

Anybus[®] Communicator[™] - Modbus TCP Server to Modbus TCP Client USER MANUAL

SCM-1202-229
Version 1.0
Publication date 2025-04-25



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 Server Network	17
6.5. Connect to Modbus TCP Client Network	18
6.6. Connect to Power	19
6.7. Security Switch	20
6.8. Lock the Cables	22
6.9. DIN Rail Demount	23
7. Configuration Quick Guide	25
7.1. Prepare Configuration	25
7.2. Setup New Configuration	28
7.3. PLC Configuration	30
7.4. Verify Operation	31
8. Communicator Configuration	33

8.1. Connect to Configure the Communicator	33
8.2. Access the Built-In Web Interface from HMS IPconfig	34
8.3. Access the Built-In Web Interface from a Web Browser	36
8.4. Communicator Built-In Web Interface Overview	37
8.5. Modbus TCP Client Communication Settings	38
8.5.1. To Use DHCP Server	38
8.5.2. To Configure IP Settings Manually	39
8.5.3. Naming the Host	40
8.6. Servers	41
8.6.1. Add Server	41
8.6.2. Server Properties	42
8.6.3. Add Transactions	43
8.6.4. Modbus Function Codes	44
8.6.5. Transaction Properties	45
8.6.6. Duplicate Transaction	47
8.6.7. Delete Transaction	47
8.7. Modbus TCP Server Settings	48
8.7.1. To Use DHCP Server	48
8.7.2. To Configure IP Settings Manually	49
8.7.3. Naming the Host	49
8.7.4. Timeout Time Settings	50
8.8. Modbus TCP Server Advanced Settings	51
8.8.1. Legacy Mode for Anybus Address Mode Modbus TCP	51
8.9. I/O Configuration	52
8.9.1. Map Area Object Order	53
8.9.2. Endian Swap	53
8.9.3. Convert Between Big-Endian and Little-Endian	54
8.9.4. Live List	55
8.9.5. Data Exchange Control	57
8.10. Configuration Notes	59
8.10.1. Add Configuration Note	59
8.10.2. View and Edit Configuration Notes	61
8.11. Apply Configuration	62
8.12. To Use an Existing Configuration	63
8.13. To Use a Legacy Modbus TCP Client Configuration	64
9. PLC Configuration	67
9.1. PLC Device Security	67
9.2. Modbus Addressing and Register Mapping	67
9.2.1. The Difference Between Address and Register Start	67
9.2.2. To Read and Write Data	68
9.2.3. Default Address Mode I/O Data Mapping	70
9.2.4. Legacy Address Mode I/O Data Mapping	71
10. Verify Operation	72
10.1. Communicator Status Monitor	72
10.2. Communicator LED Indicators	74
10.3. Ethernet LED Indicators	76
11. Maintenance	77
11.1. Action on Fatal Error	77
11.2. Configuration Port IP Settings	78
11.3. Configuration File Handling	79
11.3.1. Export Configuration	79
11.3.2. Import Configuration	80

11.4. Clear and Revert Configuration	81
11.5. Firmware Management	82
11.5.1. View the Firmware Version	82
11.5.2. Firmware and Configuration Compatibility	82
11.5.3. Firmware File Validation	82
11.5.4. Update Firmware	83
11.6. Change Language	84
12. Troubleshooting	85
12.1. Diagnostics	85
12.1.1. I/O Data	85
12.1.2. Event Log	86
12.1.3. LED Status	87
12.2. Reset to Factory Settings	88
12.3. Firmware Upgrade Error Management	91
12.4. Support	93
12.4.1. Support Package	93
13. End Product Life Cycle	94
13.1. Secure Data Disposal	94
14. Technical Data	95
14.1. Technical Specification	95

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 \(page 88\)](#).

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.

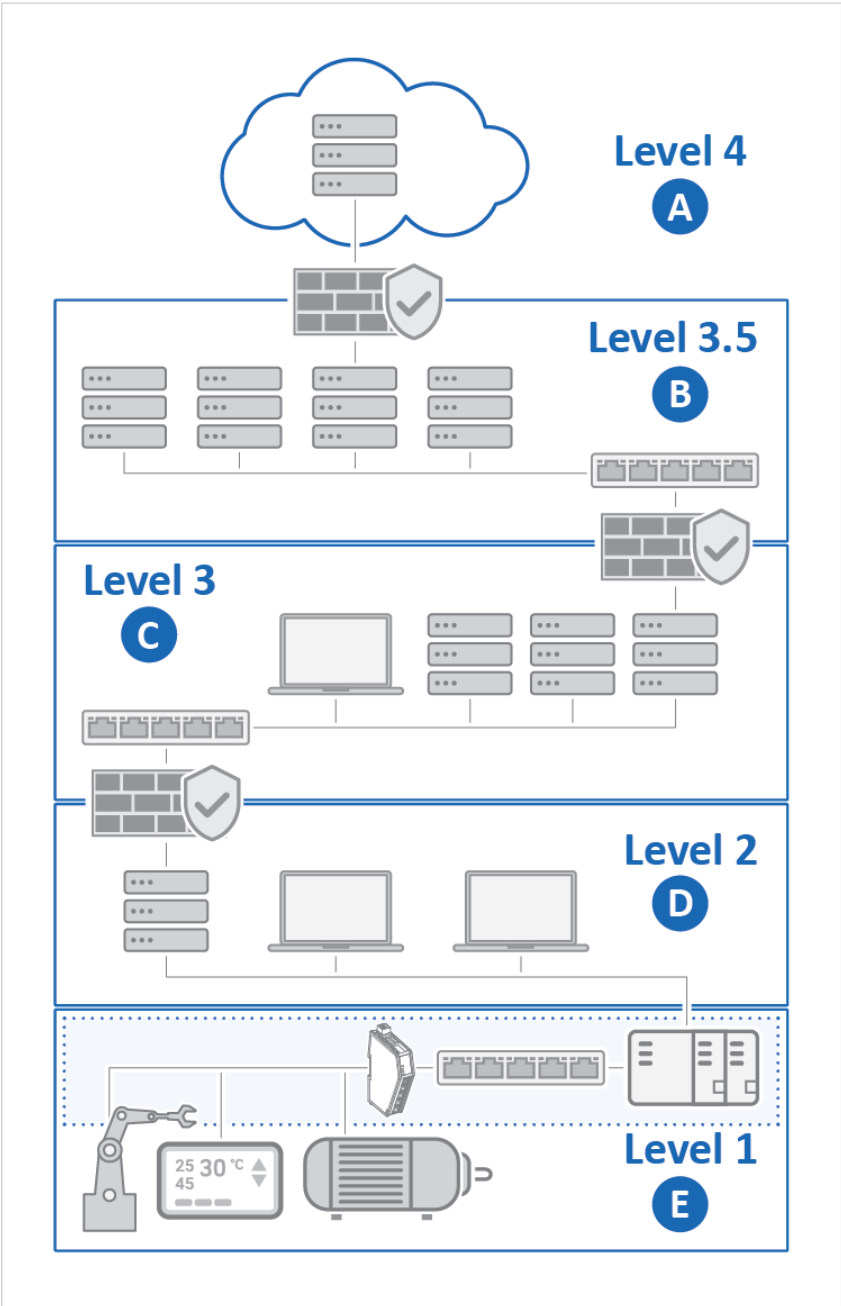


Figure 1. Purdue model, product security context

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 x 2 for connecting to the networks.

4.3. Mechanical Tools and Equipment

Have the following tools available:

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

4.4. System Requirements

4.4.1. Supported 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

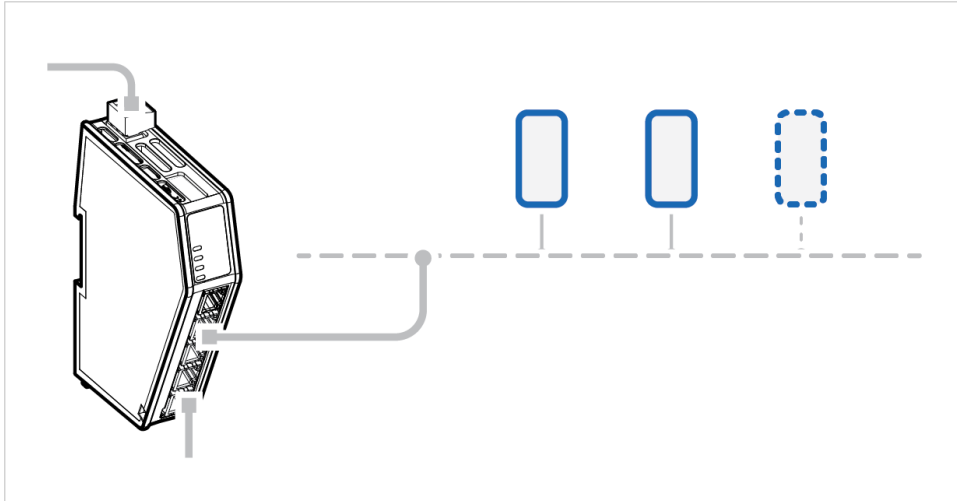


Figure 2. Servers on a Modbus TCP subnetwork

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

Servers and Transactions

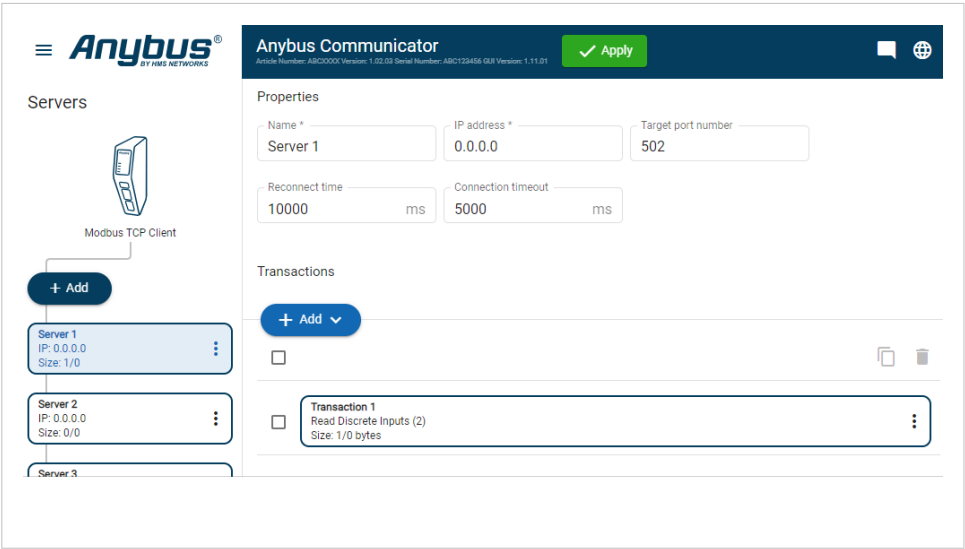


Figure 3. Server with Transactions

Transactions are based on standard Modbus transactions and define the data to be sent or received. See also [\(page 44\)](#).

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.

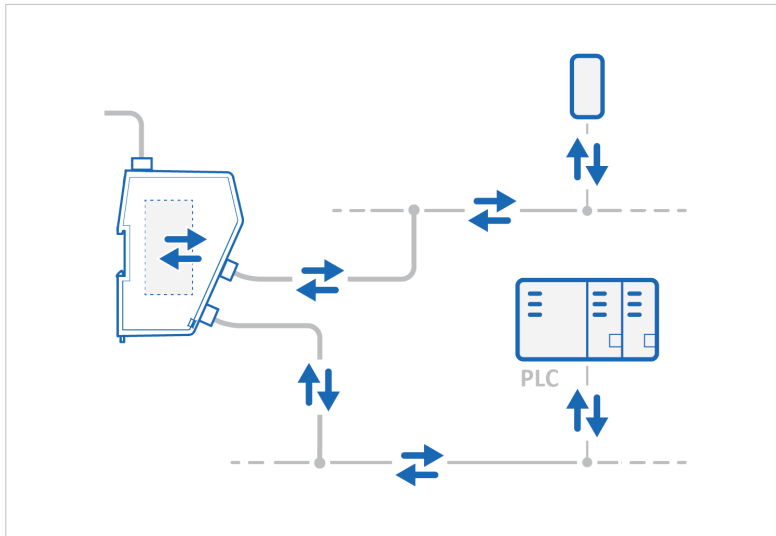


Figure 4. Process data traffic overview

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

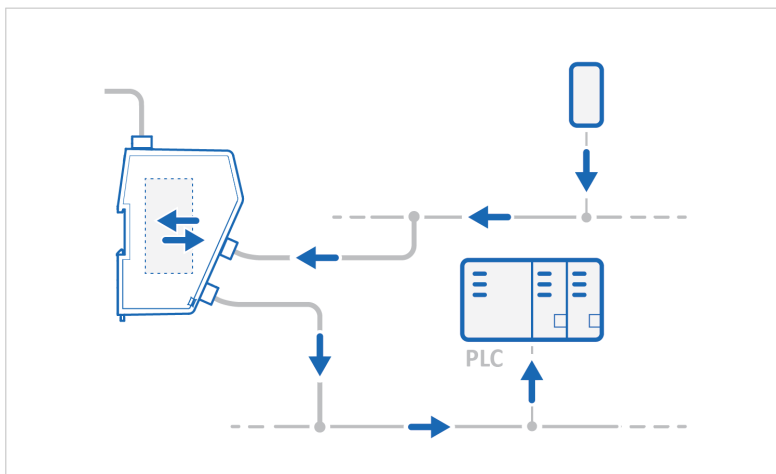


Figure 5. Process data traffic from servers to client

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

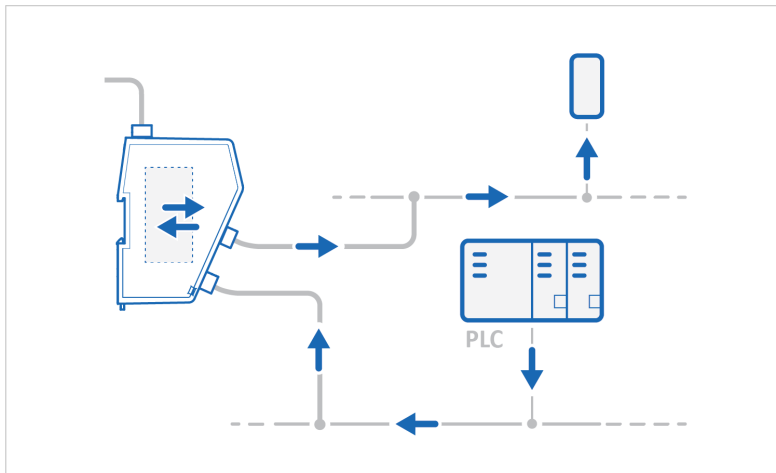


Figure 6. Process data traffic from client to servers

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

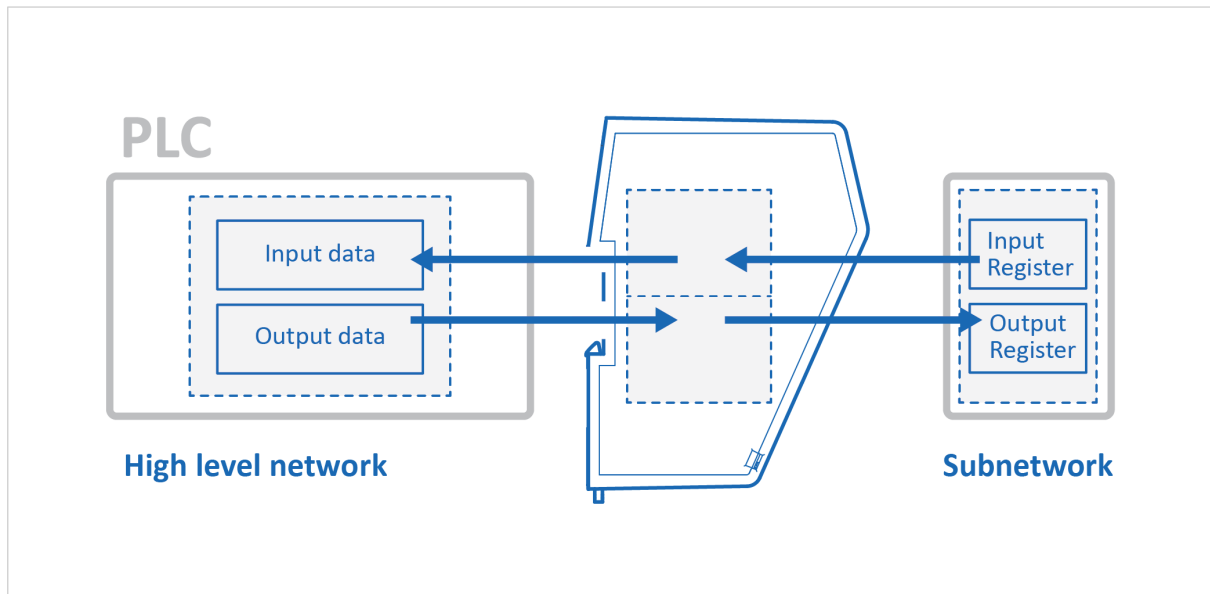


Figure 7. The Communicator internal memory areas

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

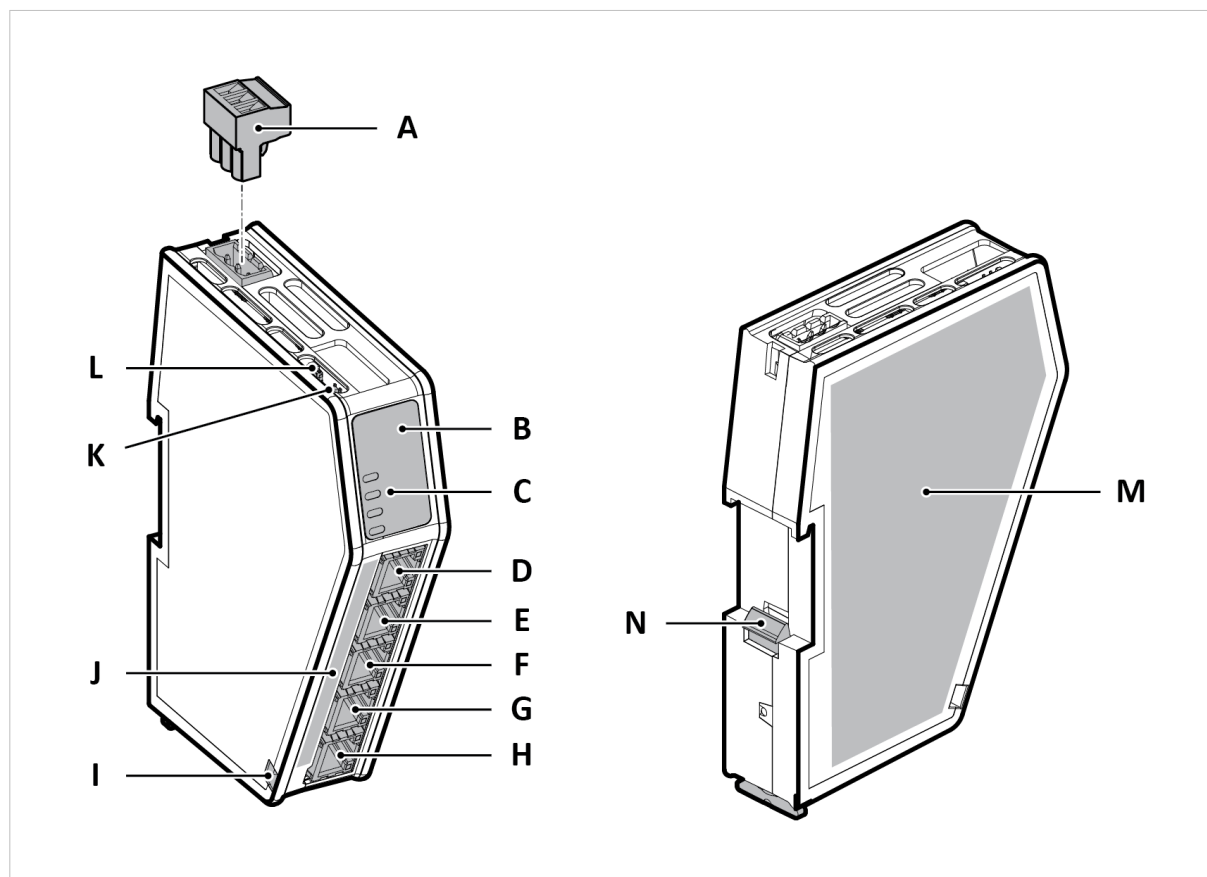


Figure 8. External parts

- | | | |
|-------------------------------|--|--|
| A. Power connector | E. Modbus TCP Client (X2.1) port | K. Security switch |
| B. Label with LED designation | F. Modbus TCP Client (X2.2) port | L. Factory reset button |
| C. Status LEDs | G. Modbus TCP Server (X3.1) port | M. Laser engraved label with product information |
| D. Configuration port (X1) | H. Modbus TCP Server (X3.2) port | N. DIN rail locking mechanism |
| | I. Cable tie mount | |
| | J. Laser engraved connectors designation | |

6.2. Connector Port Guide

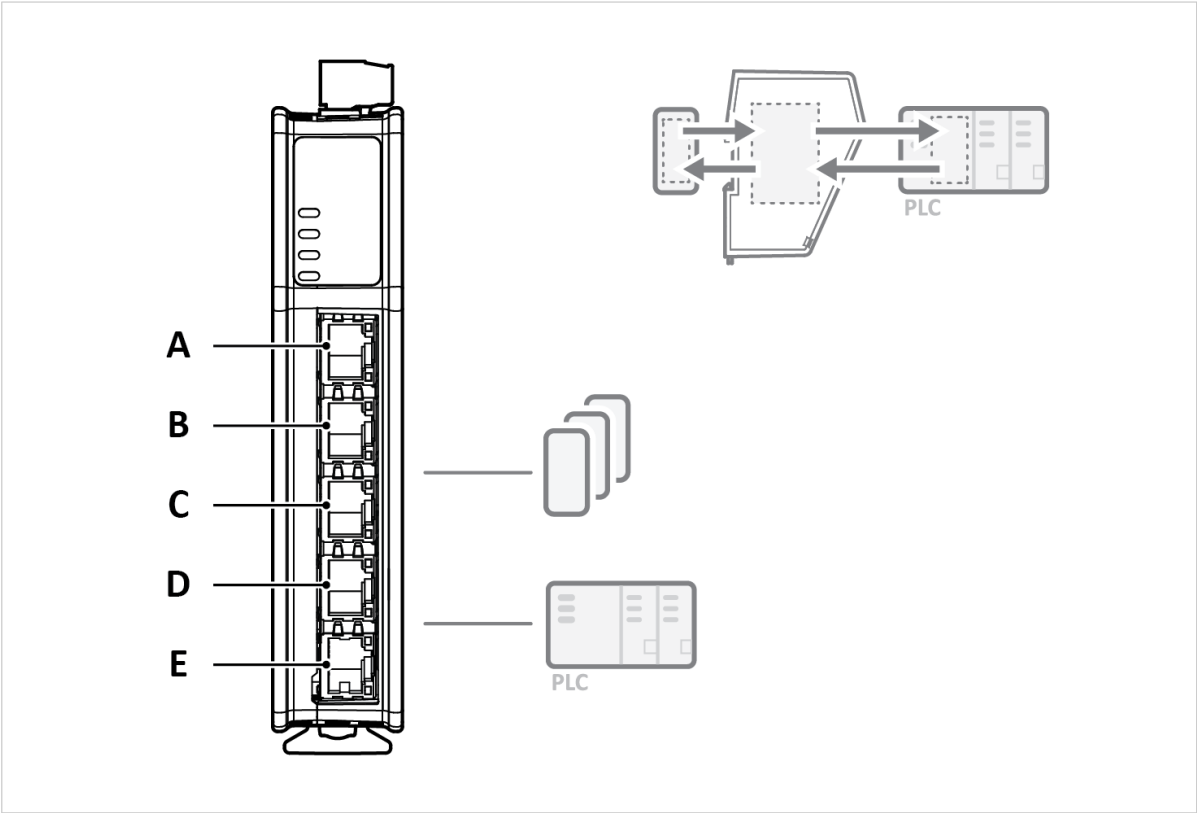


Figure 9. Communicator connector ports

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

See also [Connect to Modbus TCP Server Network \(page 17\)](#) and [Connect to Modbus TCP Client Network \(page 18\)](#).

