ENGLISH

Anybus® Communicator™ - Modbus RTU Server to Modbus TCP

USER MANUAL

SCM-1202-240
Version 1.3
Publication date 2026-03-30



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 © 2026 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

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 Operating Systems 8
4.4.2. Supported Web Browsers 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. How the Communication Works 10
5.2. How the Data Exchange Works 11
5.3. Data Integrity 11

6. Installation 12
6.1. External Parts 12
6.2. Connector Port Guide 13
6.3. DIN Rail Mounting 14
6.4. Connect to Modbus RTU Network 15
6.5. Connect to Modbus TCP Network 17
6.6. Connect to Power 19
6.7. Security Switch 21
6.8. Lock the Cables 23
6.9. DIN Rail Demount 24

7. Accessing the Communicator 25
7.1. Connect to Configure the Communicator 25
7.2. Access the Built-In Web Interface from HMS IPconfig 26
7.3. Access the Built-In Web Interface from a Web Browser 27
7.4. Communicator Built-In Web Interface Overview 29

8. User Management 30

8.1. User Roles Overview 30
8.2. User Roles Configuration Access 31
8.3. Set Up User Roles 32
8.4. Set or Change Password 33
8.5. Logout From the Communicator Web Interface 34

9. Communicator Configuration 35
9.1. Modbus RTU Settings 35
9.1.1. Communication Settings 35
9.1.2. Legacy Mode for Anybus Address Mode | Modbus RTU 37
9.2. Modbus TCP Settings 39
9.2.1. IP Settings 39
9.2.2. Timeout Time Settings 40
9.2.3. Legacy Mode for Anybus Address Mode | Modbus TCP 40
9.3. Security Settings 41
9.3.1. Local Time and Date 41
9.3.2. Network Time Protocol (NTP) Synchronization 42
9.3.3. Installing a Web Server Certificate 43
9.3.4. View Current Certificate 45
9.3.5. Update or Delete a Certificate 46
9.3.6. Secure Connection With HTTPS Mode 48
9.3.7. None Secure HTTP Mode 50
9.3.8. Device IP Address Discovery via HMS Software Applications 51
9.4. I/O Configuration 52
9.4.1. Endian Swap 52
9.4.2. Convert Between Big-Endian and Little-Endian 53
9.4.3. Build Detailed Endian Swap 54
9.4.4. Process Data Settings 55
9.5. Configuration Notes 56
9.5.1. Add Configuration Note 56
9.5.2. View and Edit Configuration Notes 58
9.6. Apply Configuration 59
9.7. To Use an Existing Configuration 60

10. PLC Configuration 61
10.1. PLC Device Security 61
10.2. Modbus Addressing and Register Mapping 61
10.2.1. The Difference Between Address and Register Start 61
10.2.2. To Read and Write Data 62
10.2.3. Default Address Mode I/O Data Mapping 64
10.2.4. Legacy Address Mode I/O Data Mapping 65

11. Verify Operation 66
11.1. Communicator Status Monitor 66
11.2. Communicator LED Indicators 68
11.3. Ethernet RJ45 LED Indicators 70

12. Maintenance 71
12.1. Action on Fatal Error 71
12.2. Configuration Port IP Settings 72
12.3. Dashboard 73
12.4. Configuration File Handling 76
12.4.1. Export Configuration 76
12.4.2. Import Configuration 77
12.5. Clear and Revert Configuration 78

12.6. Firmware Management 79
12.6.1. View the Firmware Version 79
12.6.2. Firmware and Configuration Compatibility 79
12.6.3. Firmware File Validation 79
12.6.4. Update Firmware 80
12.7. Change Language 81

13. Troubleshooting 82
13.1. Diagnostics 82
13.1.1. I/O Data 82
13.1.2. Event Log 83
13.1.3. LED Status 84
13.2. Reset to Factory Settings 85
13.3. Firmware Upgrade Error Management 88
13.4. Support 90
13.4.1. Support Package 90

14. Technical Data 91
14.1. Technical Specifications 91

15. End Product Life Cycle 92
15.1. Secure Data Disposal 92

16. Reference Guides 93
16.1. About Input Registers and Holding Registers 93
16.2. Modbus Data Model 93
16.3. Modbus Function Codes 94
16.4. Modus Exception Codes 94

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 85).

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.

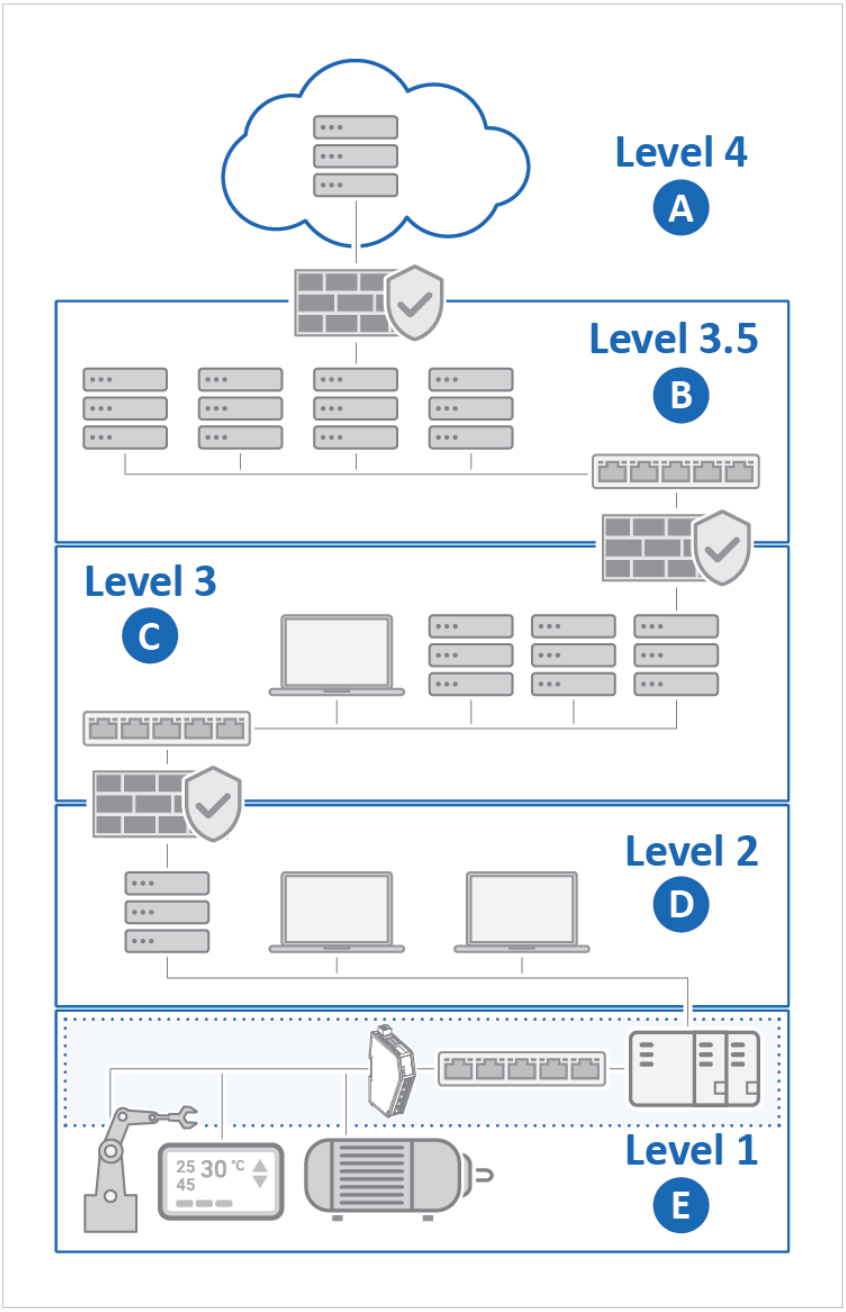


Figure 1. Purdue model, product security context

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

4.3. Mechanical Tools and Equipment

Have the following tool(s) available:

Flat-head screwdriver, size 5.5 mm

Needed when removing the Communicator from DIN-rail.

Flat-head screwdriver, size 3 mm

Needed when connecting the cables to the 7-pin connector.

4.4. System Requirements

4.4.1. Supported Operating Systems

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

4.4.2. Supported Web Browsers

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

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

4.5. HMS Software Applications

Download the software installation files and user documentation from www.hms-networks.com/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. How the Communication Works

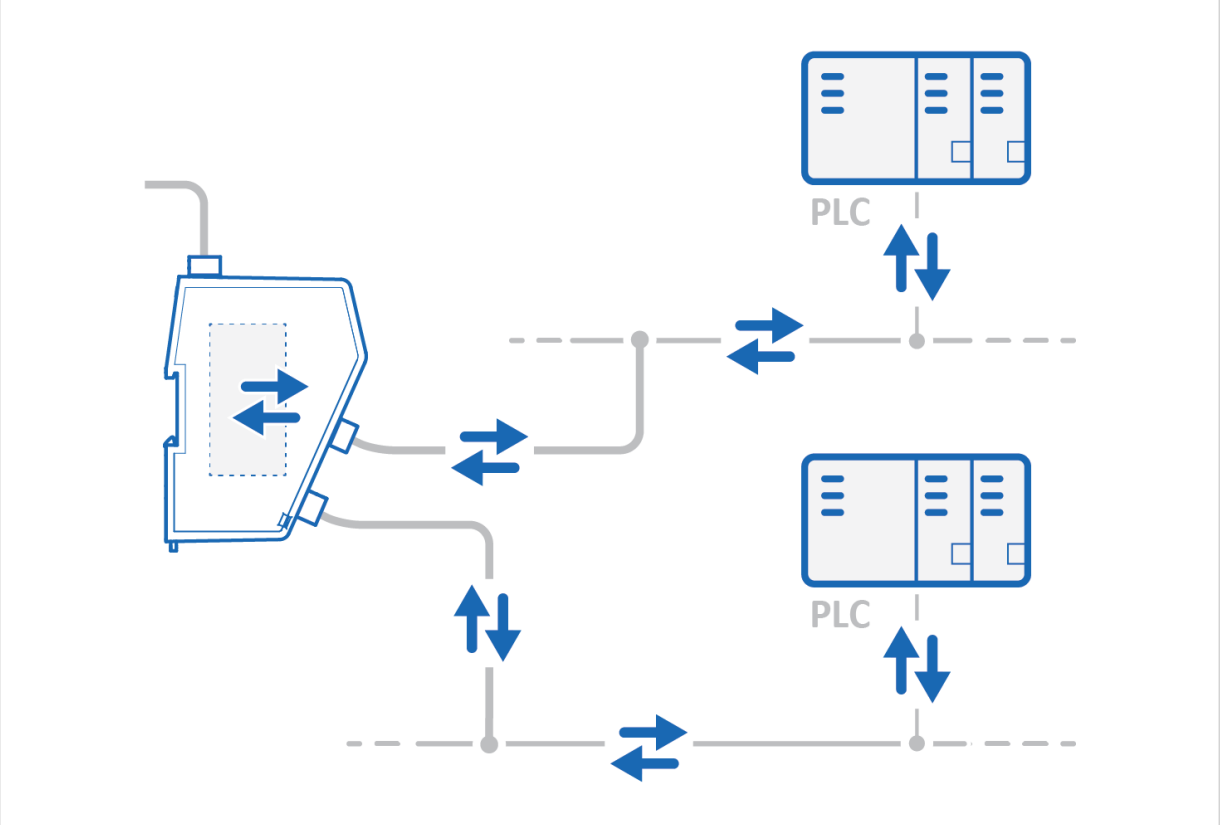


Figure 2. Process data traffic overview

The Communicator enables communication between a Client device connected to a Modbus RTU Server network and a Client device connected to a Modbus TCP network.

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

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

5.2. How the Data Exchange Works

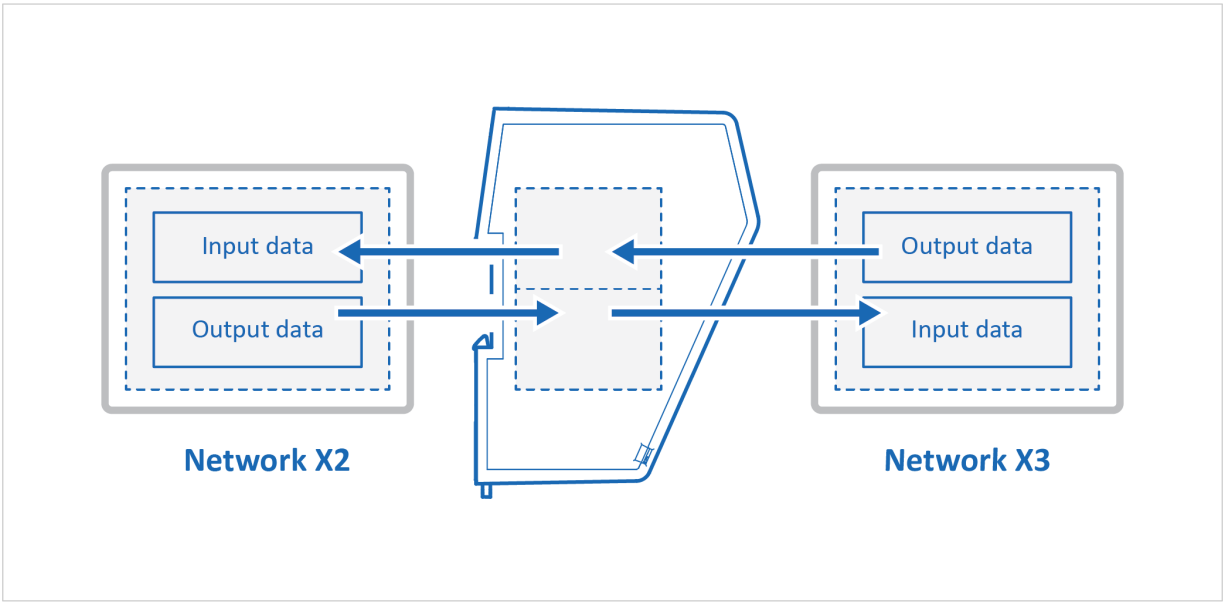


Figure 3. The Communicator internal memory areas

The data exchanged between the Communicator and the Modbus RTU Server and the Modbus TCP resides in the Communicator internal memory buffer.

Input Data

This Input data area is read by the Modbus TCP.

Output Data

The Output data area is read/written by the Modbus RTU Server.

5.3. Data Integrity

A snapshot of the process data buffer between the Client and the server interface is used during the operation of executing all the transactions within one cycle.

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

6. Installation

6.1. External Parts

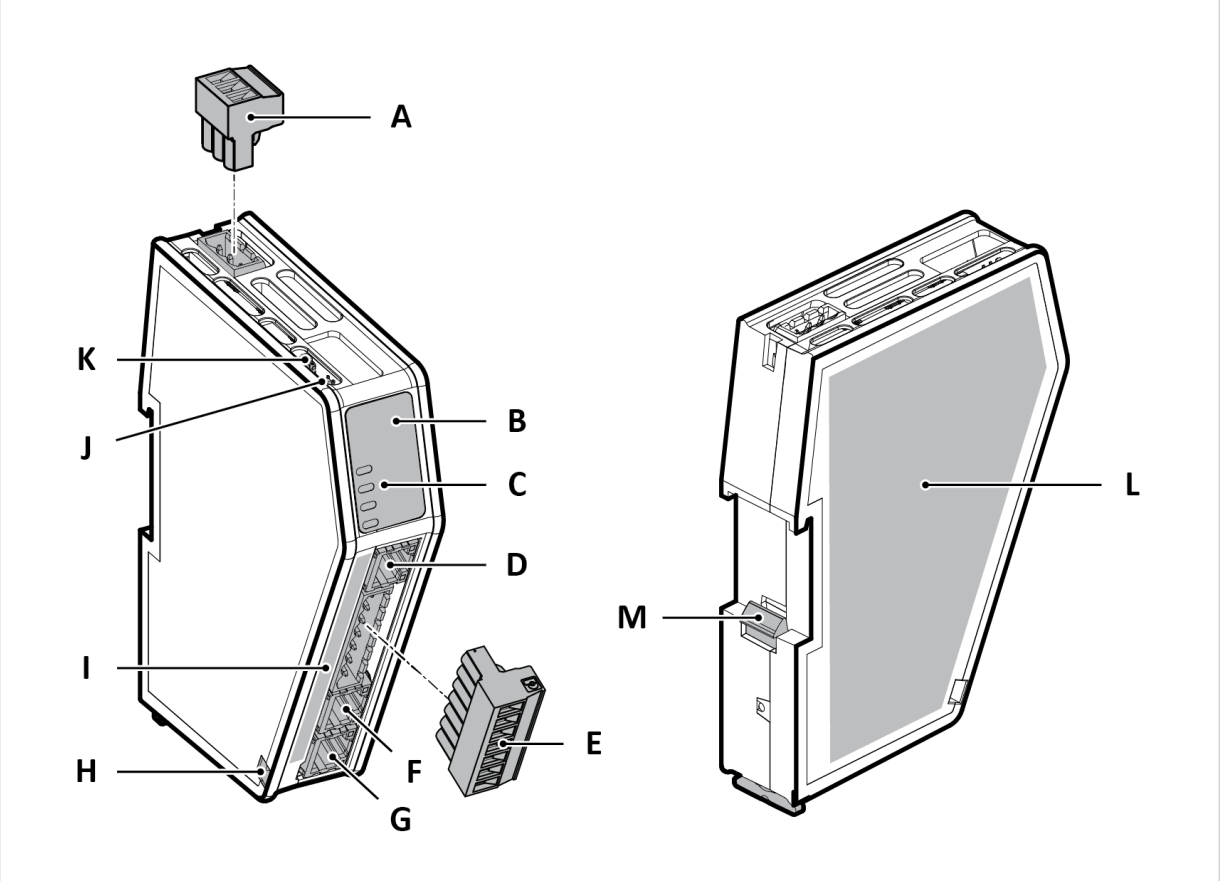


Figure 4. Communicator external parts

A. Power connector
B. Label with LED designation
C. Status LEDs
D. Configuration port
E. Modbus RTU Server (X2) 7-pin connector
F. Modbus TCP (X3.1) connector
G. Modbus TCP (X3.2) connector
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

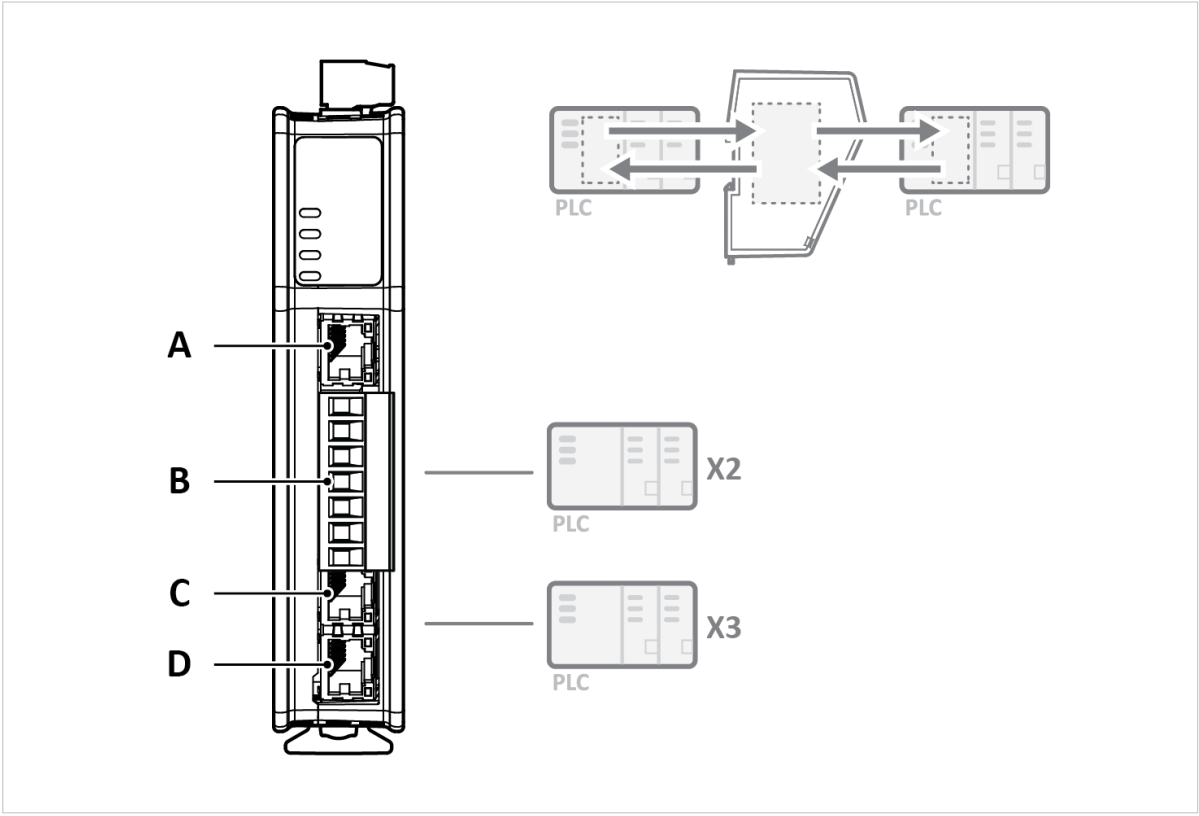


Figure 5. Communicator connector ports

Position	Port Number	Connector	Port Usage
A	X1	Ethernet RJ45	Configuration port
B	X2	7-pin screw terminal block	Modbus RTU network
C	X3.1	Ethernet RJ45	Modbus TCP network
D	X3.2	Ethernet RJ45	Modbus TCP network

See Also

Connect To Modbus RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)

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.

