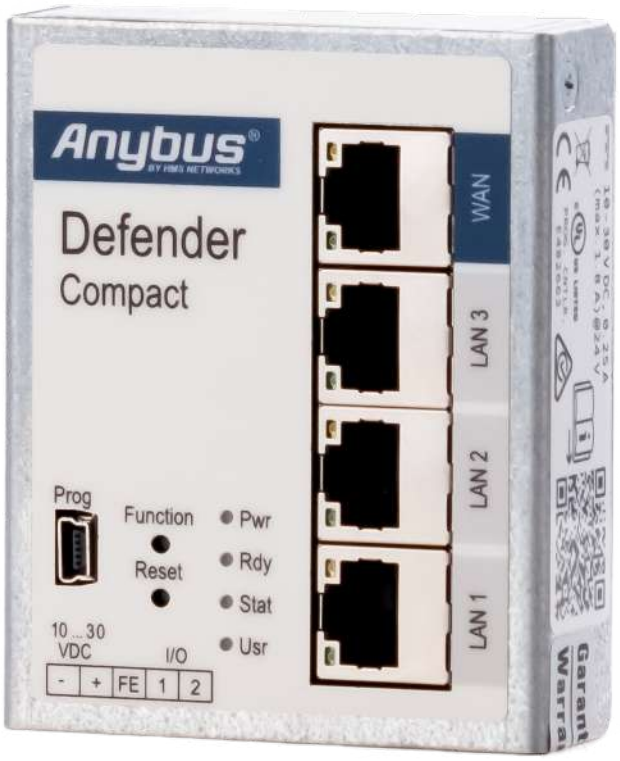
ENGLISH

Anybus® Defender Compact
User Manual

ABD1004-NATFW
Version: 2.1.0
Publication date 2025-07-22



Important User Information

Disclaimer

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

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

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

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden
E-Mail: info@hms.se

Table of Contents

1 Preface

1.1 About This Document

This document describes how to install and configure Anybus® Defender Compact.

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

1.2 Document Conventions

1.2.1 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

1.2.2 User Interaction Elements

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

1.2.3 Program Code and Scripts

```
Program code and script examples
```

1.2.4 Cross-References and Links

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

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

1.2.5 Safety Symbols

In the present operating instructions, the following symbols / warnings are used:

ADVICE	An advice signifies additional information and indications such as cyber-security that assists in the assured handling with the system.
	This symbol indicates a possible risk of damage to hardware and / or software.

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.

1.2.5.1 Information Symbols

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

TIP
Helpful advice and suggestions.

1.3 Trademarks

Anybus® is a registered trademark of HMS Networks.

All other trademarks are the property of their respective holders.

1.4 Use of open-source software

1.4.1 General

Our products include, among other things, open-source software, which is manufactured by a third party and has been published for free use by anyone. The open-source software is available under special open-source software licenses and copyright of third parties. In principle, each customer can use open-source software free of charge under the license terms of the respective manufacturers. The customer's right to use the open-source software for purposes other than those for which our products were intended is regulated in detail by the relevant open-source software licenses. The customer may freely use the open-source software as set out in the respective valid license, beyond the intended purpose of the open-source software in our products. In the event that there is a contradiction between the licensing terms of one of our products and the respective open-source software license, the respective applicable open-source software license shall take priority over our licensing terms if the respective open-source software is affected by this.

Use of the open-source software is free of charge. We do not charge any usage fees or similar charges for the use of open-source software included in our products. Customer use of open-source software in our products is not part of the profit that we obtain from the contractual remuneration. All open-source software programs contained in our products are in the available list. The most important open-source software licenses are listed in the Licenses section at the end of this publication.

If programs that are included in our products are under the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), the Berkeley Software Distribution (BSD), the Massachusetts Institute of Technology (MIT), or other open-source software license, which requires that the source code be made available, and this software was not already supplied with our product on a disk or in the source code, we will send this at any time upon request.

Requests must, where possible, be sent to the following address with the product's serial number:

HMS Networks AB

Stationsgatan 37, Box 4126

300 04 Halmstad

SWEDEN

Tel.: +46 35 17 29 56

sales@hms.se

www.hms-networks.com

1.4.2 Special liability provisions

We assume no responsibility or liability if the open-source software programs included in our products are used by customers in a manner that no longer corresponds to the purpose of the contract which serves as the basis for the purchase of our products. This applies in particular to any use of the open-source software programs outside of our products. The warranty and liability provisions, which stipulate the applicable open-source software license for the corresponding open-source software, as listed below, apply to the use of open-source software beyond the contractual purpose. In particular, we are also not liable if the open-source software in our products or the entire software configuration in our products is changed. The warranty contained in the contract, which forms the basis for the purchase of our products, applies only to unchanged open-source software and the unchanged software configuration in our products.

