

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

SCM-1202-230
Version 1.3
Publication date 2026-05-27



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-networks.com

Table of Contents

1. Preface	1
1.1. About This Document	1
1.2. Document Conventions	1
1.3. Trademarks	2
1.4. About the EtherCAT Terminology	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
3.5. Supported Transport Layer Security (TLS) 1.2 Cipher Suites	7
4. Preparation	8
4.1. Support and Resources	8
4.2. Cabling	8
4.3. Mechanical Tools and Equipment	8
4.4. System Requirements	8
4.4.1. Supported Web Browsers	8
4.4.2. Supported Operating Systems	8
4.5. HMS Software Applications	9
4.6. Third-Party Software Applications	9
4.7. Software License Information	9
5. About Anybus Communicator	10
5.1. Modbus TCP Client Communication	10
5.1.1. Modbus TCP Client Building Blocks	10
5.2. How the Communication Works	12
5.3. How the Data Exchange Works	15
6. Installation	16
6.1. External Parts	16
6.2. Connector Port Guide	17
6.3. DIN Rail Mounting	18
6.4. Connect to Modbus TCP Client Network	19
6.5. Connect to EtherCAT Network	21
6.6. Connect to Power	22
6.7. Security Switch	24
6.8. Lock the Cables	26
6.9. DIN Rail Demount	27
7. Accessing the Communicator	28
7.1. Connect to Configure the Communicator	28
7.2. Access the Built-In Web Interface from HMS IPconfig	29
7.3. Access the Built-In Web Interface from a Web Browser	30
7.4. Communicator Built-In Web Interface Overview	32

8. Role Management	33
8.1. Roles Overview	33
8.2. Roles Configuration Access	34
8.3. Set Up Roles	36
8.4. Set or Change Password	38
8.5. Logout From the Communicator Web Interface	38
9. Configuration Quick Guide	39
9.1. Prepare Configuration	39
9.2. Security Setup	42
9.3. Setup New Configuration	43
9.4. PLC Configuration	45
9.5. Verify Operation	46
10. Communicator Configuration	48
10.1. Modbus TCP Client Communication Settings	49
10.1.1. IP Settings	49
10.2. Modbus TCP Client Servers	50
10.2.1. Add Server	50
10.2.2. Server Properties	51
10.2.3. Add Transactions	52
10.2.4. Modbus Function Codes	53
10.2.5. Transaction Properties	54
10.2.6. Duplicate Transaction	56
10.2.7. Delete Transaction	56
10.3. EtherCAT Settings	57
10.3.1. Export Product ESI File	57
10.3.2. EtherCAT Device ID	57
10.4. Security Settings	58
10.4.1. Local Time and Date	58
10.4.2. Network Time Protocol (NTP) Synchronization	58
10.4.3. Installing a Web Server Certificate	59
10.4.4. View Current Certificate	61
10.4.5. Update or Delete a Certificate	62
10.4.6. Secure Connection With HTTPS Mode	64
10.4.7. None Secure HTTP Mode	66
10.4.8. Device IP Address Discovery via HMS Software Applications	67
10.5. I/O Configuration	68
10.5.1. Map Area Object Order	69
10.5.2. Endian Swap	69
10.5.3. Map Area	70
10.5.4. Bit Offset	71
10.5.5. Convert Between Big-Endian and Little-Endian	74
10.5.6. Live List	75
10.5.7. Data Exchange Control	77
10.6. Configuration Notes	79
10.6.1. Add Configuration Note	79
10.6.2. View and Edit Configuration Notes	81
10.7. Apply Configuration	82
10.8. To Use an Existing Configuration	83
10.9. To Use a Legacy Modbus TCP Client Configuration	84
11. PLC Configuration	87
11.1. PLC Device Security	87
11.2. Export Product ESI File	87

11.3. CANopen over EtherCAT (CoE) Objects	88
12. Verify Operation	91
12.1. Communicator Status Monitor	91
12.2. Communicator LED Indicators	93
12.3. Ethernet RJ45 LED Indicators	95
13. Maintenance	96
13.1. Action on Fatal Error	96
13.2. Configuration Port IP Settings	97
13.3. Dashboard	98
13.4. Configuration File Handling	101
13.4.1. Export Configuration	101
13.4.2. Import Configuration	102
13.5. Clear and Revert Configuration	103
13.6. Firmware Management	104
13.6.1. View the Firmware Version	104
13.6.2. Firmware and Configuration Compatibility	104
13.6.3. Firmware File Validation	104
13.6.4. Update Firmware	105
13.7. Change Language	106
14. Troubleshooting	107
14.1. Diagnostics	107
14.1.1. I/O Data	107
14.1.2. Event Log	108
14.1.3. LED Status	109
14.2. Reset to Factory Settings	110
14.3. Firmware Upgrade Error Management	113
14.4. Support	116
14.4.1. Support Package	116
15. End Product Life Cycle	117
15.1. Secure Data Disposal	117
16. Technical Data	118
16.1. Technical Specification	118

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.

1.4. About the EtherCAT Terminology

The EtherCAT® Technology Group has changed the terminology for Master and Slave.

Master is called **MainDevice**

Abbreviated: **MDevice**

Slave is called **SubordinateDevice**

Abbreviated: **SubDevice**

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 \(page 110\)](#).

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.

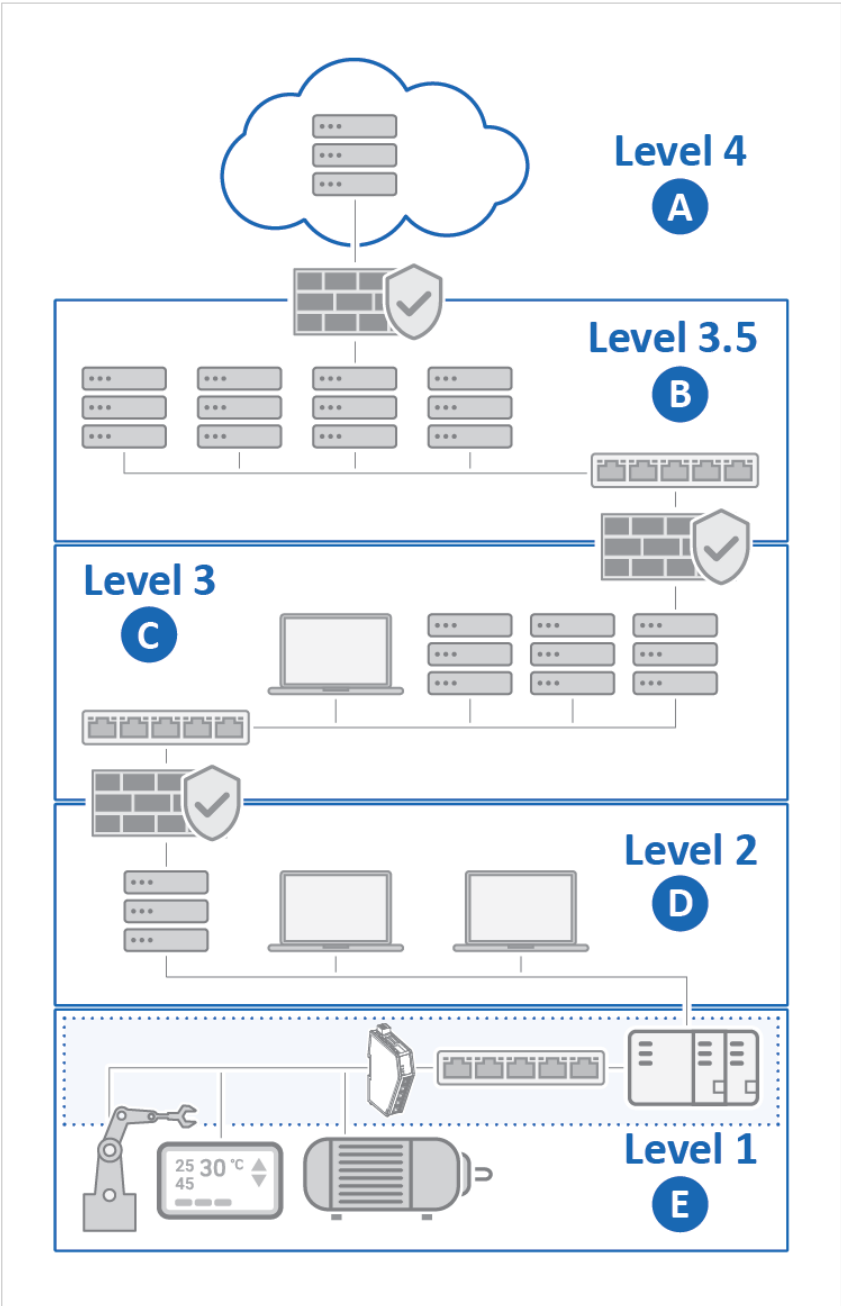


Figure 1. Purdue model, product security context

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

3.5. Supported Transport Layer Security (TLS) 1.2 Cipher Suites

The Communicator supports encrypted communication using TLS 1.2.

The following industry-recommended TLS 1.2 cipher suites are supported:

- ECDHE-ECDSA-WITH-AES128-GCM-SHA256
- ECDHE-ECDSA-WITH-AES128-CBC-SHA256
- ECDHE-RSA-WITH-AES128-GCM-SHA256
- ECDHE-RSA-WITH-AES128-CBC-SHA256
- RSA-WITH-AES128-GCM-SHA256
- RSA-WITH-AES128-CBC-SHA256
- RSA-WITH-AES256-CBC-SHA256

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 tool(s) 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

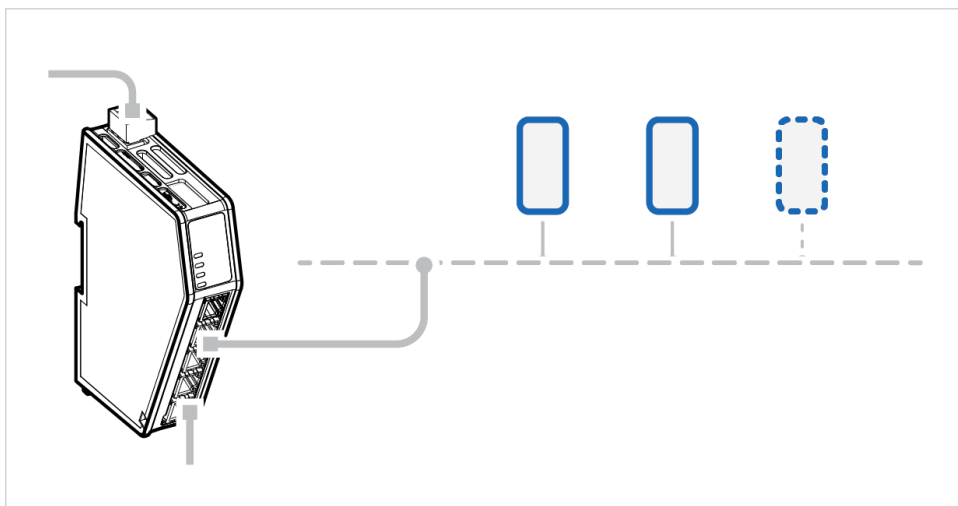


Figure 2. Servers on a Modbus TCP subnetwork

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

Servers and Transactions

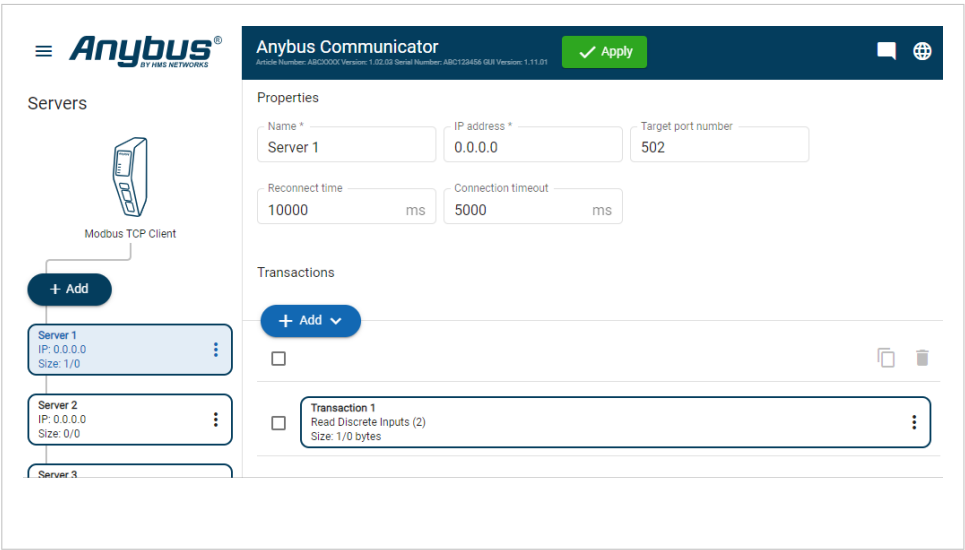


Figure 3. Server with Transactions

Transactions are based on standard Modbus transactions and define the data to be sent or received. See also [\(page 53\)](#).
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.

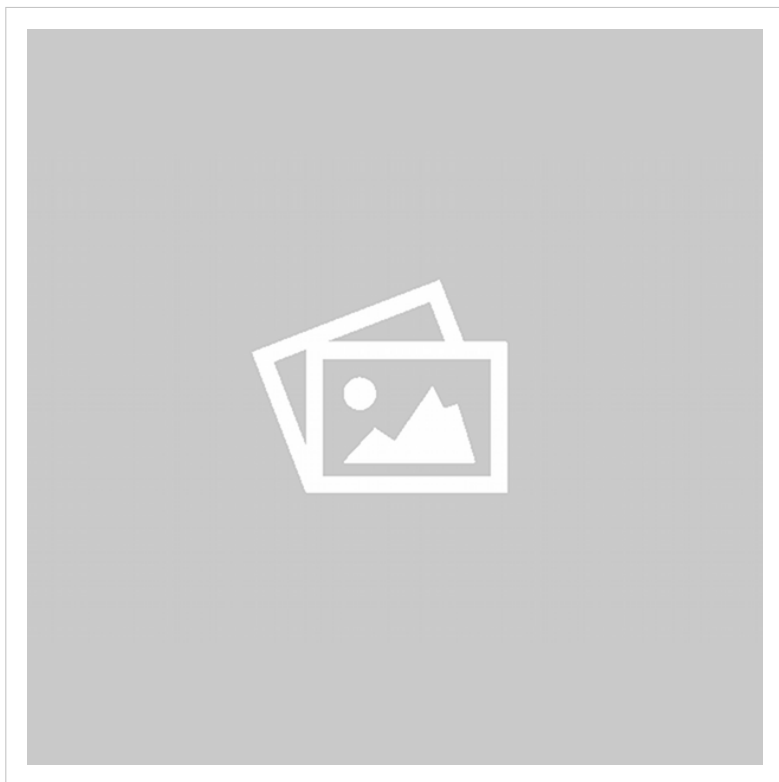


Figure 4. Process data traffic overview

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

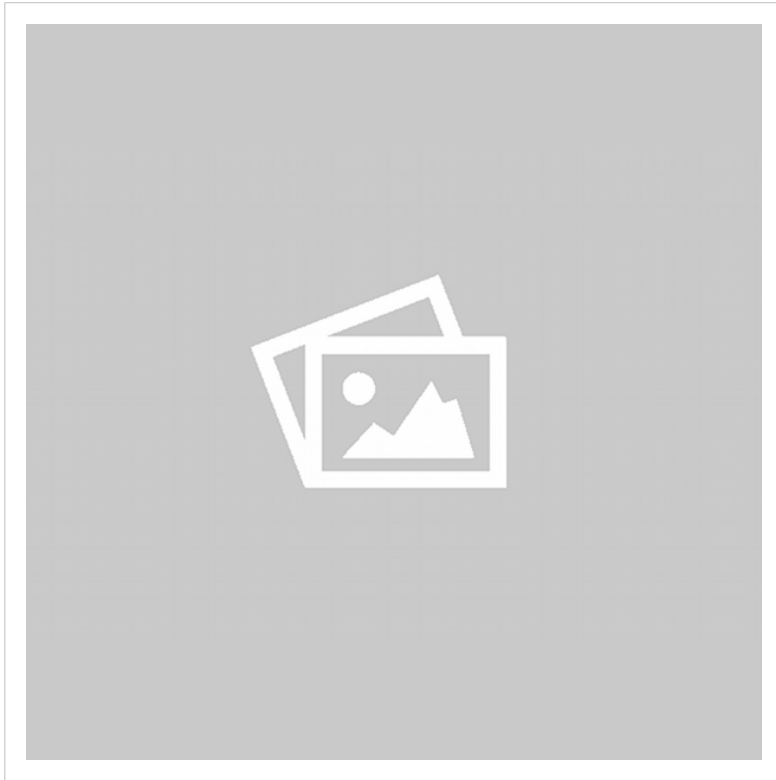


Figure 5. Process data traffic from servers to client

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

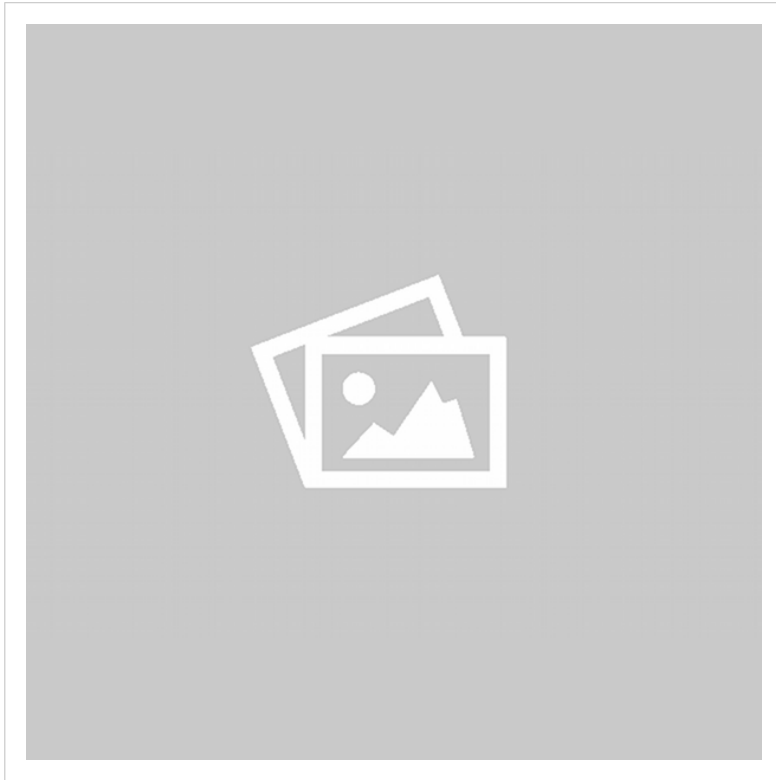


Figure 6. Process data traffic from client to servers

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

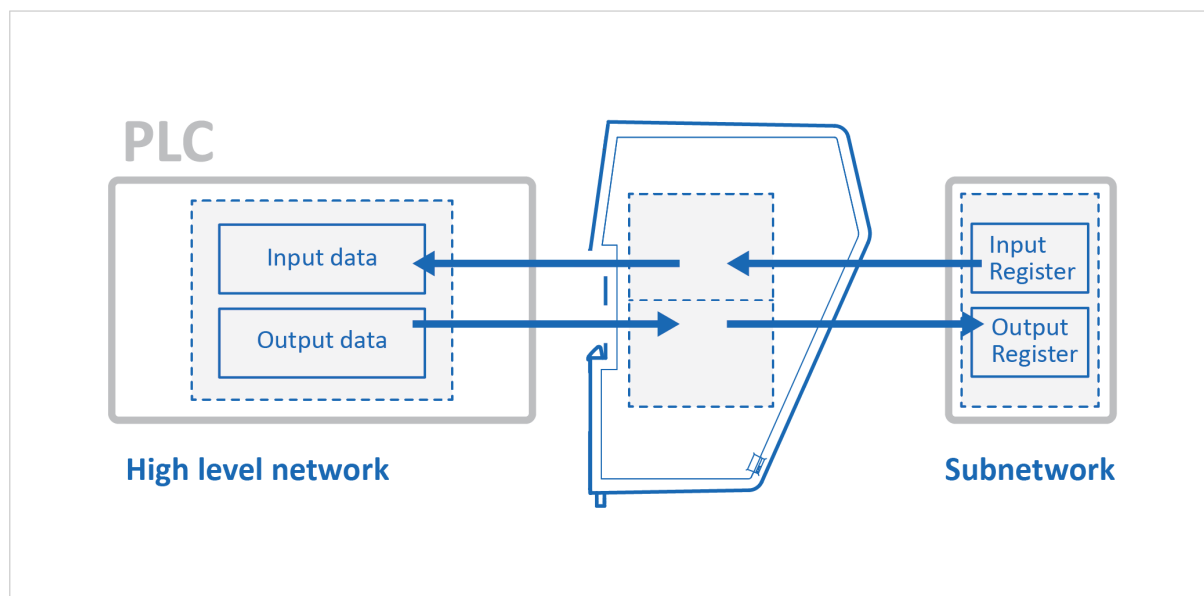


Figure 7. The Communicator internal memory areas

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

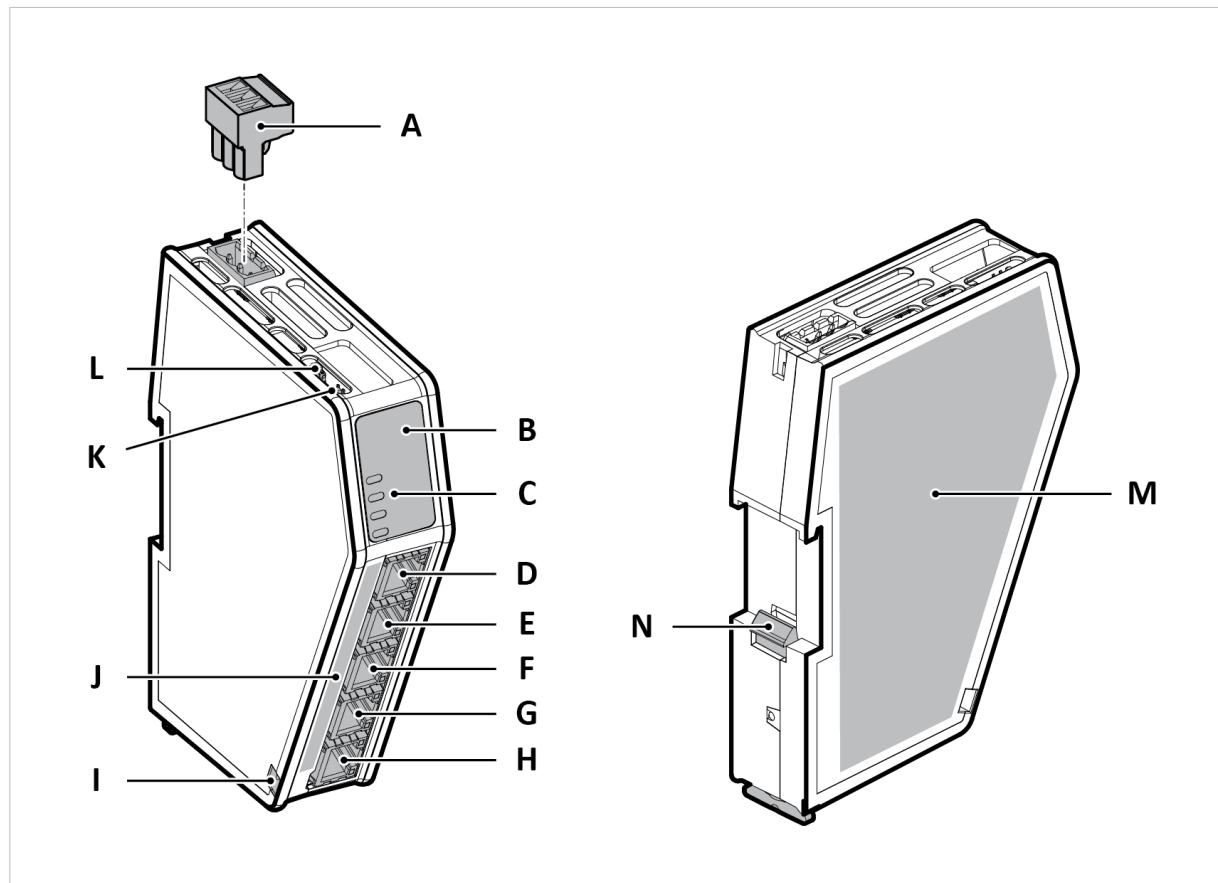


Figure 8. Communicator external parts

- | | | |
|-------------------------------|--|--|
| A. Power connector | 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. EtherCAT (X3.IN) connector — Input | M. Laser engraved label with product information |
| D. Configuration port | H. EtherCAT (X3.OUT) connector — Output | N. DIN rail locking mechanism |
| | I. Cable tie mount | |
| | J. Laser engraved connectors designation | |

6.2. Connector Port Guide

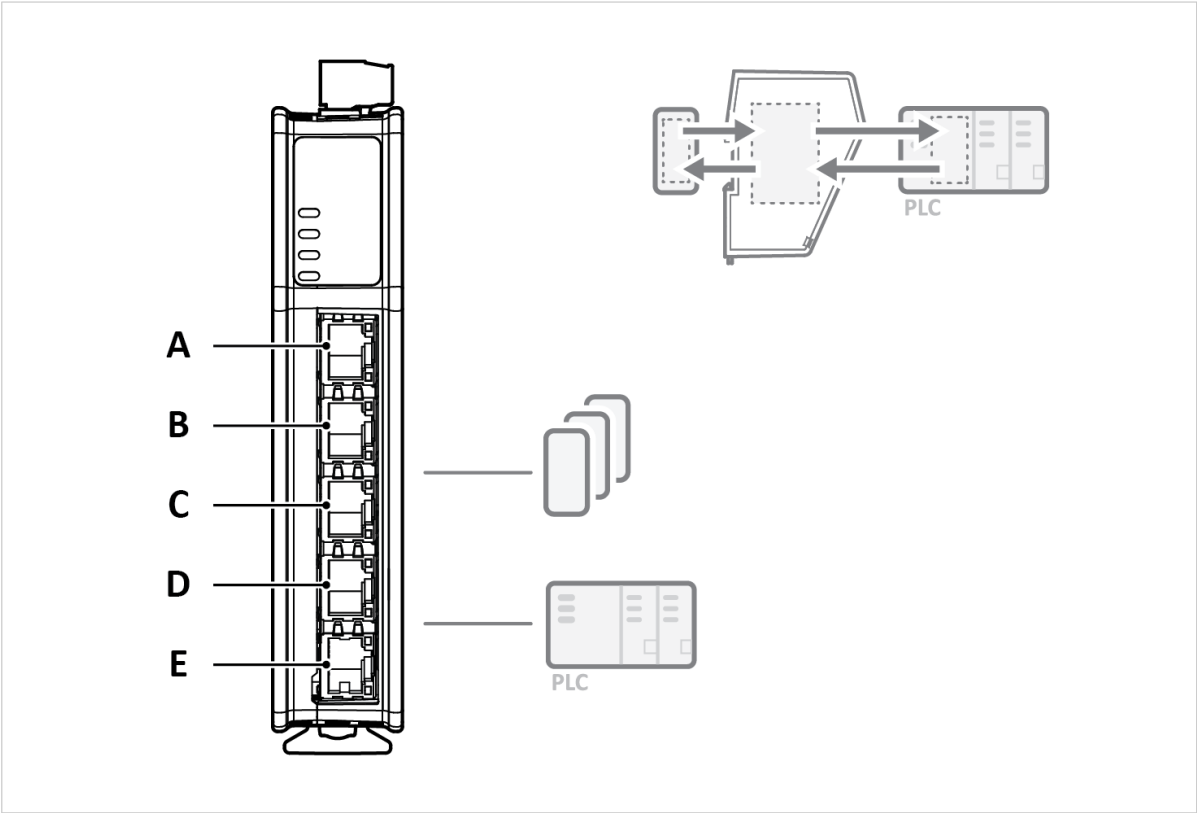


Figure 9. Communicator connector ports

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

See Also

- [Connect To Modbus TCP Client Network \(Page 19\)](#)
- [Connect To EtherCAT Network \(Page 21\)](#)

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.

