ENGLISH

Anybus® Communicator™ - PROFIBUS to Modbus TCP Client

USER MANUAL

SCM-1202-226
Version 1.2
Publication date 2025-10-23

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 © 2025 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 Web Browsers 7
4.4.2. Supported Operating Systems 7
4.5. HMS Software Applications 8
4.6. Third-Party Software Applications 8
4.7. Software License Information 8

5. About Anybus Communicator 9
5.1. Modbus TCP Client Communication 9
5.1.1. Modbus TCP Client Building Blocks 9
5.2. How the Communication Works 11
5.3. How the Data Exchange Works 13

6. Installation 14
6.1. External Parts 14
6.2. Connector Port Guide 15
6.3. DIN Rail Mounting 16
6.4. Connect to Modbus TCP Client Network 17
6.5. Connect to PROFIBUS Network 19
6.6. Rotary Switch Settings 20
6.6.1. Rotary Switches Default Setting 20
6.6.2. Set a Node Address with Rotary Switches 21
6.7. Connect to Power 25
6.8. Security Switch 27
6.9. Lock the Cables 29
6.10. DIN Rail Demount 30

7. Configuration Quick Guide 31
7.1. Prepare Configuration 31
7.2. Setup New Configuration 36
7.3. PLC Configuration 38

7.4. Verify Operation 39

8. Communicator Configuration 41

8.1. Connect to Configure the Communicator 41
8.2. Access the Built-In Web Interface from HMS IPconfig 42
8.3. Access the Built-In Web Interface from a Web Browser 44
8.4. Communicator Built-In Web Interface Overview 45
8.5. Modbus TCP Client Communication Settings 46
8.5.1. IP Settings 46
8.6. Modbus TCP Client Servers 47
8.6.1. Add Server 47
8.6.2. Server Properties 48
8.6.3. Add Transactions 49
8.6.4. Modbus Function Codes 50
8.6.5. Transaction Properties 51
8.6.6. Duplicate Transaction 53
8.6.7. Delete Transaction 53
8.7. PROFIBUS Settings 54
8.7.1. PROFIBUS Address Settings 54
8.8. PROFIBUS Advanced Settings 55
8.8.1. Legacy Mode for PROFIBUS General Station Description (GSD) File 55
8.8.2. Allow Any Module Mapping for PROFIBUS 56
8.9. I/O Configuration 58
8.9.1. Map Area Object Order 59
8.9.2. Endian Swap 59
8.9.3. Map Area 60
8.9.4. Bit Offset 61
8.9.5. Convert Between Big-Endian and Little-Endian 64
8.9.6. Live List 65
8.9.7. Data Exchange Control 67
8.10. Configuration Notes 69
8.10.1. Add Configuration Note 69
8.10.2. View and Edit Configuration Notes 71
8.11. Apply Configuration 72
8.12. To Use an Existing Configuration 73
8.13. To Use a Legacy Modbus TCP Client Configuration 74

9. PLC Configuration 77

9.1. PLC Device Security 77
9.2. Export Product GSD File 78

10. Verify Operation 80

10.1. Communicator Status Monitor 80
10.2. Communicator LED Indicators 82
10.3. Ethernet RJ45 LED Indicators 84

11. Maintenance 85

11.1. Action on Fatal Error 85
11.2. Configuration Port IP Settings 86
11.3. Configuration File Handling 87
11.3.1. Export Configuration 87
11.3.2. Import Configuration 88
11.4. Clear and Revert Configuration 89
11.5. Firmware Management 90
11.5.1. View the Firmware Version 90

11.5.2. Firmware and Configuration Compatibility 90
11.5.3. Firmware File Validation 90
11.5.4. Update Firmware 91
11.6. Change Language 92

12. Troubleshooting 93
12.1. Diagnostics 93
12.1.1. I/O Data 93
12.1.2. Event Log 94
12.1.3. LED Status 95
12.2. Reset to Factory Settings 96
12.3. Firmware Upgrade Error Management 99
12.4. Support 102
12.4.1. Support Package 102

13. End Product Life Cycle 103
13.1. Secure Data Disposal 103

14. Technical Data 104
14.1. Technical Specification 104

This page is intentionally left blank.

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/technical-support.

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 96).

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.

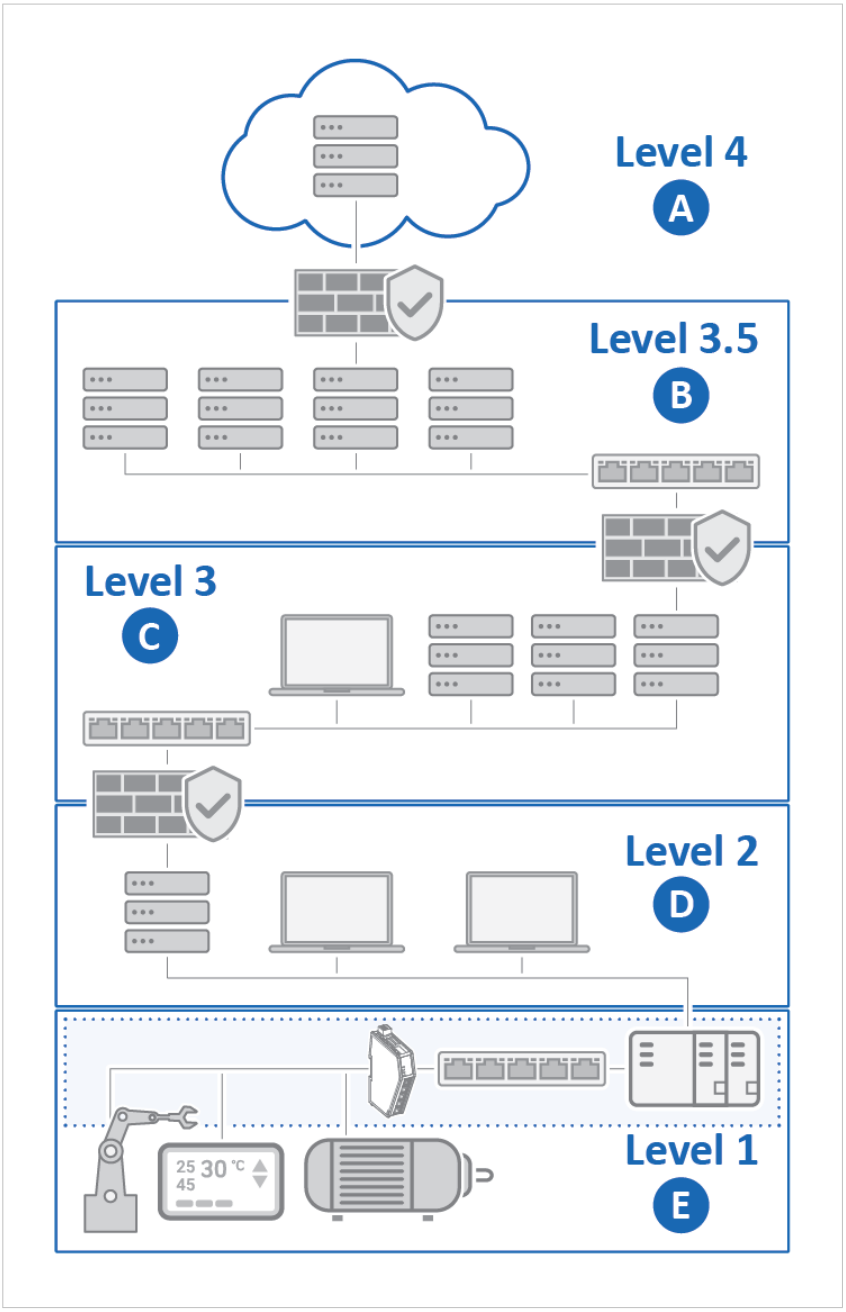


Figure 1. Purdue model, product security context

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/technical-support.

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:

- Power cable.
- Ethernet cable for configuration.
- Ethernet cable for connecting to network.
- PROFIBUS cable for connecting to network.

4.3. Mechanical Tools and Equipment

Have the following tool(s) available:

Flat-head screwdriver, size 5.5 mm

Needed when removing the Communicator from DIN-rail.

Needed when changing the position of the rotary switches.

4.4. System Requirements

4.4.1. Supported Web Browsers

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

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

4.4.2. 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

4.5. HMS Software Applications

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

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/technical-support.

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 Anybus Communicator

5.1. Modbus TCP Client Communication

5.1.1. Modbus TCP Client Building Blocks

The following building blocks are used to describe the subnetwork communication.

Server

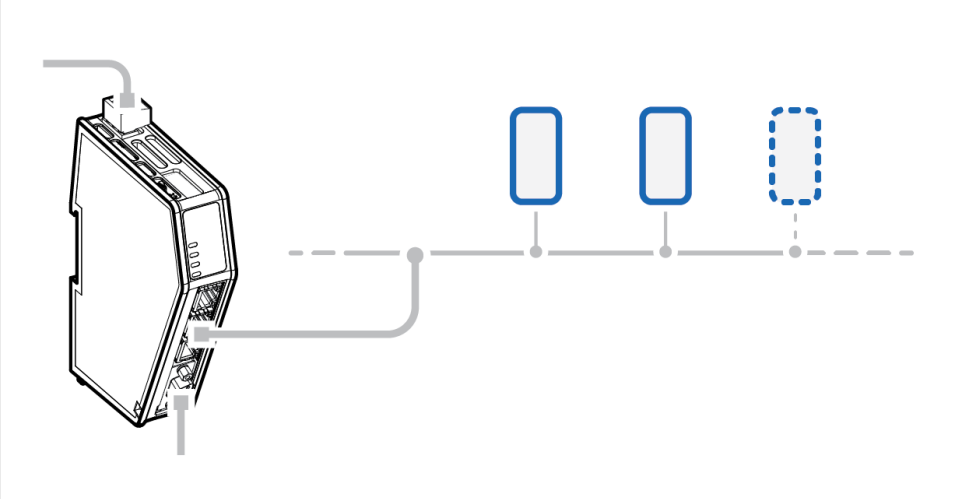


Figure 2. Servers on a Modbus TCP subnetwork

A server represents a single Modbus TCP device on the Modbus TCP subnetwork.

Servers and Transactions

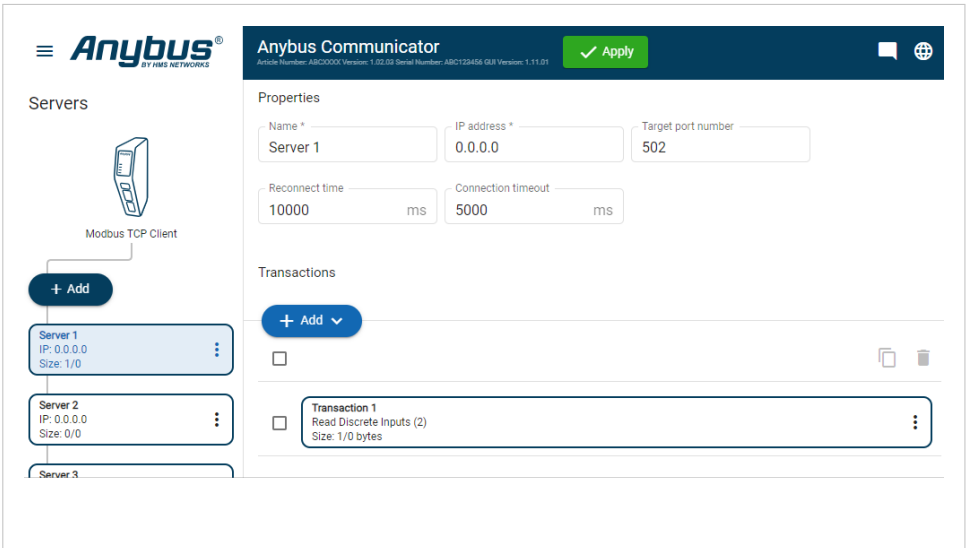


Figure 3. Server with Transactions

Transactions are based on standard Modbus transactions and define the data to be sent or received. See also (page 50).

Each transaction has a number of parameters that need to be configured to define how and when data is to be sent/received.

5.2. How the Communication Works

The Communicator enables communication, data exchange, between one or more server devices connected to a subnetwork and a client device connected to a high level network.

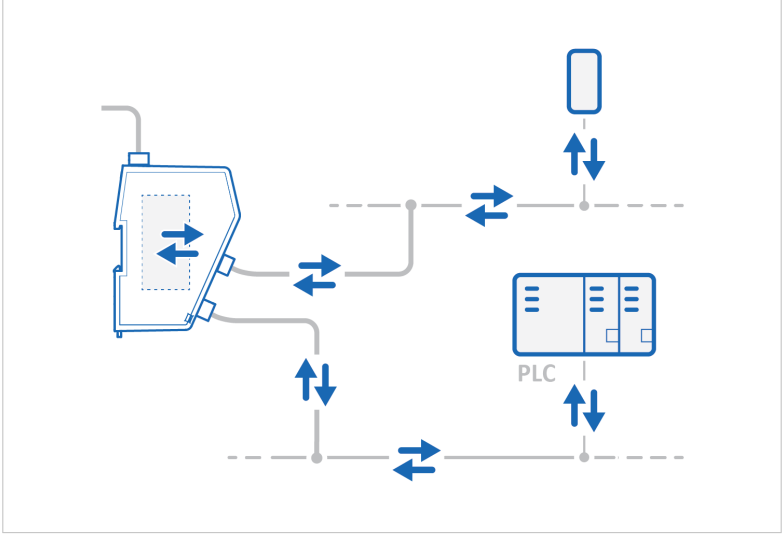


Figure 4. Process data traffic overview

For example:

- The client device can be a PLC controller or a PC.
- A server device can be a sensor, scanner, industrial robot, or sniffer.

The Communicator main task is to send the transactions that the server device(s) are configured to execute, in order to request and transfer process data.

Request Process Data

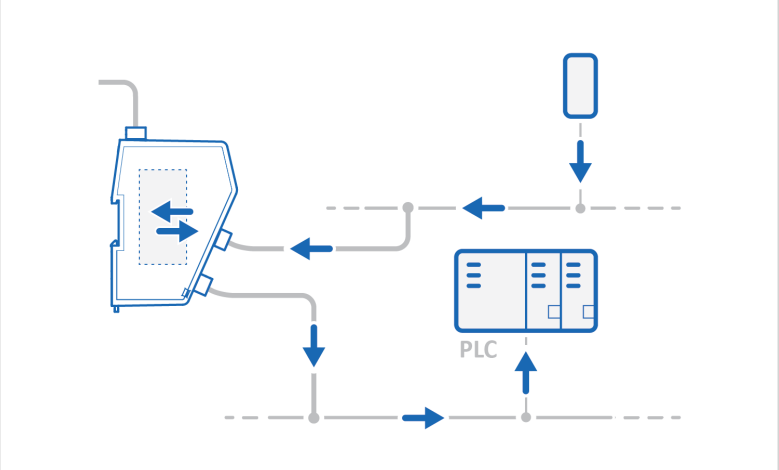


Figure 5. Process data traffic from servers to client

Request process data from the subnetwork nodes, specified in the Communicator configuration, and make the process data available on the server interface and for the high level network client device.

Transfer Process Data

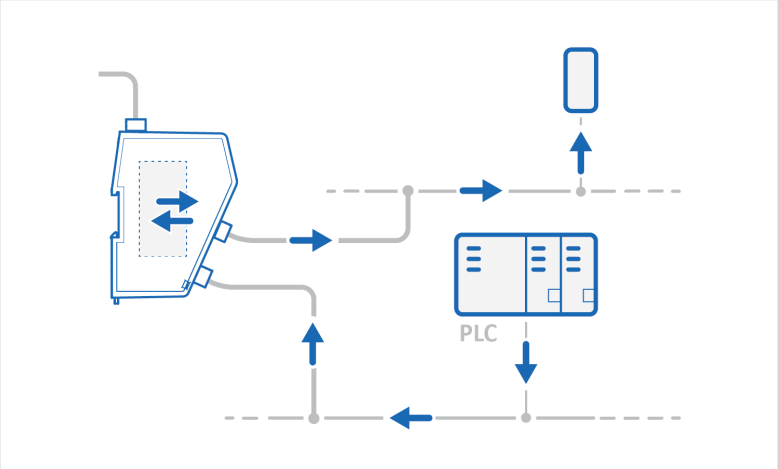


Figure 6. Process data traffic from client to servers

Transfer process data from the high level network client device and make it available on the server interface and for the subnetwork nodes included in the configuration.

5.3. How the Data Exchange Works

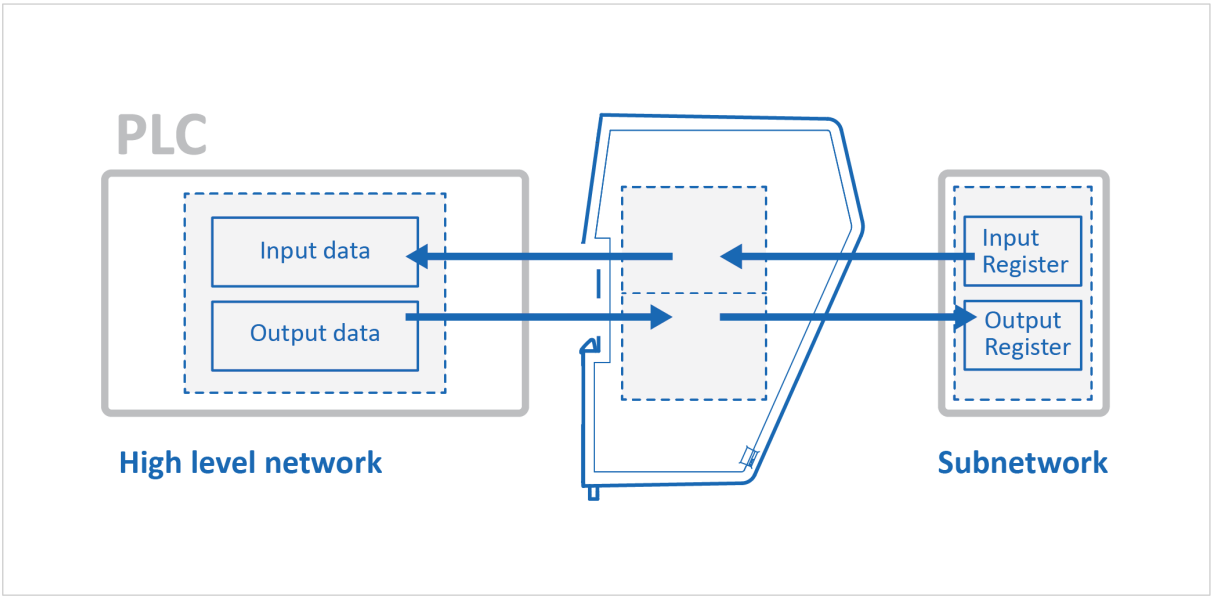


Figure 7. The Communicator internal memory areas

The data exchanged between the Communicator and the Modbus TCP Client subnetwork and the high level network resides in the Communicator internal memory buffer.

To exchange data with the Modbus TCP Client subnetwork, the high level network reads and writes data to the Communicator internal memory buffer.

The same memory locations are exchanged on the Modbus TCP Client subnetwork.

The memory locations are specified when configuring the Communicator using the Communicator built-in web interface.

Input Data

The Input data area is read by the high level network.

Output Data

The Output data area is read/written by the high level network.

6. Installation

6.1. External Parts

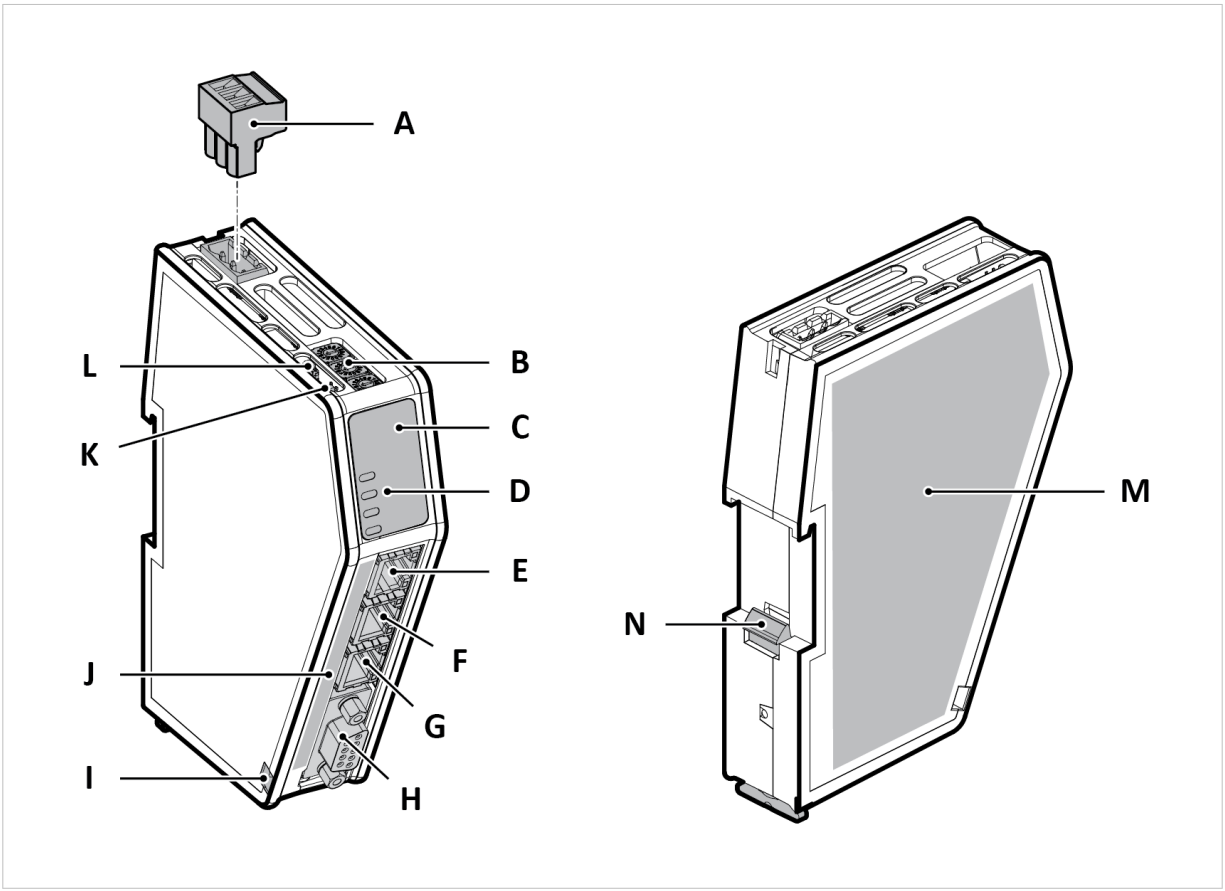


Figure 8. Communicator external parts

A. Power connector
B. Rotary Switch x 3
For PROFIBUS address
C. Label with LED designation
D. Status LEDs
E. Configuration port
F. Modbus TCP Client (X2.1) port
G. Modbus TCP Client (X2.2) port
H. PROFIBUS (X3) port
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. Connector Port Guide

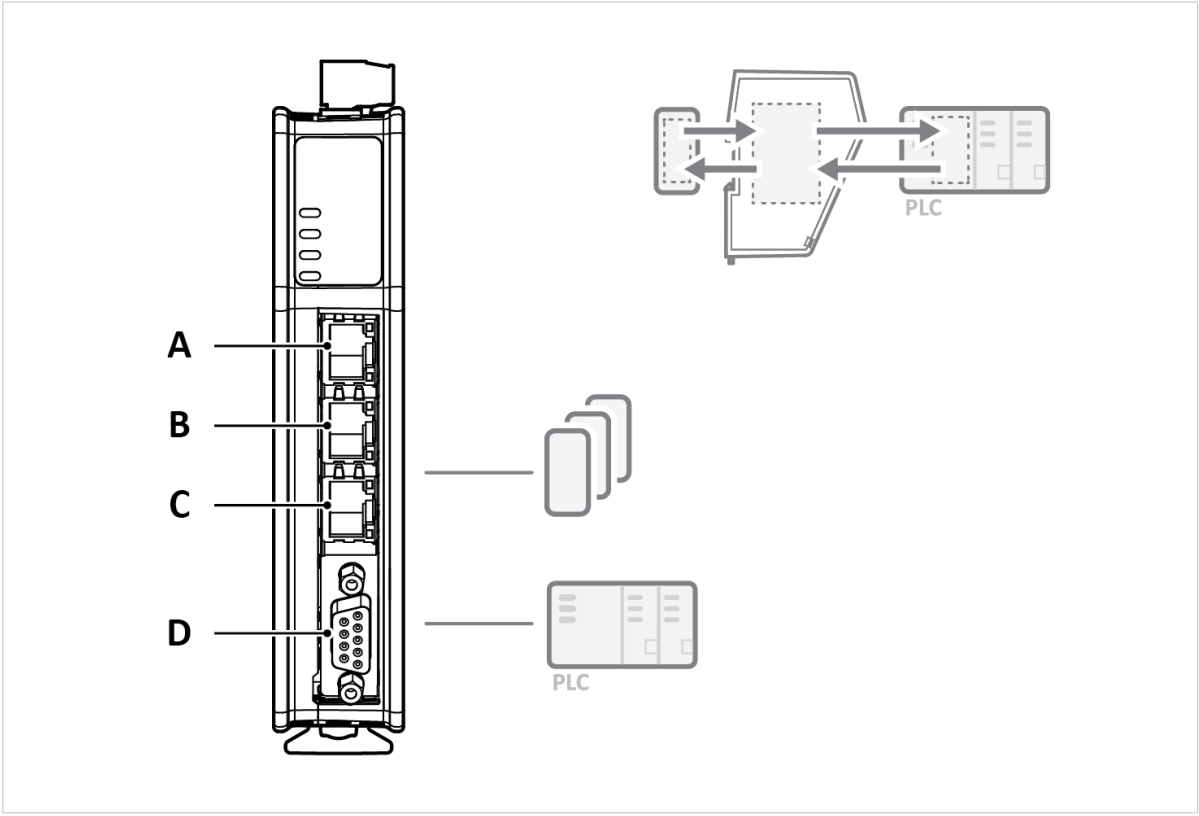


Figure 9. Communicator connector ports

Position	Port Number	Connector Type	Port Usage
A	X1	Ethernet	Configuration port
B	X2.1	Ethernet	Modbus TCP Client network
C	X2.2	Ethernet	
D	X3	D-sub	PROFIBUS network

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)

6.3. 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.