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.

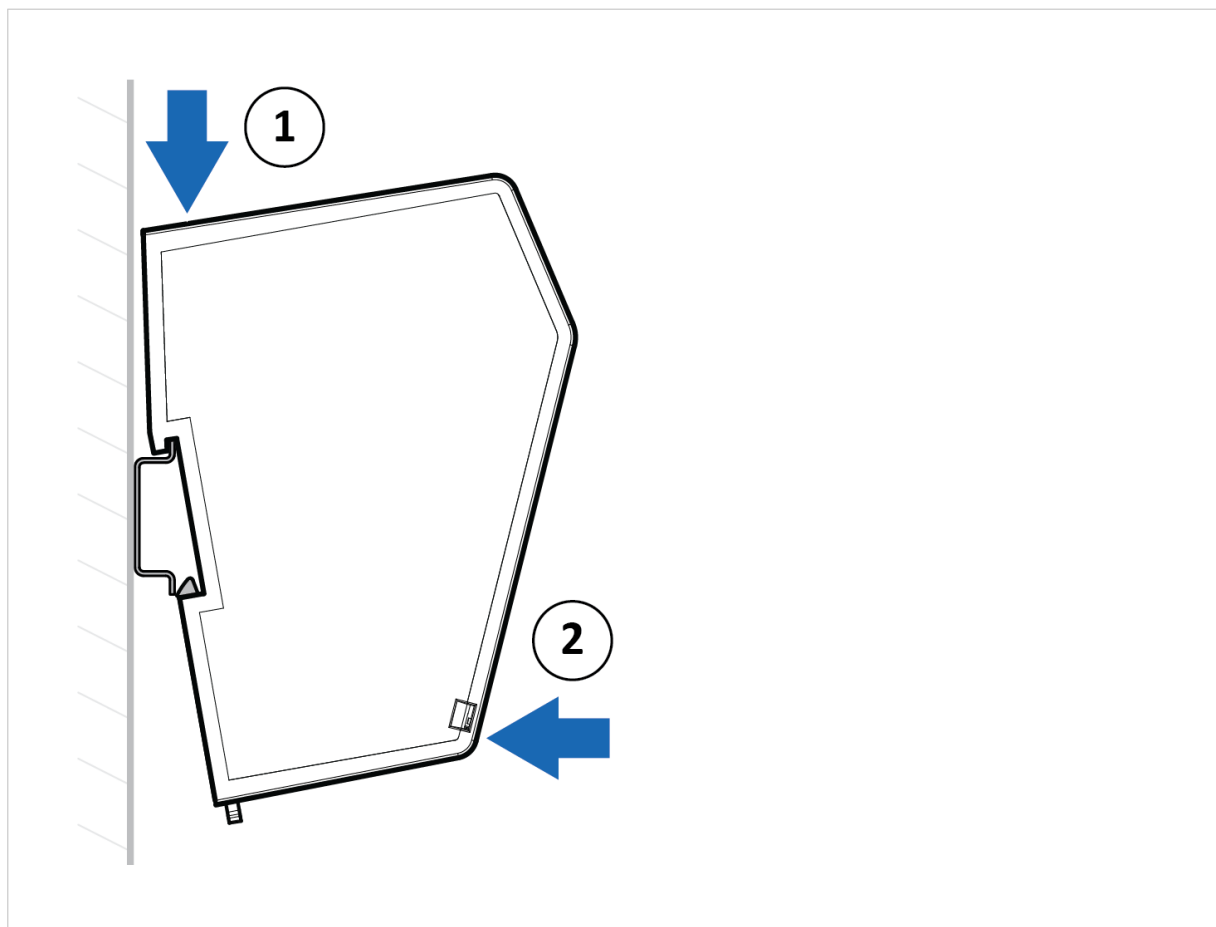


Figure 10. Attach the Communicator on the DIN rail

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 Server Network

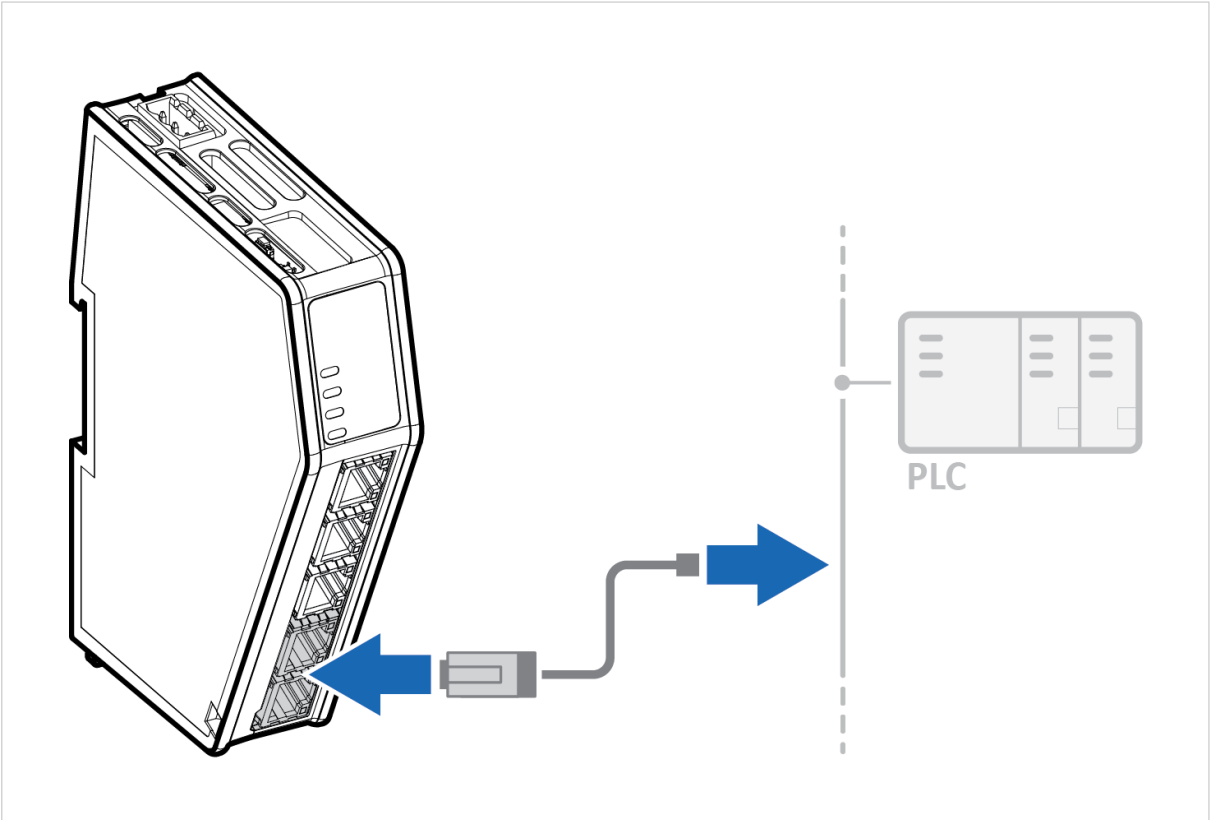
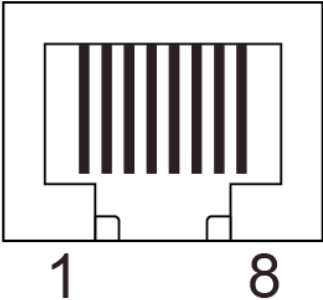


Figure 11. Connect to Modbus TCP Server network

Procedure

Connect the Communicator to your Modbus TCP Server 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

6.5. Connect to Modbus TCP Client Network

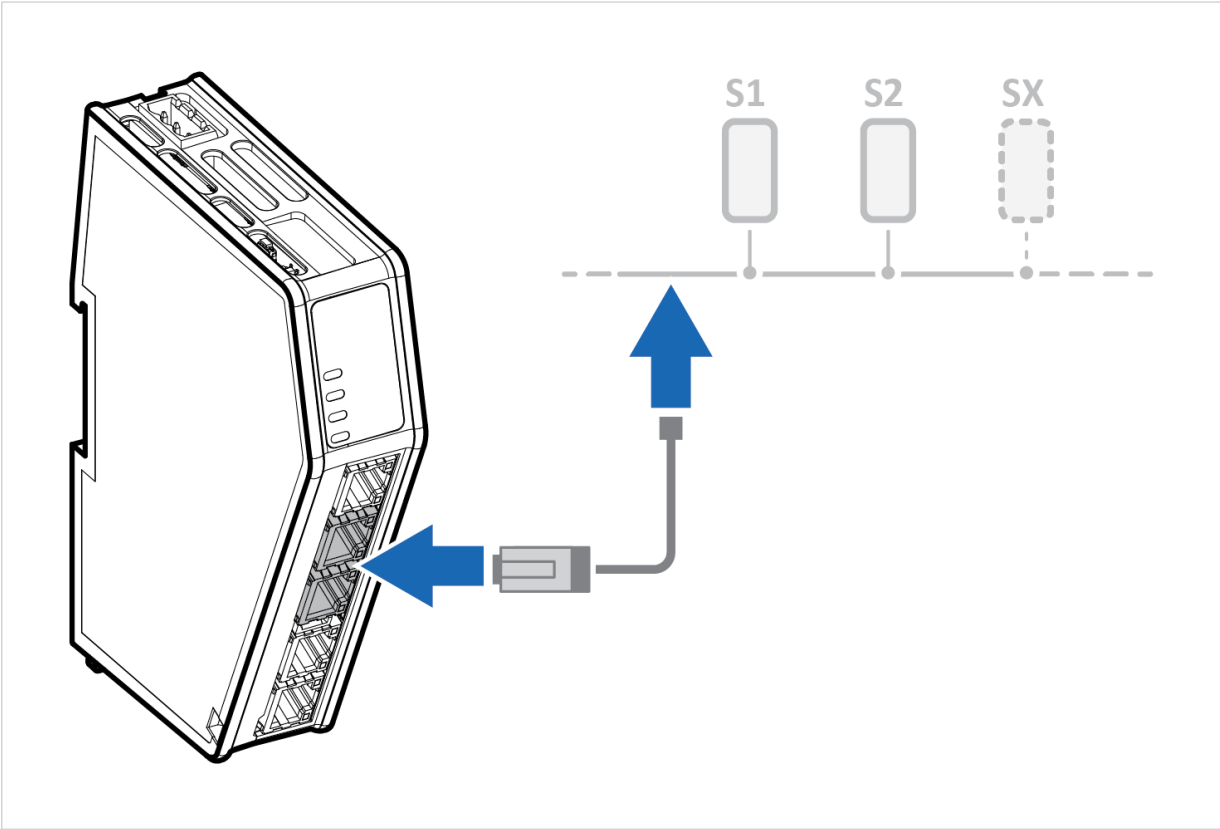
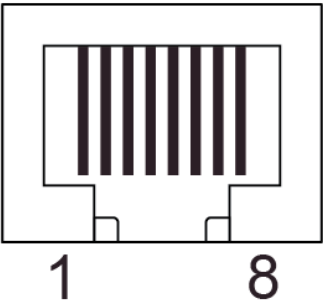


Figure 12. Connect to Modbus TCP Client network


Procedure


Connect the Communicator to your 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

6.6. 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.

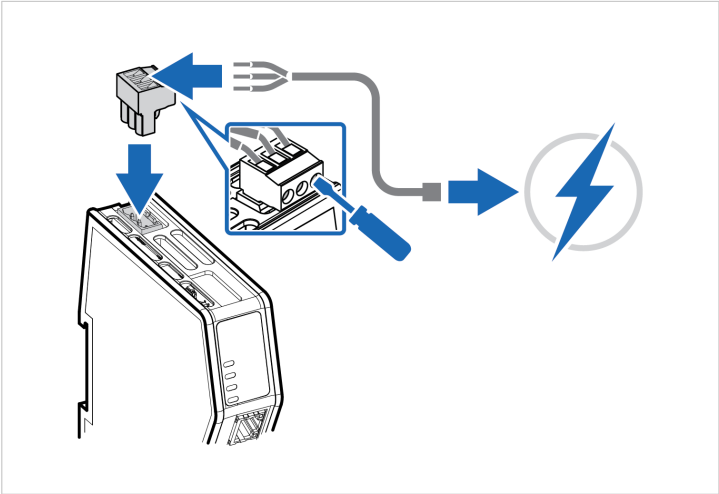
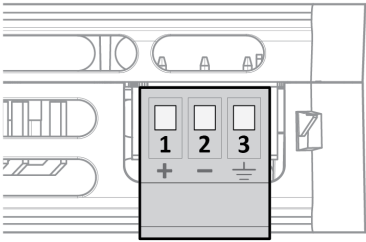


Figure 13. Connect to power

Power Connector Pinout

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

Procedure

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

6.7. 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

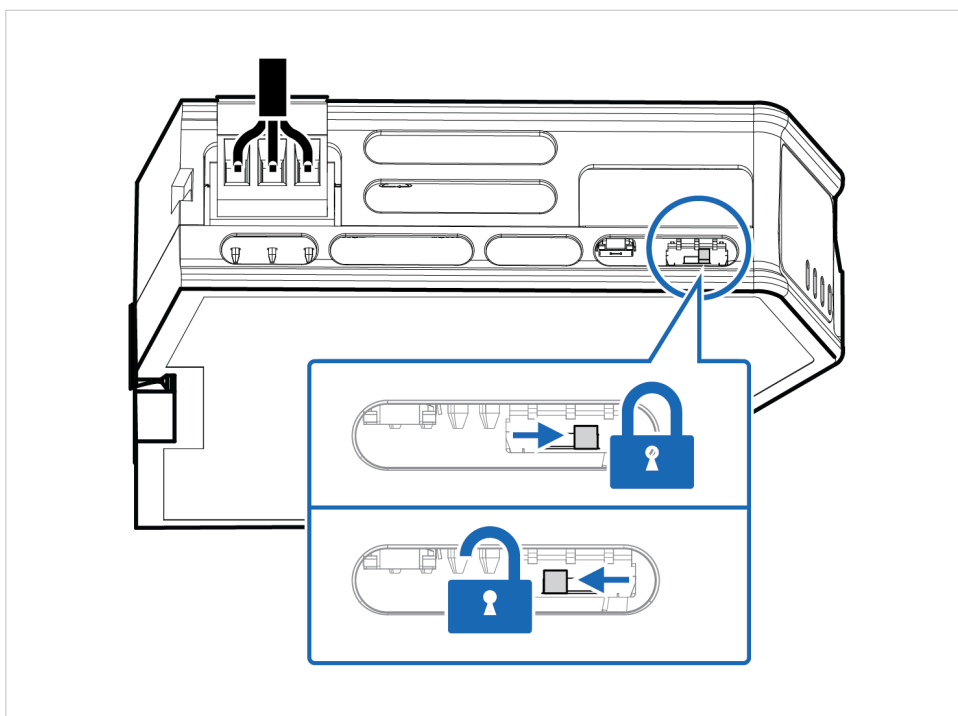


Figure 14. Security switch in locked and unlocked position

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

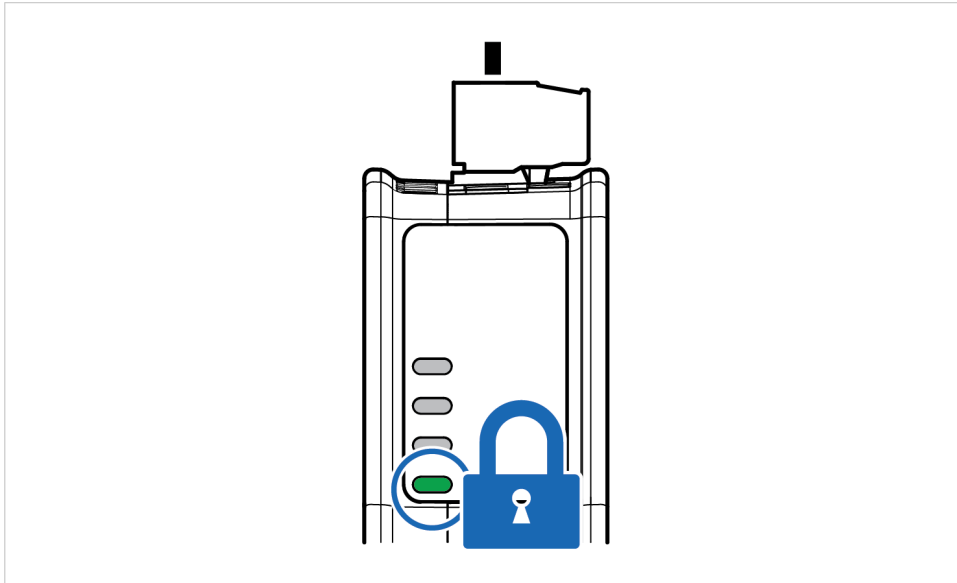


Figure 15. Security switch locked status LED

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.

6.8. Lock the Cables

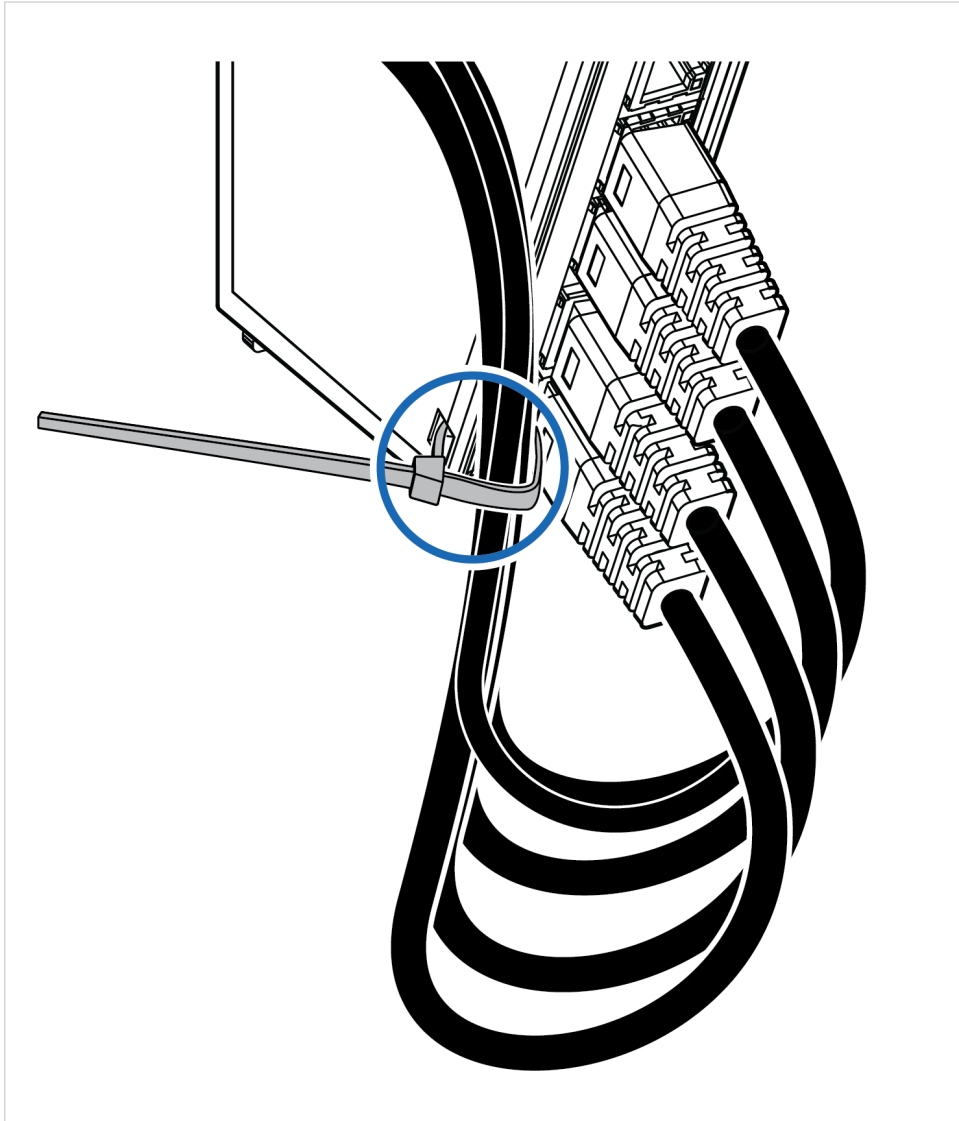


Figure 16. Lock the cables

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

6.9. DIN Rail Demount

Before You Begin

**IMPORTANT**

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

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

Procedure

Remove the Communicator from the DIN rail:

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

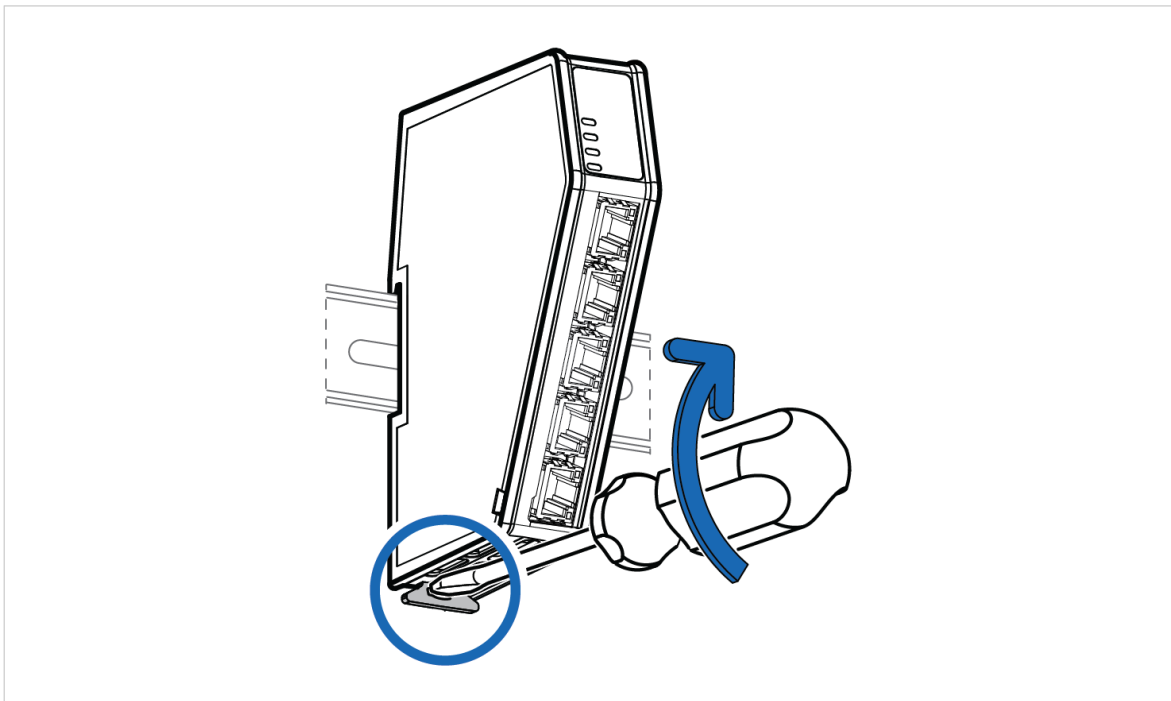


Figure 17. Unlock the Communicator

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

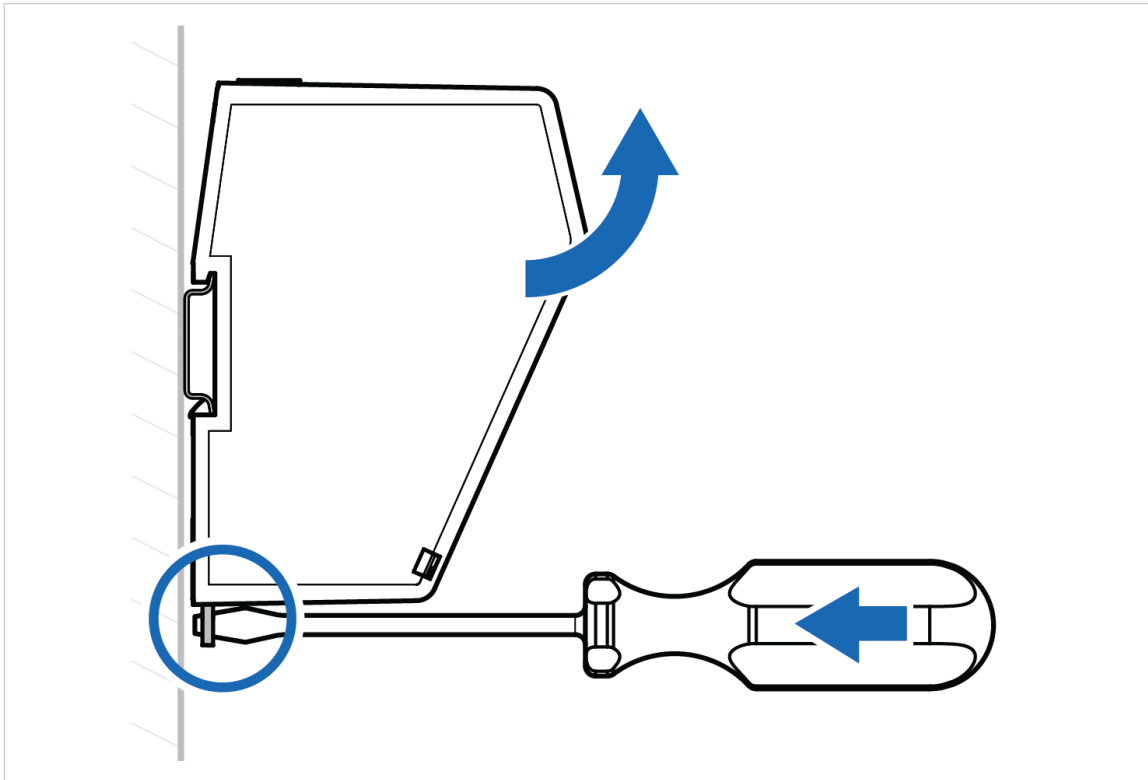


Figure 18. Unhook the Communicator

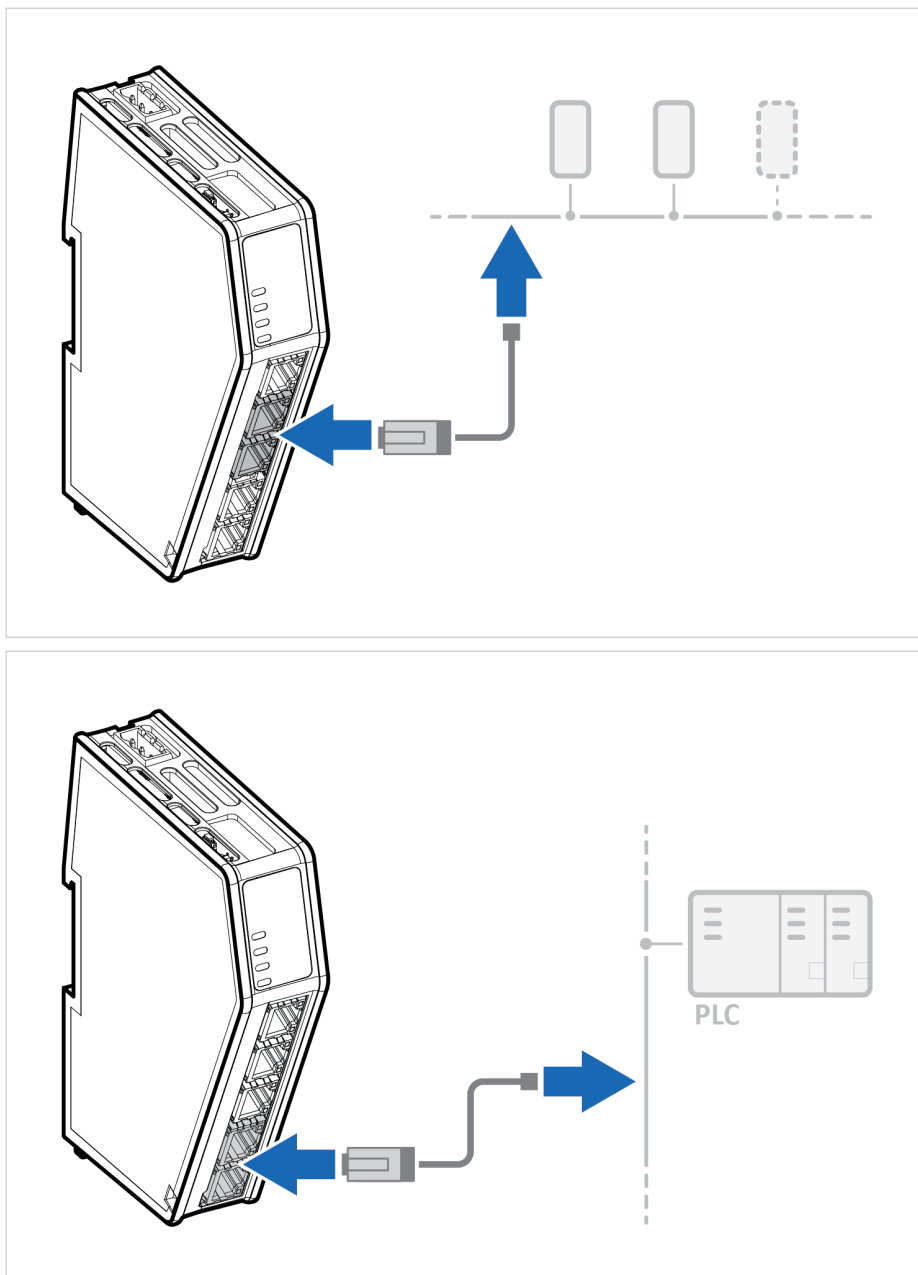
7. Configuration Quick Guide

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

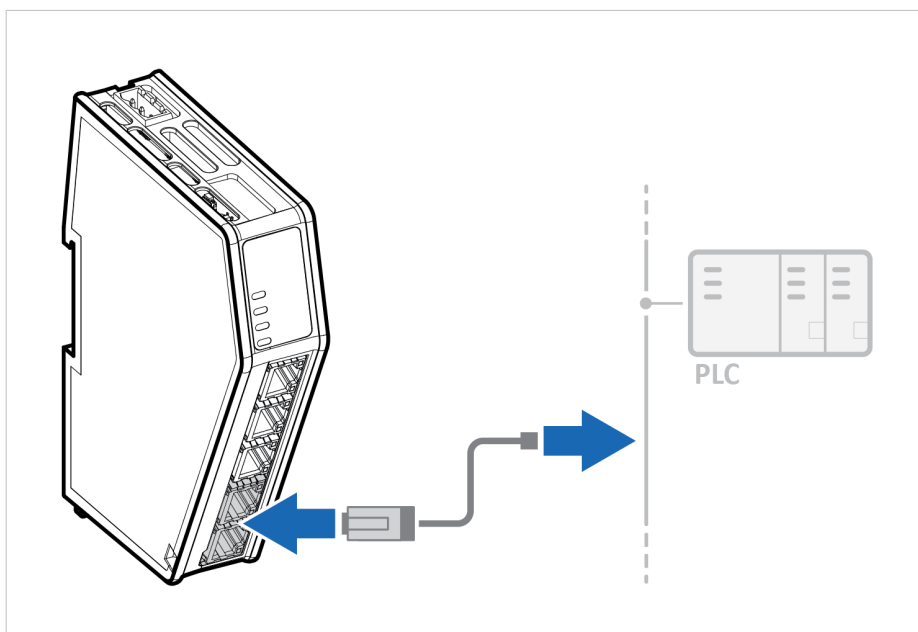
For detailed information, please refer to [Communicator Configuration \(page 33\)](#).

7.1. Prepare Configuration

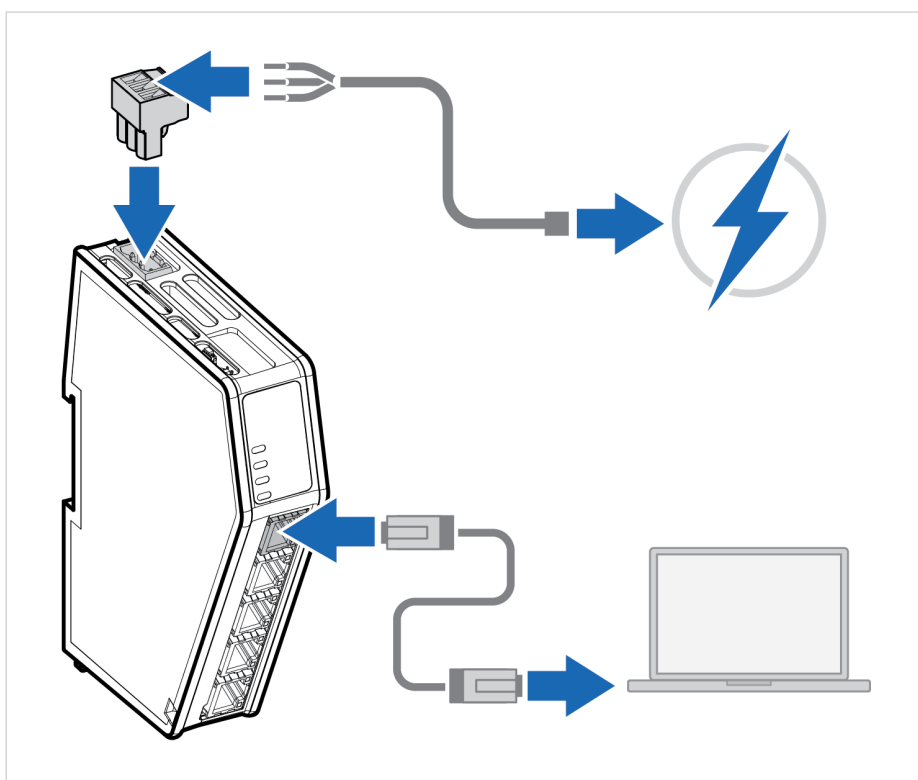
1. **Connect the Communicator to the Modbus TCP Client subnetwork**



2. Connect Communicator to the Modbus TCP Server network.





3. Connect to PC and power

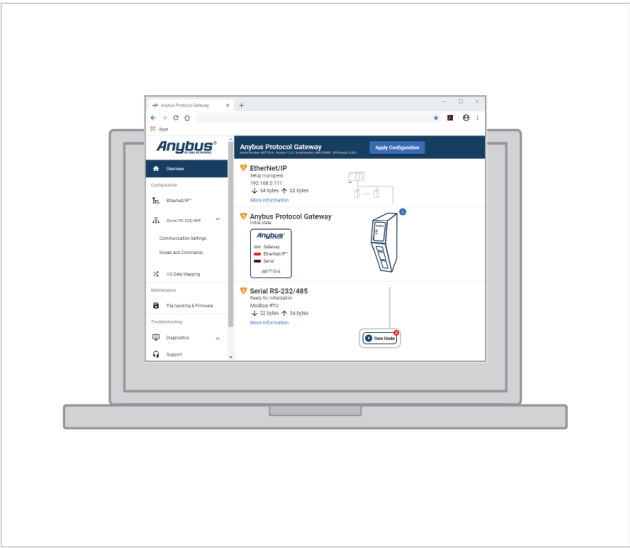


- Connect an Ethernet cable between the Communicator configuration port and your PC.
- Connect the Communicator to a power supply.

4. Find the Communicator on your PC
The Communicator default IP address is 192.168.0.10.

Option 1	Option 2
<div></div> <p>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.</p>	<div></div> <p>Change the IP address on the Communicator configuration port to one within the same IP address range as your PC.</p> <p>Use the software application HMS IPconfig to find the Communicator default IP address on your PC.</p> <p>Download the installation files and user documentation from www.hms-networks.com/technical-support.</p>

5. Access the Communicator built-in web interface



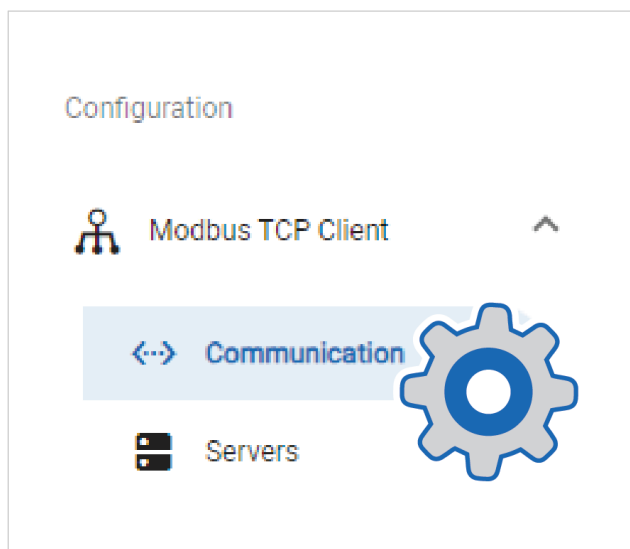
Open the Communicator built-in web interface in HMS IPconfig or enter the Communicator IP address in your web browser.

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

7.2. Setup New Configuration

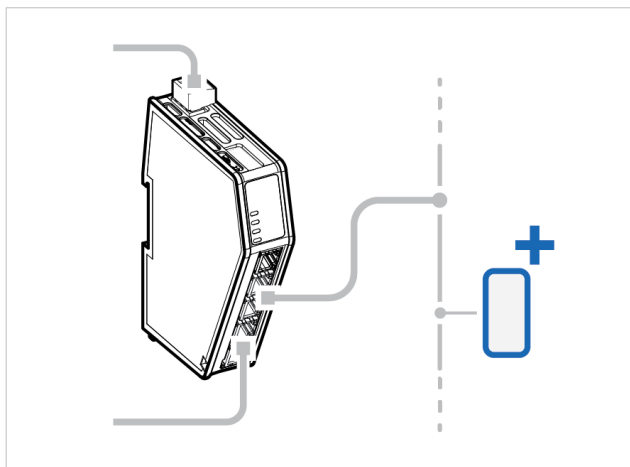
Follow these steps to setup a new Communicator configuration.

1. Subnetwork configuration



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

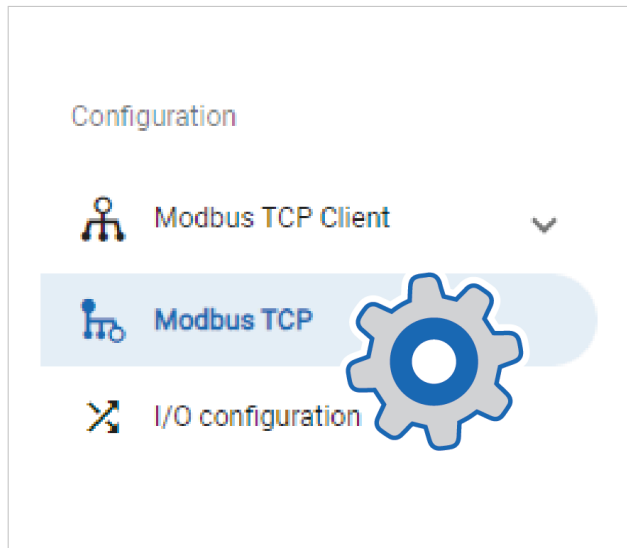
2. Add Servers



On the **Servers** page:

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

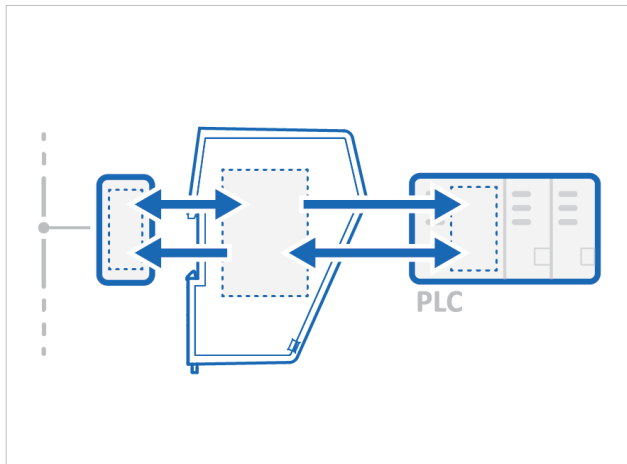
3. High level network configuration



On the **Modbus TCP Server** page:

1. Enable DHCP server or choose to set a specific IP address.
2. Configure the Timeout times settings.

4. I/O Configuration

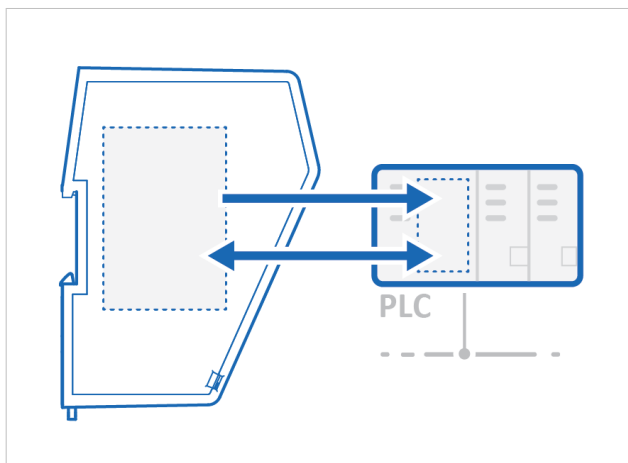


The transaction(s) for each server is automatically mapped to the Communicator internal memory area. On the **I/O configuration** page, view the mapping relation between the server connections and the layout on the process data area.

7.3. PLC Configuration

In the PLC program:

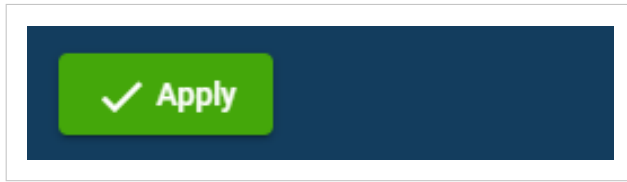
1. **Import product file**
Option if the PLC program requires an N/A file.
Import the N/A file into your PLC project.
2. **Configure the communication**



Configure the PLC to communicate with the Communicator according to the I/O data map created in the Communicator.

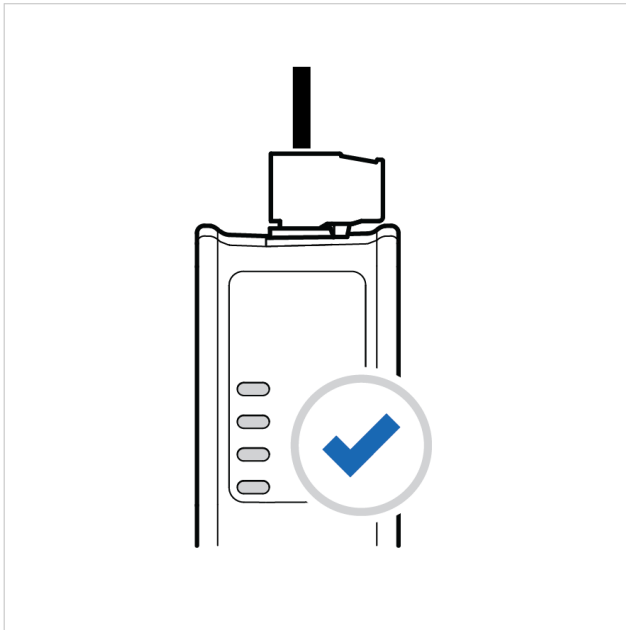
7.4. Verify Operation

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:

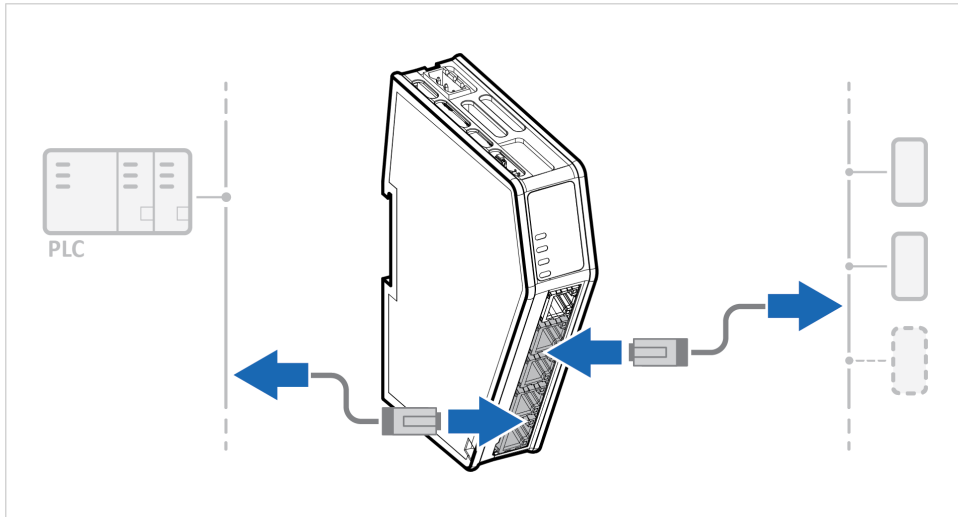
- **I/O data** page to monitor how the data flow between the **Modbus TCP Client** side and the **Modbus TCP Server** side, including any configured endian conversions.
- **Event log** page to detect failures and unexpected behavior over time.

