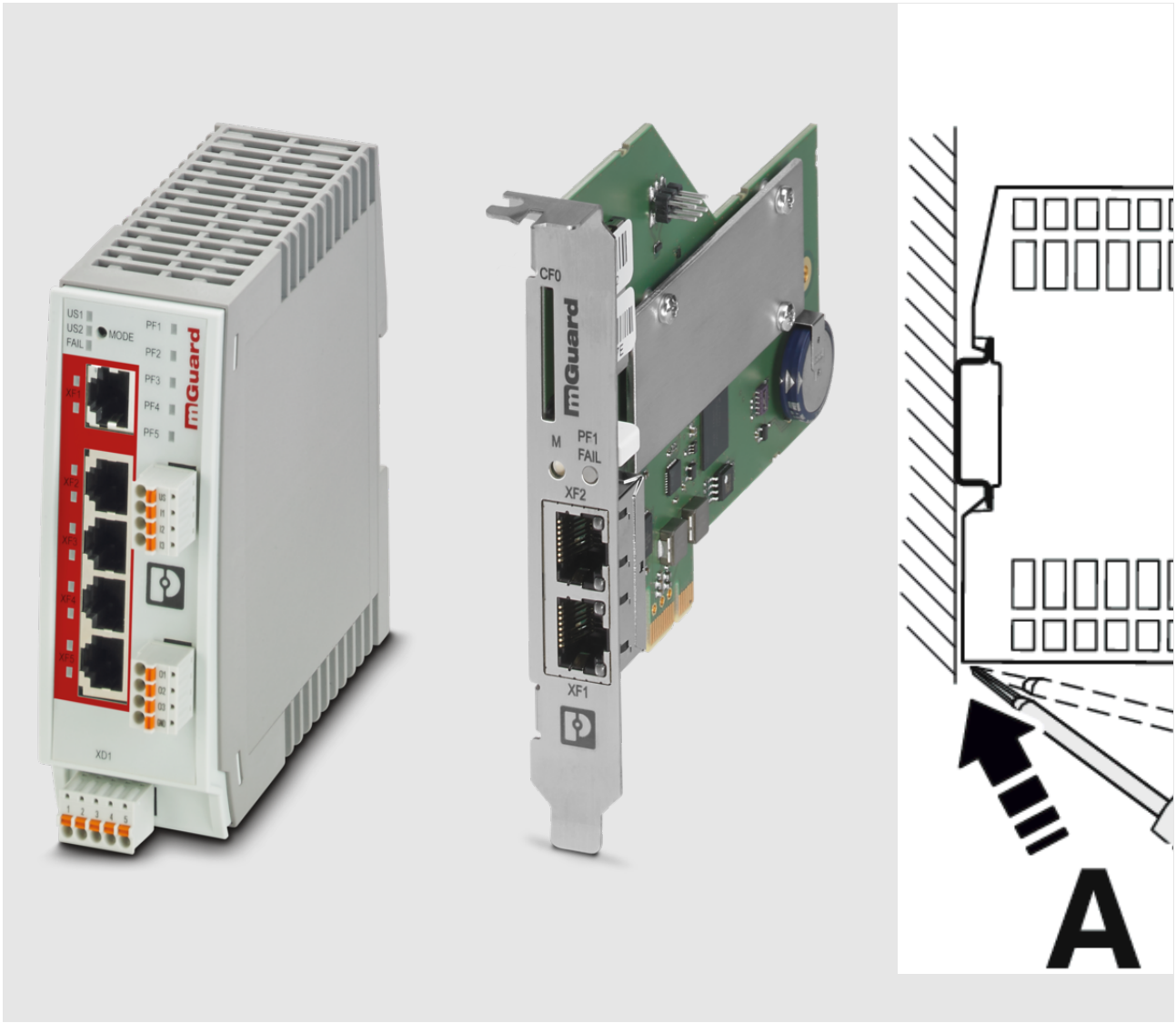


FL MGUARD 2000/4000
Installation and startup

User manual

User manual
FL MGUARD 2000/4000 - Installation and startup

UM EN HW FL MGUARD 2000/4000, Revision 08 2025-01-30

This user manual is valid for

Designation	Item No.
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Firmware version: mGuard 10.5.x

Applicable documentation (available at phoenixcontact.net/product/<item number>):

Release Notes

mGuard 10.5.x Firmware – Release Notes

User Manual „Web-based management“

UM EN FW MGUARD10 – 110191_en_xx

User Manual „Generic Administration Interface - gaiconfig User Guide“:

UM EN GAICONFIG MGUARD10 – 110193_en_xx

User Manual „Installation, Configuration and Usage of the mGuard device manager (mdm)“:

UM EN MDM 1.17 – 111024_en_xx

User Manual „IEC 62443-4-2 conform configuration of the FL MGUARD product family“:

UM EN MGUARD 62443-4-2 – 109049_en_xx

110192_en_08

Table of contents

1 For your safety

Read this user manual carefully and keep it for future reference.

1.1 Identification of warning notes

This symbol together with the **NOTE** signal word warns the reader of actions that might cause property damage or a malfunction.

Here you will find additional information or detailed sources of information.

1.2 About this user manual

The following elements are used in this user manual:

Bold	Designations of operating elements, variable names or other accentuations
Italic	– Product, module or component designations (e.g., *tftpd64.exe*, *Config API*) – Foreign designations or proper names – Other accentuations
–	Unnumbered list
1.	Numbered list
•	Operating instructions
↪	Result of an operation

1.3 Qualification of users

The use of products described in this user manual is oriented exclusively to:

– Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

– Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.4 Intended use

– The devices of the FL MGUARD series are security routers for industrial use, with integrated stateful packet inspection firewall and VPN. They are suitable for distributed protection of production cells or individual machines against manipulation and for secure remote maintenance.

– The devices are not intended for private use. They may only be used and operated in the commercial or industrial sector.

1.5 Modifications to the product

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.6 Safety notes

To ensure correct operation and the safety of the environment and of personnel, the device must be installed, operated, and maintained correctly.

NOTE: Installation only by qualified personnel
Installation, startup and maintenance of the product may only be performed by qualified specialist staff who have been authorized for this by the system operator. An electrically skilled person is someone who, because of their professional training, skills, experience, and their knowledge of relevant standards, can assess any required operations and recognize any possible dangers. Specialist staff must read and understand this documentation and comply with instructions. Observe the national regulations in force for the operation, functional testing, repairs and maintenance of electronic devices.

NOTE: Risk of material damage due to incorrect wiring
Connect the network connections of the device to Ethernet installations only. Some telecommunications connections also use RJ45 jacks; these must not be connected to the RJ45 jacks of the device.

NOTE: Electrostatic discharge
The devices contain components that can be damaged or destroyed by electrostatic discharge. When handling the devices, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and EN 61340-5-2.

NOTE: Requirements for the power supply
The module is designed exclusively for operation with safety extra-low voltage (SELV/PELV). In redundant operation, both power supplies must satisfy the requirements of the safety extra-low voltage.

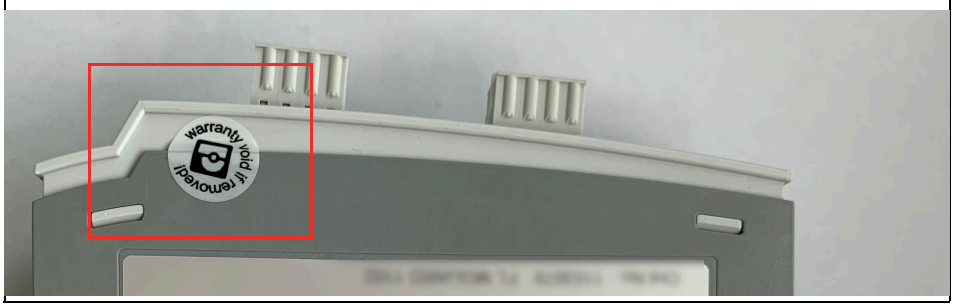
NOTE: Requirement for control cabinet/control box
DIN rail devices snap onto a DIN rail inside a control cabinet or control box. This control cabinet/box must meet the requirements of IEC/EN 62368-1 with respect to fire protection enclosure.

NOTE: Requirement for functional grounding
Mount the DIN rail devices on a grounded DIN rail. The module is grounded when it is snapped onto the DIN rail.

NOTE: Requirement for mounting location
The prescribed mounting position of DIN rail devices is vertical on a horizontally mounted DIN rail. To allow air to circulate freely, the vents must not be covered. A gap of 3 cm between the vents of the housing is recommended.

Do not open or modify the device. Do not repair the device yourself, but replace it with an equivalent device. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from non-compliance.

To prevent tampering with the device supplied and to detect unauthorized opening of the device, a security seal has been attached to the housing of DIN rail devices and to the packaging of PCI cards.
Before using the appliance for the first time, check that the seal is intact. If the seal is removed/damaged, parts of the seal would remain on the housing/packaging (see Section 5).



The IP20 degree of protection (IEC 60529-0/EN 60529-0) of the device is intended for use in a clean and dry environment. Do not subject the device to mechanical and/or thermal loads that exceed the specified limits.

NOTE: Observe the following safety notes when using the device.

- If the equipment is used in a not specified manner, the protection provided by the equipment may be impaired.
- The external circuits intended to be connected to this device shall be galv. separated from mains supply or hazardous live voltage by reinforced or double insulation and meet the requirements of SELV/PELV (Class III) circuit of UL/CSA/IEC 61010-1, 2-201.
- Use Copper Conductors Only, AWG 24-16, 90 °C
- The modules have to be build-in the final safety enclosure, which has adequate rigidity according to UL 61010-1, 61010-2-201 and meets the requirements with respect to spread of fire.
- Wiring of interfaces only inside buildings or max. 42.6 m outside buildings.
- When installing and operating the device, the applicable regulations and safety directives (including national safety directives), as well as general technical regulations, must be observed.
- The technical data is provided in the packing slip and on the certificates (conformity assessment, additional approvals where applicable).
- To avoid overheating, do not expose the device to direct sunlight or other heat sources.
- Clean the device housing with a soft cloth. Do not use aggressive solvents.

1.6.1 Safety notes for installation in zone 2 (only devices with Ex approval)

- The category 3 device is designed for installation in Zone 2 potentially explosive areas. It meets the requirements of EN 60079-0 and EN 60079-7.
- The device is not designed for use in atmospheres with a danger of dust explosions.
- The configuration of the device using DIP switches, buttons, or other accessible switches on the device is only permitted outside of potentially explosive areas.
- Observe the specified conditions for use in potentially explosive areas. Install the device in a suitable, approved housing with at least IP54 degree of protection that meets the requirements of IEC/EN 60079-7 and GB/T 3836.1-2010. Also observe the requirements of IEC/EN 60079-14.
- Only devices which are designed for operation in Ex zone 2 and are suitable for the conditions at the installation location may be connected to the circuits in the Ex zone. In potentially explosive areas, only disconnect and connect cables, SFP modules and the SD card when the power is disconnected.
- Only use fault-free Ethernet cables with functioning latches.
- Plug-in connections (e.g., connector, SD card) must have a functional interlock (e.g., locking clip, screw connection). Insert the interlock and repair any damaged interlocks immediately. Make sure that all plug-in connections are inserted completely.
- The device must be stopped and immediately removed from the Ex area if it is damaged, was subject to an impermissible load, stored incorrectly or if it malfunctions.
- The ambient temperature inside the end user housing must be measured within 25 mm of the device and maintained.
- Only connect one cable per terminal point.
- The air pressure during operation is limited to 108 kPa.
- Electrical isolation, 500 V AC in accordance with EN/IEC 60079-7. Observe the limitations in the specific conditions of use.
- Surge protective devices discharge interference of <500 V_{rms} between the voltage supply connections and FE. Therefore disconnect the power supply connector prior to measuring insulation. Otherwise, inaccurate insulation measurements may occur. Reinsert the plug into the socket provided once insulation measurement has been completed.

1.7 IT security

You have to protect components, networks, and systems against unauthorized access and ensure the integrity of data. As a part of this, you must take organizational and technical measures to protect network-capable devices, solutions, and PC-based software.

Phoenix Contact strongly recommends using an Information Security Management System (ISMS) to manage all of the infrastructure-based, organizational, and personnel measures that are needed to ensure compliance with information security directives.

Furthermore, Phoenix Contact recommends that at minimum the following measures are taken into consideration.

More detailed information on the measures described is available on the following websites (last accessed on 2024-09-15; partly only available in German):

- bsi.bund.de/it-sik.html
- ics-cert.us-cert.gov/content/recommended-practices

Use the latest firmware version

Phoenix Contact regularly provides firmware updates. Any firmware updates available can be found on the product page for the respective device.

- Ensure that the firmware on all devices used is always up to date.
- Observe the Change Notes for the respective firmware version.
- Pay attention to the security advisories published on Phoenix Contact's Product Security Incident Response Team (PSIRT) website regarding any published vulnerabilities.

Assure the integrity of downloaded files

Phoenix Contact provides checksums of files that can be downloaded on the product page for the respective device.

- To ensure that the downloaded firmware or update files as well as downloaded documentation have not been modified by third parties during the download, compare the SHA256 checksums of the files with the checksums specified on the corresponding product page (phoenixcontact.com/product/<item number>).

Use up-to-date security software

- Install security software on all PCs to detect and eliminate security risks such as viruses, trojans, and other malware.
- Ensure that the security software is always up to date and uses the latest databases.
- Use whitelist tools for monitoring the device context.
- Use an Intrusion-Detection system for checking the communication within your system.

Take Defense-in-Depth strategies into consideration when planning systems

It is not sufficient to take measures that have only been considered in isolation when protecting your components, networks, and systems. Defense-in-Depth strategies encompass several coordinated measures that include operators, integrators, and manufacturers.

- Take Defense-in-Depth strategies into consideration when planning systems.

Perform regular threat analyses

- To determine whether the measures you have taken still provide adequate protection for your components, networks, and systems, threat analyses should be performed regularly.
- Perform a threat analysis on a regular basis.

Deactivate unneeded communication channels

- Deactivate unnecessary communication channels (e.g., SNMP, FTP, BootP, DCP, etc.) on the components that you are using.

Do not integrate components and systems into public networks

- Avoid integrating your components and systems into public networks.
- If you have to access your components and systems via a public network, use a VPN (Virtual Private Network).

Restrict access rights

- Avoid unauthorized persons gaining physical access to the device. Accessing the hardware of the device could allow an attacker to manipulate the security functions.
- Restrict access rights for components, networks, and systems to those individuals for whom authorization is strictly necessary.
- Deactivate unused user accounts.

Secure access

- Change the default login information after initial startup.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Change passwords in accordance with the rules applicable for their application.
- Use a password manager with randomly generated passwords.
- Wherever possible, use a central user administration system to simplify user management and login information management.

Use secure access paths for remote access

- Use secure access paths such as VPN (Virtual Private Network) or HTTPS for remote access.

Set up a firewall

- Set up a firewall to protect your networks and the components and systems integrated into them against external influences.
- Use a firewall to segment a network or to isolate a controller.

Activate security-relevant event logging

- Activate security-relevant event logging in accordance with the security directive and the legal requirements on data protection.

Secure access to SD cards

Devices with SD cards require protection against unauthorized physical access. An SD card can be read with a conventional SD card reader at any time. If you do not protect the SD card against unauthorized physical access (such as by using a secure control cabinet), sensitive data is accessible to all.

- Ensure that unauthorized persons do not have access to the SD card.
- When destroying the SD card, ensure that the data cannot be retrieved.