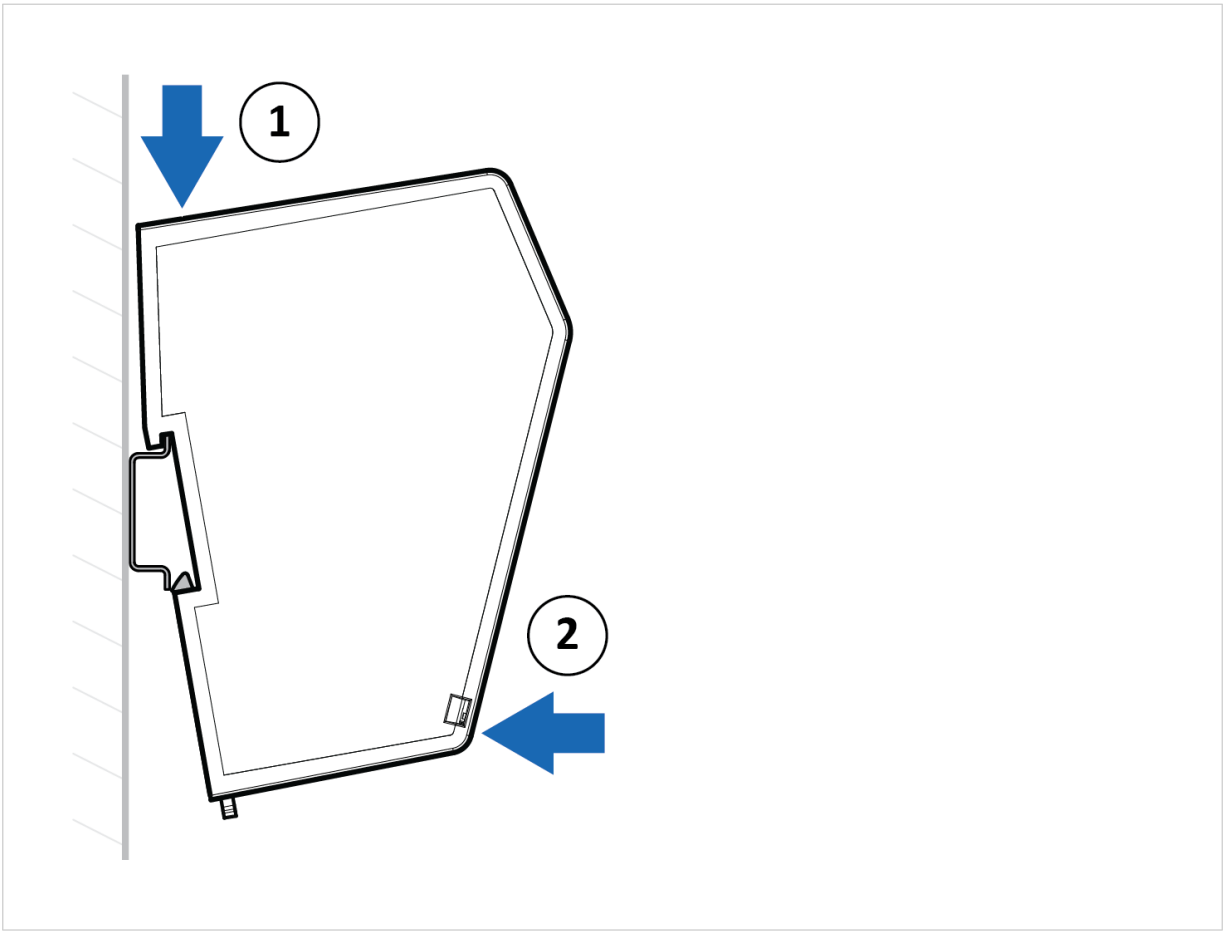


Figure 6. Attach the Communicator on the DIN rail

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 RTU Network

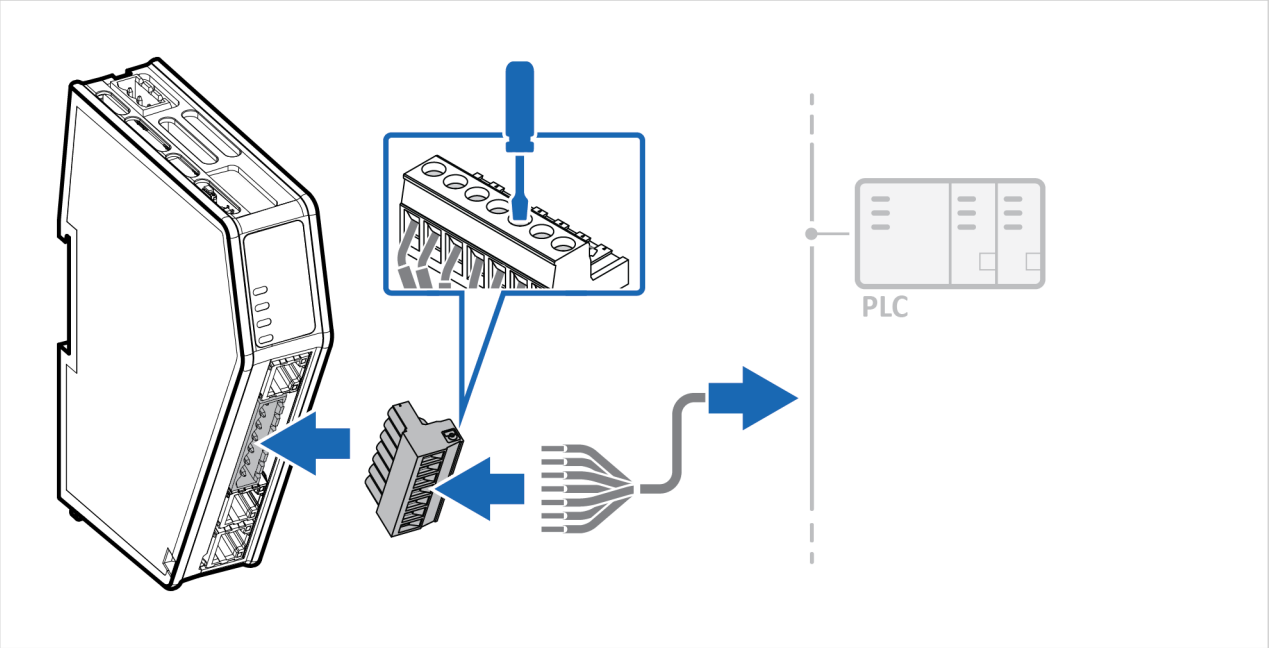
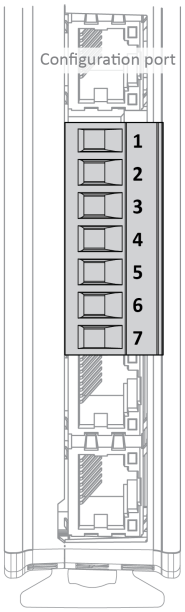


Figure 7. Connect to Modbus RTU network

Modbus RTU Connector Pinout

NOTE
Use minimum 90 °C 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

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.

See Also

Connector Port Guide (Page 13)
Connect To Modbus TCP Network (Page 17)
Connect To Power (Page 19)
Communicator Status Monitor (Page 66)
Communicator LED Indicators (Page 68)
LED Status (Page 84)
Firmware Upgrade Error Management (Page 88)

6.5. Connect to Modbus TCP Network

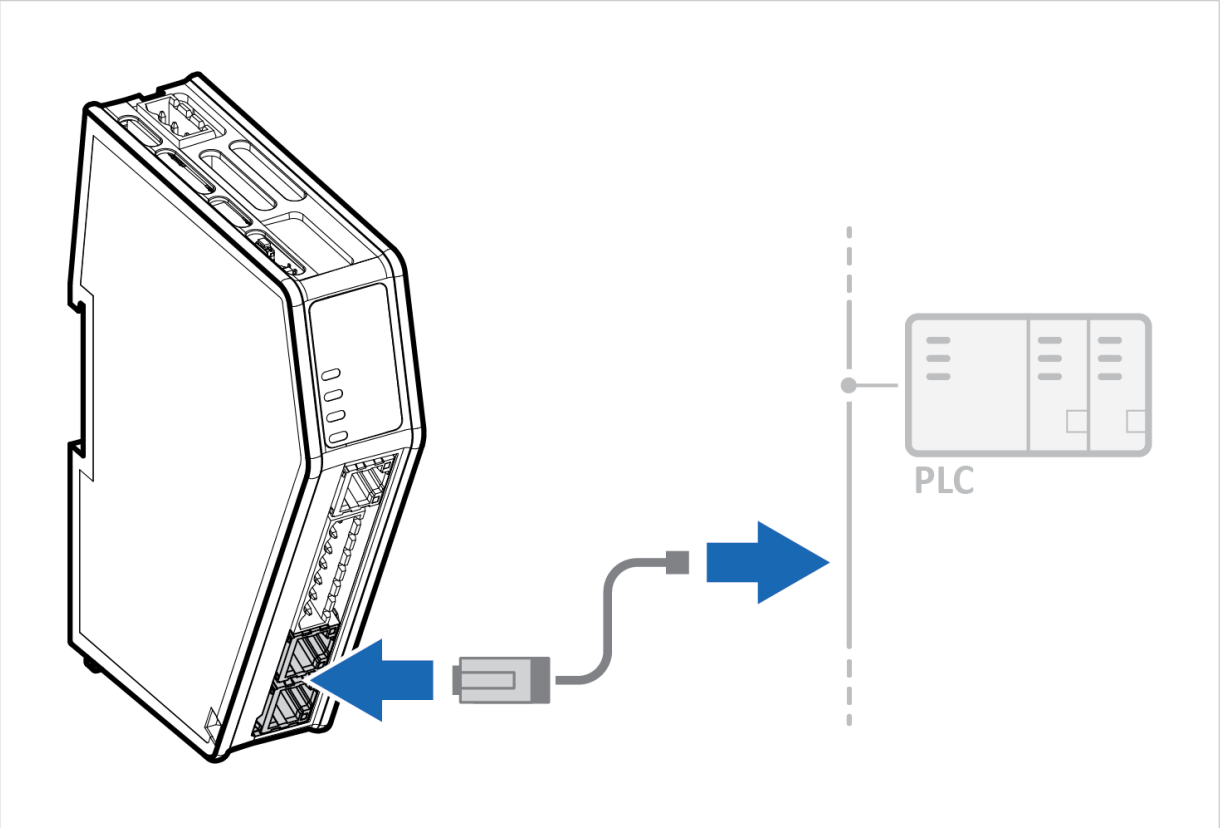
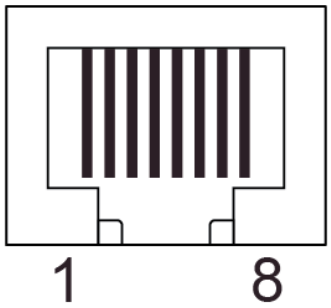


Figure 8. Connect to Modbus TCP network

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 network.

See Also

Connector Port Guide (Page 13)
Connect To Modbus RTU Network (Page 15)
Connect To Power (Page 19)

Communicator Status Monitor (Page 66)
Communicator LED Indicators (Page 68)
LED Status (Page 84)
Firmware Upgrade Error Management (Page 88)

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.

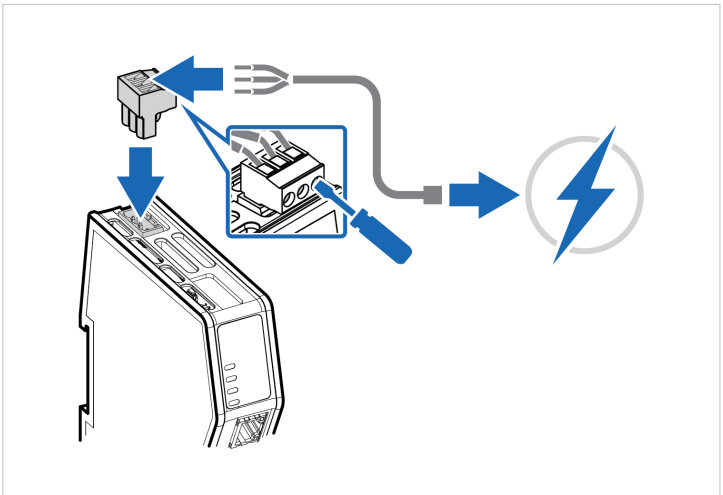
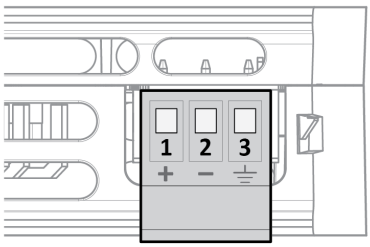


Figure 9. Connect to power

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 RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)
Communicator Status Monitor (Page 66)

Communicator LED Indicators (Page 68)
LED Status (Page 84)
Firmware Upgrade Error Management (Page 88)

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

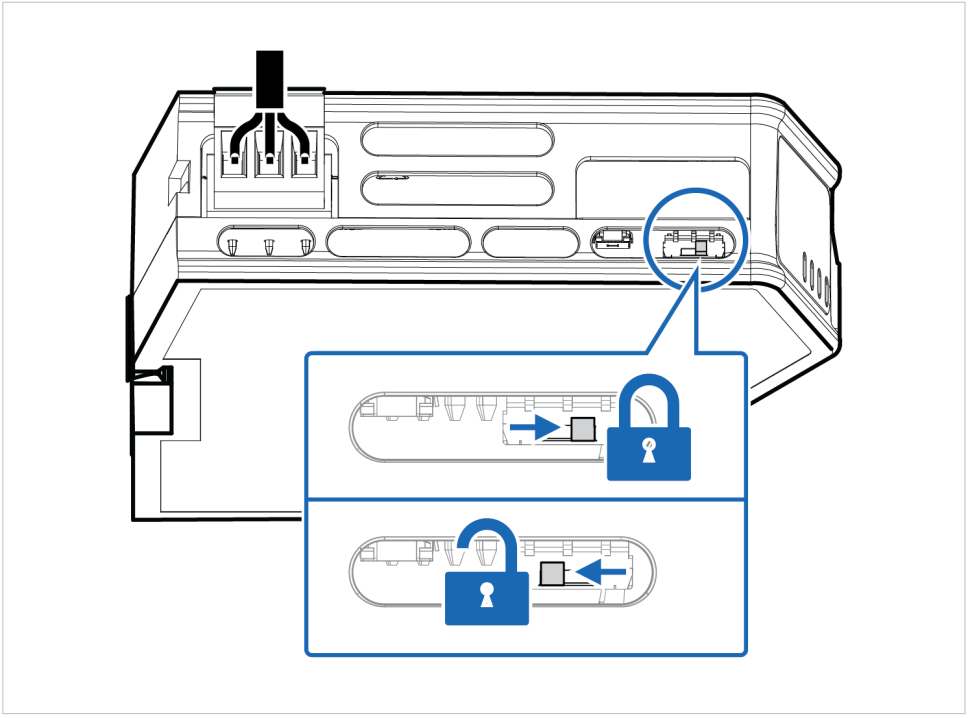


Figure 10. Security switch in locked and unlocked position

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

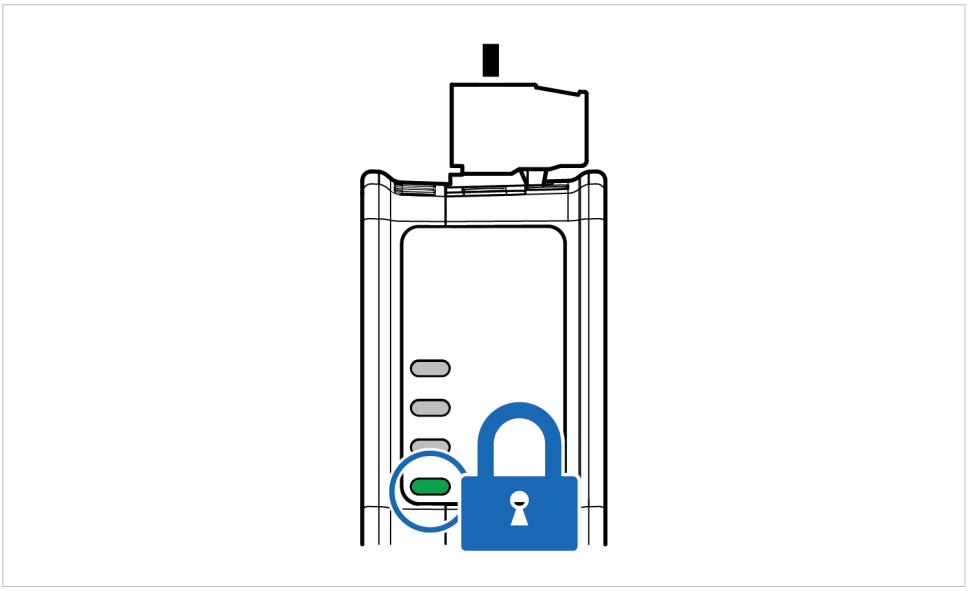


Figure 11. Security switch locked status LED

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

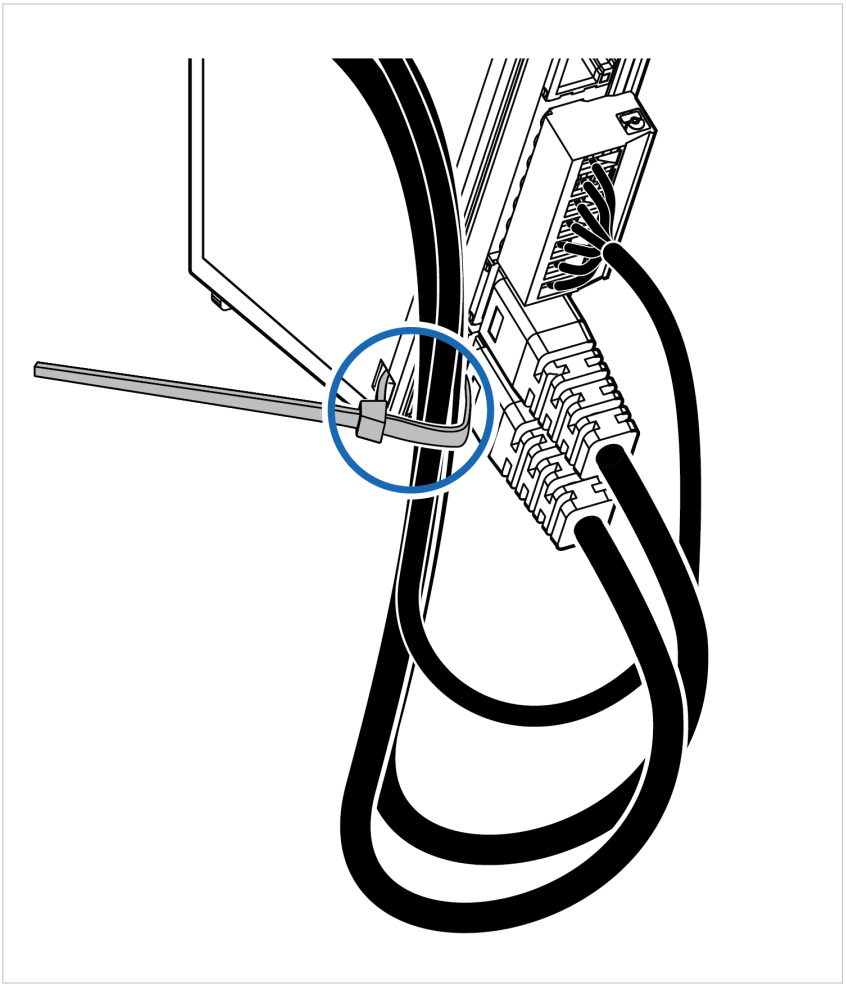


Figure 12. Lock the cables

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:

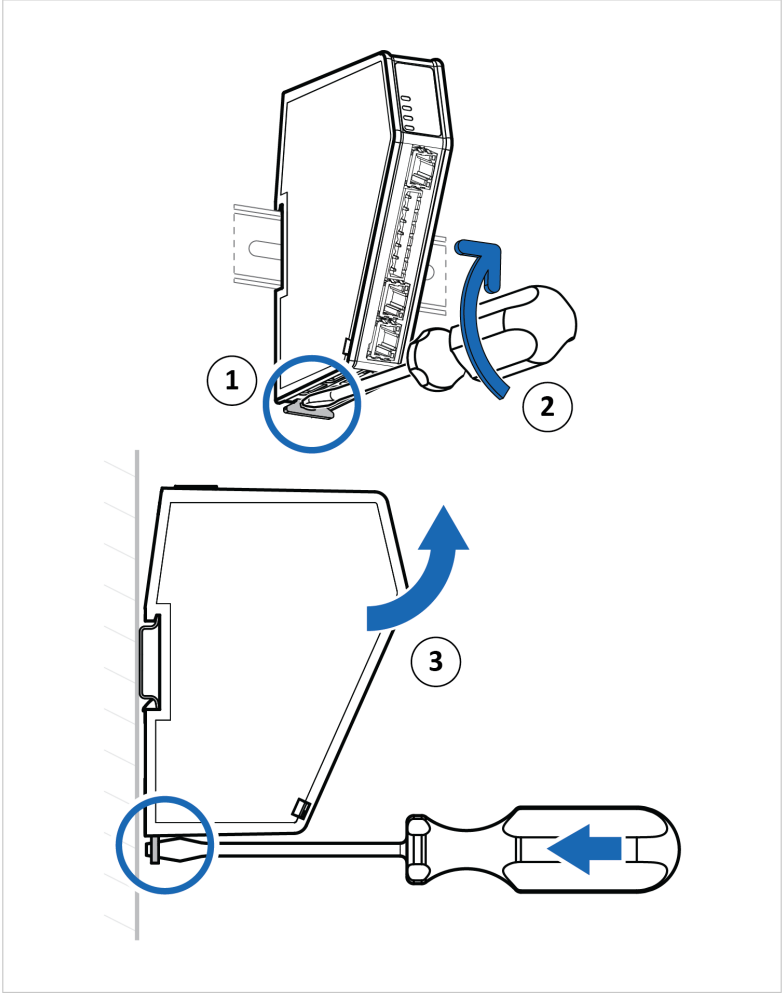


Figure 13. Unlock and unhook the Communicator

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:

   - Modbus RTU Server network — (1) (2) and (3)
   - Modbus TCP network — (4)

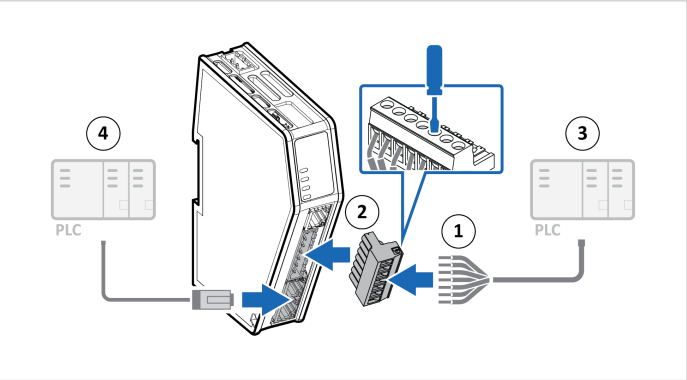


Figure 14. Connect to networks

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

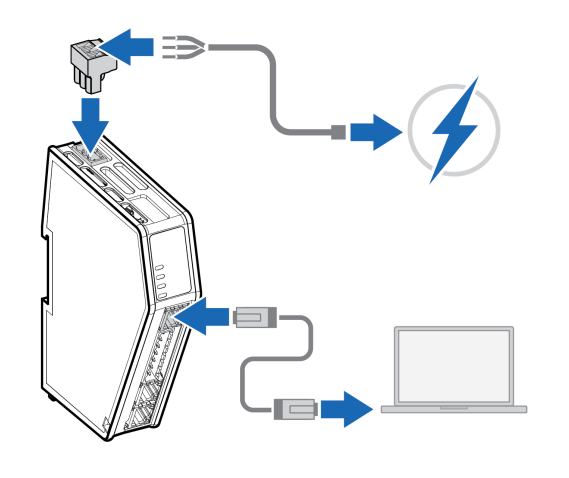


Figure 15. Connect to PC and power

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.

