ENGLISH

Anybus® Communicator™ - Modbus RTU to EtherNet/IP Scanner

USER MANUAL

SCM-1202-221
Version 1.1
Publication date 2025-04-25

Important User Information

Disclaimer

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

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

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

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

This page is intentionally left blank.

1. Preface

1.1. About This Document

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

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

1.2. Document Conventions

Lists

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

1. First do this
2. Then do this

Bulleted lists are used for:

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

User Interaction Elements

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

Program Code and Scripts

```
Program code and script examples
```

Cross-References and Links

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

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

Safety Symbols

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

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

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

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

Information Symbols

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

TIP
Helpful advice and suggestions.

1.3. Trademarks

Anybus® is a registered trademark of HMS Networks.

All other trademarks are the property of their respective holders.

2. Safety

2.1. Intended Use

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

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

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

2.2. General Safety

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

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

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

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

3. Cybersecurity

3.1. General Cybersecurity

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

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

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

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

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

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

See Reset to Factory Settings (page 83).

3.2. Security Advisories

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

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

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

3.3. How to Report a Vulnerability

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

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

3.4. Product Cybersecurity Context

3.4.1. Security Defense in Depth Strategy

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

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

3.4.2. Purdue Model

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

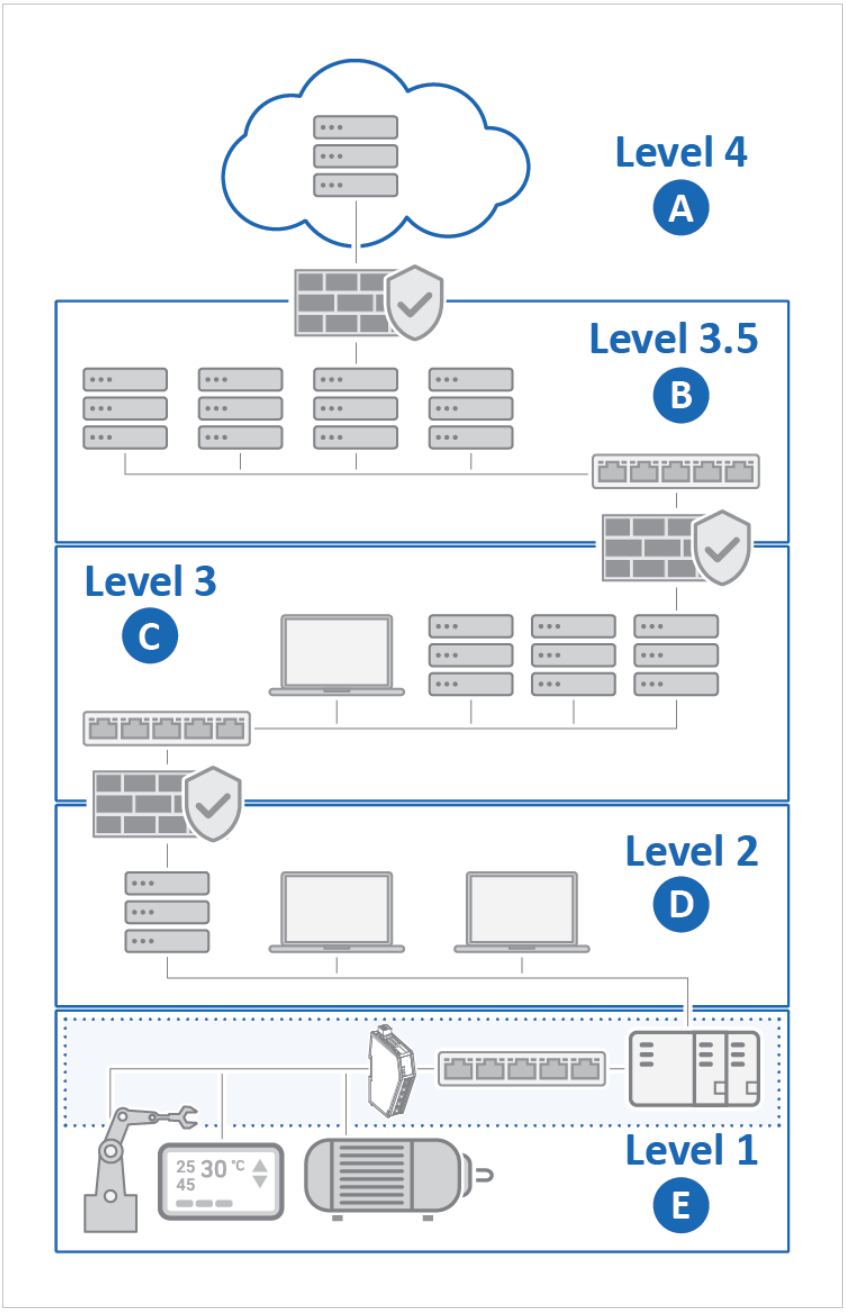


Figure 1. Purdue model, product security context

IT Network

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

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

OT Network

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

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

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

4. Preparation

4.1. Cabling

Have the following cables available:

- Ethernet cable for configuration.
- Ethernet cable for connecting to network.
- 7-pin screw terminal block connector is included with the product.
- Power cable.

4.2. Mechanical Tools and Equipment

Have the following tools available:

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

– Flat-head screwdriver, size 3 mm
  Needed when connecting the cables to the 7-pin connector.

4.3. System Requirements

4.3.1. Supported Operating Systems

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

4.3.2. Supported Web Browsers

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

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

4.4. 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.

4.5. 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.

4.6. 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.

4.7. 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.

5. About Anybus Communicator

5.1. EtherNet/IP Scanner Communication

5.1.1. EtherNet/IP Scanner Building Blocks

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

Adapter

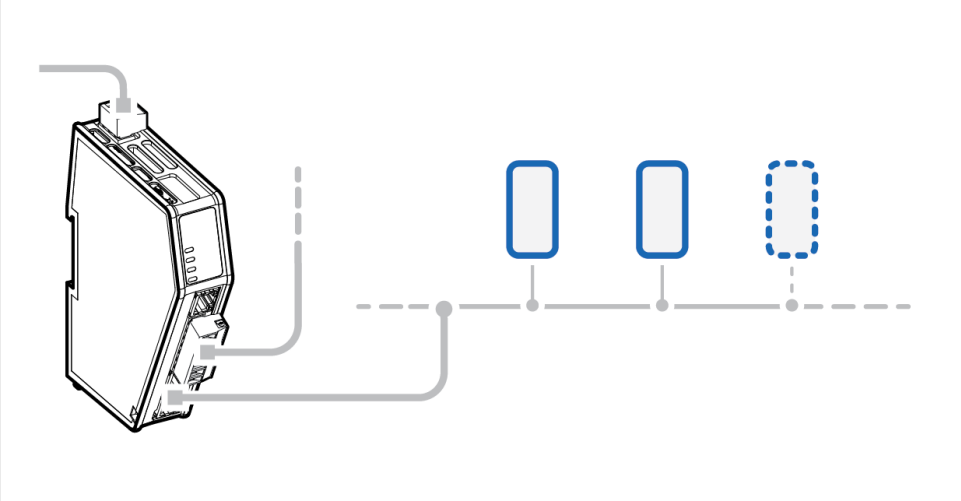


Figure 2. Adapters on a EtherNet/IP subnetwork

An adapter represents a single EtherNet/IP device on the EtherNet/IP subnetwork.

Adapters and Connections

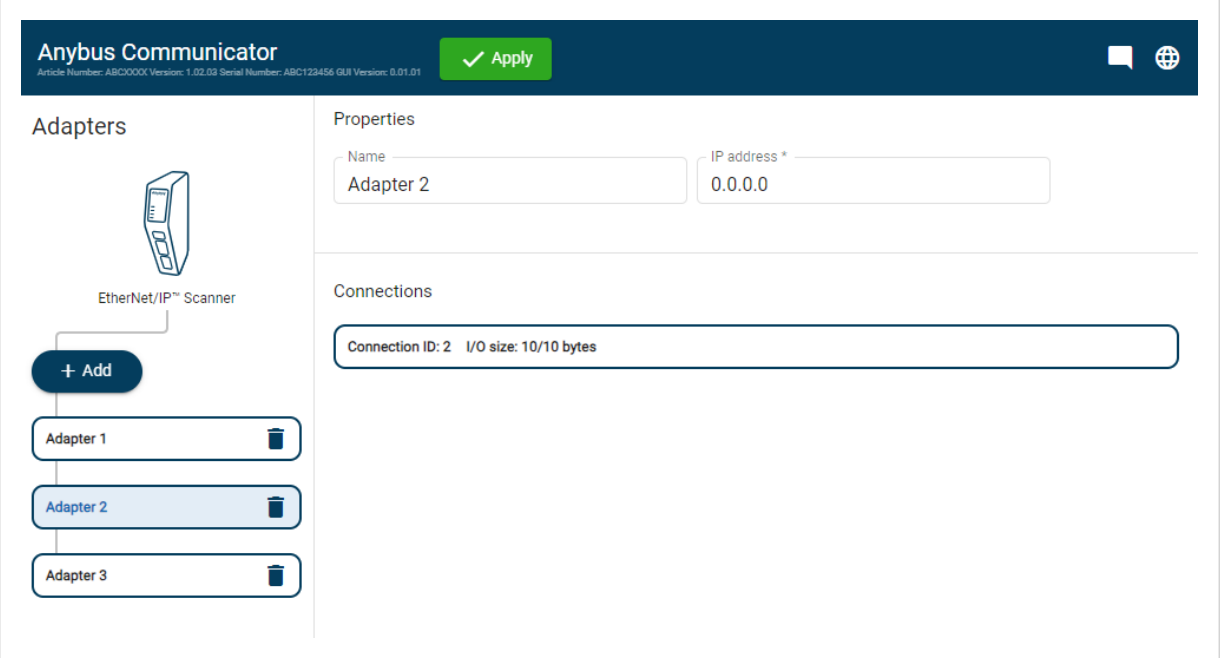


Figure 3. Adapter with Connection

To create the scan list, Adapters are added to the Ethernet/IP Scanner.

Each Adapter has one Connection that is connected to one Assembly instance for each direction.

In and Output data is sent and received over this single connection.

5.2. How the Communication Works

The Communicator enables communication, data exchange, between one or more adapter devices connected to a EtherNet/IP subnetwork and a controller device connected to a high level network.

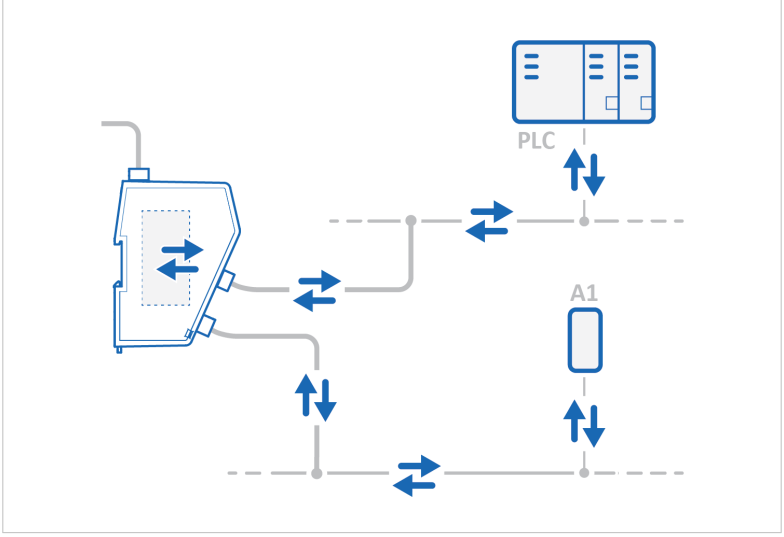


Figure 4. Process data traffic overview

For example:

- The controller device can be a PLC controller or a PC.
- An adapter device can be a sensor, barcode scanner, industrial robot or sniffer.

The Communicator main task is to setup I/O connections to adapter(s), in order to exchange input/output data.

Input Process Data

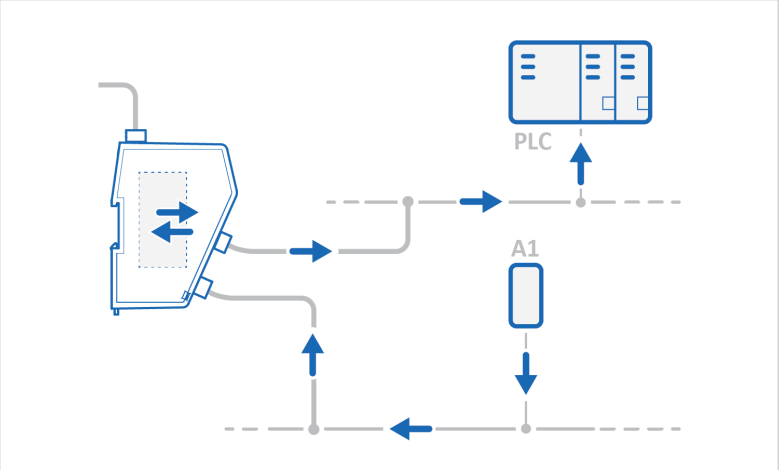


Figure 5. Process data traffic from adapters to scanner

Request process data from the EtherNet/IP adapters, specified in the Communicator configuration, and make the process data available for the PLC on the high level network.

Output Process Data

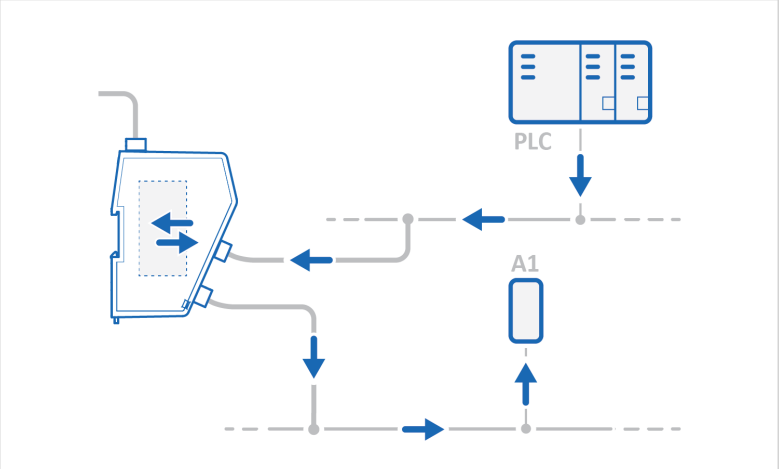


Figure 6. Process data traffic from scanner to adapters

Output data is sent from the high level network PLC to the Communicator, which forwards the data to the EtherNet/IP adapters via the subnetwork.

5.3. How the Data Exchange Works

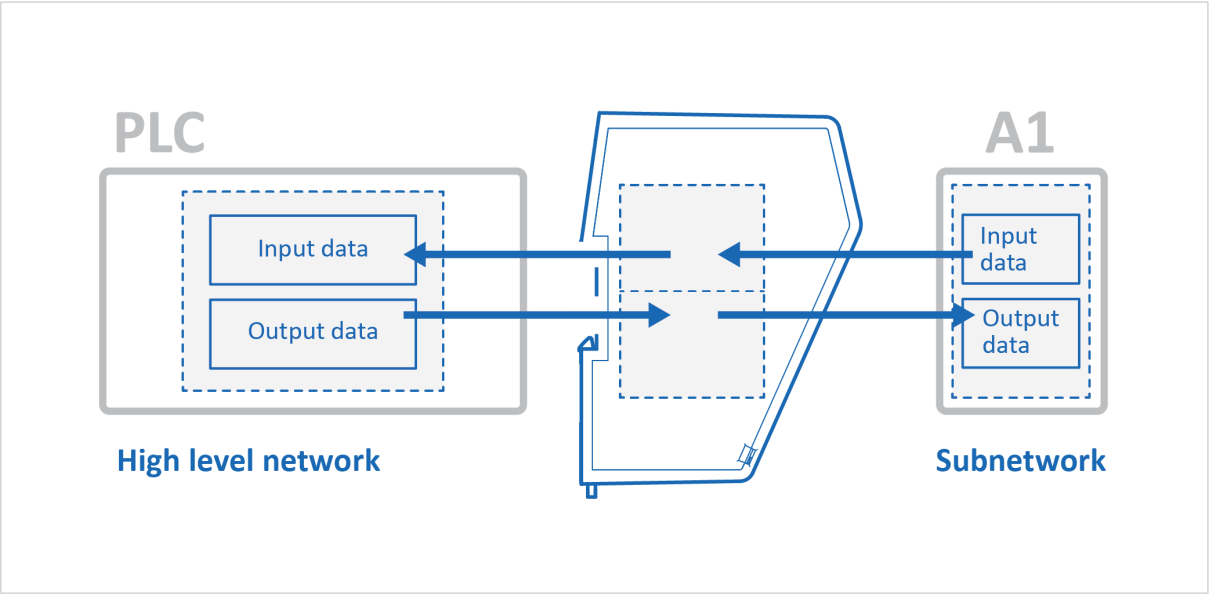


Figure 7. The Communicator internal memory areas

The data exchanged between the Communicator and the EtherNet/IP subnetwork subnetwork and the high level network resides in the Communicator internal memory buffer.

To exchange data with the EtherNet/IP subnetwork subnetwork, the high level network reads and writes data to the Communicator internal memory buffer.

The same memory locations are exchanged on the EtherNet/IP subnetwork subnetwork.

The structure of the EtherNet/IP subnetwork network I/O is 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 written by the high level network.

5.4. Data Integrity

There is no consistency between the connections on the EtherNet/IP subnetwork.

When a connection is set to produce data on the EtherNet/IP subnetwork, the output data is copied from the most recent process data sent from the highlevel network.

When a connection consumes data on the EtherNet/IP subnetwork, the input data and the most recent data from all consuming connections are copied to the high-level network.

6. Installation

6.1. External Parts

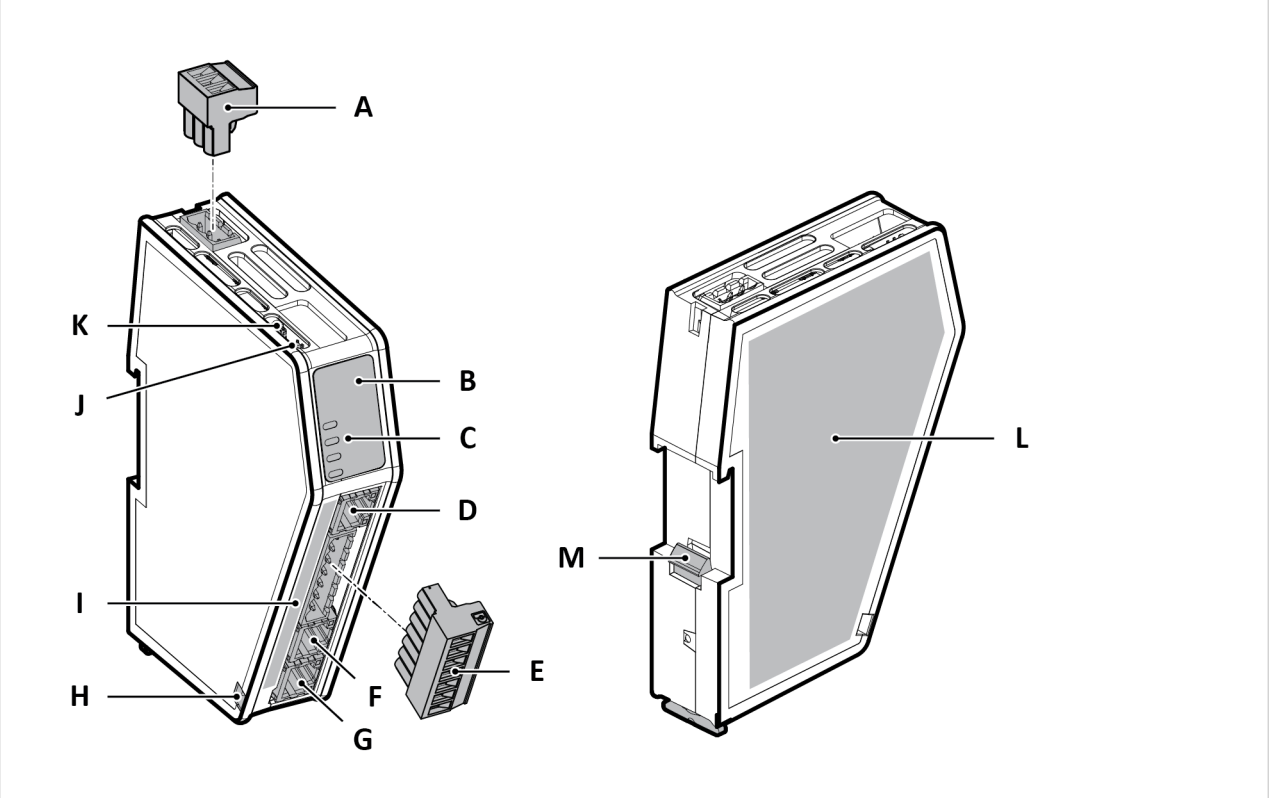


Figure 8. External parts

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

6.2. Connector Port Guide

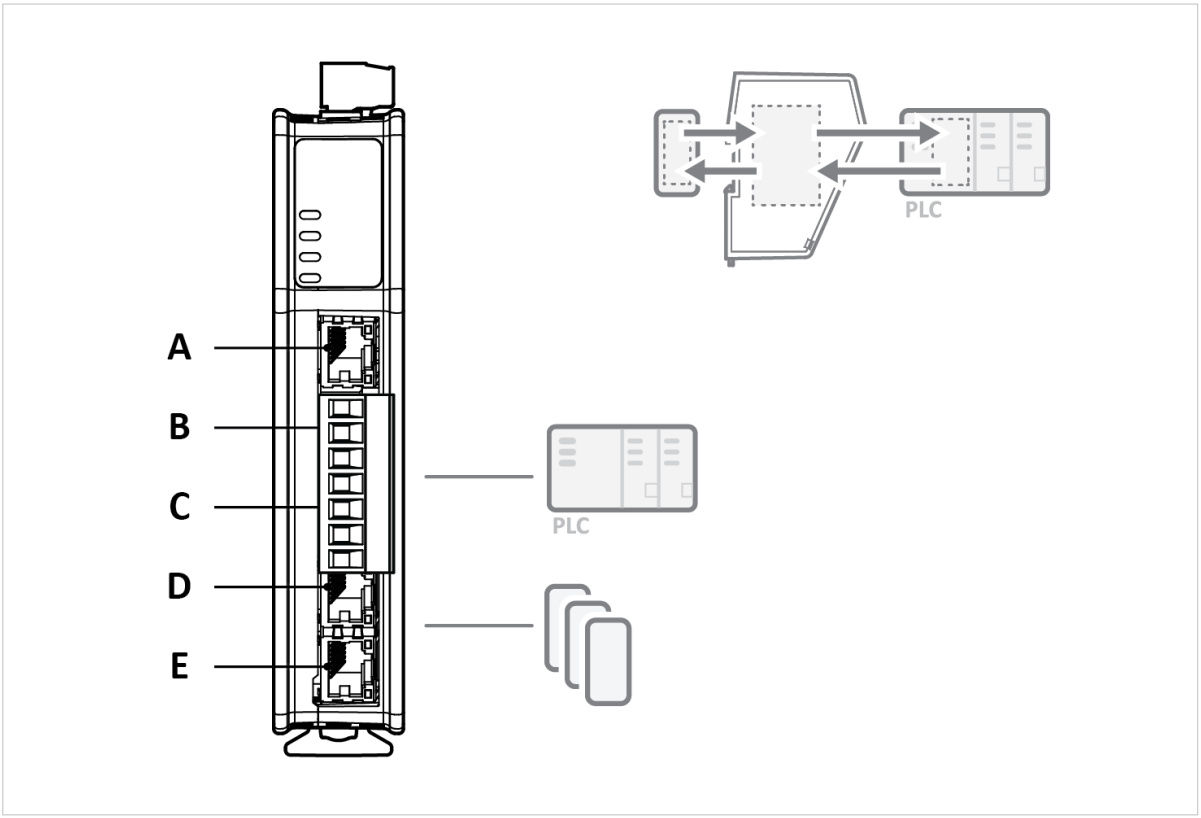


Figure 9. Communicator connector ports

Position	Port Number	Connector	Port Usage
A	X1	Ethernet RJ45	Configuration port
B	X2	7 Pin Screw Terminal Block	Modbus RTU Server network
C	X3.1	Ethernet RJ45	EtherNet/IP network
D	X3.2	Ethernet RJ45	EtherNet/IP network

See also Connect to EtherNet/IP Network (page 17) and Connect to Modbus RTU Network (page 18).