1.8 Latest safety instructions for your product

Product Security Incident Response Team (PSIRT)

The Phoenix Contact PSIRT is the central team for Phoenix Contact as well as for its subsidiaries, authorized to respond to potential security vulnerabilities, incidents and other security issues related to Phoenix Contact products, solutions as well as services.

Phoenix Contact PSIRT manages the disclosure, investigation internal coordination and publishes security advisories for confirmed vulnerabilities where mitigations/fixes are available.

The PSIRT website (phoenixcontact.com/psirt) is updated regularly. In addition, Phoenix Contact recommends subscribing to the PSIRT newsletter.

Anyone can submit information on potential security vulnerabilities to the Phoenix Contact PSIRT by e-mail.

1.9 Support

For additional information on the device as well as release notes, user assistance and software updates, visit: phoenixcontact.net/product/<item number>.

In the event of problems with your device or with operating your device, please contact your supplier.

To get help quickly in the event of an error, make a snapshot of the device configuration immediately when a device error occurs, if possible. You can then provide the snapshot to the support team.

The usage of snapshots is described in the user manual "Web-based management" (UM EN FW MGUARD10). Available in the download area of the corresponding product page in the Phoenix Contact Web Shop, e.g., at phoenixcontact.net/product/1357828.

2 Overview FL MGUARD 2000/4000 series

2.1 Product overview

The FL MGUARD 2000/4000 series adds new models to the established FL MGUARD RS2000/4000 series. The new models (MGUARD3 device platform) are equipped with high-speed Gigabit Ethernet.

The differences between the device series as well as the option for transferring configurations to the new FL MGUARD 2000/4000 series devices are described in Section 2.2.

Product overview and variants

Unless otherwise stated, when the FL MGUARD 4302 and FL MGUARD 4305 devices are mentioned in this document, the 4302/KX and 4305/KX variants are also included.

Table 2-1 Product overview and item numbers

Device	Short description	Item number
FL MGUARD 2102	DIN rail device, 2 x RJ45 ports, SD card holder, digital service I/Os, Gigabit Ethernet	1357828
FL MGUARD 4302	DIN rail device, 2 x RJ45 ports, SD card holder, digital service I/Os, Gigabit Ethernet, redundant power supply	1357840
FL MGUARD 4302/KX	DIN rail device, 2 x RJ45 ports, SD card holder, digital service I/Os, Gigabit Ethernet, redundant power supply, Ex approval	1696708
FL MGUARD 4102 PCI	PCI card, 2 x RJ45 ports, SD card holder, Gigabit Ethernet	1441187
FL MGUARD 4102 PCIE	PCI Express card, 2 x RJ45 ports, SD card holder, Gigabit Ethernet	1357842
FL MGUARD 2105	DIN rail device, 5 x RJ45 ports, ethernet switch, SD card holder, digital service I/Os, Gigabit Ethernet	1357850
FL MGUARD 4305	DIN rail device, 5 x RJ45 ports, ethernet switch, SD card holder, digital service I/Os, Gigabit Ethernet, redundant power supply	1357875
FL MGUARD 4305/KX	DIN rail device, 5 x RJ45 ports, ethernet switch, SD card holder, digital service I/Os, Gigabit Ethernet, redundant power supply, Ex approval	1696779

Field of application

The FL MGUARD 4000 series devices are security routers with intelligent stateful packet inspection firewall and integrated IPsec VPN and OpenVPN with up to 250 VPN tunnels. They are designed for use in industry to accommodate strict distributed security and high availability requirements.

The FL MGUARD 2000 series devices are a version with basic firewall and integrated IPsec VPN and OpenVPN with a maximum of 2 VPN tunnels. Their scope of functions is reduced to the essentials. The devices are suitable for secure remote maintenance applications in industry and enable the quick startup of robust field devices for industrial use, thereby facilitating error-free, independent operation.

Security by design

All mGuard devices feature the tried-and-tested *mGuard Security Technology* and thus have been developed from the ground up in accordance with the requirements for network security. The devices use a powerful firewall. System and network services have been made more rigorous.

Security vulnerabilities – quickly closed (PSIRT)

All the components used are continuously monitored via the PSIRT process (*Product Security Incident Response Team*). Any vulnerabilities discovered or reported are immediately analyzed and, if necessary, closed (see PSIRT).

Through the integrated *mGuard Security Technology*, the devices ensure distributed protection of production cells or individual machines against manipulation.

PROFINET RT

The hardware of the FL MGUARD 210X/410X/430X devices is designed in such a way that the WAN side (interface XF1) and the LAN side (interface XF2 or XF2-XF5) are securely separated from each other via the application processor.

In addition, the mGuard firmware 10.x is implemented in such a way that the transmission of Layer 2 datagrams such as PROFINET RT is excluded when using the "Router" network mode (default setting).

mGuard devices can therefore be used as a secure network boundary for PROFINET. They can be used as protective devices for PROFIsafe network cells in environments in which the uniqueness of the PROFIsafe addresses cannot be ensured.

The devices are used in accordance with the IEC 61784-3-3 standard (5.4.2 and 8.1.2).

2.2 New device platform FL MGUARD 2000/4000

The FL MGUARD 2000/4000 series devices will gradually replace the established RS2000/RS4000 and PCI(E)4000 series of mGuard devices.

The new devices with proven *mGuard Security Technology* are equipped with fast Gigabit Ethernet and are operated with the mGuard 10.x firmware version.

The devices are compatible with their predecessor models, can import existing configuration profiles (atv files), and can be configured via CGI and GAI interfaces.

The mGuard device manager can be used to manage mGuard devices with firmware versions up to 10.5.x installed (see user manual "FL MGUARD DM UNLIMITED" – 111024_en_xx).

Currently, some device functions of the predecessor models cannot yet be supported on the new models (see Section 2.2.1).

2.2.1 Functions that are no longer supported

Certain functions of the old device platform are no longer supported on the new device platform.

Hardware

The new mGuard models of the FL MGUARD 2000/4000 series are offered without a serial interface and internal modem.

In case of the DIN rail devices, the connections for the power supply as well as digital inputs and outputs are provided in the form of COMBICON connectors (see Section 3.3).

Firmware (functions)

Device functions that are not supported on the new device platform are listed in Table 2-2.

Table 2-2 Current functional differences

Functions currently not supported in the firmware mGuard 10.5.x
Network: Interfaces – PPPoE – PPTP – Secondary external interface
Network: Serial interface
Network: GRE tunnel (Generic Routing Encapsulation)
VPN redundancy
Quality of Services (QoS)
CIFS Integrity Monitoring
SEC-Stick

When transferring older device configurations to the new devices, care must therefore be taken to ensure that the functions described in Table 2-2 have been deactivated or reset to the default settings in the device configuration before export (see also Section 2.2.2).

2.2.2 Migration of the device configuration

Migrating the configuration of older mGuard devices can be done via web-based management (WBM) or via SD card (ECS).

Requirements

If device functions of the device whose configuration is to be migrated are not available on the new device, the variables must be reset to the default settings before the configuration on the old device is exported (see Table 2-2).

The exact procedure for device migration is described in document 111259_en_xx (AH EN MGUARD MIGRATE 10), available at phoenixcontact.com/product/1357875.

Further information can be found in the current user manual “Web-based Management” UM EN FW MGUARD10 - 110191_en_xx.

2.3 Scope of supply

The device is delivered in packaging together with a packing slip that provides installation instructions.

- Read the entire packing slip carefully.
- Retain the packing slip.

2.3.1 Checking the delivery

- Check the delivery for transport damage.
  Damaged packaging is an indicator of potential damage to the device that may have occurred during transport. This could result in a malfunction.
- Immediately upon delivery, refer to the delivery note to ensure that the delivery is complete.
- Before using the appliance for the first time, check that the security seal is intact. If the seal is removed/damaged, parts of the seal would remain on the housing/packaging (see Section 5).
- Submit claims for any transport damage immediately, and inform Phoenix Contact or your supplier as well as the shipping company without delay.
- Enclose photos that clearly document the damage to the packaging and/or delivery together with your claim.
- Keep the box and packaging material in case you need to return the product.
- We strongly recommend using the original packaging to return the product.
- If the original packaging is no longer available, observe the points in Section 7.

2.4 Default settings

In the default settings (delivery state), the device is configured as described below.

2.4.1 Network interfaces

The basic network functions (Ethernet) of the device are available after the device start (see Table 2-3).

The configuration of the device via the WAN interface is not possible because external access to the device is blocked by the firewall (see Section 2.4.5).

Table 2-3 **Default settings**: Configuration of the network interfaces

Function	WAN (XF1)	LAN (XF2-4 or XF2-5) (depending on the device type)	DMZ (XF5) (only FL MGUARD 4305)
IP address (IPv4)	If there is a DHCP server in the network, the IP address is assigned automatically.	192.168.1.1	-
Netmask		24	-
Default gateway	Can be assigned automatically if there is a DHCP server in the network.	-	-
IP masquerading (NAT)	Is applied to all routed data packets that leave the device via network interface XF1 (into the external WAN network).	-	-

2.4.2 User access

The WBM and shell access (SSH) user interfaces can be accessed by entering a user name and password.

User name	Password
root	*root*
admin	*mGuard*

On initial device startup, immediately change the preset administrator passwords. Additionally, network access to the device is restricted by the firewall for incoming data traffic (see “Firewall (for incoming data traffic) = device access”).

2.4.3 Active network services (device as client)

The following network services are activated by default on the device (as client).

Table 2-4 **Default settings**: active services (as client)

Service	Active via	Configuration (default settings)
DHCP client	WAN interface (XF1)	Sends DHCP requests to available DHCP servers in its network via UDP port 67.
DNS client	WAN interface (XF1)	Sends DNS requests to DNS root servers via UDP port 53.
NTP client	deactivated	

2.4.4 Active network services (device as server)

The following network services are activated on the device (as a server) in the default settings and can be accessed externally via the network interfaces.

Table 2-5 **Default settings**: active services (as server)

Service	Active via	Configuration (default settings)
Web server (HTTPS)	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Request via TCP Port 443 (HTTPS) Clients that are connected with the device via LAN can access the web-based management (WBM).
Command line / GAI (SSH)	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Request via TCP port 22 (SSH) Clients that are connected with the device via LAN can access the *Generic Administration Interface* (GAI) via the command line.
DHCP server	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Request via UDP port 67 Clients that are connected with the device via LAN can request a network configuration from its DHCP server. The following network configuration is assigned to requesting clients: – IP address from area: 192.168.1.2 ... 192.168.1.254 – Local netmask: 24 – Default gateway: 192.168.1.1 – DNS/WINS server: 192.168.1.1

Table 2-5 **Default settings**: active services (as server)

Service	Active via	Configuration (default settings)
DNS server	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	Request via TCP/UDP port 53 Clients that are connected with the device via LAN can send name resolution requests to its DNS server.
SNMP server	deactivated	
NTP server	deactivated	

2.4.5 Firewall and device access

At the firewall, a distinction is made between incoming and *routed* data traffic:

– **Incoming data traffic** is the packets that are sent to the device (e. g. device access).
– **Routed data traffic** is the packets that are *routed* through the device, for example that come in via LAN (XF2) and go out via WAN (XF1).

Firewall (for incoming data traffic) = device access

Table 2-6 **Default settings**: Firewall for incoming data traffic

Service, protocol	Incoming via	Status	Port	Description
HTTPS	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	TCP 443	Corresponding requests to the web server of the device are **permitted**: – Login and configuration via web-based management
	WAN (XF1)	⊘		Requests via the WAN interface are dropped.
SSH	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	SSH 22	Corresponding requests to the SSH server of the device are **permitted**: – shell access – configuration via GAI-Config
	WAN (XF1)	⊘		Requests via the WAN interface are dropped.
DHCP	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	UDP 67	Corresponding requests to the DHCP server of the device are **permitte.**
	WAN (XF1)	⊘		Requests via the WAN interface are dropped.
DNS	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓	TCP 53 UDP 53	Corresponding requests to the DNS server of the device are **permitte.**
	WAN (XF1)	⊘		Requests via the WAN interface are dropped.
ICMP **(IPv4)**	LAN (XF2-5) (not FL MGUARD 4305) LAN (XF2-4) (FL MGUARD 4305)	✓		Ping requests to the management IP address (in Stealth mode) are permitted.
	WAN (XF1)	⊘		Requests via the WAN interface are dropped.

Access to all other network services and network protocols of the device are rejected by the firewall.

Default settings: firewall (routed data traffic: packet filter >> outgoing rules)
All packets that are sent from the LAN network (XF2-5 or XF2-4) to any target addresses are forwarded by the device.

Default settings: firewall (routed data traffic: packet filter >> incoming rules)
All packets that are sent from the WAN network (XF1) to any target addresses are discarded by the device.

3 FL MGUARD 2102/2105 and 4302/4305

Table 3-1 Currently available products

Product designation	Phoenix Contact item number
FL MGUARD 2102	1357828
FL MGUARD 4302	1357840
FL MGUARD 4302/KX	1696708
FL MGUARD 2105	1357850
FL MGUARD 4305	1357875
FL MGUARD 4305/KX	1696779

Product description

FL MGUARD 4000: The FL MGUARD 4000 series devices are security routers with intelligent stateful packet inspection firewall and integrated IPsec VPN and OpenVPN with up to 250 VPN tunnels. They are designed for use in industry to accommodate strict distributed security and high availability requirements.

With the **FL MGUARD 4305**, a dedicated DMZ port with its own firewall rules enables segmentation and more differentiated security concepts.

The **FL MGUARD 4302/KX** and **FL MGUARD 4305/KX** variants are approved for the installation in Zone 2 potentially explosive areas (Ex approval). They are always included when the FL MGUARD 4302 and FL MGUARD 4305 devices are mentioned.

FL MGUARD 2000: The FL MGUARD 2000 series devices are a version with basic firewall and integrated IPsec VPN and OpenVPN with a maximum of 2 VPN tunnels. Their scope of functions is reduced to the essentials. The devices are suitable for secure remote maintenance applications in industry and enable the quick startup of robust field devices for industrial use, thereby facilitating error-free, independent operation.