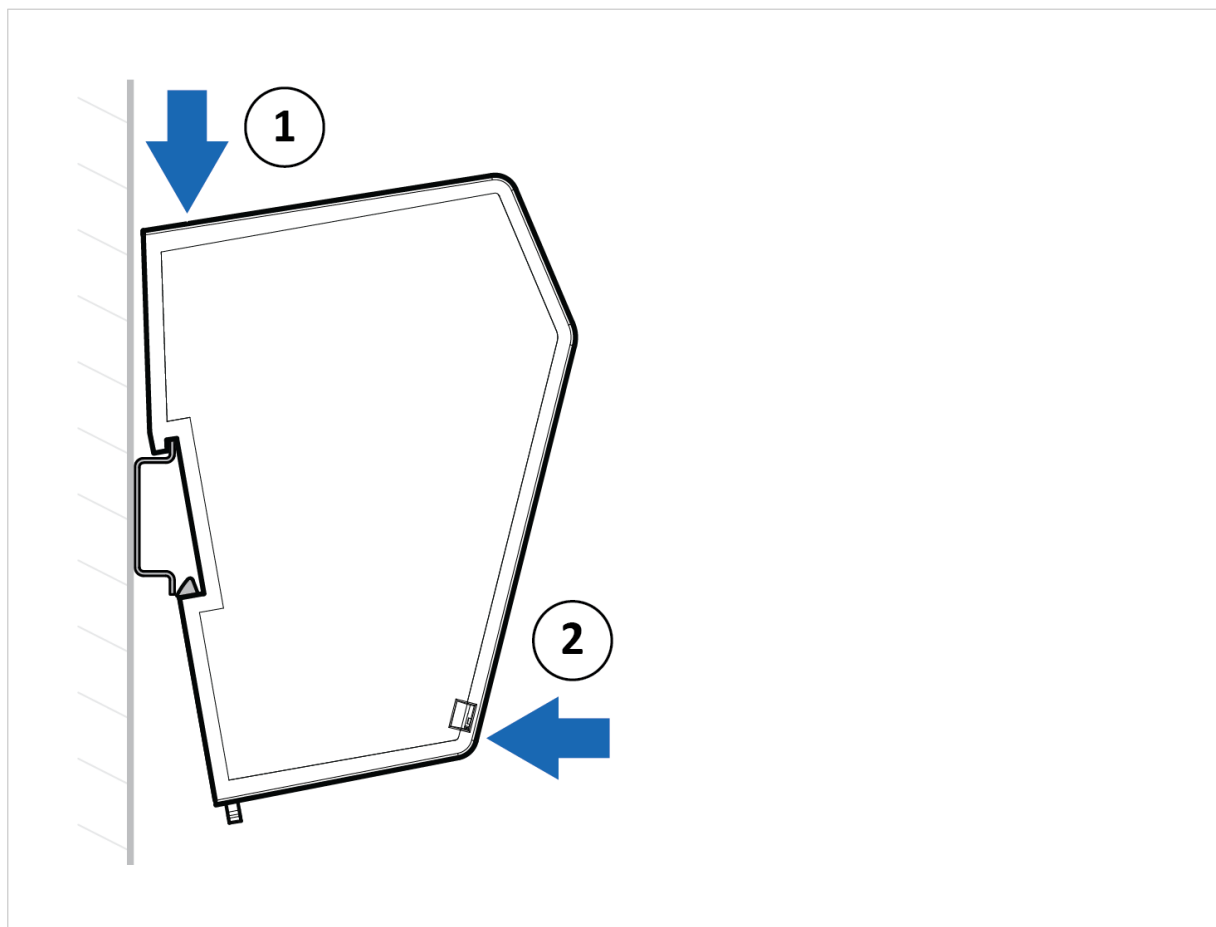


Figure 10. Attach the Communicator on the DIN rail

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

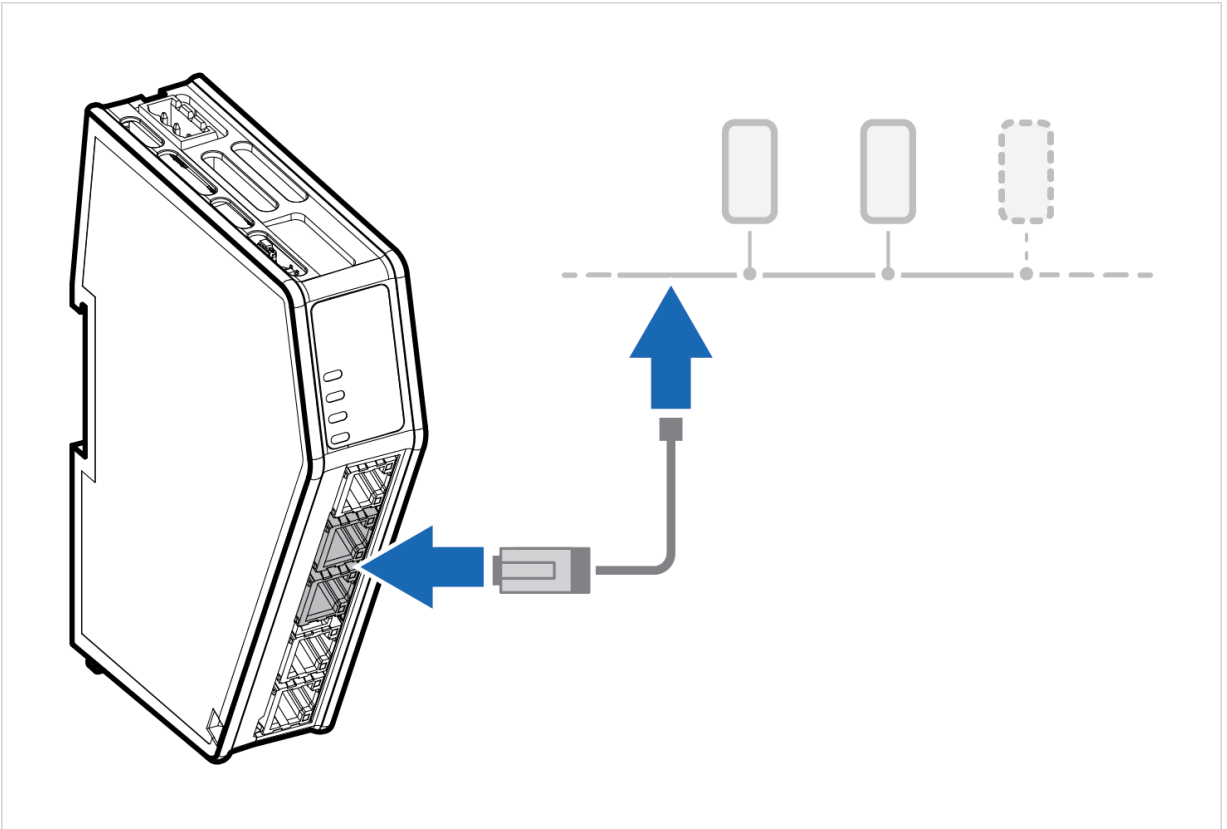
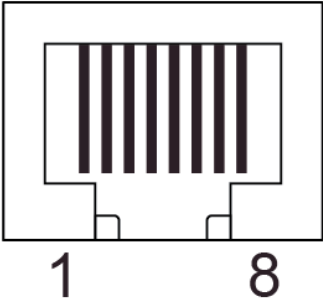


Figure 11. Connect to Modbus TCP Client network

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 \(Page 17\)](#)
- [Connect To EtherCAT Network \(Page 21\)](#)
- [Connect To Power \(Page 22\)](#)

[Communicator Status Monitor \(Page 91\)](#)

[Communicator LED Indicators \(Page 93\)](#)

[LED Status \(Page 109\)](#)

[Firmware Upgrade Error Management \(Page 113\)](#)

6.5. Connect to EtherCAT Network

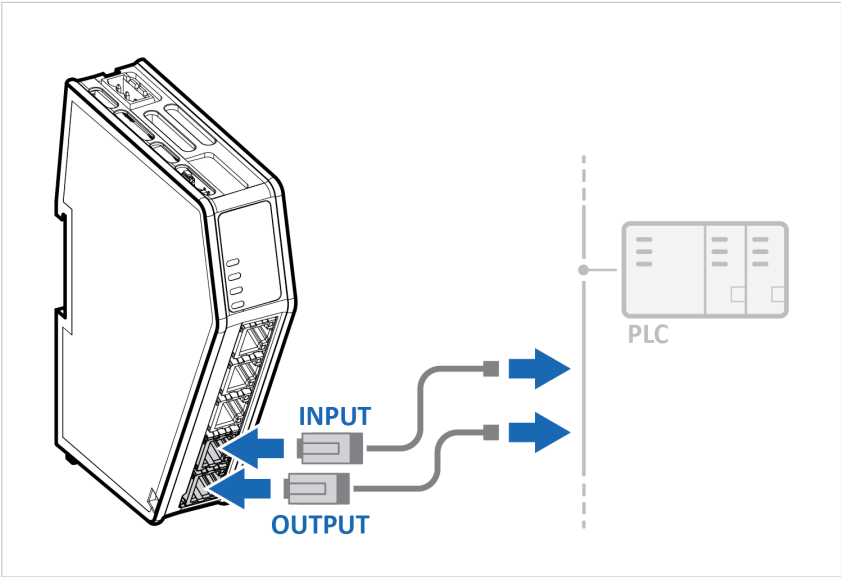


Figure 12. Connect to EtherCAT network

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 EtherCAT network.

- Upper EtherCAT Connector: Input
- Lower EtherCAT Connector: Output

See Also

- [Connector Port Guide \(Page 17\)](#)
- [Connect To Modbus TCP Client Network \(Page 19\)](#)
- [Connect To Power \(Page 22\)](#)
- [Communicator Status Monitor \(Page 91\)](#)
- [Communicator LED Indicators \(Page 93\)](#)
- [LED Status \(Page 109\)](#)
- [Firmware Upgrade Error Management \(Page 113\)](#)

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.

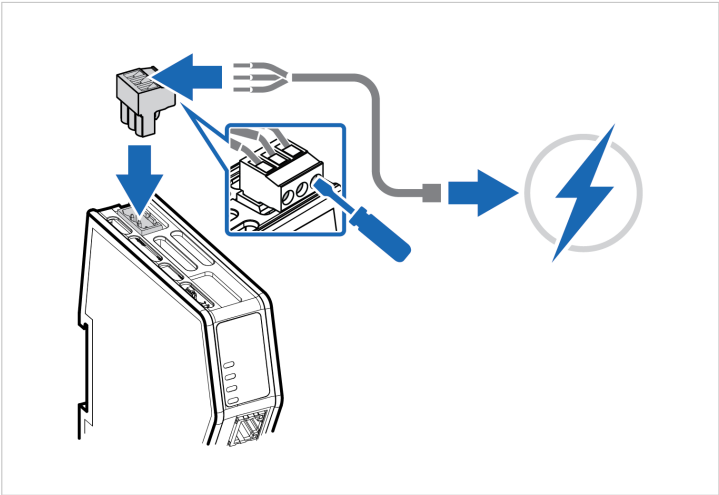


Figure 13. Connect to power

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.

See Also

- [Connect To Modbus TCP Client Network \(Page 19\)](#)
- [Connect To EtherCAT Network \(Page 21\)](#)
- [Communicator Status Monitor \(Page 91\)](#)

[Communicator LED Indicators \(Page 93\)](#)

[LED Status \(Page 109\)](#)

[Firmware Upgrade Error Management \(Page 113\)](#)

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

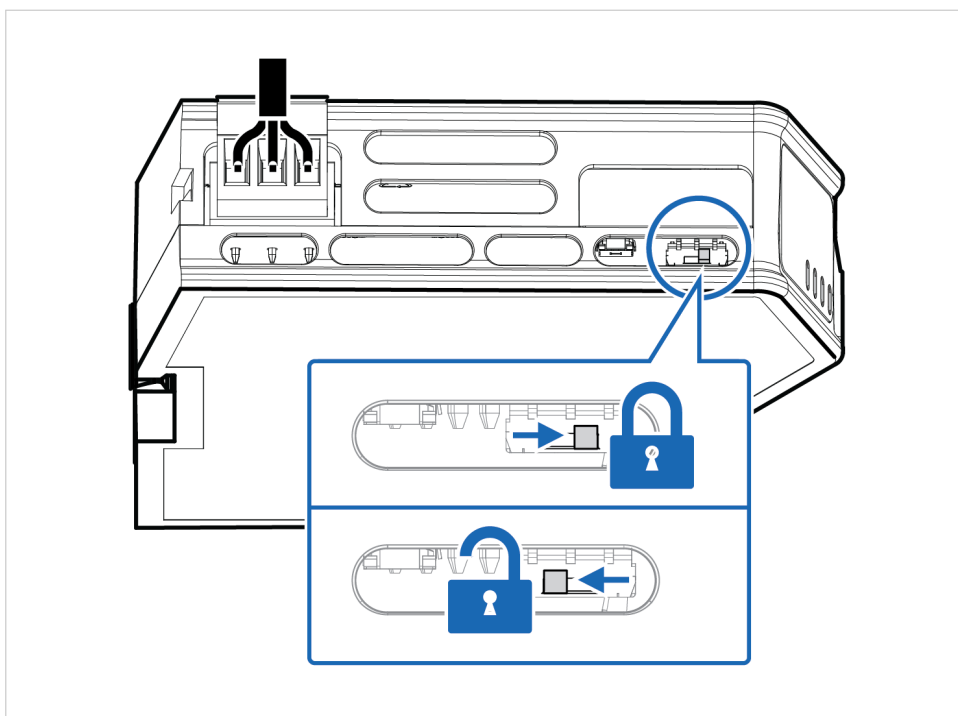


Figure 14. Security switch in locked and unlocked position

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

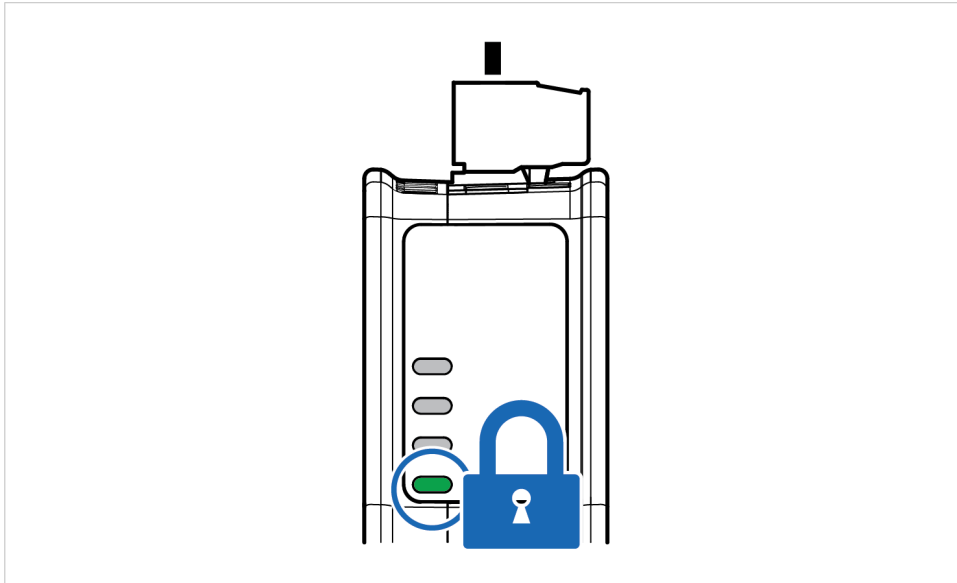


Figure 15. Security switch locked status LED

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

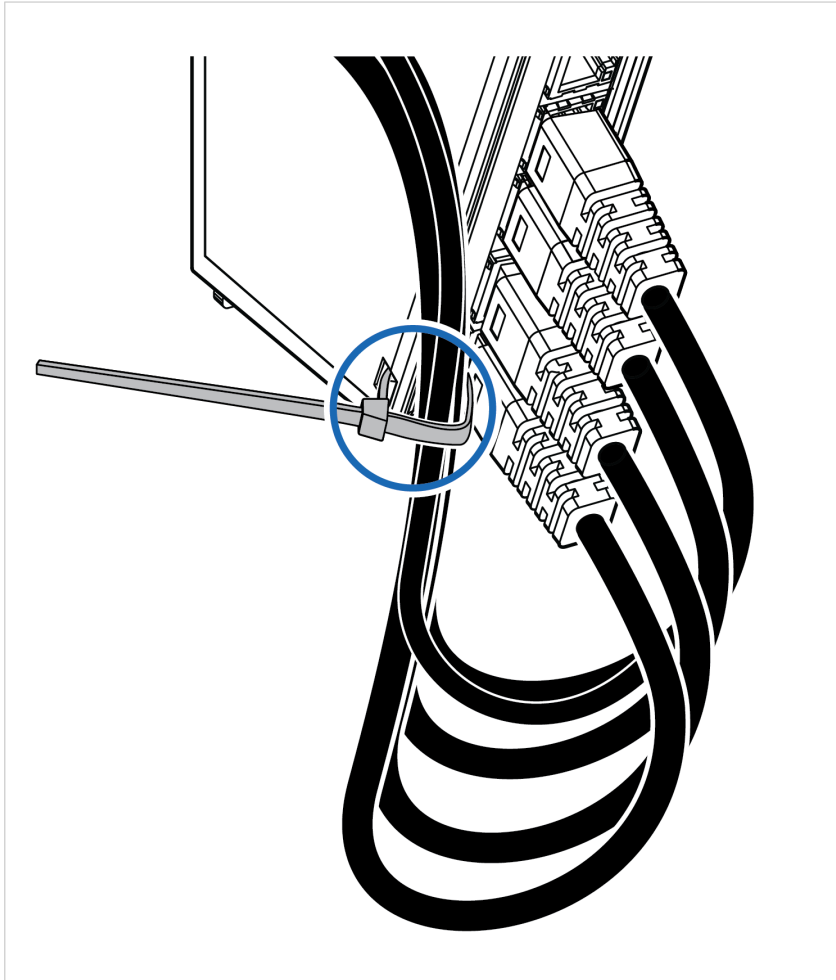


Figure 16. Lock the cables

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:

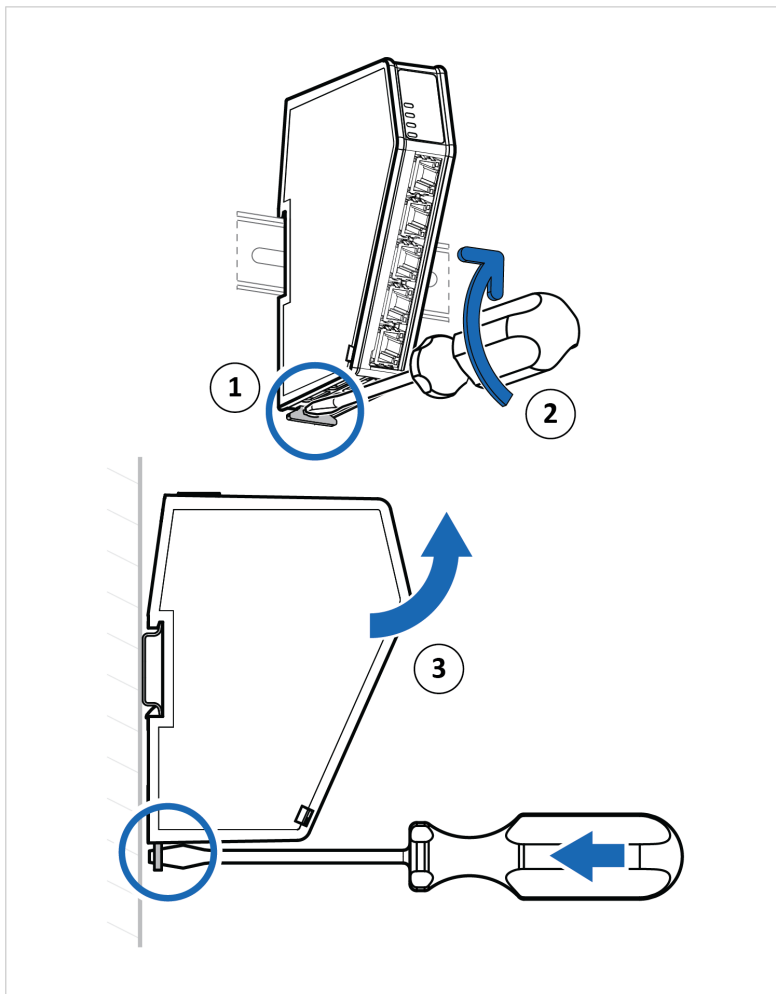


Figure 17. Unlock and unhook the Communicator

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. Accessing the Communicator

7.1. Connect to Configure the Communicator

Procedure

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

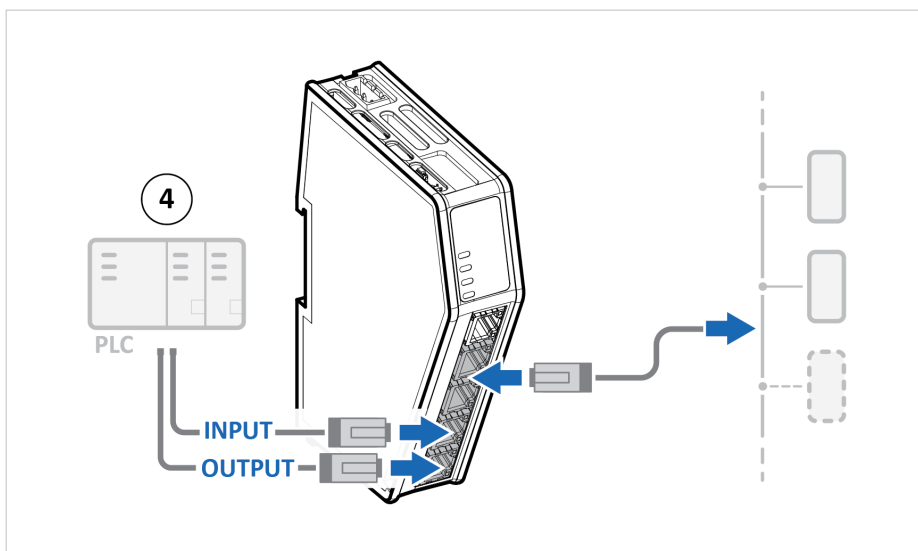


Figure 18. Connect to networks

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

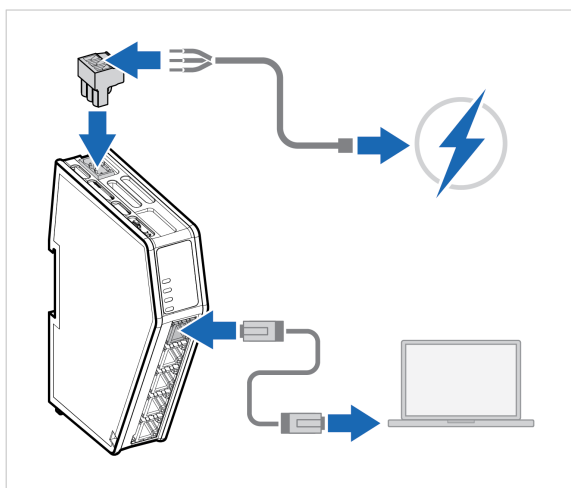


Figure 19. Connect to PC and power

7.2. 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.

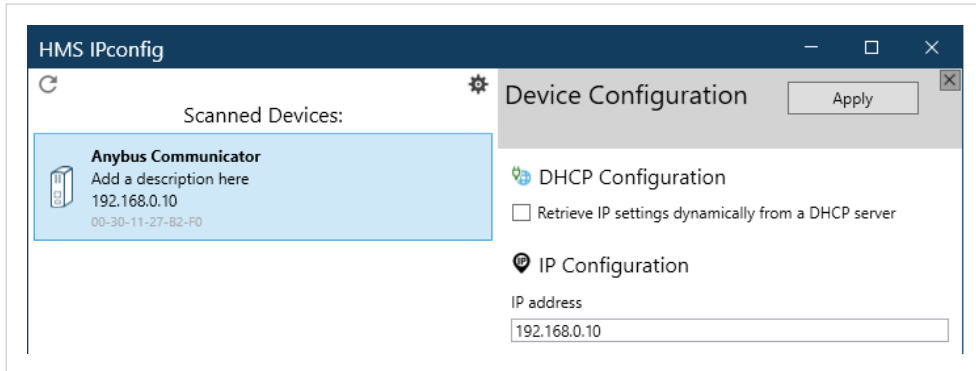
Procedure

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

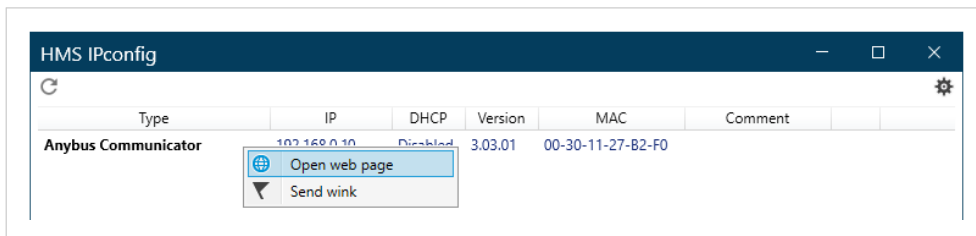


- HMS IPconfig automatically starts scanning for compatible and active HMS devices.
 - Found HMS devices are added to the device list.
3. To open the settings pane, click on the Communicator in the device list.

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

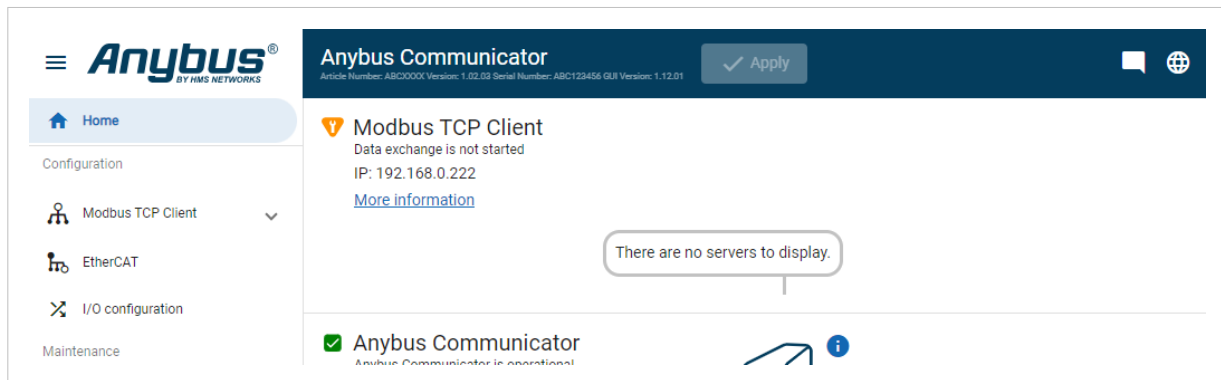


5. To open the **Open web page** built-in web interface, click Communicator.



Result

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



7.3. 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

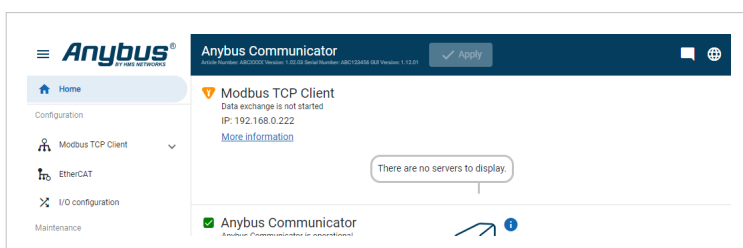
1. On the PC accessing the Communicator built-in web interface, set a static IP address within the same IP address range as the Communicator IP address.



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**.



7.4. Communicator Built-In Web Interface Overview

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

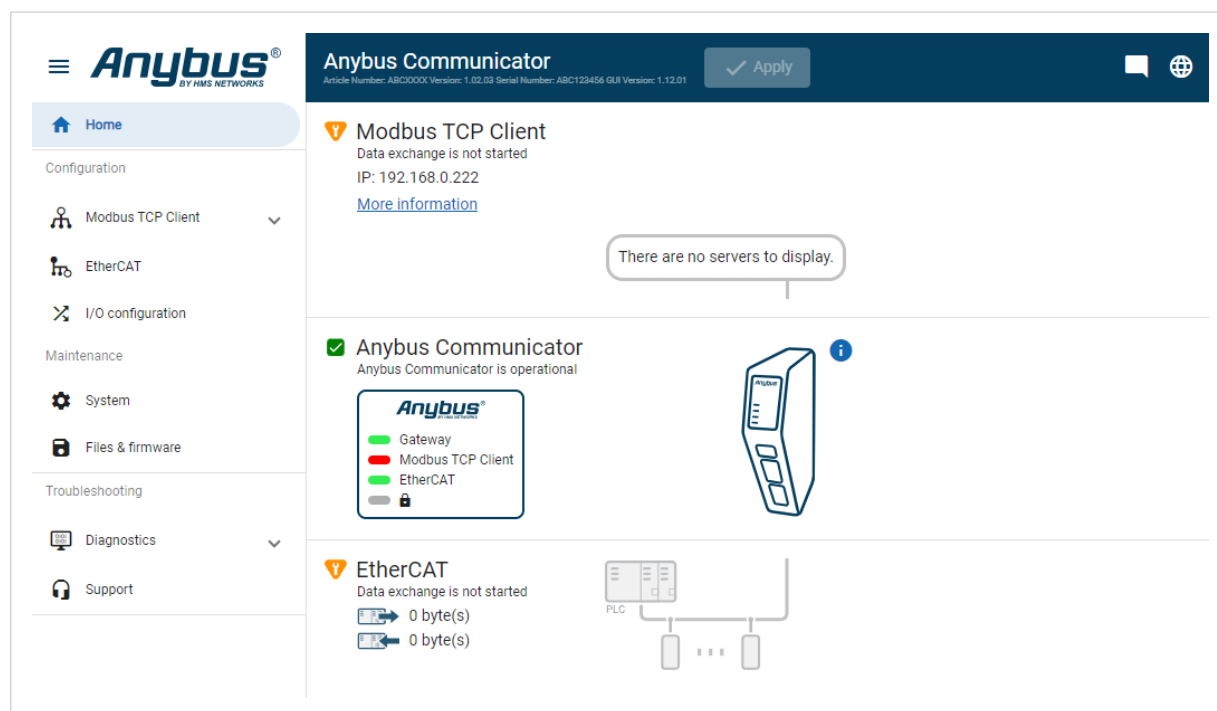


Figure 20. The Communicator built-in web interface Home page

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). Add server(s) and configure the Connections settings. Configure communication and add servers and transactions.
EtherCAT	There are no settings for EtherCAT, no configuration is needed.
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. Role Management

8.1. Roles Overview

The Communicator provides enhanced security through user roles with different permissions levels.