6.3. DIN Rail Mounting

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

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

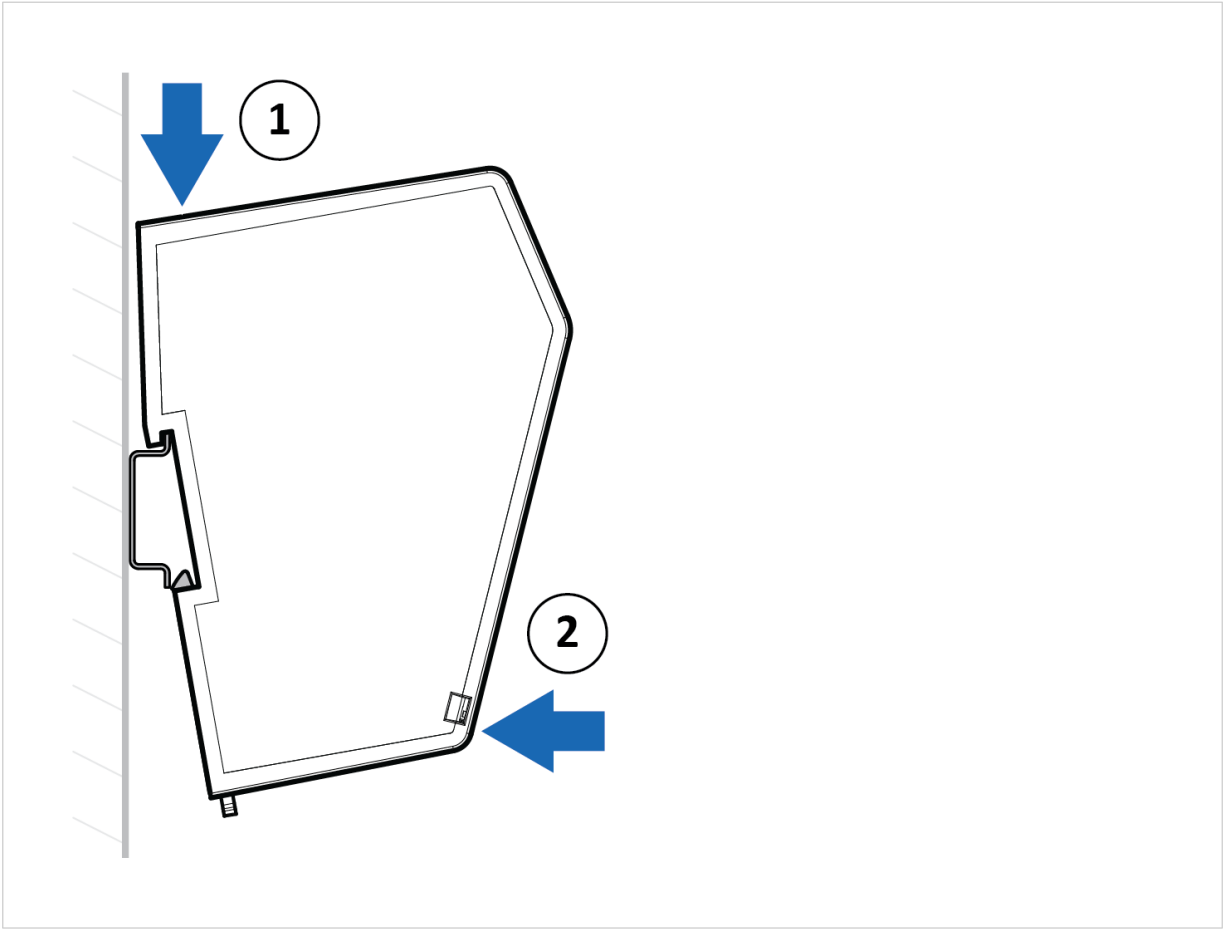


Figure 10. Attach the Communicator on the DIN rail

To attach the Communicator on the DIN rail:

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

6.4. Connect to EtherNet/IP Network

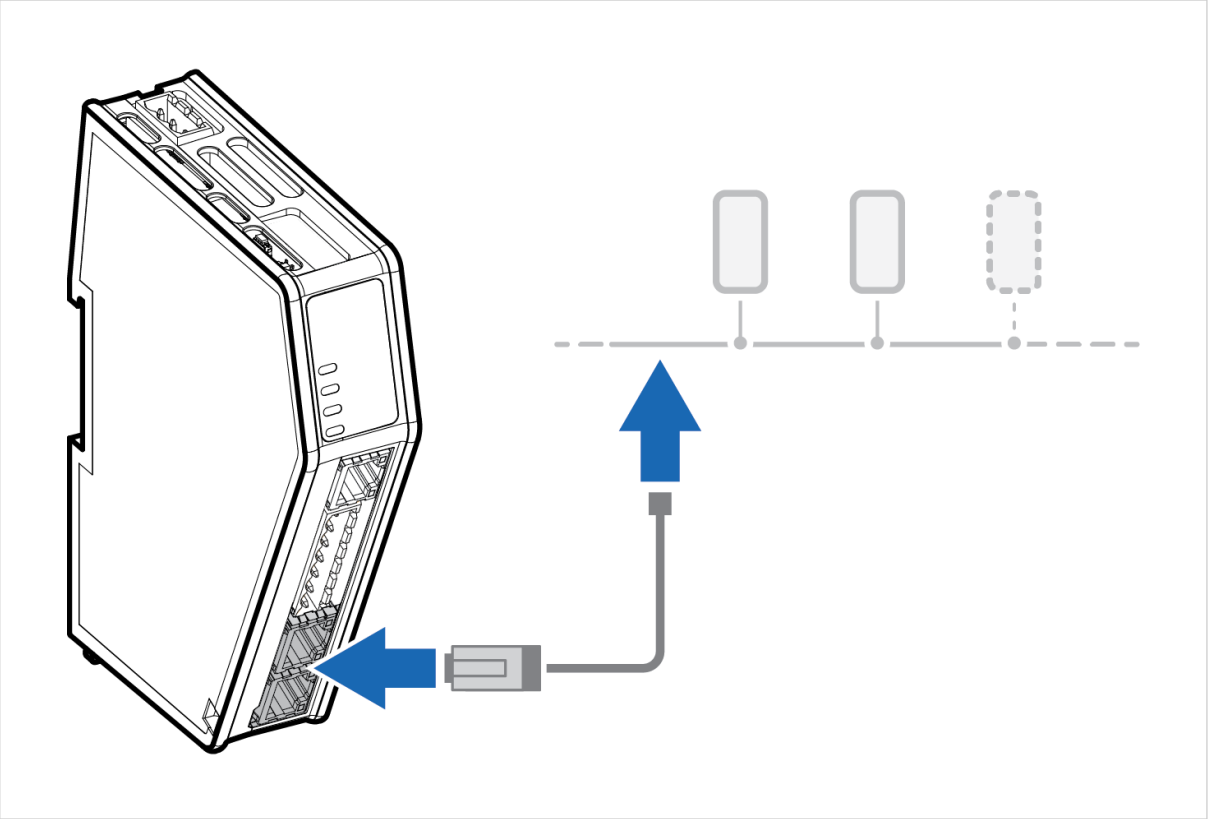
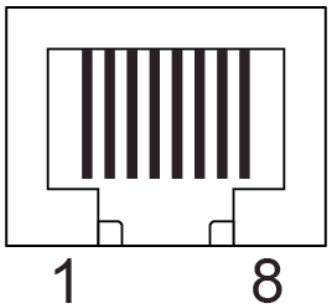


Figure 11. Connect to EtherNet/IP network

Procedure

Connect the Communicator to your EtherNet/IP network.

Ethernet RJ45 Connector Pinout

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

6.5. Connect to Modbus RTU Network

NOTE
Use minimum 90 oC copper (Cu) wire only.

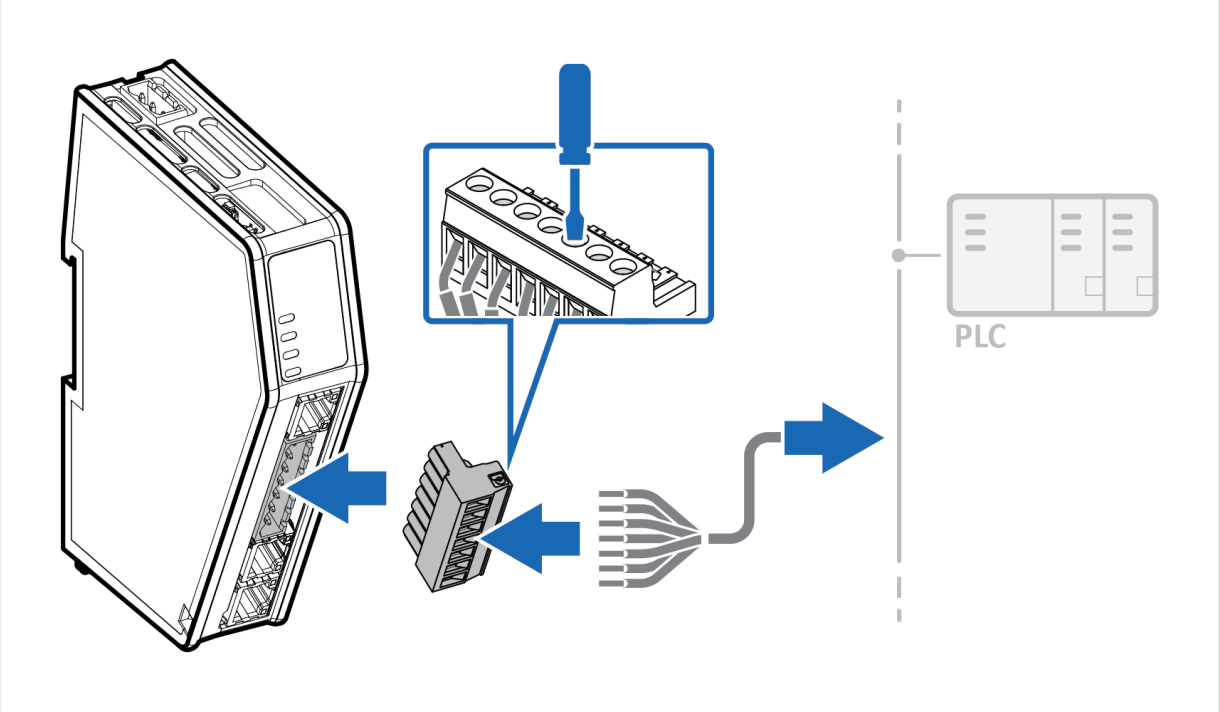


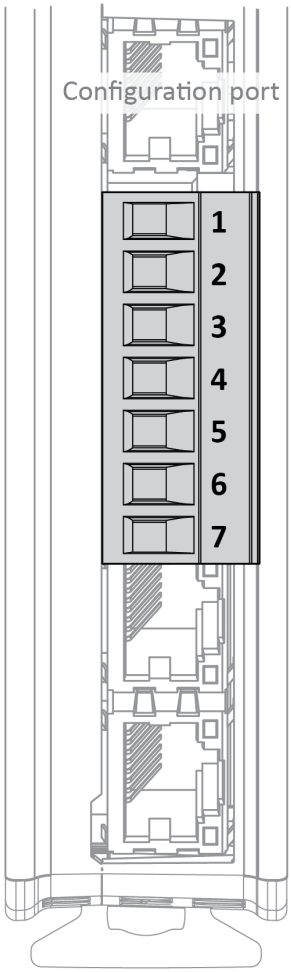
Figure 12. Connect to Modbus RTU network

Procedure

1. Insert the cable wires into the 7-pin connector and tighten the wire clamp screws.
2. Connect the 7-pin connector to the Communicator.
3. Connect the Communicator to your Modbus RTU network.

Modbus RTU Serial Connector Pinout

NOTE
Use minimum 90 oC copper (Cu) wire only.

7-pin connector	Pin	Signal
	1	+5 V OUT
	2	RS485+ A
	3	RS485- B
	4	Signal GND
	5	Functional Earth (FE)
	6	RS232 Tx Transmit Data
	7	RS232 Rx Receive Data

6.6. Connect to Power

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

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

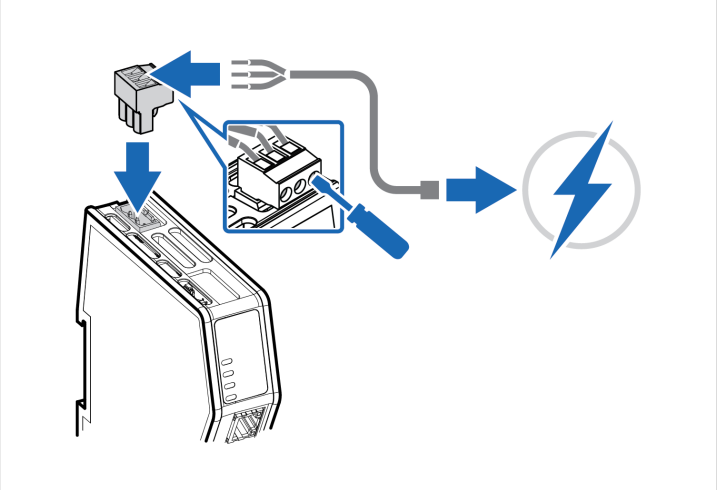
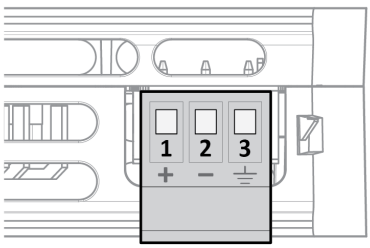


Figure 13. Connect to power

Power Connector Pinout

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

Procedure

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

6.7. Security Switch

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

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

To Lock and Unlock the Security Switch

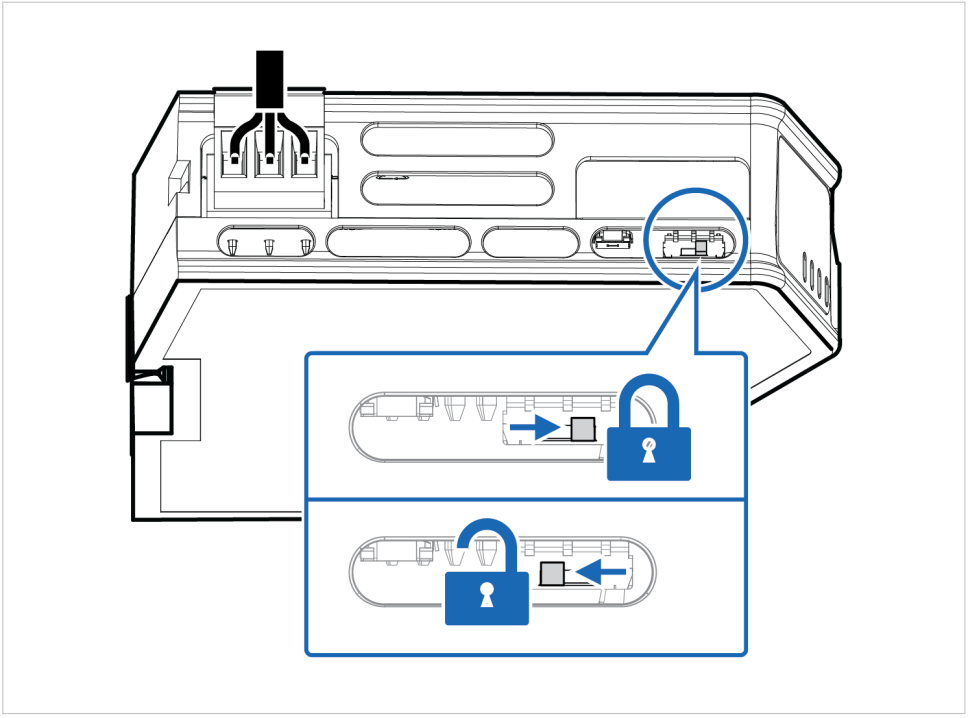


Figure 14. Security switch in locked and unlocked position

Use a pointed object, such as a ballpoint pen.

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

Security Switch Status LED

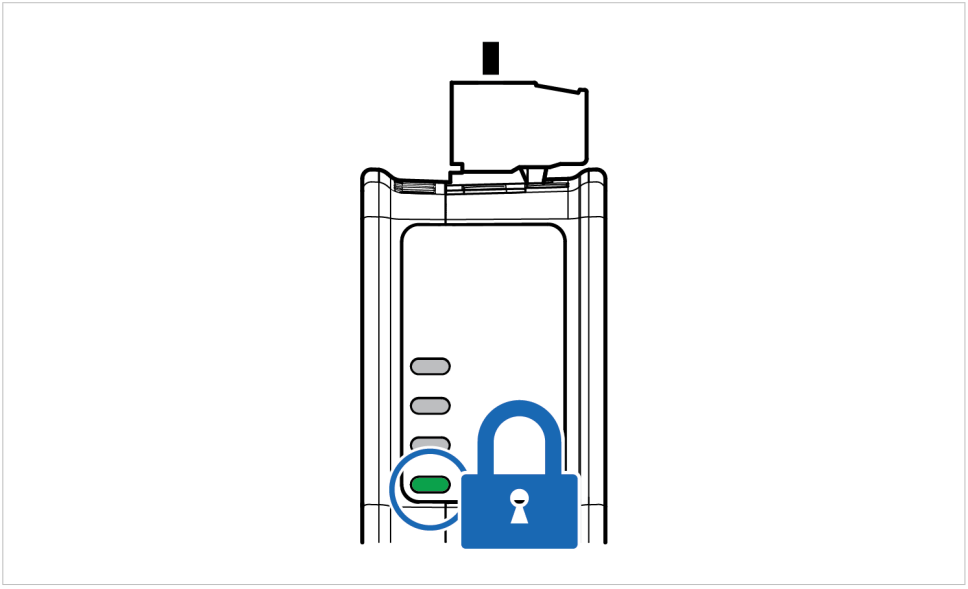


Figure 15. Security switch locked status LED

When the security switch is in its:

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

6.8. Lock the Cables

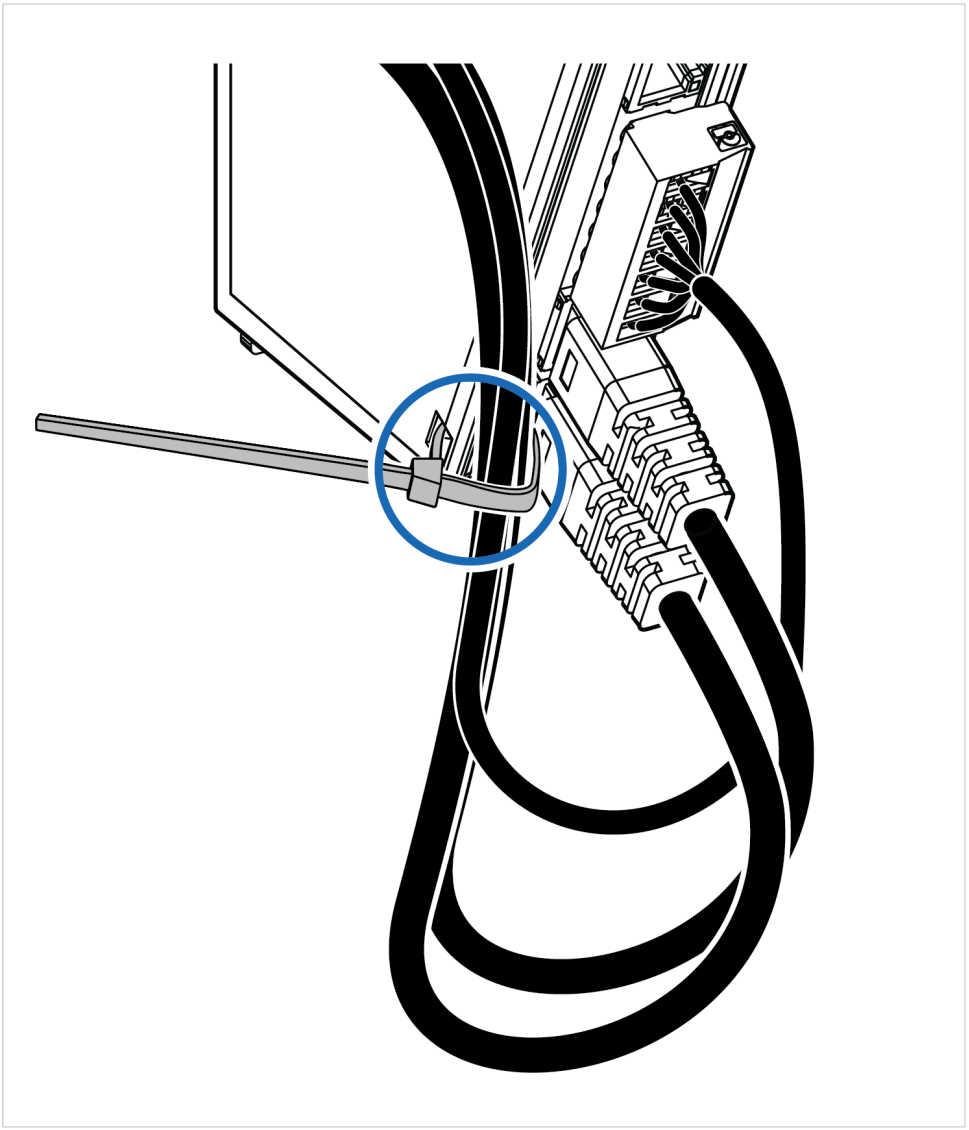


Figure 16. Lock the cables

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

6.9. DIN Rail Demount

Before You Begin

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

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

Procedure

Remove the Communicator from the DIN rail:

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

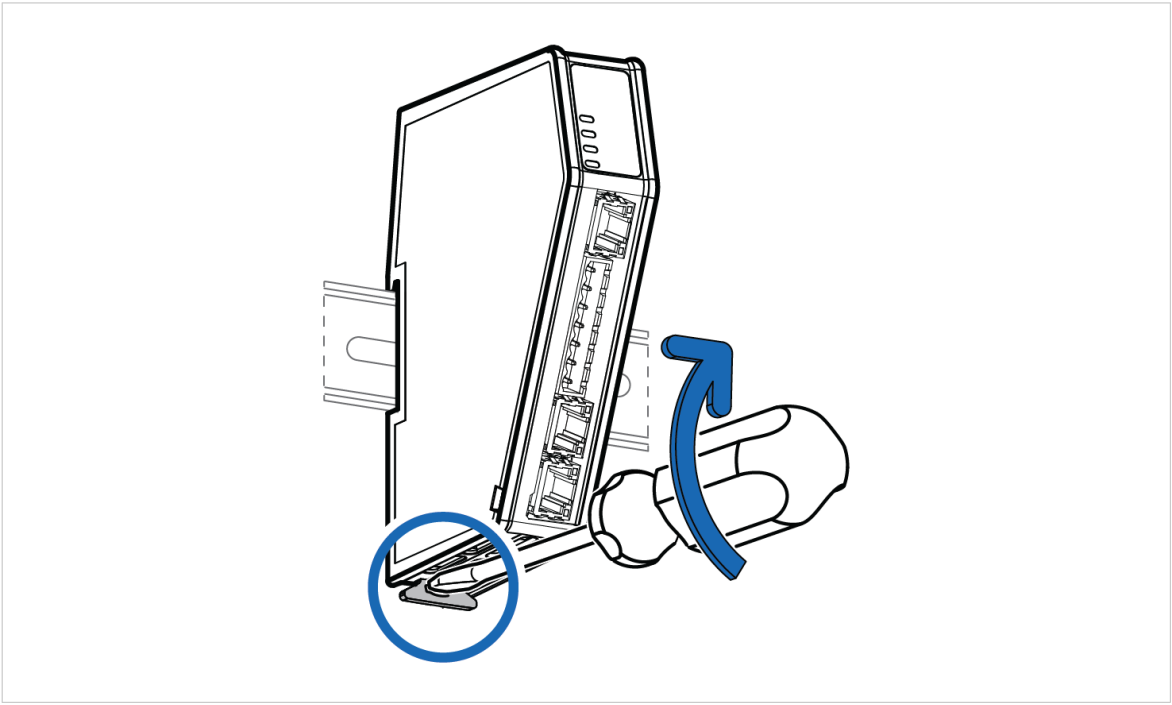


Figure 17. Unlock the Communicator

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

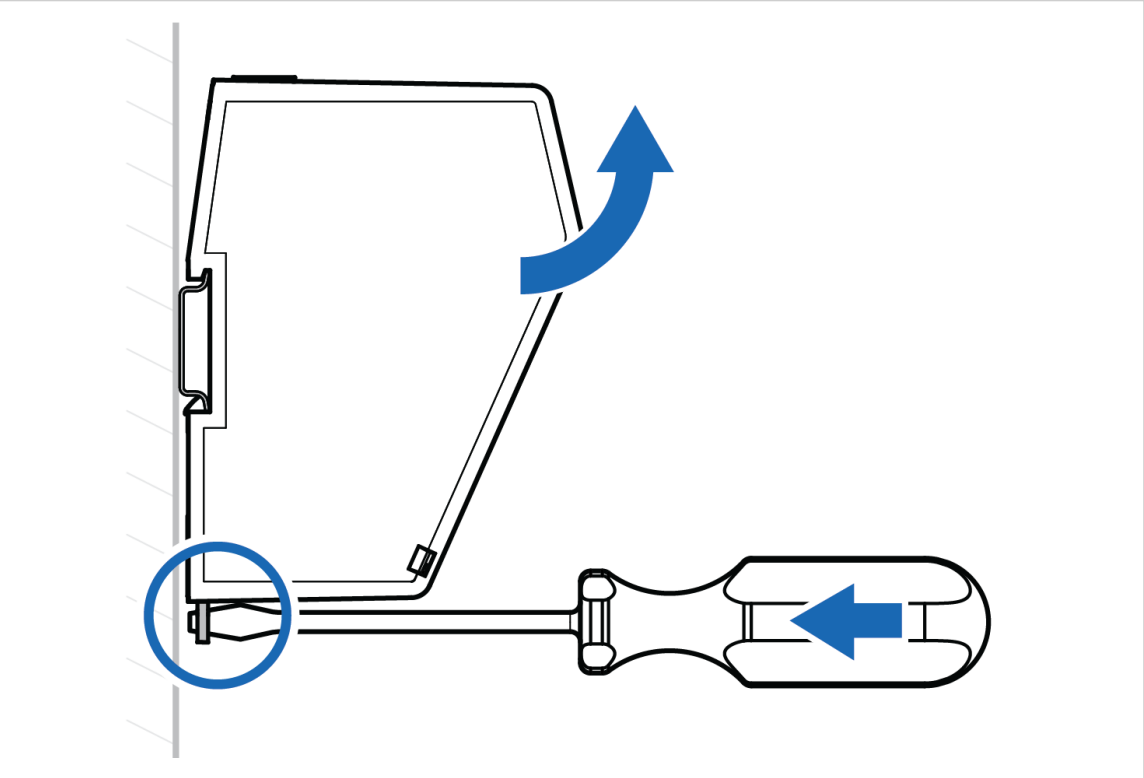


Figure 18. Unhook the Communicator

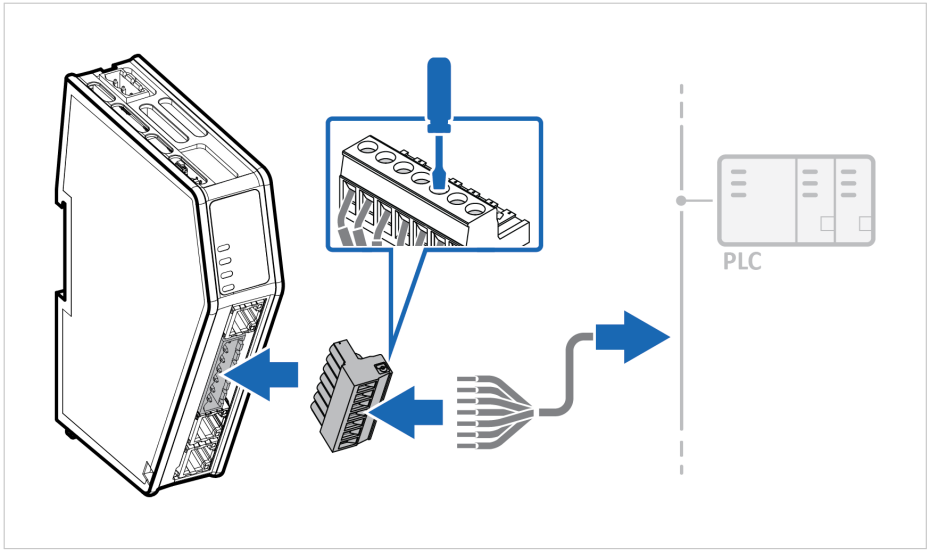
7. Configuration Quick Guide

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

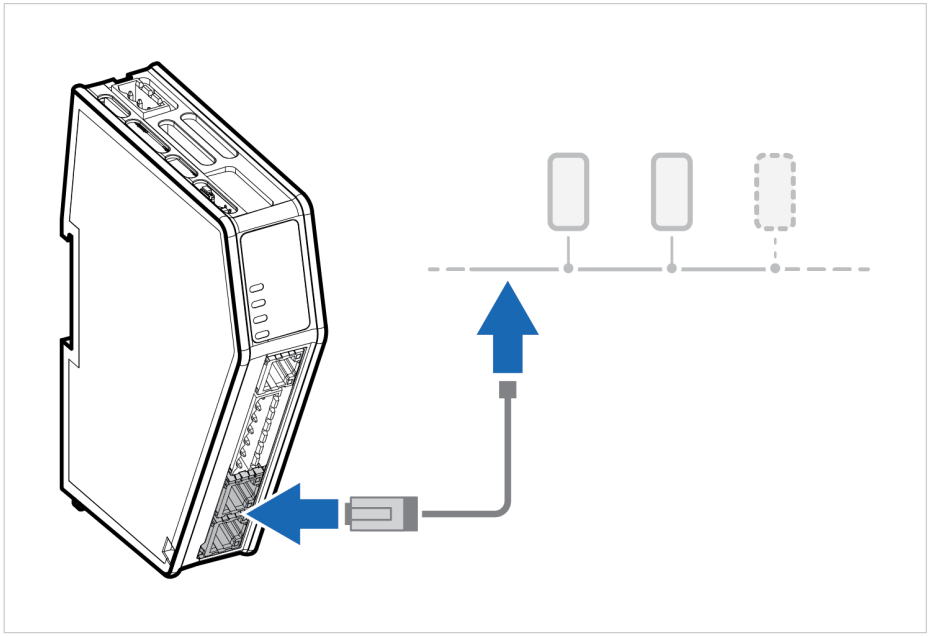
For detailed information, please refer to Communicator Configuration (page 34) .

7.1. Prepare Configuration

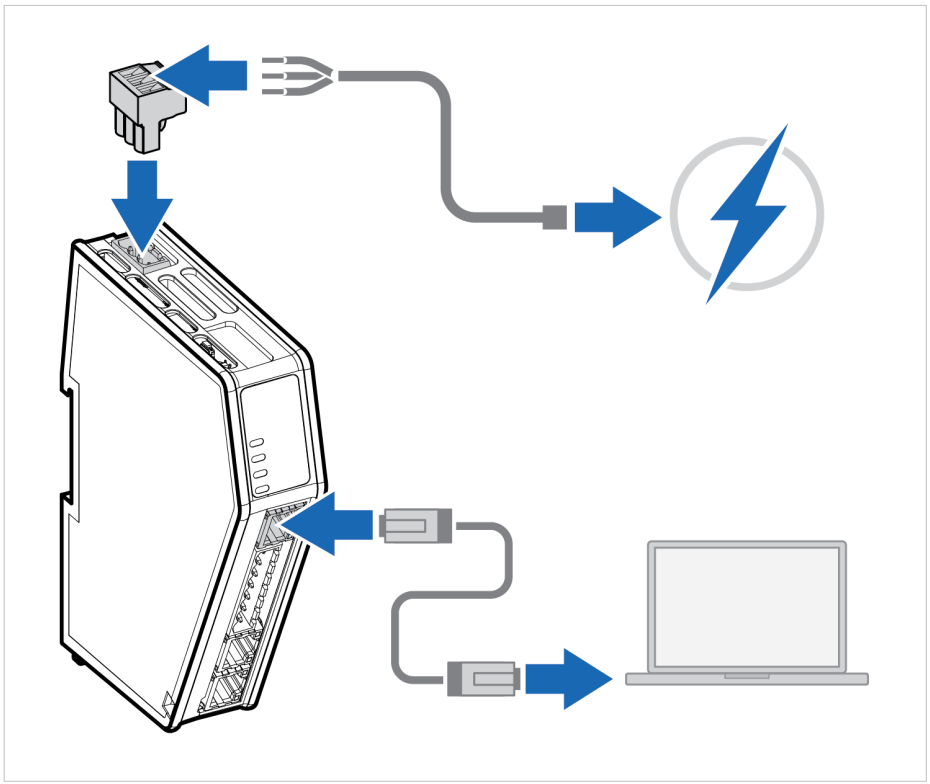
1. **Connect the Communicator to the EtherNet/IP subnetwork**



2. **Connect Communicator to the Modbus RTU network.**



3. **Connect to PC and power**



a. Connect an Ethernet cable between the Communicator configuration port and your PC.

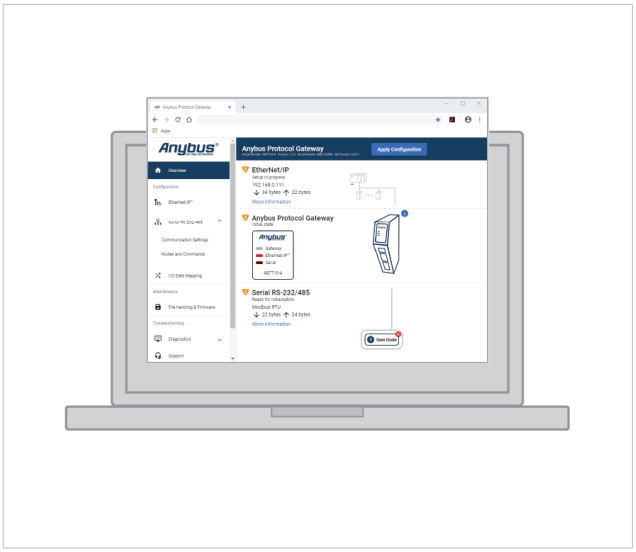
b. Connect the Communicator to a power supply.

4. **Find the Communicator on your PC**

The Communicator default IP address is 192.168.0.10.

Option 1	Option 2
	
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.	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.

5. **Access the Communicator built-in web interface**



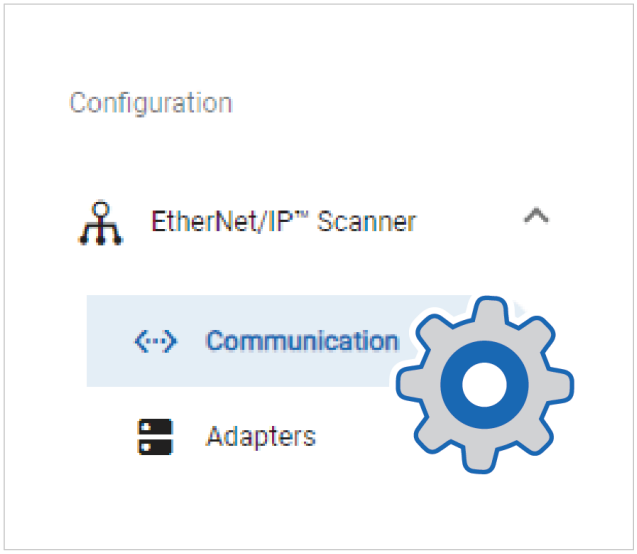
Open the Communicator built-in web interface in HMS IPconfig or enter the Communicator IP address in your web browser.

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

7.2. Setup New Configuration

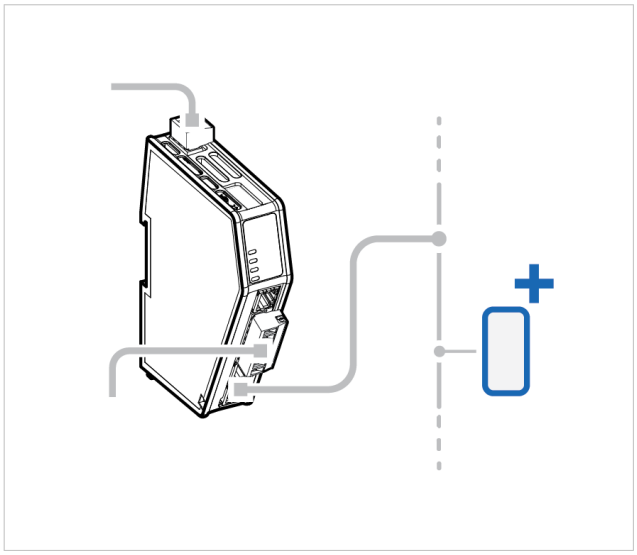
Follow these steps to setup a new Communicator configuration.

1. **Subnetwork configuration**



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

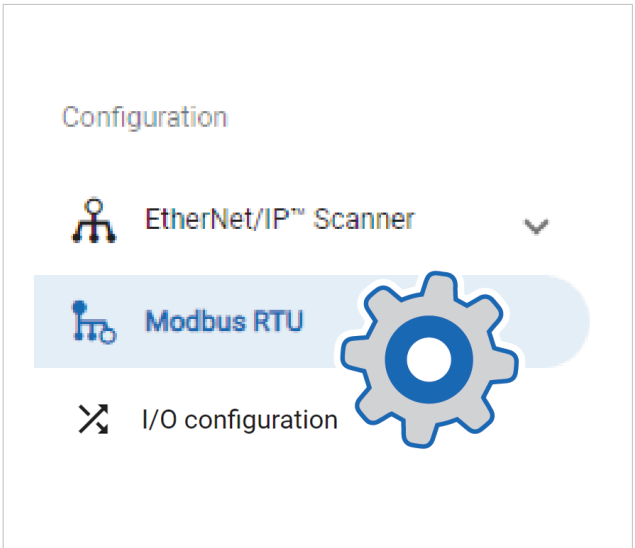
2. **Add Adapters**



On the **Adapters** page:

a. Add a adapter and configure the adapter **Properties**.
b. Configure the adapter **Connections** settings.
c. Repeat until you have added and configured all your adapters.

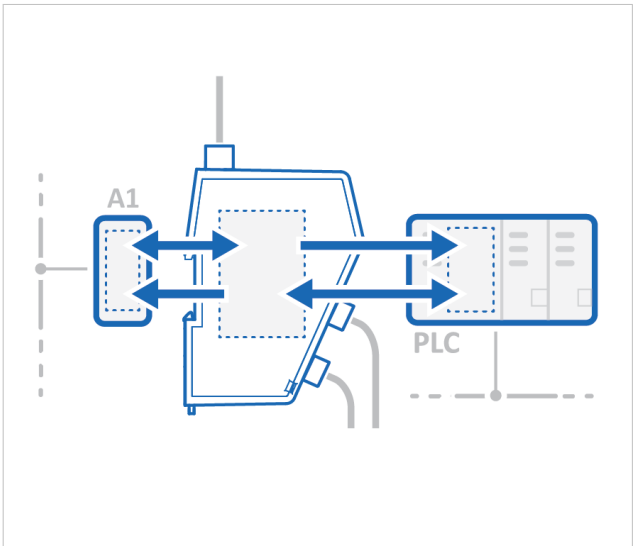
3. **High level network configuration**



On the **Modbus RTU** page:

1. Configure the Communication settings.
2. Configure the Timeout times settings.

4. **I/O Configuration**

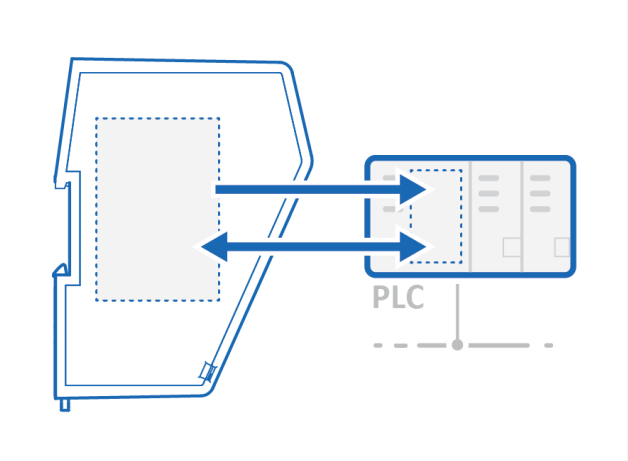


The connection for each adapter is automatically mapped to the Communicator internal memory area.
On the **I/O configuration** page, view the mapping relation between the adapter connections and the layout on the process data area.

7.3. PLC Configuration

In the PLC program:

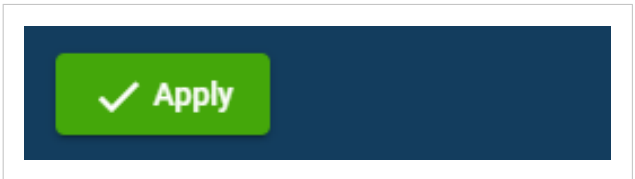
- **Configure the communication**



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

7.4. Verify Operation

1. **Apply the configuration**



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

2. **Verify status and LED indications**

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

3. **Verify and monitor communication**

In **Diagnostics**, use the:

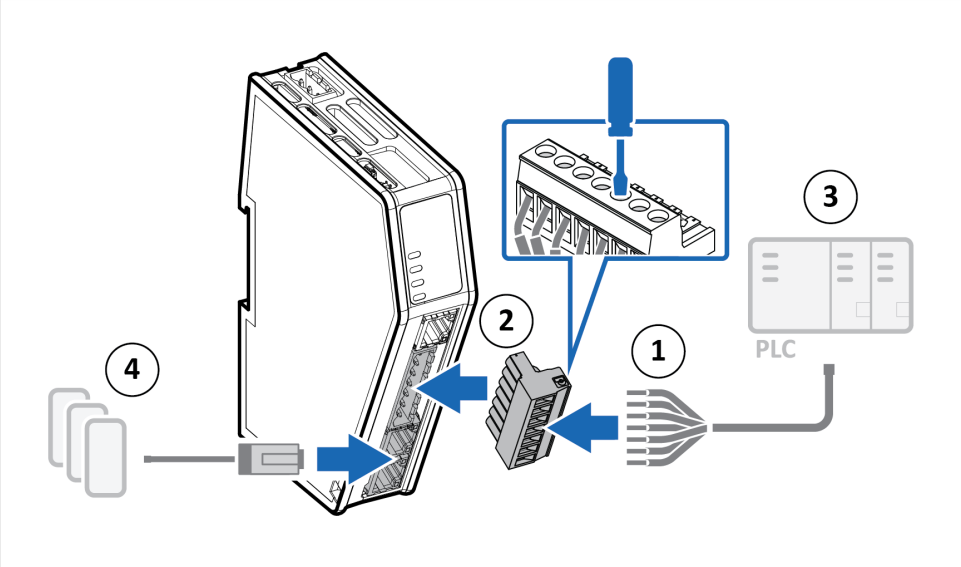
- **I/O data** page to monitor how the data flow between the **EtherNet/IP Scanner** side and the **Modbus RTU** side, including any configured endian conversions.
- **Event log** page to detect failures and unexpected behavior over time.

8. Communicator Configuration

8.1. Connect to Configure the Communicator

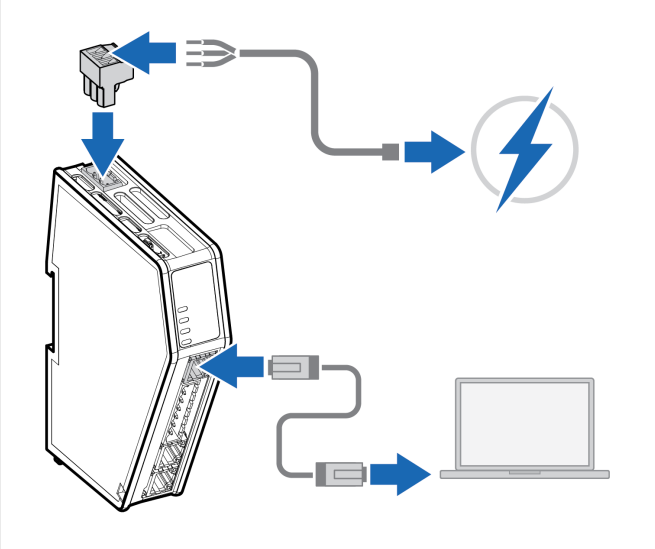
Procedure

Connect to EtherNet/IP Scanner network and Modbus RTU network



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

Connect to PC and Power



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

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

Before You Begin

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

NOTE
The Communicator default IP address is 192.168.0.10.

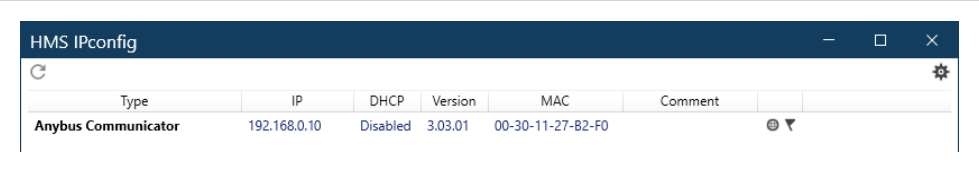
NOTE
To access the Communicator built-in web interface, ensure that Port 80 TCP is open in your Firewall. This applies to any Firewall between the web browser and the gateway.