8. Communicator Configuration

8.1. Connect to Configure the Communicator

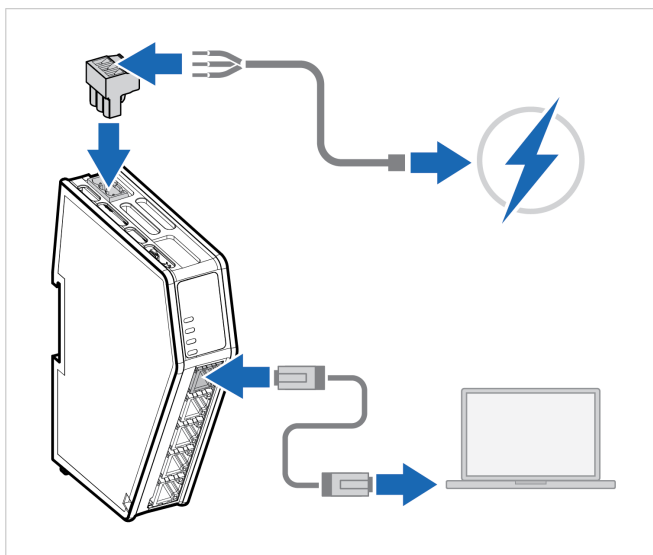
Procedure

Connect to Modbus TCP Client network and Modbus TCP Server network



1. Connect the Communicator to the high level network.
2. Connect the Communicator to the subnetwork.

Connect to PC and Power



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

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

Before You Begin

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



NOTE

The Communicator default IP address is 192.168.0.10.



NOTE

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



NOTE

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



NOTE

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

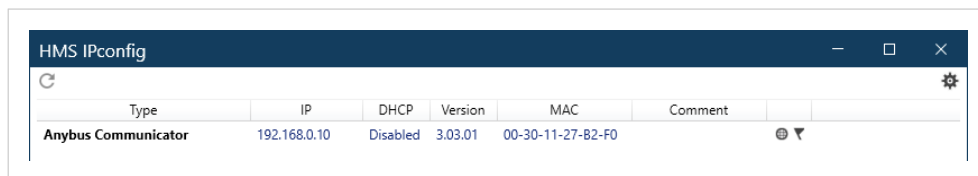


TIP

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

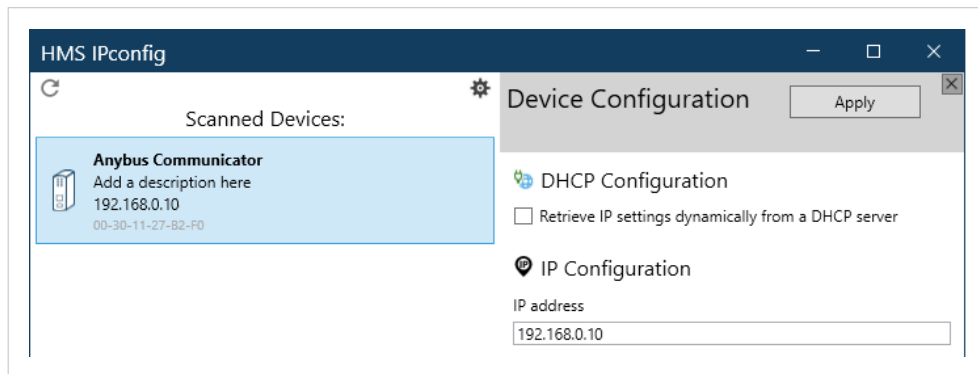
Procedure

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

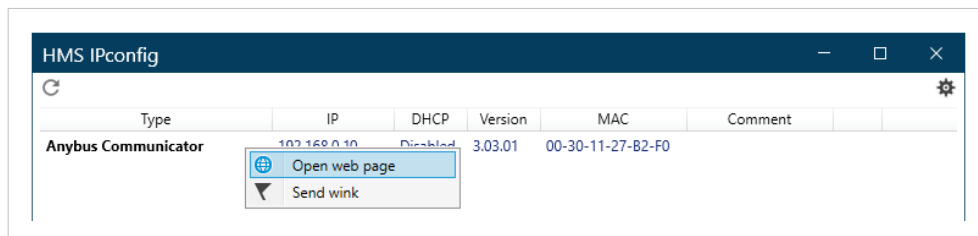


- HMS IPconfig automatically starts scanning for compatible and active HMS devices.
 - Found HMS devices are added to the device list.
3. To open the settings pane, click on the Communicator in the device list.

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

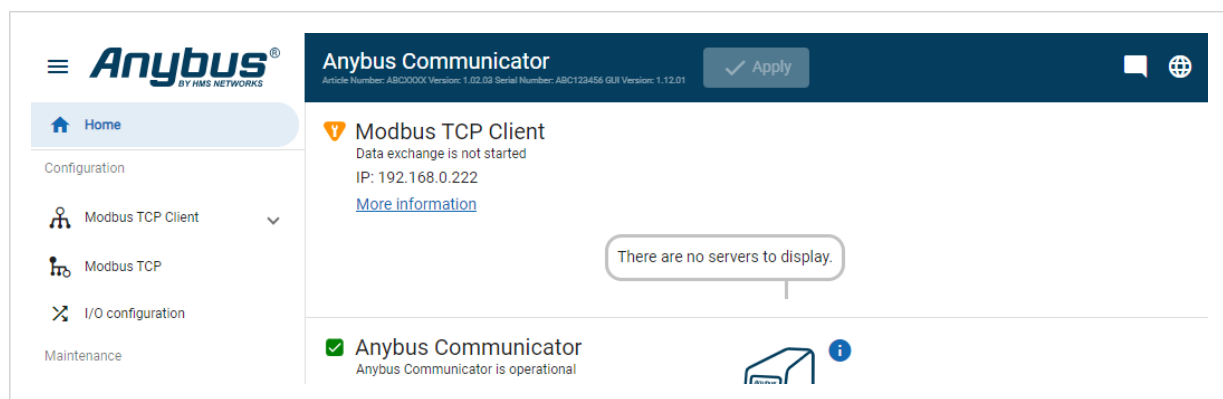


5. To open the **Open web page** built-in web interface, click Communicator.



Result

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



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

Before You Begin

**NOTE**

The Communicator configuration port default IP address is 192.168.0.10.

**NOTE**

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

**NOTE**

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

**TIP**

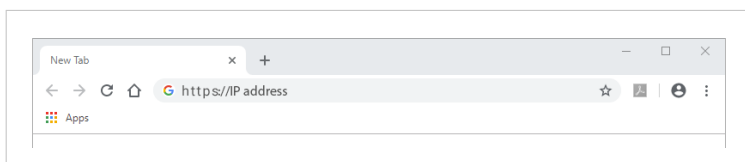
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System > Configuration port** page.

Procedure

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



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



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



8.4. Communicator Built-In Web Interface Overview

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

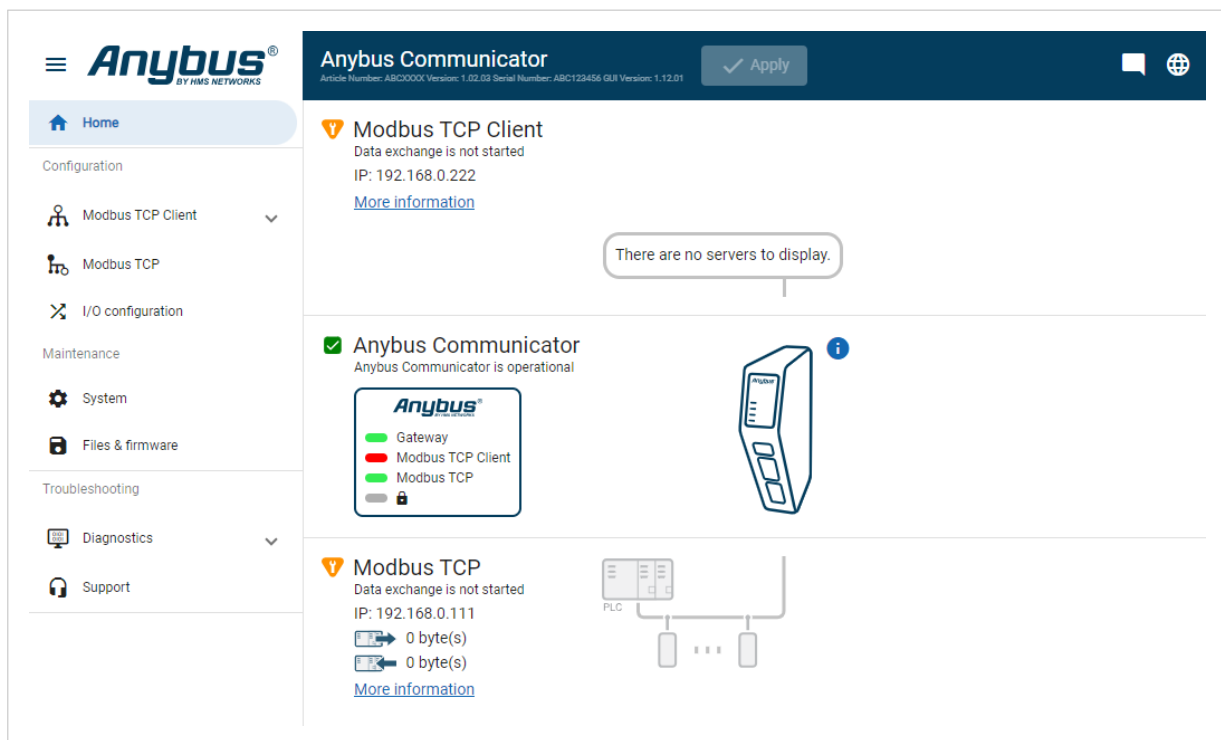


Figure 19. The Communicator built-in web interface Home page

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.
Modbus TCP Server	Configure the network settings for the Modbus TCP Server 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

8.5.1. To Use DHCP Server

Anybus Communicator

Article Number: ABCXXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.18.01

✓ Apply



IP Settings

☒ DHCP enabled

IP address*

192.168.0.222

Subnet mask*

255.255.255.0

Default gateway*

0.0.0.0

Primary DNS

0.0.0.0

Secondary DNS

0.0.0.0

Hostname

Figure 20. IP Settings, DHCP enabled

By default, the IP settings are provided by the high level network DHCP server. The **DHCP enabled** checkbox is selected.

Default Communicator IP Settings

The Communicator comes with the following factory default IP settings:



Setting	Default value
DHCP	Enabled
IP address	There is no default IP address.
Subnet mask	There is no default Subnet mask.
Gateway address	There is no default Gateway address.
Primary DNS server	There is no default Primary DNS server.
Secondary DNS server	There is no default Secondary DNS server.
Hostname	You can label the Communicator. Maximum length is 64 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Hostname as one single word.

8.5.2. To Configure IP Settings Manually

Anybus Communicator

Article Number: ABCXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.18.01

✓ Apply



IP Settings

☐ DHCP enabled

IP address*

192.168.0.222

Subnet mask*

255.255.255.0

Default gateway*

0.0.0.0

Primary DNS

0.0.0.0

Secondary DNS

0.0.0.0

Hostname

Figure 21. Modbus TCP Client IP Settings, DHCP disabled

- 1. Ensure that the **DHCP enabled** checkbox is deselected.
- 2. Configure the IP settings.

Setting	Description
IP address	The Modbus TCP Client network IP address in IPv4 dot-decimal notation
Subnet mask	The Modbus TCP Client network Subnet mask in IPv4 dot-decimal notation.
Gateway address	The Modbus TCP Client 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	The Modbus TCP Client network Primary DNS in IPv4 dot-decimal notation.
Secondary DNS server	The Modbus TCP Client network Secondary DNS in IPv4 dot-decimal notation.
DHCP	Enabled
Hostname	You can label the Communicator. Maximum length is 64 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Hostname as one single word.

8.5.3. Naming the Host

Anybus Communicator
Article Number: ABCXXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.18.01

✓ Apply

IP Settings

☒ DHCP enabled

IP address* 192.168.0.222 Subnet mask* 255.255.255.0 Default gateway* 0.0.0.0

Primary DNS 0.0.0.0 Secondary DNS 0.0.0.0

Hostname

Figure 22. IP Settings Hostname

You can label the Communicator.

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

8.6. 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 23. Modbus TCP Client, Server page

3. Repeat until you have added all your servers.

To Do Next

Configure the server Properties, see [Server Properties \(page 42\)](#).

8.6.2. Server Properties

Procedure

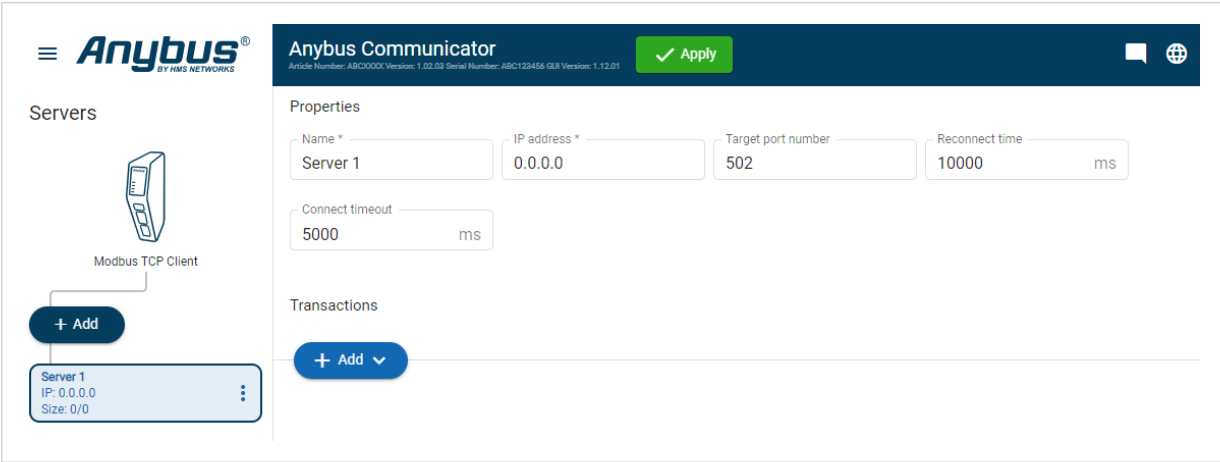


Figure 24. Servers page, Properties

- 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 \(page 43\)](#).

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.

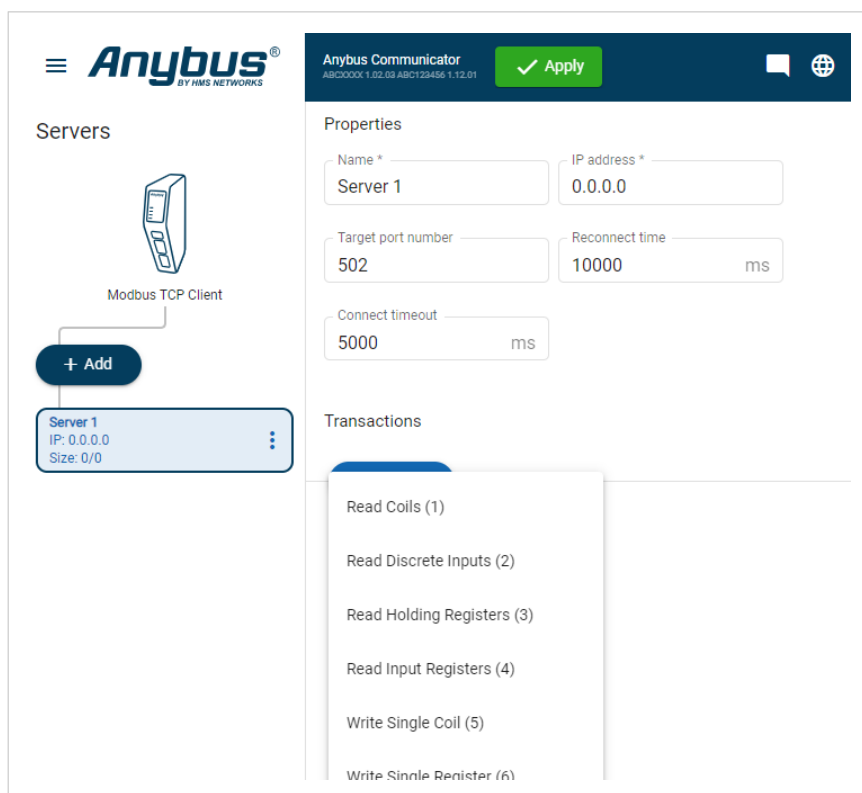


Figure 25. Add Modbus transactions

3. Repeat until you have added all your transactions.

To Do Next

Configure the transaction Properties settings, [Transaction Properties \(page 45\)](#).

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 \(page 44\)](#).

Procedure

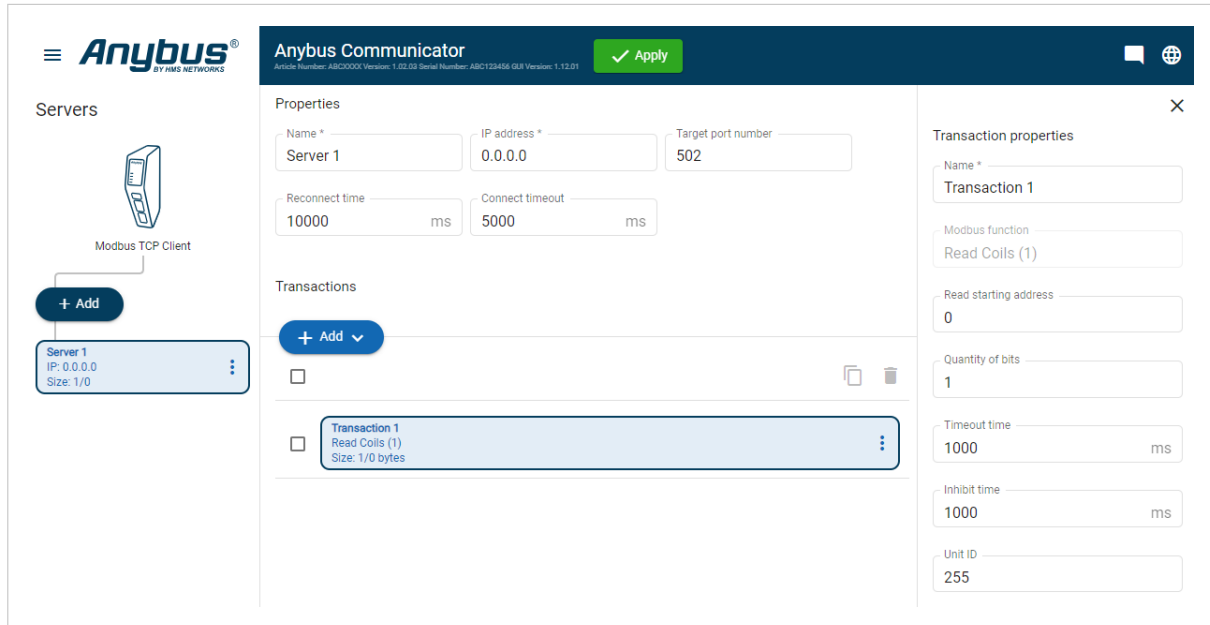


Figure 26. Transaction properties

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.

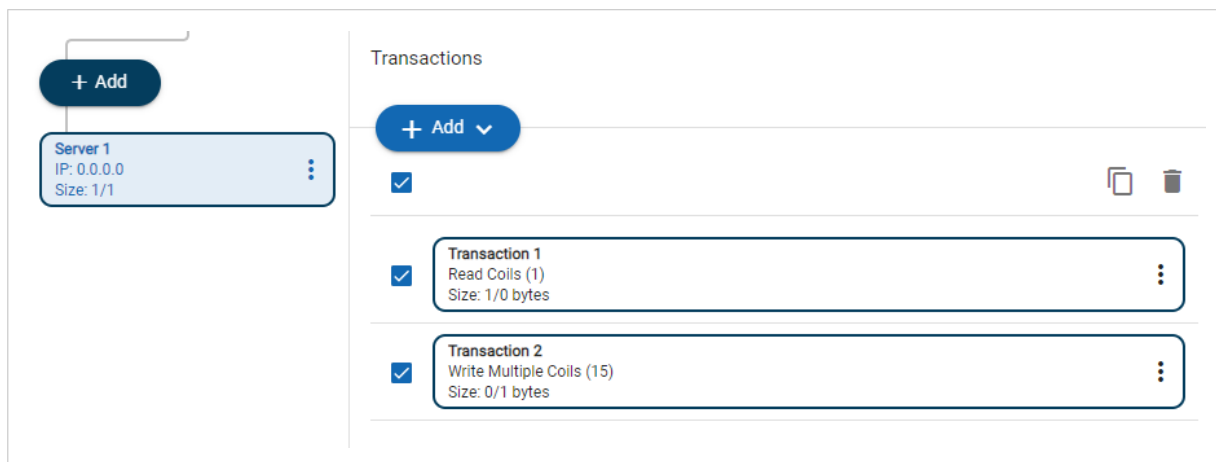


Figure 27. Duplicate transaction

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.

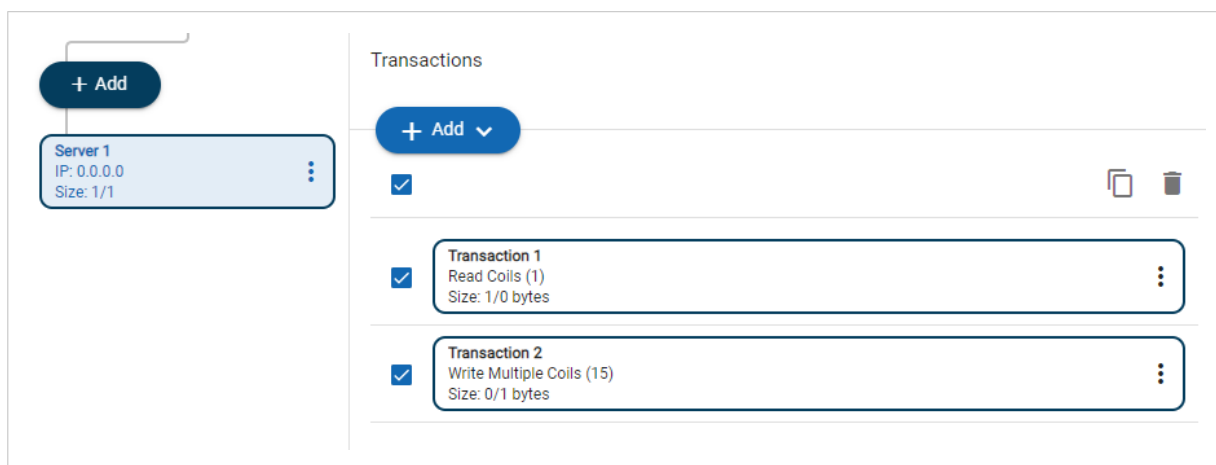


Figure 28. Delete transaction

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. Modbus TCP Server Settings

8.7.1. To Use DHCP Server

Anybus Communicator

Article Number: ABCXXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.18.01

✓ Apply



IP Settings

☒ DHCP enabled

IP address*

192.168.0.222

Subnet mask*

255.255.255.0

Default gateway*

0.0.0.0

Primary DNS

0.0.0.0

Secondary DNS

0.0.0.0

Hostname

Figure 29. IP Settings, DHCP enabled

By default, the IP settings are provided by the high level network DHCP server. The **DHCP enabled** checkbox is selected.