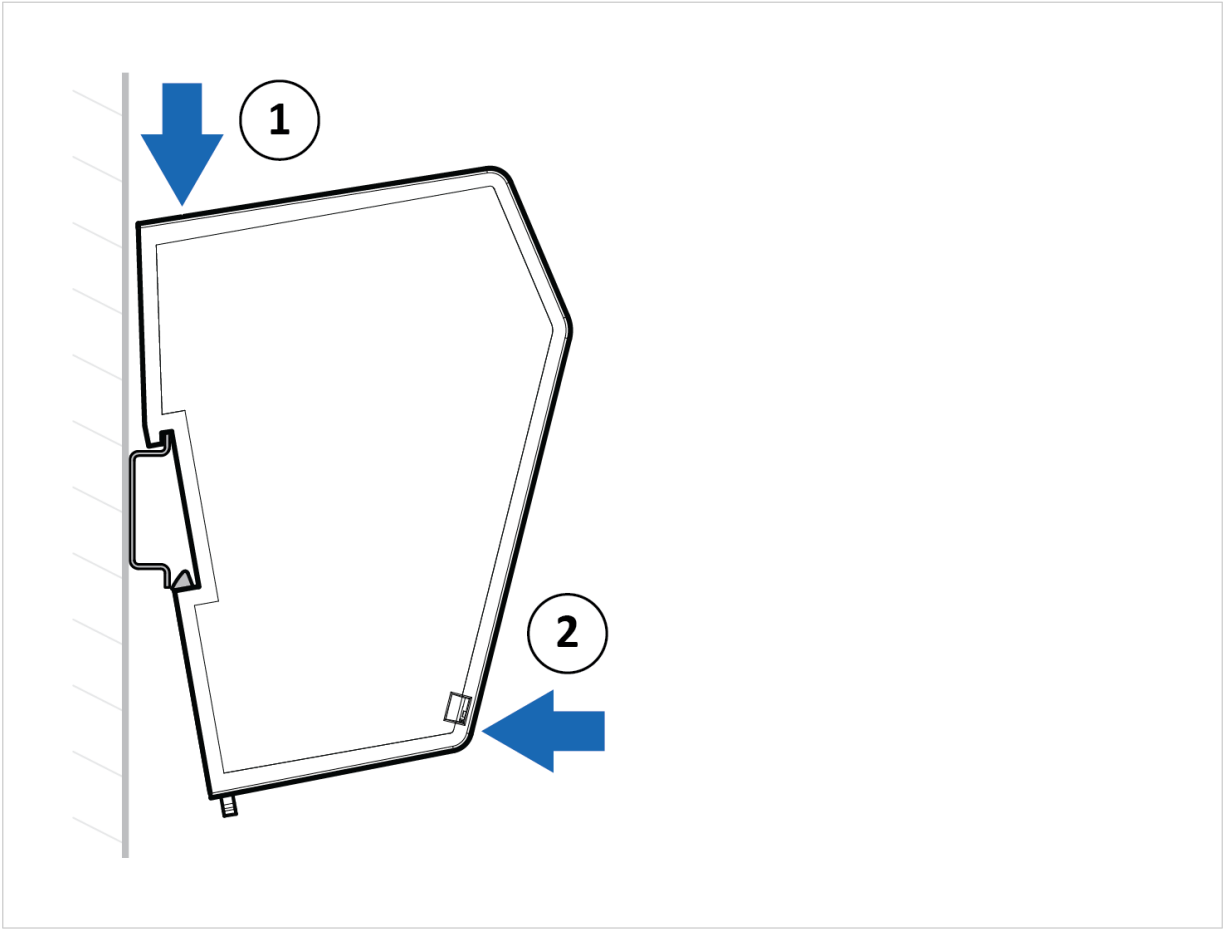


Figure 10. Attach the Communicator on the DIN rail

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.

6.4. Connect to Modbus TCP Client Network

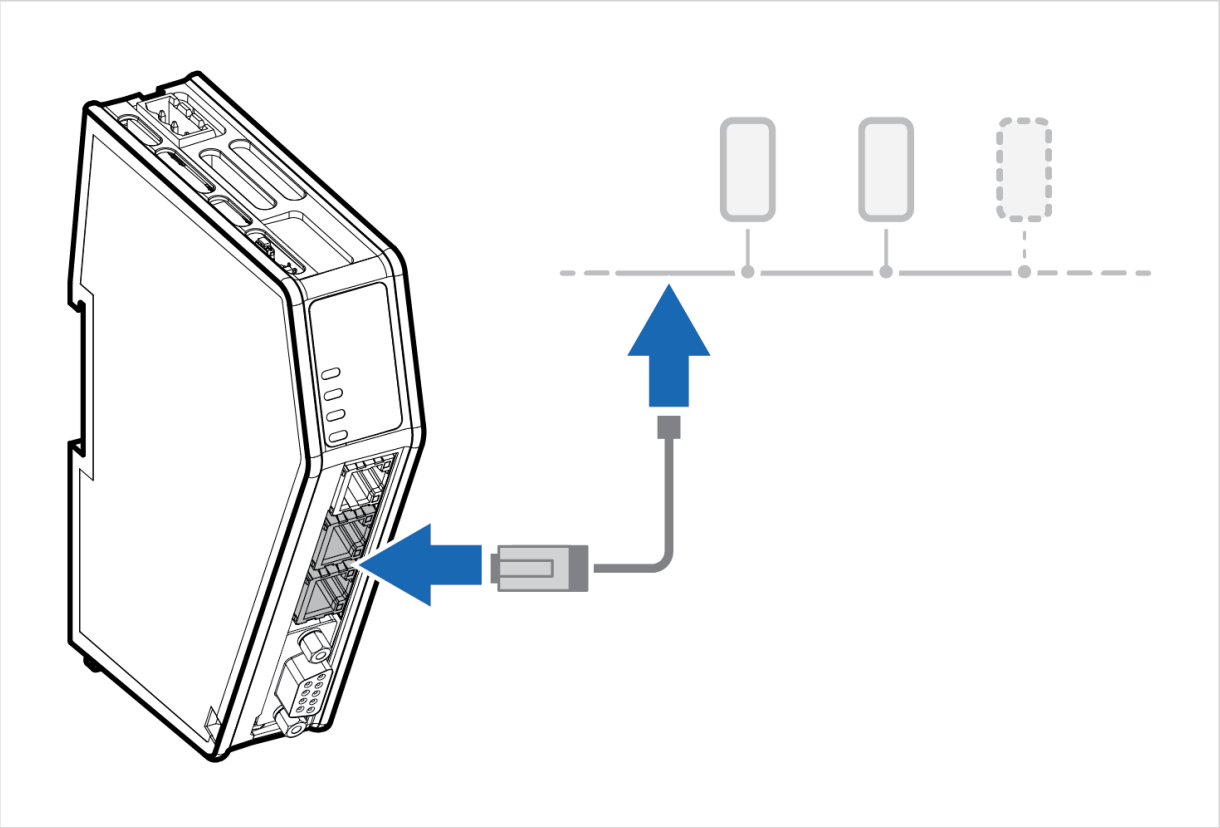
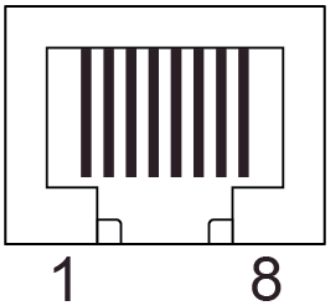


Figure 11. Connect to Modbus TCP Client network

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

Procedure

Connect the Communicator to your Modbus TCP Client network.

See Also

Connector Port Guide (Page 15)
Connect To PROFIBUS Network (Page 19)
Connect To Power (Page 25)

Communicator Status Monitor (Page 80)
Communicator LED Indicators (Page 82)
LED Status (Page 95)
Firmware Upgrade Error Management (Page 99)

6.5. Connect to PROFIBUS Network

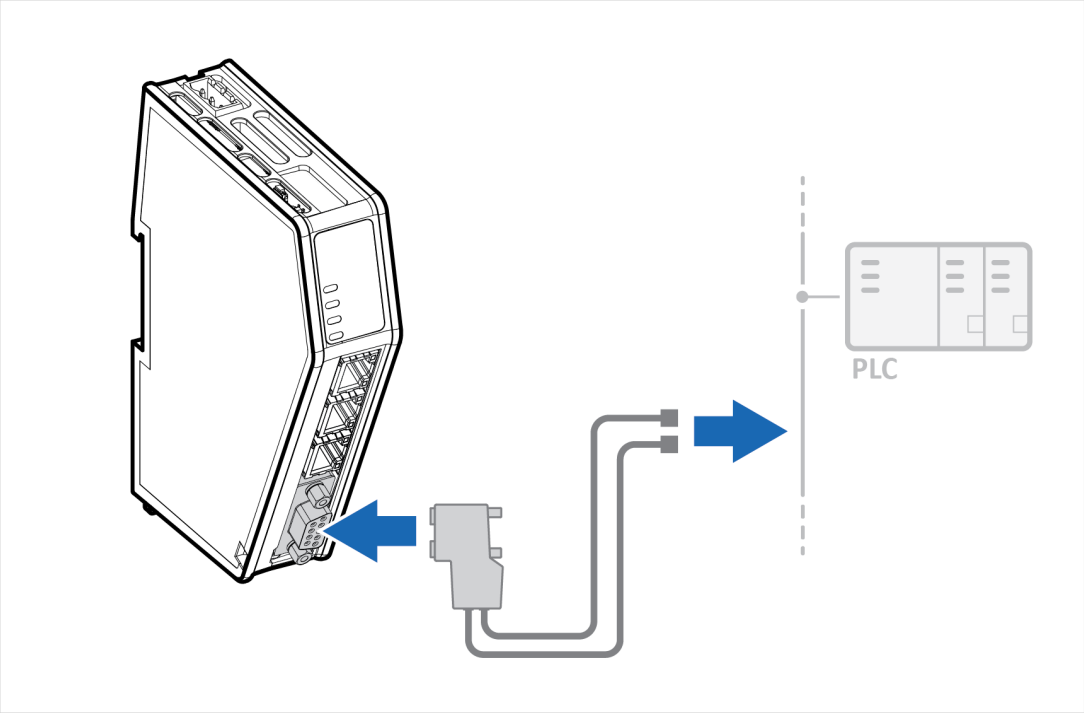
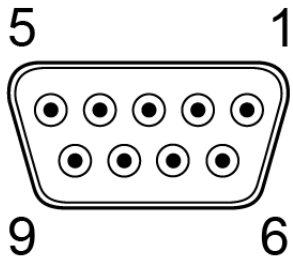


Figure 12. Connect to PROFIBUS network

PROFIBUS D-SUB Female Connector Pinout

PROFIBUS Connector	Pin	Description
	1	Not used
	2	Not used
	3	Line B
	4	RTS
	5	GND Bus
	6	+5 V Bus Out
	7	Not used
	8	Line A
	9	Not used
	Housing	PE

Procedure

Connect the Communicator to your PROFIBUS network.

See Also

Connector Port Guide (Page 15)
Connect To Modbus TCP Client Network (Page 17)
Connect To Power (Page 25)
Communicator Status Monitor (Page 80)
Communicator LED Indicators (Page 82)
LED Status (Page 95)
Firmware Upgrade Error Management (Page 99)

6.6. Rotary Switch Settings

6.6.1. Rotary Switches Default Setting

By default, the value on the three rotary switches are set to **000**.

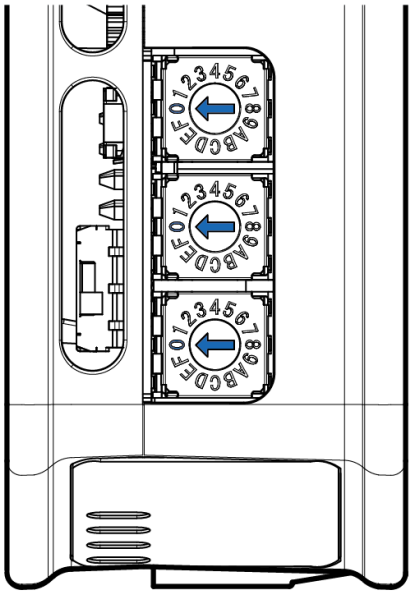


Figure 13. Rotary switches default setting **000**.

6.6.2. Set a Node Address with Rotary Switches

About the Rotary Switch Settings

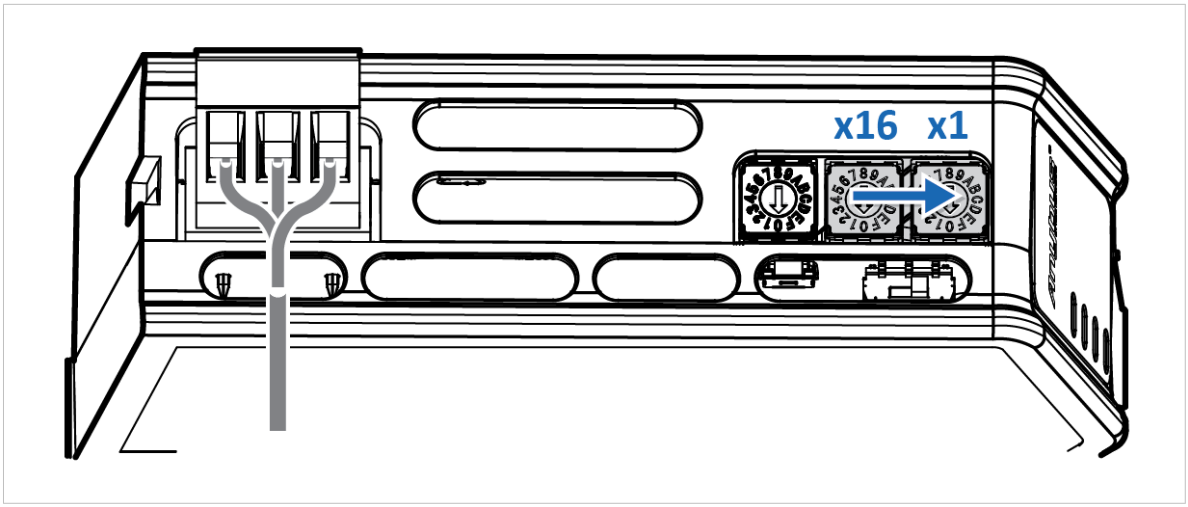
To set a node address for the PROFIBUS server, use the rotary switches located on the top front of the Communicator.

TIP

Use Windows Calculator (or similar application) to convert between hexadecimal (hex) and decimal (dec).

- When the node address setting is 000, you can sett the node address via the Communicator built-in web interface.
- Supports PROFIBUS node addresses 0-126 Dec (0-7E Hex).

- The default node address setting is 000.
- The node address values are set in hexadecimal (hex).
- Minimum value is 00.
- Each node address may only occur once in the network.
- The node address is read from the center rotary switch x16 to the front rotary switch x1.
- The rear rotary switch is not used, ensure that it is set to 0.



Before You Begin

Ensure that the Communicator is disconnected from power.

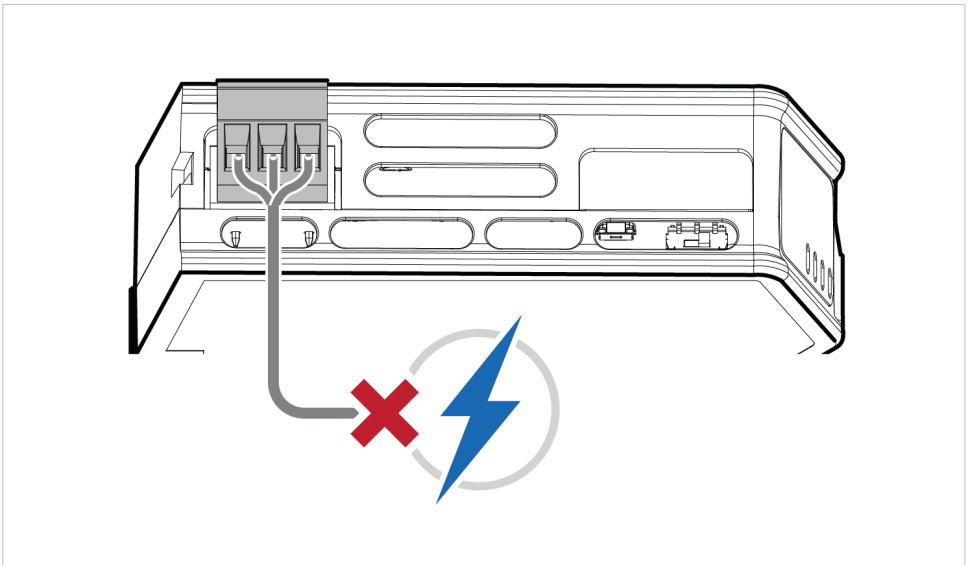
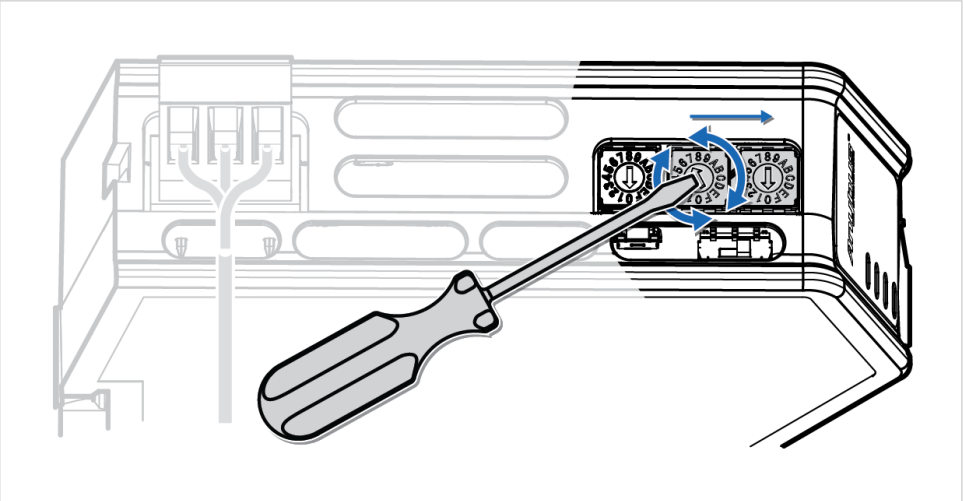


Figure 14. Disconnect Communicator from power

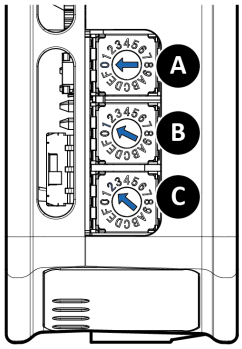
Procedure

Use a screwdriver to change the rotary switch position.

Ensure that the rotary switches engage correctly.



Example 1. To set the node address 12 hex = 18 dec

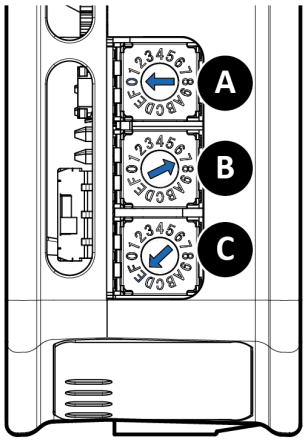


1. The rear rotary switch A is not used, ensure that it is set to 0.
2. Set the center rotary switch B to 1 hex.
3. Set the front rotary switch C to 2 hex.

The center rotary switch B 1 hex = 1 dec and the front rotary switch C 2 hex = 2 dec.

The node address expressed in decimal numbers is therefore 16 x 1 + 2 = 18.

Example 2. To set the node address 7E hex = 126 dec



- The rear rotary switch A is not used, ensure that it is set to 0.
- Set the center rotary switch B to 7.
- Set the front rotary switch C to E.

The center rotary switch B 7 hex = 7 dec and the front rotary switch C E hex = 14 dec.

The node address expressed in decimal numbers is therefore 16 x 7 + 14 = 126.

To Do Next

Connect the Communicator to power. See Connect to Power (page 25).

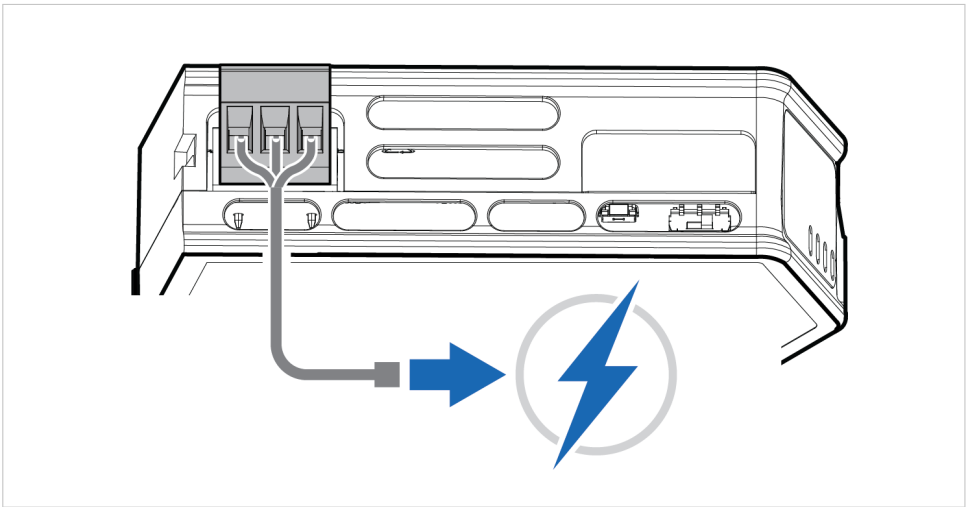


Figure 15. Connect Communicator to power

Result

The set node address is active as soon as the Communicator is powered on.

NOTE

Changing the address settings on the rotary switches during operation is ignored. For a new address to take effect, power cycle the Communicator.

See Also

PROFIBUS Address Settings (Page 54)

6.7. 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.

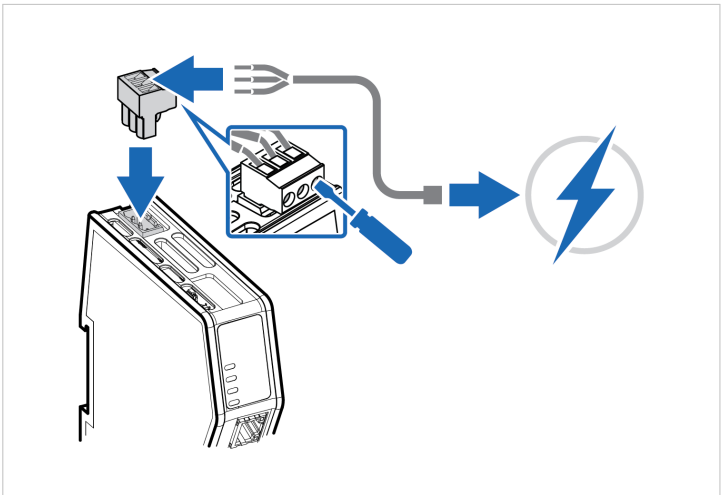
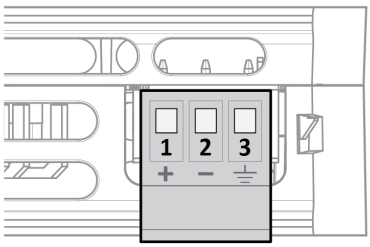


Figure 16. Connect to power

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.

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)
Communicator Status Monitor (Page 80)

Communicator LED Indicators (Page 82)
LED Status (Page 95)
Firmware Upgrade Error Management (Page 99)

6.8. 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

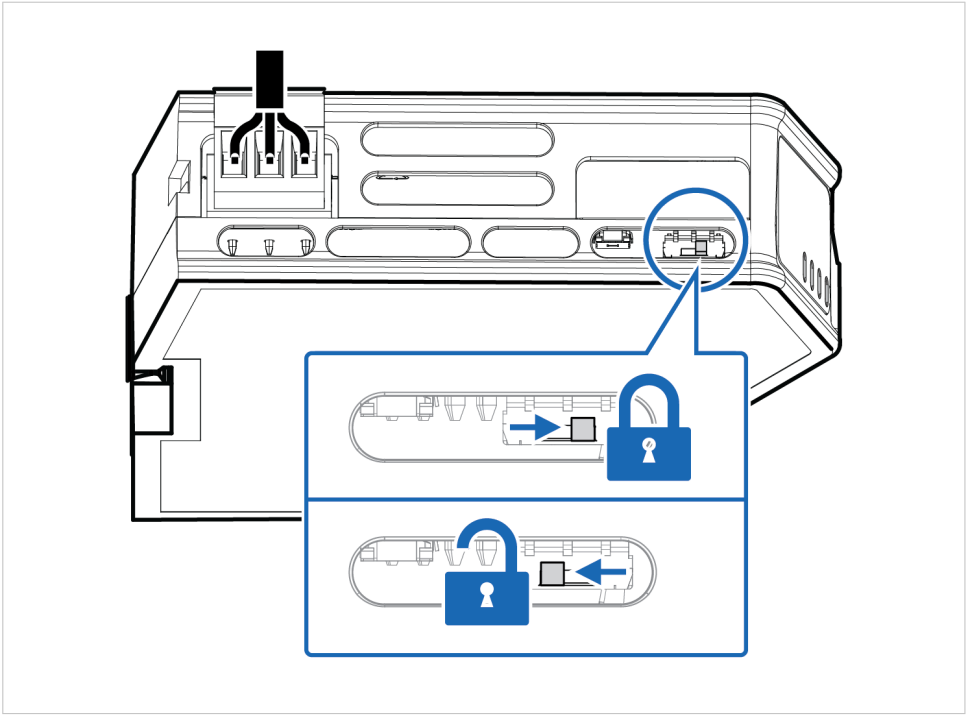


Figure 17. Security switch in locked and unlocked position

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

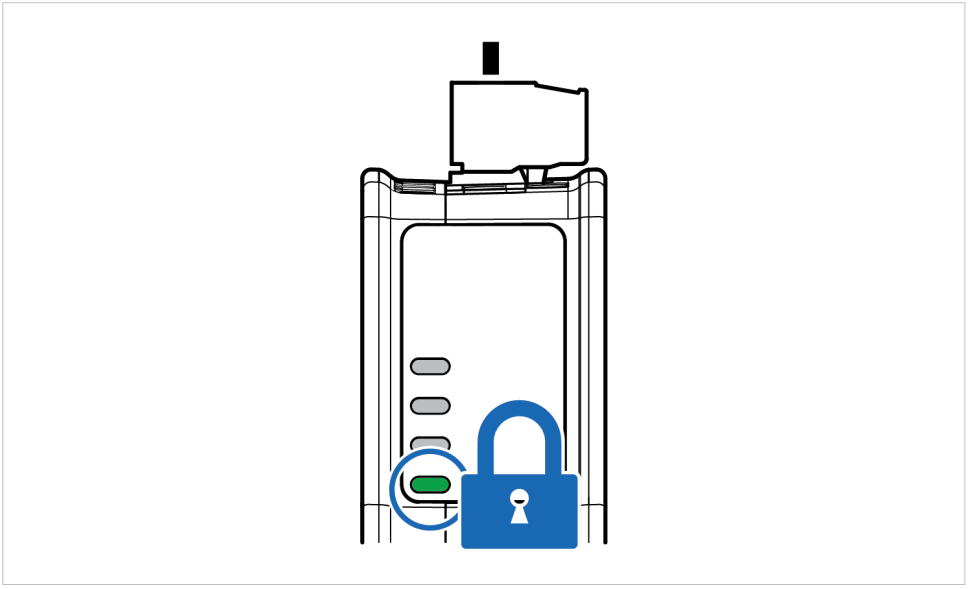


Figure 18. Security switch locked status LED

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.