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

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

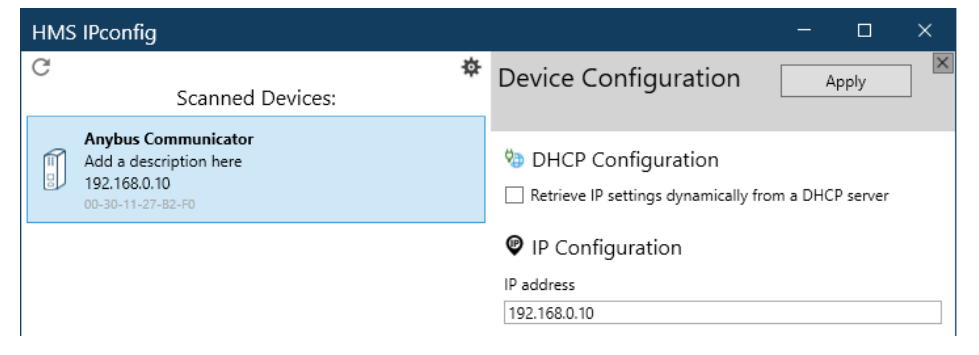
Procedure

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

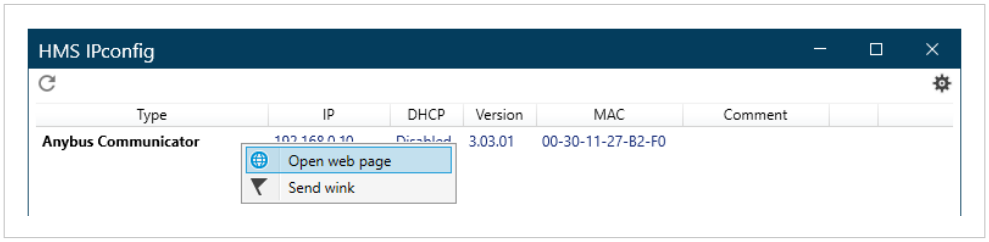


- HMS IPconfig automatically starts scanning for compatible and active HMS devices.
- Found HMS devices are added to the device list.

3. To open the settings pane, click on the Communicator in the device list.
4. Change the Communicator configuration port IP address to one within the same IP address range as your PC.

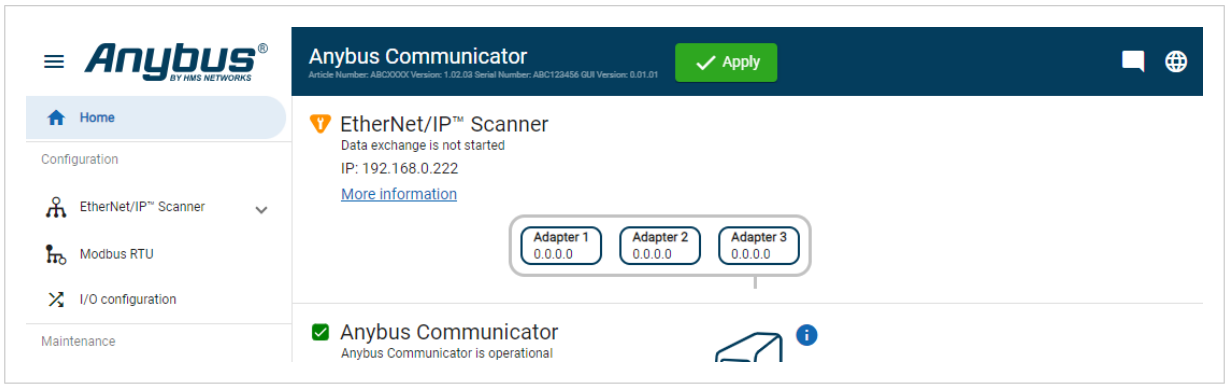


5. To open the **Open web page** built-in web interface, click Communicator.



Result

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



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

Before You Begin

NOTE
The Communicator configuration port default IP address is 192.168.0.10.

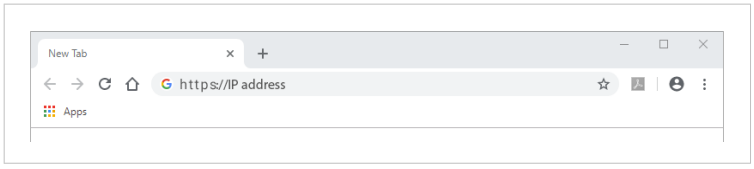
NOTE
To access the Communicator built-in web interface, ensure that Port 80 TCP is open in your Firewall. This applies to any Firewall between the web browser and the gateway.

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

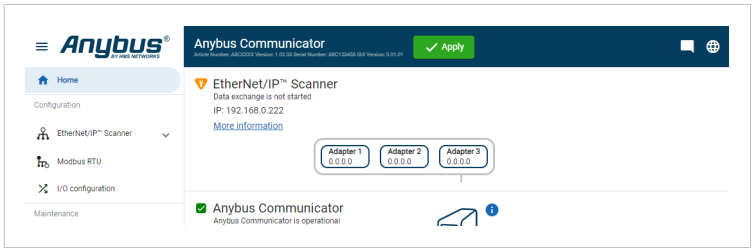
Procedure

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

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



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



8.4. Communicator Built-In Web Interface Overview

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

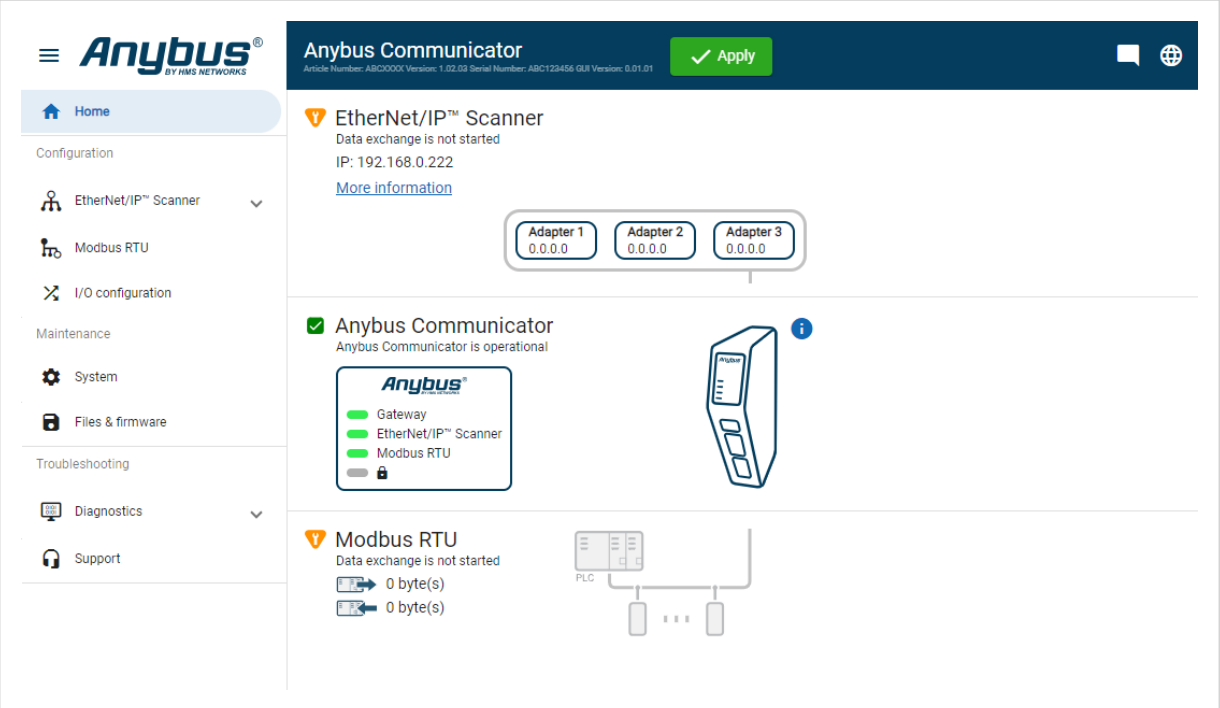


Figure 19. The Communicator built-in web interface Home page

Menu item	Description
Home	View the Communicator, network and adapter(s) status.
Apply	After configuration changes are made and verified, press Apply to make the settings take effect.
EtherNet/IP Scanner	EtherNet/IP subnetwork with adapter(s). Add adapter(s) and configure the Connections settings.
Modbus RTU	Configure the network settings for the Modbus RTU network.
I/O configuration	View the connections mapped to the Communicator internal memory area.
System	Define how the device should behave if a serious error occurs. Configure the Communicator configuration port IP settings.
Files & firmware	Save settings in a configuration files, upload configuration files and upgrade firmware.
Diagnostics	Monitor and troubleshoot the Communicator.
Support	Contains Communicator product information, Anybus contact information, link to Anybus support website, and product file for download. Here you can generate a support package with product information, to send to your Anybus support technician.

8.5. EtherNet/IP™ Scanner Communication Settings

8.5.1. To Use DHCP Server

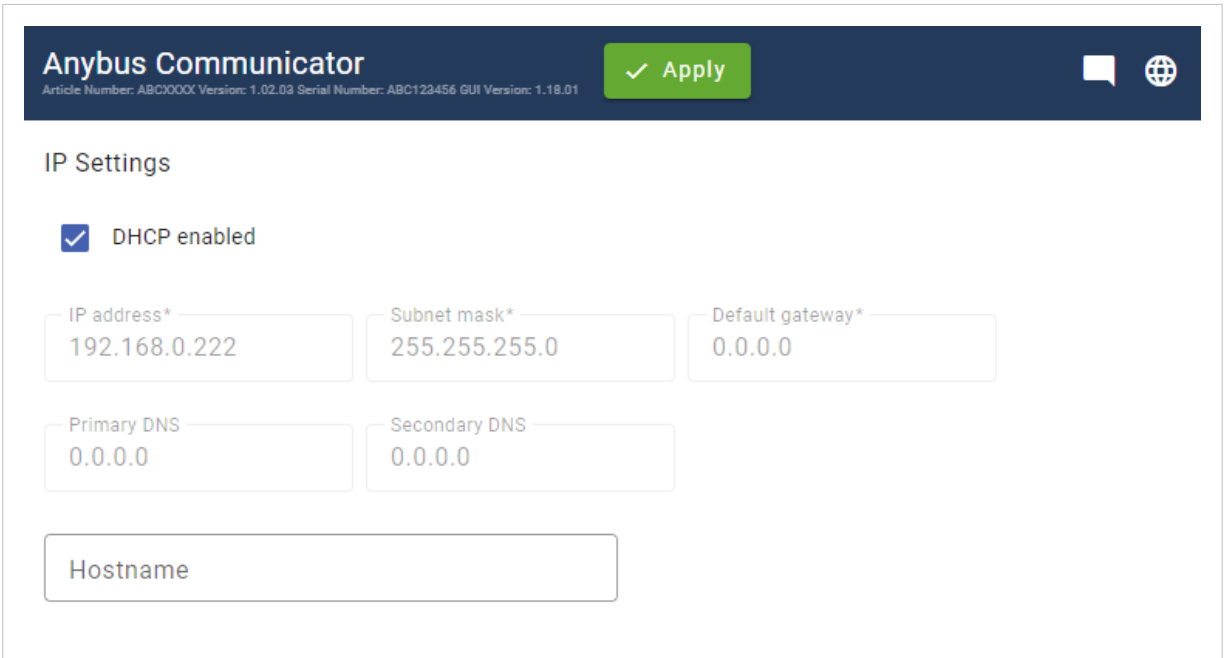


Figure 20. IP Settings, DHCP enabled

By default, DHCP is disabled.

To enable DHCP, select the **DHCP enabled** checkbox. The IP settings will be provided by the high level network DHCP server.

Default Communicator IP Settings
The Communicator comes with the following factory default IP settings:

Setting	Default value
DHCP	TBD
IP address	There is no default IP address.
Subnet mask	255.255.255.0
Gateway address	There is no default Gateway address.
Primary DNS server	There is no default Primary DNS server.
Secondary DNS server	There is no default Secondary DNS server.
Hostname	You can label the Communicator. Maximum length is 64 characters. No symbol characters, punctuation characters, or whitespace are permitted. Write the Hostname as one single word.

8.5.2. To Configure IP Settings Manually

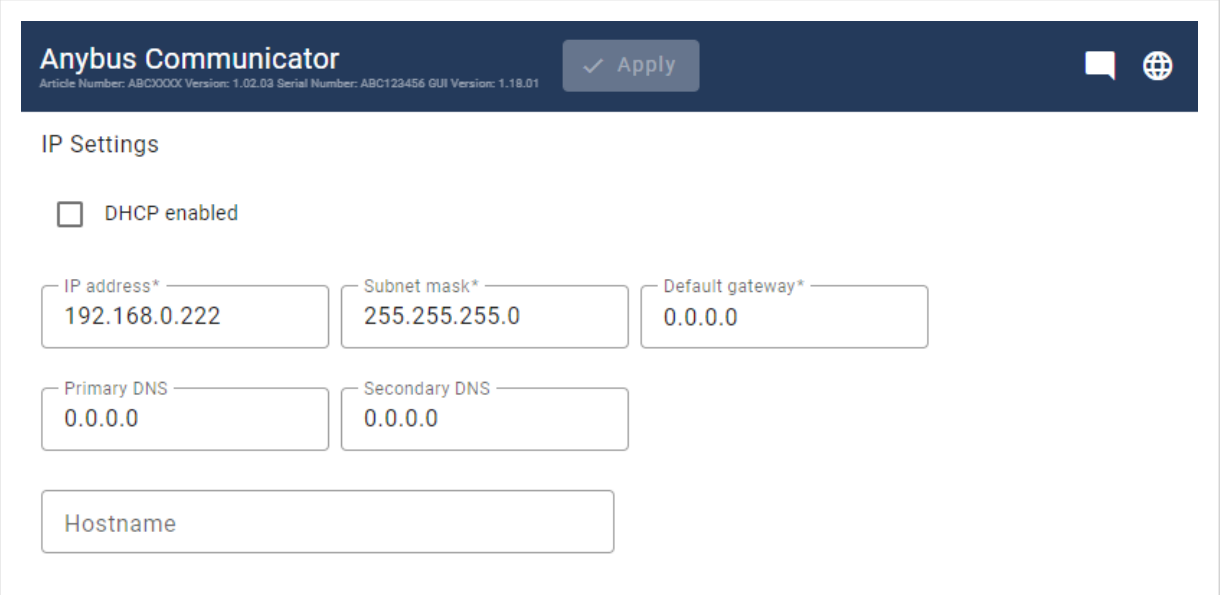


Figure 21. EtherNet/IP Scanner IP Settings, DCHP disabled

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

Setting	Description
IP address	The EtherNet/IP Scanner network IP address in IPv4 dot-decimal notation
Subnet mask	The EtherNet/IP Scanner network Subnet mask in IPv4 dot-decimal notation.
Gateway address	The EtherNet/IP Scanner network Gateway address in IPv4 dot-decimal notation. If there is no gateway available, set the Gateway address to: 0.0.0.0
Primary DNS server	The EtherNet/IP Scanner network Primary DNS in IPv4 dot-decimal notation.
Secondary DNS server	The EtherNet/IP Scanner network Secondary DNS in IPv4 dot-decimal notation.
DHCP	Off

8.5.3. Naming the Host

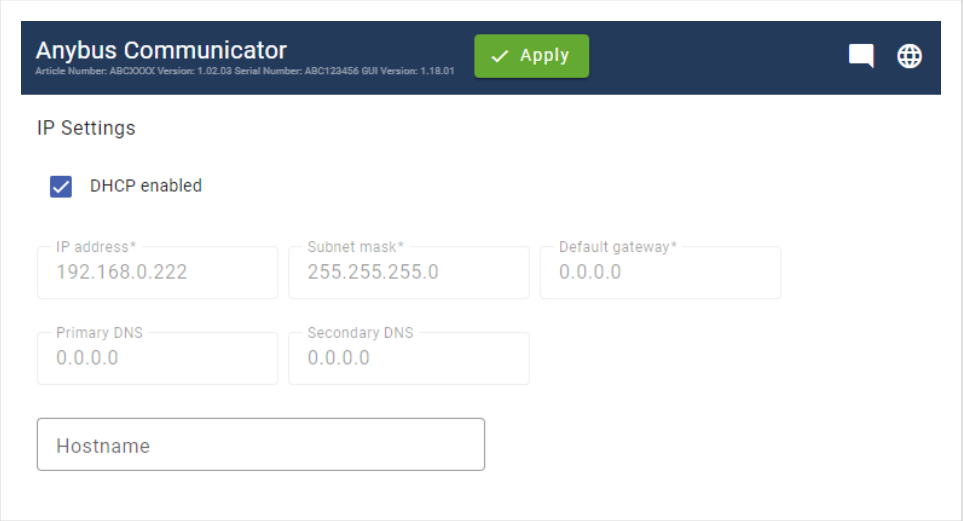


Figure 22. IP Settings Hostname

You can label the Communicator.

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

8.6. Adapters

8.6.1. About Originator and Target

The originator is the scanner that initiate data exchange with the target adapter device on the network.

The target adapter respond to the data requests generated by the originator scanner.

Who sends data to whom?		Scanner	Adapter
Originator (O) -> Target (T)	Scanner -> Adapter	Writes (Output)	Reads (Output)
Target (T) -> Originator (O)	Adapter -> Scanner	Reads (Input)	Writes (Input)

8.6.2. About Output and Input Data

Depending on how output and input are defined in the adapter's user documentation:

- Often it is defined from the scanner's point of view also in the adapter.
- The terms "input" and "output" are defined from the point of view of the scanner.
- Output I/O is the data produced by the scanner and consumed by the adapter.

8.6.3. Add Generic Adapter

Before You Begin

> **NOTE**
> The maximum number of Adapters that can be added is 32.

Procedure

1. In the web-interface left sidebar menu, click **Adapters**.
2. In the **Add** split button drop-down menu, select **Add generic adapter**.

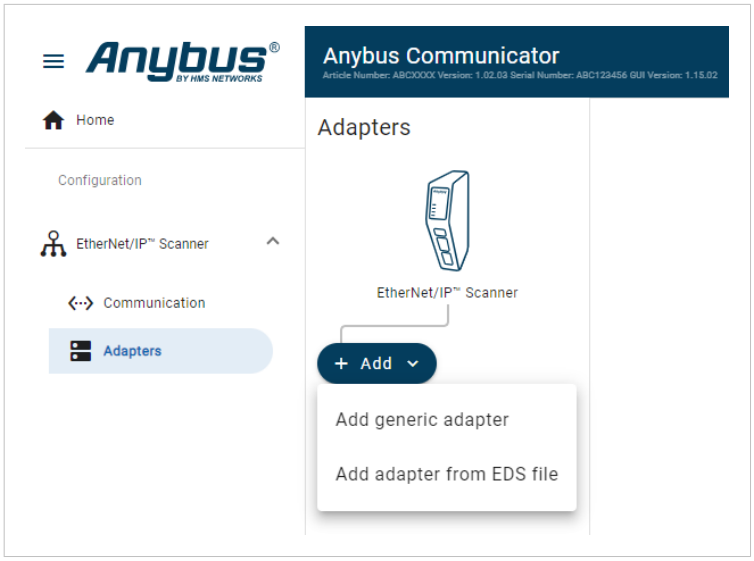


Figure 23. Add generic adapter

A new Adapter with Connection is added to the **EtherNet/IP™ Scanner** adapter list.

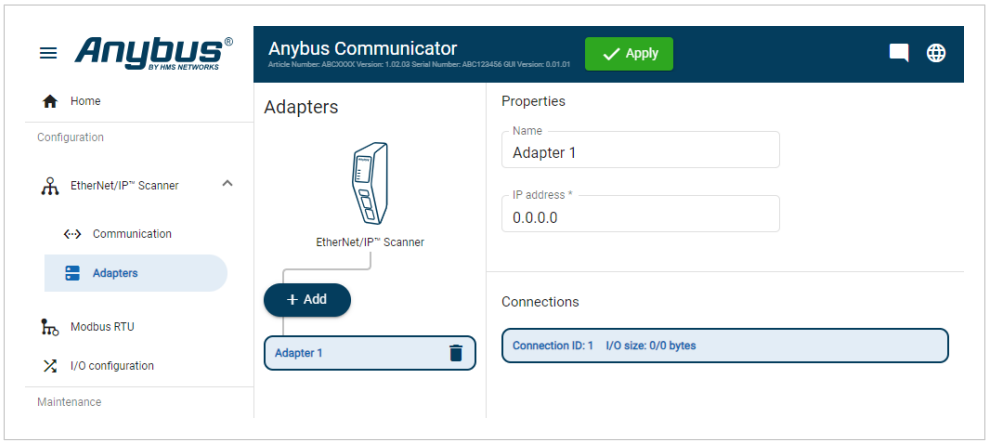


Figure 24. EtherNet/IP™ Scanner, Adapter page

3. Repeat until you have added all your adapters.

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

To Do Next

Configure the Connection settings, see Adapter Connection Settings (page 46).

8.6.4. Add Adapter from EDS File

You can use an eds file to import a preconfigured adapter type.

Before You Begin

> **NOTE**
> The maximum number of Adapters that can be added is 32.

Procedure

3. In the web-interface left sidebar menu, click **Adapters**.
4. In the **Add** split button drop-down menu, select **Add adapter from EDS file**.

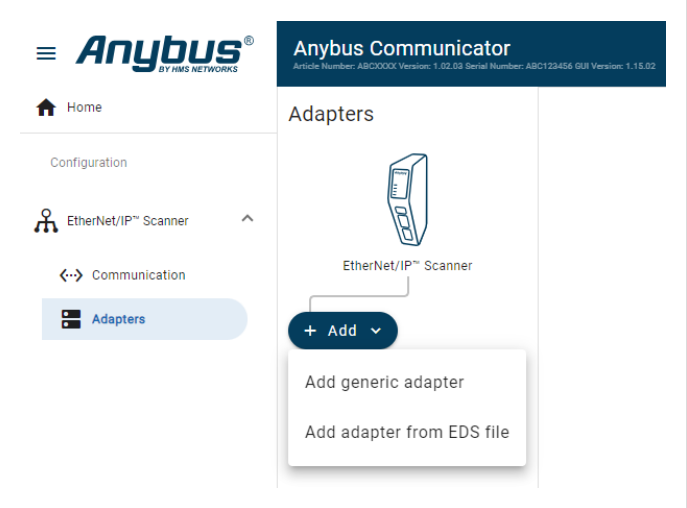


Figure 25. Add adapter from EDS file

5. In the **Open** dialog box, browse to and select the *.eds* file and click **Open**.
6. To import the *.eds* file, click **Import**.