Default Communicator IP Settings

The Communicator comes with the following factory default IP settings:



Setting	Default value
DHCP	Enabled
IP address	There is no default IP address.
Subnet mask	There is no default Subnet mask.
Gateway address	There is no default Gateway address.
Primary DNS server	There is no default Primary DNS server.
Secondary DNS server	There is no default Secondary DNS server.
Hostname	You can label the Communicator. Maximum length is 64 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Hostname as one single word.

8.7.2. To Configure IP Settings Manually

Anybus Communicator

Article Number: ABCXXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.18.01

✓ Apply



IP Settings

☐ DHCP enabled

IP address*
192.168.0.222

Subnet mask*
255.255.255.0

Default gateway*
0.0.0.0

Primary DNS
0.0.0.0

Secondary DNS
0.0.0.0

Hostname

Figure 30. Modbus TCP Server IP Settings, DHCP disabled

- 1. Deselect the **DHCP enabled** checkbox.
- 2. Configure the IP settings.

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

8.7.3. Naming the Host

Anybus Communicator

Article Number: AB7710-A Version: 1.2.3 Serial Number: ABC123456 GUI Version: 0.44.1

✓ Apply

Hostname

Figure 31. Modbus TCP Server page, IP Settings Hostname

You can label the Communicator.

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

8.7.4. Timeout Time Settings

Anybus®

BY HMS NETWORKS

Home

Configuration

Modbus TCP Client

Modbus TCP

I/O configuration

Maintenance

System

Files & firmware

Troubleshooting

Diagnostics

Support

Anybus Communicator

✓ Apply

ABC000K 1.02.03 ABC123456 1.12.01

Modbus TCP

IP Settings

☐ DHCP enabled

IP address *

192.168.0.111

Subnet mask *

255.255.255.0

Gateway address *

192.168.0.1

Primary DNS

0.0.0.0

Secondary DNS

0.0.0.0

Hostname

Timeout times

Connection timeout *

60

s

Process data active timeo...

0

ms

Advanced settings

☐ Anybus Address Mode

In this mode, several Modbus function codes can be used to access the same data allowing for more flexibility.

Figure 32. Modbus TCP Server page, Timeout times

Process Data Active Timeout

If this time is exceeded, the Modbus TCP Client network is considered to be offline.

The data sent to the Modbus TCP Server network is frozen.

A value of 0 disables this feature, i.e. the Modbus TCP Client network can never go offline.

The default value is 0 ms.

8.8. Modbus TCP Server Advanced Settings



NOTE

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

8.8.1. Legacy Mode for Anybus Address Mode | Modbus TCP

Advanced settings option for Modbus TCP.

About Legacy Mode

Use Legacy Mode when you want to make a new Communicator compatible with the X-gateway Anybus Address Mode.

See also [Legacy Address Mode I/O Data Mapping \(page 71\)](#).

To Use Legacy Mode

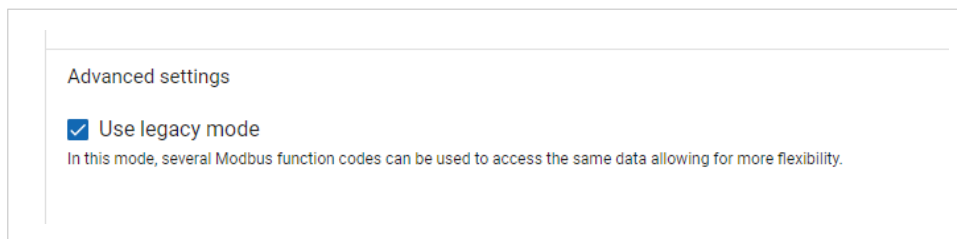


Figure 33. Advanced settings > Use legacy mode

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

8.9. I/O Configuration

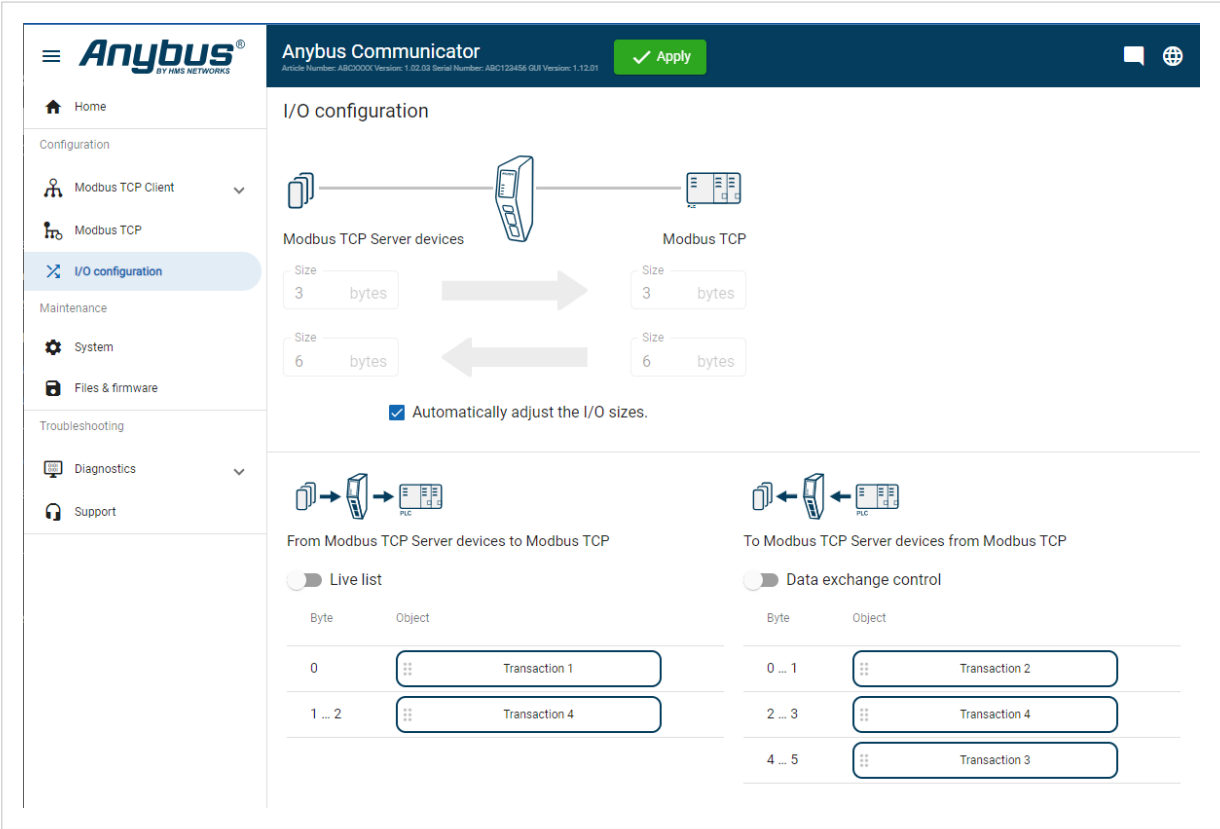


Figure 34. I/O configuration page

On the **I/O configuration** page the data communication between the Modbus TCP Server devices and the Modbus TCP Server 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 **Modbus TCP Server** page are configured.

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

I/O Size Settings

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

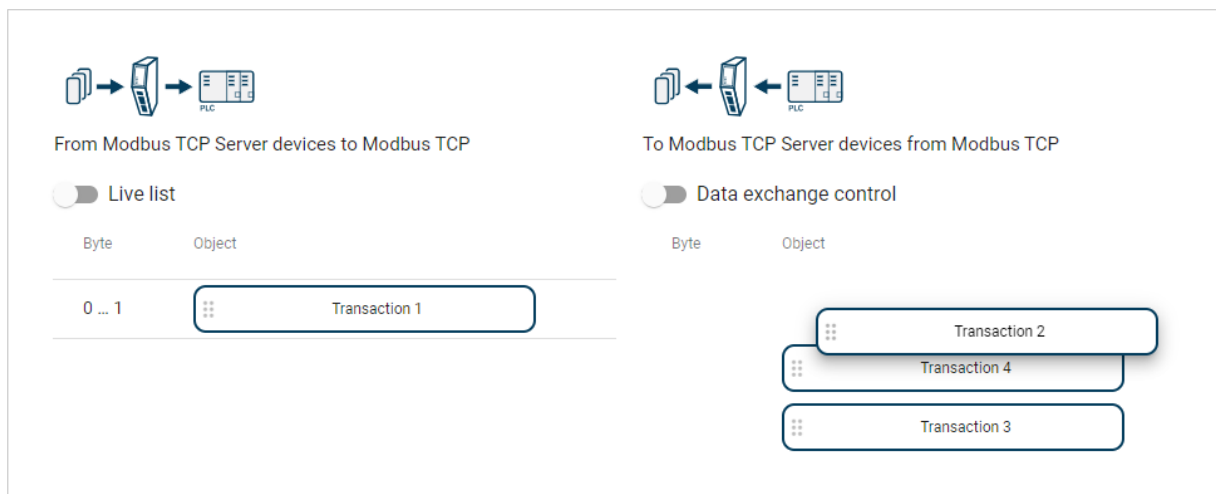


Figure 35. I/O configuration, change the order of objects

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. Convert Between Big-Endian and Little-Endian

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

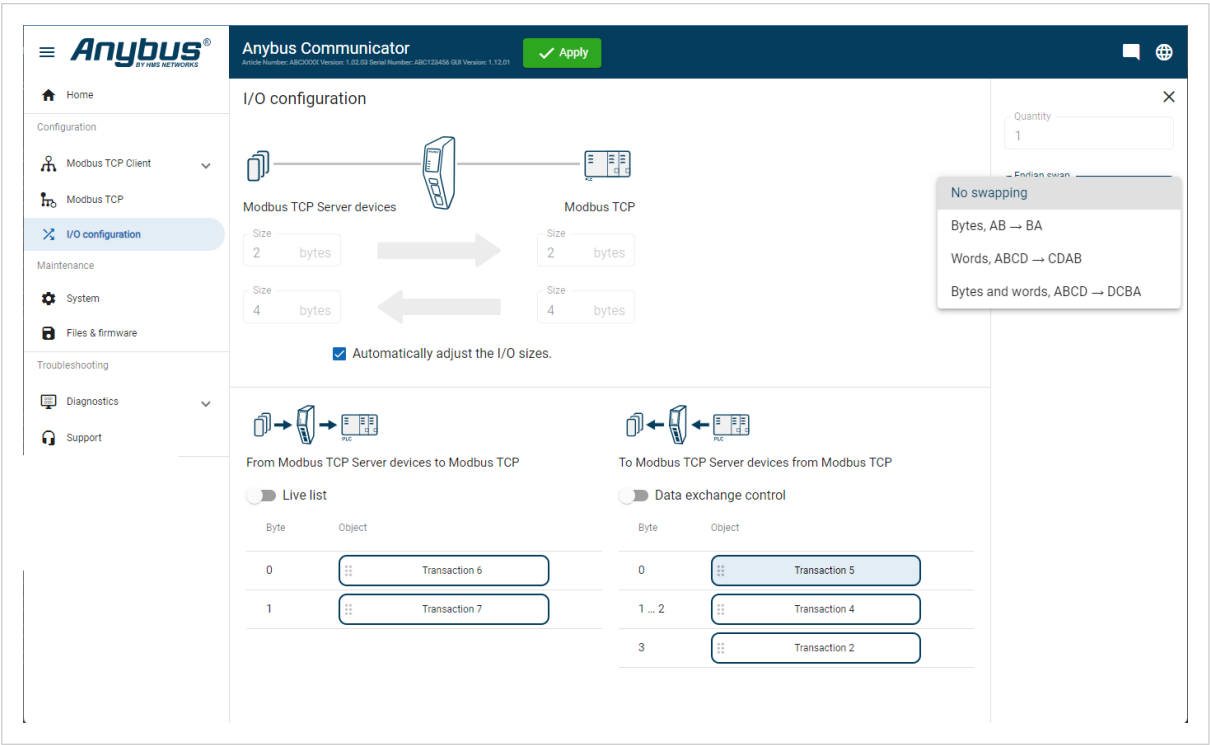


Figure 36. I/O configuration page, Endian swap

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.

8.9.4. Live List

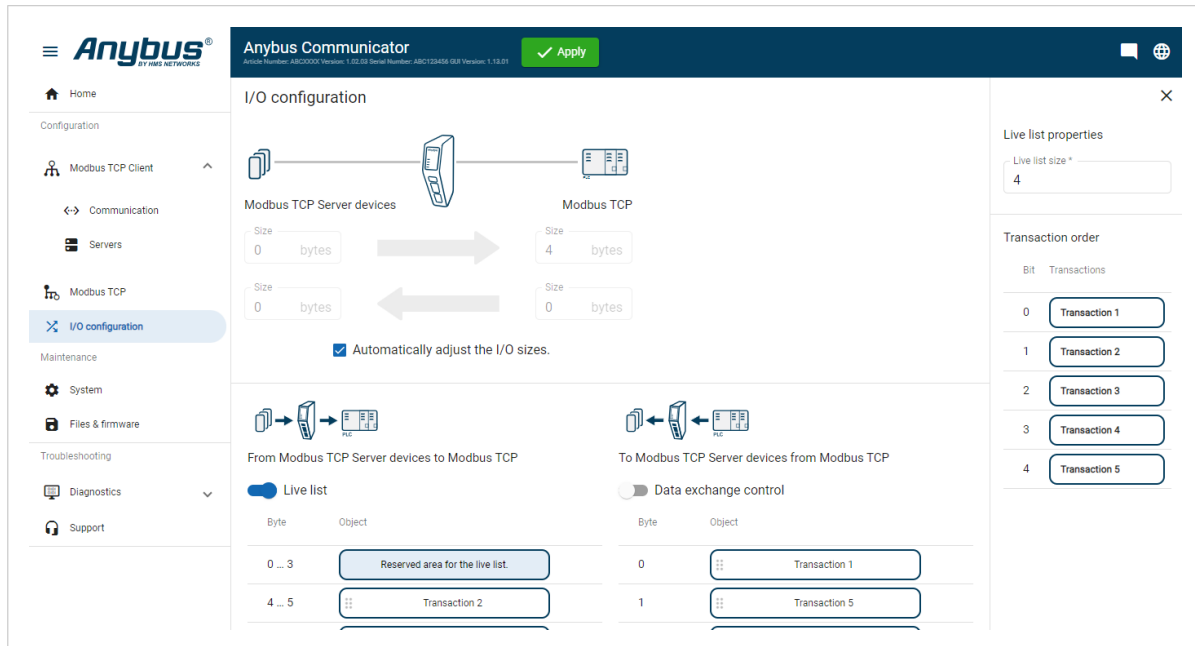


Figure 37. I/O configuration page, Live list enabled

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

About the Live List

- When **Live list** is enabled, the first four bytes of process data on the Modbus TCP Server 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

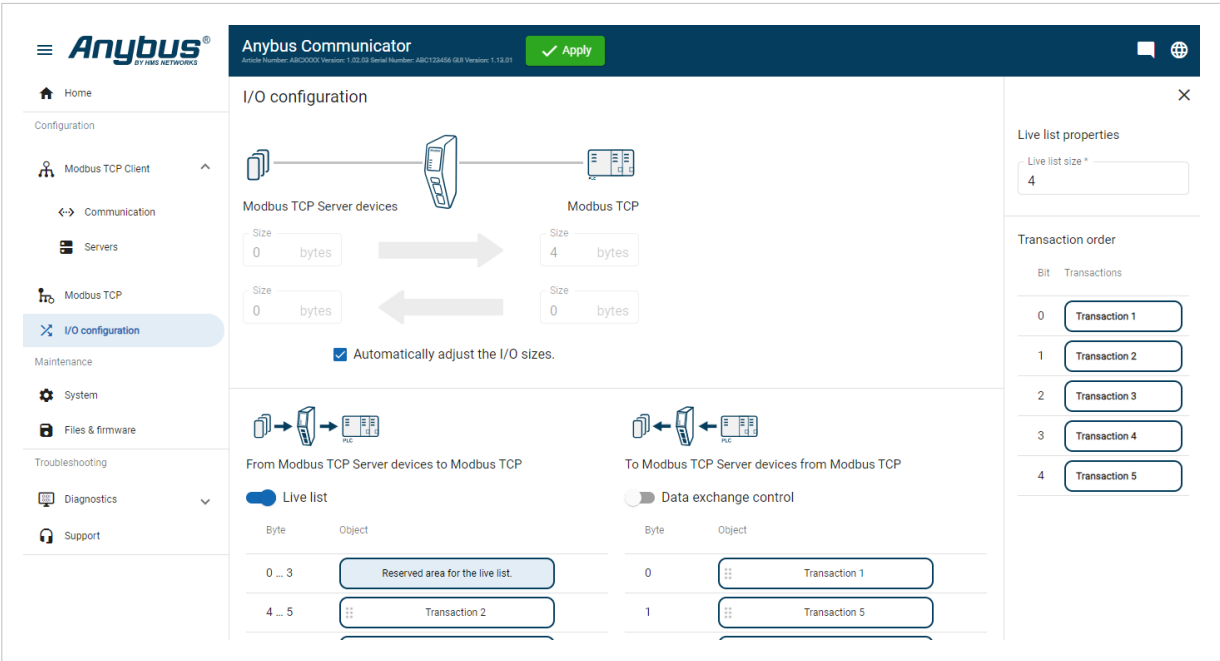


Figure 38. Live list properties and Transaction order

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.

8.9.5. Data Exchange Control

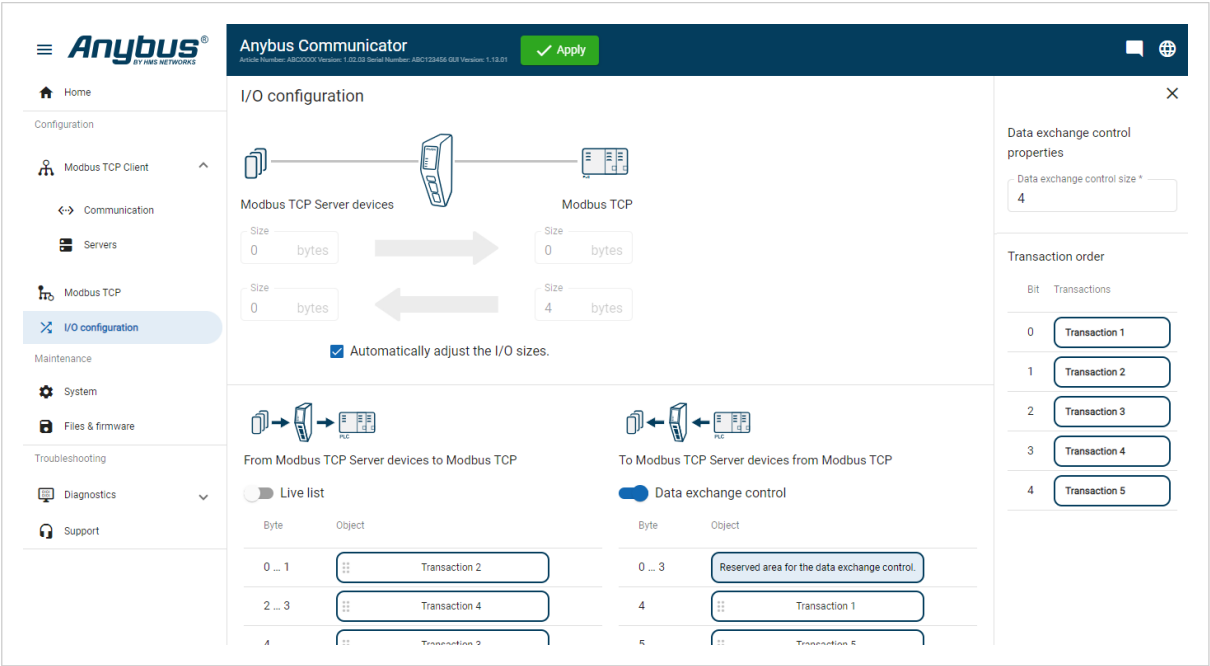


Figure 39. I/O configuration, **Data exchange control** enabled

- By default **Data exchange control** is disabled.
- When **Data exchange control** is enabled, the first four bytes of process data on the Modbus TCP Server 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

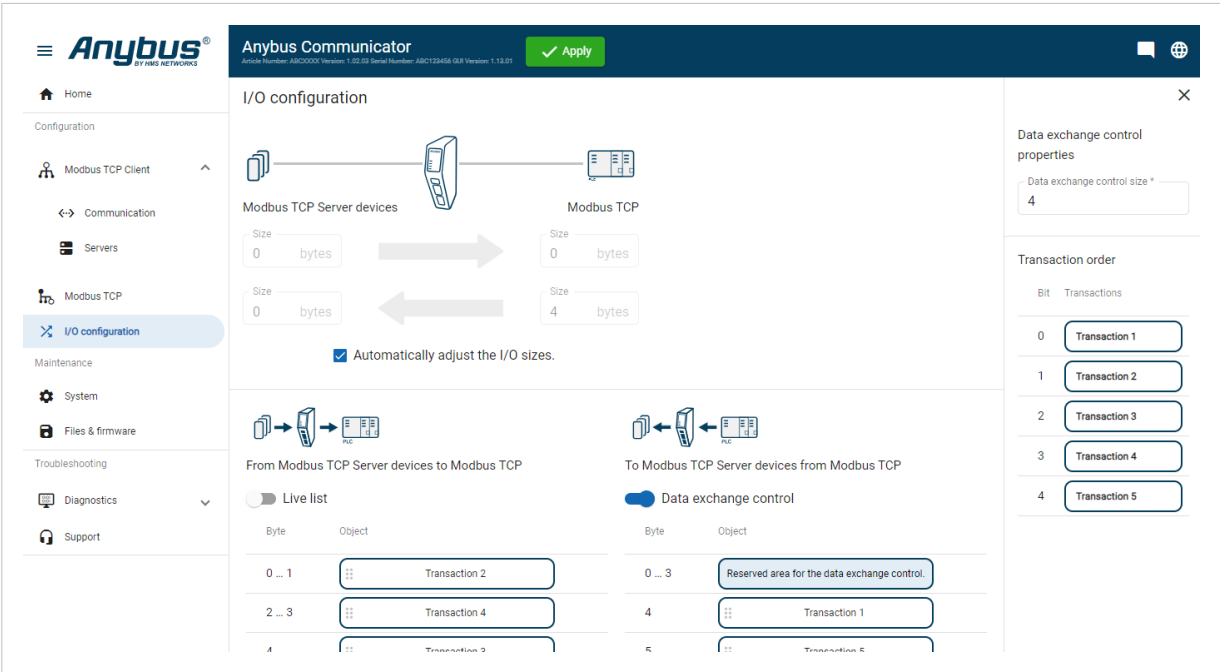


Figure 40. Data exchange control properties and Transaction order

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 41. Configuration note, comment icon