Role	Default	Permission	Password Management
Administrator	Enabled	Full access to all features and settings. Can manage other roles.	Require password to login. Default password is printed on the product housing.
Operator	Disabled	Read-only access.	Blank password by default. Administrator can enable password protection. The password can be set and changed by the Operator.
User	Disabled	Configure IO-device/adaptor/ server/slave network, maintenance and diagnostics.	Administrator can enable role. Default password is printed on the product housing.

8.2. Roles Configuration Access

Administrator Role - Full Access

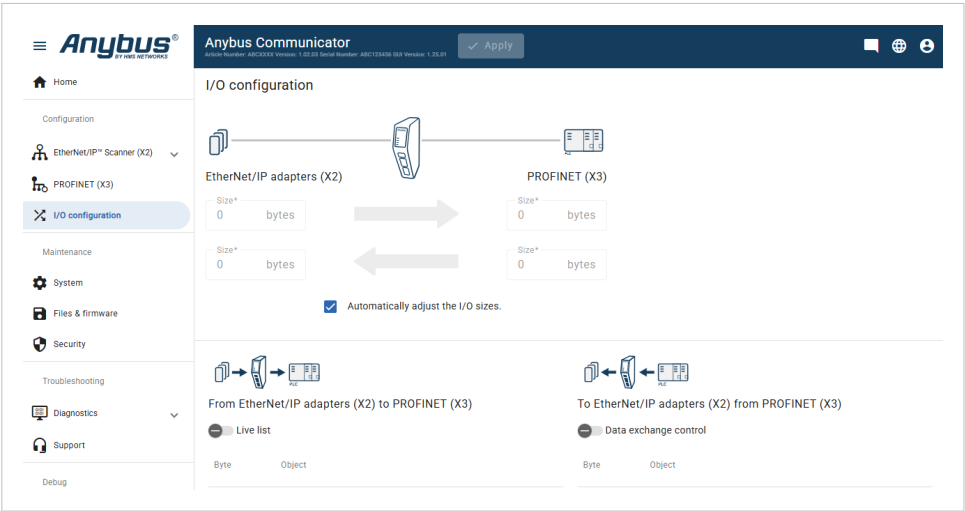


Figure 21. Example: Editable I/O configuration settings

The Administrator role has full access to all configuration settings in the Communicator web interface. All settings are available for viewing and editing without restrictions.

Operator Role - Limited Access

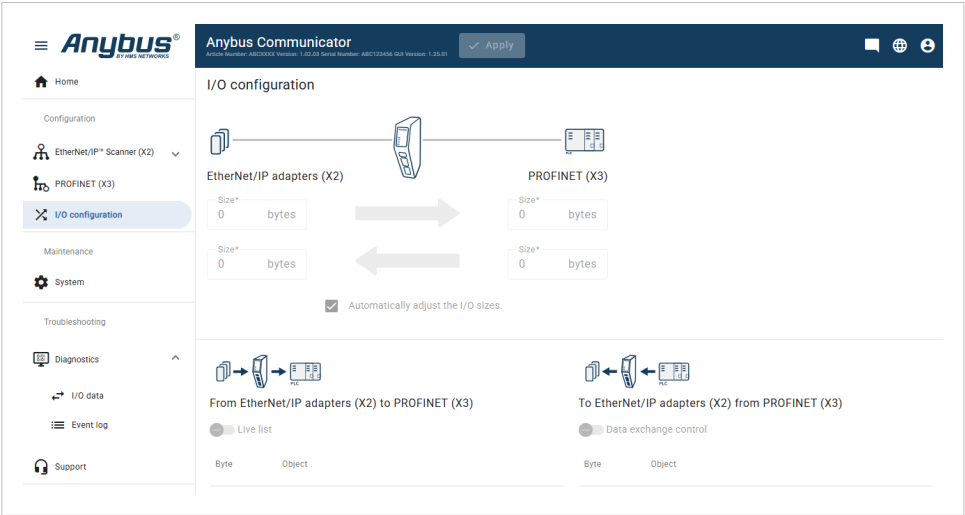
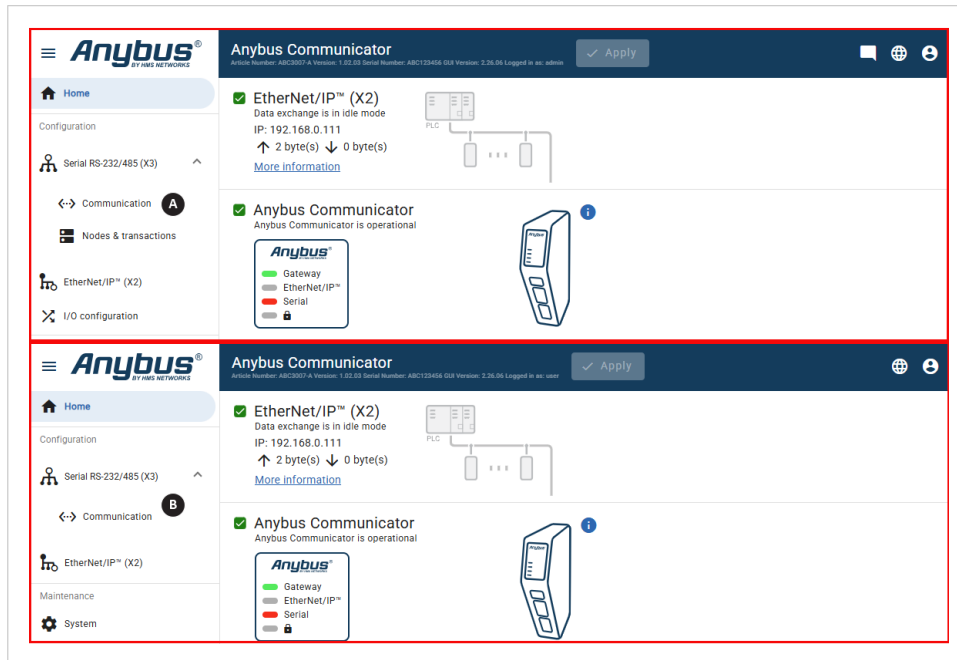


Figure 22. Example: Locked and grayed-out I/O configuration settings

The Operator role has read-only access to the configuration settings in the Communicator web interface. Restricted settings are locked and grayed out.

User Role - Configuration Access



A. Administrator

B. User

Figure 23. Example: Menu visibility by user role

The User role provides limited access to the configuration options in the Communicator web interface.

Controller network configuration settings are not available for the User role.

Other restricted settings are locked and grayed out.

8.3. Set Up Roles

By default, **Roles** are disabled, and the user is automatically logged in to the Communicator web interface. No user identity or credentials are required.

Before You Begin



NOTE

The Communicator includes default credentials: username *admin* (lowercase) and password printed on the product housing.



NOTE

If no password is set for a User account, the default password printed on the product housing is used. Always set a password during account activation.

Procedure



IMPORTANT

Enable HTTPS before activating roles to ensure passwords are encrypted.

Activate Roles:

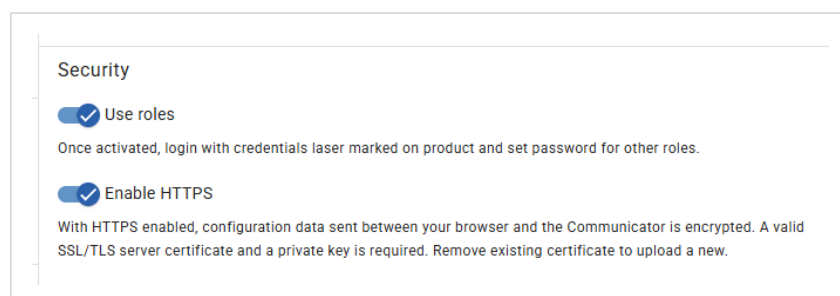


Figure 24. System page with Use role(s) activated

1. Open the **System** page.
2. In the **Security** section, click the **Use roles** toggle to activate roles.
3. Click **Apply** in the web interface header.

Manage Roles and Passwords:

1. When roles are enabled for the first time, log in using the default credentials printed on the product housing.
If an administrator password has already been configured, use that password instead.

- From the **Role** drop-down menu, select the role to configure: **Administrator**, **Operator**, or **User**.

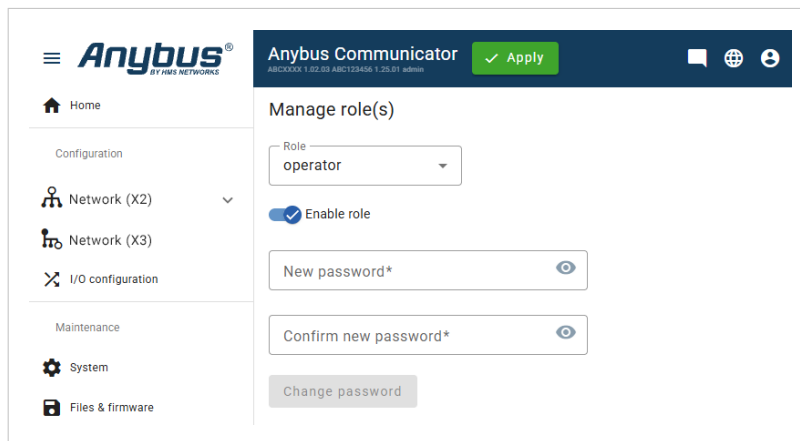


Figure 25. Manage role(s) page

- Enter the password in the **New password** field.
 - Re-enter the password in the **Confirm password** field.
 - Click **Change password** to confirm.
- The settings are applied. If the password is changed for the currently logged-in role, you are automatically logged out.

Result

Roles are enabled, and the factory default mode that does not require user credentials is turned off.

You will now be prompted to enter a username and password to access the Communicator web interface.

8.4. Set or Change Password

Procedure

Change the Communicator web interface login password:

1. In the web interface header, click  **Account** > **Manage role(s)**.

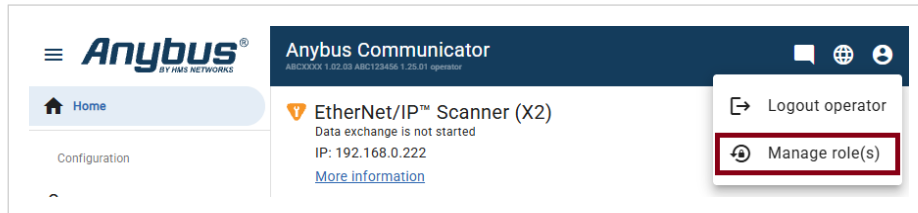


Figure 26. Account menu, **Manage role(s)**

2. From the **Role** drop-down menu, select the role for password update.

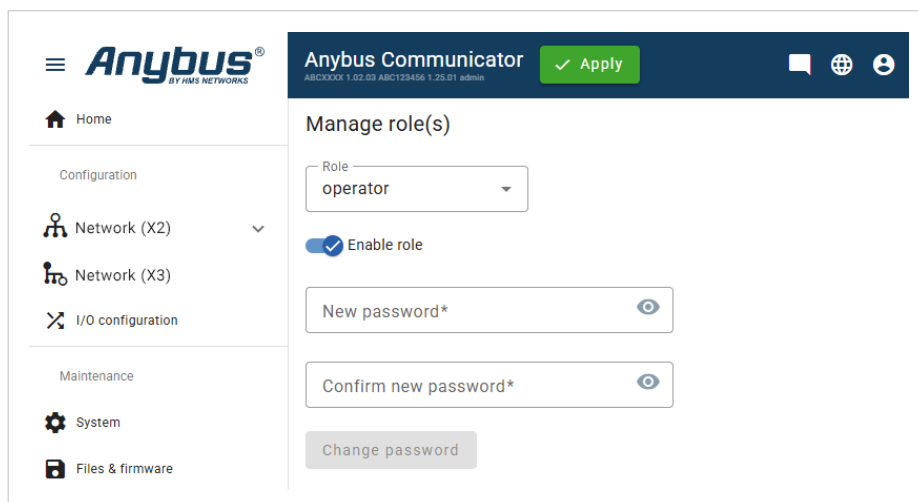


Figure 27. Manage roles(s) page

3. Enter the new password in the **New password** field.
4. Re-enter the new password in the **Confirm password** field.
5. Click **Change password** to confirm.
The password is applied and you are automatically logged out.

8.5. Logout From the Communicator Web Interface

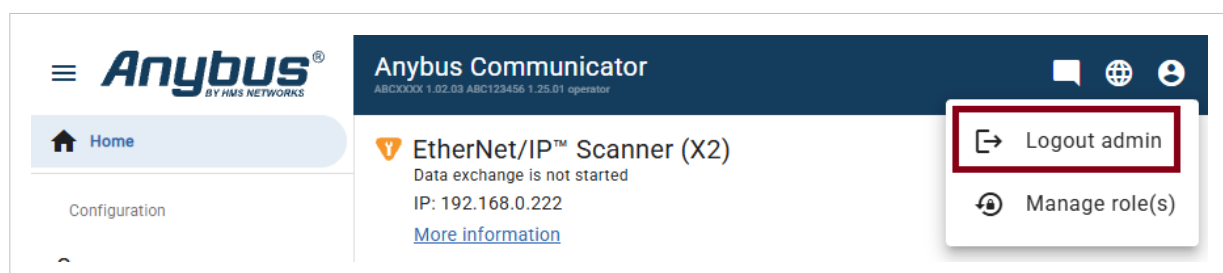


Figure 28. Account menu, Logout

Click  **Account** in the web interface header, then select **Logout** from the menu.

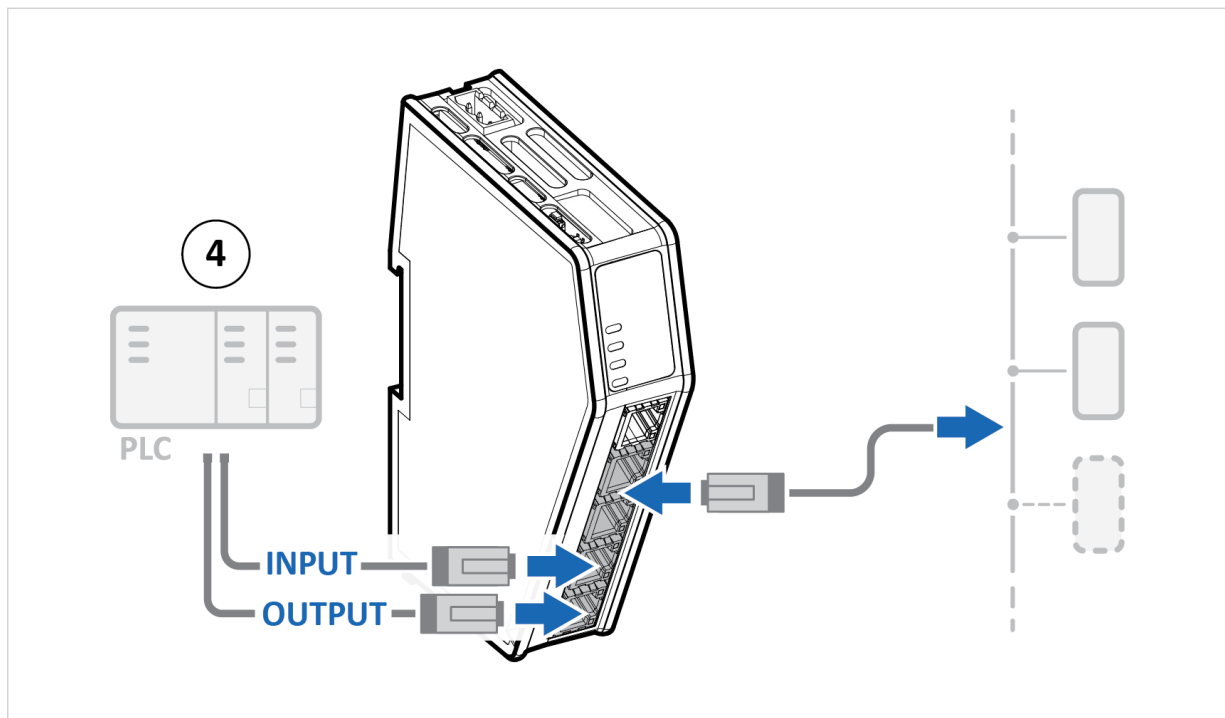
9. Configuration Quick Guide

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 \(page 48\)](#).

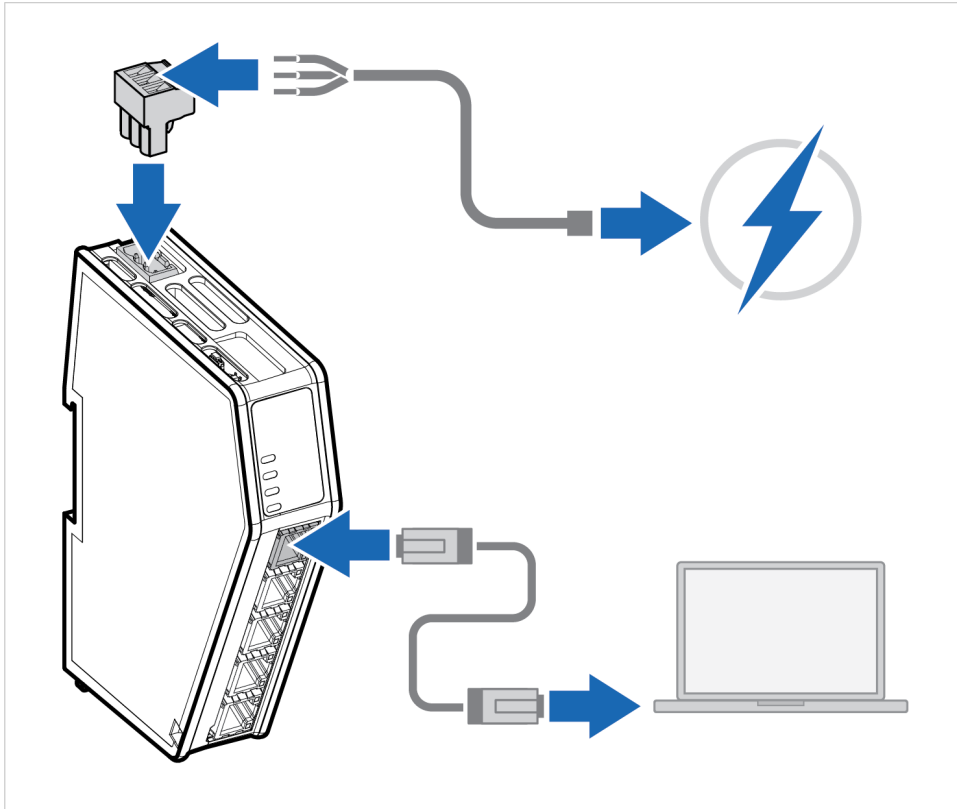
9.1. Prepare Configuration

Connect to Networks



1. Connect the Communicator to the Modbus TCP Client network.
2. Connect Communicator to the EtherCAT network.
 - Upper EtherCAT Connector: Input
 - Lower EtherCAT Connector: Output

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

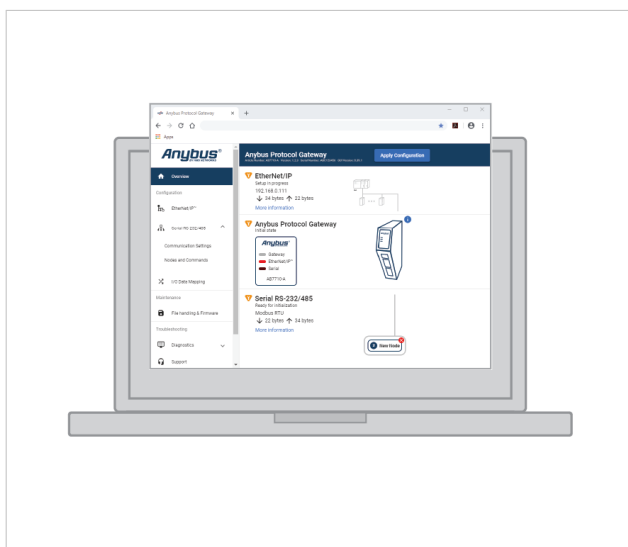


Change the IP address on the Communicator configuration port to one within the same IP address range as your PC.

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.

9.2. Security Setup

On the System page in the **Security** panel:

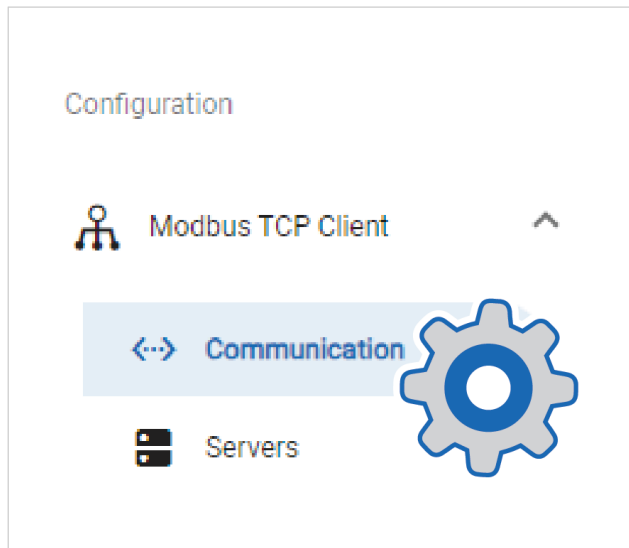
Before you begin configuring the Communicator, review these key **Security** settings:

- User roles: Enable login and assign access levels.
- Secure Connection (HTTPS): Turn on encrypted access and upload the private key and certificate.
- Time settings: Set the correct local time and enable time synchronization to ensure a valid certificate and accurate event timing.

9.3. Setup New Configuration

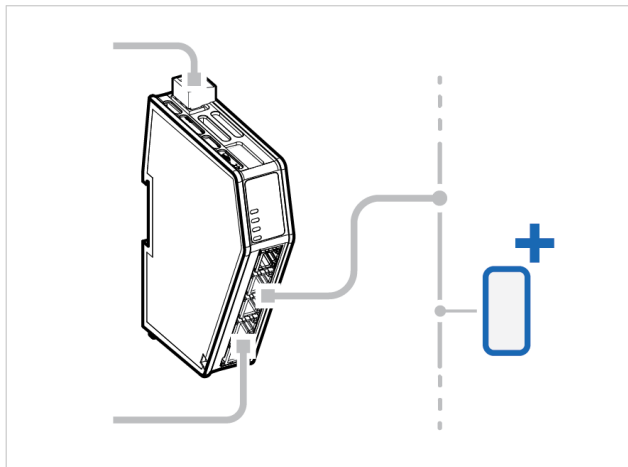
Follow these steps to setup a new Communicator configuration.

1. Subnetwork configuration



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

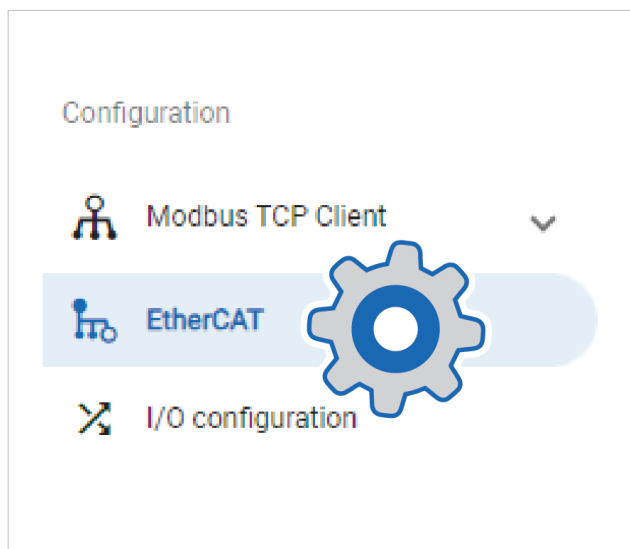
2. Add Servers



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.

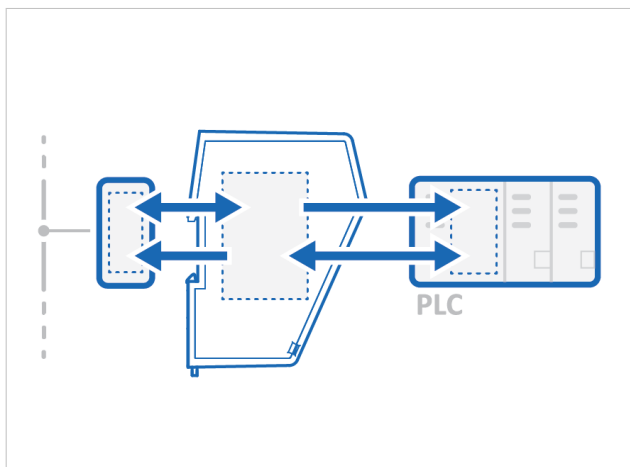
3. High level network configuration



On the **EtherCAT** page:

Option if the PLC program requires a product file, ESI (EtherCAT SubDevice Information) file: Click **ESI file** to download the file.

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.

9.4. PLC Configuration

In the In the Communicator Built-In Web Interface

- Download ESI File

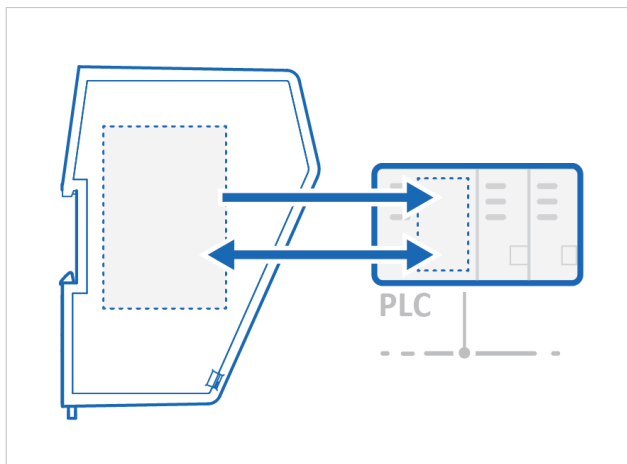


Optional if the PLC program requires an ESI (EtherCAT SubDevice Information) file.

On the **EtherCAT** page: Download the ESI file to your PC.

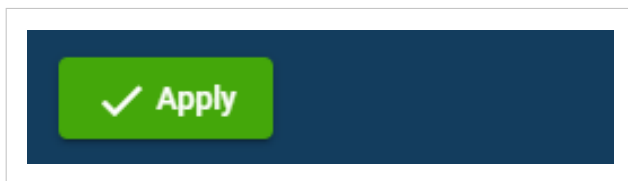
In the PLC Program

1. Optional if the PLC program requires an ESI (EtherCAT SubDevice Information) file.
Import the ESI 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.