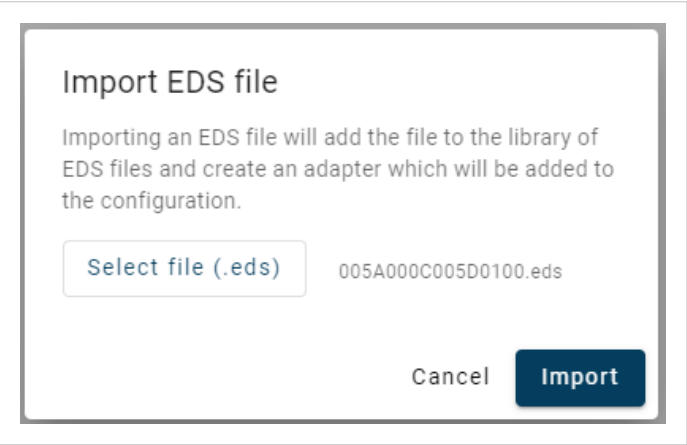


Figure 26. Example, selected .eds file

Import Messages

Import Success

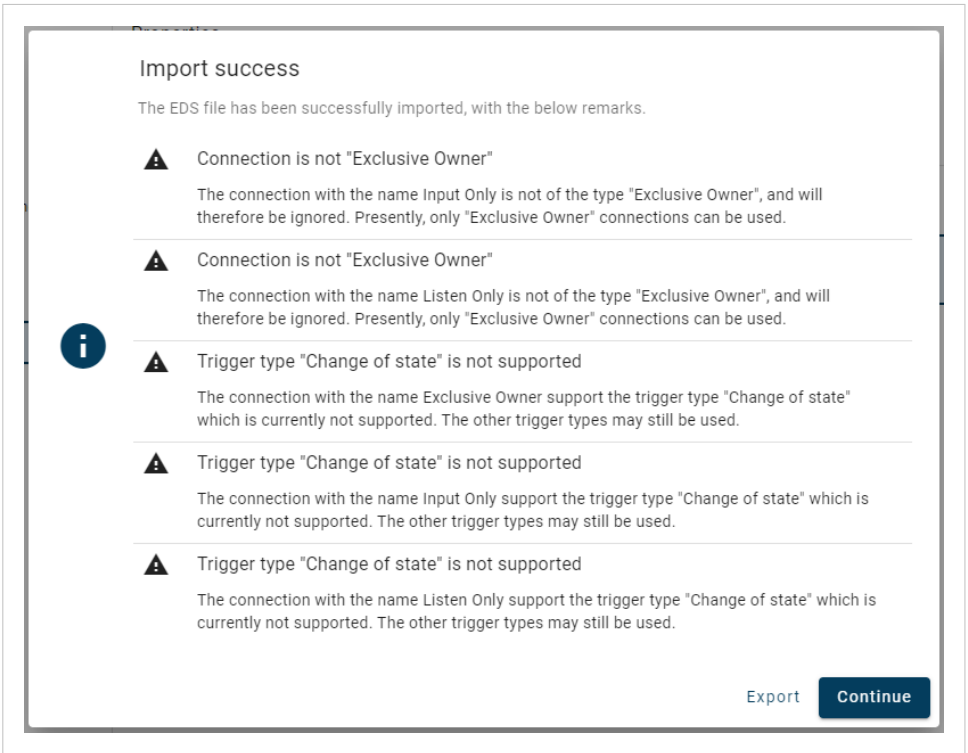


Figure 27. Example, list with remarks about the import

If the import succeeds but there are remarks, an **Import success** window appears.

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

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

To close the **Import success** window, click **Continue**.

Import Failed

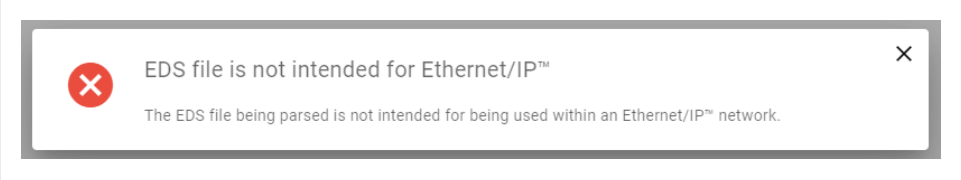


Figure 28. Example, error message related to EDS file import

If the EDS file is not supported, the import process is aborted and an error message appears.

Result

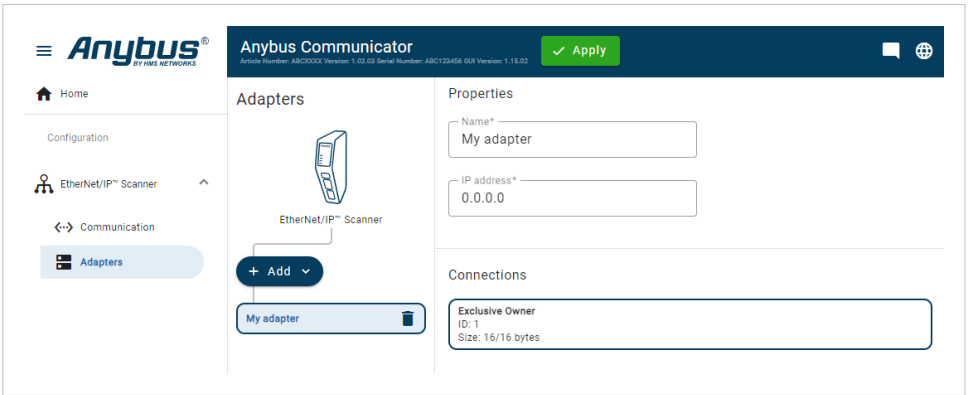


Figure 29. Example, imported adapter

The imported Adapter with Connection is added to the **EtherNet/IP™ Scanner** adapter list.

Figure 30. Example, imported adapter typ added to the Add split button drop-down menu

The imported adapter types is also added to the **Add** split button drop-down menu.

Use this menu option to add additional adapters of this type.

To Do Next

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

Configure the Connection settings, see Adapter Connection Settings (page 46).

8.6.5. Adapter Connection Settings

Before You Begin

NOTE
The connection type is Point-to-Point.

The adapter connection settings must be configured as defined in the adapter EDS (Electronic Data Sheet) for the adapter user documentation. Ensure you have the information about the adapter available.

Procedure

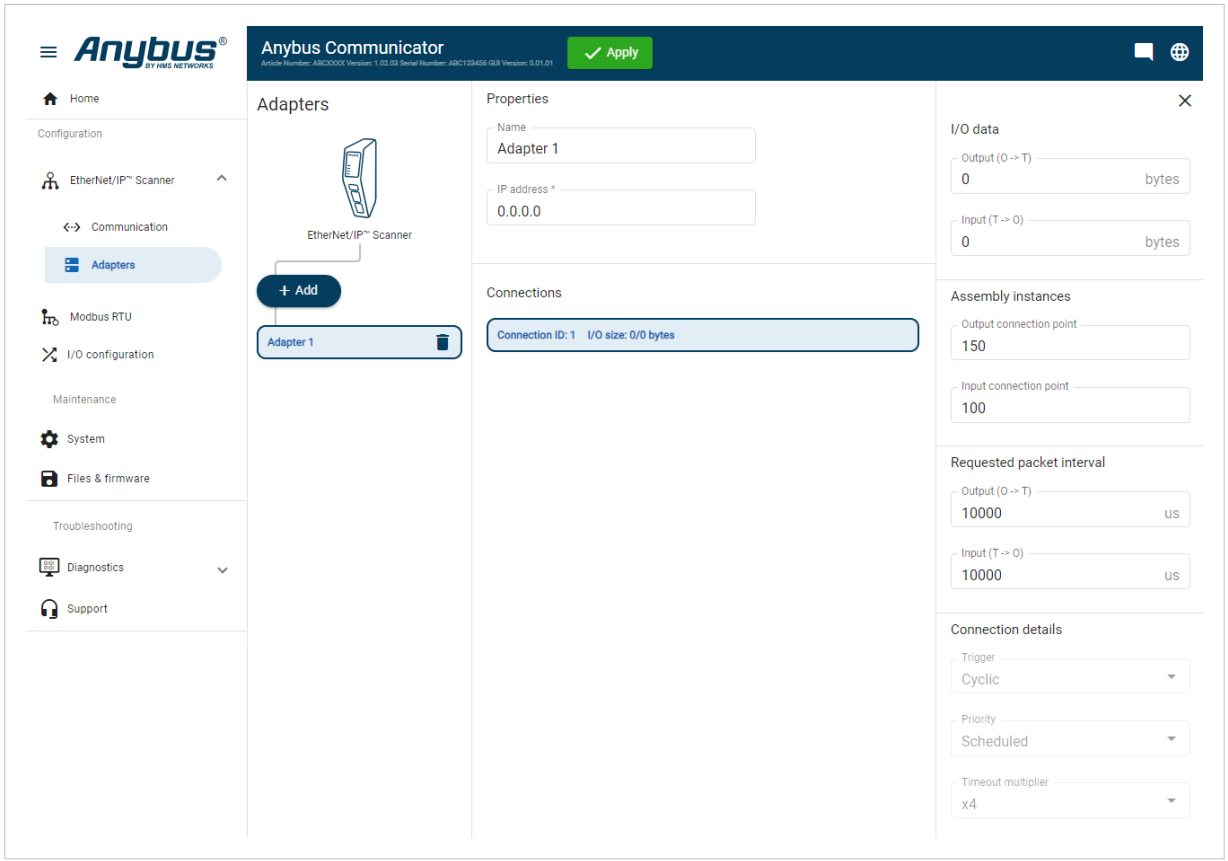


Figure 31. Adapter page, Connections settings

1. In the **EtherNet/IP™ Scanner** adapter list, select an adapter to configure.
2. In the **Properties** pane, enter:
   - **Name**: You can name the adapter to make it easier to identify.
   - **IP address**: Enter the IP address used to access the adapter.
3. Select the **Connection**.

4. In the connection menu, configure the **Connection** settings as defined in the adapter device EDS (Electronic Data Sheet) file.

Table 1. Adapter Connection settings

Setting	Value	Description
I/O Data	Output (O -> T) Default 0 bytes 0-505 bytes	Enter the data size to be transferred from the Originator (scanner) to the Target (adapter).
	Output (T -> O) Default 0 bytes 0-509 bytes	Enter the data size to be transferred from the Target (adapter) to the Originator (scanner).
Assembly instances	Output connection point Default 150 0-255	Enter the output connection point assembly number to be use when data is transferred from the Originator (scanner) to the Target (adapter).
	Input connection point Default 100 0-255	Enter the input connection point assembly number to be use when data is transferred from the Target (adapter) to the Originator (scanner).
Requested packet interval	Output (O -> T) Default 10 ms 1-3200 ms	Enter Requested Packet Interval (RPI) value, in milliseconds (ms), for the connection. The amount of time between updates of data sent from the Originator (scanner) to the Target (adapter).
	Input (T -> O) Default 10 ms 1-3200 ms	Enter Requested Packet Interval (RPI) value, in milliseconds (ms), for the connection. The amount of time between updates of data sent from the Target (adapter) to the Originator (scanner).
Connection details	Trigger **Change Of State** or **Application Triggered**	From the **Trigger** drop-down menu, select the transport type for the exchange of data on the connections: • **Change Of State** • **Application Triggered**
	Priority Default **Scheduled**	From the **Priority** drop-down menu, select the priority of the connection: • **Low priority** • **High priority** • **Scheduled** • **Urgent**
	Timeout multiplier Default **x4** **x4**, **x8**, **x16**, **x32**, **x64**, **x128**, **x256**, **x512** or **Reserved**	From the **Timeout multiplier** drop-down menu, select the multiplier to apply to the RPI value, to obtain the connection timeout value: **x4**, **x8**, **x16**, **x32**, **x64**, **x128**, **x256**, **x512**.

5. To apply the settings, click **Apply** in the web-interface header, and follow the instructions.
6. Repeat until you have configured the connections for all your adapters.

8.7. Modbus RTU Settings

8.7.1. Communication Settings

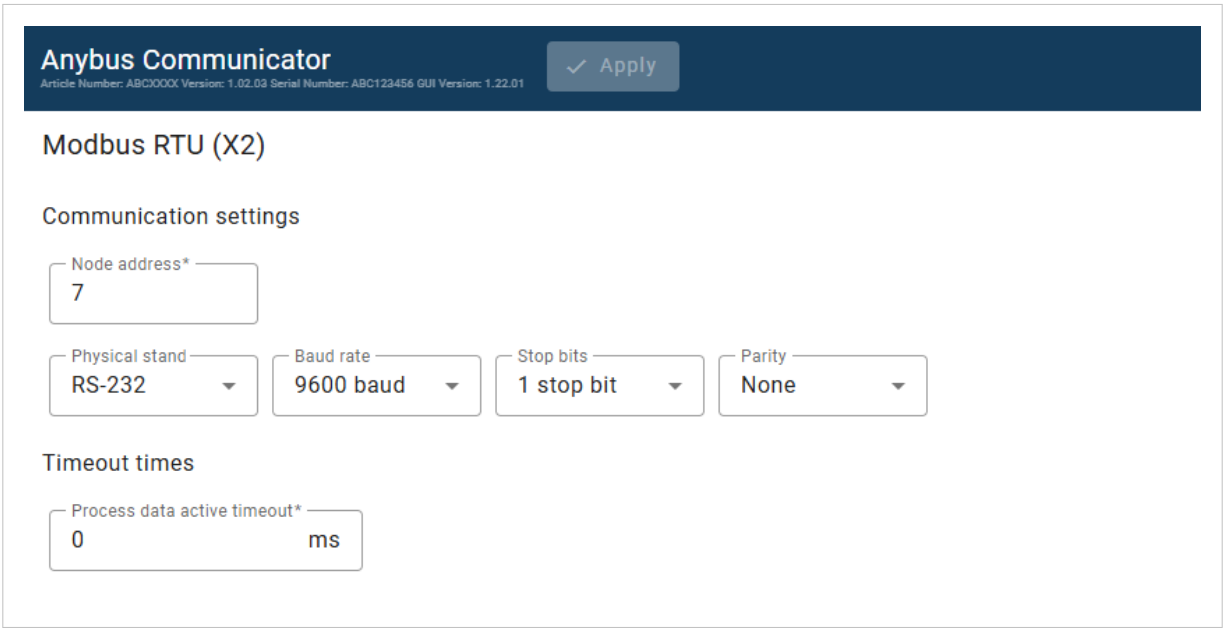


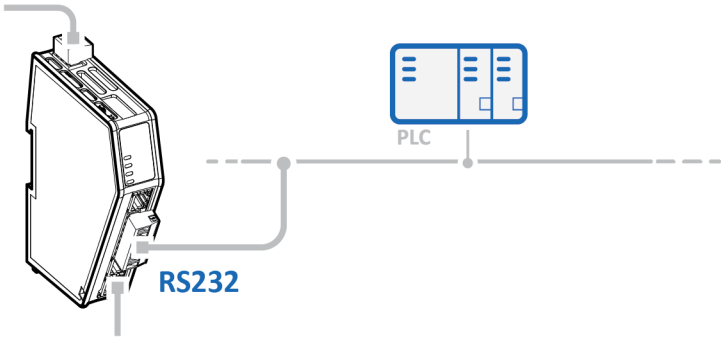
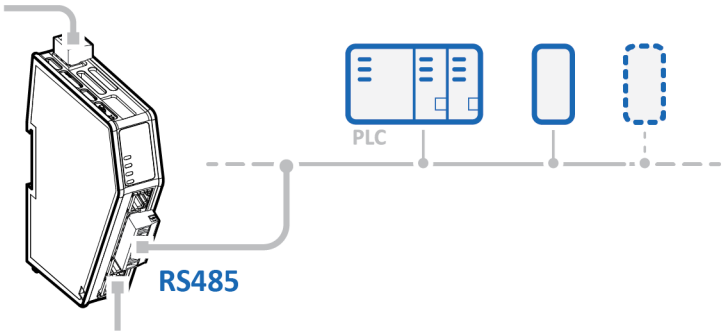
Figure 32. Communication, Basic settings

Node Address
Enter the **Node address** for the Modbus RTU server connected to the Communicator.

Physical Standard

Specify the physical interface type for the Modbus RTU network.

Select a physical standard from the **Physical standard** drop-down menu.

Setting	Value	Description
Physical standard	RS-232, Default standard	Use RS-232 when one single device is connected to the network. 
	RS-485	Use RS-485 when multiple devices are connected to the network. 

Baud Rate

Specify the baud rate; the serial transfer speed, maximum bits per second.

Select a baud rate value from the **Baud rate** drop-down menu.

Setting	Value
Baud rate	1200 baud
	1800 baud
	2400 baud
	4800 baud
	9600 baud, Default value
	19200 baud
	35700 baud
	38400 baud
	57600 baud
	115200 baud
	128000 baud

Data Bits
Data bits is the number of bits used in the data representation of characters in the telegrams.

The rate for Modbus RTU is 7 data bits or 8 data bits. The default setting is 8 data bits.

Stop Bits
Specify the number of stop bits used to indicate the end of data transmission.

Select a stop bits value from the **Stop bits** drop-down menu.

Setting	Value
Stop bits	1 stop bit, Default value
	2 stop bit

Parity
Specify if parity should be used to detect errors in the data.

Select parity value from the **Parity** drop-down menu.

Setting	Value	Description
Parity	None, Default value	No parity checking Parity bit is not transmitted
	Odd	Odd parity checking
	Even	Even parity checking

Timeout Times

Process Data Active Timeout
To enable **Process data active timeout**, enter a value between 1 and 65535 milliseconds (ms).

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

The data sent to the network is frozen.

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

The default value is 0 ms.

8.8. Modbus RTU Advanced Settings

8.8.1. Legacy Mode for Anybus Address Mode | Modbus RTU

Advanced settings option for Modbus RTU Server.

About Legacy Mode

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

See also Legacy Address Mode I/O Data Mapping (page 66).

To Use Legacy Mode

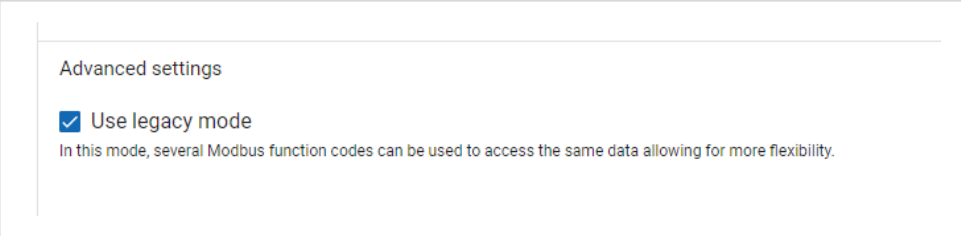


Figure 33. Advanced settings > Use legacy mode

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

8.9. I/O Configuration

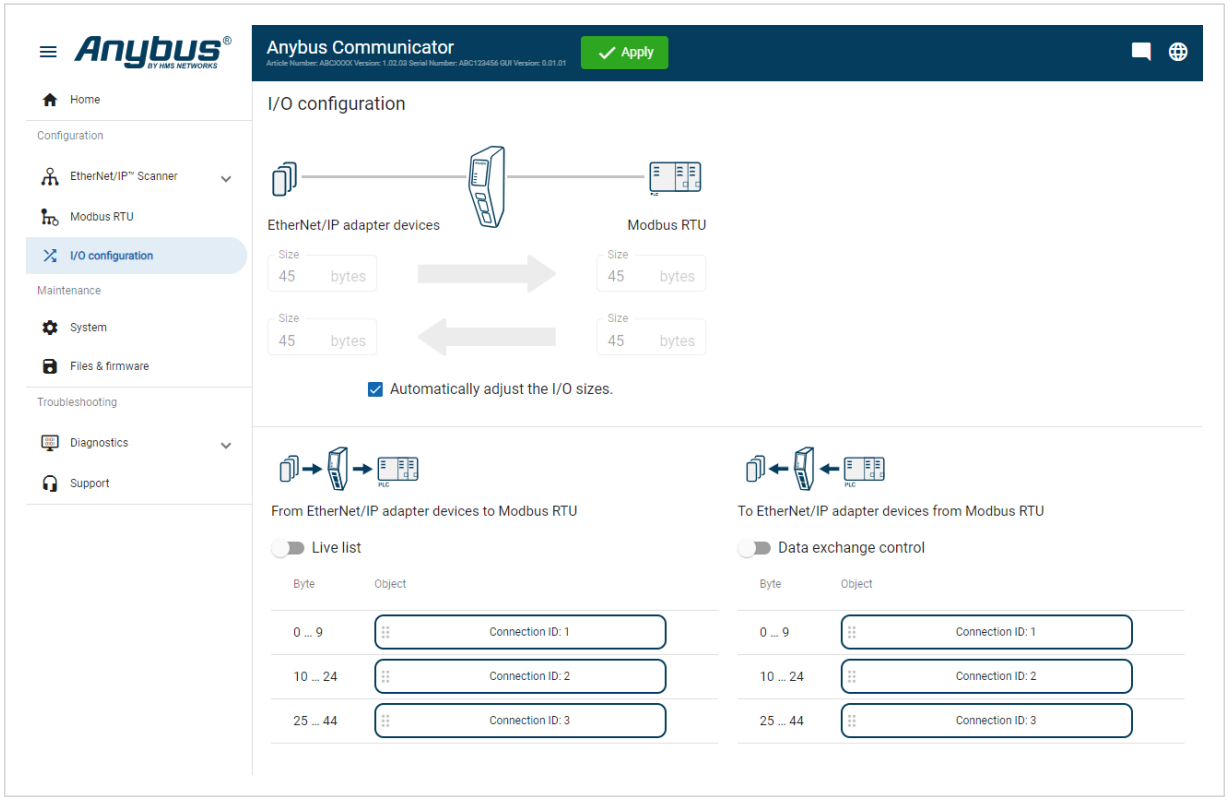


Figure 34. **I/O configuration** page

On the **I/O configuration** page the data communication between the EtherNet/IP adapter devices and the Modbus RTU network is mapped.

The allocated I/O area is auto generated based on the **EtherNet/IP adapter devices** network adapter(s) configuration and how the settings on the **Modbus RTU** page are configured.

There are two areas: **From EtherNet/IP adapter devices to Modbus RTU** and **To EtherNet/IP adapter devices from Modbus RTU**.

I/O Size Settings

By default, the Communicator is set to use the same I/O sizes for both the Modbus RTU network and the EtherNet/IP adapter devices.

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

8.9.1. Map Area Object Order

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

Objects can not share the same I/O area.