1.4.3 Open-source software used

For a list of the open-source software used in our products, visit

https://www.hms-networks.com/p/abd1004-natfw-anybus-defender-compact-1004-nat-fw?tab=tab-support

On the same URL a machine readable SBOM (Software Bill of Material) file is available in json format.

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.

- The device is built to the latest technological standards and recognized safety standards (see Declaration of Conformity).
- The device must be installed in a dry location. No liquid must be allowed to get inside the device, as this could result in electric shocks or short circuits.
- The device is for indoor use only.
- Never open the device chassis. Unauthorized opening and improper repair can pose a danger to the user. Unauthorized modifications are not covered by the manufacturer's warranty. Opening the device voids the warranty.
- The device must be disposed of in line with European regulations and German legislation on electronics and electronic devices and not in general household waste. The device should be disposed of accordingly.

3 Legal notice

3.1 Qualified personnel

The product/system described in this documentation may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are persons who, due to their training, experience, instruction in and knowledge of the relevant standards, regulations and accident prevention regulations have been authorized by the person responsible for the safety of the machine to carry out the required activities and who have the ability to recognize and avoid potential hazards.

3.2 Intended use

The device should only be used as described in the manual.

3.3 Limitation of liability

All technical information, data and notes about installation, operation and maintenance contained in the operating instructions are provided under consideration of our previous experience and findings to the best of our knowledge. No claims may be derived from the information, figures and descriptions in this operating manual. HMS Networks assumes no liability for damages due to:

- Non-compliance with these instructions
- unintended use
- technical changes

Subject to content and technical modifications.

4 Information on cyber security

To prevent unauthorized access to facilities and systems, observe the following security recommendations:

4.1.1 General

- Periodically ensure that all relevant components meet these recommendations and any additional internal security policies.
- Perform a security assessment of the entire system. Use a cell protection concept with suitable products.

  For example, "ICS-Security-Kompendium" from the BSI (Federal Office for Security in Information Technology, Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html

  Short URL: http://bit.ly/3Ya4tTH

4.1.2 Physical access

Restrict physical access to security-relevant components to qualified personnel.

4.1.3 Security of the software

Keep software/firmware updated.

- Stay informed about security updates for the product.
- Stay informed about product updates.

You can find information about this at:

4.1.4 Passwords

Define rules for the use of the devices and assigning passwords.

Change passwords regularly, to increase security.

Use only passwords with a high password strength. Avoid weak passwords such as "password1", "123456789".

Make sure that all passwords are protected and inaccessible to unauthorized personnel.

Do not use the same password for different users and systems.

4.1.5 Dealing with security incidents

In order to be able to respond appropriately to any reports of potential cybersecurity vulnerabilities, HMS Networks has established appropriate processes and measures.

Information about current threats and the associated product security of our devices and software solutions can be found at https://www.hms-networks.com/cyber-security.General

4.1.6 Purpose of this documentation

This document describes the procedure for accessing the industrial firewall ***Anybus Defender Compact*** NFH100 via SSH and configuring the ***Anybus Defender Compact*** via the CLI (Command Line Interface).

Please read carefully and retain this information.

4.1.7 Validity of this documentation

The document is valid for the industrial firewall ***Anybus Defender Compact*** NFH100, from hardware version HW 03 and firmware version from V 1.4.

4.1.8 Prerequisites / additional required components

- Standard PC with network card and a Windows or LINUX installation.
- USB connection cable (USB A to USB B) - is included in delivery.

4.1.9 Optional additionally required software

- ***Anybus Defender Compact Manager Software****

* In rare cases, you may need to install a USB driver. In this case, you must first install ***Anybus Defender Compact Manager Software***, which you can download for free at: https://www.hms-networks.com/downloads

4.1.10 Release notes

Version	Date	Comment
V 1.4	Oct 24th, 2023	First edition
V 2.0	Nov 10th, 2023	Second edition
V 2.1	July 22nd, 2025	Anybus Defender Compact Edition

5 Functional overview

5.1 Brief description

Anybus Defender Compact is a self-learning, easy-to-configure industrial firewall. It can be operated in both Bridge mode and Gateway mode.