6.9. Lock the Cables

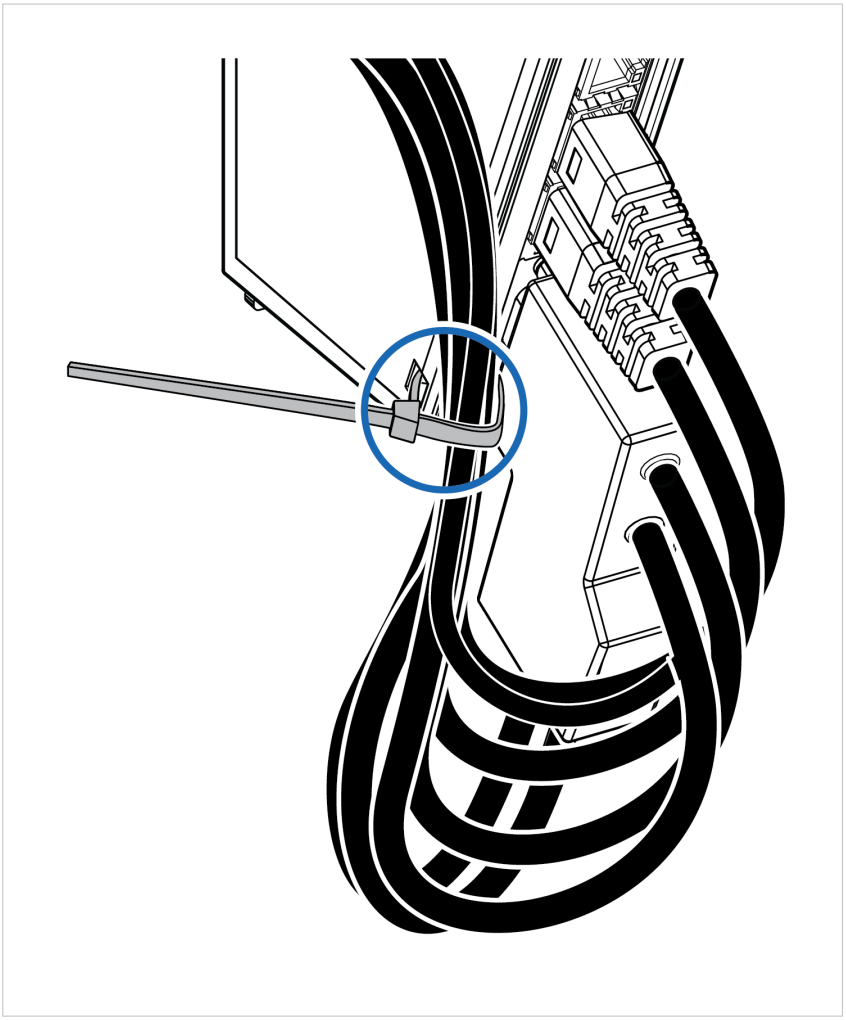


Figure 19. Lock the cables

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

6.10. 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:

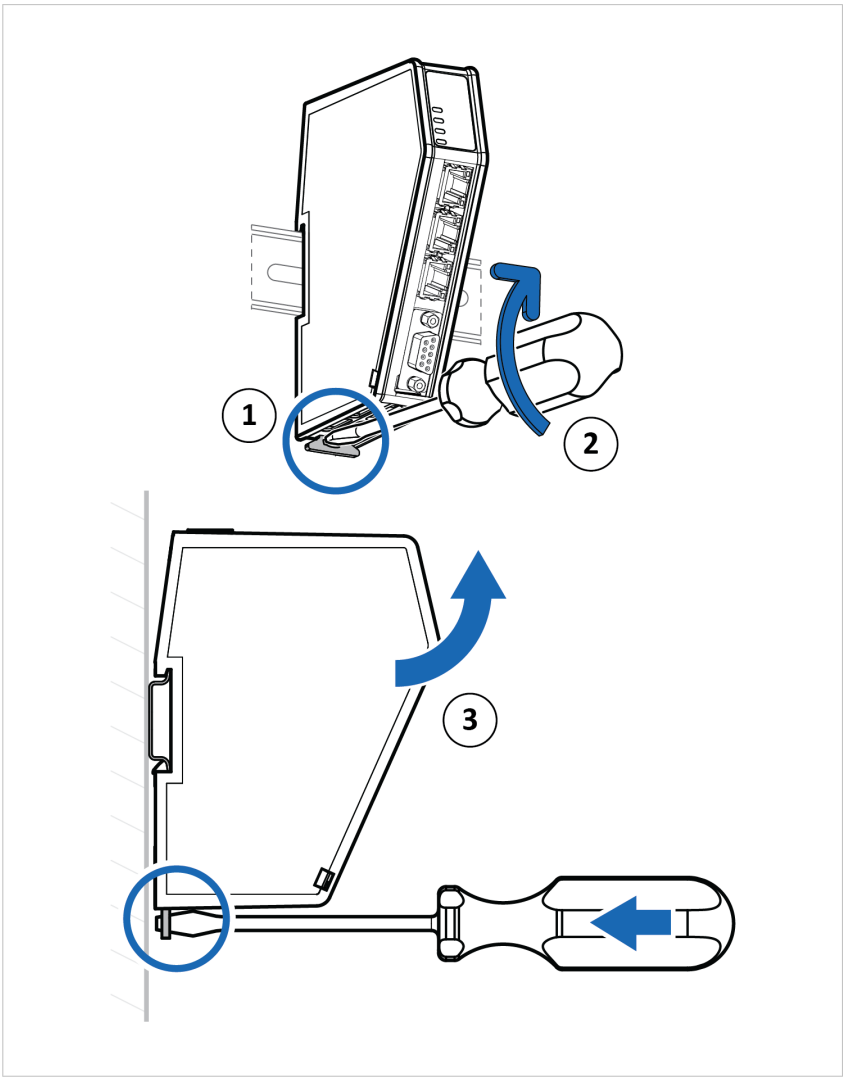


Figure 20. Unlock and unhook the Communicator

1. Insert the screwdriver into the Communicator DIN rail locking mechanism.
2. To unlock the Communicator DIN rail locking mechanism, turn the screwdriver clockwise.
3. Hold the screwdriver in the DIN rail locking mechanism while you unhook the Communicator from the DIN rail.

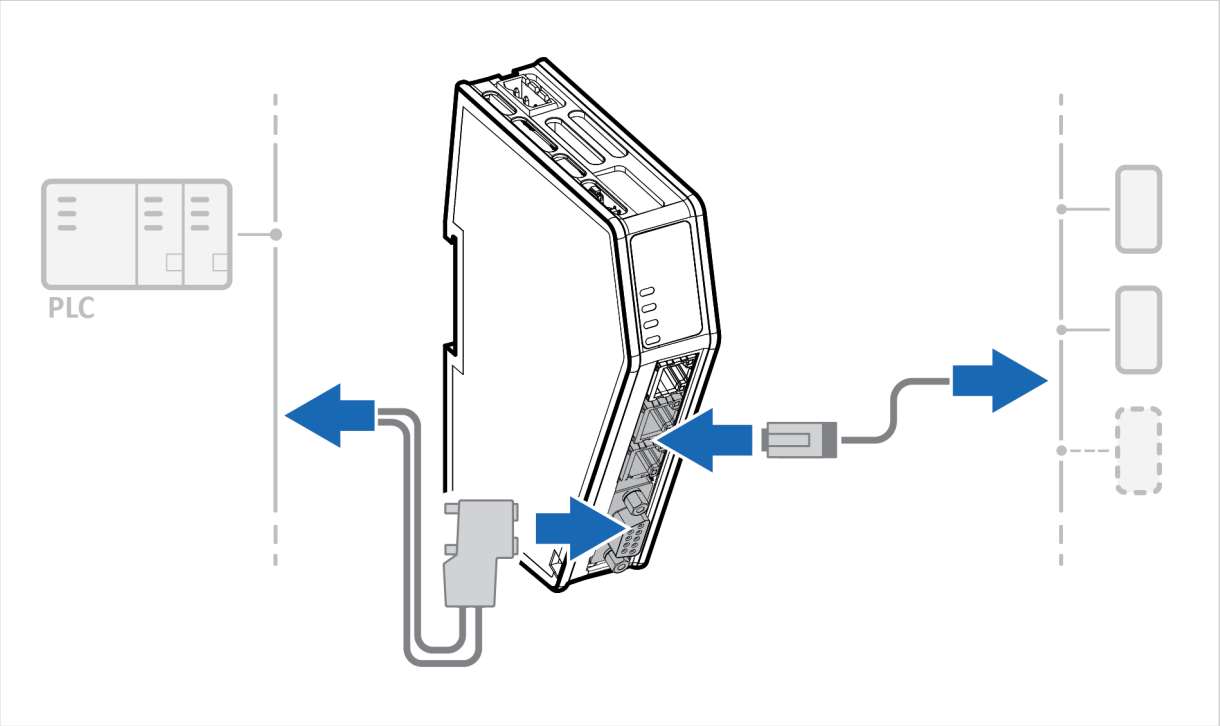
7. Configuration Quick Guide

This section is intended to give you a brief overview of the tasks you need to perform to configure the Communicator.

For detailed information, please refer to Communicator Configuration (page 41) .

7.1. Prepare Configuration

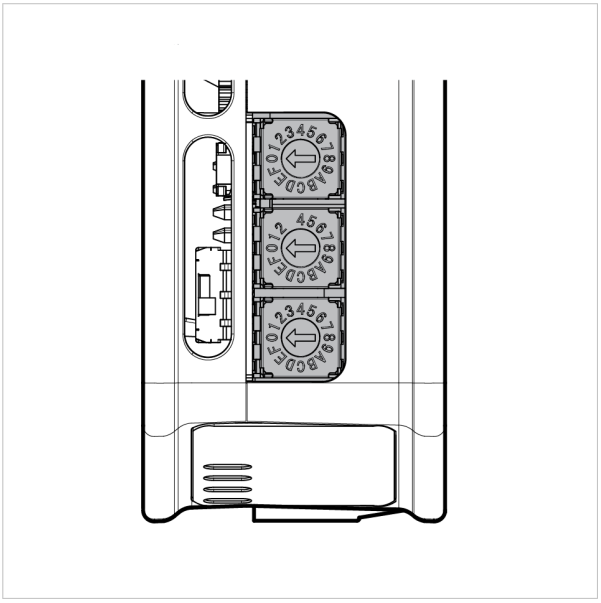
Connect to Networks



1. Connect the Communicator to the Modbus TCP Client network.
2. Connect Communicator to the PROFIBUS network.

Rotary Switch Settings

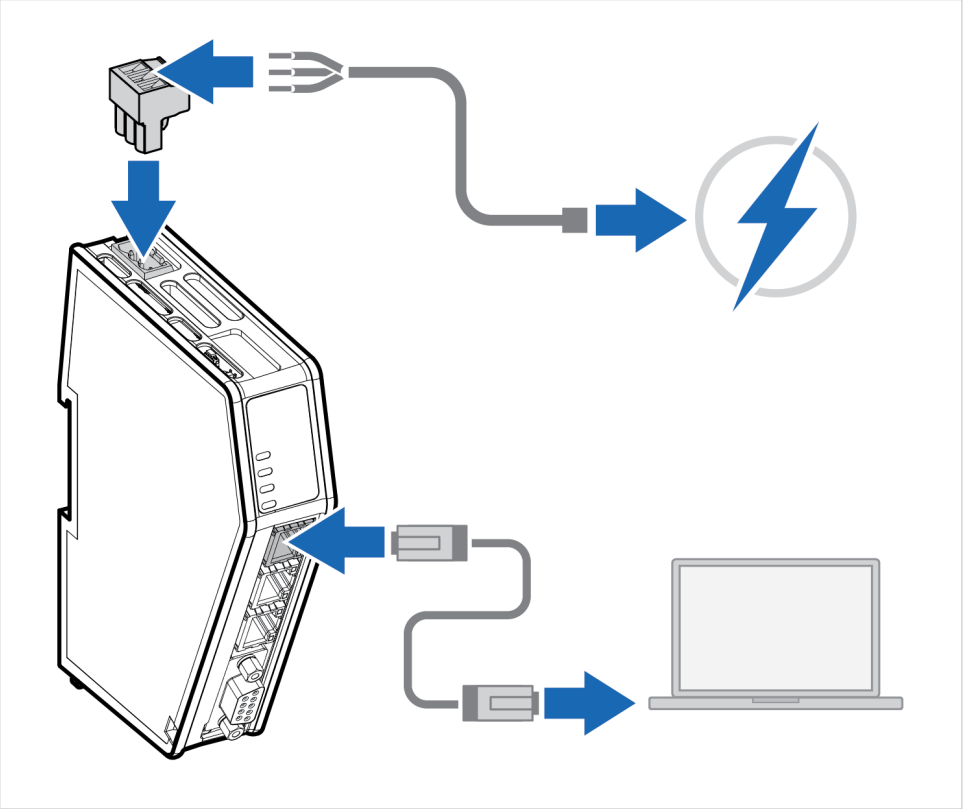
Set the desired PROFIBUS address on the Rotary Switches.



The default setting is 0.

For more info see Rotary Switch Settings (page 20).

Connect to PC and Power



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

Access the Built-In Web Interface

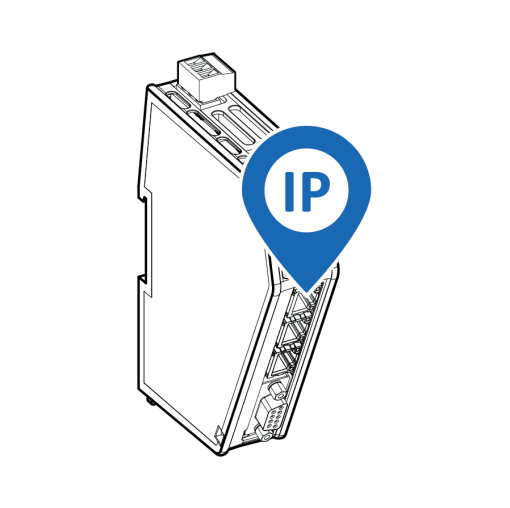
1. Find the Communicator on your PC

> **NOTE**
> The Communicator default IP address is 192.168.0.10.

Option 1 | Static IP Address

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.

Option 2 | Configuration Port IP Address

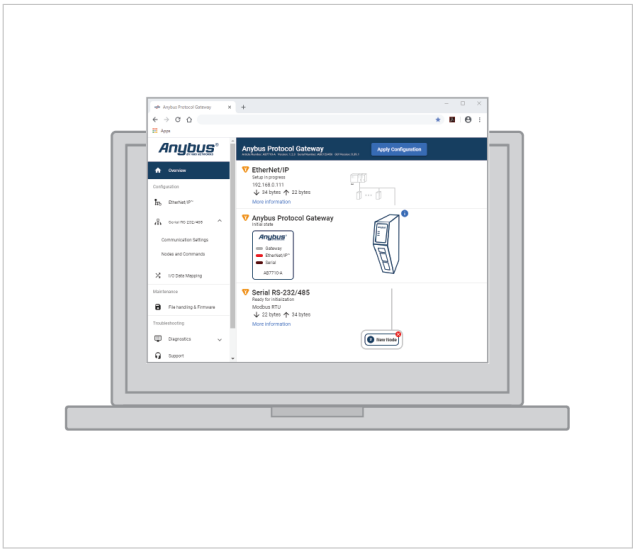


Change the IP address on the Communicator configuration port to one within the same IP address range as your PC.

Use the software application HMS IPconfig to find the Communicator default IP address on your PC.

Download the installation files and user documentation from www.hms-networks.com/technical-support.

2. Access the Communicator built-in web interface



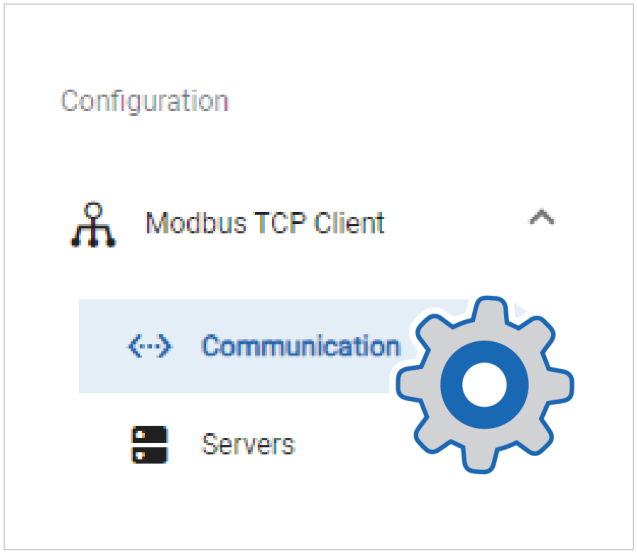
Open the Communicator built-in web interface in HMS IPconfig or enter the Communicator IP address in your web browser.

The Communicator built-in web interface overview page opens in your browser.

7.2. Setup New Configuration

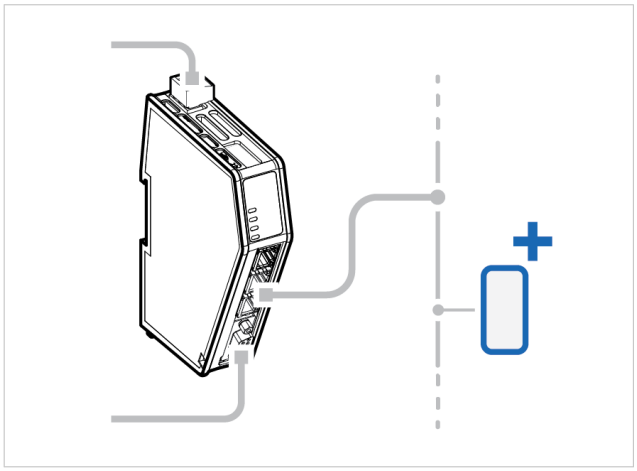
Follow these steps to setup a new Communicator configuration.

1. **Subnetwork configuration**



On the **Communication** page: Enable DHCP or configure the IP settings manually.

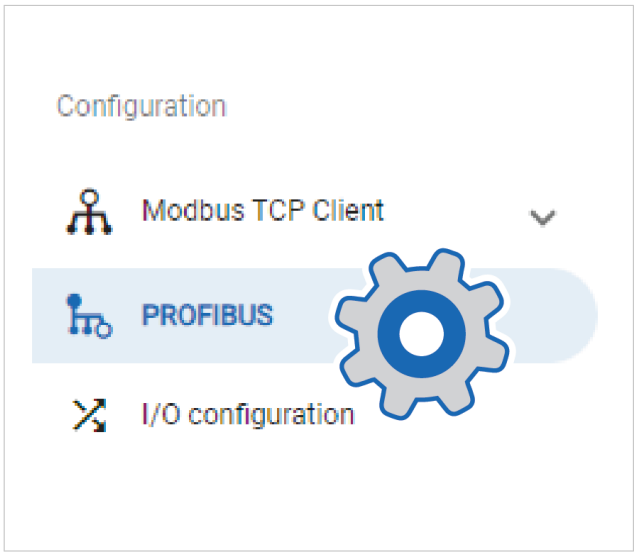
2. **Add Servers**



On the **Servers** page:

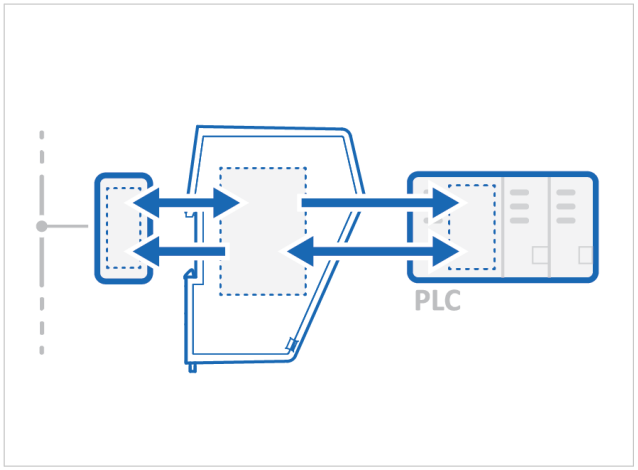
a. Add a server and configure the server **Properties**.
b. Add transaction(s) to the server and configure the **Transaction properties**.
c. Repeat until you have added and configured all your servers.

3. **High level network configuration**



On the **PROFIBUS** page:
If the rotary switches are set to 0, enter the PROFIBUS address of the Communicator.

4. **I/O Configuration**



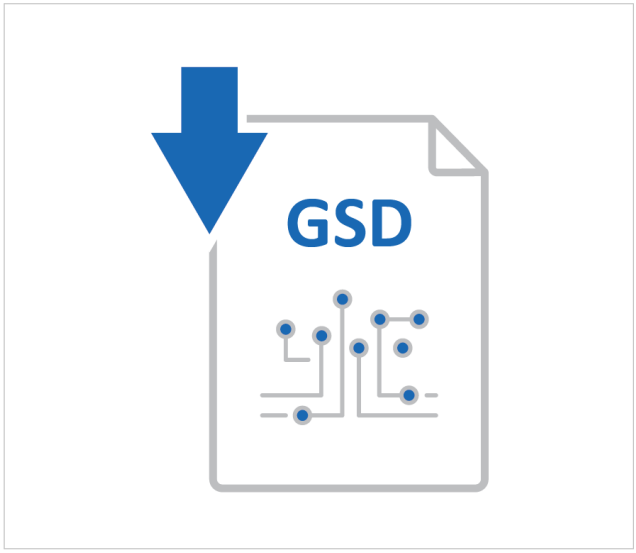
The transaction(s) for each server is automatically mapped to the Communicator internal memory area.

On the **I/O configuration** page, view the mapping relation between the server connections and the layout on the process data area.

7.3. PLC Configuration

In the In the Communicator Built-In Web Interface

- Download GSD File

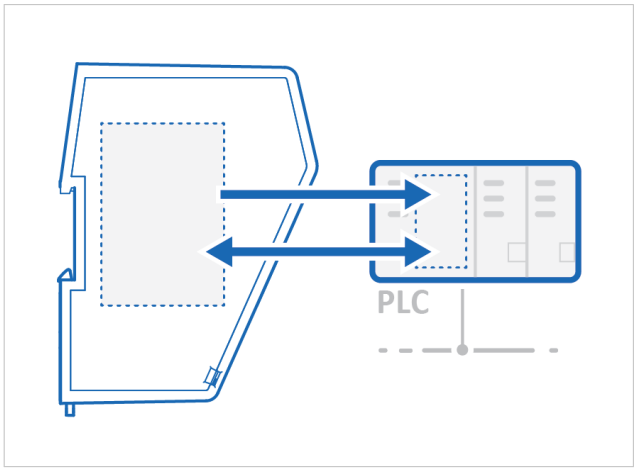


Optional if the PLC program requires an GSD (General Station Description) file.

On the **PROFBUS** page: Download the GSD file to your PC.

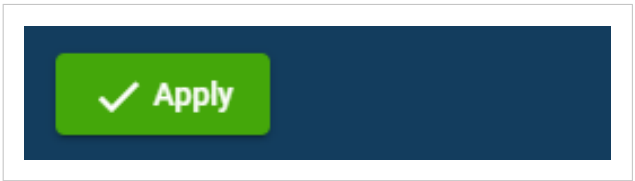
In the PLC Program

1. Optional if the PLC program requires an GSD (General Station Description) file.
   Import the GSD file into your PLC project.
2. Configure the PLC to communicate with the Communicator according to the I/O data map created in the Communicator.



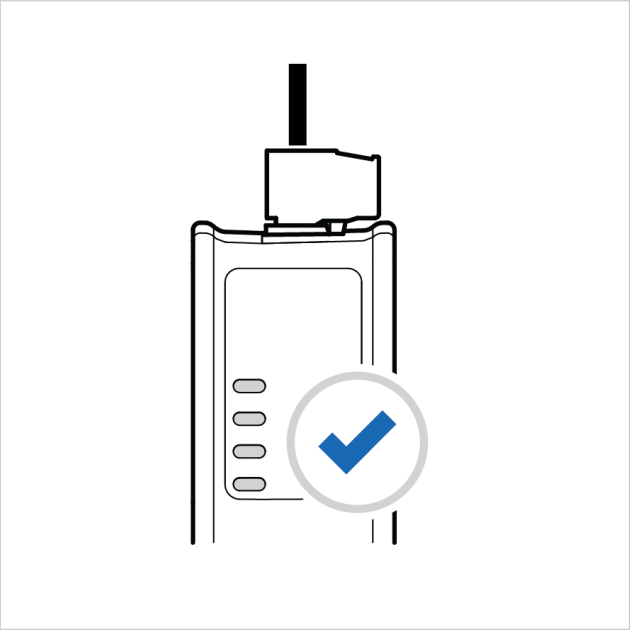
7.4. Verify Operation

1. **Apply the configuration**



When you have completed and verified the configuration, click **Apply** for the settings to take effect.

2. **Verify status and LED indications**



On the **Home** page:
Monitor the Communicator, network and server status.
You can also view the Communicator LED indications remotely.

3. **Verify and monitor communication**

In **Diagnostics**, use the:

- **I/O data** page to monitor how the data flow between the **Modbus TCP Client** side and the **PROFIBUS** side, including any configured endian conversions.
- **Event log** page to detect failures and unexpected behavior over time.

8. Communicator Configuration

This section is intended to give you detailed information about the tasks you need to perform to setup a new Communicator configure.

For a more brief overview of the configuration steps, please refer to the Configuration Quick Guide (page 31).

8.1. Connect to Configure the Communicator

Procedure

1. Connect the Communicator to your networks, Modbus TCP Client and PROFIBUS.

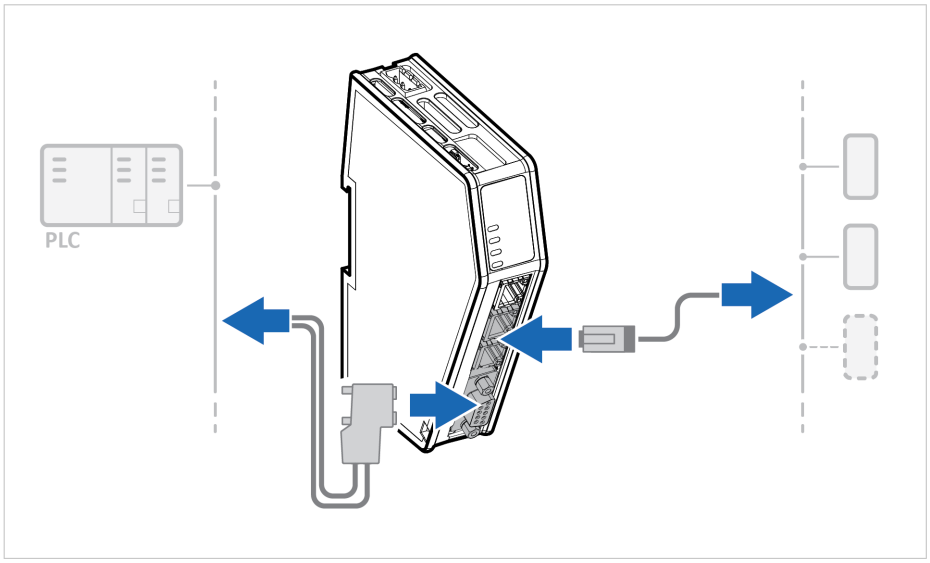


Figure 21. Connect to networks

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

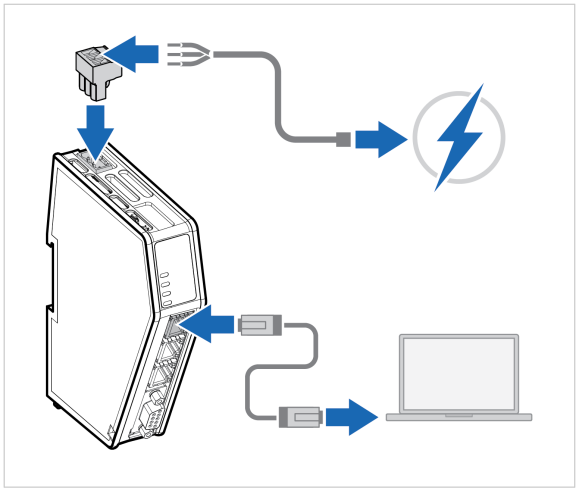


Figure 22. Connect to PC and power

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

Before You Begin

Security Settings

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

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.

IP Address

NOTE
The Communicator default IP address is 192.168.0.10.

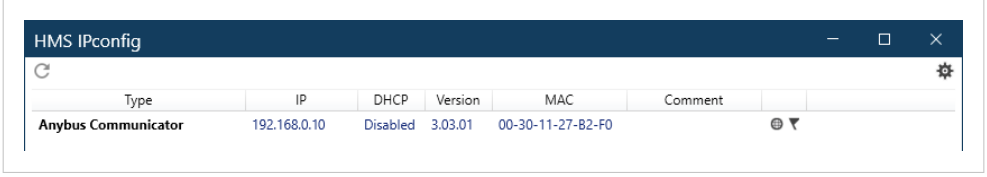
TIP
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System** > **Configuration port** page.

Download HMS IPconfig Installation Files

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

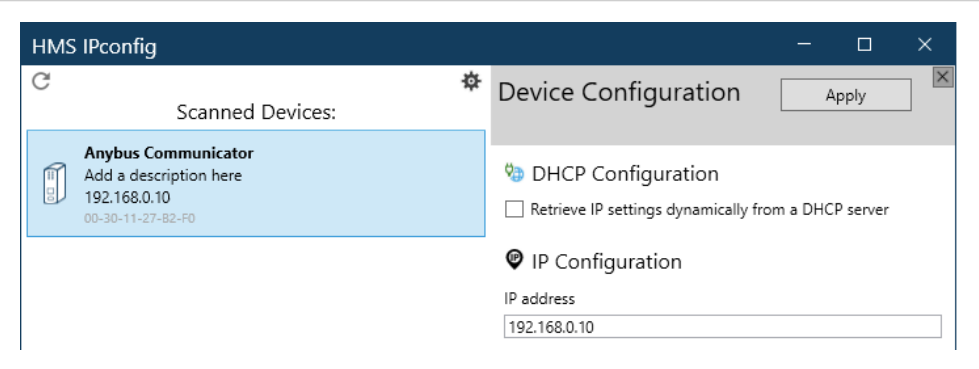
Procedure

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

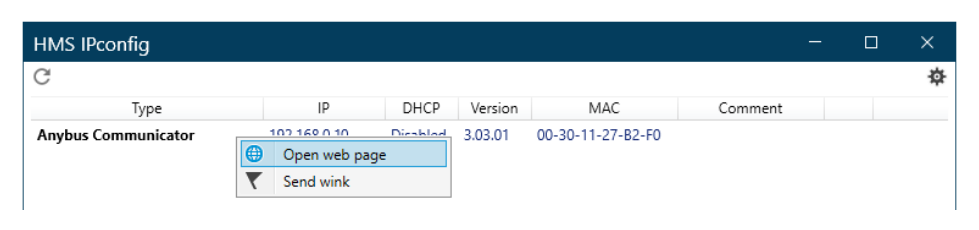


   - HMS IPconfig automatically starts scanning for compatible and active HMS devices.
   - Found HMS devices are added to the device list.
3. To open the settings pane, click on the Communicator in the device list.