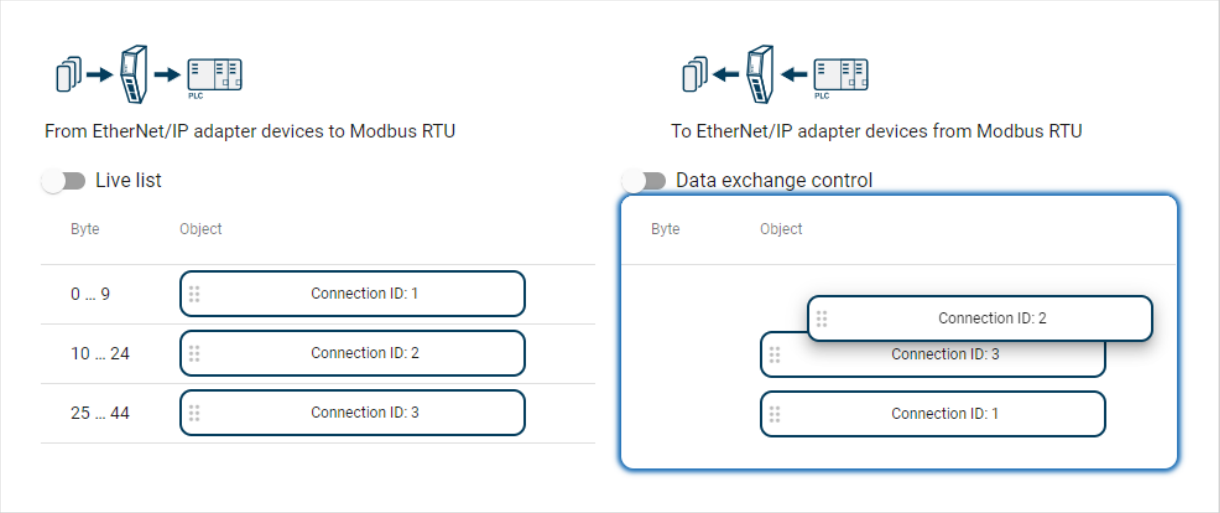


Figure 35. I/O configuration, change the order of objects

8.9.2. Endian Swap

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

About Endianness

Big-endian (BE)

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

Little-endian (LE)

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

8.9.3. Convert Between Big-Endian and Little-Endian

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

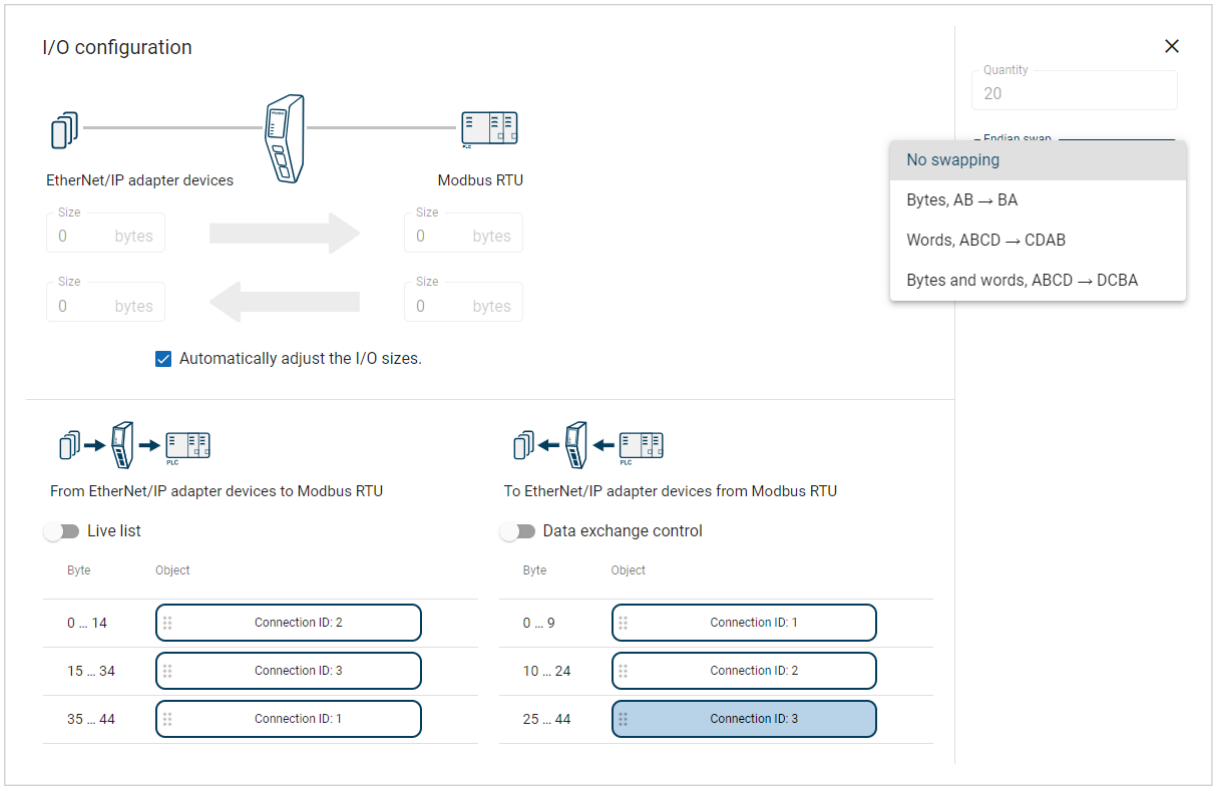


Figure 36. **I/O configuration** page, Endian swap

To reverse the byte order:

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

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

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

8.9.4. Live List

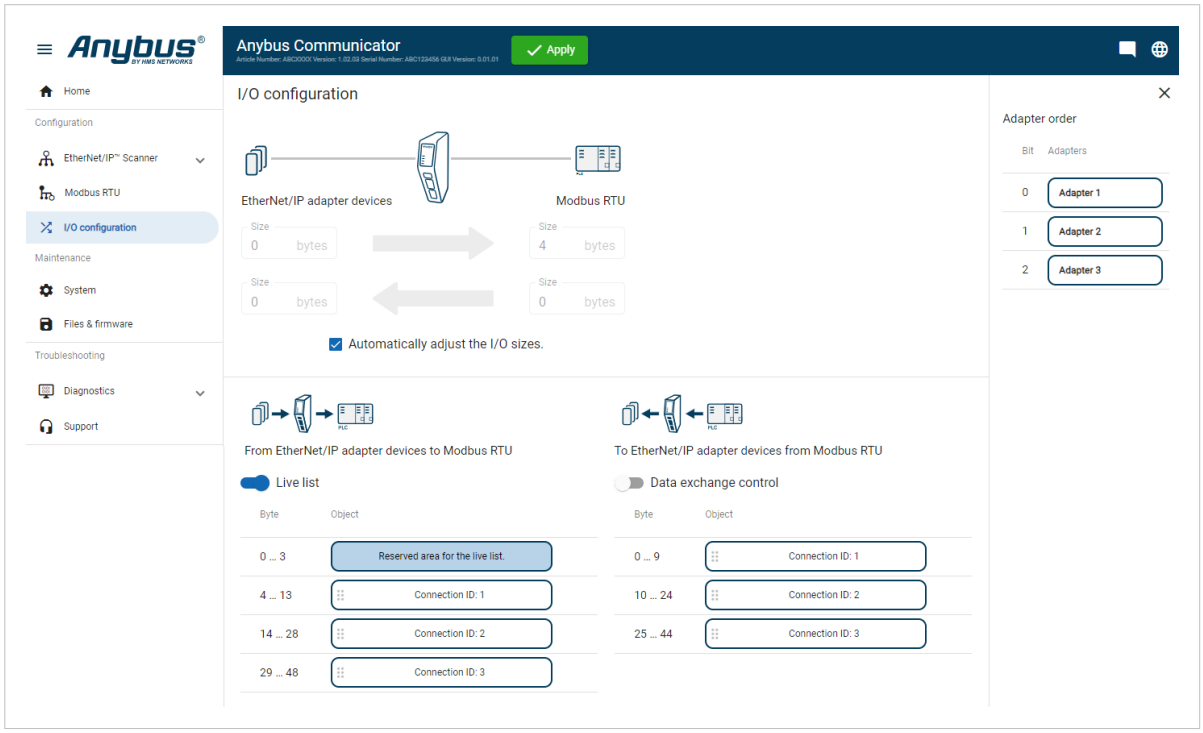


Figure 37. I/O configuration page, Live list enabled

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

About the Live List

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

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

8.9.5. Data Exchange Control

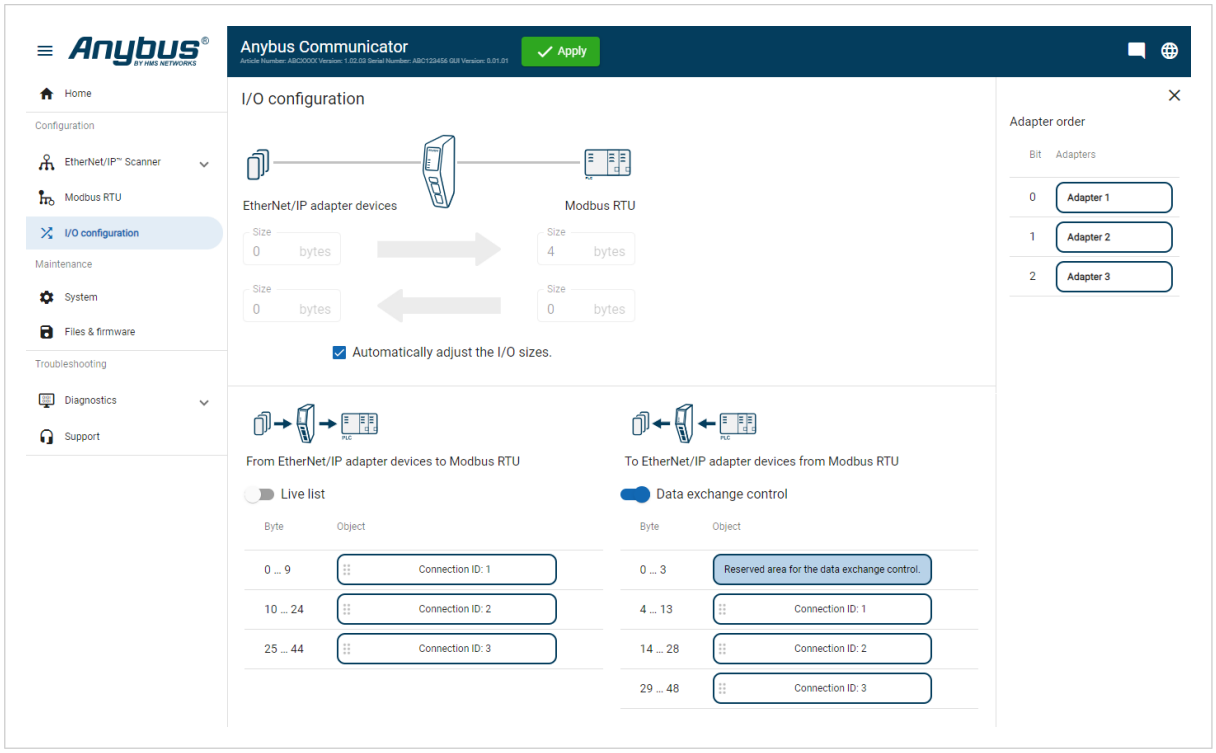


Figure 38. I/O configuration, **Data exchange control** enabled

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

When **Data exchange control** is enabled, the first four bytes of process data on the Modbus RTU 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 connection on the subnetwork.

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

When data exchange is enabled for the corresponding connection, the control bit is 1.

8.10. Configuration Notes

You can add notes to describe the Communicator configuration.

8.10.1. Add Configuration Note

Procedure

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

Figure 39. Configuration note, comment icon

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

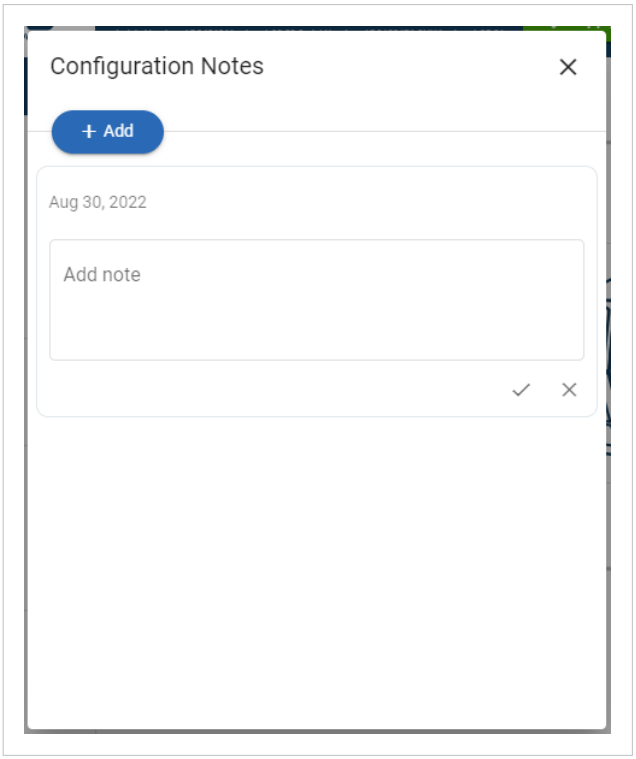


Figure 40. Add new configuration note

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

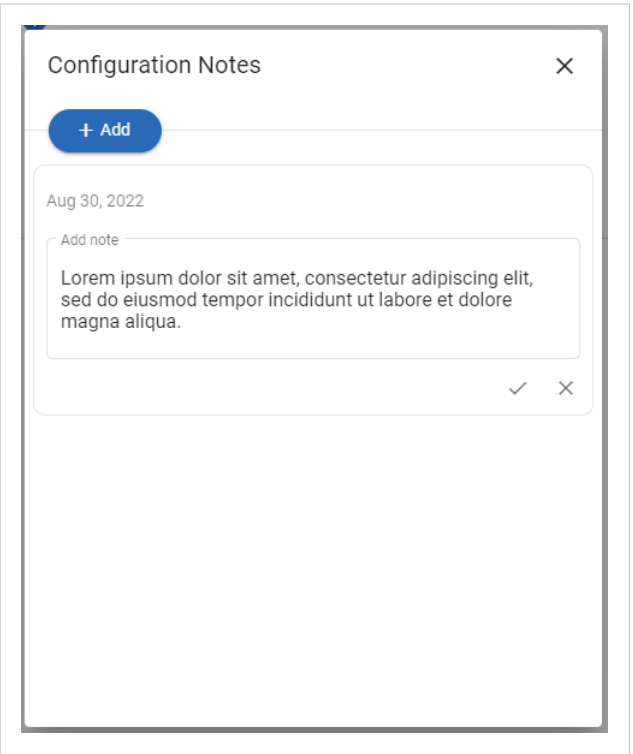


Figure 41. Write a configuration note

The configuration note is added to the list.

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

8.10.2. View and Edit Configuration Notes

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

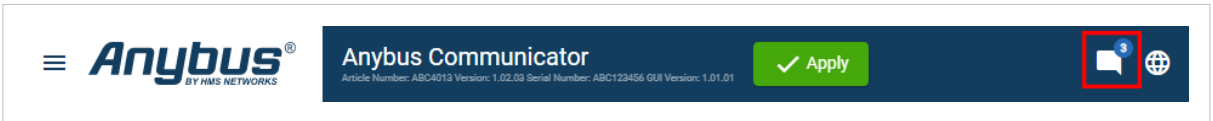


Figure 42. Example: The comment icon indicates that there are three added notes

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

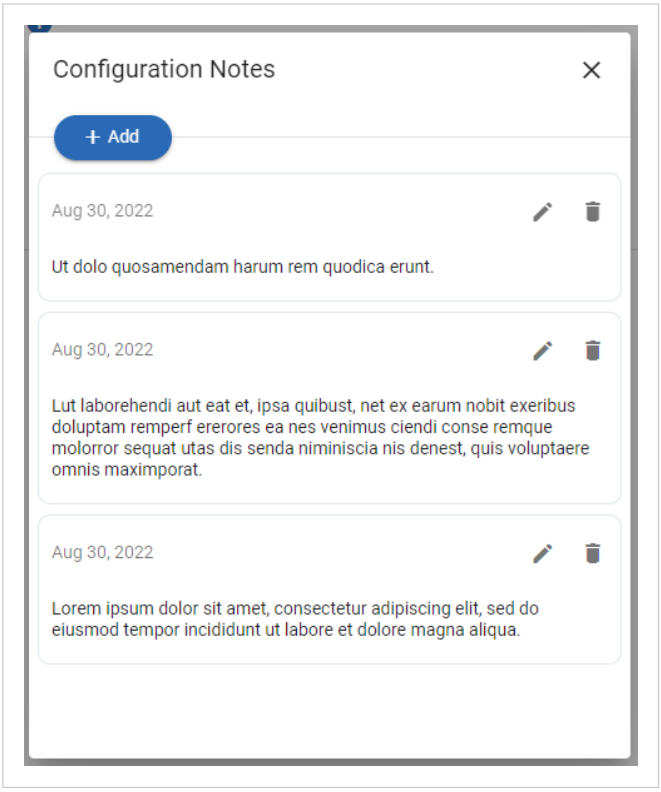


Figure 43. Example: The Configuration Notes window with added notes

8.11. Apply Configuration

Before You Begin

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

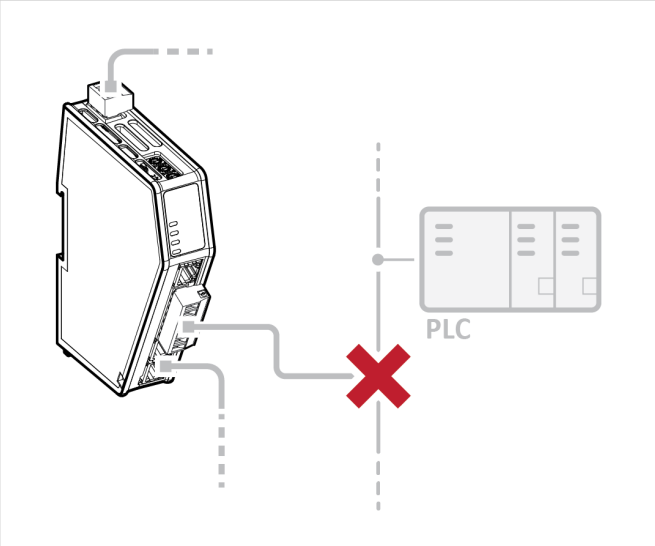


Figure 44.

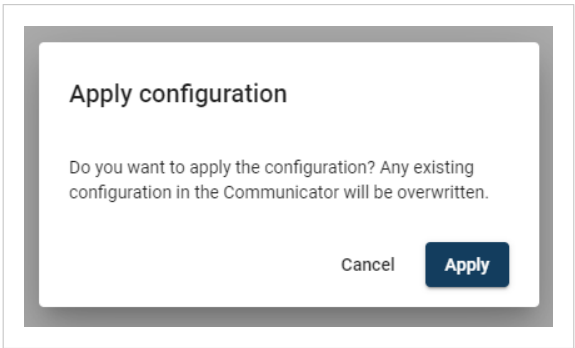
Before you can apply the configuration, ensure that there is no active communication on the Modbus RTU network where the Communicator is connected.

Procedure

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

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

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



8.12. To Use an Existing Configuration

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

Procedure

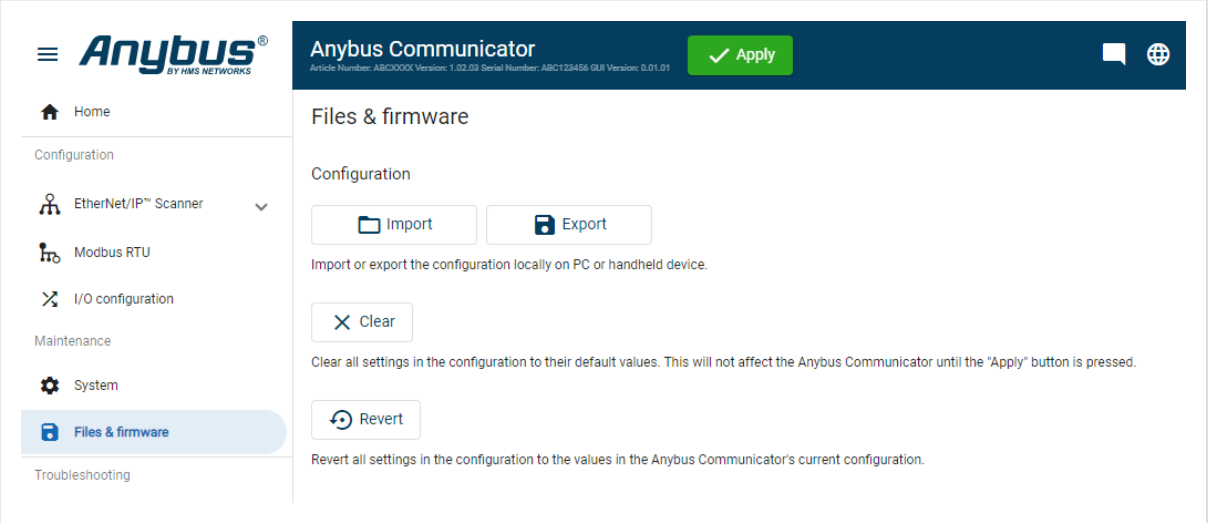


Figure 45. **Files & firmware** page

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.

9. PLC Configuration

9.1. PLC Device Security

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

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

9.2. Modbus Addressing and Register Mapping

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

9.2.1. The Difference Between Address and Register Start

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

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

Example 1. Modbus Function Code 0x04 Read Input Registers

Table 2. Modbus client values

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

Example 2. Modbus Function Code 0x03 Read Holding Registers

Table 3. Modbus client values

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

9.2.2. To Read and Write Data

To Read Data
To read data, you can use different Modbus Functions.

Discrete Inputs

- Modbus Function 0x02 Read Discrete Input Status

Discrete Input start at address 0.

Input Registers

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

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

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

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

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

To Write Data
To write data, you can use different Modbus Functions.

Coils

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

Coils starts at address 0.

Holding Registers

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

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

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

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

Data Encoding

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

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

Example 3. Big-Endian Data Encoding

For a 16-bit register value of 0x1234:

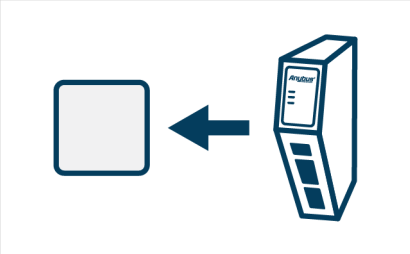
- The first byte sent is 0x12.
- The second byte sent is 0x34.

See also Convert Between Big-Endian and Little-Endian (page 54).

9.2.3. Default Address Mode I/O Data Mapping

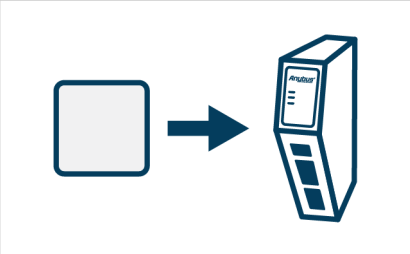
The following Modbus function codes are compatible with the default addressing mode.

Input Data to Client/Server - Data to Modbus



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

Output Data From Client/Server - Data From Modbus TCP

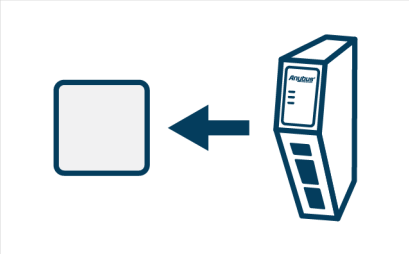


Process I/O data offset		Coil address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x0000 - 0x000F	0 - 15	0x0000	0
0x0002 - 0x0003	2 - 3	0x0010 - 0x001F	16 - 31	0x0001	1
...	...	...	...	...	...
0x05D8 - 0x05D9	1496 - 1497	0x2EC0 - 0x2ECF	11968 - 11983	0x02EC	748
0x05DA - 0x05DB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

9.2.4. Legacy Address Mode I/O Data Mapping

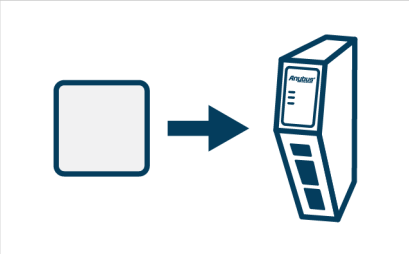
The following Modbus function codes are compatible with the Modbus **Use legacy mode** setting.

Input Data to Client/Server - Data to Modbus



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

Output Data From Client/Server - Data From Modbus



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

10. Verify Operation

Before You Begin

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

See Installation (page 14).