Figure 3-1 FL MGUARD 2102/4302 (left) and FL MGUARD 2105/4305 (right)

3.1 Device description

3.1.1 FL MGUARD 2102 / FL MGUARD 4302

The device provides the following network connections:

– **Network interface XF1/WAN**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface XF2/LAN**: Ethernet 10/100/1000 Mbps (RJ45 port)

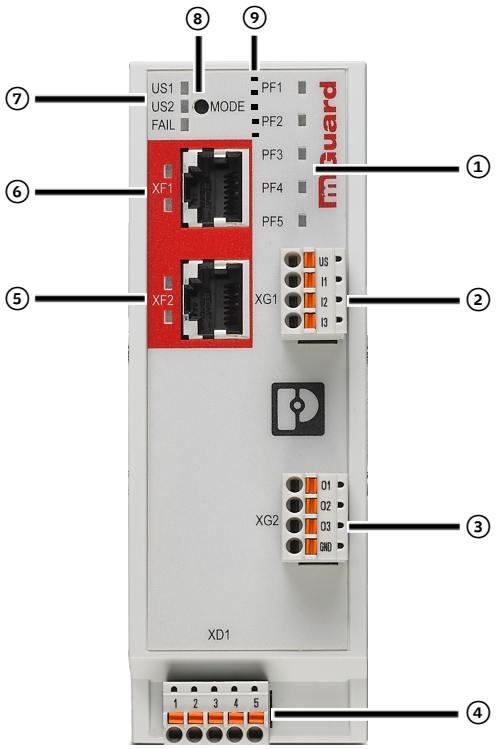


Figure 3-2 FL MGUARD 2102/FL MGUARD 4302: Operating elements and LEDs

① Status and diagnostic LEDs
(see Section 3.2.1)

② Connection of digital **inputs** via COMBICON connector (push-in contact)
(see Section 3.6)

③ Connection of digital **outputs** via COMBICON connector (push-in contact)
(see Section 3.6)

④ Connection of supply voltage via COMBICON connector (push-in contact)
(see Section 3.4)

⑤ Network interface XF2/**LAN** (RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑥ Network interface XF1/**WAN** (RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑦ Status and diagnostic LEDs
(see Section 3.2.3, 3.2.4)

⑧ Mode button
(see Section 6)

⑨ SD card holder (on the back of the device)
(see Section 3.7)

3.1.2 FL MGUARD 2105

The device provides the following network connections:

– **Network interface XF1 / WAN**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface XF2-5/LAN**: 4-Port-Ethernet Switch 10/100/1000 Mbps (RJ45 port)

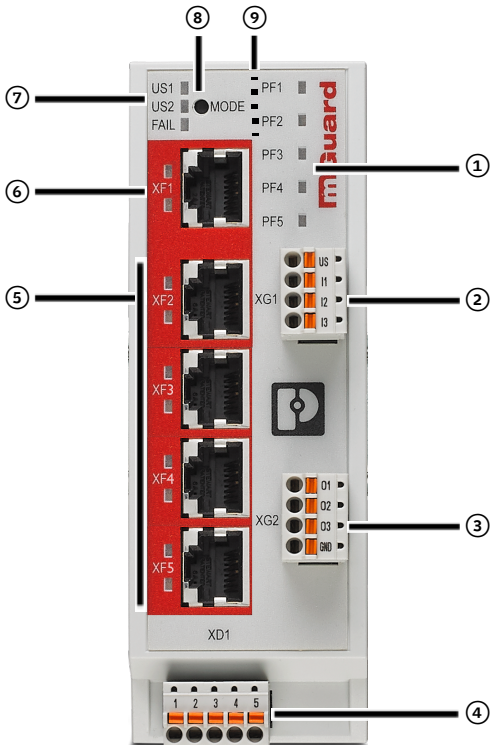


Figure 3-3 FL MGUARD 2105: Operating elements and LEDs

① Status and diagnostic LEDs
(see Section 3.2.1)

② Connection of digital **inputs** via COMBICON connector (push-in contact)
(see Section 3.6)

③ Connection of digital **outputs** via COMBICON connector (push-in contact)
(see Section 3.6)

④ Connection of supply voltage via COMBICON connector (push-in contact)
(see Section 3.4)

⑤ Network interface XF2-5/**LAN** (4x RJ45 Ethernet port / network switch) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑥ Network interface XF1/**WAN** (RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑦ Status and diagnostic LEDs
(see Section 3.2.3, 3.2.4)

⑧ Mode button
(see Section 6)

⑨ SD card holder (on the back of the device)
(see Section 3.7)

3.1.3 FL MGUARD 4305

The device provides the following network connections:

– **Network interface XF1 / WAN**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface XF2-4 / LAN**: 3-Port-Ethernet Switch 10/100/1000 Mbps (RJ45 port)
– **Network interface XF5 / DMZ**: Ethernet 10/100/1000 Mbps (RJ45 port)

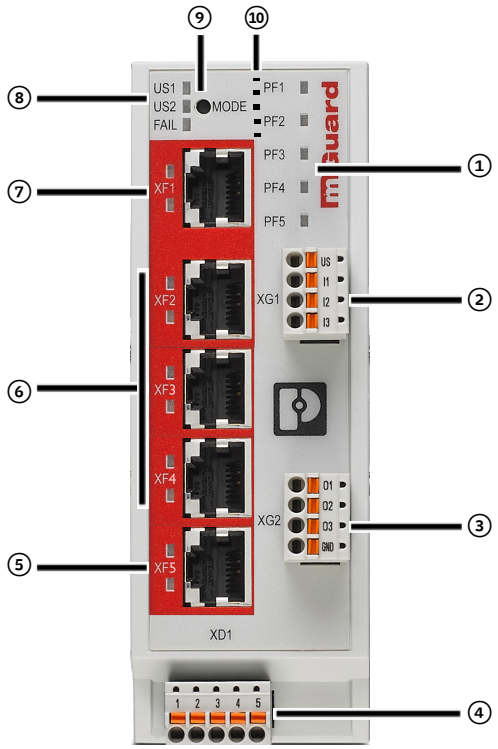


Figure 3-4 FL MGUARD 2102/FL MGUARD 4302: Operating elements and LEDs

① Status and diagnostic LEDs
(see Section 3.2.1)

② Connection of digital **inputs** via COMBICON connector (push-in contact)
(see Section 3.6)

③ Connection of digital **outputs** via COMBICON connector (push-in contact)
(see Section 3.6)

④ Connection of supply voltage via COMBICON connector (push-in contact) (see Section 3.4)

⑤ Network interface XF5/**DMZ** (RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑥ Network interface XF2-4/**LAN** (3x RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑦ Network interface XF1/**WAN** (RJ45 Ethernet port) (see Section 3.5)
LNK/ACT LED (top) | SPD LED (bottom)
(see Section 3.2.2)

⑧ Status and diagnostic LEDs
(see Section 3.2.3, 3.2.4)

⑨ Mode button
(see Section 6)

⑩ SD card holder (on the back of the device)
(see Section 3.7)

3.2 LED status and diagnostic indicators

The status and diagnostic LEDs indicate different system and error states of the device (see Table 3-5).

3.2.1 PF1 – PF5

The tricolor PF1 – PF5 LEDs (green/red/orange) indicate different statuses and system states of the device.

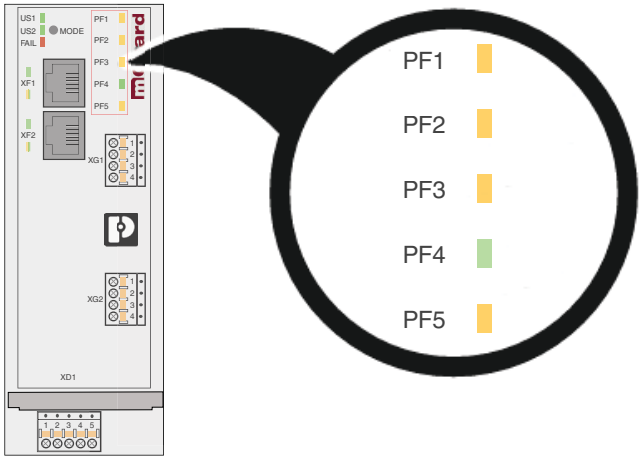


Figure 3-5 LED: PF1 – PF5

Table 3-2 LED: PF1 – PF5: Device status (examples)

Device status			
Is being started	**Ready for operation**	**VPN connection/ firewall rule record** Monitored via service contacts O1 and O2	**VPN connection/ firewall rule record** Monitored via service contacts O1 and O2
PF1 PF2 PF3 PF4 **PF5**	PF1 PF2 PF3 PF4 PF5	PF1 PF1 PF2 PF2 PF3 PF3 **PF4** **PF4** PF5 PF5	PF1 PF1 PF2 PF2 **PF3** PF3 PF4 **PF4** PF5 PF5
The device starts. When the device is starting, all PF LEDs light up briefly (orange).	The device has been started up completely. The PF1 LED flashes with the rhythm of a heartbeat.	The VPN connection/firewall rule record is^ being established/activated. O1: The PF3 LED flashes O2: The PF4 LED flashes	The VPN connection/firewall rule record has been established/activated. O1: The PF3 LED lights up O2: The PF4 LED lights up

3.2.2 LNK/ACT and SPD

The LNK/ACT (*Link/Activity)* and SPD (*Speed*) LEDs indicate the status of the network connection of the related network port (see Section 3.2.5).

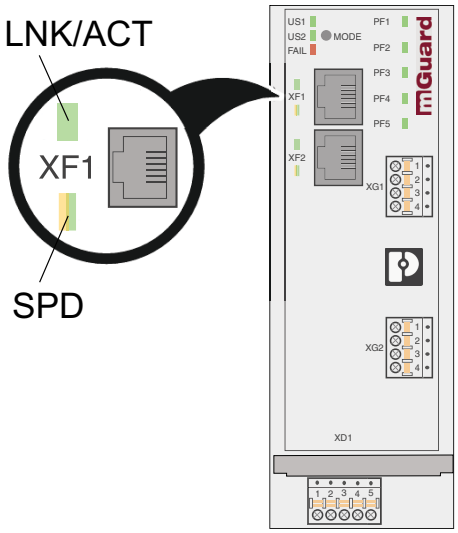


Figure 3-6 LED: LNK/ACT and SPD

Table 3-3 LED: LNK/ACT and SPD

Designation	Color	Status	Meaning
LNK/ACT (XF1–XF5) (upper LED)	Green	On	Link active
		Flashing	Data packets are being transmitted.
		Off	Link not active
SPD (XF1–XF5) (lower LED)	Green/orange	On (orange)	1000 Mbps (Gigabit Ethernet)
		On (green)	100 Mbps (Fast Ethernet)
		Off	10 Mbps (Ethernet) (if LNK/ACT LED active) or Inactive – No data transmission if LNK/ACT LED is inactive)

3.2.3 US1 and US2

The US1 and US2 LEDs indicate the status of the power supply for the device.

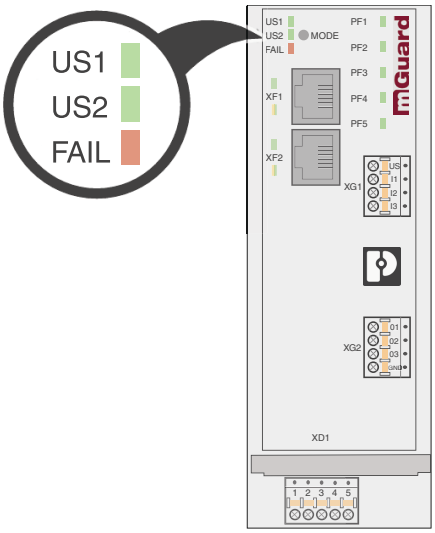


Figure 3-7 LEDs: US1 and US2

Table 3-4 LEDs: US1 and US2

Designation	Color	Status	Meaning
US1	Green	On	Supply voltage within the tolerance range (see Section 8)
		Off	Supply voltage not present or too low (see Section 8)
US2 (only FL MGUARD 4000 series)	Green	On	Supply voltage within the tolerance range (see Section 8)
		Off	Supply voltage not present or too low (see Section 8)
Only FL MGUARD 4000 series devices have a redundant power supply.			

3.2.4 FAIL

The FAIL LED indicates different statuses and error states of the device (see Section 3.2.5).

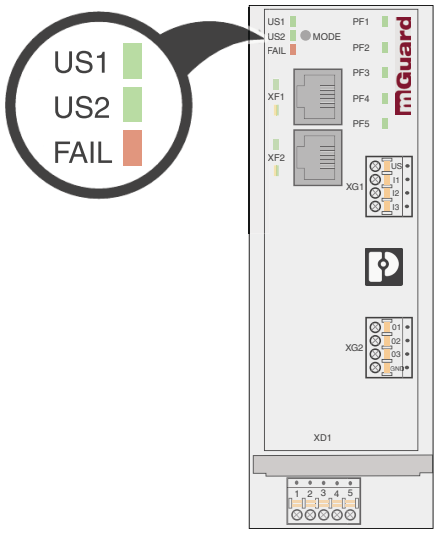


Figure 3-8 LED: FAIL

3.2.5 Visualization of system states

For the system states (status, alarm, or error messages) indicated via the illumination or flashing behavior of the LEDs, please refer to Table 3-5.

For further information about error and system states, please also refer to the corresponding log files.

Table 3-5 System states visualized by the illumination and flashing behavior of LEDs

PF1 (green)	PF2 (green)	PF3 (green)	PF4 (green)	PF5 (ERR) (red)	FAIL (FAULT) (red)	Description of the system state
Operational						
Heartbeat						The system status is OK. The PF1 LED is blinking in the rhythm "heartbeat".
System start						
Heartbeat				ON (~20 sec)	ON (~20 sec)	The system is booting. All LEDs of the Ethernet ports (LNK/ACT and SPD) briefly light up red/green. All PF LEDs (PF1-5) briefly light up orange. The PF1 LED is blinking in the rhythm "heartbeat".
Heartbeat				Blink 500/500	ON	The device failed to start after an integrity check of the file system. The file system is damaged or has been manipulated.
Heartbeat	ON (orange) (3 sec)					ECS: The configuration was successfully loaded and applied from the ECS.
Update						
				Blink 500/500		Bootloader replacement failed due to hardware error.
				Blink 500/500		Another severe error has happened.
Operation Supervision / Alarm output						
Heartbeat					ON	No connectivity on WAN interface (link supervision configurable on device)
Heartbeat					ON	No connectivity on LAN interface (link supervision configurable on device)
Heartbeat					ON	Power supply 1 or 2 failed (alarm configurable on device)
Heartbeat					ON	Temperature too high / low (alarm configurable on device)
Heartbeat					ON	(Redundancy) Connectivity check failed (alarm configurable on device)
Heartbeat					ON	Administrator passwords not configured (alarm configurable on device)

Table 3-5 System states visualized by the illumination and flashing behavior of LEDs

PF1 (green)	PF2 (green)	PF3 (green)	PF4 (green)	PF5 (ERR) (red)	FAIL (FAULT) (red)	Description of the system state
Controllable VPN connections/firewall rule records (via service contacts)						
Heart-beat		Blink				**Service contact O1**: The VPN connection switched via service contact O1 will be established.
Heart-beat		ON				**Service contact O1**: The VPN connection switched via service contact O1 was successfully established. OR **Service contact O1**: The firewall rule record switched via service contact O1 was successfully activated .
Heart-beat			Blink			**Service contact O2**: The VPN connection switched via service contact O2 will be established.
Heart-beat			ON			**Service contact O2**: The VPN connection switched via service contact O2 was successfully established. OR **Service contact O2**: The firewall rule record switched via the service contact O2 was successfully activated.
External Configuration Storage (ECS)						
Heart-beat	ON (orange) (3 sec)					ECS: The configuration was successfully loaded and applied from the ECS.
Heart-beat				ON (3 sec)		ECS: The ECS is incompatible.
Heart-beat				ON (3 sec)		ECS: The capacity of the ECS is exhausted.
Heart-beat				ON (3 sec)		ECS: The root password from the ECS does not match.
Heart-beat				ON (3 sec)		ECS: Failed to load the configuration from the ECS.
Heart-beat				ON (3 sec)		ECS: Failed to save the configuration to the ECS.
Recovery procedure						
Heart-beat				ON (2 sec)		RECOVERY: The recovery procedure failed.
ON (2 sec)						RECOVERY: The recovery procedure succeeded.
Flash procedure						
ON					ON	FLASH PROCEDURE: The flash procedure has been started. Please wait.

Table 3-5 System states visualized by the illumination and flashing behavior of LEDs

PF1 (green)	PF2 (green)	PF3 (green)	PF4 (green)	PF5 (ERR) (red)	FAIL (FAULT) (red)	Description of the system state
Running light	Running light	Running light			ON	FLASH PROCEDURE: The flash procedure is currently executed.
Blink 50/800	Blink 50/800	Blink 50/800			ON	FLASH PROCEDURE: The flash procedure succeeded.
				ON		FLASH PROCEDURE: The flash procedure failed.
				Blink 50/100 (5 sec)		FLASH PROCEDURE WARNING: Replacing the rescue system. Do not power off. When the blinking stops, the replacement of the rescue system is over.
				ON		FLASH PROCEDURE: The DHCP/BOOTP requests failed.
				ON		FLASH PROCEDURE: Mounting the data storage device failed.
				ON		FLASH PROCEDURE: Erasing the file system partition failed.
				ON		FLASH PROCEDURE: Failed to load the firmware image.
				ON		FLASH PROCEDURE: The signature of the firmware image is not valid.
				ON		FLASH PROCEDURE: Failed to load the install script.
				ON		FLASH PROCEDURE: The signature of the install script is not valid.
				ON		FLASH PROCEDURE: The rollout script failed.