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

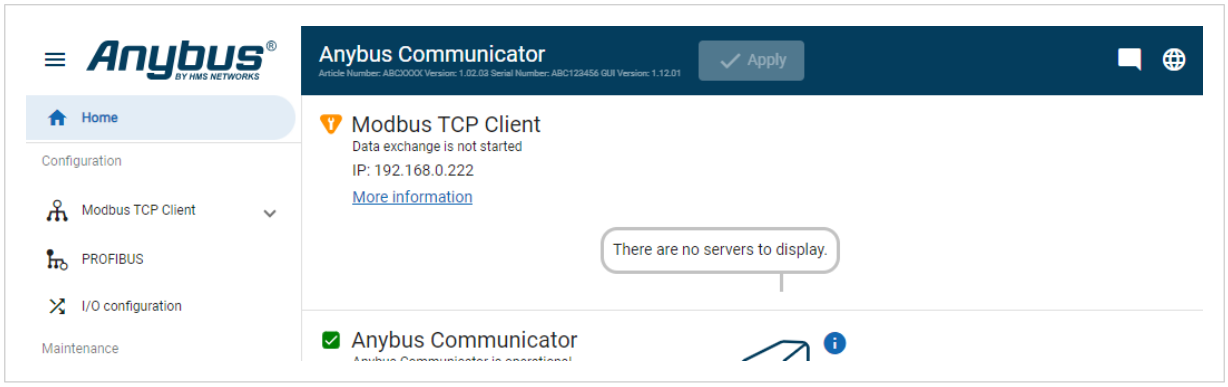


5. To open the **Open web page** built-in web interface, click Communicator.



Result

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



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

Before You Begin

Security Settings

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

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.

IP Address

NOTE
The Communicator configuration port default IP address is 192.168.0.10.

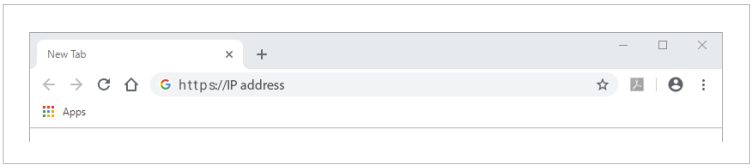
NOTE
When you change to a static IP address on your computer, internet access may be lost.

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.

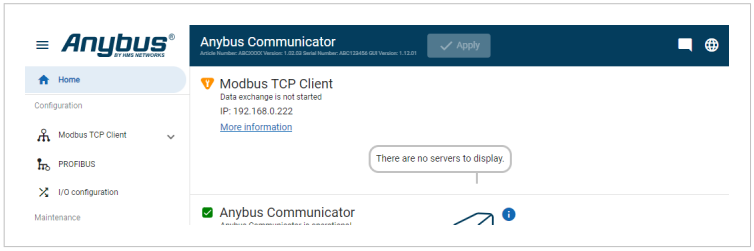
Procedure

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**.



8.4. Communicator Built-In Web Interface Overview

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

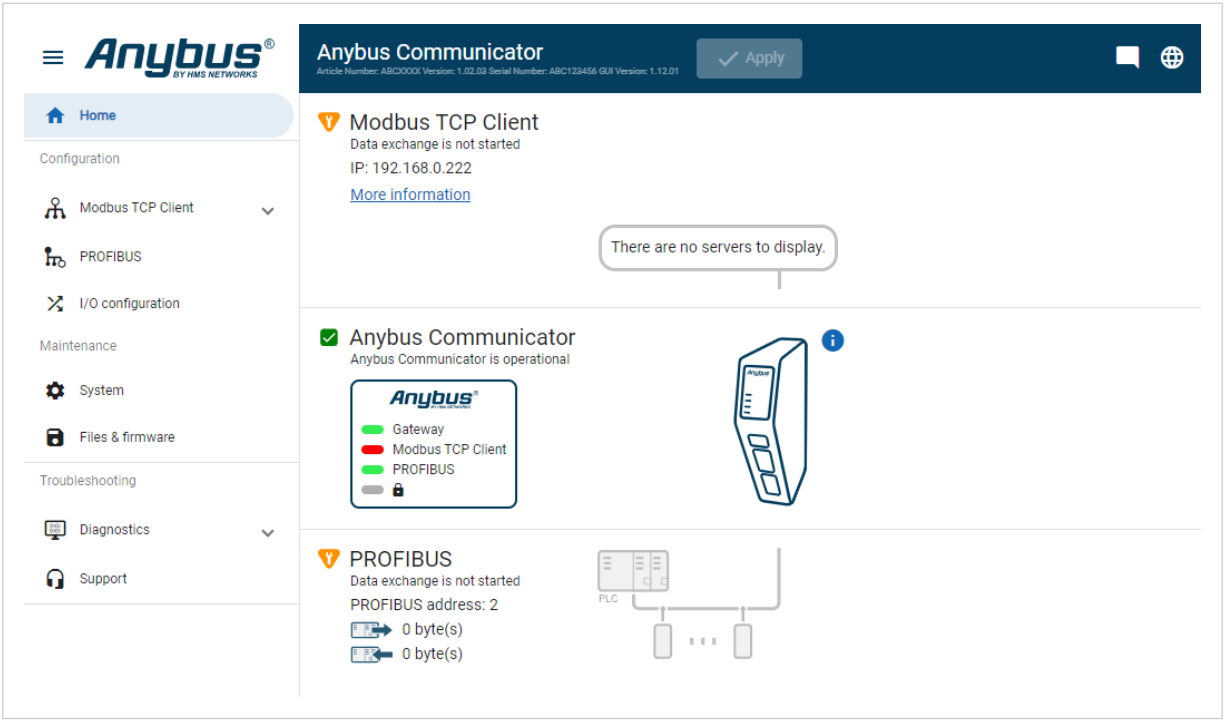


Figure 23. The Communicator built-in web interface Home page

Menu item	Description
Home	View the Communicator, network and adapter(s) status.
Apply	After configuration changes are made and verified, press Apply to make the settings take effect.
Modbus TCP Client	Modbus TCP Client subnetwork with server(s). Configure communication and add servers and transactions.
PROFIBUS	Configure the network settings for the PROFIBUS network.
I/O configuration	View the connections mapped to the Communicator internal memory area.
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.

8.5. Modbus TCP Client Communication Settings

Configure the Modbus TCP Client communication settings.

8.5.1. IP Settings

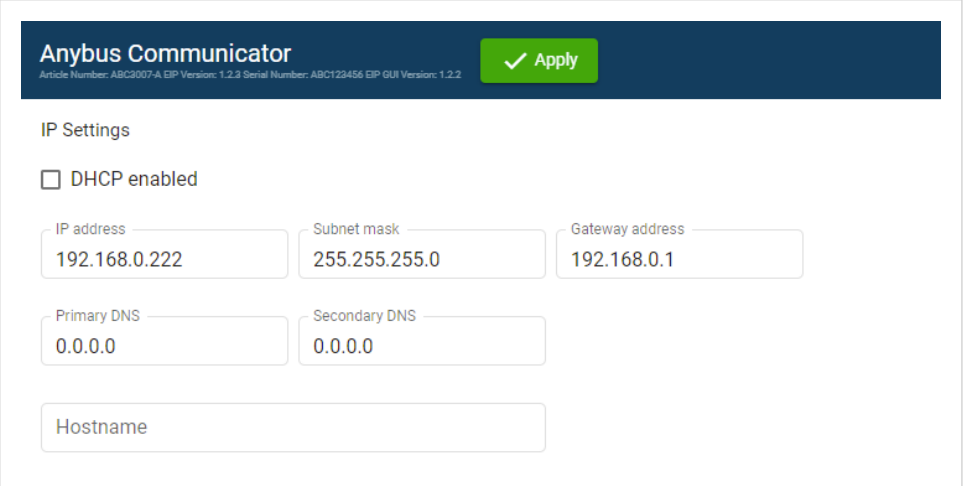


Figure 24. IP Settings

By default, DHCP is Enabled.

Default IP Settings

The Communicator comes with the following factory default IP settings:

Setting	Default value	Description
DHCP	Enabled	DHCP (Dynamic Host Configuration Protocol) automatically gives devices on a network the IP settings they need to connect and communicate.
IP address	There is no default IP address.	The EtherNet/IP network IP address in IPv4 dot-decimal notation.
Subnet mask	There is no default Subnet mask.	The EtherNet/IP network Subnet mask in IPv4 dot-decimal notation.
Gateway address	There is no default Gateway address.	The EtherNet/IP 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 server	There is no default Primary DNS server.	The EtherNet/IP network Primary DNS in IPv4 dot-decimal notation.
Secondary DNS server	There is no default Secondary DNS server.	The EtherNet/IP network Secondary DNS in IPv4 dot-decimal notation.

Using DHCP Server for IP Configuration

Procedure

With DHCP enabled, the IP settings are provided by the high level network DHCP server.

Ensure the **DHCP enabled** checkbox is selected.

To Configure IP Settings Manually

Procedure

1. To disable DHCP, deselect the **DHCP enabled** checkbox.
2. Then, enter the desired IP settings values.

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.

8.6. Modbus TCP Client Servers

8.6.1. Add Server

Before You Begin

NOTE
The maximum number of servers that can be added is 64.

Procedure

1. In the web-interface left sidebar menu, click **Servers**.
2. Click **Add**.
   A new server is added to the **Modbus TCP Client** server list.

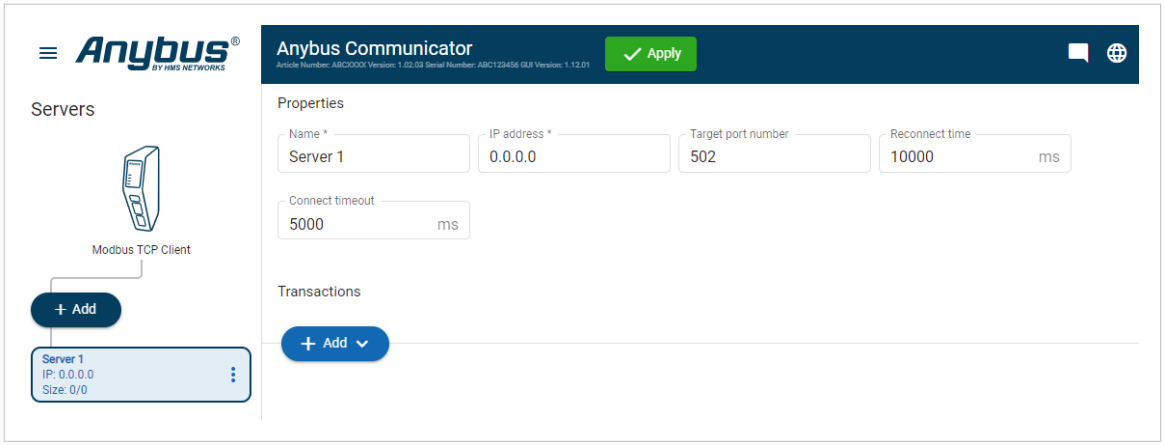


Figure 25. Modbus TCP Client, Server page

3. Repeat until you have added all your servers.

To Do Next

Configure the server Properties, see Server Properties (page 48).

8.6.2. Server Properties

Procedure

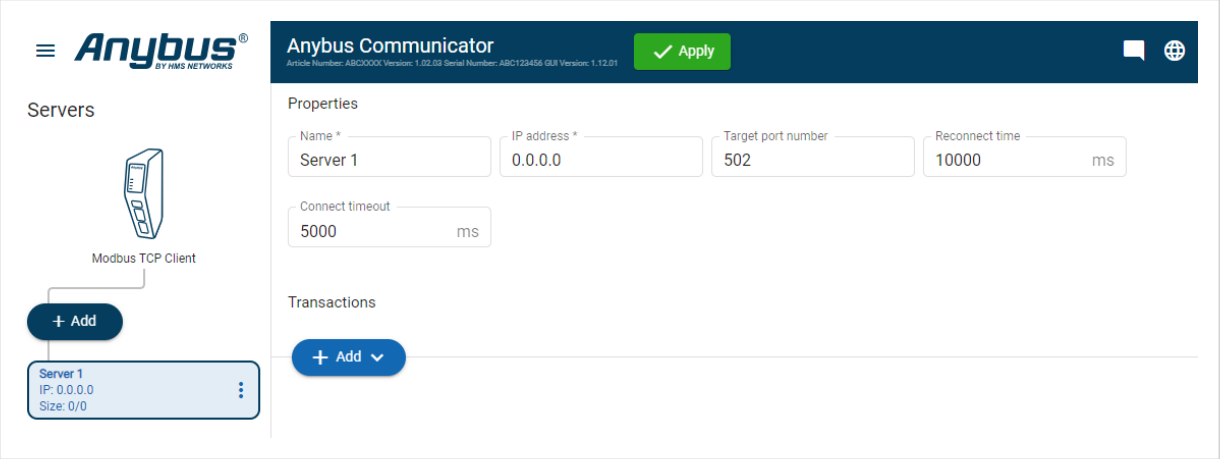


Figure 26. Servers page, Properties

1. In the server list, select a server to configure.
2. Configure the **Properties**.

Setting	Value	Description
Name	Server [n]	The default name is Server, followed by an incremental number suffix.
IP address	Default 0.0.0.0	The server IP address in IPv4 dot-decimal notation
Reconnect time	0 ms to 4294967295 ms Default 1000 ms	Specify for how long the Communicator should wait before attempting to reconnect, if the server is disconnected.
Connect timeout	0 ms to 4294967295 ms Default 5000 ms	Specify the period in which the Communicator should establish a connection with the server.
Target port number	0 to 65535 Default Modbus TCP port 502	Modbus TCP port of the target device. If the server requires it, it is possible to change.

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

To Do Next

Add Transactions, Add Transactions (page 49).

8.6.3. Add Transactions

Before You Begin

NOTE
The transactions are executed in the order they appear in the **Server Transaction** list.

NOTE
One transaction is performed at a time per connection.

NOTE
You can add a maximum of 152 transaction units distributed among the servers.

For Modbus TCP, it is possible to map up to 1500 bytes of data in either direction, including data exchange control and live list.

Procedure

1. In the **Modbus TCP Client** server list, select a server to configure.
2. Click **Add** and select a transaction from the list of standard Modbus transactions.

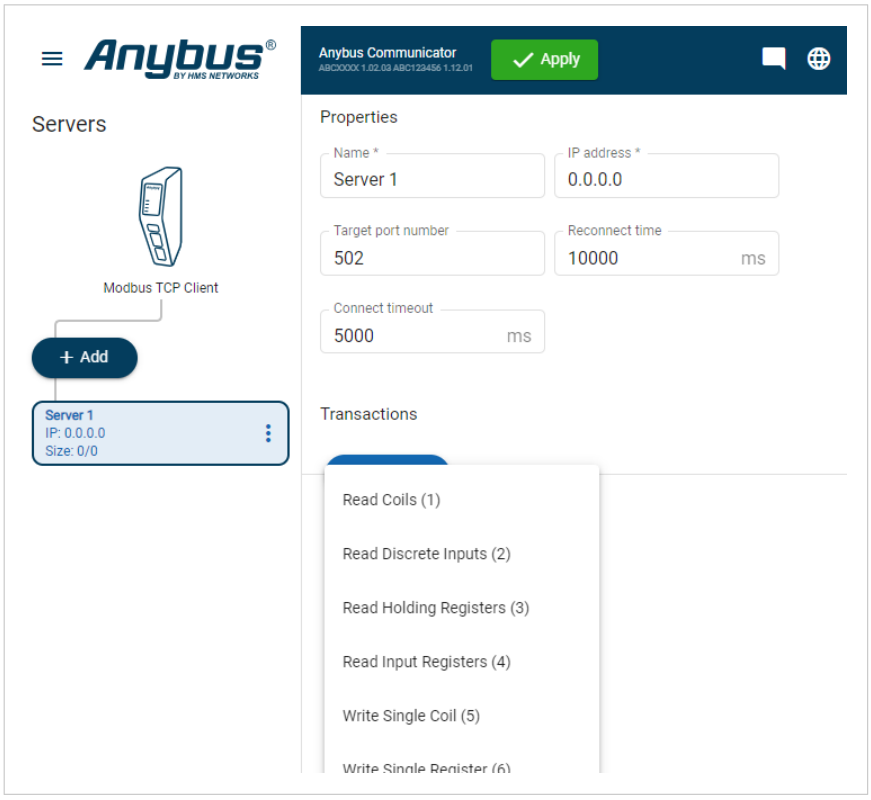


Figure 27. Add Modbus transactions

3. Repeat until you have added all your transactions.

To Do Next

Configure the transaction Properties settings, Transaction Properties (page 51).

8.6.4. Modbus Function Codes

Reference: MODBUS Application Protocol Specification V1.1b3, April 26 2012

For more information refer to the Modbus organization website.

Nr	Function	Area	Function Code	Description
1	Read Coils	Coils	0x01	Read from 1 to 2000 contiguous status of coils in a remote device.
2	Read Discrete Inputs	Discrete inputs	0x02	Read from 1 to 2000 contiguous status of discrete inputs in a remote device.
3	Read Holding Registers	Holding registers	0x03	Read the contents of a contiguous block of holding registers in a remote device.
4	Read Input Registers	Input registers	0x04	Read from 1 to 125 contiguous input registers in a remote device.
5	Write Single Coil	Coils	0x05	Write a single output to ON or OFF in a remote device.
6	Write Single Register	Holding registers	0x06	Write a single holding register in a remote device.
15	Write Multiple Coils	Coils	0x0F	In a sequence of coils, force each coil to either ON or OFF in a remote device.
16	Write Multiple Registers	Holding registers	0x10	Write a block of contiguous registers in a remote device.
23	Read/Write Multiple Registers	Holding registers	0x17	Performs a combination of one read operation and one write operation. The write operation is performed before the read.

8.6.5. Transaction Properties

Before You Begin

For Modbus transaction reference guide, refer to Modbus Function Codes (page 50).

Procedure

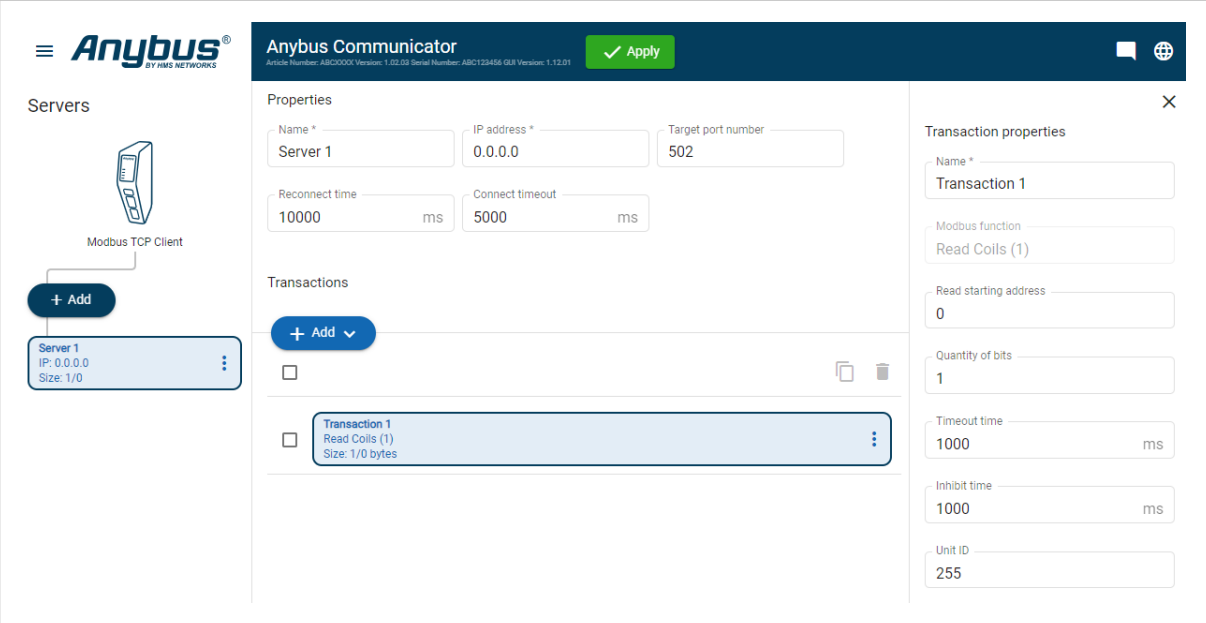


Figure 28. Transaction properties

1. In the **Modbus TCP Client** server list, select a server to configure.
2. In the **Transactions** list, select a transaction to configure.
   The **Transaction properties** sidebar opens, on the right side of the screen.
3. Enter a transaction **Name**.
   By default, the transaction is assigned the name Transaction, followed by an incremental number suffix.
4. Configure the **Transaction properties**.

Setting	Value	Setting for Modbus Transaction	Description
Name	Transaction [n]	Applicable for all.	You can name the transaction to make it easier to identify. The default name is Transaction, followed by an incremental number suffix.
Read starting address	0 to 65 535	Read Coils (1) Read Discrete Inputs (2) Read Holding Registers (3) Read Input Registers (4) Read Write Multiple Registers (23)	Specify the start address for the read/write transaction. The address acts as an address to the data position, where the data is read from or written to. Modbus holding register addresses starts at 0. Modbus address 0 = Register 1
Write starting address	0 to 65 535	Write Single Coil (5) Write Single Register (6) Write Multiple Coil (15) Write Multiple Registers (16) Read Write Multiple Registers (23)	
Quantity to read	1 to 125	Read Holding Registers (3) Read Input Registers (4) Read Write Multiple Registers (23)	Specifies the number of registers to read to follow in the read data field.

Setting	Value	Setting for Modbus Transaction	Description
Quantity to write	Write Multiple Registers (16), 1 to 123 Read Write Multiple Registers (23), 1 to 121		Specifies the quantity of registers to follow in the write data field.
Quantity of bits	Read Coils (1), 1 to 2000 Read Discrete Inputs (2), 1 to 2000 Write Multiple Coils (15), 1 to 1968 Default: 1		Specify the number of coils to follow in the read/write data field.
Unit ID	0 to 255 Default: 255	Applicable for all.	Specifies the unit identifier of the server device.
Timeout time	0 to 65 535 ms	Applicable for all.	Specify the period within which the server must return a response to the transaction. If no response is received within the timeout period, the connection to the server is closed. If the connection to the server is closed, all transactions to that server are affected.
Update time	10 to 10 000 ms	Applicable for all.	Specify the minimum time that may elapse between the transfer of two of the same transaction.
Update mode	Cyclically On data change	Write Single Coil (5) Write Single Register (6) Write Multiple Coil (15) Write Multiple Registers (16) Read Write Multiple Registers (23)	Specify when a transaction shall be sent to the server. Cyclically: The transaction is sent cyclically, at the interval specified in the Update time parameter. On data change: The transaction is sent when the data is changed. The minimum time between two transactions is specified by the Update time parameter.
Startup operation mode	Directly Wait for data	Write Single Coil (5) Write Single Register (6) Write Multiple Coil (15) Write Multiple Registers (16) Read Write Multiple Registers (23)	Directly: Data is sent as soon as possible after start-up. Wait for data: All data for the transaction must have been sent from the High Level network and received by the Communicator before the transaction is sent.
Offline option	Default: Freeze Pause Safe value; Length and Value	Write Single Coil (5) Write Single Register (6) Write Multiple Coil (15) Write Multiple Registers (16) Read Write Multiple Registers (23)	Define the action to be taken when the high level network connection is lost. Freeze: The Communicator holds the value until the network connection is restored. Pause: The transaction is suspended until the network connection is restored. Safe value: To ensure stability and reliability in the absence of a network connection, specify the Length 1 or 2 and the Value 0 to 65 535 to use during offline periods.

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

8.6.6. Duplicate Transaction

When you duplicate a transaction, all settings are preserved.

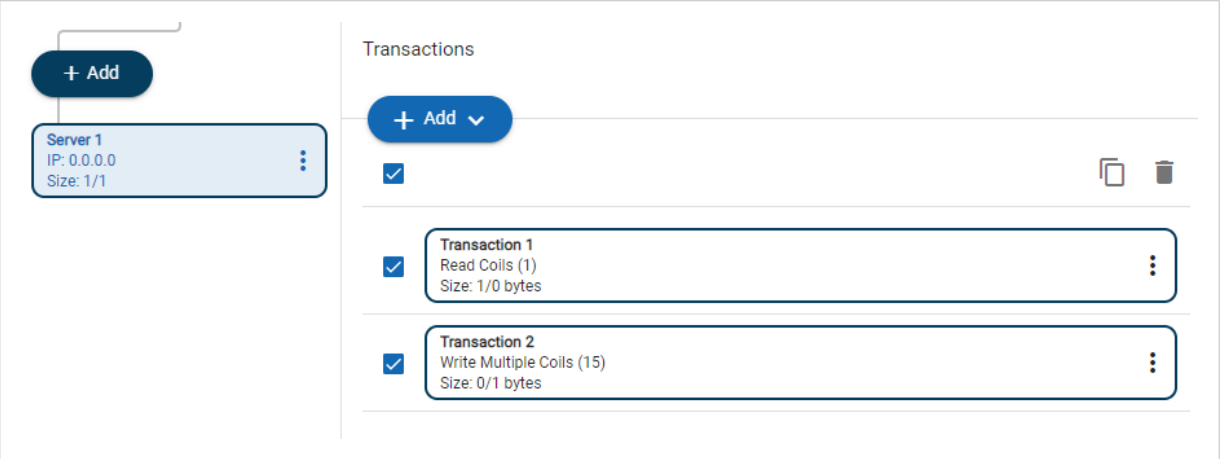


Figure 29. Duplicate transaction

To duplicate, select the checkbox in front of each transaction you want to duplicate and click the **Duplicate** icon.

The duplicated transaction(s) is added at the bottom of the transactions list.

8.6.7. Delete Transaction

When you delete a transaction, all its settings are permanently lost.

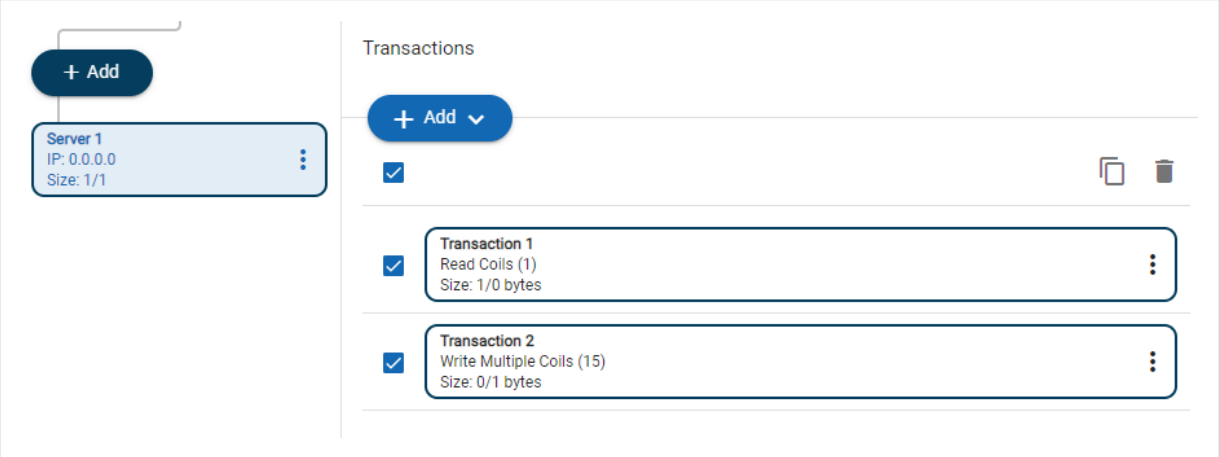


Figure 30. Delete transaction

To delete:

1. Select the checkbox in front of each transaction you want to delete and click the **recycle bin icon**.
2. To confirm, **Delete**.