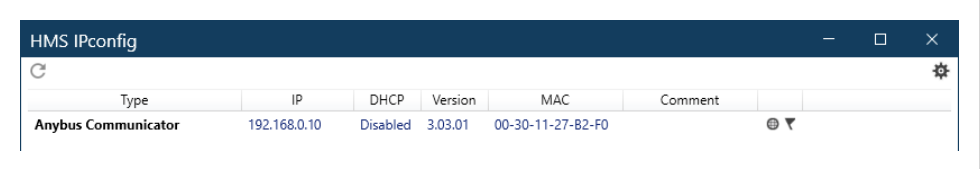
TIP
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System** > **Configuration port** page.

Download HMS IPconfig Installation Files

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

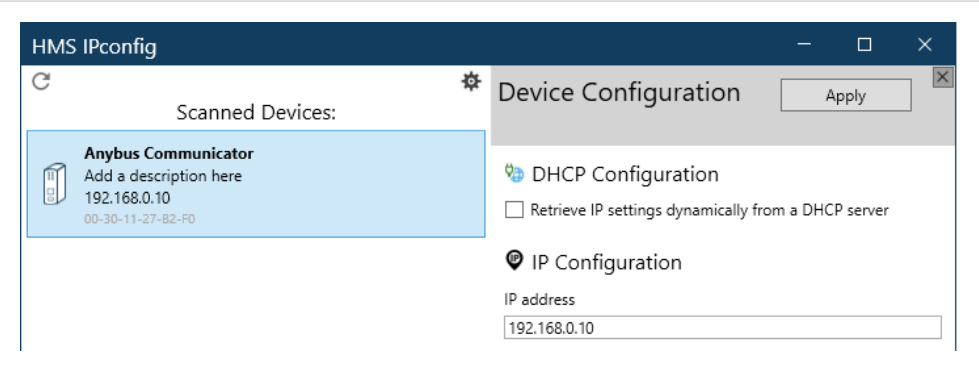
Procedure

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

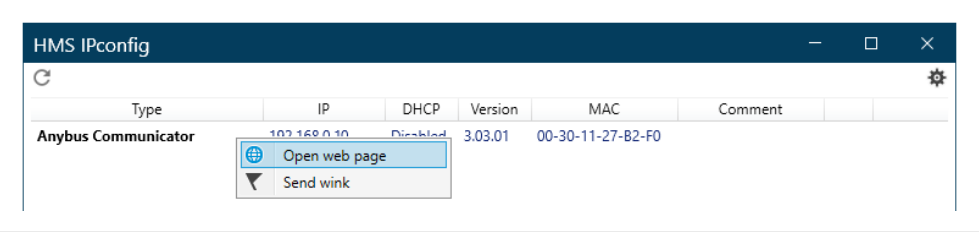


   - HMS IPconfig automatically starts scanning for compatible and active HMS devices.
   - Found HMS devices are added to the device list.
3. To open the settings pane, click on the Communicator in the device list.

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

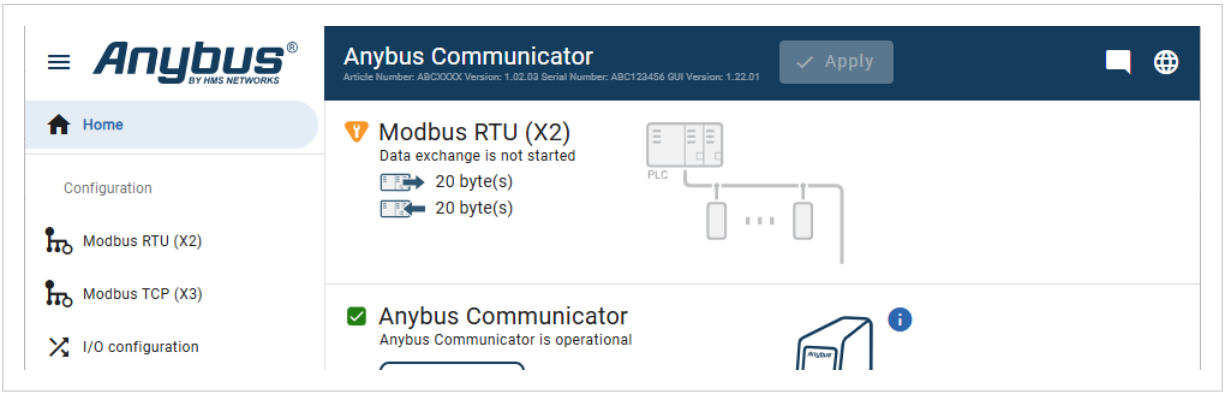


5. To open the **Open web page** built-in web interface, click Communicator.



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.

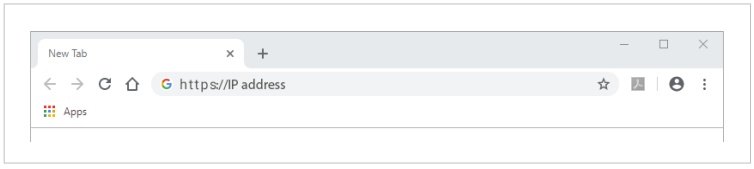
TIP
When you have accessed the Communicator built-in web interface, you can change the IP settings for the Communicator configuration port on the **System** > **Configuration port** page.

Procedure

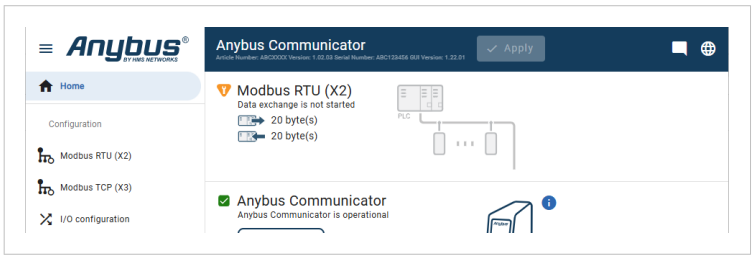
1. On the PC accessing the Communicator built-in web interface, set a static IP address within the same IP address range as the Communicator IP address.



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.

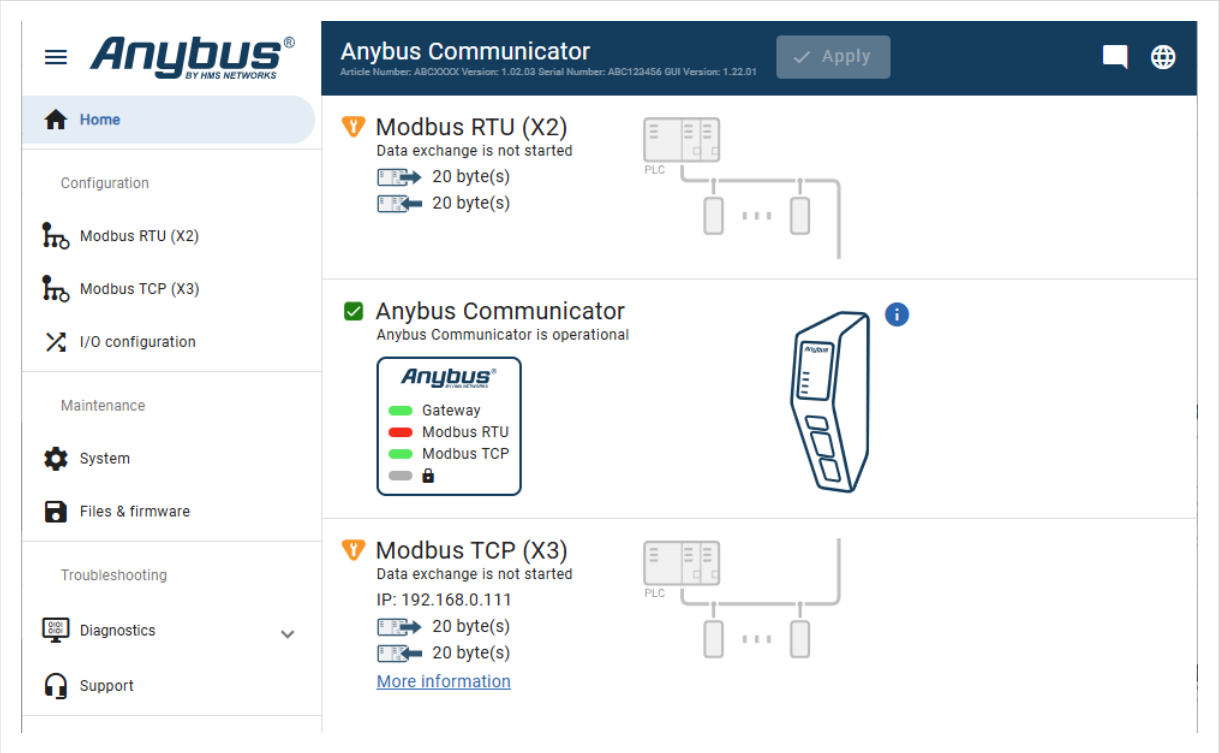


Figure 16. The Communicator built-in web interface Home page

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

8. User Management

8.1. User 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.

8.2. User Roles Configuration Access

Administrator Role - Full Access

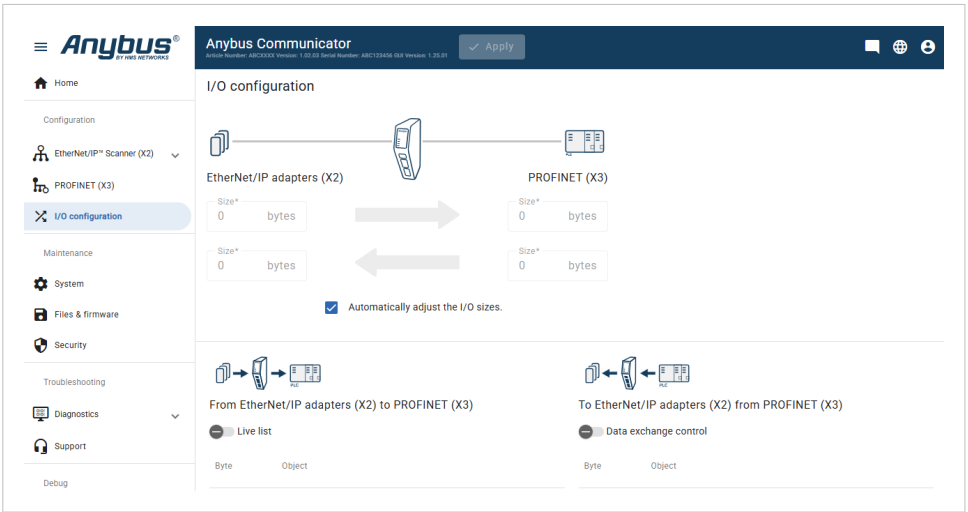


Figure 17. Example: Editable I/O configuration settings

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

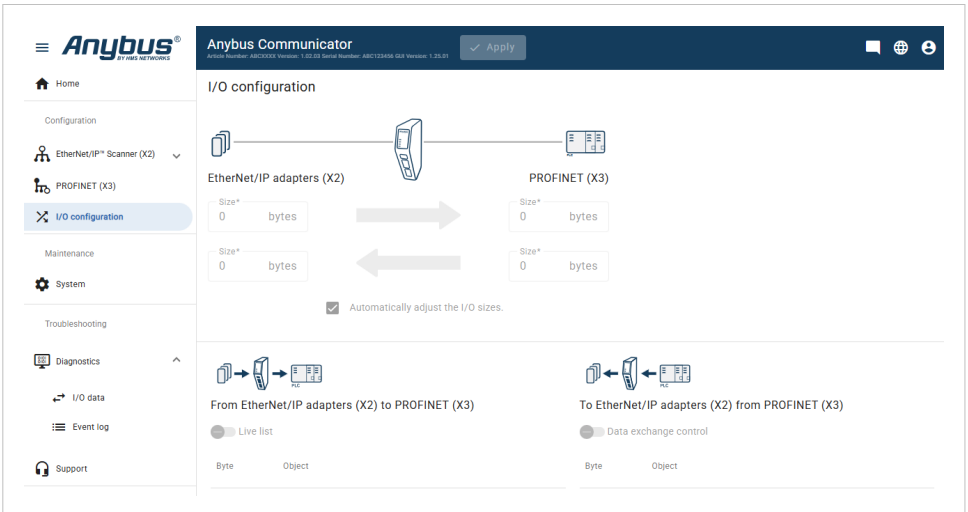


Figure 18. Example: Locked and grayed-out I/O configuration settings

The Operator role has read-only access to the configuration settings in the Communicator web interface.

Restricted settings are locked and grayed out.

8.3. Set Up User Roles

By default, **User 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.

Procedure

Enable User Roles:

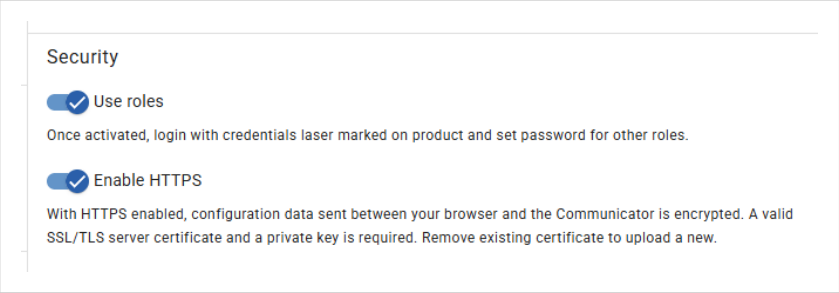


Figure 19. System page with User role(s) enabled

1. Open the **System** page.
2. In the **Security** section, click the **Use roles** toggle to enable roles.
3. Click **Apply** in the web interface header.
   The settings are applied and you are automatically logged out.

Manage Roles and Passwords:

1. When user 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.
2. From the **Role** drop-down menu, select the role to configure: Administrator or Operator.

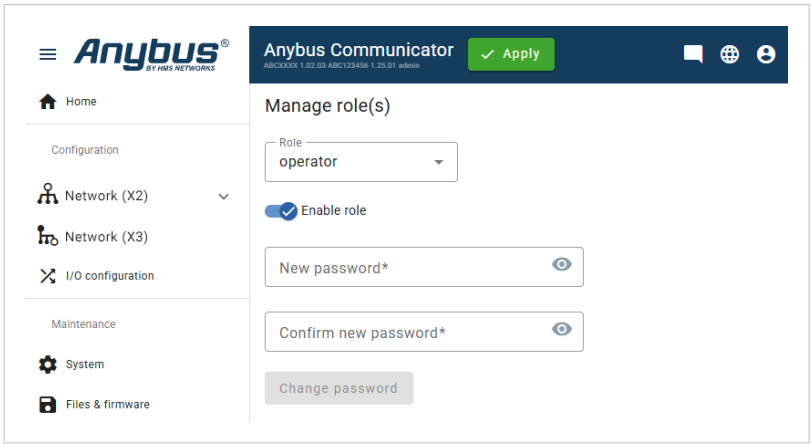


Figure 20. Manage roles(s) page

3. Enter the password in the **New password** field.

4. Re-enter the password in the **Confirm password** field.
5. Click **Change password** to confirm.
6. Click **Apply** in the web interface header.
   The settings are applied and you are automatically logged out.

Result

User roles are enabled, and the factory default mode that does not require user credentials is turned of.

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)**.

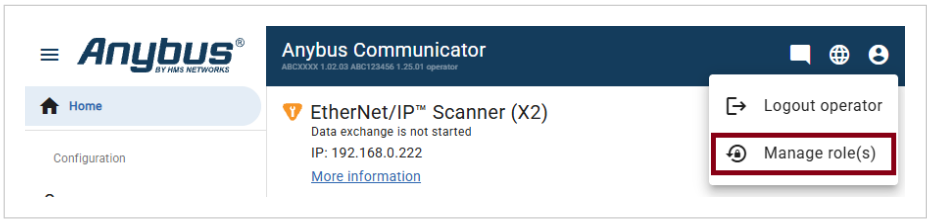


Figure 21. Account menu, **Manage role(s)**

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

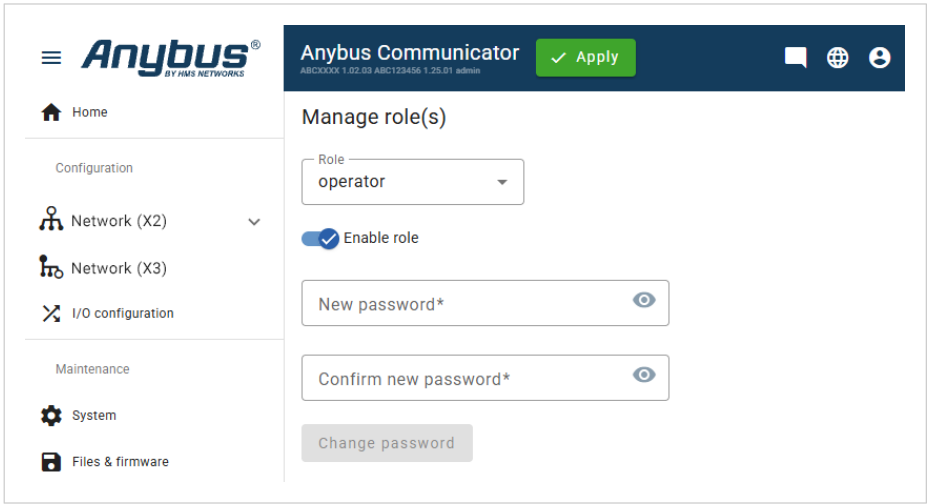


Figure 22. Manage roles(s) page

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

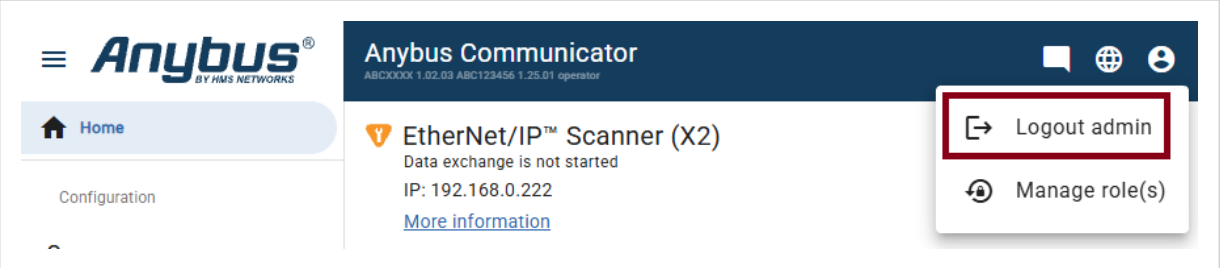


Figure 23. Account menu, Logout

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

9. Communicator Configuration

9.1. Modbus RTU Settings

Configure the Modbus RTU Server network settings.