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

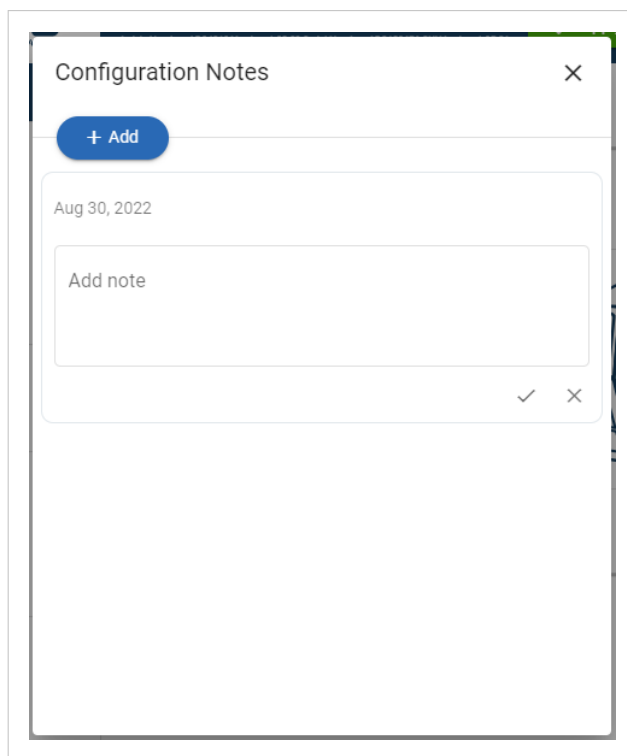


Figure 42. Add new configuration note

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

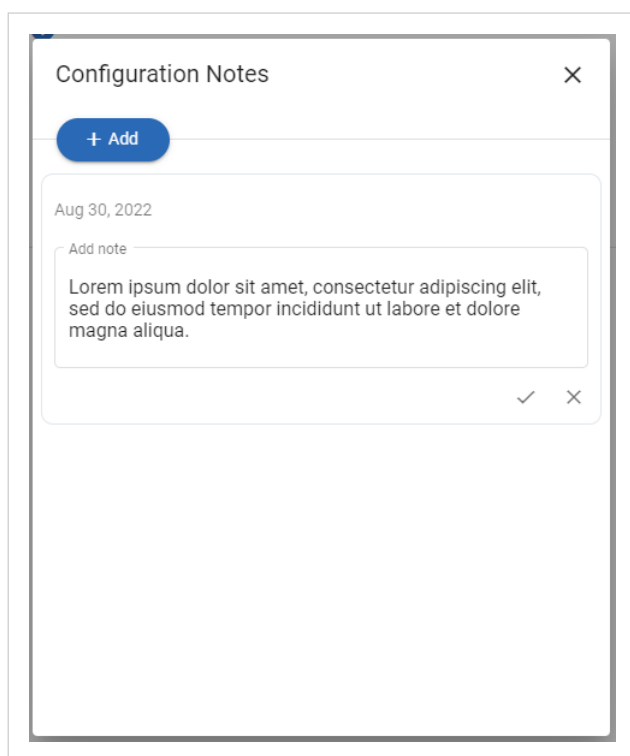


Figure 43. Write a configuration note

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

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

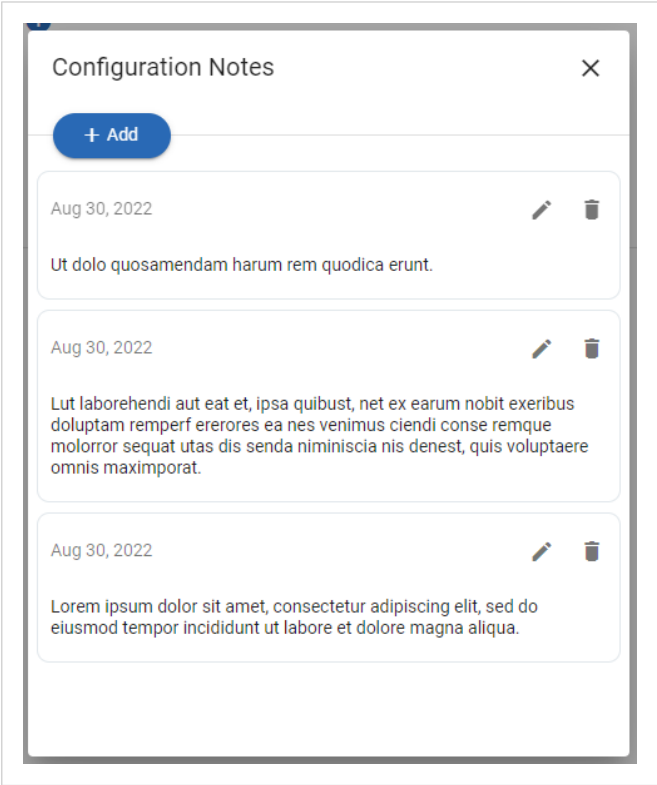


Figure 45. Example: The Configuration Notes window with added notes

8.11. Apply Configuration

Before You Begin

**NOTE**

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

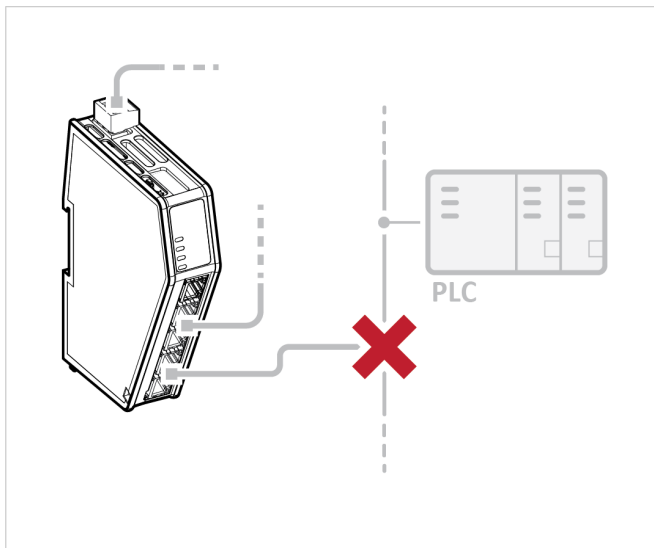


Figure 46. Disconnect the Communicator from the Modbus TCP Server network

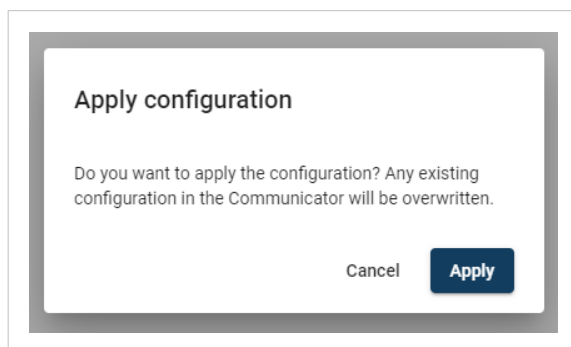
Procedure

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

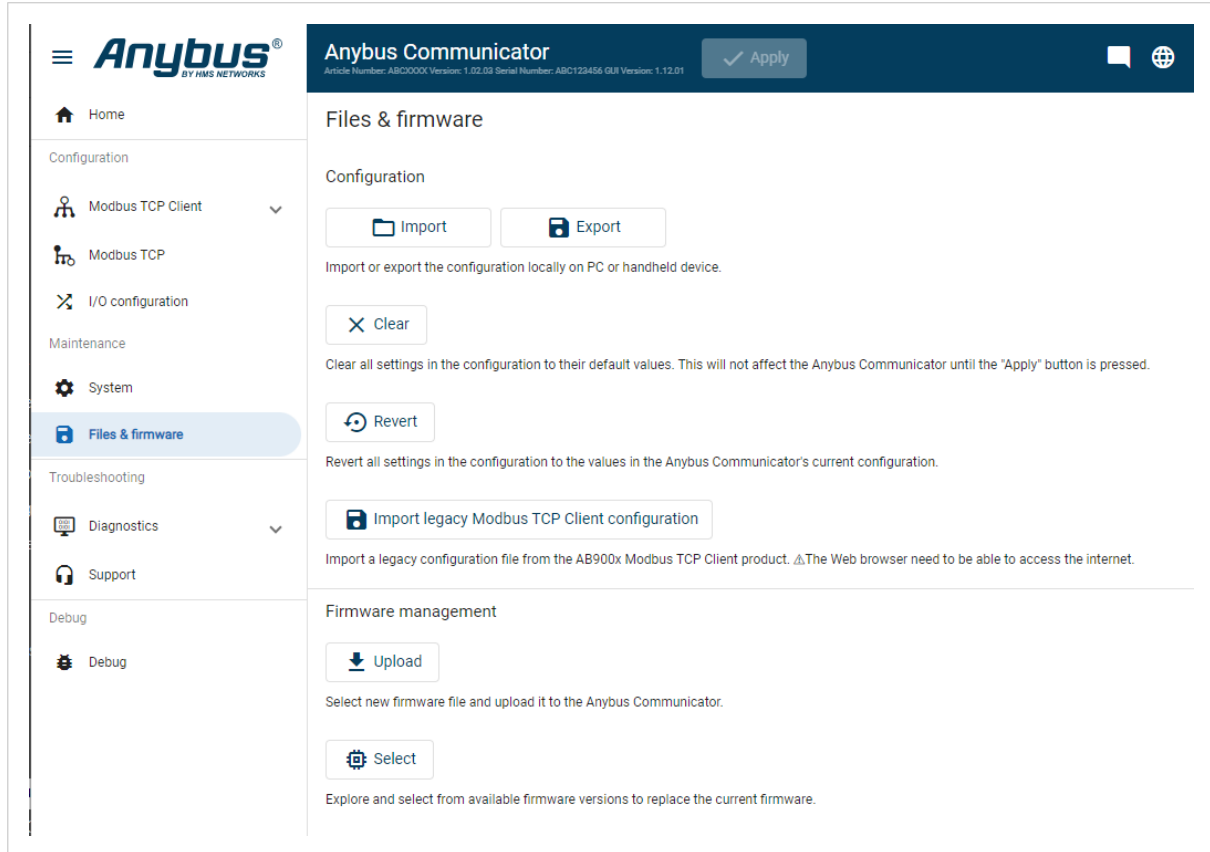


Figure 47. Files & firmware page

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

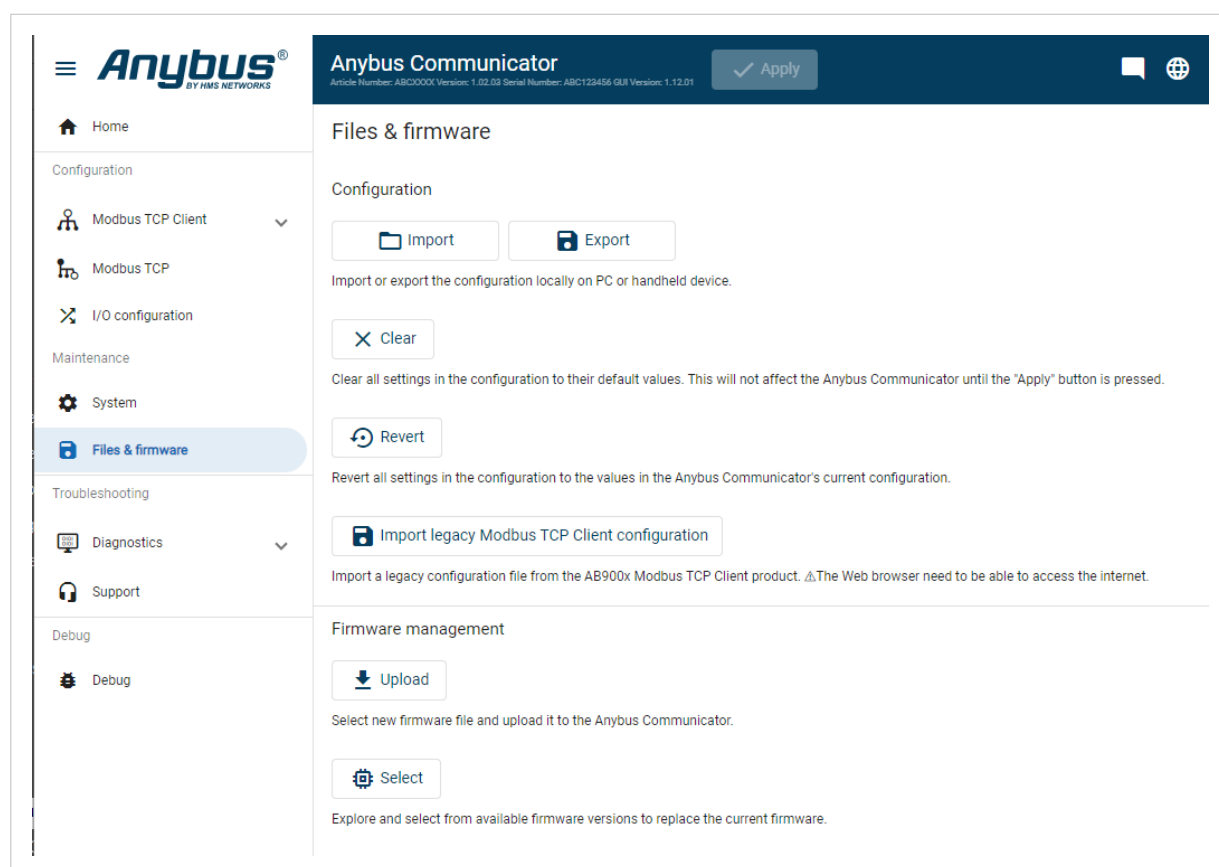


Figure 48. Files & firmware page

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**.

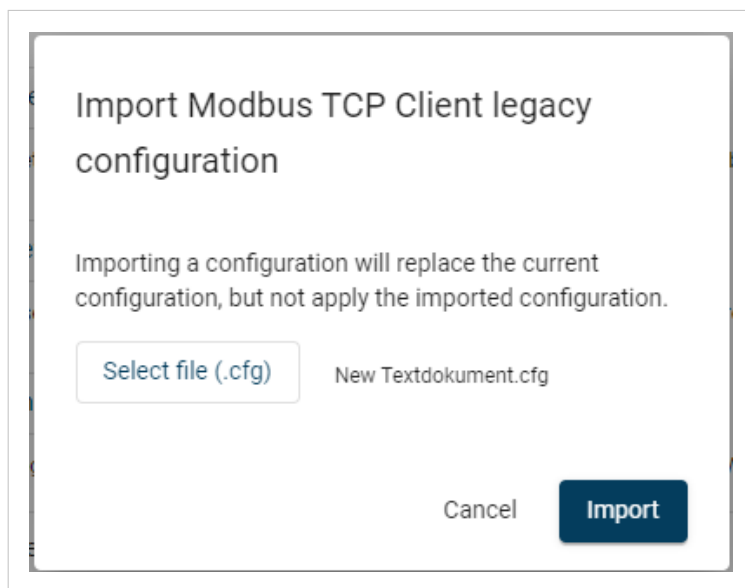


Figure 49. Example, selected .cfg file

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.

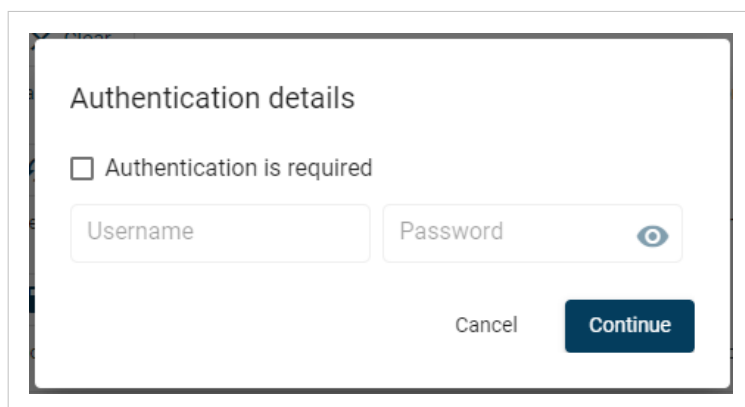
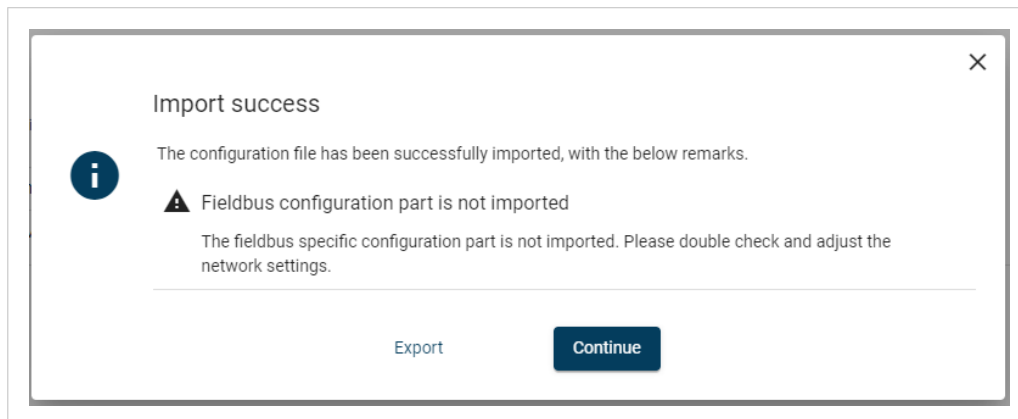


Figure 50. Authentication details

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 51. 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. Modbus Addressing and Register Mapping

For information about the Modbus Transactions, refer to the Modbus Organization.

9.2.1. The Difference Between Address and Register Start

To read or write data from a Modbus device you can use either Address or Register.



TIP
If Register is used, add +1 to the Address value.

Example 1. Modbus Function Code 0x04 Read Input Registers

Table 1. Modbus client values

Address	Register	Modicon Register
0	1	30001
1	2	30002
2	3	30003

Example 2. Modbus Function Code 0x03 Read Holding Registers

Table 2. Modbus client values

Address	Register	Modicon Register
0	1	40001
1	2	40002
2	3	40003

9.2.2. To Read and Write Data

To Read Data

To read data, you can use different Modbus Functions.

Discrete Inputs

- Modbus Function 0x02 Read Discrete Input Status

Discrete Input start at address 0.

Input Registers

- Modbus Function 0x04 Read Input Register
- Modbus Function 0x03 Read Holding Registers

The Input Registers starts at address 0 which corresponds to Register 1.

To use Read Holding Registers the address is offset to address 2048 which corresponds to Register 2049.

The first Input Register (30001)

The first Input Register (30001) can be read using Modbus Function code 0x04 Read Input Registers at Address 0 or Register 1.

You can also use Read Holding Registers (Modbus Function code 0x03) to read the same data (at Address 42048 = Register 42049) or use Read Discrete Inputs 0x02 at address 0..15.

To Write Data

To write data, you can use different Modbus Functions.

Coils

- Modbus Function 0x05 Force Single Coil
- Modbus Function 0x0F Force Multiple Coils

Coils starts at address 0.

Holding Registers

- Modbus Function 0x06 Write Single Register
- Modbus Function 0x10 Write Multiple Registers

The Holding Registers starts at address 0 which corresponds to Register 1.

Holding Register (40001)

The first Holding Register (40001) can be written to using Modbus Function code 0x06 Write Single Register at Address 0 or Register 1.

To read back what has been written, you can use Read Holding Registers 0x03 at address 0..749 = Register 1..750 (40001..40750) or Read Coils 0x01 at address 0..11999.

Data Encoding

Modbus uses the big-endian format for addresses and data items.

When a numerical value larger than one byte is transmitted, the most significant byte is sent first.

Example 3. Big-Endian Data Encoding

For a 16-bit register value of 0x1234:

- The first byte sent is 0x12.
- The second byte sent is 0x34.

See also [Convert Between Big-Endian and Little-Endian \(page 54\)](#).

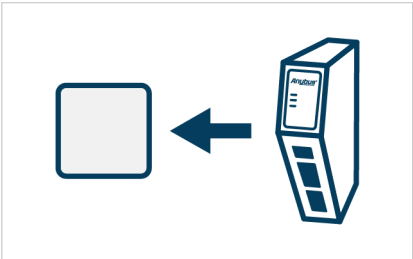
Idle Mode

Transaction	Holding Register	Description
Enter/Exit Idle Mode	0x1004	Used by the Modbus TCP client to indicate an idle/offline mode on the network.

9.2.3. Default Address Mode I/O Data Mapping

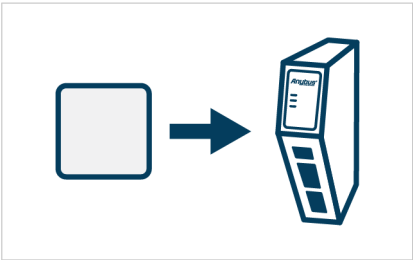
The following Modbus function codes are compatible with the default addressing mode.

Input Data to Client/Server - Data to Modbus



Process I/O data offset		Discrete input address		Input register address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x0000 - 0x000F	0 - 15	0x0000	0	0x0800	2048
0x0002 - 0x0003	2 - 3	0x0010 - 0x001F	16 - 31	0x0001	1	0x0801	2049
...
0x05D8 - 0x05D9	1496 - 1497	0x2EC0 - 0x2ECF	11968 - 11983	0x02EC	748	0x0AEC	2796
0x05DA - 0x05DB	1498 - 1499	0x2ED0 - 0x2EDF	11983 - 11999	0x02ED	749	0x0AED	2797

Output Data From Client/Server - Data From Modbus TCP

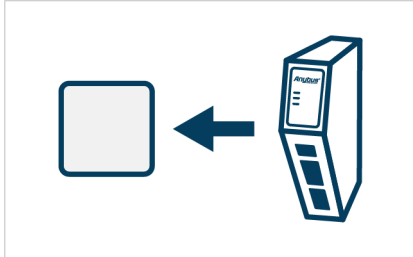


Process I/O data offset		Coil address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x0000 - 0x000F	0 - 15	0x0000	0
0x0002 - 0x0003	2 - 3	0x0010 - 0x001F	16 - 31	0x0001	1
...
0x05D8 - 0x05D9	1496 - 1497	0x2EC0 - 0x2ECF	11968 - 11983	0x02EC	748
0x05DA - 0x05DB	1498 - 1499	0x2ED0 - 0x2EDF	11983 - 11999	0x02ED	749

9.2.4. Legacy Address Mode I/O Data Mapping

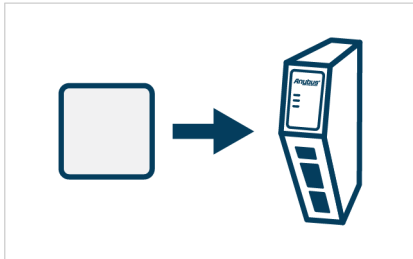
The following Modbus function codes are compatible with the Modbus **Use legacy mode** setting.