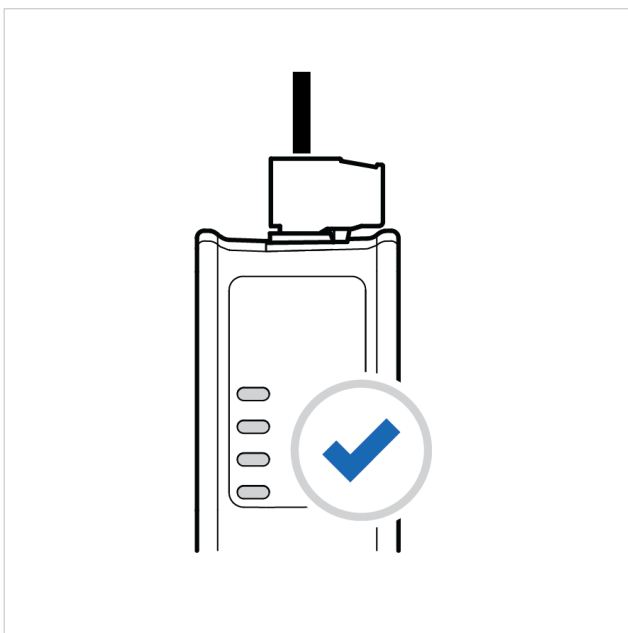
9.5. Verify Operation

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 **EtherCAT** side, including any configured endian conversions.
- **Event log** page to detect failures and unexpected behavior over time.

10. 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 \(page 39\)](#).

10.1. Modbus TCP Client Communication Settings

Configure the Modbus TCP Client communication settings.

10.1.1. IP Settings

Anybus Communicator
Article Number: ABC2007-A EIP Version: 1.2.3 Serial Number: ABC123456 EIP GUI Version: 1.2.2

☒ Apply

IP Settings

☐ DHCP enabled

IP address: 192.168.0.222 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

Figure 29. 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.

10.2. Modbus TCP Client Servers

10.2.1. 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.

The screenshot shows the Anybus Communicator web interface. The top header bar is dark blue with the Anybus logo, version information, and an 'Apply' button. The left sidebar has a 'Servers' menu item. The main content area is divided into two sections: 'Properties' and 'Transactions'. The 'Properties' section contains input fields for 'Name *' (Server 1), 'IP address *' (0.0.0.0), 'Target port number' (502), 'Reconnect time' (10000 ms), and 'Connect timeout' (5000 ms). The 'Transactions' section has a '+ Add' button. Below these sections is a list of servers, currently showing 'Server 1' with IP 0.0.0.0 and Size 0/0. A '+ Add' button is also present in the sidebar.

Figure 30. Modbus TCP Client, Server page

3. Repeat until you have added all your servers.

To Do Next

Configure the server Properties, see [Server Properties \(page 51\)](#).

10.2.2. Server Properties

Procedure

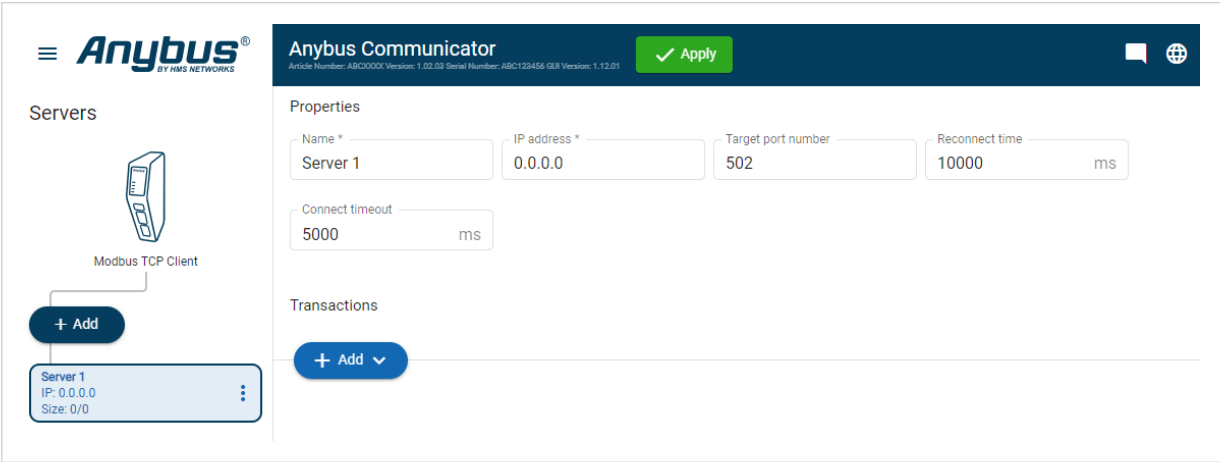


Figure 31. Servers page, Properties

- 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 \(page 52\)](#).

10.2.3. 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.

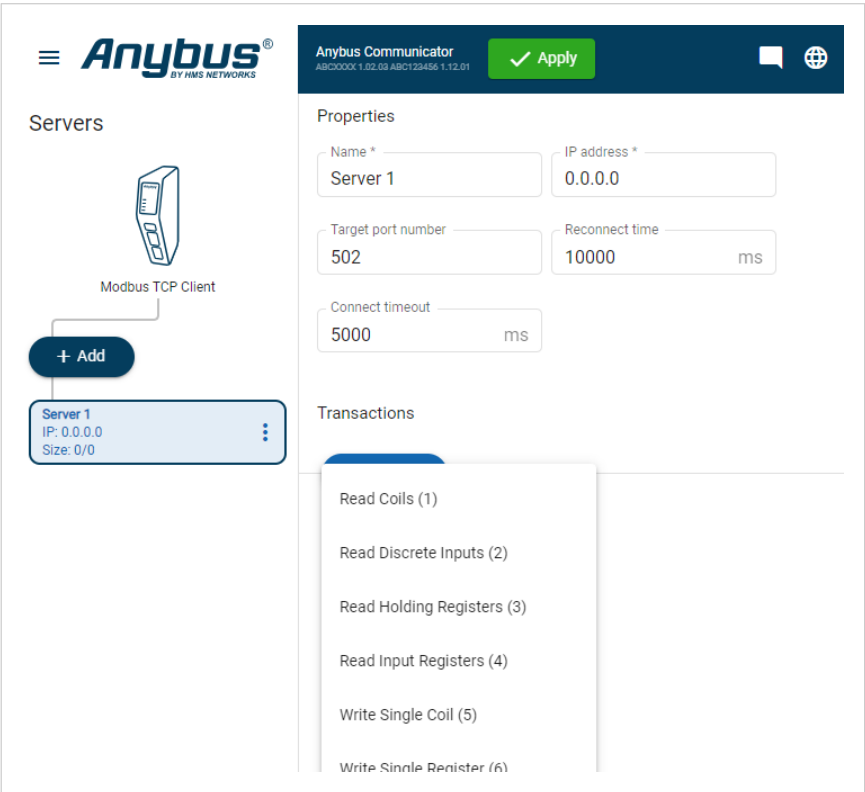


Figure 32. Add Modbus transactions

3. Repeat until you have added all your transactions.

To Do Next

Configure the transaction Properties settings, [Transaction Properties \(page 54\)](#).

10.2.4. 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.

10.2.5. Transaction Properties

Before You Begin

For Modbus transaction reference guide, refer to [Modbus Function Codes \(page 53\)](#).

Procedure

The screenshot shows the Anybus Communicator software interface. On the left, there is a 'Servers' panel with a 'Modbus TCP Client' icon and a '+ Add' button. Below it, a list shows 'Server 1' with IP: 0.0.0.0 and Size: 1/0. The main area is divided into 'Properties' and 'Transactions' sections. The 'Properties' section includes fields for Name (Server 1), IP address (0.0.0.0), Target port number (502), Reconnect time (10000 ms), and Connect timeout (5000 ms). The 'Transactions' section has a '+ Add' button and a list showing 'Transaction 1' with Read Coils (1) and Size: 1/0 bytes. On the right, the 'Transaction properties' sidebar is open, showing fields for Name (Transaction 1), Modbus function (Read Coils (1)), Read starting address (0), Quantity of bits (1), Timeout time (1000 ms), Inhibit time (1000 ms), and Unit ID (255).

Figure 33. 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.

10.2.6. Duplicate Transaction

When you duplicate a transaction, all settings are preserved.

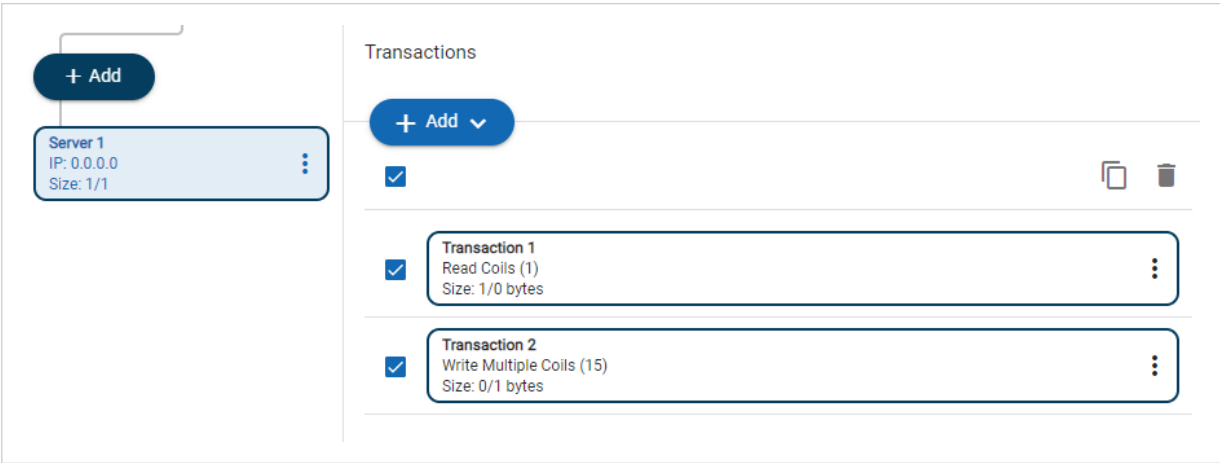


Figure 34. Duplicate transaction

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.

10.2.7. Delete Transaction

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

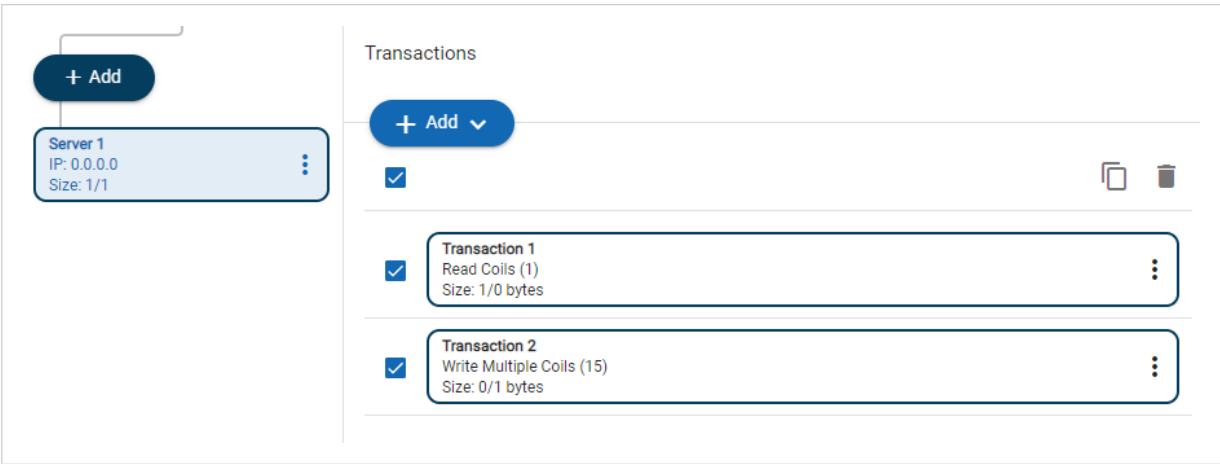


Figure 35. Delete transaction

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**.

10.3. EtherCAT Settings

Configure the EtherCAT network settings.

10.3.1. Export Product ESI File

Option for EtherCAT.

Option if the PLC program requires a product file, ESI (EtherCAT SubDevice Information) file to configure the EtherCAT PLC to use the Communicator

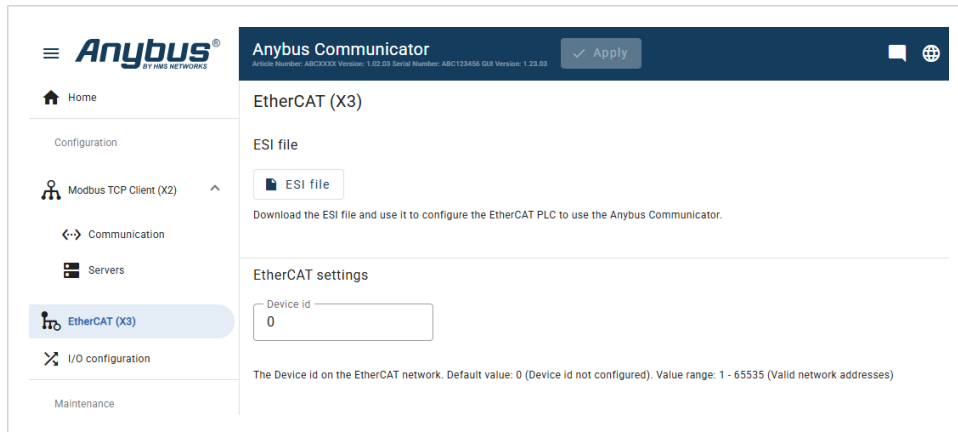


Figure 36. Export Product ESI File

You find the *EtherCAT ESI* file on the Communicator built-in web interface **EtherCAT** page.

To export the ESI file:

1. To save the configuration, click **Apply**.
The **ESI file** button is activated.
2. Click **ESI file**.
The ESI file is downloaded to your PC.

10.3.2. EtherCAT Device ID

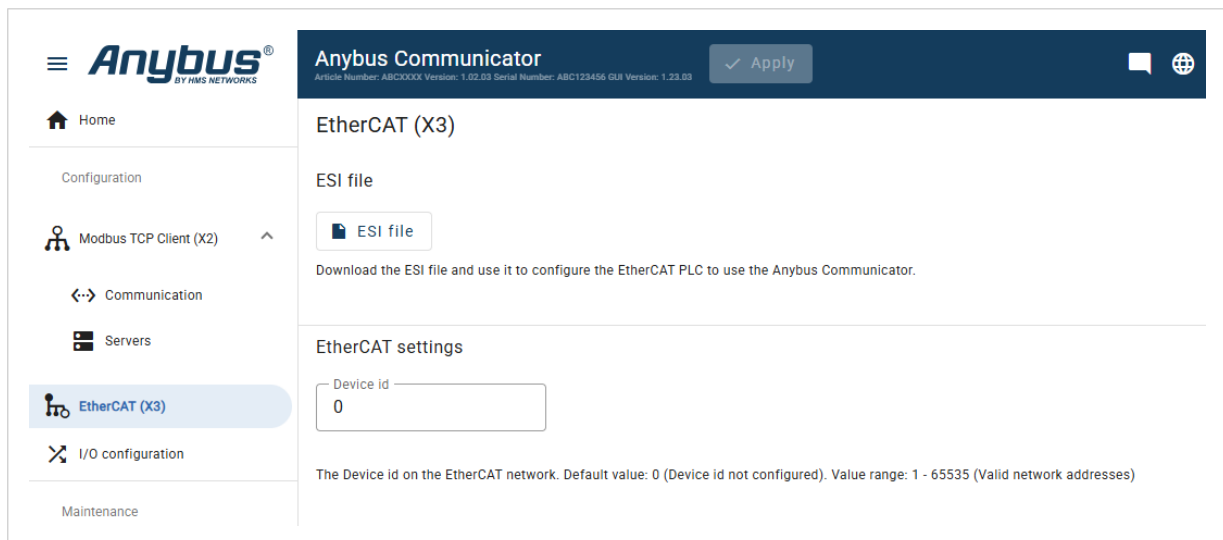


Figure 37. EtherCAT Page, Device id

An EtherCAT Device id is a unique identifier to recognize, distinguish and manage the Communicator within the network.

By default, the Device id is not configured, and its value is set to 0.

Valid value range: 1 - 65535

10.4. Security Settings

10.4.1. Local Time and Date

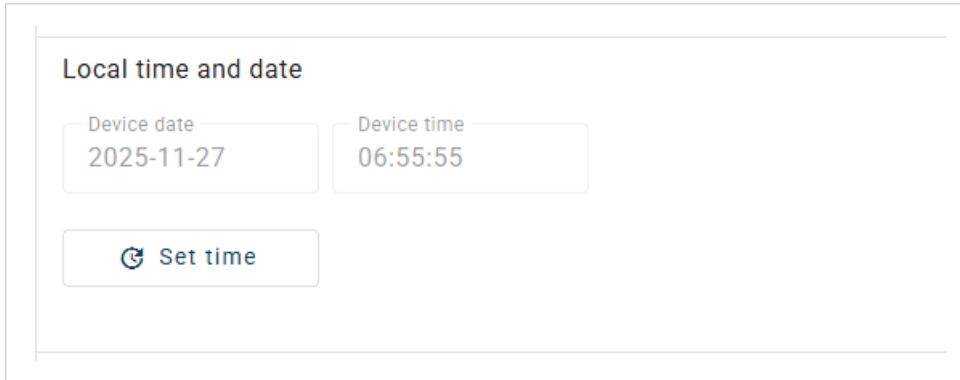


Figure 38. System page, Local time and date

You can synchronize the time in the Communicator with the current browser time and date.

Make sure the system clock on the computer connected to the Communicator is accurate before setting the time.

On the **System** page, in the **Local time and date** panel, click **Set time** to synchronize the Communicator with the time and date from the browser on the connected computer.

10.4.2. Network Time Protocol (NTP) Synchronization

The Communicator can use the **Network Time Protocol (NTP)** to synchronize its clock with network time servers.



Figure 39. System page, Time synchronization

By default, **NTP synchronization** is disabled.

To use **NTP synchronization**:

1. On the **System** page, click the **NTP synchronization** toggle.
2. In the **NTP server*** field, enter the server name or IP number of the NTP server.
3. In the **NTP port*** field, enter the port number used by the NTP server for communication.

10.4.3. Installing a Web Server Certificate

Install a web server certificate in the Communicator.

Before You Begin

**IMPORTANT**
A factory reset of the Communicator will erase all stored web server certificates.

**NOTE**
The web server certificate and private Key must be provided as two separate files.

**NOTE**
The web server certificate must be a Base64 encoded DER certificate in PEM format.

**NOTE**
If the web server certificate is used for HTTPS, the subject name (CN) must match the device address (IP or DNS name).

Procedure

To install web server certificate:

Security

☒ Use roles

Once activated, login with credentials laser marked on product and set password for other roles.

☐ HTTPS disabled

With HTTPS enabled, configuration data sent between your browser and the Communicator is encrypted. A valid SSL/TLS server certificate and a private key is required.
Remove existing certificate to upload a new.
NOTICE: The device must be rebooted after toggling HTTPS before the change becomes active.

Private key

Certificate

Select a new certificate file and upload it to the Communicator. You must first upload the private key before your certificate.

Device discovery

Read-only

Controls if the device IP address can be discovered by stand alone HMS tools including IP Config.

Local time and date

Device date

2026-01-27

Device time

09:14:17

Set time

Figure 40. System page, Security settings

1. Open the **System** page.

2. Upload the private key:
 - a. Click **Private key**,
 - b. In the **Upload private key** window, click **Select private key file (.pem)**.
 - c. In the **Open** dialog box, browse to and select the private key file and click **Open**.

**NOTE**

Ensure the .pem file corresponds to the SSL/TLS certificate.

- d. Click **Upload key**.
The message 'Private key uploaded successfully' appears when the upload is complete.
3. Upload the web certificate:
 - a. Click **Certificate**.
 - b. In the **Upload certificate** window, click **Select certificate file (.crt)**.
 - c. In the **Open** dialog box, browse to and select the web server certificate file and click **Open**
 - d. Click **Upload certificate**.
The message 'A new certificate has been uploaded.' appears when the upload is complete.
 - e. The web server certificate appears in the **Security** section.
4. Enable **Secure Connection (HTTPS)**:
Click the slide toggle HTTPS.
Secure connection encrypts data sent between your browser and the server.
See also [Secure Connection With HTTPS Mode \(page 64\)](#).

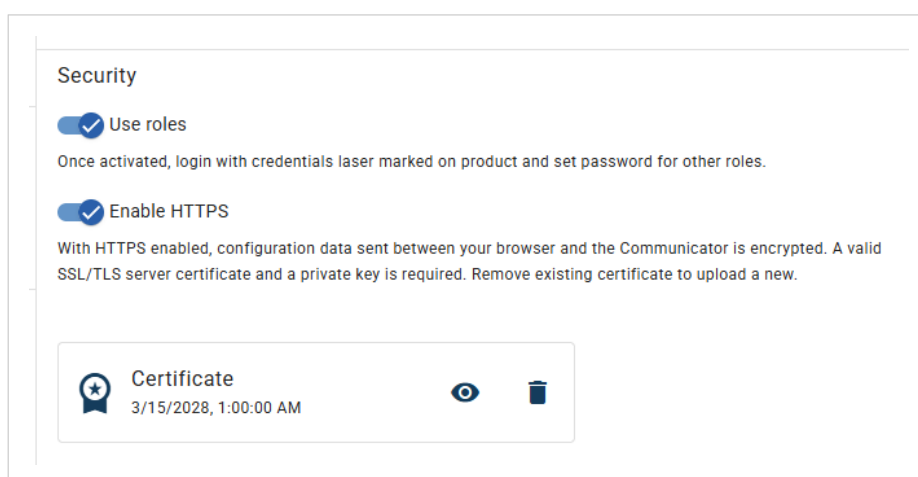


Figure 41. HTTPS enabled

5. Click **Apply** in the web interface header.
6. For the setting to take effect, restart the Communicator by disconnecting and reconnecting its power supply.

10.4.4. View Current Certificate

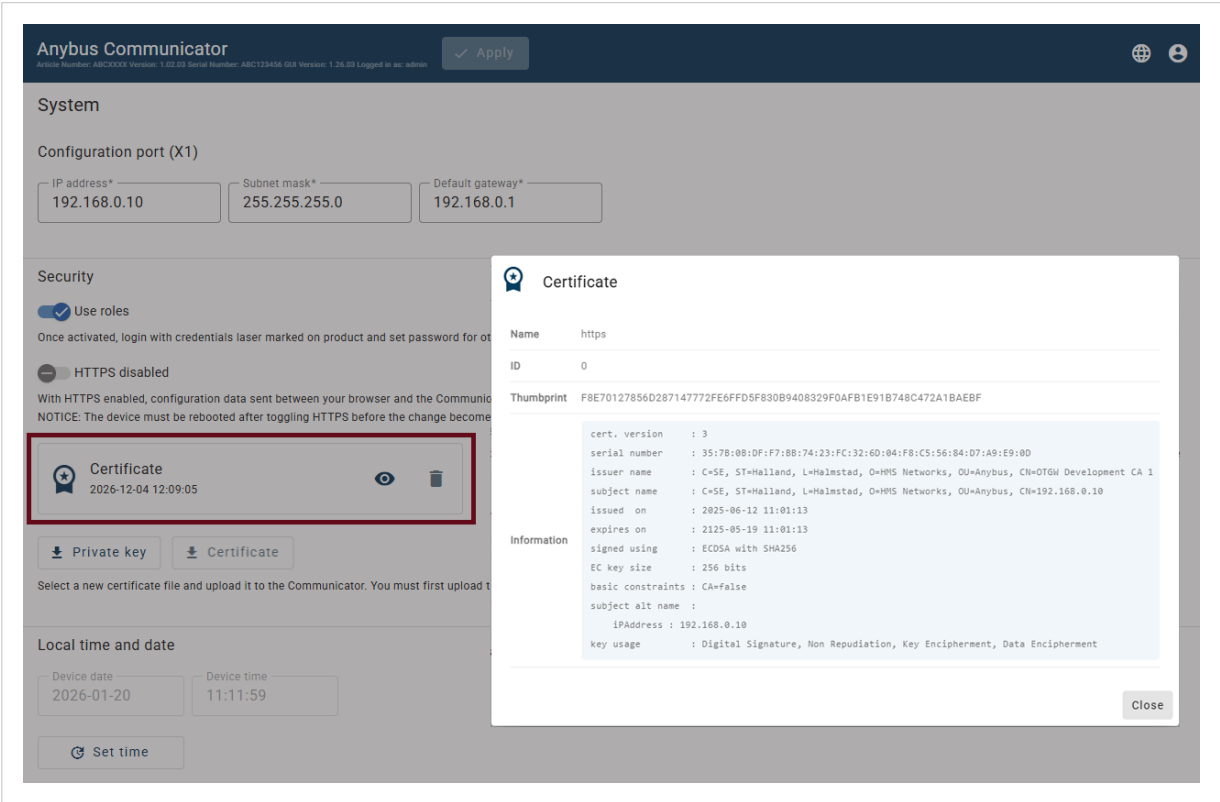


Figure 42. System page, View current certificate

To view the currently uploaded web server certificate, click the **View** (eye) icon.

The **Certificate** window opens.

10.4.5. Update or Delete a Certificate

Update an Existing Certificate

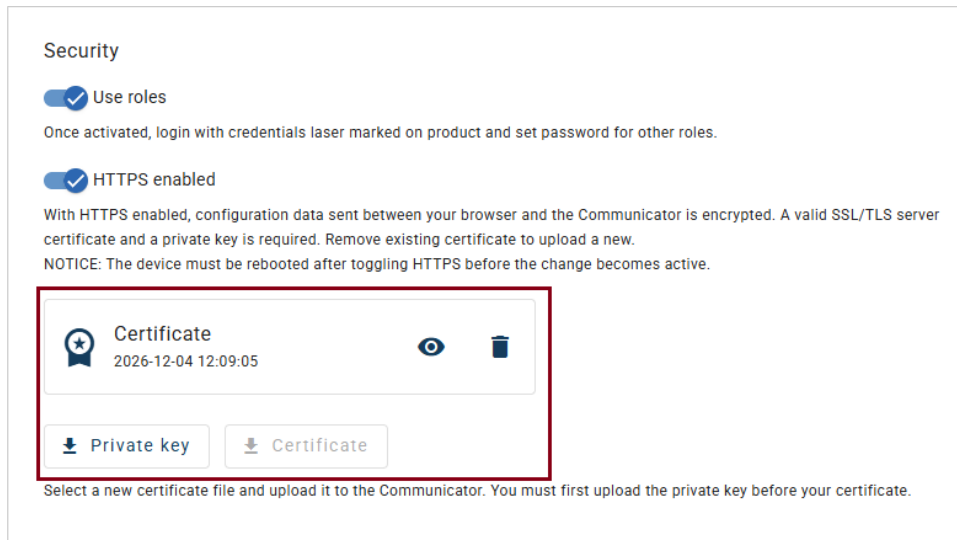


Figure 43. System page showing installed certificate

To update the existing HTTPS setup without removing it, you can upload a new certificate.

If the updated certificate uses a new key pair, first upload the matching private key.

Follow the steps in [Installing a Web Server Certificate \(page 59\)](#).

The uploaded file replaces the existing certificate — and private key, if included.

Delete a Certificate

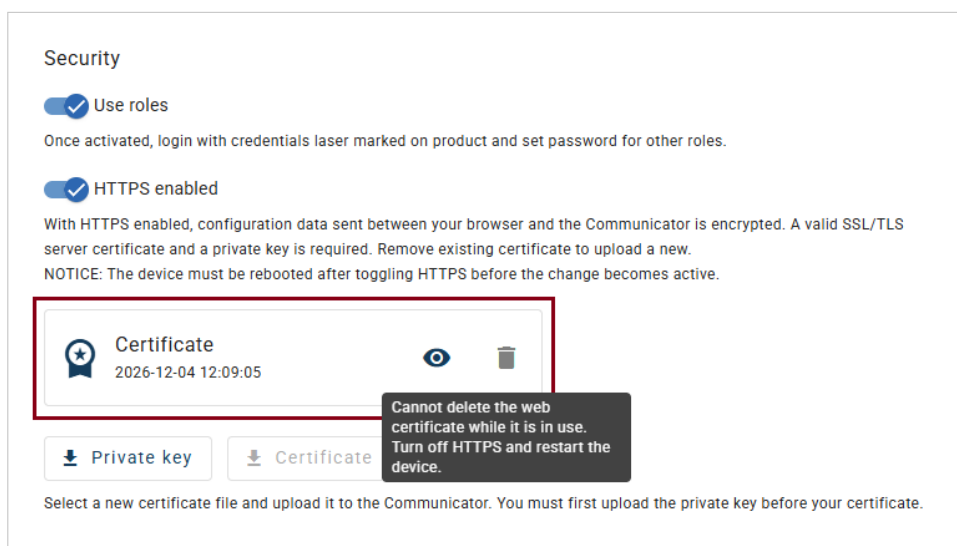


Figure 44. System page showing a locked certificate

When a certificate has been uploaded and HTTPS mode is enabled, the certificate becomes locked and cannot be deleted. In this state the trash-can delete button is disabled and grayed out.

To unlock the certificate, you must first disable HTTPS mode and then reboot the Communicator.