9.1.1. Communication Settings

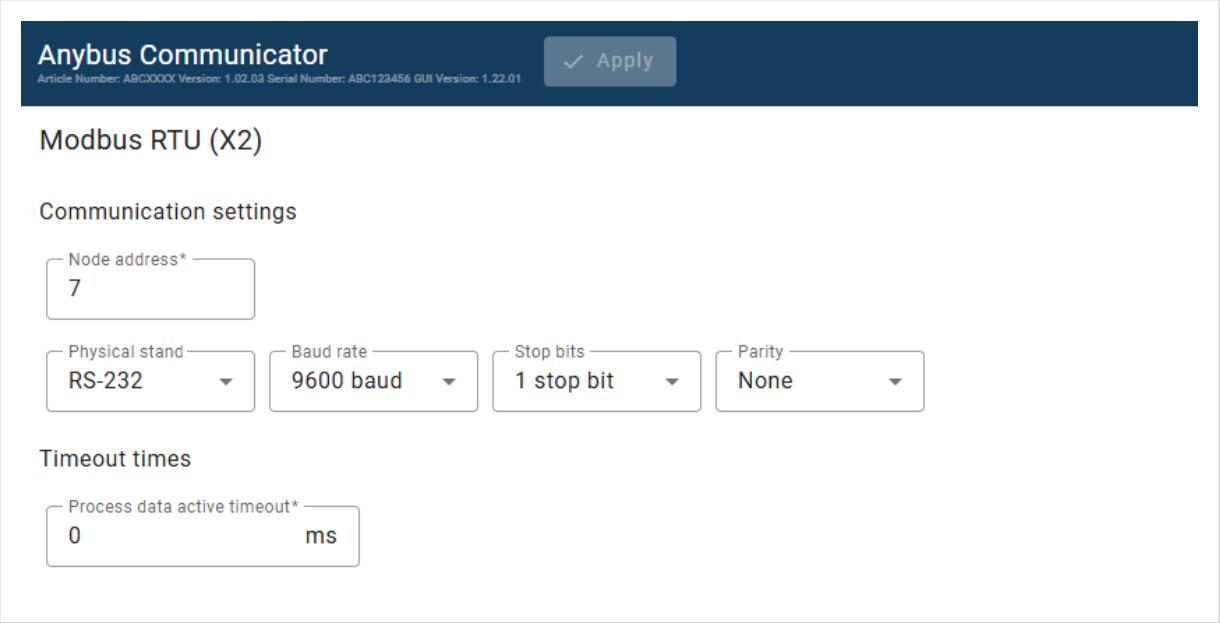


Figure 24. Communication, Basic settings

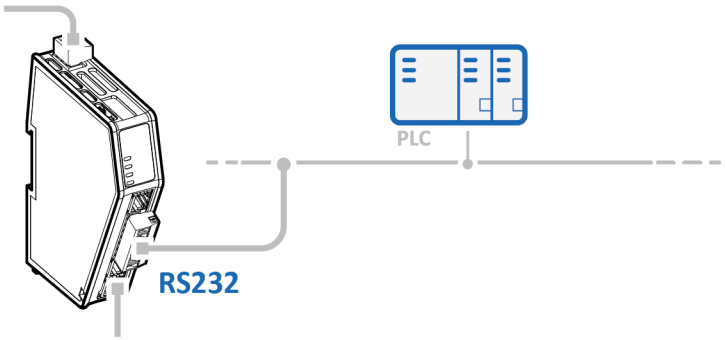
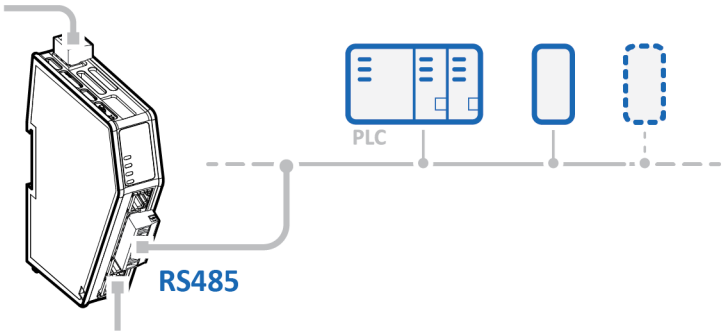
Node Address

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

Specify the maximum allowed time between two incoming messages in steps of 10 ms.

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

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

The data sent to the Modbus TCP network is frozen.

To enable clear data, see Process Data Settings (page 55).

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

The default value is 0 ms.

9.1.2. 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 65).

To Use Legacy Mode

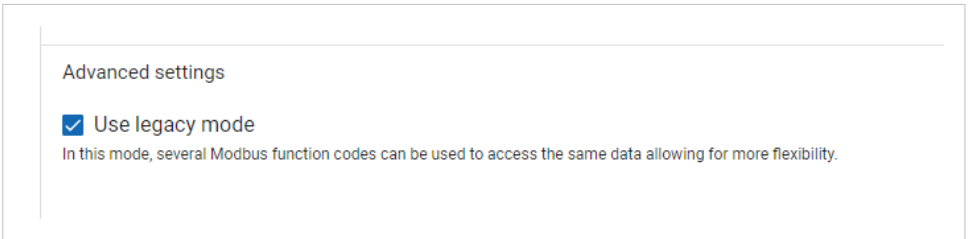


Figure 25. Advanced settings > Use legacy mode

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

9.2. Modbus TCP Settings

Configure the Modbus TCP network settings.

9.2.1. IP Settings

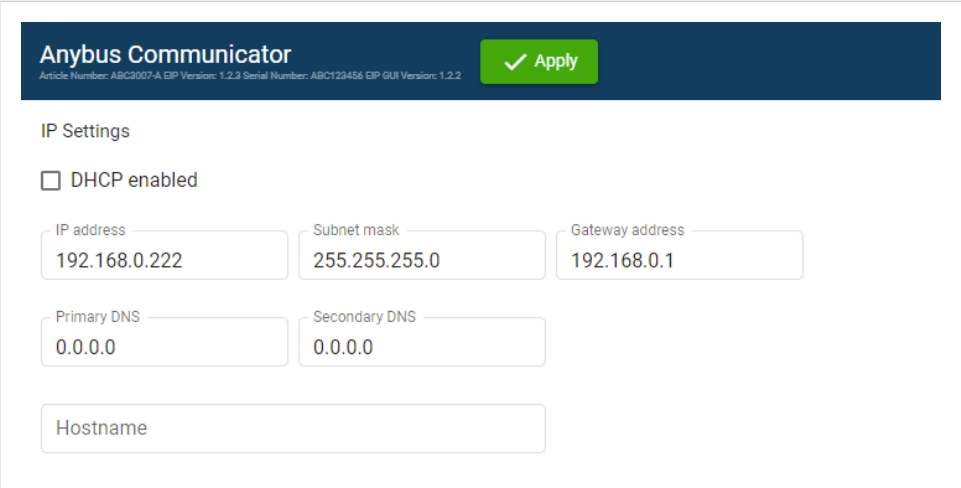


Figure 26. IP Settings

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	255.255.255.0	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.

9.2.2. Timeout Time Settings

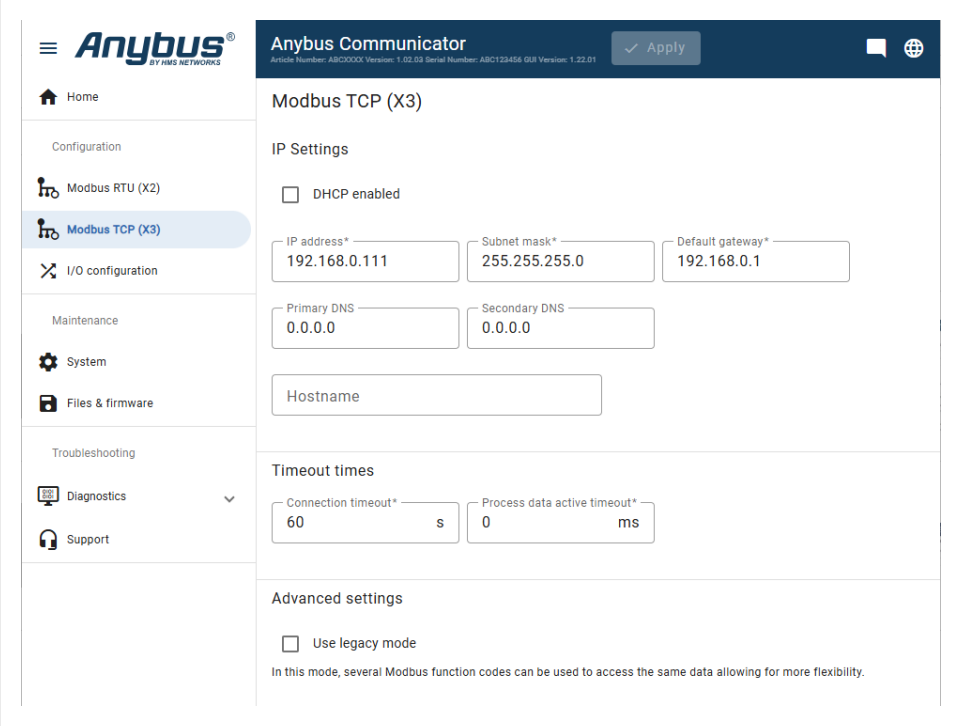


Figure 27. Modbus TCP page, Timeout times

Connection Timeout

Specify how long a Modbus TCP connection may be idle before it is closed by the Communicator.

The default value is 60 seconds.

To disable **Connection timeout**, set the value to 0.

Process Data Active Timeout

Specify the maximum allowed time between two incoming messages in steps of 10 ms.

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

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

The data sent to the Modbus TCP network is frozen.

To enable clear data, see Process Data Settings (page 55).

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

The default value is 0 ms.

9.2.3. Legacy Mode for Anybus Address Mode | Modbus TCP

Advanced settings option for Modbus TCP.

About Legacy Mode

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

See also Legacy Address Mode I/O Data Mapping (page 65).

To Use Legacy Mode

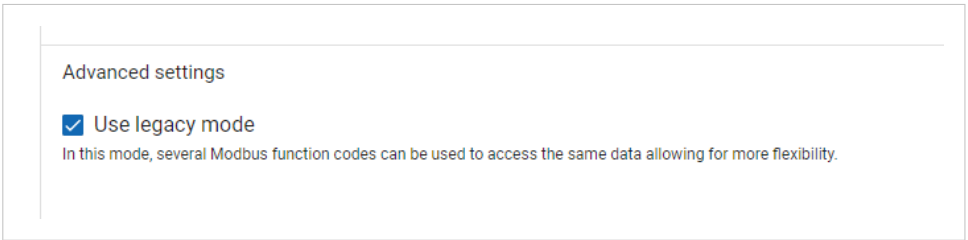


Figure 28. Advanced settings > Use legacy mode

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

See Also

Legacy Address Mode I/O Data Mapping (Page 65)

9.3. Security Settings

9.3.1. Local Time and Date

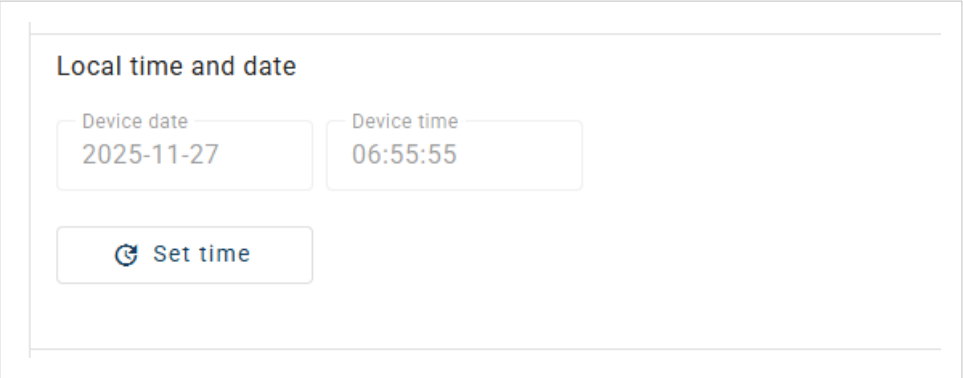


Figure 29. System page, Local time and date

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.

9.3.2. Network Time Protocol (NTP) Synchronization

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

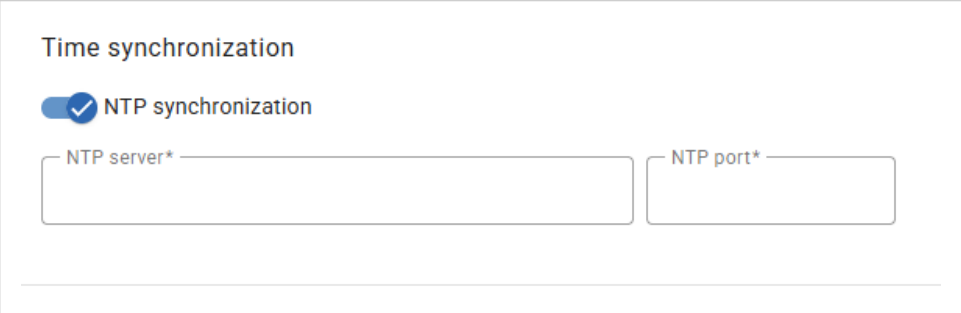


Figure 30. System page, Time synchronization

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.

9.3.3. 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:

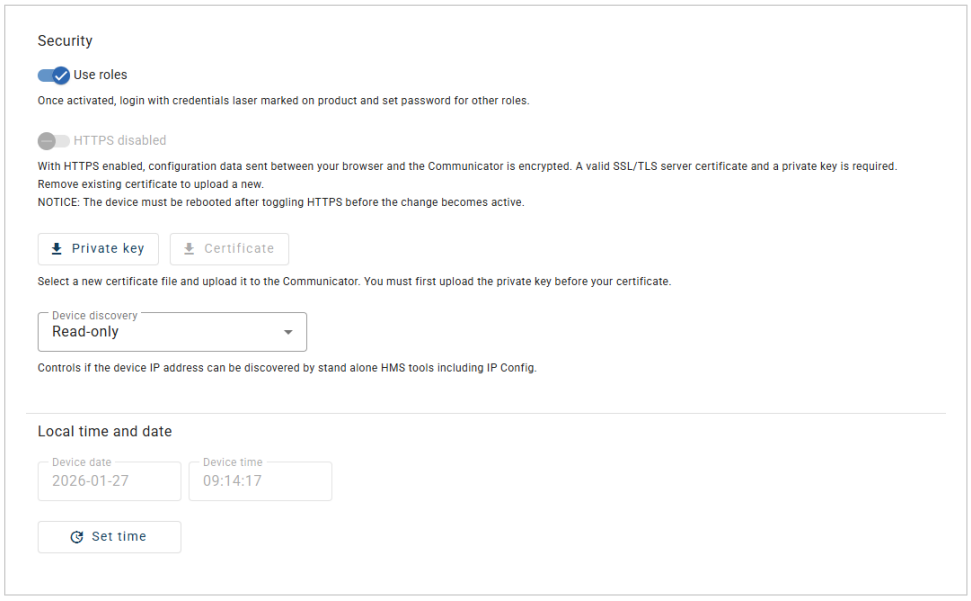


Figure 31. System page, Security settings

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 48).

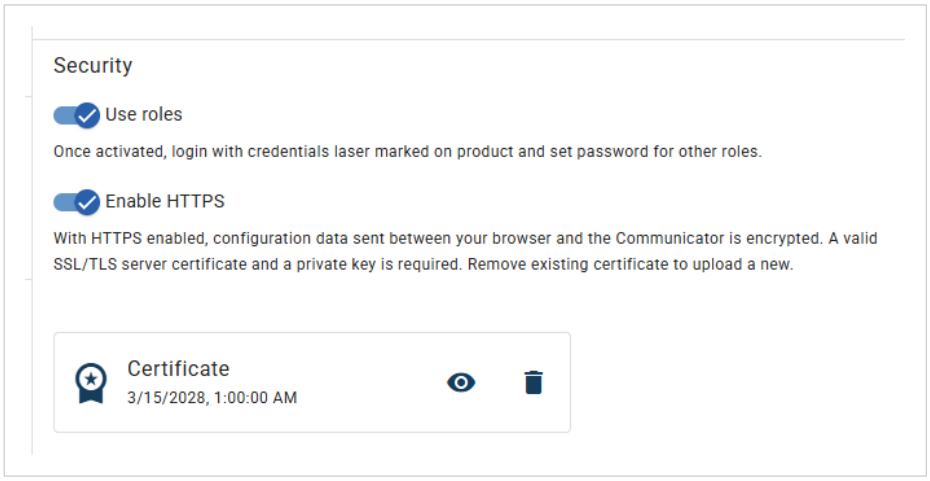


Figure 32. HTTPS enabled

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.

9.3.4. View Current Certificate

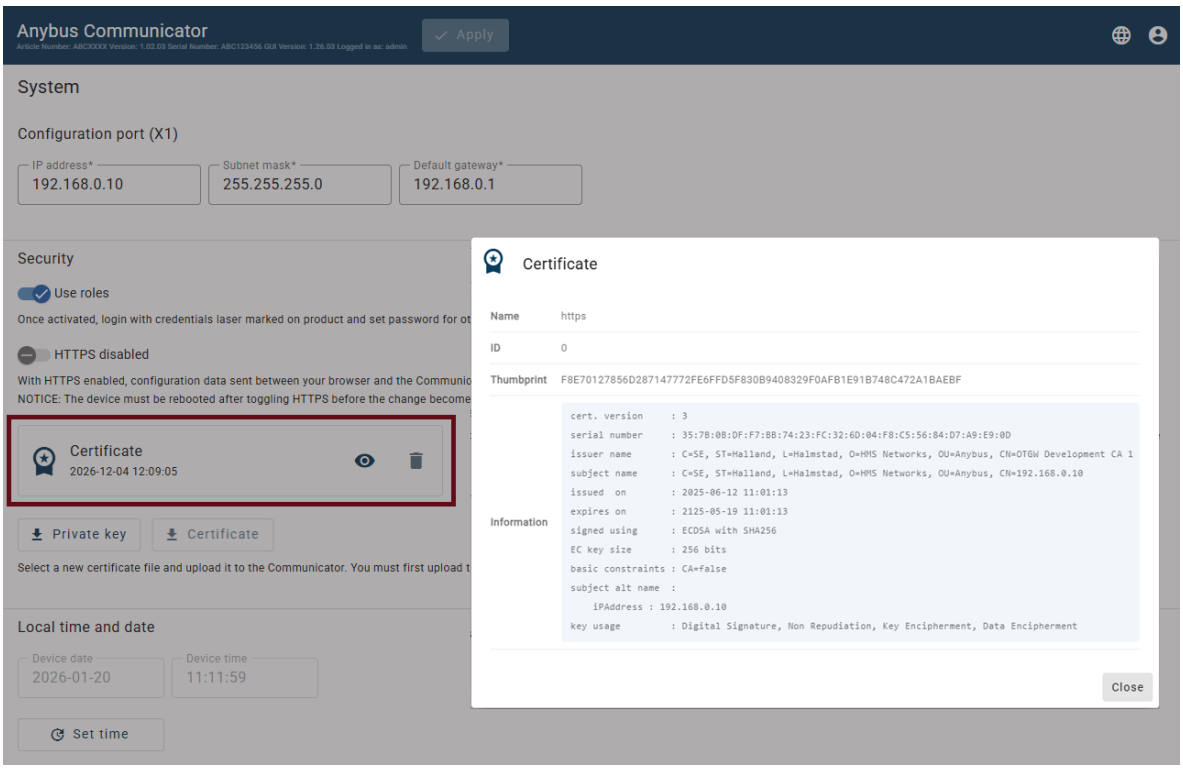


Figure 33. System page, View current certificate

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

The **Certificate** window opens.

9.3.5. Update or Delete a Certificate

Update an Existing Certificate

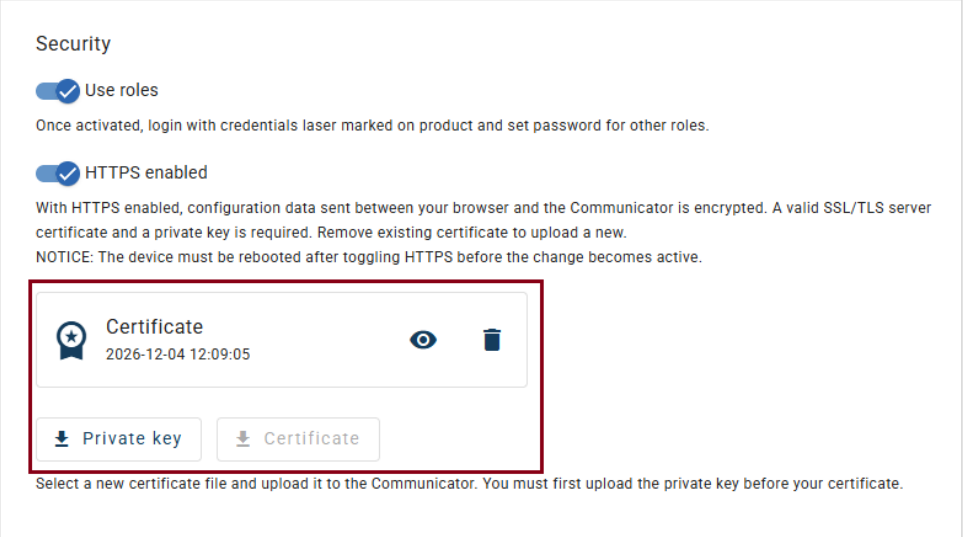


Figure 34. System page showing installed certificate

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 43).

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

Delete a Certificate

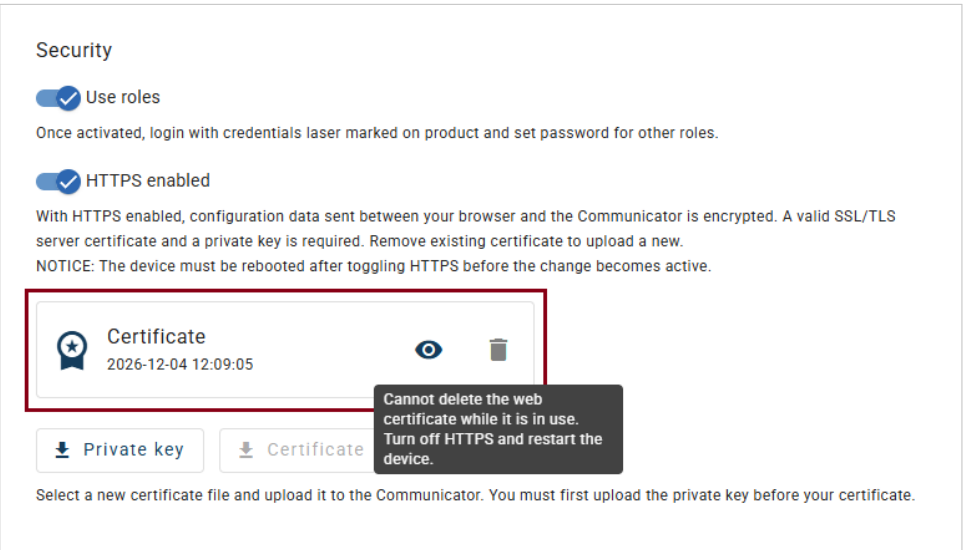


Figure 35. System page showing a locked certificate

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 48)
None Secure HTTP Mode (Page 50)

9.3.6. 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 43).