3.3 Mounting and removal

NOTE: Device damage

Only mount or remove the device when disconnected from the voltage.

The device is intended for installation in a control cabinet. Mount the device on a clean DIN rail in accordance with DIN EN 50 022.

Mounting the device

- Place the module onto the DIN rail (**A**) from above. The upper holding keyway of the module must be hooked onto the top edge of the DIN rail.
- Push the module from the front towards the mounting surface (**B**).
- Once the module has been snapped on properly, check that it is fixed securely.
- Connect the DIN rail to protective earth ground.

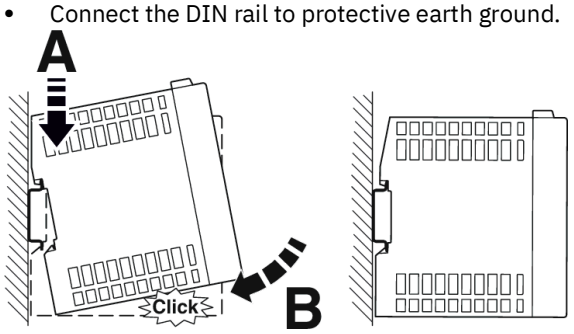


Figure 3-9 Snapping the device onto a DIN rail

Removing the device

- Pull down (**B**) the positive latch (**A**) using a suitable tool (e.g., screwdriver). The positive latch remains snapped out.
- Slightly swivel the bottom of the device away from the DIN rail (**C**).
- Lift the device upwards away from the DIN rail (**D**).

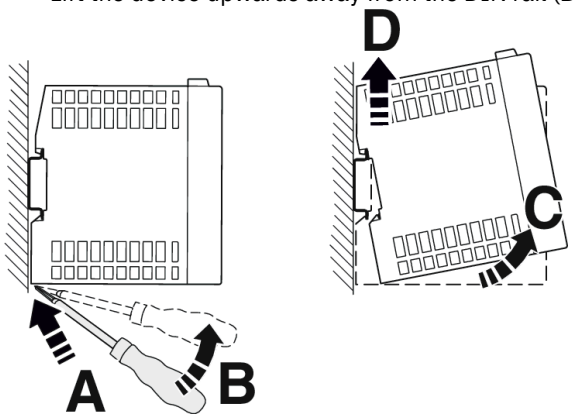


Figure 3-10 Removing the device

3.3.1 Selecting a conductor

The devices are supplied with Push-in connectors (COMBICON connectors). Observe the specifications for suitable conductors and ferrules:

Table 3-6 Selection of conductors/ferrules/screwdrivers

Conductor	Push-in	Screw
Conductor cross-section, rigid, min.	0.14 mm^2	
Conductor cross-section, rigid, max.	1.5 mm^2	
Conductor cross-section, flexible, min.	0.14 mm^2	
Conductor cross-section, flexible, max.	1.5 mm^2	
Conductor cross-section, flexible, with ferrule without plastic sleeve, min.	0.25 mm^2	
Conductor cross-section, flexible, with ferrule without plastic sleeve, max.	1.5 mm^2	
Conductor cross-section, flexible, with ferrule with plastic sleeve, min.	0.25 mm^2	
Conductor cross-section, flexible, with ferrule with plastic sleeve, max.	0.75 mm^2	0.5 mm^2
Suitable ferrule without plastic sleeve: maximum conductor cross-section	1.5 mm^2	
Suitable ferrule without plastic sleeve: maximum conductor cross-section	0.75 mm^2 (color code: gray, in accordance with DIN 46228)	0.5 mm^2 (color code: white, in accordance with DIN 46228)
Conductor cross-section, AWG, min.	24	
Conductor cross-section, AWG, max.	16	
Stripping length	9 mm	

Table 3-7 Specifications for ferrules

Recommended crimping pliers	1212034 CRIMPFOX 6
Ferrules without insulating collar, in accordance with DIN 46228-1	Cross-section: 0.25 mm^2; Length: 7 mm
	Cross-section: 0.34 mm^2; Length: 7 mm
	Cross-section: 0.5 mm^2; Length: 8 mm ... 10 mm
	Cross-section: 0.75 mm^2; Length: 8 mm ... 10 mm
	Cross-section: 1 mm^2; Length: 8 mm ... 10 mm
	Cross-section: 1.5 mm^2; Length: 10 mm

3.4 Connecting the supply voltage

NOTE: Electrical voltage

The module is designed exclusively for operation with safety extra-low voltage (SELV/PELV). In redundant operation, both power supplies must satisfy the requirements of the safety extra-low voltage. Provide overcurrent protection (I ≤ 5 A) in the installation.

The device is operated using a 24 V DC voltage.

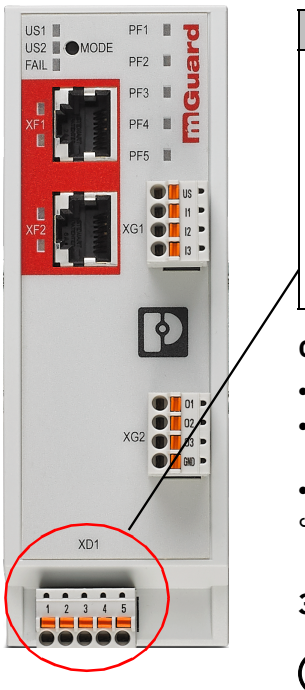


Table 3-8 Power supply via COMBICON connector

COMBICON	1	2	3	4	5
XD1	**US1**	**GND**	**US2**	**GND**	**Functional ground**
1 2 3 4 5 US1 GND US2 GND FE			**(FL MGUARD 4302/4305)**		⏚
	12...36 V	0 V	12...36 V	0 V	FE

Connecting the supply voltage

- Remove COMBICON connector **XD1** from the device.
- Connect the supply voltage to the COMBICON connector. Observe the polarity (see Table 3-8).
- Plug COMBICON connector **XD1** onto the device.

↪ As soon as one or both US LEDs are lit, the device is connected.

3.4.1 Grounding the device

NOTE: Risk of injury due to voltage

To prevent accidents due to electrical voltage, the device must be grounded correctly, taking the local conditions into account.

The devices must be grounded in order to shield the data telegram from any possible interference and to discharge such interferences to ground potential.

Grounding the device

- Mount the module on a grounded DIN rail.
- Functional grounding of the module is achieved when the module is snapped onto the grounded DIN rail or via **clamping point 5** (functional ground – FE ⏚) of COMBICON connector **XD1**.

3.5 Connecting to the network

The network can be connected (depending on the device) via RJ45 ports using twisted pair cables (IEEE 802.3i/u/ab).

NOTE: Telecommunications connections
Connect the network connections (Ethernet) of the device to LAN installations only. Some telecommunications connections also use RJ45 connections; these must not be connected to the RJ45 connections of the device.

For operation with 1000 Mbps (Gigabit), the following applies: Cables with four twisted pairs (eight wires) that meet the requirements of CAT5e as a minimum must be used.

3.5.1 Using RJ45 Ethernet connectors

Table 3-9 Pin assignment of the RJ45 connectors

Pin number	10Base-T (10 Mbps/s)	100Base-TX (100 Mbps/s)	1000Base-T (1000 Mbps/s)
1	TD+ (transmit)	TD+ (transmit)	BI_DA+ (bidirectional)
2	TD- (transmit)	TD- (transmit)	BI_DA- (bidirectional)
3	RD+ (receive)	RD+ (receive)	BI_DB+ (bidirectional)
4	–	–	BI_DB- (bidirectional)
5	–	–	BI_DC+ (bidirectional)
6	RD- (receive)	RD- (receive)	BI_DC- (bidirectional)
7	–	–	BI_DD+ (bidirectional)
8	–	–	BI_DD- (bidirectional)

Connecting RJ45 Ethernet connectors

- Observe the correct connector coding (see also Table 3-9).
- Only use twisted pair cables with an impedance of 100 Ω and a length of maximum 100 m (per segment).
- Only use shielded twisted pair cables and corresponding shielded RJ45 connectors. Insert the Ethernet cable with the RJ45 connector into a port of the twisted pair interface (network interface 1 or 2), until the connector engages with a click.

3.6 Connecting switching inputs and switching outputs (I/Os)

NOTE: Do not connect the voltage and ground outputs (**O1–3** and **GND**) to an external voltage source.

The connecting cables for inputs and outputs must not be longer than 30 meters.

Alternative designation of the I/Os in the WBM: "CMD" = "I" and "ACK" = "O" .

A push button or an on/off switch (e.g., key switch) can be connected between service contacts **US** and **I** (**1–3**) (see Table 3-10).

The service contacts can be used for various switching or signaling tasks.

The switching inputs can be connected to signals from external devices, e.g., to signals of a machine controller (PLC). In this case, ensure they have the same potential, and observe specifications on permissible voltage and current.

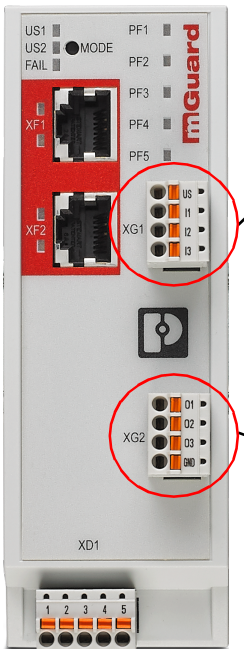


Table 3-10 **Input I1-3**: service contacts via COMBICON connector

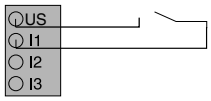
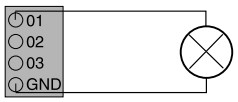
COMBICON XG1	Input (I1–3)		Example
			
	US	Voltage output (**US**) (+) (Short-circuit-proof)	
	I1	Switching inputs **(I1–3)**	
	I2		
	I3		

Table 3-11 **Output O1–3**: Service contacts via COMBICON connector

COMBICON XG2	Output (O1–3)		Example
			
	O1	Switching outputs (**O1–3**) Short-circuit-proof switching output (24 V DC)	
	O2		
	O3		
	GND	Ground connection (**GND**) (–) 0 V	

Switching outputs O1-3 are non-floating, continuously short-circuit-proof and suitable for a maximum of 250 mA at 12 ... 36 V DC.

Connecting I/Os

The COMBICON connectors of the service contacts may be removed or inserted during operation of the device.

- Remove COMBICON connector **XG1** or **XG2** from the device.
- Connect the desired connecting cable to the COMBICON connector (see Table 3-10 and 3-11).
- Plug COMBICON connector **XG1** or **XG2** onto the device.

3.7 Using an SD card

Please note that correct function of the SD card and the product can only be ensured when using a Phoenix Contact SD card (e.g., SD FLASH 2GB - 2988162).

Ensure that unauthorized persons do not have access to the SD card.

When using SD cards from other providers, it is recommended that card compatibility be verified .

The SD card holder is located on the back of the device.

Technical requirement of the SD card:

– SD and SDHC cards up to max. 8 GB
– VFAT compatible file system

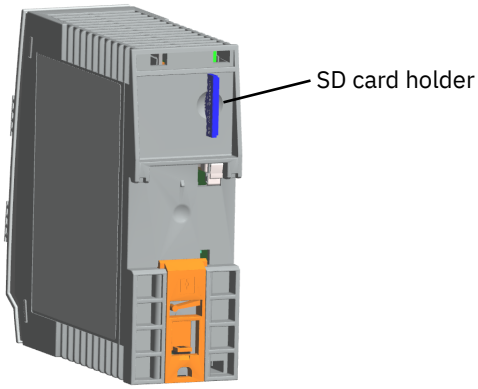


Figure 3-11 SD card holder on the back of the device

4 FL MGUARD 4102 PCI(E)

Table 4-1 Currently available products

Product designation	Phoenix Contact item number
FL MGUARD 4102 PCI	1441187
FL MGUARD 4102 PCIE	1357842

Product description

The FL MGUARD 4000 series devices are security routers with intelligent stateful packet inspection firewall and integrated IPsec VPN and OpenVPN with up to 250 VPN tunnels. They are designed for use in industry to accommodate strict distributed security and high availability requirements.

The FL MGUARD 4102 PCI(E) has the form of a PCI-compatible plug-in card. It is available in two versions:

– **FL MGUARD 4102 PCI** for devices or machines with PCI bus.
– **FL MGUARD 4102 PCIE** for devices or machines with PCI Express bus.

In this manual, the designation FL MGUARD 4102 PCI(E) is used for both versions for simplification.

Figure 4-1 FL MGUARD 4102 PCI(E)

4.1 Device description

The device provides the following network connections:

– **Network interface XF1/WAN**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface XF2/LAN**: Ethernet 10/100/1000 Mbps (RJ45 port)

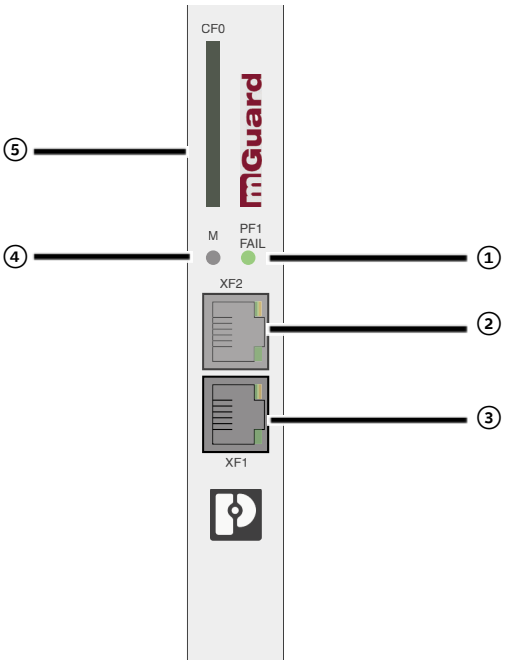


Figure 4-2 FL MGUARD 4102 PCI(E): Operating elements and LEDs

① Status and diagnostic LEDs
(see Section 4.2.2)

② Network interface XF2/**LAN** (RJ45 Ethernet port) (see Section 4.4)
SPD LED (top)
LNK/ACT (bottom) (see Section 4.2.1)

③ Network interface XF1/**WAN** (RJ45 Ethernet port) (see Section 4.4)
SPD LED (top)
LNK/ACT LED (bottom) (see Section 4.2.1)

④ Mode button
(see Section 6)

⑤ SD card holder
(see Section 4.5)

4.2 LED status and diagnostic indicators

The status and diagnostic LEDs indicate different system and error states of the device (see Table 4-2 and Table 4-3).

4.2.1 SPD and LNK/ACT

The LNK/ACT (*Link/Activity)* and SPD (*Speed*) LEDs indicate the status of the network connection of the related network port (see Table 4-2).