10.1. Communicator Status Monitor

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

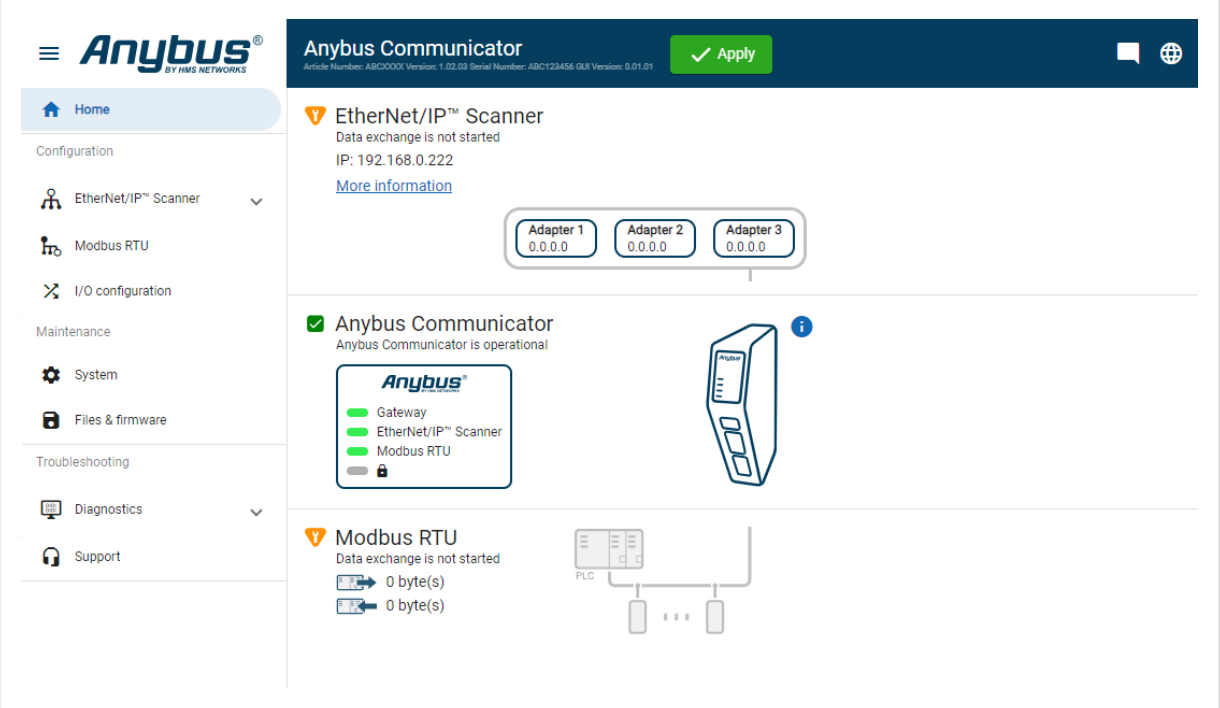


Figure 46. Home page

Gateway Status

Overview the Communicator LED indications remotely.

Refer to Communicator LED Indicators (page 69).

Adapter Status

Overview the status for each adapter 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.

10.2. Communicator LED Indicators

This topic applies to different product variants for different networks.

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

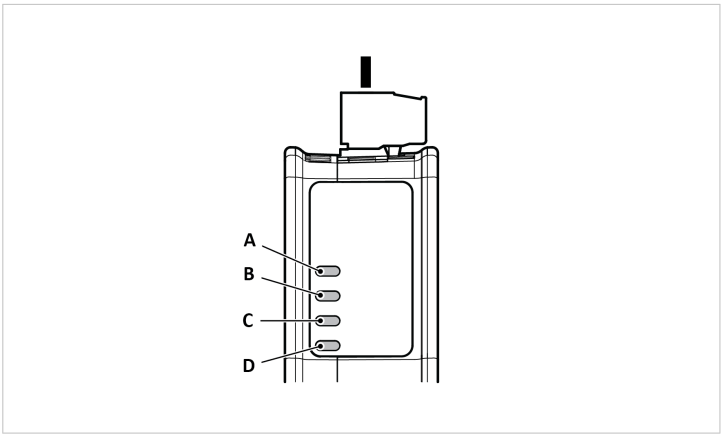


Figure 47. Gateway status (A), Network connection (B)/(C) and Security switch (D)

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

Connection to client device

- **LED B for product: ABC3313 PROFINET**
- **LED C for product: ABC3300 PROFIBUS, ABC3361 EtherCAT, ABC3328 Modbus TCP**

Operation status	Modbus TCP	EtherCAT	PROFIBUS	PROFINET	Modbus RTU
Off	No power/No IP address.	No power	No power/No data exchange.	No power/No connection with IO controller.	No power, no active nodes, or all nodes are stopped.
Green, solid	At least one Modbus TCP message received.	EtherCAT on.	Operate, data exchange.	Connection with IO controller established, IO controller in Run state.	At least one Modbus message received.
Green, one flash	N/A			Connection with IO controller established, IO controller in STOP state or IO data is inaccurate.	N/A
Green, flashing	Modbus TCP online, no messages received.	EtherCAT online, no connections established.	Clear, data exchange.	Used by engineering tools to identify the node on the network.	Waiting for first Modbus message.
Red, solid	IP address conflict detected.	Fatal event			
Red, one flash	N/A	Unsolicited state change SubDevice application has	Parameterization error.	Station name not set.	N/A

Connection to client device • LED B for product: ABC3313 PROFINET • LED C for product: ABC3300 PROFIBUS, ABC3361 EtherCAT, ABC3328 Modbus TCP					
Operation status	**Modbus TCP**	**EtherCAT**	**PROFIBUS**	**PROFINET**	**Modbus RTU**
		changed the EtherCAT state autonomously.			
Red, two flash	N/A	Sync Manager watchdog timeout.	Configuration error.	IP address not set.	N/A
Red, three flash	N/A			Expected Identification differs from Real Identification.	N/A
Red, flashing	Connection timeout.	Invalid configuration.	N/A		Connection timeout. No Modbus messages has been received within the configured process active timeout time.

Connect to EtherNet/IP Scanner device • LED C for product: ABC3313 PROFINET • LED B for product: ABC3300 PROFIBUS, ABC3361 EtherCAT, ABC3328 Modbus TCP	
Operation status	**Description**
Off	No IP address.
Red, solid	IP address conflict.
Green, flashing	No connections established.
Green, solid	One or more connections established.

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

Fatal Error and Exception Error

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

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

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

10.3. Ethernet LED Indicators

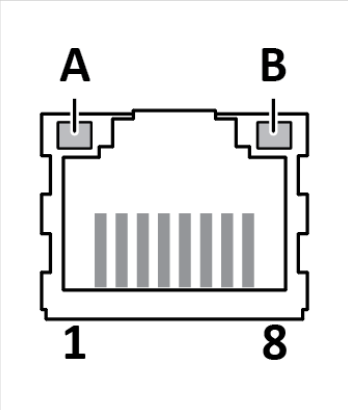


Figure 48. LED A. Activity LED B. Not used

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

LED B	Function
Off	Not used

11. Maintenance

11.1. Action on Fatal Error

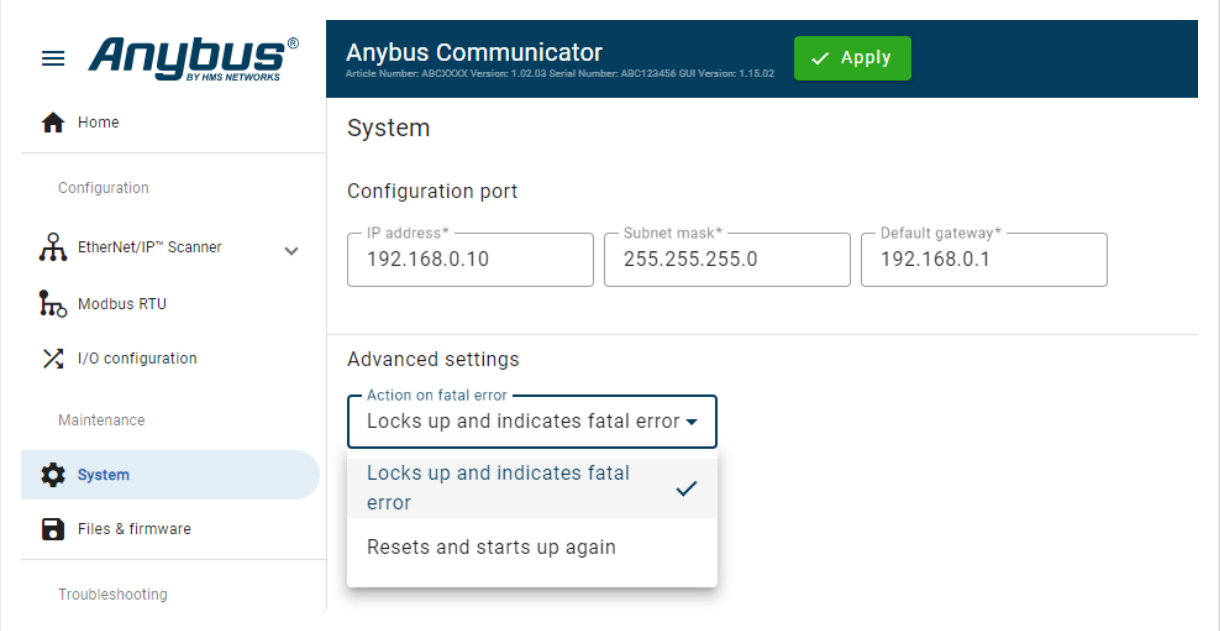


Figure 49. System page, Action on fatal error menu

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

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

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

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

11.2. Configuration Port IP Settings

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

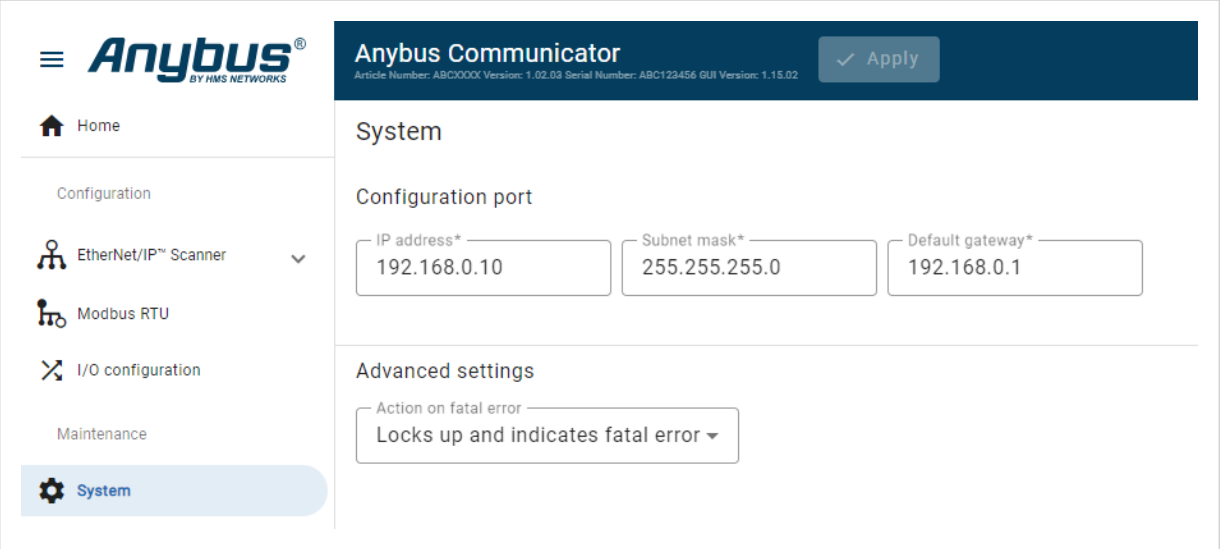


Figure 50. System page, Configuration port settings

Default Configuration Port IP settings

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

11.3. Configuration File Handling

11.3.1. Export Configuration

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

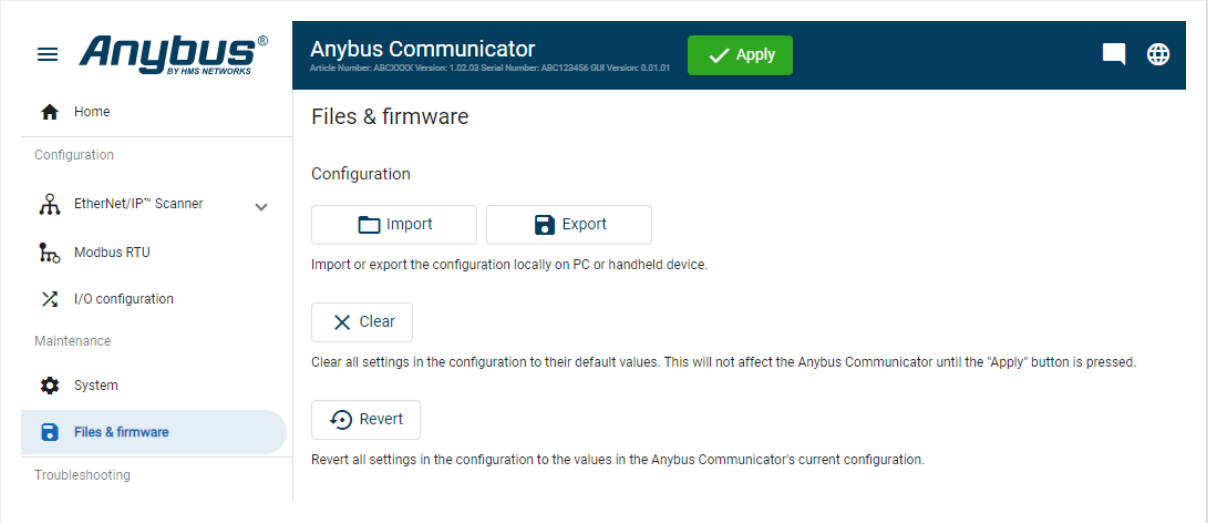


Figure 51. Files & firmware page

To export a configuration file:

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

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

11.3.2. Import Configuration

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

Before You Begin

The supported file format is .conf.

Procedure

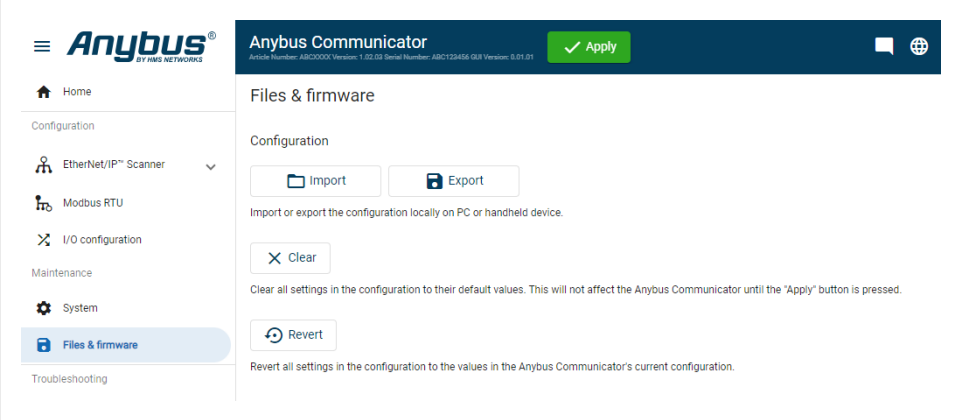


Figure 52. Files & firmware page

Import configuration file:

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

11.4. Clear and Revert Configuration

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

Procedure

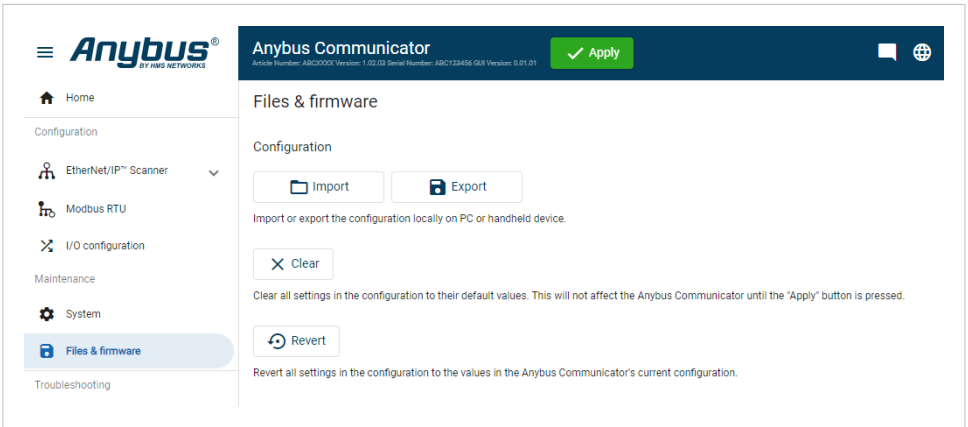


Figure 53. Files & firmware page

To Clear the Configuration

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

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

To Revert the Configuration

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

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

11.5. Firmware Management

11.5.1. View the Firmware Version

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

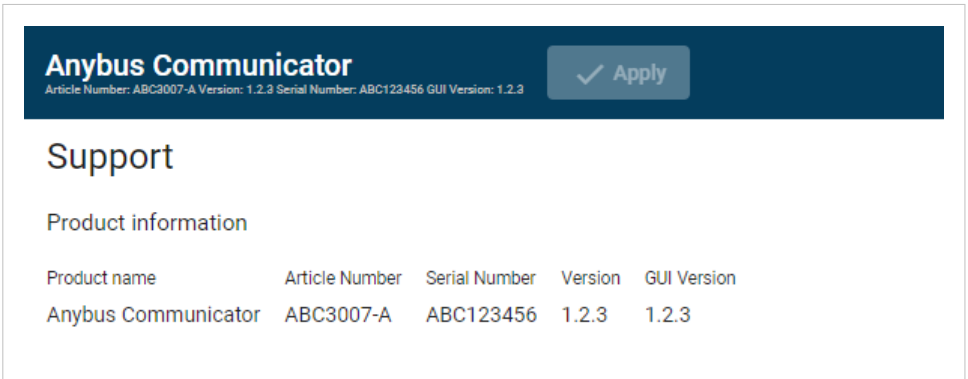


Figure 54. Support page, Product information example

11.5.2. Firmware and Configuration Compatibility

Compatibility after firmware upgrade

Current configuration is still compatible after upgrading the firmware.

Compatibility after firmware downgrade

IMPORTANT

Compatibility after a firmware downgrade cannot be guaranteed.

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

11.5.3. Firmware File Validation

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

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

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

11.5.4. Update Firmware

Before You Begin

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

Ensure to disconnect the Communicator from the OT networks.

Procedure

Figure 55. Files & firmware page

To update the firmware:

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

Result

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

11.6. Change Language

Default language is **English**.

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

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

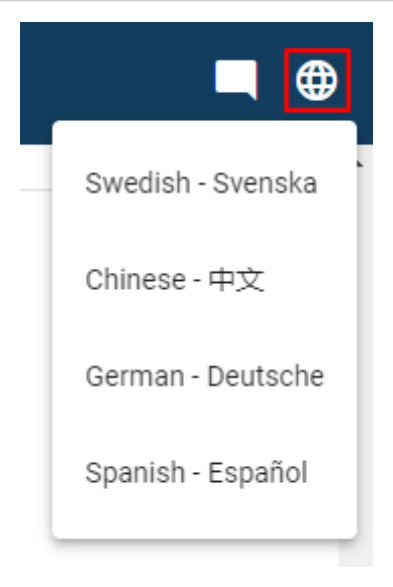


Figure 56. Language menu

2. Select a new language from the list.

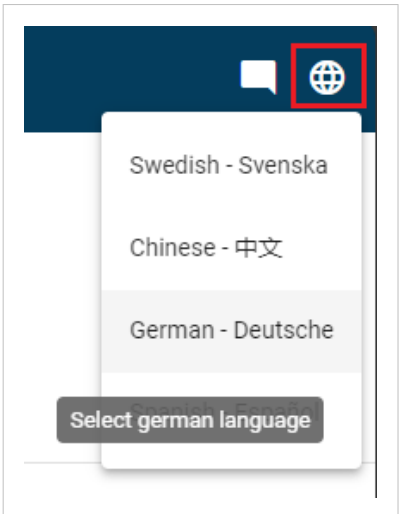


Figure 57. Example: Change language to German

The language change takes effect immediately.

12. Troubleshooting

12.1. Diagnostics

12.1.1. I/O Data

On the **Diagnostics**, **I/O data** page you can monitor how the data flow between the **EtherNet/IP Scanner** side and the **Modbus RTU** side, including any configured endian conversions.

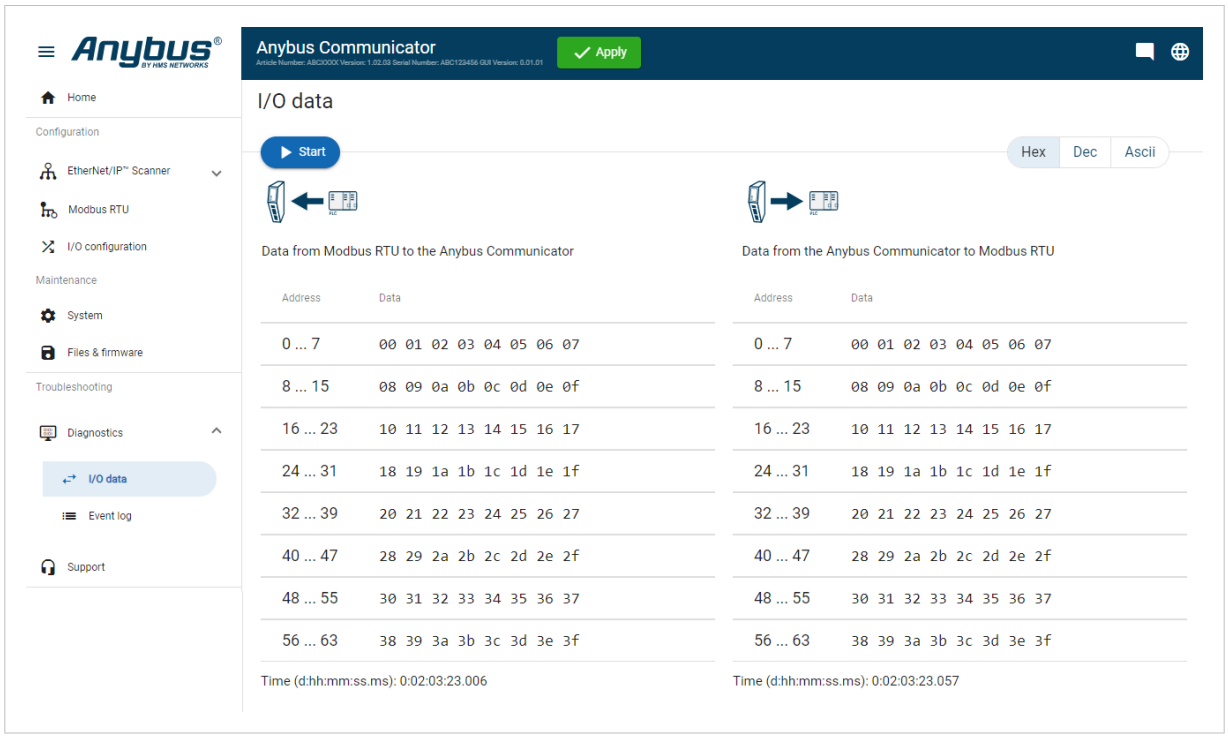


Figure 58. I/O data

I/O data is updated twice every second.