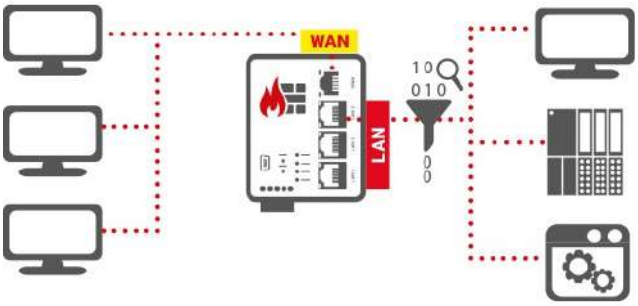
The concept is based on Security by Design right from the start. In order to keep the attack vectors as small as possible, a web interface was deliberately disregarded.

The firewall is configured via the USB port and using the ***Anybus Defender Compact Manager Software*** (not included in delivery), or via the CLI standard shell.

Download link for your free version of the Anybus Defender Compact Manager Software: https://www.hms-networks.com/downloads

5.2 Bridge mode

In **Bridge mode**, Anybus Defender Compact fits easily into existing networks without changing any network range and protects data exchange between its interfaces, filtering packets between WAN and LAN. It integrates transparently, so no IP address allocation is necessary.

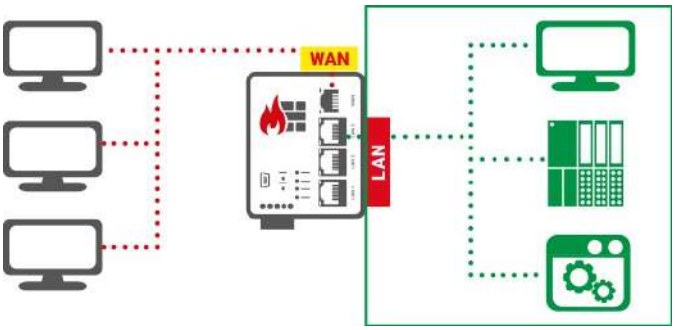


Network A
192.168.0x/24

Network A
192.168.0x/24

5.3 Gateway mode

In **Gateway mode**, WAN and LAN interfaces will get a different IP address and therefore segment the original network. Here functions such as NAT and Forwarding can be used to route data traffic to secondary networks. The packet filter is also available and manages the exchange of data between WAN and LAN.



Network A
192.168.0x/24

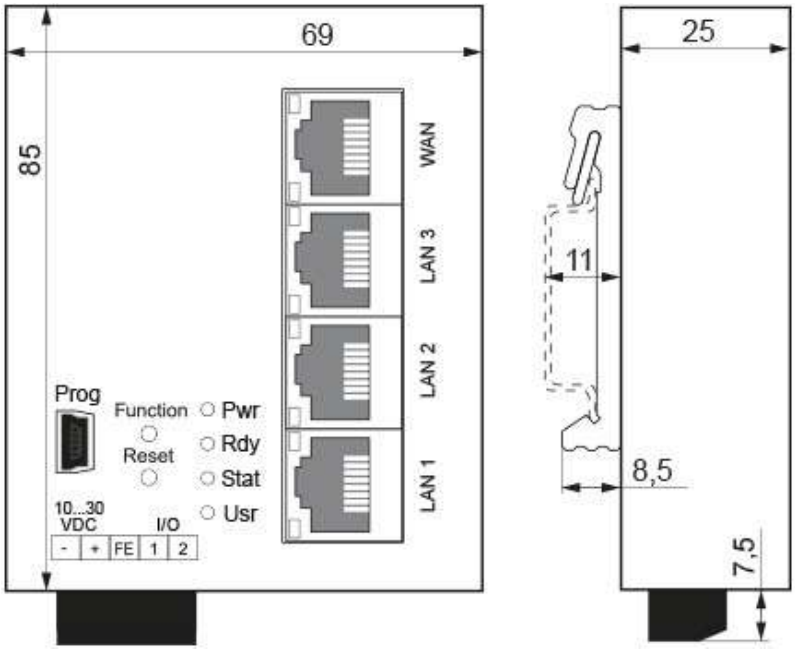
Network B
172.16.0x/24

5.4 Performance characteristics

- Protects the machines in the network from attacks from the Internet
- Easy network segmentation with controlled routing and NAT
- Convenient learning mode makes creation of filter tables simple & easy
- Integration into existing networks
- Bridge mode and Gateway mode
- IP, port and protocol filters for monitoring and restricting data traffic
- Configuration with portable software via USB or SSH (no installation required)
- Versatile NAT functionalities, e.g. 1: 1 NAT, SimpleNAT and port forwarding
- Digital inputs for dynamic control of filter rules
- 1x WAN and 3x LAN port switch
- Security by Design