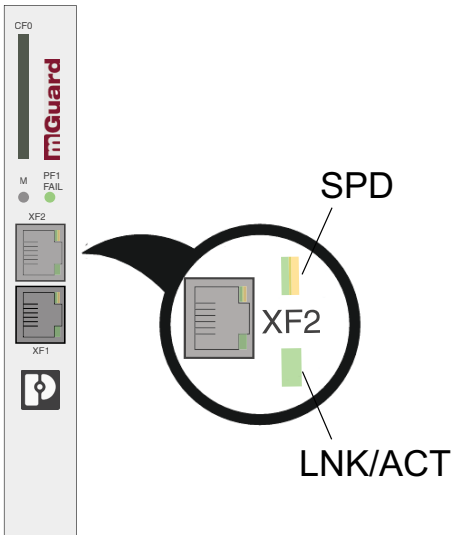


Figure 4-3 LEDs: SPD and LNK/ACT

Table 4-2 LEDs: SPD and LNK/ACT

Designation	Color	Status	Meaning
SPD (XF1/2)	Green/orange	On (orange)	1000 Mbps (Gigabit Ethernet)
		On (green)	100 Mbps (Fast Ethernet)
		Off	10 Mbps (Ethernet) (if LNK/ACT LED is active) **or** Inactive - no data transmission (if LNK/ACT LED is inactive)
LNK/ACT (XF1/2)	LANGreen	On	Link active
		Flashing	Data packets are being transmitted.
		Off	Link not active
SPD and LNK/ACT	Various LED light codes	**Rescue procedure / Flashing the firmware** See Section 6.3, “Flashing the firmware (Rescue mode)”	

4.2.2 PF1 / FAIL

The PF1 / FAIL LED (green/red) indicates different statuses and error states of the device.

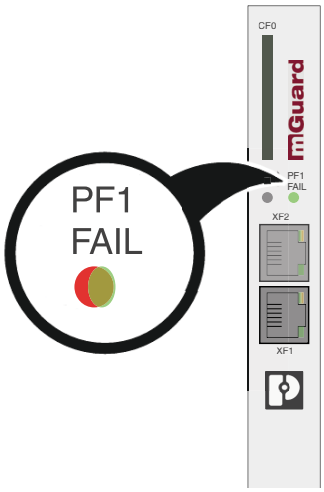


Figure 4-4 LED: PF1 / FAIL

Table 4-3 LED: PF1 / FAIL

Designation	Color	Status	Description
PF1 / FAIL	Red/Green	Flashing	**Boot process.** When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
	Green	Flashing	**Heartbeat.** The device is connected correctly and ready to operate.
	Red	Flashing	**System error.** Restart the device. • Press the Mode button (for 5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the rescue procedure (Flashing) (see Section 6, “Smart mode”) or contact your supplier.

4.3 Mounting and removal

4.3.1 Safety notes

To ensure correct operation and the safety of the environment and of personnel, the device must be installed, operated, and maintained correctly.

NOTE: Device damage
Only mount or remove the device when disconnected from the voltage.

NOTE: Electrostatic discharge
Before installation, touch the metal frame of the PC in which the device is to be installed, in order to remove electrostatic discharge.

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-2.

NOTE: Live circuits
Safe isolation of live circuits is only guaranteed if connected devices fulfill requirements specified by VDE 0106-101 (safe isolation). The supply lines must be isolated or laid separately to live circuits.

NOTE: Radio interference
This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

4.3.2 Mounting the device

Install the FL MGUARD PCI4000 in a free PCI or PCI Express slot (PCI: 3.3 V and 5 V | PCIE: 3.3 V and 12 V). Observe the notes in the documentation for your system.

4.4 Connecting to the network

The network can be connected (depending on the device) via RJ45 ports using twisted pair cables (IEEE 802.3i/u/ab).

NOTE: Telecommunications connections
Connect the network connections (Ethernet) of the device to LAN installations only. Some telecommunications connections also use RJ45 connections; these must not be connected to the RJ45 connections of the device.

For operation with 1000 Mbps (Gigabit), the following applies: Cables with four twisted pairs (eight wires) that meet the requirements of CAT5e as a minimum must be used.

4.4.1 Using RJ45 Ethernet connectors

Table 4-4 Pin assignment of the RJ45 connectors

Pin number	10Base-T (10 Mbps/s)	100Base-TX (100 Mbps/s)	1000Base-T (1000 Mbps/s)
1	TD+ (transmit)	TD+ (transmit)	BI_DA+ (bidirectional)
2	TD- (transmit)	TD- (transmit)	BI_DA- (bidirectional)
3	RD+ (receive)	RD+ (receive)	BI_DB+ (bidirectional)
4	–	–	BI_DB- (bidirectional)
5	–	–	BI_DC+ (bidirectional)
6	RD- (receive)	RD- (receive)	BI_DC- (bidirectional)
7	–	–	BI_DD+ (bidirectional)
8	–	–	BI_DD- (bidirectional)

Connecting RJ45 Ethernet connectors

- Observe the correct connector coding (see also Table 4-4).
- Only use twisted pair cables with an impedance of 100 Ω and a length of maximum 100 m (per segment).
- Only use shielded twisted pair cables and corresponding shielded RJ45 connectors. Insert the Ethernet cable with the RJ45 connector into a port of the twisted pair interface (network interface 1 or 2), until the connector engages with a click.

4.5 Using an SD card

Please note that correct function of the SD card and the product can only be ensured when using a Phoenix Contact SD card (e.g., SD FLASH 2GB - 2988162).

Ensure that unauthorized persons do not have access to the SD card.

When using SD cards from other providers, it is recommended that card compatibility be verified .

The SD card holder is located on the front of the device (see Section 4.1).

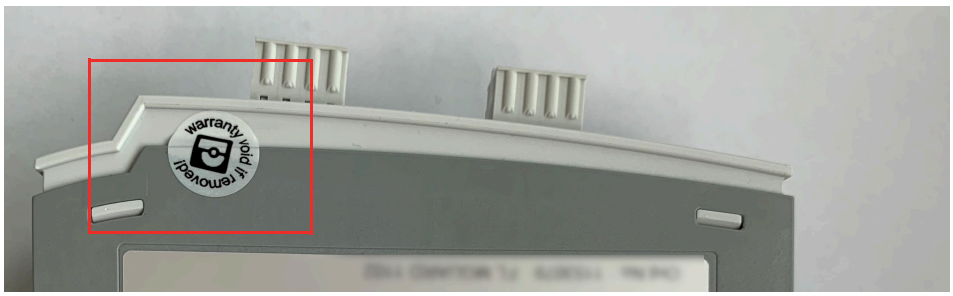
Technical requirement of the SD card:

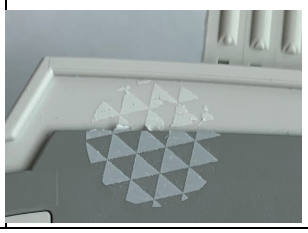
– SD and SDHC cards up to max. 8 GB
– VFAT compatible file system

5 Initial startup

The initial startup for the device is done in *Router mode*.

To prevent tampering with the device supplied and to detect unauthorized opening of the device, a security seal has been attached to the housing of DIN rail devices and to the packaging of PCI cards.
Before using the appliance for the first time, check that the seal is intact. If the seal is removed/damaged, parts of the seal would remain on the housing/packaging.



Intact	Damaged (partly)	Removed
		

Router mode (see Section 5.3)

- The device is operated as router/gateway between two subnets.
- The IP configuration of the device and the connected devices has to be adapted to the respective own network structure.
- All devices of the internal LAN network (XF2-4 or XF2-5) can automatically obtain their IP configuration from the device per DHCP.
- The firewall of the device automatically protects all devices connected via the LAN ports against external network access from the external WAN network (XF1).
- Desirable external access to protected devices can be specifically permitted (firewall and NAT rules).
- In principle, the protected devices in the LAN network can access all devices in both networks.
- The protected devices in the LAN network can access services of the device (HTTPS (WBM), SSH, DHCP, DNS).

5.1 Required components

– Network cable (Ethernet)
– 24 V power supply (only rail mounted devices)

5.2 Connection requirements

5.2.1 Local configuration via the LAN port

– The computer that is to be used for configuration must be connected to one LAN port (XF2-5) on the device (see also Section 5.3).

5.2.2 Remote configuration via the WAN port

An initial remote configuration via the WAN port (HTTPS or SSH) is not possible because this is prevented by the preset firewall rules (see also Section 5.4).

5.3 Operating the device in router mode

If the device is operated in *router mode*, it acts as gateway between different subnets (see Figure 5-1).

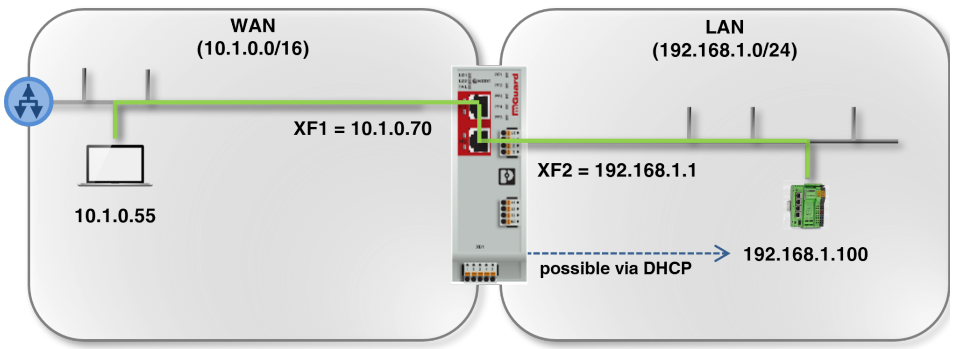


Figure 5-1 Operating the device in *router mode* (example configuration)

The data is *routed* between the two network interfaces of the device.

In the factory settings, the data traffic from WAN to LAN is blocked by the firewall.

However, it is possible for clients in one network to communicate and exchange data among each other and with clients from the other network:

– With the firewall functions, network access to individual or several network clients can be specifically permitted or blocked.
– With the NAT functions, data exchange between the networks can be enabled.

5.3.1 Starting the device

To start the device (DIN rail devices), proceed as follows:

- Connect the device with an external power supply (see Section 3.4, “Connecting the supply voltage”).

↪ The FAIL LED briefly lights up in red.

↪ During the boot process, the PF5 LED lights up red.

↪ The device is ready for operation when the PF1 LED flashes green (heartbeat).

↪ **PCI cards:** the device is ready for operation when the PF1 LED flashes green (heartbeat).

5.3.2 Establishing a network connection to the device

The IP configurations used in the following example have been randomly chosen. Adapt the IP configuration to your network environment to avoid address conflicts.

To configure the device by means of a web browser (web-based management), you first have to connect it to a configuration computer (see Figure 5-2).

Below, configuration of the device via LAN interface (e.g. XF2) is described. (In factory settings, the configuration via the WAN interface s not possible.)

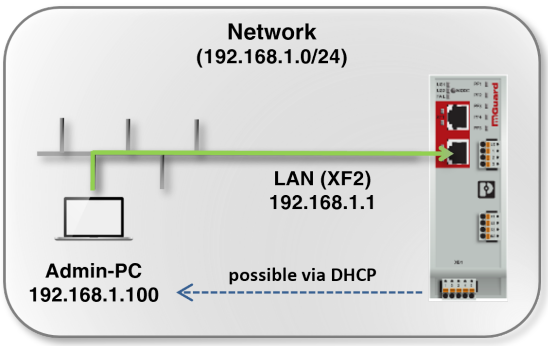


Figure 5-2 Establishing a network connection to the device (example)

Requirement

The device and the configuration computer (admin PC) has to be in the same subnet. An example of a network configuration is provided in Table 5-1.

Table 5-1 IP configuration (example): establishing a network connection

Device	IP	Net mask	Gateway
Device (Factory settings for XF2)	192.168.1.1	24 (255.255.255.0)	-
Configuration computer (**Example:** Assigned by the device per **DHCP** or **static** configuration.)	192.168.1.100	24 (255.255.255.0)	192.168.1.1

Procedure

- Either directly or via the network, connect the configuration computer with a network port (e.g. XF2) of the LAN interface of the device (see Figure 5-2).
- The IP setting of the configuration computer can be assigned automatically per DHCP, or a static configuration can be made (see below).

↪ If the configuration computer has already been configured to obtain its IP setting via DHCP, the device automatically assigns it an IP configuration (e.g. 192.168.1.100/24) in the **factory settings**, via the LAN interface (XF2).

Checking the IP configuration

- Example: Open the Windows start menu and type *"cmd"* to open a command line.
- Enter the command "*ipconfig*" and press the Enter button.

↪ *IPv4 address*, *subnet mask* and *default gateway* of the Ethernet adapter are displayed.

Obtaining the IP setting per DHCP (Windows 10)

To automatically obtain the IP setting of the configuration computer, proceed as follows (e.g. Microsoft Windows):

- Open the Windows start menu and type *"Control Panel"*.
- Open (*Network and Internet*) / *Network and Sharing Center*
- Click on "*Change adapter settings*".
- Right-click the desired network adapter and select the "*Properties*" command.
- Double-click on "*Internet Protocol, Version 4 (TCP/IPv4)*".

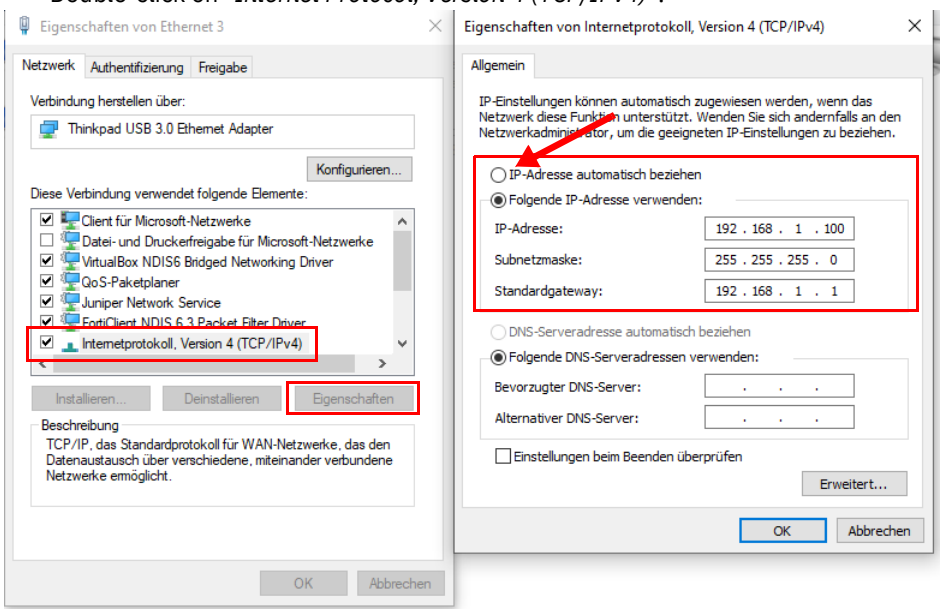


Figure 5-3 Changing the IP setting of the configuration computer (admin PC)

- Select "*Obtain an IP address automatically*".
- Confirm with "*OK*".

↪ The device assigns an IP address from subnet 192.168.1.0/24 (e.g. 192.168.1.100) to the configuration computer.

↪ The device serves as default gateway for the configuration computer.

Manually entering a static IP setting

To configure static IP settings for the configuration computer (Windows), proceed as follows:

- Open the Windows start menu and type *"Control Panel"*.
- Proceed as described above.
- Select "*Use the following IP address*".
  - Enter the values in accordance with the example in Figure 5-3 / Table 5-1.

- Confirm with “*OK*”.

↪ You have assigned an IP address from subnet 192.168.1.0/24 to the configuration computer.

