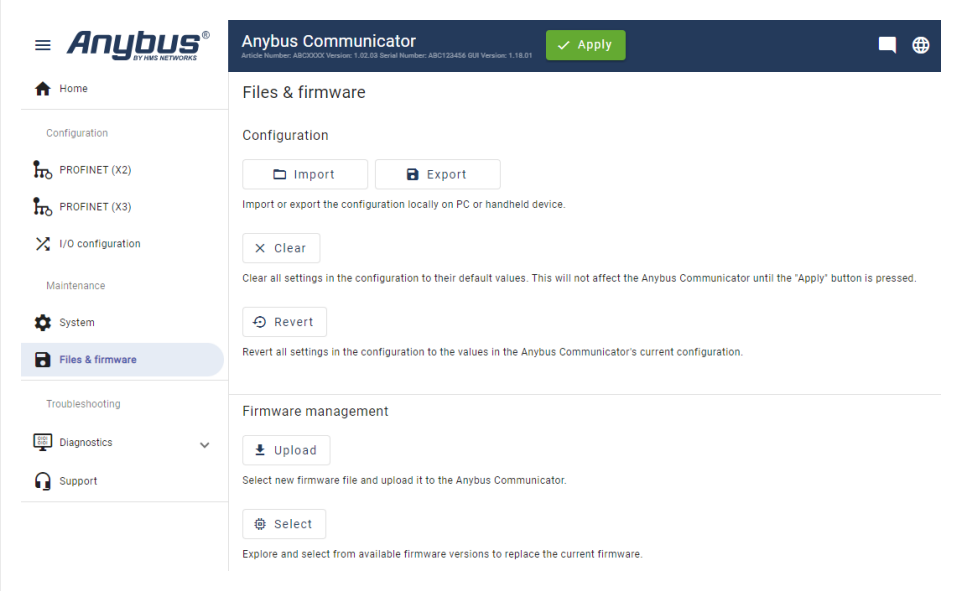


Figure 41. Files & firmware page

To Clear the Configuration

When you want to clear a configuration and return to the default settings.

1. On the **Files & firmware** page, click **Clear**.
2. In the Confirm clear window, click **Clear**.
3. To apply the change, click **Apply** in the web-interface header, and follow the instructions.

To Revert the Configuration

When you want to remove any configuration made in a current session and re-load the configuration from the gateway.

1. On the Files & firmware page, click **Revert**.
2. In the Confirm revert window, click **Revert**.
3. To apply the change, click **Apply** in the web-interface header, and follow the instructions.

10.5. Firmware Management

10.5.1. View the Firmware Version

On the **Support** page, you can view the current applied firmware version.

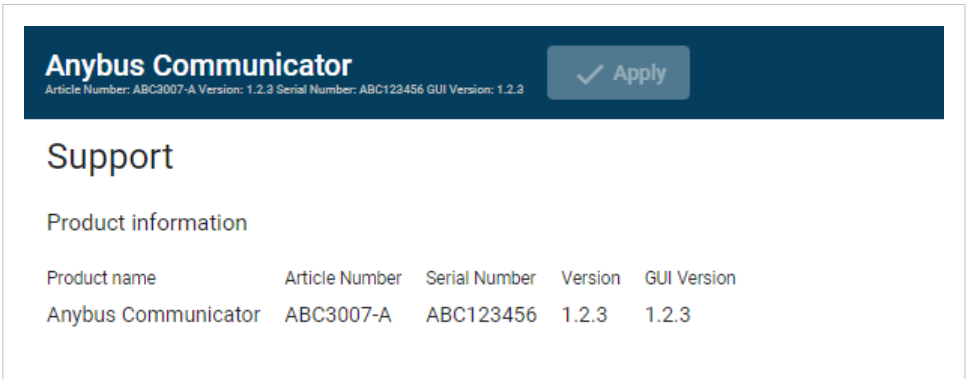


Figure 42. Support page, Product information example

10.5.2. Firmware and Configuration Compatibility

Compatibility after firmware upgrade

Current configuration is still compatible after upgrading the firmware.

Compatibility after firmware downgrade

IMPORTANT

Compatibility after a firmware downgrade cannot be guaranteed.

The current configuration may use features not available in the older firmware version.

10.5.3. Firmware File Validation

Before the firmware file is imported into the system, the firmware upgrade function performs a validation of the file, to ensure that:

- the firmware is compatible with the Communicator hardware
- the firmware is suited for the product
- the officially HMS software signatures are valid
- that the firmware file is not corrupt or damaged

If the firmware file does not pass the validation, the firmware file is rejected and an error message appear.

10.5.4. Update Firmware

Before You Begin

Ensure to disconnect the Communicator from the OT networks.