6 Technical Specifications

Industrial Firewall ***Anybus Defender Compact ABD1004-NETFW***



General data	
Voltage ⎓ V (DC)	10 - 30 V DC (SELV and Limited Energy circuit)
Power consumption	max. 250 mA @ 24 V
IP protection class	IP 30*
Area of application	Dry environments
Operating temperature	-40 – 75 °C
Storage temperature	-40 – 85 °C
Humidity	0 – 95% (non condensing)
Weight	235 g
Dimensions	69 mm (2.71 ") x 33,5 mm (1.32 ") x 92,5 mm (3.64 ") (W x D x H)
Housing (material)	metal
Mounting	DIN rail mounting (based on DIN EN 50022)

* at full occupancy of all connections and interfaces. Alternatively, unused interfaces can be covered with dust protection plugs.

Interfaces	Number	Description
USB interface	1 x	USB slave 2.0 mini
Digital inputs	2 x	10 – 30 V DC (low 0 – 3,2 V DC, high 8 – 30 V DC)
LAN interfaces	3 x	10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable
WAN interfaces	1 x	10/100 Mbit/s full and half duplex operation, autodetection patch cable / crossover cable

Network / Security	
Operating modes	Bridge / Gateway mode
Routing	In Gateway mode • Between WAN and LAN with static routing table
NAT	In Gateway mode • Forwarding (DNAT): IP and port forwarding in gateway mode for WAN > LAN and LAN > WAN • SimpleNAT: Redirect additional WAN-IP to LAN-IP • NetworkNAT: complete network switching of WAN / LAN with virtual IP ranges • SNAT: changing the sender IP with the IP address of the interface
Network filter	In Bridge / Gateway mode • IP / port / protocol filter • MAC filter • Separate filter for sender and destination. • WAN > LAN and LAN > WAN separately adjustable • Black / Whitelisting
Network learning function	In Bridge / Gateway mode • Taking over of network traffic as filter rules • Output of a network list Configuration via management software (Windows) or CLI via SSH
Access control	Four different access levels selectable
Services	NTP client, Syslog client

PROG. CNTLR.
E482663

Certificates / Declarations of Conformity can be downloaded from www.hms-networks.com.

7 Maintenance

Our devices are maintenance-free units. If a device shows signs of damage or malfunctions, the device must be put out of operation immediately and secured against unintentional operation.

NOTICE

Regardless of the maintenance-free hardware, there is a need for action in terms of IT security.

- Keep the software / firmware up to date.
- Note the "Information on cyber security" chapter.
- Keep yourself informed about security updates of the product.

Information can be found at: https://www.hms-networks.com/cyber-security

8 Include in delivery

Please check that your delivery is complete:

1 x Anybus Defender Compact ABD1004-NATFW

1 x Quick start-up guide

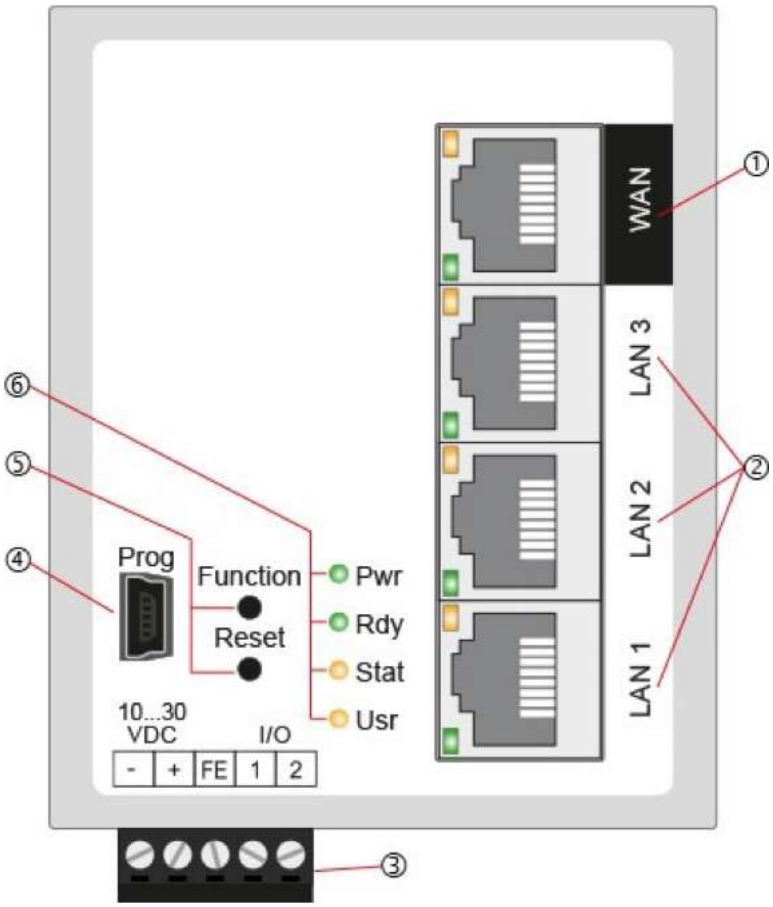
1 x cable USB-A - USB-mini-B

1 x Plug-in bridge

Should any of these parts are missing or damaged, please contact the sales representative for a replacement unit.

Please keep the original box and the original packaging in case you need to send the device for repair at a later date.

9 Displays, controls and connections



1	WAN interface
2	LAN interface
3	Connection terminal
4	USB Slave 2.0 mini
5	Button
6	LED display

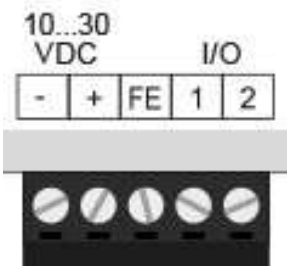
9.1 Connectors

9.1.1 WAN interface

WAN	WAN connection (customer network, DSL router).	
WAN LED	**orange** LED **flashing**	Network data transfer active.
	green LED **on**	Transfer rate = 100 MBit/s
	green LED **off**	Transfer rate = 10 MBit/s

9.1.2 LAN interface

LAN 1 - 3	AN connection (machine network).	
LAN LED	**orange** LED **flashing**	Network data transfer active.
	green LED **on**	Transfer rate = 100 MBit/s
	green LED **off**	Transfer rate = 10 MBit/s



-	0V DC connection
+	Power source connection 10 - 30 V DC
FE	Functional earth
I/O **1***	Digital input (10-30 V DC) (Low 0 – 3,2 V DC, High 8 – 30 V DC)
I/O **2**	Digital input (10-30V DC) (Low 0 – 3,2 V DC, High 8 – 30 V DC) - Function in preparation -

9.1.3 Connection terminal

Input 1 can be used during initial startup to activate the Bridge mode with the packet filter switched off. Input 1 is only evaluated until the Anybus Defender Compact has been configured for the first time - after that the state of input 1 is ignored.

9.1.4 USB Slave 2.0 mini

Prog (Programming)	USB interface mini-B for connecting to the configuration PC.

1.1 Controls - buttons

Function	Function in preparation.
Reset	Performing a device restart (cold start).

1.2 Displays - LED

Pwr (Power)	**green** LED **off**	Device power source is switched off or device is not connected to power source / power pack.
	green LED **on**	Power source is connected to terminal block and switched on.
Rdy (Ready)	**green** LED **flashing**	After the system has been checked and started, the LED flashes for the duration of the starting up process.
	green LED **on**	The device is ready for operation.
Stat (Status)	**orange** LED **on**	The packet filter is ACTIVE in **both** directions (WAN > LAN, LAN > WAN).
	orange LED **off**	The packet filter is INACTIVE in **both** directions (WAN > LAN, LAN > WAN).
	orange LED **flashing**	The packet filter is INACTIVE in **at least one** direction (WAN > LAN, LAN > WAN).
Usr (User)	**orange** LED **on**	The device is not configured.
	orange LED **off**	The device was configured.

10 Initial commissioning

⚠ CAUTION

Before connecting the device to a network or PC, first ensure that it is properly connected to a power supply, otherwise it may cause damage to other equipment

---

The compact industrial firewall can be operated in two modes, Bridge mode and Gateway mode (see chapter 5, "Functional overview").