Select how data is displayed

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

Start and Stop Data flow

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

12.1.2. Event Log

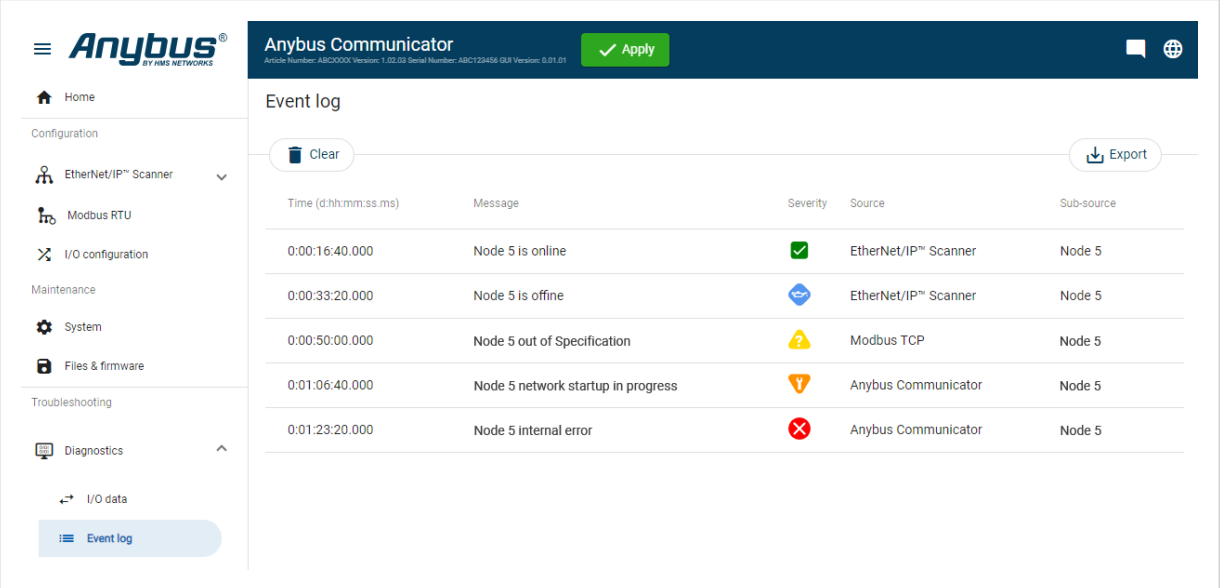


Figure 59. Event log page example

How To Analyze the Information

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

Time (d:hh:mm:ss.ms)	The duration from when the X-gateway was powered on until the event occurred.
Message	A brief description of the event.
Severity	The severity of the event occurred. For description of the symbols, see Communicator Status Monitor (page 67).
Source	Communicator
	Modbus RTU
	EtherNet/IP Scanner
Sub-source	The nodes connected to the subnetwork and the PLC connected to the high level network. If there is a problem with a node the node name is displayed in the Sub-source column. Example 4. Sub-source number If the node name is 5, number 5 is displayed in the Sub-source column.

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

12.1.3. LED Status

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

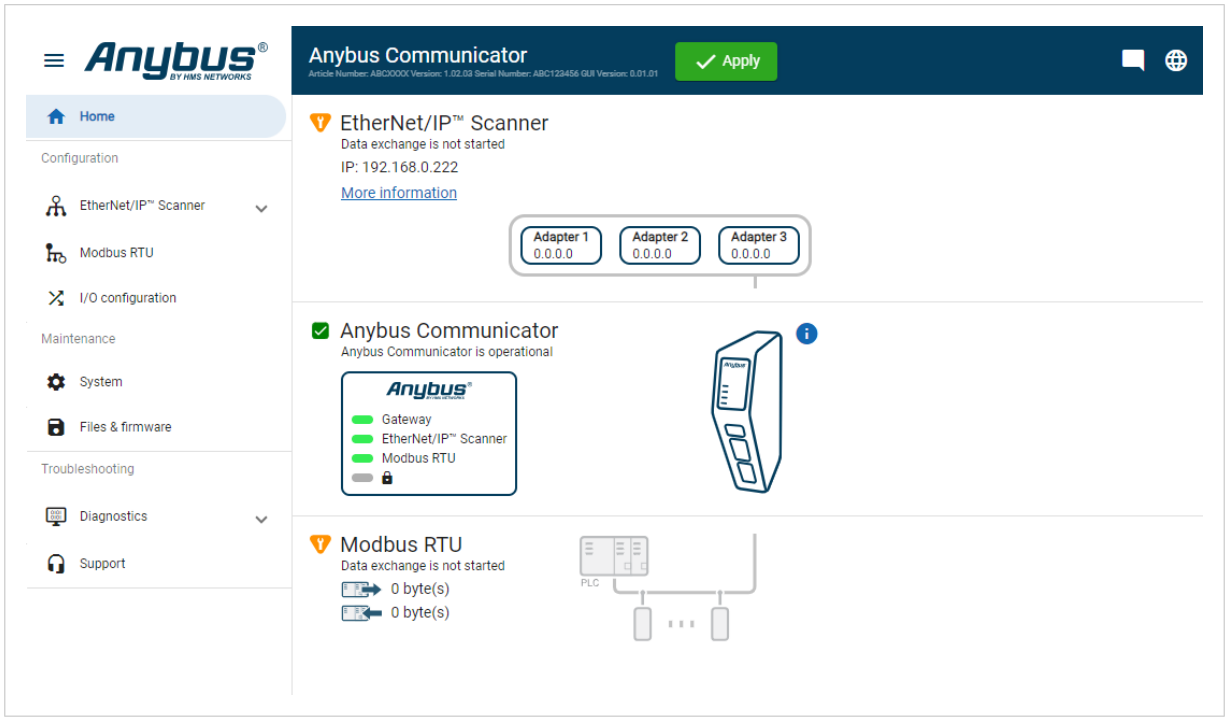


Figure 60. Home page

For information about the LED indication, see Communicator LED Indicators (page 69).

12.2. Reset to Factory Settings

Before You Begin

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

Procedure

To reset the Communicator:

1. Disconnect the Communicator from power.

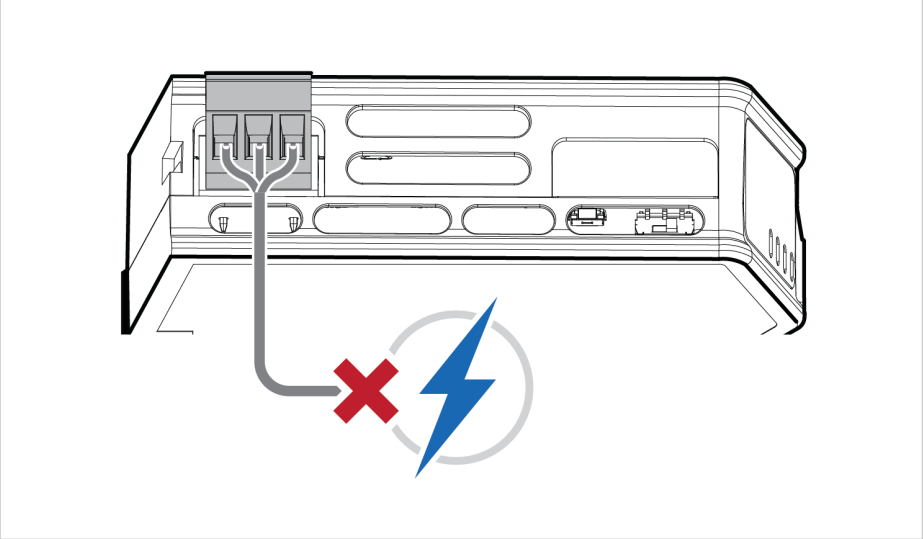


Figure 61. Disconnect power

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

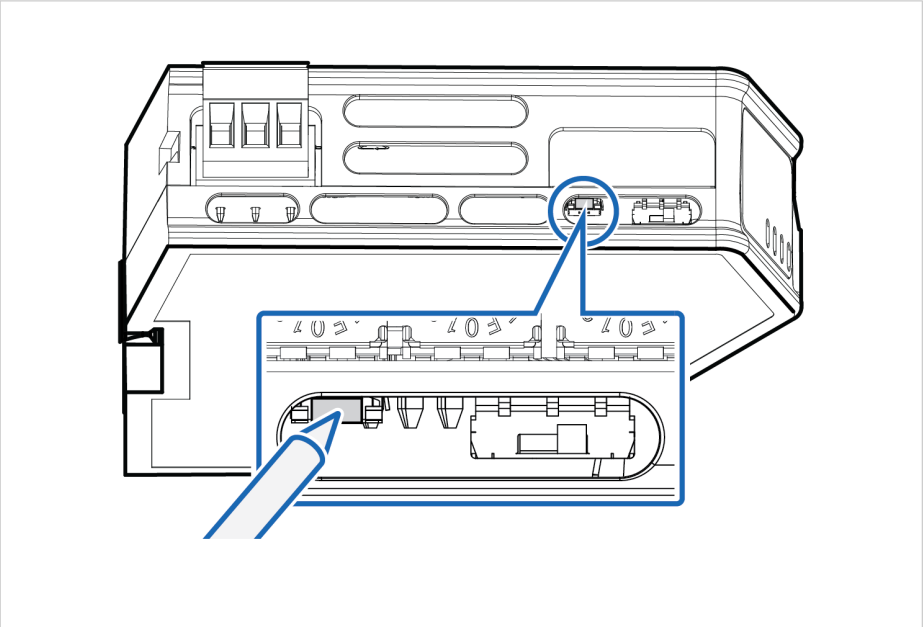


Figure 62. Press and hold **Reset** button

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

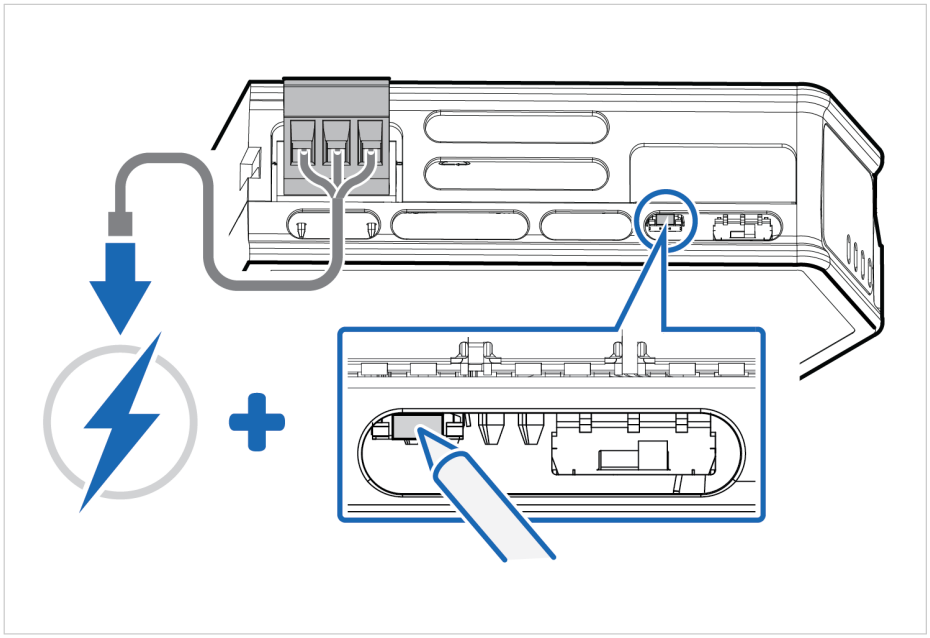


Figure 63. Hold **Reset** button and reconnect power

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

5. Reboot the Communicator.

Result

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**.

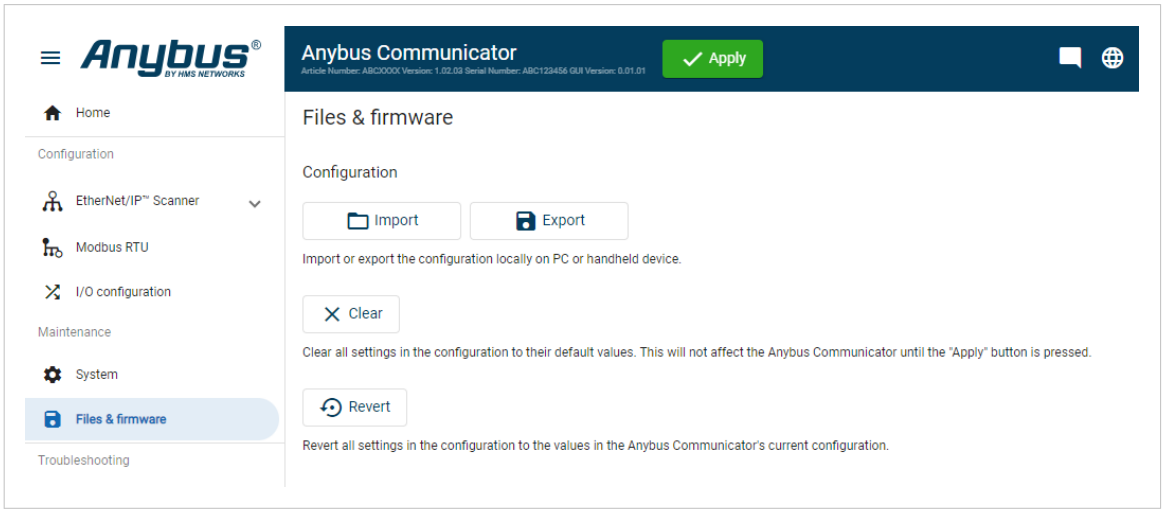


Figure 64. Files & firmware, Revert

12.3. Firmware Upgrade Error Management

Before You Begin

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

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

Procedure

To complete the interrupted firmware update:

1. Disconnect the Communicator from power.

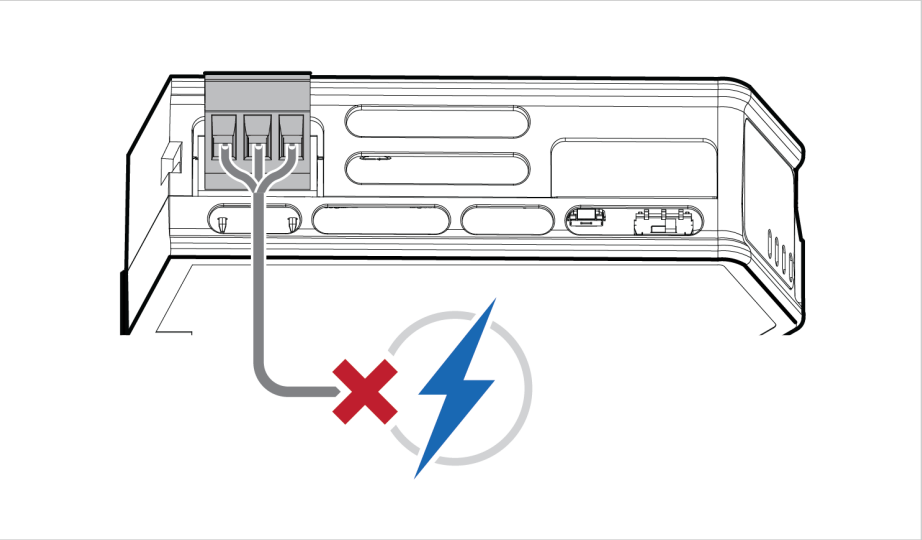


Figure 65. Disconnect power

2. Reconnect the Communicator to power.

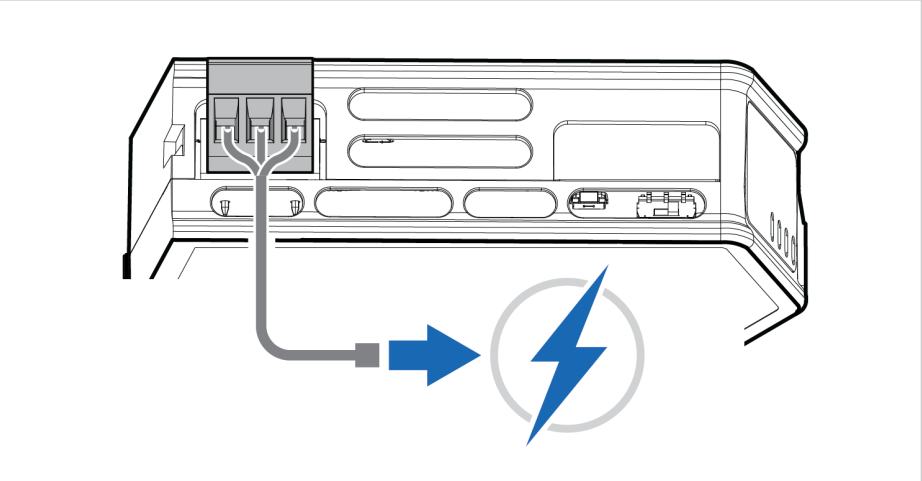


Figure 66. Reconnect power

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

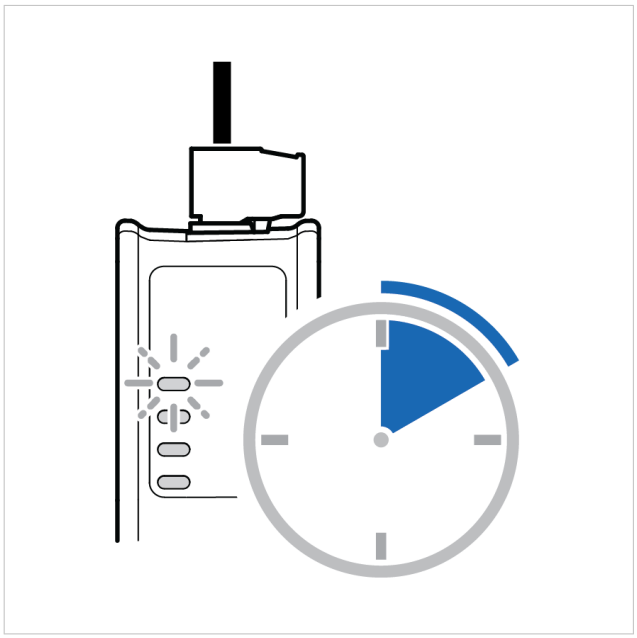


Figure 67. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

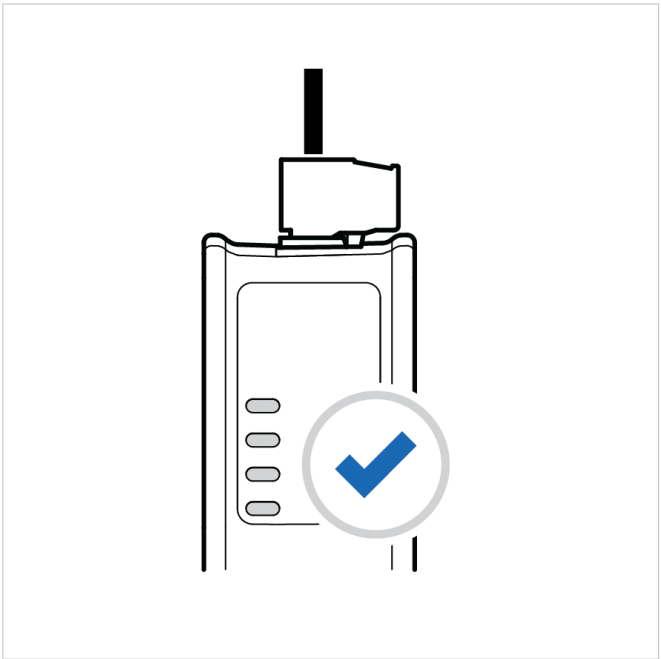


Figure 68. Recover and return to normal operation

To Do Next

To check LED status, refer to Communicator LED Indicators (page 69).

12.4. Support

12.4.1. Support Package

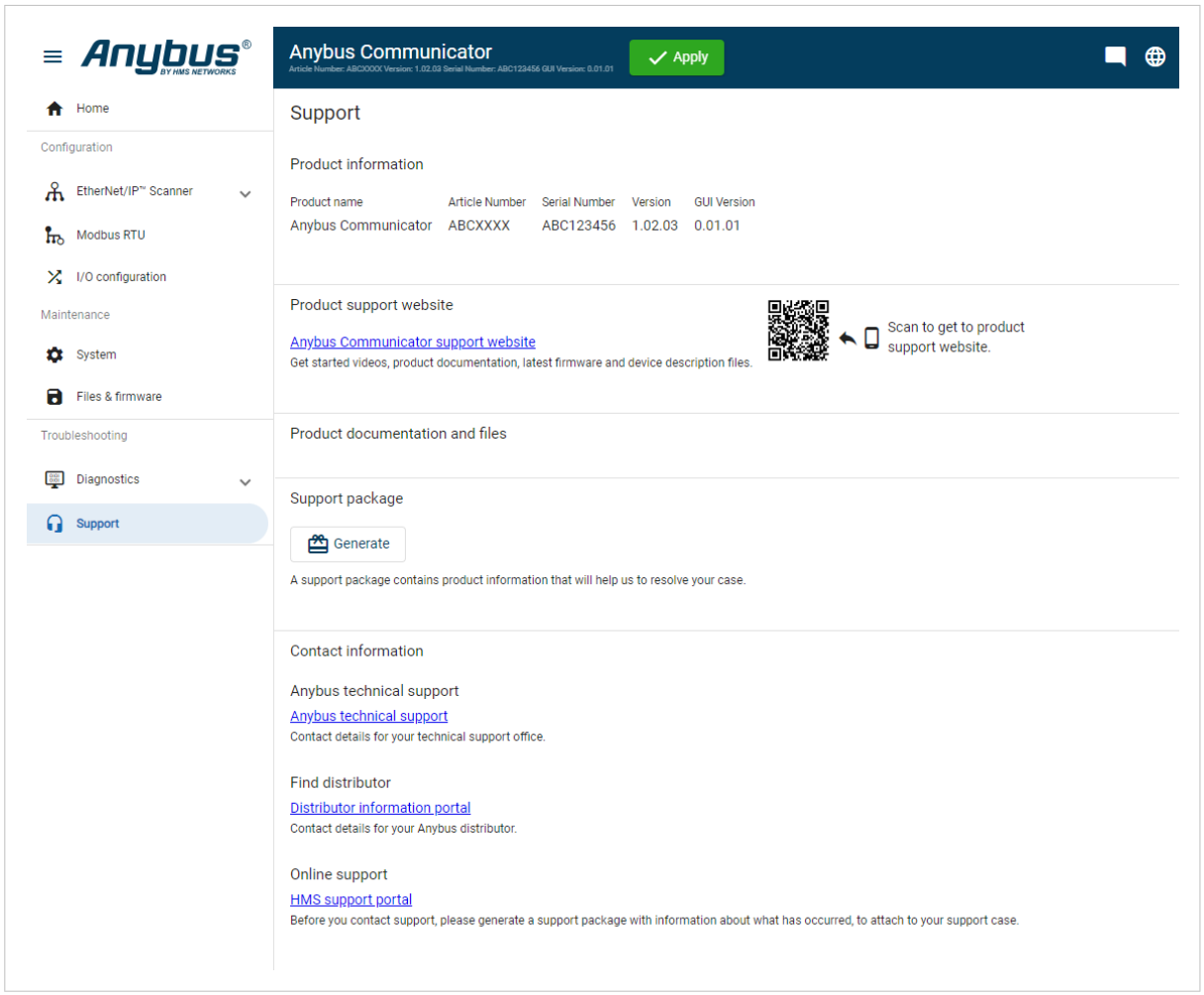


Figure 69. Support page example

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

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

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

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

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

Create a Support Ticket

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

13. End Product Life Cycle

13.1. Secure Data Disposal

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

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

See Reset to Factory Settings (page 83).

14. Technical Data

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

14.1. Technical Specifications

Article identification	ABC3310
Configuration connector	RJ45
Communication connector	7-pin screw connector
EtherNet/IP Scanner connector	RJ45 x 2
Power connector	3-pin screw connector
Power supply	12-30 VDC, Reverse voltage protection and short circuit protection
Power consumption	Typical: 90 mA @ 24 V (2.2 W) Max: 3 W
Storage temperature	-40 to +85 °C
Operating temperature	-25 to +70 °C
Humidity	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days EN 60068-2-30: Damp heat, +25°C – +55°C, 95% RH, 2 cycles
Vibration	See datasheet
Housing material	Plastic, See datasheet for details
Protection class	IP20
Product weight	150 g
Dimensions	27 x 144 x 98 mm (W x H x D) with connectors included
Mounting	DIN-rail