Procedure

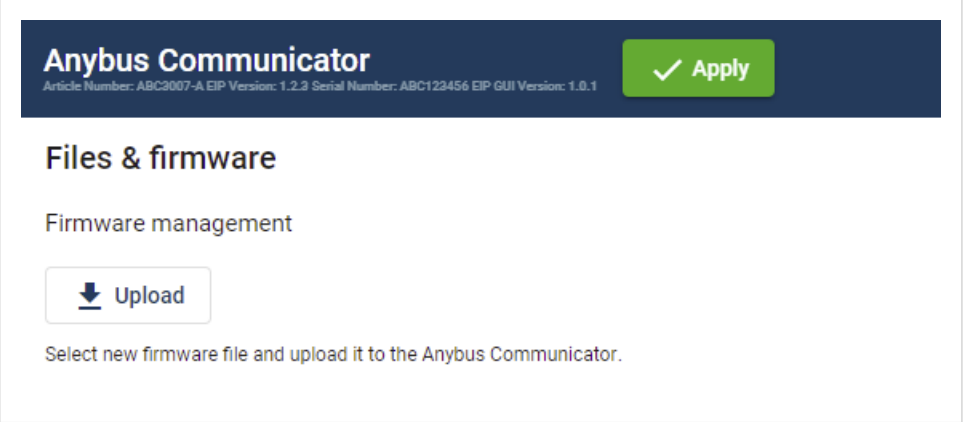


Figure 43. Files & firmware page

To update the firmware:

1. On the **Files & firmware** page, click **Upload**.
2. In the Upload Firmware window, click **Select firmware (.hiff)**.
3. In the Open dialog box, browse to and select the firmware file and click **Open**.
4. To start the firmware upgrade, click **Update firmware**.
   The firmware file is validated and transferred.

Result

- If the firmware file passes the validation: The firmware is upgraded and then the Communicator automatically reboots, for the upgrade to take effect.
- If the firmware file is rejected: An error message appears.

10.6. Change Language

Default language is **English**.

To change the language of the Communicator built-in web interface:

1. In the Communicator built-in web-interface header, click the **Language** icon .

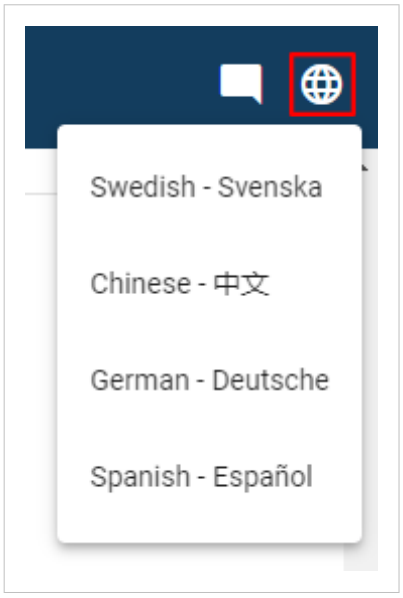


Figure 44. Language menu

2. Select a new language from the list.

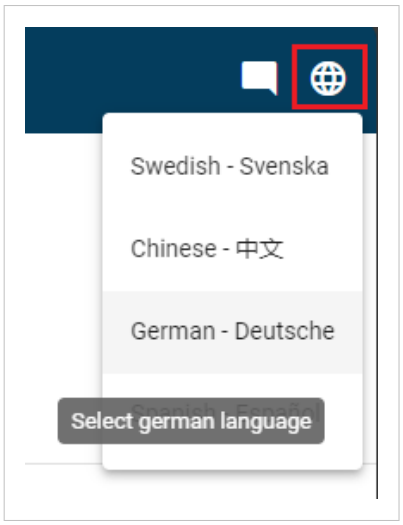


Figure 45. Example: Change language to German

The language change takes effect immediately.

11. Troubleshooting

11.1. Diagnostics

11.1.1. I/O Data

On the **Diagnostics**, **I/O data** page you can monitor how the data flow between the **PROFINET (X2)** side and the **PROFINET (X3)**side, including any configured endian conversions.