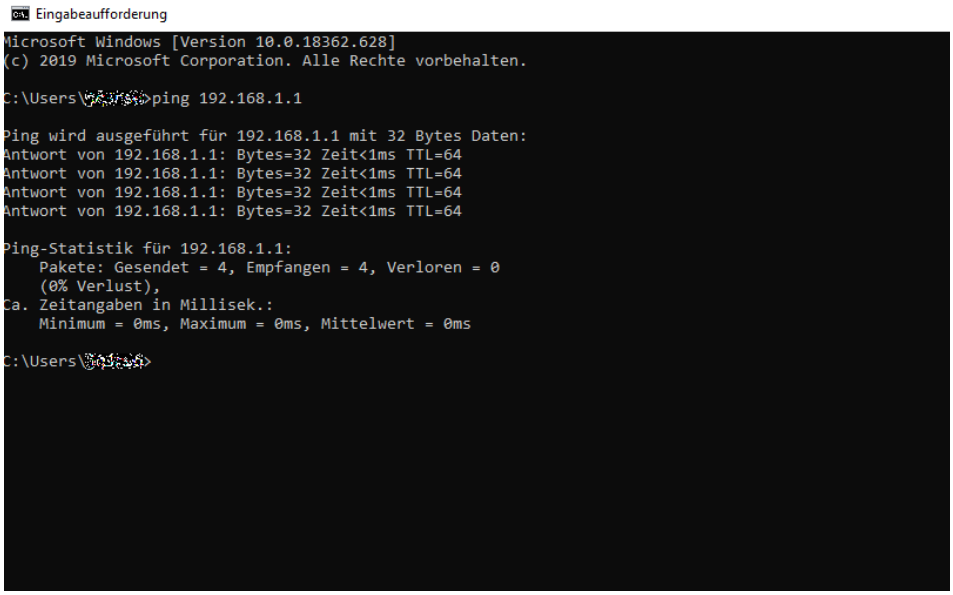
↪ The device serves as default gateway for the configuration computer.

Testing the connection

To test whether a configuration computer can reach the device via the network, proceed as follows:

- Open the Windows start menu and type *“cmd”* to open a command line.
- Enter the command “*ping 192.168.1.1*” and press the Enter button.

↪ From the answer to the ping request, you can tell whether the device reacts to requests from the configuration computer.



5.3.3 Assigning the IP address via BootP

After assigning an IP address via BootP, access via IP address 192.168.1.1 is no longer possible.

The device uses the BootP protocol for IP address assignment. The IP address can also be assigned via BootP. Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment.

Notes on BootP

During initial startup, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests. It can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the device no longer sends BootP requests, not even after it has been restarted. For the device to send BootP requests again, it must either be set to the default settings or one of the procedures (recovery or flash/rescue) must be performed.

5.3.4 If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the current address is unknown, the device can be reset to the default settings specified above for the IP address using the **Recovery** procedure (see Section 6.2).

If the administrator web page is not displayed

If the web browser repeatedly reports that the page cannot be displayed, try the following:

- Deactivate any active firewalls.
- Make sure that the browser does not use a proxy server.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

After successful connection establishment

Once a connection has been established successfully, a security alert may be displayed:

As administrative tasks can only be performed using encrypted access, a self-signed certificate is supplied with the device:

- Acknowledge corresponding security prompts with “Yes”, “OK”, “Next”, etc.

↪ The login window is displayed.

Figure 5-4 Login

- To log in, enter the preset user name and password (please note these settings are case-sensitive):

User name:	admin	root
Password:	mGuard	root

The number of simultaneous web sessions (HTTPS) is limited to 10 for the users *root*, *admin*, *netadmin* and *audit*.

The device can then be configured via the web interface. Information on this is available in the user manual UM EN FW MGUARD10 “Web-based management” in the Phoenix Contact online shop at phoenixcontact.net/product/1357828.

For security reasons, change the root and administrator passwords during initial configuration.

5.4 Remote configuration

The option for remote configuration is deactivated and blocked by the firewall settings by default.

Remote access is activated under **Management >> System Settings >> Shell Access** or **Management >> Web Settings >> Access**.

Requirement

The device must be configured so that remote configuration is permitted.

Switch on the remote access option in the web interface under **Management >> System Settings >> Shell Access** or **Management >> Web Settings >> Access**. Also configure the "Allowed networks" at this location.

Procedure

To configure the device via its web user interface from a remote computer, establish the connection to the device from there.

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the device can be accessed externally over the Internet or WAN port (XF1), together with the port number (if required).

Example

If the device can be accessed over the Internet, for example, via address https://123.45.67.89 and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer: https://123.45.67.89/

If a different port number is used, it should be entered after the IP address, e.g., https://123.45.67.89:442/

Configuration

The device can then be configured via the web interface. Information on this is available in the user manual UM EN FW MGUARD10 “Web-based management” in the Phoenix Contact online shop at phoenixcontact.net/product/1357828.

5.4.1 Protecting network clients

- Connect the devices to be protected with **the internal network (LAN)** of the device via one LAN network port (**XF2-4 or XF2-5**).

  (To protect more devices, connect them to the device via an additional switch.)
- Connect the surrounding network to **the external network (WAN)** via a switch via the network port (**XF1**).

↪ All network packets WAN --> LAN are rejected.

↪ All network packets LAN --> WAN are accepted and forwarded.

5.5 Starting up a device with a stored configuration from an SD card

To start up a device with a stored configuration from an SD card, you can save and restore configuration profiles via the WBM (see user manual UM EN FW MGUARD10 “Web-based management” in the Phoenix Contact online shop at phoenixcontact.net/product/1357828).

5.6 Using web-based management

5.6.1 Supported web browsers

The current versions of the following web browsers are supported:

– *Mozilla Firefox, Google Chrome, Microsoft Edge*

5.6.2 Supported users

The users *admin* and *root* can log in to the device (all available interfaces). They have functionally unrestricted access to the device. The number of simultaneous web sessions (HTTPS) is limited to 10. The number of simultaneous SSH logins (SSH sessions) can be configured.

5.6.3 Logging in to the device

To log in to the WBM of the device, proceed as follows:

- Connect the configuration computer to the device (see Section 5.2).
- Start a web browser on the configuration computer.
- Enter the IP address of the connected network interface of the device in the address line of the web browser (e.g., **https**://192.168.1.1).

↪ Since Phoenix Contact supplied the device with a self-signed security certificate that is unfamiliar to your browser, a certificate warning appears.

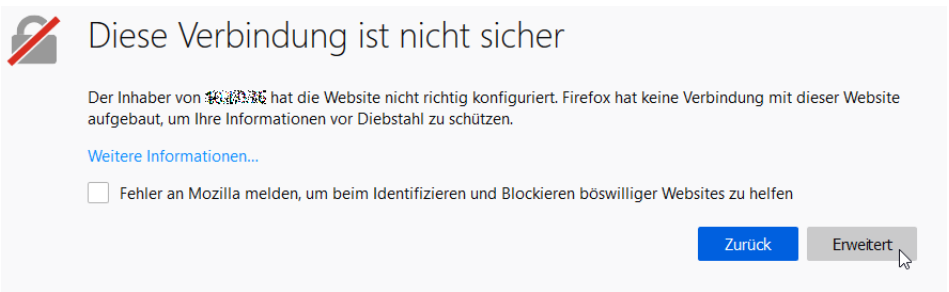


Figure 5-5 Certificate warning (Firefox)

- Confirm that you want to proceed in spite of the warning, by adding an exception to open the website that is deemed “*insecure*”.
- For example, in Firefox, click on:
  Advanced >> Add Exception... >> Confirm Security Exception
- Proceed in the same way in other browsers.

↪ The login page of web-based management opens.

Figure 5-6 Login page of web-based management

- Log in with the *admin* or *root* user name and the associated administrator password (default settings: *mGuard* or *root*).

↪ The start page for web-based management opens.

The number of simultaneous web sessions (HTTPS) is limited to 10 for the users *root*, *admin*, *netadmin* and *audit*.

The functions that can be configured by means of web-based management are described in the user manual UM EN FW MGUARD10 “Web-based management” in the Phoenix Contact online shop at phoenixcontact.net/product/1357828.

5.7 Restarting the device (reboot)

NOTE: All changes that have not been saved will be lost.

To restart (*reboot*) a device that is ready for operation, proceed as follows:

– Option 1: Press the Mode button (5 seconds).
– Option 2: Briefly interrupt the power supply.
– Option 3: Restart the device via WBM.

5.8 Using the Generic Administration Interface (GAI)

To configure the device using GAI or to retrieve information from the device, you must first log in to the device via SSH connection.

The configuration of the device via *Generic Administration Interface* (GAI) is described in the user manual UM EN GAICONFIG MGUARD10 (available e.g., at phoenixcontact.net/product/1357828).

6 Smart mode

With the Smart mode, you can call up device functions without having access to a management interface of the device. The following Smart mode functions are available:

– “Restart”
– “Restoring the configuration access (Recovery mode)”
– “Flashing the firmware (Rescue mode)”
– “Taking the device out of operation (Decommissioning Mode)”

6.1 Restart

NOTE: All changes that have not been saved will be lost.

Application

The operational device is to be restarted with the configured settings.

Result

– The device is restarted.

Procedure (rail mounted devices)

- Press and hold the Mode button for approx. 3 seconds until the **“PF5” LED** lights up red.
- Release the Mode button.

↪ The device is restarted.

Procedure (PCI cards)

- Press and hold the Mode button for approx. 3 seconds.
- Release the Mode button.

↪ The device is restarted.

6.2 Restoring the configuration access (Recovery mode)

Passwords are retained and are not reset to default settings.

Applications

– The IP configuration of the device is not known. It is therefore no longer possible to access the device.
– Portions of the device configuration (admin/root passwords and the active configuration profile excluded) are to be reset to the default settings.

Result

– The device is reset to the default settings (admin and root passwords excluded).
– Before performing the recovery procedure, the current device configuration is stored in a newly created configuration profile (“Recovery DATE”).
– Accessing the device via the default IP address is possible again:

Table 6-1 Restored default settings

LAN interface (XF2-4 or XF2-5) Management IP	WAN-Interface (XF1)
192.168.1.1	Network mode: Router Router mode: DHCP External requests to the WAN interface are blocked by the firewall.

Procedure (rail mounted devices)

- Press the Mode button six times.
- Wait approximately two seconds until the **PF1 LED** lights up green.
- Press the Mode button again six times.

↳ The device is reset to the default settings and restarted.
↳ The device is ready to operate when the PF5 LED (red) has gone out and the PF1 LED flashes green (heartbeat).

Procedure (PCI cards)

- Press the Mode button six times.
- Wait approximately two seconds until the **PF1 LED** lights up green.
- Press the Mode button again six times.

↳ The device is reset to the default settings and restarted.
↳ If successful, the PF1 LED lights up green. If unsuccessful, the PF1 LED lights up red.
↳ The device is ready to operate when the PF1 LED flashes green (heartbeat).

The configuration profile with the designation “Recovery DATE” subsequently appears in the list of configuration profiles and can be edited and restored with or without changes.

Restoring the saved configuration profile

- After completing the recovery procedure, log on to the web interface of the device.
- Open the **Management >> Configuration Profiles** menu.
- Select the configuration profile created during the recovery procedure named “Recovery-DATE” (e.g., “Recovery-2022.04.01-18:02:50”).
- Click on the “Edit profile” icon to analyze the configuration profile and subsequently restore it with or without changes.
- Click on the “Save” icon to apply the changes.

6.3 Flashing the firmware (Rescue mode)

Applications

– A new firmware version is to be installed on the device.
– The administrator password is not known. It is therefore no longer possible to log in to the device.
– The device is to be reset to the default settings.

Result

– The device is flashed with the new firmware version.
– The device will be reset to the default settings.

NOTE: Flashing the firmware deletes all passwords and configurations on the device. The device is reset to its default setting.

NOTE: From an installed firmware version mGuard 10.5.0, a downgrade to a lower firmware version is no longer possible. In this case, the PF5 LED lights up red, a restart is required.

Requirements

- Download the desired firmware version from the website: phoenixcontact.net/product <order_number>.
  – **Download file:** e.g., *Firmware-mGuard-10.5.0.zip*
  – **Update files** (= unpacked zip file):
  firmware.img.aarch64.p7s
  install.aarch64.p7s

6.3.1 Flashing (Procedure)

NOTE: Do not interrupt the power supply
Do not interrupt the power supply during the flash procedure. The device could be damaged. In this case, contact the manufacturer.

During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from an appropriately configured TFTP server if no SD card is found.

Downloading the flash files

- Open the product website in the Phoenix Contact online shop at: phoenixcontact.com/products.
- Select the *Downloads* tab and the *Firmware update* category.
- Download the desired **download file**: e.g., *Firmware-mGuard-10.5.0.zip*
- Unpack the zip file.
- Copy all unpacked files from the *aarch64* directory (*firmware.img.aarch64.p7s, install.aarch64.p7s*)
  - into a freely selected directory (e.g., */mGuard firmware*) on the TFTP server or
  - into the */Firmware* directory on the SD card.

For information on using SD cards, see Section 3.7 and 4.5.

FL MGUARD 2102/4302
FL MGUARD 2105/3405

Performing the flash procedure (rail mounted devices)

NOTE: A premature restart can damage the device
Do not interrupt the power supply! Always wait until the flash procedure has been completed (duration: approx. 2 minutes)

- Press and hold the Mode button of the device for approximately 10 seconds until all PF-LEDs (PF1–PF5) light up green.
- Release the Mode button. (Otherwise, the device will be restarted.)

↳ The flash procedure is starting.

↳ After approximately 20 seconds, the LEDs PF1, PF2 and PF3 light up in “Running light” mode (green). The FAIL LED lights up (red):
  - The device first searches for an inserted SD card and for the corresponding update files in the */Firmware* directory.
  - If the device does not find an SD card, it searches for a DHCP server via the LAN interface (XF2) in order to obtain an IP address.

↳ The files are loaded and installed from the SD card or from an existing TFTP server.

↳ After a total of approximately 60 seconds, the device will restart automatically.

↳ After the restart, the LEDs FAIL (red) and PF1 (green) light up permanently.

NOTE: Do not switch off the device prematurely in this state!
NOTE: Wait until the flash procedure is completely finished.

↳ After another 60 seconds, the PF1, PF2 and PF3 LEDs flash simultaneously (green).

↳ The flash procedure has been completed successfully.

- Restart the device by briefly pressing the Mode button or temporarily disconnecting the device from the power supply.

↳ The device is ready to operate when the LED PF1 flashes green (heartbeat).

FL MGUARD 4102 PCI(E)

Performing the flash procedure (PCI cards)

NOTE: A premature restart can damage the device
Do not interrupt the power supply! Always wait until the flash procedure has been completed (duration: approx. 2 minutes)

- Press and hold the Mode button on the front panel of the device for approximately 10 seconds until the **PF1 LED** as well as the **LEDs of the Ethernet sockets** (XF1/2) light up green.
- Release the Mode button. (Otherwise, the device will be restarted.)

↳ The flash procedure is starting.

↳ After approximately 20 seconds, the LEDs PF1/FAIL and SPD (XF1/2) light up in "Running light" mode (green):

  – The device first searches for an inserted SD card and for the corresponding update files in the */Firmware* directory.
  – If the device does not find an SD card, it searches for a DHCP server via the LAN interface (XF2) in order to obtain an IP address.

↳ The files are loaded and installed from the SD card or the existing TFTP server.

↳ After a total of approximately 60 seconds, the device will restart automatically.

↳ After the restart, the LED PF1/FAIL lights up permanently (green).

NOTE: Do not switch off the device prematurely in this state!

NOTE: Wait until the flash procedure is completely finished.

↳ After another 60 seconds, the LEDs PF1/FAIL and SPD (XF1/2) flash simultaneously (green).

↳ The flash procedure has been completed successfully.

- Restart the device by briefly pressing the Mode button.