During the initial commissioning and after each factory reset, the Anybus Defender Compact is always set in Bridge mode, with active packet filter in both directions (Security By Default).

The packet filter can be switched INACTIVE by means of activating input 1 (High 8 – 30 V DC). Select the preset via input 1 if one of the conditions listed below applies:

You want to operate the firewall as a **bridge**

and configure it at a later time

and carry out the installation now

and do not want to influence the existing network

OR

You want to **activate** the firewall's **learning function** so that you can read out the learned network traffic later during configuration.

10.1 Commissioning in bridge mode with INACTIVE packet filter - with learning function

➔ Activating (connection) of input 1

After booting, the packet filter is INACTIVE.

That is, the WAN > LAN and LAN > WAN transitions are open. All pending connection attempts / connections are detected.

NOTICE

This special form of bridge mode (connection of input 1) only remains active until the device has been configured for the first time. The status of input 1 is then ignored.

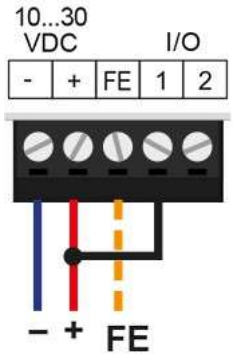
---

1 Connect equipotential bonding to the functional earth (**FE**).

2 Connect the terminals **I/O 1** and **+** (=> I1 = high).

To do this, use the supplied Plug-in bridge.

3 Connect the device to a power supply (**DC 10 – 30 V**).



Make sure the polarity is correct!

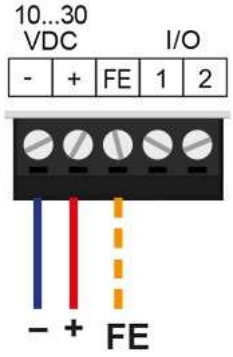
10.2 Commissioning in bridge mode with ACTIVE packet filter - without learning function

Security by default:

After the boot process, both the packet filter and the learning mode are ACTIVE.

That is, the WAN > LAN and LAN > WAN transitions are blocked. All pending connection attempts are detected.

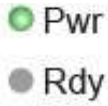
1. Connect equipotential bonding to the functional earth (**FE**).
2. Connect the device to a power supply (**DC 10 – 30 V**).



Make sure the polarity is correct!

10.3 Startup sequence - LED light codes

After switching on the supply voltage, the Pwr LED lights up.



As soon as the system has been checked and starts, the LED Rdy flashes for the duration of the boot process (about 90

seconds).

If the Anybus Defender Compact is ready, the LED Pwr + Rdy will light up.

10.4 LED light codes after start

10.4.1 Light code in bridge mode - packet filter ACTIVE -

LED **Stat** lights up => Firewall active

LED **Usr** lights up => Device has not yet been configured

10.4.2 Light code in bridge mode - packet filter INACTIVE

LED **Stat** flashes => Packet filter inactive

LED **Usr** lights up => Device has not yet been configured

11 Access to the Anybus Defender Compact via SSH

11.1 Set up your PC

To access the Anybus Defender Compact via SSH, proceed as follows:

1. Connect the Anybus Defender Compact to the power supply.
2. Connect the USB interface of the Anybus Defender Compact to your PC. Use the included USB cable (USB A to USB B) for this.

11.1.1 LINUX:

° If you are running Linux on your PC, you may need to manually assign an IP address from the 169.254.0.0/16 subnet (e.g. 169.254.0.2) to your PC's Ethernet interface.

NOTICE

Do **not use** the address 169.254.0.1 as this is assigned to the Anybus Defender Compact itself.

11.1.2 Windows:

° If you run Windows on your PC, it is not necessary to assign an IP address, since Windows automatically assigns an IP address to the respective Ethernet interface.

In rare cases, you may need to update the USB driver for the "Device to PC" connection.

In this case, you must first install the Anybus Defender Compact manager, which you can download here: https://www.hms-networks.com/downloads

In the **Extras** menu of the Anybus Defender Compact manager, select the **Install USB Driver** function.