After the reboot, the certificate unlocks, and you can delete it.

See Also

[Secure Connection With HTTPS Mode \(Page 64\)](#)

[None Secure HTTP Mode \(Page 66\)](#)

10.4.6. Secure Connection With HTTPS Mode

About the Secure Connection (HTTPS) Mode

Secure connection (HTTPS) encrypts data sent between your browser and the server to keep the connection secure.



IMPORTANT

TCP Port 443 is used for HTTPS over Transport Layer Security (TLS) in HTTPS mode.

When using HTTPS mode, ensure TCP Port 443 is available,



IMPORTANT

For the HTTPS mode to work and enable secure access to the Communicator built-in web interface, a valid SSL/TLS server certificate is required.

Install the SSL/TLS certificate before enabling the HTTPS mode. See [Installing a Web Server Certificate \(page 59\)](#).



IMPORTANT

When HTTPS mode is enabled but no valid SSL/TLS server certificate is available, users can still access a limited HTTP version of the built-in web interface to update or install a SSL/TLS certificate. See [Installing a Web Server Certificate \(page 59\)](#).



IMPORTANT

A factory reset of the Communicator restores it to the default HTTP mode.

Before You Begin

Ensure Web Server Certificate is Installed

Ensure there is a valid web server certificate installed, see [Installing a Web Server Certificate \(page 59\)](#).

Ensure Accurate Time Settings

Incorrect time can cause SSL/TLS certificates to fail. The Communicator might interpret the certificate as expired or not yet valid, which is a security risk.

Ensure **Local time and date** are set and **Time synchronization** is enabled, see [Local Time and Date \(page 58\)](#) and [Network Time Protocol \(NTP\) Synchronization \(page 58\)](#).

Procedure

To enable HTTPS mode:

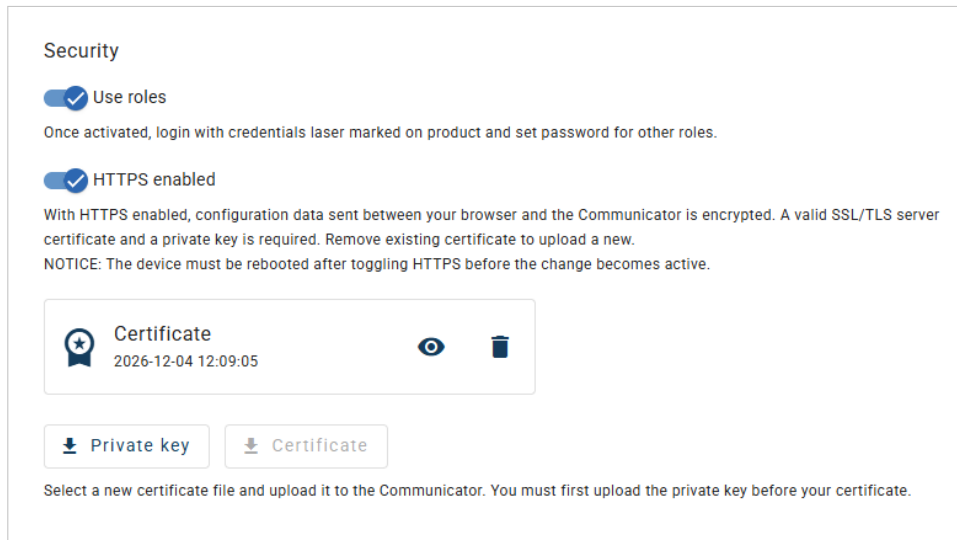


Figure 45. System page

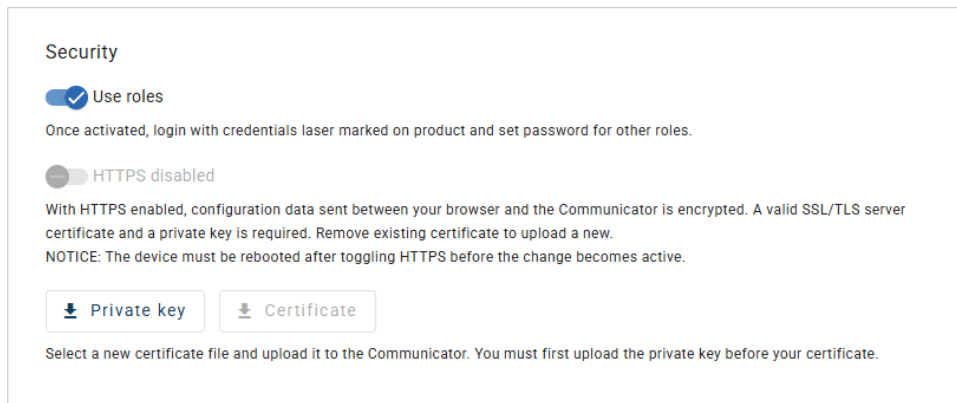
1. Open the **System** page.
2. In the **Security** section, click the **HTTPS disabled** slide toggle.
3. Click **Apply** in the web interface header.
4. For the setting to take effect, restart the Communicator by disconnecting and reconnecting its power supply.

See Also

[Update Or Delete A Certificate \(Page 62\)](#)

[None Secure HTTP Mode \(Page 66\)](#)

10.4.7. None Secure HTTP Mode



Security

☒ Use roles

Once activated, login with credentials laser marked on product and set password for other roles.

☐ HTTPS disabled

With HTTPS enabled, configuration data sent between your browser and the Communicator is encrypted. A valid SSL/TLS server certificate and a private key is required. Remove existing certificate to upload a new.

NOTICE: The device must be rebooted after toggling HTTPS before the change becomes active.

[Private key](#) [Certificate](#)

Select a new certificate file and upload it to the Communicator. You must first upload the private key before your certificate.

Figure 46. System page, Security settings, and Secure Connection (HTTPS) disabled

About the Hypertext Transfer Protocol (HTTP) Mode



IMPORTANT

By default, **Secure Connection (HTTPS)** is disabled and Communicator uses the HTTP mode.

To protect unauthorized access to the Communicator built-in web interface, ensure the security switch is locked.

To lock the security switch, see [Security Switch \(page 24\)](#).



IMPORTANT

TCP Port 80 is used for HTTP mode and for the limited version of the built-in web interface used when no certificate is available in HTTPS mode. Ensure that TCP Port 80 is open on the Communicator and network.

When using HTTP mode, ensure that TCP Port 443 is closed to prevent HTTPS access.

HTTP Mode Overview

- Data sent between the Communicator built-in web interface and the networks is transmitted in unencrypted plain text.
- Anyone on the same network could potentially intercept or manipulate the data.
- Recommended only in internal environments, such as during initial setup, or in isolated or trusted networks.

See Also

[Update Or Delete A Certificate \(Page 62\)](#)

[Secure Connection With HTTPS Mode \(Page 64\)](#)

10.4.8. Device IP Address Discovery via HMS Software Applications

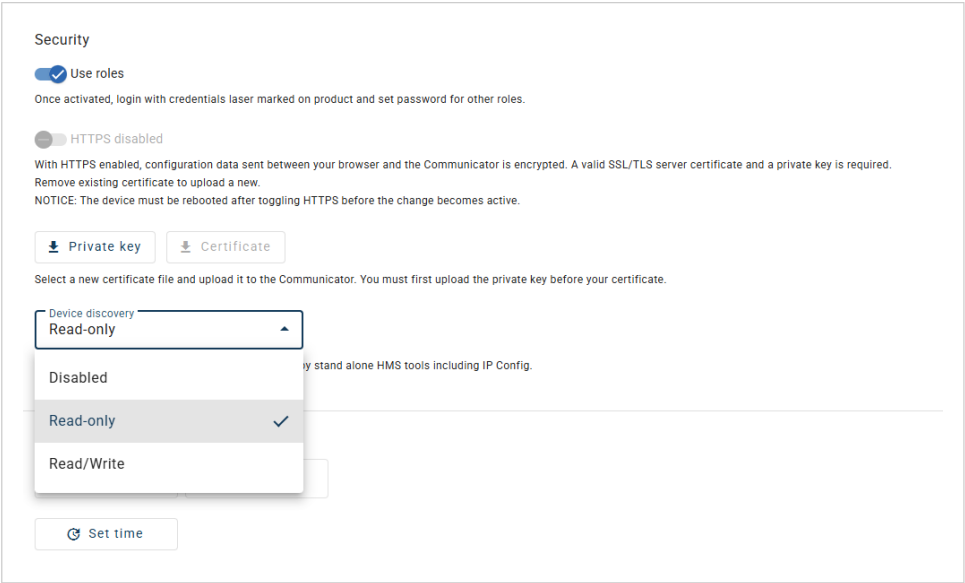


Figure 47. System page, Security settings, and Device discovery menu options

You can control whether the Communicator IP address can be discovered by stand-alone HMS software applications, including HMS IPconfig.

By default, **Read-only** mode is enabled.

The following **Device discovery** modes are available:

Mode	Description
Disabled	The Communicator does not expose its IP address to HMS software applications.
Read-only	The Communicator IP address is visible to HMS software applications and can be read, but not changed.
Read/Write	The Communicator IP address is visible to HMS software applications and can be read and changed.

10.5. I/O Configuration

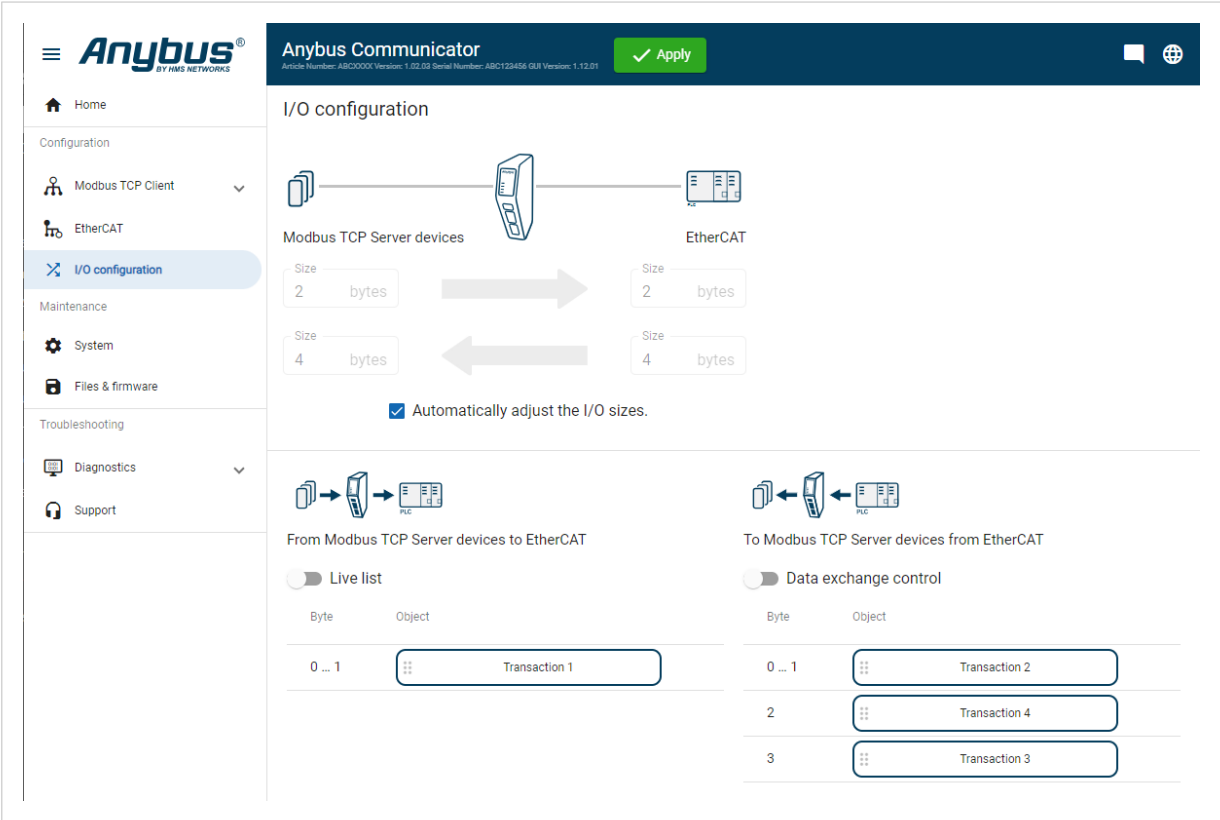


Figure 48. I/O configuration page

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

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

I/O Size Settings

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

10.5.1. 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.

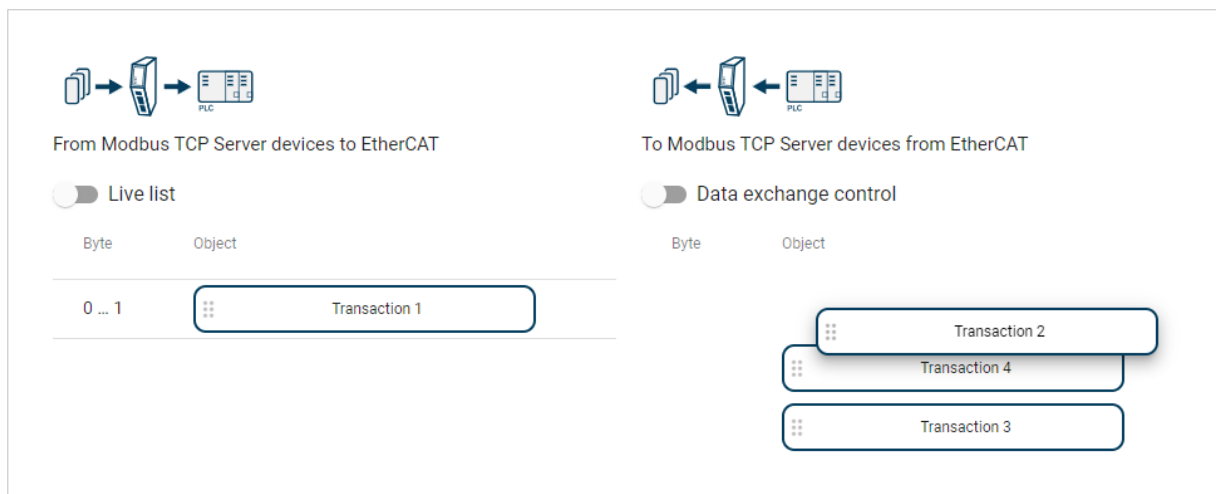


Figure 49. I/O configuration, change the order of objects

10.5.2. 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.

10.5.3. Map Area

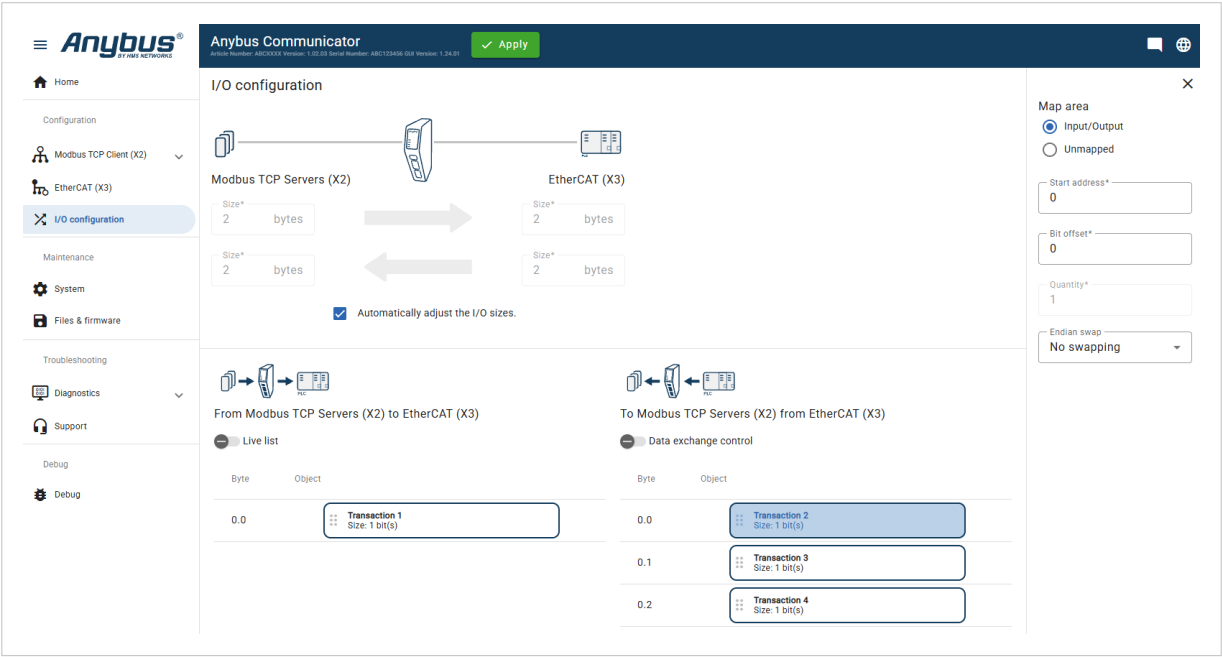


Figure 50. I/O configuration page, Map area options

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.

10.5.4. 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 1. 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 2. 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 3. 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.

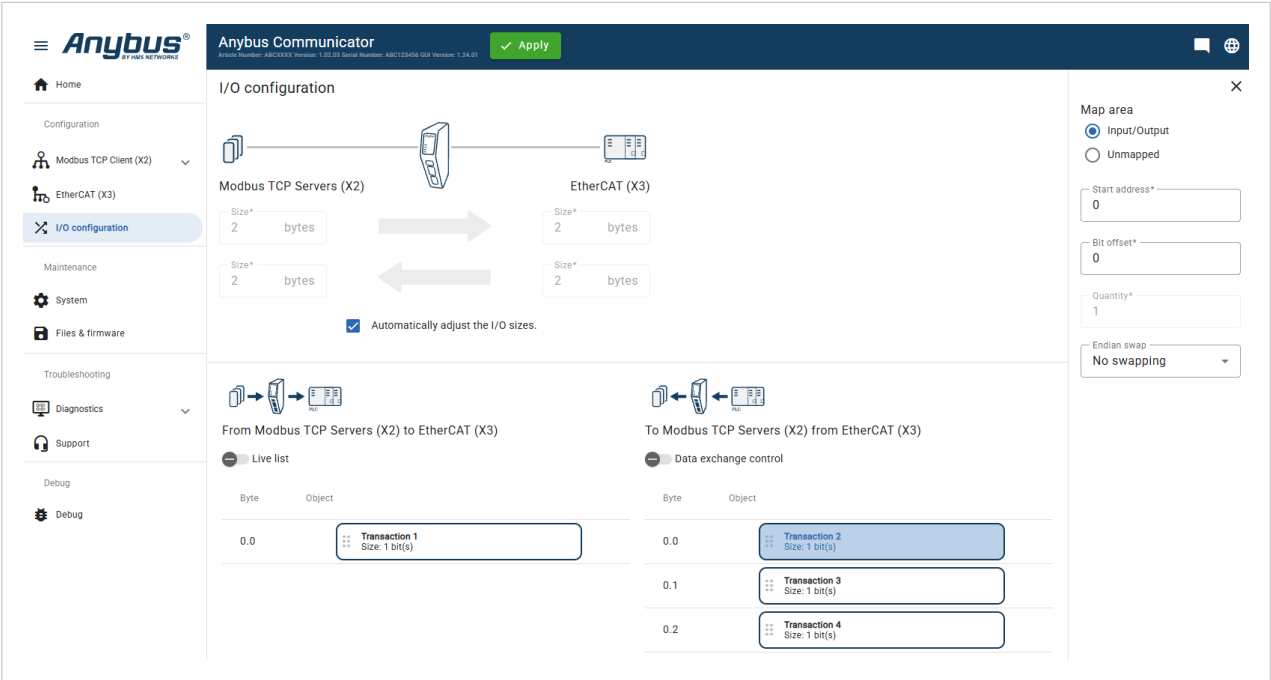


Figure 51. I/O configuration page, Bit offset

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

10.5.5. Convert Between Big-Endian and Little-Endian

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

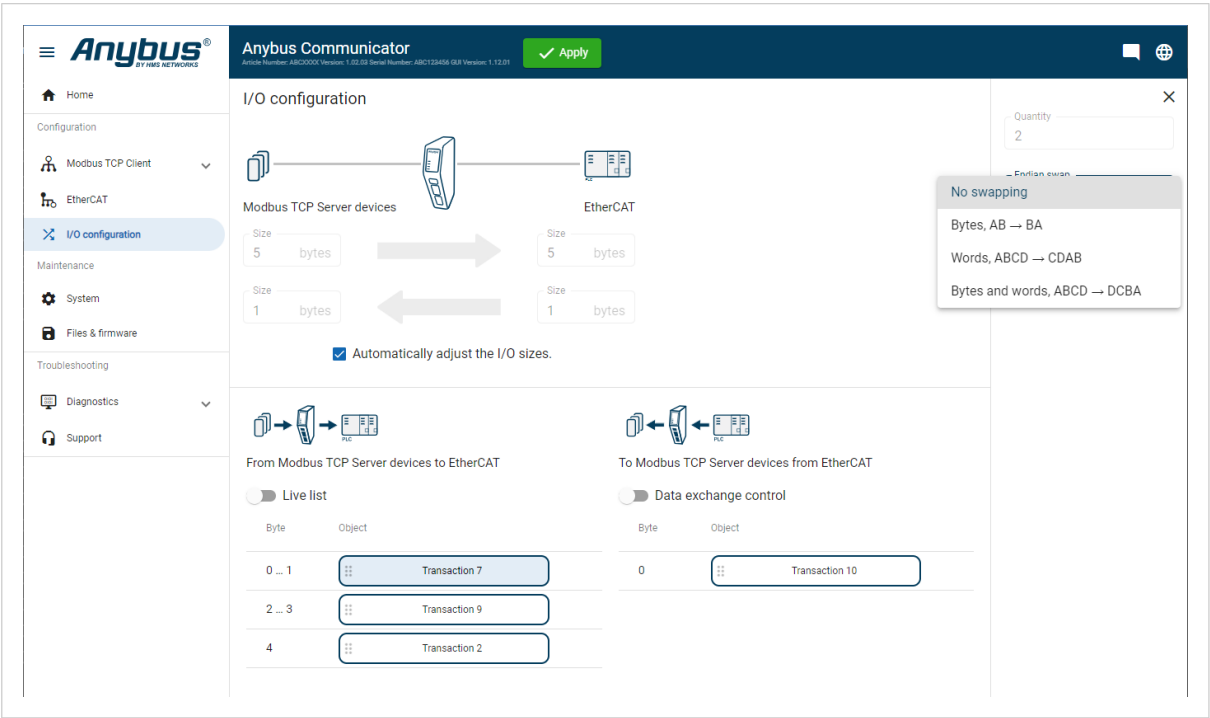


Figure 52. I/O configuration page, Endian swap

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.

10.5.6. Live List

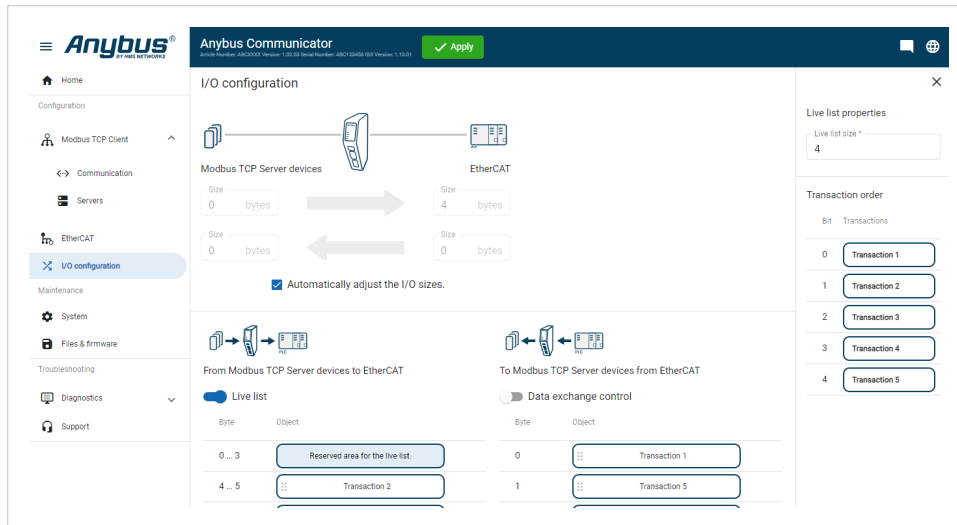


Figure 53. I/O configuration page, Live list enabled

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

About the Live List

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

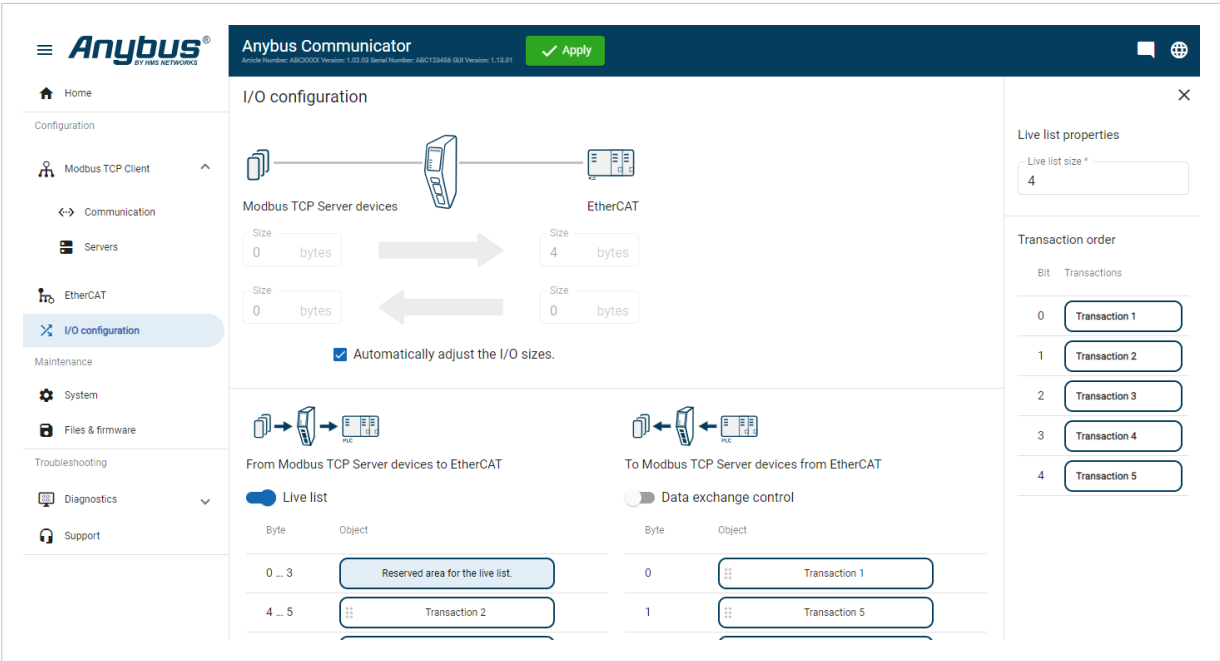


Figure 54. Live list properties and Transaction order

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.