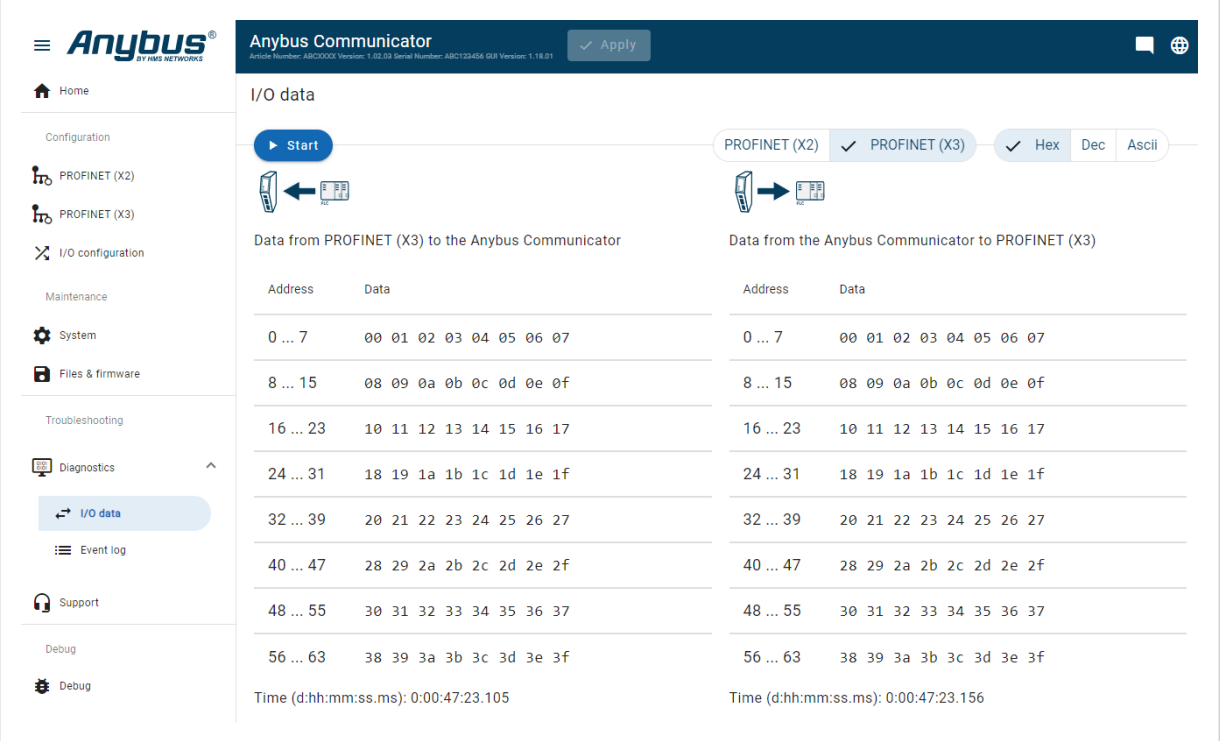


Figure 46. I/O data

I/O data is updated twice every second.

Select how data is displayed

To choose if the data should be displayed in Hexadecimal, Decimal or ASCII, click **Hex**, **Dec** or **Ascii**.

Start and Stop Data flow

- To start the data flow, click **Start**.
- To end the data flow, click **Stop**.

11.1.2. Event Log

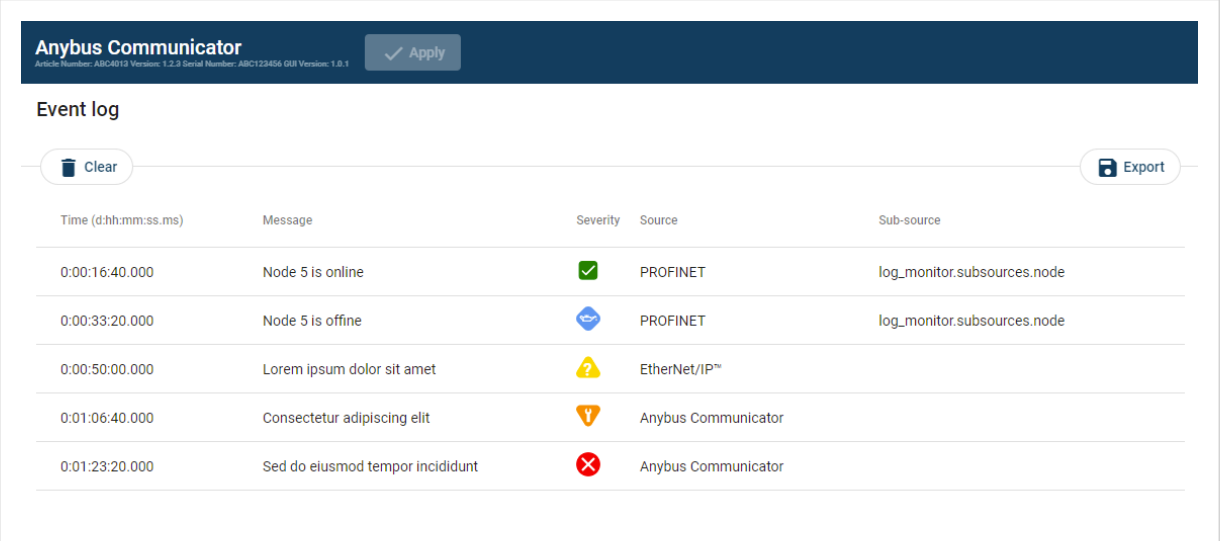


Figure 47. Event log page example

How To Analyze the Information

The log follows the FIFO principle, first in and first out. The oldest (first) value is processed first.