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 43).

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 43).

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 41) and Network Time Protocol (NTP) Synchronization (page 42).

Procedure

To enable HTTPS mode:

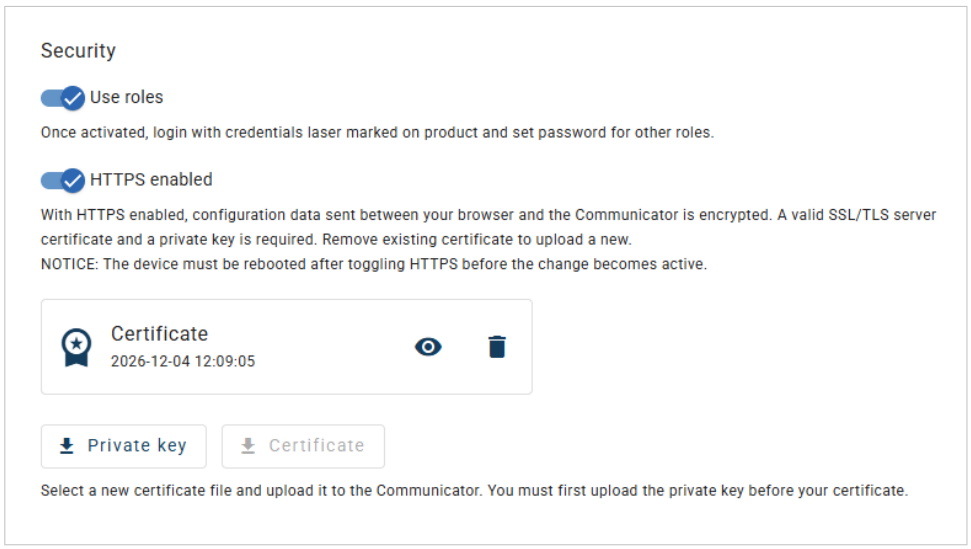


Figure 36. System page

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 46)
None Secure HTTP Mode (Page 50)

9.3.7. None Secure HTTP Mode

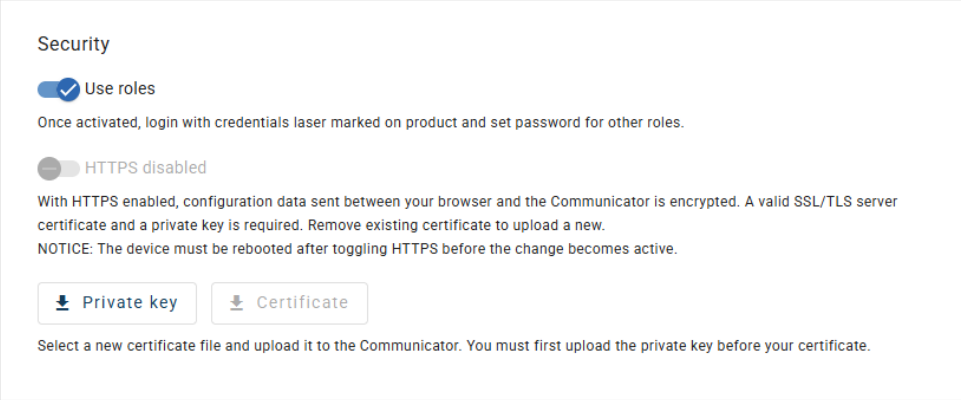


Figure 37. System page, Security settings, and Secure Connection (HTTPS) disabled

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 21).

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 46)
Secure Connection With HTTPS Mode (Page 48)

9.3.8. Device IP Address Discovery via HMS Software Applications

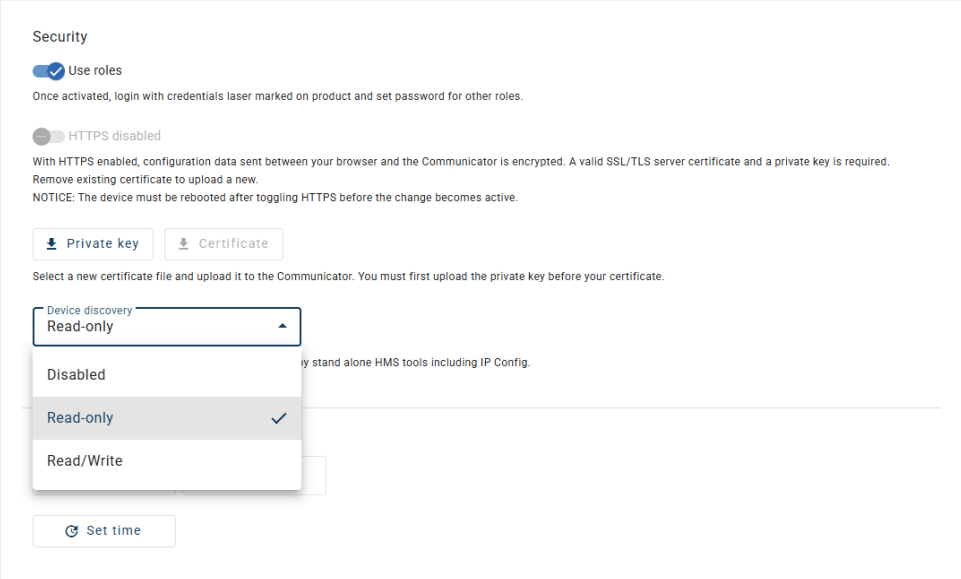


Figure 38. System page, Security settings, and Device discovery menu options

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.

9.4. I/O Configuration

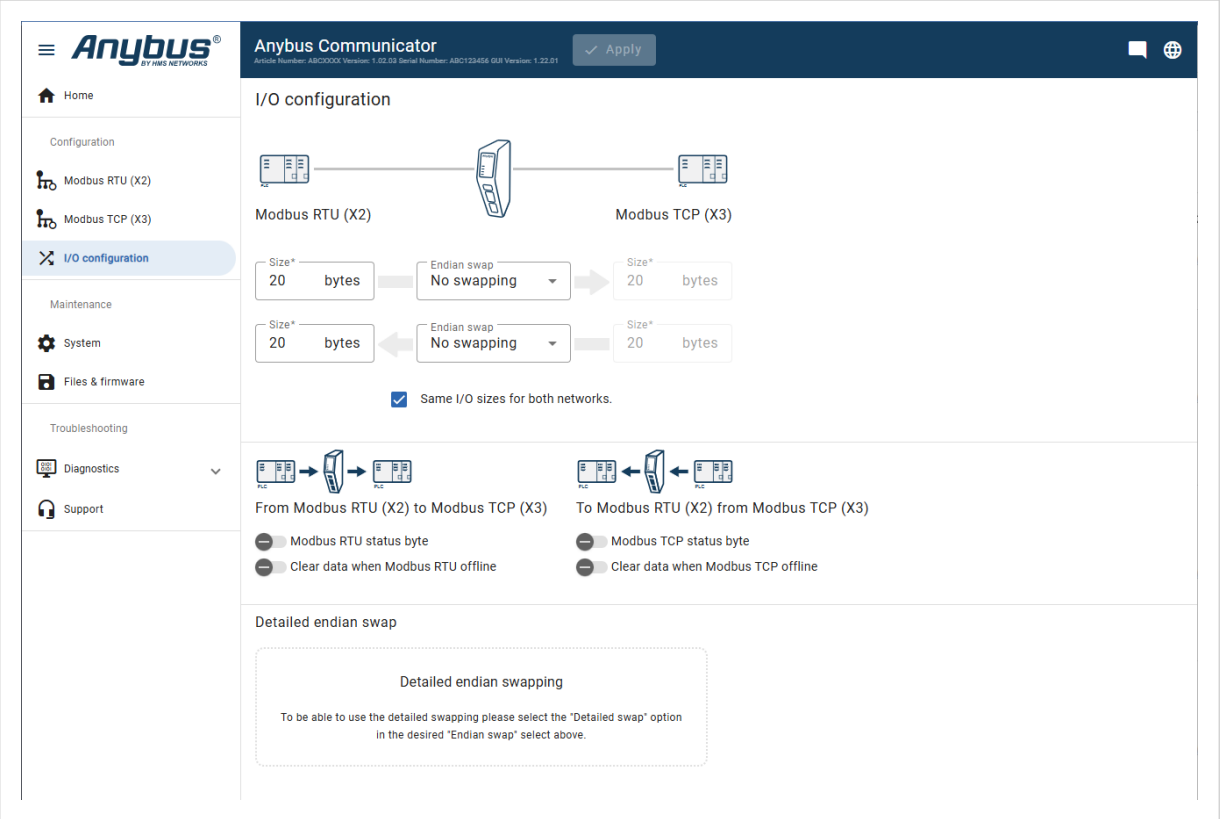


Figure 39. I/O configuration page

Enter the desired **Size** for the network input data and output data.

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

To configure different sizes for the networks, deselect the **Same I/O sizes for both networks** checkbox.

9.4.1. Endian Swap

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

About Endianness

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

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

9.4.2. Convert Between Big-Endian and Little-Endian

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

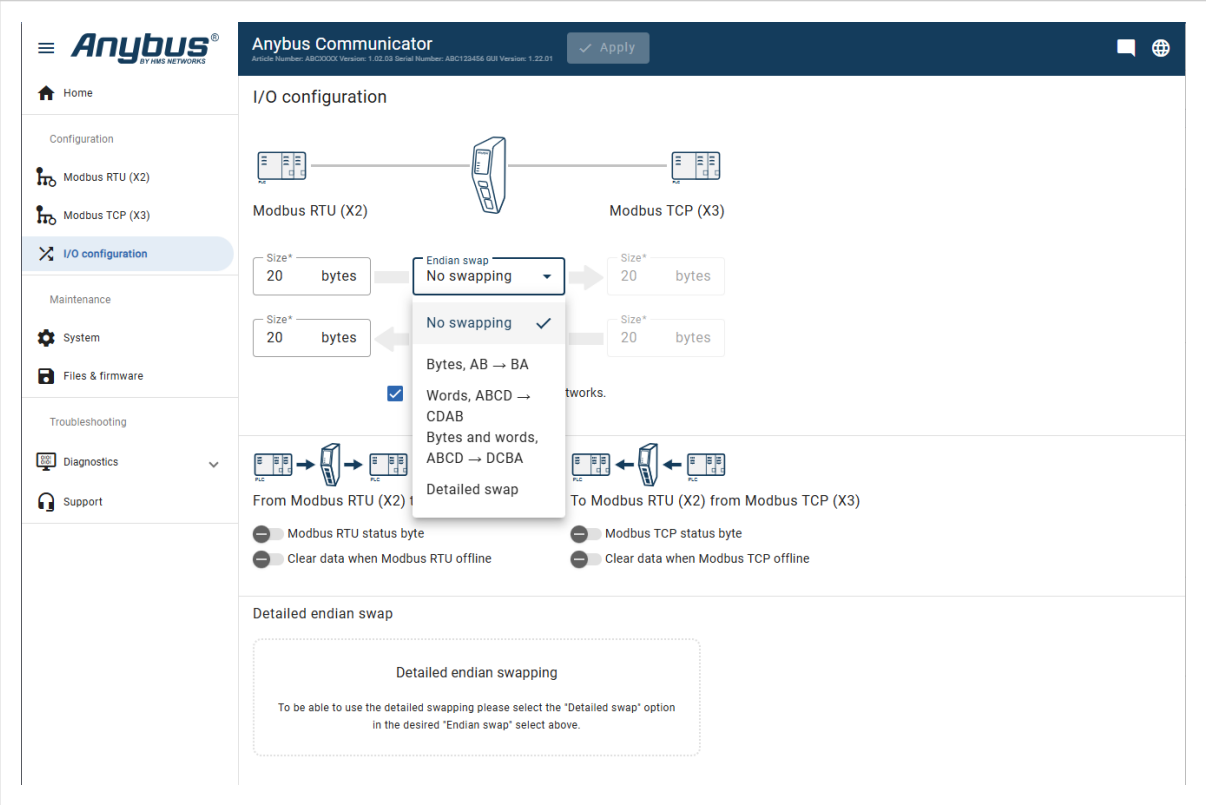


Figure 40. **I/O configuration** page, Endian swap

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
Detailed swap	With Detailed swap, you can select a Endian swap method for each byte in the I/O Configuration. Set the endian swap type **No swap**, **Bytes, AB → BA**, **Word swap, ABCD → CDAB** or **Bytes and words, ABCD → DCBA** for each bite. See Build Detailed Endian Swap (page 54).

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

9.4.3. Build Detailed Endian Swap

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

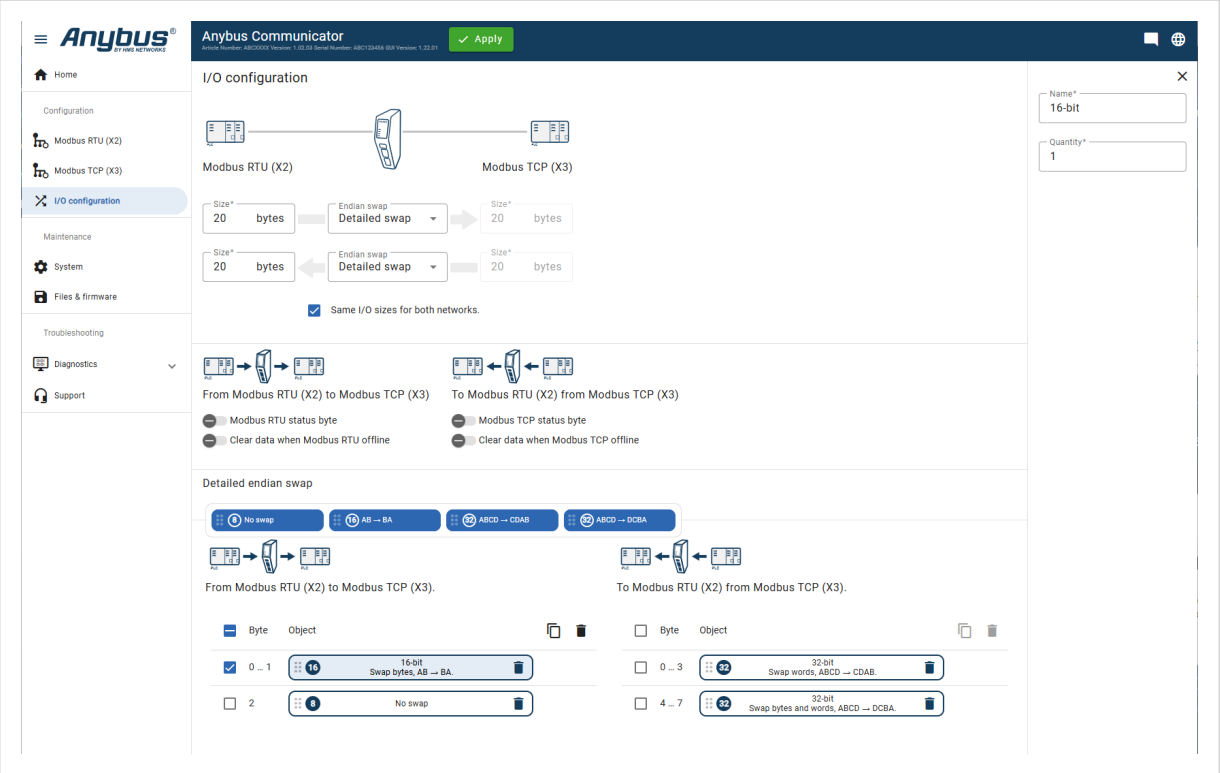


Figure 41. Detailed endian swap example

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

- To add an endian swap object: Drag and drop the desired endian swap object from the toolbar into the drag and drop fields.
- To duplicate an endian swap object: Select the checkbox in front of the endian swap object that you want to duplicate and click the **Duplicate selected** button.
  You can select multiple endian swap objects and duplicate the group.
- To change the order of the endian swap objects, drag and drop the endian swap objects in the list.

9.4.4. Process Data Settings

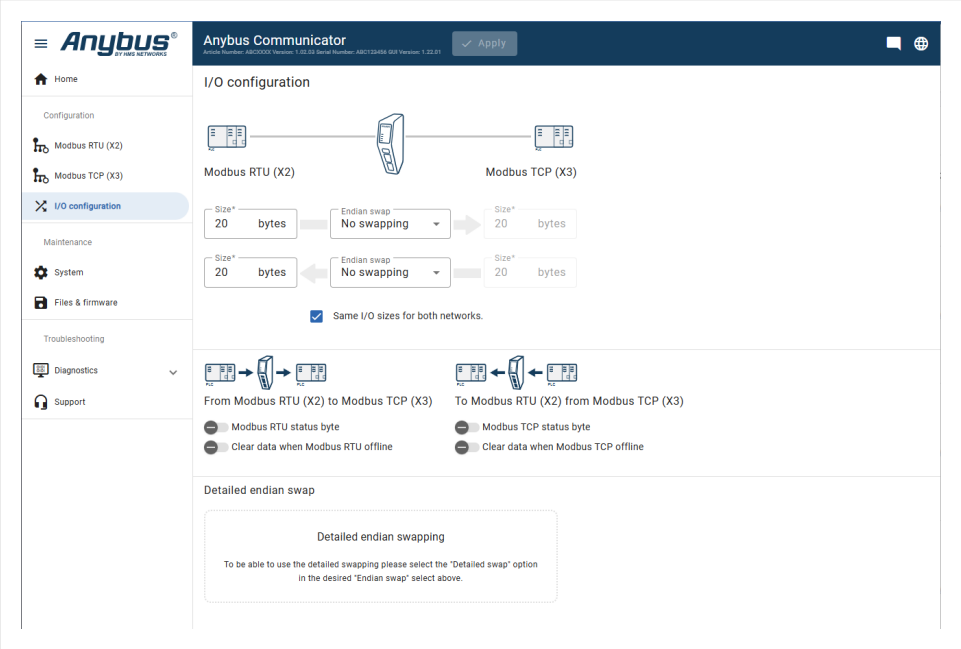


Figure 42. I/O configuration page

Status Byte

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

A status byte is used where a bit is:

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

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

By default the status byte settings are disabled.

To enable **Modbus RTU Server status byte** and/or **Modbus TCP status byte**, click the slide toggle(s).

Clear Data

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

By default the clear data settings are disabled.

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

9.5. Configuration Notes

You can add notes to describe the Communicator configuration.

9.5.1. Add Configuration Note

Procedure

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



Figure 43. Configuration note, comment icon

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

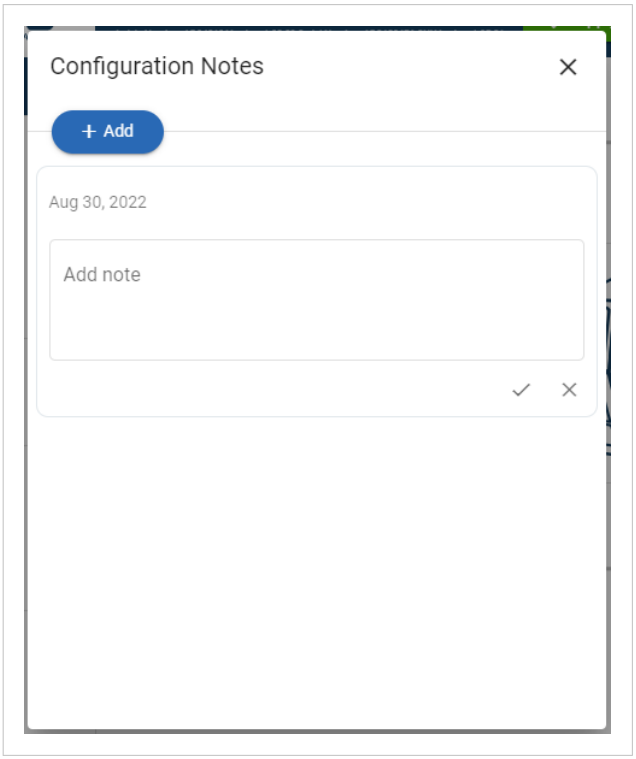


Figure 44. Add new configuration note

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

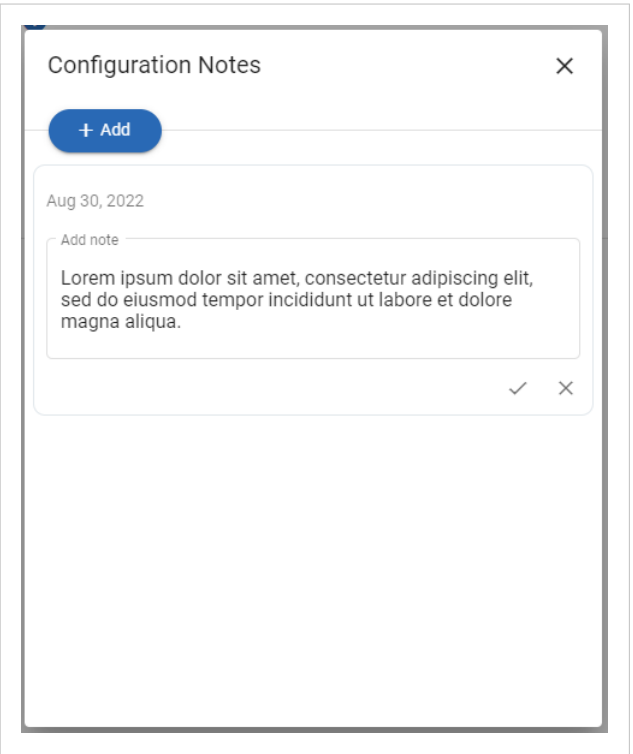


Figure 45. Write a configuration note

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.