10.5.7. Data Exchange Control

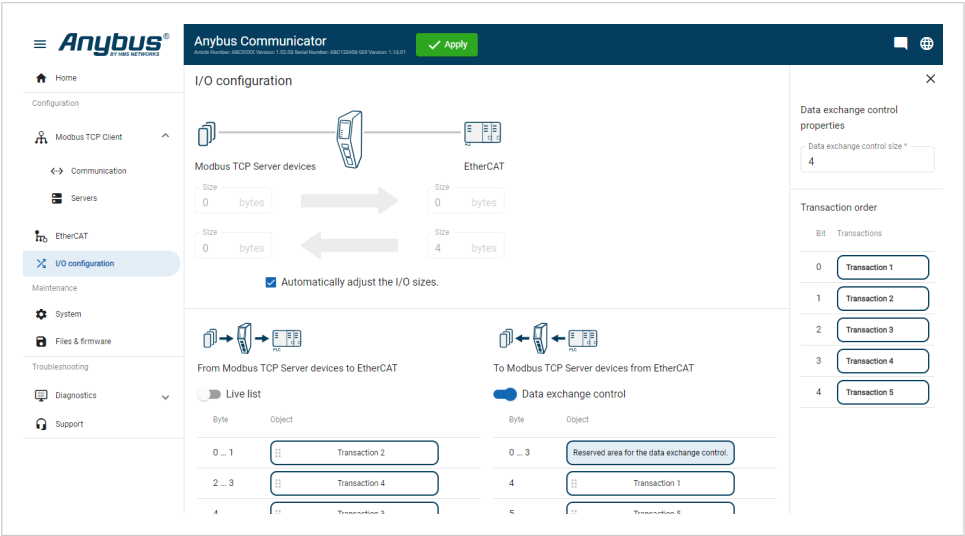


Figure 55. I/O configuration, **Data exchange control** enabled

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

When **Data exchange control** is enabled, the first four bytes of process data on the EtherCAT 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

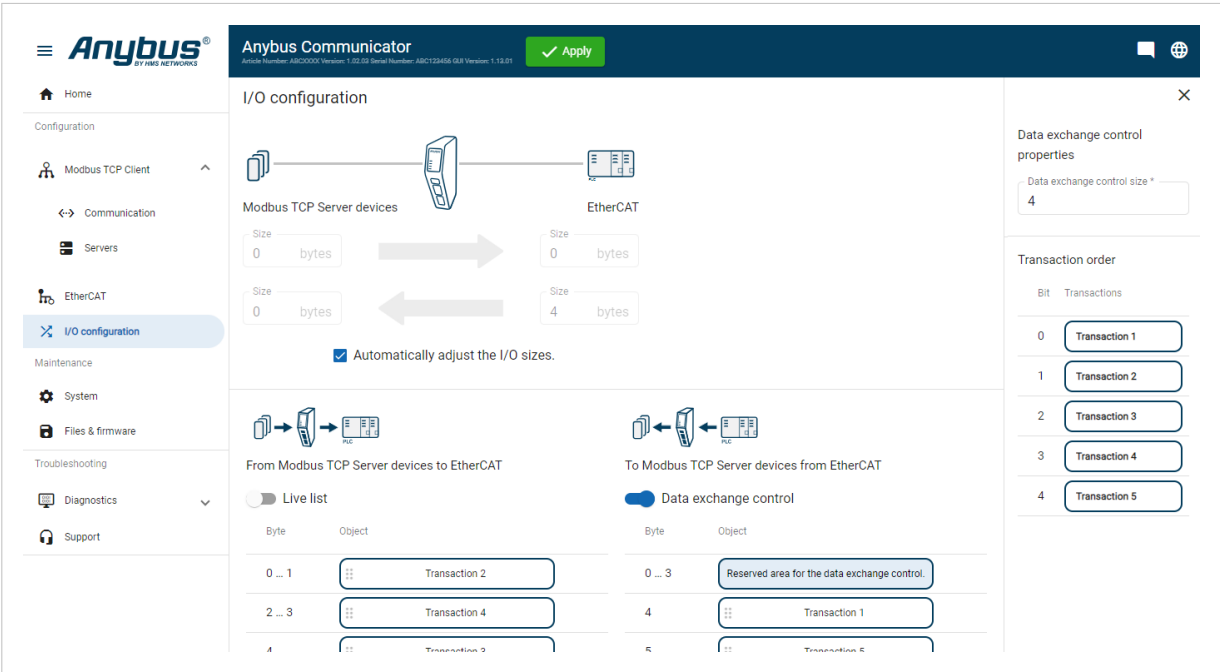


Figure 56. Data exchange control properties and Transaction order

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.

10.6. Configuration Notes

You can add notes to describe the Communicator configuration.

10.6.1. Add Configuration Note

Procedure

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



Figure 57. Configuration note, comment icon

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

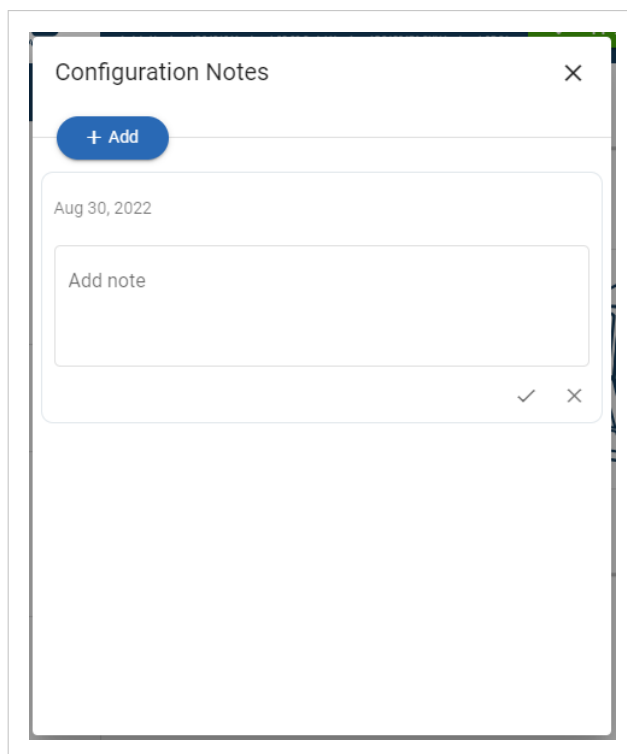


Figure 58. Add new configuration note

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

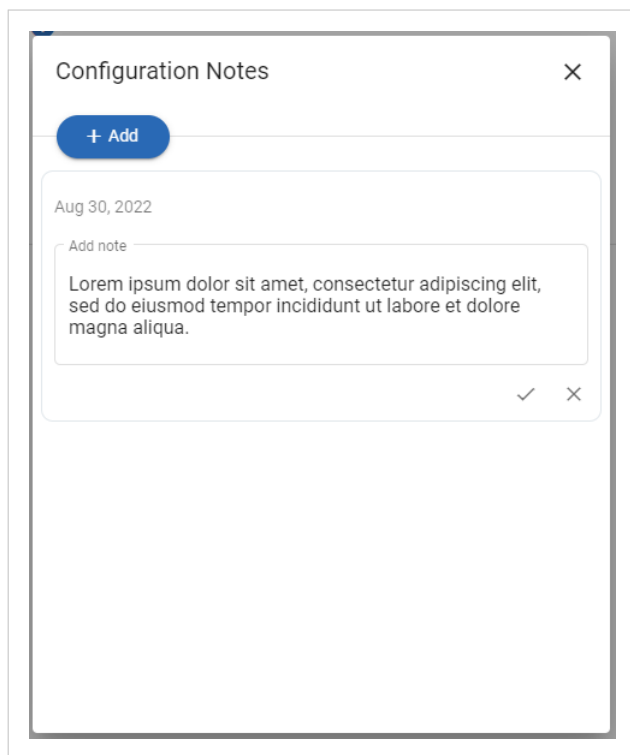


Figure 59. Write a configuration note

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.

10.6.2. View and Edit Configuration Notes

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

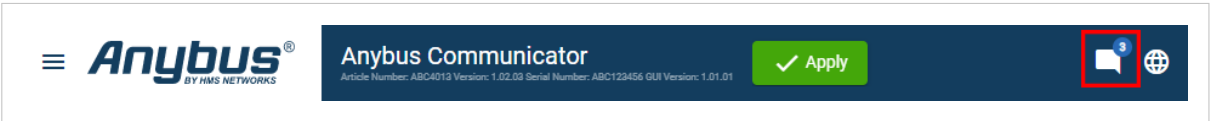


Figure 60. Example: The comment icon indicates that there are three added notes

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

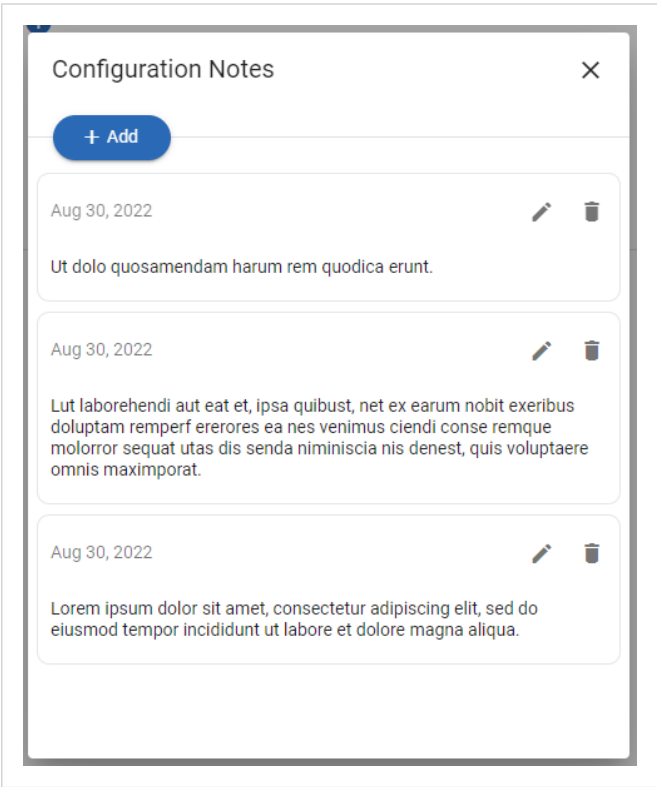


Figure 61. Example: The Configuration Notes window with added notes

10.7. Apply Configuration

Before You Begin

**NOTE**

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

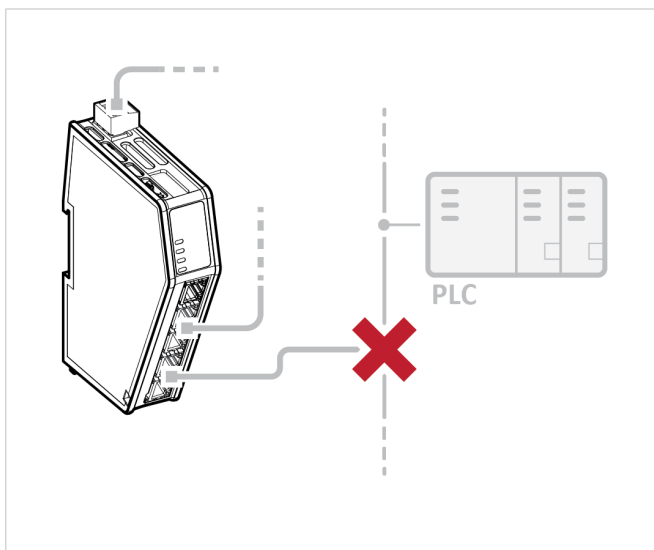


Figure 62. Disconnect the Communicator from the EtherCAT network

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

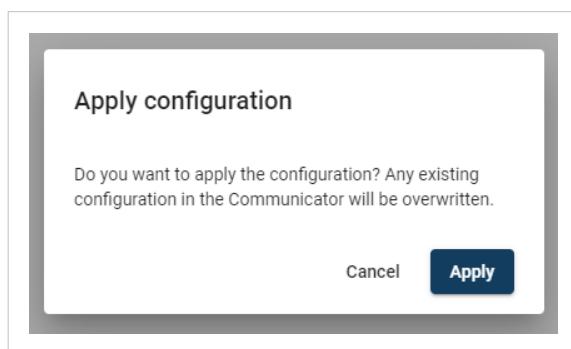
Procedure

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.



10.8. 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

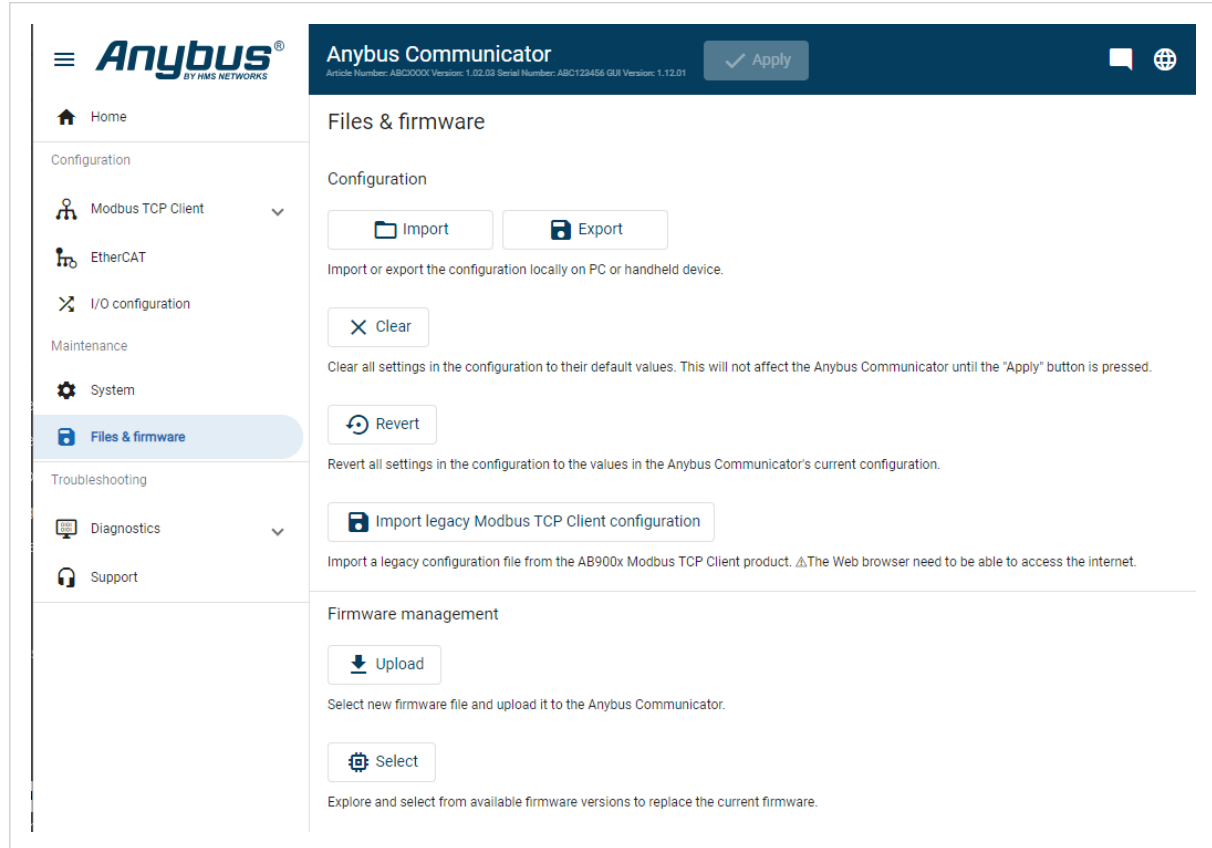


Figure 63. **Files & firmware** page

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.

10.9. 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

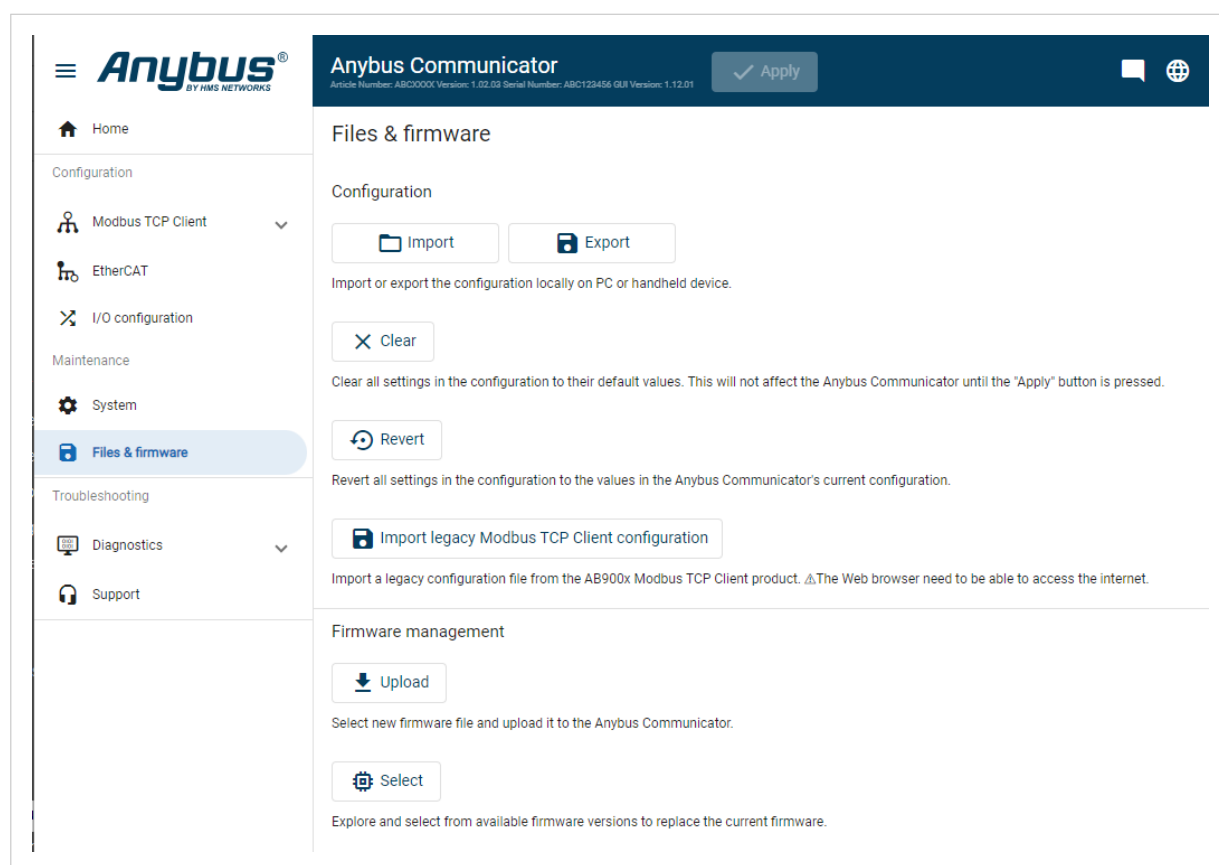


Figure 64. Files & firmware page

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**.

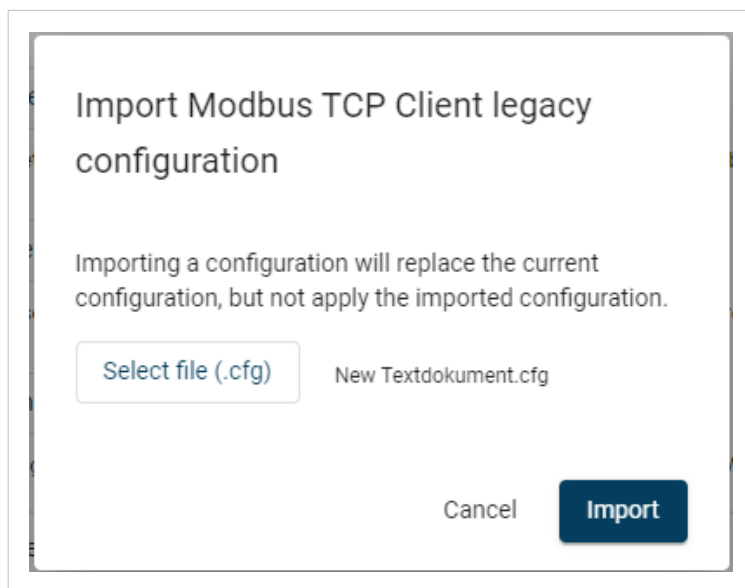


Figure 65. Example, selected .cfg file

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.

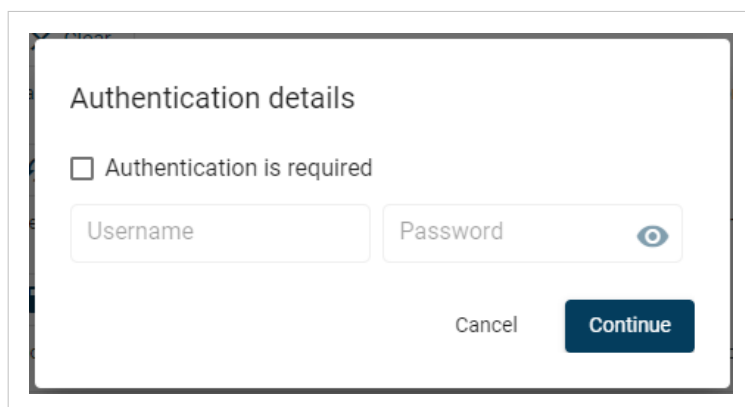
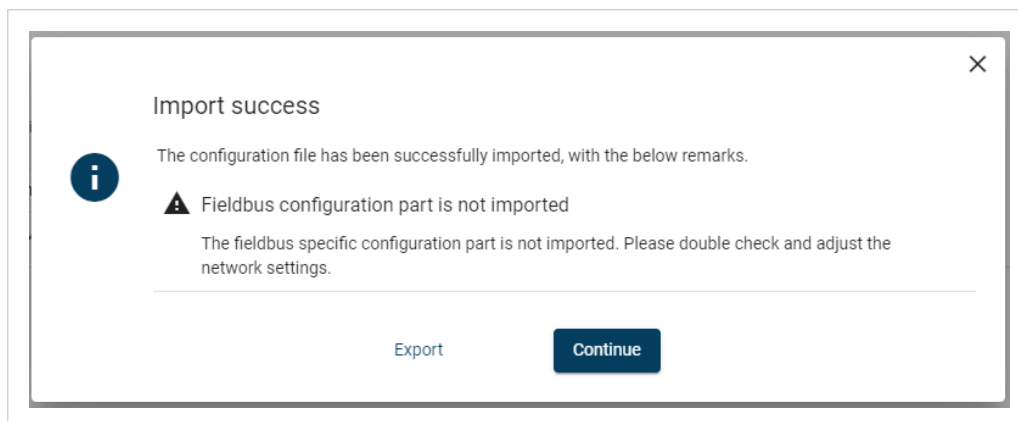


Figure 66. Authentication details

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 67. Example, list with messages about the import

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

11. PLC Configuration

11.1. 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.

11.2. Export Product ESI File

Option for EtherCAT.

Option if the PLC program requires a product file, ESI (EtherCAT SubDevice Information) file to configure the EtherCAT PLC to use the Communicator

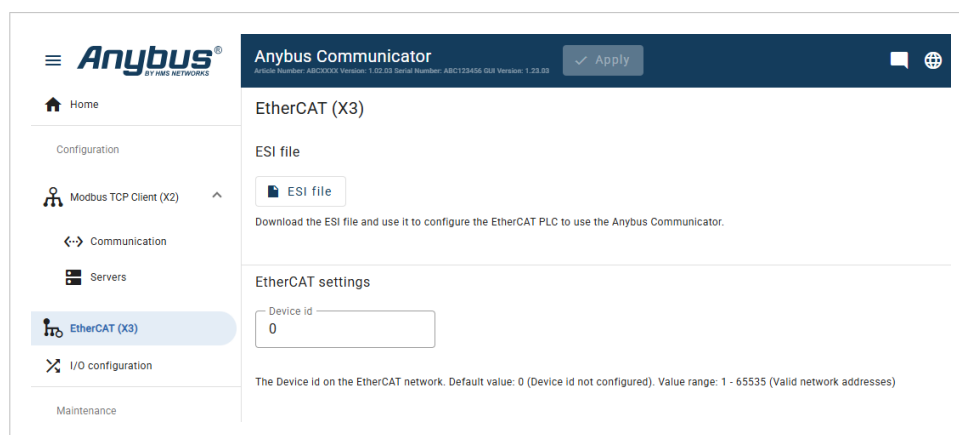


Figure 68. Export Product ESI File

You find the *EtherCAT* ESI file on the Communicator built-in web interface **EtherCAT** page.

To export the ESI file:

1. To save the configuration, click **Apply**.
The **ESI file** button is activated.
2. Click **ESI file**.
The ESI file is downloaded to your PC.

11.3. CANopen over EtherCAT (CoE) Objects



TIP

"XXXX" in the table Name column is the process data offset value.

Table 3. Product specific CANopen objects

Index	Obj.type	Subindex	Type	Access	PDO Mappable	Name	Value
0x2000	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0001	Send process data, byte 1
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 2 - 127
		128	UNSIGNED8	R	TxPDO	Input byte 0128	Send process data, byte 128
0x2001	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0129	Send process data, byte 129
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 130 - 255
		128	UNSIGNED8	R	TxPDO	Input byte 0256	Send process data, byte 256
0x2002	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0257	Send process data, byte 257
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 258 - 383
		128	UNSIGNED8	R	TxPDO	Input byte 0384	Send process data, byte 384
0x2003	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0385	Send process data, byte 385
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 386 - 511
		128	UNSIGNED8	R	TxPDO	Input byte 0512	Send process data, byte 512
0x2004	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0513	Send process data, byte 513
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 514 - 639
		128	UNSIGNED8	R	TxPDO	Input byte 0640	Send process data, byte 640
0x2005	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0641	Send process data, byte 641
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 642 - 767
		128	UNSIGNED8	R	TxPDO	Input byte 0768	Send process data, byte 768
0x2006	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0769	Send process data, byte 769
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 770 - 895
		128	UNSIGNED8	R	TxPDO	Input byte 0896	Send process data, byte 896
0x2007	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 0897	Send process data, byte 897

Index	Obj.type	Subindex	Type	Access	PDO Mappable	Name	Value
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 898 - 1023
		128	UNSIGNED8	R	TxPDO	Input byte 1024	Send process data, byte 1024
		0x2008	RECORD	N/A	UNSIGNED8	N/A	Inputs
		N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 1025	Send process data, byte 1025
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 1026 - 1151
		128	UNSIGNED8	R	TxPDO	Input byte 1152	Send process data, byte 1152
0x2009	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 1153	Send process data, byte 1153
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 1154 - 1279
		128	UNSIGNED8	R	TxPDO	Input byte 1280	Send process data, byte 1280
0x200A	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	TxPDO	Input byte 1281	Send process data, byte 1281
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 1282 - 1407
		128	UNSIGNED8	R	TxPDO	Input byte 1408	Send process data, byte 1408
0x200B	RECORD	N/A	UNSIGNED8	N/A	N/A	Inputs	N/A
		0	UNSIGNED8	R	No	Number of entries	78
		1	UNSIGNED8	R	TxPDO	Input byte 1409	Send process data, byte 1409
		...	UNSIGNED8	R	TxPDO	Input byte XXXX	Send process data, bytes 1410 - 1487
		78	UNSIGNED8	R	TxPDO	Input byte 1486	Send process data, byte 1486
0x2100	RECORD		UNSIGNED8			Outputs	
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0001	Receive process data, byte 1
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 2 - 127
		128	UNSIGNED8	R	RxPDO	Output byte 0128	Receive process data, byte 128
0x2101	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0129	Receive process data, byte 129
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 130 - 255
		128	UNSIGNED8	R	RxPDO	Output byte 0256	Receive process data, byte 256
0x2102	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0257	Receive process data, byte 257
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 258 - 383
		128	UNSIGNED8	R	RxPDO	Output byte 0384	Receive process data, byte 384
0x2103	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0385	Receive process data, byte 385
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 386 - 511
		128	UNSIGNED8	R	RxPDO	Output byte 0512	Receive process data, byte 512
0x2104	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A

Index	Obj.type	Subindex	Type	Access	PDO Mappable	Name	Value
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0513	Receive process data, byte 513
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 514 - 639
		128	UNSIGNED8	R	RxPDO	Output byte 0640	Receive process data, byte 640
0x2105	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0641	Receive process data, byte 641
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 642 - 767
		128	UNSIGNED8	R	RxPDO	Output byte 0768	Receive process data, byte 768
0x2106	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0769	Receive process data, byte 769
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 770 - 895
		128	UNSIGNED8	R	RxPDO	Output byte 0896	Receive process data, byte 896
0x2107	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 0897	Receive process data, byte 897
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 898 - 1023
		128	UNSIGNED8	R	RxPDO	Output byte 1024	Receive process data, byte 1024
0x2108	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 1025	Receive process data, byte 1025
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 1026 - 1151
		128	UNSIGNED8	R	RxPDO	Output byte 1152	Receive process data, byte 1152
0x2109	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 1153	Receive process data, byte 1153
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 1154 - 1279
		128	UNSIGNED8	R	RxPDO	Output byte 1280	Receive process data, byte 1280
0x210A	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	128
		1	UNSIGNED8	R	RxPDO	Output byte 1281	Receive process data, byte 1281
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 1282 - 1407
		128	UNSIGNED8	R	RxPDO	Output byte 1408	Receive process data, byte 1408
0x210B	RECORD	N/A	UNSIGNED8	N/A	N/A	Outputs	N/A
		0	UNSIGNED8	R	No	Number of entries	78
		1	UNSIGNED8	R	RxPDO	Output byte 1409	Receive process data, byte 1409
		...	UNSIGNED8	R	RxPDO	Output byte XXXX	Receive process data, bytes 1410 - 1487
		78	UNSIGNED8	R	RxPDO	Output byte 1486	Receive process data, byte 1486

12. 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.