Time (d:hh:mm:ss.ms)	The date and time when the event occurred.	
Message	A brief description of the event.	
Severity	The severity of the event occurred. For description of the symbols, see Communicator Status Monitor.	
Source	0	Communicator
	1	PROFINET (X3)
	2	PROFINET (X2)

To clear the current log, click **Clear**.

11.2. LED Status

On the Home page, you can remotely monitor the Communicator LED status.

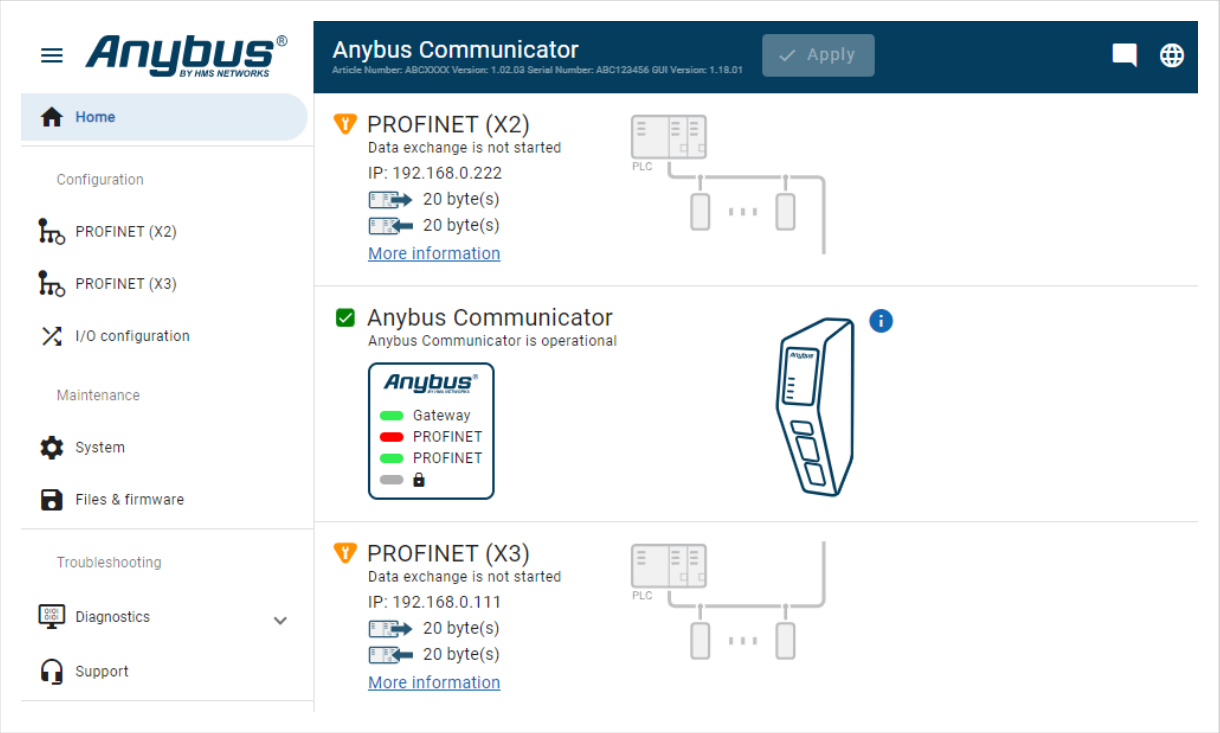


Figure 48. Home page

For information about the LED indication, see Communicator LED Indicators (page 42).

11.3. Reset to Factory Settings

Before You Begin

Factory reset will reset any on site made configuration changes and set the Communicator to the same state as leaving HMS production.

When the Firmware has been updated, factory reset will revert the Communicator configuration to initial state after the update.

Procedure

To reset the Communicator:

1. Disconnect the Communicator from power.

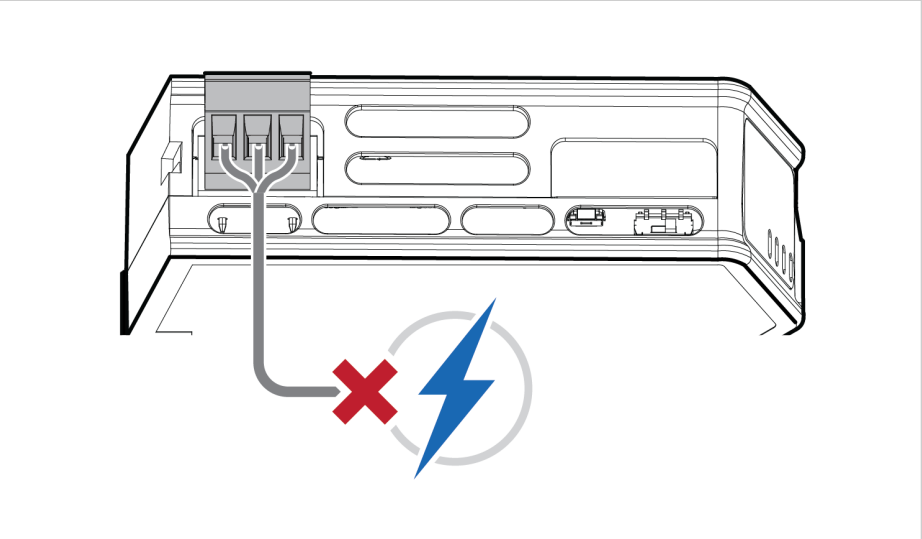


Figure 49. Disconnect power

2. Use a pointed object, such as a ballpoint pen to press and hold the **Reset** button.

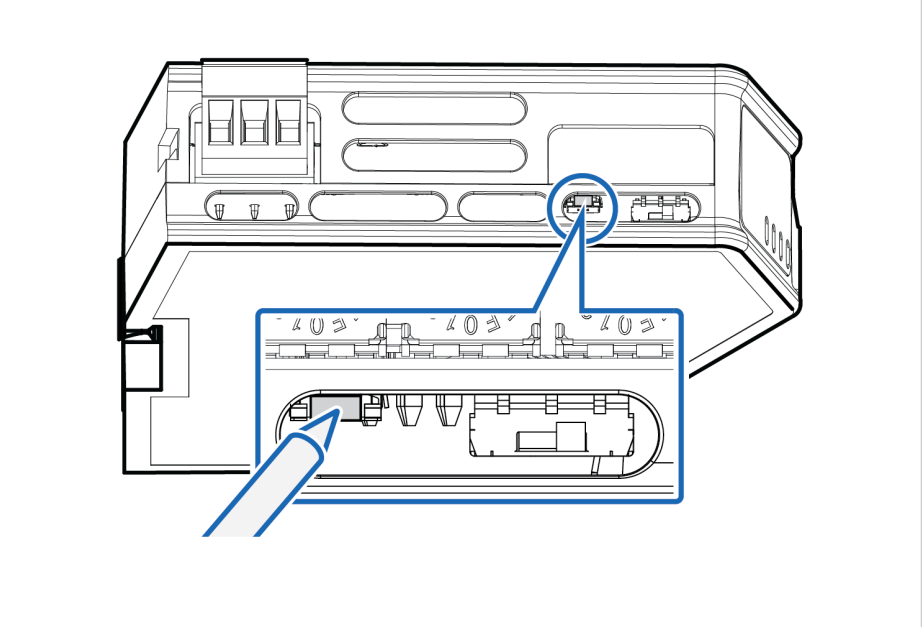


Figure 50. Press and hold **Reset** button

3. While holding the **reset** button, reconnect the Communicator to power.

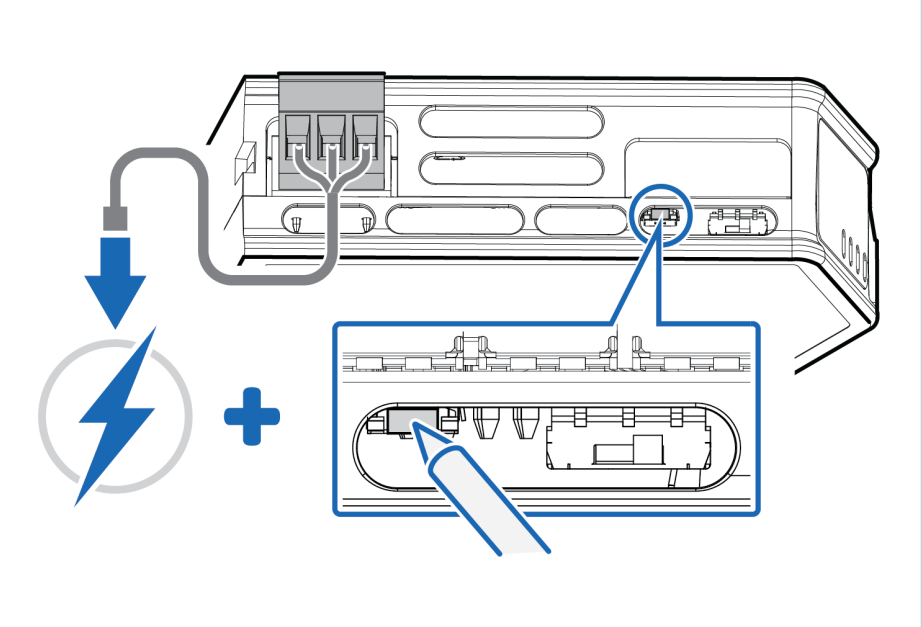


Figure 51. Hold **Reset** button and reconnect power

4. Release the **reset** button.
   The Communicator enters exception state.

5. Reboot the Communicator.

Result

When the Communicator has successfully rebooted, the Communicator configuration is reset to the factory default configuration or the current configuration after firmware upgrade.