↳ The device is ready to operate when the LED PF1 flashes green (heartbeat)

6.3.2 Uploading configuration profile during the flash process

You can automatically upload and activate a created configuration profile (ATV profile) onto the mGuard device during the flash process.

The flashing behavior of the LEDs after the flash process deviates in this case from the standard flashing behavior.

Preparation

Create the file *preconfig.sh* with the following contents. (Be aware that the file must be created in UNIX format.)

preconfig.sh: for **unencrypted** ATV profiles

```
#!/bin/sh -ex
exec gaiconfig --factory default --silent --set-all < /bootstrap/preconfig.atv
```

preconfig.sh: for **encrypted** ATV profiles (starting with firmware version mGuard 10.5.0)

```
#!/bin/sh -ex
/Packages/mguard-tpm2_0/mbin/tpm2_pkcs7 < /bootstrap/preconfig.atv.p7e > /bootstrap/preconf.atv
gaiconfig --factory-default --set-all < /bootstrap/preconf.atv
```

If you wish to upload a configuration profile encrypted with the device certificate, you should change the file's name from **.atv* to **.atv.p7e.* Encrypted and unencrypted configuration profiles can be kept apart easier in this way.

The device treats the ATV profile equally, independent of the file ending.

During the flash process, the device searches for the following files and uploads them:

- */Rescue Config/<Seriennummer>.atv*
- */Rescue Config/<Seriennummer>.atv.p7e*
- */Rescue Config/preconfig.atv*
- */Rescue Config/preconfig.atv.p7e*
- */Rescue Config/preconfig.sh*

Loading configuration profile from SD card

In order to upload and activate a configuration profile during the flash process, proceed as follows:

1. Besides the *Firmware* directory, also create the *Rescue Config* directory.
2. Rename the saved configuration profile as *preconfig.atv or <Seriennummer>.atv*.
3. Copy the configuration profile to the *Rescue Config* directory.
4. Copy the *preconfig.sh* file (UNIX-Format) to the *Rescue Config* directory.
5. Carry out the flash process as described for your device.

Loading configuration profile from the TFTP server

In order to load and activate a configuration profile during the flash process, see the description in Section Section 6.3.3.

6.3.3 Flashing (setting up DHCP and TFTP servers)

NOTE: Absatzformat „Note Bold“
Absatzformat „Note“

NOTE: Network problems
If you install a second DHCP server in a network, this could affect the configuration of the entire network.

NOTE: Third-party software
Phoenix Contact does not undertake any guarantee or liability for the use of third-party products. Any reference to third-party software does not constitute a recommendation, rather serves as an example of a program that could be used.

Under Windows

If you wish to use the third-party program “*TFTPD32.exe*”, obtain the program from a trustworthy source, and proceed as follows:

1. If the Windows PC is connected to a network, disconnect it from the network.
2. On the Windows PC, create a directory that you wish to use for the flash procedure of mGuard devices. This directory is later selected as root directory of the TFTP server. All the files required are loaded from this directory during the flash procedure.
3. Copy the desired firmware image file(s) into the created directory.
4. Start the *TFTPD32.exe* program.
   The host IP to be specified is: **192.168.10.1**. It must also be used as the address for the network card.
5. Click on **Browse** to select the folder where the mGuard image files are saved (e.g., *install.aarch64.p7s, firmware.img.aarch64.p7s*).

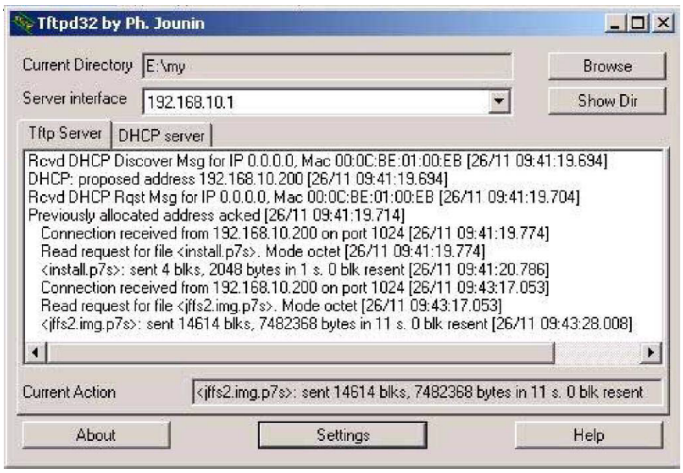
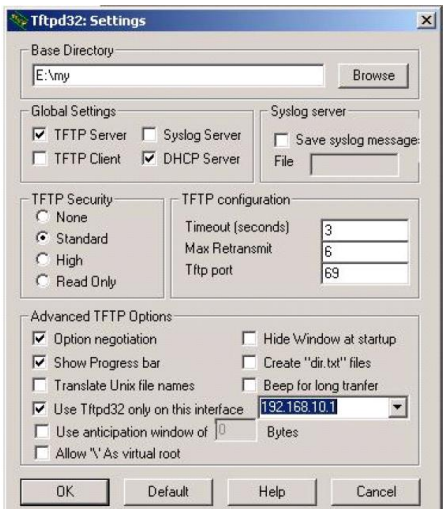


Figure 6-1 Entering the host IP

6. Switch to the “TFTP Server” or “DHCP Server” tab and click the “Settings” button to set the parameters as follows:



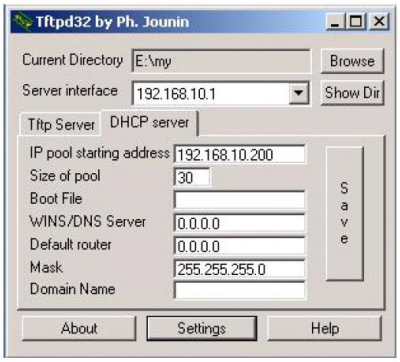


Figure 6-2 Settings

Under Linux

All current Linux distributions include DHCP and TFTP servers.

1. Install the corresponding packages according to the instructions provided for the respective distribution.
2. Configure the DHCP server by making the following settings in the */etc/dhcpd.conf* file:

   subnet 192.168.134.0 netmask 255.255.255.0 {
   range 192.168.134.100 192.168.134.119;
   option routers 192.168.134.1;
   option subnet-mask 255.255.255.0;
   option broadcast-address 192.168.134.255;}
   This example configuration provides 20 IP addresses (.100 to .119). It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file: */etc/inetd.conf*

3. In this file, insert the corresponding line or set the necessary parameters for the TFTP service. (Directory for data: */tftpboot*)

   tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

   The mGuard image files must be saved in the */tftpboot* directory:
   e.g., *install.aarch64.p7s, firmware.img.aarch64.p7s*.
4. Then restart the *inetd* process to apply the configuration changes.
5. If you are using a different mechanism, e.g., *xinetd*, please consult the corresponding documentation.

6.3.3.1 TFTP server: Error messages

During the flash process, the mGuard device searches by default for the files *rollout.sh, license.lic* and *<Seriennummer>.lic*. If these files are not available, a corresponding error message is displayed:

File rollout.sh: error 2 in system call CreateFile The system cannot find the file specified.

File <serial number>.lic : error 2 in system call CreateFile The system cannot find the file specified.

File licence.lic: error 2 in system call CreateFile The system cannot find the file specified.

The error message can be ignored if no licence file is uploaded, or the device should not be preconfigured via the *rollout.sh* script. The flash process is continued as planned in such cases.

6.4 Taking the device out of operation (Decommissioning Mode)

NOTE: All data on the device will be irrevocably deleted. The device cannot then be put back into operation by the customer.

NOTE: If you want to take the device out of operation and replace it with another mGuard device, you must first save the configuration of the device as an ATV file or on an SD card (see user manual "Web-based management" UM EN FW MGUARD10 - 110191_en_xx).

Applications

– The device is to be decommissioned and disposed of.
– The device is to be decommissioned and all data on the device is to be irrevocably deleted.
– The device is to be decommissioned and replaced with another device.

Result

– All data on the device is irrevocably deleted or overwritten:
  – File system
  – Trusted Platform Module
  – eMMC memory
  – Configurations
  – Passwords and private keys
  – Bootloader (will be overwritten with default settings)
– The device cannot be recommissioned by the customer.
– The device can be disposed of in accordance with the regulations.

6.4.1 Decommissioning (execution)

FL MGUARD 2102/4302
FL MGUARD 2105/4305

Execution (DIN rail devices)

NOTE: All data on the device will be irrevocably deleted. The device cannot then be put back into operation by the customer.

You can cancel each individual step by disconnecting the power supply or waiting 60 seconds without performing any action.

- Press the Mode button 9 times.
- Wait approx. 2 seconds until the LEDs PF1 to PF5 **light up** orange.
- Press the Mode button 9 times.
- Wait approx. 2 seconds until the LEDs PF1 to PF5 **flash** orange.
- Press the Mode button 3 times.

↳ All data on the device will be permanently deleted.
↳ The device will restart automatically.
↳ The process is complete when the LEDs PF1 to PF5 flash red.
↳ The device cannot be put back into operation by the customer.

FL MGUARD 4102 PCI(E)

Execution (PCI cards)

NOTE: All data on the device will be irrevocably deleted. The device cannot then be put back into operation by the customer.

You can cancel each individual step by disconnecting the power supply or waiting 60 seconds without performing any action.

- Press the Mode button 9 times.
- Wait approx. 2 seconds until the LED PF1 **lights up** orange.
- Press the Mode button 9 times.
- Wait approx. 2 seconds until the LED PF1 **flashes** orange.
- Press the Mode button 3 times.

↳ All data on the device will be permanently deleted.
↳ The device will restart automatically.
↳ The process is complete when the LED FAIL flashes red.
↳ The device cannot be put back into operation by the customer.

7 Device replacement, device defect, and repair

7.1 Secure deletion of sensitive data / Decommissioning

NOTE: Device Protect sensitive data from unauthorized third parties
To ensure that no protected data remains on the device during decommissioning and can be seen by unauthorized third parties, the data must be securely and irrevocably deleted.

NOTE: All data on the device will be irrevocably deleted. The device cannot then be put back into operation by the customer.

Proceed as follows:

- Remove the SD card if necessary.
- Execute the smart mode "Taking the device out of operation (Decommissioning Mode)" to securely delete data on the device (see Section 6.4).
- If an SD card is used, keep it protected from unauthorized third parties or delete its contents completely.

7.2 Device replacement

NOTE: Device damage
Only mount or remove the device when disconnected from the voltage.

Proceed as follows when replacing the device:

- Back up the customer-specific data (configurations, passwords, private keys, certificates) to an external data carrier (SD card/ECS).
- Remove the SD card.
- Remove all cables.
- Remove the device as described in Section 3.3 and 4.3.
- Replace the device with an identical device (the same Order No.), factory new or with factory settings (see Section 6).
- Restore a saved configuration of the previous device on the new device (see Section 7.2.1).
- (Optional) If you want to decommission the old device, run the smart mode “Taking the device out of operation (Decommissioning Mode)”. All data on the device will be securely deleted (see Section 6.4).

7.2.1 Restoring a saved configuration using an SD card (ECS)

For more information on using configuration profiles, see the UM DE FW MGUARD10 "Web-based management" user manual in the Phoenix Contact Web Shop at phoenixcontact.net/product/1357828.

7.3 Device defect and repair

Repairs may only be carried out by Phoenix Contact.

- Send defective devices back to Phoenix Contact for repair or to receive a replacement device.
- We strongly recommend using the original packaging to return the product.
- Include a note in the packaging indicating that the contents are returned goods.
- Include an error description with the returned product.
- If the original packaging is no longer available, observe the following points:
  - Observe the humidity specifications and the temperature range specified for transport (see Section 8).
  - If necessary, use dehumidifying agents.
  - Use suitable ESD packaging to protect components that are sensitive to electrostatic discharge.
  - Make sure that the packaging you select is large enough and sufficiently thick.
  - Only use plastic bubble wrap sheets as wadding.
  - Attach warnings to the transport packaging so that they are clearly visible.
  - Please ensure that the delivery note is placed inside the package if the package is to be shipped domestically. However, if the package is being shipped internationally, the delivery note must be placed inside a delivery note pocket and attached to the outside so that it is clearly visible.

7.4 Disposal

The symbol with the crossed-out trash can indicates that this item must be collected and disposed of separately. Phoenix Contact or our service partners will take the item back for free disposal. For information on the available disposal options, visit www.phoenixcontact.com.

Dispose of packaging materials that are no longer needed (cardboard packaging, paper, bubble wrap sheets, etc.) with household waste in accordance with the currently applicable national regulations.

8 Technical data

8.1 FL MGUARD 4305/KX

Table 8-1 Technical data (FL MGUARD 4305/KX)

General data	
Platform	Marvell Armada 3720
Network interfaces	5 Ethernet interfaces with: – 3 LAN ports (managed switch) | 1 WAN port | 1 DMZ port – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
Digital inputs and outputs	3 digital inputs and 3 digital outputs
Diagnostic tools	Status and diagnostic LEDs | digital I/Os | log files
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor
Ambient temperature (operation)	-40°C ... +60 °C
Ambient temperature (storage/transport)	-40°C ... +70 °C
Permissible humidity (operation)	5 % ... 95 % (non-condensing)
Degree of protection	IP20 (not tested by UL)
Protection class	Class III (VDE 0106; IEC 60536, indoor use only)
Overvoltage category	Class II (IEC 61010-1)
Air pressure (operation)	68 kPa ... 108 kPa, 3000 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Pollution degree	2
Mounting position	Perpendicular to a standard DIN rail
Connection to functional ground	When snapped onto a grounded DIN rail or via clamping point 5 of COMBICON connector XD1
Housing dimensions (width x height x depth) in mm	45 x 130 x 130 (depth from top edge of DIN rail)
Net weight	302 g 446 g

Firmware and power values	
Supported firmware	mGuard 10.4.1 or later
Management support	Web-based management (HTTPS) | SSH | GAI Config | SD card

Supply voltage (US1/US2) (US2 only with FL MGUARD 4305)	
Connection	Via COMBICON connector (Push-in spring connection); maximum conductor cross section = 1.5 mm^2 (use copper wires that are suitable for *90 °C* or equivalent)
Nominal value	24 V DC
Permissible voltage range	12 V DC ... 36 V DC
Permissible ripple (within the permitted voltage range)	3.6 V_{PP}
Maximum current consumption (US = min, T_{amb} = max, DO_I = max)	1.21 A
Typical current consumption (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0.16 A
Test voltage	500 V DC for one minute

Network interfaces	
Properties of RJ45 connections	
Number	5
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohm
Transmission speed	10/100/1000 Mbps/s
Maximum conductor length (twisted pair)	100 m (per segment)

Digital inputs and outputs	
Digital outputs	
Number	3
Voltage of output signal	12 V DC ... 36 V DC
Current carrying capacity	250 mA
Digital inputs	
Number	3
Voltage of input signal	0 V DC ... 36 V DC
Maximum input current	3,5 mA

Mechanical tests	
Vibration resistance in accordance with IEC 60068-2-6	Operation/storage/transport: 5g, 10 Hz ... 150 Hz
Free fall in accordance with IEC 60068-2-32	1 m

Conformance with EMC directives	
Developed in accordance with IEC 61000-6-2	
Noise emission in accordance with EN 55016-2-1:2014 (conducted noise emission)	Class B
Noise emission in accordance with EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (radiated noise emission)	Class A
Immunity in accordance with EN 61000-4-2 (IEC 1000-4-2) (ESD)	Requirements in accordance with DIN EN 61000-6-2
Contact discharge:	Test intensity 3, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 3, criterion B
Immunity in accordance with EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-4 (IEC 1000-4-4) (burst)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 3, criterion A
Power supply:	Test intensity 3, criterion A
Service contacts:	Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Service contacts:	Test intensity 1, criterion B