12.1. Communicator Status Monitor

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

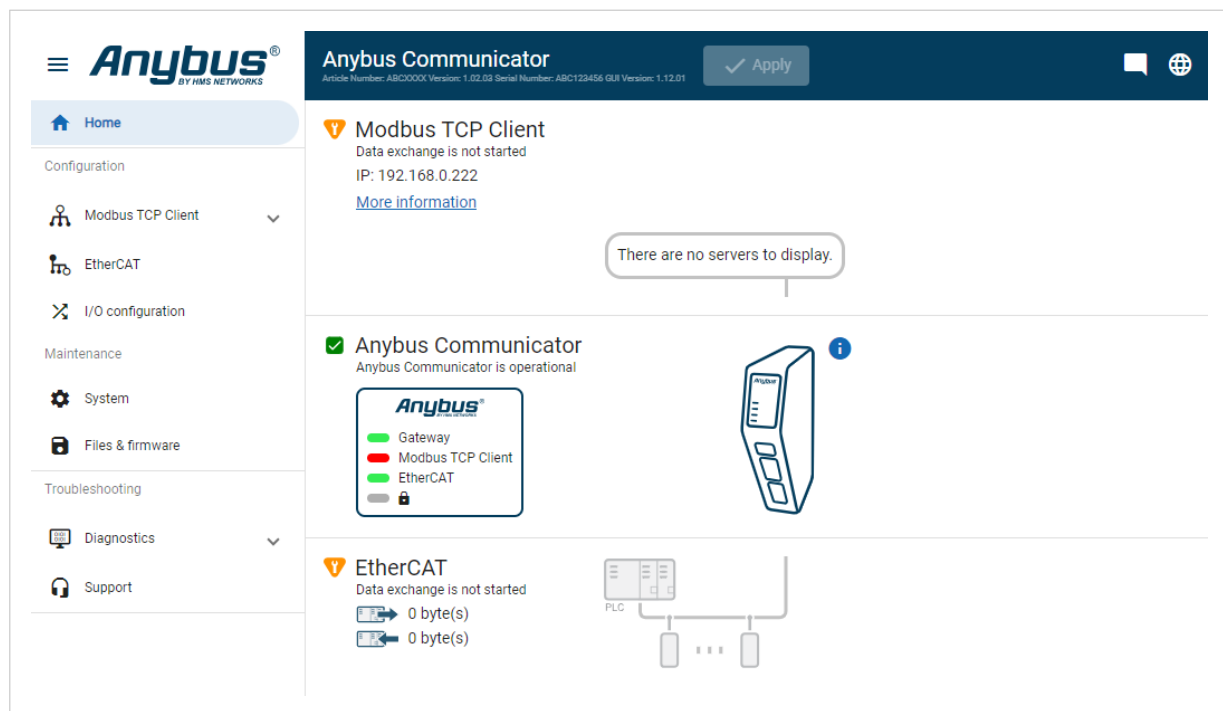


Figure 69. Home page

Gateway Status

Overview the Communicator LED indications remotely.

The Communicator EtherCAT LED status indication is only available on product.

Server Status

Overview the status for each server added to the subnetwork.

Network Status and Settings

Overview communication status and the current networks settings.

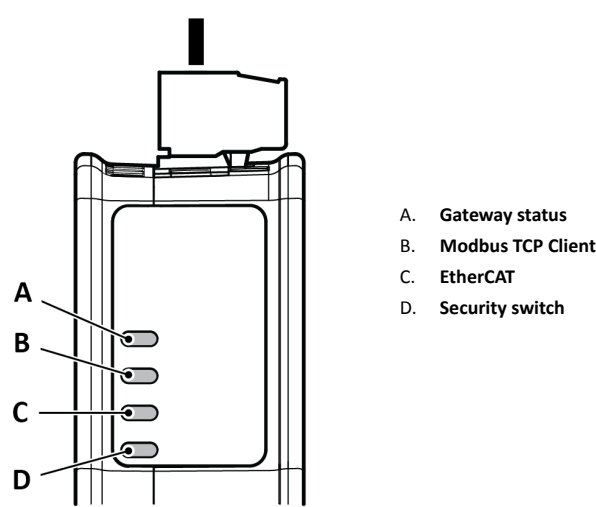
Status Symbols

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 \(Page 19\)](#)
- [Connect To EtherCAT Network \(Page 21\)](#)
- [Connect To Power \(Page 22\)](#)
- [Communicator LED Indicators \(Page 93\)](#)
- [LED Status \(Page 109\)](#)
- [Firmware Upgrade Error Management \(Page 113\)](#)

12.2. Communicator LED Indicators



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.

EtherCAT

Operation status	Description
Off	No power. EtherCAT device in 'INIT'-state.
Green, one flash	EtherCAT device in 'SAFEOPERATIONAL'-state.
Green, flashing	EtherCAT device in 'PREOPERATIONAL'-state.
Green, solid	EtherCAT device in 'OPERATIONAL'-stat.
Red, one flash	Unsolicited state change. SubDevice application has changed the EtherCAT state autonomously.
Red, two flashes	Sync Manager watchdog timeout.
Red, flashing	Invalid configuration.
Red, solid	Fatal event.
Green/Red, flashing	EtherCAT RUN (green) and ERROR (red) LED combined.*

*The EtherCAT RUN (green) and ERROR (red) LED behaviors are combined in LED (C)/(D). This can cause LED (C)/(D) to alternate between red and green. The LED behavior still represents the states described in the table.

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 \(Page 19\)](#)

[Connect To EtherCAT Network \(Page 21\)](#)

[Connect To Power \(Page 22\)](#)

[Communicator Status Monitor \(Page 91\)](#)

[LED Status \(Page 109\)](#)

[Firmware Upgrade Error Management \(Page 113\)](#)

12.3. Ethernet RJ45 LED Indicators

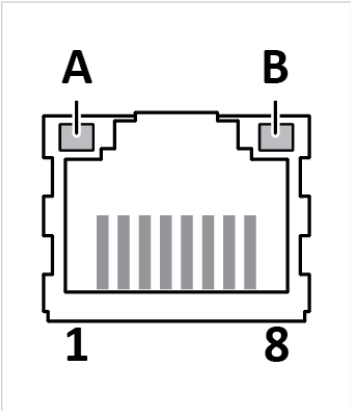


Figure 70. LED A. Activity LED B. Not used

LED A	Function
Off	No link (or no power)
Green	Link (100 Mbit/s) established EtherCAT: Link established
Green, flashing	Activity (100 Mbit/s) EtherCAT: Activity
Yellow	Link (10 Mbit/s) established EtherCAT: Yellow LED is not used
Yellow, flashing	Activity (10 Mbit/s) EtherCAT: Yellow LED is not used

LED B	Function
Off	Not used

13. Maintenance

13.1. Action on Fatal Error

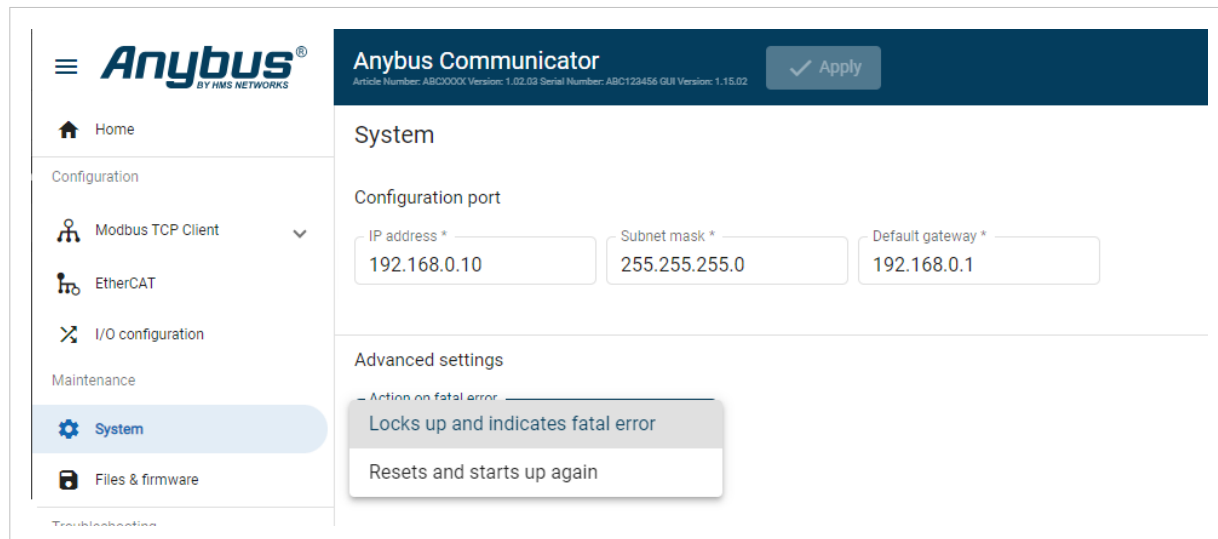


Figure 71. System page, Action on fatal error menu

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.

13.2. Configuration Port IP Settings

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

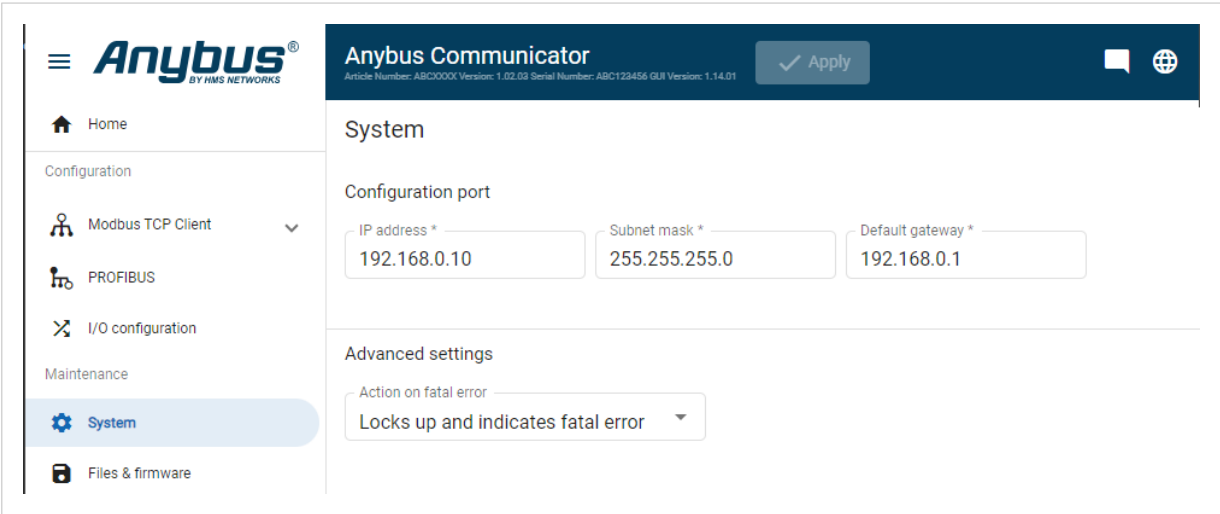


Figure 72. System page, Configuration port settings

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.

13.3. Dashboard

The **Dashboard** allows you to create a customized view of the live data that the Communicator exchanges between device(s) on the connected networks.

Using a dashboard helps reduce complexity by presenting key data and actions in one place.

Enable the Dashboard

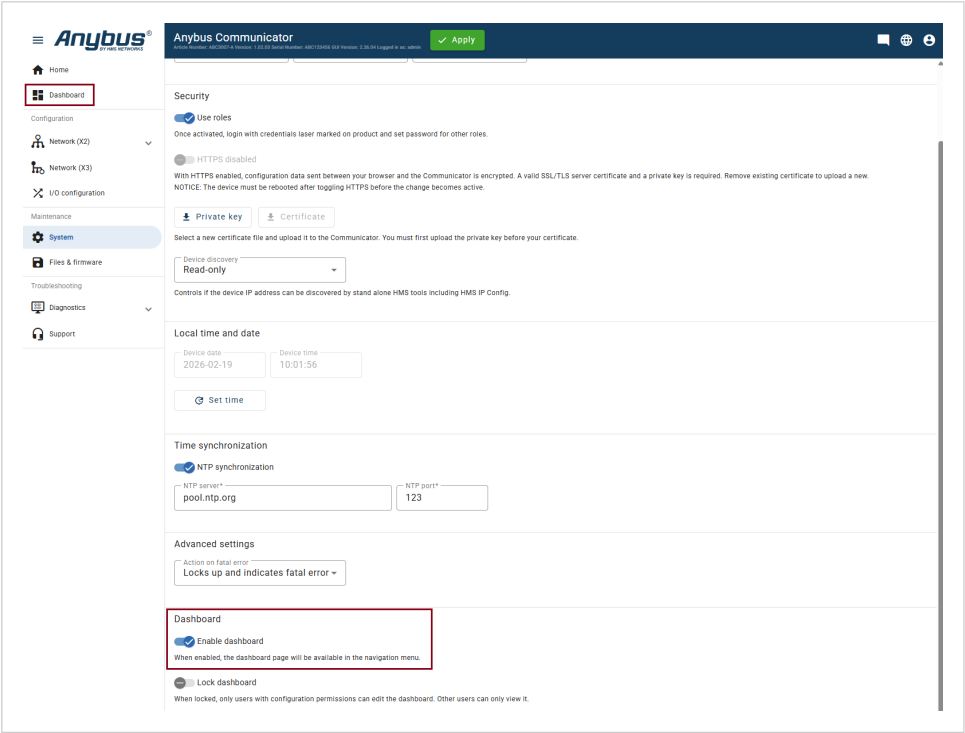


Figure 73. System page with Dashboard enabled and visible in the main menu

Procedure

1. On the **System** page, go to the **Dashboard** panel.
2. Click the **Enable dashboard** slide toggle.
3. When enabled, the **Dashboard** appears in the main menu.

To Setup the Dashboard

Before You Begin

You can add labels, data values, and images to create a simple visualization of the data exchange.

This helps you monitor values in real time and confirm that communication between networks is working as expected.

Dashboard Elements and Settings

Label

Use labels to add text descriptions on the dashboard, such as section names, group elements, or context for images or data.

Setting	Description
Label title	Enter the text you want to display in the label.

Setting	Description
Font	Select font type, size, and color.
Background	Choose a background color and opacity.
Border	Choose to show or hide the border. Adjust corner radius and border width if needed.

Image

Use images to create a simple graphical layout, for example to represent pumps, motors, or sensors.

Images can enhance clarity or support an HMI-style overview.

Data Value

Displays the current live value from a selected data point.

Setting		Description
Data	Byte address	Enter the starting address in the I/O data.
	Data type	Select UInt8 (1 byte), Int8 (1 byte), UInt16 (2 bytes), Int16 (2 bytes), UInt32 (4 bytes), Int32 (4 bytes), or Float32 (4 bytes)
	Direction	Choose whether the data direction is to or from the Communicator.
	Network	Select the network the data comes from, X2 or X3.
	Display format	Select Hex, Dec, or ASCII.
Value transformation	Formula	Apply a mathematical formula to transform the raw value. Use x to represent the raw value. Supports basic math operators (+, -, , /) and parentheses. Example: $x * 0.1 + 10$
Label font	Label, Font, Font size, and Font color	Add a label to describe the value. Select the font type, size, and color.
Value font	Font, Font size, and Font color	Select the font type, size and color for the displayed value.
Background	Background color and opacity	Choose background color and opacity.
Border	Corner radius and Border width	Choose to show or hide border. Adjust corner radius and border width if needed.

Procedure

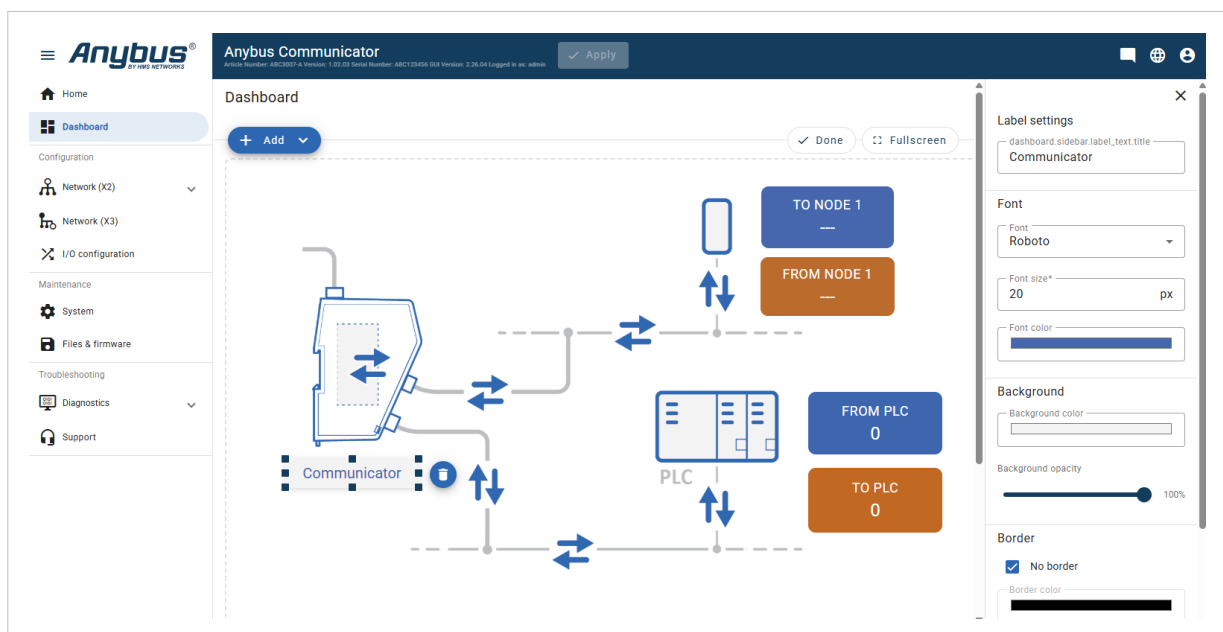


Figure 74. Dashboard example with added element

1. Navigate to the **Dashboard** page.
2. To enable edit mode, click **Edit**
3. To add an element, click **Add**, then select **Label**, **Image**, or **Data Value**.
The element is placed on the dashboard.
For **Labels** and **Data Values**, the settings panel is opened.
4. Configure the settings. See [Dashboard Elements and Settings \(page 98\)](#).
5. Drag the element to the preferred location if needed.
6. Resize the element if necessary.
7. To close edit mode, click **Done**.

Lock Dashboard

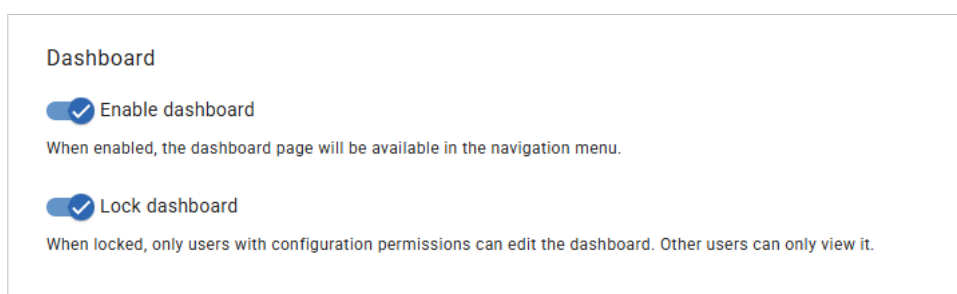


Figure 75. Dashboard enabled and locked

On the **System** page, you can lock the dashboard to prevent unauthorized changes.

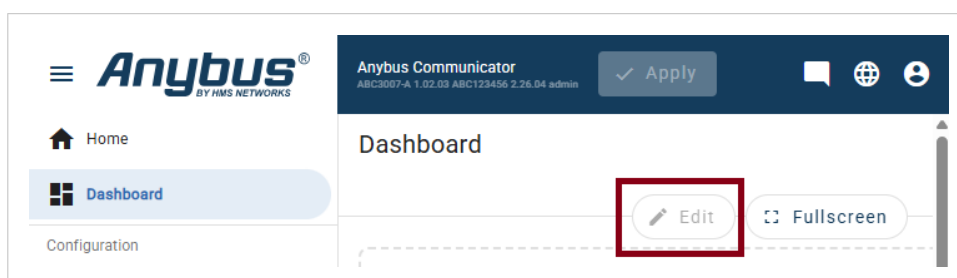


Figure 76. Dashboard locked

When locked:

- Only users with Administrator authority can edit the dashboard.
- All other users can view the dashboard but cannot modify it.

13.4. Configuration File Handling

13.4.1. Export Configuration

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

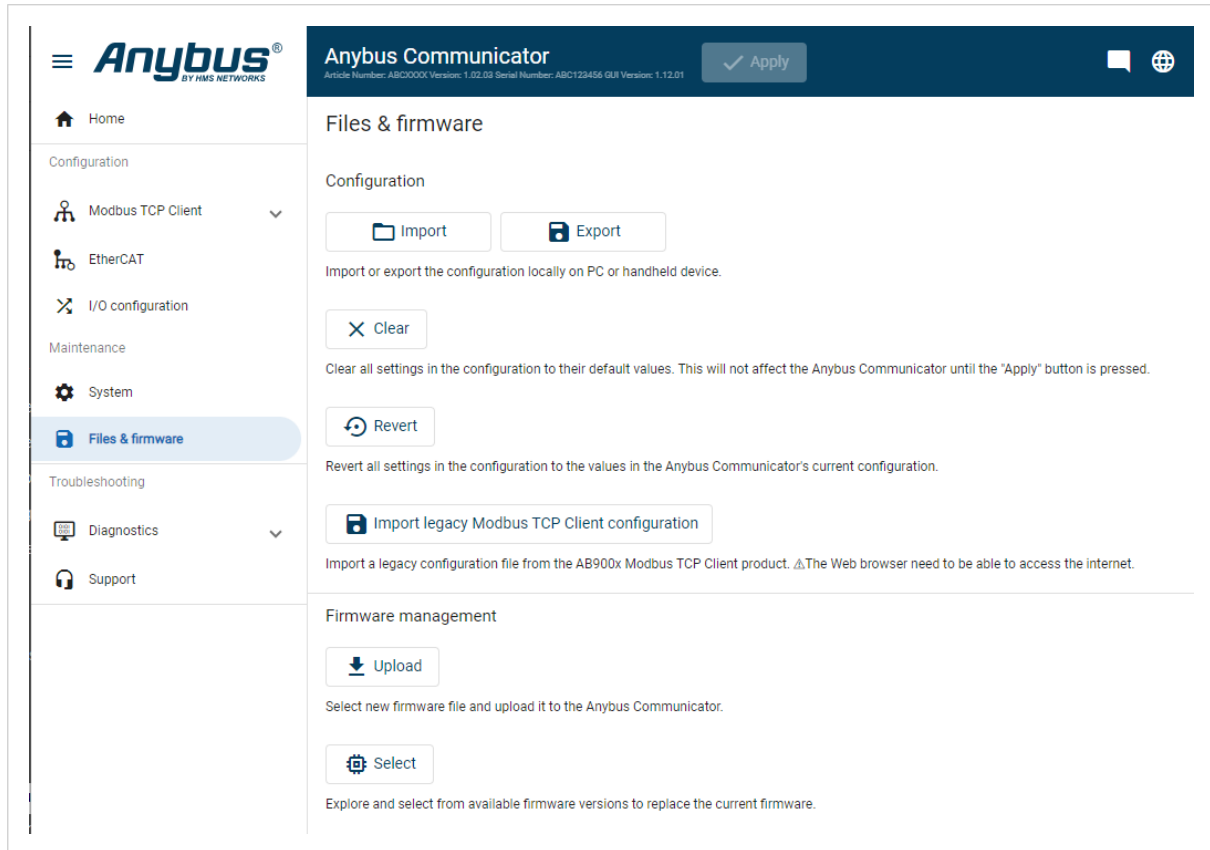


Figure 77. Files & firmware page

To export a configuration file:

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

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

13.4.2. 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

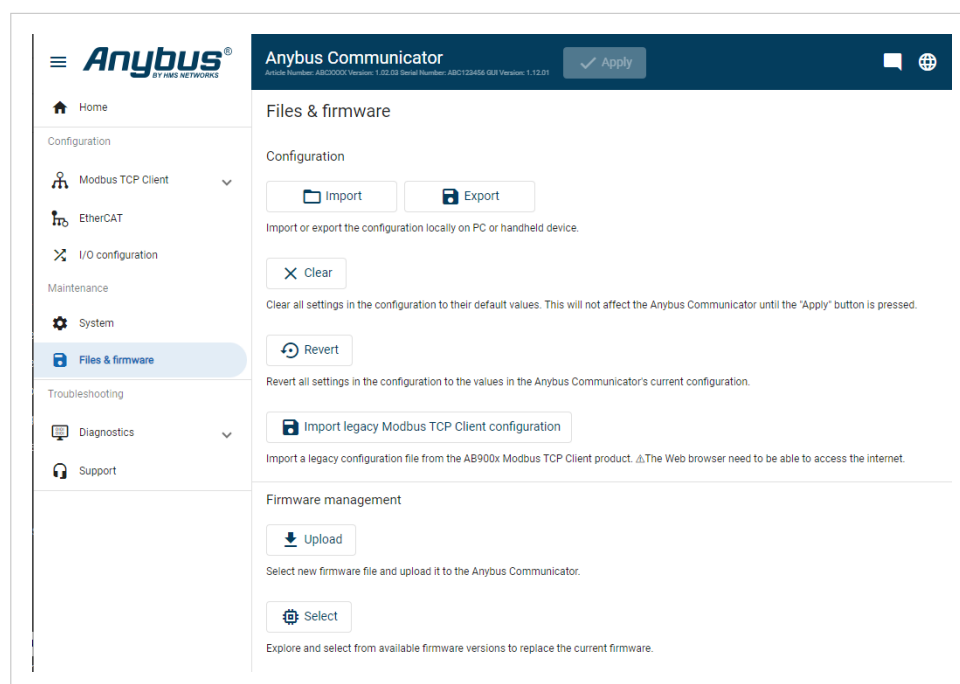


Figure 78. Files & firmware page

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.

13.5. Clear and Revert Configuration

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

Procedure

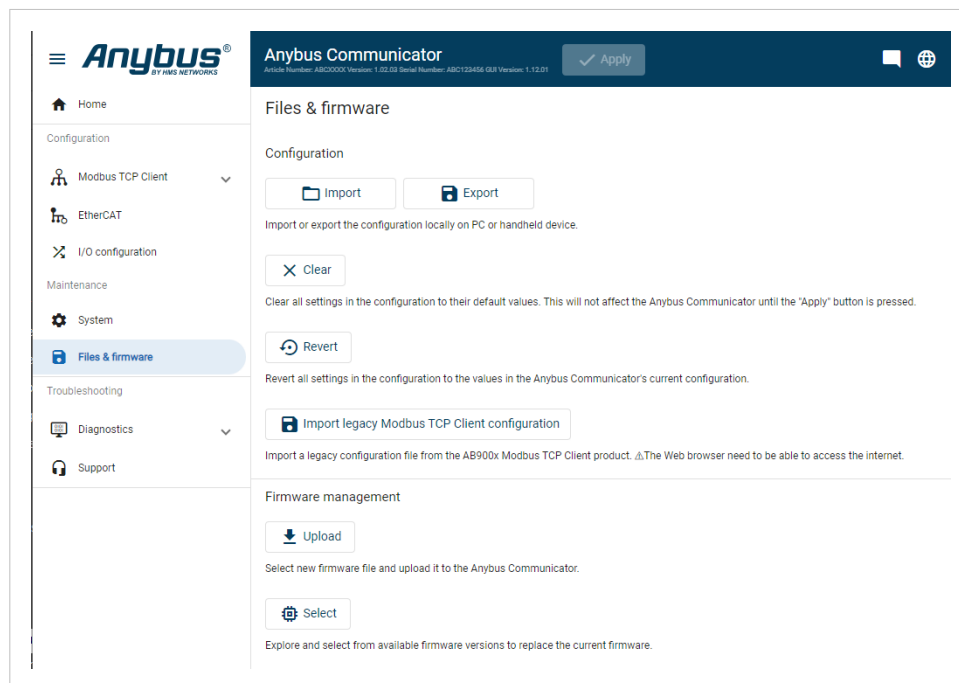


Figure 79. Files & firmware page

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.

13.6. Firmware Management

13.6.1. View the Firmware Version

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

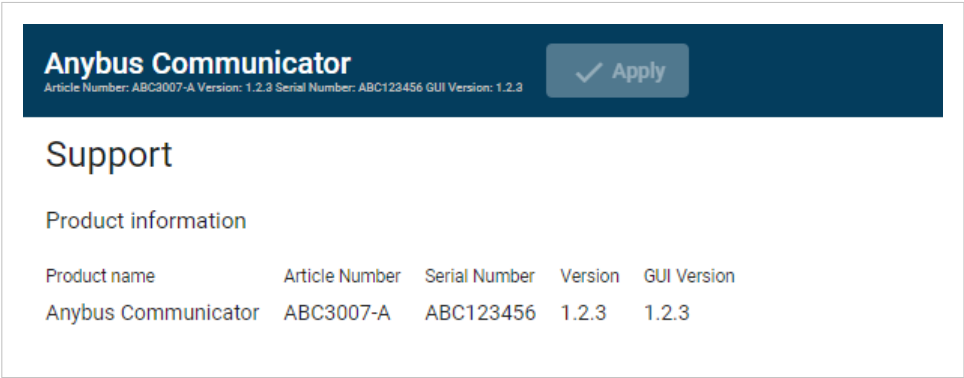


Figure 80. Support page, Product information example

13.6.2. 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.