8.7. PROFIBUS Settings

Configure the PROFIBUS network settings.

8.7.1. PROFIBUS Address Settings

NOTE
Ensure that the Communicator rotary switches are sett to 000.

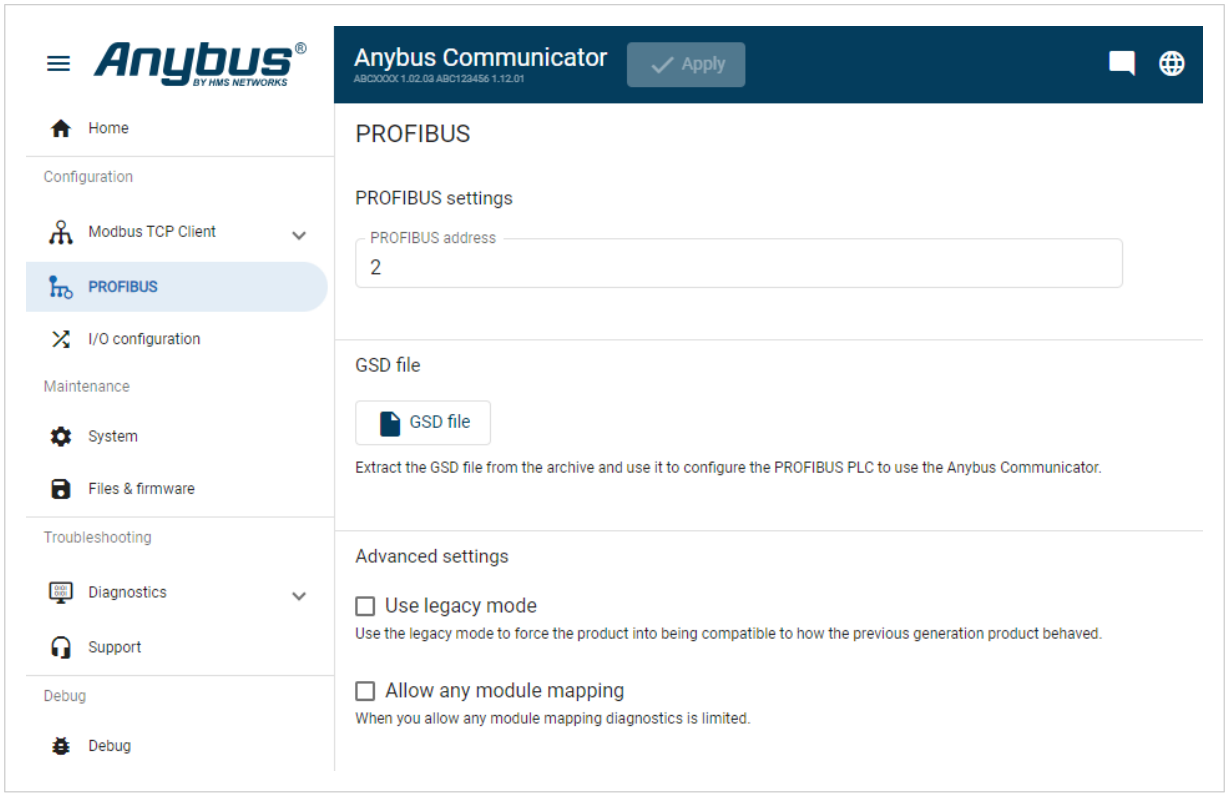


Figure 31. PROFIBUS address setting

In the PROFIBUS address field, enter the Communicator node address.

See Also

Set A Node Address With Rotary Switches (Page 21)

8.8. PROFIBUS Advanced Settings

NOTE
The Advanced settings is used to makes the Communicator compatible with the Anybus X-gateway.

8.8.1. Legacy Mode for PROFIBUS General Station Description (GSD) File

Advanced settings option for PROFIBUS.

Before You Begin

IMPORTANT
Legacy mode does not support acyclic communication.

NOTE
When Use legacy mode is enabled for PROFIBUS, **Allow any module mapping** is automatically enabled. When **Allow any module mapping** is enabled, the **Diagnostics** functionality is limited.

If you already have an Anybus X-gateway device description file installed in your PLC, legacy mode allows you to continue using the settings from the device description file for the new Communicator.

Procedure

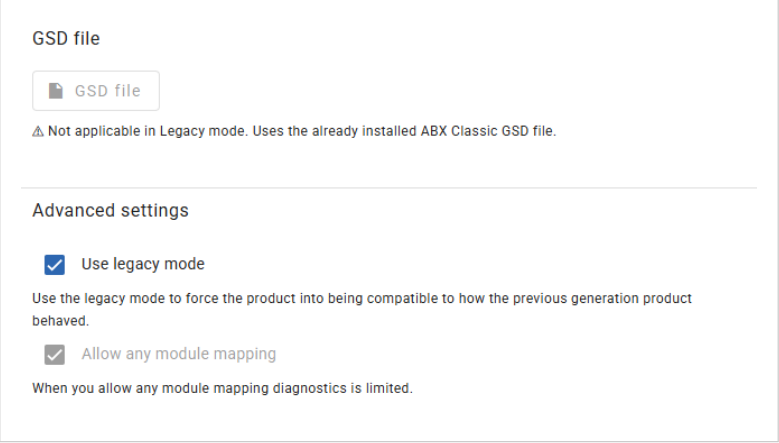


Figure 32. Advanced settings > Use legacy mode and Allow any module mapping

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

When Use legacy mode is enabled, the device description file download becomes inactive.

Legacy mode for PROFIBUS includes the **Allow any module mapping** setting, which is automatically enabled when you select the **Use legacy mode** checkbox.

See Allow Any Module Mapping for PROFIBUS (page 56).

8.8.2. Allow Any Module Mapping for PROFIBUS

Advanced settings option for PROFIBUS.

Before You Begin

NOTE
When Allow any module mapping is enabled, the **Diagnostics** functionality is limited.

NOTE
For more information, see I/O Size Restrictions for Allow Any Module Mapping.

Allow any module mapping has fewer restrictions and allows the modules to be mapped in any slot.

Option 1 - Use Legacy Mode and Allow any Module Mapping Enabled

Procedure

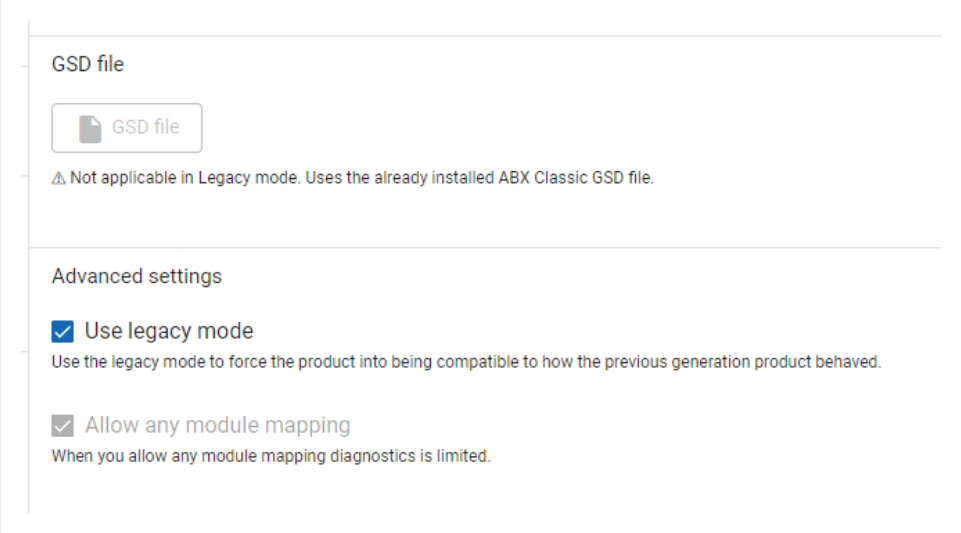


Figure 33. Advanced settings, **Use legacy mode** and **Allow any module mapping** is enabled

When **Use legacy mode** is enabled **Allow any module mapping** is automatically enabled.

Option 2 - Allow Any Module Mapping Enabled

Procedure

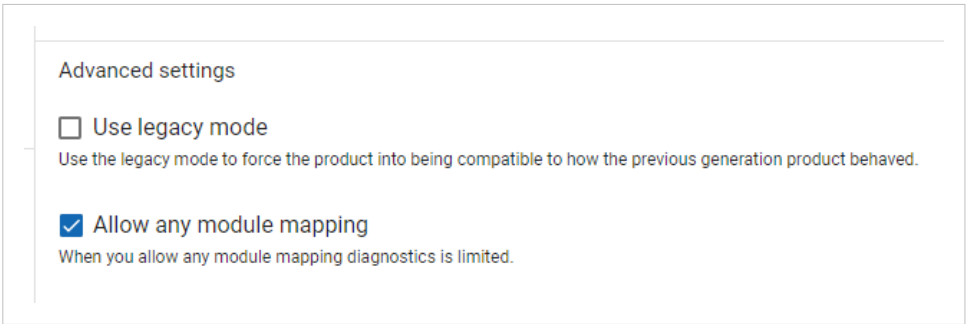


Figure 34. Advanced settings, **Allow any Module Mapping** is enabled

To enable any module mapping, select the **Allow any module mapping** checkbox.

8.9. I/O Configuration

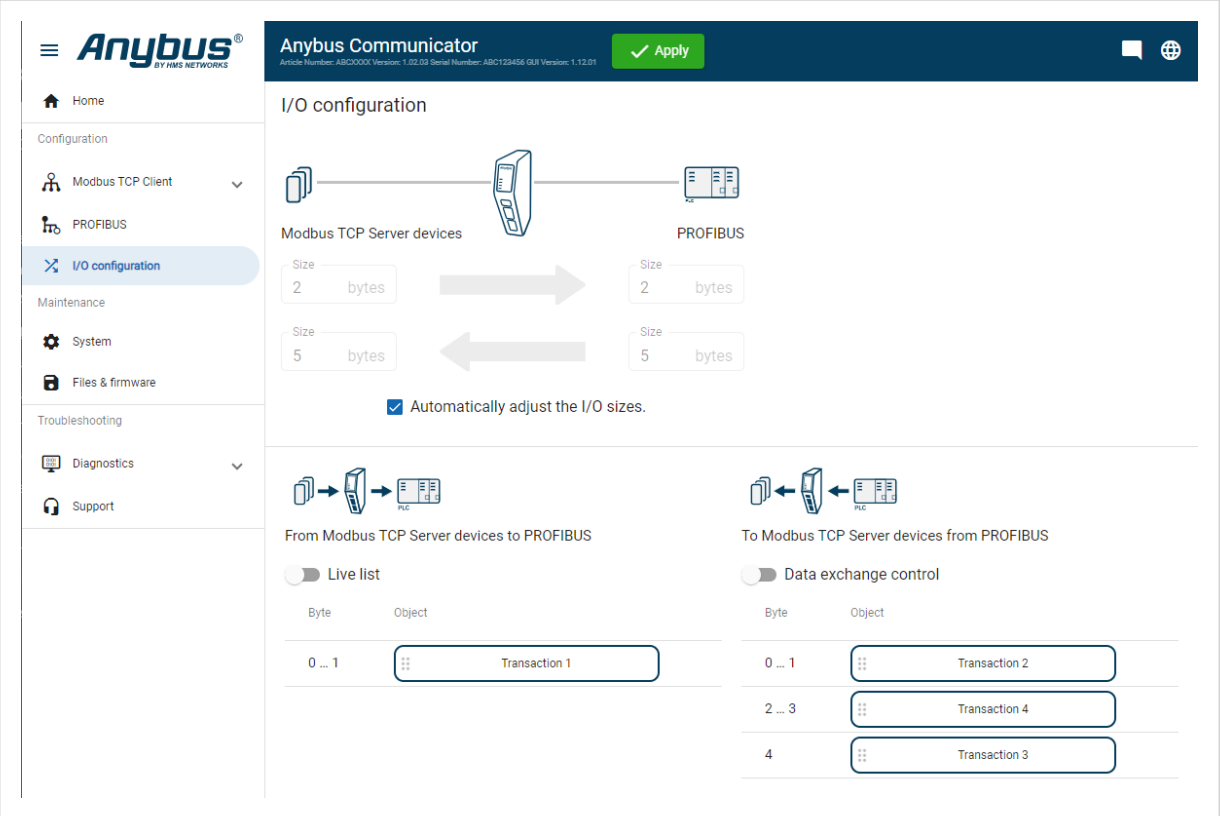


Figure 35. **I/O configuration** page

On the **I/O configuration** page the data communication between the Modbus TCP Server devices and the PROFIBUS network is mapped.

The allocated I/O area is auto generated based on the **Modbus TCP Server devices** network server(s) configuration and how the settings on the **PROFIBUS** page are configured.

There are two areas: **From Modbus TCP Server devices to PROFIBUS** and **To Modbus TCP Server devices from PROFIBUS**.

I/O Size Settings

By default, the Communicator is set to use the same I/O sizes for both the PROFIBUS network and the Modbus TCP Server devices.

To configure different sizes for the networks, deselect the **Automatically adjust the I/O sizes** checkbox and enter the desired sizes.

8.9.1. Map Area Object Order

To change the order of the objects in a map area, drag and drop the desired transaction to a new location.

Objects can not share the same I/O area.

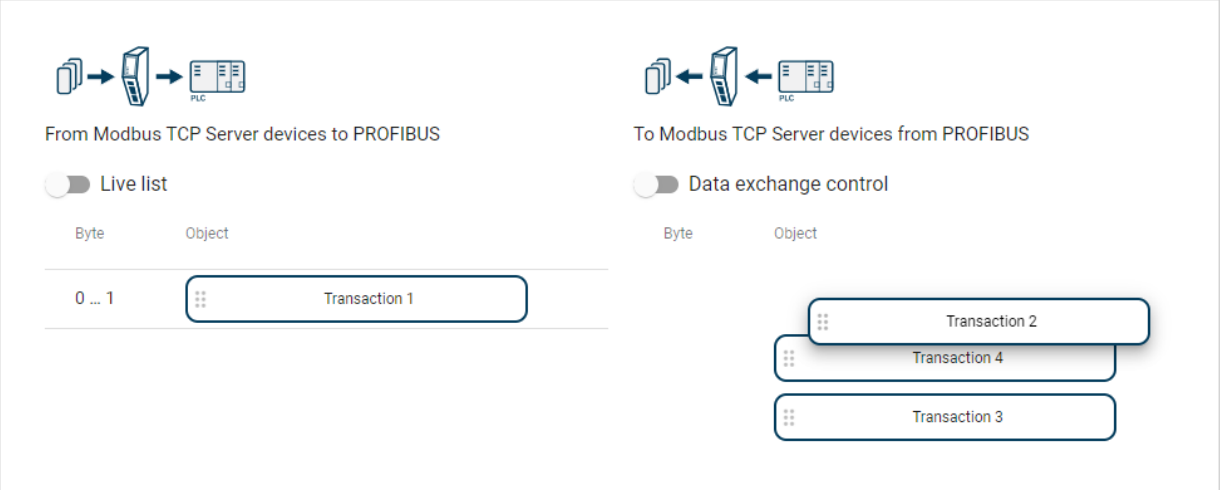


Figure 36. I/O configuration, change the order of objects

8.9.2. 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.

8.9.3. Map Area

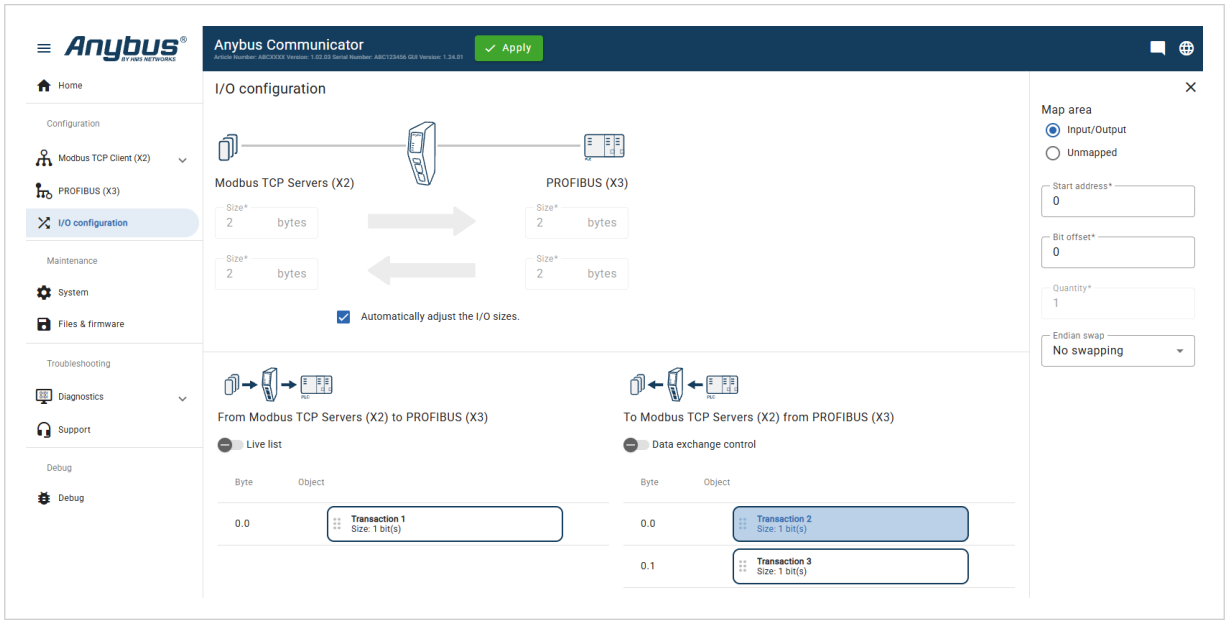


Figure 37. I/O configuration page, Map area options

Map Area Options
You must specify the map area to use for each transaction in the I/O configuration.

Select one of the following **Map area** options:

- **Input/Output**: The transaction data is sent/recieved to/from the high level network.
- **Unmapped**: The transaction data is not used.

Start Address
For Input/Output and General, you can enter a start address for the transaction data.

8.9.4. Bit Offset

Understanding Bit Offset
For certain Modbus transactions, bit offset is used to optimize IO data area usage.

With bit offset, multiple transactions can share the same byte(s) without overlapping.

This method is both memory-efficient and flexible for IO data management.

Supported Transactions
Bit offset is supported in the following Modbus function types:

- Read Coils (1)
- Read Discrete Inputs (2)
- Write Single Coil (5)
- Write Multiple Coils (15)

Read Coils and Read Discrete Inputs
The bit offset shifts the bits before they are written to the IO data area.

Only the bits associated with the specific transaction are affected.

Multiple read transactions can target the same byte(s) in the IO data area, as long as their bit ranges do not overlap.

To maintain byte alignment, set the bit offset to 0 for all transactions. Bits not written by any transaction are padded with zeroes.

Write Single Coil and Write Multiple Coils
In write operations, the bit offset shifts the bits in the IO data area before they are read and sent.

Multiple write transactions can use the same byte(s) in the IO data area without reading to the same bits.

Unsupported Transactions
Bit offset is not supported for register-based transactions, such as:

- Read Holding Registers (3)
- Read Input Registers (4)
- Write Single Register (6)
- Write Multiple Registers (16)
- Read Write Multiple Registers (23)

These transactions are byte-aligned in the IO data area.

Coil Data Packing Examples

Example 3. Byte-Aligned Coil Storage

In this example the transactions are byte-aligned in the IO data area.

8 coils would consume 8 bytes, even though each coil only needs 1.

Coil	Byte	Bit
Coil 1	Byte 1	Bit 0
Coil 2	Byte 1	Bit 1
...	...	...

Coil	Byte	Bit
Coil 8	Byte 1	Bit 7

Example 4. Bit Offset Coil Storage

In this example bit offset is used.

8 coils can be stored in 1 byte, using each bit (0–7) to represent a different coil.

Bit	Coil
Bit 0	Coil 1
Bit 1	Coil 2
...	...
Bit 7	Coil 8

Example 5. Pack Multiple Transactions Using Bit Offset

This example shows how multiple transactions with varying bit lengths can be packed into a shared process data (PD) buffer using bit offsets.

Table 1. Transaction Mapping

Transaction	Bit Length	PD Offset	PD Bit Offset
Transaction 0	1 bit	0	0
Transaction 1	3 bits	0	1
Transaction 2	7 bits	0	4
Transaction 3	8 bits	1	3

Table 2. PD Buffer Bit Layout

PD Offset	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Byte 0	T2	T2	T2	T2	T1	T1	T1	T0
Byte 1	T3	T3	T3	T3	T3	T2	T2	T2
Byte 2	-	-	-	-	-	T3	T3	T3
T0–T3 represent the individual transactions. Bits from each transaction are packed into the PD buffer across byte boundaries.								

Procedure

The bit offset is set separately for each transaction and specifies the position of the coil in the transaction data. It represents the number of bits from the start of the transaction data to the coil at that bit offset.

By setting the bit offset, you make sure your **Server** reads or writes the correct coil in each transaction.

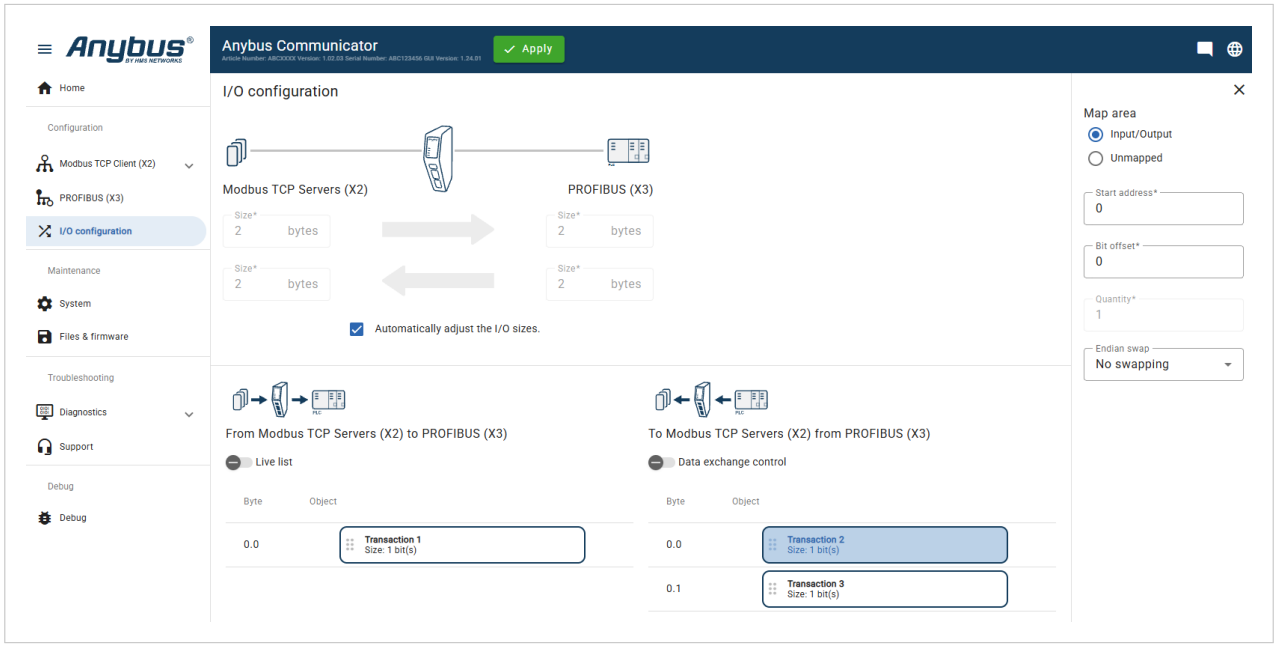


Figure 38. I/O configuration page, Bit offset

1. To set a bit offset, select the relevant **Transaction**.
2. In the **Bit offset** field, enter a value between 0 to 7.

8.9.5. Convert Between Big-Endian and Little-Endian

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

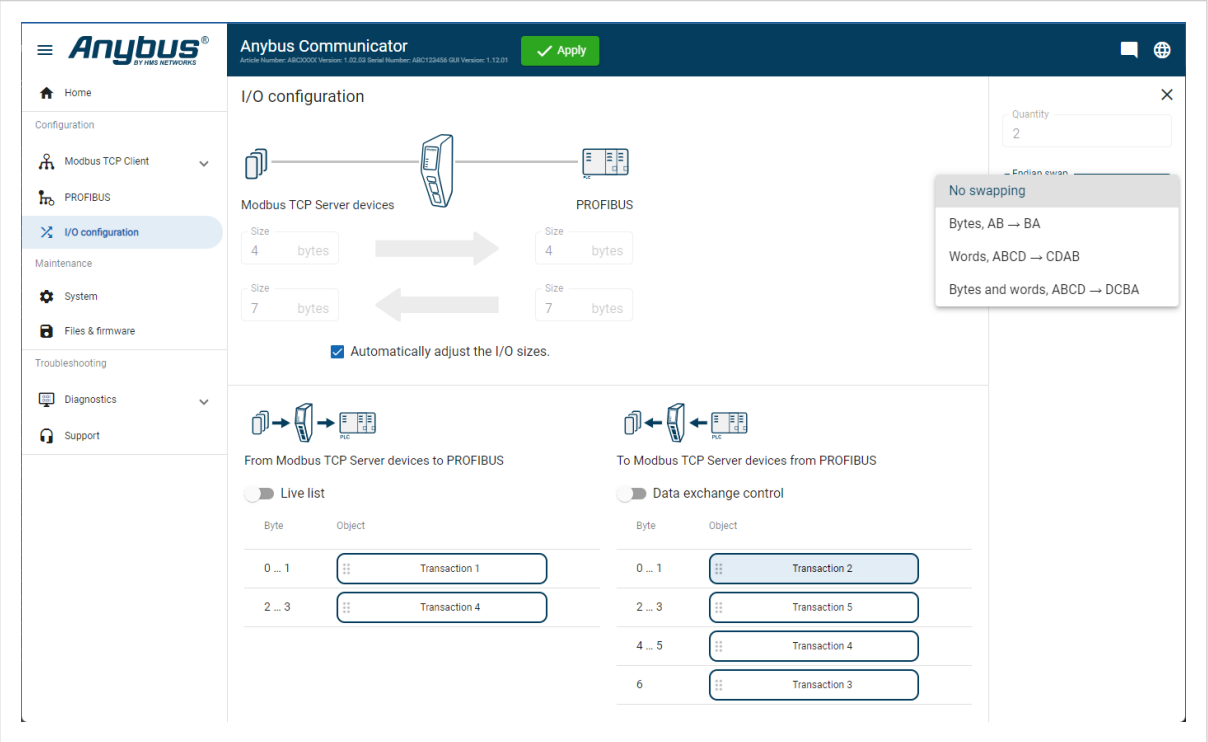


Figure 39. **I/O configuration** page, Endian swap

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.