To Do Next

To ensure that the Communicator built-in web-interface is synchronized.

1. Open the Communicator built-in web interface.

2. Navigate to the **Files & firmware** page and click **Revert**.

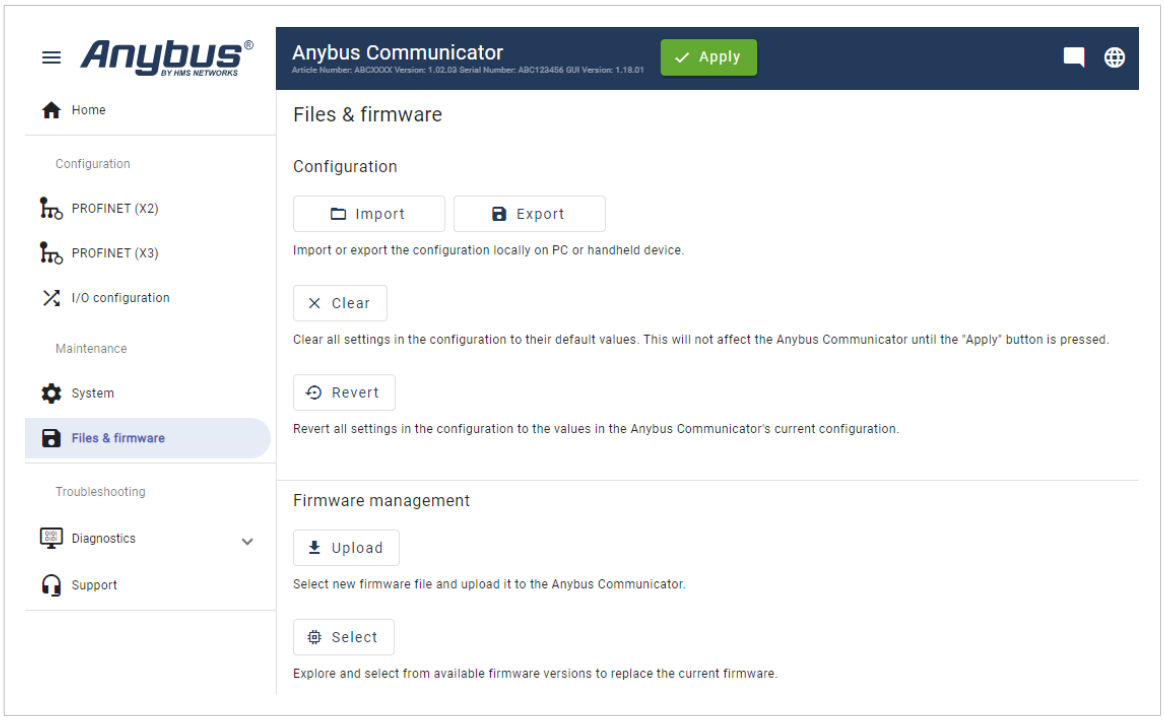


Figure 52. Files & firmware, Revert

11.4. Firmware Upgrade Error Management

Before You Begin

If the firmware update process is interrupted or if the power is lost during the update process, the Communicator goes into fallback mode.

The last working firmware is still available on the flash, but it is not active.

Procedure

To complete the interrupted firmware update:

1. Disconnect the Communicator from power.

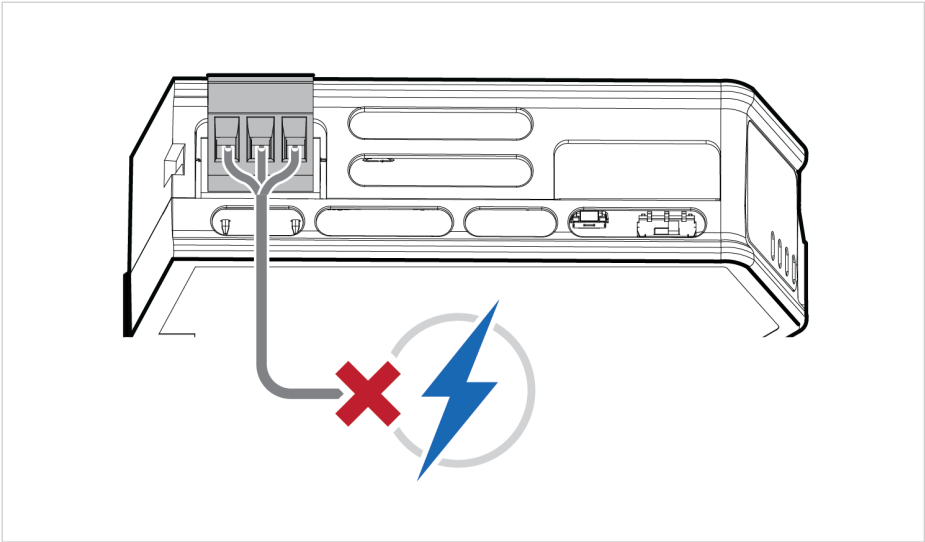


Figure 53. Disconnect power

2. Reconnect the Communicator to power.

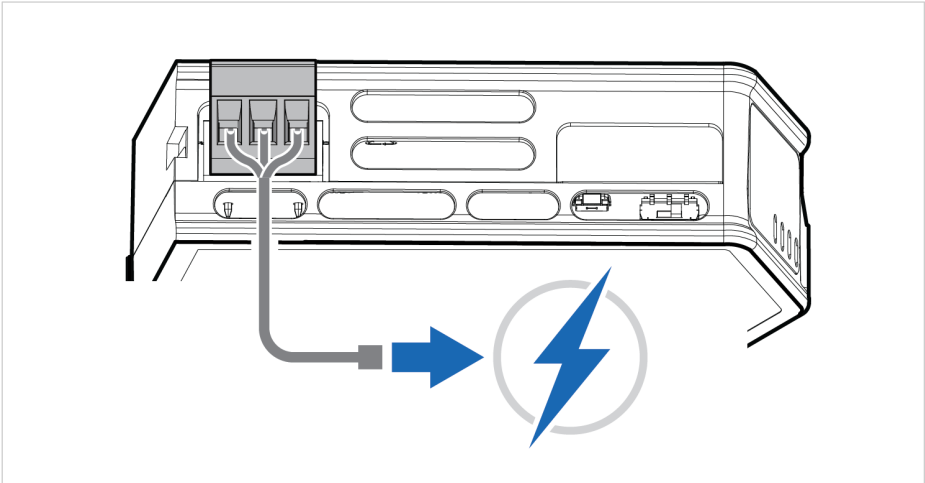


Figure 54. Reconnect power

3. Leave the Communicator for 10 minutes.
   The Gateway status led indicator flashes red and green until the firmware upgrade is completed.

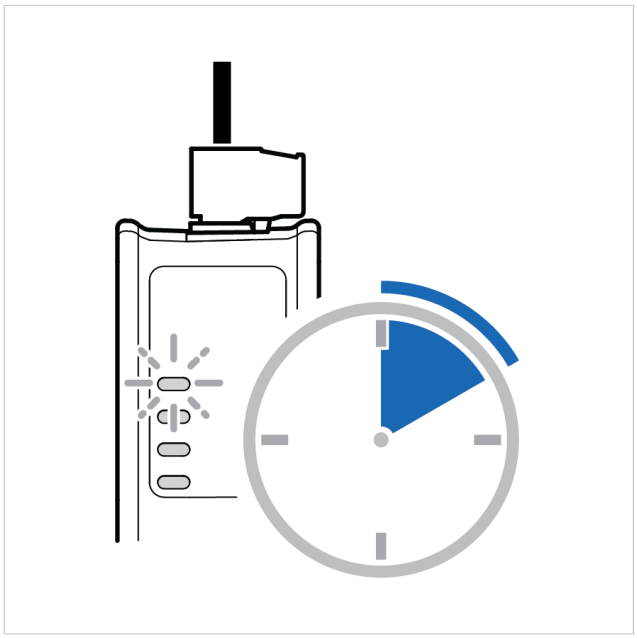


Figure 55. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

Figure 56. Recover and return to normal operation

To Do Next

To check LED status, refer to Communicator LED Indicators (page 42)