13.6.3. 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.

13.6.4. 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

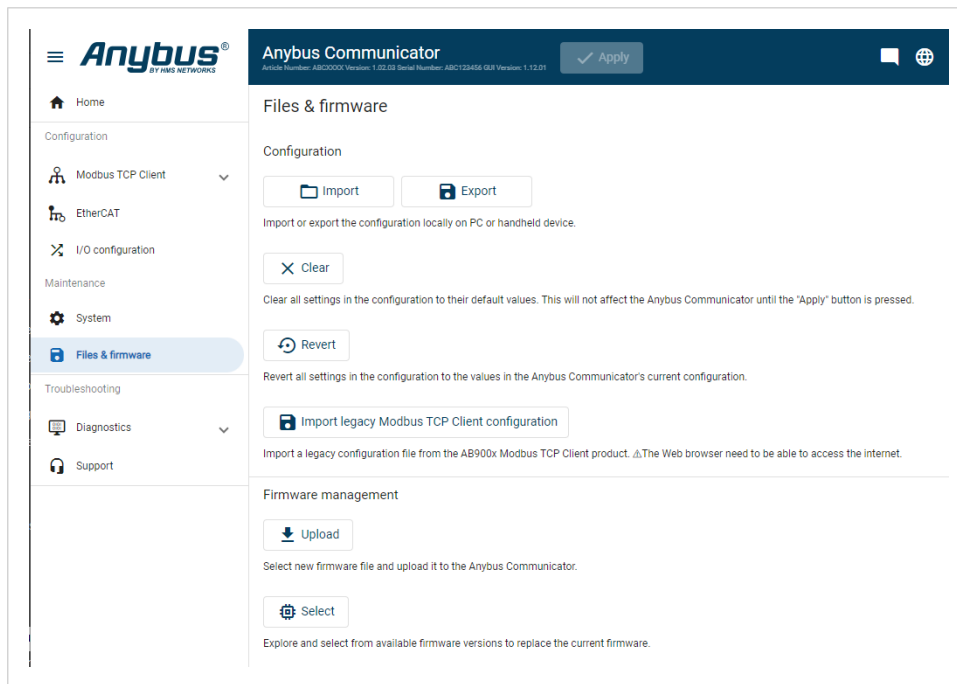


Figure 81. Files & firmware page

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.

13.7. 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 .

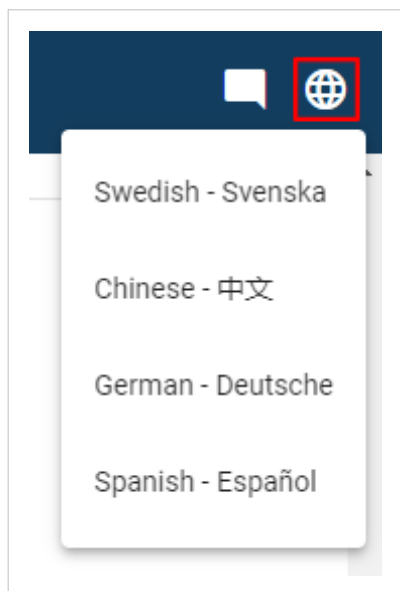


Figure 82. Language menu

2. Select a new language from the list.

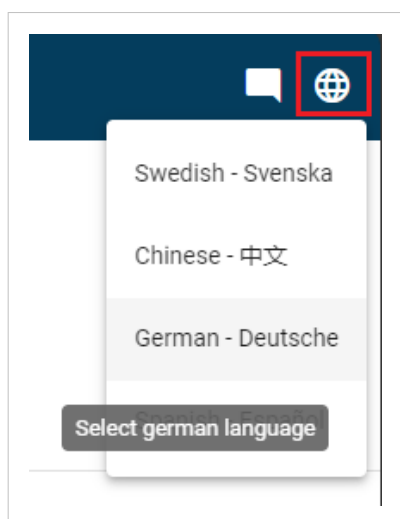


Figure 83. Example: Change language to German

The language change takes effect immediately.

14. Troubleshooting

14.1. Diagnostics

14.1.1. 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 **EtherCAT** side, including any configured endian conversions.

The screenshot displays the 'Anybus Communicator' web interface. The top header includes the logo, version information, and an 'Apply' button. The left sidebar lists various system functions. The main content area is titled 'I/O data' and features a 'Start' button to initiate data flow monitoring. Two data streams are shown side-by-side, each with a table of addresses and their corresponding hexadecimal data values. The data is updated in real-time, as indicated by the timestamps at the bottom of each table.

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): 0:00:02:11.944

Figure 84. 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**.

14.1.2. Event Log

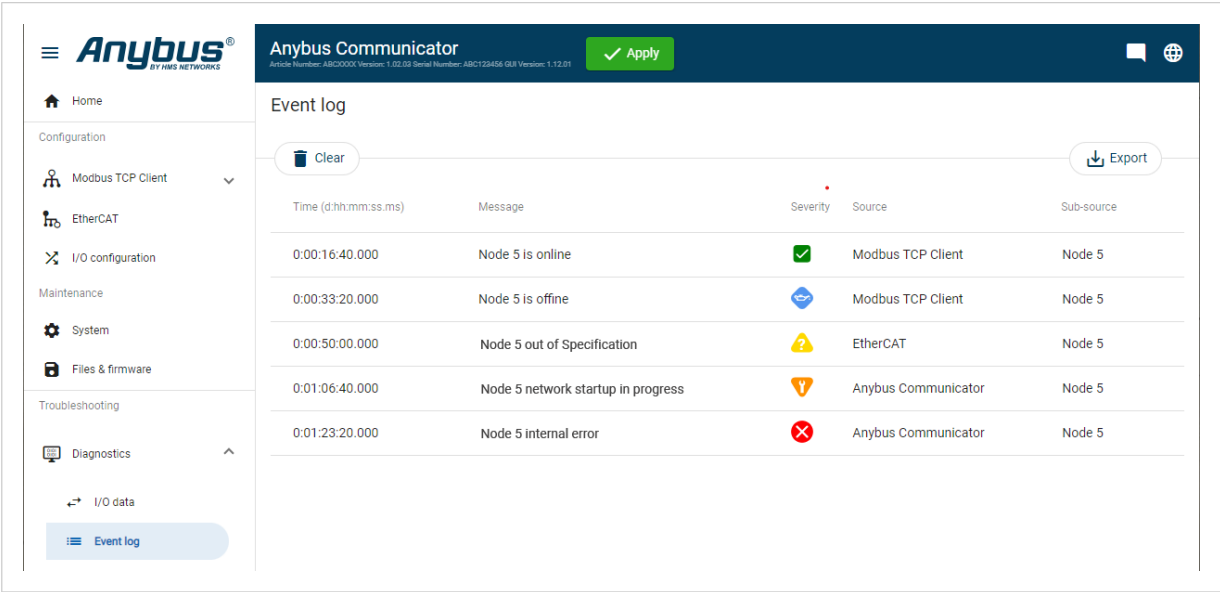


Figure 85. Event log page example

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
	EtherCAT
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**.

14.1.3. LED Status

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

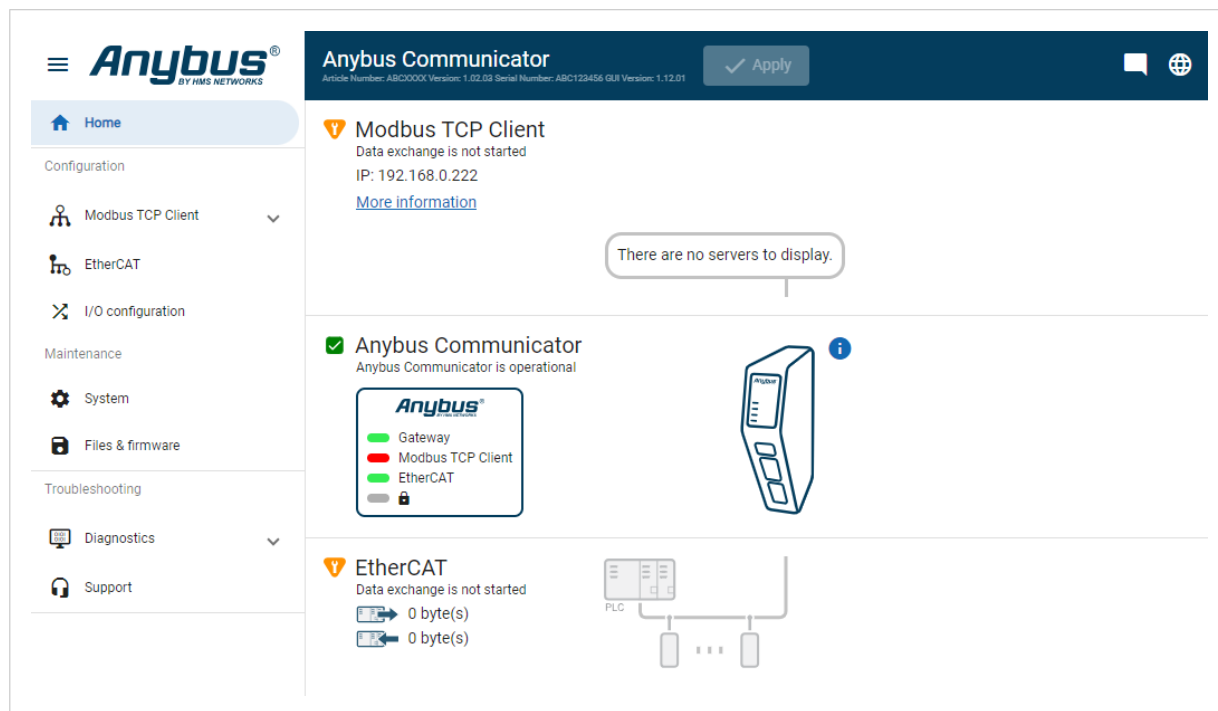


Figure 86. Home page

See Also

- [Connect To Modbus TCP Client Network \(Page 19\)](#)
- [Connect To EtherCAT Network \(Page 21\)](#)
- [Connect To Power \(Page 22\)](#)
- [Communicator Status Monitor \(Page 91\)](#)
- [Communicator LED Indicators \(Page 93\)](#)
- [Firmware Upgrade Error Management \(Page 113\)](#)

14.2. 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.

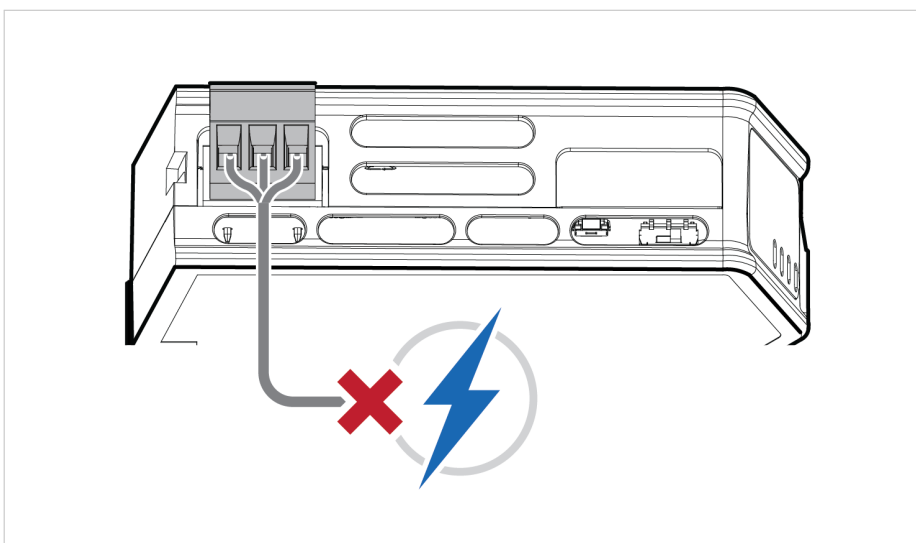


Figure 87. Disconnect power

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

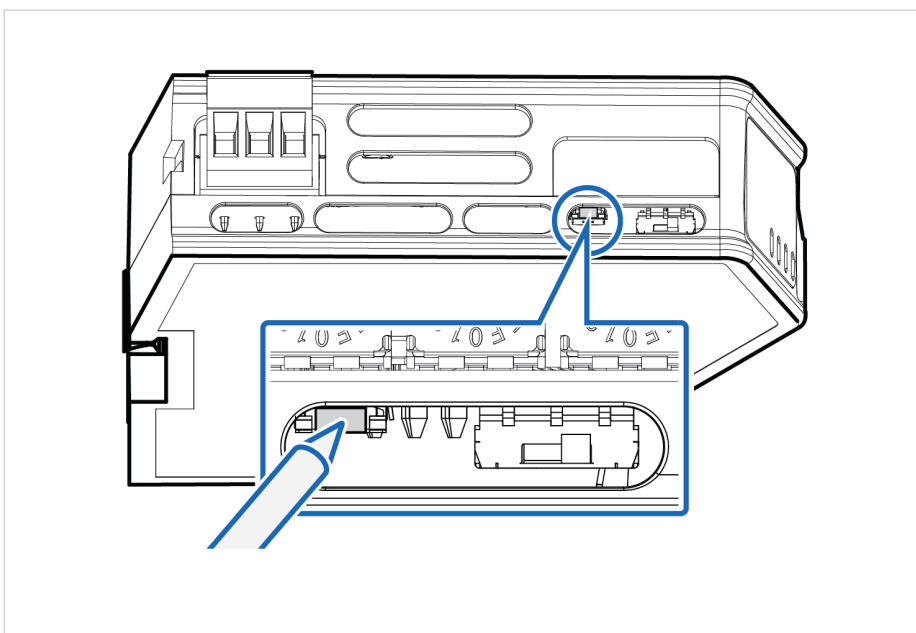


Figure 88. Press and hold **Reset** button

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

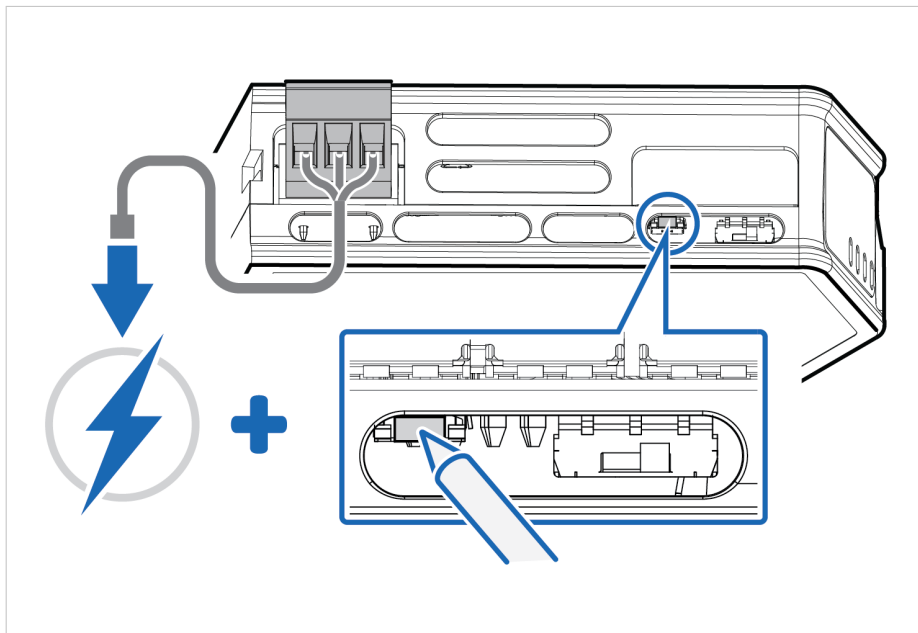


Figure 89. Hold **Reset** button and reconnect power

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**.

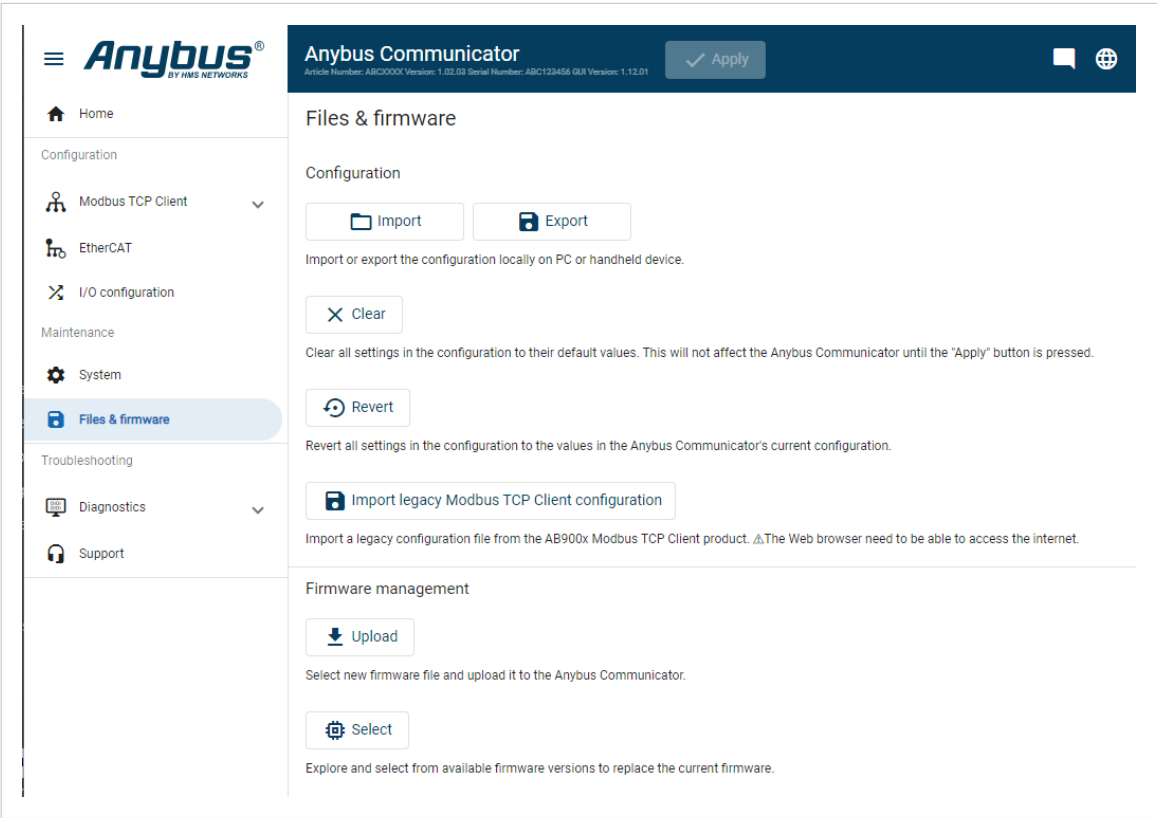


Figure 90. Files & firmware, Revert

14.3. 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.

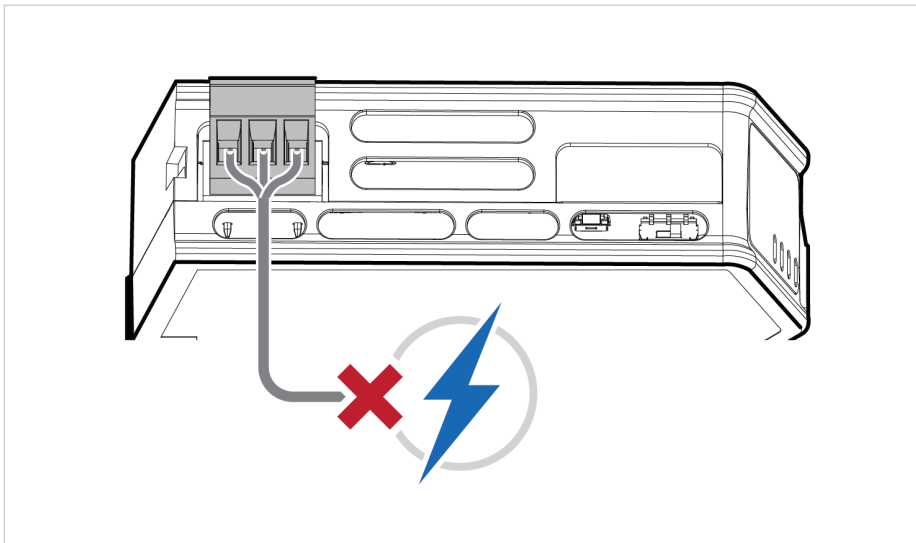


Figure 91. Disconnect power

2. Reconnect the Communicator to power.

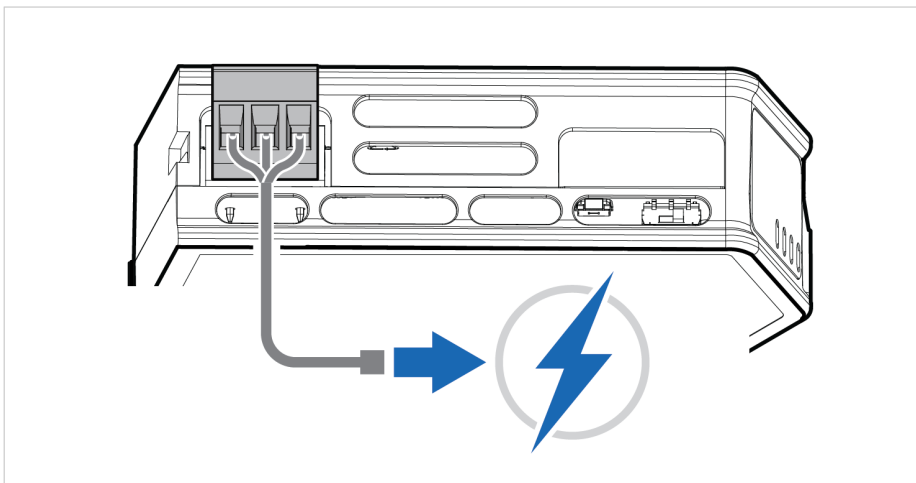


Figure 92. Reconnect power

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

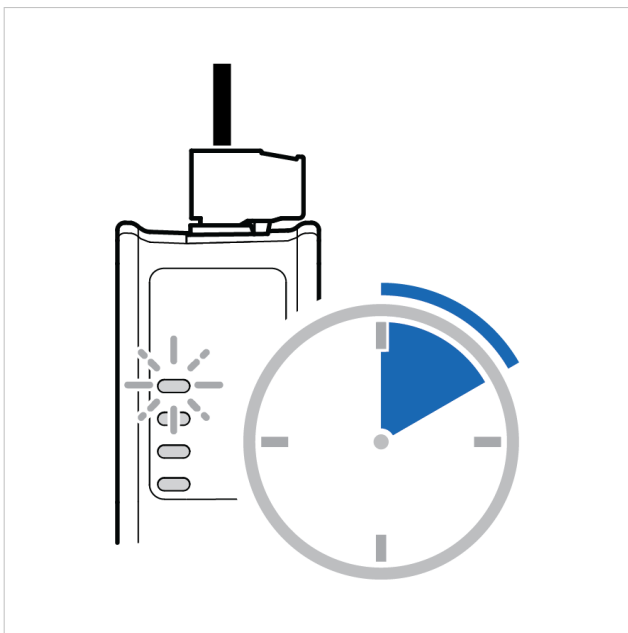


Figure 93. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

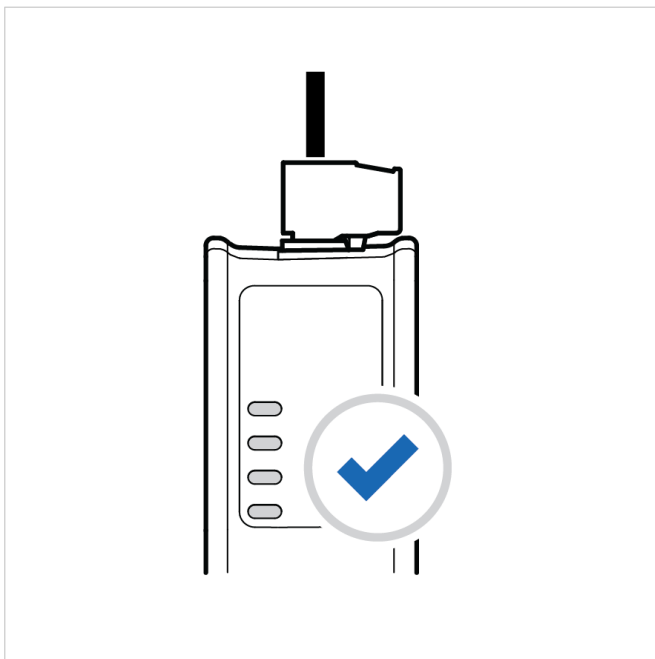


Figure 94. Recover and return to normal operation

See Also

[Connect To Modbus TCP Client Network \(Page 19\)](#)

[Connect To EtherCAT Network \(Page 21\)](#)

[Connect To Power \(Page 22\)](#)[Communicator Status Monitor \(Page 91\)](#)[Communicator LED Indicators \(Page 93\)](#)[LED Status \(Page 109\)](#)

14.4. Support

14.4.1. Support Package

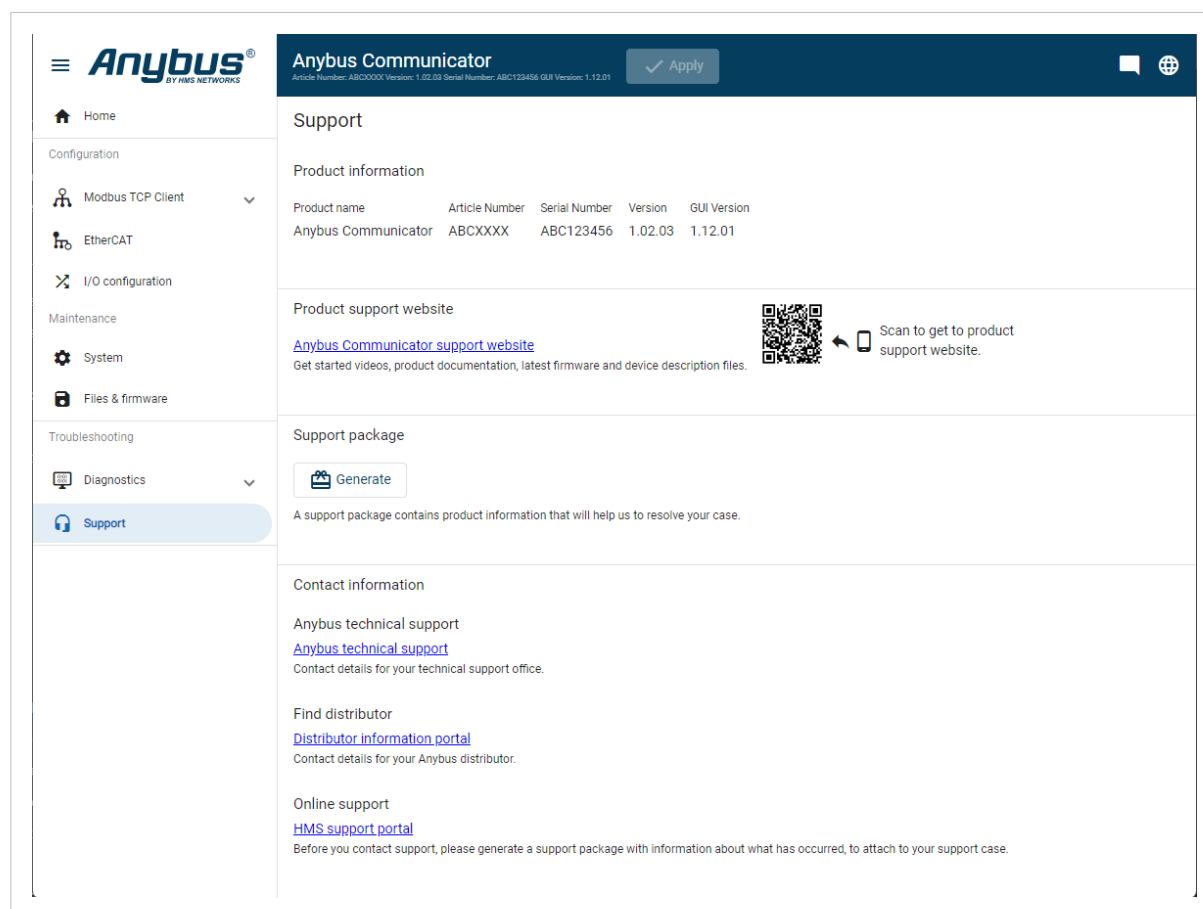


Figure 95. Support page example

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.

15. End Product Life Cycle

15.1. 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 \(page 110\)](#).

16. Technical Data

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

16.1. Technical Specification

Article identification	ABC3261
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