9.5.2. View and Edit Configuration Notes

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

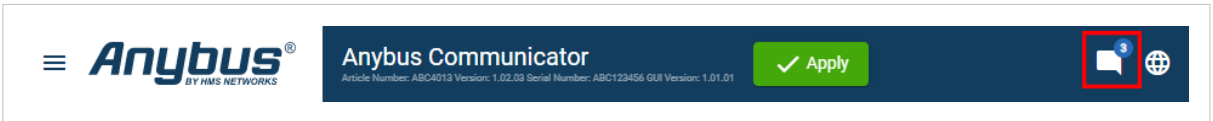


Figure 46. Example: The comment icon indicates that there are three added notes

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

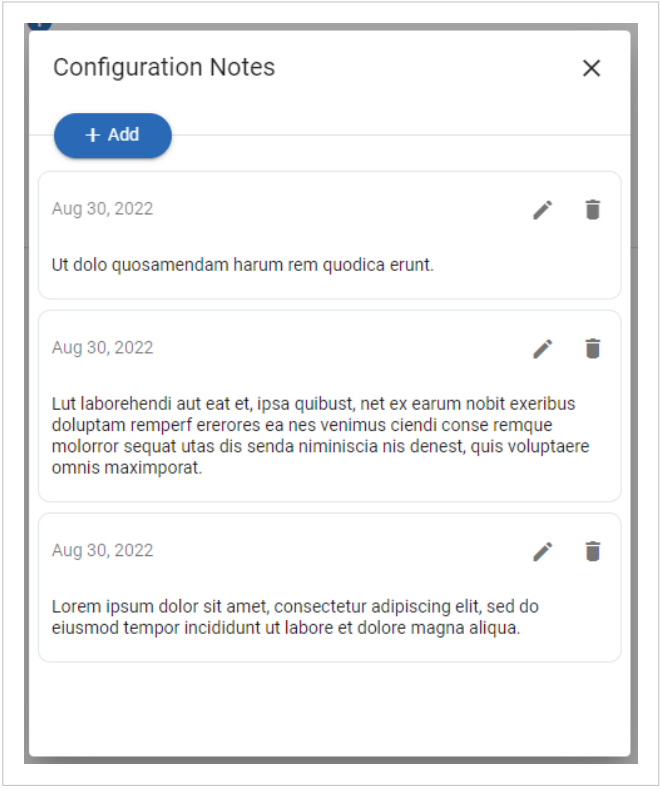


Figure 47. Example: The Configuration Notes window with added notes

9.6. Apply Configuration

Before You Begin

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

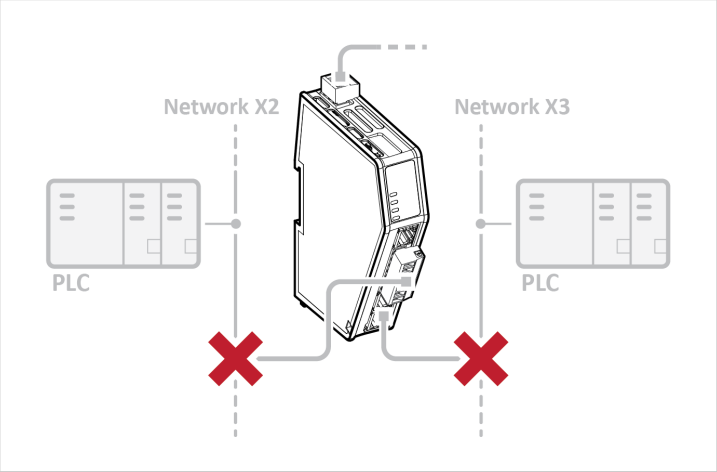


Figure 48. Disconnect the Communicator from the networks

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

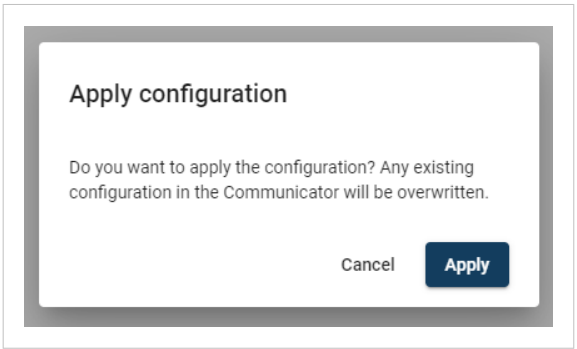
Procedure

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.



9.7. 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

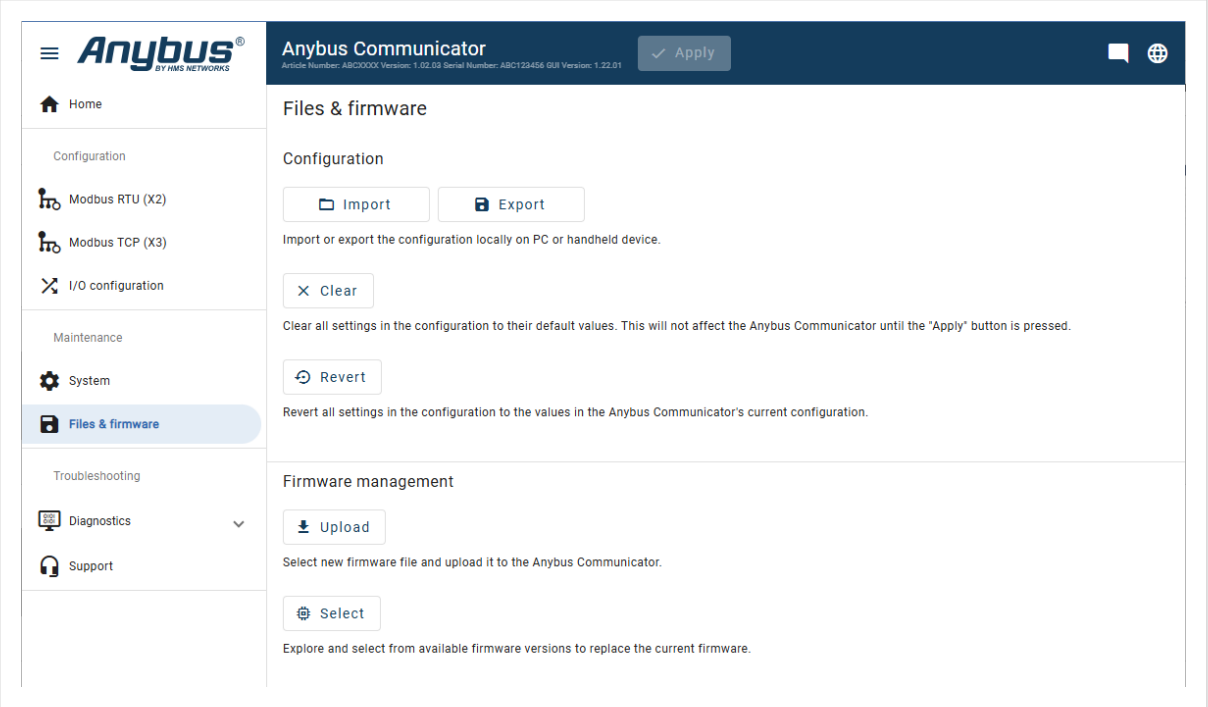


Figure 49. **Files & firmware** page

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. PLC Configuration

10.1. 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.

10.2. Modbus Addressing and Register Mapping

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

10.2.1. The Difference Between Address and Register Start

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

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

Example 1. Modbus Function Code 0x04 Read Input Registers

Table 1. Modbus client values

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

Example 2. Modbus Function Code 0x03 Read Holding Registers

Table 2. Modbus client values

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

10.2.2. 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 53).

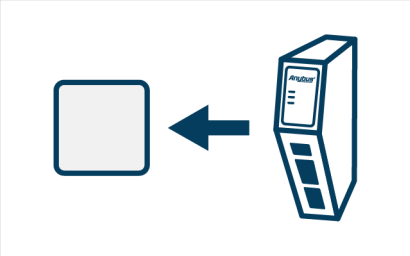
Idle Mode

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

10.2.3. Default Address Mode I/O Data Mapping

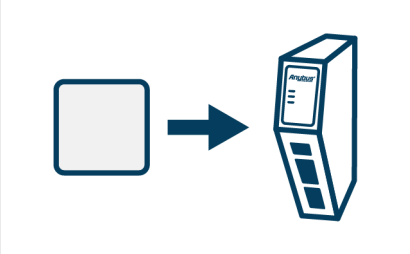
The following Modbus function codes are compatible with the default addressing mode.

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

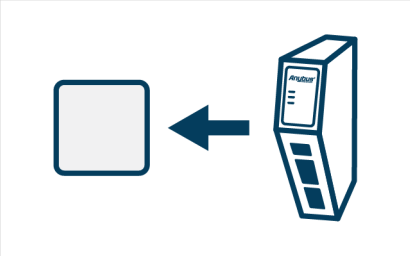


Process I/O data offset		Coil address		Holding register address	
HEX	DEC	HEX	DEC	HEX	DEC
0x0000 - 0x0001	0 - 1	0x0000 - 0x000F	0 - 15	0x0000	0
0x0002 - 0x0003	2 - 3	0x0010 - 0x001F	16 - 31	0x0001	1
...	...	...	...	...	...
0x05D8 - 0x05D9	1496 - 1497	0x2EC0 - 0x2ECF	11968 - 11983	0x02EC	748
0x05DA - 0x05DB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

10.2.4. Legacy Address Mode I/O Data Mapping

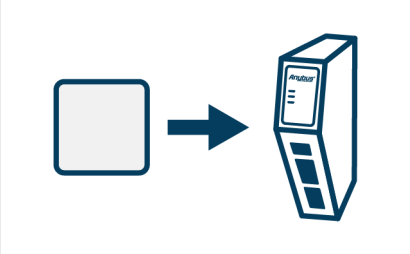
The following Modbus function codes are compatible with the Modbus **Use legacy mode** setting.

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

See Also

Legacy Mode For Anybus Address Mode | Modbus TCP (Page 40)

11. 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.

11.1. Communicator Status Monitor

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

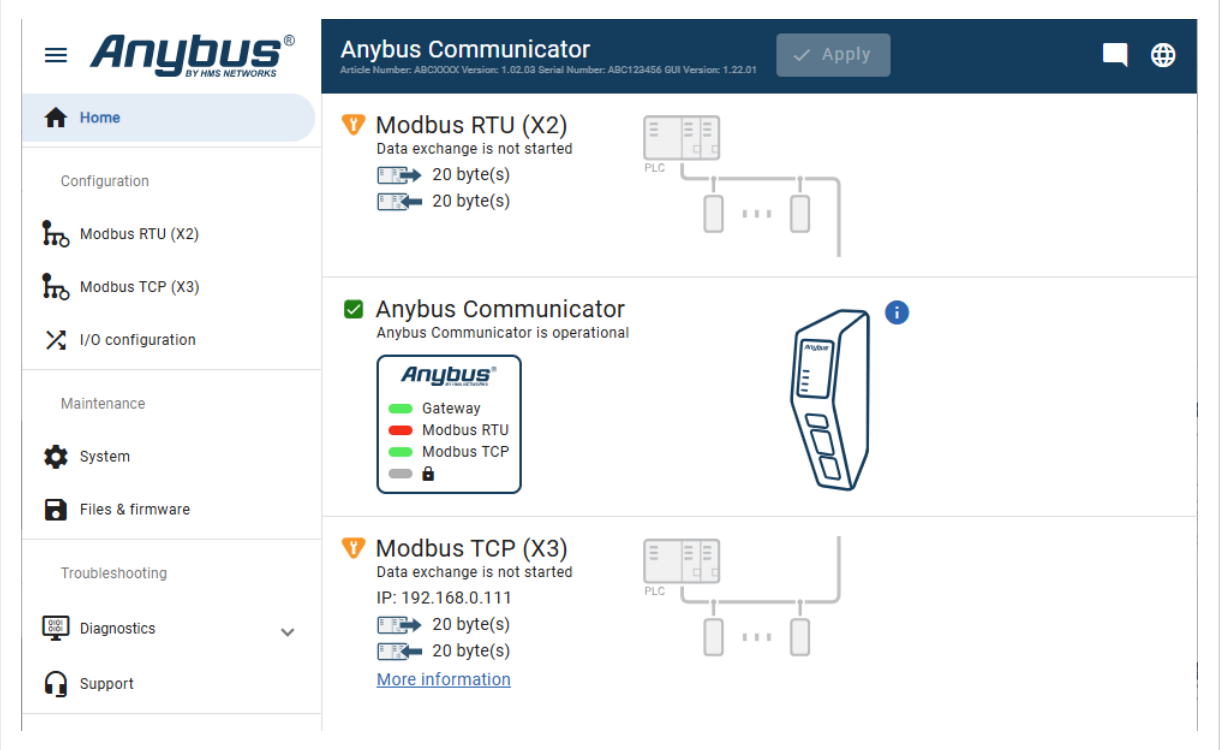


Figure 50. Home page

Gateway status

Overview the Communicator LED indications remotely.

Network Status and Settings

Overview communication status and the current networks settings.

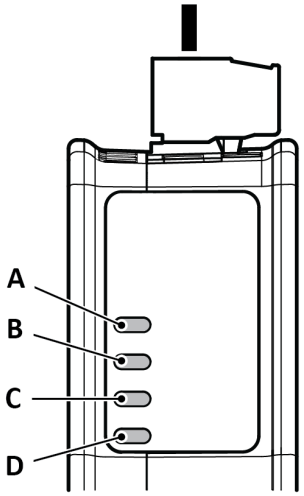
Status Symbols

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 RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)
Connect To Power (Page 19)
Communicator LED Indicators (Page 68)
LED Status (Page 84)
Firmware Upgrade Error Management (Page 88)

11.2. Communicator LED Indicators



A. **Gateway status**
B. **Modbus TCP**
C. **Modbus RTU Server**
D. **Security switch**

Gateway Status

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

Modbus RTU Server

Operation status	Description
Off	No power.
Green, flashing	Waiting for first Modbus RTU message.
Green, solid	At least one Modbus RTU message received.
Red, solid	Fatal event.
Red, flashing	Connection timeout. No Modbus RTU messages has been received within the configured process active timeout time.

Modbus TCP

Operation status	Description
Off	No power or no IP address.
Green, flashing	Modbus TCP online, no messages received.
Green, solid	Modbus TCP online, at least one message received.
Red, solid	IP address conflict detected.
Red, flashing	Connection timeout.

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 RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)
Connect To Power (Page 19)
Communicator Status Monitor (Page 66)
LED Status (Page 84)
Firmware Upgrade Error Management (Page 88)

11.3. Ethernet RJ45 LED Indicators

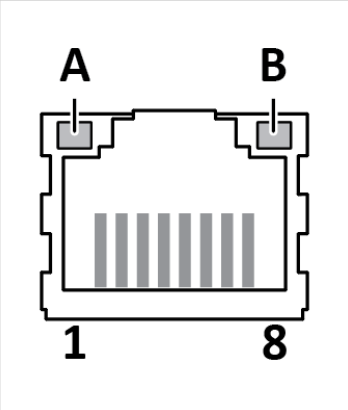


Figure 51. LED A. Activity LED B. Not used

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

12. Maintenance

12.1. Action on Fatal Error

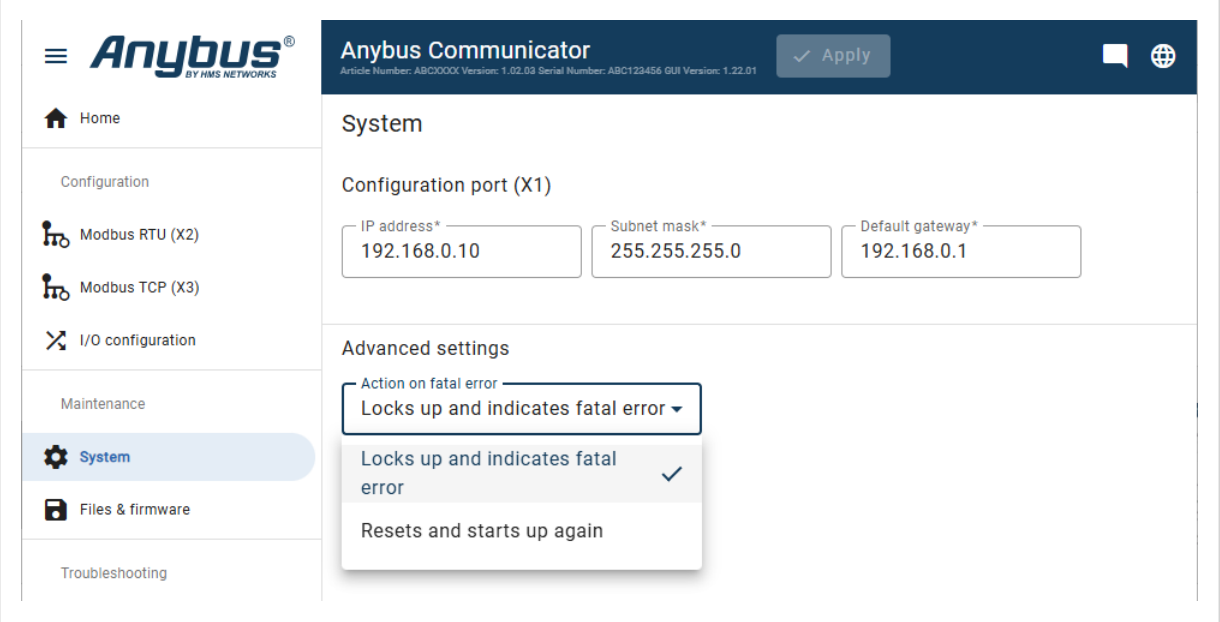


Figure 52. System page, Action on fatal error menu

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.

12.2. Configuration Port IP Settings

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

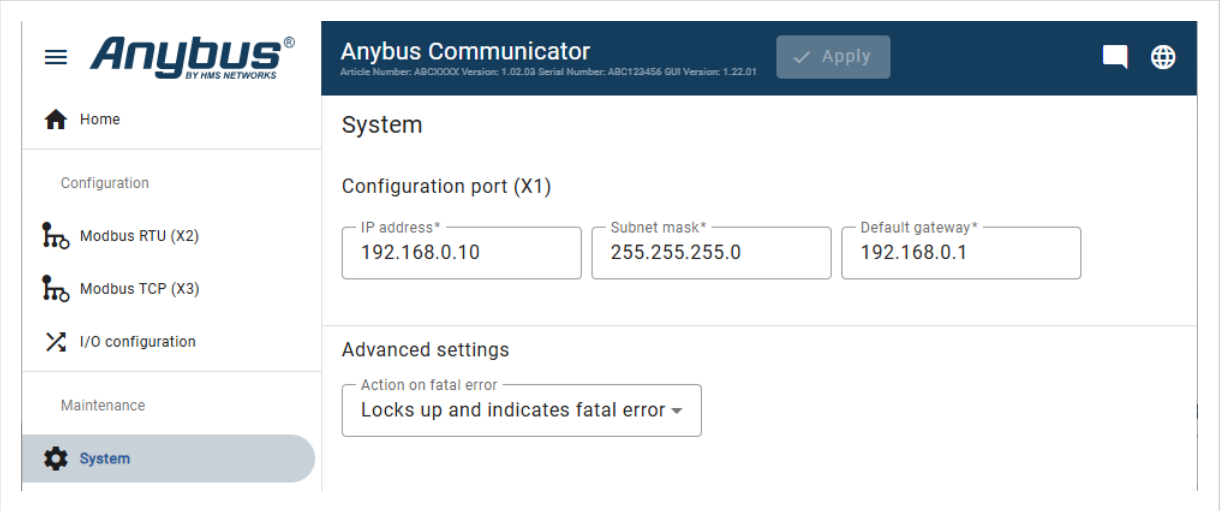


Figure 53. System page, Configuration port settings

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.