8.9.6. Live List

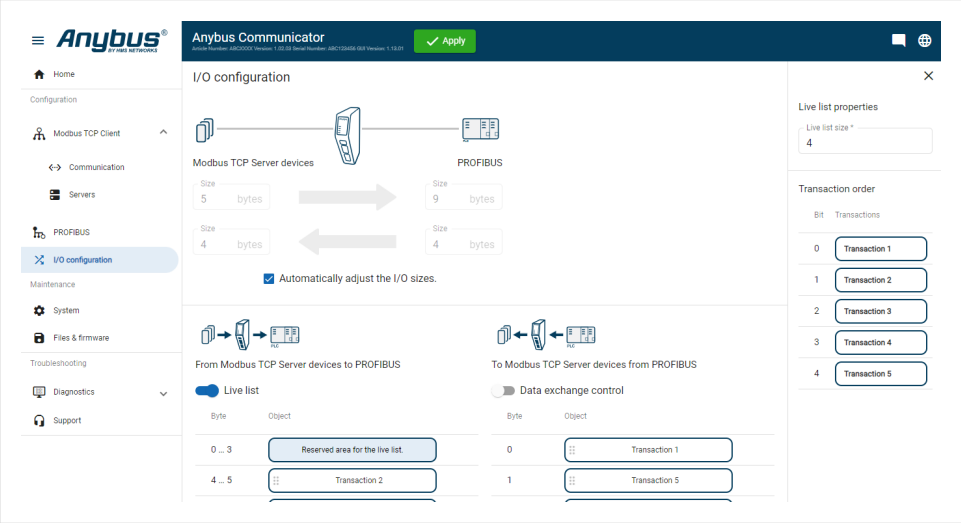


Figure 40. I/O configuration page, Live list enabled

By default, **Live list** is disabled.

About the Live List

- When **Live list** is enabled, the first four bytes of process data on the PROFIBUS network contain the live list.
- Each bit in the **Live list** can hold the status for one transaction.

- The **Live list** holds 32 bits, a total of 32 servers connected to the Communicator.
- The bit is 0 when the bit does not correspond to a configured server.
  For example, this occurs when the number of configured servers is less than 32.
- Each bit is 1 when the corresponding servers is online.

Transaction Online or Offline

The bit is 0 when the corresponding transaction is offline.

The transaction is considered offline when:

- The transaction is not sent to the server.
- The transaction have timed out, no valid response has been received within the specified timeout period.
- Another transaction on the same connection has timed out.
- The server has responded with a Modbus error.

The transaction is considered online when:

- The transaction has received a valid response within the specified timeout period.

Live List Size and Transaction Order

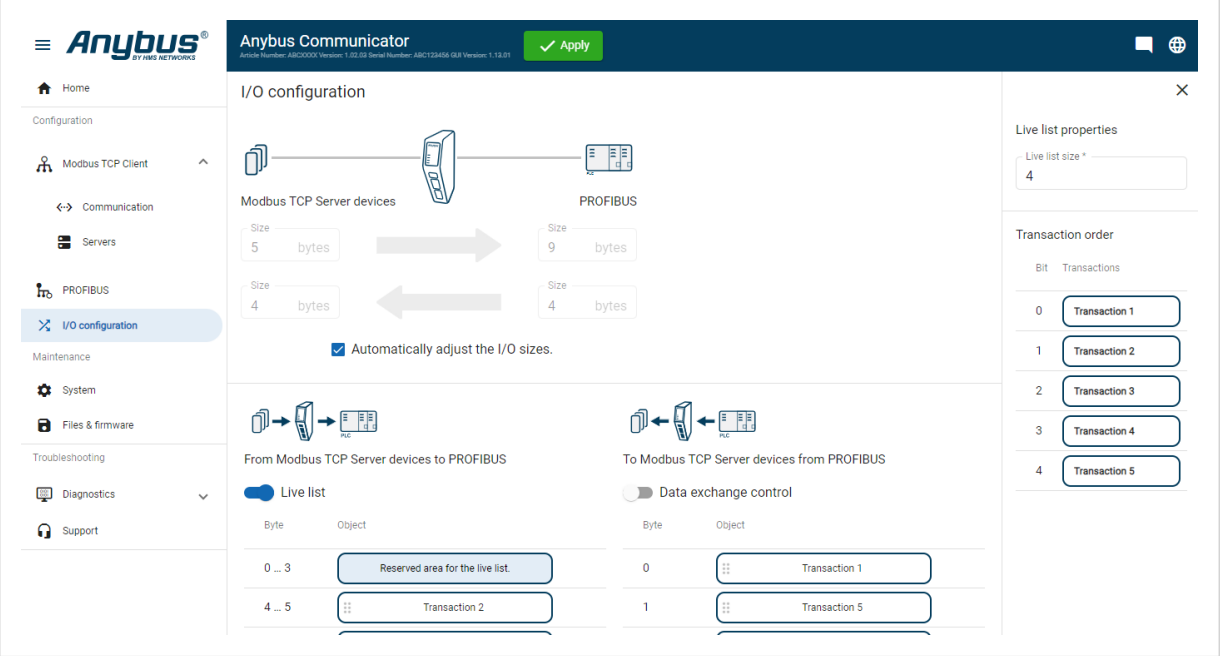


Figure 41. Live list properties and Transaction order

The default **Live list size** is 4 bytes.

The size of the live list can be configured within the range of 1 to 19 bytes.

In the **Transaction order** list, you can view the order in which the transactions are executed.

8.9.7. Data Exchange Control

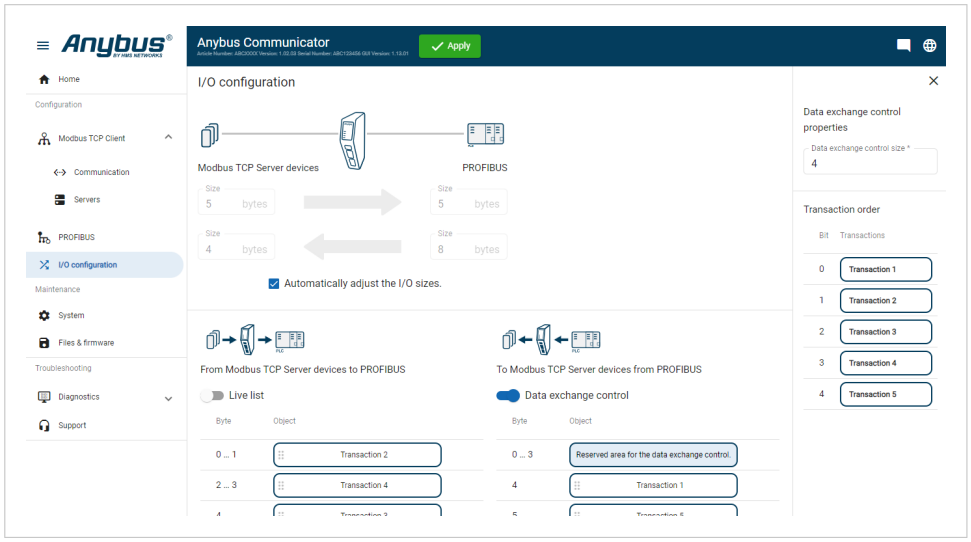


Figure 42. I/O configuration, **Data exchange control** enabled

By default **Data exchange control** is disabled.

When **Data exchange control** is enabled, the first four bytes of process data on the PROFIBUS network contain the data exchange control.

The **Data exchange control** holds 32 bits.

Each bit in the **Data exchange control** can be used to enable/disable data exchange for individual transaction on the subnetwork.

The server order in the **Data exchange control** 32 bit array always matches the Live List.

When data exchange is enabled, the transaction is sent only if the corresponding bit is 1.

Data Exchange Control Size and Transaction Order

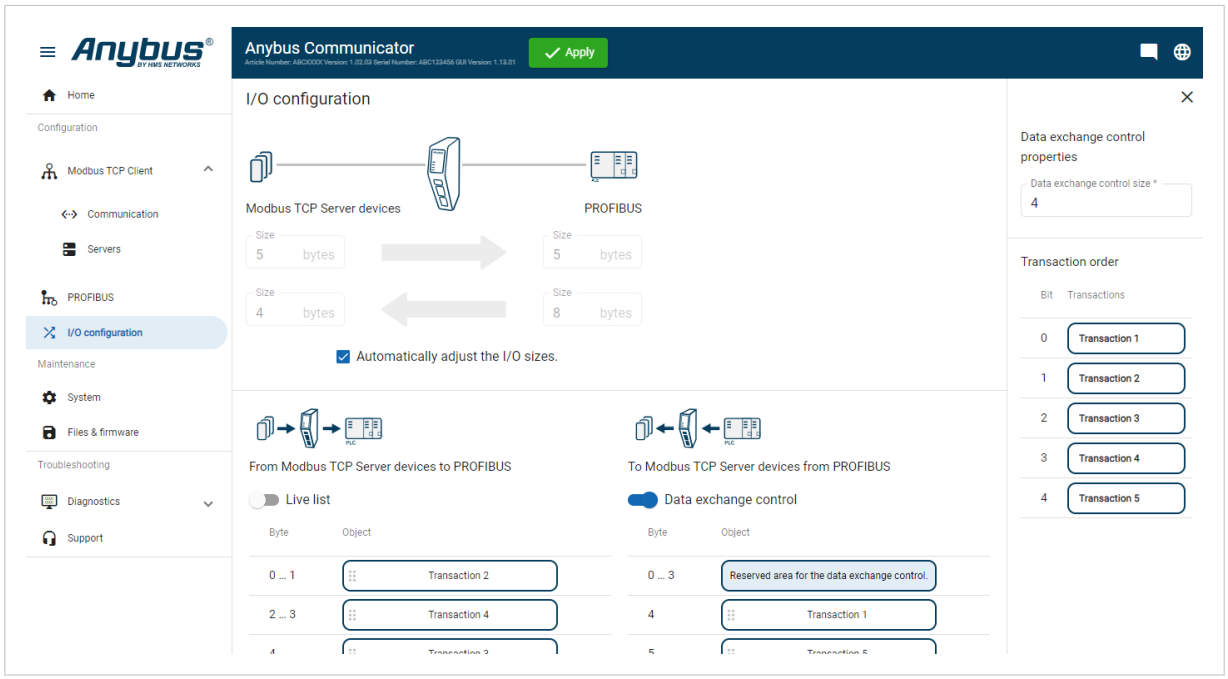


Figure 43. Data exchange control properties and Transaction order

The default **Data exchange control size** is 4 bytes.

The size of the data exchange control can be configured within the range of 1 to 19 bytes.

In the **Transaction order** list, you can view the order in which the transactions are executed.

8.10. Configuration Notes

You can add notes to describe the Communicator configuration.

8.10.1. Add Configuration Note

Procedure

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

Figure 44. Configuration note, comment icon

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

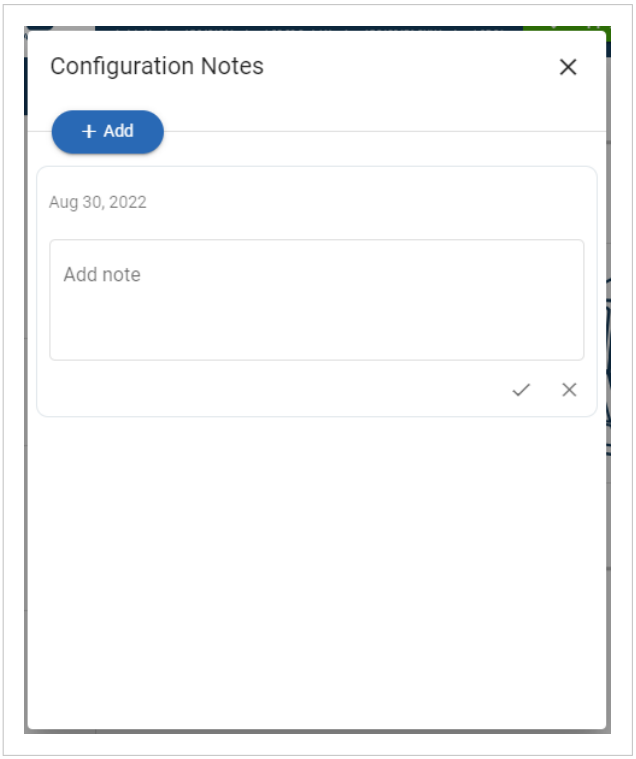


Figure 45. Add new configuration note

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

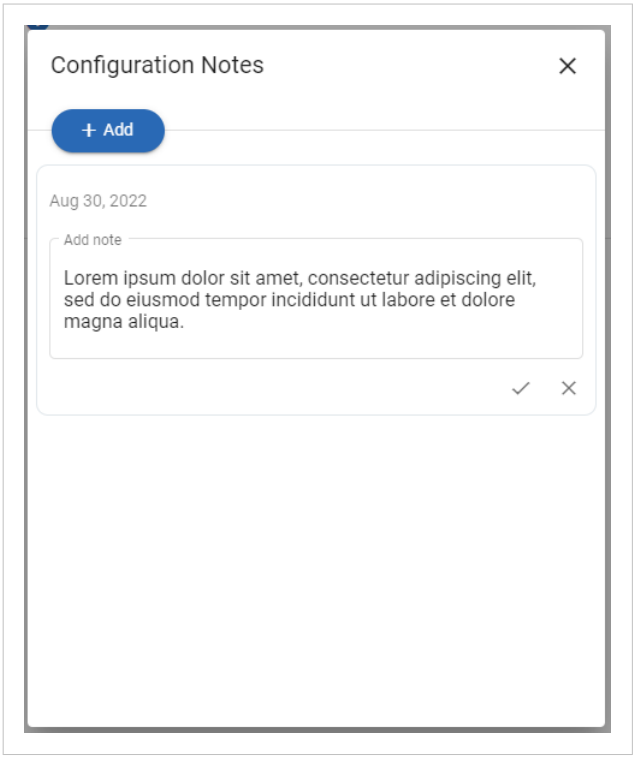


Figure 46. Write a configuration note

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.

8.10.2. View and Edit Configuration Notes

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

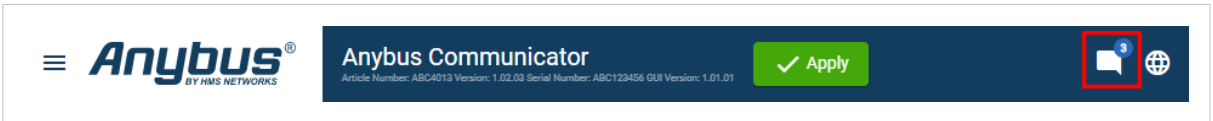


Figure 47. Example: The comment icon indicates that there are three added notes

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

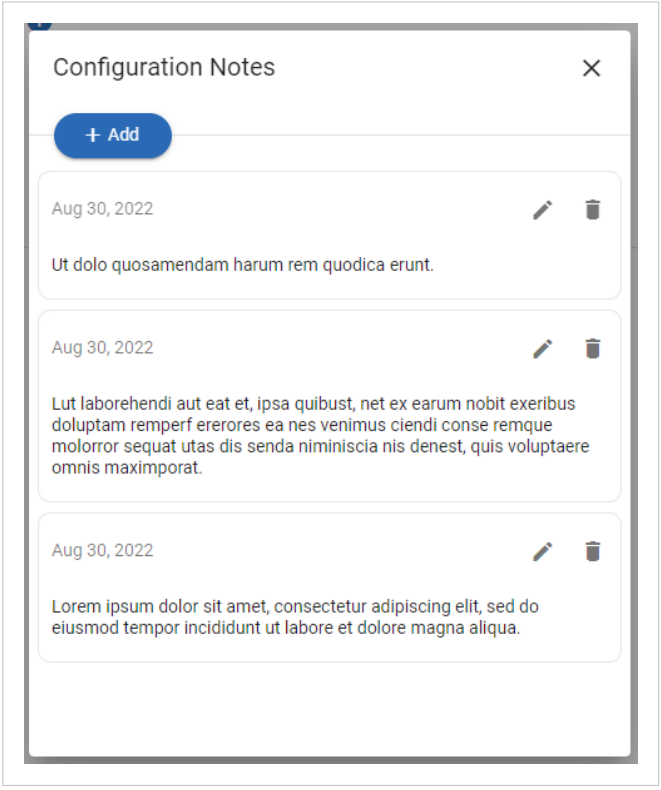


Figure 48. Example: The Configuration Notes window with added notes

8.11. Apply Configuration

Before You Begin

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

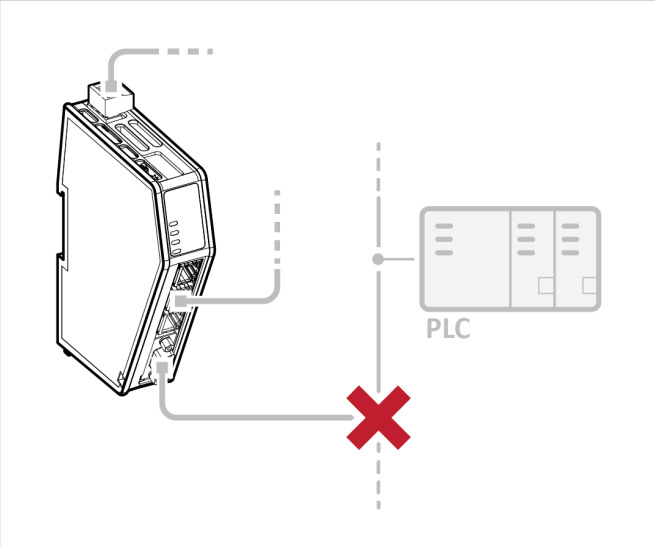


Figure 49. Disconnect the Communicator from the PROFIBUS network

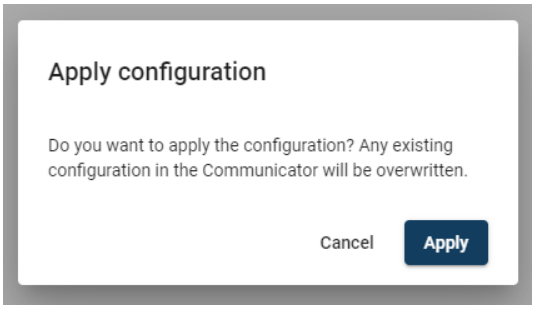
Before you can apply the configuration, ensure that there is no active communication on the PROFIBUS network where the Communicator is connected.

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.



8.12. 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

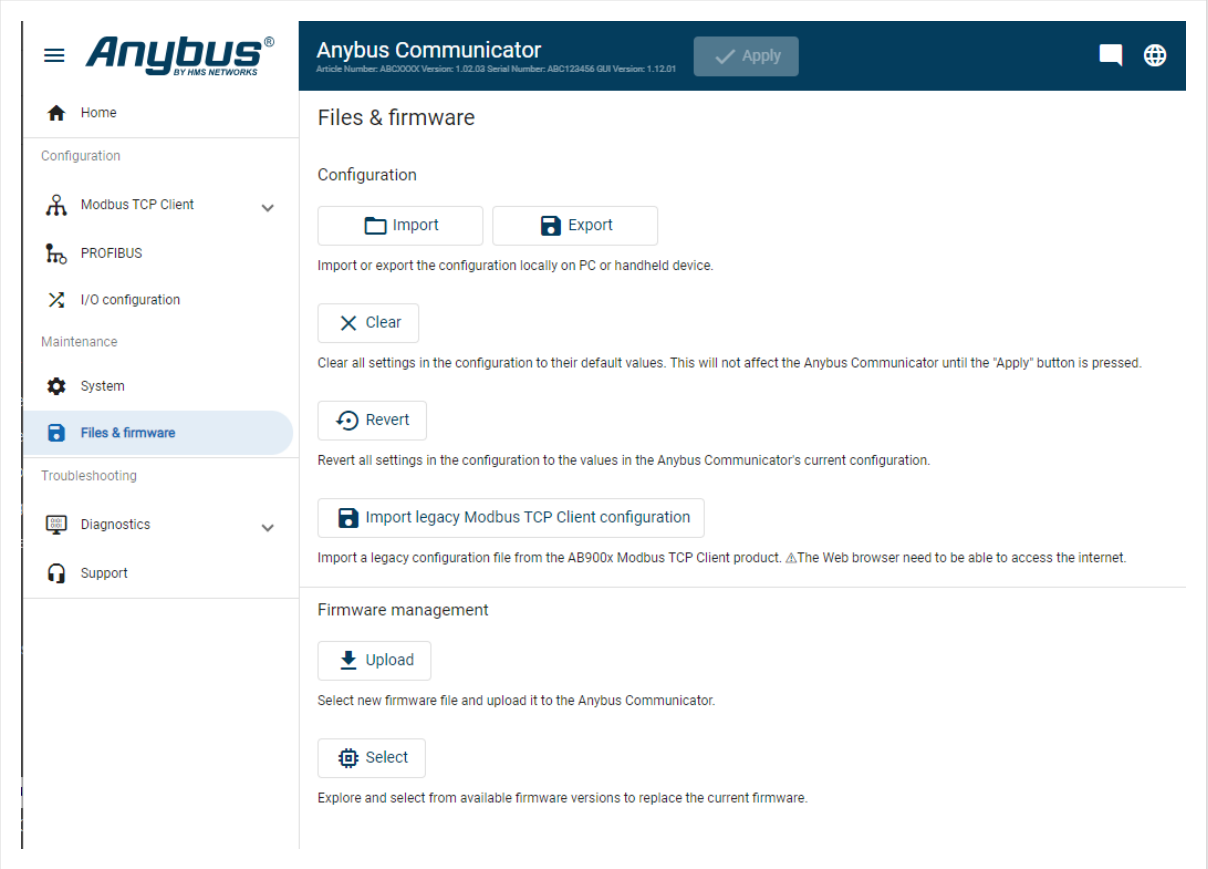


Figure 50. **Files & firmware** page

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.

8.13. To Use a Legacy Modbus TCP Client Configuration

Before You Begin

The intended use of the X-gateway configuration import is to get a new Communicator unit up and running quickly and then complete the configuration in the Communicator built-in web interface.

NOTE

Only the X-gateway Modbus TCP Client configuration settings can be imported.

The I/O data map and high-level network settings are not supported and must be set manually in the Communicator built-in web interface.

Procedure

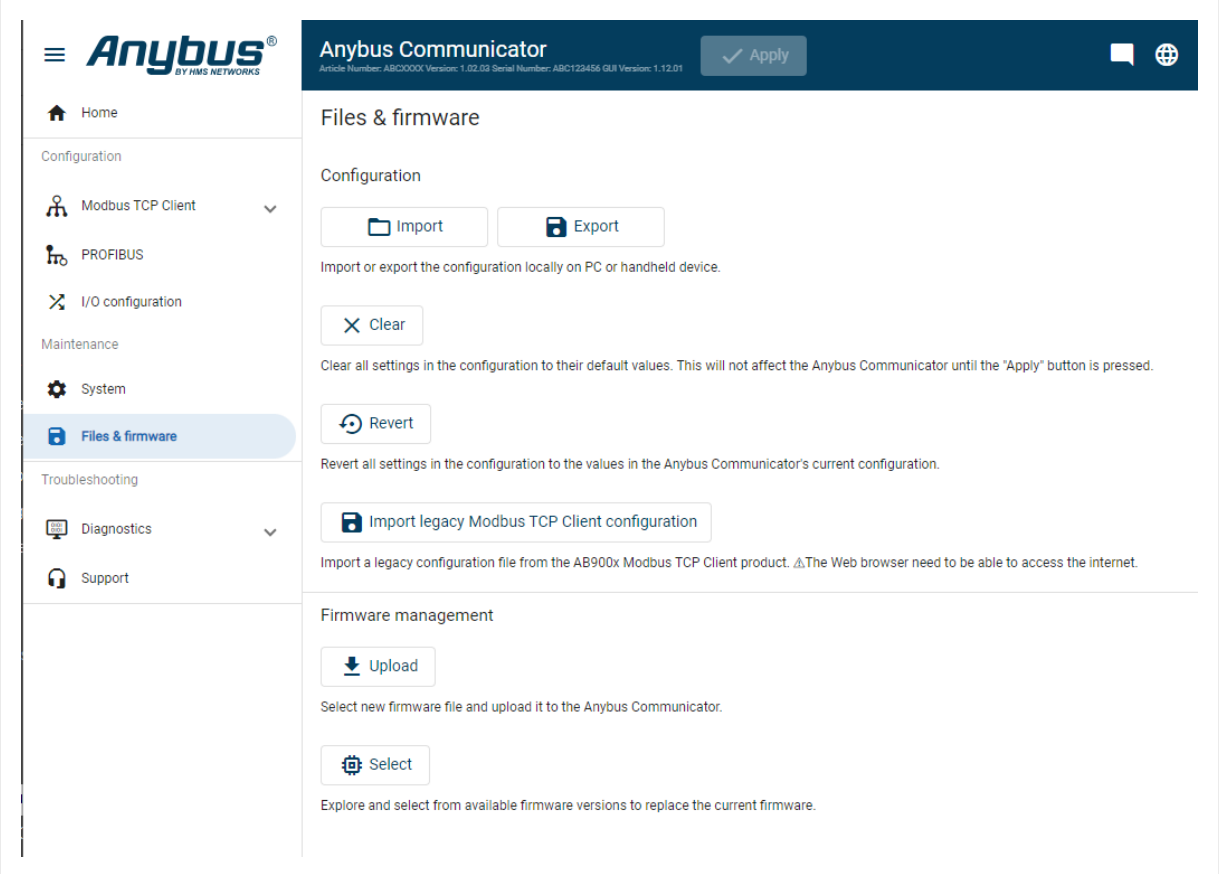


Figure 51. **Files & firmware** page

1. Ensure that the PC you are using to configure the Communicator is connected to the internet.
2. On the **Files & firmware** page, click **Import Modbus TCP Client legacy configuration**.
3. In the **Import Modbus TCP Client legacy configuration** window, click **Select file (.cfg)**.
4. In the Open dialog box, browse to and select the configuration .cfg file and click **Open**.

5. To import the configuration, click **Import**.

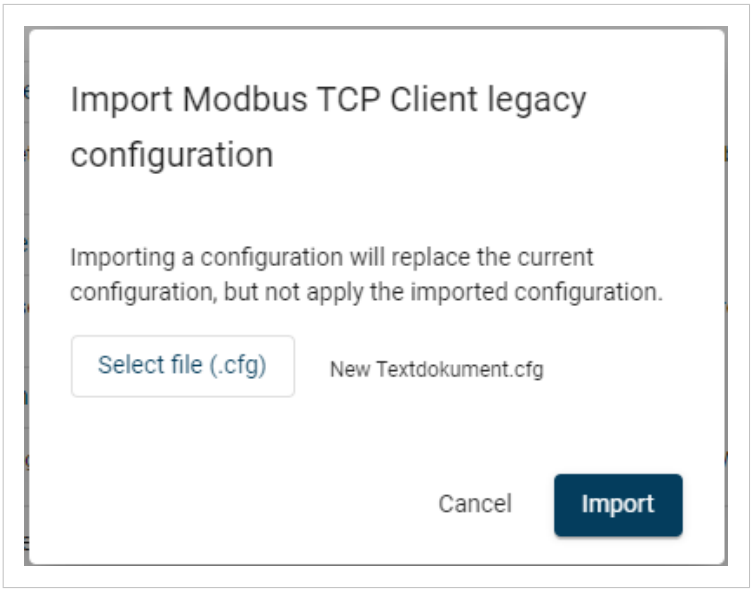


Figure 52. Example, selected .cfg file

6. Option when the X-gateway configuration file is protected with a username and password.
Select the **Authentication details** checkbox and enter the username and password.

> **NOTE**
> For information about X-gateway Authentication to protect the configuration, see the user documentation for your specific X-gateway.