11.5. Support

11.5.1. Support Package

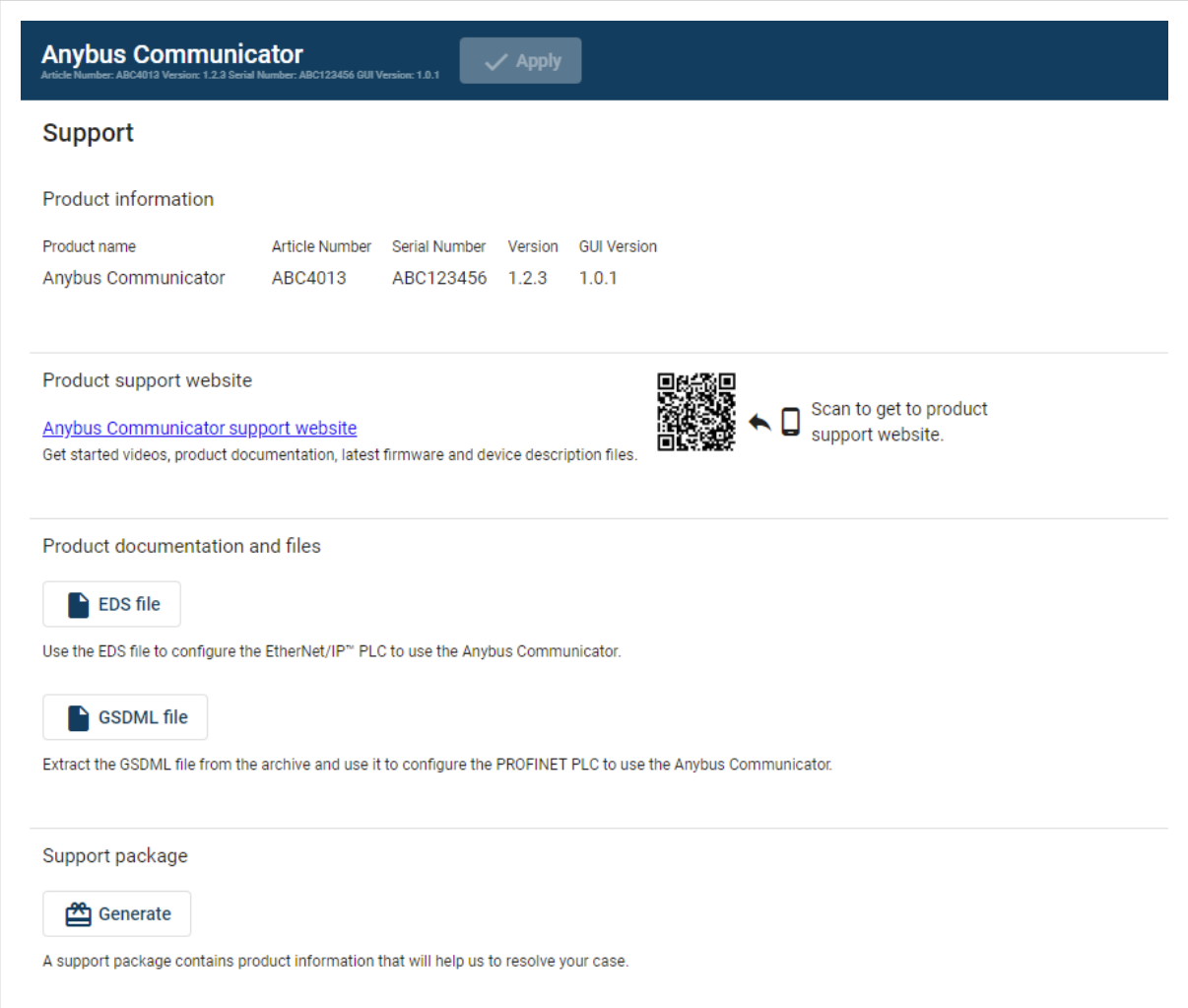


Figure 57. Support page example

Before you create a ticket for technical support, generate a support package.

The support package contains information about what has occurred and will help the Anybus technical support team resolve the support case as quickly and efficiently as possible.

Support Package Content
The information in the support package is available to open and read, the files are not locked or encrypted.

Generate Support Package
On the **Support** page, click **Generate**.

A zip file with the support files is downloaded to your PC.

Create a Support Ticket
1. On the **HMS Networks** home page, navigate to the **Support** main menu and click **Support portal**.
2. In the **Support portal**, create a support ticket and upload the support package.

12. End Product Life Cycle

12.1. Secure Data Disposal

IMPORTANT
To avoid exposure of sensitive data, always perform a factory reset before decommissioning the equipment.

Factory reset will reset any on site made configuration changes and set the Communicator to the same state as leaving HMS production.

See Reset to Factory Settings (page 55).

13. Technical Data

13.1. Technical Specification

Article identification	ABC4022
Configuration connector	RJ45
Communication connectors	RJ45 x 4
Power connector	3-pin screw connector
Power supply	12-30 VDC, Reverse voltage protection and short circuit protection
Power consumption	Typical: 90 mA @ 24 V (2.2 W) Max: 3 W
Storage temperature	-40 to +85 °C
Operating temperature	-25 to +70 °C
Humidity	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days EN 60068-2-30: Damp heat, +25°C – +55°C, 95% RH, 2 cycles
Vibration	See datasheet
Housing material	Plastic, See datasheet for details
Protection class	IP20
Product weight	150 g
Dimensions	27 x 144 x 98 mm (W x H x D) with connectors included
Mounting	DIN-rail