For more information about the ***Anybus Defender Compact Manager Software***, please read the Anybus Defender Compact Manager manual. The current manuals and further information on products relating to secure remote maintenance can be found in the download portal at https://www.hms-networks.com/p/abd1004-natfw-anybus-defender-compact-1004-nat-fw?tab=tab-support

3. Open the command line input window on your PC and enter the following: **ssh admin@169.254.0.1**

```
ssh admin@169.254.0.1
```

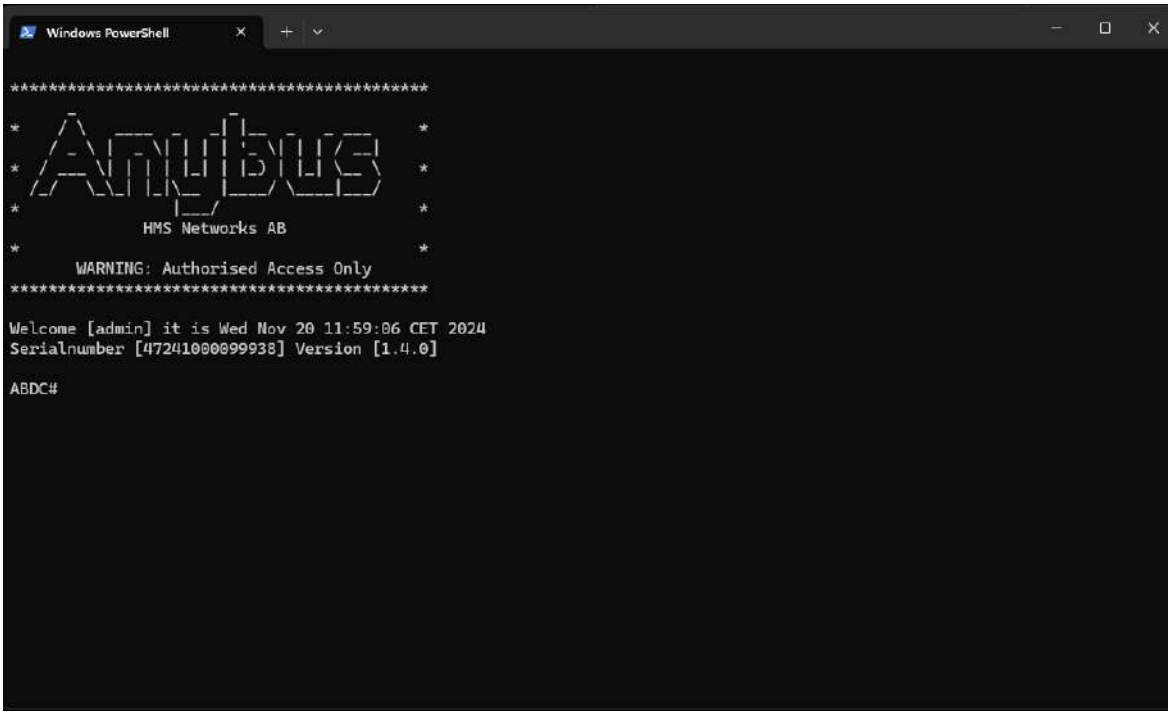
4. You will now be prompted to enter a password:

```
ssh admin@169.254.0.1
admin@169.254.0.1's password:
```

Enter the device password of your Anybus Defender Compact here.

> **NOTICE**
>
> The device password can be found on the back of your Anybus Defender Compact.

✔ **Now the command line interface (CLISH) opens on the Anybus Defender Compact.**



With the command line interface (CLISH) you can configure your Anybus Defender Compact device.

12 Decommissioning/Disposal

NOTICE

Before you dispose of an old device, make sure that all device data and/or personal data and the device configuration have been completely deleted.

1. Remove/erase **all** storage media connected to the device.
2. Disconnect the device from all networks (LAN and WAN) and **carry out the "Reset to factory settings" directly on the device**.
3. Make sure that removing a device from the network does not result in a security risk!

12.1 WEEE and Disposal Responsibilities

We are committed to ensuring that our products are disposed of in an environmentally sound manner. The Waste Electrical and Electronic Equipment (WEEE) Directive is a European regulation aimed at reducing electronic waste and promoting the recycling and proper disposal of electronic products.

Electronic products must be taken to designated WEEE collection points, do not discard electronic devices with household waste. Locate your nearest electronic waste recycling facility or contact local authorities for proper disposal information.

For further information on how to dispose of your electronic products responsibly, please contact your local waste management authority or your local HMS office. Together, we can contribute to a cleaner and more sustainable environment.