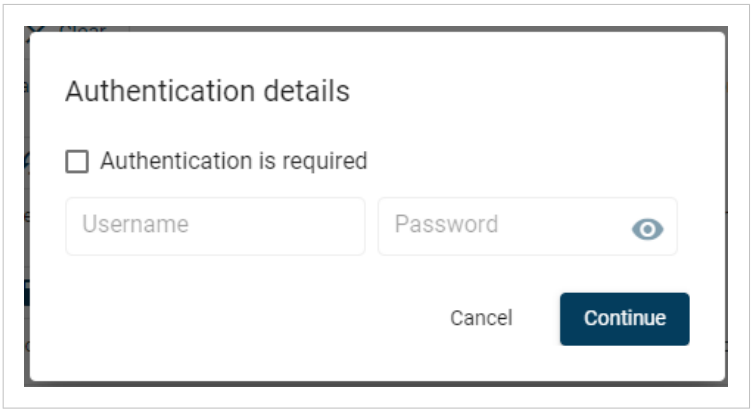
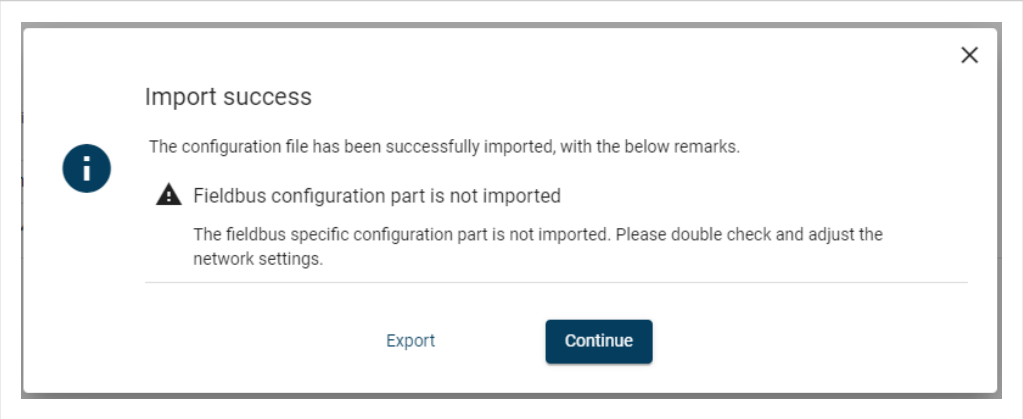


Figure 53. Authentication details

7. Click **Continue**.

Result

The X-gateway Modbus TCP Client configuration settings are imported.



A window with messages about the imported configuration appears.

In the list you can view the settings that are supported or adjusted to work with Communicator and which settings that are not supported and must be set manually in the Communicator built-in interface.

To export the messages in an Excel XLS file, click **Export Messages**.

Figure 54. Example, list with messages about the import

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

9. PLC Configuration

9.1. 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.

9.2. Export Product GSD File

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

Procedure

You find the *PROFIBUS GSD* file on the Communicator built-in web interface **PROFIBUS** page.

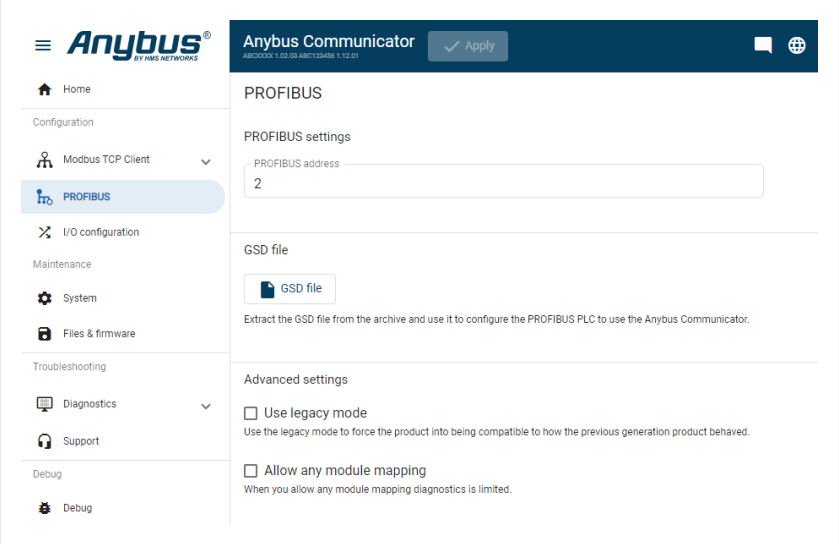


Figure 55. Export Product GSD File

To export the GSD file:

Click **GSD file**.

The GSD file is downloaded to your PC.

About the Product GSD Files

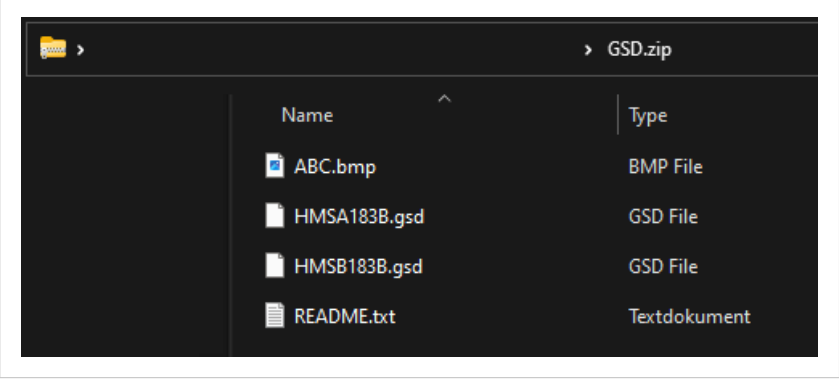


Figure 56. GSD.zip with HMSA183B.gsd and HMSB183B.gsd files

There are two GSD (General Station Description) files included in the Communicator GSD zip file:

- ***HMSA183B.gsd***
  Use this GSD file when the **Advanced settings**: **Use legacy mode** and **Allow any Module Mapping** are disabled.

- ***HMSB183B.gsd***
  Use this GSD file when the **Advanced settings**, **Allow any Module Mapping** is enabled.
  For more information about the *HMSB183B.gsd* file, see ???.

10. Verify Operation

Before You Begin

Before you can verify operation, you must configure the Communicator.

Ensure that the Communicator is connected to your PC, to a power supply and to the OT network.

10.1. Communicator Status Monitor

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

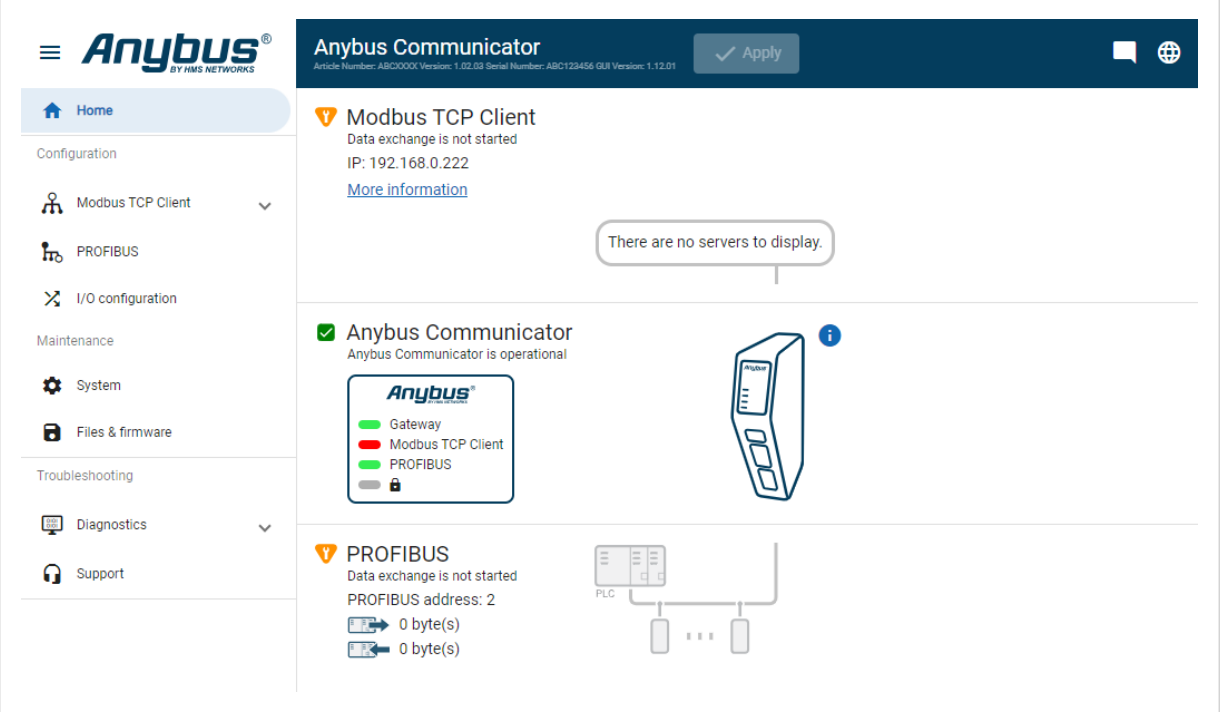


Figure 57. Home page

Gateway Status

Overview the Communicator LED indications remotely.

Server Status

Overview the status for each server added to the subnetwork.

Network Status and Settings

Overview communication status and the current networks settings.

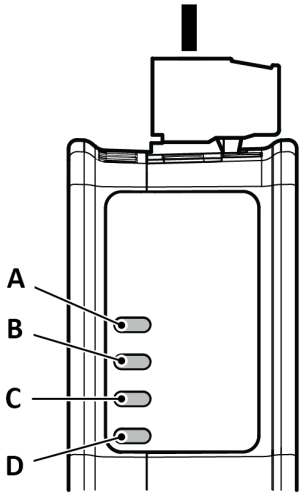
Status Symbols

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.

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)
Connect To Power (Page 25)
Communicator LED Indicators (Page 82)
LED Status (Page 95)
Firmware Upgrade Error Management (Page 99)

10.2. Communicator LED Indicators



A. **Gateway status**
B. **Modbus TCP Client**
C. **PROFIBUS**
D. **Security switch**

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.

Modbus TCP Client

Operation status	Description
Off	No power or no IP address.
Green, solid	No connections errors or timeouts.
Red, solid	IP address conflict detected, or FATAL event.
Red, flashing	At least one connection error or timeout.

PROFIBUS

Operation status	Description
Off	No power or no data exchange.
Green, flashing	Clear, data exchange.
Green, solid	Operate, data exchange.
Red, solid	FATAL event.
Red, one flash	Parameterization error.
Red, two flashes	PROFIBUS configuration error.

Security Switch

Operation status	Description
Off	No power. Security switch is unlocked. Exception.
Green, solid	Security switch is locked.

Fatal Error and Exception Error

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

Exception error: An exception error causes the Communicator to enter a controlled error state. The Communicator firmware application is still running.

LED	Fatal error	Exception error
A	Red, solid	Red, solid
B	Red, solid	Off
C	Red, solid	Off
D	Off	Off

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)
Connect To Power (Page 25)
Communicator Status Monitor (Page 80)
LED Status (Page 95)
Firmware Upgrade Error Management (Page 99)

10.3. Ethernet RJ45 LED Indicators

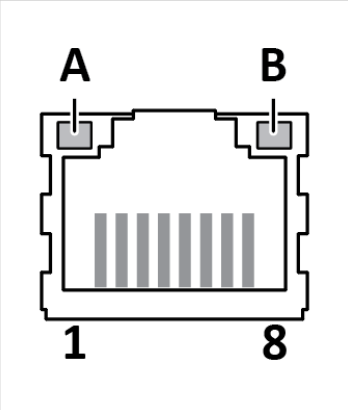


Figure 58. LED A. Activity LED B. Not used

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

11. Maintenance

11.1. Action on Fatal Error

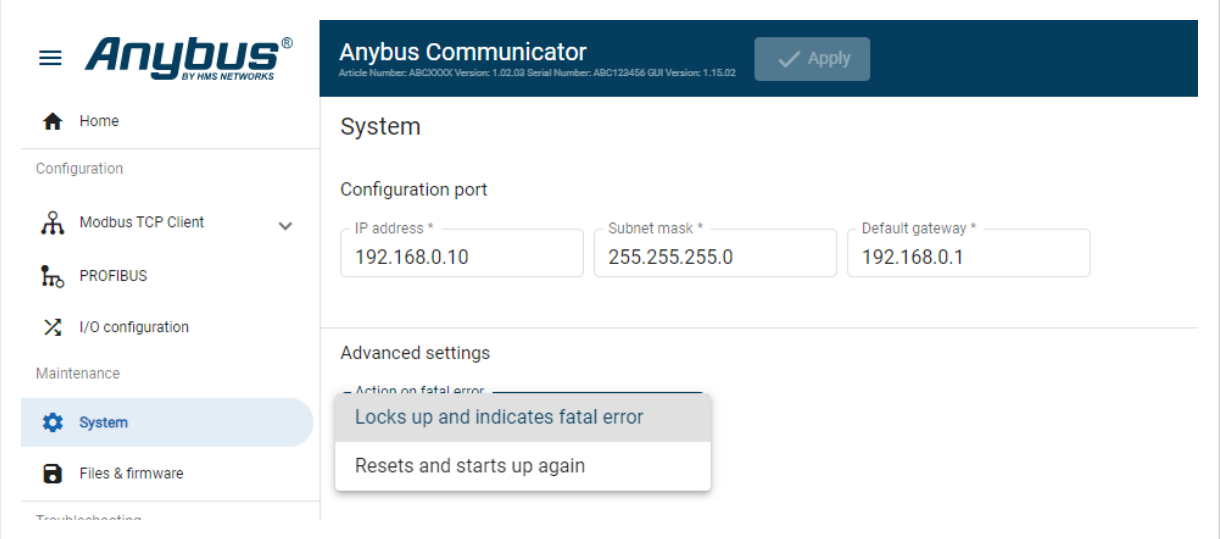


Figure 59. System page, Action on fatal error menu

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.

11.2. Configuration Port IP Settings

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

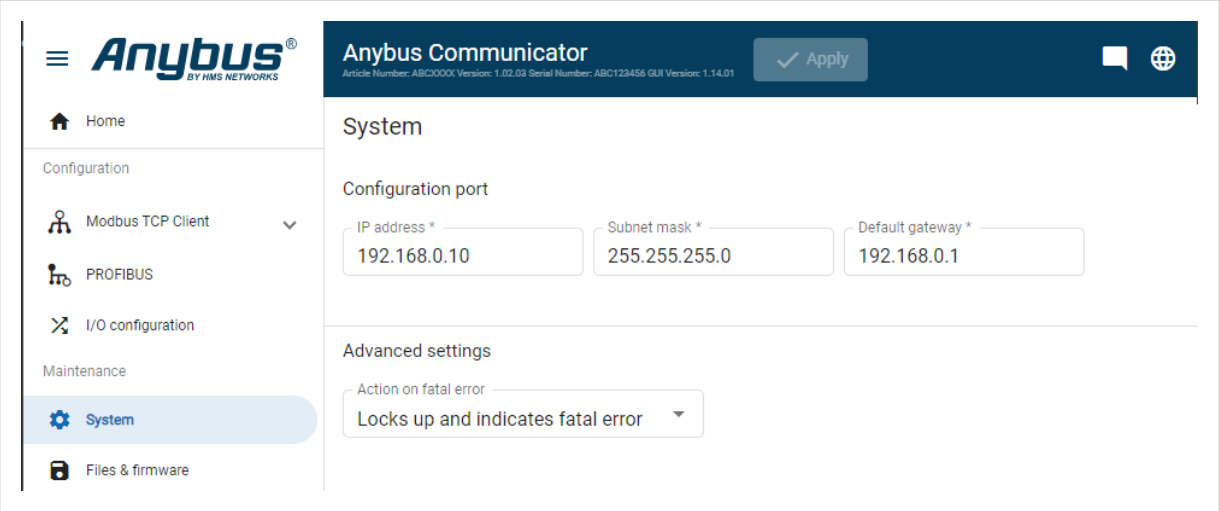


Figure 60. System page, Configuration port settings

Default Configuration Port IP settings

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

11.3. Configuration File Handling

11.3.1. Export Configuration

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

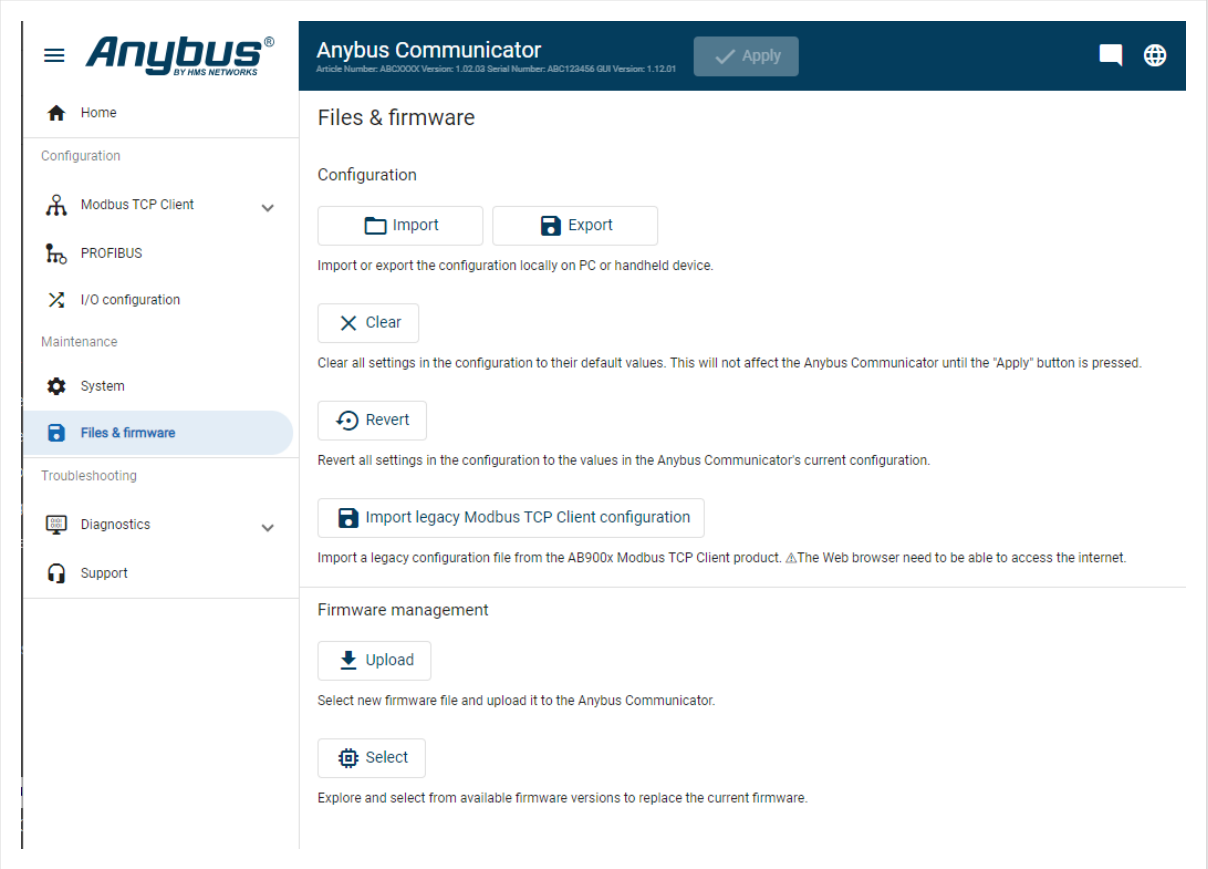


Figure 61. Files & firmware page

To export a configuration file:

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

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

11.3.2. 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

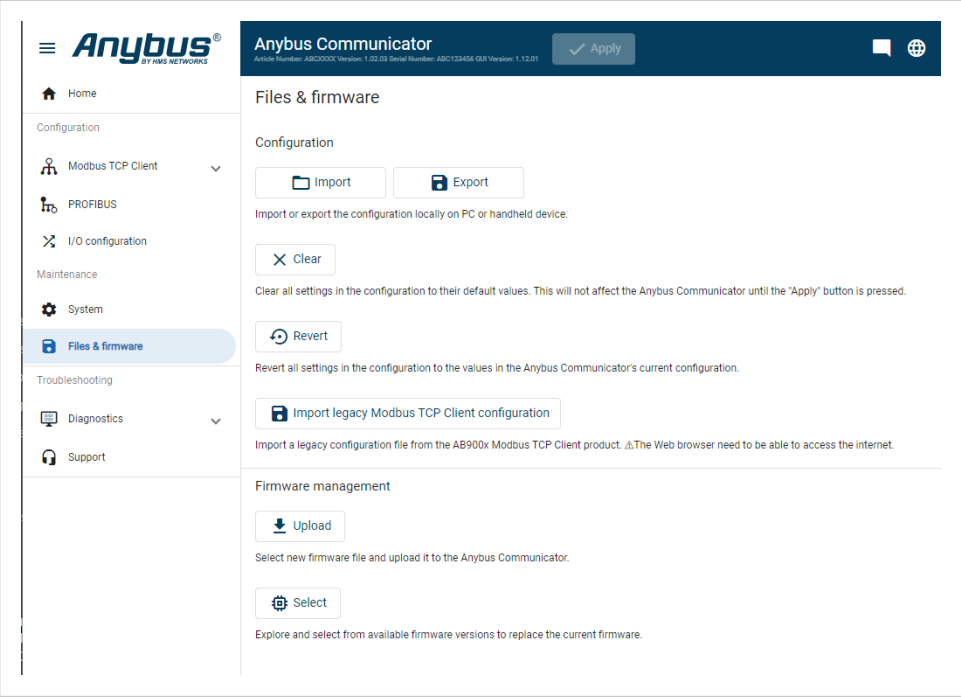


Figure 62. Files & firmware page

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.

11.4. Clear and Revert Configuration

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

Procedure

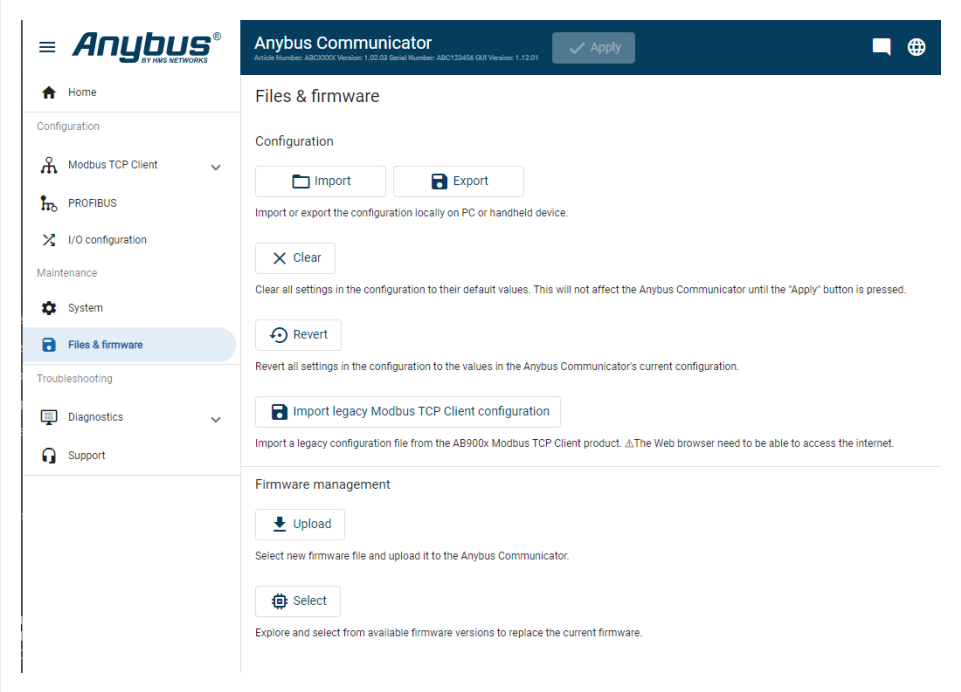


Figure 63. Files & firmware page

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.

11.5. Firmware Management

11.5.1. View the Firmware Version

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

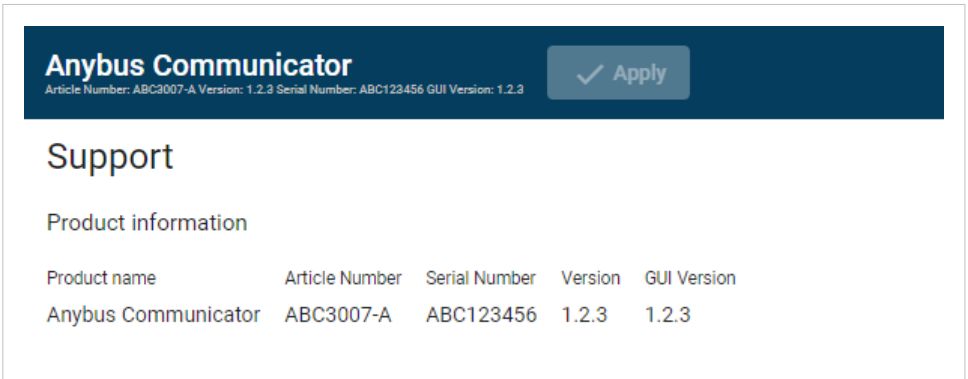


Figure 64. Support page, Product information example

11.5.2. 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.

11.5.3. 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.

11.5.4. Update Firmware

Before You Begin

IMPORTANT
To eliminate the risk of interference with plant operation, firmware update is only available when the Communicator is disconnected from the OT networks.

Ensure to disconnect the Communicator from the OT networks.

Procedure

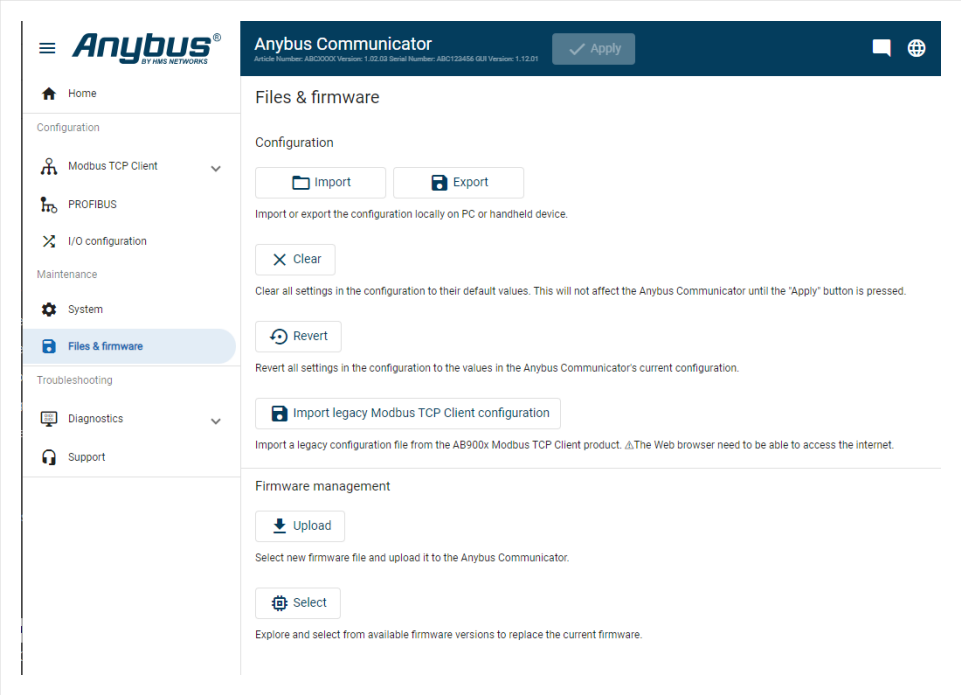


Figure 65. Files & firmware page

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.

11.6. 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 .

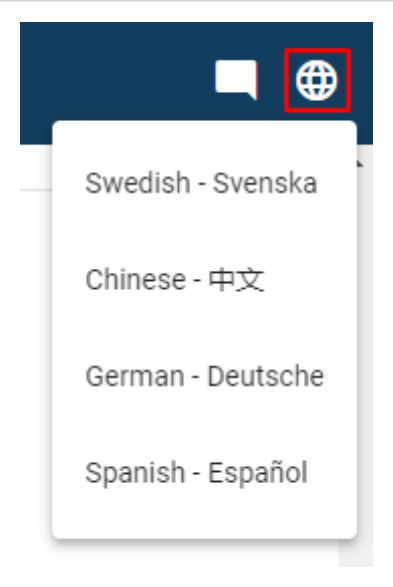


Figure 66. Language menu

2. Select a new language from the list.

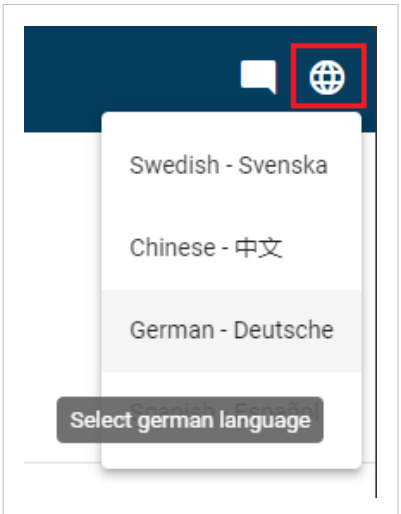


Figure 67. Example: Change language to German

The language change takes effect immediately.