Input Data to Client/Server - Data to Modbus



Process I/O data offset		Discrete input address		Coil address		Input register address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x0000 - 0x000F	0 - 15	0x0000 - 0x000F	0 - 15	0x0000	0	0x0000	0
0x0002 - 0x0003	2 - 3	0x0010 - 0x001F	16 - 31	0x0010 - 0x001F	16 - 31	0x0001	1	0x0001	1
...
0x01FC - 0x01FD	508 - 509	0x0FE0 - 0x0FEF	4064 - 4079	0x0FE0 - 0x0FEF	4064 - 4079	0x00FE	254	0x00FE	254
0x01FE - 0x01FF	510 - 511	0x0FF0 - 0x0FFF	4080 - 4095	0x0FF0 - 0x0FFF	4080 - 4095	0x00FF	255	0x00FF	255

Output Data From Client/Server - Data From Modbus



Process data offset		Discrete input address		Coil address		Input register address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x4000 - 0x400F	16384 - 16399	0x4000 - 0x400F	16384 - 16399	0x0400	1024	0x0400	1024
0x0002 - 0x0003	2 - 3	0x4010 - 0x401F	16400 - 16415	0x4010 - 0x401F	16400 - 16415	0x0401	1025	0x0401	1025
...
0x01FC - 0x01FD	508 - 509	0x4FE0 - 0x4FEF	20448 - 20463	0x4FE0 - 0x4FEF	20448 - 20463	0x04FE	1278	0x04FE	1278
0x01FE - 0x01FF	510 - 511	0x4FF0 - 0x4FFF	20464 - 20479	0x4FF0 - 0x4FFF	20464 - 20479	0x04FF	1279	0x04FF	1279

10. Verify Operation

10.1. Communicator Status Monitor

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



Figure 52. Home page

Gateway Status

Overview the Communicator LED indications remotely.

Refer to [Communicator LED Indicators \(page 74\)](#)





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: <ul style="list-style-type: none">• Initial state where non network components are started and configured.• Network startup in progress.• Invalid configuration detected.
	Normal operation.

10.2. Communicator LED Indicators



NOTE

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

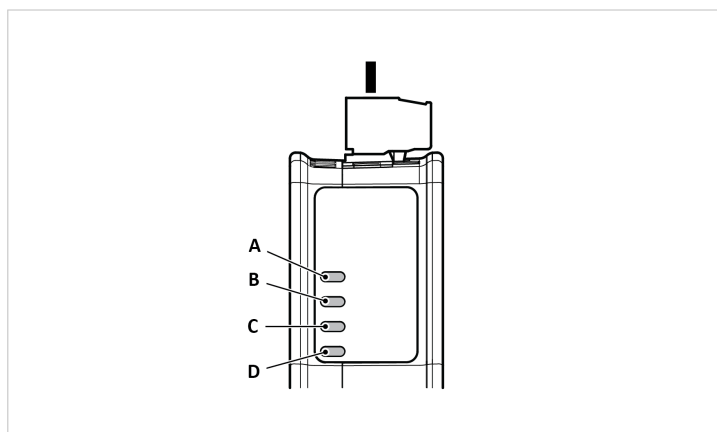


Figure 53. Gateway status (A), Network connection (B)/(C) and Security switch (D)

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

Connection to high level network IO controller device						
<ul style="list-style-type: none"> LED B for PROFINET network LED C for EtherNet/IP, EtherCAT, PROFIBUS, Modbus TCP, or Modbus RTU networks 						
Operation status	EtherNet/IP	EtherCAT	PROFIBUS	PROFINET	Modbus TCP	Modbus RTU
Off	No power/No IP address.	No power	No power/No data exchange.	No power/No connection with IO controller.	No power/No Modbus TCP IP address.	No power, no active nodes, or all nodes are stopped.
Green, solid	Connection with IO controller established.	EtherCAT on.	Operate, data exchange.	Connection with IO controller established. IO controller in Run state.	Modbus TCP online, at least one message received.	At least one Modbus message received.
Green, one flash	N/A	N/A	N/A	Connection with IO controller established. IO controller in STOP state or IO data is inaccurate.	N/A	N/A
Green, flashing	EtherNet/IP online, no connections established.	EtherCAT online, no connections established.	Clear, data exchange.	Used by engineering tools to identify the node on the network.	Modbus TCP online, no messages received.	Waiting for first Modbus message.
Red, solid	IP address conflict detected.	Fatal event			IP address conflict detected.	Fatal event

Connection to high level network IO controller device						
<ul style="list-style-type: none"> LED B for PROFINET network LED C for EtherNet/IP, EtherCAT, PROFIBUS, Modbus TCP, or Modbus RTU networks 						
Operation status	EtherNet/IP	EtherCAT	PROFIBUS	PROFINET	Modbus TCP	Modbus RTU
Red, one flash	N/A	Unsolicited state change SubDevice application has changed the EtherCAT state autonomously.	Parameterization error.	Station name not set.	N/A	
Red, two flash	N/A	Sync Manager watchdog timeout.	Configuration error.	IP address not set.	N/A	
Red, three flash	N/A	N/A	N/A	Expected Identification differs from Real Identification.	N/A	
Red, flashing	Connection timeout	Invalid configuration.	N/A	N/A	Connection timeout	Connection timeout. No Modbus messages has been received within the configured process active timeout time.

Connection to subnetwork Modbus TCP client device	
<ul style="list-style-type: none"> LED C for PROFINET network LED B or EtherNet/IP, EtherCAT, PROFIBUS, Modbus TCP, or Modbus RTU networks 	
Operation status	Description
Off	No IP address.
Red, flashing	At least one connection error or timeout.
Red, solid	IP address conflict detected, or FATAL event.
Green, solid	No connections errors or timeouts.

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

10.3. Ethernet LED Indicators

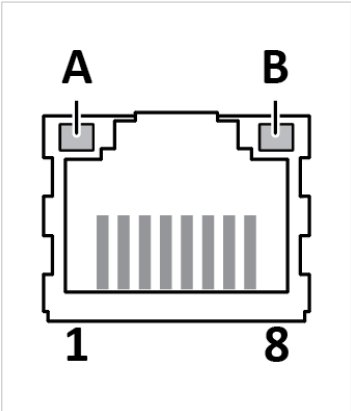


Figure 54. LED A. Activity LED B. Not used

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

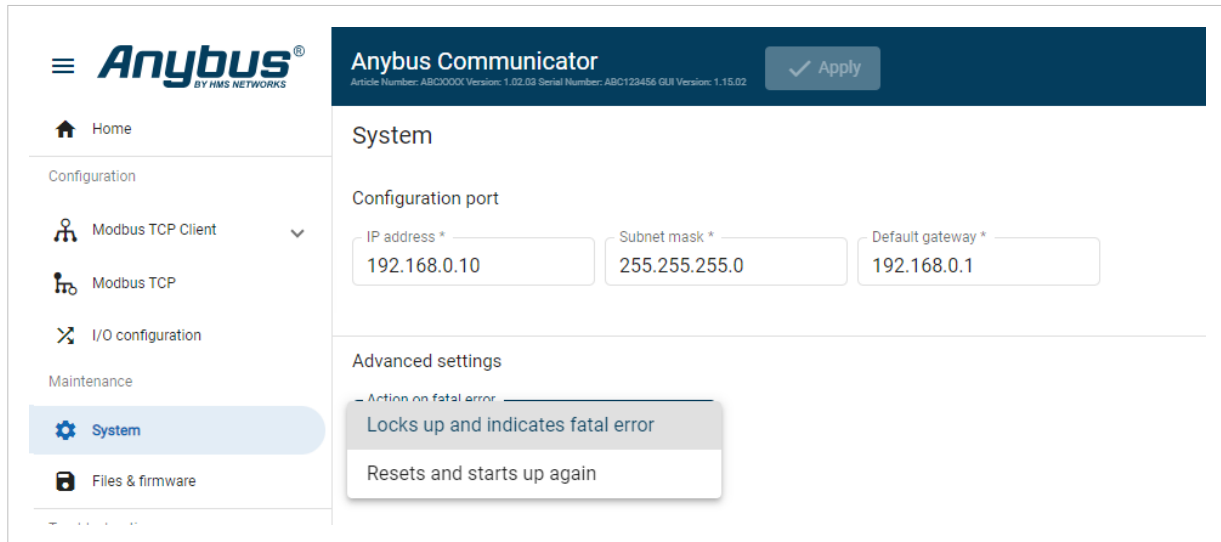


Figure 55. System page, Action on fatal error menu

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 indicate 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.



Home

Configuration

Modbus TCP Client (X2)

Modbus TCP (X3)

I/O configuration

Maintenance

System

Files & firmware

Anybus Communicator

Article Number: ABCXXXXX Version: 1.02.04 Serial Number: ABC123456 GUI Version: 1.22.01

Apply

System

Configuration port (X1)

IP address*

Subnet mask*

Default gateway*

192.168.0.10

255.255.255.0

192.168.0.1

Advanced settings

Action on fatal error

Locks up and indicates fatal error

Figure 56. 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.

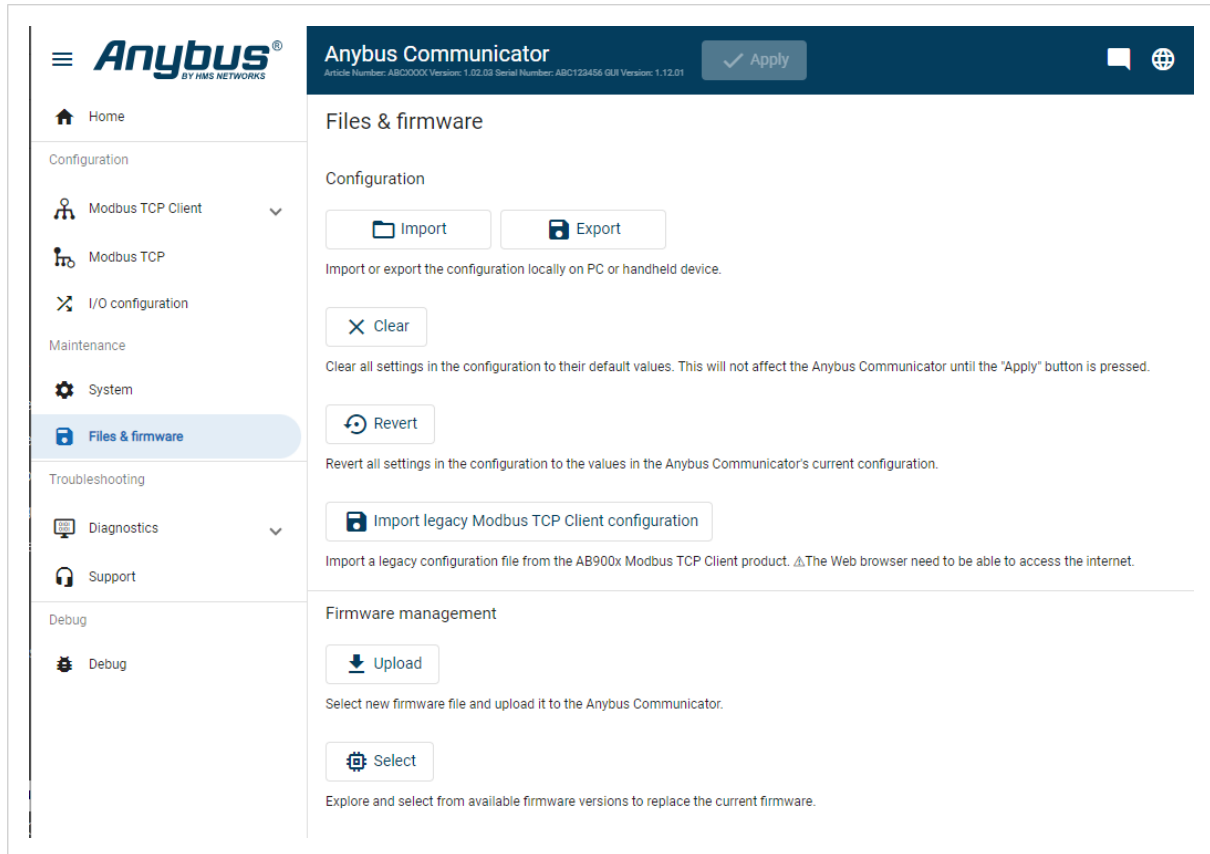


Figure 57. Files & firmware page

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

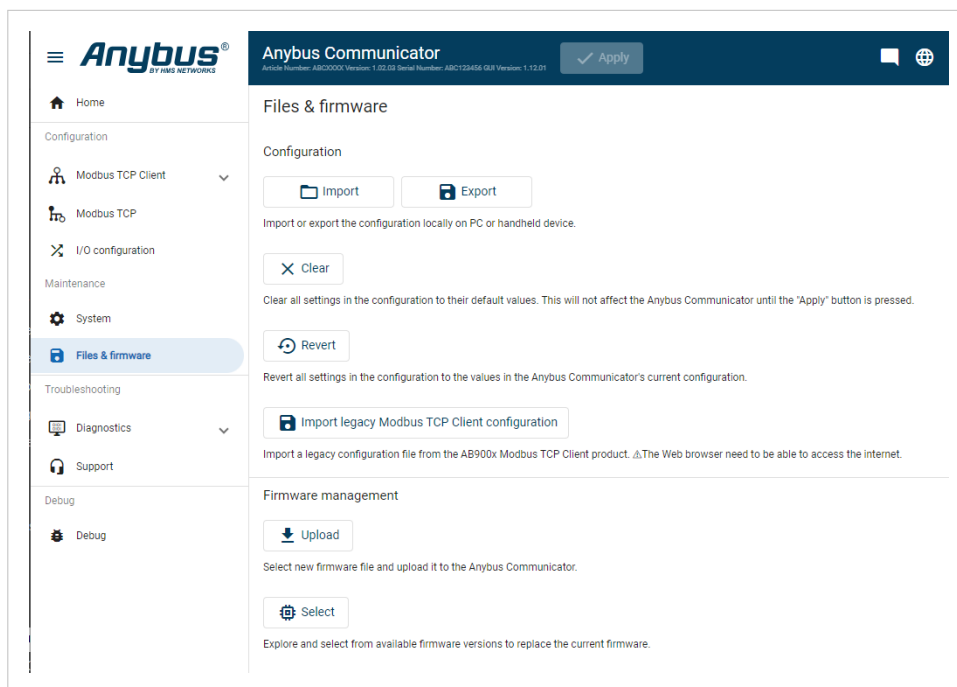


Figure 58. Files & firmware page

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

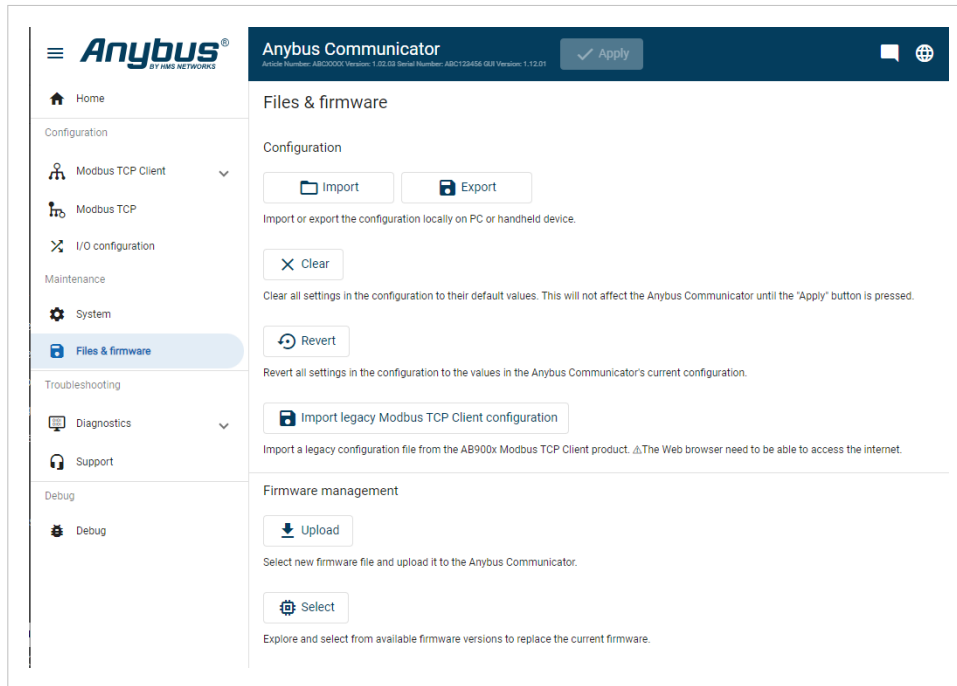


Figure 59. Files & firmware page

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 60. 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

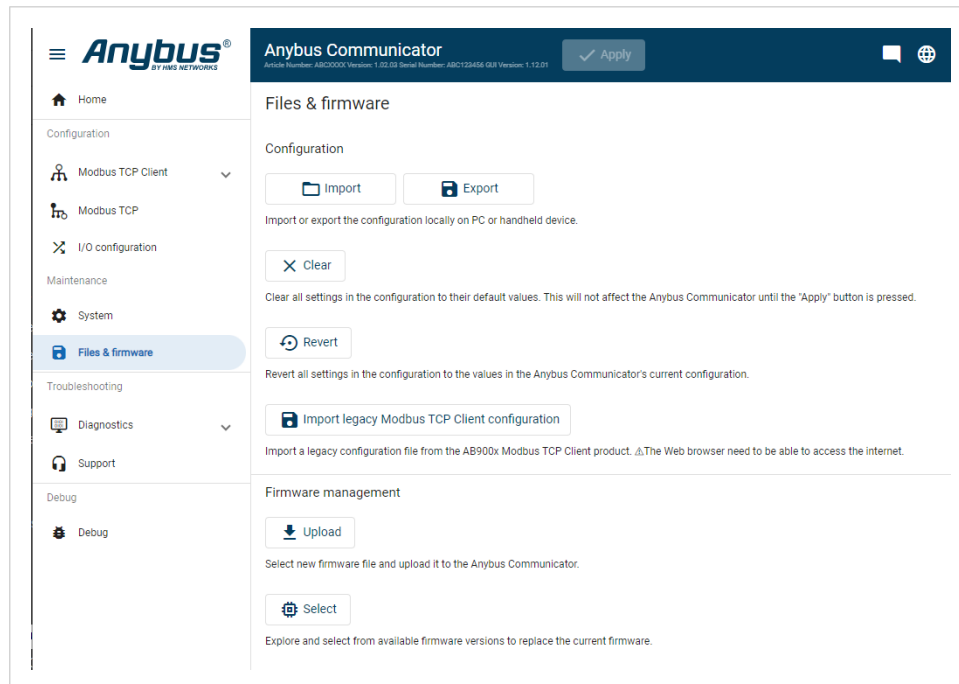


Figure 61. Files & firmware page

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 .

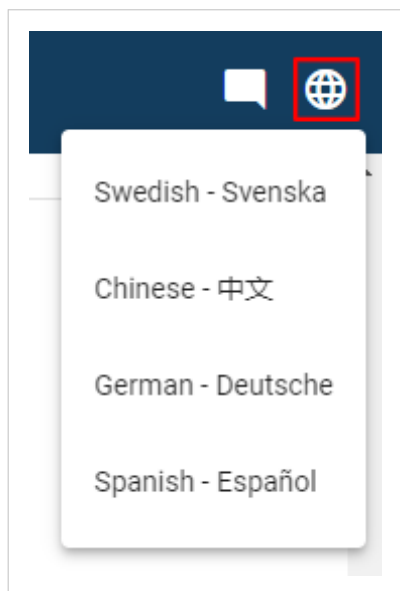


Figure 62. Language menu

2. Select a new language from the list.

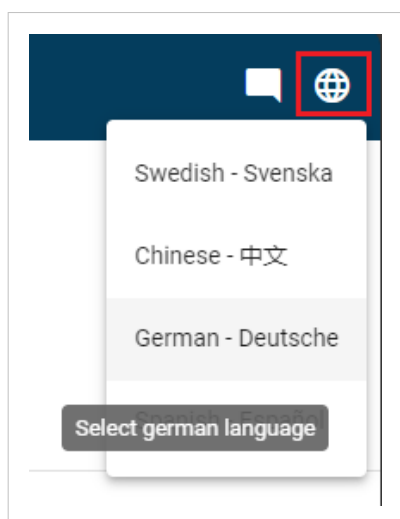


Figure 63. Example: Change language to German

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 **Modbus TCP Server** side, including any configured endian conversions.

Anybus Communicator
Article Number: ABCXXXXX Version: 1.02.03 Serial Number: ABC123456 GUI Version: 1.12.01

I/O data

Start Hex Dec Ascii

Data from Modbus TCP to the Anybus Communicator

Address	Data
0 ... 7	00 01 02 03 04 05 06 07
8 ... 15	08 09 0a 0b 0c 0d 0e 0f
16 ... 23	10 11 12 13 14 15 16 17
24 ... 31	18 19 1a 1b 1c 1d 1e 1f
32 ... 39	20 21 22 23 24 25 26 27
40 ... 47	28 29 2a 2b 2c 2d 2e 2f
48 ... 55	30 31 32 33 34 35 36 37
56 ... 63	38 39 3a 3b 3c 3d 3e 3f

Time (d:hh:mm:ss.ms): 0:00:04:17.966

Data from the Anybus Communicator to Modbus TCP

Address	Data
0 ... 7	00 01 02 03 04 05 06 07
8 ... 15	08 09 0a 0b 0c 0d 0e 0f
16 ... 23	10 11 12 13 14 15 16 17
24 ... 31	18 19 1a 1b 1c 1d 1e 1f
32 ... 39	20 21 22 23 24 25 26 27
40 ... 47	28 29 2a 2b 2c 2d 2e 2f
48 ... 55	30 31 32 33 34 35 36 37
56 ... 63	38 39 3a 3b 3c 3d 3e 3f

Time (d:hh:mm:ss.ms): 0:00:04:17.966

Figure 64. 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

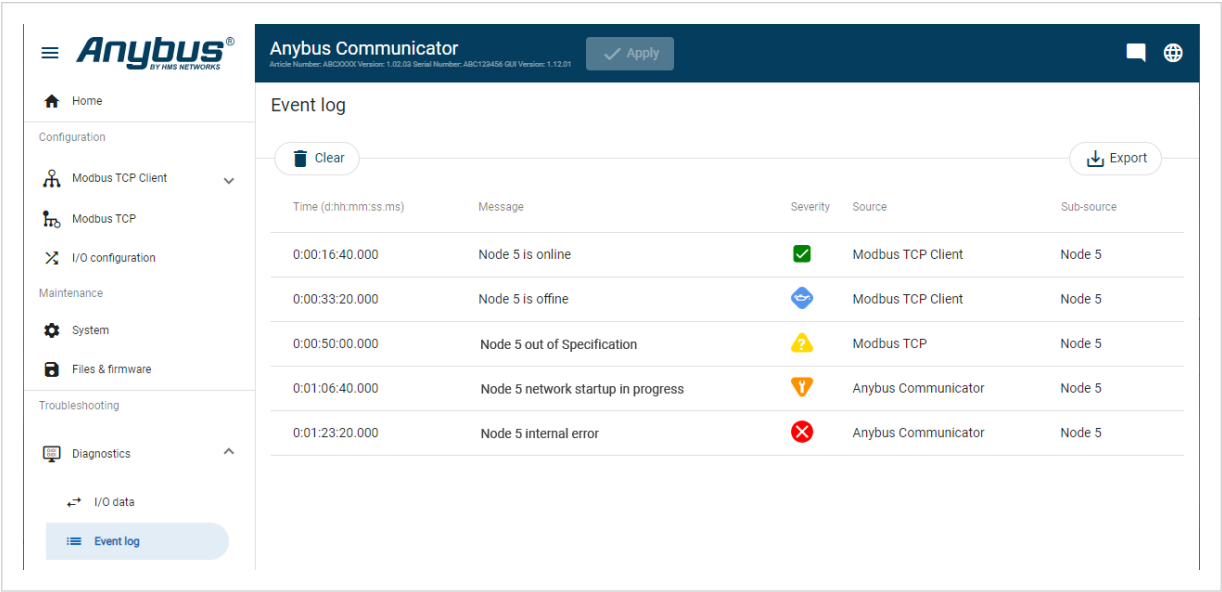


Figure 65. Event log page example

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. For description of the symbols, see Communicator Status Monitor (page 72) .
Source	Communicator Modbus TCP Server Modbus TCP Client
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 4. 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.