12.3. 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

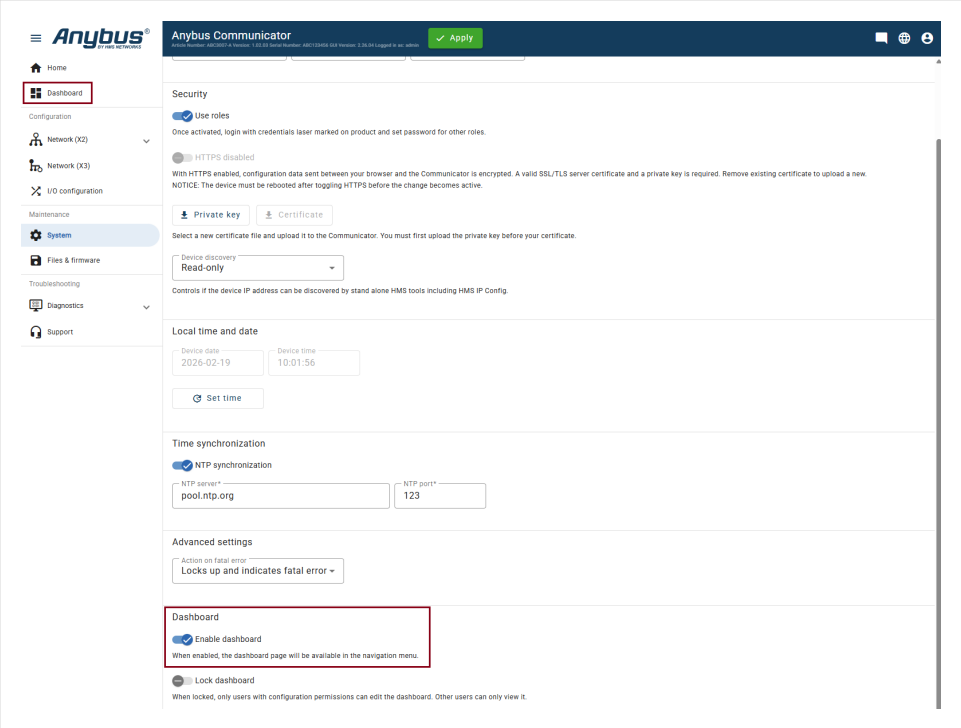


Figure 54. System page with Dashboard enabled and visible in the main menu

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 whant to desplay 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

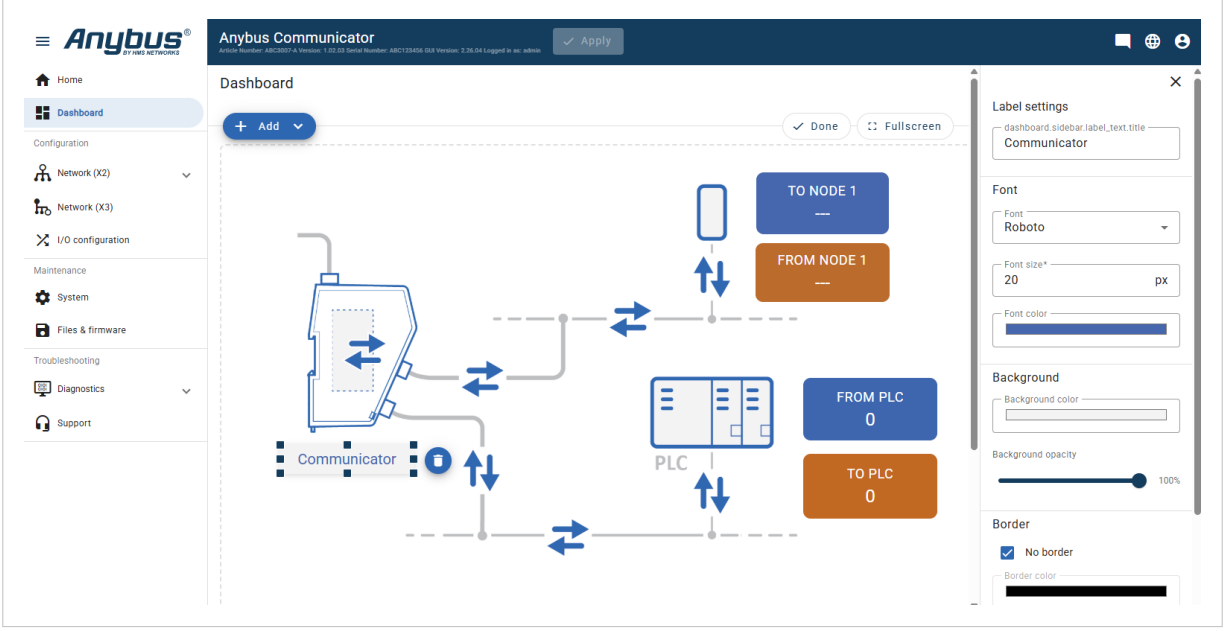


Figure 55. Dashboard example with added element

1. Navigate to the **Dashboard** page.
2. To enable edit mode, click **Edit**
3. To add and 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 opens.
4. Configure the settings. See Dashboard Elements and Settings (page 73).
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

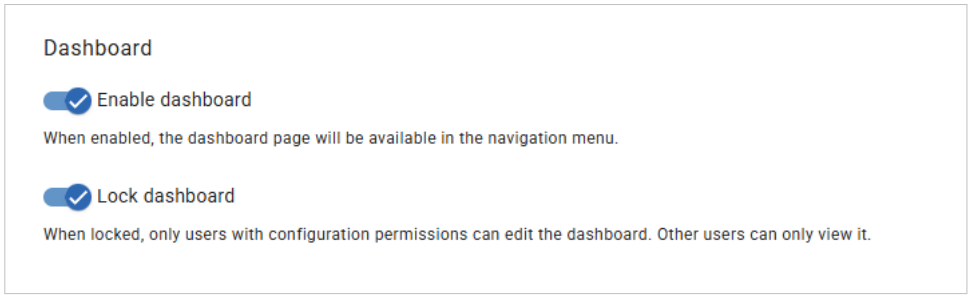


Figure 56. Dashboard enabled and locked

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

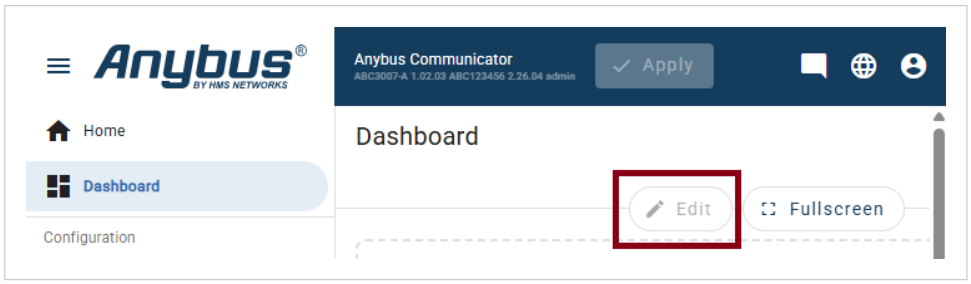


Figure 57. Dashboard locked

When locked:

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

12.4. Configuration File Handling

12.4.1. Export Configuration

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

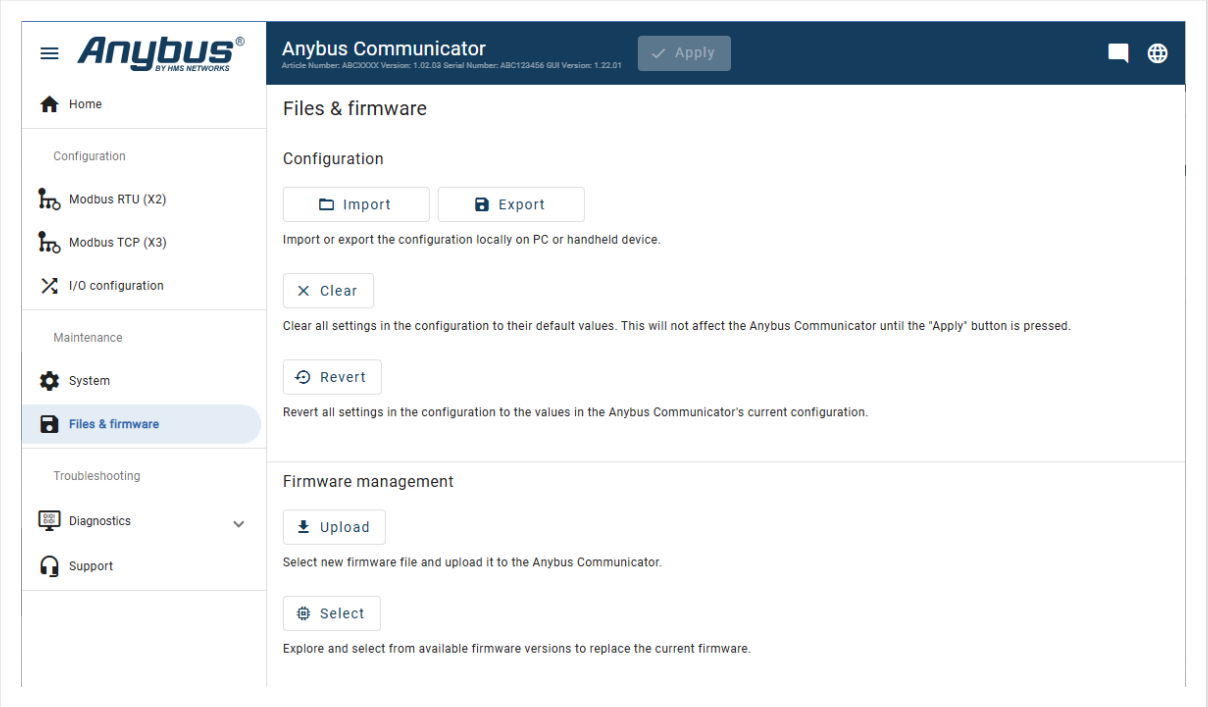


Figure 58. Files & firmware page

To export a configuration file:

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

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

12.4.2. 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

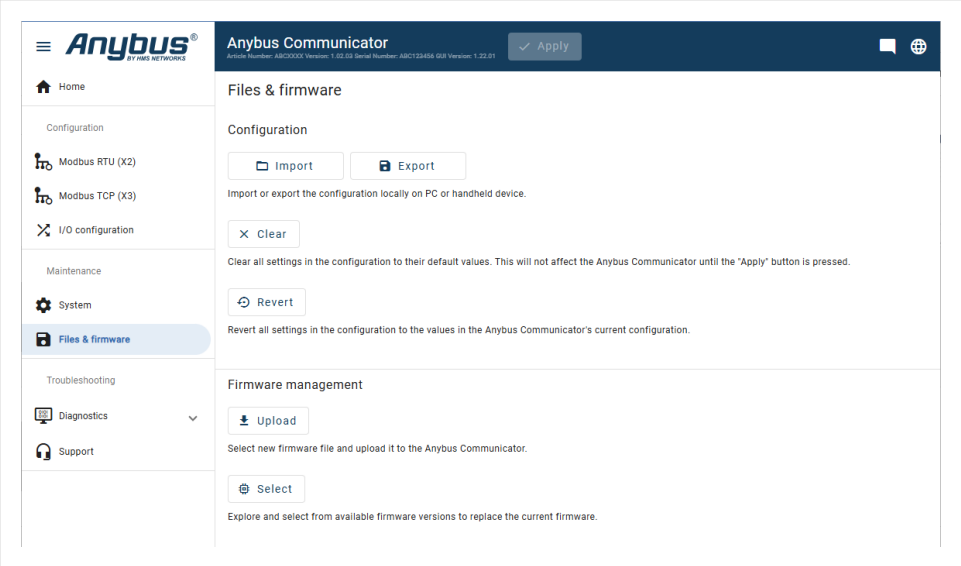


Figure 59. Files & firmware page

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.

12.5. Clear and Revert Configuration

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

Procedure

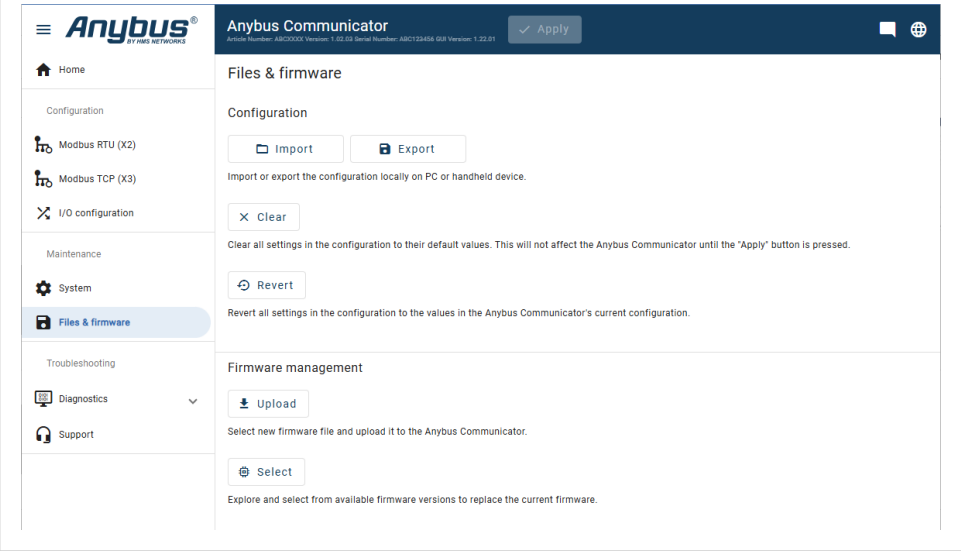


Figure 60. Files & firmware page

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.

12.6. Firmware Management

12.6.1. View the Firmware Version

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

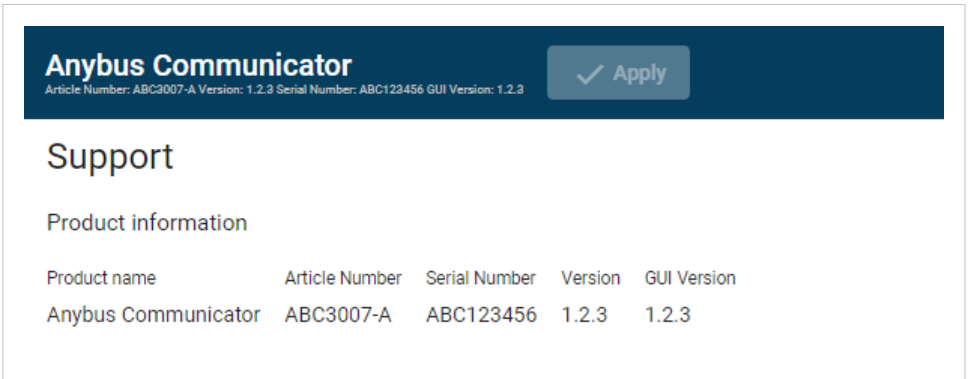


Figure 61. Support page, Product information example

12.6.2. 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.

12.6.3. 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.

12.6.4. Update Firmware

Before You Begin

Ensure to disconnect the Communicator from the OT networks.

Procedure

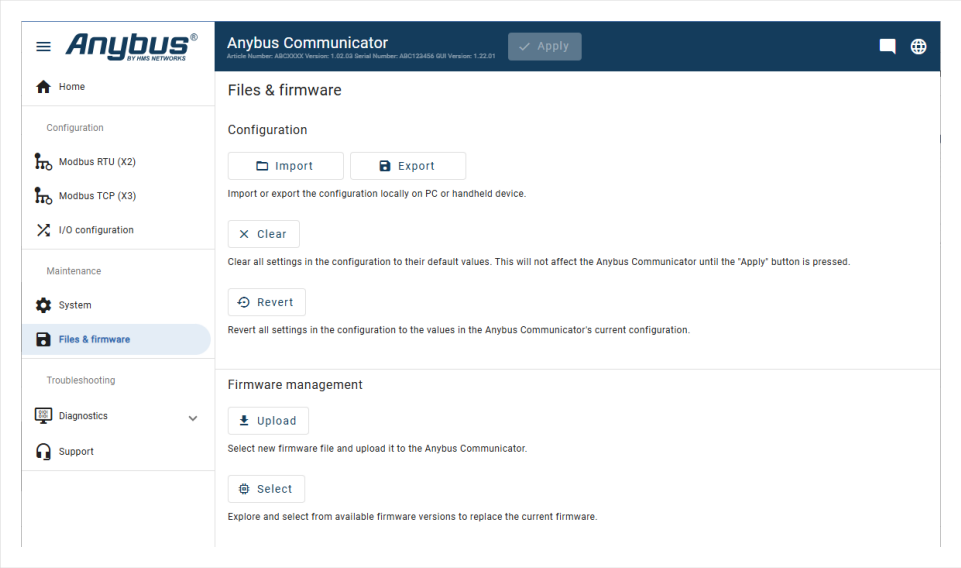


Figure 62. Files & firmware page

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.

12.7. 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 .

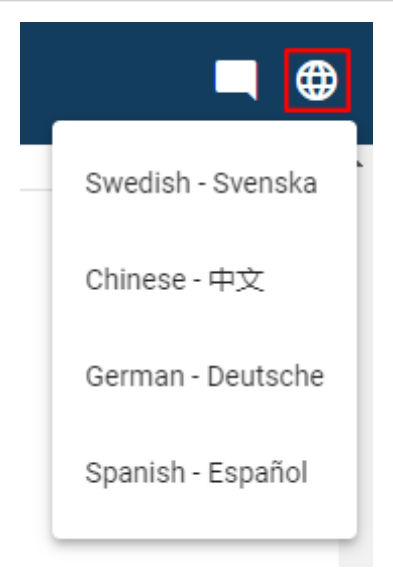


Figure 63. Language menu

2. Select a new language from the list.

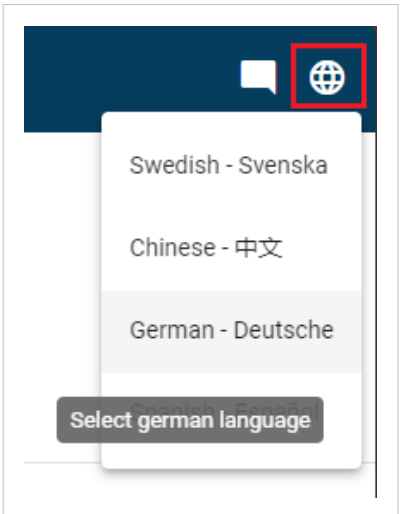


Figure 64. Example: Change language to German

The language change takes effect immediately.

13. Troubleshooting

13.1. Diagnostics

13.1.1. I/O Data

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

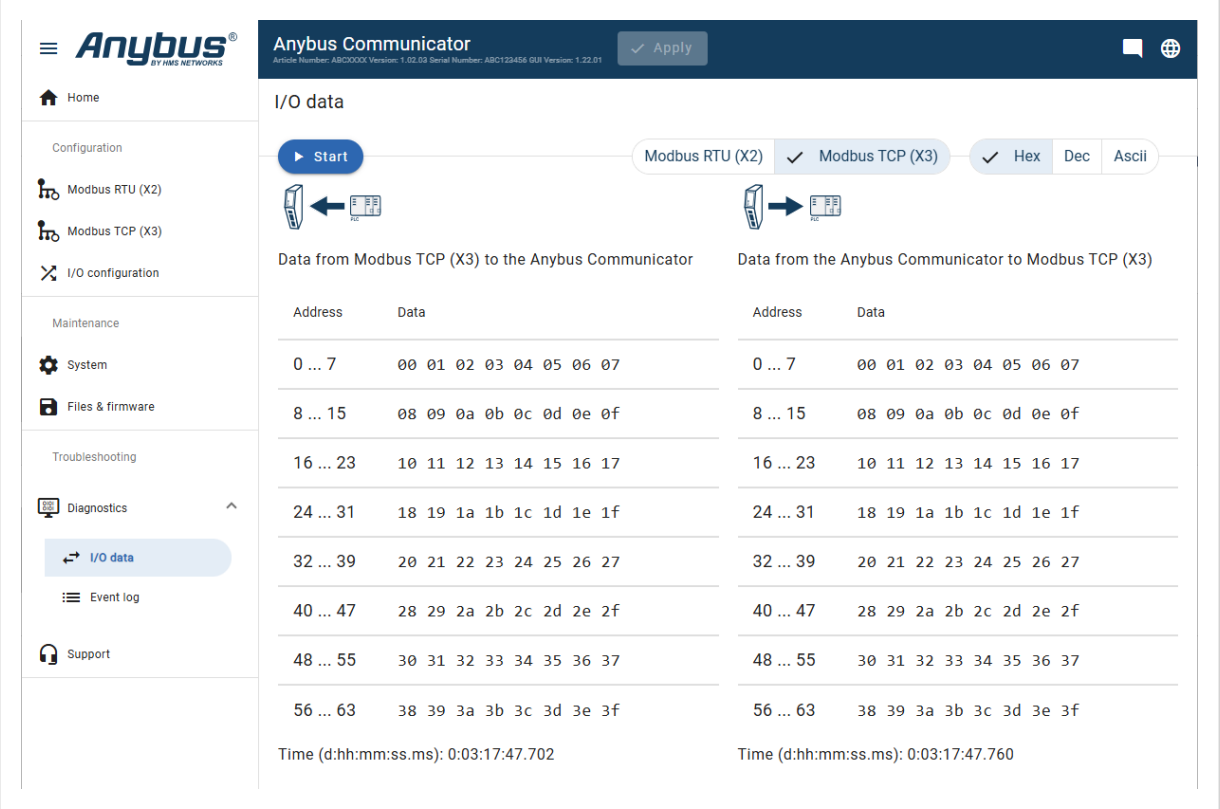


Figure 65. I/O data

I/O data is updated twice every second.

Switch between the OT networks

To switch between the networks, select **Modbus RTU Server** or **Modbus TCP**.

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**.

13.1.2. Event Log

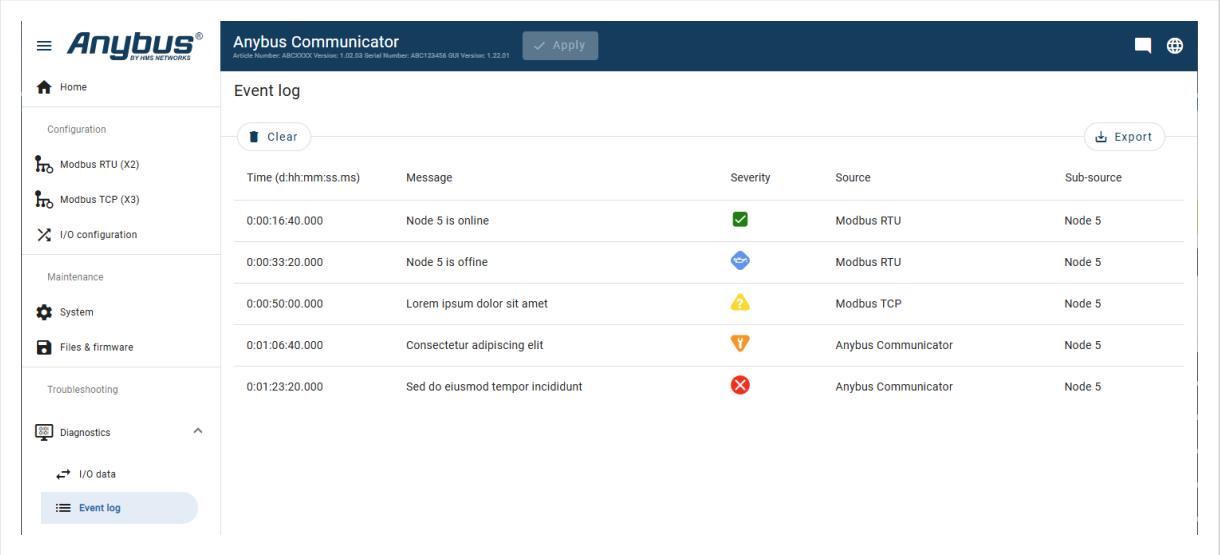


Figure 66. Event log page example

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 RTU
	Modbus TCP
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**.