12. Troubleshooting

12.1. Diagnostics

12.1.1. I/O Data

On the **Diagnostics**, **I/O data** page you can monitor how the data flow between the **Modbus TCP Client** side and the **PROFIBUS** side, including any configured endian conversions.

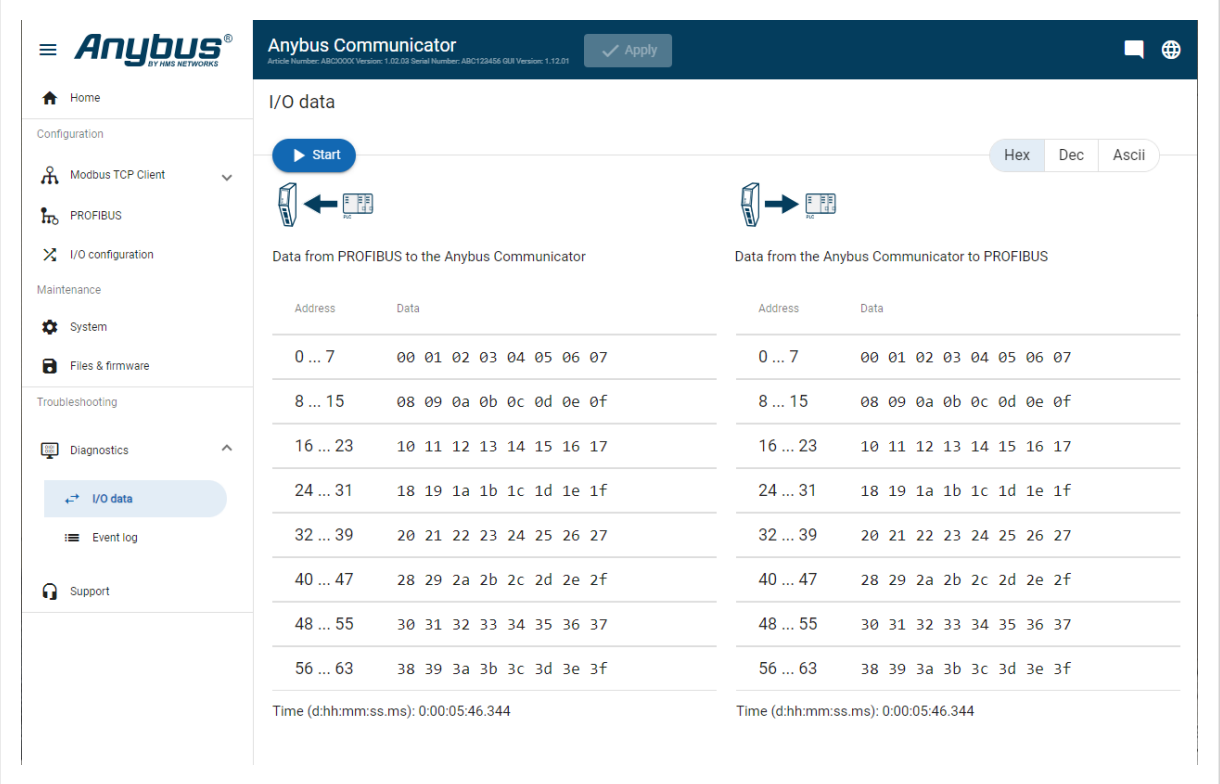


Figure 68. I/O data

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**.

12.1.2. Event Log

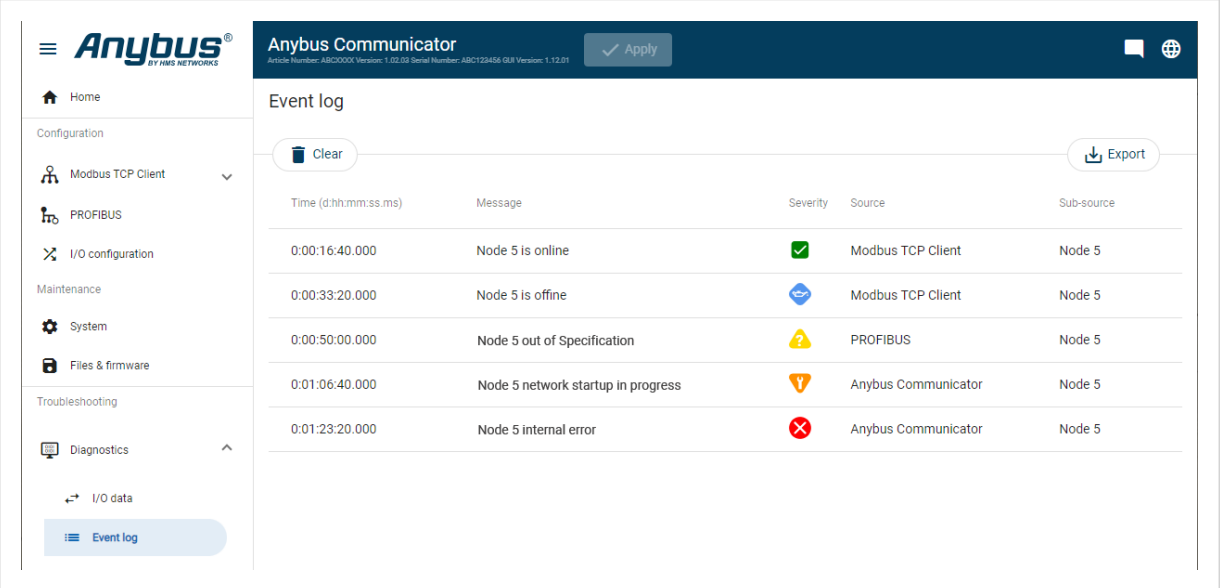


Figure 69. Event log page example

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 duration from when the X-gateway was powered on until the event occurred.
Message	A brief description of the event.
Severity	The severity of the event occurred.
Source	Communicator
	Modbus TCP Client
	PROFIBUS
Sub-source	The nodes connected to the subnetwork and the PLC connected to the high level network. If there is a problem with a node the node name is displayed in the Sub-source column. Example 6. Sub-source number If the node name is 5, number 5 is displayed in the Sub-source column.

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

12.1.3. LED Status

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

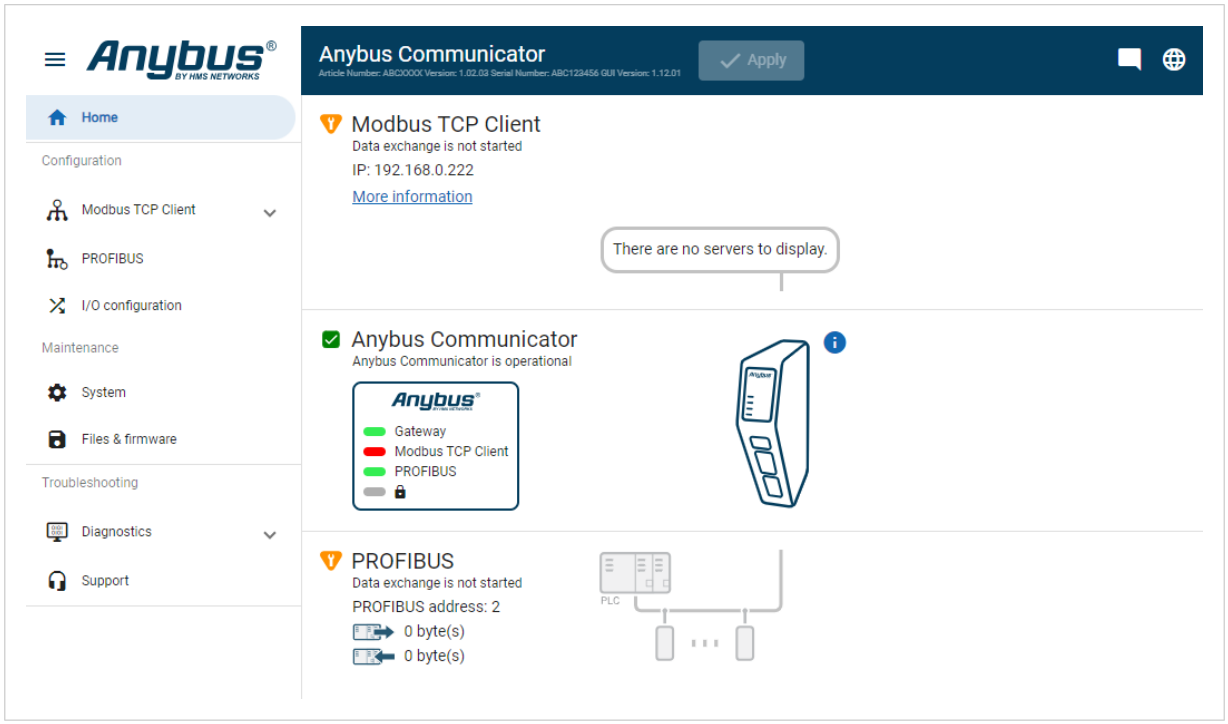


Figure 70. Home page

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)
Connect To Power (Page 25)
Communicator Status Monitor (Page 80)
Communicator LED Indicators (Page 82)
Firmware Upgrade Error Management (Page 99)

12.2. 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.

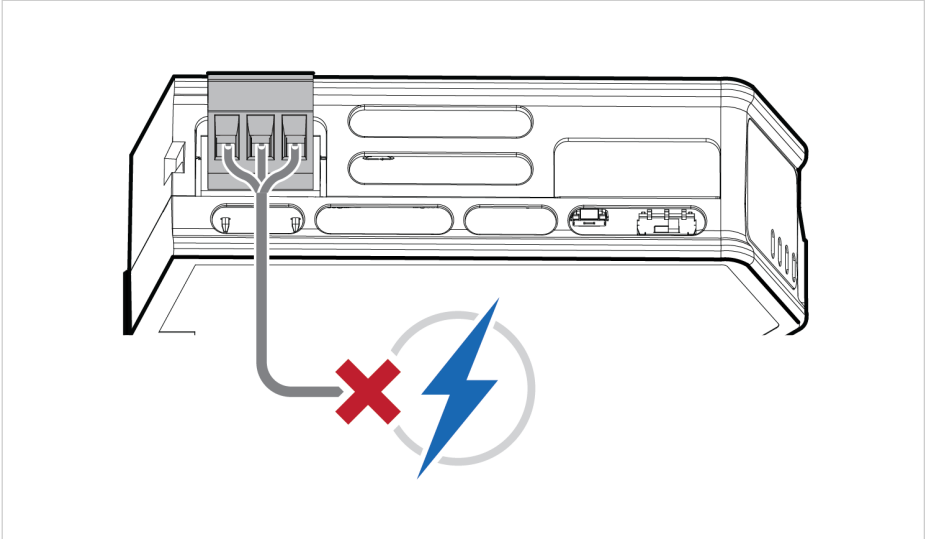


Figure 71. Disconnect power

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

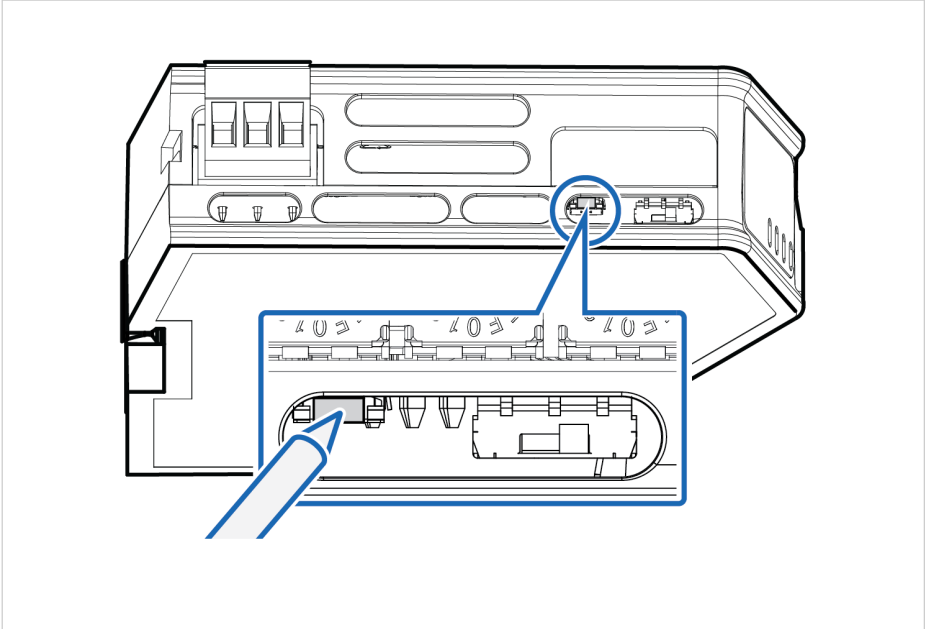


Figure 72. Press and hold **Reset** button

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

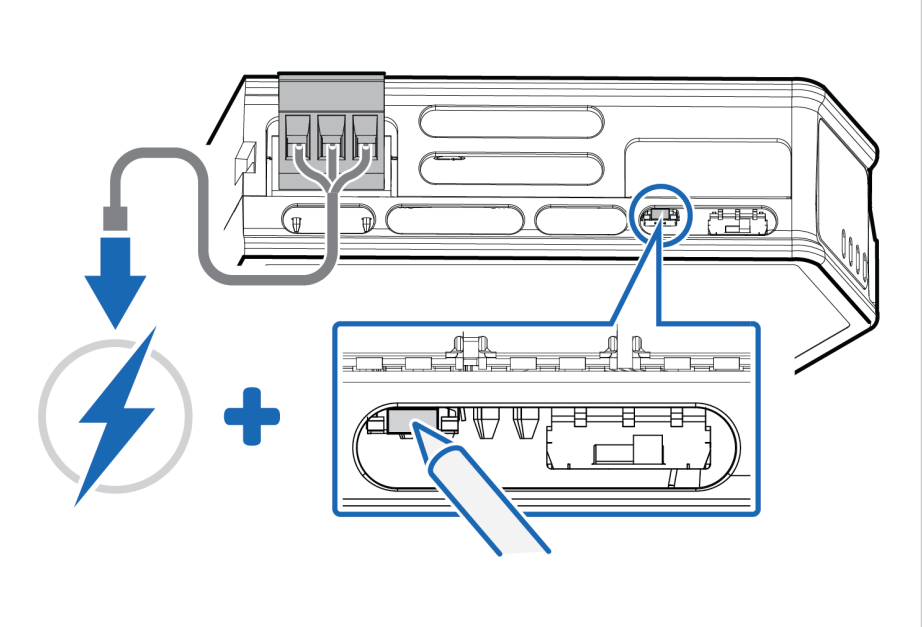


Figure 73. Hold **Reset** button and reconnect power

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**.

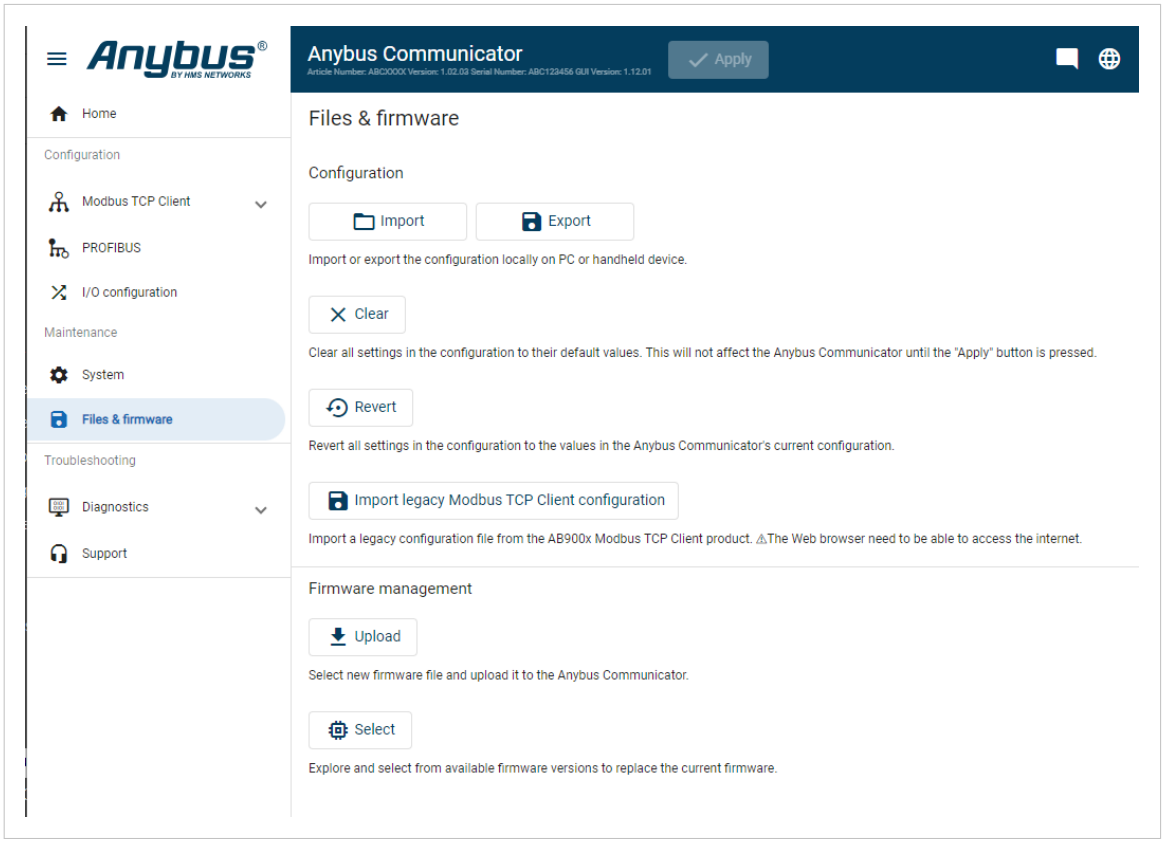


Figure 74. Files & firmware, Revert

12.3. 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 firmware file from the latest update attempt remains in the flash memory, but it is not active.

Procedure

To complete the interrupted firmware update:

1. Disconnect the Communicator from power.

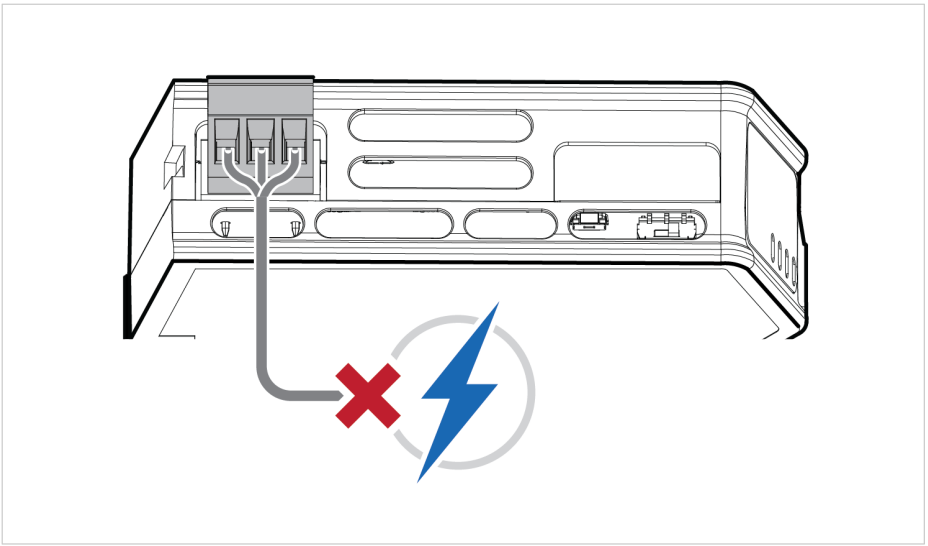


Figure 75. Disconnect power

2. Reconnect the Communicator to power.

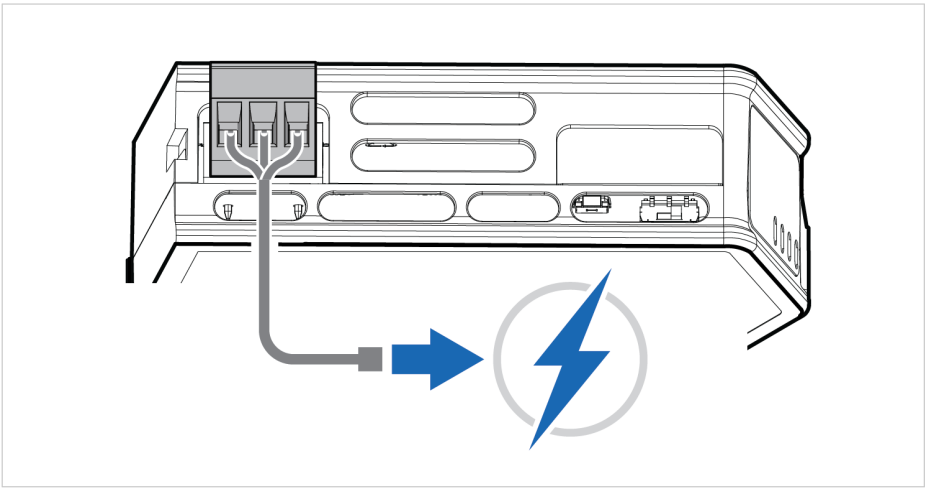


Figure 76. Reconnect power

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

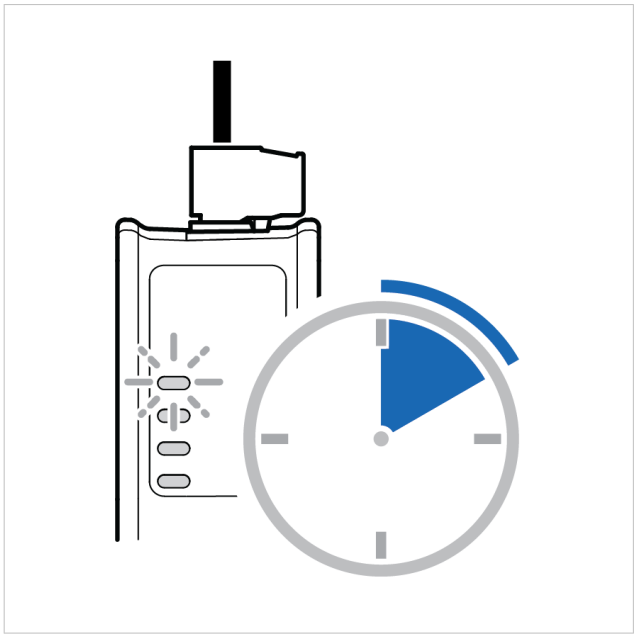


Figure 77. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

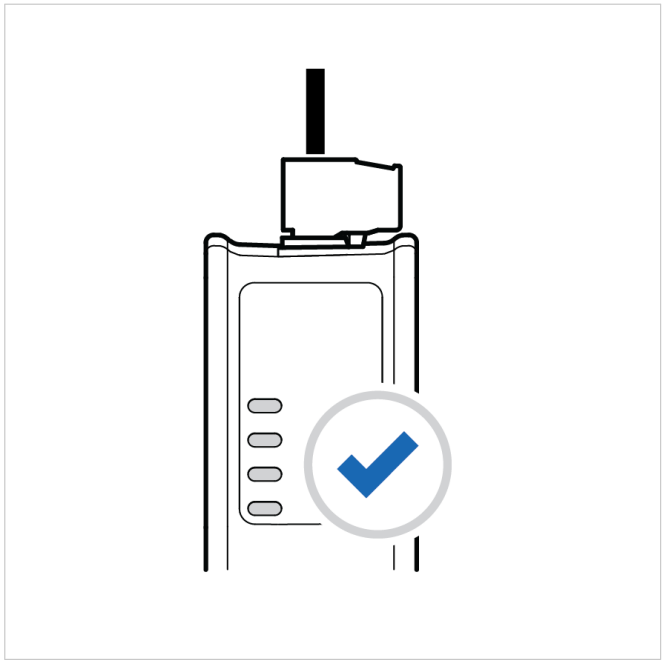


Figure 78. Recover and return to normal operation

See Also

Connect To Modbus TCP Client Network (Page 17)
Connect To PROFIBUS Network (Page 19)

Connect To Power (Page 25)
Communicator Status Monitor (Page 80)
Communicator LED Indicators (Page 82)
LED Status (Page 95)

12.4. Support

12.4.1. Support Package

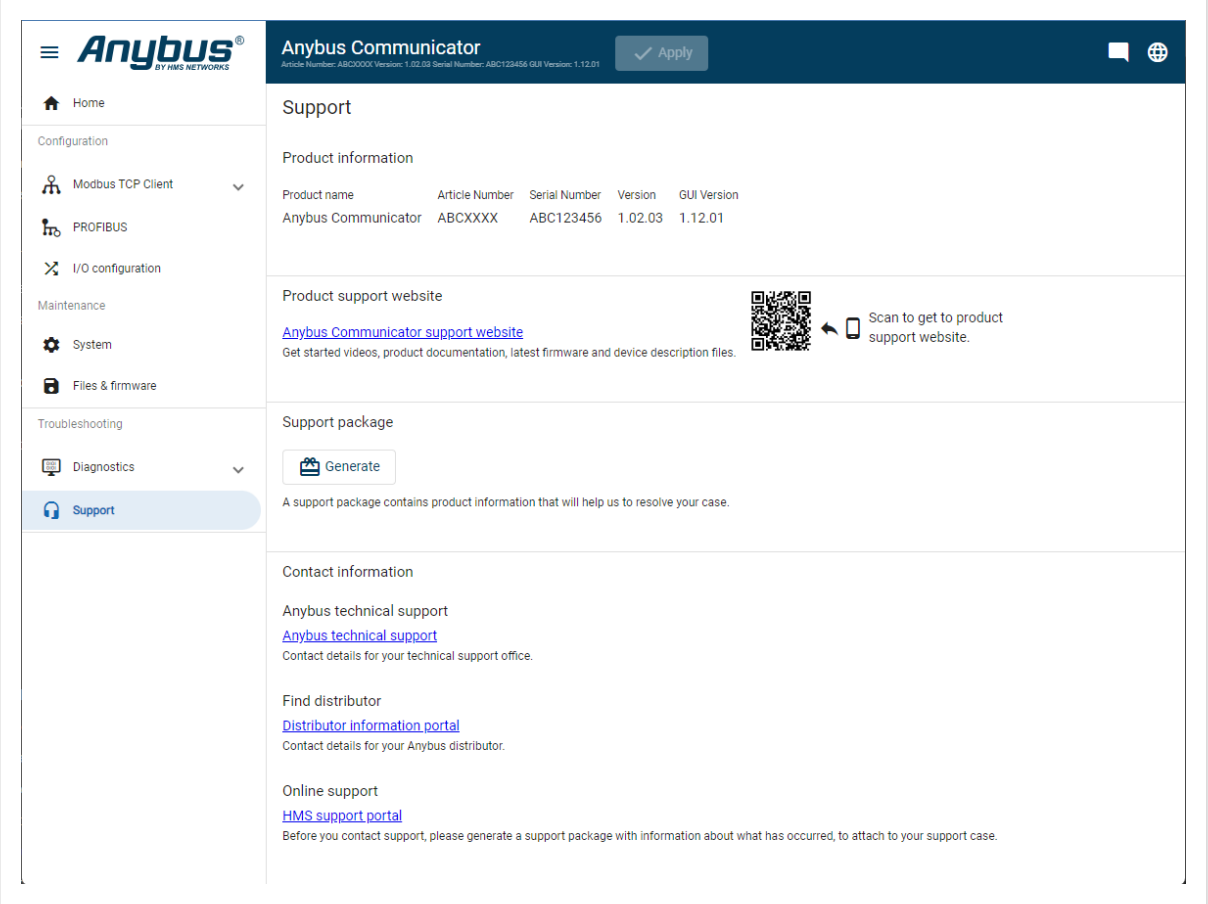


Figure 79. Support page example

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.

13. End Product Life Cycle

13.1. 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 96).

14. Technical Data

For complete technical specifications and regulatory compliance information, please visit www.hms-networks.com.

14.1. Technical Specification

Article identification	ABC3200
Configuration connector	RJ45
Communication connector	PROFIBUS DSUB connector
Modbus TCP Client connector	RJ45 x 2
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