Approvals / Certificates	
ATEX	Ⓔx II 3 G Ex ec IIC T4 Gc (EN IEC 60079-0:2018, EN IEC 60079-7:2015/ A1:2018)
IECEx	Ex ec IIC T4 Gc (IEC 60079-0 Ed. 7 (2017-12) + Corr. 1 (2020-01), IEC 60079-7 Ed. 5.1 (2017-08))
UL, USA / Kanada	cULus
UL Ex, USA / Kanada	Class I, Division 2, Groups A, B, C und D, T4 Class I, Zone 2, AEx ec IIC T4 Ex ec IIC T4 Gc X UL 60079-0 Ed. 7 / UL 60079-7 Ed. 5, CSA C22.2 No. 60079-0 Ed. 4, CSA C22.2 No. 60079-7 Ed. 2
CCC / China-Ex	Ex ec IIC T4 Gc
UKCA Ex (UKEX)	Ⓔx II 3 G Ex ec IIC T4 Gc

8.2 FL MGUARD 4302/KX

Table 8-2 Technical data (FL MGUARD 4302/KX)

General data	
Platform	Marvell Armada 3720
Network interfaces	2 Ethernet interfaces with: – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
Digital inputs and outputs	3 digital inputs and 3 digital outputs
Diagnostic tools	Status and diagnostic LEDs | digital I/Os | log files
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor
Ambient temperature (operation)	-40°C … +60 °C
Ambient temperature (storage/transport)	-40°C … +70 °C
Permissible humidity (operation)	5 % … 95 % (non-condensing)
Degree of protection	IP20 (not tested by UL)
Protection class	Class III (VDE 0106; IEC 60536, indoor use only)
Overvoltage category	Class II (IEC 61010-1)
Air pressure (operation)	68 kPa … 108 kPa, 3000 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Pollution degree	2
Mounting position	Perpendicular to a standard DIN rail
Connection to functional ground	When snapped onto a grounded DIN rail or via clamping point 5 of COMBICON connector XD1
Housing dimensions (width x height x depth) in mm	45 x 130 x 130 (depth from top edge of DIN rail)
Net weight	302 g 446 g

Firmware and power values	
Supported firmware	mGuard 10.4.1 or later
Management support	Web-based management (HTTPS) | SSH | GAI Config | SD card

Supply voltage (US1/US2)	
Connection	Via COMBICON connector (Push-in spring connection); maximum conductor cross section = 1.5 mm^2 (use copper wires that are suitable for *90 °C* or equivalent)
Nominal value	24 V DC
Permissible voltage range	12 V DC … 36 V DC

Supply voltage (US1/US2)	
Permissible ripple (within the permitted voltage range)	3.6 V_{PP}
Maximum current consumption (US = min, T_{amb} = max, DO_I = max)	1.12 A
Typical current consumption (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0.12 A
Test voltage	500 V DC for one minute

Network interfaces	
Properties of RJ45 connections	
Number	2
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohm
Transmission speed	10/100/1000 Mbps/s
Maximum conductor length (twisted pair)	100 m (per segment)

Digital inputs and outputs	
Digital outputs	
Number	3
Voltage of output signal	12 V DC ... 36 V DC
Current carrying capacity	250 mA
Digital inputs	
Number	3
Voltage of input signal	0 V DC ... 36 V DC
Maximum input current	3,5 mA

Mechanical tests	
Vibration resistance in accordance with IEC 60068-2-6	Operation/storage/transport: 5g, 10 Hz ... 150 Hz
Free fall in accordance with IEC 60068-2-32	1 m

Conformance with EMC directives	
Developed in accordance with IEC 61000-6-2	
Noise emission in accordance with EN 55016-2-1:2014 (conducted noise emission)	Class B
Noise emission in accordance with EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (radiated noise emission)	Class A

Conformance with EMC directives	
Immunity in accordance with EN 61000-4-2 (IEC 1000-4-2) (ESD)	Requirements in accordance with DIN EN 61000-6-2
Contact discharge:	Test intensity 3, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 3, criterion B
Immunity in accordance with EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-4 (IEC 1000-4-4) (burst)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 3, criterion A
Power supply:	Test intensity 3, criterion A
Service contacts:	Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Service contacts:	Test intensity 1, criterion B

Approvals / Certificates	
ATEX	Ⓔx II 3 G Ex ec IIC T4 Gc (EN IEC 60079-0:2018, EN IEC 60079-7:2015/ A1:2018)
IECEx	Ex ec IIC T4 Gc (IEC 60079-0 Ed. 7 (2017-12) + Corr. 1 (2020-01), IEC 60079-7 Ed. 5.1 (2017-08))
UL, USA / Kanada	cULus
UL Ex, USA / Kanada	Class I, Division 2, Groups A, B, C und D, T4 Class I, Zone 2, AEx ec IIC T4 Ex ec IIC T4 Gc X UL 60079-0 Ed. 7 / UL 60079-7 Ed. 5, CSA C22.2 No. 60079-0 Ed. 4, CSA C22.2 No. 60079-7 Ed. 2
CCC / China-Ex	Ex ec IIC T4 Gc
UKCA Ex (UKEX)	Ⓔx II 3 G Ex ec IIC T4 Gc

8.3 FL MGUARD 2105 / FL MGUARD 4305

Table 8-3 Technical data (FL MGUARD 2105 / FL MGUARD 4305)

General data	
Platform	Marvell Armada 3720
Network interfaces	
FL MGUARD 2105	5 Ethernet interfaces with: – 4 LAN ports (unmanaged switch) | 1 WAN port – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
FL MGUARD 4305	5 Ethernet interfaces with: – 3 LAN ports (managed switch) | 1 WAN port | 1 DMZ port – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
Digital inputs and outputs	3 digital inputs and 3 digital outputs
Diagnostic tools	Status and diagnostic LEDs | digital I/Os | log files
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor
Ambient temperature (operation)	
FL MGUARD 2105	-20°C ... +60 °C
FL MGUARD 4305	-40°C ... +60 °C
Ambient temperature (storage/transport)	-40°C ... +70 °C
Permissible humidity (operation)	5 % ... 95 % (non-condensing)
Degree of protection	IP20 (not tested by UL)
Protection class	Class III (VDE 0106; IEC 60536, indoor use only)
Overvoltage category	Class II (IEC 61010-1)
Air pressure (operation)	68 kPa ... 108 kPa, 3000 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Pollution degree	2
Mounting position	Perpendicular to a standard DIN rail
Connection to functional ground	When snapped onto a grounded DIN rail or via clamping point 5 of COMBICON connector XD1
Housing dimensions (width x height x depth) in mm	45 x 130 x 130 (depth from top edge of DIN rail)
Net weight	302 g 446 g

Firmware and power values	
Supported firmware	mGuard 10.2.0 or later
Management support	Web-based management (HTTPS) | SSH | GAI Config | SD card

Supply voltage (US1/US2) (US2 only with FL MGUARD 4305)	
Connection	Via COMBICON connector (Push-in spring connection); maximum conductor cross section = 1.5 mm^2 (use copper wires that are suitable for *90 °C* or equivalent)
Nominal value	24 V DC
Permissible voltage range	12 V DC ... 36 V DC
Permissible ripple (within the permitted voltage range)	3.6 V_{PP}
Maximum current consumption (US = min, T_{amb} = max, DO_I = max)	1.21 A
Typical current consumption (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0.16 A
Test voltage	500 V DC for one minute

Network interfaces	
Properties of RJ45 connections	
Number	5
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohm
Transmission speed	10/100/1000 Mbps/s
Maximum conductor length (twisted pair)	100 m (per segment)

Digital inputs and outputs	
Digital outputs	
Number	3
Voltage of output signal	12 V DC ... 36 V DC
Current carrying capacity	250 mA
Digital inputs	
Number	3
Voltage of input signal	0 V DC ... 36 V DC
Maximum input current	3,5 mA

Mechanical tests	
Vibration resistance in accordance with IEC 60068-2-6	Operation/storage/transport: 5g, 10 Hz ... 150 Hz
Free fall in accordance with IEC 60068-2-32	1 m

Conformance with EMC directives	
Developed in accordance with IEC 61000-6-2	
Noise emission in accordance with EN 55016-2-1:2014 (conducted noise emission)	Class B
Noise emission in accordance with EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (radiated noise emission)	Class A
Immunity in accordance with EN 61000-4-2 (IEC 1000-4-2) (ESD)	Requirements in accordance with DIN EN 61000-6-2
Contact discharge:	Test intensity 3, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 3, criterion B
Immunity in accordance with EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-4 (IEC 1000-4-4) (burst)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 3, criterion A
Power supply:	Test intensity 3, criterion A
Service contacts:	Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Service contacts:	Test intensity 1, criterion B

8.4 FL MGUARD 2102 / FL MGUARD 4302

Table 8-4 Technical data (FL MGUARD 2102 / FL MGUARD 4302)

General data	
Platform	Marvell Armada 3720
Network interfaces	
FL MGUARD 2102 / FL MGUARD 4302	2 Ethernet interfaces with: – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
Digital inputs and outputs	3 digital inputs and 3 digital outputs
Diagnostic tools	Status and diagnostic LEDs | digital I/Os | log files
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor
Ambient temperature (operation)	
FL MGUARD 2102 FL MGUARD 4302	-20°C ... +60 °C -40°C ... +60 °C
Ambient temperature (storage/transport)	-40°C ... +70 °C
Permissible humidity (operation)	5 % ... 95 % (non-condensing)
Degree of protection	IP20 (not tested by UL)
Protection class	Class III (VDE 0106; IEC 60536, indoor use only)
Overvoltage category	Class II (IEC 61010-1)
Air pressure (operation)	68 kPa ... 108 kPa, 3000 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Pollution degree	2
Mounting position	Perpendicular to a standard DIN rail
Connection to functional ground	When snapped onto a grounded DIN rail or via clamping point 5 of COMBICON connector XD1
Housing dimensions (width x height x depth) in mm	45 x 130 x 130 (depth from top edge of DIN rail)
Net weight	302 g 446 g

Firmware and power values	
Supported firmware	mGuard 10.0.0 or later
Management support	Web-based management (HTTPS) | SSH | GAI Config | SD card

Supply voltage (US1/US2) (US2 only with FL MGUARD 4302)	
Connection	Via COMBICON connector (Push-in spring connection); maximum conductor cross section = 1.5 mm^2 (use copper wires that are suitable for *90 °C* or equivalent)
Nominal value	24 V DC
Permissible voltage range	12 V DC ... 36 V DC
Permissible ripple (within the permitted voltage range)	3.6 V_{PP}
Maximum current consumption (US = min, T_{amb} = max, DO_I = max)	1.12 A
Typical current consumption (US= 24 V, T_{amb} = 25 °C, DO_I = 0/OFF)	0.12 A
Test voltage	500 V DC for one minute

Network interfaces	
Properties of RJ45 connections	
Number	2
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohm
Transmission speed	10/100/1000 Mbps/s
Maximum conductor length (twisted pair)	100 m (per segment)

Digital inputs and outputs	
Digital outputs	
Number	3
Voltage of output signal	12 V DC ... 36 V DC
Current carrying capacity	250 mA
Digital inputs	
Number	3
Voltage of input signal	0 V DC ... 36 V DC
Maximum input current	3,5 mA

Mechanical tests	
Vibration resistance in accordance with IEC 60068-2-6	Operation/storage/transport: 5g, 10 Hz ... 150 Hz
Free fall in accordance with IEC 60068-2-32	1 m

Conformance with EMC directives	
Developed in accordance with IEC 61000-6-2	
Noise emission in accordance with EN 55016-2-1:2014 (conducted noise emission)	Class B
Noise emission in accordance with EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (radiated noise emission)	Class A
Immunity in accordance with EN 61000-4-2 (IEC 1000-4-2) (ESD)	Requirements in accordance with DIN EN 61000-6-2
Contact discharge:	Test intensity 3, criterion B
Air discharge:	Test intensity 3, criterion B
Indirect discharge:	Test intensity 3, criterion B
Immunity in accordance with EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-4 (IEC 1000-4-4) (burst)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 3, criterion A
Power supply:	Test intensity 3, criterion A
Service contacts:	Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Service contacts:	Test intensity 1, criterion B

8.5 FL MGUARD 4102 PCI / FL MGUARD 4102 PCIE

Table 8-5 Technical data (FL MGUARD 4102 PCI / FL MGUARD 4102 PCIE)

General data	
Platform	Marvell Armada 3720
Network interfaces	2 Ethernet interfaces with: – RJ45 | full duplex | auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
Power supply	PCI: 3,3 V and 5 V PCIE: 3,3 V and 12 V Via PCI or PCI Express bus. Follow the instructions in the documentation for your system.
Power consumption	typical T_{amb} = 25 °C Throughput 10 % (100 Mbit) = 2,72 W max. T_{amb} = 70 °C max. throughput = 4,2 W
Maximum current consumption (US = Min, T_{amb} = Max)	
FL MGUARD 4102 PCI	3,3 V = 0,935 A 5 V = 0,33 A
FL MGUARD 4102 PCIE	3,3 V = 0,935 A 12 V = 0,1 A
Typical current consumption (T_{amb} = 25 °C, duty cycle 10 % bandwidth)	
FL MGUARD 4102 PCI	3,3 V = 0,52 A 5 V = 0,24 A
FL MGUARD 4102 PCIE	3,3 V = 0,52 A 12 V = 0,093 A
Diagnostic tools	Status and diagnostic LEDs | log files
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor
Ambient temperature (operation)	-40°C ... +60 °C
Ambient temperature (storage/transport)	-40°C ... +70 °C
Permissible humidity (operation)	5 % ... 95 % (non-condensing)
Degree of protection	Depending on the type of installation, depending on the host system
Protection class	Class III (VDE 0106; IEC 60536, indoor use only)
Air pressure (operation)	68 kPa ... 108 kPa, 3000 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Pollution degree	2

General data	
Overvoltage category	None
Mounting position	Free PCI or PCI Express slot on the host system
Connection to functional ground	Via slot plate

Firmware and power values	
Supported firmware	mGuard 10.1.0 or later
Management support	Web-based management (HTTPS) | SSH | GAI Config | SD card

Network interfaces	
Properties of RJ45 connections	
Number	2
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm^2 to 0.22 mm^2
Cable impedance	100 ohm
Transmission speed	10/100/1000 Mbps/s
Maximum conductor length (twisted pair)	100 m (per segment)

Conformance with EMC directives	
Developed in accordance with IEC 61000-6-2	
Noise emission in accordance with EN 55016-2-1:2014 (conducted noise emission)	Class B
Noise emission in accordance with EN 55016-2-3:2010 + A1:2010 + AC:2013 + A2:2014 (radiated noise emission)	Class A
Immunity in accordance with EN 61000-4-2 (IEC 1000-4-2) (ESD) Contact discharge: Air discharge: Indirect discharge:	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion B Test intensity 3, criterion B Test intensity 3, criterion B
Immunity in accordance with EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements in accordance with DIN EN 61000-6-2 Test intensity 3, criterion A

Conformance with EMC directives	
Immunity in accordance with EN 61000-4-4 (IEC 1000-4-4) (burst)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 3, criterion A
Immunity in accordance with EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements in accordance with DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B

Please observe the following notes

General terms and conditions of use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any technical changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on modifications to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current standard Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.net/products

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

PHOENIX CONTACT Development and Manufacturing, Inc.
586 Fulling Mill Road
Middletown, PA 17057
USA

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Fax: +49 5235 3-41200
E-mail: info@phoenixcontact.com
phoenixcontact.com

110192_en_08
Order No. —08

INSPIRING INNOVATIONS