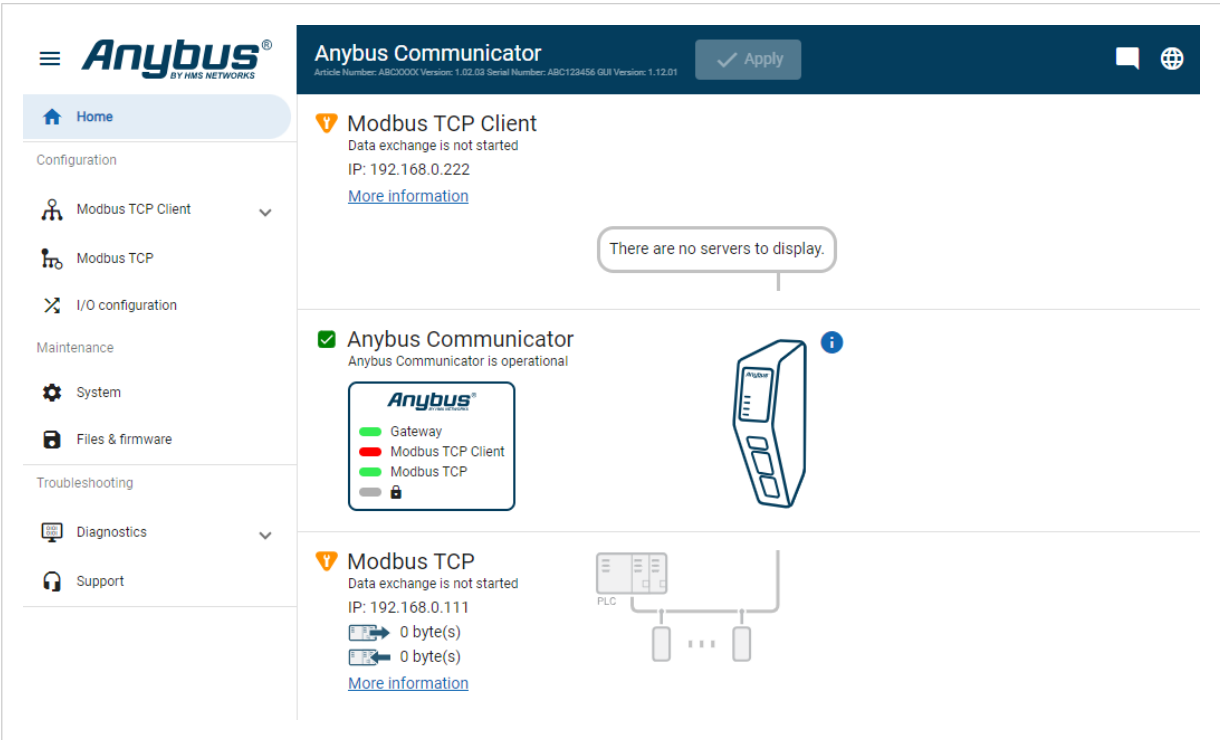


Figure 66. Home page

For information about the LED indication, see [Communicator LED Indicators \(page 74\)](#).

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.

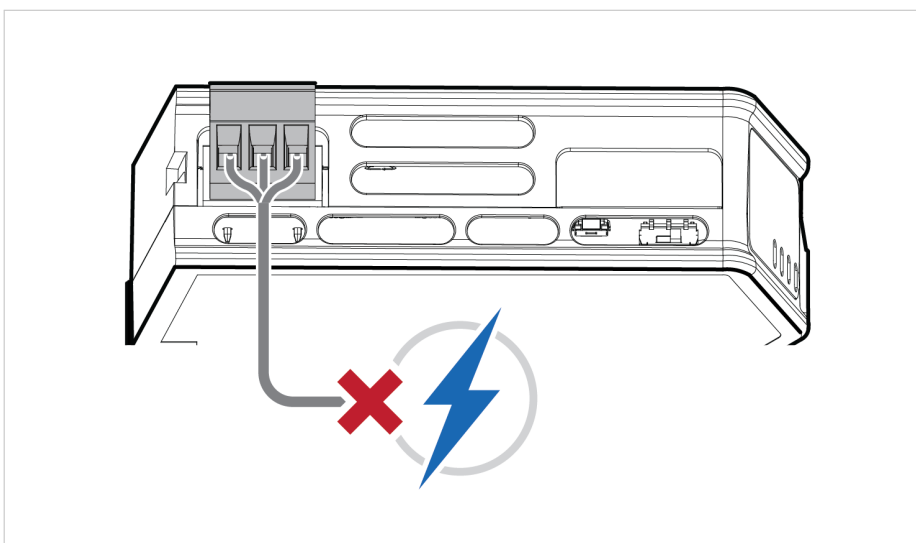


Figure 67. Disconnect power

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

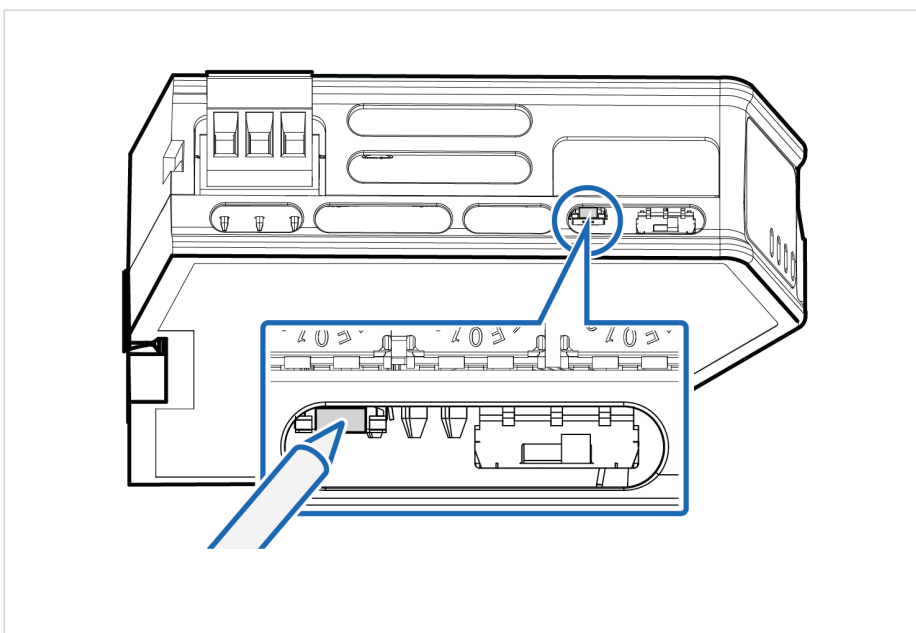


Figure 68. Press and hold **Reset** button

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

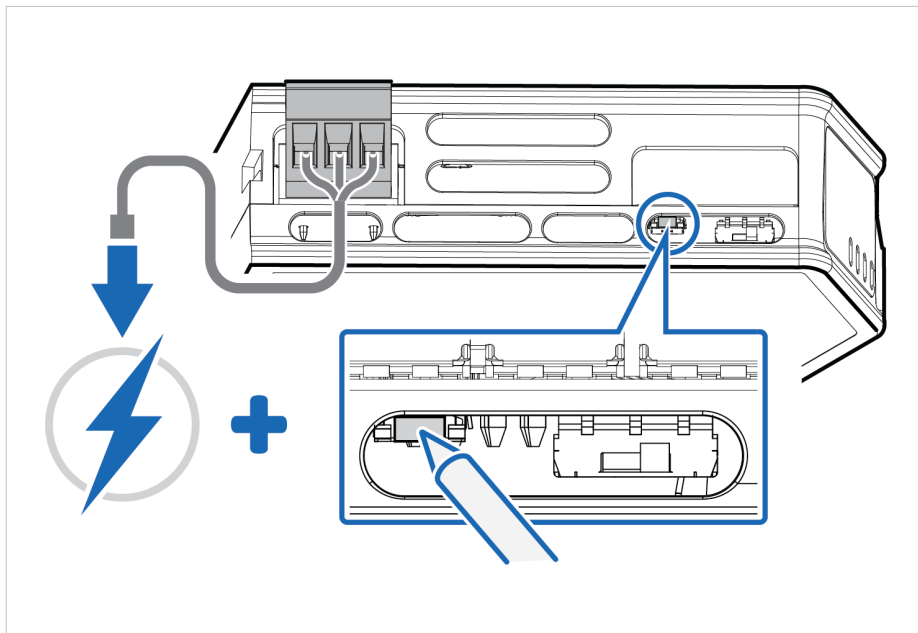


Figure 69. Hold **Reset** button and reconnect power

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**.

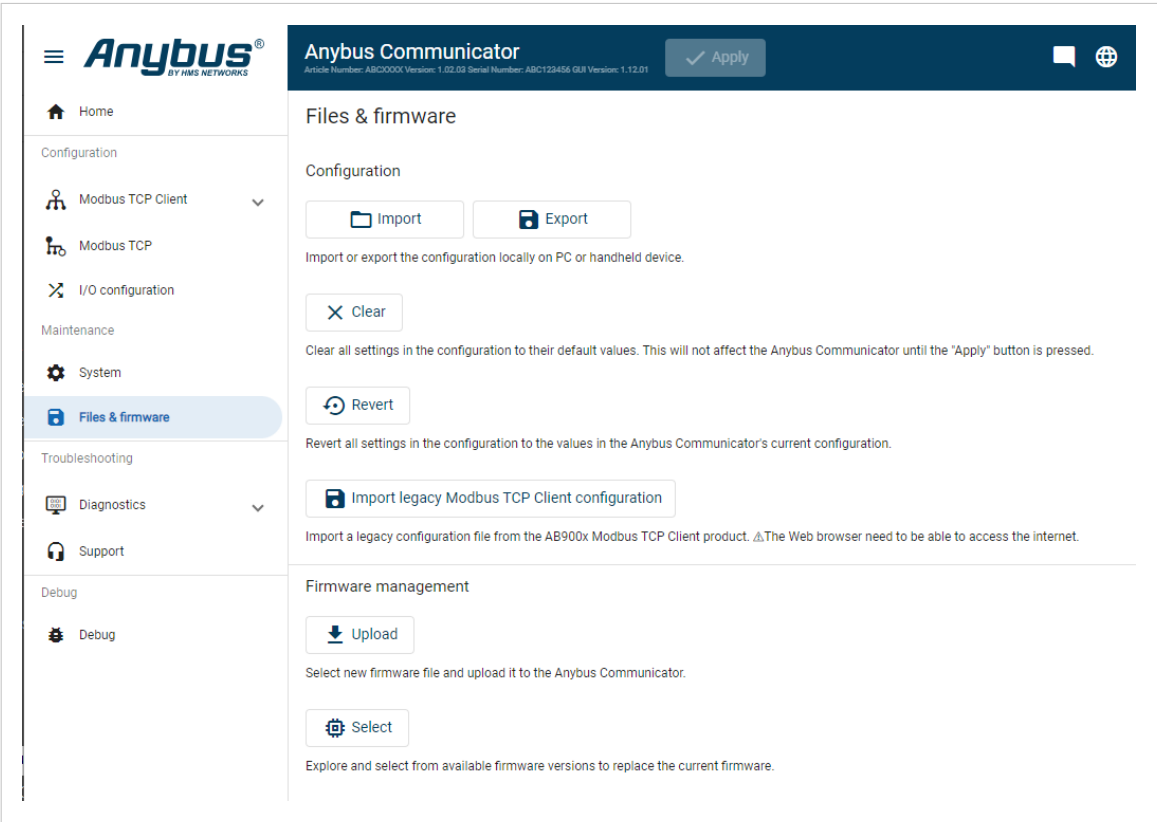


Figure 70. Files & firmware, Revert

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.

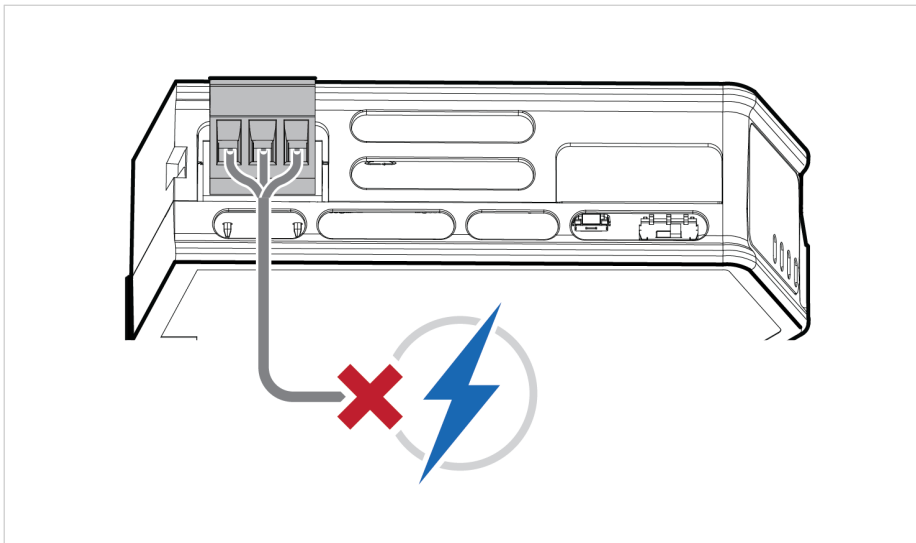


Figure 71. Disconnect power

2. Reconnect the Communicator to power.

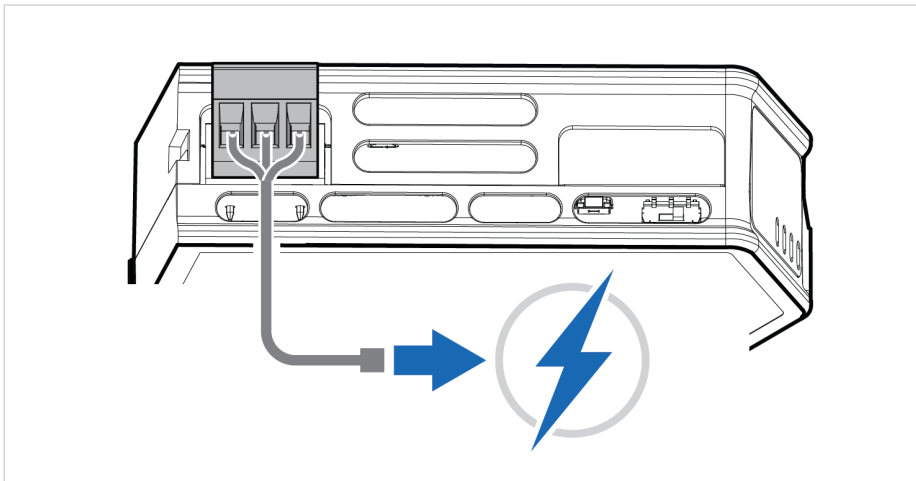


Figure 72. Reconnect power

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

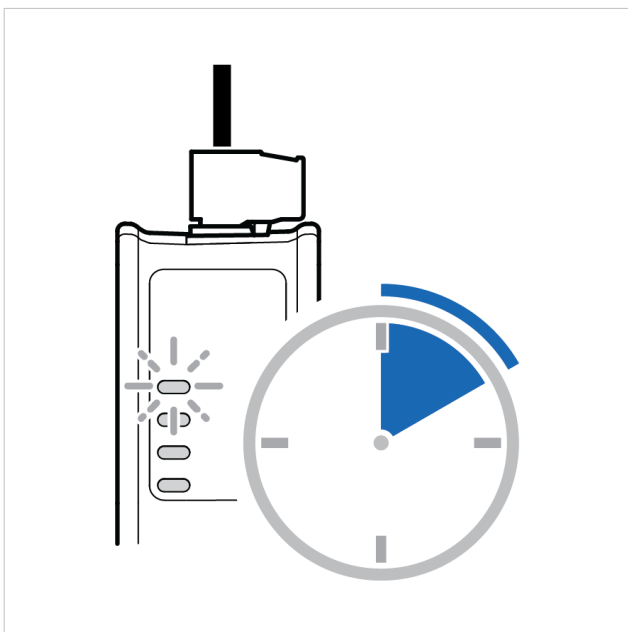


Figure 73. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

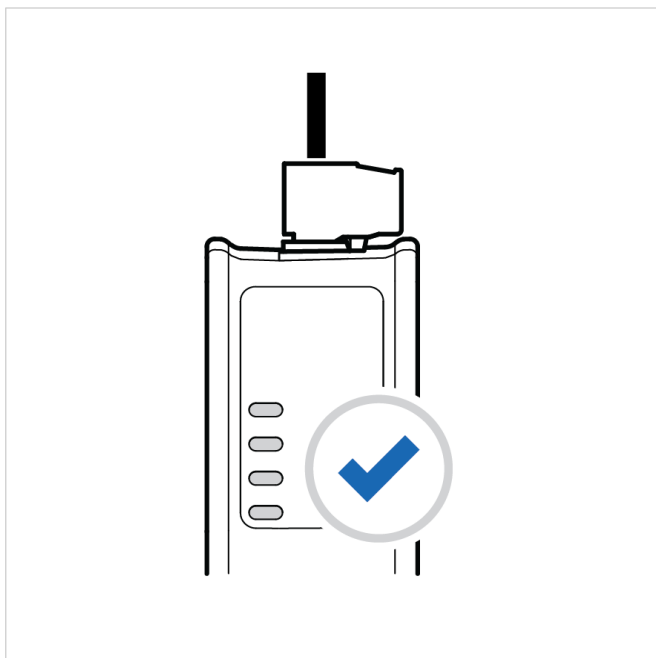


Figure 74. Recover and return to normal operation

To Do Next

To check LED status, refer to [Communicator LED Indicators \(page 74\)](#)

12.4. Support

12.4.1. Support Package

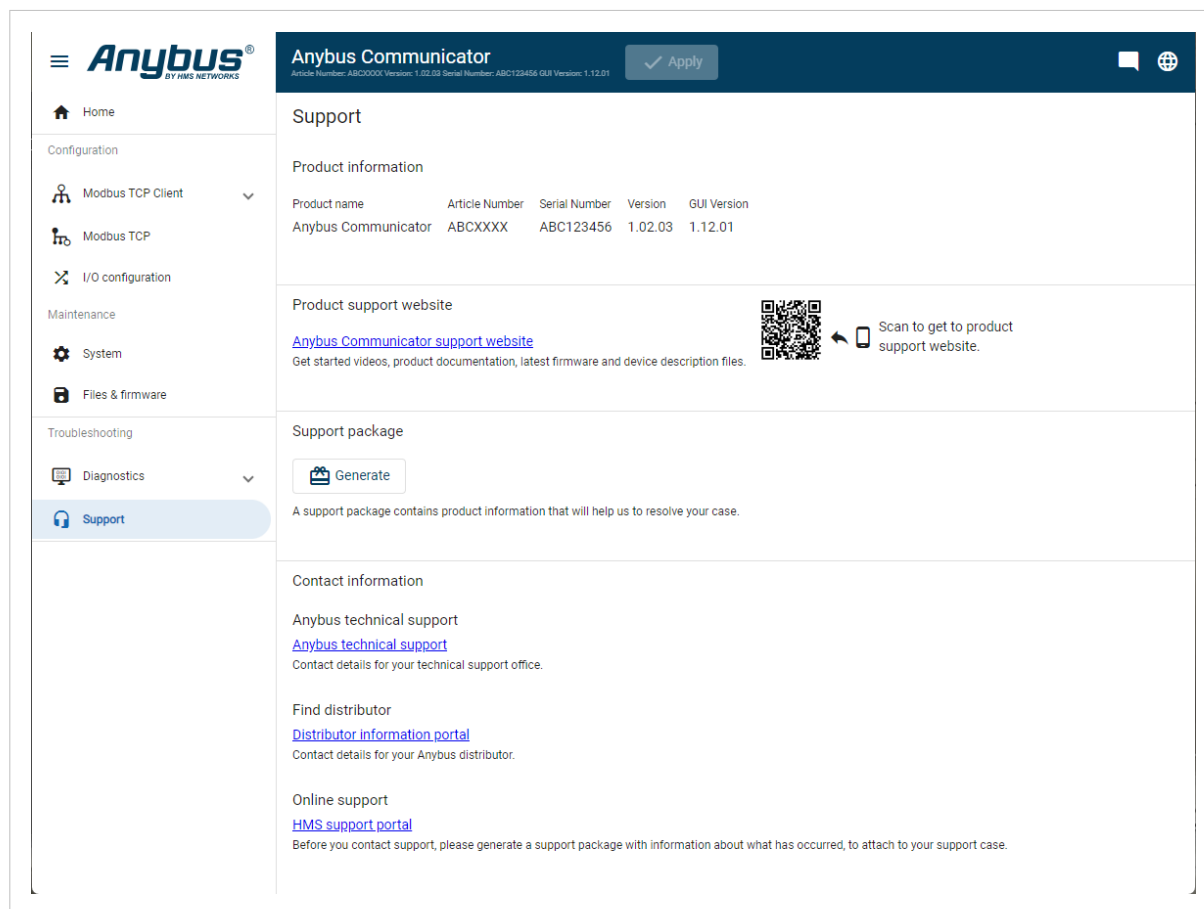


Figure 75. Support page example

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 \(page 88\)](#).

14. Technical Data

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

14.1. Technical Specification

Article identification	ABC3228
Configuration connector	RJ45
Communication connector	RJ45 x 2
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 60068-2-78: 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