13.1.3. LED Status

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

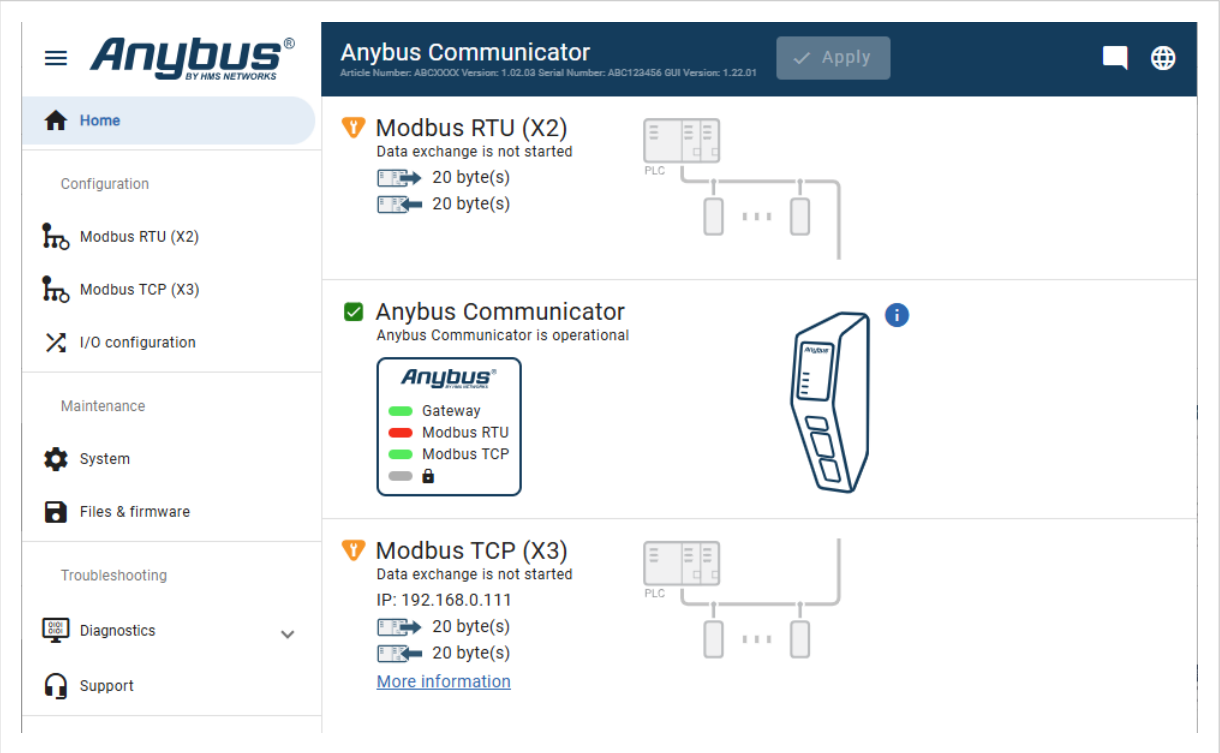


Figure 67. Home page

See Also

Connect To Modbus RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)
Connect To Power (Page 19)
Communicator Status Monitor (Page 66)
Communicator LED Indicators (Page 68)
Firmware Upgrade Error Management (Page 88)

13.2. 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.

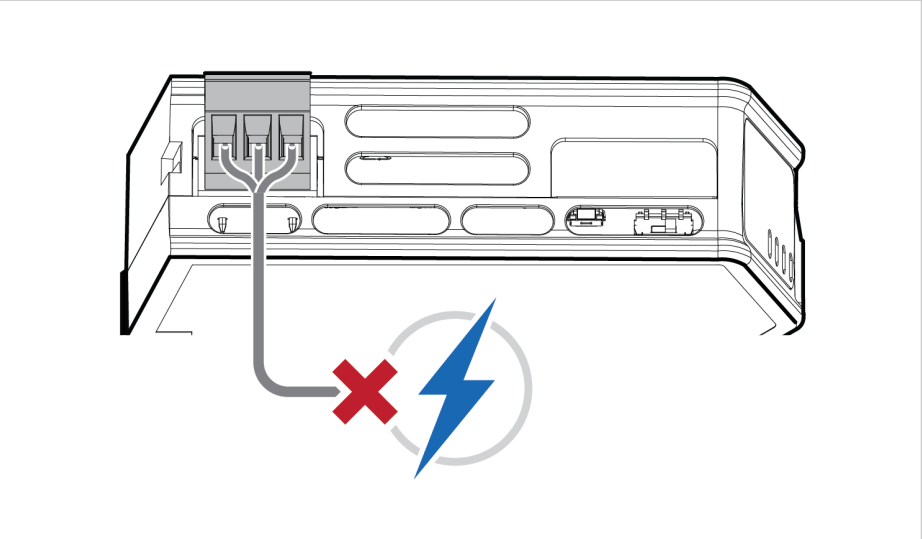


Figure 68. Disconnect power

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

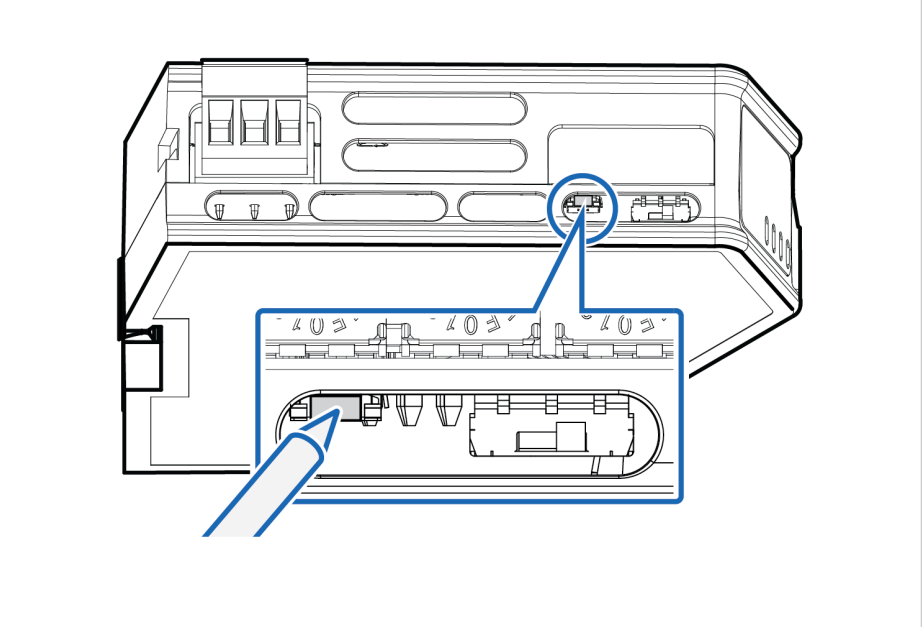


Figure 69. Press and hold **Reset** button

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

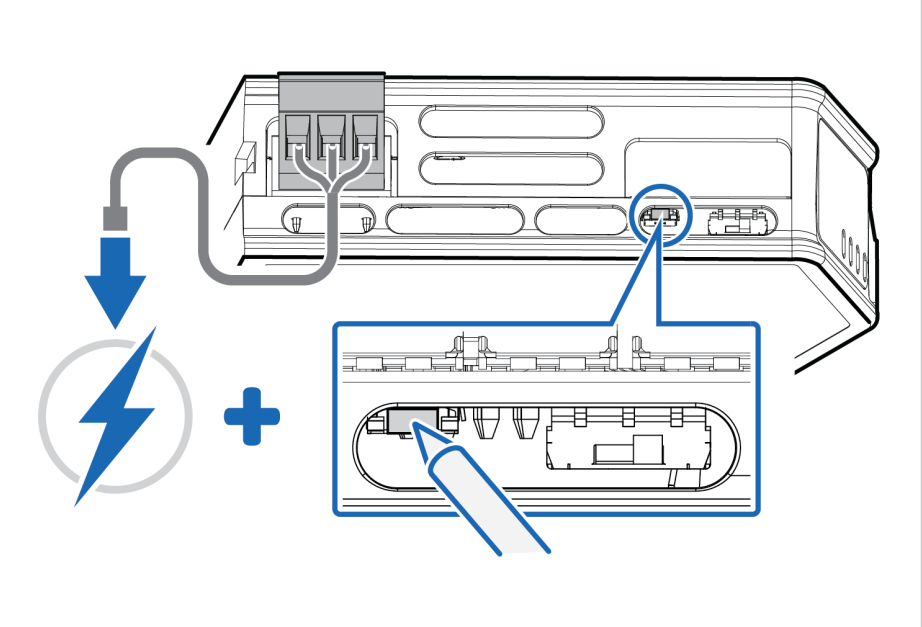


Figure 70. Hold **Reset** button and reconnect power

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**.

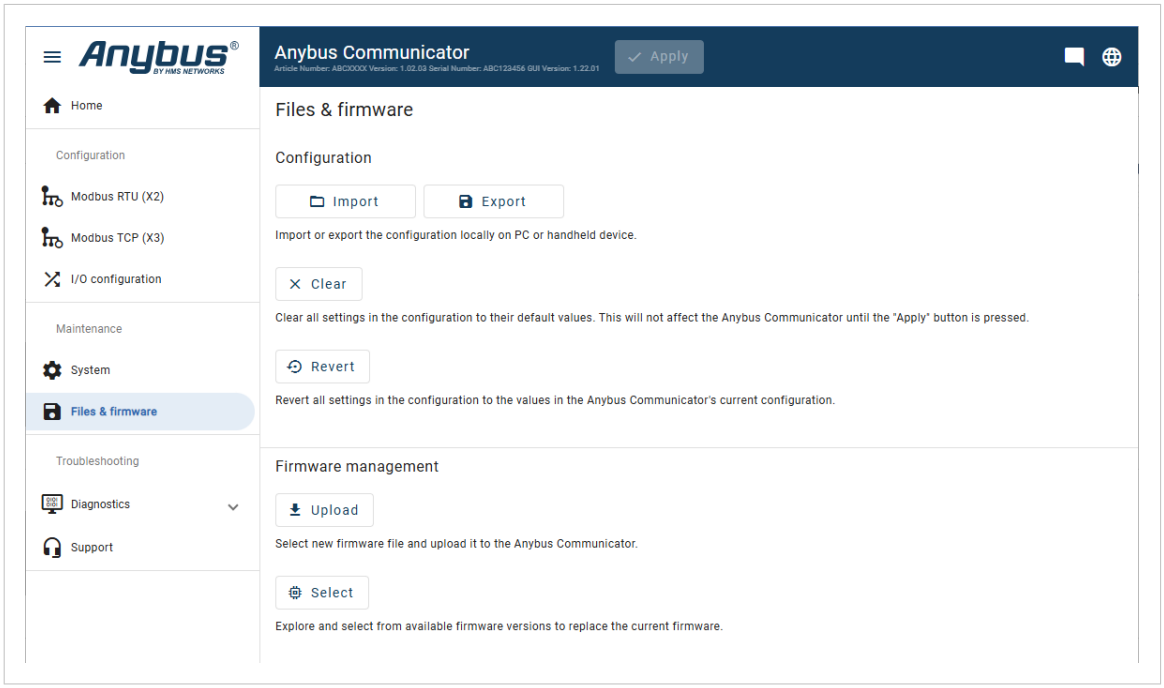


Figure 71. Files & firmware, Revert

13.3. 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.

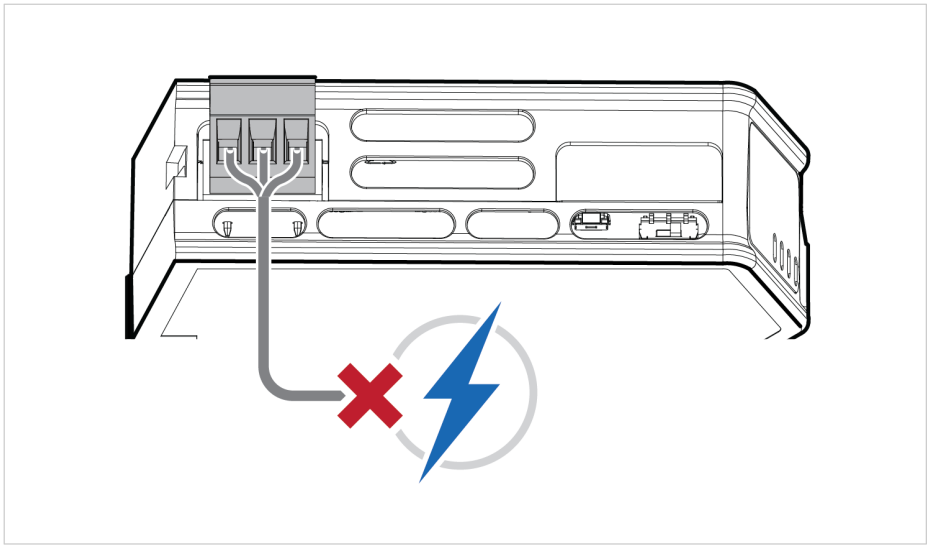


Figure 72. Disconnect power

2. Reconnect the Communicator to power.

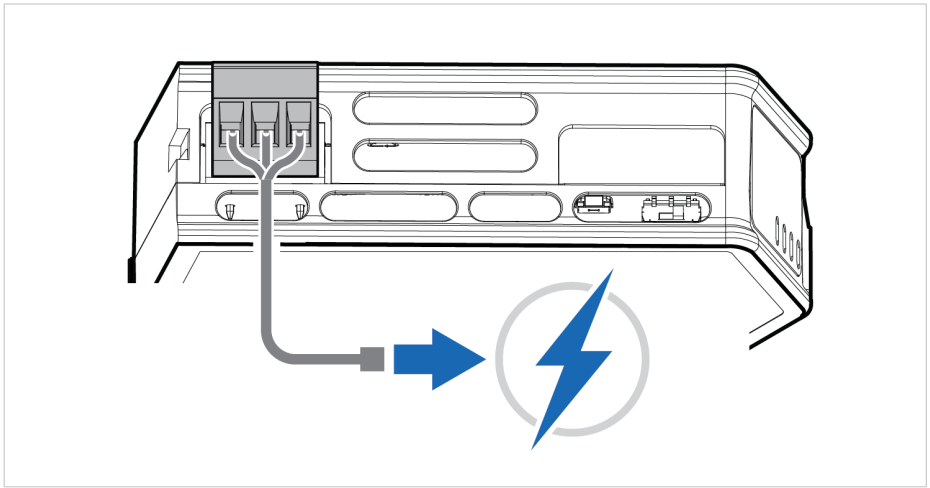


Figure 73. Reconnect power

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

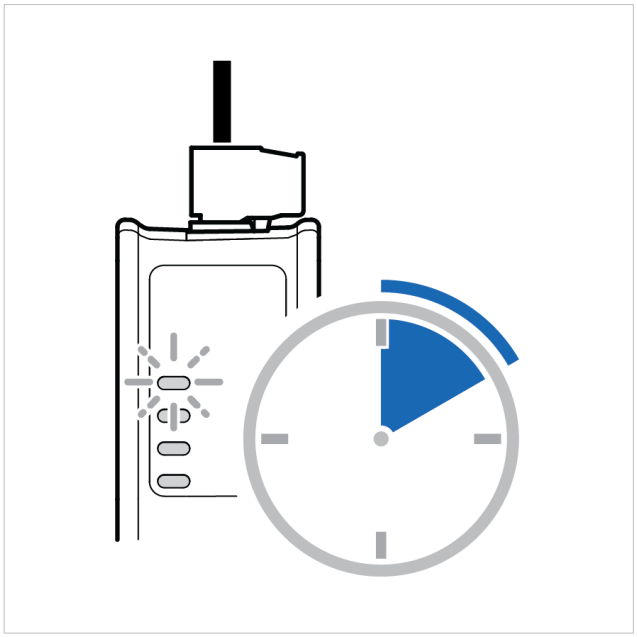


Figure 74. Firmware upgrade LED indication

Result

The Communicator recover and return to normal operation.

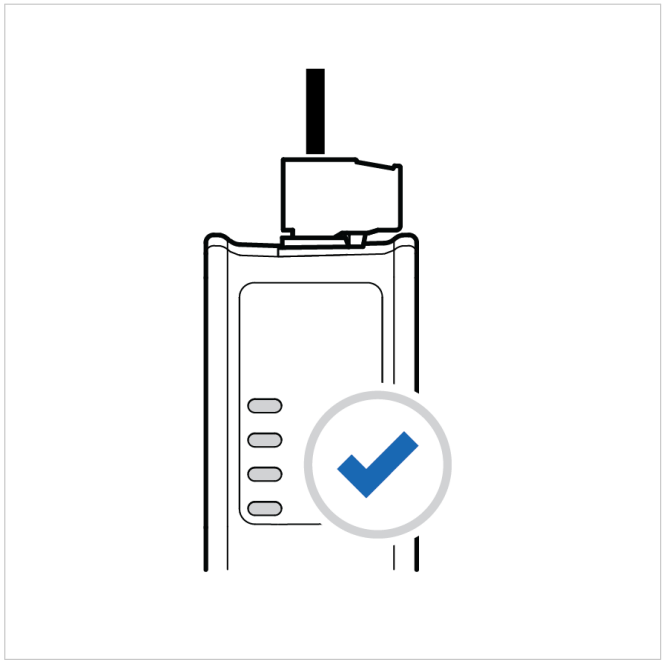


Figure 75. Recover and return to normal operation

See Also

Connect To Modbus RTU Network (Page 15)
Connect To Modbus TCP Network (Page 17)

Connect To Power (Page 19)
Communicator Status Monitor (Page 66)
Communicator LED Indicators (Page 68)
LED Status (Page 84)

13.4. Support

13.4.1. Support Package

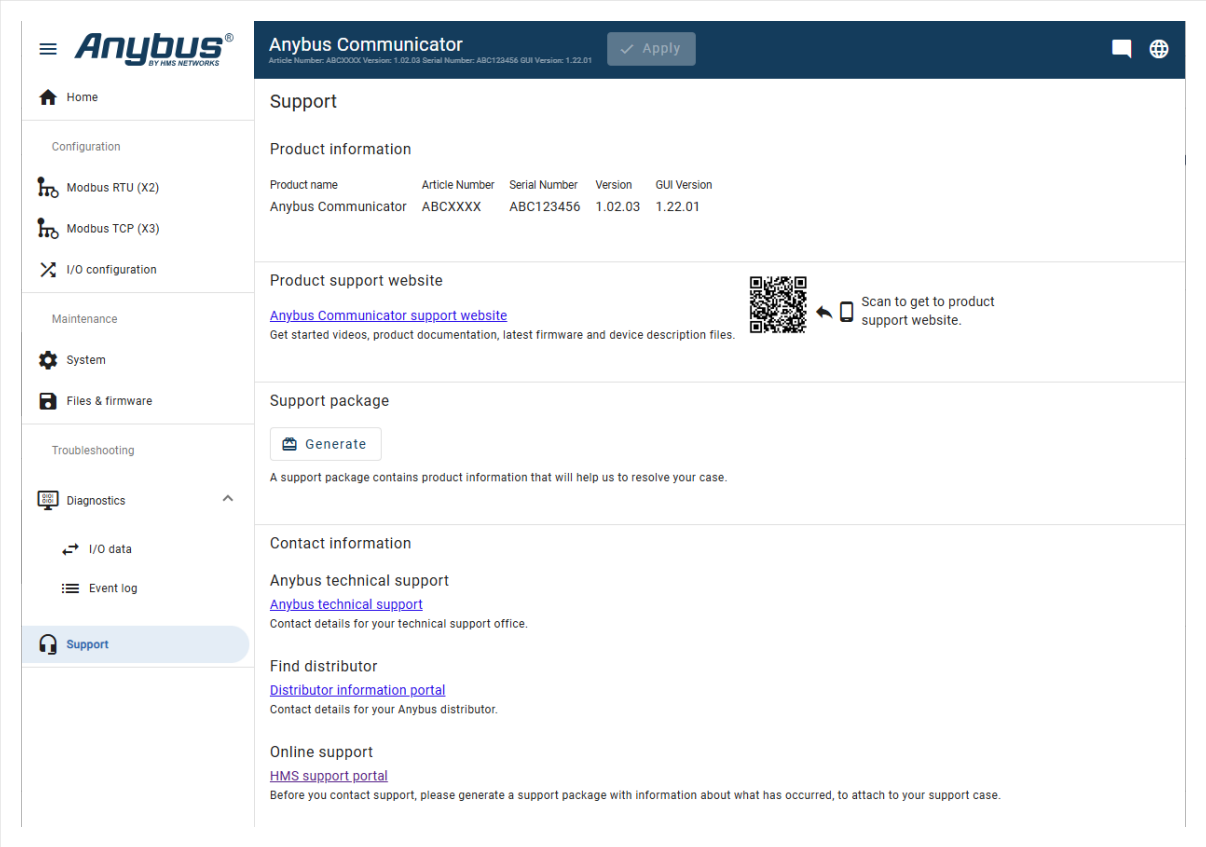


Figure 76. Support page example

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.

14. Technical Data

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

14.1. Technical Specifications

Article identification	ABC4025
Configuration connector	RJ45
Upper connector	7-pin screw connector
Lower 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

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 85).

16. Reference Guides

16.1. About Input Registers and Holding Registers

Modbus data is most often read and written as registers which are 16-bit pieces of data.

Holding registers and Input registers are both 16-bit registers.



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

Input Registers

Input registers can only be read.

Holding Registers

Holding registers can be read or written.

These registers can be used for a variety of things such as inputs, outputs, configuration data, or other requirement for holding data.

16.2. Modbus Data Model

Discrete Inputs	Single bit	Read-Only	Data can be provided by the I/O system.
Coils	Single bit	Read-Write	Data can be alterable by the application program.
Input Registers	16-bit word	Read-Only	Data can be provided by the I/O system
Holding Registers	16-bit word	Read-Write	Data can be alterable by the application program.

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

For more information refer to the Modbus organization website.

16.3. 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.
43/14	Read Device Identification	N/A	0x2B/0x0E	Read the vendor name, product code (article number), firmware version, vendor URL and product name.

16.4. Modus Exception Codes

Exception Code	Name	Description
01	Illegal Function	The server does not recognize or permit the function code.
02	Illegal Data Address	The data address (register, discrete input or coil number) is not an permitted address for the server. If multiple registers were requested, at least one was not permitted.
03	Illegal Data Value	A value in the query data field is not allowed by the server. This indicates there is a problem with the structure of the rest of the request, such as an incorrect implied length.

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

For more information refer to the Modbus organization website.